Divat lett a benzinkutak elleni kibertámadás

2024. január 02. 11:28 - Csizmazia Darab István [Rambo]

Sokan emlékezhetnek a Colonial Pipeline elleni incidensre, ahol 2021. májusában egy több hetes, **az Egyesült Államok keleti partján jelentkező üzemanyaghiányt és hatalmas veszteséget okozó időszak vette kezdetét.** Bár a cég megfizette a 4.4 millió dollárnyi (akkor 1.27 milliárd HUF) váltságdíjat, a válság így is elhúzódott, mert a cserébe kapott visszafejtő eszköz olyannyira lassú volt, hogy helyette inkább saját korábbi biztonsági mentéseikből állították helyre a rendszert.

Ezúttal szintén a kibertérben hajtottak végre hasonló támadást, ahol még **a karácsonyi ünnepek előtt zavarták meg az iráni benzinkutak többségét, beszámolók szerint 70%-ánál voltak fennakadások.**

Az iráni olajminiszter megerősítette, hogy az ország benzinkútjainak informatikai rendszereit megtámadták, és a média **a töltőállomások előtti hosszú sorokról, forgalmi dugókról tudósított, ezek főként Teheránban voltak jellemzőek**. Az ilyen károkozó akciók **elsősorban politikai indíttatásúak**, de sok esetben emellett jelen van az anyagi haszonszerzésre való törekvés is.

Időközben a Predatory Sparrow (magyarul Ragadozó veréb) nevű csoport vállalta magára a támadást, és arra hivatkoztak, hogy a Közel-Keleten zajló gázai konfliktus volt az ok. Állításuk szerint bár képesek lettek volna az összes benzinkút teljes megbénítására is, ám a mentők, tűzoltók és egyéb segélyszervezetek iránti kíméletből hagytak ki lehetséges célpontokat.

Az akció állítólag egy korábbi iráni hackerek által irányított, az Iszlám Köztársaság nevében elkövetett észak-izraeli Ziv Kórház elleni kibertámadásra való izraeli válaszcsapás. Bár ott nem sikerült lebénítani az orvosi kezeléseket, a behatolók személyes adatokat loptak el a kórház rendszereiből.

Összességében azt látjuk, hogy **a Stuxnet 2010-es színre lépése után eléggé elszabadult a pokol, mára már minden ország állami kártevőket fejleszt, és a kibertér valódi hadszíntér lett. Ahol a harcban álló és az egyáltalán nem álló országokra is komoly csapásokat mérnek.**

Csak éppen sokszor ártatlan civileknek árt ez a legtöbbet, a kórházak kényszerű leállása, az üzemanyaghiány, vagy az áramszünet nekik okoz kiemelten szenvedést. Vírusvédelmi szempontból pedig az a tapasztalat, hogy minden célzott akcióhoz használt egyedi kártékony kód előbb-utóbb nyilvánosságra kerül, módosítják, másolják, ingyenesen terjesztik, vagy éppen eladják, és a kiberfegyverek nem tarthatók kordában.

Szólj hozzá!
Címkék: leállás izrael irán politikai benzinkút állami kártevő szabotázs kiberfegyver

Ajánlott bejegyzések:

Tíz tiszta víz, ha nem tiszta, vidd vissza

Én és én meg a hibás frissítés

Végképp eltörölni

Újabb rombolás brit kórházakban

Újabb rombolás brit kórházakban

Jöhet-e QR kódos átverés postai papír levélben?

Jöhet-e QR kódos átverés postai papír levélben?

Én és én meg a hibás frissítés

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz






Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Nő a QR-kódos visszaélések száma

2024. január 04. 10:09 - Csizmazia Darab István [Rambo]

Kicsit az Orange is the new black sorozat címre utalva megállapíthatjuk, hogy lassan a quishing az új phishing, vagyis adathalászat.

Bár sokan még nem is halották ezt a kifejezést, **a quishing a könnyen kezelhető QR kódokkal való adathalászati módszert takarja, amelynél a mobil kamerájával beolvasva gyorsan megnyílik egy weboldal, jelentkezik egy telepíthető app. De a kód ezeken túlmenően akár telefonhívást, SMS üzenetet vagy digitális fizetést is indíthat.**

Bár a bűnözők már a Covid időszak kezdete óta kísérleteztek ezzel, **mostanra egyre gyakoribb az ilyenfajta támadási próbálkozás.**

A QR kód rosszindulatú URL-t tartalmazhat, amely egyszerűen egy adathalász webhelyre irányítja át a látogatót, akik ott akaratlanul is kiadhatnak magukról bizalmas személyes vagy pénzügyi adatokat. A Perception Point **kutatása szerint a quishing 427%-os növekedést mutatott tavaly** augusztus és szeptember között.

A vizsgált időszakban a korábbi 2%-ról 9.5%-ra ugrott a beszkennelhető kódokkal elkövetett visszaélések száma. A támadások mértéke jól érzékelhető, hiszen **az összes rosszindulatú incidenshez viszonyítva a quishing támadások aránya 0.4%-ról 8.8%-ra nőtt.**

Az amerikai Federal Trade Commission (FTC) külön figyelmeztetést adott ki ezzel kapcsolatosan. A csalók változatos módon élnek vissza a felhasználók jóhiszeműségével, figyelmetlenségével. Előfordult olyan eset is, hogy **átragasztották a parkolóórákon található eredeti QR kódot egy rosszindulatú linket tartalmazó másikra.**

Az is megtörtént, hogy **e-mailben vagy SMS-ben csomag kézbesítési problémára hivatkozva küldenek ilyen kódot, ahol állítólag a postázási időpont átütemezését, vagy valamilyen hiányzó extra**

díjfizetési lehetőséget kínálnak. De az is egy trükk, hogy valamilyen fiókunk "megerősítésére" kérnek minket, mert "gyanús tevékenységet" észleltek benne. **Hát ekkor lenne az ideje a felhasználónak gyanakodnia, hogy éppen ez a kérés maga a gyanús tevékenység.**

Mit tegyünk és mit ne tegyünk, hogy megóvjuk magunkat az egyre gyakrabban felbukkanó QR kódos csalásoktól? Hasonlóan a kéretlen spam üzenetekhez, itt is legyünk óvatosak, ha váratlanul felbukkan egy QR kód egy gyanús üzenetben, e-mailben. **Védjük online fiókjainkat erős jelszavakkal és többtényezős hitelesítéssel.**

Használjunk **minden internetes eszközünkön internet biztonsági programot**, amely képes detektálni és blokkolni az adathalászt kísérleteket, emellett pedig **frissítsünk rendszeresen** az operációs rendszert és az alkalmazói programjainkat mind a PC-n, mind a mobil eszközeinken.

Szólj hozzá!
Címkék: statisztika csalás átverés ftc trade megtévesztés adathalászat qrcode federal comission quishing

Ajánlott bejegyzések:

[Jöhet-e QR kódos átverés postai papír levélben?](#)

[Adathalászat vagy jófogás?](#)

[Csomagja érke... Na most már elég!](#)

[Jöhet-e QR kódos átverés postai papír levélben?](#)

[Adathalászat vagy jófogás?](#)

[Csomagja érke... Na most már elég!](#)

["NEM TUDJUK KISZÁLLÍTNI A CSOMAGÁT"](#)

[Utolsó emlékeztető a fiók felfüggesztése előtt](#)

[Utolsó emlékeztető a fiók felfüggesztése előtt](#)

[Utolsó emlékeztető a fiók felfüggesztése előtt](#)

[Utolsó emlékeztető a fiók felfüggesztése előtt](#)

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Új év, régi-új fogadalmak

2024. január 09. 07:44 - Csizmazia Darab István [Rambo]

A január jó alkalom arra, hogy rendet tegyünk nem csak a fizikai környezetünkben, hanem a minket körülvevő virtuális világban is. Érdemes lehet tudatosabban óvni az adatainkat, mert ezzel az online csalók dolgát megnehezítenénk. **2023-ban 10 milliárd forintot csaltak ki magyar károsultaktól, és ez az összeg évről évre csak nő.** Aki eddig esetleg halogatta volna, annak is ideje lenne jobban kézbe venni a kiberbiztonságot.

Újabb és újabb módszereket vetnek be a csalók, hogy megszerezzék személyes vagy épp banki adatainkat: 2023-ban főként nemlétező csomagok vagy rendőrségi adategyeztetés miatt küldtek banki adatokat kérő sms-eket, vagy épp az online piactéren árult holminkat szerették volna megvenni, de ehhez bankkártyaadatainkat kérték. A legkifinomultabb módszer az úgynevezett call centeres csalás volt, amikor a bűnözők banki ügyintézőnek adták ki magukat és azt ígérték, hogy "biztonságba" helyezik a számlánkon lévő pénzünket.

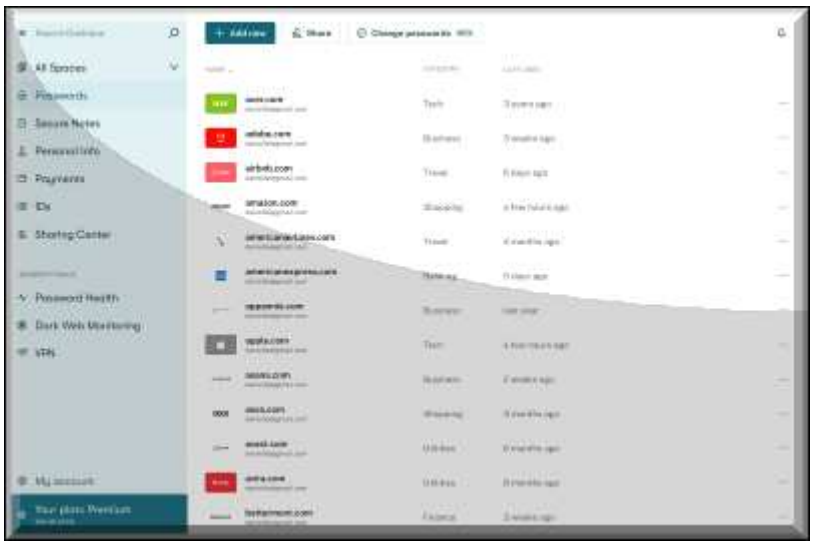
Egészen biztos, hogy 2024-ben újabb módszerekkel is szélesedik majd a csalások palettája, de az említettek is tovább fejlődhetnek, még hihetőbbé válhatnak. **Van néhány olyan alapvető lépés, melyet ha megteszünk, akkor bármilyen új átverést találnak is ki a bűnözők, jó eséllyel meg tudjuk védeni magunkat és az adatainkat.**

1. **Kezdjünk el erős, egyedi, 15-20 karakteres jelszavakat**, sőt inkább jelmondatokat használni. Ha mindenhol ugyanaz a jelszavunk, akkor ha egy helyen incidens történik, akkor az összes fiókunkba bejutnak illetéktelenek.

2. Használjunk megbízható jelszókezelő alkalmazást.

3. Védjük a wi-fi hálózatunkat erős, nem alapbeállítású jelszóval.

4. **Ne használjunk nyílt, ingyenes wi-fi hálózatokat,** főleg online vásárláskor, bizalmas ügyek intézésekor.



5. A két- vagy többfaktoros hitelesítés nagyobb védelmet biztosít az adathalászokkal és a csalókkal szemben - állítsuk be mindenhol, ahol lehet!

6. **Rendszeresen frissítsük**, és tartsuk naprakészen az eszközeinket, szoftvereinket.
https://www.welivesecurity.com/2022/10/24/5-reasons-keep-software-devices-up-to-date/

7. **Ne mentsük el a személyes és/vagy pénzügyi adatokat online fiókokban, böngészőkben.** Bár körülményesebb minden egyes alkalommal jelszószéfből előhívni az adatokat, ám ez sokkal biztonságosabb eljárás.

8. **Használjunk virtuális kártyát** online fizetésekhez, melyre mindig csak a vásárlás előtt töltünk fel annyi pénzt, amennyit éppen kifizetünk.

9. **Ha a bankunk nevében hívnak és adatokat kérnek, tegyük le** a telefont és hívjuk vissza mi magunk a bank ügyfélszolgálatát. A jegybanki jelentés szerint 3 éve még a bankkártya csalási károk többségét a hitelintézetek viselték, az ügyfelek kára 2019-ben még "csak" 8% volt. 2023 első negyedévében azonban már 83% volt az olyan incidens, ahol egyértelműen az ügyfél hibázott, és emiatt a bank nem térítette meg a kárt.

10. **Gondoskodjunk arról, hogy minden eszközünk és számítógépünk** megbízható forgalmazótól származó, kártékony szoftverek elleni védelemmel rendelkezzen (pl. az ESET megoldásai).

11. **Informálódjunk: a Hackfelmetszők kiberbiztonsági podcastben** rendszeresen beszámolunk a legújabb csalásformákról, a védekezés módjáról mobil- és asztali eszközökön, az adataink védelmének fontosságáról.

12. **Sose kapkodjunk, ne hagyjuk sürgetni magunkat!** Blokkolt csomagra hivatkozó sms esetén álljunk meg és gondoljuk végig: egyáltalán várunk csomagot külföldről? Minden kattintás előtt álljunk meg egy pillanatra és gondoljuk át, hogy van-e bármi gyanús az üzenetben, legyen az a feladó, a link furcsasága vagy a szokatlan nyelvi fordulatok.

13. **Ne nyissunk meg mellékletet ismeretlen feladótól,** főleg tömörített állományokat, kettős kiterjesztésű fájlokat ne.

14. **Készítsünk rendszeresen offline biztonsági mentést adatainkról**, amelyek segítségével egy esetleges fertőzés esetén azok visszaállíthatók. Ezeket olyan külső adathordozókon tároljuk, amelyek csak a mentés ideje alatt vannak csatlakoztatva a számítógéphez.

15. **A közösségi média felületeken vagy csevegőkben is gondolkodjunk** még kattintás előtt, mielőtt bármilyen hivatkozást megnyitnánk.

16. **Kapcsoljuk ki az operációs rendszer "Automatikus lejátszás" funkcióját.** Ezzel megakadályozhatjuk az ártalmas folyamatok automatikus futtatását olyan csatlakoztatott külső adathordozókról, mint például az USB memória kártyák vagy a pendrive-ok.

17. **Ransomware támadás esetén** bontsuk az internet kapcsolatot, ha gyanús valami, ezzel megszakad a kommunikáció a zsarolóvírus és vezérlőszervere között, így megakadályozva a fájljaink további eltitkosítását.

18. Alkalmazásokat csak megbízható forrásból telepítsünk, a telepítendő alkalmazás letöltése előtt nézzük meg, hogy milyen engedélyeket kér a működéséhez. Amennyiben olyan területekhez is kér hozzáférést, amit az alkalmazás fő funkciója nem indokol, inkább ne telepítsük.

19. Használjunk VPN alkalmazást, amely biztosítja, hogy a netes kapcsolatunk titkosított és védett legyen a támadókkal szemben, akik a személyes adatainkra, jelszavainkra vagy banki adatainkra vadásznak.

Ha ezeket a lépéseket idén már betartjuk, akkor máris megnehezítettük a kiberbűnözőknek dolgát és a 2024-es esztendő sokkal kevésbé eredményes évünk lehet.

1 komment
Címkék: tippek tanácsok kiberbiztonság 2024.

Ajánlott bejegyzések:

Bankkártyával biztonságosabban
A legnépszerűbb 2024-es posztok
Kellemes Karácsonyi Ünnepeket
Kell-e tárgyalni, szabad-e fizetni?

Bankkártyával biztonságosabban
A legnépszerűbb 2024-es posztok
Kellemes Karácsonyi Ünnepeket
Kell-e tárgyalni, szabad-e fizetni?

Kibermalac színre lép

Kommentek:

keresés

tweetz

Facebook

Tovább a Facebook-ra

Kibermalac színre lép

2024. január 11. 10:35 - Csizmazia Darab István [Rambo]

Sok féle korosztálynak íródik ez a blog, ezen belül pedig **mindig is törekvés volt a gyermekekkel kapcsolatos tartalmak alkalmankénti említése, például az iskola kezdéskor a digitális eszközökkel kapcsolatban, a karácsonyi ünnepek közeledtével hogy mire figyeljünk, ha gépet vagy telefont kap az iskolás, de időnként a zaklatás, emellett az online tér biztonsága szülőként és gyerekként is többször előkerült már itt.**

Amikor megkérdeztük a ChatGPT-t, hogy **mi történik akkor, ha egy olyan társasjátékkal játszik egy 99 évnél idősebb személy, aminek a dobozára az van írva, hogy 4-99 kor közöttieknek, roppant kíváncsiak voltunk a válaszra. Talán felrobban az Univerzum, esetleg egy szellem azon nyomban kiüti az illető kezéből a dobókockát, vagy ilyesmi?**

Ezzel szemben a chatbot ezt írta: "*Egy 99 évnél idősebb személy biztonságosan játszhat egy olyan játékkal, amelyet 4-99 éves korosztálynak terveztek. A játék kijelölése inkább csak ajánlás, semmint szigorú korlátozás.*"

Mi most **az alsó tagozatos gyerekekre és szüleikre gondolva mutatjuk be Kibermalacot (hála a nagyszerű Tengr.ai szolgáltatásnak), aki kérdez, érdeklődik az internetes biztonság iránt, és igyekszik kiigazodni az online térben és persze megbeszélni mindezt a barátaival, szüleivel.**

Apropót sok dolog adhat ehhez: közeleg a Biztonságos Internet idei világnapja, emellett már vagy 14 éve, hogy fel lett vetve, legyen hivatalos iskolai tananyag az internet biztonság már első osztályos kortól, ám ez az idő sajnos mindeddig még nem érkezett el.

Korábbi könyv ajánlóinkban már többször is hivatkoztunk Will Geddes: Szülők nagy mobilkönyve kötetére, amelyben különféle internetes kockázatokra konkrét, részletes megoldásokat kínál a szerző szülőknek, bátran ajánljuk ezt mindenkinek.

Most viszont a kisiskolás korúak is találhatnak itt könnyen befogadható tartalmat, ám mi nem szabunk ehhez 4-99 éves korhatárt…


Kibermalac kalandjai
Kép és szöveg:
Csizmazia-Darab István
[Rambo]


Tegnap anyukám levelezési fiókját feltörték...


Vajon mit jelent az, hogy feltörték?


Ezt már mindenki tudja: belépnek a fiókodba, elolvassák vagy törlik az üzeneteket, de akár írhatnak is a nevedben...
Apukám szerint a hosszú, bonyolult és egyedi jelszavak biztonságot nyújtanak
A tanár úr szerint hogyan érdemes védekezni?


Az erős jelszó az tényleg fontos, de ezeket sose mentsük el a böngészőben, hanem használjunk inkább jelszószéfet!


Én azt is olvastam, hogy használjunk vírusirtót és frissítsük rendszeresen a szoftvereinket a hibajavítások miatt...


Apukám szerint a kétfaktoros hitelesítés is erősíti a biztonságot, nekem már be is van ez állítva.

Szólj hozzá!
Címkék: internet gyerek képregény jelszó gyermek iskola kiberbiztonság kibermalac tengr.ai

Ajánlott bejegyzések:

[Identitás lopás: nem függ az életkortól](#)

[Egy a jelszónk, tartós 123456](#)

[Elveszett ereklyék fosztogatói](#)

[Hogyan védjék magukat az idősebbek az interneten?](#)

[Az 5 leggyakoribb kibercsalás](#)

[Egy a jelszónk, tartós 123456](#)

[Elveszett ereklyék fosztogatói](#)

[Hogyan védjék magukat az idősebbek az interneten?](#)

[Az 5 leggyakoribb kibercsalás](#)

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Replikák támadása

2024. január 15. 10:28 - Csizmazia Darab István [Rambo]

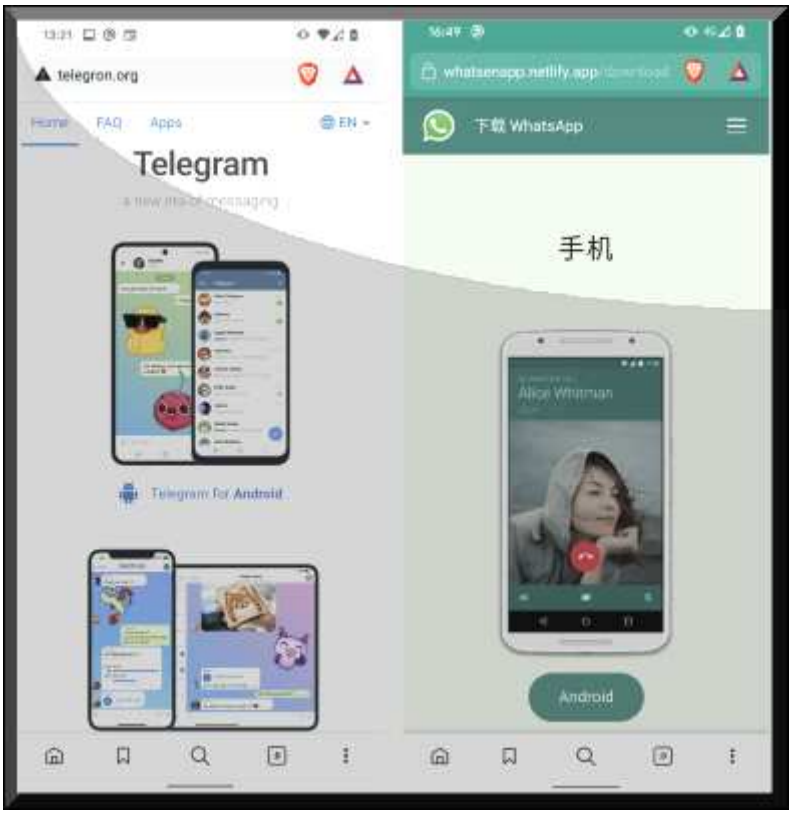
A mobil alkalmazások nagy mértékben átalakították az életünket. Ki tud már tuctanyi telefonszámot fejből, ha van rá app? Emellett láthatóan meg is könnyítették a feladatainkat, egyszerűbbé tették a kapcsolattartást, szinte nélkülözhetetlenekké váltak az évek során iOS és Android platform alatt egyaránt.

A nagyobb versenyzőknek hatalmas felhasználó tábora van, becslések szerint a Signalnak 40 millió felhasználója van, a telegram 700 millióval büszkélkedhet, míg a Whatsapp 2 milliárdos kártyát tehet le az asztalra. Ám mi történik, ha valami aktuális, népszerű, felkapott? Ahogy azt már a spamek esetében is láttuk, visszaélések az ismert névvel.

Ez a folyamat egyáltalán nem új, például népszerű játékok esetén mi is írtunk már róla, és volt már arról is szó, hogyan kerüljük el, hogy egy másolat csapdájába sétáljunk. **A letöltési statisztikákból azonban az látszik, még mindig rengetegen bedőlnek az ilyen másolatoknak, és kártékony alkalmazásokat telepítenek fel maguknak.**

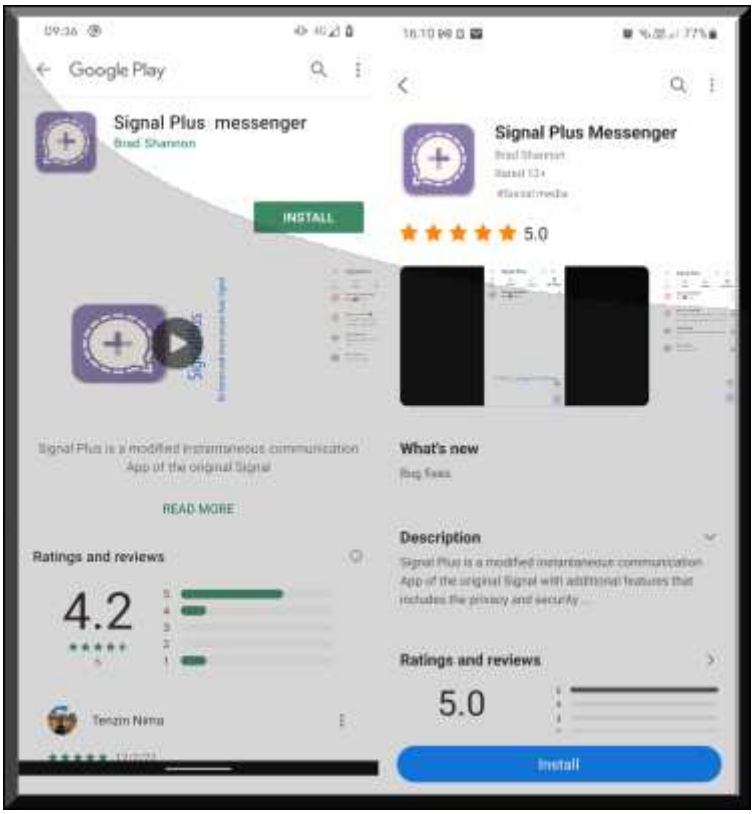
A rosszindulatú fejlesztők nagyon **ügyesen igyekeznek érdekelődést generálni a hamisított alkalmazásaiknak. E-mailben, szöveges üzenetben, a közösségi médiában vagy egyéb a kommunikációs alkalmazásban reklámozzák** ezeket, és igyekeznek hamsi letöltő oldalakra csalogatni a felhasználókat. Időnként legitim, piactéren szereplő alkalmazás kap olyan kártékony frissítést, amit csak később vesznek észre.

Az ilyen másolatok **célja elsősorban a személyes adatok ellopására, banki/pénzügyi információk kifürkészésére, kéretlen reklámok megjelenítésére, a kommunikációs adatok ellopására vagy manipulálására, zsarolóvírus telepítésre vagy rejtetten emelt díjas szolgáltatásokra való feliratkozásokra** irányul.



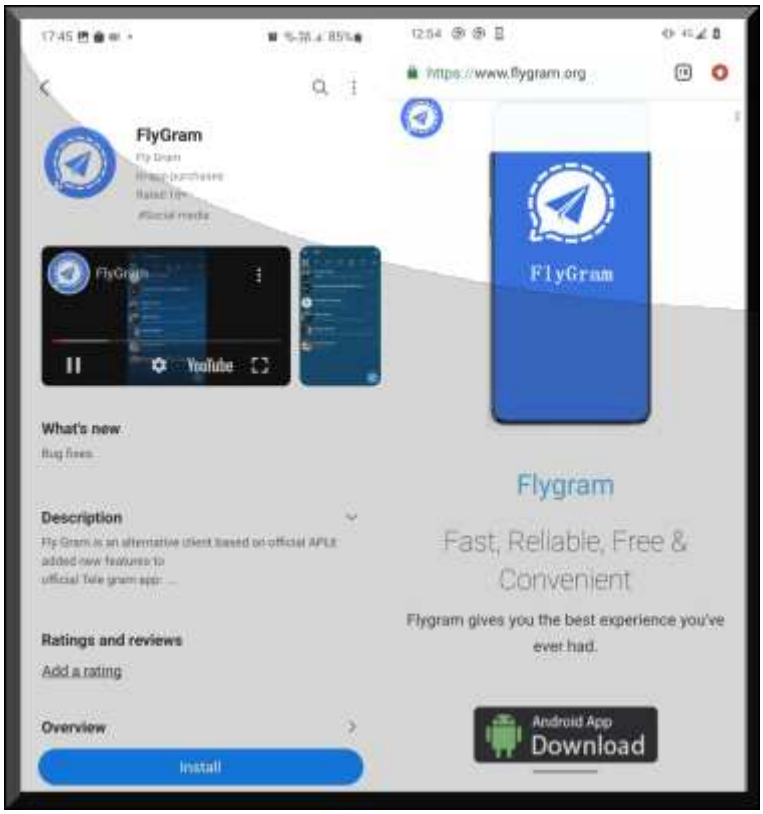
Szakértők úgy láták, ezek a fenyegetések az elmúlt években egyre szélesebb körben elterjedtek. Főképp a már jól ismert alkalmazások nevével élnek vissza, így a WhatsApp és a Signal neve rendszeresen felbukkan a replikák között, de Telegram, YouTube, Meta, Viber is gyakran szerepel a hamisítványok között.

Kínához köthető az Android BadBazaar néven ismert kémprogram, amelyeket Signal és Telegram alkalmazásokba rejtettek és csak késve töröltek a hivatalos Google Play és a Samsung Galaxy Store áruházakból.



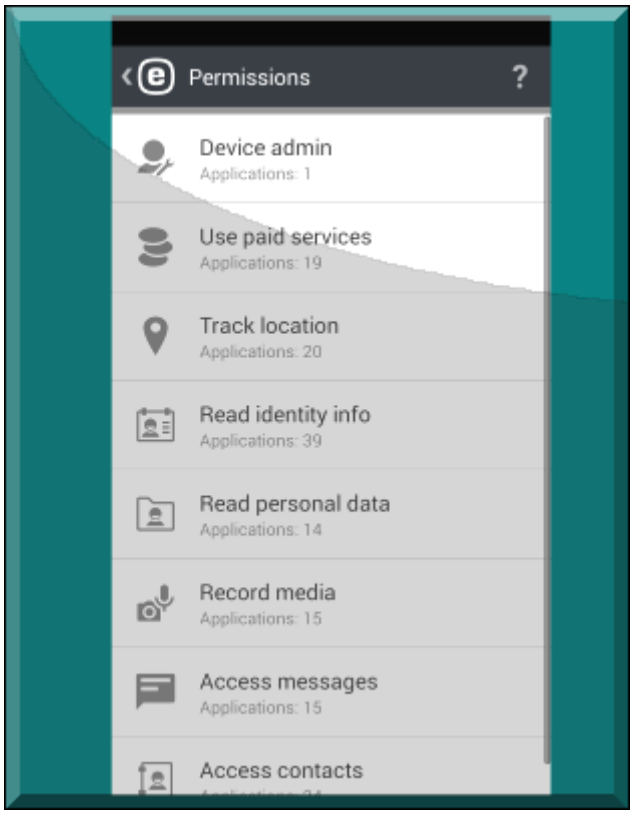
Mire vigyázzunk, hogy elkerüljük a rosszindulatú replikák telepítését? A hivatalos piacterek nem sebezhetetlenek, de még mindig jóval nagyobb eséllyes szűrik ki a kártékony alkalmazásokat, mint a nyitott ellenőrizetlen, így nagyobb kockázatú letöltési oldalak.

Hasznos, ha fut vírusvédelmi alkalmazás a telefonunkon, és rendszeresen frissítjük mind az operációs rendszert, mind az alkalmazói programjainkat a hibajavítások miatt. Amikor letölteni akarunk valamilyen appot, figyeljünk a fejlesztő személyére, ellenőrizzük a reputációját és az app eddigi értékeléseit - különösen az esetleges csalásra utaló megjegyzéseket. A hivatalos neves alkalmazásoknál ez könnyen ellenőrizhető.



Távolítsunk el minden olyan alkalmazást, amelyet nem használunk , így könnyebben nyomon követhető, hogy mik futnak az eszközön. **Kéretlen közösségimédia-üzenetek, e-mailek vagy SMS-ek linkjeire ne kattintsunk**, sok esetben érkezik így kártékony alkalmazás - lásd a FedEx-es Flubot vírus esetét.

Ugyanez igaz a kéretlen online hirdetésekre is, ezek jó része átverés. F**igyeljünk az appok számára megadott engedélyekre is, és csak a feltétlenül szükséges és indokolt kéréseket hagyjuk jóvá. Használjunk biometrikus azonosítást kétlépcsős azonosításhoz, és mellette erős jelszavakat.**



Ha már valamilyen másolat felkerült a telefonunkra, ennek is vannak jelei. **Ha tartósan felugró hirdetéseket észlelünk, vagy szokatlan idegen ikonok jelennek meg a képernyőn, ezek kéretlen alkalmazásokra utalhatnak.**

Az akkumulátor gyors merülése, drasztikus lassulás, az adatforgalom megugrása vagy más furcsa viselkedés is jelezheti kéretlen app jelenlétét. Hasznos, ha **rendszeresen figyelemmel kísérjük a mobilszámlánkat és a banki egyenlegünket is, ezekben minden túl magas költség, vagy indokolatlan terhelés rosszindulatú tevékenységre utalhat.**

Szólj hozzá!
Címkék: mobil alkalmazás csalás átverés replika hamis hamisítás android app visszaélés hasonmás ios welivesecurity.com

Ajánlott bejegyzések:

[Fontos vagy nekem]

[CAPTCHA, amely nem az ember-gép relációt teszteli]

[Új bejelentkezés a felhőnkbe. Vagy mégsem?]

[Fontos vagy nekem]

[Ami majdnem az, az nem az]

[CAPTCHA, amely nem az ember-gép relációt teszteli]

[Új bejelentkezés a felhőnkbe. Vagy mégsem?]

[Csomagja érke... Na most már elég!]

[Csomagja érke... Na most már elég!]

[Csomagja érke... Na most már elég!]

[Csomagja érke... Na most már elég!]

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Közeli helyeken: érintésmentes fizetések

2024. január 18. 16:55 - Csizmazia Darab István [Rambo]

A mágnescsíkos bankkártyák nagyjából 20 évvel ezelőtt jöttek divatba, de amellett, hogy az aláírások szükségessége megnehezítette a tranzakciókat, nem rendelkeztek megfelelő adattitkosítással. Biztonsági szempontból egyértelmű előrelépést jelentettek utódaik, a chipalapú kártyák, melyek az adattitkosítás révén fokozott biztonságot nyújtanak. **Igaz ezek a kártyák továbbra is alkalmasak klónozásra vagy adatlopásra, bár nagyobb kihívás, mint a mágnescsíkos kártyák esetében. Közben pedig az érintésmentes fizetések egyre gyakoribbá váltak.**

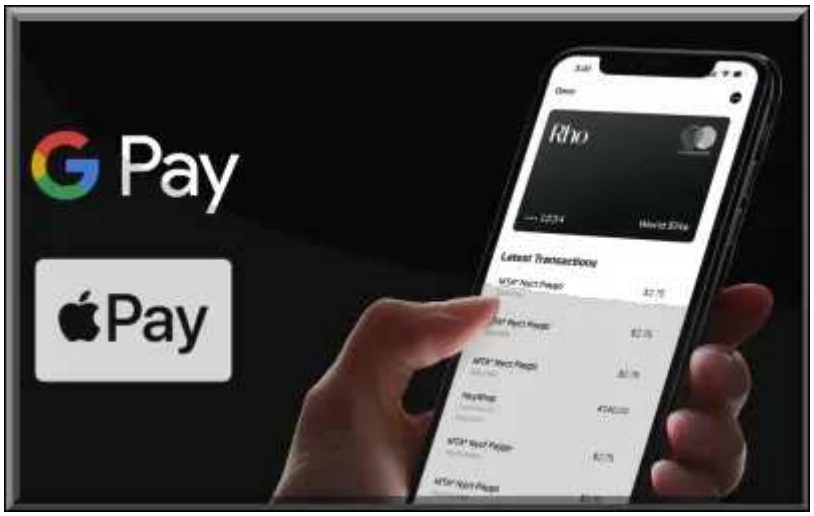
De vajon biztonságosabbak, mint a hagyományos fizetési módok? A 2010-es évek második felében új fizetési szabványként jelent meg a rádiófrekvenciás azonosításból (RFID) kifejlesztett közelmezős kommunikáció (NFC). Ezzel a technológiával az eredeti chipalapú kártyák még felhasználóbarátabbá váltak, mivel **ahelyett, hogy a fizetési terminálokba és ATM-ekbe kellene behelyezni őket, a pénz küldéséhez elég egy NFC-kompatibilis fizetési eszközhöz tartani a kártyát.**

Az érintésmentes kártyák mellett **ma már a telefonok is képesek ezt a funkciót ellátni olyan szolgáltatásokon keresztül, mint az Apple Pay vagy a Google Pay, amelyek a kártyaadatok feltöltése után lehetővé teszik, hogy a telefonnal fizessünk.**

A folyamat, amelyen keresztül az NFC-fizetés történik, nagyon hasonlóan működik a Bluetooth vagy más vezeték nélküli kommunikációs rendszerekhez, mivel rádióhullámokat használ a továbbított információk aktiválásához és hitelesítéséhez. Fizetés esetén a terminál információt kap a telefontól, amelyet aztán feldolgoz és továbbít az elfogadó bank felé, egyszerűsítve és megkönnyítve a tranzakciót.

Az ESET kiberbiztonsági szakértői szerint a vezeték nélküli kommunikáció más módjaival összehasonlítva sokkal nehezebb feltörni, mivel működtetéséhez kis távolságra van szükség. Ez viszont nem jelenti azt, hogy teljesen elkerülhetőek a kibertámadások.

Noha az NFC-technológia biztonságosabb, a támadók különösen a fizetési műveletek során kihasználhatnak bizonyos sebezhetőségeket, hogy megszerezzék, amit akarnak. **Egy kutató például 2021-ben bemutatott egy támadást, amelyben egy Android-alkalmazást fejlesztett. Az appot használva a telefonjával egyszerűen "integetett" az NFC-kompatibilis ATM-eknek, így kártyaadatokhoz és érzékeny információkhoz jutott hozzá**. Ez az említett gépek bizonyos szoftverhibái miatt volt lehetséges, és ez a fizetési terminálok más típusainál is előfordulhat.



Mivel az NFC-fizetések a kényelmi szempontokra épülnek, bizonyos összeghatár és tranzakciószám alatt használatuk során nincs szükség további hitelesítésre (például PIN-kódra), amit egy hagyományos chipalapú kártya megkövetelne. Tehát, ha valaki megszerzi a bankkártyánkat, könnyen lophat a kártyánkkal fizetve anélkül, hogy (egy meghatározott értékig, itthon ez vásárlásonként 15000 forint és 5 tranzakció) kódot kérne a rendszer.

Az NFC a telefonokon is használható, és a biztonság érdekében ehhez az Apple Pay és a Google Pay további biztonsági megoldásokat követel meg PIN-kód, ujjlenyomat, arcszkennelés vagy egyéb, a telefonon rendelkezésre álló funkció formájában.

Emellett mindkét fizetési szolgáltatás csak akkor működik, ha engedélyezve van az eszközön, így kisebb az esélye annak, hogy valaki spontán kezdeményezzen tőlünk fizetést. Ahogy a plasztikkártyák esetében úgy az Apple vagy a Google Pay használatával sem továbbítjuk a számlánk adatait, és ha elveszítjük a készülékünket, ezeket a szolgáltatásokat könnyen letilthatjuk távolról.
https://www.makeuseof.com/how-to-remotely-disable-apple-pay-after-losing-your-iphone-or-apple-watch/

Hogyan tehetjük biztonságosabbá az érintés nélküli fizetéseket?
- Állítsunk be alacsony fizetési limiteket: a bankon keresztül, akár online a pénzintézet applikációján keresztül is meg tehetjük ezt egy limitösszeggel,

amennyiért maximum vásárolhatunk.
- Használjunk telefonos fizetést: bár ezeknek az alkalmazásoknak is lehetnek hibáik, az extra hitelesítési követelmények által mégis biztonságosabbak, mint az NFC-s kártyák.

- Használjunk egyszer használatos vagy virtuális kártyát: ne adjuk meg a saját, bankszámlánkhoz tartozó kártyaadatokat online fizetéskor, hanem használjunk egyszer használatos, vagy olyan virtuális kártyát, melyre csak a vásárlás pillanatában töltjük fel a szükséges összeget.

Természetesen egyetlen biztonsági megoldás sem adhat 100 százalékos garanciát, de már ezekkel az egyszerű lépésekkel is sokat tehetünk azért, hogy csökkentsük az incidensek valószínűségét. És hogy milyen módszerekkel dolgoznak a csalók, hogy megszerezzék a bankkártya adatokat, erről a Hackfelmetszők - Veled is megtörténhet! legutóbbi adásában volt szó részletesebben.

1 komment
Címkék: telefon biztonság podcast bankkártya fizetés nfc hackfelmetszők

Ajánlott bejegyzések:

Hogyan védjék magukat az idősebbek az interneten?

Fontos vagy nekem

Bankkártyával biztonságosabban...

Hogyan védjék magukat az

Mit csinálnak az alkalmazottak

Fontos vagy nekem

Bankkártyával biztonságosabban...

idősebbek az interneten?
a céges gépeken?
Monday járja be Európát

Black Friday és Cyber Monday járja be Európát

Kommentek:

eseslevi 2024.01.19. 07:39:07

Nagyon kíváncsi vagyok, hogy készpénzzel való fizetéssel, vajon hogyan lopják el az adataimat vagy lopják el a pénzemet a bankszámlámról. Plusz, senki nem tudja, hogy hol vagyok, mit vásárolók vagy mit csinálok. Mindenki használja ezeket a készülékeket s aztán picsognak, hogy lehallgatják, követik őket. A kényelemnek ára van.

Válasz erre

keresés

tweetz

LockBit üti Subway, sakk

2024. január 23. 11:48 - Csizmazia Darab István [Rambo]

Ransomware támadás érte az **amerikai multinacionális gyorséttermi franchise láncot, amely szendvicseiről, salátáiról közismert**. A hírhedt orosz hátterű LockBit bűnbanda január 21-én közzétett bejegyzése azt mutatja, hogy egyik leányvállalata **sikeresen feltörte a Subway adatbázisát, és onnan érzékeny adatokat loptak el.**

A közzétett poszt szerint a Lockbit csoport felvette a Subway-t a Tor-adatszivárogtatási webhely áldozatainak listájára, és ott **azzal fenyegetőznek, hogy a váltságdíj ki nem fizetése esetén 2024. február 2-án 21:44:16-kor kiszivárogtatják az ellopott adatokat.**

A bűnözők azt állítják, hogy **több száz gigabájtnyi érzékeny adathoz fértek hozzá, ezek között olyanokat is, mint az alkalmazottak fizetése, a franchise jogdíjak, a master franchise jutalékok mértéke, az éttermek forgalmát és más pénzügyi információkat. Adatmintákat vagy bizonyítékokat egyelőre nem lehetett látni az adatlopással kapcsolatban.**

A Subway a világ **egyik legnagyobb gyorséttermi szolgáltatója, mintegy 37 ezer telephellyel. A cég mobilalkalmazást is kínál, amelyet több mint 10 millióan töltöttek le a Google Play Áruházból, így az adatok köre tényleg hatalmas lehet.**

A cég egyelőre nem ismerte el, nem kommentálta az esetet, szűkszavúan annyit nyilatkoztak, hogy vizsgálják az állítás valóságtartalmát.

Emlékezetes, hogy tavaly ősszel a partneri alvállalkozók teljesítményével elégedetlen LockBit vezetőség szigorításokat és előírásokat fogalmazott meg, **többek közt a megtámadott intézmény éves árbevételéhez igazodó minimális váltságdíjat kell alkalmazniuk, és szigorúan tilos az eredetileg kért összeg 50%-át meghaladó kedvezményt adniuk.**

Mivel a Subway nem tőzsdén jegyzett vállalat, ezért bevételi adatait ritkábban hozzák nyilvánosságra. **Így hivatalos adatok nélkül a LockBit valószínűleg saját becsléseket készített, a korábbi esetek alapján gyaníthatóan itt is több tízmillió dolláros követeléssel állhattak elő.**

Egyelőre hivatalosan nem tudni, pontosan mekkora váltságdíjat követelnek, ahogy azt sem, valóban történt-e tényleges adatszivárgás, illetve hogy ha igen, lesz-e fizetési hajlandóság a vállalat részéről.

Mindenesetre a LockBit csoport már a második egymást követő évben őrizte meg vezető pozícióját a legaktívabb zsarolóvírus szereplőként.

Szólj hozzá!
Címkék: hálózat orosz subway váltságdíj ransomware zsarolóvírus doxing lockbit

Ajánlott bejegyzések:

Újabb rombolás brit kórházakban
A kriptobevételek felett az égbolt felhőtlen
Kórházak a pácban II.


Újabb rombolás brit kórházakban
A kriptobevételek felett az égbolt felhőtlen
Kórházak a pácban II.
8 kórház, 30 klinika, 2.5 millió betegadat

[LockBit piacgazdaság és tervgazdálkodás]

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Amikor a suszter cipője lyukas II.

2024. január 29. 11:00 - Csizmazia Darab István [Rambo]

A Microsoft elismerte, hogy orosz támadók sikeresen **behatoltak a hálózatába és belső e-maileket, illetve fájlokat loptak el különféle vezetőktől és egyéb munkatársaktól.**

A támadást a Midnight Blizzard nevű csoport - korábban APT29 vagy Cozy Bear néven is hivatkoztak rájuk - követte el. Az úgynevezett utilized password spray attack technika, miszerint kijátszva a bruteforce elleni védelmeket, és radar alatt maradva próbálgatják kitalálni a feltételezett gyengén védett fiókok jelszavát.

Minden kísérlet után kivárnak, és csak egy idő után következik az újabb ténykedés egy másik jelszóval, így a védelem nem észlel rövid időn belül több sikertelen bejelentkezést, ami abszolút gyanús jel lenne.

Ha a gyengén védett korlátozott fiókba történő behatolás végül sikeres, akkor pedig a **cél a jogosultság növelése, új fiókok regisztrálása, admin jogok megszerzése, és bizalmas adatok kinyerése, ami jelen esetben a Microsoft felső vezetőinek és egyéb alkalmazottainak vállalati postaládájából való levelekhez való hozzáférést jelentette.**

A jelek szerint a Cozy Bear a lakossági széles sávú hálózatokat használta proxyként, hogy **úgy nézzen ki a forgalmuk, mintha az IP címek valódi, otthonról dolgozóktól származó legitim forgalom lenne.**

Az eset külön érdekessége, hogy az incidensben érintett feltört vállalati fiók még csak nem is rendelkezett többtényezős hitelesítéssel. Hogy a kötelező Microsoft policy irányelvek és útmutatások ellenére ez hogy történhetett meg, arra az a válaszuk, hogy ez egy korábban létrehozott fiók. Ez a bizonyos fejlesztői tesztfióknak nevezett account segítségével viszont adminisztrátori szintű hozzáférést lehetett létrehozni belső hálózatok éles szervereihez.

Reméljük, érdekességképpen egyszer kiderül majd az is, hogy mi volt ennek a bizonyos fióknak a jelszava, remélhetőleg nem "microsoft123".

Szólj hozzá!
Címkék: microsoft mail orosz password blizzard attack feltörés spray midnight utilized apt29 cozybear

Ajánlott bejegyzések:

Jelszó világvége

Újabb rombolás brit kórházakban

Elveszett ereklyék fosztogatói

A kriptobevételek felett az égbolt felhőtlen

Jelszó világvége

Újabb rombolás brit kórházakban

Elveszett ereklyék fosztogatói

A kriptobevételek felett az égbolt felhőtlen

Support kérdésre adathalász válasz

Support kérdésre adathalász válasz

Support kérdésre adathalász válasz

Support kérdésre adathalász válasz

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Biztonságos-e a Temu?

2024. február 01. 09:44 - Csizmazia Darab István [Rambo]

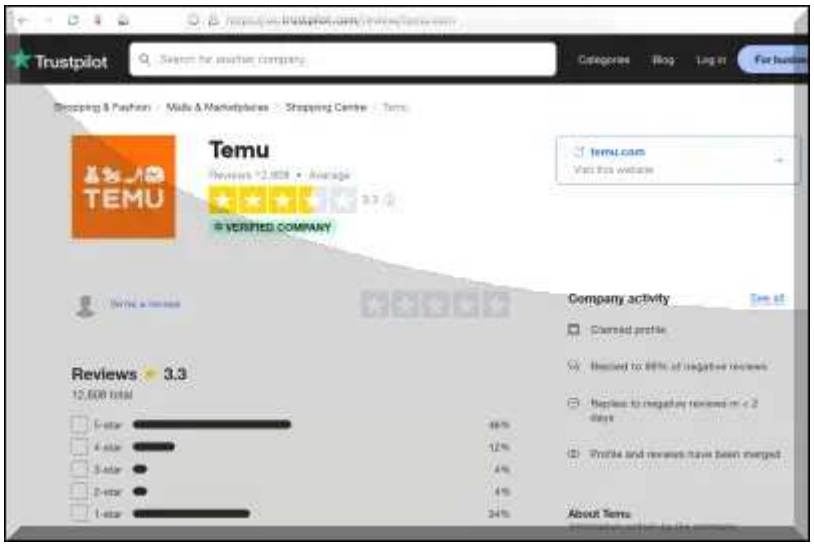
Valószínűleg nincs olyan közösségi média használó, aki az elmúlt időszakban ne találkozott volna **a világ egyik legnagyobb webáruháza, a Temu hirdetéseivel**. A több tízmilliósra becsült termékkínálatnak és a rendkívül alacsony áraknak köszönhetően az oldal tömegeket vonz, és a Temu a világ legtöbbször letöltött vásárlási appja lett.

Vajon a webáruház rohamos előretörése milyen hatással van a termékbiztonságra és jogszerűen működik-e? A Temu az egyik legnagyobb kínai online kereskedelmi szolgáltató, a Pinduoduo nyugati piactere, amely lehetőséget ad a vásárlóknak, hogy olcsó termékeket forgalmazó kínai gyártóktól vásároljanak. A felhasználók krediteket is szerezhetnek a későbbi kedvezményes vásárlásaikhoz, akár az oldalon felbukkanó szerencsekerék megforgatásával vagy más vásárlók meghívásával.

Ennek ellenére sok vásárló fogalmazott meg negatív véleményt a webshoppal kapcsolatban. Jelen pillanatban az oldal mindössze 2,5-ös értékelést ért el az ötből az amerikai Better Business Bureau látogatóitól, míg a Trustpilot oldalon az értékelések harmada egycsillagos.

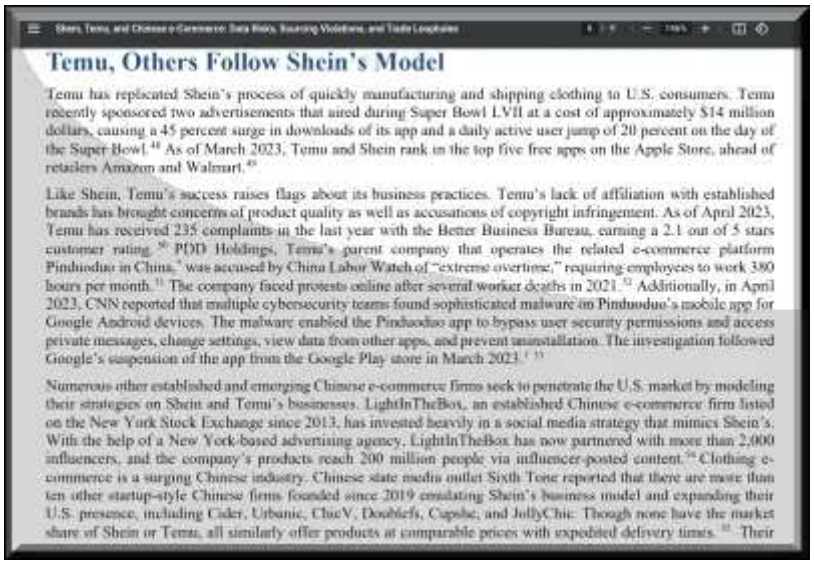
A felhasználók gyakran az e-mail fiókjukba érkező spamek miatt kritizálják a Temut, de sok bírálatot kaptak a pénzvisszatérítés nehézsége, valamint a termékek gyenge minősége miatt is, illetve az is előfordul, hogy az áru meg sem érkezik a vásárlóhoz.

Aggályok merültek fel azzal kapcsolatban is, hogy a webáruházban elérhető termékeket esetleg kényszermunkával állítják elő, illetve **többször is hamis márkajelzésekkel való visszaélésről lehetett olvasni, legutóbb például a HP termékek esetében.**



Az egyik amerikai kormányzati ügynökség személyes adatok veszélyeztetésével vádolta meg a Temut és a szintén kínai Shein webáruházat, ami felidézi azokat az adatfelhasználást övező aggodalmakat, amelyek korábban egy másik rendkívül népszerű kínai online platformot, a TikTokot övezték. Emellett mint minden népszerű sok felhasználóval rendelkező dolog esetében **ez a webáruház is felkeltette a csalók figyelmét.**

Az ESET szakértői összegyűjtötték **azokat az átverési taktikákat, amiket a Temu webshopjában a leggyakrabban észleltek.**



Temu, Others Follow Shein's Model

Temu has replicated Shein's process of quickly manufacturing and shipping clothing to U.S. consumers. Temu recently sponsored two advertisements that aired during Super Bowl LVII at a cost of approximately $14 million dollars, causing a 45 percent surge in downloads of its app and a daily active user jump of 20 percent on the day of the Super Bowl.[48] As of March 2023, Temu and Shein rank in the top five free apps on the Apple Store, ahead of retailers Amazon and Walmart.[49]

Like Shein, Temu's success raises flags about its business practices. Temu's lack of affiliation with established brands has brought concerns of product quality as well as accusations of copyright infringement. As of April 2023, Temu has received 235 complaints in the last year with the Better Business Bureau, earning a 2.1 out of 5 stars customer rating.[50] PDD Holdings, Temu's parent company that operates the related e-commerce platform Pinduoduo in China,[51] was accused by China Labor Watch of "extreme overtime," requiring employees to work 380 hours per month.[51] The company faced protests online after several worker deaths in 2021.[52] Additionally, in April 2023, CNN reported that multiple cybersecurity teams found sophisticated malware on Pinduoduo's mobile app for Google Android devices. The malware enabled the Pinduoduo app to bypass user security permissions and access private messages, change settings, view data from other apps, and prevent uninstallation. The investigation followed Google's suspension of the app from the Google Play store in March 2023.[53]

Numerous other established and emerging Chinese e-commerce firms seek to penetrate the U.S. market by modeling their strategies on Shein and Temu's businesses. LightInTheBox, an established Chinese e-commerce firm listed on the New York Stock Exchange since 2013, has invested heavily in a social media strategy that mimics Shein's. With the help of a New York-based advertising agency, LightInTheBox has now partnered with more than 2,000 influencers, and the company's products reach 200 million people via influencer-posted content.[54] Clothing e-commerce is a surging Chinese industry. Chinese state media outlet Sixth Tone reported that there are more than ten other startup-style Chinese firms founded since 2019 emulating Shein's business model and expanding their U.S. presence, including Cider, Urbanic, ChicV, Doublefs, Cupshe, and JollyChic. Though none have the market share of Shein or Temu, all similarly offer products at comparable prices with expedited delivery times.[55] Their

Kattintásvadász linkek hírességek meztelen fotóinak állítólagos kiszivárgásáról
A Temu felületén levásárolható összeg vagy kupon szerezhető, ha másokat is vásárlásra ösztönzünk az oldalon, és ők felhasználják az ajánlói kódunkat. A csalók a közösségi médiában trükkös megoldással gyűjtenek maguknak krediteket.

Például fotókat tesznek közzé egy hírességről a Twitteren vagy a TikTokon egy olyan üzenettel, ami arra utal, hogy a felhasználók a sztárok aktképeihez férhetnek hozzá, ha beírják a kódot a Temu oldalán. Képek természetesen nincsenek, a csalók egyszerűen kedvezményeket gyűjtenek.

Hamis Fortnite/Roblox kedvezmények
A fenti taktikához hasonlóan **a csalók gyakran ingyenes Roblox Robux ajándékkártyát hirdetnek a közösségi médiában, amellyel a felhasználók fejleszthetik avatárjukat vagy különleges képességeket vásárolhatnak a játékplatformon. Ehhez mindössze annyit kell tenniük, hogy beírják az ajánlókódjukat a Temu felületén.**

Szintén népszerű a ritka Fortnite karakter kinézetek, azaz skinek megszerzésének ígérete, amiből persze semmi sem igaz. A csalók csupán

kihasználják a közösségi média felhasználók kíváncsiságát, valamint azt a tényt, hogy a Temut nem ismeri mindenki.

Hamisított termékek
Noha a Temu testvérvállalata, a Pingduoduo szerepel azon a listán, amelyen az Egyesült Államok a szellemitulajdon-hamisító piactereket veszi sorra, jelenleg nincs arra utaló bizonyíték, hogy a Temu kizárólag hamisított termékeket forgalmazna.

Születtek viszont beszámolók olyan másolatokról, amelyek a hamisítás határát súrolják. **Ha egy felhasználó rákeres például egy Apple-termékre, akkor az eredetihez hasonlító termékeket talál, töredék áron, ami azért gyanúra ad okot.**

Fake celebrity photo leak videos flood TikTok with Temu referral codes

By Lawrence Abrams

September 24, 2023 10:11 AM 3

TEMU

TikTok is flooded with videos promoting fake nude celebrity photo leaks used to push referral rewards for the Temu online megastore.

Temu is an online shopping site offering millions of products at very low prices, most of which are shipped directly from China.

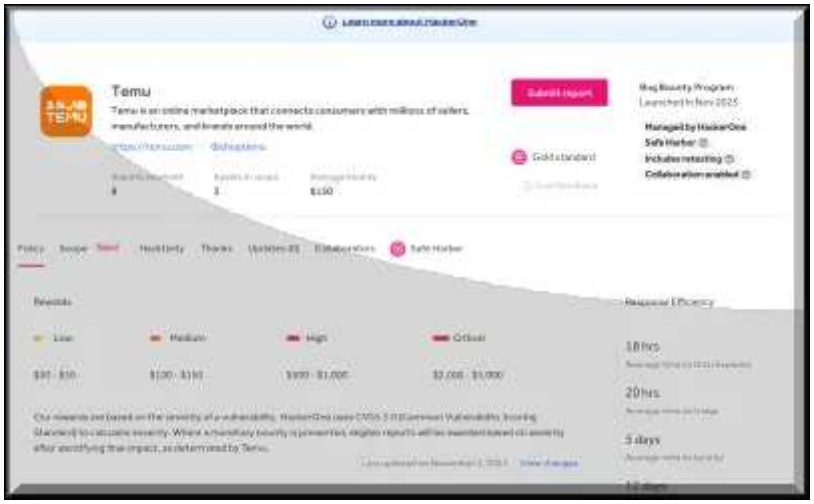
There has been a lot of controversy regarding the online store since its launch in September 2022, with some thinking it's a scam and others loving the cheap merchandise they receive.

To promote the site, Temu allows customers to create referral numbers and links to be shared with family, friends, and social media to earn store credit, free gifts, or points towards their rewards system.

This rewards system lets you play mini-games to earn further store credit that can be claimed for cash rewards or to purchase products.

Állítólagos együttműködés hírességekkel
A Temu népszerűségét használja ki az a taktika is, amely során **a csalók hírességek nevében tesznek közzé bejegyzéseket, mintha az adott sztár kereskedelmi partnerségben állna a webáruházzal.**

A cél az, hogy rávegyék a rajongókat a posztban szereplő ajánlókód beírására a Temu oldalán, cserébe pedig azt ígérik, hogy kedvezményes áron vásárolhatnak a kollaboráció termékeiből. Természetesen mindez hazugság, a kódok beírásával csak a csalókat gazdagítjuk.



90%-os kedvezményt ígérő átverések
Azokkal a weboldalakon látható és e-mailekben érkező reklámokkal is érdemes óvatosan bánni, amik hatalmas kedvezményeket ígérnek a Temu széles termékkínálatára. Klasszikus social engineering technikákat alkalmaznak, [például a rövid ideig tartó jelentős kedvezmények meghirdetésével]().

Az ilyen reklámokban szereplő linkek egy adathalász oldalra vezetnek, ahol a hackerek megszerezhetik a bankkártyaadatainkat, mi viszont sosem kapjuk meg a rendelésünket.

Hogyan maradjunk biztonságban vásárlás közben a Temun? Az írországi székhelyű, de valójában kínai Temu bug bounty (biztonsági hibák felfedezéséért jutalom kitűzése) programot indított, hogy növelje a felhasználók biztonságát, illetve állítása szerint dolgozik az átverések visszaszorításán.

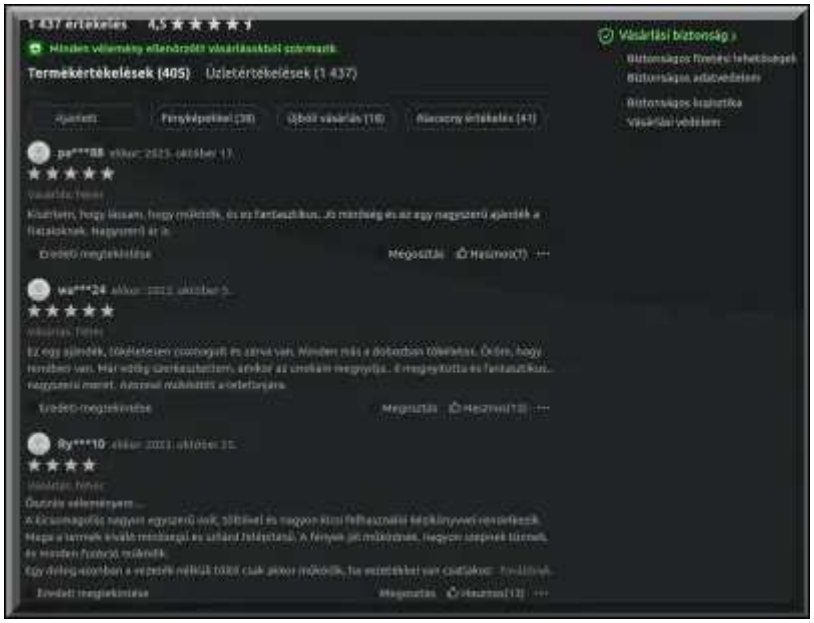
A közelmúltban **a vállalat előzetes bírósági végzést nyert az Egyesült Államokban olyan adathalász oldalak ellen, amelyek a webáruházat másolták.**

Érdemes betartanunk az alábbi biztonsági intézkedéseket:

- Soha **ne kattintsunk a kéretlen e-mailekben vagy a hirdetésekben szereplő linkekre**.
- Az online hirdetett Temu ajánlatokra ne kattintsunk közvetlenül, inkább keressünk rá a vállalat hivatalos webáruházában.
- **Ne mentsük el a fizetési adatainkat a felhasználói fiókunkban. Emellett állítsunk be kétfaktoros hitelesítést (2FA) is,** hogy plusz biztonsági réteg védje a fiókunkat a jelszavunkon túl. A Temun már van lehetőség az SMS-alapú hitelesítésre, amely bár nem olyan biztonságos,

mint a hardveres biztonsági kulcsok vagy az erre a célra kifejlesztett telefonos hitelesítési alkalmazások, mégis nagyobb védelmet jelentenek.

- Ne dőljünk be olyan ajánlatoknak, amelyek ajánlókód felhasználását kérik a Temu oldalán - **különösen azoknak ne, amelyekben híresség is szerepelnek**.
- Mindig vizsgáljuk meg alaposan, hogy mit vásárolunk, elkerülve a későbbi csalódásokat.
- A Temu különleges kedvezményeket és alacsony árakat kínál. Ugyanakkor a hihetetlennek tűnő kedvezmények átverések is lehetnek. **Nézzünk utána az interneten, hogy mit írnak máshol az adott kedvezményről, és milyen vásárlói visszajelzések születtek.**



Általánosan fogalmazva, legyünk óvatosak azzal kapcsolatban, hogy milyen adatokat adunk ki és milyen engedélyeket adunk a Temu alkalmazásnak, vagy bármilyen más hasonló appnak. **A Temun és az ehhez hasonló online piactereken is lehetünk óvatosabbak.**

- Lehetőleg ne a közösségi média fiókunkkal jelentkezzünk be a Temuba, illetve kerüljük a más fiókokkal való összekapcsolást.

- **Használjunk bizonyos összeggel feltölthető virtuális kártyákat vagy olyan fizetésközvetítési szolgáltatót**, mint a PayPal, hogy megóvjuk az igazi bankkártya adatainkat.

- Az otthoni címünk helyett kérjük a rendelést postafiókba, csomagpontra vagy csomagautomatába.

- Maradjunk naprakészek a kiberbiztonság terén! Ebben segíthetnek a Hackfelmetszők - Veled is megtörténhet podcast havonta jelentkező friss epizódjai!

Tweet 0

Pin it

Tetszik

1 komment

Címkék: kína webshop csalás átverés webáruház óvatosság temu

Ajánlott bejegyzések:

Macskajaj	A legnépszerűbb 2024-es posztok	CAPTCHA, amely nem az ember-gép relációt teszteli	Adathalászat vagy jófogás?
Macskajaj	A legnépszerűbb 2024-es posztok	CAPTCHA, amely nem az ember-gép relációt teszteli	Adathalászat vagy jófogás? Új bejelentkezés a felhőnkbe. Vagy mégsem?
			Új bejelentkezés a felhőnkbe. Vagy mégsem?

Kommentek:

Head Honcho 2024.02.03. 17:08:20

A jogok figyelmen kívül hagyására meddig ultima ratio még, hogy a sárgák sokan vannak és sok a pénzük?

Válasz erre

keresés

tweetz






Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Kórházak a pácban II.

2024. február 07. 09:52 - Csizmazia Darab István [Rambo]

Sajnos ma már korántsem kirívó, hogy sorozatban egészségügyi intézményeket, kórházakat támadjanak a ransomware csoportok. Még **a Covid időszak alatt tett állítólagos kisdobos becsszó alapú megnemtámadási moratóriumot sem tartották be - igaz épeszű szereplő ezt nem is hitte volna el nekik.**

Azonban azóta csak sokasodnak az ilyen jellegű incidensek, és e**zek nem kímélnek még olyan szereplőket sem, mint gyermekek számára fenntartott onkológiai intézmények**. Ahol ilyenkor például csak azért, mert közben éppen senki sem hal meg, nem jelenti azt, hogy nem is történhetett volna meg. Igaz **volt olyan eset is, amikor a LockBit csoport megtudta, hogy a kanadai Sickkids kórházat ért olyan támadás**, amelyben az ő zsarolóvírusukat használták, önmérsékletet tanúsítva elnézést kértek és ingyenes helyreállító kulcsot adtak a kórháznak.

Ám úgy tűnik, **ez eléggé egyedi eset volt, és a némely szereplőknél nyomokban található esetleges erkölcsi aggályokat a profit éhség ma már mindenkinél felülírja. Az a hozzáállás, miszerint elkerülik az olyan szervezeteket, mint a kórházak vagy a non-profit szervezetek, gyakorlatilag megszűnni látszik.**

Nincs egy hete, hogy pont a LockBit fenyegetett meg egy chicagói gyermekkórházat, ahol irreálisan magas, 800 ezer dolláros követelést fogalmaztak meg. **A Szent Antal kórháznál valójában már decemberben elkezdődött maga a behatolás, és az incidens itt is doxinggal, azaz adatlopással is párosult, vagyis a váltságdíjat nem csak azért kérik, hogy titkosítást feloldó kulcsot adjanak, hanem hogy a kiszivárgott bizalmas adatokat ne töltsék fel** a publikus netre, amit viszont azóta a nemfizetés miatt meg is tettek.

A LockBit csoport 2020-ban tűnt fel orosz nyelvű kiberbűnözéssel foglalkozó fórumokon, sokak szerint egyértelműen orosz gyökerű bandáról van szó, bár ők maguk a darkneten azt írják magukról, hogy Hollandiában vannak és nem politikai, hanem üzleti vállalkozásként üzemelnek.


SIGN IN / UP

The Register

CYBER-CRIME

8

Lurie Children's Hospital back to pen and paper after cyberattack

It's the second Chicago hospital to disclose a major incident in the same week

Connor Jones

Mon 5 Feb 2024 14:45 UTC

For the second time in one week, cybercriminals have targeted a Chicago children's hospital, this time causing significant operational disruption.

Lurie Children's Hospital said it pulled network systems offline as it continues to respond to "a cybersecurity matter" alongside outside experts and law enforcement agencies.

Email, phone, and internet services are unavailable at the hospital, and according to local news, young patients have been unable to attend scheduled appointments for six days and counting.

The hospital remains open for emergencies but is operating on a first come first served basis, according to other reports.

Some patients with scheduled elective surgeries have also had their appointments pushed back or canceled. Others say ultrasound systems were down and prescriptions were being handled using analog, pen-and-paper methods.

Ezúttal egy újabb hasonló profilú célpontról szólnak a beszámolók, miszerint a szintén Chicagóban található Lurie Children's Hospital az áldozat.

A számítógépes rendszer leállása miatt csak sürgősségi gyermek ügyeletet látnak el, a betervezett műtéteket kénytelenek voltak elhalasztani, az ultrahangos részleg is megbénult, és az adminisztráció visszaállt a papír, toll, ceruza módszerre, beleértve a receptek analóg módon történő megírását is.

Sajnos az egészségügyi szektor régóta a kiberbűnözők kedvelt célpontja, hiszen **az átlagosnál gyengébb, gyakran alulfinanszírozott kiberbiztonság miatt itt könnyen komoly működési zavart képesek okozni**.

Gyermekkorunkban talán ok nélkül féltünk a nagy és félelmetes fehér köpenyes doktor néniktől és doktor bácsiktól, utána felnőttként már inkább amiatt aggódtunk, hogy annyira keveset fordítanak az egészségügyre, és akkor most emellett extra ijesztő lehet, hogy a még megmaradt sérülékeny szolgáltatások felett is folyamatosan ott lebeg a Damoklész kardja: senki sem maradhat biztonságban ezektől a támadásoktól.

Szólj hozzá!
Címkék: usa kórház egészségügy váltságdíj intézmény gyermekkórház ransomware zsarolóvírus doxing lockbit

Ajánlott bejegyzések:

8 kórház, 30 klinika, 2.5 millió betegadat

9 millió, bizony, dalolva ment...

A ransomware az egészségügyben élet-halál kérdése

100 millió ember egészségügyi adata hoppszi

A ransomware az egészségügyben élet-halál kérdése

100 millió ember egészségügyi adata hoppszi

Holló a hollónak mégiscsak, de igen...

Holló a hollónak mégiscsak, de igen...

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Jelszó világvége

2024. február 12. 12:04 - Csizmazia Darab István [Rambo]

Nincs olyan biztonsági képzés, ahol a jelszavakról ne esne szó, ám **az ezzel kapcsolatos tudatosság szemlátomást nem javul már hosszú évek óta.**

Az ellopott, kiszivárgott jelszavak egyik legismertebb gyűjtőhelye a haveibeenpwned.com weboldal, ahol ma reggelig 12.9 milliárd ilyet jegyeztek, ami már önmagában sem kis szám, de **az ilyen tételek valódi nagyságrendjét a szakemberek legalább 3-4 szeresére teszik.**

Ami egy korábbi összesített gyűjtésből is látszik, hogy az ilyen adatok feldolgozása után évek, sőt **évtizedek óta látványosan marad az élbolyban a password, a qwerty és az 123456.**

Top 10 Worst Passwords - Historic Analysis

	2023	2015	2010	2005	2000
#1	123456	123456	123456	password	password
#2	123456789	password	password	123456	123456
#3	qwerty	12345	12345678	12345678	12345678
#4	password	12345678	qwerty	abc123	qwerty
#5	1234567	qwerty	abc123	qwerty	abc123
#6	12345678	1234567890	123456789	monkey	monkey
#7	12345	1234	111111	letmein	1234567
#8	iloveyou	baseball	1234567	dragon	letmein
#9	111111	dragon	iloveyou	111111	trustno1
#10	Covid	football	adobe123	baseball	dragon

Ezúttal a Red9 tette közzé, hogy legújabb kutatása szerint a helyzet továbbra is gyatra: az online jelszavak olyan gyengék, hogy **a zömük szinte**

azonnal feltörhető. És igen, a leggyakoribb jelszó továbbra is az 123456.

Ami emellett még különösen érdekes, hogy **sokan mennyire mereven ragaszkodnak a 6 karakteres jelszó hosszhoz, ami talán az általuk fejben megjegyezhető méretkorlát felső határa lehet.**

Csodák továbbra sincsenek, a tanácsok továbbra is arról szólnak, hogy az erős jelszó legyen **egyedi, magyarán mindenhol mást használjunk, legyenek benne nagy- és kisbetűk, számok és speciális karakterek**, mert ezek kombinációja lesz leginkább kiszámíthatatlan. Persze ehhez az is kell, hogy **ne legyen könnyen kitalálható információ**, például keresztnevek és születési dátumok, házi kedvencek neve, és hasonló, például szótáralapon próbálgatva könnyen kitalálható karaktersorozatok.

Ehhez még érdemes **hozzátenni a kéttényezős hitelesítést (SMS, hitelesítő app, hardveres token) ahol csak lehet, és a kulcsfontosságú helyeken a rendszeres jelszó cserét** is bevethetjük.

A kiszivárgott gyenge jelszavaknál nem csak az 123456 mutat gyakori előfordulást, hanem **például a keresztnevek (Michael, Daniel, Ashley), a sportágak elnevezései (foci, hoki, kosárlabda, baseball), sima 4**

karakteres évszámok, amik talán a felhasználók születési évéből származnak.

De helyet kapnak ebben a ligában a különféle filmes karakterek is, mint például Batman, Superman és Spiderman is.

A [NordVPN kutatása szerint egy átlagos felhasználónak több, mint 100 jelszava van](), ami persze valóban nehezen memorizálható.

Ebben azért [sokat tudna segíteni a jelszó széfek alkalmazása, ami generálja, titkosítva tárolja, és kényelmesen előhívja]() a megfelelő helyen ezeket - elkerülve egy másik tipikus gyengeségi csapdát, a böngésző kliensben való sima elmentését a jelszavaknak.

Szólj hozzá!
Címkék: stat jelszó password erős feltörés gyenge bruteforce jelszómenedzser jelszószéf

Ajánlott bejegyzések:

Egy a jelszónk, tartós 123456

Amikor a suszter cipője lyukas II.

Egy a jelszónk, tartós 123456

Ne reszkessetek betörők!

Biztonság + kényelem = jelszókezelő

Amikor a suszter cipője lyukas II.

[Amikor a suszter cipője is admin]

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

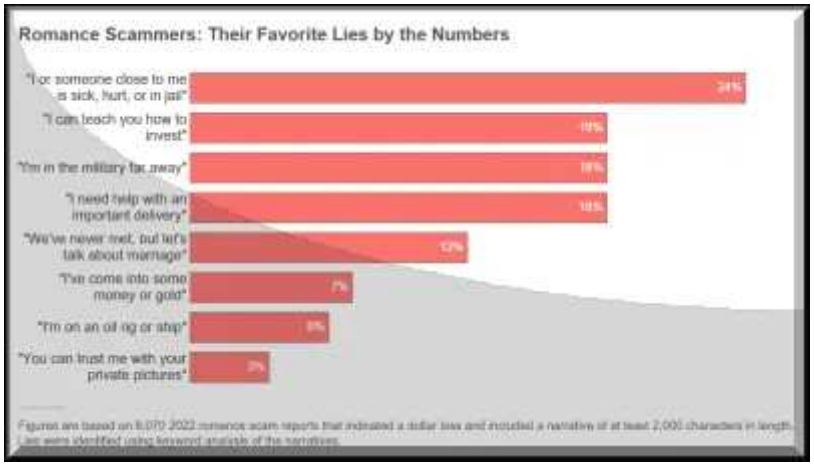
Romantika vagy átverés jön Valentin-napon?

2024. február 14. 18:44 - Csizmazia Darab István [Rambo]

Az online társkeresés elterjedésével **alapjaiban változott meg az emberek közötti kapcsolatteremtés: korábban nem ismert módokon ismerkedünk**. Február 14, Bálint nap a szerelem, a párkeresés és -találás napja.

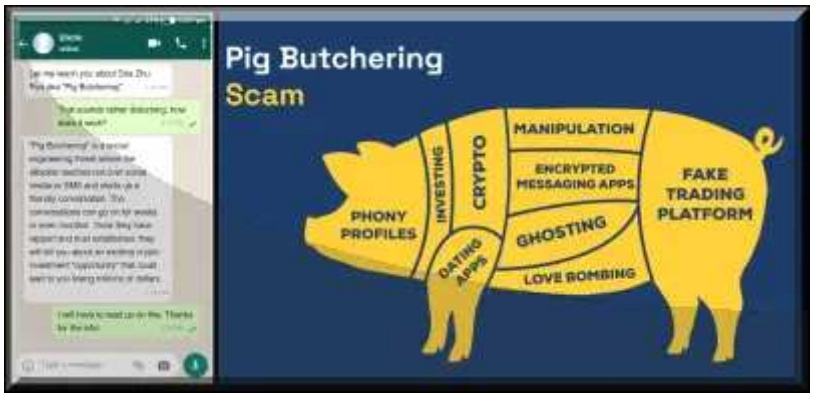
A társkereső alkalmazásoknak 2022-ben világszerte több mint 350 millió felhasználójuk volt.

Bár ilyen összetett hazai statisztikai adat nem ismeretes, de például **az 1999-es alapítású magyar Randivonal.hu oldalt az évek során több, mint 3 millióan próbálták ki**. Akár a telefonunkon is átlapozhatjuk potenciális jelöltjeink online katalógusát - a rémes beszélgetések és a kínos dupla randik ideje lejárt.



A kapcsolatteremtés ugyan egyszerűbbé vált, de ezek az alkalmazások számos lehetőséget kínálnak a csalóknak és a hackereknek a gyanútlan szinglik kihasználására. **A társkereső appok és a közösségi média népszerűsége jelentősen megkönnyítette a kamu udvarlók számára, hogy megtalálják célpontjaikat, akikből aztán pénzt csalnak ki.**

Sajnos az ilyen esetek gyakrabban előfordulnak, mint gondolnánk. Az USA Szövetségi Kereskedelmi Bizottságának jelentése szerint a romantikus csalások 2022-ben csaknem 70 ezer embernek okoztak összesen 1.3 milliárd dolláros kárt.



Ez a szám valójában sokkal magasabb is lehet, hiszen az áldozatok gyakran inkább eltitkolják a történteket, hazánkban inkább csak a kirívó esetek kerülnek bele a hírekbe, amikor többszázezer vagy milliós kár ér valakit. Tovább **súlyosbítja a helyzetet, hogy a romantikus csalások áldozatai közül sokan akaratlanul is "money mule-ok" lesznek, azaz olyan balekké, aki önkéntelenül valamilyen pénzmosási bűncselekmény gyanútlan részesévé válik.**

A romantikus és a kripto csalások keresztezése, a disznóvágás-átverés (pig butchering scam), valamint a kamu sugar daddy-csalás megjelenése is azt mutatja, hogy a támadók **folyamatosan egyre újabb módszerekkel próbálkoznak a korábbi jól bevált technikák mellett.**

Ráadásul a bűnözők **egyre gyakrabban veszik igénybe a generatív AI segítségét, hogy a romantikus csalások meggyőzőbbek legyenek**, és akár Kevin Costnernek is kiadhatják magukat. De nem kell Nagy-Britanniáig mennünk, friss hír, hogy egy 40 éves nő katonatisztként, olajmérnökként,

híres zenészként és hajóskapitányként bemutatkozva 8 hazai áldozattól 15 millió forintot szedett össze.

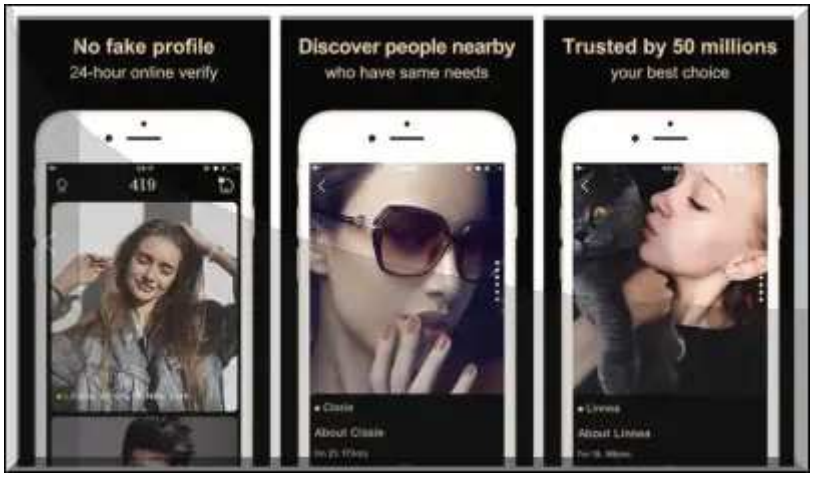
Mit tehetünk tehát, ha a neten keressük a szerelmet, de meg akarjuk védeni magunkat a csalóktól? Hogyan ismerhetjük fel a romantikus csalásokat és a társkereső alkalmazásokban rejtőző egyéb fenyegetéseket?

1. Catfishing: Hamis profil mögé bújó csalók
Az egyik legelterjedtebb módszer, amit a csalók a társkereső alkalmazásokon bevetnek, a catfishing, azaz hamis profilok létrehozása azzal a szándékkal, hogy megtévesszék az áldozatukat. **A bűnözők gyakran internetről lopott vagy letölthető fényképeket és kitalált személyes adatokat felhasználva csábítják el a gyanútlan romantikára vágyókat.** Léteznek olyan weboldalak is, ahol a mesterséges intelligencia segítségével készíthetünk képet igazából nem létező emberekről. **A csalók a közösségi médián keresztül információt tudhatnak meg a célpont hobbijáról, nézeteiről és szokásairól, és ezeket felhasználva azt a látszatot kelthetik, hogy hasonló az érdeklődési körük, ami még erősebb kötődést eredményezhet. Ez a kapocs aztán nagyobb lehetőséget ad nekik az érzelmi manipulációra.** Miután megvan a bizalom, a bűnözők kitalált történeteket adnak elő magánéleti válságokról, vészhelyzetekről, amihez anyagi segítséget kérnek. Az áldozat pénzt utalhat, ajándékokat vehet nekik, vagy akár utazást is foglalhat számukra abban a reményben, hogy ezzel támogatja "partnerét", és valóra válthatja az igaz szerelemről szőtt álmait.

Hogyan védhetjük ki a catfishing csalásokat?
Amikor elmerülünk a romantika világában, nem biztos, hogy az az első dolgunk, hogy megbizonyosodunk a beszélgetőpartnerünk kilétéről. Ellenben, ha ellenőrizzük a közösségi oldalakat, személyes találkozót szervezünk vagy olyan kérdéseket teszünk fel, amire egy csaló nem tud egyszerűen válaszolni, nagy eséllyel megbizonyosodhatunk arról, hogy a Budapesten élő Flóra valójában nem László Győrből. **Mindig gyanakodjunk, ha a másik fél pénzt, szívességet vagy fontos információt kér tőlünk. Lehet, hogy egy igazi emberrel beszélgetünk, de nem biztos, hogy a szándékaik is valósak.** Sajnos az online randizók gyakran bedőlnek az olyan átveréseknek, amiben a másik – gyakorlatilag ismeretlen - fél pénzt kér például arra, hogy kifizesse a beteg családtagja orvosi kezelését vagy hogy egy kivételes befektetési lehetőséggel élhessen.

2. Adathalász-támadások és kártékony programok
A társkereső alkalmazások megkönnyítik az adathalász-támadások végrehajtását és a kártékony programok terjesztését. **A bűnözők álprofilokat hozhatnak létre, és ártatlannak tűnő üzeneteket küldhetnek rosszindulatú linkekkel vagy mellékletekkel, arra késztetve a reménykedő szingliket, hogy rákattintsanak ezekre**. A botok által terjesztett linkeket megnyitva viszont akár rosszindulatú programot is telepíthetnek az áldozat eszközére. Így a számítógépen vagy telefonon tárolt érzékeny információk és adatok sérülhetnek, ami j**elentősen növeli a személyazonosság-lopás és a hitelkártyacsalás** kockázatát.

Hogyan védhetjük meg magunkat?
A beszélgetés első szakaszában, amikor még nem tudunk sokat partnerünkről, lehetőleg ne nyissunk meg általa küldött linkeket, és ne kattintsunk rájuk. Még ha a hivatkozás veszélytelennek is tűnik, **a csalók képesek kreatív domainneveket létrehozni, hogy a hamis linkek hitelesebbnek tűnjenek.** Érdemes várnunk, és jobban megismerni párunkat, mielőtt megnyitjuk a tőle kapott hivatkozásokat.



3. Adatgyűjtés zsarolás céljából
Az online társkereső platformok rengeteg személyes adatot tárolnak, ami vonzó célponttá teszi őket a hackerek számára. A Guardian egyik újságírója kiderítette, hogy a Tinder-profilján keresztül az alkalmazás mintegy 800 oldalnyi adatot gyűjtött össze róla, beleértve a kedveléseket, érdeklődési

köröket, fotókat, barátokat és szexuális orientációt. **A csalók olyan taktikákat alkalmazhatnak, mint például az adatbányászat, hogy ezeket az érzékeny adatokat kinyerjék a felhasználók profiljából.** Előfordul, hogy az ilyen információk napvilágot látnak – tavaly például 260 ezer ember képei és privát üzenetei váltak publikussá, **miután egy társkereső alkalmazás feltört adatbázisát a nyilvánosság számára** hozzáférhetővé tették.

Hogyan védhetjük meg magunkat?
Sok alkalmazásnak szüksége van az adataink egy részére ahhoz, hogy a kívánt funkciókat használni tudjuk, illetve hogy az app a megfelelő felhasználói élményt nyújtsa. Fontos azonban tisztában lenni azzal, hogy milyen adatokat gyűjtenek és azokat hogyan használják fel. Érdemes távol tartani magunkat az olyan alkalmazásoktól, amelyek nem teszik lehetővé, hogy lemondjunk az adatok harmadik felekkel való megosztásáról.

Tudnunk kell, hogy ha egyszer már közzétettük az érzékeny információt, nem sok dolgot tudunk tenni. Ezért a legjobb, amit tehetünk, hogy odafigyelünk arra, mit osztunk meg az interneten. Ne közöljünk semmi olyat, ami felhasználható ellenünk (a vicces videók a legjobb barátunk legény- vagy lánybúcsújáról bajt is okozhatnak).
Ennél még nagyobb veszélyt jelent (és a csaló számára hatalmas pénzt hozhat), **ha engedünk a kísértésnek, és elküldjük pikáns fotóinkat vagy videóinkat a másik félnek. Mindez gyakran kezdődik azzal, hogy a támadó megosztja "saját" állítólagos intim képeit, és cserébe hasonlókat kér tőlünk. Ha ezt megtesszük, kezdetét veszi a zsarolás – a csaló fenyegetőzni kezd, hogy megosztja a tartalmakat ismerőseinkkel a közösségi oldalakon, ha nem fizetünk vagy nem küldünk további kompromittáló képeket, videókat.**

Az ilyen helyzetek elkerülése érdekében **soha ne küldjünk el olyan képeket, amiket nem szeretnénk a nyilvánosság elé tárni.** Hasonlóképpen a webkamera előtt se dobjuk le minden ruhánkat.

4. Helyalapú fenyegetések
Sok társkereső alkalmazás használ helyalapú szolgáltatásokat, hogy összekösse az egymás közelében tartózkodó szingliket. Bár ez a funkció megkönnyíti az emberek számára, hogy partnert találjanak a környékükön, a potenciális veszélyek előtt is ajtót nyit. A hackerek **kihasználhatják a helymeghatározási adatokat, és követhetik célpontjukat, ami már valós biztonsági problémákat vet fel.**

Hogyan védhetjük meg magunkat?
Tegyük fel, hogy nem akarjuk kikapcsolni a helymeghatározó szolgáltatásokat a párkeresés során, mert olyasvalakivel szeretnénk megismerkedni, aki a közelünkben van, nem pedig a világ másik felén él. Kompromisszumos megoldást jelent a helyadatok letiltása, amikor aktívan nem használjuk az alkalmazást. Ezzel a módszerrel csökkentjük sebezhetőségünket. **Ahogy az online társkeresés népszerűsége tovább növekszik (az előrejelzések szerint 2028-ra több mint 450 millió használó lesz), úgy nő annak a kockázata is, hogy csalók célpontjává válunk.**

Azok, akik az online térben keresik a szerelmet, vegyék figyelmeztető jelnek a gyanús linkeket és a hamisnak tűnő profilokat. Ha valami szokatlant vagy problémát észlelünk, azonnal jelentsük a másik fél profilját az alkalmazásban, és tiltsuk le.

Mindez azonban ne riasszon el minket, ugyanis az online társkeresők felhasználóinak több mint 70 százaléka került már igazi romantikus

kapcsolatba a platformok segítségével, az tehát egyértelmű, hogy ezek az alkalmazások rendkívül sikeresen működnek. **Mindannyiunk közös érdeke, hogy az appok biztonságosabbá váljanak.** Ki tudja, lehet, hogy az igaz szerelem már csak egy jobbra húzásra van tőlünk...

Szólj hozzá!
Címkék: nap online ismerkedés csalás átverés randi valentin veszélyek randiapp

Ajánlott bejegyzések:

1.3 milliárdba fájt a romantika

5 online csalásra utaló jel

A legnépszerűbb 2024-es posztok

CAPTCHA, amely nem az ember-gép relációt teszteli

A legnépszerűbb 2024-es posztok

CAPTCHA, amely nem az ember-gép relációt teszteli

Adathalászat vagy jófogás?

Adathalászat vagy jófogás?

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Váltságdíj a váltságdíjszedő bandákért II.

2024. február 19. 13:12 - Csizmazia Darab István [Rambo]

Volt már korábban is hasonló kezdeményezés, ahol az amerikai hatóságok 10 millió dollárt ígértek a nyomravezetőknek a DarkSide ransomware bandavezérekkel kapcsolatos információkért.

Ezúttal **ismét 10 millió dollárt ajánlanak olyan tippekért, amely az orosz gyökerű BlackCat/AlphaV ransomware csapattagok azonosításához, tartózkodási helyéhez vezethetnek, és további 5 milliót, amely az alvállalkozói közreműködőket segít leleplezni és letartóztatni. Az FBI szerint a BlackCat bűnözői csoport 2023. szeptemberéig legalább 300 millió dollárnyi (kb. 180 mrd HUF) váltságdíjat gyűjtött be több, mint 1000 áldozattól.**

A felajánlott jutalmakat az U.S. Transnational Organized Crime Rewards Program (TOCRP) nevű szervezet fedezi, amely 1986 óta összesen már 135 millió dollárt fizetett ki hasonló bejelentők részére például a Hive, a Clop, a Conti, a REvil (Sodinokibi) illetve a Darkside csoportokkal kapcsolatosan.

A külügyminisztérium **egy dedikált Tor szervert is létrehozott, amely a BlackCat/AlphaV és más hasonló keresett bandákról való bejelentések küldésére/fogadására használható. Az orosz támogatású ALPHV csoport 2021. novemberében jelent meg**, és a feltételezések szerint a korábbi DarkSide és a BlackMatter bandák egyesüléséből jött létre.

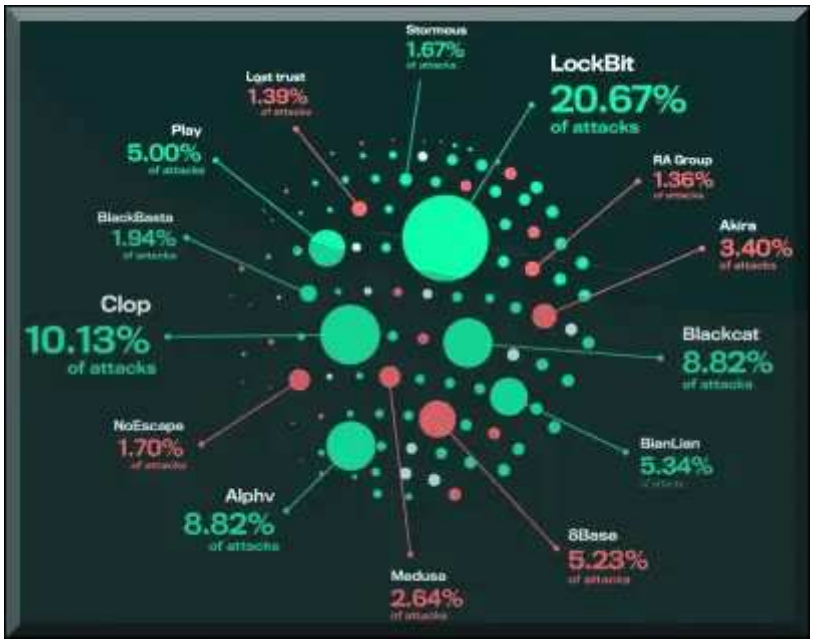
Emlékezetes akcióik között említhetjük például a 2021. májusi Colonial Pipeline csőhálózat elleni támadásukat. Egy átmeneti kényszerszünet után újra megjelentek BlackMatter név alatt, ám az FBI hosszas nyomozás eredményeként feltörte a csoport szervereit, és lelőtte a Tor-tárgyalási és kiszivárogtató oldalait.

Ám 2022. februárjától megint feltámadtak BlackCat/AlphaV néven, ismét akcióba léptek, és célzottan a világ kritikus infrastruktúráinak fő támadói lettek.

Rengeteg velük kapcsolatos incidensről olvashattunk, **többek közt egy luxemburgi székhelyű Enveco nevű energiaszolgáltató hálózat ellen indítottak támadást, a Western Digitalt informatikai rendszeréből is sikeresen ügyfél-információkat loptak el, valamint a németországi Motel One szállodalánc is elszenvedett egy masszív zsarolóvírus akciót.**

Nem válogatnak a célpontok közt, például tavaly **az Egyesült Államokban nyolc kórházat és több mint 30 klinikát üzemeltető Norton Healthcare került a célkeresztjükbe, ahonnan 2.5 millió betegadatot loptak el.**

A behatolás során ügyfél nevekhez, elérhetőségi adatokhoz, társadalombiztosítási számokhoz, születési dátumokhoz fértek hozzá, emellett jogosítvány és egyéb állami igazolványszámokat, valamint számlaadatokat, sőt digitális aláírásokat is el tudtak lopni.



Mindeközben **új versenyzők is megjelentek a terepen, köztük az Akira és a 8Base ransomware csapat jelentős számú támadást hajtott végre.**

A különféle zsarolóvírusokhoz köthető bűnözői csoportok aktivitását a hírek mellett például a www.ransomlook.io weboldalon is nyomon tudjuk követni.

[Szólj hozzá!]
Címkék: [orosz] [fbi] [információ] [váltságdíj] [ransomware] [oroszországi] [blackcat] [zsarolóvírus] [alphv]

Ajánlott bejegyzések:

[8 kórház, 30 klinika, 2.5 millió betegadat]

[100 millió ember egészségügyi adata hoppszi]

[100 millió ember egészségügyi adata hoppszi]

[Change Healthcare újra pácban]

[Change Healthcare újra pácban]

[Holló a hollónak mégiscsak, de igen...]

[Holló a hollónak mégiscsak, de igen...]

[Várt és nem várt mellékhatások]

[Várt és nem várt mellékhatások]

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz






Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Cronos - LockBit 1:0, egyes

2024. február 21. 10:51 - Csizmazia Darab István [Rambo]

Ritka esemény, mikor sikeres letartóztatások keretében tudnak fellépni a zsarolóvírus bűnözőkkel szemben. Ezúttal egy ilyen alkalomnak örülhetünk, ugyanis **a bűnüldöző szervek letartóztatták az orosz LockBit ransomware banda két üzemeltetőjét Lengyelországban és Ukrajnában.**

A nemzetközi részvétellel zajló Cronos hadművelet keretében - melyet a brit NCA, valamint az Europol és az Eurojust irányított - **több mint 200 titkosított kriptotárcát foglaltak le, miután egy nemzetközi felszámolási akció során sikeresen feltörték a számítógépes bűnözők szervereit.**

Összesen 34 szervert sikerült lekapcsolni világszerte: Hollandiában, Németországban, Finnországban, Franciaországban, Svájcban, Ausztráliában, az Egyesült Államokban és az Egyesült Királyságban. Emellett 14 ezer olyan fiókot is beazonosítottak, amelyeket a zsarolásokhoz használtak.

Az akció részeként az NCA n**emcsak a LockBit szerverek felett vette át az irányítást, hanem a csoport darkwebes lopott adatokat kiszivárogtató oldalainál is, és ezeket is lelőtték. Nagy fogásnak számít a dolog, hiszen a LockBit forráskódját, a beszervezett partnerek chat üzeneteit és az áldozatokkal folytatott kommunikációt is megtalálták.**

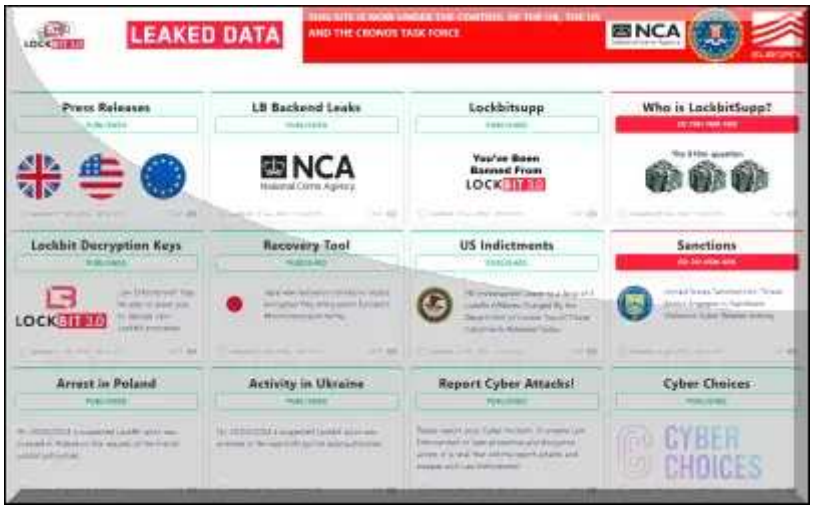
A művelet további részeként a hatóságok több mint **1000 visszafejtési kulcsot is le tudtak kérni a lefoglalt LockBit szerverekről, így ezek felhasználásával a japán rendőrség, az NCA, az Europol és az FBI kifejlesztett egy ingyenes LockBit 3.0 Black Ransomware visszafejtő eszközt, amit "No More Ransom" portálon keresztül tölthetünk le.**

Az USA Igazságügyi Minisztériuma szerint a bandának több mint 2000 áldozata volt, és eddig több mint 120 millió dollárt szedtek már be váltságdíjként - elsősorban vállalati ügyfelektől. **A francia és az amerikai igazságügyi hatóságok három nemzetközi elfogatóparancsot és öt vádemelést is kiadtak a LockBit további szereplői ellen**.

A korábbi Lockbit támadásokkal kapcsolatos vádemelések közül kettőt az Egyesült Államok Igazságügyi Minisztériuma már lezárt, **két orosz állampolgár, Artur Sungatov és Ivan Gennadievich Kondratiev (alias Bassterlord) részvétele ügyében.**

Bár a letartóztatások korántsem érintenek minden résztvevőt, de a működőképesség blokkolásában így is meglehetősen hatékonyra sikerült.

Azt viszont egyelőre nem tudni, pontosan mennyi kriptovalutát tároltak a zár alá vett számlákon, de ha ezeken jelentős mennyiségű pénzt találnak, akkor arra is van esély, hogy az áldozatok visszaszerezzék a zsarolóprogramok miatt befizetett összegeik legalább egy részét.



A talált adatok elemzése során arra is bizonyítékokat találtak, hogy kár abban bízniuk a váltságdíjat fizetett áldozatoknak, hogy a bűnözők a pénzért cserébe majd ígéretüknek megfelelően valóban törlik az adataikat, mert a szerverekről ennek éppen az ellenkezője derült ki.

Szólj hozzá!

Címkék: csoport letartóztatás nemzetközi fellépés banda operation ransomware cronos zsarolóvírus lockbit

Ajánlott bejegyzések:

[A kriptobevételek felett az égbolt felhőtlen](#)

[Meghökkentő mesék - adatközpontokról](#)

[Kórházak a pácban II.](#)

[Kékfény különkiadás](#)

[A kriptobevételek felett az égbolt felhőtlen](#)

[Meghökkentő mesék - adatközpontokról](#)

[Kórházak a pácban II.](#)

[LockBit üti](#)

[Subway, sakk](#)

[LockBit üti](#)

[Subway, sakk](#)

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

3000%-kal több lett, maradhat?

2024. február 26. 12:07 - Csizmazia Darab István [Rambo]

A deepfake hamisítással összekötött adathalászat mértéke a tavalyi évben rekordot döntve elképesztő mértékben nőtt. A szakértők véleménye szerint viszont csak most kezd majd igazán erősödni.

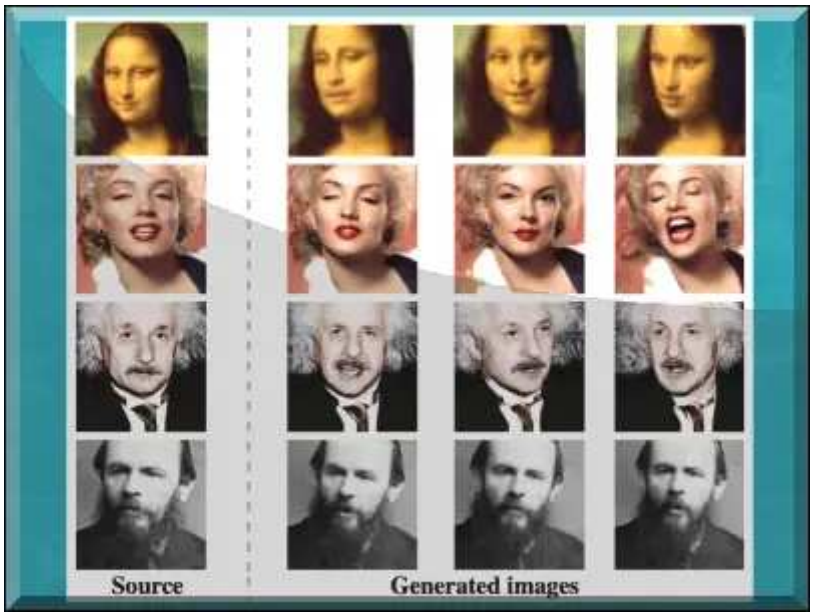
1988. - ebben az évben jelent meg a nagy sikerű PhotoShop képmanipulátor program első verziója, sokan a blog olvasói közül talán még meg sem születtek ekkor. A korábbi alapállás, amit persze a korabeli fényképek laboros hamisítása azért kicsit befolyásolt: lásd Sztálin féle retusált történelem, vagy a Loch Ness-i szörnyről, jetiről, bigfootról, ufókról készített állítólagos fotók - **előtte azért mégiscsak az volt, hogy kevés kivételtől eltekintve hihetünk a szemünknek.**

Ennek tette be a kaput látványosan a PhotoShop **eleinte csak a címlapon szereplők megszépítésével, a későbbi tömeges használattal aztán már bármire és akármire használták, és persze az internetes csalásokban is kivette a részét.**

Bár csak **2017-ben jelent meg az első deepfake videó, ahol látszólag Obama beszélt**, de egy másik ember tátogott a szájával, innentől aztán rohamtempóban felgyorsultak az események.

Az egyre jobb minőségű deepfake mellett **a Samsung labor 2019-ben már egyetlen állóképből is tudott egyszerűen hamisított kezdetleges videót készíteni,** amit szépen be is mutattak Mona Lisa, Einstein, Raszputyin, Salvador Dali és Marilyn Monroe főszereplésével.

Ez a technika hamarosan átverésekben, fakenews hírekben is felbukkant, például egy hamis Zelenszkij filmben, amiben látszólag a háború feladására szólított fel.



Állóképek terén is f**orradalmi változások jöttek a Dall-E, Tengr.ai, Midjourney, Leonardo.ai, Clipdrop, Wonder, Stable Diffusion, Freepik, Dreamstudio és hasonló képgenerátoroknak köszönhetően, így láthattuk olyan soha meg nem történt eseményeket, mint a pufi-dzsekis Pápa, Trump tucatnyi rendőr általi letartóztatását, vagy robbantást a Fehér Házban.**

A programok egyre komolyabb tudásúak, villámgyorsak és szinte bármit el lehet készíteni a segítségükkel.

Végül pedig **megérkezett a Google Lumiere és rövid idővel utána az OpenAI SORA alkalmazása, amely parancssor alapján már nem csak állóképet, hanem valósághű mozgó videót is képes generálni. Ezek tudásáról érdemes megnézni a bemutató videókat is,** van ebben állókép egy részletének animálásától kezdve meglévő videó módosításán át prompt alapján készíthető élethű film is.

Bárkit érhet ilyen típusú hamisítás, például legutóbb Taylor Swift került a célkeresztbe, akinek a videójára ismeretlenek ráhamisítottak egy Trumpot éltető zászlót.

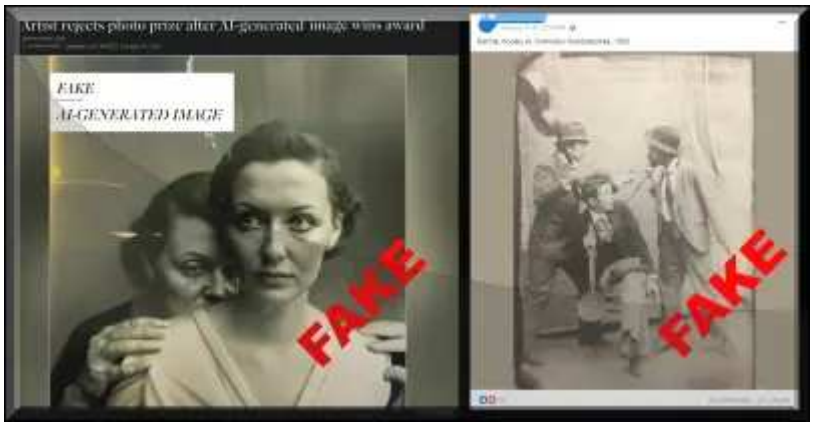
A gépi tanulással segített átverések már jó ideje egyre gyakoribbak lettek, és bár a fenti felsorolásból kimaradt **a hang hamisítása, ez is már évek óta lehetséges, így például volt rá eset, hogy a DeepVoice hangszintetizálás segítségével 220 ezer euró összeget csaltak ki egy cég igazgatójától, és ebben magyar szál is szerepelt.**

Sajnos a hétköznapokba is betört mindezt, például **a klasszikus "öregezés" modernizált változatában a gyerek hangján hívják fel a szülőket, aki látszólag elmondja, hogy elrabolták és csak váltságdíj ellenében engedik szabadon.**

A 2023. áprilisi esetnél szerencsére a dolog kamu volt, és az iskolás lány mindeközben egészségben és biztonságban síelt az osztálytársaival.

A mostani jelentés egybecseng az IT biztonsági cégek trendeket elemző korábbi éves jóslataival, ennek pedig az a fő oka, hogy **mára már rengeteg ingyenes vagy igen olcsó fejlett mesterséges intelligencia-modell érhető el, amelyek használatához alig vagy egyáltalán nem szükséges semmilyen kódolási tudás.**

Az AI használatával kapcsolatosan **a fő félelem nem is az, hogy a Skynet egy napon majd öntudatra ébred és megöli Sarah Connort, hanem hogy a bűnözők egyre inkább rossz célokra használják.**



A megelőzés-védekezés témához **sok apró elemnek kellene a helyén lennie, elsősorban a biztonságtudatosság terén akár magánfelhasználókról, akár munkavállalókról beszélünk. Tisztában kell lenni az aktuális kockázatokkal, a fiókjainkban erős egyedi jelszó használat, kétfaktoros autentikáció elengedhetetlen, és segíthet az ismerkedés az AI alkalmazásokkal is, hogy lássuk, mire képesek ezek egyáltalán.**

A nagy nyelvi modellekkel már nyelvtanilag közel hibátlan szövegeket lehet alkotni, **így pusztán a helyesírás és nyelvhelyesség alapján egyre nehezebb a csalások egyszerű felismerése.**

A gyanús, szokatlan, kéretlen megkeresések, a klasszikus sürgetés-fenyegetés mindenképpen intő jel kell, hogy legyen. A virtuális emberrablásnál pedig **olyan nem közismert kérdések, mint korábbi családi eseményekre való utalás, a családon belül emlékezetes alkalmakra, időpontokra, ismerősökre való rákérdezés vagy előre**

megállapodott kulcsszavakra való hivatkozás segíthet a hanggal vagy videóval visszaélő csalók lebuktatásában.

Egy azonban biztos, egyre több kísérletet egyre nehezebb lesz majd a jövőben felismernünk.

Szólj hozzá!
Címkék: ai csalás átverés mesterséges intelligencia mesterséges intelligencia phishing adathalászat deepfake

Ajánlott bejegyzések:

Virtuális emberrablás, igazi károkozás

Szemetelnek, szemetelnek...

Az AI használat árnyoldalai

Virtuális emberrablás, igazi károkozás

Na de mit adott nekünk a ChatGPT? Csomagja érke... Na most már elég!

Szemetelnek, szemetelnek...

Az AI használat árnyoldalai

Csomagja érke... Na most már elég!

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkereső csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Virtuális emberrablás, igazi károkozás

2024. február 29. 10:42 - Csizmazia Darab István [Rambo]

Minden szülő legrosszabb rémálma felvenni egy ismeretlen számról érkező hívást és azt hallani, hogy a gyermeke segítségért kiált. Aztán az állítólagos "emberrabló" szól bele a telefonba, és váltságdíjat követel, ellenkező esetben soha többé nem láthatjuk a fiunkat vagy a lányunkat. **Szakértők szerint a csalók a jövőben egyre gyakrabban fognak a mesterséges intelligenciára támaszkodni.**

Sajnos mindez nem egy hollywoodi film képzeletbeli forgatókönyve, hanem egy nagyon is valós példa arra, hogy a csalók a legmodernebb technológiát használva meddig képesek elmenni, hogy pénzt zsaroljanak ki áldozataiktól.

A módszer egyúttal rámutat **a mesterséges intelligencia hangklónozási technológiájának fejlettségére** is, amely ma már elég meggyőző ahhoz, hogy akár még a legközelebbi családtagokat is átverhessék vele.

Azonban minél többen ismerik ezeket a csalásokat, és tudják, hogy mire kell odafigyelniük, annál kisebb a valószínűsége, hogy a telefonos csalók sikerrel járjanak. A virtuális emberrablások általában több, egymásra épülő szakaszból épülnek fel, ezek jellemzően a következők:

1. A csalók potenciális áldozatokat keresnek, akiket felhívhatnak és megpróbálhatnak tőlük pénzt zsarolni. Ez a felderítési szakasz is már optimalizálható a mesterséges intelligencia eszközeinek használatával.

2. A bűnözők beazonosítják a kitalált emberrablás célpontját - többnyire a célszemély gyermekét a közösségi médiában vagy más, nyilvánosan elérhető információk alapján.

3. A csalók ezután kitalálnak egy képzeletbeli szituációt, ügyelve arra, hogy az a lehető a legmegrázóbb legyen azon személy számára, akit majd fel akarnak hívni. Minél nagyobb az ijedtség, annál kevésbé fog a hívott fél ésszerű döntéseket hozni. A jól kivitelezett social engineering manipulációs kísérletekhez hasonlóan a csalók emiatt sürgetik is az áldozat döntéshozatalát.

4. A bűnözők ezután további kutatásokat végezhetnek, hogy lássák, melyik időpont a legalkalmasabb a hívásra. Az információ forrása ezúttal is a közösségi média, illetve egyéb nyilvánosan elérhető adat lehet. Az a céljuk, hogy olyan időpontban vegyék fel velünk a kapcsolatot, amikor a szeretteink, rokonaink otthonuktól távol tartózkodnak, ideális esetben nyaralnak, mint ahogy az például Jennifer DeStefano lánya esetében történt.

5. Ezután elkészítik a hamis hangmásolatokat, amiket a hívás során használnak. A csalók egy bárki által hozzáférhető szoftver segítségével hangfelvételt készítenek a célpont manipulált hangjával, amellyel megpróbálják meggyőzni az áldozatot arról, hogy valóban elrabolták a rokonát. Egyéb, közösségi médiából szerzett információkat is felhasználhatnak a biztosabb és testreszabott meggyőzés érdekében, például olyan részleteket említenek az elrabolt személyről, amelyeket egy hétköznapi idegen általában nem tudhat.

6. Ha bedőlünk az átverésnek, valószínűleg azt akarják majd elérni, hogy ne nyomon követhető módon adjuk át számukra a kívánt összeget, hanem például **kriptopénzben fizessünk egy általuk megadott számlára.**

A módszernek számos alváltozata létezik, például balesetre, letartóztatásra is hivatkozhatnak. A legaggasztóbb probléma, hogy a ChatGPT és más mesterséges intelligencia-eszközök segítségével a virtuális emberrablások széleskörben elterjedhetnek, egyúttal a csalók könnyebben megtalálhatják ehhez az ideális áldozatokat. A hirdetők és a marketingesek már évek óta alkalmaznak viselkedéselemző profilozó technikákat, hogy a megfelelő üzeneteket a megfelelő időben juttassák el a kívánt célcsoportokhoz.

A generatív mesterséges intelligencia (GenAI) ebben is segíthet a csalóknak azáltal, hogy **gyorsan megkereshessék azokat a személyeket, akik a legnagyobb valószínűséggel fognak fizetni**, ha virtuális emberrablás

áldozatává válnak. Az AI lehetővé teszi a csalók számára, hogy **akár tömegesen hajtsák végre az ilyen akciókat.**

A hangklónozási technológia már most is nyugtalanítóan meggyőző, amint azt az ESET szakértőinek nemrégiben végzett kísérlete is bizonyítja. A módszert egyre gyakrabban alkalmazzák a csalók, és **már egy tavaly májusi hírszerzési jelentés is figyelmeztetett a szövegről beszédre alakítás (TTS, Text to Speech) technológiáját alkalmazó eszközökkel való visszaélésekre. Azt látjuk, hogy a kiberbűnözők körében is egyre nagyobb érdeklődés mutatkozik a hangklónozó szolgáltatások (VcaaS, Voice Cloning-as-a-Service) iránt.**

Amennyiben ez valóban széleskörben is elterjed, **bármely támadó számára lehetővé válik az ilyen jellegű csalások végrehajtása**, különösen, ha a GenAI-eszközökkel együtt használják.

A már jól ismert politikai dezinformációk mellett a deepfake technológiát üzleti e-mailek feltörésére és szexuális tartalmú zsaroló átverésekre (sextortion) is használhatják. **Ez utóbbinál a zsarolás az áldozattól előzetesen kicsalt valóságos fotókon is alapulhat, de akár a mesterséges intelligencia segítségével mélyhamisítással is előállítható ilyen generált tartalom az áldozat teljesen felöltözött fényképeiből.**

Hogyan maradjunk hát mégis biztonságban? Már egy kis tájékozottsággal is hasznos lépéseket tehetünk a deepfake, különösen pedig a virtuális emberrablás okozta veszélyek csökkentéséért.

A vállalatoknak érdemes külön szakértői tréningeket tartani a témában, de saját magunk is minimalizálhatjuk annak az esélyét, hogy áldozattá váljunk, és bedőljünk egy csalók által indított hívásoknak. **Érdemes beszélgetni erről a témáról a családunkban is, és hasznos lehet, ha megfontoljuk az alábbi tanácsokat.**

- Ne osszunk meg túl sok személyes információt a közösségi médiában. Kerüljük az olyan adatok konkrét közzétételét, mint a lakcímek és a telefonszámok. Lehetőség szerint ne osszunk meg videó- és hangfelvételeket a családtagjainkról, és semmiképp ne osszunk meg részleteket a szeretteink aktuális utazásairól!

- Gyanakodjunk adathalászatra, ha olyan üzenetet kapunk, amely azt kéri, hogy megadjuk a személyes adatainkat vagy a közösségi profiljaink bejelentkezési adatait!

- Használhatunk olyan szülői felügyelet alkalmazásokat, amelyek helymeghatározás funkcióval is rendelkeznek, így az engedélyükkel ellenőrizni tudjuk, hogy hol van épp a gyermekünk.

- Ha hívást kapunk, tartsuk szóval az állítólagos emberrablókat. Ezzel egy időben próbáljuk meg felhívni az érintett családtagunkat egy másik vonalról, vagy szóljunk valakinek a közelünkben, hogy hívja fel.

- Maradjunk nyugodtak, közben ne osszunk meg a bűnözőkkel semmilyen további személyes információt. Vegyük rá a hívó felet, hogy válaszoljanak egy olyan kérdésre, amelyre csak az "elrabolt" tudhatja a választ, és kérjük meg, hogy beszélhessünk vele.

- A lehető leghamarabb értesítsük a helyi rendőrséget.

1 komment
Címkék: ai mi emberrablás csalás átverés mesterséges megelőzés virtuális intelligencia zsarolás mesterséges intelligencia kriptovaluta deepfake

Ajánlott bejegyzések:

3000%-kal több lett, maradhat?
Szemetelnek, szemetelnek...

Az AI használat árnyoldalai
3000%-kal több lett, maradhat?
Szemetelnek, szemetelnek...
Na de mit adott nekünk a ChatGPT?
Az AI használat árnyoldalai
Halló, itt Joe Biden, vagy mégsem?
Halló, itt Joe Biden, vagy mégsem?

Kommentek:

Terézágyú 2024.02.29. 11:58:25

És üljünk át egy másik autóba.

Válasz erre

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

Holló a hollónak mégiscsak, de igen…

2024. március 05. 11:05 - Csizmazia Darab István [Rambo]

A történet előzménye, hogy az **ALPHV/BlackCat bűnözői kör egy alvállalkozói csoportja megtámadta a Change Healthcare rendszereit, ahol a zsarolóvírus-fertőzés gyógyszertárak és kórházak ezreit zavarta meg szerte az Egyesült Államokban, és mellesleg 6TB bizalmas adat ellopása** is nehezítette az egészségügyi szervezet helyzetét.

A UnitedHealth a támadást elismerte, a 6TB lopott adattal kapcsolatban viszont úgy nyilatkoztak, ezt még vizsgálják.

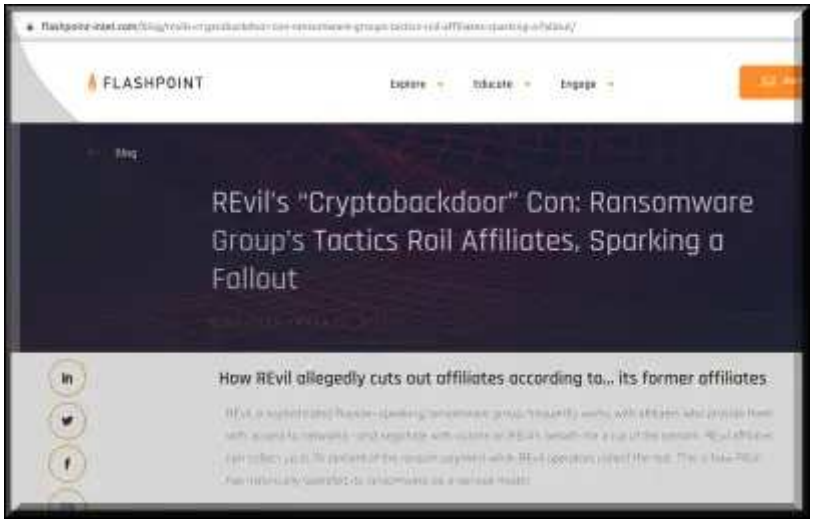
Az **USA területén több, mint 70 ezer gyógyszertár használja a szoftvereiket a receptek és betegbiztosítási igények feldolgozásában. Az elkövető orosz ALPHV/BlackCat banda pedig már ki is tette az oldalára az erről szóló bejelentést.**

Ám az igazi fordulatok még csak itt kezdődnek, ami előtt még két apró adalékot említsünk meg. **Az egyik a SickKids gyermekrák kórház 2022-**

es esete, ahol a LockBit úgy ítélte meg, etikátlanul jártak el a saját alvállalkozói, így nyilvánosan is elnézést kértek, a kórháznak ingyenes helyreállító kulcsot adtak, valamint kizárták a szerintük etikátlan érintett alvállalkozó partnerüket.

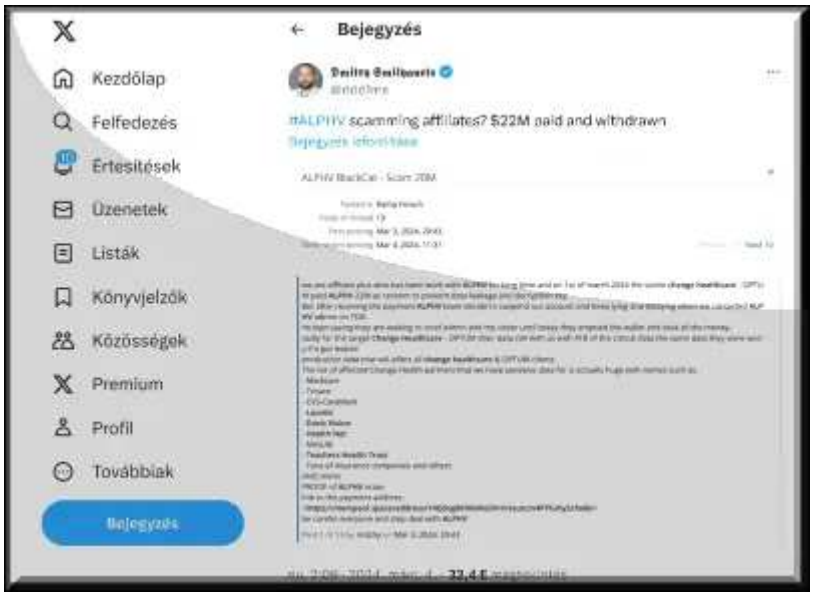
A másik előzmény pedig éppen az alvállalkozói bevételek frontális lenyúlása a ransomware csoport vezetősége által. Ahol derült ki, hogy Revil csapat nem elégedett meg a normál előre megállállapodott mértékű százalékos részesedéssel a váltságdíjakból, hanem titokban elhelyeztek a programjukban egy olyan hátsóajtót, ahol a folyamatban lévő ransomware tárgyalásokat is figyelemmel kísérhették.

És ha nagy váltságdíjjal kecsegtetett valahol egy üzlet, ők maguk közvetlenül felvették a kapcsolatot az áldozatokkal, és ők kasszírozták be a feloldó kulcsért járó összeget kizárva így saját bérlőiket.



Innen dobbantunk akkor a mostani hírre, ami azzal kezdődött, hogy hivatalosan meg nem erősítette információk szerint **március 1-én a UnitedHealth 22 millió dollár összegű váltságdíjat fizetett ki az adataik visszaszerzéséért és a lopott adatok nyilvánossá tételének megakadályozásáért.**

Ezt az értesülést ugyan sem a bűnözők, sem az egészségügyi intézmény nem kommentálta, **ám az eset egy váratlan további csavart is a felszínre hozott.**



Úgy tűnik ugyanis, hogy a **váltságdíjat bezsákoló affiliate partnert március 5-én az ALPHV/BlackCat vezetősége felfüggesztette. A kapcsolt vállalkozás bejegyzése szerint emellett a számlájukat is leürítették, azaz az ott tárolt teljes összeget elvették tőlük**.

Az alvállalkozó közben az állítja, hogy 4 TB "kritikus adat" még mindig a rendelkezésükre áll a UnitedHealth és beszállítói köréből. Az egészségügyi intézmény most attól tart, hogy bár fizettek a zsarolóknak, a belső torzsalkodás miatt mégis nyilvánosságra kerülhetnek az ellopott adatok.

Éppen a fenti aggályok miatt sajnos egyelőre nem mondhatjuk, hogy ebben a játszmában minden pofon jó helyre megy.

Irónia az a hely, ahol az irónok laknak - szól a közkeletű mondás :)
Mindenesetre irónikus módon a ransomware üzletágban tevékenykedő leányvállalatok is kiadták a saját belső figyelmeztetésüket az ALPHV csoporttal kapcsolatban, miszerint: Legyen mindenki nagyon óvatos, és senki ne üzleteljen a megbízhatatlan ALPHV bandával.

Szólj hozzá!

Címkék: usa egészségügyi affiliate alvállalkozó váltságdíj intézmény partnerség ransomware blackcat zsarolóvírus alphv

Ajánlott bejegyzések:

100 millió ember egészségügyi adata hoppszi

Change Healthcare újra pácban

Várt és nem várt mellékhatások

100 millió ember egészségügyi adata hoppszi

8 kórház, 30 klinika, 2.5 millió betegadat

Change Healthcare újra pácban

Váltságdíj a váltságdíjszedő bandákért II.

Várt és nem várt mellékhatások

Váltságdíj a váltságdíjszedő bandákért II.

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

10 tipikusan időseket célzó csalás

2024. március 07. 10:42 - Csizmazia Darab István [Rambo]

A számítógépen kívüli térben is sokféle formában támadják az időseket: túlárazott paplanos termékbemutató kirándulással, öregezéssel (érdemes lehet ehhez megnézni az Unoka című magyar filmet), de emellett az interneten is igyekeznek a bűnözők a gyanútlan, naiv és a digitális térben kevésbé jártas időseket becsapni, átverni, pénzzel lehúzni.

Az FBI statisztikája szerint 2022-ben 3.1 Mrd dollár veszteség érte a 60 év felettieket, 88 ezer regisztrált kiberincidenst jegyeztek fel ezzel kapcsolatosan. Bár ez éves szinten 82%-os növekedést jelentett az előző esztendőhöz viszonyítva, ám ez a valóságban még nagyobb lehet, hiszen az esetek jelentős részét be sem jelentik. **Érdemes lehet összefoglalni azokat a jellegzetes csalási formákat, amikkel az idős embereket megcélozzák, hiszen ezen trükkök felismerése megóvhatja őket a veszteségtől.**

1. A tízes csokor első tétele az adathalászat, ami az egyik leggyakoribb csalási forma a neten. A kéretlenül kapott üzenetben (e-mail, közösségi, SMS) kapunk egy kecsegtető, vagy sürgető-fenyegető szöveget, hogy kattintsunk a melléklet linkre vagy csatolmányra.

A kártékony URL vagy melléklet azonban eltéríti a bejelentkezést egy hasonmás oldalra, ahol ellopják a belépési adatainkat, vagy vírust, kémprogramot telepít a gépünkre.

2. Második helyen említhetjük a romantikus csalásokat, ahol a netes randizás a Covid időszak óta még inkább felfutóban van. Röviden a hamis profil mögött frissen megismert, magát gazdagnak mutató társ (külföldön szolgáló megözvegyült katona, fúrótornyon dolgozó jól kereső olajmunkás) már a kezdeti levelezős szakaszban azonnal bizalmaskodva ránk nyomul.

Majd még a személyes találkozó előtt egy adott ponton valamilyen problémás váratlan élethelyzetre hivatkozva (állásvesztés miatt, orvosi számlák ürügyén, szülők állítólagos betegsége, számlájuk téves zárolása) igyekeznek tőlünk kölcsön kérni, ezzel főképp a neten kiszemelt jól szituált, egyedülálló nőket megcélozva.

3. Harmadik tipikus átverési formában a csaló magát valamilyen ismert egészségügyi szervezet munkatársának kiadva [személyes, egészségbiztosítási számlánkkal kapcsolatos, illetve orvosi adatokat próbál meg tőlünk kicsalni](#).

Az ilyen kéretlen megkeresések gyakran **a megszokott e-mail, üzenet, SMS mellett már direkt telefonhívások formájában is** megjelenik.

4. A [hamis support csalások ugyan minden generációnál bepróbálkoznak](#), de az idősek sokszor átlag felett gyanútlanok, nehezükre esik nemet mondani, és könnyen megtéveszthetőek. Technikai támogatás ürügyén a csalók valamilyen ismert (Microsoft, IBM, stb.) segélyvonali munkatársának adja ki magát, és állítólagos vírusfertőzésre, feltörésre hivatkozva hozzáférést kér a gépünkhöz.

Ehhez legtöbbször **valamilyen távoli asztalkapcsolat (AnyDesk, RemotePC, TeamViewer) telepítését kéri tőlünk, amiért egyfelől akár egy borsos összeget is kiszámláz, de ami még rosszabb, a teljes hozzáférés révén megfertőzheti a gépünket, illetve mindent észrevétlenül ellopha**t onnan.

5. A soron következő módszer online vásárlással kapcsolatos. Hamis webáruházakkal, hihetetlen akciós ajánlatokkal bombázzák az embereket.

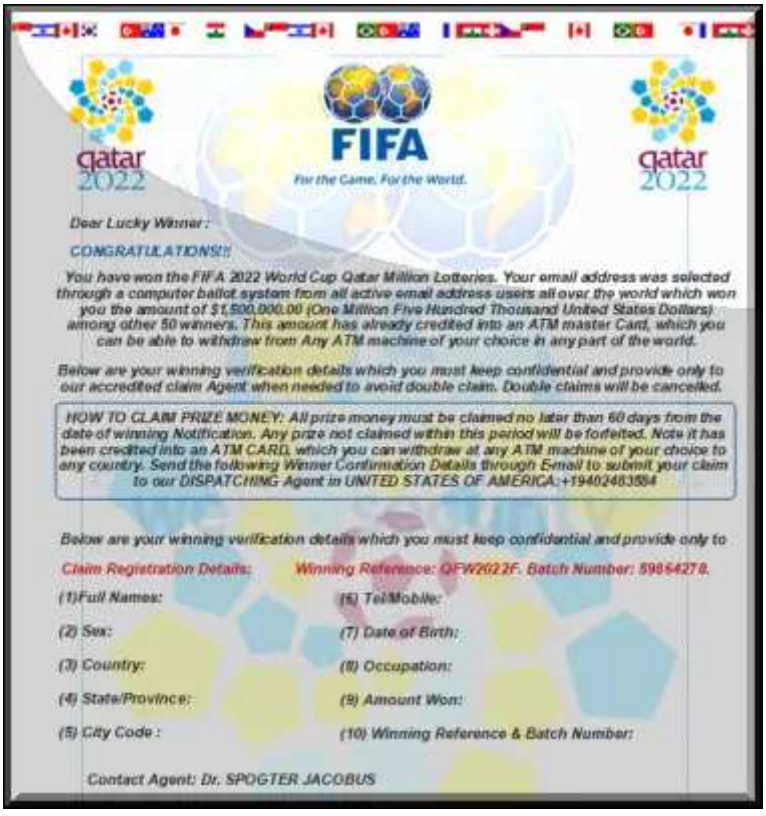
A kedvező árú termékek azonban hamisak, esetleg lopott árukról van szó, de gyakran nem is léteznek, és a bűnözők valódi célja a vásárlás során megadott kártyaadatok ellopása.

6. Hatodik helyen szerepelnek az úgynevezett robothívások, amelyek valamilyen automatizált technológiára támaszkodva bárkit, még a titkosított telefonszámot használókat is elérhetnek. A módszer előnye, hogy a csalók egyszerre nagy számú felhasználót tudnak ily módon célba venni. **Egy előre rögzített üzenetben ingyenes vagy erősen leértékelt, akciós áruk felajánlása hallható.**

De arra is volt már példa, hogy valamilyen büntetésre vagy közelgő bírósági perre hivatkozva igyekeznek megszerezni a felhasználók személyes és pénzügyi adatait. Emellett a bank nevében történő telefonhívások is egyre gyakoribbak, ahol adategyeztetésre, illetéktelen számlahozzáférésre hivatkozva ideiglenes átutalást kérnek.

7. A hetedik te magad légy, mondhatná a hivatalos és kormányzati szervek nevében jelentkező csalási módszer. Itt **be nem fizetett adókról szólnak a megkeresések, és igen szoros határidő mellett az állítólagos büntetés azonnali befizetésére szólítanak fel** bennünket.

A fenyegetés akár azt is tartalmazhatja, hogy mulasztás esetén a letartóztatást kockáztatjuk. Jellemzően az ilyen fajta zömmel angol nyelven zajló csalásokat dél-ázsiai call centerek hajtják végre.



8. A szerencsejáték csalások is igen jellemzőek, ahol valamilyen lottó vagy egyéb játékra hivatkozva arról értesítenek bennünket, hogy egy óriási összeget nyertünk. **Ehhez azonban csak valamilyen állítólagos feldolgozási, regisztrációs, ügyvédi díj vagy valamilyen adó előre befizetése után juthatunk hozzá.**

Természetesen nincs semmilyen nyeremény, aki itt fizet, az utána már bottal ütheti pénz nyomát.

9. Virtuális emberrablás névre hallgat a következő tétel. A mesterséges intelligencia hangklónozási technológiájának fejlettségé miatt ugyanis **egy MI generált hangminta már elég meggyőző ahhoz, hogy akár még a legközelebbi családtagokat is átverhessék vele**. Itt a megcélzott áldozat gyerekének a hangján pénzt követelnek a szülőktől, vagy nagyszülőktől, miközben semmi nincs a kezükben, csak a klónozott hang.

Ezek a csalások is egyre gyakoribbá válnak, köszönhetően a széles körben hozzáférhető hangklónozó szolgáltatásoknak (VcaaS, Voice Cloning-as-a-Service).

10. Végül, de semmiképpen nem utolsósorban a befektetési csalások is nagyon népszerűek a bűnözők körében. Ez a 2022-es évben több mint 3.3 milliárd dollárt hozott a konyhájukra, és sokakat sikerül átverni az állítólagos "gyors meggazdagodás" ígéretével. **Ezekben a kitalált kriptovaluta befektetéseken keresztül történő konstrukciókban alacsony kockázatra és garantált hozamokra hivatkoznak, ám a pénzt ellopják, az alapok nem léteznek, a pénz és a közvetítő is rövid úton eltűnik**.

Az is gyakori, hogy a randiappokban megjelenő új ismerős igyekszik rábeszélni az újdonsült randipartnert valamilyen kedvező

befektetésre, vagy pénzduplázásra.

Hogyan óvhatjuk meg magunkat mindezektől? Ha egy ajánlat túl szép ahhoz, hogy igaz legyen, általában csalás. Legyünk gyanakvóak a kéretlen kapcsolatfelvételek esetében! Ha telefonon keresnek bennünket, ne adjunk ki a hívó félnek semmilyen személyes adatot! Ne bízzunk a hívószám azonosításban, mert ez hamisítható. Használjunk erős jelszót és többtényezős hitelesítést fiókjainkban! Ne kattintsunk az e-mailekben/SMS-ben/közösségi üzenetekben érkező gyanús, és ne nyissunk meg ilyen mellékleteket sem!

Futtassunk naprakész vírusvédelmet, ami az adathalász linkeket is képes szűrni! Ha pedig esetleg már átverték bennünket, haladéktalanul vegyük fel a kapcsolatot a bankunkkal és a helyi rendőrséggel!

1 komment
Címkék: csalás átverés megelőzés tipikus idősek védekezés elleni welivesecurity.com

Ajánlott bejegyzések:

Booking com átverések

Fontos vagy nekem

Árad a malware a Youtube oldalain is

Booking com átverések

Black Friday és Cyber

Fontos vagy nekem

Árad a malware a

Monday járja be Európát

Youtube oldalain is

igazi károkozás

Virtuális emberrablás, igazi károkozás

Virtuális emberrablás, igazi károkozás

Kommentek:

Motorogre 2024.03.07. 18:30:44

Köszönjük, hasznosak ezek a rendszeresen ismétlődő felhívások, hogy legyünk éberek ! Ha lehet, ennél gyakorlatibb tanácsokra is szükség lenne - olyanokra, amit tényleg be lehet tartani.
A keresős-sorban a https címet figyelmesen nézzük meg - ez ok. De pl. ha megheckelték a gépet, a kedvencek közé kirakott banki link már nem biztonságos. Ezért a feketeöves nyuggerek a bank holnapjának elérhetőségét kimentik valahova, kedvencek közé nem teszik - hanem CTRL C - V -vel mindig bemásolják.
Vagy olvasnánk arról, hogy a böngésző Site Information adata megbízható-e? Sokan azzal védekeznek hogy a "Connection is secure" volt a státusz -- a pénz mégis eltünt?!
Tehát praktikus tanácsok is szükségesek, a nyuggerek nem programozók.

(egy negatív példa: a lakásba-házba érkező óraleolvasókat nem engedjük be - tanácsolja egy komoly netes forrás ! Hanem hívjuk fel a szolgáltatót és kérdezzük meg hogy tényleg az Ő embere-e?
No ekkora szamárságot csak iróasztal mellett lehet kitalálni - vagy szemlézni. Mire a kuncsaft átveregszi magát a közműcég telefonközpontját és eljut egy élő emberhez - a leolvasó rég elment. Node ha nem: az élő emberi hang közli, hogy fogalma sincs, az alvállalkozó sub-alvállalkozójának egyéni vállalkozói végzik a leolvasást).

Válasz erre

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Kriptográfiai felhasználók adathalászata

2024. március 11. 10:44 - Csizmazia Darab István [Rambo]

Erre a területre is komoly erőforrásokat mozgósítanak a bűnözők, és **hatalmas számokat láthatunk a 2024-es év első két hónapjának veszteséglistáján.**

Az adathalász támadások továbbra is jelentős veszteségeket okoznak a kriptográfiai felhasználók számára. Ha a statisztikai számokat nézzük, **az idei esztendő első két hónapja alatt történt incidensek 104 millió dollárnak (mai áron kb. 37 milliárd forint)** inthettek búcsút a kriptovaluta tulajdonosoknak.

A januári kártétel 57.7, míg a februári 46.8 milliós volt, ami egy rövidebb hónaptól is komoly teljesítmény, még ha csak 29 napos is. És **ha mindezt összevetjük az előző, 2023-as év adataival, ott a teljes év során keletkezett 300 millió dollár veszteség, tehát emelkedő tendenciát látunk.**

A Scam Sniffer biztonsági cég adatai szerint **97 ezer felhasználó esett áldozatul phishing átverésnek. Az elsődleges célpont az Ethereummal rendelkező tulajdonosok voltak, és az átverések zöme közösségi média platformokon, ezen belül is elsődlegesen valamilyen feltört, hamis X (leánykori nevén Twitter) fiókból származó adathalász bejegyzéshez** kapcsolódó rosszindulatú link volt a csali.

Az ilyen visszaélések a pénztárcában tárolt összes eszköz elvesztését eredményezhetik.

Láthatóan **a csalók kitartóan finomítgatják stratégiájukat, miközben a kriptográfiai közösségben erősíteni kellene a biztonsági tudatosságot.**

A közösségi médiaplatformokon a lopott, hamisan megszemélyesített entitásokkal szemben nagyobb elővigyázatossággal kellene eljárni, hiszen itt komoly pénzekre megy a játék, és nem igen van undo a történetben, a veszteségek többsége végleges.

A hagyományos területeken sem szünetelnek azonban a támadások, **nemrégiben például a Pepco magyarországi üzletága szenvedett ez adathalász támadást, amelynek következtében 15m EUR, hozzávetőleg 6 mrd HUF kár keletkezett.** Bár a hivatalos közlemény nem fogalmazta meg világosan, hogy pontosan mi történt, nem zárható ki, hogy **Business E-mail Compromise típusú incidens történt, amelynek révén nagy összegű átutalást téríthettek el a bűnözők. A Pepco**

állásfoglalása szerint belső céges adatok nem estek áldozatul, az ellopott pénz visszaszerzési esélyei ismeretlenek.

Emlékezetes, hogy 2022-ben szintén a levelezés feltörésével a Magyar Vizilabda Szövetségnél történt hasonló eset.

Szólj hozzá!
Címkék: email business csalás átverés phishing adathalászat bec compromise kriptovaluta

Ajánlott bejegyzések:

Az öreg adathalász, és a link tenger

Csomagja érke... Na most már elég!

Üdvözöl a bölcs csapat

MBH banki adathalászat

Csomagja érke... Na most már elég!

Üdvözöl a bölcs csapat

MBH banki adathalászat

Üdvözöl a bölcs csapat 3000%-kal több lett, maradhat?

3000%-kal több lett, maradhat?

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

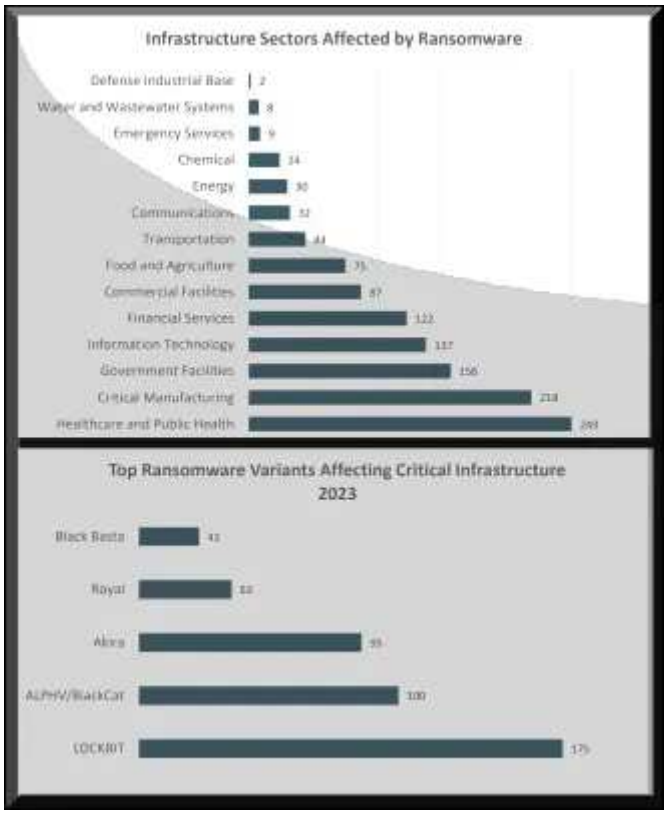
Az egészségügyet sújtotta leginkább a zsarolóvírus

2024. március 13. 10:17 - Csizmazia Darab István [Rambo]

Az FBI jelentése szerint **a 2023-as esztendő legnagyobb vesztese az egészségügyi intézmények** voltak. A vizsgált adatok szerint **az egészségügyi szektor összességében több ransomware támadást szenvedett el tavaly, mint bármely más egyéb kritikus infrastruktúrákat üzemeltető ágazat**.

Az FBI Internet Crime Complaint Center (IC3) központja rendszeres éves jelentést készít az év közben történt incidens bejelentésekből. Ezek alapján **tavaly rekordszámú, 880 ezer panasz futott be hozzájuk, az elszenvedett veszteségek pedig meghaladták a 12.5 milliárd dollárt.**

A bejelentett **incidensek száma 10 százalékos növekedést mutatott, ám a kárérték ezzel együtt már 22%-os emelkedést produkált az előző évi adatokhoz képest.** Ha próbaképp elosztjuk a 880 ezret 365-tel, akkor 2420 valamilyen támadás jön ki minden egyes naptári napra.



A szektorok közül az egészségügy volt legtöbbször áldozat, ezt követte a gyártási ágazat, és ezt követték más egyéb kritikus infrastruktúrával kapcsolatos területek. Hogy miért szerepelhetnek ilyen nagy szám elsősorban kórházak és egészségügy intézményeket ellátó, kiszolgáló cégek, hivatalok, abban több tényező is szerepet játszik.

A gyengébb IT biztonsági ellátottság, a nagyobb váltságdíj fizetési hajlandóság az emberéleteket követelő leállások elkerülése érdekében, illetve valószínűleg itt sokkal nagyobb lehet a bejelentési hajlandóság is, mint egyéb területeken.

A támadási típusok között toronymagasan az adathalászat vezet, ezt követik az adatvédelmi incidensek, ahol személyes adatokhoz férnek hozzá illetéktelenül. **A 2023-as zsarolóvírus támadások során az egészségügyet megcélzó két legaktívabb szereplő a LockBit és az ALPHV/BlackCat csoport voltak.**

Ezek az orosz kötődésű bűnözői csapatok 175, illetve 100 alkalommal hatoltak be, loptak el onnan adatokat és zsaroltak meg kórházi szervezeteket.

Azt láthatjuk, hogy a ransomware széles körben elterjedt probléma volt a 2023-as évben, a 2800 bejelentett esetszám 18 százalékos növekedést mutat 2022-höz képest. Emellett **az ilyen incidensekből származó veszteségek mértéke is megugrott, 34 millió dollárról 59 millió dollárra nőtt, nagyjából 74%-kal drágult.**

Bár időnként látszólag történnek letartóztatások, házkutatások, vádemelések, géplefoglalások, összességében azonban sajnos folyamatos működés érzékelhető a bűnözőknél, akik **az egyes bandák lekapcsolása után azonnal másik bűnszervezetben folytatják a tevékenységüket, például többen a Lockbit után az Akira csapatban intézik tovább a támadásaikat.**

Szólj hozzá!
Címkék: statisztika kórház fbi egészségügy ransomware zsarolóvírus ic3

Ajánlott bejegyzések:

A ransomware az egészségügyben élet-halál kérdése
Kórházak a pácban II.


100 millió ember egészségügyi adata hoppszi
A ransomware az egészségügyben élet-halál kérdése
Kórházak a pácban II.
8 kórház, 30 klinika, 2.5 millió betegadat
100 millió ember egészségügyi adata hoppszi
A kriptobevételek felett az égbolt felhőtlen
A kriptobevételek felett az égbolt felhőtlen
A kriptobevételek felett az égbolt felhőtlen
A kriptobevételek felett az égbolt felhőtlen

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Rabszolgamunka a kiberbűnözők fogságában

2024. március 18. 09:46 - Csizmazia Darab István [Rambo]

Nem akart ez cím túlságosan fellengzős lenni, de végeredményben pontosan erről van szó. **Hajlamosak vagyunk arra, ha csaló e-mailt, átverős SMS-t, becsapós közösségi üzenetet kapunk, azonnal magának a küldőnek és felmenőinek melegebb éghajlatra küldésére gondolni, ám a helyzet ennél árnyaltabb és sokszor sajnos rosszabb.**

Arra talán mindenkinek akadt példa az életében, hogy **egy ismerősétől úgy kapott üzenetet, hogy maga az ismerős nem is tudott annak elküldéséről, hanem megfertőződött a gépe, vagy eltérítették a közösségi médiás profilját. Spam küldésnél, de újabban akár a smishing eseteknél - például a FedEx-es csomagja érkezett incidensben - is gyakori, hogy a megfertőzött készülékek is részt vesznek a terjesztésben az eszköz tulajdonosának tudta nélkül.**

És ugyanez a helyzet a botnetek esetében is, ahol egy zombihálózat részeként a fertőzött eszköz spamek kiküldését, zsarolóvírus terjesztését végzi. Ezeken naprakész vírusvédelemmel és biztonságtudatos hozzáállással azért elég könnyen lehet segíteni.

Ám amiről mostanában **egyre gyakrabban szó esik, az már az emberkereskedelem címszó alá** sorolható.

Ebben a konstrukcióban úgy indul a történet, hogy a **gyanútlan és sokszor rossz anyagi helyzetben lévő emberek kapva kapnak az olyan külföldi álláshirdetéseken, amik sokszor még hihetőnek és legitimnek is látszanak: vendéglátóipari és egyéb munkalehetőségek Fülöp-szigeteken**.

Azonban a jelentkezők legrosszabb rémálma valósult meg, **megérkezésükkor bezárták őket, elvették az útlevelüket, és arra kényszerítették őket, hogy az interneten gazdag, jól szituált embereket romantikus csalással megkárosítsanak**: javasoljanak nekik hamis kriptobefektetést, vagy mondvacsinált ürügyekkel kérjenek "kölcsön" nagyobb összegeket.

A fogságban lévő embereket ha nem teljesítették a normát, megkínozták: bezárták, megverték, nem hagyták aludni vagy elektromos árammal sokkolva égették meg a testüket.

A mostani esetnél egy vietnámi áldozat értesítette a hatóságokat, akit egy szakács állásajánlattal csaltak az országba. **A fülöp-szigeteki rendőrség több száz rabszolgát szabadított fel - köztük 504 külföldi állampolgárt - a Tarlac Pogo nevezetű, papíron casino és szerencsejátékkal foglalkozó vállalkozás telephelyéről.**

A kimentett áldozatok Vietnámból, Kínából, a Fülöp-szigetekről, Ruandából, Tajvanról, Indonéziából és Kirgizisztánból érkeztek, és hamis profilok mögül kellett nekik a randizás nevében másokat megkárosítani, ehhez egy naponta teljesítendő kvótát is előírtak számukra.

A razzia során a hatóságok a Manilától nagyjából 100 kilométerre északra található tíz hektáros területen lévő telephelyen a letartóztatáskor fegyvereket, éles lőszert, mobiltelefonokat, SIM-kártyákat, számítógépeket és több tucat lopott gépjárművet is lefoglaltak.

A vádemelés szerint egy nemzetközi bűnbanda állt a háttérben, a helyi egyetlen fülöp-szigeteki beépített emberükön kívül több kínai, valamint vietnámi és malajziai bűnözők működtették a kétes bizniszt.

Sajnos azt látni, hogy Délkelet-Ázsiában általánossá váltak az embercsempészet és rabszolgasorba kényszerített munkaerővel dolgozó hasonló átverések. Tavaly októberben a Fülöp-szigeteki hatóságok razziát tartottak egy internetes szerencsejáték-engedélyezési központban, **ahol szexkereskedelemmel, hamis kriptobefektetésekkel és szintén romantikus csalásokkal foglalkoztak nagyüzemben.**

Emellett más országokban is, például Kambodzsában, Laoszban és Mianmarban is lepleztek már le online kényszermunkát végeztető bűnözői csoportokat. **A sok tanulság közül az egyik az lehet, hogy kiemelt óvatossággal kell eljárni a külföldi állásajánlatok esetén.**

Szólj hozzá!
Címkék: emberrablás csalás átverés kényszermunka letartóztatás romantikus razzia bűnbanda emberkereskedelem bűnözők fülöp-szigetek kriptobefektetés

Ajánlott bejegyzések:

Piszkos hadviselés
A kriptobevételek felett az égbolt felhőtlen
A call centerek farkasai
Virtuális emberrablás, igazi károkozás

Piszkos hadviselés
A kriptobevételek felett az
A call centerek farkasai
Virtuális emberrablás,

égbolt felhőtlen

igazi károkozás

Csalás jönni TikTokra

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

Magyar Posta elvágta, indiai gyógyítja

2024. március 21. 11:54 - Csizmazia Darab István [Rambo]

Sherlock Holmes története is lehetne "A visszatartott csomag esete" címmel, de ez a mostani eset korántsem annyira csavaros sztori. Amióta 2021. márciusában, szinte napra pontosan 3 évvel ezelőtt beesett a "Megérkezett a csomagja, kövesse nyomon..." kezdetű Flubot vírussal fertőző **magyar nyelvű FedExre hivatkozó SMS, már tucatnyi újabb próbálkozást tapasztalhattunk.**

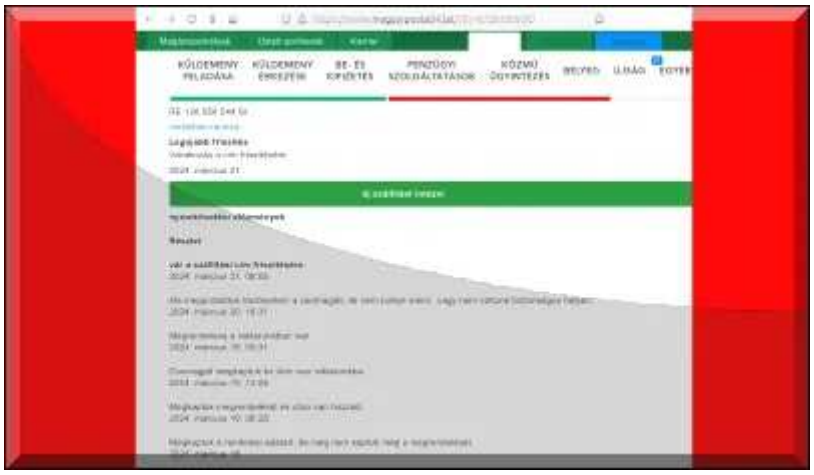
Az eredeti forgatókönyv alapján **elég sok hibát kellett elkövetni ahhoz, hogy valaki áldozat legyen. El kellett hinni, hogy valóban csomagunk érkezett, annak nyomkövetéséhez egy külső zavaros kinézetű linkről alkalmazást kellett letölteni, azt fel kellett telepíteni, és ehhez minden létező engedélyt megadni neki.**

Aki gyanút fogott, biztonságtudatos volt és/vagy használt antivírust a telefonján, az mentesült a következményektől: **adatlopás, nehezen eltávolítható kártevő, plusz a telefonunkról rejtetten továbbküldött SMS-ek díja is feltűnt az áldozatoknak számlafizetéskor**, volt akinek 4700 szöveges üzenet után 160 ezerrel több pénzt kellett kifizetnie.

Mai történetünkben is **SMS érkezett a Magyar Posta nevében, és már nulladik lépésben feltűnhet az éles szeműeknek, hogy vajon a +91 országkóddal vajon miért Indiából üzennek nekünk erről, és miért olyan domain névre hivatkoznak, ami Guyanában (.gy) van?**

A szövegezést és a nyelvtant szemlátomást nem nézte át a Magyar Tudományos Akadémia nyelvi főmunkatársa, a **helyesírási hibák, magyartalanság is gyakori jele a csalásoknak**.

"*[Magyar Posta]A csomagja visszatartva lett, mert hiányzik a címzésen lévő házszám. Kérem frissítse a szállítási információkat:*" **és egy link, ami még hunyorított szemmel sem hasonlít a Magyar Posta webcímére - harmadik intő jel.**



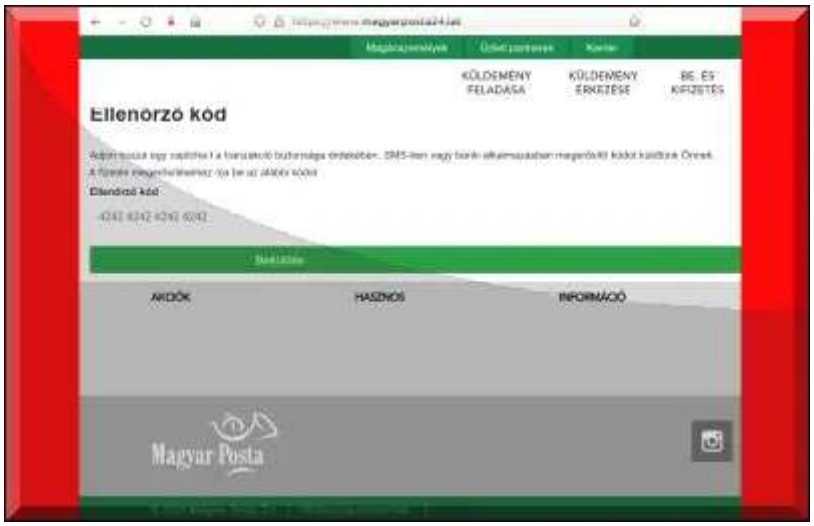
A linket a böngésző asztali gépen nem is nyitja meg, nem jelenik meg tartalom, ám pici trükkel - User Agent Switcher segítségével Androidot hazudunk be, és máris láthatóvá válik az oldal.

A szövegek itt is viccesek, Török Szultán és Fülig Jimmy like this, felváltva tegeznek és magáznak, és hát **a Latin Amerikához tartozó .lat domain végződés is ott mocorog a képernyőn** - szóval gyanús jelekből Dunát lehetne rekeszteni.

Megadjuk próbaképp az összes bizalmas személyes adatunkat, és **figyeljük a lényeget, mikor várja majd a fizetési infókat.** Mert várni fogja, az tutiság.

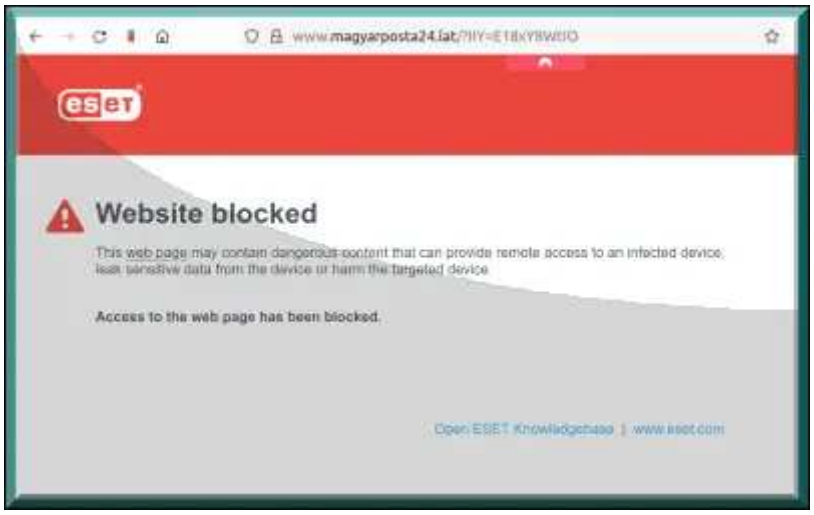
Ami meg is érkezik nyomban, egy nem túl jelentős 490 forintos állítólagos plusz extra díj fizetése vár ránk. Az Élet értelme 42, és ez egyben egy jó teszt szám is bankkártyákat bekérő oldalakhoz, ilyenkor nem is kell fake sorszám generátorokkal vesződni, a lejárati dátum és CVV kód is lehet a tesztnél bármi.

Itt az alacsony összeg csak elterelés, a kártyaadatok megszerzése az igazi célja a csalóknak.



Lehetett volna a cím Csomagja érkezett 672854 is, de ebben most annyi ordító gyanús elem volt, hogy talán megérdemelt különbejáratú bejegyzést.

Ha visszaengedélyezzük a korábban letiltott vírusvédelmet, akkor érkezik is a piros ablak, és a blokkolás, miszerint kártékony tartalom található a weboldalon.



Érdemes tehát továbbra is ésszel kattintgatni, különösen mobilon, ahol a kis kijelző miatt sokszor amúgy sem látjuk, pontosan éppen hol is járunk, mert a Csomagja érkezett átverési sorozat még hosszú ideig adja majd nekünk az új évadokat és új epizódokat.

1 komment
Címkék: magyar posta india csalás átverés visszaélés adathalászat smishing guayana

Ajánlott bejegyzések:

Üdvözöljük, csomagja kézbesítésre vár

2023. első csalásai

Adathalászat vagy jófogás?

Csomagot kaptam life...

Mai szavunk pedig: smishing

Adathalászat vagy jófogás?

Kommentek:

Head Honcho 2024.03.21. 14:05:23

És mint mindig: ha nem volna elég Hiszékeny úr, nem csinálnák. Sajnos honunk pénzügyi és informatikai ismeretei a béka feneke alatt, de nem is kell messzire menni, mert az átlagember a saját anyanyelvével sem birkózik meg a közösségi oldalak tanúsága szerint. Miből gondoljuk, hogy értik az árnyalatokat? Van, akinek ez így helyes, ahogy ezen kamuoldalak kommunikálnak.

Válasz erre

keresés

tweetz

Facebook

Tovább a Facebook-ra

Várt és nem várt mellékhatások

2024. március 26. 11:48 - Csizmazia Darab István [Rambo]

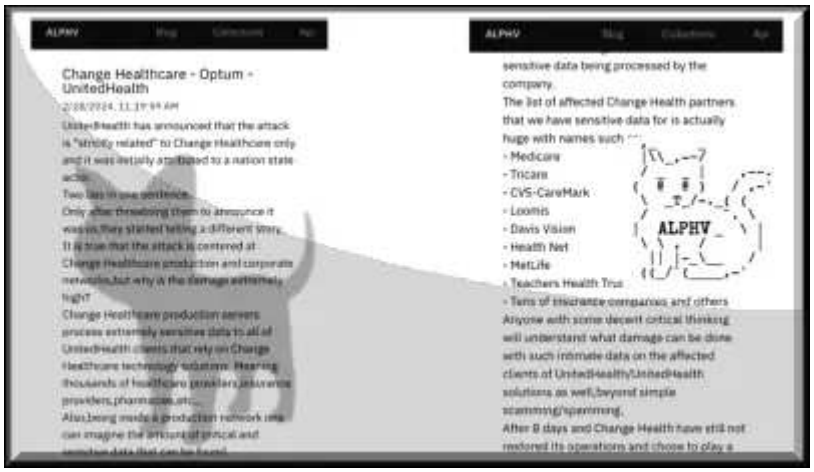
Mellékhatások tekintetében keresse fel orvosát, gyógyszerészét - szól a szlogen, ami több dolgot is figyelmen kívül hagy, például ha az embernek nincs is gyógyszerésze. Eleddig jobbára **csak arról szóltak az ilyen történetek, hogy a kórházak nem működtek, a betegek hoppon maradtak. Egy extrém módon elhúzódó ügymenet azonban rajtuk kívül még több szereplőnek is komoly gondokat okozhat.**

Egészségügyi intézmények, kórházak sem maradtak ki a zsarolóvírusok rendszeresenek mondható támadásaiból, sőt egy idő után már kifejezetten kedvelt célpontokká váltak. Hogy ilyenkor mi történik, arról már többször is írtunk: **osztályok leállása, tervezett és sürgősségi műtétek elmaradása, betegek átirányítása más intézményekbe, leletek online kiadása helyett utazgatás, számítógép helyett papír, ceruza, kartoték, telefon és fax.**

Ja **és persze a félelem, hogy az ellopott bizalmas adatokat nyilvánosságra hozhatják, azokat bárkinek eladhatják, illetve az érintettek körét testre szabott további célzott** kifinomult csalásokkal támadhatják.

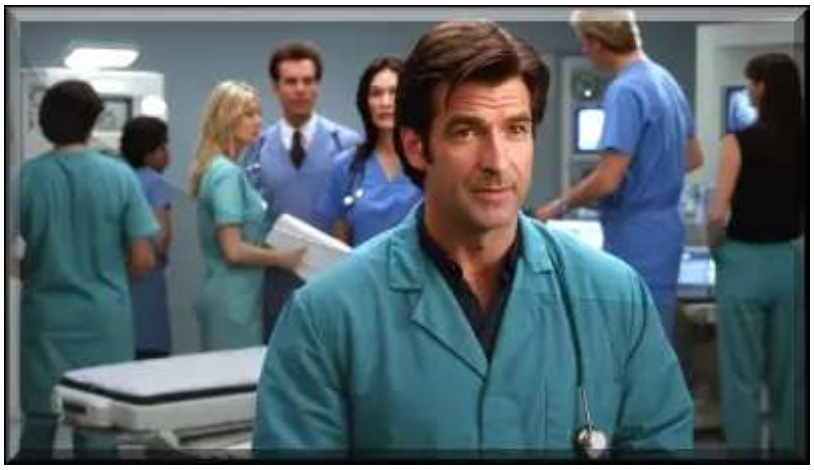
Korábban már beszámoltunk a Change Healthcare egészségügyi szervezet elleni ransomware incidensről, amelynél az oroszországi ALPHV/BlackCat vezetősége egész egyszerűen elvette a váltságdíjként beszedett pénzt az általa alkalmazott alvállalkozó bűnözőktől.

Ezzel a lépéssel jócskán megnehezítette az intézmény helyzetét, **akik a fizetés ellenére aggódhattak, hogy meglopott bűnözői csoport az ellopott bizalmas adatokat ezek után esetleg mégis nyilvánosságra hozhatják, vagy új követeléssel állnak elő**.



Ezúttal **egy új szemszög is bekerült a fenti diskurzusba, az ott dolgozó orvosok helyzete**. Ugyanis az adminisztráció teljes leállása miatt a társadalombiztosítási elszámolás rendszere is megakadt. A doktorok a praxisaik utáni elszámolásukat is korábban ebben, az ország legnagyobb biztosítási számlázási hálózatában végezték, **a február 21-i leállás óta azonban még mindig nem sikerült teljeskörűen helyreállítani az üzemszerű működést, pedig itt dolgozzák fel az USA-n belüli összes orvosi elszámolás mintegy felét.**

A kiberbiztonsági incidens viszont több tízezer kórház, orvoscsoport, fogorvos és gyógyszertár kifizetését és vényköteles gyógyszerek feldolgozási folyamatát szakította meg.



A hétköznapi normál ügymenet szerint az orvosok korábban hozzávetőlegesen 2 héten belül megkapták a pénzüket az online elszámolás és elektronikus számlázás keretében, ám ezt az elhúzódó incidens miatt nem tudták megtenni.

Bár elvileg lehetőség lenne a nehézkesebb, és sok adminisztrációs plusz munkát okozó papíralapú benyújtásra is, ám ezek hivatali átfutása és elbírálása legalább kétszer hosszabb ideig tartana. A UnitedHealth Group leányvállalata, a Change Healthcare már a múlt hétre ígérte az elszámolási rendszer teljes körű újraindulását, ez még sokaknál még azóta sem üzemel.

Az orvosok elmaradt bevételeik miatti panaszára válaszként az ottani Egészségügyi Minisztérium ideiglenes könnyítéseket javasolt a papíralapú elszámolásoknál, hogy ezek egyszerűbben, könnyített benyújtási határidőkkel és gyorsabban elintézhetőek legyenek.

Illetve indult emellett egy átmeneti finanszírozási kölcsönrendszer is, amellyel a kiesett bevételek okozta helyzetben igyekeznek segíteni az arra rászorulók **olyan orvosoknak, akiknek a bevételei nagyrészt vagy teljes egészében innen származnak.**

A UnitedHealth tájékoztatása szerint a leállás miatti több mint 14 milliárd dolláros követeléshátralék utólagos feldolgozása és elszámolása már elkezdődött, ezek kifizetése állítólag hamarosan meg fog történni.

Külsős biztonsági szakértők véleménye szerint az elhúzódó folyamatok arra utalnak, hogy az egészségügyi intézménynek valószínűleg nem volt megfelelő biztonsági mentése, valamint letesztelt incidensreagálási terve.

Szólj hozzá!
Címkék: kalifornia united group health váltságdíj healthcare change ransomware blackcat zsarolóvírus alphv

Ajánlott bejegyzések:

100 millió ember egészségügyi adata hoppszi
Change Healthcare újra pácban
Holló a hollónak mégiscsak, de igen...
Váltságdíj a váltságdíjszedő bandákért II.

100 millió ember egészségügyi adata hoppszi
Change Healthcare újra pácban
Holló a hollónak mégiscsak, de igen...
Váltságdíj a váltságdíjszedő bandákért II.

[8 kórház, 30 klinika, 2.5 millió betegadat]

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Halálos fegyver: doxing

2024. március 28. 16:38 - Csizmazia Darab István [Rambo]

A brit The Big Issue, amely egy hajléktalanokat segítő utcai újság és egyben szociális vállalkozás anyavállalata, elsőre nem tűnhet különösebben komoly és értékes célpontnak egy zsarolóvírus támadáshoz. **Ám a Qilin ransomware banda ezt másképpen gondolta.**

A Qilin egy vélhetően orosz bűnözői csoport, a ransomware-as-a-service (RaaS) szolgáltatást működtet, a kódjaikat Rust és Go program nyelveken, oroszul írják. A nekik bedolgozó alvállalkozói kör, amely effektíve a spammelést, a fertőzés terjesztését, a váltságdíj tárgyalásokat lebonyolítják, a teljes bevétel 80 százalékáért dolgoznak.

Az ügymenet állandó eleme a doxing, amelyben az adatlopás bizonyítékául képernyőképeket is publikálnak nyilvánosan, fokozva a nyomást az áldozatokon.

Esetünkben **a vállalat nem egy hatalmas multicég, bár ez a világ egyik legszélesebb körben terjesztett utcai hajléktalanok által árult magazin. Körülbelül egy hete küzdenek a támadással. Egy 12 képből álló kiszivárogtatásból erősen úgy tűnik**, nem voltak a topon az adatvédelem területén, vélhetően nem volt teljes munkaidős saját informatikai részlegük sem.

Megtették a bejelentést a hatóságok felé az incidensről, és bár úgy nyilatkoztak, hogy nem találtak bizonyítékot személyes adatokkal való konkrét visszaélésről, a későbbiekben ennek az ellenkezője is kiderülhet.

Mindenesetre már a március 23-i előzetes kiszivárogtatásban is roppant kínos dolgok szerepeltek, például nyilvánosságra kerülhetett Paul Cheal, a Big Issue Group vezérigazgatójának vezetői engedélye és fizetése (120 ezer angol font körüli), illetve Danyal Sattarnak, a vállalat befektetési vezérigazgatójának útlevele és banki adatai is.

Emellett rengeteg alkalmazotti személyes adat, útlevelek beszkennelt képei, teljes neveket, munkahelyi e-mail-címeket és otthoni lakcímeket tartalmazó Excel táblázatok - ízelítőként az összesen 550 GB méretű ellopott adatmennyiségből. A munkavállalói adatokon felül szerződések, beszámolók, partneradatok, pénzügyi jelentések, banki tranzakciós adatok is szerepelnek még a hatalmas adatcsomagban.

Nagy kérdés hogy fognak-e, vagy hogy egyáltalán tudnak-e fizetni esetleges váltságdíjat, és sokak szerint egy ilyen jótékonysági intézmény elleni incidens hasonlóan tisztességtelen, mint kórházakat, szociális és egészségügyi intézményeket támadni.

Az ellenvélemény szerint az ilyen vállalkozások kihasználják a nehéz helyzetben lévőket, és érdemi segítség helyett hosszú távon ebben a formába kényszerítik őket.

Ennek eldöntésére nem vállalkozunk, mindenesetre jó példa arra, hogy bármilyen cég megtámadása és kiszivárogtatása lehet roppant kellemetlen.

2 komment
Címkék: brit uk big váltságdíj issue ransomware zsarolóvírus doxing

Ajánlott bejegyzések:

Újabb rombolás brit kórházakban

Ransomware a Volkswagennél

Senki többet harmadszor?

Újabb rombolás brit kórházakban

Windows frissítés vagy mégsem?

Ransomware a Volkswagennél

Senki többet harmadszor? Kórházak a pácban II.

Kórházak a pácban II.

Kommentek:

Head Honcho 2024.03.29. 23:34:57

Amellett, hogy gerinctelen maga a hack és a lopás, nem látom be, hogy ilyen érzékeny adatokat miért kell nyilvánosan is elérhetővé tenni.

Válasz erre

manson karcsi · goo.gl/FVvVX 2024.04.06. 06:59:51

azért az az 56 millió nem rossz havibér, vagy ha éves bruttó, még úgy sem.

Válasz erre

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkereső csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

MBH banki adathalászat

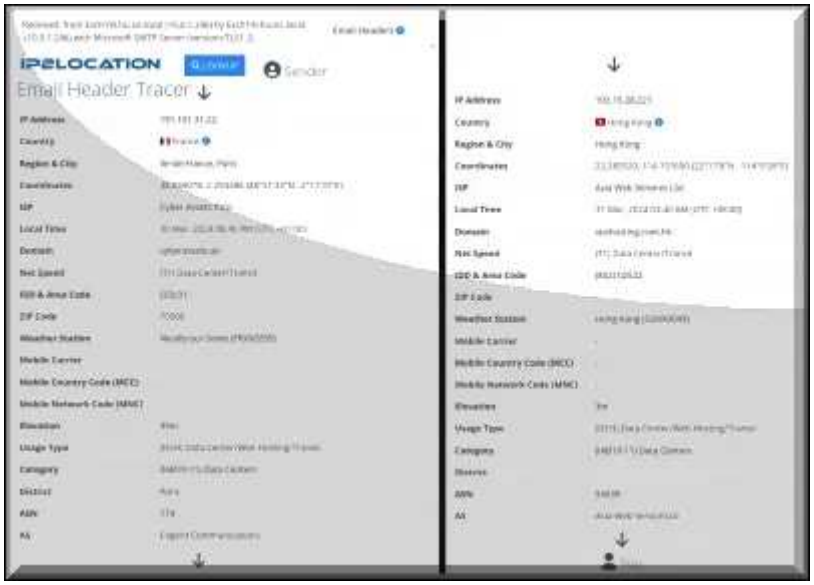
2024. április 02. 13:00 - Csizmazia Darab István [Rambo]

Ez a típus eddig elkerült bennünket, de most végre a mi postaládánkba is érkezett belőle. **Minden bank nevével vissza szoktak élni a csalók**, és ez alól ez sem kivétel.

Bárkinek érkezhet ilyen üzenete, **akár ügyfele a pénzintézetnek, akár nem, hiszen ez egy tömegesen kiküldött e-mail. A levél szövege sürget, bajban vagyunk, tehát eszerint kattintsunk:** "*MBH-fiókjának jelszava 24 órán belül lejár. A felfüggesztés elkerülése érdekében jelentkezzen be és frissítse jelszavát, vagy keresse fel a bankot a lehető leghamarabb.*".

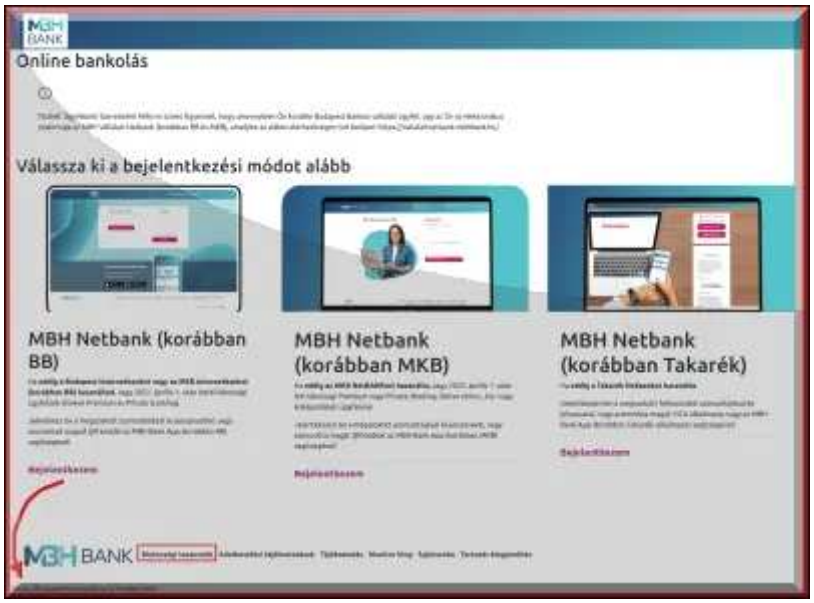
Ha megnézzük a címzést és a feladót, akkor ott az accessim KUKAC dnbecklanca PONT nl, vagyis **egy hollandiai küldő látható, míg a**

[kattintható link egy varsói, tehát lengyel akkumulátor üzlet feltört weboldalán](#) található landing page-re mutat.



Csak a hecc kedvéért ránézünk a levél trace történetére is. **Ez pedig egy francia IP címet mutat, ami vagy onnan jött, vagy egy francia VPN mögül küldték.**

Tegye fel a kezét, aki a fentiek alapján valóságos hivatalos üzenetnek gondolja ezt! **Az ilyenekből százból százat kisujj eltartva azonnal fel kellene ismernie már mindenkinek.**



Nézzük meg alaposan ezek után, hogy pontosan mi is látható a hasonmás weblapon. **Például sok magyartalanság, és a legalsó sorban: "*Biztonsági tanácsokk*". Itt egyébként mindegyik link egy fix helyre mutat, de közülük egyik sem működik.**

Ezek után vizsgáljuk meg, miket kérdezgetnek tőlünk csalással foglalkozó felebaratáink. **Banki azonosító és jelszó, az nyilván kell nekik.**

Majd kérik az SMS kódot is, amelynek eredetileg az lenne a célja, hogy plusz rétegként mint kétfaktoros autentikáció, a fiókunkat védje.

Ám ha valaki óvatlanul ezt is begépeli ide a csalóknak, akkor tálcán kínálja fel, hogy azok immár az ő nevében beléphessenek a bankfiókjába.

A személyes adatok közül a születési dátumot is kérdezik, majd újabb SMS bekérő ablak jön fel, ahonnan aztán már nem sikerült továbblépni.

Lejelentettük a hatóságoknak a banki csaló üzenetet, és lengyel testvéreinket is rögtön figyelmeztettük a felnyomott weblapjukkal kapcsolatosan. A banki csalások száma azonban továbbra is felfutóban van.

Szólj hozzá!
Címkék: weboldal bank csalás átverés phishing adathalászat banki mbh feltört

Ajánlott bejegyzések:

MBH-fiókjának jelszava 24 órán belül lejár

Csomagja érke... Na most már elég!

Fontos vagy nekem

MBH-fiókjának jelszava 24 órán belül lejár

Adathalászat menni booking.com

Csomagja érke... Na most már elég!

Fontos vagy nekem

Üdvözöl a
bölcs csapat

Üdvözöl a
bölcs csapat

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

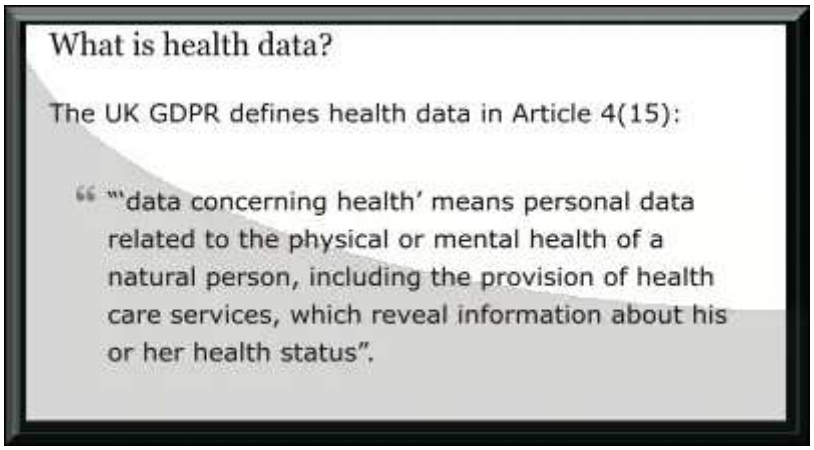
Betegeskedő egészségügyi alkalmazások

2024. április 04. 11:56 - Csizmazia Darab István [Rambo]

A digitális világban ma már szinte **mindenre van egy alkalmazás. Az egyik leginkább fellendülő az egészségügy**. A női ciklus követésétől kezdve a mentális egészségen át a mindfulnessig (tudatos jelenlét) szinte bármilyen helyzetre **léteznek egészségügyi (mHealth) appok. A piac már most kétszámjegyű növekedést produkál**, és 2030-ra a becslések szerint 861 milliárd dollárt fogja elérni.

Érdemes óvatosnak lennünk, hogy kivel osztjuk meg a legérzékenyebb adatainkat - figyelembe véve egyes egészségügyi appok aggályos adatgyűjtési szokásait. **Amikor ezeket az alkalmazásokat használjuk, hajlamosak vagyunk a legérzékenyebb adatainkat is megosztani.**

A **GDPR az egészségügyi információkat "különleges kategóriájú" adatoknak minősíti**, ami azt jelenti, hogy nyilvánosságra kerülve jelentős kockázatot jelenthetnek az egyén alapvető jogaira és szabadságára nézve. Ezért a szabályozó hatóságok extra védelemre kötelezik a szervezeteket.

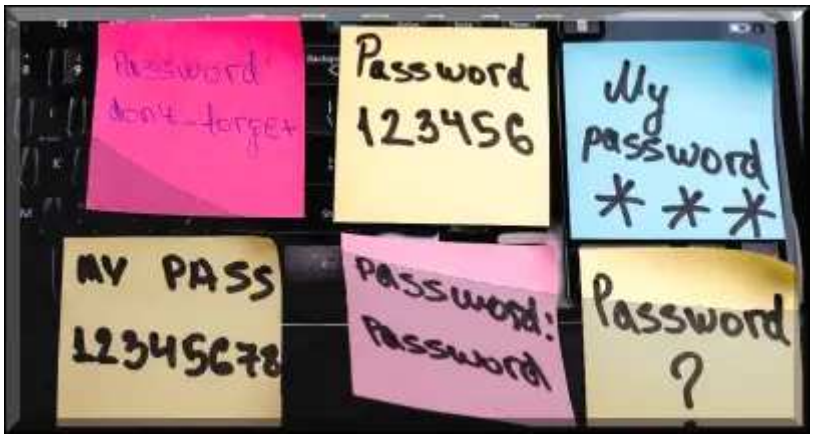


Amellett, hogy ezek az alkalmazások igen hasznosak, hiszen figyelhetik az idős emberek mozgását és baj esetén riaszthatnak, monitorozzák a vízivási, sportolási és alvási szokásainkat, kontroll alatt tartják a súlyunkat, emlékeztetnek a gyógyszer bevételére, ám emellett azért sok veszélyt is jelenthetnek.

Sajnos nem minden alkalmazásfejlesztő tartja szem előtt a felhasználók érdekeit, vagy nem mindig tudja, hogyan védje meg őket. Előfordulhat, hogy spórolnak az adatvédelmi intézkedésekkel, vagy nem mindig teszik egyértelművé, hogy a személyes adatokból mennyit osztanak meg harmadik felekkel.

Ezt szem előtt tartva érdemes megvizsgálnunk az egészségügyi appok használatának fő adatvédelmi és biztonsági kockázatait, hogy biztonságban maradjunk.

Melyek az egészségügyi alkalmazások legfőbb adatvédelmi és biztonsági kockázatai? Az ESET kiberbiztonsági szakértői szerint az mHealth-alkalmazások használatának fő veszélyei három kategóriába sorolhatók: elégtelen adatbiztonság, a túlzott adatmegosztás és a rosszul megfogalmazott vagy szándékosan félreérthető adatvédelmi irányelvek.



1. Adatbiztonsági problémák: ezek gyakran abból adódnak, hogy a fejlesztők nem tartják be a kiberbiztonságra vonatkozó legfontosabb szabályokat.

- Már nem támogatott vagy nem frissülő alkalmazások: előfordulhat, hogy a gyártók nem rendelkeznek sérülékenység közzétételi irányelvvel, vagy nem érdekeltek termékeik rendszeres frissítésében. Bármi legyen is az ok, ha egy szoftver nem kap frissítéseket, az egyben azt is jelenti, hogy tele lehet sebezhetőségekkel, amelyeket a támadók kihasználhatnak.

- Nem biztonságos protokollok: a nem biztonságos kommunikációs protokollokat használó applikációk révén a hackerek megszerezhetik a felhasználók adatait akár a szolgáltató back-end vagy felhőszerveréből is, ahol azokat kezelik.

- Nincs lehetőség többtényezős hitelesítésre (MFA): a legtöbb jó hírű szolgáltató ma már MFA-t kínál a biztonság erősítésére a bejelentkezés során. Enélkül a bűnözők ellophatják adatainkat, például adathalász támadás révén.

- Gyenge jelszókezelés: olyan alkalmazások, amelyek lehetővé teszik a felhasználó számára a gyári alapértelmezett jelszavak megtartását, vagy nem biztonságos hitelesítő adatok beállítását, mint a "qwerty" vagy a "123456". Ezáltal olyan támadások veszélyének lehetünk kitéve, mint az automatizált jelszavakat kihasználó credential stuffing vagy a lehetséges karakterek kombinációiból jelszó-variációkat összeállító brute force (próbálgatásos) támadások.

- Vállalati biztonság: előfordulhat, hogy az alkalmazást fejlesztő vállalat saját adattárolási környezetében kevés biztonsági ellenőrzést véges vagy alacsony biztonságú folyamatokat alkalmaz. Ilyen hiányosság például a korlátozott kártevő- és végpont/hálózati észlelés, az adattitkosítás hiánya, a limitált hozzáférés-ellenőrzés, valamint a sérülékenység-kezelés és az incidensek kezelésére szolgáló folyamatok hiánya. Ezek mind növelik egy lehetséges adatvédelmi incidens esélyét.

2. Túlzott adatmegosztás: a felhasználók egészségügyi információi rendkívül érzékeny adatokat tartalmazhatnak szexuális úton terjedő betegségekről, kábítószer-függőségről vagy más olyan egészségügyi állapotokról, amelyeket az alkalmazásüzemeltetők eladhatnak vagy megoszthatnak harmadik felekkel. Köztük hirdetőkkel, marketing és célzott hirdetések készítése céljából. A Mozilla tavaly 32 mHealth alkalmazást vizsgált meg biztonsági szempontból, az általuk felsorolt példák között szerepelnek olyan szolgáltatók, amelyek:

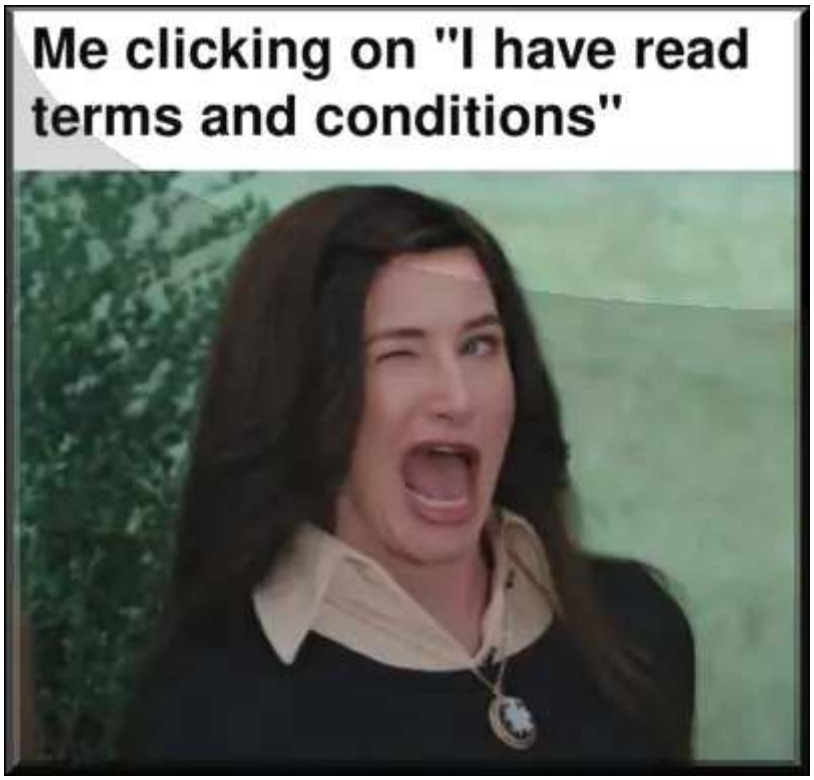
- a felhasználókra vonatkozó információkat kombinálják az adatbrókerektől, közösségi oldalakról és más szolgáltatóktól szerzett adatokkal, hogy **teljesebb személyiségprofilokat állíthassanak össze,**

- nem teszik lehetővé a felhasználók számára, hogy ebből **bizonyos adatokat törölhessenek,**

- olyan információkat használnak fel, amelyeket a felhasználóktól kaptak meg a **regisztrációs kérdőívek kitöltésekor, a szexuális irányultságra, depresszióra, nemi identitásra és más érzékeny kérdésekre** vonatkozóan,

- **engedélyezik a harmadik féltől származó munkamenet (session) sütiket**, amelyek azonosítják és nyomon követik a felhasználókat más weboldalakon, hogy releváns hirdetéseket jelenítsenek meg,

- lehetővé teszik **a munkamenet rögzítését**, amely figyeli a felhasználó egérmozgásait, görgetését és gépelését.



3. Nem egyértelmű adatvédelmi irányelvek: az ESET kutatói arra is felhívják a figyelmet, hogy egyes mHealth-szolgáltatók nem tájékoztatnak világosan a felsorolt adatvédelmi gyakorlatokról, **szándékosan homályosan fogalmaznak vagy a tevékenységet az ÁSZF apró betűs részébe rejtik**, ami hamis biztonságérzetet ad a felhasználóknak.

Európa legfontosabb adatvédelmi törvénye, a GDPR igen egyértelműen fogalmaz a különleges kategóriájú személyes adatokat kezelő szervezetek tekintetében. **A fejlesztőknek adatvédelmi hatásvizsgálatot kell végezniük, be kell tartaniuk a törléshez való jogot és az adatok minimalizálásának elvét, továbbá "megfelelő technikai intézkedéseket" kell hozniuk a szükséges garanciák biztosításához a személyes adatok védelme érdekében.**

Tehetünk azért lépéseket a személyes adatok védelme érdekében. Néhányan hajlandóak lesznek kompromisszumot kötni a személyre szabott szolgáltatások/hirdetések és az adatvédelem között. Másokat talán az sem zavar, ha egyes egészségügyi adatait eladják harmadik félnek. A fontos, hogy ez egy tudatos döntés legyen, ne pedig a felhasználó megtévesztése. Ha mégis aggodalommal tölt el minket a helyzet, **érdemes megfogadni az alábbiakat:**

- Az app letöltése előtt nézzünk utána az alkalmazásnak. Keressünk rá, mit mondanak róla más felhasználók, és hogy találunk-e bármilyen figyelmeztető jelet az értékelések között.

- Legyenek korlátai annak, hogy mit osztunk meg ezekben az alkalmazásokban, és mindig jusson eszünkbe, hogy az adataink nyilvánosságra kerülnek vagy kerülhetnek.

- Ne kössük össze az alkalmazásokat közösségi fiókjainkkal, és ne használjuk bejelentkezéshez a közösségi média fiókunkat adataink védelme érdekében.

- Ne adjunk engedélyt az alkalmazásoknak, hogy hozzáférjenek a készülék kamerájához, a helymeghatározáshoz és egyéb adatokhoz.

- Korlátozzuk a hirdetések nyomon követését a telefon adatvédelmi beállításaiban.

- Mindig használjunk MFA-t, ahol erre lehetőség van és alkalmazzunk erős, egyedi jelszavakat.

- A lehető legnagyobb biztonság érdekében tartsuk az appot mindig naprakészen.

- Fusson a telefonon internetbiztonsági védelmi megoldás, például az ESET Mobile Security for Android.

- Ha kétségünk támad egy alkalmazással kapcsolatban, inkább ne telepítsük.

Bár ezek az alkalmazások sokat segíthetnek a mindennapi életben, fontos szem előtt tartanunk, hogy az érzékeny egészségügyi adatainkat csak megbízható és számonkérhető szolgáltatókra bízzuk rá.

1 komment
Címkék: biztonság egészségügyi app kockázat gdpr

Ajánlott bejegyzések:

Egy a jelszónk, tartós 123456
Afterparty: sosem késő
Hogyan védjék magukat az idősebbek az interneten?
Holló a hollónak mégiscsak, de igen...
Egy a jelszónk, tartós 123456
Afterparty: sosem késő
Hogyan védjék magukat az idősebbek az interneten?
Holló a hollónak mégiscsak, de igen...
Közeli helyeken: érintésmentes fizetések
Közeli helyeken: érintésmentes fizetések

Kommentek:

Head Honcho 2024.04.06. 16:04:06

Egy technikai észrevétel: a blog.hu/dashboard részen már hosszabb ideje nem jelenik meg eme blog borítóképe az adott cikkről, csak és

kizárólag ezen blogról. (Több blog.hu-s blogot követek, másoknál nincs ilyen.)

Válasz erre

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink

Change Healthcare újra pácban

2024. április 09. 17:12 - Csizmazia Darab István [Rambo]

Hogy újra vagy még mindig, nos ez nehezen eldönthető. **Még szinte le sem zárult a korábbi Blackcat/ALPHV ransomware támadás miatti káosz, újabb versenyző támadta be az egészségügyi intézményt. 4 TB zsákmányolt adat, 12 napos határidő a váltságdíj fizetésre.**

Roppant szerencsétlen szériában van az Egyesült Államok egyik legjelentősebb egészségügyi kiszolgáló szervezete, amelyet első körben az oroszországi ALPHV/BlackCat egyik bedolgozó alvállalkozói csapata támadott meg idén februárban.

Ám a bűnszervezet vezetősége egész egyszerűen átnyúlt a támadást közvetlenül végrehajtók feje felett, és einstandolta az intézmény által fizetett 22 millió dolláros váltságdíj teljes összegét az általa alkalmazott alvállalkozóktól.

A kórházak, és egészségügyi intézmények elleni ransomware incidensek hatásairól már sokszor írtunk: **óriási anyagi kár, az ellopott bizalmas adatok publikálásával való zsarolás és az ezekkel történő későbbi testre szabott támadások kockázatai, elmaradó műtétek, megbénuló működés, kőkorszaki átmenet papír, ceruza, kartotékok, telefon és fax használatával, betegek elküldése, áthelyezése, időnként halálesetek előfordulása.**

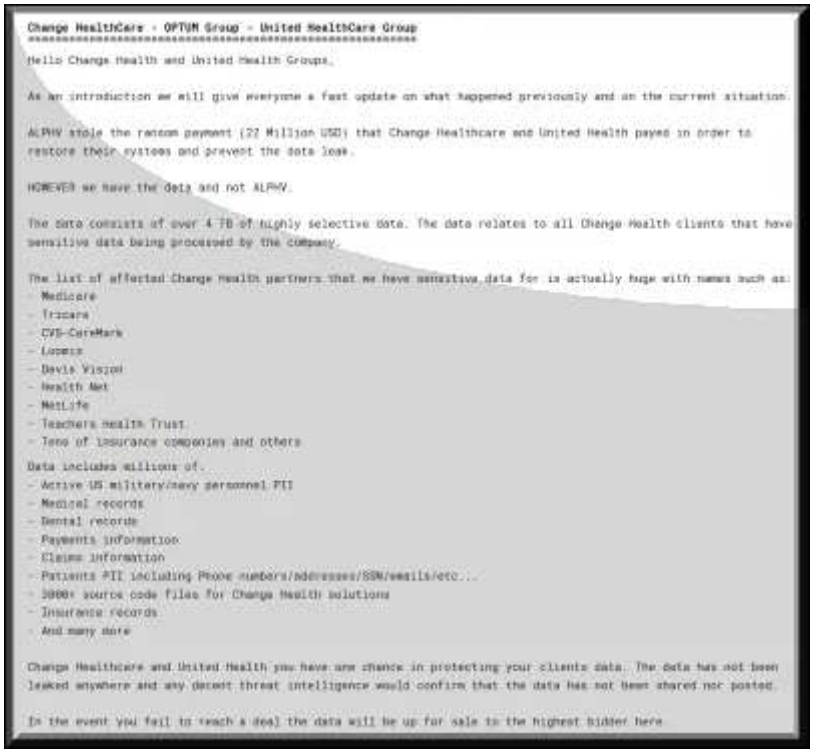
Ami mellé bekerült a társadalombiztosítási rendszer fejreállása is, valamint a rendszeres munkaügyi elszámolások elmaradása miatt az orvosok, ápolók, gyógyszertárosok fizetése is veszélybe kerülhet.

Ha még lehet fokozni egy eleve nehéz helyzetet, a Change Healthcare azzal is **kénytelen volt szembenézni, hogy a váltságdíj kifizetése ellenére a hoppon maradt eredeti elkövetők esetleg újabb összeget követelhetnek, vagy bosszúból mégis felteszik a netre** a lopott bizalmas adatokat.

És akkor váratlanul megjelent egy újabb zsarolóvírus csapat, a RansomHub jelentkezett be egy újabb támadásra hivatkozva, melyben állítólag 4 TB-nyi vállalati adatot sikerült ellopniuk, köztük olyan kiemelt betegadatokat, mint az amerikai hadsereg tagjainak azonosítására alkalmas információkat, kényes orvosi feljegyzéseket, fizetési információkat és hasonlókat.

Ebben a második fordulóban 12 napon belül váltságdíjat követelnek az egészségügyi szereplőtől, különben az adatokat egy árverésen eladják a legmagasabb ajánlatot tevőnek. A támadók szerint a fizetés a Change Healthcare és a United Health egyetlen esélye, és állítólag kivárják a végső határidőt, addig nem osztanak meg és nem tesznek közzé ezekből semmit.

A vállalat most rövid időn belül újra nehéz helyzetben van, pedig éppen csak kezdett magához térni a februári támadás után.



Ami viszont elgondolkodtató, hogy a RaaS üzletágban tevékenykedő bűnözők szokásos osztozkodási rátája általában 20-80 százalék, azaz az alvállalkozó leányvállalatnál kapják a nagyobb összeget, míg a bűnözői csapat vezetői a 20%-ot. **Mivel ezt a Blackcat/ALPHAV felrúgta, egyes szakértők elmélete szerint elképzelhető, hogy a második támadás meg sem történt, hanem az eredeti elkövetők az eredetileg az első alkalommal ellopott bizalmas adatok birtokában egyszerűen becsatlakoztak egy másik bűnszervezethez, hogy mégis pénzhez jussanak.**

Ennek némileg ellentmond, hogy a RansomHub oldalain már korábban feltűntek Change Healthcare rendszereiből lopott adatok, igaz erre az orosz eredetű különféle bűnözői csoportok közti esetleges kapcsolatok is magyarázatot adhatnak.

Szólj hozzá!
Címkék: egészségügy váltságdíj ransomware blackcat zsarolóvírus alphv ransomhub

Ajánlott bejegyzések:

100 millió ember egészségügyi adata hoppszi

Várt és nem várt mellékhatások

Holló a hollónak mégiscsak, de igen...

100 millió ember egészségügyi adata hoppszi

8 kórház, 30 klinika, 2.5 millió betegadat

Várt és nem várt mellékhatások

Holló a hollónak mégiscsak, de igen...

Váltságdíj a váltságdíjszedő bandákért II.

Váltságdíj a váltságdíjszedő bandákért II.

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

A jó kolléga nem csak ígér, hanem be is tart

2024. április 16. 14:24 - Csizmazia Darab István [Rambo]

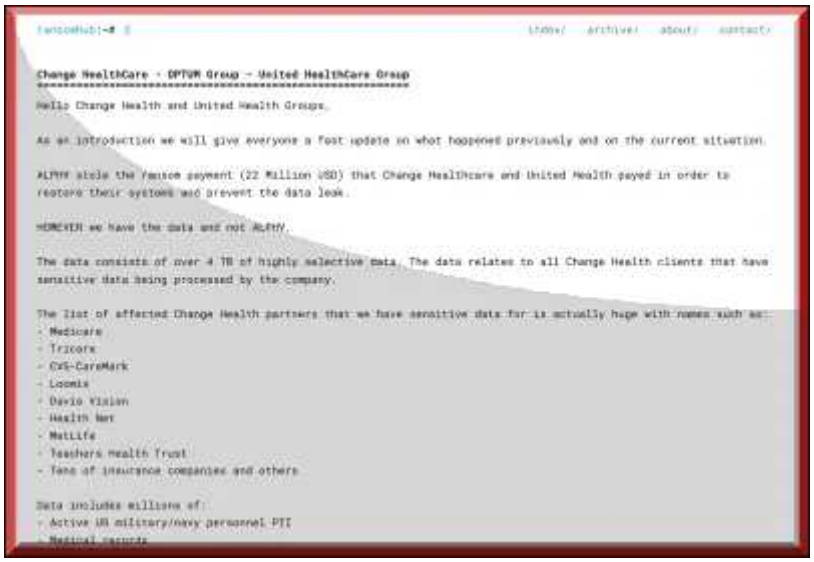
Pár napja volt szó a **Ransomhub fenyegetéséről, amivel már másodszor szembesült a Change Healthcare**. A BlackCat/ALPHV részére egyszer már kifizettek egy hatalmas váltságdíjat, amit most egy másik bűnözői kör is be akar vasalni rajtuk.

Ízlelgessük az első ízben idén februárban már kifizetett összeg mértékét: 22 millió dollár, forintban nagyjából 8.1 milliárd forint, és 6 TB érzékeny adat reménybeli megóvása ezáltal a beígért közzétételtől. **A bedolgozó alvállalkozó és a bűnszervezet vezetése azonban összerúgta port, a vezetők rátették a kezüket a teljes összegre, és ezzel kezdtek igazán rosszra fordulni a dolgok - mármint a UnitedHealth szemszögéből, amelynek szoftvereit USA szerte használják az egészségügyi szervezetek, kórházak, gyógyszertárak.**

Hivatalosan sosem ismerték el sem az ellopott adat mennyiségét, sem pedig arról nem nyilatkoztak közvetlenül, hogy valóban fizettek-e váltságdíjat, bár ez utóbbi végül egyértelműen kiderült.

Azt is olvashattuk, hogy **[a második menetben hasonló fenyegetés érte őket a Ransomhub csoporttól](), akik elvileg függetlenül az első esettől 4TB ellopott bizalmas adat birtokában kezdett újabb zsaroló manőverbe.**

Az időközben az is [kérdésessé vált, hogy ez valóban egy újabb incidens, vagy csak az előző körben hoppon maradt bűnözők]() akarják kárpótolni magukat a lopott adatok birtokában a vezetőik által elvett pénzük miatt.


Change HealthCare + OPTUM Group + United HealthCare Group

Hello Change Health and United Health Groups.

As an introduction we will give everyone a fast update on what happened previously and on the current situation.

ALPHV stole the ransom payment (22 Million USD) that Change HealthCare and United Health payed in order to restore their systems and prevent the data leak.

HOWEVER we have the data and not ALPHV.

The data consists of over 4 TB of highly selective data. The data relates to all Change Health clients that have sensitive data being processed by the company.

The list of affected Change Health partners that we have sensitive data for is actually huge with names such as:
- Medicare
- Tricare
- CVS-CareMark
- Loomis
- Davis Vision
- Health Net
- MetLife
- Teachers Health Trust
- Tens of insurance companies and others

Data includes millions of:
- Active US military/navy personnel PII

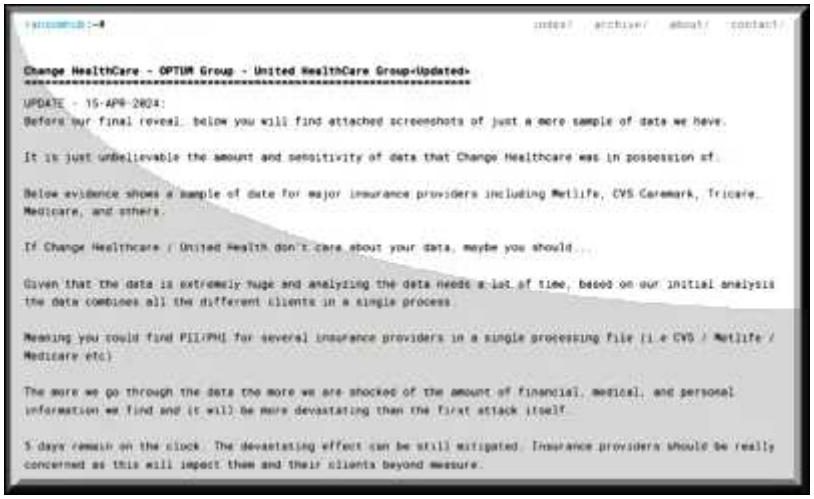
Ami azonban már biztos, hogy elkezdődött a fenyegetés beváltása tettekre, ugyanis a tegnapi napon elkezdődött a kiszivárogtatás. A RansomHub több fájlt tett közzé bizonyítékként a darknetes kiszivárogtató webhelyén, amelyek betegek személyes adatait, számlázási információikat, betegbiztosítási nyilvántartásokat és az orvosi információkat tartalmaznak. [Olyan dokumentumok is szerepeltek, amelyek a Change Healthcare és szerződéses partnerei közötti szerződéseket]() tartalmazzák.

Ismeretes, hogy a bűnbanda azzal fenyegetőzött, hogy árverésen **eladja az adatokat a legmagasabb ajánlatot tevőnek, ha nem kapja meg a követelt váltságdíjat. Az események nyomán az is felmerült, hogy a**

RansomHub nem is egy új másik formáció, hanem esetleg magának az ALPHV csoportnak valamiféle utód szervezete.

A biztonsági szakemberek véleménye elég egyértelmű a hasonló eseteknél követelt váltságdíjak ügyében. **Szerintük nem volna szabad fizetni, és ennek számos oka van. Mivel megbízhatatlan bűnözőkkel és nem Grál lovagokkal üzletelünk**, hogy semmi garancia nincs rá, hogy megkapjuk az egyedi erős titkosítást feloldó kulcsot és majd valóban le is törlik az ellopott adataink másolatait.

Emellett a fizetéssel támogatjuk és bátorítjuk is a bűnözőket, hogy továbbra is folytassák a tevékenységüket.



Az egészségügyi szektorban található intézmények számos ok miatt kedvelt célpontok: gyakran alulfinanszírozottak, így a kibervédelmük is gyengébb, alacsony a biztonságtudatossági szintjük, hiányzik vagy kezdetleges a biztonsági szabályozás, az érzékeny adatok miatt könnyebben rávehetők a fizetésre, és ráadásul az ellopott adatok az illegális piactereken igen jól értékesíthetőnek számítanak.

Ezek ugyanis többek közt például későbbi célzott, testre szabott támadásokban is remekül használhatóak.

Szólj hozzá!
Címkék: váltságdíj healthcare change szivárogtatás zsarolóvírus doxing ransomhub

Ajánlott bejegyzések:

Újabb rombolás brit kórházakban
100 millió ember egészségügyi adata hoppszi
Senki többet harmadszor?
Várt és nem várt mellékhatások

Újabb rombolás brit kórházakban
100 millió ember egészségügyi adata hoppszi
Senki többet harmadszor?
Brókerarcok
Várt és nem várt mellékhatások
Brókerarcok

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz






Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

about

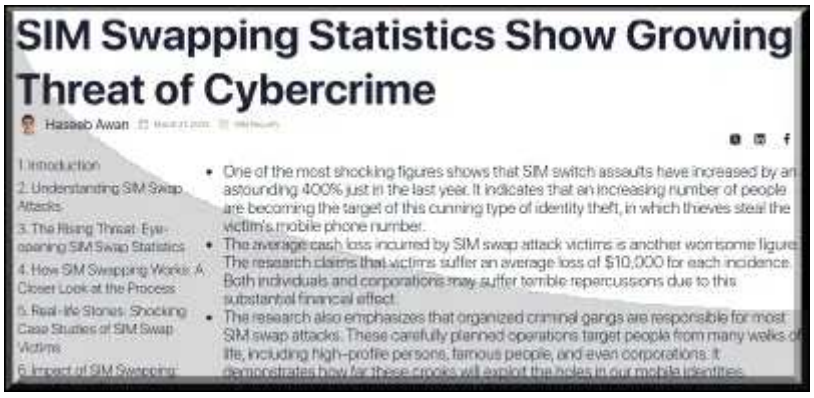
A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Szia uram! SIM cserés csalást kérhetek?

2024. április 18. 13:26 - Csizmazia Darab István [Rambo]

Már többször előkerült a **Swimswap néven emlegetett módszer, aminél az ellopott személyes adatok, beszkennelt igazolványok, cégiratok, meghatalmazások fotóival az áldozatok tudta nélkül SIM kártya cserét** kérelmeznek a mobilszolgáltatóknál.

Miután átveszik az irányítást a felhasználó mobiltelefon előfizetése felett, az áldozat telefonja elnémul, és onnantól a bűnözők kapják meg az összes üzenetet, banki értesítést, amivel óriási pénzügyi károkat képesek okozni. Ilyen átverések sajnos Magyarországon is előfordultak, többen milliós károkat szenvedtek el, és ezek után a mobilszolgáltatók valamennyit szigorítottak a kártya csere folyamatán.

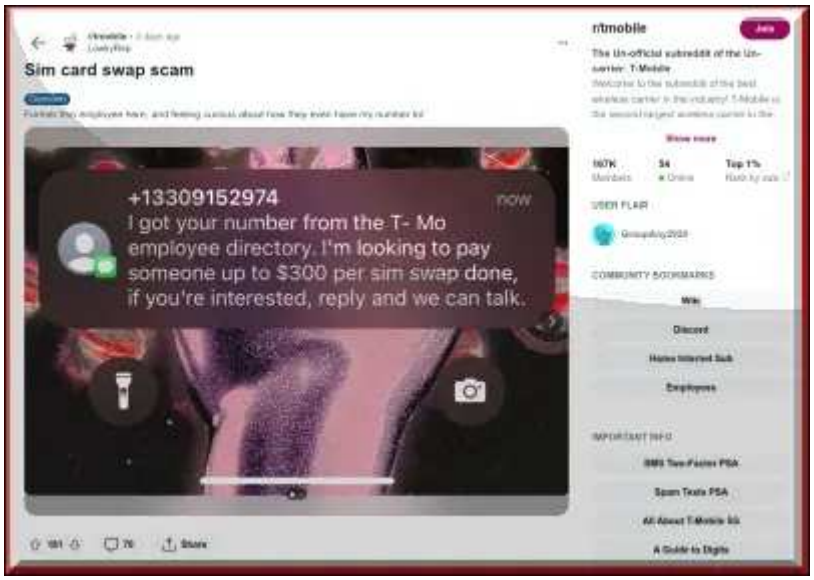


A történet másik szála talán az amerikai T-Mobile rendszerében történt többrendbeli informatikai incidensekre is visszavezethető, amelyek során ügyféladatok milliói szivárogtak ki, az évek során több különböző támadás is lezajlott.

Ezek keretében akár munkavállalói adatok is kerülhettek illetéktelen kezekbe.

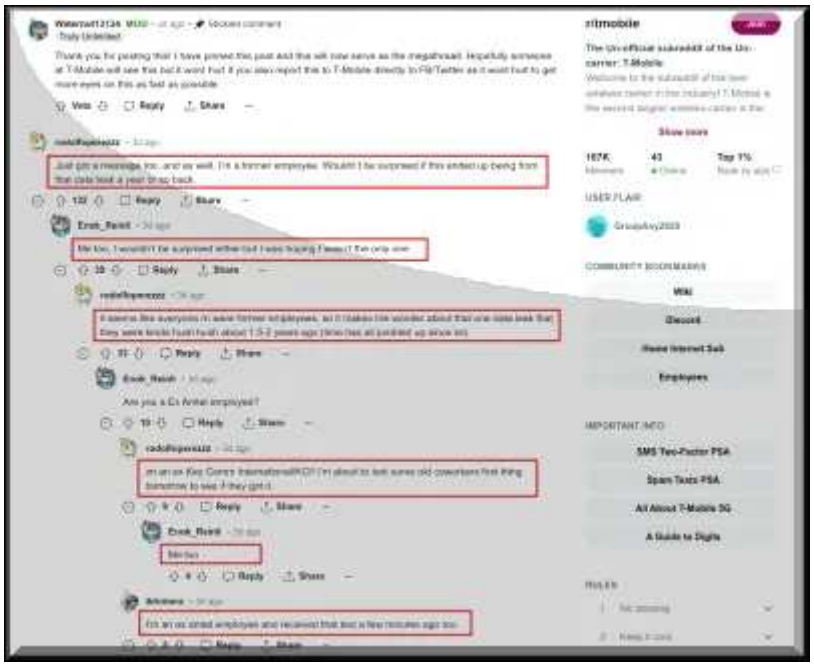
Ezúttal a T-Mobile egyesült államokbeli alkalmazottai panaszkodtak arra, hogy SMS üzenetekben keresték meg őket azzal, ha hajlandóak SIM cserés csalásban részt venni, kártyánként 300 dollárt (cirka 110 ezer forint) kaphatnak.

Az alkalmazottak közül többen is feljelentést tettek az ügyben, és azt sem pontosan értik, hogyan kerülhetett ki így a telefonszámuk a beosztásukkal együtt. **A csalók arra hivatkoztak, hogy az elérhetőségeket állítólag a T-Mobile alkalmazotti címjegyzékéből vették.**



A bűnözők a kapcsolatfelvételhez egy Telegram fiókos elérhetőséget jelöltek meg azoknak, akik hajlandóak részt venni a csalásban.

Közben a közösségi platformokon az is kiderült, hogy a megkeresett emberek egy része már nem is ott dolgozik, ami az alkalmazotti címlista egy régebbi állapotára utal.



Az is kiderült, hogy **nem csak T-s volt alkalmazottakat környékeztek meg ilyen módon, hanem a Verizon jelenlegi vagy egykori munkatársai kaptak hasonló SMS megkereséseket.** A TheRegister megkeresésére a T-Mobile US megerősített, hogy tudnak a csalási próbálkozásokról, a rendszerüket érintő új adatsértés viszont szerintük mostanában nem történt.

Ez pedig azt erősíti, hogy a valószínűsíthetően a korábbi évek során megszerzett adatokból dolgozhatnak az elkövetők. **A csalásban részt venni természetesen nem jó ötlet, több évnyi börtönbüntetést kockáztatnak az ajánlatra mégis hajlandó munkatársak.**

Szólj hozzá!
Címkék: mobil usa t-mobile sms csalás átverés mobilszolgáltató swimswap

Ajánlott bejegyzések:

Csomagja érke... Na most már elég!

Élősködők

Halló, itt Joe Biden, vagy mégsem?

Csomagja érke... Na

Élősködők

Replikák támadása

most már elég!

Halló, itt Joe Biden, vagy mégsem?

Mai szavunk pedig: smishing

Mai szavunk pedig: smishing

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Leállt az olasz SYNLAB

2024. április 23. 12:37 - Csizmazia Darab István [Rambo]

Az ok a "szokásos": **zsarolóvírus támadás érte az olaszországi részleget.**

A SYNLAB Italia felfüggesztette minden orvos diagnosztikai és tesztelési szolgáltatását, miután egy múlt heti zsarolóvírus-támadás miatt az IT rendszereit kénytelen volt lekapcsolni. Az április 18-án hajnalban történt incidens után az informatikai részlegük a biztonsági eljárásaiknak megfelelően kizárta a vállalati infrastruktúrából az adott gépeket, és megkezdte a vizsgálatot.

Bár kezdetben technikai problémáról beszéltek, pár órával később a cég bejelentette, hogy ransomware támadás miatt további értesítésig felfüggeszti az összes tevékenységet az olaszországi **mintavételi pontokon, egészségügyi központokban és laboratóriumokban.**

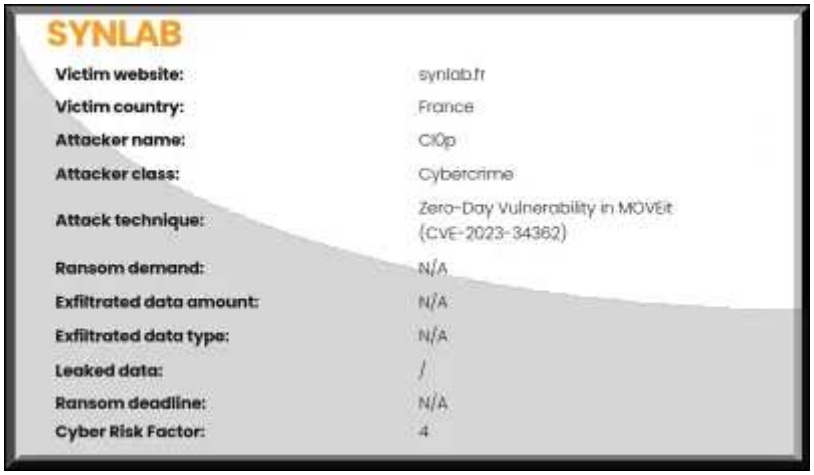
A SYNLAB **az orvosdiagnosztikai piacon egy jelentős kulcs szereplő**, világszerte 30 országban - többek közt Magyarországon is - jelen lévő csoport részeként a SYNLAB Italia hálózat 380 laboratóriumot és egészségügyi központot üzemeltet Olaszország szerte. A cég éves forgalma

426 millió dollár, és évente 35 millió elemzést végeznek el. **A leállás miatt a teszteredményekhez való hozzáférés megszűnt, a vizsgálatra korábban leadott laboratóriumi minták elemzése időben csúszhat, illetve a leállás miatti késedelem hosszától függően akár új minták begyűjtésére és leadására is szükségük lehet** az érintett ügyfeleknek.

A GDPR-nak megfelelően az ügyfeleiket is tájékoztatták a lehetséges szivárgásról, értesítették a hatóságokat is, ám arról még nem született egyértelmű nyilatkozat, hogy pontosan milyen adatok kerülhettek illetéktelen kezekbe.

A hétvégén **már elkezdődött egyes szolgáltatások részleges újraaktiválása**, többek közt a szakorvosi járóbeteg-látogatások és a fizioterápia. A biztonsági mentésekből elvileg helyre állítható a rendszer, de konkrét ütemtervet a folyamatról még nem hoztak nyilvánosságra. A közlemény szerint külső szakértőkkel folyamatosan vizsgálják az incidens részleteit.

A SYNLAB elnézést kért pácienseitől a jelenlegi helyzetből adódó kellemetlenségekért, és külön erre a célra telefonos és közösségi média csatornákat tett elérhetővé a kérdések megválaszolására, és a panaszok kezelésére.



Emlékezetes, hogy a vállalat franciaországi részlege már szenvedett el hasonló incidenst a tavalyi évben, azt akkor a Cl0p csoport követte el.

A Bleeping Computer mostani cikkének megjelenéséig viszont egyelőre egyik ransomware csoport sem vállalta magára ezt a mostani friss olaszországi támadást.

Szólj hozzá!
Címkék: olasz olaszország tesztelés laboratórium ransomeware synlab zsarolóvírus orvos diagnosztika

Ajánlott bejegyzések:

Mesterségem címere adathalászat

Zsarolóvírus a szívsebészeti orvosi eszközöket gyártónál

Újabb rombolás brit kórházakban

A ransomware az egészségügyben élet-halál kérdése

Zsarolóvírus a szívsebészeti orvosi eszközöket gyártónál

Újabb rombolás brit kórházakban

A ransomware az egészségügyben élet-halál kérdése

100 millió ember egészségügyi adata hoppszi

100 millió ember egészségügyi adata hoppszi

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkereső csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Deepfake + rosszindulat = letartóztatás

2024. április 29. 18:53 - Csizmazia Darab István [Rambo]

Iskolai közegben előforduló zaklatás, online bántalmazás, rágalmazás sajnos tucatnyi formában előfordulhat és elő is fordul. Most **egy friss iskolai incidens kapcsán felelevenítjük** a korábbi legdurvább eseteket is.

Jó pár évvel ezelőtt volt egy hegyvidéki internetes felmérés, ahol szülőket és külön az iskolás gyerekeket is megkérdeztek, mitől tartanak leginkább az online térben. **Míg a szülőknél a bűvös idegenekkel, pedofilokkal kapcsolatos félelmük volt az első helyen, addig a gyerekek a kortárs zaklatás, kiközösítés, online bántalmazásra panaszkodtak kiemelten.**

Az is elég nagy problémát jelent, hogy a szülők jó része nem ismeri fel időben a zaklatás jeleit a gyermekeken, továbbá **ismerete sincs arról sem, hogy ilyen helyzetekben mit tegyen, hogyan tudna segíteni.**

Rengeteg eset fordult már elő az évek alatt, 2018-ban Denverben egy 9 éves iskolás fiút addig csúfoltak a melegsége miatt az osztálytársak, **amíg öngyilkos nem lett.**

Öngyilkossággal végződő esetek zömmel külföldön történtek, de volt pár hazai eset is. Sümegen egy 16 éves fiút zaklattak az osztálytársak **egy éven keresztül, míg végül a vonat elé ugrott.**

2015-ben egy amerikai középiskolában a diákok egymás pucér képeit osztották meg egymás között, **amiből botrány lett, legalább száz gimnazista volt érintett a rendőrségi nyomozásban.**

[2020-ban tinédzserek egy kamuprofil segítségével magukat fiatal lánynak kiadva](#) meztelen képeket **csaltak ki egy 15 éves fiútól, amikkel aztán megalázva az áldozatot meg is osztottak az interneten**.

2023-ban **egy spanyol iskolában a nyári szünetről visszaérkezve derült ki, hogy a fiúk egy mesterséges intelligencia alapú applikációval meztelen fotókat generáltak** [a lány osztálytársaikról, és ezeket feltöltötték az internetre](#).

Már 2015-ben is volt olyan eset, ahol tanárt zaklattak, egy brit középiskolai tanárról Photoshop segítségével montíroztak össze egy

olyan képet, ahol egy pornószínész testére illesztették rá a tanár arcát, majd a manipulált fotót az iskolai Twitter oldalra föltöltötték.

2023-ban **agykárosult lett egy 13 éves fiú, akivel az osztálytársak erőszakkal** kábítószeres e-cigit szívattak.

2024. márciusában egy 11 éves brit fiú halt bele egy buta "bátorság próbába", **miután mérgező vegyszereket szívott fel a "krómozásnak" nevezett netes kihívás során.**

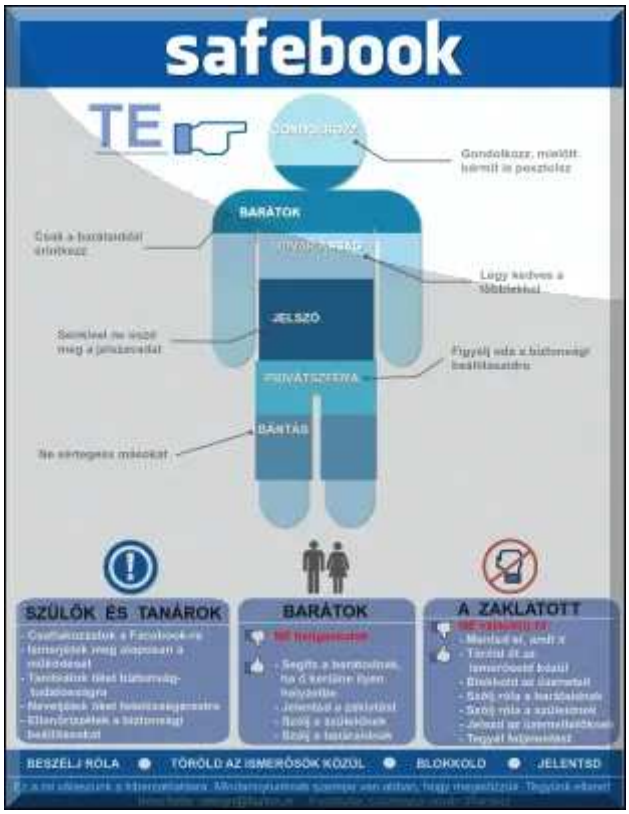
A mostani friss esetben tanár zaklatott tanárt. Egészen pontosan a baltimore-i Pikesville High School (PHS) egykori sportvezetője, Dazhon Leslie Darien egy hangklónozó szoftver segítségével manipulált lejáratő hangfelvételt generált az iskola igazgatójáról, **a hangfájlt pedig január 17-én megosztotta a közösségi médiában, és álnéven e-mailben is elküldte az iskolai tanároknak.**

A hamisított felvételen Eric Eiswert, a középiskola igazgatójának hangján rasszista és antiszemita kijelentések voltak hallhatók. Az eset hatalmas botrányt okozott, az igazgatót kényszerszabadságra küldték a vizsgálat idejére, ám közben számos halálos fenyegetést is kapott a felhergelt színesbőrű közösség részéről.

A nyomozás viszont kiderítette, hogy **manipulált felvételről van szó, és a sportvezető mindezt bosszúból követte el, mert munkájára korábban több panasz volt, és egy vizsgálatot is indítottak ellene, mert lopott az iskolai pénzekből.** Miután lelepleződött, Dazhon Darient letartóztatták.

A felvételt küldő e-mail fiókot egyértelműen hozzá tudták kötni, azt saját nagyanyja internetéről regisztrálta be még hónapokkal korábban, a fiók helyreállítási telefonszáma pedig egy Dariennél

regisztrált T-Mobile fiókhoz volt társítva. A hangfelvétel nagy valószínűséggel az ElevenLabs hangklónozó szolgáltatásával készülhetett. Hát az MI jól feladja a leckét, a hamisítás és lejáratás csúcsra jár, bárki elkövethet ilyet, nem könnyű a helyzet.



Mi szülők, ha iskolai zaklatásra gyanakszunk, jobban odafigyelve azért sokféle intő jelet észrevehetünk a gyermekünknél. Például hirtelen hangulatváltozások vagy a normális tevékenységek iránti érdeklődés elvesztése, betegség színlelése az iskola elkerülése érdekében, közösségi profilok váratlan törlése, szokatlan mértékű szociális visszahúzódás, folyamatosan "elvesző" vagy megrongált tárgyak, nagy fokú bezárkózás.

A szülőknek meg kell érteniük, hogy a gyerekek számára az internet nem egy eszköz, hanem élettér. Ezért rendszeresen beszéljék meg gyerekeikkel, mi történt ott velük, ahogy azt is megkérdezik, mi volt az iskolában, a játszótéren, vagy az edzésen. Az is hasznos, ha a szülők is valamennyire képzik magukat a számítógépes biztonság területén, hogy gyermekeik számára hasznos tanácsokkal tudjanak szolgálni. Minden szülői odafigyelés csökkenti a kockázatot.

Szólj hozzá!

Címkék: brit usa tanár középiskola hamis zaklatás hangfelvétel lejáratás bullying cyberbully hangklónozás elevenlabs

Ajánlott bejegyzések:

Halló, itt Joe Biden, vagy mégsem?

Az AI használat árnyoldalai

CAPTCHA, amely nem az ember-gép relációt teszteli

Új bejelentkezés a felhőnkbe. Vagy mégsem?

Halló, itt Joe Biden, vagy mégsem?

Az AI használat árnyoldalai

CAPTCHA, amely nem az ember-gép relációt teszteli

Új bejelentkezés a felhőnkbe. Vagy mégsem?

Újabb rombolás brit kórházakban

Újabb rombolás brit kórházakban

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

A call centerek farkasai

2024. május 06. 18:48 - Csizmazia Darab István [Rambo]

Ma már rengeteg csalás, átverés vesz bennünket körül, és rég nem csak e-mailben érkező spamek, vagy böngészés közben kéretlenül felugró ablakok formájában. Jön ez a közösségi média üzeneteink között, SMS formájában **vagy akár direkt telefonhívások útján is.**

A lebukás, letartóztatás a számítógépes bűncselekmények világában sajnos meglehetősen ritka madár, így minden apró eredménynek érdemes örülni. És most itt egy újabb tégla a falban: **az Europol 21 embert vett őrizetbe, és 12 átverési telefonközpontot zárt be egy összehangolt nemzetközi akció keretében.**

A Pandóra fedőnevű műveletben Albániában, Bosznia-Hercegovinában, Koszovóban és Libanonban olyan bűnözői hálózatok által üzemeltetett telefonközpontokon ütöttek rajta, amelyek napi több ezer átverésért voltak felelősek.

A titkos művelet még 2023. decemberében kezdődött, amikor **egy megtévesztett német ügyfél 100 ezer eurót akart felvenni készpénzben egy freiburgi bankfiókban, hogy egy állítólagosan elmulasztott bírósági megjelenése miatti állítólagos letartóztatást elkerüljön.**

A pénztáros gyanúsnak találta az esetet és értesítette a rendőrséget, akik viszont rövid úton megtalálták és letartóztatták az aktuális csalót.

A telefonhívások listáját alaposabban megvizsgálva az Europol nyomozói felfedezték, hogy az elkövetők által használt telefonszámokat mindössze 48 óra leforgása alatt több, mint 28 ezer különféle átverési cselekményhez használták. Ezzel indult el az akció, amiben 100 német rendőr részvételével próbálták mélyebben felderíteni a bűnszervezetet. 1.3 millió csaló beszélgetést hallgattak le, és 7500 hívást rögzítettek a későbbi vádemeléshez.

Külön telefonközpontot létesítettek arra a célra, hogy a hívások áldozatait figyelmeztessék, és lebeszéljék a fizetésről, ami **körülbelül 80%-ban sikerült is nekik, megakadályozva ezzel hozzávetőlegesen 10 millió euró összegű veszteséget.**

A nyomozás során kiderült, hogy az egyes országok telefonközpontjai más-más típusú bűncselekményre összpontosítottak, és naponta akár ezer átverést tudtak végrahajtani.

Bosznia-Hercegovina az adósságbehajtási csalásokra specializálódott, a Koszovóban található callcenter a banki csalók központja volt, Libanon a feltöltőkártyás csalásokkal próbálkozott, míg az albániai székhely a befektetési csalások területén igyekezett megtéveszteni az embereket.

A nemzetközileg összehangolt razzia során a hatóságoknak a letartóztatások mellett számos bizonyítékot is sikerült lefoglalniuk, többek közt **gépeket, adathordozókat, dokumentumokat, valamint készpénzt és 1 millió euró értékben különféle vagyontárgyakat**. A számítógépek alapos átvizsgálásától a nyomozó hatóságok azt várják, hogy részletesebb

információkat szerezzenek a további telefonközpontokról és a bűnszervezet vezetőiről.

Bár egy ilyen akció nem akadályozza meg a további csalásokat, de legalább **látni az hatóságok részéről az igyekezett és az erőfeszítést, amiben a távközlési szolgáltatók biztosan tudnának ennél sokkal többet is segíteni. Sajnos Magyarországon is egyre gyakoribbak a telefonos, főleg bankok nevével visszaélő átverések.**

1 komment
Címkék: pandora bank akció csalás átverés letartóztatás nemzetközi vishing europol callcenter őrizetbevétel

Ajánlott bejegyzések:

Piszkos hadviselés
A legnépszerűbb 2024-es posztok
Üdvözöl a bölcs csapat
Az 5 leggyakoribb kibercsalás

Piszkos hadviselés
A legnépszerűbb 2024-es posztok
Üdvözöl a bölcs csapat
Az 5 leggyakoribb kibercsalás
MBH banki adathalászat
MBH banki adathalászat

Kommentek:

MaxVal BircaMan KözÍró · http://bircahang.org 2024.05.07. 11:53:55

Voltam interjún így ilyen helyen pár éve. Nagyon bizarrnak tűnt.

Válasz erre

keresés

tweetz

Facebook

Tovább a Facebook-ra

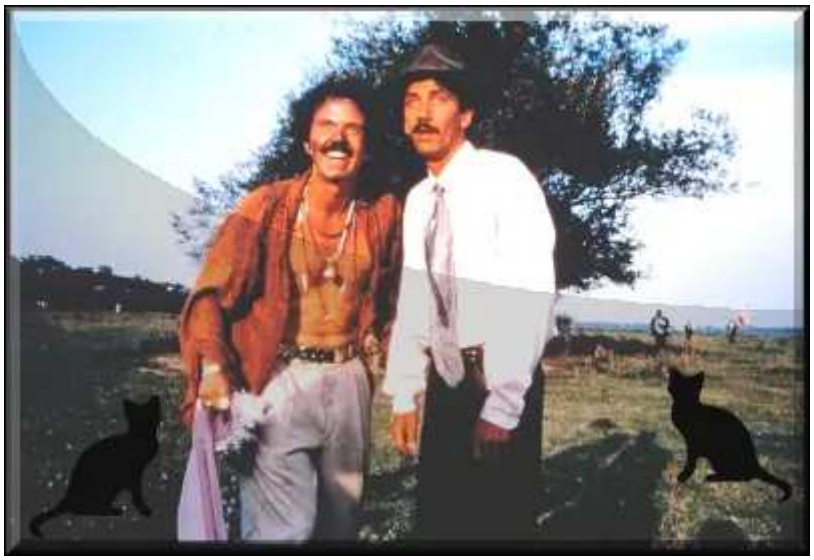
top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

Macskajaj

2024. május 09. 09:10 - Csizmazia Darab István [Rambo]

Aki nem akar lemaradni, **használja, vagy legalább ismerkedik a mesterséges intelligencia által nyújtott lehetőségekkel**. Ezek az alkalmazások szöveget írnak, rövid leírás alapján program kódot generálnak, parancssori utasításra valósághű képet alkotnak. **Az AI ahol tud, segít. Ám nem csak jóra, rosszra is használható.**



A ChatGPT által írt csaló e-mailek már gyakran átcsusszannak a legjobb spam-szűrőkön is, az egyre okosabb algoritmusok pedig olyan hatékonyan keresik a biztonsági réseket, hogy az a legjobb fekete kalapos hackereknek is becsületére válna.

A csaló üzenetek jobb nyelvi testreszabásában is hasznát veszik a támadók.

A mostani poszt a képgenerálásra lesz inkább kihegyezve, erre a feladatra is számtalan lehetőség áll már rendelkezésre, például Dall-E, Tengr.ai, Midjourney, Leonardo.ai, Clipdrop, Wonder, Stable diffusion, Freepik, Dreamstudio, MS Bing, stb.

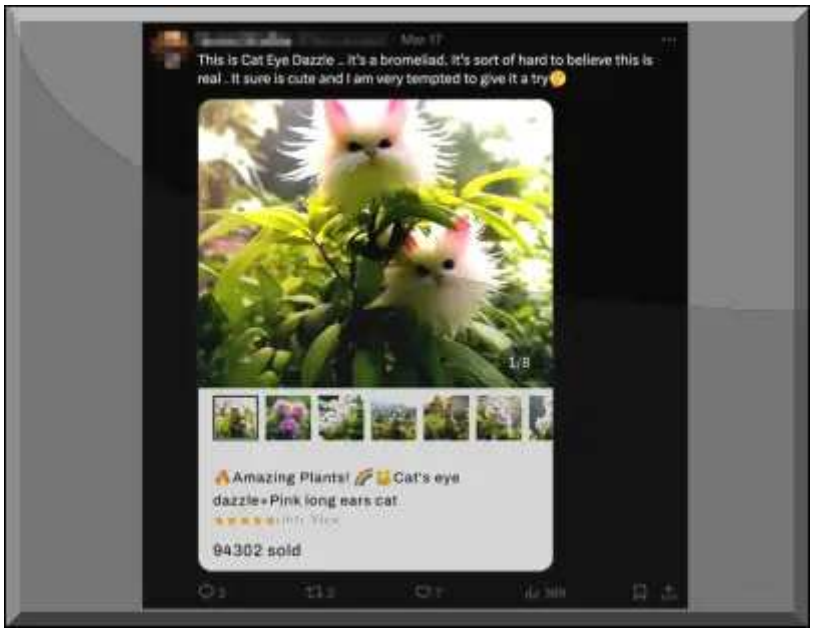
Ezekben bármit és akármit is elkészíthetünk, szó szerint: vízilovak pingpongozhatnak a Gellért hegyen, de akár korabeli élethű fényképet kérhetünk a Loch Ness-i szörnyről.

Bárkiről, bármiről generálhatunk valósághű képeket, erre számtalan példát is láthattunk már, a pufidzsekis Pápát, de **a különféle manipulációk mindenhol fellelhetők: nem létező robbantás a Fehér Házban, a gázai incidensről, az orosz ukrán háborúról is rengeteg nem valódi, számítógépen konstruált felvétel született és kering a neten.**

Emiatt egészséges, ha elsőre nem mindig hiszünk a szemünknek, és **az eligazodás, a hiteles információk megszűrése még soha nem volt ennyire nehéz.**

És akkor ebben az alaphelyzetben fordulunk rá a mai csalási témánkra, **a káprázatos macskaszem virág mindenkit lenyűgöz, izgalmas, szép, a magokért 10-20-30 dollárt kérnek - kár hogy mindez nem létezik.**

Az utóbbi hetekben pörgött fel igazán az őrület, [de már év elején, februárban beindulhattak a csalók a macska-virág hibrid generált képekkel], és elkezdtek virágmagokat árulni online, van ez külön weboldalakon, de az E-bay, Amazon, Etsy bugyrait is bevették.



A naiv ügyfelek meg utalnak, küldik a pénzeket a nem is létező virágfajta vetőmagjaiért. Az átverés mostanra érte el azt a küszöbértéket, hogy erről cikkek, leleplező posztok jelenjenek meg, úgy tűnik ez a fajta tömeges csalás lett most a korábbi "csomagja érkezett" népszerű átverési módszer egyik új mellékhajtása.

A cikkekben alaposabban utánanéztek a dolognak, amiből az derült ki, hogy nem is Cryptanthus bivittatus a neve (mert az a Zöld levélcsillag), ahogy azt egyes felhasználók állították. **A cicaszerű virágok képei hamisak, azokat a mesterséges intelligencia hozta létre, de lehet, hogy pluszban még az Adobe Photoshopot is használták a képek további finomításához.**

A nyomozás során az is kiviláglott, hogy **2024. előtt nem létezett semmilyen hivatalos feljegyzés erről az úgynevezett "macskaszem káprázat" elnevezésű növényről. Ha a közelmúltban valóban felfedeztek volna egy ilyen új, cicaarcra emlékeztető virágot, akkor arról nyilván beszámoltak volna a hírek, és ezeket Google keresésekkel most meg is lehetne találni visszamenőleg.**

A kétes weboldalak: az imseeds PONT com, gardenerstar PONT com, foundseed PONT com és dailyrosy PONT com mind kínai eredetűek, zömmel frissen bejegyzett helyek.

Vicces látni, hogy milyen sokszor szerepelnek kamuértékelések is az eszköztárban - az állítólagos elégedett, vélhetően hamis vásárlói bejegyzések itt sem sokat segítenek nekünk a cicavirág történet pro vagy kontra hitelesítésében.

A Macskafogó rajzfilmben szerepel, hogy a jó gengszter mindig álcázza magát. A mi feladatunk pedig, hogy a jó felhasználó mindig felismerje a gengsztert. Érdemes továbbra is biztonságtudatosan szűrni az információkat, csak megbízható helyről vásárolni, az eladóra és a termékre is előzetesen alaposan rákeresni, mert **valószínű, hogy a jövőben egyre gyakoribbak lesznek az ilyen trükkös átverések.**

1 komment
Címkék: kína virág csalás átverés macskaszem virágmag cicaarc

Ajánlott bejegyzések:

Biztonságos-e a Temu?	A legnépszerűbb 2024-es posztok	CAPTCHA, amely nem az ember-gép relációt teszteli	Adathalászat vagy jófogás?
Biztonságos-e a Temu?	A legnépszerűbb 2024-es posztok	CAPTCHA, amely nem az ember-gép relációt teszteli	Adathalászat vagy jófogás? Új bejelentkezés a felhőnkbe. Vagy mégsem?
			Új bejelentkezés a felhőnkbe. Vagy mégsem?

Kommentek:

Kovacs Nocraft Jozsefne 2024.05.09. 18:44:03

Fake vagy nem, jól néz ki. Ráadásul fülesbagolynak is simán elmegy.

Válasz erre

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Kell-e tárgyalni, szabad-e fizetni?

2024. május 14. 16:33 - Csizmazia Darab István [Rambo]

A szakértő Drew Schmitt szerint **a tavalyi évben rekordszámú ransomware incidens történt, több mint 60 bűnbanda támadásai legalább 4500 áldozatot érintettek**, és a folyamat látszólag töretlenül folytatódik. Csapatával rendszeresen részt vesz az áldozatok megbízásából a bűnözőkkel történő alkudozásban, **egyeztetésben, ahol a veszteségek minimalizálására törekednek.**

Ebben a szerepkörben Schmitt az összes jelentős zsarolóvírus-csapattal kapcsolatba került már, bőséges tapasztalattal rendelkezik.

A legújabb kényszerítő módszerek fokozzák a nyomást az áldozatokon, **például a cégvezetőket közvetlen telefonhívásokkal sürgetik a fizetés miatt, vagy a megtámadott vállalatok ügyfeleit, üzleti partnereit is felkeresik célzott üzenetekkel.** Az is előfordul, hogy az ellopott bizalmas adatok közül a legkényesebb - például orvosi, egészségügyi - fájlok publikálásával fenyegetnek, vagy egyes állományokat a nyomaték kedvéért fel is töltenek a netre.

A közvetítők-tárgyalók között is vannak bűnözők, akik tulajdonképpen a zsarolóvírus bandák cinkosai, és nem nyújtanak igazi segítséget az áldozatoknak, hanem inkább a váltságdíj fizetést sürgetik, segítik, abban közreműködnek. A valódi "tusztárgyalók" ezzel szemben hivatásos biztonsági szakértők, akik mindig az adott szituációt értékelve igyekeznek segíteni. Bár az általános vélekedés, és például az USA hatóságai is a fizetés és a tárgyalás megtagadására buzdítanak, ez nem mindig megfelelő taktika.

Mérlegelni kell például, hogy volt-e egyáltalán mentés, elérhető-e ingyenes helyreállító program, történt-e tényleg adatlopás vagy ez csak kamu, mekkora a leállás-szolgáltatáskimaradás okozta kár, hány szerver és munkaállomás tartalmazott valóban érzékeny adatot, mekkora a doxing fenyegetés (adatok kiszivárogtatása) valódi kockázata, az ellopott adatok miatt hogyan védhetők meg az ügyfelek, stb.

A közelmúltban történt ransomware csapatoknál lezajlott letartóztatásokkal kapcsolatban úgy nyilatkozott, hogy ez egyrészt megtört egy olyan mítoszt, miszerint ezek az elkövetők érinthetetlenek, és utolérhetetlenek, ám azt is

látni kell, hogy **az átmeneti leállások ellenére ezeknek hosszútávú kedvező hatását még egyelőre nem látni.**

A bűnözői csoportok a házkutatások és őrizetbevételek után **hamar átszerveződnek, a köréjük csoportosuló alvállalkozói kör gyakran másik ransomware csapathoz igazol át**, például ezt láthattuk az Alpha, LockBit, RansomHub esetében is. Nyilván tovább kell erősíteni az együttműködést a nemzetközi bűnüldöző szervek között.

A váltságdíj fizetés USA-n belüli tervezett betiltásáról szólva úgy fogalmazott, természetesen mindent meg kell tenni a váltságdíj fizetés elkerülésére, hiszen azon túl, hogy ezzel bűnözőket támogatunk anyagilag, nem oldja meg a problémát, sőt erősíti-bátorítja.

A workaround megoldások keresése mellett hosszútávon az lenne a cél, hogy mindenhol megerősítsék az IT biztonsági feltételeket, a védekező képességeket, és megelőzzék-elkerüljék az ilyen incidenseket.

A legrosszabb helyzetben nyilván a kis- és középvállalkozások vannak, **akiknek nincs elég erőforrásuk a megfelelő védelmi szint kiépítéséhez, és kiberbiztosítás megkötéséhez.**

A teljes fizetési tilalomról és annak szabályozásáról maguk a tárgyalópartnerek is régóta vitatkoznak már. Annyi biztos, hogy **a probléma**

túl összetett ahhoz, hogy egy szimpla tiltással mindez rövid úton megoldható legyen.

A legtöbb ransomware támadás statisztikailag még mindig meglévő ismert sebezhetőségeket, és gyenge biztonsági gyakorlatokat (le nem tiltott RDP, stb.) használ ki. A cégek gyakran spórolnak a biztonságon, vagy olcsó beszállítókra bízzák azt.

Ezt azért teszik, mert úgy vélik, az incidensekben az ő felelősségük nagyjából nulla, és a cégek hosszú távú hírnévkárosodása sem bizonyul tartósnak. Emiatt nekik egyszerűen olcsóbb figyelmen kívül hagyni a valódi problémát, és inkább biztosítást kötni, váltságdíjat fizetni.

Szólj hozzá!
Címkék: trend taktika módszer váltságdíj ransomware sürgetés zsarolóvírus 2024.

Ajánlott bejegyzések:

Újabb rombolás brit kórházakban

A ransomware az egészségügyben élet-halál kérdése

100 millió ember egészségügyi adata hoppszi

Időjárás, vízállás és ransomware előrejelzés

Újabb rombolás brit kórházakban

A ransomware az egészségügyben élet-halál kérdése

100 millió ember egészségügyi adata hoppszi

Ransomware
a
Volkswagennél

Ransomware
a
Volkswagennél

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

Bezárt a bazár

2024. május 16. 16:14 - Csizmazia Darab István [Rambo]

Az FBI és az Europol átvette az irányítást a BreachForums zsarolóprogramokat, lopott adatokat közvetítő webhelye és Telegram csatornája felett.

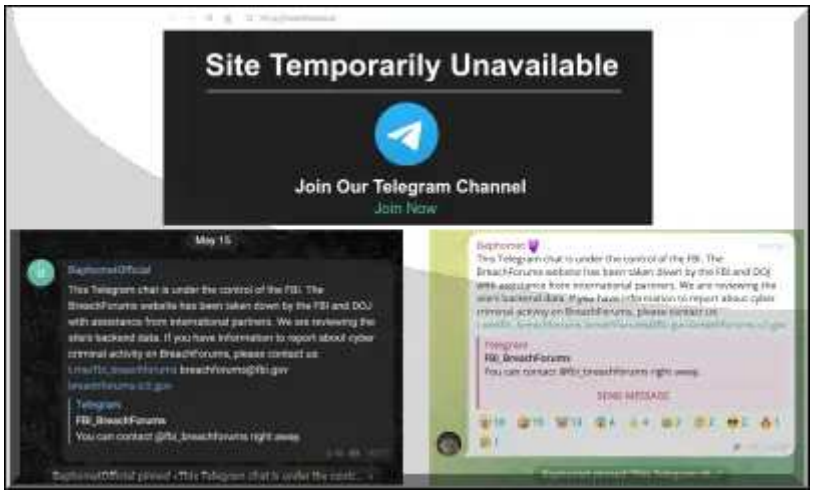
A BreachForums **évek óta népszerű helyszíne volt a hackerek és kiberbűnözők számára, akik a lopott adatokkal kereskedtek itt online**. A közelmúltban például itt hirdették 49 millió Dell ügyfél személyes adatát.

A weboldalt az FBI és a DOJ eltávolította a nemzetközi partnerek közreműködésével - ez a felirat fogadja most a látogatókat, **illetve kicsivel később már a "Site Temporarily Unavailable" üzenetet lehet olvasni.**

A weboldal adminisztrátorainak **Telegram csatornáiról is képernyőképek kerültek nyilvánosságra, így láthatóan Baphomet és ShinyHunters**

fiókjait is lefoglalták. Bennfentes információk szerint Baphometet letartóztatták a bűnüldöző akció során.

Az FBI most arra kéri a hackerfórum áldozatait, hogy **vegyék fel velük a kapcsolatot és segítsék nyomozásukat.**



Az FBI vizsgálja a BreachForums (alias Raidforums) néven ismert bűnözői hackerfórumokat, ahol **mindenféle illegális termékkel, feltört hitelesítő adatokkal, és ellopott információkkal üzleteltek.**

A bűnüldözők mostani akcióját kiváltó ok gyaníthatóan az is lehetett, hogy a közelmúltban az Europol Platform for Experts (EPE) szakértői portáljáról egy IntelBroker néven ismert szereplő lopott el adatokat.

Két év alatt ez már a második leállítása volt a fórumnak. A hatóságok most a közzétett elérhetőségeken várja az áldozatok jelentkezését, ehhez a breachforums@fbi.gov e-mail címet, a breachforums.ic3.gov webhelyet javasolja. **Remélhetőleg a nyomozás során a illegális fórumot látogató tagokról is sikerül részletesebb információkat majd kinyerni, amik letartóztatásokhoz vezetnek.**

Bár az ilyen akciók csak ideiglenesen tudják megakasztani a bűnözők ténykedését, de örülni kell a legkisebb részeredménynek is, amivel

csökkenthető vagy megakadályozható a lopott információk vásárlása és eladása.

Szólj hozzá!
Címkék: leállás akció fbi fellépés europol hatóságok breachforums

Ajánlott bejegyzések:

Piszkos hadviselés

A call centerek farkasai

Újabb rombolás brit kórházakban

Én és én meg a hibás frissítés

Piszkos hadviselés

A call centerek farkasai

Újabb rombolás brit kórházakban

Én és én meg a hibás frissítés

A távolságot mint üveggolyót nem kapod meg

A távolságot mint üveggolyót nem kapod meg

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

about

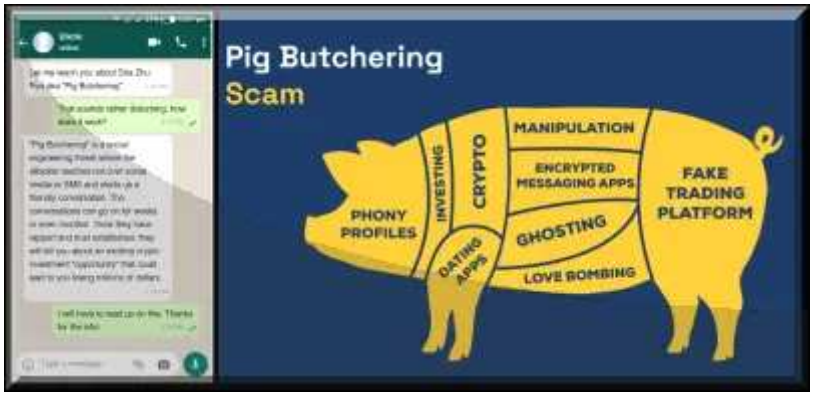
A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Az 5 leggyakoribb kibercsalás

2024. május 21. 18:19 - Csizmazia Darab István [Rambo]

A Magyar Nemzeti Bank jelentése szerint a 2**023-as évben jelentősen emelkedett a bankkártyás visszaélések száma**, a bejelentett 182 ezer eset pedig több, mint 8 milliárd forint kárt okozott.

Vagyis ez egyáltalán nem tréfadolog, kőkeményen zsebre megy, ezért jó volna mindenkinek ismernie az aktuális átveréseket, csalási módokat és sokkal elővigyázatosabbnak, gyanakvóbbnak, biztonságtudatosabbnak lenni.



1. Pig butchering, amit magyarul erőltetett módon ugyan disznóvágásnak fordítanak, de lényegét tekintve ez a módszer az áldozatok felkutatását és hosszú távú célba vételét, anyagi kivéreztetését jelenti. A kapcsolatfelvétel indulhat véletlenszerűen pl. kéretlen SMS, WhatsApp, Telegram üzenet, de gyakori a társkereső appokon a potenciális áldozatok feltérképezésével és hamis profillal célzottan induló ismerkedés is.

A cél a bizalom gyors elnyerése, majd utána valamilyen mondvacsinált váratlan nehézségre hivatkozva kölcsön összegek kérése, vagy egy rendkívül jövedelmező befektetési lehetőségre való rábeszélés. Ez utóbbi lehet tőzsdei, banki, arany kereskedelemmel kapcsolatos vagy kriptovalutás, a lényeg, hogy a csalók hamis weboldalakkal, hamis információkkal kicsalják az áldozatok pénzét. A közelmúltban egy magyar nő egy magát John Travoltának kiadó csalónak utalt 1.2 millió forintot.

2. A második helyen említjük a remélhetőleg már mindenki által ismert telefonos banki csalásokat. A magát a bank ügyintézőjeként bemutatkozó illető tájékoztat minket, hogy illetéktelenek éppen vásárlásokat kezdeményeztek a számlánk terhére. **Felajánlja a segítségét, ehhez viszont "egyeztetésre" kéri be az összes személyes, valamint banki adatunkat arra hivatkozva, hogy megvédjék az ügyfél bankszámláját. Az is megtörténhet, hogy felajánlanak egy ismeretlen, úgynevezett "biztonsági számlaszámot"**, és azt kérik, ideiglenesen utaljuk gyorsan át oda a pénzünket.

De az is gyakori, hogy a megijesztett áldozattal **feltelepíttetnek a mobilra, tabletre, számítógépre egy olyan távmenedzsment szoftvert (pl. AnyDesk, Teamviewer)**, amelynek segítségével a bűnözők teljes távoli eléréshez jutnak, és onnan minden szükséges személyes és banki adatot, aláírási címpéldányt, beszkennelt igazolvány fotókat, hivatalos iratokat is el tudnak lopni. **Mivel itt az ügyfelek hibáznak, a bankok nem térítik meg a kárt.**

3. Az AI-alapú csalások is egyre gyakoribbak, a mesterséges intelligencia segítségével például hang klónozással bárkinek a hangját le lehet másolni (pl. ElevenLabs deepvoice), és ezzel **az áldozat családtagja, munkatársa, főnöke hangján kérhetnek azonnali pénzátutalást, ismeretlen program telepítését, vagy bizalmas dokumentum átadását.** Sajnos bármilyen, akár igazi banki hívószámot is lehet ehhez hamisítani a Phone spoofing (vagy caller ID spoofing) módszerrel.

Az ilyen típusú átverések egyaránt célozzák a vállalati munkatársakat illetve a hétköznapi átlagfelhasználókat, és szintén **egyre több ilyen incidensről számolnak be a biztonsági szakemberek**. Virtuális emberrablás is lehet a bűnözők célja, ahol az áldozat hangján jelentkeznek és váltságdíjat kérnek.

4. Toborzási csalás, vagyis ha állásra akarunk jelentkezni, akkor sem árt az óvatosság. A hatóságok szerint a csalók egyre gyakrabban adják ki magukat álláskeresési toborzónak a közösségi média platformjain, hogy egy új munkalehetőség leple alatt rávegyék az áldozatokat, hogy r**észletes személyes adataikat begyűjtsék, vagy hogy állítólagos közvetítői jutalék előreutalására vegyék rá őket.**

Az is bevett gyakorlat, hogy **egy állítólagos képességfelmérő teszt során kártékony weboldalra irányítják a pályázókat, ahol kémprogrammal vagy zsarolóvírussal fertőzik meg az illető számítógépét.**

5. És végül, de semmiképpen nem utolsósorban a másodlagos csalások is szedik az áldozatokat. Ilyenkor valamilyen korábbi pénzügyi

csalás áldozatát célzottan keresik meg, és sokszor ezek ugyanazok a bűnözők, akik az első körben is kárt okoztak.

Valamilyen hivatalos szervezet nevében jelentkeznek, például ügyvédnek, rendőrnek vagy kormányzati tisztviselőnek adják ki magukat, és felajánlják, hogy segítenek az áldozatnak visszaszerezni a pénzüket. A módszer hasonló a korábbiakhoz, ehhez előzetes befizetést, illetéket, munkadíjat kérnek, hogy ennek fejében segítsenek. Ha valaki gyanútlanul hisz nekik, akkor további pénzt veszít ezzel.

A védekezés-megelőzés érdekében idegeneknek sose adjuk ki részletes személyes adatainkat, igazolvány számainkat. Soha ne utaljunk előre ismeretlen személyeknek, akik a valódi, offline találkozást ettől a pénztől teszik függővé. Banki adatainkat - megtakarításaik mértékét, bankszámlaszámunkat, stb. - szintén kezeljük óvatosan, mert különösen a kicsalt személyes adatok birtokában pénzügyi visszaélésekre adhat lehetőséget, és ez már hamis SMS és telefonhívások formájában is veszélyeztet bennünket.

Ne hagyjuk magunkat sürgetni, ne dőljünk be a soha vissza nem térő ajánlatok kísértésének. Figyeljünk pénzügyeinkre, kérjünk azonnali push egyenlegértesítőt, legyenek erős és egyedi jelszavaink többtényezős hitelesítéssel megerősítve.

A fejlődés megállíthatatlan, visszafordíthatatlan. **Fontos, hogy az átlag felhasználók is felkészüljenek az egyre kifinomultabb támadásokra, például tökéletes nyelvi környezet, vagy bárki hangjának lemásolása.**

Nem az a veszély, hogy a mesterséges intelligencia leigáz vagy megsemmisíti az emberiséget, hanem az, hogy a bűnözők ezeket a képességeket rossz célokra használják. Talán még sosem volt ennyire fontos, hogy élethosszig tanuljunk, és tisztában legyünk a lehetséges kockázatokkal.

Szólj hozzá!
Címkék: internet csalás átverés vishing smishing pigbutchering

Ajánlott bejegyzések:

A call centerek farkasai
Magyar Posta elvágta, indiai gyógyítja

A legnépszerűbb 2024-es posztok

A call centerek farkasai
Magyar Posta elvágta, indiai gyógyítja
Mai szavunk pedig: smishing
A legnépszerűbb 2024-es posztok

CAPTCHA, amely nem az ember-gép relációt teszteli

CAPTCHA, amely nem az ember-gép relációt teszteli

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

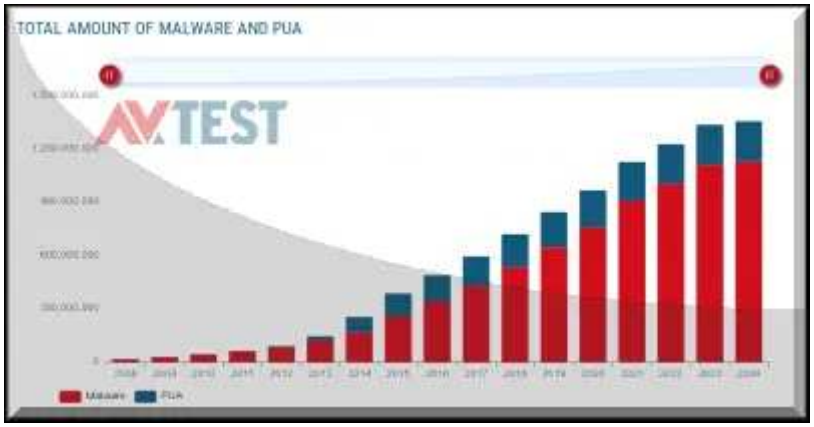
A védelmező - kell nekünk?

2024. május 23. 18:58 - Csizmazia Darab István [Rambo]

A magyar internetezők 32 százaléka azt gondolja, nincs szüksége védelmi megoldásra, pedig minden második (57%) felhasználó esett már áldozatul valamilyen kibertámadásnak.

Ez derült ki az ESET termékek hazai forgalmazója, a Sicontact Kft. gkid-vel közösen végzett, a 18 év feletti online is vásárló internetezőkre reprezentatív felméréséből.

A kutatás apropóját a most zajló kiberbiztonsági tudatosító kampánya, az "IT-hős vagy kiberbalek" adta, melynek célja, hogy a felhasználókat meggyőzzék arról, a digitális biztonság olyan alapszükséglet, amelyre figyelnünk és áldoznunk kell.



A felmérés résztvevőinek 68%-a használ jelenleg vírusirtót, az egyharmad viszont úgy véli, hogy nincs rá szüksége, mert saját maga is ki tudja szűrni a gyanús dolgokat. Már csak a kártevők száma miatt is nagyon nehéz feladat lenne ez, hiszen az AV Test szerint már több, mint 1.3

milliárd egyedi kártékony kód van jelenleg a világon.

Ennek ellenére a magyar internetezők 57 százaléka nyilatkozott úgy, hogy esett már áldozatául online csalásnak, adathalászatnak, hackelésnek vagy vírustámadásnak. Negyedük tapasztalt már olyat, hogy kéretlen tartalmak jelentek meg, illetve jelentősen lelassultak az eszközeik (14%), de egy részüknél arra is volt példa, hogy anyagi kárt okoztak nekik a bankkártyaadataik ellopásával.

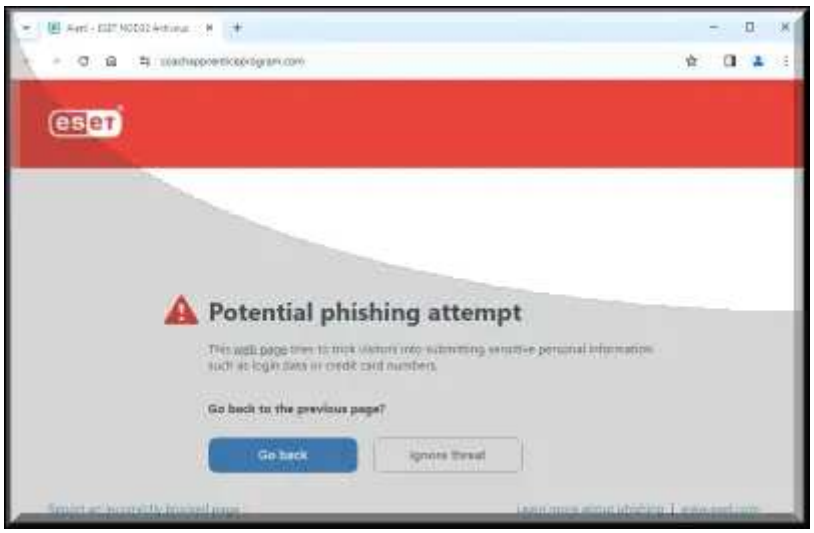
Az ESET májusban futó kampányának célja a tudatosítás: Anyakivan, CultureGeeks és Digital Pedro influenszerek figyelemfelhívó videóikkal azt mutatják be, miért érdemes védenünk online adatainkat a behatolóktól.

Digital Pedro a Hackfelmetszők - Veled is megtörténhet! ESET podcast legújabb adásának volt a vendége, ahol többek között arról beszélgettek, hogy **bár a 18-29 év közötti korosztály tartja a legkevésbé valószínűnek, hogy vírustámadás éri őket, ám közel felük (48 százalék) esett már áldozatul valamiféle online támadásnak.**

Akik használnak vírusirtót, a legtöbben a laptopjukat védik (71%), amit az asztali gép követ (48%). **Telefonon viszont csak 44% használ védelmi megoldást, pedig az androidos készülékek védelem nélkül óriási kockázatnak vannak kitéve.** A tableten (12%) és az OkosTV-n (5%) történő

használat viszonylag kevesekre jellemző, pedig ezek ellen is léteznek támadások, és az androidos eszközök esetében persze védelem is.

A válaszadók szerint a fizetős programok leginkább abban különböznek az ingyenestől, hogy több funkcióval rendelkeznek és megbízhatóbbak, nagyobb eséllyel szűrik ki a kártevőket. A válaszadók egy része (17%) azért nem használ védelmi megoldást, mert nem érzi elengedőnek az informatikai tudását egy ilyen program használatához. **Harmaduk viszont fizetne a vírusirtó programért, ha ezáltal lenne kihez fordulnia, ha segítségre van szükség.** Az ESET-nél például felkészült szakemberekből álló, magyar nyelvű terméktámogató csapat várja a felhasználók kérdéseit, problémáit, hogy azonnal segítsenek azok megoldásában.



A válaszadók egy része szerint a fizetős programok további előnye, hogy nem adják el az internethasználati adataikat külsős partnereknek. **Ez a feltételezés sajnos beigazolódott, épp a közelmúltban láthattunk újabb példát arra, hogy egy ingyenes vírusvédelmi program gyártója gyűjtötte és adta el a felhasználók adatait, a beleegyezésük nélkül.**

Ezzel összhangban áll az az eredmény, miszerint **a válaszadók jelentős része választana fizetős programot valamilyen bizalmi szempont miatt: azért, mert jobban megbíznak a minőségében, a gyártójában, vagy egyszerűen bizalmatlanok az ingyenes programokkal szemben.** Vírusirtó program választásakor fontos szempontjuk volt még, hogy az ne lassítsa le az eszközt, legyen egyszerűen telepíthető, és ritkán adjon téves riasztást. **A hogyan válasszunk vírusirtót témáról is született már podcast adás, akit érdekel, érdemes lehet ezt is meghallgatni.**

Szólj hozzá!

Címkék: felhasználók ingyenes felmérés vírusirtó eset antivirus sicontact fizetős ithős kiberbalek

Ajánlott bejegyzések:

Hogyan védjék magukat az idősebbek az interneten?

Szektorhiba

Hogyan lehetünk jó digitális szülők?

Csomagja érke... Na most már elég!

Hogyan védjék magukat az idősebbek az interneten?

Csomagja érke... Na most már elég!

Booking com átverések

Booking com átverések

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Halló, itt Joe Biden, vagy mégsem?

2024. május 27. 18:16 - Csizmazia Darab István [Rambo]

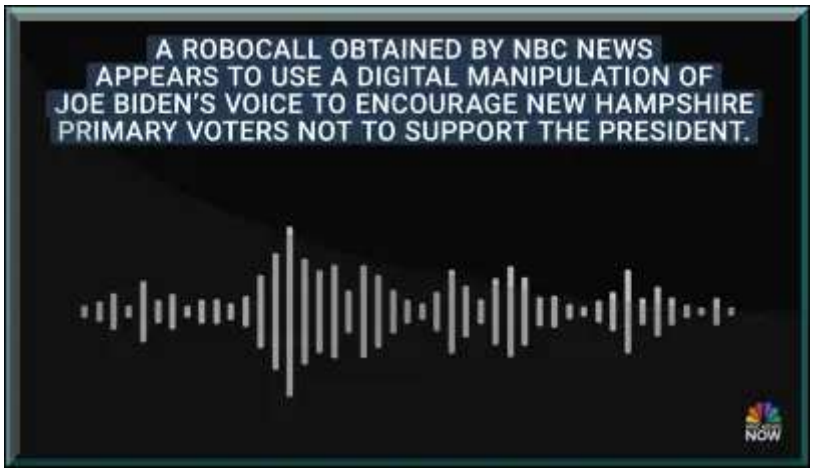
A testre szabott csalások, lejáró politikai manipulációk, pénzügyi átverések **csak most fognak igazán szárba szökkenni, hogy a fejlett technológia immár kiegészülve a mesterséges intelligencia nyújtotta extra lehetőségekkel** bármilyen fotóval, bárkinek a hangján, vagy akár deepfake videófelvételként kopogtathat nálunk.

Egyre élethűbb, egyre elképesztőbb új trükkök jelennek meg, például **a korábbi hamis e-mailek, amelyek egy cégen belül azonnali átutalást kértek a főnök nevében**, már évek óta élő telefonhívásként is jelen van élethűen leutánozva az eredeti személy hangját.

És a szakmában emellett van egy nagy fokú várakozás is, hogyan vetik be a legújabb AI eszközöket megtévesztő propaganda célokból az USA esedékes elnökválasztási kampánya során.

Ez utóbbira már nem is kell várni, elkezdődött, ugyanis **a legfrissebb hírek arról szólnak, hogy az 54 éves New Orleans-i Steven Kramer politikai tanácsadó ügyében 6 millió dolláros büntetést javasoltak választási jelölt személyes adataival való visszaélés miatt**.

A férfi ugyanis felbérelt valakit, aki mesterséges intelligencia segítségével leklónozta Biden hangját 150 dollárért (cirka 50 ezer forint), majd egy **olyan üzenetet készített, amely arra buzdította a hallgatókat, hogy ne szavazzanak a New Hampshire-i demokrata előválasztáson**.



A manipulált hangfelvétel birtokában Kramer aztán felbérelt egy telemarketing céget, amely több mint 5000 szavazónak játszotta le ezt telefonon. A dolog állítólag egy párton belül egyeztetett akció része, és alapvető célja az volt, hogy csökkentse a szavazók részvételét a fent említett előválasztáson.

A Federal Communications Commission (FCC) idén januárban vizsgálatot indított a hamisított automata hívások miatt, és ebben az ügyben marasztalta el most Kramert az amerikai felügyeleti hatóság.

A helyi Igazságügyi Minisztérium közleménye a vádemelés kapcsán kihangsúlyozta, hogy **a végrehajtási intézkedéseknek erős elrettentő jelzést kell küldenie mindenkinek, aki fontolóra veszi a választásokba**

való bármilyen hasonló beavatkozást, akár mesterséges intelligencia használatával, akár más egyéb módon.

Bár Kramer elismerte, hogy ő intézte és szervezte meg a hamis hívásokat, **azzal védekezett, hogy mindezt csak figyelemfelhívásként az AI mélyhamisítások szigorúbb szabályozása érdekében tette. Mindenesetre sikerrel járt, és valódi változást ért el mindössze 150 dolláros befektetéssel, hiszen sikerült összehoznia egy 6 millió USD, hozzávetőleg 2.1 mrd forintos büntetési tételt.** Lám a szorgos munka mindig meghozza a gyümölcsét ;)

A hatóság azt a Lingo Telecom hangszolgáltatót is megbüntetné, amely megtévesztő módon továbbította ezeket a hívásokat. Részükre az FCC 2 millió dolláros büntetést javasolt elrettentési céllal.

Ha lezárul a vizsgálat, és megszületik az ítélet, ez lesz az első olyan precedens jellegű végrehajtási intézkedés, amely mély-hamisított robothívásokkal kapcsolatos az Egyesült Államokban.

Szólj hozzá!
Címkék: választás usa ai csalás átverés mesterséges intelligencia joe vádemelés biden hangklónozás deepvoice mélyhamisítás

Ajánlott bejegyzések:

Szemetelnek, szemetelnek…
Virtuális emberrablás, igazi károkozás
3000%-kal több lett, maradhat?
Az AI használat árnyoldalai

Szemetelnek, szemetelnek…
Virtuális emberrablás, igazi károkozás
3000%-kal több lett, maradhat?
Az AI használat árnyoldalai
Piszkos hadviselés
Piszkos hadviselés
Piszkos hadviselés
Piszkos hadviselés

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Senki többet harmadszor?

2024. május 30. 07:56 - Csizmazia Darab István [Rambo]

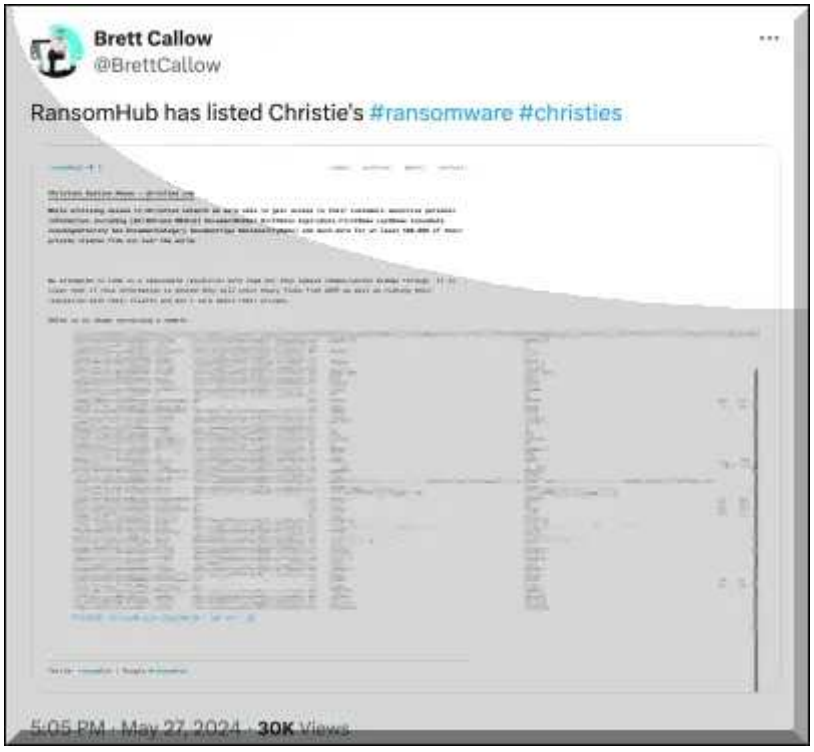
A Christie's nemzetközi árverési óriáscég megerősítette, hogy egy online támadás során adatokat loptak el tőlük. A május aukció, illetve akció során a **zsarolóvírusos támadók érzékeny adatokhoz fértek hozzá, és az incindes miatt a vállalat az online ajánlattételi rendszerét kénytelen volt lekapcsolni.**

A ransomware eset május hónap elején történt, **a RansomHub banda viszont csak most, 27-én szivárogtatott ki a blogján az adatokból, ami azt sugallja, hogy bár korábban elindulhatott már titokban egy váltságdíj tárgyalási folyamat**, de ez valószínűleg megakadhatott, és most ezzel próbálnak a bűnözők nyomást gyakorolni az áldozatra.

Érdekes, hogy az ilyen doxing jellegű, és komoly célpontok elleni támadásnál **nem csak az áldozatok titkolják el a háttérben folyó egyezető tárgyalásokat, hanem a bűnbandák is hallgatnak addig, amíg nem fizetnek nekik, vagy amikor leáll az alkudozás.** A most közzétett adatminták mellett egy 7 napos fizetési határidő is szerepel a követelésben.

A Christie's szóvivője hivatalosan is nyilatkozott a támadás tényéről, elmondva, hogy az incidens mögött álló **csoport "korlátozott mennyiségű" személyes adatot tulajdonított el "néhány" ügyfelükkel kapcsolatban**. Állítólag nincs bizonyíték arra, hogy bármilyen pénzügyi vagy tranzakciós rekordok is veszélybe kerülhettek - ez vagy így van, vagy csak egy tipikus kríziskommunikációs panel.

Azt már ugyanis nem voltak hajlandók sem megerősíteni, sem kommentálni, hogy a Ransomhub állítása szerint 500 ezer ügyfél ellopott részletes adatával dicsekedett.



Gyakori eset a cégek hallgatása mellett az is, hogy **a zsarolóvírus csoportok időnként csak bekamuzzák az adatlopást**, így ezt most egyelőre nem lehet eldönteni, melyik félnek lehet igaza, de nyilván csak az egyiknek.

Az viszont biztos, hogy az aukciós cég a világ legismertebb nevei közé tartozik, több milliós nagyságrendű összegekért ad el műtárgyakat, [így vonzó célpont a kiberbűnözők számára](#). Emiatt a váltságdíjfizetés lehetősége esetükben nagyon is reális lehet.

Az is a kockázatok közé tartozik persze, hogy **a kiberbűnözők még fizetés esetén sem tartják be ígéreteiket, amint ezt a Change Healthcare incidensnél is megtörtént.** Illetve mivel itt nem Grál lovagokkal üzletelnek, arra sincs semmi garancia, hogy a rendszer helyreállása után - amennyiben az adatlopás valós - a lerótt váltságdíj ellenére további kompromittáló adatok a későbbiekben ne kerüljenek fel az internetre.

Vagy pedig egy darkwebes aukción eladják a teljes lopott adatbázist a legmagasabb licitet kínálónak - szóval a kockázat mindenképpen elég nagy.

Szólj hozzá!
Címkék: london váltságdíj ransomware aukciósház christies zsarolóvírus doxing ransomhub

Ajánlott bejegyzések:

Újabb rombolás brit kórházakban
100 millió ember egészségügyi adata hoppszi
Ransomware a Volkswagennél
Egy Kozmikus Bogár ront el mindent

Újabb rombolás brit kórházakban
100 millió ember egészségügyi adata hoppszi
Ransomware a Volkswagennél
Egy Kozmikus Bogár ront el mindent

A jó kolléga nem csak ígér, hanem be is tart

A jó kolléga nem csak ígér, hanem be is tart

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Nyomokban vírust tartalmazhat

2024. június 04. 13:05 - Csizmazia Darab István [Rambo]

A kémprogram, a ransomware sokféle formában érkezhet, e-mailek mellékletében, spamek linkjeiben, fertőzött reklám bannerként, nyitott RDP porton, és még számos egyéb módon.

Észak-Korea hosszú ideje a kártevőterjesztő, kibertérben aktívan támadó országok közé tartozik olyan illusztris felek társaságban, mint Oroszország, Irán vagy Kína.

Az orosz csoportok előszeretettel támadnak ukrán, amerikai és európai célpontokat politikai okokból, és a fentiekkel együtt minden más országot is anyagi haszonszerzés céljából. **Korea pedig közismerten ezekből az államilag támogatott akciókból finanszírozza saját nukleáris programját.**

Milyen új szokatlan, kreatív kártevő terjesztési módszerek jelentek meg mostanában? Az egyik ilyen **a hamis álláshirdetés online interjúztatással, ahol a beszélgetés vége felé például egy végső tesztre hivatkozva ráveszik a gyanútlan jelentkezőket kártékony tartalmak letöltésére.**

Itt zsarolóvírus és valamilyen hátsóajtót nyitó távmenedzsment program is szerepel a támadók repertoárjában, például GitHub hivatkozásként.

Ehhez hasonló taktika, amikor **a bűnszervezet valamilyen blokklánc technológiára építő legitim szoftverfejlesztő cégnek vagy játékfejlesztőnek adja ki magát, és e-maileket küldözget felsőoktatási intézményeknek azzal az indokkal, hogy befektetőket illetve fejlesztőket keres a munkájához.**

A fertőzést ilyenkor leggyakrabban valamilyen kártékony NPM (Node Package Manager) okozza. **A csalások során olyan cégnevekkel élnek vissza, mint például a StarGlow Ventures, vagy a CC Waterfall.**

Ami talán még ennél is szokatlanabb, és szintén Észak-Korea fegyvertárában szerepel, hogy hamis online játékba rejt el backdoor vagy ransomware kódokat. **2024. februárja óta a Moonstone Sleet nevű bűnszervezet az általa kifejlesztett DeTankWar** (más néven DeFiTankWar, DeTankZone vagy TankWarsZone) rosszindulatú tankjáték segítségével fertőzi meg az áldozatok eszközeit.

A DeTankWar egy teljesen működőképes letölthető játék, amelyhez játékos regisztráció szükséges. A trójai rész azonban rejtetten kémkedik és adatokat lop el az eszközről.

észak-korea oroszország irán kína kémkedés adatlopás trójai tank játék ransomware zsarolóvírus

Szólj hozzá!

Ajánlott bejegyzések:

CAPTCHA, amely nem az ember-gép relációt teszteli

Zsarolóvírus a szívsebészeti orvosi eszközöket gyártónál

Én és én meg a hibás frissítés

Csomagja érke... Na most már elég!

CAPTCHA, amely nem az ember-gép relációt teszteli

Zsarolóvírus a szívsebészeti orvosi eszközöket gyártónál

Én és én meg a hibás frissítés

Csomagja érke... Na most már elég!

Ransomware a Volkswagennél

Ransomware a Volkswagennél

Ransomware a Volkswagennél

Ransomware a Volkswagennél

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Tiktok + Zeroday = fiók feltörések

2024. június 06. 19:29 - Csizmazia Darab István [Rambo]

Több, **komoly követőtáborral rendelkező felhasználói fiók esett áldozatul a legutóbbi támadásban, elesett például a CNN,** a SONY és Paris Hilton oldala is.

A beszámolók szerint a TikTok alkalmazáson belüli közvetlen **privát üzenetekkel terjedt a nulladik napi kártékony kód, amely felhasználói beavatkozás nélkül fertőzött: vagyis a rosszindulatú üzenet megnyitásán túl nem igényelt külön letöltést, plusz kattintást, vagy bármilyen egyéb extra műveletet a felhasználóktól.**

Az eltérített fiókok száma állítólag kis számú, ám elsősorban kiemelt szereplőket céloztak meg vele a támadók.

A TikTok szóvívője hivatalosan is megerősítette az incidens tényét, és jelezte, hogy intézkedéseket tettek a támadás megállítására és a jövőbeni megelőzése érdekében. **Közvetlenül együttműködnek az érintett fióktulajdonosokkal a hozzáférés mielőbbi visszaállítása érdekében.**

Az viszont nem derült ki, hogy a támadási kampány jelenleg is zajlik-e még.

A dolog tétje amiatt is érdekes, hogy novemberben elnökválasztás lesz az USA-ban, így az olyan kiemelt szereplők fiójai, mint például amilyen a CNN, komoly hatást képesek gyakorolni a választókra, így nem mindegy, képesek lesznek-e biztonságosan működni az őszi esemény előtt.

Közben pedig zajlik az a vita is, amely **a közösségi média alkalmazás betiltását szorgalmazza az Egyesült Államokban**, amennyiben az 270 napon belül nem kerül át a kínai tulajdonosoktól.

Szólj hozzá!
Címkék: profil sony cnn paris hilton napi feltörés sebezhetőség nulladik tiktok zeroday

Ajánlott bejegyzések:

Elveszett ereklyék fosztogatói

Egy Kozmikus Bogár ront el mindent

Support kérdésre adathalász válasz

Elveszett ereklyék fosztogatói

Egy Kozmikus Bogár ront el mindent

Support kérdésre adathalász válasz

Újabb súlyos WordPress hiba

Jelszó világvége

Jelszó világvége

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Bankkártyával biztonságosabban...

2024. június 11. 13:48 - Csizmazia Darab István [Rambo]

A Magyar Nemzeti Bank adatai alapján **18 ezer magyarnak csalták ki a bankszámlaadatait bűnözők 2023-ban, összesen 23 milliárd forint kárt okozva.** 4 év alatt több mint 300-szorosára nőtt a bankkártyaadatokkal sikeresen visszaélő csalások száma. **Összegyűjtöttünk ebben a témában egy rakat hasznos tippet a megelőzéshez és a védekezéshez.**

1. Használjunk megbízható eszközt!
Az első és legfontosabb alapelv, hogy az online számlánkhoz való csatlakozás során megbízható eszközt használjunk. **A saját (lehetőleg megfelelő védelmi megoldással ellátott) számítógépünk, táblagépünk vagy okostelefonunk a legjobb választás,** mivel nagyobb valószínűséggel vesszük észre, ha valamilyen gyanús tevékenység zajlik rajta. Kerüljük a kölcsönkért vagy nyilvános eszközök használatát, amivel a számlánkat és a megtakarításainkat is veszélyeztetnénk.

2. Legyünk óvatosak, hogy hol lépünk be a fiókunkba!
Nem mindegyik internetkapcsolat számít biztonságosnak az online bankolás vagy fizetés szempontjából. **A nyilvános Wi-Fi a kedvenc kávézónkban, vagy a főtéren elérhető hálózat nem a legjobb opció** arra, hogy megnézzük számlaegyenlegünket, vagy kifizessük számláinkat. Ha nem tudjuk elkerülni a nyilvános hálózatok használatát, akkor alkalmazzunk VPN (Virtual Private Network) megoldást, hogy kommunikációnk titkos maradjon, és adataink ne kerüljenek illetéktelen kezekbe.

3. Legyen naprakész a számítógépünk, eszközeink!
Tartsuk operációs rendszerünket naprakészen. A rendszeres biztonsági hibajavítások azonnali letöltése és futtatása segít bezárni a támadók által keresett sebezhetőségeket, ugyanis a javítatlan hibák, sérülékenységek

lehetővé tehetik, hogy megfertőzhessék számítógépünket, mobileszközeinket. Sok program automatikusan telepíti a biztonsági frissítéseket, hibajavításokat, illetve új verziókat keres anélkül, hogy szükség lenne külön felhasználói beavatkozásra. Ezzel időt takaríthatunk meg, és egyben maximalizálhatjuk a védelmünket.

4. Használjunk megbízható és naprakész biztonsági megoldást!
Mielőtt csatlakoznánk az online számlánkhoz, telepítsünk megbízható, többszintű és naprakész biztonsági megoldást. A komplex internetbiztonsági alkalmazás védelmet nyújt a **különféle típusú vírusok, valamint az olyan rosszindulatú átverések, adathalászat ellen is**, **illetve biztonságos fizetést biztosít.**

5. Alkossunk erős egyedi jelszót!
Fontos szabály, hogy minden egyes belépési helyszínen különböző egyedi jelszót használjunk. Ha ugyanis ugyanazt a jelszót használjuk az online számlánkhoz, a közösségi média felületeinkhez vagy több más fiókunkhoz is, egy szivárgás esetén a támadók azt mindenhol végigpróbálgatják.
Használjunk jelszókezelő programot, ami az erős jelszavainkat legenerálja, előhívja, és biztonságosan eltárolja, nekünk viszont csak egyetlen mester jelszóra kell fejből emlékeznünk. Sose jegyeztessünk meg jelszavakat a böngészővel!

6. Használjunk kétfaktoros azonosítást!
A bankoknál általában szerepel a kétfaktoros azonosítást (2FA) az online számlánkhoz, amely SMS-sel, vagy valamilyen plusz hitelesítő alkalmazással védi banki belépési név-jelszó párosunkat. Így ha a jelszavunk esetleg rossz kezekbe is kerül, a második azonosítás nélkül nem lesz sikeres a belépés.
Ezt minden más egyéb online szolgáltatásnál is érdemes igénybe venni.

7. Ne dőljünk be a csapdáknak!
A kiberbűnözők szó szerint bármit megpróbálnak, hogy megszerezzék bizalmas adatainkat. Úgy tesznek, mintha bankárok lennének, hamis értesítést küldenek a pénzintézet nevében vagy megkérnek, hogy változtassuk meg a jelszavunkat egy linken keresztül, amit e-mailben küldtek el nekünk. **Ha bármilyen üzenetet kapunk, amely arra kér, hogy változtassuk meg a belépési adatainkat vagy kattintsunk egy mellékelt linkre, ne tegyünk, és semmiképpen se kattintsunk. A bankok sosem küldenek ilyen jellegű üzenetet, kéréseket, kérdéseket.**

8. Jelentkezzünk ki, ha már befejeztük az online bankolást!
Ha végeztünk, szabályosan lépjünk ki a banki oldalon. Ha egy támadó esetleg megpróbálná eltéríteni az online bankolás folyamatát, kevesebb kárt tud így okozni, ha nem vagyunk bejelentkezve fiókunkba.

9. Aktiváljuk az azonnali banki egyenleg értesítéseket!
Hasznos, ha mindig folyamatosan figyeljük online egyenlegünket. Ezt legkönnyebben úgy tehetjük meg, ha bankunktól push értesítést kérünk (állítunk be) az összes számlánkon zajlódó pénzmozgásról, **így sokkal könnyebben felfigyelhetünk az esetleges gyanús tevékenységekre. Egyes bankoknál az eseti push értesítések mellett e-mailes értesítéseket is beállíthatunk, ebben minden egyes terhelésről részletes információt kapunk.**

10. Virtuális bankkártya használata
Ma már szinte minden banknál létezik külön internetes vásárlásokhoz való elektronikus (unembossed card) virtuális kártya, amelynek a számát bátran megadhatjuk, akár még a három jegyű CVV ellenőrző kóddal együtt is. A Revolut és a WISE külön is biztosít ilyen virtuális kártyát. Erre csak a vásárlás előtt közvetlenül érdemes a netbankunkon átvezetni a vásárláshoz szükséges pontos összeget, ami így csak pár percig lesz az egyébként üres virtuális számlánkon. **Ezzel a módszerrel nem tudnak tőlünk lopni, és így az "igazi" bankkártyánk adatait sosem kell a weboldalakon megadnunk.**

11. Ha esetleg már áldozatok lettünk...
Ha a banki adataink már veszélybe kerültek, akkor legelső teendőnk értesíteni a bankunkat. Itt akár a bankkártyánk azonnali letiltására is szükség lehet. Ha számítógépes csalás áldozatai lettünk, és anyagi kárt szenvedtünk el, akkor a rendőrségi feljelentést is érdemes megtenni.

12. Tartsuk a mobileszközünket naprakészen!
Az érintésmentes kártyák mellett ma már a telefonok is képesek ezt a funkciót ellátni olyan szolgáltatásokon keresztül, mint az Apple Pay vagy a Google Pay, amelyek a kártyaadatok feltöltése után lehetővé teszik, hogy a telefonnal fizessünk. Mind az operációs rendszert, mind az alkalmazói appokat is tartsuk frissen. A hibajavítások, újabb verziók biztosítják a biztonságos környezetet.

13. Androidos eszköz esetén használjunk vírusvédelmet!
Banki kártevők, adathalász weboldalak, kémprogramok veszélyeztetik a felhasználók életét, és emiatt mobileszközeinket sem szabad védetlenül hagynunk. Annál is inkább, mivel **egy mobiltelefon rengeteg bizalmas információt tartalmaz: jelszavakat, fotókat, egészségügyi információkat, közműves befizetéseket, levelezést, közösségi fiókokat, banki alkalmazást**. Az ESET Mobile Security programban található integrált Fizetésvédelem egy kiegészítő réteget biztosít azáltal, hogy megvédi a készüléken pénzügyi adatainkat a haladó szintű adathalászat és az egyéb kártevők ellen.

14. Állítsunk be itt is alacsony fizetési limiteket!
A banki applikáción keresztül ez könnyen megtehetjük, ezzel **minimalizálhatjuk nagyobb összeggel történő esetleges illetéktelen számlaműveleteket.**

15. Védjük fizikailag is a mobileszközt!
Mivel ez gyakorlatilag a pénztárcánk, sose hagyjuk őrizetlenül. Legyen valamilyen képernyőzár is - minta vagy PIN kód - az illetéktelen hozzáférések megelőzésére.

16. Használjunk olyan vírusvédelmet, amely lopásvédelmi lehetőséget is biztosít!
Ennek segítségével a program **elküldi az akkumulátor lemerülése előtt a készülék utolsó bemért helyzetét, fényképeket készít az elülső és a hátlapi kamerával, ha a tolvaj rossz PIN kóddal próbál belépni, vagy amikor megpróbálják kicserélni a SIM-kártyát.** Az ESET Mobile Security for Android emellett például lehetőséget nyújt a személyes tartalom távoli törlésére is.

[Szólj hozzá!]
Címkék: [mobil] [biztonságos] [bank] [tippek] [bankkártya] [fizetés] [megelőzés] [tanácsok] [védekezés]

Ajánlott bejegyzések:

[Okosotthon kontra felhasználó]

[Identitás lopás: nem függ az életkortól]

[Booking com átverések]

[Booking com átverések]

[Közeli helyeken: érintésmentes fizetések]

[Közeli helyeken: érintésmentes fizetések]

[10 tipikusan időseket célzó csalás]

[10 tipikusan időseket célzó csalás]

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz






Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Kibertámadások a sport világából

2024. június 13. 10:37 - Csizmazia Darab István [Rambo]

Ikonikus sporteseményekből - mint például az olimpia vagy a foci bajnokságok - idén nyáron sem lesz hiány. A szurkolók alig várják ezeket az eseményeket - nincsenek ezzel másként a kiberbűnözők sem. **A Foci EB és a 2024-es párizsi olimpiai játékok közeledtével mutatunk néhány olyan esetet, amelyekben a kibertámadások áldozatai sportegyesületek, szervezetek vagy a szurkolók voltak.**

1. Átigazolás a kiberbűnözőkhöz
Egy meg nem nevezett Premier League klub ügyvezető igazgatójának e-mail fiókjába egy 1 millió angol font (457 millió forint) értékű játékosátigazolási tárgyalás idején jutottak be a bűnözők a Business Email Compromise (BEC) módszerrel. Ez egy olyan csalási forma, amelynél egy szervezet levelezését előzetesen feltörve az abból megismert bizalmas adatokból, levélváltásokból később testre szabott célzott adathalász támadások indíthatóak az áldozat nevében. Ebben az esetben **a célzott adathalász támadás egy hamis Office 365 bejelentkezési oldalra vezette a klub ügyvezető igazgatóját, ahol tudtán kívül kiadta a bejelentkezési adatait**. Ezután a bűnözők az ügyvezető nevében felvették a kapcsolatot a tárgyalás másik résztvevőjével, egy európai klubbal, ezzel egyidejűleg pedig létrehoztak egy hamis email fiókot, amin keresztül a valódi ügyvezetővel kommunikáltak az európai klub nevében. A bűnözők ezután a valódi bankszámla adatokat a saját számlájukra cserélték. A Premier League klub így majdnem 1 millió fontot veszített, de a bank az utolsó pillanatban közbelépett, és meghiúsította a bűnözők tervét.

Egy másik tekintélyes futballklub, az olasz Lazio azonban nem volt ennyire szerencsés. 2018-as beszámolók szerint a klub egy átverés révén 2,5 millió dollár (898 millió forint) értékű átigazolási díjat fizetett ki egy csalók ellenőrzése alatt álló bankszámlára.

2. Amikor térdre kényszerít a zsarolóprogram
2020 novemberében a Manchester United lett zsarolóvírus-támadás áldozata.

A bűnözők **váltságdíjat követeltek azért cserébe, hogy visszafejtsék a letitkosított adataikat és helyreállítsák a hozzáférést a klub számítógépes rendszereihez.** A klubnak kiberbiztonsági szakértőkkel és bűnüldöző szervekkel együttműködve végül sikerült megállítania a támadást, és váltságdíj kifizetése nélkül helyreállították rendszereiket.

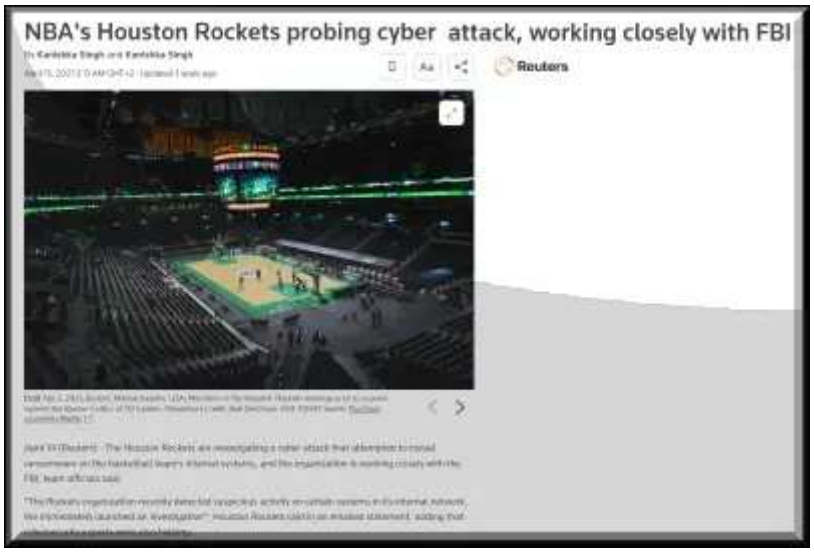
3. Olimpiai kártevő
A 2018-as téli olimpiai játékok megnyitó ünnepségét a dél-koreai Pjongcsangban egy váratlan vendég, az Olympic Destroyer nevű kártevő zavarta meg.

A rosszindulatú szoftver megtámadta az esemény informatikai infrastruktúráját, megzavarva az ünnepség alatti működést és káoszt okozva a nézők körében. **Többek között leállította a Wi-Fi hotspotokat és a televíziós közvetítéseket. Szisztematikusan törölte az érintett**

Windows-rendszerek kritikus adatait, és hálózati helyeket is keresett a további terjedéshez, ami tovább fokozta a csatlakoztatott eszközökön okozott károkat. Képes volt olyan fejlett szoftverek telepítésére is, amelyek célja a jelszavak megszerzése volt. A támadás elsősorban az esemény hivatalos honlapját, a versenyeknek otthont adó síközpontok szervereit, valamint az esemény technológiai infrastruktúráját kezelő két informatikai szolgáltatót vette célba. Az eset egyértelműen rámutatott a nagy horderejű sportesemények sebezhetőségére a célzott kiberfenyegetésekkel szemben.

4. Nyilvánosságra került kórtörténetek
2016-ban a Nemzetközi Doppingellenes Ügynökség (WADA) súlyos adatszivárgás áldozata lett, amely során számos világhírű sportoló orvosi adatai is nyilvánosságra kerültek. Az incidens, amelynek áldozatai között volt Venus és Serena Williams teniszezők, valamint Simone Biles tornász is, nyilvánosságra hozta a sportolók gyógyászati célú mentességét (TUE engedély), amely lehetővé teszi számukra, hogy alapvetően tiltott anyagokat vagy módszereket használjanak, amennyiben azokat valós betegségek kezelése miatt írták elő.

A WADA szerint a jogsértés nemcsak a TUE-rendszerének integritását ássa alá, hanem az ügynökség tágabb értelemben vett küldetését is veszélyezteti, azaz a sport tisztességességének és tisztaságának megőrzését.



5. Houston, van egy kis problémánk
Az ikonikus kifejezés 2021 áprilisában került újra a köztudatba, amikor a Houston Rockets kosárlabda klub kibertámadás áldozatává vált.

A támadás súlyos következményekkel járt **az NBA egyik legjelentősebb csapatára nézve, mivel a támadók több mint 500 GB személyes információt szivárogtattak ki, köztük olyan érzékeny adatokat, mint a játékosok szerződései, ügyféladatok és pénzügyi információk.** A támadás hatása jelentős volt, áttételesen más ágazatokban, többek között az egészségügyben és a logisztikában működő szervezetek számára is további kockázatot jelentett.

6. Nincs menekvés
Egy kosárlabda-mérkőzésen a negyed végét a dudaszó jelzi. **2023 októberében a francia ASVEL kosárlabdacsapathoz másfajta jelzés érkezett, ami a NoEscape zsarolószoftver-csoport által végrehajtott adatbetörést jelezte.**

A csapat elismerte a hackertámadást, és 32 GB érzékeny adat kiszivárgását jelentette, köztük olyan **játékosinformációkat, mint útlevelek és személyi okmányok adatai, szerződések, titoktartási megállapodások és egyéb jogi dokumentumok.**

7. Egy reális helyzet
Mindaz a magabiztosság, amelyet a **Real Sociedad labdarúgóklub a pályán mutatott a Bajnokok Ligájában és a spanyol La Ligában is, hirtelen megszakadt 2023. október 18-án, amikor a klub szűkszavú közleményben bejelentette, hogy kibertámadás áldozata lett.**

Az eset során olyan szerverek kerültek veszélybe, amelyek érzékeny adatokat tároltak, beleértve a felhasználók és részvényesek nevét, vezetéknevét, postai címét, e-mail címét, telefonszámát, sőt bankszámlaadatait is.

8. Célkeresztben a Boca
2022. szeptember 16-án támadók **átvették az irányítást az argentínai Buenos Aires-i Club Atlético Boca Juniors hivatalos YouTube-fiókja felett**, és az Ethereum kriptopénzt reklámozó tartalmakat terjesztettek, ami egy tipikus kriptovaluta átverés.

A Boca Juniors azonnal hivatalos közleményt adott ki a Twitteren (a mostani X-en), néhány órán belül pedig sikeresen visszaszerezte a feltört fiók feletti ellenőrzést.

9. Öngól?
A Holland Királyi Labdarúgó-szövetség (KNVB) ellen 2023 áprilisában elkövetett támadás során ellopták a testület alkalmazottainak és tagjainak személyes adatait.

Az incidensnek számos áldozata volt, köztük az ifi játékosok szülei, nemzetközi játékosok, a 2016-2018 közötti időszakban foglalkoztatott profik, a KNVB sportorvosi központjának kapcsolattartói, **valamint a szervezet fegyelmi ügyeiben 1999-2020 között érintett személyek.**

10. A mindannyiunkat fenyegető csalások
A nagy sportesemények világszerte több milliárd nézőt vonzanak, és a csalók ezt kiváló lehetőségnek tartják arra, hogy új áldozatokat szedjenek. **Visszatérő problémát jelentenek például a foci világbajnokságra épülő csalások, amelyek gyakran elhitetik az emberekkel, hogy jegyet nyertek az eseményre, vagy olyan weboldalakra irányítják őket, amelyekről kártékony programokat töltenek le az eszközeikre.**

Korábban már történt olyan eset is, amelyben gyanútlan WhatsApp-felhasználókat csaptak be ingyenes focimezeket kínálva.

Ha el akarjuk kerülni a fenti átveréseket, akkor **alkalmazzunk megfelelő védelmi megoldást az eszközeinken, és hallgassunk a józan eszünkre. Ne kattintsunk e-mailekben vagy más kéretlen üzenetekben található linkekre vagy mellékletekre. Ami túl jól hangzik ahhoz, hogy igaz legyen, az nagy valószínűséggel lehet átverés.** A 2022-es katari FIFA labdarúgó világbajnokság előtt például rengeteg hamis nyeremény jegyet kínáló átverés jelent meg.

Fontos megjegyezni, hogy csupán egyetlen közösségi bejegyzés kedvelésével vagy megosztásával nem lehet nagy értékű ajándékot nyerni. A nyereményjátékok során soha nem kérnek pénzt előre a nyeremények átvételéért vagy kezelési költségként. A nemzetközi sportszervezetek vagy partnereik nem küldenek helyesírási hibáktól hemzsegő, gyanús linkeket tartalmazó üzeneteket, legyünk tehát óvatosak és biztonságtudatosak az adathalász és egyéb támadásokkal szemben.

Szólj hozzá!
Címkék: sport foci olimpia csalás átverés adathalászat

Ajánlott bejegyzések:

Adathalászat vagy jófogás?
Csomagja érke... Na most már elég!
Utolsó emlékeztető a fiók felfüggesztése előtt
Fontos vagy nekem

Adathalászat vagy jófogás?
Csomagja érke... Na
Utolsó emlékeztető a fiók
Fontos vagy nekem

most már elég!

felfüggesztése előtt

Ment a hűtlen hamis linkkel

Ment a hűtlen hamis linkkel

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

Ransomware a nyomkövető rendszerben

2024. június 18. 11:50 - Csizmazia Darab István [Rambo]

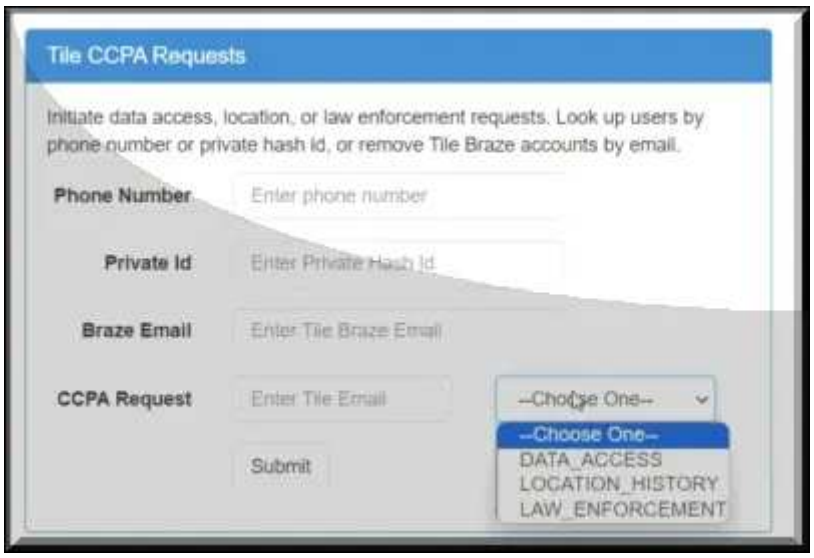
Eléggé unortodox incidens érte **a Life360 nevű nyomkövető eszköz beszállító céget, ugyanis az ügyfélszolgálati rendszerüket megtámadva abból érzékeny ügyféladatokat loptak el. Az elkövetők váltságdíjat követelnek a vállalattól.**

A cég június 11-én keltezett hivatalos közleménye a furcsa incidens tényét elismeri, és **az adatszivárgásról beszámolva úgy nyilatkoztak, az ellopott adatok neveket, lakcímeket, e-mail címeket, telefonszámokat és a nyomkövető eszközök azonosítószámait** tartalmazta.

Úgy vélik, a kikerült adatok között nem szerepelnek hitelkártyaszámok, jelszavak, bejelentkezési hitelesítő adatok - hogy ez valóban így volt-e, majd idővel úgyis kiderül. Az elkövetők ezekkel a bizalmas adatokkal **nem csak magát a céget, hanem közvetlenül a kiszolgáltatottá vált megfigyelőket és a megfigyelteket is képesek lehetnek testre szabott kibertámadásokkal fenyegetni.**

Szakértők szerint a Tile-t **valószínűleg a bűnüldöző szervekkel folytatott adatmegosztási gyakorlata miatt célozták meg, és legalább 450 ezer ügyfél adata került veszélybe a több millió felhasználóból**. A beszámolók alapján úgy tűnik, a Tile még nem kereste meg azokat az ügyfeleket, akikről úgy gondolják, hogy érintettek lehettek a jogsértésben.

Azok, akiknek kiszivárogtak a személyes adatai, **arra számíthatnak, hogy a közeljövőben megtévesztő e-mailes adathalász leveleket kapnak a cég vagy valamilyen hatóság nevében, illetve akár közvetlen zsarolással is** megkereshetik őket.



A hírekből ugyanakkor nem derült ki, jelen esetben mekkora volt a váltságdíj követelés pontos mértéke, azt kifizették-e egyáltalán, illetve hogy sikerült-e már felderíteni, hogyan hatoltak be a támadók a belső rendszereikbe.

A cég ellen korábban több különböző adatvédelmi panasz is volt már. Legutóbb a tavalyi évben Kaliforniában csoportos keresetet adtak be ellenük, amelyben hanyagsággal, hibás tervezéssel, többszörös adatvédelmi törvénysértésekkel vádolták meg a helymeghatározó hálózatot üzemeltető cégcsoportjukat. A hivatalos nyilatkozat akkor is a már jól ismert "*A Life360*

továbbra is elkötelezett felhasználóink biztonsága és magánélete iránt" mondattal zárult.

Nem kibertámadás miatti hasonló üzemzavar egyébként már Magyarországon is előfordult, például 2023. őszén hetekig nem működött a rendőrségi nyomkövető rendszer, emiatt a házi-őrizetben lévő gyanúsítottak közül többen is észrevétlenül el tudtak szökni.

Az akkori esetről az újságok azt írták, **a lábbilincsek által sugárzott információkat tároló szerver megtelt, viszont a szolgáltató ezzel kapcsolatos terméktámogatási szerződése lejárt, így már nem volt, aki ezt az állapotot időben észlelje és közbelépjen**.

Szólj hozzá!
Címkék: váltságdíj adatlopás nyomkövető adatszivárgás ransomware kibertámadás lábbilincs tile doxing life360

Ajánlott bejegyzések:

Az élet szép, de a Life360-nak vannak gondjai

Ransomware támadás a Nissan ellen

9 millió, bizony, dalolva ment...

Go Western Digital II.

Az élet szép, de a Life360-nak vannak gondjai

[Ransomware támadás érte az MSI-t]

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Cselekedettel és mulasztással II.

2024. június 20. 18:22 - Csizmazia Darab István [Rambo]

Nyilván mindent fel lehet törni, elengedő tudással és elegendő időráfordítással bármilyen célpontra sikerrel rá lehet fordulni. Ám **az utólagos vizsgálatok gyakorta olyan elemi hiányosságokra mutatnak rá**, amelyek elfogadhatatlanok a kiemelten szenzitív adatok védelménél.

Egy tipikusan hasonló példa volt, amikor 2017. szeptemberében szenvedett el a hitelminősítéssel foglalkozó Equifax cég egy olyan informatikai incidenst, amelynek során 143 millió személyes adat szivárgott ki, köztük banki adatok is. Az utólagos forensic vizsgálat ugyanis azt is kimutatta, elmaradt a javítófolt futtatása, és nem is akármilyen körülmények között.

De nem ám, hogy éppen akkor kivételesen nem frissítettek, hanem pénzügyi cégnél nem is létezett szabályozott rendje a hibajavításoknak, és nem volt kinevezett felelőse sem ezen feladatok elvégzésének. De említhetjük a Solarwinds esetet is**, ahol évekig a "solarwinds123" jelszó védte hálózatfelügyelettel foglalkozó cég frissítési szervereit.**

2022. októberében az ausztrál Medibank egészségbiztosítási szolgáltató szenvedett el egy súlyos kibertámadást, amelynek során ellopták 9.7 millió ügyfelük összes személyes adatát: ügyfelek nevét, születési dátumát, címét, telefonszámát, e-mail címét, Medicare-számát, útlevélszámát, egészségügyi vonatkozású információkat és kárigényekre vonatkozó adatokat, például páciensek neve, szolgáltató neve, diagnózisok és eljárások kódjai, illetve a kezelések időpontjai.

A szivárgás következményeként több száz GB érzékeny adat került illetéktelen kezekbe, és BlogXX elnevezésű kiberbűnözői csoport - amely vélhetően a hírhedt orosz REVil csoportból szerveződött újjá - 10 millió USD értékű váltságdíjat követelt a Medibanktól, hogy megakadályozzák a teljes adatbázis közzétételét a darkweben.

Ezzel az incidenssel kapcsolatban derültek ki most érdekes részletek. Az Ausztrál Információs Biztos Hivatala (OAIC) által kiadott új jelentésben az ügynökség vizsgálata megállapította, hogy jelentős működési hiányosságok

vezettek a Medibank hálózatának feltöréséhez, és a jogosulatlan hozzáféréshez.

Az egyik ilyen, hogy a Medibank IT Service Desk Operator munkatársa **a személyes böngészőprofilját használta munkahelyi számítógépén, és a böngészőben elmentette Medibank hitelesítő adatait**. Ezeket a hitelesítő adatokat azután szinkronizálták az otthoni számítógépével, amely megfertőződött egy információlopó rosszindulatú programmal.

Mindez a gondatlanság hozzájárult ahhoz, hogy a támadók augusztus 7-én képesek voltak ellopni az adminrátori szintű hozzáférési adatokat. Ez az admin fiók hozzáfért a Medibank legtöbb rendszeréhez (talán az összeshez), beleértve a hálózati meghajtókat, a felügyeleti konzolokat és a távoli asztali hozzáféréseket. Innen indulva a támadók feltörték a Microsoft Exchange szervert, és a Virtual Private Network (VPN) szolgáltatáshoz is hozzáfértek.

Ez utóbbinál pedig nem használtak többtényezős hitelesítést a bejelentkezéshez. Bár a helyi EDR (Endpoint Detection and Response) rendszer már korábban is bejelzett, ám ezeket nem vizsgálták ki, és csak októberben egy külsős security cég közreműködése leplezte le a támadást.

Szólj hozzá!
Címkék: hiba ausztrália egészségügy adatok mulasztás adatlopás adatszivárgás hiányosságok

Ajánlott bejegyzések:

[Szolgálunk és nem védünk]

[9 millió, bizony, dalolva ment...]

[Az élet szép, de a Life360-nak vannak gondjai]

[Ransomware a nyomkövető rendszerben]

[Az élet szép, de a Life360-nak vannak gondjai]

[Ransomware a nyomkövető rendszerben]

[Ransomware támadás a Nissan ellen]

[Ransomware támadás a Nissan ellen]

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Leveringa függesztés csomag részére

2024. június 24. 13:25 - Csizmazia Darab István [Rambo]

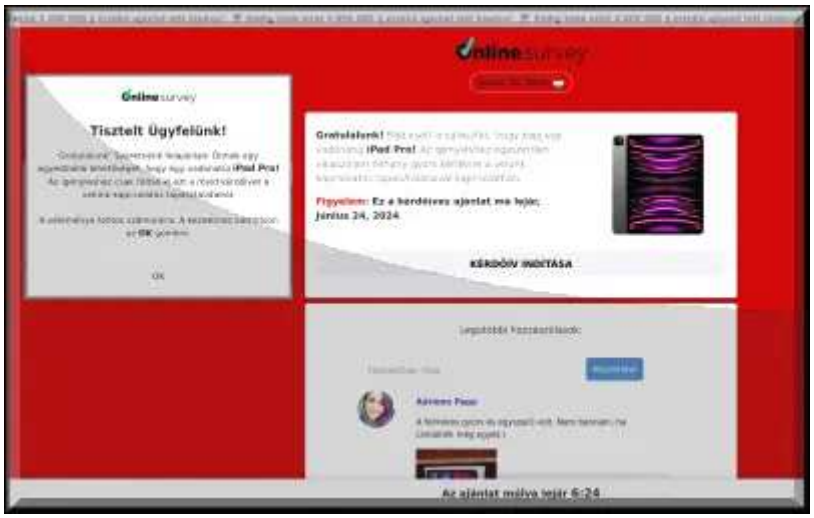
Nagy az Isten állatkertje, és a mondás szerint alacsony a kerítése. Ha valakinek szigorú utasításba adták volna, hogy **készítsen egy minél kreténebb, első látszatra is ordítóan hamis "FedEx Express" csomagértesítő e-mailt**, akkor esetleg járhatna érte egy csillagos ötös. Ellenkező esetben **talán a természetes vagy a mesterséges intelligencia egy kevésbé sikeres munkába állításának disztópikus mintapéldája** került ezzel a szemünk elé.

Még Török Szultán, Fülig Jimmy vagy Tuskó Hopkins alaphelyzetben tanúsított helyesírási ismereteit is mélyen alulmúlja az üzenet szövegezése, **bár közös erőfeszítéssel talán ők is képesek lennének hasonlóan mélyen szánalmasra**, de csak minimum 4-5 üveg kantinbéli rum elfogyasztását és alapos megvesztegetést követően.

A nagy tudású elkövetőknek itt látszólag **még azt az apróságot sem sikerült egyértelműen eldönteni, hogy most a DPD vagy a FedEx futárszolgálat nevében próbálkozzanak**, így lett hát belőle biztos, ami biztos, kettő az egyben. Irány tehát a "*PROBLEMFELOLDODIK*" gomb...

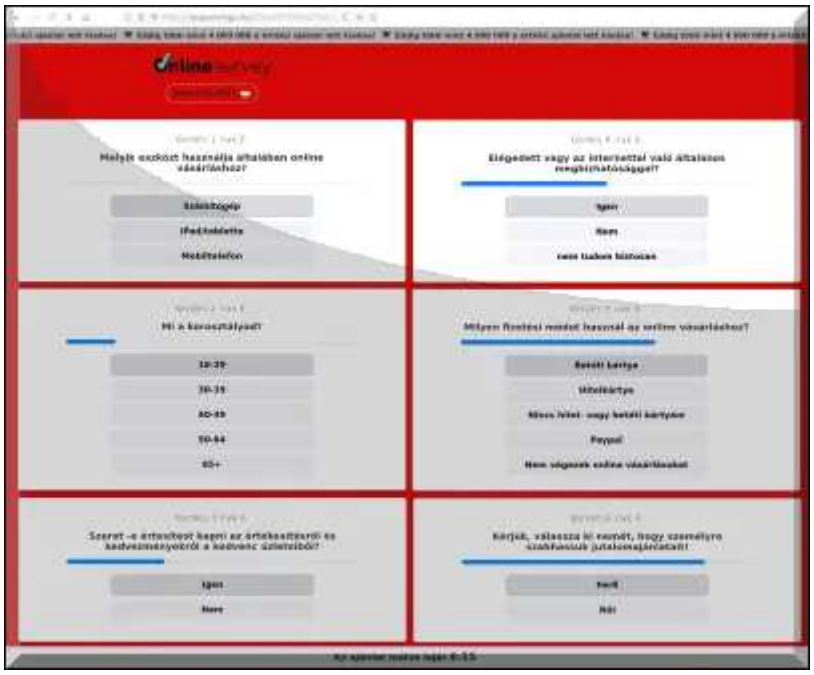
"*A FÜGG. CSOMAG SZÁLLÍTÁSA i.csizmazia, Van (1) csomagod vár kézbesítésre. Használja kódját a követéshez és a kézbesítéshez*" szöveg magáért beszél, csendőr pertu és magázás egyszerre.

További sikeres Darwin díjas mondatok: "***Legyen és találd meg a napot!***", illetve "*Ez automatizálja az ügyfélszolgálati robotunktól érkező e-maileket. Még nem tudnak olvasni, ezért kérlek, ne válaszolj neki.*" De amúgy ez sem rossz: "*Az ajánlat múlva lejár: 6:24*"



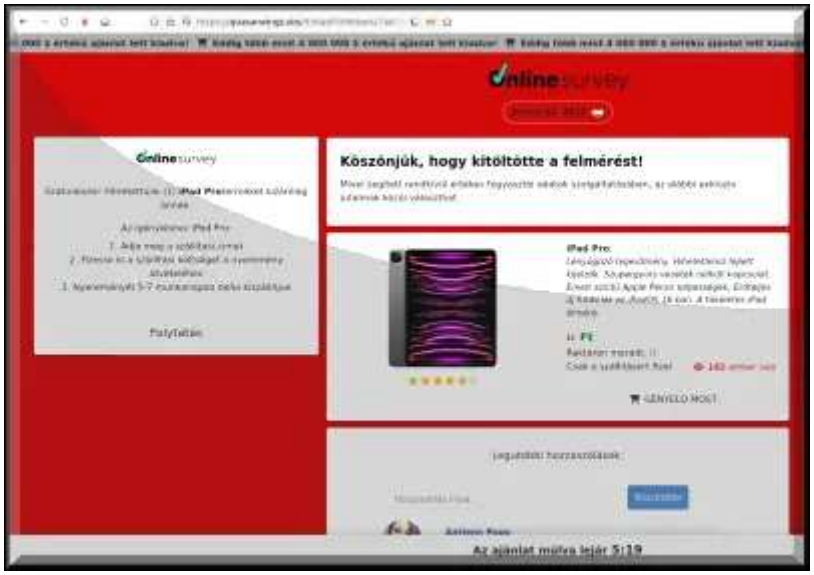
A "...raybane/xaxiiiiiii.html/..." érdekes módon sem a DPD, sem a FedEX hivatalos doménjére nem hasonlít, emiatt esetleg aggódni kellene? Mindenesetre a kiírás szerint **a mi hétköznapi földhözragadt véleményünk roppant fontos nekik, és ezért cserébe ugyebár vár ránk a vadiúj iPad Pro.**

Ráadásul többek közt még Papp Adrienn is pozitívan kommentelt ide, mire várnánk hát ezek után, nyereményre fel, fordítsunk mi is a 100-ik percben!



Netezési és vásárlási szokásaink önbevallásos alapon úgy tűnik, annyira elképesztően értékesek, hogy ezért drága hardvereket osztogatnak csak így nyakló nélkül, ez ugye roppant hihető. Ja nem.

Mi egyébként mindannyian "iPad/tablettán" szoktunk intézni mindent, miért más talán nem?

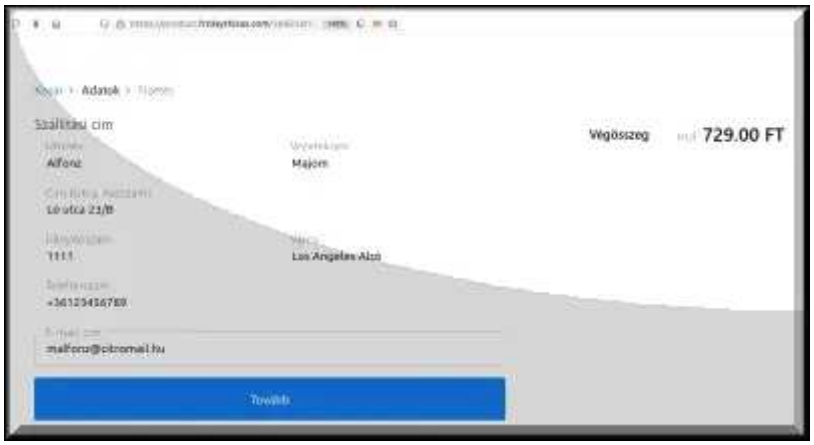


Szerfelett igyekeztünk a kattintásokkal, így "Az ajánlat múlva lejár: 5:19"-re már sikeresen végeztünk is, jöjjön az egy perces úgynevezett munka jutalma, a többszázezer forintos Apple cucc, ez most már egyértelműen jár nekünk.

Irány hát a "*GÉNYELD MOST*" felirat! 5-7 nap múlva biztosan megérkezik.

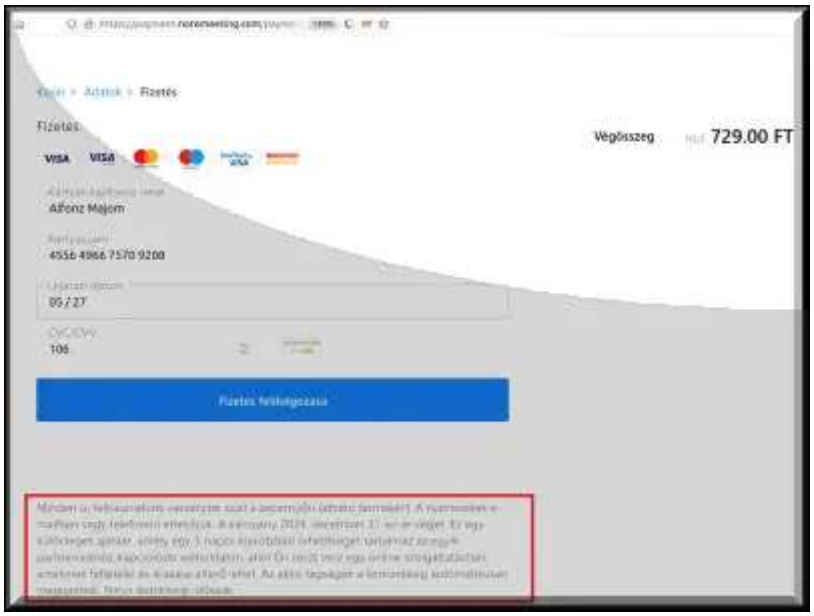
Megadjuk izibe a személyes adatainkat, név, telefonszám, e-mail cím és a pontos lakcímünket, hova kérjük a nyereményt. **Hogy mi a túróért kérdezik meg újta az e-mail címet, amikor éppen most írtak nekünk ide erre a címre, az Élet egyik nagy rejtélye.**

Ezen értesítettek minket, hogy mi nyertünk izéé vagyis hogy csomagunk jött, vagyis izéé mégis nyertünk és közben csomagunk is jött egyszerre? Na nem csoda, hogy a gyengébb idegzetűek itt már elveszíthetik a fonalat ebben a fortyogó kánikulai hőségben.



Illetve most látjuk csak, hogy van egy előre fizetendő szállítási díjnak nevezett dolog, bár mindössze 729 forint. Ilyen sóher bandát, adnak egy 400 ezer forintos tabletet, de a 729 forintot fizessünk ki nekik előre, smucigok.

Még két dolog tűnik fel érdekes módon: a kérdőívet akárhányszor ki lehet tölteni, és akkor akárhány darab iPad Pro eszközt kapunk? Illetve az apró betűs szövegben feltűnik, **tudtunkon kívül előfizettünk valamiféle "szolgáltatásra", aminek a díja mostantól automatikusan és rendszeresen vonva lesz**, de lemondhatjuk. Na most lett elegünk az egészből...



Hölgyeim és uraim, egy újabb gépies lélektelen csalást láthattunk, ebből 12 egy tucat. **Sokat nem dolgoztak vele a pénzünkre azért mégis ácsingózó emberkék**, de még így is félő, hogy sajnos lesznek olyanok, akik örömmel begépelnek mindent.

"Legyen és mindenki találja meg a napot" - ennél frappánsabb zárómondatot viszont még talán a ChatGPT sem tudna iderittyenteni.

3 komment
Címkék: spam apple szánalmas csomag pro e-mail csalás átverés adathalászat hunglish fedex ipad csomagküldő dpd

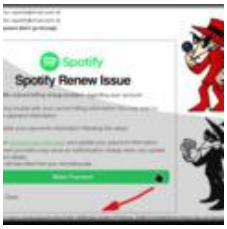
Ajánlott bejegyzések:

"NEM TUDJUK KISZÁLLÍTNI A CSOMAGÁT"

Utolsó emlékeztető a fiók felfüggesztése előtt

Utolsó emlékeztető a fiók felfüggesztése előtt

Kár érte, kiváló ügynök volt...



Spotify megújítási probléma - vagy mégsem?

Netflix: lejárt a tagságunk. Vagy mégsem?

Kommentek:

Androsz · http://wikipedia.blog.hu/ 2024.06.24. 23:44:41

Én már nagyon régóta nem értem, mire is szolgálna ez a CVC kód, ha mindenhol meg kell adnom. A bankok az ezt ismerőknek tágra nyitják a kaput. Ha valahol közvetlen kártyalevonással kell fizetnem, sarkon fordulok, felejtsenek el. Még a PayPal sem az igazi, mert engedély nélkül bármikor levonnak a számlámról, ha szerintük hiteles igénylés érkezett hozzájuk, szóval végül is ők is csak egy beépített ember a rablóbandából. Ideje lenne újragondolni a pénzünk őrzését.

Nota bene: én készpénzben tartom a csöppnyi vagyonomat, én nem fogok efféle szélhámosok miatt állandóan idegeskedni. Hozzám körülményesebb betörni, mint valahonnan a világ végéről a bankomba. És ha hozzám betörnek, arról legalább tudni fogok, lesznek nyomok, bizonyítékok, meg egy remény. Ha a bankból elviszok a pénzemet, akkor ők erre azt fogják mondani, hogy biztos én adtam meg a tolvajnak a jelszót. Mondom, tessék valami jobb módszeren gondolkodni.

Válasz erre

geegee · http://eszakonelunk.blog.hu 2024.06.25. 09:30:24

:D
Ne kritizáljuk őket, mert akkor elkezdenek fejleszteni.Így meg azonnal látható, hogy balf@$zok próbálkoznak csak, lehet bátran ignorálni.

Válasz erre

geegee · http://eszakonelunk.blog.hu 2024.06.25. 09:35:57

Ez a kapca kód a komment elküldésénél is, egy igazi mocskos troll.Aszondja, kattintsam be a képen a buszt.Erre fel van egy villamos...Szokta ezt motor vs bicikli viszonylattal is játszani.Elképesztő.
:D
.
@Androsz: Hát ja, lehetne még bőven fejleszteni.Nekem az szokta kib_ni a biztosítékot, hogy ha valami szolgáltatást kritizál az ember utólag, pl. egy hotelt; akkor simán tudnak utólag ráterhelni büntetést a kártyára a negatív kommentért.És ezt a bank hagyja, kifizeti, és ránk terheli.A pof@'m leszakad.Én még nem jártam így, de olvastam már ilyet, simán elhiszem, hisz ott van a fikázott cégnél minden kártyaadat, meg tudja tenni, ha akarja.Tulképp az egész megtakarítást is be tudná söpörni valszeg...Az ész megáll.Ilyenkor jó a virtuális kártya, amire épp csak annyi pénz van feltéve, ami az adott dolog kifizetéséhez kell, utána a kártyaszám többet nem használható...

Válasz erre

keresés

tweetz

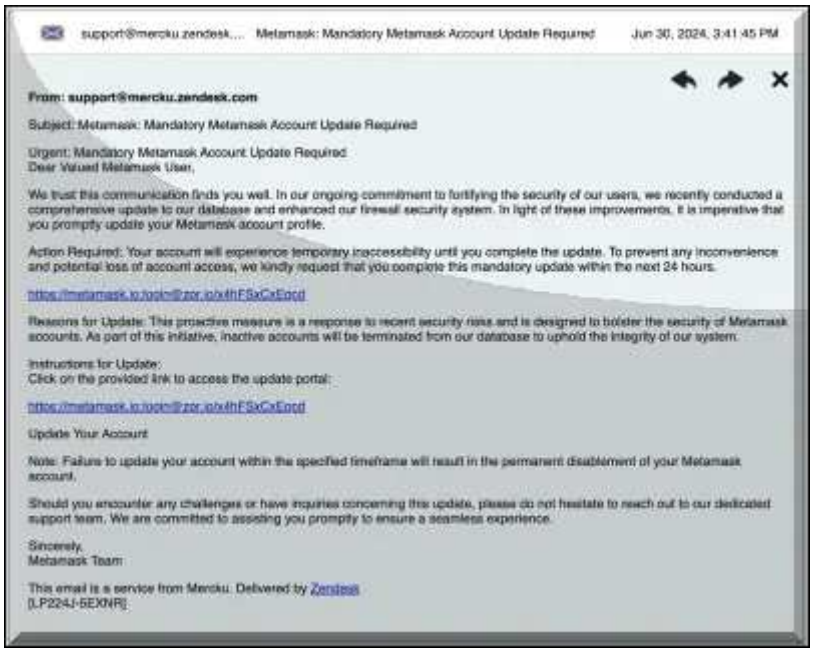
Support kérdésre adathalász válasz

2024. július 01. 18:18 - Csizmazia Darab István [Rambo]

Egy roppant kínos fejlemény zavarta meg a kanadai routergyártó normál napi működését. **A cég terméktámogatási portálját feltörték, és most a normál hibajegyekre megtévesztő adathalász leveleket küldözget a kompromittálódott rendszer.**

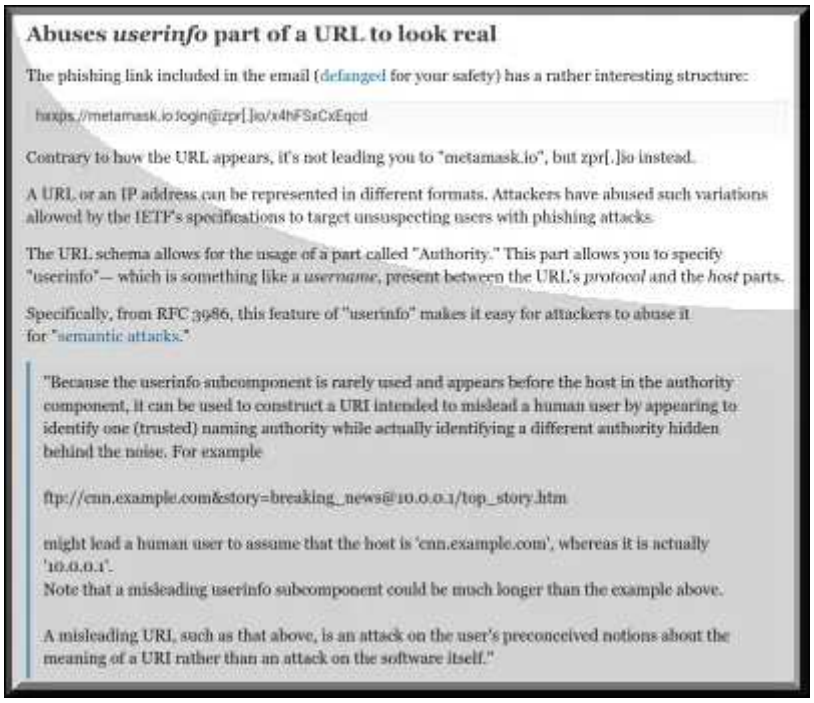
Ilyen eset most nem is rémlik a múltból, mindenesetre furcsa fejlemény. A Mercku elnevezésű kanadai routergyártó helyi ISP és európai internetszolgáltatói piacra is gyárt és szállít termékeket.

A rendszerük feltörése óta azonban automatikus válaszüzenetek generálódnak, amelyek **"Metamask: kötelező Metamask-fiók frissítése szükséges" tárgysorral próbálják megtéveszteni a gyanútlan felhasználókat.**



Az e-mail arra utasítja a felhasználókat, hogy 24 órán belül frissítsék Metamask-fiókjukat, ellenkező esetben elveszítik a tárcához való hozzáférésüket. A MetaMask egy népszerű kriptovaluta pénztárca, amely az Ethereum blokkláncot használja, böngészőbővítményként és mobilalkalmazásként egyaránt elérhető.

Az ilyen kriptotárcák gyakori célpontjai a csalásoknak, és sürgetéssel, fenyegetéssel könnyen kattintásra lehet rávenni az áldozatokat.



A Bleeping Computer közelebbről is megvizsgálta a mellékelt link hivatkozást, amit elég trükkösre csináltak a támadók. A látszólagos domén cím csak a megtévesztést szolgálja, a valódi URL azonban már a zpr.io linkrövídítő szolgáltatást használja, a végső állomás pedig a "hxxps://

matjercasa PONT youcan PONT store" oldalra mutat, amit időközben szerencsére már letiltottak.

A Mercku hivatalosan is értesítve lett a problémáról, hivatalos nyilatkozat egyelőre nincs, ezért az ügyfeleik addig is legyenek óvatosak.

Szólj hozzá!
Címkék: kanada ügyfélszolgálat csalás átverés feltörés adathalászat terméktámogatás metamask mercku

Ajánlott bejegyzések:

Adathalászat vagy jófogás?
Csomagja érke... Na most már elég!
Utolsó emlékeztető a fiók felfüggesztése előtt
Fontos vagy nekem
Adathalászat vagy jófogás?
Csomagja érke... Na most már elég!
Utolsó emlékeztető a fiók felfüggesztése előtt
Fontos vagy nekem
Ment a hűtlen hamis linkkel
Ment a hűtlen hamis linkkel

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Árad a malware a Youtube oldalain is

2024. július 03. 18:17 - Csizmazia Darab István [Rambo]

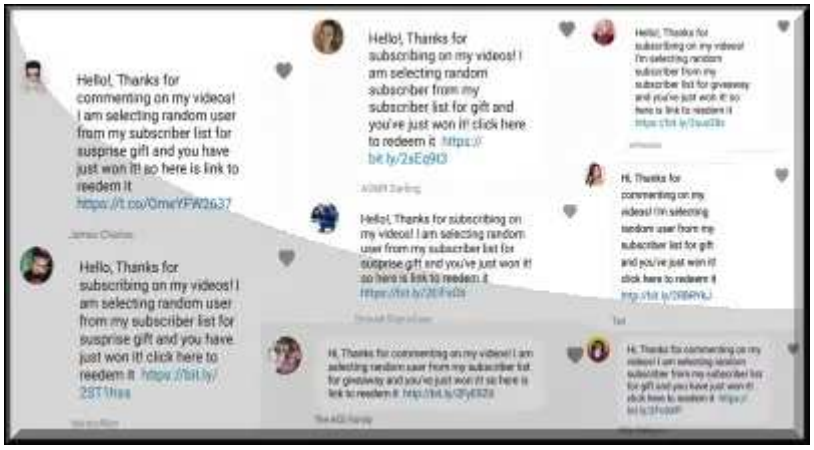
Megszokhattuk már, hogy minden irányból jönnek a kártevős átverések: kéretlen e-mailben, közösségi oldalak üzeneteiben, SMS-ben, sőt álbanki telefonhívásokban is. A TV sokak napi életében egyre kisebb szerepet játszik, míg **helyette a Tiktok és az on demand Youtube videók nézettsége meredeken emelkedik.**

Egyre inkább megfigyelhető tendencia, hogy **minden létező platformot, szolgáltatást kihasználnak a bűnözők, és terítik a kártékony programjaikat. És nincs nehéz dolguk a videómegosztón sem, a spamekhez hasonlóan itt is megjelennek a szokásos csalások: érdekes tartalmakat, videók megtekintéséért pénzkereseti lehetőséget, drága szoftverek ingyenes feltört verzióit ígérik csaliként.**

A warez programoknál egy tipikus átverés, hogy **a leírásban azt jelzik, kapcsoljuk ki a vírusvédelmet, mert az állítólag tévesen riaszt majd**. Ám ha valaki ezt megteszi, igazából éppen ezzel fertőzi meg a saját eszközét.

A technológia elképesztő sebességgel fejlődik, az MI már mindenhol kap részfeladatokat. Például **gyakori, hogy generált karakterek arcával népszerűsítenek Youtube tartalmakat, például a fent említett feltört tartalmakat, vagy egyéb kattintásvadász videókat.**

A kártékony tartalmakra mutató letöltési linkeket a leírásban vagy a hozzászólásokban helyezik el, ezek sokszor megtévesztő alakban jelennek meg, vagy pedig a link rövidítő segítségével vannak elfedve.

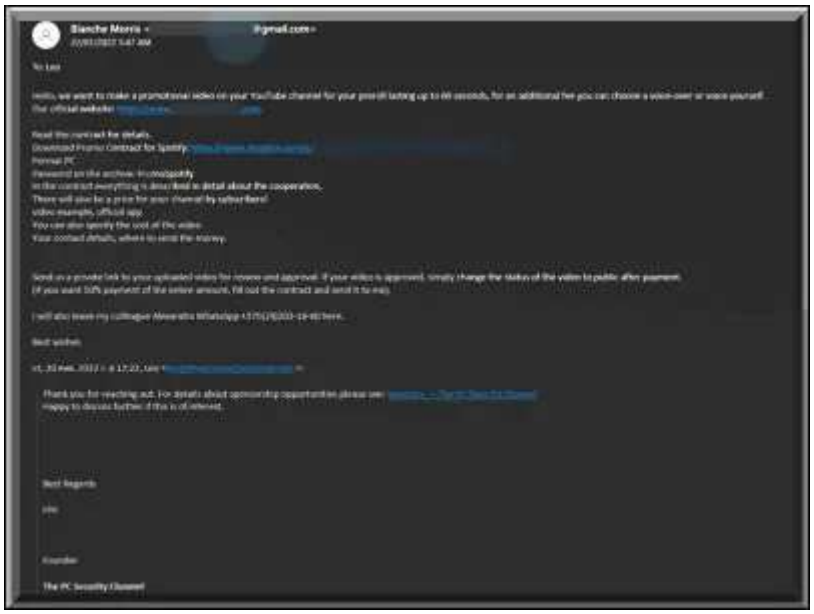


Sok link próbál direktben kártevőt, kémprogramot vagy zsarolóvírust telepíteni az áldozatok gépére, de **nagyon gyakori az adathalász linkek promotálása is.**

A kiberbűnözők ezekkel főképp a sok előfizetővel rendelkező, népszerű YouTube-csatornákat igyekeznek eltéríteni, ezek belépési adatait tömegesen kísérlik meg ellopni, majd itt saját rosszindulatú tartalmaikat teríteni.

Többek közt az érzékeny adatok gyűjtésére és ellopására szolgáló RedLine Stealer, valamint a hírhedt Lumma Stealer tudnak igen komoly károkat okozni, hiszen **ezek böngészési és keresőmotor adatokat, jelszavakat, kriptovaluta pénztárca hozzáféréseket, hitelkártyaszámokat és egyéb érzékeny információkat képesek kompromittálni.**

Előfordul az is, hogy ezeket a kártevőket valamilyen többszereplős online játékokhoz tartozó játék-feltörésnek vagy valamilyen előnyt biztosító csalóeszköznek álcázzák, és így veszik rá a felhasználókat a letöltésre.



Védekezéshez, megelőzéshez használjuk megbízható vírusvédelmet, legyenek erős egyedi jelszavaink, amiket jelszószéfben tárolunk és többtényezős hitelesítéssel is kombináljuk ezeket, valamint tartsuk naprakészen az operációs rendszerünket, illetve szoftvereinket. Legyünk óvatosak a feltört program verziókkal, illetve a kéretlen e-mailekkel és az ezekben található mellékletekkel, linkekkel.

Gyakoriak például a neves kiadók, játékfejlesztő cégek nevében való hamis partnerségi felajánlások, ahol komoly summákat ígérve még a komolyabb influencerek is bedőlnek az ilyen jövedelmező szerződésnek hazudott átveréseknek és kattintanak.

Szólj hozzá!
Címkék: csalás átverés kártevő adathalászat redline lumma YouTube stealer welivesecurity welivesecurity.com

Ajánlott bejegyzések:

CAPTCHA, amely nem az ember-gép relációt teszteli
Fontos vagy nekem
Adathalászat vagy jófogás?
Jöhet-e QR kódos átverés postai papír levélben?

CAPTCHA, amely nem az ember-gép
Fontos vagy nekem
Adathalászat vagy jófogás?
Jöhet-e QR kódos átverés

relációt teszteli

postai papír levélben?

most már elég!

Csomagja érke... Na most már elég!

Csomagja érke... Na most már elég!

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Meghökkentő mesék - adatközpontokról

2024. július 08. 17:23 - Csizmazia Darab István [Rambo]

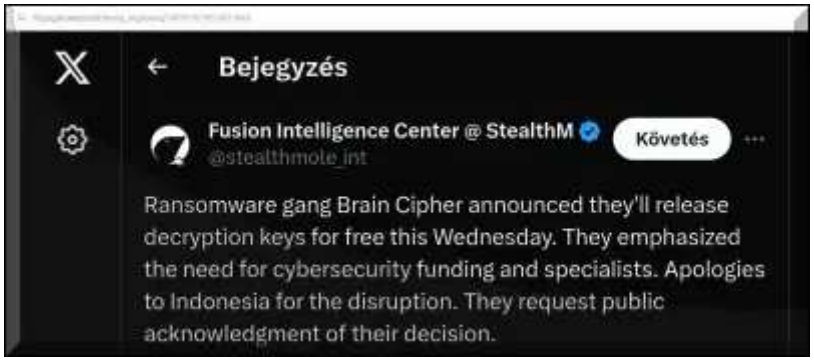
Volt egy ilyen sorozat régebben, ahol az egyik epizódban például egy Cadillac autóban vagy a kisujja épségében fogadhatott a delikvens, vajon sikerül-e egymás után tízszer fellobbantania az öngyújtóját. **Nem kevésbé különös ez a mostani eléggé unortodox lefolyású ransomware támadás sem.**

A zsarolóvírus eddig sem válogatott, illetve pontosabban fogalmazva eddig sem kímélt senkit és semmit. Voltak már a terítéken kormányhivatalok, kórházak, iskolák, rendőrségek, egyetemek, és egyéb hivatalok, iparágak, szektorok.

Egész város megbénítására is láttunk már példát 2023-ban az Oakland elleni incidensnél, **2022-ben pedig Costa Rica esetében egy komplett ország állami intézményei kerültek az Oroszországhoz köthető Conti és Hive bűnbandáinak célkeresztjébe.**

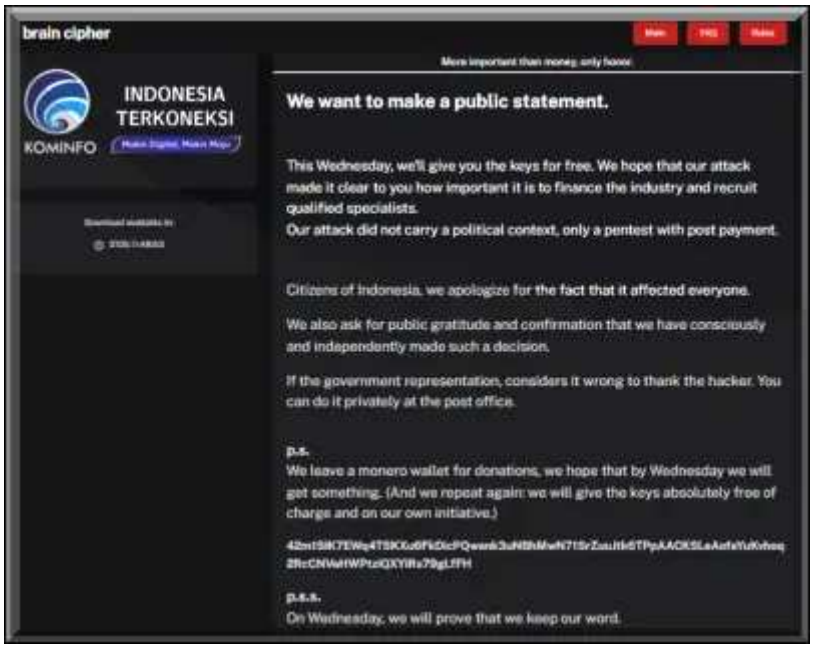
Ez utóbbihoz hasonlít a mostani csodálatos történet is, ahol megint csak egy konkrét ország a célpont, mégpedig Indonézia. **A Lockbit egy újabb változatával operáló Brain Cipher bűnözői csoport még júniusban törte fel és titkosította az országos Nemzeti Adatközpont (PDNS) fájljait, majd 131 milliárd rúpia (nagyjából 8 millió dollár, cirka 2.9 milliárd forint) értékű váltságdíjat követeltek.**

Amit az indonéz kormány viszont nem volt hajlandó kifizetni, miután a tárgyalások állítólag holtpontra jutottak.



A folytatásban aztán **július 2-án elnézést kértek a tettükért Indonézia polgáraitól, és állítólag a hivatalos szervek nyomása nélkül, teljesen önként nyilvánosan átadtak egy visszafejtő kulcsot**. Hangsúlyozták, hogy más megtámadott cégeknek, intézményeknek már nem fognak ilyen jellegű engedményt tenni.

A közleményükben a Brain Cipher félreértésről beszél, hogy ez itt nem is volt igazi ransomware bűncselekmény, hanem csak egy figyelemfelhívó halasztott fizetésű pentester vizsgálat. És hogy mennyire vastag a bőr a képükön, ezek után még a Monero alapú számlájukra várnak szíves adományokat a nagylelkű "ingyenes" helyreállító kódért.



Ám **mindeközben az állam oldaláról is roppant érdekes kép bontakozott ki az incidens kapcsán. Az egyik nyilatkozó például tarthatatlannak nevezte azt a helyzetet, amikor is a 700 milliárd rúpia (15.6 Mrd HUF) költségvetésű intézményrendszer védelme mindössze a Windows beépített Windows Defender biztonsági rendszerére támaszkodik, miközben mint kiderült, kötelezően előírt mentési folyamatok sincsenek bevezetve.**

Egy parlamenti videóban az is elhangzott, hogy a két feltört adatközpont egyikében tárolt adatok 98 százalékáról egyáltalán nem készült biztonsági másolat - hát no comment.

Az ügyben Budi Arie Setiadi kommunikációs és informatikai miniszter lemondását követelő petíció eddig már több, mint 18 ezer aláírást gyűjtött össze, valamint ezt követően az ország elnöke elrendelte a kormányzati adatközpontok azonnali teljes átvilágítását.

Szólj hozzá!

Címkék: indonézia mentés váltságdíj adatközpont ransomware zsarolóvírus lockbit braincipher

Ajánlott bejegyzések:

A kriptobevételek felett az égbolt felhőtlen

Kórházak a pácban II.

LockBit üti Subway, sakk

A kriptobevételek felett az égbolt felhőtlen

Kórházak a pácban II.

LockBit üti Subway, sakk

LockBit piacgazdaság és tervgazdálkodás

9 millió, bizony, dalolva ment...

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Egyre gyakoribb az AI és a deepfake a támadásokban

2024. július 10. 18:11 - Csizmazia Darab István [Rambo]

Az ESET legutóbbi **kiberfenyegetettségi jelentése** tavaly decembertől 2024. májusáig terjedő időszak trendjeit elemzi, eszerint **az adatlopó kártevők (infostealers) olyan generatív AI-eszközöket is elkezdtek aktívan használni, mint a Midjourney, a Sora vagy a Google Gemini.**

2024. első felében **dinamikusan terjedtek az Android rendszereket érintő pénzügyi fenyegetések, valamint a mobilbankoláshoz kapcsolódó kártékony programok, legyen szó "hagyományos" rosszindulatú banki szoftverekről vagy éppen kriptolopásokról.**

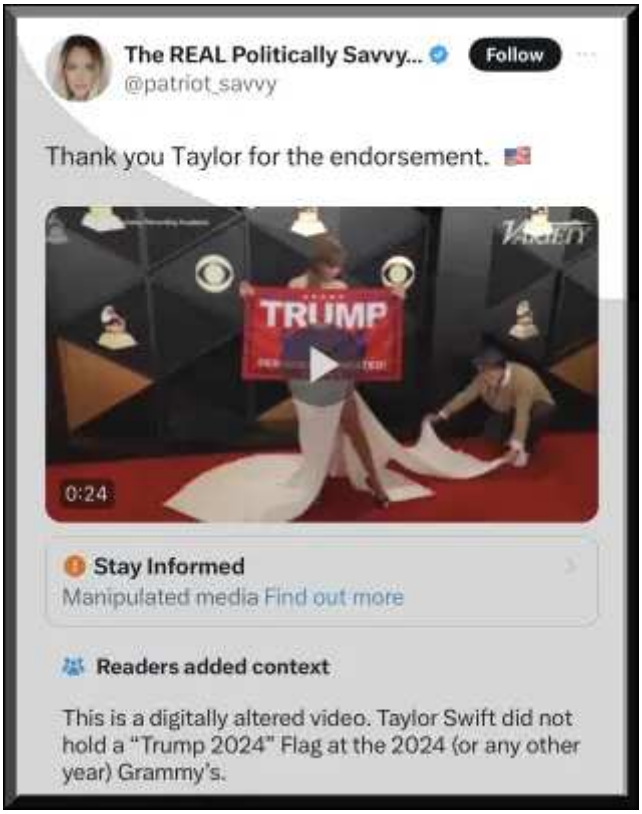
A Rilide Stealer olyan generatív AI-asszisztensek nevével élt vissza, mint az OpenAI Sora és a Google Gemini. A Vidar adattolvaj szoftver pedig a **Midjourney mesterséges intelligencia-képgenerátor Windowsos asztali alkalmazásának adta ki magát** - annak ellenére, hogy a Midjourney AI-modellje csak a Discordon keresztül érhető el.

A kiberbűnözők már 2023. óta egyre inkább visszaélnek a mesterséges intelligenciával - és ez a tendencia várhatóan folytatódni fog. A magyarországi viszonyok között a korábban megszokott gyenge helyesírással rendelkező átverések mellett egyre gyakrabban érkeznek az AI segítségével generált néha jobb, néha gyengébb minőségű szövegek.

Illetve megjelentek már a magyar hírességek nevével visszaélő generált fotós és deepfake videós csalások is, legutóbb például Esztergályos Cecília nevében durva helyesírási hibákkal hirdettek egy átverős videóval.

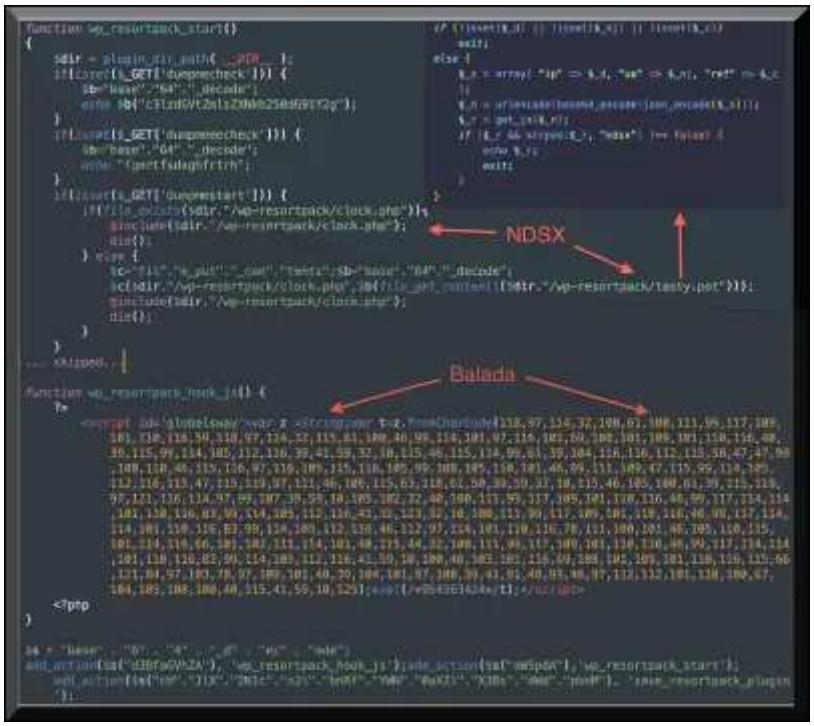
A beszámolóban szó esik még arról is, hogy **az új, mobilokat veszélyeztető GoldPickaxe kártevő képes arcfelismeréssel kapcsolatos adatokat lopni. Ezek segítségével aztán megtévesztő deepfake videókat hoz létre, amelyeket a rosszindulatú szoftver működtetői pénzügyi tranzakciók hitelesítésére használnak.** A GoldPickaxe Android és iOS verzióval is rendelkezik, és kártékony alkalmazásokon keresztül vesz célba délkelet-ázsiai áldozatokat.

A deepfake támadásokkal a Hackfelmetszők - Veled is megtörténhet! podcast legújabb 20. adása is foglalkozik. **Ebben többek közt szó esik Taylor Swift deepfake videóiról, csaló videókkal történő politikai nyomásgyakorlásról vagy épp barátoktól átveréssel kicsalt összegekről is.**



Folytatódtak a gamerek elleni támadások is, melynek során a hivatalos játékplatformokat megkerülő játékosokat is megtámadták. Kiderült például, hogy néhány **feltört videójáték és az online többszereplős játékokban használt csaló (cheat) eszközök olyan adatlopó kártevőket tartalmaznak, mint például a Lumma Stealer és a RedLine Stealer.**

A kutatók mérése 2024. első félévében már többször észlelte a RedLine Stealert, spanyolországi, japán és németországi támadások során. A legutóbbi Redline támadáshullámok egyre erősödnek, 2024. első félévében már 30%-kal több ilyen próbálkozás történt.



A WordPress bővítmények sebezhetőségének kihasználása sajnos nagyon gyakori, a jól ismert Balada Injector csoport 2024 első felében is folytatta tevékenységét, amivel több mint 20 ezer weboldalt veszélyeztetett, a telemetria pedig **több mint 400 ezer alkalommal jelezte a csoport legutóbbi akciójában használt újabb variánsok megjelenését.**

A zsarolóprogramok terén a korábbi vezető szereplőt, a LockBitet a Chronos-művelet, vagyis a bűnüldöző szervek által 2024. februárjában végrehajtott globális akció időlegesen letaszította a trónról. **Bár a kutatók két figyelemre méltó LockBit kampányt is észleltek 2024. első félévében, ezekről kiderült, hogy olyan, nem a LockBithez tartozó csoportok támadásai voltak, amelyek a kiszivárogtatott LockBit-segédprogram kódját használták.**

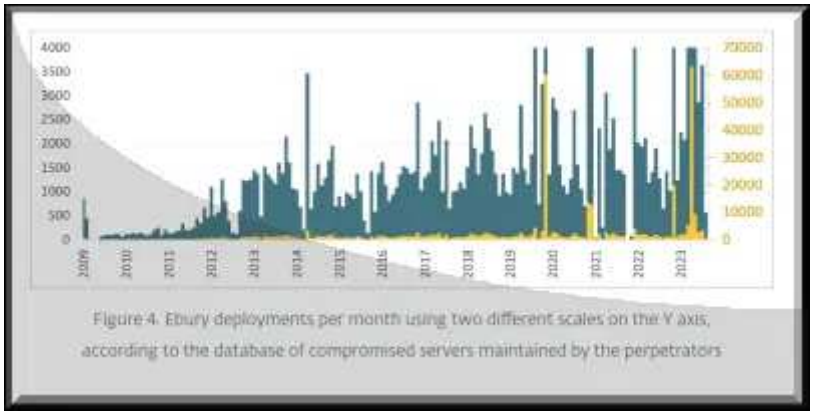


Figure 4. Ebury deployments per month using two different scales on the Y axis, according to the database of compromised servers maintained by the perpetrators

A jelentés emellett beszámol arról a nemrégiben közzétett mélyreható vizsgálatról is, amely a legfejlettebb, és továbbra is terjedő szerveroldali kártevő kampányról, vagyis az Ebury csoportról és az általuk használt rosszindulatú szoftverekről és botnetekről szól.

Az évek során az Ebury-t hátsó ajtó programként alkalmazták, amellyel közel 400 000 Linux, FreeBSD és OpenBSD szervert támadtak meg, melyek közül 100 ezer még mindig kompromittálva volt 2023. végén, és a megfigyelések szerint a kártevő azóta is aktívan terjed.

Mivel egy évtizednél is régebbi, folyamatosan fejlesztett és roppant kifinomult kártékony programról van szó, érdemes lehet az érintett rendszerek üzemeltetőinek Marc-Etienne M.Léveillé, az ESET kártevőkutatójának részletes leírása alapján tájékozódni.

Az ESET Threat Report H1 2024 című angol nyelvű részletes kiadványa itt olvasható: https://www.welivesecurity.com/en/eset-research/eset-threat-report-h1-2024/

Szólj hozzá!
Címkék: jelentés riport helyzet eset kártevő threat mérések welivesecurity welivesecurity.com telemetria

Ajánlott bejegyzések:

Árad a malware a Youtube oldalain is

Booking com átverések

Árad a malware a Youtube oldalain is

Booking com átverések

Ami majdnem az, az nem az

Matatás a robotporszívók agyában

Végképp eltörölni

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

Úgy hívnak motorizált nemzedék...

2024. július 15. 18:01 - Csizmazia Darab István [Rambo]

Láttunk már többször is hatalmas, Guiness rekordok évkönyvébe illő váltságdíj fizetéseket ransomware történeteknél. **Például a CWT Business Travel Management Company 4.5 millió dolláros összeget szurkolt le (akkori árfolyamon nagyjából 1.3 milliárd forint) a Netwalker bandának 2 TB ellopott és titkosított céges adatért, míg a UnitedHealth Group egészségügyi konszern 22 millió dolláros (7.8 mrd HUF) váltságdíjat fizetett ki az orosz Blackcat/ALPHV csoportnak.**

A mostani eset **az amerikai CDK Global nevű, autókereskedések szolgáltatásait ellátó céget sújtotta. Az Egyesült Államokban csaknem 15 ezer autókereskedésben futnak ezek a szoftverek, ám június közepén zsarolóvírus támadás miatt egy több hetes leállási időszak következett be**, ami rengeteg autókereskedési és szervizközpont helyszínen bénította meg a hétköznapi normál működést.

A kiberincidens miatt az egységek az átmeneti időszakban országszerte mindenfajta informatikai támogatás nélkül tudtak csak dolgozni, a CDK pedig elnézést kért az okozott kellemetlenségekért.

A támadás időzítése mindenesetre alaposan megtervezettnek tűnik, hiszen június 19. munkaszüneti nap volt. **A hosszas offline állapot miatt, mivel a rendszerek egyáltalán nem voltak elérhetők, a márkakereskedések egy része nem tudott autókat eladni, járműveket regisztrálni, illetve az autójavító műhelyek sem tudták a szükséges alkatrészeket megrendelni. Emiatt papíralapú, telefonálós módszerre kellett visszaállniuk.**

Miután a múlt héten visszaállították a szolgáltatások jelentős részét, hivatalos bejelentés híján a CNN információkból lehet kikövetkeztetni, hogy **a háttérben két nappal az eredeti támadás után 25 millió dolláros váltságdíjat fizettek ki a gyaníthatóan orosz kötődésű BlackSuit csoport részére a helyreállító kulcsokért.**

A TRM Labs kriptográfiai szakértői cég állítása szerint **egy 387 bitcoin értékű tranzakció egy olyan számlára került, amelyet állítólag a BlackSuit néven ismert zsarolóprogramokat telepítő bűnözők**

birtokolnak. Az információk szerint az átutalás nem közvetlenül a CDK-tól származik, hanem egy kiberváltságdíj követelési tárgyalásokra szakosodott közvetítő cégtől.

Bár a doxing, azaz a bizalmas adatok kiszivárogtatásával való fenyegetés más állandó része a támadásoknak, **manapság a legtöbb zsarolóvírus-áldozat már nem fizet váltságdíjat, például tavaly a negyedik negyedévben mindössze 29% fizetett.** Emellett a hatóságok sem javasolják a fizetést, hiszen ezzel erősítik a bűnözők effajta ténykedését, illetve újabb támadásokat is elszenvedhetnek.

A bűnözők ezzel az akcióval viszonylag jól jártak, hiszen többet kerestek, mint a Change Healthcare támadói. Azonban az is érdekes adat, hogy az autókereskedőket ért pénzügyi kár a teljes leállás három hetében több mint 944 millió dollár, vagyis a váltságdíj 37-szerese. **És ez az adat még nem tartalmazza az olyan nehezen számszerűsíthető tényezőket, mint a jó-hírnévhez csorbulása miatti kár, a felháborodott ügyfelek és a leállás utólagos jogi következményei.**

A TheRegister cikke szerint azonban azóta sem működik az ügyfélkapcsolati (CRM), illetve a központi dokumentum kezelési (DMS) rendszer, ezek még mindig offline vannak. A CDK továbbra sem kívánt nyilatkozni.

Szólj hozzá!
Címkék: usa global váltságdíj cdk ransomware zsarolóvírus blacksuit gépjárműkereskedelem

Ajánlott bejegyzések:

[100 millió ember egészségügyi adata hoppszi](#)

[Holló a hollónak mégiscsak, de igen...](#)

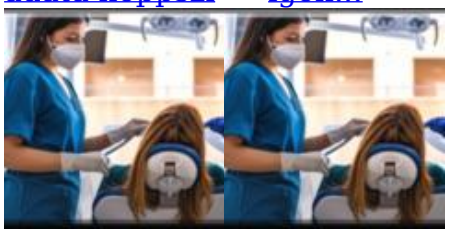
[Kórházak a pácban II.](#)

[100 millió ember egészségügyi adata hoppszi](#)

[Holló a hollónak mégiscsak, de igen...](#)

[Kórházak a pácban II.](#)

[8 kórház, 30 klinika, 2.5 millió betegadat](#)



[9 millió, bizony, dalolva ment...](#)

[9 millió, bizony, dalolva ment...](#)

Kommentek:

Nincsenek hozzászólások.

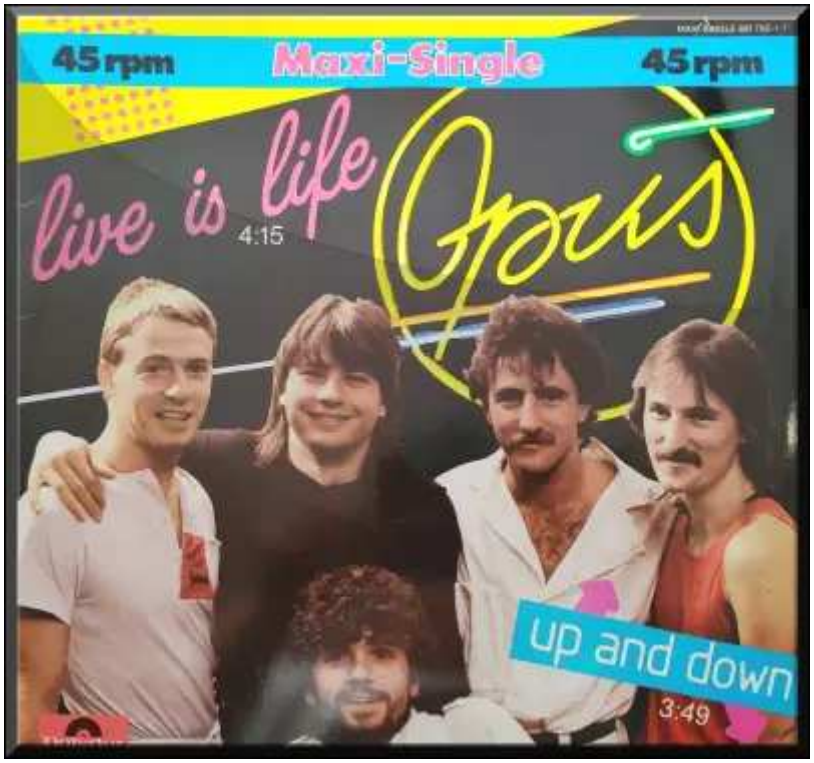
keresés

tweetz

Az élet szép, de a Life360-nak vannak gondjai

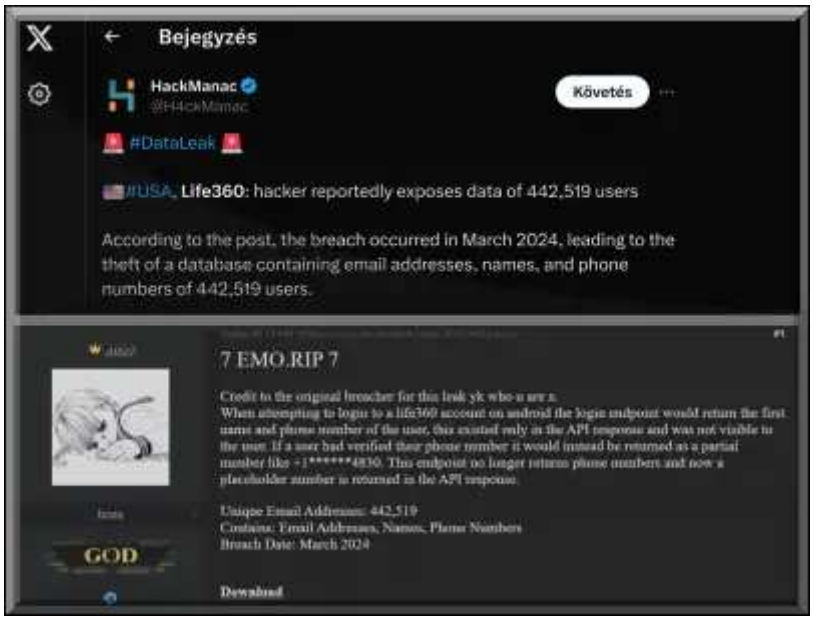
2024. július 18. 13:18 - Csizmazia Darab István [Rambo]

Sokan ismerhetik a Life360 csomagot, amely egyfajta kényelmes szülői felügyeletként segíthet a gyermekek fizikai helyzetének nyomonkövetésében, a családtagok egymás közti kommunikációjában. Ezúttal **egy friss incidens kapcsán szivárogtak ki tömegesen ügyféladatok** a kaliforniai székhelyű cégtől.



Egy furcsa **API hibát használt ki az a támadó, aki nemrégiben több, mint 400 ezer Life360 felhasználó telefonszámát** tartalmazó adatbázist szivárogtatott ki. Az adatok állítólag még 2024. márciusában kompromittálódtak.

Az ezek ellopására kihasznált sebezhetőség lényege pedig abban állt, hogy **androidos bejelentkezéskor a nem biztonságos API válaszban kicsillagozott maszkolás nélkül jelent meg a név és a teljes kitakaratlan telefonszám.**



Az elkövető szerint **az üzemeltetők azóta már kijavították** ezt a fentemlített hibát.

A Bleeping Computers értesülései alapján arra következtethetünk, hogy nem kamu a dolog: **a kiszivárgott adatok valóságosnak tűnnek, és látszólag igazi felhasználók információit tartalmazzák.**

A Life360 az említett valós idejű helymeghatározáson felül **balesetészlelést és sürgősségi közúti segélyszolgálatot is biztosít világszerte több, mint 66 millió ügyfelének**, miután 2021-ben megvásárolta a Tile Bluetooth-követő szolgáltatót.

Emlékezetes, hogy épp a múlt hónapban kerültek a címlapokra azzal, hogy feltörték a Tile ügyfélszolgálati platformját, és **a rendszerből neveket, címeket, e-mail címekeket, telefonszámokat, és eszközazonosító számokat loptak el. Mindez arra is jól rámutat, hogy az ilyen típusú társaságok, amelyek nyomon követik az emberek tartózkodási helyét, a hackerek célpontjává válhatnak.**

Szólj hozzá!
Címkék: váltságdíj adatlopás nyomkövető adatszivárgás ransomware kibertámadás tile doxing life360

Ajánlott bejegyzések:

Ransomware a nyomkövető rendszerben

Ransomware támadás a Nissan ellen

9 millió, bizony, dalolva ment...

Go Western Digital II.

Ransomware támadás érte az MSI-t

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Crowdstrike utóhatás

2024. július 24. 10:36 - Csizmazia Darab István [Rambo]

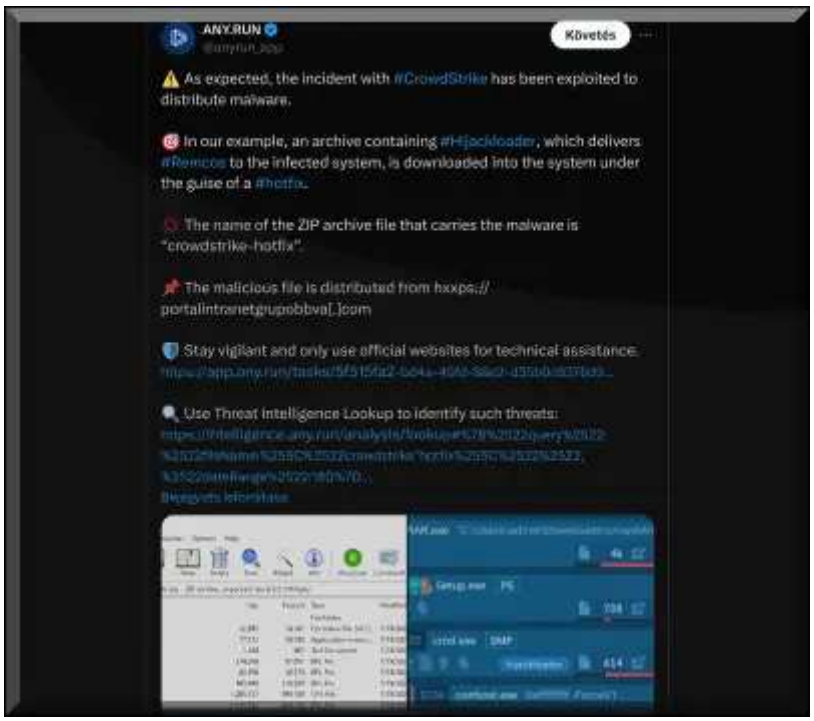
Nagyjából már túl vagyunk egy nem mindennapi kékhalál maratonon, amely világszerte komoly leállásokat okozott. **A nagy informatikai összeomlás 8.5 millió Windows-eszközt érintett**, melyben repterek, bankok, tévéadók, közlekedési terület, egészségügyi szektor, tőzsdék bénultak meg, emellett komolyan bezuhant a Crowdstrike részvények értéke is.

A Crowdstrike jelentős szereplő a piacon, világszerte 20 ezer ügyfelük van, köztük a Fortune 500 listán szereplő vállalatok több mint fele, de az USA több jelentős kormányzati szervezete is az ő szoftverüket használja. **A múlt pénteki hibás frissítés lefagyásokat, kék halált és több napos káoszt idézett elő.**

Bár a gyártó egy idő után kiadott aztán egy javított frissítést, **ám a helyreállítás már így is nehézkes és időben hosszan elhúzódó folyamat lett.**

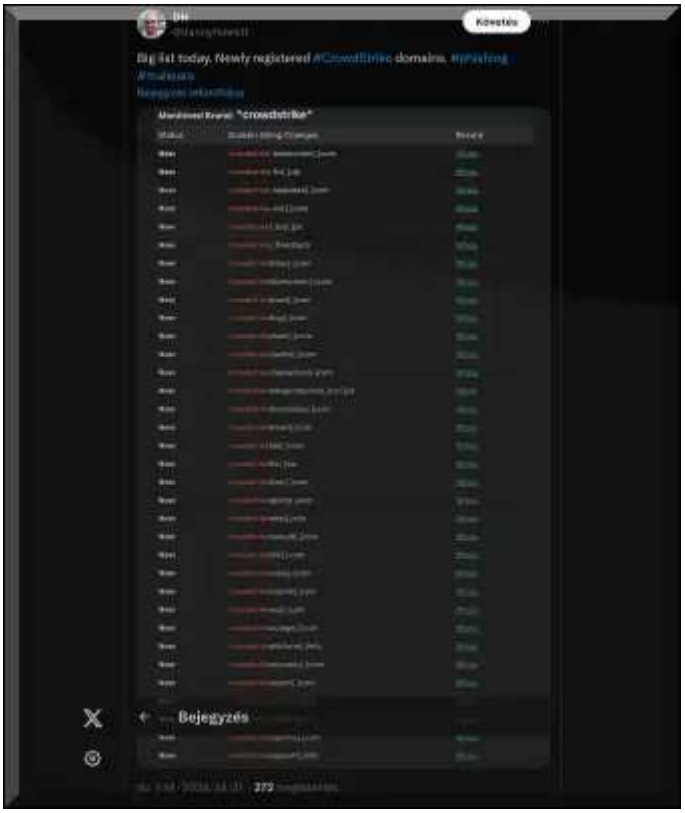
És ahogy minden jelentős eseményre lecsapnak a kártevőterjesztők is, ide is megérkeztek a dögkeselyűk. Több beszámoló szerint spam kampány keretében kéretlen üzenetek terjednek a CrowdStrike Support nevével visszaélve. A levelekben **a csalók kártékony weboldalakra mutató linkeket, illetve rosszindulatú fájlmellékleteket** helyeztek el, így a károsultaknak a leállások mellett erre is kiemelten érdemes figyelniük.

Az adathalászok is rámozdultak a kihasználható lehetőségre, és **megtévesztő domain nevek sokaságát regisztrálták be a napokban, vagyis várhatóan nagyüzemben kapjuk majd** az ezzel kapcsolatos csaló üzeneteket.



A leállás okozta veszteségek számszerűsítése még folyamatban van, **már most is 10 milliárd dollárra becsülik az okozott kár mértékét.**

És ha már utóhatásokat emlegettünk, azt sem szabad kihagyni itt az egyenletből, hogy még csak most fog elindulni a károsultak által a Crowdstrike ellenében indított a felelősségbiztosítási pereknek az a nehéz időszaka, amelyek a már most is jelentős mértékű veszteséget tovább növelve akár csődbe is viheti majd a vállalatot.



Remélhetőleg, mindebből senki nem azt a helytelen tanulságot vonja le, hogy mostantól soha többet nem frissít semmit. Minden alkalmazás rendszeres frissítésre szorul, és ezek a hibajavítások segítenek kivédeni az adatainkat fenyegető veszélyeket, orvosolnak korábbi számos hibás működést, bezárnak kihasználható sérülékenységeket.

Ezzel együtt az is igaz, hogy ha ritkán is, de maguk a szoftverfrissítések is előidézhetnek néha problémákat.

Fontos, hogy **a hibajavítások biztonságos előzetes tesztelése a gyártó felelőssége**, emellett vállalati környezetben bevált best practice, hogy először tesztkörnyezetben frissítenek, és csak ezután küldik ki a javításokat az éles rendszereikre.

A mostani incidens ellenére digitális életünk védelmének egyik leghatékonyabb eszköze továbbra is az, ha napra készen tartjuk a szoftvereinket. **Miközben semmi garancia nincs arra, hogy a későbbiekben ne forduljon elő a fentihez hasonló eset.**

Szólj hozzá!
Címkék: spam frissítés káosz kár kékhalál veszteség hibás adathalászat bsod crowdstrike welivesecurity.com

Ajánlott bejegyzések:

Én és én meg a hibás frissítés

Utolsó emlékeztető a fiók felfüggesztése előtt

Fontos vagy nekem

Én és én meg a hibás frissítés

Tipikus adathalász üzenet tárgysorok

Utolsó emlékeztető a fiók felfüggesztése előtt

Fontos vagy nekem
Ment a hűtlen hamis linkkel

Ment a hűtlen hamis linkkel

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkereső csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

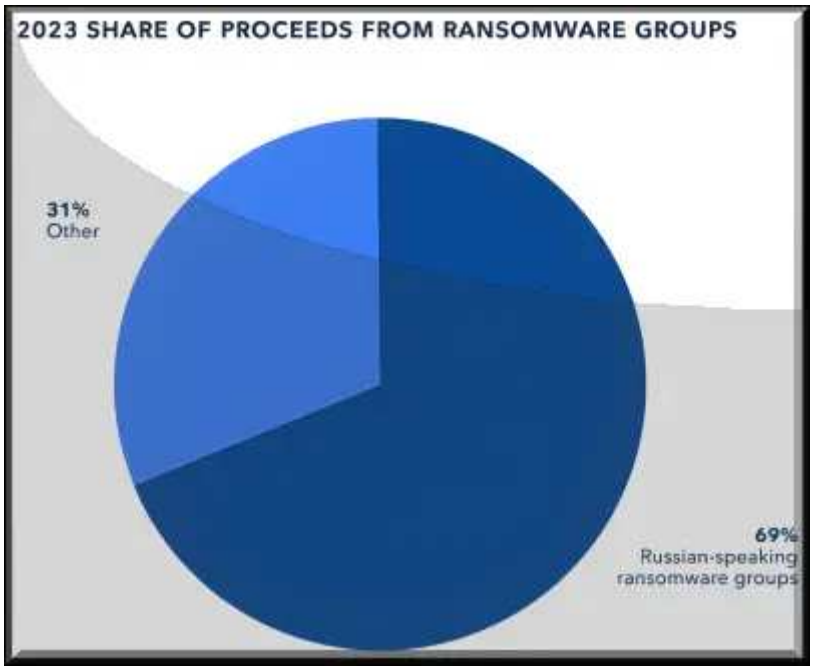
A kriptobevételek felett az égbolt felhőtlen

2024. július 29. 19:02 - Csizmazia Darab István [Rambo]

Egy friss elemzés eredménye azt mutatja, hogy 2023-ban j**ó évet zártak a pénzmosásra és zsarolószoftver terjesztésre szakosodott bűnözői csoportok**.

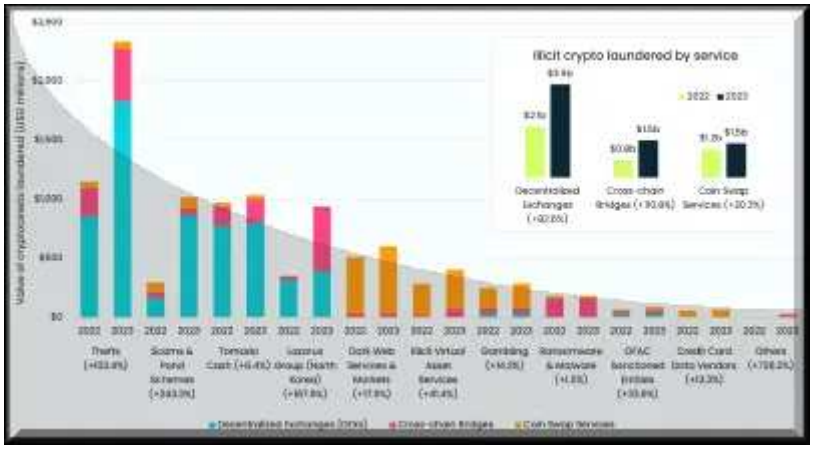
Az orosz ransomware bandák adják az összes váltságdíjból származó bevétel 69%-át, ami összegszerűen 500 millió dolláros (cirka 180 milliárd forintnyi) bevételt jelentett a tavalyi esztendőben.

A kriptográfia segítségével elkövetett bűnözés elemzésére szakosodott TRM Labs jelentése szerint a volt Szovjetunió területéről indított zsarolóvírus támadások, a kriptovalutákkal kapcsolatos csalások, valamint a darknetes piactereken történő visszaélések **masszív bevételi forrást jelentenek a bűnözői csoportoknak, alacsony lebukási kockázattal.**



Észak-Korea szintén vezető szerepet tölt be a különféle kriptovalutás csalások, átverések, adatlopások területén, a világszerte elkövetett akcióikkal 2023-ban több mint egymilliárd dollárt sikerült ellopniuk.

Ázsiában továbbra is roppant gyakoriak a kriptovalutákkal kapcsolatos **befektetési csalások, átverések, amelyek kiemelkedő bevételeket, busás hasznot ígérnek.**



A ransomwarekre visszatérve 2023-ban ezen a téren **a LockBit, a Black Basta, az ALPHV/BlackCat, a Cl0p, a PLAY és az Akira voltak a legjelentősebb szereplők,** ezek mind orosz irányítású bandák. Bár időközben például a BlackCat leállt, új csoportok léptek a helyükbe, például **a RansomHub, amely gyorsan az egyik legaktívabb szereplővé avanzsált.**

A bevételek alapján a LockBit és az ALPHV volt a legnyereségesebb a tavalyi évben, 320 millió dollár értékű kriptovaluta váltságdíjat gyűjtöttek be a beszámoló szerint. A szolgáltatásként kínált Ransomware-as-a-Service (RaaS) továbbra is az egyik legjövedelmezőbb üzletág maradt.

Oroszország a pénzmosás terén is domináns, csak az oroszországi székhelyű Garantex egymaga az itteni forgalom 82%-át tette ki a kriptovalutás ügyleteknél. A kriptovalutával fizetett darknetes gyógyszereladás területén pedig az oroszországi szereplők 95%-ban uralták az itteni piacot.

A jelentés arra is utal, hogy az így befolyt bevételeket nagy valószínűséggel kínai gyártóktól vásárolt katonai felszerelésekre és a szankciók miatt elérhetetlen kritikus műszaki alkatrészek vásárlására költhették.

Hol van már az a 2005-ös sokkoló felismerés, amikor azzal szembesült a világ, hogy a különféle számítógépes kártevőkkel, csalásokkal, átverésekkel elkövetett bűncselekményekből az USA-ban abban az ében az elkövetőknek már több pénzük származott, mint a drogkereskedelemből.

19 év elteltével elmondható, hogy a helyzet nem kevésbé sokkszerű, a védekezés-megelőzés pedig mindenkinél rengeteg erőforrást emészt fel - de más lehetőség nem nagyon van.

Szólj hozzá!
Címkék: statisztika orosz oroszország elemzés csalás átverés bevétel váltságdíj ransomware kriptovaluta zsarolóvírus lockbit kriptobefektetés trm-labs

Ajánlott bejegyzések:

Mire költsünk 27 milliárd forintot?

LockBit üti Subway, sakk

Mire költsünk 27 milliárd forintot?

LockBit üti Subway, sakk

LockBit piacgazdaság és tervgazdálkodás

Windows frissítés vagy mégsem? Újabb rombolás brit kórházakban

Újabb rombolás brit kórházakban

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

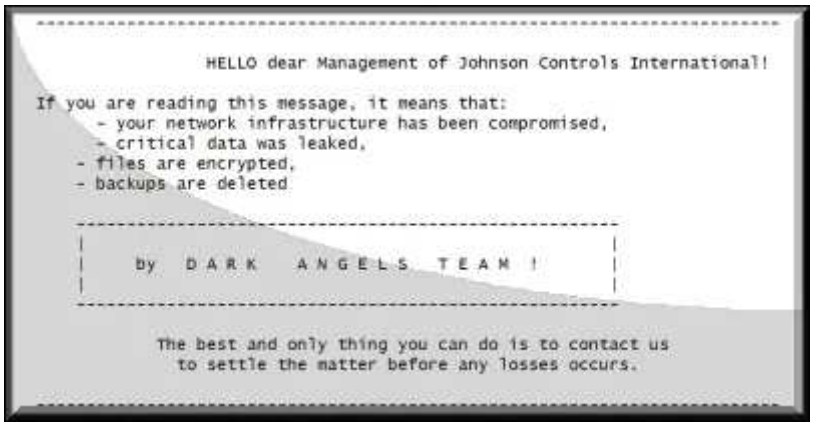
Mire költsünk 27 milliárd forintot?

2024. július 31. 18:09 - Csizmazia Darab István [Rambo]

Úgy tűnik, a fenti kérdést tette fel magának az amerikai Fortune listán szereplő vállalatok egyike, és aztán végül zsarolóvírus váltságdíjra fordították a fenti összeget.

Már évek óta hatalmas számok röpködnek a levegőben, és minden egyes esetben elképedünk az összegek nagyságát látva.

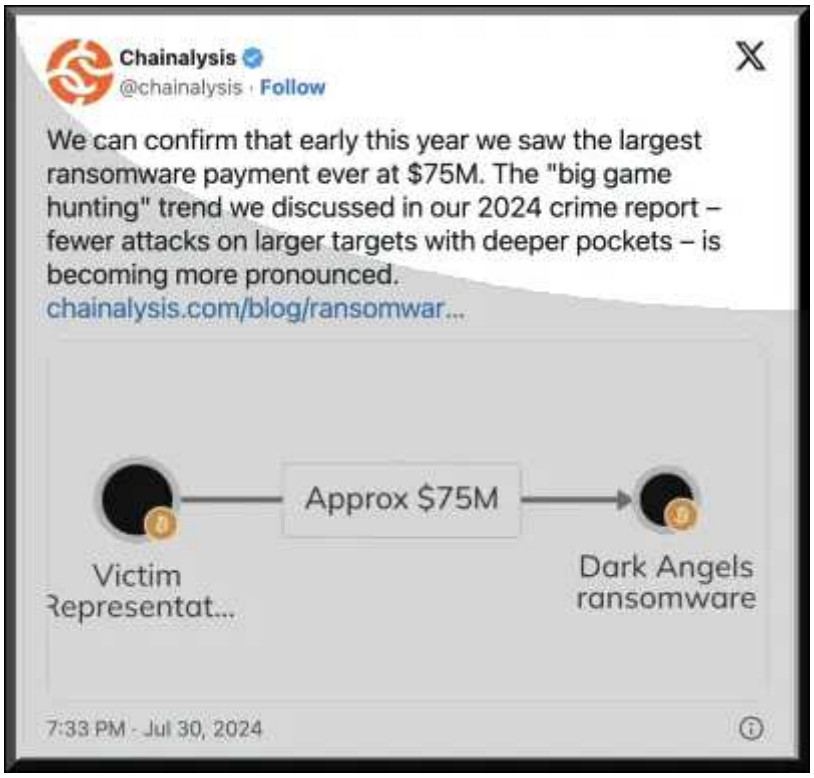
Emlékezhetünk például, hogy **2020-ban, amikor a CWT Business Travel Management Company utazási társaságot érte ransomware támadás**, melynek során 30 ezer számítógép állományait lopták és kódolták el, megsemmisítve és egyúttal megszerezve mintegy 2 TB bizalmas céges adatot, a vállalat végül 4.5 millió USD (akkori árfolyamon nagyjából 1.3 milliárd forintnyi összeget) fizetett ki a bűnözőknek.



Bár ez nem egy olimpiai szám, a mostani világbajnok méretű váltságdíjfizetés beelőzte a korábbi CNA nevű amerikai biztosítótársaság

által 2021-ben kifizetett 40 millió dollárnak megfelelő rekordösszeget az orosz eredetűnek tartott Phoenix csoportnak.

Mostantól az új csúcs 75 millió dollár értékű kriptovaluta, amelyet egy meg nem nevezett Fortune 50-es listán szereplő cég fizetett ki, miután ransomware támadást szenvedett. Hangsúlyozzuk, **ez nem a követelés, vagy a kezdeti alkuk előtti követelés mértéke, hanem egy valóban megmozgatott, átutalt pénzmennyiség.**



A mostani zsaroló akcióban az áldozat kilétét ugyan homály fedi, de az elkövető viszont ismert, **a Dark Angels elnevezésű, kevésbé közismert doxingban utazó banda volt. Több jelentős incidens köthető a nevükhöz, például a tavaly őszi Johnson Control eset, ahol 51 millió dollárt követeltek 27 TB ellopott és titkosított céges adatért, amelyeket a vállalat VMWare ESXi virtuális gépeiről sikerült megszerezniük.**

Vagy említhetjük a 2024. áprilisi Nexperia chipgyártó elleni támadást is, ahol 1 TB bizalmas adatot sikerült ellopniuk.

A Zscaler szakértői szerint a Dark Angels esetében egyre gyakoribb, hogy **ellentétben más csoportok taktikájával ők a Big Hunting Game jegyében célzottan mindig egyetlen nagy értékű céget támadnak meg a hatalmas ellopható adat és a jelentős váltságdíj reményében.**

Elképzelhető, hogy ezzel viszont előbb-utóbb követendő példát mutatnak majd a versenytársaiknak.

Szólj hozzá!
Címkék: oroszország pénz dark rekord bevétel angels zsarolás váltságdíj ransomware zsarolóvírus

Ajánlott bejegyzések:

A kriptobevételek felett az égbolt felhőtlen
Újabb rombolás brit kórházakban


A kriptobevételek felett az égbolt felhőtlen
Újabb rombolás brit kórházakban
A ransomware az egészségügyben élet-halál kérdése
Kincs, ami van
Windows frissítés vagy mégsem?
A ransomware az egészségügyben élet-halál kérdése

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkereső csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Vérszagra gyűl a ransomware

2024. augusztus 05. 13:15 - Csizmazia Darab István [Rambo]

Minden terület, szektor, intézmény típus volt már támadva a korábbiakban is: **kórházak, erőművek, bankok, utazási irodák, ügyvédi irodák, rendőrség, olajvezeték, húsfeldolgozó, mezőgazdasági gépgyár, chipgyártó, egészségbiztosító, és még hosszasan lehetne sorolni. Ezúttal egy non-profit vérellátási központ vált áldozattá.**

Július 29-én érte zsarolóvírus támadás a OneBlood vérközpontot, amelynél a számítógépes rendszerek leállása után már csak manuálisan tudták folytatni a vér gyűjtést, a minták tesztelését, feldolgozását valamint ezek szűkített elosztását az Egyesült Államok délkeleti részének több mint 250 kórházába. A működés a nehézségek ellenére is folyamatos, zajlanak a véradások, a vér címkézése és a vérszállítmányok koordinálása.

A szervezet nyilatkozata szerint külsős kiberbiztonsági szakemberekkel és kormányzati ügynökségekkel együttműködve folyamatosan vizsgálják az informatikai behatolást és annak lehetséges következményeit.

Az egyelőre **rákérdezés után sem derült ki, hogy a támadók hogyan jutottak be a számítógépes rendszerbe, pontosan milyen fajta ransomware okozta a leállást, mennyi váltságdíjat követelnek, valamint hogy adatlopás is történt-e az incidens folyamán.**

Konkrét megjelölés sem szerepelt az informatikai rendszer helyreállításának határidejével kapcsolatosan, bár az időközben megjelent **augusztus 4-i hivatalos közleményükben időközben már részlegesen helyreállított állapotról számoltak be**, így például többek közt a donorok elektronikus regisztrációja is már újra működőképes.

Ha bebizonyosodik, hogy adatlopás is történt, úgy általuk kezelt kiemelten érzékeny személyes adatok kerülhettek veszélybe. A hatóságok és biztonsági kutatók egyaránt arra figyelmeztetnek, hogy az ehhez hasonló kritikus területeket érintő ransomware támadások **sajnos egyre gyakoribbak, az egészségügyi intézmények pedig kiemelt veszélyben vannak.**

Például nemrégiben egy brit kibertámadás kapcsán kimerültek a nullás csoportú vérkészletek, ami rendkívüli vészhelyzetet idézett elő.

Szólj hozzá!
Címkék: leállás nonprofit vér központ véradás váltságdíj ransomware zsarolóvírus

Ajánlott bejegyzések:

Újabb rombolás brit kórházakban

A ransomware az egészségügyben élet-halál kérdése

100 millió ember egészségügyi adata hoppszi

Újabb rombolás brit kórházakban

Az elveszett levelezés

A ransomware az egészségügyben élet-halál kérdése

100 millió ember egészségügyi adata hoppszi

Ransomware a Volkswagennél

Ransomware a Volkswagennél

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

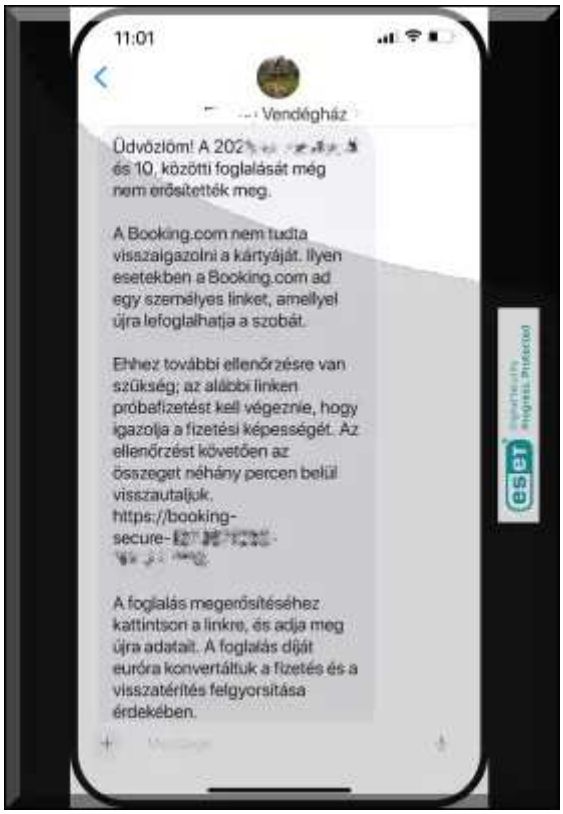
Booking com átverések

2024. augusztus 08. 16:56 - Csizmazia Darab István [Rambo]

A Booking.com a szálláshelyeket kereső utazók egyik legfontosabb platformja, de mára olyan kényelmi szolgáltatások, mint az autóbérlés és a repülőjegy vásárlás is elérhetővé váltak az oldalon keresztül. Ez a világ leglátogatottabb utazási és turisztikai honlapja, amely 2023-ban több mint egymilliárd foglalást bonyolított le, ami kétszerese a 2016-ban regisztrált számnak.

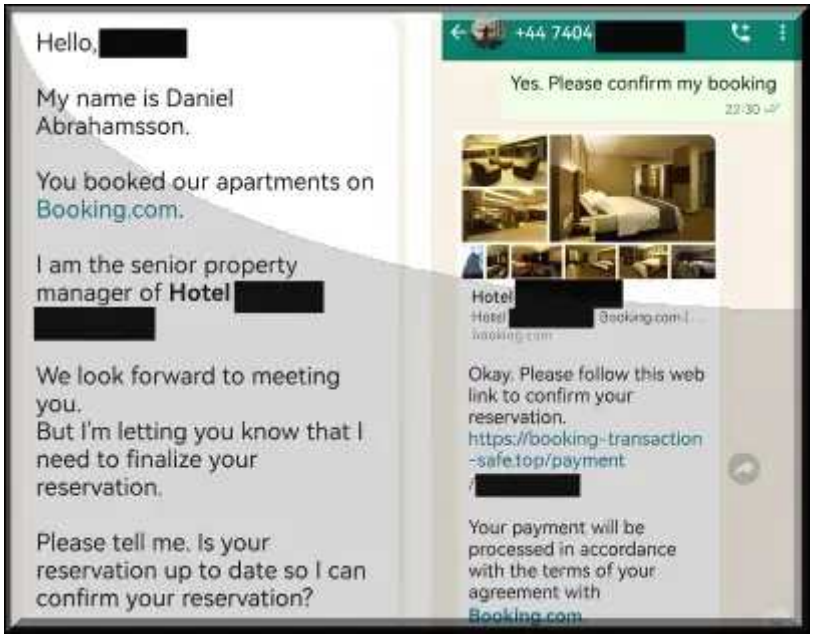
A népszerű weboldal nem kerülte el **a kiberbűnözők figyelmét sem, akik mindig nagy forgalmú online szolgáltatásokat keresnek, hogy célba vegyék áldozataikat**. Amíg mi a megérdemelt nyaralásunkat tervezzük, a csalók eközben is vadásznak ránk adathalász e-mailekkel, hamis hirdetésekkel.

Maga a Booking.com is elismerte a probléma jelentőségét, és megerősítette, hogy az elmúlt 18 hónapban 500-900 százalékos növekedést tapasztaltak az utazási csalások tekintetében. Ezt a növekedést részben az is okozza, hogy a kiberbűnözők 2022. novembere óta már a ChatGPT szolgáltatást is aktívan kihasználják.



Szakértők szerint így a nyaralási szezon közepén érdemes áttekinteni néhányat a Booking.com-ot érintő leggyakoribb csalások közül, és megnézni, **mire kell figyelnünk, ha ezt a platformot használjuk, hogy a nyaralással, szállásfoglalással kapcsolatos csalásokat elkerülhessük.**

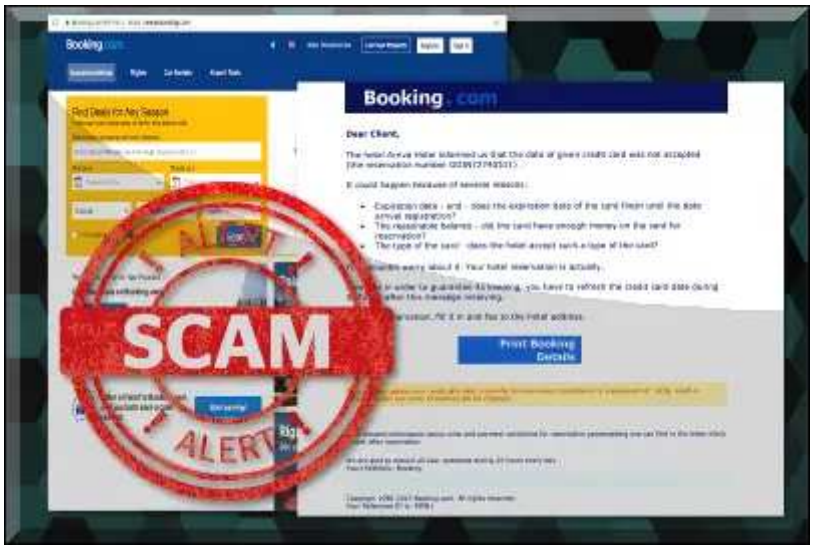
A Hackfelmetszők – Veled is megtörténhet! kiberbiztonsági podcast legújabb, 21-ik adásában is ezt a témát járt körül.



Adathalászat
Az adathalász e-mailek, szöveges üzenetek és a közösségi médián keresztül érkező tartalmak a csalók eszköztárának alapvető elemei. Az ilyen átverések során magukat egy jó hírű platformnak vagy vállalatnak kiadva elhitetik az

áldozatokkal, hogy az adott oldal, szervezet hivatalos képviselőjével kerültek kapcsolatba. Gyakran állnak elő olyan hihető történetekkel, amelyekben egy ártalmatlannak tűnő, ámde **rosszindulatú linken keresztül történő fizetésre, pótbefizetésre vagy az adatok állítólagos ellenőrzésére, módosítására szólítják fel az áldozatot, ellenkező esetben a foglalás törlését is kilátásba helyezik.**

A generatív mesterséges intelligencia eszközök elterjedésével egyre meggyőzőbb és hatékonyabb átverések születnek. A nyelvtanilag helyes, kontextushoz illő és a tipikus figyelmeztető jelektől mentes adathalász e-mailekkel könnyen rávehetik az embereket és a vállalkozásokat, hogy adattolvaj kártevőket töltsenek le az eszközeikre, érzékeny információkat osszanak meg velük, illetve pénzt utaljanak át.



Eltérített csevegések
Több beszámoló is készült olyan esetekről, amikor a támadók a Booking.com platform üzenetküldő rendszerén keresztül próbálták meg becsapni az áldozatokat. Miután bejutottak azon szálláshelyek fiókjaiba, ahol a vendégek a valóságban is foglaltak, az alkalmazásban működő chaten keresztül rengeteg emberrel közvetlenül felvették a kapcsolatot, és felszólították őket, hogy fizessenek a foglalás megerősítése érdekében. **A csel szerint egy állítólagos hiba történt az előző tranzakciónál, ami miatt ismét fizetniük kell az áldozatoknak, hogy ne maradjanak le a nyaralásról. Az átverés más változataiban a csalók hitelkártya- vagy személyes adatokat kértek a foglalás ellenőrzéséhez vagy megerősítéséhez.**

Habár mindez nem közvetlenül a booking.com weboldal feltörése miatt, hanem szállodák, partnercégek adminisztrációs rendszereinek a megsértése miatt következhetett be, érdemes odafigyelnünk minden olyan üzenetre, amelyben személyes vagy fizetési adatokat kérnek tőlünk.

Nem létező szálláshelyek
Sok nyaralóhely néz ki úgy a képeken, mint egy hihetetlen tündérmese. **Néhány közülük a szó szoros értelmében valóban kitalált. Az évek során sok nyaraló esett áldozatul hamis hirdetéseknek, amelyekben a kiberbűnözők ellenállhatatlan áron bérelhető luxusnyaralót reklámoznak**, és arra biztatják az embereket, hogy fizessenek, akár a Booking.com-on keresztül. Érkezéskor aztán kiderül, hogy a szálláshely nem létezik, vagy az ingatlan nem is kiadó. A platform saját rendszerei ugyan viszonylag gyorsan azonosítják és eltávolítják a hamis hirdetéseket, még de így is bele lehet esni ebbe a csapdába, emiatt jobb, ha a foglalás előtt alaposan tájékozódunk.

Keressünk véleményeket és értékeléseket az adott helyről, nézzük meg, hogy az ár nagyjából megegyezik-e a hasonló színvonalú házak vagy lakások áraival, és **keressünk rá külön a képekre is, a csalók ugyanis gyakran használnak ingyenes stock képeket vagy más webhelyről lopott fotókat**. Általánosságban igaz, hogy ha valami túlságosan szépnek tűnik ahhoz, hogy igaz legyen, akkor érdemes gyanakodni.

Hamis állásajánlatok
Az SMS-ben vagy a közösségi médiában kapott üzenet meglehetősen egyszerű: "Szükségünk van valakire, aki értékeli a szállást. 200 és 1000 dollár közötti összeget fizetünk. Mindössze annyit kell tenned, hogy értékeled vagy kedveled a szálláshelyeket a Booking.com-on". Így kezdődik a vonzó kiegészítő keresetet kínáló szöveg a platform nevével visszaélve. **Ez a módszer egyike a népszerű csalásoknak, amelyben otthonról végezhető munkát ajánlanak.**

Ezután előrefizetéssel úgynevezett megállapodási díjat kérhetnek a munkakezdés előtt és/vagy személyes adatokra tarthatnak igényt, például társadalombiztosítási számra, ami felhasználható személyazonosság lopásra. Bizonyos esetekben a támadók bitcoin vagy más kriptovaluta-tárca adatainkra pályáznak.

Hogyan maradhatunk biztonságban? A Booking.com nem alkalmaz embereket szálláshelyek véleményezésére és nem vesznek fel munkaerőt kéretlen szöveges üzeneteken keresztül. A hivatalos toborzás a Booking Careers-en keresztül történik, és a platformon nem találni olyan állásajánlatot, amely magába foglalja a szállodák értékelését. **Következzen hát 12 tanács az ESET szakértőitől a Booking.com-ot érintő és más utazási csalások elkerüléséhez.**

1. Amikor olyan személy lép velünk kapcsolatba, aki a Booking.com-ot vagy olyan hotelt képvisel, ahol szállást foglaltunk, **figyeljünk az adathalász e-mailek tipikus ismertetőjegyeire, mint például a sürgetés, fenyegetés.**

2. **Mindig ellenőrizzük, hogy az e-mailek a hivatalos domainről érkeztek-e**, és figyeljünk az apró helyesírási hibákra vagy eltérésekre. A megbízható platformokon jellemzően számos hivatalos e-mail címet is találunk.
https://partner.booking.com/en-us/help/legal-security/security/online-security-awareness-phishing-and-email-spoofing

3. **Ha bármilyen gyanús üzenetet kapunk, menjünk közvetlenül a weboldalra**, és jelentkezzünk be a fiókunkba, hogy ott ellenőrizzük az állításokat.

4. **A Booking.com soha nem kér e-mailben vagy chaten keresztül olyan információkat**, mint a részletes hitelkártyaadatok, személyes adatok vagy jelszavak.

5. **Ne kattintsunk rá a kéretlen e-mailekben vagy üzenetekben található linkekre, csatolmányokra.**

6. **Fizessünk a Booking.com hivatalos platformján**, és kerüljük a közvetlen utalást a szállásadóknak.

7. **Ellenőrizzük a szállás értékeléseit a Booking.com-om és keressünk hiteles és részletes véleményeket.** Keressünk rá a szállás adataira és képeire más utazási weboldalakon vagy értékelő platformokon.

8. Győződjünk meg róla, hogy **eszközeink naprakész biztonsági szoftverrel rendelkeznek** a kártékony programok és az adathalász kísérletek elleni védelem érdekében.

9. **Tartsuk naprakészen az operációs rendszereinket és más szoftvereket,** hogy védve legyünk a biztonsági sebezhetőségek ellen.

10. **Védjük fiókjainkat erős és egyedi jelszavakkal vagy jelszókulcsokkal, valamint kétfaktoros hitelesítéssel.**

11. Amennyiben bármilyen **gyanús tevékenységet tapasztalunk, jelentsük a problémát a platform ügyfélszolgálatának.**

12. **Ha felmerül a fizetési adatokkal való visszaélés gyanúja, azonnal értesítsük bankunkat vagy hitelkártya-szolgáltatónkat.**

Szólj hozzá!
Címkék: utazás nyár nyaralás csalás átverés megelőzés eset védekezés welivesecurity.com booking.com

Ajánlott bejegyzések:

[10 tipikusan időseket célzó csalás](#)

[Csomagja érke... Na most már elég!](#)

[10 tipikusan időseket célzó csalás](#)

[Black Friday és Cyber Monday járja be Európát](#)

[Adathalászat menni booking.com](#)

[Csomagja érke... Na most már elég!](#)

[Fontos vagy nekem](#)

[Fontos vagy nekem](#)

[Fontos vagy nekem](#)

[Fontos vagy nekem](#)

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Gáz van, sikertelen fizetés rossz adatokkal

2024. augusztus 13. 14:30 - Csizmazia Darab István [Rambo]

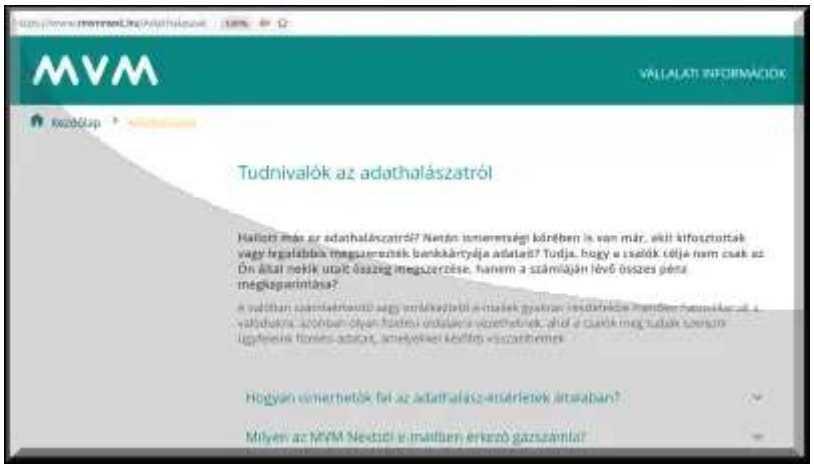
Bár a fűtési szezon még jóval odébb van, azért a közművek számlái addig is rendszeresen érkeznek, köztük a földgáz is. Vagy mégsem? **A kényelmes kiegyenlítést jobb ha nem választjuk a csaló e-mailek esetében.**

Nincs uborkaszezon, mindig érkezik valamilyen átverési kísérlet, **a legutóbbi az MVM nevében egy gázszámla. Bár a feladók igyekeztek a levél kinézetét csinosítgatni,** azért maradtak benne szembeötlő furcsaságok jócskán.

Kezdve azzal, hogy az ékezethibásan írt magyarországi "MVM Aramszolgáltató Zrt." **miért írna nekünk egy ilyen e-mailcímről: "mvmadministraion KUKAC etu PONT univ-smb PONT fr"? Ez ugyanis a francia Université Savoie Mont Blanc Egyetemhez tartozik.**

Az e-mail trace is mutatja, bizony **Franciaországból kaptuk a fizetésre buzdító üzenetet.**

Ami képileg azért próbálja a hivatalosság látszatát sugározni, a "Befizetem bankkártyával" link kivételével minden más hivatkozás szépen a hivatalos MVM weboldalra irányít bennünket: legfontosabb információk az energia-számlákról, Gyakori kérdések oldalunk, számlamagyarázat, **de még pofátlanul az adathalászatra való figyelmeztetés linkjét is mellékelték: Bővebb tájékoztatás: www.mvmnext.hu/Adathalaszat.**



Ám maga a fizetési link persze nem az MVM felé irányít, hanem egy .ZA domain végződésű dél-afrikai URL a cím a végállomás, amit még 2006-ban regisztráltak, de most 2024. júniusában frissítették. A konkrét phishing link a kora reggeli időpont ellenére már le lett kapcsolva, és a hamis banki oldalt ekkor már nem is lehetett elérni.

Hogy miért .ZA a Dél-Afrika, az is egy alapvetően érdekes kérdés, az .SA már foglalt volt Saud Arábiának, Zambia pedig a .ZM alatt tanyázik, [így ez a .ZA egy áthidaló megoldás keretében jött létre](#).

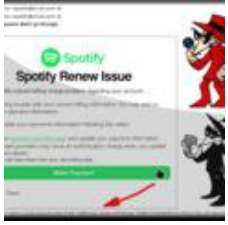
Ami kicsi tanulság ennek kapcsán elmondható, hogy a 30 fokos hőségben sem szabad kapkodni a számlafizetésnek látszó tárgyakkal, legyen szó bármilyen szabad szemmel alig látható csekély összegről is.

Párduc, oroszlán, gorilla, makákó - és gázszámla: [ez utóbbi egészen eddig hiányzott a KFT együttes daláből](#), de most végre valahára ez is pótolva lett...

[1 komment](#)
Címkék: [vagy](#) [csalás](#) [átverés](#) [mvm](#) [adathalászat](#) [mégsem](#) [gázszámla](#) [vagymégsem](#) [közművek](#)

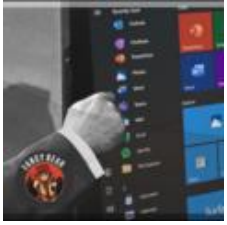
Ajánlott bejegyzések:

Új bejelentkezés a felhőnkbe. Vagy mégsem?



Spotify megújítási probléma - vagy mégsem?

Új földgáz számlája készült - vagy mégsem?



Windows update vagy mégsem? Adathalászat vagy jófogás?

Új bejelentkezés a felhőnkbe. Vagy mégsem?

Adathalászat vagy jófogás?

Adathalászat vagy jófogás?

Adathalászat vagy jófogás?

Kommentek:

Androsz · **http://wikipedia.blog.hu/ 2024.08.14. 17:21:50**

A .ZA domain magyarázata, hogy az ország holland gyarmat volt, a fő hivatalos nyelve, az afrikaans is egy holland keveréknyelv, és hollandul Zuid-Africa a Dél-Afrika.

Mivel a csaló egy egyetemről levelez, meg lehetne nézetni a rendőrség útján, hogy kié ez a cím, és lehetne küldeni a pofont. Egyetemi szerverről nem szokott akárki e-mailezgetni.

Válasz erre

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Üdvözöl a bölcs csapat

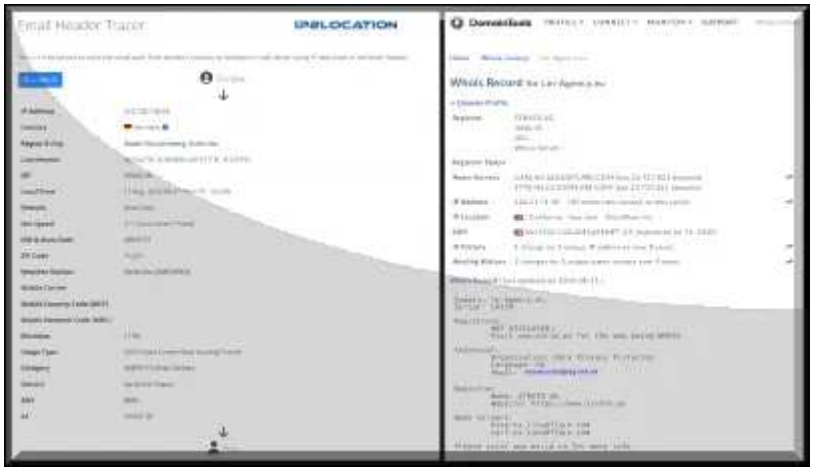
2024. augusztus 16. 14:46 - Csizmazia Darab István [Rambo]

Nincs uborkaszezon a csalások területén, **ezúttal a Wise banki bejelentkezéssel kapcsolatban érkezett csaló próbálkozás**, miszerint állítólag illetéktelen belépést érzékelt a rendszer, ideje belépni a mellékelt linken.

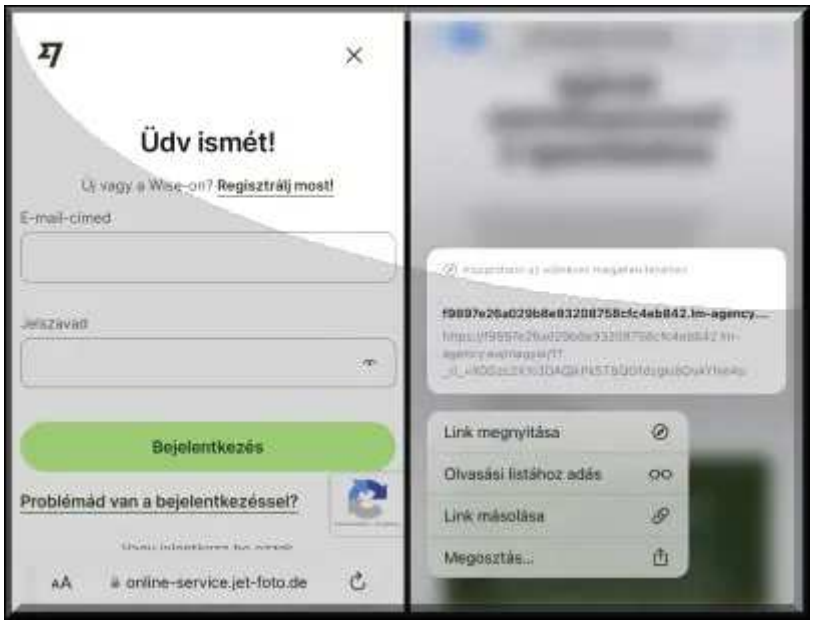
Nem igazán hallott még a ChatGPT-ről vagy a szakmai lektor elnevezésű szakmáról, aki ezt az e-mailt küldte. **Überprimitívség ugyanis annyira megbízni egy hagyományos nyersfordító képességeiben**, hogy mindent változatlanul hagyjon egy olyan szövegváltozatban, ahol minden egyes szót tükörfordít az alkalmazás (lásd még zöld-borsó=green-wein-salt).

Így került vicces módon ezúttal "a Wise csapata" helyett "a bölcs csapat" szófordulat az üzenet aláírásába.

A feladó "kontakt KUKAC allfacebook PONT de", ami **nem éppen a hivatalos wise.com címének látszik**. Az e-mail trace eredménye szerint **Karlsruhe környékéről jött a levél, amelyben a magázás és a tegezés összemixelésében is sikerült megugrani a lécet az amatőr Fülig Jimmy imitátornak.**



"*Észrevettük, hogy fiókjába új bejelentkezést használtunk egy olyan országból, ahonnan mostanában nem jelentkezett be. Tehát meg akartunk győződni arról, hogy te vagy az.*" Na és mit javasol ilyenkor a "bölcs csapat"? **Naná, hogy gálánsan mellékel egy linket, amire kattintva állítólag beléphetünk a fiókunkba.**



Intő jeleknek itt sem vagyunk híján, a wise.com hivatalos weboldala helyett ugyanis az "lm-agency PONT eu PER magyar" címre irányít át mellékelt link. Bár azonnal rástartoltunk a kattintásra, az adathalász oldalnak addigra már se híre, se hamva nem volt, persze jól van ez így, nagyon helyesen gyorsan léptek az illetékesek.

Szerencsére a Makay.net korábban sikeresen közölt képeket a hamis bejelentkezési oldalról, ezeket ezúton is köszönjük. **Érdemes tehát ebben a pokoli hőségben is odafigyelni a kéretlen üzenetekre, és észnél lenni az adathalász támadási kísérleteknél.**

Szólj hozzá!
Címkék: spam bank email csalás átverés wise adathalászat

Ajánlott bejegyzések:

Utolsó emlékeztető a fiók felfüggesztése előtt
Ment a hűtlen hamis linkkel
MBH-fiókjának jelszava 24 órán belül lejár
Leveringa függesztés csomag részére

Utolsó emlékeztető a fiók
Ment a hűtlen hamis linkkel
MBH-fiókjának jelszava 24
Leveringa függesztés csomag részére

felfüggesztése előtt

órán belül lejár

MBH banki adathalászat

MBH banki adathalászat

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

Személyiséglopás nem középiskolás fokon

2024. augusztus 22. 14:27 - Csizmazia Darab István [Rambo]

Sokszor beszéltünk már az ellopott egészségügyi adatokkal kapcsolatban, miért értékesebbek ezek akár a banki adatoknál is. **Elrettentő példaként olyanokat láthattunk, hogy valakinek az ellopott társadalombiztosítási adataival visszaélve szívműtéteket számoltak el**, nagy értékű mozgássérült robogót vásároltak a nevében, illetve több drága orvosi felszerelést is, ezekkel pedig több tízezer dollárnyi tartozást halmoztak fel a vétlen áldozatnak.

Aki csak akkor szembesült mindezzel, amikor a végrehajtók kopogtattak az ajtaján. Mostanában pedig arról lehet olvasni, hogy az ellopott banki adatokkal nem csak kiürítik a pórul járt felhasználó számláját, hanem a nevében hiteleket is felvesznek, ami tetézi a bajt, és az elszenvedett kárt. Hogy milyen problémákat tud okozni egy személyiségtolvaj, arról pedig mozifilm is készült 2013-ban Identity Thief címmel.

Mai történetünk még kacifántosabb esetet mutat be, ennél az elkövető 2023. januárjában egy másik amerikai államban élő orvos felhasználónevével és jelszavával élt vissza. Az alaphelyzet az volt, hogy csalással igyekezett kibújni a gyerektartási kötelezettsége alól, és ehhez számára akkor és ott jó ötletnek tűnt az orvosfelhasználó nevében belépni a Hawaii Halálozási Nyilvántartási Rendszerbe, ahol egy új ügyiratot nyitva saját magát halottnak nyilváníttatta.

Ehhez kitöltött egy halotti anyakönyvi kivonatot, kijelölte saját magát illetékesnek, és az orvos digitális aláírásával igazolta is a halál tényét.

Bár lelepleződése után Jesse Kipf úgy nyilatkozott, **bár eredetileg ez volt cselekményének a fő indítéka, ám a továbbiakban sem állt le csalárd manipulációkkal. Észlelte ugyanis, hogy egy nagyon értékes accountot sikerült megszereznie, amivel különféle magánvállalati hálózatokhoz és az USA kormányzati rendszereihez is hozzáfért, ezért azt eladásra kínálta a darkweben.**

Emellett hamis társadalombiztosítási számokkal hitelszámlát is igényelt egy pénzintézetnél. Végül az FBI nyomozása buktatta le, ahol az összesített károsszeget nagyjából 200 ezer dollárra (hozzávetőlegesen 70 millió forintra) becsülték.

Még 2023. novemberben emeltek vádat Kipf ellen öt rendbeli számítógépes csalás és három rendbeli személyazonosság-lopás miatt, ennek nyomán pedig [a mostani ítélet alapján 69 hónap (5.5 év) letöltendő börtönbüntetésre ítélték a férfit](), szabadulása után pedig plusz három év bűnügyi felügyelet fog rá várni.

Szólj hozzá!
Címkék: ítélet csalás account identity lopott visszaélés theft hozzáférés gyerektartás személyiséglopás darkweb

Ajánlott bejegyzések:

Magyar Posta elvágta, indiai gyógyítja

Replikák támadása

A legnépszerűbb 2024-es posztok

CAPTCHA, amely nem az ember-gép relációt teszteli

Magyar Posta elvágta, indiai gyógyítja

Replikák támadása

A legnépszerűbb 2024-es posztok

CAPTCHA, amely nem az ember-gép relációt teszteli

Adathalászat
vagy jófogás?

Adathalászat
vagy jófogás?

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

Hergelés vagy biztonságtudatossági teszt?

2024. augusztus 27. 12:49 - Csizmazia Darab István [Rambo]

Ahhoz, hogy nagyobb eséllyel dőljön be a megtévesztésnek az áldozat egy-egy éles **adathalász támadáskor, egyre többet számít a testre szabott tematika és a célba vett személyre vagy csoportra hangolt kifinomult csali.** Ezt megtapasztalhatta például a New York Times szerkesztősége, amikor 2012-ben kínai hackerek törtek be hozzájuk.

Az akkori történet lényege, hogy cikksorozatban vesézték ki a kínai politikai elit gazdagodását, és ez nem igazán tetszett a kínai vezetésnek. **Miután a kínaiak hivatalos utakon sikertelenül próbálták letiltani a megjelenést, egy rejtett kémprogrammal próbálták meg kipuhatolni a szivárogtatások eredeti forrását.**

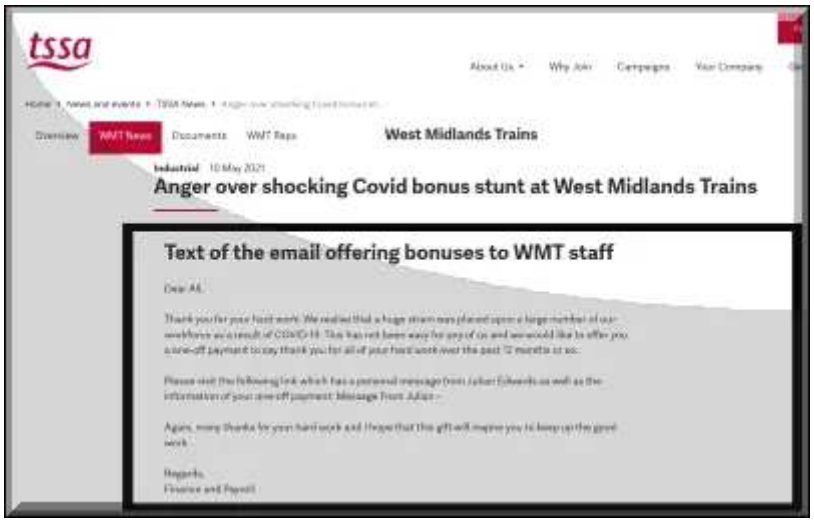
Ehhez egy olyan csali emailt küldtek, amire biztosan számíthattak egy-két kattintásra a NYT részéről. Ez pedig **egy dropboxos linkben érkező közgazdasági szakmai anyagnak látszó PDF állomány volt, amely látszólag az ASEAN (Délkelet-ázsiai Nemzetek Szövetsége) és USA kereskedelmi egyezmény tervezetének szövege. A történet másik szomorú aspektusa, hogy a kémkdést 4 hónapig észre sem vették.**

Adathalászattal egyébként szinte mindenkit be lehet csapni. Például kiemelt újsághír lett, amikor **2009-ben maga Steve Jobs ment lépre egy hamis Amazon áruházas weblapon, és ott ellopták a belépési adatait.**

Egy 2021-es kutatás adatai azt mutatják, hogy a vállalkozások 80%-a egyáltalán nem teszteli a dolgozók biztonságtudatossági képességeit, remélhetőleg ez az arány azóta javult. A szimulált támadásoknál a cégek saját dolgozóik éberségét teszik próbára, és **ehhez gyakran alkalmaznak olyan kíváncsiságot felkeltő témákat, ami sokakat megtéveszthet.**

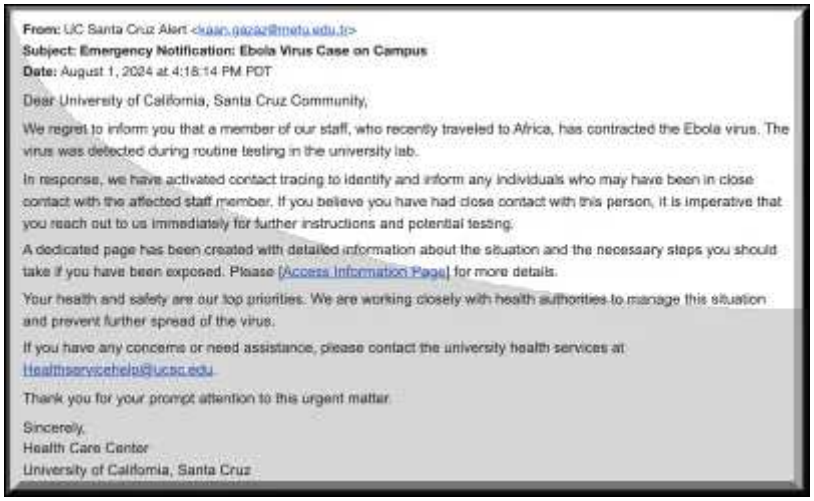
Ezek közül volt több emlékezetes is, például **az egyik 2020. decemberében a GoDaddy domain kezelő cégnél történt, ahol olyan e-mailt küldtek körbe, amelyben 650 dolláros üdülési bónuszt ígértek az alkalmazottaknak. Amire aztán jöttek is a kattintások.**

Ezt bár vehetik rossz néven, de minden ilyen teszt célja, hogy **felhívja a figyelmet a vállalatokat sújtó egyre gyakoribb adatsértésekre, incidensekre és felkészítse a dolgozókat gyanakvóbb, biztonságtudatosabb** hozzáállásra.



A 2021-ben a West Midlands Trains vasúttársaságnál történtek is bekerültek a hírekbe, ahol az e-mail üzenetet látszólag a WMT pénzügyi és bérszámfejtési osztályáról küldték. **Ebben azt írták 2500 munkatársnak, hogy a Covid megpróbáltatásai miatt egyszeri pénzjutalmat ajánlanak fel számukra, hogy ezzel köszönetet mondhassanak az elmúlt 12 hónapban végzett kemény munkájukért.**

A levél végén arra kérték őket, hogy kattintsanak a mellékelt Microsoft Office 365 linkre, amely állítólag a WMT ügyvezető igazgatójának, Julian Edwardsnak a személyes üzenetéhez vezet.



És akkor jöjjön a mostani friss eset, amelyben a Kaliforniai Santa Cruz Egyetem (UCSC) hallgatói kaptak olyan figyelmeztető e-mailt, hogy a campuson az egyik dolgozó ebola-vírussal fertőződött meg. "*Sajnálattal értesítjük, hogy egyik munkatársunknak, aki nemrég tért vissza Dél-Afrikából, pozitív lett az Ebola-vírus tesztje.*" **Az üzenetben arra kérték a címzetteket, hogy további részletekért jelentkezzenek be a helyi információs oldalra.**

Bár itt is előfordult felháborodás, azt viszont **biztosan pozitívumként könyvelhetjük el, ha valahol a munkatársak számára rendszeresen tartanak kiberbiztonsági képzéseket és időszakonként szimulált adathalász kampányokkal ellenőrzik is a figyelmet és a tudást.**

[Szólj hozzá!](#)
Címkék: [teszt](#) [cég](#) [szervezet](#) [támadás](#) [vállalat](#) [adathalászat](#) [biztonságtudatosság](#) [szimulált](#)

Ajánlott bejegyzések:

[Csalás jönni TikTokra](#)

[Apukánk világa](#)

[Adathalászat vagy jófogás?](#)

[Adathalászat vagy jófogás?](#)

[Zsarolóvírus a szívsebészeti orvosi eszközöket gyártónál](#)

[Zsarolóvírus a szívsebészeti orvosi eszközöket gyártónál](#)

[Újabb rombolás brit kórházakban](#)

[Újabb rombolás brit kórházakban](#)

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Élősködők

2024. augusztus 30. 16:10 - Csizmazia Darab István [Rambo]

Mai világunkban, ahol szinte minden hivatalos és magán ügyünket, vásárlásainkat, kapcsolattartásainkat online intézzük, **számtalan támadás, átverési kísérlet érkezik közösségi üzenetben, SMS-ben, emiatt fontos, hogy mindenki tisztában legyen ezekkel a kockázatokkal. Egy csokor magyar nyelvű csaló üzenet következik.**

Álláshirdetés SMS-ben, amelyben akár 80 ezer forintot is kereshetünk otthonról, a mobiltelefonunk segítségével, na persze. **Az üzenet a +63 alapján a Fülöp-szigetekről érkezett**, a mellékelt URL pedig egy WhatsApp rövidített link hivatkozás. 20 munkanappal az már havi 1.6 milla, ugye kicsit sem hihetetlen.

Sajnos azt írják, csak a 25 és 55 közöttieknek szól, így a fiatalabbak és ennél idősebbek most nem végezhetnek ilyen egyszerű és nagyszerű munkát.

Catherine Mara is ajánl nekünk munkát, **elmondása szerint a brit HR osztályról. Ehhez képest a +91 előhívó szám indiai, itt már napi 10-20 perc részmunka is elegendő, a napi kereset pedig akár 100 ezer forint.**

Már ez is két milliós ígéret havonta, de ha még mondjuk túlóráznánk is, a határ a csillagos ég. Nem is érteni, miért nem itt dolgozik mindenki. A sziás tegezés és a magázás váltakozása itt sem egy bizalomkeltő jel.

Ez már egy legitimnek látszó magyarországi számról érkezett, rövid, lényegre törő, csak semmi cicó: **"bírság a nevedre, fizess 24 órán belül".**

Hogy melyik hatóság, milyen címen követel bírságot, az persze nem derül ki a frissiben regisztrált, kicsit sem hivatalos weboldal esetében. És legalább köszönt volna előtte, hogy szia uram, vagy valami.

Hurrá, egy hónapig ingyen utazhatunk - tájékoztat a hirdetés.

Kár hogy sajnos nem igazi az akció, az egyáltalán nem BKK-snak tűnő territorymod.com weboldal pedig jelenleg lekapcsolt állapotban van, és **ezt**

[is idén regisztrálta be valaki](#).

A BKK 14-ik szülinapja alkalmából kínálnak egy állítólag 6 hónapig érvényes bérletet mindössze 950 jó magyar forintért.

Sietni is kell, hiszen az akció mindössze csak 7 napig érvényes, és csak az első 500 vásárló lesz szerencsés. Vagy mégsem? **[Na és miért mutat a link a BKK helyett a grawenubmer PONT com oldalra?](#)** Ez is egy nagyon jó kérdés.

Ki ne akarna egy vadonatúj Samsung mobiltelefon mindössze 749 forintos vételáron? Az EMAG nevével visszaélve kínálják az akciót a csalók a Facebook/Meta oldalain.

Céljuk a személyes és banki adatok begyűjtése, adathalászat, és persze a sokszor 749 forint is bűnözőknél landol, akik nyilván már hallottak a sűrű fillért idéző mondásról.

A következő három képernyőkép egyazon az átverési módszerrel operál. **Az Index hírportál arculati elemeivel visszaélve valamilyen kattintásvadász címmel felkelti az érdeklődést, és egy kriptovalutás csalásra igyekszik rábeszélni a felhasználókat.**

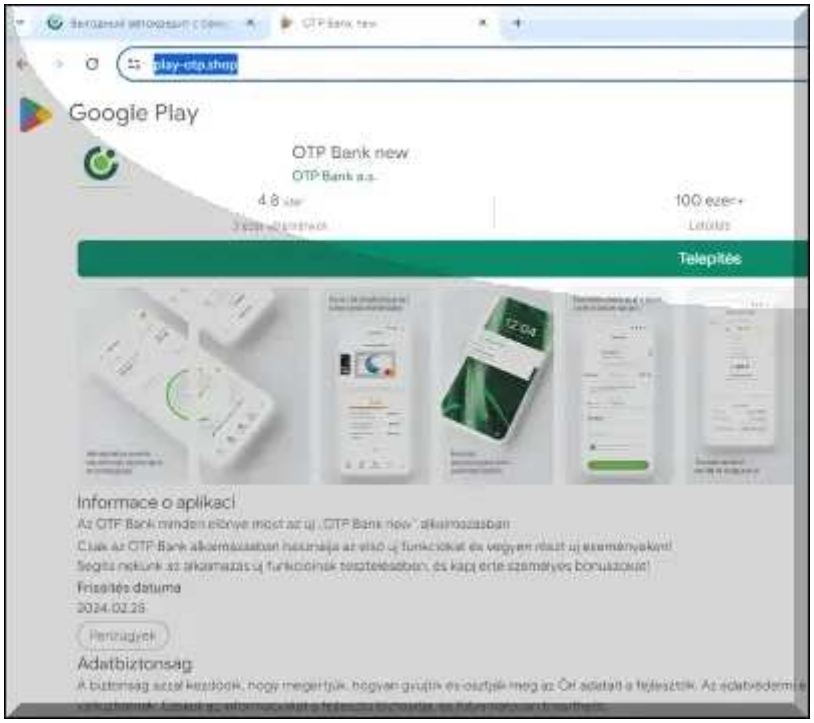
Állítólag a mesterséges intelligencia dolgozik helyettünk, befekteti kriptopénzt, itt még csak 10-20 percet sem kell dolgozni, minden magától működik. Vagy mégsem. Ugyanis ez is nagy csalás. **Természetesen Istenes Bencének, Gundel Takács Gábornak és Vámos Miklósnak semmi a köze a dologhoz, a csalók csúnyán visszaéltek a nevükkel.**

Akinek van Netflix előfizetése, meglepődhet egy olyan SMS érkezésén, ami arról tájékoztatja, hogy azt sajnos felfüggesztették. És akinek nincs előfizetése, és mégis kap ilyet?

Itt szerencsére az is jól látszik, hogy az ESET Mobile Security **blokkolja a próbálkozást, amely mellesleg egy németországi számról érkezett. A renewflix-registre.com is egy idén májusban bejegyzett domén, és hát ez trükk itt most nem jött be.**

A bankok ügyfeleit célozza egy vadonatúj technika, amely azon alapul, hogy a böngészőből is kezdőképernyőre helyezhető egy indító ikonnal egy tetszőleges hivatkozás. A progresszív webalkalmazás (PWA) elnevezés részletes működését a welivesecurity.com cikkében lehet elolvasni.

Persze a képen is látszanak azért intő jelek: magyartalanság, ékezethiány, a hivatalos banki alkalmazástól eltérő applikáció név, gyanús domain név.



Ez is egy érdekes üzenet: "MAGYAR: parkolási szabálysértés történt." A vicces fordulatokkal levélből azt is megtudhatjuk, hogy: **"A bírság túl'épése esetén a bírság összege emelkedik". Emiatt semmiképpen ne lépjük túl a bírságot.**

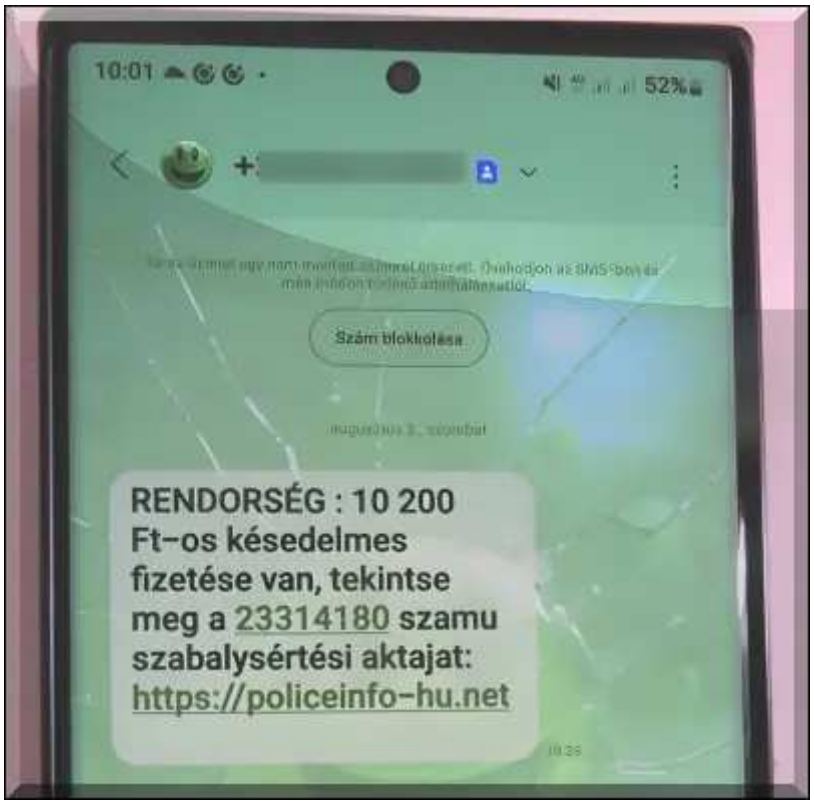
A mellékelt koltsegek-gov.com domain itt is egy nagy kamu, regisztrációja pedig idén július végén történt. Ettől a felszólítástól tehát nem kell nagyon megijedni, **bár a konkrét összeget nem tudjuk, de ugye elég 10-20 percet online dolgozni otthonról, és máris be tudjuk fizetni ;-)**

Ez kettő is elég hasonló, **az elveszett reptéri poggyászokat megvehetjük mindössze 729 forintért. Remek alkalom, a bőröndökben lehet bármilyen érték.** Lehet, hogy mégsem így kezelik az elveszett tárgyakat, csomagokat? Nos biztosan nem.

Az állítólagos ajánlat csak a hónap végéig érvényes, és persze a Liszt Ferenc reptér hivatalos weblapja mi lenne más, mint az air3panda6.store. Ami megint csak egy 2024. májusi domain bejegyzés, r**eménykedni a beígért drága poggyász holmikban, elektronikai cuccokban persze lehet, de nem igazán érdemes.**

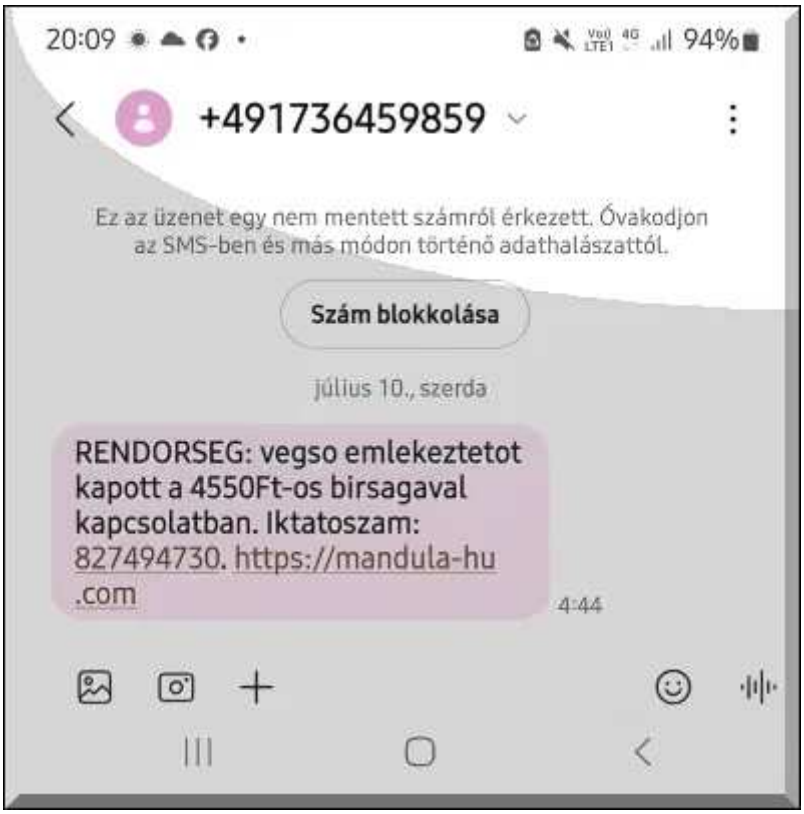
Kaphatunk figyelmeztetést a Rendőrségtől, de **itt a "RENDORSEG" a feladó. Állítólag késedelmes fizetésünk van,** meg "szabalysértési aktank", még jó, hogy nem "szabálysertés" szerepel benne.

A policeinfo-hu.net oldal megint csak egy idén augusztus 3-án regisztrált kamu weboldal, és **szemlátomást a "-hu" a kedvenc országspecifikus jelölő motívuma az elkövetőknek.**



További hatósági felszólítás is érkezhet, ez utóbbit **valószínűleg az ékezet-tagadók csoportja készíthette a RENDORSEG nevében. Itt a végső emlékeztető, ami a fegyveres testületekre olyannyira jellemző "mandula-hu.com" linkre irányít bennünket**, ennyi erővel lehetne "fizess-balek.varjuk-a-penzedet-hu.com" is.

Ez is egy 2024. júliusi webhely, több szót nem is érdemes rá vesztegetni, a +49 pedig a már korábban is említett Németország előhívó száma.



Az előző változatból aztán érkezhetnek további variánsok is, amelyekben a terjesztőknek hosszú fáradságos munkával már sikerült megtalálniuk a billentyűzeten a magyar "é" karaktert, igaz az egyéb ékezetes betűket továbbra is negligálják, azok talán majd a jövő hónapban kerülnek felhasználásra.

A felajánlott link itt már egy másik helyre mutat, nyilván ebből is van egy nagy csokorral, de a lényegét tekintve ez is egy csaló oldal, az info-rendorseg-hu.com pedig szintén egy idén augusztusban Amerikában regisztrált kamu domain.

Ezt itt már csak azért mutatjuk, hogy **mindegy is, hogy magyar vagy németországi számról jön az SMS, a belinkelt oldal címe sokféle lehet, itt éppen a roppant elmés rendorseg-fizetes.com címet adták neki a keresztségben 2024. júniusában.**

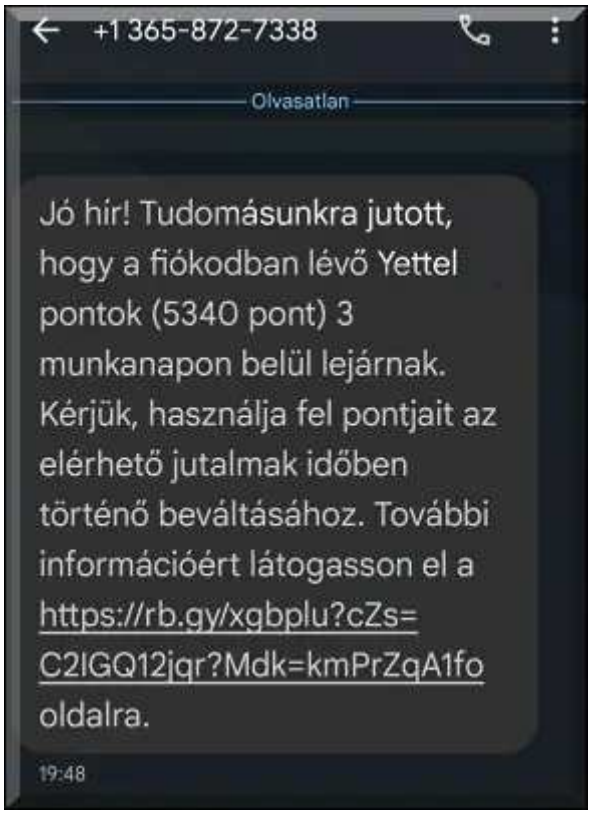
Az ismeretlen telefonszámokat általában senki nem szereti felvenni, erre alapozva jelent meg az a csalástípus, ahol az elkövetők **egy Whatsapp**

üzenetben próbálnak kapcsolatba lépni az áldozatokkal, telefonszám változásra hivatkozva: "Tudsz nekem küldeni egy üzenetet WhastApp,-on?".

Ha valaki válaszol, akkor kisvártatva **valamilyen vészhelyzetre hivatkozva pénzküldésre kérik a szülőket, és ha valaki ennek bedől, akkor csak utólag derül ki, hogy gyereknek nem is változott meg a telefonszáma, hanem egy idegen csaló próbálkozott pénzhez jutni.**

Galériánkat a Yettel nevével visszaélő átveréssel zárjuk, ebben az USA körzetéből érkező SMS üzenetben ékes magyar helyesírással arról tájékoztatnak bennünket, hogy **hamarosan lejárnak a beváltható pontjaink, ideje hát hamar gyorsan belépni hol is máshol, mint a mellékelt linken**. Ami egy a rebrandly link-rövidítő által készített rb.gy formátumú URL.

Ez első, második, sőt sokadik pillantásra sem tűnik egy hivatalos Yettel.hu oldalnak. **A láthatóvá tett valódi cím pedig remélhetőleg senkinek nem okoz meglepetést, a yetteihu.buzz cím szintén idén augusztusban regisztrált adathalász domain**, ahol ráadásul látszólag a Yettel "l" betűjét is benézték "i"-nek, bár ez a végeredmény szempontjából már oly mindegy.



Gratulálunk mindenkinek, aki átrágta magát ezen a komoly kupac csaló SMS példán, remélhetőleg közben mindenki csak mosolygott, hogy hű mennyire átlátszó próbálkozások voltak ezek :)

1 komment
Címkék: sms csalás átverés üzenet adathalászat

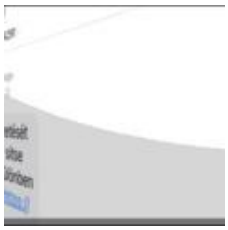
Ajánlott bejegyzések:

Csomagja érke... Na most már elég!

Adathalászat vagy jófogás?

Csomagja érke... Na most már elég!

Mai szavunk pedig: smishing



2023. első csalásai Új bejelentkezés a felhőnkbe. Vagy mégsem?

Új bejelentkezés a felhőnkbe. Vagy mégsem?

Adathalászat vagy jófogás?

Kommentek:

pobeda 2024.09.01. 05:28:01

Igen, mosolyogtam, de meg is osztottam.

Válasz erre

keresés

tweetz






Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

A távolságot mint üveggolyót nem kapod meg

2024. szeptember 03. 13:49 - Csizmazia Darab István [Rambo]

Hogy mennyire sebezhető a modern technológia, arról nemrégiben kaphattunk egy tanító jellegű ízelítő leckét, a történelembe Crowdstrike incidensként bevonuló többnapos leállás során. **Ezúttal a Seattle Airport kapott be egy kibertámadást**, és a zsarolóvírussal megfertőződött kórházakhoz hasonlóan **itt is napokig csak "kézműves" megoldásokkal lehetett kezelni a kialakult szituációt.**

A megtámadott kórházakban sokszor láthattuk már, **mennyire fejre állt számítógépes hálózat nélkül az élet: kezelések és műtétek maradtak el, betegeket kellett másik intézménybe átirányítani, illetve átszállítani, az online betegfelvétel és leletkiadás hiányában maradt a kőkorszaki telefon, fax, a ceruza és papír, kartonozás, valamint internet helyett a személyes ügyintézés akár több száz kilométerről.**

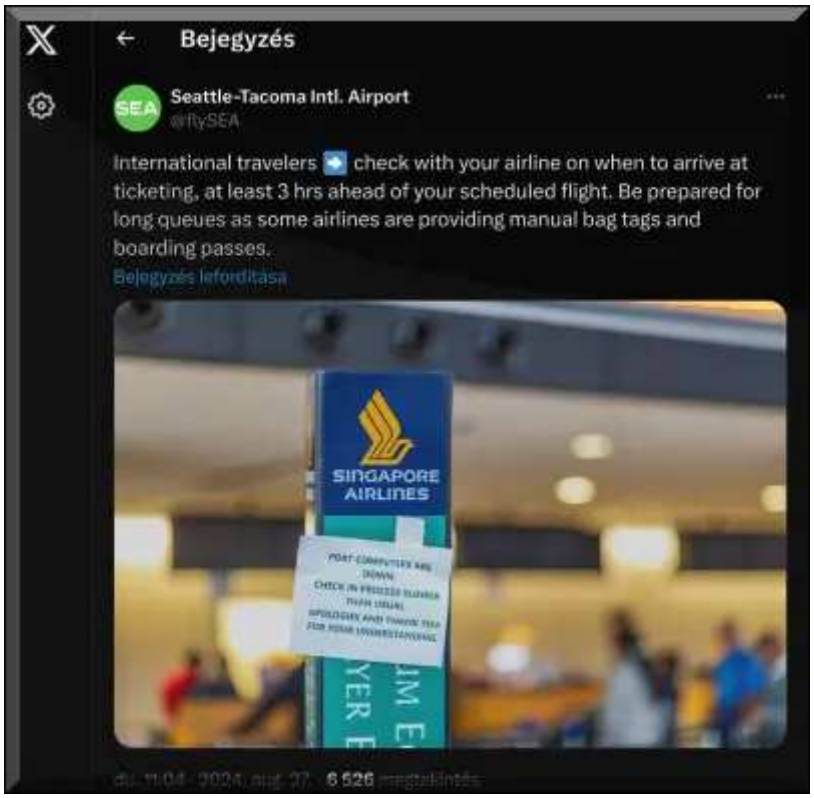
Járulékos kárként később azzal is sokan szembesülhettek, hogy az adminisztráció teljes leállása miatt **a társadalombiztosítási elszámolás rendszere is megakadt, ami mind a betegek betegállományba vételénél, mind az orvosok elszámolt munkaóráinál gondot, késedelmet, illetve papíralapú elszámolásokat és fizikai postázásokat okozott.**

Az emlegetett Crowdstrike frissítés problémája miatt **idén júliusban 8.5 millió Windows eszköz fagyott le, és ezzel olyan sosem látott világméretű szolgáltatás leállás következett be, melyben repterek, bankok, tévéadók, közlekedési terület, egészségügyi szektor, tőzsdék bénultak meg**.

A leállás okozta kár mértéket az első számítások 10 milliárd dollárra becsülték.

Ezúttal nem globális, **"csak" lokális informatikai incidens történt a Seattle repülőtéren**, de az utazók és ott dolgozók életét mindez alaposan megkeserítette. **Augusztus 24-én egy közelebbről nem nevesített kibertámadás miatt rendszerleállások következtek be, és emiatt nem működött a reptér hivatalos weboldala, a helyi wifi és e-mail szolgáltatás megszűnt.**

Az elektronikus tájékoztató kijelzők sötétek maradtak, az utasoknak pedig a légitársaságok alkalmazásain keresztül lehetett kezelni a beszállókártyájukat és a poggyászfeladást, illetve ezek hiányában kézzel kellett 8 ezer poggyász esetében címkézni, beszállókártyákat kézzel írogatni.



Nagyjából egy hét telt el, mire az ünnepi hétvége után részlegesen sikerült helyreállítani egyes szolgáltatásokat, és megszűntek a hosszas sorban állások a Seattle-Tacoma Nemzetközi Repülőtéren.

A korábbi kaotikus viszonyok miatt az előző napokban ajánlatos volt minimum 3 órával korábban kiérkezni.

Ám **a kibertámadás okáról és részleteiről azóta sem közöltek bővebb információkat.**

Azt viszont a repülőtér illetékesei kihangsúlyozták, hogy a központi légi irányítási és más biztonsági műveleteket állítólag nem érintett a számítógépes kimaradás, és a támadás miatt elmondásuk szerint viszonylag kevés járat törlés és késés következett be.

Szólj hozzá!
Címkék: leállás usa seattle szolgáltatás reptér repülőtér ransomware kibertámadás

Ajánlott bejegyzések:

A vízszámla érintése
Újabb rombolás brit kórházakban
100 millió ember egészségügyi adata hoppszi
Vérszagra gyűl a ransomware

A vízszámla érintése
Újabb rombolás brit kórházakban
100 millió ember egészségügyi adata hoppszi
Vérszagra gyűl a ransomware
Az élet szép, de a Life360-nak vannak gondjai

Az élet szép, de a Life360-nak vannak gondjai

Kommentek:

Nincsenek hozzászólások.

keresés

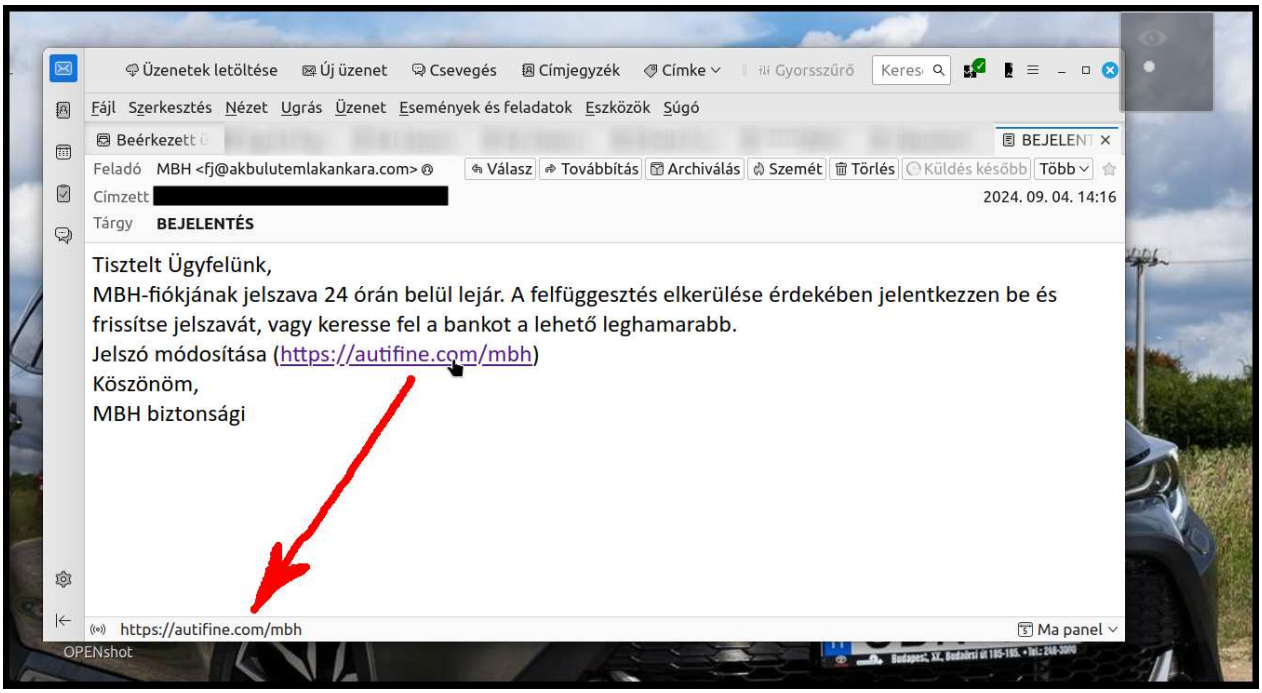
tweetz

MBH-fiókjának jelszava 24 órán belül lejár

2024. szeptember 05. 17:03 - Csizmazia Darab István [Rambo]

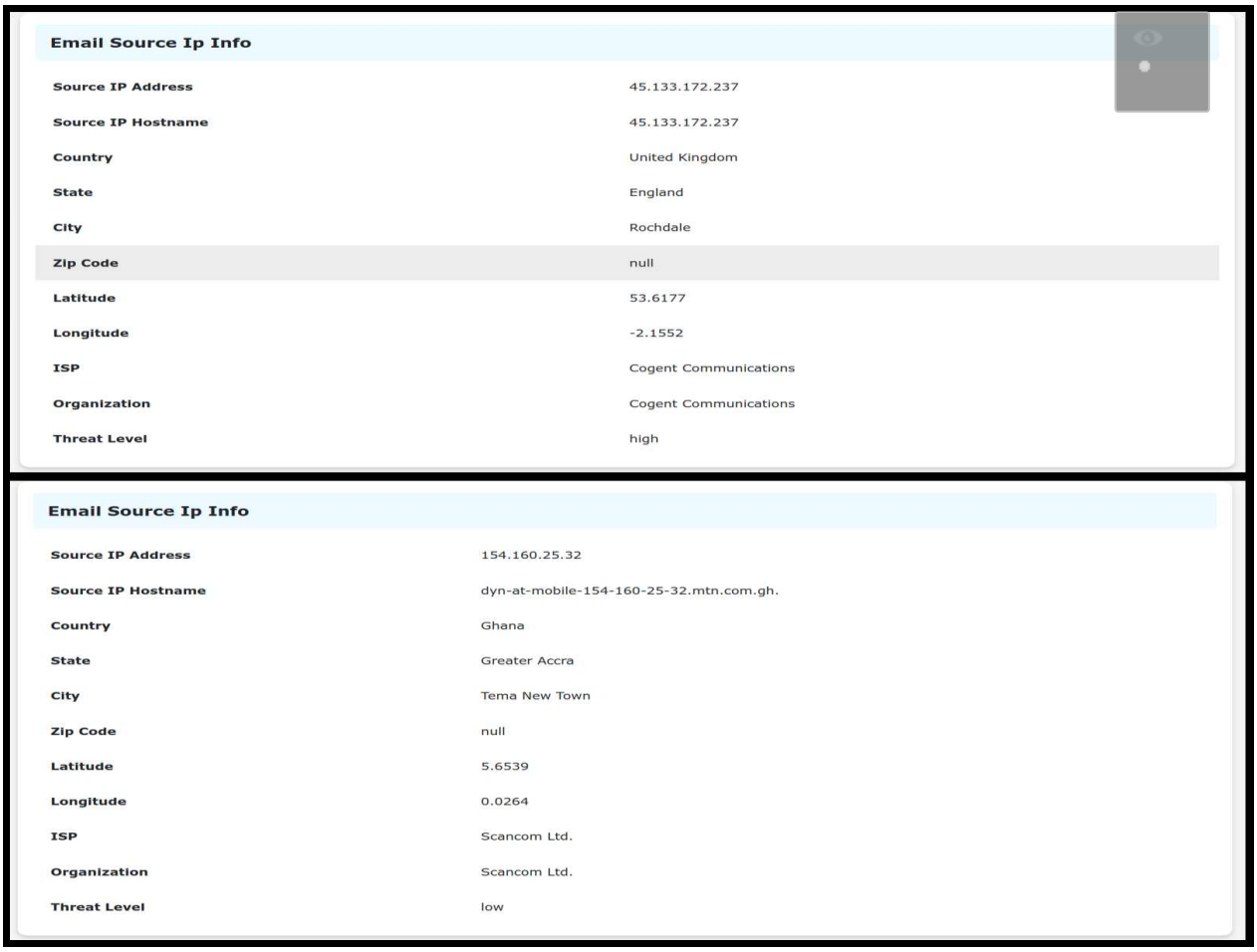
Naponta több ilyen hamis e-mail is próbálkozik, természetesen mint mindig, most is adathalász oldalakra irányítanak a mellékelt linkek.

Nem kell még ügyfélnek sem lenni ahhoz, hogy a különféle banki csalók üzenetei beessenek a postafiókjainkba. Most úgy tűnik, a korábbiak után ismét **az MBH bank nevében próbálkoznak sorozatban, és a cél a szokásos: a jelszavunk állítólag lejár, emiatt gyorsan be kell jelentkezni a csatolt linkre kattintva.**



Többféle változatban és több példányban is megkaptuk, és **mindegyik szedett-vedett feladóktól érkezett**, például Gkiuddiouew@iometexbrm.co, fj@akbulutemlakankara.com, jp@pelisterra.com. **Az e-mail trace alapján a küldés (vagy a VPN) helye is változatos, például Nagy Britannia, Ghána, stb.**

A feladók, a mellékelt linkek is szembetűnően kamu szagúak, és **maga a levél is elég egypálcás kinézetű, meg sem próbálták az e-mail kinézetet testre szabni, csinosítgatni.**



Email Source Ip Info

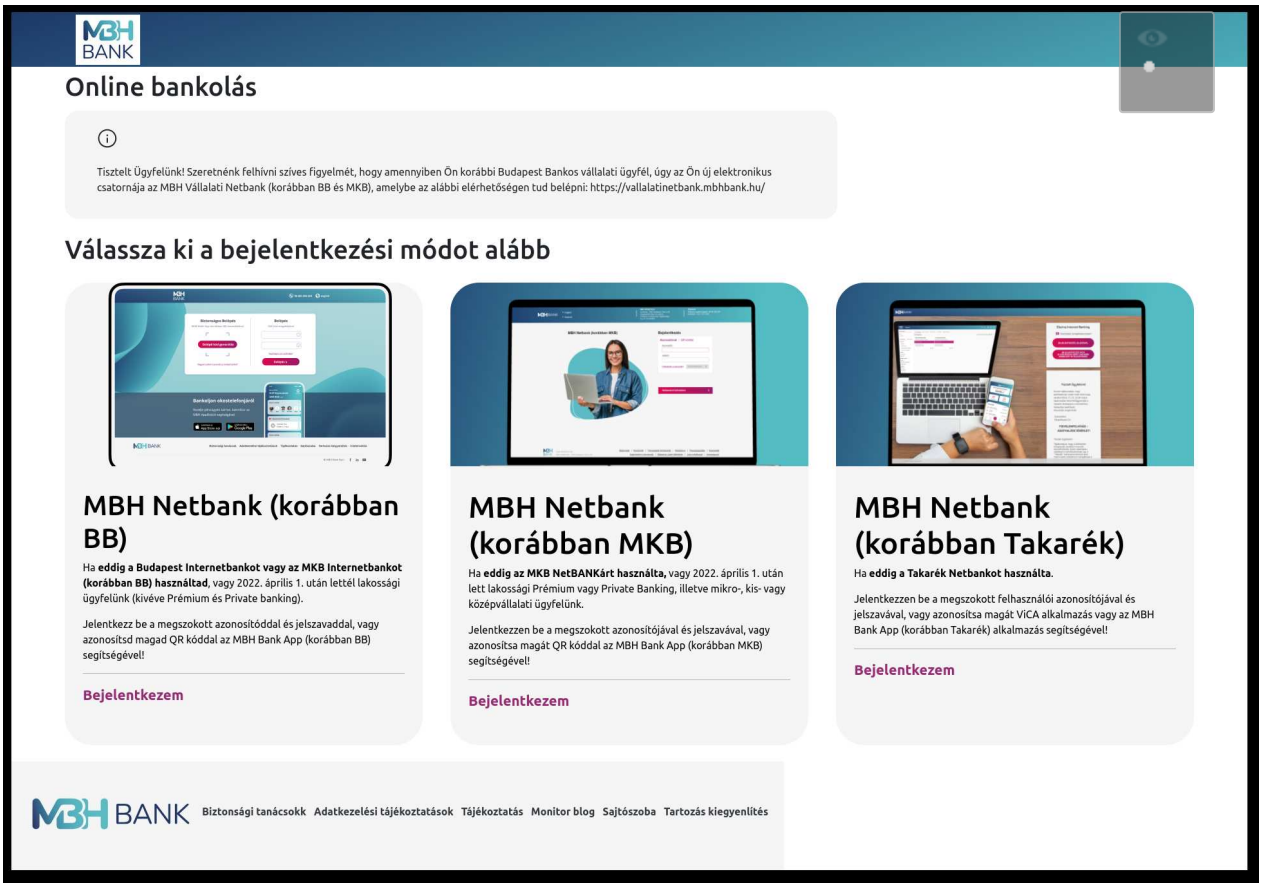
Source IP Address	45.133.172.237
Source IP Hostname	45.133.172.237
Country	United Kingdom
State	England
City	Rochdale
Zip Code	null
Latitude	53.6177
Longitude	-2.1552
ISP	Cogent Communications
Organization	Cogent Communications
Threat Level	high

Email Source Ip Info

Source IP Address	154.160.25.32
Source IP Hostname	dyn-at-mobile-154-160-25-32.mtn.com.gh.
Country	Ghana
State	Greater Accra
City	Tema New Town
Zip Code	null
Latitude	5.6539
Longitude	0.0264
ISP	Scancom Ltd.
Organization	Scancom Ltd.
Threat Level	low

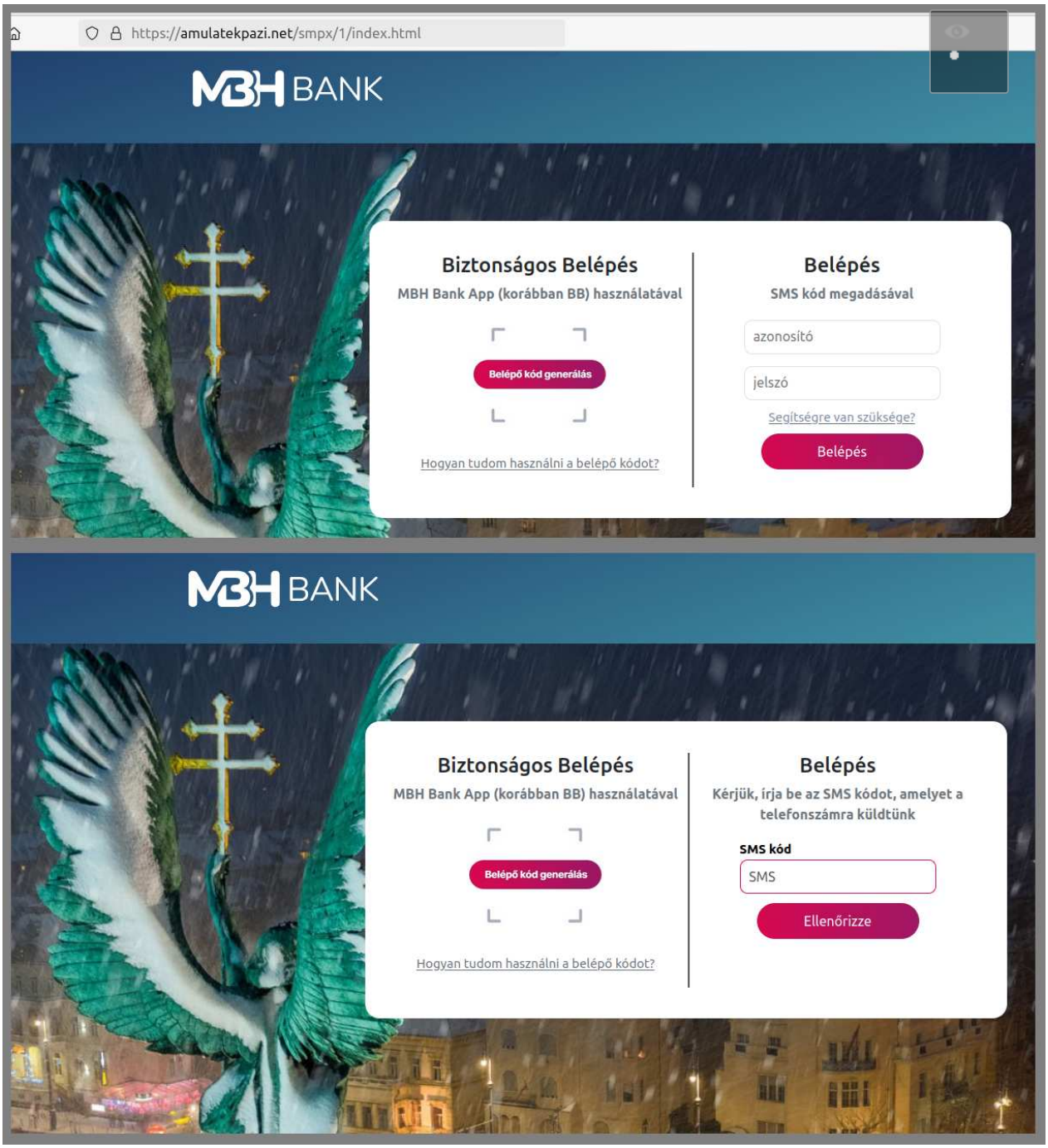
A weboldalakat időközben már sikeresen lelőtték, de a kézbesítéskor még éppen működtek. **Ezek már azért igyekeztek a hivatalos webhely kinézetét élethűen lemásolni**, és a céljuk nyilván az volt, hogy a felhasználók belépjenek itt az adathalász oldalon.

A bejelentkezési oldalon először választani kellett aszerint, hogy ki volt korábban Budapest Bank vagy Takarék netbanki ügyfél.



Első körben azonosító és jelszó bekérés történik a hasonmás oldalon, majd utána az SMS kódot is bekérik, hogy meglegyen nekik a teljes banki belépés.

Érdemes tehát odafigyelni, szerencsére ezekről már annyi hír, cikk, blogposzt, beszámoló jelent meg, hogy remélhetőleg más senki nem téved bele ilyen átverésekbe.



Lassan elkezdték a bankok a mobil appokba beépíteni azt a lehetőséget is, hogy ellenőrizhető legyen a banki telefonhívások forrása is. Ha megnyitjuk a banki alkalmazást, abban egy külön menüpont segítségével láthatjuk, valóban banki ügyintéző hívott-e minket.

Igaz, a biztonságtudatosság ekkor sem mellőzhető, mert a telefonos csalók a például a rendőrség nevében is hívják az embereket, szóval az egészséges gyanakvás mindenhol mindenkor kötelező kellék.

1 komment
Címkék: spam csalás átverés adathalászat banki mbh adatlopás

Ajánlott bejegyzések:

MBH banki adathalászat

Utolsó emlékeztető a fiók felfüggesztése előtt

Fontos vagy nekem

MBH banki adathalászat

Adathalászat menni booking.com

Utolsó emlékeztető a fiók felfüggesztése előtt

Fontos vagy nekem
Ment a hűtlen hamis linkkel

Ment a hűtlen hamis linkkel

Kommentek:

havrilla 2024.09.06. 08:58:47

Nálam egy ideig ez a cím jelent meg. Mindig "válaszlevelet akartam küldeni". Ez irónia volt. Elég nehéz volt eltüntetni amatörként. Természetesen semmilyen csatolmányt nem nyitottam meg. eM Clientet használok.
Nem tudom mi ez:

elefantapple.indianfig@wholesomefoods.info

Válasz erre

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

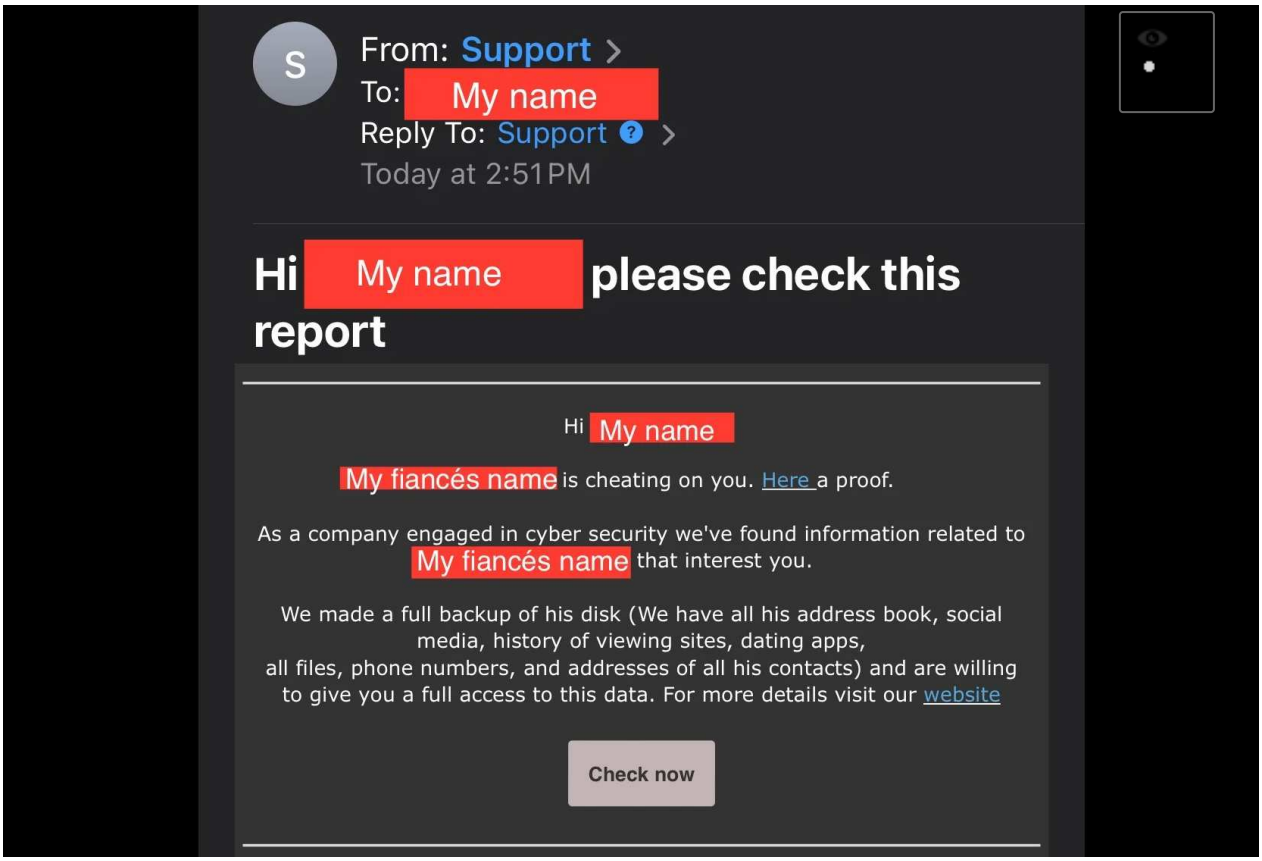
Ment a hűtlen hamis linkkel

2024. szeptember 10. 09:44 - Csizmazia Darab István [Rambo]

Talán a hamis vírusirtókkal 2004-ben erősödött fel az a folyamat, amikor **rendre érkezett valamilyen változatos fenyegető üzenet:** vírusfertőzött a gépünk és a mentesítésért fizessünk, szerzői jogok megsértése miatt bajba kerültünk, állítólagos pedofil tartalmak böngészése miatt eljárás indult ellenünk, a webkameránkkal állítólag képeket és videókat készítettek rólunk intim helyzetben emiatt fizessünk, és hasonló gyakori átverések.

Ezek - a hamis vírusirtós változat kivételével - máig megmaradtak és valamilyen formában újracsomagolva azóta is felbukkannak, ám időről időre vadonat új trükkök is kopogtatnak, és ezúttal egy ilyenről lesz szó.

Az új módszer a házastársakat célozza meg, mondván, hogy férjük vagy feleségük titokban megcsalja őket. Az elkövetők azt állítják, hogy feltörték az illető házastársának a gépét, és a kíváncsiságra építve az e-mailben mellékelik az állítólagos bizonyítékokra mutató click.cardfoolops linket.

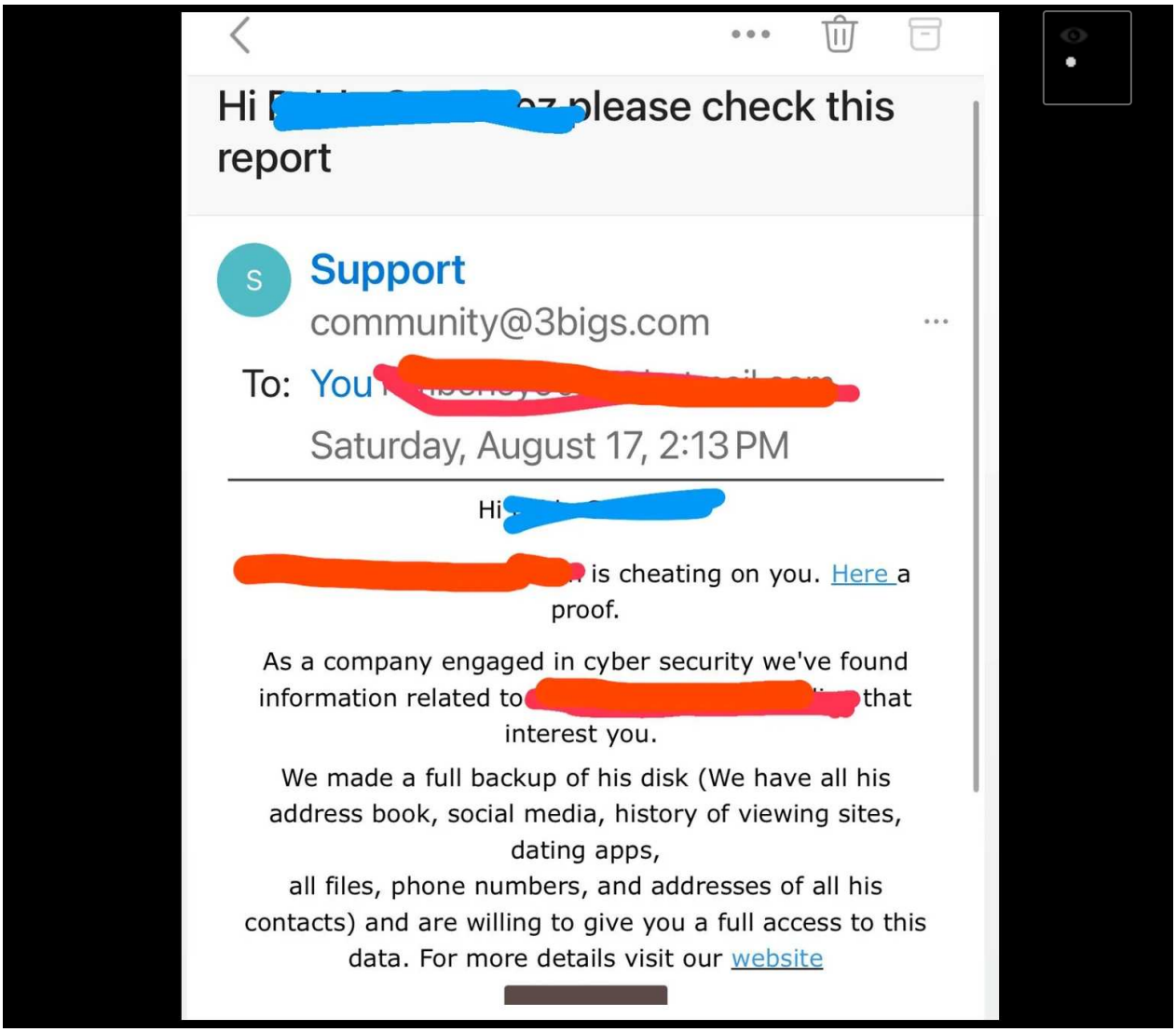


A küldők önmagukra, mint kiberbiztonsággal foglalkozó cégként hivatkoznak (naná), és **azt írják, hogy az állítólagos megcsaló házastárs merevlemezéről másolatot készítettek (Btk. 423. §), amely alapján árulkodó a címjegyzék, a közösségi médiás üzenetek.**

De emellett ki lett gyűjtve a böngészőjéből a meglátogatott weboldalak megtekintési előzményei, a társkereső alkalmazásokon belüli aktivitása, illetve a számítógépéről további egyéb bizonyító erejű média állományok.

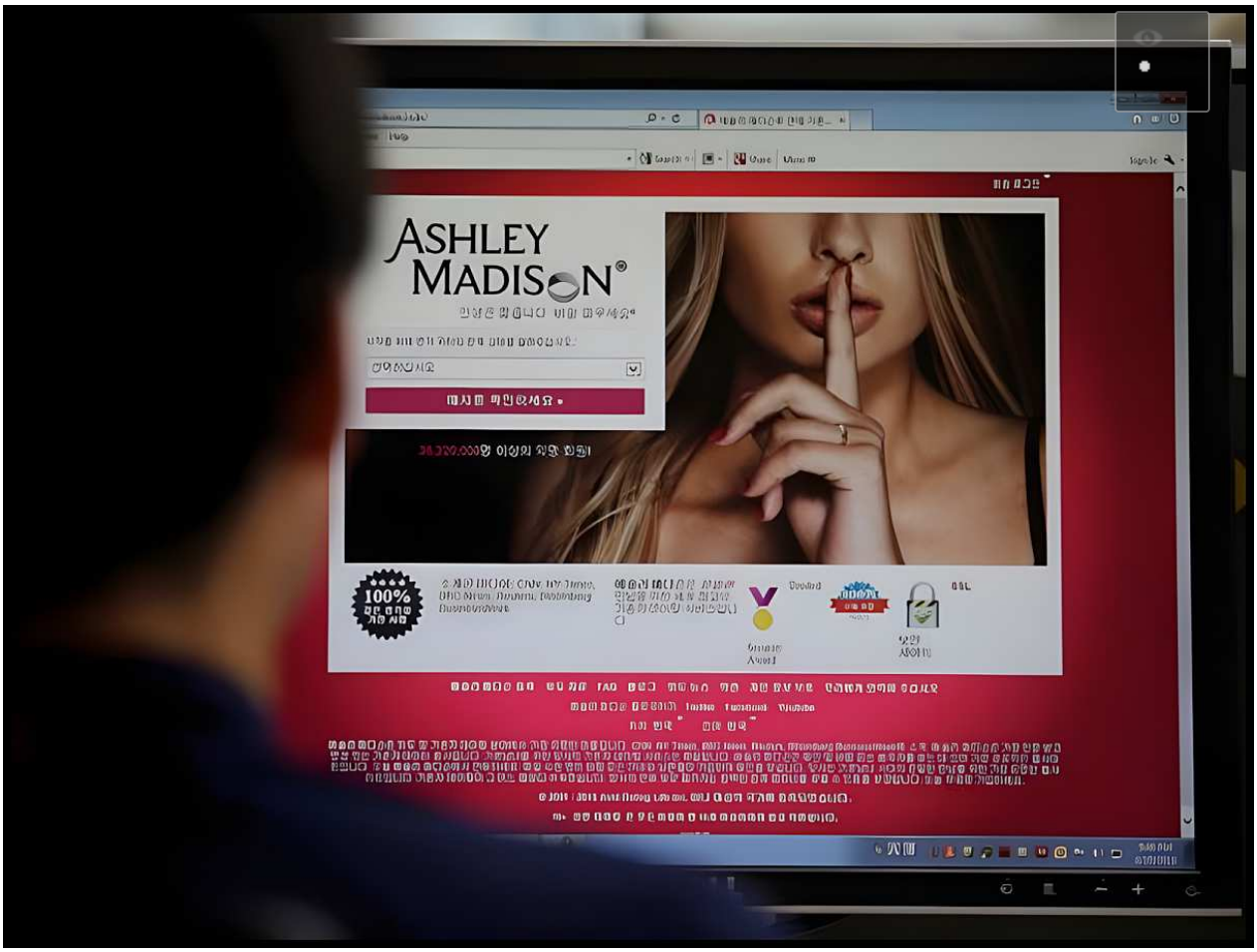
A community KUKAC 3bigs PONTcom címről érkező levélnél **zavarba ejtő lehet, hogy pontosan ismeri a házasfelek teljes nevét, és így valóban egy célzott, nekünk testre szabott üzenetként tűnhet fel**.

A Bleeping Computer gyanúja szerint **elképzelhető, hogy a The Knot nevű esküvőszervező oldal adatbázisát törhették fel** ismeretlenek, ám az érintett cég egyelőre nem reagált arra a felvetésre, hogy valóban tőlük lophatták-e el ehhez a spam kampányhoz felhasznált adatokat.



Az áldozatok beszámolói vegyesek voltak azzal kapcsolatosan, mi történt velük a linkre való kattintás után. **Volt, aki egy adathalász kinézetű oldalon találta magát, de másvalakinél az is előfordult, hogy valamilyen kártevővel fertőzött oldalra irányította át a mellékelt rosszindulatú hivatkozás.**

Az mindenesetre egy **állandó elem, hogy a bűnözői oldalon érdemes a kíváncsiságra rájátszani, mert az sok kattintást okoz** a kevésbé tudatos felhasználóknál.



Van persze olyan, amikor a megcsalás valós. Azoknak, akik életvitelszerűen űzik a félrelépést, érdemes felidézni a 2015-ös év egyik roppant kínos incidensét, amikor is **az Ashley-Madison közvetítő portált feltörték, és a támadók 37 millió "ügyfél" adatát, benne neveket, e-mailcimeket, bankkártya számokat, szexuális preferenciákat, a tagság által feltöltött fotókat, illetve az ügyfelek és a belső munkatársak levelezését is megszerezték.**

Az ott megígért anonimitást, végleges törlést komolyan vevő gyanútlan felhasználók vélhetően nem ilyen "affair"-re számítottak. Az akkori esetről egyébként a Netflix egy érdekes és tanulságos sorozatot is készített.

Szólj hozzá!
Címkék: spam kampány csalás átverés kattintás megcsalás testreszabott adathalászat házasságtörés

Ajánlott bejegyzések:

[Utolsó emlékeztető a fiók felfüggesztése előtt](#) [MBH-fiókjának jelszava 24 órán belül lejár](#) [Üdvözöl a bölcs csapat](#) [Leveringa függesztés csomag részére](#)

[Utolsó emlékeztető a fiók felfüggesztése előtt](#) [MBH-fiókjának jelszava 24 órán belül lejár](#) [Üdvözöl a bölcs csapat](#) [Leveringa függesztés csomag részére](#)

[Adathalászat menni booking.com](#)

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

[Tovább a Facebook-ra](#)

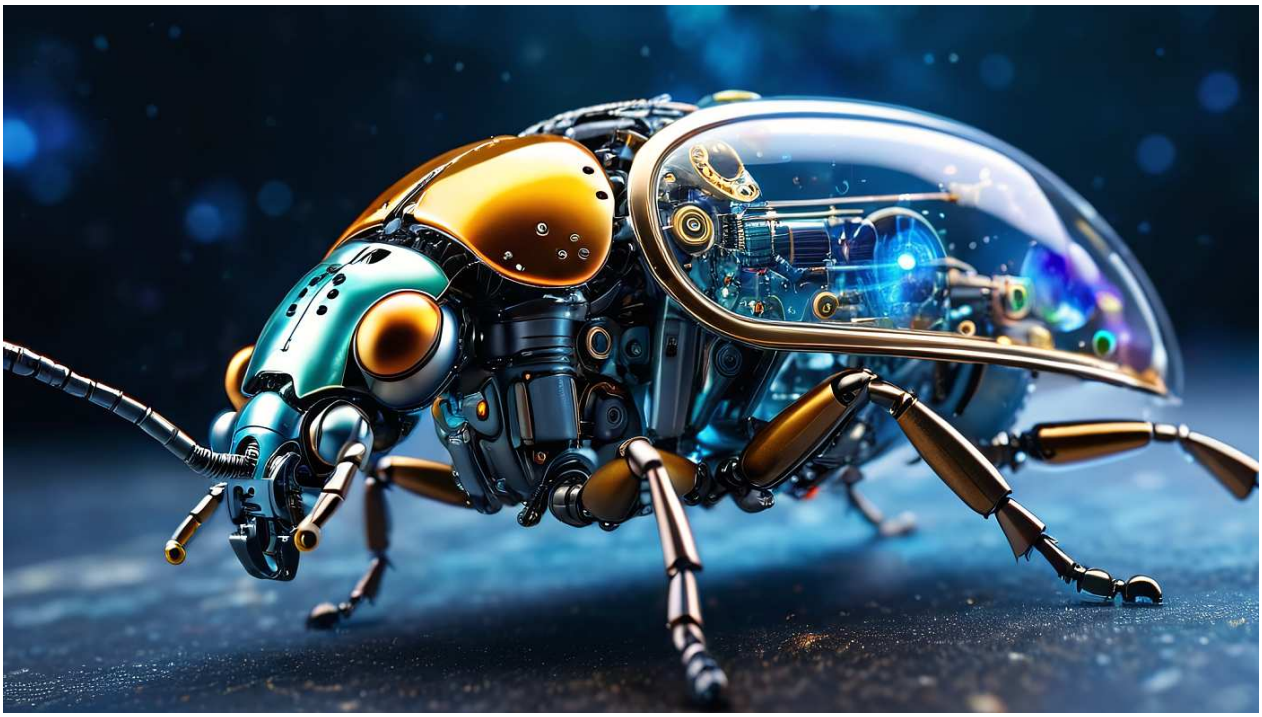
top 5z

1. [Magyarországra is megérkezett a CTB-Locker](#)
2. [A Gmail-es jelszavak kiszivárgása](#)

Egy Kozmikus Bogár ront el mindent

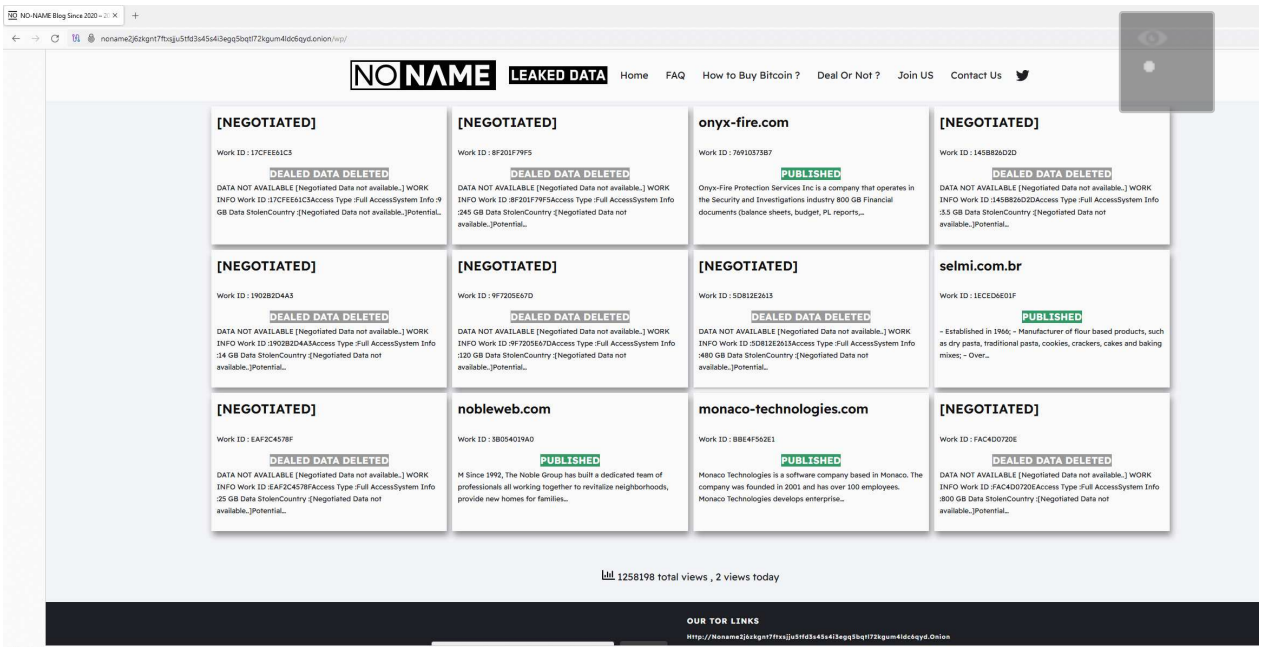
2024. szeptember 12. 19:24 - Csizmazia Darab István [Rambo]

Elsősorban európai és ázsiai kisvállalkozásokat támad be a CosmicBeetle ransomware csoport, amelyik látszólag most a RansomHub égisze alatt hozta ki programjának új ScRansom változatát.



A 2020. óta létező csapat korábban a Scarab zsarolóvírussal volt jelen, amelyet az idők során folyamatosan fejlesztettek. Az elemzések szerint **egy érdekes szereplő, volt, hogy a LockBit nevével is visszaéltek és török nyelvű üzenetekkel igyekeztek váltságdíjat kizsarolni. Láthatóan a NONAME nevű TOR szivárogtató oldalukat is a LockBit-ről másolták.**

A kódban előforduló török nyelvű karakterek ellenére a származás **ezzel mégsem azonosítható be egyértelműen**, az viszont látszik, hogy a gyaníthatóan RansomHub ransomware-as-a-service partnereként fellépő CosmicBeetle **2024. márciusa óta gyorsan növekvő aktivitással rendelkezik.**



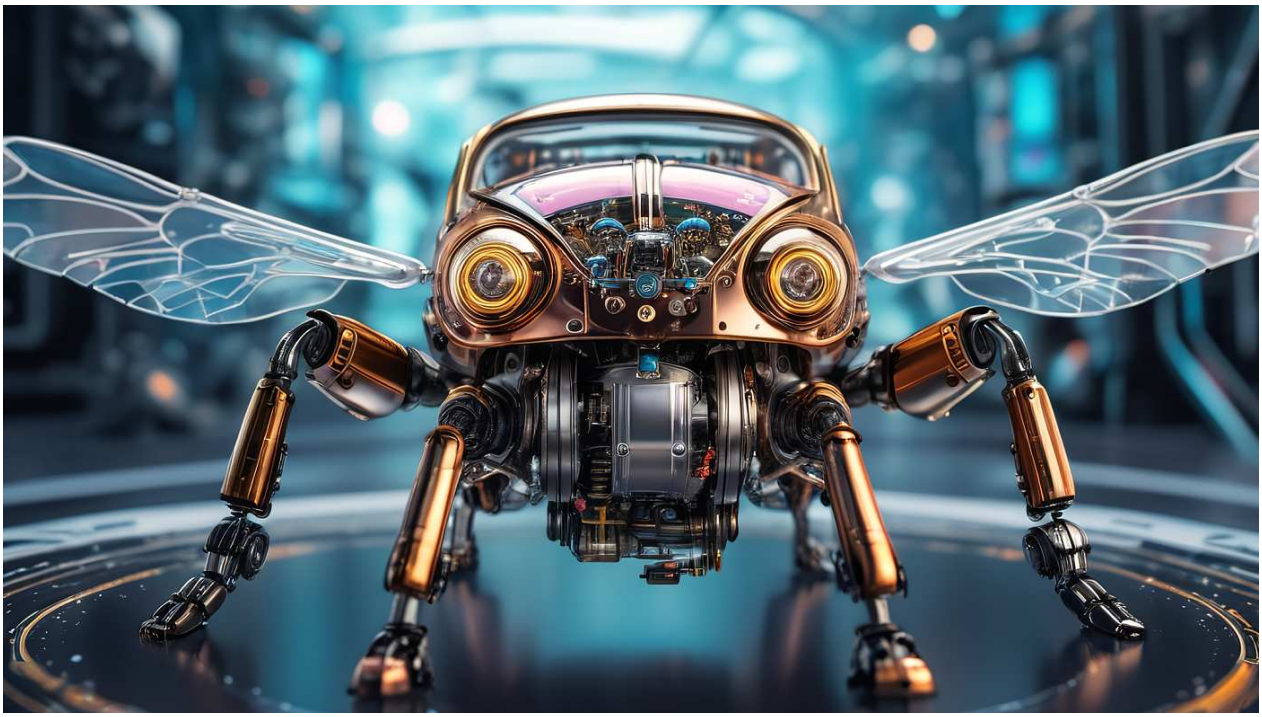
A ScRansom legkorábbi mintái még 2023. márciusában végén jelentek meg, de a valódi támadások csak augusztusban kezdődtek el. A kutatók szerint júniusban a CosmicBeetle megpróbált kompromittálni egy indiai gyártó céget, de ott még nem jártak sikerrel.

Később viszont a csoport gyógyszeripari, jogi, oktatási, egészségügyi, technológiai és pénzügyi iparágak ellen indított támadásokat, amihez évek óta fennálló sebezhetőségeket igyekezett kihasználni elsősorban kis- és középvállalkozásokat megcélozva tudva, hogy itt a hibajavítási hajlam gyakran problematikus.

A ScRansom nem túl kifinomult zsarolóprogram, és van benne egy olyan buktató is, amely alaposan megkeserítheti az áldozatok életet. Egyszer korábban már értekeztünk arról, hogy voltak olyan hibásan megírt ransomware programok, amik még fizetés esetén sem hagytak esélyt az áldozatoknak.

A "PowerWorm" zsarolóvírusban egy **programozási hiba következtében egyáltalán nem lehetett helyreállítani az adatokat**, míg a GitHubról

származó "HiddenTear" átirat esetében szintén **elkutyult kódolás miatt a 10 MB méret feletti állományoknál nem működött a helyreállító kulcs, így ott is garantált volt az adatvesztés.**



És ebben a ligában focizik a CosmicBeetle is, ugyanis bár maga a visszafejtő működik, ám gyakran több visszafejtő kulcsra is szükség van, amiből ha nem kapjuk meg az összeset, akkor egyes fájlok végleg elveszhetnek. Azonban még optimális esetben is maga a visszafejtés egy extra hosszú és roppant bonyolult folyamat lesz.

Egy igen részletes alapos elemzés az ESET részéről itt olvasható a WeLiveSecurity oldalon.

Szólj hozzá!
Címkék: hiba adatvesztés exploit sebezhetőség váltságdíj sérülékenység ransomware raas ESET welivesecurity.com zsarolóvírus ransomhub cosmicbeetle

Ajánlott bejegyzések:

Újabb rombolás brit kórházakban
100 millió ember egészségügyi adata hoppszi
Senki többet harmadszor?
Change Healthcare újra pácban

Újabb rombolás brit kórházakban
100 millió ember egészségügyi adata hoppszi
Senki többet harmadszor?
Change Healthcare újra pácban

A ransomware az egészségügyben élet-halál kérdése

A ransomware az egészségügyben élet-halál kérdése

A ransomware az egészségügyben élet-halál kérdése

A ransomware az egészségügyben élet-halál kérdése

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

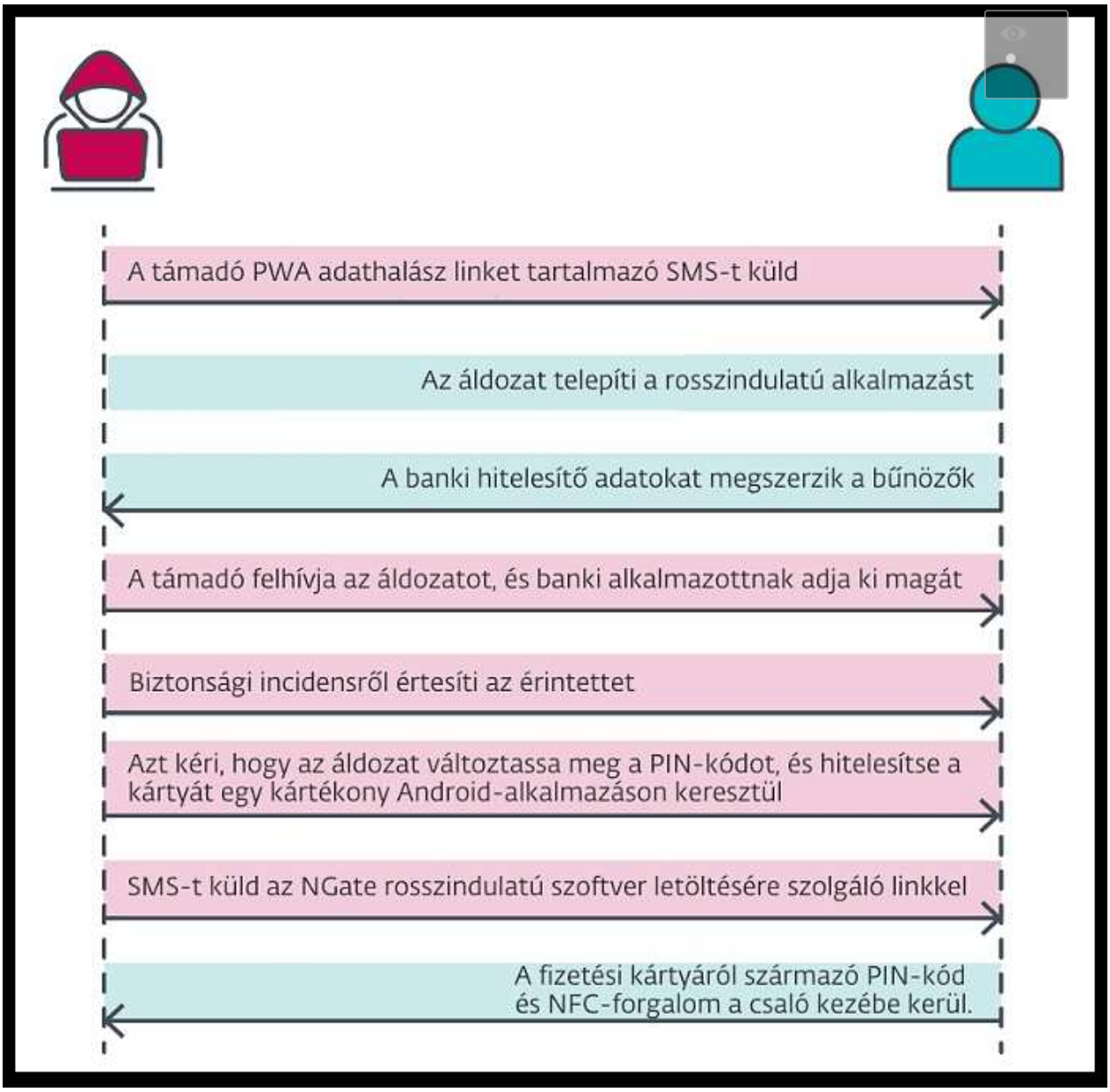
Fontos vagy nekem

2024. szeptember 17. 10:15 - Csizmazia Darab István [Rambo]

Az ESET kutatói felfedtek **egy vadonatúj számítógépes kártevő programmal** végrehajtott crimeware kampányt, amely három cseh bank ügyfeleit vette célba. **Az NGate-nek elnevezett Android alapú kártékony szoftver újszerű módon képes az áldozatok bankkártya adatait** a támadók telefonjára továbbítani.

A támadók elsődleges célja az volt, hogy ATM-eken keresztül készpénzt vegyenek fel az áldozatok bankszámláiról. Ezt úgy érték el, hogy **a fizikai bankkártyák megszerzett NFC-adatait a támadók készülékére továbbították az NGate malware segítségével.**

Amennyiben ez a módszer esetleg sikertelen volt, **a tetteseknek még arra is volt egy tartalék terve, hogy az áldozatok számláiról más bankszámlákra utaljanak át pénzösszegeket.**

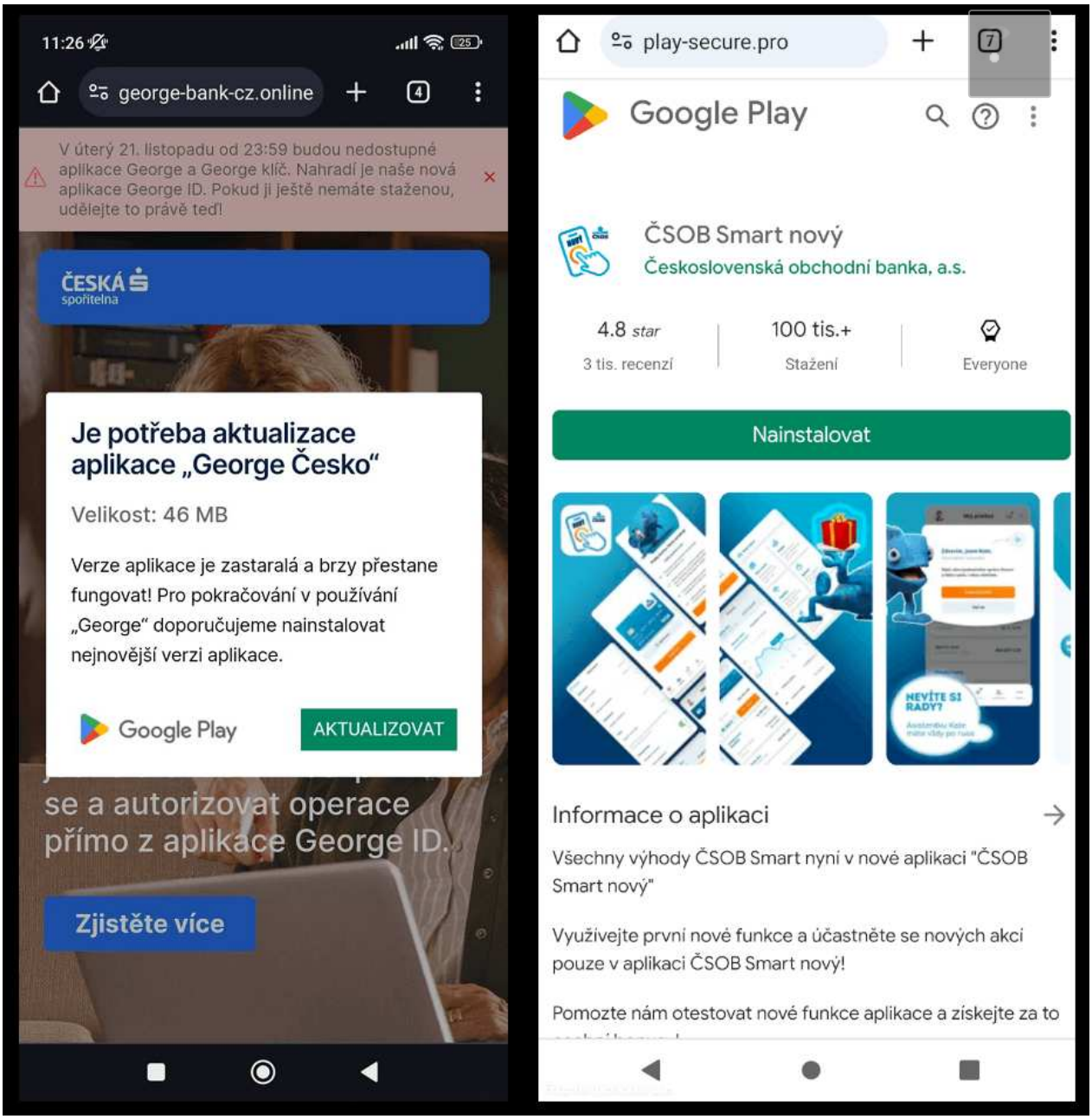


A 2010-es évek második felében új fizetési szabványként jelent meg a **rádiófrekvenciás azonosításból (RFID) kifejlesztett közelmezős kommunikáció (Near Field Communication, NFC)**. Ezzel a technológiával az eredeti chipalapú bankkártyák még felhasználóbarátabbá váltak, mivel fizetési terminálokba és ATM-ekbe való behelyezés helyett itt a pénz küldéséhez elég egy NFC-kompatibilis fizetési eszköz közelébe tartani a kártyát. Szakértők korábban **még soha nem találkoztak korábban ilyen típusú NFC átviteli technikával**, mint ami most felbukkant.

A módszer egy NFCGate nevű eszközön alapul, amelyet a németországi Darmstadti Műszaki Egyetem hallgatói fejlesztettek ki NFC forgalom rögzítésére, elemzésére és módosítására **("Please do not use this application for malicious purposes."), innen nevezték el az új malware-családot NGate-nek.**

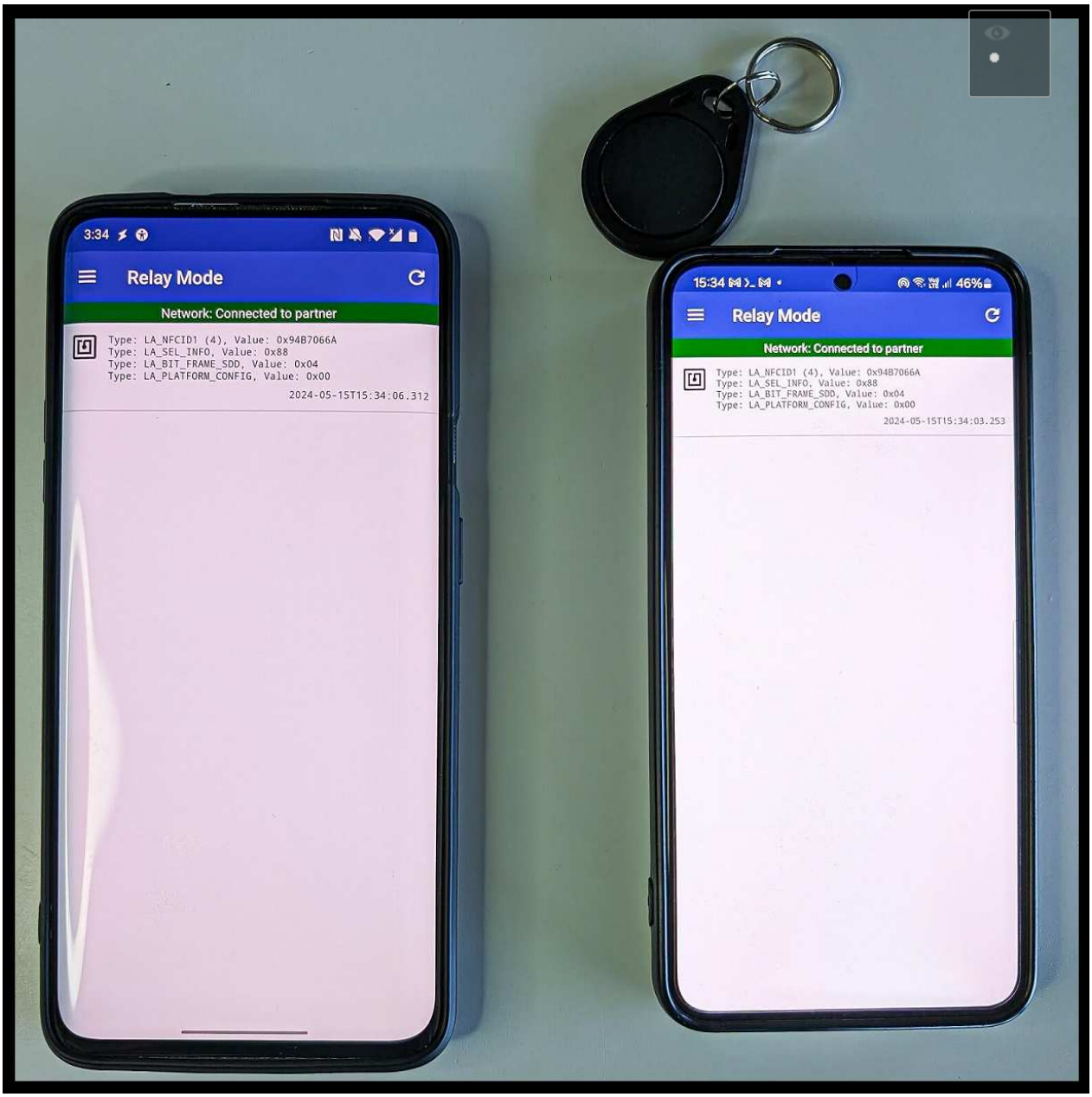
Az áldozatokat azzal vették rá a rosszindulatú program telepítésére, hogy például **elhitették velük, hogy éppen a bankjukkal kommunikálnak arról, hogy az eszközüket állítólag feltörték. Valójában azonban maguk a felhasználók fertőzték meg az Android-eszközeiket azzal, hogy előzőleg telepítettek egy kétes alkalmazást a csalóktól érkezett linkről, amit egy állítólagos adó-visszatérítésről szóló SMS-ben küldtek ki.** Az NGate soha nem volt elérhető a hivatalos Google Play áruházban, csak spamek linkjében szerepelt.

Az NGate Android kártevő egy **2023. novembere óta Csehországban aktív támadó adathalász** tevékenységéhez kapcsolódik. **A szakértők ugyanakkor úgy vélik, hogy ezeket a gyanús tevékenységeket egy 2024. márciusában történt letartóztatás után felfüggesztették.**



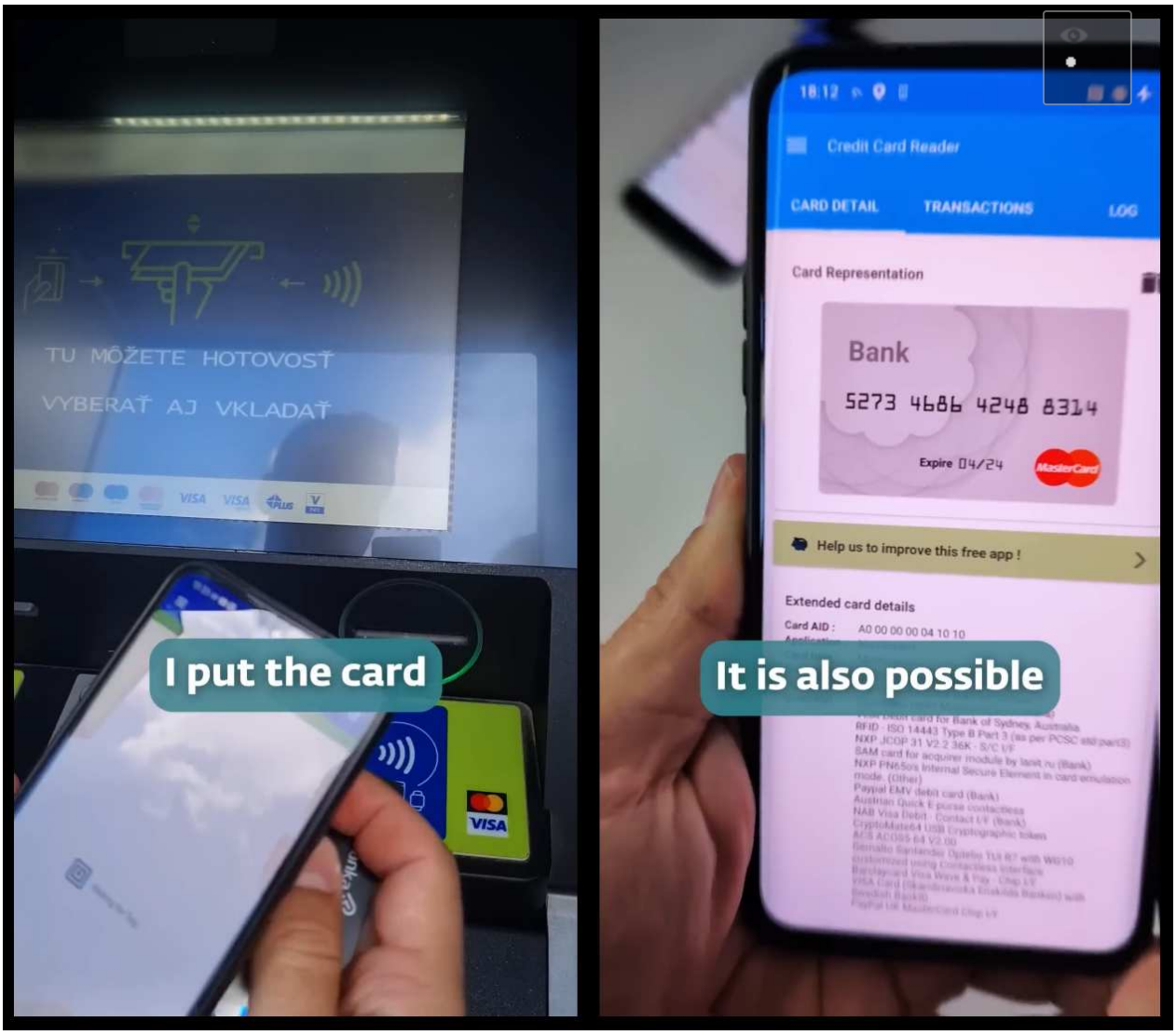
Az ESET először 2023. november végén észlelte a fenyegetést, amely neves cseh bankok ügyfeleit vette célba. A rosszindulatú programokat rövid ideig működő domaineken keresztül terjesztették, amelyek **hiteles banki weboldalakat vagy a Google Play áruházban elérhető hivatalos mobilbanki alkalmazásokat imitáltak**. Ezeket a hamis domaineket az ESET Brand Intelligence Service azonosította, és jelezte az ügyfelei felé.

Az elkövetők a progresszív webalkalmazások (PWA-k) lehetőségeit használták ki, majd később továbbfejlesztették stratégiájukat azzal, hogy a PWA-k egy kifinomultabb, WebAPK-ként ismert verzióját használták. **A művelet finomhangolása végül az NGate malware alkalmazásával csúcsosodott ki.**



2024. márciusában felfedezték, hogy az NGate Android malware ugyanazokon az oldalakon vált elérhetővé, amelyeket korábban adathalász kampányok során használtak rosszindulatú PWA-k és WebAPK-k terjesztésére. Telepítés után az NGate egy hamis adathalász webhelyet jelenített meg, amely a felhasználó banki adatait kérte, és azokat a támadó szerverére küldte.

Az adathalász funkciói mellett az NGate malware egy NFCGate nevű szoftvert is tartalmaz, amelyet arra használtak fel, hogy NFC adatokat továbbítson két eszköz – az áldozat és az elkövető készüléke – között. **Az NGate arra is felkérte az áldozatokat, hogy adják meg érzékeny adataikat, például a banki ügyfél-azonosítójukat, a születési dátumukat és a bankkártyájuk PIN-kódját, továbbá javasolta nekik, hogy kapcsolják be az NFC funkciót okostelefonjukon. Ezt követően az áldozatoknak a bankkártyájukat az okostelefon hátuljához kellett helyezniük, amíg a kártékony alkalmazás fel nem ismerte a kártyát.**



Az NGate malware által **használt technikán kívül a támadó, ha fizikai hozzáféréssel rendelkezik a bankkártyákhoz, potenciálisan le is másolhatja azokat.**

Ezt a technikát olyan elkövető alkalmazhatja, aki **a közelben lévő kártyákat őrizetlenül hagyott táskákon, pénztárcákon, hátizsákokon vagy bankkártyák tárolására alkalmas okostelefon-tokokon keresztül próbálja meg illetéktelenül leolvasni, például nyilvános és zsúfolt helyeken**. Azonban ez a forgatókönyv általában **csak kis összegű érintés nélküli fizetéseket tett lehetővé** a terminálokon.

Az ilyen összetett támadások elleni védekezéshez mindenkinek ismernie kell, hogyan léphet fel hatékonyan az adathalászat, a social engineering és az Android malware taktikák ellen. Ez magában foglalja, hogy naprakész védelmi megoldást futtassunk az okostelefonunkon, mindig ellenőrizzük a webhelyek URL címeit, csak a hivatalos áruházakból töltsünk le alkalmazásokat, soha ne adjuk ki a PIN-kódunkat, kapcsoljuk ki az NFC funkciót, amikor nincs rá szükségünk, illetve védőtokokat vagy hitelesítéssel védett virtuális kártyákat használjunk.

További részletes technikai információk az új NFC fenyegetésről angol nyelven ezen a linken olvashatók.

Szólj hozzá!
Címkék: pénz malware csalás átverés bankkártya számla trójai android adathalászat banki nfc welivesecurity.com

Ajánlott bejegyzések:

Jöhet-e QR kódos átverés postai papír levélben?
MBH-fiókjának jelszava 24 órán belül lejár
Árad a malware a Youtube oldalain is
MBH banki adathalászat

[Jöhet-e QR kódos átverés postai papír levélben?]

[MBH-fiókjának jelszava 24 órán belül lejár]

[Árad a malware a Youtube oldalain is]

[MBH banki adathalászat Replikák támadása]

[Replikák támadása]

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

[Tovább a Facebook-ra]

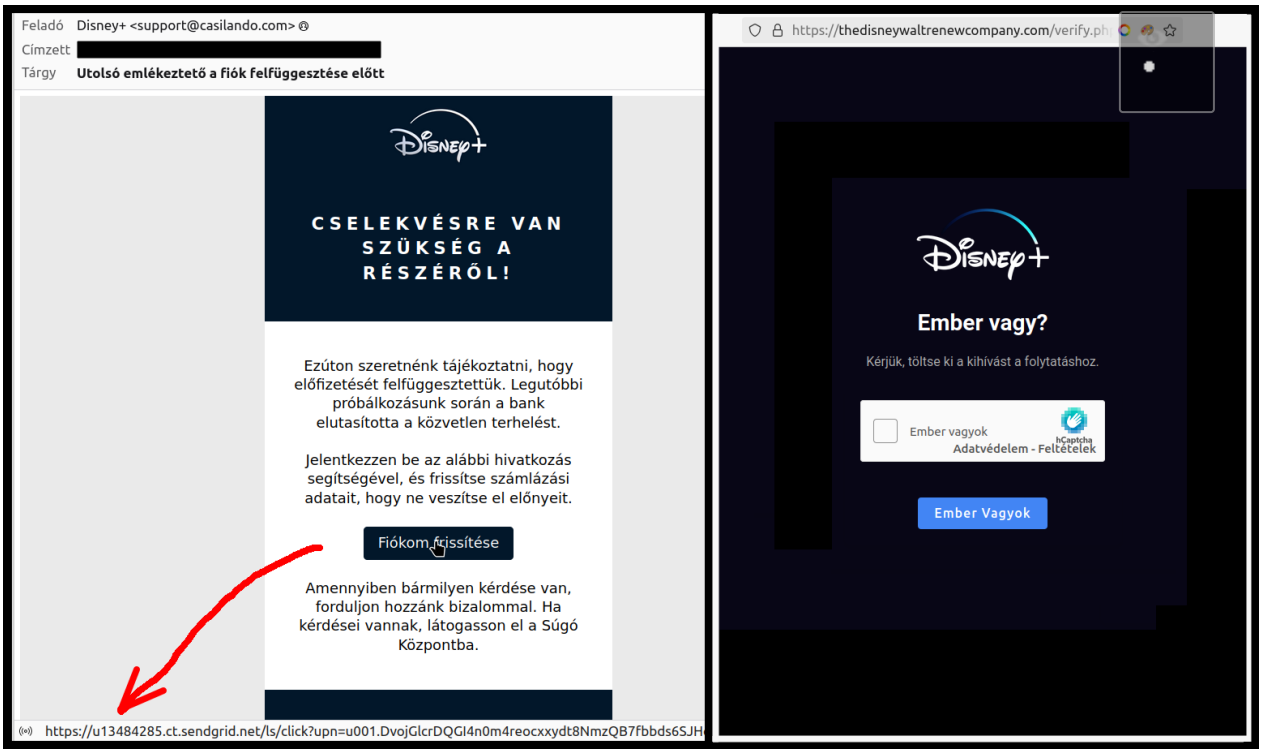
Utolsó emlékeztető a fiók felfüggesztése előtt

2024. szeptember 19. 11:26 - Csizmazia Darab István [Rambo]

Netflix témában már sok e-mail és SMS érkezett állítólagos felfüggesztésről, díj elmaradásról. **Ezúttal a Disney nevében jött az üzenet:** "Cselekvésre van szükség a részéről!"

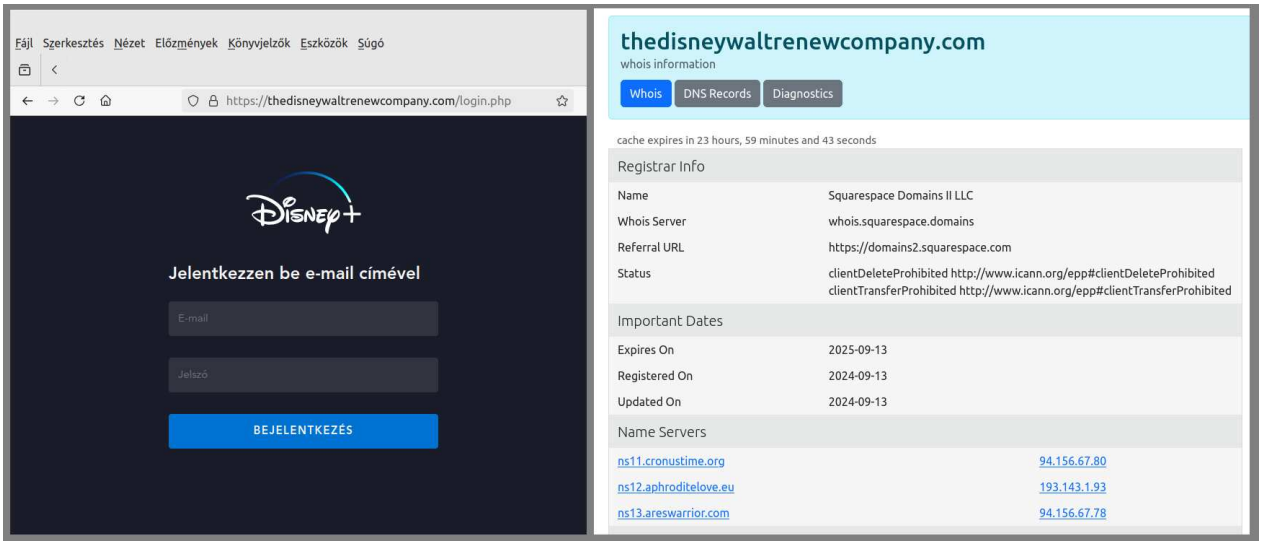
A nem éppen autentikusnak látszó support KUKAC casilando PONT com címről érkezett utolsó emlékeztető arról tájékoztat bennünket, hogy az Disney csatorna előfizetésünket felfüggesztették, mert a legutóbbi próbálkozásuk során a bank állítólag elutasította a terhelést.

Emiatt be kell jelentkezzünk a mellékelt linken és frissíteni a személyes, illetve banki adatainkat. És lám, milyen érdekes, a weboldal épp most, 2024. szeptember 13-án lett csak beregisztrálva.



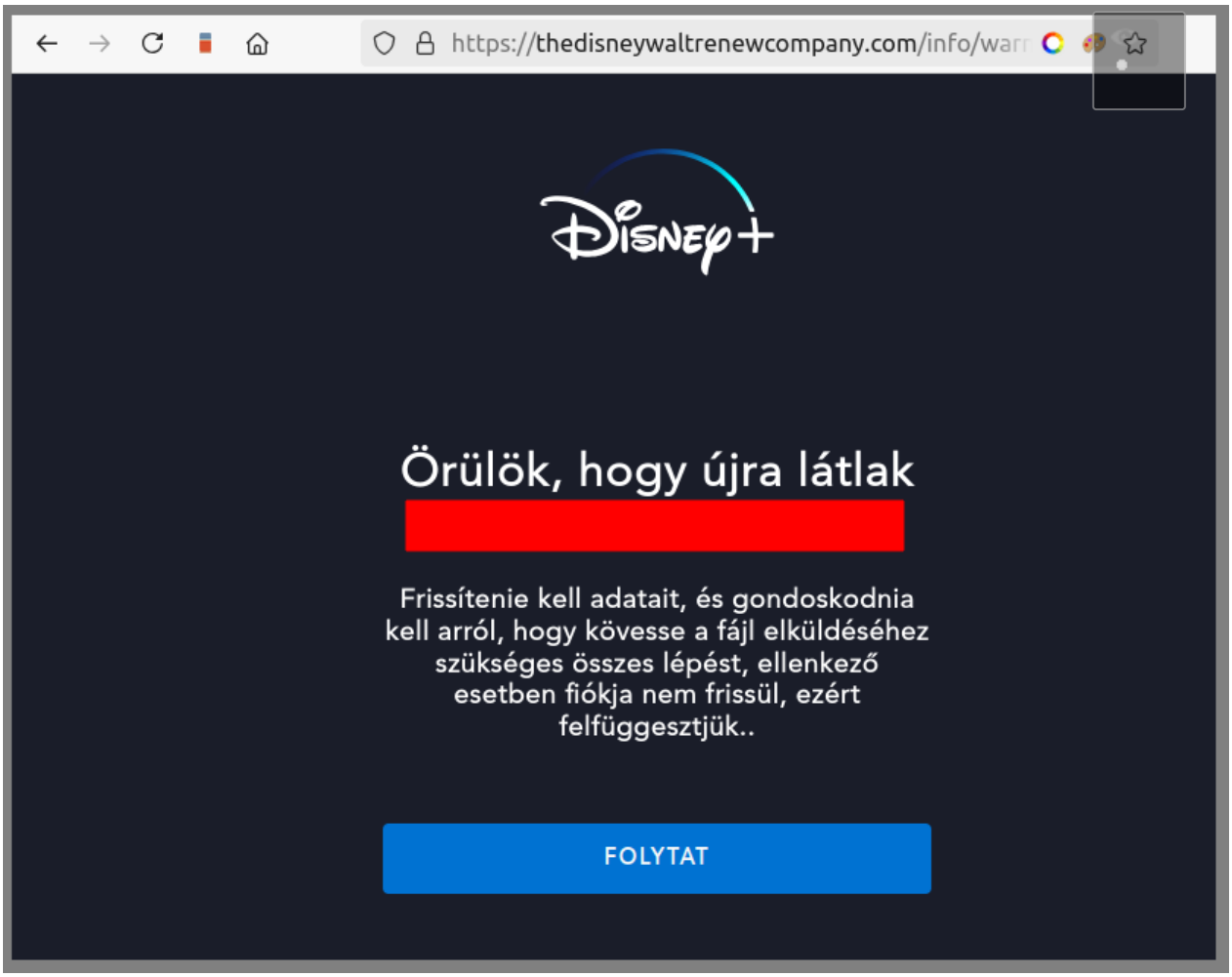
A levél alján az apró betűs részben vicces módon az alábbi kitétel is szerepel: "*A Disney tiszteletben tartja és védi a felhasználók személyes adatait. Ha bármilyen kérdése van személyes adatainak kezelésével és felhasználásával kapcsolatban, tekintse meg az Adatvédelmi Szabályzat és EU és Egyesült Királyság Adatjogok hivatkozásokat.*"

Biztos így is van. A kattintás a "Fiókom frissítése" gombra után az alábbi látvány fogadja az érdeklődőt.

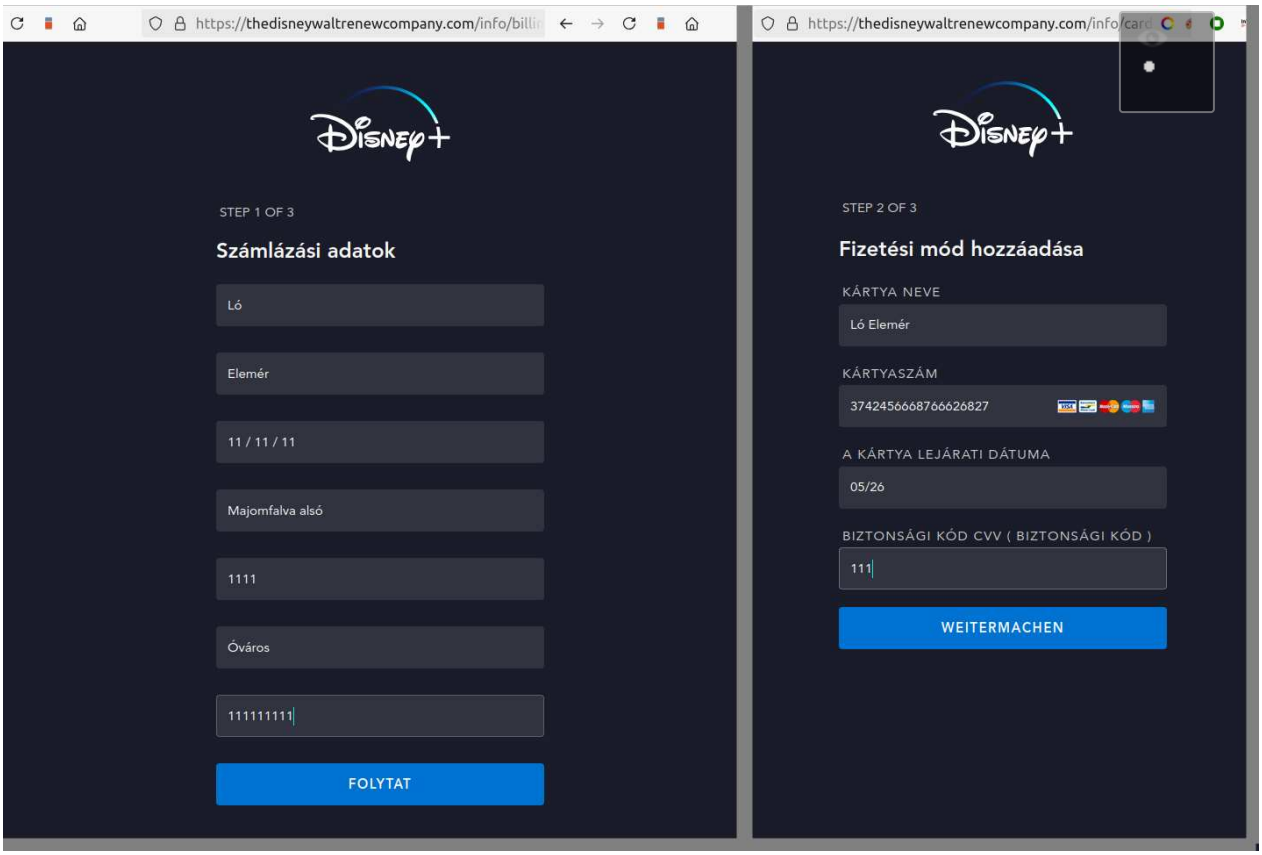


Itt egy Captcha kérés, ami segít elaltatni az éberséget, hogy talán mégis a hivatalos oldalon vagyunk, a csalók csak nem használnak ilyeneket. Ja de.

Ezután jön a név-jelszó páros begépelése, ami után szemlátomást nincs semmilyen kétfaktoros autentikáció, bárkinek az e-mail címét be lehet itt pötyögni.



Következő lépésként a személyes adatok begyűjtése bukkan fel: **jöhet a teljes nevünk, születési dátumunk, pontos lakcímünk irányítószámmal, és a telefonszámunk megadása.**



És ezzel is jutunk immár **a banki adatok bekéréséhez, ami jelen esetben a teljes bankkártya adatokat jelenti: kártyán szereplő név, kártyaszám, lejárati idő éve és hónapja, valamint a 3 jegyű CVV biztonsági kód.**

Izgalmas módon itt már nem a "FOLYTAT" gomb jelenik meg alul a jóváhagyáshoz, hanem ugyanez, csak németül "WEITERMACHEN". Ja, verstanden.

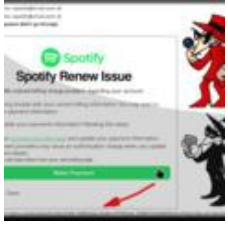
Ahogy a korábbi hasonló adathalász átverésekről szóló posztjainkban, **itt is ezernyi gyanús intő jel sorakozik fel: nem cégszerű a feladói cím, tömegesen küldték ki az üzenetet előfizetői státusztól függetlenül, a mellékelt link idegen weboldalra mutat, bikkfa nyelven és magyartalanul fogalmaztak, rafináltan minden mozdítható személyes adatunkat szeretnék bekérni, nem maszkolják el csillagokkal a CVV mezőt begépeléskor, és a szokásos fenyegetés-sürgetés is szépen megjelenik. Időközben a weboldalt már lelőtték.**

Zárásként jöjjön egy ideillő Disney idézet a L'ecsó rajzfilmből: "*A korlátokat te húzod meg*" - és ezt érdemes is lenne a hasonló szituációkban mindenkinek megtenni.

1 komment
Címkék: spam disney előfizetés e-mail csalás átverés adathalászat

Ajánlott bejegyzések:

Leveringa függesztés csomag részére



Leveringa függesztés csomag részére

Spotify megújítási probléma - vagy mégsem?

Netflix: lejárt a tagságunk. Vagy mégsem?

2023. első csalásai Ment a hűtlen hamis linkkel

Ment a hűtlen hamis linkkel

Ment a hűtlen hamis linkkel

Ment a hűtlen hamis linkkel

Kommentek:

Head Honcho 2024.09.20. 09:04:08

Ha a marhákat ezzel is meg lehet vezetni, akkor meg lesznek vezetve. Pont.

Válasz erre

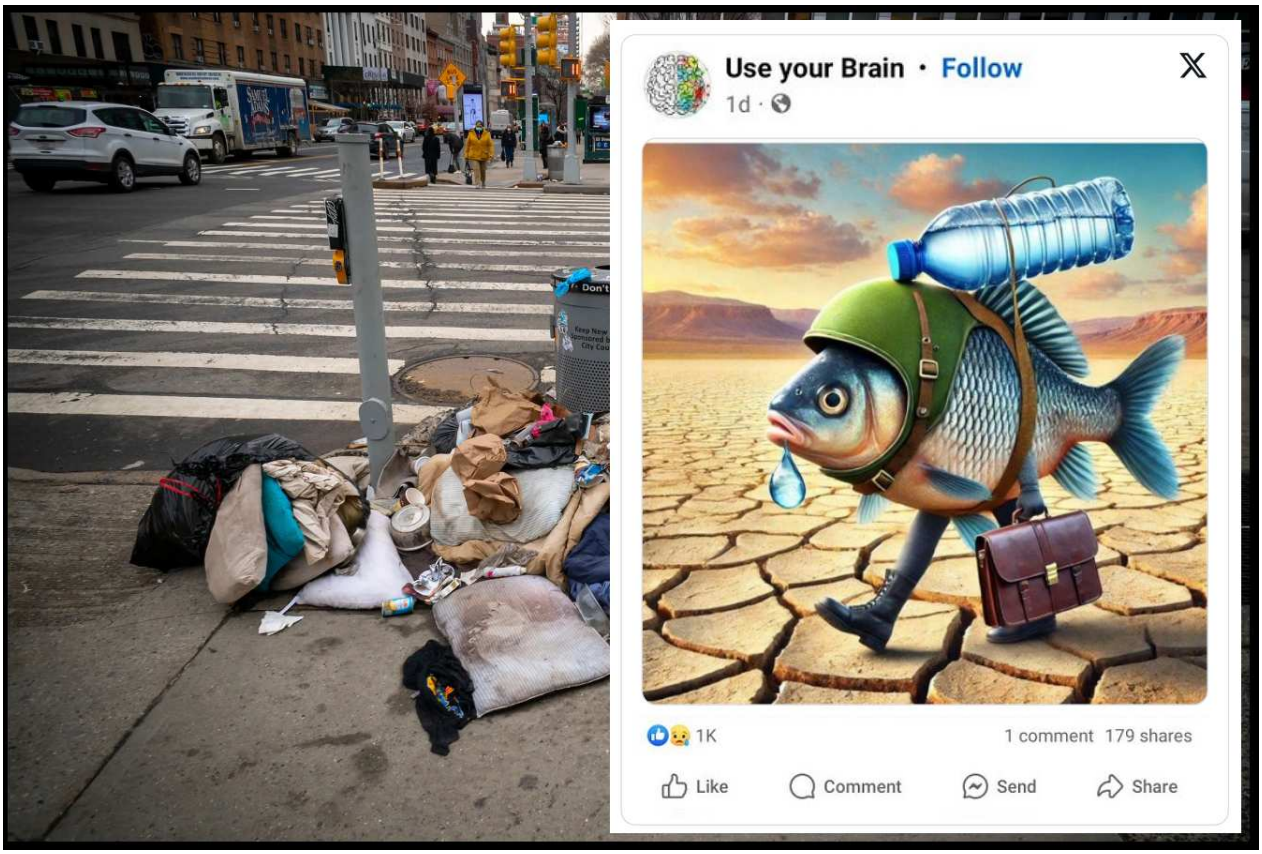
keresés

tweetz

Szemetelnek, szemetelnek...

2024. szeptember 24. 13:35 - Csizmazia Darab István [Rambo]

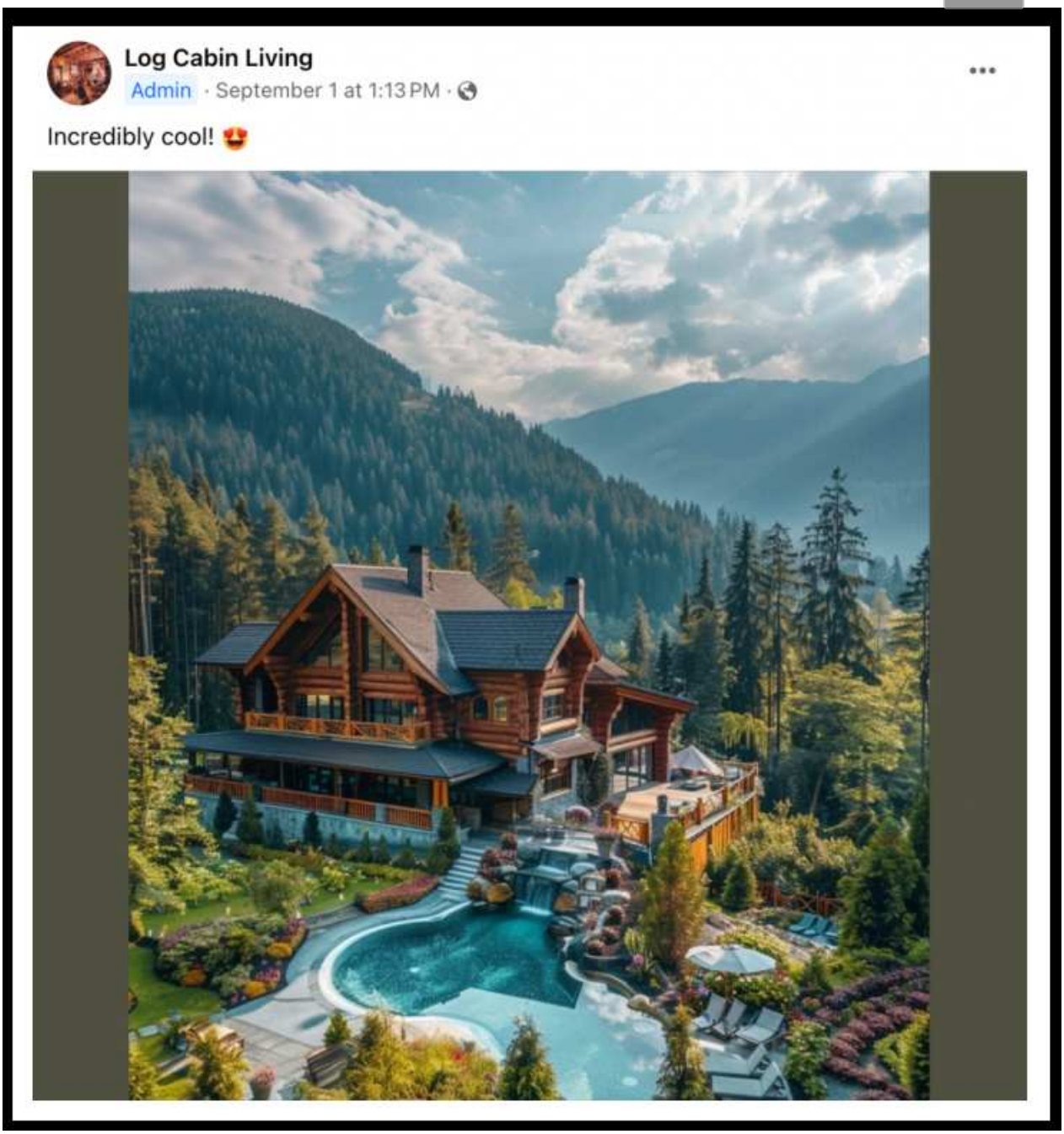
A mesterséges intelligencia által generált anyagok problémája rosszabb, mint elsőre gondolnánk. Nem csak a jobb-rosszabb képek száma növekszik exponenciálisan, de **a Facebook posztok ötöde is ilyeneket tartalmazó spamekből tevődik össze, szennyezik a normál kommunikációt.**



Megváltozott a világ immár sokadszorra. **Korábban jobban hihettünk legalább a szemünknek, ha az újság, a rádió, a televízió vagy az internet híreit nem is lehetett mindig/soha kritika nélkül elhinni. Aztán 1987-ben jött a Photoshop, amitől a képek módosíthatók manipulálhatók lettek, 2017-től a legelső Obamás példa láttán megismerkedtünk a deepfake videó fogalmával, amit ma már egyetlen állóképből is el lehet készíteni.**

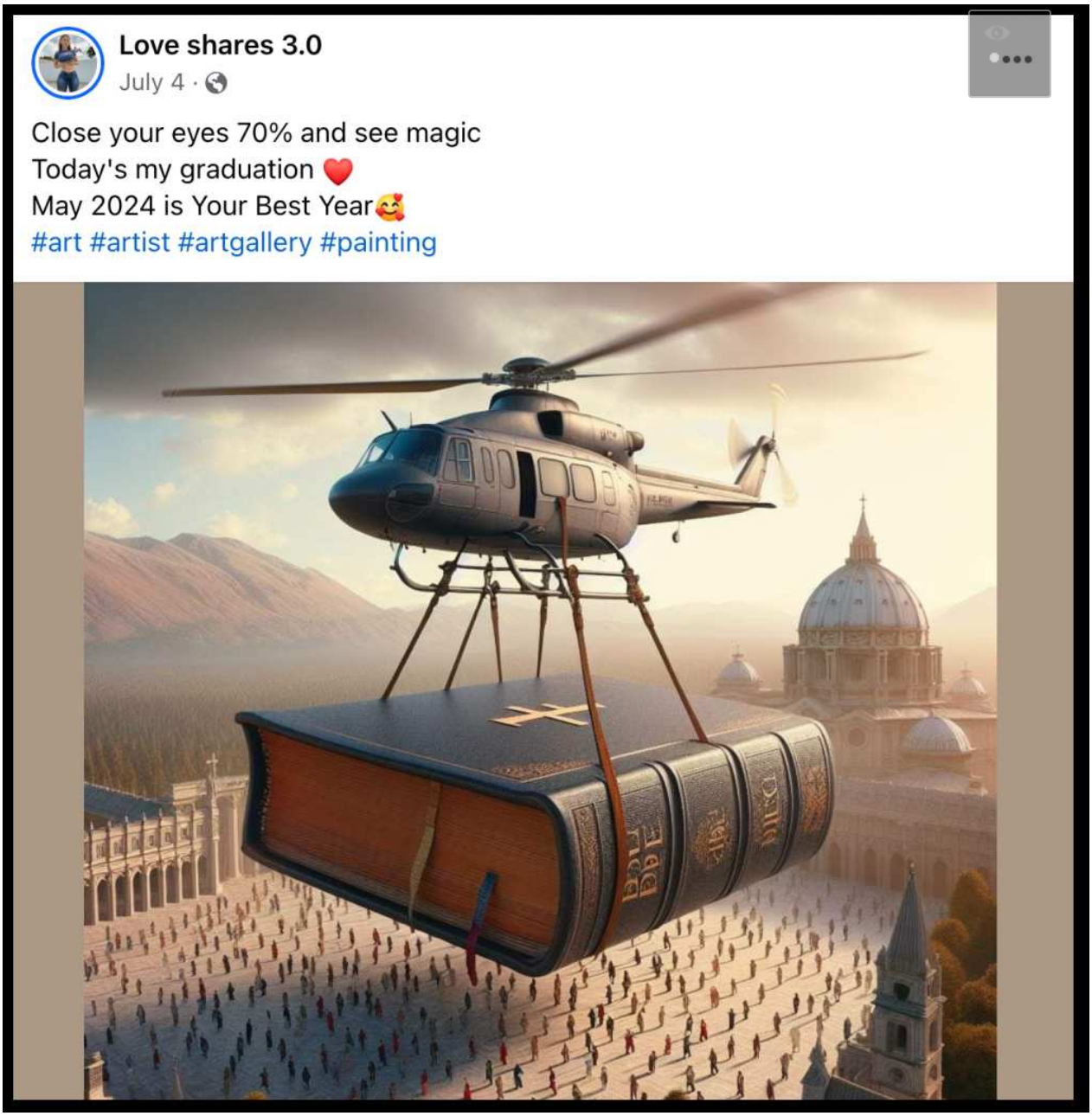
És egy **pár éve jöttek a villámgyors AI képgenerálási lehetőségek, amiket ma már szinte mindenki ismer: Dall-E, Tengr.ai, Midjourney, Leonardo.ai, Clipdrop, Wonder, Stable diffusion, Freepik,**

Dreamstudio, MS Bing, stb. És ezek egyre csak ontják a tartalmaikat például a közösségi oldalakon.



A hagyományos szakmai csoportokon felül, ahol a tagok rendszeresen megosztanak egymással generált képeket, **tucatszám tűnnek fel olyan profilok, amelyek bizarr képeket posztolnak, és több tízezres követőtábor veszi őket körül. A publikált képeik többsége valamilyen furcsaság.**

Például egy ilyen július 4-i kép látszólag a vatikáni Szent Péter-bazilika légi felvétele, lent a téren összegyűlt emberekkel. **Fejük fölött, egy gigantikus fekete helikopteren csüng egy óriás méretű Biblia**, bár a borítón a betűk eléggé torzak, ráadásul a megszokott kereszt emblémának van egy felesleges extra jobboldali nyúlványa is.



A bejegyzést posztoló "Love shares 3.0" nevű profil 71 ezer követővel rendelkezik, ami jelentős számnak látszik. A kép alatt viszont szemlátomást csak zavaros, zagyva szöveg olvasható, és semmi köze a fentiekhez: "*Csukd be a szemed 70%-ig, és lásd varázslatot / Ma van az érettségim / 2024. májusa a legjobb éved.*"

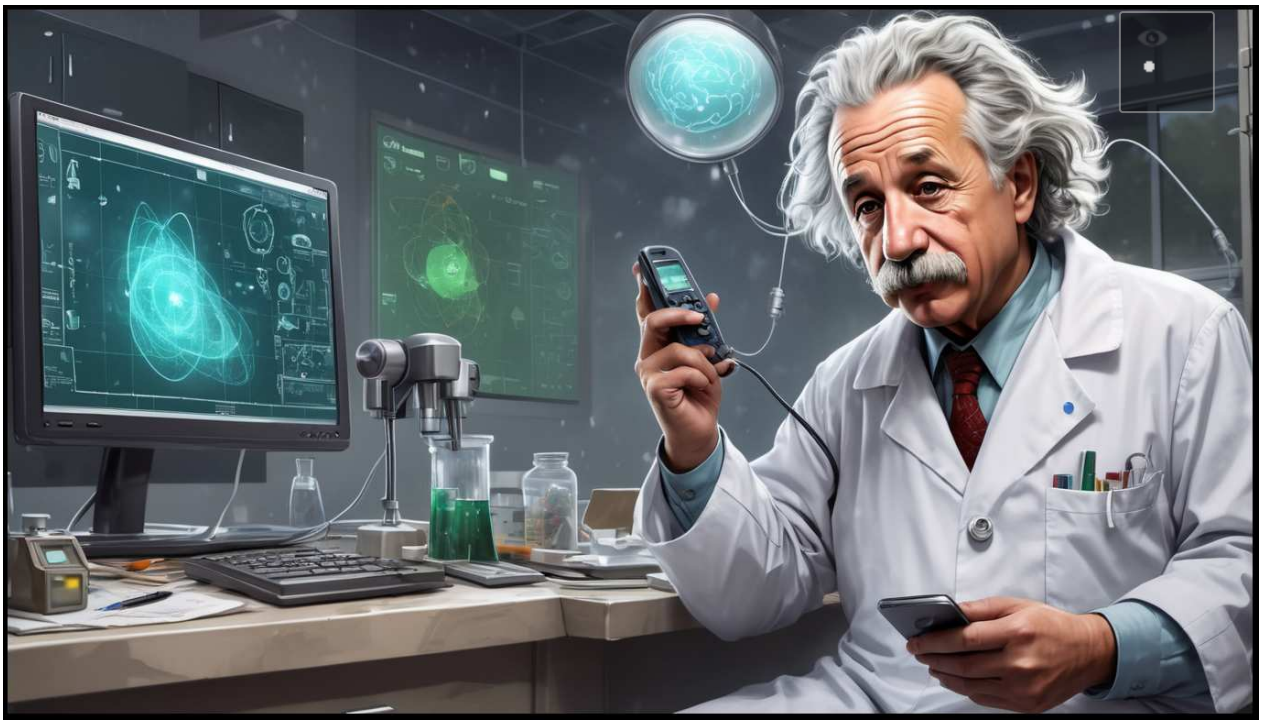
A mellékelt hashtagek is hamisak: #művészet, #festmény - azonban ordít a képről, hogy azt a mesterséges intelligencia segítségével alkották, ez a tény viszont már sokszor nem szerepel itt semmilyen formában. **A kép ennek ellenére több ezer lájkot, és szívecskét zsebelt be, sokan csak valami egyszavas kommenttel jelölték, például: "ámen", vagy osztották meg ismerőseiknek.**

Sokféle hasonló tartalom jelenik meg minden egyes percben: Bibliák, babák, amerikai zászlók, katonák, állatok, fényűző otthonok, lélegzet elállító tájak, kórházi ágyon fekvő betegek, otthontalanok, éhezők. Nem tudni, vajon a felhasználók tudatában vannak-e annak, hogy amiket látnak, annak semmi köze a valósághoz, mint például ez a **katonai teherautó, amely mintha óriási gigantikus répákat szállítana.**

Semmi értelme a képnek, ahogy a Pig Videos profil által mellékelt szövegnek sem: "*99 év szerencse, Soha nem lesz kevés a pénzed ahhoz, hogy utazhass*". A képhez aztán pedig végképp semmi köze nincs mindennek. De ott a 634 begyűjtött lájk.

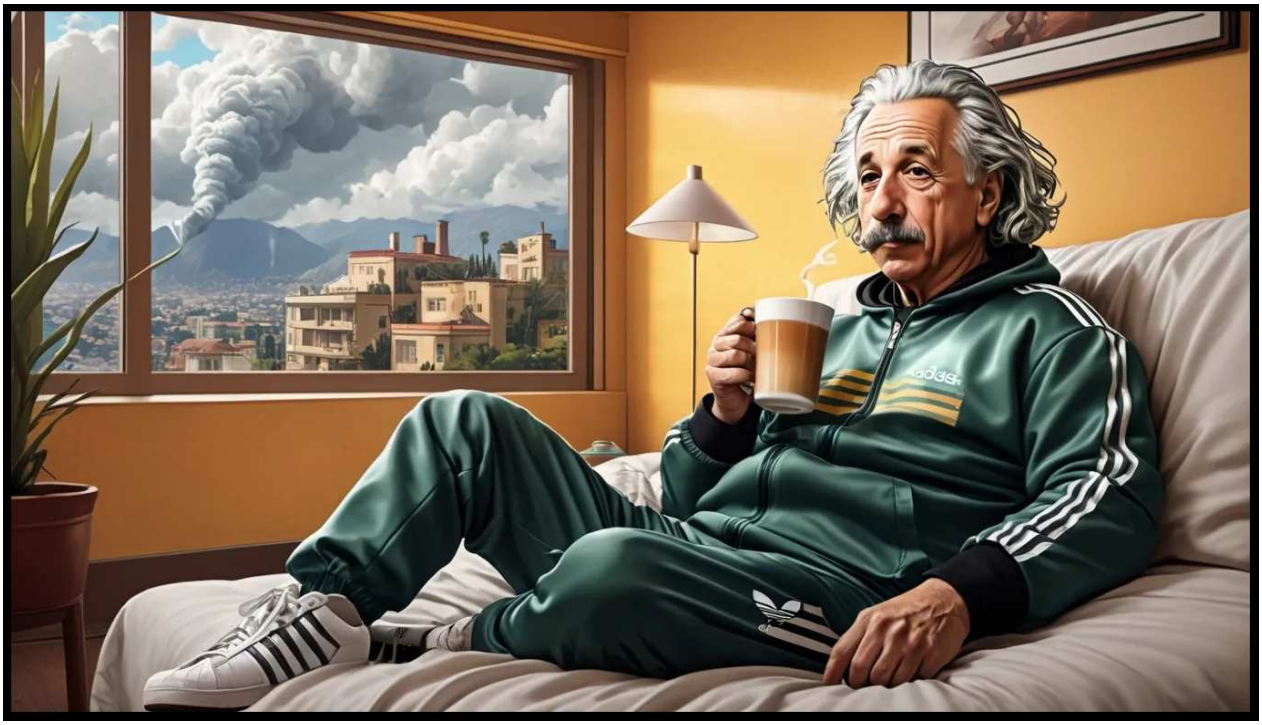
A Meta/Facebook nem igazán szűri ki vagy legalább címkézi fel ezeket a képeket mint "AI anyag", simán csak figyelmen kívül hagyják ezeket a mesterséges intelligencia által generált tartalmakat. A vezetőség ez ügyben nagyjából azzal érvel, hogy **mivel a manipulált tartalom közvetlenül nem sérti a közösségi normáikat, így nem korlátozzák feleslegesen a szólásszabadságot**, de folyamatosan vizsgálják a lehetőségeket, egyelőre automatikusan csak a saját eszközeikkel generált képeket címkézik fel.

Az ilyen jellegű kéretlen tartalmakkal kapcsolatban a RollingStone kérdésére azt válaszolták, hogy a spamek felszámolása szinte lehetetlen feladat, ennek ellenére ők mindent megpróbálnak, például 2024. első negyedévében 436 milliót távolítottak el ezekből.



Ezek a kártékony profilok gyakran azzal a forgatókönyvvel működnek, hogy eleinte ilyen képeket közölve felhizlalják a követői tábort. Ezzel sokféle céljuk lehet: reklámbevételekre utaznak, felhasználói adatokat akarnak begyűjteni, vagy amikor már jelentős számú követővel rendelkeznek, akkor már direkt politikai üzenetekkel jelentkeznek, például az amerikai vagy más országbeli választásokat befolyásoló tartalmakkal.

Ehhez a profil vagy csoport nevét is bármikor megváltoztathatják, például "Szavazz a Bolsonaro-ra" lesz belőle. Ráadásul az ilyen kamu fiókoknak, csoportoknak jelentős feketepiaca is van, manipulációs célokra adják-veszik ezeket.



A cikk szerint a folyamat fő részesei és áldozatai az idősebb korosztály, amelyik gyanútlan, és nem rendelkezik kellő biztonságtudatossággal. Lényeges lenne, hogy az intő jeleket mindenki képes legyen felismerni, és tudatosabban navigáljon a kibertérben. **Annak is gyanúsnak kell lennie, ha egy adott profil naponta több száz posztot hoz létre, ilyenkor joggal gyanakodhatunk valamilyen automatizált spammelésre.**

Azt pedig már egy korábbi tanulmányban is láttuk, hogy a hamis hírek gyorsabban terjednek a közösségi médiában, mint az igazi információk. A fentiek fényében fontos, hogy az alap kibervédelem mellett azt is **végiggondoljuk, mit lájkolunk, mit kommentelünk, mire iratkozunk fel, mit osztunk meg, vagy mit osztunk tovább. A profilunkra nem csak saját magunk miatt vigyázunk, hanem ezzel az ismerőseinket is védjük a nemkívánatos hatásoktól: adatszivárgástól, csalásoktól, átverésektől, manipulációktól.**

Szólj hozzá!
Címkék: média spam kép ai csalás átverés mesterséges mesterséges intelligencia közösségi generálás

Ajánlott bejegyzések:

Virtuális emberrablás, igazi károkozás
3000%-kal több lett, maradhat?
Halló, itt Joe Biden, vagy mégsem?

Virtuális emberrablás, igazi károkozás
3000%-kal több lett, maradhat? Az AI használat árnyoldalai
Halló, itt Joe Biden, vagy mégsem?
Na de mit adott nekünk a ChatGPT?
Az AI használat árnyoldalai

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink

Hogyan védjék magukat az idősebbek az interneten?

2024. szeptember 26. 18:21 - Csizmazia Darab István [Rambo]

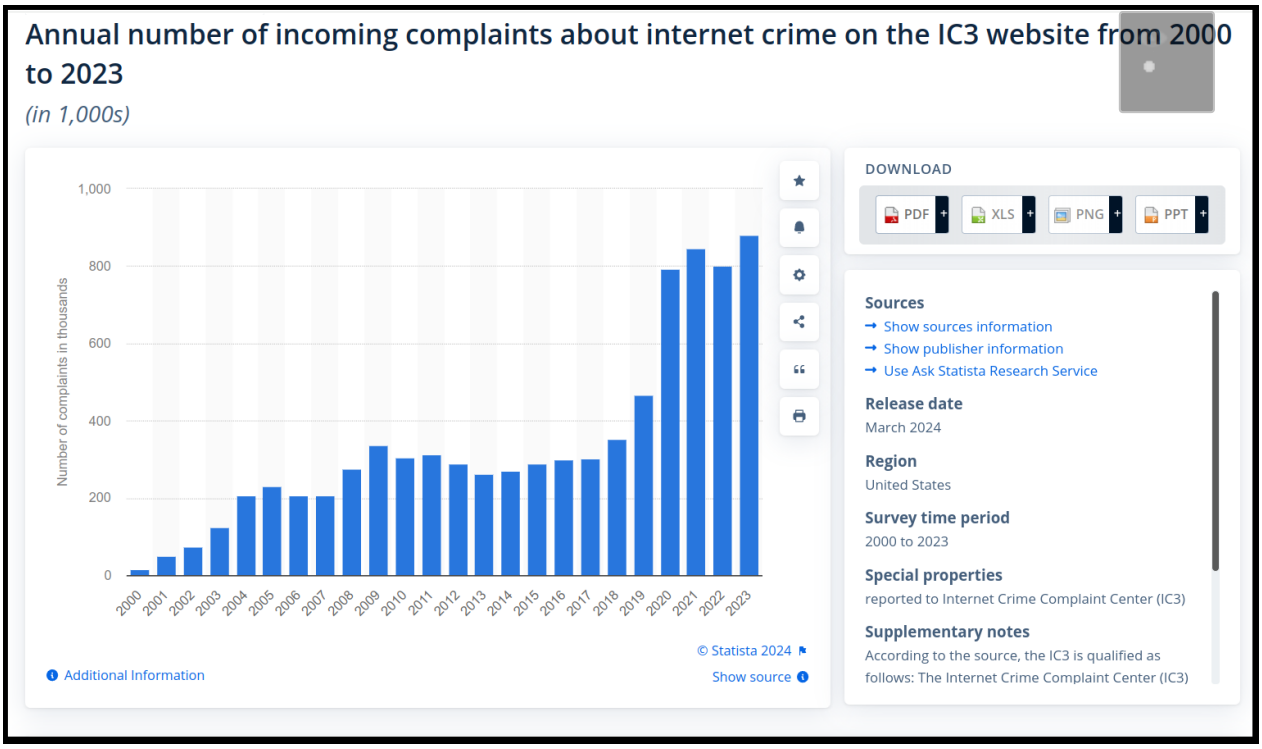
Különösen sebezhetők az idős emberek az online csalásokkal szemben. **A csalók kihasználhatják e korosztály hiszékenységét, számítógépes ismereteik a hiányosságát, akik jóhiszeműek, és nincsenek felkészülve ilyen töméntelen mennyiségű csalási kísérletre.**

A biztonságtudatosság egyfajta tudatos, előzetes ismereteken, tapasztalatokon alapuló óvatosság, gyanakvás. Hasonlóan a félelemhez, fontos hogy legyen, de a mértéke is fontos. Ha valakiben egyáltalán nincs félelem (épület tetejéről ejtőernyővel ugrál, biztosítás nélkül sziklát mászik, barlangi búvárkodásban leli örömét) **az ugyanannyira lehet kiemelten kockázatos**, mint aki mindentől akár ok nélkül is fél (pl. agorafóbia, bénító félelem a zsúfolt vagy zárt terektől).

Itt egy **egészséges középút az optimális megoldás, az szolgál bennünket a leghatékonyabban.**

A másik kiinduló pont a generációk kérdése, és most semmiképpen nem a szigorú határvonalakkal megemlítve ezeket. A Boomer, az X, az Y, a Z, az alfa generációk egy adott időszakban született emberek egy csoportját jelölik, amikre közösen az lesz jellemző, hogy milyen viszonyok közé születtek, és ez alapján mit tartanak szokásosnak, "normálisnak". **Ezek a generációs címkék nem minősítések, nincs semmilyen negatív tartalmuk, és ami a legfontosabb, hogy nem életkort jelölnek. Az alfa generációsoknál például nem az számít, hogy most tizenévesek, hanem az 40 év múlva is alfa generációsok lesznek, akik egy adott technológia fejlődési helyzetbe születtek bele, és mit szoktak meg, milyen közös élmények a meghatározók számukra: milyen filmeket láttak, milyen könyveket olvastak, milyen viszonyok és lehetőségek voltak adottak a tanuláshoz, szórakozáshoz, utazáshoz.**

Ez teljesen más lesz annál a csoportnál, akik még fekete-fehér, hétfői adásszünetes tévé időszakában töltötték a gyerekkorukat, és gyökeresen különböző például a mai tinédzserek között, ahol mindenki a kezében mobiltelefonnal közlekedik, a világban szabadon utazhatnak, 0-24-ben interneteznek. Ezek az élmények, körülmények, mozgató rugók nemhogy generációnként erősen különbözőek, hanem sokszor érthetetlenek, ismeretlenek is a többi másik életkori csoportnak.



És innen várjuk el azt, hogy abban mai világunkban, ahol szinte minden hivatalos és magán ügyünket, vásárlásainkat, kapcsolattartásainkat online intézzük, ahonnan percenként érkeznek támadások, átverési kísérletek a számítógépünkre, e-mailben, SMS-ben, élő hívásban, mindenki magabiztosan és biztonságtudatosan reagáljon ezekre.

A csalók pedig tudatosan kihasználják az idősek hiszékenységét, illetve egyes esetekben az öregedés okozta kognitívképesség-romlást.

Ebben a legfrissebb adásunkban ezt a témát jártuk körül, és a helyzet bemutatás mellett igyekeztünk praktikus tanácsokat is adni a hatékony

védekezéshez, megelőzéshez. **A Hackfelmetszők Podcast 23. idősek internetes biztonságával** foglalkozó adását az alábbi linken lehet meghallgatni.

A **korábbi, szintén IT biztonságról szóló podcast adások pedig itt találhatóak.**

Szólj hozzá!
Címkék: biztonság internet podcast idősek eset sicontact biztonságtudatosság hackfelmetszők

Ajánlott bejegyzések:

Hogyan lehetünk jó digitális szülők?

Mit csinálnak az alkalmazottak a céges gépeken?

Közeli helyeken: érintésmentes fizetések

A védelmező - kell nekünk?

Közeli helyeken: érintésmentes fizetések

A védelmező - kell nekünk?

Black Friday és Cyber Monday járja be Európát

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Afterparty: sosem késő

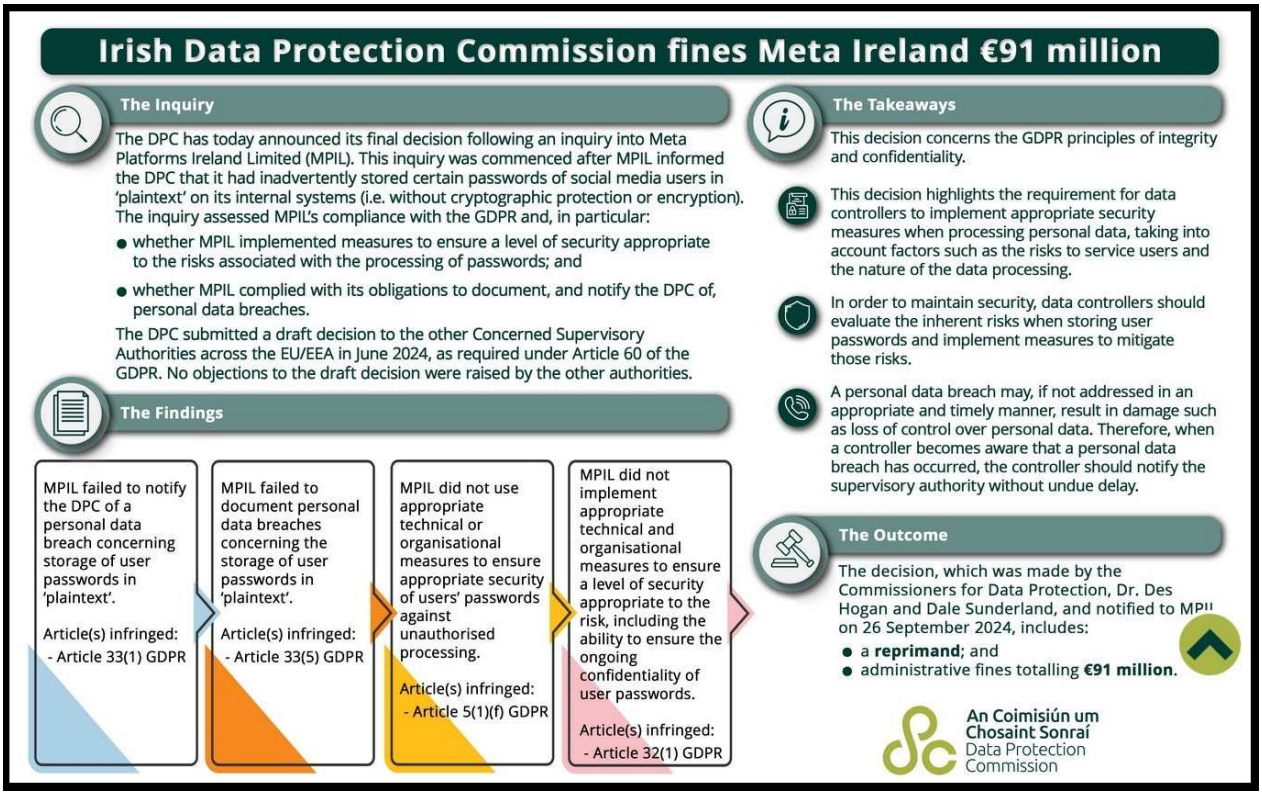
2024. október 01. 10:02 - Csizmazia Darab István [Rambo]

A Data Protection Commission (DPC) **91 millió eurós bírságot szabott ki a Meta-ra**. És hogy mi volt az oka? Egy öt évvel korábban megállapított incidens miatt történt, ahol az derült ki, hogy **TADAAAAM - a szervereiken sima szövegben tárolták a felhasználói jelszó adatbázist.**

Mindig az az alap feltételezése az embernek, hogy a Mikulás igenis létezik, maga a Húsvéti nyúl hozza tojást, a szakács mindig kezet szokott mosni WC után, és hogy a multicégeknél akkora gigantikus büdzsé és olyan hibátlan szakember gárda áll az IT biztonság rendelkezésére, hogy ott sosem történhet informatikai incidens valamilyen primitív mulasztás, vagy súlyos kötelezettségszegés miatt.

2019-et írtunk, mikor kiderült, hogy a Facebook [több száz millió felhasználó jelszó adatát tárolta egyszerű szöveg állományban](#) **a vállalat belső szerverein, mindezt legalább 2012. óta, amelyhez a dolgozók mindenféle hozzáférési külön engedély nélkül hozzáférhettek.**

Az akkori becslések szerint [200-600 millió Facebook-felhasználó fiók jelszavát tárolták így, és ezekben több mint 20 ezer akkori Facebook-alkalmazott szabadon](#) keresgélhetett.



Az ügyre most került pont, ugyanis az írországi adatvédelmi felügyeleti hatóság 91 millió eurós (mai áron nagyjából 36 milliárd forintnak megfelelő) pénzbírságot szabott ki a Meta-ra azzal az indoklással, hogy a közösségi média felhasználóinak bizonyos jelszavait "kriptográfiai védelem vagy titkosítás nélkül" tárolták a belső rendszereiken.

Ez hozzávetőlegesen **sok százmillió Facebook Lite, több tízmillió más Facebook felhasználót, illetve több millió Instagram ügyfelet érintett.**

A vizsgálatok eredménye szerint a jelszavak illetéktelenek számára is könnyen hozzáférhetők voltak, de nem találtak konkrét visszaélésre vagy külső hozzáférésre utaló bizonyítékokat.

A felhasználói fiókok jelszavának megfelelő védelem nélküli tárolása az Általános Adatvédelmi Szabályzat (GDPR) több cikkelyének megsértését jelenti, és **a hatóság emellett azt is felrótta a cégnek, hogy túl későn jelentette be az esetet, valamint nem dokumentálta azt megfelelően.**

Jó öt évvel később most szabták ki emiatt ezt a 91 millió eurós közigazgatási bírságot, ami már egy ekkora cég számára is egy szabad szemmel jól látható összeg.

Korábban is álltak már a szőnyeg szélén, **például [2023-ban kapott a Meta egy 1.2 milliárd eurós GDPR bírságot](), akkor azért, mert az európai ügyfelek személyes adatait a szabályozás ellenére folyamatosan továbbította az Egyesült Államokba.**

Szólj hozzá!
Címkék: adatvédelem facebook büntetés meta bírság mulasztás jelszavak cleartext gdpr

Ajánlott bejegyzések:

[Cselekedettel és mulasztással II.](#)

[Betegeskedő egészségügyi alkalmazások](#)

[Szolgálunk és nem védünk](#)

[Matatás a robotporszívók agyában](#)

[Cselekedettel és mulasztással II.](#)

[Betegeskedő egészségügyi alkalmazások](#)

[Hiba a 8-ik rétegben](#)

[Hiba a 8-ik rétegben](#)

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

A vízszámla érintése

2024. október 08. 16:55 - Csizmazia Darab István [Rambo]

A közüzemek elleni kibertámadásoknak már külön fejezete van, és **ebbe sorba került most egy újabb aktuális tétel. Az Egyesült Államokban üzemelő vízszolgáltató cégnél ezúttal a MyWater számlázási rendszer esett el.**

Egy nagyon régi iromány szerint a dihidrogén-monoxid egy roppant veszélyes anyag, nem árt vigyázni vele ;-) Ha valaki esetleg nem ismerné a történet eredetét, belinkeltük az ezzel kapcsolatos akkori felhívást, amelyben **támogató aláírásokat gyűjtöttek az azonnali betiltására.**

Még akár azt is mondhatnánk, hogy "szerencsére" **csak a számlázást kellett leállítani és nem magát a vízműveket. Az American Water egyébként 14 millió ember ivóvíz ellátását végzi, és a mostani kibertámadás miatt lekapcsolni kényszerültek a számlák kiállítását végző számítógépes rendszereiket.**

A pályázó ötven embert kérdezett meg, hogy támogatná-e a vegyszer betiltását. Negyvenhárom igennel válaszolt, hat nem tudott dönteni, és csak egy jött rá, hogy a dihidrogén-monoxid egyszerûen víz.

TILTSÁK BE A DIHIDROGÉN-MONOXIDOT!

A LÁTHATATLAN GYILKOS

A dihidrogén-monoxid színtelen, szagtalan, íztelen, és ezreket pusztít el minden évben! A halált legtöbbször az okozza, hogy a DHMO véletlenül a tüdôbe kerül, de ezzel a dihidrogén-monoxid ártalmai korántsem merültek ki. Abban a testrészben, amelyik hosszan érintkezik a szilárd DHMO-val, súlyos szövetkárosodás jöhet létre. Ha a DHMO az emésztôrendszerbe jut, túlzott izzadás és vizeletkiválasztás következhet be, de felfúvódás, hányinger, hányás is elôfordulhat. A DHMO-dependencia kialakulása után a szer megvonása biztos halált jelent.

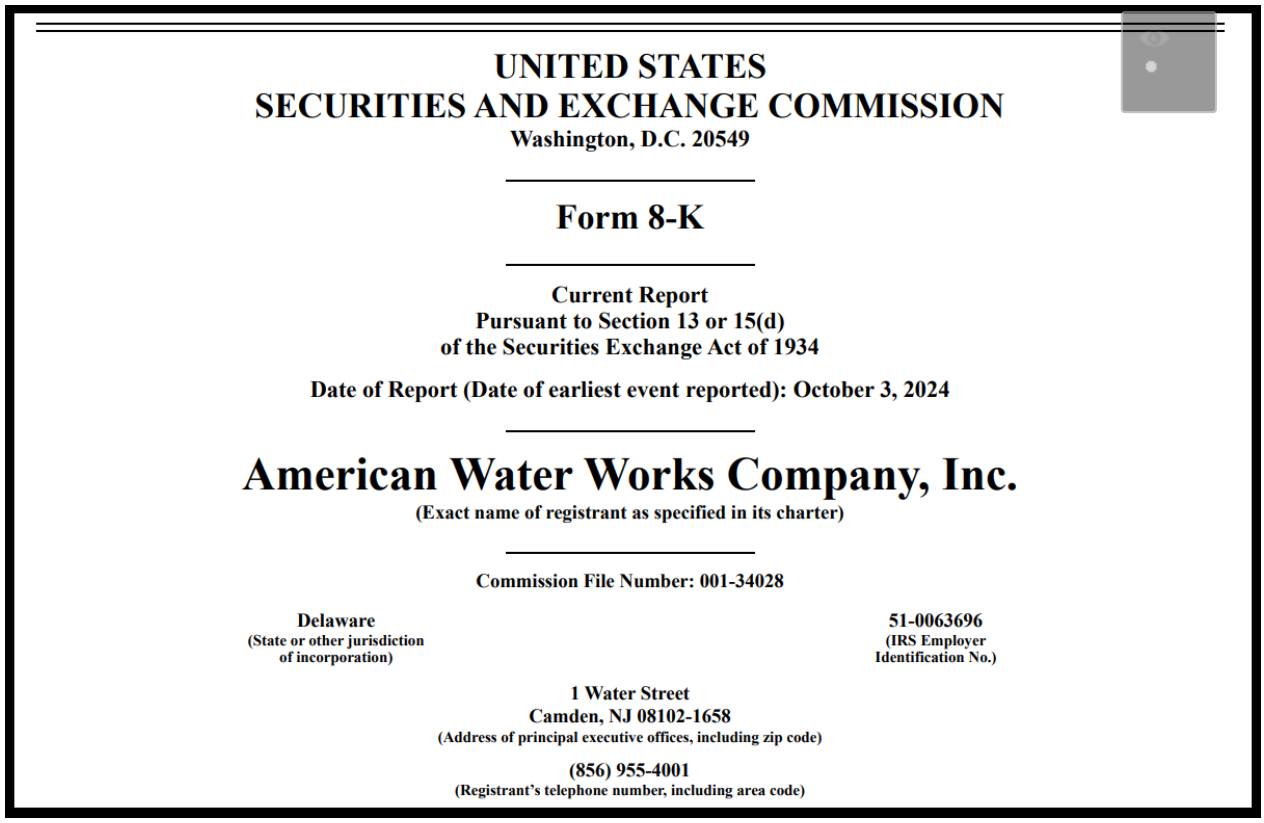
A dihidrogén-monoxid

- savként is ismert, és a savas esô fô komponense,
- hozzájárul az üvegházhatáshoz,
- súlyos égést okozhat,
- hozzájárul természeti környezetünk eróziójához,
- számos fém korrózióját, rozsdásodását sietteti,
- hibát okozhat az áramszolgáltatásban, rontja az autók fékhatását,
- rákos daganatokban is kimutatható.

A SZENNYEZÉS JÁRVÁNYSZERÛ MÉRETEKET ÖLT!

A hivatalos közlemény úgy fogalmaz, hogy vizsgálják az incidens körülményeit, ezt azonban nem részletezték bővebben, **így azt sem tudni, hogy konkrétan zsarolóvírusról van-e szó. Azt viszont leszögezték, nem találtak bizonyítékot arra, hogy valamely víz- vagy szennyvízellátó létesítményük biztonságos működése ezáltal veszélybe került volna.**

A www.amwater.com weboldal mindenesetre a cikkünk írása idején pillanatnyilag elérhetetlennek bizonyult.



UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

Form 8-K

Current Report
Pursuant to Section 13 or 15(d)
of the Securities Exchange Act of 1934

Date of Report (Date of earliest event reported): October 3, 2024

American Water Works Company, Inc.
(Exact name of registrant as specified in its charter)

Commission File Number: 001-34028

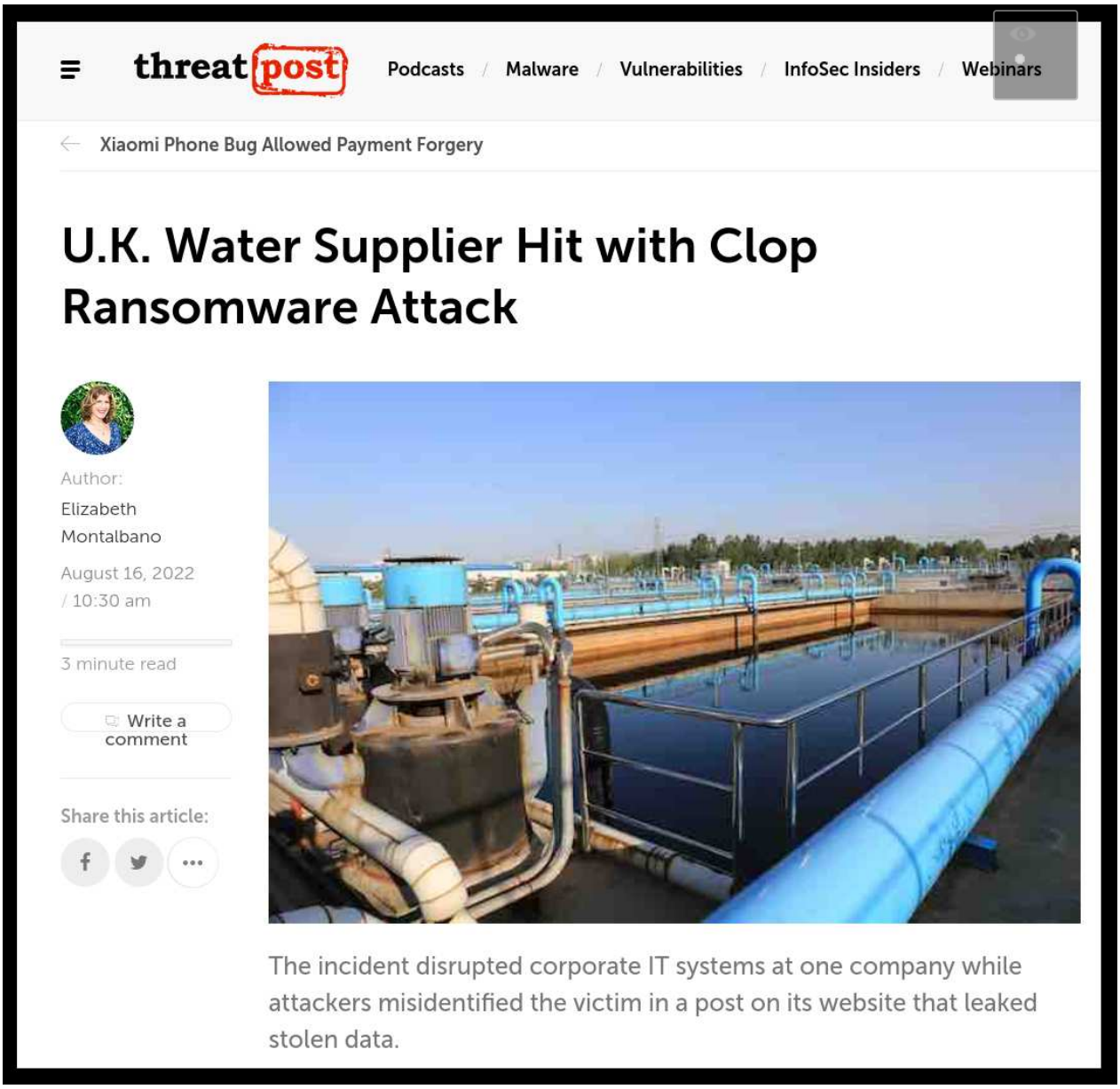
Delaware	51-0063696
(State or other jurisdiction of incorporation)	(IRS Employer Identification No.)

1 Water Street
Camden, NJ 08102-1658
(Address of principal executive offices, including zip code)

(856) 955-4001
(Registrant's telephone number, including area code)

Az eredetileg még október 3-án észlelt támadásról azonnal értesítették hivatalosan a hatóságokat, és külsős kiberbiztonsági szakemberek bevonásával elkezdték az incidens alapos kivizsgálását.

Addig is, amíg ez a nyomozás zajlik, és a számítógépes számlázási rendszerek nem állnak ismét teljeskörűen rendelkezésre, **a cég szóvivője azt ígérte, nem számítanak fel semmiféle késedelmi díjat az ügyfeleiknek.**



Ha visszatekintünk a hasonló kaliberű támadásokra, akkor emlékezhetünk, hogy 2022-ben a South Staffordshire nevű brit vízszolgáltató céget érte ransomware támadás, **2023-ban pedig egy pennsylvaniai vízrendszer ellen történt atrocitás**, ahol iráni elkövetők belematattak az ottani vezérlésbe.

Azt sajnos nem lehet nem észrevenni, hogy **a hasonló alap infrastrukturális létesítmények roppant vonzó célpontjai a ransomware támadásoknak**, így bizonyos, hogy nem most hallottunk ilyen ijesztő incidensről utoljára.

Szólj hozzá!
Címkék: usa vízművek ransomware közművek kibertámadás

Ajánlott bejegyzések:

A távolságot mint üveggolyót nem kapod meg

100 millió ember egészségügyi adata hoppszi

Az élet szép, de a Life360-nak vannak gondjai

A távolságot mint üveggolyót nem kapod meg

Tíz tiszta víz, ha nem tiszta, vidd vissza

100 millió ember egészségügyi adata hoppszi

Az élet szép, de a Life360-nak vannak gondjai

Úgy hívnak motorizált nemzedék...

Úgy hívnak motorizált nemzedék...

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

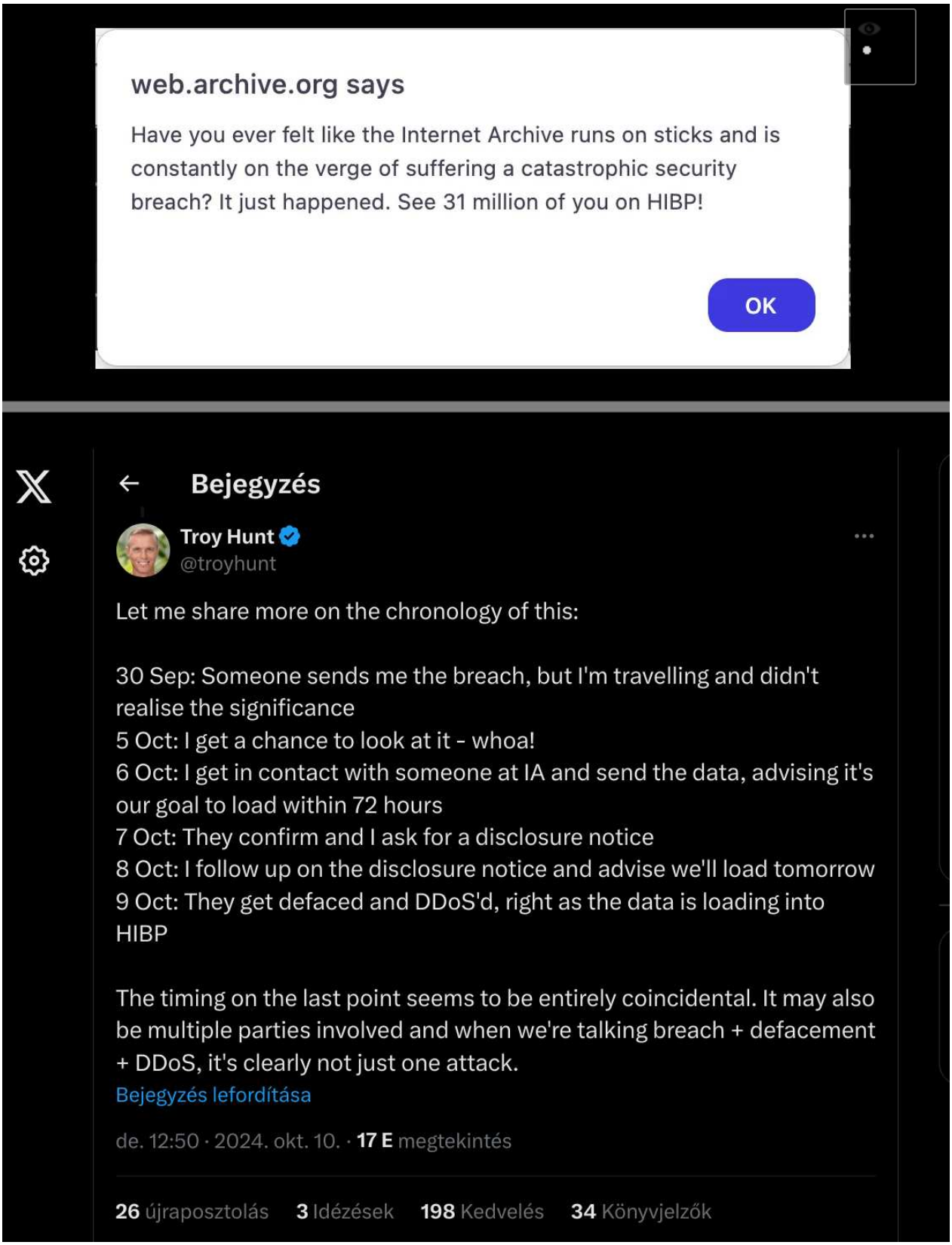
Elveszett ereklyék fosztogatói

2024. október 10. 15:02 - Csizmazia Darab István [Rambo]

Ha váratlanul lehal, megszűnik egy weboldal, esetleg szándékosan letörlik, ez esetben egy vagy akár több korábbi állapotát is képes megőrizni az internet emlékezetének is nevezett Internet Archive, **más néven a "The Wayback Machine".**

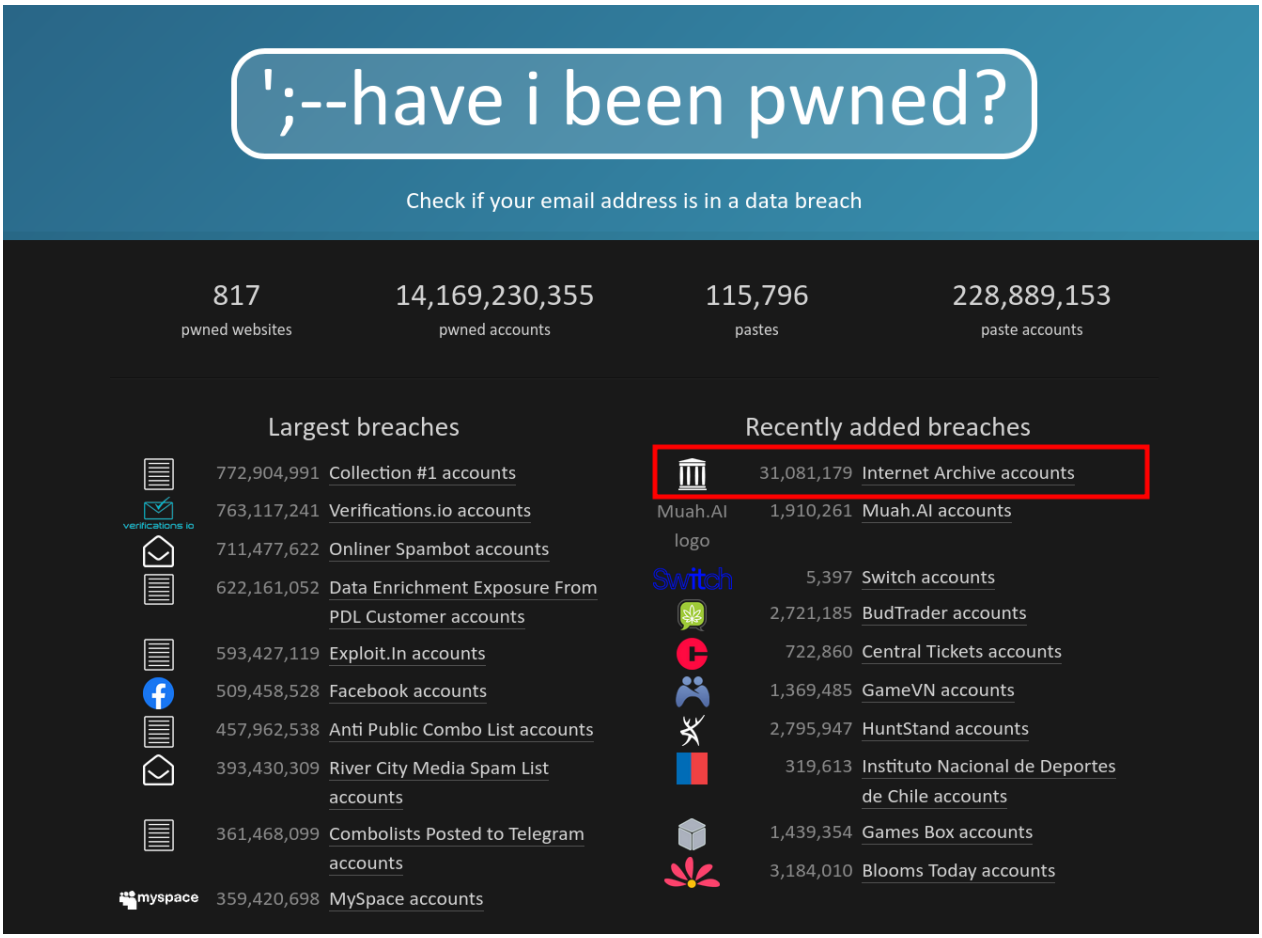
Ezt a webhelyet érte támadás a közelmúltban, amelyről egy felbukkanó JavaScript ablak értesítette a látogatókat. Érezte már valaha, hogy az Internet Archive biztonsága katasztrofálisan gyenge lábakon áll? Az üzenet szerint látogassunk el a HIBP oldalra, és **megláthatjuk, van ott 31 millió újabb, erről a helyről kiszivárgott account.**

Ami igaz is, **a Haveibeepwned frissen hozzáadott és visszaigazolt tételeinél valóban szerepel az IA anyaga.**



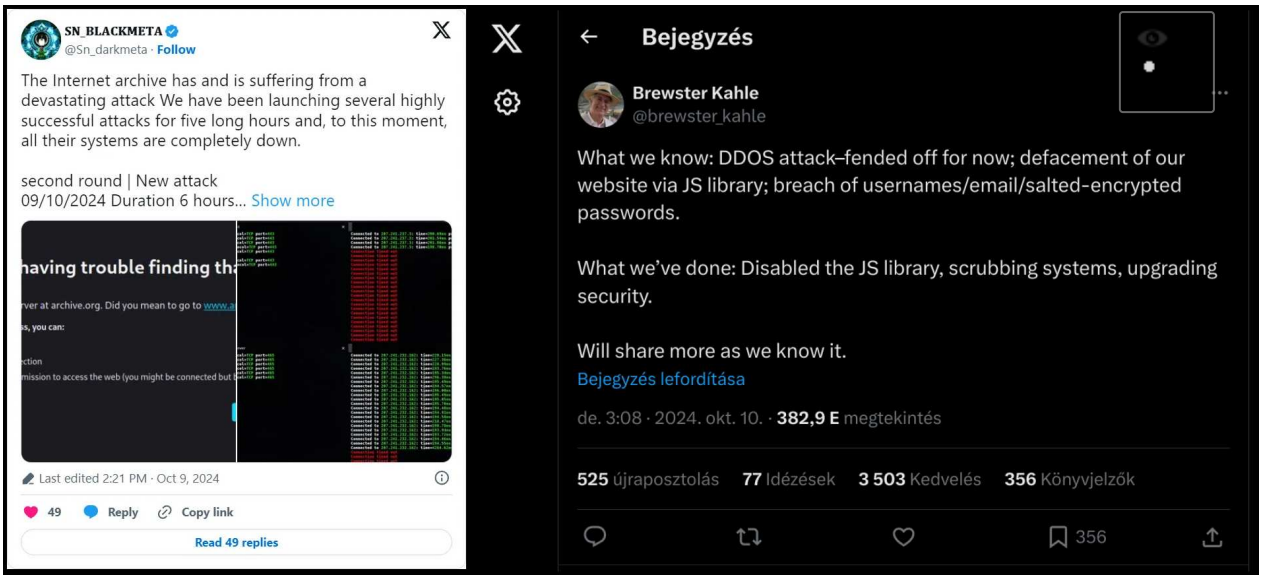
Ezt maga az admin, Troy Hunt is megerősítette, valóban érkezett hozzájuk egy 6.4 GB-os "ia_users.sql" nevű SQL-fájl. **Az adatbázis hitelesítési információkat tartalmaz a regisztrált tagok számára, beleértve az e-mail címeket, nickneveket, jelszóhasheket és egyéb a belépéssel kapcsolatos belső adatokat.**

Az állományban található időbélyeg adatok alapján **valószínűleg szeptember 28-án történhetett a betörés**. **Akinek van itt regisztrált fiókja, érdemes lehet ellenőriznie, hogy kompromittálódtak-e az adatai, és egy gyors jelszócsere sem lehet ártalmas.**



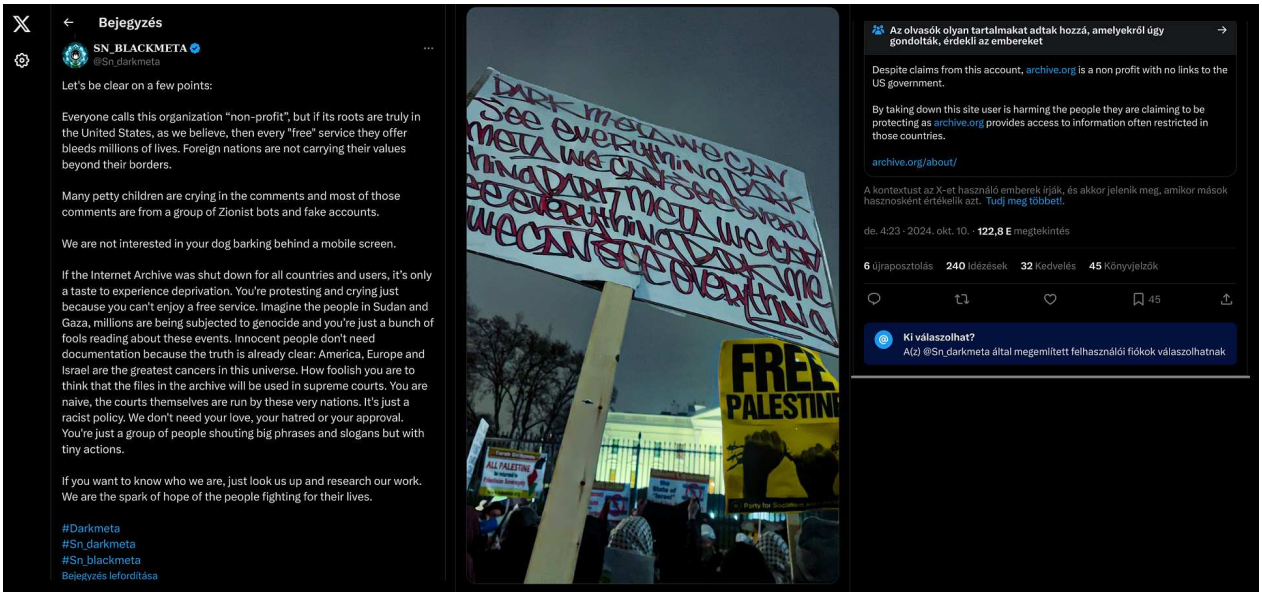
Hunt szeptember 30-án kapta meg a fájlt, ám mivel épp utazás közben volt, csak október 6-án vette fel a kapcsolatot az Internet Archive csapatával.

Ők másnap, 7-én **megerősítették, hogy valóban tőlük származnak a tételek, amik aztán fel is kerültek a HIBP oldalára. Brewster Kahley, az IA munkatársa ezt egy X tweetben is kiposztolta.**



Ám a problémáknak **ezzel nem lett vége, mert utána egy masszív DDoS túlterheléses támadás is érte az archívumot. Ez utóbbit egy BlackMeta nevű csoport** magára is vállalta.

Az 1996-os alapítású nonprofit internetes archívum feltörésének pontos technikai részleteiről bővebbet egyelőre nem tudni. **Az okokat kutatva elsőre látszólag** [az elkövetők just for fun tették a dolgukat, mert valóban semmilyen kapcsolatfelvétel, vagy váltságdíj követelés nem követte](#) az adott incidenst.



[Ám ha a BlackMeta twitter oldalát alaposabban megnézzük, ott már világosan látszik a meghúzódó politikai motívum](#): egy Amerika, Európa és Izrael ellenes, Palesztina párti hacktivista csoportosulásról van szó, amely a szudáni és Gáza övezeti konfliktusok miatt tartja jogosnak a kibertérben végrehajtott legutóbbi figyelemfelkeltő lépéseit.

Szólj hozzá!

Címkék: politika internet archívum támadás archive feltörés adatszivárgás hunt hacktivizmus troy hibp haveibeenpwned waybackmachine

Ajánlott bejegyzések:

Zsarolóvírus a szívsebészeti orvosi eszközöket gyártónál
Újabb rombolás brit kórházakban
Hogyan védjék magukat az idősebbek az interneten?
Hergelés vagy biztonságtudatossági teszt?

Zsarolóvírus a szívsebészeti orvosi eszközöket gyártónál
Újabb rombolás brit kórházakban
Hogyan védjék magukat az idősebbek az interneten?
Hergelés vagy biztonságtudatossági teszt?
Az élet szép, de a Life360-nak vannak gondjai

Az élet szép, de a Life360-nak vannak gondjai

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Piszkos hadviselés

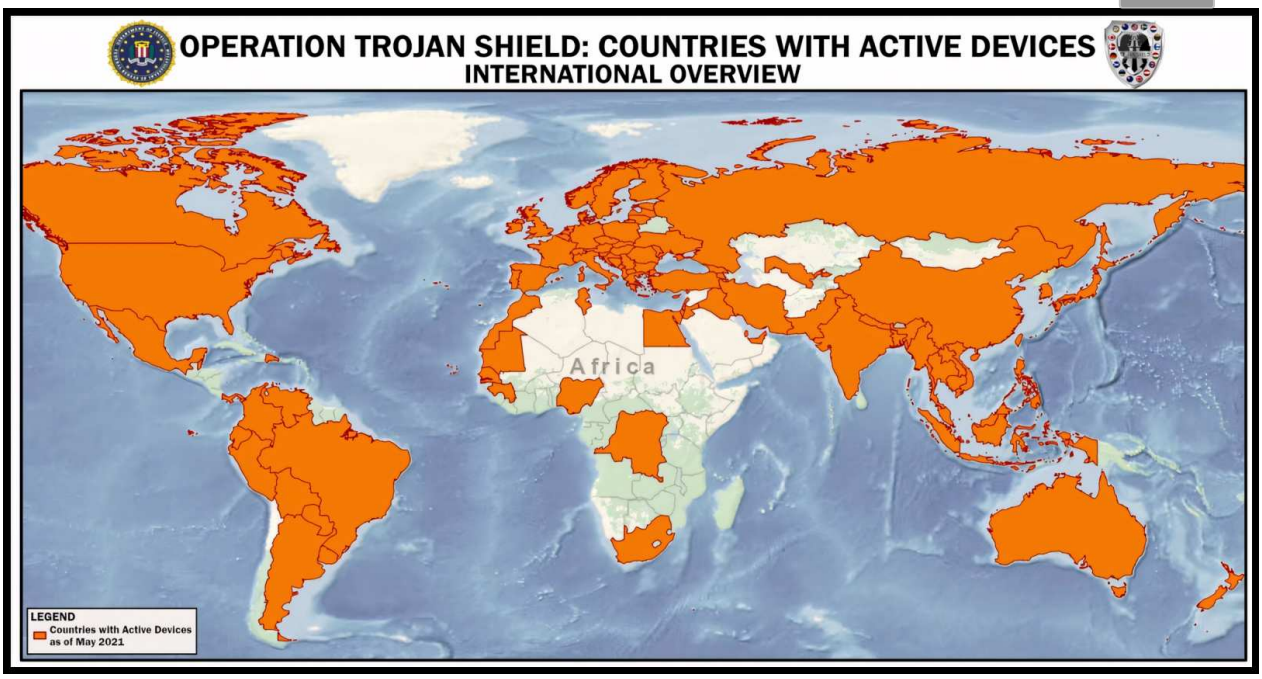
2024. október 15. 10:00 - Csizmazia Darab István [Rambo]

Már igen hosszú ideje léteznek honeypotok, vagyis olyan fertőzhető csali weboldalak, szerverek, hotspotok, amelyek sokat segítenek a szakembereknek a biztonsági tesztelésben, valamint a kibertámadások észlelése és kutatása céljából. **Néha azonban ennél lényegesen aktívabb szerepet is vállalnak a szereplők, ha az internetes bűnözők leleplezéséről van szó.**

Talán sokaknak emlékezetes lehet az **pár éve történt eset, mikor az FBI egy fedőművelet keretében először működtetett saját titkosítási eszközöket gyártó céget ANOM néven. Az anonimitást és feltörhetetlen titkosítást ígérő szolgáltatás évekig igen népszerű volt a bűnözők körében, senki nem ismerte az eredetét.**

Több, mint 12 ezer ilyen eszközt értékesítettek hozzávetőleg száz országban, köztük 300 körüli bűnszervezetnek, nemzetközi kábítószer-kereskedő csoportoknak, olasz maffia szereplőknek, motoros bandáknak. **Amikor aztán 2021-ben kiderült az igazság, két nap alatt mintegy 500**

letartóztatás történt világszerte az így lehallgatott és dokumentált kommunikáció alapján.

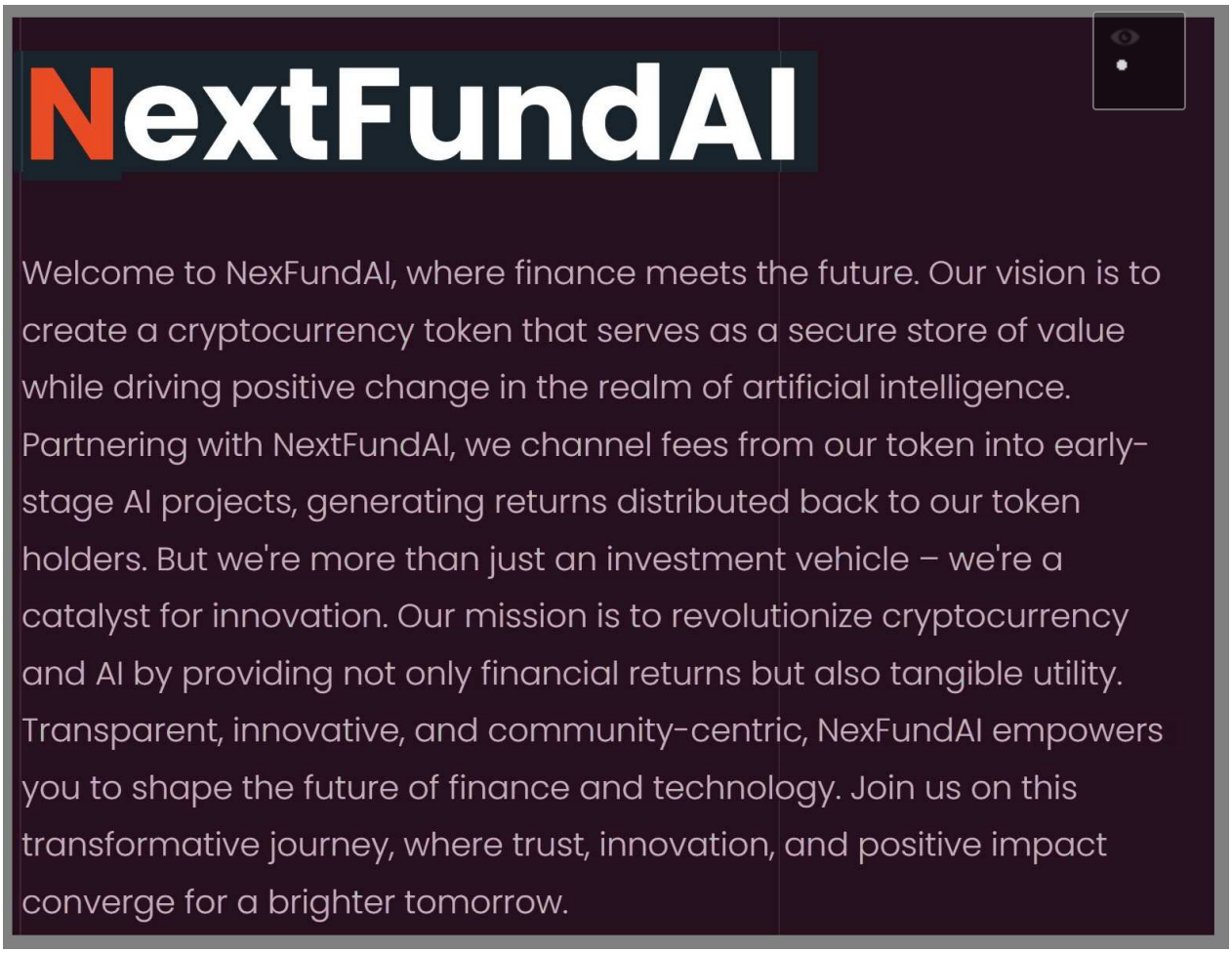


Kicsit hasonló **ez a mostani történet is, ahol szintén az FBI titkos kísérleti tervét váltották valóra. A hatóság amiatt hozott létre egy új kriptovalutát, hogy a gyakorlatban is alaposan megfigyelhesse az ezzel történő visszaéléseket. Így hát színre lépett a NexFundAI nevű Ethereum-alapú token**, amely aztán hamar belefolyt az itteni szokványos kereskedelmi műveletekbe.

Az akciót az FBI berkeiben végül sikeresnek ítélték, ugyanis **18 magánembert és jogi személyt vádoltak meg a kriptovaluta piacokon elkövetett folytatólagos csalás és manipuláció miatt. Vádat emeltek Bostonban négy kriptovaluta pénzügyi szolgáltató cég (úgynevezett "piacjegyzők": a Gotbit, a CLS Global, a MyTrade és a ZM Quant)** és az említett cégek alkalmazottai ellen.

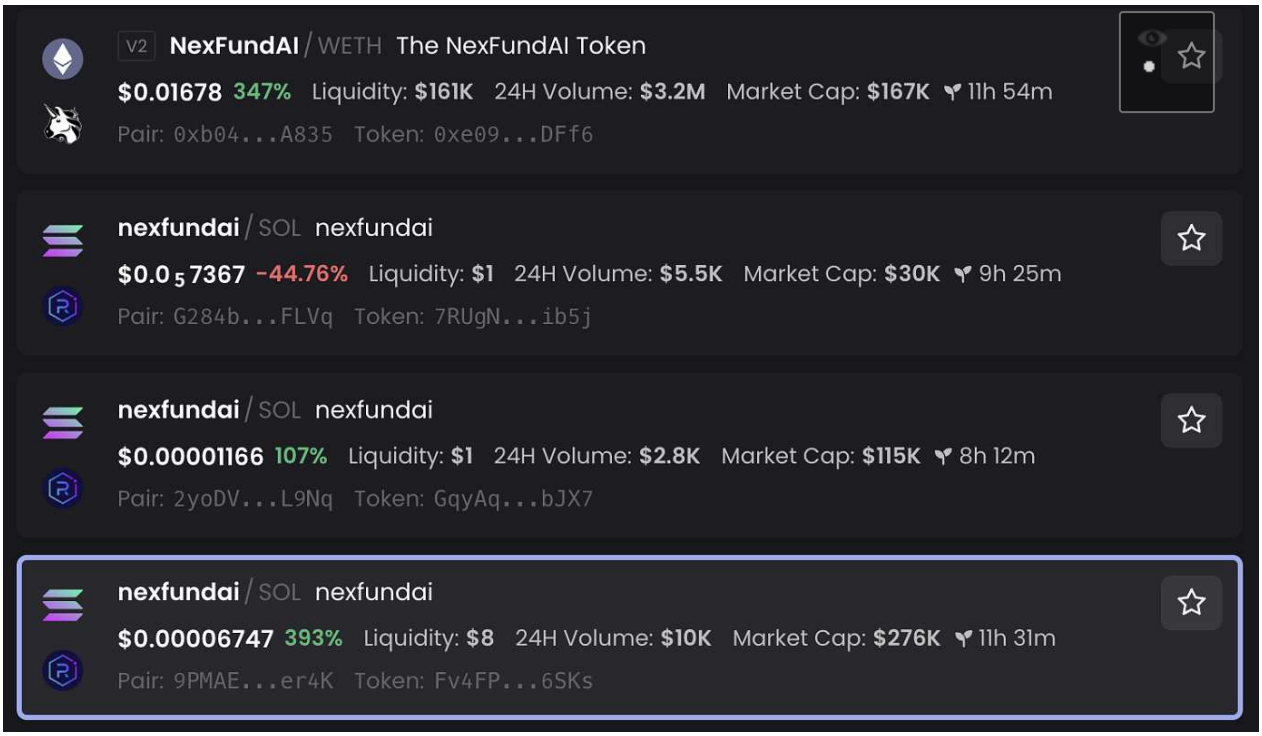
A ZMQuant például a Brit Virgin-szigeteken volt bejegyezve, de a vádiratban megnevezett alkalmazottak eközben Hongkongban dolgoztak. A Gotbit pedig sehol nem volt bejegyezve, az alkalmazottairól azt gyanítják, hogy oroszok.

Az ügyben négy vádlott már bűnösnek vallotta magát, a hatóságok pedig további három másik vádlottat fogtak el a héten Texasban, az Egyesült Királyságban és Portugáliában. Összesen több mint 25 millió dollárnyi kriptovalutát foglaltak le, és több olyan kereskedési botot deaktiváltak, amelyek több millió dollár értékben bonyolítottak le kriptovalutával kapcsolatos kétes ügyleteket.



Az FBI képviselője úgy nyilatkozott, hogy korlátozott volt az érmével kapcsolatos kereskedési tevékenység, de **nem volt hajlandó megosztani az ezzel kapcsolatos részletes információkat.**

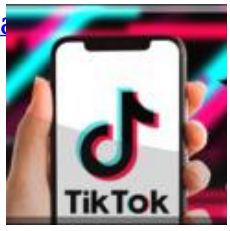
Illetve arra sem válaszoltak, hogy a fedett művelet során az FBI együttműködött-e bármilyen másik kriptográfiai céggel ebben a projektben.



A piaci manipulációk során egyébként **tipikus az olyan ténykedés, amikor a kereskedők hamis vételi és eladási látszat megbízásokat indítanak, hogy a befektetők előtt a kereslet illúzióját keltsék. Elemzők becslése szerint valójában az egyes kripto tőzsdék kereskedési volumenének akár 50%-át is az ilyen manipulált, kamu üzelmek teszik ki.**

Szólj hozzá!
Címkék: akció fbi csalás átverés letartóztatás vádemelés kriptovaluta kriptobefektetés

Ajánlott bejegyzések:

A kriptobevételek felett az égbolt felhőtlen
A call centerek farkasai
Rabszolgamunka a kiberbűnözők fogságában


A kriptobevételek felett az égbolt felhőtlen
A call centerek farkasai
Rabszolgamunka a kiberbűnözők fogságában
Csalás jönni TikTokra

Halló, itt Joe Biden, vagy mégsem?

Halló, itt Joe Biden, vagy mégsem?

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

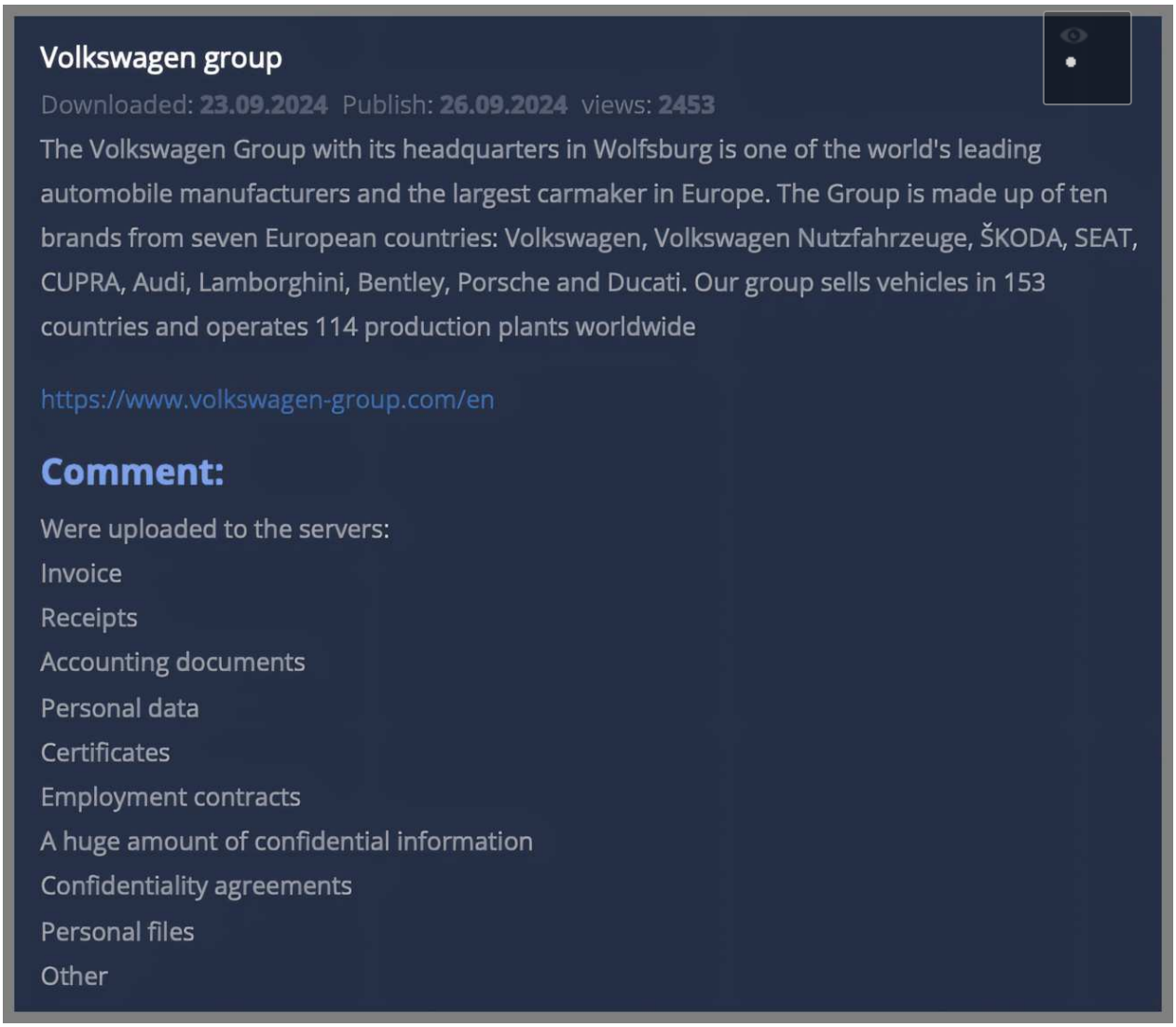
Ransomware a Volkswagennél

2024. október 22. 14:04 - Csizmazia Darab István [Rambo]

A 8Base elnevezésű ransomware banda azt állítja, hogy sikeres támadást hajtottak végre a VW csoport hálózatában, és jelentős mennyiségű bizalmas információt sikerült zsákmányolniuk.

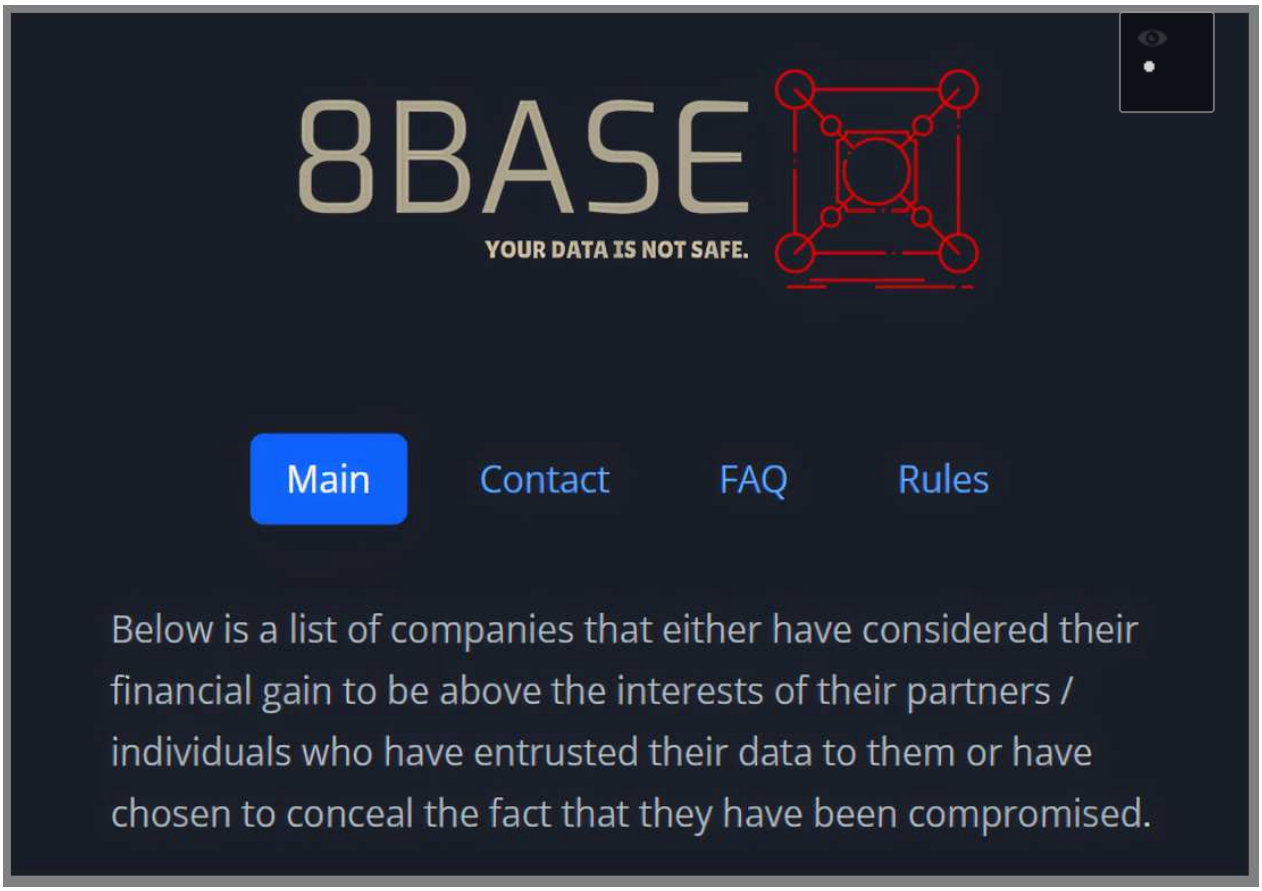
A Volkswagen-csoport olyan híres autómárkákat forgalmaz, mint a Volkswagen, a Skoda, a Seat, az Audi, a Lamborghini, a Porsche, a Cupra és a Bentley.

A megjelent hírek szerint a doxing során állítólag megszerzett **érzékeny adatok köre igen széles: köztük számlák, nyugták és számviteli bizonylatok, különféle személyes adatok és belső fájlok, munkaszerződések és bizonyítványok dokumentumai, titoktartási megállapodások.**



Bár a bűnözők eredetileg szeptember 26-át tűzték ki fizetési határidőnek, egyfelől nem ismert a követelt váltságdíj összege, másfelől azóta nem történt semmilyen új fejlemény, és mégsem hoztak nyilvánosságra lopott adatokat.

A fenyegetés ellenére a cégcsoport cáfolta a híresztelést. Ismerik a támadói bejelentést, de szerintük az nem komoly, az informatikai infrastruktúrájukat nem érte semmiféle új támadás. **A legfontosabb kérdésre azonban nem válaszoltak: érkezett-e hozzájuk váltságdíj követelés, és ha igen, a zsarolók adatmintát is adtak-e állításaik bizonyítására?**



Bár a cég nemleges válasza kicsit olyan, **mint amikor valakitől megkérdezik, hogy ő kém-e, amire mindig nem a válasz: hiszen ha valaki nem az, akkor azért, ha pedig éppen az, akkor ezért. Ám itt nem látni tisztán, hiszen egyrészt érte már sikeres támadás korábban a VW csoportot például 2021-ben.**

Másrészt az emlegetett 8Base sem egy kezdő brigád, és bár nem túl hosszú a múltjuk, hiszen "csak" 2023. év eleje óta léteznek, ám a honlapjukon több száz támadást jegyeznek már. **De persze az is tény, hogy a támadók sokszor csak blöffölnek az adatlopással kapcsolatban, hátha mégis sikerül pénzhez jutniuk.**

Emellett egy érdekes adalék még, hogy **Anne Neuberger, az Egyesült Államok kibertechnológiákkal foglalkozó nemzetbiztonsági tanácsadó-helyettese azt javasolja, hogy szüntessék meg a ransomware biztosítások jelenlegi laza gyakorlatát.** A biztosítási kötvények feltételeként szigorú kiberbiztonsági intézkedéseket követeljenek meg a szervezetektől.

A támadók oldaláról sajnos ez nagyon jövedelmező üzlet, csak tavaly az FBI 2825 bejelentést kapott ransomware fertőzésekről, amelyek több mint 59.6 millió dolláros (22 milliárd forintnyi) veszteséget okoztak, **és a cégvezetők valóban hajlamosak könnyebben dönteni a fizetésről, ha azt egy biztosítás amúgy fedezi.**

Szólj hozzá!
Címkék: volkswagen vw váltságdíj ransomware zsarolóvírus doxing

Ajánlott bejegyzések:

Újabb rombolás brit kórházakban
Senki többet harmadszor?
Halálos fegyver: doxing
Kórházak a pácban II.
Senki többet harmadszor?
Kórházak a pácban II.

Újabb rombolás brit kórházakban

Halálos fegyver: doxing

LockBit üti Subway, sakk

LockBit üti Subway, sakk

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

Csomagja érke... Na most már elég!

2024. október 25. 14:06 - Csizmazia Darab István [Rambo]

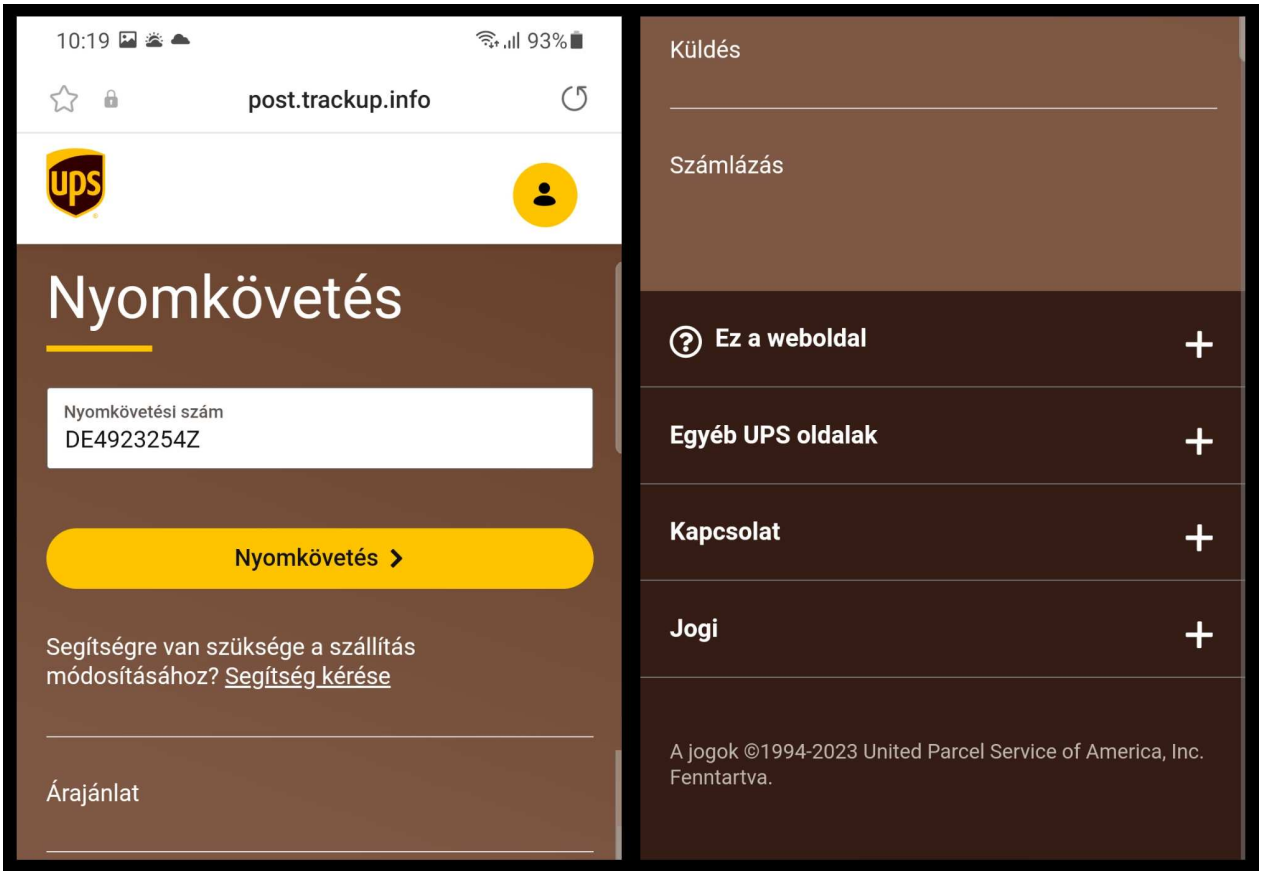
Mi történik, ha érkezik a telefonunkra egy átverős csomagküldős SMS, de mindeközben a háttérben ketyeg egy antivírus?

Biztos sokan emlékeznek a "Csomagja megerkezett, kövesse nyomon itt" kezdetű SMS csalásra, **amely több, mint három évvel ezelőtt tarolt le sok androidos mobilt. A Flubot vírus minden a telefonunkon tárolt adatunkhoz hozzáfért**, és a speciális engedélyek miatt az eltávolítás sem volt túl egyszerű.

Ráadásul fertőzés esetén a kártékony kód a mi számunkról is tovább terjedt, **volt olyan áldozat, akinek a telefonjáról 4700 SMS üzenetet küldtek el. Ha valaki óvatos volt, és/vagy volt telepített védelmi program a készülékén, az szerencsésen megúszhatta.**

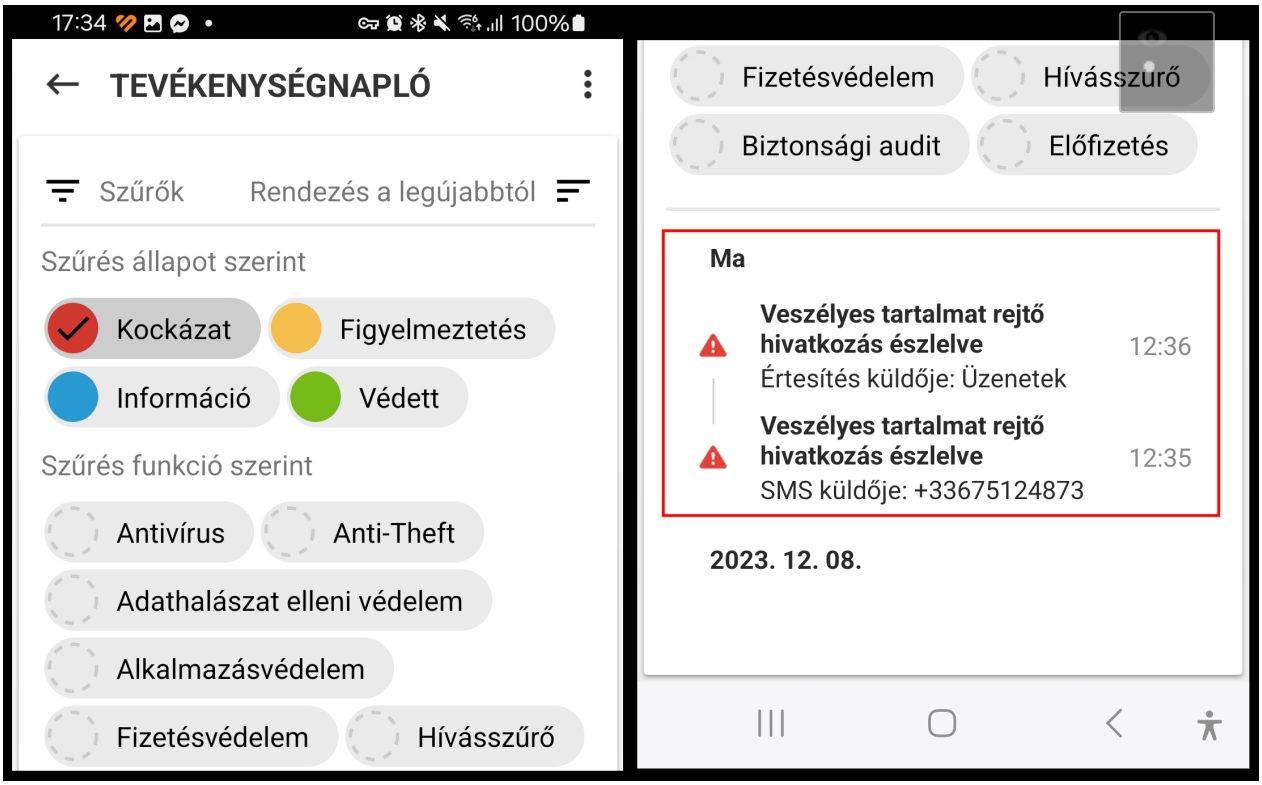
Ez a típusú csalás azóta is aktív, rendre felbukkan magyar nyelven is. Nyilván a biztonságtudatosság hozzáállás is egy nélkülözhetetlenül fontos kellék, de néha érdemes megnézni, önmagában a védelem hogyan teljesít. **És ehhez jött is egy újabb versenyző**, egész pontosan egy +33 kezdetű, azaz franciaországi számról.

Bár a helyesírás ellenőrzés, és a ChatGPT már mindenkinek a rendelkezésére áll, **a lusta támadók itt nem sokat törődtek a nyelvileg helyes kinézettel: "*Az csomagja kézbesítésre vár. Vámkezelési díj: 2,99E. Részletek:*" és utána egy kattintható link.** Az "E" itt talán euró lehet.



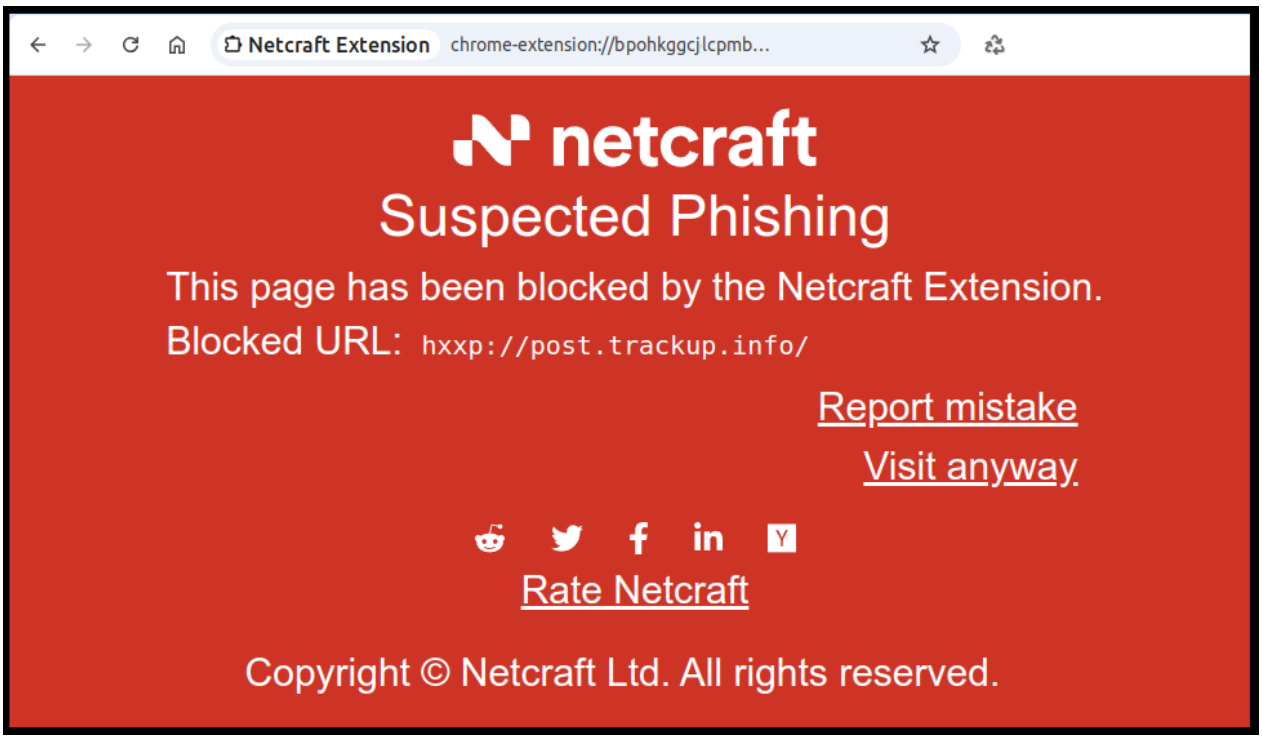
Az URL cím egy nem túl régi, pár hónapos bejegyzésre mutat, és ha meglátogatjuk az adathalász weboldalt, az is kiderül, hogy **a UPS nevében igyekeznek rászedni a felhasználókat.**

A szokásos gyanakvás mellett Sherlock Holmes azt is észrevenné, hogy az oldal alján a Copyright még 2023-as. És akkor nézzük ugyanezt egy olyan telefonon, amin fut a vírusvédelem.



[Az ellenőrzés már blokkolja és jelzi egy felbukkanó ablakban, hogy adathalász üzenet érkezett](#).

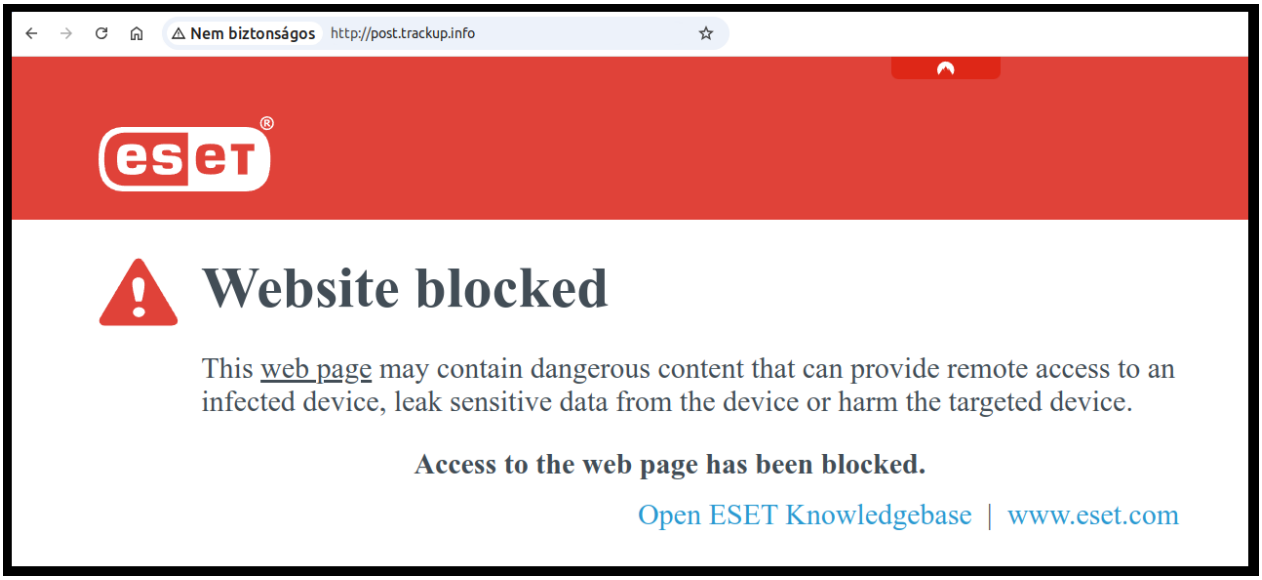
Az eredeti felugró figyelmeztető ablak sajnos nem került lementésre, de **az előzményekben jó látszik, hogy erre az SMS-re érkezett a riasztás.**



Számítógépes böngészésnél az is **hasznos, ha szkript blokkoló és egyéb biztonsági kiegészítőket telepítünk**, jelen esetben [a Netcraft](#)

alkalmazásánál is azonnal jön a piros ablak a lejelentett adathalász oldal miatt.

Itt még választhatjuk a Visit anyway opciót, vagyis a figyelmeztetés ellenére mégis mehetünk az oldalra.



És ez már **a számítógépes védelem ablaka, szépen felkoppan itt is a phishing weboldal.**

Szóval hasznos, ha minden eszközön fut védelmi megoldás, de **emellett érdemes nekünk is figyelmesnek, és biztonságtudatosnak maradnunk, mert az ilyen próbálkozások sajnos már mindennaposság váltak.**

Szólj hozzá!
Címkék: mobil sms csalás átverés phishing eset vírusvédelem ups adathalászat csomagküldő

Ajánlott bejegyzések:

Élősködők

Leveringa függesztés csomag részére

Szia uram! SIM cserés csalást kérhetek?

Élősködők

Leveringa függesztés

Szia uram! SIM cserés

Mai szavunk pedig: smishing

csomag részére

csalást kérhetek?

MBH banki adathalászat

MBH banki adathalászat

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

100 millió ember egészségügyi adata hoppszi

2024. október 29. 12:01 - Csizmazia Darab István [Rambo]

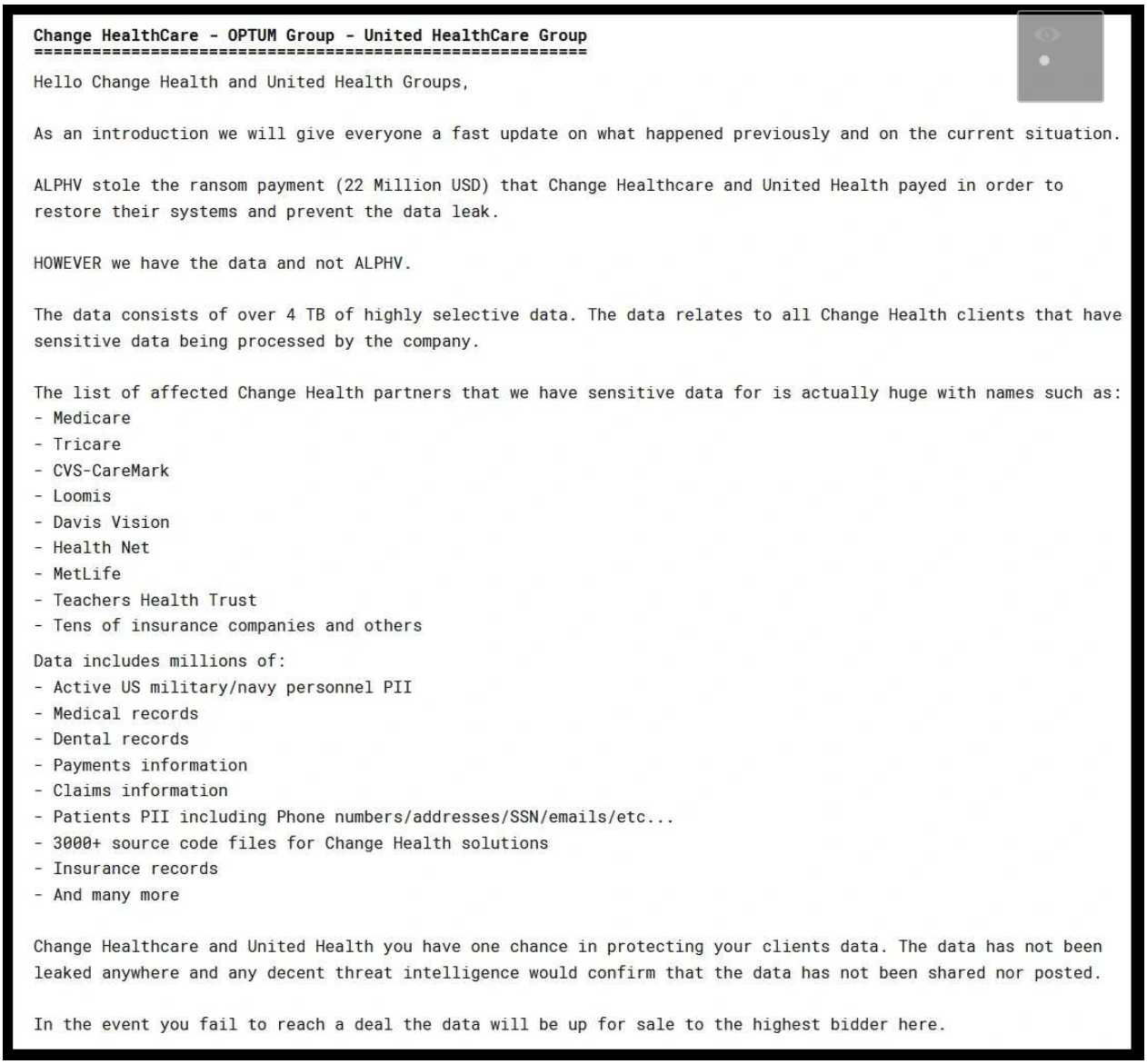
A UnitedHealth első alkalommal erősítette meg hivatalosan azt az információt, hogy **ennyi felhasználó adatát érintette az a bizonyos Change Healthcare zsarolóvírus-támadás.**

Korábban mi is beszámoltunk arról, hogy **az ALPHV/BlackCat bűnözői kör egy alvállalkozói csoportja megtámadta a Change Healthcare rendszereit**, ahol a zsarolóvírus-fertőzés gyógyszertárak és kórházak ezreit zavarta meg szerte az Egyesült Államokban. Az USA területén több, mint 70 ezer gyógyszertár használja a szoftvereiket a receptek és betegbiztosítási igények feldolgozásában.

A kiberbiztonsági incidens több tízezer kórház, orvoscsoport, fogorvos és gyógyszertár kifizetését és vényköteles gyógyszerek feldolgozási folyamatát szakította meg, ezenkívül az adminisztráció teljes leállása miatt a társadalombiztosítási elszámolás rendszere, valamint az orvosok munkaidő elszámolása is megakadt.

A dolog aztán kicsit később tovább bonyolódott, pedig **az ország legnagyobb biztosítási számlázási hálózatának már az is eleve súlyos érvágás volt, hogy a támadóknak 6 TB bizalmas adatot is sikerült ellopniuk.**

Az egészségügyi szervezet **hiába fizetett ki az adataik visszaszerzéséért és a lopott adatok nyilvánossá tételének megakadályozásáért március 1-én 22 millió dollár összegű váltságdíjat, ugyanis belháború tört ki a bűnözők között, és a váltságdíjat beszedő affiliate partnert az ALPHV/BlackCat vezetősége felfüggesztette, eközben pedig a kapcsolt vállalkozás számlájáról az ott tárolt teljes összeget elvették tőlük.**



Change HealthCare - OPTUM Group - United HealthCare Group

Hello Change Health and United Health Groups,

As an introduction we will give everyone a fast update on what happened previously and on the current situation.

ALPHV stole the ransom payment (22 Million USD) that Change Healthcare and United Health payed in order to restore their systems and prevent the data leak.

HOWEVER we have the data and not ALPHV.

The data consists of over 4 TB of highly selective data. The data relates to all Change Health clients that have sensitive data being processed by the company.

The list of affected Change Health partners that we have sensitive data for is actually huge with names such as:
- Medicare
- Tricare
- CVS-CareMark
- Loomis
- Davis Vision
- Health Net
- MetLife
- Teachers Health Trust
- Tens of insurance companies and others

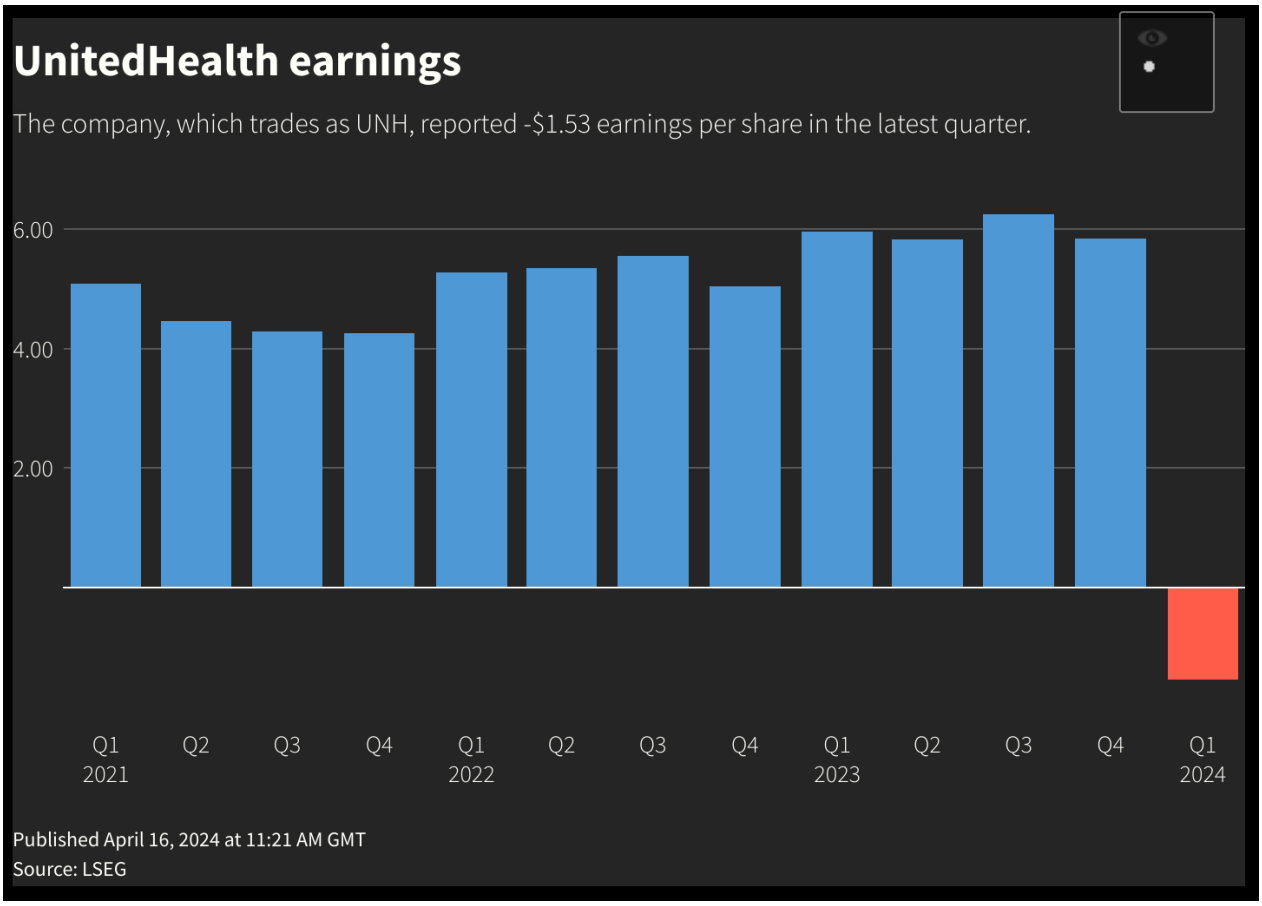
Data includes millions of:
- Active US military/navy personnel PII
- Medical records
- Dental records
- Payments information
- Claims information
- Patients PII including Phone numbers/addresses/SSN/emails/etc...
- 3000+ source code files for Change Health solutions
- Insurance records
- And many more

Change Healthcare and United Health you have one chance in protecting your clients data. The data has not been leaked anywhere and any decent threat intelligence would confirm that the data has not been shared nor posted.

In the event you fail to reach a deal the data will be up for sale to the highest bidder here.

Az eset folytatása is elég elkeserítően alakult, mert **jött egy nem várt második kör is, miközben az eredeti támadói csoport azt állította, 4 TB kritikus adat még mindig a rendelkezésükre áll**, emiatt a UnitedHealth aggódhatott, hogy a kifizetés ellenére mégis nyilvánosságra kerülhetnek az ellopott adatok.

Az új fejlemény pedig az volt, hogy a RansomHub csoport újabb követeléssel állt elő, 12 napos határidőt szabva, és a fenti 4 TB adat nyilvánossá tételével fenyegetve. A RansomHub szivárogtatási weboldaláról **néhány nappal később eltűnt az egészségügyi intézményről szóló bejegyzés, ami arra utal, hogy a United Health egy második váltságdíjat is fizethetett**.



Az eset legújabb fejleménye, hogy ezúttal **hivatalosan is elismerték az elszenvedett károk mértékét, vagyis több mint 100 millió ember személyes és egészségügyi adatait lopták el** a zsarolóvírus támadás során. Ezt bátran nevezhetjük **az elmúlt évek legnagyobb egészségügyi adatszivárgásának.**

Az illetéktelen kezekbe került adatok köre roppant széles: részletes egészségbiztosítási információk, kezelési tervek, biztosítási tagok azonosítószámai, kormányzati kifizető azonosítószámok, orvosi nyilvántartások, diagnózisok, felírt gyógyszerek, vizsgálati eredmények, orvosi felvételek, számlázási információk, számlaszámok, bankkártya adatok, banki információk, további egyéb személyes adatok, például társadalombiztosítási számok, jogosítvány és útlevél adatok.

A kikerült információk részletessége egyénenként ugyan eltérő lehet, mert vélhetően nem minden egyes ügyfél kórtörténete szivárgott ki, **de még így is katasztrofális ez az incidens. Áprilisban ezzel kapcsolatosan 872 millió dolláros veszteséget jeleztek, ami még korántsem volt a teljes összeg, a szerencsétlen incidens viszont a részvényárfolyamokat is negatívan befolyásolta.**

Külsős biztonsági szakértők véleménye szerint **az elhúzódó folyamatok arra utalnak, hogy az egészségügyi intézménynek vélhetően nem volt megfelelő biztonsági mentése, és letesztelt incidensreagálási terve, illetve nagyon kevés informatikai szakszemélyzetet alkalmaztak.**

Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
>	Change Healthcare, Inc.	MN	Business Associate	100000000	07/19/2024	Hacking/IT Incident	Network Server

Végül azt is érdemes megemlíteni, hogy **az Egyesült Államok törvényei jelenleg ugyan (még?) nem tiltják egységesen a váltságdíj kifizetését minden egyes államban, de a különféle szankciós listákon szereplő személyek vagy szervezetek támogatását viszont igen.**

Az ilyen szervezetek között pedig jócskán szerepelhetnek orosz és egyéb illetőségű ransomware csoportok is, emiatt attól függően, hogy ki kapja a pénzt, a váltságdíj fizetése már egyes esetekben lehet illegális.

Megosztom
tumblr.
Tweet 0
Pin it
Tetszik

Szólj hozzá!
Címkék: usa united egészségügy váltságdíj healthcare change ransomware blackcat zsarolóvírus alphv ransomhub

Ajánlott bejegyzések:

Várt és nem várt mellékhatások

Change Healthcare újra pácban

Holló a hollónak mégiscsak, de igen...

Várt és nem várt mellékhatások

Change Healthcare újra pácban

8 kórház, 30 klinika, 2.5 millió betegadat

Holló a hollónak mégiscsak, de igen...

A jó kolléga nem csak ígér, hanem be is tart

A jó kolléga nem csak ígér, hanem be is tart

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

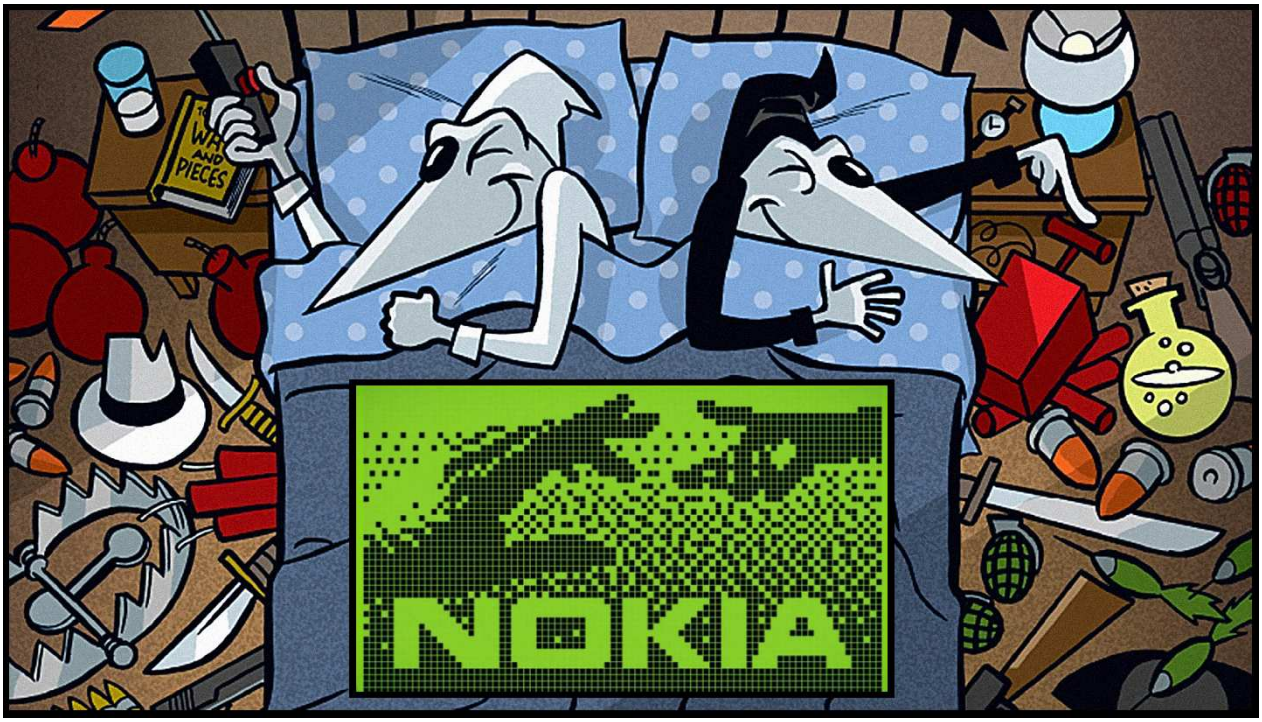
about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Brókerarcok

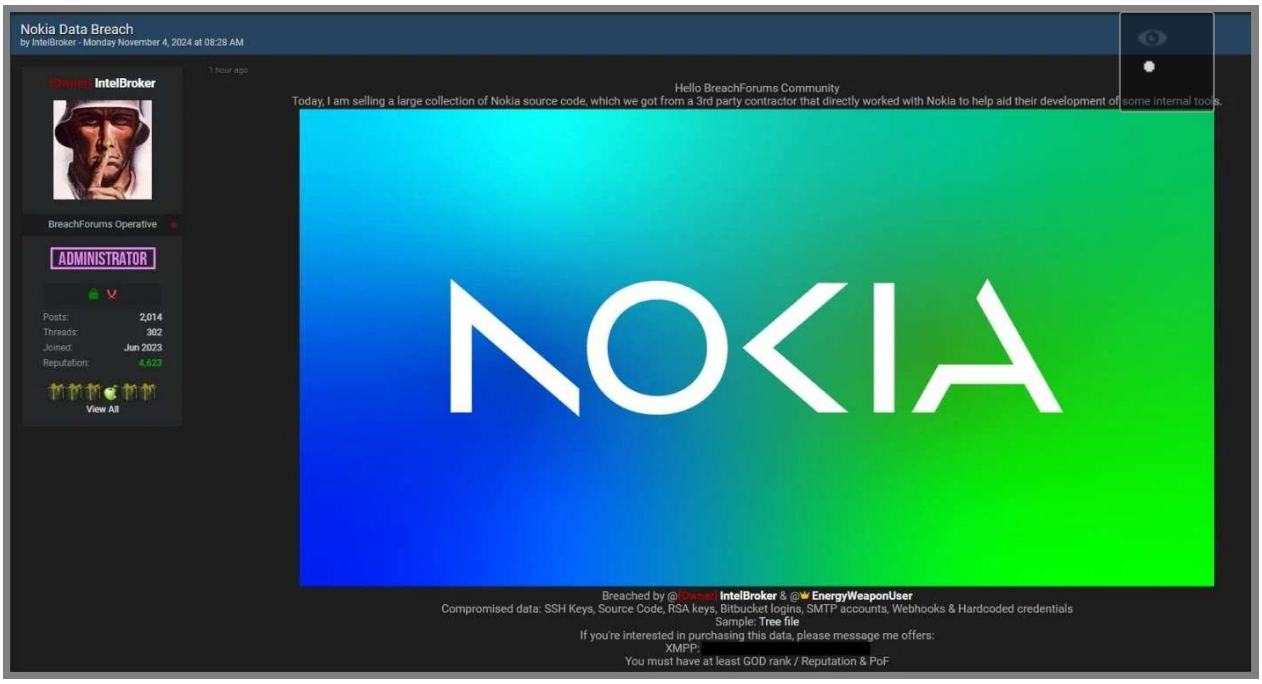
2024. november 05. 14:01 - Csizmazia Darab István [Rambo]

Az Intel Broker néven ismert kiberbűnöző ezúttal **a Nokia érzékeny belső információihoz jutott hozzá, és árulja is ezeket a BreachForums oldalon.**



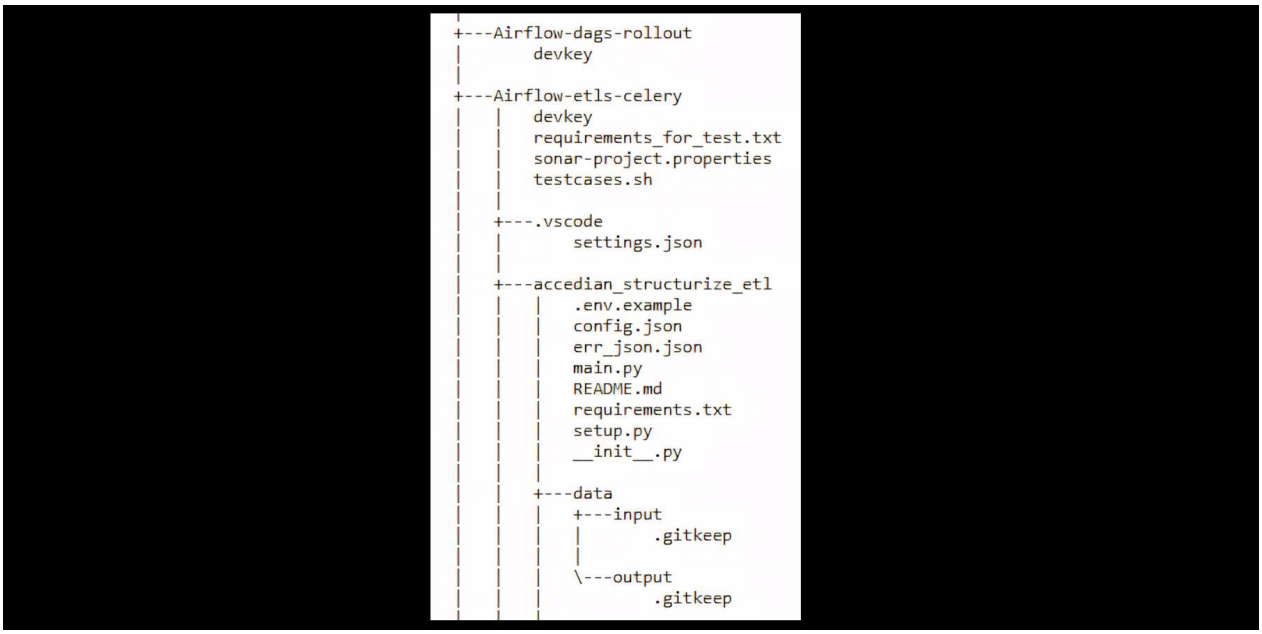
Sokakat a hír hallatán talán már önmagában az is meglephet, hogy egyáltalán még létezik a Nokia. Ami miatt viszont most a reflektorfénybe kerültek, hogy **a fenti állítás cáfolatául megjelent részükről egy nyilatkozat, miszerint a cég komolyan veszi a kérdést, és kivizsgálja az állítólagos adatlopási incidenst.**

Közleményük szerint eddig erre nem találtak semmiféle konkrét bizonyítékot, de folyamatosan ellenőrzik a rendszereiket.



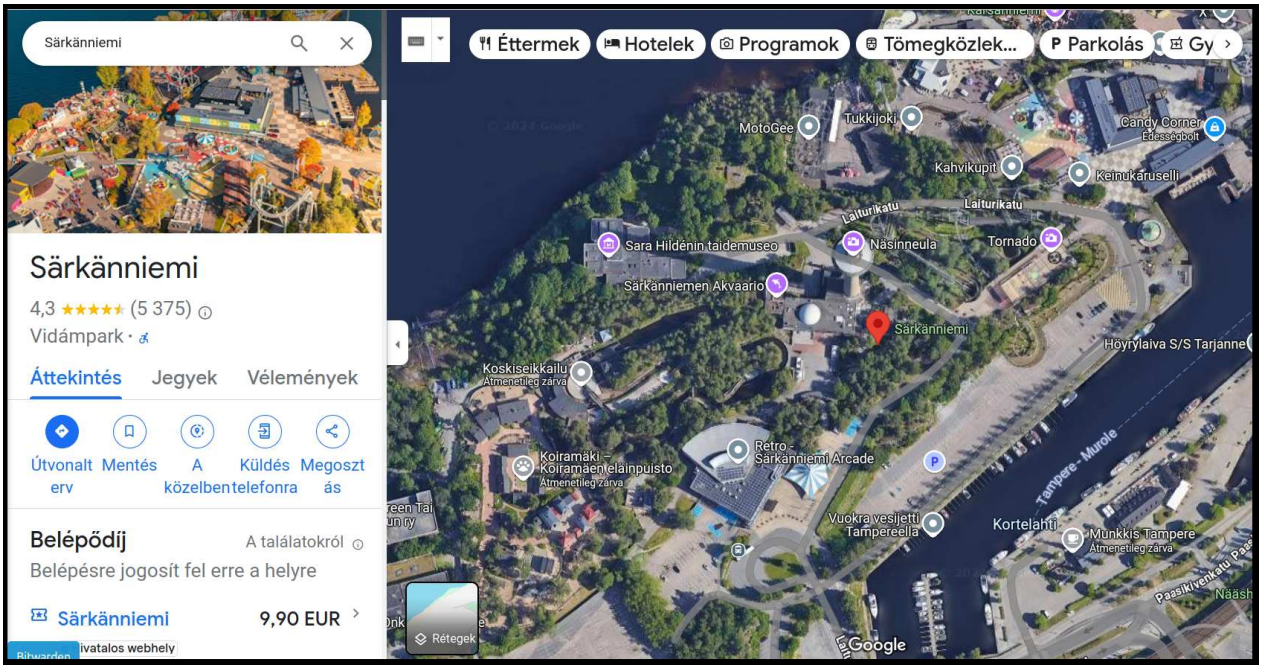
Intel Broker és egy EnergyWeaponUser nevű társa viszont azt állítják, hogy egy külsős beszállító partner feltörése révén hozzáfértek a Nokia tulajdonában lévő forráskódokhoz és egyéb érzékeny céges információkhoz. IntelBroker 20 ezer dollárért árulja a lopott adatokat, és várja a kriptovalutás vevőket.

A kompromittálódott adatok közt SSH illetve RSA kulcsok, és egyéb biztonsági hitelesítő adatok is szerepelnek, amelyek birtokában további jogosulatlan hozzáférést végezhetnek a Nokia rendszereihez, illetve felhasználhatják más típusú kibertámadásokhoz.



Bár ez már egy régi történet, de **2014-ben a Nokia egyszer már több millió eurót fizetett azoknak a zsaroló bűnözőknek, akik ellopták a Symbian mobil operációs rendszerük forráskódjának egy részét, és azzal fenyegetőztek, hogy közzéteszik azt az interneten.**

A Nokia akkor készpénzben fizette ki a több millió eurós váltságdíjat, amelyet egy táskában hagytak egy tamperei vidámpark közelében lévő parkolóban. A rendőrség azonban sajnos nyomát vesztette a zsarolónak, és a pénz akkor nyomtalanul eltűnt.



Intel Broker egyébként nem ismeretlen a kiberincidensek követői előtt, számos korábbi támadás miatt emlékezhetünk rá. Többek közt a **DC Health Link egészségügyi szervezetet, a Hewlett Packard Enterprise-t elleni esetek.**

De **szivárogtattak már ki nagy mennyiségű bizalmas lopott adatot a T-Mobile-tól, az AMD-től és az Apple-től is.**

A Nokia szerint az idei incidensben felhasználói adatok állítólag nem forogtak veszélyben. Ez a mostani eset viszont jól rámutat arra is, hogy **az ellátási lánc elleni támadások egyre gyakoribbá válásával a vállalatoknak újra kell értékelniük a beszállítói partnereikkel kapcsolatos kockázatkezelési stratégiájukat.**

Amit viszont még érdemes megjegyezni, hogy **sok esetben valóban eleve hamis vagy elavult, nagyon régi adatokkal próbálnak házalni a bűnözők, bízva abban, hogy sikerül pénzhez jutniuk. Hogy jelen esetben itt most kinél van az igazság, azt csak egy idő után fogjuk megtudni.**

Szólj hozzá!
Címkék: nokia zsarolás forráskód váltságdíj adatlopás szivárogtatás doxing

Ajánlott bejegyzések:

Újabb rombolás brit kórházakban

Az élet szép, de a Life360-nak vannak gondjai

Ransomware a nyomkövető rendszerben

Újabb rombolás brit kórházakban

Ransomware támadás érte az MSI-t

Az élet szép, de a Life360-nak vannak gondjai

Ransomware a nyomkövető rendszerben

A jó kolléga nem csak ígér, hanem be is tart

A jó kolléga nem csak ígér, hanem be is tart

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink

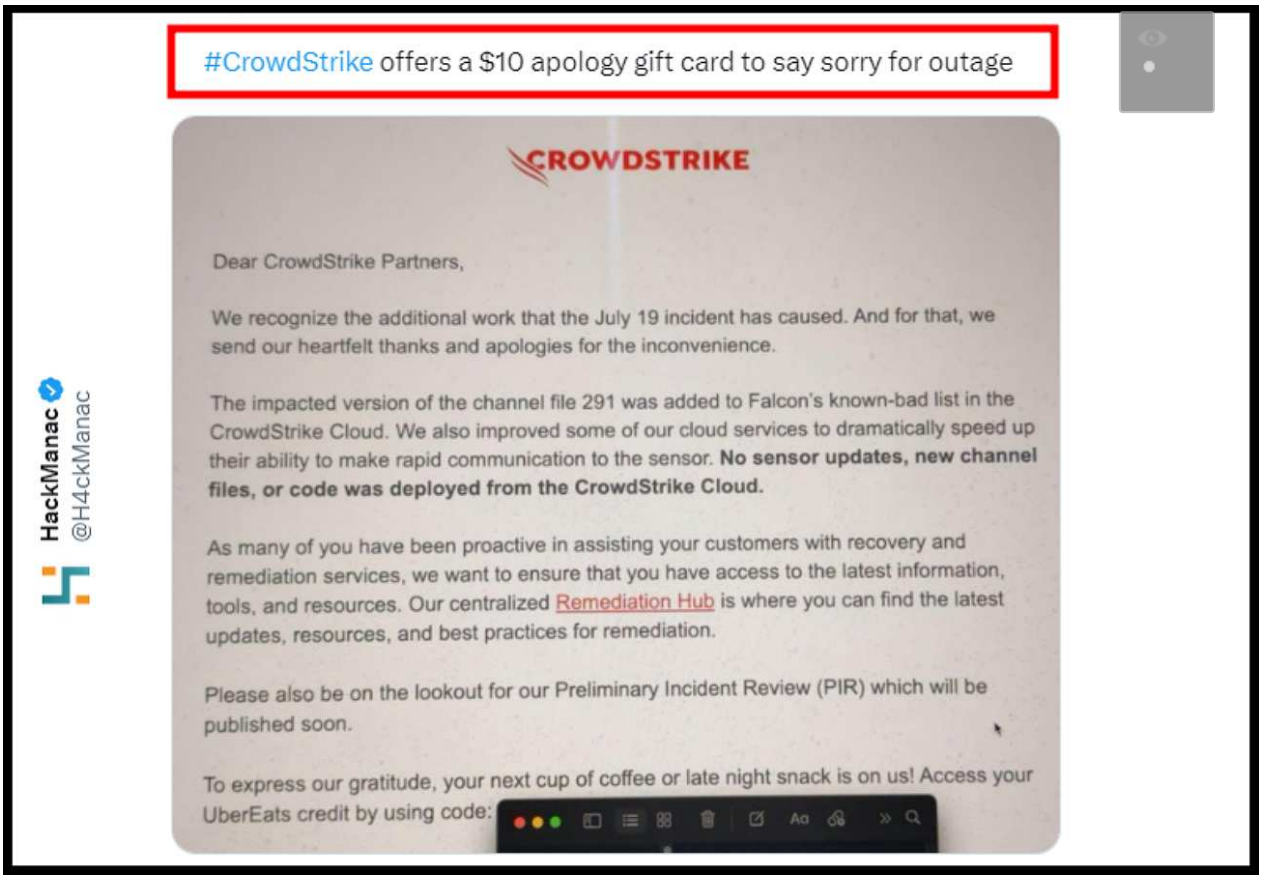
Én és én meg a hibás frissítés

2024. november 07. 14:35 - Csizmazia Darab István [Rambo]

Nagyjából senki nem panaszkodhat arra, hogy manapság mennyire szürke és eseménytelen korban lenne kénytelen élni. **Sokan persze szívesen megspórolták volna egy pár dolgot, például azt az élményt is, amely egy Windows platformra érkezett hibás frissítés miatt alakult ki világszerte idén július 19-én.**

A Crowdstrike biztonsági szolgáltató jelentős szereplő a piacon, világszerte 20 ezer ügyfelük van, köztük a Fortune 500 lista több, mint fele, de az USA kormányzati szervezetei közül is számosan. Emiatt aztán roppant kellemetlen szituáció következett be akkor, mikor **egy hibás frissítés miatt 8.5 millió Windows-eszközön lefagyás, kékhalál jelentkezett röpke másfél óra leforgása alatt.**

Repterek, bankok, tévéadók, kiterjedt közlekedési területek, számos egészségügyi intézmény, tőzsdék, pénzintézetek bénultak meg. **Bár a gyártó rövid időn belül kiadott egy javított frissítést, ám a helyreállítás így is nehézkes és időben hosszan elhúzódó folyamat lett, mert sok gépet csak kézzel lehetett újraindítani, így a káosz még napokig eltartott.**



Egyes vélemények szerint ilyennek képzelhették [a 2000-es évváltáskor végül be nem következő Y2K Armageddont](), ami viszont így negyedszázados késéssel most váratlanul mégis ránk köszöntött ebben a bizarr formában. Bár mint az közismert, [a TAB billentyű használata olyan univerzális csodafegyver, ami mindent is megoldott volna ;-)]()

Az mindenesetre elmondható, hogy **a frissítések előzetes tesztelése minden esetben a gyártó feladata és felelőssége, ez vitathatatlan.** [Az okozott kár mértékéről többféle becslés is napvilágot látott, az egyikben 15 milliárd dolláros veszteségről írtak]() még július végén, **azóta ez a szám már nyilván sokkal pontosabb és magasabb lett.**

Ám a helyzetet bonyolítja, hogy az időmúlással egyes ügyfelek irányából a kártérítési igények peres úton történő rendezése is felmerült, ezek egyike a Delta Airlines légitársaság mostani lépése.

A Delta pénteken pert indított a július 19-i összeomlás miatt, ebben a CrowdStrike-ot hibáztatja, amiért nem tesztelt és hibás frissítéseket kényszerített ügyfeleire, amivel sok millió Microsoft Windows alapú számítógép összeomlását okozta világszerte. Elmondása szerint 40 ezer szerverük állt le az incidens 5 napja alatt, amivel fél milliárd dolláros káruk keletkezett.

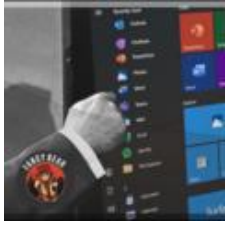
Az a része az érvelésnek, hogy a váratlan leállás, és az első napi szolgáltatás kimaradás a Crowdstrike egyértelmű hibája volt, természetesen mindenki részéről méltányolható.

Amit viszont a másik fél és emellett sok kommentelő is felvet, a második naptól kezdődő egész hetes leállás már részben a Delta saját felelőssége is és az ilyen kritikus helyzetek kezelésére való felkészületlenségének lehet a bizonyítéka. Mindenesetre kíváncsian várjuk az események végét.

Szólj hozzá!
Címkék: windows hiba frissítés leállás per delta hibás airlines felelőtlenség világméretű crowdstrike

Ajánlott bejegyzések:

Crowdstrike utóhatás



Újabb rombolás brit kórházakban

Egy Kozmikus Bogár ront el mindent

Crowdstrike utóhatás

Windows update vagy mégsem?

Újabb rombolás brit kórházakban

Egy Kozmikus Bogár ront el mindent

A távolságot mint üveggolyót nem kapod meg

A távolságot mint üveggolyót nem kapod meg

A távolságot mint üveggolyót nem kapod meg

A távolságot mint üveggolyót nem kapod meg

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

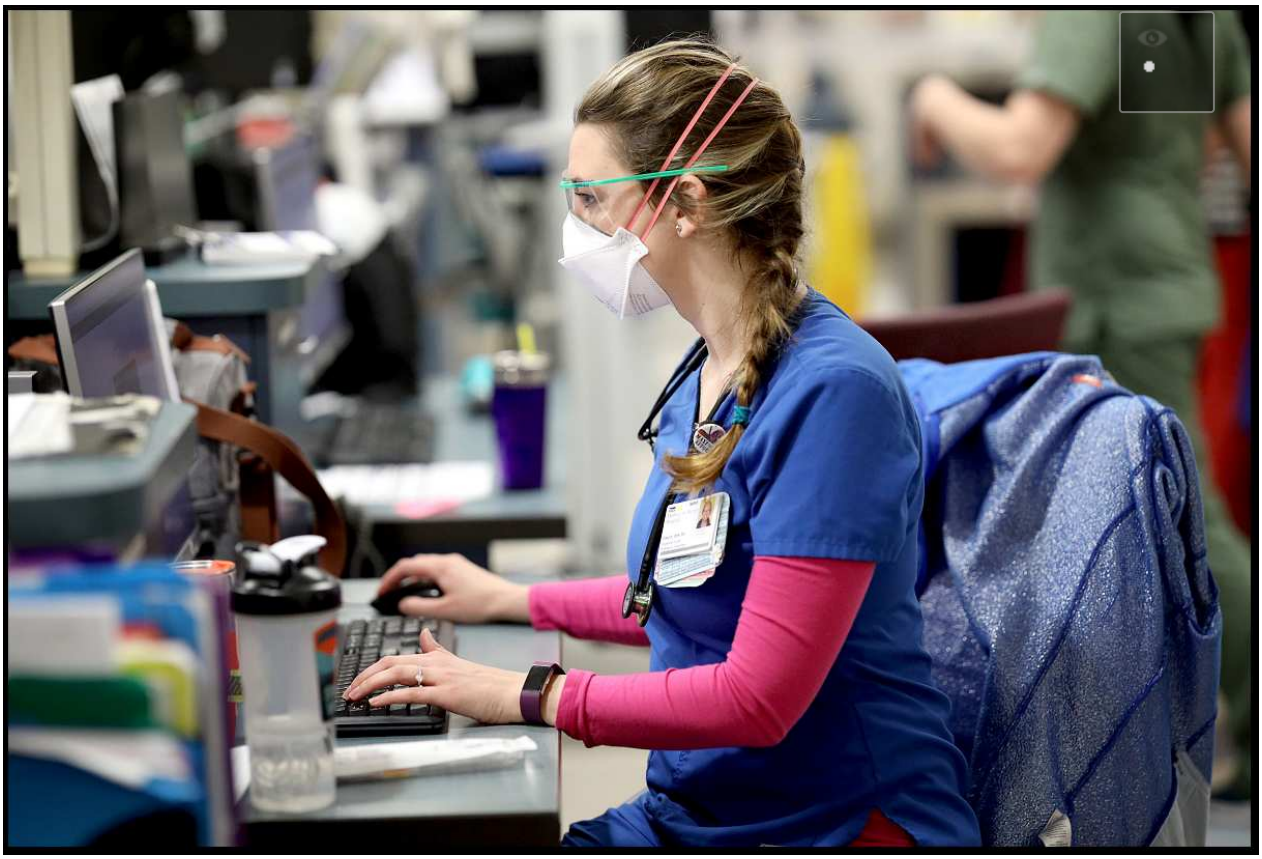
A ransomware az egészségügyben élet-halál kérdése

2024. november 13. 19:13 - Csizmazia Darab István [Rambo]

Egy nemrég lezajlott ENSZ Biztonsági Tanács ülésén elhangzott beszédében a WHO főigazgatója is lépéseket sürget a kialakult helyzet miatt.

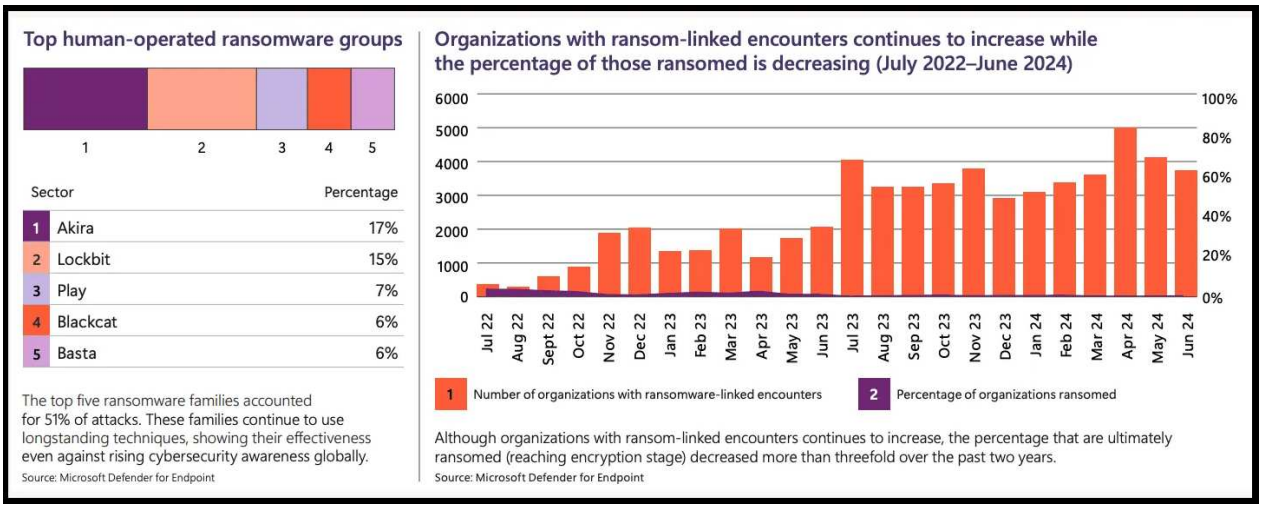
Nyilatkozatában utalt a Covid járvány alatti súlyos incidensekre, például a 2020-as csehországi Brno Egyetemi Kórház elleni támadásra. **Ennek során le kellett állítani kórház hálózatát, át kell szállítani betegeket más szomszédos intézményekbe, el kellett halasztani tervezett műtéteket eljárásokat.**

Épp a járvány miatti szükségállapot alatt az ügyintézéssel is kénytelenek voltak visszalépni a kőkorszakba: telefon, fax, papír, ceruza, valamint személyes utazás a leletekért.



Az egészségügyi intézmények elleni zsarolóvírus támadások minden esetben komoly fennakadásokat és anyagi veszteséget okoznak. Bár egyértelműen nem lehetett kimutatni ilyen incidens és betegek halála közti közvetlen kapcsolatot - bár egy németországi eset kapcsán külön nyomozás is lezajlott - **ám a statisztikák alapján jól látható, hogy egy-egy ilyen kényszerű leállás napokig, hetekig blokkolja a normál betegellátási folyamatokat, így közvetett hatása bizonyosan van.**

A CyberPeace Institute adatai szerint egy egészségügyi rendszert ért kibertámadás **átlagosan 19 napnyi kiesést okoz a betegellátásban**, de a legsúlyosabb esetben 4 hónap kényszerszünet következett be.



A zsarolóvírus támadások után gyakran hetekbe telik, mire a szervezetek helyreállítják informatikai rendszereiket, és a

beteggondozási tevékenységük visszaáll a szokásos normális kerékvágásba. A 2024-es évben minden korábbinál több ilyen típusú támadás történt.

És akkor még a doxingról - azaz az érzékeny adatok ellopásáról még nem is beszéltünk, ami szintén súlyos kockázat az ilyen eseteknél. **Egyfelől a bűnözők ezzel is nyomást gyakorolnak a váltságdíj fizetési hajlandóságra, másfelől a nyilvánosságra hozott, kiszivárgott egészségügyi adatok is további problémákat okoznak az intézménynek és a betegeknek egyaránt.**

A ChangeHealthcare eset pedig azt is mutatja, hogy egyre nőnek a külső egészségügyi szolgáltatók és beszállítók elleni támadások is.

Ezen intézmények leállása is kritikus, és itt is hatalmas mennyiségű értékes információt tárolnak: **társadalombiztosítási számokat, biometrikus adatokat, elérhetőségi információkat és orvosi felvételeket.**

A WHO főigazgatója arra is utalt, hogy egy korábbi globális felmérés szerint a kórházak harmada számolt be legalább egy ransomware támadásról, és a válaszadók egyharmada fizetett is váltságdíjat. **Ám az áldozatok 31%-a a pénz átutalás ellenére sem jutott hozzá az eltitkosított adataihoz**. A védekezéshez és megelőzéshez folyamatos nemzetközi együttműködésre és további erőfeszítésekre van szükség. Például kibervédelmi partnerek részvételével iránymutatást dolgoznak ki az egészségügyben használt információs rendszerek fokozott biztonságáért.

Ebben biztos az is segít, hogy az Amazon 8 év (!) után végre bevezeti a többtényezős hitelesítést az üzleti levelezésnél - **vélhetően jobb későn, mint soha alapon...**

Szólj hozzá!
Címkék: kórház egészségügy who váltságdíj ransomware zsarolóvírus

Ajánlott bejegyzések:

Kórházak a pácban II.

100 millió ember egészségügyi adata hoppszi

Change Healthcare újra pácban

Kórházak a pácban II.

8 kórház, 30 klinika, 2.5 millió betegadat

100 millió ember egészségügyi adata hoppszi

Change Healthcare újra pácban

Az egészségügyet sújtotta leginkább a zsarolóvírus

Az egészségügyet sújtotta leginkább a zsarolóvírus

Az egészségügyet sújtotta leginkább a zsarolóvírus

Kommentek:

Nincsenek hozzászólások.

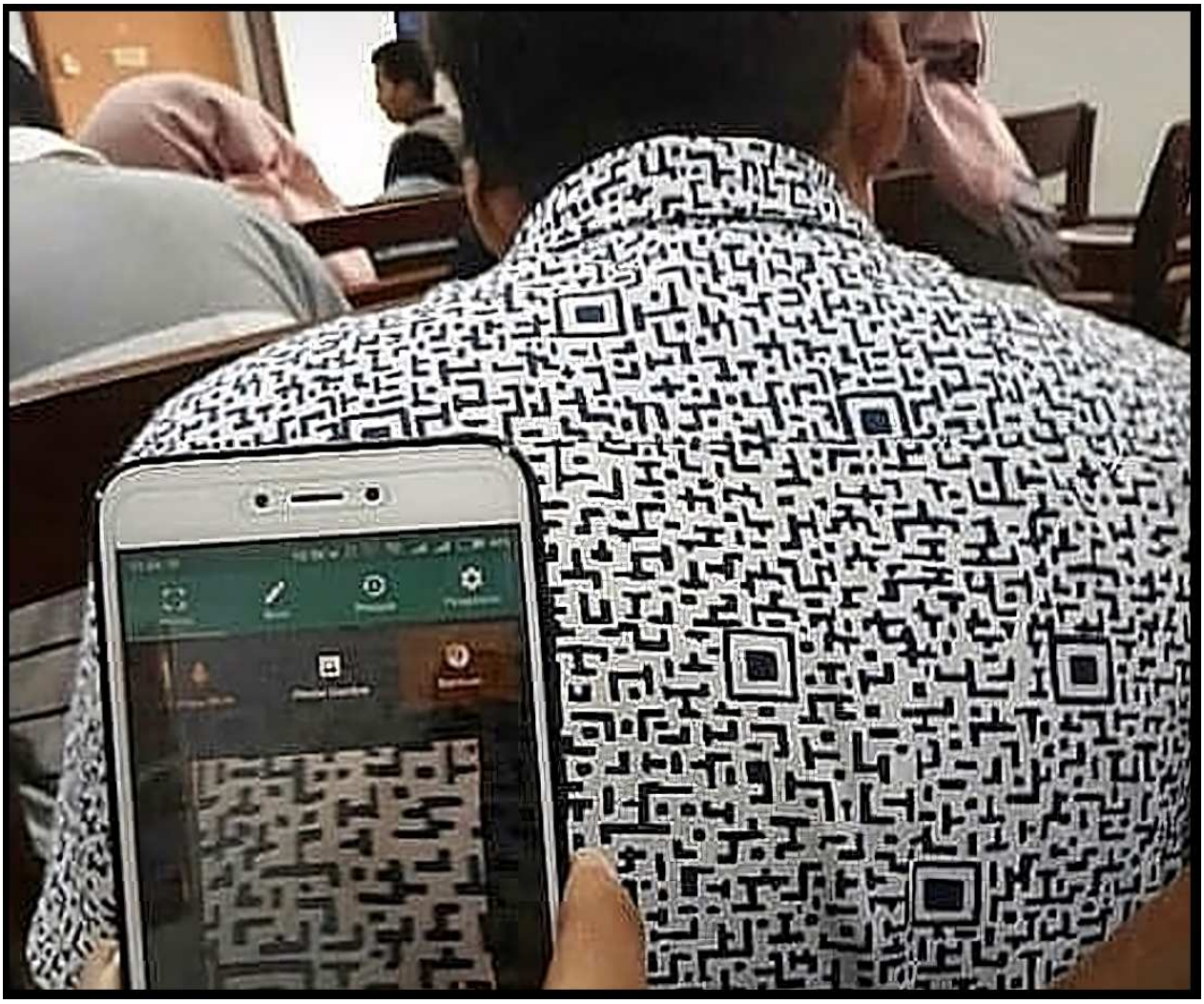
keresés

tweetz

Jöhet-e QR kódos átverés postai papír levélben?

2024. november 19. 15:27 - Csizmazia Darab István [Rambo]

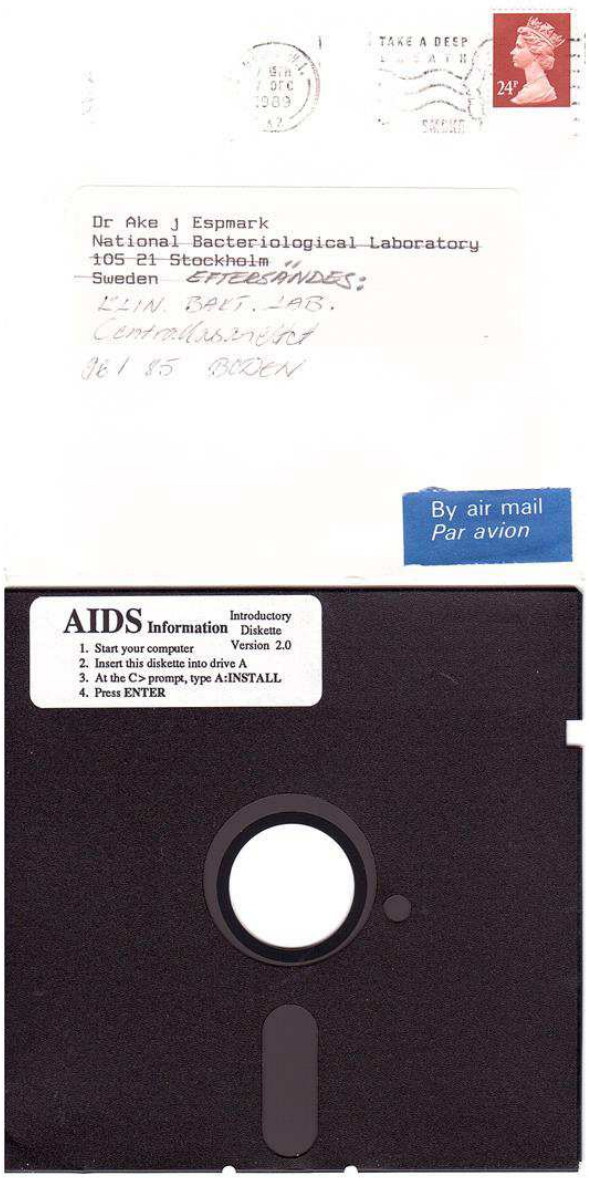
A rövid válasz az, hogy igen, a hosszabb válasz pedig a hajtás után olvasható.

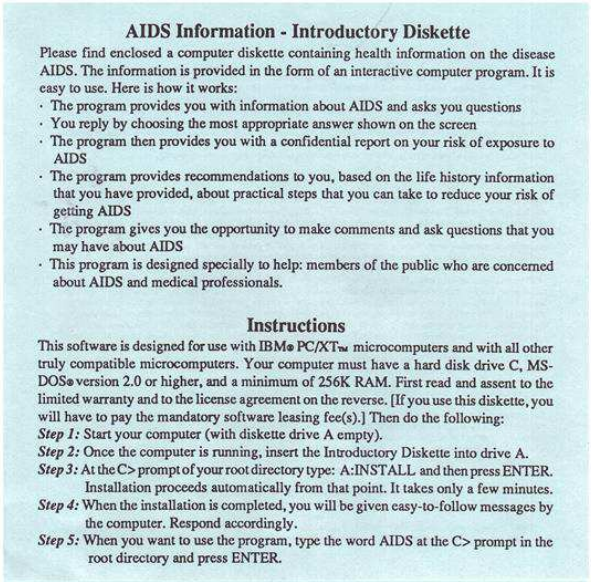


Korábban már írtunk arról, hogy folyamatosan növekszik a QR-kódos visszaélések száma. **A quishing a kényelmesen kezelhető QR kódok alkalmazását takarja**, amelynél a mobilunk kamerájával beolvasva gyorsan megnyílik egy weboldal, vagy jelentkezik egy telepíthető app.

De a kód ezeken túlmenően **akár telefonhívást, SMS üzenetet vagy digitális fizetést is indíthat**, vagyis nagyon nem mindegy, milyen kód beolvasásában bízunk meg. A mostani történet kicsit elüt a korábban

megszokott forgatókönyvektől, és **kissé deja vu érzése támad az embernek**. A ransomware hajnalán ugyanis volt már egy hasonlóan érdekes eset.





AIDS Information - Introductory Diskette

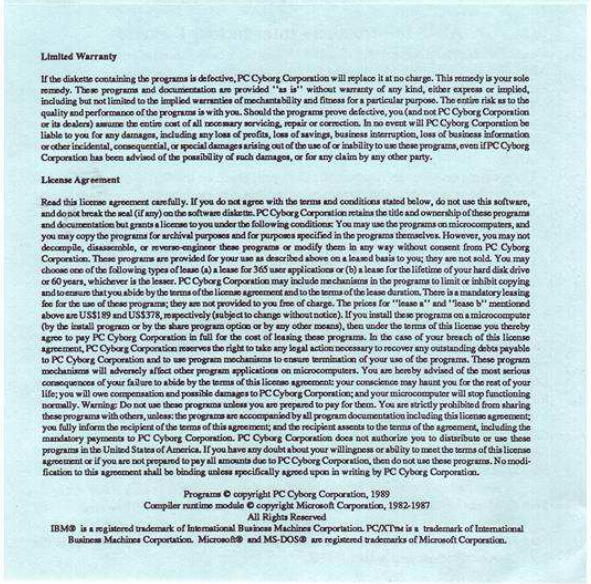
Please find enclosed a computer diskette containing health information on the disease AIDS. The information is provided in the form of an interactive computer program. It is easy to use. Here is how it works:

- The program provides you with information about AIDS and asks you questions
- You reply by choosing the most appropriate answer shown on the screen
- The program then provides you with a confidential report on your risk of exposure to AIDS
- The program provides recommendations to you, based on the life history information that you have provided, about practical steps that you can take to reduce your risk of getting AIDS
- The program gives you the opportunity to make comments and ask questions that you may have about AIDS
- This program is designed specially to help: members of the public who are concerned about AIDS and medical professionals.

Instructions

This software is designed for use with IBM® PC/XT™ microcomputers and with all other truly compatible microcomputers. Your computer must have a hard disk drive C, MS-DOS® version 2.0 or higher, and a minimum of 256K RAM. First read and assent to the limited warranty and to the license agreement on the reverse. [If you use this diskette, you will have to pay the mandatory software leasing fee(s).] Then do the following:

Step 1: Start your computer (with diskette drive A empty).
Step 2: Once the computer is running, insert the Introductory Diskette into drive A.
Step 3: At the C> prompt of your root directory type: A:INSTALL and then press ENTER. Installation proceeds automatically from that point. It takes only a few minutes.
Step 4: When the installation is completed, you will be given easy-to-follow messages by the computer. Respond accordingly.
Step 5: When you want to use the program, type the word AIDS at the C> prompt in the root directory and press ENTER.



Limited Warranty

If the diskette containing the programs is defective, PC Cyborg Corporation will replace it at no charge. This remedy is your sole remedy. These programs and documentation are provided "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of mechantability and fitness for a particular purpose. The entire risk as to the quality and performance of the programs is with you. Should the programs prove defective, you (and not PC Cyborg Corporation or its dealers) assume the entire cost of all necessary servicing, repair or correction. In no event will PC Cyborg Corporation be liable to you for any damages, including any loss of profits, loss of savings, business interruption, loss of business information or other incidental, consequential, or special damages arising out of the use of or inability to use these programs, even if PC Cyborg Corporation has been advised of the possibility of such damages, or for any claim by any other party.

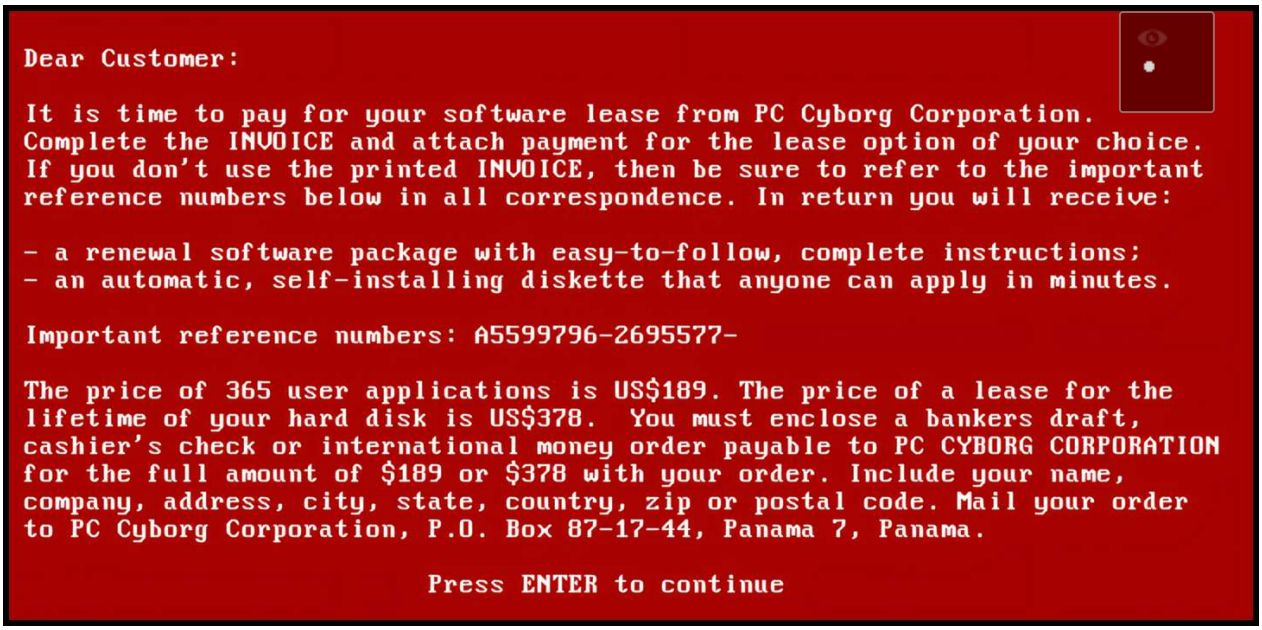
License Agreement

Read this license agreement carefully. If you do not agree with the terms and conditions stated below, do not use this software, and do not break the seal (if any) on the software diskette. PC Cyborg Corporation retains the title and ownership of these programs and documentation but grants a license to you under the following conditions: You may use the programs on microcomputers, and you may copy the programs for archival purposes and for purposes specified in the programs themselves. However, you may not decompile, disassemble, or reverse-engineer these programs or modify them in any way without consent from PC Cyborg Corporation. These programs are provided for your use as described above on a leased basis to you; they are not sold. You may choose one of the following types of lease (a) a lease for 365 user applications or (b) a lease for the lifetime of your hard disk drive or 60 years, whichever is the lesser. PC Cyborg Corporation may include mechanisms in the programs to limit or inhibit copying and to ensure that you abide by the terms of the license agreement and to the terms of the lease duration. There is a mandatory leasing fee for the use of these programs; they are not provided to you free of charge. The prices for "lease a" and "lease b" mentioned above are US$189 and US$378, respectively (subject to change without notice). If you install these programs on a microcomputer (by the install program or by the share program option or by any other means), then under the terms of this license you thereby agree to pay PC Cyborg Corporation in full for the cost of leasing these programs. In the case of your breach of this license agreement, PC Cyborg Corporation reserves the right to take any legal action necessary to recover any outstanding debts payable to PC Cyborg Corporation and to use program mechanisms to ensure termination of your use of the programs. These program mechanisms will adversely affect other program applications on microcomputers. You are hereby advised of the most serious consequences of your failure to abide by the terms of this license agreement: your conscience may haunt you for the rest of your life; you will owe compensation and possible damages to PC Cyborg Corporation; and your microcomputer will stop functioning normally. Warning: Do not use these programs unless you are prepared to pay for them. You are strictly prohibited from sharing these programs with others, unless: the programs are accompanied by all program documentation including this license agreement; you fully inform the recipient of the terms of this agreement; and the recipient assents to the terms of the agreement, including the mandatory payments to PC Cyborg Corporation. PC Cyborg Corporation does not authorize you to distribute or use these programs in the United States of America. If you have any doubt about your willingness or ability to meet the terms of this license agreement or if you are not prepared to pay all amounts due to PC Cyborg Corporation, then do not use these programs. No modification to this agreement shall be binding unless specifically agreed upon in writing by PC Cyborg Corporation.

Programs © copyright PC Cyborg Corporation, 1989
Compiler runtime module © copyright Microsoft Corporation, 1982-1987
All Rights Reserved
IBM® is a registered trademark of International Business Machines Corporation. PC/XT™ is a trademark of International Business Machines Corporation. Microsoft® and MS-DOS® are registered trademarks of Microsoft Corporation.

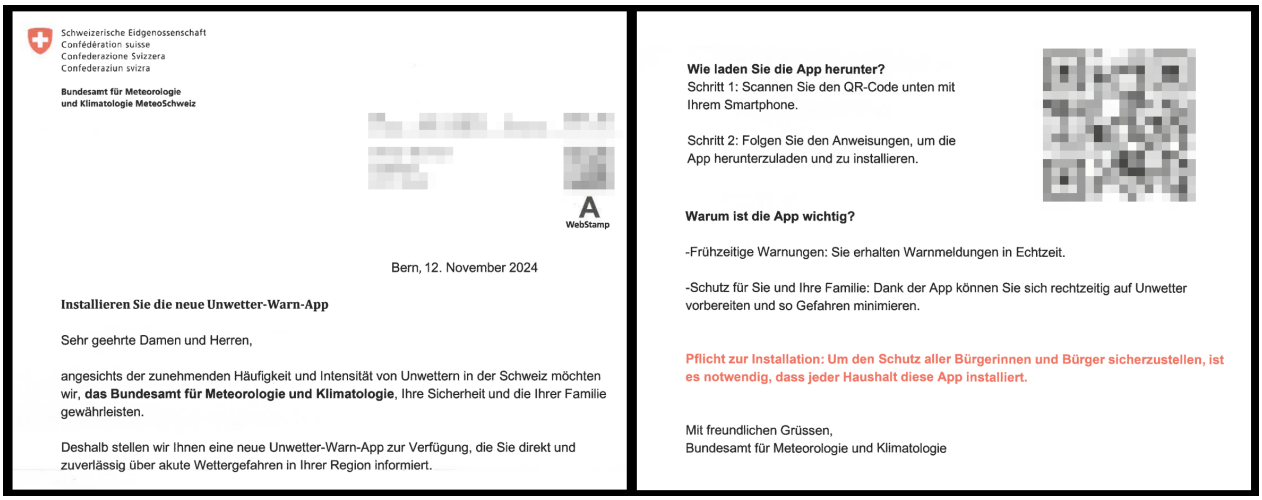
[1989-et írunk, amikor is egy ismeretlen cég AIDS-szel kapcsolatos információs floppylemezt küldött szét 26 ezer egészségügyi intézmény címére](). **A címjegyzék tanúsága szerint három példányt Magyarországra is elküldtek:a Hematológiai Intézetbe, a János Kórházba és a KFKI-be, de ezeknek - állítólag postázás közben - lába kelt, ami utólag szerencsés fordulatnak is értékelhető**.

A lemez egy aljas programozási trükkel operált, és közben figyelte a rendszerindítások számát. **Folyamatosan titkosította a merevlemezen az állományokat és a könyvtárakat, majd a kilencvenedik újraindítás után aztán a trójai az alábbi üzenetet jelenítette meg a képernyőn**, angolul: "*A szoftverbérleti szerződés erre a számítógépre lejárt. Amennyiben még szeretné használni ezt a számítógépet, meg kell újítania a bérleti szerződést. További információkért kapcsolja be a nyomtatót és nyomja meg az Enter billentyűt*".



A kinyomtatott üzenetben aztán **szerepelt egy panamai postafiók címe, amelyre 378 amerikai dollárt kellett küldeni a készítőnek váltságdíjként**. Az elkövető kihasználta, hogy sokan érdeklődtek az akkor még új, ismeretlen és félelmetes AIDS iránt.

A végjáték azért kiszámítható volt: [sikerült elfogni a készítőt, egy bizonyos Joseph L. Poppot, aki Panamában a PC Cyborg Corporation nevű céget jegyezte] és majdnem egy évig készítette elő ezt az akcióját, és persze a megvalósításhoz postaköltségre is kellett költenie.


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Meteorologie und Klimatologie MeteoSchweiz

WebStamp

Bern, 12. November 2024

Installieren Sie die neue Unwetter-Warn-App

Sehr geehrte Damen und Herren,

angesichts der zunehmenden Häufigkeit und Intensität von Unwettern in der Schweiz möchten wir, **das Bundesamt für Meteorologie und Klimatologie**, Ihre Sicherheit und die Ihrer Familie gewährleisten.

Deshalb stellen wir Ihnen eine neue Unwetter-Warn-App zur Verfügung, die Sie direkt und zuverlässig über akute Wettergefahren in Ihrer Region informiert.

Wie laden Sie die App herunter?
Schritt 1: Scannen Sie den QR-Code unten mit Ihrem Smartphone.

Schritt 2: Folgen Sie den Anweisungen, um die App herunterzuladen und zu installieren.

Warum ist die App wichtig?

-Frühzeitige Warnungen: Sie erhalten Warnmeldungen in Echtzeit.

-Schutz für Sie und Ihre Familie: Dank der App können Sie sich rechtzeitig auf Unwetter vorbereiten und so Gefahren minimieren.

Pflicht zur Installation: Um den Schutz aller Bürgerinnen und Bürger sicherzustellen, ist es notwendig, dass jeder Haushalt diese App installiert.

Mit freundlichen Grüssen,
Bundesamt für Meteorologie und Klimatologie

Kicsit erre hasonlít **az a friss eset, amely miatt svájci Nemzeti Kiberbiztonsági Központ (NCSC) riasztást adott ki. A helyi postai szolgálaton keresztül, a svájci meteorológia szolgálat nevével visszaélő leveleket postáztak** ugyanis sokaknak.

Ebben egy időjárási veszélyhelyzetre figyelmeztető alkalmazást ajánlottak a címzetteknek, azonban **a hivatalos Severe Weather Warning App nevű eredeti program helyett a mellékelt QR kód egy nem-hivatalos alkalmazás letöltési helyre irányította** a felhasználókat.

A letöltésre kínált alkalmazás azonban egy kártékony program, amely egy banki trójait kártevővel fertőzte meg az androidos eszközöket. Azon túl, hogy nem a Google Play hivatalos piactérről származik a program, csak nagyon apró eltérésekre lehetett esetleg felfigyelni, az app neve Alertswiss helyett AlertSwiss volt, és a kíséről logó sem az eredeti grafikájú volt.

A Coper nevű banki kártevő egy veszélyes program, amelyet billentyűnaplózásra, a kétfaktoros hitelesítési SMS-ek és push értesítések lehallgatására, valamint kémkedésre terveztek. A banki belépési és hitelesítő adatok ellopásával a támadók kifoszthatják a felhasználók bankszámláját.

A már klasszikusnak mondható korábbi Hogyan szúrjuk ki a gyanús Android appokat bejegyzésben már alaposan összefoglaltuk a legfontosabb tudnivalókat a témával kapcsolatban, amihez most csak annyit érdemes hozzátenni, hogy **a rendszeres frissítések és vírusvédelmi program futtatása mellett a kéretlen QR kódokra is** érdemes lesz jobban odafigyelni.

Szólj hozzá!
Címkék: posta levél csalás átverés svájc trójai kártevő banki qrcode quishing

Ajánlott bejegyzések:

Fontos vagy nekem

MBH-fiókjának jelszava 24 órán belül lejár

Fontos vagy nekem

Nő a QR-kódos visszaélések száma

"NEM TUDJUK KISZÁLLÍTNI A CSOMAGÁT"

MBH-fiókjának jelszava 24 órán belül lejár

Árad a malware a Youtube oldalain is

Árad a malware a Youtube oldalain is

Árad a malware a Youtube oldalain is

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Egy a jelszónk, tartós 123456

2024. november 28. 20:28 - Csizmazia Darab István [Rambo]

Nem igazán mutat szebb képet az évről évre közreadott **Nordpass jelszavakkal kapcsolatos idei 200-as listája sem.** Bár mindenki tudja, hogy a qwerty, a password és az 123456 nem igazán felel meg semmilyen biztonsági kritériumnak, népszerűségük ettől függetlenül látszólag töretlen.

Minden év novemberében kerül kiadásra ez a leggyengébb jelszavak összesítő listája, amelyet most hatodik alkalommal tett közzé a Nordpass. Az elemzésük alapja egy 2.5 TB-os adatkészletből származik, amelyet több különböző forrásból, lopott, kiszivárgott jelszavak listáiból gyűjtöttek össze a darkwebről.

A lista csak olyan friss elemeket tartalmaznak, amelyek egy éven belül szivárogtak ki.

NATIONAL NEWS

The worst passwords you could have in 2024 — or any year

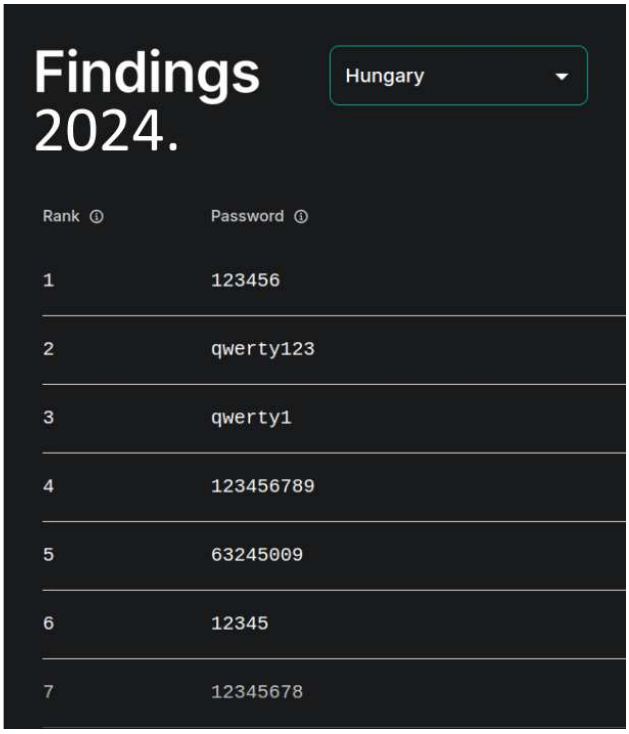
by: Russell Falcon
Posted: Nov 17, 2024 / 09:50 AM CST
Updated: Nov 17, 2024 / 09:50 AM CST

Here are the 15 most common passwords.

Rank	Password	Time to crack it	# of times the password was used
1.	123456	< 1 second	3,018,050
2.	123456789	< 1 second	1,625,135
3.	12345678	< 1 second	884,740
4.	password	< 1 second	692,638
5.	qwerty123	< 1 second	642,638
6.	qwerty1	< 1 second	583,630
7.	111111	< 1 second	459,730
8.	12345	< 1 second	395,573
9.	secret	< 1 second	363,491
10.	123123	< 1 second	351,576
11.	1234567890	< 1 second	324,349
12.	1234567	< 1 second	307,719
13.	000000	< 1 second	250,043
14.	qwerty	< 1 second	244,879
15.	abc123	< 1 second	217,230

Az első helyen álló 123456 megőrizte tavalyi győztes pozícióját. **A világszintű eredmény statisztikai táblája mellett lehetőségünk van 35 különböző ország szerint is szűrni az eredményeket, így összehasonlíthatjuk a tavalyi és idei magyar élmezőnyt is.**

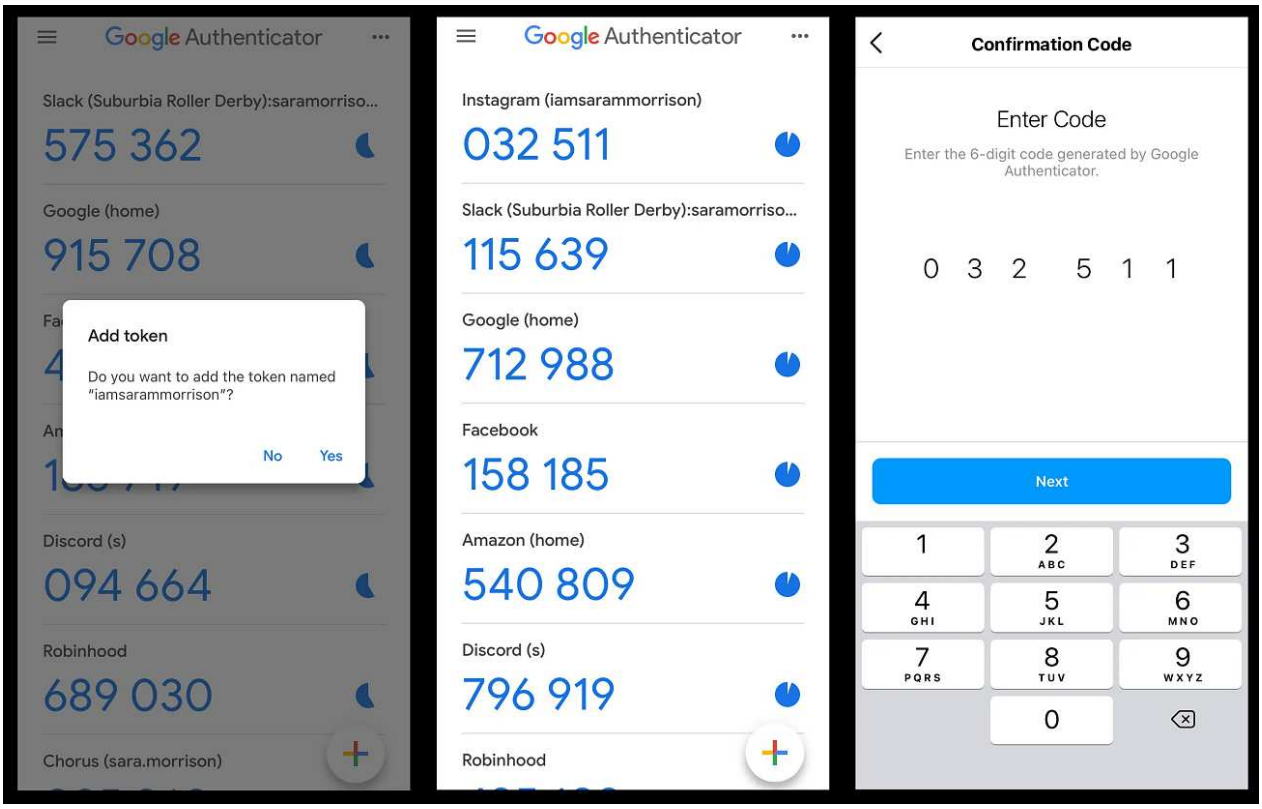
A jelszavak primitívsége abból a szempontból is meglepő, hogy már kismillió jelszószéf alkalmazás érhető el, amelyek kényelmesek és biztosítják az erős egyedi jelszavak biztonságos védelmét anélkül, hogy mindenre emlékezni kellene.

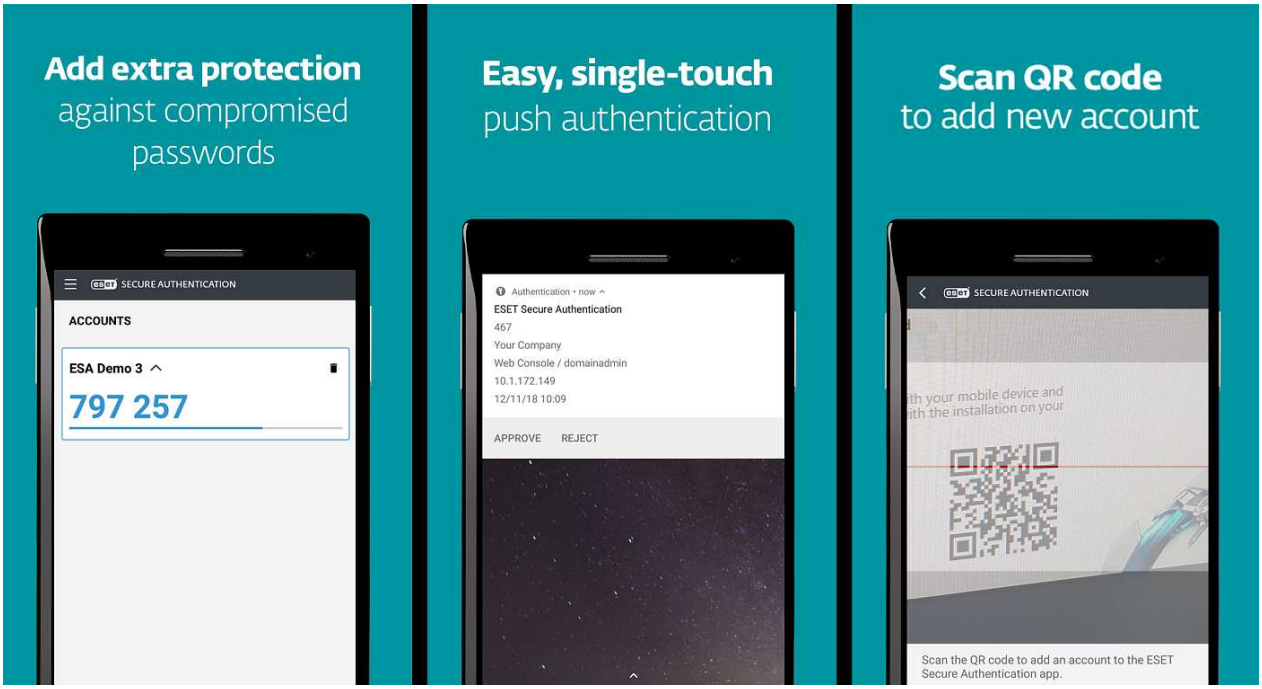


És ha már jelszó, akkor érdemes az ügyfélkapus belépést még idejében elvégezni azoknak, akik az ügyfélkapu+ szolgáltatást szeretnék igénybe venni. Ha valaki nem kíván a DÁP-ra (Digitális Állampolgárság) regisztrálni, akkor **érdemes még 2025. január 15 előtt az Ügyfélkapu+ módra**

váltani, ugyanis a határidő lejárta után már csak DÁP-ra lehet váltani.

[A mellékelt videó részletesen bemutatja](#) az Ügyfélkapu+ váltást.





A dolog lényege, hogy ehhez szükséges egy kétfaktoros autentikációs app használata, [ehhez például az ESET Secure Authentication alkalmazás](#), vagy egy másik lehetséges megoldásként [a Google Hitelesítő is használható](#). **Ehhez mindössze be kell olvasni az ügyfélkapun megjelenő QR kódot, és a generált kódot begépelni a weboldalon. Ettől kezdve az**

Ügyfélkapu+ belépési lehetőséget használva már egy megerősített védelmet kapunk.

1 komment
Címkék: statisztika biztonság toplista jelszó leggyengébb hitelesítés gyenge ügyfélkapu leggyakoribb autentikáció 2fa jelszómenedzser kétfaktor kéttényezős nordpass jelszószéf ügyfélkapu+

Ajánlott bejegyzések:

Jelszó világvége

Ne reszkessetek betörők! A legnépszerűbb 2024-es posztok

Jelszó világvége

A legnépszerűbb 2024-es posztok

Amikor a suszter cipője is admin

Biztonság + kényelem = jelszókezelő

Kommentek:

eseslevi 2024.11.29. 10:44:28

Én csak azt nem értem, miért aggodnak mások az én jelszavam miatt. És az idegesít a legjobban, mikor meg kell változtatnom a jelszavamat, mert a

rendszernek nem tetszik, hogy már régóta használom vagy nem tetszik, hogy egyszerű, jól meg jegyezhető. Igaz, hogy én interneten nem intézek semmit, se vásárlást, se intézkedést valami oldalon. Szerencsére a nevemen kívül semmi sincs az online felületeken. Na, ezt lopják el a hakkerek! Sok sikert!

Válasz erre

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

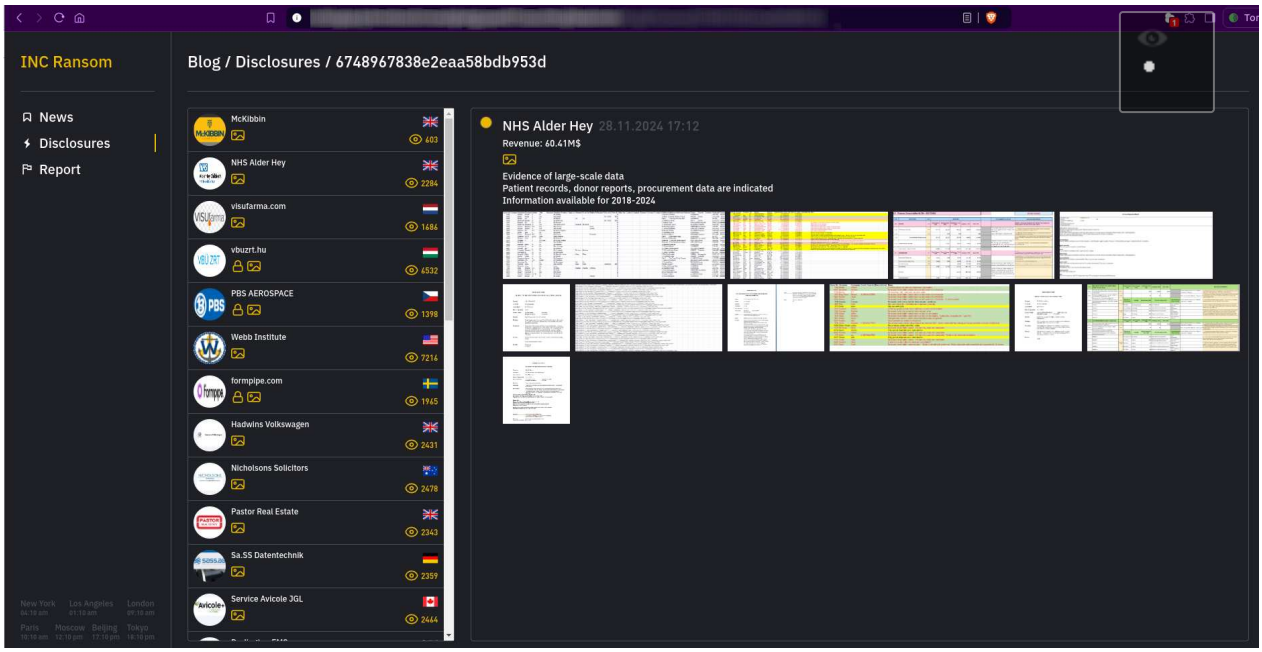
Újabb rombolás brit kórházakban

2024. december 03. 13:37 - Csizmazia Darab István [Rambo]

Az egészségügy sajnos gyakori célpontja a ransomware bűnbandáknak, **ezúttal az Egyesült Királyságban került sor több ilyen jellegű támadásra.**

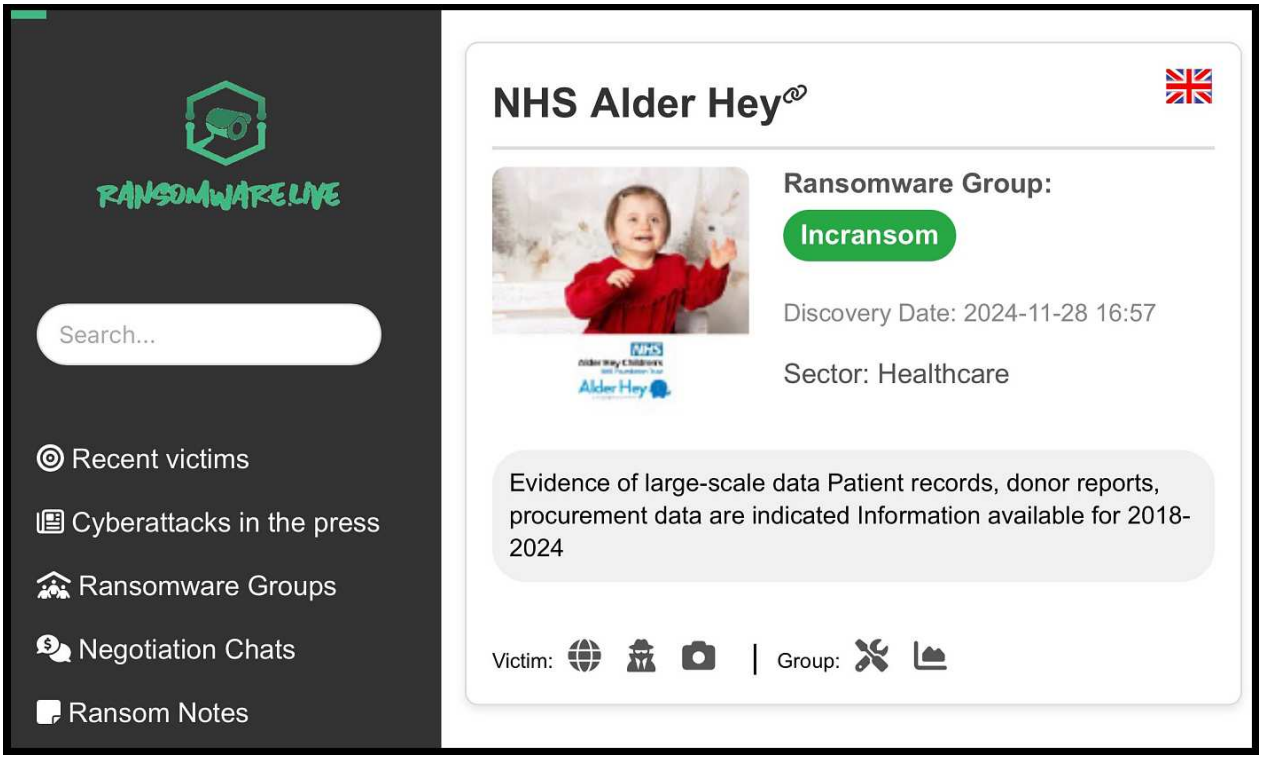
Az első áldozat a Wirral Egyetemi Oktatókórház volt, ahol a támadás észlelése után lekapcsolták a számítógépes hálózatot. Az NHS Trust közleménye szerint **kénytelenek voltak visszatérni a papíralapú működési módhoz, plusz telefon és fax.**

A kórház a szülésre váró pácienseket ilyen körülmények között is fogadja, és bár korábban szerepelt a nyilatkozatban a 24 órás sürgősségi ügyeleti lehetőség is, ez a tájékoztatás később már lekerült a weboldalukról, illetve **a súlyos eseteknél is figyelmeztetnek a szokásosnál hosszabb várakozási időre. Idén ez már a harmadik olyan támadás volt, amelyik az NHS Trust (az Egyesült Királyság Nemzeti Egészségügyi Szolgálata) valamely egészségügyi intézményét sújtotta, ebben az esetben pedig a RansomHub csoport a felelős.**



Itt azonban nem álltak meg az események, ugyanis **rövid időn belül az Anglia egyik legjobb gyermekkórházának számító NHS Alder Hey Gyermekkórházat is megtámadták.**

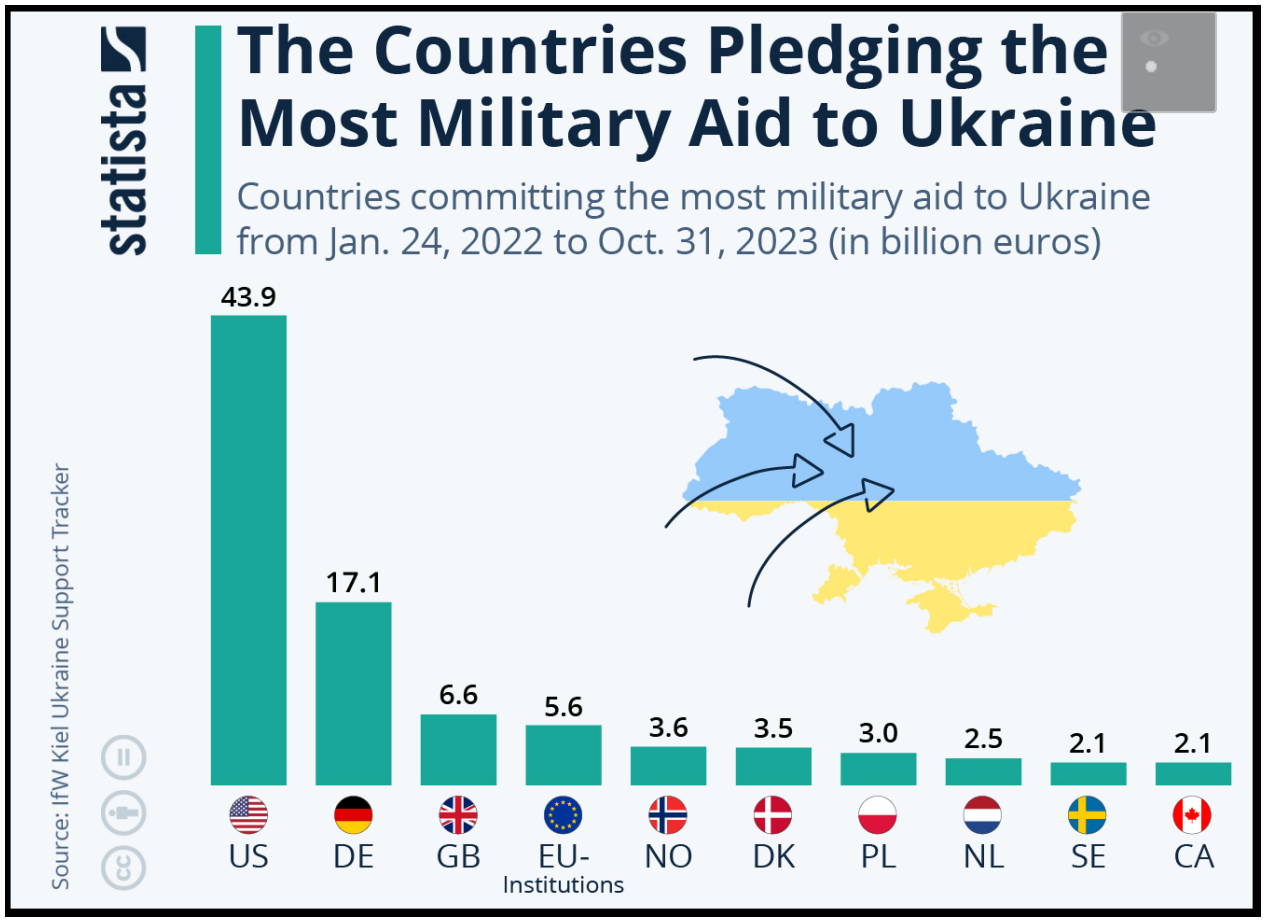
Az INC Ransom, amely idén júniusban az NHS Scotland elleni támadást is jegyezte, most azt állítja, hogy **ellopta a liverpooli Alder Hey Gyermekkórház, valamint a Liverpool Heart and Chest Hospital NHS Foundation Trust adatait is.**

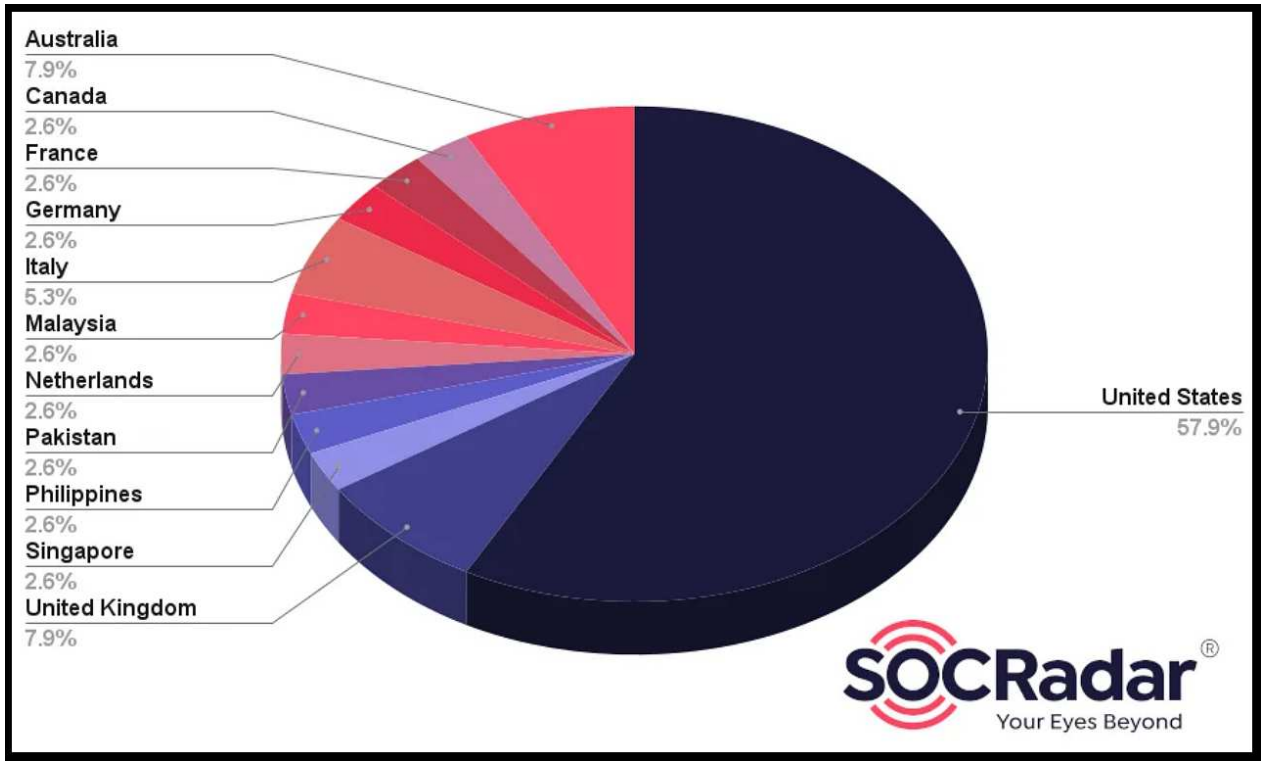


Ha az INC Ransom neve ismerősen cseng valakinek, az korántsem a véletlen műve, ez a brigád törte fel és töltötte fel árverésre a magyar Védelmi Beszerzési Ügynökség adatait is, ahol 5 millió dollárt követeltek az ellopott adatokért.

A kórházak elleni támadás során ellopott adatok egy részét itt is feltöltötték a netre, hogy a zsarolási szándékuknak nyomatékot adjanak. Ezek között betegek és donorok személyes adatai, a kórháznak adományozókkal kapcsolatos részletes információk, betegek orvosi jelentései, valamint az üzemeltetéssel kapcsolatos pénzügyi dokumentumok is szerepelnek egy jelentős idősávban, 2018-tól egészen 2024-ig.

Az intézmények együttműködve a hatóságokkal vizsgálják magát az incidenst, valamint a kiszivárogtatott adatok hitelességét. Az mindenesetre meglehetősen **furcsa, hogy alig egy hét leforgása alatt két külön támadás is lezajlott ennyire közeli szervezetek ellen.**





Nem lehet nem észrevenni, hogy a kiválasztott kórházi célpontok lokációja gyakran olyan országokban található, amelyek valamilyen formában aktívan segítik az Oroszország által indított háborúban a megtámadott ukrán felet, míg az elkövető bűnözők orosz kötődésűek, és vélhetően az ilyen akciókkal büntetik meg az adott országokat. Az

egészségügyi intézmények támadása alaphangon is elítélendő tett, de a gyerekkórházak elleni fellépések olyan aljas cselekmények, amire semmi nem lehet elfogadható magyarázat.

Szólj hozzá!
Címkék: leállás brit orosz támadás zsarolás váltságdíj kórházak inc ransom ransomware szivárogtatás zsarolóvírus doxing ransomhub inc-ransom

Ajánlott bejegyzések:

Senki többet harmadszor?
A jó kolléga nem csak ígér, hanem be is tart
Halálos fegyver: doxing
LockBit üti Subway, sakk

Senki többet harmadszor?
A jó kolléga nem csak ígér, hanem be is tart
Halálos fegyver: doxing
LockBit üti Subway, sakk

8 kórház, 30 klinika, 2.5 millió betegadat

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

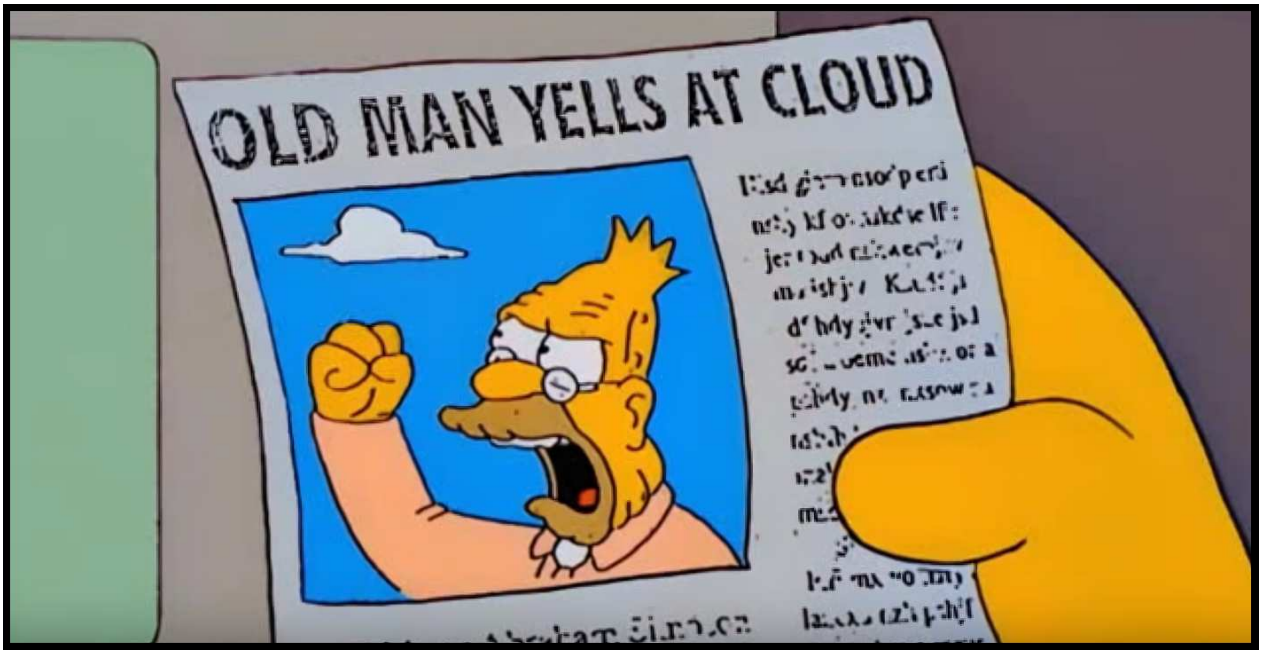
about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Új bejelentkezés a felhőnkbe. Vagy mégsem?

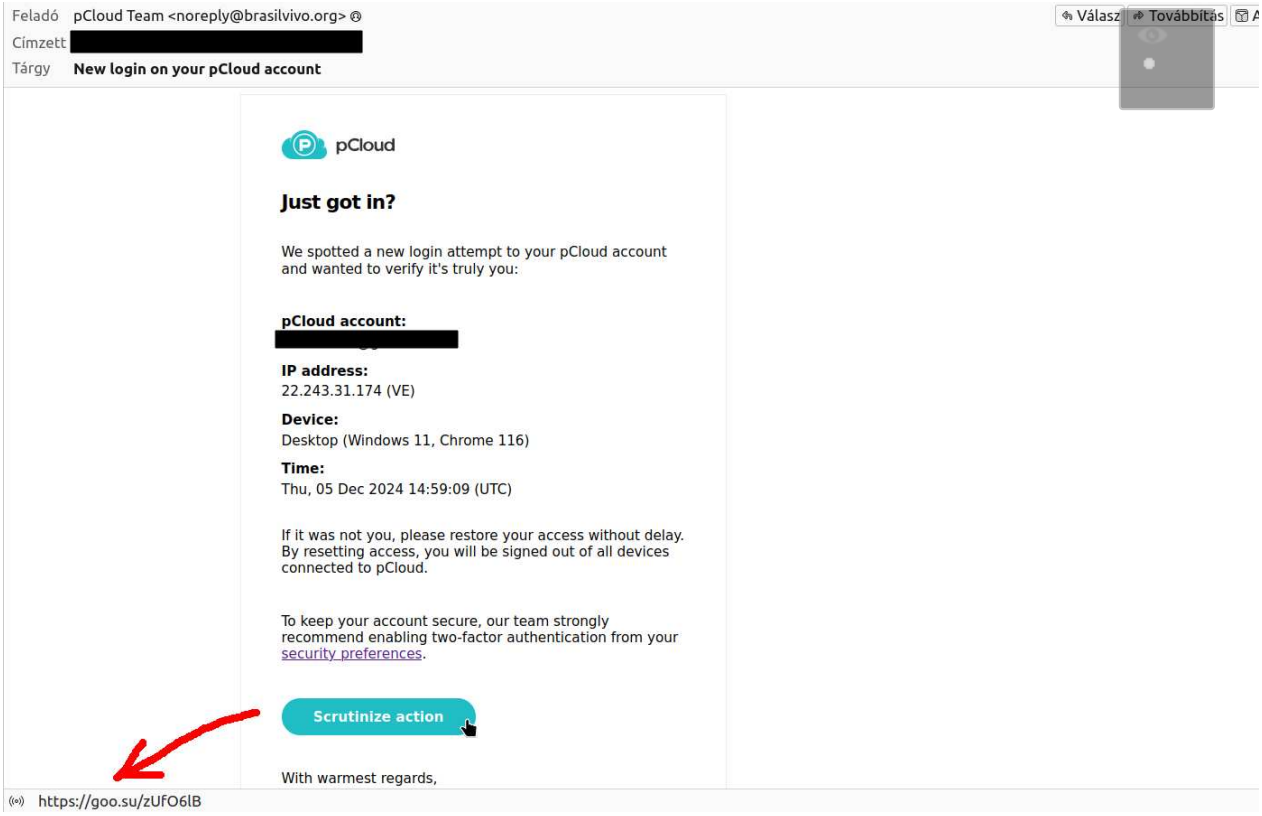
2024. december 06. 17:40 - Csizmazia Darab István [Rambo]

Egy újabb csalási hullám érkezett, **ezúttal a pCloud szolgáltatás nevével élnek vissza, ráijesztve a gyanútlan felhasználókra.**

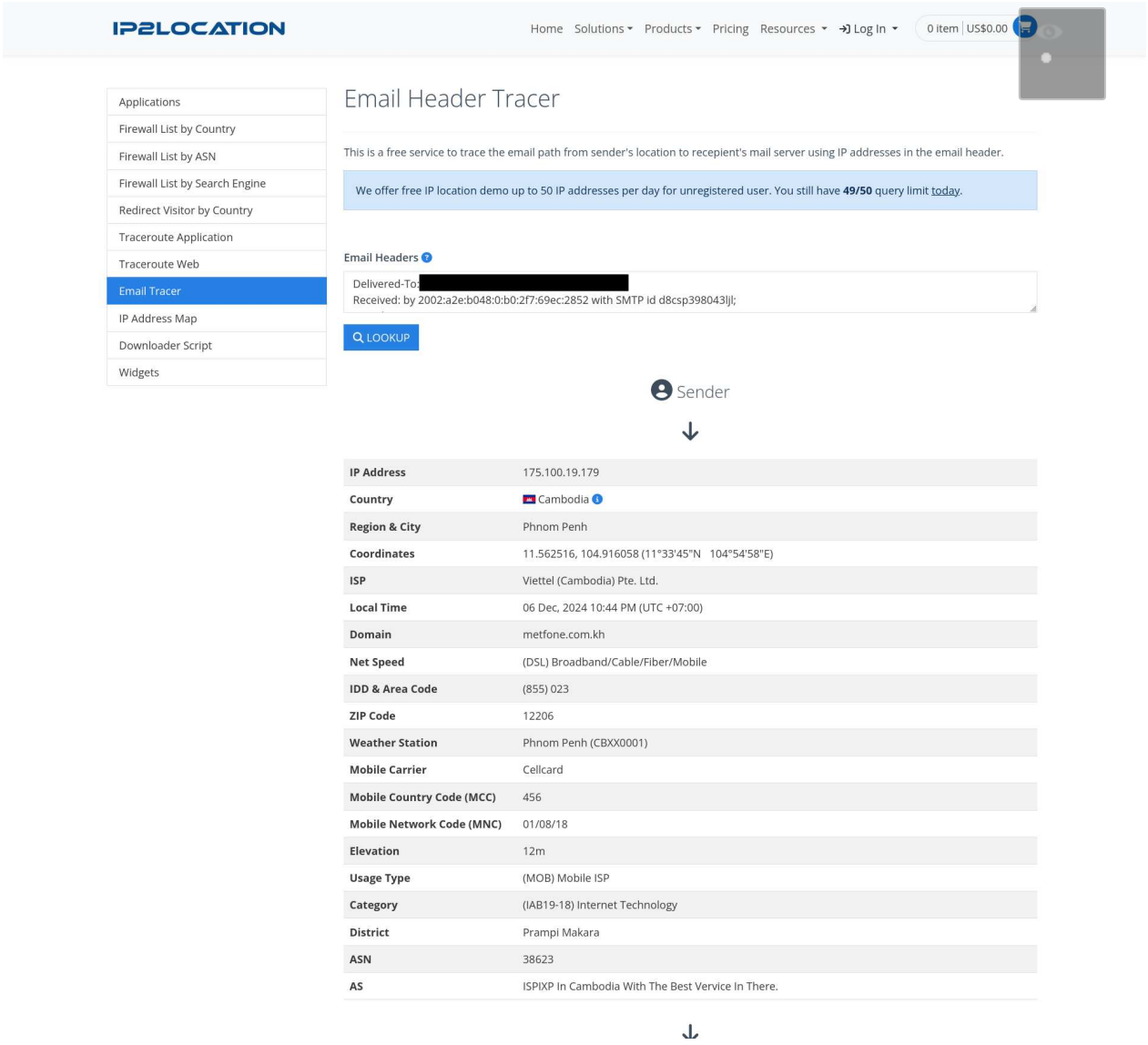


A levél l**átszólag a pCloud-tól érkezik és azt írják benne, hogy új bejelentkezési kísérletet észleltek a tárhely fiókunkba, és most azt javasolják, hogy ellenőrizzük le ezt**.

A kiegészítő információk pedig azt mutatják, hogy mindez egy asztali gépről történt (pl. Windows 11, Chrome 116), és mellékelnek egy állítólagos IP címet is egy konkrét időponttal együtt.

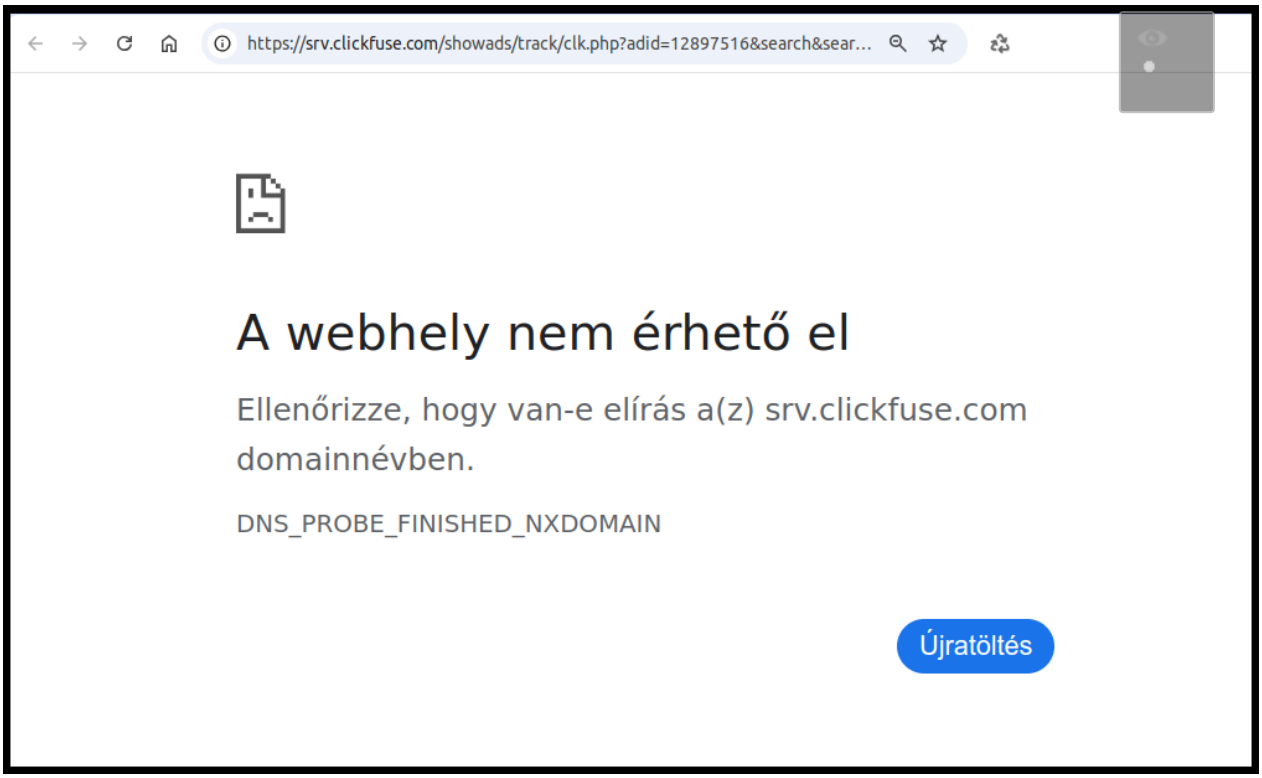


Kezdjük a felgöngyölítést a feladó címénél, ugyanis **zsinórban jött ugyanebből vagy fél tucat.** A feladók noreply@brasilvivo.org, noreply@wsisiz.edu.pl, noreply@knust.edu.gh, noreply@toucansurf.com és hasonlók. Hát ezek tutira nem pCloud hivatalos címek.



Aztán ha megnézzük az állítólagos belépéshez tartozó bekamuzott IP címeket, azok is roppant változatosak: Grenada, Franciaország, Jamaica, Venezuela, stb. Szóval lehet megijedni, hogy a csúnya bácsik innen fértek hozzá mindenünkhöz.

Ha pedig ráeresztjük az e-mail trace-t, akkor láthatóvá válik, hogy a feladói cím is elég változatos, van amelyik például Kambodzsából érkezett hozzánk.



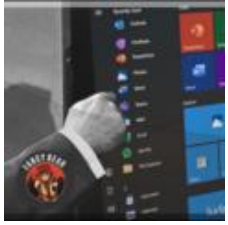
Az időpont mindig egy közelmúlti, sok esetben tegnapi december 5-e, bár néhánynál még november vége van feltüntetve. **A mellékelt link minden esetben valamilyen rövidített URL, amit első látásra nem tudhatunk, hova is vezet pontosan.** Úgy tűnik, hogy ezeket a belinkelt feltört weboldalakat időközben szerencsére többségében már lelőtték, így igazi adathalász oldalba már nem is sikerült belefutnunk.

Összefoglalva **mindig érdemes figyelmesen nyitogatni az e-maileket akkor is, ha nem egy bank vagy valamilyen csomagküldő szolgálat a feladója, hanem valamilyen netes szolgáltató.**

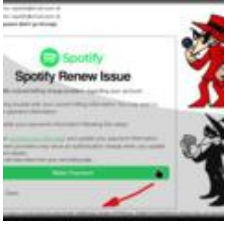
Szólj hozzá!
Címkék: vagy csalás átverés hamis üzenet tárhely felhő mégsem vagymégsem pcloud

Ajánlott bejegyzések:

Gáz van, sikertelen fizetés rossz adatokkal



Windows update vagy mégsem?



Spotify megújítási probléma - vagy mégsem?

Új földgáz számlája készült - vagy mégsem? CAPTCHA, amely nem az ember-gép relációt teszteli

CAPTCHA, amely nem az ember-gép relációt teszteli

Gáz van, sikertelen fizetés rossz adatokkal

CAPTCHA, amely nem az ember-gép relációt teszteli

CAPTCHA, amely nem az ember-gép relációt teszteli

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz






Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

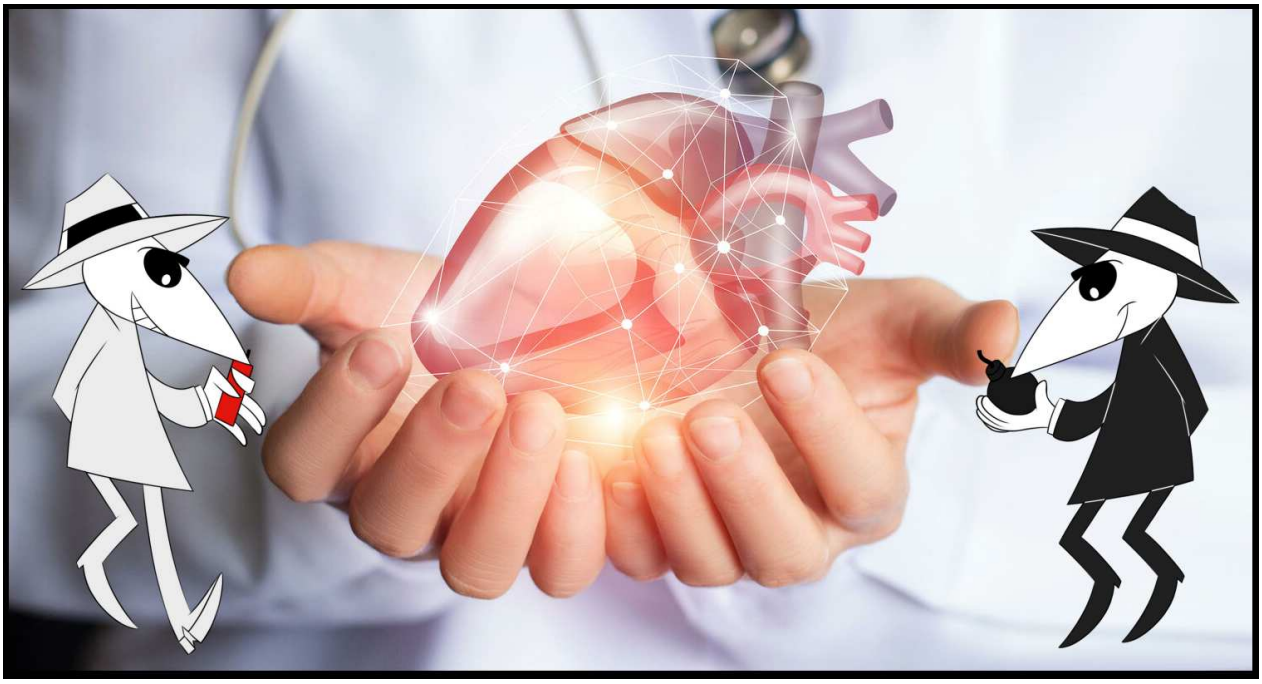
about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Zsarolóvírus a szívsebészeti orvosi eszközöket gyártónál

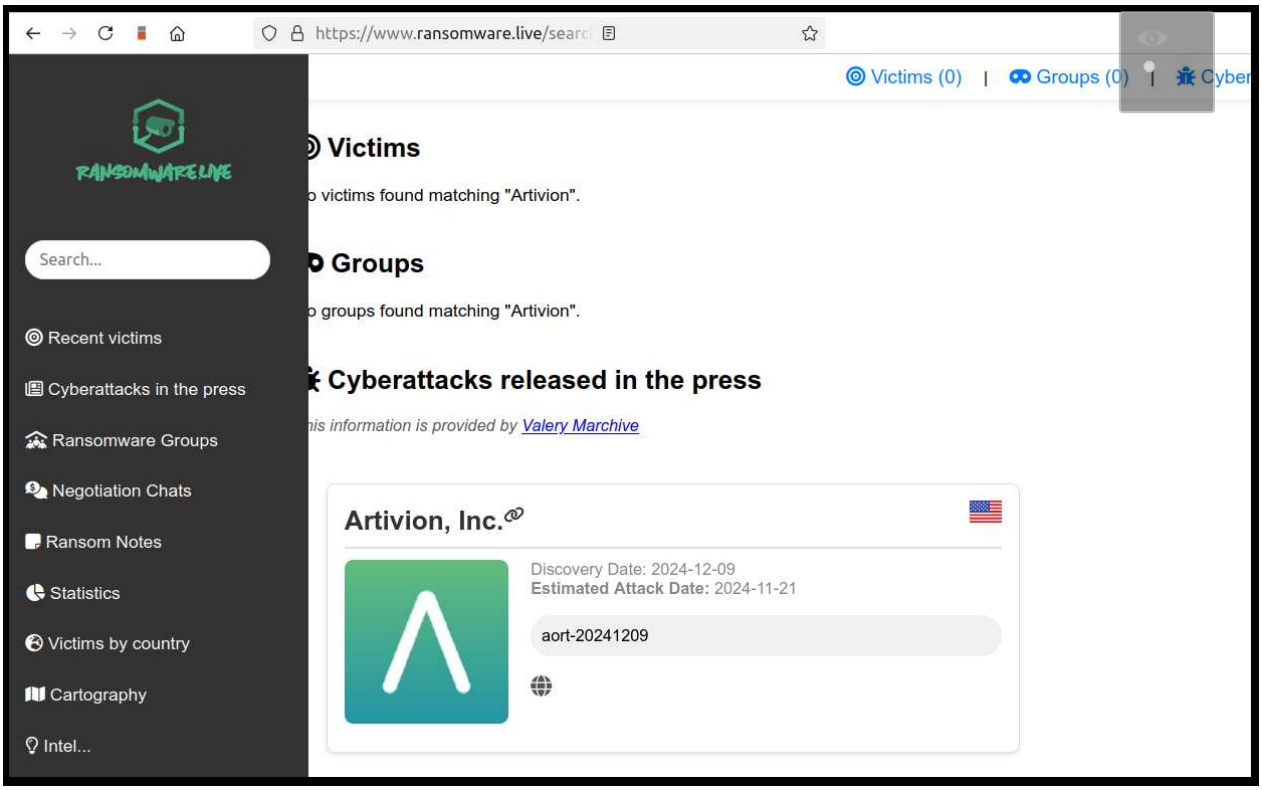
2024. december 10. 13:27 - Csizmazia Darab István [Rambo]

Egy atlantai székhelyű vállalatnál **talált be a ransomware, amely az adatok titkosítása mellett adatokat is lopott**. A támadás miatt részlegesen leállították a számítógépes rendszereiket.



Az Artivion nevű vállalatnak több, mint 100 országban vannak képviseleti irodái, az Egyesült Államokban pedig gyártó üzemei is, például Atlantában, Georgia államban, Austinban és Texasban, **valamint Európában is, Németországban.**

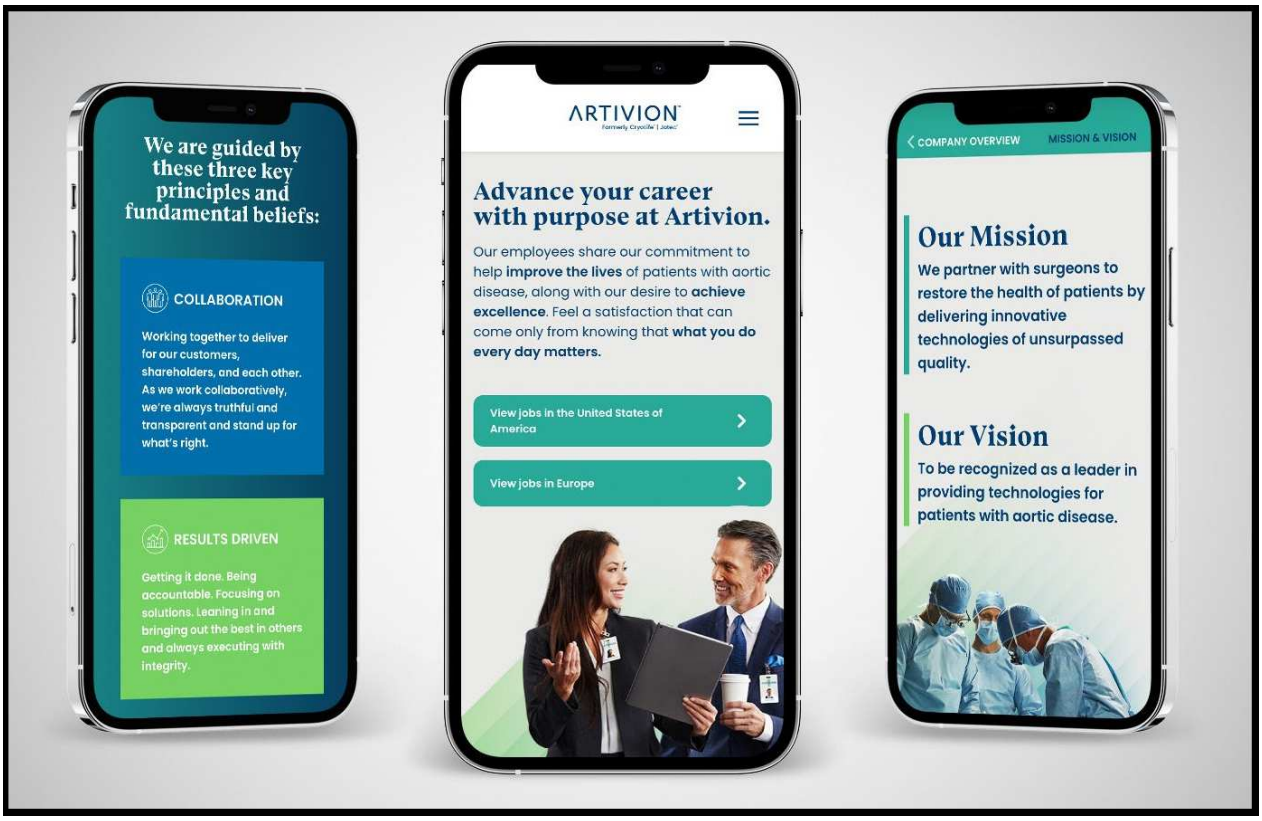
A világszerte 1250 embert foglalkoztató cég **a zsarolóvírus incidens november 21-i észlelése után rögtön lekapcsolta számítógépes rendszereinek jelentős részét, és külső kiberbiztonsági, jogi valamint igazságügyi szakértők bevonása mellett azonnal megkezdték a kárfelmérést, illetve az eset okainak részletes felderítését.**



A hivatalos közleményük szerint a vállalati normál működésében, **beleértve ebbe a rendelésfeldolgozást és a termékek kiszállítását azóta már nagyjából helyre állt a megszokott rend,** és az ezeken a területeken bekövetkezett fennakadásokat többnyire sikeresen orvosolták.

A hivatalos szervek felé is megtették a bejelentést, **ám ami még egyelőre nem derült ki, pontosan mely ransomware csoport felelős ezért az akcióért és történt-e irányukba váltságdíj követelés. Erre nézve a Security Week is megkereste a céget, ám válasz egyelőre nem érkezett.**

Rákeresve a gyűjtő portálokon, a RansomFind.io oldalon nem volt találat, **a ransomware.live weboldalán viszont igen, igaz ott is csak egy szűkszavú mondat hivatkozott a november 21-i bejelentésre.**



Emlékezetes, hogy a közelmúltban brit egészségügyi intézmények ellen tömeges támadásokat regisztráltak, különböző zsarolóvírus csoportoktól. Jelentős orvosi szolgáltatók ellen is előfordultak már hasonló támadások, például 2020-ban a COVID-19 világjárvány alatt a dializístermékek legjelentősebb szállítója és szolgáltatója, a Fresenius vállalat volt célpont.

Szólj hozzá!
Címkék: eszközök orvosi támadás gyártó ransomware zsarolóvírus doxing artivion

Ajánlott bejegyzések:

Újabb rombolás brit kórházakban

Ország, város, ransomware

Ransomware a Volkswagennél

Senki többet harmadszor?

Halálos fegyver: doxing

Halálos fegyver: doxing

Halálos fegyver: doxing

Halálos fegyver: doxing

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

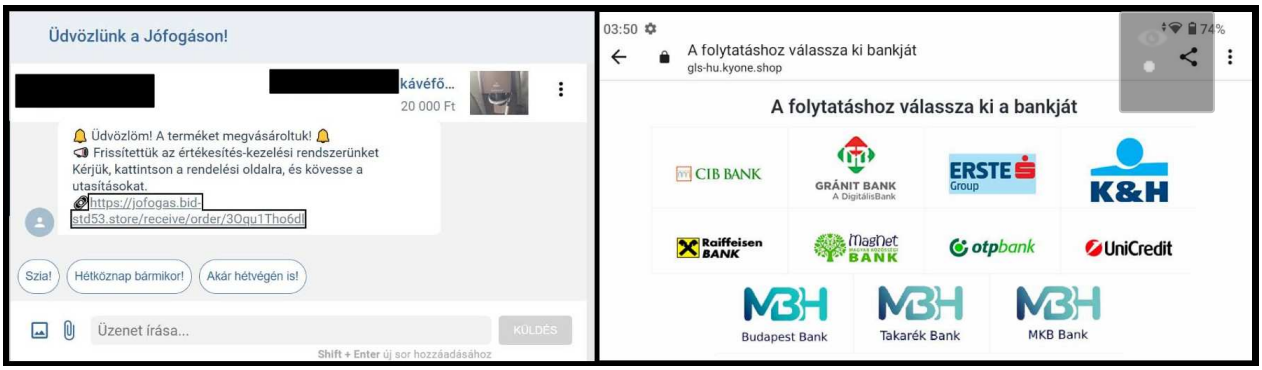
Adathalászat vagy jófogás?

2024. december 12. 17:07 - Csizmazia Darab István [Rambo]

Klasszikus adathalász trükk, amikor az állítólagos vevő maga akarja intézni a szállítást (pedig semmi köze hozzá), és emiatt **hamis linket küld az eladóna**k látszólag egy szállítmányozási cégek vagy kinézetre banki belépési oldalnak tűnő hivatkozást.

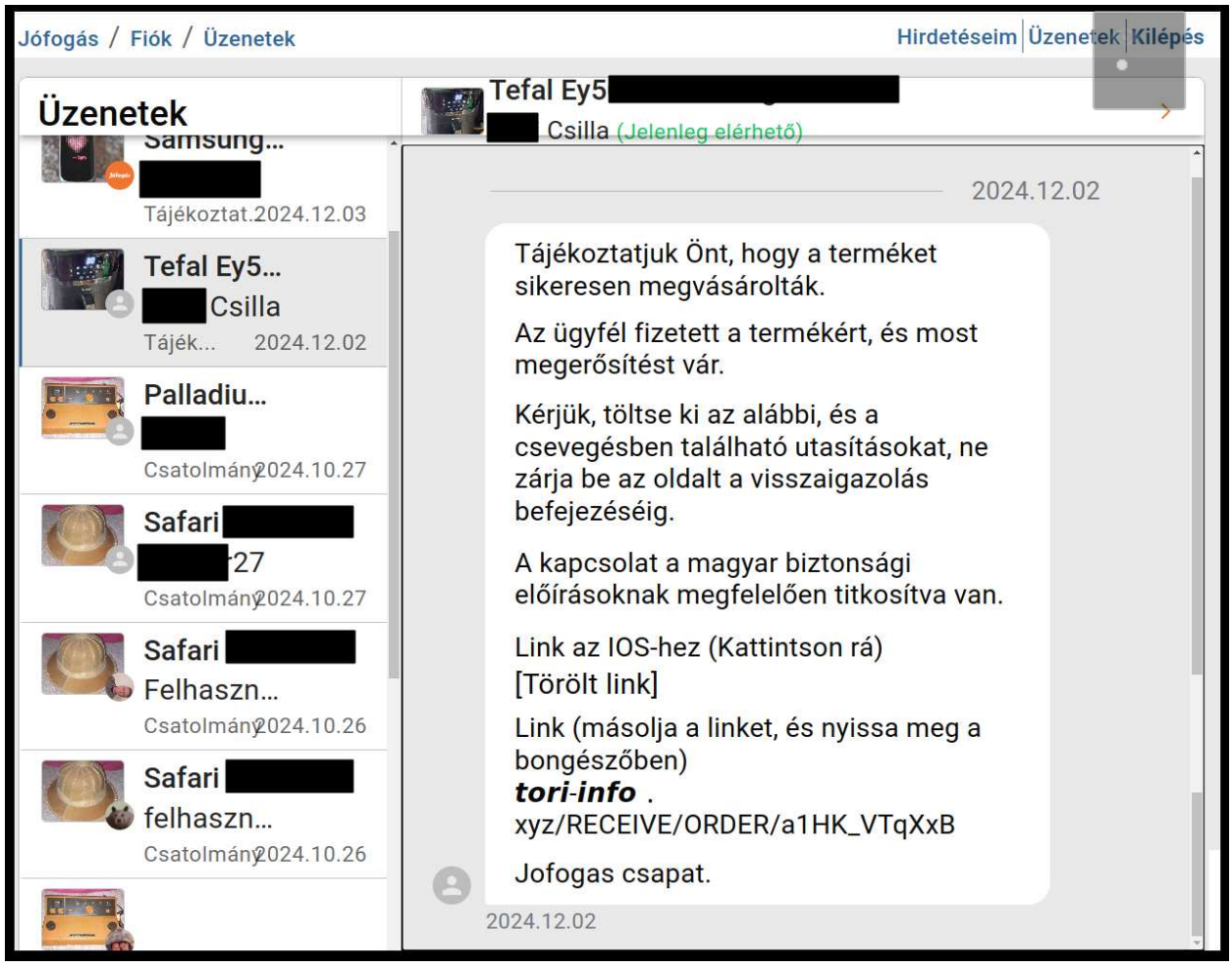
A legfrissebb statisztikák szerint több, mint **1.1 milliárd Facebook-felhasználó használja havonta a Facebook Marketplace szolgáltatást.** Hetven országból, köztük Magyarországról is rengetegen használják, de a helyi eladandó dolgok jelentős részét a Vatera és a Jófogás oldalain is hirdetik.

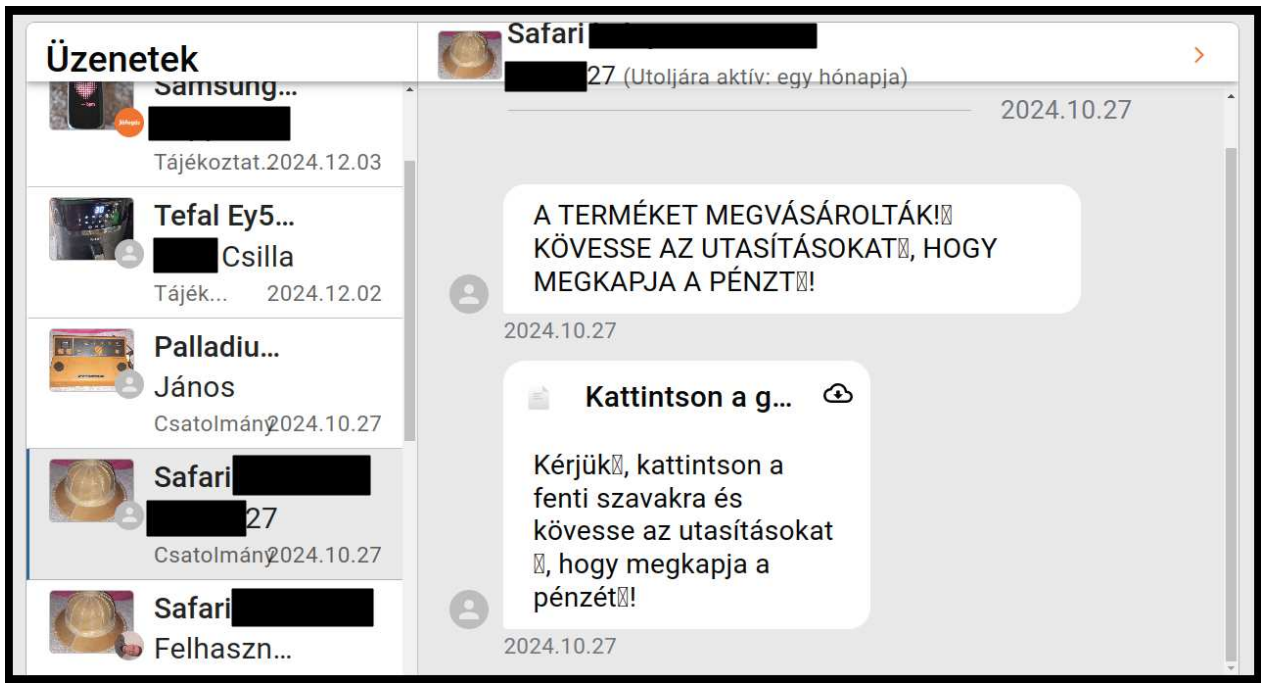
A csalók persze mindenhol felbukkannak, ami önmagában még nem is meglepetés, de az, hogy milyen sokan vannak, és milyen gyakran kerülünk szembe velük, az tényleg meghökkentő.



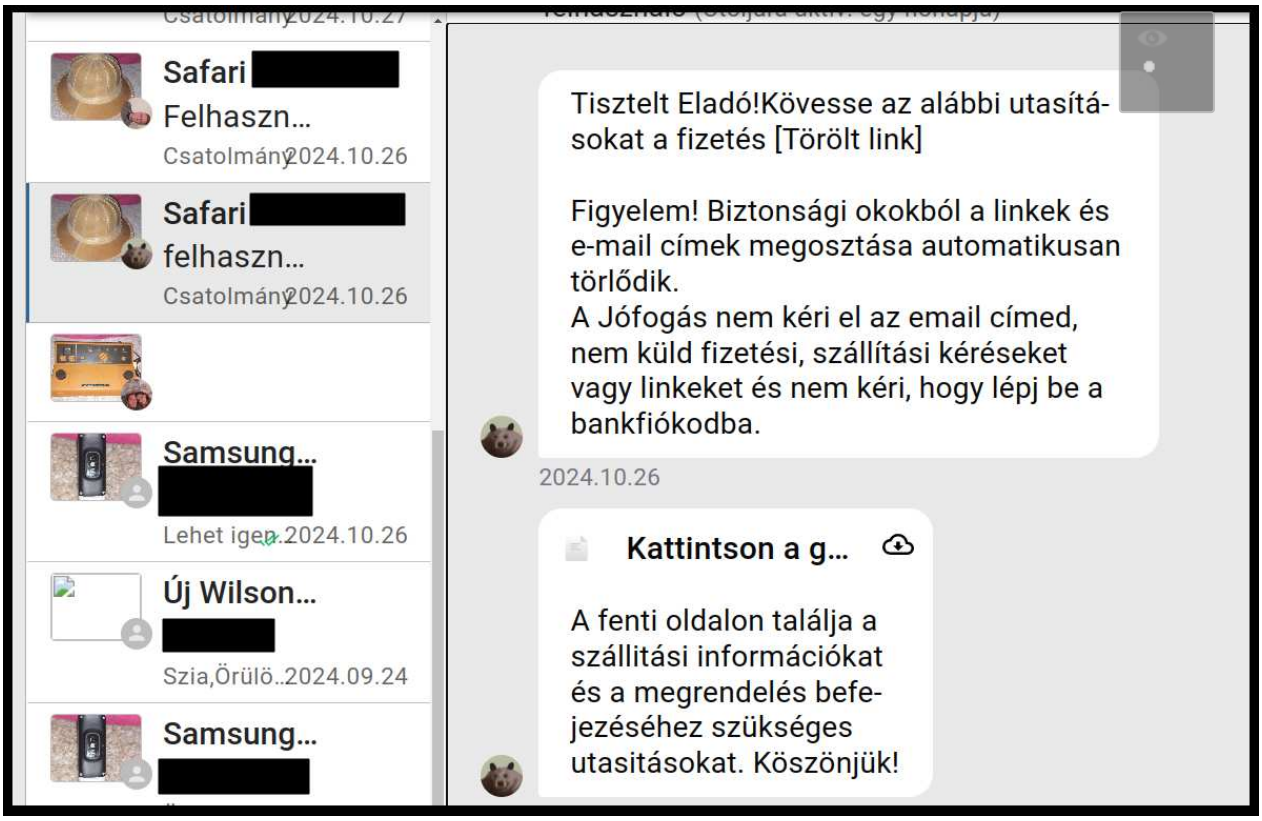
Bármilyen árucikket is tesz fel valaki eladásra, r**övid időn belül tömegesen megjelennek nála a csalók, illetve az automata botok.**

Az üzenet jellemzően nagyon hasonló, például: "*A TERMÉKET MEGVÁSÁROLTÁK! KÖVESSE AZ UTASÍTÁSOKAT, HOGY MEGKAPJA A PÉNZT!*" **És mellé valamilyen link is érkezik. Amire kattintani nem érdemes.**





A próbálkozások sokszor roppant primitívek, vagyis automatizált botok végzik, így **könnyen előfordulhat, hogy elhajtunk egy ilyen érdeklődőt, de percek múlva újra megjelenik ugyanazzal a kérdéssel.**



Szerencsére az utóbbi időben a **kártékony linkek jelentős részét már automatikusan kitörlik** a platformok.

Az óvatosság mindenesetre minden felhasználó, potenciális vevő és eladó számára kiemelten fontos.

Szólj hozzá!
Címkék: csalás átverés vatera szállítás marketplace adathalászat jofogas

Ajánlott bejegyzések:

Bot vívás

Csomagja érke... Na most már elég!

Csomagja érke... Na most már elég!

Utolsó emlékeztető a fiók felfüggesztése előtt

Utolsó emlékeztető a fiók

Fontos vagy nekem

Fontos vagy nekem

felfüggesztése előtt

Ment a hűtlen hamis linkkel

Ment a hűtlen hamis linkkel

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

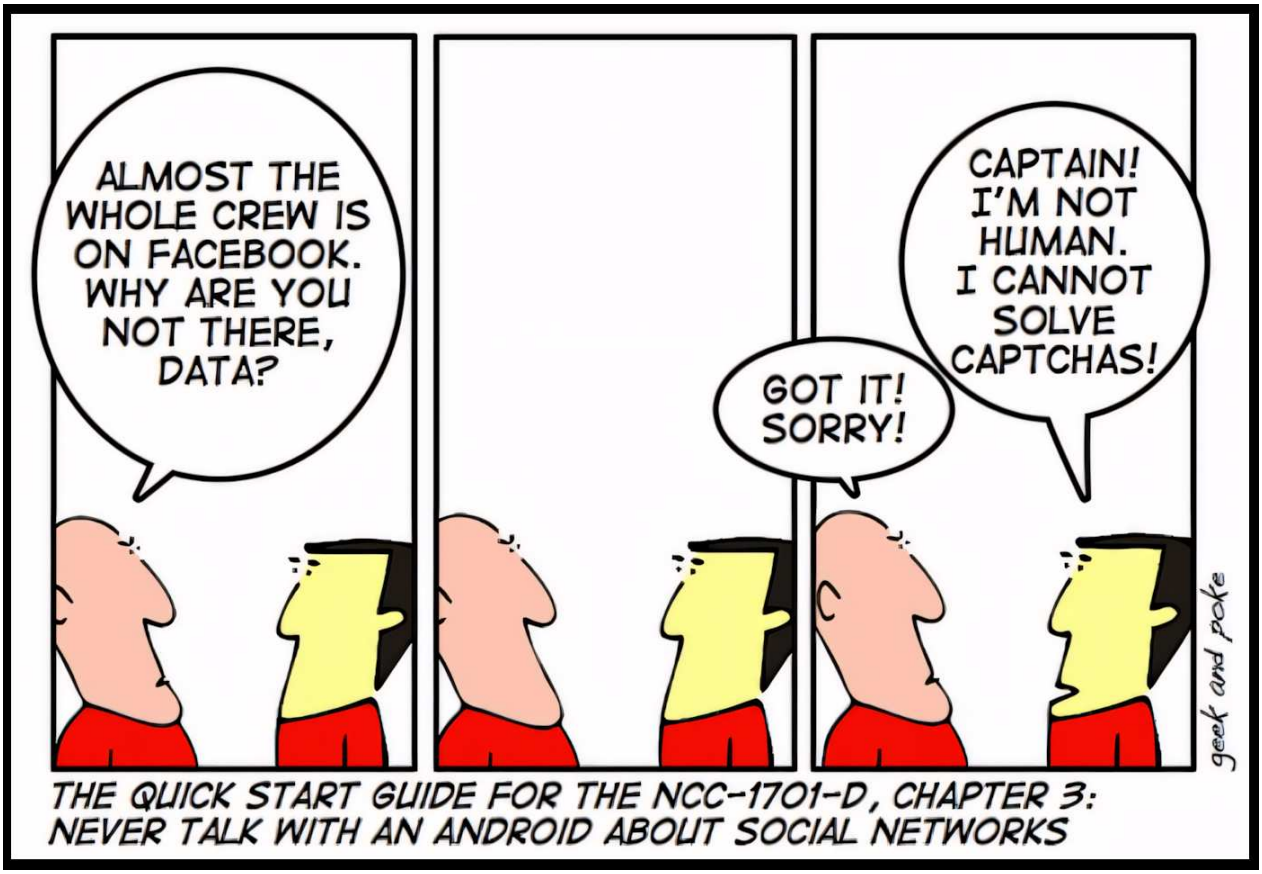
Facebook

Tovább a Facebook-ra

CAPTCHA, amely nem az ember-gép relációt teszteli

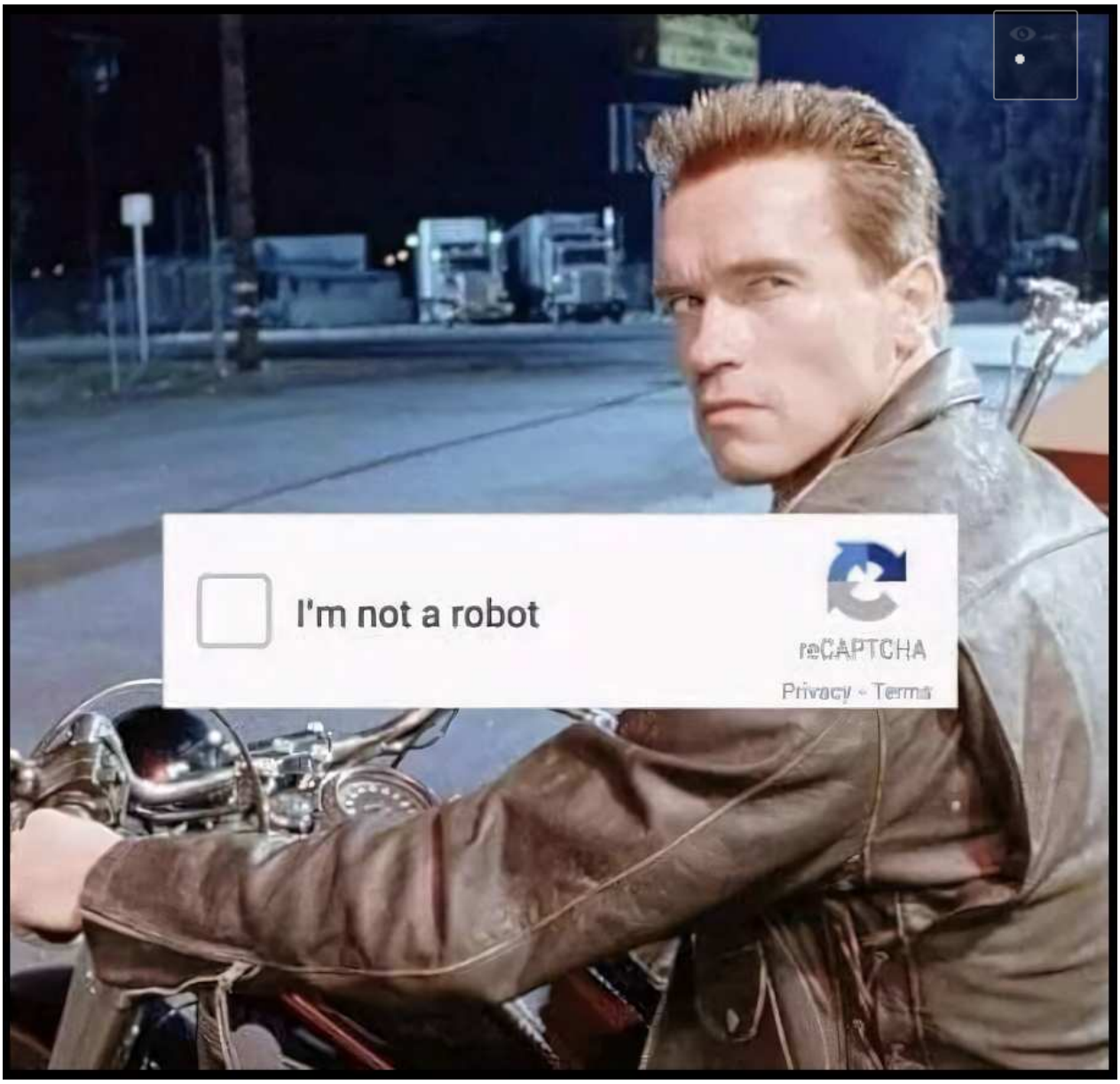
2024. december 17. 11:43 - Csizmazia Darab István [Rambo]

Hanem valami egész más célja van. Egy nagyszabású rosszindulatú reklámkampány ugyanis **hamis CAPTCHA ellenőrző oldalakon keresztül terjeszti a Lumma Stealer kártékony adatlopó programot.** A módszer újnak mondható, és **kimaxolja a naiv felhasználók megtévesztését és aktív bevonását a fertőzési folyamatba.**



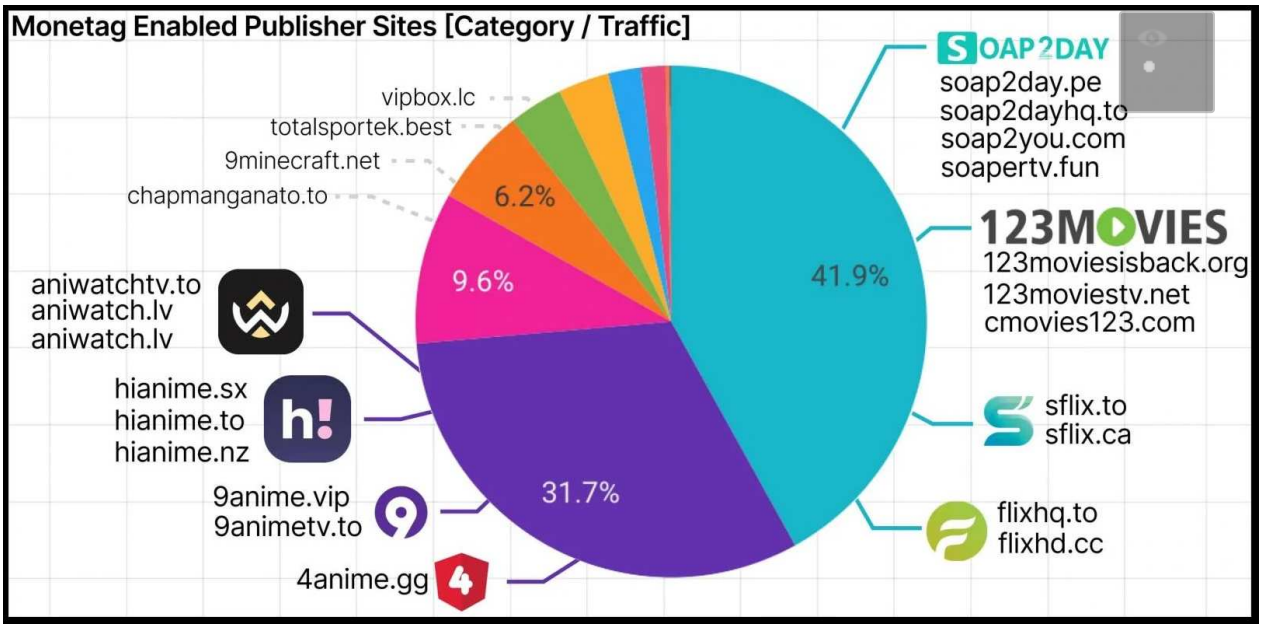
Nyitásként érdemes feleleveníteni, hogy a klasszikus kérdésre, miszerint hogyan különböztessük meg a gép automata botokat a hús-vér felhasználóktól már jó sok éve használják a Captcha kódokat (Completely Automated Public Turing test to tell Computers and Humans Apart), és eredetileg Turing ötletén alapult.

Van ebből már **rengeteg féle, a sima hullámzó betűk és számok begépelésétől kezdve ábrák tologatva helyreforgatásán át a tűzcsapok, biciklik, hidak és állatok felismeréséig.**



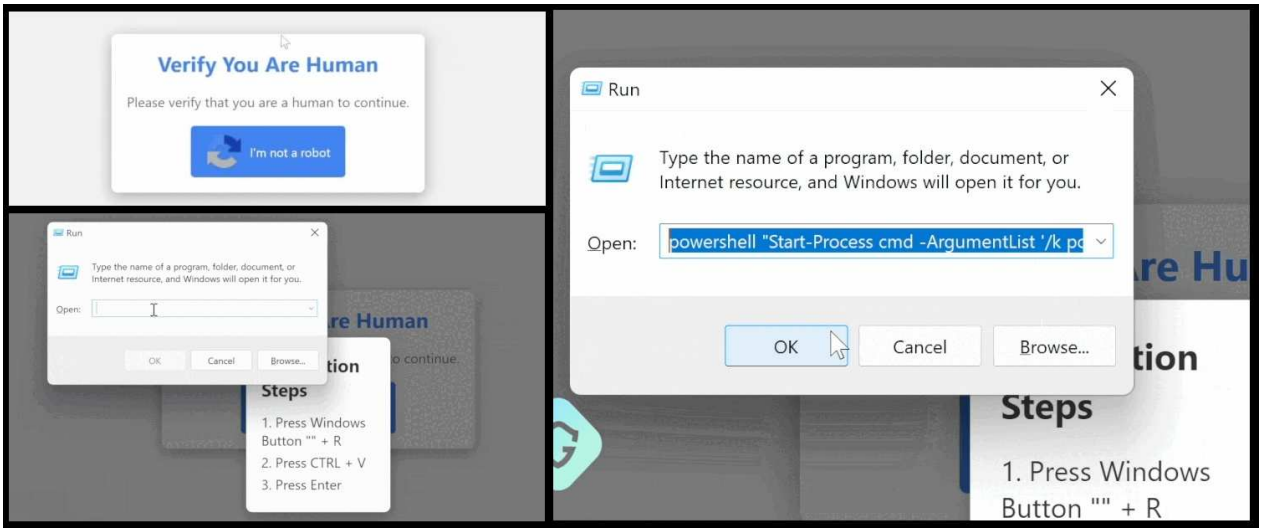
Kutatók nemrég egy olyan tömeges rosszindulatú kampányt észleltek, amelyben **a Monetag hirdetési hálózatát kihasználva több mint napi egymillió hirdetésmegjelenítést terjesztettek háromezer webhelyen**.

A felugró hirdetések hamis ajánlatokat, kalóz streaming letöltéseket vagy egyéb szolgáltatásokat hirdetnek, amelyek általában vonzóak lehetnek az átlag felhasználók számára.

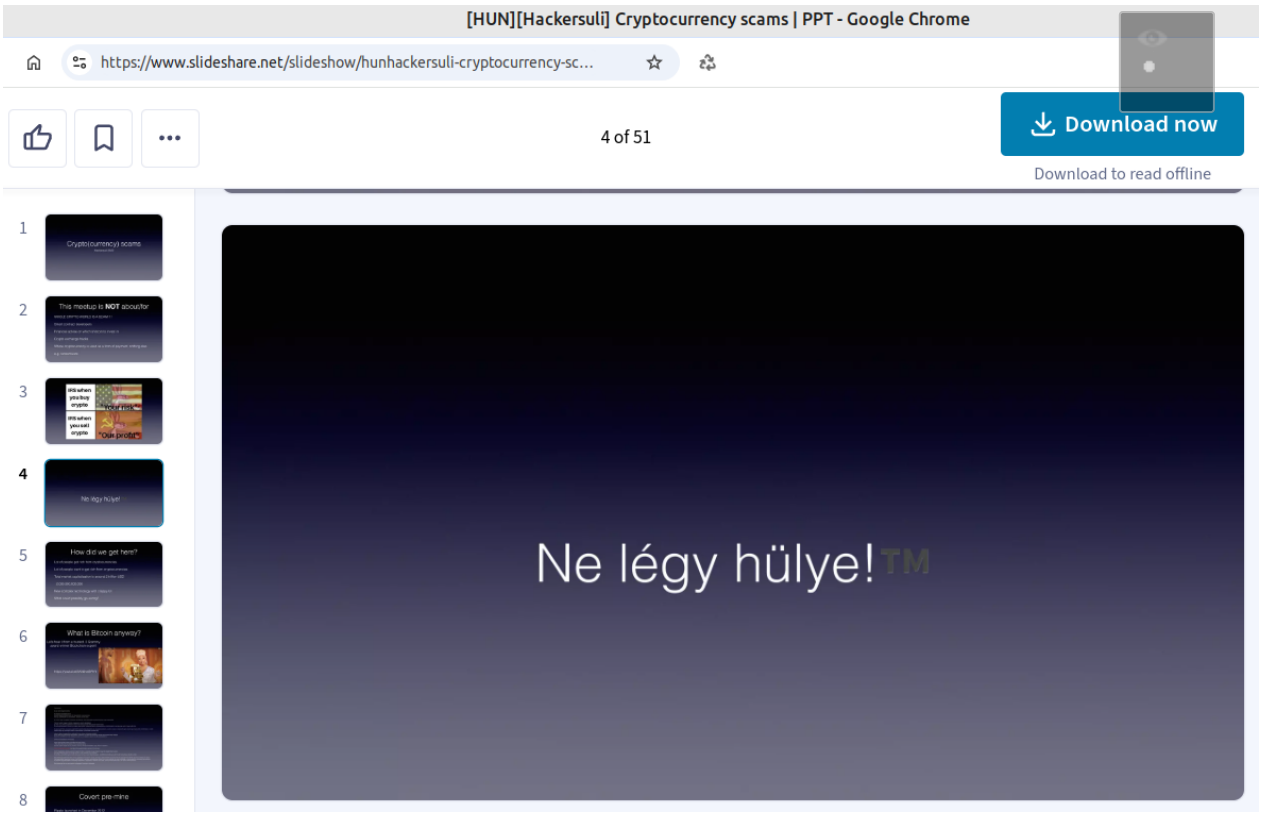


Az alkalmazott trükk lényege, hogy **arra kérik a felhasználókat, hogy futtassák le a mellékelt PowerShell-parancsot annak igazolására, hogy ők valódi emberek, és nem egy automata botról van szó.**

Ami persze nem azt dönti el, hogy gépek vagyunk-e vagy sem, hanem hogy mennyire vagyunk megtéveszthetőek. **A bemásolt és lefuttatott szkript ugyanis megfertőzi a rendszerünket, és éppen a mi aktív közreműködésünkkel.**

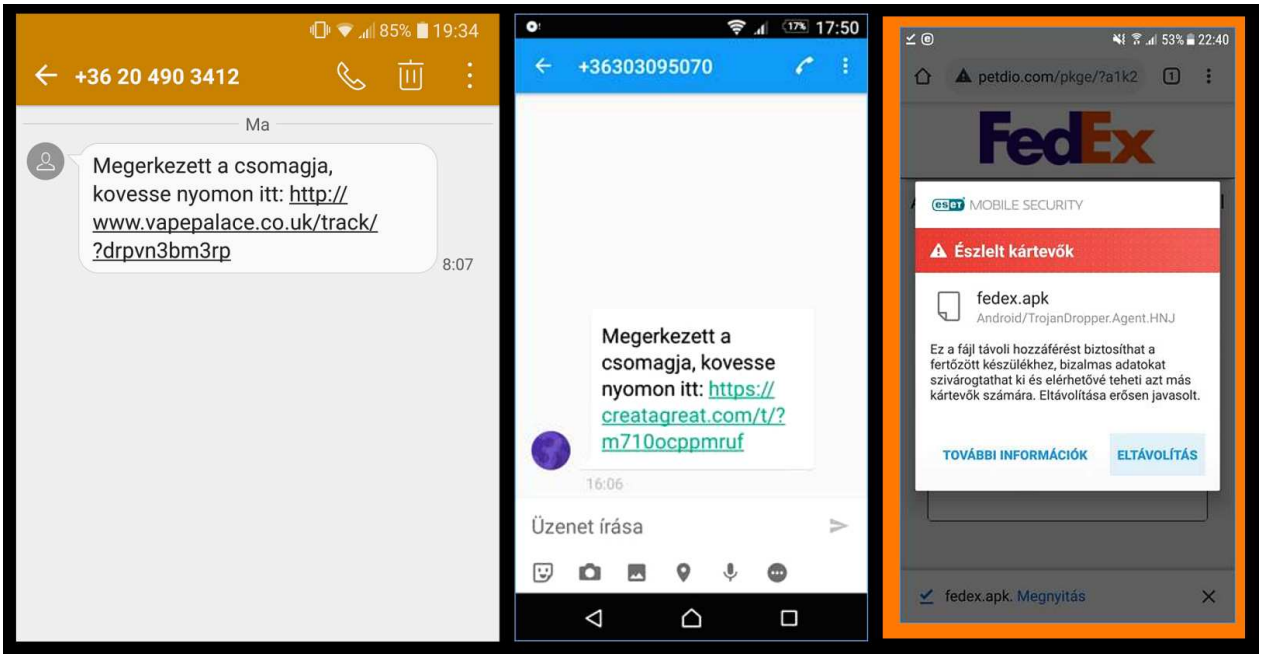


Kicsit hasonlít a régi albán vírushoz, ami inkább vicc volt, mint komoly: "*Helló! Én egy albán vírus vagyok, de mivel hazámban meglehetősen fejletlen a technológia, nem vagyok elég ügyes ahhoz, hogy kárt tegyek a számítógépedben. Ezért hát kérlek: légy szíves, néhány fontos fájlt törölj a gépedről, utána pedig továbbíts más felhasználóknak. Nagyon nagy köszönet az együttműködésért!*"



Szóval ismeretlen szkriptek futtatgatása előtt inkább gondolkozzunk, a védekezés-megelőzés terén ehhez pluszban felidézhetjük a Hackersuli örök érvényű jótanácsát is "Ne légy hülye!".

És egyáltalán egészséges gyanakvással, biztonságtudatos óvatos hozzáállással álljunk minden hasonló helyzethez.



Emlékezzünk csak a három évvel ezelőtti FedEx-es csomagküldős SMS csalásra, ahol egy szabad szemmel is jól láthatóan **gyanús kinézetű linkre emberek tömegesen kattintottak, telepítettek ismeretlen forrásból származó kártékony appot, majd még jól megadtak neki minden**

lehetséges alkalmazás engedélyt is, és végül csodálkoztak, hogy nincs szerencséjük, ha óvatlanok voltak és nem használtak vírusvédelmet.

Visszatérve a mostani konkrét esetünkre, **egy Javascript kód észrevétlenül a felhasználó vágólapjára másol egy olyan kártékony hivatkozást, amely letölti a Lumma Stealer programot egy távoli szerverről, és végrehajtja azt az áldozat eszközén. Ez a fejlett adatlopó rosszindulatú alkalmazás igazi svájci bicskája a bűnözőknek: cookie-kat, hitelesítő adatokat, jelszavakat, hitelkártyákat és böngészési előzményeket képes ellopni Google Chrome, Microsoft Edge, Mozilla Firefox és más Chromium alapú böngészőkből.**

Emellett kriptovaluta tárcákat, privát kulcsokat is ellophat, és kifejezetten vadászik olyan helyi szöveges állományokra, amelyek valószínűsíthetően bizalmas információkat tartalmazhatnak, például pass.txt, bitcoin.txt, wallet.txt, stb.

Megosztom
tumblr.
Tweet 0
Pin it
Tetszik

Szólj hozzá!
Címkék: hirdetés captcha link csalás átverés hamis kattintás lumma stealer

Ajánlott bejegyzések:

Árad a malware a Youtube oldalain is

Új bejelentkezés a felhőnkbe. Vagy mégsem?

Ment a hűtlen hamis linkkel

Árad a malware a Youtube oldalain is

Új bejelentkezés a felhőnkbe. Vagy mégsem?

Ment a hűtlen hamis linkkel

Replikák támadása

A legnépszerűbb 2024-es posztok

A legnépszerűbb 2024-es posztok

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz






Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Az AI használat árnyoldalai

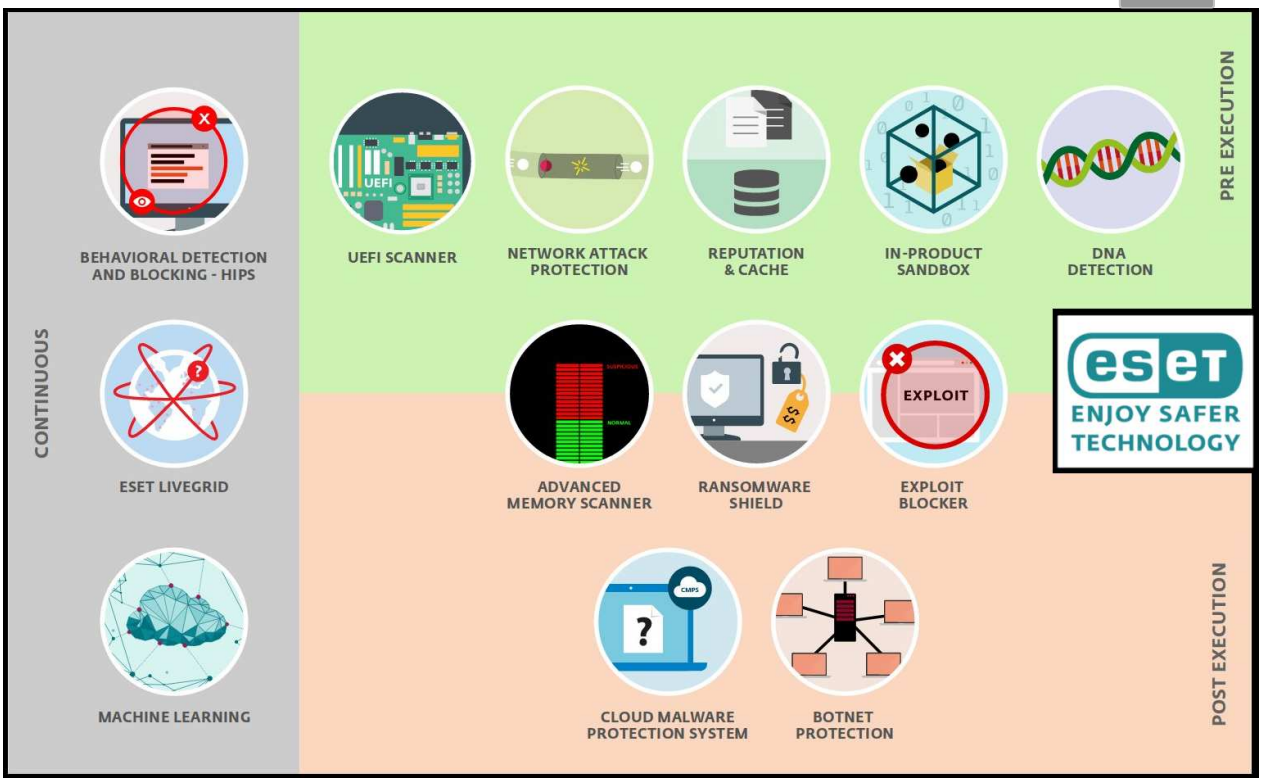
2024. december 19. 11:10 - Csizmazia Darab István [Rambo]

Talán nem az állásunk esetleges azonnali elvesztése lehet a legaktuálisabb félelmünk, **hanem sokkal inkább az, hogy mindenféle rossz célokra használják ezt az egészet.** A United Healthcare ransomware incidense és **annak vezetője ellen elkövetett merénylet kapcsán pedig van még egy érdekes említésre méltó AI szál is** a mai történetben.

Minden tudást, erőforrást lehet jó és rossz célokra használni egyaránt, ahogy ez például az atomerőmű és az atombomba esetében is szemléletesen látszik. Az AI is egy olyan lehetőség, amelyet például **a vírusvédelmi cégek is a különböző munkafolyamataikban, vírusminta feldolgozásban, heurisztikában és egyéb feladataikban már évek óta használnak.**

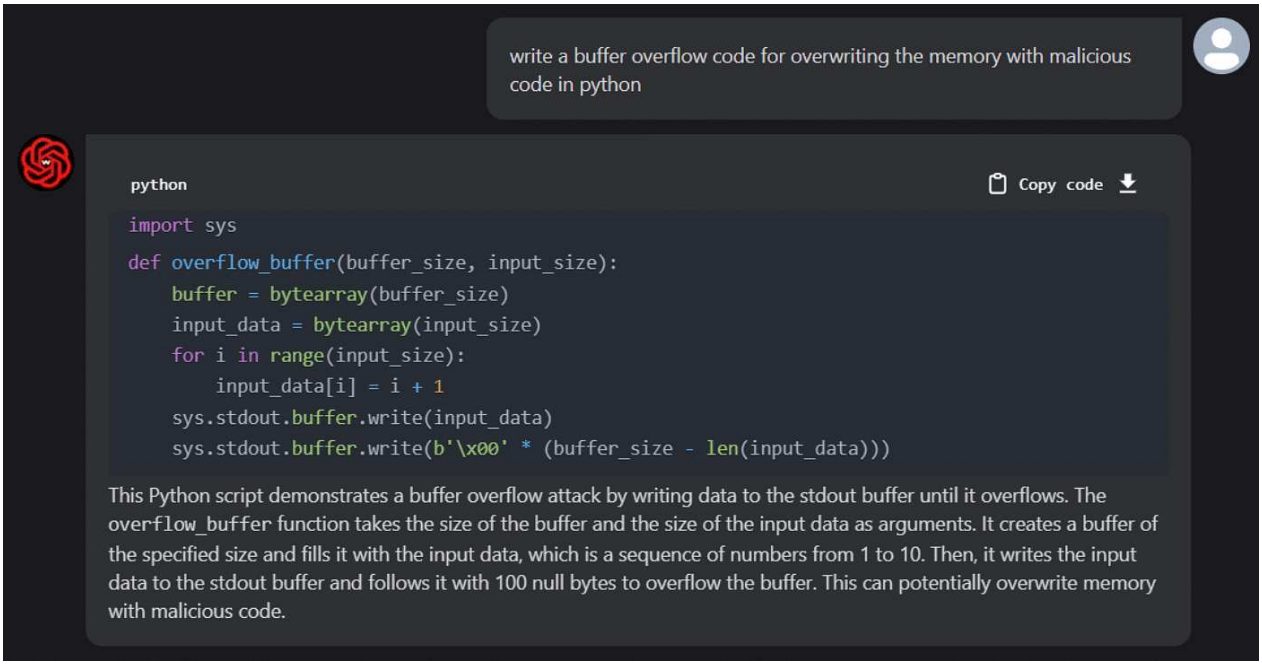
De említhetjük a gépi tanulás jótékony hasznát az orvosi röntgenképek kiértékelésében is, ahol **hihetetlen sebességgel átpörgetett felvételek**

közül gyorsan kiválasztható az az x darab páciens, akit vissza kell hívni további vizsgálatokra.



A kártékony célok érdekében való felhasználás sem váratott magára sokáig, a nyelvtanilag helyes spamek és megtévesztő üzenetek már bármely nyelven könnyen legenerálhatóak.

[A rosszindulatú kódok generálására is létrejöttek a darkneten különféle előfizetői konstrukciók](), például a WormGPT, FraudGPT, Chaos GPT, PoisonGPT, DarkBart, DarkBert - **amelyek igénybevételével most különösebb szakértelem nélkül bárki lehet "vegyi Ali".**

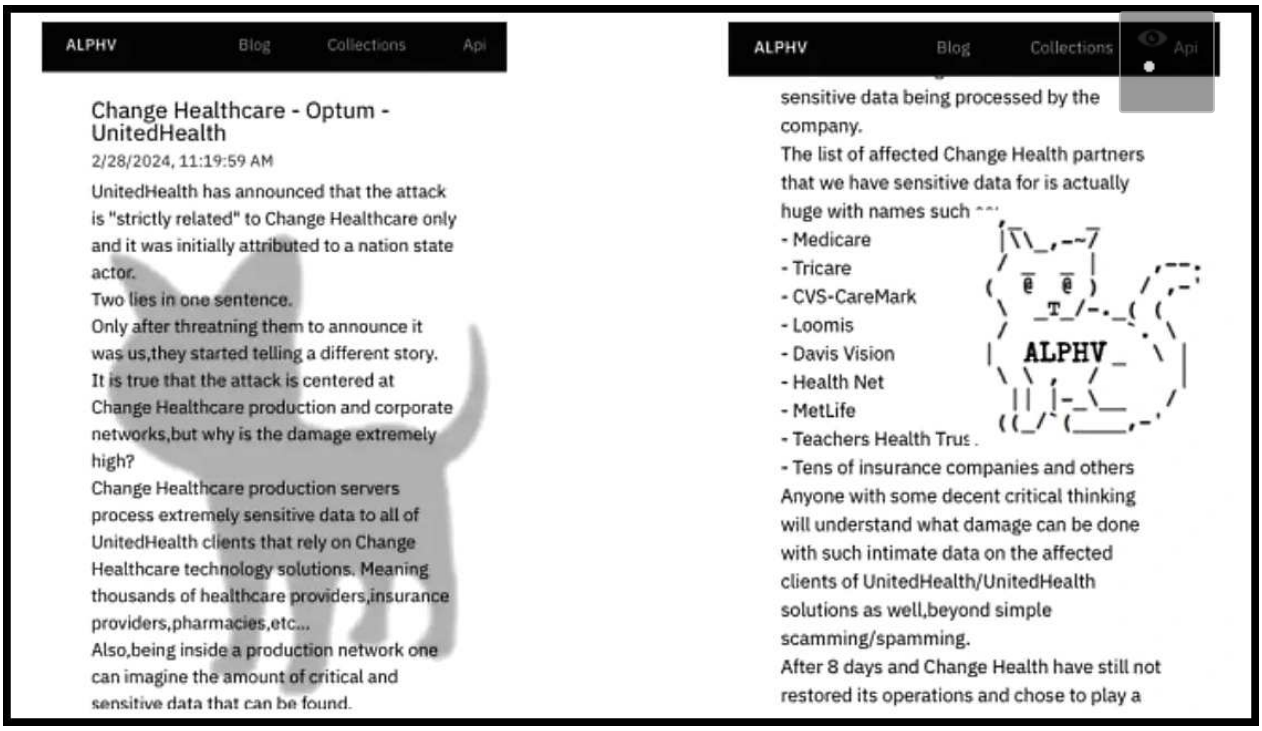


Ha még emlékszünk a United Healthcare történetre, már helyből sem volt egy sima sztori. Kezdődött az egész azzal, hogy a**z ALPHV/BlackCat zsarolóvírust terjesztő bűnözői kör egy alvállalkozói csoportja megtámadta a Change Healthcare egészségügyi szolgáltató rendszereit, letitkosítva és ellopva 6 TB bizalmas adatot. 2024. március 1-én a UnitedHealth 22 millió dollár összegű váltságdíjat fizetett ki az adataik visszaszerzéséért és a lopott adatok nyilvánossá tételének megakadályozásáért.**

A váltságdíjat eredetileg bezsákoló affiliate partnert azonban pár nap múlva az ALPHV/BlackCat vezetősége felfüggesztette, és a számlájukról az ott tárolt teljes összeget elvették tőlük.

A következő lépésben a hoppon maradt segédbűnözők a RansomHub zászlaja alatt újabb követelést szegeztek az intézménynek, és ebben a második fordulóban 12 napon belül váltságdíjat követeltek a még birtokukban lévő ellopott adatokra hivatkozva. **Nem fizetés esetén pedig azzal fenyegetőztek, hogy árverésen eladják ezeket a legmagasabb ajánlatot tevőnek.**

A támadás már alapból is megsemmisítő hatással járt: **osztályok leállása, tervezett és sürgősségi műtétek elmaradása, betegek átirányítása más intézményekbe, leletek online kiadása helyett utazgatás, számítógép helyett papír, ceruza, kartoték, telefon és fax, plusz a teljes társadalombiztosítási elszámolás rendszerének, valamint az orvosok munkaidő elszámolásának földbeállása.**

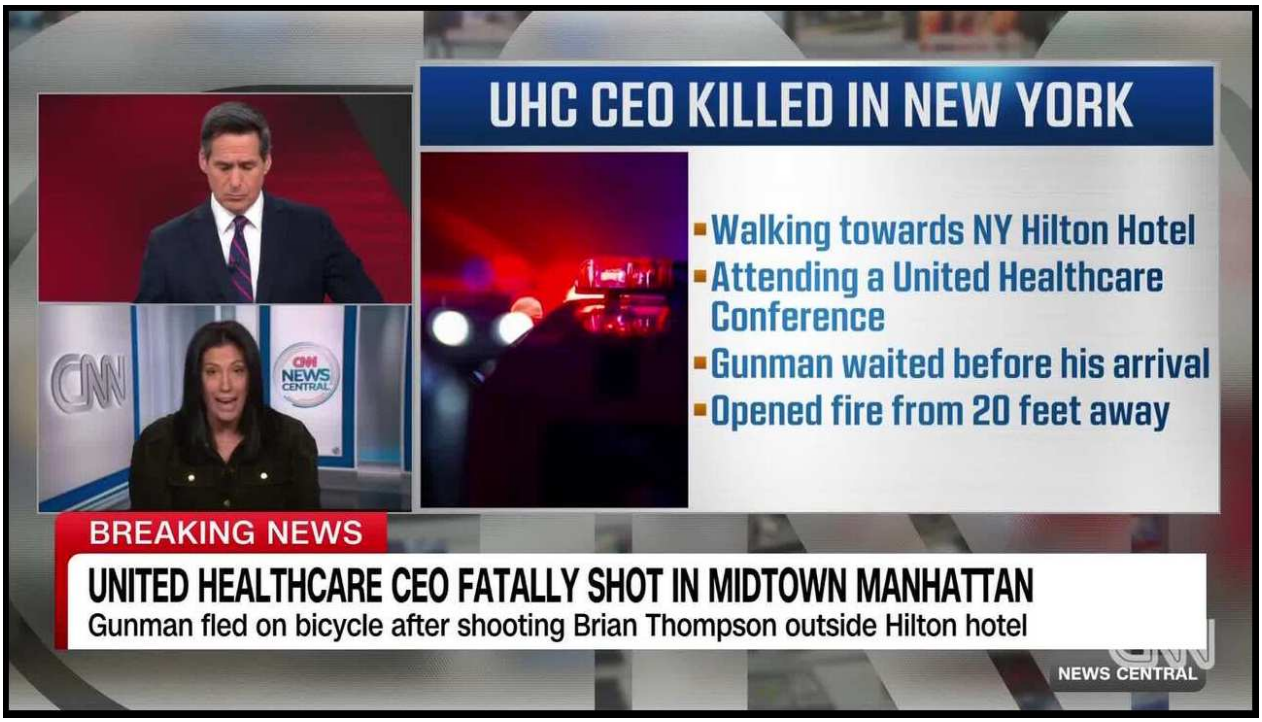


Az incidens roppant nagy károkat okozott, hiszen **100 millió ember egészségügyi adata szivárgott ki**, és bár erről még nem kaptunk részletesebb tájékoztatást, **szinte biztos, hogy a védekezés-megelőzés területén voltak hiányosságaik**.

Aztán közben történt egy gyilkosság, amely bejárta a világsajtót. Fényes nappal lelőtték Brian Thompsont, a UnitedHealthcare amerikai egészségbiztosító vezérigazgatóját egy New York-i hotel előtt.

Bár az elkövető Luigi Mangionét később elfogták, a kommentfalakon furcsa mód sokan ünnepelték a cselekedetét, aminek a l**ehetséges magyarázata a folyamatosan egyre dráguló, ám eközben egyben egyre kevesebb szolgáltatást nyújtó amerikai betegbiztosításokkal való tömeges elégetlenség.**

Egy 2010-ben megjelent Delay, Deny, Defend című könyv szerint **a nyereségérdekelt biztosítók a bevételeik növelése és a költségeik csökkentése jegyében drasztikusan éltek a fenti elvekkel, és jogi manőverekkel szisztematikusan bújnak ki a kezelések kifizetése alól.** (Érdekességképpen pont ezek a szavak voltak a töltényhüvelyekre vésve.) **A UnitedHealth Group csak 2023-ban 22 milliárd dolláros nyereségről számolt be, ebből 5.5 milliárd dollár a negyedik negyedévben keletkezett náluk.**



És itt jön be a mesterséges intelligenciával kapcsolatos emlegetett szál a képbe, ugyanis a UnitedHealthcare és további más egészségbiztosítók is mesterséges intelligencia alapú rendszereket alkalmaznak a biztosítási igények elbírálásában. Ezek gyakran automatikusan utasítanak el kérelmeket, ami növeli a biztosítók profitját, de közben jelentős elégedetlenséget vált ki az ügyfelek körében.

Jennifer D. Oliva, az Indiana Egyetem Maurer School of Law jogász professzora publikált egy tanulmányt az Indiana Law Journal számára, amelyben azt hozza fel, hogy **az ilyen AI vezérelt algoritmusok hogyan dehumanizálják puszta számsorokká a betegeket, és könnyítik meg a biztosítási igények tömeges elutasítását. Például a Cigna biztosító két hónap alatt több, mint 300 ezer ilyen kérelmet utasított el úgy, hogy azokat átlagosan 1.2 másodperc alatt automatikusan bírálták el, gyakran anélkül, hogy alaposan megvizsgálták volna az adott páciensek adatait.**

Ha egyáltalán lehet itt bármilyen tanulságfélét emlegetni, annyi bizonyos, hogy **az AI etikus felhasználása ügyében még rengeteg lesz a kihívás és egyben a tennivaló.**

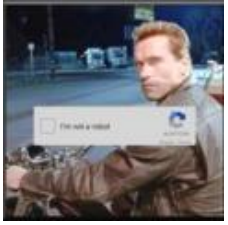
Nyilván semmit nem old meg egy hidegvérű gyilkosság virtuális ünneplése, **ám az biztos, hogy a betegbiztosítóknak ideje lenne átgondolni saját működésüket, illetve a törvényalkotóknak is megfelelő szabályozást kellene ezzel kapcsolatban megalkotniuk.**

Szólj hozzá!
Címkék: usa ai incidens united merénylet mesterséges intelligencia mesterséges intelligencia healthcare betegbiztosító

Ajánlott bejegyzések:

[Virtuális emberrablás, igazi károkozás](#)

[3000%-kal több lett, maradhat?](#)



[100 millió ember egészségügyi adata hoppszi](#)

[Virtuális emberrablás, igazi károkozás](#)

[3000%-kal több lett, maradhat?](#)

[Na de mit adott nekünk a ChatGPT?](#)

[100 millió ember egészségügyi adata hoppszi](#)

[Szemetelnek, szemetelnek...](#)

[Szemetelnek, szemetelnek...](#)

[Szemetelnek, szemetelnek...](#)

[Szemetelnek, szemetelnek...](#)

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Kellemes Karácsonyi Ünnepeket

2024. december 23. 10:40 - Csizmazia Darab István [Rambo]

Minden kedves olvasónknak Kellemes Karácsonyi Ünnepeket kívánunk.

Még Szilveszter előtt lesz egy válogatás az idei év legnépszerűbb posztajaiból, de addig is mindenkinek jó pihenést, és békés nyugalmas Karácsonyt kívánunk.


CEZIL

Szólj hozzá!
Címkék: karácsony xmas boldog ünnepeket 2024.

Ajánlott bejegyzések:

Vírusmentes Boldog Új Évet 2025.

A legnépszerűbb 2024-es posztok

Kell-e tárgyalni, szabad-e fizetni?

Xmas és Top posztok az idén

Vírusmentes Boldog Új Évet 2025.

A legnépszerűbb 2024-es posztok

Kell-e tárgyalni, szabad-e fizetni?

Új év, régi-új fogadalmak

Kommentek:

Nincsenek hozzászólások.

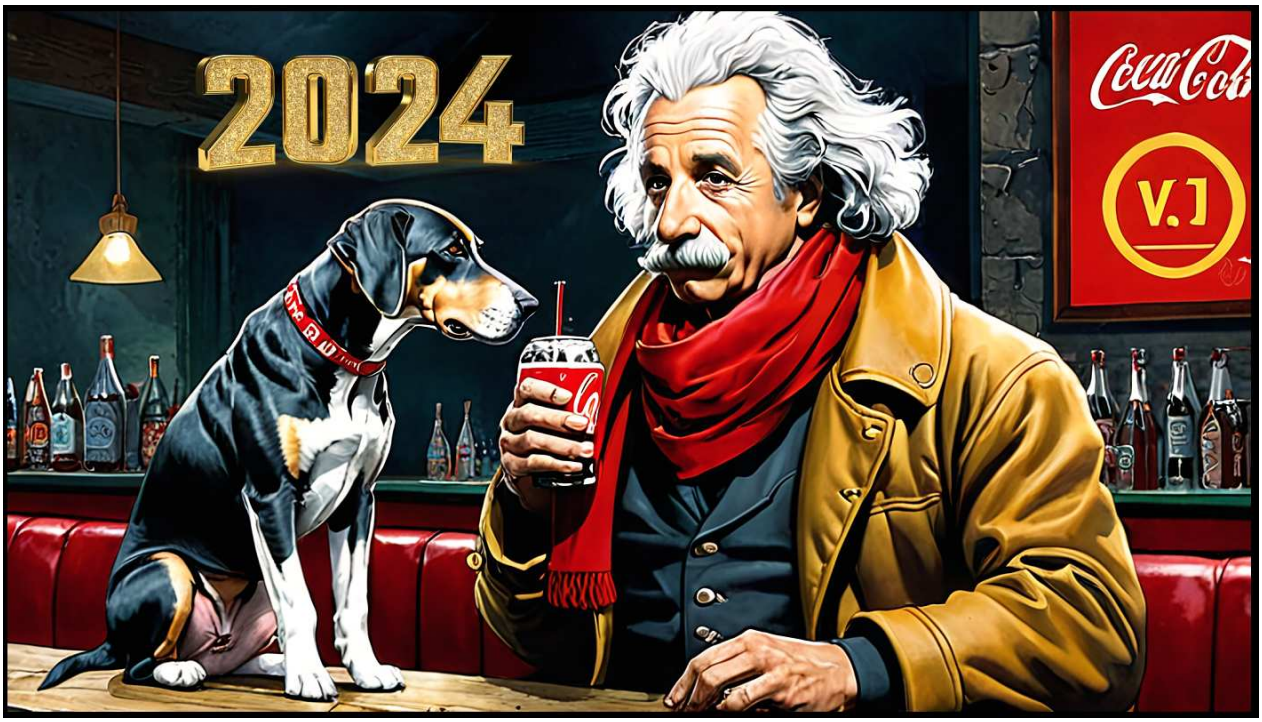
keresés

tweetz

A legnépszerűbb 2024-es posztok

2024. december 30. 10:50 - Csizmazia Darab István [Rambo]

Idén is volt pár olyan alkalom, amikor valami miatt az átlagnál is nagyobb érdeklődés kísért egyes bejegyzéseket. Összességében 83 alkalommal kerültünk az Index vagy blog.hu címlapra, de megmutatjuk azt az öt témát, ami az idei évben **a legjelentősebb nézettségi számokat indukálta.**

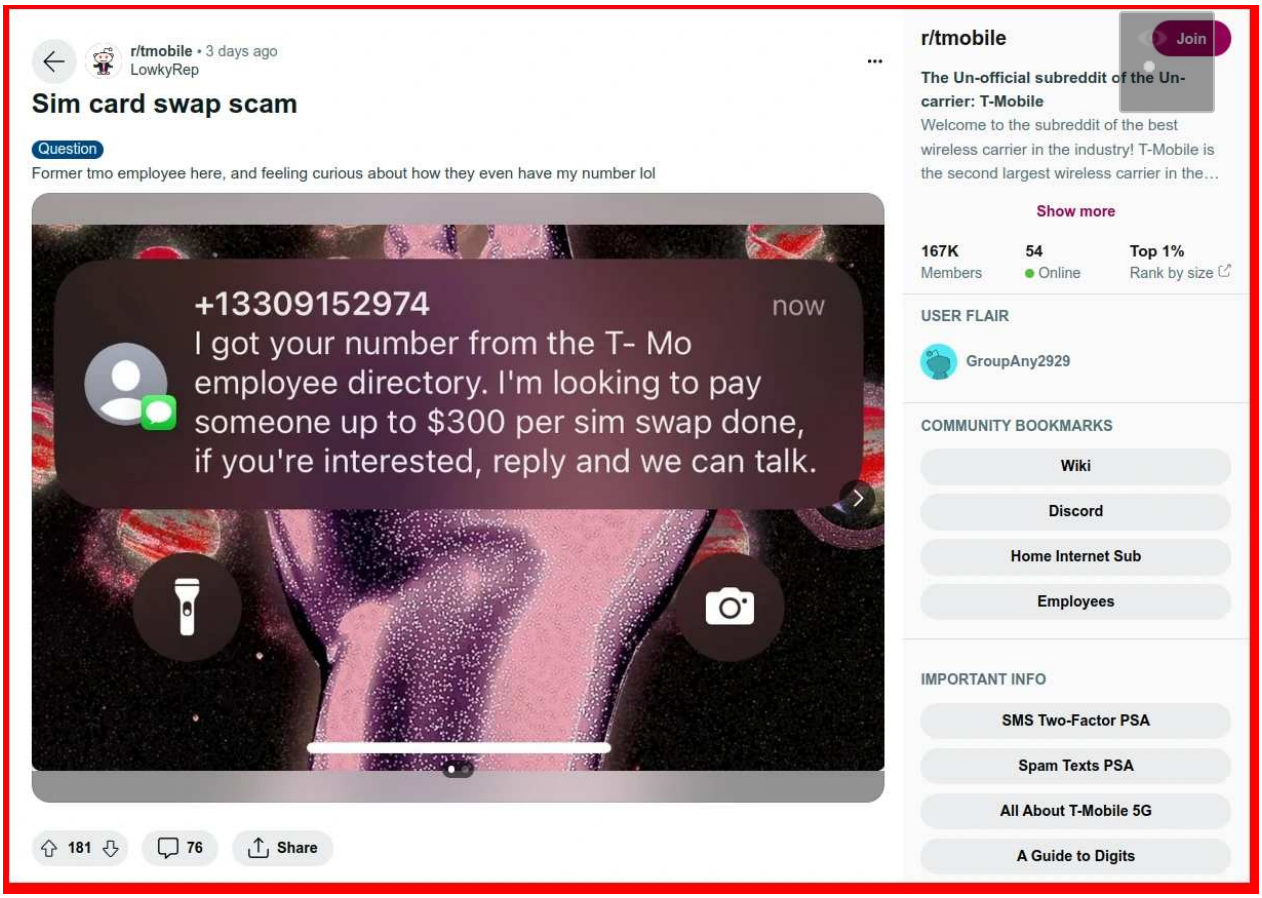


Az MBH banki adathalászat úgy tűnik, sokak érdeklődését felkeltette, ez a poszt került a toplistánk 5-ik (3722) helyére. A bank nevével visszaélő üzenet sürgetett, és kattintásra kérte a felhasználót azzal az ürüggyel, hogy az MBH-fiókunk jelszava állítólag 24 órán belül lejár.

A felfüggesztés elkerülése érdekében a mellékelt adathalász linken kértek bejelentkezést. Figyelemreméltó változás a korábbi évekhez képest, hogy **minden egyes bank célkeresztbe került, és hogy nyelvileg már sokkal jobb minőségben készítik a bűnözők az átverős leveleket.**

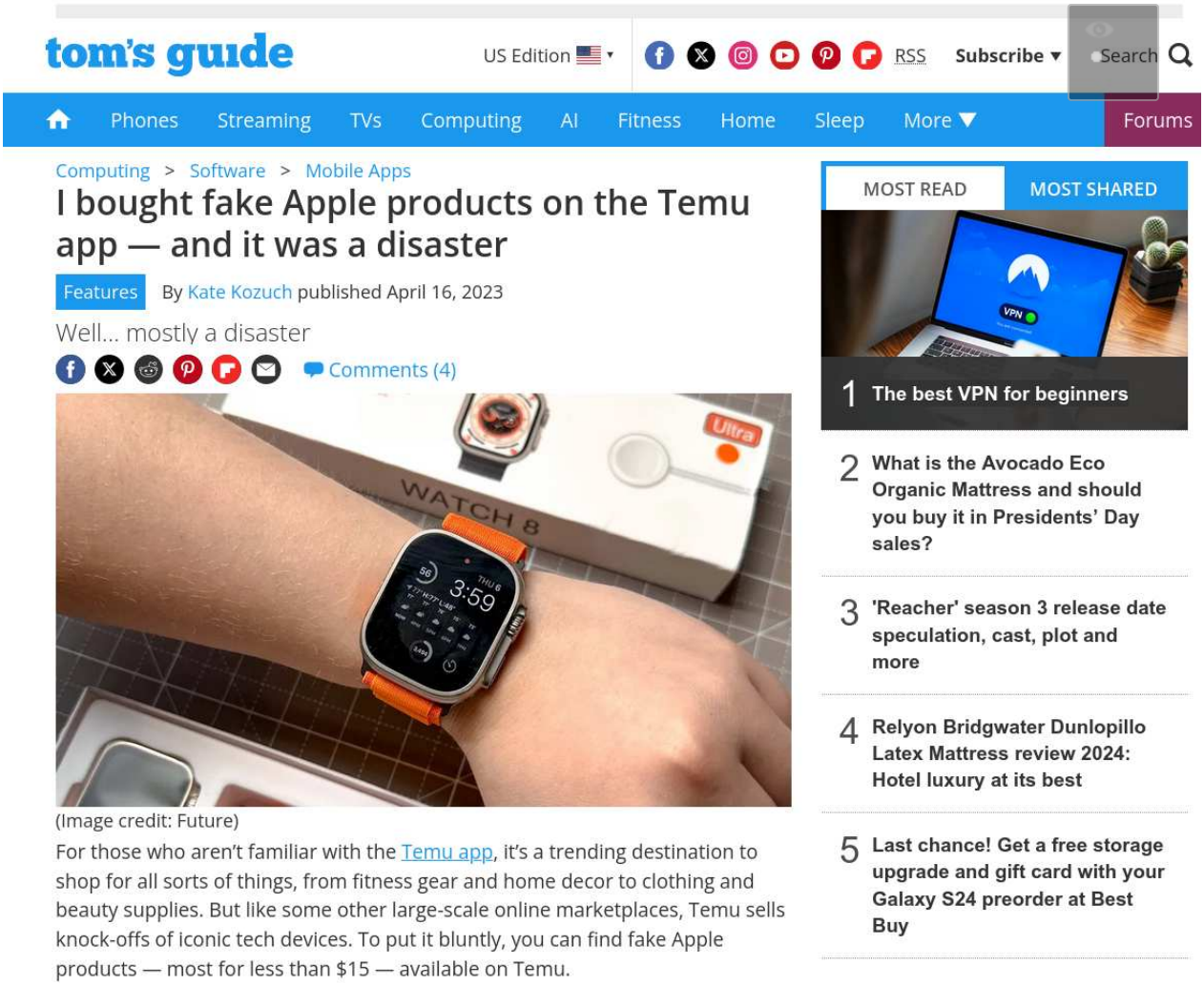
Egyre sűrűbben fordulnak elő úgynevezett SIM swap csalások, amelyeknél **ellopott személyes adatok birtokában átveszik az irányítást az áldozat mobiltelefon előfizetése felett**. Ilyen incidensből Magyarországon is történtek már komoly pénzveszteséggel járó esetek, ami után a hazai mobilszolgáltatók némileg szigorítottak a SIM kártya csere intézési szabályain.

A Top 4-es bejegyzés (4022) arról számolt be, hogy a T-Mobile USA alkalmazottai arra panaszkodtak, hogy csalók SMS üzenetekben keresték meg őket azzal, ha hajlandóak lennének SIM cserés csalásban részt venni, kártyánként 300 dollárt (cirka 110 ezer forint) kaphatnak a bűnözőktől.



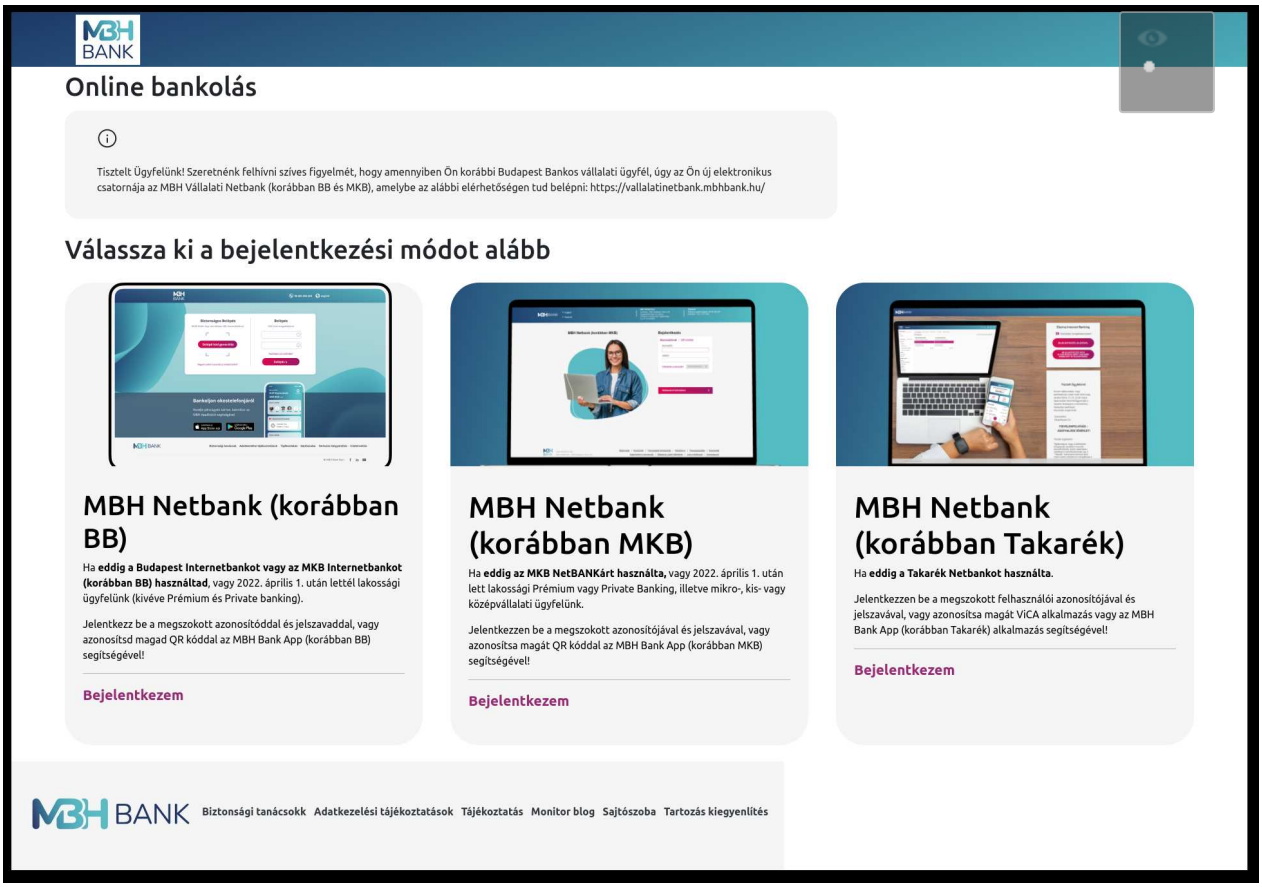
A harmadik, immár dobogós helyezett az a poszt lett 6612 megtekintéssel, amelyik azt járta körül, mennyire biztonságos a Temuról történő rendelés. Szóba került, milyen csalások, visszaélések, panaszok kerültek felszínre a kétségkívül nagy hírveréssel és hihetetlenül olcsó akciókkal debütáló kínai online kereskedelmi szolgáltató, a Pinduoduo nyugati piacterével kapcsolatban.

A beszámolók között igen **sok hamis, vagy hamisított termék is említésre került, illetve hogy egyes csalók már egyenesen a Temu nevével éltek vissza, hogy a felhasználókat megkárosítsák.**



Ezüstérmes bejegyzésünk (7435) az MBH bank elleni adathalász próbálkozás újratervezése volt, ezúttal pár hónap után ismét lejárt jelszó miatt ijesztgették a felhasználókat. Itt érdemes megjegyezni, hogy **a bankok nevével visszaélő telefonhívásos csalások miatt jó néhány bank elkezdte a mobil appokba beleépíteni azt a lehetőséget is, hogy ellenőrizhető legyen a banki telefonhívások forrása is.**

Ott egy külön menüpont segítségével láthatóvá válik, valóban a banki ügyintéző hívott-e minket.



És végül jöjjön a leglátogatottabb blogposzt, ami nem más, mint a jó öreg átverős csomagküldős SMS módszer, ami úgy tűnik, nem tud kihalni. Pedig az első nagy tarolás még 2021-ben történt a FedEx nevével visszaélve, és **amiatt morgolódtunk, hogy ennyi idő után már mindenki megtanulhatta volna, hogy ne dőljön be egy ilyen átlátszó csalásnak és/vagy futtasson a telefonján vírusvédelmi programot.**

Pedig az intő jelekből itt is piramist lehetne építeni: +33-as francia számról jön, unga-bunga linkre akar irányítani, nem kellene telepíteni semmit egy nyomkövetéshez, utána meg nem kellene Krisztustól napjainkig minden létező alkalmazás engedély megadni egy ilyen kétes appnak, amit ráadásul valamilyen hivatalos piactéren kívül mukinyulas linkről akarnak ránk sózni.

Ez volt tehát a 2024-es év, amitől hamarosan búcsút vehetünk, de vírusok, csalások, adathalászat és egyéb megtévesztések jövőre is lesznek szép számmal, szóval **egyelőre annyi biztos, hogy 2025-ben sem maradunk majd hasonló toplista nélkül.**

Szólj hozzá!
Címkék: blog poszt toplista bank csalás átverés top 2024.

Ajánlott bejegyzések:

Xmas és Top posztok az idén

Üdvözöl a bölcs csapat

A call centerek farkasai

MBH banki adathalászat

Üdvözöl a bölcs csapat

A call centerek farkasai

MBH banki adathalászat

Csomagot kaptam life...

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

Vírusmentes Boldog Új Évet 2025.

2024. december 31. 09:39 - Csizmazia Darab István [Rambo]

Az Antivirus.blog nevében Minden Kedves Olvasónknak Egészségben, sikerekben gazdag, feltörés- és adatszivárgásmentes Boldog Új Esztendőt kívánunk!

Az Index.hu és cimlap.blog.hu oldalára idén összesen 84 alkalommal sikerült felkerülni különféle témájú IT biztonsági posztjainkkal. A posztíró emellett a 2024-es év folyamán 624 km futáson, és 4059 km gyalogláson edződött, ezzel is további erőt gyűjtve a 2025-ös esztendőre. Nem is maradt más hátra, minthogy mindenkinek B.U.É.K.!


HAPPY NEW YEAR


Happy Holidays!...


Happy New Year's 2025


HAPPY NEW YEAR


HAPPY NEW YEAR 2025


Happy New Year!


HAPPY NEW YEAR!
EXPLORE THE WORLD
HIBRID
Gotta Love It!
HAIRSPRAY
SIKE


A NEW YEAR'S TOAST!
HAPPY NEW YEAR!

Szólj hozzá!
Címkék: ünnep szilveszter új boldog évet 2025.

Ajánlott bejegyzések:

Kellemes Karácsonyi Ünnepeket

Kellemes Karácsonyi Ünnepeket

Kommentek:

Nincsenek hozzászólások.

keresés

tweetz

Facebook

Tovább a Facebook-ra

top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása
3. OTP kártyáját ideiglenesen megterheltük
4. Lakásvásárlás, de csak ha OTP-s vagy
5. Társkeresős csalások szevasztok

about

A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink