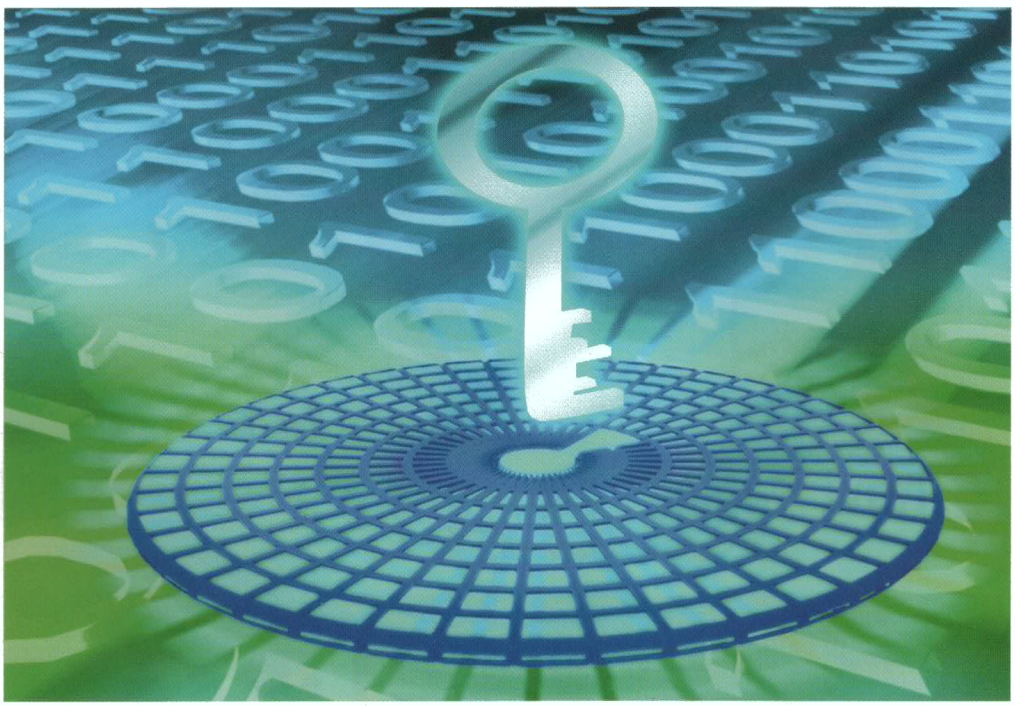
HONNAN JÖN A FERTŐZÉS?

MINDENNAPI ÁTVERÉSEK

Sok számítógép-felhasználó nincsen tisztában azzal, milyen veszélyek fenyegetik az interneten. Elégedetten hazaviszi a gépet az áruházból, az adatait szinte soha nem archiválja, és nem figyel oda, milyen linkekre kattint. Azután meglepődik, amikor megfertőződik számítógépe, és nincs kitől segítséget kérnie.



VESZÉLYZÓNA

Annak a valószínűsége, hogy a számítógépünk megfertőződik, semmiképpen sem nulla, kivéve természetesen, ha az internettől elvágva és folyamatosan kikapcsolva tartjuk.

Akadnak, akik még ma sem fordítanak kellő figyelmet arra, hogy a gépükön egy megbízható és frissített vírusirtót használjanak, olyat, amihez tartozik terméktámogatás is. Pedig ez utóbbi is elengedhetetlen, hiszen Fred Cohen, egy amerikai számítógéptudós már 1987-ben – Gödel úgynevezett nem teljességi tételének felhasználásával – matematikai úton bebizonyította, hogy lehetetlen olyan vírusvédelmet készíteni, amely

FERTŐZÖTT PREZENTÁCIÓ

Újnak mondható az a módszer, melyről az ESET Threat Center blogjában olvashattunk először. Az átverés lényege, hogy egy Power Point prezentáció (.ppt) egy olyan oldalt tartalmaz, amely egy linkre mutat. Maga a bemutatófájl ilyenkor természetesen tiszta és vírusmentes lesz az ellenőrzéskor, ám ha valaki a prezentációban elhelyezett linkre kattint, az már bármilyen weboldal bármilyen állományára mutathat. Így tehát érdemes kétszer is megnéznünk, hogy milyen weboldalon járunk éppen.

FERTŐZÖTT MP3-LEJÁTSZÓK

Nem számít újdonságnak, viszont még mindig jelentős mennyiségű fertőzésért felelősek az Autorun típusú kártevők. Ezek külső USB-eszközök (például USB-kulcs, mobiltelefon, digitális fényképezőgép, memóriakártya, MP3-lejátszó, stb.) csatlakoztatásakor a Windows által automatikusan lefuttatott folyamat manipulálásával érik el, hogy végrehajtódjon a kódjuk. A naprakész vírusvédelem mellett az is fontos, hogy az Autorun automatikus lefuttatását kikapcsoljuk a rendszerben.

minden kártevő ellen 100%-os védelmet biztosít. Egy esetlegesen bekövetkező fertőzés esetén pedig kizárólag a vírusirtónkat gyártó cég terméktámogatására vagyunk utalva, ők azok, akik az esetek nagy többségében még képesek lehetnek arra, hogy speciális eszközök segítségével megtisztítsák a fertőzött számítógépet.

A bajt azonban meg lehet és meg is kell próbálni elkerülni, ehhez pedig nem árt ismerni, hogy milyen módszerekkel próbálnak meg minket átverni az interneten.

MICHAEL JACKSON ÉL

Továbbra is divatos az emberek kíváncsiságára építve hamis, de érdekes és vonzónak ígérkező tartalmakat küldeni. Így nemrégiben Michael Jackson halálhírével, majd „eddig soha meg nem jelent dalaival" kapcsolatos üzenetek kezdtek el terjedni az interneten, amelyek közül számos vírust tartalmazott. Érdemes óvakodni akkor is, amikor „itt nézhető meg a legújabb Harry Potter mozifilm" és ehhez hasonlatos linkek érkeznek hozzánk e-mailen vagy közösségi oldalakról származó üzenetekben. Ezekben az esetekben, ha a címzett a linkre kattint, akkor az állítólagos videó egy hiányzó kodeket (a lejátszáshoz szükséges algoritmust) ajánl fel letöltésre, ez azonban csak átverés, maga a kártevő fog letöltődni. Az ilyen, emberi közreműködést is igénylő trükkök nemcsak Windows-platformon, hanem Macintosh gépeken is egyre gyakrabban megjelennek.

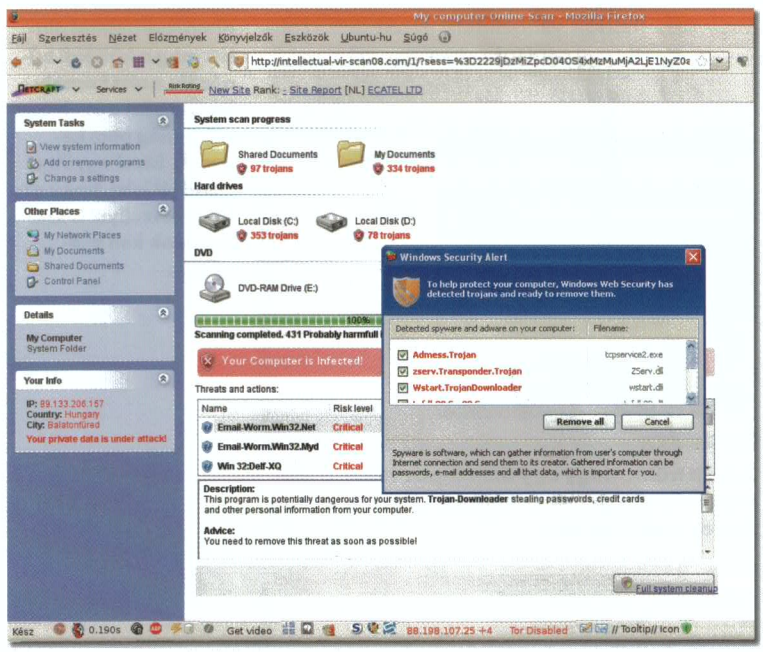
RÖVIDÍTETT LINKEK

Ugyancsak felkapott módszerré vált a kártevőt tartalmazó oldalak linkjeinek elrejtése oly módon, hogy a manapság egyre népszerűbb URL rövidítési technikákkal elfedik az eredeti link adatait. A MessageLabs jelentése szerint a bűnözők hihetetlen mértékben rákaptak az URL rövidítési technikákra. A módszer lényege, hogy bármilyen kacifántosan hosszú linkből képes egy rövidke új linket generálni. Természetesen sokszor jól jöhet ez a szolgáltatás, rengetegen alkalmazzák például a Twitteren, de mint annyi mindent, ezt is lehet rossz célra használni.

A problémát az jelenti, hogy a kattintás előtt nem tudhatjuk, hova is fogunk megérkezni. A Firefox böngészőhöz mindenesetre már megjelent egy plugin, amelynek segítségével a Bit.ly linkeknél elég a link fölé vinni az egeret, és máris teljes terjedelmében látszik az eredeti weboldal-hivatkozás. Ha a link például a bankunk nevében jött, de a cím valahova Kínába vezet, akár el is állhatunk a rákattintástól.

TELEFONOS ÁTVÁGÁSOK

Folyamatosan nő – igaz, egyelőre csak külföldön – a trükkös elkövetők által üzött vishing, vagyis a telefonos adathalászat. Nem csupán elszórt próbálkozásokról van szó, a bűnözők iparszerűen hamis call centereket üzemeltetnek. Nemrég koreai áldozatok bejelentése alapján indítottak nyomozást Kínában, és olyan elkövetőket kerestek, akik érzékeny információkat kíséreltek meg gyanútlan áldozatoktól megszerezni. Az akció keretében 22 embert tartóztattak le, nyolc tajvani és 14 kínai-koreai állampolgárt. A csalók tisztviselőknek, banki alkalmazottaknak, rendőröknek adták ki magukat, és napi tíz órában véletlenszerű tárcsázással hívogattak koreai állampolgárokat, akikkel személyes adatokat, jelszavakat, banki hozzáféréseket próbáltak állítólagos ellenőrzés céljából bediktáltatni, illetve begépeltetni. A leleplezés sikeréhez nagyban hozzájárult, hogy egy



Egyre gyakoribbak a hamis antivírusprogramok

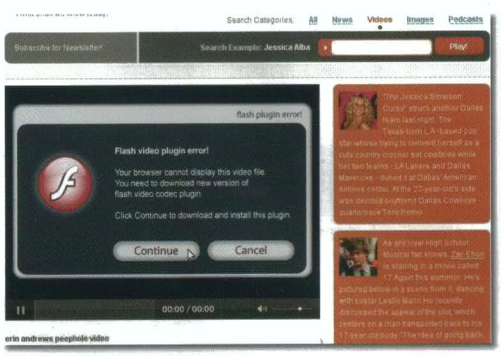
KÖNNYEN ELKAPHATÓ

Akiknek nem megfelelő a vírusvédelmük, vagy nincs rendszeresen frissítve a Windows rendszerük, könnyen elkaphatnak valamilyen szoftversebezhetőségen alapuló kártevőt.

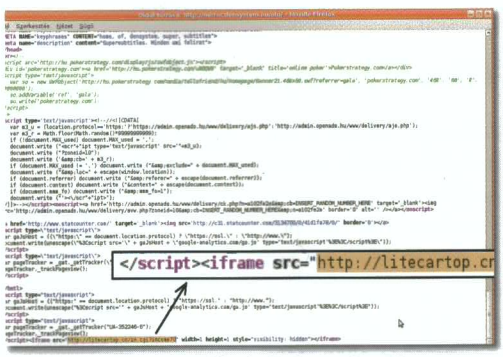
titkos ügynök beépült az adathalász-maffiába, így a belülről megszerzett információk segítségével sikerült végül letartóztatni a társaságot.
A nyomozás kiderítette, jól szervezett bűnbandával volt dolguk. A profi bűnözők Dél-Kínában nemcsak egyszerűen üzemeltettek egy hamis call centert, hanem magas fokon konspiráltak, lakásokat béreltek, amelyeket rendszeres időközönként cseréltek, hogy nehezítsék a felderítést. A csoport tagjai a munkát felosztották részlegeik között, így voltak, akik a telefonos hálózatért voltak felelősök, egy másik csapat a szükséges beszélgetési sémákat fejlesztette, míg egy harmadik brigád végezte e forgatókönyvek alapján a telemarketinges munkát a véletlenszerű számok tárcsázásával. „Munkájuk" után nemcsak alapfizetést kaptak, de teljesítmény-ösztönző bérezésben is részesültek.

HAMIS SZOFTVEREK

Sokféle hamisítással találkozhatunk, azonban egyet mindenképpen érdemes megjegyezni. Programot csak és kizárólag a gyártó, forgalmazó weboldaláról töltsünk le, mert többször is előfordult már, hogy a kétes letöltési oldalakon a telepítőcsomagokba kártevőket csomagoltak, vagy más módon változtattak az eredeti szoftveren. Korábban például sokan úgy tekintettek



Bevált trükk, hogy egy állítólagos videóra mutató linket küldenek e-mailben, ami azután egy kodek letöltését kéri



Sok weblapba kerül bele láthatatlan Iframe tag, és ezzel a látogatók gépére igyekeznek kártevőket letöltetni.

VIGYÁZAT, MACESEK!

Bevált trükk, hogy egy állítólagos videóra mutató linket küldenek e-mailben, ami azután egy kodek letöltését kéri. Ha a felhasználó kattint, már tölti is le a kártevőt a gépére. Ezt újabban már a sokkal biztonságosabb Macintosh gépeken is alkalmazzák, ahol a fertőzések egyetlen lehetséges módja, hogy a felhasználó maga kattintson, és ő maga telepítse fel a kártevőt.

MAGYAR BANKOK NEVÉBEN

Egyre gyakrabban jelennek meg a magyar nyelvű banki adathalászlevelek is, amelyek hazai bankok nevében írnak nekünk. A legtöbben még mindig sok ordító helyesírási hibával érkeznek, valamint a fordítást is valamilyen nyers fordítóprogrammal oldják meg a külföldi bűnözők, ezért komoly károkozásra ezek egyelőre még nem képesek. Ezzel együtt a trend jól jelzi, hogy ezzel a veszéllyel is számolnunk kell a jövőben.

a .pdf állományra, mint abszolút megbízható és biztonságos formátumra – nos, ez a helyzet mára gyökeresen megváltozott. Az Adobe Readertől sokan nemcsak az olvasó lomhasága, nagy mérete, hanem ritka biztonsági frissítései miatt pártoltak el, és választottak helyette alternatív olvasókat, például a Sumatrát vagy a FoxIt Readert. De minden csapástól ez sem óv meg. Természetesen jó választások lehetnek ezek a kisebb, gyorsabb és biztonságosabb dokumentumolvasók, de arról szó sincs, hogy ezekben ne lehetne kihasználható biztonsági rést keresni és találni. Egy mostanában lezajlott akció keretében ismeretlenek a Foxit Reader for Mac verziót ajánlgatták az érdeklődőknek, és ebben az a tény sem zavarta őket, hogy a nevezett szoftvert csak és kizárólag Windows, Windows Mobile, illetve U3/Desktop Linux platformokra tervezték. A nem létező Mac változathoz irányító link azonban egy kártevőre mutatott, és a gyanútlan kattintókat igyekezett megfertőzni.

MIT TEHETÜNK?

Folyamatos veszélyhelyzetet idéz elő, ha nincs rendszeresen frissítve az operációs rendszer, a kártevők döntő többsége ugyanis befoltozatlan biztonsági réseket, úgynevezett exploitokat használ ki a támadáshoz. A frissítés és a szoftverek naprakészen tartása nem úri passzió, és nemcsak a vállalati környezet követelménye, hanem minden magánfelhasználó számára is olyan lehetőség, amellyel minimalizálhatja a számítógépe ellen irányuló sikeres támadásokat.
Ezenkívül nem hagyható el a saját munkáink és adataink rendszeres mentése sem. Bizonyos vírusok – mint például a Win32/Mebroot.K trójai – ugyanis törölhetik számítógépen tárolt dokumentumainkat. Azt is tartsuk észben, hogy a számítógép alkatrészei, különösen a merevlemez, bármikor meghibásodhatnak, illetve naprakész védelem mellett is előfordulhat, hogy valamilyen vadonatúj kártevő megfertőzi a rendszerünket, hiszen – ahogyan ezt már említettük – 100 százalékos védelem nem létezik.

■ CSIZMAZIA ISTVÁN
vírusvédelmi tanácsadó