**A zsaroló programok rövid története**

2013.04.15. hétfő

***Ha valaki már a kezdetektől követi a számítógépes vírusok történetét, emlékezhet egy 1989-es történetre, melyben egy PC Cyborg Corporation nevű cég egy AIDS-szel kapcsolatos információs floppylemezt küldött szét mintegy huszonhatezer egészségügyi intézmény címére. Az eredeti címjegyzék tanúsága szerint három példányt Magyarországra is elküldtek: a Hematológiai Intézetbe, a János Kórházba és a KFKI-be, de ezeknek - állítólag postázás közben - lába kelt, ami jelen esetben utólag szerencsés fordulatnak is értékelhető.***

A lemez egy aljas programozási trükkel operált, és egy saját algoritmus alapján folyamatosan titkosította a merevlemezen az állományokat és a könyvtárakat. A kilencvenedik újraindítás után aztán a trójai az alábbi üzenetet jelenítette meg a képernyőn, angolul: "A szoftverbérleti szerződés erre a számítógépre lejárt. Amennyiben még szeretné használni ezt a számítógépet, meg kell újítania a bérleti szerződést. További információkért kapcsolja be a nyomtatót és nyomja meg az Enter billentyűt". A kinyomtatott üzenetben aztán szerepelt egy panamai postafiók címe és hogy 189, illetve 378 amerikai dollárt kell küldeni a készítőnek váltságdíjként, amit fizethettünk csekken vagy átutalással is.

Ez az eset indíthatta el szép lassan a lavinát, és ha a OneHalf nevet említjük, arra azért már biztosan többen felkapják a fejüket. Az 1995-ben megjelent DOS-os vírus a merevlemezről történő bootolásonként 2-2 cilinder teljes tartalmát titkosította, a merevlemez végéről indulva. Itt valójában ugyan nem kértek váltságdíjat, de a rongálást igyekeztek minél tovább rejtve tartani, hogy ezzel is fokozhassák a felhasználót érő kárt. Ha megnézzük a vírusok, kártevők evolúciós fejlődését, azt láthatjuk, hogy az nagyjából 2000 körül fordult erőteljeset, a korábbi öncélú, látványos magamutogatást egyre intenzívebben felváltotta a rejtőzködés, az adatlopás, és ez a terület egyben komoly pénztermelő ágazattá vált. A bűnözőknek nagyon is kifizetődő lett a különféle elektronikus kártevőkkel, csalásokkal foglalkozni, hiszen 2005-ben az USA-ban ebből már több pénzük származott - 105 milliárd dollár - mint a drogkereskedelemből.

Aztán eljött a mindenki által ismert hamis antivírusok korszaka: XP Antivirus 2008, 2009, és hasonló neveken találkozhattunk velük, és ennek a próbálkozásnak tulajdonképpen a mai napig nincs vége, még Macintosh-ra is készült jó néhány. A hamis riasztási ablakokban látszólag a mi könyvtárainkat ellenőrizve különféle kémprogramokra figyelmeztetnek, ám a valódi vírusirtókkal ellentétben itt sem a mentesítés, sem az adatbázis-frissítés nem működik: előbb fizetni kellene egy 50-100 dollár közötti összeget. Ha végiggondoljuk, hány tájékozatlan átlagfelhasználó eshet áldozatul naponta, megértjük, mi motiválja ezeket az embereket. A botnetek segítségével terített hamis antivírusok elképesztő összegekhez juttatják a bűnözőket, az antivírusblogban már 2008-ban írtunk olyan esetről, melyben az elkövetők nagyjából 32 millió forintnak megfelelő bevételt zsebelhettek be - hetente.

Ez a sikeres vonal szemlátomást megtetszett a kártevő terjesztőknek, a későbbiekben változatos neveken rengeteg álantivírust generáltak, amelyek tulajdonképpen kinézetükben nem is nagyon, inkább csak az elnevezésükben különböztek egymástól. Aki úgy gondolta, hogy ennél rosszabb már nem is lehet, tévedett. Egy idő után a valódi, létező piaci termékek nevéhez hasonlító elnevezésekkel is elkezdtek játszani, így keletkezett aztán a Wireshark Antivirus, a SysInternals Antivirus, de volt XP Smart Security, AVG Anti-virus 2008, ahol a weblapon még a TÜV, Virus Bulletin, ICSA Labs logókat is odabiggyesztették. A trükkök itt még korántsem értek véget, idővel bővült a portfólió a hamis rendszerkarbantartó programokkal, mint Smart Defragmenter, HDD Doctor, Windows Restore, Windows Recovery vagy Windows Repair. A közös mindegyikben az, hogy az állítólagosan észlelt

"rendellenesség" elhárítását itt is csak a bankkártyás utalás utánra ígérik.

Még mindig nincs vége, újabb ötlettől vezérelve előkerült egy új módszer, melyben valamilyen hivatalos jogvédő szervezet illegális letöltés nyomát, vagy egyenesen merevlemezünkön található illegális állományok jelenlétét „érzékelte”, és felajánlja: a pereskedést csak úgy kerülhetjük el, ha fizetünk. A már eddig is elképesztő bevételeket produkáló hamis antivírusok mellé ezzel hétmérföldes lépésekkel felzárkóztak immár a rendőrségi, RIAA, FBI, DEA és egyéb váltságdíjat szedő kártevők is. Ez a módszer aztán tovább csiszolódott, és manapság nem ritka, hogy állítólagos pedofil letöltésekre figyelmeztetnek, egyre gyakrabban előfordul, hogy a saját gépünkből kiolvasott böngészési előzményekből választanak linket a felugró állítólagos szerzői jogsértésre figyelmeztető ablakban, sőt a tavalyi év végén a magyar rendőrség nevében is felbukkant egy kártevő. Ez a "szolgálunk és védünk" szlogen kíséretében azt állította, hogy a számítógép hivatalosan le lett tiltva jogellenes tevékenység miatt, és csak 20 ezer forint Ukash átutalása után oldják fel a zárolását.

Súlyosbítja a helyzetet, hogy a sokszor országhatárokon átívelő csalássorozatok valódi kitervelőit és elkövetőit nagyon ritkán tudják elcsípni. Ahogy Al Capone esetében is, itt is ígéretes csapásirány lehet a pénz követése, remélhetőleg ebben majd látunk a bankok, fizetésközvetítők részéről is megfelelő akaratot, együttműködést. Egy IT biztonsággal foglalkozó portál azt írta, 2013. a rosszindulatú, váltságdíjszedő szoftverek éve lehet. A felhasználók részéről hasznos lenne a biztonságtudatosabb hozzáállás: magyarul óvatos vagyok, nem hiszek el mindent, ami a képernyőre van írva, és sosem fizetek váltságdíjat. Ha pedig már meg van a baj, a tapasztaltabbak sikerrel próbálkozhatnak a csökkentett módban való indításnál végzett mentesítéssel, míg a kevésbé tapasztaltak mindehhez inkább a környezetükből kérjenek szakmai segítséget.

Egy biztos, nekünk felhasználóknak ezek az esetek tanulságos példák arra, hogy mindig naprakész valódi antivírust és rendszeresen frissített operációs rendszert használjunk, emellett sose hanyagoljuk el munkáink gyakori és rendszeres mentését külső adathordozóra.

---

IT Business Online