VAN ITT MINDEN, MINT KARÁCSONYKOR

Pénzt vagy életet!

A múlt hónapban a hamis antivírus programokkal foglalkoztunk. Ezek fő jellemzője, hogy nem létező fertőzéseket imitálva pénzt próbálnak meg kizsarolni tőlünk. A nagy elől, a magyar Furkó Antivírus lehet, hogy talán mintául szolgálhatott az utódoknak. Sorozatunk mostani, tizenhatodik epizódjában mindenesetre bemutatjuk ezt a korát megelőző programot, valamint néhány más váltságdíjszedő kártevőt.

Ki a múltat háborgatja, folyjon ki a fél szeme. De ki a múltat elfelejti, annak mind a kettő – mondja *Alexander Szolzsenyicin*. Mi sem tehetjük meg, hogy korábbi malőrökről elfeledkezünk, és igazság szerint nem is érdemes ezt tenni, hiszen nagyon tanulságos esetekről van szó.

Ransomware – ezt a kategóriát magyarul zsaroló, váltságdíjat követelő kártevőnek nevezhetjük. Megszületését egy 1989-es esethez kötik, ahol egy cég AIDS-szel kapcsolatos információs floppylemezt küldött szét mintegy huszonhatezer egészségügyi intézmény címére. A címjegyzék tanúsága szerint három példányt Magyarországra is elküldtek: a Hematológiai Intézetbe, a János Kórházba és a KFKI-be, de ezeknek – állítólag postázás közben – lába kelt, ami jelen esetben utólag szerencsés fordulatnak is értékelhető. A lemez egy aljas programozási trükkel operált, és közben figyelte a rendszerindítások számát. Egy saját algoritmus alapján folyamatosan titkosította a merevlemezen az állományokat és a könyvtárakat. Szerencsés esetben, ha valaki idejekorán észlelte, korai fázisban tiszta rendszerlemezről bootolva még el tudta menteni a saját adatait. 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 fizethetünk csekken vagy átutalással is. Ez egy színtiszta zsarolási manőver volt, és vegyük észre azt is, hogy remek érzékkel kihasználta, hogy sokan érdeklődtek az akkor még új, ismeretlen és félelmetes AIDS iránt. A történet utóéletéhez tartozik, hogy később sikerült elfogni a készítőt, egy bizonyos *Joseph L. Poppot*, aki Panamában a PC Cyborg Corporation nevű céget jegyezte és majd' egy évig készítette elő ezt az akcióját.

Hány fél egy egész?

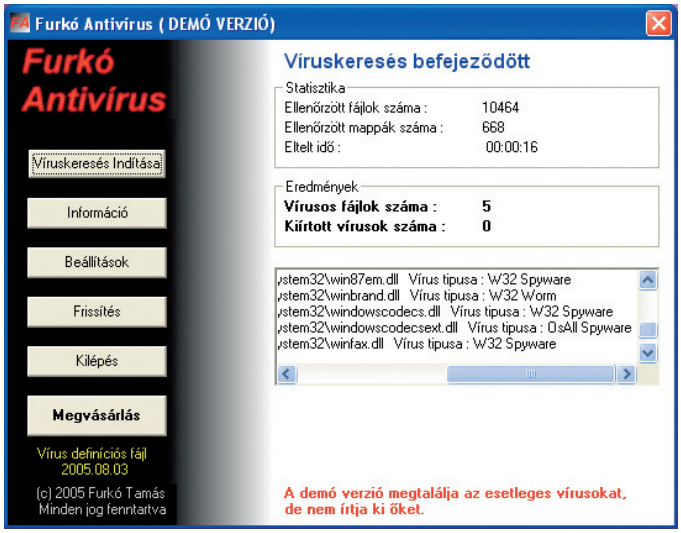
Korábban, *a 12. epizódban* már megemlékeztünk a körülbelül 1995-ben feltűnt One Half nevű DOS-os vírusról, amely a merevlemezről történő bootolásonként 2-2 cilinder teljes tartalmát titkosította, a merevlemez végéről indulva. Ha csak simán mentettük a gépet, az elkódolt részhez soha többé nem fértünk hozzá, hiszen a szükséges kulcsfontosságú információt a Master Boot Recordba (MBR) beköltözött vírusban tárolták. Egy meggondolatlan „fdisk /mbr" parancs után – az egyedi kód hiányában már lehetetlen volt az adatok visszaalakítása. Szerencsére később *Leitold Ferenc* vírusvédelmi szakértő készített hozzá egy egyedi dekódoló segédprogramot OneHalf Killer néven, amely a tényleges fizikai mentesítés előtt képes volt visszaalakítani az eredeti adatokat. Itt valójában ugyan nem kértek váltságdíjat, de a károkozást igyekeztek minél tovább rejtve tartani, hogy ezzel is fokozhassák a felhasználót érő kárt.

Csak kiegészítésként érdemes megemlíteni, hogy a OneHalf vírus kora ellenére nem feltétlenül csak a múltat jelképezi. Képes arra, hogy egy mai windowsos rendszeren is tényekedjen,

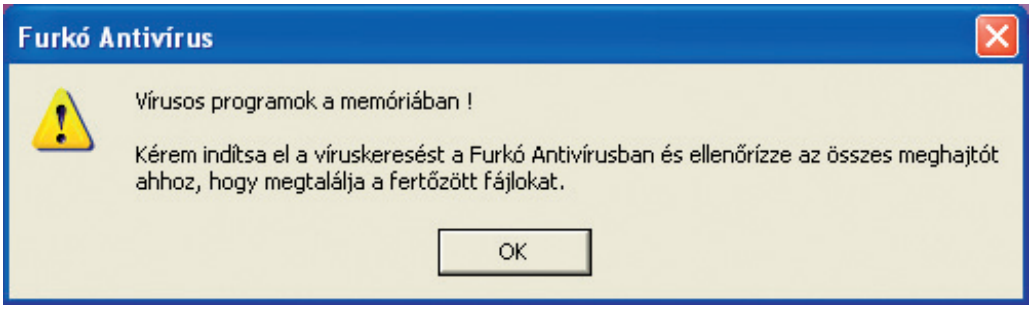
```
Dear Customer:

It is time to pay for your software lease from PC Cyborg corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed invoice, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:
a renewal software package with easy to follow, complete instructions;
an automatic, self-installing diskette that anyone can apply in minutes.

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378. You must enclose a bankers draft,
cashiers check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, PO Box 87-17-44, Panama 7, Panama.
```

Az AIDS tájékoztatólemezen terjesztett trójai szerzője állítólag egy évig készítette elő az akcióját. Azt nem tudni, hogy mire gondolt, amikor megadta cége nevét és a panamai postafiókot. Mindenesetre ezzel nem tette túl magasra a lécet az utána nyomozó szövetségi és titkos ügynököknek

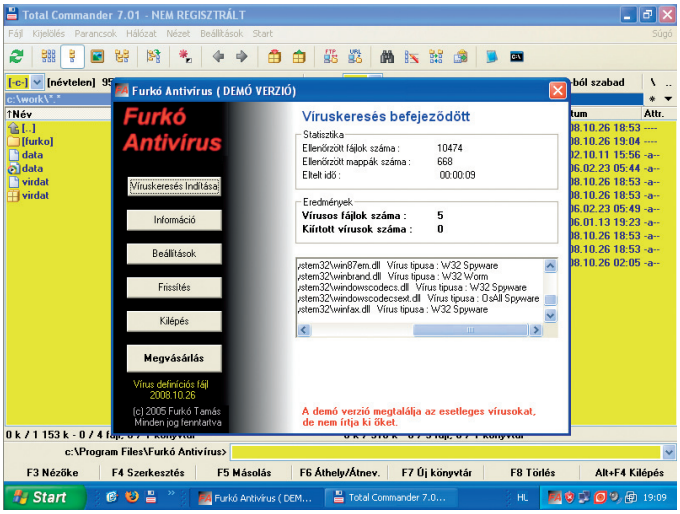
Bár a PC Cyborg Corporation már megszűnt, az emléke megmaradt a Wikipédián: en.wikipedia.org/wiki/PC_Cyborg_Trojan



Furkó Tamás műve valódi szellemi elődnek tekinthető a mai hamis antivírusok szempontjából. Íme a szokásos öt .dll állomány, ami állítólag mindenkinél „fertőzött". Mi most mosolygunk ezen, de igazából egyáltalán nem mulatságos a kevésbé hozzáértők ilyen átverése



Még az újonnan telepített gépeken is megkaptuk a figyelmeztetést. Valószínűleg ez indíthatta be a felhasználók fantáziáját, hogy itt valami nagyon gyanús machináció zajlik a háttérben



Ez a kép azért vicces, mert a frissítés idejéhez beírta az aznapi dátumot

Lustaság és hanyagság – akár ez is lehetne ennek kisplasztikai biennálén induló műnek a címe. A letöltési oldalak jól láthatóan nagy ívben tesznek arra, mit kínálnak fel letöltésre

hiszen a MBR-ből indul. Ezt igazolja, hogy azóta is felbukkan néha néhány számítógépen. Terjedni persze nehezen tud, mert a Windows elindulását követően már törlődik a memóriából, viszont ahányszor újraindítjuk a gépet, annyiszor végzi el a következő 2 cilinder kódolását.

Hát ennyit a távoli múltról, és most nézzünk néhány további frissebb érdekességet a zsarolás műfajából.

Magyar gépre magyar „antivírust”

2005 táján megjelent az interneten egy Furkó Antivirus nevű csomag, amely nemcsak a **www.furkoantivirus.com** weblapon, hanem számos letöltőoldal kínálatában is szerepelt.

Ha valaki vette a fáradtságot és letöltötte, érdekes dolgokat tapasztalhatott. Először is a többi vírusirtó próbaváltozathoz képest nem egy időkorlátozással szembesülünk a demóban, ami amúgy teljes értékűen működik, hanem szokatlan módon az ingyenes próbaváltozat csak kijelezte a veszélyeket, de irtani csak és kizárólag a fizetős változattal tudtunk a készítő ígérete szerint.

Csiszér Béla (a NOD32 programot Magyarországon forgalmazó Sicontact Kft. vezetője) nevéhez kötődik a nagy leleplezés, rájött ugyanis, hogy a program könyvtárában található data.dat fájl valójában egy *EA Sports* játékból származó MP3 audiofájl, ahol a bemondó egy autóverseny kezdetét jelenti be – ezt érdemes is átnevezés után meghallgatni, ahol világosan hallani benne, hogy a Nascar autóverseny nevét is emlegetik. Nem érdemi vírusadatbázis állomány az eredeti virdat.dat sem, ez pedig egy jelszóval védett közönséges RAR tömörített állomány. A vírusirtó adatbázisának „frissítésekor” egy ingyenes magyar tárhelyszolgáltató szerveréről letöltődő új virdat.dat sem tartalmaz a kártevők azonosításához használható információkat, ugyanis ez az állomány a *Moorhuhn 2* című csirkevadász sikerjáték mudGE.dll fájlja volt, átnevezve. Mi a mostani kísérletnél már ezt nem is tudtuk letölteni, a „frissítés” után csak egy 0 bájt hosszú virdat.dat állományt kaptunk, viszont a program felhasználói menüjében a frissítés ideje az aktuális dátumra frissült. Szóval szemfényvesztés az egész.

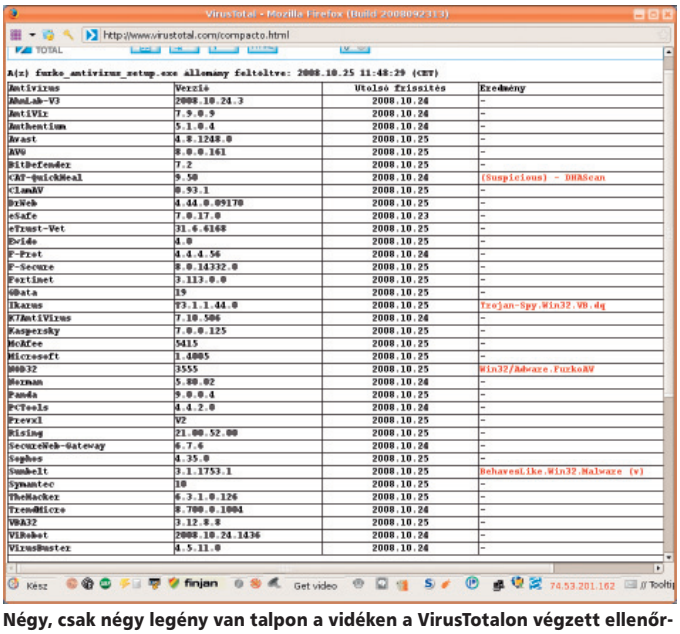
A király meztelen

Főleg a fertőzésre, a kéretlen ablakokra és a fizetős változat megvásárlására tett erőfeszítésekre koncentráltuk eddig figyelmünket, azonban van még egy fontos szempont, amit mindenképpen érdemes megemlíteni. Amivel még nagy bajt okozhat egy ilyen hamis antivírus program, az a hamis biztonságérzet, amit a gyanútlan felhasználókban kelthet: aki telepíti, azt hiheti, hogy így már védve van a vírusoktól, kémprogramoktól – holott erről, ahogyan láttuk is, szó nincsen.

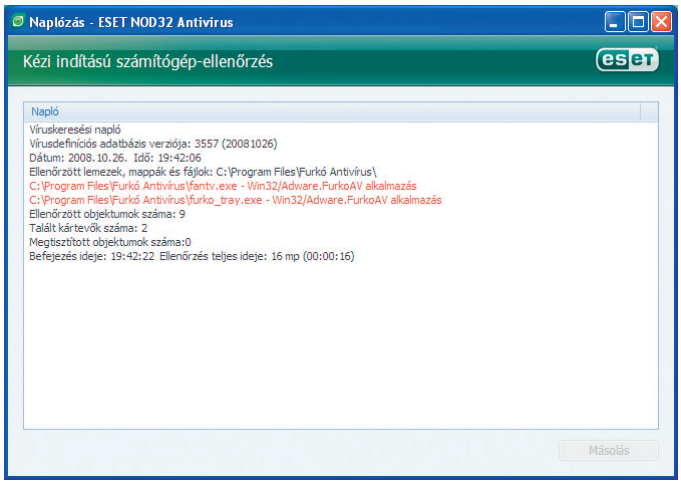
A Furkó Antivirust szinte minden tekintetben nagy elődnek tekinthetjük a manapság ipari méretekben zajló hamis antivírus biznisz szempontjából: nem végez érdemi vírusirtást, mert saját maga a kártevő; újonnan telepített tiszta rendszeren is talál

```
meta name "description"
content="A Furkó Antivírus egy 5 csillagos értékelésû nagyon gyors és hatékony antivírus szoftver"

meta name "keywords"
content="antivirus.com antivirus, virusirto, antivírus, anti-virus,anti-vírus,vírus irtó, virus irto, szex, sex, tini, szex, baszas, pina, fuck, víruskereső, virus kereső, viruskereso, virus, kereso, szex,sex,mp3,zene,film,dvd,cd,letöltés, dwonload, software, ferrari, lamborghini, porshe, mercedes, bmw, schumaher, forma 1, sport, foci, football, internet, hardware, vásárlás"
```

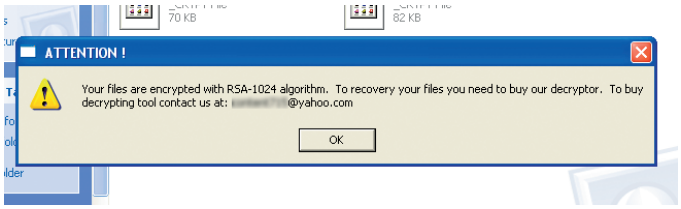
Bár a weboldal már nem működik – a leleplező HWSW-s, illetve origós cikk után azonnal megszűnt –, a lementett változat sok mindenről árulkodik a figyelmes szemlélőnek. Az biztos, hogy az ilyen kulcsszavak nem sok bizalmat ébresztenek abban, aki egy komoly biztonsági program weblapján véletlenül belekukkant az oldal HTML-kódjába



Négy, csak négy legény van talpon a vidéken a VirusTotalon végzett ellenőrzés szerint. Azaz a hazai ál-antivírus termést külföldön csak kevesen ismerik fel kártevőként



A kísérletezéshez ki kellett kapcsolni a NOD32 antivírust, mert azonnal beriasztott már a Furkó telepítőcsomagjára is



Amit senki sem szeretne látni a saját monitorán: „Az ön állományait RSA-1024 algoritmussal elkódoltuk. Ezek visszaalakításához szüksége lesz a mi dekódoló programunk megvásárlására. A dekódoló eszköz megvásárlásához kérjük, írjon a következő e-mail címre!"

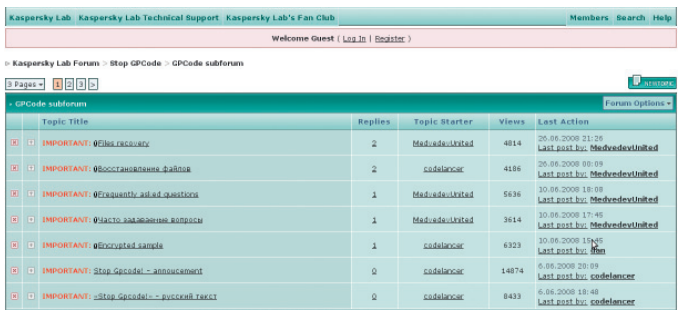
„fertőzést"; az adatbázis-frissítés egyáltalán nem oldja meg a gondjainkat vagy nem is csinál semmit; és végül, de nem utolsósorban pénzt akar – ez a program fő célja.

Ami még nevetséges vagy inkább sírnivaló, hogy a Furkó Antivírus még a mai napig (2008. novemberben készült ez az írás) szerepel számos letöltéssel foglalkozó honlap kínálatában. Egy magára valamit is adó letöltőoldal egy termékről hogy mondhat olyat vagy másolhat át bambán, hogy „Uses cutting edge technology to detect virus and remove them immediately"? Ki sem próbálták, annyi szent, csak ment az iparszerű tartalom- és linkgyártás, kopi meg a paszta, amelyet egy megfelelően idomított pávián is megtehetne megfelelő mennyiségű banánnal dresszírozva. Sajnos, ahogy az élet más területén is, sok mindenben a felhígulást és a spórolást látjuk: könyvek jelennek meg futószalagon szakmai lektor és nyelvi ellenőrzés nélkül, de ez már messzire vezetne, kanyarodjunk vissza a ransomware témájához.

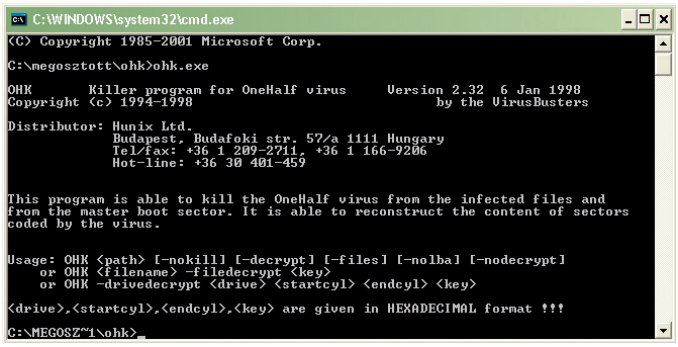
Zsarolók és váltságdíjak

Mintha ez a gondolatmenet éledt volna ismét újjá a GPCode kártevő 2008-ban megjelent új változata esetében is, amelyre a Kaspersky kutatói hívták fel a figyelmet. A család első tagja még 2005 decemberében látott napvilágot. A GPCode kártevő új változata különösen erős, 1024 bites RSA-titkosítással kódolja el a felhasználó adatait (például a .doc, .jpg, .pdf kiterjesztésű fájlokat), majd letörli az eredeti, kódolatlan példányokat. Ha végzett, akkor üzenetet küld a felhasználónak, hogy az állományai túszul lettek ejtve, és némi készpénz fejében felajánlja a titkosítást feloldó kulcsot. A titkosítás ezekben az esetekben a brute force (azaz nyers erő, vagyis próbálgatásos) módszerrel akár több millió évig is eltarthatna, de szerencsére az antivírus cégek összefogásával sikerült hibát találni a kártevőben és ennek segítségével visszaállítani a kódolt fájlokat. Az új, GPCode.AK jelű változat már 143-féle állománytípust tesz olvashatatlanná, amihez a Windows beépített Microsoft Enhanced Cryptographic Provider modulját használja. A Kaspersky cég nyáron felhívást tett közzé, amelyben titkosítási szakembereket toborzott a visszafejtéshez. Ennek meg is lett az eredménye, első körben sikerült kideríteni, hogy a már elkódolt állományok eredeti állományainak törlése egyszerű delete funkcióval történik, ezért minden „Undelete" segédprogram segíthet ezekben az esetekben, ha még nem történt felülírás. Ez kétségkívül hiba volt a támadók részéről, amit a következő kártevőverzióban már biztosan javítani fognak. Később aztán érdemi megoldás is született az állományok mentesítésére, bár a visszakódolás hatékonysága itt csak körülbelül 80–90 százalékosra sikerült.

Annyit mindenesetre láthatunk, hogy bár szinte minden esetben viszonylag kis összegeket kértek az elkövetők, a zsarolásból befolyó pénz átvétele elég körülményes és rendszerint kinyomozható, ezért e rizikótényező mellett valószínűleg nem találták meg a számításukat. Erre utal az is, hogy néhány esetben – a nulladik napi sebezhetőségek demonstrációs exploit kódjaihoz hasonlóan – igyekeztek közvetlenül az antivírus cégeknél kopogtatva pénzzé tenni a titkosítórutinjukat. Egy biztos, nekünk felhasználóknak ezek az esetek remek példák arra, hogy ne hanyagoljuk el munkáink rendszeres mentését külső adathordozóra.



A GPCode zsaroló vírus visszafejtésére nemcsak felhívást tett közzé a Kaspersky cég, de a kapcsolódó fórumon a szakemberek a világ minden tájáról meg is osztották a tapasztalataikat



OneHalf Killer: ez a remek segédprogram sokaknak mentette meg a merevlemezen csapdába esett létfontosságú adatait

Vírusirtót készítene, de nem boldogul? Sebaj, vegyen egy DLL-t egy lövöldözős játékból, egy MP3 állományt egy másik, autóversenyes játékból, és máris kész az új vírusismereti adatbázis. Akármilyen hihetetlen, de volt, aki tényleg így csinálta

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemeny@pcworld.hu).

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

KAPCSOLÓDÓ WEBOLDALAK

www.eset.hu/virus
www.antivirus.hu