A HAMIS ANTIVÍRUSOK ÚJABB FEJEZETE

Ipari forradalom

Sorozatunk huszonnyolcadik epizódjában ismét műsorra tűzzük a hamis antivírusok problematikáját. Éppen egy éve írtunk erről hosszabban, az egész cikket a témának szánva. Hogy mi a csalás lényege, arról sok mindent elmondtunk már korábban, de az, hogy hogyan vált mindez a hétköznapok részévé, hogyan vetnek be a készítők tömegesen és egyre kifinomultabban minden technikai, illetve megtévesztésen alapuló trükköt – ez már szinte felér egy ipari forradalommal.

Sorozatunk 18. epizódját ott fejeztük be, hogy az orosz Bakasoftware egyik tagja nyilatkozott a hamis vírusirtóval kapcsolatos tevékenységük részleteiről. Az illető nem volt főnök a bandában, de részt vett a fejlesztési munkában, és a hamis fertőzésekkel riogató program egyik készítőjeként 158 ezer dolláros (mintegy 30 millió forintos) keresetet tehetett zsebre hetente. Ezzel már tudjuk is a miérteket: ez egy mocskos, de jól jövedelmező üzlet. Ha akkor úgy gondoltuk, hogy csak néhány ilyen ember, illetve banda van, akiktől még nyugodtan alhatunk, hét nagyon nagyot tévedtünk.

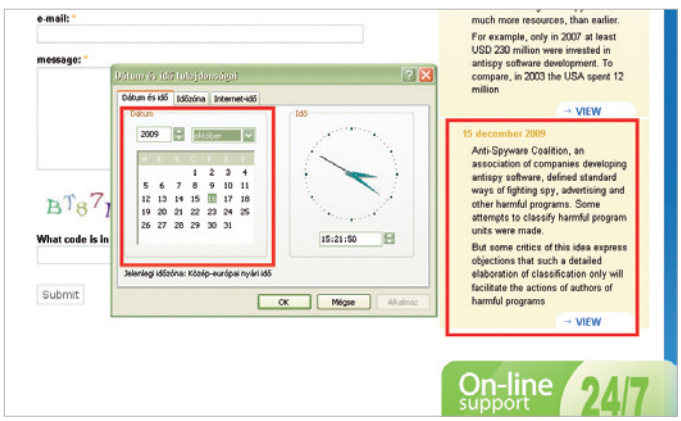
Pénzért bármit

Az USA-ban több millió számítógép lett fertőzött ezzel a módszerrel, állapította meg többek közt a Symantec kiberbűnözésről szóló jelentése. Több százféle ilyen program létezik, és számuk napról napra emelkedik, sőt a csaló honlapot generáló webkészlet már árucikké vált.

A *Networkworld* számolt be róla, hogy egy pay-per-install nevű weboldalon nyílt színen folyik a kártevőkkel történő üzletkötés. A virtuális piactér célja, hogy összehozza a potenciális megbízókat a botnetek alkotóival. Nem lepődtünk meg persze korábban sem azon, hogy a BBC hogyan és honnan jutott olyan könnyen botnet-vezérlésre alkalmas programhoz, hogyan béreltek ki egy ilyet – valószínűleg egyáltalán nem volt nehéz dolguk. De míg az ő akciójuk inkább a figyelemfelkeltést szolgálta, az átlagos kuncsaftok jelentős része persze nem ezért megy oda. Az árak a beszámoló szerint országonként változnak, egy 1000 tagú botnet 110 USD-t kóstál az Egyesült Királyságban, 60 USD, ha mindez Olaszországban van, a franciaországi ezer gépért már csak 30

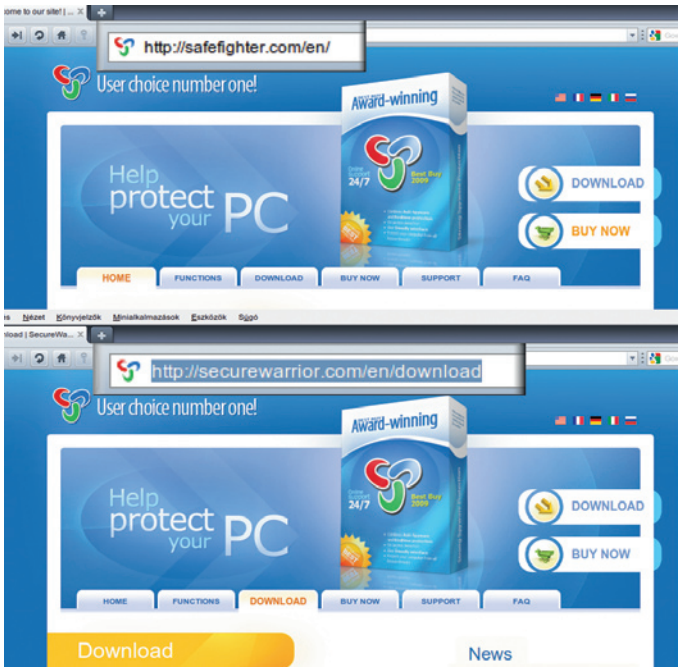
Advanced Cleaner	MacSweeper	SpySpotter
AlfaCleaner	MalCrush 3.7	Spyware Cleaner
AntiSpyCheck 2.1	Malware Bell 3.2	Spyware Quake
AntiSpyStorm	MalwareAlarm	Spyware Stormer
AntiSpyware Shield	MalwareCore	SpywareGuard 2008
AntiSpywareExpert	MS Antivirus	SpywareStrike
AntiSpywareMaster	PAL Spyware Remover	SpyWiper
AntiSpywareSuite	PC Antispy	System anti virus 2008
Antivermins	PC Clean Pro	System Live Protect
Antivirgear	PC SpeedScan Pro	SystemDoctor
Antivirus 2008	PC-Antispyware	TheSpyBot
Antivirus 2009	PCPrivacytool	Total Secure 2009
AntiVirus Gold	PCSecureSystem	TrustedAntivirus
Antivirus Master	Perfect Cleaner	Ultimate Antivirus
Antivirus pro 2009	PersonalAntiSpy	Free UltimateCleaner
Antivirus XP 2008	PestTrap	Virus Isolator
Avatod Antispyware 8.0	PSGuard	Virus Respone Lab 2009
Awola	Rapid AntiVirus	Virus Trigger
BestsellerAntivirus	Registry Great	VirusBurst
Brave Sentry	Saliar	VirusHeat
Cleanator	SecurePCCleaner	VirusProtectPro
ContraVirus	Security toolbar 7.1	VirusRanger
Disk Knight	Smart Antivirus 2008	VirusRemover2008
Doctor Antivirus	Smart Antivirus 2009	Vista Antivirus 2008
DriveCleaner	Spy Away	WinAntiVirus Pro 2006
EasySpywareCleaner	SpyAxe	WinDefender
Errorsafe	SpyCrush	WinFixer
free-viruscan.com	Spydawn	WinSpywareProtect
IE Antivirus	SpyGuarder	WorldAntiSpy
IEDefender	SpyHeal	XP AntiSpyware 2009
InfeStop	Spylocked	XP Antivirus
Internet Antivirus	Spy-Rid	Zinaps AntiSpyware 2008
KVMSecure	SpySheriff	

Pár név a többezer variációból. Van egy névgenerátor, bedobják a hozzávalókat, és alul kijönnek a variációk: Soft Soldier, Trust Soldier, Trust Warrior, Soft Warrior, lehetőleg a jövő évi dátum, de hasonlíthat meglévő valós antivírus megoldás elnevezésére is



A soha nem létezett és soha fejbe nem lőtt moszkvai spammer állítólagos haláláról hírt adó „blog" juthat erről az eszünkbe. Igaz, itt nem a pár napja foglalt domain mutat több hónapos „archívumot", hanem simán előre dátumozva jelentetnek meg fiktív cikket. Lehet, hogy közben azt gondolják, aki még ezt is benézi, az meg is érdemli. Vegyük észre, hogy a bűnözőknek írni csak captcha-biztosítással lehet, ők maguk nem szeretnek botok által támadva lenni

Egy bölcs tanács: „Ne telepíts olyan szoftvert a gépedre, amelynek nevére a Google-ben rákeresve csupa »How to Remove?« kezdetű találatot kapsz!"



Viccesen szokták mondani, hogy a tévéreklámokban a frissen mosott ruhák azért látszanak újnak, mert valóban újak. Nos, ennek analógiájára a hamis antivírusok azért látszanak hasonlónak, vagy éppen egyformának, mert pénzért árult generáló kitekkel készülnek egy kaptafára. A vásárlónak nem szükséges számítástechnikai programozónak lennie, elég, ha a befolyt pénz tisztára mosásához ért jól

USD-t kell leszurkolni, és ugyanez Ázsiában mindössze 6 amerikai dollárba fáj. Biztonsági cégek szerint az ilyen kártékony kódok készítői Kelet-Európában, illetve a volt Szovjetunió területéről próbálnak meg ily módon jövedelemhez jutni.

Az egyik legkelendőbb árucikk jelenleg is a hamis antivírus program, ez most éppen 70 USD. *Eric Chien* (Symantec) szerint kevés az esély az ilyen ellenőrizetlen piacok bezárására, mert mindig megfelelő érinthetetlen tárhelyszolgáltatót találnak maguknak, illetve szükség esetén sűrűn költözködnek is.

Böngészés közben jön az „áldás”

Vicces látni, amikor egy fehér köpenyes hamis antivírus program az alternatív operációs rendszereken fertőzött DLL-eket fedez fel, és hogy Win32-es vírusokat is lel OS X, illetve Linux alatt. Ennek persze az az oka, hogy itt szó sincs valódi keresésről, hanem csak egy animáció fut le a szemünk előtt, állandóan azonos eredménnyel, ha elindítjuk a fertőzött weboldalt Ubuntu Linux vagy Snow Leopard alatt. A javascriptes ablakok meg egyre csak jönnek. Riasztó, hogy milyen agresszívan nyílnak ezek a popup ablakok, nagy számban, sűrűn és rendkívül idegesítően, a hétköznapi felhasználókat hidegrázósra ijesztően.

Csilivili „antivírus” weblapok

Szőke nő, barna nő, fekete nő, és mindegyik ránk mosolyog. A Kft.

Ha egy adott alkalmazás weboldala hajszálra olyan, mint a másiké, ennek is komoly kétségeket kellene ébresztenie a látogatókban. Persze a lépre menő 5 százalék sajnos nem profi, hanem átlagos felhasználó, aki nem néz se jobbra, se balra, hanem szépen bejárja a jól megtervezett és neki felállított „megijed, megörül, fizet” útvonalat

Szőke nő, barna nő, fekete nő, és mindegyik ránk mosolyog. Ahogy a használtautó-vásárlásnál mondani szokták, nemcsak az autót kell megnézni, hanem azt is, kitől vesszük. Nos a teszt- és egyéb győzelmeket sugalló plecsnikkel is ez a helyzet. Ha a domaint előző héten jegyezték be Kínában, akkor szerintünk a plecsnijét a kalapja mellé tűzheti

zenekar albumának címét („Siker, pénz, nők, csillogás”) kölcsönözve a sort még kiegészíthetjük még a jól ismert szimbólumokkal és plecsnikkel is. Ahogy a használtautó-vásárlásnál mondani szokták: nemcsak az autót kell megnézni, hanem azt is, kitől vesszük. Nos, a teszt- és egyéb győzelmeket sugalló plecsnikkel is ez a helyzet, különösen, ha a domaint előző héten jegyezték be Kínában. Az „emberes” kép, reklám, weboldal pszichológiai hatása is megerősítő, pozitív. Van egy névgenerátor, bedobják a hozzávalókat, és alul kijönnek a variációk: Soft Soldier, Trust Soldier, Trust Warrior, Soft Warrior stb. Lehetőleg szerepeljen a névben a jövő évi dátum is, de hasonlíthat meglévő valós antivírus szoftver elnevezésére is, így lehet például „Windows Enterprise Defender” (l. BitDefender) vagy éppenséggel Smart Antivírus 2009 (az ESET Smart Security után).

A vicces az egészben, hogy a többtucatnyi programnévhez tartozó domainregisztrációkat is folyamatosan, szépen, szervezetten oldják meg. Az APWG (Anti-Phishing Working Group) 2009-es jelentése szerint csak az első félévben 485 ezer olyan mintát gyűjtöttek, amelyeket hamis biztonsági programként soroltak be. A dolog a szimpla bosszantó kategóriából

Az ipari méretű csalás nem ismer országhatárokat, és nyelvi korlátokat sem. Angol, francia, német, olasz és orosz nyelvű honlapot is elkészítettek a csaló készletben, így csak egy kattintás kell hozzá

Itt szemlátomást kihagyták a korábban bemutatott captcha-védelmet, de azért az jól látszik, hogy a kérdezni szándékozó nyájas ügyfél bedobja az e-mail címét és nevét – Vaszilij pedig majd örül ennek, hiszen ő gyűjti a címeket –, a megrendelő aztán várhatja, hogy az ígért 24/7 terméktámogatás megérkezzen. Kicsit olyan „Királyfi, és te még hiszel a mesékben?"-érzésünk van. A megbízható, valódi vírusvédelmi cégek az adott országbeli elérhető telephellyel, postacímmel, nyilvános e-mail címmel és telefon-, faxszámmal nyújtják a legális technikai támogatást

vészesen növekvő léptékűvé vált, és ezt a helyzetet kezelni kell.

How to remove?

Ősi dakota közmondás szerint „Ne telepíts olyan szoftvert a gépedre, amelynek nevére a Google-ben rákeresve csupa »How to Remove?« (Hogy lehet eltávolítani?) kezdetű találatot kapsz!" Van néhány olyan honlap, ahol viszont kimerítő részletességgel és dicséretes naprakészséggel vezetik az összes új hamis antivírus program letakarítási útmutatóit. Ilyen például a *remove-malware.net*, vagy a **www.myantispyware.com**. A mentesítés nehézségét fokozza, hogy nem ritka a rejtett rootkit-komponens sem. Sajnos a hamis antivírus programok készítői is alaposan dolgoznak. Ha megnézünk egy ilyen How to Remove leírást, számtalan „ragaszkodó" Registry bejegyzés, letiltott Regedit, blokkolt antivírus

VIRUS TOTAL

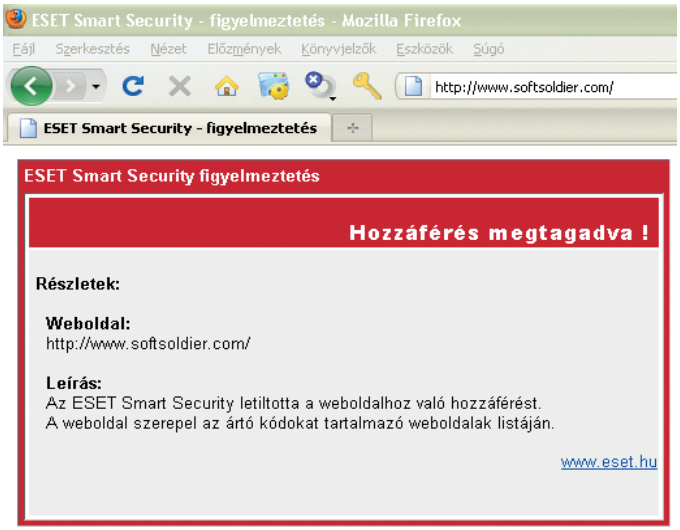
A VirusTotal **egy olyan szolgáltatás, amellyel számos antivírus motor segítségével gyanús állományokat elemezhetünk**, használata megkönnyíti a vírusok, férgek, trójai falovak és más kártevők gyors észlelését. További információ...

A(z) **install.exe** állomány feltöltve: **2009.10.16 14:02:50 (UTC)**
Pillanatnyi állapot: **befejeződött**
Eredmény: **22/41 (53.66%)**

Formázott | Eredmény nyomtatása

Antivírus	Verzió	Utolsó frissítés	Eredmény
DrWeb	5.0.0.12182	2009.10.16	-
eSafe	7.0.17.0	2009.10.15	-
eTrust-Vet	35.1.7071	2009.10.16	-
F-Prot	4.5.1.85	2009.10.15	-
F-Secure	8.0.14470.0	2009.10.16	FraudTool.Win32.PersonalAntivirus.dv
Fortinet	3.120.0.0	2009.10.16	-
GData	19	2009.10.16	Gen:Trojan.Heur.@xW@vf3BOPlcx
Ikarus	T3.1.1.72.0	2009.10.16	Gen.Trojan
Jiangmin	11.0.800	2009.10.16	-
K7AntiVirus	7.10.872	2009.10.16	Trojan.Win32.Malware.1
Kaspersky	7.0.0.125	2009.10.16	not-a-virus:FraudTool.Win32.PersonalAntivirus.dv
McAfee	5772	2009.10.15	-
McAfee+Artemis	5772	2009.10.15	Artemis!27FBA2A82EEA
McAfee-GW-Edition	6.8.5	2009.10.16	Trojan.Spy.4876800
Microsoft	1.5101	2009.10.16	Virus:Win32/Induc.A
NOD32	4514	2009.10.16	a variant of Win32/Kryptik.APD

Sajnos a hamis antivírus programok készítői is alaposan dolgoznak. Ha megnézünk egy ilyen How to Remove leírást, számtalan „ragaszkodó" Registry bejegyzés, kéretlen állomány, különféle mappákban szétszórt kártevőmásolatok gondoskodnak arról, hogy a kivakarás minél nehezebb legyen. Az egyre újabb változatok is próbára teszik az antivírus motorok intelligenciáját, szó sincs minden valódi antivírus termék általi százszázalékos észlelésről, és mindig akad egy olyan új variáns, ami a korábbi sikeres detektálást kijátszva újra munkát ad a víruslaborosoknak



A bejelentések nyomán a vírusvédelmi programok feketelistára teszik a kártevőterjesztő domaineket, így segítve a naprakész vírusirtóval böngésző felhasználókat. Persze a rosszfiúknak is van erre a válaszuk: egyre rövidül az az idő, amíg egy adott webcímet használnak, mielőtt másikra költöznének

weblap, kéretlen állomány, különféle mappákban szétszórt kártevőmásolatok gondoskodnak arról, hogy a kivakarás minél nehezebb legyen. Az egyre újabb változatok is próbára teszik az antivírus motorok intelligenciáját, szó sincs minden valódi antivírus termék általi százszázalékos észlelésről, és mindig akad olyan új variáns, ami a korábbi sikeres detektálást kijátszva újra munkát ad a víruslaborosoknak.

A jel hiánya is jel

A jogi problémák elkerülésére (hogy ne indítsanak ellenük kártevő-terjesztésért eljárást) néhány helyen már olyan weboldal is feltűnt, amelyikről nem lehet letölteni semmilyen szoftvert, csak egy üres ciklus fut le rendre. Nincs letölthető, analizálható kártevő, nem lehet őket hamis vagy rossz minőségű biztonsági program terjesztéséért okolni. Viszont így is megmaradnak nekik a megtévesztettek személyes adatai (a supporthoz küldött név, e-mail cím eladható a spamadatbázisba), a megijedt felhasználók körülbelül öt százaléka átutalja nekik az 50-100 amerikai dollár közötti összeget – ezt több országon keresztül, verbuvált önkéntesekkel (mule) tovább utaltatják, és így mossák tisztára. A megfertőzött gépek is rendszerint felhasználhatók további botnetes károkozásokra: a tulajdonos tudta nélkül küldhetők például további spam hirdetések akár erről a remek, Trust Soldier nevű antivírus programról. És aztán az új címzettek öt százaléka megint kattint, és így tovább.

Sorozatunk következő számában ennek a témának egy másik vetületével fogunk foglalkozni, itt már a szürke zóna és az antivírus cégek ügyvédei is egyaránt a ringbe lépnek majd.

***

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

Hogyan távolítsuk el az ál-antivírusokat:
remove-malware.net, www.myantispyware.com
32 millió forint bevétel hetente: **hopp.pcworld.hu/6425**
Amikor a fagylalt visszanyal: **hopp.pcworld.hu/6426**
Vészesen terjednek az ál-antivírusok: **hopp.pcworld.hu/6424**