JOGI LÉPÉSEK, PRÓBAPEREK – VALÓBAN EZ VÁR RÁNK?

Jogászok a víruslaborban

Sorozatunk huszonkilencedik epizódjában ott folytatjuk, ahol a múltkor befejeztük: a jogi szakértők, ügyvédek lassan az antivírus laborok oszlopos tagjai lesznek. Hogy ez furcsa? Hát meglepőnek meglepő, de ha az elmúlt évek történéseit vizsgáljuk ebből a szemszögből, akkor viszont minden egy csapásra világossá válik.

Kicsit kilógott a sok technikai téma közül az egyik előadás, amelyet a Virus Bulletin konferencián *Juraj Malcho* tartott. Az ESET vírusszakértőjének *Van-e jogász a laborban?* című prezentációja olyan kérdésre irányította rá a szakemberek figyelmét, amely minden antivírus cégnél problémát okoz. Egyre nehezebb az egyes reklámterjesztő alkalmazások megítélése, és ezzel egy időben egyre agresszívebb eszközökkel igyekeznek a kétes programok fejlesztői, a szürke zóna gátlástalan haszonélvezői a vírusvédelmi cégeket fenyegetni, döntéseiket befolyásolni.

Felismerni vagy nem felismerni, ez itt a kérdés

A bővülő lehetőségek és a számítógépes felhasználók egyre növekvő száma magával vonja számos rejtett vagy félrevezető szándékkal kifejlesztett, illetve a legjobb esetben is kétes hasznosságú alkalmazás megjelenését. Ezek létrehozását az anyagi haszonszerzés motiválja, célcsoportjuk pedig jellemzően a népesség szakmailag felkészületlenebb része. Számos ilyen szoftver nem az internetes bűnözésben használatos kártevők (például botok vagy kémprogramok) közül kerül ki, hanem inkább potenciálisan veszélyes vagy kéretlen program. Ezek a gyanús szoftverek ugyanakkor gyakran kapcsolatba hozhatók a kártevők terjesztéséért felelős csoportokkal, és továbbításuk is tisztességtelen módszerekkel, többek közt levélszemétkampányok révén vagy kártevők által végrehajtott push-alapú telepítésekkel történik.

Amikor a vírusirtó laboratóriumok felfigyelnek ezekre a módszerekre, és felkészítik termékeiket az efféle alkalmazások felismerésére, a vírusirtó szoftverek gyártói és a kéretlen szoftverek terjesztői között érdekellentét keletkezik. Ezek az ellentétek időnként jogi csatározásokhoz vezetnek, amelyek sok munkatársnak, közöttük a jogi osztály szakembereinek a részvételét is megkövetelik a döntéshozatali eljárásban, és így jelentős mennyiségű emberi és pénzügyi erőforrást vonnak el a vállalattól. Az ilyen szoftverek kategorizálására vonatkozó döntést sok esetben maguk a felhasználók teszik még nehezebbé, amikor egyéniségük, társadalmi hovatartozásuk, sőt még nemzetiségük szerint is más-más kívánalmakat és véleményeket fogalmaznak meg.

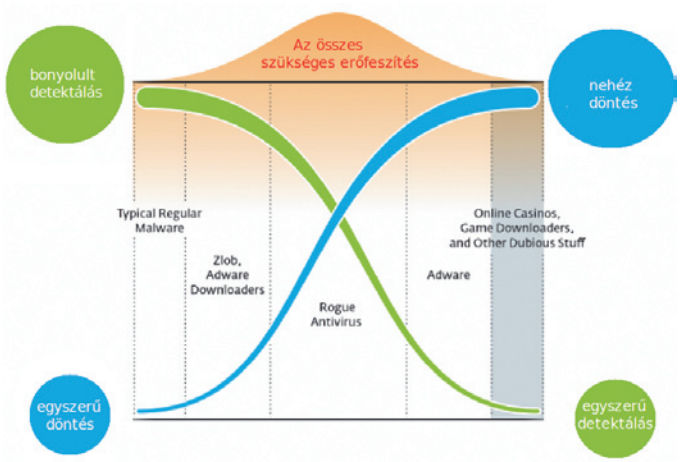
AntispywareXpPro – a maga idejében a leginkább elterjedt XP platformra fókuszáltak a bűnözők. Licencimitáció és hamis díjak, elismerések. Nem ritka a kitalált dicsérő olvasói levél sem

A javunkat akarják, ne adjuk oda!

Annak ellenére, hogy a napjainkban kifejlesztett rendszerek egyre összetettebbek, így a védelmük biztosítása is nagyobb erőfeszítést igényel, gyakran előfordulnak hibák a tervezés és a megvalósítás fázisában is. A technológiák és eszközök egyre nagyobb száma növeli a támadók számára elérhető támadási felületet is, így ők a meglévő biztonsági rések kihasználásából próbálnak hasznot húzni. Pontosan ez az alapja a számítógépes fertőzéseknek. Napjaink hatalmas mennyiségű kártékony vagy kéretlen kódja mögött az anyagi haszonszerzés szándéka áll. Még azt is kijelenthetjük, hogy ellenyésző a szerző vélt „rátermettségét" bizonyító számítógépes behatolások száma – akár kártékony szándékú, akár nem.

Szürke zóna, vékony jég

Tegyük félre a pontosan definiált kártékony kódokat, és fordítsuk figyelmünket a „greyware" gyűjtőnéven ismert kéretlen programok, azaz a szürke zóna szoftverei felé. Az ezekkel az alkalmazásokkal kapcsolatos problémák rendszerint nem a kódok összetettségében, védelmében vagy összezavarásában, illetve a felismerés megvalósításában gyökereznek. A kérdés annak megállapításától függ, hogy a szoftver kártékony-e vagy sem, illetve valamilyen szempontból hasznos-e. A való világban azonban az ilyen szoftverek hasznos vagy jogszerű voltáról végtelen vitákat lehetne folytatni. Rosszabb esetben ez néha még perekhez is vezethet. Egyre gyakrabban fordul elő, hogy hosszadalmas elemzés után egy vírusvédelmi vállalat elhatározza valamely alkalmazás ellenőrzését, amelynek a fejlesztői viszont az ellenőrzés után néhány nappal már



Az összes szükséges erőfeszítés több dimenzióban mozog. A klasszikus kártevőket viszonylag nehéz detektálni, de nem okoz gondot annak eldöntése, belekerüljenek-e a felismerési adatbázisba. A kéretlen reklámoknál viszont már nehezebb a megítélés

Európai ésszel szokatlan az úgynevezett zöld szoftverek sikere Kínában. Az alacsony ár a megjelenített reklámok miatt működik, és az ottani vásárlók nem panaszkodnak ezek miatt, míg Európában szinte egybehangzóan kiáltanának ugyanerre „kártevőt"

indokolatlan észlelésre panaszkodva kérik a szerintük téves felismerés megállapítását. Az ezt követő döntések és szempontok sorát az érdekek ütközése rendszerint igencsak nehézzé teszi. Számos tényezőt kell számításba venni – nemcsak magát a szoftvert, hanem a felhasználói kört is, továbbá ellenőrizni kell az adott vállalat hitelességét, a terjesztési csatornáit pedig elemezni kell. A csalárd vállalkozások és termékeik (hamisított vírusirtó és kémprogram-elhárító szoftverek) gondosan kidolgozzák a megtévesztés minden apró részletét – weboldalaik professzionális megjelenésűek, termékeik pedig a valódi vírusirtó szoftverek jegyeit is magukon viselik. Ezeken a weboldalakon rengeteg hamisított Gyakori kérdések-lista látható a nem létező felhasználóktól és másoktól származó „kedvező" visszajelzésekkel és színlelt tanúságtételekkel együtt.

Hamis antivírusok más aspektusból

Nem szokatlan a legálisan működő webhelyek fertőzött állapota, ha azok HTML-kódjába Iframe-átirányításokat szúrtak. Az Iframe-elemek a támadó szerverére mutatnak, amely a kártékony kódot szolgálja ki. A telepítők/letöltők a trójaiak összes funkciójával rendelkeznek, így eddig minden meglehetősen világos, és nem kell sok időt szánni a besorolás megállapítására. Ezek a kódok általában a trójaiak vagy a trójai letöltők kategóriájába tartoznak. Ez azonban nem érvényes a trójai letöltő által éppen letöltött szoftverre, amely besorolása szerint reklámprogram, kémprogram vagy kéretlen alkalmazás lehet. Miért? Az ok, hogy a kényszerített telepítés ellenére rendszerint megjelenik egy végfelhasználói licencszerződés, amely a hamisított szoftverre vonatkozó összes szempontot tartalmazza, és amelyet a felhasználó ténylegesen jóváhagy. Így a program telepítése valóban a felhasználó hozzájárulásával megy végbe. Természetesen a licencszerződés semmit sem mond a terjesztés eszközeiről, maguk a szoftvergyártók pedig tagadják, hogy közük lenne a terjesztési csatornákhoz. Mindezt több-kevesebb sikerrel teszik, az egyes esetektől függően. Ilyen esetben azonban tanulmányozni kell a szoftverek minden apró jellemzőjét és részletét. A legfontosabb tulajdonságok: a támadó képesség, a rendszer stabilitására gyakorolt hatás, a biztonság és az integritás, valamint az, hogy a szoftver szerzői milyen mértékben próbálják összezavarni a kódokat, kivédeni a felismerést stb. Manapság száz és száz ilyen hamis alkalmazáscsaládot regisztrálnak – színlelt jogszerűségük szintje és minősége pedig a gyerekes, jelentéktelen kísérletektől a komoly, szakszerű megjelenést nyújtó megoldásokig terjed.

Ezeknek a szoftvereknek a születése és az elterjedésükre utaló előjelek 2005-re keltezhetők, amikor a WinAntivirus és más hasonló családok megjelentek. A hamisított alkalmazások (különösen a vírusirtóknak) Win vagy az Antivirus szavakkal kezdődő nevei nyilvánvaló okokból hamar népszerűek lettek. Ez természetesen idővel átalakult, és a vírusvédelmi adatbá-

Juraj Malcho **(ESET) előadását Budapesten is meghallgathattunk a Magyar Villamosmérnök- és Informatikus-hallgatók Egyesülete (MAVE) szervezésében 2009 őszén tartott Ethical Hacking Workshop 2009 keretében. Amikor egy vírusszakértő úgy dönt, hogy nem tetszenek neki valamelyik szoftver egyes elemei, talán mert nem biztonságosak, kéretlenek vagy problematikusak – akkor jó eséllyel igaza lehet**

From: support [mailto:support@emediacodec.com]
Sent: Wednesday, April 12, 2006 4:28 PM
To: xxx
Subject:
Hello xxx.
We are eMediaCodec support team. we would like to know why your software NOD32 detects our codec as virus "Win32/TrojanDownloader.Zlob.II".
Our emediacodec is provided with Terms and Conditions located at http://www.emediacodec.com/terms.html where we describe in details what is the codec itself. We do tell surfers about what being installed on their computers.
We would very appreciate if you remove our eMediaCodec from your virus list.
Thanks

Régebben csak elvétve fordult elő, hogy a kártevőket, kéretlen reklámokat terjesztő cégek még reklamálljanak is – a képen a semmire sem jó eMediaCodec terjesztői próbálkoznak. Természetesen bármennyire szakszerűtlennek is tűnik ez a levél, mégis kétségeket és némi bizonytalanságot ébreszt, így szükségessé teszi a probléma ellenőrzését

From: xxx [mailto:xxx@pornmagbucks.com]
Sent: Wednesday, July 12, 2006 3:53 PM
To: xxx
Subject: Attn: AV Research Team. Urgent.
Dear Research Team,
I am writing to you on behalf of DIGITAL MEDIA DEVELOPERS.
Why does your AV detec our software as "Win32/TrojanDownloader.Zlob.UR"? There must be mistake. Our software has License Agreement on the very first page of install wizzard, the product itself does not include any trojan or any software to download anything secretly, furthermore all ad components are downloaded with user permission and without any secret. If you have a look at our product more closely, you will find that it can be easily removed from PC with the help of Add or Remove Programs menu.
Could you please explain your policy on naming and detecting our software as "Trojan"?
Here is the URL of our product
http://www.pornmagpass.com/download/pornmagpass_ver1.107.exe
Best Regards,
xxx

Amikor a farok csóválja a kutyát – a széles körben hírhedt Zlob készítői arra hivatkoznak, hogy nem is kártevő az, amit a víruskereső annak ítél. A későbbiekben azután még érkezett néhány megismételt panasz, ám végül a Zlob mögött álló csoport a trójaiak új hullámának olyan nagy tömegű létrehozásába kezdett, hogy felismerte, ebben a reklámlós irányban a legkisebb esélyük sincs a sikerre

Subject: NOD32 detects our products as malware
Date: 21 Aug 2006 10:21:51 -0500
From: xxx@winsoftware.com
To: xxx

I am contacting you on behalf of WinSoftware Company.
Recently our Quality Assurance Department discovered that parts of our product, WinAntiVirus Pro 2006, were added to your anti-malware database, and are currently being detected as malware.
WinSoftware believes this may have been done inadvertently; nevertheless this has a big impact on our Company's reputation and on customer satisfaction level. WinSoftware, therefore, requests that you remove these product from your base no later than fourteen (14) days from receipt of this notification.
Please confirm receipt of this message.

Best regards,
xxx
Senior Vice-President, Legal Compliance
WinSoftware Ltd.

Ennyire már a rinocérosz bőre sem lehet vastag: még a hamis antivírus készítők is követelőznek, hogy az adatbázisból 14 napon belül távolítsák el a WinAntiVírus Pro 2006 detektálását. A hosszadalmas Zango-per óvatossá tette az antivírus cégeket, bár szerencsére győzött az igazság

Aggodalomra adnak okot a számok. Három év alatt megháromszorozódott az ilyen reklamációs esetek száma. Biztosra vehető, hogy ezek száma tovább fog emelkedni, és csak reménykedhetünk abban, hogy nem exponenciálisan

zisok szervezése és gyűjteményei is vállalatról vállalatra változhattak, ami újbóli besoroláshoz vezethetett.

Reklámprogramok – nos, kinek jó ez?

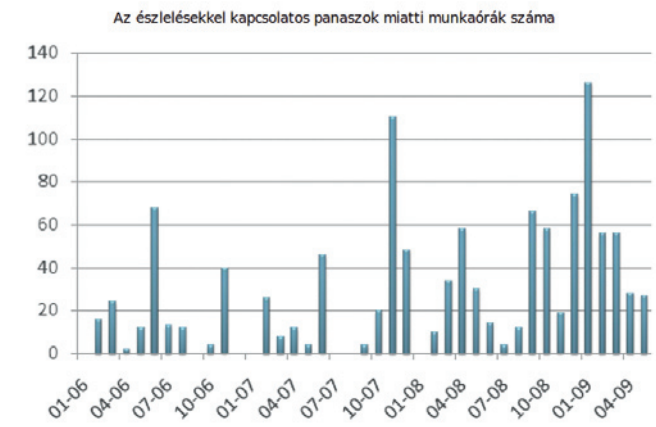
Minél agresszívebb egy szoftver, annál könnyebb a besorolását megállapítani. Másfelől az agresszivitás szintjének növekedésével az észlelés megvalósításának összetettsége is arányosan nő. Mint már utaltunk rá, a döntési eljárás gyakran jóval több időt emészt fel, mint a felismerési minták létrehozási folyamata. A valódi vírusirtó és a problematikus kártevő ténylegesen két, egymással szemben álló szoftver, amelyeknek a rendszeren való jelenlétét a jóváhagyott végfelhasználói licencszerződések biztosítják (amelyeket a felhasználó gyakran a tudtán kívül és elolvasás nélkül fogadott el).

A gyanús szoftvereket gyártók valódi törekvésének szemléltetésére idézzük fel a számos múltbeli jogi esetek egyikét. 2007-ben a Zango nevű (180Solutions néven is szereplő), hírhedt reklámprogram-terjesztőként ismert vállalat vádat emelt a Kaspersky Lab ellen, kifogásolva, hogy az igazságtalanul tiltja le a Zango által forgalmazott szoftvereket. Ezenközben a Zango azt is állította, hogy a Kaspersky sérti a jó hírnevét, és gátolja az üzletmenetét. A bíróság első döntése igen kedvezően hangzott, mivel alapvetésként megállapította, hogy egy interaktív számítógépes szolgáltató (a tartalomszűréssel összefüggésben) jogosult az olyan anyagok terjesztésének az akadályozására, amelyeket az ügyfelei kifogásolhatónak tartanak. A történet ezzel még nem ért véget, mert további fellebbezések következtek. A végső jó hír azonban 2009 áprilisában az volt, hogy a Zango a pert elvesztve, bejelentette az üzleti életből való visszavonulását.

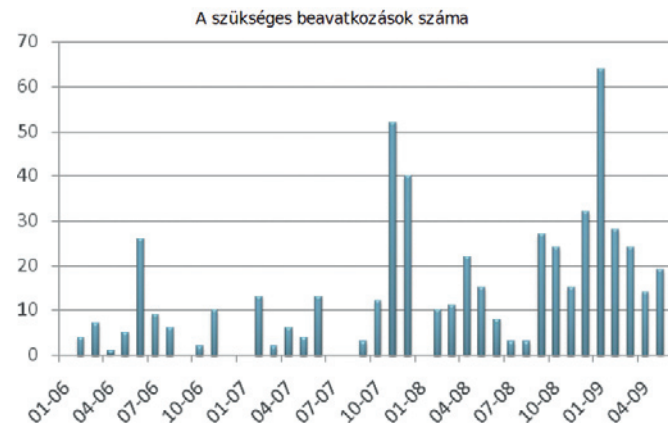
Bármely (legalábbis a törvény előtt) jogosulatlannak bizonyuló észlelés a befektetett erőforrásokat és az időt illetően igen sokba kerülhet a vírusvédelmi vállalatnak – akinek küldetése, hogy meghallja ügyfelei kérését, és megvédje azok számítógépét a nemkívánatos szoftverektől. Általában senki sem kíván reklámprogramokat tárolni a számítógépén, csak ha nincs tisztában a következményekkel, illetve azzal, hogy ezekkel a programokkal számítógépe hatékonyságát és stabilitását veszélyezteti. De azért van ez alól kivétel is, nézzünk hát egy példát.

Amitől a nyugati szoftvercégek szívbajt kapnának

A Kínával, mint a világ egyik legnagyobb reklámprogram-előállítójával kapcsolatos összes problémát félretéve megállapíthatjuk, hogy a kínaiak számos területen – a kultúrától a technológiai fejlődésig – igen tehetségesek. Köztudottak Kína problémái a szoftverkalózkodással, valamint az olyan programokkal kapcsolatban, amelyek egyéb funkcióik mellett különféle hirdetéseket jelenítenek meg. Ezek a reklámprogramok a víruselemzők mindennapi rémálmának okozói. Az alaposabb kutatás azonban feltárja azt is, hogy ez a reklámprogram-jelenség csak az egyik okozata a bonyolult kínai szoftverhasználati szokásoknak. A probléma része az úgynevezett „zöld" szoftver. A zöld szoftver általában olyan önálló csomagot jelent, amelynek használatakor nincs szükség a program telepítésére, elegendő azt letölteni, majd duplán rákattintani, és máris megjelenik a képernyőn például az Adobe Photoshop CS4 teljes verziója. A kicsomagolás előtt természetesen a szoftver feltörése és módosítása, majd „feljavítása" szükséges, hogy megoldjuk az összevissza való telepítésből adódó nehézségeket, azután a licencaktiválás következik. A sorozatszám vagy a licenckulcs miatt fölösleges aggódni: ezekhez ugyanis könnyen hozzá lehet jutni azon a több tucatnyi vagy talán több száz webhelyen, amelyek ezeket a zöld csomagokat kínálják. Egyesek számára a zöld szoftver azonos az ingyenessel, amely ráadásul olykor még honosított is. A „zöld" webhelyek összes anyaga gondosan rendezett, így bárki könnyen hozzájuthat kedvenc alkalmazásának a másolatához. Az ismert kínai feketepiac „erede-



A detektálásokkal kapcsolatos reklamációk kezelésére 2009-ben már sokkalta többször kellett időt fordítani, mint pár évvel ezelőtt. Juraj Malcho adatai az ESET laborjára vonatkoznak, de ezzel a problémával minden antivírus labornak meg kell küzdenie



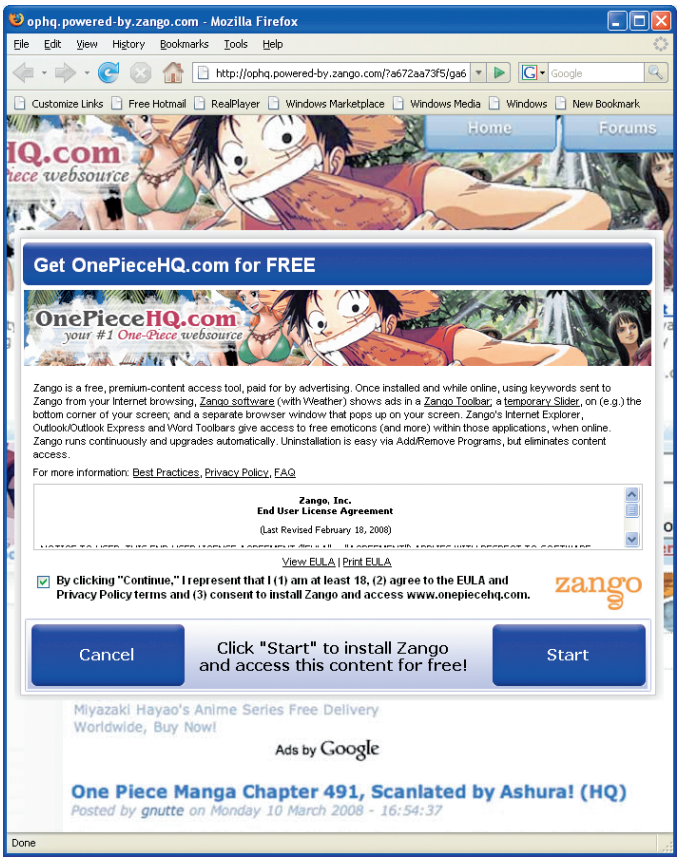
A sok panasz, az egyre több kérelem sok extra munkaórát igényel, minden reklamáló beadványt alaposan, illetve meggondoltan kell kezelni, és csak a 100 százalékig biztos eseteket lehet könnyen rövidre zárni, ellenkező esetben elindul a végeláthatatlan pereskedés

ti” CD-ihez és DVD-ihez hasonlóan a zöld webhelyekről származó eredeti és feltört változatok között is gyakran igen nehéz különbséget tenni. Ezért sok magánszemély és üzleti vállalkozás futtat illegális szoftvereket anélkül, hogy tudna róla, még ha ez éles ellentétben áll is az elveivel. Az ilyen környezetben a szoftvergyártók kénytelenek termékeiket ingyenesen forgalomba hozni – legfeljebb némi reklámot helyeznek el bennük. De ezzel szemben mi a helyzet a világ többi részével? Az emberek végletesen allergiásak még a reklám gondolatára is, ügyes reklámblokkolókkal és szűrőkkel rendelkeznek, továbbá minden olyan alkalmazás eltávolítását megkövetelik, amely reklámot tartalmazhat. Akkor hát mi is pontosan az a reklámprogram? Vajon menynyire képes az átlagos felhasználó különbséget tenni a „jó” és a „rossz” reklám között, és tud-e helyesen választani? Ez a probléma komoly fejfájást okoz a víruslaborokban szerte a világon.

A nemzetközi helyzet fokozódik

Elég gyakran megesik, hogy ezeknek az alkalmazásoknak a telepítése kétes csatornákon keresztül történik, amelyek ellenőrzésére a felhasználók nem feltétlenül képesek, így számítógépükön a szoftver valójában kéretlen tartalomként jelenik meg. Napjaink kényes témája az online kaszinó. Rengeteg ember akar játszani és nyerni – a játékban pedig valódi pénz forog. A kapcsolódó alkalmazások – nem kötelezően – szolgáltathatnak hirdetéseket is. Elég gyakran megesik, hogy bizonyos időközönként adnak reklámot, máskor meg nem. Az ezekkel kapcsolatos fő probléma az, hogy a belépéshez a nyílt terjesztési modellt használják, és minden sikeres telepítés után jutalékot adnak. A jelenlegi „botnet-korszakban” ez a modell a gyors és könnyű pénzkereset esélye révén komoly visszaélésekre adhat és ad is alkalmat, így bevett gyakorlat, hogy ezeket az alkalmazásokat levélszemét, sőt trójaiak segítségével is terjesztik. Ennek eredményeként egyre több pénz folyik a bűnözők zsebébe, miközben a szoftverek egyre több számítógépre telepítik magukat – a felhasználók jóváhagyása nélkül. Mióta ezek a cégek az online kaszinókkal üzletelnek, a pénzzel való kapcsolatuk igen szorossá vált, és nem haboznak a vizsgálatok beszüntetése érdekében felhívásokkal támadni a vírusvédelmi vállalatokat, még azon az áron is, ha perrel végződik az ügy. Így a víruselemzők munkája új és váratlan dimenziójú tevékenységgé alakult, a problémák megoldása pedig rendkívül időigényes elfoglaltsággá vált.

Aki pókerezni szeretne, annak ez nem zavaró, hanem még örül is neki. Aki viszont nem kártyázna online, annak kéretlen reklám. Akkor most hogyan lehet ezt besorolni? Nem véletlen, hogy a „Potenciálisan Veszélyes Alkalmazások” és a „Kéretlen Alkalmazások” kategória kialakult, és az is szándékos, hogy ezek keresésének nincsen a telepítéskor alapértelmezett állapota, magának a felhasználónak kell döntenie



Egy per, amiről akár írhatna is valaki egy könyvet. *Eugene Kaspersky* cégét a Zango nevű online reklámcég beperelte az USA-ban arra hivatkozva, hogy a kártevőként való detektálás rontja az üzletmenetüket és a jó hírnevüket. Az évekig tartó per vége a Zango (korábban 180Solutions) csődjével és az antivírus cég győzelmével zárult

Mi lesz itt megfizetve?

Murphy szerint ha már nem romolhatnak tovább a dolgok, akkor tovább romlanak. Sajnos senkit nem tudunk azzal vigasztalni, hogy a cikkben leírt esetek egyediek, és soha többet nem fognak megismétlődni. Ennek pont az ellenkezőjétől lehet tartani: ezek az ügyek nem kerülhetők ki, és egyre gyakrabban, egyre több kétes szoftverrel kapcsolatosan lehet majd ilyenre számítani. Egy bírósági perben pedig lehet reménykedni, lehet az igazság diadalát várni, de a sokszor évekig tartó, sok idegeskedéssel járó procedúrák eredményét sohasem lehet teljes bizonyossággal előre megjósolni.

Olyan ez, mint egy teniszmeccs, amelynek az eredménye végig nyitott, s a mérkőzés csakis a kézfogással ér véget.

***

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

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

KAPCSOLÓDÓ WEBOLDALAK

32 millió forint bevétel hetente: **hopp.pcworld.hu/6425**
Kiütötték a hírhedt reklámprogramot: **hopp.pcworld.hu/6556**
ESEt Threat Blog - Is There A Lawyer In The Lab?: **hopp.pcworld.hu/6557**