A 32 LOVAS FOGAT

Totális ellenőrzés

A vírusok varázslatos világa című sorozatunk első részében arról lesz szó, hogyan ellenőrizhetünk egy gyanús állományt egyszerre többféle vírusirtó segítségével. Emellett arra is fény derül, miként jutnak feldolgozandó vírusmintákhoz az antivíruscégek laboratóriumai.

Mindenkivel előfordulhat, hogy gyanú ébred benne egy számítógépes állománnyal szemben. Mintha azóta lenne lassú a gépem, amióta azt a fránya levélmellékletet megnyitottam! Mintha azóta lennének rendszeres lefagyások, hogy azt a bizonyos alkalmazást telepítettem! Lehet, hogy az általam használt vírusirtó egy tiszta állományra riaszt, vagy talán csak vakriadó? Nem merem megnyitni a levélben kapott mellékletet, hátha fertőzött, de vajon hogyan győződhetnék meg róla?

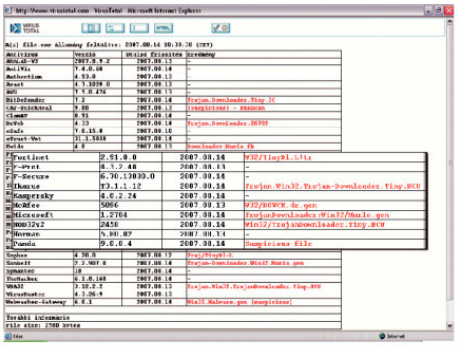
Ilyen és ehhez hasonló kérdések esetében jól jönne egy olyan alkalmazás, amely csatasorba állítja a piacon kapható antivírusprogramok színe-javát, és elvégezne számunkra egy alapos vizsgálatot egy adott gyanús fájl esetében. És ez nem vágyálom, ez már valóság! Egy spanyol weboldal, a VirusTotal már évek óta kínálja ezt a lehetőséget a felhasználók millióinak. Az amerikai *PC World* magazin a „2007. év 100 legjobb terméke” díjat adományozta a VirusTotalnak a biztonsági weboldalak kategóriában. Gyanús állományok vizsgálatára mi is jó szívvel ajánljuk ezt az igen hasznos oldalt.

VirusTotal, a biztos pont

Ez év júliusától megújult külsővel és kibővített palettával jelentkezett a VirusTotal ingyenes online vírus- és kártevővizsgáló szolgáltatása. A VirusTotal egy független IT-biztonsági laboratórium, a Hispasec Sistemas által kifejlesztett ingyenes szolgáltatás, amely számos parancssori antivírusmotort alkalmaz, és ezeket a fejlesztők által hivatalosan kibocsátott vírusadatállományokkal rendszeresen frissíti. A keresőmotorok készítői között olyan nagy neveket találunk, mint az ESET NOD32, F-Secure, Frisk, Kaspersky, McAfee, Panda, Symantec és még sokan mások; összesen 32 vírusvédelmi alkalmazás neve sorakozik a listán.

Ám amellett, hogy küllemében átalakult az oldal, számos egyéb hasznos funkcióval is gazdagodott a kínálat. A megvizsgálandó mintaállomány beküldése nemcsak a webes felületen történhet, hanem elektronikus postán is eljuttathatjuk azt a VirusTotalnak. Ez utóbbi esetben levélben kapjuk meg az ellenőrzés eredményét. Emellett akár titkosított csatornán (SSL) is lehetőségünk van elküldeni a vizsgálandó mintát.

További hasznos beállítási lehetőség, hogy a beküldött állomány esetében nyilatkozhatunk úgy is, hogy a vizsgálandó fájl bizalmas természetű, nem publikus. Ebben az esetben a VirusTotal nem küldi tovább elemzésre gyanú esetén a projektben részt vevő antivíruscégek víruslaborjaiba – hiszen az oldalnak ez is az egyik nagy haszna a fejlesztők szempontjából.



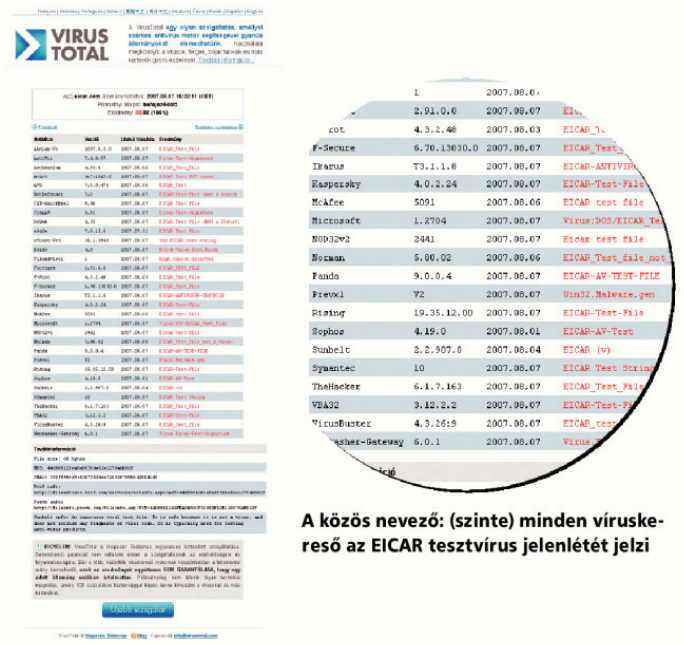
Egy adott vírust vizsgálva látható, hogy sokan nem is találják meg azt, a találatokat átböngészve pedig felfigyelhetünk arra, hogy a különféle termékek többnyire nem egységesen, hanem összevissza nevezik el azt

Magyarul beszél, és sírva vigad

Bővült a webes felület nyelvi támogatása is: a korábbi angol és spanyol mellé bekerült a német, cseh, lengyel és a magyar nyelv is. A magyarítást nekem volt szerencsém elkészíteni, ebben hihetetlenül rugalmas partnerekre találtam bennük, név szerint is hadd említsem meg *Francisco Santost*. Az ötlet felvetése után felajánlottam a segítségemet e-mailben, és néhány gyors levélváltást követően – alig másfél nap múlva – már ki is kerülhettünk a választható nyelvek közé. Azóta is rendszeresen látogatom az oldalt, és olybá tűnik, valóságos hullámot indítottunk el a fordításokkal: azóta már a svéd, portugál, olasz, kínai nyelv (alap- és tajvani változat) is felkerült a palettára.

Számok, számok...

Az új weboldalon számos statisztikai adatot is nyomon követhetünk az eddigi Top 10-es kártevőlista mellett: ilyen a szolgáltatás kihasználtságát a legutóbbi 24 órában jellemző grafikon, a különféle víruskereső motorok frissítési adatai. Találunk tortadiagramot azon kártevők számáról is, amelyeket minden résztvevő kivétel nélkül felismert, illetve az olyan fertőzött fájlokról, amelyeket viszont legalább egy keresőmag észlelt.



A közös nevező: (szinte) minden víruskereső az EICAR tesztvírus jelenlétét jelzi

A vírusirtót nem pótolja!

A weboldal készítői fontosnak tartják leszögezni: a VirusTotal nem helyettesítheti a számítógépre telepített egyedi vírusvédelmi szoftvert, használatával csak egy kiválasztott állományt vizsgálhatunk. A felhasználó rendszerének állandó vírusvédelmére a módszer nem alkalmas. Bár a több, különféle víruskereső motornak köszönhetően a felismerési arány kiemelkedő, ezek az eredmények együttesen sem garantálják, hogy egy adott állomány valóban ártalmatlan. Pillanatnyilag nem létezik olyan technikai megoldás, amely 100 százalékos biztonsággal mutatná ki a vírusokat és más kártevőket. Vigyázzunk, hogy ne váljunk félrevezető reklámok áldozatává, és legyünk gyanakvók, ha valaki netán 100 százalékos biztonságot ígérne!

Tanulságok

Igen érdekes hozzászólások születnek a VirusTotal blog szekciójában. Következzen most innen néhány hasznos és tanulságos gondolat!

Általánosságban kijelenthetjük, hogy napjainkban minden vírusvédelmi terméknek vannak különféle észlelési problémái az elszaporodott kártevők elképesztően nagy száma miatt. Hasonlóképpen előfordulhat olyan eset, hogy egy termék egyedül észlel egy vadonatúj mintát – például jó minőségű heurisztikájának köszönhetően, vagy mert elsőként készítették el az adott kártevőre a vírusadatbázis-frissítést. Ez az oka annak, amiért egy ilyen eset nem alkalmas arra, hogy egyetlen minta alapján bizonyítsa egy termék (ideiglenes) fölényét a többivel szemben.

Nem győzzük elégszer ismételni, hogy a VirusTotal nem terepe egy antivírus-összehasonlító elemzésnek, hanem olyan eszköz, amely párhuzamosan több AV-programmal is képes ellenőrizni gyanús mintákat, és segíti a különböző víruslaboratóriumokat azzal, hogy továbbítja szá-

KAPCSOLÓDÓ WEBOLDALAK

A VirusTotal magyar honlapja: www.virustotal.com/hu/

VirusTotal blog: blog.hispasec.com/virustotal/

Jotti online kártevő-azonosító szolgáltatása: virusscan.jotti.org

ESET Online Scanner, az online NOD32 kereső: www.eset.com/onlinescan/

Panda NanoScan online kereső: www.nanoscan.com

Trend Micro Housecall online kereső: housecall65.trendmicro.com

A Symantec Security Check online kereső: security.symantec.com/sscv6/

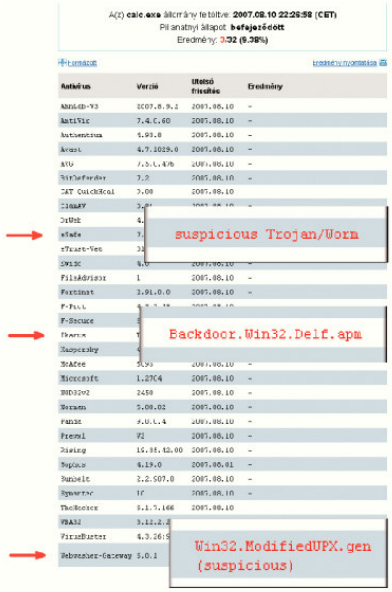
EICAR tesztvírus: www.eicar.com

mukra azokat a kártevőket, amelyeket képtelenek voltak észlelni.

Azoknak, akik arra használják a VirusTotal oldalt, hogy antivírus-összehasonlító elemzéseket végezzenek, tudniuk kellene, hogy ezzel hibás módszert választanak, több okból is – lássuk a legnyilvánvalóbbakat!

– A VirusTotalban szereplő keresőmotorok parancssori programok, tehát semmiképpen sem hasonlíthatók össze ennek alapján egy telepített munkaállomáson futó programcsomag-változattal: például számos esetben egy telepített programcsomag viselkedéselemzési technikát hajt végre, és mindeközben támaszkodik a tűzfalas védelemre, ezzel csökkentve a lehetséges belépési pontokat, és mérsékelve a fertőzést.

– A VirusTotalban a munkaállomás-alapú megoldások egyidejűleg működnek a komplett hálózati alapú (tűzfal, átjáróvédelem stb.) megvalósítá-



Ebben az állományban nincs vírus, hiszen a Windows Calc.exe-t tömörítettük az UPX segítségével – mégis a résztvevők közel 10 százaléka minden ok nélkül riaszt

sokkal; az utóbbi csoportban található heurisztikák agresszívebb és paranoiásabb működésűek lehetnek, mialatt a hamis riasztások (false positive) száma kevésbé látványosan jelentkezik. Emiatt egyszerűen nem tisztességes összehasonlítani e két csoportot.

– Egyáltalán nem könnyű feladat egy megbízható és hiteles antivírus-elemzés megvalósítása; ez nagyszámú reprezentatív és hiteles vírusmintát igényel, amelyek közt egyaránt szerepelnek az úgynevezett vadon élő (In The Wild) kártevők, valamint a víruslaboratóriumi (Zoo Collection) egyedek, a téves riasztást adó, valamint a sérült, korrupt végrehajtható fájlokkal egyetemben. Emellett a munkaállomás-alapú új vírusellenes technikák bevezetésére való tekintettel az volna a korrekt eljárás, ha minden termékkel valós környezetben ellenőrizhetnénk az adott mintát – ez lenne az igazi próbatétel a programok valós észlelési és megelőző képességeire. Mindmáig nincs egyetlen olyan antivírusteszt, amelyben ezek az alapelvek maradéktalanul érvényesülhetnének.

Kísérletezzünk és gondolkozzunk!

A fenti címet Öveges professzor egyik könyvének címéből kölcsönöztük; kísérletezzünk mi is egyet: létezik egy úgynevezett EICAR tesztvírus, amelyet egy nemzetközi megállapodás szerint minden víruskereső felismer, ezzel szokták tesztelni a vírusvédelmi programokat. Természetesen ez nem egy fertőző állomány, hanem egy 68 bájt hosszú, .COM kiterjesztésű fájl, amelyet a **www.eicar.com** oldalról lehet letölteni. Ha ezt megvizsgáljuk a VirusTotal oldalon, meglepve tapasztalhatjuk, hogy szabvány ide, megállapodás oda, a Prevx1 „Win32.Malware.gen” néven egy generikus Windows alatt futó kártékony programnak jelzi, míg az összes többi résztvevő – helyesen – EICAR tesztvírusnak mutatja. Jöjjön a kísérlet második része: válasszuk ki a Windows Számológép alkalmazást (\Windows\System32\Calc.exe), és vizsgáltassuk meg. Az eredmény, ahogy vártuk, 32-ből 32 tiszta állapotot mutat. Ha most ugyanezt a Calc.exe állományt az UPX (Ultimate Packer for eXecutables) program segítségével tömörítjük, és az újonnan keletkezett ártalmatlan, de UPX tömörítésű állományt vizsgáljuk a VirusTotallal, meglepetésben lesz részünk: három kereső is, az eSafe, az Ikarus és a WebWasher-Gateway fertőzöttnek jelzi azt, minden alap nélkül.

Ha a rendszer netán pillanatnyilag túlterhelt lenne, az e-mailben elküldött minta eredményéről válaszlevélben kapjuk meg az értékelést

Alternatíva és online keresők

Létezik egy másik, szintén ingyenes oldal is a kártevőminták vizsgálatára: itt azonban lényegesen szerényebb a rendelkezésre álló keresőmotorok száma. A Jotti holland weboldalon szintén lehetőség van tetszőleges fájl feltöltésére és vizsgálatára, és ezt követően kapunk egy táblázatos jelentést az eredményről, hogy mely keresőmagok ítélték tisztának, illetve melyek fertőzöttnek a vizsgált mintát.

Mint írtuk, a VirusTotal és persze a Jotti sem alkalmas gépünk vírusellenőrzésére, csak az elküldött gyanús minta kivizsgálására. A normál, telepíthető keresők mellett léteznek úgynevezett online keresők is, amelyek az adott vírusvédelmi alkalmazás installálása nélkül képesek végigvizsgálni számítógépünket. A megoldások többségében a detektálásra szorítkoznak, mentesítést nem végeznek. A neves antivírusgyártók közül többek közt az ESET NOD32, a Panda Security, a Symantec és a TrendMicro nyújtanak ilyet. Ez a módszer mindkét fél számára hasznos: a géptulajdonos egy alternatív megoldással is megbizonyosodhat vírusmentes állapotáról, míg a gyártók ily módon pontos fertőzési statisztikákhoz jutnak a még hatékonyabb védekezéshez.

Dexter laboratóriuma

A víruslaborokban történő feldolgozás és az adott kártevő felismerését biztosító vírusaláírás-bővítéshez mintákra van szükség. Ezek egy része az adott gyártó saját ügyfeleitől érkezik kivizsgálásra. Vannak aztán a levelezőszervereken elhelyezett vírusvédelmi megoldások, ahol a gyanús fájlokat tárolják, majd elemzésre továbbítják őket, végül pedig az úgynevezett honey-potok, azaz mézesbödön típusú csalihelyek is begyűjtik azokat. A fent említett VirusTotal ugyancsak egy ilyen lehetséges mintaforrás, amely hasznosan segíti az antivírusgyártókat naprakészségük folyamatos fenntartásában azzal, hogy az általuk fel nem ismert, de a többi résztvevő által detektált mintákat rendszeresen átadják számukra részletes elemzésre.

***

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

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 magyarországi képviselete