Az antivírus nem lift

Bemutató – Írta: **Csizmazia István [Rambo]** | 2013-08-22 12:53

A vírusirtó programok tesztelése, összehasonlítása már hosszú évek óta folyik. Ezek célja pedig kettős: információhoz juttatni az antivírusok fejlesztőit, és tájékoztatni, segíteni a választásban a felhasználókat.

Miről NEM szól az igazi műszaki tesztelés?

Mi most a műszaki tesztekről fogunk beszélni, de ezektől függetlenül léteznek például különféle számítástechnikai kiadványok, népszerű magazinok által végzett házi tesztek is, ahol olyan szempontok is szerepelhetnek a súlyozott eredményekben, mint hogy az adott szerkesztő szubjektív véleménye szerint szép-e és logikus felépítésű-e a menü, tetszetős pasztell színek szerepelnek-e a programban, hány darab frissítés érkezik naponta, vagy mennyiért vásárolható meg egy adott termék a viszonteladóknál. Rosszabb esetben 10-15 saját kártevő mintával is „tesztelik” a mezőnyt, majd az olvasóközönségnek győztest és sorrendet hirdetnek. Természetesen a gyártók az ilyen helyzeteket „értékén kezelik”, ám ezekre a visszajelzésekre is gondosan odafigyelnek, sőt meg is szívlelik, ha sokan úgy gondolják, hogy például baj van a menü felépítésével, nem logikus szerkezetű vagy túl bonyolított.

Előfordulnak aztán olyan esetek is, hogy például valaki azzal érvel, azért nem jó szerinte egy vírusirtó, mert egy adott, általa a VirusTotalra feltöltött mintát az nem érzékelt. Tudni kell, hogy a VT oldalán parancssoros programok futnak, így az, hogy egy adott mintát vagy kártékony oldalról érkező fenyegetést a valódi gépre feltelepített termék észlelne-e vagy sem, nem tudhatjuk meg kizárólag ebből az eredményből. A később részletesebben is ismertetésre kerülő, úgynevezett komplex védelmi típusú tesztek jellemzik legjobban ezt a bizonyos képességet, ahol a védelem minden rétege részt vesz a folyamatban, és például egy komplett internetbiztonsági csomagon belül a viselkedéselemzés „beszélgethet” a tűzfal modullal, a kártékony linkeket szűrő komponenssel vagy a felhőalapú reputációs adatbázissal. De hangsúlyozzuk, egyetlenegy minta ottani látszólagos nem észlelése akkor sem minősítheti messzemenően egy termék tudását, képességeit. A valódi és alapos műszaki tesztelés egy teljesen más kategória, ez utóbbiról szól majd ez a cikk is.

John Hawes (Virus Bulletin) az egyik olyan szakember, aki valószínűleg a legtöbbet tud a különféle antivírus tesztekről a világon

Ezek a vizsgálatok folyamatosan zajlanak, egy-két havonta adják ki például az AV-Test, AV-Comparatives értékelését vagy éppen az aktuális Virus Bulletin teszteredményeinek összefoglalóját. Ilyenkor rendre azt kérdezgetik az emberek, miért van, hogy különböző eredmények születnek ezekben, honnan tudjuk, melyiknek higgyünk? Mitől jobb vagy rosszabb egy tesztelési eredmény, mint a másik, és mennyire hasznosak ezek, vagy éppenséggel elfogultak? Ezekre a felvetésekre őszintén szólva nem könnyű válaszolni. Következzen hát néhány hiánypótló értékes és praktikus gondolat, ebben rengeteget támaszkodunk John Hawes (Virus Bulletin) e témájú összefoglalójára ahhoz, hogy némileg reálisabban láthassuk a különféle antivírus tesztek súlyát, jelentőségét.

Melyik a legjobb vírusirtó?

Bemelegítésül mindenkinek javasoljuk elolvasni a Prohardver fórum **#1-es számú indító összefoglaló bejegyzését**, "Melyik a legjobb vírusirtó?" címmel. Azonkívül, hogy ez minden szempontból alaposan körüljárja a kérdéskört, megemlíti természetesen a teszteket is. Ezek közül a független és az **AMTSO** (erről később szót ejtünk) szakmai irányelveknek megfelelő metódusok szerint dolgozó laboratóriumok eredményei számítanak a legtöbbet, ilyen például a **www.av-comparatives.org**, a **www.av-tests.org**, és a **www.virusbulletin.com**. Innen már ugorhatunk is a mai témára.

Az antivírusok tesztelése egy szerfelett összetett és bonyolult folyamat, és ezek minősége nagyban befolyásolja azt, mennyire kapunk reális és hasznos képet ahhoz, hogy tisztán lássunk. Először is néhány alapvető információt nem árt tisztázni. Összehasonlító vagy

tanúsítvány megszerzéséért folyik az adott teszt? Ez a két legfőbb típus ugyanis, ahol az első, az összehasonlítás esetében bedobnak a ringbe egy tucat vírusirtót, remélhetőleg gondoskodva a tisztességes és egyenlő versenyfeltételek megteremtéséről, majd különböző mutatók alapján keletkezik egy győztes és egy sorrend. Ezzel szemben a tanúsítvány megszerzéséért zajló küzdelem esetében nem a rangsorolás a cél, hanem rögzített és szabványos feltételek szerinti vizsgálatokon elért eredmények alapján az adott körben minden sikeresen vizsgázó termék megkapja a minősítést. A valóságban aztán ezenfelül léteznek a két modell ötvözéséből származó tesztelési metodikák is, többek közt a Virus Bulletin is erre törekszik.

Nézzük akkor először, mit jelent, ha egy tisztán a minősítésért folyó tesztet végeznek. Ilyenkor általában minimális vagy semmilyen információnk nincs arról, pontosan mi zajlik a háttérben. A tesztelők viszont folyamatosan együttműködnek és kommunikálnak a gyártókkal, és általában az egész procedúra tartama alatt biztosítják a konzultációt. A hibridnek nevezett ötvözött módszer esetében nyitottabban zajlik mindez, megismerhetőek a résztvevők eredményei, de vissza is hívhatóak azok a versenyzők, akik esetleg túlságosan rosszul veszik az akadályokat. Azt is meg kell említeni, hogy sajnos vannak olyan tesztlaborok is, ahol nyomást próbálnak gyakorolni a gyártókra, például esetleges gyengébb szereplésük részleteit csak egy jelentős összeg - úgynevezett tanácsadói díj - befizetése után ismerhetik csak meg. Erre példa az AMTSO szervezetből **2010-ben kizárt NSS Labs**, amely komoly summáért árulta a részletes teszteredményeket, sőt 5000 dollárért már a tesztelésbe is engedett volna beleszólni. Szerencsére nem ez az általános, így a legtöbb esetben tisztességes és legitim tesztelést biztosítanak a gyártóknak, és ellátják őket bőséges információkkal ahhoz, hogy ellenőrizni, diagnosztizálni és javítani tudják a felmerülő problémákat.

A liftek falán általában megtaláljuk a minősítő alumínium TÜV plakettet. Ez nem azt jelenti, hogy ez a lehető legjobb termék a világon, hanem mindössze annyit jelez, hogy a biztonsági előírásoknak megfelelően tesztelték

A minősítésekért folyó küzdelem, és ezek eredménye a fejekben is okozhat némi zűrzavart, hiszen meglepően sok ember tévesen azt hiszi, egy ilyen minősítő embléma azt jelenti, az adott termék a lehető legjobb a világon. Például ha beszállunk egy liftbe, és a falon ott találjuk az alumínium TÜV plakettet, ez mindössze annyit jelez, hogy a biztonsági előírásoknak megfelelően tesztelték és kiállta a próbát. Érthetőbben, a minősítések megszerzése bizonyos értelemben inkább a minőségbiztosítás érdekében megtett lépés, és nem mondjuk a kimagasló innovációt jelzi.

Virus Bulletin VB100% díj

A VB100% díjnál, amely önmagában azért már jelez egyfajta alapvető megfelelőséget is, megmutatja, hogy egy valóban jól összerakott és megfelelően karbantartott termékről van szó. Mint ismeretes, ezen a teszten a résztvevő programoknak úgy kell 100%-osan felismerni az aktuális válogatott "WildList" lista kártevőit, hogy közben nem okozhatnak vakriasztást (false positive). Ez a rendszer emellett számos más hasznos, sebességbeli és teljesítmény mutatókat is közöl, beleértve például a nemrég hozzáadott rendszerstabilitási minősítést. Sőt 2009 óta a RAP, azaz „Reactive And Proactive” szavak rövidítéséből keletkező mutatóval azt is értékelik, hogy az egyes gyártók milyen gyors frissítési reakció időt produkálnak, illetve, hogy a még ismeretlen kártevők elleni heurisztikus, azaz pusztán viselkedés alapú szűrésük mennyire hatékony. Emellett mind az AV-Test, mind pedig az AV-Comparatives is kombinált tényezőkre alapozzák a tesztsorozataikat. Az AV-Test-en egy sor különféle területen kell értékelhető pontszámot elérni, majd ezeket összesítve kell megfelelni, míg az AV-Comparatives esetében egy többszintű díjrendszer került kitalálásra, amelynél a magasabb értéket - több csillag - a legjobbak kapják meg.

Összefoglalva, nem könnyű eligazodni a minősítésért folyó vírusirtó tesztek dzsungelében. Tipikus hiba például, amikor a tesztelést elvégző személy vagy szervezet hiányos vírusmintákkal dolgozik. Ha egy tesztben azt látjuk, hogy valamelyik védelmi képesség (például heurisztikus védelem) esetében a felhasznált vírusminták száma csak alig néhány tucatnyi, az biztos jele annak, hogy a teszt végső eredményét ez a módszertan eltorzította. Ha jó antivírust szeretnénk választani, amely a legjobban megfelel az igényeinknek, éppen ezért azt is érdemes megnézni, ki és hogyan végezte a tesztet. Ha a labor nevét "csak a Google ismeri", akkor valószínűleg kevésbé

relevánsnak tekinthetjük az ott kapott eredményeket. Éppen emiatt létezik már jó ideje egy **AMTSO** (The Anti-Malware Testing Standards Organisation) nevű nemzetközi szervezet, amely 2008 óta éppen az ilyen tesztelések javításán munkálkodik, szorgalmazza, hogy a vizsgálatok minél inkább objektívek, ésszerűek, szakszerűek, és átláthatóak legyenek, ezáltal a felhasználók is minél jobban megbízhassanak ezekben.

A különböző megszerezhető minősítések közül azok a legfontosabbak, amelyek az AMTSO szakmai szervezet irányelveknek megfelelő metódusok szerint tesztelnek

Ha egy tesztelési metódus mindenki által megismerhető, akkor rendszerint az eredményekkel kapcsolatos bizalom is stabilabb. Egyetlen minősítő jelvény feltüntetése pedig önmagában még nem dönti el, hogy az egyik termék jobb-e, mint egy másik. Ezzel szemben viszont az érdemi teszteken hosszú távon mutatott folyamatos, stabil, kiegyensúlyozott jó szereplés mindenképpen fontos fegyvertény.

Összehasonlító és csoportos tesztek

A fentiekkel a tanúsítási rendszerek áttekintésén vagyunk túl, a folytatásban pedig az összehasonlító és csoportos teszteket vesszük nagyító alá. A tesztek világában ez már egy sokkal árnyaltabb terület, ahol jobbára jól ismert szaktekintélyek, valódi profik végzik ezeket. Másfelől azt is gyakran tapasztaljuk, hogy bárki, akinek van egy számítógépe és egy kis indíttatása, ezek birtokában máris kvalifikáltnak érzi magát egy összehasonlító teszt elvégzéséhez. Van ugyanis egy csomó buktató, amin az önjelölt, amatőr tesztelők elvérezhetnek, és ezek alapján aztán teljesen elfogult, félrevezető következtetéseket vonnak le.

Mentesítési teszt (Cleanup)

Az összehasonlító tesztek egyik kiemelt pontja ez a hatékony felismerés, a védelem minél kevesebb vakriasztással, és a teljesítmény, sebesség témakörök mellett. Ez a terület kívánja talán a legtöbb technikai szakértelmet, és annak a folyamatnak a teljes megértését, hogy pontosan mi játszódik le, amikor egy kártevő megfertőz egy rendszert, az mennyire súlyos és tartós változásokat okoz. Ahogy annak pontos és megbízható mérése is, hogy ezek a változások mennyire fontosak, hogyan értékeljük ezeket.

Kíván továbbá egyfajta mérlegelést az is, hogy a különféle termékek által a mentesítés után hátrahagyott részek mikor tekinthetők ártalmatlannak, és mikor nem, míg más programok esetén meg esetleg éppen a mentesítéskor történő helyreállítás okozhat kárt. Mivel ez a szakterület igényli a legalaposabb ismereteket, végrehajtása pedig hosszadalmas és munkaigényes, nem meglepő, hogy az egyik legritkábban elvégzett tesztfajta, különösen az amatőrök részéről.

Sebességteszt (Speed)

A sebesség tesztelése a fentiekhez képest nagyságrendekkel egyszerűbb procedúra, és nem igényel mélyreható kártevő ismereteket sem. Ahogy az időjárásra, kedvenc antivírusára is mindenki szeret panaszkodni, hogy lassú, lelassítja a rendszert (és persze közben nem ad 100%-os védelmet, ilyet soha nem is fog). Épp ezért érdekes azt látni, hogy különböző termékek hogyan teljesítenek ezeken a megmérettetéseken. Szakszerűtlenséggel persze itt is el lehet rontani a dolgokat. Dióhéjban az számít jónak, ha a pontosság érdekében reális felhasználói körülmények között többször is elvégezzük ugyanazokat a teszteket. Nincs ugyanis rosszabb, mintha egy kívülálló véletlen tényező eltorzítja az egyetlen egyszer elvégzett mérés eredményét, majd ezeket, mint szenzációt világgá kürtölik.

Hamis riasztás teszt (False positive)

Ez egy kulcsfontosságú tulajdonság, hiszen lehet egy vírusirtó bármilyen gyors, ha mindeközben nem biztonságos. Ahogy a sebességtesztnek is csak akkor van értelme, ha közben ezt a védelmi képességektől nem elkülönítve vizsgáljuk, ugyanígy a védelem minőségében kiemelkedő szerepe van a vakriasztások számának. Egy termék, ha észleli ugyan az összes létező kártevőt, még közel sem nevezhető tökéletesnek, ha eközben a tiszta szoftverkomponensekre, illetve weboldalakra is tévesen riaszt.

Ha elég gondosan felkészülünk egy ilyen tesztre, akkor ezt bárki elvégezheti, ehhez tulajdonképpen nem a válogatott kártevőkből, vagy potenciálisan fertőző weboldalakból kell hatalmas mennyiség, hanem inkább a garantáltan tiszta, fertőzésmentes állományokból szükséges egy jelentős adatbázis. Ha a senki által nem ismert és nem használt Fűnyíró Szimulátor 2008 nevű programcsomag egyik

eleme vakriasztást okoz, ettől még nem dől össze a világ, ám ha például a Windows egyik alapvető komponensére riaszt tévesen egy antivírus, az már könnyen felkerül az újságok címlapjára. (Saját tapasztalat alapján a vírusirtó csapatok technikai részlegei között nincs ilyenkor semmilyen káröröm, se rosszindulatú rivalizálás, hanem készségesen segítenek egymásnak, ha tudnak valamiben, és azzal is tisztában vannak, ez a fajta Damoklész kardja kicsit mindegyikük felett ott lebeg.) Éppen ezért bár fontos, hogy a vakriasztások száma valóban a lehető legalacsonyabb legyen, ha teszt közben jelentkeztek ilyenek, érdemes megnézni azt is, hogy pontosan mik ezek, mennyire jelentős állományok okozták ezeket.

Egy hamis riasztás a rosszabbik fajtából: 2009. márciusában a Microsoft Windows Defender tévesen riasztott az operációs rendszer „C:\Windows\system32\drivers\etc\hosts ” állományára

Észlelési teszt (Detection)

Ez a legtöbb összehasonlító teszt fő alkotóeleme, hiszen a védelmi és felismerési képességek vizsgálata mindenkinek egyaránt fontos, de persze ebben is lehetnek zavaros dolgok. Az ilyen vizsgálat egyfelől igényel egy hatalmas kártevői adatbázist, amelyre rá lehet zavarni a versenyzőket. Az ilyen tesztek általában kevésbé tükrözik egy komplex, többrétegű védelem minőségét, de természetesen így is hasznos mutató arra nézvést, hogy az adott termék kliens, szerver vagy éppen gateway terméke milyen rátájú felismerést produkált. Emellett még rengeteg dolgot kell ilyenkor szem előtt tartani, például hogy a minták minden szempontból megfelelőek legyenek. A korábban emlegetett tiszta fájlokhoz hasonlóan, itt is gondosan kell azokat ellenőrizni, valóban lefedik-e az aktuálisan jelentkező sokrétű valós fenyegetéseket.

Ez egy hálás teszt, azonban itt is szükséges a tesztelő részéről a képesség és rengeteg idő mellett az is, hogy pontosan tudja milyen mintákat használ, miért használja azokat, és ne mindössze csak pár tucattal vizsgálódjon. Arra is volt például eset, hogy az egyik antivírus gyártó megfellebbezte egy tesztbeli eredményét arra hivatkozva, hogy a fel nem ismert minta nem is valódi kártevő, hanem csak egy ártalmatlan, futásképtelen sérült példány. A tesztlabor emiatt később igazat adott az illető gyártónak, és emiatt minden résztvevőnek újraszámolták az eredményeit.

Védelmi teszt (Protection)

A teljeskörű tesztek Szent Grálja, amelynél reális, valós támadások kivédésében szükséges képességeket igyekeznek ellenőrizni úgy, hogy abban a rendelkezésre álló védelem minden rétege részt vegyen. Első pillanatra talán úgy tűnhet, hogy ez így elég egyszerű, nem is kell hozzá sok szakértelem. Ám ahhoz, hogy ilyen vizsgálatokat ismételten és rendszeresen végrehajthassunk úgy, hogy a versenytársak egyenlő esélyekkel, összehasonlíthatóan és mérhetően birkózzanak meg ugyanazokkal a veszélyekkel, kiemelten nehéz feladat.

Mivel ennek végrehajtása inkább egy egyesével végrehajtandó precíz feladat, így időigényességben is kiemelkedően sokat kíván a tesztelőktől. Az automatizálás (például virtuális gépekben) olyan kifinomult és tapasztalatot igénylő gyakorlat, amely alaposan megtervezett és jól felépített körülmények között több hónapot is igénybe vehet pár száz minta vizsgálata esetében. És természetesen itt is előjön a megfelelően kiválasztott minták fontossága, hogy ezek valóban reprezentatívak legyenek még egy ilyen szűkebb, kisebb számú halmazon végzett tesztelési esetben is.

Éles határvonal van a valódi és a hamis antivírusok között. Utóbbiak nem ritkán saját honlappal is hirdetik magukat, és ott gyakran valós eredmények nélkül, csak úgy hasraütésszerűen is elhelyeznek, odahamisítanak különböző ismert minősítő emblémákat, logókat

Módszertan (Methodology)

Minden jó összehasonlító teszthez mellékelni kell valamilyen módszertant is, amely részletesen ismerteti, hogyan és mikre alapozva zajlott a vizsgálat. Ezeknek a részleteknek az ismerete segít megérteni, mely elemnek mi volt a szerepe, mik voltak az aktuális beállítások, milyen intézkedésekre került sor, hogyan gyűjtötték az adatokat, és hogyan értelmezték végül azokat. Egy módszertan olvasásakor a részletek hiánya legtöbbször arra utal, nem volt kellően átgondolva, megtervezve a vizsgálat, és ilyenkor akaratlanul is arra kell gondoljunk, hogy a leszűrt eredmények és következtetések is ingatag talajon állhatnak.

Tippek tesztelőknek

Igazság szerint ez tényleg egy rendkívül bonyolult tevékenység. A fentieken kívül mindez magában foglalja a tesztelendő termékek kiválasztását, a kapott nyers eredményekből a következtetések levonását, és számos egyéb dolgot. Néhányszor használtuk itt az amatőr tesztelők megnevezést, arra utalva, hogy a hivatásos tesztelők világa eléggé zárt közösség, ám ezzel senkit nem kívántunk megbántani. Mindenesetre ha valaki azt tervezi, hogy esetileg vagy akár rendszeresebben ilyen összehasonlítási tesztelési feladatba vágna bele, kaphatott most hozzá muníciót. Ha valaki rendszeresen részt vesz ilyen tesztekben, vagy saját tesztet kíván készíteni, akkor okvetlenül érdemes az AMTSO ezzel kapcsolatos dokumentumait, állásfoglalásait tanulmányozni, ezek sokkal mélyebben foglalkoznak a témával. Ha a teszteléssel kapcsolatban valami nem világos, vagy kérdés merül fel, a legtöbb hivatásos tesztelő nyitott és válaszolni fog nekünk, ha e-mailben megkeressük őket.

Mire figyeljünk?

A fogyasztók mindig örömmel fogadják az összehasonlítási teszteket, hiszen ők információkat keresnek ahhoz, hogy melyik terméket érdemes választaniuk. A teszteredmények alapján két lehetőség közük választhatunk. Az első az egyszerűbb megoldás, a kijött értékek alapján automatikusan kihirdetjük a numerikus rangsort, és bízunk abban, hogy szerencsénk volt, és semmi sem zavarta meg a munkánkat.

A másik, ha tisztában vagyunk azzal, hogyan és miért választottuk az adott tesztet, és annak minden lépését megértjük. Ez persze jóval időigényesebb, sok tesztelési módszertanon kell átrágni magunkat, ha valami gyanús, akkor az AMTSO irányelveket és módszereket kell lapozgatni, megnézni más összehasonlító teszteléseket. A mi véleményünk az, hogy a második út adja a jobb, pontosabb eredményeket. Minden résztvevőnek az a közös érdeke, hogy ezek alaposak és átgondoltak legyenek, hogy valóban jól használható, megbízható, hiteles eredmények szülessenek általa, és ha ebben valamilyen részlet esetleg nem világos, abban szabadon lehessen tájékozódni.

És ha már azt sikeresen megállapítottuk, hogy az antivírus mi nem (például egy lift), zárszóként egy Alfred Hugertől (Immunet) származó frappáns idézetet is szeretnénk megosztani: „Az embereknek meg kell érteniük, hogy az antivírus inkább biztonsági öv, mint páncélozott autó: megvédhet egy balesetben, de cserben is hagyhat.”