KÁRTEVŐELEMZÉS „HÁZILAG”

Mindentudó fekete dobozok

Sorozatunk huszonharmadik epizódjában kipróbálunk néhány olyan szolgáltatást, amelyekkel kártevőket elemezhetünk. A résztvevők mind igyekeznek többet nyújtani, mint egy virustotalos gyorsvizsgálat, és pontosan erre a többletre leszünk majd nagyon kíváncsiak.

Onnan indult el a lassan már két esztendős cikksorozatunk, hogy A *32 lovas fogat címmel* a VirusTotal (**www.virustotal.com**) weboldalról írtunk. Az azóta már 39 „lovas” szolgáltatás minden ismert antivírus programmal megvizsgálja a feltöltött (vagy e-mailben elküldött) mintaállományt, és pillanatokon, esetleg perceken belül megkapjuk a végeredményt: hányból hányan látták fertőzöttnek a fájlt. A fertőzéseknél használt nevek aztán sok esetben már annyira eltérőek, vagy átfedik egymást, hogy a további nyomozás miatt a kedvenc biztonsági programunk elnevezésével érdemes megnyitni a Google keresőablakát.

Extrák a VirusTotalban

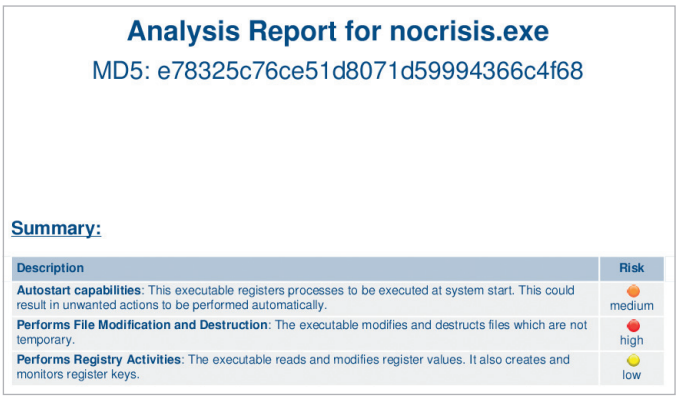
A figyelmes szemlélő – különösen, ha kicsit járatos a Windows-programozás és/vagy a kártevők területén – észrevehet már itt egy-két érdekes pluszsort a vizsgálat táblázata alatt is. Az ellenőrzött állomány bájtban mért hossza, valamint az azonosításhoz használt MD5, SHA1, SHA256 és Ssdeep hash értékek után további érdekes sorokat láthatunk, ha például EXE vagy DLL állományt vizsgálunk. A TrID egy olyan segédprogram, amely a fájltípus megbízható beazonosításában segíthet. Ugye egy fájl látszólagos kiterjesztése és a fájl valódi fájltípusa között néha nincs összefüggés, illetve eltérés esetén ez kimondottan a szándékos megtévesztés része. Szeretjük, ha egy állomány valóban az, aminek mondja magát, ellenkező esetben a homlokunk máris enyhe ráncot vet.

A Portable Executable rejtelmei

A PE EXE fájlok fejlécszerkezete sok olyan információt hordoz, amelyből a szakemberek számos következtetést tudnak levonni. Nincs olyan vírusvédelmi program, amely valamilyen szinten ne ellenőrizné ezeknek az adatoknak a meglétét, helyességét, ellentmondásait. Sajnos maga a Windows meglehetősen rugalmasan kezeli ezeket, így olyan programok futtatását is engedélyezi, amelyeket egy alapos segédprogram vagy egy antivírus alkalmazás szerfelett gyanúsnak talál. A VirusTotalban mindenesetre a PEiD és a pefile elemzése ad plusz támpontokat. Még ha minden antivírus motor néma marad, akkor is lehetnek itt kártevőkre utaló momentumok. Aki pedig az EXE fájlok birodalmában szeretne mélyebben megmerítkezni, annak hasznos további olvasmány lehet *Pavol Cerven* Programvédelem fejlesztőknek című könyve a Kiskapu kiadótól.

Ha feldobom, PDF, ha lesik, mi lesz?

Természetesen nemcsak az EXE állományok fejléc- és fájlszerkezete lehet olyan, ami barkácsolásra, trükközésre, exploit kódra utal, hanem



Analysis Report for nocrisis.exe

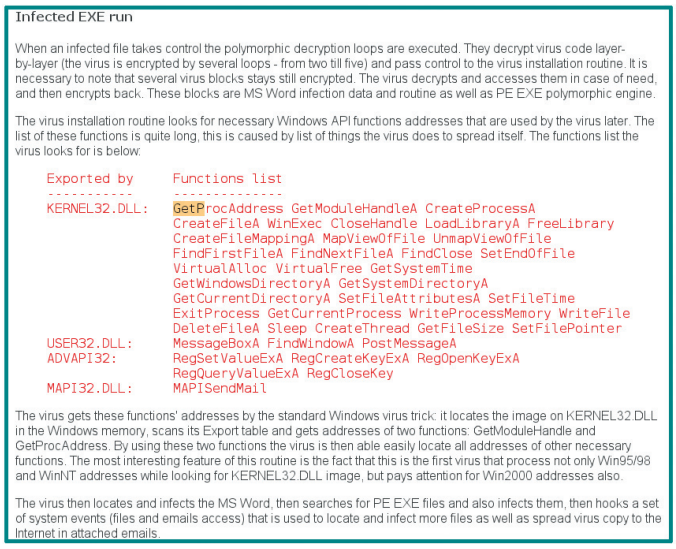
MD5: e78325c76ce51d8071d59994366c4f68

Summary:

Description	Risk
Autostart capabilities: This executable registers processes to be executed at system start. This could result in unwanted actions to be performed automatically.	medium
Performs File Modification and Destruction: The executable modifies and destructs files which are not temporary.	high
Performs Registry Activities: The executable reads and modifies register values. It also creates and monitors register keys.	low

Az Anubis PDF-riportja elején található összefoglalóban máminden fontos dolog látszik: a kártevő megpiszkálja az Autorunt, valódi (nem átmeneti) állományokat módosít, illetve töröl, és a rendszerleíró adatbázisban is változtatgat. Ezek közül az állományok módosítása/törlése látszik a legveszélyesebb tulajdonságnak a maga piros (high) jelzésével

A Sunbelt CW Sandbox oldalán a feltöltött minta alapos elemzésen esik át. Az eredményről e-mailben értesülünk



Infected EXE run

When an infected file takes control the polymorphic decryption loops are executed. They decrypt virus code layer-by-layer (the virus is encrypted by several loops - from two till five) and pass control to the virus installation routine. It is necessary to note that several virus blocks stays still encrypted. The virus decrypts and accesses them in case of need, and then encrypts back. These blocks are MS Word infection data and routine as well as PE EXE polymorphic engine.

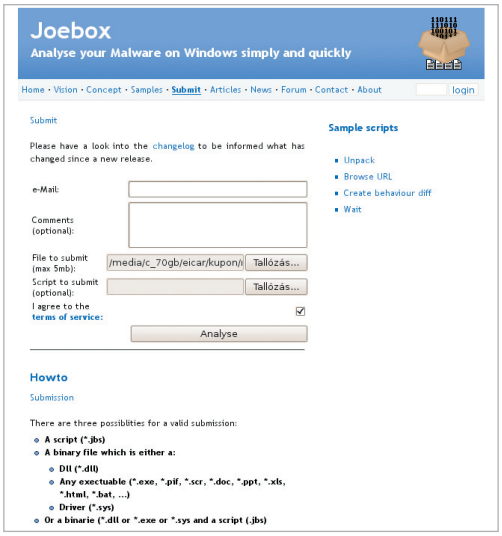
The virus installation routine looks for necessary Windows API functions addresses that are used by the virus later. The list of these functions is quite long, this is caused by list of things the virus does to spread itself. The functions list the virus looks for is below:

Exported by	Functions list
KERNEL32.DLL:	GetProcAddress GetModuleHandleA CreateProcessA CreateFileA WinExec CloseHandle LoadLibraryA FreeLibrary CreateFileMappingA MapViewOfFile UnmapViewOfFile FindFirstFileA FindNextFileA FindClose SetEndOfFile VirtualAlloc VirtualFree GetSystemTime GetWindowsDirectoryA GetSystemDirectoryA GetCurrentDirectoryA SetFileAttributesA SetFileTime ExitProcess GetCurrentProcess WriteProcessMemory WriteFile DeleteFileA Sleep CreateThread GetFileSize SetFilePointer
USER32.DLL:	MessageBoxA FindWindowA PostMessageA
ADVAPI32:	RegSetValueExA RegCreateKeyExA RegOpenKeyExA RegQueryValueExA RegCloseKey
MAPI32.DLL:	MAPISendMail

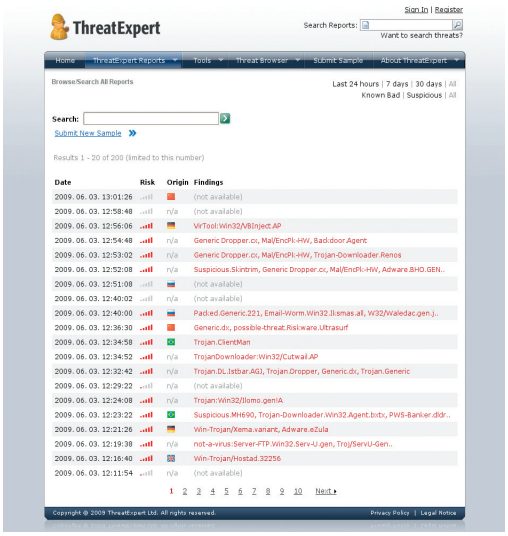
The virus gets these functions' addresses by the standard Windows virus trick: it locates the image on KERNEL32.DLL in the Windows memory, scans its Export table and gets addresses of two functions: GetModuleHandle and GetProcAddress. By using these two functions the virus is then able easily locate all addresses of other necessary functions. The most interesting feature of this routine is the fact that this is the first virus that process not only Win95/98 and WinNT addresses while looking for KERNEL32.DLL image, but pays attention for Win2000 addresses also.

The virus then locates and infects the MS Word, then searches for PE EXE files and also infects them, then hooks a set of system events (files and emails access) that is used to locate and infect more files as well as spread virus copy to the Internet in attached emails.

Tipikus API-függvények egy programban, amelyekre érdemes kiemelt figyelmet fordítani. Előfordulásuk önmagában még nem jelez kártevőt, de sokszor tűntek fel ilyen szerepben



Egy újabb online víruselemző a színen: Joe bácsi varázsdoboza. Az elkészült eredményeket e-mailben várhatjuk, ezért nem érdemes hamis címmel operálni

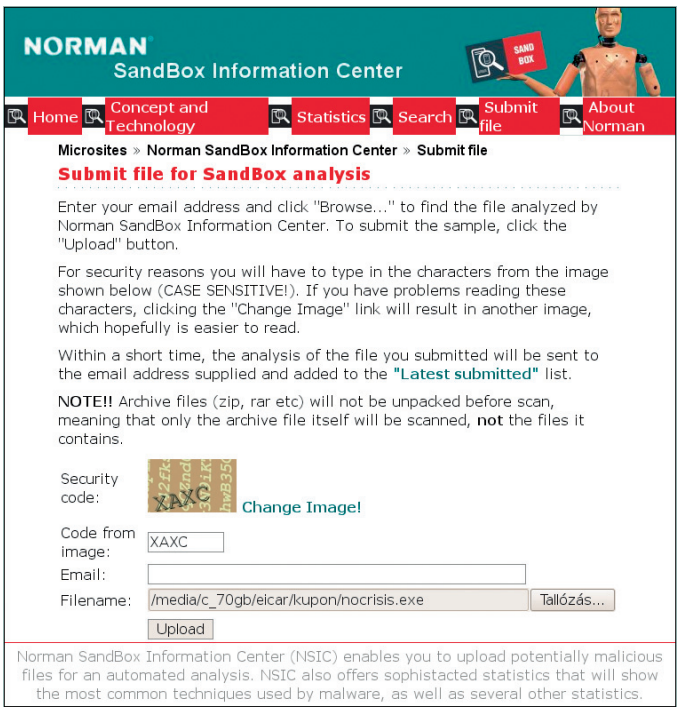


A ThreatExpert oldalán beleolvashatunk a mások által feltöltött állományok vizsgálati eredményeibe, és azt is láthatjuk, melyik mintát mikor és milyen országból töltötték fel

napjaink egyik slágere, a Portable Document Format alapú dokumentumoké, azaz a PDF fájloké is. Emiatt került be a VirusTotal eszközei közé a PDFiD nevű alkalmazás, amellyel hatékonyan különböztethetjük meg a szabályos és nagy valószínűséggel kártékony PDF állományokat. Ez utóbbi eszköz, szemben a PE-segédprogramokkal, nem egy elemző (parser), hanem ismert, veszélyes stringrészleteket keres, illetve vizsgál, és ennek alapján hozza meg a döntést.

Mindenkit elküldünk különböző helyekre

Ha van egy gyanús állományunk, amit már bedobtunk kedvenc VirusTotalunkba, esetleg további kísérletezés céljából a **novirusthanks.org**, a **virscan.org**, avagy a **virusscan.jotti.org** oldalakra, akkor feltámadhat az igény: jó lenne tudni, mit rejt még magában az állomány, mit tenne, ha futtatnánk? Milyen kellemes lenne, ha léteznének olyan webhelyek, ahová csak bedobjuk a gyanú tárgyát, és készen „kijön" az elemzés. Nos, jó hírrel szolgálhatunk, létezik ilyen, és a fenti vágyunkat ingyen és bérmentve megtehetjük. Az erre szakosodott weboldalak között csatangolunk most egy kicsit, hegymászó-felszerelés nélkül, de azért tornacipőben és a terjedelmi korlátok okán a teljesség igénye nélkül.



A szakma egyik legjobb automata kártevőelemző programja a Norman SandBox. A homokozóba dobott fájl kódemulációs végrehajtása biztonságos körülmények között leplezi le az orvul végrehajtott fájlkészítési és -törlési, valamint hálózati kapcsolat létesítésének kísérleteit

A sakál lapja

Első állomásunk a Secure Business Austria által üzemeltetett Anubis (**anubis.iseclab.org**). Ahhoz, hogy információhoz jussunk a vizsgálandó állományról, azt egyszerűen csak fel kell tölteni a weboldalra, ahol az automata, gépi próbálkozásokat kiszűrő CAPTCHA-kód begépelése után indul is az elemzés. Azonosítani semmilyen módon nem szükséges magunkat, kattintsunk rá a Jóváhagy (*Submit*) gombra és máris indul a folyamat. Ha szerencsénk van, ez azonnal meg is történik, viszont ha mások is éppen használják az Anubist, akkor pár percig egy várólistára kerülünk. Maga az elemzés sem tart tovább, és az eredményt többféle állományformátumban (HTML, XML, PDF vagy sima szövegfájl) is letölthetjük.

Mi a szívünknek kedves PDF (Portable Document Format) kiterjesztést választottuk, tesztünk állandó szereplője pedig egy Kryptik (Waledac) trójai program volt, amelyet korábban egy fertőzött weboldalról töltöttünk le. Eredményképpen listát kapunk a kártevő által olvasott minden állományról, Registry-értékről, hálózati aktivitásról, minden módosított, valamint újonnan létrehozott bejegyzés, illetve állomány is elénk tárul.

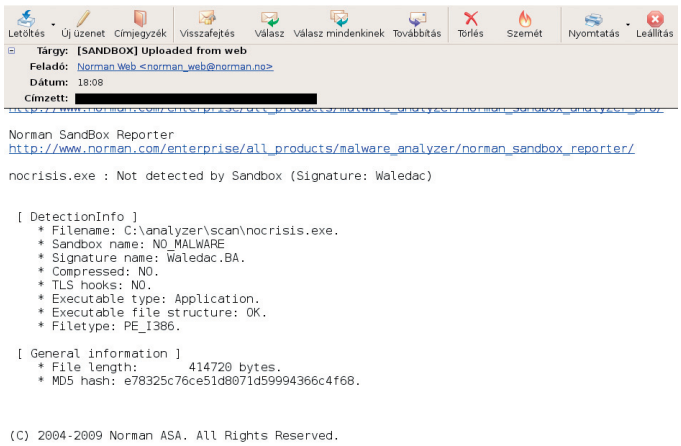
Az eszköz másik jól használható extrája, hogy nemcsak feltöltött állományokat lehet vele elemeztetni, hanem egy adott weboldal címe is begépelhető ellenőrzésre. Ez a manapság előforduló rengeteg IFRAME-fertőzött weboldal esetében különösen hasznos szolgáltatás. Ekkor a riportban a webszerverrel történő kommunikáció fontosabb részleteit is megtalálhatjuk, de ehelyett persze a HTTPLiveHeaders Firefox-plugint (**livehttpheaders.mozdev.org**) is használhatjuk a felderítésre.

CWSandbox: az ígéret szép szó...

A következő lehetőség a CWSandbox weboldal (**www.cwsandbox.org**). Itt is feltölthetjük a vizsgálandó állományainkat – 12 megabájtos méretkorláttal –, és az eredményt kérhetjük sima szöveges vagy HTML formátumban is. A feltöltéskor kapunk egy egyedi ID-t (azonosítót), és ennek birtokában tekinthetjük meg aztán az elemzés eredményét. Sajnos cikkünk írásakor karbantartás miatt már több mint egy hete állt a szolgáltatás, ezért feladtuk eredeti tesztelési terveinket. Remélhetőleg a későbbiekben – mondjuk újságunk megjelenése után – már működni fog.

Joe bácsi varázsdoboza

Következő vizsgálatunkat a Joebox oldal (**www.joebox.org**) elemző készüléke (**www.joebox.org/submit.php**) segítségével végeztük, szerencsére itt minden az elvárásainknak megfelelően zajlott. Az állomány feltöltése után azonban itt meg kellett adnunk az e-mail címünket, mert magát a riportot levélben fogjuk



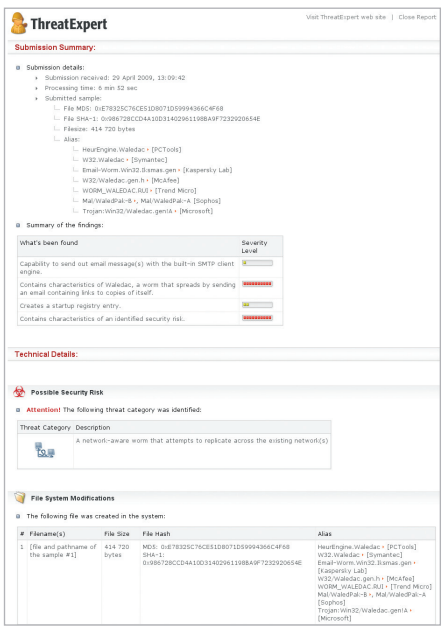
A Norman Sandbox online változataszűkszavú, mindössze néhány kulcsinformációt szolgáltat

megkapni. (Akik sűrűn használják a VirusTotal weboldalt, azok emlékezhetnek rá, hogy a weben megjelenő értékelés mellett ott is van lehetőség elektronikus levélben kérni az eredményt.) Néhány perc leforgása alatt meg is érkezett egy ZIP mellékletben a riport, amely egy másfél megabájt méretű HTML fájlt rejtett magában. A jelentés különféle szekciókból áll, és ezekre kattintva merülhetünk el az olyan részletekbe, mint a Registry-bejegyzések manipulációi, a fájlok megnyitása olvasásra, módosításra, létrehozásra, processzek és végrehajtási szálak indítása, hálózati aktivitás stb. Összességében itt is azt kaptuk, amit vártunk, ráadásul a riport fastruktúrája kényelmes böngészést tesz lehetővé.

Egy pehelysúlyú versenyző

A ThreatExpert.com elemzője (**www.threatexpert.com/submit.aspx**) szintén bekéri e-mail címünket a fájl feltöltésekor, és ide érkezik pár perc múlva a „threatexpert" jelszóval titkosított riport, amely a korábbi indulók teljesítményéhez képest elég rövid és kivonatos.

Van azért érdekes újdonság is, kicsit a VirusTotal lehetőségei is visszaköszönnek: láthatjuk néhány víruskereső motor által adott detektálás eredményét is. Ugyancsak érdekes, hogy lehetőségünk van a mások által feltöltött elemzések olvasgatására is, ugyanis minden feldolgozás eredménye felkerül a weblapra, és az utolsó 200 riport nyilvános.



Nyitott portok, frissen létrehozott Registry-kulcsok. A ThreatExpert riportjában a felismert kártevők különféle antivírus cégek szerinti elnevezéseit (alias) is megtaláljuk

A vizsgálat minőségének szempontjából mindenesetre, aki a már korábban megismert elemzési részletességet igényli, az sokkal jobban jár az Anubis vagy a Joebox valemelyikével.

Hoppon maradás Norman-módra

Végül sétánkat az igazi nagyágyúnak számító Norman SandBoxnál fejezzük be (**hopp.pcworld.hu/6007**). Az elemzésre küldendő állomány feltöltése itt is a szokott módon zajlik, mindössze egy CAPTCHA-kód begépelése szükséges. A riport ezúttal is e-mailen keresztül érkezik, ám nagy meglepetésre alig pár sorból áll. Szó sincs a fent említett DLL-hívások, Registry-, állománykezelési és hálózati aktivitás kibontásáról. Lévén, hogy ismerjük a professzionális Norman SandBox Analyzer Pro képességeit, amelyek között minden korábbi vizsgálat mellett olyan extrák is megtalálhatóak, mint az önkicsomagoló tömörítők, a rootkitek és exploitkódok felismerése, ezért ebben az esetben úgy summázhatjuk az eredményt, hogy az ingyenes szolgáltatást nem kívánták használható, kedvcsináló formára hozni. Az ingyenes elemzési lehetőségnél nemhogy egy korlátozott riportot sem kapunk, az eredmény a használhatóságát tekintve – de a versenytársakhoz viszonyítva is – értéktelen.

A PEInfo segédprogram eredményei csak annak jelentenek újdonságot, aki mostanában még nem használta a VirusTotal.com kártevődetektorát. A szekciók nevei, méretei, a program belépési pontja, és még sok egyéb fontos infó bukkan elő gombnyomásra

Zárszó

Egy átlagos felhasználónak jól használhatóak az ismertetett ingyenes lehetőségek, hiszen csak esetenként él a lehetőséggel, és nem is annyira a technikai részletekre kíváncsi, hanem jobbára a saját biztonságáért aggódik. A felsorolt online eszközök képességei természetesen csupán töredékei – rendelkezésre állásban éppúgy, mint a tudás mélységében – a valóban jól használható, de fizetős, és igen borsos árú csúcs célprogramokhoz képest. Azonban vannak olyan munkahelyek, amelyek fizetőképes keresletet tudnak felmutatni az utóbbiak iránt – így például víruslaboratóriumokban, bankoknál, nemzetbiztonsági és nyomozó szerveknél ezek nélkülözhetetlen és naponta használt segédeszközök.

***

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

Az ESET magyar nyelvű víruslexikonja: **www.eset.hu/virus**
Online vírusazonosítók: **www.virustotal.com, virscan.org, virusscan.jotti.org, scanner.novirusthanks.org**
Anubis onliprogramelemző: **anubis.iseclab.org**
A Sunbelt online programelemzője (CWSandbox): **www.cwsandbox.org**
Joebox online programelemző: **www.joebox.org/submit.php**
A ThreatExpert online programelemzője: **www.threatexpert.com/submit.aspx**
A Norman SandBox online változata: **hopp.pcworld.hu/6007**
Ssdeep tudnivalók: **www.forensicswiki.org/wiki/Ssdeep**
TrID fájltípus-azonosító program: **mark0.net/soft-trid-e.html**
PDFiD PDF-kártevő kereső: **blog.didierstevens.com/2009/03/31/pdfid/**