SZÍNRE LÉP AZ ESET SYSINSPECTOR

Bigyó felügyelő

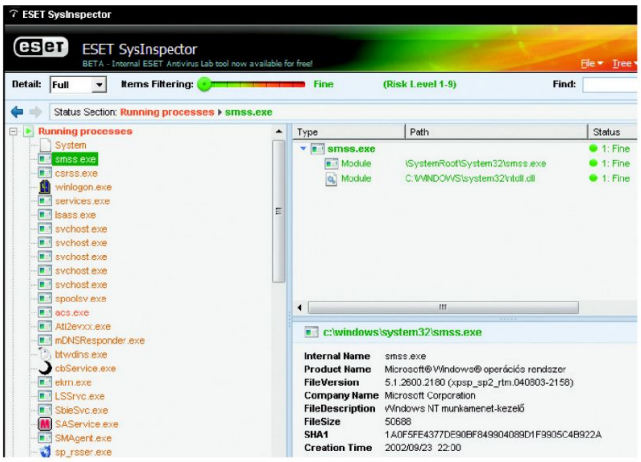
CD2/DVD
A cikkben jelzett ingyenes programok megtalálhatók a lemezmellékleten

Sorozatunk hetedik epizódjában a legsebezhetőbb operációs rendszer, a Windows folyamatairól, illetve károkozók állományainak és processzeinek megtévesztő nevéről lesz szó. Ennek kapcsán bemutatunk egy olyan segédprogramot, amellyel kicsit alaposabban is szemügyre vehetjük a gép belső folyamatait.

Az új NOD32 3.0 és az ESS (ESET Smart Security) komplett védelmi csomagja mellé érkezett még egy további újdonság is: egy SysInspectornak nevezett és jobbára hozzáértőknek ajánlott diagnosztikai program, amely ugyancsak érdekes dolgokra képes. A 32 és 64 bites Windows rendszerekhez készült, és telepítés nélkül, azonnal futtatható a SysInspector.exe állomány indításával, majd a gép teljesítményétől függően egy-két perces várakozás (tesztelési ciklus) után egy szép, Vista stílusú ablak jelenik meg. Ez az adott rendszer szoftver- és hardverkörnyezetéről minden részletre kiterjedő információkat jelenít meg egy fastruktúrában, az alábbi csoportosítás szerint:

Első helyen a futó folyamatokat (Process) láthatjuk: ez a csomópont részletesen kibontja a gépen futó összes folyamat és alkalmazás listáját. Ebben a hivatkozott DLL-könyvtárak is fel vannak tüntetve.

A következő csoport neve hálózati kapcsolatok (Network Connections); itt kapunk egy listát azokról az alkalmazásokról, amelyek TCP vagy UDP protokollon keresztül hálózati forgalmat bonyolítanak le, valamint ellenőrizhetjük az aktuális DNS- (Domain Name System) szerverbeállításokat is.



A Microsoft Windows futó folyamatai természetesen az 1-es kategóriában eveznek

A program segítségével nemcsak az egyszerű felhasználók tudnak diagnosztikai vizsgálatot végezni, de a gyanús esetek kivizsgálásánál a szakértő kezében is aranyat ér. Hamarosan megjelenik végleges angol nyelvű változata

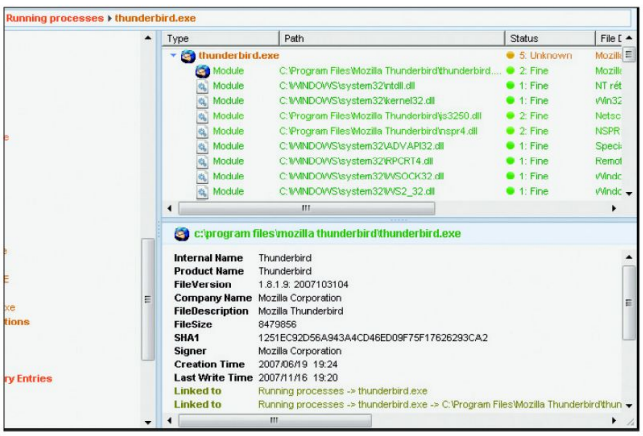
Miért fontos ez?

Külön kategóriát képeznek a rendszerleíró adatbázis fontosabb bejegyzései (Important Registry Entries). Ezek közül elsőként az automatikus végrehajtással kapcsolatos (autostart) részek szerepelnek, hiszen számos kártevő igyekszik ezek manipulálásával gondoskodni arról, hogy a kártékony kód a gép újraindítása után automatikusan lefusson. Ezen a listán találhatók még a szintén lehetséges támadási felületet adó belépéssel (Winlogon), valamint a BHO-val, azaz a böngésző-segédobjektumokkal (Browser Helper Object) kapcsolatos információk, és természetesen a támadások kedvelt célpontját jelentő Internet Explorerre vonatkozó adatok sem maradhattak ki.

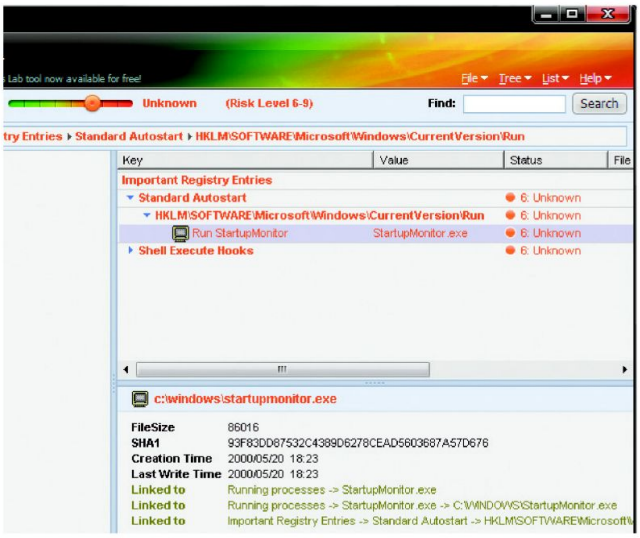
A következő csoportban a szervizfolyamatok (Services) kaptak helyet: itt minden rendszerszolgáltatásként az operációs rendszer hasznos és integráns része (eredeti nevén Generic Host Process for Win32 Services), és mindig Windows/System32 mappában található. A Jeefo. A a fertőzés alkalmával elkódolja az állományokat, illetve egyes esetekben a fertőzött fájlban hasznos területeket is felülír, így az működésképtelenné is válhat, tehát elég veszélyesnek ítélhetjük. Ha esetleg számítógépünkre nincs megfelelő vírusfigyelő program telepítve, akkor a Feladatkezelőben (TaskManager) laikus számára nehéz feladat lehet a többféle svchost.exe folyamat között átlátni a helyzetet, de a SysInspector ilyenkor is segíthet.

Szintén megtaláljuk a számítógépre telepített eszközök meghajtó-futó folyamatot megjelenít a program. A Microsoft Windows futó folyamatai például az 1-es kategóriában szerepelnek. Itt érdemes egy konkrét kártevőt is megemlíteni, legyen például a december havi statisztikában is előkelő helyen szereplő Win32/Jeefo.A vírus (www.nod32.hu/virus/jeefo-a).

Ezt a károkozót 2003 nyarán észlelték először, és érdekessége, hogy megtévesztésül egy svchost.exe nevű állományt hoz létre a Windows könyvtárában. Az igazi svchost

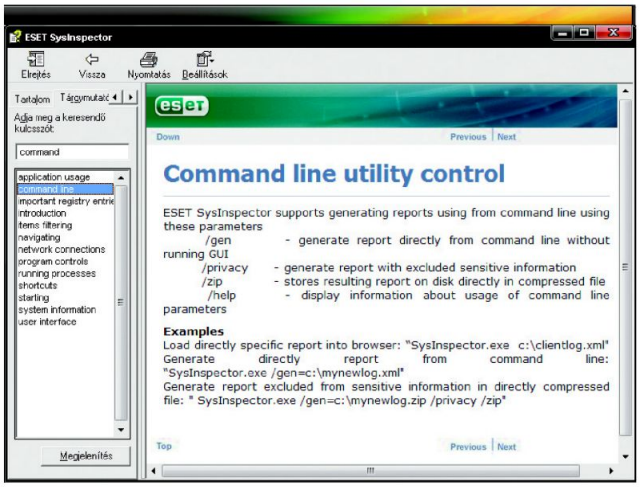


Ebben a nézetben már a hivatkozott DLL-könyvtárak is fel vannak tüntetve



Itt a felügyelő kissé ráncolja a homlokát, mert a StartupMonitor fontos rendszerváltozókkal kerül kapcsolatba, és az alkalmazás egyelőre ismeretlen számára

A különféle bejegyzések eltérő, egy kilencfokozatú veszélyességi skálán szereplő értékhez tartozó számot viselnek



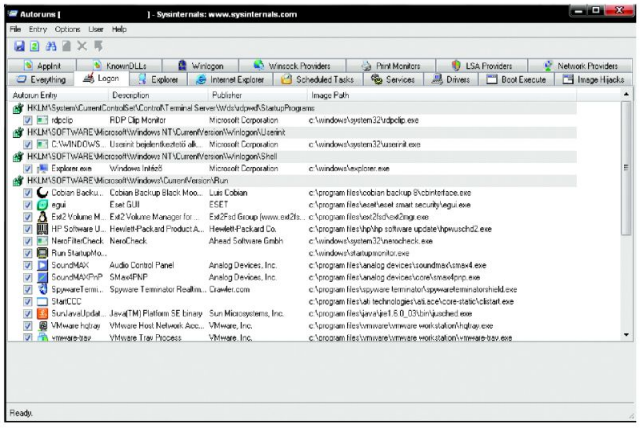
A parancssori futtatásnál a /privacy kapcsoló segítségével visszatarthatjuk a bizalmas személyes információkat, illetve riportot is készíthetünk közvetlenül egy csomagolt ZIP-állományba

programjait (Drivers) is. Ez a fül kilistázza az összes szoftver- és hardverillesztő programot, részletes verziószámmal, gyártóval, dátummal és egyéb adatokkal.

Korábban már említettük a Registry AutoRunnal kapcsolatos bejegyzéseit, de nem árt tudni, hogy az újraindítás utáni beavatkozások nemcsak a rendszerleíró adatbázissal végzett trükközés révén befolyásolhatók, hanem léteznek olyan nevezetes, kritikus Windows-állományok (Critical Files), amelyek védelme külön szót, illetve védelmet érdemel. Ebbe a csoportba a win.ini, system.ini és a hosts fájlok tartoznak. A Win.ini és a System.ini megváltoztatásával például az AutoStart folyamatokat lehet manipulálni, míg a hosts állomány módosításával elérhető, hogy bizonyos weboldalak ne működjenek. Az ilyen átirányításokkal egy támadó például megakadályozhatja a biztonsági programok frissítéseit, de az adathalászok is előszeretettel szokták a hosts mérgezését alkalmazni arra, hogy egy megbízható webhely helyett egy másik URL-re térítsék az áldozat böngészőjét.

Az adott számítógép feltérképezését segíti a részletes rendszerinformáció (System Information) menüpont is. Itt az operációs rendszer adatait, környezeti változóit, a telepített szoftverek és frissítési csomagok listáját, valamint a bejelentkezett felhasználók adatait és jogosultságait szemrevételezhetjük.

Ugyancsak külön kiemelve látjuk viszont a fontosabb fájlokat (File



A SysInternals által készített AutoRuns segédprogram is jó szolgálatot tehet egy alapos ellenőrzés során

A már korábban emlegetett StartupMonitor éberen figyeli, ha egy alkalmazás együtt próbál indulni a rendszerrel. Itt éppen az ártalmatlan és igen hasznos Orbit Downloader letöltésvezérlő programra kérdez rá

Details). Ebben a csoportban pedig a főbb rendszerfájlok, a telepített végrehajtható állományok részletes információit találjuk.

Többféle szűrési lehetőséggel is élhetünk az adatok megjelenítésekor: a teljes adatmennyiséget a Full módban, egy közepes információhalmazt a Medium, míg egy szűk összefoglalót a Basic módban kaphatunk. Emellett a különféle bejegyzések eltérő, egy kilencfokozatú veszélyességi skálán szereplő értékhez tartozó számot viselnek. A százszázalékosan ismert, közismert és megbízható állomány, folyamat, elem kapja az 1-es besorolást, a biztonságosnak tűnő, de a program számára jelenleg ismeretlen az 5-ös számmal van jelölve, míg az ismert, de kártékony objektumok a nagyon veszélyes, 9-es csoportba kerülnek. Ezt a kilenc csoportot is ki lehet listázni, vagyis vadászhatunk a különféle veszélyeztetettséget jelentő elemekre is. Emellett természetesen ott van a szabad szavas keresés, ahol egy beírt keresőszó minden előfordulását vizsgálhatjuk.

A fejlesztők természetesen a parancssori futtatást kedvelő képzett felhasználókat és a rendszergazdákat sem felejtették ki a számításukból: a program grafikus felület (GUI) nélkül, a parancssorból is indítható egyedi kapcsolókkal, sőt XML- vagy ZIP-állományba képes különféle tartalmú riportokat generálni. Ezeket utólagosan is lehet elemezni, hiszen magába a SysInspectorba a külső riportok egyetlen kattintással beolvashatók. Természetesen az is nagy előny, hogy egy ilyen riportot probléma esetén könnyen el tudunk küldeni a technikai támogatást végző support munkatársnak további vizsgálatra.

Szinte minden egyben

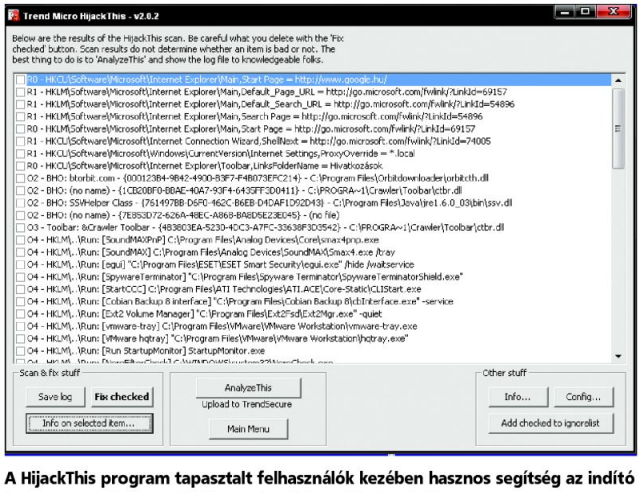
Régóta léteznek már hasonló programok, hogy csak az ismertebbeket említsük: a Sysinternals (www.sysinternals.com) Autoruns, ProcessMonitor és ProcessExplorer alkalmazásai, valamint a Startup Monitor (www.mlin.net/StartupMonitor.shtml), a HijackThis (www.spywareinfo.com/~merijn/), a System Information for Windows (SIW) (www.gtopala.com). Mindenesetre az ESET SysInspector egy jól összeállított és hadra fogható univerzális eszköznek látszik a kártevők ellen folytatott harcban.

A SysInspector futtatásához valóban minimális rendszerkövetelmények társulnak: 32 vagy 64 bites Intel vagy AMD processzor, NT-alapú Microsoft (2000, XP, Vista, Server 2003) operációs környezet, 35 megabájt szabad memória, illetve 2 megabájt szabad hely a merevlemezen. A program egyelőre még béta-állapotban van (www.eset.eu/download/beta), de várhatóan hamarosan megjelenik a végleges angol nyelvű változata, amelyet az ESET vásárlóinak ingyenesen bocsát a rendelkezésére.

***

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



A HijackThis program tapasztalt felhasználók kezében hasznos segítség az indító bejegyzések és hasonló kényes területek ellenőrzésében