Mi lesz itt megfizetve? Várható kártevő trendek 2011-re.

Semmi sem állandó, kivéve a változást. Az élet minden területén érezhető ez a folyamatos mozgás, fejlődés, átalakulás. A vírusok hőskorának elmúlásával kialakultak bizonyos trendek, ezek viszonylag stabilan tartják magukat, és folyamatosan bővítve a megjelenési formájukat egyre újabb köntösben, egyre hatásosabb megtévesztéssel jelennek meg.

Vajon mi várható majd 2011-ben vírus és kártevő fronton. A CARO 2010 elnevezésű vírusvédelmi konferencián tavaly májusban hivatalosan is megerősítették, hogy meghaladta a 40 milliót az egyedi kártevőminták száma. Ami biztos, hogy ez az irdatlan nagy szám sajnos 2011-ben még tovább fog növekedni. Az első negyedév elteltével határozottan állíthatjuk, az internet 2011-ben sem lesz biztonságosabb hely a korábbinál. Az ESET szakértőinek segítségével összegyűjtöttük, hogy mik azok a legjelentősebb fenyegetések, amelyekkel majd szembe kell néznünk.

Mobil vírusok:
Az okos-telefonok növekvő népszerűségének köszönhetően a mobil készülékeket érő támadások 2011-ben várhatóan megtöbbszöröződnek. A bűnözők számára az egyre növekvő piac jó terepet kínál, mivel a mobil biztonsági szoftverek használata még nem tartozik a felhasználói kultúra alapelemei közé.

Zombik támadása:
Az ESET adatai szerint a botnetek mérete a számítógépeket zombivá tevő fertőzések számával együtt folyamatosan növekszik. A bűnözők a hálózatok irányítására a legkülönbözőbb csatornákat - például a Twittert - használják. Jó hír, hogy a biztonsági vállalatok egyre nagyobb sikereket érnek el a nagyobb botnetek lekapcsolásában, de ennek ellenére számolni kell a hálózatok számának növekedésével.

Vírusok Mac-en:
A Java/Boonana.A 2010. novemberi megjelenésével egyértelművé vált, hogy az OS/X rendszerek elterjedésének köszönhetően a Macintosh számítógépek felhasználói már vonzó célpontot jelentenek a bűnözők számára. Annak ellenére, hogy az Apple operációs rendszere szigorú biztonsági beállításokat tartalmaz, a kevésbé hozzáértő felhasználók bedőlhetnek a megtévesztő kártevőknek, és maguk kapcsolják ki azokat a korlátozásokat, amik megakadályoznák azok terjedését.

Mérgezett keresők:
A legnagyobb keresők találati listájának eltérítése vagy mérgezése már 2010-ben is elterjedt volt. A technika lényege, hogy a bűnözők különböző keresőkifejezésekre optimalizálnak weboldalakat, majd megvárják, hogy ezek felkerüljenek a keresők találati listájának elejére. Miután ez megtörtént, megfertőzik őket, és rajtuk keresztül a felhasználók számítógépeit. Ugyan a keresők folyamatosan próbálják kiszűrni a mérgezett oldalakat a találati listájukból, a nagyobb volumenű támadásokkal szemben sokszor tehetetlennek bizonyulnak. Ez jelenleg lehet éppen a japán földrengés, de mindig lesz olyan aktuális esemény, amelyre az emberek kíváncsiak lesznek.

Fertőző közösségi oldalak:
A közösségi oldalakon az adathalászok rendszerint valamilyen vicces, érdekes üzenettel és képpel vagy videóval keltik fel a felhasználók érdeklődését, majd egy alkalmazás segítségével megpróbálják megszerezni személyes adataikat. A problémát az jelenti, hogy lehetetlen megkülönböztetni, hogy egy adott bejegyzést valóban az ismerősünk írta ki saját üzenőfalára, vagy az egy kártevő működésének köszönhetően került oda. A támadások hatására a Facebook több beállítást is elérhetővé tett, melyek segítségével szabályozhatjuk, hogy a különböző alkalmazások

készítői milyen adatainkhoz férnek hozzá. Ezeket azonban a felhasználóknak kell aktiválniuk, amire a legtöbben nem fordítanak kellő figyelmet. Az ESET szakértői folyamatosan figyelmeztetnek a Facebookon megjelenő új kártevőkre a http://www.facebook.com/biztonsag oldalon keresztül.

Divat az exploit, most a PDF a sláger
Az exploit olyan sebezhetőség, amit egy, külön erre a célra szánt támadókóddal ki is használnak. A nem frissített rendszereken ha egy kéretlen levél mellékletére kattintanak, egy kéretlen linkre vagy egy preparált weboldalra tévedünk, akkor a beágyazott rosszindulatú kód automatikusan lefut, és a támadó kedve szerint tetszőleges program futtatását, jelszavaink ellopását tudja végrehajtani. A 2010-es évben a veszélyes fájlmellékletek közül leginkább a PDF dokumentumok okozták a legtöbb fejfájást. Egy tavalyi évre vonatkozó összesítés szerint a veszélyes dokumentum fájltípusok között a PDF emelkedett ki leginkább, 61 százalékban tartalmazott valamilyen hibát kiaknázható exploitot. És csak ezt követte aztán a többi, maradékon osztozó Office fájltípus: Excel, Word, PowerPoint. Érdemes tehát alaposan megválogatni, kitől fogadunk el PDF dokumentumot, a felesleges, gyanús, kéretlen leveleket, levélmellékleteket pedig legjobb azonnal olvasatlanul kitörölni. Fontos ügyeknél esetleg érdemes magától a feladótól megerősítést kérni, valóban ő küldte-e azt - persze mindezt szigorúan még a megnyitás előtt. Ugyancsak hasznos lehet gyanús esetben a VirusTotal oldalon is ellenőrizni a gyanús dokumentumokat.

Botnet, zombi - ebből jobb kimaradni
A korábbi feltűnősködés helyét átvette a rejtőzködés, minél tovább láthatatlanul ott maradni, onnan minden használható adatot ellopva, a gép erőforrásait alattomban távolról további támadásokhoz, bűncselekményekhez felhasználva botnet hálózatokba szervezve működnek ezek a fertőzött számítógépek. Ha össze akarnánk foglalni a leggyakoribb botnetre figyelmeztető jelzéseket, akkor az alábbiakra érdemes - mint intő jelekre - figyelni. Ezek külön-külön még nem okvetlenül jelentenek kártevőt, ám ha egyszerre több pont is ismerős, érdemes lehet gyanakodni.

1. Túlságosan sokszor pörögnek fel ok nélkül a hűtőventilátorok jelezve azt, hogy erősen dolgozik a gép, akkor is, amikor éppen nem is dolgozunk rajta. Persze ez még önmagában nem jelent semmit, lehet hogy éppen most tölti le és telepíti a gép a Microsoft frissítéseket, illetve a poros számítógép belső is okozhat intenzívebb ventilátor tevékenységet. Mindenesetre azért ez egy elég feltűnő jel, amire érdemes odafigyelni.

2. Minden ok nélkül túlságosan sok ideig tart, amíg a gép kikapcsol (shutdown), vagy ez nem is sikerül neki. Ez a pont is hasonlít az előzőre abból a szempontból, hogy ezt is okozhatja számos dolog, ami lehet kártevő is, de lehet rosszul megírt meghajtóprogram, kevés lemezhely, és még sok minden más. Természetesen a szokásos havi második kedden végzett frissítéssel egybekötött kikapcsolás egy teljesen más tészta, de ott ki is van írva mindez. De az összes többi esetben ez is egy jelzés lehet a sok közül.

3. A Facebook üzenő falon hosszú tömött sorban állnak a látszólag nevünkben küldött üzenetek. Érdemes haladéktalanul Facebook jelszót változtatni, és új erős, teljesen egyedi jelszóra cserélni, végül a számítógép teljes kártevő ellenőrzése is szükséges ilyenkor.

4. A programjaink igen lassan futnak. Ez persze adódhat a gyenge hardver miatt, vagy ha valóban több ezer állományt kell feldolgozni. A pontosabb megfogalmazás így inkább a szokatlanul lassan az eddigiekhez képest lehetne, ez már jól fedi a lényeget.

5. A rendszer nem engedi letölteni a legfrissebb Microsoft frissítéseket. Ez szintén eléggé jellemző szimptóma, ezzel igyekeznek megakadályozni a kihasználható sebezhetőség befoltozását. Azért ha lopott Windowst használunk, akkor ennél a pontnál ne csak botnetre gyanakodjunk elsősorban ;-)

6. A rendszer nem engedi letölteni a legfrissebb vírusadatbázist, illetve egyes vírusvédelmi weboldalak nem is jönnek be a böngészőben. Ez már egy nagyon jellemző tünet, például a Conficker féreg esetében üzemel is egy ilyen teszt weblap, ami pontosan ezekre támaszkodva mutatja ki a fertőzést.

7. Rövidebb-hosszabb ideig az internet sebessége drámaian lelassul. Mivel a fertőzött zombi gépek gyakran vesznek részt távoli DoS támadásokban, hatalmas mennyiségű spam levél kiküldésében, ezért a bejövő-kimenő forgalom figyelése, hirtelen megváltozása ugyancsak érdekes lehet. Egy állandó internetforgalom figyelő diagram a tálcán vagy az asztalon, illetve a tűzfal naplófájlok rendszeres ellenőrzése segíthet ilyenkor a nyomozásban.

8. A barátok, családtagok, ismerősök azt jelzik, leveleket, üzeneteket kaptak tőlünk, pedig mi nem is küldtünk nekik semmit. Ez utalhat botnetre, de emellett előfordulhat más kártevő fertőzése, illetve előfordulhat a postafiókunk feltörése is. A haladéktalan jelszó csere, és az alapos vírusellenőrzés mellett könnyen ellenőrizhetjük ez utóbbit például a Gmail esetében, ahol azt is meg tudjuk nézni, hogy legutóbb milyen IP címekről léptek be postafiókunkba.

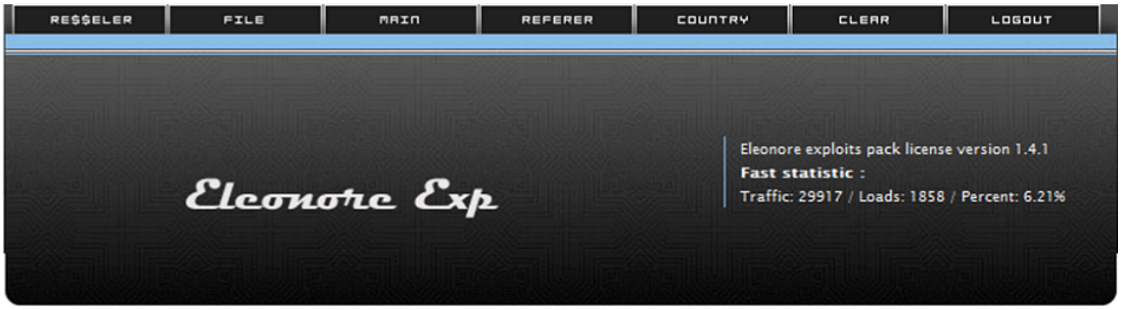
9. Hirtelen popup ablakok kezdenek el megnyílni, reklámok jelennek meg, akár úgy is, hogy a böngésző el sincs indítva. Ez a jelenség valamilyen reklámmal kapcsolatos bot kártevő jelenlétéről árulkodik.

10. A Windows Feladatkezelőben furcsa nevű programok, folyamatok tűnnek fel. Ez megint csak nem egy kizárólagos jellemző, hiszen számos hardver, illetve szoftver komponens használ ilyeneket. Sőt megfelelő programozói tudással láthatatlan folyamatok készítése is könnyen lehetséges. Ennek ellenére sokszor láthatóak ezek, és vannak igen jellegzetes nevűek, ahol könnyen következtethetünk konkrét kártevőre. Az alaposabb nyomozásban pedig jó szolgálatot tehet az ESET SysInspector modulja, amely pontosan ezekről a futó programokról, futó folyamatokról képes igen árnyalt képet mutatni, veszélyes komponensekre figyelmeztetni.

Záróra, jöhet a tanulság

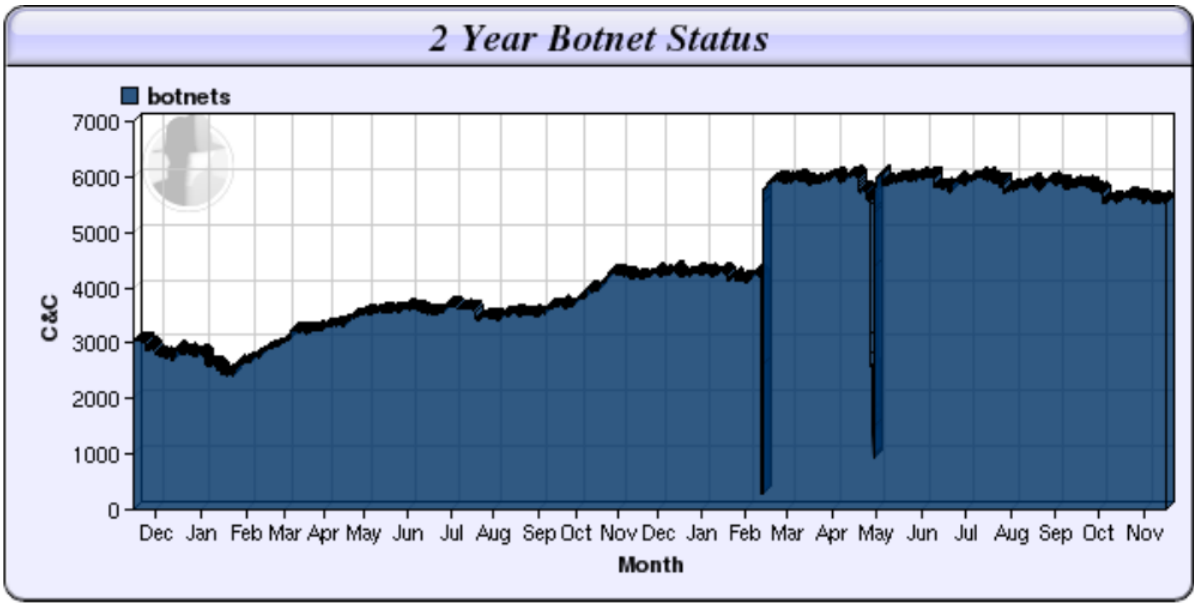
Zárásképp ha idézni akarjuk Isaac Asimov egyik híres mondását: "I don't fear computers, I fear the lack of them", akkor ennek szellemében az lehet a zárógondolat, hogy nem akarjuk, de nem is tudjuk számítógép nélkül elképzelni a jövőnket. Ezért ahogy megtanuljuk, hogyan zárjuk kulcsra lakásunkat, vigyázunk kimondott szavainkra egy idegen országban, lassan lépcsőzetesen terheljük csak összeforrt csontunkat a gyógyulás után, ugyanígy mindenkinek - igen, valóban mindenkinek - el kell sajátítania privát-szférája védelmét, számítógépének biztonságos körülményeit, valamint a különféle social engineering megtévesztések ellen való hatékony védekezést. Ehhez persze remek társ a vírusirtó vagy az internetbiztonsági csomag, de nekünk is oda kell tennünk magunkat fejben, folyamatos tanulással.

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

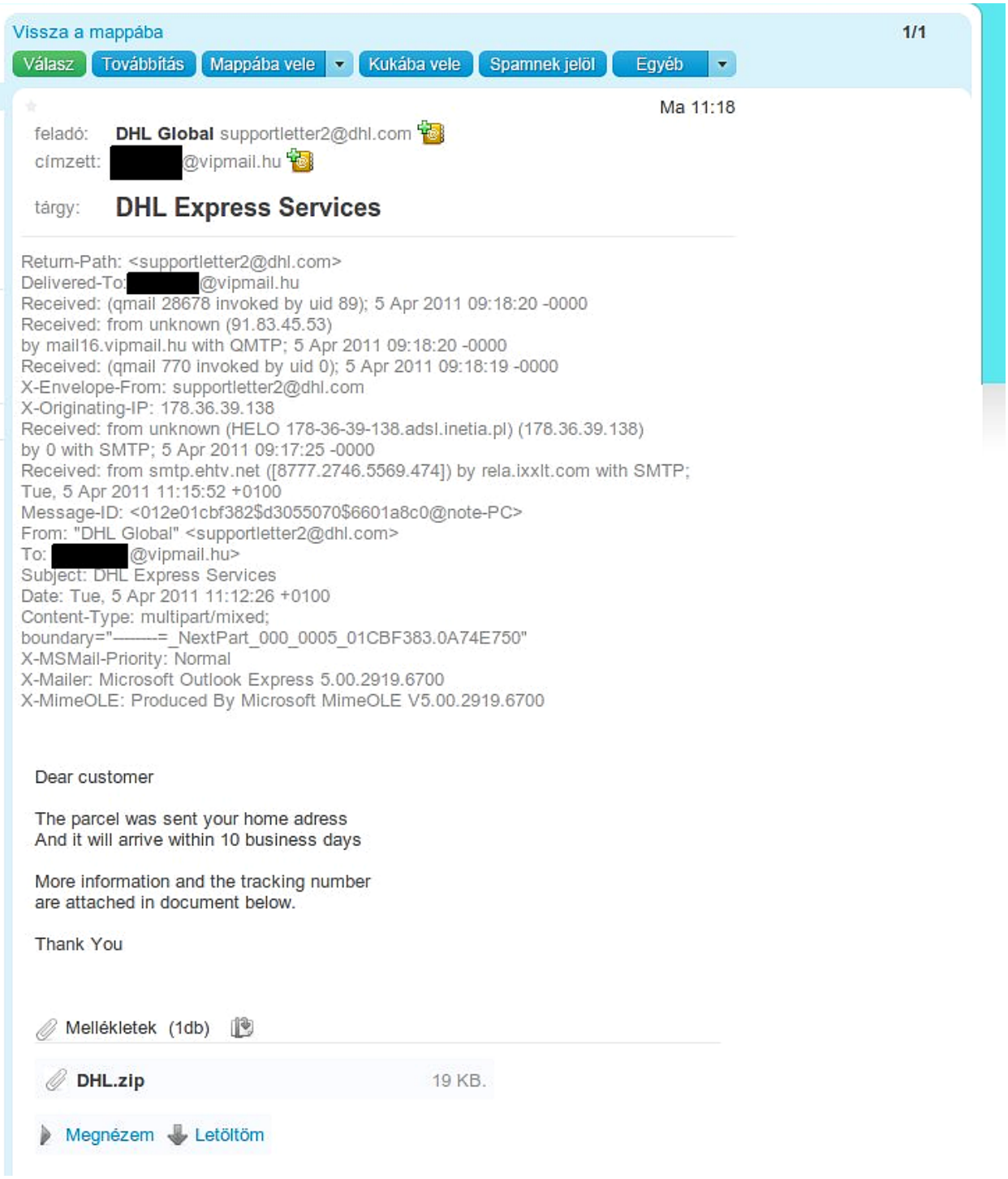


Operation Systems:	Totals:
Windows XP	23529
Windows 7	4060
Windows Vista	1585
Linux	168
Mac OS	162
Windows 2000	115
Windows 2003	111
Mobile phone	76
Unknown OS :(	25
Power PC	25
Windows 98	22
Symbian OS	15
iPhone OS	11
Windows ME	5
Windows 95	3
Bots	2
Windows NT 4	1
PlayStation	1

Az ábra az Eleonore Exploit Pack admin felületét mutatja. A megfertőzött rendszerek számának arányából lehet következtetéseket levonni arra nézvést, mely operációs rendszerek, platformok, programok a legveszélyeztetebbek

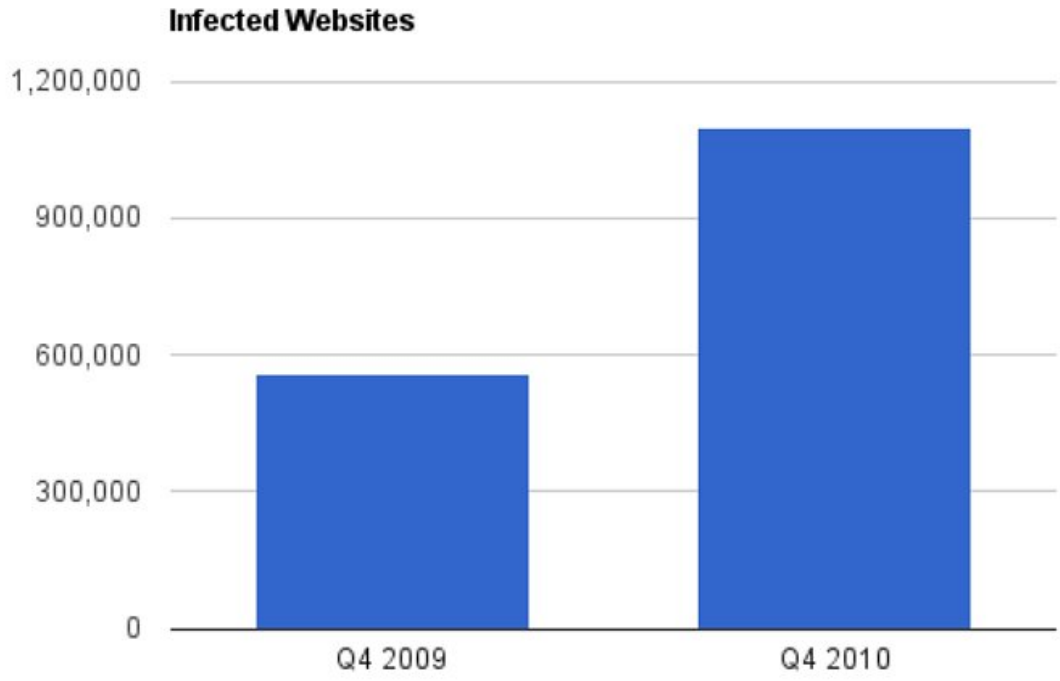


Ha a botneteket nézzük 2009 elejétől 2010 év végéig, számuk mindenféleképpen növekvő tendenciát jelez, 2011-re akár a hétezret is elérheti a különféle zombihálózatok mennyisége

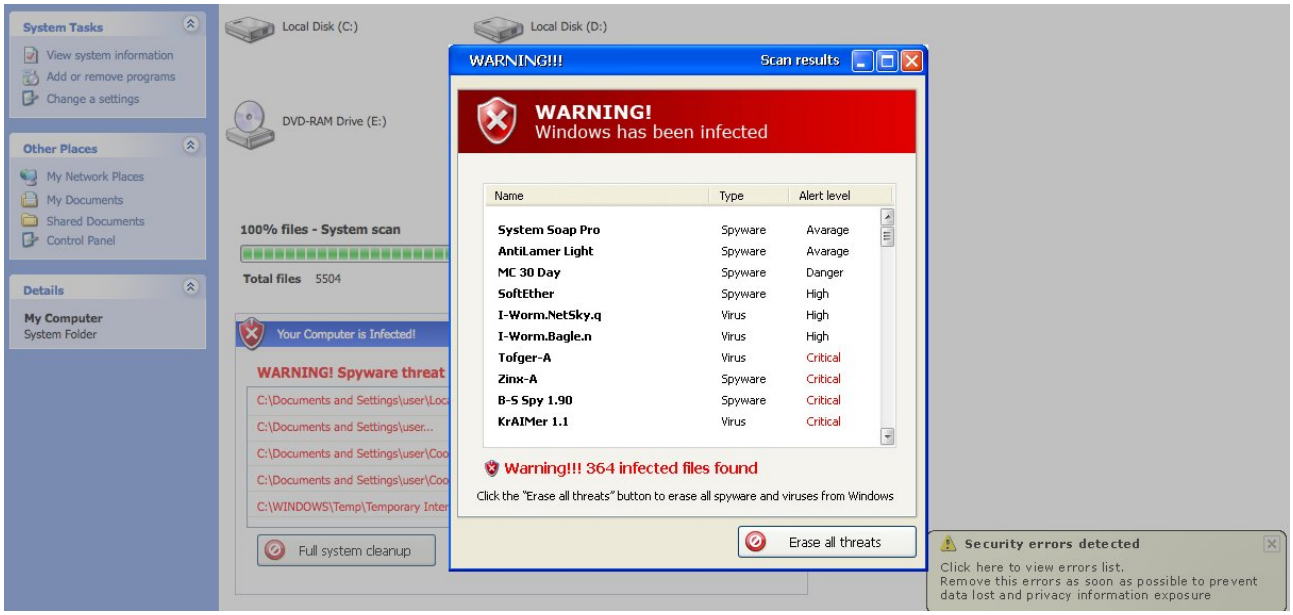


Ha olyan kéretlen levelet kapunk, amelynél csak és kizárólag a mellékletből derül ki minden számunkra fontos részlet, az már egy komoly intő jel: csalás, kukába az egésszel

Örökzöld módszer kártevők terjesztésére, hozzávalók: 1 db lenge öltözetű hölgyet ábrázoló fotó, 1 db link, 1 db Facebook kattintás, csatlakozás egy ismeretlen csoporthoz vagy lájk látatlanban még azelőtt, hogy megnézhetnénk, pontosan miről is van szó



Ha a fertőzött weboldalak számát vesszük górcső alá, a tendencia egyértelműen leolvasható: számuk egyre jobban gyarapszik



Az egyik legkellemetlenebb csalástípus a hamis antivírusok. A csalók milliókat keresnek a nem létező fertőzésre figyelmeztető programokkal, amelyek azt hazudják, 50-100 USD átutalása ellenében "megtisztítják" számítógépünket