Kell-e Macintoshra vírusirtó? Hogyan változnak a vírusok, van-e olyan vírus, ami minden platformon tud terjedni?

Manapság, ha azt olvassuk, hogy új vírus jelent meg, már senki nem kapja fel a fejét, nem rezzen össze, és ezzel egyidejűleg annak az esélye, hogy az új kártevő a Windows platformon garázdálkodik, mintegy 99 százalék. De vajon ez azt jelenti, hogy az alternatív operációs rendszerrel ellátott gépek tökéletesen védettek a kártevőktől? "Ha nagy tömegben keresünk fertőzhető gépeket, naiv júzereket, akkor irány a legelterjedtebb Windows" - ezt állítja Bruce Schneier biztonsági szakértő és hihetünk neki. Vigyázni azonban mindenütt kell valamennyire, de az kétségtelen, hogy az alternatív platformok használóinak nagyságrendekkel egyszerűbb az élete.

Alternatívák

Biztonsági szempontból a Linux is lehet jó választás, de a szintén UNIX-alapokon álló Macintosh is már egyre népszerűbb, ha munkaállomásról beszélünk. Felépítéséből adódóan nagyságrenddel biztonságosabb, mint például a Win7 előtti Windows-változatok. Például Linux és OS X alatt nem fut csak úgy minden rendszergazdai joggal, minden egyes telepítéshez be kell gépelni a rendszergazdai jelszót, és elképzelhetetlen egy olyan forgatókönyv, mind például annak idején egy XP alatt az alapértelmezetten rejtett! fájlkiterjesztéssel érkezik valamilyen fájl az Outlook Expressben, ami aztán admin jogokkal automatikusan le is fut. Mac-en vírusok inkább csak PoC, azaz Proof Of Concept, vagyis kísérleti jelleggel léteznek, inkább a trójai programok a jellemzőek, például trójai kodekcsomagok, alkalmazások, hamis telepítőkészletek. Ennek ellenére teljesen ez sem védett, már történtek kisebb-nagyobb próbálkozások: rootkitek is vannak közepes számban, de klasszikus fertőző, terjedő működőképes vírusok nem nagyon léteznek. Elképzelhető, hogy a fokozatos elterjedése miatt később e rendszer is a kártevőkészítők látókörébe kerülhet.

Frissíteni, frissíteni, frissíteni

Kihasználható sebezhetőség minden operációs rendszerben létezik. Ezeknek a réseknek a lezárása, a rendszeres biztonsági frissítések végrehajtása emiatt az egyik leghatékonyabb módszer a védekezéshez. Emellett segíthetnek külső segédprogramok is, például a RootkitHunter és Checkrootkit program is - mindkét alkalmazás a GPL-licenc alá tartozik -, ezek mind a Linux, mind pedig a Mac platformra ingyenesen elérhetők. Segítségükkel az esetleg települt rootkiteket kereshetjük meg, illetve a rendszer sértetlenségét vizsgálhatjuk MD5 és SHA1 ellenőrzésekkel kombinálva. Ha például valamilyen nem hivatalos helyről töltünk le olyan programot, amely manipulált trójai programokra cserélné le parancsainkat, szkriptjeinket, akkor ezzel azonnal észrevehetjük az illegális módosításokat. Az nem is lehet kérdés, hogy rendszerünket muszáj frissíteni, naprakészen tartani, inkább ennek technikai és időbeli nehézségei az érdekesek. De mennyire könnyű egy operációs rendszer, illetve azon belül egy számítógépes környezet frissen tartása? Ehhez hasonlítsuk össze gyorsan a három legjelentősebb OS lehetőségeit ebből a szempontból.

Mit tud a Windows Automatikus Frissítés és mit nem?

A Windows eredetiségét vizsgáló folyamat (WGA, Windows Genuine Advantege) után lehetőség van frissíteni a biztonsági javításokat. A rendszeres frissítés rendre minden hónap második keddjén, az úgynevezett Patch Thuesday napján, azaz a foltozó kedden történik, leszámítva a rendkívüli, sürgős eseteket. A biztonsági frissítések elmaradásának szempontjából sok a szűk keresztmetszet: a felhasználók elég fontosnak tartják-e, hogy megtegyék, illetve aki tudatosan lopott kópiát használ, az szándékoltan kerüli a licenc ellenőrzést is kiváltó frissítési folyamatot. A Windows-frissítések egy részéhez mindenki hozzáférhet ugyan, viszont a szintén az exploitok célkeresztjében álló Microsoft Office-nál már nem ez a helyzet. Ott csak és kizárólag a legális ügyfelek tölthetik le a biztonsági frissítéseket. És akkor ezek még csak a Windows részei, de mi van a többi szoftverrel? A többi program igencsak sokféle lehet, nem is mindig jelzik maguktól, ha elavultak, így érdemes külső program segítségét kérni. Erre a feladatra egy lehetséges jó választás a telepíthető, vagy akár

online is futtatható Secunia Personal Software Inspector, amely képes levenni vállunkról ezeket a terheket, és folyamatosan értesít a frissítésekről, sőt a letöltésüket is felajánlja, megkönnyíti. Ezt már csak azért is érdemes megtenni, mert hosszú idő óta már nem a Microsoft Office a leginkább támadott fájlformátum, hanem már a Adobe PDF állományok kerültek főképp a célkeresztbe.

Linux alatt frissíteni gyerekjáték
Igazán kényelmes viszont mindez például egy Debian vagy Ubuntu Linux alatt. Ennél egyszerűbb ugyanis már nem is lehetne. Egy gombnyomás (vagy beállítjuk, hogy automatikusan pattanjon fel egy ablak, ha érkezik frissítés) és egy az adminjelszó után, és máris naprakészen tudhatjuk az egész rendszert: tehát figyelem, nem csak az OS, de ezzel együtt minden alkalmazásunkat is. Az is nagyon jó pont, hogy mennyire informatív a folyamat – pontosan tudhatjuk, mit hagyunk jóvá, mi és miért frissül, pontosan mi történik. Nemcsak azt látjuk, hogy a KB123456 nevű nagyon fontos frissítés készen áll, hanem külön keresgélés nélkül is tudjuk, mi ez, mit csinál, melyik szoftverhez kapcsolódik, és ott a checkbox, szabadon dönthetünk, kérjük-e egyáltalán. Emellett még az is egy érdekes szempont, hogy tudtunkon kívül itt sosincs rejtett frissítés, mint például a Windows alatt.

Macintoshnál az alkalmazói programokra kell külön odafigyelni
A fentiekhez hasonlóképpen automatizált és kényelmes az OS X frissítések jövetele és kezelése is. Elfogadjuk, adminjelszót begépeljük és ennyi. Ha azonban összevetjük a Windows- és a Linux-frissítések tulajdonságaival, azt láthatjuk, hogy bár kényelmi szintje a Linuxéhoz hasonlít, de sok tekintetben a Windows rendszerrel rokon. Ugyanis bár van automatikusan felpattanó ablak, de az ebben megjelenő frissítések csak és kizárólag az Apple programjainak frissen tartását végzik: OS X, iTunes, Safari, Quick Time. A további alkalmazói programok frissen tartásáról nekünk kell gondoskodni, és azokat egyesével, manuálisan frissítgetni.

Social engineering, én így szeretlek
Ha már van ütőképes védelmi programunk, mindent naprakészen és frissen tartunk, még mindig ott a human faktor, azaz a megtévesztéssel bevihető találatok. A dolog nagyszerűsége abban rejlik, hogy minden platformon működik. Megtévesztéssel bármelyik felhasználó rávehető arra, hogy egy érdekes levélmellékletre kattintson, gyorsan megerősítse banki adatait, egy izgalmas webhelyet meglátogasson, vagy egy szükségesnek látszó külső programot feltelepítsen. Az emberi megtévesztéssel minden operációs rendszer, még a Mac OS X felhasználója is csőbe húzható. Ehhez elég egy érdekesnek látszó videót ígérni, és hozzá egy kodeknek látszó alkalmazás telepítését kérni.

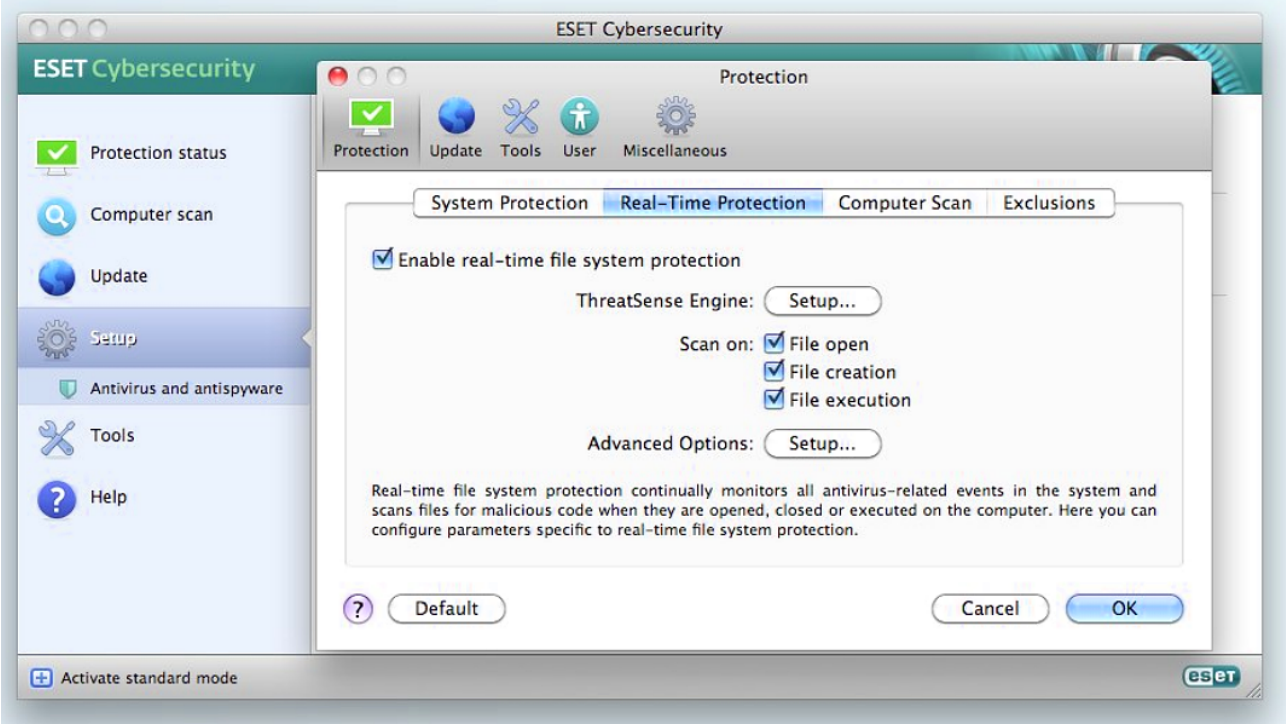
Összegezve: aki Mac-et használ, kevésbé van kitéve támadásoknak. Aki tudni akarja, mi történik a gépében, az viszont platform függetlenül őrt állít oda. Igaz, a biztonságérzetet az is fokozza, hogy a támadás gyakran a külső programokon keresztül érkezik, márpedig Mac-re sokkal ritkábban telepítenek fel bizonytalan eredetű harmadik gyártó alkalmazását, hiszen az operációs rendszerrel és a számítógéppel rengeteg szoftvert kapunk, illetve ez nagyon helyesen egyfajta bizalmi kérdés is, sokan csak az ellenőrzött Apple Store-nak szavaznak bizalmat.

Gyenge láncszemek - mire vigyázzunk
Ám mindannyian ugyanazt az internet böngésszük, ugyanazokat a közösségi hálókat vesszük igénybe, így különösen az utóbbiak jó táptalajt adnak a kártevők terjesztéséhez. Ha nem idegentől, hanem látszólag egy ismerősünktől érkezik egy üzenet, egy link, abban általában megbízhatunk - gondolják sokan. Sajnos ez egyre inkább nincs így, erre elég jó példa az "az emberek 98 százaléka nem tudja 17 másodpercnél tovább nézni ezt a videót" átverés. Ahogy a klasszikus e-mailek esetében is érdemes ódzkodni a kéretlen levelek linkjeitől, mellékleteitől, a közösségi oldalak üzeneteit is érdemes óvatosan kezelni: ha barátunk küld valamit, de nem ír semmit, csak egy linket küld, vagy nem magyarul írja az üzenetét, érdemes lehet átverésre gyanakodni. Ugyancsak gyanús az, ha valamit csak azután nézhetünk meg, hogy előtte látatlanban lájkolni kell. Ez gyakorlatilag azt

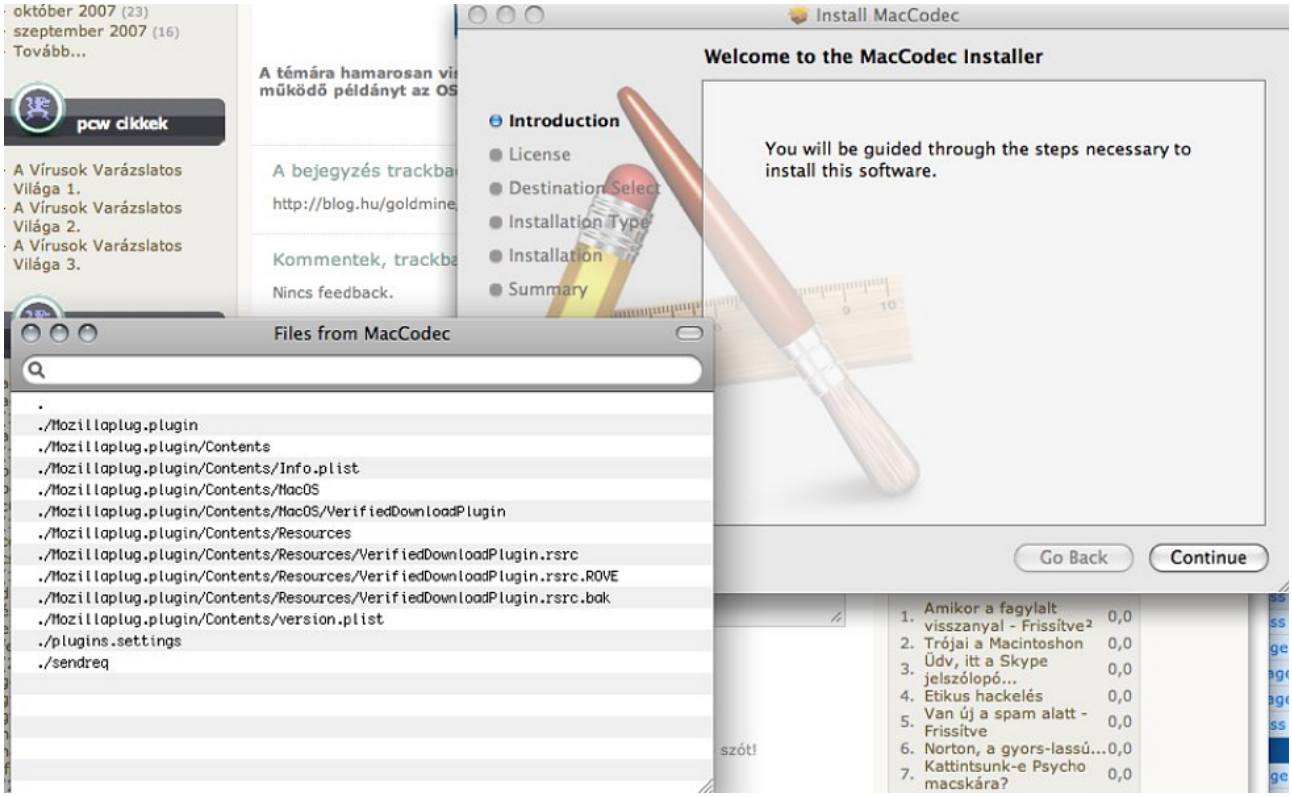
jelenti, hogy a jó biztonsági programot és a szoftver környezet naprakész frissítését minden esetben biztonságtudatos hozzáállással, rendszeres oktatással kell ötvözni, ez így együttesen adja a leghatékonyabb védelmet.

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

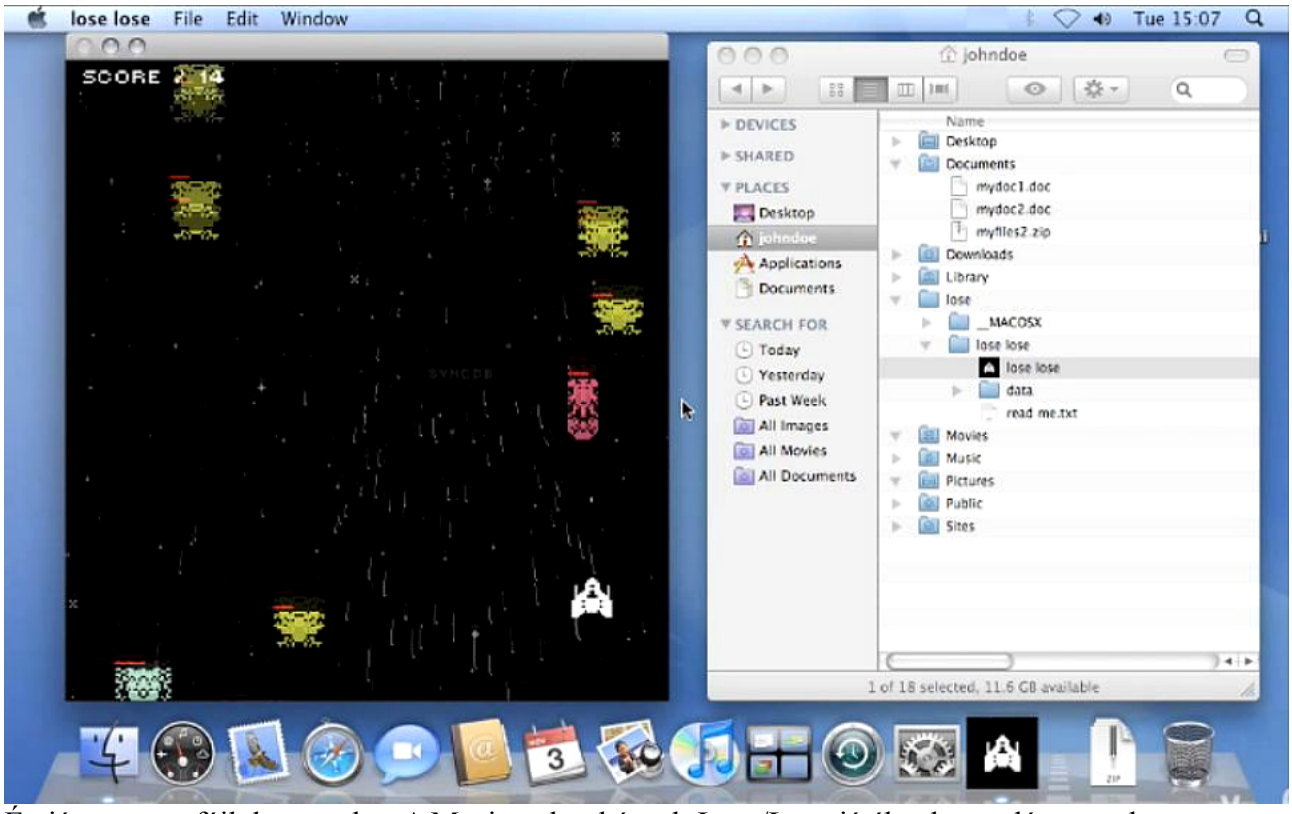
Képek:



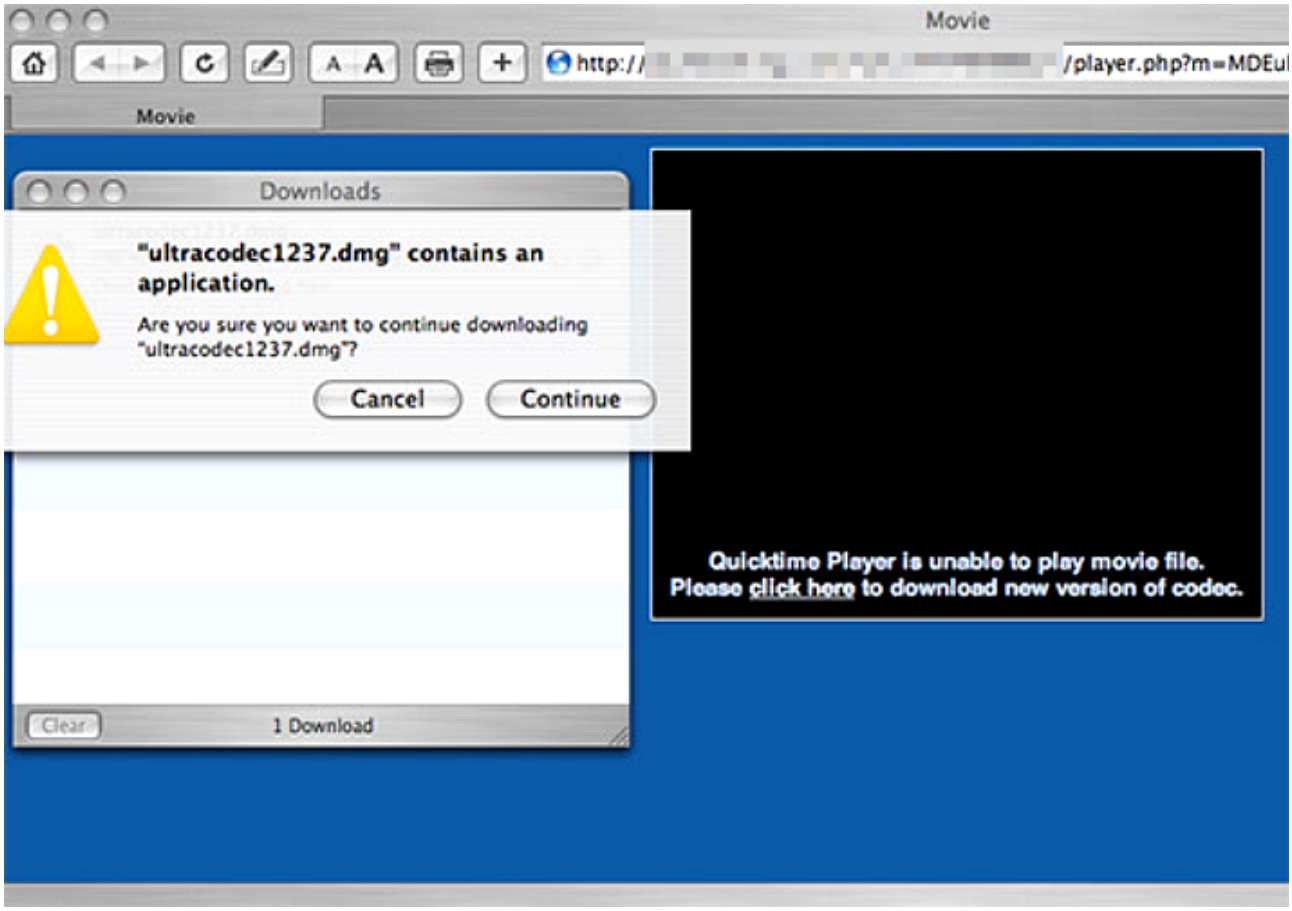
Az ESET Cybersecurity teljes körű védelmet kínál a Mac felhasználók számára az internetes kártevőkkel szemben. A szoftver nem csupán a Macintoshokra írt vírusokat állítja meg, de a Windows és Linux platformra készült kártevőket is.



Social engineering módszerrel bármely operációs rendszer felhasználója csőbe húzható. Itt éppen egy kodeknek látszó kémprogram telepítését követjük figyelemmel



Én játszom, te fájlokat törölsz. A Macintoshra készült Lose/Lose játéknak az a lényege, hogy közben véletlenszerűen fájlokat töröl a gépről. Igaz, ez a dokumentációban szerepel, de nem mindenki olvassa azt végig figyelmesen.



Egy bevált megtévesztő recept minden platformra: erotikus tartalmakat kínáló oldalon felbukkan egy üzenet, hogy a film megnézéséhez egy új verziójú kodeket kell letölteni.

Minden operációs rendszer biztonsági alapja a naprakész védelmi programok mellett a rendszeres és azonnali biztonsági frissítés.