A processzora miatt ismét a piac élvonalába került az iPad. A Speedshop szervizében szétkapva kiderült, hogy logikusabb és strapabíróbb a belseje is.

- **Friderikusz és az Appleblog**

Két éve halt meg Steve Jobs. Friderikusz Sándorral beszélgettünk az Apple alapítójának jelleméről és különcségeiről.

Következő elem

Kell-e antivírus a Macre?

- 2010.10.26. 07:50
- szucsadam
- Címkék: vírus
- 66 hozzászólás

Legutóbb 2008-ban volt napirenden ez a kérdés. Ekkor történt, hogy az Apple oldalán megjelent egy elemzés, ami azt ajánlotta, hogy valamilyen antivírus programot azért használjunk a Maceken is, biztos, ami biztos. Ezt az anyagot aztán törölte az Apple, továbbra is azt állítva, hogy a Mac úgy biztonságos, ahogy van.

Kíváncsiak lettünk, hogy állunk ezzel a kérdéssel 2010-ben, ezért egy szakértő csapattal leültünk beszélgetni, hogy megtaláljuk a végső választ: telepítsünk-e vírusirtót a Macre vagy ne? Van-e vírus Macre vagy nincs? A kerekasztalnál ült Csizmazia István vírusvédelmi tanácsadó a Sicontact külsős szakértője, az antivirus.blog.hu szerzője, Kiss Zoltán a Sicontacttól (ő a most megjelenő maces NOD32 magyarországi támogatásáért felelős), valamint Dr. Leitold Ferenc a CheckVir laboratóriumból. Ő az egyetlen az országban, aki Maces vírusok gyűjtésével, tesztelésével, leírásával foglalkozik.

A "van-e vírus Macre?" kérdés nagyjából folyamatosan vitaalapot képez a macesek körében a különféle fórumokon, a válasz előtt viszont valamit muszáj tisztázni: mi az a vírus? A vírus definíció szerint alapvetően olyan tulajdonsággal rendelkezik, mint az önmaga másolása, és saját másolatainak terjesztése állományokban vagy dokumentumokban, károkozás a gépen. Ezzel a definícióval azonban le kell számolnunk, amivel a szakemberek is egyetértenek. A vírus szót manapság a malware szinonímiájaként alkalmazzák (úgy tűnik, a szakmában is), vagyis minden, támadó céllal létrehozott kódot így hívunk. Tehát a vírusirtó kifejezés alatt egy olyan programot értünk, ami véd a vírusok mellett a férgek, a kémprogramok, az adware-ek és a rootkitek ellen is.

Ilyen értelemben egyértelműen létezik vírus a Macre. Az elsőt 1982-ben regisztrálták, ez még az Apple II-esek között terjedt, de az Elk Cloner semmilyen kárt nem okozott a rendszerben. Aztán jöttek a többiek, Dr. Leitold Ferencnek például egy néhány száz darabból álló maces vírusadatbázisa van, és ezeket a károkozókat nem laborban tenyésztették: élesben fogták őket. A legkorábbi nála tárolt támadó 1998-ból származik.

De akkor hogy lehet, hogy mégsem tapasztaljuk semmilyen jelét a vírusoknak? Hogy lehet, hogy Csaba és én is lefuttattuk a maces NOD32-t a gépünkön, és noha évek óta böngészünk védelem nélkül (szigorúan a munkánk miatt nemegyszer pornóoldalakra is tévedve), semmiféle károkozót nem találtunk? És ha ez a helyzet, minek vírusirtó Macre?

Itt kettéoszlik a tábor, és a józert kétségek között hagyják. Egyrészt az Apple kommunikációja azt sugallja, hogy a Mac abszolút biztonságos, de az évente megrendezendő hacker-versenyeken elvérző Macintoshok, a böngészőkben folyamatosan felfedezett új exploitok kételkedésre adnak okot. Másrészt itt vannak a vírusirtókat készítő cégek, akik nyilván szeretnék eladni a terméküket, éppen ezért nekik is nehezen hihetünk, amikor védtelen rendszerről beszélnek. A szélsőségek között keressünk egy elfogadható középutat.

Tény, hogy aki Macet használ, kevésbé, szinte egyáltalán nincs kitéve támadásoknak. És ez vonzó, mindannyiunknak, akik pc-ről tértünk át (sogenannte switcher), ez volt az egyik legfőbb érvünk a váltás mellett. Hogy a vírusok nemlétének mi az oka, más kérdés, viszont fontos: kevesebb a létező fenyegetés, kevesebb a féreg, gyakorlatilag alig létezik vírus, viszont vannak olyan biztonsági rések az operációs rendszerben, és ami még fontosabb, a böngészőkben, amiket kihasználva gyorsan lehet készíteni egy támadó programot vagy weboldalt. A pc és a Mac-világ már összeért, mivel mindannyian ugyanazt a webet nézegetjük - fogalmazott Leitold Ferenc. Nincs a korábbi szeparáltság, a webről érkezhet támadás bármelyik platformra.

A biztonságérzetet fokozza, hogy a támadás gyakran a külső programokon keresztül érkezik, márpedig Macre sokkal ritkábban rakjuk fel harmadik gyártó alkalmazását, hiszen az operációs rendszerrel és a számítógéppel rengeteg szoftvert kapunk. Ráadásul Kiss Zoltán szerint a Macre szebb kódokat írnak, ezen a platformon inkább szokás betartani a szabványokat, nagyobb energiákat ölnek a munkába, ugyanakkor bármikor érkezhet egy olyan, népszerű alkalmazás, ami simán átengedi majd a támadó kódot.

Akárhogy is, a Secunia 2010-es felmérése szerint a gyártók közül az Apple-nek van a legtöbb sebezhetősége, már évek óta az Oracle és a cupertinói cég vezeti a listát, a Microsoft csak a harmadik. Az is igaz, hogy a réseket az Apple folyamatosan tömi, a felhasználók meg rendszeresen frissítenek, ami további biztonságot ad a platformnak, a hackerversenyek nyilvánvaló tanulsága mégis az, hogy mindig maradnak támadási felületek.

Hogy lehet akkor, hogy nincs, pontosabban nem tapasztalható támadás a Macek ellen? Erről kérdeztük a szakértőket, akik először is azzal kezdték, hogy a támadást nem feltétlenül lehet észrevenni, a károkat okozó programok aránya egyre csökken, újabban inkább észrevétlen kémprogramok lopják el az adatokat, és adják el a jelszócsomagokat tömbönként. Dr. Leitold Ferenc maces malware-jeinek fele is trójai.

"Ha nagy tömegben keresel naiv júzereket, irány a Windows" - ezt állítja Bruce Schneier biztonsági szakértő, és ebben erősítettek meg minket a velünk szemben ülők is. Meg kell ugyanis különböztetni egymástól a social engineering támadásokat, amikor a hacker a felhasználó segítségét, tapasztalatlanságát veszi igénybe, és azokat a támadásokat, amik a böngészőben vagy operációs rendszerben tátongó lyukat használják ki.

Előbbi kevesebb energiaráfordítást igényel, és gyors sikert ígér, mert sokan frissítenek, feltelepítenek bármit, amit eléjük raknak. És amíg a Windowst használók közül egymillióan, addig a Mac-használók közül néhány tízezren kapnak csak rá a csalira a két tábor arányaiból következően, éppen ezért a hackerek inkább a Windowst választják, nem éri meg a fáradtságot a Macesek ellen támadni.

Érdekes kérdés, hogy hány százalékos piaci részesedésnél érdemes nagyobb erőforrásokat fordítani a maces vírusok írására. A Cloudmarknál dolgozó Adam O'Donnell játékelméleti szabályait figyelembe véve ha a piac 16 százaléka Macet használna, már megérné a támadás. Figyelembe véve, hogy az Egyesült Államokban a Maces gépek aránya 11, Magyarországon 1 százalék, a világpiaci részesedés meg 5 százalék köröl alakul, ennek a veszélye még nem igazán érezhető.

Éppen ezért abban az általunk megkeresett szakértők is egyetértettek, hogy felesleges riogatni az embereket. De a félelemkeltés, miszerint akár holnap jöhet egy összetett támadás a Mac-júzerek ellen, vagy a túlzott optimizmus, ami meg a rendszer támadhatatlanságáról beszél, ugyanúgy káros. A kettő közt kell keresni kell egy kapaszkodót, amit valahogy a következőképp lehetne összefoglalni.

Jelenlegi tapasztalataink szerint szerint alig vannak vírusok a Macre. Néhány száz létezik a víruslaborokban, miközben több millió nyüzsög a Windowsos gépeken. Ha azonban egyszer a Macre is megindulnak a támadások, a vírusok evolúciója nem fogja bejárni azt a hosszú utat, mint a pc-ken bejárt, éppen ezért észrevétlenül és gyorsan fognak támadni. Akit ez a lehetőség megrémiszt, annak érdemes katonát állítania az ajtók elé, ami folyamatosan frissíti a képességeit, és gyorsan reagál egy esetleges támadásra. Mert jelenleg is vannak rések az operációs rendszerben, ezeket pedig jelenleg csak gazdaságossági megfontolás miatt nem használják ki.