Publicisztika

A szerző összes írása

Csizmazia István

A támadhatatlan operációs rendszerek legendája
2014. 12. 04. csütörtök 16:00

Ha jól rémlik, még anno 2010-ben beszélgettünk Szőr Péterrel arról, hogy miért is választotta annak idején a Macintosht. Az ok prózaian egyszerű volt: mert ott nem voltak vírusok. A beszélgetés kapcsán aztán szóba került, hogy ez az állapot sem biztos, hogy örökké fog tartani, hiszen minden változik, és később ebben is történhet változás.

A kártevő készítőket egy idő után ez a platform is elkezdte érdekelni, és aztán ahogy a Mac-esek tábora nőtt, voltak már időnként sikeres próbálkozások. Elég ha csak a 2012-es 600 ezer gépet megfertőző Flashback botnetre gondolunk, vagy 2013-ból arra a valódi, érvényes Apple Developer ID-vel rendelkező trójaira, amely sikeresen kerülte meg a 10.8-as OS X egyik újdonságaként bevezetett Apple Gatekeeper Execution Prevention technológiát. Természetesen meg kell megjegyezni, még mind a mai napig sokkal olcsóbb Windows alapú PC-ket támadni, és persze ezekből létezik a legtöbb fajta - óvatos becslés szerint is több, mint 200 millió - kártevő.

A leggyakoribb témák
NSA(1) trójai(1) it-biztonság(1) kiszivárogtatás(1) adatvédelem(1) it biztonság(1) Snowden(1) fenyegetés(1) kártevő(1) Csizmazia-Darab István(1)
A rovat ajánlója
A Snowden-ügy meglepetései és tanulságai
Szülők iskolája
Meghökkentő mesék
Hosszú búcsú
Legolvasottabb cikkek
Pénzutalás mobilszámra
Felhők felett a Kék Óriás
Jócskán spórolhatnak a háztartások új számítógépekkel
Fel kéne már ébredni - helyzet van
Döbbenetes nyomtatók

Eseménynaptár

Kiemelt esemény:

December 10.
ITB Club december: Mit tartogat a mobiljövő?

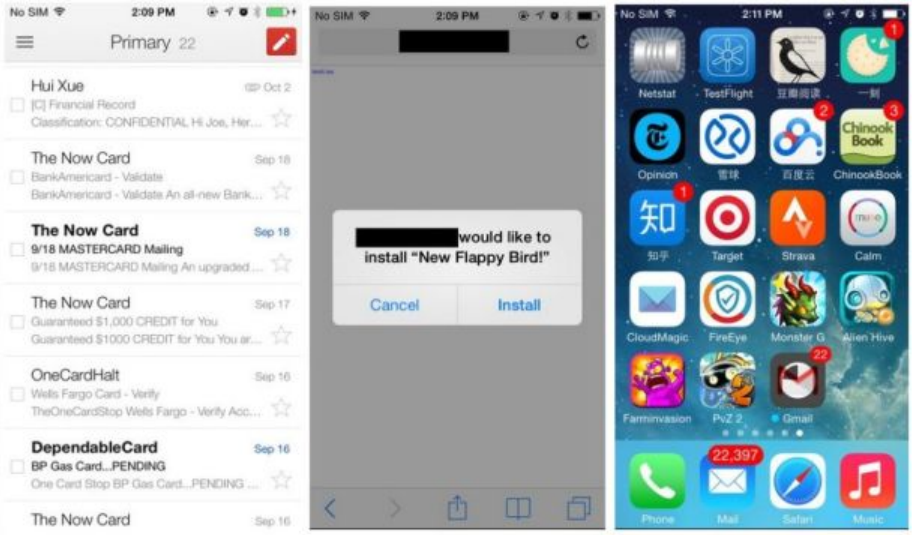
2014.
December

H	K	Sz	Cs	P	Sz	V
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Nemrégiben volt egy olyan érdekes Apple rendszerek elleni próbálkozás, amiről úgy gondoljuk, érdemes lehet szót ejteni. Az úgynevezett WireLurker kártevő ugyanis feltörés nélkül volt képes fertőzni az iPhone-okat. Ez úgy történt, hogy a kártevő az OS X alatt várta azt, hogy USB-vel rádugjanak valamilyen iOS rendszerű eszközt. Akkor aztán akcióba lépett, és a támadók észrevétlenül programot telepíthettek rá, vagy rosszabb esetben - ez a rosszabb eset a feltört eszköz használójával történhetett meg - akár bizalmas, például fizetéssel kapcsolatos adatokat lophattak el. Az Apple saját App Store-jában szerencsére nem fenyegetett bennünket ez a veszély, ezt a beszámolók szerint csak a kínai Maiyadi App Store online boltjában található alkalmazásokban észlelték.

Azt el kell ismerni, voltak és vannak időnként meglepően hatékony lépései az Apple-nek is, emlékezhetünk például, hogy az emlegetett Java sebezhetőségen alapuló Flashback kártevő megjelenése után olyan Flashback Trojan Remover Tool biztonsági javítást adtak ki, amely aztán alapból letiltotta a felhasználók gépein az esetlegesen aktív és sebezhető Java plugineket.

Nos a WireLurker esetében is hasonlóképpen jártak el, így egy gyors frissítéssel - emlékezzünk, a Mountain Lion óta ilyen csendes biztonsági frissítések naponta érkeznek - bezárta azt a lehetőséget, hogy ilyen fertőzött alkalmazást egyáltalán futtatni lehessen. Nyilván magát az eredeti biztonsági sebezhetőséget is előbb-utóbb be kell majd foltoznia, de azonnali elsősegélynek ez a technika most sem volt rossz ötlet.



Maradva az aktuális történetnél, még az a ritka szerencse is kísérte itt az utóeseményeket, hogy az elkövetőkkel szemben is sikerült fellépni, és persze a kártékony kódot tartalmazó weboldalt leállítani. Az akció kapcsán a kínai hatóságok november közepén három olyan személyt is letartóztattak, akik alaposan gyanúsíthatóak azzal, hogy részt vettek a WireLurker kártevő létrehozásában és terjesztésében.

Azt azonban mindenféleképp látni kell, hogy OS X alatt a hivatalos frissítéseket sok - elsősorban vállalati felhasználó - nem tartja elegendően hatékony kártevő elleni védelemnek, így aztán nem meglepő, hogy főképpen céges környezetben van nagyobb keletje a thirdparty védelmi szoftverek használatának. Jól ráérzett erre amúgy a Google is, aki épp a napokban bocsátott ki egy olyan Santa nevű nyíltforráskódú segédeszközt, amely egy olyan kernel kiegészítés, mellyel a felhasználói programok monitorozását lehet elvégezni. A program fő feladata a nem kívánt alkalmazások, műveletek blokkolása, ezeknek fekete, illetve fehér listák szerinti engedélyezése felhasználói értesítéssel és részletes naplózással egybekötve.

Egy szó, mint száz, összefoglalva bármely platformról vagy rendszerről is beszéljünk, legyen az akár Android, OS X vagy éppen Ubuntu Linux, ab ovo eleve száz százalékosan védett rendszer nem létezik, ezt egészen bátran kijelenthetjük. Így az egyre gyakoribb, és az alternatív rendszereket célzó támadási próbálkozások mellett a megfelelő külső védelmi programokat, megoldásokat mellőzni, vagy azokat e platformokon presztízs okokból feleslegesnek ítélni szerintünk biztonsági szempontból igen komoly hiba.

Csizmazia-Darab István, IT biztonsági szakértő
a NOD32 antivírus termékek magyarországi képviselete
antivirus.blog.hu

Címkék: Csizmazia-Darab_István, it_biztonság, trójai, kártevő, fenyegetés