Android: védeni vagy nem védeni?

2013.06.11. kedd

Ez itt a kérdés, mondhatjuk a hamleti felvetést ebben a speciális kontextusban. Bár a vélemények ebben is – mert miben nem – megoszlanak, összegyűjtöttünk pár elgondolkodtató adalékot ahhoz, hogy aztán a kellő információk birtokában mindenki maga tudja ezt eldönteni.

Az okostelefonok közül főként az Android lehet veszélyben, de persze a többi platform sem mentes automatikusan a támadhatóságtól. Igaz, nem véletlenül emelik ki sűrűn az Androidot, hiszen a 2012-es adatok alapján 56 százalékos tortaszelettel elterjedtségben a legjelentősebb szereplő volt. Az erre a rendszerre készült kártevők számának elképesztően meredek emelkedése miatt viszont az Android lett az új vadnyugat, vagy más szavakkal az új Windows.

Az úgynevezett fejlődés hozadéka például, hogy a korábban egyáltalán nem ostromlott platformokon is egyre gyakrabban érkeznek hamis antivírusok. Emlékezetes, hogy OS X alatt a Mac Defender és hasonló kártevők miatt az Apple 2012. májusában külön biztonsági frissítést kényszerült kiadni. Újabban pedig az Androidot is elérte ez a hullám, több hasonló esetről is beszámoltak már a biztonsági cégek. Persze egy valódi és egy hamis antivírus közti különbséget egy gyakorlottabb felhasználó akár azonnal észre is vesz, ám a trójai programok esetében – amelyek ugye mást csinálnak, mint amit ígérnek, vagy mást IS csinálnak – már nehezebben leplezhető le ideje korán a kártékony funkcionalitás. A gyengébb megoldásoknál közvetlenül az applikáció kódjába írják, hogy milyen számra fog emelt díjas sms-eket küldeni, vagy hívásokat indítani az alkalmazás, a kifinomultabb esetekben már távolról is folyamatosan frissíthető a lista. Az Apple viszonylag szigorúan ellenőrzött App Store-jával ellentétben a Google alkalmazásboltjába bárki tölthet fel saját fejlesztésű applikációt, és a Bouncer szisztéma szúrópróba jellegű ellenőrzése láthatóan kevés az üdvösséghez.

A trójai programok szemszögéből több területen is célkeresztbe került már az Android, egyrészt a már említett hagyományos, klasszikus emelt díjas sms-ek rejtett küldözgetésével okozhat a felhasználóknak bosszúságot és extra költségeket, másrészt a telefonról lementett adatokat – címjegyzék, fényképek, jelszavak, dokumentumok, stb. – ellopásával. Emellett jelentkezhetnek a kétfaktoros azonosítás sms-eire vadászó Zeus banki trójai változatok, ezek első megjelenését már 2011-ben észlelték. Itt azért azt is meg kell jegyezni, ha valaki ugyanarról az okostelefonról bankol, amelyre a visszaigazoló mobilaláírási hitelesítési kódot is kapja, már messze nem beszélhetünk az eredeti klasszikus kétfaktoros biztonságról, hiszen fizikailag nem két külön készüléken történik mindez.

Ha weboldalakat nyitunk meg, a hordozhatósággal kapott kényelem mellett számos szűk keresztmetszettel vagyunk kénytelenek együtt élni: a kisméretű kijelző miatt gyakori az URL helytakarékosság miatti elrejtése, ami miatt sosem lehetünk száz százalékosan biztosak benne, hol járunk pontosan: bankban vagy egy hasonmás adathalász oldalon. Nem látni, pontosan mik futnak a háttérben, nincs kontrollunk a scriptek felett, és az is elmondható, sajnos még mindig csak kevesen használnak biztonsági programot. Ha valaki pedig tűzfalat szeretne, akkor azt csak a rootolt készüléken teheti.

De ha már szóba kerül a jailbreakelés és rootolás. Nem kevés számban amiatt is alkalmazzák ezeket a módszereket, hogy a különben fizetős tartalmakat ingyen lehessen telepíteni, használni. Ha a 2013. márciusi adatokat nézzük, csak az iOS 6.x-hez tartozó Cydia letöltések száma meghaladta a 14 milliót, de hasonlóan nagy számokat láthatunk Android esetében is, ahol csak az elmúlt három hónapban 5.3 millió CyanogenMod telepítést regisztráltak. Igaz, hogy például a tűzfal itt már valóban minden forgalmat pontosan megmutat, és ha nincs gyári frissítés, akkor egyetlen lehetőség, jön a rootolás és lelkes hekkerek firmware-jeinek használata. Ebben a felállásban a bizalmunkat a gyártó helyett a feltörő kezébe helyeztük, és a kétségtelen előnyök mellett mindez másfajta biztonsági kockázatokat vet

fel.

Nevezetesen az ellenőrizetlen telepítéseknek vagyunk kiszolgáltatva leginkább, a statisztikák szerint az okostelefonos fertőzéseknek éppen ez az elsődleges okozója, veszélyforrása. Mint a fentiekből is láthatjuk, az okostelefonok védelmének tétje óriási, hiszen egyetlen óvatlan letöltés kiszolgáltathatja az összes személyes információnkat, például címjegyzékünket, sms-einket, különféle jelszavainkat, bankkártyánk adatait, és mindez igen gyorsan kézzel fogható, akár anyagi károkat is okozhat.

Emlékezetes, hogy 2012 októberében micsoda váratlan káoszt okozott az akkor felbukkant USSD távtörlési incidens. Az USSD (az Unstructured Supplementary Service Data) kódok eredeti célja, hogy a távközlési szolgáltatók távolról is támogatni tudják a telefonkészülékeket. Ilyen szerviz kód például az IMEI szám, vagy a telefonok gyári beállításainak visszaállításához használt sztring is. A biztonsági hibák viszont egyúttal lehetővé tették a kiberbűnözőknek, hogy távolról törölhessenek adatokat az androidos telefonkészülékekről, például úgy, hogy a felhasználót egy URL címre irányítják, akár közvetlenül, akár egy egyszerű szöveges üzenettel vagy QR kód használatával. A gyenge pontot bezáró ingyenes segédprogramot már másnap letölthetővé tette az ESET, és később számos antivírus gyártó elkészítette a saját alkalmazását, illetve ami még szerencsésebb, idővel többen implementálták ezt a saját antivírus, illetve mobile biztonsági csomagjaik eszköztárába.

És zárásképp még valami: emlékezhetünk, hogy számítógépes környezetben – legyen az Windows, Macintosh vagy Linux – milyen hatalmas szerepe is van a frissítéseknek, elég ha csak például az Autorun vírusra vagy az évek óta toplistás Conficker féregre gondolunk. A foltok kihasznált vagy kihasználható sebezhetőségeket zárnak be, javítják a biztonságot, ám mindez Android esetében nem igazán jól működik. Ha belegondolunk, hány gyártó, hányféle modellel, mennyi külön builddel szerepel itt, olyan hihetetlenül töredezett és kaotikus képet kapunk, ami nem csak a szoftverfejlesztőket gondolkodtatja el erősen, vajon éppen most melyik verzió(k)ra érdemes fejlesztenie, hanem nekünk, felhasználóknak is jócskán megnehezíti az életünket.

Nevezetesen, ha a szerencsés módon Google Nexus, vagy valamilyen drága, neves, például Samsung Galaxy készülékünk van, ott még reménykedhetünk a rendszeres alkalmi frissítésekben, sőt időnként új operációs rendszer verzióban is, míg a kisebb gyártók – például ZTE – jellemzően az egyszerűbb vagy régebbi modelljeinél feltörés nélkül a megvételtől kezdve örökre ugyanaz az Android változat fut, és (szinte) sosem jelennek meg hozzá EGYSZERŰEN lefuttatható gyári biztonsági frissítések. Ehhez persze akár azt is hozzáfűzhetnénk, üdvös lenne, ha a gyártó részére kötelezően elő lenne írva valamilyen fix, például 3 vagy 5 éves vállalás, garancia a szoftverfrissítésekre. Mert az még elfogadható érv, hogy az újabb OS verziók már magasabb hardverkövetelményeket támasztanak, és ezért nem upgradelhetők mindig, ám az exploitokkal terhelt "hibajavítatlanság" folyamatos, évekig tartó elviselése az átlagfelhasználóknak semmiképpen nem egy megfelelő opció biztonságunk szempontjából.

IT Business Online