Mit tudhatnak meg rólunk a mobilunkon (okostelefonunkon) keresztül

Előző cikkünkben már körbejártuk, mi is lehet kényes adat. A "mit tudhatnak meg" kérdés előtt tisztázzuk azt, hogy kikről is beszélünk. Az illetéktelen kíváncsiskodók lehetnek a különféle leplezett, de valójában trójai alkalmazások fejlesztői, és lehetnek támadók, akik lehetnek ismeretlenek a világ másik feléről, de lehetnek akár családtagok, közeli barátok, osztálytársak vagy kollégák is.

Kémek a játékban

Az első kör arról szól, hogy akárcsak az asztali PC-nken, itt is érdemes tudatosan, alaposan utánanézve kiválasztani, dönteni egy-egy telepítendő alkalmazásról. Az alkalmazásokba rejtett trójai sok mindenre alkalmas, lehet hogy "csak" kéretlen reklámokat kapunk miatta, de akár minden leütésünk illetéktelen kezekbe kerülhet. Még 2009-ben az Egyesült Államokban, Észak Karolinában zajlott per a Storm8 fejlesztők ellen, mert az ingyenesen letölthető játékaik - mint például a iMobsters vagy a Vampires Live - egy beépített hátsóajtón titokban továbbították a fejlesztőknek a felhasználó telefonszámát, illetve telefonkönyvében szereplő számokat, hogy ösztönözhessék őket a teljes változat megvásárlására. A trükk végül mégiscsak kiderült, ekkor a fejlesztők azzal védekeztek, hogy ez "véletlen programhiba volt".

Telepítek, tehát vagyok

Legyen az akár IOS, akár Android, sokszor mi magunk engedélyezzük telepítéskor a hozzáférést címjegyzékhez és egyéb erőforrásainkhoz, ezért érdemes ilyenkor résen lenni. A fenti iMobster példában valószínűleg az App Store alkalmassági vizsgálat sokkal jobban odafigyelt arra, hogy nehogy üzletileg csorbuljon az Apple üzleti érdeke, és csak kevésbé alaposan ellenőrizte az alkalmazás egyéb biztonsági vonatkozásait. Ám ha valaki azt gondolja, ez csak a zárt forráskód átka, akkor ehhez elég egy pillantást vetni az Android Marketre. Ott sokkal nagyobb számban találhatók trójai, rosszindulatú alkalmazások, ez talán annak is köszönhető, hogy ott korlátozás nélkül bárki lehet fejlesztő. Ahogy növekszik az Android népszerűsége, úgy kerül egyre jobban a kártevőszerzők érdeklődési körébe is. Lassan itt a telefonos applikációk esetében is egyre nehezebb lesz eldönteni, mi a kártevő és mi nem az, milyen funkciók gyanúsak, kétesek és legálisak. Ha csillagászati számlát kapunk kézhez, emeltdíjas SMS-ek garmadáját fogadjuk, érdemes visszagondolni, nem mi magunk engedélyeztük-e mindezt.

Feltörés, alapjelszó, alaphiba

Emlékezetes és tanulságos esetek történtek az iPhone háza táján, ahol az úgynevezett jailbreak segítségével hálózatfüggetleníteni lehetett, illetve feltörve a telefont tetszőleges program futtatására nyílt lehetőség, nem korlátozott többé az iTunes. De ha valaki már jailbreakeli a telefont, akkor illene az SSH jelszót menten lecserélni az alapértelmezett "ohshit"-ről egy egyedire. 2009-ben egy holland hacker végigpásztázta a helyi T-Mobile IP hálózatát nyitott SSH portok után kutatva, a megtalált eszközökre pedig megpróbált bejutni ezzel az alapértelmezett jelszóval. Ha sikerrel járt, egy SMS-értesítőhöz hasonló üzenetben figyelmeztette a védtelen áldozatot. Őt követte aztán 2009 novemberében egy másik PoC

kártevő szerző, aki pedig Rick Astley képeket varázsolt a távoli készülékekre. A további követők később már nem voltak ennyire viccesek és kíméletesek, szabadon garázdálkodtak a telefonokban, sőt új SSH jelszóval akár ki is zárták az eredeti tulajdonost.

Human faktor

Egy 2011. októberében ismertetett ThinLine nevű, amerikai felmérés lesújtó eredményeket mutatott arról, hogy hány ember közösségi accountját, mobiltelefonját babrálja, töri fel, kutatja át néha vagy rendszeresen egy családtag, barát, vagy éppen osztálytárs. Tíz megkérdezett fiatalból három tapasztalta már a feltörést, és a 2009-es ugyanilyen felmérés eredményével összehasonlítva az incidensek száma megduplázódott. Sajnos a fiatalok többsége mindezt jó mókának tartja, és a rendszeres zaklatástól, kémkedéstől, lehallgatástól sem riadnak vissza.

Piaci termékek is ajánlkoznak

És zárjuk a támadók lehetőségeinek tárházát egy abszolút "legális" termékkel, a Flexispy már 2000-es évek óta kínálja különféle típusú mobiltelefonokra telepíthető alkalmazását, amely mindössze évi 99 USD összeg fejében egyszerű telepítést, észrevétlen működést, továbbá teljes hozzáférést kínál a telefonhívások és SMS-ek listájához, valamint az áldozat pillanatnyi GPS koordinátáinak követési lehetőségét is ígéri, sokak szerint a legális és illegális határmezsgyéjén egyensúlyozva.

Tudom, hol jártál tavaly nyáron

Ám ha azt gondoljuk, minden fekete és fehér, és a mobil OS gyártó jó és csak azért van, hogy mindenkit megvédjen, akkor érhetik az embert meglepetések. Az Androidos telefonok már idén februárban felhívták magukra a figyelmet azzal, hogy az alkalmazások 11%-ban volt valamilyen kártékony funkció, vagy éppenséggel a felhasználók GPS adatainak illegális kikémlelése, továbbítása. Ám szemben az alkalmazások fejlesztőivel, sokszor a gyártók is okoznak csalódást. Említhetjük például azt a még 2007-ben kipattant esetet, amikor felmerült annak a gyanú, hogy az iPhone "hazatelefonál" és továbbítja az Apple szervereire a látogatott weboldalak, emailcímek, hívások adatait, ezt akkor cáfolták. Ám nem is olyan régen mindkét platform látványosan demonstrálta a gyakorlatban azt, hogyan működik az alkalmazások távoli letiltása, visszahívása módszer, idén áprilisban pedig végképp hegyomlásszerűen jöttek a dolgok: előbb az iPhone esetében bizonyosodott be, hogy már egy éve titokban gyűjti egy consolidated.db nevű fájlba a felhasználó által érintett összes GPS adatot, majd végül minden mobiltelefon platformnál kiderült ugyanez.

Spóroljunk a biztonság rovására, juhé

Az adathalászati veszély is jóval nagyobb a mobileszközökön. Mivel a kényelem és a kis kijelző miatti egyszerűsítés jegyében a böngészett URL kiírása rejtésre kerül, ez komoly veszélyeket hordozhat magában. Amint az eredeti oldal már betöltődik, és a link eltűnik, az kicserélhető egy kártevőt tartalmazó hasonló kinézetű linkre, amelynek például iPhone alatti igazi címe így rejtve marad. A felhasználó csak akkor észlelheti azt, ha és amennyiben a képernyő legtetejére scrollozva újra leellenőrzi a címsort. Mobil böngészőkliensekben már eleve nehezebb a kétséget kizáró ellenőrzése annak, hogy biztosan a hiteles, kívánt oldalon

vagyunk-e éppen. Ez tulajdonképpen minden mobilplatformon jelentkező veszély, ezért erre érdemes odafigyelni.

Eszközök profiknak és amatőröknek

Ezeken kívül léteznek már nagyon kifinomult megoldások is, például biztonsági kutatók sikeresen demonstrálták már olyan man-in-the-middle típusú, azaz két kommunikációs fél közé való beékelődéses támadást, ahol a hivatalos banki SMS aláírást is manipulálni tudták, magyarul eltéríthető volt ez a hitelesítő biztonsági üzenet. Ennek megvalósítása szerencsére nem túl egyszerű, de érdemes tudni róla.Ám sajnos léteznek olyan hétköznapi egyszerű eszközök is, amelyekkel sokkal könnyebben kivitelezhetőek különféle támadások. Erre példa az Android Network Toolkit nevű alkalmazás, ami sok tekintetben a sok vihart kavart Firesheep Firefox kiegészítőre hasonlít. A lényeg, hogy segítségével bárki képes kilistázni a közelében található nyitott hálózatokat, és a program segítségével egy gombnyomással akár támadást is tud indítani a hálózat sebezhető gépei ellen - ami lehet bármi: hagyományos PC, iPhone vagy akár egy másik Androidos eszköz.

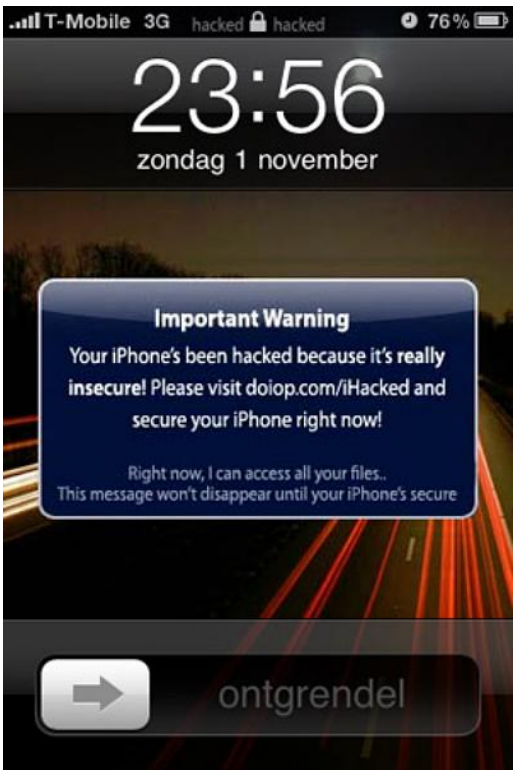
Mit tehetünk, gyorstalpaló dióhéjban

Legyen lock jelszó, vigyázzunk fizikailag is a készülékünkre, ami hamarosan pénztárcaként is funkcionálni fut. Telepítsünk lopás ellenes és vírusvédelmi programot, jegyzeteinket mindig jelszóval védve, titkosítottan tároljuk, zsúfolt helyen vagy megbízhatatlan környéken ne vegyük elő, ne lobogtassuk, jelszavunk begépelésekor gondoljunk a térfigyelő és egyéb megfigyelő kamerákra, idegen kíváncsiskodókra, ne kattintsunk kéretlen üzenetek linkjeire, ne osszuk meg pillanatnyi helyzetünket társasági oldalakon, ne jelentsük be előre, ha elutazunk, az alapértelmezett jelszó cseréjének is benne kellene lenni azoknak a széles körben alkalmazott számítógépes ismereteknek a tárházában és még hosszan lehetne sorolni, amit most nem teszünk már csak helyhiány miatt sem.

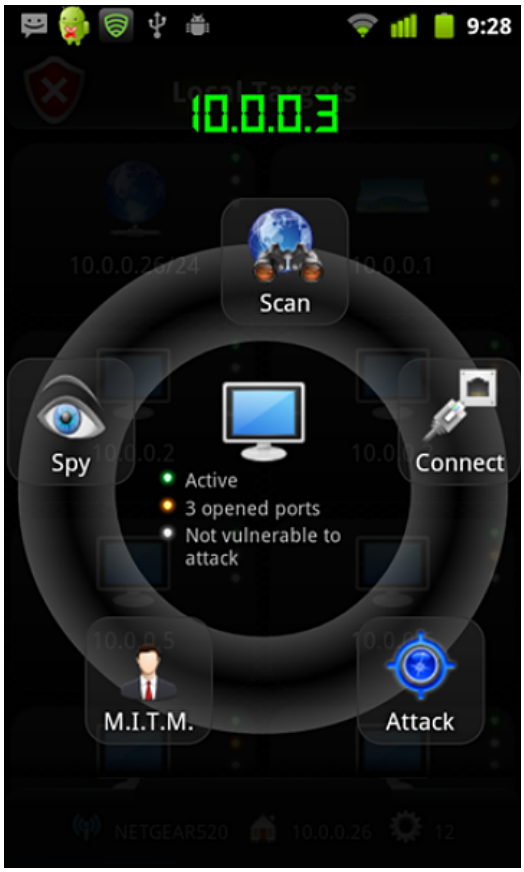
Összegezve ami fontos: védelem a mobilra, fejben meg ott lenni

Szóval jó ha van egy megfelelő védelmi program és mellé - nem helyette - szükséges a gondos odafigyelés is. Segíthet az is, ha rendszeresen olvasunk valamilyen számítógépes újságot, portált, blogot, hogy a lehetséges és aktuális veszélyekről naprakészen tájékozódjunk. A hétköznapi embereknek is mindenképpen el kell sajátítani a biztonságtudatos viselkedést, hacsak nem akarnak áldozatok vagy a digitális analfabéták lenni.

Csizmazia István, IT biztonsági szakértő
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

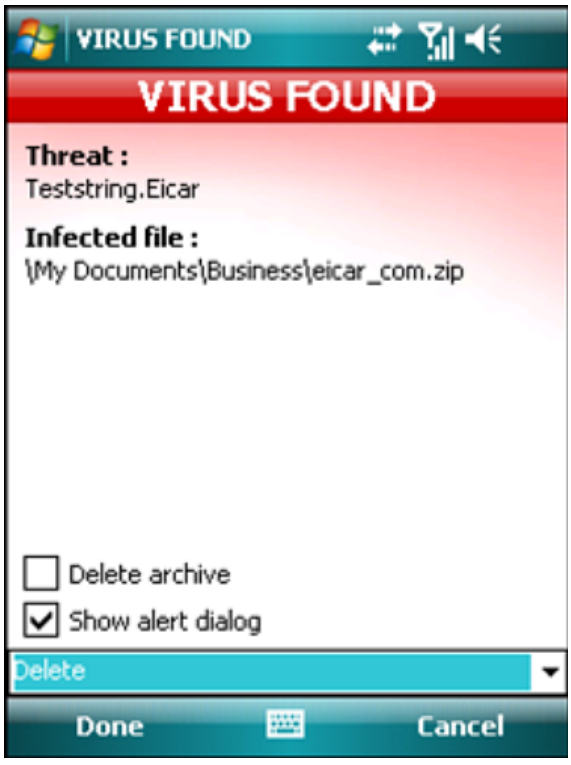


Kérlek, ha nem vagy túl elfoglalt, ugyan cseréld már le az alapértelmezett SSH jelszót, mert mások nem lesznek ilyen kedvesek, mint én.



Ha már egy szimpla menüből lehet támadást választani, akkor nem érdemes arra számítani, hogy ezt senki nem fogja a közelünkben kipróbálni

Várhatóan hamarosan Androidra is megjelenik majd a Mobile Security okostelefon biztonsági csomag



Az ESET Windows Mobile és Symbian platformra már régóta kínál védelmi megoldásokat, a képen egy Eicar teszt fájlra kapott riasztást látni