Az Android az új vadnyugat

[ORIGO] | 2012. 05. 23. 9:37

Ez a cikk 1 éve frissült utoljára. A benne szereplő információk a megjelenés idején pontosak voltak, de mára elavultak lehetnek.

3 KOMMENT

CÍMKÉK:
- android
- okostelefon
- csalás

A telefonhackerek célkeresztjében már nem a vezetékes készülékek tulajdonosai, hanem az okostelefonos felhasználók állnak. Az okoskütyük bebiztosításának óriási a tétje, mert egy figyelmetlen letöltés kiszolgáltathatja a bankkártyák adatait, és akár milliós károkat okozhat.

Néhány nap alatt csinált százmilliós telefonszámlát egy budapesti csaló, akit őrizetbe vett a BRFK - számolt be róla korábban az [origo]. Arról, hogy M. József mit követett el, milyen eszközt és technikát használt, a BRFK nem nyitatkozott portálunknak, mert nem beszélhetnek folyamatban lévő ügyről. Gombás László, a védelmi szoftvereket fejlesztő Symantec biztonsági szakértője szerint "az elkövető kölcsönös haszonszerzés fejében egy eszközt telepített a károsult készülékére".

Nehezen kivédhető a visszaélés a vezetékes telefonokkal, ha a lakóházakban lévő külső kábeleket bütykölik meg - mondta az [origo]-nak Csizmazia István, biztonságtechnikai szakértő. A szakértő szerint talán az a leghatékonyabb, ha ezt az elavult technológiát az optikai szálasra cserélik, mert azt már sokkal körülményesebb feltörni.

Az App Store biztonságosabb, mint a Google Play

Csizmazia szerint manapság már nem a vezetékes készülékek, hanem az okostelefonok a legnépszerűbb célpontjai a hackereknek. "Általában a telepített vírusok valamilyen, a hacker által beregisztrált emeltdíjas számra mutatnak, amire előre beprogramozottan folyamatosan küld szöveges üzeneteket, vagy kimenő hívásokat indít a megpiszkált telefon" - mondta Csizmazia az [origo]-nak. A szakértő szerint legtöbbször a felhasználók követnek el mulasztást, mert nem nézik meg alaposan, hogy mire is adnak engedélyt egy új alkalmazás telepítésekor.

"A gyengébb hackerek az applikáció kódjába írják, hogy milyen számra fog sms-eket küldeni, vagy hívásokat indítani az

alkalmazás" - mondta Csizmazia, aki szerint a jobbak úgy is elő tudják készíteni a csalást, hogy annak letöltéskor és telepítéskor semmilyen nyoma sincsen. "Az Android az új vadnyugat. Az Apple szigorúan ellenőrzött Appstore-jával ellentétben a Google alkalmazásboltjába bárki tölthet fel saját fejlesztésű applikációt, ez pedig nagyon kockázatos" - mondta a szakember.

Minden letöltés előtt érdemes böngészni a fórumokat

Az alkalmazásoka támadó kiberbűnözők ellen a legjobb védekezés, ha minden appnak alaposan utánanézünk, mielőtt feltelepítjük őket - mondta a biztonsági szakember. Csizmazia szerint telepítés előtt érdemes böngészni az alkalmazásokról szóló fórumokat, illetve mindenkinek ajánlott valamilyen antivírus programot telepíteni az okostelefonjára. Emeltdíjas számokat tárcsázó robotszoftverek ellen hatékony a Call Confirm nevű app, ami minden kimenő hívás előtt megkérdezi a felhasználót, valóban szeretné-e tárcsázni a számot - mondta Csizmazia, aki kéretlek szöveges üzenetek küldését kivédő alkalmazásról még nem hallott.

Kijelzi, hogy melyik kontinensről hívnak

A Call Cornfirm nevű alkalmazás az alábbi linken érhető el ingyenesen a Google Play webáruházából (korábban Android Market), iOS operációs rendszerű okostelefonra egyelőre nem elérhető. Ötös skálán eddig 4.7-es minősítésű több mint tizenkétezer felhasználó értékelése alapján. Letöltés és feltelepítés után a a szoftver minden kimenő hívás előtt megkérdezi, hogy a felhasználó valóban szeretné-e elindítani az adott hívást vagy sem.
Fizetős alkalmazások közül a Tiny Call Confim Plus-t ajánlja a legtöbb felhasználó. Az 594 forintért letölthető alkalmazás ötszáz szavazat alapján 4.6-os minősítést kapott a Google Play-ben, az előző alkalmazáshoz képest plusz szolgáltatása, hogy Google Mapsen bejelöli, hol van a kimenő vagy bejövő hívás mögött álló személy, így véd a kéretlen külföldi telefonbeszélgetések ellen.

Az egyik legnagyobb veszély, ami az okostelefonos felhasználókat fenyegetni, hogy a készülékükről átkerül egy vírus a számítógépükre és bankkártyaadatokat küld ki a csalók számára - mondta Gombás. A szakértő szerint is az androidos felhasználók a legveszélyeztetettebbek, bár elmondása alapján a Google próbál változtatni a helyzeten, és például ingyenes antivírus programot ajánlani az embereknek, de nincs könnyű helyzetben az éterben keringő körülbelül száznyolcvan vírustörzs három-négyezer mutációjával szembeni védekezés során.

QR-kódok leolvasásával is csalnak már

Az okostelefonok nemcsak letöltött alkalmazásokon és megnyitott weblapokon keresztül fertőződhetnek meg, hanem a látszólag ártalmatlannak tűnő QR-kódokon keresztül is. Az úgynevezett kétdimenziós vonalkódok tavaly ősztől terjedtek el igazán, Magyarországon is már kedvelt eszköze a marketingeseknek: a BKV-jegytől számtalan termék csomagolásán át szinte mindenhol megtalálhatóak. Itthon még nem regisztráltak visszaélést a QR-kóddal, de a Mediapost.com nevű kommunikációs lap szerint Oroszországban és Kínában már eléggé elterjedtek az ilyen esetek.

Orosz okostelefon lett a kedvencünk. Igen, orosz

A postás, aki direkt a cigánysorra kérte magát

Az orosz és kínai hatóságok szerint legtöbb esetben a felhasználók egy alkalmazást szerettek volna elérni a QR-kód leolvasásával, ehelyett viszont a vonalkód olyan linkre mutatott, ami vagy valamilyen fertőzött webhelyre mutatott, vagy az áldozat telefonjáról kéretlenül küldött hatdolláros emeltdíjas szöveges üzeneteket a csalók kontójára. Ezekben az országokban ugyanis bárki egyszerűen regisztráltathat magának emeltdíjas számot, így a QR-kódok leolvasása könnyen megszerzett pénz a bűnözők számára.

HOZZÁSZÓLÁSOK (3)

Sorrend - Legfrissebb

(3000/3000)

A belépéshez kattintson ide...

Hozzászólás »

Az Origo komment szolgáltatás felhasználási feltételei 2014. január 1-jén megváltoznak. Ha Ön ez után is használja az Origo komment szolgáltatást, ezzel elfogadja az új felhasználási feltételeket.

azimut2 | 2012-05-24 12:30:13

Azt gondolom meglehetősen felelőtlen magatartás ez mind a készülék-gyártók, mind a hálózatszolgáltatók részéről. Nem elég hogy pocsék napi alkalmazásokal telepített készülékeket, meg teletömik törölhetetlen semmire se jó alkalmazásokkal forgalmaznak (pl. SonyE. Xperia pro MK16i),még nem is biztosítják a megfeleleő védelmet. A google pay csak a készülék pinkódja alapján már le is emeli a pénzt. Persze, nem kell használni...

Válaszolok (0)

asdf | 2012-05-23 22:33:43

"Néhány nap alatt csinált százmilliós telefonszámlát egy budapesti csaló, akit őrizetbe vett a BRFK - számolt be róla korábban az [origo]. Arról, hogy M. József mit követett el, milyen eszközt és technikát használt, a BRFK nem nyitatkozott portálunknak, mert nem beszélhetnek folyamatban lévő ügyről. "
Ehhez kepest olvashato volt netszerte, hogy adattovabbitasra berelte a megkarositottak telefonvonalat a csoka amirol emeltdijas szamokat hivott (gondolom hardveres dialert helyezett ki a telefonvonalra, ezek 06 90-es szamokat hivtak, melyeknek teljesen veletlenul o volt az elofizetoje, igy az emeltdijas hivasokta kiszamlazott zseton kb. fele nala kotott -volna- ki).

Válaszolok (0)

5perc | 2012-05-23 13:23:28

"Általában a telepített vírusok valamilyen, a hacker által beregisztrált emeltdíjas számra mutatnak, amire előre beprogramozottan folyamatosan küld szöveges üzeneteket, vagy kimenő hívásokat indít a megpiszkált telefon"
Igy konfugurálva árulta tavalyig a t-mobil az intenet előfizetés nélküli okostelefonjait. Folyamatos frissítésre állították az összes alkalmazást, amik csak büdösdrága gprs-es tudtak kommunikálni. A felhasznláó nem is tudott róla. Eredmény: az első számlaküldésig 100 ezer forintos tartozás.

Válaszolok (0)