Rizici korištenja pametnih telefona

Ljubitelji pametnih telefona uglavnom koriste dva OS-a: Apple iOS na iPhoneu i Google Android na većini ostalih uređaja. U ovom ćemo se članku pozabaviti ranjivostima tržišnog lidera Androida i rizicima kojima se izlažu korisnici noseći sa sobom nesiguran uređaj.

Microsoft je kupio Nokiu kako bi uspješnije lansirao svoje Windowse na smartphoneu, a kanadski Blackberry smo već počeli zaboravljati. Upravo na tržište stiže novi takmac koji bi mogao uzeti značajan dio tržišta: Cannonical je lansirao Ubuntu Linux za pametne telefone.

Kako stvari trenutno stoje, Android je lider, u prvom kvartalu 2015. zaposjeo je 78% tržišta. Najveći dio tog kolača uzeo je Samsung, a slijede ga Kinezi s različitim markama: Lenovo, Huawei, Xiaomi itd. Appleov udio smanjio se na 18,3%, ali iPhone se i dalje dobro prodaje i ima svoje vjerne kupce koji žele posjedovati original i ne pada im na pamet kupovati "jeftine kopije". Microsoft napreduje puževim korakom, Windows phone se popeo na 2,7%.

Dakle, ako je Android ranjiv, ranjiv je najveći broj pametnih telefona! Radi toga smo se pozabavili sigurnošću tog popularnog uređaja. Malo guglanja i zapljusnuo nas je *tsunami* članaka o nesigurnosti te platforme. Pa hajdemo redom.

Preko 600 miliona korisnika Samsung Galaxy telefona, uključujući i najnoviji S6, koriste Samsungovu aplikaciju SwiftKey IME, koja dolazi predinstalirana i ne može se deinstalirati. Ta aplikacija povremeno kontaktira server pitajući za novu verziju, a promet, gle čuda, nije kriptiran! Ukoliko ste na WiFi mreži, napadač to može iskoristiti za Man in the middle napad. SwiftKey ima visoke privilegije koje napadač može iskoristiti da bi na telefon instalirao maliciozni softver, a uz to ima pristup mikrofonu, kameri, GPS-u, može čitati poruke, prisluškivati razgovore, ukrasti fotografije, poruke itd its. Ukratko, ako se Samsungovim pametnim telefonom spojite na neku nesigurnu WiFi mrežu, izlažete se riziku da vam neki zločko preuzme upravljanje vašim telefonom. Ne vjerujete? Pogledajte video demonstracije s nedavne BlackHat [1] konferencije u Londonu.

Ako vaš telefon ima instaliran Android 4.3 Jelly Bean ili neku raniju verziju, onda koristite ranjivi web preglednik WebView. Android KitKat 4.4 i Lollipop 5.0 koriste noviji preglednik zasnovan na Chromeu, pa nisu ranjivi. Milioni ljudi koriste starije, verzije pa bismo očekivali da će Google izdati zakrpe. No u Googleu su to glatko odbili, prepustivši proizvođačima telefona i korisnicima da se sami nose s tim problemom.

WebView je ranjiv na *Cross site scripting* (XSS), ali ako se ovo kombinira s XSS ranjivošću na Googlovom app-storeu, *crackeri* dobijaju mogućnost da potiho, bez korisnikova pristanka, na uređaj instaliraju softver po želji. Ako se umjesto WebViewa koristi neki drugi preglednik, moguće je da je i on ranjiv na XSS, pa opet vrijedi isti scenarij. Više na ovom linku [2].

Nedavno je otkriven trojanac za Android koji je nazvan PowerOffHijack [3]. Trojanac radi ovako: kad pritisnete tipku za gašenje, vidjet ćete animaciju koja glumi gašenje, ali telefon zapravo radi i dalje. Napadač može snimati fotografije, prisluškivati korisnika, ili mu nabiti račun šaljući poruke i nazvajući prekooceanske brojeve. Trojanac se najprije pojavio u Kini, gdje su korisnici skinuli inficirane aplikacije sa lokalnog app storea. Ako vam je mobitel zaražen, preporučuje se da izvadite bateriju, ponovo ga uključite i zatim deinstalirate sve nepotrebne aplikacije. Savjetuje se da aplikacije skidate samo s originalnog Googleovog dućana, te da instalirate neki antivirusni program..

Kad već spominjemo Kinze, evo još jedne zanimljive vijesti. Otkriveno je da se neki mobiteli

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

proizvedeni u Kini isporučuju s predinstaliranim špijunskim softverom. Star N9500, popularni jeftini kineski mobitel, isporučuje se s predinstaliranim Trojancem Uupay.D, koji se pretvara da je inačica Google Play Storea. Uz ostale funkcije, omogućuje uključivanje mikrofona i pretvaranje mobitela u "bubu" koja napadaču prenosi razgovore u blizini mobitelja čak i kad se ne telefonira,.Trojanac je ugrađen u *firmware* i ne može ga se ukloniti. Više na ovom linku [4].

Nije, čini se, bezražložna odluka američkih vlasti da državnim službenicima zabrani korištenje mobitela proizvedenih u Kini. Domaći *spyware* ih pri tom ne brine nimalo, samo strani.

Idemo dalje. Uber je najveća taksi tvrtka na svijetu koja nema ni jedan taksi. Radi se usluzi pomoću koje korisnici njihove aplikacije koji imaju automobil mogu ponuditi usputan prijevoz korisnicima bez automobila. Na primjer, idete poslom u Rijeku, oglasite to na Uberu, a onda vas kontaktira netko kome baš treba prijevoz do Karlovca. Zgodan način da podijelite troškove puta pa se isplati objema stranama. Naravno, ne isplati se taksistima koji su prestravljeni mogućnošću da se Uber pojavi i na našem tržištu. Mreža će ih pobijediti! No ovdje spominjem Uber iz drugog razloga. Nedavno je napravljen reverzni inženjering Uberove aplikacije, pri čemu je otkriveno da je taj program pravi pravcati spyware! Na ovom linku https://news.ycombinator.com/item?id=8660336 možete naći popis podataka kojim aplikacija pristupa i šalje ih tvrtki. Praktički ste Uberu dali sve informacije sa svog telefona. Tvrtka je izdala priopćenje u kojem kaže da prikupljaju te informacije kako bi korisicima pružili bolju uslugu. Uostalom, kažu iz Ubera, sami ste odlučili instalirati tu aplikaciju, a mnoštvo je drugih aplikacija koje na isti način prikupljaju informacije, pa Uber nije nikakva iznimka.

Wow! Zapravo su na neki izopačen način u pravu: nedavno sam instalirao aplikaciju koju mi je banka ponudila za mobilno bankarenje. I ta aplikacija, da bi radila, traži pristup svemu i svačemu. Oklijevao sam trenutak prije nego sam to prihvatio. Ako želiš plaćati račune mobilnim telefonom, aplikacija mora imati pristup kameri i datotekama. Da li će banka usput pregladavati i ostale moje fotografije, koje nemaju veze s bankarenjem? To je rizik koji možete ili ne morate prihvatiti. Možete lijepo stati u red i obaviti posao na šalteru. Odluka je vaša.

Ovako bismo mogli nastaviti u nedogled. Ali mislim da će biti dovoljno ovih nekoliko primjera. Ranjivi su OS-ovi, ranjive su aplikacije, ranjivi su web siteovi, a k tome nas još svi skupa špijuniraju i prikupljaju naše podatke. Zakonska regulativa se trudi zaštiti građane, ali regulativa obično kasni, zakonodavci naknadno reagiraju na zloporabe nakon što se one otkriju, a procedure donošenja zakona su spore i komplicirane, podložne lobiranju interesnih grupa, među kojima su i one koje zastupaju interese protivne zaštiti privatnosti. Nama običnim korisnicima ne preostaje drugo nego donijeti "informiranu odluku". To bi trebalo značiti da prije odluke imamo na raspolaganju sve informacije, da bismo mogli odvagnuti dobrobiti i rizike pa odlučiti što možemo prihvatiti a što ne. Ovako, svi vole nove igračke, ne razmišljajući previše o rizicima.

Osobno, nadam se da će se pojaviti OS s kojim ćemo imati bolju kontrolu nad uređajem nego što to je slučaj s Androidom i iOS-om. Možda će to biti Ubuntu? Vidjet ćemo.

pon, 2015-07-13 08:17 - Aco Dmitrović**Kategorije:** Sigurnost [5]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1560

Links
[1] https://youtu.be/uvvejToiWrY
[2] http://thehackernews.com/2015/02/hackers-can-remotely-install-malware_12.html

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

[3] http://now.avg.com/malware-is-still-spying-on-you-after-your-mobile-is-off/
[4] http://thehackernews.com/2014/06/chinese-android-smartphone-comes-with.html
[5] https://sysportal.carnet.hr/taxonomy/term/30

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr