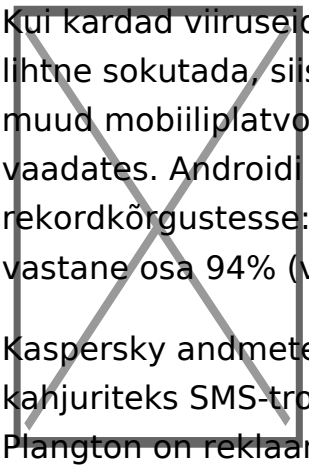
Spioonid ja viiruseloojad keskenduvad Androidile

13 aastat tagasi - 14.03.2013 Autor: AM



Kui kardad viiruseid ja nuhkimist ning usud, et mobiilidesse on viiruseid juba üsna lihtne sokutada, siis hangi mobiilile viirusetõrje või kasuta Androidi asemel mõnda muud mobiiliplatvormi, kõlab lihtne soovitus 2012. aasta viirusteülevaadet vaadates. Androidi osa mobiiliviiruste ja pahalaste levikus jõudis eelmisel aastal rekordkõrgustesse: 2012. aasta mobiilsest pahavarast moodustas Androidi-vastane osa 94% (võrdluseks: 2011. aastal oli see näitaja 65%).

Kaspersky andmetel olid petturite seas kõige populaarsemateks Androidi kahjuriteks SMS-troojalased. Teisel kohal asuvad Plangtoni ja Hamobi moodulid. Plangton on reklaamimoodul, mis teeb lisaks ka väikseid sigadusi, näiteks vahetab mobiilibrauseril avalehekülje. hamob on pealtnäha tavaline mobiiliäpp, kuid peale installi selgub kasutaja hämminguks, et see näitab vaid reklaame. Osad rakendused näivad olevat Androidi nn turvaäppid kõlavate "Security Suite" nimedega, kuid tegelikult on vastupidi - troojalased või infonäppajad.

Kolmandasse rühma kuuluvad Lotoori exploitide modifikatsioonid, mis võimaldavad juurdepääsu Androidi eri versioone kasutavatele nutitelefonidele.

2012. aastal levisid laialt ka mobiilsed pangatroojalased. Suurim osa nendest ohtudest oli samuti sihitud Androidi platvormi pihta. Mobiilsed troojalased püüavad pangatehingute autoriseerimise SMS-sõnumeid ja suunavad neid otse küberkurjategijatele.

Robotvõrgud ründavad

Mobiilsete robotivõrkude ilmumine eksperte ei üllatanud, kuna selle ohu esimesed nähud avastati juba kolm aastat tagasi. Kuid 2012. aastal tuvastati nende kõige ulatuslikum levik Androidi platvormil eri maailma riikides. Näiteks robotvara Foncy suutis Kaspersky andmetel Euroopas nakatada üle 2000 seadme, tagaukseprogramm RootSmart muutis aga pahavararobotiks üle saja tuhande nutitelefoni. Nimetatud ja ka muu pahavara töötas sama skeemi järgi: koostöös SMS-troojalastega saadavad nad nutitelefoni omaniku teadmata laiali sõnumeid

tasulistele numbritele. Ainuüksi Foncy loojad said sellise skeemiga teenida ligi sada tuhat eurot.

IOS sai ka oma pahalased

Juulis avastati ka esimene pahavara IOS-i App Store´is, seega pole ka Apple´i toodete kasutajad sajaprotsendiliselt immuunsed. kahtlase äppi nimi oli Find and Call, mis ilmus samal ajal ka Androidi rakendustepoodi. rakendus tahtis teada kasutaja e-posti aadressi ning telefoninumbrit ja seejärel saadeti andmed koos telefoniraamatu sisuga küberpättide serverisse.

Kübernuhkimine kolis ka mobiilidesse

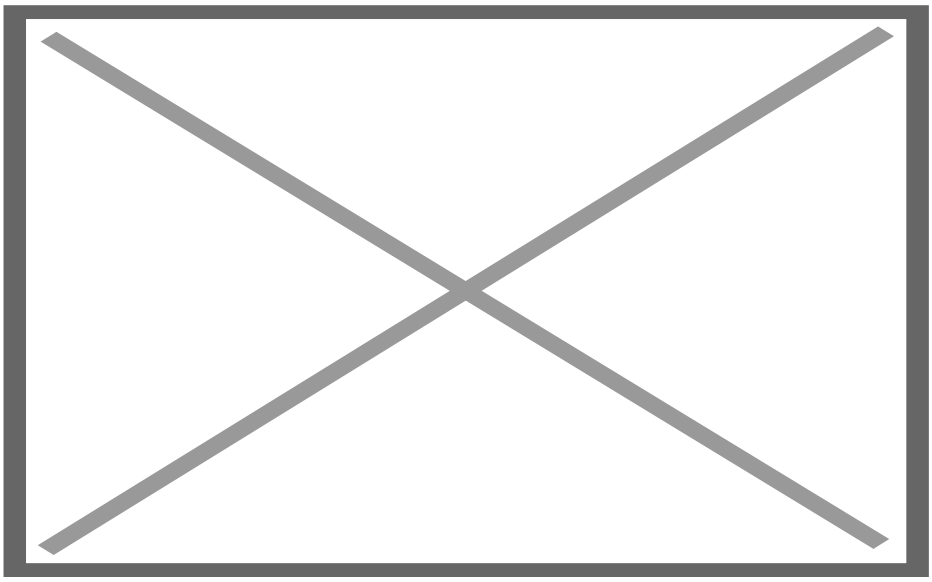
Üldkokkuvõttes oli üks 2012. aasta olulisi avastusi kinnitus asjaolule, et küberluure tarkvara kogub andmeid mitte ainult arvutitelt, vaid ka mobiilseadmetelt.

Küberluure operatsiooni „Punane oktoober” uurimisel said Kaspersky Labi eksperdid kinnituse, et pahavara üritab koguda ka rünnatavalt mobiilseadmelt selliseid andmeid nagu kõnede nimekiri, SMS-sõnumid, kalendri ja märkuste sissekanded, internetis surfamise ajalugu ning mitmesugused teksti- ja graafilised failid. Kõik see toimus ainult ühe operatsiooni raames.

Androidipõhised rünnakutarkvarad peidavad end tihti ka turvasertifikaatide pakkuja või mobiili turvatarkvara nimetuse taha. Nuhkimistarkvarad Zeus- ja SpyEye-in-the-Mobile (ZitMo ja SpitMo) peidetakse tihti niimoodi pealtnäha kahjututesse rakendustesse.

Võib kindlalt öelda, et mobiilsete küberkuritegude ajalugu sai tõeliselt rahvusvaheliseks: pahavara loojad ründasid aasta jooksul nutitelefonide omanikke mitte ainult suurimates riikides, vaid ka paljudes teistes maades. Küberluure levikuga tungis selline pahavara ka mobiilsesse keskkonda ja seda võib ühtlasi nimetada uue ajastu alguseks.

Sellised olid enamlevinud pahalased mobiilidele 2012. aastal:



PILDID: Kaspersky Lab

- Uudised

- Turvalisus
- Mobiiltelefonid
- Androidiblog