Gooligan murdis sisse rohkem kui miljonisse Google´i kasutajakontosse

9 aastat tagasi - 09.12.2016 Autor: AM

Massirünnak nimega Gooligan sai novembri lõpus hakkama enam kui miljonisse Google´i kasutajakontosse sissemurdmisega. See number kasvab pidevalt tempoga ligi 13 000 kontot päevas. Gooligan on uus variant Androidi pahavarast, mille avastasid Check Pointi uurijad SnapPea mobiilirakendusest eelmisel aastal.

Check Pointi uuring näitab, kuidas pahavara käivitub nakatunud seadmetes juurprogrammina ja varastab autentimismärgiseid, mida saab kasutada teenuste Google Play, Gmail, Google Photos, Google Docs, G Suite, Google Drive jt andmetele ligipääsuks.

Giedrius Markevicius, Check Point Balti piirkonna juht: „Praegustel andmetel kuulub 9% nakatunud kontodest Euroopa kasutajatele. See tähendab aga ligi 100 000 kasutajakontot, mis on siin piirkonnas nakatunud. See arv ei tundu esialgu väga suur, aga kasvab pidevalt. Gooligan levib kõige enam Aasias ja Ameerikas. “

Ohtlik ongi nimetatud pahavara just sellepärast, et levib väga kiiresti: Gooligani rünnakud nakatavad iga päev 13 000 mobiilseadet. Rünnatakse seadmeid, millel on Android 4 (Jelly Bean, KitKat) või Android 5 (Lollipop), neid versioone kasutavad praegu ligi 74% kõigist Androidiseadmetest. Seega, kui kasutate vanemaid Androidiga nutitelefone ilma võimaluseta uuendada seda mobiilitootja või mobiilioperaatori kaudu, olete suures ohus.

Soovitused turvalisusekspertidelt

- Uuenda alati oma seadme operatsioonisüsteemi kohe, kui see on võimalik.
- Väldi kolmandate osapoolte rakendustepoode, kui võimalik. Kontrolli võltsprogrammide nimekirja järgi, kas mõni soovitud rakendustest on Gooliganiga nakatunute nimekirjas.
- Ole väga ettevaatlik mistahes rakenduse installimisel saadetud veebilingi või avaliku QR koodi kaudu.

- Jälgi oma seadme akukasutust ja andmesidet. Kui andmekasutus suureneb järsult ja aku tühjeneb märgatavalt kiiremini, võib see olla märk pahavaraga nakatumisest.
- Mõelge ka oma mobiilseadme kaitsmisele turvatarkvaraga, nii nagu teete seda oma laua- või sülearvutis.

Rohkem infot blogis, sealt leiab ka nakatunud rakenduste nimistu.

Check Point võttis Gooliganist teada saades ühendust Google´i turvaüksusega ja andis neile kogu teadaoleva info rünnakute kohta. Praegugi tegutsetakse koos Google´iga, et leida ühiselt üles Gooligani rünnakute allikas.

„Me hindame väga Check Pointi uurimistööd selle rünnaku avastamises ja koostööd Google´iga," ütles Google´i Androidi turvalisuse osakonna direktor **Adrian Ludwig**. "Pingutame, et kasutajaid kaitsta Ghost Pushi pahavaraperekonna rünnakute eest. Selleks oleme parandanud nii Androidi operatsioonisüsteemi turvalisust kui ka üldse kogu Androidi keskkonda."

Kes on mõjutatud?

Gooligan ohustab seadmeid, millel on vanema põlvkonna operatsioonisüsteemid Android 4 (Jelly Bean, KitKat) või Android 5 (Lollipop). Neid versioone kasutavad praegu üle 74% kõigist Androidiga seadmetest, millest 57% asuvad Aasias ja 9% Euroopas.

Avastatud on kümneid võltstarkvarasid, mis on pahavaraga juba nakatunud. Kui olete alla laadinud mõne rakenduse, mis on ära nimetatud blogipostituse lõpus asuvas lisas A, siis võib seade olla nakatunud. Oma paigaldatud rakendusi saab vaadata seadmes menüüst "Settings -> Apps". Kui seal leidub mõni nimetatutest, tasub tõsiselt mõelda mobiilse seadme antiviiruse paigaldamisele – näiteks Check Point ZoneAlarm suudab kontrollida, kas seade on nakatunud.

Sajad e-posti aadressid, mis on nakatunute hulgas, kuuluvad ettevõtetele.

Kuidas teada saada, kas Google´i kontole on sisse murtud?

Seda, kas kontole on sisse murtud, saab vaadata vastavalt veebilehelt.

Kui Google´i kontot on rünnatud, tuleks ette võtta järgmised sammud:

- Vajalik on operatsioonisüsteemi puhas install seadmele (nn "flashing"). See on keerukas protsess, mida tavakasutaja ei pruugi osata. Soovitame oma seadme välja lülitada ja viia tehnilisele spetsialistile või oma

mobiilioperaatori esindusse, kus tuleks paluda seadme tarkvara täielikult taastada tehaseseadetes, teha nn “re-flash”.
- Pärast seda tuleks oma Google´i konto salasõna kohe ära vahetada.

Kuidas Androidiga seadmed nakatuvad?

Gooligani pahavara programmikoodi on leitud kümnetest pealtnäha täiesti normaalsetest mobiilirakendustest, mida saab mõnest kolmanda osapoole Androidipoest. Sellised rakendustepoed on üsna atraktiivsed, sest pakuvad paljusid muidu tasulisi rakendusi ilma rahata. Samas pole turvalisus neis poodides nii hea, kui ametlikus Google Play poes.

Gooliganiga nakatunud mobiilirakendusi võib telefoni sattuda ka spämmikirjade ja SMS-ide või teiste sõnumikeskkondade kaudu.

Check Pointi uurijad avastasid pahavara Gooligan koodi eelmisel aastal näiteks mobiilirakendusest SnapPea. Eelmisel aastal avastasid selle pahavara ka mitmed turvatarkvara tootjad ja pidasid seda pahavaraperekondadesse Ghostpush, MonkeyTest ja Xinyinhe kuuluvaks. 2015. aasta lõpust alates aga polnud enam sellest pahavarast midagi kuulda kuni 2016. aasta suveni, kui pahavara ilmus uuesti välja hoopis keerukama struktuuriga ja võimega nakatada oma koodiga Androidi süsteemiprotsesse.

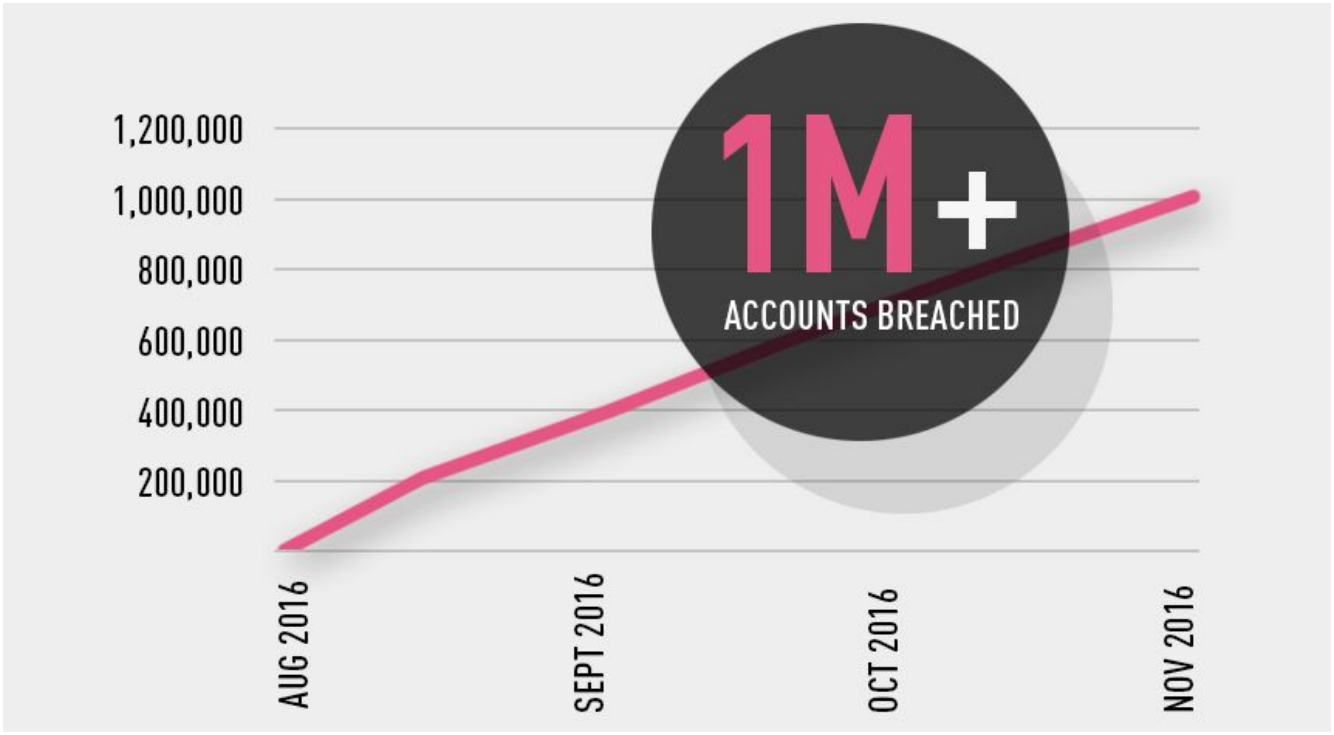
Pahavara tööpõhimõtte muutumine on tänaseks aidanud ründeid finantseerida ka kahjulike reklaamikampaaniatega. See nimelt simuleerib vajutusi reklaamidel ja sunnib kasutajaid uusi rakendusi seadmesse installima. Kui vastav rakendus on installitud, saab ründaja selle eest tarkvara loojalt tasu.

Check Pointi kogutud logiteadete järgi installib Gooligan end iga päev vähemalt 30 000 seadmesse, kogu ajaloo jooksul on pahavara end paigaldanud ligi kaks miljonit korda.

- Uudised

- Turvalisus

Pilt


1,200,000
1,000,000
800,000
600,000
400,000
200,000
1M+
ACCOUNTS BREACHED
AUG 2016
SEPT 2016
OCT 2016
NOV 2016