Punane Oktoober - ülemaailmne riikide järgi nuhkimise võrgustik

11 aastat tagasi Autor: AM

Vene päritolu turvatarkvarafirma Kaspersky Lab avalikustas äsja aruande uuringu kohta, mis käsitleb mastaapset küberkurjategijate korraldatud eri riikide diplomaatiliste, valitsus- ja teadusasutuste jälitamise kampaaniat üle maailma koodnimega *Red October* ehk Punane Oktoober.

Kurjategijate eesmärk oli saada salainfot, mis avaks ligipääsu arvutisüsteemidele, isiklikele mobiilseadmetele ja korporatiivvõrkudele ning aitaks koguda geopoliitilisi andmeid. Põhirõhk oli suunatud endise NSV Liidu vabariikidele, Ida-Euroopa riikidele ning mitmele Kesk-Aasia riigile. Muuhulgas sattusid rünnaku alla ka Läti ja Leedu diplomaatilised esindused, Eesti esinduste ründeid ei leitud.

2012. aasta oktoobris Kaspersky Labis turvajuhtumeid uurides avastatigi laiaulatuslik küberjälituse võrgustik, mille analüüsi tulemusena jõudsid eksperdid järeldusele, et Punane Oktoober sai alguse juba 2007. aastal ja kestab tänapäevani.

Küberkurjategijate põhisihiks said diplomaatilised ja valitsusstruktuurid üle maailma. Samas leidub ohvrite nimekirjas teadusuuringuinstituute, energeetikaga, sh aatomienergiaga tegelevaid ettevõtteid, kosmoseagentuure ning kaubandusettevõtteid.

Punase Oktoobri loojad töötasid välja oma pahavara: sellel on unikaalne moodularhitektuur, mis koosneb kahjurlaiendustest ehk andmevarguseks mõeldud moodulitest.

Kaspersky Labi viiruste andmebaasis on selle pahavara nimeks Backdoor.Win32.Sputnik.

Nakatatud arvutivõrgu juhtimiseks kasutati rohkem kui 60 domeeninime ja üle maailma asuvaid servereid. Suurem osa neist paiknes Saksamaal ja Venemaal. Serverite analüüs näitas, et kurjategijad kasutasid põhiserveri asukoha varjamiseks puhverserverite ketti.

Kurjategijad varastasid nakatatud süsteemidest infot, mis sisaldus näiteks „acid*" tüüpi failides: see viitab, et failid pärinevad salastamistarkvarast Acid Cryptofiler, mida rakendab hulk Euroopa Liidu ja NATO asutusi.

Süsteemide nakatamiseks kasutasid kurjategijad mõne organisatsiooni konkreetsele kasutajale saadetud õngitsemiskirju. Seal sisaldus troojalane, mille paigaldamiseks olid kirjades Microsoft Office'i turvaauke kasutavad *exploit*id. Need *exploit*id olid loodud kaaskurjategijate poolt ning kasutusel mitmes küberrünnakus, mis olid suunatud nii Tiibeti aktivistide kui ka mõne Aasia riigi militaar- ja energiaharu pihta.

Küberjälituse ohvrite tuvastamiseks rakendasid Kaspersky Labi eksperdid kahest allikast saadud andmeid: pilveserverist Kaspersky Security Network (KSN) ning juhtserveritega ühendust otsivate nakatatud arvutite jälgimiseks mõeldud *sinkhole*-serveritest.

- KSN-i statistilised andmed aitasid tuvastada mõnisada unikaalset nakatatud arvutit, suurem osa neist kuulus saatkondadele, konsulaar- ja valitsusasutustele ning teadusuuringuinstituutidele. Tähelepanu vääriv osa nakatatud süsteemidest tuvastati Ida-Euroopa riikides.

- *Sinkhole*-serverite andmeid koguti 2. novembrist 2012 kuni 10. jaanuarini 2013. Selles ajavahemikus fikseeriti üle 55 000 ühenduse 250-lt nakatatud IP-aadressilt, mis olid registreeritud 39 riigis. Valdav osa nakatatud IP-aadresside ühendusi tuvastati Šveitsis Kasahstanis ja Kreekas.

Küberkurjategijad olid loonud rünnakute tegemiseks multifunktsionaalse platvormi: see sisaldas mitutkümmet laiendust ja kahjurfaili, mis olid suutelised kiiresti kohanema eri süsteemikonfiguratsioonidega ning koguma nakatatud arvutitelt konfidentsiaalseid andmeid.

Moodulite kõige tähelepanuväärsemad omadused on järgmised:

- taastumismoodul, mis lubas kurjategijatel nakatatud arvuteid taaselavdada. Moodul paigaldub Abode Readeri ja Microsoft Office'i pistikprogrammina ning võimaldab ründajatel kordusjuurdepääsu süsteemile juhul, kui pahavara on tuvastatud ja kustutatud või kui süsteemi on uuendatud;

- täiustatud krüptograafilised jälitusmoodulid, mis on mõeldud andmete varastamiseks mitmesugustest krüptograafilistest süsteemidest, näiteks Acid Cryptofilerist, mida kasutatakse aastast 2011 sellistes organisatsioonides nagu NATO, Euroopa Liit, Euroopa Parlament ja Euroopa Komisjon;

- võimalus nakatada mobiilseadmeid. Lisaks traditsiooniliste tööarvutite nakatamisele võis see pahavara varastada andmeid ka mobiilseadmetelt, sh nutitelefonilt (iPhone, Nokia ja Windows Phone). Kurjategijad said varastada isegi USB-andmekandjatelt kustutatud faile.

Juhtserverite registreerimisandmed ja pahavara käivitusfailides sisalduv info annavad alust arvata, et kurjategijatel on vene juured.

Lätis ja Leedus sattusid rünnaku alla mitmed diplomaatilised esindused, Eestis ei ole praegu Punase Oktoobriga seotud intsidente tuvastatud, mis aga ei tähenda, et neid pole kunagi toimunud.

Detailsem info Punase Oktoobri võrgust on kättesaadav aadressilt www.securelist.com/en/analysis.

- Uudised

- Turvalisus