Eestis on levinuimad pahavarad Kometaur ja Cryptowall

7 aastat tagasi Autor: AM

Eestis on levinuim troojalane Kometaur, mis levib Windowsi platvormidel. See võtab ühendust juhtimisserveriga ja saadab nakatunud seadmest andmeid. Pahavara võib proovida end arvutis ise uuendada. Samuti Cryptowall, väljapressimistarkvara ja troojalane, mis krüpteerib nakatunud seadmes failid ja küsib andmete tagasisaamise eest lunaraha. Levib pahavarareklaamide ja õngitsemiskirjade kaudu. Cryptowall ilmus esimest korda välja 2014. aastal. Levivad neli põhiversiooni, viimane uusim versioon tuli välja sügisel 2015**.**

Küberturvalisuse lahendusi pakkuva ettevõtte Check Point ohuhinnangud näitavad, et nii pahavara erinevate levivate versioonide arv on suurenenud kui ka kasvab rünnete arv – eelmisel kuul suurenes see viis protsenti. Ettevõte avaldas eelmisel kuul toimunud pahavararünnete ülevaate, kust on näha, et rünnete arv suurenes. Küberturvalahenduste ettevõte avaldab igal kuul Globaalse Ohu Indseksit (*Global Threat Index*), mis paneb edetabelissse kõige levinumad pahavarad, mis möödunud kuul ettevõtete arvutivõrke ründasid.

Check Point'i küber-ohtude uurimistiim leidis, et nii aktiivsete pahavaraversioonide kui ka rünnakute arv kasvasid eelmisel kuul 5%. See tegi oktoobrist ühe selle aasta kõige rünnakuterohkeima kuu. Väljapressimistarkvara Locky intsidendid jätkusid suurenenud mahus, tõstes selle pahavara edetabelis kolmandale kohale, samal ajal kui pangandustroojalane Zeus liikus ülespoole kahe koha võrra, pääsedes samuti esikolmikusse.

Põhjus, miks Locky levik muudkui kasvab, peitub selle tarkvara võimes pidevalt uute variantidena välja ilmuda ja ka leviku- ja laienemismehhanisme muuta. Põhiliselt kasutatakse selleks spämmikirjade saatmist. Pahavara loojad muudavad pidevalt failitüüpe, millega virus kaasa pannakse, kasutades .doc, .xls ja .wsf laiendiga faile, samuti muutes masspostitatavate e-kirjade struktuuri ja sisu, millega pahavaraga nakatunud failid kaasa lähevad. Väljapressimistarkvara ise pole midagi erilist ja uut, kuid selle taga olevad küberkriminaalid püüavad maksimaalselt suurendada sellega nakatunud arvutite hulka.

Seitsmendat kuud järjest on Androidi pahavara HummingBad paigaldanud Rootkit´i tüüpi rakendusi mobiiltelefonidele, et teha nakatunud seadmetes mitmeid pahategusid. HummingBad on saanud kõige levinumaks mobiilseadmete pahavaraks.

Conficker säilitas oma esimese koha edetabelis kui maailma kõige levinum pahavara. Koguni 17% kõigist tuvastatud rünnakutest tegi see viirus. Teisel kohal olev Locky, mis hakkas levima selle aasta veebruaris ja kolmandal kohal olev Zeus on kumbki viie protsendi tuvastatud rünnete taga.

TOP 3 pahavara maailmas, oktoober 2016

2. ↔ **Conficker** – ussviirus, mis lubab nakatatud arvutit eemalt üle võtta ja sellesse pahavara paigaldada. Nakatunud masinat juhib botnet ehk ülevõetud arvutite võrk, see on ühenduses võrgu juhtimiskeskusega, saades sealt käske järgmisteks rünnakuteks.
3. ↑ **Locky** – väljapressimistarkvara, mis hakkas levima veebruaris 2016 ja levib peamiselt masspostitusega spämmikirjade kaudu. Lisandis on pahavara allalaadimisprogramm, mis peidab end Word´i pakitud arhiivifailis. Selle käivitamisel krüpteeritakse kasutaja failid ja nõutakse krüpteerimisvõtme eest lunaraha.

3. ↑ **Zeus** – troojalane, mis levib Windowsi platvormidel ja mida kasutatakse põhiliselt pangainfo näppamiseks. Meetodiks on nn *man-in-the-browser* klahvivajutuste salvestamine brauserist ja toidetavate veebivormide sisu salvestamine.

Mobiilidele suunatud pahavara jätkab endiselt ettevõtete ohustamist ja TOP 200 levinud pahavarast 15 ründavad mobiilseid seadmeid. Kolm kõige levinumat pahavaraperekonda on järgmised.

1. ↔ **HummingBad** – Androidi pahavara, mis paigaldab mobiilsesse seadmesse Rootkit´i tüüpi käivitustarkvara, kahjulikke äpp´e ja tekitab võimaluse lisada klahvivajutuste registraator, krediitkaardiandmete koguja ning kõrvaldab e-kirjade krüpteerimise.

2. ↔ **Triada** – Androidi tagaukse-tüüpi pahavara annab endale superkasutaja õigused, et alla laadida muud pahavara. Triada on mõnede teadete kohaselt võltsinud ka veebiaadresse, kui neid avada mobiilibrauseris.
3. ↑ **XcodeGhost** – nakatatud iOS´i arendusplatvorm Xcode. Mitteametlik Xcode´i versioon sisaldab muudatusi, mis süstivad arendatava mobiilirakenduse koodi kahjulikke koodijuppe. Nakatunud koodiga äpp saadab infot oma juhtimiskeskusse ja loeb seadme puhvrist andmeid.

Check Pointi ohtude ennetamise osakonna juht Nathan Shuchami selgitab eelmise kuu tulemusi lähemalt: “Koos pahavaraperekondade rünnakute arvu ja erinevate variatsioonide arvu kasvuga suureneb ettevõtete väljakutse neile kõigile vastu astuda tohutult. See, et TOP 10 pahavara jäid enam-vähem samaks võrreldes septembriga lubab arvata, küberkurjategijad naudivad edasi seniste rünnakumeetodite edukust. See on murettekitav, et sellised üldtuntud pahavaraperekonnad nagu Conficker tegutsevad endiselt nii efektiivselt. Võib oletada, et paljud ettevõtted ei kasuta uusimaid, mitmekihilisi kaitsemeetodeid.”

“Selleks, et end kaitsta, peavad organisatsioonid kasutusele võtma ennetavad meetmed nii oma võrgus, lõppseadmetes kui mobiilsetes seadmetes, et takistada pahavara levikut juba enne nakatumist. Näiteks Check Point’i SandBlast™ Zero-Day Protection ja Mobile Threat Prevention tagavadki selle lahenduse, mis kaitseb varakult viimaste levinud küberohtude eest,” lisas Shuchami.

Check Point’i ohuindeks põhineb „luureandmetel“, mida kogutakse üle maailma keskkonnas ThreatCloud World Cyber Threat Map. See kontrollib, kus ja millal küberründed üle maailma toimuvad. Ülemaailmse küberohtude kaardi töö tagab Check Point ThreatCloud^{TM} tarkvara, mis on üks maailma suurimatest ühendatud võrkudest küberkuritegevusega võitlemiseks. ThreatCloud´i andmebaas sisaldab üle 250 miljoni võrguasukoha, mida analüüsitakse, üle 11 miljoni pahavarakirjelduse ja üle 5,5 miljoni nakatunud veebilehe. Iga päev avastatakse miljoneid uusi pahavaraversioone.

- Uudised

- Tarkvara
- Turvalisus