Teises kvartalis suurenesid finantsrünnakud 16%, pahavara loojad on oma jõud ühendanud

9 aastat tagasi - 02.09.2016 Autor: AM

Häkkerid ja viiruseloojad ei tee pahandust juba ammu mitte enam lõbu pärast, vaid ikka käegakatsutava kasu saamise eesmärgil. Sellepärast levib aina enam finantspahavara, mis korjab looja(te)le suurt raha.

Kaspersky Lab'i teise kvartali aruanne IT ohu levimise kohta annab teada, et kräkkerite omavahelise koostöö tulemuseks on finantspahavara levimine. Teise kvartali jooksul blokeerisid Kaspersky Lab'i tooted rohkem kui 1 132 031 finantspahavara rünnakut, mis on 15,6% rohkem, kui eelmises kvartalis. Kasvu üheks põhjuseks on koostöö kahe juhtiva pangatroojalase autori vahel. Need troojalased on Gozi ja Nymaim, mis mõlemad kuuluvad finantspahavara esikümnesse.

Pangatroojalased on jätkuvalt kõige suurem võrgus pesitsev oht. Neid viiruseid levitatakse sageli nakatatud või võltside veebilehtede või rämpsposti teel ja need matkivad pärast kasutaja seadme nakatamist panga ametlikku veebilehte, püüdes varastada kasutaja isiklikku informatsiooni, nagu tema pangakonto, kasutajatunnused ja salasõnad või krediitkaardi andmed.

Kaspersky Lab'i kvartaliaruande statistika kohaselt suunati kõige rohkem seda tüüpi rünnakuid Türgi vastu, kus sellise rünnaku ohu alla sattus kvartali jooksul 3,45% Kaspersky Lab'i toodete kasutajatest. Venemaa oli teisel kohal 2,9 protsendiga, järgnes Brasiilia 2,6 protsendiga. Tänu olümpiamängudele võib Brasiilia tõusta kolmandas kvartalis esikohale.

Peamisteks süüdlasteks olid pangatroojalased Gozi ja Nymaim, kelle autorid on oma jõupingutused ühendanud. Pangatroojalane Nymain töötati algselt välja lunavarana, mis blokeeris arvutis juurdepääsu kasutajatele olulistele andmetele ja siis nõudis raha, et need andmed taas kättesaadavaks teha. Uusim versioon sisaldab aga ka Gozi lähtekoodi pangatroojalase funktsiooni, mis annab ründajatele kaugjuurdepääsu ohvri arvutile. Lisaks on tehtud täiendavad ja ilmselt ka ühiseid pingutusi pahavara levitamiseks ja see koostöö on mõlemad viirused viinud 10 kõige enam levinud finantspahavara hulka. Gozi saavutas teise koha, käivitades 3,8 protsendil kasutajatest finantspahavara tuvastamise, Nymaim jäi 1,9 protsendiga kuuendale kohale. Finantspahavara nimekirja juhib jätkuvalt

troojalane Zbot, kes ründas 15,17 protsenti kõigist finantspahavara rünnaku ohvritest.

“Finantspahavara on endiselt aktiivne ja areneb tormiliselt. Uute pangatroojalaste funktsionaalsus on märkimisväärselt laienenud, lisades neile uusi mooduleid nagu lunavara. Kui kurjategijatel ei õnnestu kasutaja isiklikke andmeid varastada, krüpteeritakse need ja nõutakse lunaraha. Veel üheks näiteks on troojalaste perekond Neurevt. Seda pahavara kasutati mitte ainult andmete varastamiseks võrgupanganduse süsteemidest vaid ka rämpsposti laiali saatmiseks. Kaspersky Lab'is reageerime me toimuvale laiendades ja parandades viise, kuidas tuvastada ja klassifitseerida finantspahavara - et oleksime võimelised seda veel kiiremini blokeerima," märgib Kaspersky Lab'i turvaspetsialist Denis Makrushin.

2016. aasta teise kvartali aruande kohaselt varitsevad võrgus alljärgnevad ohud:

- Kokku blokeerisid Kaspersky Lab'i tooted teises kvartalis 171 895 830 võrgurünnakut kasutajate vastu.
- Pahavara oli pärit 191 riigist, ehkki rõhuvalt suur osa, tervelt 81% pärines vaid kümnest riigist, mille eesotsas olid USA (35.4%), Venemaa (10.3%) ja Saksamaa (8.9%).
- Ettevõtte turvalahendused tunnistasid pahavaraliseks 54 539 948 internetiaadressi, mis on 17% vähem kui 2015. aasta samas kvartalis.
- Korra kvartalis puutus rünnakuga kokku iga viies arvutikasutaja.
- Kaspersky Lab'i tooted tuvastasid 16 119 489 pahavaralist objekti: skripti, vallutust, käivitatavat faili, etc.
- Kõige turvalisemad riigid võrgust lähtuvate ohtude suhtes olid Kanada (15%), Rumeenia (14.6%) ja Belgia (13.7%); suurima internetinakkuste ohuga riskiriigid olid Aserbaidžaan (32.1%), Venemaa (30.8%) ja Hiina (29.4%).

Kolm soovitust finantspahavara ohu vähendamiseks:

- Kasuta usaldusväärseid turvalahendusi ja uuenda tarkvara värskeimaks versiooniks.
- Vii regulaarselt läbi süsteemi skannimine, et kontrollida võimalikku nakatumist.
- Toimi veebis mõistlikult. Ära sisestada isiklikku infot veebilehele, kui on pisimgi kahtlus või ebakindlus selle usaldusväärsuse suhtes.

- Uudised

- Turvalisus

Pilt