Iknedēļas ziņas
Sagatavotas 7.11.2016.
Numurs 2016/39

Mēģina pārņemt internetu ar masīvu DDoS uzbrukumu palīdzību

Oktobra sākumā tika publiskots "Mirai" robottīkla pirmkods. Šī ļaunatūra skenē nedrošas IoT (*internet of things*) ierīces un pievieno tās robotu tīklam, ko tālāk izmanto DDoS uzbrukumiem.
Divas nedēļas atpakaļ "Mirai" IoT robotu tīkls veica masīvu DDoS uzbrukumu DNS pakalpojuma nodrošinātājam "Dyn". Uzbrukums uz dažām stundām padarīja nepieejamas daudzas "Dyn" klientu vietnes, tādas kā Twitter, Reddit, Github, Soundcloud, Spotify u.c.

Tiek lēsts, ka uzbrukumā piedalījās 100,000 inficētas IoT iekārtas. Latvijā identificēti vairāki simti ievainojamu iekārtu, kuras iespējams izmantot šāda tipa uzbrukumos.
Eksperti uzskata, ka nākotnes DDoS uzbrukumi varētu sasniegt 10 Tbps, kas ir pietiekami, lai spētu atslēgt no interneta veselu valsti. Vairāk: http://thehackernews.com/2016/11/ddos-attack-mirai-botnet.html

Tā kā "Mirai" robotu tīkls tiek veidots, pateicoties lielam skaitam nedroši konfigurētu IoT iekārtu, lietotājiem jāpievērš uzmanība savu iekārtu drošībai, nomainot noklusētās paroles, atslēdzot attālinātās vadības iespēju un nodrošinot atjauninājumus. "Mirai" iekļautās ierīces netika uzlauztas, bet vairumā gadījumu tika izmantotas sen zināmas ievainojamības un noklusējuma paroles. Pieslēdzot tīklam iekārtu ar nepietiekamu drošības līmeni, ļaundariem tiek pasniegts vēl viens rīks, ar kuru izmantot uzbrukumā.

Kompromitēta kāda novada vietne

Kāda novada mājas lapa tika uzlauzta, un tajā ievietotas saites uz ļaunatūras izplatīšanas vietnēm. CERT.LV identificēja vairākas bojātas mājas lapas sadaļas, kurās tika ievietots ļaundabīgs kods. Pēc CERT.LV brīdinājuma lapa tika iztīrīta, tuvākajā laikā tā tiks atjaunināta un pārcelta uz citu serveri.

Nedroša lietotāju piekļuves datu pārraide

Vairāku tirgotāju lapās tika konstatēta nešifrēta HTTP savienojuma izmantošana lojalitātes karšu klientu informācijas pārraidē. HTTPS savienojums uz tām netika nodrošināts. Pēc CERT.LV brīdinājuma viens no tirgotājiem salaboja savu vietni, un tā tagad nodrošina šifrētu HTTPS savienojumu. Pārējie lapu vēl nav izlabojuši.

Aktīva "Locky" datorvīrusa izplatīšanas kampaņa

Vairākas dienas turpinās aktīva „Locky" saimes šifrējošā izspiedējvīrusa izplatīšanas kampaņa. Tā lejupielādētājs tiek atsūtīts e-pasta pielikumos iekļautos .zip arhīvos, kas satur Windows skripta failu .wsf, .com, .vbs formātos. Pēc datorvīrusa aktivizācijas, tas šifrē lietotājam pieejamos dokumentus lokālajā datorā un tīkla diskos, un piešķir tiem „.thor" paplašinājumu.
Šis vīruss nošifrējis darbstacijas kādā valsts iestādē (dati atgūti no rezerves kopijām), kādā pašvaldībā un vairākām privātpersonām.

Izķēmotas valsts iestāžu mājaslapas

29.10. uzbrucēji izķēmojuši divu iestāžu mājas lapas. Tajās, izmantojot SQL injekcijas, ievietoti politiski motivēti paziņojumi arābu valodā. Abas lapas bija izvietotas vienā koplietošanas serverī, ko uzturēja viens datu centrs. Citas šajā serverī esošās lapas nav izķēmotas.

Masveidā izsūtītas e-pasta piekļuves datu izkrāpšanas vēstules

Neatslābst uzbrucēju interese par e-pasta kontiem. Vēstules arvien biežāk tiek noformētas latviski, un krāpniecisko tekstu kvalitāte uzlabojas.

```
Subject:     Sistēmas administrators
Date:     Tue, 19 Apr 2016 04:47:11 -0430
From:     Web Mail <inffoo@ivss.gob.ve>
Reply-To:     weblinkss@qq.com
Organization:     Web Mail


--
Dārgie lietotājs
Mēs šobrīd mūsu servera Update/verifikāciju, palielināt efektivitāti un noņemti konti, kuras vēl nav aktīva. lūdzu

ierakstiet savu informāciju zemāk, pārbaudīt un atjaunināt savu kontu:

(1) e-pasts:
(2) nosaukums:
(3) parole:
(4) alternatīvā e-pasta:

paldies
Sistēmas administrators
```

Pieejami atjauninājumi

Apple IOS atjauninājums
Apple publicējusi IOS jauninājumu https://support.apple.com/en-us/HT207287, kas labo vairākas kritiskas ievainojamības. Dažas no tām ļāva uzbrucējiem iegūt kontroli pār upura datorsistēmu.

Adobe Flash player atjauninājums
Adobe publicējusi Flash player jauninājumu https://helpx.adobe.com/security/products/flash-player/apsb16-36.html, kas labo kritisku ievainojamību. Tā ļāva uzbrucējiem iegūt kontroli pār upura datorsistēmu.

Jooma CMS atjauninājums
Populārā satura vadības sistēma Joomla atjaunināta uz versiju 3.6.4
https://www.joomla.org/announcements.html Šis labojums novērš vairākas ievainojamības, no kurām kritiskākās ļāva uzbrucējiem iegūt nesankcionētu piekļuvi tīmekļa vietnei, kura izmanto Joomla CMS.