Iknedēļas ziņas
Sagatavotas 12.09.2016.
Numurs 2016/34

## Draudu vēstule uzņēmumam

Kādam Latvijas uzņēmumam tika atsūtīta draudu vēstule grupējuma "Armada Collective" vārdā. Tika draudēts veikt apjomīgu DDoS uzbrukumu, kas traucēs uzņēmuma darbību, ja uz grupējuma Bitcoin adresi netiks pārskaitīts 1 BTC (Bitcoin).
CERT.LV informēja uzņēmumu, ka šis ir krāpšanas mēģinājums, jo "Armada Collective" nekad neveic reālus uzbrukumus, bet izspiež naudu ar tukšiem draudiem. Līdzīgas draudu vēstules vairāki Latvijas uzņēmumi saņēmuši arī iepriekš.
Vairāk par šo krāpšanu: https://blog.cloudflare.com/empty-ddos-threats-meet-the-armada-collective/

## Sekmīgs šifrējošā vīrusa uzbrukums

Kāda uzņēmuma serveris cieta no šifrējošā datorvīrusa "Cryptolocker" aktivitātes. Pārbaudot serveri, tika konstatēts, ka tas ir kompromitēts un uzbrucēji tajā izveidojuši papildu lietotāja kontu.
CERT.LV konsultēja uzņēmumu par darbiem, kas veicami datortīkla drošības uzlabošanai. Šifrētos failus uzņēmums atguva no rezerves kopijām.

## Brīvi pieejams maršrutētāja vadības panelis

Kādas valsts iestādes tīklā CERT.LV konstatēja no publiskā interneta tīkla pieejamu maršrutētāja vadības paneli. Tajā, bez autentifikācijas bija redzama uzstādītā konfigurācija, ko gan nebija iespējams izmainīt. Tāpat šis maršrutētājs bija izmantojams kā DNS open resolver. Pēc CERT.LV brīdinājuma, piekļuve šim panelim tika slēgta, kā arī tika salabota DNS servisa konfigurācija.

## Kritiska ievainojamība Wordpress

07.09.2016. tika publicēta jauna satura vadības sistēmas Wordpress versija - 4.6.1. Šis labojums novērsa divas kritiskas ievainojamības, no kurām vienu ir iespējams izmantot, lai iegūtu pilnīgu kontroli pār ievainojamo lapu.