Iknedēļas ziņas
Sagatavotas 22.08.2016.
Numurs 2016/31

Kontakti: prese@cert.lv
Tālrunis: 67085888

Mēģina izkrāpt e-pasta datus

Vairāku finanšu institūciju darbinieki saņēmuši krāpnieku sagatavotus e-pastus, kas sūtīti ar mērķi izkrāpt lietotāja datus, ievilnot saņēmēju apmeklēt interneta vietni, kas noformēta līdzīgi leģitīma pasta pakalpojumu sniedzēja vietnei. Uzbrukums bija nesekmīgs un šajā krāpšanas shēmā upuru nav. Zināms, ka kaitīgo vietni krāpnieki izvietoja uz uzlauzta tīmekļa serveru pakalpojumu sniedzēja servera Čehijā.

Kiberuzbrukuma mēģinājums valsts iestādē

Tika identificēts un novērsts mērķēts kiberuzbrukums kādai valsts iestādei. Uzbrukums tika noformēts e-pastā, kā uzaicinājums uz konferenci, kas notiek ASV, Orlando.
Lai arī uzbrucēji mēģinājuši e-pastu noformēt tā, lai tas izskatītos kā Starptautiskās cilvēktiesību organizācijas sūtīts, iesaistītie tehniskie resursi noteica, ka izsūtītājiem nav nekādas saistības ar Starptautisko cilvēktiesību organizāciju.
Rezultātā uzbrukums tika apturēts.

"CEO krāpšana" ar viltotiem .lv domēniem

Identificēts "CEO krāpšanas" mēģinājums, kura realizācijā uzbrucēji ieguldījuši izdomu. Kāda liela Latvijas uzņēmuma vārdā uzbrucēji piereģistrējuši uzņēmuma nosaukumam līdzīgu domēnu .lv zonā, kā arī mēnesi pirms uzbrukuma izveidojuši *Wikipēdijas* ierakstus par viltus uzņēmuma identitāti, lai izskatītos ticamāki. Pēc tam no viltotā domēna tie sākuši saraksti ar mērķi izkrāpt naudu par kādu darījumu.
Uzņēmuma IT sistēmu administratori krāpniecību atpazinuši un ziņojuši CERT.LV un Valsts policijai.
Uzbrucēju darbības veids, "CEO krāpšana" ir pēdējo 5 mēnešu laikā izplatīti sociālās inženierijas un elektroniskās sarakstes iejaukšanās/pārtveršanas uzbrukumi, ar kuru starpniecību uzņēmumu pārstāvji tiek pārliecināti par nepieciešamību veikt naudas transakcijas uz it kā partneru uzņēmumu kontiem par preču vai pakalpojumu piegādi. Lieki teikt, ka sarakstē norādītie kontu numuri nepieder patiesajiem partneriem, bet gan uzbrucējiem.

Apjomīga "Locky" šifrējošā vīrusa izplatīšanas kampaņa

Neskatoties uz to, ka šifrējošā vīrusa uzbrukuma kampaņas kļuvušas teju par ikdienu, pagājušās nedēļās bija vērojama agresīva "Locky" vīrusa izsūtīšanas kampaņa. Tā saturēja e-pasta ziņojumus, kas satur .docm paplašinājuma failus, kas ir Microsoft Word dokuments ar Macros aktīvā koda funkcionalitāti.
Lai arī šī vīrusa aktivitāte neraisa izbrīnu, tā piegādes veidi ir cieši saistīti ar sociālās inženierijas elementiem un nereti neuzmanīgs lietotājs cieš no šiem uzbrukumiem.