Iknedēļas ziņas
Sagatavotas 12.10.2015.
Numurs 2015/18

Kontakti: prese@cert.lv
Tālrunis: 67085888

Valsts iestādes tīklā izplata Crypto vīrusu.

Pagājušajā nedēļā caur kādas valsts iestādes tīklu tika izplatīts Crypto vīruss, galvenokārt citām valsts un pašvaldību iestādēm, arī adresātiem ārpus Latvijas. Vīruss tika sūtīts e-pasta pielikumos .ZIP failā. Turpinās incidenta izmeklēšana.

Macros vīruss bankas darbiniekiem.

Kādas bankas darbinieki masveidā saņēma e-pastus ar pielikumos esošu Excel failu, kas saturēja inficētu macros datni. Salīdzinājumā ar šī vīrusa paraugiem no pagājušās nedēļas, mainās pieprasītais fails un IP adrese. Tas varētu liecināt, ka vīruss pieprasa vairāk nekā divus failus.

DHL vārdā Pony ļaunatūra.

Nedēļas sākumā CERT.LV saņēma paraugu ar Pony Botnet ļaunatūru, kas izplatīta e-pastos kurjerservisa DHL vārdā. Testējot iegūto paraugu, tika atklāts, ka ļaunatūra zog privāto informāciju no Interneta pārlūkiem un komunicē ar komandcentru.

Latvijas interneta pakalpojumu sniedzēja IP adrese iesaistīta Retefe banking trojāņa izplatīšanā.

Tika saņemta informācija par Retefe banking trojāņa izplatīšanos. Šis trojānis mērķēts uz vienu no bankām ārpus Latvijas, bet tika izplatīts no IP adreses, kas atrodas Latvijas pakalpojumu sniedzēja pārziņā. Zināms, ka uz šīs IP adreses servēts viens no komponentiem, kas nepieciešams vīrusa izplatībai. Šobrīd kaitīgā satura lapa vairs nav aktīva.

Turpinās banku datu pikšķerēšana.

Atkal kādas Latvijas bankas vārdā izsūtīta informācija ar īsziņu jeb SMS starpniecību ar aicinājumu izmantot “it kā” bankas mājas lapas mobilo versiju ar mērķi izkrāpt bankas lietotāju datus. Banka lūdza CERT.LV palīdzību lapas aizvēršanā, kas arī veiksmīgi tika paveikts.