Iknedēļas ziņas
Sagatavotas 11.11.2015.
Numurs 2015/14

Kontakti: prese@cert.lv
Tālrunis: 67085888

Valsts iestādes datorus inficē ar trojāni.

Izplata e-pastus ar inficētiem ZIP pielikumiem, apdraudot valsts iestāžu drošību.

Kāda valsts iestāde saņēma vairākus e-pastus ar inficētu ZIP pielikumu. Pielikumā bija .exe fails, kas saturēja Upatre lejupielādes rīku, kas pēc programmas palaišanas veic datorvīrusa Dyre lejupielādi un izpildi upura datorā. Dyre trojānis tiek izmantots naudas zādzībām no internetbanku kontiem. Viena no valsts iestādes ierīcēm tika inficēta.
Vīruss no inficētā datora vienlaicīgi izsūtījis inficētos .zip pielikumus tikai 5 adresātiem no e-pasta klienta kontaktiem, tādējādi to bija grūtāk identificēt.

Detalizētāka informācija: https://cert.lv/resource/show/720

Inbox.lv lietotāji cieš no krāpnieciskiem epastiem.

Kārtējo reizi Inbox.lv lietotāji saņēma vēstules ar mērķi izkrāpt datus. E-pasta teksts aicināja sniegt datus, pretējā gadījumā lietotājs zaudēs savu e-pasta kontu. CERT.LV sazinājās ar inbox.lv ar aicinājumu novērst krāpniecisko e-pastu izsūtīšanu.

Pikšķerēšanas mēģinājumi domēnu reģistratūru vārdā.

Vairāku domēnu reģistratūru vārdā izsūtīts e-pasts ar saiti uz "uzlauztu" interneta vietni ar mērķi izkrāpt interneta lietotāju datus. Šobrīd "uzlauztā" vietne ir aizvērta.

E-pasta vēstules un pikšķerēšanas saites paraugs:

Dear Vladimirs Metlovs,

The Domain Name brw-brokers.com have been suspended for violation of the Ascio Technologies, Inc Abuse Policy.

Multiple warnings were sent by Ascio Technologies, Inc Spam and Abuse Department to give you an opportunity to address the complaints we have received.

We did not receive a reply from you to these email warnings so we then attempted to contact you via telephone.

We had no choice but to suspend your domain name when you did not respond to our attempts to contact you.

[1]Click here and download a copy of complaints we have received.

Please contact us for additional information regarding this notification.

Sincerely,

Ascio Technologies, Inc

Spam and Abuse Department

[1] http://www.heliolithe.fr/abuse.php?brw-brokers.com

Pieejamas vakances darbam CERT.LV.

CERT.LV aicina darbā IT drošības inženieri un IT drošības incidentu apstrādes un novēršanas speciālistu. Detalizētāka informācija: https://cert.lv/section/show/140