Iknedēļas ziņas
Sagatavotas 20.06.2016.
Numurs 2016/23

Kontakti: prese@cert.lv
Tālrunis: 67085888

Turpina apkrāpt uzņēmumus ar viltus rēķinu palīdzību

15.06.2016. Kāda Latvijas uzņēmuma ārzemju klients saņēma šī uzņēmuma vārdā noformētu rēķinu, taču ar viltotiem maksājuma rekvizītiem. Rēķinu klients saņēma pa e-pastu un tā izveidei par pamatu tika ņemts reāls rēķins.
Uzņēmums uzsācis šī gadījuma pārbaudi, sadarbībā ar saviem klientiem. Noskaidrots, ka viltus rēķini nav izsūtīti no Latvijas uzņēmuma e-pasta, kā arī nav notikusi nelikumīga pieslēgšanās tā serveriem.

Izsūta Cerber šifrējošo datorvīrusu

E-pasta vēstuļu kampaņā tika izplatīts Cerber datorvīruss ar pielikumiem .ace un .zip formātā kas satur .vbs skriptus. Kaitīgais kods bija izvietots kādā mājas lapā. Šobrīd kaitīgais saturs vairs nav pieejams un lietotāju inficēšana nenotiek.

Krāpniecība caur Google kontu

16.06.2016. no kādas Latvijas IP adreses tika veikts nelikumīgs pieslēgums Google pakalpojumu kontam, un no kontam piesaistītās kredītkartes tika iegādāts Google balss zvanu kredīts. Šo aizdomīgo aktivitāti noteica un arī apturēja Google automatizētā monitoringa sistēma, tāpēc zaudējumi netika nodarīti un konta īpašnieks atguva pieeju savam kontam.
Tika noskaidrots, ka IP adrese, no kuras notikusi krāpšana, ir Sality P2P robottīklā. CERT.LV par šo vairākkārtēji ir informējis atbildīgo interneta pakalpojumu sniedzēju.

Kaitīgi skripti mājas lapā

Kārtējais gadījums, kad izmantojot novecojušas satura vadības sistēmas WordPress ievainojamības, vietnē ievietoti kaitīgi skripti. Pēc saņemtā brīdinājuma uzturētājs tos dzēsis, lapu daļēji atjauninājis.
CERT.LV turpina lapas pārbaudi.

Pieejami vairāki drošības labojumi

16.06.2016. ADOBE publicējusi programmu Adobe Flash Player un Adobe AIR ievainojamību APSB16-18 un APSB16-23 labojumus. Šīs ievainojamības ļauj uzbrucējam attālināt iegūt kontroli pār upura datoru. To detalizētāki apraksti pieejami: https://helpx.adobe.com/security/products/flash-player/apsb16-18.html un https://helpx.adobe.com/security/products/air/apsb16-23.html

15.06.2016. CISCO publicējis bezvadu maršrutētāju RV110W, RV130W un RV215W vadības paneļa drošības labojumus. Atklātās ievainojamības ļāvušas veikt nesankcionētu piekļuvi šiem maršrutētājiem caur to vadības paneļa lapu. Vairāk informācijas:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160615-rv
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160615-rv1
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160615-rv2
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160615-rv3

Pieejami arī Microsoft drošības atjauninājumi: https://technet.microsoft.com/en-us/library/security/ms16-jun