Iknedēļas ziņas
Sagatavotas 06.05.2016.
Numurs 2016/17

Kontakti: prese@cert.lv
Tālrunis: 67085888

Masveidā izsūta e-pastus ar Locky datorvīrusu

05.05.2016. valsts un pašvaldību iestādēm masveidā tika iesūtīti inficēti e-pasti, kas noformēti kā viltus rēķini angļu un spāņu valodās, kas satur .zip arhīvu ar .js failu, kurš pēc izpildes lejupielādē Locky šifrējošo datorvīrusu. Lai bloķētu Javascript pielikumu izpildi, iesakām atslēgt WSH.
Vairāk par WSH atslēgšanu: https://cert.lv/resource/show/818
Vairāk par Locky vīrusu: https://blog.malwarebytes.org/threat-analysis/2016/03/look-into-locky/

Atklāj konfigurācijas kļūdu iestādes serverī

Pārbaudot sūdzību par masveida mēstuļu iesūtīšanu kādas pašvaldību iestādes darbiniekiem, CERT.LV atklāja servera konfigurācijas kļūdu, kas ļauj masveidā iesūtīt e-pastus iestādes novada serverī, ja par izsūtītāju norāda jebkādu e-pasta adresi no iestādes domēna. CERT.LV informēja servera uzturētājus.

Bīstama ievainojamība ImageMagick aplikācijā

Populārā attēlu apstrādes aplikācijā ImageMagick, kas bieži tiek lietota attēlu apstrādei serveros, atklāta kritiska ievainojamība (CVE-2016-3714), kas ļauj uzbrucējam izpildīt dažādas komandas uz bilžu apstrādes servera. Ievainojamība ir novēršama, izmantojot ImageMagick konfigurācijas faila parametrus, ar kuriem jāatslēdz MVG, HTTPS, EPHEMERAL, un MSL komandu izpilde attēlu failiem.
Sīkāks apraksts: https://blog.sucuri.net/2016/05/imagemagick-remote-command-execution-vulnerability.html