Iknedēļas ziņas
Sagatavotas 30.06.2016.
Numurs 2016/24

Kontakti: prese@cert.lv
Tālrunis: 67085888

Locky šifrējošais izspiedējvīruss atgriežas ar jaunu kampaņu

Ar jaunu kampaņu Latvijā un citās valstīs atgriezies *Locky* šifrējošais izspiedējvīruss, kas šobrīd novērots, mērķējot uzbrukumus uz valsts iestādēm. Šobrīd zināms, ka ar e-pastu starpniecību tiek izsūtīts Javascript fails, kuru atverot, tas mēģina savienoties ar kaitīgām tīmekļa vietnēm un ielādēt vīrusu datorā. CERT.LV aicina neatvērt nepazīstamu sūtītāju sūtītos pielikumus, lai izvairītos no datora inficēšanas ar kādu no šifrējošajiem vīrusiem, un savlaicīgi nodrošināt svarīgo failu rezerves kopijas.

WordPress atjauninājumi 20 ievainojamību novēršanai

WordPress nācis klajā ar atjauninājumiem, lai novērstu vairāk nekā 20 ievainojamības, kas atklātas satura vadības sistēmā. Daudzas no šīm ievainojamībām ļauj uzbrucējam attālināti kontrolēt mājas lapas, kas veidotas, izmantojot *WordPress* satura vadības sistēmas. Atklātās ievainojamības ietekmē versijas 4.5.2 un agrākas, tāpēc ieteicams atjaunināt *WordPress* uz 4.5.3 versiju.
Vairāk: https://threatpost.com/wordpress-security-update-patches-two-dozen-flaws/118863/

Symantec ievainojamības

Šonedēļ *Symantec* izlaidis atjauninājumus vairākiem drošības produktiem, novēršot vairākas atklātas ievainojamības. Zināms, ka dažu ievainojamību izmantošana ļauj uzbrucējiem pārņemt kontroli pār ievainojamo sistēmu un izraisīt servisa atteices apstākļus (DoS). Ieteicams pārskatīt *Symantec* ieteikumus un ieviest nepieciešamos atjauninājumus. Vairāk:
https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160628_00

Ļaunatūra Google Play lietotņu veikalā

Google Play veikalā, kas tiek izmantots ierīcēs ar *Android* operētājsistēmu, atklāta lietotne ar nosaukumu *LevelDropper*, kas satur ļaunatūru un, tiklīdz lejupielādēta ierīcē, dod uzbrucējam pilnīgu kontroli pār inficēto ierīci. Šis ir nesenākais piemērs šāda veida ļaundabīgām lietotnēm, kas atklātas *Google Play* veikalā. Tendences rāda, ka šādas lietotnes parādās arvien biežāk, tāpēc, pirms lejupielādēt kādu no lietotnēm, skatiet lietotnes atsauksmes, vērtējumus un lejupielāžu skaitu, tāpat būtu ieteicams izmantot lietotņu verifikācijas funkciju, kas atrodama ierīces uzstādījumos.
Vairāk: https://threatpost.com/google-play-hit-with-rash-of-auto-rooting-malware/118938/