Iknedēļas ziņas
Sagatavotas 07.04.2016.
Numurs 2016/13

Kontakti: prese@cert.lv
Tālrunis: 67085888

Šifrējošais vīruss valsts iestādē

Marta nogalē kādā iestādē ar šifrējošo datorvīrusu TeslaCrypt tika sašifrēts dators. Pēc vīrusa pamanīšanas, ar antivīrusa palīdzību tika atrasts un izdzēsts kaitīgais fails Win32/Filecoder.TeslaCrypt.A trojan, tādējādi apturot vīrusa tālāko iespējamo izplatību iestādes tīklā. Sašifrētie faili tika atgūti, pateicoties rezerves kopijām. Turpinās incidenta izpēte, lai noskaidrotu vīrusa izplatīšanās mehānismu.

Facebook lietotāju konti izsūta mēstules

Pagājušajā nedēļā vairāki Facebook lietotāju konti tika izmantoti mēstuļu izplatīšanai. Lietotājiem nezinot, no to kontiem tika izsūtītas mēstules visiem lietotāja kontaktiem. Saite saturēja video failu. Ja kāds cits lietotājs atvēra saiti, mēstuļu izsūtīšanas ķēde turpinājās. Šobrīd saitē esošie video faili vairs nav pieejami un nav zināms vai ar šo saiti izplatījies arī kāds datoram bīstams vīruss.
Vienā no variantiem video saite pārvirzīja lietotājus uz pikšķerēšanas vietni, ar kuras palīdzību tika mēģināts izkrāpt lietotāja datus.

Jauns šifrējošā vīrusa paveids

Parādījies jauns šifrējošā vīrusa paveids Petya, kas atšķirībā no citiem šifrējošajiem vīrusiem, kas sašifrē datorā esošos failus, sašifrē cieto disku, liedzot turpmāku datora lietošanu. Šī vīrusa mērķauditorija ir biznesa lietotāji.
Vīruss izplatās ar e-pastu, kas satur saiti uz DropBox lietotni, kurā it kā atrodams fails ar personas CV, bet tā vietā tas ir izpildāmais fails, kas lejuplādē vīrusu datorā, kas veic cietā diska šifrēšanu. Pašreiz nav zināms veids, kā atgūt Petya sašifrēto informāciju, nemaksājot.
Labā ziņa ir tā, ka šobrīd DropBox ir izņēmis ļaunprātīgos arhīvus ar Petya, taču, visticamāk, uzbrucēji atradīs arī citus veidus, kā izplatīt vīrusu.
Plašāk par vīrusu: https://blog.kaspersky.com/petya-ransomware/11715/

Firefox ievainojamība

Atklāts, ka simtiem populāri Firefox paplašinājumi ir neaizsargāti pret uzbrukumiem, kas var sniegt uzbrucējam kontroli pār Mac OS X un Windows datoriem. Ievainojamība ir saistīta ar Firefox vecāku pārlūkprogrammu paplašinājumu platformas atbalstu un Mozilla Foundation spraudņa drošības pārbaudes procesu Firefox pārlūkprogrammā. Uzbrucēji var uzrakstīt paplašinājumu, kas izskatās nekaitīgs. Pievienots pie Firefox, it kā labdabīgais paplašinājums var izmantot otru Firefox paplašinājumu, lai pievienotu ļaunatūru lietotāja datoram. Plašāk par ievainojamību: https://threatpost.com/firefox-add-on-flaw-leaves-apple-and-windows-computers-open-to-attack/117183/