Iknedēļas ziņas
Sagatavotas 28.04.2016.
Numurs 2016/16

Kontakti: prese@cert.lv
Tālrunis: 67085888

Atsāk izplatīt banku vīrusu

Eiropā sāk izplatīties jauna banku ļaunatūra GozNym, kas mēģina izkrāpt lietotāja bankas datus. Metode, kas tiek izmantota lietotāju datu izkrāpšanai, ir lietotāju pārvirzīšana uz identiski izveidotu bankas mājas lapu. Lietotāji tiek apmānīti, rādot īsto bankas URL un SSL sertifikātu, kas tiek panākts, sūtot tukšus pieprasījumus uz banku, lai saglabātu SSL pieslēgumu aktīvu. Tiklīdz lietotājs ir pārvirzīts uz kaitīgo vietni, lietotājs tiek aicināts ievadīt savu bankas lietotājvārdu un paroli, no kurienes šī informācija tiek pārsūtīta uz citu serveri.
Vairāk par ļaunatūru: https://securityintelligence.com/time-is-money-goznym-launches-redirection-attacks-in-poland/

Atklāj ievainojamas valsts iestāžu vietnes

Ar kāda datordrošības entuziasta palīdzību atklāta XSS jeb starpvietņu skriptēšanas ievainojamība divās valsts iestāžu vietnēs. Izmantojot ievainojamību, vietnēs iespējams veikt SQL injekcijas. Atbildīgās iestādes ir informētas par nepieciešamību novērst šo ievainojamību.

Android izspiedējvīrusam jauna uzbrukuma metode

Atklāts, ka izpildes rīks, kas izmantots izspiedējvīrusa "Dogspectus" ielādei Android ierīcēs, izmanto vairākas ievainojamības, lai nepamanīti lejuplādētu vīrusu ierīcē. Uzbrukums notiek, kad bez lietotāja līdzdalības ierīcē tiek lejuplādēta kaitīgā lietotne, neparādot “lietotnes atļauju” dialoglodziņu, kas parasti parādās pie lejupielādes.
Jāatzīmē, ka šis vīruss nesašifrē lietotāja datus, taču tur ierīci aizslēgtā režīmā, liedzot jebkādas darbības, izņemot pieprasītās apmaksas veikšanu, divu $100 iTunes dāvanu karšu vērtībā. Ierīci ir iespēja atbloķēt, atjaunojot rūpnīcas režīmu, taču tas dzēš visas uzinstalētās lietotnes, telefonā esošos datus, bildes u.c.
Arī mobilo telefonu lietotājiem svarīgi veidot rezerves kopijas, lai šādā gadījumā var atjaunot rūpnīcas režīmu un nesatraukties par datu zudumu un neveikt pieprasīto samaksu.
Lai nekļūtu par šī vīrusa upuri, regulāri nepieciešams veikt sistēmas atjauninājumus. Vairāk par šo vīrusu: https://www.bluecoat.com/security-blog/2016-04-25/android-exploit-delivers-dogspectus-ransomware