Iknedēļas ziņas
No 27.07. līdz 31.07.2015.
Numurs 2015/01

Kontakti: prese@cert.lv
Tālrunis: 67085888

Nedrošas Latvijas tīmekļa vietnes tiek izmantotas pikšķerēšanas uzbrukumu veikšanai pret Brazīlijas banku klientiem.

Šonedēļ vairākas Latvijas domēnu zonā esošas tīmekļa vietnes bija iesaistītas Brazīlijas bankas CAIXA klientu datu izkrāpšanā, uzturot pikšķerēšanas resursus. Visas iesaistītās tīmekļa vietnes bija kompromitētas un ir uzskatāmas par uzbrucēju upuriem, taču tas bija iespējams dēļ resursu turētāju paviršās attieksmes pret drošības ielāpiem. Šīs vietnes parasti tiek uzturētas uz novecojušām Joomla un Wordpress satura vadības sistēmām. Visā pasaulē populārās satura vadības sistēmas Joomla, Wordpress, Drupal tiek regulāri pakļautas uzbrukumiem, taču tās nav uzskatāmas par sliktām, ja regulāri atjauno drošības ielāpus. Pēc CERT.LV novērojumiem, ***Latvijā ir liels atkārtoti uzlauztu tīmekļa vietņu skaits, kas norāda uz lietotāju nespēju vai nevēlēšanos atbilstoši uzturēt savas sistēmas***. Ar iesaistīto resursu turētājiem CERT.LV ir sazinājies, incidenti ir novērsti, taču datus analīzei nav izdevies iegūt, jo uzturētāji tos nav saglabājuši.

Latvijā populārs iepazīšanās portāls pārsūta apmeklētājus uz Policijas vīrusa WEB versiju saturošu vietni.

Virkne Latvijas portālu reklāmām izmanto banneru apmaiņas servisus. Šie servisi visbiežāk tiek uzturēti ārpus Latvijas un nereti satur ievainojamības.
Šajā gadījumā kāds iepazīšanās portāls lieto ārvalstu baneru apmaiņas sistēmas, pār kurām viņiem nav nekādas kontroles. Uzbrucējiem kompromitējot šo banneru sistēmu, ir izdevies piegādāt kaitīgu kodu visām tīmekļa vietnēm, kas lieto ievainojamo banneru sistēmu. Minētais iepazīšanās portāls ir viena no tām.
Resursa turētājam ir ieteikts izmantot pārbaudītas banneru apmaiņas sistēmas un problēmas risināšanai, sazināties arī ar esošo sistēmu uzturētājiem.
Mājas lapu lietotājiem ieteicams tīmekļa pārlūkos iespējot tādas papildu funkcijas kā add-block, no-script, no-flash. Šie spraudņi pasargā tīmekļa lapas apmeklētāju, neļaujot pārlūkam izpildīt tādas aktīvās komponentes kā javascript un flash.
CERT.LV pētījumi saistībā ar šādiem incientiem: https://www.cert.lv/resource/show/474.

Pikšķerēšanas uzbrukumi pret banku klientiem Latvijā.

CERT.LV kopā ar vairākām bankām šonedēļ strādāja pie incidentu risināšanas, kuros Latvijas interneta lietotājiem masveidā tika izsūtītas pikšķerēšnas e-pasta vēstules, kas it kā sūtītas bankas vārdā ar aicinājumiem apmeklēt tīmekļa vietni, kas izskatās līdzīgi banku internetbanku vietnēm. ***Uzbrukuma mērķis bija izkrāpt lietotāju datus. CERT.LV panāca kaitīgo resursu aizvēršanu dažu stundu laikā.***
Uzbrukuma ietekme: neviena lietotāja konts necieta uzbrukumā. Uzbrukumā bija iesaistīti inficēti serveri.

Iknedēļas ziņas
No 27.07. līdz 31.07.2015.
Numurs 2015/01

Kontakti: prese@cert.lv
Tālrunis: 67085888

Pikšķerēšanas uzbrukums pret Paypal servisa lietotājiem.

Arī šajā globāla mēroga uzbrukumā vairāki Latvijas lietotāji saņēma pikšķerēšanas e-pastus. CERT.LV iesaistījās incidenta risināšanā sadarbībā ar ASV kolēģiem.

No 27.07.-31.07. Latvijā uzlauztas un izķēmotas septiņas tīmekļa vietnes.

Visas kompromitētās vietnes tika uzturētas uz novecojušas Joomla un Wordpress satura vadības sistēmas. Būtisks kaitējums vietnēm netika radīts, bojāts tikai vietnes tēls. Neviens no cietušajiem resursiem nav saistīts ar valsts sektoru.