Iknedēļas ziņas
No 03.08. līdz 07.08.2015.
Numurs 2015/02

Kontakti: prese@cert.lv
Tālrunis: 67085888

Latvijas (.lv) domēna vārdu zonā tiek identificēti 3 interneta forumi, kuros noziedznieki pārdod zagtus kredītkaršu datus.

Konkrētie domēni jau ir bijuši iesaistīti šādās aktivitātēs iepriekš. Pēc Policijas pieprasījuma tie tiek bloķēti, bet pēc vairākiem mēnešiem tos reģistrē atkārtoti, kas no domēna reģistrācijas viedokļa nav pretlikumīgi.
Nav zināms, vai kredītkaršu dati, kuri tiek pārdoti minētajās vietnēs, ir īsti. CERT.LV rīcībā ir forumu autentifikācijas informācija, kas ir nodota Valsts Policijai, un sniegtas rekomendācijas tālākai rīcībai. CERT.LV par šo incidentu informēja arī Latvijas DNS reģistru NIC.LV, lai uzsāktu pārbaudi, vai domēni nav apmaksāti no zagtām kredītkartēm.

Latvijas akadēmiskajā tīklā esošs serveris piedalās masveida mēstuļu izsūtīšanā.

Veicot incidenta analīzi, ir konstatēts, ka iesaistītais serveris, kas tiek uzturēts akadēmiskajā tīklā, ir uzlauzts un tiek izmantots masveida mēstuļu izsūtīšanai. Uzbrukuma vektors ir bijis ievainojama tīmekļa vietne, caur kuru uzbrucējs ir spējis izvietot kaitīgo kodu. Šobrīd tīmekļa vietne ir bloķēta līdz tās turētājs novērsīs drošības trūkumus.

Identificēts uzbrukums kāda novada domes e-pasta serverim un lietotāju kontiem.

Uzbrukuma metodes, galvenokārt, bija paroļu piemeklēšanas mēģinājumi. Neviens sekmīgs, nesankcionētas pieslēgšanās gadījums nav konstatēts. Konkrētās domes e-pasta sistēma ir atbilstoši konfigurēta, lai šāda veida uzbrukumi neradītu apdraudējumu. Uzbrukumā iesaistīta viena IP adrese no Nigērijas.

CERT.LV saņem ziņas par uzbrukuma kampaņu, kurā tiek izsūtīti kaitīgu kodu saturoši Microsoft Word dokumenti. Datori tiek inficēti ar ZEUS saimes trojāni.

Uzbrucēji izsūta kaitīgos dokumentus masveidā, taču, lai sekmīgi inficētu upura datoru, lietotājam ir jāpiekrīt izpildīt aktīvo dokumenta komponenti Macro.
Šobrīd zināmais pielikuma faila nosaukums: item_list.doc.
Kontrolcentri un serveri: puurwellness[.]be (46.21.173.133), thitruongximang[.]com (198.57.166.64), www.ritmicapiemonte[.]it (62.149.142.168). Lai mēģinātu identificēt

inficētos lietotājus, iesakām novērot komunikāciju ar augstāk minētajiem domēna vārdiem. Ja komunikācija ir notikusi, tad lietotājs ir atļāvis izpildīt kaitīgo Macro kodu. Incidenta risināšana turpinās.

Turpinās pikšķerēšanas uzbrukumi pret Brazīlijas banku lietotājiem. Latvijā uzturētas ievainojamas tīmekļa vietnes tiek iesaistītas uzbrukumos.

Šie uzbrukumi tika pieminēti jau pagājušās nedēļas ziņu numurā. Arī šonedēļ uzbrukumu kampaņa turpinās, un tiek iesaistītas arvien jaunas tīmekļa vietnes, kas tiek kompromitētas arī [.lv] domēnu zonā. Uzbrukumi vietnēm tiek realizēti, izmantojot publiski zināmas ievainojamības Joomla un Wordpress satura vadības sistēmās.