Iknedēļas ziņas
Sagatavotas 29.10.2015.
Numurs 2015/12

Kontakti: prese@cert.lv
Tālrunis: 67085888

Adobe Flash ievainojamības aktīvi izmanto uzbrukumiem.

Nepilnas divas nedēļas atpakaļ atklātā kritiskā ievainojamība Adobe Flash Player jau ir integrēta populārākajos uzbrucēju rīkos, tādos kā Angler EK.
Latvijā Adobe Flash Player ievainojamības CVE-2015-7645 izmantošana pamanīta, izplatot Vawtrak ļaunatūru ar Angler EK.
Zināms, ka ļaunatūras mērķis ir internetbanku lietotāji, taču pastāv aizdomas, ka šī pati ievainojamība lietota arī mērķētos uzbrukumos pret NATO valstu ārlietu ministrijām kiberuzbrukumu kampaņā "Pawn Storm". Ievainojamība skar gandrīz visas Flash versijas līdz 19.00.207.

CERT.LV aicina Latvijas interneta lietotājus pārliecināties, ka tiek izmantota jaunākā Adobe Flash Player versija. Iesakām Adobe Flash Player atļaut izmantot tikai uzticamos resursos.

Turpinās bīstamā šifrēšanas vīrusa CryptoWall 3.0 izplatība.

Latvijā konstatēti jauni inficēšanās gadījumi ar CryptoWall 3.0. vīrusu, kurš datorā pieejamo informāciju efektīvi nošifrē un uzbrucēji pieprasa izpirkuma maksu par informācijas atšifrēšanu.
Vīrusa izplatīšana lielākajā daļā gadījumu notiek caur e-pastu sūtījumiem, kas satur kaitīgus pielikumus, taču ir arī virkne gadījumu, kad kaitīgais kods tiek piegādāts caur uzlauztām tīmekļa vietnēm. Pielikumi var būt kā arhīvs (.ZIP) ar izpildāmo failu .EXE vai .SCR, kā arī kaitīgu kodu saturoši MS Office un PDF dokumenti. Apskatot uzbrucēju izmantoto infrastruktūru, jāsecina, ka paši mājas lapu īpašnieki nerūpējās par vietnes drošību. Uzbrucēji kā daļu no uzbrukuma infrastruktūras izmanto novecojušas, uzlauztas Wordpress tīmekļa vietnes.
Šis vīruss dažu gadu laikā radījis desmitiem miljonu eiro zaudējumus visā pasaulē.

Noticis sekmīgs uzbrukums valsts iestādes mājas lapai.

Izmantojot zināmu ievainojamību, uzbrucēji veica sekmīgu ielaušanos kādas valsts iestādes mājas lapā, nesankcionēti mainot tās saturu.
Incidenta izmeklēšana turpinās, taču arī šis incidents papildina bēdīgi slaveno statistiku par tīmekļa vietnēm, kuras netiek pienācīgi atjaunotas. Kompromitētā mājas lapa uzturēta uz novecojušas satura vadības sistēmas versijas Joomla 1.7.

Simtiem "uzlauzti" datorlietotāju konti izplata bīstamus e-pastus.

E-pastu izsūtīšanas kampaņa ir saistīta ar Dyre banking trojāni, kurš tiek izmantots naudas zādzībām no internetbanku kontiem.
Kaitīgo e-pastu izplatība notika arī no inficētiem valsts un pašvaldību iestāžu datoriem. Vēstuļu pielikumā izplatītais .zip fails saturēja izpildāmo failu, kas lietotāju maldināšanai Windows datorsistēmās attēlojas ar PDF dokumentam līdzīgu ikonu. Fails satur lejupielādes rīku, kas pēc programmas palaišanas veic datorvīrusa Dyre (zināmu arī kā Dureza.A, Dyreza) lejupielādi un izpildi upura datorā. Detalizētāka informācija pieejama CERT.LV mājas lapā:
https://cert.lv/resource/show/720