Iknedēļas ziņas
No 17.08. līdz 21.08.2015.
Numurs 2015/04

Kontakti: prese@cert.lv
Tālrunis: 67085888

Pikšķerēšanas uzbrukumu kampaņa pret Apple kontu lietotājiem

Globālā pikšķerēšanas uzbrukumu kampaņā, kas vērsta pret Apple kontu lietotājiem, riskam tika pakļauti arī Latvijas interneta lietotāji. Cilvēki saņēma e-pasta vēstules, kas sūtītas it kā Apple kompānijas vārdā, lai informētu lietotāju par Apple konta bloķēšanu drošības apsvērumu dēļ. Lai atbloķētu kontu un apliecinātu savu identitāti, ir jāveic pieslēgums ar savu Apple ID viltotā, uzbrucēju sagatavotā vietnē.

Uzņēmuma darbinieki saņem mērķētus uzbrukumus e-pastā

Kāda uzņēmuma darbinieki e-pastā saņēma inficētus MS Word dokumentus, kas aprīkoti ar jaunākajiem zināmajiem exploit kodiem.
CERT.LV iesaistās incidenta izmeklēšanā. Uzbrucēji pielieto iepriekš zināmas ievainojamības CVE-2012-0158 un/vai CVE-2014-1761, taču jaunā izpildījumā, kas joprojām ir efektīvs uz jaunākajām MS Office pakotnēm. Pēc sekmīgas inficēšanās upura dators sāk komunicēt ar domēnu clairelefebvre.com.au, lai lejupielādētu vīrusa papildinājumus failā k3.exe MD5sum:8cf4ab7e15a6f51ff0372182afedbc3a.
Uzņēmuma tehniskais departaments reaģēja profesionāli, apdraudējums tika atpazīts laicīgi, taču viena lietotāja dators tika inficēts un šobrīd ir jau pārinstalēts. CERT.LV turpina incidenta izmeklēšanu.

Latvijas interneta lietotāji saņēmuši masveida elektroniskās vēstules ar kaitīgu failu pielikumā. Pielikums ir Bladabindi vīrus

Uzbrukuma kampaņa ir starptautiska un nav mērķēta tieši uz Latvijas interneta lietotājiem, taču vismaz vairāki simti (pārsvarā privātā sektora) e-pasta kontu Latvijā ir tos saņēmuši.
Bladabindi vīruss ir informācijas zagšanas rīks, kas nodrošina arī jebkādas papildu funkcionalitātes pievienošanu uzbrucējam, lejupielādējot tās uz upura datora. Uzbrucējam ir pilna kontrole pār upura datoru (Remote Administration). Pagaidām CERT.LV rīcībā nav informācijas par sekmīgi inficētām iekārtām šīs kampaņas ietvaros, taču kopumā Latvijā ir vairāki tūkstoši, ar šo vīrusu inficētu iekārtu. Līdz šim zināmie vīrusa paraugi tiek labi atpazīti ar lielāko daļu antivīrusu risinājumiem. **Diemžēl liela daļa Latvijas interneta lietotāju nelieto pretvīrusu risinājumus un neapdomīgi atver nezināmus e-pasta pielikumus.**

Bladabindi tiek izplatīts ar masveida e-pasta starpniecību, kas satur pielikumus ar nosaukumiem:
“My Picture.SCR”
“my pictures.zip”
“specification.zip”
Pielikuma nosaukums var atšķirties.

Vairāk informācijas par Bladabindi:
https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=MSIL/Bladabindi

Vairāk informācijas par konkrētās kampaņas vīrusa paraugu:
https://www.virustotal.com/en/file/d9e149fd42d3c5b9d59991b43e0b55a1924df0890b1855ff681119cb75631518/analysis/

Kāda interneta vietne .lv domēnu zonā piegādā kaitīgu kodu vietnes apmeklētājiem

Veicot incidenta analīzi konstatēts, ka vietne uzturēta uz novecojušas satura vadības sistēmas Joomla 1.5 versijas. Pagaidām nenoskaidroti uzbrucēji ir izmantojuši publiski zināmu ievainojamību, lai izvietotu vietnē kaitīgu kodu, kas mēģina inficēt šīs vietnes apmeklētāju datorus. Lietotāji pret šāda veida uzbrukumiem var pasargāt savus datorus, lietojot tādus papildfukcionalitātes tīmekļa pārlūka spraudņus (plugins) kā noscript/addblock/noflash. Šie spraudņi bloķē skriptu komponentes, kas izpildās uz apmeklētāja datora. Tādas komponentes kā javascript/java/flash tīmekļa tehnoloģijās tiek pielietotas ļoti plaši, galvenokārt, lai padarītu lietotāja pieredzi vizuāli patīkamāku. Diemžēl ar šo komponentu starpniecību arī galvenokārt tiek realizēti pret lietotāju vērsti uzbrukumi.

Iestāde saņem krāpnieciskus e-pastus, aicinot iesaistīties tiešsaistes naudas piramīdās

Darbinieki reaģē profesionāli, uz saitēm neviens nav klikšķinājis un par incidentu tiek informēts CERT.LV.