Iknedēļas ziņas
Sagatavotas 12.02.2016.
Numurs 2016/6

Kontakti: prese@cert.lv
Tālrunis: 67085888

Apple ierīču ievainojamība

Pagājušajā nedēļā atklāts, ka Apple ierīces ar iOS 8 un iOS 9 versiju ir ievainojamas un tām var tikt apiets ekrāna nobloķēšanas kods bez autentifikācijas, tādējādi piekļūstot ierīces lietotāja datiem. Tas iespējams, ja uzbrucējam izdodas uzstādīt ierīci režīmā, kas veic lietojumprogrammu atjauninājumu atkārtotu ciklu, kas īslaicīgi padara ekrāna bloķēšanas kodu neaktīvu.
Plašāka informācija: http://www.vulnerability-lab.com/get_content.php?id=1710

TeslaCrypt šifrējošais izspiedējvīruss

Kādā mājas lapā tika izvietots kaitīgs Javascript, kas satur Angler Exploit Kit rīku, veicot TeslaCrypt šifrējošā datorvīrusa lejupielādi apmeklētāju datoros. Šis incidents atklāts, pateicoties lietotāja anti-vīrusa programmai, kas uztvērusi šo draudu.
Nav pieejama informācija par inficētu ierīču gadījumiem.

Dridex banku trojāņa kampaņa

Arī šajā nedēļā aktivizējies Dridex banku trojānis, izplatot vīrusu e-pasta pielikumos .doc vai .xls formāta failā ar makros datni, mērķējot uzbrukumu uz valsts iestāžu sektoru. Šobrīd ir zināmi vairāki indikatori, pēc kuriem atpazīstama šī kampaņa un inficētās ierīces.
Dridex bankas trojānis zināms kā datorvīruss ar mērķi iegūt lietotāju internetbankas datus, lai tos pielietotu naudas zādzībai no lietotāju internetbankas kontiem.

Interneta provaideris uztur krāpniecisku mājas lapu

Kāds Latvijas interneta pakalpojumu sniedzējs uzturējis krāpnieciska satura mājas lapu, kas tika izmantota Ukrainas mobilo telefonu lietotāju datu izkrāpšanai.
Pēc uzturētāja informēšanas, mājas lapa tika izdzēsta no servera, taču nupat krāpnieciskā mājas lapa atkal ir atjaunojusi darbību uz ārzemēs esošiem serveriem un turpina datu izkrāpšanu.