Iknedēļas ziņas
Sagatavotas 19.02.2016.
Numurs 2016/7

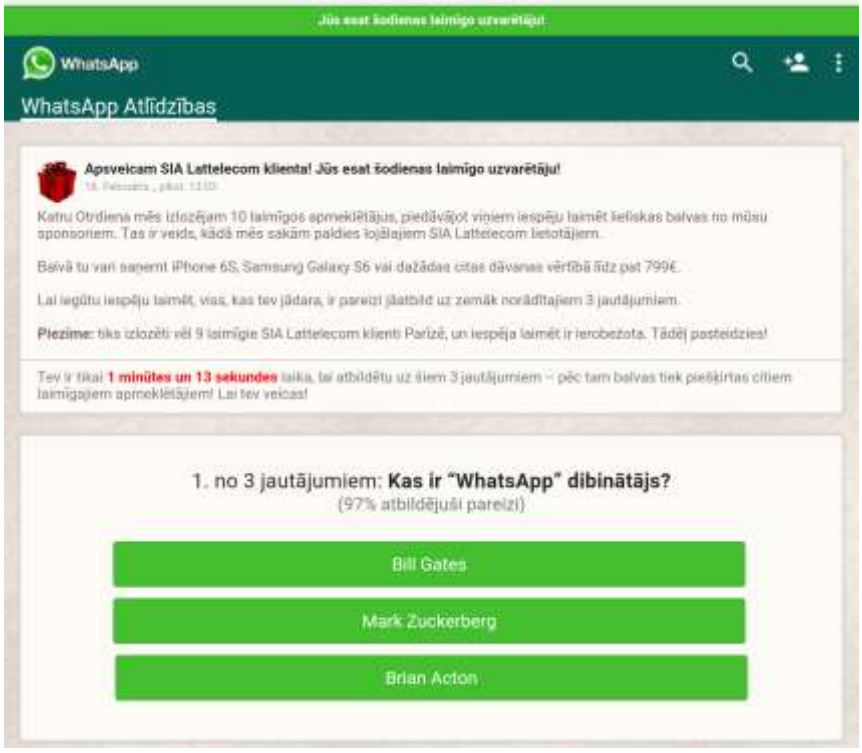
Kontakti: prese@cert.lv
Tālrunis: 67085888

Jauna šifrējošā datorvīrusa kampaņa Locky

Latviju sasnieguši pirmie šifrējošā datorvīrusa "Locky" gadījumi. Vīruss tiek izsūtīts e-pasta pielikumos - parasti kā viltus rēķins MS Word dokumentā ar iestrādātu makros datni. Tiklīdz upuris iespējo prasīto makros datni, tiek lejupielādēts izpildāmais fails, kas satur "Locky" šifrējošo izspiedējvīrusu. Vīrusam nonākot datorā, tas sašifrē tajā esošos failus, nomaina failu nosaukumus un pieprasa 0.5 Bitcoin (digitālā valūta) par failu atšifrēšanu. Diemžēl šobrīd nav zināms veids, kā citādi failus atšifrēt.
Šajā nedēļā no vīrusa cietuši vien pāris datori, taču tā kā kampaņa ir starptautiska, paredzamas jaunas vīrusa izsūtīšanas kampaņas.
Tāpat aktualizējas datu rezerves kopiju jautājums, jo no izspiedējvīrusiem visvairāk cieš tie lietotāji, kuri neveido rezerves kopijas. Savlaicīga un regulāra rezerves kopiju veidošana ir vislabākā profilakse šādiem vīrusiem, vēl bez drošības pasākumu ievērošanas un regulāras atjauninājumu veikšanas.

Viltus akcija Lattelecom vārdā

Kādā vietnē tika izvietots viltus saturs WhatsApp lietotnes un Lattelecom vārdā, aicinot piedalīties neeksistējošā akcijā, kurā var laimēt dažādas balvas. Šādā veidā tika mēģināts panākt lapas apmeklētāju pierakstīšanos uz iknedēļas abonēšanas maksu, lai it kā palielinātu izredzes laimēt loterijā.
Ekrānšāviņš no viltus lapas:



Mājas lapā paslēpts trojānis

Kādā mājas lapā tika atklāts JS/Kryptik.AZ trojānis, kas aktivizējās, atverot mājas lapu ar Internet Explorer interneta pārlūku. Šis trojānis spēj nodarīt lielu kaitējumu Windows sistēmām un var tikt lejupielādēts datorsistēmā automātiski, izpildot kaitīgas darbības. Tas var arī atslēgt drošības programmas, lai datorvīruss varētu palikt nepamanīts, tādējādi pakļaujot datoru arī citiem draudiem. Šajā gadījumā mājas lapa tika salabota un kaitējums novērsts. Nav pieejama informācija par datoru inficēšanās gadījumiem šajā incidentā.

Linux operētājsistēma pakļauta attālināta koda izpildes riskam

Šī gada 16.februārī tika atklāta GNU C bibliotēkas jeb glibc ievainojamība, kas ietekmē lielāko daļu ierīces ar Linux operētājsistēmu. Ievainojamība rodas, izmantojot getaddrinfo() bibliotēkas funkciju, kas var tikt izmantota attālināta koda izpildei. Zināms, ka ievainojamas ir glibc versijas sākot no 2.9. Ir rekomendēts veikt sistēmas atjauninājumus.
Glibc ir bibliotēka, kas definē sistēmas pieprasījumus un citas pamatfunkcijas Linux sistēmās.
Vairāk par ievainojamību: https://threatpost.com/critical-glibc-vulnerability-puts-all-linux-machines-at-risk/116261/