Iknedēļas ziņas
Sagatavotas 05.11.2015.
Numurs 2015/13

Kontakti: prese@cert.lv
Tālrunis: 67085888

Jauni CTB-Locker vīrusa izplatības gadījumi

Juristi Latvijā masveidā saņēmuši e-pasta ziņojumus ar pievienotu saiti, kas ved uz dokumentu inbox.lv failu apmaiņas vietnē. Dokuments ir .exe izpildāmais fails. Ja to lejupielādē, tas inficē ierīci ar CTB-Locker vīrusu un sašifrē uz ierīces esošos failus, prasot izpirkumu.

Kaitīgā e-pasta piemērs:

```
From: Arnolds Līdums
Sent: Wednesday, November 4, 2015 1:41 PM
To:
Subject: Sūdzība par sniegtajiem juridiskajiem pakalpojumiem!

Labdien,

Vēlos iesniegt sūdzību par jūsu sniegtajiem juridiskajiem pakalpojumiem! Ceru radīsim mierīgu risinājumu!
Ar mani jūs varat sazināties atbildot uz šo epastu vai zvanot uz tel. nr. +371 29142666

Sūdzība:
http://files.inbox.lv/ticket/b3830a69e0a52843caa49e21cd07e5e759629dfc/Sudziba_par_pakalpojumiem.pdf

Ar cieņu,
Arnolds Līdums
```

Apple lietotāju datu izkrāpšanas gadījumi turpinās

Arvien tiek saņemti ziņojumi par e-pasta vēstulēm Apple atbalsta grupas vārdā, lai izkrāptu Apple lietotāju datus.

Kaitīgā e-pasta piemērs (teksts var atšķirties):

Dear Customer

We are unable to confirm your account information.

As a result, your account has been temporarily suspended.
All the services related to your account has been suspended pending resolution.

Please provide us with your details as soon as possible..
Just click on Confirm My Account **and Log In to your ID and follow the instructions :**

Confirm My Account

This is an automated message. Please do not reply to this email. If you need additional help, visit Apple Support.

Notice: If this email was sent to you in your Junk or Spam folder please mark it as not spam due to our new security update.

No šifrēšanas vīrusa CryptoWall cietusi kāda pašvaldība

Saņemts ziņojums par kādas pašvaldības datoru, kura faili tikuši sašifrēti. Pēc sākotnējās izpētes secināts, ka uzbrukums veikts ar CryptoWall vīrusu. Tiek veikta izpēte.

Jau pagājušajā nedēļā CERT.LV ziņoja, ka Latvijā konstatēti inficēšanās gadījumi ar CryptoWall 3.0. vīrusu, kurš datorā pieejamo informāciju 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.

Sociālos tīklus izmanto pikšķerēšanas mēģinājumiem

Kādā sociālajā tīklā ar kompromitētu lietotāju kontu starpniecību tika izplatīta saite uz interneta vietni ar mērķi izkrāpt bankas karšu datus. Šobrīd kaitīgā saite padarīta nepieejama.

Jauns datorvīrusa paveids

CERT.LV saņēmis līdz šim maz zināma datorvīrusa paraugu. Datorvīruss var tikt izmantots DDoS uzbrukumu veikšanai. Sākta vīrusa izpēte. Ja vīruss inficē datoru, tad tas izveido failu ar nosaukumu "gamers.exe".