Iknedēļas ziņas
Sagatavotas 10.02.2017.
Numurs 2017/4

Aicina veikt eParakstītāja atjauninājumus

eParaksta lietotājiem ir pieejams programmatūras eParakstītājs 3.0 atjauninājums un LVRTC aicina lietotājus nekavējoties atjaunināt programmatūru eParakstītājs uz tās jaunāko versiju 1.3.9.
Programmatūras lietotājiem eParakstītājs 3.0 versijas atjauninājums tiek piedāvāts automātiski, atverot programmatūru. Tiem eParakstītāja lietotājiem, kuriem iestādes drošības politika liedz patstāvīgi veikt atjauninājumus, atverot programmatūru eParakstītājs automātisks uzaicinājums veikt atjauninājumu var neparādīties, tāpēc aicinām šī procesa organizēšanā iesaistīties IT drošības pārziņiem.
Ja iestāde izmanto arī eParaksta integrācijas risinājumus, tad jāveic arī atjauninājumi Java bibliotēkai, kas pieejami VAS LVRTC tīmekļa vietnē: https://www.eparaksts.lv/lv/palidziba/lejupielades/java-edoc-bibliotekas-1/.

Notiek SPAM uzbrukums ar mērķi izspiest naudu

Kāda finanšu iestāde informēja CERT.LV par pārdomātu un mūsdienīgu SPAM uzbrukumu ar mērķi izspiest naudu.
Sākot ar 22.01.2016. iestādei tika nosūtīti ap 60 tūkstošiem e-pastu un tika veikts neliels demonstratīvs DDoS uzbrukums, izmantojot UDP Flood.
Izsūtītie e-pasti bija no leģitīmiem serveriem, piemēram, scientificamerican.com, robly.com, u.t.t. No katra e-pasta izsūtīšanas servera tika nosūtītas ne vairāk par 20 - 30 vēstulēm. Pamatā tika izmantoti dažādi ziņu un mediju portāli, kuriem ir iespēja pierakstīties uz paziņojumiem par kādu raksta tēmu.
CERT.LV sniedza instrukcijas, kā rīkoties izspiešanas gadījumos. Tika pieprasīts slēgt uzbrucēju Google e-pasta adresi. Nav ziņas, ka solītais pilna apjoma uzbrukums būtu noticis.

Naudas izspiešanas e-pasta piemērs:
"Hi! If you dont pay 10 bitcoin until 30. january your network will be hardly ddosed and your emails continuosly bomber! Our attacks are super powerfull (Mirai botnet). And if you dont pay until 30. january ddos attack will start and price to stop will double! We are not kidding and we will already run small demo bomb on few your emails and now we do small demo now on just one of your servers to show we are serious. It will not be strong just small flood to show we are not hoax. Pay and you are safe from us forever. Ignore, your all servers go down for long time, emails massively flood and price go up. OUR BITCOIN ADDRESS: 1HjjxRGk3BipJfVEHA83sieXy6AgJv5kSG Dont reply, we will ignore! Pay and we will be notify you payed and you are safe. You never hear us again! Cheers! Stealth Ravens"

Akciju tirdzniecības kompānija izkrāpj naudu

27.01.2017. pie CERT.LV vērsās vīrietis, kas kļuvis par kiberkrāpniecības upuri, iesaistoties nelicenzētā akciju tirdzniecības kompānijā "Everest trade".

Vīrietis vēlējās, lai CERT.LV pārbauda kompānijas mājaslapu un pasaka, vai tā ir viltojums. Akciju tirdzniecībā vīrietis zaudējis vairāk kā 10 000 Eiro. Naudu nav iespējams atgūt, gadījums šobrīd tiek risināts policijā. Vīrietis arī devis uzbrucējiem piekļuvi pie sava datora caur remote desktop, lai parāda, kā rīkoties ar tirdzniecības platformu.

Vīrietis nosūtījis krāpniekiem savu pases kopiju, vadītāja apliecības kopiju, rēķina paraugu, kur redzama viņa dzīvesvietas adrese, un bankas kartes kopijas, aizsedzot tikai pēdējos 3 ciparus.

CERT.LV sniedza konsultācijas, kā labāk sevi pasargāt turpmāk.