Latvijas Universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

Publiskais pārskats par CERT.LV uzdevumu izpildi

2018

2018. gada 1. ceturksnis (01.01.2018. – 31.03.2018.)

Pārskatā iekļauta vispārpieejama informācija, tas nesatur informāciju par tiem CERT.LV darbības rezultātiem, kas satur ierobežotas pieejamības informāciju. Pārskatam ir tikai informatīva nozīme.

Saturs

Kopsavilkums

2018.gada 1.ceturksnī CERT.LV apkopoja informāciju par 191 822 apdraudētām IP adresēm. Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (143 026 unikālas IP adreses) ar pieaugumu 3% pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs kods (38 002 unikālas IP adreses) ar kritumu 7%, bet trešais - ielaušanās mēģinājumi (213 unikālas IP adreses) ar pieaugumu 3%.

Ļaunatūru topā uzreiz otrajā vietā ierindojās jaunpienācējs Monerominer. Ļaunatūra veic kriptovalūtas Monero (uz privātumu orientēta kriptovalūta, kas ieguvusi popularitāti kriminālajās aprindās) ieguvi, izmantojot iekārtas resursus, lietotājam to nezinot. Ļaunatūra var radīt bīstamu iekārtas noslodzi vai pat to neatgriezeniski sabojāt. Kriptovalūtas ieguves ļaunatūras kļuva populāras pēc negaidīti straujā kriptovalūtu cenu kāpuma 2017.gada nogalē.

Pārskata periods iezīmējās ar virkni DDoS uzbrukumu, kas ieguva arī plašu rezonansi medijos. Perioda sākumā DDoS uzbrukumu piedzīvoja e-veselība, kuras darbība pārslodzes rezultātā uz laiku tika pārtraukta. Datu noplūde šajā uzbrukumā nenotika. Paralēli e-veselībai DDoS uzbrukumam tika pakļauts arī nacionālais ziņu portāls LETA un vairākas valsts iestāžu tīmekļa vietnes. Veicot visu augšminēto uzbrukumu analīzi, tika novērota zināma uzbrukumos iesaistīto resursu sakritība.

Lielai daļai pārskata periodā DDoS uzbrukumiem pakļauto sistēmu netika nodrošināta vai bija nepietiekama DDoS aizsardzība.

Beidzot ieviešot labās prakses standartu BCP-38 vismaz Eiropas līmenī, būtu iespējams rast risinājumu DDoS uzbrukumu problēmai, novēršot iespēju izsūtīt tīkla paketes ar viltotu paketes avotu (IP spoofing), kas ir lielākās daļas DDoS uzbrukumu pamatā. Tas ļautu samazināt arī resursu uzturēšanas izmaksas uz DDoS aizsardzības risinājumu rēķina.

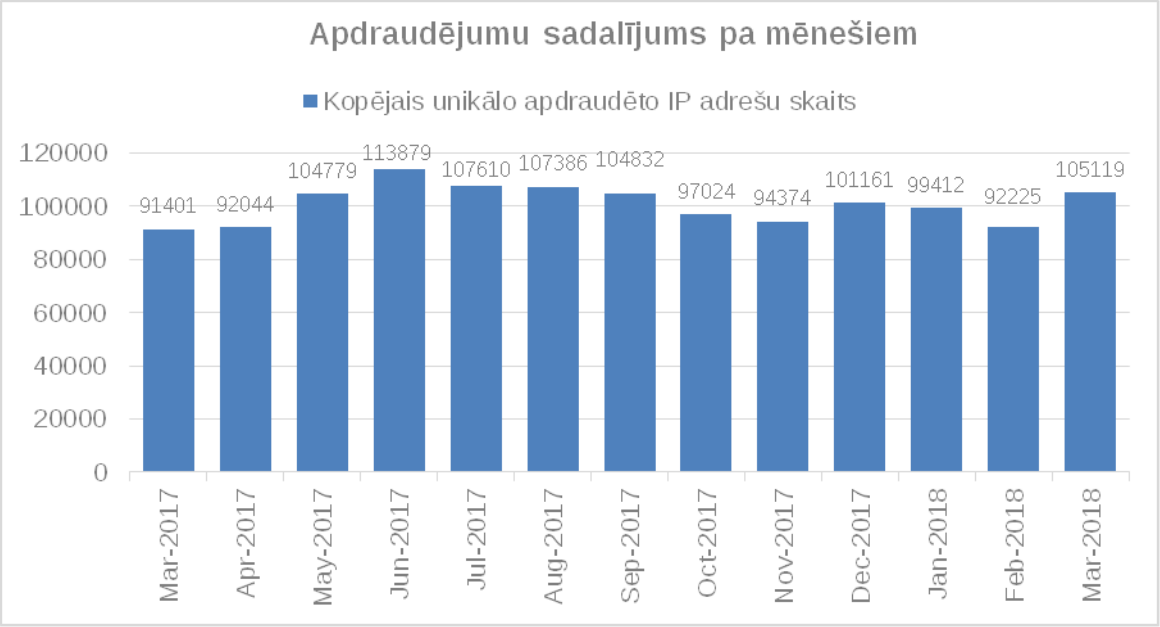
Pārskata periodā CERT.LV sadarbībā ar NATO CCDCoE pirmo reizi Latvijā organizēja tehniskās kiberdrošības mācības „Crossed Swords 2018". Tās bija līdz šim tehniski sarežģītākās un izaicinošākās mācības, kas aptvēra vairākus ģeogrāfiskus atrašanās punktus, iesaistot tajās gan informācijas tehnoloģiju (IT) kritiskās infrastruktūras uzturētājus, gan militārās vienības. Mācībās piedalījās vairāk kā astoņdesmit kiberdrošības ekspertu no piecpadsmit NATO CCD CoE dalībvalstīm

Pārskata periodā CERT.LV par IT drošību izglītoja 2292 cilvēkus, iesaistoties 36 izglītojošos pasākumos.

1. Elektroniskās informācijas telpā notiekošo darbību atainojums.

Ik mēnesi CERT.LV apkopo informāciju par apdraudētajām Latvijas IP adresēm. Lai sniegtu pilnvērtīgāku Latvijas kibertelpas pārskatu un nodrošinātu datu starptautisku salīdzināmību, no 2017. gada 1. janvāra apdraudējumu uzskaitei CERT.LV izmanto starptautiski lietotu incidentu taksonomiju (eCSIRT.net projekta izveidotā taksonomija). Statistikā visi CERT.LV reģistrētie apdraudējumi tiek uzskaitīt vienkopus, sadalot tos pa apdraudējumu veidiem (piemēram, ļaunatūra, ielaušanās, krāpšana), kā arī pa infekciju (piemēram, *Confiker, Zeus, Mirai*) un ievainojamību (piemēram, *Opendns, Openrdp*) tipiem.

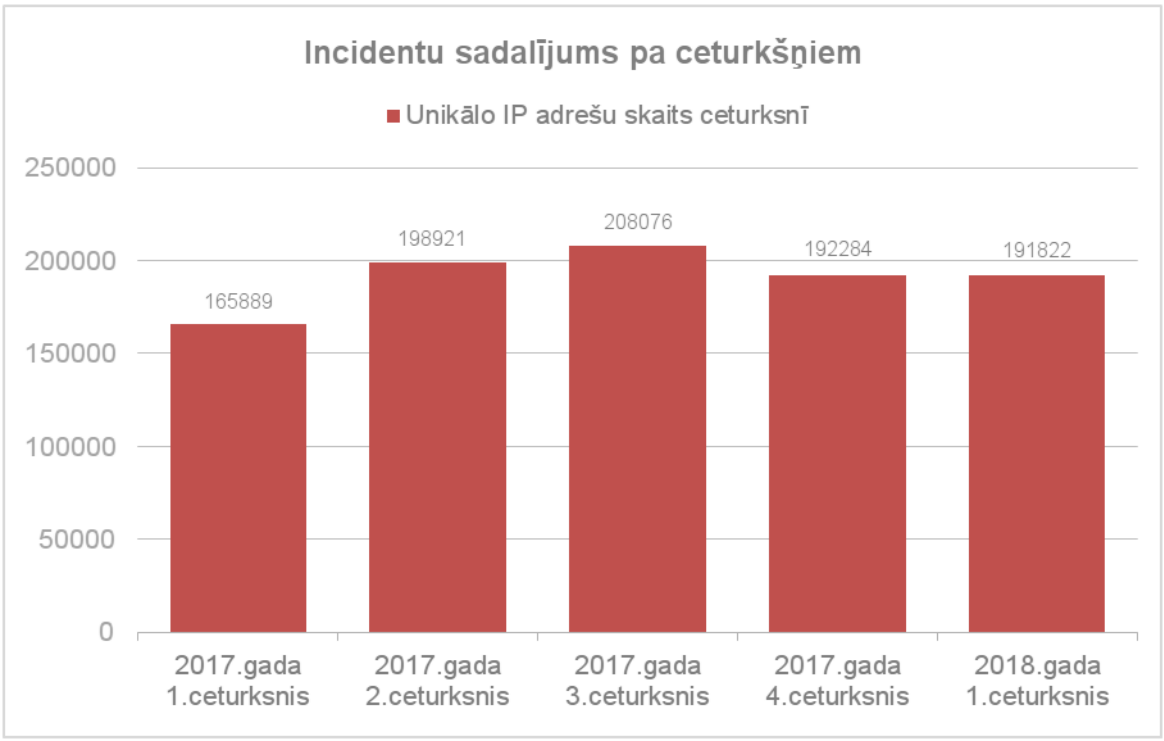
CERT.LV pārskata periodā ik mēnesi apkopoja informāciju par 90 000 – 105 000 ievainojamu unikālu IP adrešu.



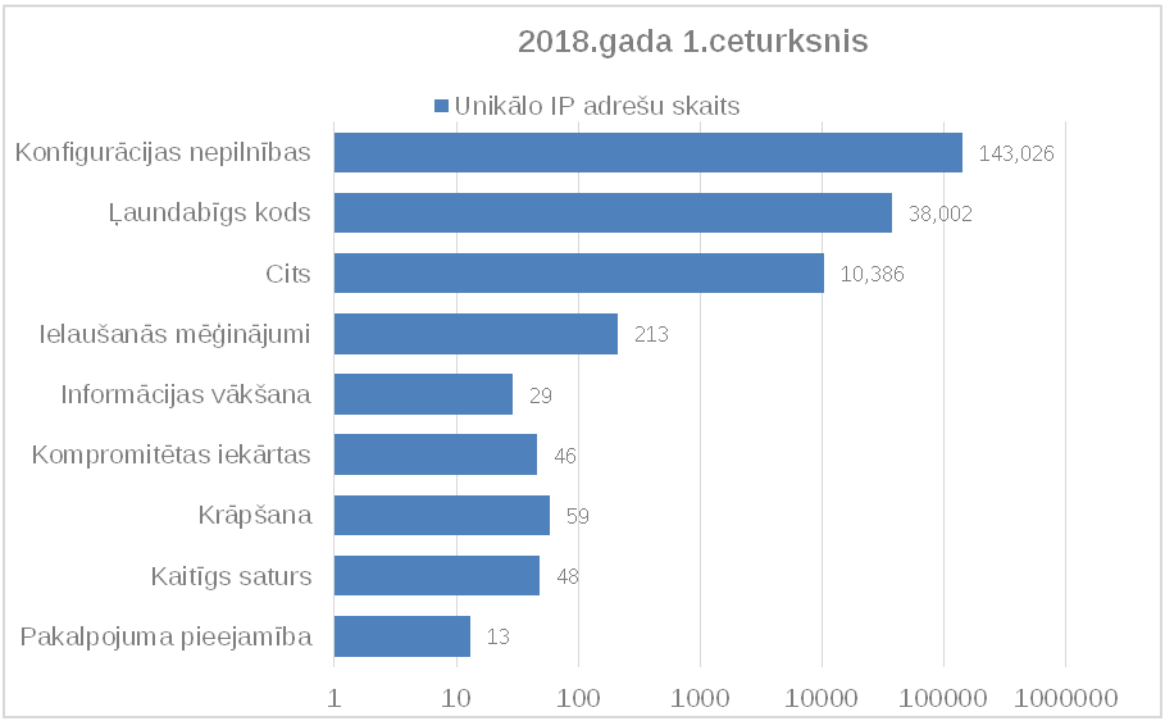
1.attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa mēnešiem 12 mēnešu griezumā.

Pārskata periodā nav vērojamas būtiskas izmaiņas mēnesī reģistrēto apdraudēto IP adrešu daudzumā.

2018. gada 1. ceturksnī tika reģistrētas 191 822 unikālas apdraudētas IP adreses, kas ir par nepilnu 1% mazāk nekā iepriekšējā ceturksnī un par 15% vairāk nekā šajā pašā periodā pirms gada.

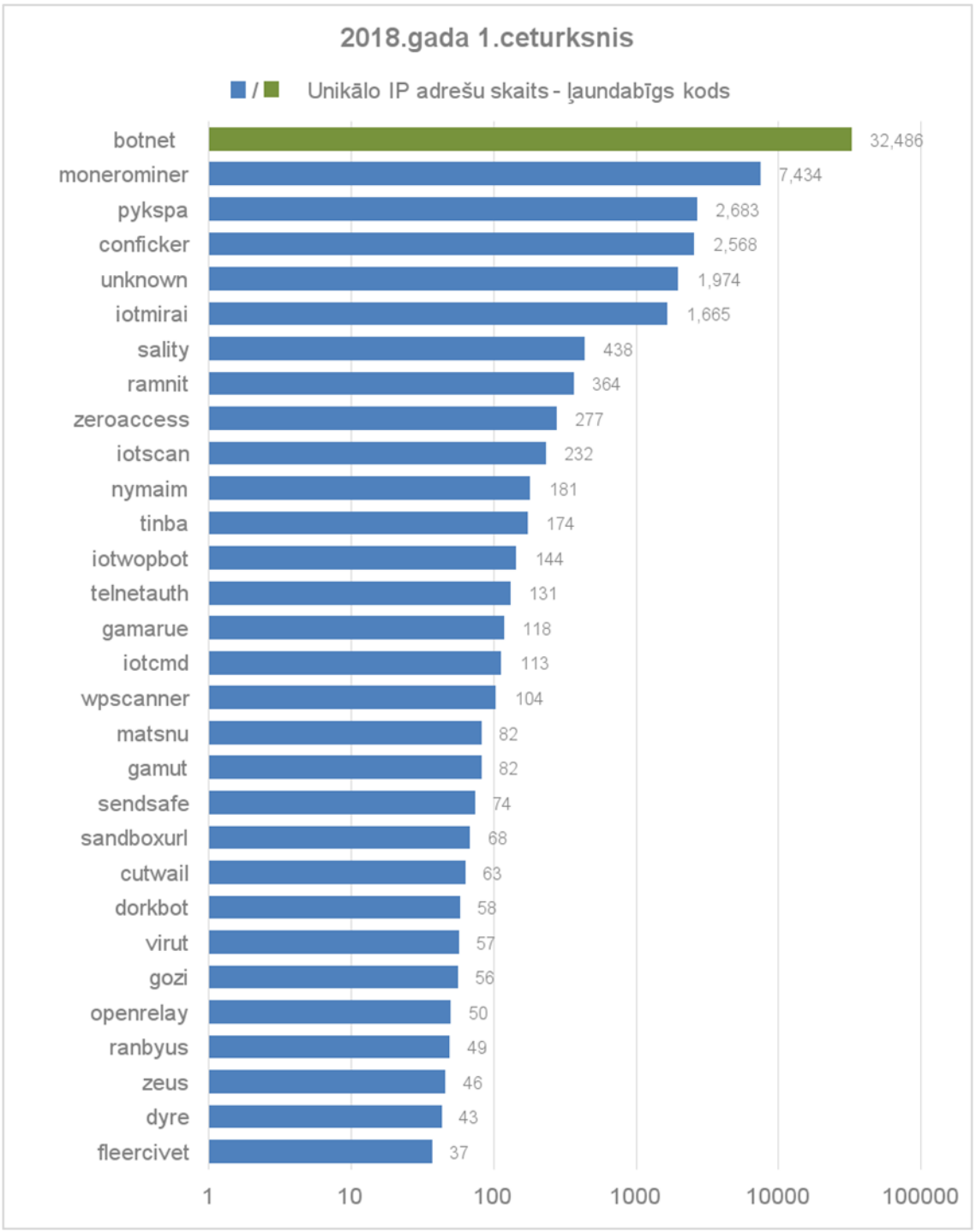


2.attēls – CERT.LV reģistrētās apdraudētās IP adreses pa ceturkšņiem 2017. un 2018. gadā.



3.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2018. gada 1. ceturksnī pa apdraudējumu veidiem.

Izplatītākais apdraudējuma veids pārskata periodā nemainīgi bija konfigurācijas nepilnības (pieaugums par 3% pret iepriekšējo periodu), otrs izplatītākais bija ļaundabīgs kods (kritums par 7%), bet trešais - ielaušanās mēģinājumi (pieaugums par 3%).



4.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2018. gada 1. ceturksnī ar apdraudējuma veidu - ļaundabīgs kods.

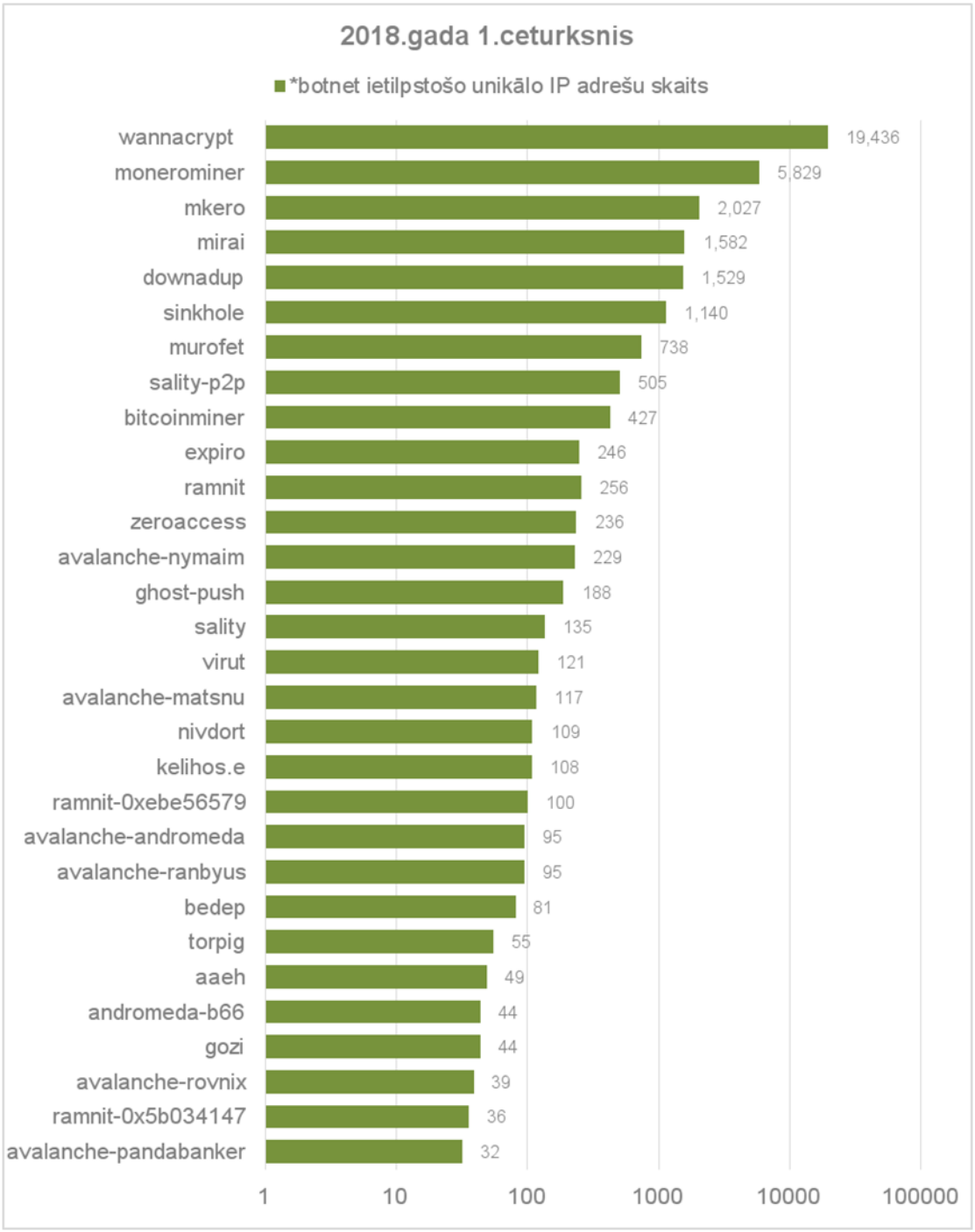
Pirmo vietu ļaunatūras izplatības topā šajā ceturksnī stabili ieņem *botnet* ļaundabīgā koda grupa; tās detalizēts atšifrējums redzams 4.1.grafikā.

Otro vietu ļaunatūru topā ieņem ceturkšņa jaunpienācējs – *Moneromіner*. Ļaunatūra veic kriptovalūtas Monero (uz privātumu orientēta kriptovalūta, kas ieguvusi popularitāti kriminālajās aprindās) ieguvi, izmantojot iekārtas resursus, lietotājam to nezinot. Nesaudzīgi izmantojot iekārtas jaudu, var bīstami noslogot iekārtu vai pat to neatgriezeniski sabojāt. Kriptovalūtas ieguves ļaunatūras kļuva populāras pēc negaidīti straujā kriptovalūtu cenu kāpuma 2017.gada nogalē. Topā ienākot *Moneromіner* ļaunatūrai, par 45% kritās *Bitcoinminer* ļaunatūras apjoms (Bitcoin ir viena no plašāk pazīstamajām kriptovalūtām, un tās ieguve ir kļuvusi ļoti resursietilpīga).

Vietu ļaunatūras topa augšgalā nemainīgi saglabā *Conficker*, kaut arī tā ir jau sen pazīstama un salīdzinoši vienkārši „ārstējama" ļaunatūra.

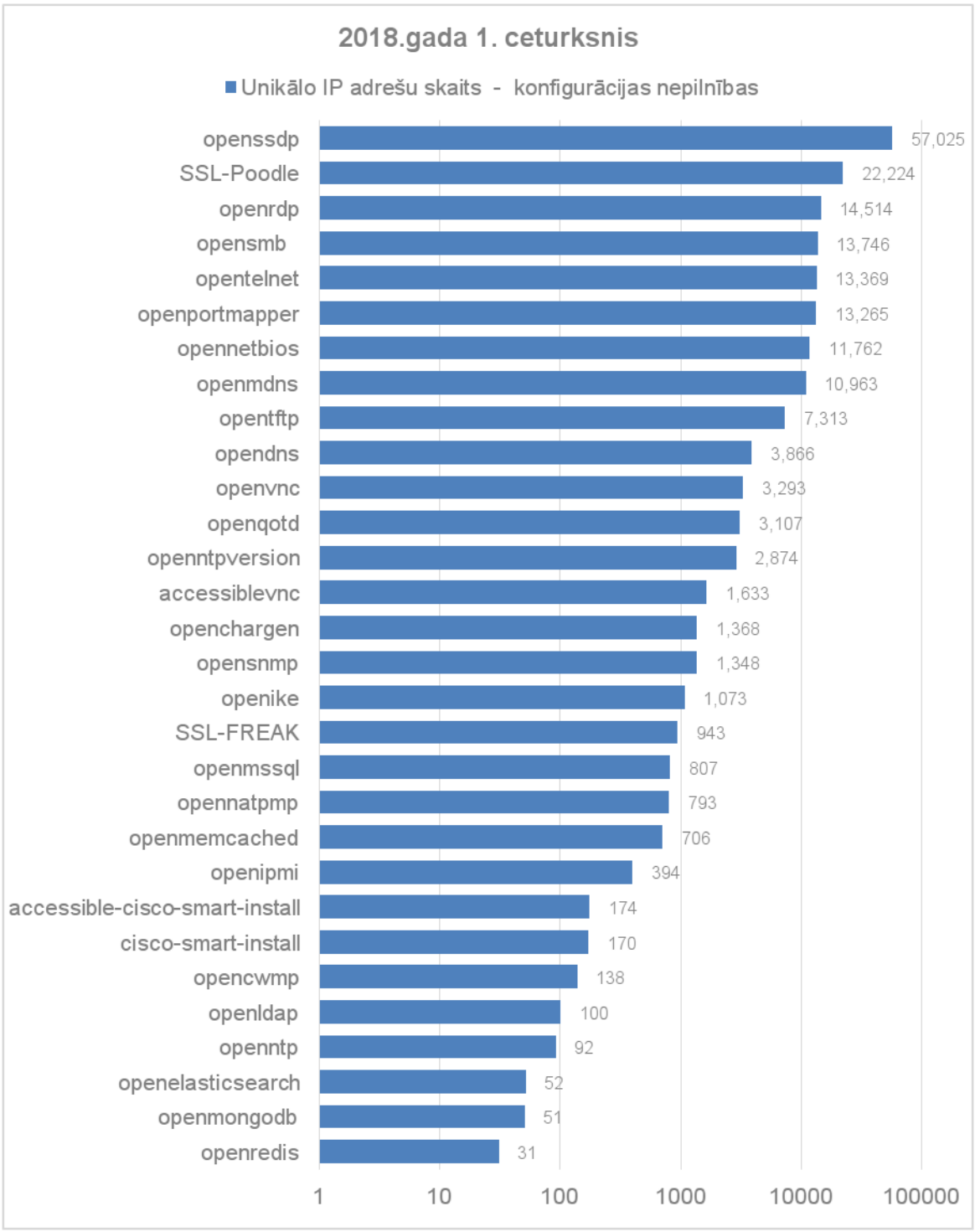
Nākamā izplatītākā ļaunatūra aiz *Conficer* topa augšgalā ir Iotmirai, kas apdraud neatbilstoši konfigurētas un nepietiekami aizsargātas IoT (lietu internets) iekārtas, iekļaujot tās robotu tīklos, kas tiek izmantoti tālākiem uzbrukumiem.

Arī *Mirai* ir ļaunatūra, kas apdraud neatbilstoši aizsargātas IoT iekārtas, un šīs ļaunatūras apjoms šajā ceturksnī ir pieaudzis par gandrīz 50%.



4.1.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2018. gada 1. ceturksnī ar apdraudējuma veidu - ļaundabīgs kods.

Augsti izplatības rādītāji joprojām ir ļaunatūrai *WannaCry* (*WannaCrypt*), taču šajā ceturksnī vērojams tās apjoma kritums par gandrīz 7500 IP adresēm (~30%) salīdzinājumā ar iepriekšējo periodu.



5.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2018. gada 1. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

Opensmb - diezgan plaši izplatīta konfigurācijas nepilnība, kas bija vainojama tādu šifrējošo izspiedējvīrusu kā *WannaCry* un *NotPetya* straujajā izplatībā – no piektās vietas pagājušajā ceturksnī pakāpusies uz ceturto vietu.

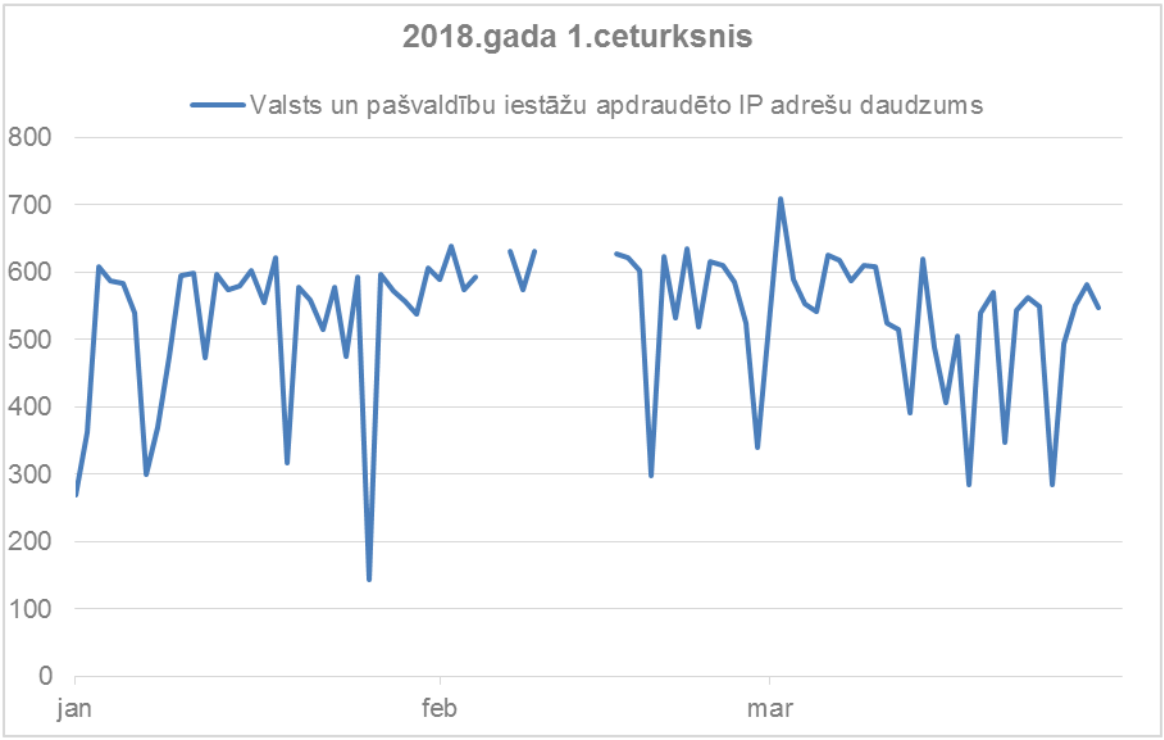
Savukārt pirmo vietu ieņem *OpenSSDP* – iekārtas ar nedrošu konfigurāciju, kas var tikt izmantotas apjomīgos piekļuves atteices (DoS) uzbrukumos. Simple Service Discovery Protocol (SSDP) ir iebūvēts daudzās tīkla iekārtās, lai tās veiklāk varētu „atrast" viena otru un savstarpēji sazināties.

Lai samazinātu kopējo apdraudēto IP adrešu skaitu, CERT.LV kopā ar Latvijas Interneta asociācijas Net-Safe Latvija Drošāka interneta centru ir izveidojuši saprašanās memorandu, kas tiek slēgts ar interneta pakalpojumu sniedzējiem (IPS), kas vēlas pievienoties iniciatīvai „Atbildīgs interneta pakalpojumu sniedzējs" un informēt savus klientus par to iekārtās konstatētajiem apdraudējumiem. Atbildīgo IPS skaits līdz pārskata perioda beigām saglabājās bez izmaiņām – 13.

2. Atbalsts informācijas tehnoloģiju drošības incidentu novēršanā vai to novēršanas koordinēšanā.

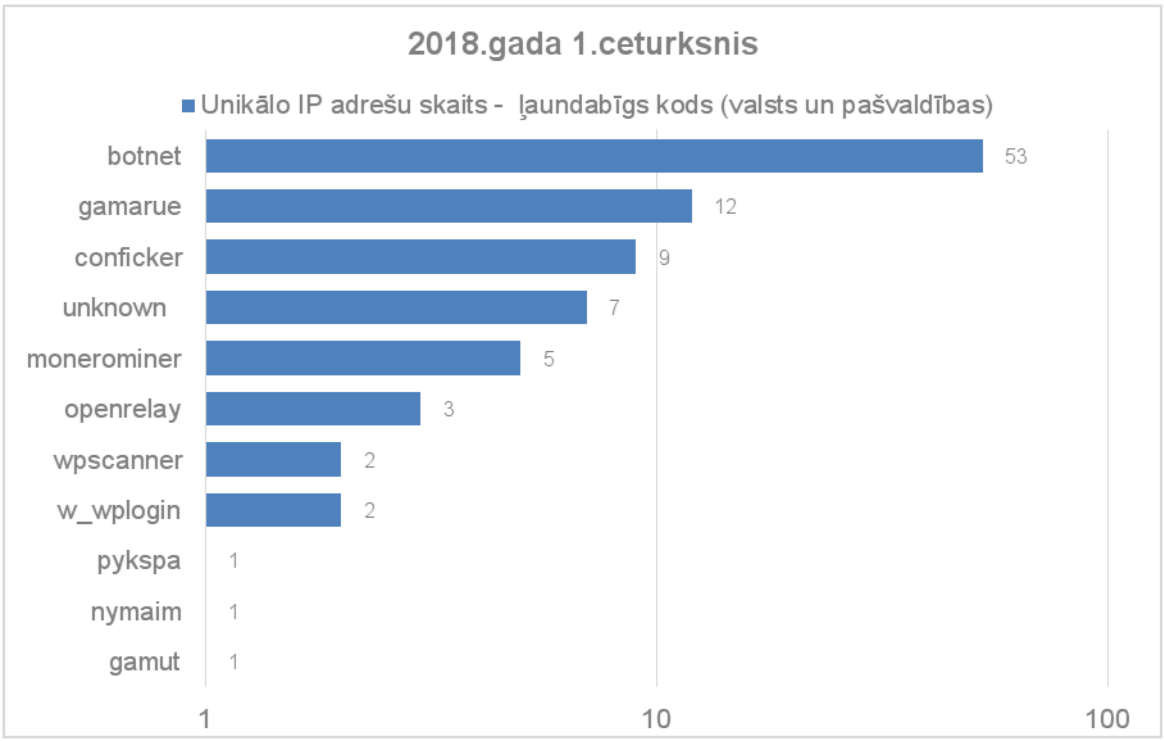
CERT.LV apkopo informāciju no valsts un pašvaldību institūcijām par to izmantotajām IP adresēm un tīmekļa vietnēm, lai CERT.LV varētu operatīvāk reaģēt šo iestāžu IT drošības incidentu gadījumos. CERT.LV informē valsts un pašvaldību institūcijas, ja viņu IP adreses uzrādās kādā no ziņojumiem kā apdraudētas.

Izmaiņas katras dienas saņemtajos ziņojumos par valsts un pašvaldību iestādēm:

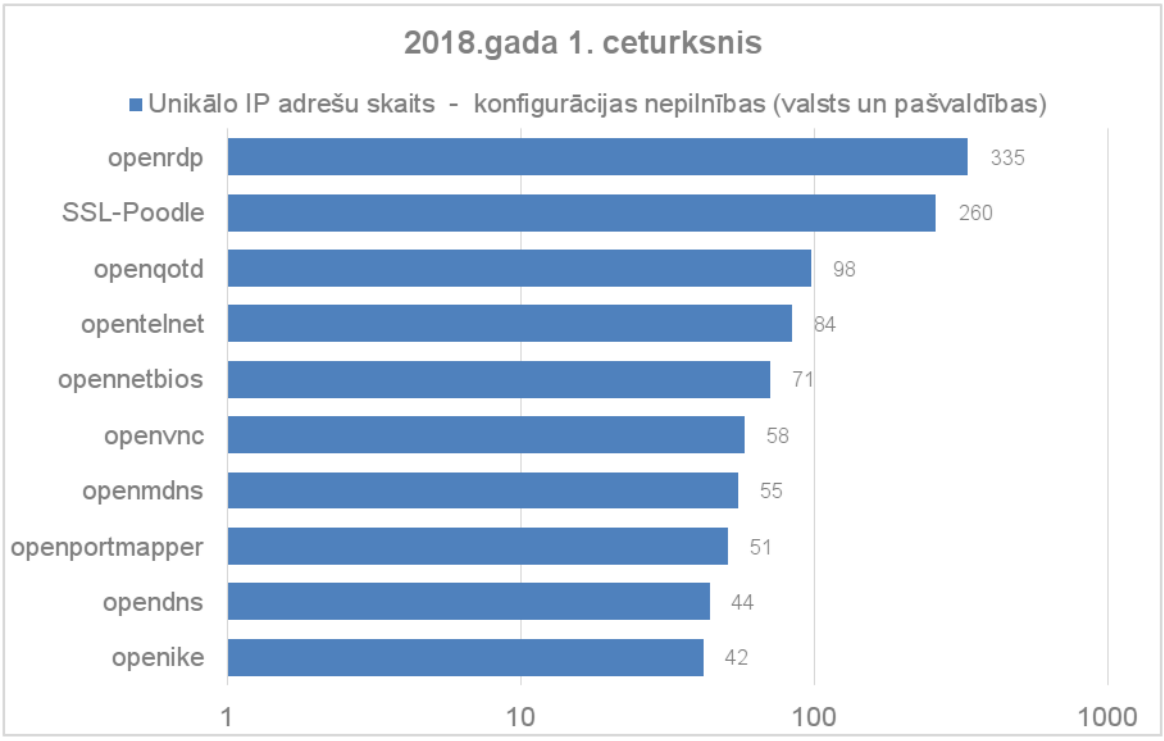


6.attēls – Iestāžu apdraudēto IP adrešu daudzums katras dienas saņemtajos ziņojumos 2018. gada 1. ceturksnī.

Vidējais apdraudēto valsts un pašvaldību iestāžu IP adrešu daudzums katras dienas saņemtajos ziņojumos pārskata periodā bija 600 unikālas IP adreses dienā. Samazinājums salīdzinājumā ar iepriekšējo pārskata periodu (iepriekš vidēji 1500 unikālas IP adreses dienā) skaidrojams ar veiktajām izmaiņām statistikas apkopošanas algoritmā.

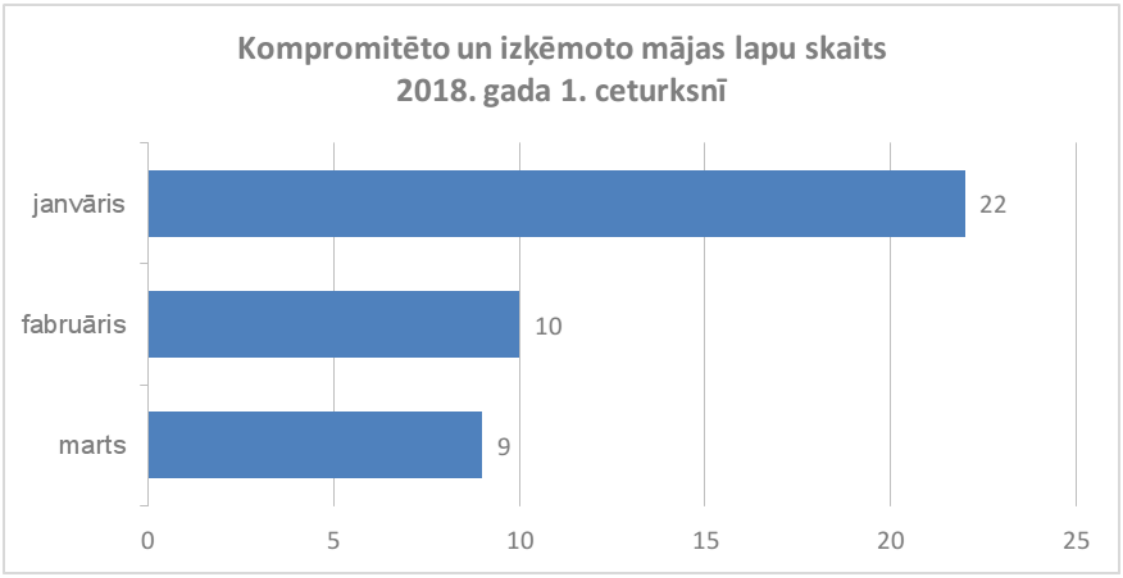


7.attēls - CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2018. gada 1. ceturksnī ar apdraudējuma veidu – ļaundabīgs kods (TOP 10 ļaundabīgs kods).



8.attēls - CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2018. gada 1. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība (TOP 10 konfigurācijas nepilnības).

CERT.LV uzskaita arī kompromitēto un izķēmoto tīmekļa vietņu gadījumus. Pārskata periodā tika fiksēta 41 kompromitēta un izķēmota tīmekļa vietne. No visām izķēmotajām vietnēm 40 gadījumos vietnes uzturēšanai tika izmantota Linux operētājsistēma, 1 gadījumā - FreeBSD. Viena no visām pārskata periodā izķēmotajām tīmekļa vietnēm pēdējā gada laikā izķēmota atkārtoti.



9.attēls – Kompromitēto un izķēmoto tīmekļa vietņu skaits pa mēnešiem 2018. gada 1. ceturksnī.

CERT.LV sadarbojās ar valsts un pašvaldību institūcijām, bankām, interneta pakalpojumu sniedzējiem un citām organizācijām dažādas bīstamības incidentu risināšanā. Visos zemāk aplūkotajos incidentos uzbrukumu mēģinājumi bijuši nesekmīgi un zaudējumi nav radīti, ja vien nav norādīts citādi

DDoS

Janvārī pakalpojumu atteices uzbrukumu (DDoS) piedzīvoja veselības aprūpes kvalitātes un efektivitātes uzlabošanas programma e-veselība. Sistēma uz laiku tika padarīta nepieejama, bet datu noplūde nenotika. Uzbrukumu izdevās apturēt, atslēdzot sistēmai piekļuvi no ārvalstīm. Izpētes rezultātā tika secināts, ka sistēmai netika nodrošināta pienācīga DDoS aizsardzība.

Paralēli e-veselības sistēmai DDoS uzbrukumi tika veikti arī ziņu portālam LETA, kura darbība uz laiku tika traucēta, un vēl vairākām valsts iestāžu tīmekļa vietnēm. Veicot visu augšminēto uzbrukumu analīzi, tika novērota zināma uzbrukumos iesaistīto resursu sakritība.

Tika saņemts ziņojums par vēl vienu iespējamu uzbrukumu kādas valsts iestādes sistēmai. Sistēma piedzīvoja periodisku pārslodzi, kas apgrūtināja un brīžiem traucēja sistēmas darbību. Izpētes rezultātā tika noskaidrots, ka problēmu radīja neatbilstoši konfigurēta darbinieku apmācības programma, kā rezultātā darbinieki, izmantojot mācību vidi, negribot kļuva par uzbrucējiem.

CERT.LV veica vairāku pārslodzes uzbrukumu analīzi, kas tika vērsti pret kādu mediju portālu. Tika konstatēts, ka uzbrukuma avots atradās ārpus Latvijas. CERT.LV sniedza ieteikumus aizsardzības uzlabošanai pret DDoS uzbrukumiem.

DDoS uzbrukums tika vērsts arī pret interneta vietni bilesuparadize.lv. Uzbrukums pārslogoja sistēmu, kas jau piedzīvoja palielinātu noslodzi saistībā ar XXVI Vispārējo latviešu Dziesmu un XVI Deju svētku biļešu tirdzniecības uzsākšanu. CERT.LV sniedza ieteikumus DDoS aizsardzības uzlabošanai.

Pikšķerēšana

Tika fiksēti vairāki kampaņveidīgi mēģinājumi izkrāpt e-pasta lietotāju piekļuves datus. Lietotāji saņēma e-pastus, kuros tika aicināti gan veikt atjauninājumus, gan novērst it kā radušās problēmas, atbildot uz krāpniecisko e-pastu un norādot savus lietotāja datus. Kampaņas tika vērstas gan uz uzņēmumiem, gan valsts un pašvaldību iestādēm.

Tika saņemti arī vairāki ziņojumi par tiešsaistes platformu PayPal un Apple piekļuves datu izkrāpšanas mēģinājumiem. Krāpnieciskos e-pastos nosūtīti aicinājumi autentificēties atbilstošajās vietnēs, sekojot e-pastā norādītajai saitei, lai atrisinātu it kā radušos piekļuves vai pakalpojuma izmantošanas problēmu.

Google konta piekļuves datu izkrāpšanas mēģinājumā upurim tika nosūtīts e-pasts, kurā papildinformācijas iegūšanai lietotājs tika aicināts aplūkot neīstu Google dokumentu, ievadot savu Google konta lietotājvārdu un paroli.

Pārskata periodā izplatīta bija personas datu pikšķerēšana, upurim nosūtot e-pastu ar aicinājumu sūtīt personīgu informāciju (vārds, uzvārds, adrese, dzimšanas dati, pases kopija), lai saņemtu laimestu, mantojumu, kompensāciju vai vienkārši naudas pārskaitījumu.

Savukārt uzņēmumiem joprojām aktīvi tika iesūtītas e-pasta vēstules uzņēmuma vadītāja vārdā ar jautājumu par konta atlikumu un iespēju veikt steidzamu pārskaitījumu uz ārvalstīm. Ticamības palielināšanai summas netika izvēlētas “apaļas”, piemēram, 52 826.81 eiro. Daži e-pasti sagatavoti labā latviešu valodā.

Viens no krāpnieciskajiem e-pastiem tika noformēts kā pēdējais brīdinājums parāda atmaksai pirms lietas nodošanas parādu piedzinējiem.

Tika saņemts arī lūgums palīdzēt izvērtēt iepirkšanās vietnes uzticamību. Pārbaudē konstatēts, ka vietne nav uzticama. Lietotājam tika nosūtīta saite uz portālu esidross.lv, kur var iepazīties ar padomiem drošākai interneta pārlūkošanai.

Tika saņemta informācija par vairākām uzlauztām .lv vietnēm un Latvijas IP adresēm, kurās tika izvietota pikšķerēšana, kas vērsta uz ārvalstu banku, PayPal, Apple un MS Office 365 klientiem.

Vairāki lietotāji ziņoja arī par maldinošu vietni, kurā neuzmanīgiem lietotājiem piedāvā aizpildīt anketu, sniedzot savus personas datus un bankas informāciju, kā arī veikt pārskaitījumu 1 USD apmērā, lai iegūtu iPhone. Vietnē ievietotā nemanāmā atrunā tika norādīts, ka informācijas sniegšana negarantē iPhone saņemšanu un ka, sniedzot datus, lietotājs piekrīt pakalpojuma abonēšanai, kura maksa ir 49 USD mēnesī.

Krāpšana

Kādai sievietei tika izkrāpti 1000 EUR. Iepazīšanās nolūkos tika uzsākts kontakts ar svešinieku, saziņai izmantojot Skype. Svešinieks apgalvojis, ka ir jūrnieks, kurš vēlas priekšlaicīgi lauzt darba līgumu un atgriezties Latvijā, bet nepieciešamas finanses jurista pakalpojumu apmaksai.

Saņemts arī ziņojums par mēģinājumu izspiest maksājumu 290 USD (izmantojot bitcoin), lai nepublicētu video, kas it kā uzņemts ar tīkla kameru, lietotājam apmeklējot pieaugušo satura vietni. Lietotājam tika ieteikts nemaksāt un ar izspiedējiem nekomunicēt.

Ielaušanās un mēģinājumi

Tika saņemti ziņojumi par uzbrukumu mēģinājumiem Sony Interactive Entertainment LLC tīkla servisiem no Latvijas IP adresēm ar mērķi iegūt piekļuvi lietotāju kontiem.

Ļaunatūra

Tika saņemti ziņojumi lielākoties par ļaundabīga koda izplatīšanu ar e-pastu starpniecību, pievienojot e-pastam ISO diska attēlu, ZIP arhīvu ar izpildāmiem .EXE failiem, vai .DOC dokumenta datni. Atsevišķos gadījumos e-pastā tika norādīta saite, kuru aktivizējot, notika vīrusa ielāde no interneta.

Vairumā gadījumu lietotājiem nosūtītais ļaundabīgais kods bija paredzēts lietotāju elektroniskās informācijas (lietotājvārdi, paroles) iegūšanai, lai to nosūtītu uz saimniekserveri. Tika saņemti arī vairāki ziņojumi par šifrējošo izspiedējvīrusu iekļūšanu sistēmā. Par šo uzbrukumu upuriem pamatā tika izvēlēti uzņēmumi. Visos gadījumos dati atjaunoti no rezerves kopijām.

Kādam uzņēmumam tika atsūtīta e-pasta vēstule it kā IBM Trusteer Rapport vārdā ar brīdinājumu, ka uzņēmuma resursi tiek izmantoti pikšķerēšanas uzbrukumos. Lai iepazītos ar incidenta plašāku aprakstu, tika norādīts uz e-pastam pievienoto .DOC datni, kas saturēja lietotāju datus (lietotājvārdi, paroles) ievācošu ļaunatūru.

Tika saņemti arī vairāki ziņojumi par Latvijas IP adresēs uzturētiem kontrol- un komandcentriem: tārpa Dorkbot (nodrošina sāneju – backdoor – upura iekārtā) kontrolieri, Hancitor (ļaunatūra, kas tiek piegādāta ar inficētiem MS Office dokumentiem un tiek izmantota citu ļaunatūru, piemēram, banku trojāņu vai izspiedējvīrusu lejupielādei) kontrolieri, JBifrost (attālinātās piekļuves trojāņa RAT modifikācija) kontrolieri un Neutrino mūķa (exploit kit) kontrolieri.

Mobilā ļaunatūra

Pārskata periodā netika fiksēti incidenti, kas skar mobilās iekārtas.

Ievainojamības procesoru darbībā

Ceturkšņa sākumā tika konstatētas divas kritiskas ievainojamības - Meltdown un Spectre - galvenokārt Intel, AMD un ARM izstrādātajos procesoros, kas sniedz iespēju potenciālajiem uzbrucējiem nozagt sensitīvus datus, piemēram, paroles un citu lietotāja informāciju. CERT.LV pagaidām nav saņēmis informāciju, ka Latvijā minētās ievainojamības būtu sekmīgi izmantotas uzbrukumam.

CERT.LV pasākumi incidentu novēršanā:

- Informācija par jaunatklātiem apdraudējumiem un ievainojamībām tiek publicēta CERT.LV sagatavotajās ziņās un sociālā tīkla Twitter kontā (@certlv).

Cita veida sadarbība ar dažādām iestādēm ir norādīta atskaites 6. punktā.

3. Pētnieciskais darbs, izglītojošo pasākumu organizēšana un mācības informācijas tehnoloģiju drošības jomā.

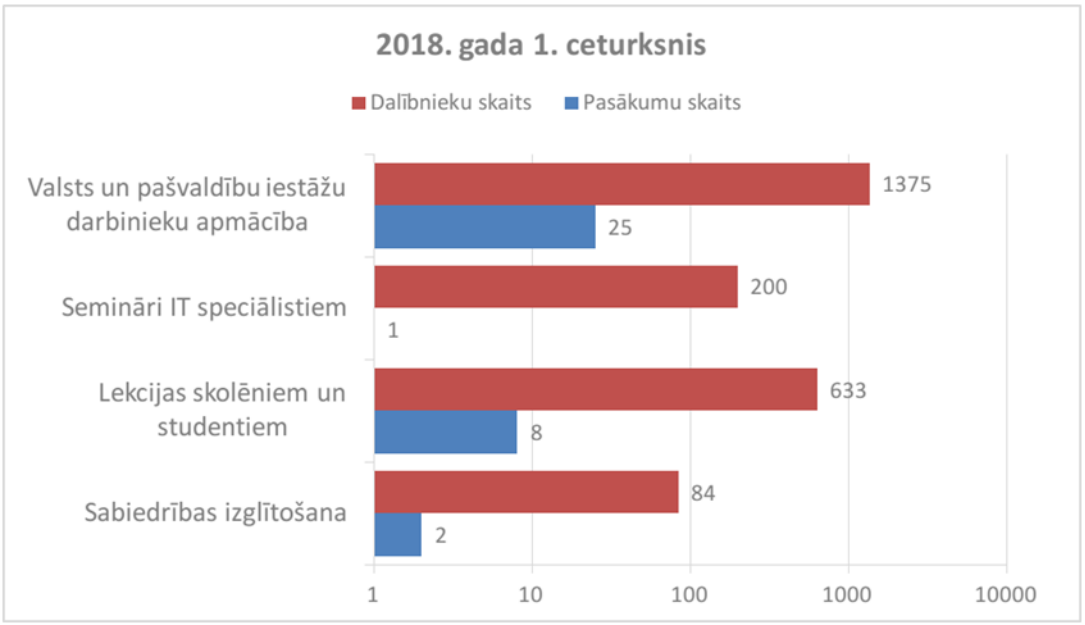
16. februārī norisinājās kiberdrošības hakatons Garage48, kurā mentora statusā iejutās arī CERT.LV eksperts. Pasākums pulcēja dažādu nozaru speciālistus, kuri izstrādāja un vēlāk komandās attīstīja dažādas kiberdrošības idejas. Mentoru uzdevums bija komandām palīdzēt ar padomiem un ieteikumiem izvēlētās idejas attīstīšanai.

19.-23. marts bija Digitālā nedēļa, kuras ietvaros 20. martā tika atzīmēta Digitālās drošības diena un tika organizētas vairākas diskusijas-tiešraides. CERT.LV piedalījās diskusijā „Drošība un pārliecība digitālajā vidē" un pasākumā „Kiberdrošības nakts", kas bija augsta līmeņa ekspertu diskusija par nacionālās kiberdrošības jautājumiem.

21. martā CERT.LV organizēja kiberdrošības semināru „Esi drošs". Semināra tēmas: ievainojamību Meltdown un Spectre ietekme, mākoņdatošanas iespējas un riski, NIS direktīvas ieviešana Latvijā, Vispārīgā datu aizsardzības regula un drošības prasības, kā arī iepazīšanās ar CERT.LV un NIC.LV DNS ugunsmūra projektu. Pasākumam pieteicās 250 interesenti, bet klātienē to apmeklēja 200 IT drošības speciālisti.

Sadarbībā ar Valsts policiju un Drošāka interneta centru tika izstrādāta mobilā lietotne pusaudžiem „Mana drošība". Tā sniedz iespēju pārbaudīt savas zināšanas par drošību internetā, aizpildot interaktīvu testu un izspēlējot improvizētu „čatu", kā arī turpat lietotnē ziņot par kaitīgu un nelegālu saturu vai problēmsituācijām.

Pārskata periodā CERT.LV par IT drošību izglītoja 2292 cilvēkus, iesaistoties 36 izglītojošos pasākumos.



10.attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2018. gada 1. ceturksnī

4. Atbalsts valsts institūcijām valsts drošības sargāšanā, noziedzīgu nodarījumu un likumpārkāpumu atklāšanā.

Sadarbības tikšanās, konsultācijas un prezentācijas:

- CERT.LV piedalījās likumdošanas paketes izstrādē, lai Latvijā varētu tikt ieviesta NIS (Tīklu un informācijas drošības) direktīva. Šī procesa ietvaros CERT.LV kopā ar Aizsardzības ministriju piedalījās izmaiņu sagatavošanā Informācijas tehnoloģiju drošības likumam un MK noteikumiem Nr.442 (Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām), lai tos varētu attiecināt uz pamatpakalpojumu sniedzējiem, digitālo pakalpojumu sniedzējiem un kritisko infrastruktūru. Papildu izmaiņas būs nepieciešamas arī citos saistītajos MK noteikumos. Paralēli noritēja darbs pie vairāku jaunu MK noteikumu izstrādes, kas noteiks, kuras organizācijas būs pamatpakalpojumu sniedzēji NIS direktīva izpratnē, kādi būs ziņojamo incidentu sliekšņi un incidentu paziņošanas kārtība.
- Dalība Saeimas sēdē un tikšanās ar Saeimas Juridisko biroju, lai piedalītos izmaiņu sagatavošanā, kas saistītas ar identificēto nepieciešamību grozīt Elektronisko sakaru likumu un Informācijas tehnoloģiju drošības likumu, kuri šobrīd nosaka, ka lēmums par domēna vārda atslēgšanu un citām papildu darbībām ir jāpieņem augstākā līmeņa domēna .lv reģistra uzturētājam pēc Drošības incidentu novēršanas institūcijas pieprasījuma. Praksē konstatēts, ka Drošības incidentu novēršanas institūcija, nodrošinot atbalstu drošības incidenta novēršanā, ir tā, kas izvērtē un pieņem lēmumu par domēna vārda atslēgšanu un citām nepieciešamajām papildu darbībām. Drošības incidentu novēršanas institūcija ir vienīgā iestāde, kuras rīcībā ir fakti un informācija, kas nepieciešama lēmuma pieņemšanai atbilstoši Administratīvā procesa likuma normām. Savukārt augstākā līmeņa domēna .lv reģistra uzturētājam būtu tikai jānodrošina lēmuma izpilde.

Sadarbība ar valsts iestādēm incidentu risināšanā aplūkota atskaites 2. punktā.

5. Sadarbība ar starptautiski atzītām informācijas tehnoloģiju drošības incidentu novēršanas institūcijām.

CERT.LV starptautiskā sadarbība pārskata periodā:

- NIS (Tīklu un informācijas drošības) direktīvas CERTu tīkla ietvaros CERT.LV pārstāvis piedalās "CSIRT Maturity" darba grupā. Šīs darba grupas ietvaros CERT.LV piedalījās nozares ekspertu (peer-review) audita vizītē Portugālē, Lisabonā, kur tika auditēta CERT.PT komanda (Portugāles valdības un nacionālais CERT), izmantojot SIM3 metodoloģiju (Security Incident Management Maturity Model) un „CSIRT Maturity" darba grupas vadlīnijas.
- 14.-16.03. CERT.LV pārstāvji piedalījās FIRST Technical Colloquium Osakā, Japānā, sniedzot divas prezentācijas: "Die Hard 104: Attacking and Controlling IEC-60870-5-104 Protocol-Based ICS/SCADA IoT Network Devices." un "Beyond paste monitoring: deep information leak analysis".
- CERT.LV pārstāvji piedalījās ENISA organizētajās mācībās „Cyber SOPEx", kas vērstas uz Eiropas CERT vienību savstarpējās sadarbības stiprināšanu. Mācībās piedalījās vairāk kā 70 speciālisti no nacionālajām kiberdrošības incidentu novēršanas institūcijām un CERT-EU.
- CERT.LV sadarbībā ar NATO CCD CoE Latvijā organizēja tehniskās kiberdrošības mācības „Crossed Swords 2018". Šogad mācību mērogs, salīdzinot ar citiem gadiem, bija daudz plašāks, tehniski sarežģītāks un izaicinošāks. Mācības aptvēra vairākus ģeogrāfiskus atrašanās punktus, iesaistot tajās gan informācijas tehnoloģiju (IT) kritiskās infrastruktūras uzturētājus, gan militārās vienības. Mācībās piedalījās vairāk kā astoņdesmit kiberdrošības ekspertu no piecpadsmit NATO CCD CoE dalībvalstīm.
- Notika aktīva gatavošanās dalībai NATO CCD CoE organizētajās kiberdrošības mācībās „Locked Shields 2018", kas notiks aprīlī. CERT.LV pārstāvji iesaistījās gan mācību organizēšanā, strādājot pie mācību scenārija attīstīšanas, tehniskās vides izveides un vadot sarkanās (uzbrucēju) komandas darbu, gan veidojot nacionālā līmeņa zilo (aizstāvošo) komandu.
- Noritēja sagatavošanās darbi dalībai ENISA rīkotajās kiberdrošības mācībās „Cyber Europe 2018", kas notiks jūnijā.

Sadarbība konkrētu incidentu risināšanā aplūkota pārskata 2. punktā.

6. Citi normatīvajos aktos noteiktie pienākumi.

- Tika uzsākts darbs pie CERT.LV un NIC.LV izstrādātā DNS RPZ (Domain Name Service Response Policy Zone) jeb DNS ugunsmūra (DNS firewall) projekta ieviešanas. Projekts sniedz iespēju aizsargāt lietotājus no ļaundabīga satura internetā, kas saistīts ar kiberdrošības institūcijām jau zināmiem incidentu identifikatoriem (domēnu vārdi, IP adreses u.c.).
- Martā uz CERT.LV vizītē ieradās valsts prezidents Raimonds Vējonis, lai pārrunātu kiberdrošības stāvokli valstī, īpašu uzmanību pievēršot faktam, ka šis ir vēlēšanu gads.

7. Papildu pasākumu veikšana.

Atskaite par Latvijas Interneta asociācijas Net-Safe Latvia Drošāka interneta centra ziņojumu līnijas darbību.

Latvijas Interneta asociācijas „Net-Safe Latvia" drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.01.2018. līdz 31.03.2018. ir saņēmusi un izvērtējusi 154 ziņojumus. No tiem 29 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 7 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 32 ziņojumos konstatēta personas goda un cieņas aizskaršana un 2 ziņojumi saņemti par naida runu. Par finanšu krāpšanas mēģinājumiem internetā saņemti 7 ziņojumi, 9 ziņojumu saturs nav bijis pretlikumīgs, 68 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 8 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 20 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kuru atrašanās vieta bija ārpus Latvijas, ir ievietoti INHOPE asociācijas datu bāzē un iesniegti attiecīgās INHOPE valsts ziņojumu līnijai turpmāko darbību veikšanai, lai dzēstu nelegālo saturu no publiskas aprites.

Sagatavotājs – Līga Besere,
tālrunis 67085888
e-pasts liga.besere@cert.lv