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 2. ceturksnis (01.04.2018. – 30.06.2018.)

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 2.ceturksnī CERT.LV apkopoja informāciju par 182 436 apdraudētām IP adresēm. Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (135 796 unikālas IP adreses) ar kritumu 3% pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs kods (33 730 unikālas IP adreses) ar kritumu 10%, bet trešais - ielaušanās mēģinājumi (1118 unikālas IP adreses) ar pieaugumu 500%.

Kāpums ielaušanās mēģinājumu apjomā skaidrojams ar ievainojamību, kura aktīvi tika izmantota globālajā tīmeklī, MikroTik maršrutētājos. MikroTik operētājsistēmai pielāgota ļaunatūra agresīvi meklēja attiecīgos maršrutētājus un iekļāva tos robotu tīklā, uzlaužot paroli ar pilnās pārlases uzbrukumu (*brute-force*).

Pārskata periodā izplatītākais apdraudējums bija krāpnieciski telefona zvani krievu valodā it kā no kādas investīciju kompānijas, kas piedāvā iesaistīties apšaubāmās finanšu operācijās. Upuri tika pārvirzīti uz *Skype*, aicināti dalīties ar savas iekārtas ekrānu, iegādāties bitcoin kriptovalūtu, ievadot maksājumu kartes datus, kā arī investēt šo iegādāto kriptovalūtu krāpnieku norādītajā finanšu platformā. Zvanītāji izcēlās ar neatlaidību un uzstājību, tika arī draudēts, ja upuris atteicās pildīt zvanītāju norādījumus.

Tika novēroti arī kampaņveidīgi mēģinājumi izkrāpt iestāžu un uzņēmumu darbinieku e-pasta piekļuves datus, izsūtot krāpnieciskas e-pasta vēstules it kā e-pasta administratora vārdā ar brīdinājumu par problēmu, kuru jāatrisina, sekojot saitei un ielogojoties. Vairāki no šiem pikšķerēšanas gadījumiem, iespējams, bijuši veiksmīgi, notiek situācijas izpēte.

Aprīlī CERT.LV piedalījās gan NATO CCD CoE kiberdrošības mācību „Locked Shields 2018" organizēšanā, gan norisē. Šogad mācību vidē tika integrētas vairāk kā 4000 virtualizētas IT sistēmas un vairāk kā 2500 dažādi uzbrukumi. CERT.LV piedalījās gan nacionālā līmeņa stratēģiskajā spēlē, gan sadarbībā ar Kiberaizsardzības vienību, US EUCOM un Kanādas bruņoto spēku pārstāvjiem, veidojot nacionālā līmeņa zilā karoga (aizstāvošo) komandu.

CERT.LV par ieguldīto darbu ieguva „Locked Shields 2018" partneru statusu un kopā ar Aizsardzības ministriju un Kiberaizsardzības vienību saņēma NATO CCDCoE pateicības rakstu par ieguldījumu mācību organizācijā un norisē.

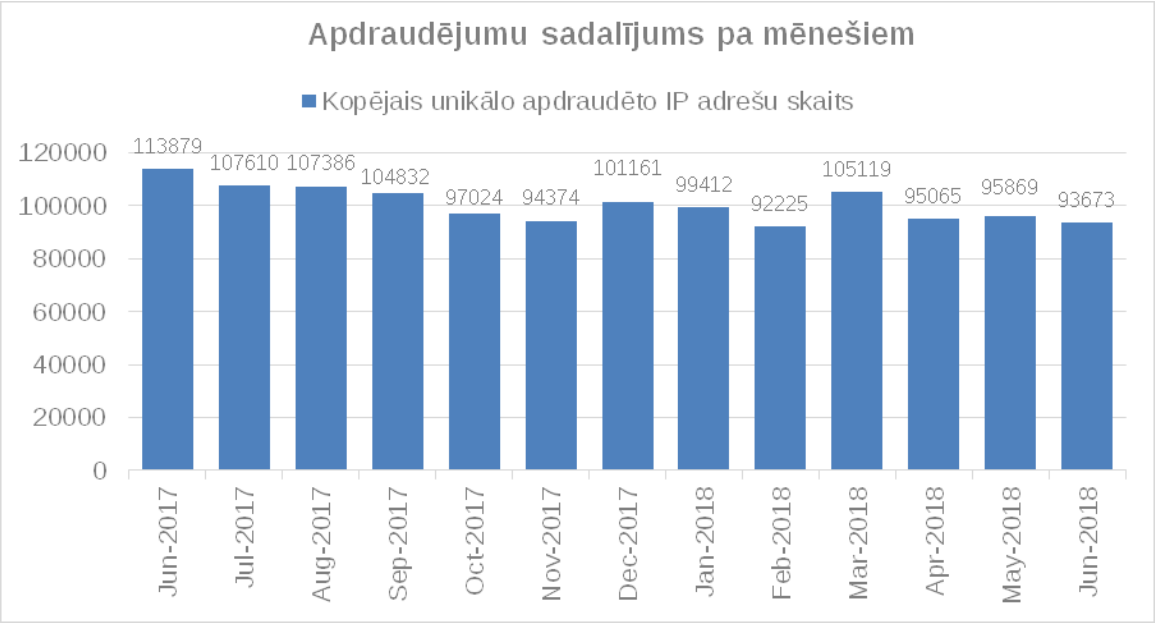
Jūnijā CERT.LV pārstāvji piedalījās ENISA rīkoto kiberdrošības mācību „Cyber Europe 2018" veidošanā, organizēšanā, vadīšanā un izpildē. Mācībās šogad iesaistījās vairāk kā 900 kiberdrošības speciālistu no 30 Eiropas Savienības (ES) dalībvalstīm, lai risinātu Eiropas līmeņa aviācijas krīzi. Tās bija līdz šim visaptverošākās ES kiberdrošības mācības. Kopējais simulēto mācībās izsūtīto scenārija vadības ziņojumu skaits sasniedza 23 222 e-pasta vēstules.

Pārskata periodā CERT.LV par IT drošību izglītoja 2331 cilvēku, iesaistoties 40 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.

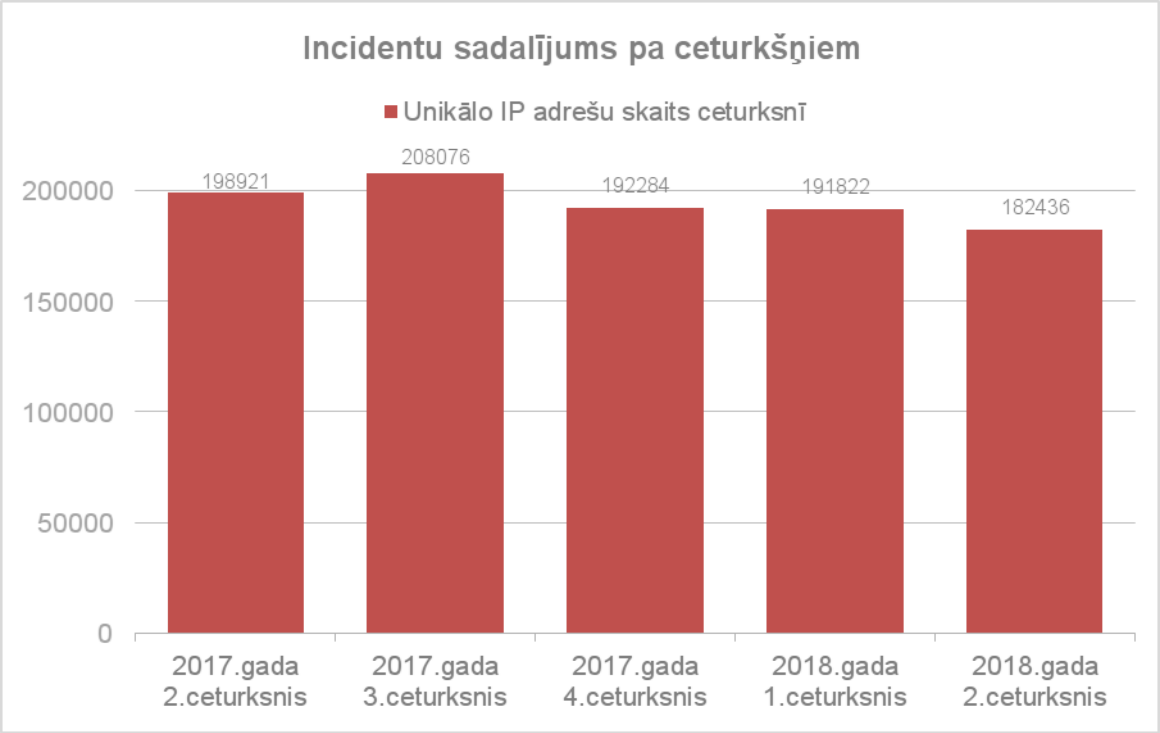
CERT.LV pārskata periodā ik mēnesi apkopoja informāciju par 90 000 – 95 000 ievainojamu unikālu IP adrešu.



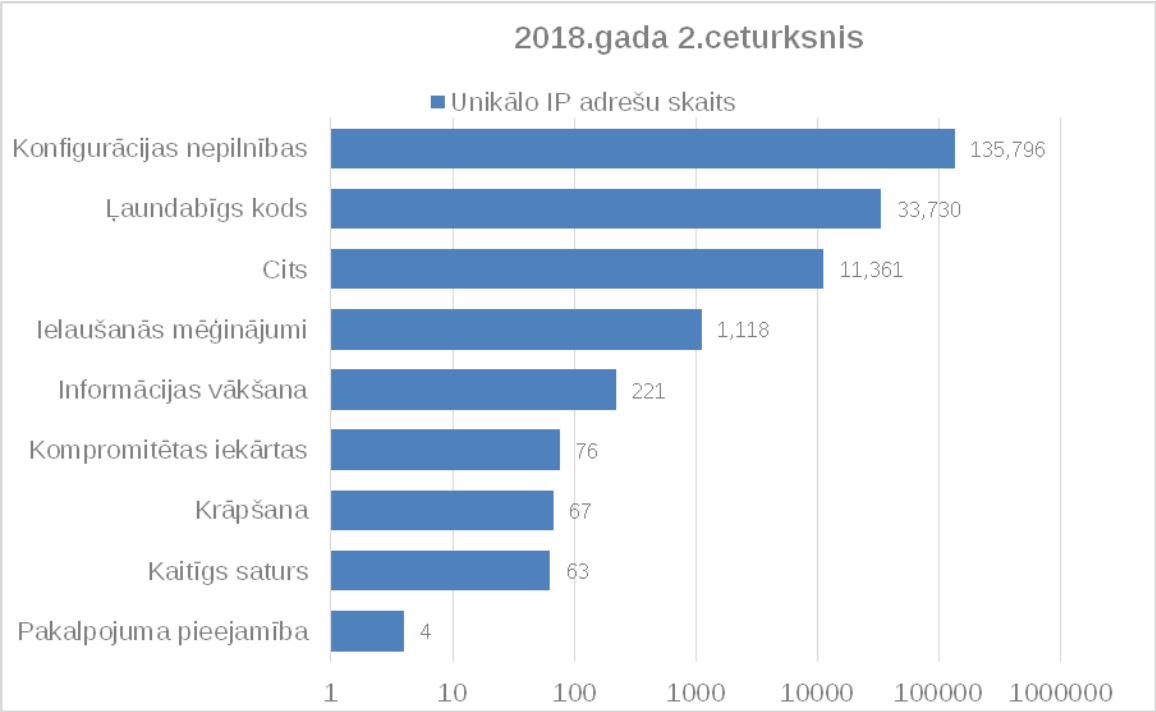
1.attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa mēnešiem 12 mēnešu griezumā.

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

2018. gada 2. ceturksnī tika reģistrētas 182 436 unikālas apdraudētas IP adreses, kas ir par nepilniem 5% mazāk nekā iepriekšējā ceturksnī un par 8% mazāk nekā šajā pašā periodā pirms gada.



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

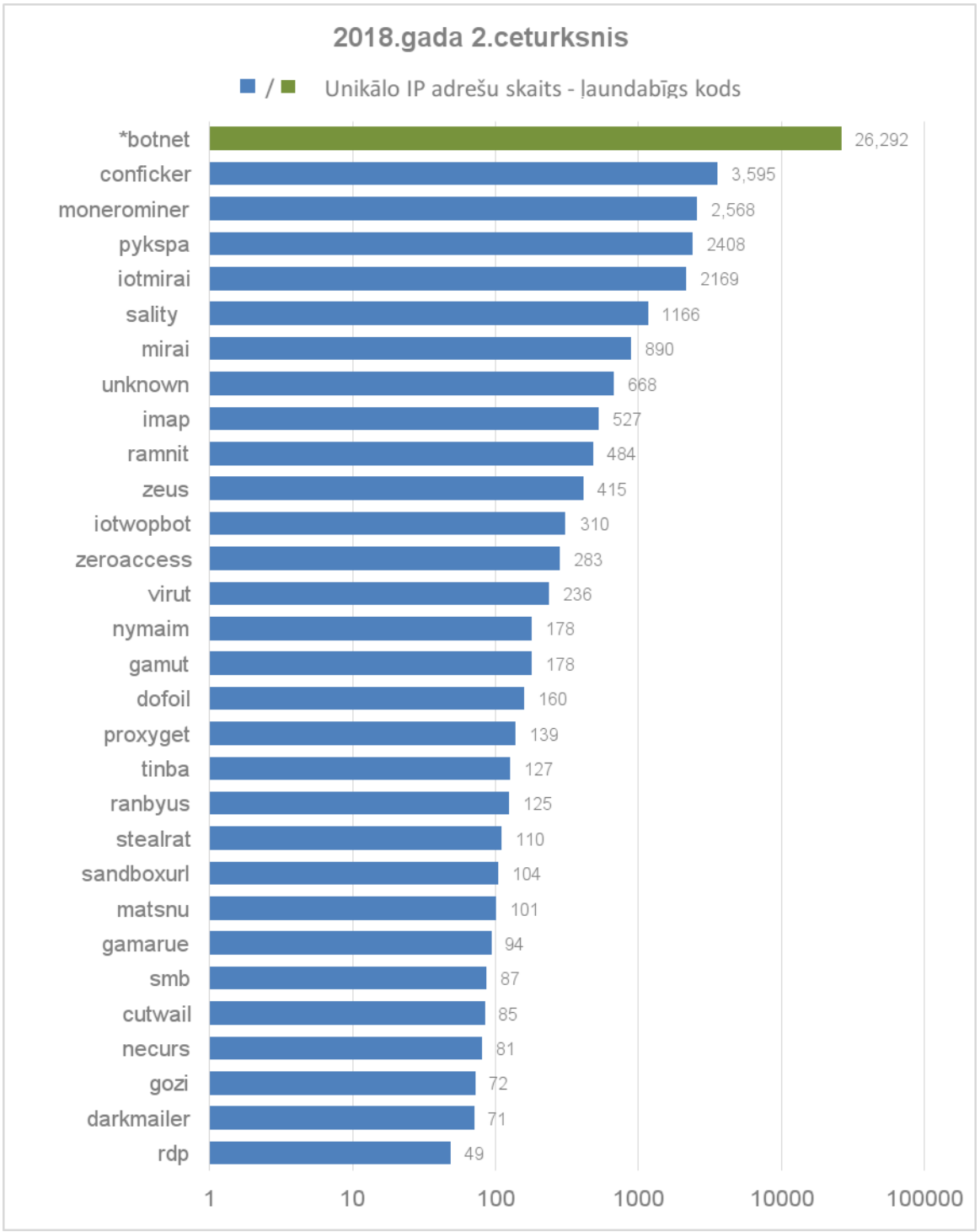


3.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2018. gada 2. ceturksnī pa apdraudējumu veidiem.

Izplatītākais apdraudējuma veids pārskata periodā nemainīgi bija konfigurācijas nepilnības (samazinājums par 5% pret iepriekšējo periodu), otrs izplatītākais bija ļaundabīgs kods (kritums par 10%), bet trešais - ielaušanās mēģinājumi (pieaugums par 500%).

Kāpums ielaušanās mēģinājumu apjomā skaidrojams ar bufera pārpildes (*buffer owerflow*) ievainojamību, kura aktīvi tika izmantota globālajā tīmeklī, MikroTik maršrutētājos. MikroTik operētājsistēmai pielāgota ļaunatūra (*Hajime*) agresīvi meklēja attiecīgos maršrutētājus un iekļāva tos robotu tīklā.

CERT.LV plāno veikt pārbaudes un apzināt ievainojamo maršrutētāju īpašniekus, aicinot salabot ievainojamās iekārtas un informējot par iekārtu konfigurācijas labo praksi.



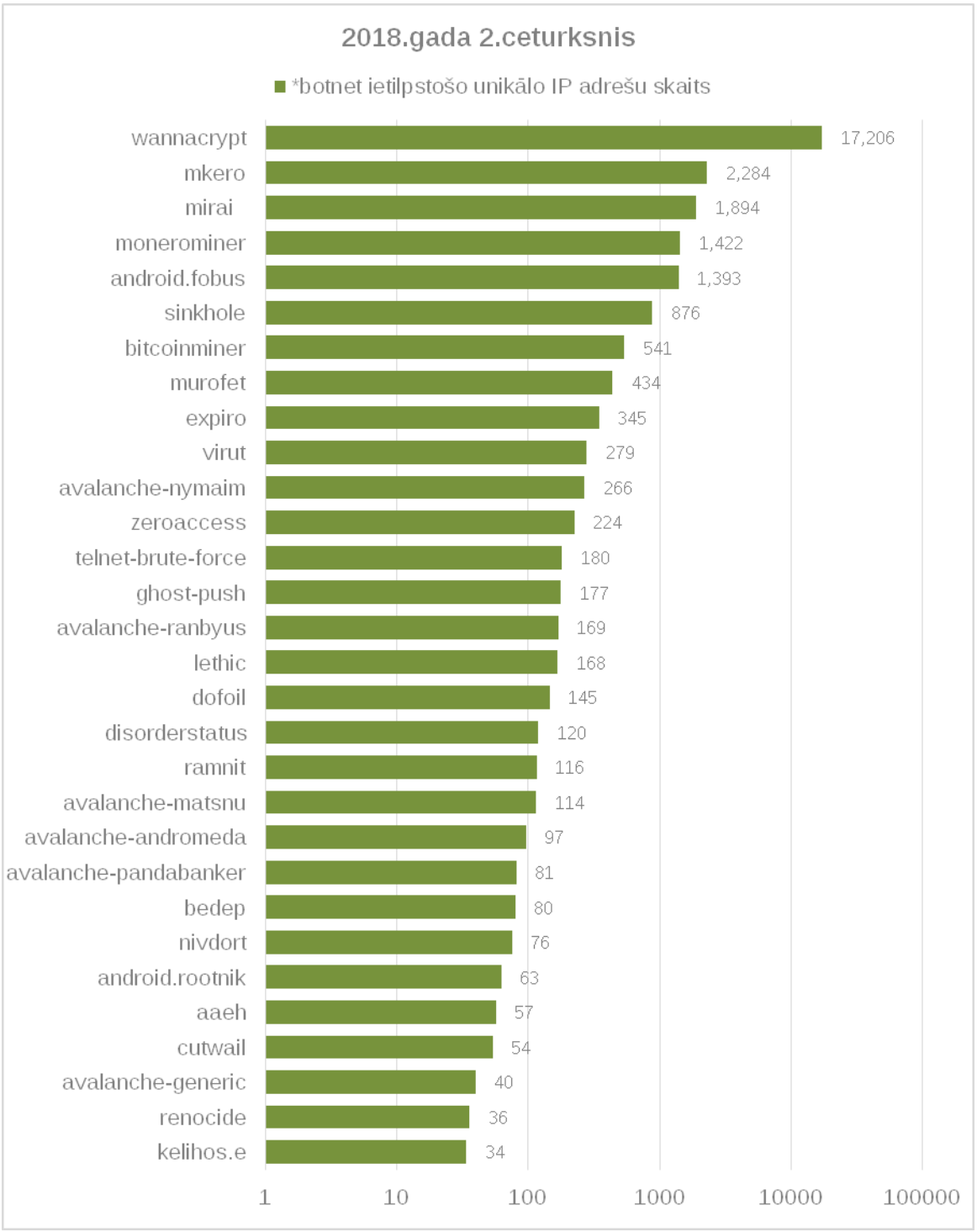
4.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2018. gada 2. ceturksnī ar apdraudējuma veidu - ļaundabīgs kods.

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

Otro vietu ļaunatūru topā atguvusi *Conficker*, kaut arī tā ir jau sen pazīstama un salīdzinoši vienkārši „ārstējama" ļaunatūra.

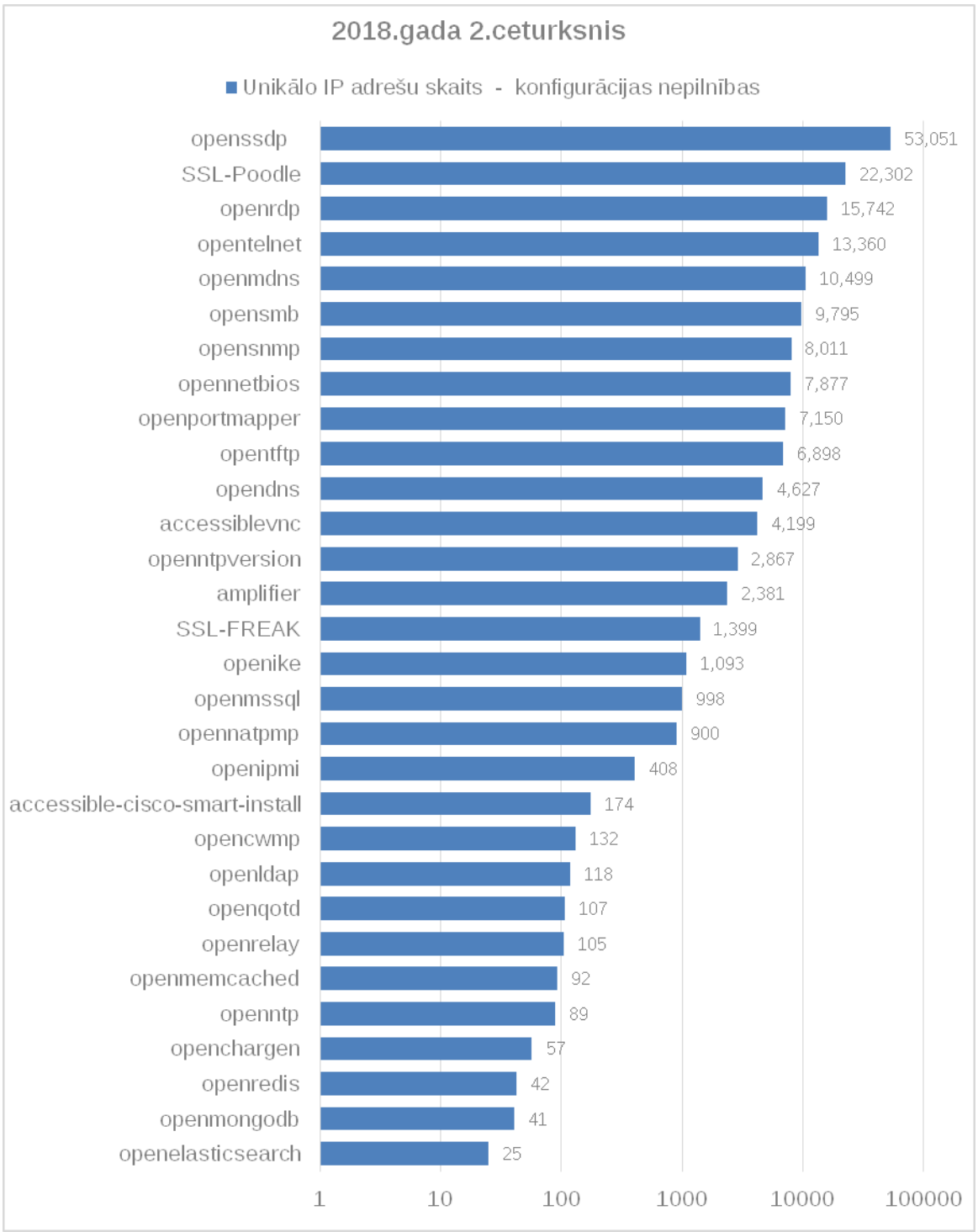
Trešo vietu ieņem – *Moneromіner*. Ļaunatūra veic kriptovalūtas *Monero* (uz privātumu orientēta kriptovalūta, kas ieguvusi popularitāti kriminālajās aprindās) ieguvi, izmantojot

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



4.1.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2018. gada 2. ceturksnī ar apdraudējuma veidu - ļaundabīgs kods.

Augsti izplatības rādītāji joprojām ir ļaunatūrai *WannaCry* (*WannaCrypt*), kas ir šifrējošais izspiedējvīruss, un, nonākot upura iekārtā, nošifrē iekārtas saturu, pieprasot samaksu par datu atgūšanu.



5.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2018. gada 2. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

Pirmo vietu konfigurācijas nepilnību topā 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.

Trešajā vietā esošā *OpenRDP* un ceturtajā vietā esošā *Opentelnet* norāda uz vairumā gadījumu neatbilstoši konfigurētām iekārtām, kurām iekārtas attālinātās piekļuves porti ir brīvi atvērti uz internetu un iekārta ir pakļauta uzbrukuma riskam.

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.

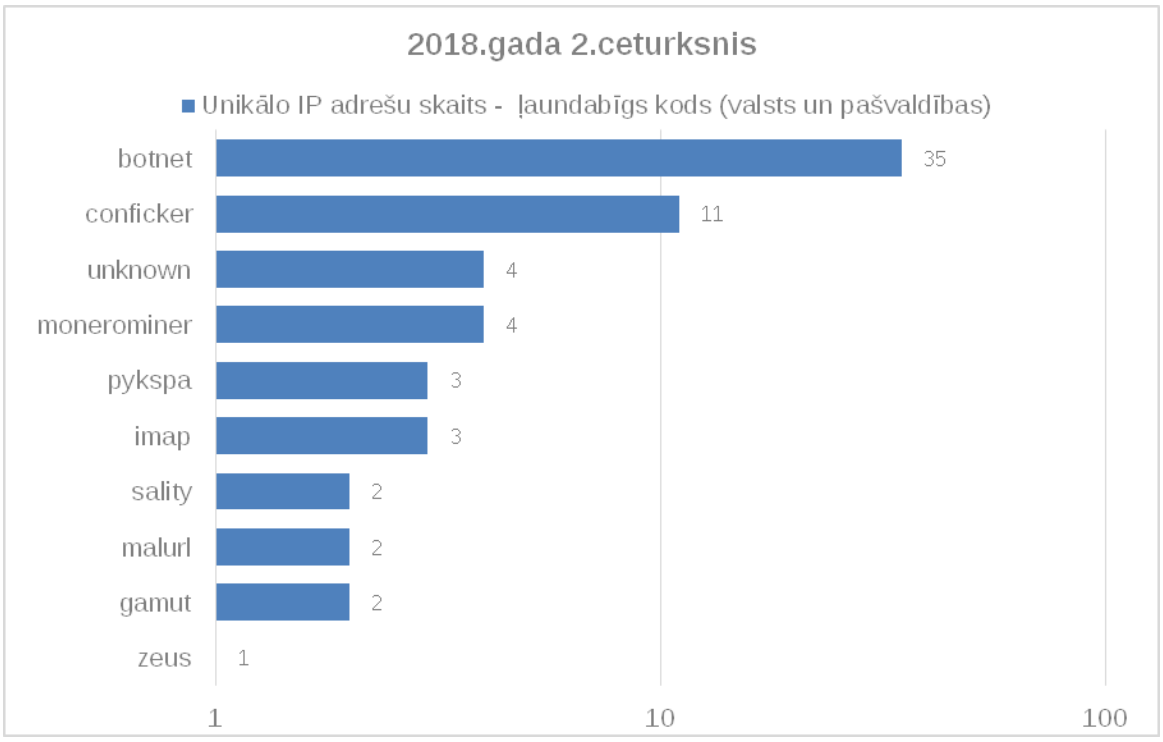
2. Atbalsts informācijas tehnoloģiju drošības incidentu novēršanā vai to novēršanas koordinēšanā.

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.

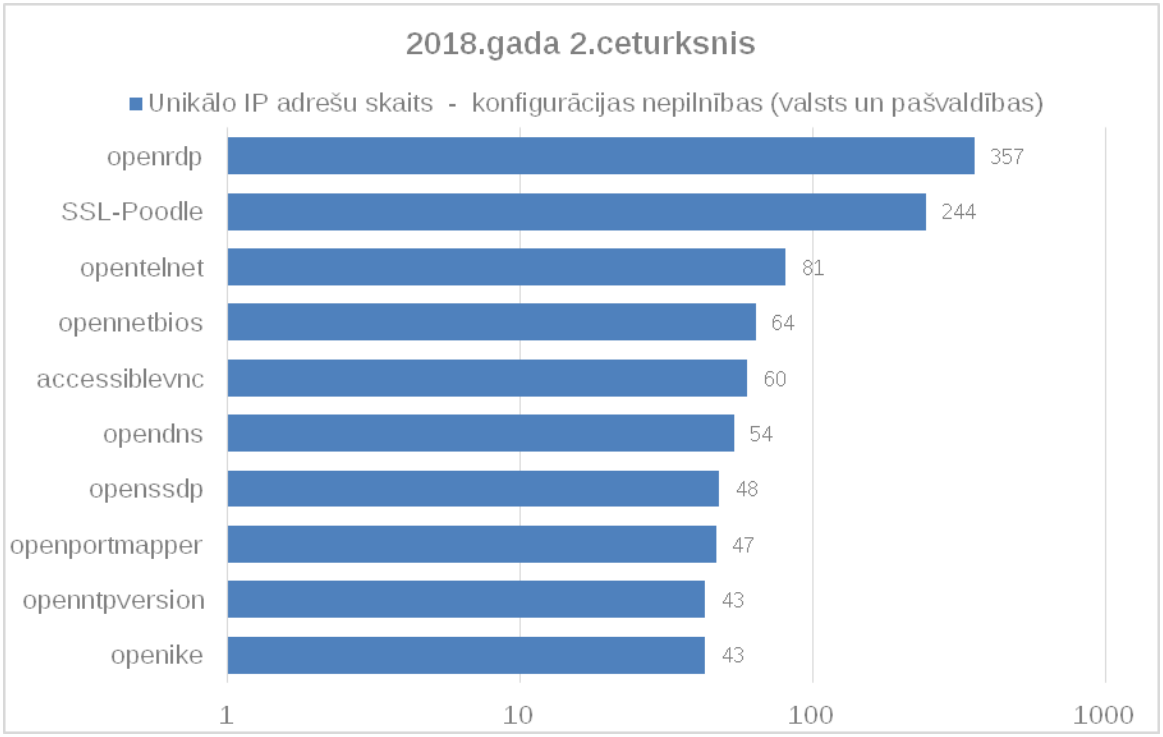
Izmaiņas katras dienas saņemtajos ziņojumos par valsts un pašvaldību iestādēm:

6.attēls – Iestāžu apdraudēto IP adrešu daudzums katras dienas saņemtajos ziņojumos 2018. gada 2. ceturksnī.

Vidējais apdraudēto valsts un pašvaldību iestāžu IP adrešu daudzums katras dienas saņemtajos ziņojumos pārskata periodā bija 550 unikālas IP adreses dienā. Salīdzinot ar iepriekšējo pārskata periodu, nav novērojamas būtiskas izmaiņas.

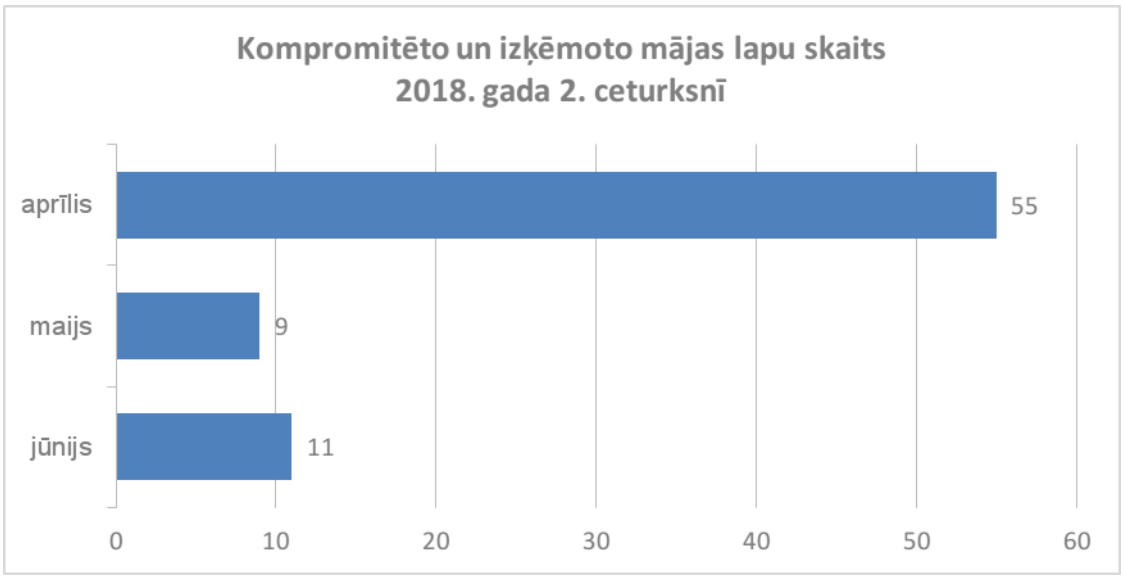


7.attēls - CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2018. gada 2. ceturksnī ar apdraudējuma veidu – ļaundabīgs kods (TOP 10 ļaundabīgs kods).



8.attēls - CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2018. gada 2. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība (TOP 10 konfigurācijas nepilnības).

CERT.LV uzskaita arī kompromitēto un izķēmoto tīmekļa vietņu gadījumus. Pārskata periodā tika fiksētas 75 kompromitētas un izķēmotas tīmekļa vietnes. Visos gadījumos izķēmotās vietnes uzturēšanai tika izmantota Linux operētājsistēma. 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 2. ceturksnī.

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

DDoS

Pārskata periodā netika fiksēti nozīmīgi piekļuves atteices (DDoS) uzbrukumi.

Pikšķerēšana

Tika saņemts ziņojums par vēstuli it kā no Francijas pasta Chronopost par sūtījuma saņemšanu ar aicinājumu sazināties, zvanot uz norādīto telefona numuru, kas, iespējams, ir paaugstinātas maksas pakalpojums. Kontaktinformācijā tika norādīta arī viltota e-pasta adrese.

Vairāku pašvaldību grāmatveži saņēma e-pastu it kā domes vadītāja vārdā ar aicinājumu veikt steidzamu maksājumu uz Vāciju. Tika atpazīta nekorekta atbildes (Reply-to) adrese. Kādas pašvaldības finansu nodaļas vadītāja saņēma aicinājumu veikt maksājumu 29 500 eiro apmērā, un sākotnēji krāpniecību nepamanīja, atbildot, ka pārskaitījums ir iespējams. Atbildes (Reply-to) adrese tika atpazīta kā krāpnieciska pēc bankas informācijas saņemšanas pārskaitījumam. Līdzīgu e-pastu saņēma arī kāda uzņēmuma grāmatvedis. CERT.LV ieteica uzņēmumam izveidot SPF un DKIM pārbaudes ienākošajiem e-pastiem, tas atfiltrētu šādus krāpnieciskus e-pastus kā SPAMu.

Virkne valsts iestāžu darbinieku saņēmuši e-pastu it kā e-pasta administratora vārdā ar aicinājumu atjaunot kontu, sekojot e-pastā norādītajai saitei. E-pastu mērķis bija izkrāpt e-pastu piekļuves informāciju. Uzsākta pārbaude par dažiem, iespējams, sekmīgiem uzbrukumiem.

Krāpnieciskas vēstules tika sūtītas arī PayPal, Microsoft Outlook un Office 365 vārdā, informējot par neatļautām darbībām no konta, kas jāpārtrauc, vai par pakalpojuma funkcionalitātes samazināšanu vai apturēšanu, ja netiks veikta atkārtota autorizācija, sekojot e-pastā norādītajai saitei. Dažos gadījumos tika norādīts 48 stundu limits.

Tika saņemti ziņojumi arī no kādas pašvaldības un vairākiem uzņēmumiem par e-pasta piekļuves pikšķerēšanas vēstulēm e-pasta administratora vārdā, kurās tiek draudēts ar e-pasta konta slēgšanu, jo nav „atjaunināta konta drošība" vai nav veikta pāreja uz jauno e-pasta versiju, gan izteikts brīdinājums par kvotas pārsniegšanu vai konta deaktivāciju. Visos gadījumos problēmas novēršanai izteikts aicinājums sekot e-pastā norādītajai saitei un autorizēties. Atsevišķos gadījumos tika norādīts 48 stundu laika limits. Neviens no šiem pikšķerēšanas gadījumiem nav bijis veiksmīgs.

Saņemti vairāki e-pasta piekļuves datu izkrāpšanas mēģinājumi, sūtot e-pastus transporta kompāniju (DHL, Maersk) vārdā un aicinot aplūkot pielikumā esošo dokumentu un apstiprināt piegādes adresi vai saņemt sūtījuma izsekošanas numuru.

Tika saņemta informācija par vairākām uzlauztām .lv interneta vietnēm un Latvijas IP adresēm, kurās tika izvietota pikšķerēšana, kas vērsta uz ārvalstu banku, Apple, Microsoft un Netflix klientiem.

Tika reģistrēta krāpnieciska vietne Facebook datu izkrāpšanai, kuru krāpnieks reklamēja arī savā Facebook profilā kā Facebook statistikas vietni. Krāpnieciskās vietnes uzturētāji brīdināti, vietne aizvērta.

Pārskata periodā bija izplatīta arī personas datu pikšķerēšana, upurim nosūtot paziņojumu par laimestu loterijā, kurš ir ieskaitīts bankas maksājumu kartē. Lai ar kurjerpastu saņemtu laimestu saturošo bankas maksājumu karti, jāsazinās ar loterijas pārstāvi un jāsniedz savi personas dati. Upuri tiek arī aicināti sūtīt savus personas datus, lai kļūtu par mantinieku bez īpašnieka palikušam bankas kontam.

Krāpšana

Tika saņemts ziņojums par aizdomīgu interneta veikalu salomonshoes.online, kurš izveidots neilgu laiku atpakaļ, izmantojot identitātes slēpšanas starpnieka pakalpojumu, un piedāvā visu preci ar 80% lielu atlaidi. Lietotājam tika ieteikts konkrētās vietnes pakalpojumus neizmatot, jo pastāv augsts krāpšanas risks.

Saņemts ziņojums par krāpšanas mēģinājumu, nosūtot vairākus e-pastus it kā PayPal vārdā un pieprasot veikt samaksu, izmantojot Western Union, lai norēķinātos par neapmaksātajiem transporta pakalpojumiem, pretējā gadījumā draudot ar konta slēgšanu un arestu.

Saņemti vairāki ziņojumi par aizdomīgiem zvaniem krievu valodā it kā no kādas investīciju kompānijas, kas piedāvā iesaistīties apšaubāmās finanšu operācijās, solot pasakainu peļņu. Sākotnējā telefonsaruna tiek pārvirzīta uz *Skype* un zvanītāji aicina upuri dalīties ar savas iekārtas ekrānu, kam seko aicinājums iegādāties bitcoin kriptovalūtu, ievadot maksājumu kartes datus, un investēt šo iegādāto kriptovalūtu krāpnieku norādītajā finanšu platformā. Zvanītāji izcēlās ar neatlaidību un uzstājību, tika pielietoti arī draudi, ja upuris atteicās pildīt zvanītāju norādījumus.

Ielaušanās un mēģinājumi

Marta beigās, aprīļa sākumā un jūnija otrajā pusē notika mēģinājumi pieslēgties un izsūtīt e-pastus no kādas Latvijas iestādes domēna, izmantojot gan eksistējošas lietotāju e-pasta adreses, gan ģenerētas. Uzbrukums bija neveiksmīgs, e-pasta vēstules līdz lietotājiem nenonāca.

Tika saņemti vairāki ziņojumi par Latvijas IP adresēm, kas veikušas uzbrukumus Sony Interactive Entertainment tīkam, cenšoties iegūt kontroli pār lietotāju kontiem, un, visticamāk, saistītas ar kompromitētām iekārtām.

Ļaunatūra

Saņemts ziņojums par vairāku ļaunatūru - *JBifrost botnet, Necurs, Pony botnet, NanoCore, Loki botnet* un *Remcos RAT* – komand- un kontroles centriem (C&C) Latvijas IP adresēs. *JBifrost* ir ļaunatūra, kas uzbrucējam sniedz attālinātu piekļuvi upura iekārtai. *Necurs* zombiju tīkls jeb *botnet* izplata dažāda veida ļaunatūru, no kurām zināmākā ir *Locky* šifrējošais vīriss. *Pony* ir ļaunatūra, kas specializējas personīgo datu zādzībā, taču spēj veikt arī kriptovalūtas, piem., bitcoin zādzību. *NanoCore* trojānis ļauj uzbrucējam attālināti kontrolēt upura iekārtu un ievākt informāciju par, piemēram, ievadītajām parolēm. *Loki* ļaunatūra paredzēta paroļu un citas sensitīvas informācijas zādzībai. *Remcos* – attālinātas kontroles rīks. Visos gadījumos apzināti iekārtu, kurās izvietoti C&C, uzturētāji, iekārtas salabotas un apdraudējums novērsts.

Kādas pašvaldības darbinieki saņēma it kā kolēģu e-pastus ar saiti uz tīmekļa vietni, kas saturēja ļaunatūru. E-pasta teksta vulgārais tonis ļāva atpazīt kaitniecību.

Tika saņemti vairāki ziņojumi par it kā biznesa e-pastiem ar piedāvāto produktu sarakstu pielikumā. Parakstā minēta reāla kompānija Arābu Emirātos un kontaktinformācija. Pielikumā atradās .iso fails, kas saturēja šifrējošo vīrusu (citā gadījumā trojāni).

DHL zīmols tika izmantots arī ļaunatūras izplatīšanai, izsūtot paziņojumus it kā DHL vārdā par nepiegādātu sūtījumu, jo trūkst saņēmēja adreses. E-pastā izteikts aicinājums atvērt un aizpildīt pielikumu, norādot saņēmēja adresi. Pielikumā kaitīgs .JAR fails. Saņēmējs pielikumu neatvēra.

Tika saņemts ziņojums par ļaunatūras, kas izmanto Microsoft ievainojamību attālinātai koda izpildei upura iekārtā, komand- un kontrolcentru Latvijas IP adresē. Uzturētāji tika informēti, apdraudējums tika novērsts un iekārta salabota.

Tika saņemts ziņojums par *CoinHive* kriptovalūtas ieguves ļaunatūru kādas iestādes tīmekļa vietnē. Vietnes uzturētāji informēti.

Saņemts ziņojums par šifrējošo izspiedējvīrusu kādas pašvaldības serverī. Serveris nesaturēja būtisku informāciju. Žurnālfaili nodoti CERT.LV analīzei.

Mobilā ļaunatūra

Pārskata periodā netika fiksēti nozīmīgi incidenti, kas skar mobilās iekārtas.

Atbildīga ievainojamību atklāšana

Atbildīgas ievainojamību atklāšanas ietvaros tika saņemti divi ziņojumi par starpvietņu skriptēšanas (XSS) ievainojamību valsts iestāžu tīmekļa vietnēs. Ievainojamības ļāva uzbrucējam izpildīt sev vēlamus skriptus upura pārlūkprogrammā, izmantojot īpaši sagatavotu saiti. Vietnes uzturētāji tika informēti, problēma tika novērsta.
Abos gadījumos ievainojamību atklājējiem nosūtīts pateicības raksts.

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.

Pārskata periodā CERT.LV tikās ar kustības „Atkrāpies" pārstāvjiem, lai pārrunātu iespējamo sadarbību, veicinot iedzīvotāju izpratni par to, kā atšķirt negodprātīgu tirgotāju internetā un atpazīt krāpniecisku tīmekļa vietni.

Pārskata perioda beigās notika sadarbības tikšanās ar projekta Samsung Skola nākotnei pārstāvjiem, lai vienotos par kopīgu materiālu izstrādi jauniešu digitālo zināšanu un prasmju uzlabošanai, ņemot vērā dažādus digitālās drošības aspektus.

Sadarbībā ar Aizsardzības ministriju tapa video sižets Re:TV bērnu raidījumam „Mēs ar brāli kolosāli" par drošu komunikāciju internetā.

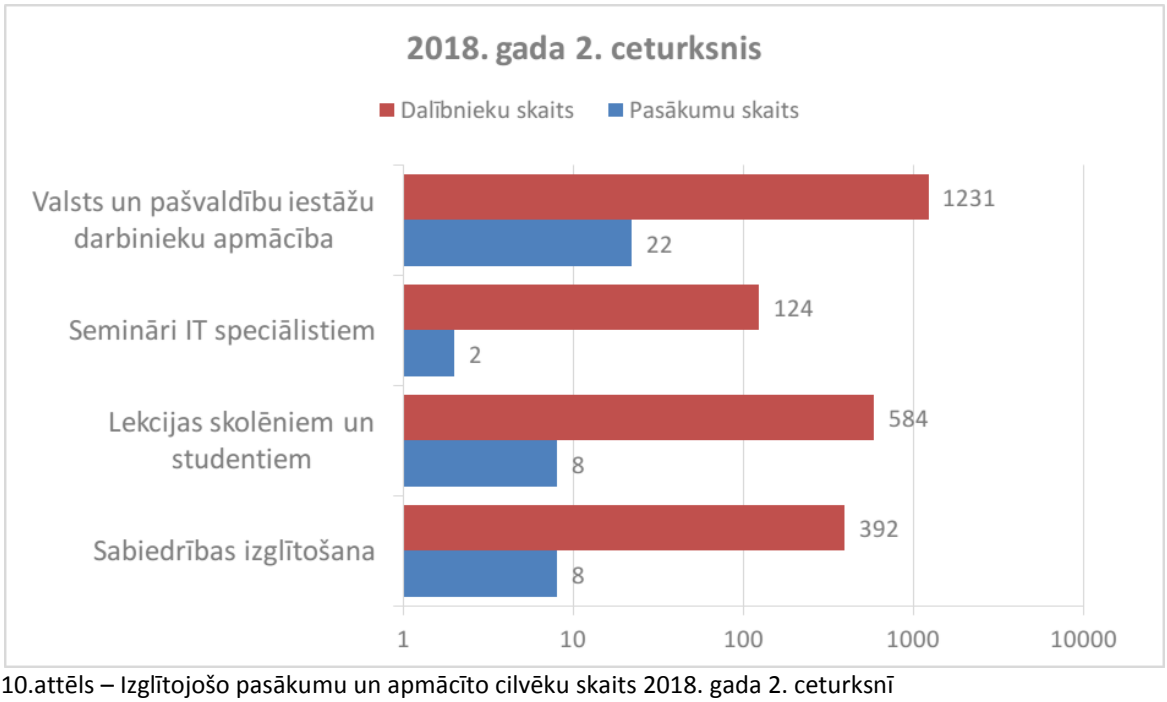
5. aprīlī CERT.LV pārstāvis piedalījās paneļdiskusijā „Development of Global Supply Chains and Ensuring Adequate Risk Management of Disruptions", kas norisinājās konferences „Global Transport Security and Safety for a Century" ietvaros.

19. aprīlī CERT.LV pārstāvis vadīja paneļdiskusiju „Domains and cybercrime:is there a light at the end of the tunnel?" Baltijas valstu domēnu nozarei veltītajā pasākumā „Baltic Domain Days".

25. aprīlī CERT.LV pārstāvis piedalījās paneļdiskusijā „Tiesiskums kibertelpā", kas notika konferences „Tiesiskās problēmas Latvijas simtgadē: retrospektīva un perspektīva" ietvaros.

1.jūnijā Accenture sadarbībā ar CERT.LV organizēja NightHack 2018, kuram pieteicās 40 IT drošības eksperti, bet par galveno balvu nakts garumā sacentās 25 speciālisti, pierādot savas zināšanas, prasmes un atjautību.

Pārskata periodā CERT.LV par IT drošību izglītoja 2331 cilvēku, iesaistoties 40 izglītojošos pasākumos.



10.attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2018. gada 2. ceturksnī

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

Sadarbības tikšanās, konsultācijas un prezentācijas:

- CERT.LV piedalījās sanāksmē ar Aizsardzības ministrijas (AiM) pārstāvjiem par Eiropas Parlamenta un Padomes 2016.gada 6.jūlija direktīvas (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (turpmāk – NIS direktīvu) ieviešanas atsevišķiem aspektiem. Sanāksmes laikā CERT.LV un AiM pārstāvji vienojās par to, kādus drošības incidenta, kam ir būtiska ietekme uz pamatpakalpojuma nepārtrauktību, kritērijus iesniegt apspriešanai nozaru ministrijām – Ekonomikas ministrijai, Finanšu ministrijai, Satiksmes ministrijai, Veselības ministrijai, Vides aizsardzības un reģionālās attīstības ministrijai un Zemkopības ministrijai.

  Sanāksmē starp AiM, CERT.LV un nozaru ministrijām un iestādēm CERT.LV uzklausīja priekšlikumus un apsprieda ar nozares pārstāvjiem minētos kritērijus. Tika identificēta nepieciešamība precizēt kritēriju robežvērtības. Kā arī pēc sanāksmes AiM tika nosūtīts priekšlikums atbildei uz Egona Spalāna (Ventspils pašvaldības pārstāvis) 29.05. elektroniski iesniegtajiem iebildumiem..

- CERT.LV un AiM pārstāvji tikās ar Finanšu un kapitāla tirgus komisijas (FKTK) pārstāvjiem, lai apspriestu kritērijus, kādi būtu jānosaka ziņošanai CERT.LV par drošības incidentiem, kam ir būtiska ietekme uz pamatpakalpojuma nepārtrauktību. FKTK norādīja, ka kredītiestāžu, finanšu tirgus infrastruktūras jomā izstrādāti "Normatīvie ieteikumi par ziņošanu par maksājumu pakalpojumu sniedzēju būtiskiem incidentiem", kur noteikti kritēriji, kad par incidentu ir jāziņo FKTK, tāpēc būtu jāizvērtē vēl citu papildu kritēriju lietderīgums. FKTK kritēriji daļēji pārklājas ar CERT.LV un AiM izstrādāto priekšlikumu, tāpēc tika skaidrots, ka, NIS direktīvu ieviešot, mērķis ir harmonizēt ziņošanu par būtiskiem informācijas tehnoloģiju drošības incidentiem un ziņošana tikai FKTK nav iespējama.

- Tieslietu ministrijas starpinstitūciju darba grupas sanāksmē par Eiropas Parlamenta un Padomes regulu par Eiropas izsniegšanas un saglabāšanas rīkojumu elektroniskajiem pierādījumiem krimināllietās CERT.LV pārstāvji pauda atbalstu tam, ka tiesībsargājošajām iestādēm tiek piedāvāts vēl viens instruments ātrākai elektronisko pierādījumu iegūšanai, un norādīja, ka CERT.LV šī regula tieši neskars, jo regula attiecināma uz kriminālprocesu veicošām tiesībsargājošām iestādēm.

- Aizsardzības, iekšlietu un korupcijas novēršanas komisijas (12.Saeima) sēdē pirms likuma grozījumu izskatīšanas 1.lasījumā CERT.LV pārstāvji atbildēja uz deputātu jautājumiem par to kā plānotie Grozījumi Informācijas tehnoloģiju drošības likumā (Nr. 1263/Lp12) ietekmēs CERT.LV darbību, kādas praktiskas izmaiņas tiks ieviestas. Grozījumu mērķis ir ieviest NIS direktīvas prasības nacionālā līmenī.

- CERT.LV un AiM pārstāvji kopā ar Saeimas Juridisko biroju precizēja Grozījumus Informācijas tehnoloģiju drošības likumā (Nr. 1263/Lp12), kas ievieš NIS direktīvu. Vairāku sanāksmju laikā tika identificēta nepieciešamība redakcionāli precizēt 3^1 pantu, 5^1 pantu, 6.pantu, 8.pantu. CERT.LV pārstāvji apkopoja tikšanās laikā identificētās problēmas un risinājumus un tos nosūtīja AiM.

- CERT.LV pārstāvis piedalījās Virtuālo valūtu darba grupas sanāksmē, kas ir ekspertu darba grupa rekomendāciju izstrādei Eiropas Parlamenta un Padomes Direktīvas 2009/101/EK (AML 5 direktīva) ieviešanai nacionālajā regulējumā, iekļaujot virtuālo valūtu regulējumu normatīvajos aktos.

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:

- CERT.LV pārstāvis piedalījās Moldovas kiberdrošības centra akreditācijas procesā, kas nodrošināja centra iekļaušanu FIRST (Forum of Incident Response and Security Teams) dalīborganizācijās.
- CERT.LV pārstāvji tikās ar Austrijas kolēģiem, lai dalītos pieredzē par sensoru tīkla izveidi.
- 23.-27. aprīlī notika NATO CCD CoE organizētās kiberdrošības mācības „Locked Shields 2018", kurās CERT.LV iesaistījās gan mācību organizēšanā, strādājot pie mācību scenārija attīstīšanas, tehniskās vides izveides un vadot sarkanā karoga (uzbrucēju) komandas darbu, gan piedalījās mācību norisē. Šogad mācību vidē tika integrētas vairāk kā 4000 virtualizētas IT sistēmas un vairāk kā 2500 dažādi uzbrukumi. Mācībās tika izmantotas reālistiskas tehnoloģijas, tīkli un uzbrukumu metodes.

  CERT.LV gan sadarbībā ar Kiberaizsardzības vienību, US EUCOM un Kanādas bruņoto spēku pārstāvjiem veidojot nacionālā līmeņa zilā karoga (aizstāvošo) komandu, gan piedalījās nacionālā līmeņa stratēģiskajā spēlē, risinot sarežģītus juridiskus un politiskus jautājumus un komunicējot tos ar medijiem.

  CERT.LV par ieguldīto darbu ieguva „Locked Shields 2018" partneru statusu un kopā ar Aizsardzības ministriju un Kiberaizsardzības vienību saņēma NATO CCDCoE pateicības rakstu par ieguldījumu mācību organizācijā un norisē.
- CERT.LV pārstāvis piedalījās „Locked Shields 2018 After Actions Report" sanāksmē un mācību „Crossed Swords 2019" sākotnējās plānošanas konferencē Tallinā.
- CERT.LV pārstāvis par augstiem sasniegumiem un būtisku ieguldījumu centra un alianses kiberdrošības stiprināšanā un prestiža celšanā saņēma NATO CCDCoE vēstnieka titulu. Šāds statuss tiek piešķirts uz diviem gadiem, un vēstnieku skaits ir ļoti ierobežots, - tas nepārsniedz septiņus vēstniekus.
- 16. aprīlī CERT.LV pārstāvis NATO CCDCoE pasniedza „Cyber Executive Seminar" Tallinā, Igaunijā.
- 16.-24. aprīlī Sanfrancisko norisinājās RSA konference, kurā CERT.LV pārstāvis kopā ar pētnieku Dr. Kenneth Geers sniedza prezentāciju „Cyberwar on a Shoestring: How Kim Jong Un Stole My Malware".
- 24. aprīlī notika sadarbības tikšanās ar NCSC-UK pārstāvi, lai apspriestu Latvijas un Apvienotās Karalistes sadarbību kiberdrošības jomā.
- CERT.LV pārstāvji aktīvi piedalījās NIS direktīvas CERTu tīkla darbībā, jūnijā apmeklējot sanāksmi Atēnās, kā arī darbojoties divās darba grupās - vienā, kas papildināja un uzlaboja CERTu tīkla „Terms of Reference" dokumentu un otrā, kas veido Eiropas „Cyber Weather".
- 23.-25. maijā Varšavā notika „54th TF-CSIRT meeting", kurā CERT.LV pārstāvis sniedza prezentāciju „Technical Incident Analysis".
- 27.-30. maijā CERT-EE simpozijā Tallinā CERT.LV pārstāvis sniedza prezentāciju „Responsible disclosure and ICS/SCADA security".

- 30.maijs - 02.jūnijs NATO CCDCoE konferencē „CyCon" Tallinā CERT.LV pārstāvis un pētnieks Dr. Kenneth Geers sniedza prezentāciju „Aladdin's Lamp: The Theft and Re-weaponization of Malicious Code".
- 24.-29. jūnijā Kualalumpurā, Malaizijā FIRST konferencē „30th Annual FIRST conference" CERT.LV pārstāvis sniedza prezentāciju „Malware Reweaponization - A Case Study".
- 26. jūnijā CERT.LV pārstāvis Štutgartē, Vācijā, sniedza prezentāciju US EUCOM par „Responsible disclosure and ICS/SCADA security".
- CERT.LV eksperti atklāja četras kritiskas industriālo vadības sistēmu ICS/SCADAs ievainojamības (CVE-2018-10603, CVE-2018-10607, CVE-2018-10609, CVE-2018-XXXXX) un vairāku mēnešu garumā koordinēja un sniedza atbalstu ievainojamo iekārtu izstrādātājam šo ievainojamību novēršanā. Vienas ievainojamības novēršana arvien vēl ir procesā tās tehniskās sarežģītības dēļ.
- 04.-09. jūnijā CERT.LV pārstāvji piedalījās ENISA rīkoto kiberdrošības mācību „Cyber Europe 2018" veidošanā, organizēšanā, vadīšanā un izpildē. Mācībās šogad iesaistījās vairāk kā 900 kiberdrošības speciālistu no 30 Eiropas Savienības dalībvalstīm, lai risinātu Eiropas līmeņa aviācijas krīzi. Intensīvā divu dienu mācību scenārijā, kas veidoja līdz šim visaptverošākās Eiropas Savienības kiberdrošības mācības, inscenētie notikumi risinājās simulētā mācību vidē, kurā mācību dalībniekiem nācās spēt identificēt un novērst liela mēroga apdraudējumus, reaģēt uz tiem, kā arī labāk izprast incidentu pārrobežu ietekmi. Kopējais simulēto mācībās izsūtīto scenārija vadības ziņojumu skaits sasniedza 23 222 e-pasta vēstules.

Sadarbība konkrētu incidentu risināšanā aplūkota pārskata 2. punktā.

6. Citi normatīvajos aktos noteiktie pienākumi.

- CERT.LV pārstāvji tikās ar Valsts policijas pārstāvi, kas maģistra darba ietvaros plāno izstrādāt kiberdrošības terminu latviešu valodas glosāriju. Notika informācijas apmaiņa par līdz šim izmantotajiem terminiem un ar kiberdrošību saistītu tekstu tulkošanu.
- CERT.LV pārstāvis piedalījās Drošāka interneta centra konsultatīvās padomes sēdē un informācijas apmaiņā par plānotajām aktivitātēm un izstrādātajiem materiāliem jauniešu izglītošanai par kiberdrošību.
- Tika turpināts 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.). Veikta divu pilotprojektu ieviešana un uzsāktas vairākas sarunas ar potenciālajiem interesentiem.
- Saskaņā ar MK 2015. gada 3. februāra sēdes protokolā Nr. 6 27. §, ar kuru pieņemts zināšanai informatīvais ziņojums "Par kompetento un atbildīgo iestādi, kura nodrošinās kvalificētu un kvalificētu paaugstinātas drošības elektroniskās identifikācijas pakalpojumu sniedzēju uzraudzību", noteikto CERT.LV pārskata periodā piedalījās Eiropas savienības dalībvalstu eID shēmu priekšpaziņošanas procesā - Peer Review.

- CERT.LV vadītāja un vadītājas vietnieks svinīgā ceremonijā Aizsardzības ministrijā saņēma pateicības rakstus no aizsardzības ministra Raimonda Bergmaņa par veiksmīgu sadarbību, atbalstu un ieguldījumu kiberdrošības stiprināšanā.

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 01.04.2018. līdz 30.06.2018. ir saņēmusi un izvērtējusi 130 ziņojumus. No tiem 47 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 14 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 18 ziņojumos konstatēta personas goda un cieņas aizskaršana un 3 ziņojumi saņemti par naida runu. Par finanšu krāpšanas mēģinājumiem internetā saņemti 5 ziņojumi, 11 ziņojumu saturs nav bijis pretlikumīgs, 32 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 17 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 27 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