Latvijas Universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

Līdzfinansē Eiropas Savienības Eiropas
infrastruktūras savienošanas instruments

Publiskais pārskats par CERT.LV uzdevumu izpildi

2018

2018. gada 4. ceturksnis (01.10.2018. – 31.12.2018.)

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 4.ceturksnī CERT.LV apkopoja informāciju par 203 455 apdraudētām IP adresēm. Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (131 394 unikālas IP adreses) ar kritumu 8% pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs kods (23 993 unikālas IP adreses) ar kritumu 22%, bet trešais - ielaušanās mēģinājumi (2469 unikālas IP adreses) ar kritumu 4%.

Lielāko pieaugumu pārskata periodā piedzīvoja informācijas vākšanas mēģinājumi jeb mērķtiecīga noteiktu servisu ievainojamību meklēšana (pieaugums par 184%) un kompromitētu iekārtu apjoms (pieaugums par 168%). Ievainojamību meklēšanas apjoma pieaugums skaidrojams ar kompromitētu lietu interneta (IoT) iekārtu skaita palielināšanos, kas iekļautas botnetos un meklē citas ievainojamas iekārtas.

Pārskata periodā notika aktīvs darbs Saeimas vēlēšanu darba grupā, veicot vēlēšanu infrastruktūras stiprināšanu pirmsvēlēšanu periodā, un nodrošinot infrastruktūras uzraudzību vēlēšanu gaitā. Vēlēšanu dienā tika saņemts ziņojums par portāla Draugiem.lv kompromitēšanu un izķēmošanu, kuras rezultātā portāls lietotājiem uz laiku bija nepieejams, bet fonā bija redzami ar Krievijas Federāciju saistīti attēli un skanēja Krievijas himna.

No lietotājiem pārskata periodā aktīvi tika saņemti ziņojumi par krāpnieciskiem e-pastiem, kuros uzbrucējs paziņo, ka ir uzlauzis upura datoru, uzfilmējis kompromitējošu video un draud izsūtīt šo video visiem upura kontaktiem, ja netiks samaksāta izpirkuma maksa. Kā pierādījumu uzbrucējs norāda, ka zina upura paroli. CERT.LV norādīja, ka šīs paroles iegūtas internetā publicētās datu noplūdēs.

Devītajā oktobrī Eiropas Kiberdrošības mēneša ietvaros ar projekta "Improving Cyber Security Capacities in Latvia" atbalstu CERT.LV sadarbībā ar ISACA Latvijas nodaļu organizēja kiberdrošībai veltīto konferenci „Kiberšahs 2018", kuru klātienē apmeklēja 500 dalībnieki, bet attālināti vēroja vairāk kā 2000.

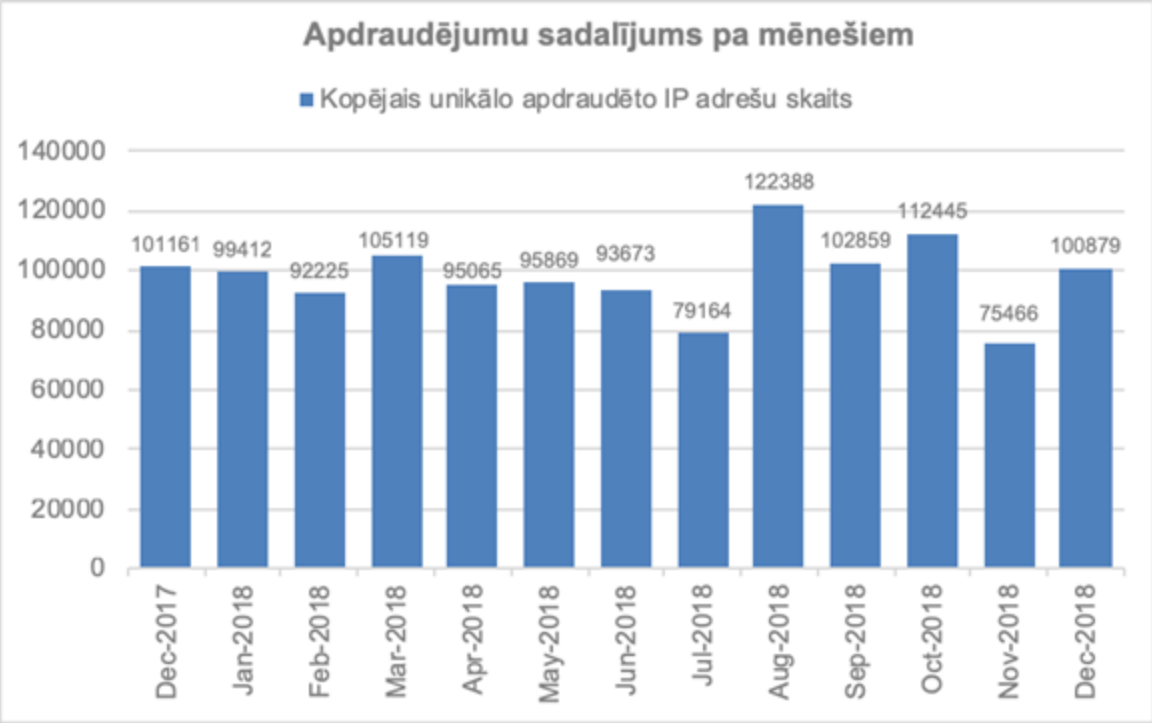
Pastiprinātu mediju interesi pārskata periodā radīja 6.oktobrī notikušais uzbrukums vietnei Draugiem.lv un kopējā drošības situācija Latvijas kibertelpā Saeimas vēlēšanu laikā, Kaspersky antivīrusa izmantošanas drošība un krāpnieciskie brīdinājumi par nokavētu nodokļu maksājumu, kas decembra sākumā tika izplatīti Finanšu ministrijas vārdā.

Pārskata periodā CERT.LV par IT drošību izglītoja 2913 cilvēkus, iesaistoties 41 izglītojošā pasākumā.

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.

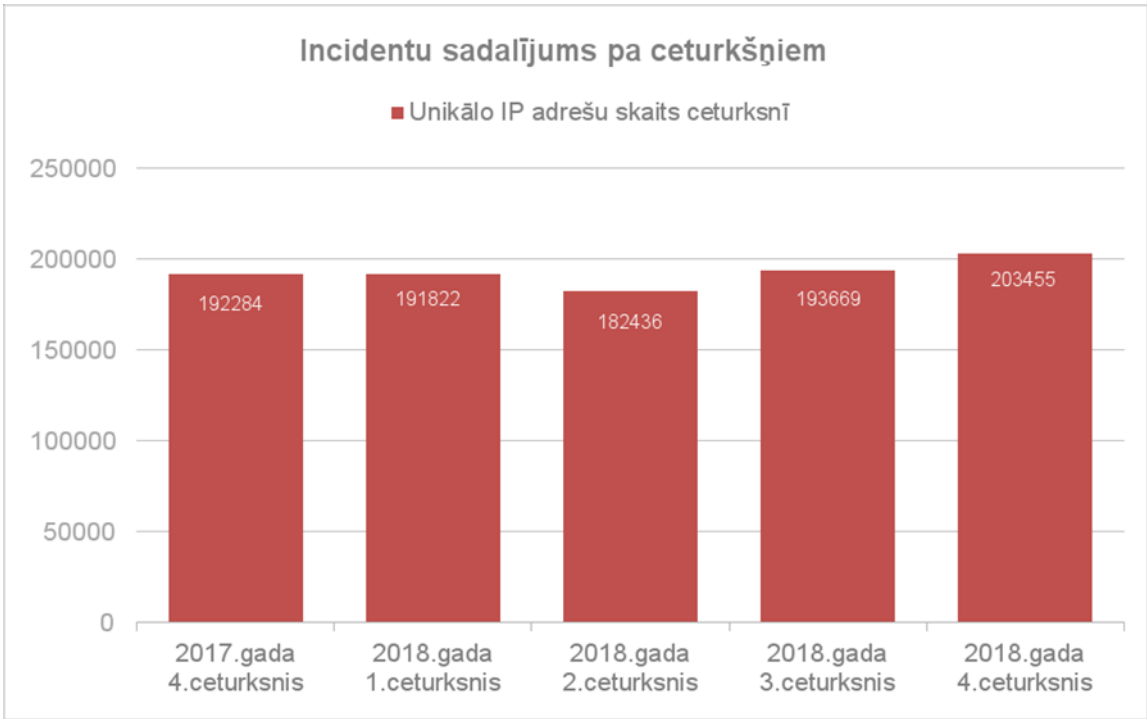
CERT.LV pārskata periodā ik mēnesi apkopoja informāciju par 95 000 – 100 000 ievainojamu unikālu IP adrešu.



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. Novērotais kritums novembrī radās nevienmērīgas ienākošās datu plūsmas rezultātā.

2018. gada 4. ceturksnī tika reģistrētas 203 455 unikālas apdraudētas IP adreses, kas ir par 5% vairāk nekā iepriekšējā ceturksnī, un par 5% vairāk nekā šajā pašā periodā pirms gada.



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

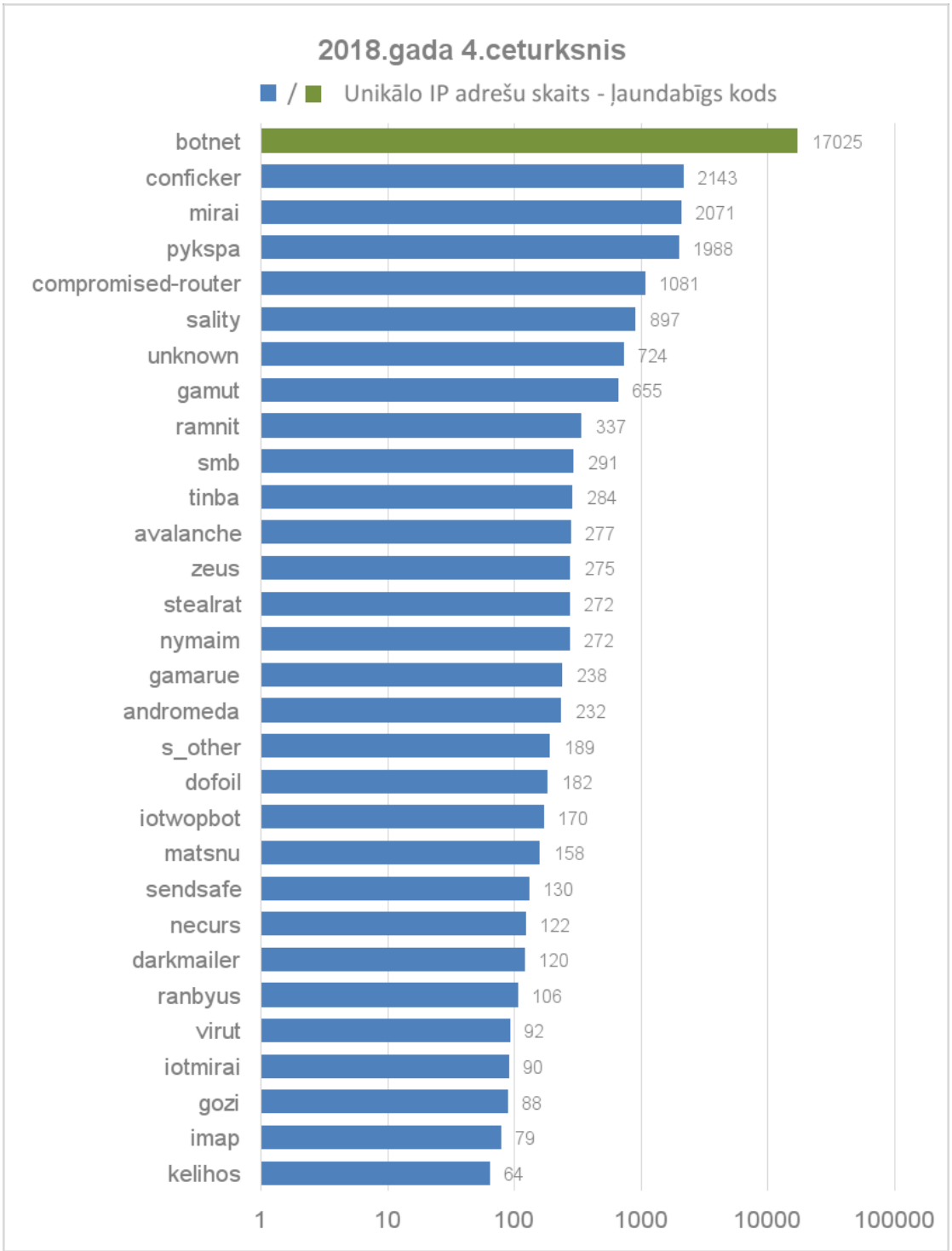
3.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2018. gada 4. ceturksnī pa apdraudējumu veidiem.

Izplatītākais apdraudējuma veids pārskata periodā nemainīgi bija konfigurācijas nepilnības (kritums par 8% pret iepriekšējo periodu), otrs izplatītākais bija ļaundabīgs kods (kritums par 22%), bet trešais - ielaušanās mēģinājumi (kritums par 4%).

Lielāko pieaugumu pārskata periodā piedzīvoja informācijas vākšanas mēģinājumi jeb mērķtiecīga noteiktu servisu ievainojamību meklēšana (pieaugums par 184%) un kompromitētu iekārtu apjoms (pieaugums par 168%). Informācijas vākšanas apjoma pieaugums skaidrojams gan ar to, ka daži datu avoti no oktobra pievienoja šo kategoriju

savam datu klāstam, gan arī ar kompromitētu lietu interneta (IoT) iekārtu skaita palielināšanos, kas iekļautas botnetos un meklē citas ievainojamas iekārtas.

Lai mazinātu inficēto iekārtu apjomu, CERT.LV veic iekārtu īpašnieku apziņošanu, taču bieži vien lietotājiem trūkst zināšanu un izpratnes par to, kā savu inficēto iekārtu salabot.

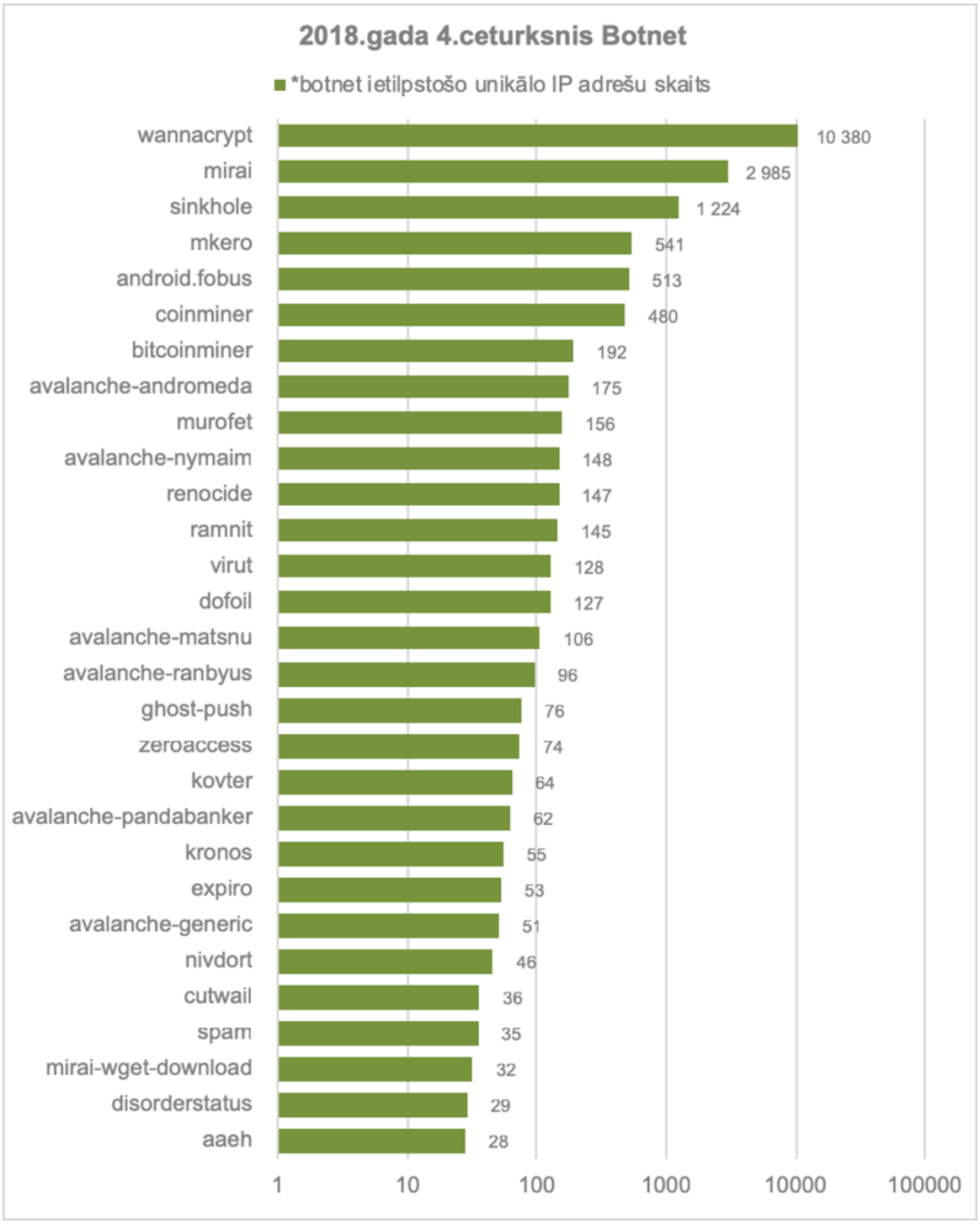


4.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2018. gada 4. ceturksnī ar apdraudējuma veidu - ļaundabīgs kods.

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

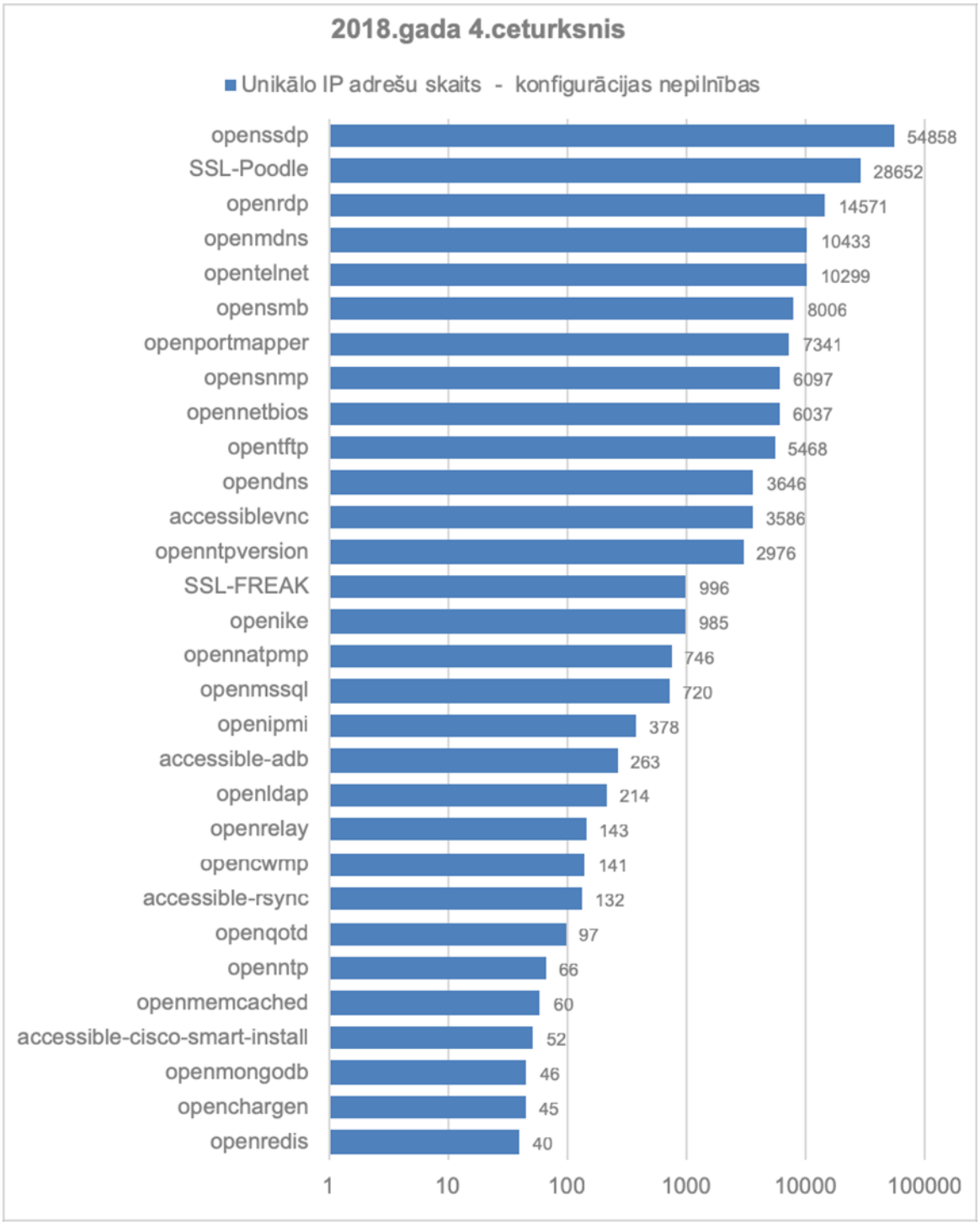
Otro vietu ļaunatūru topā notur *Conficker*, kaut arī tā ir jau sen pazīstama un salīdzinoši vienkārši „ārstējama" ļaunatūra.

Trešo vietu ieņem *Mirai* – ļaunatūra, kas inficē un iekļauj robotu tīklos jeb botnetos lietu interneta (IoT) iekārtas, lai izmantotu tās tālākiem uzbrukumiem un citām pretlikumīgām darbībām.



4.1.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2018. gada 4. 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 4. 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 konfigurācijas nepilnība *OpenRDP* pārskata periodā bija saistīta ar iekārtu un datu nesēju nošifrēšanu. Trešās puses bija piekļuvušas neatbilstoši konfigurētām iekārtām, kurās attālinātās piekļuves porti bija brīvi atvērti uz internetu un tām nebija pietiekami droša vai nebija uzstādīta piekļuves parole. Arī šo gadījumu mazināšanai CERT.LV veica neatbilstoši konfigurēto iekārtu īpašnieku apziņošanu, taču iekārtu īpašnieki ne vienmēr ar izpratni

izturas pret potenciālo apdraudējumu, uzskatot, ka ērtība ir svarīgāka par drošību. Apdraudēto iekārtu skaits, neskatoties uz apziņošanu, pagaidām samazinās lēni.

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.

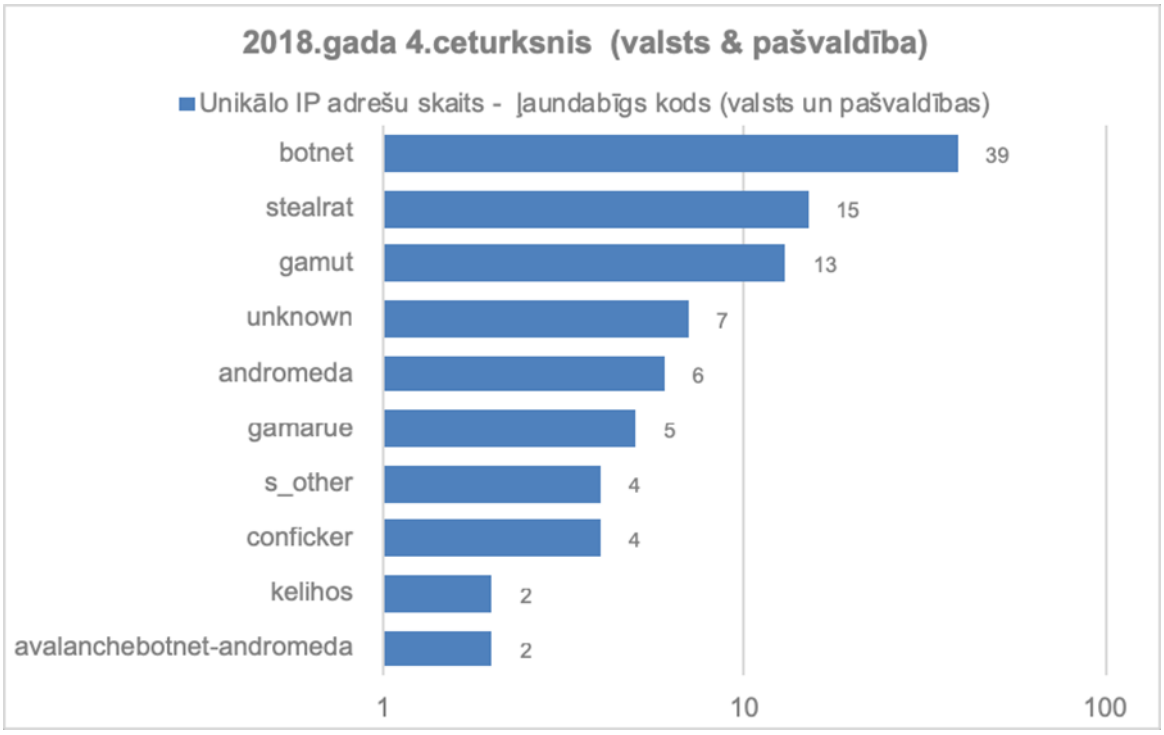
2. Atbalsts informācijas tehnoloģiju drošības incidentu novēršanā vai to novēršanas koordinēšanā.

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.

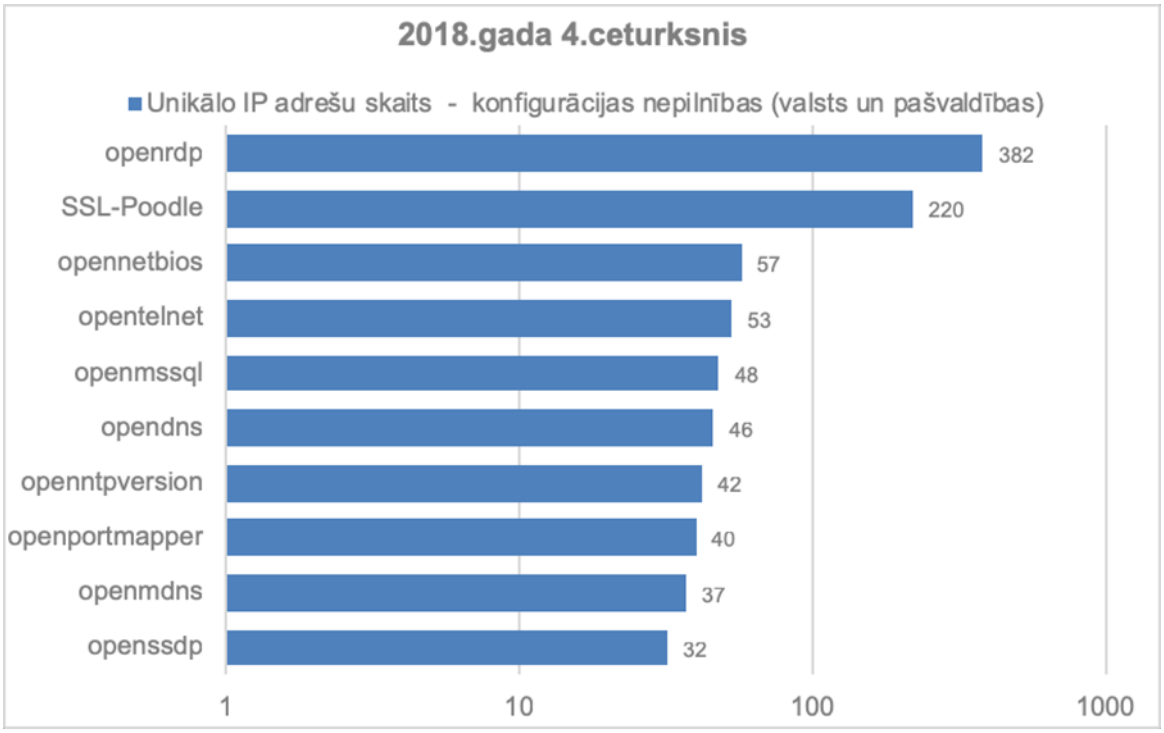
Izmaiņas katras dienas saņemtajos ziņojumos par valsts un pašvaldību iestādēm:

6.attēls – Iestāžu apdraudēto IP adrešu daudzums katras dienas saņemtajos ziņojumos 2018. gada 4. ceturksnī.

Vidējais apdraudēto valsts un pašvaldību iestāžu IP adrešu daudzums katras dienas saņemtajos ziņojumos pārskata periodā bija 550 unikālas IP adreses dienā.

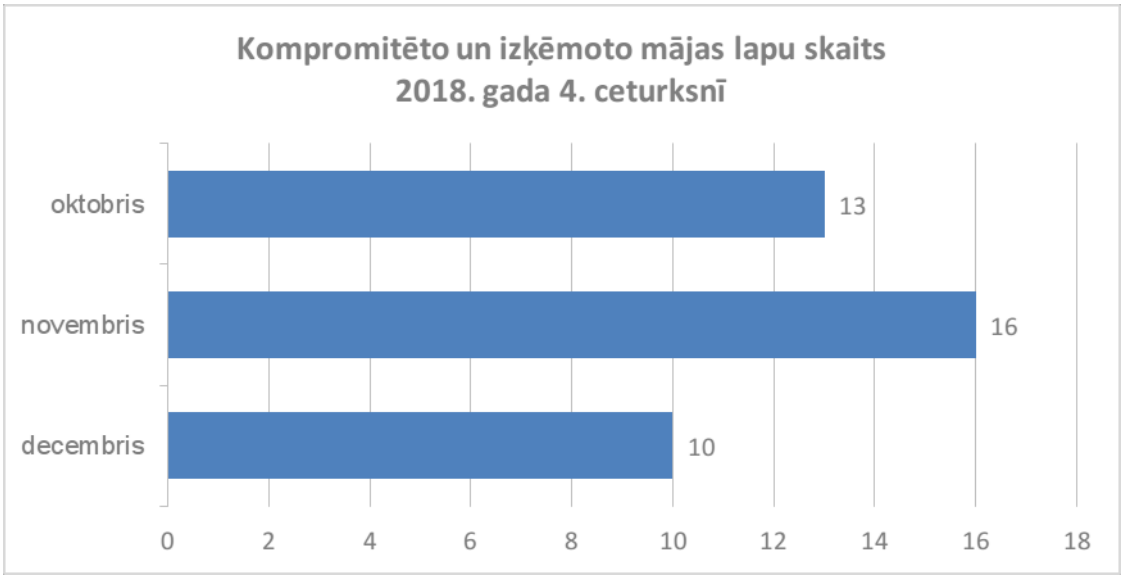


7.attēls - CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2018.gada 4.ceturksnī ar apdraudējuma veidu – ļaundabīgs kods (TOP 10 ļaundabīgs kods).



8.attēls - CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2018.gada 4. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība (TOP 10 konfigurācijas nepilnības).

CERT.LV uzskaita arī kompromitēto un izķēmoto tīmekļa vietņu gadījumus. Pārskata periodā tika fiksētas 39 kompromitētas un izķēmotas tīmekļa vietnes. Trīsdesmit piecos gadījumos izķēmotās vietnes uzturēšanai tika izmantota Linux operētājsistēma, trijos gadījumos Windows, bet vienā - FreeBSD. Piecas no visām pārskata periodā izķēmotajām tīmekļa vietnēm pēdējā gada laikā izķēmota atkārtoti.



9.attēls – Kompromitēto un izķēmoto tīmekļa vietņu skaits pa mēnešiem 2018. gada 4. 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

Pieejamība

Jau iepriekšējā pārskata periodā tika saņemti vairāki ziņojumi no tūrisma operatoriem par piekļuves atteices (DDoS) uzbrukumiem kompāniju tīmekļa vietnēm ar mērķi nodarīt kaitējumu uzņēmumu darbībai. Oktobra sākumā tika saņemts ziņojums no kāda tūrisma uzņēmuma par DDoS uzbrukumu kompānijas tīmekļa vietnei. Uzbrukums nodarīja kompānijai nopietnus zaudējumus, atstājot ietekmi uz kompānijas darbību arī nākotnē. Iepriekšēji draudi kompānijai izteikti netika. Uzņēmums vērsās ar iesniegumu policijā.

Tika saņemta informācija arī no kādas tūrisma aģentūras par piedzīvotu DDoS uzbrukumu. Novēršot uzbrukuma sekas un pilnveidojot tīmekļa vietnes uzturēšanai izmantotos risinājumus, vietne nebija pieejama gandrīz diennakti. Pirms tam bija saņemti telefoniski draudi.

Decembra vidū tika saņemts ziņojums no kādas valsts iestādes par iestādes vietnes nepieejamību. Vietnes darbības traucējumus radījušas problēmas ar virtualizācijas vidi, bet paredzētā pāreja uz rezerves risinājumu nenostrādāja. Šo traucējumu cēloņi pagaidām nav noskaidroti.

Pikšķerēšana jeb personīgo datu izkrāpšana

Saņemti vairāki ziņojumi par pikšķerēšanas vēstulēm, kurās saņēmēji aicināti nosūtīt personas datus, lai saņemtu mantojumu, ko kāds radinieks atstājis kādā ārzemju bankā. E-pasti bija lauzītā latviešu valodā.

Saņemts ziņojums par e-pasta piekļuves datu pikšķerēšanas mēģinājumu angļu valodā, kas izpaužas kā paziņojums par e-pasta konta slēgšanu. Paziņojumā saņēmējs tiek aicināts sekot saitei un atcelt konta slēgšanu, ja konta slēgšanu nav pieprasījis vai uzskata, ka paziņojumu ir saņēmis kļūdas pēc, pretējā gadījumā konts īsā laikā tiks slēgts.

Tika saņemti vairāki ziņojumi par pikšķerēšanas mēģinājumiem, kuros brīdināts, ka e-pasta konts tiks bloķēts un nevarēs nosūtīt un saņemt ziņas, jo pārsniegta administratora norādītā kvota vai tiek lietoti novecojuši drošības iestatījumi. Lietotāji tika aicināti sekot saitei, autentificēties un palielināt e-pasta kastītes limitu vai atjaunināt iestatījumus. Saņemti ziņojumi arī par brīdinājumu, ka konts tiks bloķēts, ja netiks veikta Microsoft Outlook konta atjaunināšana, sekojot saitei.

Tika saņemts ziņojums par krāpniecisku e-pastu it kā e-pasta pakalpojuma sniedzēja vārdā, aicinot lietotāju ievadīt e-pasta lietotāja vārdu un paroli norādītajā saitē, lai saņemtu vairākas aizturētas e-pasta vēstules, kas „novietotas gaidīšanas statusā, sakarā ar neseno datubāzes jaunināšanu".

Vairākkārtēji saņemti ziņojumi par PayPal piekļuves datu izkrāpšanai paredzētu e-pastu, kurā saņēmējs tika informēts par aizdomīgām aktivitātēm, kas reģistrētas viņa kontā, kā rezultātā konts ir ticis iesaldēts, un darbības atjaunošanai nepieciešams sekot saitei.

Tika saņemts ziņojums par kaitīgu skriptu kādā tiešsaistes tirdzniecības vietnē, kas pieprasa ievadīt maksājumu kartes informāciju. Arī vietnes noteikumos tika skaidri definēts, ka maksājumi ar karti netiek pieņemti. Vietnes uzturētāji tika informēti, kaitīgais skripts tika izņemts.

Ziņojums no kāda Lietuvas uzņēmuma par darbinieku e-pasta piekļuves informācijas pikšķerēšanu Latvijas kompānijas vārdā, aicinot sekot norādītajai saitei un ievadīt e-pasta piekļuves datus, lai aplūkotu pasūtījuma statusu. E-pastā tiek vairākkārtēji uzsvērts, ka kompānijai kā sadarbības partnerim norādītajā tīmekļa vietnē ir izveidots lietotāja konts, kurā darbiniekiem ir iespēja autorizēties, izmantojot aktuālos e-pastus un paroles.

Tika saņemts paziņojums no kāda lietotāja par uznirstošu logu, apmeklējot iepazīšanās vietnes. Lietotājs tika aicināts ievadīt personīga rakstura informāciju, lai laimētu mobilo telefonu. CERT.LV brīdināja, ka tā ir pikšķerēšanas kampaņa. Par līdzīgu uznirstošu logu informēja arī kāds cits lietotājs, kuram tika paziņots, ka viņš iekļuvis nelielā to lojālo Google Chrome lietotāju lokā, kuriem ir iespēja laimēt Samsung Galaxy S9, aizpildot mazu aptauju. Arī šajā gadījumā CERT.LV apstiprināja, ka tas ir datu izkrāpšanas mēģinājums.

No kāda lietotāja tika saņemta ziņa par krāpniecisku reklāmu, kas sociālajā tīklā Facebook tiek rādīta arī Latvijas lietotājiem un reklamē CNBC pikšķerēšanas vietni. Tika ieteikts ziņot Facebook par neatbilstošu reklāmu.

Decembra beigās no kāda lietotāja tika saņemta ziņa par krāpnieciskām reklāmām Facebook sociālajā tīklā, kurās tika reklamēts krāpniecisks interneta veikals – nemainījās veikala izskats, bet katru reizi mainījās veikala adrese.

Saņemts ziņojums no kāda lietotāja par personas datu pikšķerēšanas mēģinājumu, paziņojot par vinnestu Jackpot loterijā. E-pasts bija noformēts lauzītā latviešu valodā.

Tika saņemts ziņojums no kādas valsts iestādes par vairākiem pikšķerēšanas e-pastiem darbinieku e-pasta piekļuves datu izgūšanai, kuri sūtīti administratora vārdā un informē lietotājus par sastrēgumu datubāzē, kura novēršanai visi neizmantotie konti tiks slēgti. Lai pierādītu sava konta aktīvu darbību, lietotāji aicināti sekot saitei un ievadīt prasīto informāciju. E-pasti, lai arī lauzītā latviešu valodā, bija tikuši cauri visiem ugunsmūriem. Nav informācijas, ka kāds lietotājs datus būtu ievadījis.

Tika saņemta informācija par vairākām uzlauztām .lv vietnēm un Latvijas IP adresēm, kurās tika izvietota pikšķerēšana, kas vērsta uz Amazon, Bank of New Zealand, Netflix, Microsoft, UniCredit, Blockchain, Beļģijas bankas Argenta, The Canadian Imperial Bank of Commerce, First National Bank of PA, Francijas valsts institūcijas, kas nodrošina veselības apdrošināšanu, un Spānijas banku Caja Rural un CajaMar klientiem.

Krāpšana

Tika saņemts ziņojums par loteriju PayPal vārdā. E-pasta saņēmējs tika aicināts nomaksāt nodokli 3.99 eiro apmērā, sekojot saitei, lai saņemtu pārsteiguma balvu 1300 eiro vērtībā.

Tika saņemta informācija no kādas valsts iestādes par krāpniecības mēģinājumu latviešu valodā, kurā jautāts par konta atlikumu un aicināts veikt steidzamu pārskaitījumu 49 245.00 eiro apmērā uz kontu Turcijā. No kāda uzņēmuma tika saņemts līdzīgs ziņojums par krāpniecību angļu valodā, kurā tika izteikts aicinājums veikt steidzamu pārskaitījumu 34 240 eiro apjomā.

Ziņojums no kāda novada pašvaldības par krāpniecisku e-pastu, kas saistīts ar publiskā iepirkuma rezultātā noslēgta līguma izpildi. E-pastā norādīts, ka tiek mainīts līgumā norādītais bankas konts, un ir lūgums pārsūtīt līguma kopiju, kā arī pēdējo rēķinu, ja tāds ir ticis izrakstīts.

Tika saņemti 76 ziņojumi par e-pastu, kurā uzbrucējs apgalvo, ka uzlauzis upura datoru, ieguvis kontaktu sarakstu un ierakstījis upura pieaugušajiem domātas tīmekļa vietnes apmeklējumu, kuru draud izsūtīt visiem kontaktiem, ja netiks samaksāta izpirkuma maksa. Atsevišķos gadījumos kā pierādījumu visu apgalvojumu patiesumam uzbrucējs norādīja, ka zina upura paroli vai daļu telefona numura. 12 izspiešanas mēģinājumi tika fiksēti latviešu valodā, pārējie - angļu. Saņēmēji – gan privātpersonas, gan uzņēmumu un valsts iestāžu darbinieki. CERT.LV visos gadījumos uzsvēra, ka draudi nav pamatoti un uzbrukums nav noticis, bet parole iegūta kādā no internetā publiskotajām datu noplūdēm, atgādinot, ka sev svarīgos interneta resursos jālieto drošas un unikālas paroles, kā arī jāizmanto divu faktoru autentifikācija.

Saņemts ziņojums no kāda uzņēmuma par krāpniecības mēģinājumu, piesaistot lasītāja uzmanību ar brīdinājumu par viņa lietotā domēnvārda reģistrācijas termiņa beigām un aicinot veikt maksājumu. Veicot ziņojuma analīzi, tika secināts, ka to par krāpniecisku nevar uzskatīt, jo sūtītājs tekstā ir skaidri norādījis, ka atgādina par reģistrācijas termiņa beigām, bet reģistrāciju neveic, tā vietā pārdodot iespēju uzlabot savu pozīciju interneta meklētājos (SEO).

Ielaušanās mēģinājumi

Saņemti ziņojumi par virkni automatizētu ielaušanās mēģinājumu, kas veikti no robotu tīklos iekļautām inficētām iekārtām ar lielākoties novecojušu satura vadības sistēmu (CMS) vai labajai praksei neatbilstošu ievainojamu konfigurāciju.

Tika saņemts ziņojums par aktīviem neautorizētiem mēģinājumiem pieslēgties RDP servisam, neskatoties uz to, ka konkrētajā gadījumā RDP servisam tika izmantots nestandarta ports. CERT.LV aicināja ierobežot piekļuvi šim servisam no noteiktām IP adresēm, pieslēgumam izmantot VPN, un lietotājiem, kuriem atļauts pieslēgums, izmantot vismaz 14 simbolus garas paroles. Porta maiņa no šādiem uzbrukumiem nepasargā.

Saņemti vairāki ziņojumi no Sony Interactive Entertainment LLC par servisu lietošanas nosacījumiem neatbilstošu uzvedību no Latvijas IP adresēm. Neatbilstošās aktivitātes pārtrauktas.

Oktobra beigās un novembrī tika saņemti ziņojumi no kādas valsts iestādes par neveiksmīgiem mēģinājumiem autentificēties SMTP servisā no ārvalstu IP adresēm.

Novembra otrajā pusē tika saņemts incidenta pieteikums, kurā ziņots, ka CSDD darbinieki saskārušies ar kādas personas nesankcionētu mēģinājumu piekļūt Transportlīdzekļu reģistram un centieniem veikt naudas izspiešanu. Sadarbībā ar Valsts policiju iespējamais vainīgais tika aizturēts. Aizturētajai personai nebija izdevies piekļūt CSDD reģistrā esošajiem datiem un nebija notikusi datu noplūde. Izmantotā ievainojamība e-CSDD portālā tika apzināta un novērsta. Pret personu tika uzsākts kriminālprocess pēc Krimināllikuma 183.panta pirmās daļas, 241.panta trešās daļas, un 15.panta ceturtās daļas, proti, par informācijas sistēmas darbības traucēšanas mēģinājumu un izspiešanas mēģinājumu mantkārīgos nolūkos.

Saņemts lūgums no Čehijas CERT vienības apzināt automatizētā uzbrukumā iesaistīto Latvijas IP adrešu īpašniekus un novērst pārkāpumu. Informācija nodota atbilstošajiem interneta pakalpojumu sniedzējiem.

Decembra beigās saņemta informācija par uzbrukumu kādai valsts iestādes vietnei. Vairāki desmiti tūkstoši pieprasījumu nāca no Krievijas IP adresēm, un veica mēģinājumus izpildīt dažādus SQL injection paņēmienus, kas veiksmīga uzbrukuma gadījumā ļautu apmeklētāja pārlūkā manipulēt ar vietnes saturu un sīkdatnēm vai izmantot pārlūkam piemērotus mūķus (exploits). Uzbrukums portāla darbību neietekmēja.

Ļaunatūra

Pārskata periodā tika saņemti vairāki ziņojumi par ļaunatūras izplatīšanu saitēs vietnē failiem.lv. Kaitīgais saturs tika dzēsts.

Oktobra beigās saņemts ziņojums par e-pastu, kurā saņēmējs aicināts aplūkot it kā pielikumā esošu pasūtījuma specifikāciju un nekavēties ar pasūtījuma informāciju, lai padarītu iespējamu laicīgu preces piegādi, jo Ziemassvētki vairs nav aiz kalniem. Pielikums saturēja par PDF dokumentu maskētu .GZ arhīvu ar vīrusu, kurš ievāc informāciju par visām iekārtā saglabātajām parolēm no e-pastu klientiem, interneta pārlūkiem un attālinātās piekļuves klientiem.

Novembra otrajā pusē tika saņemts ziņojums no kāda uzņēmuma par kaitīgu e-pastu, kas DHL vārdā tika nosūtīts uzņēmuma darbiniekam. E-pasts saturēja RAR arhīva pielikumu ar šifrējošo izspiedējvīrusu.

Tika saņemts ziņojums par kaitīgu e-pastu, kurā sūtītājs aicina saņēmēju aplūkot pielikumā pievienoto maksājuma dokumentu un sazināties ar sūtītāju, izmantojot maksājumā norādīto kontaktinformāciju, ja saņēmējam ir radušies kādi jautājumi šī maksājuma sakarā. E-pasta pielikumā .ARJ datne, kas saturēja e-pasta klientu, tērzētavu (*messenger*) un pārlūkprogrammu paroļu zādzībai paredzētu ļaunatūru.

Decembra sākumā no kāda uzņēmuma tika saņemts ziņojums par e-pastu no nezināmas e-pasta adreses, kurā, atsaucoties uz iepriekšēju vienošanos, sūtītājs pielikumā nosūta saņēmējam maksājuma apstiprinājumu. Analīzes rezultātā tika noskaidrots, ka pielikumā esošais fails satur klaviatūras rakstzīmju ievades pārtveršanas programmatūru (*keylogger*).

Decembrī tika saņemti vairāki ziņojumi par Finanšu ministrijas vārdā izplatītu e-pastu ar tēmu „nokavētu nodokļu maksājumu", kas pielikumā saturēja par PDF dokumentu maskētu .ZIP arhīvu. Atverot šo failu, dators tika inficēts ar vīrusu, kas ievāc datorā uzglabātās paroles un, iespējams, sašifrē iekārtā esošos failus, lai pieprasītu izpirkuma maksu par failu atgūšanu.

Tika saņemts ziņojums par kādas pašvaldības vietnē ievietotu ļaunatūru, kura, apmeklētājam apmeklējot šo vietni pirmo reizi, izveidoja apmeklētājam sīkdatni (*cookies*) un veica apmeklētāja pārvirzīšanu uz citu vietni. Ļaundabīgais kods no vietnes tika izņemts, bet vietnes satura vadības sistēma netika atjaunināta.

Saņemts ziņojums par vairāku ļaunatūru – *Citadel botnet*, *Loki botnet*, *Gozi botnet*, *AZORult botnet*, *RevCodeRAT botnet*, *NanoCore botnet* un *Zbot* ļaunatūras – komand- un kontroles centriem (C&C) Latvijas IP adresēs.

Citadel trojānis paredzēts upura finanšu informācijas zādzībai un bankas kontu iztukšošanai. *NanoCore* trojānis ļauj uzbrucējam attālināti kontrolēt upura iekārtu un ievākt informāciju par, piemēram, ievadītajām parolēm. *Gozi* spiegojošā ļaunprogrammatūra pārtver tīkla plūsmu, nolasa lietotāja piekļuves datus, kas saglabāti pārlūkprogrammās un e-pasta klientos, kā arī fiksē klaviatūras taustiņu nospiedienus (*keylogger*) un uz ekrāna redzamo informāciju (screen capture). *AZORult* arī ir trojānis, kas paredzēts informācijas – pārlūkos saglabāto paroļu, dažādu aptaujas formu automātiski aizpildāmās informācijas, tērzētavu sarakstes, iekārtā instalēto programmu, lietotājvārdu, failu – zādzībai, kuru ļaunatūra pārtver un nosūta tālāk uz komandcentru. *RevCodeRAT* ir trojānis upura iekārtas attālinātai piekļuvei un pārvaldībai. *Zbot* (*Zeus*) ir spiegojošā ļaunprogrammatūra, kas primāri orientēta uz informāciju par upura iekārtu, tiešsaistes piekļuves datiem un finanšu informāciju, bet var tikt pielāgota jebkuras citas informācijas ieguvei vai modificēta, lai traucētu iekārtas darbību vai iznīcinātu iekārtu. Taču visvairāk C&C pārskata periodā bija *Loki* ļaunatūrai, kas paredzēta paroļu un citas sensitīvas informācijas zādzībai.

Visos gadījumos apzināti iekārtu, kurās izvietoti C&C, uzturētāji, un apdraudējums novērsts.

Kompromitētas iekārtas

Saeimas vēlēšanu dienā tika saņemts ziņojums par uzbrukumu portālam Draugiem.lv. Portālā bija redzami ar Krievijas Federāciju saistīti attēli un fonā skanēja Krievijas himna. Portāls uz laiku bija nepieejams lietotājiem. To pārbaudot, netika konstatēts portālā ievietots ļaundabīgs saturs, kas būtu kaitīgs lietotāja iekārtai, uzbrukums vērtējams kā vietnes kompromitēšana un izķēmošana. Incidenta risināšanā tika iesaistīta Valsts policija.

No vairākiem lietotājiem tika saņemts lūgums palīdzēt atgūt informāciju, jo visi iekārtā esošie faili ir tikuši nošifrēti. Lietotājiem tika ieteikts pārbaudīt vietnē nomoreransom.org, vai viņu „noķertajam" vīrusam ir pieejama atšifrēšanas atslēga, kā arī ieteikti daži papildu rīki, ar kuriem varētu mēģināt atgūt vismaz daļu failu. Tāpat tika norādīts, ka drošākais informācijas atgūšanas veids būtu rezerves kopijas izmantošana.

Saņemts iesniegums no kāda uzņēmuma par kaitīgu nodarījumu, kura rezultātā uzņēmums ir cietis būtiskus zaudējumus. Nezināmas personas veikušas uzbrukumu uzņēmuma interneta veikalam, pilnībā iznīcinot veikala funkcionēšanai nepieciešamos failus, kuru atgūšana iespējama no rezerves kopijām, bet ar nepilnīgiem datiem, jo kopēšana tiek veikta tikai reizi nedēļā. Uzbrukumā pilnīgi izdzēsta arī internetveikala preču uzskaites programma, kuras atjaunošana nav iespējama. Uzņēmumam ieteikts ar iesniegumu vērsties policijā.

Tika saņemts ziņojums no kāda uzņēmuma par nošifrētu serveri. Uzbrucēji piekļuvuši datiem, izmantojot RDP servisu, uzminot pārāk vienkāršo piekļuves paroli. Iznīcināta arī datu rezerves kopija. Citas uzņēmuma iekārtas netika skartas. Uzbrucēju pieprasītā izpirkuma maksa uzņēmumam bija nepieņemami augsta, tādēļ, lai arī pagaidām nav zināms veids, kā konkrētā veidā ietekmētos datus atgūt, nesamaksājot, uzņēmums izpirkuma maksājumu neveica.

Decembrī saņemts ziņojums no kāda lietotāja par kompromitētu kriptovalūtas kontu, kā rezultātā lietotājs ir cietis finansiālus zaudējumus. Uzbrucējiem bija izdevies kompromitēt kontu, apejot drošu paroli un divu faktoru autentifikāciju. Konta uzturētāji un CERT.LV aicināja lietotāju vērsties ar iesniegumu policijā.

Atbildīga ievainojamību atklāšana

Pārskata periodā atbildīgas ievainojamību atklāšanas ietvaros tika saņemti ziņojumi par starpvietņu skriptēšanas (XSS) ievainojamībām 6 valsts iestāžu tīmekļa vietnēs.

Ievainojamības ļautu izpildīt uzbrukumu apmeklētāja pārlūkā, sniedzot uzbrucējam iespēju, piemēram, manipulēt ar vietnes saturu un sīkdatnēm vai izmantot pārlūkam piemērotus mūķus (*exploits*). CERT.LV koordinēja ievainojamību novēršanu.

CERT.LV pasākumi incidentu novēršanā:

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

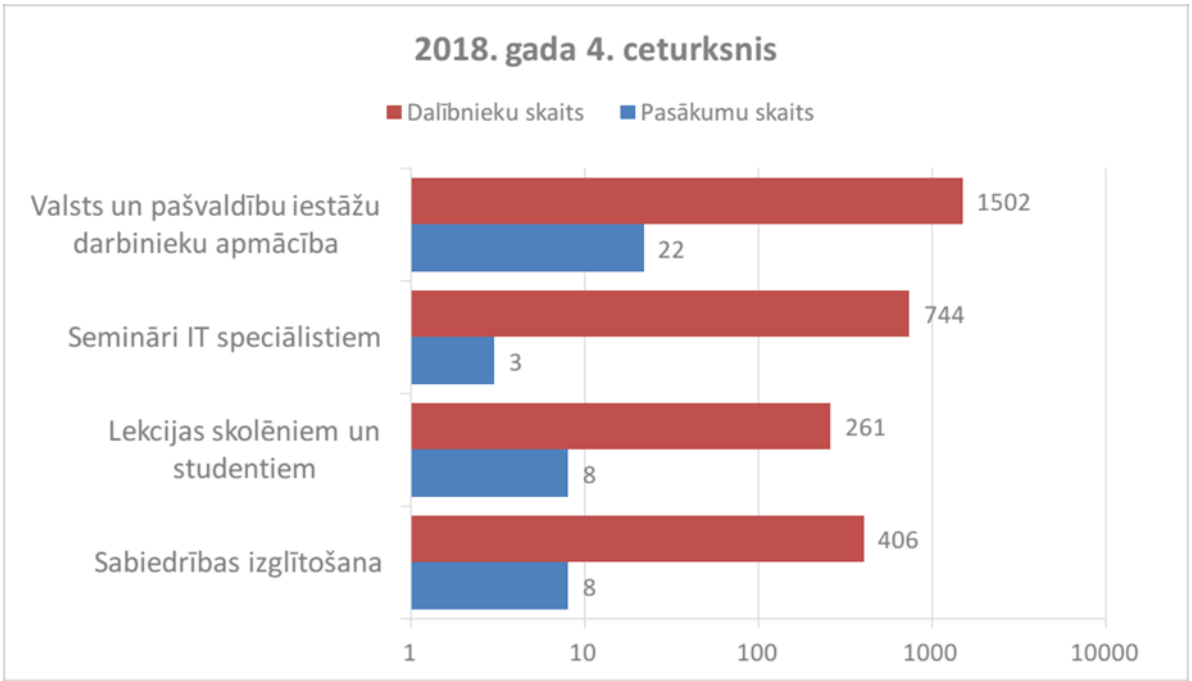
Cita veida sadarbība ar dažādām iestādēm ir norādīta atskaites 6. punktā.

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

Oktobrī CERT.LV pārstāvis piedalījās praktiskajā konferencē "Kiberdrošības kompetence Latvijā: iespējas un izaicinājumi Eiropas Savienības kiberdrošības stratēģijas kontekstā", diskutējot par aktuālo situāciju kiberdrošības kompetenču jomā Latvijā, ieskicējot problēmas un iespējas, lai izveidotu tādu kiberdrošības kompetenču nodrošināšanas modeli, kas varētu radīt priekšnoteikumus kiberdrošības tehnoloģiskajai un pārvaldības kvalitātei gan publiskajā, gan privātajā sektorā.

Pārskata periodā CERT.LV pārstāvis sniedza atbalstu Eiropas Komisijas pārstāvniecībai Latvijā digitālās spēles #DigiSafe izstrādē, kurā jaunieši atraktīvā veidā var pārbaudīt savas zināšanas par drošību un tiesībām internetā.

Pārskata periodā CERT.LV par IT drošību izglītoja 2913 cilvēkus, iesaistoties 41 izglītojošā pasākumā.



10.attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2018. gada 4. ceturksnī

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

Sadarbības tikšanās, konsultācijas un prezentācijas:

- CERT.LV piedalījās diskusijās par darba grupas izveidi, gatavojoties Eiropas Parlamenta vēlēšanām, lai izmantotu Saeimas vēlēšanās gūto pieredzi kiberapdraudējumu mazināšanai.
- Varis Teivāns un Baiba Kaškina tika apbalvoti ar Aizsardzības ministrijas goda rakstiem par veiksmīgu sadarbību un atbalstu, tā sniedzot savu ieguldījumu Latvijas valsts aizsardzībā un drošībā.
- Varis Teivāns tika apbalvots ar jubilejas goda zīmi „Latvijas Valsts policijai 100".

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:

- Pārskata periodā CERT.LV pārstāvis turpināja pildīt TF-CSIRT Steering komitejas vadītāja pienākumus, piedaloties gan klātienes, gan attālinātās sanāksmēs un organizējot TF-CSIRT darbu.
- 15. oktobrī CERT.LV pārstāvis piedalījās NATO CCDCoE kiberdrošības mācību „Cyber Coalition 2018" organizēšanas sanāksmē Tallinā, Igaunijā.
- 06.-09. novembrī CERT.LV pārstāvji piedalījās „NIS CSIRT network" sanāksmē Vīnē, kā arī

„Cyber Weather" un „Toolings" darba grupu sanāksmēs.

- 08.-10. novembrī CERT.LV pārstāvis kopā ar līdzautoru Arturu Lavrenovu (Latvijas Universitāte) AIEEEE2018 konferencē Viļņā prezentēja „Security Implications of Using Third-Party Resources in the World Wide Web".
- 26.-28. novembrī CERT.LV pārstāvis pasniedza NATO CCDCoE „Cyber Executive Seminar" kursu Tallinā, Igaunijā.
- 27.-30. novembrī CERT.LV pārstāvji piedalījās NATO CCDCoE kiberdrošības mācībās „Cyber Coalition 2018", kurās tika iesaistīti aptuveni 700 sabiedroto spēku, partneru, industrijas un akadēmiskās vides pārstāvju, lai uzlabotu sadarbību un procedūras informācijas apmaiņai, kibertelpas novērtējumam un lēmumu pieņemšanai.
- 27.11.-01.12. CERT.LV pārstāvis piedalījās ENISA kiberdrošības mācību „Cyber Europe 2018" izvērtēšanas sanāksmē Atēnās, Grieķijā.
- 28.novembrī CERT.LV pārstāvis piedalījās CEF Governance board sanāksmē Briselē, Beļģijā.
- 02.-09. decembrī CERT.LV pārstāvji piedalījās NATO CCDCoE kiberdrošības mācību "Crossed Swords 2019" pārbaudes pasākumā Tallinā, Igaunijā.

Sadarbība konkrētu incidentu risināšanā aplūkota pārskata 2. punktā.

6. Projekta "Improving Cyber Security Capacities in Latvia" īstenošana

1.septembrī CERT.LV ir uzsākusi 2017 CEF Telecom-Cyber Security uzsaukumā apstiprinātā projekta "Improving Cyber Security Capacities in Latvia" (līguma ar Eiropas Komisiju Nr.INEA/CEF/ICT/A2017/1528784) (turpmāk – Projekts) īstenošanu.

Pārskata periodā CERT.LV turpināja realizēt Projektu. Projekta ietvaros tika nodrošināts finansējums nepieciešamajai starptautiskajai sadarbībai - no projekta līdzekļiem līdzfinansēti CERT.LV darbinieku komandējumi uz konferencēm un dalība dažādos kursos. Tika uzsākta arī "Deep Analysis System" izstrāde un pielāgošanas darbi.

2018.gada 9.oktobrī notikusī kiberdrošības konference "Kiberšahs 2018" tika līdzfinansēta no projekta līdzekļiem.

2019.gadā projekta ietvaros tiks rīkoti vairāki tehnikas iepirkumi, ir uzsākta gatavošanās šiem iepirkumiem.

7. Projekta ‘‘Cyber Exchange’’ īstenošana

1.novembrī CERT.LV ir uzsākusi 2017 CEF Telecom-Cyber Security uzsaukumā apstiprinātā projekta “Cyber Exchange” (līguma ar Eiropas Komisiju Nr. INEA/CEF/ICT/A2017/1528784) (turpmāk – Sadarbības projekts) īstenošanu.

Novembrī CERT.LV pārstāvji piedalījās Sadarbības projekta atklāšanas sanāksmē, ko organizēja projekta koordinators - CZ.NIC, z. s. p. o., un kas 5.novembrī notika Vīnē, Austrijā. Sanāksmē tika uzsāka kiberdrošības ekspertu apmaiņas plāna sastādīšana un citas projekta aktivitātes.

8. Citi normatīvajos aktos noteiktie pienākumi.

- 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 (domēna vārdi, IP adreses u.c.). Projekta ieviešana turpinās 4 iestādēs. Projekta ietvaros ir bijuši jau vairāki gadījumi, kuros nostrādājusi aktīvā aizsardzība, pasargājot iekārtas no inficēšanas.
- CERT.LV turpināja darbu 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.

9. 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 01.10.2018. līdz 31.12.2018. ir saņēmusi un izvērtējusi 176 ziņojumus. No tiem 58 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 15 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 25 ziņojumos konstatēta personas goda un cieņas aizskaršana un 2 ziņojumi saņemti par naida runu. Par finanšu krāpšanas mēģinājumiem internetā saņemti 26 ziņojumi, 14 ziņojumu saturs nav bijis pretlikumīgs, 36 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. 41 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