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

2019

2019. gada 1. ceturksnis (01.01.2019. – 31.03.2019.)

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

2019.gada 1.ceturksnī CERT.LV apkopoja informāciju par 199 210 unikālām apdraudētām IP adresēm, kas ir par 3% mazāk nekā iepriekšējā ceturksnī, bet par 3% vairāk nekā šajā pašā periodā pirms gada.

Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (137 209 unikālas IP adreses) ar pieaugumu 4% pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs kods (19 859 unikālas IP adreses) ar kritumu 17%, bet trešais - ielaušanās mēģinājumi (2436 unikālas IP adreses) ar kritumu 2%.

Lai arī uz gala lietotājiem orientētā krāpnieciskā kampaņa, kurā e-pasta sūtītājs apgalvo, ka ir uzlauzis upura iekārtu un zina upura paroli, ilgst jau gandrīz gadu un par šo kampaņu ir bijuši sižeti medijos, CERT.LV turpina saņemt satrauktus ziņojumus ar lūgumu palīdzēt.

Otra pārskata periodam raksturīga iezīme ir bijusi loterijas gan Latvijā populāru interneta pakalpojumu sniedzēju, gan VAS „Latvijas pasts", gan arī dažādu interneta pārlūku vārdā, kas piedāvā iespēju laimēt Galaxy S9 vai iPhone XS, ja tiks sniegtas atbildes uz vienkāršiem jautājumiem. Vietnē ievietota nemanāma atruna, ka šis ir maksas pakalpojums.

Pārskata periodā notika aktīva gatavošanās NATO tehniskajam semināram, kas marta vidū notika Rīgā, kā arī noritēja aktīvs darbs, gatavojoties NATO CCDCoE organizētajām kiberdrošības mācībām "Locked Shields 2019", kuru norise plānota aprīļa sākumā un kurās CERT.LV aktīvi iesaistījās gan zilās (aizstāvošās) komandas, gan sarkanās (uzbrūkošās) komandas aktivitātēs, gan arī organizatoriskajās norisēs.

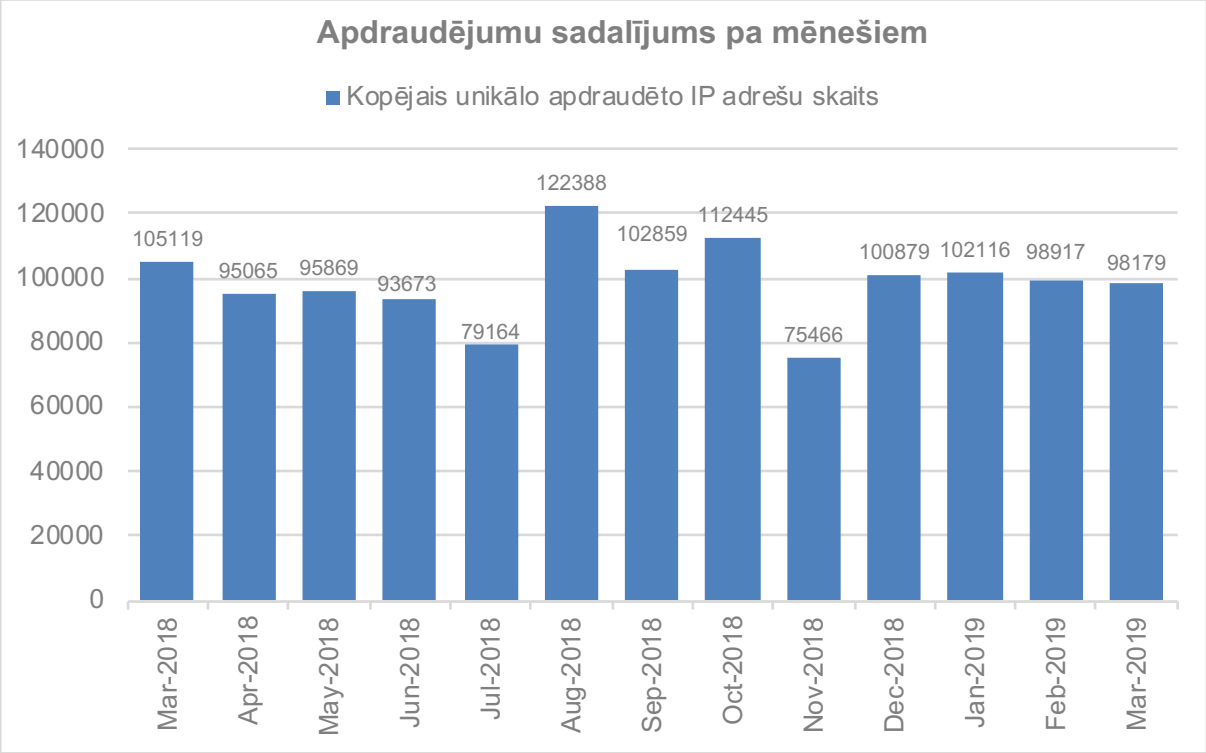
Janvārī CERT.LV pārstāvji piedalījās ikgadējās tehniskajās kiberdrošības mācībās "Crossed Swords 2019", kas tapa, sadarbojoties NATO CCDCoE un CERT.LV, un notika Tallinā, Igaunijā. Mācību galvenā uzmanība tika vērsta uz sarkanā karoga komandu ofensīvo prasmju attīstību kiberoperāciju plānošanā, izpildē un reaģēšanā uz apdraudējumu. Mācībās piedalījās vairāk nekā 100 dalībnieki no 21 valsts.

Pārskata periodā CERT.LV par IT drošību izglītoja 1470 cilvēkus, iesaistoties 24 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.

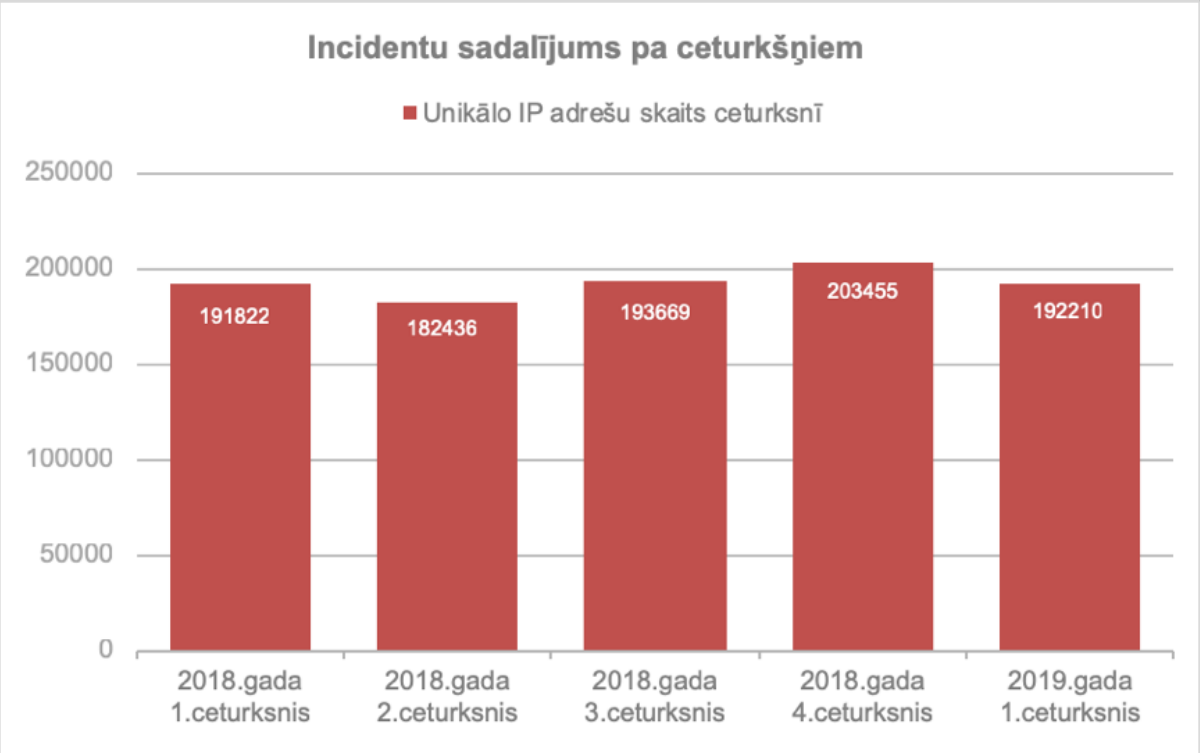
CERT.LV pārskata periodā ik mēnesi apkopoja informāciju par 95 000 – 100 000 ievainojamu unikālu IP adrešu.



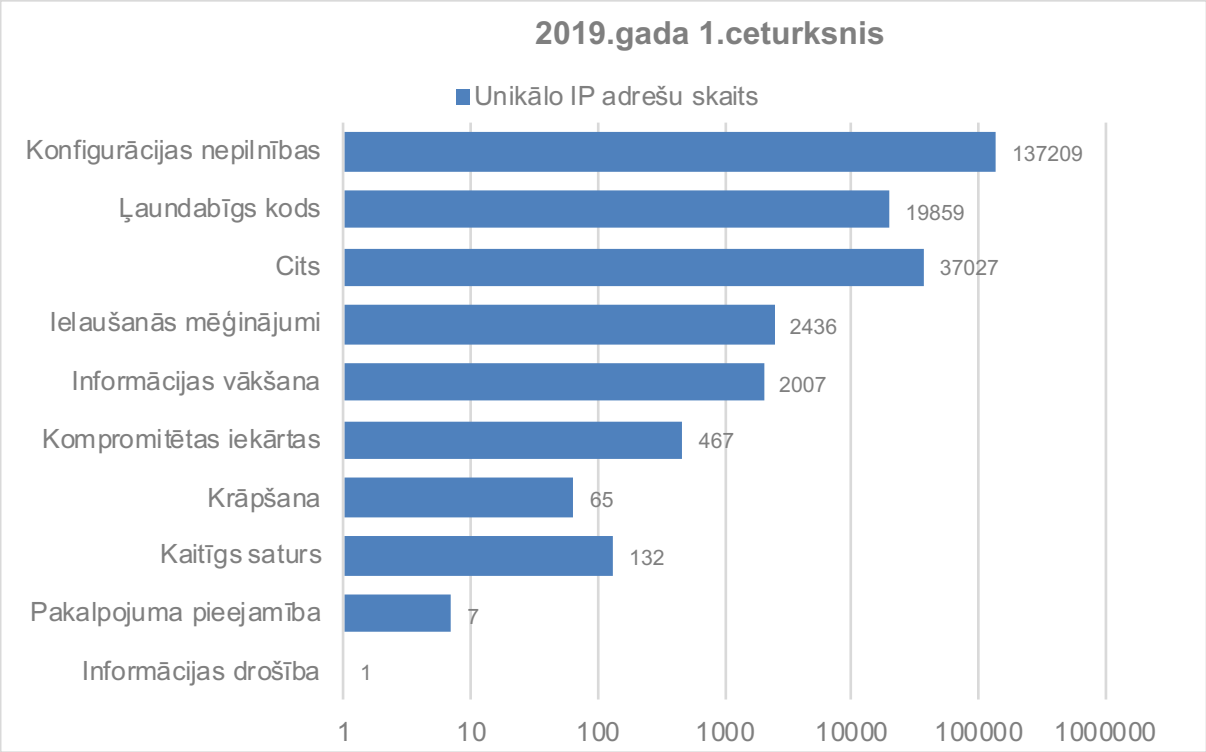
1.attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa mēnešiem 12 mēnešu griezumā.

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

2019. gada 1. ceturksnī tika reģistrētas 199 210 unikālas apdraudētas IP adreses, kas ir par 3% mazāk nekā iepriekšējā ceturksnī, bet par 3% vairāk nekā šajā pašā periodā pirms gada.

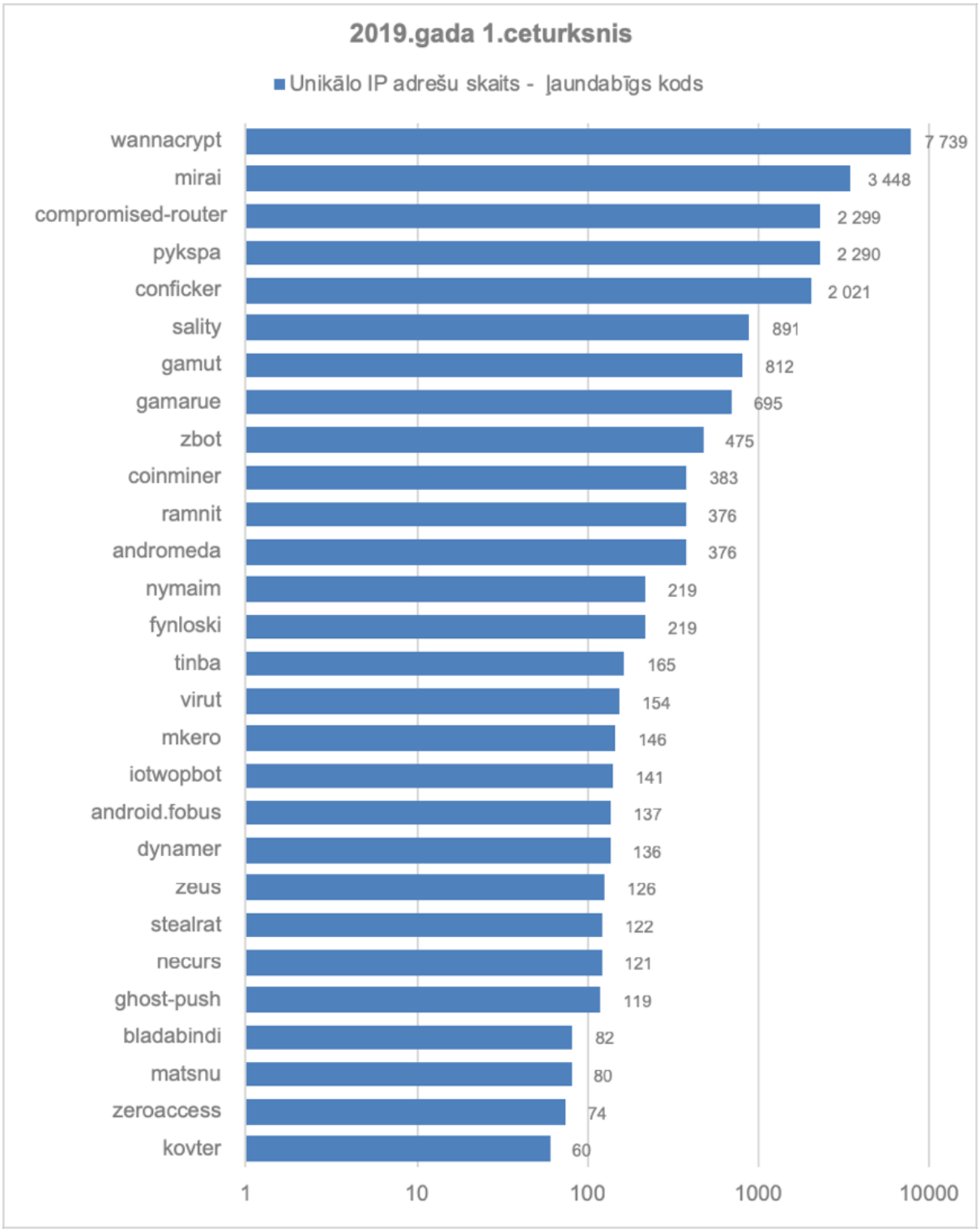


2.attēls – CERT.LV reģistrētās apdraudētās IP adreses pa ceturkšņiem 2018. un 2019. gadā.



3.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2019. gada 1. ceturksnī pa apdraudējumu veidiem.

Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (137 209 unikālas IP adreses) ar pieaugumu 4% pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs kods (19 859 unikālas IP adreses) ar kritumu 17%, bet trešais - ielaušanās mēģinājumi (2436 unikālas IP adreses) ar kritumu 2%.



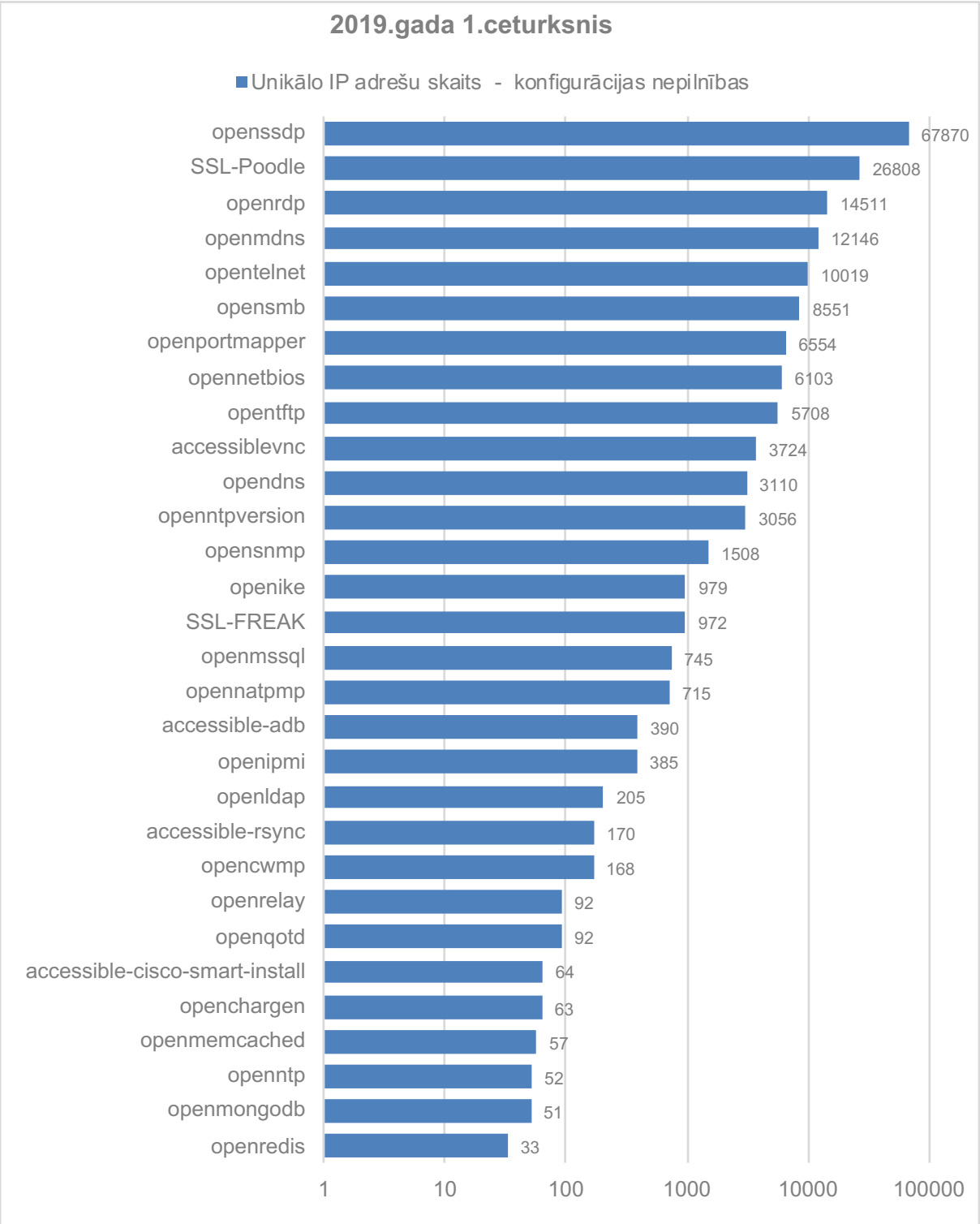
4.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2019. gada 1. ceturksnī ar apdraudējuma veidu - Ļaundabīgs kods.

Pirmo vietu Ļaunatūras izplatības topā šajā ceturksnī stabili ieņem Ļaunatūra *WannaCry* (*WannaCrypt*), kas ir šifrējošais izspiedējvīruss, un, nonākot upura iekārtā, tā nošifrē iekārtas saturu, pieprasot samaksu par datu atgūšanu.

Otro 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.

Topa trešajā vietā atrodas kompromitēti maršrutētāji (*routers*), kas nesalaboti, esot trešo

pušu kontrolē, var tikt izmantoti pretlikumīgām darbībām, piemēram, uzbrukumiem citām iekārtām vai datortīkliem.



5.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2019. gada 1. 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.

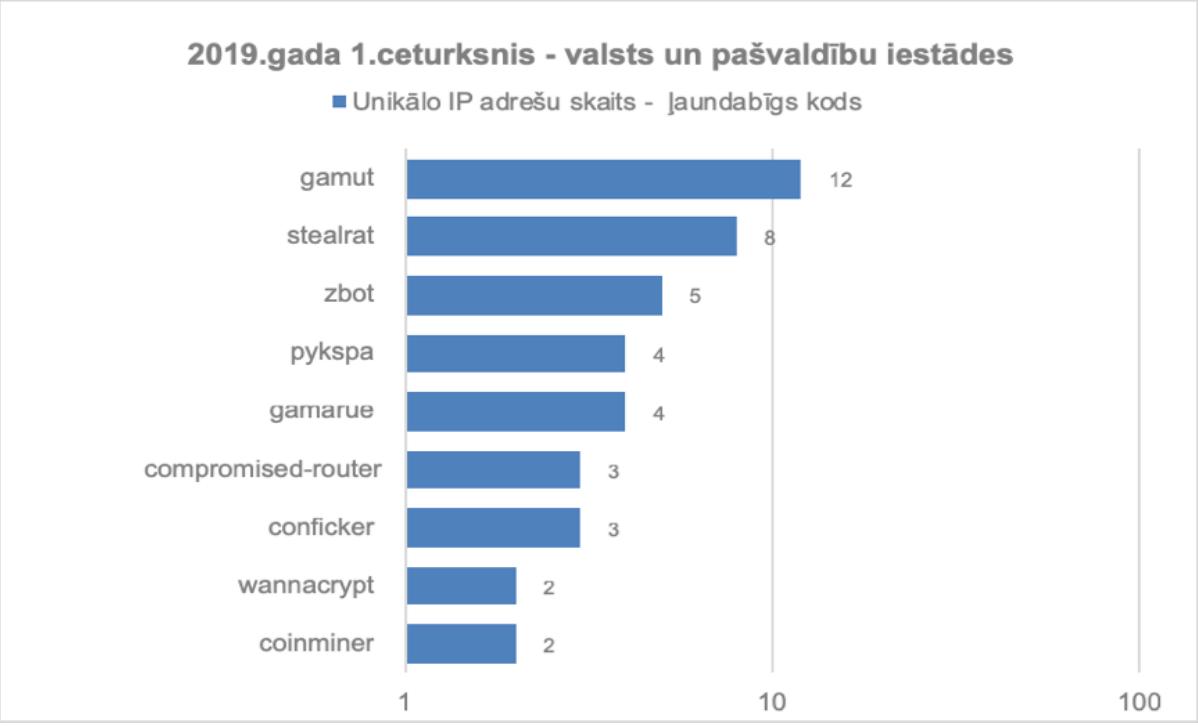
Trešajā vietā esošā konfigurācijas nepilnība *OpenRDP* pārskata periodā bija saistīta ar iekārtu un datu nesēju nošifrēšanu. Trešās puses bija piekļuvušas neatbilstoši konfigurētām iekārtām, kurās attālinātās piekļuves porti bija brīvi atvērti uz internetu un tām nebija pietiekami droša vai vispār nebija 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.

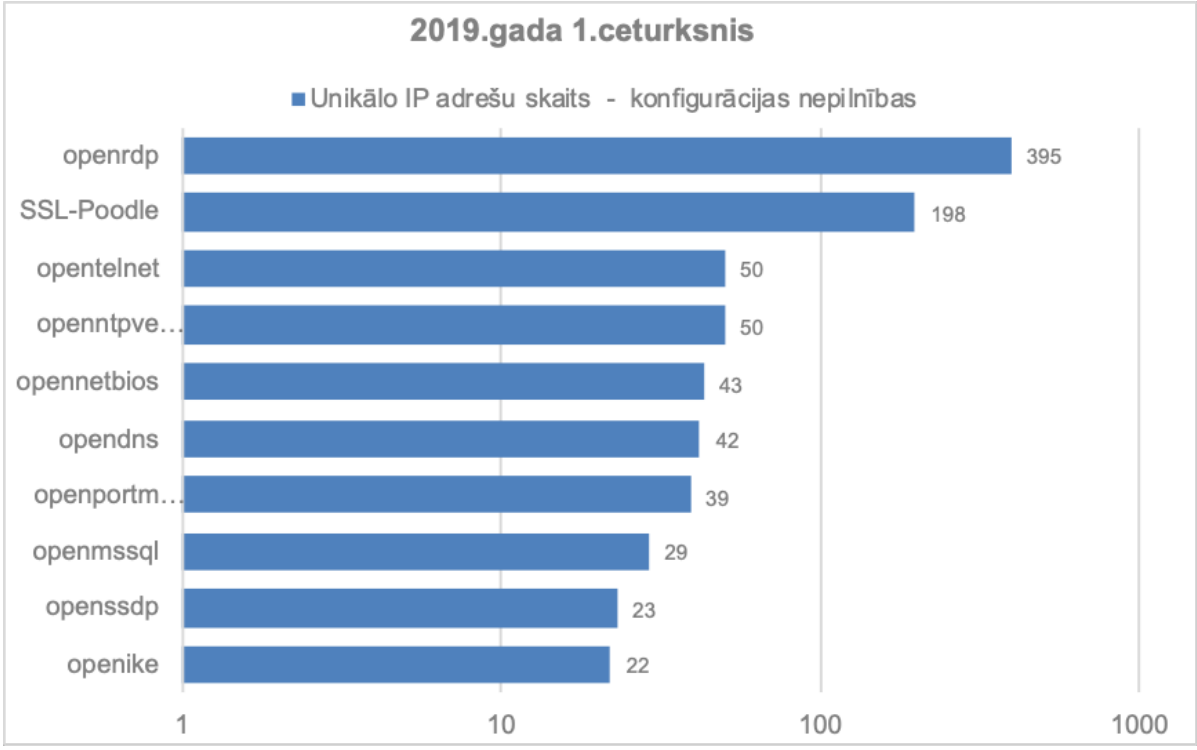
2. Atbalsts informācijas tehnoloģiju drošības incidentu novēršanā vai to novēršanas koordinēšanā.

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.

Vidējais apdraudēto valsts un pašvaldību iestāžu IP adrešu daudzums katras dienas saņemtajos ziņojumos pārskata periodā bija 400 unikālas IP adreses dienā.

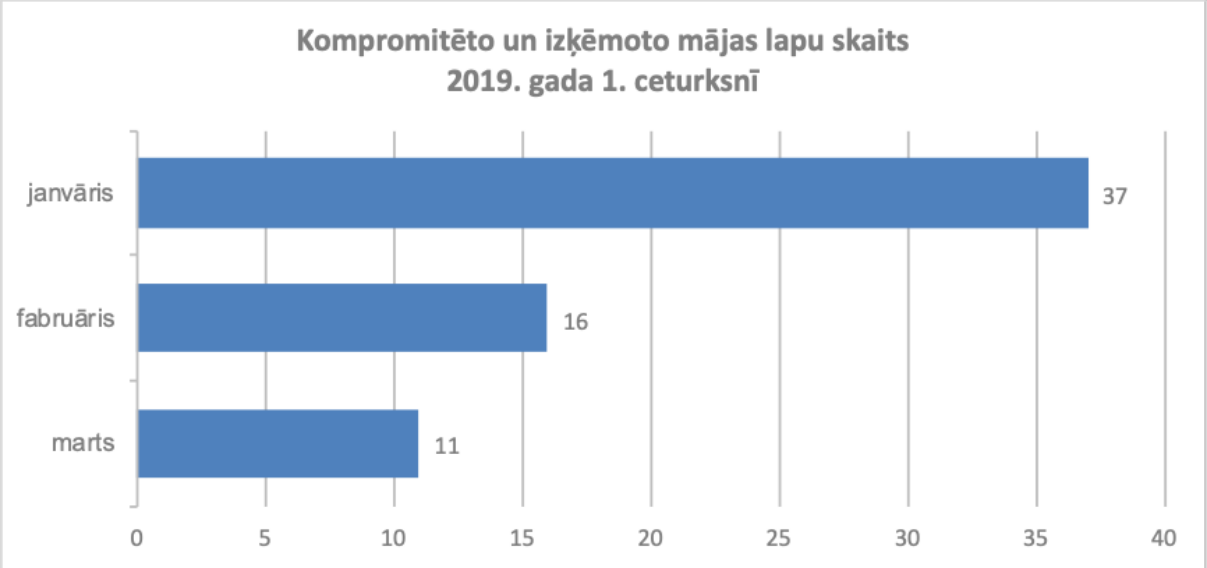


6.attēls - CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2019.gada 1.ceturksnī ar apdraudējuma veidu – Ļaundabīgs kods.



7.attēls - CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2019.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 fiksētas 64 kompromitētas un izķēmotas tīmekļa vietnes. Sešdesmit divos gadījumos izķēmotās vietnes uzturēšanai tika izmantota Linux operētājsistēma, bet divos gadījumos - FreeBSD. Šajā pārskata periodā neviens no izķēmošanas gadījumiem nav tāds, kas pēdējā gada laikā būtu noticis atkārtoti.



8.attēls – Kompromitēto un izķēmoto tīmekļa vietņu skaits pa mēnešiem 2019. gada 1. 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

Tika saņemts ziņojums par piekļuves lieguma (DDoS) uzbrukumu Slovēnijas WHOIS serverim no Latvijas IP adresēm. Veicot incidenta analīzi, tika konstatēts, ka uzbrukumā iesaistītās IP adreses saistītas ar kompromitētiem maršrutētājiem un citām mājas iekārtām. Informācija nodota atbildīgajiem interneta pakalpojumu sniedzējiem, kas tālāk apzināja atbilstošos gala lietotājus.

Tika saņemts ziņojums par kādas iestādes meklētāja pakalpojuma atteices uzbrukumu, kas panāca pakalpojuma pārslodzi vairāk kā 6h garumā. Tika secināts, ka pieprasījumi vietnes meklētājam tika veikti ne no Latvijas IP adresēm, un tie bija izkliedēti. CERT.LV rekomendēja papildu pārbaužu ieviešanu robotu nošķiršanai no leģitīmiem apmeklētājiem, piemēram, izmantojot CAPCHA.

Tika saņemts ziņojums par publiski pieejamu NTP serveri ar Latvijas IP adresi, kas atkārtoti iesaistīts liela mēroga DDoS uzbrukumā. Šis ir ilustratīvs piemērs tiem daudzajiem gadījumiem, kad iekārtu īpašnieki ignorē labo praksi un vieglprātīgi izturas pret iekārtas konfigurāciju un iestatījumiem, kā rezultātā šīs iekārtas tiek izmantotas, lai uzbruktu citiem.

Tika saņemts ziņojums par iespējamu uzbrukumu VID EDS sistēmai, bet izpētes rezultātā tika konstatēts, ka DDoS situācija ir radusies dabīgā ceļā, jo, stājoties spēkā nodokļu reformai, iedzīvotāji vēlējās noskaidrot, vai viņiem ir izveidojies nodokļu parāds un kāds ir tā apjoms.

Tika saņemts ziņojums par DDoS uzbrukumu kādas iestādes tīmekļa vietnei. Veicot incidenta analīzi, tika secināts, ka uzbrukumā izmantotas iekārtas, kurām bija aktīva atvērtā proxy funkcionalitāte, kas norāda uz iekārtu ar neatbilstošu konfigurāciju vai tādu iekārtu, kas satur ievainojamības. Abos gadījumos neautorizēta trešā puse spēja piekļūt iekārtai un izmantot to saviem mērķiem. CERT.LV sniedza konsultāciju DDoS aizsardzības ieviešanā.

Tika saņemti ziņojumi par traucējumiem Swedbank bankas pakalpojumu darbībā. Efektīvas sadarbības rezultātā CERT.LV apstiprināja, iegūtā informācija liecināja par tehniskas dabas kļūmi sistēmā, kuru Swedbank ekspertiem izdevās operatīvi novērst. CERT.LV nekonstatēja ļaunprātīgu ārēju ietekmi.

Tika saņemts ziņojums no kādas tirdzniecības vietnes uzturētājiem par automatizētiem mēģinājumiem pārslogot vietni ar visdažādākajiem pieprasījumiem. Pieprasījumi tika veikti, izmantojot TOR anonimizācijas tīkla serveri.

Pikšķerēšana jeb personīgo datu izkrāpšana

Tika saņemts ziņojums par e-pasta datu izkrāpšanas mēģinājumu, nosūtot krāpniecisku e-pastu e-pasta uzturētāja vārdā ar aicinājumu sekot saitei, lai atjauninātu pakalpojumu un iegūtu piekļuvi ienākošajām ziņām, kas ir tikušas aizturētas.

Fiksēts arī mēģinājums izkrāpt e-pasta piekļuves datus, norādot, ka konkrētā e-pasta paroles derīguma termiņš beigsies pēc trīs dienām un jāseko e-pastā norādītajai saitei, lai atjauninātu iestatījumus un nodrošinātu veiksmīgu autorizāciju arī nākotnē. Citā variantā tika dotas 48 stundas no konkrētās autorizācijas brīža, lai sekotu saitei un nokļūtu administratīvajā portālā, kur veicami nepieciešamie sistēmas atjauninājumi, pretējā gadījumā zaudējot iespēju saņemt ziņojumus.

Tika saņemta informācija par mēģinājumiem izkrāpt e-pasta piekļuves datus no valsts un pašvaldību institūciju darbiniekiem, aicinot atjaunināt e-pasta klientu uz jaunāko Microsoft Outlook 2019 versiju, sekojot saitei.

Saņemts arī ziņojums par e-pasta piekļuves izkrāpšanas mēģinājumu ar tehniska izskata e-pastu, kas lietotājam rada iespaidu, ka tas ir automātiski sagatavots ziņojums par kļūdu e-pasta piegādē, kuru iespējams atrisināt, veicot atkārtotu autorizāciju norādītajā saitē, lai saņemtu 5 nepiegādātās ziņas.

E-pasta piekļuves izkrāpšanai izmantots arī brīdinājuma e-pasts par trešās puses mēģinājumiem piekļūt e-pasta kontam, kā rezultātā iespējama konta deaktivācija. To apturēt iespējams, veicot autorizāciju norādītajā saitē. Saņemts arī ziņojums par e-pasta piekļuves izkrāpšanas mēģinājumu, atsūtot brīdinājumu, ka e-pasta adrese iekļauta melnajā sarakstā (*blacklist*) par spamošanu un tiks neatgriezeniski slēgta, ja nenotiks konta verifikācija, sekojot saitei.

Tika saņemts ziņojums arī par e-pasta piekļuves izkrāpšanas mēģinājumu, izmantojot paziņojumu par dokumentiem, ko kāds ir koplietojis ar saņēmēju. Tiek norādīts, ka koplietotie dokumenti tiks dzēsti dažu dienu laikā. Lai tos lejuplādētu, aicināts sekot saitei.

Tika saņemts ziņojums par Google piekļuves datu izkrāpšanas mēģinājumu, izmantojot e-pastu ar saiti uz pikšķerēšanas vietni.

Tika saņemts ziņojums par mēģinājumu izkrāpt personas datus (vārds, uzvārds, pilsonība, kontaktinformācija, ģimenes stāvoklis, vecums, darba vieta, nodarbošanās) - ar paziņojumu par laimestu Powerball vai Jackpot loterijā. Laimesta saņemšanai tika lūgts datus nosūtīt e-pastā. Līdzīga informācija par laimestu loterijā ar lielu naudas summas tika izplatīta arī Facebook vārdā, pieprasot personas datus.

Tika saņemta informācija par e-pastu it kā Starptautiskā Valūtas fonda vārdā, kas saņēmējam sola kompensāciju par krāpšanā piedzīvotajiem zaudējumiem. Kompensācijas iegūšanai lūgts nosūtīt personas datus un pases kopiju.

Tika saņemts ziņojums par Intara Busuļa Instagram konta uzlaušanu. E-pastā tika saņemts viltots paziņojums par konta verificēšanu un īpašā, apstiprinātā statusa piešķiršanu. Lai saņemtu piešķirto atšķirības zīmi, tika izteikts aicinājums sekot saitei un autorizēties kontā, kas arī tika izdarīts, neatgriezeniski zaudējot konta piekļuves datus.

Tika saņemts ziņojums par krāpniecisku e-pastu, kurā tiek norādīts maksājumu kartes numurs un norādīta summa, kura ir tikusi noskaitīta no kartes, kā arī atlikums, kuru e-pasta saņēmējs var pārskaitīt, ja seko saitei. E-pasts domāts maksājumu kartes datu izkrāpšanai.

Tika saņemti vairāki ziņojumi par e-pastiem it kā SEB un Citadele banku vārdā, kuros saņēmējs tiek informēts par saņemtu tiešsaistes ziņu un ir aicināts autorizēties, sekojot saitei. Saite norādīja uz bankas piekļuves datu izkrāpšanas vietni.

Tika saņemts ziņojums par UPS piekļuves datu izkrāpšanas mēģinājumu, nosūtot e-pastu ar paziņojumu par konfidenciālu informāciju saturošu sūtījumu, par kuru papildinformāciju var iegūt, sekojot saitei.

Tika saņemts ziņojums par e-pastu, kas, izmantojot viltotu e-pasta adresi, no Krievijā bāzētiem serveriem Latvijas Republikas aizsardzības ministra Arta Pabrika vārdā izsūtīts uz vairākiem adresātiem Latvijas valsts iestādēs ar nepatiesu un kompromitējošu saturu. E-pasts saturēja skriptu, kas, e-pastu atverot, ievāca informāciju par saņēmēju.

Tika saņemta informācija par vairākām uzlauztām .lv vietnēm un Latvijas IP adresēm, kurās tika izvietota pikšķerēšana, kas vērsta uz Apple, Barclays bankas, Nets, Amazon, bet galvenokārt Netfix klientiem.

Krāpšana

Gada sākumā tika saņemts ziņojums par aizdomīgām Facebook reklāmām, kuru galamērķis vairāku dienu garumā bija praktiski identiska izskata vietnes, bet ar atšķirīgiem domēna vārdiem, kas visi reģistrēti neilgu laiku. Vietņu mērķis bija ievākt personu un maksājumu karšu datus, kā arī, iespējams, izkrāpt maksājumus par precēm, kas netiktu piegādātas.

Tika saņemti vairākkārtēji ziņojumi par krāpniecisku loteriju populāru interneta pakalpojumu sniedzēju vārdā. Loterija piedāvāja iespēju iegūt Samsung Galaxy S9, iPhone XS vai iPad Air2, ja tiks atbildēts uz dažiem vienkāršiem jautājumiem. Balvas iegūšanai jānorāda telefona numurs. Lapā izvietota nemanāma atruna, ka šī ir maksas pakalpojuma – spēļu - abonēšana ar pakalpojuma cenu 29 eiro mēnesī. Līdzīgas loterijas tika publicētas arī Google Chrome un Firefox vārdā.

Tika saņemti 11 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. Kā pierādījumu apgalvojumu patiesumam uzbrucējs dažos gadījumos norādīja, ka zina upura paroli, bet dažos gadījumos viltota izsūtītāja adrese, norādot to vienādu ar saņēmēja e-pasta adresi. CERT.LV 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.

Tika saņemta informācija no VAS “Latvijas pasts” par uzņēmuma vārdā izplatītiem naudas izkrāpšanas e-pastiem un SMS ar informāciju par laimētu iPhone XS, kura saņemšanai jāapmaksā sūtīšanas izdevumi.

Tika saņemts ziņojums par zvanu no kāda Igaunijas numura, kurā runātājs krievu valodā aktīvi piedāvāja nopelnīt, izmantojot datoru, bet, kad zvana saņēmējs sāka uzdot jautājumus, zvanu pārtrauca. Šādi zvani raksturīgi mēģinājumiem iesaistīt darījumos augsta riska finanšu instrumentu tirdzniecības platformās, kas nav licencētas investīciju piesaistei Latvijā.

Tika saņemts ziņojums par SMS no sveša numura, kurā paziņots par naudas pārvedumu un norādīta saite, kurai jāseko, lai pabeigtu transakciju. Saite veda uz maksājumu karšu izkrāpšanas vietni.

Aktualizējušies krāpnieciskie telefona zvani, kuros zvanītāji sāk ar piedāvājumu par nelielu samaksu nopelnīt akciju tirgos. Tālāk viņi pāriet uz Skype sesiju un beigās aicina instalēt ekrāna koplietošanas rīku, lai krāpnieku vadībā iegādātos kriptovalūtu, kuru investētu nelicenzētā finanšu tirdzniecības platformā un zaudētu.

Tika saņemts ziņojums no kāda Latvijas uzņēmuma par krāpniecību, kas vērsta pret uzņēmuma meitas uzņēmumu Igaunijā, cenšoties izkrāpt maksājumu ar e-pastu vadītāja vārdā. E-pasta adrese bija izveidota tīmekļa vietnē www.inbox.lv, un tā pat nav bijusi īpaši pielāgota.

Tika saņemts ziņojums no kāda ārvalstu uzņēmuma par krāpniecības mēģinājumu, kurā no inbox.lv e-pasta adreses uzņēmuma darbiniekiem vadītāja vārdā tika izsūtīts e-pasts ar lūgumu palīdzēt, jo ir steidzams jautājums, kas jāatrisina, bet vadītājs atrodas sanāksmē.

Viens no darbiniekiem bija atsaucies un saņēmis aicinājumu veikt iegādi Google play dāvanu kartēm, kuras būs nepieciešams nosūtīt sadarbības partneriem. Darbinieks krāpniecību laicīgi atpazina.

Tika saņemta informācija no kādas iestādes par mēģinājumu izkrāpt maksājumu 14 980 eiro apmērā pārskaitījumam uz Lielbritāniju, nosūtot grāmatvedei e-pastu it kā vadītāja vārdā.

Tika saņemts ziņojums par e-pastu it kā Norvēģijas starptautiskās kompānijas Statoil valdes locekļa Jeroen van der Veer vārdā ar glaimojošu sadarbības piedāvājumu, kas slēpj aicinājumu iesaistīties naudas atmazgāšanas shēmā, kurā pirms tam jāiegulda arī sava nauda.

Ielaušanās mēģinājumi

Tika saņemts ziņojums no kādas valsts iestādes par intensīvu masveida mēģinājumu piekļūt iestādes IP adresei no IP adreses Krievijas federācijā. Tika veikti TCP pieprasījumi, kas, lai arī intensīvi, neradīja ietekmi uz izvēlēto mērķa servisu.

Tika saņemts ziņojums no Slovākijas CERT vienības par automatizētu uzbrukumu Slovākijas universitātes e-pasta serverim no Latvijas IP adresēm. Uzbrukumā iesaistīti kompromitēti maršrutētāji vai citas iekārtas. Iekārtu turētāji tika apzināti caur "Atbildīgs interneta pakalpojumu sniedzējs" programmu.

Tika saņemts ziņojums par ļaundabīgām aktivitātēm, kas vērstas pret Krievijas federācijas valsts pārvaldes informācijas tehnoloģiju un telekomunikāciju tīklu no Latvijas IP adreses. Apdraudējums tika novērsts.

Tika saņemts ziņojums no kādas valsts iestādes par mēģinājumu vairāku dienu garumā pieslēgties un izsūtīt e-pastus no iestādes domēna. Izmantotas gan eksistējošas lietotāju e-pasta adreses, gan ģenerētas. Uzbrukumi traucējumus neradīja, e-pasta vēstules līdz lietotājiem nenonāca.

Tika saņemts ziņojums par masveida ielaušanās mēģinājumiem kādas pašvaldības e-pasta kastītei. Uzbrukumi veikti no dažādām IP adresēm apmēram reizi 1,5 minūtēs divi pieslēgšanās mēģinājumi no vienas IP adreses, kas katru reizi mainās.

Ļaunatūra

Tika saņemti vairāki ziņojumi par ļaundabīgu failu izvietošanu serveros ar Latvijas IP adresēm. Serveru uzturētāji tika apzināti. Ļaundabīgais saturs tika dzēsts.

Tika saņemts ziņojums par vairākkārtējiem e-pasta sūtījumiem, kas uzdodas par biznesa sadarbības piedāvājumu Europower Components Ltd vārdā un aicina aplūkot pielikumā esošo pasūtījumu, lai precizētu sūtījuma apjomu, bet atvēršanas rezultātā nodrošinātu vīrusa Heur lejupielādi iekārtā.

Tika saņemts ziņojums no kāda uzņēmuma par kompromitētu IT infrastruktūru – nošifrētiem vairākiem servera diskiem, izmantojot BitLocker šifrējošo izspiedējvīrusu. Biznesam kritiskos datus uzņēmumam izdevās atjaunot no datu rezerves kopijām, izņemot vienu koplietojamo disku, kas saturēja būtisku finanšu un mārketinga informāciju. Izspiedēji pieprasīja izpirkuma maksu 2 BTC apmērā par viena servera satura atgūšanu. Uzņēmums vērsās ar iesniegumu policijā.

Tika saņemts ziņojums no kāda uzņēmuma par nošifrētu darbstaciju, kā arī bojātu grāmatvedības datu bāzi tīkla diskā. Šifrējošais izspiedējvīruss Wdharma sistēmā nonācis, uzbrucējam piemeklējot paroli. Uzņēmumam datus atjaunot izdevās tikai daļēji.

Tika saņemts ziņojums par neautorizētu maksājumu karšu datu ieguves kodu kādā tiešsaistes tirdzniecības vietnē, lai arī vietnē ir atruna, ka maksājumi ar kartēm netiek pieņemti. Vietnes uzturētāji informēti un aicināti kaitīgo kodu izņemt, kā arī pārbaudīt un atjaunot vietnes CMS un tās spraudņu versijas.

Tika saņemts ziņojums no kādas iestādes par incidentu ar iestādes vietnē ievietoto reklāmas baneri, kurā līdzās oriģinālajam saturam vērās vaļā arī azartspēļu totalizatoru vietņu reklāmas. Uz izmeklēšanas laiku baneru mašīnas kods tika izņemts no tīmekļa vietnes.

Tika saņemts ziņojums no kādas viesnīcas par šifrējošā izspiedējvīrusa Nemesis uzbrukumu. Neskarti palikuši tikai viesnīcas rezervācijas dati. Izdevās atjaunot e-pastus, par pārējo datu atgūšanas veiksmīgumu ziņu nav.

Kompromitētas iekārtas

Tika saņemts ziņojums par kompromitētu kādas pašvaldības e-pasta kontu, no kura tika izsūtītas krāpnieciskas e-pasta vēstules. Uzlauztais konts tika salabots.

Tika saņemti vairāki ziņojumi par kompromitētām iekārtām ar Latvijas IP adresēm, kuras iesaistītas uzbrukumos citiem datortīkliem. Iekārtu uzturētāji brīdināti.

Tika saņemts ziņojums par SPAM e-pastu izsūtīšanu no kādas iestādes e-pasta adreses. Sazinoties ar iestādes par IT drošību atbildīgo, tika konstatēts, ka ir ticis atvērts kāds no SPAM e-pastiem, kas acīmredzamas sekas nav radījis, kā rezultātā lietotājs nav problēmu piefiksējis. Papildus lietotājs ir ļāvis veikt paroļu saglabāšanu interneta pārlūkā. Problēma tika novērsta, kā arī veiktas izglītojoši skaidrojošas aktivitātes.

Tika saņemts iesniegums par kompromitētu Gmail un Facebook lietotāja kontu. Operatīvo darbību veikšanai sniegts ieteikums vērsties policijā un iespējot divu faktoru autentifikācijas iespējas.

Tika saņemts ziņojums no kādas izglītības iestādes par neautorizētu attālinātu pieslēgšanos iestādes datoram. Pēc CERT.LV ieteikuma darbstacija tika pārbaudīta ar antivīrusa programmatūru, kā arī nomainītas datorā izmantotās lietotāju kontu paroles.

Saņemts ziņojums par incidentu kādas valsts iestādes tīmekļa vietnē. Vietnē tika publicēta ziņa ar saiti uz ārēju skriptu, kas tika noteikts kā kaitīgs. Uzsākta pārbaude, kā arī notiek aktīva komunikācija ar vietnes CMS izstrādātājiem, lai veiktu koda pārbaudi. Identisks nevēlams skripts konstatēts arī citā vietnē. CERT.LV lūdza informēt par datora pārbaudes rezultātiem un atsūtīt attiecīgā datuma vietnes piekļuves žurnālfailus.

Atbildīga ievainojamību atklāšana

Pārskata periodā atbildīgas ievainojamību atklāšanas ietvaros tika saņemts ziņojums par kādu valsts iestādes tīmekļa vietni, kas tiek uzturēta uz ievainojamas Nginx servera versijas. Ievainojamība radīja pārmērīgas CPU noslodzes vai pārmērīga atmiņas patēriņa draudus.

Tika saņemti 3 ziņojumi par starpvietņu skriptēšanas (XSS) ievainojamībām. 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.

Ievainojamības un konfigurācijas nepilnības

Tika saņemta informācija, ka kādas iestādes darbinieki ir saņēmuši e-pastus paši no sevis. CERT.LV sazinājās ar iestādi, lai informētu par pastāvošo apdraudējumu – iespēju viltot kolēģu e-pastus un nosūtīt ārpuses darbiniekiem vizuāli ticamus e-pastus ar bīstamu saturu. Tika ieteikts ieviest DMARC - Domain-based Message Authentication, Reporting & Conformance (iekļaujot SPF un DKIM) tehnoloģiju vm.gov.lv e-pasta serverī, kas liegtu lietotājiem saņemt šādas viltotas e-pasta vēstules un vairākas citas SPAM vēstules kopumā.

Kādas iestādes tīmekļa vietnē tika konstatēts uz āru eksponēts nedrošs fails, paverot jaunu vektoru uzbrukumam. Vietnes uzturētāji tika informēti, fails tika dzēsts.

Tika konstatētas vairākas drošības nepilnības kādā Latvijas vietnē. Viena no būtiskajām nepilnībām ļāva vairākkārtēji izmantot autentifikācijas drošības marķierus – lietotājs, sekmīgi autorizējoties vietnē, tos pašus autentifikācijas drošības marķierus var izmantot atkal un ielogoties citā pārlūkā/ datorā, apejot bankas autentificēšanās procedūru. Uzturētāji tika informēti

CERT.LV pasākumi incidentu novēršanā:

- CERT.LV veica ielaušanās drošības testus 4 valsts un pašvaldību iestāžu tīmekļa vietnēs.
- 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 4. punktā.

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

Janvārī CERT.LV pārstāvis kopā ar NIC.lv tikās ar Latvijas Tirdzniecības un rūpniecības kameras pārstāvjiem, lai pārrunātu iespēju rīkot informatīvi izglītojošu semināru mazajiem un vidējiem uzņēmējiem par aktuālajiem kiberdrošības jautājumiem.

Janvāra beigās CERT.LV sadarbībā ar Eiropas Komisijas pārstāvniecību Latvijā sagatavoja jautājumu LTV1 jauniešu izglītojošajam raidījumam „Gudrs, vēl gudrāks".

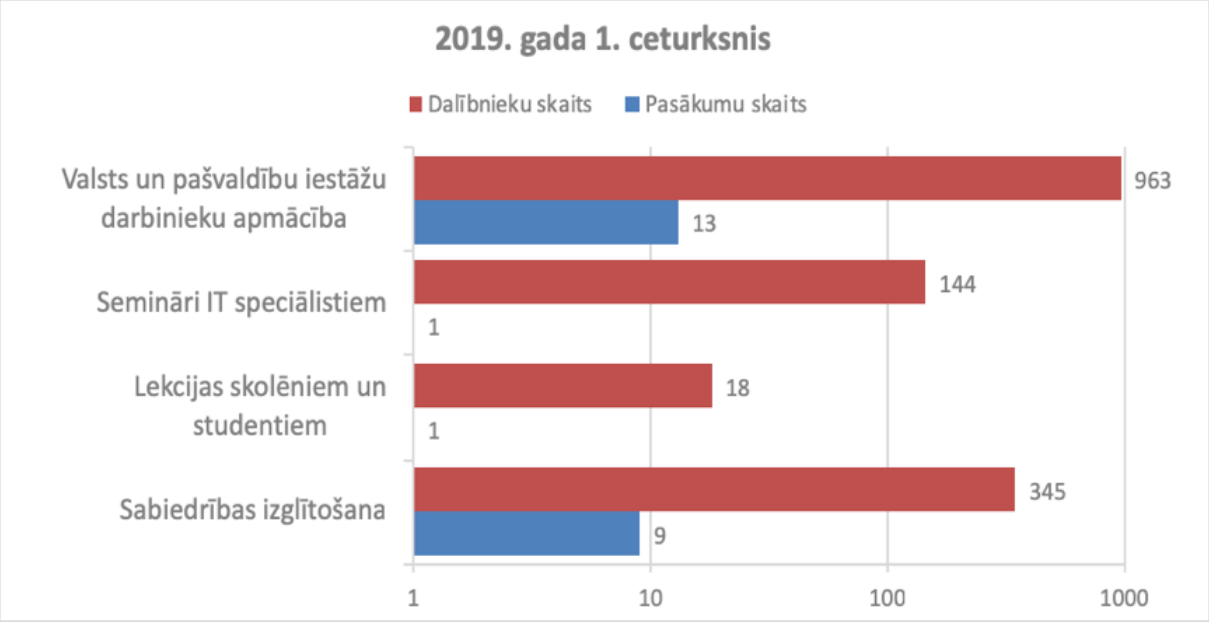
12. februārī jaunuzņēmumu akselerators Startup Wise Guys organizēja pasākumu „CyberNorth Warm Up", kurā CERT.LV pārstāvis piedalījās paneļdiskusijā par kiberuzbrukumiem, kā arī iesaistījās žūrijā un vērtēja uz kiberdrošību orientēto jaunuzņēmumu prezentācijas.

28.martā CERT.LV piedalījās LVRTC organizētajā pasākumā „Kibernakts 2019", kas notika Eiropas Digitālās nedēļas ietvaros. Pasākums tika organizēts ekspertu diskusijas formā ar mērķi paplašināt gan nozares speciālistu, gan sabiedrības izpratni par kibertelpu, digitālo higiēnu, elektroniski identitāti, tās nozīmi un aizsardzību.

CERT.LV pārstāvis 28.martā piedalījās arī LVRTC organizētajā e-Identitātes dienā, un sniedza prezentāciju „Identitātes zādzība. Vai varam nosargāt virtuālu identitāti?".

28.martā Digitālās nedēļas ietvaros CERT.LV organizēja semināru „Esi drošs", kas paredzēts galvenokārt valsts un pašvaldību iestāžu par IT drošību atbildīgajiem, un aplūkoja tādas tēmas kā DNS over HTTPS, tīmekļa lietojumu drošība, mobilo iekārtu droša izmantošana valsts un pašvaldību iestādēs. Notika arī aktīva paneļdiskusija par e-adreses ieviešanu un izaicinājumiem.

Pārskata periodā CERT.LV par IT drošību izglītoja 1470 cilvēkus, iesaistoties 24 izglītojošos pasākumos.



9.attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2019. gada 1. ceturksnī

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

Sadarbības tikšanās, konsultācijas un prezentācijas:

- CERT.LV piedalījās Eiropas Parlamenta vēlēšanu darba grupas sanāksmēs, lai gatavotos maijā gaidāmajām vēlēšanām.
- CERT.LV piedalījās Aizsardzības ministrijas sanāksmē ar nozaru ministrijām par pamata pakalpojumu sniedzēju identifikāciju atbilstoši NIS direktīvai.

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 attālinātās sanāksmēs un organizējot TF-CSIRT darbu.
- Pārskata periodā CERT.LV pārstāvji piedalījās NATO CCDCoE kiberdrošības mācību "Locked Shields 2019" sagatavošanās procesā gan zilās (aizstāvošās) komandas sastāvā, gan sarkanās (uzbrūkošās) komandas, kā arī organizatoru rindās.

- 17. janvārī CERT.LV Aizsardzības ministrijā tikās ar Ukrainas vēstniecības pārstāvjiem, lai pārrunātu iespējamo sadarbību.
- 21. janvārī CERT.LV pārstāvis tikās ar Hārvardas universitātes studentiem, lai sniegtu atbalstu pētījumā par Baltijas valstu vēlēšanu procesu kiberdrošību un informācijas drošību.
- 21.-25. janvārī notika TF-CSIRT & FIRST simpozijs Tallinā, Igaunijā, kurā CERT.LV pārstāvis uzstājās ar prezentāciju "Beyond paste monitoring: deep information leak analysis".
- No 28.janvāra līdz2.februārim CERT.LV pārstāvji piedalījās ikgadējās tehniskajās kiberdrošības mācībās "Crossed Swords 2019", kas tapa, sadarbojoties NATO CCDCoE un CERT.LV, un notika Tallinā, Igaunijā. Mācību galvenā uzmanība tika vērsta uz sarkanā karoga komandu ofensīvo prasmju attīstību kiberoperāciju plānošanā, izpildē un reaģēšanā uz apdraudējumu. Mācībās piedalījās vairāk nekā 100 dalībnieki no 21 valsts.
- 09.-14. februārī CERT.LV pārstāvji piedalījās „NIS CSIRT network" sanāksmē Briselē.
- 22. februārī CERT.LV pārstāvis tikās ar Frenchtech jaunuzņēmumu inkubatora direktori, lai pārrunātu potenciālo sadarbību tehniski orientētu jaunuzņēmumu ideju apmaiņā.
- 22.-27. februārī Čehijā CERT.LV pārstāvis piedalījās akadēmiskajā konferencē ICISSP2019 ar publikācijas prezentāciju "Remote Exploit Development for Cyber Red Team Computer Network Operations Targeting Industrial Control Systems".
- 25.-27. martā CERT.LV pārstāvis pasniedza NATO CCDCoE „Cyber Executive Seminar" kursu Tallinā, Igaunijā.

Sadarbība konkrētu incidentu risināšanā aplūkota pārskata 2. punktā.

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

2018. gada 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 turpināta arī "Deep Analysis System" izstrāde un pielāgošanas darbi.

Projektā paredzēts īstenot sabiedrību informējošas kampaņas un pasākumus, lai veicinātu iedzīvotāju izpratni un uzlabotu zināšanas par kiberdrošību - regulāri norisinās informatīvi un izglītojoši semināri visā Latvijā, tiek plānota lielāka apjoma kampaņu rīkošana, notika informatīvais seminārs "Esi drošs!".

2019.gadā projekta ietvaros tiks rīkoti vairāki tehnikas iepirkumi, notiek specifikāciju sagatavošana šiem iepirkumiem.

7. Projekta ‘‘Cyber Exchange’’ īstenošana

2018. gada 1.novembrī CERT.LV ir uzsākusi 2017 CEF Telecom-Cyber Security uzsaukumā apstiprinātā projekta “Cyber Exchange” (līguma ar Eiropas Komisiju Nr. INEA/CEF/ICT/A2017/1528866) (turpmāk – Sadarbības projekts) īstenošanu.

Projekta mērķis ir stiprināt starptautisku sadarbību starp nacionālajām un valdības CSIRT/CERT organizācijām. CyberExchange projekts ir kā atbilde arvien pieaugošajiem draudiem kiberdrošības jomā, īpašu akcentu vēršot uz nepieciešamo pārrobežu sadarbību cīņā pret tiem. Latvija ir viena no 10 Eiropas valstīm, kas piedalās projektā. 2019. gada 1. ceturksnī aktīvi notika gatavošanās maijā plānotajai kiberapmaiņas vizītei, kad Latvijā viesosies kolēģi no Horvātijas.

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 ietvaros ir bijuši jau vairāki gadījumi, kuros nostrādājusi aktīvā aizsardzība, pasargājot iekārtas no inficēšanas. Daļu no DNS PRZ pakalpojuma var izmantot arī bez līguma slēgšanas un autorizēšanās jebkurš interneta lietotājs. Lai to izmantotu, jālieto NIC.lv rekursīvie DNS serveri.
- 13. februārī CERT.LV piedalījās “Ēnu dienas” projektā un uzņēma ēnotājus, lai iepazīstinātu topošos profesionāļus ar nozari un palīdzētu veikt sev atbilstošu, jēgpilnu karjeras izvēli.
- 27. martā CERT.LV tikās ar Vidzemes augstskolas pārstāvi, lai apspriestu iespējas, kā atbalstīt kiberdrošības maģistra programmu.
- 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 Elektronisko dokumentu likuma grozījumu izstrādē.

9. Papildu pasākumu veikšana.

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

Latvijas Interneta asociācijas Drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.01.2019. līdz 31.03.2019. ir saņēmusi un izvērtējusi 346 ziņojumus. No tiem 147 ziņojumu saturā ir konstatēti materiāli par bērnu seksuālu izmantošanu , 25 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 31 ziņojumā konstatēta personas goda un cieņas aizskaršana, 4 ziņojumi saņemti par naida runu un 2 ziņojumi par vardarbību atainojošiem materiāliem. Par finanšu krāpšanas mēģinājumiem internetā saņemti 36 ziņojumi, 36 ziņojumu saturs nav bijis pretlikumīgs, bet 65 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 80 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā un 1 par narkotiku tirdzniecību. 64 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.

Pārskata periodā no Latvijā uzturētajiem 147 ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem 131 ziņojums ir dzēsts no publiskas aprites un 16 ziņojumu saturs atrodas dzēšanas procesā sadarbībā ar Valsts policiju un interneta pakalpojumu sniedzējiem.

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