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 3. ceturksnis (01.07.2018. – 30.09.2018.)

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 3.ceturksnī CERT.LV apkopoja informāciju par 193 669 apdraudētām IP adresēm. Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (142 687 unikālas IP adreses) ar pieaugumu 5% pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs kods (30 641 unikāla IP adrese) ar kritumu 9%, bet trešais - ielaušanās mēģinājumi (2579 unikālas IP adreses) ar pieaugumu 131%.

Kāpums ielaušanās mēģinājumu apjomā skaidrojams ar inficētiem MikroTik maršrutētājiem un citām iekārtām, kuras iekļautas robotu tīklos un veic automatizētus uzbrukumus, lai šos tīklus paplašinātu. Inficēto iekārtu apjoma mazināšanai CERT.LV veica iekārtu īpašnieku apziņošanu, taču inficēto iekārtu apjoms sarūk lēni, jo daļai lietotāju trūkst izpratnes vai zināšanu par infekcijas novēršanu.

Pārskata periodā notika aktīvs darbs Saeimas vēlēšanu darba grupā, veicot drošības testus, gatavojot ieteikumus un koordinējot drošības uzlabošanas pasākumus. Septembra sākumā tika novērota paaugstināta uzbrukumu aktivitāte, kas varētu tikt saistīta ar priekšvēlēšanu periodu. Apjomīgs pakalpojuma atteices uzbrukums (DDoS) tika virzīts pret Delfi.lv infrastruktūru laikā, kad tika raidītas premjera amata kandidātu debates. Lai arī apjomīgs, uzbrukums tika veiksmīgi atvairīts un neietekmēja gala lietotājam sniegtos pakalpojumus.

Pastiprinātu mediju interesi pārskata periodā radīja Yandex.Taxi lietotne. Sekojot Lietuvas Nacionālā kiberdrošības centra veiktajai izpētei, CERT.LV Aizsardzības ministrijas uzdevumā veica neatkarīgu lietotnes analīzi, kuras rezultātā netika konstatēta funkcionalitāte, kas tehniski vērtējama kā ļaunprātīga. CERT.LV veiktās analīzes rezultātus apkopojusi Latvijas Aizsardzības ministrija un nosūtījusi tālāk izvērtēšanai Datu valsts inspekcijai un Latvijas Republikas Tieslietu ministrijai, lai noskaidrotu, vai „Yandex.Taxi" lietotnes apkopotie dati ir samērīgi un atbilstoši GDPR (Vispārīgā datu aizsardzības regula). Valsts sektorā strādājošajiem ir izteikts aicinājums izvērtēt lietotnes lietošanas nepieciešamību un iespējamos riskus.

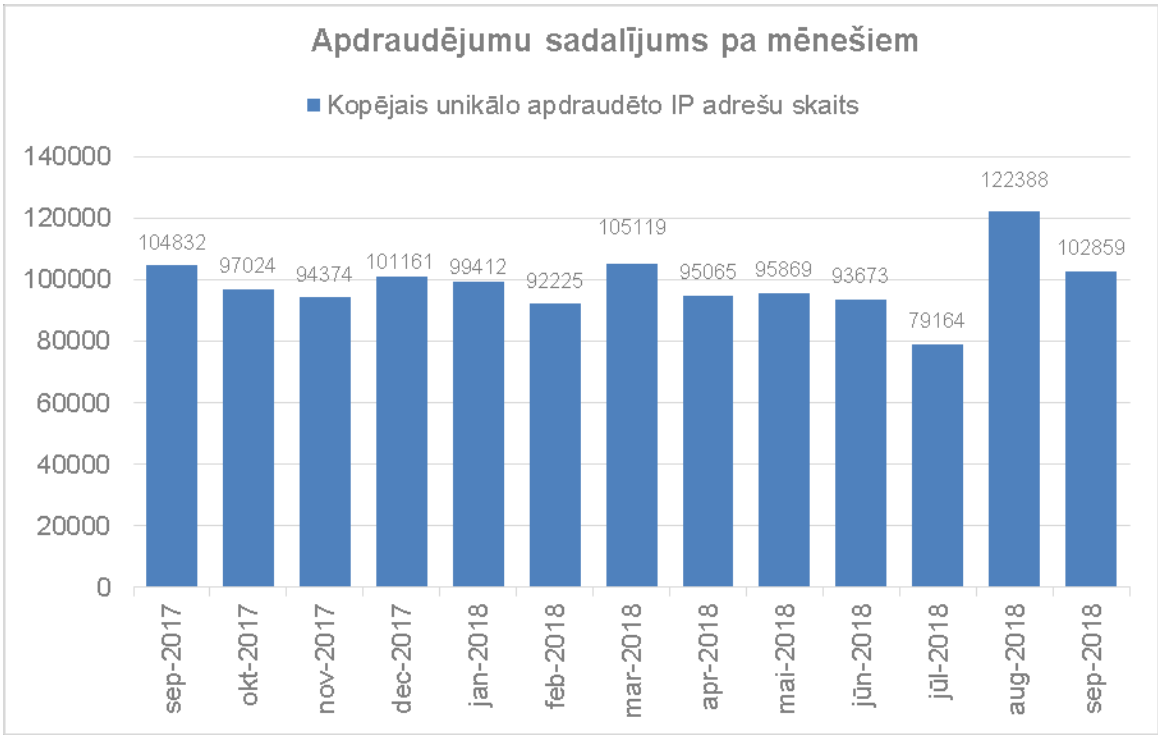
Notika aktīva gatavošanās gada lielākajam kiberdrošības pasākumam – konferencei „Kiberšahs 2018", izstrādājot aktualitātēs bāzētu programmu, pieaicinot pieredzes bagātus ekspertus un nodrošinot maksimāli efektīvu pasākuma sagatavošanas un norises procesu, atbilstoši Eiropas Kiberdrošības mēneša idejām un projekta "Improving Cyber Security Capacities in Latvia" vadlīnijām.

Pārskata periodā CERT.LV par IT drošību izglītoja 467 cilvēkus, iesaistoties 10 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.

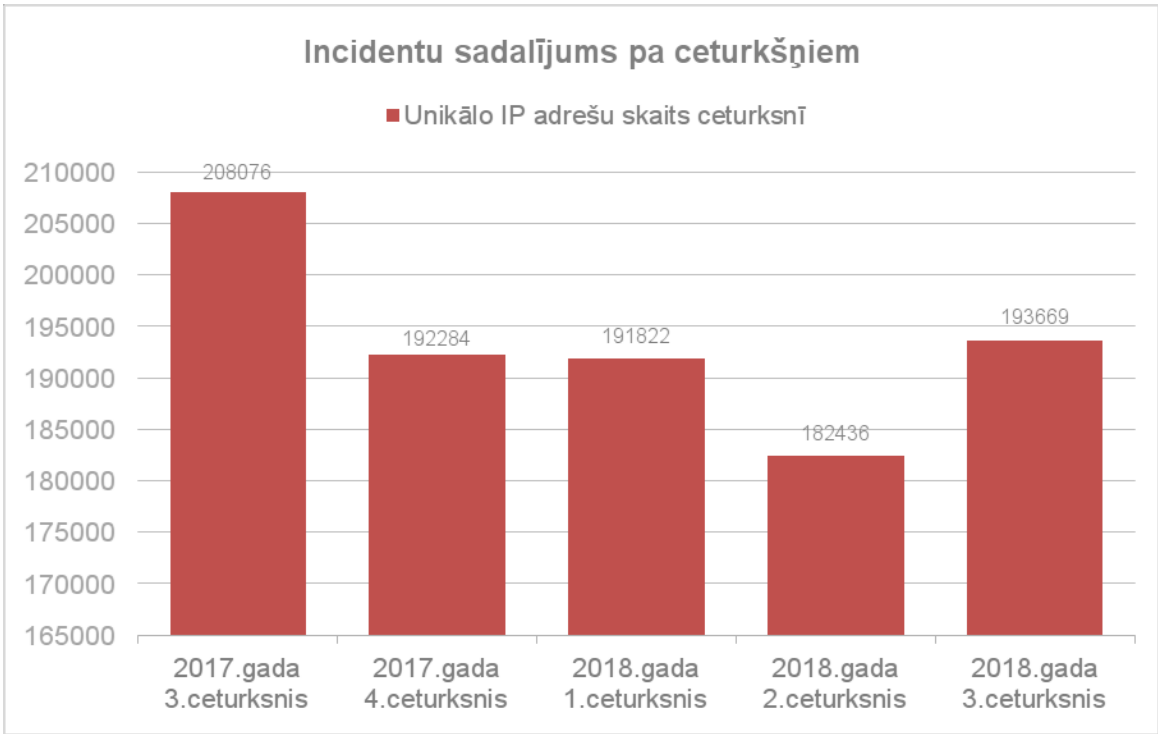
CERT.LV pārskata periodā ik mēnesi apkopoja informāciju par 95 000 – 100 000 ievainojamu unikālu IP adrešu.



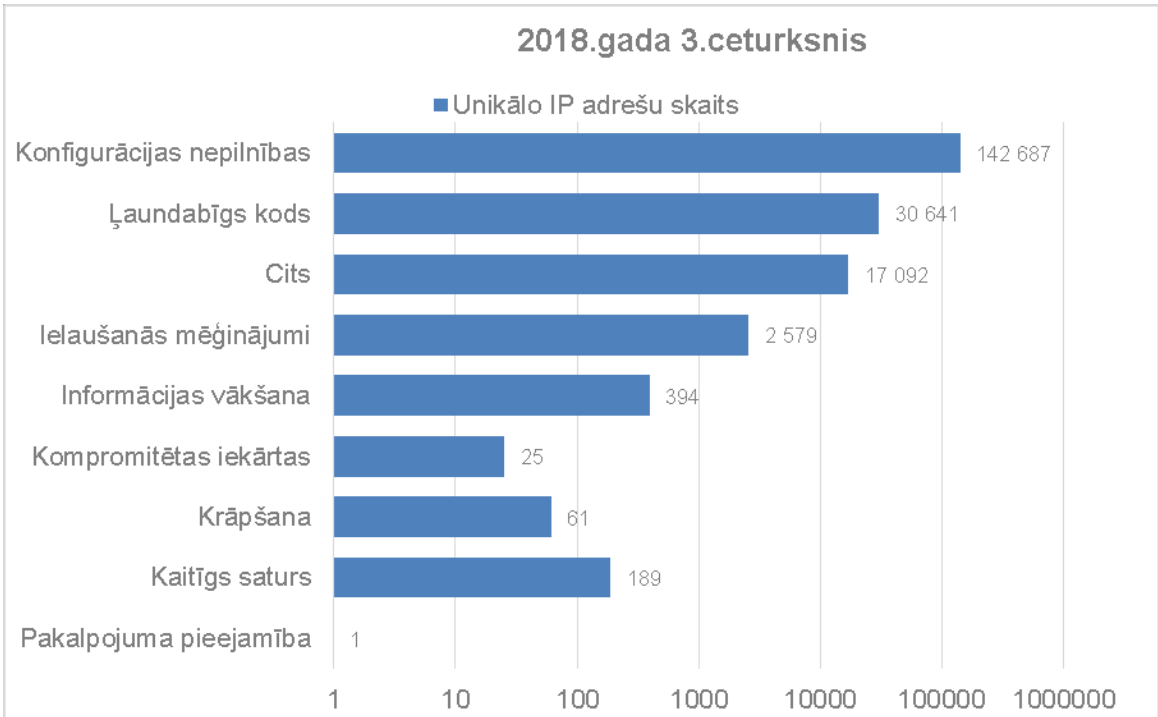
1.attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa mēnešiem 12 mēnešu griezumā.

Pārskata periodā nav vērojamas būtiskas izmaiņas mēnesī reģistrēto apdraudēto IP adrešu daudzumā. Novērotais kritums jūlijā un kāpums augustā ir skaidrojams ar nevienmērīgu ienākošo datu plūsmu.

2018. gada 3. ceturksnī tika reģistrētas 193 670 unikālas apdraudētas IP adreses, kas ir par nepilniem 6% vairāk nekā iepriekšējā ceturksnī, bet par 7% mazāk nekā šajā pašā periodā pirms gada.



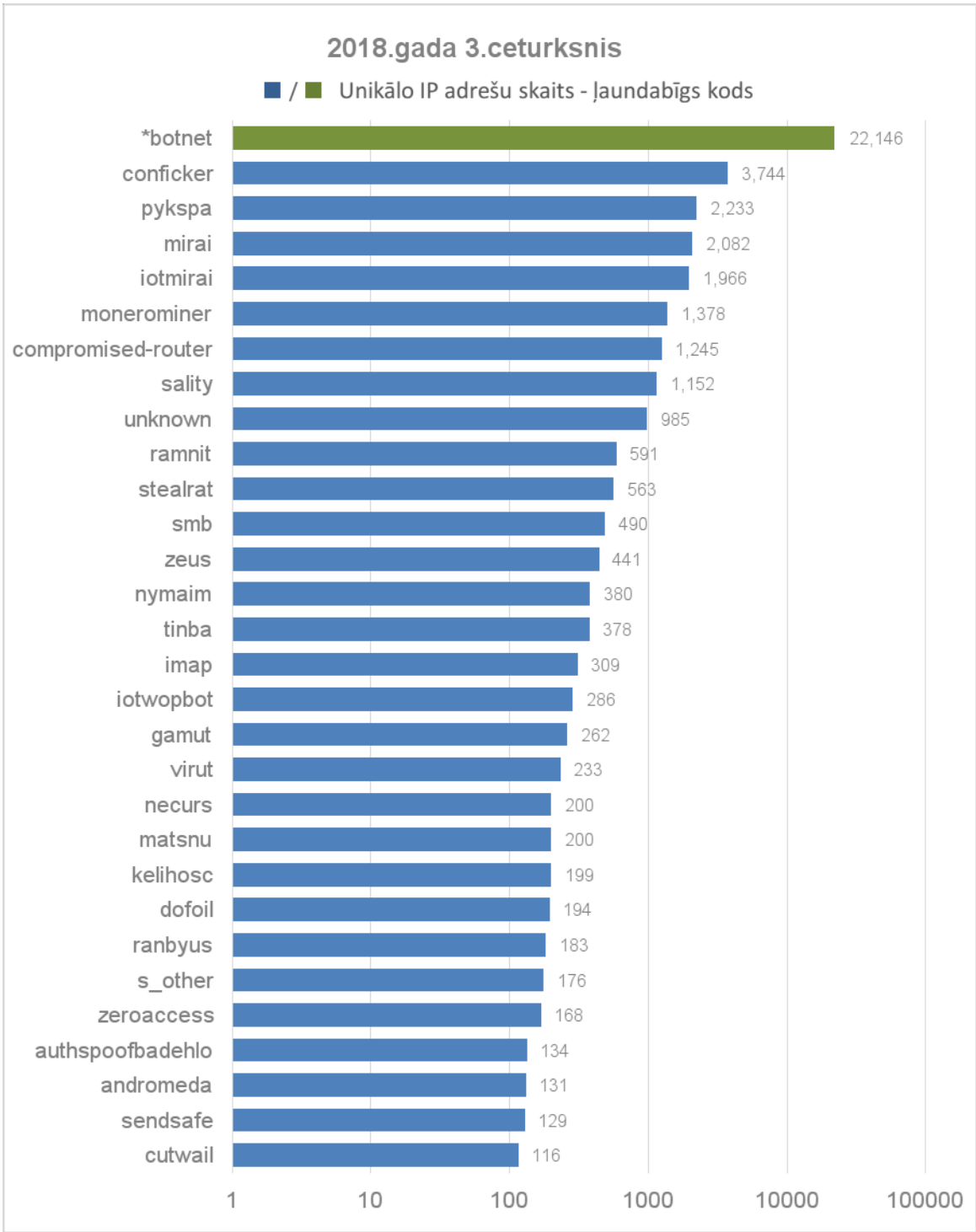
2.attēls – CERT.LV reģistrētās apdraudētās IP adreses pa ceturkšņiem 2017. un 2018. gadā.



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

Izplatītākais apdraudējuma veids pārskata periodā nemainīgi bija konfigurācijas nepilnības (pieaugums par 5% pret iepriekšējo periodu), otrs izplatītākais bija ļaundabīgs kods (kritums par 9%), bet trešais - ielaušanās mēģinājumi (pieaugums par 131%). Ielaušanās mēģinājumu pieaugums saistīts ar inficētiem maršrutētājiem un citām iekārtām, kas iekļautas robotu tīklos un veic automatizētus uzbrukumus šo tīklu paplašināšanai.

Lai mazinātu ar ļaunatūru inficēto maršrutētāju apjomu, CERT.LV veic iekārtu īpašnieku apziņošanu, taču inficēto iekārtu apjoms krītas lēni, jo bieži vien lietotājiem trūkst zināšanu un izpratnes par to, kā savu inficēto iekārtu salabot.



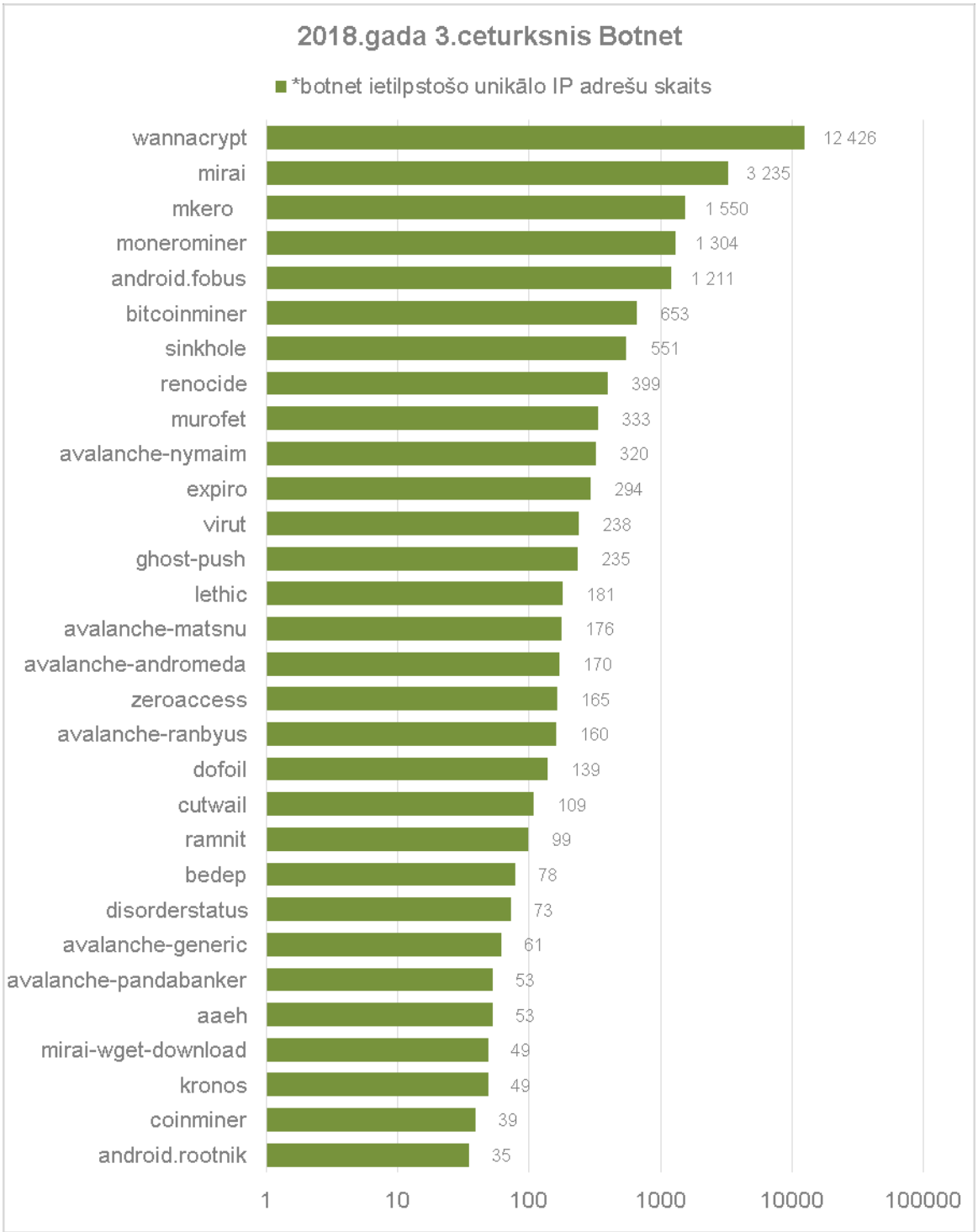
4.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2018. gada 3. ceturksnī ar apdraudējuma veidu - ļaundabīgs kods.

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.

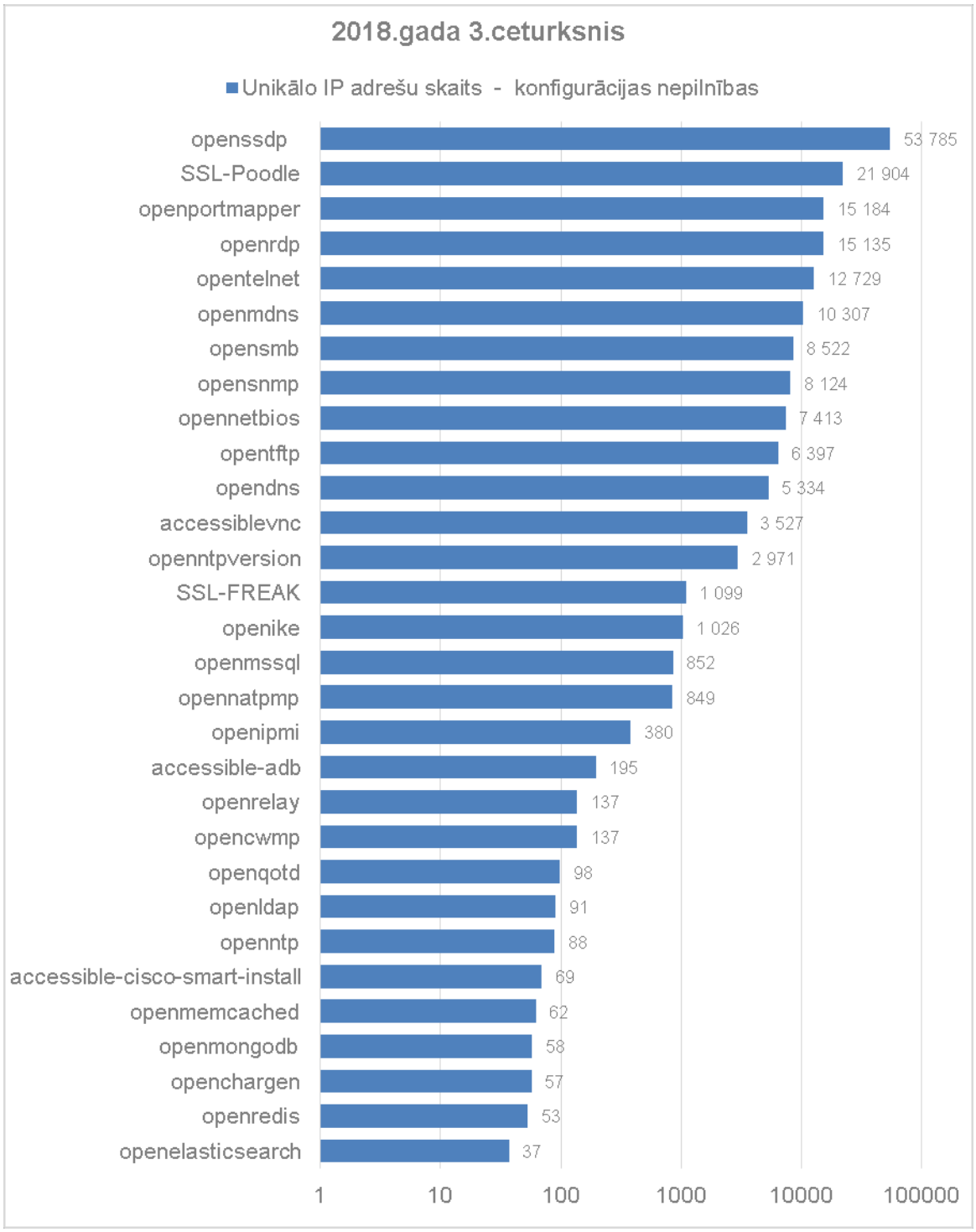
Trešo vietu ieņem *Pykspa* – datortārps, kas izplatās, izmantojot tīkla diskus, Skype, Twitter

un satur mūķi (*backdoors*), kas ļauj uzbrucējam attālināti izpildīt upura iekārtā patvaļīgu kodu.



4.1.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2018. gada 3. 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 3. 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.

Ceturtajā vietā esošā konfigurācijas nepilnība *OpenRDP* pārskata periodā bija iemesls daudziem iesniegumiem policijā, kas bija saistīti 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.

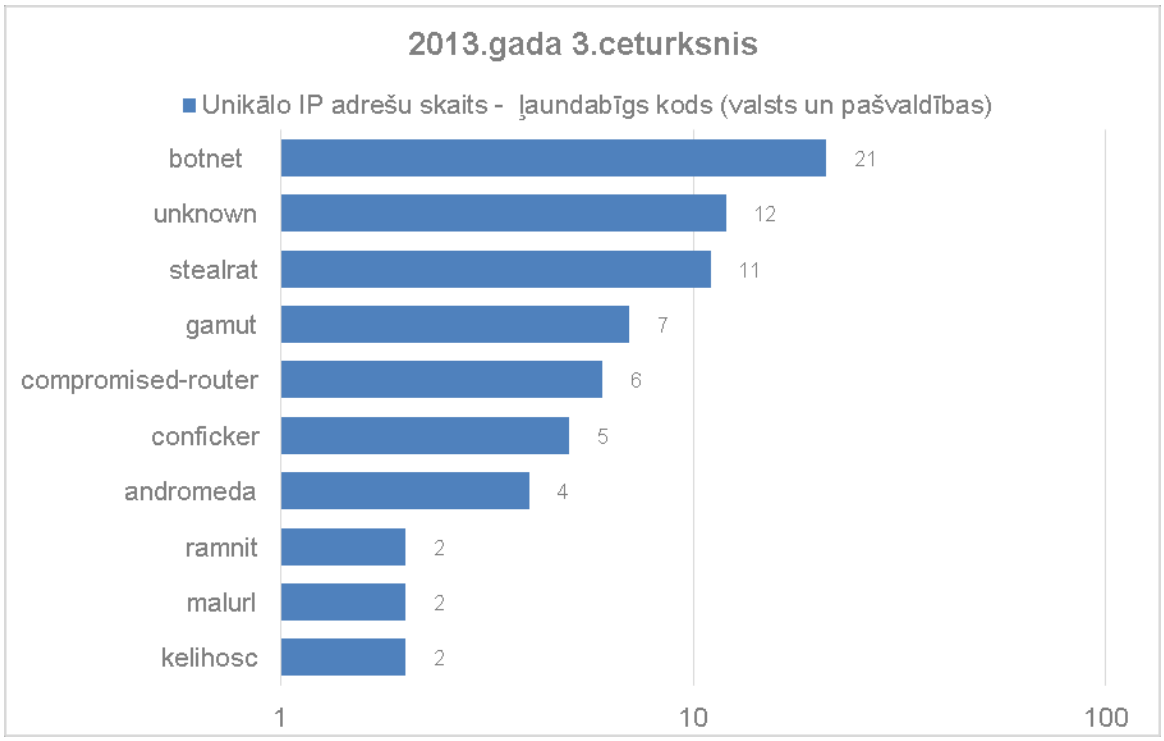
2. Atbalsts informācijas tehnoloģiju drošības incidentu novēršanā vai to novēršanas koordinēšanā.

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.

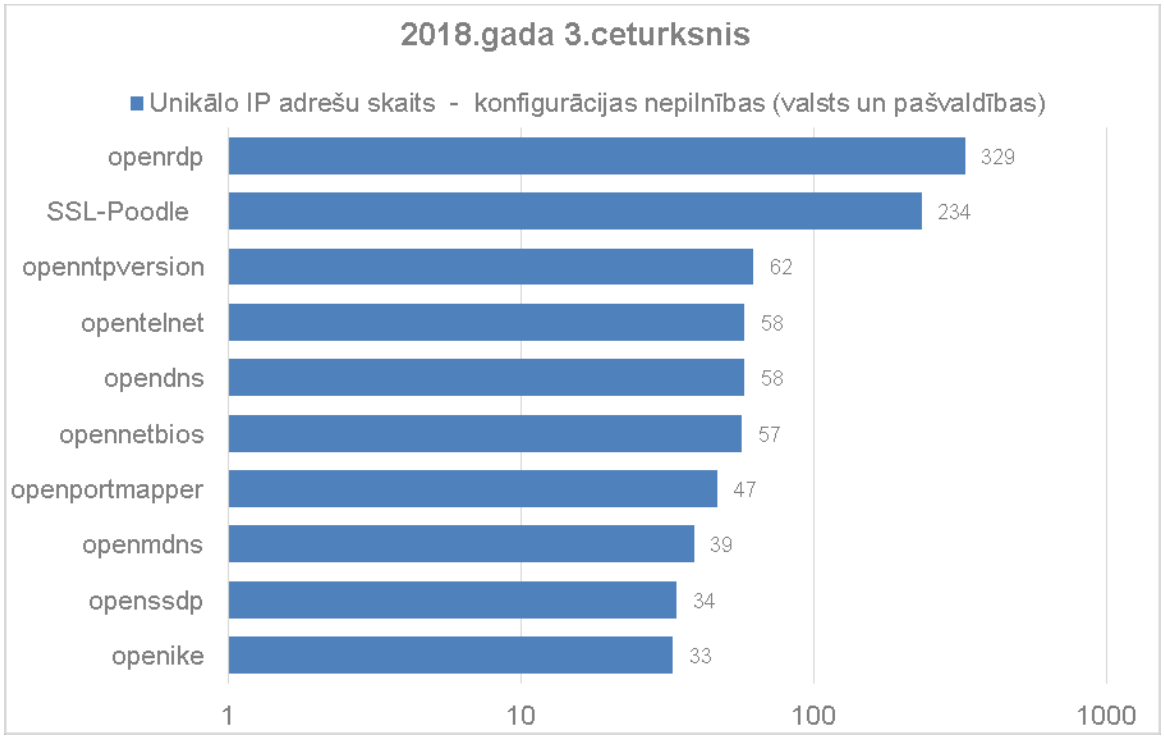
Izmaiņas katras dienas saņemtajos ziņojumos par valsts un pašvaldību iestādēm:

6.attēls – Iestāžu apdraudēto IP adrešu daudzums katras dienas saņemtajos ziņojumos 2018. gada 3. 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.

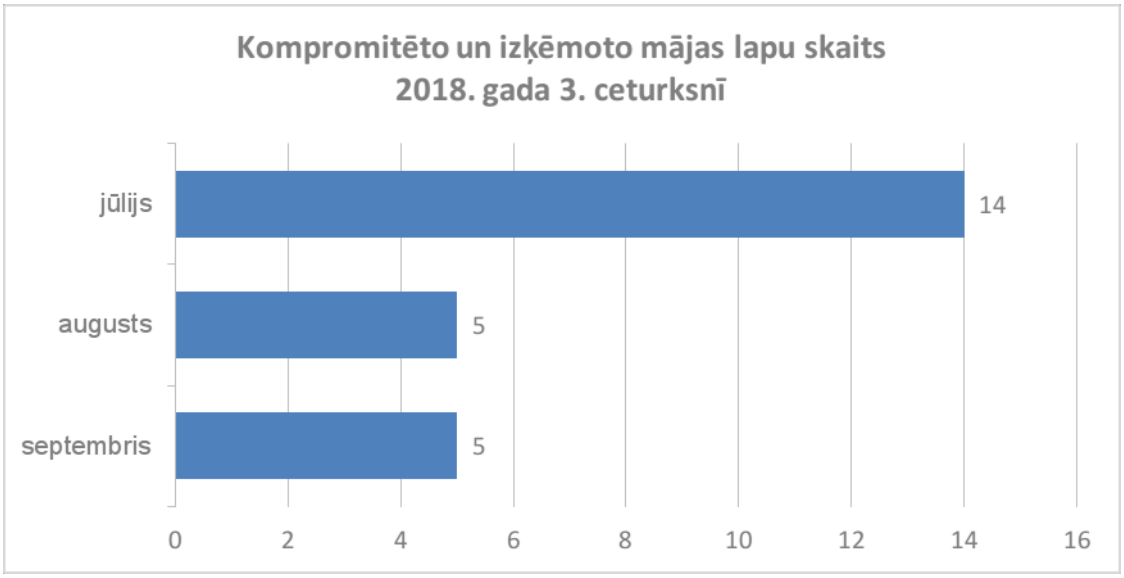


7.attēls - CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2018.gada 3.ceturksnī ar apdraudējuma veidu – ļaundabīgs kods (TOP 10 ļaundabīgs kods).



8.attēls - CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2018.gada 3. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība (TOP 10 konfigurācijas nepilnības).

CERT.LV uzskaita arī kompromitēto un izķēmoto tīmekļa vietņu gadījumus. Pārskata periodā tika fiksētas 24 kompromitētas un izķēmotas tīmekļa vietnes. Divdesmit divos gadījumos izķēmotās vietnes uzturēšanai tika izmantota Linux operētājsistēma, bet divos gadījumos informācija par vietnes operētājsistēmu nav pieejama. 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 3. 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

Jūlija sākumā pret kādu valsts iestādes tīmekļa vietni tika vērsts 300 Mbps liels pakalpojuma atteices (DDoS) uzbrukums, izmantojot UDP *flood* un NTP amplifikāciju. Uzbrukums ilga 10 minūtes. Vietnes darbība uzbrukuma ietekmē netika traucēta.

Septembra sākumā pret kādu valsts iestādes tīmekļa vietni tika vērsts DDoS uzbrukums ar mainīgu jaudu, kas intensīvākajā periodā sasniedza 456 Mbps. Uzbrukumam izmantots UDP *flood*. Uzbrukums pamīšus atkārtojās 2 dienas.

Septembra sākumā tika saņemts ziņojums par DDoS uzbrukumu ziņu portālam Delfi.lv. Šis uzbrukums tiek saistīts ar priekšvēlēšanu periodu, jo notika dienā, kad portāls translēja premjera amata kandidātu debates. Uzbrukuma intensitāte sasniedza 20 Gbps, bet uzbrukums tika veiksmīgi atvairīts, un lietotāji uzbrukuma ietekmi uz pakalpojumu neizjuta.

Divas dienas vēlāk notika DDoS uzbrukums kādai valsts iestādes tīmekļa vietnei. DNS amplifikācijas uzbrukums, kurā izmantoti atvērti DNS un RDP servisi, sasniedza 1,2 Gbps, ierobežojot vietnes pieejamību no dažiem tīkliem uz apmēram 8 stundām.

Septembra beigās tika saņemts ziņojums par Latvijas IP adresēm, kas tika izmantotas UDP amplifikācijas tipa DDoS uzbrukumā, kas vērsts pret Google IP adresēm.

Septembra beigās tika saņemti ziņojumi par DDoS uzbrukumiem divu tūrisma firmu tīmekļa vietnēm, kas uzņēmumiem nodarījuši zaudējumus. Pēc saziņas ar uzņēmumiem, no vienas kompānijas iegūti žurnalēšanas pieraksti analīzei. Iepriekšējus draudus kompānijas nebija saņēmušas.

Pikšķerēšana

Saņemts ziņojums par Swedbank internetbankas datu izkrāpšanas mēģinājumu, paziņojot, ka darbības ar kontu ir ierobežotas uz 24h un nepieciešama papildu informācija pilnas piekļuves atjaunošanai. Pieprasītos datus – informāciju par identitāti vai pēdējiem darījumiem – aicināts ievadīt e-pastā norādītajā saitē, kas ved uz krāpniecisko vietni.

Vairāku valsts iestāžu un uzņēmumu darbinieki saņēmuši e-pasta piekļuves datu izkrāpšanai paredzētus pikšķerēšanas e-pastus, kuri sūtīti it kā administratora vārdā, norādot uz pārsniegtu kvotu, lietošanas noteikumu pārkāpumu vai e-pasta aizvēršanu un visu failu dzēšanu, ja lietotājs nesekos saitei un neievadīs pieprasīto informāciju.

Kādas valsts iestādes darbinieki saņēma e-pastu latviešu valodā, kas saturēja aicinājumu pārbaudīt konta statusu, sekojot saitei, kas bija paredzēta darbinieku e-pasta piekļuves izgūšanai. Pikšķerēšanas uzbrukums bija veiksmīgs un attiecīgo lietotāju konti tika kompromitēti.

Tika saņemti ziņojumi no vairākiem inbox.lv un kādas pašvaldības lietotājiem par pikšķerēšanas e-pastu, kurā aicināts sekot saitei, lai veiktu obligātos drošības atjauninājumus ar personalizētiem ieteikumiem un novērstu mēstules – aktuāli aspekti, lai mudinātu lietotāju noklikšķināt.

Tika saņemta informācija par Office365 paroļu izkrāpšanas kampaņu. E-pasti bija angļu valodā un informēja lietotājus par konta slēgšanu, ja konts netiks atjaunināts, noklikšķinot uz saites.

Tika saņemts ziņojums par personas datu izkrāpšanas mēģinājumu, it kā Facebook vārdā nosūtot paziņojumu par laimestu loterijā. E-pastā saņēmējs tiek informēts par laimestu 2 miljonu eiro apmērā lūgts nosūtīt personīga rakstura informāciju, kā arī aicināts drošības apsvērumu dēļ neizpaust nevienam informāciju par šī e-pasta saņemšanu, līdz datu apstrāde būs notikusi un laimests būs piešķirts.

Tika saņemts ziņojums par mēģinājumu izmantot typosquatting pikšķerēšanā, izmantojot kādas valsts iestādes domēnvārdam līdzīgu domēnu, lai izkrāptu e-pastu piekļuves.

Tika saņemta informācija par vairākām uzlauztām .lv vietnēm un Latvijas IP adresēm, kurās tika izvietota pikšķerēšana, kas vērsta uz iTunes, Apple, Amazon(3), First National Bank of South Africa, British Telecom(6), BMO Financial Group, DVLA, Caixa Bank, HSBC Europe, HSBC Middle East, TOKAI NETWORK CLUB un Microsoft klientiem.

Krāpšana

Tika saņemti vairāki ziņojumi no lietotājiem par krāpniecisku e-pastu vācu vai angļu valodā, kurā apgalvots, ka uzbrucējs ir uzstādījis lietotāja datorā vīrusu, un, lietotājam apmeklējot pieaugušajiem domātas tīmekļa vietnes, veicis ierakstu, un izplatīs šo ierakstu visiem lietotāja kontaktiem, ja noteiktā laikā netiks samaksāta izpirkuma maksa bitcoin kriptovalūtā 900 eiro apmērā. Lai palielinātu apgalvojuma ticamību, uzbrucējs e-pastā norādīja arī lietotāja paroli, kas viņam kļuvusi zināma it kā šī uzbrukuma rezultātā, bet patiesībā iegūta kādā no internetā publicētajām datu noplūdēm.

Vairāku iestāžu un uzņēmumu grāmatveži it kā direktora vai vadītāja vārdā saņēma e-pastu ar jautājumu par konta atlikumu un vai iespējams veikt neatliekamu starptautisku pārskaitījumu (CEO fraud).

Tika saņemts ziņojums par vietni onlineecco.com, kas lietotājam radīja aizdomas par krāpniecību. CERT.LV apstiprināja vairākas krāpnieciskas vietnes pazīmes: nesen reģistrēts domēna vārds, nav pieejama reāla īpašnieka kontaktinformācija, informatīvajos tekstos ir kļūdas un norādes uz neeksistējošām tīmekļa vietnēm. Lietotājam tika ieteikts sazināties ar savu banku, lai noskaidrotu iespēju atgūt naudu, kas samaksāta šajā vietnē, ja prece netiks saņemta.

Ielaušanās un mēģinājumi

Jūlija sākumā notika mēģinājumi pieslēgties un izsūtīt e-pastus no kādas valsts iestādes domēna vārda, izmantojot gan eksistējošas lietotāju e-pasta adreses, gan ģenerētas. Uzbrukums bija neveiksmīgs, e-pasta vēstules līdz lietotājiem nenonāca. Līdzīgi mēģinājumi tika novēroti arī iepriekšējā pārskata periodā.

Reģistrēts liels apjoms automatizētu ielaušanās mēģinājumu, ko veikušas inficētas iekārtas, piemēram, maršrutētāji, kas iekļauti robotu tīklā un uzbrūk citām līdzīgām iekārtām ar mērķi tīklu paplašināt, lai vēlāk veiktu citas ļaunprātīgas darbības, piemēram, pakalpojuma atteices jeb DDoS uzbrukumus.

Ļaunatūra

Saņemti vairāki ziņojumi no kāda uzņēmuma par e-pastiem ar ļaundabīgiem pielikumiem. E-pasts ar it kā .DOC formāta rēķinu pielikumā saturēja trojāni, tāpat kā DHL vārdā sūtītais krāpnieciskais e-pasts ar aicinājumu apstiprināt piegādes adresi, kas norādīta pielikumā esošajā .RAR arhīvā. Arī kādam citam e-pastam pievienotais .DOC maksājuma uzdevums saturēja trojāni. Visos gadījumos izmantotais antivīruss atpazina ļaunatūru.

Tika saņemts ziņojums par kaitīgu e-pastu, kurā sūtītājs apgalvo, ka iepriekšēja sarakste jau ir notikusi un tagadējā sarakste notiek no nepazīstama e-pasta, jo e-pasta serverim ir bijusi nepieciešama apkope. E-pastam pievienots it kā piegādes dokumentu fails, kas imitē PDF dokumentu, bet pārvirza lietotāju uz vietni, kura nolasa dažādu tīmekļa resursu saglabātās paroles.

Jūlija vidū tika saņemts ziņojums par e-pastu kampaņu, kurā Danske Bank vārdā aicina saņēmēju atvērt e-pastā esošo pielikumu, lai iegūtu papildinformāciju par neizdevušos bankas transakciju. Pielikums veica mēģinājumu lejupielādēt saņēmēja iekārtā vīrusu.

Augustā no kādas valsts iestādes tika saņemts ziņojums par viltotu vīrusu saturošu e-pastu izplatīšanu iestādes vārdā. E-pasti aicināja klientus veikt datu atjaunošanu, izmantojot e-pasta pielikumu, un saturēja .ZIP arhīvu ar .JAR failu tajā. Norādītā e-pasta adrese nav reģistrēta iestādes domēnā, un izmantotajam domēnam jau bija izveidoti SPF ieraksti, kas nosaka izmantotos e-pasta serverus, bet, lai šī tehnoloģija darbotos, arī klientiem jāveic ienākošo e-pastu nosūtītāju atbilstības pārbaude, kas ļautu atpazīt un marķēt šādas vēstules kā aizdomīgas. CERT.LV ieteica domēnam izmantot arī DKIM tehnoloģiju. Pārbaude apliecināja, ka vēstuļu izsūtīšanai netika izmantota uzlauzta iestādes konta pieteikšanās informācija. CERT.LV ieteica iestādei informēt klientus par kaitīgajiem e-pastiem.

Tika saņemts ziņojums par ļaunatūras izplatīšanu no kādas Latvijas IP adreses. Uzturētājs tika informēts, ļaunatūra tika dzēsta.

Septembra beigās tika saņemts ziņojums par ļaunatūras pieejamību vietnē failiem.lv. Atbilstošā saite tika nosūtīta vietnes uzturētājiem un iesniegts pieprasījums par satura dzēšanu.

Saņemts ziņojums par vairāku ļaunatūru - *JBifrost botnet, Pony botnet, NanoCore, Loki botnet, NetWire* un *AgentTesla* – komand- un kontroles centriem (C&C) Latvijas IP adresēs.

JBifrost ir ļaunatūra, kas uzbrucējam sniedz attālinātu piekļuvi upura iekārtai. *NanoCore* trojānis ļauj uzbrucējam attālināti kontrolēt upura iekārtu un ievākt informāciju par, piemēram, ievadītajām parolēm. *Loki* ļaunatūra paredzēta paroļu un citas sensitīvas informācijas zādzībai. *NetWire* trojānis veic maksājumu karšu datu zādzību. *AgentTesla* ir programmatūra, kas paredzēta taustiņu nospiedienu fiksēšanai jeb *keylogger*. Taču visvairāk C&C pārskata periodā bija *Pony* ļaunatūrai, kas, lai arī specializējas personīgo datu zādzībā, spēj veikt arī kriptovalūtas, piem., bitcoin zādzību.

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

Mobilā ļaunatūra

Tika saņemta informācija no kāda lietotāja par ļaundabīgām aktivitātēm kāda uzņēmuma mobilajā tīmekļa vietnes versijā. Apmeklējot vietni, lietotājam tika parādīts paziņojums, ka viņš ir laimējis iespēju piedalīties īpašas Google balvas izlozē, atbildot uz vairākiem vienkāršiem jautājumiem. Vietnes baneru sistēmā tika konstatēts inficēts baneris, kas bija paredzēts lietotāju datu izkrāpšanai. Baneru sistēmas uzturētāji tika informēti, beneris tika dzēsts.

Kompromitētas iekārtas

Jūlija sākumā tika saņemts ziņojums no kādas pašvaldības par uzlauztu tīkla serveri. Serveris tika uzlauzts un gandrīz visas datnes nošifrētas (.HRM). Serveris nesaturēja svarīgus datus. Sazinoties ar cietušo institūciju, tika noskaidrots, ka uzbrukums veikts, izmantojot Remote Desktop pieslēgumu, ielogojoties no konta ar vāju paroli.

Tika saņemti ziņojumi par kaitīgu saturu vairāku valsts iestāžu tīmekļa vietnēs. Vietnēs tika konstatētas novecojušas satura vadības sistēmas versijas, kuras atsevišķos gadījumos saturēja kritiskas ievainojamības. Uzturētāji tika informēti, un tika lūgts atjaunināt vietnes uz jaunāko satura vadības sistēmas versiju. Visos gadījumos kaitīgais kods no vietnes tika dzēsts, bet ne visas vietnes tika atjauninātas, tādejādi pakļaujot tās atkārtotas inficēšanas riskam.

Mēstules (SPAM)

Augusta beigās tika saņemts ziņojums par mēģinājumiem manuāli izsūtīt e-pastus kādas valsts iestādes vārdā. Tā kā iestāde bija veikusi nepieciešamos drošības pasākumus un nokonfigurējusi Sender Policy Framework (SPF) ierakstu, tad šie mēģinājumi neizdevās.

Atbildīga ievainojamību atklāšana

Septembrī atbildīgas ievainojamību atklāšanas ietvaros tika saņemti ziņojumi par starpvietņu skriptēšanas (XSS) ievainojamībām 11 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.

Septembra beigās tika saņemti arī ziņojumi par kritiskām SQL injekcijas ievainojamībām divās valsts iestāžu tīmekļa vietnēs, kas ļautu uzbrucējam brīvi izgūt datus no sistēmu datubāzes. Vienā no šīm vietnēm tika konstatēta arī neatbilstoši konfigurēta PHP instalācija – pirmkodā

tika atklāta informācija, kas ļautu ļaundarim pārņemt kontroli pār sistēmas e-pasta kontu. 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.

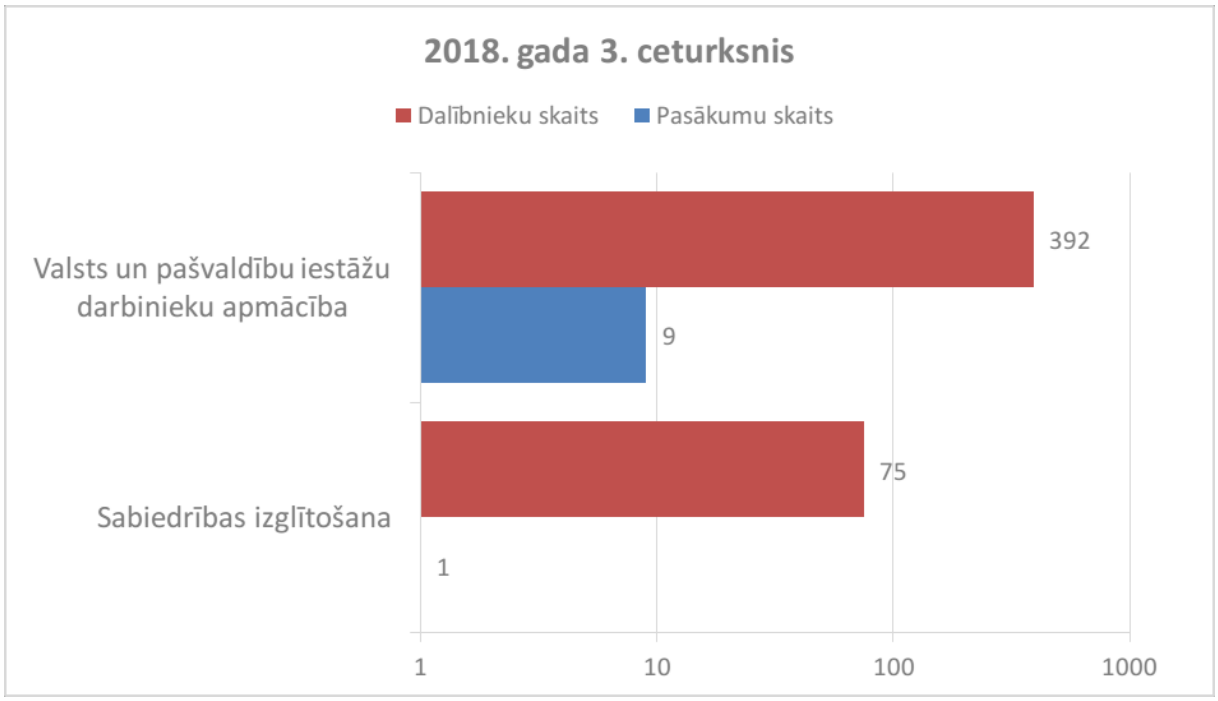
3. Pētnieciskais darbs, izglītojošo pasākumu organizēšana un mācības informācijas tehnoloģiju drošības jomā.

Augustā CERT.LV pārstāvji piedalījās Samsung Skola nākotnei projektā, sagatavojot vairākas video lekcijas jauniešiem ar padomiem paroļu veidošanai, viedierīču un sociālo tīklu lietošanai un privātuma aizsardzībai.

Pārskata periodā CERT.LV pārstāvji piedalījās starptautiskā izglītošanas projekta APSTĀJIES.PADOMĀ.PIESLĒDZIES. sanāksmē. Projekta mērķis ir aktualizēt lietotāju atbildīgu attieksmi pret savām ierīcēm un datiem, ievērojot kiberhigiēnu un citus labās prakses principus.

Septembrī sadarbībā ar APSTĀJIES.PADOMĀ.PIESLĒDZIES un Eiropas Tīklu un informācijas drošības aģentūru (ENISA) tika latviskots Eiropas Kiberdrošības mēnesim paredzētais informatīvi-izglītojošais materiāls.

Pārskata periodā CERT.LV par IT drošību izglītoja 467 cilvēkus, iesaistoties 10 izglītojošos pasākumos.



10.attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2018. gada 3. ceturksnī

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

Sadarbības tikšanās, konsultācijas un prezentācijas:

- CERT.LV sniedza atbalstu Latvijas Republikas Aizsardzības ministrijai, ieviešot NIS direktīvu Informācijas tehnoloģiju drošības likumā un saistītajos Ministru kabineta noteikumos Nr.442, tai skaitā:

  - tika skaidrota informācijas tehnoloģiju terminoloģija, darbības principi un procesi;

  - tika iesniegti iebildumi par Finanšu ministrijas priekšlikumu izslēgt kreditēšanas, noguldījumu un citu atmaksājamo līdzekļu piesaistīšanas pakalpojumu jomas no pamatpakalpojumu sniedzēju saraksta, jo CERT.LV pieļauj, ka esošais jomu regulējums nav atzīstams par līdzvērtīgu NIS direktīvas 9.apsvēruma izpratnē;

  - tika iesniegti priekšlikumi normatīvo aktu projektu pilnveidošanai (piemēram, precizējot sistēmu auditācijas pierakstu saturu, elektroniskā pasta sistēmu drošības prasībām);

  -tika apspriesti normatīvo aktu projekti ar atbildīgo jomu ministrijām, uzņēmumiem, Saeimas Aizsardzības, iekšlietu un korupcijas novēršanas komisijas sēdēs, kā arī CERT.LV pārstāvji piedalījās konsultāciju sanāksmēs Saeimas Juridiskajā birojā.

- Tikšanās ar CVK sanāksmē par gatavošanos Eiropas Parlamenta vēlēšanām.

- Aizsardzības ministrijas uzdevumā veikta mobilās lietotnes Yandex.Taxi izpēte un sagatavots informatīvais ziņojums ar ieteicamo rīcību valsts un pašvaldību iestāžu darbiniekiem. Uzmanība Yandex taxi lietotnei tika pievērsta pēc Lietuvas Aizsardzības ministrijas paziņojumiem, ka tā ir nacionālās drošības apdraudējums.

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.

- 02.-08. septembrī CERT.LV pārstāvis pasniedza NATO CCDCoE "Malware and Exploitation Essentials" kursu Tallinā.

- 13. septembrī CERT.LV pārstāvis piedalījās sanāksmē ar Norvēģijas vēstnieku Latvijā, kurā tika pārrunāta abu valstu sadarbības attīstība.

- 20. septembrī projekta “Improving Cyber Security Capacities in Latvia” ietvaros CERT.LV piedalījās tiešsaistes sanāksmē par sadarbības platformas MeliCERTes attīstību un izmantošanas iespējām.

- 23.-26. septembrī projekta "Improving Cyber Security Capacities in Latvia" ietvaros CERT.LV pārstāvis piedalījās SIM3 auditoru kursos Viļņā, lai iegūtu SIM3 auditora sertifikāciju.
- 26.-29. septembrī CERT.LV pārstāvji piedalījās TF-CSIRT sanāksmē Viļņā, gan vadot sanāksmi, gan sniedzot prezentāciju „How can "know-how" exchange between CERT communication specialists improve our daily lives?", iepazīstinot ar sabiedrisko attiecību lomu un specifiku CERT darbībā un aicinot veidot atsevišķu sadarbības grupu tikai CERTu sabiedrisko attiecību speciālistiem.
- 28. septembrī CERT.LV pārstāvji Viļņā tikās ar Lietuvas CERT institūciju CERT.LT un NRDCS pārstāvjiem, lai pārrunātu sadarbības attīstības iespējas.
- Trīs mēnešu garumā notika aktīvi NATO CCDCoE kiberdrošības mācību „Crossed Swords 2019" sagatavošanās darbi.

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. Tika īstenotas nepieciešamās projekta publicitātes aktivitātes (publicēta informācija mājas lapā , turpināta sadarbība un nepieciešamā informācijas apmaiņa ar Eiropas Komisijas Inovāciju un tīklu aģentūru (INEA)).

Pārskata periodā ir uzsākta nepieciešamā iekšējo procedūru pārskatīšana un formalizēta nepieciešamā sadarbība ar Aizsardzības ministriju.

No projekta līdzekļiem līdzfinansēta kiberdrošības konference "Kiberšahs 2018". Projekta ietvaros tika nodrošināts finansējums nepieciešamajai starptautiskajai sadarbībai - pārskata periodā no projekta līdzekļiem līdzfinansēti CERT.LV darbinieku komandējumi uz konferencēm un kursiem.

7. 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 ir uzsākta 4 iestādēs.

- 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 turpināja noteikto funkciju veikšanu.

8. 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 01.07.2018. līdz 30.09.2018. ir saņēmusi un izvērtējusi 119 ziņojumus. No tiem 46 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 8 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 19 ziņojumos konstatēta personas goda un cieņas aizskaršana un 1 ziņojums saņemts par naida runu. Par finanšu krāpšanas mēģinājumiem internetā saņemti 7 ziņojumi, 8 ziņojumu saturs nav bijis pretlikumīgs, 30 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 25 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 15 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