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 3. ceturksnis (01.07.2019. – 30.09.2019.)

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 3. ceturksnī tika reģistrētas 202 493 unikālas apdraudētas IP adreses, kas ir par 18% mazāk nekā iepriekšējā ceturksnī, bet par 5% vairāk nekā šajā pašā periodā pirms gada.

Pārskata periodā Latvijas interneta telpā izplatītākie apdraudējumi:

- konfigurācijas nepilnības (118 687 unikālas IP adreses) ar kritumu 9% pret iepriekšējo periodu;
- ļaundabīgs kods (15 941 unikāla IP adrese) a kritumu 11%;
- ielaušanās mēģinājumi (1827 unikālas IP adreses) ar kritumu 25%.

CERT.LV sabiedrības informēšanas aktivitāšu rezultātā lēnām turpina kristies potenciāli apdraudēto iekārtu skaits, kurās attālinātās piekļuves serviss (*Remote Desktop* jeb RDP) ir eksponēts internetā. RDP izmantošana bez pienācīgiem aizsardzības pasākumiem – drošas paroles, piekļuves ierobežošanas no noteiktām IP adresēm vai caur VPN - pakļauj lietotāju palielinātam uzbrukuma riskam. CERT.LV ikdienā apstrādā incidentus par uzlauztiem un nošifrētiem serveriem un darbstacijām, kurām uzbrucējs piekļuvis, uzminot pārāk vienkāršo lietotāja paroli, vai iegūstot to no publiski nopludinātām datu bāzēm.

Ceturksnim bija raksturīgas daudzas pikšķerēšanas kampaņas Smart-ID, internetbankas piekļuves datu izkrāpšanas uzbrukumi un krāpšanas ar telefona zvanu starpniecību. Arī globāli bija vērojama tendence, ka finansiāli motivēti noziedznieki interneta vidē arvien vairāk koncentrēja savas darbības uz cilvēku pielietoto biznesa procesu nepilnību un nepārzināšanas izmantošanu savā labā. Upurus interneta vidē apmuļķoja vai ar viltu ievilināja krāpnieciskos darījumos, nevis uzlauza sarežģītas datorsistēmas.

CERT.LV saņēma ziņojumus par kampaņām, kas vērstas uz dažādu Latvijas banku klientiem. Sadarbībā ar policiju un bankām noritēja darbs pie krāpniecisko vietņu aizvēršanas un sabiedrības informēšanas, nodrošinot lielāku izpratni par banku autentifikācijas līdzekļu un maksājumu procesu darbību, kā arī pievēršot lietotāju pastiprinātu uzmanību tam, kā atpazīstama krāpniecība, piemēram, atgādinot, ka banka nemēģinās veikt saziņu ar klientu e-pastā, lai mudinātu uz darbībām internetbankā.

Turpinājās iejaukšanās biznesa sarakstē (*Business E-mail Compromise*) ar finansiāliem zaudējumiem vairāk nekā 10 000 eiro apmērā. Šī tendence saistīta ar visā pasaulē aktīvajām e-pastu piekļuves datu pikšķerēšanas kampaņām, kuru rezultātā uzbrucēji atsevišķos gadījumos ieguvuši piekļuvi uzņēmumu e-pastiem, lai sekotu sarakstei un īstajā brīdī nosūtītu rēķinu ar viltotiem rekvizītiem. Diemžēl, netiek pietiekami pielietotas daudzfaktoru autentifikācijas iespējas un ievērota paroļu veidošanas un lietošanas labā prakse – pietiekami garas paroles un unikālas katram resursam, ļaujot uzbrucējiem izmantot internetā nopludināto paroļu resursus. Abos gadījumos nepārtraukta lietotāju izglītošana ir veids kā uzlabot drošību.

Arī krāpšanas kampaņas, kas tika vērstas pret iestādes vai uzņēmuma finanšu darbiniekiem joprojām bija ievērojamā apjomā. Krāpnieki interneta vidē tās veica, nosūtot viltus e-pastus it kā vadītāja vārdā ar aicinājumu veikt pārskaitījumu. Lai arī kampaņas ir bijušas aktīvas, e-pastu saņēmēji krāpšanu atpazina arvien labāk, un CERT.LV nav ziņu par upuriem. CERT.LV iesaka izmantot SPF DNS ierakstus, DKIM un DMARC tehnoloģijas e-pasta sistēmu aizsardzībai un e-pastu viltošanas iespēju mazināšanai. Minēto tehnoloģiju lietošanas

vadlīnijas ir publicētas CERT.LV tīmekļa vietnē. 2020.gada 1.ceturksnī ir paredzēts aktīvs darbs ar valsts un pašvaldību iestādēm e-pasta sistēmu un DNS ierakstu labās prakses aktualizēšanā.

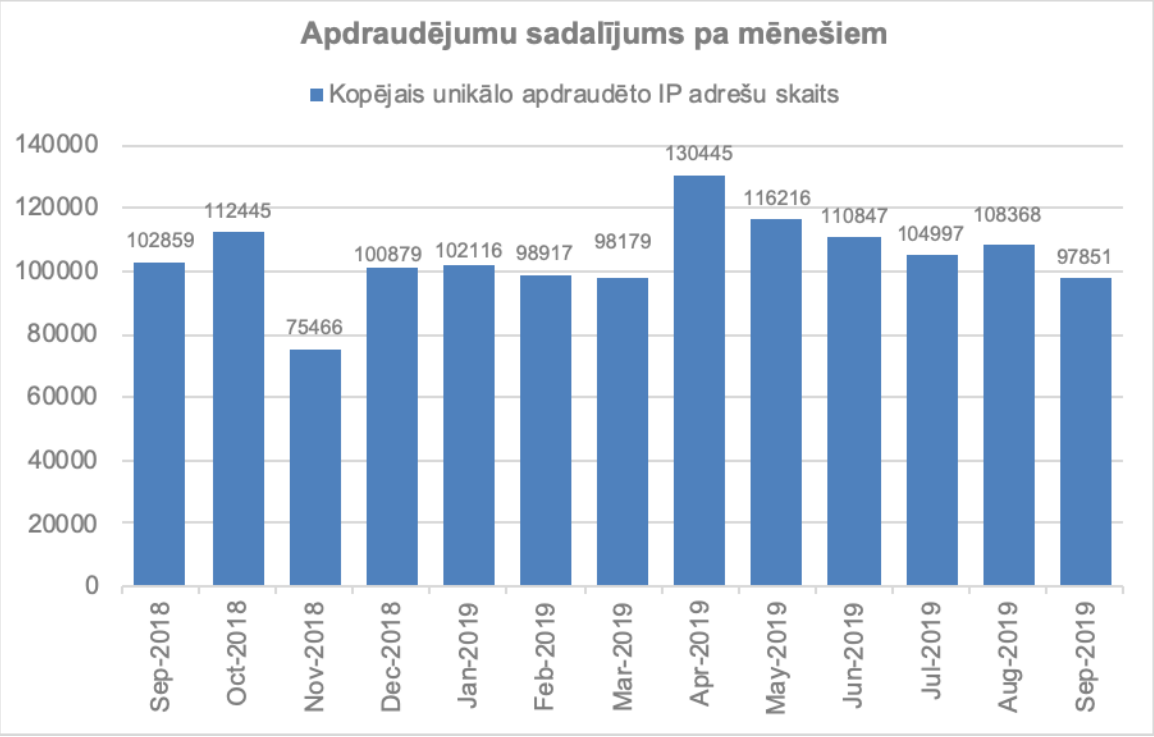
Pārskata periodā CERT.LV par IT drošību izglītoja 521 cilvēku, iesaistoties 14 izglītojošos pasākumos, galvenokārt organizējot apmācības valsts un pašvaldību iestāžu darbiniekiem.

TF-CSIRT sanāksmes ietvaros CERT.LV svinīgā ceremonijā saņēma arī TI (*Trusted Introducer*) sertifikātu par veiksmīgi izietu re-sertifikācijas procesu (tā jāatjauno ik pēc 3 gadiem). CERT.LV jau kopš 2016.gada ir viena no 26 Eiropas TF–CSIRT/Trusted Introducer sertificētajām komandām, kas apliecina CERT.LV komandas augsto brieduma un sagatavotības līmeni.

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, kas tagad nosaukta par „Reference Security Incident Taxonomy"). Taksonomija ir formalizēts veids kā CERT.LV apkopo, sadala kategorijās un reprezentē par incidentiem iegūto tehnisko informāciju. Statistikā visi CERT.LV reģistrētie apdraudējumi tiek uzskaitīti vienkopus, sadalot tos pa apdraudējumu veidiem (piemēram, ļaunatūra, ielaušanās, krāpšana), kā arī pa infekciju (piemēram, Confiker, Zeus, Mirai) un ievainojamību (piemēram, Opendns, Openrdp) tipiem.

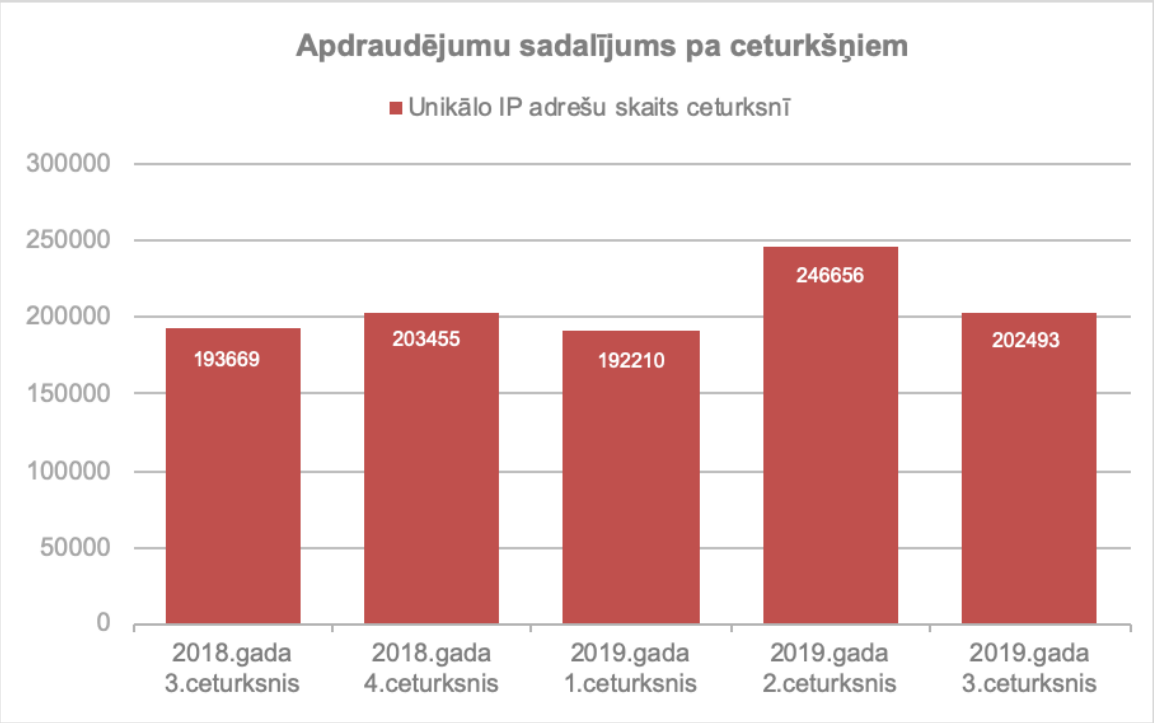
CERT.LV pārskata periodā ik mēnesi apkopoja informāciju par 100 000 – 110 000 ievainojamu unikālu IP adrešu.



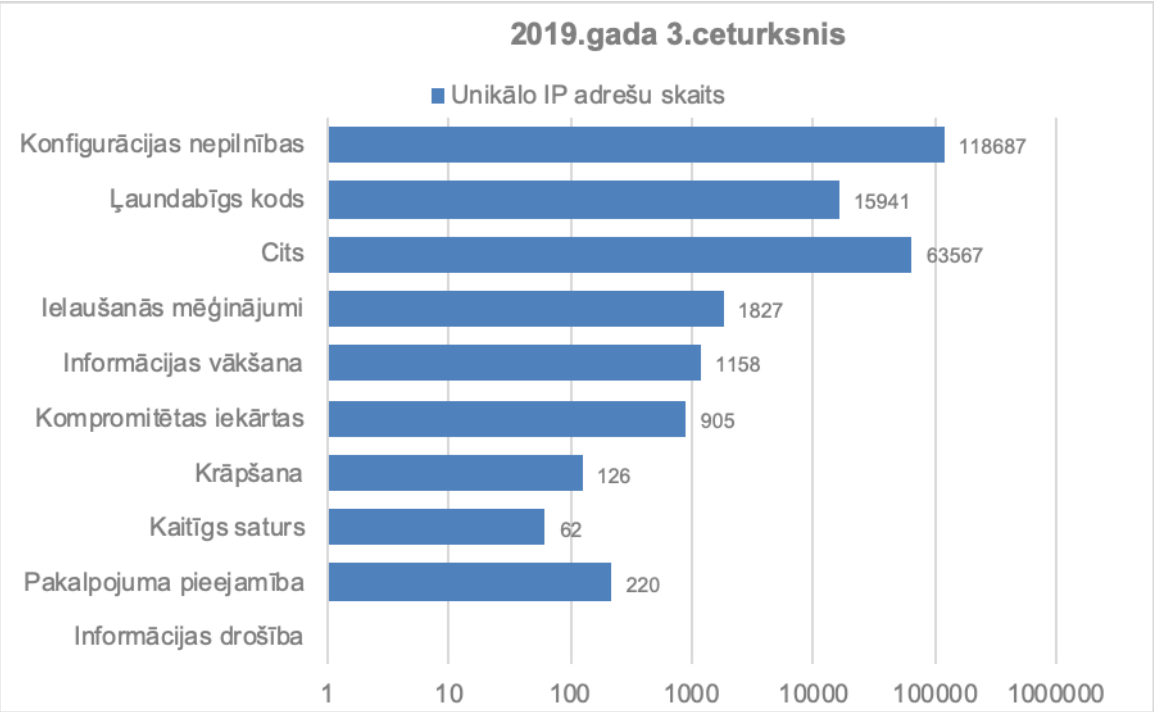
1.attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa mēnešiem 12 mēnešu griezumā.

2019. gada 3. ceturksnī tika reģistrētas 202 493 unikālas apdraudētas IP adreses, kas ir par 18% mazāk nekā iepriekšējā ceturksnī un par 5% vairāk nekā šajā pašā periodā pirms gada.

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



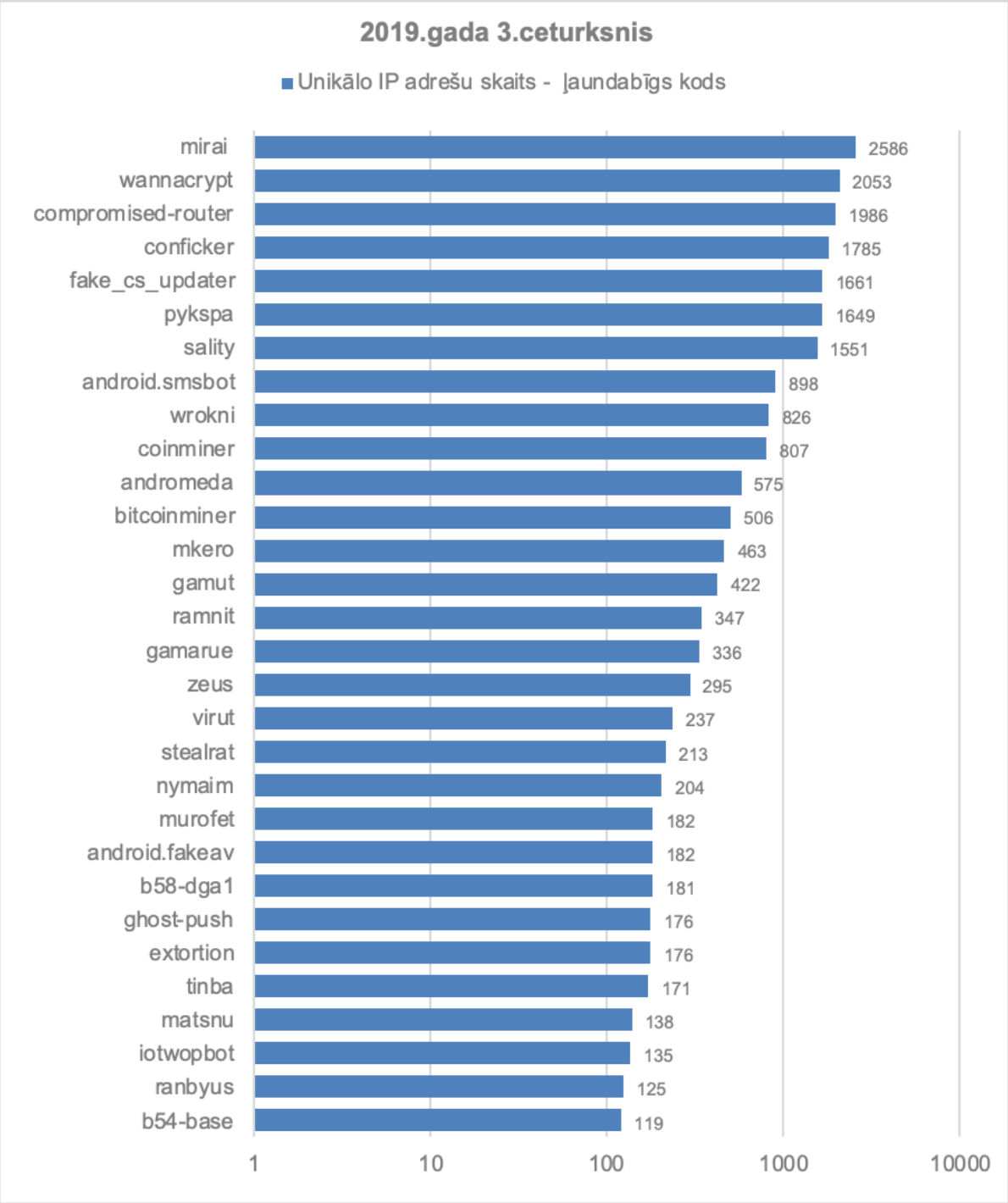
2.attēls – CERT.LV reģistrētās apdraudētās IP adreses pa ceturkšņiem 2018. un 2019. gadā.



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

Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (118 687 unikālas IP adreses) ar kritumu 9% pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs kods (15 941 unikāla IP adrese) a kritumu 11%, bet trešais - ielaušanās

mēģinājumi (1827 unikālas IP adreses) ar kritumu 25%.



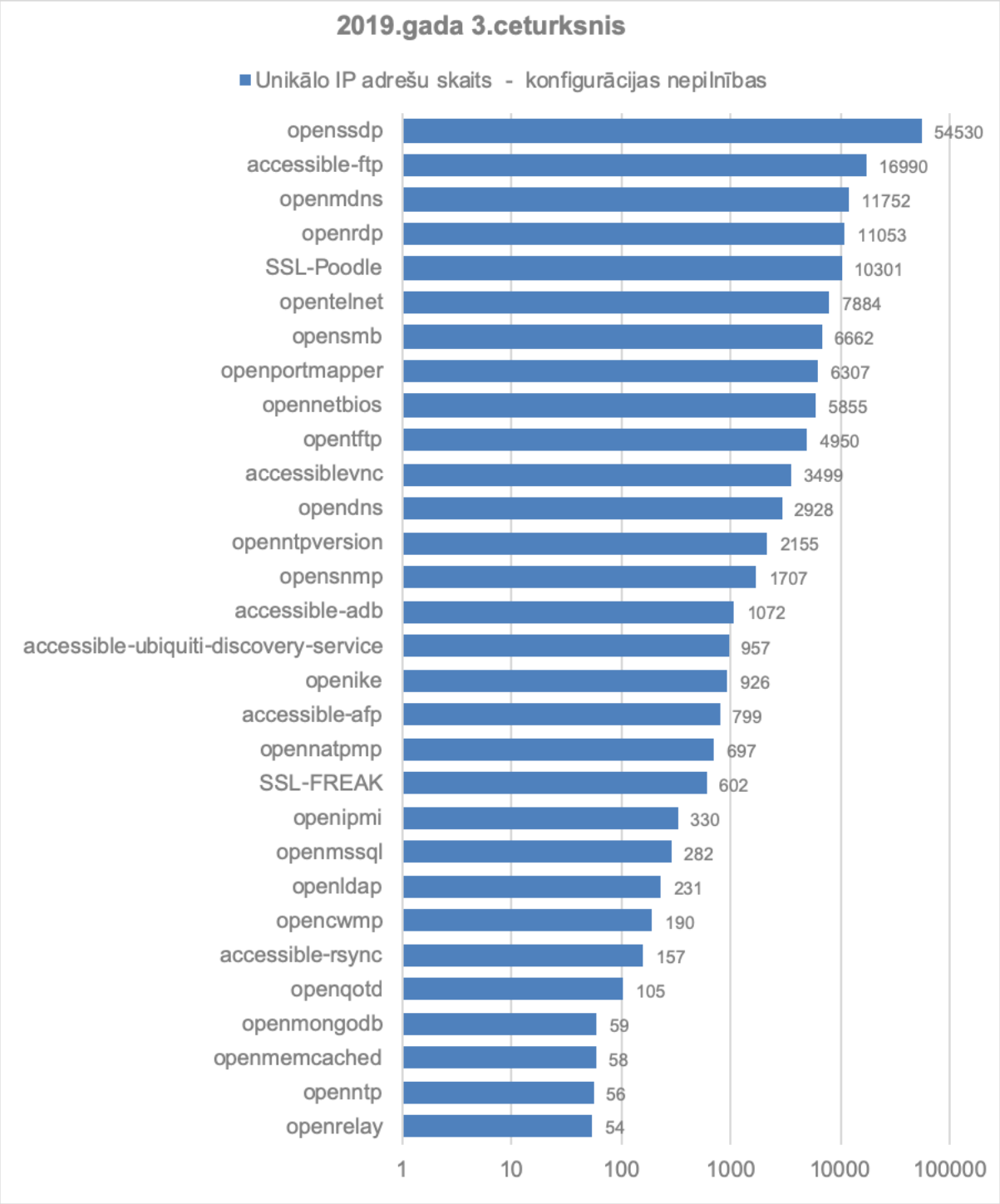
4.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2019. gada 3. ceturksnī ar apdraudējuma veidu - Ļaundabīgs kods.

Pirmo vietu ļaunatūras izplatības topā ieņem *Mirai* – ļaunatūra, kas inficē un iekļauj robotu tīklos jeb botnetos lietu interneta (IoT) iekārtas, lai izmantotu tās tālākiem uzbrukumiem un citām pretlikumīgām darbībām. Par uzbrucēju upuriem parasti kļūst iekārtas, kuras pēc iegādes pieslēgtas internetam, nenomainot ražotāja uzstādītos iestatījumus – noklusēto lietotājvārdu un paroli. Lai pasargātu sevi no lieka riska un līdzcilvēkus no papildu apdraudējuma, pirms jebkuras jaunas iekārtas pieslēgšanas internetam rūpīgi jāizvērtē, vai konkrētajai iekārtai šis pieslēgums tiešām ir nepieciešams? Ja tomēr ir, tad jāparūpējas par iekārtas drošību, vismaz nomainot noklusēto paroli.

Otro vietu topā ieņem ļaunatūra *WannaCry* (*WannaCrypt*), kas ir šifrējošais izspiedējvīruss, un, nonākot upura iekārtā, nošifrē iekārtas saturu, pieprasot samaksu par datu atgūšanu.

Topa trešajā vietā atrodas kompromitēti maršrutētāji (*routers*), kas nesalaboti, esot trešo pušu kontrolē, var tikt izmantoti pretlikumīgām darbībām, ilgstošai lietotāju informācijas nopludināšanai vai uzbrukumiem citām iekārtām un datortīkliem.

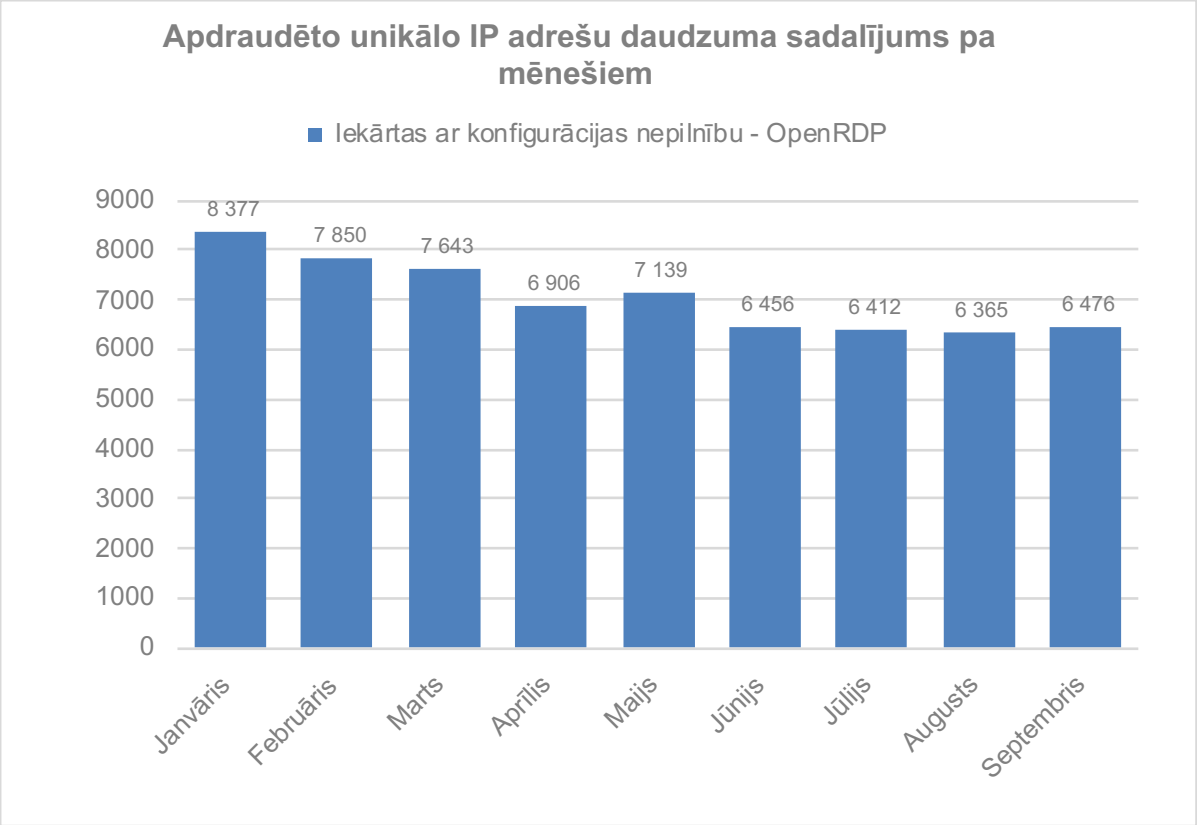
Ceturto vietu ļaunatūru topā joprojām notur *Conficker*, kaut arī tā ir jau sen pazīstama un salīdzinoši vienkārši „ārstējama" ļaunatūra. Šī indikācija vērojama tieši privātā sektorā un mājsaimniecībās, par ko CERT.LV regulāri informē elektronisko sakaru komersantus.



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

Konfigurācijas nepilnība *OpenRDP* pārskata periodā joprojām atrodas ceturtajā vieta. Tā bieži saistīta ar iekārtu un datu nesēju nošifrēšanu. Ja netiek ievērota labā prakse un netiek ierobežota piekļuve RDP servisam, piemēram, limitējot IP adreses, kurām atļauts pieslēgties, vai nosakot piekļuvi caur VPN, uzbrucējs var pārņemt kontroli pār neatbilstoši konfigurētām iekārtām, kurās attālinātās piekļuves porti ir brīvi atvērti uz internetu un nav pietiekami droša vai vispār nav uzstādīta piekļuves parole. Šādu gadījumu mazināšanai CERT.LV veica neatbilstoši konfigurēto iekārtu īpašnieku apziņošanu. Rezultātā potenciāli apdraudēto iekārtu apjoms ar atvērtu *Remote Desktop* servisu, lai arī lēnām, bet samazinājās (5.1. att.).



5.1.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2019. gada 1., 2. un 3. ceturksnī ar konfigurācijas nepilnību *OpenRDP*.

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.

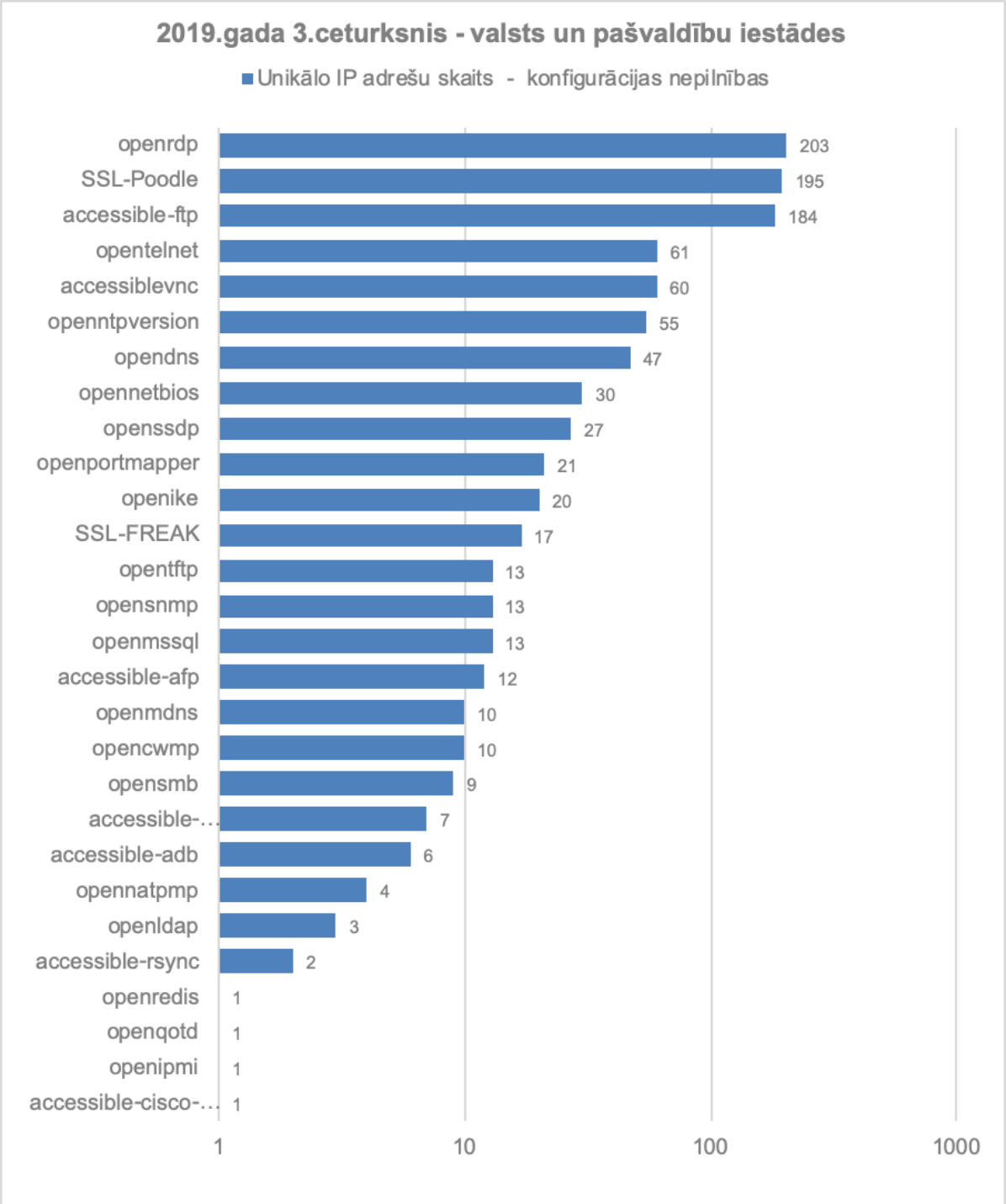
Lai aktualizētu sadarbību ar interneta pakalpojumu sniedzējiem un iniciatīvu "Atbildīgs interneta pakalpojumu sniedzējs", 31.oktobrī CERT.LV un LIA plāno rīkot semināru IPS pārstāvjiem, kurā informētu par sadarbības iespējām un izvērtētu abpusējus ieguvumus.

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 500 unikālas IP adreses dienā. Galvenokārt tās ir iekārtas, kuru konfigurācijā vērojamas nepilnības vai iekārtu konfigurācija neatbilst labajai praksei, pakļaujot tās uzbrukuma riskam un padarot par apdraudējumu vai nu pašam iekārtas lietotājam, piemēram, zaudējot datus, vai sabiedrībai kopumā, piemēram, iekārta var tikt izmantota uzbrukumā citām iekārtām.

6.attēls - CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2019.gada 3.ceturksnī ar apdraudējuma veidu – ļaundabīgs kods.



7.attēls - CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2019.gada 3. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

CERT.LV uzskaita arī kompromitēto un izķēmoto tīmekļa vietņu gadījumus. Pārskata periodā tika fiksētas 17 kompromitētas un izķēmotas tīmekļa vietnes. 12 gadījumos izķēmotās vietnes uzturēšanai tika izmantota Linux operētājsistēma, bet 5 gadījumos - Windows. Neviena no izķēmotajām vietnēm pēdējā gada laikā nav tikusi izķēmotas atkārtoti.

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

Krāpšana

Tika saņemts ziņojums no kādas ceļojumu aģentūras, kas cieta zaudējumus 12 336 eiro apmērā, veicot viesnīcas rezervāciju Grieķijā. Grieķu sadarbības partnera e-pasta konts tika uzlauzts un viesnīcas vārdā komunikāciju veica krāpnieki, pieprasot maksājumu uz sev piederošu kontu. Ceļojumu aģentūra vērsās ar iesniegumu bankā un Valsts policijā. CERT.LV ieteica pārbaudīt maksājumus, verificējot tos ar telefona zvanu.

Tika saņemts ziņojums par darījumu sarakstes kompromitēšanu un mēģinājumu Latvijas uzņēmuma ārvalstu sadarbības partnerim nosūtīt viltotu rēķinu, taču partneris laicīgi pamanīja neatbilstošo e-pasta adresi - darbinieks@uzņēmums.com nevis darbinieks@uzņēmums.lv.

CEO krāpšanas mēģinājumi, kurā uzņēmuma vai iestādes finanšu darbiniekam tiek nosūtīts e-pasts it kā vadītāja vārdā ar lūgumu veikt pārskaitījumu, tika vērsts pret vairākiem uzņēmumiem un valsts iestādēm. Vienas kampaņas raksturīga inovatīva iezīme – From adresē "@" zīme tika aizvietota ar "©" Copyright zīmi, kas ir vizuāli līdzīga, bet, iespējams, ļauj apiet dažus e-pasta filtrus.

Vairāki uzņēmumi saņēma maldinošu paziņojumu, kas tika noformēts kā brīdinājums par domēna vārda reģistrācijas termiņa pagarināšanas nepieciešamību, bet patiesībā mēģināja pārdot SEO (*Search Engine Optimization*) pakalpojumus.

Tika saņemts ziņojums par krāpšanu, kuras rezultātā upuris cieta zaudējumus 101 eiro apmērā un piedzīvoja mēģinājumu izkrāpt vēl 189 eiro. Krāpnieki uzdevās par aizdevumu kompāniju, kas uztur vietni sociālajā tīklā Facebook un komunicē, izmantojot WhatsApp un Gmail. Pirms aizdevuma izsniegšanas tika pieprasīts maksājums (kas tika samaksāts), kuram sekoja apdrošināšanas maksājuma pieprasījums. Pēc otrā maksājuma pieprasījuma upuris draudēja ziņot par krāpšanu; krāpnieki pārtrauca komunikāciju un vietni Facebook sociālajā tīklā dzēsa.

Tika saņemta virkne ziņojumu, kuros upuriem tika izteikti draudi un pieprasīta samaksa par kompromitējoša video neizplatīšanu. Dažos gadījumos kā “pierādījums” tam, ka uzbrucējs tiešām ir “uzlauzis” upura iekārtu, tika minēta viena vai pat vairākas upura lietotas paroles, kas patiesībā iegūtas kādā no internetā publicētām datu noplūdēm. Vairākumā gadījumu uzbrucējs izvēlējās neizmantot papildu pārliecināšanas metodes, cerot, ka iebiedēšana ar video esamību būs pietiekami efektīva. Atsevišķos gadījumos e-pastā tika izmantota uzsvērti agresīva runas maniere, lai demonstrētu saņēmējam uzbrucēja pārliecinātību par savu rīcību.

Vairākos gadījumos e-pasta saņēmējam tika izteikti aicinājumi sniegt atbalstu investīciju operācijās, iesaistīties finanšu darījumos, kas potenciālā partnera mītnes zemē nav atļauti, saņemt mantojumu, ziedojumu, vinnestu loterijā vai kompensāciju, kas dažādu pasaulē populāru organizāciju, piemēram, Starptautiskā Valūtas fonda, vārdā tiek piesolīta interneta krāpšanās cietušiem upuriem. Paziņojumus par laimestu loterijā ar pievienotu saiti lietotāji saņēma arī īsziņu formātā.

Raksturīgās krāpniecisko e-pastu iezīmes: aicinājums neizpaust e-pasta saņemšanas faktu citiem (ar aizbildinājumu, ka citi varētu gribēt labumu iegūt sev), tiek minētas milzīgas naudas summas un pieprasīti salīdzinoši nelieli maksājumi (jurista apmaksai, transporta izdevumiem, apdrošināšanas maksājumam, bankas komisijai u.t.t.) šo lielo summu iegūšanai, bieži tiek dots limitēts laika posms, kurā prasīto izpildīt.

Paziņojumi par loterijām tika izplatīti arī Latvijas uzņēmumu vārdā. „Latvijas pasts" vārdā izplatītajā loterijā lietotāji tika aicināti aizpildīt īsu anketu, lai it kā laimētu Samsung Galaxy S10 viedtālruni. Aizpildot anketu, lietotājs patiesībā parakstījās uz maksas pakalpojumu. Tika saņemts arī ziņojums no viena cietušā, kurš zaudēja 3.61 eiro Google vārdā izplatītā loterijā, cerot vinnēt viedtālruni.

Tika saņemts ziņojums par krāpniecības mēģinājumu kādā iepazīšanās vietnē, kurā vīrietis uzdevās par amerikāņu karavīru, apgalvojot, ka romantisku jūtu vadīts vēlas tikties, bet tam nepieciešams atvaļinājums, un aicinājis sievieti nosūtīt ziņu norādītajā vietnē, kur tika pieprasīts arī maksājums. Sieviete atpazina krāpšanu un to pauda. Sievietei tika izteikti draudi, sākās svešu cilvēku uzmācīga izturēšanās sociālajā vietnē Facebook. CERT.LV ieteica pārtraukt saziņu ar svešiniekiem un padarīt profilu pieejamu tikai draugiem.

Tika saņemts ziņojums par negodprātīgu sociālā tīkla Facebook reklāmu, kurā reklāmdevējs reklamējās kā leģitīms ziņu portāls, bet lietotāji tika pārvirzīti uz vietni, kur it kā varēja laimēt viedtālruni par 1 USD, bet patiesībā tika veikta parakstīšanās uz maksas tiešsaistes servisiem, piemēram, nepieprasītas informācijas regulāru saņemšanu vai kādas vietnes piekļuves abonēšanu.

Tika saņemta informācija par krāpnieciskām darbībām ar neskaidru motivāciju. Krāpnieks uzsācis un uzturējis kontaktu ar upuri internetā vairāk kā 3 mēnešus. Tad paziņojis, ka nepieciešama palīdzība piekļūt internetbankai, jo viņa atrašanās vietā esot pārāk slikts interneta pieslēgums (bet instrukcijas tika sniegtas, izmantojot Skype), un nodevis upurim savas internetbankas piekļuves datus un lūdzis veikt vairākus pārskaitījumus, no kuriem viens bijis veiksmīgs, bet atlikušie divi neveiksmīgi, tehniskas kļūmes dēļ. Norādītā internetbankas vietne izrādījusies viltota, bet veiktie pārskaitījumi – simulācija. Upuris atpazina krāpniecisko darbību pazīmes, un informāciju iesniedza policijā. Iespējams, krāpnieki centās pārliecināt upuri par savu finansiālo nodrošinātību, lai vēlāk lūgtu veikt kādu darījumu no upura konta, vai arī aicinātu upuri veikt pārskaitījum no kāda uzlauzta konta, tādejādi iesaistot upuri likumpārkāpumā.

Tika konstatēta kādu portālu imitējoša vietne, kas nesaskaņoti izmantoja Latvijas slavenības un to attēlus, lai reklamētu investīcijas kriptovalūtā, nepatiesi norādot, ka slavenības to jau ir izdarījušas, guvušas peļņu un rekomendē citiem.

Pikšķerēšana jeb personīgo datu izkrāpšana

Tika saņemta informācija par vairākām uzlauztām .lv vietnēm un Latvijas IP adresēm, kurās tika izvietota pikšķerēšana, kas vērsta uz Apple, Facebook, Clarks, Bank of America, UniCredit, BNP Paribas.Net, Virgin Media, BAWAG P.S.K., SNB Bank, Linkedin, bet lielākoties Microsoft klientiem.

Tika saņemti vairāki ziņojumi par PayPal piekļuves datu izkrāpšanas mēģinājumiem. Vienā no PayPal pikšķerēšanas gadījumiem tika atsūtīts paziņojums, kurā norādīta sveša e-pasta adrese un jautājums, vai lietotājs ir vēlējies padarīt šo e-pasta adresi par primāro un turpmāk saņemt visu informāciju uz šo adresi. Ja jā, lietotājs aicināts sekot saitei un apstiprināt izvēli. Savukārt, ja lietotājs nav veicis adreses maiņas pieprasījumu, seko aicinājums sekot saitei un ziņot par neautorizētu mēģinājumu, lai veicinātu konta drošību. Abas e-pastā norādītās saites ved uz konta piekļuves datu izkrāpšanas vietni.

Citos gadījumos lietotājs brīdināts par neautorizētām darbībām kontā vai informēts par it kā saņemtu maksājumu, arī atsaucoties uz upura internetā izvietotu pārdošanas sludinājumu, padarot krāpšanu ticamāku.

Brīdinot par neautorizētām darbībām kontā un aicinot verificēt kontu, mēģināts izkrāpt arī Amazon un e-pasta piekļuves datus.

Virknē e-pasta piekļuves datu pikšķerēšanas mēģinājumu lietotājs tika informēts par potenciālajiem sarežģījumiem – nespēju saņemt ziņojumus, piekļūt sarakstēm, pielikumiem, kontam -, ja netiks uzstādīti atjauninājumi vai verificēts konts, sekojot saitei.

Tika saņemts ziņojums par Facebook piekļuves datu izkrāpšanas mēģinājums, publicējot ziņu par traģisku negadījumu un saiti, ar lūgumu pierakstīties grupā, lai veiktu upuru identifikāciju.

Visa pārskata perioda garumā intensīvi turpinājās Smart-ID un internetbanku piekļuves datu izkrāpšanas kampaņas.

Jūlija beigās tika saņemts ziņojums par pikšķerēšanas kampaņu, kas bija paredzēta internetbankas piekļuves datu izkrāpšanai. Kampaņas ietvaros tika izsūtītas krāpnieciskas SMS ar saiti (izmantots saites saīsinātājserviss), aicinot atjaunot datus un pieslēgties internetbankai, izmantojot Smart-ID. Nedēļu vēlāk sekoja kaitīgu e-pastu vilnis. E-pasts aicināja saņēmēju atjaunināt paroli, sekojot saitei, un bija paredzēti internetbankas piekļuves datu izkrāpšanai.

Augusta sākumā sekoja vēl viens kaitīgu e-pastu vilnis ar aicinājumu sekot saitei, lai atvērtu divus tiešsaistē esošus dokumentus.

Augusta vidū sekoja vēl viena pikšķerēšanas e-pastu kampaņa, aicinot atjaunot savu paroli norādītajā saitē. Pēc nedēļas notika nākamā pikšķerēšanas kampaņa, izsūtot e-pastus ar informāciju par daudzu klientu saņemtajām sūdzībām un nepieciešamību pārbaudīt sava Smart-ID darbību.

Augusta otrajā pusē kādas bankas vārdā tika izplatītas krāpnieciskas īsziņas lietuviešu valodā par it kā saņemtu maksājumu un pievienotu saīsinātu saiti internetbankas piekļuves datu izkrāpšanai.

Septembra sākumā atkal tika veikta pikšķerēšana, aicinot sekot saitei, jo daudzi klienti esot ziņojuši par datu noplūdi trešajām personām un ir ieviesti jauni Smart-ID drošības pasākumi. Saņēmēji tika aicināti pārliecināties, ka arī viņu kontā šie drošības pasākumi ir aktivizēti.

Septembrī tika fiksētas vēl divas pikšķerēšanas kampaņas. Vienā lietotāji saņēma aicinājumu aplūkot 2 tiešsaistes dokumentus, sekojot saitei. Kampaņa tika paredzēta internetbankas piekļuves datu izkrāpšanai. Otrā kampaņā izplatītajos pikšķerēšanas e-pastos lietotāji tika informēti, ka banka veikusi drošības pārbaudes, un tika aicināti pārbaudīt savu kontu informāciju, vai tā nav tikusi apdraudēta.

Gan bankas, gan CERT.LV izplatīja informatīvus materiālus par internetbanku piekļuves datu izkrāpšanas kampaņām un centās vērst uzmanību uz galvenajām pazīmēm, kas liecina, ka ziņojums ir krāpšana: banka saziņai ar klientu nesūtīs e-pastu vai sms, kā arī, veicot bankas darbību apstiprinājumus, jāpievērš uzmanība informatīvajam tekstam, kas norāda, kāda darbība tiks apstiprināta.

Pakalpojuma pieejamība (DDoS)

Tika saņemts ziņojums par īslaicīgu DDoS uzbrukumu kādam portālam. Uzbrukums tika sekmīgi atvairīts. Portāls piedzīvoja UDP/ LDAP amplifikācijas tipa uzbrukumu, kas varētu nozīmēt arī to, ka pats portāls nebija mērķis, bet tika izmantots uzbrukumā kādam citam resursam.

Septembrī tika saņemts lūgums no Čehijas CERT vienības novērst ilgstošu SYN flood DDoS uzbrukumu resursam Čehijā. Uzbrukumā tika iesaistītas arī Latvijas IP adreses. Tika izsūtīti ziņojumi iesaistīto iekārtu uzturētājiem.

Tika saņemts lūgums no Somijas CERT vienības palīdzēt identificēt iekārtu, kas iesaistīta DDoS uzbrukumā pret resursiem Somijā, un novērst apdraudējumu. Iesaistītās iekārtas uzturētājs tika apzināts un informēts.

Tika saņemts ziņojums par aplikācijas līmeņa (L7) uzbrukumu kādas valsts iestādes resursam. Četru dienu laikā tika iesūtīti aptuveni 1.5 miljoni neleģitīmi pieprasījumi, taču pieprasījumu jauda bija neliela un sākotnēji tie netika bloķēti kā DDoS. Tika veikts mēģinājums atslēgt uzbrucēju IP adreses līmenī, taču uzbrucējs mainīja IP adresi. Resursam tika pieslēgts WAF (*Web Application Firewall*) pakalpojums, un sākta neleģitīmo L7 pieprasījumu bloķēšana.

Ļaundabīgs kods

Ļaunatūra tika izplatīta diviem mērķiem – lai iegūtu informāciju un gūtu peļņu. Informācijas gūšanai tika izplatīta spiegojošā ļaunatūra, kas nosūtīja upura iekārtā iegūtos datus, piemēram, paroles, uzbrucējam. Peļņas gūšanai tika izplatīti šifrējošie izspiedējvīrusi, kuru uzbrukuma rezultātā dati upura iekārtā tika nošifrēti, un datu atgūšanai tika pieprasīta izpirkuma maksa, kuras lielums bieži vien bija atkarīgs no tā, vai nošifrētā iekārta ir darbstacija vai serveris, vai cietušais ir uzņēmums vai privātpersona, vai nošifrētie dati ir dokumenti vai datubāzes – jo svarīgāki dati, jo augstāka cena.

Ļaunatūras izplatīšanai uzbrucēji izvēlējās galvenokārt e-pastu ar kaitīgu pielikumu (.PDF, .ZIP, .DOC, .IMG u.c.), e-pasta tēmu izvēloties tādu, lai pielikums šķistu pašsaprotams, piemēram, preču vai materiālu saraksts piedāvājuma, pasūtījuma vai piegādes gadījumā, neapmaksāts rēķins par piegādi, maksājuma uzdevums informācijas saskaņošanai, informācija no kurjerkompānijas par neveiksmīgu piegādi.

Pielikumu nosaukumi tika veidoti tā, lai maksimāli slēptu patieso pielikuma paplašinājumu, piemēram, PO#august_pdf.img kurā .IMG fails tiek maskēts par .PDF.

Tika saņemta informācija no Somijas Nacionālā kiberdrošības centra (NCSC) par *Stealth worker* ļaunatūras darbību, un identificētas Latvijā uzturētas tīmekļa vietnes, kuras ir tikušas uzlauztas un kurās ievietoti potenciāli ļaundabīgi faili. Vietņu uzturētāji tika apzināti, un abpusējā sadarbībā tika uzsākts darbs pie problēmas novēršanas, kā arī iegūts materiāls papildu izpētei.

Septembra otrajā pusē tika saņemta informācija par e-pasta kampaņu "Latvijas pasts" vārdā. E-pastā tika paziņots par nepiegādātu paciņu nepareizas adreses dēļ. Lai saņemtu paciņu, upuris tika aicināts atvērt un izdrukāt pielikumu, un doties uz tuvāko pasta nodaļu. Pielikumā atradās .r11 arhīva fails, kas savukārt saturēja Nanocore Rat ļaunatūru, kas ļautu uzbrucējam iegūt pastāvīgu piekļuvi upura datoram. Par ļaundabīgajiem e-pastiem tika informēta sabiedrība.

Tika saņemts lūgums no Slovēnijas CERT vienības SI-CERT sniegt informāciju par Latvijā uzturētu iekārtu, kas tika izmantota ļaunatūras izplatīšanai. Slovēnijas banku klienti bija saņēmuši e-pastus ar kaitīgu Javascript pielikumu, kura aktivizācija ļautu uzbrucējam iegūt informāciju par upura iekārtu un izpildīt tajā jebkuru saiti (URL), kas tiktu sniegta kā atbilde. CERT.LV lūdza papildu informāciju par iekārtas aktivitātēm, lai iesaistītu policiju.

Ielaušanās mēģinājumi

Tika saņemti ziņojumi par aplikācijas līmeņa (L7) uzbrukumiem un SQL injekciju mēģinājumiem vairāku valsts iestāžu resursiem. Dažos gadījumos tika izpildīti mēģinājumi veikt arī starpvietņu skriptēšanu (XSS) un veikta ievainojamību meklēšana. Katrā uzbrukumā tika iesūtīti vairāki desmiti tūkstoši neleģitīmu pieprasījumu. Lielākoties uzbrukumi tika veiksmīgi atvairīti. Vienā no gadījumiem uzbrukums netika pilnīgi atvairīts, jo resursam nebija ieviests WAF (*Web Application Firewall*) pakalpojums. Arī uz pārskata beigām šis pakalpojums bija ieviešanas stadijā, risinot iespējamo nepamatoti bloķēto (*false positive*) gadījumu jautājumu.

Tika saņemta informācija no kādas valsts iestādes par ielaušanās mēģinājumiem e-pasta sistēmā. Uzbrukuma rezultātā 20 e-pasta konti tika bloķēti.

Tika saņemts ziņojums, ka 12 dienu garumā uzbrucēji mēģināja pieslēgties un izsūtīt e-pastus no kādas valsts iestādes resursiem. Izmantotas gan eksistējošas, gan ģenerētas e-pasta adreses. Uzbrukumi veikti no vairāk nekā 2000 IP adresēm, ģenerējot gandrīz 145 000 pieprasījumus. Uzbrukums traucējumus e-pasta sistēmas darbībā neradīja, kaitīgās vēstules līdz lietotājiem nenonāca.

Kompromitētas iekārtas un datu noplūdes

Tika saņemta informācija par kompromitētu kādas pašvaldības darbinieka kontu, no kura tika izsūtīti pikšķerēšanas e-pasti it kā Microsoft vārdā tālākai e-pasta piekļuves datu izkrāpšanai. E-pasta uzturētāji tika informēti. Tika konstatēts, ka lietotājs bija kļuvis par pikšķerēšanas upuri.

Tika saņemta informācija par kiberuzbrukumu kādam uzņēmumam. Uzbrukums tika veikts, uzminot paroli attālinātās piekļuves servisam RDP, kas bija “password”. Vīruss nošifrēja visus datus serverī, tīkla diskos un pievienotajās darbstacijās. Uz incidenta brīdi atšifrēšanas rīks konkrētajam vīrusa paveidam nebija pieejams. Uzņēmums nebija sagatavojis datu rezerves kopijas. Pamatojoties uz zaudējumiem, CERT.LV ieteica uzņēmumam vērsties ar iesniegumu policijā.

Tika saņemts ziņojums par kompromitētu kādas valsts iestādes darbinieka Office 365 kontu. Izmantojot iegūto pieeju, tika izsūtīti pikšķerēšanas e-pasti ar saiti ārējiem kontaktiem, kā arī veikta vairāku dokumentu lejuplāde. Kaitīgā e-pasta saņēmēji tika brīdināti; pēc lejuplādēto dokumentu pārbaudes tika secināts, ka tie bija publiskojami dokumenti. Konta paroli uzbrucēji, iespējams, ieguva pikšķerēšanas ceļā, bet otro autentifikācijas faktoru apgāja, izpildot procedūru laikā, piemēram, naktī, kad lietotājs nevelta pietiekamu uzmanību atbilstošai situācijas izvērtēšanai un pietiekami neiedziļinās notiekošajā procesā, kā rezultātā, saņemot pārbaudes zvanu vai īsziņu, veic automātisku apstiprināšanu. Lietotāja piekļuves dati tika nomainīti.

Tika saņemta informācija no kādas valsts iestādes par ārējās ietekmes pazīmēm iestādes informācijas sistēmā. Lai novērstu turpmākus draudus sistēmai, tika pieņemts lēmums izslēgt

visus fiziskos serverus un atslēgt tīkla infrastruktūru. Izpētes rezultātā tika konstatēts, ka uzbrucēji veikuši paroles piemeklēšanu RDP servisam, un uzbrukuma rezultātā veikuši divu serveru un domēna kontroliera kompromitēšanu. Datu bojājumi vai zudumi netika izraisīti, netika konstatēta arī piekļuve tiem. Pēc situācijas analīzes tika atjaunota sistēmas darbība un veikta drošības pasākumu uzlabošana.

Ievainojamības

Tika saņemta informācija par to, ka kāda veselības aprūpes iestāde izsūta e-pastus ar klientu izmeklējumu datiem nešifrētā veidā, kas ļauj uzbrucējam pārtvert sūtījumu un izgūt sūtītos datus. Veselības aprūpes iestāde tika informēta par apdraudējumu, un aicināta ievērot labo praksi.

Atbildīgas ievainojamību atklāšanas ietvaros tika saņemti ziņojumi par starpvietņu skriptēšanas (XSS) ievainojamībām vairāku valsts iestāžu vietnēs. Ievainojamo vietņu uzturētāji tika informēti; ievainojamību informācijas iesniedzējiem tika nosūtīti pateicības raksti.

Ielaušanās testi

Tika veikti ielaušanās testi kādas valsts iestādes informācijas sistēmai. Veicot testus, kritiska riska ievainojamības netika atrastas, bet tika konstatēta augsta riska starpvietņu skriptēšanas ievainojamība (XSS) un sensitīvas informācijas atkāšana vietnes kļūdu paziņojumos. CERT.LV sniedza rekomendācijas drošības līmeņa uzlabošanai.

Tika veikti vēl vairāki valsts iestāžu tīmekļa vietņu ielaušanās testi. Nevienā no vietnēm kritiskas un augsta riska ievainojamības netika konstatētas. Dažās tika konstatētas vidēja riska XSS ievainojamības, kas veiksmīga uzbrukuma gadījumā ļautu pārtvert lietotāja sesiju. Kopumā tika sniegti ieteikumi par labās prakses ievērošanu un drošības līmeņa paaugstināšanu.

CERT.LV pasākumi incidentu novēršanā:

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

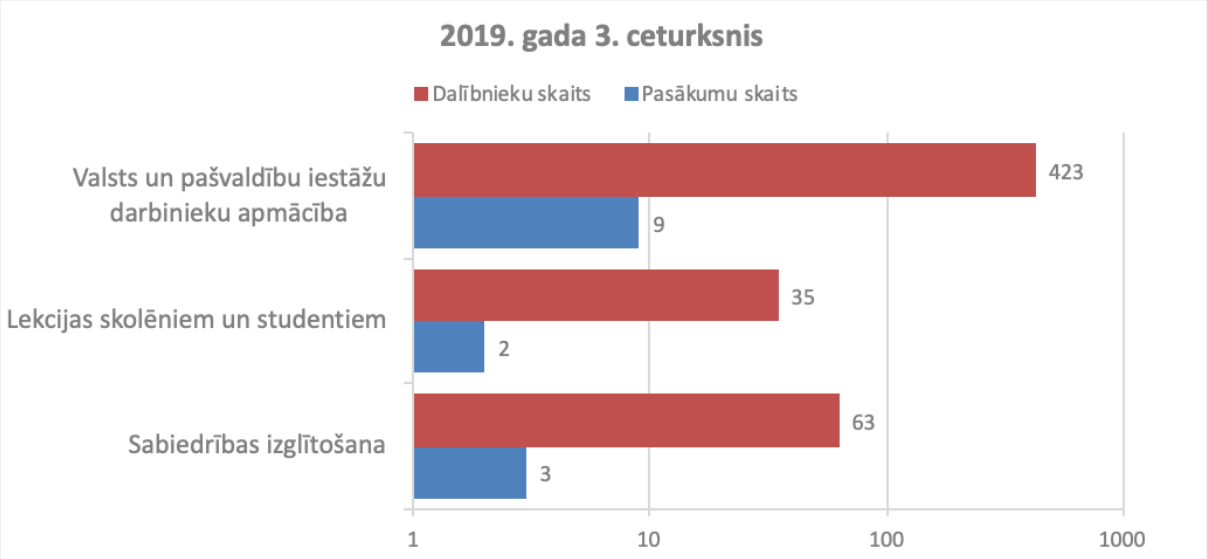
Cita veida sadarbība ar dažādām iestādēm ir norādīta atskaites 4. punktā.

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

20. augustā CERT.LV pārstāvis piedalījās Drossinternets.lv organizētajās apmācībās Drošāka interneta vēstnešiem, stāstot par krāpšanu internetā un citiem apdraudējumiem. Drošāka interneta vēstneses katra savā novadā aktīvi darbojas, lai veicinātu drošāku interneta lietošanu ciema, pilsētas un novada iedzīvotāju vidū, protams, īpašu uzmanību veltot tieši bērnu izglītošanai par drošu un atbildīgu moderno tehnoloģiju izmantošanu.

24. septembrī CERT.LV pārstāvis kopā ar NIC.lv pārstāvi vadīja semināru “Kā uzņēmējam viegli (ne)pazaudēt naudu kibertelpā?” Latvijas Tirdzniecības un rūpniecības kameras biedriem Valmierā. Semināra mērķauditorija primāri bija mazie un vidējie uzņēmumi, kuri pēdējo divu gadu laikā arvien biežāk kļūst par kiberuzbrukumu upuriem. Seminārā tika aplūkota virkne vienkāršu darbību, kas palīdzētu izvairīties no apdraudējumiem.

Pārskata periodā CERT.LV par IT drošību izglītoja 521 cilvēku, iesaistoties 14 izglītojošos pasākumos.



9.attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2019. gada 3. ceturksnī

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

Sadarbības tikšanās, konsultācijas un prezentācijas:

- Tika veidota ciešāka sadarbība ar valsts nozīmīgākajiem interneta pakalpojumu sniedzējiem informācijas apmaiņas veicināšanai.
- Tika veikta Valsts policijas iesniegto materiālu izpēte un sagatavoti ziņojumi par veiktās analīzes rezultātiem .

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. Šie pienākumi noslēdzās 58. TF-CSIRT sanāksmē, kas notika Kiprā 16.-17. septembrī.
- 3. – 7. jūlijā Portugālē notika ECCWS2019 akadēmiskā konference, kurā CERT.LV pārstāvis prezentēja publikāciju “Crossed Swords: A Cyber Red Team Oriented Technical Exercise”.
- 9. – 10. septembrī NIS direktīvas CERTu tīkla ietvarā notika CERT komandu savstarpējie auditi (peer review). CERT.LV pārstāvis viesojās Viļņā un veica auditu CERT-LT komandai.

- 11. – 12. septembrī CERT.LV komanda piedalījās OAS (Organization of American States), INCIBE (Spanish National Cybersecurity Institute) un CNPIC (Spanish National Centre for Infrastructure and Cybersecurity) organizētajās starptautiskajās kiberdrošības mācībās CyberEx 2019, kurās 87 komandu konkurencē ieguva 16. vietu. Mācību mērķis ir stiprināt dalībnieku spēju reaģēt uz kiberdrošības incidentiem, veicinot sadarbību šādu incidentu risināšanā.
- 14. – 19. septembrī Kiprā notika 58. TF-CSIRT sanāksme, kuras ietvaros CERT.LV pārstāvji sniedza prezentāciju par robotu tīkla (botnet) izpēti, piedalījās paneļdiskusijā "Incident Response Landscape 2025 and beyond" un vadīja pirmreizējo sanāksmi CSIRT komandu komunikāciju speciālistiem "PR and Communications Working Group".
- Septembrī CERT.LV pārstāvis piedalījās Eiropas Komisijas organizētā aptaujā "Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment", paužot viedokli, ka drošības līmenis paaugstinātos, ja tiktu implementētas pamata drošības funkcijas autentifikācija, identifikācija un integritāte, ņemot vērā, ka drošība nedrīkst būt papildu lieta, bet gan produktos iebūvēta pamata funkcija. Papildu tika ierosināts ieviest dzīves cikla pārraudzību un ražotāja atbildību produkta drošības atjauninājumu uzturēšanai. Tika uzsvērts, ka nav nepieciešama papildu regulējuma izstrāde, bet veicama sadarbība ar industriju un iesaistīšanās industrijas standartu izstrādē, pozicionējot Latvijas iniciatīvu "Atbildīgs interneta pakalpojumu sniedzējs" kā labo praksi".

Sadarbība konkrētu incidentu risināšanā aplūkota pārskata 2. punktā.

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

Turpinājās 2018. gada 1.septembrī CERT.LV uzsāktā 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) īstenošana.

Darbs turpinājās visās sešās projektā definētajās darba pakās:

- Tika turpināta "Deep Analysis System" izstrāde, gatavojoties nākamajā gadā paredzētajai beta versijas publiskošanai.
- 15. – 17. jūlijā Rīgā notika MeliCERTes – Cybersecurity Core Service Platform – mācības, kurās piedalījās CERTu tīkla un CEF projekta pārstāvji no dažādām Eiropas valstīm. Mācību mērķis bija iepazīstināt jaunos lietotājus ar MeliCERTes darbību, praktiski demonstrējot platformas darbību un izspēlējot dažādus starpvalstu sadarbības scenārijus gan teorētiski, gan praktiski, izmantojot platformu. Mācību laikā Rīgā CERT.LV tika aktivizēta projektā pirmā pilnvērtīgi strādājoša MeliCERTes instance.
- Ar projekta atbalstu notika darbs pie kiberdrošības konferences "Kiberšahs 2019" organizēšanas. Konferences norises nodrošināšanai pārskata periodā tika izsludināts publisks iepirkums ar sarunu procedūru "Telpu, ēdināšanas un tehniskās aparatūras nodrošinājums konferencei "Kiberšahs 2019"". Konkursā uzvarēja Radisson Blu Latvija Conference & Spa Hotel. Ceturksnī notika aktīvs darbs pie konferences

programmas, vizuālās identitātes un dalībnieku reģistrācijas sistēmas izstrādes. Informācija par konferences norisi tiks iekļauta nākamajā atskaitē.

- Projekta ietvaros paredzēts organizēt sabiedrību izglītojošu kampaņu un pārskata periodā tika uzsākta iepirkuma procedūra kampaņai "Informācijas tehnoloģiju drošība darbavietā". Tika realizēta iepirkuma pirmā kārta, un turpinās darbs pie kandidātu izvērtēšanas. Plānotais kampaņas norises laiks ir 2020.gada 1./2. ceturksnis.
- Sagatavota un iesniegta sešu mēnešu informatīvā projekta progresa atskaite Eiropas Komisijai.

7. Projekta "Cyber Exchange" īstenošana

Turpinājās 2018. gada 1.novembrī CERT.LV uzsāktā 2017 CEF Telecom-Cyber Security uzsaukumā apstiprinātā projekta "Cyber Exchange" (līguma ar Eiropas Komisiju Nr. INEA/CEF/ICT/A2017/1528866) (turpmāk – Sadarbības projekts) īstenošana.

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 3. ceturksnī projekta ietvaros CERT.LV pārstāvis viesojās CIRCL, Luksemburgā, kur tikās ar plaši izmantotās platformas MISP (*Malware Information Sharing Platform*) izstrādātājiem, gūstot vērtīgu pieredzi darbam ar platformu, sniedzot atgriezenisko saiti platformas izmantošanā un saņemot padomus no ārvalstu kolēģiem platformas efektīvākai lietošanai. Apmaiņas vizīte veicināja platformas funkcionalitātes paplašināšanu. Paralēli tika iepazīti arī jauni rīki, kuri sniegs iespēju pilnveidot CERT.LV ikdienas darbu.

13. – 15. augustā Latviju apmeklēja projekta koordinatori no CSIRT.CZ (Čehija), lai tiktos ar CERT.LV, NIC.LV un Latvijas Drošāka interneta centra pārstāvjiem, veicot informācijas apmaiņu par izglītojošu kampaņu sociālo mediju stratēģijām, CSIRT komandu sabiedrisko attiecību speciālistu starptautisko sadarbību un Čehijas CSIRT vienības izstrādātās izglītojošās spēles lokalizācijas iespējām.

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 īstenošanas. 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.
- Pārskata periodā tika aktualizēts jautājums par iniciatīvu "Atbildīgs interneta pakalpojumu sniedzējs", tiekoties ar LIA (Latvijas Interneta asociācija), tika atjaunots sadarbības memorands, un plānota jaunu dalībnieku piesaiste. 31.oktobrī tiks organizēts informatīvs seminārs interneta pakalpojumu sniedzējiem.

- TF-CSIRT sanāksmes ietvaros CERT.LV svinīgā ceremonijā saņēma arī TI (Trusted Introducer) sertifikātu par veiksmīgi izietu re-sertifikācijas procesu (tā jāatjauno ik pēc 3 gadiem). CERT.LV jau kopš 2016.gada ir viena no 26 Eiropas TF–CSIRT/Trusted Introducer sertificētajām komandām, kas apliecina CERT.LV komandas augsto brieduma un sagatavotības līmeni.
- 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 veica institūcijai uzticētos pienākumus.

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 01.07.2019. līdz 30.09.2019. ir saņēmusi un izvērtējusi 1313 ziņojumus. No tiem 1188 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 16 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 23 ziņojumos konstatēta personas goda un cieņas aizskaršana un 3 ziņojumi par vardarbību atainojošiem materiāliem. Par finanšu krāpšanas mēģinājumiem internetā saņemti 31 ziņojumi, 15 ziņojumu saturs nav bijis pretlikumīgs, 37 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 1180 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 9 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 internetā.

Pārskata periodā no Latvijā uzturētajiem 1180 ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem 1119 ziņojumu saturs ir dzēsts no publiskas aprites un 61 ziņojuma saturs atrodas dzēšanas procesā sadarbībā ar Valsts policiju un interneta pakalpojumu sniedzējiem.

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