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 2. ceturksnis (01.04.2019. – 30.06.2019.)

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 2. ceturksnī tika reģistrētas 246 656 unikālas apdraudētas IP adreses, kas ir par 28% vairāk nekā iepriekšējā ceturksnī un par 35% vairāk nekā šajā pašā periodā pirms gada.

Kopējais ceturkšņa pieaugums skaidrojams ar vienreizēju kampaņveidīgu aktivitāti viena datu avota ietvaros. Attiecīgā aktivitāte aptvēra uz internetu atvērtu iekārtu/ maršrutētāju apzināšanu, neveicot papildu izpēti par šīm iekārtām. Rezultātā iegūta apjomīga datu kopa (vairāk nekā 48,8 tk. unikālu IP adrešu), taču iegūtā informācija neļauj izdarīt viennozīmīgus secinājumus par šo iekārtu apdraudējumu.

Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (130 096 unikālas IP adreses) ar kritumu 5% pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs kods (17 907 unikālas IP adreses) ar kritumu 10%, bet trešais - ielaušanās mēģinājumi (2436 unikālas IP adreses) ar kritumu 22%.

CERT.LV apziņošanas aktivitāšu rezultātā lēnām krītas potenciāli apdraudēto iekārtu skaits ar uz internetu atvērtu attālinātās piekļuves servisu (*Remote Desktop* jeb RDP), kas pēdējā gada laikā ir bijis par iemeslu daudziem iekārtu un sistēmu nošifrēšanas gadījumiem.

Turpinās krāpniecisku e-pastu kampaņas gan individuāliem lietotājiem, gan uzņēmumiem un iestādēm, kuros uzbrucēji izmanto izsūtītāja (*From*: lauks) viltošanu saņēmēja iebiedēšanai vai e-pasta ticamības palielināšanai. Uzņēmumiem un iestādēm tika ieteikts izmantot SPF ierakstu, lai noteiktu, kam ir atļauts izsūtīt e-pastus ar attiecīgo domēna vārdu, DKIM ienākošo e-pastu digitālā paraksta pārbaudei un DMARC protokolu aizsardzībai pret nosūtītāja viltošanu.

Pārskata periodā tika reģistrētas vairākas krāpnieciskas e-pasta kampaņas, kas bija paredzētas internetbanku piekļuves datu izkrāpšanai un bija vērstas uz vairāku Latvijas banku klientiem. Sadarbībā ar policiju un bankām noritēja darbs pie krāpniecisko vietņu aizvēršanas un sabiedrības informēšanas. Tika saņemta informācija par vairākiem upuriem, bet nav zināms nodarītā kaitējuma apjoms.

Eiropas Parlamenta vēlēšanu laikā tika veikta nepārtraukta vēlēšanu sistēmu uzraudzība, novērojot pārtraukumus vēlēšanu sistēmas darbībā. Pieejamās informācijas izpēte liecināja, ka traucējumi nebija saistīti ar ārēju ietekmi un nebija uzskatāmi par drošības incidentu.

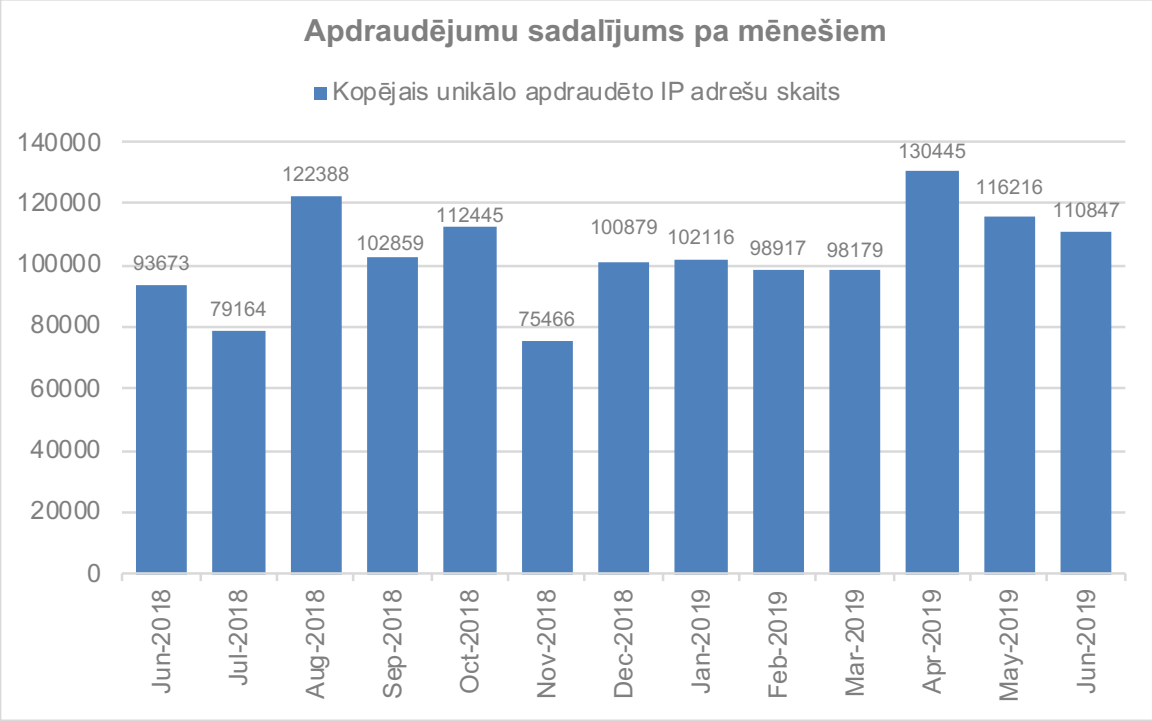
Aprīļa sākumā CERT.LV sadarbībā ar Zemessardzes Kiberaizsardzības vienību, Kanādu un ASV piedalījās NATO CCDCoE kiberdrošības mācību “Locked Shields 2019”. CERT.LV pārstāvji piedalījās arī mācību organizēšanas un vadīšanas procesā. Šogad mācībās tika uzsvērta nepieciešamība tehnisko ekspertu un lēmumu pieņēmēju dialoga uzlabošanai. Tika palielināta mācībās izmantoto sistēmu sarežģītība, salīdzinājumā ar iepriekšējo gadu. Kopumā mācībās piedalījās vairāk nekā 1200 eksperti no gandrīz 30 valstīm.

Pārskata periodā CERT.LV par IT drošību izglītoja 2330 cilvēkus, iesaistoties 45 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.

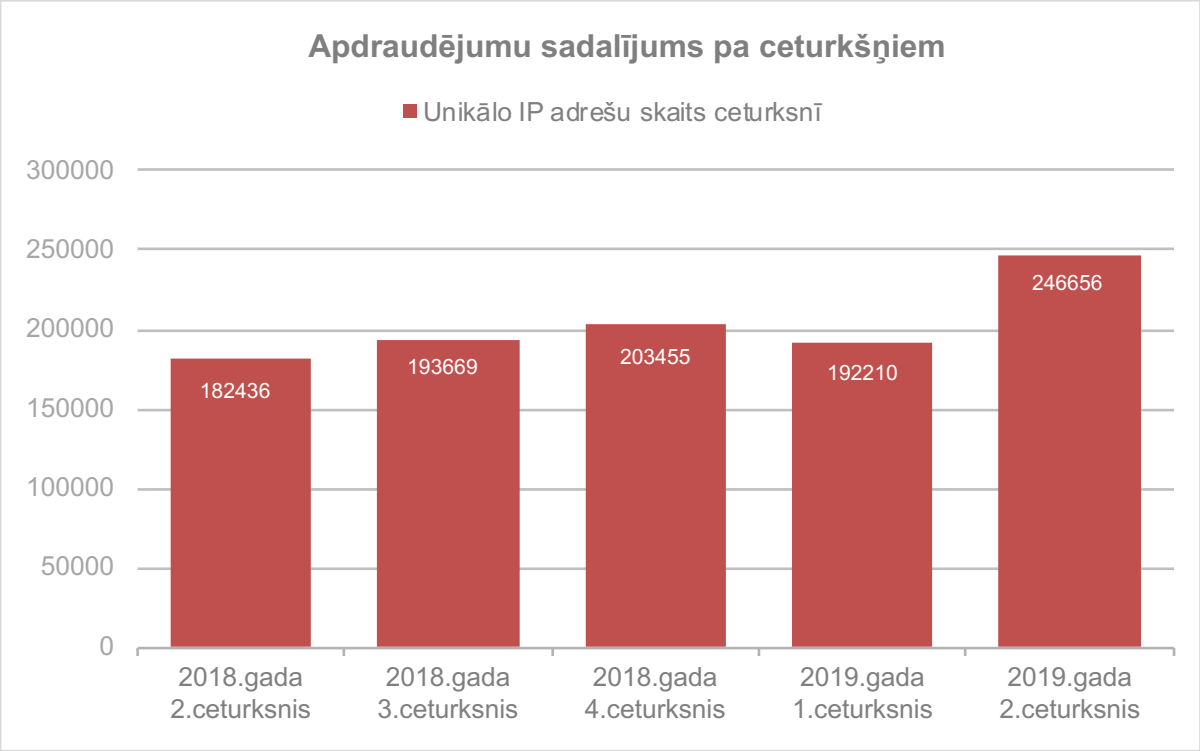
CERT.LV pārskata periodā ik mēnesi apkopoja informāciju par 110 000 – 120 000 ievainojamu unikālu IP adrešu.



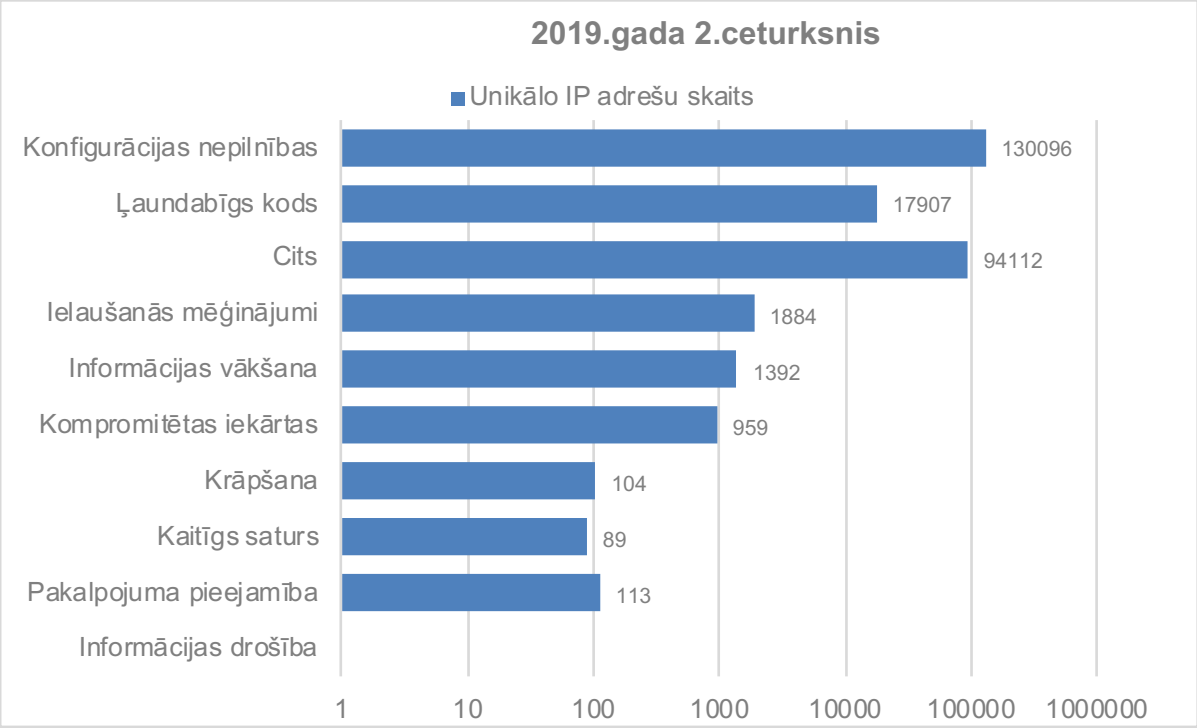
1.attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa mēnešiem 12 mēnešu griezumā.

2019. gada 2. ceturksnī tika reģistrētas 246 656 unikālas apdraudētas IP adreses, kas ir par 28% vairāk nekā iepriekšējā ceturksnī un par 35% vairāk nekā šajā pašā periodā pirms gada.

Pārskata periodā nav vērojamas būtiskas izmaiņas mēnesī reģistrēto apdraudēto IP adrešu daudzumā. Kopējais ceturkšņa pieaugums skaidrojams ar vienreizēju kampaņveidīgu aktivitāti viena datu avota ietvaros (atrodama kategorijā "Cits", 3.att.). Attiecīgā aktivitāte aptvēra uz internetu atvērtu iekārtu/ maršrutētāju apzināšanu, neveicot papildu izpēti par šīm iekārtām. Rezultātā iegūta apjomīga datu kopa (vairāk nekā 48,8 tk. unikālu IP adrešu) taču šī informācija neļauj viennozīmīgi spriest par to, vai iekārta ir apdraudēta, jo, iespējams, iekārtā tiek izmantots atbilstošs ugunsmūris (*firewall*) un droša parole.

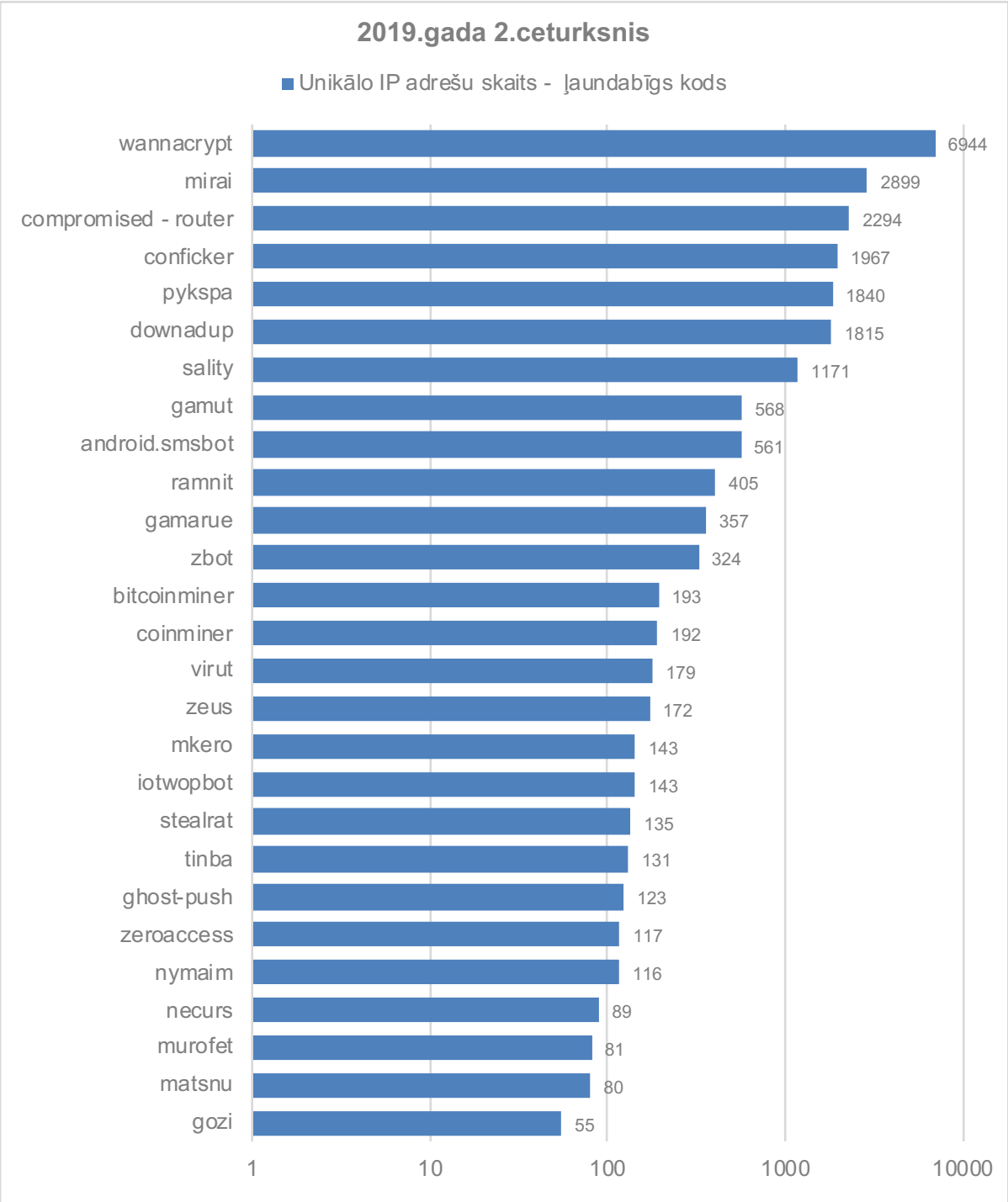


2.attēls – CERT.LV reģistrētās apdraudētās IP adreses pa ceturkšņiem 2018. un 2019. gadā.



3.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2019. gada 2. ceturksnī pa apdraudējumu veidiem.

Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (130 096 unikālas IP adreses) ar kritumu 5% pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs kods (17 907 unikālas IP adreses) ar kritumu 10%, bet trešais - ielaušanās mēģinājumi (2436 unikālas IP adreses) ar kritumu 22%.



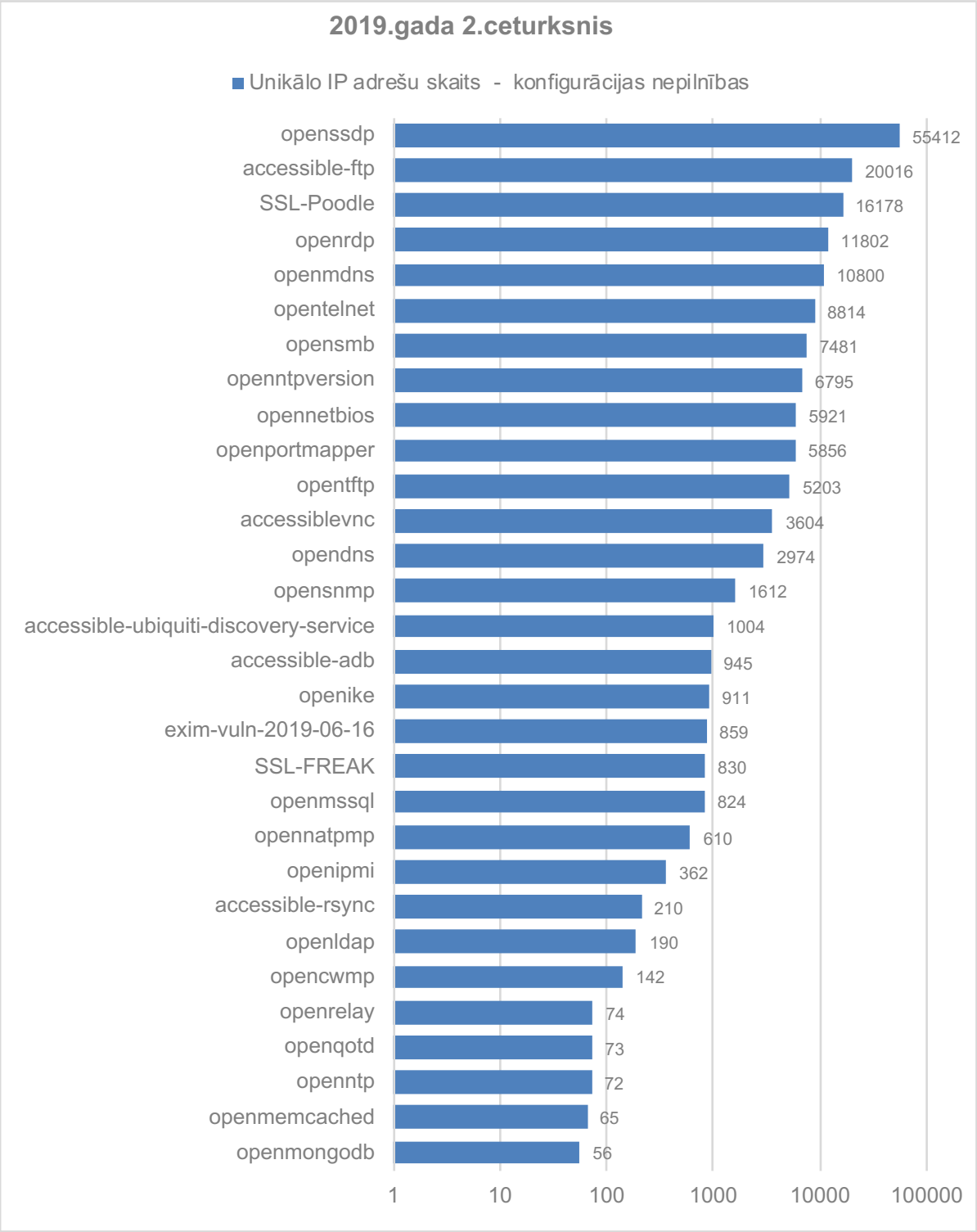
4.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2019. gada 2. ceturksnī ar apdraudējuma veidu - ļaundabīgs kods.

Pirmo vietu ļaunatūras izplatības topā 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.

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

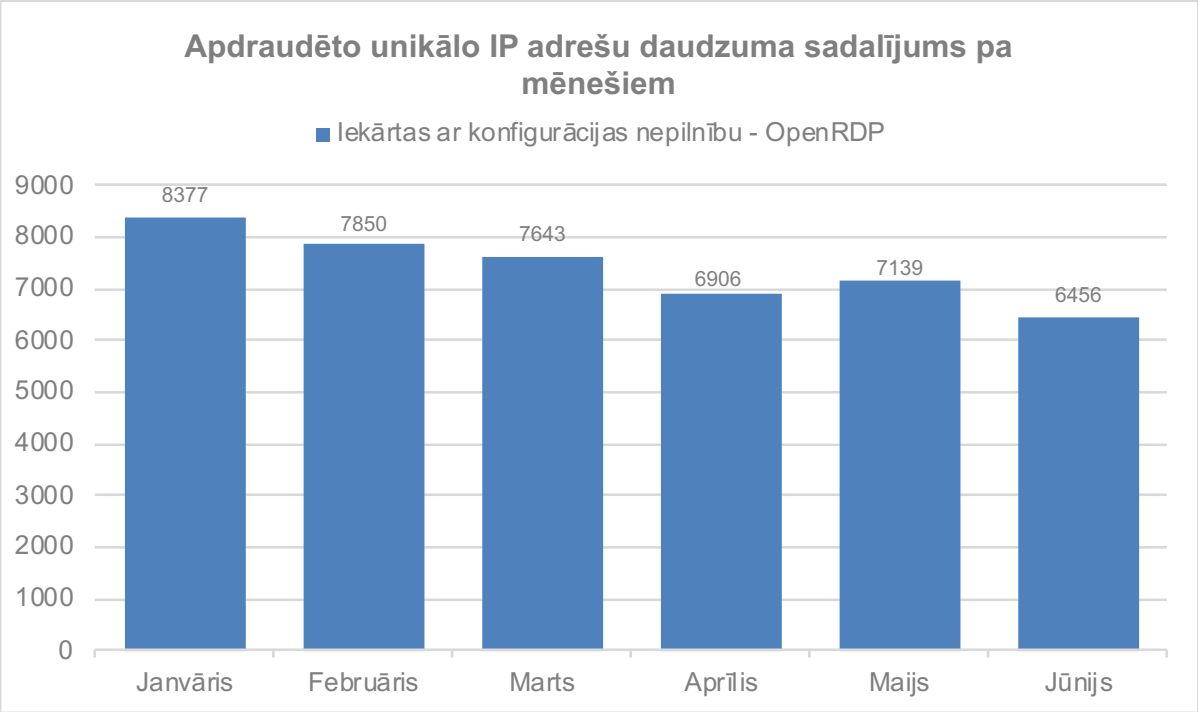


5.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2019. gada 2. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

Pirmo vietu konfigurācijas nepilnību topā ieņem *OpenSSDP* – iekārtas ar nedrošu konfigurāciju, kas var tikt izmantotas apjomīgos piekļuves atteices (DoS) uzbrukumos. *Simple Service Discovery Protocol* (SSDP) ir iebūvēts daudzās tīkla iekārtās, lai tās veiklāk varētu „atrast" viena otru un savstarpēji sazināties.

Konfigurācijas nepilnība *OpenRDP* pārskata periodā nokritusi uz ceturto vietu. Tā bieži

saistīta ar iekārtu un datu nesēju nošifrēšanu. Trešās puses piekļūst neatbilstoši konfigurētām iekārtām, kurās attālinātās piekļuves porti ir brīvi atvērti uz internetu un tām 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. un 2. 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.

2019.gada otrajā ceturksnī CERT.LV pārstāvji tikās ar SIA "Tet" pārstāvjiem, lai apspriestu līdzšinējo sadarbību iniciatīvas "Atbildīgs IPS" ietvaros un iespējas šo sadarbību paplašināt un uzlabot. Abas puses nolēma strādāt pie precīzāku paziņojumu izsūtīšanas gala lietotājiem, lai uzlabotu viņu izpratni un panāktu augstāku reaģēšanas procentu.

Tāpat CERT.LV tikās ar SIA "BITE Latvija" pārstāvjiem, lai izskaidrotu iniciatīvas "Atbildīgs IPS" būtību un aicinātu uzņēmumu pievienoties iniciatīvai.

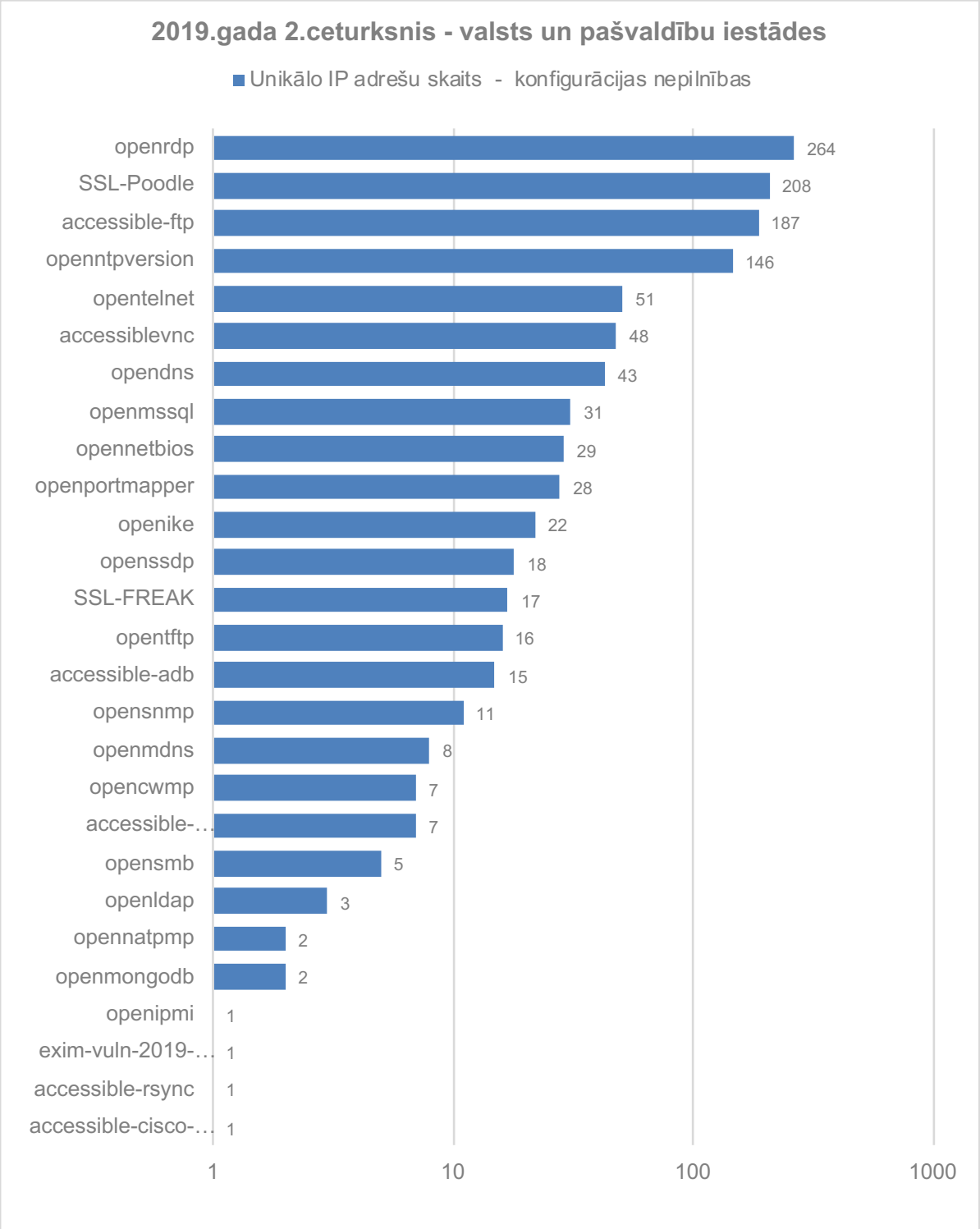
2. Atbalsts informācijas tehnoloģiju drošības incidentu novēršanā vai to novēršanas koordinēšanā.

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.

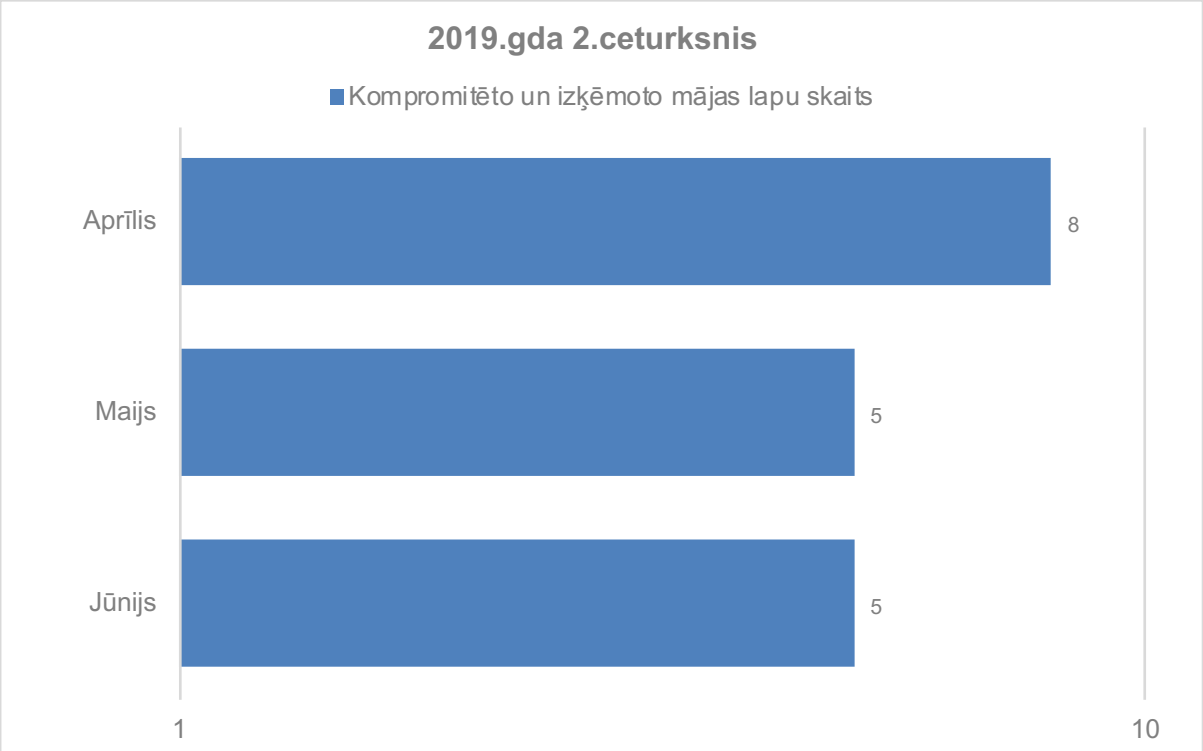
Vidējais apdraudēto valsts un pašvaldību iestāžu IP adrešu daudzums katras dienas saņemtajos ziņojumos pārskata periodā bija 500 unikālas IP adreses dienā.

6.attēls - CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2019.gada 2.ceturksnī ar apdraudējuma veidu – ļaundabīgs kods.



7.attēls - CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2019.gada 2. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

CERT.LV uzskaita arī kompromitēto un izķēmoto tīmekļa vietņu gadījumus. Pārskata periodā tika fiksētas 18 kompromitētas un izķēmotas tīmekļa vietnes. 15 gadījumos izķēmotās vietnes uzturēšanai tika izmantota Linux operētājsistēma, bet 3 gadījumos - Windows. Divas vietnes pēdējā gada laikā tika izķēmotas atkārtoti.



8.attēls – Kompromitēto un izķēmoto tīmekļa vietņu skaits pa mēnešiem 2019. gada 2. ceturksnī.

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

Krāpšana

Tika novērotas vairākas krāpnieciskas kampaņas, kas tika vērstas uz dažādu Latvijas internetbanku lietotājiem un tika paredzētas internetbanku lietotāju datu izkrāpšanai. Tika saņemta informācija par atsevišķiem gadījumiem, kuros lietotāji ievadījuši savus datus krāpnieciskajās vietnēs, bet CERT.LV nav informācijas par nodarīto kaitējumu apjomu.

Turpinājās biznesa e-pastu krāpšanas (*CEO fraud*) kampaņas, kuru rezultātā cieta kāds uzņēmums. Uzbrucējs veiksmīgi viltoja e-pasta sūtītāja (*From*:) lauku un uzņēmuma vadītāja vārdā aicināja veikt maksājumu uz uzbrucēja norādīto kontu. Uzņēmums cieta zaudējumus 41 000 eiro apmērā. Konkrētais uzņēmums no šāda tipa uzbrukuma bija cietis jau agrāk, zaudējot 5 000 eiro, taču nebija sekojis ieteikumiem ieviest SPF filtru, lai novērstu sūtītāja lauka viltošanas (*spoofing*) iespēju. Pēc otrā incidenta ieteikumi tika ieviesti.

Tika saņemti ziņojumi gan no individuāliem lietotājiem, gan arī uzņēmumu un iestāžu pārstāvjiem 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. Dažos gadījumos kā pierādījumu apgalvojumu patiesumam uzbrucējs norādīja, ka zina upura paroli, bet citkārt tika izmantota viltota izsūtītāja adrese, padarot 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.

Līdzīgi kā gada sākumā vairāku telekomunikāciju pakalpojumu sniedzēju un „Latvijas Pasts" vārdā, tā jūnijā kāda mobilo sakaru operatora vārdā tika izplatīta krāpnieciska loterija. Interneta lietotāji informāciju par krāpniecisko loteriju saņēma gan SMS, e-pastu, gan interneta pārlūkprogrammā uznirstošu logu veidā. Loterija piedāvāja laimēt jaunākos Samsung un Apple viedtālruņus vai arī palielas naudas summas. Krāpnieku mērķis bija panākt, ka, piesakoties loterijai, lietotājs brīvprātīgi, taču neizlasot Līguma noteikumus, parakstās uz dažādiem maksas servisiem, par kuriem ik mēnesi no lietotāja bankas konta tiktu ieturēta konkrēta naudas summa. Tika novērota iespēja dinamiski mainīt loterijā norādīto pakalpojuma sniedzēju atbilstoši klienta IP adrešu apgabalam. Tas nozīmē, ka līdzīgus loterijas paziņojumus, iespējams, saņēmuši vairāku mobilo operatoru klienti.

Tika saņemts ziņojums par krāpniecisku tīmekļa vietni, kurā nesaskaņoti tika ievietota informācija par biļešu izplatīšanu uz Latvijas kultūras pasākumiem. Tie pircēji, kas bija veikuši biļešu apmaksu konkrētajā vietnē un centušies iegādātās biļetes izņemt, konstatējuši, ka ir cietuši no krāpniecības. CERT.LV uzsāka darbu pie krāpnieciskās vietnes slēgšanas.

Kāda novada pašvaldība saņēma krāpniecisku e-pastu ar brīdinājumu par domēna vārda reģistrācijas termiņa beigām ar saiti, kas veda uz SEO (*search engine optimization*) vietni, reklamējot mājas lapu pielāgošanu interneta meklētājprogrammām (Google, Yahoo u.c.).

Saņemts ziņojums no kādas privātpersonas, kas kļuvusi par interneta krāpniecības upuri – ar iepazīšanos internetā un sociālās inženierijas metodēm tika izkrāpti 1250 eiro.

Pikšķerēšana jeb personīgo datu izkrāpšana

Tika saņemta virkne ziņojumu par mēģinājumiem izkrāpt lietotāju datus kāda labdara, Starptautiskā monetārā fonda, FBI vai Facebook vārdā. Lielākoties tie bija paziņojumi par ziedojuma saņemšanu, mantojumu, laimestu loterijā vai kompensāciju interneta krāpšanu upuriem. Visos gadījumos krāpnieciskā e-pasta saņēmējs tiek aicināts nosūtīt uz norādīto e-pastu savus personas datus, sākot ar vārdu, uzvārdu, adresi un beidzot ar pases kopiju. Atsevišķos gadījumos tika norādīts, ka finanšu līdzekļus iespējams saņemt, izmantojot Visa vai Mastercard, un lūgts norādīt kartes lietotāja vārdu, kartes numuru, derīguma termiņu un CVV numuru.

Turpinājās e-pasta piekļuves datu izkrāpšanas mēģinājumi gan sūtot brīdinājumu it kā administratora vārdā par nespēju pārbaudīt lietotāja datus, gan aizdomīgu pierakstīšanos kontā, gan arī nepieciešamību atjaunināt kontu sekojot saitei.

Tika saņemts ziņojums par pikšķerēšanas uzbrukumu kādas valsts iestādes e-pasta lietotājiem, bet izpētē tika konstatēts, ka uzbrukums nav bijis mērķēts. Līdzīgs uzbrukums no attiecīgajiem resursiem tika vērsts arī uz vairāku citu tīmekļa e-pastu (webmail) lietotājiem – bankām, universitātēm, uzņēmumiem citviet pasaulē. Ir zināmi seši gadījumi, kad lietotāji ir mēģinājuši atvērt e-pastā norādīto saiti, bet nevienā gadījumā nav notikusi e-pasta piekļuves datu zādzība. Kaitīgā vietne tika aizvērta.

Tika saņemts ziņojums par veiksmīgu pikšķerēšanas uzbrukumu kādai valsts iestādei. Iestādes lietvedības darbiniece saņēma ticami noformētu e-pastu, kurā tika aicināta sekot saitei, lai piekļūtu ziņai tiešsaistē, kuru citādi nav izdevies piegādāt. Krāpnieciskajā vietnē ievadītie piekļuves dati nekavējoties tika nomainīti.

Pakalpojuma pieejamība (DDoS)

Tika saņemts ziņojums par kādas pašvaldības DNS serveri, kurš tika izmantots UDP *flood* tipa uzbrukumā Microsoft serverim, uzbrukumā tika viltotas nosūtīto pakešu adreses.

Saņemts ziņojums par DoS uzbrukumu kādas valsts iestādes resursam, īsā laika periodā saņemot lielu apjomu pieprasījumu no vienas IP adreses. Gandrīz 14 000 pieprasījumu tika bloķēti. Iestāde informēja, ka norādītā IP adrese nav zināma un attiecīgajā laika periodā nav bijuši auditi, kā rezultātā secināms, ka bloķētie pieprasījumi, visticamāk, nav bijuši leģitīmi.

Tika saņemts ziņojums par DDoS uzbrukumu kādas iestādes resursam. Uzbrukumā kombinēti tika izmantotas trīs dažādas metodes (TCP *push flood*, TCP SYN *flood*, TCP *half open*), un tas ilga gandrīz 10 h. Uzbrukums tika veiksmīgi atvairīts.

CERT.LV, veicot nepārtrauktu Eiropas Parlamenta vēlēšanu sistēmas uzraudzību, novēroja pārtraukumus vēlēšanu sistēmas darbībā. Pieejamās informācijas izpēte liecināja, ka sistēmas darbības traucējumi nebija saistīti ar ārēju ietekmi un nav uzskatāmi par drošības incidentu.

Ļaundabīgs kods

Tika saņemta informācija no uzņēmumiem par Latvijas uzņēmumu vārdā izsūtītiem kaitīgiem e-pastiem ar pielikumā pievienotu ļaunatūru (.ISO pielikums), kas izgūst upura iekārtā saglabātos piekļuves datus (lietotājvārdus, paroles). E-pasti bija sagatavoti diezgan labā latviešu valodā, un teksts mudina uz pielikuma atvēršanu. CERT.LV ieteica izveidot SPF (*Sender Policy Framework*) ierakstus un izmantot citas papildu metodes e-pastu aizsardzībai pret viltošanu, kā arī biznesa sarakstei izmantot elektroniski parakstītus dokumentus.

Ielaušanās mēģinājumi

Tika saņemts ziņojums par uzbrukumu kādas valsts iestādes e-pasta serverim. Uzbrukuma ietvaros tika minētas paroles esošiem lietotājiem, izmantojot IMAP servisu. Uzbrukuma laikā pakalpojums bija daļēji pieejams, pie kam tikai ierobežotam lietotāju skaitam.

Tika saņemts ziņojums par mērķtiecīgu uzbrukumu kādas valsts iestādes resursam. Uzbrukums ilga nedaudz vairāk kā stundu un sastāvēja no lietotņu līmeņa DDoS (L7), SQL injekciju, starpvietņu skriptēšanas (XSS) un ievainojamību meklēšanas tipa uzbrukumiem. Kopumā tika bloķēti vairāk kā 16 000 pieprasījumi. Uzbrukums tika veiksmīgi atvairīts.

Kompromitētas iekārtas un datu noplūdes

Tika saņemts ziņojums par veiksmīgu ielaušanos kāda uzņēmuma Confluence serverī. Uzbrucējs izmantoja 20.martā publicēto Atlassian Confluence lietotnes ievainojamību. Uz servera atradās uzņēmuma izpildīto projektu dokumentācija. Uzņēmums apziņoja skartos klientus.

CERT.LV saņēma ziņojumu no kāda interneta lietotāja par kāda Latvijas uzņēmuma vietnē publiski pieejamu tā klientu datu bāzi. Datu bāze, kas saturēja klientu vārdus, e-pastus, adreses, telefona numurus un konta numurus, publiskai apskatei bija pieejama saistībā ar nepareizi konfigurētu uzņēmuma serveri. CERT.LV informēja uzņēmumu par servera konfigurācijas nepilnībām, kā arī norādīja uz citām vietnes vājajām vietām. Tāpat uzņēmums tika informēts par nepieciešamību sazināties ar Datu valsts inspekciju (DVI). Uzņēmums veica nepieciešamos vietnes/ servera uzlabojumus.

Tika saņemta informācija no kādas pašvaldības par uzbrukumu Horizon serverim, kas tika veikts, izmantojot RDP ievainojamību. Uzbrukuma rezultātā tika sašifrētas grāmatvedības programmas un, iespējams, arī citi dati. Incidenta rezultātā tika konstatēta datu rezerves kopiju neesamība. Tika izmantots ārpakalpojums.

CERT.LV saņēma informāciju no kādas pašvaldības par šifrējošo izspiedējvīrusu, kas nošifrējis visus datus pašvaldības lietvedības serverī. Uz servera bija atvērts *Remote desktop* savienojums, bet pieeja tika ierobežota, atļaujot piekļuvi tikai noteiktām IP adresēm (*whitelist*). Serveris tika atslēgts no pārējā iestādes tīkla. Citās iekārtās problēma netika novērota.

Tika saņemts ziņojums par veiksmīgu uzbrukumu kādas pašvaldības e-pastu sistēmai. Sniegtā informācija norāda, ka uzbrucēji serverī ievietoja sistēmlaužņus (*rootkits*), iegūstot superlietotāja tiesības un spējas modificēt servera saturu, kuram citādi negūtu piekļuvi.

Tika saņemts ziņojums no kāda tiešsaistes medija par vietnes uzlaušanu. Uzlauztajā vietnē tika ievietots nepatiesu informāciju saturošs raksts, kas tika saistīts ar NATO mācībām. Vietnes uzturētāji viltus saturu dzēsa un ievietoja informāciju par kompromitēšanas faktu.

Ievainojamības

Tika apzināti un informēti ievainojamo Confluence serveru turētāji, brīdinot par kritisku ievainojamību CVE-2019-3396 (*Remote code execution via Widget Connector macro*), kas ļāva uzbrucējam attālināti izpildīt komandas serverī. Tika izteikts aicinājums atslēgt serveri no publiskā tīkla līdz brīdim, kad tiek uzstādīta versija ar ievainojamību labojumiem.

Tika saņemta informācija par kļūdu kādas mācību iestādes tīmekļa vietnes autentifikācijas procesa kontrolē. Kļūdas rezultātā bija iespējams apiet autentifikācijas procesa aizsardzības mehānismu, atkārtoti izmantojot saglabātās sesijas datus. Informācija tika nodota vietnes uzturētājam.

Tika atklāta ievainojamība kādā tīmekļa vietnē, kas ļāva trešo pušu vietnēm neatkarīgi no to atrašanās vietas vai saistības ar vietni iegūt pieeju vietnes lietotāju e-pastiem, ieskaitot pielikumus, un tos nolasīt, izmantojot standarta JavaScript funkcionalitāti. Uzbrukums bija iespējams, ja lietotājs vienā un tajā pašā pārlūkā apmeklēja konkrēto trešās puses vietni, paralēli esot pierakstīts (log-in) ievainojamajā vietnē. Uzbrukums darbojās arī tad, ja lietotājs bija iespējojis divfaktoru autentifikāciju, vai bija aizvēris ievainojamo vietni pārlūkā, bet nebija no tās izrakstījies (log-out). Tīmekļa vietnes uzturētāji tika informēti par atklāto ievainojamību, ievainojamība tika operatīvi novērsta. Pēc vietnes sniegtās informācijas neviena lietotāja dati kompromitēti netika.

Tika apzināti un informēti sistēmu turētāji, uz kuriem attiecās kritiska Oracle serveru programmatūras ievainojamība CVE-2019-2729, kas ļāva uzbrucējiem attālināti pārņemt kontroli pār ievainojamo serveri, apejot autentifikāciju. Ievainojamo iekārtu turētāji tika aicināti veikt steidzamus iekārtu atjauninājumus.

Ielaušanās testi

Tika veikti ielaušanās testi kādas organizācijas tiešsaistes resursam. Tika konstatēts, ka vietnei tika izmantota novecojusi satura vadības sistēma (CMS), kas saturēja vairākas kritiskas ievainojamības, kā arī spraudnis, kas saturēja kritisku ievainojamību. Tika sniegti

ieteikumi ievainojamību novēršanai.

Tika saņemta informācija no kādas valsts iestādes par problēmām ar tīmekļa vietnes noslodzi un lūgums veikt tīmekļa vietnes pārbaudi. Tika veiktas pārbaudes un atklātas vairākas konfigurācijas nepilnības, par kurām informēts uzturētājs un sniegti ieteikumi uzlabojumiem.

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.

11. aprīlī CERT.LV pārstāvis piedalījās laikraksta Dienas Bizness organizētajā konferencē "Uzņēmuma digitālā drošība". Konference aplūkoja izaicinājumus, kas saistīti ar kiberdrošību uzņēmumos. CERT.LV pārstāvis sniedza prezentāciju "Informācijas drošības kultūra".

16. aprīlī CERT.LV pārstāvis piedalījās seminārā "Pirmais gads datu regulas gaismā – gūtās mācības un pārkāpuma ABC", kas notika "GDPR Rīgas Forums 2019" ietvaros. Seminārā tika aplūkotas uzņēmumu atziņas, kas bijuši lielākie izaicinājumi, kā risinātas problēmsituācijas, aplūkojot arī drošības incidentus, to sekas un galvenās mācības.

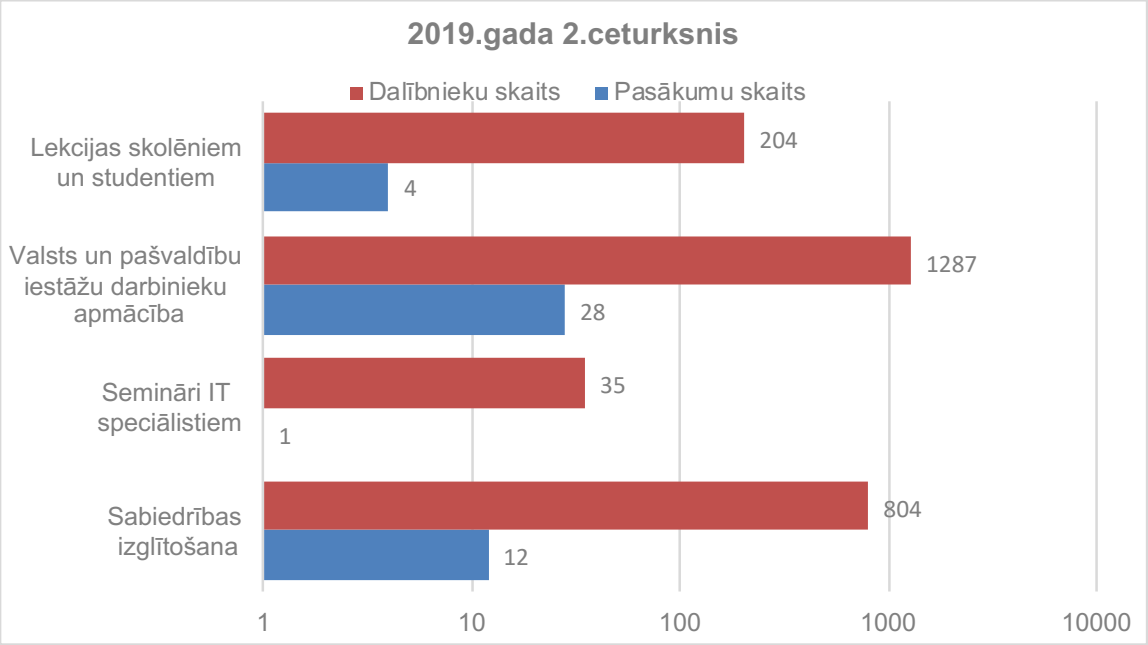
22. maijā CERT.LV pārstāvis piedalījās Latvijas Transatlantiskās Organizācijas (LATO) organizētajā diskusijā Daugavpils Universitātē diskusiju cikla "Parunāsim par NATO" ietvaros.

29. maijā CERT.LV pārstāvis piedalījās paneļdiskusijā "Mākslīgais intelekts un personas datu aizsardzība", kas notika DSS organizētā foruma "Digitālā ēra" ietvaros.

5. jūnijā CERT.LV sadarbībā ar NIC Latvijas Tirdzniecības un rūpniecības kamerā (LTRK) vadīja semināru uzņēmējiem "Kā uzņēmējam viegli (ne) pazaudēt naudu kibertelpā". Semināra mērķis bija sniegt mazo un vidējo uzņēmumu pārstāvjiem zināšanas, kā atpazīt viltotus e-pastus, kas ir šifrējošie izspiedējvīrusi un kāpēc tie strādā, kā darbojas pikšķerēšana un kā hakeri izmanto domēnus, lai veiktu uzbrukumus.

28. jūnijā CERT.LV pārstāvji piedalījās sarunu festivāla "Lampa" diskusijās: "Glabā savas paroles, tāpat kā savu apakšveļu" par paroļu drošību un "Maldināšana – katra diena kā 1.aprīlis?" par eksperimenta rezultātiem ar reālā laika datiem, par datu interpretācijas nozīmi un kā mācēt kritiski izvērtēt apkārt esošo informāciju ikdienā.

Pārskata periodā CERT.LV par IT drošību izglītoja 2330 cilvēkus, iesaistoties 45 izglītojošos pasākumos.



9.attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2019. gada 2. 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 grupā, gatavojoties maijā gaidāmajām vēlēšanām, kā arī vēlēšanu laikā veica nepārtrauktu vēlēšanu sistēmu uzraudzību.
- CERT.LV piedalījās Saeimas Nacionālās drošības komisijas sanāksmēs par 5G jautājumiem, sniedza atbalstu 5G tehnoloģiju tehnisko risku novērtēšanā un dokumentācijas gatavošanā, kā arī saistīto dokumentu izskatīšanā.

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.
- CERT.LV pārstāvis piedalījās vairākās sanāksmēs saistībā ar NATO mācību "Crossed Swords 2020" plānošanu un organizēšanu, iesaistoties mācību scenārija izveidē, partneru piesaistē un mācību menedžmentā.
- Aprīļa sākumā CERT.LV sadarbībā ar Zemessardzes Kiberaizsardzības vienību, Kanādu un ASV piedalījās NATO CCDCoE kiberdrošības mācībās "Locked Shields 2019".

CERT.LV pārstāvji piedalījās arī mācību organizēšanas un vadīšanas procesā. Šogad mācībās tika uzsvērta nepieciešamība tehnisko ekspertu un lēmumu pieņēmēju dialoga uzlabošanai. Šim nolūkam mācībās tika integrēta tehniskā un stratēģiskā spēle, ļaujot dalībvalstīm būtiskas kiberkrīzes apstākļos pilnveidot dažādus komunikāciju posmus, iekļaujot gan civilos, gan militāros aspektus. Mācībās tika aplūkoti reāli kiberapdraudējumi, par galveno uzdevumu liekot kritiskās infrastruktūras aizsardzību. Tika palielināta mācībās izmantoto sistēmu sarežģītība, salīdzinājumā ar iepriekšējo gadu. Kopumā mācībās piedalījās vairāk nekā 1200 eksperti no gandrīz 30 valstīm.

- 4. – 7. aprīlī CERT.LV pārstāvis piedalījās Eiropas Parlamenta, ES dalībvalstu, Eiropas Komisijas un ENISA organizētajās krīzes vadības mācībās "EU ELEx19" Briselē, lai uzlabotu gatavību potenciāliem kiberdrošības incidentiem Eiropas Parlamenta vēlēšanu laikā.
- 30. aprīlī CERT.LV pārstāvis piedalījās sanāksmē ar OECD pārstāvjiem, lai apspriestu situāciju Latvijā kiberdrošības jomā un palīdzētu veidot OECD pilnīgāku izpratni par šīs jomas regulējumu un praktisko realizāciju Latvijā.
- 5. - 11. maijam CERT.LV pārstāvis pasniedza NATO CCDCoE „*Malware and Exploitation Essentials*" kursu Tallinā, Igaunijā.
- 8. maijā CERT.LV pārstāvji tikās ar aizsardzības nozares maģistrantūras studentiem no ASV, prezentējot CERT.LV un kiberdrošības organizāciju Latvijā.
- 8. - 10.maijā CERT.LV notika Trusted Introducer resertifikācijas seminārs, kurā kā novērotāji piedalījās CERT-EE un CERT.hr pārstāvji.
- 15. - 16. maijam CERT.LV pārstāvji piedalījās ENISA rīkotajās Eiropas kiberdrošības mācībās "CyberSOPEx". kuru mērķis bija veicināt ES dalībvalstu sadarbību liela mēroga kiberincidenta gadījumā.
- 30. maijā CERT.LV uzņēma Uzbekistānas CERT vizīti, lai veiktu pieredzes apmaiņu organizācijas darbībā, incidentu apstrādē un prevencijā, kā arī sabiedrības izglītošanas jautājumos.
- 5. - 6. jūnijam CERT.LV pārstāvji piedalījās "NIS CSIRT network" sanāksmē Bukarestē, Rumānijā. CERT.LV pārstāvis dalījās ar informāciju par jaunu algoritmu pielietošanu apdraudējumu izsekošanā Latvijā. Sanāksmes ietvaros notika arī tematiskās darba grupas, un CERT.LV aktīvi piedalījās divās darba grupās: "Cyber Weather" darba grupā, kura regulāri apkopo informāciju par būtiskākajiem kiberincidentiem un reizi ceturksnī izstrādā kiberlaikapstākļu pārskatu Eiropai; un "Maturity" darba grupā, kura rūpējas par ES dalībvalstu CSIRT komandu brieduma līmeņa paaugstināšanu.
- 16. - 21. jūnijam CERT.LV pārstāvji piedalījās 31. FIRST konferencē Edinburgā. Šī gada konference bija lielākā FIRST konference vēsturē, pulcējot vairāk nekā 1000 pārstāvjus no dažādām CERT komandām un citām saistītām organizācijām no vairāk nekā 80 valstīm. CERT.LV pārstāvji vadīja vairākas tehniskās sesijas, pārstāvēja Latviju ikgadējā biedru kopsapulcē, kā arī startēja "*capture the flag*" izaicinājumu risināšanas sacensībās. CERT.LV pārstāvis piedalījās arī FIRST konferences programmkomitejā.

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 notika darbs pie papildu moduļa integrācijas.

Ar projekta atbalstu tiek organizēta kiberdrošības konference "Kiberšahs 2019". Konferences norises nodrošināšanai pārskata periodā tika izsludināts publisks iepirkums "Telpu, ēdināšanas un tehniskās aparatūras nodrošinājums konferencei "Kiberšahs 2019"", kas noslēdzās bez rezultātiem. Iepirkums tika turpināts kā sarunu procedūra.

2019.gadā projekta ietvaros tiks rīkoti vairāki tehnikas iepirkumi, notiek specifikāciju sagatavošana šiem iepirkumiem, kā arī līgumu slēgšanas un piegādes procesi.

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 2. ceturksnī notika pirmā kiberapmaiņas vizīte, kuras ietvaros Latvijā viesojās Horvātijas CERT pārstāvji, lai vairāku dienu garumā veiktu vērtīgu pieredzes apmaiņu par organizācijas procesu norisi, incidentu risināšanu, apstrādes metodēm, izmantotajiem rīkiem un apstrādes kārtību, incidentu prevencijas metodēm, izglītošanas jautājumiem un citiem aktuāliem darbības aspektiem.

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.
- CERT.LV pārstāvis Bernhards Blumbergs ieguva doktora grādu, aizstāvot disertāciju "Specialized Cyber Red Team Responsive Computer Network Operations" Tallinas Tehniskajā universitātē.

- CERT.LV pārstāvji Uldis Koškins un Jānis Narbuts saņēma Aizsardzības ministrijas apbalvojumus par ieguldījumu Latvijas kiberdrošībā.
- 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 VAS "Latvijas Valsts radio un televīzijas centrs" re-sertifikācijas procesā.

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 01.04.2019. līdz 30.06.2019. ir saņēmusi un izvērtējusi 1189 ziņojumus. No tiem 1055 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 14 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 27 ziņojumos konstatēta personas goda un cieņas aizskaršana, 2 ziņojumi saņemti par naida runu un 1 ziņojums par vardarbību atainojošiem materiāliem. Par finanšu krāpšanas mēģinājumiem internetā saņemti 22 ziņojumi, 31 ziņojuma saturs nav bijis pretlikumīgs, 37 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 1008 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 17 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, lai dzēstu nelegālo saturu no publiskas aprites. 8 ziņojumi pārsūtīti INHOPE ziņojumu līnijām turpmāko darbību veikšanai.

Pārskata periodā no Latvijā uzturētajiem 1030 ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem 1029 ziņojumu saturs ir dzēsts no publiskas aprites un 1 ziņojuma saturs atrodas dzēšanas procesā sadarbībā ar Valsts policiju un interneta pakalpojumu sniedzējiem.

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