Latvijas Universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

Publiskais pārskats par CERT.LV uzdevumu izpildi 2018. gadā

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

Kopējais kiberdrošības apdraudējuma līmenis Latvijas kibertelpā vērtējams kā mērens. Komerciāli motivēto uzbrukumu apjoms bija nemainīgi augsts, tendence - lēni pieaugoša. Galvenie cietušie bija mazie un vidējie uzņēmēji. Publiskajā sektorā pārsvarā cieta pašvaldības Latvijas reģionos. Finanšu sektors bija stabils un būtiski incidenti novēroti netika. Latvija turpināja būt interesants mērķis uzbrucējiem ar NATO un ES pretēju ideoloģiju.

Aizvadītajā gadā pastiprināta uzmanība tika pievērsta Saeimas vēlēšanu procesa pārskatāmībai un kiberdrošībai. CERT.LV vērtējumā kibertelpā vēroto aktivitāti vēlēšanu laikā jāklasificē kā mērenu, valsts drošību un vēlēšanas neapdraudošu, bez būtiskiem pavērsieniem. Ar dažādu intensitāti tika novēroti vairāki uzbrukumi e-pasta sistēmām, tīmekļa vietnēm un tīkla infrastruktūrai, arī mērķiem valsts sektorā. Taču tiem neizdevās radīt kaitējumu, vai iedzīvotājiem jūtamu efektu, jo tos izdevās veiksmīgi atvairīt. Pamanāmākais incidents vēlēšanu laikā bija sociālā tīkla Draugiem.lv sākuma lapas izķēmošana.

Pievēršot uzmanību konkrētiem incidentiem, pārskata periods iezīmējās ar virkni DDoS uzbrukumu, kas ieguva arī plašu rezonansi medijos (e-veselība, LETA, Dziesmu un deju svētku biļešu izplatītājs bilesuparadize.lv, Delfi.lv). Beidzot ieviešot labās prakses standartu BCP-38 vismaz Eiropas līmenī, būtu iespējams rast risinājumu DDoS uzbrukumu problēmai, novēršot iespēju izsūtīt tīkla paketes ar viltotu paketes avotu (*IP spoofing*), kas ir lielākās daļas DDoS uzbrukumu pamatā. Tas ļautu samazināt arī resursu uzturēšanas izmaksas uz DDoS aizsardzības risinājumu rēķina.

Ilgstoši un regulāri CERT.LV turpināja saņemt ziņojumus par nošifrētām iekārtām, kurām uzbrucēji piekļuvuši, izmantojot vāji aizsargātu attālinātās piekļuves sistēmu (RDP) un uzminot pārāk vienkāršo paroli gan privātajā, gan arī valsts sektorā.

Uz lietotājiem orientētajās krāpnieciskajās kampaņās tika novēroti inovatīvi paņēmieni, izmantojot personalizētāku pieeju krāpniecisko e-pastu sagatavošanā. Lai palielinātu vēstulē minēto draudu ticamību, e-pastā tika norādīta lietotāja personīgā informācija, piemēram, parole vai daļa telefona numura, kas iegūta kādā datu noplūdē, bet izmantota kā „pierādījums" iekārtas uzlaušanai.

2018.gada pozitīvā tendence ir interneta lietotāju pieaugošā modrība un atbildības sajūta, par ko liecināja CERT.LV saņemtie informatīvie ziņojumi par dažādām krāpnieciskām kampaņām, kā arī sabiedrības pieaugošā interese par dažādu programmatūru un ierīču izcelsmi un ar to saistītajiem riskiem, kā tas bija vērojams ar Yandex Taxi, Kaspersky un Huawei.

Pārskata periodā CERT.LV sadarbībā ar NATO CCDCoE pirmo reizi Latvijā organizēja tehniskās kiberdrošības mācības „Crossed Swords 2018". Tās bija līdz šim tehniski sarežģītākās un izaicinošākās mācības, kas aptvēra vairākus ģeogrāfiskus atrašanās punktus, iesaistot tajās gan informācijas tehnoloģiju (IT) kritiskās infrastruktūras uzturētājus, gan militārās vienības. Mācībās piedalījās vairāk nekā astoņdesmit kiberdrošības ekspertu no piecpadsmit NATO CCD CoE dalībvalstīm.

Devītajā oktobrī Eiropas Kiberdrošības mēneša ietvaros ar projekta "Improving Cyber Security Capacities in Latvia" atbalstu CERT.LV sadarbībā ar ISACA Latvijas nodaļu organizēja

kiberdrošībai veltīto konferenci „Kiberšahs 2018", kuru klātienē apmeklēja 500 dalībnieki, bet attālināti vēroja vairāk kā 2000.

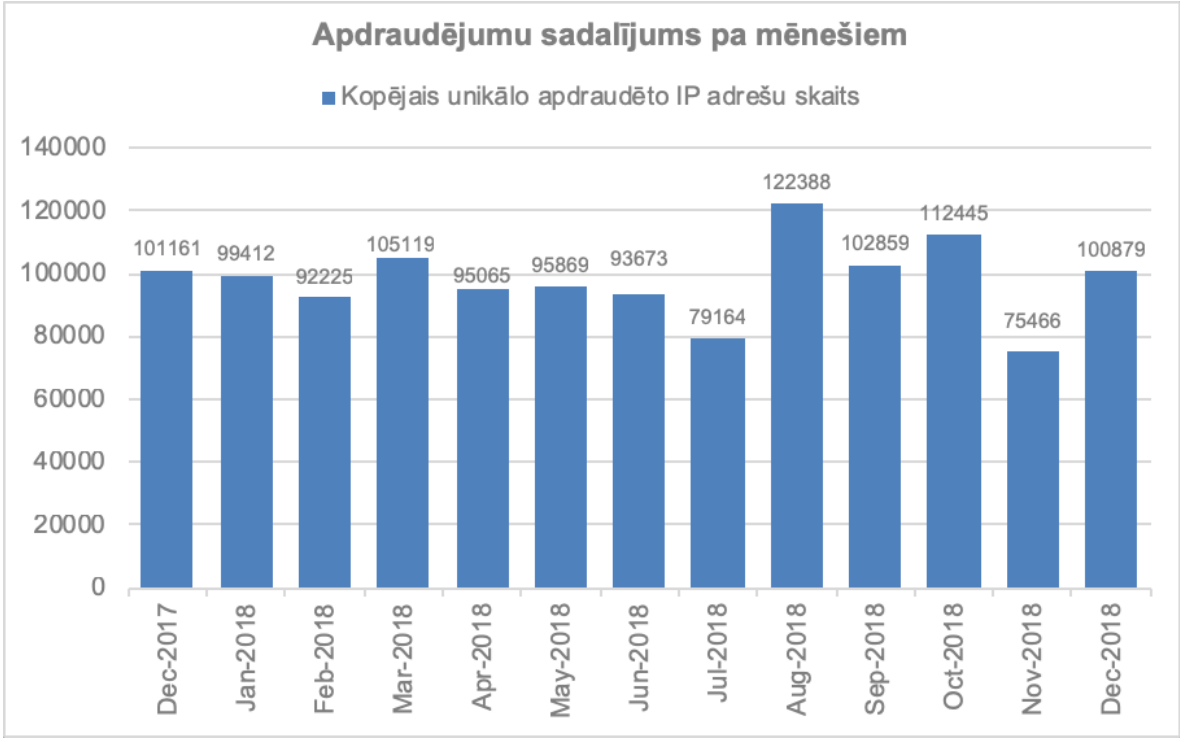
2018. gadā CERT.LV uzsāka realizēt Eiropas Komisijas "Connecting Europe Facility, Telecom-Cyber Security" 2017. gada uzsaukumā apstiprināto projektu "Improving Cyber Security Capacities in Latvia" (līguma ar Eiropas Komisiju Nr.INEA/CEF/ICT/A2017/1528784) un sadarbības projektu "CyberExchange" (līguma ar Eiropas Komisiju Nr. INEA/CEF/ICT/A2017/1528784), lai stiprinātu CERT.LV reaģēšanas spējas uz informācijas tehnoloģiju drošības incidentiem, paaugstinātu zināšanas un kapacitāti un gatavību izpildīt NIS direktīvas prasības.

Kopumā pārskata periodā CERT.LV reģistrēja 491 974 apdraudētas unikālās IP adreses, sniedza nepieciešamo atbalstu gan publiskajam, gan privātajam sektoram, gan arī tiesībsargājošajām iestādēm incidentu risināšanā, piedalījās 127 dažādos pasākumos un izglītoja gandrīz 8000 cilvēkus.

1. Incidentu apstrāde

Ik mēnesi CERT.LV apkopo informāciju par apdraudētajām Latvijas IP adresēm. 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.

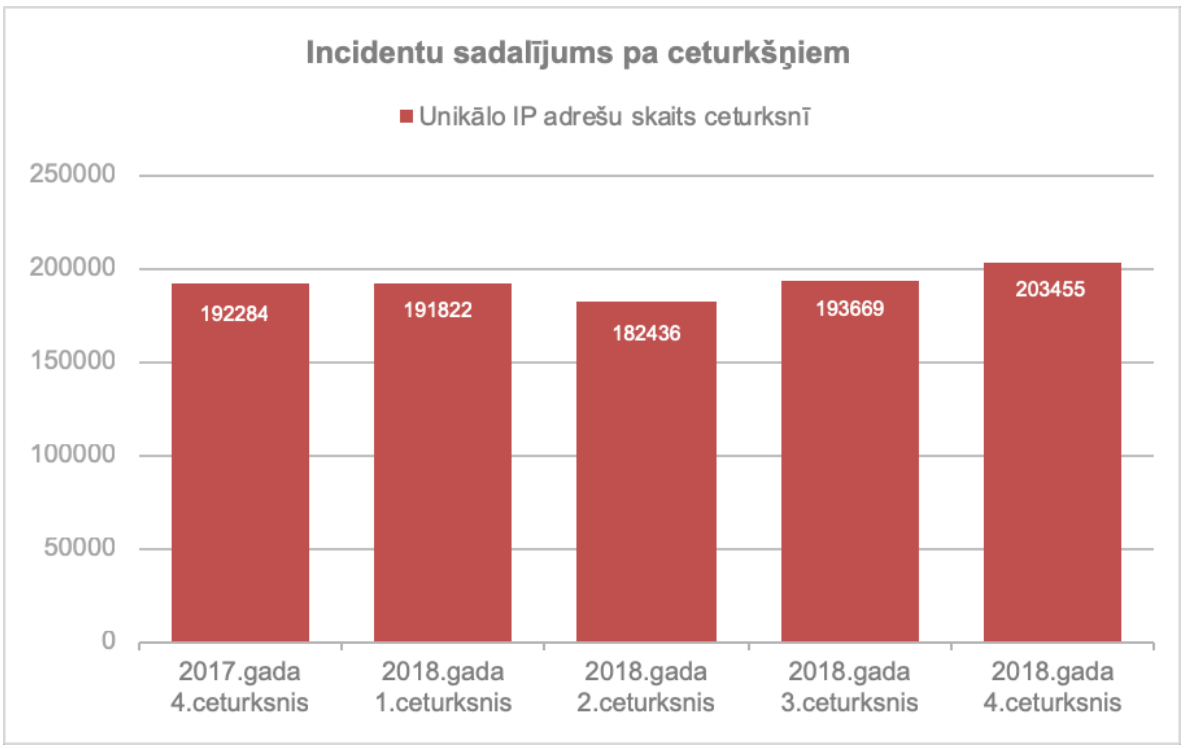
CERT.LV pārskata periodā ik mēnesi apkopoja informāciju par vidēji 95 000 – 105 000 ievainojamu unikālu IP adrešu.



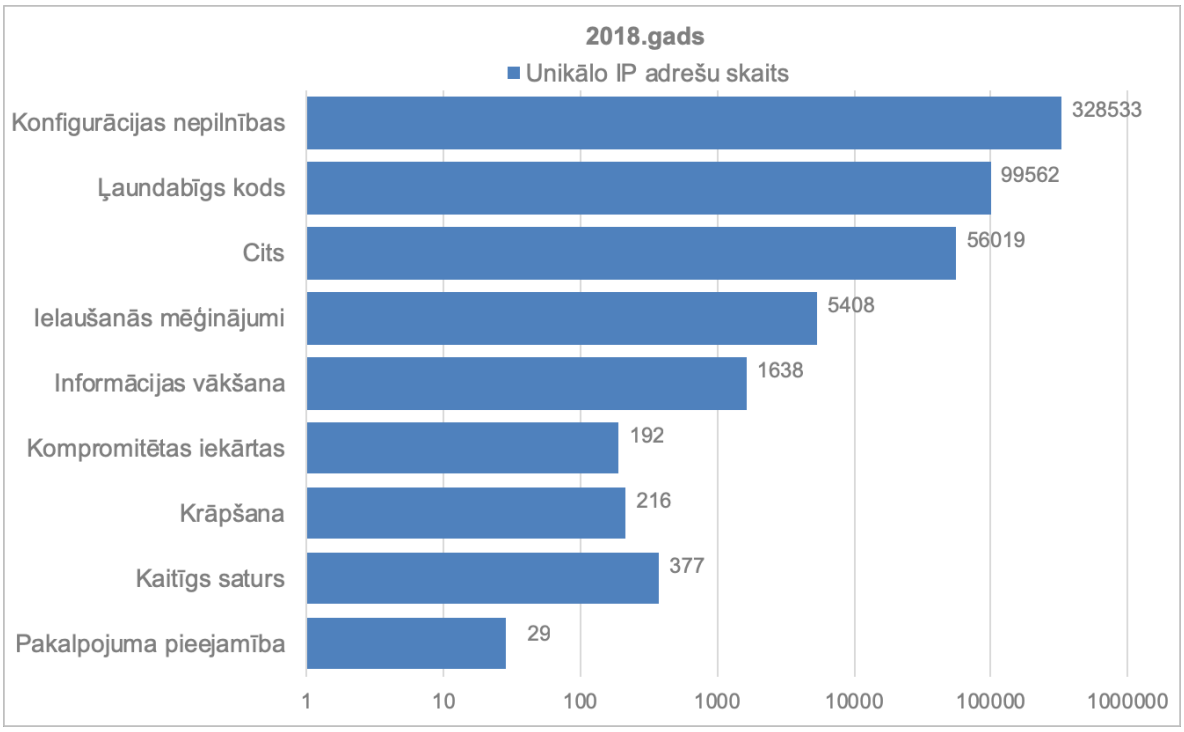
1.attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa mēnešiem 2018. gadā.

Nevienmērīga ienākošo datu plūsma rezultējās ar kritumu jūlija un kāpumu augusta rādījumos, bet oktobra kāpums skaidrojams ar jaunas apdraudējumu kategorijas ieviešanu vairākos datu avotos (1. attēls). Arī novembra kritumu izraisīja nevienmērīga ienākošo datu plūsma.

2015.gada MK noteikumu Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 15. un 24. punkts paaugstinātas drošības IS tiek piemērots no 2018.gada 1.janvāra un turpina paaugstināt valsts informācijas sistēmu drošības līmeni. Nozīmīgu lomu spēlē arī regulārie darbinieku izglītošanas pasākumi.

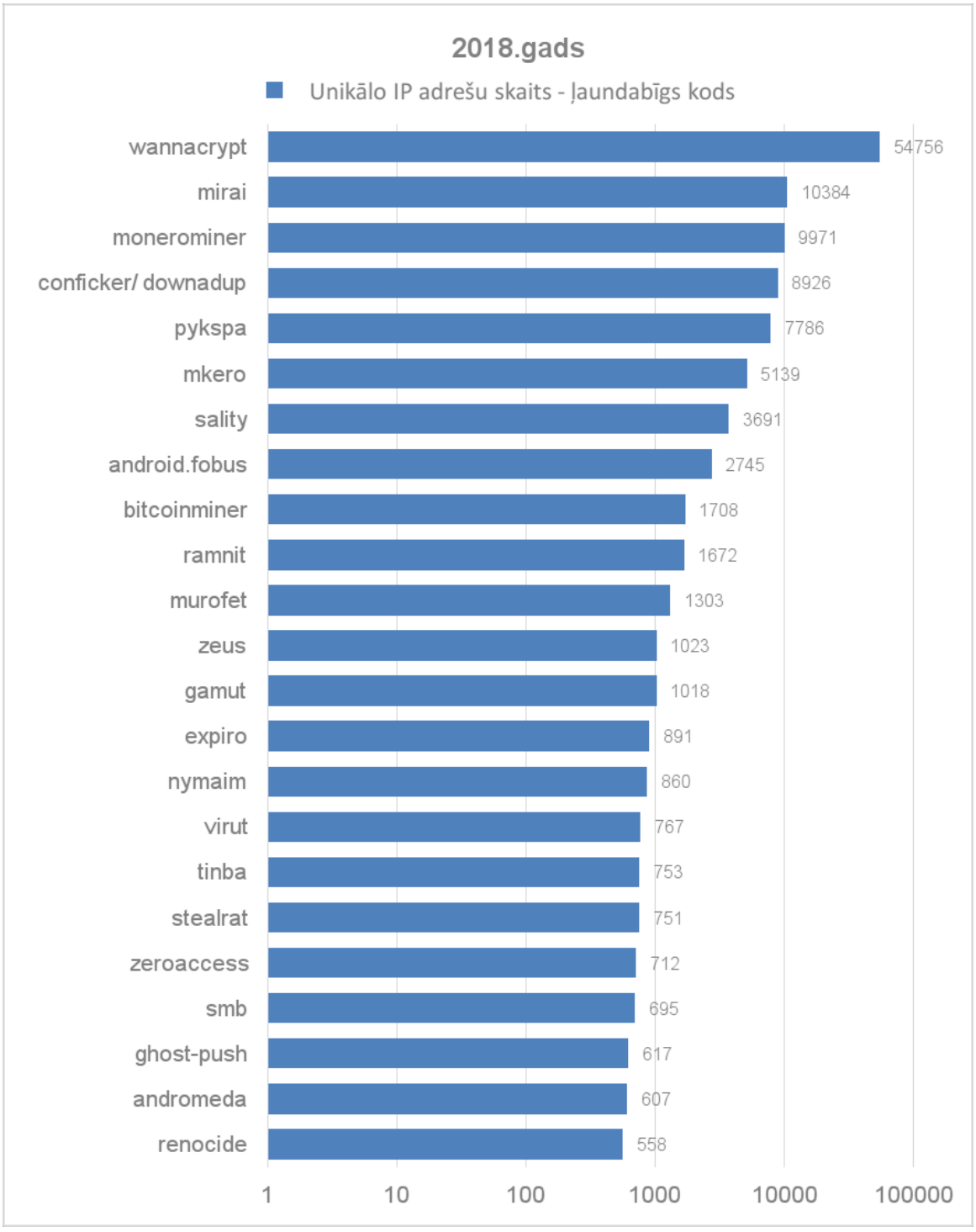


2.attēls – CERT.LV reģistrētās apdraudētās IP adreses pa ceturkšņiem 2018. gadā.



3.attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa apdraudējuma veidiem 2018. gadā.

Izplatītākais apdraudējuma veids pārskata periodā nemainīgi bija konfigurācijas nepilnības, otrs izplatītākais bija ļaundabīgs kods, bet trešais - ielaušanās mēģinājumi.



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

Pirmo vietu ļaunatūras izplatības topā šajā gadā stabili ieņēma *WannaCrypr* jeb *Wannacry*, kas ir šifrējošais izspiedējvīruss. Tas ietekmē iekārtas ar Microsoft Windows operētājsistēmu un izplatās, izmantojot ievainojamību SMB protokolā. Vīrusa ietekmi un izplatību iespējams

novērst, uzstādot Microsoft sagatavotos programmatūras atjauninājumus, kas pieejami pat tādām Windows versijām kā Windows XP un Windows Server 2003. Jāatzīst gan, ārkārtīgi lielais šīs ļaunatūras skarto unikālo IP adrešu skaits, kas būtiski pārsniedz visu pārējo ļaunatūru apjomu, varētu norādīt uz to, ka inficētas ir tikušas iekārtas, kurām piešķirtas dinamiskas adreses, izmantojot DHCP (*Dynamic Host Configuration Protocol*), un patiesais inficēto iekārtu apjoms ir mazāks. Taču tas nenozīmē, ka apdraudējums nav būtisks un vērā ņemams, īpaši tāpēc, ka norāda uz inficētām iekārtām ar, ticamākais, novecojušu operētājsistēmu, piemēram Windows XP, kura vairs nesaņem automātiskos atjauninājumus, un pakļauj iekārtu paaugstinātam riskam.

Topa otrajā vietā atrodas *Mirai* – ļaunatūra, kas apdraud neatbilstoši aizsargātas lietu interneta (IoT) iekārtas. Visbiežāk inficēti tiek viedie televizori, interneta maršrutētāji vai citas līdzīgas iekārtas, kas pēc iegādes tiek pieslēgtas internetam, nenomainot ražotāja iestatīto lietotājvārdu un paroli. Šīs iestatītās jeb noklusējuma paroles ir plaši zināmas, un to izmantošana pakļauj iekārtas uzbrukuma riskam.

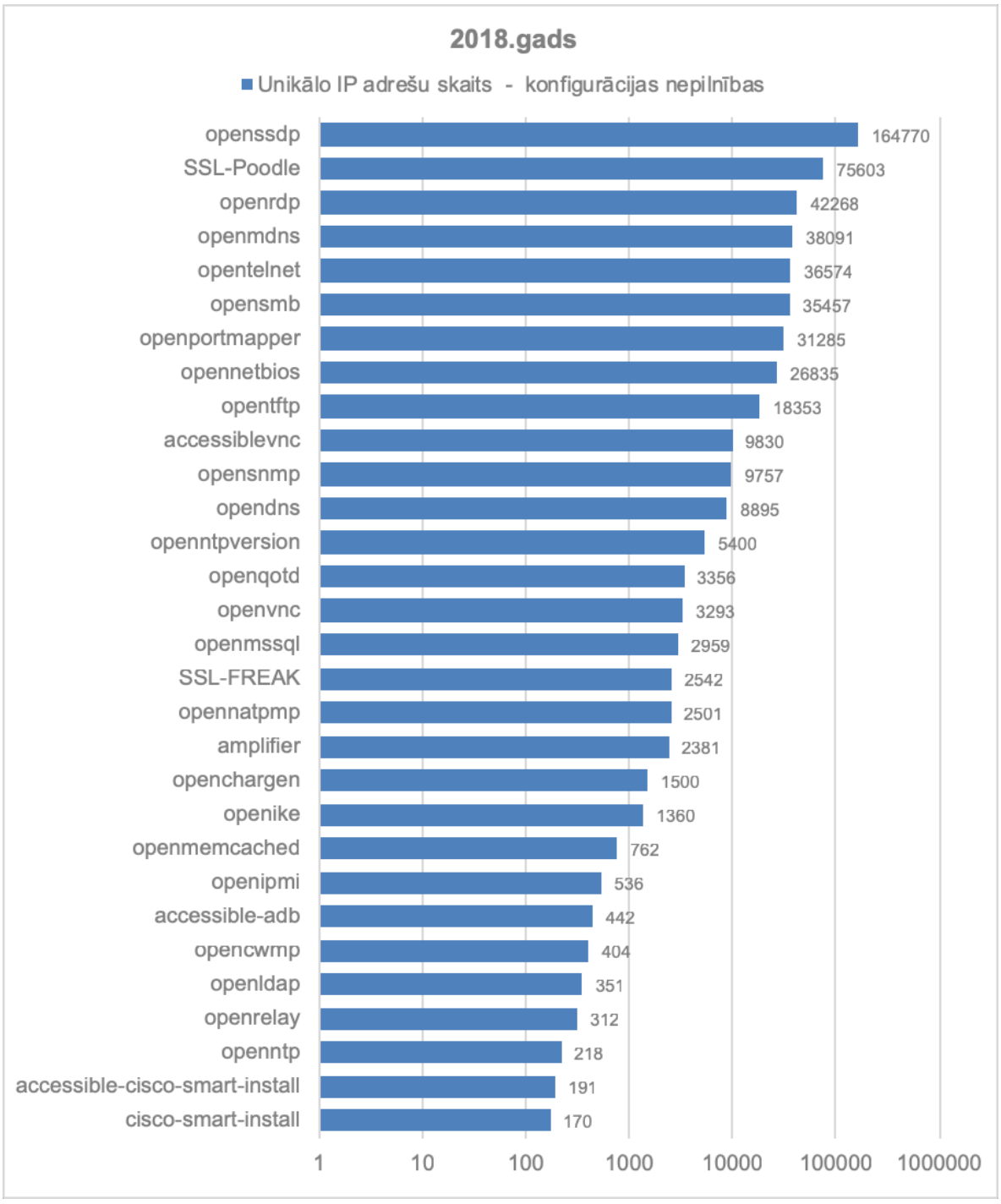
Trešo vietu topā ieņem *Moneromіner* – ļaunatūra, kas veic kriptovalūtas *Monero* (uz privātumu orientēta kriptovalūta, kas ieguvusi popularitāti kriminālajās aprindās) ieguvi, izmantojot iekārtas resursus, lietotājam to nezinot. Nesaudzīgi izmantojot iekārtas jaudu, var bīstami noslogot iekārtu vai pat to neatgriezeniski sabojāt. Kriptovalūtas ieguves ļaunatūras kļuva populāras pēc negaidīti straujā kriptovalūtu cenu kāpuma 2017.gada nogalē, bet kritās, strauji krītoties kriptovalūtu cenām. *Moneromіner* darbība pārskata periodā visaktīvākā bija jūnijā un jūlijā.

Vietu ļaunatūras topa augšgalā nemainīgi saglabā *Conficker*, kaut arī tā ir jau sen pazīstama un salīdzinoši vienkārši „ārstējama" ļaunatūra.

Topa augšgalā ir nokļuvušas arī *Mkero* un *Android Fobus*, kas ir mobilās ļaunatūras. *Mkero* spēj apiet *captcha* pārbaudes un, lietotājam nezinot, parakstās uz paaugstinātas maksas SMS saņemšanu. Savukārt *Android.Fobus* uzdodas par reklāmu bloķētāju (*ad-block*), bet patiesībā veic paaugstinātas maksas zvanus un ievāc lietotāju personīgo informāciju.

Viens veids, kā šāda mobilā ļaunatūra nonāk iekārtā, ir lietotājam pašam to uzinstalējot, gadījumos, kad šī ļaunatūra uzdodas par noderīgu lietojumprogrammu, piemēram, mobilo antivīrusu vai reklāmu bloķētāju, bet patiesībā slēpj sevī kaitīgu funkcionalitāti.

Otrs veids ir, lejupielādējot programmatūru no neoficiālas vietnes, kurā, atšķirībā no *Google Play* vai *App Store*, netiek veikta lietojumprogrammu drošības pārbaude. Šādam riskam ir pakļauti arī tie lietotāji, kuri iegādājas mobilo telefonu vai planšetdatoru internetā, izdarot izvēli par labu maksimāli zemākajai cenai. Rezultātā iespējams saņemt iekārtu ar neoficiālu *Android* operētājsistēmu, kurā uzstādītā programmatūra jau satur kaitnieciskas komponentes. Šādā iekārtā netiek arī nodrošināta iespēja pieslēgties *Google Play*, lai lejupielādētu nepieciešamās lietojumprogrammas, tā vietā lejupielāde notiek no kādas vietnes ķīnā, kura, visticamāk, neveic programmatūras pārbaudi, vai sliktākajā gadījumā apzināti atbalsta kaitnieciskas programmatūras izplatīšanu.



5.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2018. gadā ar apdraudējuma veidu – konfigurācijas nepilnība.

Openrdp ievainojamība, kas ir konfigurācijas nepilnību jeb ievainojamību topa (5.attēls) trešajā vietā, norāda uz aktivizētu attālināto piekļuvi jeb RDP (*Remot Desktop Protocol*), kas pieejama no publiskā tīkla un rada apdraudējumu, ja tiek izmantota pārāk vienkārša parole un netiek

ierobežota piekļuve, piemēram, izmantojot privāto savienojumu jeb VPN. 2018. gada ietvaros CERT.LV regulāri saņēma ziņojumus no cietušajiem par gadījumiem, kad uzbrucēji ir veiksmīgi iekļuvuši iekšējā tīklā, uzminot vāju RDP paroli, un radījuši darbības traucējumus vai pat finansiālus zaudējumus, nošifrējot vienas vai vairāku iekārtu (darbstaciju, serveru) saturu, par kuru atgūšanu pieprasījuši izpirkuma maksu.

CERT.LV uzskaita arī uzlauzto un izķēmoto mājaslapu gadījumus. 2018. gadā tika uzlauztas un izķēmotas 179 mājaslapas. Astoņos gadījumos tīmekļa vietne gada laikā tika uzlauzta atkārtoti.

2. Nozīmīgākie incidenti 2018. gadā

Pārskata periodā CERT.LV sadarbojās ar valsts un pašvaldību institūcijām, bankām, interneta pakalpojumu sniedzējiem un citām organizācijām dažādas bīstamības incidentu risināšanā. Pārskatā apkopoti nozīmīgākie incidenti, kas iezīmē gada tendences.

2.1. Piekļuves lieguma uzbrukumi (DoS un DDoS)

Janvārī pakalpojumu atteices uzbrukumu (DDoS) piedzīvoja veselības aprūpes kvalitātes un efektivitātes uzlabošanas programma e-veselība. Sistēma uz laiku tika padarīta nepieejama, bet datu noplūde nenotika. Uzbrukumu izdevās apturēt, atslēdzot sistēmai piekļuvi no ārvalstīm. Izpētes rezultātā tika secināts, ka sistēmai netika nodrošināta pienācīga DDoS aizsardzība un bija nepieciešami dažādi konfigurācijas uzlabojumi.

Paralēli e-veselības sistēmai DDoS uzbrukumi tika veikti arī ziņu portālam LETA, kura darbība uz laiku tika traucēta, un vēl vairākām valsts iestāžu tīmekļa vietnēm. Veicot visu augšminēto uzbrukumu analīzi, tika novērota zināma uzbrukumos iesaistīto resursu sakritība.

DDoS uzbrukums tika vērsts arī pret interneta vietni bilesuparadize.lv. Uzbrukums pārslogoja sistēmu, kas jau piedzīvoja palielinātu noslodzi saistībā ar XXVI Vispārējo latviešu Dziesmu un XVI Deju svētku biļešu tirdzniecības uzsākšanu. CERT.LV sniedza ieteikumus DDoS aizsardzības uzlabošanai.

Gada sākumā CERT.LV veica vairāku pārslodzes uzbrukumu analīzi, kas tika vērsti pret kādu mediju portālu. Tika konstatēts, ka uzbrukuma avots atradās ārpus Latvijas. CERT.LV sniedza ieteikumus aizsardzības uzlabošanai pret DDoS uzbrukumiem.

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.

Pārskata perioda otrajā pusē tika saņemti vairāki ziņojumi no tūrisma operatoriem par piekļuves atteices (DDoS) uzbrukumiem kompāniju tīmekļa vietnēm ar mērķi nodarīt kaitējumu uzņēmumu darbībai. Vairāki uzbrukumi ir nodarījuši kompānijām finansiālus zaudējumus. Atsevišķos gadījumos pirms uzbrukuma kompānijām izteikti telefoniski draudi.

2.2. Pikšķerēšana jeb personīgo datu izkrāpšana

Visa pārskata perioda garumā tika novēroti mēģinājumi izkrāpt lietotāju e-pasta piekļuves datus, izmantojot pikšķerēšanas e-pastus. Biežākie e-pastos izmantotie paņēmieni:

- aicinājums sekot e-pastā norādītajai saitei, lai veiktu atjauninājumus vai novērstu kādu radušos problēmu;
- aicinājums sekot saitei, lai pārietu uz jaunāko e-pasta versiju vai atjauninātu konta drošību;
- lai veiktu obligātos drošības atjauninājumus un saņemtu personalizētus ieteikumus;
- aicinājums sekot saitei, lai novērstu konta deaktivāciju, jo pārsniegta kvota vai noticis noteikumu pārkāpums;
- aicinājums administrator vārdā sekot saitei, lai pārbaudītu konta status.

Ja lietotājs atvēra e-pastā norādīto saiti un redzamajā formā ievadīja e-pasta lietotāja vārdu un parole, dati tika nosūtīti krāpniekiem. Kampaņas tika vērstas gan uz uzņēmumiem, gan valsts un pašvaldību iestādēm.

Tika saņemti arī vairāki ziņojumi par tiešsaistes platformu PayPal un Apple piekļuves datu izkrāpšanas mēģinājumiem. Krāpnieciskos e-pastos nosūtīti aicinājumi autentificēties atbilstošajās vietnēs, sekojot e-pastā norādītajai saitei, lai atrisinātu it kā radušos piekļuves vai pakalpojuma izmantošanas problēmu, vai aktivizētu kontu, kas ticis bloķēts pēc aizdomīgu aktivitāšu konstatēšanas.

Pārskata periodā izplatīta bija arī personas datu pikšķerēšana, upurim nosūtot e-pastu ar aicinājumu sūtīt personīgu informāciju (vārds, uzvārds, adrese, dzimšanas dati, pases kopija), lai saņemtu laimestu, mantojumu, kompensāciju vai vienkārši naudas pārskaitījumu.

Pārskata perioda sākumā viena no krāpniecisko e-pastu kampaņām tika noformēta kā pēdējais brīdinājums parāda atmaksai pirms lietas nodošanas parādu piedzinējiem.

2.3. Krāpšana

Saņemts ziņojums par krāpšanas mēģinājumu, nosūtot vairākus e-pastus it kā PayPal vārdā un pieprasot veikt samaksu, izmantojot Western Union, lai norēķinātos par neapmaksātajiem transporta pakalpojumiem, pretējā gadījumā draudot ar konta slēgšanu un arestu.

Pārskata periodā tika reģistrētas krāpnieciskas kampaņas, kurās iedzīvotāji saņēma zvanus krievu valodā it kā no kādas investīciju kompānijas, kas piedāvāja iesaistīties apšaubāmās finanšu operācijās, solot pasakainu peļņu. Sākotnējā telefonsaruna tika pārvirzīta uz *Skype* un zvanītāji aicināja upuri dalīties ar savas iekārtas ekrānu, kam sekoja aicinājums iegādāties bitcoin kriptovalūtu, ievadot maksājumu kartes datus, un investēt šo iegādāto kriptovalūtu krāpnieku norādītajā finanšu platformā. Zvanītāji izcēlās ar neatlaidību un uzstājību, tika pielietoti arī draudi, ja upuris atteicās pildīt zvanītāju norādījumus.

Visa gada garumā regulāri tika saņemti ziņojumi no lietotājiem par krāpniecisku e-pastu angļu vai latviešu 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. 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.

Savukārt uzņēmumiem joprojām aktīvi tika iesūtītas e-pasta vēstules uzņēmuma vadītāja vārdā ar jautājumu par konta atlikumu un iespēju veikt steidzamu pārskaitījumu uz ārvalstīm. Ticamības palielināšanai summas netika izvēlētas "apaļas", piemēram, 52 826.81 eiro. Daži e-pasti sagatavoti labā latviešu valodā. Lai novērstu šāda tipa uzbrukumus, CERT.LV iesaka izmantot rīkus, kas slēpj uzņēmuma vai iestādes tīmekļa vietnē izvietotās e-pasta adreses no skeneriem, kā arī izveidot SPF ierakstus, kas noteiktu, no kādiem serveriem atļauts sūtīt e-pastus ar noteiktiem domēna vārdiem, lai novērstu krāpniecisku e-pastu izplatīšanu.

Oktobrī tika saņemti vairāki ziņojumi par krāpniecisku loteriju, kas tika izplatīta lietotnē WhatsApp un solīja iespēju laimēt divas bezmaksas biļetes uz Ed Sheeran koncertu Lucavsalā, ja tiks sniegtas atbildes uz četriem vienkāršiem jautājumiem un telefona numurs koda saņemšanai. Taču, norādot savu telefona numuru, lietotājs veica parakstīšanos uz maksas īsziņu saņemšanu (informācija bija izlasāma turpat lapas lejasdaļā).

2.4. Ielaušanās mēģinājumi

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.

2.5. Ļaunatūra

Tika saņemti ziņojumi lielākoties par ļaundabīga koda izplatīšanu ar e-pastu starpniecību, pievienojot e-pastam ISO diska attēlu, ZIP vai RAR arhīvu ar izpildāmiem .EXE failiem, vai .DOC dokumenta datni. Atsevišķos gadījumos e-pastā tika norādīta saite, kuru aktivizējot, notika vīrusa ielāde no interneta.

Vairumā gadījumu lietotājiem nosūtītais ļaundabīgais kods bija paredzēts lietotāju elektroniskās informācijas (lietotājvārdi, paroles) iegūšanai, lai to nosūtītu uz saimniekserveri. Tika saņemti arī vairāki ziņojumi par šifrējošo izspiedējvīrusu iekļūšanu sistēmā. Par šo uzbrukumu upuriem pamatā tika izvēlēti uzņēmumi.

Tika saņemti arī vairāki ziņojumi par Latvijas IP adresēs uzturētiem kontrol- un komandcentriem (C&C):

- tārpa *Dorkbot* (nodrošina sāneju – backdoor – upura iekārtā) kontrolieri;
- *Hancitor* (ļaunatūra, kas tiek piegādāta ar inficētiem MS Office dokumentiem un tiek izmantota citu ļaunatūru, piemēram, banku trojāņu vai izspiedējvīrusu lejupielādei) kontrolieri;
- *JBifrost* (attālinātās piekļuves trojāņa RAT modifikācija) kontrolieri;

- *Neutrino* mūķa (exploit kit) kontrolieri;
- *Necurs* (zombiju tīkls jeb *botnet*, kas izplata dažāda veida ļaunatūru, no kurām zināmākā ir *Locky* šifrējošais vīruss) kontrolieri;
- *Pony* (ļaunatūra, kas specializējas personīgo datu zādzībā, taču spēj veikt arī kriptovalūtas, piem., bitcoin zādzību) kontrolieri;
- *NanoCore* (trojānis, kas ļauj uzbrucējam attālināti kontrolēt upura iekārtu un ievākt informāciju par, piemēram, ievadītajām parolēm) kontrolieri;
- *NetWire* (trojānis, kas veic maksājumu karšu datu zādzību) kontrolieri;
- *Loki* (ļaunatūra, kas paredzēta paroļu un citas sensitīvas informācijas zādzībai) kontrolieri;
- *Remcos RAT* (attālinātas kontroles rīks) kontrolieri;
- *AgentTesla* (programmatūra, kas paredzēta taustiņu nospiedienu fiksēšanai jeb *keylogger)* kontrolieri;
- *Citadel* (trojānis, kas paredzēts upura finanšu informācijas zādzībai un bankas kontu iztukšošanai) kontrolieri;
- *Gozi* (spiegojošā ļaunprogrammatūra, kas pārtver tīkla plūsmu, nolasa lietotāja piekļuves datus, kas saglabāti pārlūkprogrammās un e-pasta klientos, kā arī fiksē klaviatūras taustiņu nospiedienus (*keylogger*) un uz ekrāna redzamo informāciju (screen capture)) kontrolieri;
- *AZORult* (trojānis, kas paredzēts informācijas – pārlūkos saglabāto paroļu, dažādu aptaujas formu automātiski aizpildāmās informācijas, tērzētavu sarakstes, iekārtā instalēto programmu, lietotājvārdu, failu – zādzībai, kuru ļaunatūra pārtver un nosūta tālāk uz komandcentru) kontrolieri;
- *RevCodeRAT* (trojānis upura iekārtas attālinātai piekļuvei un pārvaldībai) kontrolieri;
- *Zbot*/*Zeus* (spiegojošā ļaunprogrammatūra, kas primāri orientēta uz informāciju par upura iekārtu, tiešsaistes piekļuves datiem un finanšu informāciju, bet var tikt pielāgota jebkuras citas informācijas ieguvei vai modificēta, lai traucētu iekārtas darbību vai iznīcinātu iekārtu) kontrolieri.

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

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

2.6. Kompromitētas iekārtas

Latvija turpināja būt interesants mērķis uzbrucējiem ar NATO un ES pretēju ideoloģiju. Par to liecināja arī CERT.LV jau iepriekš apzinātā ļaunatūra Latvijas Republikas Iekšlietu ministrijas IT sistēmās.

Ļaunatūras tehniskie parametri norādīja uz iespējamu Krievijas Federācijas drošības dienestu nesankcionētu iejaukšanos. Nozīmīgs darbs pie seku analīzes un instrukciju atjaunošanas noritēja arī 2018. gadā.

Pārskata periodā CERT.LV saņēma ziņojumus par kaitīgu saturu arī 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.

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

Pārskata periodā CERT.LV regulāri saņēma ziņojumus no uzņēmumiem, kas cietuši no šifrējošā izspiedējvīrusa uzbrukuma, kura rezultātā uzņēmumam ir tikuši nošifrēti serveri un darbstacijas. Parasti uzbrucēji piekļuvuši datiem, izmantojot RDP servisu, kuram uzminējuši pārāk vienkāršo piekļuves paroli. Bieži vien iznīcinātas arī datu rezerves kopijas.

2.7. Atbildīga ievainojamību atklāšana

Atbildīgas ievainojamību atklāšanas ietvaros tika saņemti 19 ziņojumi par starpvietņu skriptēšanas (XSS) ievainojamību 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.

Septiņiem ievainojamību atklājējiem nosūtīts pateicības raksts.

3. Informatīvie komunikācijas pasākumi

CERT.LV eksperti arī 2018. gadā turpināja sniegt intervijas un atbildēt uz mediju jautājumiem gan TV, gan presē un radio par dažādām aktuālām ar kiberdrošību saistītām tēmām. Pārskata periodā mediji lielāko interesi izrādīja par uzbrukumu e-veselības sistēmai un e-veselības datu drošību, uzbrukumu Dziesmu un deju svētku biļešu izplatītājam bilesuparadize.lv, Maksātnespējas administrācijas administratoru rindas sistēmas darbību un tās iespējamo ietekmēšanu, Facebook lietotāju datu drošību un *Yandex.Taxi* lietotnes drošību, dažādu drošības risinājumu, piemēram, *Kaspersky*, izmantošanu, kā arī par 6.oktobrī notikušo Saeimas vēlēšanu drošību.

3.1. Informatīvie pasākumi medijiem

6. martā CERT.LV piedalījās preses konferencē, kurā mediji tika informēti par sistēmas pārslodzes uzbrukumu Dziesmu un deju svētku biļešu izplatītājam bilesuparadize.lv.

3.2. Komunikācija digitālajā vidē

2018. gada laikā stabili pieauga sekotāju skaits populārajās sociālo tīklu platformās *Twitter* un *Facebook*:

- *Twitter* konta twitter.com/certlv sekotāju skaits pārskata perioda beigās bija **2086.**
- *Facebook* profila facebook.com/certlv sekotāju skaits pārskata perioda beigās bija **1075.**

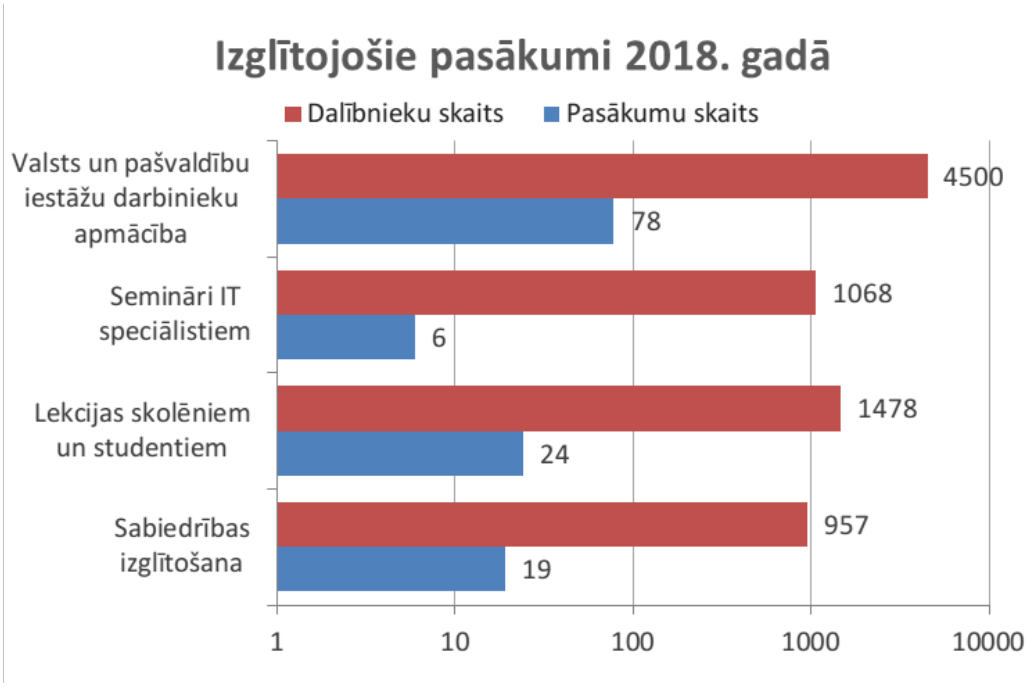
CERT.LV uztur tīmekļa vietni https://www.cert.lv, kurā tiek publicēta informācija par aktuāliem apdraudējumiem, ieteikumi IT drošības līmeņa paaugstināšanai, informācija par dažādiem notikumiem un pasākumu kalendārs. **Kopā gada laikā CERT.LV lapai bijuši 69,589 unikāli apmeklējumi jeb sesijas, kurus veikuši 42,249 lietotāji.**

CERT.LV turpināja uzturēt arī lietotāju izglītošanas portālu www.esidross.lv, regulāri publicējot jaunus rakstus un atbildot uz lietotāju komentāriem.

Pārskata periodā katru mēnesi sadarbībā ar SANS institūtu tika izdoti informatīvie kiberdrošības biļeteni „OUCH!" ikvienam interneta lietotājam.

4. Izglītojošie pasākumi

2018. gadā CERT.LV turpināja rīkot izglītojošus pasākumus par kiberdrošības jautājumiem IT drošības speciālistiem, valsts un pašvaldību iestāžu darbiniekiem, studentiem, skolēniem un citiem interesentiem. Pārskata periodā CERT.LV piedalījās 127 pasākumos un izglītoja 8003 klausītājus.



7.attēls – Pasākumu un apmācīto cilvēku skaits 2018. gadā.

Gada lielākais pasākums bija ikgadējā IT drošības konference „Kiberšahs 2018", kas notika 9. oktobrī *Radisson Blu Hotel Latvija* telpās. Konferenci klātienē apmeklēja vairāk nekā 500 dalībnieku, savukārt tiešsaistē tai bija 2000 unikālu skatījumu.

Konference tika organizēta sadarbībā ar *ISACA Latvijas nodaļu*, bet *LMT* un *dots.* arī šogad sniedza savu atbalstu. Konference tika daļēji līdzfinansēta no Eiropas Savienības CEF projekta "Improving Cyber Security Capacities in Latvia" (INEA/CEF/ICT/A2017/1528784).

4.1. CERT.LV organizētie pasākumi IT drošības speciālistiem

21. martā CERT.LV rīkoja semināru IT drošības speciālistiem „Esi drošs", kurā iepazīstināja klātesošos ar IT drošības aktualitātēm un aplūkoja tādas tēmas kā ievainojamību Meltdown un Spectre ietekme, mākoņdatošanas iespējas un riski, NIS direktīvas ieviešana Latvijā, Vispārīgā datu aizsardzības regula un drošības prasības, kā arī iepazīšanās ar CERT.LV un NIC.lv DNS ugunsmūra projektu.

9. oktobrī CERT.LV sadarbībā ar *ISACA Latvija nodaļu* rīkoja IT drošības konferenci „Kiberšahs 2018". Šogad konferences uzmanība tika pievērsta globālai kibertelpai, apdraudējumu

tendencēm, dažādiem rīkiem šo apdraudējumu ietekmes mazināšanai, kā arī dažādu tehnoloģisku un mazāk tehnoloģisku izaicinājumu pārvarēšanai.

6. decembrī CERT.LV rīkoja semināru IT drošības speciālistiem „Esi drošs", kurā iepazīstināja klātesošos ar CERT.LV aktualitātēm un aplūkoja tādas tēmas kā izmaiņas IT likumā, NIS direktīva, mūsdienīgu e-pasta standartu ieviešanas nosacījumi valsts un pašvaldību iestādēs, svarīgākās atziņas e-adreses ieviešanas posmā, sekas domēna vārda nepagarināšanai un kā uzlabot drošību, darbiniekam strādājot attālināti.

4.2. CERT.LV prezentācijas par IT drošību sabiedrības izglītošanai

No 19. līdz 23. martam Latvijā un visā Eiropā notika jau devītā Digitālā (agrāk pazīstama kā E-prasmju) nedēļa. 20. martā tika atzīmēta Digitālās drošības diena un tika organizētas vairākas diskusijas-tiešraides. CERT.LV pārstāvji piedalījās diskusijā „Drošība un pārliecība digitālajā vidē" un pasākumā „Kiberdrošības nakts", kas bija augsta līmeņa ekspertu diskusija par nacionālās kiberdrošības jautājumiem.

5. aprīlī CERT.LV pārstāvis piedalījās paneļdiskusijā „Development of Global Supply Chains and Ensuring Adequate Risk Management of Disruptions", kas norisinājās konferences „Global Transport Security and Safety for a Century" ietvaros.

19. aprīlī CERT.LV pārstāvis vadīja paneļdiskusiju „Domains and cybercrime: is there a light at the end of the tunnel?" Baltijas valstu domēnu nozarei veltītajā pasākumā „Baltic Domain Days".

25. aprīlī CERT.LV pārstāvis piedalījās paneļdiskusijā „Tiesiskums kibertelpā", kas notika konferences „Tiesiskās problēmas Latvijas simtgadē: retrospektīva un perspektīva" ietvaros.

26. maijā CERT.LV piedalījās Microsoft un VARAM organizētajā akcijā „Strādā jebkur", informējot pasākuma dalībniekus par IT drošības aspektiem, kas jāievēro, atrodoties ceļā un publiskās vietās.

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.

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

25. oktobrī CERT.LV pārstāvis uzstājās ar prezentāciju "Informācijas drošības kultūra" konferencē DSS ITSEC2018.

29. oktobrī CERT.LV pārstāvis piedalījās *Digital Freedom Festival* un EK rīkotajā diskusijā "Kas nodrošinās digitālās nākotnes kiberdrošību?".

31. oktobrī CERT.LV pārstāvis piedalījās *Valsts bērnu tiesību aizsardzības inspekcijas* organizētajā konferencē – domnīcā interneta drošības jautājumos "Iespējas, izaugsme un drošība internetā un dzīvē!", uzstājoties ar prezentāciju "Digitālā vide - kā sevi pasargāt".

16. novembrī CERT.LV pārstāvis piedalījās LMT tehnoloģiju dienā, uzstājoties ar prezentāciju "Kiberdrošības izaicinājumi mobilajos tīklos".

22. novembrī CERT.LV pārstāvis sniedza prezentāciju par aktualitātēm kiberdrošības jomā Valsts policijas rīkotajā starptautiskajā mācību konferencē "Kibernoziedzības apkarošana un prevencija".

4.3. CERT.LV dalība citos pasākumos un aktivitātēs

16. februārī CERT.LV pārstāvis mentora statusā piedalījās *Garage48* hakatonā. Mentoru uzdevums bija palīdzēt komandām, kuras izstrādāja un attīstīja dažādas kiberdrošības idejas, sniedzot padomus un ieteikumus izvēlētās idejas attīstīšanai.

1. jūnijā Accenture sadarbībā ar CERT.LV organizēja NightHack 2018, kuram pieteicās 40 IT drošības eksperti, bet par galveno balvu nakts garumā sacentās 25 speciālisti, pierādot savas zināšanas, prasmes un atjautību.

Sadarbībā ar Valsts policiju un Drošāka interneta centru tika izstrādāta mobilā lietotne pusaudžiem „Mana drošība". Tā sniedz iespēju pārbaudīt savas zināšanas par drošību internetā, aizpildot interaktīvu testu un izspēlējot improvizētu „čatu", kā arī turpat lietotnē ziņot par kaitīgu un nelegālu saturu vai problēmsituācijām.

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

5. Sadarbība ar valsts iestādēm

5.1. Sadarbība ar Aizsardzības ministriju

Regulāri notika tikšanās ar ministrijas Valsts sekretāru un komunikācija ar Nacionālās kiberdrošības politikas koordinācijas nodaļu.

CERT.LV regulāri piedalījās Aizsardzības ministrijas darba grupā par NIS direktīvas ieviešanu. Šī procesa ietvaros CERT.LV kopā ar Aizsardzības ministriju piedalījās izmaiņu sagatavošanā Informācijas tehnoloģiju drošības likumam un MK noteikumiem Nr.442 (Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām), lai tos varētu attiecināt uz pamatpakalpojumu sniedzējiem, digitālo pakalpojumu sniedzējiem un kritisko infrastruktūru. Tika iesniegti priekšlikumi normatīvo aktu projektu pilnveidošanai (piemēram, precizējot sistēmu auditācijas pierakstu saturu, elektroniskā pasta sistēmu drošības prasībām).

Pārskata periodā Aizsardzības ministrijas uzdevumā tika 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.

CERT.LV darbinieki Varis Teivāns un Baiba Kaškina tika apbalvoti ar Aizsardzības ministrijas goda rakstiem par veiksmīgu sadarbību un atbalstu, tā sniedzot savu ieguldījumu Latvijas valsts aizsardzībā un drošībā.

5.2. Citi sadarbības partneri

CERT.LV sadarbojās ar *Zemessardzes Kiberaizsardzības vienību*, kopīgi piedaloties dažādās tehniskajās mācībās, kā arī nodrošinot vienībai virtuālu treniņu vidi drošības incidentu risināšanas pilnveidei.

CERT.LV turpināja atbalstīt *Drošības ekspertu grupas (DEG)* darbību, kas nodrošina diskusiju forumu IT drošības speciālistiem gan no privātā, gan valsts sektora. *DEG* sanāksmes notika reizi mēnesī.

Pārskata periodā notika aktīvs CERT.LV darbs Saeimas vēlēšanu drošības koordinācijas grupā, veicot vēlēšanu infrastruktūras stiprināšanu pirmsvēlēšanu periodā, un nodrošinot infrastruktūras uzraudzību vēlēšanu gaitā. Vēlēšanu laikā kibertelpā novēroto aktivitāti CERT.LV vērtē kā mērenu, valsts drošību un vēlēšanas neapdraudošu. Ar dažādu intensitāti tika novēroti vairāki uzbrukumi e-pasta sistēmām, tīmekļa vietnēm un tīkla infrastruktūrai, arī mērķiem valsts sektorā. Taču tiem neizdevās radīt kaitējumu vai iedzīvotājiem jūtamu efektu; tos izdevās veiksmīgi atvairīt.

CERT.LV piedalījās diskusijās par darba grupas izveidi arī gatavojoties Eiropas Parlamenta vēlēšanām, lai izmantotu Saeimas vēlēšanās gūto pieredzi kiberapdraudējumu mazināšanai.

Latvijas Republikas Valsts policija 2018.gada 5.decembrī atzīmēja savu 100.gadi, kuras ietvaros tika pasniegtas jubilejas goda zīmes "Latvijas Valsts policijai 100". Arī CERT.LV vadītājas vietnieks Varis Teivāns par sniegto atbalstu Valsts policijai saņēma šādu apbalvojumu.

6. Starptautiskā sadarbība

Pārskata periodā CERT.LV stiprināja sadarbību ar citu valstu IT drošības incidentu novēršanas vienībām un starptautiskām organizācijām. CERT.LV speciālisti uzstājās ar prezentācijām starptautiskās konferencēs, semināros un apguva jaunas prasmes tehniskajās mācībās.

No 16. līdz 24. aprīlim Sanfrancisko norisinājās RSA konference, kurā CERT.LV pārstāvis Kārlis Podiņš kopā ar pētnieku Dr. Kenneth Geers sniedza prezentāciju „Cyberwar on a Shoestring: How Kim Jong Un Stole My Malware".

CERT.LV eksperti atklāja četras kritiskas industriālo vadības sistēmu ICS/SCADAs ievainojamības

(CVE-2018-10603, CVE-2018-10607, CVE-2018-10609, CVE-2018-10605) un vairāku mēnešu garumā koordinēja un sniedza atbalstu ievainojamo iekārtu izstrādātājam šo ievainojamību novēršanā. Šo ievainojamību izmantošana varētu novest pie neautorizētu komandu izpildes industriālo procesu vadības sistēmās, pakalpojuma atteices vai koda izpildes klienta iekārtā. Atklātās ievainojamības skāra enerģētikas sektoru visā Eiropā un pasaules valstīs, kurās tiek lietots IEC-60870-5-104 protokols, kā arī "MartemTELEM-GW6/GWM" iekārtas, kas pārsvarā tiek lietotas Baltijas valstīs un Somijā.No 8. līdz 10. novembrim Viļņā notika AIEEEE2018 konference, kurā CERT.LV pārstāvis Kārlis Podiņš kopā ar līdzautoru Arturu Lavrenovu (Latvijas Universitāte) prezentēja „Security Implications of Using Third-Party Resources in the World Wide Web".

6.1. Sadarbība ar CERT kopienu

Pārskata periodā CERT.LV vadītāja Baiba Kaškina turpināja pildīt TF-CSIRT Steering komitejas vadītāja pienākumus, piedaloties gan klātienes, gan attālinātās sanāksmēs un organizējot TF-CSIRT darbu. CERT.LV pārstāvji piedalījās *TF-CSIRT* un *FIRST* tehniskajos semināros un sanāksmēs.

NIS (Tīklu un informācijas drošības) direktīvas CERTu tīkla ietvaros CERT.LV pārstāvis piedalās "CSIRT Maturity" darba grupā. Šīs darba grupas ietvaros CERT.LV piedalījās nozares ekspertu (peer-review) audita vizītē Portugālē, Lisabonā, kur tika auditēta CERT.PT komanda (Portugāles valdības un nacionālais CERT), izmantojot SIM3 metodoloģiju (Security Incident Management Maturity Model) un „CSIRT Maturity" darba grupas vadlīnijas.

CERT.LV pārstāvis piedalījās Moldovas kiberdrošības centra akreditācijas procesā, kas nodrošināja centra iekļaušanu FIRST (Forum of Incident Response and Security Teams) organizācijā.

No 14. līdz 16. martam FIRST Technical Colloquium Osakā, Japānā, CERT.LV pārstāviji sniedza divas prezentācijas: "Die Hard 104: Attacking and Controlling IEC-60870-5-104 Protocol-Based ICS/SCADA IoT Network Devices." un "Beyond paste monitoring: deep information leak analysis".

NIS direktīvas CERTu tīkla ietvaros CERT.LV apmeklēja vairākas starptautiskas sanāksmes, kā arī darbojās divās darba grupās - vienā, kas papildināja un uzlaboja CERTu tīkla „Terms of Reference" dokumentu un otrā, kas veido Eiropas „Cyber Weather".

No 23. līdz 25. maijam „54th TF-CSIRT meeting" Varšavā CERT.LV pārstāvis sniedza prezentāciju „Technical Incident Analysis".

No 27. līdz 30. maijam CERT-EE simpozijā Tallinā CERT.LV pārstāvis sniedza prezentāciju „Responsible disclosure and ICS/SCADA security".

No 26. līdz 29. septembrim TF-CSIRT sanāksmē Viļņā CERT.LV pārstāvji gan vadīja sanāksmi, gan sniedza 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.

6.2. Sadarbība ar ENISA

Daudzveidīga sadarbība notika ar Eiropas Tīkla un informācijas drošības aģentūru.

CERT.LV pārstāvji piedalījās ENISA organizētajās mācībās „Cyber SOPEx", kas vērstas uz Eiropas CERT vienību savstarpējās sadarbības stiprināšanu. Mācībās piedalījās vairāk kā 70 speciālisti no nacionālajām kiberdrošības incidentu novēršanas institūcijām un CERT-EU.

No 4. līdz 9. jūnijam CERT.LV pārstāvji piedalījās ENISA rīkoto kiberdrošības mācību „Cyber Europe 2018" veidošanā, organizēšanā, vadīšanā un izpildē. Mācībās šogad iesaistījās vairāk kā 900 kiberdrošības speciālistu no 30 Eiropas Savienības dalībvalstīm, lai risinātu Eiropas līmeņa aviācijas krīzi. Intensīvā divu dienu mācību scenārijā, kas veidoja līdz šim visaptverošākās Eiropas Savienības kiberdrošības mācības, inscenētie notikumi risinājās simulētā mācību vidē, kurā mācību dalībniekiem nācās spēt identificēt un novērst liela mēroga apdraudējumus, reaģēt uz tiem, kā arī labāk izprast incidentu pārrobežu ietekmi. Kopējais simulēto mācībās izsūtīto scenārija vadības ziņojumu skaits sasniedza 23 222 e-pasta vēstules.

6.3. Sadarbība ar NATO CCDCoE

CERT.LV sadarbībā ar *NATO Cooperative Cyber Defence Centre of Exelence* Latvijā organizēja tehniskās kiberdrošības mācības „Crossed Swords 2018". Šogad mācību mērogs, salīdzinot ar citiem gadiem, bija daudz plašāks, tehniski sarežģītāks un izaicinošāks. Mācības aptvēra vairākus ģeogrāfiskus atrašanās punktus, iesaistot tajās gan informācijas tehnoloģiju (IT) kritiskās infrastruktūras uzturētājus, gan militārās vienības. Mācībās piedalījās vairāk kā astoņdesmit kiberdrošības ekspertu no piecpadsmit NATO CCD CoE dalībvalstīm.

No 23. līdz 27. aprīlim notika NATO CCD CoE organizētās kiberdrošības mācības „Locked Shields 2018", kurās CERT.LV iesaistījās gan mācību organizēšanā, strādājot pie mācību scenārija attīstīšanas, tehniskās vides izveides un vadot sarkanā karoga (uzbrucēju) komandas darbu, gan piedalījās mācību norisē. Šogad mācību vidē tika integrētas vairāk kā 4000 virtualizētas IT sistēmas un vairāk kā 2500 dažādi uzbrukumi. Mācībās tika izmantotas reālistiskas tehnoloģijas, tīkli un uzbrukumu metodes.

CERT.LV gan sadarbībā ar Kiberaizsardzības vienību, US EUCOM un Kanādas bruņoto spēku pārstāvjiem veidoja nacionālā līmeņa zilā karoga (aizstāvošo) komandu, gan piedalījās nacionālā līmeņa stratēģiskajā spēlē, risinot sarežģītus juridiskus un politiskus jautājumus un komunicējot tos ar medijiem.

CERT.LV par ieguldīto darbu ieguva „Locked Shields 2018" partneru statusu un kopā ar Aizsardzības ministriju un Kiberaizsardzības vienību saņēma NATO CCDCoE pateicības rakstu par ieguldījumu mācību organizācijā un norisē.

CERT.LV pārstāvis Bernhards Blumbergs par augstiem sasniegumiem un būtisku ieguldījumu centra un alianses kiberdrošības stiprināšanā un prestiža celšanā saņēma NATO CCDCoE

vēstnieka titulu. Šāds statuss tiek piešķirts uz diviem gadiem, un vēstnieku skaits ir ļoti ierobežots, - tas nepārsniedz septiņus vēstniekus.

16. aprīlī CERT.LV pārstāvis NATO CCDCoE pasniedza „Cyber Executive Seminar" Tallinā, Igaunijā.

No 30. maija līdz 02. jūnijam NATO CCDCoE konferencē „CyCon" Tallinā CERT.LV pārstāvis Kārlis Podiņš sadarbībā ar pētnieku Dr. Kenneth Geers sniedza prezentāciju „Aladdin's Lamp: The Theft and Re-weaponization of Malicious Code".

No 2. līdz 8. septembrim CERT.LV pārstāvis pasniedza NATO CCDCoE "Malware and Exploitation Essentials" kursu Tallinā, Igaunijā.

No 26. līdz 28. novembrim CERT.LV pārstāvis pasniedza NATO CCDCoE „Cyber Executive Seminar" kursu Tallinā, Igaunijā.

No 27. līdz 30. novembrim CERT.LV pārstāvji piedalījās NATO CCDCoE kiberdrošības mācībās „Cyber Coalition 2018", kurās tika iesaistīti aptuveni 700 sabiedroto spēku, partneru, industrijas un akadēmiskās vides pārstāvju, lai uzlabotu sadarbību un procedūras informācijas apmaiņai, kibertelpas novērtējumam un lēmumu pieņemšanai.

7. ES projektu īstenošana

7.1. 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.

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

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

No 23. līdz 26. septembrim projekta "Improving Cyber Security Capacities in Latvia" ietvaros CERT.LV pārstāvis piedalījās SIM3 auditoru kursos Viļņā, lai iegūtu SIM3 auditora sertifikāciju.

9.oktobrī notika kiberdrošības konference "Kiberšahs 2018", kas tika līdzfinansēta no projekta līdzekļiem.

7.2. Projekta "Cyber Exchange" īstenošana

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

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

8. Citi uzdevumi

Tika uzsākts 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 (domēnu vārdi, IP adreses u.c.). Projekta ieviešana uzsākta 4 iestādēs. Projekta ietvaros ir bijuši jau vairāki gadījumi, kuros nostrādājusi aktīvā aizsardzība, pasargājot iekārtas no inficēšanas.

Atskaiti sagatavoja:
CERT.LV sabiedrisko attiecību grupas vadītāja Līga Besere, tālrunis 67085888,
e-pasts liga.besere@cert.lv

2019. gada 31. maijā