Latvijas universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

2020 C4

Publiskais pārskats par CERT.LV uzdevumu izpildi

2020. gada 4. ceturksnis (01.10.2020 – 31.12.2020.)

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

2020. gada 4. ceturksnī tika reģistrētas 166 603 unikālas apdraudētas IP adreses, kas ir par nepilniem 5% vairāk nekā iepriekšējā ceturksnī, bet par 17% mazāk nekā šajā pašā periodā pirms gada.

Pārskata periodā Latvijas interneta telpā izplatītākie apdraudējumi:

- konfigurācijas nepilnības (78 811 unikāla IP adrese) ar kāpumu par 2% pret iepriekšējo periodu;
- otrs izplatītākais bija ļaundabīgs kods (15 755 unikālas IP adreses) ar kāpumu par 12%;
- bet trešais - ielaušanās mēģinājumi (2015 unikālas IP adreses) ar kāpumu 3%.

Ceturksni iezīmēja galvenokārt piekļuves atteices (DDoS) uzbrukumi uzņēmumiem ar izspiešanas mēģinājumiem un krāpnieciskas aktivitātes, ar mērķi iegūt iedzīvotāju finanšu līdzekļus.

Uzņēmumi turpināja saņemt draudu vēstules no izspiedējiem, kurās tika pieprasīts maksājums *Bitcoin* kriptovalūtā, lai novērstu uzņēmuma darbības apturēšanu ar līdz pat 2 Tb/s lielu DDoS uzbrukumu. Iebiedēšanas nolūkos tika veikti īslaicīgi piekļuves atteices uzbrukumi 20 -180 Gb/s apmērā, kas ilga no nepilnas stundas līdz pāris dienām. Lai arī dažu uzņēmumu pakalpojumi uzbrukumu rezultātā vairāku stundu garumā nebija pieejami, uzņēmumi noziedznieku prasībām nepakļāvās un veica preventīvas darbības, lai nodrošinātos pret līdzīgiem pasākumiem nākotnē.

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.

Iedzīvotāji turpināja saņemt krāpnieciskus telefona zvanus. Daļā gadījumu krāpnieki uzdevās par banku darbiniekiem, apgalvojot, ka noplūduši lietotāju norēķinu karšu dati un nepieciešamas steidzamas darbības, lai pasargātu lietotāja finanses, un aicināja izpaust konta piekļuves informāciju. Citkārt zvanītāji uzdevās par kādas iestādes darbiniekiem, kas apkaro finanšu krāpniecību, un aicināja iedzīvotājus uzstādīt savās iekārtās *AnyDesk* programmatūru, kas nodrošinātu uzbrucējiem attālinātu piekļuvi upura iekārtai, apgalvojot, ka minētā programmatūra nepieciešama failu apmaiņas nodrošināšanai.

Lietotnē *WhatsApp* tika novērotas vairākas krāpnieciska loterijas, kurās lietotāji tika aicināti ievadīt savu maksājumu karšu datus, lai saņemtu *Adidas* apavus vai jaungada balvu no *Huawei*. Svētku sezonai tuvojoties, strauji pieauga arī krāpniecisku interneta veikalu skaits.

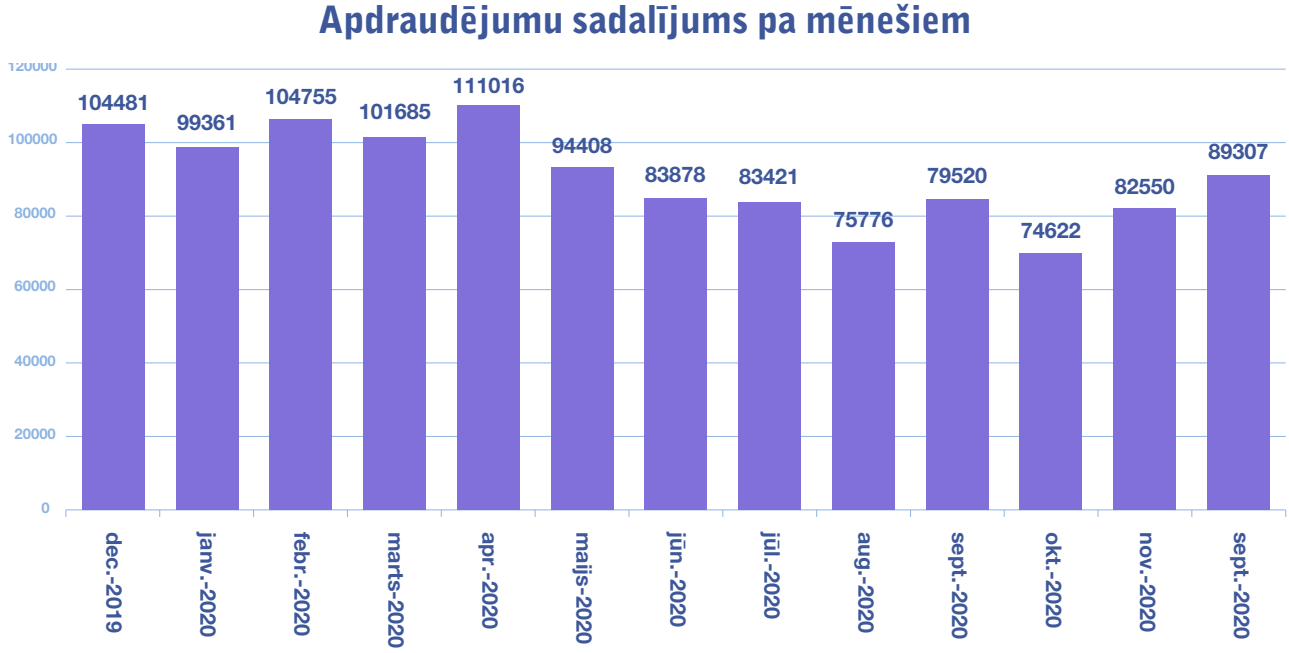
Tika novērotas arī veiksmīgas uzbrucēju aktivitātes ar kaitīgu e-pastu izmantošanu. Aktīvi turpinājās ļaunatūras *Emotet* izplatība, lietotājiem atverot inficētu e-pasta pielikumu un iespējojot pielikumā iekļauto *Macros* funkcionalitāti. Tika fiksētas arī veiksmīgas pikšķerēšnas aktivitātes, kuru rezultātā valsts iestāžu darbinieki ievadīja savu e-pastu piekļuves datus krāpnieku izveidotās tīmekļa vietnēs.

1.-2. oktobrī, uzsākot *Eiropas Kiberdrošības mēnesi*, tiešsaistē notika CERT.LV organizētā tehniskā kiberdrošības konference *Kiberšoks 2020*, kurā ar praktiskiem piemēriem un demonstrācijām tika padziļināti aplūkotas dažādas tehniskas ar kiberdrošību saistītas tēmas. Konferencei pieteicās un to attālināti vēroja 760 dalībnieki; prezentācijas sniedza septiņi lektori no piecām dažādām valstīm. Paralēli konferencei sadarbībā ar *Cybexer Technologies* un *Tet group* norisinājās arī *Capture the Flag (CTF)* sacensības, kurās spēkiem mērojās 100 dalībnieki jeb 29 komandas.

Pārskata periodā CERT.LV par IT drošību izglītoja 2922 cilvēkus, iesaistoties 27 izglītojošos pasākumos. Ņemot vērā epidemioloģisko situāciju valstī, lielākā daļa pasākumu notika tiešsaistē.

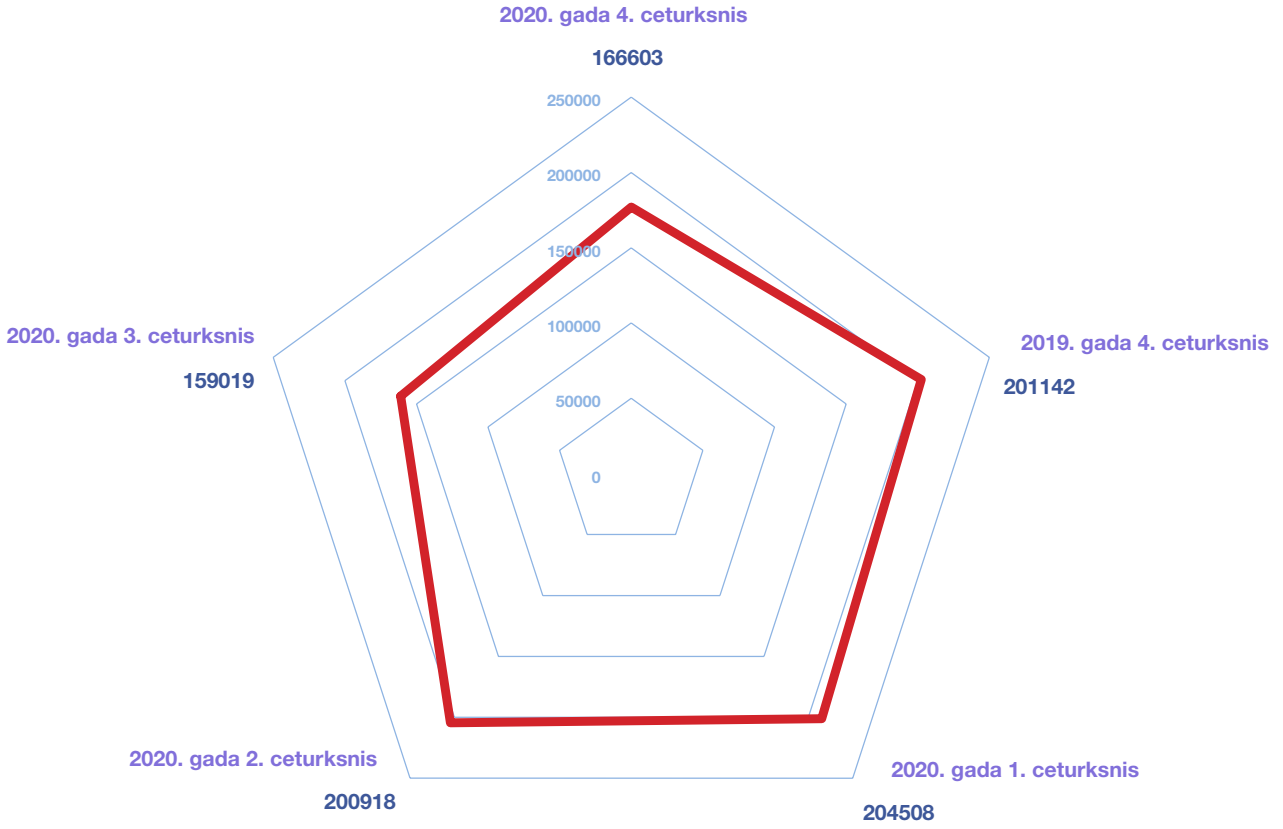
1. Elektroniskās informācijas telpā notiekošo darbību atainojums

Ik mēnesi CERT.LV apkopo informāciju par apdraudētajām Latvijas IP adresēm. Lai sniegtu pilnvērtīgāku Latvijas kibertelpas pārskatu un nodrošinātu datu starptautisku salīdzināmību, CERT.LV apdraudējumu uzskaitei izmanto starptautiski lietotu incidentu taksonomiju (eCSIRT.net projekta izveidotā taksonomija, kas nosaukta par *Reference Security Incident Taxonomy*). Taksonomija ir formalizēts veids kā CERT.LV apkopo, sadala kategorijās un reprezentē par apdraudējumiem iegūto tehnisko informāciju. Statistikā visi CERT.LV reģistrētie apdraudējumi tiek uzskaitīti vienkopus, sadalot tos pa apdraudējumu veidiem (piemēram, ļaunatūra, ielaušanās, krāpšana), kā arī pa ļaunatūru (piemēram, *Confiker*, *Zeus*, *Mirai*) un konfigurācijas nepilnību (piemēram, *Opendns*, *Openrdp*) tipiem.



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

Apdraudējumu sadalījums pa ceturkšņiem

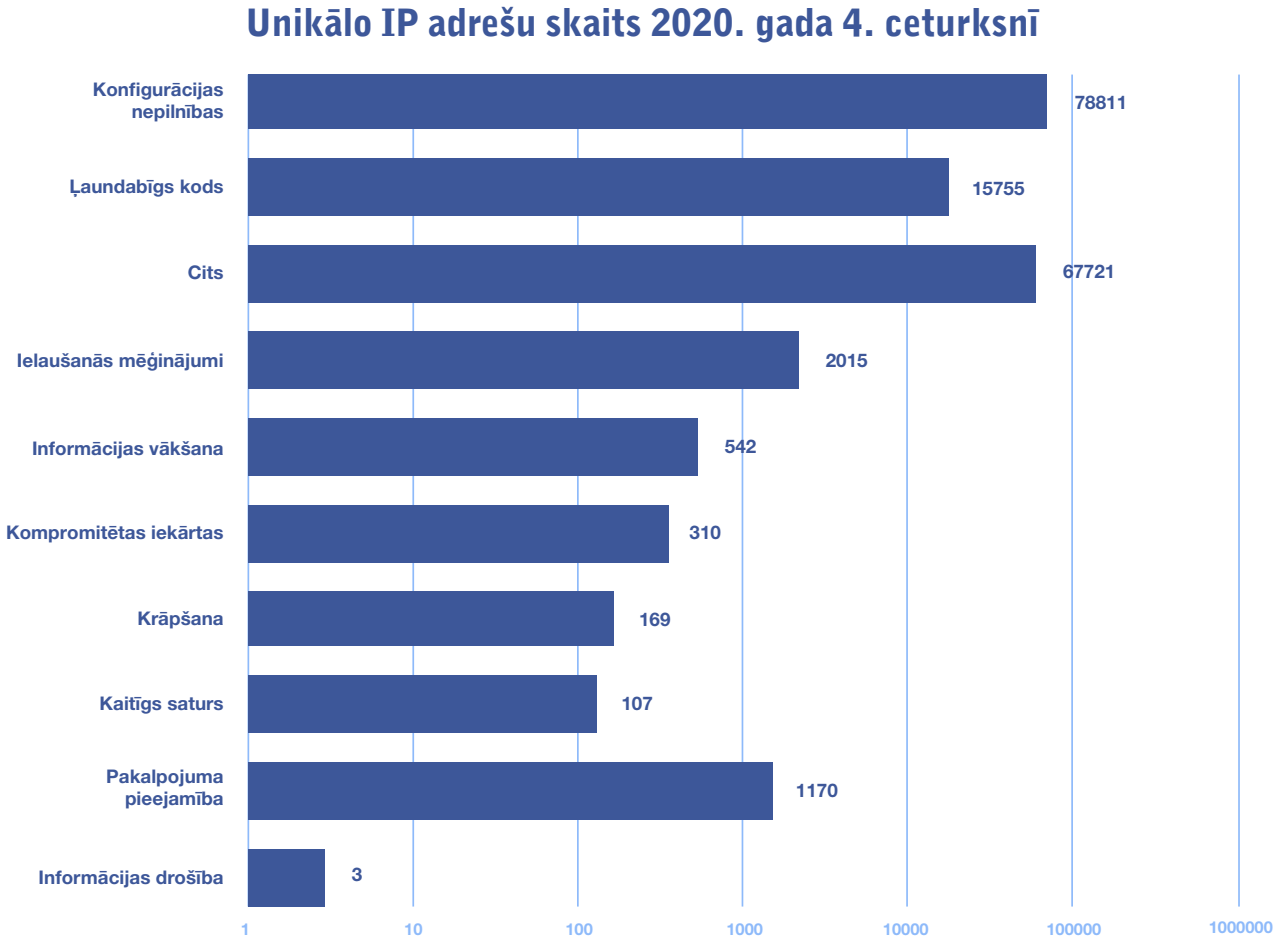


2. attēls – CERT.LV reģistrētās apdraudētās IP adreses pa ceturkšņiem 2019. un 2020. gadā.

CERT.LV pārskata periodā ik mēnesi apkopoja informāciju vidēji par 75 000 – 80 000 ievainojamu unikālu IP adrešu.

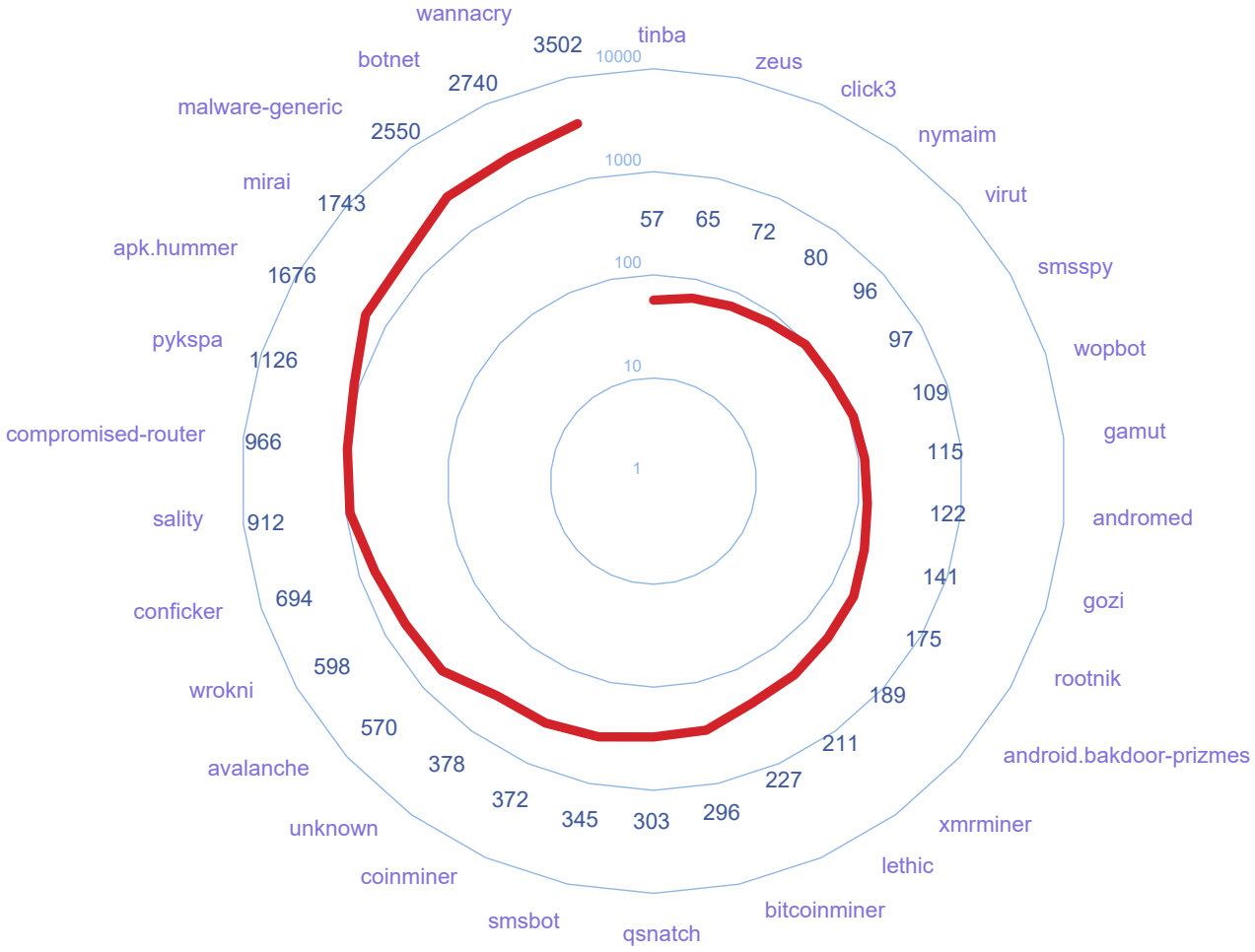
2020. gada 4. ceturksnī tika reģistrētas 166 603 unikālas apdraudētas IP adreses, kas ir par nepilniem 5% vairāk nekā iepriekšējā ceturksnī, bet par 17% mazāk nekā šajā pašā periodā pirms gada.

Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (78 811 unikāla IP adrese) ar kāpumu par 2% pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs kods (15 755 unikālas IP adreses) ar kāpumu par 12%, bet trešais - ielaušanās mēģinājumi (2015 unikālas IP adreses) ar kāpumu 3%.



3. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2020. gada 4. ceturksnī pa apdraudējumu veidiem.

Unikālo IP adrešu skaits – ļaundabīgs kods 2020. gada 4. ceturksnī



4. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2020. gada 4. ceturksnī ar apdraudējuma veidu – ļaundabīgs kods.

Ceturkšņa ietvaros novērotās izmaiņas reģistrēto apdraudēto IP adrešu apjomā ir nebūtiskas.

Topa augšgalā turpina atrasties *WannaCry* (*WannaCrypt*) – ļaunatūra ar šifrējošo potenciālu. Šīs ļaunatūras izplatība vērojama galvenokārt privātajā sektorā. Izplatību iespējams novērst, uzstādot *Windows* iekārtu atjauninājumus.

Nemainīgi topa augšgalā atrodas *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, nomainot noklusēto paroli.

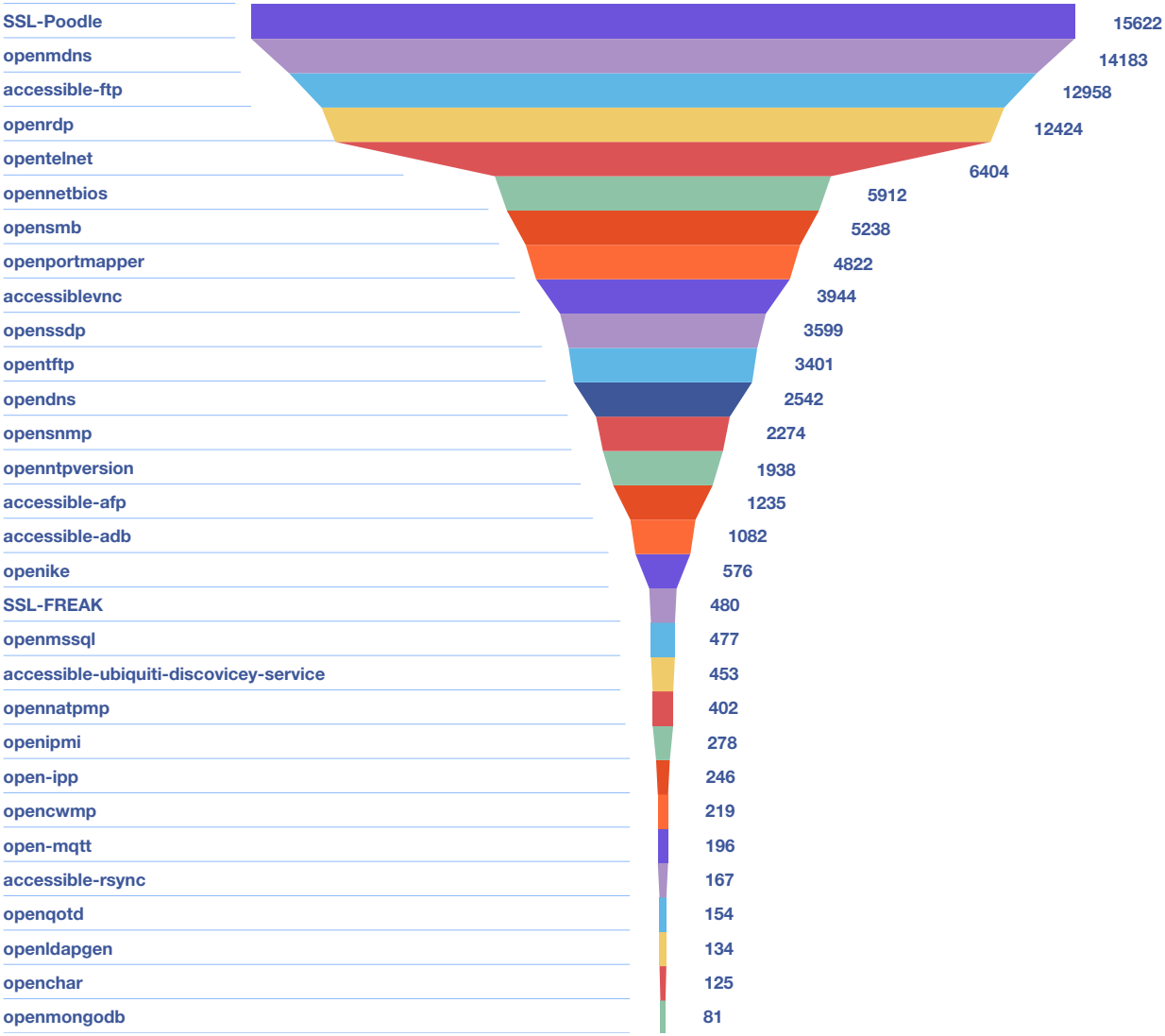
Piekto pozīciju ļaunatūras topā ieņem *Android Hummer* (*Hummingbad*), kas tiek novērota kopš decembra, ir paredzēta *Android* operētājsistēmām un tiek izmantota, lai demonstrētu lietotājam reklāmas, kā arī veikt citu lietotņu lejupielādi, tādejādi radot peļņu kiberuzbrucējiem.

Konfigurācijas nepilnību topa augšgalā esošā *OpenmDNS* (*multicast DNS*) pakļauj iekārtas liela apjoma informācijas noplūdes riskam, kā arī šīs iekārtas var tikt izmantotas UDP amplifikācijas uzbrukumos, radot piekļuves traucējumus citām iekārtām un organizāciju resursiem.

Arī konfigurācijas nepilnība *Accessible-FTP* pakļauj noplūdes riskam sensitīvu informāciju un piekļuves datus, jo FTP datu pārraides protokols nenodrošina pārraidāmo datu šifrēšanu, ja vien netiek izmatota papildu aizsardzība TLS vai SSL protokola formā (attiecīgi FTPS).

Konfigurācijas nepilnība *OpenRDP* arī joprojām atrodas topa augšgalā. Tā bieži tiek izmantota, lai piekļūtu iekārtām un tās sašifrētu. Ja netiek ievērota labā prakse un netiek ierobežota piekļuve RDP servisam, piemēram, ierobežojot 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 uzstādīta pietiekami droša piekļuves parole.

Unikālo IP adrešu skaits - konfigurācijas nepilnības 2020. gada 4. ceturksnī



5. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2020. gada 4. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

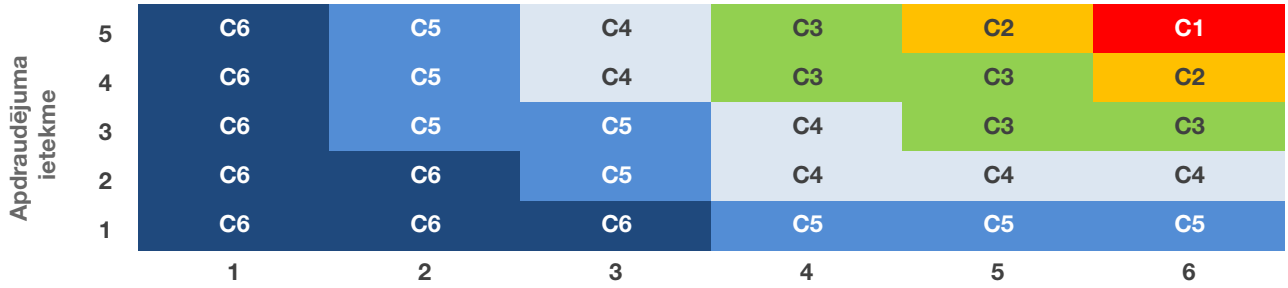
Pilnvērtīgākam kibersituācijas novērtējumam CERT.LV pirmajā ceturksnī ir uzsākusi Apvienotās Karalistes Nacionālā kiberdrošības centra (NCSC) izveidotās apdraudējumu matricas adaptāciju. Matricā ievietotie apdraudējumi tiek grupēti pēc tā, cik nozīmīga ir skartā iestāde vai uzņēmums un/vai cik plašu sabiedrības daļu apdraudējums ietekmē, kā arī pēc tā, cik būtiskas sekas attiecīgais apdraudējums radīs. Apvienojot visus faktorus, apdraudējumi tiek iedalīti 6 kategorijās:

- C1 – nacionāla līmeņa apdraudējums, ietekmēta pamatpakalpojumu sniegšana, apdraudēta ekonomiskā vai politiskā stabilitāte;
- C2 – augstas nozīmes apdraudējumi, ietekmētas valsts iestādes, nacionālā infrastruktūra;
- C3 – nozīmīgi apdraudējumi, plaša ietekme uz komerciālo sektoru, valsts un pašvaldību iestādēm;
- C4 – būtiski apdraudējumi, vidēja ietekme uz komerciālo sektoru, valsts un pašvaldību iestādēm;
- C5 – mēreni apdraudējumi, neliela ietekme uz komerciālo sektoru, valsts un pašvaldību iestādēm;
- C6 – ikdienas apdraudējumi, ietekmē atsevišķus indivīdus, nenozīmīga ietekme uz uzņēmumiem vai valsts un pašvaldību iestādēm.

Gandrīz 99% apdraudējumu ietilpst maznozīmīgu apdraudējumu kopā (C6), un ir saistīti ar individuālu lietotāju iekārtām vai plaši izplatītiem ikdienišķiem, automatizētiem uzbrukumu mēģinājumiem uzņēmumiem vai valsts un pašvaldību iestādēm.

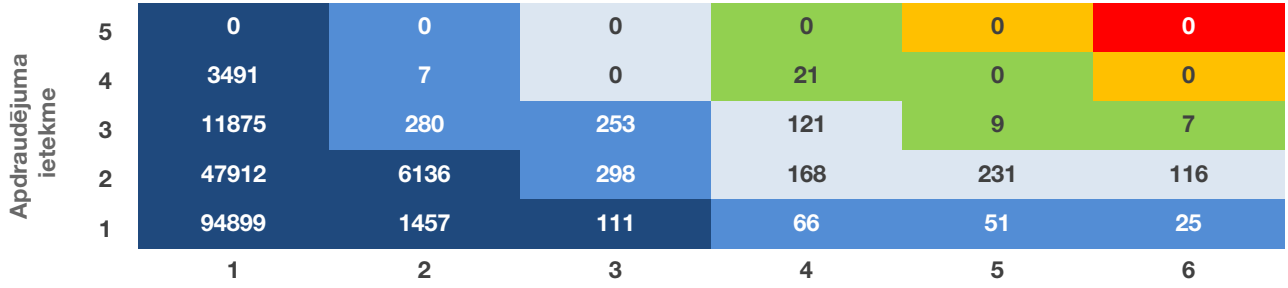
Nacionāla līmeņa apdraudējumi (C1) un augstas nozīmes apdraudējumi (C2) pārskata periodā nav reģistrēti. Nozīmīgi plašas ietekmes apdraudējumi (C3) veido 0,03% (37 unikālas apdraudētas IP adreses/gadījumi) no visiem kategorizētajiem apdraudējumiem. Lielākā daļa šo apdraudēto IP adrešu saistītas ar ļaundabīgu kodu valsts un pašvaldību iestādēs, kā arī vairākās veselības aprūpes iestādēs. Tās ir galvenokārt ļaunatūra *WannaCry* ar šifrējošo potenciālu, ļaunatūra

Apdraudējumu matrica



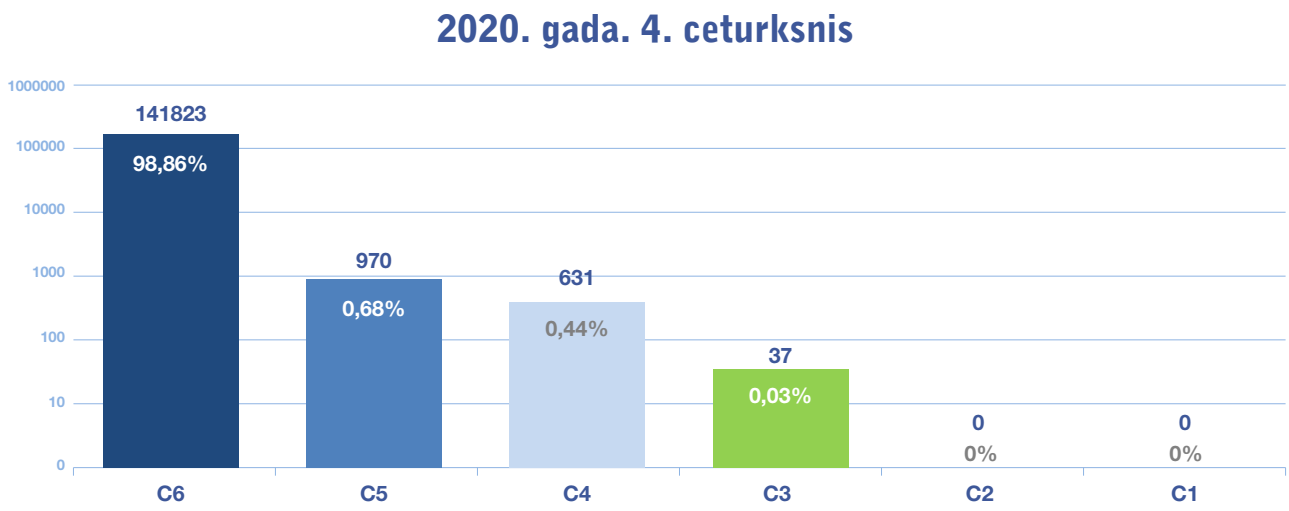
6. attēls – Apdraudējumu matricas sadalījums kategorijās.

2020. gada. 4. ceturksnis



7. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu izvietojums matricā 2020. gada 4. ceturksnī valsts un pašvaldību institūcijās.

Android Hummer, kas ģenerē ienākumus uzbrucējam, demonstrējot reklāmas un lejupielādējot citas lietotnes inficētajā iekārtā, *Emotet* spiegojošā ļaunatūra, kas paredzēta sensitīvas informācijas izgūšanai, kā arī ļaunatūra *Sality* ar *backdoor* funkcionalitāti, kas paver ceļu uz iekārtu citām ļaunatūrām, kā arī pievieno inficētās iekārtas robotu tīklam.



8. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu sadalījums apdraudējumu kategorijās pēc apdraudējuma ietekmes (matrica) 2020. gada 4. ceturksnī.

Lielākā daļa C4 līmeņa incidentu (būtiski apdraudējumi ar vidēju ietekmi) bija konfigurācijas nepilnības (*Accessible-ftp*, *OpenRDP*, *Openntpversion*, *OpenDNS*, *Openike*, u.c.), kas, galvenokārt, rada informācijas noplūdes riskus, pakalpojuma pieejamība un ielaušanās mēģinājumi, kas novēroti augstas un vidēji augstas prioritātes iestādēs – vairākās valsts iestādēs, kā arī virknē pašvaldību un universitāšu.

Lai mazinātu kopējo apdraudēto IP adrešu skaitu, CERT.LV kopā ar Latvijas Interneta asociācijas (LIA) Net-Safe Latvija Drošāka interneta centru ir izveidojuši iniciatīvu *Atbildīgs interneta pakalpojumu sniedzējs*, kuras ietvaros saprašanās memorands tiek parakstīts ar ieinteresētajiem interneta pakalpojumu sniedzējiem (IPS), lai tie varētu informēt savus klientus par viņu iekārtās konstatētajiem apdraudējumiem. Atbildīgo IPS skaits līdz pārskata perioda beigām saglabājās bez izmaiņām – 13.

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

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

2.1 Krāpšana

Oktobra vidū lietotnē *WhatsApp* izplatījās krāpnieciska rakstura ziņas par iespēju saņemt bezmaksas *Adidas* apavus un T-kreklus. Lai dabūtu šo balvu, lietotājs tika aicināts nosūtīt šo ziņu vēl 20 draugiem, pēc tam parādījās lejupielādes poga. Pēc saņemtajiem ziņojumiem, atkarībā no iekārtas, lejupielādes poga lietotājus pāradresēja uz apšaubāmas reputācijas vietnēm vai servisiem, piemēram, iepazīšanās portālu, pārlūka paplašinājumu u.c. CERT.LV ieteica lietotājiem šo krāpniecisko *WhatsApp* ziņu ignorēt un nekādā gadījumā nepārsūtīt savam kontaktu lokam!

Līdzīgi kā iepriekš, arī oktobrī tika saņemti ziņojumi par krāpniekiem, kas zvanīja un izlikās par banku darbiniekiem. Zvanītāji apgalvoja, ka noplūduši lietotāja norēķinu kartes dati un nepieciešams ātri reaģēt, lai pasargātu lietotāja finanses. Sarunas gaitā tika pieprasīts nosaukt bankas konta piekļuves informāciju, kas it kā nepieciešama kartes bloķēšanai. Krāpnieki parasti sazinājās krievu valodā. Bankas un CERT.LV atgādināja, ka bankas pašas nekad nezvana ar lūgumu izpaust PIN kodus vai citu lietotāja informāciju.

Novembra izskaņā CERT.LV saņēma pirmos ziņojumus par krāpnieciskiem interneta veikaliem, kas piedāvāja iegādāties preces un pakalpojumus par neticami zemām cenām. Krāpnieciski interneta veikali pastāv visu laiku, taču pirmssvētku periodā krāpnieki kļūst īpaši aktīvi un cenšas izmantot pircēju vēlmi veikt īpaši izdevīgus pirkumus vai atrast unikālus piedāvājumus.

Novembra vidū CERT.LV saņēma vairākus ziņojumus no Latvijas iedzīvotājiem par aizdomīgām īsziņām it kā no Valsts policijas un TELE2, kurās brīdināts uzmanīties no banku krāpniekiem. Īsziņā tika norādīta arī saite papildu informācijai. Tā kā minētā saite veda uz manadrosiba.lv, nevis Valsts policijas vai TELE2 oficiālajām vietnēm, tad SMS saņēmēji pauda neuzticību saņemtajai informācijai. Tika noskaidrots, ka īsziņās iekļautā informācija ir patiesa un tās izsūtījusi Valsts policija un TELE2, kas par šo kampaņu publicēja informāciju arī savos sociālajos tīklos. Par saņemtajiem ziņojumiem CERT.LV informēja Valsts policiju. CERT.LV aicina lietotājus, saņemot aizdomīgu informāciju, pārbaudīt tās patiesumu, apmeklējot oficiālu avotu tīmekļa vietnes un sociālos tīklus. Savukārt uzņēmumiem un iestādēm, rīkojot šādas un līdzīgas kampaņas – savās vietnēs un sociālajos tīklos uzturēt aktuālu un viegli pamanāmu informāciju par notiekošo kampaņu.

Decembra otrajā pusē liela daļa Latvijas iedzīvotāju saņēma īsziņu ar aicinājumu ziedot akcijai *Eņģeļi pār Latviju*. Īsziņās un saistītajā tīmekļa vietnē ievietotajā banerī bija norādīts ar labdarības akciju nesaistīts telefona numurs ziedojumiem. Akcijas *Eņģeļi pār Latviju* organizatori par minēto krāpniecību vērsās ar iesniegumu Valsts policijā.

2.2. Pikšķerēšana jeb svarīgo datu izkrāpšana

Gan oktobrī, gan arī decembrī īsi pirms svētkiem, CERT.LV saņēma daudzus ziņojumus par pikšķerēšanas e-pastiem, kas izsūtīti Latvijas Pasta vārdā par it kā aizturētu sūtījumu. E-pastā tika skaidrots, ka sūtījums aizturēts, jo nav veikta piegādes apmaksa. E-pastā tika norādīta pikšķerēšanas saite, kur nokavēto maksājumu iespējams veikt. Krāpniecības mērķis – iegūt lietotāja norēķinu kartes datus. Līdzīgi e-pasti tika novēroti arī citu piegādes uzņēmumu vārdā – *DHL* un *Omniva*. CERT.LV aicināja iedzīvotājus būt modriem, saiti vaļā nevērt un saņemtos e-pastus dzēst. Savukārt gadījumā, ja tomēr dati ievadīti – aicināja operatīvi sazināties ar savu banku un informēt par notikušo.

Decembra beigās tika saņemti ziņojumi par telefonkrāpniekiem, kuri zvanīja Latvijas iedzīvotājiem un izlikās par kādas iestādes darbiniekiem, kas it kā apkaro finanšu krāpniecību. Krāpnieki krievu

valodā apgalvoja, ka lietotāja dati iesaistīti aizdomīgos finanšu darījumos, un aicināja upuri operatīvi sadarboties, lai darījumus apturētu. Krāpnieki pieprasīja uz upura iekārtas instalēt *AnyDesk* programmu, it kā failu apmaiņai (realitātē *AnyDesk* nodrošina attālinātu piekļuvi iekārtai). CERT.LV aicināja iedzīvotājus būt modriem un neuzķerties, kā arī sazināties ar Valsts policiju, ja ir nācies kļūt par upuri šādām krāpnieciskajām darbībām.

Gada nogalē lietotnē *WhatsApp* izplatījās krāpnieciska rakstura ziņas par iespēju saņemt bezmaksas *Huawei* Jaungada dāvanu. Lai šo balvu iegūtu, lietotājs tika aicināts piedalīties laimes akā un atvērt pareizo dāvanu, kā arī aizpildīt īsu aptaujas anketu. Šādas loterijas tiek rīkotas, lai panāktu, ka lietotājs parakstās uz kādu maksas servisu, vai iegūtu maksājumu kartes datus/piekļuvi kartes finanšu līdzekļiem. Lietotājs tiek aicināts ievadīt maksājumu kartes informāciju norādītajā formā, lai it kā veiktu laimētās balvas piegādes apmaksu, parasti dažu eiro apmērā.

2.3. Pakalpojuma pieejamība (DDoS)

Virkne finanšu institūciju un uzņēmumu gan Latvijā, gan arī Eiropā pārskata periodā piedzīvoja apjomīgu izkliedēto piekļuves lieguma (DDoS) uzbrukumu (20-180 Gb/s), kā rezultātā atsevišķu institūciju resursi/pakalpojumi vairāku stundu garumā bija pieejami ar darbības pārtraukumiem. Minētie uzbrukumi bija domāti kā iebiedēšanas mēģinājums un varas demonstrācija. Noziedznieki uzņēmumiem e-pastā nosūtīja ultimātu, kurā pieprasīja veikt maksājumu *Bitcoin* kriptovalūtā. Tika draudēts ar vēl apjomīgāku uzbrukumu (līdz pat 2 Tb/s), ja prasības līdz noteiktam datumam netiks apmierinātas. Uzņēmumi noziedznieku prasībām nepakļāvās, tā vietā tika veiktas preventīvās darbības, lai nodrošinātos pret līdzīgiem uzbrukumiem nākotnē. CERT.LV aicināja nekomunicēt ar izspiedējiem un neveikt maksājumus, lai neveicinātu šādu uzbrukumu atkārtošanos nākotnē, kā arī sniedza rekomendācijas apdraudējuma novēršanai.

Pārskata perioda otrajā pusē ar izspiešanu nesaistītus DDoS uzbrukumus piedzīvoja vairāki valsts iestāžu resursi. Uzbrukumu apjoms sasniedza no 600 Mb/s līdz pat 6 Gb/s. Vienam no resursiem uzbrukumu izdevās bloķēt tikai daļēji. Pārējos gadījumos uzbrukumus izdevās veiksmīgi atvairīt.

2.4. Ļaundabīgs kods

Latvijas kibertelpā oktobrī tika novērota jauna *Emotet* vīrusa kampaņa, kuras ietvaros lietotāji saņēma e-pastus no pazīstamām organizācijām vai uzņēmumiem ar aicinājumu atvērt pielikumā esošo dokumentu un iespējot *Macros* funkcionalitāti. Kampaņas mērķauditorija bija Latvijas uzņēmumu un organizāciju darbinieki. CERT.LV brīdināja, ka minētie e-pasti var saturēt fragmentus no vēsturiskām sarakstēm, tādā veidā lietotājam radot maldīgu uzticības sajūtu. Starp upuriem bija vairākas valsts iestādes un pašvaldības. Kampaņai turpinoties, CERT.LV turpināja saņemt paziņojumus par kaitīgo e-pastu izplatību, bet arvien biežāk ar norādi, ka e-pasts atpazīts kā ļaundabīgs.

Oktobrī kādas finanšu institūcijas vārdā tika izplatīti kaitīgi e-pasti, kuru pielikumā atradās *MS Excel* dokuments. Šoreiz dokumentā netika izmantota *Macros* funkcionalitāte, bet gan mūķis (*exploit*), kura veiksmīgai pielietošanai bija nepieciešama vairākus gadus neatjaunināta sistēma.

Oktobra noslēgumā tika saņemts ziņojums no kādas Latvijas pašvaldības par sašifrētu organizācijas serveri, cietušas bija arī datu rezerves kopijas. Pēc sākotnējās analīzes tika secināts, ka pašvaldību skāris *Avaddon* tipa vīruss. Ļaundaru pieprasītā izpirkuma maksa bija 1000$. Sadarbībā ar CERT.LV tika skaidroti incidenta apstākļi un ceļš, kādā vīruss iekļuva pašvaldības sistēmā.

Novembra sākumā CERT.LV saņēma ziņojumus no Latvijas iedzīvotājiem par aizdomīgiem e-pastiem šķietami *Swedbank* un *SEB* bankas vārdā. Saņemto e-pastu pielikumā bija ļaunatūra, kas paredzēta lietotāju paroļu un citas sensitīvas informācijas izgūšanai. Pielikuma atvēršanas gadījumā CERT.LV aicināja sazināties ar savu sistēmadministratoru.

2.5. Ielaušanās mēģinājumi

Tika saņemts ziņojums par uzbrukumu kādas valsts iestādes resursam – bloķēti 18 tk neleģitīmu pieprasījumu, ar kuriem tika veikti mēģinājumi piekļūt konfigurācijas, žurnālfailiem, u.c. failiem, kā arī veikt koda injekcijas. Tika saņemts arī ziņojums par uzbrukumu kādas valsts iestādes tīmekļa

vietnei, kura ietvaros tika bloķēti 56 tk neleģitīmu pieprasījumu, kas bija ievainojamību skenēšana un koda injekciju mēģinājumi. Abi uzbrukumi tika veiksmīgi atvairīti. Tika novērots, ka abi uzbrukumi tika realizēti no vienas un tās pašas IP adreses.

Novembra sākumā tika novērots mērķtiecīgs uzbrukums kādas valsts iestādes resursam, kura ietvaros tika veikti gandrīz 6000 koda injekciju mēģinājumi. Uzbrukums tika veiksmīgi atvairīts, ietekme uz resursa darbību netika konstatēta.

Decembra vidū tika saņemts ziņojums par uzbrukuma mēģinājumu kādas valsts iestādes resursam, kura ietvaros tika veikti 19 tk pieprasījumu ar mērķi izpildīt SQL injekcijas. Uzbrukumu mēģinājumi tika veiksmīgi atvairīti.

Pārskata periodā tika novērota atkārtota krāpnieku aktivitāte, kas bija vērsta uz lietotnes *WhatsApp* lietotāju kontu pārņemšanu. Upuri no kāda paziņas jau kompromitētā konta saņēma lūgumu pārsūtīt sešciparu kodu, kas it kā kļūdas pēc viņiem nosūtīts. Attiecīgais kods nodrošināja atbilstošā *WhatsApp* konta aktivizēšanu citā iekārtā, sniedzot uzbrucējam pilnīgu kontroli pār kontu (taču nenodrošina pieeju upura sarakstes vēsturei).

2.6. Kompromitētas iekārtas un datu noplūdes

Tika saņemts ziņojums par datu noplūdi no kāda Latvijas loģistikas uzņēmuma vietnes, kura darbojās uz novecojušas platformas un bija pakļauta vairākām ievainojamībām. Ļaundariem izdevās izgūt lietotāju e-pastus, rēķinu informāciju, kā arī lietotāju paroles, kas tikušas izmantotas, lai reģistrētos vietnē. CERT.LV sazinājās ar uzņēmumu un informēja par notikušo, kā arī lūdza uzņēmumu novērst vietnes nepilnības.

Kāda mācību iestāde ziņoja par problēmām ar iestādes tīmekļa vietni, - tās apmeklētāji tika pāradresēti uz apšaubāmiem ārējiem resursiem. Minētajos resursos lietotāji tika aicināti piedalīties viltus loterijās. Konstatējot, ka vietne tikusi uzlauzta, CERT.LV ieteica tīmekļa vietnes izstrādātājiem

atjaunot vietni no rezerves kopijām, kā arī aicināja atjaunināt vietnes satura vadības sistēmas *WordPress* versiju un tajā integrētos spraudņus. Iestāde rekomendācijas operatīvi īstenoja un nepilnības novērsa.

Vairākas pašvaldības un uzņēmumi novembrī ziņoja CERT.LV par uzlauztiem serveriem un sašifrētiem datiem. Daļā gadījumu skartas bija arī rezerves kopijas. Pēc izpētes tika konstatēts, ka vainojams ir *Phobos* izspiedējvīruss, kuru pārskata periodā nebija iespējams atšifrēt. Serveri tika uzlauzti, izmantojot RDP (attālināto pieeju) no publiskā interneta. Lai šādas situācijas neatkārtotos, CERT.LV aicināja paaugstināt RDP drošību, kā arī rezerves kopijas uzglabāt tā, lai tās ir neatkarīgas no kopējamās sistēmas. CERT.LV rekomendēja nemaksāt uzbrucējiem, bet izveidot šifrēto failu kopiju, jo pastāv iespēja, ka šos failus nākotnē varēs atšifrēt. Kā arī, ja uzbrukums uzņēmumam radījis būtiskus zaudējumus, CERT.LV aicināja vērsties ar iesniegumu Valsts policijā.

Novembrī Latvijas medijos plašu rezonansi ieguva ziņa par datu noplūdi no Ķīnas uzņēmuma *Zhenhua Data*, kas skārusi aptuveni 2,4 miljonus iedzīvotāju visā pasaulē. To vidū bija atrodama arī informācija par 480 iedzīvotājiem no Latvijas. Nopludinātie dati liecināja, ka uzņēmums par personām vācis publiski pieejamu informāciju – no medijiem, sociālajiem tīkliem utt. Informācijas vākšanai izmantotas speciāli tam izstrādātas programmas.

Tika saņemti ziņojumi no vairākām valsts iestādēm par zaudētu iestādes *Facebook* lapu. Veicot iegūtās informācijas analīzi, tika secināts, ka visos gadījumos ticis kompromitēts konkrētās lapas administratora privātais profils, kas tālāk izmantots organizācijas lapas pārņemšanai un citu kolēģu piekļuves tiesību anulēšanai. Atsevišķos gadījumos nebija skaidra kontu pārņemšanas motivācija, jo uzbrucēji pēc kontroles iegūšanas pār iestādes *Facebook* lapu necentās mainīt tās saturu vai izvietot jaunu informāciju. Visu lapu piekļuves tiesības sadarbībā ar *Facebook* tika atgūtas.

Decembra otrajā pusē tika novēroti veiksmīgi pikšķerēšanas uzbrukumi, kuru rezultātā vairāku iestāžu darbinieki savadīja savu e-pastu piekļuves datus uzbrucēju sagatavotajās viltus vietnēs, lai arī uzbrucēju izmantotā metode būtu varējusi raisīt aizdomas par saņemtā e-pasta leģitimitāti. E-pastā tika norādīts, ka ar saņēmēju tiek kopīgots dokuments pārskatīšanai, bet e-pastā tika

iekļauta saite uz PDF dokumentu, kurā tika iekļauta saite uz tīmekļa vietni. CERT.LV uzsvēra nepieciešamību ieviest vairāku faktoru autentifikāciju arī *Microsoft* kontu aizsardzībai.

CERT.LV uzskaita kompromitēto un izķēmoto tīmekļa vietņu gadījumus. Pārskata periodā tika fiksētas 14 kompromitētas un izķēmotas tīmekļa vietnes. Visu izķēmoto vietņu uzturēšanai tika izmantota *Linux* operētājsistēma. Viena no izķēmotajām vietnēm pēdējā gada laikā tika izķēmota atkārtoti.

2.7. Ievainojamības

CERT.LV veica pašvaldību un valsts iestāžu e-pasta iestatījumu pārbaudes, lai konstatētu to atbilstību MK noteikumiem Nr. 442 *Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām*. Prasības paredz DMARC protokola izmantošanu. Pārbaužu rezultātā tika atklāts, ka tikai viena trešā daļa no pārbaudītajiem resursiem vismaz teorētiski atbilda noteiktajām prasībā, jo tika konstatēta atbilstošo tehnoloģiju izmantošana, taču šādās pārbaudēs nav iespējams līdz galam pārliecināties, vai tehnoloģijas ir ieviestas korekti.

Kādā novecojušā Latvijas uzņēmuma vietnē tika konstatētas vairākas kritiskas ievainojamības, kas sniegtu iespēju uzbrucējam izpildīt SQL pieprasījumu tīmekļa vietnes datubāzē, lai iegūtu visus tur pieejamos datus. Tā kā vietne darbojas jau ilgu laiku, paredzams, ka datubāzes apjoms varētu būt ievērojams. Vietnes uzturētāji tika informēti.

Oktobrī tika saņemta informācija par ievainojamām *Fortinet* VPN iekārtām. Ievainojamība tika novērtēta kā kritiska un tika konstatēta aktīva tās izmantošana kiberuzbrukumu veikšanā globālajā kibertelpā. Ievainojamība sniegtu iespēju neautentificētiem uzbrucējiem piekļūt sensitīvām datnēm, kas var atklāt VPN lietotāju paroles un lietotājvārdus. Par ievainojamību tika brīdināti vairāki Latvijas uzņēmumi.

Decembrī publiski izskanēja informācija par incidentu, kurā tika kompromitēta *SolarWinds* programmatūras *Orion* atjauninājumu piegādes sistēma. Incidenta rezultātā *SolarWinds* klienti visā

pasaulē no 2020. gada marta līdz 2020. gada jūnijam lejuplādējuši un uzstādījuši kompromitētus atjauninājumus, tādejādi padarot iekārtas pieejamas uzbrucējiem. Decembra vidū *SolarWinds* publicēja atjauninājumus apdraudējuma novēršanai un drošības uzlabošanai. Sadarbībā ar ārvalstu kolēģiem CERT.LV izvērtēja *SolarWinds* incidenta potenciālo ietekmi uz Latvijas infrastruktūru. Incidenta ietekme uz Latvijas resursiem pagaidām netika konstatēta.

2.8. Atbildīgu ievainojamību atklāšana

Tika saņemts ziņojumi par starpvietņu skriptēšanas (*XSS*) ievainojamību sešos valsts iestāžu tīmekļa resursos. Starpvietņu skriptēšanas ievainojamība sniedz uzbrucējam iespēju izpildīt patvaļīgu kodu citu lietotāju aplūkotajās tīmekļa vietnēs, piemēram, pārvirzot lietotāju uz kaitīgu vietni, kā arī apiet vietņu piekļuves drošības mehānismus. Piecos gadījumos ievainojamība tika novērsta, vienā gadījumā tika izstrādāta jauna tīmekļa vietne.

Tika saņemts ziņojums par drošības ievainojamību kādas organizācijas tīmekļa vietnē, kas ļāva uzbrucējam izpildīt SQL injekcijas uzbrukumus, lai iegūt datus no tīmekļa vietnes datubāzes. Ievainojamība tika novērsta.

Tika saņemts ziņojums par ievainojamību kādā pakalpojumā, kas paredzēts laika uzskaites veikšanai. Uzturētāji bija pakļāvuši pakalpojum attālinātā koda izpildes riskam, pievienojot IPV6 adreses. Ievainojamība tika novērsta.

No drošības pētnieka Latvijā tika saņemta informācija par jaunatklātu nulles dienas (*zeroday*) ievainojamību *MS Teams* platformā. Ievainojamība sniedza uzbrucējam iespēja pārņemt visu infrastruktūru un *Office 365* kontus, veicot *remote code execution*. Uzbrukuma realizācijai nebija nepieciešama lietotāja iesaiste (*zero-click*), tas tika veikts, nosūtot lietotājam atbilstoši sagatavotu ziņojumu.

Tika saņemts ziņojums par ievainojamību kādas valsts iestādes resursā ar potenciālu personas datu noplūdi. Ievainojamība sniedza iespēju nesankcionēti aplūkot citu lietotāju privāto informāciju.

Izstrādātāji veica ievainojamības novēršanu. Veikto izmaiņu rezultātā radās jauna nepilnība, kuras ietekmē lietotājiem nebija iespēja pārtraukt savu autentifikāciju sistēmā (*log-out*). Iestāde veica resursa papildu drošības auditu.

Tika saņemts ziņojums par ievainojamībām kādas valsts iestādes resursā, kas ļāva uzbrucējam veikt pilnās pārlases (*bruteforce*) uzbrukumu, kā arī izmantot resursu DDoS uzbrukumu veikšanai pret citiem resursiem. Uzturētājs tika informēts.

2.9. Ielaušanās testi

Veicot drošības pārbaudes kādas valsts iestādes resursam, tika atklātas vairākas ievainojamības, kā arī novecojuša, apdraudēta moduļa izmantošana, kuram ražotājs vairs nenodrošina tehnisko atbalstu un atjauninājumus. Lai arī atklātās ievainojamības tika novērstas, turpinās iespēju izvērtēšana novecojušā moduļa nomaiņas veikšanai. Konkrētais gadījums spilgti ilustrē nepieciešamību paredzēt finansējumu ne tikai projekta izstrādei, bet arī tālākai uzturēšanai un atbilstoša drošības līmeņa nodrošināšanai visā projekta vai resursa dzīves laikā.

Kādas valsts iestādes tiešsaistes risinājumam tika veikti moduļa papildinājumi un CERT.LV aicināja veikt drošības testus. CERT.LV veica koda auditu, kura rezultātā tika konstatēta tikai viena starpvietņu skriptēšanas ievainojamība, par kuru tika informēts izstrādātājs.

CERT.LV saņēma uzaicinājumu veikt drošības testus kādas valsts iestādes resursam. Veicot detalizētu analīzi un ielaušanās testus, tika konstatēts, ka resurss ir izstrādāts kvalitatīvi un drošības nepilnības nav konstatētas.

2.10. CERT.LV pasākumi incidentu novēršanā

- 27. novembrī valsts un pašvaldību iestāžu atbildīgajiem par IT drošību tika izsūtīti atgādinoši e-pasti ar ieteikumiem drošāka attālinātā darba organizēšanai.
- 1. decembrī valsts un pašvaldību iestāžu atbildīgajiem par IT drošību tika izsūtīts aicinājums sekot līdzi publiski pieejamajai informācijai par datu noplūdēm, kurās iesaistīti šo iestāžu darbinieki, lai laicīgi novērstu nopludināto piekļuves datu ļaunprātīgu izmantošanu. Aicinājums sagatavots, ņemot vērā saņemto informāciju par kārtējo nopludināto datu pieejamību nelegālās datu apmaiņas vietnēs.
- 4. decembrī valsts un pašvaldību iestāžu atbildīgajiem par IT drošību tika izsūtīta informācija par vairākām kritiskām *Drupal* ievainojamībām.
- 15. decembrī valsts un pašvaldību iestāžu atbildīgajiem par IT drošību tika izsūtīts aicinājums nekavējoties veikt infrastruktūras drošības pārbaudes, ja tiek lietota *SolarWinds Orion* programmatūra.

Informācija par jaunatklātiem apdraudējumiem un ievainojamībām tiek publicēta arī CERT.LV tīmekļa vietnē un sociālo tīklu *Twitter* (@certlv) un *Facebook* (@cert.lv) kontos. Kopš ārkārtas stāvokļa izsludināšanas CERT.LV ļoti aktīvi informē sabiedrību par jaunām uzbrukumu kampaņām.

Cita veida sadarbība ar dažādām iestādēm ir norādīta atskaites 4. un 8. punktā.

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

1.-2. oktobrī, uzsākot Eiropas Kiberdrošības mēnesi, tiešsaistē notika CERT.LV organizētā tehniskā kiberdrošības konference *Kiberšoks 2020*, kurā ar praktiskiem piemēriem un

demonstrācijām tika padziļināti aplūkotas dažādas tehniskas ar kiberdrošību saistītas tēmas, piemēram, šifrējošo izspiedējvīrusu izmantotās metodes aizsardzībai pret atklāšanu, *Yara* rīka izmatošana un digitālo attēlu metadatu analīze. Konferencei pieteicās un to attālināti vēroja 760 dalībnieki; prezentācijas sniedza septiņi lektori no piecām dažādām valstīm. Paralēli konferencei sadarbībā ar *Cybexer Technologies* un *Tet group* norisinājās arī *Capture the Flag* (*CTF*) sacensības, kurās spēkiem mērojās 100 dalībnieki jeb 29 komandas.

Oktobra vidū CERT.LV organizēja praktiskus seminārus IT drošības speciālistiem *E-pastu sistēmas aizsardzības labā prakse*, sniedzot praktiskas zināšanas par DMARC ieviešanas procesu un e-pastu sistēmas drošības auditēšanu. Lielās intereses rezultātā semināri tika organizēti atkārtoti. Semināros kopumā piedalījās 113 informācijas tehnoloģiju drošības speciālisti.

29. oktobrī CERT.LV pārstāvis piedalījās Latvijas Zinātnes padomes (LZP) organizētajā sarunā par datu drošību un aizsardzību – *Kā dzīvot sociālajos tīklos?* Pasākuma mērķis bija dot iespēju dzirdēt atzītu profesionāļu vai zinātnieku viedokļus par sabiedrībā aktuāliem jautājumiem.

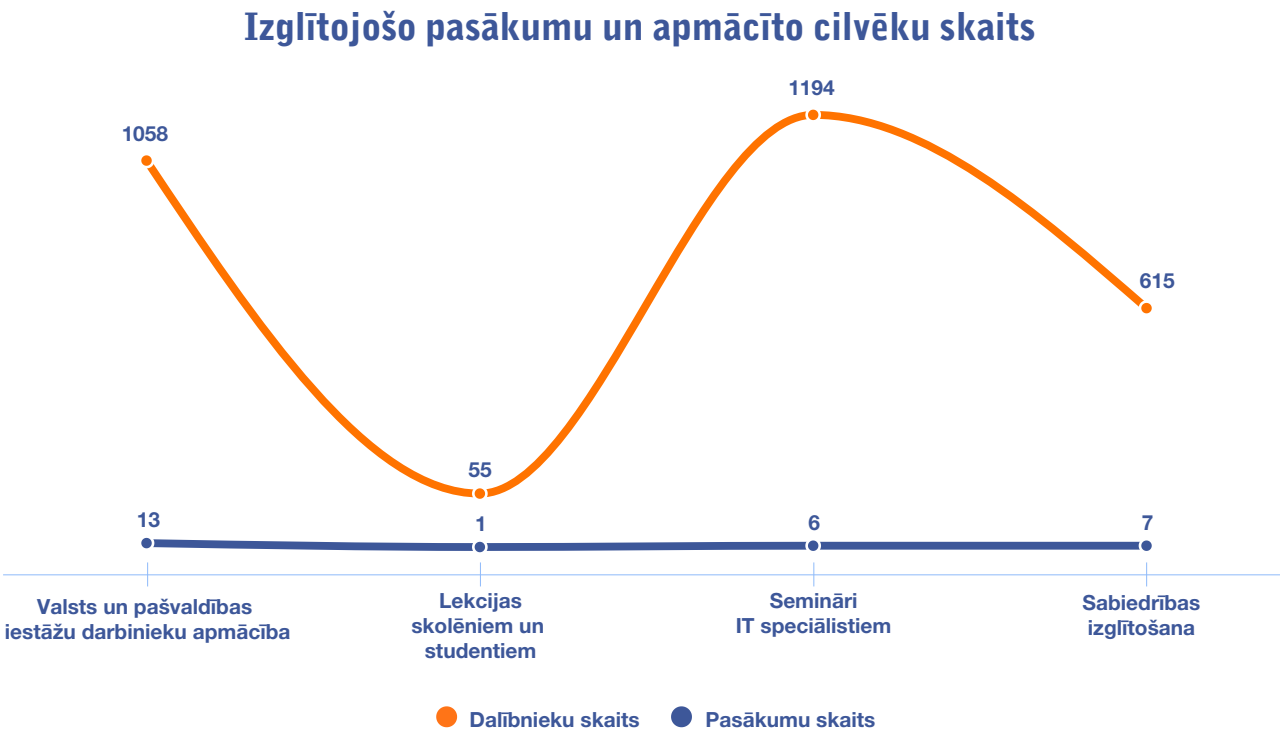
11. novembrī CERT.LV pārstāvis *Riga Conference 2020* ietvaros sniedza interviju par personīgās kiberdrošības jautājumiem (https://www.rigaconference.lv/video/).

2. decembrī LIKTA ikgadējās IKT nozares konferences *DIGI->FIT 2020* ietvaros tika piešķirta IKT nozares prestižākā balva *Platīna pele 2020* arī kategorijā *Labākā kiberdrošības iniciatīva*. To šogad saņēma *PwC cyber security escape room*, kas kiberdrošības izlaušanās spēles (*escape room*) formā izglīto darbiniekus par kiberdrošību. Kategorijas mērķis ir palielināt kiberdrošības jautājumu nozīmi IKT risinājumu izstrādē, veicinot izpratni par kiberdrošību, kā arī sekmēt inovatīvu risinājumu radīšanu un veicināt to atpazīstamību. Balvas tika pasniegtas vēl 4 kategorijās, kā arī pasniegta viena specbalva. CERT.LV piedalījās balvai *Platīna pele 2020* iesniegto pieteikumu vērtēšanas komisijā.

10. decembrī CERT.LV organizēja semināru *Esi drošs* valsts un pašvaldību iestāžu par IT drošību atbildīgajiem, aplūkojot CERT.LV aktualitātes un piedāvātos pakalpojumus, uzticamības

pakalpojumu sniedzējus un elektronisko identitāti, pētījumu par *Eiropas komisijas digitālās drošības likumu*, *Valsts un pašvaldību vienotā tīmekļa platformas* ieviešanu, rīcību kiberincidenta gadījumā, kā arī aktuālās kiberuzbrukumu kampaņas Latvijā 2020.gadā.

Pārskata periodā CERT.LV par IT drošību izglītoja 2922 cilvēkus, iesaistoties 27 izglītojošos pasākumos. Ņemot vērā epidemioloģisko situāciju valstī un ar to saistītos ierobežojumus, pasākumi notika tiešsaistē.



9. attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2020. gada 4. ceturksnī

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

Sadarbības tikšanās, konsultācijas un prezentācijas:

- CERT.LV piedalījās *Finanšu nozares asociācijas* organizētā sanāksmē par banku, elektronisko sakaru komersantu un regulatora sadarbību. CERT.LV sniedza konsultācijas par tehniskajiem aspektiem attiecībā uz krāpnieciskajiem telefona zvaniem, zvanu numerāciju un iepriekš notikušajiem incidentiem.
- Tika uzsākta sadarbība ar *Patērētāju tiesību aizsardzības centru* (*PTAC*) lietu interneta (IoT) iekārtu pētīšanā, lai novērtētu IoT lietu drošību.
- CERT.LV piedalījās atbildīgas ievainojamību atklāšanas iekļaušanā normatīvajos aktos, sniedzot informāciju par praktiskiem ievainojamību atklāšanas scenārijiem.
- CERT.LV piedalījās sanāksmē ar Valsts kontroli par to, kā valsts iestādes nodrošina pakalpojuma nepārtrauktību, kādi incidenti ir bijuši, kā tiek organizēta un kontrolēta paziņošana par incidentu.

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:

- CERT.LV pārstāvis darbojās *FIRST 2021* konferences programmkomitejā, regulāri piedaloties sanāksmēs un palīdzot izstrādāt uzsaukumu referātu iesniegšanai

(*Call for Papers* jeb *CFP*), kas tiks publicēts 2021. gada sākumā. *FIRST 2021* konference notiks attālināti.

- Visa pārskata perioda garumā CERT.LV pārstāvis aktīvi piedalījās kiberdrošības mācību *Crossed Swords 2020/II* organizēšanā, gan plānojot mācību scenārijus un vidi, gan piedaloties mācību testēšanā, gan arī vadot mācību norisi. Ar mācību organizēšanu saistītās aktivitātes norisinājās gan tiešsaistē, gan klātienē Tallinā. Mācības notika no 7. līdz 11. decembrim, dalībniekiem atrodoties attālināti, bet organizatoriem atrodoties NATO CCDCoE, Tallinā.

- Notika arī pārrunas un sagatavošanās darbi dalībai kiberdrošības mācībās *Locked Shields 2021*. Latvijas komanda 2021. gada mācībās piedalīsies apvienībā ar Dienvidkorejas komandu. Tā būs pirmā reize *Locked Shields* mācību vēsturē, kad notiks šāda starpreģionālā sadarbība vienas komandas ietvaros, sniedzot vērtīgu pieredzi gan kulturālo, gan tehnoloģisko, gan arī ģeogrāfisko faktoru ietekmē.

- CERT.LV sniedza viedokli un ieteikumus attiecībā uz kiberdrošības prasībām informācijas un komunikāciju tehnoloģiju produktiem un ar to saistīto tiesisko regulējumu, aizpildot Eiropas Komisijas sagatavoto aptaujas anketu.

- 1. oktobrī CERT.LV pārstāvis piedalījās attālinātajās TF-CSIRT un *Future Working group* sanāksmēs.

- 7. oktobrī CERT.LV vadītāja Baiba Kaškina tika ievēlēta par *FIRST Membership Committee* (Jauno biedru uzņemšanas komitejas) līdzpriekšsēdētāju (*co-chair*), un viņa aktīvi darbojās šajā grupā, gan vadot sanāksmes, gan arī uzlabojot un papildinot biedru uzņemšanas procesa dokumentāciju.

- 20. novembrī CERT.LV tika uzņemta enerģētikas informācijas apmaiņas un sadarbības grupā *Energy ISAC Camelot*. Šo grupu šobrīd veido EEZ valstu enerģētikas un nacionālo CERT vienību komandas no Austrijas, Zviedrijas, Norvēģijas, Šveices, Somijas un Latvijas.

- 3.-9. decembrī notika NIS (Tīklu un informācijas drošības) direktīvas CERTu tīkla virtuālā

sanāksme, kurā CERT.LV pārstāvji sniedza trīs prezentācijas, informējot par CERT.LV organizētās informatīvi-izglītojošās kampaņas *Kiberdrošība darbavietā* rezultātiem, kā arī iepazīstinot ar CERT.LV izstrādātajiem tehniskajiem risinājumiem, kuri varētu būt noderīgi arī citu CERT vienību ikdienas darbā - *Pastelyzer* un *Graphoscope*. CERT.LV pārstāvji aktīvi piedalījās arī divās no četrām darba grupām: *Cyber Weather* darba grupā, kura regulāri apkopo informāciju par būtiskākajiem kiberincidentiem un reizi ceturksnī izstrādā kiberlaikapstākļu pārskatu Eiropai, kā arī aktīvi darbojās *Maturity* darba grupā, kura rūpējas par ES dalībvalstu CSIRT komandu brieduma līmeņa paaugstināšanu.

CERT.LV moderē un vada *Cyber Weather* darba grupu Pārskata periodā notika vairākas darba grupas sanāksmes tiešsaistē, tika publicēti 2020.gada 3. ceturkšņa kiberlaikapstākļi. Turpinājās aktīvs darbs pie tā, lai Eiropas CERTu tīkls vienotos par kiberlaikapstākļu publicēšanu plašākai auditorijai. Tika izstrādāta informācijas tālākas izmantošanas atruna un izstrādāti biežāk uzdotie jautājumi un atbildes. Dokumenti ir apstiprināšanas procesā CERTu tīkla pārstāvjiem.

Sadarbība konkrētu incidentu risināšanā aplūkota pārskata 2. punktā.

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

2020. gada 31. decembrī noslēdzās 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 – ICSC projekts) īstenošana.

Ievērojot COVID-19 vīrusa izplatības radītos ierobežojumus, darbs turpinājās un ir sekmīgi pabeigts visās sešās projektā definētajās darba pakās. Visi izvirzītie projekta uzdevumi ir veiksmīgi sasniegti.

Visi projekta nodevumi noteiktajos termiņos iesniegti. Līdz 2021. gada 1. martam notiks projekta gala atskaišu gatavošana iesniegšanai Eiropas Komisijā.

Pārskata perioda projekta galvenā aktivitāte bija sabiedrību izglītojoši informējoša kampaņa *Kiberdrošība darbavietā*. Tās norise no 2020. gada 14. septembra līdz 2020. gada 11. oktobrim. Ar jaunvārdiem parolīze, muļķerēšana un spaidonis atraktīvā veidā tika uzrunāti organizāciju un uzņēmumu darbinieki – interneta lietotāji. Četru nedēļu garumā, uzrunājot sabiedrību ar īpašu video, reklāmas un rakstu palīdzību, tika sasniegti vairāk nekā 500 tūkstoši Latvijas interneta lietotāji. Kampaņas materiālos CERT.LV eksperti sniedza padomus, kā veidot noturīgus un efektīvus kiberdrošības paradumus, kā vislabāk rūpēties par savu iekārtu drošību, kā veidot efektīvas paroles un atcerēties tās. Kampaņas video materiālu kopējais skatījumu skaits platformā *YouTube* sasniedza 427 tūkstošus, gandrīz 400 dalībnieki savas jauniegūtās zināšanas nolēma pārbaudīt arī praktiski, atbildot uz āķīgiem jautājumiem kampaņas digitālajā rokasgrāmatā – rokasgramata.esidross.lv. Visi kampaņas materiāli arī turpmāk būs pieejami vietnē www.esidross.lv.

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 *CyberExchange*) 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.

CyberExchange projekts turpināsies līdz 2021. gada 30. jūnijam. Arī 2020. gada 4. ceturksnī COVID-19 vīrusa izplatības ierobežošanai noteikto ceļojumu ierobežojumu dēļ un organizācijām turpinot darbu attālināti nebija iespējamas projekta ietvaros plānotās apmaiņas vizītes, kas ir projekta pamata aktivitāte.

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. Tīmekļa vietnē https://dnsmuris.lv pieejamas ērti lietojamas instrukcijas DNS ugunsmūra aktivizēšanai.
- CERT.LV neklātienē tikās ar vairākām slimnīcām, kas ir pamatpakalpojumu sniedzēji, lai iepazītos ar to infrastruktūru un izveidotu efektīvāku sadarbību gan ikdienā, gan ārkārtas situācijās kiberdrošības incidenta gadījumā.
- Viens CERT.LV pārstāvis piedalījās prakses darbu aizstāvēšanas komisijā Vidzemes augstskolas Kiberdrošības programmā, bet otrs – vadīja divus maģistra darbus.
- 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 Digitālās drošības uzraudzības komitejas (DDUK) ietvaros izskatīja un pārapstiprināja LVRTC kā kvalificētu elektroniskās identifikācijas pakalpojumu sniedzēju un tā kvalificētos elektroniskās identifikācijas līdzekļus. DDUK turpināja arī uzraudzīt uzticamības pakalpojumu sniedzējus. Decembra sākumā *ENISA Article 19th* virtuālajā sanāksmē CERT.LV pārstāvis prezentēja DDUK paveikto uzticamu sertifikācijas pakalpojumu sniedzēju uzraudzības jomā 2020. gadā.

9. Papildu pasākumu veikšana

Latvijas Interneta asociācijas *Drošāka interneta centra ziņojumu līnija* (*ZL*) laika posmā no 01.10.2020. līdz 31.12.2020. ir saņēmusi un izvērtējusi 1072 ziņojumus. No tiem 909 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 12 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 16 ziņojumos konstatēta personas goda un cieņas aizskaršana, 1 ziņojums saņemts par naida runu un 2 ziņojumi par vardarbību atainojošiem materiāliem. Par finanšu krāpšanas mēģinājumiem internetā saņemti 34 ziņojumi, 26 ziņojumu saturs nav bijis pretlikumīgs, 72 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 791 ziņojums par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 92 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kuru atrašanās vieta bija ārpus Latvijas, tika ievietoti INHOPE asociācijas datu bāzē un iesniegti attiecīgās INHOPE valsts ziņojumu līnijai turpmāko darbību veikšanai, lai dzēstu nelegālo saturu no publiskas aprites.

Pārskata periodā no Latvijā uzturētajiem 909 ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem 897 ziņojumi ir dzēsti no publiskas aprites internetā un 12 ziņojumi atrodas dzēšanas procesā.

2021. gada 20. janvāris.

CERT.LV misija ir veicināt informācijas tehnoloģiju (IT) drošību Latvijā.

Galvenie CERT.LV uzdevumi ir uzturēt un aktualizēt informāciju par IT drošības apdraudējumiem, sniegt atbalstu valsts institūcijām IT drošības jomā, sniegt atbalstu IT drošības incidentu novēršanā jebkurai fiziskai vai juridiskai personai, ja incidentā iesaistīta Latvijas IP adrese vai .LV domēns, organizēt informatīvus un izglītojošus pasākumus gan valsts iestāžu darbiniekiem, gan IT drošības profesionāļiem, gan citiem interesentiem.

Saziņa ar CERT.LV:

Telefons: +371 67085888

E-pasts: cert@cert.lv

Tīmekļa vietne: www.cert.lv

Sekot CERT.LV aktualitātēm:

www.twitter.com/certlv

www.facebook.com/certlv

Līdzfinansē Eiropas Savienības Eiropas infrastruktūras savienošanas instruments