Latvijas universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

2020 C2

Publiskais pārskats par CERT.LV uzdevumu izpildi

2020. gada 2. ceturksnis (01.04.2020 – 30.06.2020.)

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 2. ceturksnī tika reģistrētas 200 918 unikālas apdraudētas IP adreses, kas ir par nepilniem 2% mazāk nekā iepriekšējā ceturksnī un par nepilniem 20% mazāk nekā šajā pašā periodā pirms gada.

Pārskata periodā Latvijas interneta telpā izplatītākie apdraudējumi:

- konfigurācijas nepilnības (113 995 unikālas IP adreses) ar kāpumu par nepilniem 2% pret iepriekšējo periodu;
- otrs izplatītākais bija ļaundabīgs kods (6987 unikālas IP adreses) ar kritumu par 38%;
- bet trešais - ielaušanās mēģinājumi (2204 unikālas IP adreses) ar kritumu 12%.

Kritums ļaundabīgā koda apjomā skaidrojums ar vairāku informācijas avotu ienākošās datu plūsmas pārrāvumu pārskata perioda sākumā.

Pārskata periodu iezīmēja jauna tendence – šantāžas e-pastiem, kas līdz šim tika sūtīti individuāliem lietotājiem, pievienojās arī izspiešanas mēģinājumi uzņēmumiem un organizācijām. Lietotājiem tika draudēts ar kompromitējoša materiāla, kas iegūts lietotājam apmeklējot pieaugušajiem domātas tīmekļa vietnes, publicēšanu, savukārt uzņēmumiem tika draudēts nopludināt klientu datubāzi, kas iegūta, uzlaužot uzņēmuma tīmekļa vietni. Reputācijas glābšanai tika pieprasīta izpirkuma maksa.

Savukārt krāpnieciskiem e-pastiem, kas tika sūtīti uzņēmumu un organizāciju vadītāju vārdā attiecīgo uzņēmumu grāmatvežiem ar jautājumu par konta atlikumu un lūgumu veikt steidzamu

maksājumu, pievienojās e-pasti darbinieku vārdā ar jautājumu par algas izmaksas datumu un lūgumu veikt algas izmaksu uz jaunu bankas kontu.

Izmantojot pandēmiju un ārkārtas stāvokli, gan pikšķerēšanas, gan ļaunatūras izplatīšanas aktivitātes tika veiktas dažādu piegādes kompāniju aizsegā (*Latvijas pasts*, *DHL*, *UPS*, *AliExpress*), izplatot e-pastus par nepiegādātiem sūtījumiem vai nepieciešamību precizēt piegādes informāciju. Uzbrucēji turpināja aktīvi izmantot arī lietotāju nepilnīgās zināšanas par dažādiem pašu izmantotajiem drošības risinājumiem, gan gūstot piekļuvi pie lietotāju sociālo tīklu kontiem un lietotnēm, neskatoties uz iespējotu divfaktoru autentifikāciju, gan izkrāpjot piekļuvi lietotāju banku kontiem, sūtot *Smart-ID* PIN kodu pieprasījumus, kurus lietotāji mēdz apstiprināt, lai arī tobrīd paši neveic darbības internetbankā. Situācija skaidri liecina par nepieciešamību veikt papildu informatīvi skaidrojošas aktivitātes par daudzfaktoru autentifikācijas darbību.

Pārskata periodā CERT.LV par IT drošību izglītoja 338 cilvēkus, iesaistoties 5 izglītojošos pasākumos. Ņemot vērā ārkārtas stāvokli valstī, visi pasākumi notika tiešsaistē.

1. Elektroniskās informācijas telpā notiekošo darbību atainojums

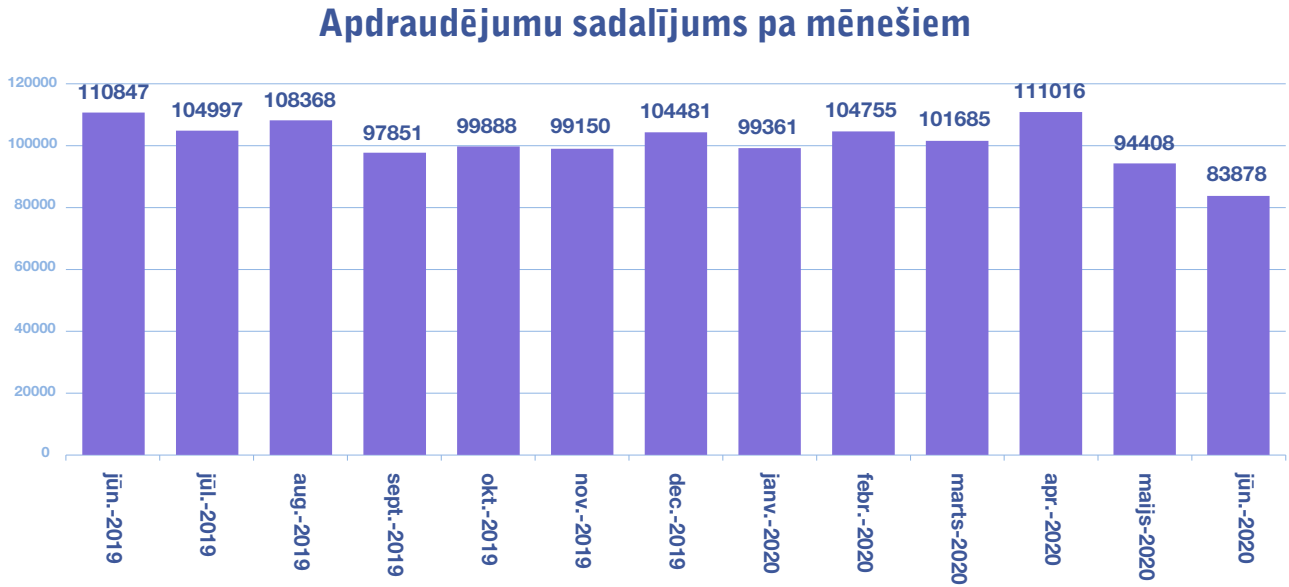
Ik mēnesi CERT.LV apkopo informāciju par apdraudētajām Latvijas IP adresēm. Lai sniegtu pilnvērtīgāku Latvijas kibertelpas pārskatu un nodrošinātu datu starptautisku salīdzināmību, CERT.LV apdraudējumu uzskaitei izmanto starptautiski lietotu incidentu taksonomiju (*eCSIRT.net* projekta izveidotā taksonomija, 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 infekciju (piemēram, *Confiker*, *Zeus*, *Mirai*) un ievainojamību (piemēram, *Opendns*, *Openrdp*) tipiem.

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

2020. gada 2. ceturksnī tika reģistrētas 200 918 unikālas apdraudētas IP adreses, kas ir par nepilniem 2% mazāk nekā iepriekšējā ceturksnī un par gandrīz 20% mazāk nekā šajā pašā periodā pirms gada.

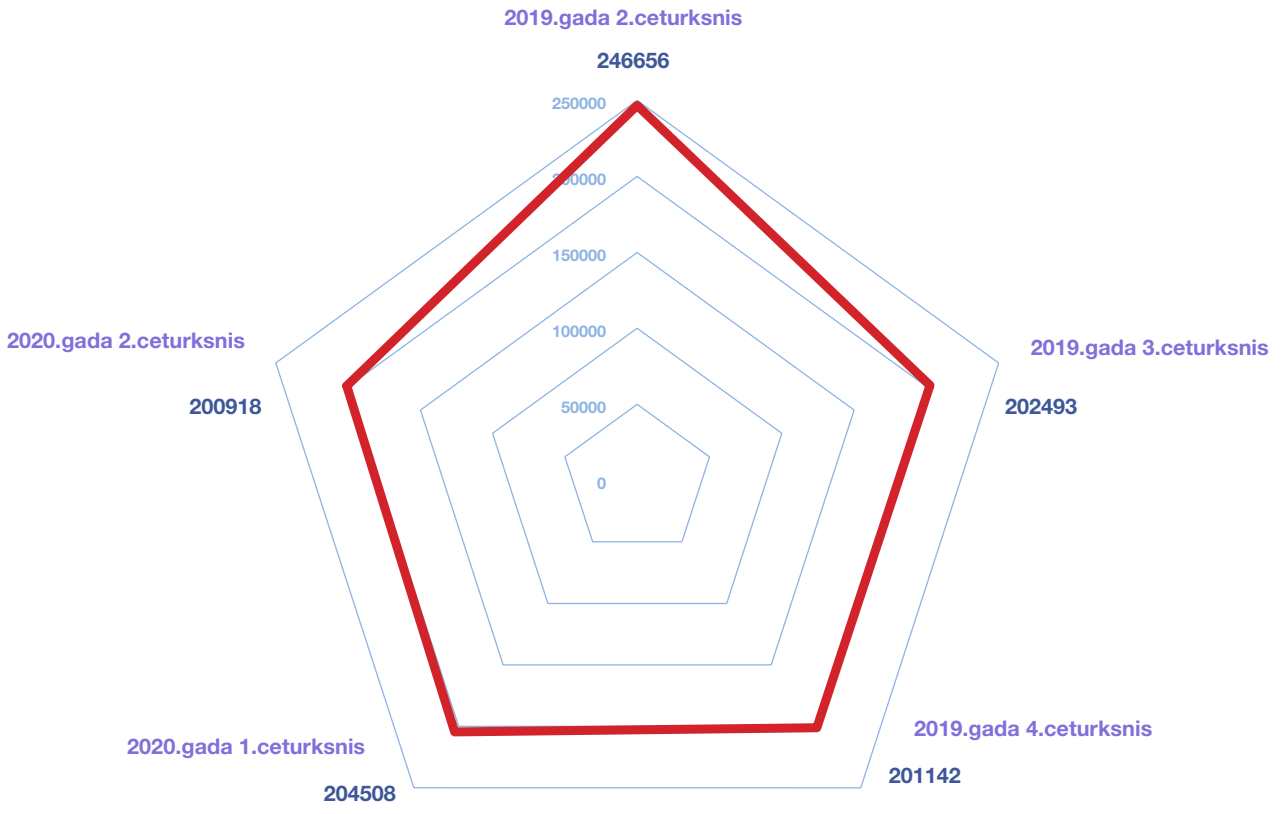
Pārskata periodā nav vērojamas būtiskas izmaiņas mēnesī reģistrēto apdraudēto IP adrešu daudzumā.

Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (113 995 unikālas IP adreses) ar kāpumu par nepilniem 2% pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs kods (6987 unikālas IP adreses) ar kritumu par 38%, bet trešais - ielaušanās mēģinājumi (2204 unikālas IP adreses) ar kritumu 12%.



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

Apdraudējumu sadalījums pa ceturkšņiem

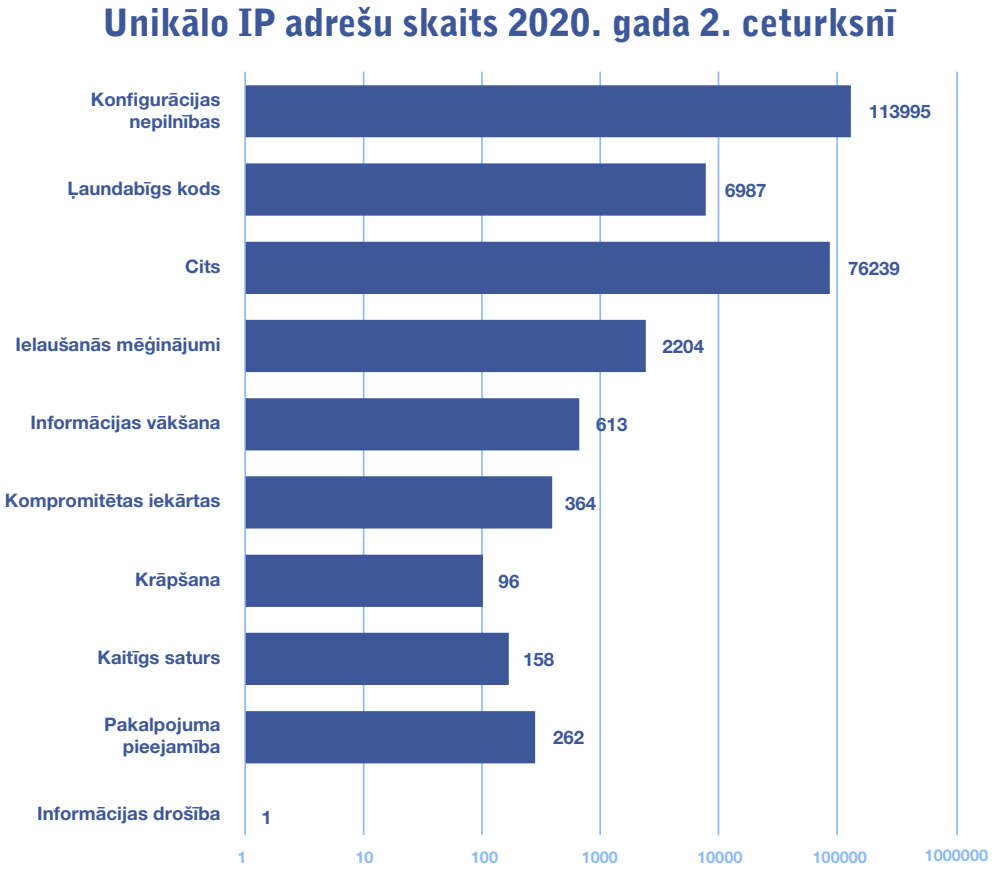


2. attēls – CERT.LV reģistrētās apdraudētās IP adreses pa ceturkšņiem 2019. un 2020. gadā.

Kritums ļaundabīgā koda apjomā skaidrojums ar vairāku informācijas avotu ienākošās datu plūsmas pārrāvumu pārskata perioda sākumā. Tiek skaidroti pārtraukuma iemesli.

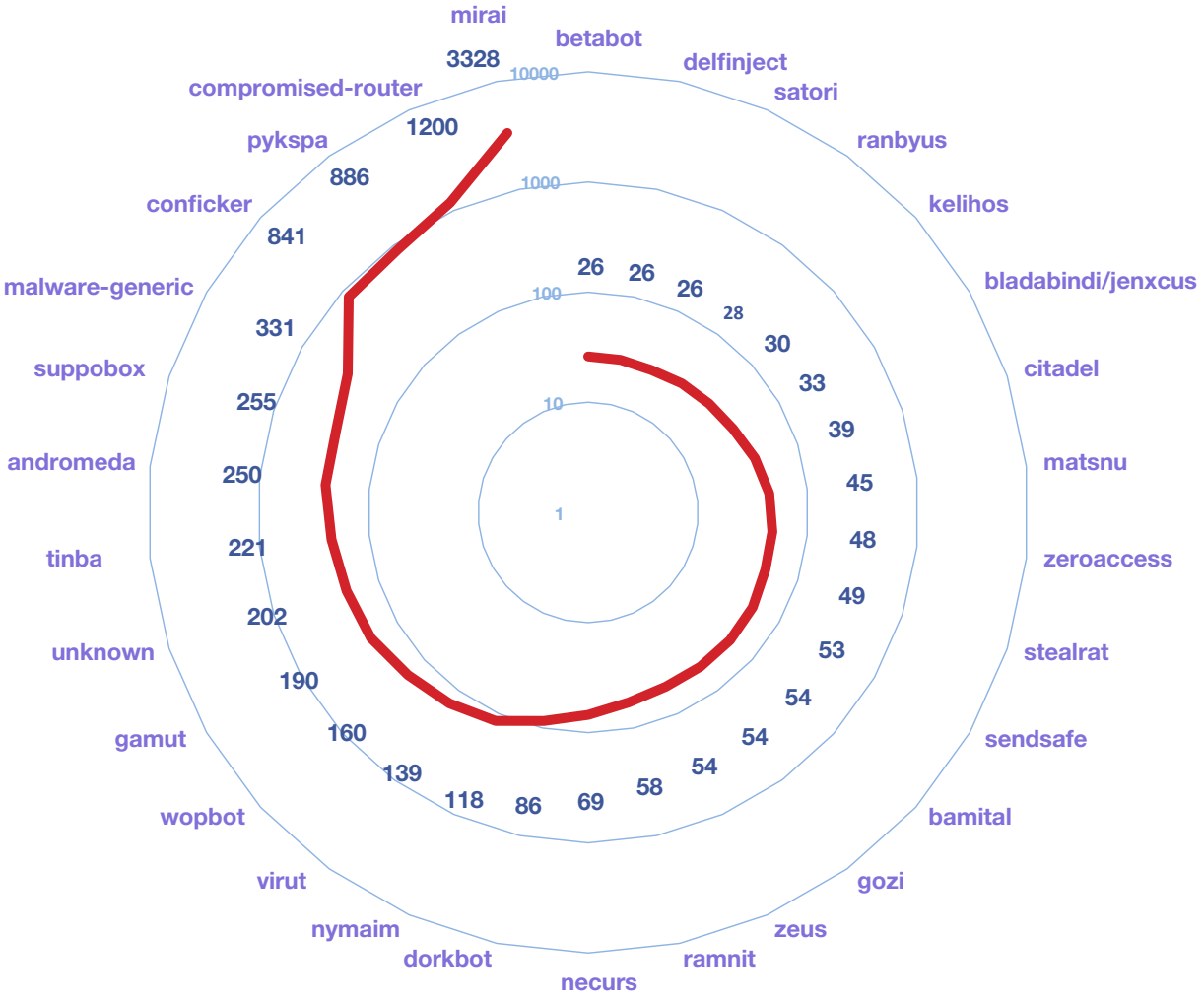
Iepriekšējā ceturksnī popularitāti atguvušie kriptovalūtas ieguves rīki, piemēram, ļaunatūra *Minr*, šajā pārskata periodā atkal zaudēja aktualitāti.

Ļaunatūras topa augšgalā nemainīgi 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.



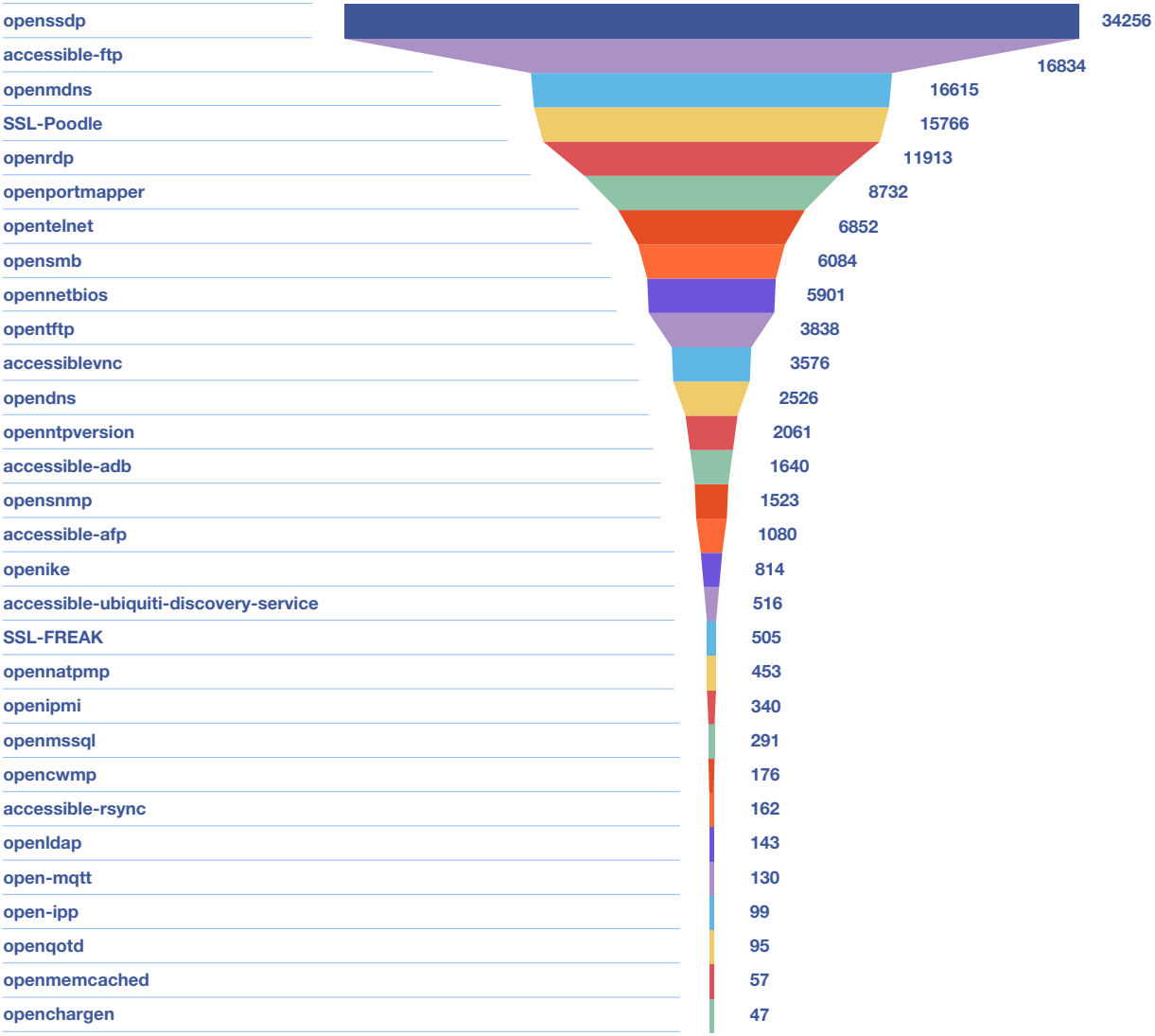
3. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2020. gada 2. ceturksnī pa apdraudējumu veidiem.

Unikālo IP adrešu skaits - ļaundabīgs kods 2020. gada 2. ceturksnī



4. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2020. gada 2. ceturksnī ar apdraudējuma veidu - ļaundabīgs kods.

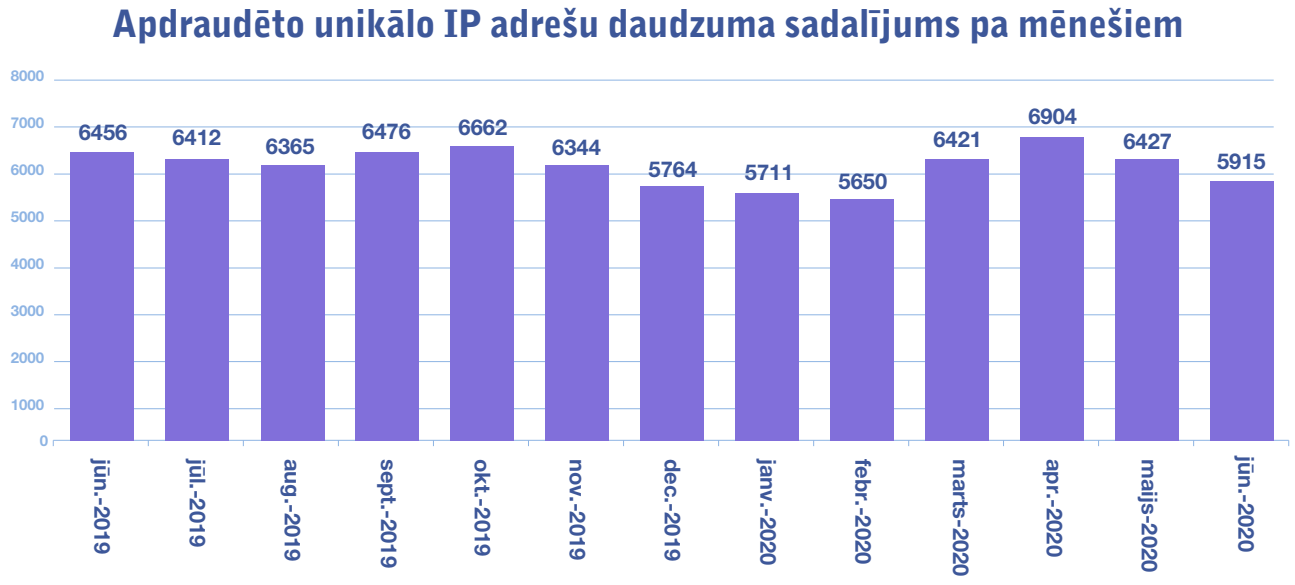
Unikālo IP adrešu skaits - konfigurācijas nepilnības 2020. gada 2. ceturksnī



5. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2020. gada 2. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

Arī *Conficker* saglabāja savu vietu topa augšgalā, kaut ir sen zināma un viegli ārstējama ļaunatūra – nepieciešams veikt iekārtu atjauninājumus. *Conficker* plašā izplatība, iespējams, norāda uz internetam pieslēgtām novecojušām iekārtām, kurām vairs netiek nodrošināti atjauninājumi. Šādu iekārtu izmantošana pakļauj infrastruktūru un datus pastiprinātam uzbrukumu riskam.

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



6. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2020. gadā ar konfigurācijas nepilnību *OpenRDP*.

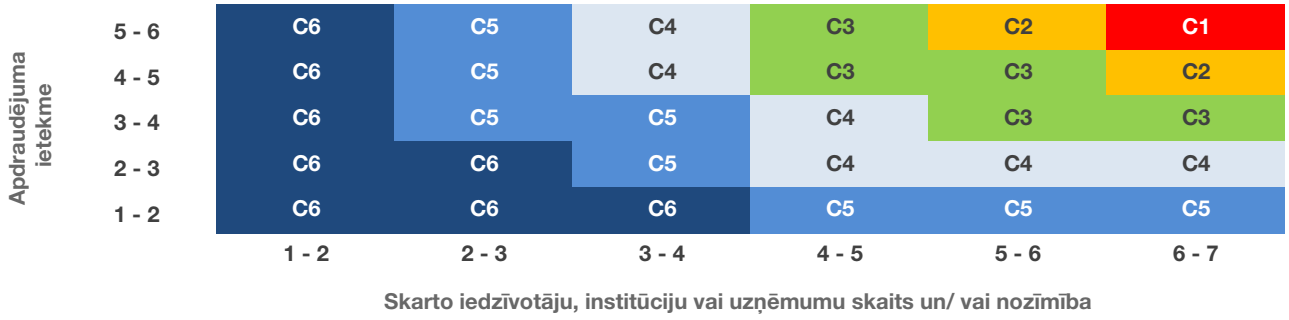
Lai arī šādu gadījumu mazināšanai CERT.LV veica regulāru neatbilstoši konfigurēto iekārtu īpašnieku apziņošanu, un vairāku mēnešu garumā bija vērojams *OpenRDP* ievainojamību samazinājums, martā aizsākās un pārskata periodā turpinājās šādu ievainojamo iekārtu apjoma kāpums (6. att.). Tas, visticamāk, skaidrojams ar attālinātā darba organizēšanas nepieciešamību valsts mērogā. Iespējams, daudzviet primārais uzdevums ārkārtas apstākļos bija ātra darbinieku nodrošināšana ar papildu iekārtām un iespēju piekļūt nepieciešamajām sistēmām attālināti, drošības jautājumus sakārtojot pēc tam: *OpenRDP* apjoma pieaugums no februāra līdz aprīlim bija 12%, bet samazinājums no aprīļa līdz jūnijam 15%.

Pilnvērtīgākam kibersituācijas novērtējumam CERT.LV pirmajā ceturksnī ir uzsācis *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 abus 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.

Apdraudējumu matrica

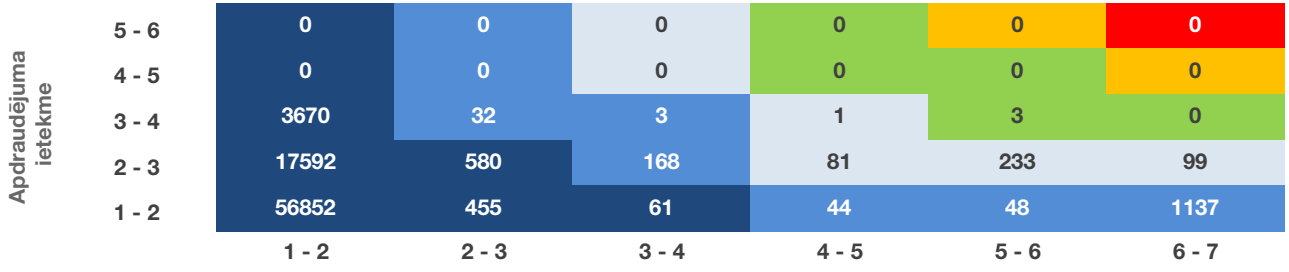


7. attēls – Apdraudējumu matricas sadalījums kategorijās.

Jāuzsver, ka matrica šobrīd vēl ir ieviešanas stadijā un turpinās incidentu kategorizēšana pēc to nozīmīguma, kā arī skarto IP adrešu kategorizēšana pēc to piederības.

Gandrīz 98% 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.

2020. gada. 2. ceturksnis

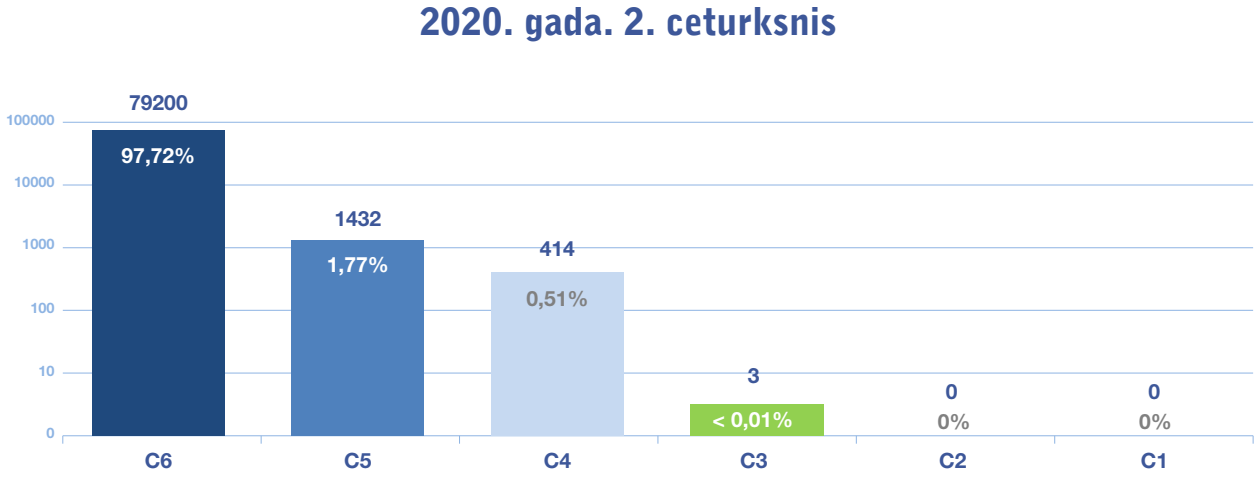


8. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu izvietojums matricā 2020. gada 2. ceturksnī valsts un pašvaldību institūcijās.

Nacionāla līmeņa apdraudējumi (C1) un augstas nozīmes apdraudējumi (C2) pārskata periodā nav reģistrēti. Nozīmīgi plašas ietekmes apdraudējumi (C3) veido 0,004% (3 unikālas apdraudētas IP adreses/gadījumi) no visiem kategorizētajiem apdraudējumiem. Visas trīs apdraudētās IP adreses saistītas ar kādu pamatpakalpojumu sniedzēju, kura pārvaldībā tika konstatēts kompromitēts maršrutētājs un pykspa ļaunatūra.

Lielākā daļa C4 līmeņa incidentu (būtiski apdraudējumi ar vidēju ietekmi) bija konfigurācijas nepilnības (*OpenRDP*, *OpenTelnet*, *OpenDNS*, *Openike*, u.c.), ielaušanās mēģinājumi un ļaundabīgs kods (*Minr*), kas novēroti augstas un vidēji augstas prioritātes iestādēs.

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.



9. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu sadalījums apdraudējumu kategorijās pēc apdraudējuma ietekmes (matrica) 2020. gada 2. ceturksnī valsts un pašvaldību institūcijās.

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

Turpinājās krāpnieciskas loterijas, kurās krāpnieki sabiedrībā atpazīstamu zīmolu vārdā aicināja atbildēt uz 3 vienkāršiem jautājumiem, lai iegūtu viedtālruni. Krāpniecības mērķis bija lietotāju maksājumu karšu informācijas ievākšana, kura tika iegūta, aicinot lietotājus veikt sūtījuma apdrošināšanu 2 eiro apmērā, vai lietotāja pierakstīšanās uz kādu maksas servisu, par kura abonēšanu tiktu ieturēta ikmēneša maksa no maksājuma kartes, kuru lietotājs izmantoja 2 eiro apmaksai. Krāpniecībā cietuši vairāki Latvijas iedzīvotāji.

CERT.LV atgādināja, ka pirms jebkādu datu ievades nepieciešams pārliecinieties, ka vietnes adrese nav kļūdaina un atbilst tai, par ko uzdodas.

Tika novēroti kārtējie šantāžas e-pasti gan angļu, gan krievu valodā. Šādas kampaņas fiksētas arī citviet Eiropā. E-pastos tika apgalvots, ka ļaundaris uzlauzis lietotāja iekārtu (ticamības palielināšanai e-pastā tika iekļauta lietotāja izmantotā parole), un ieguvis lietotāju kompromitējošu informāciju. Tika draudēts šo informāciju izsūtīt lietotāja kontaktiem, ja netiks veikts maksājums. CERT.LV aicināja nemaksāt un neuzsākt komunikāciju ar krāpniekiem, kā arī pārliecināties, ka e-pastā norādītā parole vairs netiek izmantota, jo krāpnieku rokās nonākusi kādā no datu noplūdēm. Katram tiešsaistes resursam izmantojama droša un unikāla parole, un, ja iespējams, arī divu faktoru autentifikācija.

Aprīlī tika novērota jauna tendence – šantāžas e-pasti, kas izsūtīti uzņēmumiem. Līdzīgi e-pastiem, kas tika izplatīti individuāliem lietotājiem ar draudiem publicēt kompromitējošu informāciju, vēstulēs uzņēmumiem tika norādīts, ka uzbrucējs uzlauzis uzņēmuma tīmekļa vietni un ieguvis klientu datubāzi, kuru draud nopludināt, ja netiks samaksāta izpirkuma maksa.

CERT.LV aicināja krāpniekiem nemaksāt un neuzsākt komunikāciju. Profilaksei tika ieteikts periodiski veikt mājas lapas drošības pārbaudes un sekot līdzi atjauninājumiem.

Vairāku uzņēmumu grāmatveži saņēma e-pastus vadītāju vārdā ar lūgumu veikt pārskaitījumu uz nezināmu partneruzņēmumu un solījumu rēķina kopiju nosūtīt vēlāk. Lai arī teksts bija lakoniskāks, nekā ierasts, sākotnēji aizdomas tas neradīja. Krāpniecība tika atpazīta, ievērojot neatbilstošu atbildes (*Reply-to*) adresi. Ņemot vērā, ka *COVID-19* pandēmijas apstākļos daudzi uzņēmumi darbojas attālināti, arī rēķinu apstiprināšana daudziem uzņēmumiem notiek elektroniski, un drošības pasākumi, iespējams, nav tik stingri. To centās izmantot arī krāpnieki.

Ja tiek pieprasīts steidzami veikt maksājumu, apejot ierasto kārtību, vai parādījušās izmaiņas maksājuma informācijā, iesakāms pirms maksājuma veikšanas vēlreiz sazināties ar vadītāju/ kolēģi/ sadarbības partneri, izmantojot citus, pārbaudītus saziņas kanālus, lai pārliecinātos par informācijas patiesumu.

Tika novērota arī jauna tendence: e-pasta sarakstē ļaundari izlikās par kādu no uzņēmuma darbiniekiem, nosūtot jautājumu, kurā datumā būs nākamā alga, un lūdzot mainīt bankas kontu, uz kuru šajā datumā algu pārskaitīt.

Vairāki .LV domēna vārda lietotāji maijā saņēma maldinošus e-pastus no *Domain Service (info@shuiaearth.top)* ar aicinājumu veikt maksājumu par .lv domēna vārdu.

E-pasta saņēmējiem tika norādīts, ka šis nav paziņojums par .lv domēna vārda lietošanas tiesību pagarināšanu, bet gan aicinājumu samaksāt rēķinu par domēna vārdam piesaistāmiem apšaubāmiem *SEO (Search Engine Optimization*) pakalpojumiem.

Kāds uzņēmums Latvijā un viņu klients ārvalstīs piedzīvoja mēģinājumu izkrāpt maksājumu 2800 eiro apmērā. Uzbrucēji kompromitēja uzņēmuma klienta e-pasta kontu un Latvijas uzņēmuma vārdā veica saraksti ar klientu ar mērķi izkrāpt pārskaitījumu uz sev piederošu bankas kontu, nosūtot viltus rēķinu. Krāpniecība tika savlaicīgi atklāta un neviens zaudējumus necieta. CERT.LV ieteica uzņēmumam un tā klientam nomainīt e-pasta paroles, kā arī e-pasta iestatījumos pārbaudīt, vai e-pasti netiek pārsūtīti trešajām pusēm. Uzņēmums tika aicināts krāpnieciskos maksājuma rekvizītus pārsūtīt policijai tālākai izmeklēšanai.

Ārkārtas situācijas laikā tika saņemti ziņojumi no iedzīvotājiem par aizdomīgām īsziņām, kurās saņēmējs tika aicināts pasargāt savu un savu tuvāko veselību, sekojot saitei. Izpētes rezultātā tika konstatēts, ka saite nav paredzēta datu izkrāpšanai, bet gan aizved uz tīmekļa vietni, kurā tiek reklamēti medikamenti.

2.2. Pikšķerēšana jeb svarīgo datu izkrāpšana

Tika saņemta virkne ziņojumu no inbox.lv lietotājiem par e-pastiem ar brīdinājumu, ka tiks bloķēts *Apple ID* konts, ja netiks veikta autorizācija. Atverot e-pastā pievienoto saiti, lietotājs tika pārvirzīts uz pikšķerēšanas vietni *Apple ID* piekļuves datu izgūšanai.

CERT.LV atgādināja nekad neatklāt krāpniekiem savus datus, vienmēr pārliecinoties, ka apmeklējamās vietnes domēna vārds ir atpazīstams un nav kļūdains.

Maija beigās aktivizējās krāpnieki, kas sūtījumu piegādes aizsegā izplatīja krāpnieciskus e-pastus *Latvijas Pasts* un *AliExpress* vārdā.

Krāpnieciskajos e-pastos saņēmēji *Latvijas Pasts* vārdā tika aicināti sniegt papildinformāciju nepiegādāta sūtījuma saņemšanai. Atsūtītajā e-pastā tika iekļauta saite uz vietni, kas paredzēta maksājumu karšu datu un personīgās informācijas izkrāpšanai.

Savukārt *AliExpress* vārdā sūtītajos e-pastos saņēmējs tika brīdināts par aizdomīgu pasūtījumu, kas veikts no viņa konta, un tika aicināts, ja nepieciešams, pasūtījumu atcelt. Spiežot uz "Atcelt pasūtījumu" (*Cancel Order*) pogas, lietotājs tika aicināts ievadīt savus *AliExpress* profila datus. Pēc datu ievades lietotājam tika parādīts kļūdas paziņojums, bet piekļuves dati nosūtīti krāpniekiem.

CERT.LV no Polijas kolēģiem saņēma informāciju par pikšķerēšanas uzbrukumu - no domēna odp.gov.pl uz kādu Latvijas valsts iestādes resursu tika izsūtīti e-pasti, kas, visticamāk, saturēja saiti uz viltus *Office 365* vietni. Kaitīgais e-pasts bija sagatavots, par bāzi izmantojot kādas valsts iestādes sūtītu e-pastu darbiniekiem par darba aizsardzību attālinātā darba gadījumā, parakstā atsaucoties uz reālu iestādes darbinieci. Ņemot vērā to, ka šādi iekšējās komunikācijas e-pasti tiek sūtīti arī uz ārējām pasta kastītēm (*Gmail*, *Inbox*) darbinieku attālināta darba gadījumā, tad noskaidrot, kura iekārta ir potenciāli kompromitēta vai no kura e-pasta konta ir notikusi informācijas noplūde, neizdevās.

Saņemtas sūdzības no iedzīvotājiem par negaidītiem pieprasījumiem apstiprināt PIN1 *Smart-ID* lietotnē, lai arī tobrīd netika veiktas nekādas darbības internetbankā vai kur citur. Negaidītajiem pieprasījumiem dažkārt sekojis arī telefona zvans, kurā zvanītājs, komunicējot krievu valodā un uzdodoties par *Smart-ID* klientu servisu, aicinājis apstiprināt dažādu ar lietotāju saistītu informāciju, lai it kā pēc bankas lūguma novērstu radušās sistēmas kļūdas.

CERT.LV aicināja iedzīvotājus būt vērīgiem, un, ja tiek saņemti pieprasījumi apstiprināt PIN1 vai PIN2, kad netiek veiktas darbības internetbankā, šos pieprasījumus ignorēt, kā arī sazināties ar *Smart-ID* atbilstoši norādēm.

Tika saņemta informācija par krāpniecisku īsziņu izplatīšanu bankas *Citadele* klientiem. Īsziņā ietvertā saite veda uz krāpniecisku vietni, kas imitēja *Citadele* bankas tīmekļa vietni un bija paredzēta bankas klientu informācijas izkrāpšanai.

Tika novērota *Facebook* kontu izkrāpšanas kampaņa – tās ietvaros sociālā tīkla lietotāji saņēma šķietami no drauga vai paziņas (konts kompromitēts) sūtītu saiti uz it kā vimeo video. Mēģinot atvērt saiti, lietotājs tika aicināts autentificēties *Facebook Messenger*. Ja lietotājvārds un parole tika

ievadīti, parādījās kļūdas paziņojums, bet piekļuves dati tika nosūtīti krāpniekiem. Zaudētu kontu atgūšanai CERT.LV aicināja sekot *Facebook* norādījumiem.

Saņemti ziņojumi arī par *Facebook* piekļuves datu izkrāpšanas aktivitātēm sociālā tīkla sludinājumu grupās. Uzbrukums izpaudās kā kāda lietotāja ievietots grupas saturam neatbilstošs bieži šokējoša satura ieraksts ar saiti, kuru nospiežot, parādījās *Facebook* piekļuves datu pikšķerēšanas vietne.

Veicot pikšķerēšanas vietņu izpēti, CERT.LV konstatēja, ka šo vietņu izveidei ir ticis izmantots tam speciāli sagatavots rīks, kurš sniedz iespēju lietotājiem bez specifiskām tehniskām zināšanām veidot *Facebook* un citu populāru vietņu pikšķerēšanas lapas. Jaunizveidotās pikšķerēšanas lapas tika ievietotas uzlauztās tīmekļa vietnēs. Rīkam ir sava saskarne, kurā uzrāda arī lietotājus ar lielāko pēdējo 24h laikā iegūto paroļu skaitu un citu lietotāju izveidotās pikšķerēsanas vietnes. Kompromitētie *Facebook* lietotāju konti tika izmantoti pikšķerēšanas saites tālākai izplatīšanai. Lai arī rīki, kas atvieglo kiberuzbrukumu izpildi, nav jaunums, šis CERT.LV praksē ir pirmais gadījums, kad tik liels sagatavošanās darbu apjoms tiek izdarīts potenciālā uzbrucēja vietā (nodrošināta pikšķerēšanas lapas izveide, kā arī uzlauztā vietne, kur šo lapu izvietot). Par šo rīku tika informēts *Facebook*.

2.3. Pakalpojuma pieejamība (DDoS)

Tika saņemta informācija par *Smart-ID* pakalpojuma darbības traucējumiem, kas ilga gandrīz 12h. Informācija no pakalpojuma sniedzēja liecināja par tehniskiem sarežģījumiem, kuru risināšanai bija nepieciešama īslaicīga plānveida darbības pārtraukšana.

Naktī no 28. maija uz 29. maiju *Smart-ID* lietotnes izstrādātājs – uzņēmums *SK ID Solutions* – veica sistēmas uzturēšanas darbus, kā rezultātā tika novēroti īslaicīgi traucējumi tiem pakalpojumiem, kas saistīti ar *Smart-ID* izmantošanu – pieslēgšanās interneta bankai, maksājumu veikšana u.c. Par šādiem uzturēšanas darbiem savlaicīgi tika brīdināts arī CERT.LV, kā arī *SK ID Solutions* klienti.

2. maijā publiskajā telpā izskanēja brīdinājums par nekontrolēti lidojošu dronu. Kontrolēta lidojuma laikā tehnisku iemeslu dēļ atslēdzās bezpilota gaisa kuģa vadības sistēma, un ar 26 kilogramus smago lidaparātu tika zaudēti sakari. Drons tika atrasts 15.maijā Garkalnes novada meža masīvā.

Tika saņemta informācija no LVRTC par pakalpojuma atteices (*DDoS*) uzbrukumiem, kas ilga vairāk par 10 minūtēm un tika vērsti pret vairākām ministrijām. Visi uzbrukumi tika veiksmīgi atvairīti.

2.4. Ļaundabīgs kods

Pārskata periodā Latvijas Universitātes vārdā vairākkārtēji masveidā tika izsūtīti inficēti e-pasti ar *LokiBot* vīrusu pielikumā. Līdzīgi e-pasti tika izplatīti jau š.g. februārī. Minētais vīruss paredzēts paroļu un sensitīvas informācijas zagšanai no upura iekārtas.

Lietotāji tiek aicināti būt modriem, nevērt vaļā aizdomīgus e-pasta pielikumus un saites, kā arī pievērst pastiprinātu uzmanību e-pasta sūtītāja adresei, e-pasta valodai un gramatikas kļūdām, kā arī tam, vai e-pasta saturs rada steidzamības sajūtu.

Ļaundari centās izmantot ārkārtas stāvokli un to, ka aktīvāk tiek izmantoti dažādi preču piegādes pakalpojumi. Piegādes uzņēmumu *DHL* un *UPS* vārdā nesankcionēti tika izsūtīti krāpnieciski e-pasti ar pielikumā pievienotu ļaunatūru. Vīruss bija paredzēts paroļu un sensitīvas informācijas zagšanai no upura iekārtas. CERT.LV rīcībā esošā informācija liecina par vairākiem veiksmīgiem uzbrukumiem.

Maijā CERT.LV saņēma incidenta pieteikumu no kādas veselības iestādes par šifrējošā izspiedējvīrusa uzbrukumu. Skarti tika faili uz divām iekārtām. Sašifrētajiem failiem tika konstatēts paplašinājums "*.corona-lock*" – jauns vīrusa paveids, kas tika aktualizējies pandēmijas laikā. Pēc incidenta analīzes tika secināts, ka ļaunatūra lejupielādēta, atverot e-pasta pielikumu. Organizācijai tika ieteikts iespējams atšifrēšanas rīks, ar kura palīdzību datus atgūt tomēr neizdevās.

Kāda veselības iestāde ziņoja par pastiprinātu ienākošo e-pastu plūsmu, kuros kā sūtītājs tika norādīta neeksistējoša iekšēja organizācijas e-pasta adrese. Sūtītie e-pasti saturēja pielikumus ar paplašinājumiem *.ace*, *.iso*, *.img* un tamlīdzīgiem. Iestādes izmantotais kiberdrošības risinājums pasargāja darbiniekus no šo e-pastu saņemšanas.

Tika saņemts palīdzības lūgums no Slovēnijas kolēģiem ļaunatūras izplatīšanas kampaņas izmeklēšanā. Kādas Slovēnijas veselības iestādes vārdā tika izplatīti e-pasti ar ļaundabīgu pielikumu, kas saturēja *LokiBot* vīrusu (paredzēts sensitīvas informācijas izgūšanai). E-pasti tika izsūtīti, izmantojot kompromitētu e-pastu kādā slovēņu kompānijā, izmantojot Latvijas IP adresi. Kopumā tikuši izsūtīti gandrīz 32000 kaitīgi e-pasti, kas veiksmīgi piegādāti saņēmējiem: slimnīcām, universitāšu klīnikām, uzņēmumiem, pašvaldībām. E-pasta ziņojums bija saistīts ar *COVID-19* aizsarglīdzekļu piegādi. CERT.LV vērsās pie Valsts policija pēc atbalsta nepieciešamās informācijas iegūšanai no atbilstošā interneta pakalpojumu sniedzēja.

2.5. Ielaušanās mēģinājumi

Saņemti ziņojumi no vairākiem uzņēmumiem par uzbrukumiem attālinātās piekļuves pakalpojumam *RDP*, kas tiek izmantots, lai attālināti pieslēgtos datoram vai sistēmai. Uzbrukumos tika mēģināts uzminēt piekļuves paroles. Tieši *RDP* ar vājām parolēm un neatbilstošu papildu aizsardzību (piemēram, nav ierobežojumu piekļuvei no noteiktām IP adresēm) bieži noved pie veiksmīga uzbrukuma ar postošām sekām – šifrētām darbstacijām vai serveriem.

Tika saņemta informācija par uzbrucēju centieniem pieslēgties kādas valsts iestādes e-pasta serverim un izsūtīt e-pastus no iestādes domēna. Uzbrukumā tika izmantotas gan eksistējošas, gan ģenerētas e-pasta adreses.

Uzbrukumu piedzīvoja arī kādas valsts iestādes tīmekļa vietne. Veiksmīgi atvairīti tika vairāk nekā 13000 neleģitīmi pieprasījumi, kuros tika mēģināts piekļūt dažādiem vietnes administrācijas resursiem.

2.6. Kompromitētas iekārtas un datu noplūdes

Kāda valsts iestāde saņēma ziņu par savas tīmekļa vietnes šķietamu uzlaušanu un draudus par iegūto datu nopludināšanu. Pārbaužu rezultātā tika konstatēts, ka, lai arī saņemtā vēstule bija krāpnieciska rakstura un dati vēl nebija izgūti, vietne patiešām bija ievainojama un saturēja apdraudējumus, kas pakļāva vietni datu izgūšanas riskam. CERT.LV sniedza ieteikumus ievainojamību novēršanai.

Visa pārskata perioda garumā bija novērojama jauna krāpniecības kampaņa, kas vērsta pret *WhatsApp* lietotājiem. Krāpniecības rezultātā ļaundari savā kontrolē pārņēma lietotāja *WhatsApp* kontu, piekļūstot visām lietotāja sarakstēm ar iespēju veikt tajās izmaiņas. Uzbrukums tika realizēts, lietotājam šķietami no paziņas vai tuvas personas, kuras konts, visticamāk, ticis kompromitēts, saņemot ziņu, ka šī persona kļūdas pēc uz lietotāja telefona numuru nosūtījusi SMS ar 6 ciparu kodu, kuru lūdz pārsūtīt. CERT.LV saņēma informāciju par vairākiem uzbrukuma upuriem.

Tika saņemts incidenta pieteikums, kurā norādīts, ka kādai Latvijā organizētai tiešsaistes sanāksmei *ZOOM* platformā pieslēgusies sveša persona un traucējusi sanāksmes norisi, demonstrējot sanāksmes dalībniekiem ar likumu aizliegtus pornogrāfiska rakstura materiālus. Valsts policija demonstrēto materiālu sakarā uzsākusi kriminālprocesu. Jānorāda, ka sanāksmes organizētāji nebija pietiekami parūpējušies par sanāksmes drošību – tiešsaistes sanāksmes saite tika publicēta asociācijas sociālā tīkla *Facebook* profilā un sanāksmei varēja pievienoties jebkurš, kurš atvēra norādīto saiti, attiecīgi, sanāksmei nebija iespējota paroles pieprasīšana un dalībnieku apstiprināšana, ko nodrošina *ZOOM* platforma.

Tika saņemts informācija par mobilo lietotņu veikalos pieejamu viltotu mazumtirdzniecības uzņēmuma *Maxima* lietotni, kas imitēja uzņēmuma nesen izstrādāto oficiālo lietotni. Viltus lietotne, visticamāk, tika paredzēta agresīvai reklāmu izplatīšanai, tādejādi nodrošinot lietotnes izstrādātājiem peļņu.

Tika saņemts ziņojums no kādas valsts iestādes par incidentu, kura rezultātā institūcija zaudēja piekļuvi saviem sociālo tīklu kontiem, kuri tika izmantoti gan sabiedrības informēšanai, gan saziņai ar iedzīvotājiem. Kontiem bija iespējota divfaktoru autentifikācija, taču iestādes darbinieks neatpazina kiberuzbrukumu saņemtajā paziņojumā par šķietamu autortiesību pārkāpumu. Tā vietā, lai saņemto ziņu ignorētu, darbinieks veica prasīto autorizāciju, ievadot arī otro faktoru, tā sniedzot krāpniekiem piekļuvi kontiem. Kļūda tika operatīvi atpazīta un kontus izdevās atgūt. CERT.LV aicina atbildīgi attiekties pret informāciju, kas ir ikviena pārvaldībā, un nesteidzīgi izvērtēt katru situāciju pirms paroļu un kodu ievadīšanas.

CERT.LV uzskaita kompromitēto un izķēmoto tīmekļa vietņu gadījumus. Pārskata periodā tika fiksētas 24 kompromitētas un izķēmotas tīmekļa vietnes. 19 gadījumos izķēmotās vietnes uzturēšanai tika izmantota *Linux* operētājsistēma, 1 gadījumā – *FreeBSD*, bet par četru vietņu operētājsistēmu nav informācijas. Viena no izķēmotajām vietnēm pēdējā gada laikā tika izķēmota atkārtoti.

2.7. Ievainojamības

Aprīlī reģistrētas 21000 unikālas IP adreses ar konfigurācijas nepilnību *OpenSSDP*, kuras var tikt izmantotas *DoS* uzbrukumos pret uzņēmumiem, tiešsaistes tirdzniecības vietnēm un valsts iestādēm. Daļa no neatbilstoši konfigurētajām iekārtām ir *Smart TV*.

Tika saņemts ziņojums par ievainojamībām kāda ar veselības nozari saistīta uzņēmuma tīmekļa vietnē. Ievainojamības pakļāva vietni *XSS* tipa uzbrukumiem, kas ļāva no vietnes izgūt personas datus, vietnē izvietotajos datu ievades laukos ierakstot atbilstoši sagatavotus pieprasījumus. Vietnes uzturētāji tika informēti par atklātajām ievainojamībām. CERT.LV koordinēja ievainojamību novēršanu.

Neatbilstošas konfigurācijas rezultātā internetā brīvi pieejams bija kādas ar veselības aprūpi saistītas iestādes serveris, kurā tika ievietoti un uzglabāti pacientu dati attālinātai apstrādei.

CERT.LV sazinājās ar iestādi un sniedza rekomendācijas drošai servera konfigurācijai un datu aizsardzībai. Par incidentu informēta arī *Datu Valsts inspekcija*.

Kāda valsts iestāde ziņoja par iespējamu uzbrukumu tās resursam, kurā, iespējams, izgūta datubāze, par kuru uzbrucēji pieprasa izpirkumu. Veicot pārbaudi, tika konstatēts, ka vietne nav kompromitēta un šantāžas e-pasts ir krāpniecības mēģinājums, bet pārbaužu rezultātā tika atklātas arī vairākas ievainojamības attiecīgajā tīmekļa vietnē, kas pakļauj vietni reālam uzbrukuma riskam. Iestāde tika informēta par atklātajiem draudiem, CERT.LV veica ievainojamību novēršanas koordinēšanu.

CERT.LV aicināja interneta pakalpojumu sniedzējus (IPS) informēt klientus par nekorekti pieslēgtām *UPnP* iekārtām, kā arī rekomendēja tīkla līmenī ierobežot piekļuvi *SSDP* servisam, bloķējot *UDP* 1900 portu vai centralizēti izslēdzot *UPnP* funkcionalitāti vadāmajās klientu interneta piekļuves iekārtās. Nepareizi konfigurētas iekārtas ar internetā atvērtu *UDP* 1900 portu var tikt izmantotas apjomīgu *DoS* uzbrukumu veikšanai pret uzņēmumiem, tiešsaistes tirdzniecības vietnēm un valsts iestādēm. Porta bloķēšana neietekmēs individuālo galalietotāju iekārtu darbību, bet būtiski novērsīs apjomīgu *DoS* uzbrukumu risku.

Veicot izpēti ievainojamās lietu interneta (*IoT*) iekārtās, tika konstatēts, ka trešo pušu nesankcionētai izmantošanai ir pakļautas virkne novērošanas kameru, t.sk. kādas valsts iestādes. CERT.LV koordinēja ievainojamību novēršanu.

Jūnija vidū pasauli saviļņoja ziņa par *Ripple20* ievainojamību kopu, kas apvieno 19 ievainojamības (daļa no tām kritiskas) kādā plaši izmantotā nelielā bibliotēkā un skar dažādas lietu interneta (*IoT*) iekārtas: gudrās mājas, veselības aprūpes iekārtas, elektroapgādes un transporta sistēmas, industriālās iekārtas, printerus, maršrutētājus, mobilās/ satelītu komunikācijas iekārtas, datu centrus, komerciālo avio pārvadātāju iekārtas, dažādus biznesa risinājumus un daudz ko citu. Šī ievainojamā bibliotēka ir daudzviet integrēta iekārtu ražotāju izmantotā trešo pušu kodā, padarot iespējamu situāciju, kad ražotāji nav informēti par konkrētās ievainojamības esamību savos izstrādājumos.

Uzbrucējiem šīs ievainojamība sniedz iespēja iegūt pilnīgu kontroli pār ievainojamo iekārtu attālināti, vai, atsevišķos gadījumos, nokļūstot iekšējā tīklā ar, piemēram, kompromitēta maršrutētāja palīdzību.

CERT.LV veica pārbaudes, lai konstatētu iespējami ievainojamas iekārtas Latvijā. Pārbaužu rezultātā tika konstatēti vairāki desmiti šādu iekārtu, kuru vidū bija gan datu centru ekipējums, gan industriālās sistēmas. Ievainojamo iekārtu turētāji tika informēti, sniedzot rekomendācijas ievainojamību novēršanai.

Tika saņemta informācija par nepilnībām kādas lietotnes darbībā. Nepilnības skāra lietotāju datu apstrādi, pieļaujot it kā no lietotnes dzēsta maksājumu līdzekļa izmantošanu vai iespēju norēķināties ar svešu maksājumu karti. Lietotnes izstrādātāji tika informēti, nepilnības tika novērstas.

Atbildīgu ievainojamību atklāšana

Pārskata periodā tika saņemti daži maznozīmīgi ziņojumi.

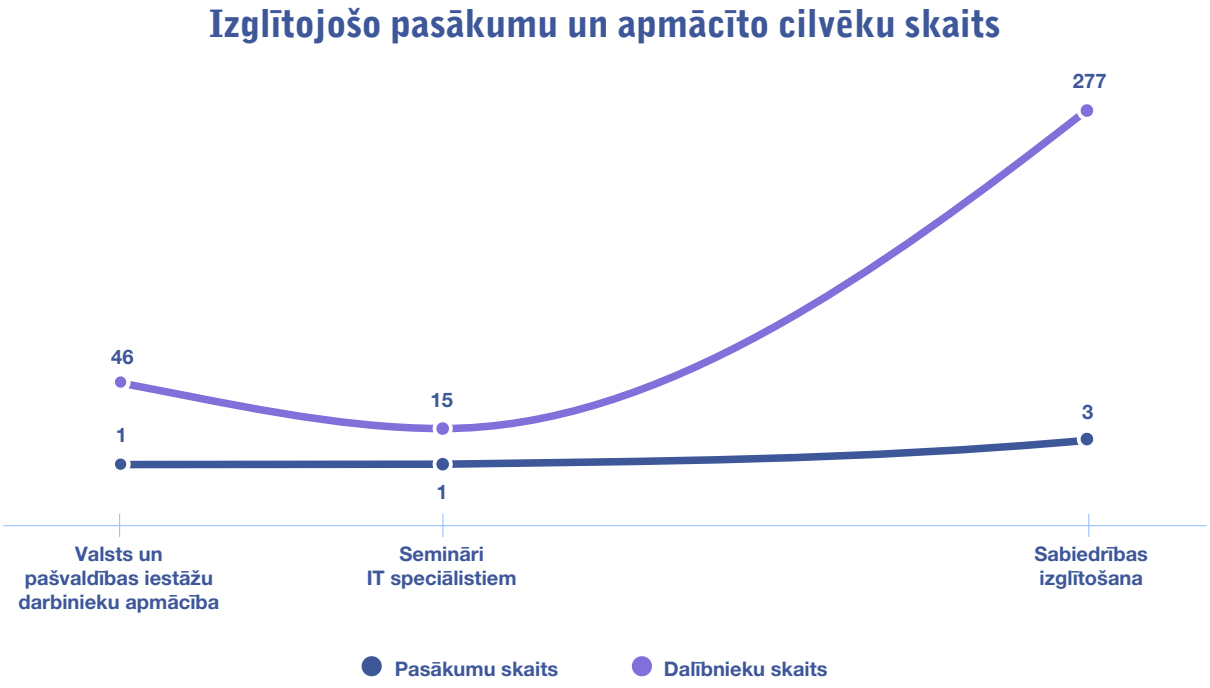
CERT.LV pasākumi incidentu novēršanā:

- 17. aprīlī slimnīcām (PPS) un NMPD tika izsūtīta informācija par iespējamajiem uzbrukumiem, kuru CERT.LV saņēma no starptautiskajiem sadarbības partneriem.
- 6. maijā interneta pakalpojumu sniedzējiem tika izsūtīts aicinājums informēt lietotājus par *UPnP* iekārtām, kuras pieslēgtas internetam, izmantojot drošības prasībām neatbilstošu konfigurāciju, kā arī izteikts aicinājums ierobežot piekļuvi *SSDP* servisam, bloķējot *UDP* 1900 portu vai centralizēti izslēdzot *UPnP* funkcionalitāti vadāmajās klientu interneta piekļuves iekārtās. Nepareizi konfigurētas iekārtas ar internetā atvērtu *UDP* 1900 portu var tikt izmantotas apjomīgu *DoS* uzbrukumu veikšanai.
- 15. maijā valsts un pašvaldību iestāžu un PPS atbildīgajiem par IT drošību tika izsūtīta informācija par agresīvu pikšķerēšanas kampaņu *Office 365* piekļuves datu izgūšanai.

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 7.punktā.

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



10. attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2020. gada 2. ceturksnī

Sadarbībā ar Drošāka interneta centru tapa informatīvs materiāls telekonferenču rīku *ZOOM* un *MS Teams* drošai izmantošanai, lai pasargātu bērnus un jauniešus. Materiāls tika publicēts e-klase.lv, kā arī drossinternets.lv un CERT.LV tīmekļa vietnē.

Lai atvieglotu iniciatīvas *Atbildīgs interneta pakalpojumu sniedzējs* dalībnieku saziņu ar saviem gala lietotājiem par viņu iekārtās konstatētajiem apdraudējumiem, kā arī sniegtu lietotājiem iespēju jebkurā laikā iepazīties ar informāciju par dažādiem apdraudējumiem, to ietekmi un novēršanas iespējām, CERT.LV tīmekļa vietnē esidross.lv publicēja aktīvo apdraudējumu aprakstus. Pārskata periodā CERT.LV par IT drošību izglītoja 338 cilvēkus, iesaistoties 5 izglītojošos pasākumos. Ņemot vērā ārkārtas stāvokli valstī, visi pasākumi notika tiešsaistē.

Ar starptautiskās kiberdrošības konferences Kiberšahs organizēšanu saistītie darbi:

Ņemot vērā pandēmiju un ar to saistītos ceļojumu ierobežojumus, un nenoteiktības apstākļus attiecībā uz iespējamajām darbībām nākotnē, visi ar konferences Kiberšahs klātienes norisi saistītie organizatoriskie darbi tika apturēti. Tika pieņemts lēmums 1.oktobrī organizēt tehnisku tiešsaistes konferenci aptuveni 100 kiberdrošības ekspertiem, piesaistot ārvalstu lektorus prezentācijām tiešsaistes platformā. Tika uzsākta tirgus izpēte pakalpojumiem profesionālas tiešsaistes konferences nodrošināšanai (atbilstošas vides/ studijas pieejamība moderatora vajadzībām, tiešraides materiālu sagatavošana, filmēšana, tiešraides nodrošināšana, ieraksta apstrāde u.c).

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

Sadarbības tikšanās, konsultācijas un prezentācijas:

- Aprīļa sākumā ministriju atbildīgajiem par IT drošību tika novadīts tiešsaistes seminārs, kurā tika diskutēts par tiešsaistes sanāksmju rīku drošību, balstoties uz CERT.LV veikto rīku analīzi, kuras rezultāti pirms semināra tika izsūtīti visiem pasākuma dalībniekiem.

- Pēc Aizsardzības ministrijas pieprasījuma tika sagatavotas instrukcijas *MS Excahnge* serveru konfigurācijai, kas veicinātu efektīvāku mēstuļu filtrēšanu un potenciāli kaitīgu e-pastu atpazīšanu. Ieteikumi ar Aizsardzības ministrijas starpniecību tika izplatīti arī citām valsts iestādēm.

- CERT.LV sniedza konsultācijas iesaistītajām ministrijām un to padotības iestādēm MK noteikumu nr.442 *Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām* izmaiņu saskaņošanas gaitā. Izmaiņas saistās ar prasībām par *DMARC* ieviešanu e-pasta sistēmām.

- CERT.LV veica attālinātās tikšanās ar divu slimnīcu, kas ir noteiktas kā pamatpakalpojumu sniedzēji - pārstāvjiem, informējot par PPS statusu un no tā izrietošajiem pienākumiem IT drošības jomā, par CERT.LV piedāvāto pakalpojumu klāstu, kā arī lietišķās sadarbības iespējām.

- CERT.LV pārstāvji piedalījās atklāšanas sanāksmē, kas tika veltīta *NIS (Tīklu un informācijas drošības direktīvas)* ieviešanas izvērtējumam un iespējamām izmaiņām. CERT.LV pārstāvji piedalījās anketas aizpildīšanā par *NIS* direktīvas ieviešanu Latvijā, kā arī piedalījās EK pārstāvju organizētā intervijā par šo jautājumu, gan kā nacionālā CERT vienība, gan kā Digitālās drošības uzraudzības komitejas pārstāvji. CERT.LV pauda viedokli par *NIS* direktīvas problēmjautājumiem, piemēram, nepieciešamajiem precizējumiem *NIS* direktīvā digitālo pakalpojumu sniedzēju identifikācijai saistībā ar izņēmumiem. CERT.LV pauda arī bažas par plāniem veidot arvien jaunus ES mēroga administratīvos regulējumus, radot papildu slogu.

- CERT.LV piedalījās tiešsaistes sanāksmēs par *VARAM* uzsākto Digitālās transformācijas pamatnostādņu sagatavošanu R2 darba grupā Digitālā drošība un uzticamība.

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:

- 27. maijā CERT.LV pārstāvis vadīja paneļdiskusiju *NATO CCDCoE* organizētajā kiberdrošības konferences *CyCon* grāmatas izlaišanas pasākumā, kas, kā daudzi pasākumi pandēmijas ietekmē, notika tiešsaistē. CERT.LV bija iesaistīta arī konferences sagatavošanās darbos, izvērtējot saturu, veidojot programmu, un piesaistot starptautiska līmeņa runātājus.
- 1. – 4. jūnijā CERT.LV pārstāvis piedalījās *NIS* direktīvas CERTu tīkla sanāksmē tiešsaistē un aktīvi piedalījās *Cyber Weather* darba grupā, kura regulāri apkopo informāciju par būtiskākajiem kiberincidentiem un reizi ceturksnī izstrādā kiberlaikapstākļu pārskatu Eiropai.
- CERT.LV aktīvi darbojās arī *NIS* direktīvas CERTu tīkla *Maturity* darba grupā, kura rūpējas par ES dalībvalstu *CSIRT* komandu brieduma līmeņa paaugstināšanu.
- CERT.LV pārstāvis piedalījās *NATO CCD CoE* kiberdrošības mācību *Crossed Swords* organizēšanas sanāksmēs, iesaistoties mācību satura sagatavošanā, izspēles dizaina izstrādē un attīstāmo spēju virzienu noteikšanā.
- Pārskata periodā tika turpināta *COVID-19* pandēmijas ietekmē *NIS* direktīvas CERTu tīkla ietvarā uzsāktās informācijas apmaiņa grupas darbība. Grupa primāri veica informācijas apmaiņu par incidentiem, kas saistīti ar *COVID-19* tēmu un kiberdrošību veselības nozarē. Ik nedēļu tika apkopota situācija visās Eiropas valstīs un gatavots pārskats lēmumu pieņēmējiem *NIS Cooperation* grupā, kā arī citās grupās. Latvija šajā procesā aktīvi piedalījās un informēja partnerus par kibertelpas aktualitātēm un tendencēm.

Sadarbība konkrētu incidentu risināšanā aplūkota pārskata 2. punktā.

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

Turpinās 2018. gada 1.septembrī CERT.LV uzsāktā *2017 CEF Telecom-Cyber Security* uzsaukumā apstiprinātā projekta I*mproving Cyber Security Capacities in Latvia* (līguma ar Eiropas Komisiju Nr.INEA/CEF/ICT/A2017/1528784) (turpmāk – *ICSC* projekts) īstenošana.

Darbs turpinājās visās sešās projektā definētajās darba pakās. Lai nodrošinātu sekmīgu aktivitāšu īstenošanu, jo īpaši izglītojošās kampaņas Informācijas tehnoloģiju drošība darbavietā sekmīgu norisi, kas sākotnēji plānotajā termiņā nebija iespējama ar *COVID-19* saistītās ārkārtas situācijas dēļ, tika uzsākta saskaņošana ar Eiropas Komisiju par projekta īstenošanas pagarināšana līdz 2020. gada 31. decembrim. Tika saņemts mutisks apstiprinājums no Eiropas Komisijas, ka projekta pagarinājums tiks sniegts. Gaidāms, ka dokumentācija tiks sakārtota 2020. gada jūlija un augusta mēnešos.

7. Projekta "Cyber Exchange" īstenošana

Turpinās 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.

2020. gada 2. ceturksnī *COVID-19* vīrusa izplatības ierobežošanai noteikto ceļojumu ierobežojumu dēļ nebija iespējamas projekta ietvaros plānotās apmaiņas vizītes. Tika uzsāktas sarunas par

iespējamu projekta pagarinājumu līdz 2021. gada 30. jūnijam, lai sekmīgi varētu nodrošināt plānoto pieredzes apmaiņas vizīšu īstenošanu.

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 dnsmuris.lv pieejamas ērti lietojamas instrukcijas *DNS* ugunsmūra aktivizēšanai. CERT.LV aktīvi popularizēja *DNS* ugunsmūri mājas lietotāju vidū ārkārtas stāvokļa laikā, ņemot vērā aktīvo mājas interneta izmantošanu ne tikai pirkumiem un atpūtai, bet arī mācībām un darbam.
- CERT.LV pārstāvis piedalījās Vidzemes augstskolas maģistra programmas *Kiberdrošības inženierija* kvalifikācijas darbu vērtēšanas komisijā, sniedzot visu 6 maģistra darbu novērtējumu un rekomendācijas zināšanu pilnveidošanai.
- 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 piedalījās *LVRTC* pakalpojuma *eParaksts* sertifikācijas veikšanā atbilstoši *eIDAS* prasībām, un pēc pozitīva audita ziņojuma saņemšanas atzina to par kvalificētu elektronisko parakstu. Tika izvērtētas un akceptētas izmaiņas *eID* karšu PIN/PUK koda izsniegšanas kārtībā.

9. Papildu pasākumu veikšana

Latvijas Interneta asociācijas Drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.04.2020. līdz 30.06.2020. ir saņēmusi un izvērtējusi 1022 ziņojumus. No tiem 883 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 17 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 18 ziņojumos konstatēta personas goda un cieņas aizskaršana, 1 ziņojums saņemts par naida runu un 1 ziņojums par vardarbību atainojošiem materiāliem. Par finanšu krāpšanas mēģinājumiem internetā saņemti 27 ziņojumi, 27 ziņojumu saturs nav bijis pretlikumīgs, 48 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 830 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 50 ziņojumu saturu dzēsuši interneta pakalpojumu sniedzēji pirms paziņojuma Valsts policijai. 3 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 880 ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem visi ziņojumi ir dzēsti no publiskas aprites internetā.

Līdzfinansē Eiropas Savienības Eiropas
infrastruktūras savienošanas instruments