Latvijas universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

2021 C3

Publiskais pārskats par CERT.LV uzdevumu izpildi

2021. gada 3. ceturksnis (01.07.2021. – 30.09.2021.)

Pārskatā iekļauta vispārpieejama informācija, un tas nesatur informāciju par tiem CERT.LV darbības rezultātiem, kas satur ierobežotas pieejamības informāciju. Pārskatam ir tikai informatīva nozīme.

Saturs

Kopsavilkums

2021. gada 3. ceturksnī CERT.LV kibertelpā novēroja pieaugošu pakalpojuma atteices uzbrukumu aktivitāti pret Latvijas publiskā sektora resursiem, kā arī pieaugošu zvanītāja numura viltošanas izmantošanu uzbrukumos.

Pārskata periodā tika reģistrētas 99 325 unikālas apdraudētas IP adreses, kas ir par 10% mazāk nekā iepriekšējā ceturksnī un par 38% mazāk nekā šajā pašā periodā pirms gada.

Pārskata periodā Latvijas interneta telpā izplatītākie apdraudējumi:

- konfigurācijas nepilnības (70 138 unikālas IP adreses) ar kritumu par 7% pret iepriekšējo periodu;
- ļaundabīgs kods (12 604 unikālas IP adreses) ar kritumu par 21%;
- ielaušanās mēģinājumi (3032 unikālas IP adreses) ar kritumu par 26%.

Kritums ar ļaundabīgo kodu inficēto iekārtu apjomā skaidrojams ar *Android.Hummer* apjoma samazinājumu no ārvalstu sadarbības partneriem saņemtajos datos. Savukārt ielaušanās mēģinājumu kritums skaidrojams ar ielaušanās mēģinājumu apjoma samazinājumu par 50% jūlija mēnesī.

Lai arī bija vērojama pieaugoša pakalpojuma atteices uzbrukumu (DDoS) aktivitāte, kas tika vērsta pret Latvijas publiskā sektora resursiem, mērķētu uzbrukumu pazīmes, piemēram, draudu e-pasti, kuros tiktu pieprasīts izpirkums par uzbrukumu pārtraukšanu, netika konstatētas.

Turpināja pieaugt zvanītāja numura viltošanas izmantošana krāpniecībās (zvani no bankas u.tml.). Šai problēmai eksistē tehnoloģiski risinājumi, piemēram, STIR/SHAKEN protokolu kopa. Operatīvi jāpanāk tehnoloģisko risinājumu ieviešana – dialogā ar operatoriem vai normatīvā regulējuma veidā.

Pārskata periodā CERT.LV par IT drošību izglītoja 1126 cilvēkus, iesaistoties 13 izglītojošos pasākumos.

1. Elektroniskās informācijas telpā notiekošo darbību atainojums

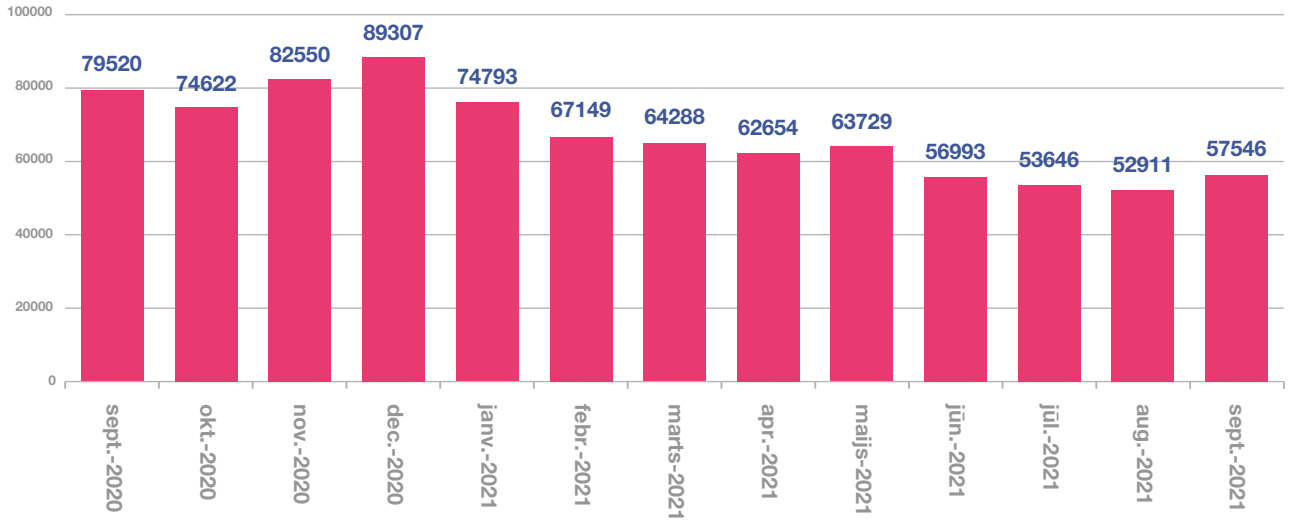
Ik mēnesi CERT.LV apkopo informāciju par apdraudētajām Latvijas IP adresēm. Lai sniegtu pilnvērtīgāku Latvijas kibertelpas pārskatu un nodrošinātu datu starptautisku salīdzināmību, CERT.LV apdraudējumu uzskaitei izmanto starptautiski lietotu incidentu taksonomiju (eCSIRT.net projekta izveidotā taksonomija, 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.

CERT.LV pārskata periodā ik mēnesi apkopoja informāciju vidēji par 55 000 ievainojamu unikālu IP adrešu.

2021. gada 3. ceturksnī tika reģistrētas 99 325 unikālas apdraudētas IP adreses, kas ir par 10% mazāk nekā iepriekšējā ceturksnī un par 38% mazāk nekā šajā pašā periodā pirms gada.

Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (70 138 unikālas IP adreses) ar kritumu par 7% pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs kods (12 604 unikālas IP adreses) ar kritumu par 21%, bet trešais – ielaušanās mēģinājumi (3032 unikālas IP adreses) ar kritumu par 26%.

Apdraudējumu sadalījums pa mēnešiem



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

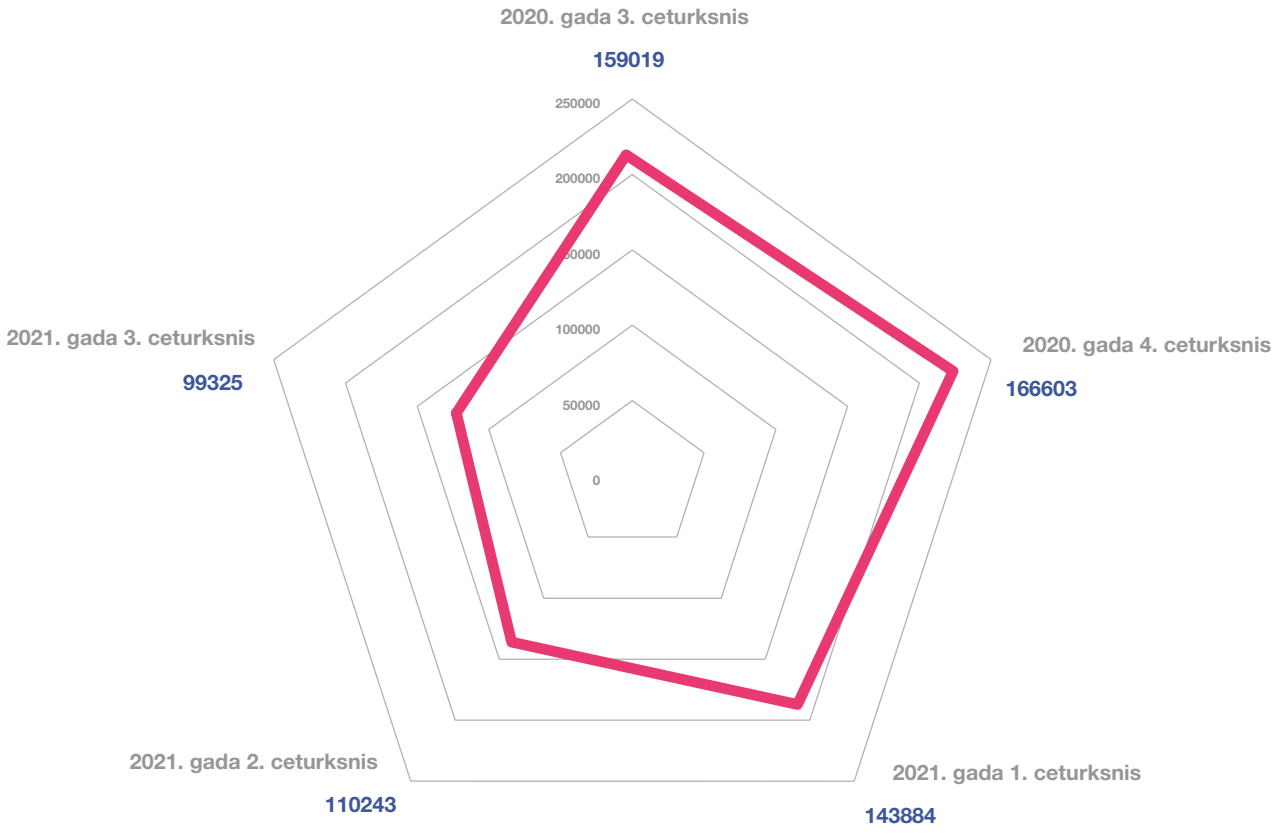
Kritums ar ļaundabīgo kodu inficēto iekārtu apjomā skaidrojams ar *Android.Hummer* apjoma samazinājumu no ārvalstu sadarbības partneriem saņemtajos datos. Savukārt ielaušanās mēģinājumu kritums skaidrojams ar ielaušanās mēģinājumu apjoma samazinājumu par 50% jūlija mēnesī.

Ļaunatūras topa pirmo vietu saglabā *Android.Hummer*, kas iekārtās ar *Android* operētājsistēmu (planšetdatoros un viedtālruņos) demonstrē uznirstošas (*pop-up*) reklāmas un patstāvīgi lejupielādē dažādas lietotnes.

Otrajā vietā izvirzījusies ļaunatūra *Stantinko*, kas paredzēta dažādu kriptovalūtu ieguvei, nesankcionēti izmantojot upura iekārtas resursus un potenciāli radot iekārtas pārslodzi, kā arī demonstrē lietotājam reklāmas, tādējādi nodrošinot reklāmu izvietotājiem peļņu.

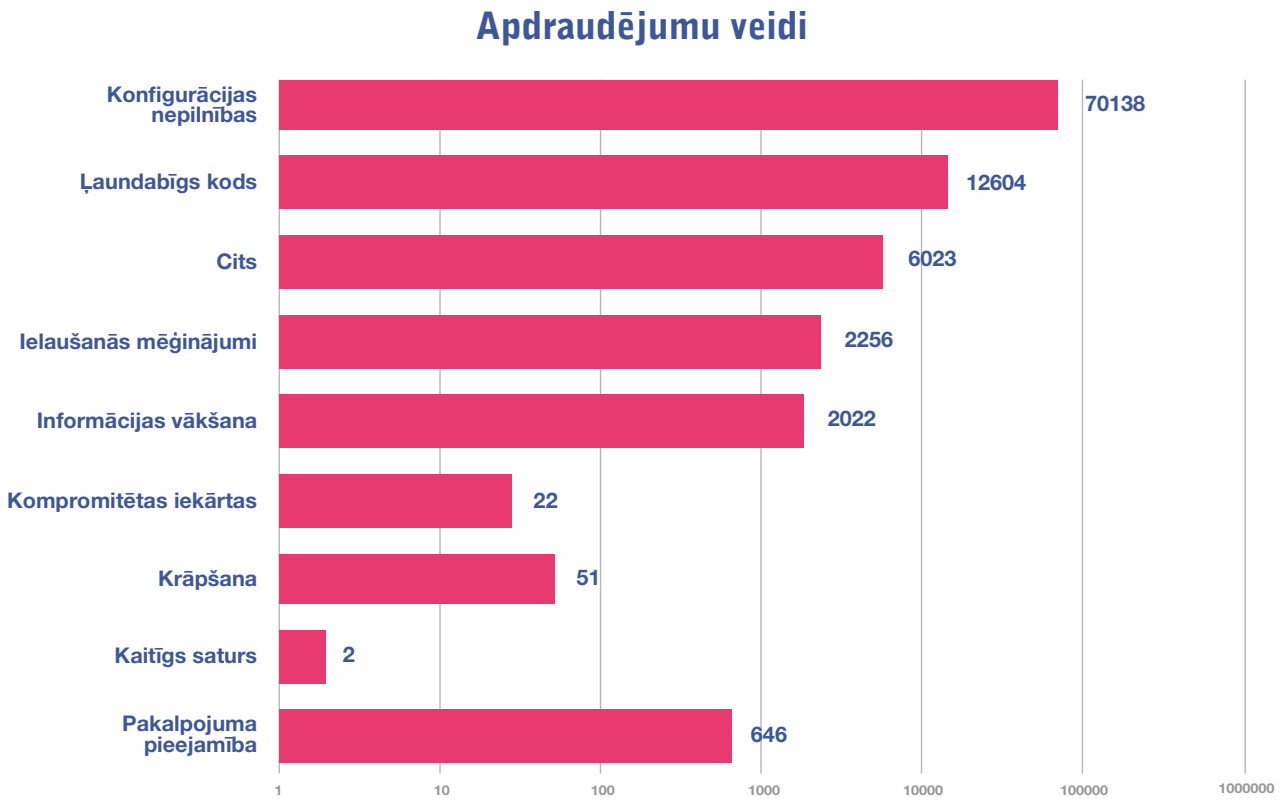
Vietu topa augšgalā nemainīgi saglabā arī *WannaCry* (*WannaCrypt*) – ļaunatūra ar šifrējošo potenciālu. Šīs ļaunatūras izplatība vērojama galvenokārt privātajā sektorā. Izplatību iespējams novērst, uzstādot *Windows* iekārtu atjauninājumus.

Apdraudējumu sadalījums pa ceturkšņiem



2. attēls – CERT.LV reģistrētās apdraudētās IP adreses pa ceturkšņiem 2020. un 2021. gadā.

Konfigurācijas nepilnību topa augšgals saturiski paliek nemainīgs, līderiem nedaudz apmainoties vietām. Līderpozīciju ieņem *Accessible-FTP*. FTP datu pārraides protokols nenodrošina pārraidāmo datu šifrēšanu, ja vien netiek izmatota papildu aizsardzība TLS vai SSL protokola formā (attiecīgi FTPS). Šī konfigurācijas nepilnība pakļauj noplūdes riskam sensitīvu informāciju un piekļuves datus. Otrajā vietā atrodas *OpenRDP*. RDP ir attālās piekļuves risinājums, kas bieži tiek izmantots

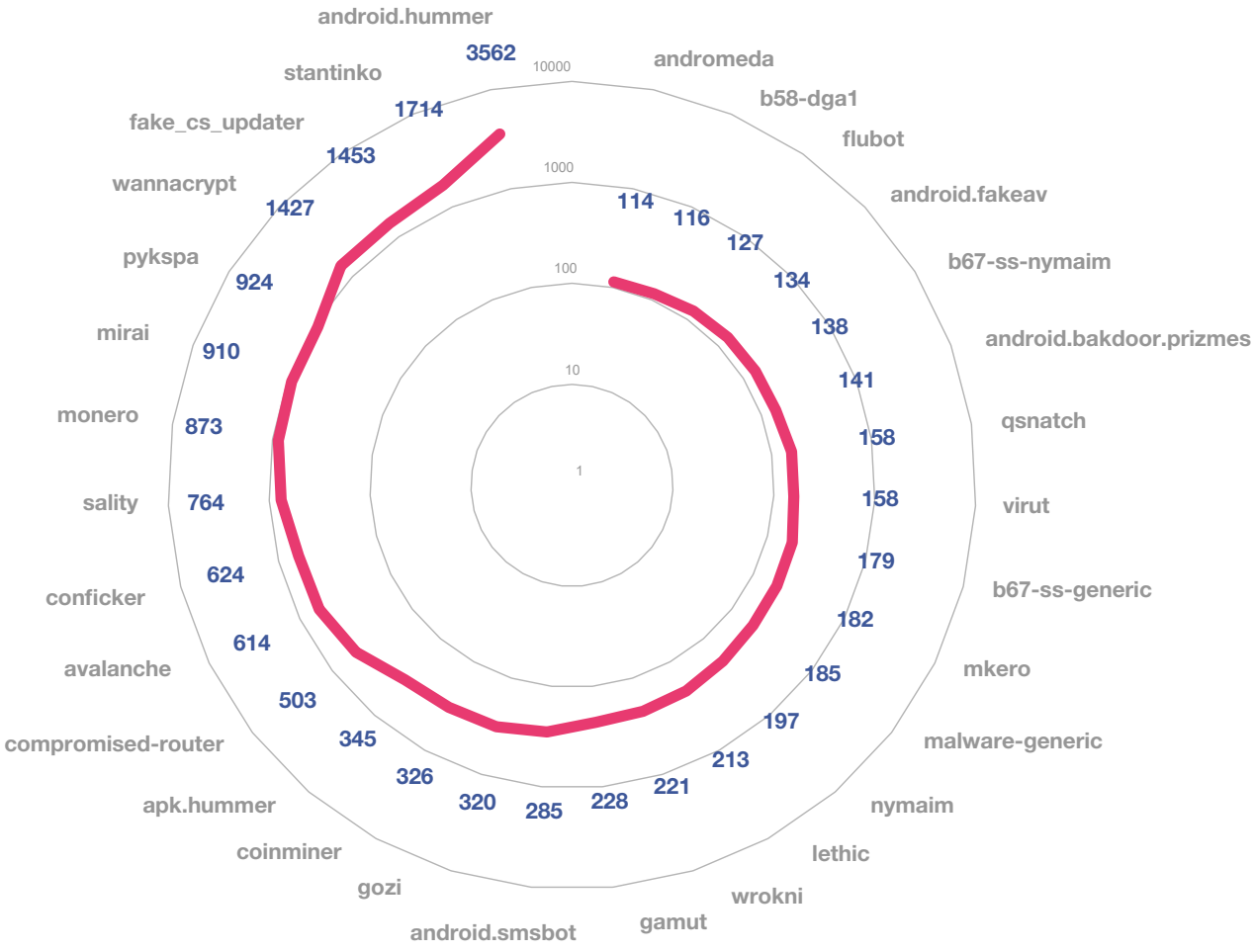


3. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2021. gada 3. ceturksnī pa apdraudējumu veidiem.

arī uzbrukumos. 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.

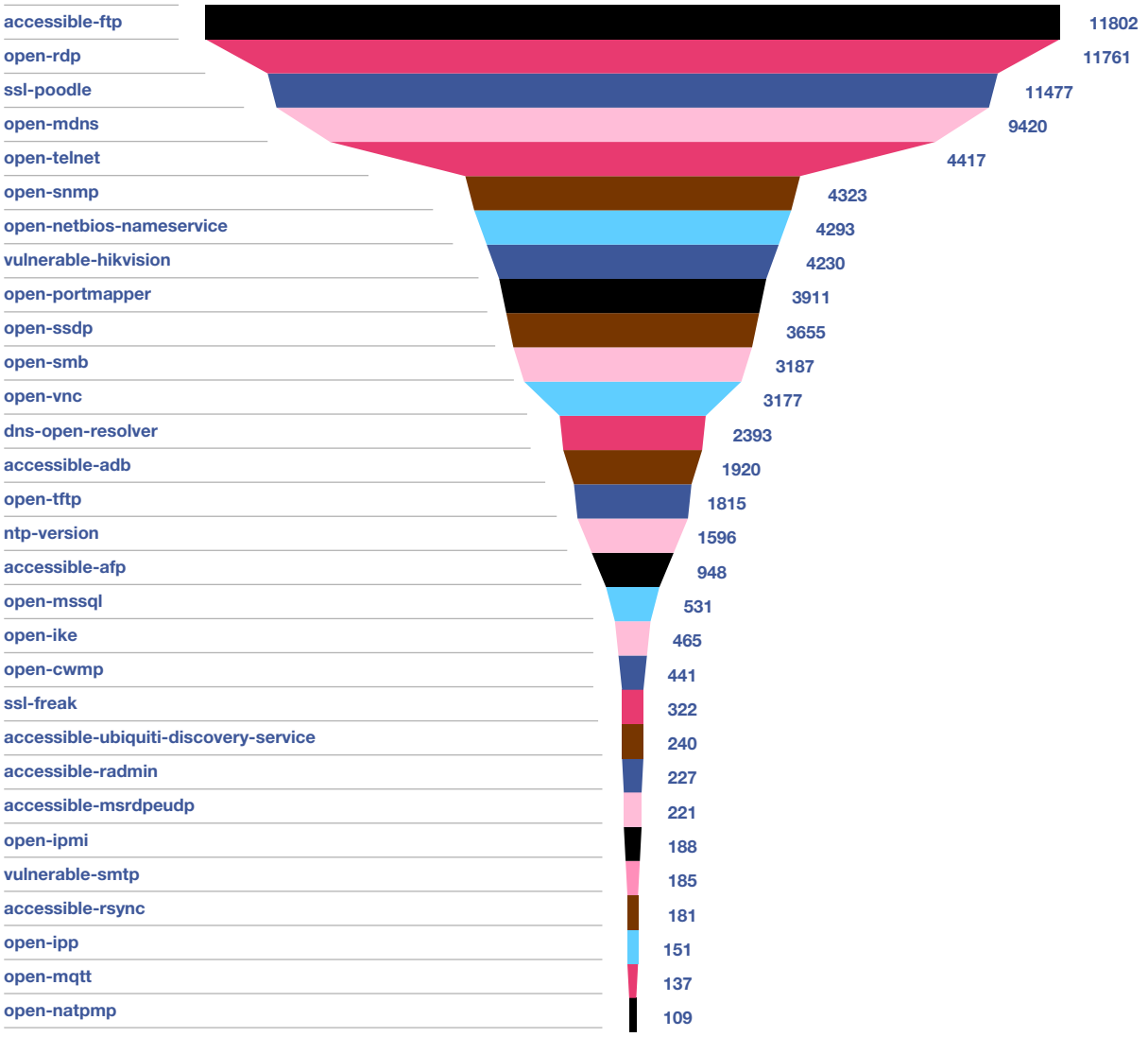
Trešo vietu ieņem konfigurācijas nepilnība *SSL-Poodle,* kas pakļauj iekārtu *POODLE* (*Padding Oracle On Downgraded Legacy Encryption*) uzbrukumam, sniedzot uzbrucējiem iespēju pārtvert šifrētu datu plūsmu, piemēram, lietotājvārdus, paroles, *cookies* u.c., un izlikties par iekārtas lietotāju.

Unikālo IP adrešu skaits – ļaundabīgs kods



4. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2021. gada 3. ceturksnī ar apdraudējuma veidu – ļaundabīgs kods.

Unikālo IP adrešu skaits – konfigurācijas nepilnības



5. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2021. gada 3. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

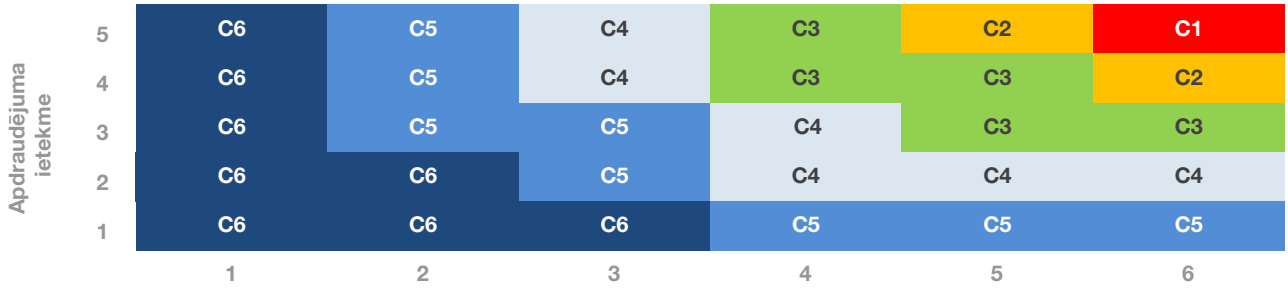
Pilnvērtīgākam kibersituācijas novērtējumam CERT.LV 2020. gadā ir uzsākusi Apvienotās Karalistes Nacionālā kiberdrošības centra (NCSC) izveidotās apdraudējumu matricas lietošanu. Matricā ievietotie apdraudējumi tiek grupēti pēc tā, cik nozīmīga ir skartā iestāde vai uzņēmums un/vai cik plašu sabiedrības 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% (28 unikālas apdraudētas IP adreses/gadījumi) no visiem kategorizētajiem apdraudējumiem. 80% šo apdraudējumu veido augstas un vidējas ietekmes ļaundabīgs kods (*Android.Hummer, Tinba, Stantinko* u.c.), bet 20% pakalpojuma atteices jeb DDoS uzbrukumi augstas prioritātes iestādēs.

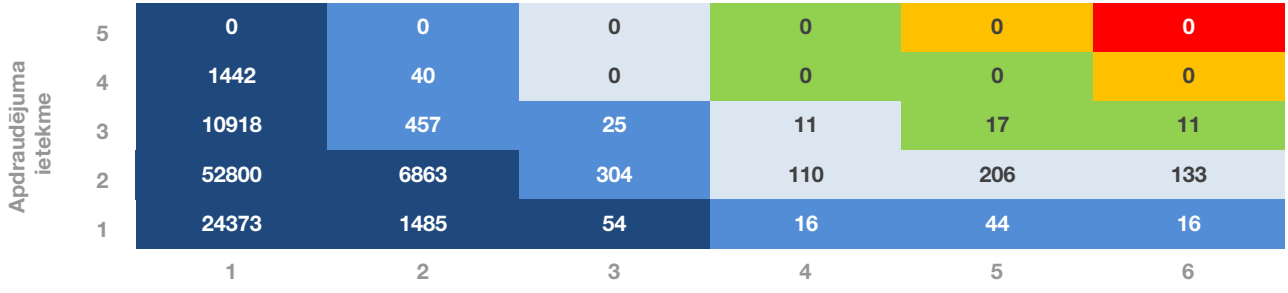
Apdraudējumu matrica



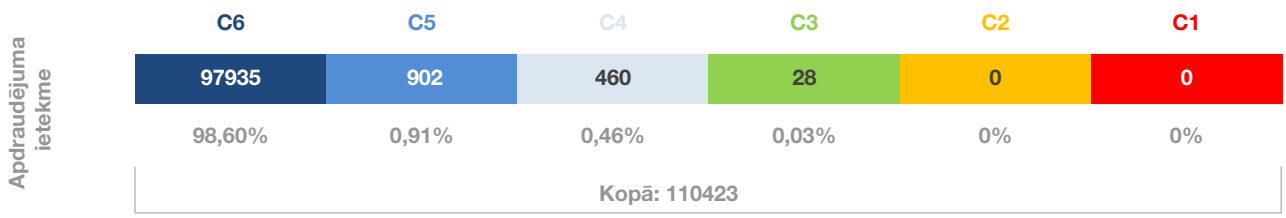
6. attēls – Apdraudējumu matricas sadalījums kategorijās.

Lielākā daļa C4 līmeņa apdraudējumu (būtiski apdraudējumi ar vidēju ietekmi) bija konfigurācijas nepilnības (*Accessible-ftp*, *NTP-Version, SSL-Poodle*, u.c.), ielaušanās mēģinājumi, pakalpojuma atteices (DDoS) uzbrukumi un ļaundabīgs kods (*Android.Hummer, Android.Rootnik u.c.*), kas novēroti augstas un vidēji augstas prioritātes valsts iestādēs, kā arī virknē augstākās izglītības iestāžu un pašvaldību.

Apdraudēto unikālo IP adrešu izvietojums



7. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu izvietojums matricā 2021. gada 3. ceturksnī valsts un pašvaldību institūcijās.



8. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu sadalījums apdraudējumu kategorijās pēc apdraudējuma ietekmes (matrica) 2021. gada 3. ceturksnī.

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 tiek parakstīts saprašanās memorands 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.

Iniciatīvas *Atbildīgs interneta pakalpojumu sniedzējs* ietvaros ar interneta pakalpojumu sniedzēju starpniecību lietotājiem tiek nosūtīta ne tikai informācija par apdraudējumiem, kas konstatēti viņu lietotajās iekārtās, bet arī rekomendācijas šo apdraudējumu novēršanai. Lai padarītu šo informāciju izmantojamu plašākam interneta pakalpojumu sniedzēju klientu lokam, apdraudējumu un ieteikumu apraksti tika sagatavoti arī angļu valodā.

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

Krāpnieciskās saites, kuras iesūtījuši iedzīvotāji un identificējusi CERT.LV, operatīvi tiek ievietotas CERT.LV un NIC.LV uzturētajā DNS ugunsmūrī https://dnsmuris.lv, tādējādi pasargājot no uzbrukuma DNS ugunsmūra lietotājus. DNS ugunsmūris bez maksas ir pieejams ikvienam Latvijas iedzīvotājam un uzņēmumam.

Lielākā daļa krāpniecību bija vērstas uz iedzīvotāju maksājuma karšu piekļuves datu un finanšu līdzekļu izkrāpšanu. Uzbrucēji veica krāpnieciskus telefona zvanus, bieži vien viltojot zvanītāja numuru, vai sūtīja iedzīvotājiem e-pastus, uzdodoties, galvenokārt, par banku, tiesībsargājošo iestāžu vai piegādes uzņēmumu darbiniekiem. Iedzīvotāji cieta finansiālus zaudējumus līdz pat 60 000 eiro, iesaistoties kriptovalūtu investīcijās, bet uzņēmumi cieta no iejaukšanās biznesa sarakstē – apmaksājot viltus rēķinus. Uzņēmumu kopējie zaudējumi sasniedza gandrīz 200 000 eiro. Viltotu telefona zvanu problēmai iespējami tehnoloģiski risinājumi, piemēram STIR/SHAKEN protokolu kopa. Operatīvi būtu jāpanāk tehnoloģisko risinājumu ieviešana – dialogā ar operatoriem vai normatīvā regulējuma veidā.

Pārskata periodā pieauga to uzbrukumu skaits, kuru mērķis bija izkrāpt *Office 365* piekļuves tiesības, nevis iegūstot lietotāja pieejas datus (lietotājvārdu un paroli), bet piesaistot *Office 365* kontu ļaundabīgai lietotnei (*Azure App*). Šādi uzbrucēji varēja iegūt piekļuvi dažādiem lietotājam

pieejamiem resursiem, piemēram, e-pastam, kalendāram, *SharePoint*, *Skype*, *OneDrive* u.c., kā arī visiem trešo pušu risinājumiem, kuros organizācijas ietvaros tiek izmantota vienota pierakstīšanās (*Single Sign-On*), piemēram, *Zoom* platformā.

Tika fiksēti jauna veida izspiešanas e-pasti. Līdzšinējos gadījumos krāpnieki mēdza apgalvot, ka uzlauzuši upura datoru un ieguvuši kompromitējošu video materiālu, par kura nenopludināšanu tika pieprasīta izpirkuma maksa. Jaunajos krāpnieciskajos e-pastos rakstītājs komunicēja krievu valodā un uzdevās par pasūtījuma slepkavu, kas pieprasa izpirkuma maksājumu, lai it kā atceltu pasūtījumu. CERT.LV aicināja ar krāpniekiem nekomunicēt un izpirkumu nemaksāt.

Septembra sākumā CERT.LV speciālistu rīcībā nonāca krāpnieciskas saziņas paraugs, kurā uzbrucējs uzdevās par uzņēmuma vai iestādes vadītāju un aicināja darbinieku – e-pasta saņēmēju – norādīt savu telefona numuru, lai pretēji ierastajam paņēmienam – sarakstei e-pastā – tālāk turpinātu saziņu *WhatsApp*. CERT.LV savos sociālo tīklu kontos aicināja iedzīvotājus atsaukties, ja saņemti šādi e-pasti, un iesūtīt e-pastu paraugus, lai iegūtu plašāku tehnisko informāciju par šiem krāpniecību mēģinājumiem un pārliecinātos, ka šādi netiek izplatīta ļaunatūra. Tika noskaidrots, ka uzbrukuma mērķis bija panākt dāvanu kartes iegādi, un ļaunatūras izplatīšanas mēģinājumi netika konstatēti.

Tika saņemti vairāki ziņojumi par viltus loteriju, kurā nesankcionēti izmantots *Maxima* zīmols. Krāpniecības mērķis bija panākt, lai lietotājs piezvana uz maksas telefona numuru. Pastāv iespēja, ka atkarībā no lietotāja iekārtas un izmantotā interneta pārlūka krāpnieciskās ziņas saturs mainījās. CERT.LV aicināja lietotājus būt modriem, pievērst uzmanību vietnes adresei un neuzķerties.

2.2. Pakalpojuma pieejamība (DDoS)

Pārskata periodā bija vērojama pieaugoša pakalpojuma atteices uzbrukumu aktivitāte pret Latvijas publiskā sektora resursiem. Uzbrucēju identitātes un motivācija nav noskaidrota, taču

netika fiksētas arī mērķētu uzbrukumu pazīmes, piemēram, draudu e-pasti, pieprasot izpirkumu par uzbrukumu pārtraukšanu.

Tika saņemts ziņojums par traucējumiem Saeimas tiešsaistes platformas *e-Saeima* darbībā Saeimas ārkārtas sēdes laikā 4. augustā. CERT.LV sadarbībā ar Saeimas drošības biroju veica tehnisko datu padziļinātu analīzi. Tās rezultāti ļāva secināt, ka ārēja ietekme uz tiešsaistes platformas *e-Saeima* sistēmu nav notikusi. Īslaicīgus *e-Saeimas* darbības traucējumus radīja iekšējo sistēmu darbības īpatnības.

Īslaicīgi traucēta tika vairāku valsts iestāžu resursu darbība. Divos gadījumos ārēja ietekme netika konstatēta; darbības traucējumus izraisīja nepilnības sistēmas darbībā vai neatbilstoša DDoS aizsardzības risinājuma konfigurācija.

Virkne DDoS uzbrukumu, kas tika vērsti pret valsts un pašvaldību iestāžu resursiem, tika veiksmīgi atvairīti. Vienā no gadījumiem uzbrukuma ietekmes mazināšanai resursam tika liegta piekļuve no ārvalstīm, izņemot Eiropu.

No vairākām mācību iestādēm tika saņemti ziņojumi par mācību procesa traucējumiem, kurus izraisījuši DDoS uzbrukumi pret skolu infrastruktūru. Ņemot vērā, ka uzbrukumi tikai novēroti tikai attālināto mācību laikā, laika posmā starp pulksten 9:00 un 14:00, tad viens no pieņēmumiem ir, ka šo uzbrukumu iniciatori ir skolu audzēkņi, un uzbrukumu veikšanai tiek izmantoti atbilstoši maksas pakalpojumi. Turpinās incidentu analīze.

2.3. Ļaundabīgs kods

Tika saņemts ziņojums par šifrējošā izspiedējvīrusa uzbrukumu kādam tehnoloģiju uzņēmumam. Uzbrucēji iekļuvuši sistēmā, izmantojot RDP. Pirms datu nošifrēšanas uzbrucēji iznīcinājuši datu rezerves kopijas. Uzbrukumā izmantota *Dharma* un *Raik* izspiedējvīrusu kombinācija. CERT.LV

aicināja uzņēmumu veikt pārbaudes, lai konstatētu, vai uzbrukuma rezultātā ir notikusi klientu datu noplūde, un noplūdes gadījumā informēt savus klientus.

Banku, organizāciju un uzņēmumu vārdā tika izplatīti e-pasti ar ļaundabīgiem pielikumiem, kuros esošie vīrusi bija paredzēti sensitīvas informācijas (lietotājvārdi, paroles u.tml.) ievākšanai no inficētajām iekārtām.

CERT.LV aicināja pievērst uzmanību e-pasta pielikumā pievienotā dokumenta paplašinājumam – burtiem, kas seko aiz pēdējā punkta dokumenta nosaukumā labajā pusē – un, ja paplašinājums ir .iso, .exe, .zip vai .rar, pielikumu vaļā nevērt.

Kāda uzņēmuma vārdā uzņēmuma klientiem tika izsūtīti e-pasti ar ļaundabīgu pielikumu. Uzņēmums iepriekš bija cietis incidentā ar iejaukšanos biznesa sarakstē. Uzbrucēji bija pārtvēruši uzņēmuma komunikāciju ar sadarbības partneriem un izsūtījuši viltus rēķinus, kā arī ieguvuši uzņēmuma klientu datubāzi.

Mērķēts uzbrukums tika vērsts pret kādas apvienības biedriem, apvienības vārdā izsūtot e-pastus ar ļaundabīgu pielikumu un aicinot apvienības biedrus pārtraukt jebkādu sadarbību ar pielikumā minētajām 50 apvienības dalīborganizācijām, kuru darbībās konstatēti apvienības noteikumu pārkāpumi.

Tika saņemta informācija par mērķētu uzbrukumu kādas valsts iestādes darbiniekiem. Uzbrucējs individuāli uzrunāja iestādes vadības līmeņa darbiniekus, uzdodoties par Krievijas žurnālistu, un e-pasta sarakstē nosūtīja inficētu *MS Word* dokumentu. Sākotnēji dokuments neradīja aizdomas par ļaundabīgu saturu, jo saturēja iestādes kompetencei atbilstošus jautājumus, uz kuriem tika lūgtas atbildes. Inficētās darbstacijas tika atvienotas no tīkla. Incidents tiek izmeklēts.

2.4. Ielaušanās mēģinājumi

Ielaušanās mēģinājumi lielākajā daļā gadījumu veikti, izmantojot paroļu minēšanu (*brute-force*). Uzbrukumi veikti galvenokārt pret dažādiem interneta pakalpojumu sniedzējiem un pret dažām valsts iestādēm, kā arī dažām pašvaldībām un privāto sektoru. Pēc CERT.LV rīcībā esošās informācijas šie uzbrukumi nav bijuši sekmīgi.

2.5. Kompromitētas iekārtas un datu noplūdes

Tika atklāta epasta konfigurācijas datu noplūde, ja *Microsoft Outlook* epasta klienta programmatūru izmanto, lai pieslēgtos pie epasta servera. Latvijas interneta telpā tika konstatēts domēns, kas varētu tikt izmantots šajā uzbrukumā (autodiscover[.]lv), taču šis domēns uzbrukumā izmantots nebija.

Lai aizsargātu publiskā sektora lietotājus, CERT.LV operatīvi izveidoja domēnu autodiscover.gov.lv, kas *.gov.lv lietotāju datiem neļauj nonākt potenciālo uzbrucēju rīcībā.

CERT.LV aicina izvērtēt publisko sektoru izmantot *.gov.lv zonu, jo tas gan identificē domēna lietotāju kā publiskā sektora pārstāvi, gan var papildus sniegt centralizētu aizsardzību.

Tika saņemts ziņojums par veiksmīgu uzbrukumu kādas valsts iestādes infrastruktūrai, kurā tika kompromitēts *Confluence* serveris. Servera kompromitēšana notika laikus neuzstādītu atjauninājumu rezultātā. CERT.LV norādīja uz nepieciešamību neaprobežoties ar atjauninājumu uzstādīšanu, bet atjaunot sistēmu, izmantojot rezerves kopijas, lai novērstu iespēju uzbrucējiem saglabāt kontroli pār sistēmu.

2.6. Ievainojamības

Tika atklāta kritiska ievainojamība *Hikvision* video novērošanas kamerās, kas ļoti plaši tiek izmantotas arī Latvijā gan publiskā, gan privātā sektora objektos. Ievainojamība ļāva attālināti pārņemt kontroli pār iekārtu, t.sk. skatīt/atslēgt/mainīt videosignālu. Latvijas interneta telpā tika konstatētas vismaz 6000 šī ražotāja kameras. CERT.LV par ievainojamību informēja sabiedrību.

Publiskajā telpā nonāca informācija par nopludinātiem *Fortinet VPN* lietotāju piekļuves datiem (lietotājvārdi un paroles). Pārbaudot publiskajā telpā pieejamo datu kopu, tika konstatēts, ka tajā iekļauta arī informācija par diviem Latvijas publiskā sektora resursiem. Resursu turētāji tika informēti par apdraudējumu un tika aicināti veikt *Fortinet VPN* lietotāju paroļu nomaiņu, kā arī pārbaudīt žurnalēšanas pierakstus, vai nav reģistrēti netipiski pieslēgšanās mēģinājumi.

2.7. Atbildīga ievainojamību atklāšana

29. jūlijā tika publicēts pētījums par drošības problēmām, elektroniski parakstot dokumentus ar dinamisku saturu. Apdraudējums nav kritisks, taču elektroniskā paraksta joma sabiedrībā ir sensitīva. Problēmu rada elektroniskā paraksta sistēmas dizains, kas ir identisks praktiski visās pasaules valstīs.

Lai gan parasta lietotāja skatījumā elektroniskais paraksts apliecina ekrānā redzamo informāciju, tas tā nav, jo tiek parakstīta datne, neiedziļinoties tās saturā. Populārākie datņu formāti .docx (*Microsoft Office*), .odt (*Libre Office*) un .pdf var saturēt dinamiskas daļas, kas var būt mainīgas no dokumenta atvēršanas reizes uz reizi, t.sk. dinamiski lejuplādējamas no interneta. Šādi parakstītam līgumam var mainīties, piemēram, summas, apjomi, atrunas, utt.

LVRTC kā e-paraksta uzturētājs sadarbībā ar CERT.LV ir publicējuši informāciju par atklāto ievainojamību un plāno uzrunāt programmatūras ražotājus *Microsoft*, *Adobe* un *The Document Foundation*, lai meklētu iespējas centralizētam risinājumam.

Tika saņemti ziņojumi par starpvietņu skriptēšanas (XSS) ievainojamību vairāku valsts iestāžu tīmekļa vietnēs. XSS ievainojamība sniedz uzbrucējiem iespēju veikt patvaļīgu *JavaScript* izpildi, izdarot izmaiņas tīmekļa vietnes saskarnē, izgūstot informāciju no lietotāja pārlūka vai pārsūtot lietotājus uz citu, ļundabīgu tīmekļa vietni. Par ievainojamību tika informēti vietņu uzturētāji.

Tika saņemts arī ziņojums par divām starpvietņu skriptēšanas (XSS) ievainojamībām *MikroTik* maršrutētājos. Par ievainojamībām tika informēts ražotājs. Lai arī *MikroTik* neuzskatīja ievainojamības par kritiskām, labojumi to novēršanai tika iekļauti 8. septembrī publicētajos atjauninājumos.

Tika saņemta informācija par ievainojamību kādas valsts iestādes e-pakalpojumā. Ievainojamība sniedza iespēju izgūt citu lietotāju dokumentus, izmantojot dokumenta identifikācijas numuru. Iestāde tika informēta par ievainojamību.

Tika saņemts ziņojums par vairākām tīmekļa vietnēm, kurām bija publiski pieejams vietnes monitoringa rīks, sniedzot iespēju ikvienam apmeklētājam aplūkot tīmekļa servera statistisko informāciju. Par ievainojamību tika informēti uzturētāji.

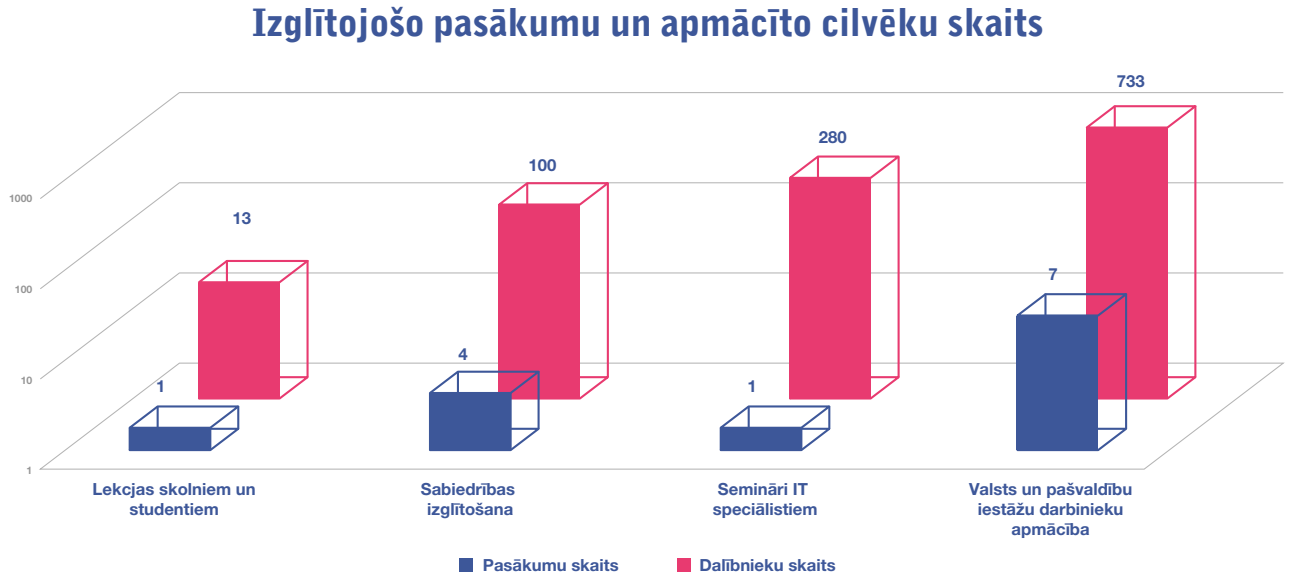
Informācija par jaunatklātiem apdraudējumiem un ievainojamībām tiek publicēta arī CERT.LV tīmekļa vietnē un sociālo tīklu *Twitter* (@certlv) un *Facebook* (@cert.lv) kontos.

Cita veida sadarbība ar dažādām iestādēm ir norādīta atskaites 4. un 5. punktā.

3. Pētnieciskais darbs, izglītojošo pasākumu organizēšana, mācības IT drošības jomā un sabiedrības informēšanā

8. jūlijā CERT.LV sniedza prezentāciju Latvijas Tirdzniecības un rūpniecības kameras (LTRK) biedriem par to, kas ir šifrējošie izspiedējvīrusi (kriptovīrusi) un kā tie apdraud uzņēmējus Latvijā.

26. augustā notika CERT.LV organizētais praktiskais tiešsaistes seminārs par pierādījumu apkopošanu pēc kiberincidenta, kurā tika aplūkota kiberincidentu izvērtēšana (triāža), pierādījumi un to vākšanas procedūra, kā arī sniegti praktiski padomi un demonstrācijas. Pasākumam tiešsaistē sekoja 280 dalībnieki.



9. attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2021. gada 3. ceturksnī

21. septembrī CERT.LV piedalījās *F9 Distribution Latvia* rīkotajā ražotāju un to pārstāvju seminārā, kurā tika aplūkotas IT nozares attīstības tendences, aktuālie drošības izaicinājumi un tehnoloģiju nākotne, sniedzot prezentāciju par kiberdrošības tendencēm un potenciālajiem apdraudējumiem.

Septembra noslēgumā CERT.LV eksperti iesaistījās Latvijas Eiropas Kopienas studiju asociācijas (LECSA) vadītajā projektā CYBER.EU.VET, kura mērķis ir jauniešu un pedagogu izpratnes veicināšana un zināšanu pilnveidošana par kiberdrošības jautājumiem. Projekta ietvaros jauniešiem bija jāizveido spēle, kas palīdzētu sasniegt projekta mērķus. CERT.LV eksperti iepazīstināja jauniešus ar informāciju par aktuālajiem kiberapdraudējumiem, kā arī piedalījās vērtēšanas komisijā.

Pārskata periodā CERT.LV par IT drošību izglītoja 1126 cilvēkus, iesaistoties 13 izglītojošos pasākumos.

Mediju uzmanības centrā bija mobilo iekārtu drošība, e-pastu drošība, kā arī šifrējošo izspiedējvīrusu uzbrukumi un aizsardzība pret tiem.

Tīmekļa vietnē www.cert.lv ik mēnesi CERT.LV ievieto mēneša kiberlaikapstākļu informāciju, kas ir atskats uz Latvijas kibertelpas iepriekšējā mēneša aktuālākajiem notikumiem. Kiberlaikapstākļu pārskats tiek gatavots, izmantojot vadlīnijas Eiropas Savienības Tīklu un informācijas sistēmu direktīvas (NIS Directive) CSIRT tīkla darba grupa *Cyber Weather* gatavotajam Eiropas kiberlaikapstākļu pārskatam, kurā reizi ceturksnī tiek apkopota informācija par būtiskākajiem kiberincidentiem.

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

Sadarbības tikšanās, konsultācijas un prezentācijas:

- CERT.LV piedalījās Ministru kabineta noteikumu Nr. 442 *Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām* (MK Nr. 442) izmaiņu sagatavošanas darbā, norādot, ka noteikumus jātuvina starptautiskajiem standartiem, tajos iekļaujot pamatprincipus, un atsevišķās nodaļās pievēršoties prasībām, kas ir specifiskas un attiecināmas tieši uz Latviju vai noteiktu darbības sektoru.
- CERT.LV turpināja projekta par valkājamo ierīču drošību norises vadību. Sadarbībā ar LUMII Mākslīgā intelekta laboratoriju un Elektronikas un datorzinātņu institūtu (EDI) tika turpināta tehniskā prototipa koncepta izstrāde.
- Dalība Izglītības un zinātnes ministrijas vadītajā profesijas standarta *Informācijas drošības vadītājs* projekta izvērtēšanas darba grupā, sagatavojot komentārus par darba dokumentiem un piedaloties sanāksmēs. 11. augustā Profesionālās izglītības un nodarbinātības trīspusējās sadarbības apakšpadomes (PINSTA) sēdē tika pieņemts atbilstošais profesijas standarts.

Sadarbība ar valsts iestādēm incidentu risināšanā aplūkota atskaites 2. punktā.

5. Sadarbība ar starptautiski atzītām informācijas tehnoloģiju drošības incidentu novēršanas institūcijām (vienībām)

CERT.LV starptautiskā sadarbība pārskata periodā:

- CERT.LV aktīvi piedalījās trijās NIS (Tīklu un informācijas drošības) direktīvas CERTu tīkla darba grupās:
  - *Cyber Weather* darba grupā, kura regulāri apkopo informāciju par būtiskākajiem kiberincidentiem un reizi ceturksnī izstrādā kiberlaikapstākļu pārskatu Eiropai.
  - *Maturity* darba grupā, kura rūpējas par ES dalībvalstu CSIRT komandu brieduma līmeņa paaugstināšanu.
  - *TOR Review* darba grupā, kas pārskata tīkla statūtus un nolikumu, atbilstoši tos aktualizējot.
- CERT.LV vadītāja Baiba Kaškina turpināja darbu kā *FIRST Membership Committee* (Jauno biedru uzņemšanas komitejas) līdzpriekšsēdētāja (*co-chair*), piedaloties jauno biedru pieteikumu izskatīšanā un veicinot biedru uzņemšanas procesa uzlabošanu.
- Darbs FIRST darba grupas *CSIRT Services Framework* darbā, lai izstrādātu vienotu ietvaru CERT komandu dalībnieku lomām, kompetencēm un prasmēm.
- CERT.LV turpināja darbu TF-CSIRT *Futures* darba grupā, lai izstrādātu jaunu pārvaldības modeli TF-CSIRT un *Trusted Introducer* Eiropas CERTu sadarbībai. Darba grupas darbība tika noslēgta 2021. gada septembrī, jo darba grupas mērķi tika sasniegti – kā nākotnes modelis TF-CSIRT tiek rekomendēts dibināt bezpeļņas organizāciju Nīderlandē. TF-CSIRT *Steering commitee* turpinās darbu, lai šo rekomendāciju īstenotu.

- Dalība ENISA Eiropas kiberdrošības indeksa (*EU Cybersecurity index*) darba grupā, kurā tiek izstrādāta kiberdrošības indeksa vērtības aprēķina metodoloģija dalībvalstu kiberdrošības novērtēšanai. Sadarbībā ar Aizsardzības ministriju un Satiksmes ministriju (aizpildot anketu) tika pausts Latvijas viedoklis par komponentēm, kuras izmantojamas Eiropas kiberdrošības indeksa veidošanā (brieduma līmeņa novērtēšanā). Indeksa komponentes tiek grupētas, par pamatu izmantojot ES Kiberdrošības akta struktūru (https://eur-lex.europa.eu/eli/reg/2019/881/oj).

- CERT.LV pārstāvis aktīvi piedalījās NATO CCDCoE organizēto praktisko kiberdrošības mācību *Crossed Swords 2021* organizēšanā, iesaistoties mācību plānošanā, tehniskā scenārija izstrādē un izpildes vadīšanas sagatavošanas darbos. Mācības plānotas 2021.gada decembrī.

- Dalība EU *CyberNet* projektā kā vienam no partneriem. Projekta mērķis ir stiprināt kiberdrošības ekspertīzi un attīstīt to ne tikai Eiropas Savienībā, bet arī ārpus tās robežām (www.eucybernet.eu). Dalība projektā sniegs iespēju CERT.LV ekspertiem, iesaistoties projekta dalībvalstu projektos, stiprināt savas zināšanas un kapacitāti, kā arī dalīties ar to ārpus Eiropas Savienības robežām, tā stiprinot starptautisko kiberdrošības kopienu.

- Turpinājās aktīva dalība enerģētikas informācijas apmaiņas un sadarbības grupā *Energy ISAC Camelot*, lai veicinātu informācijas apmaiņu un sekmētu enerģētikas sektora kiberdrošību.

- 08. septembrī CERT.LV uzņēma Igaunijas kolēģu delegāciju no RIA un CERT-EE, lai veicinātu pieredzes apmaiņu sarežģītu incidentu risināšanā, efektīvākā rīku un risinājumu izmantošanā, preventīvajos pasākumos un sabiedrības informēšanā.

Sadarbība konkrētu incidentu risināšanā aplūkota pārskata 2. punktā.

6. Projekta Joint Threat Analysis Network īstenošana

2021. gada 1. jūlijā CERT.LV uzsāka dalību *2020 CEF Telecom Call – Cybersecurity* uzsaukumā apstiprinātajā projektā *Joint Threat Analysis Network* (turpmāk – JTAN projekts), līguma ar Eiropas Komisiju Nr. INEA/CEF/ICT/A2020/2373165.

Projekta vadošais partneris ir Informācijas tehnoloģiju drošības incidentu novēršanas institūcija Polijā CERT.PL, kas darbojas institūta *Naukowa i Akademicka Sieć Komputerowa* (NASK) struktūrā. JTAN projektā piedalās arī partneri no Austrijas, Francijas, Igaunijas, Luksemburgas, Rumānijas un Slovākijas.

Kopējais JTAN projekta mērķis ir izveidot vienotu draudu analīzes tīklu (*Joint Threat Analysis Network – JTAN*). Tīkls būtu atvērts Eiropas CSIRT (*Computer Security Incident Response Team*) sadarbības grupai, kuras galvenā uzmanība pievērsta tehnisko, operatīvo un stratēģisko draudu izlūkošanas informācijas apmaiņai un analīzei.

Pārskata periodā tika parakstīts JTAN projekta Dotācijas līgums ar Eiropas Komisiju un Konsorcija līgums, CERT.LV piedalījās attālinātās JTAN projekta sanāksmēs. CERT.LV turpināja darbu pie rīka *Graphoscope* izstrādes, tā attīstīšanas un pilnveidošanas, kā arī prezentēja šo rīku citiem projekta partneriem.

Grafoskops ir rīks, kas paredzēts, lai korelētu datus no dažādiem datu avotiem un parādītu tos vizuālā formā. Kā datu avotu var izmantot arī rīku *Pastelyzer*, kas tika izstrādāts iepriekšējā Eiropas finansētajā projektā (*Improving Cyber Security Capacities in Latvia*, 2017-LV-IA-0058). Galvenās Grafoskopa iezīmes: 1) atbalsts daudziem datu avotiem; 2) tīmekļa bāzēta saskarne, kas nav atkarīga no iepriekš instalētām datu bāzēm; 3) vienkārša sistēmas uzstādīšana; 4) saskarne nodrošina elastīgus filtrus, kas atvieglo liela apjoma datu analīzi.

JTAN projekta īstenošana plānota līdz 2024. gada 30. jūnijam.

7. Projekts Cyber Excange 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 – *Cyber Exchange*) īstenošana.

Projekta mērķis ir stiprināt starptautisku sadarbību starp nacionālajām un valdības CSIRT/CERT organizācijām. *Cyber Exchange* 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.

Projekta pamata aktivitāte ir pieredzes apmaiņas vizīšu organizēšana – Latvijas CERT.LV pārstāvjiem viesojoties pie citu projekta dalībvalstu CSIRT/CERT komandām vai uzņemot vizītē kolēģus no citām CSIRT komandām.

Pārskata periodā projektā paredzēto apmaiņas vizīšu īstenošana nenotika, taču ir plānota viesošanās pie poļu CERT komandas nākamajā pārskata periodā.
Projektu plānots īstenot līdz 2022. gada 30. jūnijam.

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. DNS mūris ik dienu tiek papildināts ar Latvijas iedzīvotāju un kiberdrošības ekspertu sniegto informāciju par kiberuzbrucēju aktivitātēm Latvijas kibertelpā un sniedz iespēju aizsargāt lietotājus no ļaundabīga satura internetā.

  Projekta ietvaros ir bijuši jau daudzi gadījumi, kuros nostrādājusi aktīvā aizsardzība, pasargājot lietotājus no ļaundabīga satura un iekārtas no inficēšanas. Pārskata

periodā lietotāji tika pasargāti no vairāku viltus lapu apmeklējumiem, kredītkaršu datu zādzībām, viltus kurjerkompāniju tīmekļa vietņu apmeklējuma, kā arī liedz inficētām iekārtām sazināties ar vīrusu kontroles serveriem. Kopējais bloķēto domēnu skaits:

- Jūlijā – 6300
- Augustā – 2680
- Septembrī – 64939

Daļu no DNS PRZ pakalpojuma var izmantot 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.

► 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 turpināja uzraudzīt sertificētu uzticamības pakalpojumu sniedzēju darbību.

9. Institūta papildu pasākumu veikšana – atskaite par Latvijas Interneta asociācijas Net-Safe Latvia Drošāka interneta centra ziņojumu līnijas darbību

Latvijas Interneta asociācijas Drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.07.2021. līdz 30.09.2021. ir saņēmusi un izvērtējusi 2471 ziņojumu. No tiem 2292 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 14 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 7 ziņojumos konstatēta personas goda un cieņas aizskaršana, 3 ziņojumi saņemti par naida runu un 3 ziņojumi par vardarbību atainojošiem materiāliem. Par finanšu

krāpšanas mēģinājumiem internetā saņemti 30 ziņojumi, 75 ziņojumu saturs nav bijis pretlikumīgs, 47 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 2158 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 10 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kuru atrašanās vieta bija ārpus Latvijas, ir ievietoti INHOPE asociācijas datu bāzē un iesniegti attiecīgās INHOPE valsts ziņojumu līnijai turpmāko darbību veikšanai, lai dzēstu nelegālo saturu no publiskas aprites.

Pārskata periodā no Latvijā uzturētajiem 2292 ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem 2247 ziņojumi ir dzēsti no publiskas aprites un 45 ziņojuma saturs atrodas dzēšanas procesā sadarbībā ar Valsts policiju un interneta pakalpojumu sniedzējiem.

2021. gada 20. oktobrī.

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

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija