Latvijas universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

2022 C2

Publiskais pārskats par CERT.LV uzdevumu izpildi

2022. gada 2. ceturksnis (01.04.2022. – 30.06.2022.)

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

Jau kopš janvāra vidus Latvijas kibertelpā bija jūtama paaugstināta aktivitāte, kas līdz ar 9. maija notikumiem Latvijā pastiprinājās, Latvijas kibertelpai piedzīvojot intensīvākos kiberuzbrukumus savā pastāvēšanas vēsturē.

Pamatā tie bija piekļuves atteices jeb DDoS uzbrukumi, kas tika vērsti gan pret Latvijas valsts un pašvaldību iestāžu resursiem, gan Latvijas privātā sektora uzņēmumiem, bankām, medijiem, medicīnas iestādēm un kritisko infrastruktūru. Par daļu no šiem uzbrukumiem atbildību savā *Telegram* kanālā uzņēmies Krievijas agresiju atbalstošais grupējums *Killnet*, savukārt pārējie uzbrukumi ir attiecināmi uz kādu no šī grupējuma atzariem vai pro-krieviski noskaņotiem indivīdiem. Latvijas IT drošības sistēma ir savlaicīgi gatavota šādu uzbrukumu atvairīšanai. LVRTC, SIA TET un CERT.LV sadarbojoties un koordinējot IKT aizsardzības stratēģiju, ir sekmīgi panākta augsta noturība pret DDoS uzbrukumiem, īpaši valsts un kritiskās infrastruktūras IKT resursiem.

Uz pārskata perioda beigām ir konstatēti jau vairāki kompromitēti uzņēmumi, kas sniedz IT pakalpojumus gan valsts pārvaldes iestādēm, gan plašam privātā sektora uzņēmumu lokam. Apdraudēti ir visi šo uzņēmumu klienti. CERT.LV sniedz atbalstu uzņēmumiem un to klientiem, lai, veicot pārbaudes, apstiprinātu vai noliegtu konkrētu sistēmu kompromitēšanu, novērtētu potenciālā kaitējuma apjomu, kā arī mazinātu incidenta ietekmi un sekmētu infrastruktūras kibernoturības stiprināšanas pasākumus Ar augstu ticamību var pieņemt, ka tuvāko nedēļu vai mēnešu laikā uzbrukumu intensitāte vai ietekme var palielināties, kā arī iespējami jauni piegāžu ķēžu uzbrukumi.

Pārskata periodā tika reģistrētas 260 617 unikālas apdraudētas IP adreses, kas ir par 122% vairāk nekā iepriekšējā ceturksnī un par 136% vairāk nekā šajā pašā periodā pirms gada. Izplatītākie apdraudējumi:

- konfigurācijas nepilnības (125 334 unikālas IP adreses) ar pieaugumu par 90% pret iepriekšējo periodu;
- ļaundabīgs kods (9 801 unikāla IP adrese) ar pieaugumu par 10%;
- pakalpojuma pieejamība (2 663 unikālas IP adreses) ar pieaugumu par 414%.

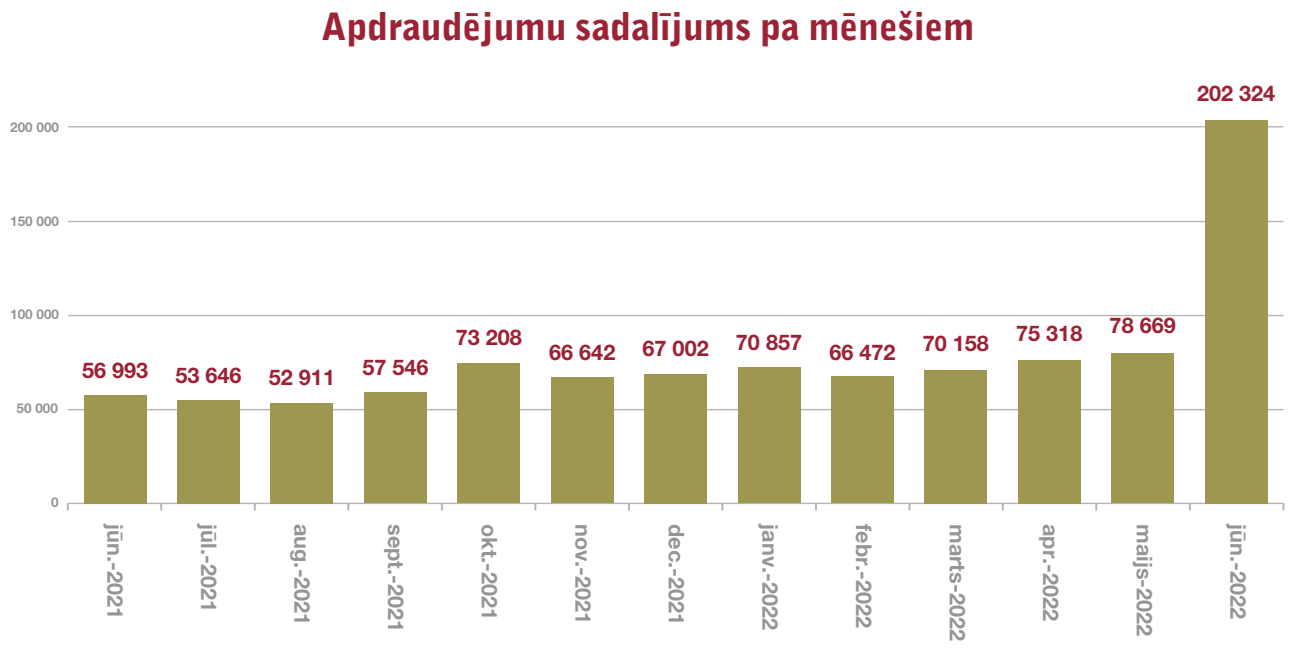
Lai piekļūtu iedzīvotāju finanšu līdzekļiem, krāpnieki izmantoja jaunu krāpšanas metodi – apmaksātas *Google* reklāmas viltotām banku tīmekļa vietnēm, tādējādi nodrošinot, ka viltus vietnes parādīsies kā pirmie meklēšanas rezultāti, meklējot konkrētu banku. Sākotnēji tika reklamētas galvenokārt viltotas *Luminor* bankas tīmekļa vietnes, bet vēlāk parādījās arī reklāmas ar *Citadele* un *Swedbank* vietņu viltojumiem. Saņemta informācija par vairākiem cietušajiem.

Pārskata periodā CERT.LV par IT drošību izglītoja 5806 cilvēku, iesaistoties 34 izglītojošos pasākumos.

Apdraudējuma līmenis Latvijas kibertelpā pārskata periodā bijis nepieredzēti augsts, tomēr kopumā situācija Latvijas kibertelpā vērtējama kā stabila, bet ar augstu riska potenciālu plašākiem incidentiem. Situācija tiek veiksmīgi kontrolēta, CERT.LV sadarbībā ar partneriem turpina uzraudzīt tajā notiekošo.

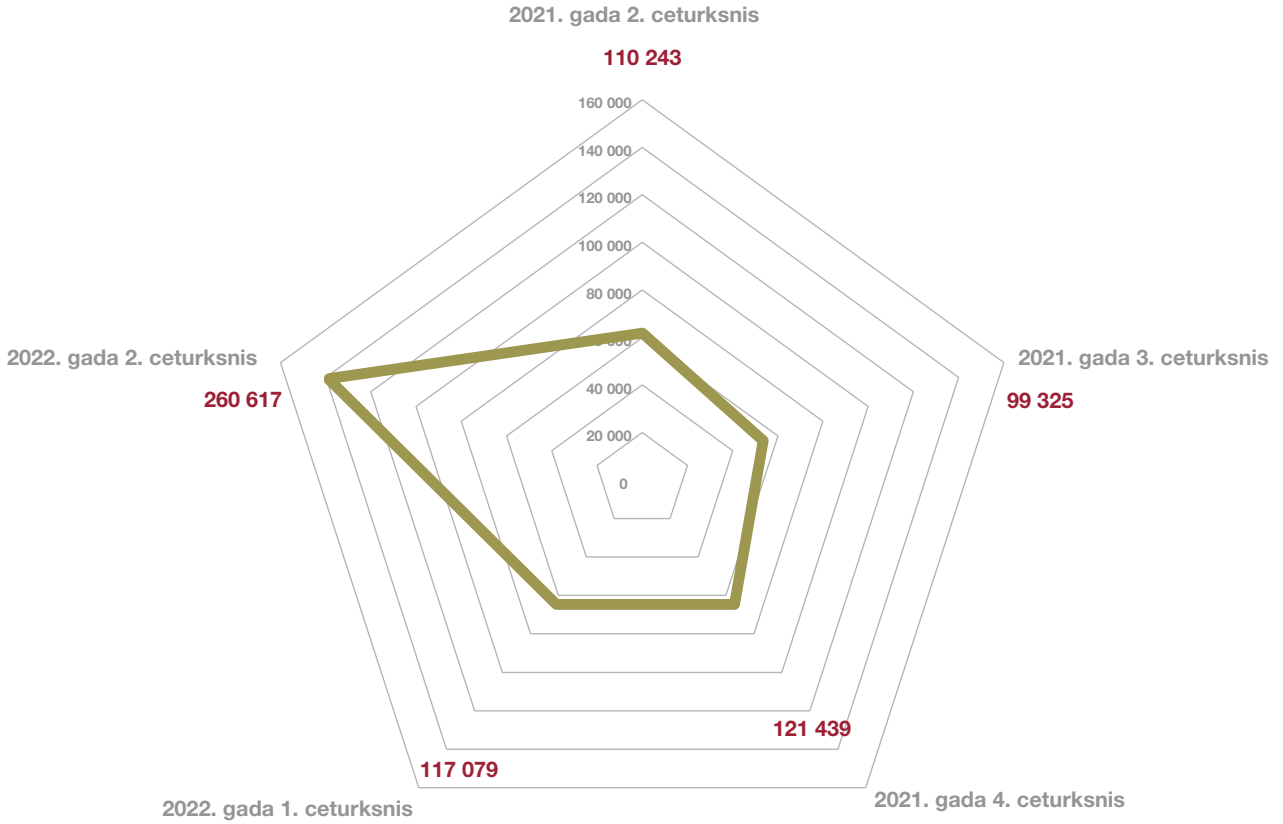
1. Vienota atainojuma uzturēšana par elektroniskās informācijas telpā notiekošajām darbībām

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.



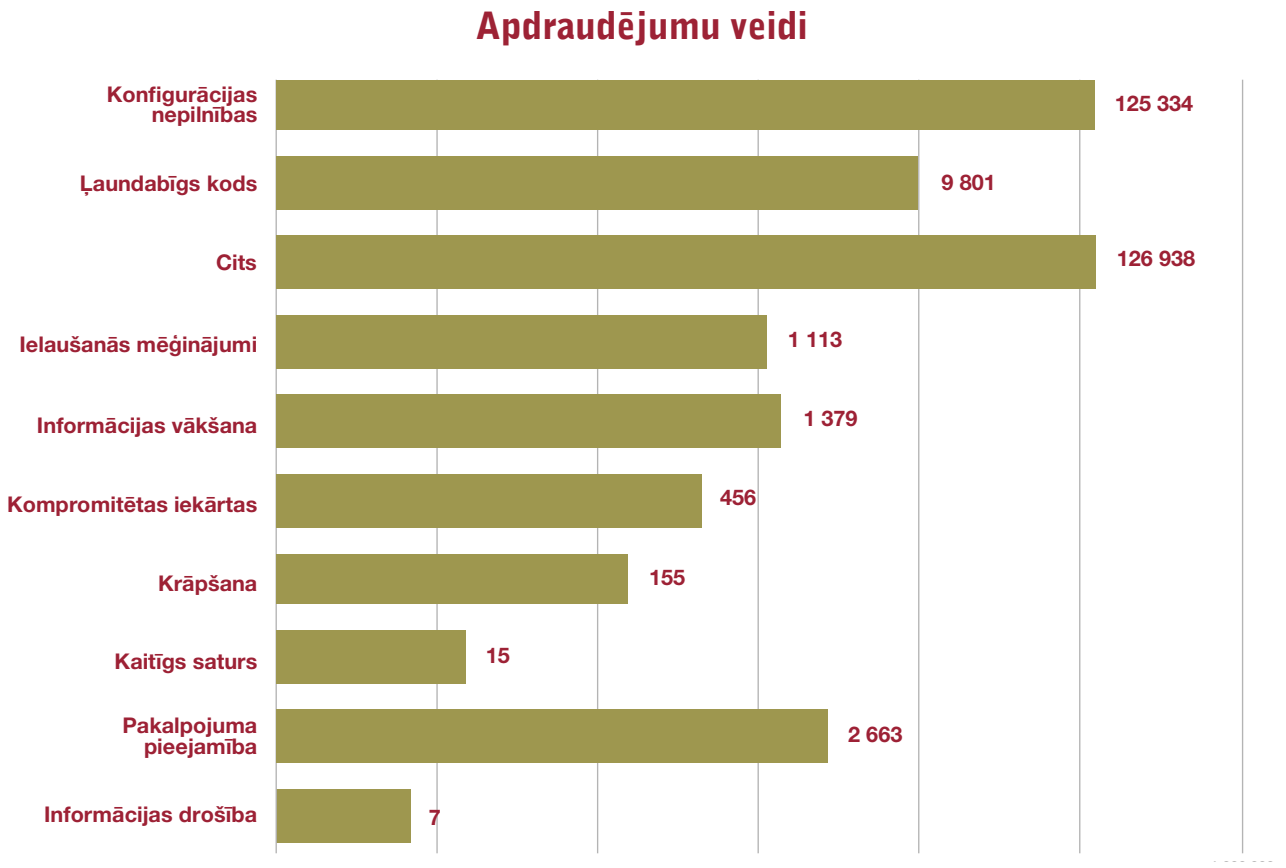
1. attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa mēnešiem 12 mēnešu griezumā.

Apdraudējumu sadalījums pa ceturkšņiem



2. attēls – CERT.LV reģistrētās apdraudētās IP adreses pa ceturkšņiem 2021. un 2022. gadā.

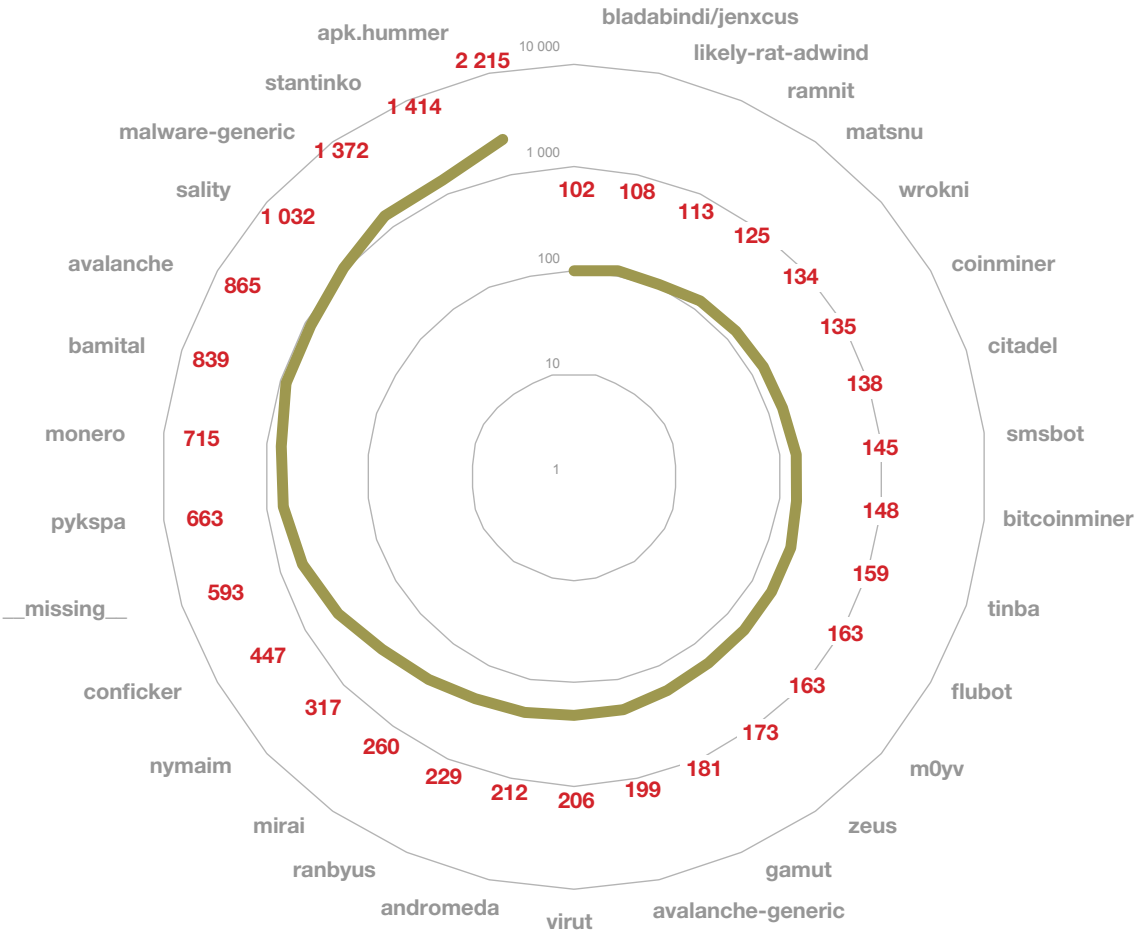
2022. gada 2. ceturksnī tika reģistrētas 260 617 unikālas apdraudētas IP adreses, kas ir par 122% vairāk nekā iepriekšējā ceturksnī un par 136% vairāk nekā šajā pašā periodā pirms gada. Kopējā apdraudēto IP adrešu apjoma pieaugums skaidrojams ar palielinājumu konfigurācijas nepilnību skaitā un pakalpojuma pieejamības incidentu apjomā.



3. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2022. gada 2. ceturksnī pa apdraudējumu veidiem.

Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (125 334 unikālas IP adreses) ar pieaugumu par 90% pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs kods (9801 unikāla IP adrese) ar pieaugumu par 10%, bet trešais – pakalpojuma pieejamība (2663 unikālas IP adreses) ar pieaugumu par 414%.

Unikālo IP adrešu skaits – ļaundabīgs kods



4. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2022. gada 2. ceturksnī ar apdraudējuma veidu – ļaundabīgs kods.

Konfigurāciju nepilnību pieaugums skaidrojams ar jaunām datu kategorijām (tādām kā *Accessible-ssl, Accessible-ssh, Accessible-smtp* u.c.), par kurām informāciju uzsākuši apkopot CERT.LV sadarbības partneri. Šīs kategorijas nenorāda uz tūlītēji bīstamām iekārtām, bet vērš uzmanību uz potenciālu apdraudējumu, kas var rasties, ja iekārtas pieejamība internetā ir nejauša, tā nav aizsargāta ar drošu paroli, vai šāda iekārta tiek aizmirsta un netiek pienācīgi atjaunināta.

Pakalpojuma pieejamības pieaugums demonstrē pārskata periodā novēroto piekļuves atteices (DDoS) uzbrukumu intensitāti, kas tika vērsta pret Latvijas IT infrastruktūru gan publiskajā, gan privātajā sektorā.

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

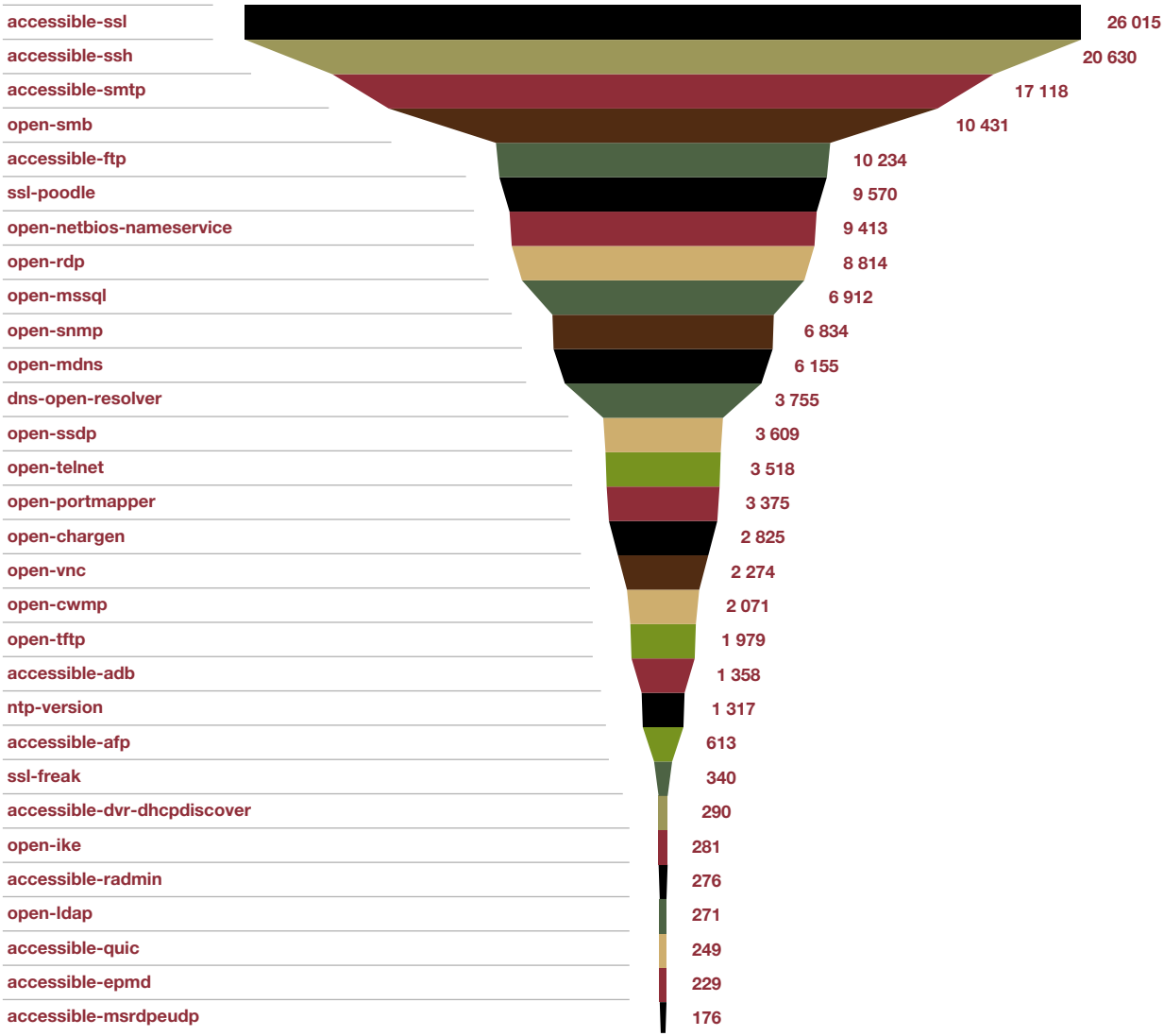
Otro vietu saglabā ļaunatūra *Stantinko*, kas paredzēta dažādu kriptovalūtu ieguvei, nesankcionēti izmantojot upura iekārtas resursus un potenciāli radot iekārtas pārslodzi, kā arī demonstrē lietotājam reklāmas, tādējādi nodrošinot reklāmu izvietotājiem peļņu.

Trešo vietu ieņem *Sality* – ļaunatūra, kas ievāc informāciju no inficētās iekārtas, kā arī nodrošina sānejas (*backdoors*) un mūķa (*exploit*) funkcionalitāti, kas ļauj uzbrucējiem piekļūt iekārtai un veikt tajā nesankcionētas darbības, tajā skaitā uzstādīt papildu ļaunatūru.

Pirmo vietu konfigurācijas nepilnību topā ieņem *Accessible-ssl*, kas, lai arī nenorāda uz viennozīmīgi bīstamiem serveriem, ietver informāciju par internetā pieejamiem SSL/TLS serveriem, kas noteiktos apstākļos var radīt apdraudējumu infrastruktūrai.

Otrajā vietā ierindojas *Accessible-ssh*, kas norāda uz internetā pieejamām iekārtām, kurās ir iespējots SSH protokols. Šis protokols tiek izmantots, galvenokārt, drošai komunikācijai nedrošā tīklā, piemēram, lai veiktu attālinātu autentifikāciju. Tas tiešā veidā nenorāda uz nepilnību, bet šim ir jāpievērš uzmanība, ja SSH šķiet nevietā vai tā versijas – neatbilstošas.

Unikālo IP adrešu skaits – konfigurācijas nepilnības



5. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2022. gada 2. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

Trešo vietu ieņem *Accessible-smtp*, kas, līdzīgi kā *Accessible-ssl*, nenorāda uz tūlītēji bīstamām iekārtām, taču vērš uzmanību uz internetā pieejamiem SMTP serveriem, kuri, iespējams, netīši padarīti publiski pieejami, kā arī atgādina par nepieciešamību pārliecināties, ka šiem serveriem ir uzstādīti visi pieejamie atjauninājumi.

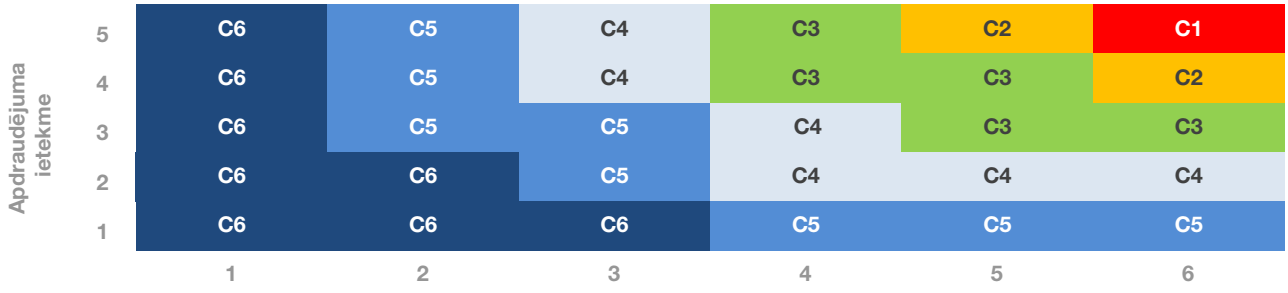
Pilnvērtīgākam kibersituācijas novērtējumam CERT.LV 2020. gadā ir uzsākusi *Apvienotās Karalistes Nacionālā kiberdrošības centra (NCSC)* izveidotās apdraudējumu matricas lietošanu. Matricā ievietotie apdraudējumi tiek grupēti pēc tā, cik nozīmīga ir skartā iestāde vai uzņēmums un/vai cik plašu sabiedrības 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 97% 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.

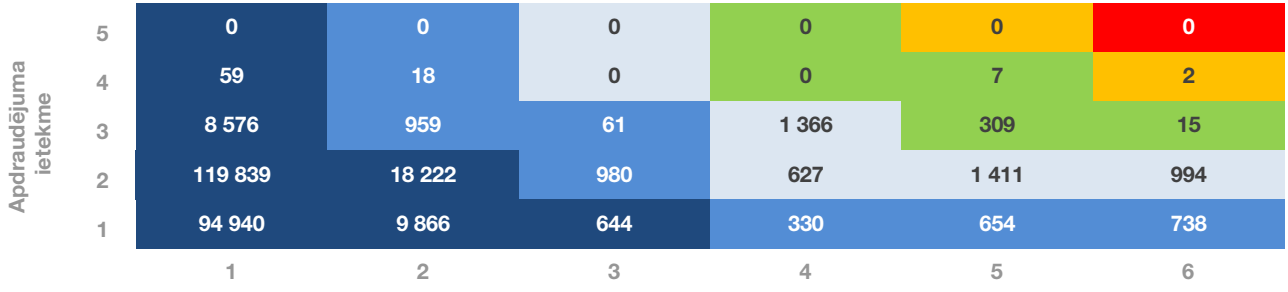
Nacionāla līmeņa apdraudējumi (C1) pārskata periodā nav reģistrēti, savukārt augstas nozīmes apdraudējumu kopā (C2) reģistrētas divas apdraudētas IP adreses, kas abas saistītas ar vienu incidentu – kādā uzņēmumā, kurš sniedz pakalpojumus plašai sabiedrībai, neatbilstošas

Apdraudējumu matrica



6. attēls – Apdraudējumu matricas sadalījums kategorijās.

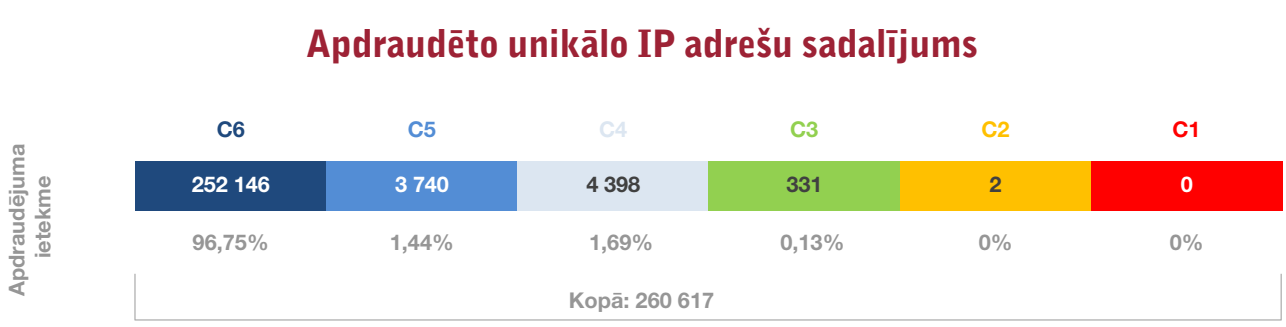
Apdraudēto unikālo IP adrešu izvietojums



7. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu izvietojums matricā 2022. gada 2. ceturksnī valsts un pašvaldību institūcijās.

konfigurācijas rezultātā publiski pieejama bija izstrādes vide (tostarp konfigurācijas faili) vienai no uzņēmuma datu apmaiņas sistēmām.

Nozīmīgi plašas ietekmes apdraudējumi (C3) veido 0,13% (331 unikāla apdraudēta IP adrese/gadījums) no visiem kategorizētajiem apdraudējumiem. 91% šo apdraudējumu veido pakalpojuma



8. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu sadalījums apdraudējumu kategorijās pēc apdraudējuma ietekmes (matrica) 2022. gada 2. ceturksnī.

pieejamības incidenti, savukārt 5% veido ļaundabīgs kods (*Android.Hummer, Avalanche, Monero* u.c.), bet pārējos 4% veido kompromitētas iekārtas un informācijas drošības apdraudējumi.

Lielākā daļa C4 līmeņa apdraudējumu (būtiski apdraudējumi ar vidēju ietekmi) jeb 61% bija konfigurācijas nepilnības (*Accessible-ssl*, *Open-mssql, Open-chargen,* u.c.), bet 35% pakalpojuma pieejamības (DDoS) incidenti, kas novēroti augstas un vidēji augstas prioritātes iestādēs – virknē valsts iestāžu, kā arī vairākās pašvaldībās.

Lai mazinātu kopējo apdraudēto IP adrešu skaitu valstī, 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 (pieejamas 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.

Šajā pārskata periodā krāpnieki galvenokārt centās iegūt iedzīvotāju finanšu līdzekļus, gan veicot krāpnieciskus telefona zvanus un uzdodoties par tiesībsargājošo iestāžu pārstāvjiem, gan viltojot banku un kurjerkompāniju (DPD) mājas lapas, kā arī piedāvājot viltus investīcijas. CERT.LV saņēmusi informāciju par vairākiem krāpnieku upuriem, kas cietuši finansiālus zaudējumus: gandrīz 2000 eiro krāpnieciskās investīcijās (3 incidenti), vairāk nekā 300 eiro krāpnieciskos pārdošanas sludinājumos (2 incidenti), gandrīz 5000 eiro viltus banku vietnē (1 incidents), vairāk nekā 32500 viltota rēķina rezultātā (1 incidents).

Tika saņemti ziņojumi par krāpnieciskiem e-pastiem, kuros krāpnieki izlikās par Citadele banku un draudēja pārtraukt norēķinu karšu darbību, ja e-pasta saņēmējs neapstiprinās papildu drošības prasības, sekojot e-pastā norādītajai saitei uz krāpniecisku vietni. Vietnē ievadītie bankas piekļuves dati nonāca krāpnieku rīcībā.

Iedzīvotāji saņēma arī krāpnieciskus telefona zvanus, kuros zvanītāji uzdevās par tiesībsargājošo iestāžu pārstāvjiem un apgalvoja, ka zvana saņēmēja vārdā tiek veiktas pretlikumīgas darbības ar kriptovalūtu un nepieciešama tūlītēja iesaiste darbību pārtraukšanai un kontu aizvēršanai. Uzbrucēju mērķis – iebiedējot iegūt personas un finanšu datus.

Lai piekļūtu iedzīvotāju finanšu līdzekļiem, krāpnieki izmantoja arī jaunu krāpšanas metodi – apmaksātas *Google* reklāmas viltotām banku tīmekļa vietnēm, tādējādi nodrošinot, ka viltus vietnes parādīsies kā pirmie meklēšanas rezultāti, meklējot konkrētu banku. Sākotnēji tika reklamētas galvenokārt viltotas *Luminor* bankas tīmekļa vietnes, bet vēlāk parādījās arī reklāmas ar *Citadele* un *Swedbank* vietņu viltojumiem. Saņemta informācija par vairākiem cietušajiem. Uzbrucēji reāllaikā pārtver un izmanto krāpnieciskajās vietnēs ievadītos lietotāju datus, lai piesavinātos upurim piederošos finanšu līdzekļus. CERT.LV aicināja sabiedrību būt piesardzīgiem un pirms datu ievades pievērst uzmanību tīmekļa vietnes adresei, vai tā atbilst īstajai bankas mājas lapai.

Tika saņemti atsevišķi ziņojumi par krāpnieciskiem e-pastiem, kuros sabiedrībā atpazīstamu personu vārdā vai norādot, ka pārstāv Ukrainas sadraudzības pilsētas, saņēmējus aicina veikt ziedojumus Ukrainai. CERT.LV aicināja neuzķerties un ziedojumu veikšanai izmantot labi zināmas un pārbaudītas organizācijas, informāciju meklējot oficiālos avotos, piemēram, vietnē: https://www.palidzibaukrainai.lv.

Iedzīvotāji ziņoja par krāpnieciskiem e-pastiem, kuros ļaundari izlikās par uzņēmumu *Latvijas Pasts*, un aicināja e-pasta saņēmējus apmaksāt muitas nodevas, lai saņemtu sūtījumu. E-pastos norādītās saites veda uz viltus vietnēm, kas paredzēta norēķinu karšu datu izkrāpšanai.

Krāpniecībām tika izmantots arī straumēšanas serviss *Netflix*. Krāpnieki, uzdodoties par *Netflix* atbalsta dienesta darbiniekiem, izsūtīja e-pastus ar brīdinājumiem latviešu valodā par it kā bloķētu pieeju platformai, jo nav norādīta derīga maksājumu informācija. Lai atjaunotu piekļuvi pakalpojumam, iedzīvotāji tika aicināti ievadīt maksājumu karšu datus krāpnieku norādītajā viltus vietnē. CERT.LV vērsa iedzīvotājus uzmanību uz nepieciešamību pārbaudīt tīmekļa vietnes adresi pirms datu ievades, kā arī uz iespēju papildu drošībai izmantot CERT.LV un NIC.LV izstrādāto DNS ugunsmūri, kurā CERT.LV regulāri un operatīvi ievieto saites no aktuālajām pikšķerēšanas kampaņām.

Tika saņemta informācija arī par jaunu krāpniecības veidu, kurā uzbrucēju mērķis ir nelieli uzņēmumi, kuriem varētu būt aktuāla papildu investoru un klientu piesaiste. Šiem uzņēmumiem tika zvanīts un piedāvāts iegādāties *kredītspējas sertifikātu*, kas padarītu uzņēmumu pievilcīgāku potenciālajiem sadarbības partneriem. Zvanītāju norādītajā tīmekļa vietnē bija aplūkojama informācija par uzņēmumiem, kas it kā jau šādu sertifikātu ir iegādājušies. Nākamajā dienā, mēģinot apmeklēt norādīto tīmekļa vietni vai atzvanīt uz attiecīgo telefona numuru, tika saņemts paziņojums, ka ne vietne, ne numurs neeksistē. CERT.LV aicināja būt piesardzīgiem un, saņemot šādus piedāvājumus, vērsties ar iesniegumu policijā, bet, ja izdarīts maksājums krāpniekiem, nekavējoties informēt par notikušo savu banku.

Kāda mācību iestāde piedzīvoja iejaukšanos biznesa sarakstē un cieta finansiālus zaudējumus vairāk nekā 32500 eiro apmērā, apmaksājot viltotu sadarbības partnera rēķinu. Iestādes pārstāvjiem, saņemot rēķinu ar mainītiem rekvizītiem un lūgumu veikt pārskaitījumu ar jaunajiem datiem, situācija likās aizdomīga, un sadarbības partneriem tika lūgts apstiprinājums, ka rekvizītu maiņa ir leģitīma. Sadarbības partneris neuzmanības vai kļūdas pēc sniedza apstiprinājumu, ka komunikācija ir uzticama un jaunie rekvizīti ir korekti, pēc kā tika veikts bankas pārskaitījums uz krāpniekiem piederošu bankas kontu. Iestādei tika rekomendēts vērsties ar iesniegumu policijā.

2.2. Pakalpojuma pieejamība

Pieaudzis pakalpojumu atteices (DDoS) uzbrukumu skaits pret dažādiem mērķiem Latvijā, uzbrukumu intensitātei būtiski palielinoties pēc 9. maija notikumiem Latvijā. Par uzbrukumu mērķiem kļuva valsts iestādes, mediji, finanšu institūcijas un privātais sektors. Uzbrukumi valsts iestādēm, un kritiskās infrastruktūras uzņēmumiem, sadarbojoties CERT.LV, LVRTC un SIA TET tika veiksmīgi atvairīti, bez būtiskiem traucējumiem sniegto pakalpojumu pieejamībai.

DDoS uzbrukumus veica vairākas Krievijas agresīvo režīmu atbalstošas kiberaktīvistu grupas. Tās ir veikušas uzbrukumus arī Igaunijas, Polijas, Čehijas un citu Eiropas valstu iestāžu un uzņēmumu tīmekļa vietnēm. Uzbrukumu mērķis bija padarīt tīmekļa vietnes un to nodrošinātos pakalpojumus

nepieejamus, taču uzbrukumi nebija tehnoloģiski sarežģīti, un iestādes ar adekvātiem IT resursiem neizjuta ietekmi uz pakalpojumu pieejamību.

Šie grupējumi neveica kvalitatīvu mērķu priekšizpēti, par ko liecināja dažādu iestāžu jaukšana grupējumu publiskotajos paziņojumos, kā arī uzbrukumi pret neaktuāliem mērķiem. Kopš 9. maija šo grupu uzmanība Latvijai bija nerimstoši liela un, atšķirībā no citām Eiropas valstīm, pret Latviju uzbrukumi tika organizēti katru dienu, taču Latvijas valsts un pašvaldību kritiskākajām sistēmām ir veikti atbilstoši priekšdarbi, lai šādi uzbrukumi nebūtu efektīvi.

Kaut arī lielāko daļu uzbrukumu izdevās veiksmīgi atvairīt, bija arī izņēmuma gadījumi, kuru efektu izjuta lielāka sabiedrības daļa. Vieni no redzamākajiem uzbrukumiem tika veikti pret ziedot.lv, inbox.lv, *Mobilly*, Pasažieru vilciena biļešu tirdzniecības vietni, LETA un NRA portālu, kā rezultātā šo organizāciju klientiem tika traucēta atsevišķu pakalpojumu saņemšana tiešsaistē.

Kādam uzņēmumam DDoS uzbrukuma rezultātā īslaicīgi tika traucēta tīmekļa vietnes darbība. Lai arī uzņēmums bija iegādājies DDoS aizsardzības pakalpojumu, nesakārtotu iekšējo procesu un nepārbaudītu procedūru rezultātā aizsardzība nenostrādāja korekti.

2.3. Ļaundabīgs kods

Turpinājās ļaunatūras izplatīšanas kampaņa platformā *E-klase*. Izmantojot *E-klase* pasta sūtījumā iekļautu saiti vai pielikumu, tika izplatīts *Gozi* vīruss, kas, nonākot datorā, uzbrucējiem nosūtīja datorā izmantotos lietotājvārdus un paroles, kā arī sniedza uzbrucējiem pilnu kontroli pār iekārtu. Uzbrukumu grūti identificējamu padarīja tas, ka ļaundabīgo sūtījumu upuri saņēma no pazīstamiem sūtītājiem, kuru datori bija inficēti, kā arī ziņojums bija tematiski atbilstošs un sagatavots labā latviešu valodā. CERT.LV sniedza atbalstu platformas *E-klase* uzturētājiem incidenta izmeklēšanā un rekomendācijas kiberdrošības stiprināšanā. *E-klase* veica ierobežojošus pasākumus identificēta ļaundabīgā satura izplatības apturēšanai, taču uzbrucēju aktivitātes raisa bažas, vai, uzsākoties jaunajam mācību gadam un aktivizējoties platformas izmantošanai, izdosies novērst jaunu ļaunatūras izplatīšanas kampaņu uzliesmojumus.

Maijā šifrējošo vīrusu uzbrukumos cietuši vairāki uzņēmumi un organizācijas Latvijā. To vidū arī kāds Latvijas muzejs, kuram uzbrukuma rezultātā tikusi sašifrēta darbstacija, uz kuras glabājās iekšējā biļešu kontroles sistēma. Tā kā muzejam nebija datu rezerves kopijas, tad nācās visu iekārtu instalēt no jauna. Cietušo vidū bija arī kāds starptautisks Latvijas tirdzniecības uzņēmums, kuram tika sašifrēti vairāk kā puse no visiem darbinieku datoriem. Abos gadījumos CERT.LV aicināja nemaksāt ļaundariem izpirkumu, jo šāda rīcība ne tikai negarantē datu atgūšanu, bet arī veicina jaunu ļaunatūru izstrādi.

2.4. Ielaušanās mēģinājumi

Pārskata periodā samazinājās pret Latvijas iestādēm un kritiskās infrastruktūras uzņēmumiem vērstu tīklu skenēšanas un ievainojamību meklēšanas uzbrukumu intensitāte, pieaugot DDoS uzbrukumu apjomam.

Pret kādu valsts iestādi tika veikts mērķēts uzbrukums, kurā 38 darbinieki saņēma e-pastu it kā Ukrainas Aizsardzības ministrijas vārdā ar aicinājumu sniegt papildu atbalstu Ukrainai, nodrošinot pielikumā pievienotajā sarakstā minēto. Pielikums saturēja vīrusu. Uzbrukums nav bijis sekmīgs, iestādē nav fiksētas aktivitātes, kas būtu saistītas ar ļaundabīgajiem domēniem.

Mērķētus uzbrukumus pikšķerēšanas e-pastu formā piedzīvoja arī citas valsts iestādes.

Ar augstu ticamību var pieņemt, ka tuvāko nedēļu vai mēnešu laikā var palielināties uzbrukumu intensitāte vai to ietekme, kā arī ir gaidāmi piegāžu ķēžu uzbrukumi. Potenciālie uzbruceju mērķi: iekšlietu sektors, ārlietu sektors, lēmumpieņēmēji, nevalstiskās organizācijas, pakalpojumu sniedzēji (primārie mērķi – šo uzņēmumu klienti valsts pārvaldē un kritiskajā infrastruktūrā), enerģētikas sektors, citi pamatpakalpojumu sniedzēji, nacionālie mediji. Mērķu plašais spektrs norāda uz centieniem panākt postošu efektu.

2.5. Kompromitētas iekārtas un datu noplūdes

Tika veikta kādas valsts iestādes tīmekļa resursa incidenta analīze, kuras rezultātā tika konstatēts, ka resursa kompromitēšana notikusi jau 2021. gada janvārī, izmantojot ievainojamību satura vadības sistēmā. Tika konstatēts, ka mērķa sistēma tikusi izstrādāta, ignorējot vispārpieņemtos labās prakses principus, kā arī ilgstoši uzturēta, neveicot atjauninājumus un ignorējot labo praksi. Analīzes rezultātā identificētās ievainojamības liecināja, ka sistēmai nav veiktas arī drošības pārbaudes jeb audits un ir ignorētas Ministru kabineta noteikumu Nr. 442 prasības. Mērķa sistēma uzskatāma par pilnībā kompromitētu un viss tās saturs un datu bāze par noplūdušu. CERT.LV sniedza rekomendācijas incidenta novēršanā un ietekmes mazināšanā. CERT.LV pieļauj, ka uzbrukumu sekmējis arī incidents uzņēmumā, kura IT pakalpojumus iestāde ir izmantojusi.

Tika konstatēta kāda programmatūras izstrādes uzņēmuma kompromitēšana, kas sniedz pakalpojumus, gan valsts iestādēm, gan uzņēmumiem. Uzbrucējs kompromitējis uzņēmuma iekšējo tīklu, iegūstot potenciālu piekļuvi sistēmām, klientu datiem, izstrādes vidēm. CERT.LV sniedz atbalstu incidenta analīzē un ietekmes mazināšanā.

Tika uzsākta izpēte kādā uzņēmumā, saņemot informāciju par iespējamiem kompromitēšanas indikatoriem. Izpētē tika konstatēts, ka no dažu darbinieku kontiem veiktas tiem netipiskas darbības uzņēmuma iekšējā tīklā. Turpinās incidenta analīze.

Tika pabeigta kādas valsts iestādes infrastruktūras analīze, kuras rezultātā sistēmā tika atklāta komerciāli motivēta ļaunatūra. Lai arī netika konstatētas citas uzbrucēju klātbūtnes pazīmes, atsevišķas infrastruktūrā pamanītas aizdomīgas darbības un tas, ka sistēmu uzturēšanā nav ievēroti labās prakses principi (tika lietotas nedrošas paroles, kā arī kompromitējot jebkuru internetā pieejamu iestādes sistēmu, uzbrucējs iegūst pilnu piekļuvi tīklam), ar augstu varbūtību ļauj pieņemt, ka uzbrucēji ir iekļuvuši infrastruktūrā. CERT.LV sniedza rekomendācijas drošības pasākumu uzlabošanai.

Veicot incidentu analīzi, nācās secināt, ka daudzviet attieksme pret kiberdrošības jautājumiem ir nolaidīga un paviršа gan publiskajā, gan privātajā sektorā, neskatoties uz iesaistīto uzņēmumu ilggadīgo pieredzi un tirgus pozīcijām.

Krieviju atbalstošie kiberaktīvistu grupējumi, cenšoties iebiedēt un pārliecināt sabiedrību, ka tikusi uzlauzta Valsts Prezidenta kancelejas tīmekļa vietne www.president.lv, lejupielādējuši kancelejas tīmekļa vietnē brīvi pieejamas datnes un publicējuši savos komunikāciju kanālos, apgalvojot, ka notikusi veiksmīga ielaušanās un datu noplūde. Katrs šāds gadījums un apgalvojums tika izmeklēts individuāli, taču neviens no šiem apgalvojumiem līdz šim nav izrādījies patiess.

2.6. Ievainojamības

Kādā valsts iestādē tika konstatēta brīvi pieejama atvērta platforma, kurā, izmantojot attālinātās piekļuves rīku RDP, varēja piekļūt jebkura darbinieka darbstacijai. Iestāde tika informēta, konfigurācijas nepilnība tika novērsta. Radusies situācija tikai skaidrota ar personāla pieļautu kļūdu. Tika veiktas rūpīgas pārbaudes, lai konstatētu, vai šī ievainojamība ir tikusi izmantota ļaunprātīgi. Līdzšinējā izpēte liecina, ka ļaunprātīga izmantošana nav notikusi.

CERT.LV tīmekļa vietnē tika publicēti brīdinājumi par kritiskām *Java* ievainojamībām *SpringCloud* (CVE-2022-22963) un *Spring4Shell* (CVE-2022-22965), kas ļāva uzbrucējiem veikt nesankcionētu attālināto koda izpildi, par 3 bīstamām programmatūras ievainojamībām (CVE-2021-3970, CVE-2021-3971 un CVE-2021-3972) *Lenovo* portatīvajos datoros, kā arī par uzbrukumos aktīvi izmantoto kritisko *Atlassian Confluence* ievainojamību (CVE-2022-26134), kas sniedza uzbrucējam iespēju veikt attālināto koda izpildi.

2.7. Atbildīga ievainojamību atklāšana

Tika saņemts ziņojums par ievainojamību *WordPress* funkcionalitātē, kas nodrošina satura publicēšanas iespējas, izmantojot trešo pušu rīkus, kādas valsts iestādes tīmekļa vietnē. CERT.LV informēja vietnes uzturētājus, kuri veica piekļuves ierobežošanu attiecīgajai funkcionalitātei.

Tika saņemts arī ziņojums par starpvietņu skriptēšanas (XSS) ievainojamību kādas mācību iestādes resursā. Ievainojamība sniedza uzbrucējam iespēju nodot serverim izpildei patvaļīgi izvēlētas komandas. Vietnes uzturētāji tika informēti, ievainojamība tika novērsta.

Informācija par jaunatklātiem apdraudējumiem un ievainojamībām tiek publicēta arī CERT.LV tīmekļa vietnē un sociālo tīklu *Twitter* (@certlv) un *Facebook* (@cert.lv) kontos. Tā pat arī Mattermost saziņas platformā notiek regulāra informācijas apmaiņa starp CERT.LV, atbildīgajiem par IT drošību un citiem kiberdrošības kopienas locekļiem.

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

Šogad Eiropā Digitālās nedēļas pasākumi norisinājās vesela mēneša garumā laika posmā no 14. marta līdz 14.aprīlim. 5. aprīlī CERT.LV piedalījās vienā no Ventspils digitālā centra Digitālās nedēļas pasākumiem, kurā iepazīstināja skatītājus ar drošiem paroļu veidošanas un uzglabāšanas principiem, kā arī aplūkoja citus ar paroļu drošību saistītus jautājumus.

5. aprīlī CERT.LV četriem zinātkāriem jauniešiem Ēnu dienas 2022 ietvaros sniedza iespēju iepazīties ar institūcijas ikdienas darbību un CERT.LV eksperta vadībā iejusties kiberdrošības

speciālista lomā. Ēnu dienas mērķis ir iepazīstināt skolēnus ar dažādu profesiju un nozaru prasībām, lai palīdzētu jauniešiem izvēlēties profesiju un atbilstoši sagatavotos darba tirgum.

22. aprīlī CERT.LV piedalījās Latvijas Interneta asociācijas (LIA) biedru kopsapulcē, kurā elektronisko sakaru uzņēmumiem sniedza prezentāciju par kiberdrošības izaicinājumiem pastāvošajos ģeopolitiskajos apstākļos.

26.aprīlī dalība ESET rīkotajā DELFI tiešraides diskusijā par *Bezprecedenta laiki kiberdrošībā kara laikā*, analizējot pret Ukrainu vērstos kiberapdraudējumus un iespējamos scenārijus Latvijas kibernoturības uzlabošanai.

28. aprīlī CERT.LV piedalījās pirmajā Drošības profesionāļu asociācijas konferencē *Latvijas drošības konference 2022*, kurā iepazīstināja klātesošos ar aktuālajiem kiberdrošības apdraudējumiem un kiberdrošības situāciju Latvijā (https://www.facebook.com/dpalatvia/videos/320361886899563).

13. maijā CERT.LV vadīja semināru Latvijas iedzīvotājiem par paroļu drošību. Semināru organizēja *Google* sadarbībā ar Ekonomikas ministriju, LIAA un citiem partneriem programmas *Izaugsme ar Google* ietvaros, kuras mērķis ir veicināt mūsdienīgu prasmju apgūšanu biznesa attīstībai digitālajā vidē.

25. maijā CERT.LV piedalījās vienā no *Industrijas dienas NBS 2022* plenārsesijām, kurā kopā ar A. Pabriku, E. Egli, NBS Apvienotā štāba priekšnieka vietnieku atbalsta jautājumos pulkvedi Kasparu Zdanovski un *Brasa Defence Systems* pārstāvi Kristiānu Brēdermani diskutēja par drošības un aizsardzības industriju noturību (https://www.facebook.com/watch/live/?ref=watch_permalink&v=988343391853576).

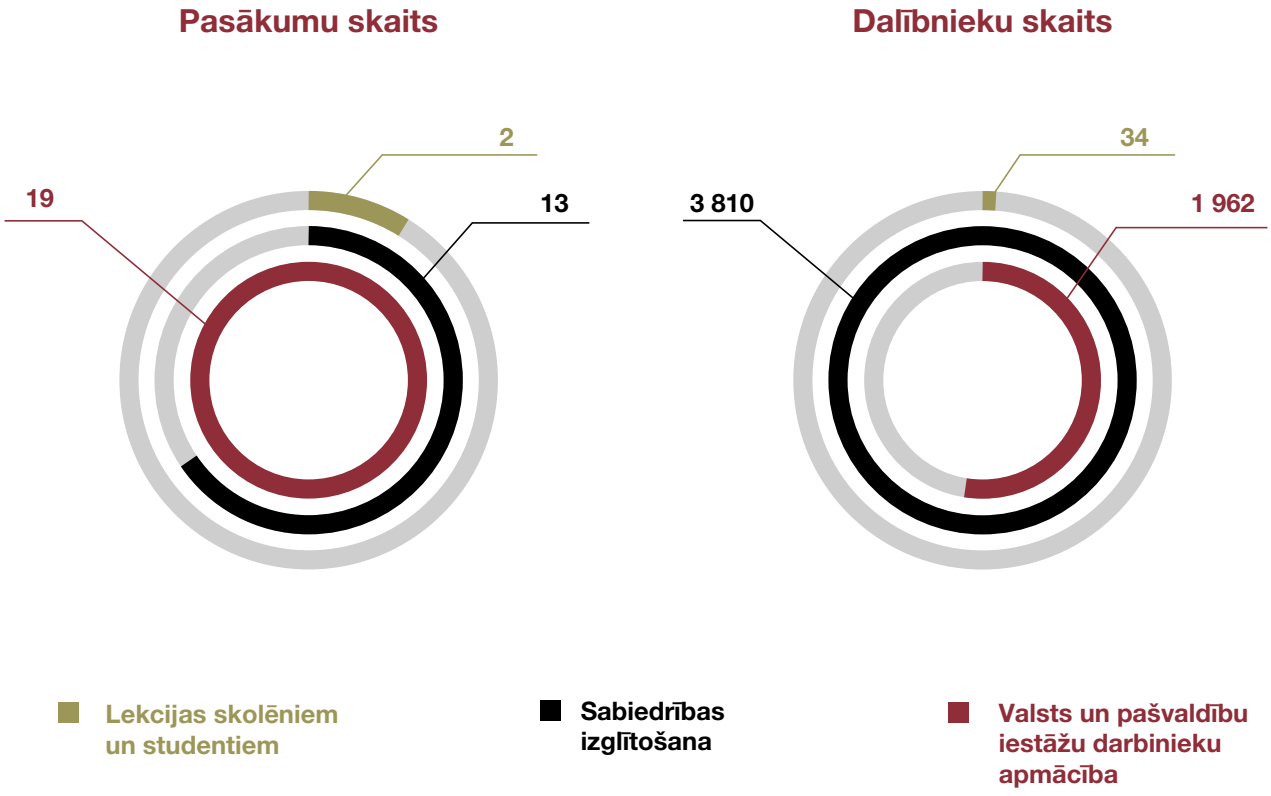
6. jūnijā CERT.LV sniedza prezentāciju Banku augstskolas un RISEBA organizētajā 15. ikgadējā zinātniskajā Baltijas biznesa vadības konferencē *Building Strategic Resilience in times of Uncertainty* par aktuālo situāciju kibertelpā.

CERT.LV iesaistījās *Mastercard* un Finanšu nozares asociācijas (FNA) organizētās kampaņas #viedpircējs realizēšanā, gan piedaloties diskusijā par telefonkrāpniekiem, gan sniedzot atbalstu

informatīvu materiālu sagatavošanā. Kampaņas mērķis bija mudināt iedzīvotājus un uzņēmējus aktīvi izmantot e-komercijas risinājumus un karšu norēķinus, vienlaikus veicinot zināšanas par digitālās drošības un ilgtspējas jautājumiem.

Pārskata periodā CERT.LV par IT drošību izglītoja 5806 cilvēku, iesaistoties 34 izglītojošos pasākumos.

Izglītojošo pasākumu un apmācīto cilvēku skaits



9. attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2022. gada 2. ceturksnī

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

Sadarbības tikšanās, konsultācijas un prezentācijas:

- Aprīļa sākumā CERT.LV pārstāvis piedalījās LIKTA diskusijā par atvērtā koda izmantošanu valsts pārvaldē. CERT.LV norādīja uz nepieciešamību pilnveidot valsts iestāžu personāla zināšanas par atvērto kodu un tā izmantošanu, pirms izvirzīt to kā obligātu nosacījumu valsts līmeņa IT sistēmu izstrādei un iekļaut iepirkumu prasībās. Rekomendējama arī kopīgu vadlīniju izstrāde.
- CERT.LV tikās ar Aizsardzības ministriju un LVRTC, lai pārrunātu jauno likumprojektu, kas tiks izstrādāts, lai pielāgotu Latvijas likumdošanu NIS2 direktīvas prasībām, tostarp definētu Aizsardzības ministrijas un CERT.LV tiesības un pienākumus Nacionālā kiberdrošības centra kontekstā. Tiek paredzēts, ka tas aizstās Informācijas tehnoloģiju drošības likumu.
- Aizsardzības ministrijai tika iesniegti komentāri par Nacionālā kiberdrošības centra ziņojuma protokollēmumu.
- CERT.LV turpināja projekta par valkājamo ierīču drošību norises vadību.
- Turpinājās koordinētas ievainojamību atklāšanas ziņojumu reģistrēšanas platformas izstrāde, kas tika uzsākta, balstoties uz Ministru kabineta apstiprināto Aizsardzības ministrijas izstrādāto informatīvo ziņojumu, kas paredz valsts pārvaldē ieviest vienotu procesu, kādā ikviens iedzīvotājs var ziņot par ievainojamībām valsts un pašvaldību uzturētās informācijas sistēmās. CERT.LV nodrošina platformas izstrādi, kā arī procesa aprakstu un ziņošanas vadlīniju sagatavošanu. Ņemot vērā aktuālo situāciju kibertelpā un incidentu daudzumu, platformas izstrādes process notiek lēnāk nekā plānots.

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 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. Pārskata periodā CERT.LV pārstāve Madara Krutova darbojas kā šīs darba grupas līdzpriekšsēdētāja.
  - *Maturity* darba grupā, kura rūpējas par ES dalībvalstu CSIRT komandu brieduma līmeņa paaugstināšanu.
  - *TOR Review* darba grupā, kas pārskata CERTu 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.
- Turpinājās darbs FIRST darba grupas *CSIRT Services Framework* darbā, lai izstrādātu vienotu ietvaru CERT komandu dalībnieku lomām, kompetencēm un prasmēm. Jūnijā darba grupas izstrādātais dokuments tika nodots apspriešanai plašākai kiberdrošības ekspertu kopienai.
- Turpinājās aktīva dalība enerģētikas informācijas apmaiņas un sadarbības grupā *Energy ISAC Camelot*, lai veicinātu informācijas apmaiņu un sekmētu enerģētikas sektora kiberdrošību.
- Dalība EU *CyberNet* projektā kā vienam no partneriem un piedalīšanās ikmēneša sanāksmēs. Projekta mērķis ir stiprināt kiberdrošības ekspertīzi un attīstīt to ne tikai

Eiropas Savienībā, bet arī ārpus tās robežām (www.eucybernet.eu). Dalība projektā sniedz iespēju CERT.LV ekspertiem iesaistīties dažādos projektos, stiprināt savas zināšanas un kapacitāti.

- Dalība ENISA Eiropas kiberdrošības indeksa (*EU Cybersecurity index*) darba grupā, kurā tiek izstrādāta kiberdrošības indeksa vērtības aprēķina metodoloģija dalībvalstu kiberdrošības novērtēšanai.
- Dalība darba grupā *Task Force Guidelines on Coordinated Vulnerability Disclosure Policies*, kurā ENISA plāno izveidot koordinētas ievainojamību atklāšanas politikas vadlīnijas. Darba grupā tika pārrunāts dokumentā iekļaujamais saturs. Paredzēts, ka notiks ikmēneša sanāksmes, kurās ES dalībvalstu speciālisti izskatīs un komentēs ENISA sagatavotos materiālus.
- Dalība Igaunijas e-lietu pārvaldības aģentūras (eGA) vadītajā *ES Balkānu kiberspēju attīstības projektā*. 14.-15. jūnijā CERT.LV pārstāvis piedalījās *Western Balkan Digital Security Forum* semināra paneļdiskusijā *Digitalisation & Cybersecurity – Two Sides of the Same Coin*.
- 27.-28. aprīlī CERT.LV pārstāvis piedalījās ENISA un CERTu tīkla rīkotajā seminārā par iespējām un veidiem, kā dalībvalstu CERTi nodrošinās NIS2 direktīvā iekļauto prasību izpildi attiecībā uz CERT iesaisti koordinētas ievainojamības atklāšanas procesā. Seminārā tika pārrunātas idejas un prasības koordinētas ievainojamību atklāšanas politikas vadlīniju izveidošanai, kā arī iecere veidot ES ievainojamību reģistru.
- 10.-11. maijā CERT.LV pārstāvis piedalījās TF-CSIRT 66.sanāksmē, kas notika Amsterdamā, Nīderlandē, un uzstājās ar prezentāciju par CERT.LV aktualitātēm, tajā skaitā par notikumiem kibertelpā kara kontekstā, DNS ugunsmūra plašāku izmantošanu, NCSC-UK matricas pieejas izmantošanu statistiku veidošanā un koordinētas ievainojamību atklāšanas programmas izveidi.
- 16.-17. maijā CERT.LV pārstāvji piedalījās kārtējā NIS direktīvas CERTu tīkla sanāksmē, kas notika Parīzē, Francijā. CERT.LV uzstājās ar prezentāciju par aktuālajiem

notikumiem kibertelpā ģeopolitiskā konflikta laikā, tajā skaitā par mērķētiem uzbrukumiem Latvijas valsts iestādēm un kritiskajai infrastruktūrai.

- 18. maijā CERT.LV piedalījās Vācijas-Baltijas Tirdzniecības kameras organizētā paneļdiskusijā *Challenges of IT- and Cyber security with participation of experts from Estonia, Latvia, Lithuania and TeleTrusT from Germany*. Diskusija notika projekta *Civilā aizsardzība un kiberdrošība Baltijas valstīs* rīkotās konferences *Innovative IT security technologies and services from Germany* ietvaros.
- No 31. maija līdz 3. jūnijam dalība NATO CCDCoE organizētajā konferencē *CyCon* un tehniskā paneļa par virtuālajām sistēmām un kiberdrošību vadīšana.
- 8.-9. jūnijā dalība ENISA rīkotajās mācībās *Cyber Europe*, lai piedalītos scenārija izspēlē, kas saistīts ar krīzi veselības sektorā. Mācību laikā tika pilnveidoti gan dažādi tehniskie, gan stratēģiski operacionālie aspekti.
- No 25. jūnija līdz 1. jūlijam CERT.LV pārstāvji piedalījās FIRST konferencē, kas notika Dublinā, Īrijā. CERT.LV pārstāvis konferences laikā piedalījās vairākās FIRST *Membership Committee* sanāksmēs, lai apspriestu turpmākos noteikumus biedru uzņemšanā un piesaistīšanā, kā arī SIM3 modeļa izmantošanas pirmā gada rezultātus.
- Pārskata periodā CERT.LV pārstāvji ir piedalījušies vairākās intervijās ar ENISA vai tās apakškontraktoriem par dažādām tēmām – CERTu un likumdevēju sadarbība, koordinētas ievainojamību atklāšanas programmas īstenošana, NIS direktīvas ieviešana un aktivitātes CERTu tīklā.

Sadarbība konkrētu incidentu risināšanā aplūkota pārskata 2. punktā.

6. Projekta Joint Threat Analysis Network īstenošana

Turpinājās 2021. gada 1. jūlijā CERT.LV uzsāktā *2020 CEF Telecom Call – Cybersecurity* uzsaukumā apstiprinātā projekta *Joint Threat Analysis Network* (turpmāk – JTAN projekts), līguma ar Eiropas Komisiju Nr. INEA/CEF/ICT/A2020/2373165, īstenošana.

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 apdraudējumu 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.

2022. gada 2. ceturksnī CERT.LV turpināja darbu pie *Grafoskopa* attīstīšanas un pilnveidošanas, ņemot vērā citu projekta partneru ieteikumus un pieredzi *Grafoskopa* izmantošanā. Pārskata periodā CERT.LV piedalījās attālinātās JTAN projekta sanāksmēs, kurās projekta partneri prezentēja savus projekta uzdevumus un sasniegumus. Darbs pie JTAN projekta iepirkuma ir iesaldēts resursu trūkuma dēļ, ņemot vērā globālo ģeopolitisko situāciju un ar to saistītos incidentus Latvijas kibertelpā.

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 elastīgu filtrus, kas atvieglo liela apjoma datu analīzi.

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

7. Projekta Cyber Exchange īstenošana

Noslēdzās 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 projekta ietvaros CERT.LV piedalījās tehniskajā vizītē Heraklionā, Grieķijā, kur satikās ar projekta partneri FORTH, lai demonstrētu Grafoskopa rīka tehniskās iespējas un apspriestu iespējamos Grafoskopa papildinājumus. Vizītes laikā tika apspriesti arī citi sadarbības jautājumi.

2022. gada jūnijā Spiltā, Horvātijā, notika *Cyber Exchance* projekta noslēguma sanāksme un teorētiskās (*table top*) mācības, kurās piedalījās divi CERT.LV pārstāvji. Mācību laikā tika izspēlēts iespējams pārrobežu incidents, kas skar enerģētikas sektoru un kura laikā jāiesista vairāku valstu atbildīgās iestādes. Tika apspriests arī *Cyber Exchange* projekts kopumā, tajā paveiktais un galvenie secinājumi.

Projekts noslēdzās 2022. gada 30. jūnijā, turpmākajos mēnešos tiks gatavoti projekta noslēguma pārskati.

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.

  DNS mūra darbības 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, maksājumu karšu datu zādzībām, viltus kurjerkompāniju tīmekļa vietņu apmeklējuma, kā arī tika liegts inficētām iekārtām sazināties ar vīrusu kontroles serveriem.

  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.

- Lai aktualizētu kiberdrošības jautājumus plašākā sabiedrībā un veicinātu CERT.LV atpazīstamību, CERT.LV preču zīme tika pieteikta konkursam *Gada preču zīme 2021*. Konkursa dalībniekus vērtēja gan sabiedrība, gan arī kompetenta žūrija. CERT.LV saņēma simpātiju balvas gan no Patentu valdes, gan no Latvijas Dizaineru savienības.
- 2. aprīlī tikšanās ar Latvijas Universitātes pārstāvi par iespējamo CERT.LV atbalstu kiberaizsardzības kursa izveidei, kas tiktu veidots kā daļa no civilās aizsardzības kursa. CERT.LV programmas izstrādē tiks iesaistīts konsultatīvā kapacitātē.
- 25. aprīlī CERT.LV kiberdrošības eksperts Bernhards Blumbergs saņēma NBS Zemessardzes komandiera apbalvojumu par ilggadēju ieguldījumu Zemessardzes kiberspēju attīstībā, prestiža celšanā un mācību organizēšanā.

- 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 vērtēja LVRTC iesniegtās izmaiņas sertifikātu pārizdošanas procesam eID kartē, kā arī pēc attiecīgo iestāžu lūguma veica Fizisko personu elektroniskās identifikācijas likumā noteikto auditēt tiesīgo ekspertu izmaiņas.

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 01.04.2022. līdz 30.06.2022. ir saņēmusi un izvērtējusi 1500 ziņojumus. No tiem 980 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 10 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 15 ziņojumos konstatēta personas goda un cieņas aizskaršana, 117 ziņojumi saņemti par naida runu un 2 ziņojumi par vardarbību atainojošiem materiāliem. Par finanšu krāpšanas mēģinājumiem internetā saņemti 65 ziņojumi, 258 ziņojumu saturs nav bijis pretlikumīgs, 53 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 308 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 50 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 980 ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem 959 ziņojumi ir dzēsti no publiskas aprites un 21 ziņojumu saturs atrodas dzēšanas procesā sadarbībā ar Valsts policiju un interneta pakalpojumu sniedzējiem.

2022. gada 20. jūlijā.

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