Latvijas universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

2023 C2

Publiskais pārskats par CERT.LV uzdevumu izpildi

2023. gada 2. ceturksnis (01.04.2023. – 30.06.2023.)

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

Lai arī kiberapdraudējumu līmenis Latvijas kibertelpā joprojām ir augsts, situācija vērtējama kā stabila.

Visa pārskata perioda garumā bija vērojami periodiski intensīvi Krievijas agresiju atbalstošu haktīvistu veikti piekļuves lieguma jeb DDoS uzbrukumi gan enerģētikas un transporta nozarēm, gan virknei valsts iestāžu resursu, taču lielākoties tie neradīja nekādu ietekmi uz mērķētajiem resursiem vai arī ietekme bija neliela.

31. maijā, pēc jaunā Latvijas Valsts prezidenta Edgara Rinkēviča ievēlēšanas amatā, Saeimas resursi piedzīvoja pastiprinātus DDoS uzbrukumus, taču tie neradīja ietekmi uz resursu darbību. Savukārt 23. jūnija vakarā nekādas anomālijas, kas būtu saistāmas ar notikumiem Krievijā, Latvijas kibertelpā netika novērotas. Arī XXVII *Vispārējio latviešu Dziesmu* un XVII *Deju svētku* kontekstā netika novēroti DDoS uzbrukumi un svētku periods noritēja mierīgi.

Pārskata periodā tika pabeigtas ievainojamību pārbaudes un draudu medību operācijas vairākās Latvijas IKT sistēmās. Šajās sistēmās netika konstatēti būtiski trūkumi vai apdraudējumi. Virknē IKT sistēmu pārbaudes turpinās.

Pārskata periodā tika reģistrētas 335 742 unikālas apdraudētas IP adreses, kas ir par 8% mazāk nekā iepriekšējā ceturksnī un par 29% vairāk nekā šajā pašā periodā pirms gada. Izplatītākie apdraudējumi:

- konfigurācijas nepilnības (76 092 unikālas IP adreses) ar kritumu par 4% pret iepriekšējo periodu;
- ļaundabīgs kods (6982 unikālas IP adreses) ar kritumu par 37%;
- pakalpojuma pieejamība (891 unikāla IP adrese) ar kritumu par 11%.

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. Pārskata perioda laikā lietotāji tika pasargāti **50 480** reizes.

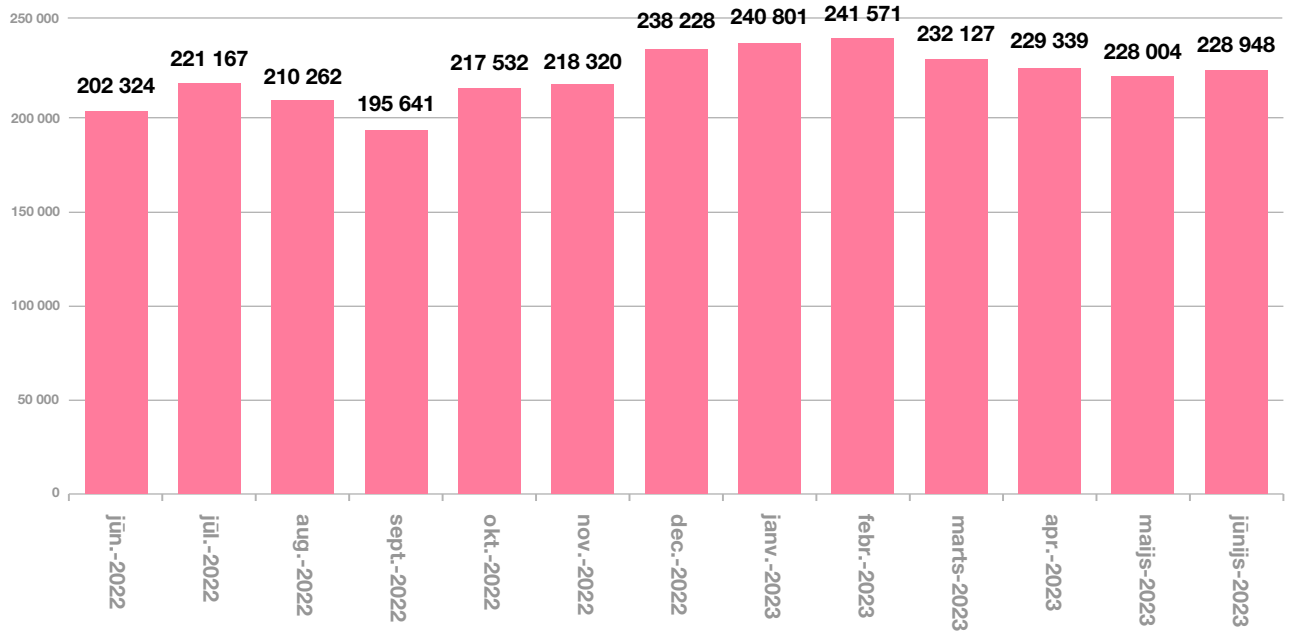
Notiek aktīvs darbs pie starptautiskās kiberdrošības konferences organizēšanas, kura norisināsies 2023. gada 4.-5.oktobrī.

Pārskata periodā CERT.LV par IT drošību izglītoja 4370 cilvēkus, iesaistoties 48 izglītojošos pasākumos.

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.

Apdraudējumu sadalījums pa mēnešiem

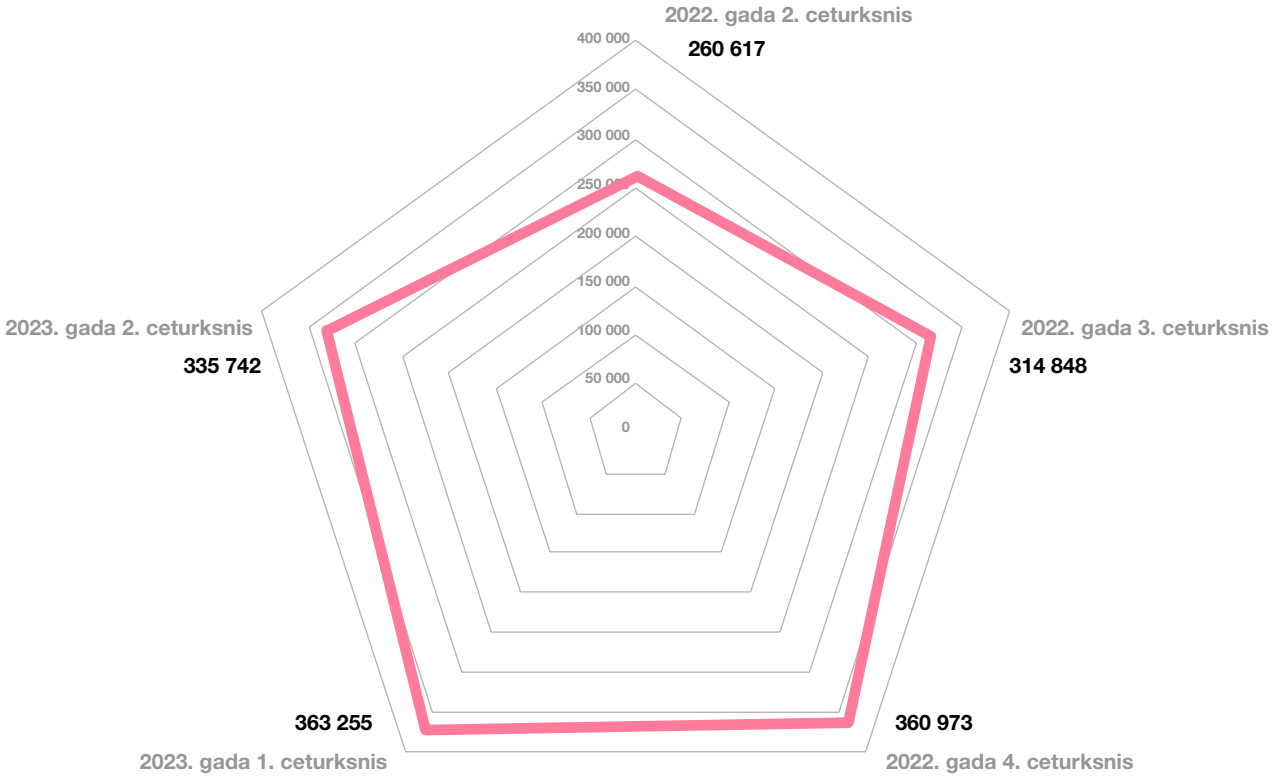


1. attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa mēnešiem 12 mēnešu griezumā.

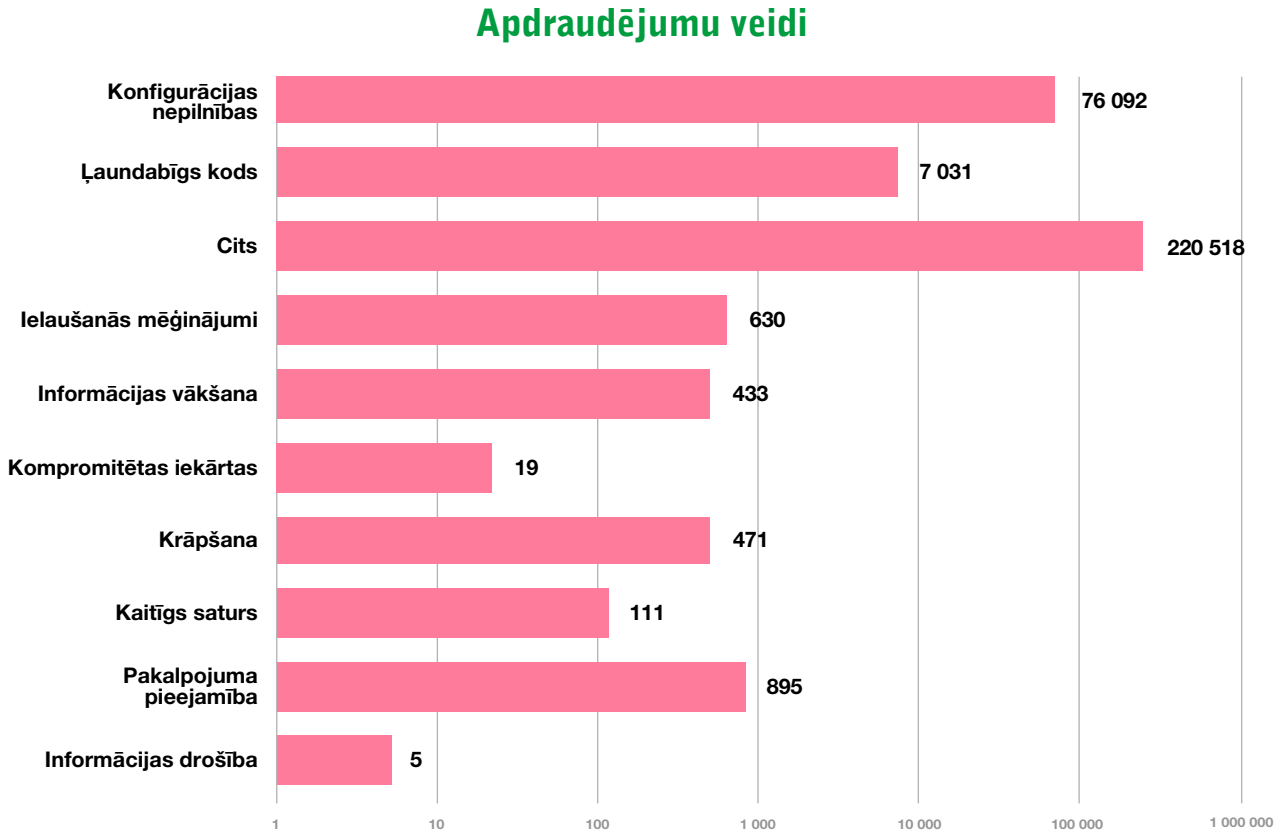
2023. gada 2. ceturksnī tika reģistrētas 335 742 unikālas apdraudētas IP adreses, kas ir par 8% mazāk nekā iepriekšējā ceturksnī, bet par 29% vairāk nekā šajā pašā periodā pirms gada. Kopš pagājušā gada vidus apdraudējumu līmenis Latvijas kibertelpā ir būtiski audzis. To ietekmējusi karadarbība Ukrainā un Krieviju atbalstošu haktīvistu, kā arī valsts sponsorētu grupējumu darbības. Pārskata periodā apdraudējumu līmenis bija stabils.

Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (76 092 unikālas IP adreses) ar kritumu par 4% pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs kods (6982 unikālas IP adreses) ar kritumu par 37%, bet trešais – pakalpojuma pieejamība (891 unikāla IP adrese) ar kritumu par 11%. Būtiskais kritums ļaunatūras apjomā skaidrojams ar starptautisku tiesībsargājošo

Apdraudējumu sadalījums pa ceturkšņiem



2. attēls – CERT.LV reģistrētās apdraudētās IP adreses pa ceturkšņiem 2022. un 2023. gadā.

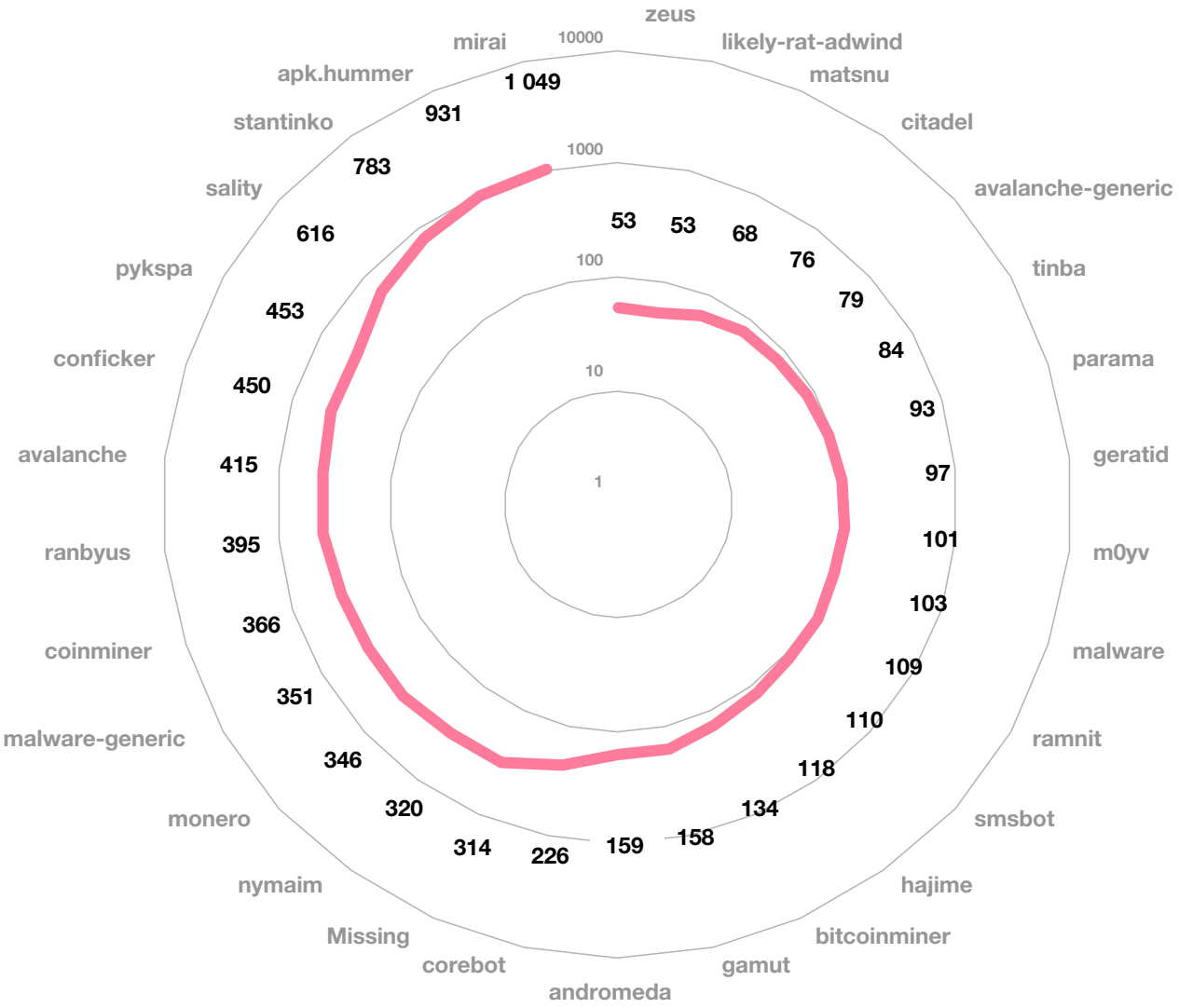


3. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2023. gada 2. ceturksnī pa apdraudējumu veidiem.

iestāžu operāciju, kuras rezultātā aprīļa sākumā tika aizvērta tiešsaistes tirdzniecības vietne *Genesis Market*, kas bija viena no vadošajām kompromitētu iekārtu piekļuves informācijas tirdzniecībā. Dažādu ļaunatūru izplatītāji izmantoja šos piekļuves datus, lai inficētu kompromitētās iekārtas.

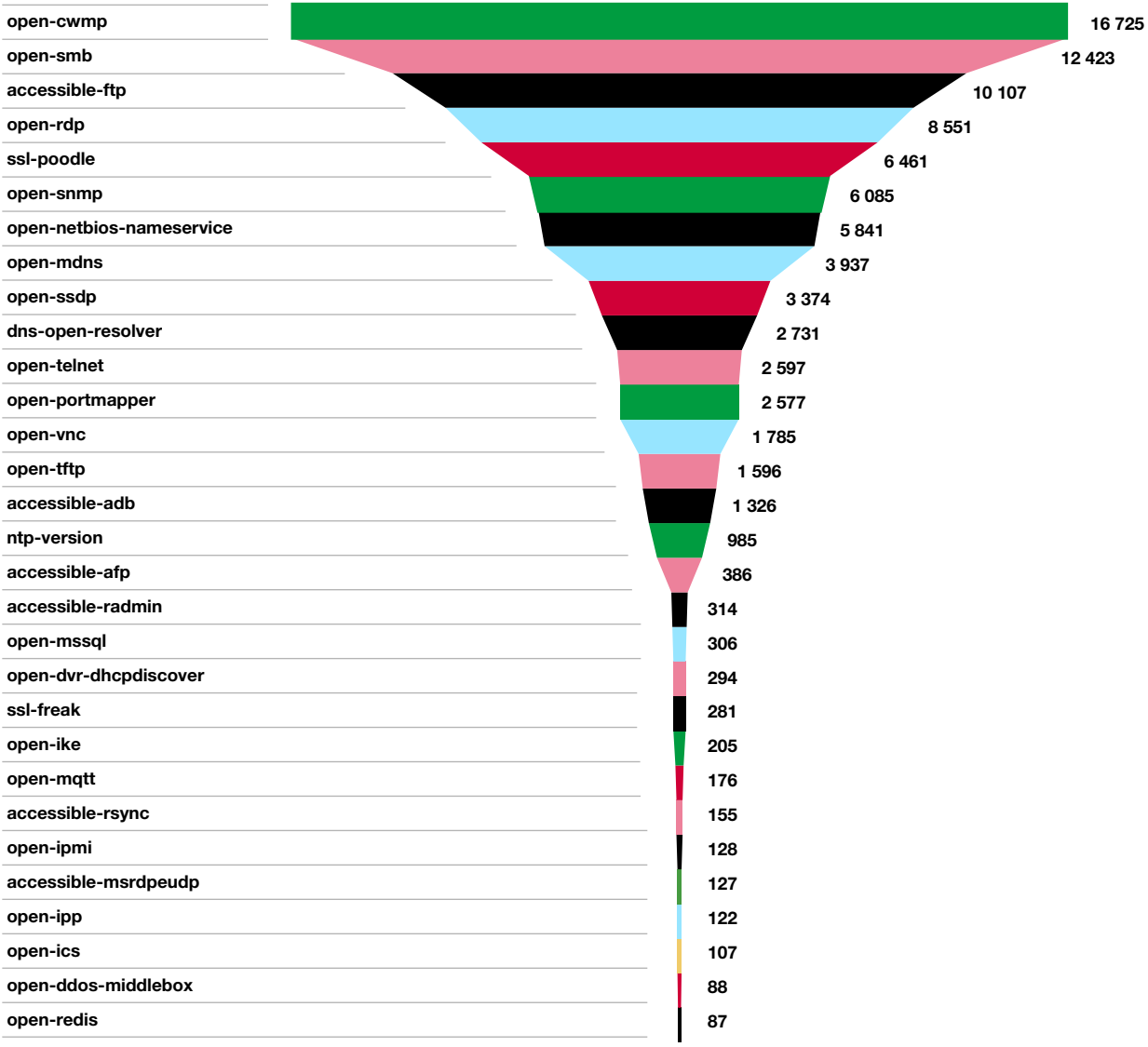
Ļaunatūras topa pirmo vietu ieņem ļaunatūra *Mirai*, kas inficē un iekļauj robotu tīklos jeb *botnetos* lietu interneta (IoT) iekārtas, lai izmantotu tās tālākiem uzbrukumiem un citām pretlikumīgām

Unikālo IP adrešu skaits – ļaundabīgs kods



4. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2023. gada 2. ceturksnī ar apdraudējuma veidu – ļaundabīgs kods.

Unikālo IP adrešu skaits – konfigurācijas nepilnības



5. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2023. gada 2. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

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.

Otrajā vietā ierindojas ļaunatūra *Apk.hummer*, kas iekārtās ar *Android* operētājsistēmu (planšetdatoros un viedtālruņos) demonstrē uznirstošas (*pop-up*) reklāmas un patstāvīgi lejupielādē dažādas lietotnes.

Trešajā vietā ir 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.

Konfigurācijas nepilnību tops šajā ceturksnī paliek nemainīgs. Pirmo vietu joprojām ieņem *Open-cwmp*. CWMP ir pārvaldības protokols, kas tiek izmantots, lai nodrošinātu individuālu iekārtu, piemēram, maršrutētāju vai VoIP telefonu, pieslēgšanos pie telekomunikāciju pakalpojumu sniedzēja nodrošinātā tīkla (interneta). Lai šim pārvaldības rīkam novērstu neautorizētas piekļuves riskus, tiek rekomendēts ierobežot piekļuves tiesības, piemēram, izmantojot VPN.

Otro vietu saglabā *Open-smb*. Ievainojamība norāda, ka konkrētajām iekārtām uz publisko internetu ir atvērts ports, kuru izmanto SMB protokols, kas paredzēts, lai piekļūtu datnēm un iekārtām iekšējā tīklā. Kompromitējot SMB protokolu, uzbrucēji iegūtu iespēju piekļūt iekšējā tīkla iekārtām un inficēt tās, piemēram, ar izspiedējvīrusu.

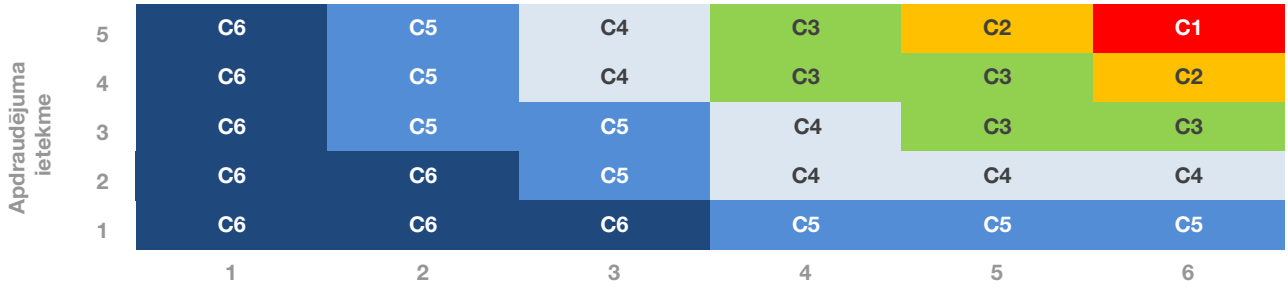
Trešajā vietā ierindojas *Accessible-FTP*. FTP datu pārraides protokols nenodrošina pārraidāmo datu šifrēšanu, ja vien netiek izmatota papildu aizsardzība TLS vai SSL protokola formā (attiecīgi FTPS). Šī konfigurācijas nepilnība pakļauj noplūdes riskam sensitīvu informāciju un piekļuves datus.

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.

Apdraudējumu matrica

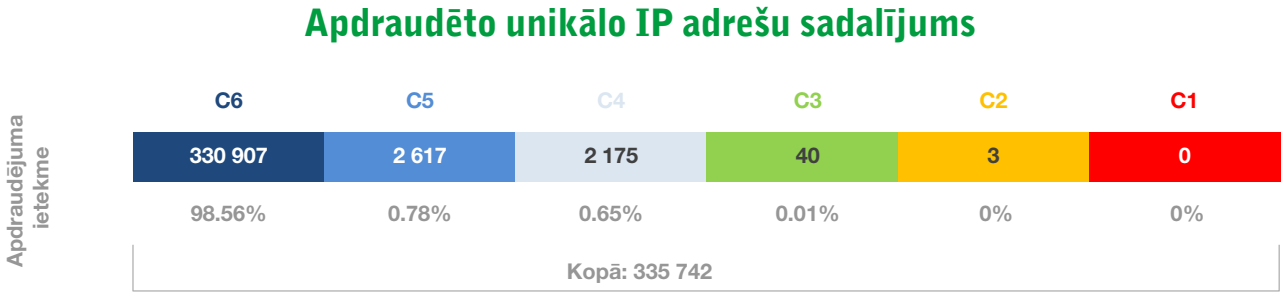


6. attēls – Apdraudējumu matricas sadalījums kategorijās.

Vairāk nekā 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.

Nacionāla līmeņa apdraudējumi (C1) pārskata periodā nav reģistrēti. Augstas nozīmes apdraudējumu (C2) kategorijā reģistrētas trīs apdraudētas IP adreses. Apdraudējums saistīts ar e-pasta drošības sistēmas kompromitēšanu kādā valsts iestādē. Pārbaužu rezultātā tika noskaidrots, ka kompromitētie serveri atradās izolētā vidē un liela apjoma datu izgūšana no uzbrucēja puses netika veikta, kā arī netika ietekmētas citas iekšējās iekārtas.

Nozīmīgi plašas ietekmes apdraudējumi (C3) veido 0,01% (40 unikālas apdraudētas IP adreses/gadījumi) no visiem kategorizētajiem apdraudējumiem. 63% šo apdraudējumu bija ļaundabīgs kods, bet 37% veidoja pakalpojumu pieejamības incidenti.
Būtiski apdraudējumi ar vidēju ietekmi (C4) veido 0,65% (2175 unikālas apdraudētas IP adreses/

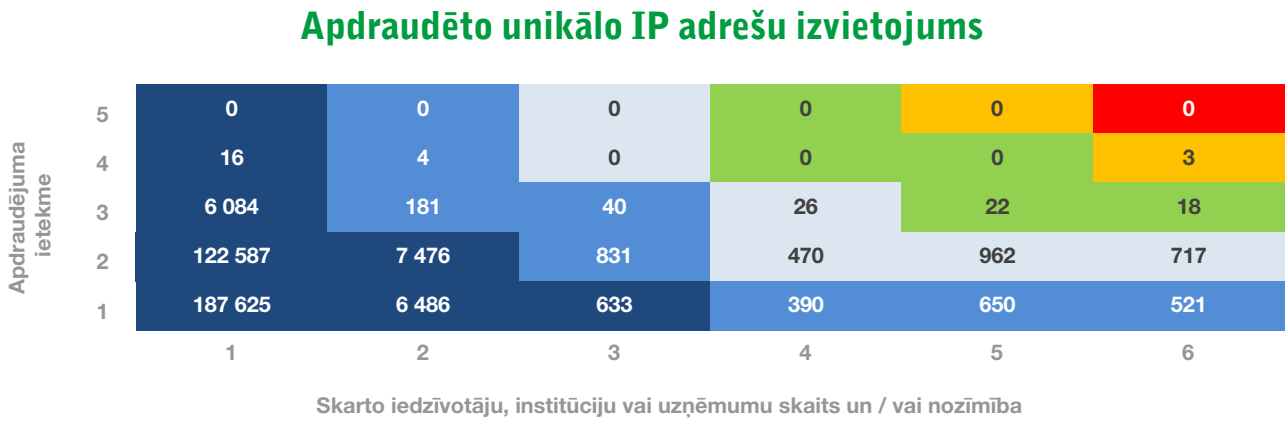


7. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu sadalījums apdraudējumu kategorijās pēc apdraudējuma ietekmes (matrica) 2023. gada 2. ceturksnī.

gadījumi) no visiem kategorizētajiem apdraudējumiem. 10% šo apdraudējumu bija konfigurācijas nepilnības (*Accessible-ftp, ntp-version, Open-telnet* u.c.), bet pārējo veidoja ielaušanās mēģinājumi, ļaundabīgs kods, pakalpojuma pieejamības incidenti, krāpšana un informācijas vākšanas incidenti augstas un vidēji augstas prioritātes iestādēs.

Lai sekmētu kopējo kiberdrošību valstī, CERT.LV sadarbībā ar NIC.LV ir izstrādājusi DNS RPZ (*Domain Name Service Response Policy Zone*) jeb DNS ugunsmūri (*DNS firewall*). 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. Šis risinājums bez maksas ir pieejams jebkuram Latvijas iedzīvotājam, uzņēmumam un organizācijai. Informācija par darbību un uzstādīšanu: https://dnsmuris.lv/



7. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu izvietojums matricā 2023. gada 2. ceturksnī valsts un pašvaldību institūcijās.

2. Atbalsta sniegšana informācijas tehnoloģiju drošības incidentu novēršanā vai novēršanas koordinēšana

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.

Pārskata periodā tika novēroti vairāki SMS krāpniecības viļņi. Uzbrucēji izmantoja aktuālas tēmas iedzīvotāju bankas piekļuves datu izgūšanai.

Aprīļa beigās tika saņemti ziņojumi par krāpnieciskām SMS it kā latvija.lv vārdā, kurās saņēmēji tika aicināti apmaksāt administratīvo sodu. SMS norādītā saite veda uz viltus vietni. Uzbrukumā tika izmantots augstākā līmeņa (*top-level-domain*) .net domēna vārds, kuru krāpnieki mēģināja nomaskēt par .gov.lv.

Maijā un jūnijā krāpnieki turpināja izsūtīt krāpnieciska rakstura īsziņas Latvijas Pasta vārdā, šoreiz no ārvalstu tālruņa numuriem, aicinot apmaksāt muitas nodokli. Savukārt maija vidū virkne Latvijas iedzīvotāju SMS veidā saņēma krāpnieciskas ziņas par it kā pozitīvu HIV testu. Īsziņas šķietami tika sūtītas no e-veselības portāla.

CERT.LV rīcībā nonākusi informācija par vismaz 50 cietušajiem, kas ievadījuši savus datus krāpnieciskajā Latvijas Pasta vietnē, atbildot uz saņemto SMS.

Krāpnieki centās iegūt arī lietotāju e-pasta piekļuves datus. Aprīlī CERT.LV saņēma ziņojumus no vairākām valsts un pašvaldību iestādēm par mērķētiem pikšķerēšanas e-pastiem, kas sūtīti konkrēto iestāžu darbiniekiem, lai iegūtu darbinieku e-pastu lietotājvārdus un paroles. Krāpnieki uzdevās par palīdzības dienestu un apgalvoja, ka lietotāja e-pasta kontam radušās problēmas un aizturēta e-pastu piegāde. Darbinieki savlaicīgi atpazina pikšķerēšanas mēģinājumus un uzbrukumā necieta.

Maijā tika saņemti arī vairāki ziņojumi par krāpniekiem, kas izlikās par inbox.lv atbalsta komandu un lūdza verificēt lietotājam savu e-pastu, pretējā gadījumā tā darbība pēc 48h tiktu apturēta. E-pastā bija iekļauta saite, kas lietotāju nogādāja pikšķerēšanas vietnē, kas vizuāli atgādināja īsto inbox.lv mājaslapu. Krāpnieku mērķis šādā veidā bija izvilināt lietotāju e-pastu piekļuves datus.

Pret uzņēmumiem tika vērsta dažādas uzbrukumu kampaņas - gan iejaukšanās biznesa sarakstē un viltus rēķinu izsūtīšana ar mērķi panākt maksājuma veikšanu uz uzbrucēja kontu, gan e-pasti uzņēmumu grāmatvežiem it kā vadītāju vai citu darbinieku vārdā.

Kādas reģionālās slimnīcas grāmatvede atkārtoti saņēma aizdomīgu e-pastu it kā no slimnīcas vadītāja ar jautājumu par konta atlikumu un iespējām pārskaitīt 35 000 EUR. Ciešāk izpētot sūtītāja e-pasta adresi, grāmatvede savlaicīgi atpazina krāpniecību un uzbrukumā necieta.

Tika saņemts ziņojums no kādas medicīnas iestādes darbinieces, kuras vārdā krāpnieki sūtījuši viltus e-pastus sievietes darba devējam, un lūguši mainīt bankas kontu algas saņemšanai. Līdzīgs incidents noticis arī pērnā gada nogalē, kad krāpniekiem izdevās izkrāpt kādu darba algu. Šoreiz darba devējs krāpniecību atpazinis un par notikušo informējis arī savu darbinieci. CERT.LV kā vienu no risinājumiem rekomendēja ieviest elektroniski parakstītu dokumentu apriti - vienoties ar vadību, ka turpmāk līdzīga veida pieprasījumi tiek sūtīti un pieņemti tikai elektroniski parakstīti.

Kāds ar veselīgu dzīvesveidu saistīts uzņēmums cieta no iejaukšanās biznesa sarakstē (BEC), kuras rezultātā no uzņēmuma ar viltus rēķina palīdzību tika izkrāpti 13 700 eiro. Uzņēmuma

darbinieka e-pastam tika izmantota vairāku faktoru autentifikācija (MFA) un netika saņemti paziņojumi par mēģinājumiem pieslēgties kontam. Tiek pieļauts, ka kompromitēts ir ticis sadarbības partnera e-pasta konts.

No iejaukšanās biznesa sarakstē pēdējo gadu laikā cietuši arī citi Latvijas uzņēmumi, taču šis incidents bija unikāls ar to, ka uzņēmējs un biznesa partneris pēc uzbrukuma saņēma arī ziņu no kāda anonīma avota, kurš apgalvoja, ka zinot par notikušo krāpniecību un zina, kā naudu atgūt. Par šādu *izpalīdzēšanu* anonīmais ziņotājs pieprasīja 3 500 eiro. Uzņēmums ar iesniegumu vērsies Valsts policijā.

Peļņas un finanšu aspekts tika izmantots arī krāpnieciskos uzbrukumos, kas tika vērsti pret iedzīvotājiem. Iedzīvotāju uzticību nereti izpelnās informācija un paziņojumi, kas publicēti sociālajā tīklā *Facebook*.

CERT.LV turpināja saņemt ziņojumus par krāpnieciskiem e-pastiem it kā Valsts ieņēmumu dienesta vārdā. E-pastā tika minēts, ka lietotājs veiksmīgi saņēmis nodokļu atmaksu *Nodokļu portālā*, un ticamībai atsūtīta arī pagaidu parole, lai piekļūtu šim portālam. Pēc pieslēgšanās portālam tika prasīts ievadīt personas kodu un telefona numuru. Pēdējā solī krāpnieki lūdza ievadīt arī bankas piekļuves datus, lai lietotājs varētu it kā saņemt nodokļu atmaksu uz savu bankas kontu. Datu ievadīšanas gadījumā tie tika nosūtīti krāpniekiem. Tika saņemtas ziņas arī par cietušajiem, kas steigā un citu apstākļu sakritības rezultātā krāpniecību nepamanīja un datus ievadīja. CERT.LV aicināja iedzīvotājus saglabāt modrību, savukārt cietušajiem ieteica operatīvi sazināties ar savu banku un vērsties Valsts policijā ar iesniegumu.

Kāds iedzīvotājs, izmantojot informāciju, kas iegūta sociālajā tīklā *Facebook*, kādā interneta vietnē veica traktortehnikas iegādi. No tirgotāja tika saņemts rēķins 14 580 eiro apmērā, kas arī tika apmaksāts. Iedzīvotājam iepriekšējā pozitīvā pieredze ar pirkumiem internetā, kā arī konkrētā tirgotāja vietne un izrakstītais rēķins neradīja aizdomas par krāpšanu. Pēc rēķina apmaksas tirgotājs komunikāciju pārtrauca un arī interneta vietne beidza savu darbību. CERT.LV sniedza rekomendācijas krāpniecisku vietņu atpazīšanai. Iedzīvotājs vērsās ar iesniegumu policijā.

Tika saņemta ziņa no kāda iedzīvotāja par zaudējumiem aptuveni 3000 eiro apmērā. Iedzīvotājs sociālajā tīklā Facebook ieguva informāciju par iespēju nopelnīt un sazinājās ar kontaktinformācijā norādīto personu. Krāpnieki pierunāja veikt iemaksas krāpnieku norādītajā vietnē, simulējot finanšu pieaugumu. Cenšoties *nopelnīto* pārskaitīt uz savu kontu, iedzīvotājs saskārās ar dažādiem šķēršļiem – paziņojumiem, ka ir jāgaida, pēc tam, ka nepieciešams veikt dažādu nodokļu apmaksu, ieskaitot papildu finanšu līdzekļus. Iedzīvotājs apjauta, ka ir notikusi krāpšana, un vērsās ar iesniegumu policijā.

2.2. Pakalpojuma pieejamība

Pārskata periodā turpinājās Krievijas agresīvo politiku atbalstošo haktīvistu aktivitātes. DDoS uzbrukumus piedzīvoja gan enerģētikas un transporta nozare, gan virkne valsts iestāžu resursu. Uzbrukumi sadarbībā ar LVRTC un SIA Tet tika veiksmīgi atvairīti un neradīja būtiskus traucējumus sistēmu pieejamībai.

31. maijā pēc jaunā Latvijas Valsts prezidenta Edgara Rinkēviča ievēlēšanas amatā Saeimas resursi piedzīvoja pastiprinātus DDoS uzbrukumus. Haktīvisti savos Telegram kanālos aicināja sekotājus jauno prezidentu *apsveikt* kā pienākas jeb ar DDoS uzbrukumu Saeimas mājaslapai. Uzbrukums bija neveiksmīgs un mājaslapas darbība netika traucēta.

Savukārt 23. jūnija vakarā, kad algotņu grupējuma *Vagner* vadītājs Jevgeņijs Prigožins paziņoja, ka *Vagner* algotņi no Ukrainas iegājuši Krievijā un dodas uz Maskavu nolūkā gāzt Krievijas militāro vadību, nekādas anomālijas, kas būtu saistāmas ar notikumiem Krievijā, Latvijas kibertelpā netika novērotas. Arī XXVII *Vispārējio latviešu Dziesmu* un XVII *Deju svētku* kontekstā netika novēroti DDoS uzbrukumi un svētku periods noritēja mierīgi.

2.3. Ļaundabīgs kods

Aprīlī CERT.LV redzeslokā nonāca vairākas individuālas iekārtas no dažādām pašvaldībām, kurās tika identificēta ļaunatūru klātbūtne. Vairumā gadījumu tika konstatēta *Stantinko* ļaunatūra, kas uz upura iekārtas var, piemēram, lejupielādēt ļaundabīgus interneta pārlūka spraudņus, kas tālāk lietotāju pārvirza uz dažādām reklāmas vietnēm. Otra izplatītākā ļaunatūra bija *Android Hummer* trojānis, kas atbildīgs par citu lietotņu lejupielādi uz upura iekārtas un uzlecošiem reklāmas logiem. Visos gadījumos CERT.LV informēja iestāžu atbildīgās personas, un sniedza konsultācijas tālākai rīcībai.

Kāds tirdzniecības uzņēmums cieta *Mallox* šifrējošā izspiedējvīrusa uzbrukumā. Sašifrēta tika MS SQL datubāze un cita vērtīga informācija. Datubāzei bija atvērta piekļuve no interneta. Uzņēmums nebija veidojis rezerves kopijas. Tika sniegtas rekomendācijas iespējamai datubāzes atgūšanai. CERT.LV informēja uzņēmumu arī par pieejamajiem *Avast* un nomoreransom.org dešifrēšanas rīkiem konkrētās ļaunatūras gadījumā.

Kāda loģistikas uzņēmuma vārdā tika izplatīti e-pasti ar kaitīgiem pielikumiem. E-pasta izsūtītājs tika viltots, bet pielikumā iekļautā *AgentTesla* ļaunatūra tika maskēta kā rēķins. *AgentTesla* ir komerciāla ļaunatūra un tās mērķis ir sniegt uzbrucējam piekļuvi pie inficētās iekārtas un veikt informācijas ievākšanu. Saņēmēju vidū bija arī vairākas valsts iestādes. Kaitīgais e-pasts tika atpazīts, kaitējums nodarīts netika.

Tika saņemti vairāki ziņojumi par ļaundabīgiem e-pastiem, kas šķietami sūtīti SEB bankas vārdā. E-pasta tēmā bija norādīts – *Paziņojums Par ienākošo Bankas Maksājumu*, un tālāk tekstā apgalvots, ka kāds no lietotāja paziņu / klientu loka pieteicis bankai nosūtīt lietotājam šo ziņu. Tālāk lietotājs tika aicināts papildu informāciju lasīt pielikumā pievienotajā *maksājuma dokumentā*, kas patiesībā saturēja ļaunatūru. Pielikumā pievienotais vīruss bija paredzēts sensitīvas informācijas izgūšanai no upura iekārtas.

2.4. Ielaušanās mēģinājumi

Ielaušanās mēģinājumi 84% gadījumu veikti, izmantojot paroļu minēšanu (*brute-force*). Uzbrukumi vērsti galvenokārt pret dažādiem interneta pakalpojumu sniedzējiem. Pēc CERT.LV rīcībā esošās informācijas šie uzbrukumi nav bijuši sekmīgi.

Tika saņemts ziņojums par draudu e-pasta vēstulēm it kā *Lazarus Grupas* Latvijas iecirkņa vārdā, draudot ar uzbrukumiem medicīnas iestādēm, finanšu institūcijām un enerģētikas uzņēmumiem. Par izteiktajiem draudiem papildus tika izsūtīta informācija veselības aprūpes institūcijām, kā arī informācija nodota drošības dienestiem.

2.5. Kompromitētas iekārtas un datu noplūdes

Tika saņemta informācija, ka kādas veselības aprūpes iestādes tīmekļa vietnē ir nesankcionēti ievietots *webshell*, kas sniedz uzbrucējiem iespēju attālināti piekļūt resursam. Uzbrucēji bija izmantojuši zināmu *WordPress* ievainojamību. Vietnes uzturētājs tika informēts un sniegtas rekomendācijas apdraudējuma novēršanai, kā arī kiberdrošības situācijas uzlabošanai. Incidents tika operatīvi novērsts.

Notika nesankcionēta trešo pušu piekļūšana kāda uzņēmuma konfigurācijas/ monitoringa serverim. Cilvēciskas kļūdas dēļ servera atjaunināšanas darbu laikā uz brīdi tikusi apturēta servera ugunsmūra darbība, kuras rezultātā trešās puses piekļuvušas servera datiem. Uzbrucēji veica datu kopēšanu un uzņēmuma serverī esošos datus dzēsa. Dati, kas incidenta rezultātā kļuva pieejami trešajām personām, ir tehniska rakstura. Uzņēmumam bija datu rezerves kopija. Par incidentu informēta DVI.

Tika saņemts ziņojums par *Barracuda* e-pasta drošības sistēmas kompromitēšanu kādā valsts iestādē. Pārbaužu rezultātā tika noskaidrots, ka kompromitētie serveri atradās izolētā vidē un liela apjoma datu izgūšana no uzbrucēja puses netika veikta, kā arī netika ietekmētas citas iekšējās iekārtas.

Tika saņemta informācija par internetā nopludinātām parolēm, kuru vidū bija atrodama arī kādas pašvaldības darbinieka datora paroles. Tika veikta pašvaldībai piederošā datora analīze, lai noteiktu potenciālo veidu, kādā notikusi paroļu noplūde.

Tika saņemts ziņojums par kompromitētu kādas valsts iestādes e-pasta adresi, no kuras vairākiem publiskā sektora saņēmējiem tika izsūtīti pikšķerēšanas e-pasti. Darbiniece bija ievadījusi savus e-pasta piekļuves datus pikšķerēšanas vietnē, bet atskārtusi pieļauto kļūdu un informējusi par notikušo. Pikšķerēšanas e-pastā ļaundabīgas komponentes netika konstatētas. Tiek veikta kompromitētās iekārtas analīze.

Tika identificētas uzbrucēju aktivitātes kādā portālā. Uzbrucēji piekļuva lietotāju profiliem, izmantojot vēsturiskas datu noplūdes. Tas bija iespējams pateicoties tam, ka lietotāji dažādiem resursiem neapdomīgi izmantojuši vienas un tās pašas paroles, kā rezultātā tika kompromitēti vairāk nekā 100 portāla lietotāju konti. Vienā no gadījumiem, lietotājam bijušas paaugstinātas privilēģijas, ko noziedznieki izmantojuši, lai dzēstu un modificētu atsevišķus ierakstus portālā. Incidents tika operatīvi novērsts, - dzēstais saturs tika atjaunots un kompromitēto lietotāju profiliem nomainīti piekļuves dati.

Saņemta informācija no kāda uzņēmuma par incidentu, kurā uzbrucēji nesankcionēti piekļuvuši uzņēmuma sistēmām, veikuši datu izgūšanu un sistēmu šifrēšanu. Incidentu izdevies lokalizēt un uzņēmuma pamatfunkcijas netika ietekmētas. Uz pārskata perioda beigām netika konstatēta ietekme uz klientu sistēmām vai produktu drošību. Uzņēmums turpina darbu pie incidenta izmeklēšanas.

CERT.LV un NIC.LV uzturētais DNS mūris bloķēja pieprasījumu no kāda valsts iestādes resursa uz kaitīgu vietni. Pārbaužu rezultātā tika konstatēts, ka kompromitēts viens lietotājs, uzbrucējam izmantojot publiski plaši pieejamus rīkus. Tika konstatēts, ka administratora panelim uzbrucējs piekļuva, neveicot ielaušanās mēģinājumus, bet izmantojot iepriekš iegūtu paroli. Uzbrucēja IP adrese fiksēta arī citos incidentos, kuros izmantotas līdzīgas metodes. Incidents nav uzskatāms par mērķētu. Tiek veikta incidenta padziļināta analīze. Uzbrukuma indikatori liecina, ka potenciāli tas saistāms ar Ķīnu.

2.6. Ievainojamības

Aprīļa vidū CERT.LV publicēja brīdinājumu par ievainojamību *Microsoft Message Queuing* (*MSMQ*) risinājumā, kas sniedza iespēju neautentificētam lietotājam veikt attālinātu koda izpildi ievainojamajā sistēmā. CERT.LV aicināja visus pēc iespējas ātrāk uzstādīt Microsoft publicētos atjauninājumus.

Maijā tika saņemts ziņojums no kāda uzņēmuma par tajā izmantoto *Alcatel* tīklu pārvaldības risinājumu. Risinājuma programmnodrošinājumā tiek izmantota novecojusi *Java* programmatūras versija, kas satur *Log4shell* ievainojamību (*Log4shell* ievainojamība atklāta 2021. gadā un ļauj uzbrucējiem iegūt pilnīgu kontroli pār ievainojamo serveri). Servera atjaunināšana uzņēmumā nav iespējama, ja vien netiek veikta jaunas programmatūras versijas iegāde, kas, savukārt prasa apjomīgas investīcijas.

1. jūnijā tika izsūtīti brīdinājumi par kritisku ievainojamību *Barracuda Email Security Gateway* e-pasta drošības sistēmā. Ievainojamība sniedza uzbrucējam iespēju veikt attālinātu koda izpildi un jau tika aktīvi izmantota uzbrukumos. Cietušie tika konstatēti arī Latvijā.

14. jūnijā tika saņemta informācija par kritisku ievainojamību *FortiGate* ugunsmūra risinājumā. Ievainojamība sniedza uzbrucējam iespēju veikt attālinātu koda izpildi. Pēc pārbaužu veikšanas tika apzinātas iestādes, kas izmanto šo risinājumu, un šīm iestādēm tika nosūtīti brīdinājumi par konstatēto apdraudējumu, kā arī aicinājums nekavējoties uzstādīt atjauninājumus kompromitēšanas riska novēršanai.

15. jūnijā tika izsūtīti brīdinājumi par kritisku ievainojamību MS Exchange e-pasta apmaiņas serveros. Ievainojamība sniedza uzbrucējam veikt attālinātu koda izpildi. Informācijas saņēmēji tika aicināti nekavējoties uzstādīt Microsoft publicētos atjauninājumus.

2.7. Atbildīga ievainojamību atklāšana

Pārskata periodā tika saņemts ziņojums par iespējamām nepilnībām kādā lietotnē. Nepilnības potenciāli sniedz iespēju autorizētam lietotājam piekļūt citu lietotāju informācijai, tajā skaitā, izmantot lietotāja kontam pievienotos maksāšanas līdzekļus. Iesniegtajam ievainojamības ziņojumam tiek veikta pārbaude sadarbībā ar izstrādātāju.

2.8. Drošības testi

Pārskata periodā tika veikta IP kameru pārbaude, lai identificētu publiskajā tīklā eksponētas kameras Latvijas IP adrešu apgabalā un veiktu minēto tīmekļa iekārtu ievainojamību testēšanu. Projekts tika fokusēts uz ievainojamu kameru identificēšanu. Tika konstatētas 157 iekārtas, kurās tika izmantotas noklusējuma paroles vai kuru ievainojamības sniedza iespēju veikt neautorizētu pieslēgumu iekārtām.

3. Pētnieciskā darba veikšana, kā arī apmācību un izglītojošu pasākumu organizēšana informācijas tehnoloģiju drošības jomā

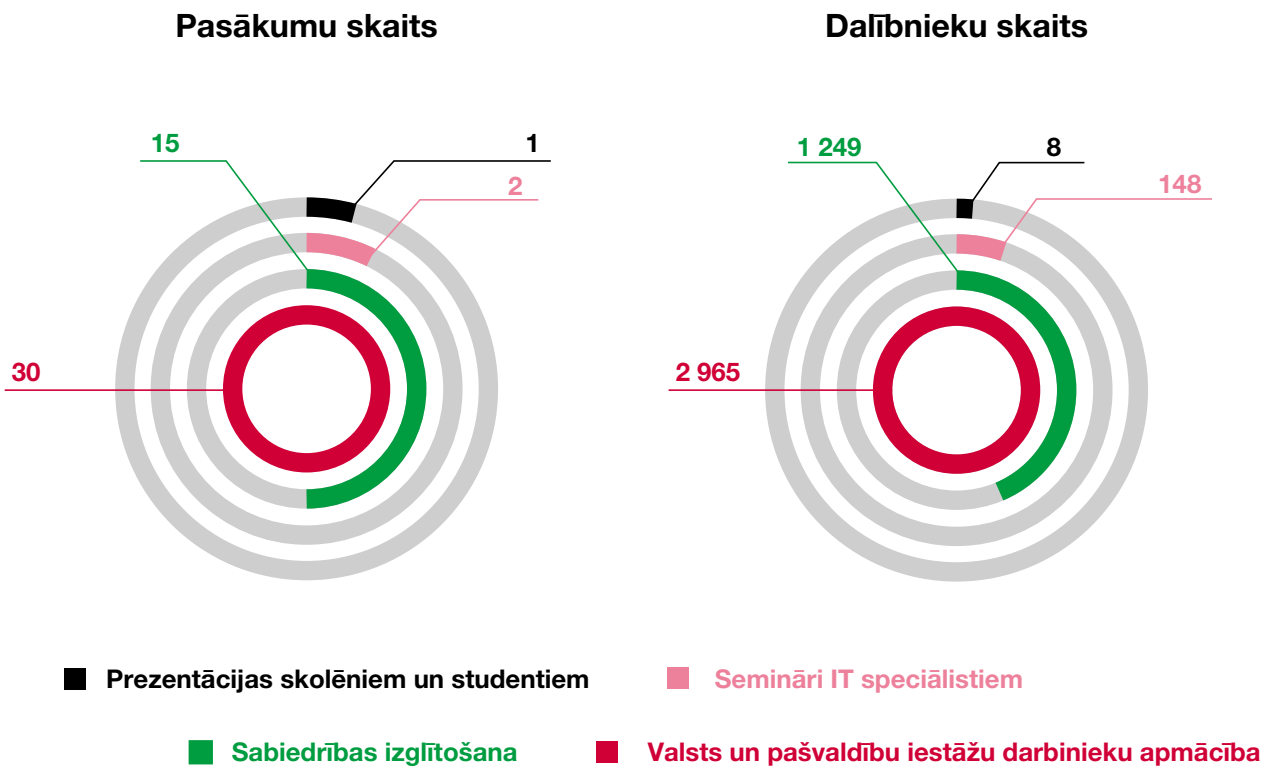
5. aprīlī CERT.LV piedalījās Ēnu dienas pasākumā un uzņēma ēnotājus, lai iepazīstinātu jauniešus ar kiberdrošības sfēru un veicinātu interesi par kiberdrošības speciālista profesiju.

No 24. līdz 29. aprīlim norisinājās Digitālā nedēļa Latvijā, kas tika organizēta Eiropas Savienības prasmju gada *un All Digital Weeks 2023* ietvaros. Digitālās nedēļas mērķis ir veicināt iedzīvotāju un uzņēmēju digitālo prasmju attīstību, kā arī digitālo iespēju paplašināšanu. 26. aprīlis jeb Digitālās drošības diena tika veltīts kiberdrošības jautājumiem. LVRTC sadarbībā ar CERT.LV, NIC un Valsts policiju tiešsaistes seminārā *Krāpnieciska e-pasta anatomija* sniedza

ieskatu krāpnieku izmantotajās viltībās, izplatot viltus e-pastus (https://www.facebook.com/events/551627423706015).

26. aprīlī CERT.LV piedalījās iniciatīvas Women4Cyber Latvia atklāšanas pasākumā. Iniciatīvas mērķis ir veidot stipru kiberdrošības kopienu, pulcējot gan speciālistes, kuras jau darbojas kiberdrošības jomā, gan tās, kuras interesējas un vēlas iesaistīties nozarē, iedrošinot un izglītojot. (https://women4cyberlatvia.com/) CERT.LV piedalījās arī Women4Cyber Latvia organizētajā

Izglītojošo pasākumu un apmācīto cilvēku skaits



9. attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2023. gada 2. ceturksnī

vebinārā *Kiberdrošība kā profesija*, kas notika 31. maijā. Vebinārā tika aplūkoti kiberdrošības dažādie virzieni un daudzpusīgās iespējas. (https://www.youtube.com/watch?v=Xkf3zBMvw1Q)

25. maijā CERT.LV eksperts piedalījās sarunu festivāla LAMPA ievaddiskusijā *Drošība: Ierakumi digitālajā frontē jeb cik viegli tevi "uzlauzt",* kuru organizēja Valsts kanceleja. Sarunas mērķis bija noskaidrot, cik labi institūcijas un sabiedrība spēj kopīgi pretoties gan naidīgiem vēstījumiem un manipulācijām informatīvajā telpā, gan arī reāliem kiberuzbrukumiem? (https://www.facebook.com/valdibasmaja/videos/206995715482109)

9. jūnijā CERT.LV piedalījās CVK organizētajā diskusijā *Vēlēšanas 2.0 - skats nākotnē*, kas notika sarunu festivāla LAMPA ietvaros. Diskusijas mērķis bija pulcināt jauniešus, vēlētājus, ekspertus un nevalstisko organizāciju pārstāvjus, lai meklētu atbildes uz jautājumiem, kādai būtu jāizskatās vēlēšanu nākotnei, kādas iespējas un riski ir tehnoloģiju pielietošanai, kā arī ko mēs varam mācīt ies no kaimiņu valstīm? (https://festivalslampa.lv/lv/programma/pasakumi/2115)

21. jūnijā CERT.LV piedalījās seminārā datu aizsardzības speciālistiem, stāstot par datu nozīmi kiberaizsardzībā, kādi dati nepieciešami kiberincidenta izmeklēšanā un kāpēc, kā arī, kādas ir iespējamās pretrunas datu glabāšanā no datu aizsardzības un kiberdrošības skatpunktiem.

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

Sadarbības tikšanās, konsultācijas un prezentācijas:

- CERT.LV piedalījās Nacionālā kiberdrošības likuma izskatīšanas sanāksmē un pēc sanāksmes tikās ar Finanšu nozares asociāciju un Latvijas Banku, lai pārrunātu iespējamu Latvijas Bankas izņemšanu no likuma tvēruma, jo uz bankām attiecināms DORA regulējums. Sniegti komentāri Aizsardzības ministrijai par likumā izmantoto terminoloģiju.

- Dalība jaunu MK noteikumu izstrādē par datu centriem un drošības operāciju centriem (SOC). Pārskata periodā noritēja darbs pie noteikumu satura. CERT.LV gatavoja prasības datu centru auditoriem, prasības dažādu gradāciju datu centriem, kā arī nosacījumus drošības operāciju centriem datu centros.

- Tika sniegti komentāri par Vides aizsardzības un reģionālās attīstības ministrijas izstrādāto MK noteikumu Nr. 597 *Informācijas sistēmu vispārējās tehniskās prasības* projektu, papildinot sadaļas, kas skar IS aktivitāšu kiberdrošības izvērtēšanu.

- Dalība Saeimas Sociālo un darba lietu komisijas organizētajā *Datu otrreizējās izmantošanas* likuma darba grupā, lai sekotu līdzi likuma virzībai un aspektiem, kas saistīti ar datu otrreizējo izmantošanu un kiberdrošību.

- CERT.LV piedalījās sanāksmēs ar Aizsardzības ministriju un Ekonomikas ministriju par *Kibernoturības akta* ieviešanu Latvijā, lai sniegtu skatījumu par iespējamajiem veidiem, kādos iespējams nodrošināt IKT produktu sertifikāciju Latvijā.

- Turpinājās darbs pie koordinētas ievainojamību atklāšanas ziņojumu reģistrēšanas platformas attīstības. Platformas izstrāde tika uzsākta, balstoties uz Ministru kabineta apstiprināto Aizsardzības ministrijas sagatavoto informatīvo ziņojumu *Par koordinētas ievainojamību atklāšanas procesa ieviešanu valsts pārvaldē*, ar kuru ir uzsākta koordinētu ievainojamību atklāšanas procesa (turpmāk – CVD) ieviešana valsts pārvaldē, paredzot iespēju iestādēm brīvprātīgi iesaistīties CVD. Platforma nodrošina iespēju pētniekam reģistrēt ziņojumu par novērotajām ievainojamībām iestāžu resursos, kā arī visiem iesaistītajiem (iestādei, pētniekam un CERT.LV) izvērtēt iesniegtos ziņojumus un sekot ievainojamību novēršanas gaitai. Pārskata periodā iestāžu atbildīgajiem par IT drošību tika nosūtītas programmu apraksta vadlīnijas. Uz pārskata perioda beigām platformā bija reģistrējušies 23 iestāžu/uzņēmumu atbildīgie par koordinātas ievainojamību atklāšanas ziņojumu apstrādi, 34 drošības pētnieki un bija izveidotas 3 ievainojamību atklāšanas programmas.

- Aizsardzības ministrijas uzdevumā sagatavoti 2 sākotnējie izvērtējumi valsts informācijas sistēmu attīstības aktivitātēm un 6 atkārtoti izvērtējumi.

- 19 aprīlī tikšanās ar Finanšu ministriju, lai pārrunātu ministrijas virzītā prioritārā audita tvērumu 2024. gadam. Auditā viens no iekļautajiem jautājumiem ir IKT drošības pārvaldība (t.sk. kiberdrošības risku un to mazināšanas kontroļu novērtēšana). Pārrunātas plānotās pārbaudes, rekomendējot papildinājumus IKT drošības audita tvērumā.
- 19. aprīlī dalība Saeimas Valsts pārvaldes un pašvaldību komisijas sēdē par plānoto vēlēšanu procesu norisi gaidāmajās Eiropas Parlamenta vēlēšanās, lai sniegtu komentārus un atbildētu uz jautājumiem, kas saistīti ar vēlēšanu sistēmu kiberdrošību.

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

CERT.LV starptautiskā sadarbība pārskata periodā:

- Turpinājās darbs FIRST SIG darba grupā *CSIRT Services Framework*, izstrādājot vienotu ietvaru CERT komandu dalībnieku lomām, kompetencēm un prasmēm. Pārskata periodā turpinājās CERT komandu tipu noteikšanas metodoloģijas izstrāde, kas sekmētu veicamajiem uzdevumiem nepieciešamo lomu un kompetenču identificēšanu.
- Dalība FIRST *Membership Committee* (Jauno biedru uzņemšanas komitejas) sanāksmēs, lai apspriestu turpmākos noteikumus biedru uzņemšanā un piesaistīšanā, kā arī SIM3 modeļa izmantošanu. CERT.LV vadītāja Baiba Kaškina turpināja darbu kā FIRST *Membership Committee* priekšsēdētāja (*chair*), piedaloties jauno biedru pieteikumu izskatīšanā un veicinot biedru uzņemšanas procesa uzlabošanu.
- 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. Pārskata periodā pēc sākotnējā prototipa testēšanas darba grupa turpināja attīstīt *Cybersecurity index* platformu.
- Dalība ENISA vadītajā darba grupā *Coordinated Vulnerability Disclosure (CVD) Task Force*, kurā norit darbs pie ES līmeņa koordinētas ievainojamību atklāšanas politikas vadlīniju veidošanas.
- CERT.LV piedalījās ENISA organizētajās *Cyber Europe 2024* mācību plānošanas sanāksmēs, kurās notika diskusijas par mācību misiju, vīziju un mērķiem, mācību scenārija variantiem un apmācāmajiem sektoriem, laika grafiku, kā arī plānoto mācību platformu (būs pieejama no 2023.gada septembra). Par mācību centrālo sektoru tika izvirzīts enerģētikas sektors, bet kā divi atbalstošie sektori – digitālā infrastruktūra un sabiedrības pārvalde. Spēlētāji tiks uzrunāti šā gada rudenī, kad būs veikta vismaz sākotnējā scenārija izstrāde. CERT.LV aktīvi iesaistās mācību plānošanā, papildinot mācību dokumentāciju ar idejām, sekojot līdzi aktualitātēm un piedaloties diskusijā ENISA plānotāju platformā.
- Regulāra dalība *CSIRT Network Situation Update* sanāksmēs, kuru mērķis ir veikt informācijas apmaiņu par aktuālo kibertelpā starp CSIRT tīkla biedriem.
- No 17. līdz 21. aprīlim norisinājās NATO CCDCoE organizētās kiberdrošības mācības *Locked Shields 2023*. Šogad CERT.LV piedalījās mācībās gan *Green Team* sastāvā, nodrošinot mācību vērtēšanu, gan dalībnieku komandas (*Blue Team*) sastāvā tehniskajā un stratēģiskajā spēlē.
- No 22. maija līdz 8. jūnijam CERT.LV pārstāvis piedalījās Taivānas ICDF (International Cooperation and Development Fund) organizētā seminārā, kurā tika aplūkoti dažādi

ar kiberdrošību saistīti aspekti un to organizācija no Taivānas perspektīvas. Semināra dalībnieki veidoja darba grupas un sniedza savu skatījumu un rekomendācijas.

- No 23. līdz 26. maijam Bukarestē, Rumānijā, notika 69. TF-CSIRT sanāksme, kurā CERT.LV sniedza prezentāciju Coordinated vulnerability disclosure process in Latvia – chapter II, iepazīstinot klausītājus ar atbildīgas ievainojamību atklāšanas procesa ieviešanu Latvijā.
- No 1. līdz 11. jūnijam Monreālā, Kanādā notika 35. ikgadējā FIRST konference, kuras mērķis ir veicināt kiberdrošības un incidentu apstrādes komandu globālu sadarbību. CERT.LV pārstāvji konferencē vadīja vairākas sesijas, kā arī pirms konferences piedalījās FIRST mentoringa programmā, lai atbalstītu tās organizācijas, kas varētu kļūt par jaunajiem FIRST biedriem. Atbalsts tika sniegts CERT komandām no Albānijas un Serbijas, informējot par FIRST konferences norisi, sadarbības iespējām un darba grupām.
- 28. jūnijā CERT.LV iesniedza sākotnējos komentārus par valsts vietotā interneta apmaiņas punkta (GLV-IX) darbību reglamentējošajiem MK noteikumiem.

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.

2023. gada 2. ceturksnī CERT.LV tupināja *Grafoskopa* risinājuma izstrādes darbus atbilstoši plānam. Pārskata periodā CERT.LV piedalījās attālinātās JTAN projekta sanāksmēs, kurās projekta partneri informēja par saviem projekta uzdevumiem un rezultātiem.

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. 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.

CERT.LV sadarbojas arī ar citām iestādēm, kuru uzdevums ir veidot bloķējamo vietņu sarakstus, un iekļauj šos sarakstus DNS ugunsmūrī, lai interneta pakalpojumu sniedzējiem, izvēloties izmantot DNS RPZ, būtu iespēja vienuviet iegūt visu informāciju par filtrējamajiem resursiem.
Pārskata perioda laikā lietotāji tika pasargāti **50 480** reizes.

- 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 uzticamības pakalpojumu sniedzējus un kvalificētus elektroniskās identifikācijas pakalpojumu sniedzējus.

8. 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 01.04.2023. līdz 30.06.2023. ir saņēmusi un izvērtējusi 476 ziņojumus. No tiem 279 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 9 gadījumos konstatēta

pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 19 ziņojumos konstatēta personas goda un cieņas aizskaršana, 11 ziņojumi saņemti par naida runu un 4 ziņojumos konstatēti vardarbīgi materiāli. Par finanšu krāpšanas mēģinājumiem internetā saņemti 73 ziņojumi, 46 ziņojumu saturs nav bijis pretlikumīgs, 35 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 72 ziņojumi par naida runu un bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 53 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 64 ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem 38 ziņojumi ir dzēsti no publiskas aprites un 26 ziņojumu saturs atrodas dzēšanas procesā sadarbībā ar Valsts policiju un interneta pakalpojumu sniedzējiem.

2023. gada 22. 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