CERT.LV DARBĪBAS PĀRSKATS

C1
2024

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Latvijas universitātes
Matemātikas un informātikas institūts

Aizsardzības ministrija

Pārskatā iekļauta vispārpieejama informācija par CERT.LV aktivitātēm un darbības rezultātiem, neietverot ierobežotas pieejamības informāciju. Pārskatam ir tikai informatīva nozīme.

Satura rādītājs

Kopsavilkums

CERT.LV ir aktīvi veicinājusi savu lomu kā draudu medību operāciju līdere Eiropas Savienībā, stiprinot Latvijas kritiskās infrastruktūras un digitālo pakalpojumu kibernoturību. Līdz šim analizētas vairāk nekā 100 000 iekārtas 25 organizācijās. Partnerībā ar NATO un Kanādas Bruņoto spēku kiberpavēlniecību, CERT.LV turpina stiprināt starptautisko sadarbību un kolektīvo aizsardzību, kas ir svarīgi ne tikai Latvijas, bet arī visas alianses kiberdrošībai.

Kiberdrošības apdraudējumi un to tendences: Pārskata periodā nav reģistrēti nacionāla līmeņa vai augstas nozīmes apdraudējumi. Nozīmīgi apdraudējumi ar plašu ietekmi uz komerciālo sektoru, valsts un pašvaldību iestādēm veido tikai 0,03% no visiem kategorizētajiem apdraudējumiem, tomēr šajā kategorijā reģistrēto apdraudēto unikālo IP adrešu skaits ir par 218% vairāk nekā 2023. gada 1. ceturksnī; augšupejoša tendence turpinās arī salīdzinājumā ar pagājušā gada 4. ceturksni, pieaugums ir 26%.

Kopš Krievijas pilna mēroga iebrukuma Ukrainā joprojām Latvijā ir novērojams augsts kiberapdraudējumu līmenis. 2024. gada 1. ceturksnī apdraudējumu un incidentu skaits ir samazinājies tikai par 3% salīdzinājumā ar 2023. gada attiecīgo periodu, turklāt tas ir par 5% lielāks nekā pagājušā gada pēdējos trijos ceturkšņos. Tomēr Latvija demonstrējusi pārliecinošu kibernoturību, un līdz šim fiksētie kiberuzbrukumi nav radījuši būtisku vai paliekošu ietekmi uz sabiedrību.

Ielaušanās mēģinājumi, ļaundabīgs kods un kaitīgs saturs ir galvenie apdraudējuma veidi ar lielāko aktivitātes pieaugumu 2024. gada 1. ceturksnī. It īpaši augšupejoša tendence ir ielaušanās mēģinājumiem; salīdzinot ar 2023. gada attiecīgo periodu, pieaugums ir 118%. Pašreizējā ģeopolitiskajā situācijā var pieņemt, ka tas ir skaidrojams ar politiski motivētiem Krievijas hakeru uzbrukumu mēģinājumiem, it īpaši centieniem kompromitēt NATO un ES dalībvalstu kritisko infrastruktūru. Šādas tendences norāda uz nepieciešamību pastiprināt drošības pasākumus un izglītot sabiedrību par potenciālajiem draudiem.

Politiski motivēti pakalpojumu atteices uzbrukumi (DDoS), ko veic Krievijas haktīvistu grupējumi, turpinās viļņveidīgi un ir mērķēti pret valsts pārvaldi un specifisku nozaru uzņēmumiem. Sekmīgo uzbrukumu īpatsvars samazinās, kas liecina par Latvijas infrastruktūras gatavību, Aizsardzības ministrijas finansētās centralizētās DDoS aizsardzības pakalpojuma efektivitāti un sakaru operatoru spēju nodrošināt pakalpojumus nepārtraukta ārēja uzbrukuma gadījumā.

Finansiāli motivētos uzbrukumos visbiežāk izmantotas e-pasta vēstules un īsziņas, kas nāk no šķietami uzticama avota. Pārskata periodā visbiežāk krāpnieki uzdevās par Valsts ieņēmumu dienesta, Valsts policijas, tiesas vai banku pārstāvjiem. Turpinās aktīva smikšķerēšana dažādu kurjerpasta dienestu vārdā, tāpat aktivizējušies krāpnieki ar viltus darba piedāvājumiem. Telefonkrāpnieki sākuši aktīvi izmantot mākslīgā intelekta rīkus, radot imitētas īstu cilvēku balsu versijas**.** 21% upuru iekrīt krāpnieku izliktajās lamatās tieši steigas un neiedziļināšanās dēļ.

Ievainojamības un ietekmējamas sistēmas ir pastāvīgs risks, ko ietekmē jaunatklātās kritiskās ievainojamības, nepareiza IT sistēmu konfigurācija un novecojuši IT risinājumi. Pret organizācijām ar augstu drošības līmeni novēroti piegādes ķēžu uzbrukumi – uzbrucēji iegūst piekļuvi mērķim, veicot uzbrukumus programmatūras izstrādātājiem u.c. ārpakalpojumu sniedzējiem.

DNS ugunsmūra aktīvās aizsardzības efektivitāte: Pārskata periodā DNS ugunsmūra lietotāji tika pasargāti no ļaundabīgām vietnēm vairāk nekā pusmiljons reižu. Ikviens atklātais apdraudējuma indikators nonāk centralizētā aktīvās aizsardzības infrastruktūrā - DNS ugunsmūrī, lai efektīvi pasargātu visus Latvijas iedzīvotājus, uzņēmumus

un organizācijas, kas izmanto CERT.LV nodrošināto aizsardzību. Divu gadu laikā DNS ugunsmūra pakalpojuma lietošana pieaugusi aptuveni 5 reizes, mēnesī apstrādājot ap 1,5 miljoniem DNS pieprasījumu.

Koordinēta ievainojamību atklāšana (CVD): Darbs pie CVD platformas darbības attīstības un popularizēšanas tika turpināts, ieviešot drošības pētnieku reitingu, lai motivētu drošības ekspertus aktīvāk ziņot par atklātajām ievainojamībām, un ieguldot darbu jaunu dalībnieku iesaistē, lai nodrošinātu daudzveidīgu perspektīvu un pieeju ievainojamību pārvaldībā.

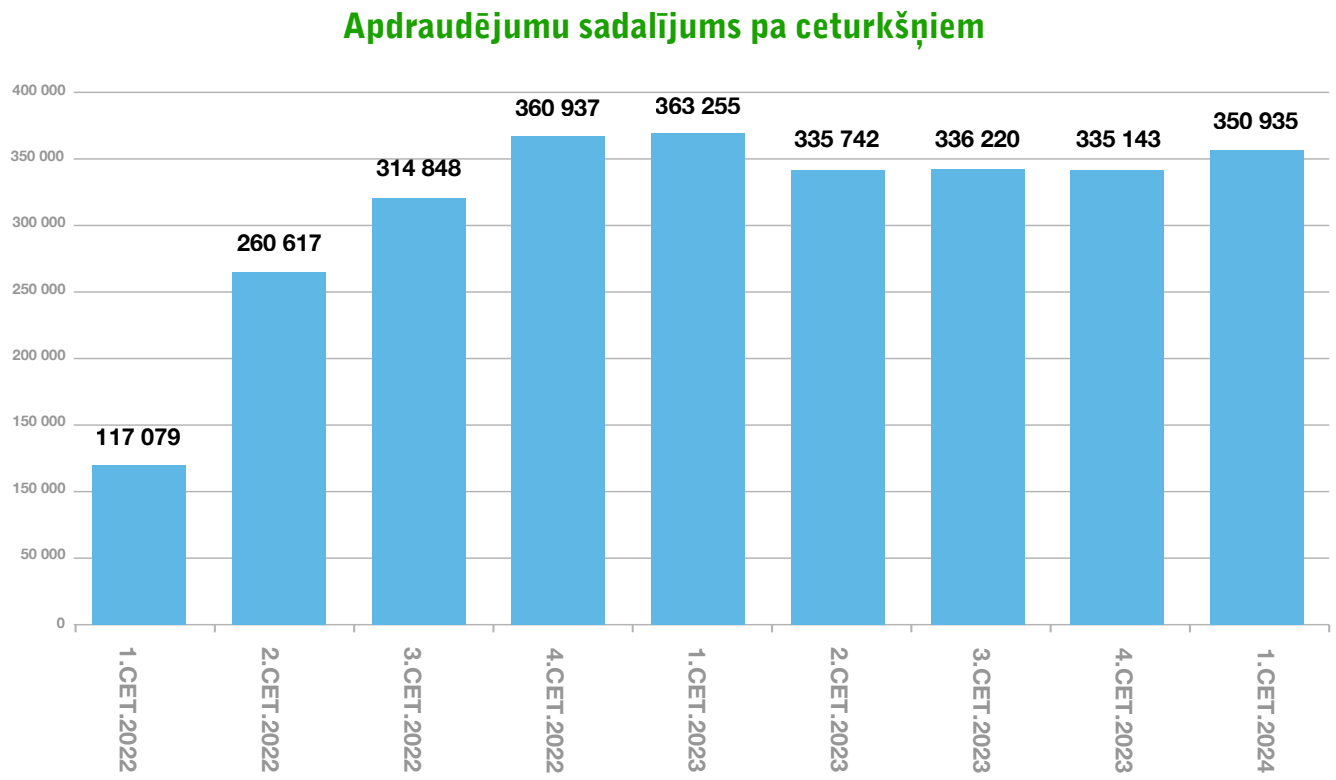
Sabiedrības izglītošana: Pārskata periodā, iesaistoties 31 izglītojošā pasākumā, CERT.LV par IT drošību izglītoja 4737 dalībniekus, veicinot gan individuālu lietotāju, gan organizāciju kiberpratību, lai ikviens spētu nodrošināt savu datu un sistēmu drošību.

CERT.LV turpina veicināt kiberdrošību un būt par uzticamu viedokļa līderi Latvijas kibertelpā.

1. Kibertelpas drošības apdraudējumi: statistika un tendences

Krievijas pilna mēroga iebrukums Ukrainā pirms diviem gadiem ir izraisījis kiberapdraudējumu līmeņa celšanos par 40% Latvijas kibertelpā, un draudu līmenis saglabājas joprojām augsts. Turklāt 2024. gada 1. ceturksnī bija augšupejoša tendence salīdzinājumā ar pēdējiem trim ceturkšņiem.

Pārskata periodā CERT.LV tika reģistrētas 350 935 apdraudētas unikālas IP adreses, kas ir trešais augstākais rādītājs pēdējo divu gadu laikā. Apdraudējumu un incidentu skaits ir samazinājies tikai par 3% salīdzinājumā ar 2023. gada 1. ceturksni, un ir par 5% lielāks nekā pagājušā gada pēdējos trijos ceturkšņos.



1. attēls. Apdraudētās unikālās IP adreses pa ceturkšņiem 2022. - 2024. gadā

CERT.LV vērtējumā Latvija saskaras ar lielākiem kiberdrošības riskiem nekā jebkad iepriekš, taču Latvija ir demonstrējusi pārliecinošu kibernoturību, un līdz šim fiksētie kiberuzbrukumi nav radījuši būtisku vai paliekošu ietekmi uz sabiedrību.

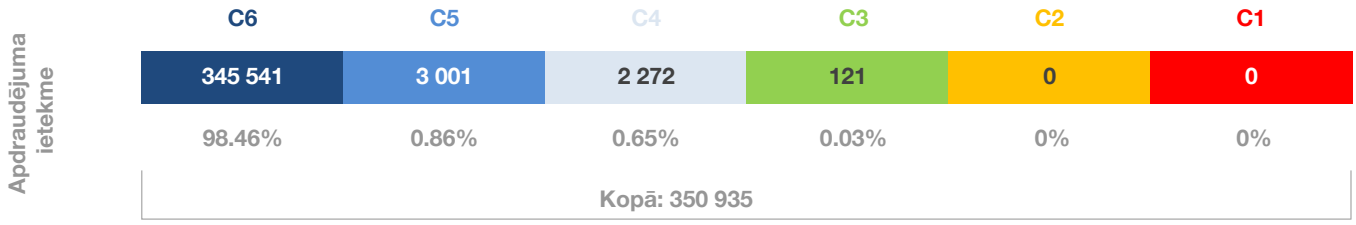
Pārskata periodā apdraudēto unikālo IP adrešu sadalījums matricā

Pilnvērtīgākam kiberdrošības situācijas ikmēneša novērtējumam CERT.LV izmanto Apvienotās Karalistes Nacionālā kiberdrošības centra izstrādāto apdraudējumu matricas metodoloģiju. Matricā ievietotie apdraudējumi tiek grupēti pēc trim būtiskākajiem kritērijiem:

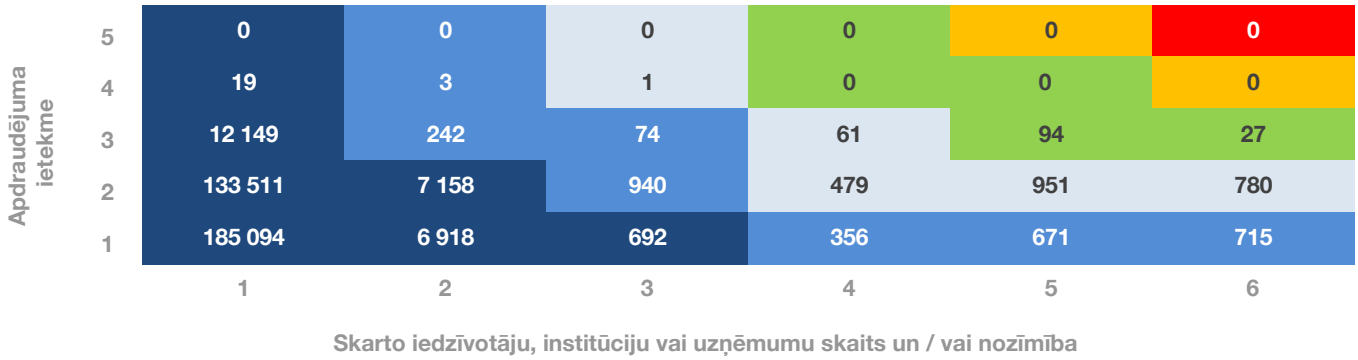
- **cik nozīmīga ir skartā iestāde/uzņēmums;**
- **cik plašu sabiedrības daļu apdraudējums ietekmē;**
- **cik būtiskas sekas attiecīgais apdraudējums radīs.**

Apvienojot visus faktorus un izmantojot krāsas, apdraudējumi 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.



2. attēls. 1. ceturksnī apdraudēto unikālo IP adrešu sadalījums kategorijās pēc apdraudējuma ietekmes



3. attēls. 1. ceturksnī apdraudēto unikālo IP adrešu izvietojums matricā pēc ietekmes, skaita un/vai nozīmības

Pārskata periodā C1 jeb nacionāla līmeņa apdraudējumi un C2 jeb augstas nozīmes apdraudējumi nav reģistrēti.

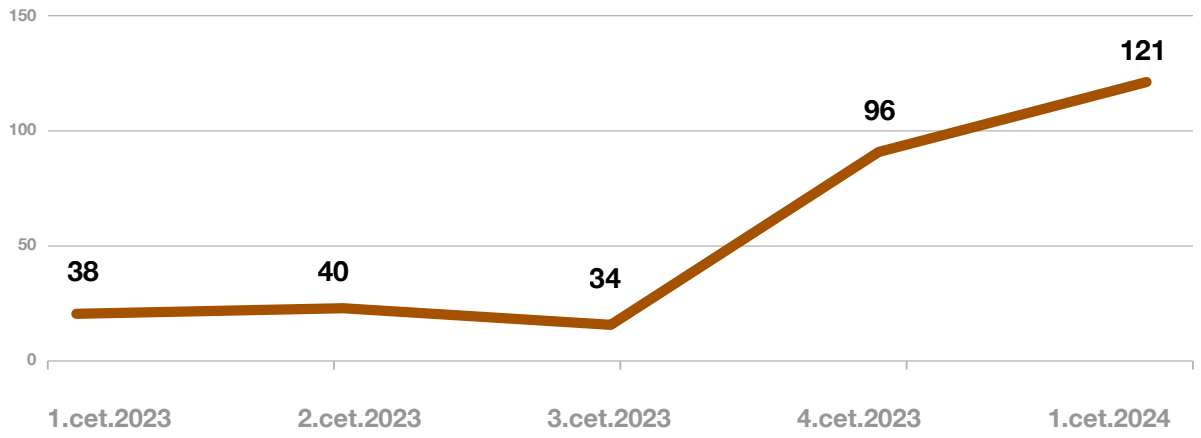
C3 jeb nozīmīgi apdraudējumi ar indikatīvi plašu ietekmi uz komerciālo sektoru, valsts un pašvaldību iestādēm veido 0,03% jeb 121 apdraudēta unikāla IP adrese no visiem kategorizētajiem apdraudējumiem. Fiksētie kiberuzbrukumi C3 kategorijā nav radījuši būtisku vai paliekošu ietekmi uz sabiedrību.

2024. gada 1. ceturksnī C3 kategorijā reģistrēto apdraudēto unikālo IP adrešu skaits ir par 218% vairāk nekā 2023. gada attiecīgajā periodā, kas ir ievērojams pieaugums. Turklāt augšupejoša tendence turpinās arī salīdzinājumā ar pagājušo ceturksni, pieaugums ir 26%.

C3 kategorijā kiberapdraudējumi reģistrēti vairākās pašvaldību un valsts iestāžu, valsts kapitālsabiedrību, veselības aprūpes un izglītības iestāžu, enerģētikas un elektronisko sakaru komersantu iekārtās un sistēmās. Pārskata periodā TOP 3 apdraudējuma veidi:

- **Lielāko daļu apdraudējumu veido ielaušanās mēģinājumi**, kas tika reģistrēti kāda enerģētikas sektora uzņēmuma, atsevišķu valsts un pašvaldības iestāžu, kā arī elektronisko sakaru komersanta iekārtās un sistēmās;
- **Ievērojams skaits ar ļaundabīga koda apdraudējumiem** atsevišķu izglītības un kultūras institūciju, kā arī atsevišķu valsts un pašvaldības iestāžu iekārtās un sistēmās;

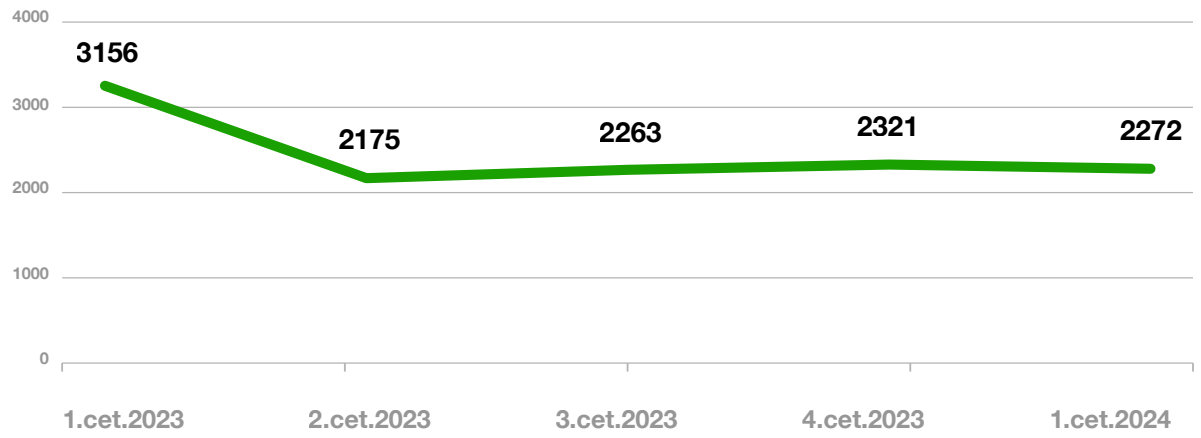
DDoS uzbrukumi, kas tika vērsti pret atsevišķu valsts iestāžu iekārtām un sistēmām, kā arī pret kādu valsts kapitālsabiedrību IKT sektorā.



4. attēls. Apdraudēto unikālo IP adrešu skaits C3 kategorijā

C4 jeb būtiski apdraudējumi ar indikatīvi vidēju ietekmi uz komerciālo sektoru, valsts un pašvaldību iestādēm veido 0,65% jeb 2272 apdraudētas unikālas IP adreses no visiem kategorizētajiem apdraudējumiem. Fiksētie kiberuzbrukumi C4 kategorijā nav radījuši būtisku vai paliekošu ietekmi uz sabiedrību.

2024. gada 1. ceturksnī C4 kategorijā reģistrēto apdraudēto unikālo IP adrešu skaits ir sarucis par 28% salīdzinājumā ar 2023. gada attiecīgo periodu un turpina samazināties, lai gan samazinājums salīdzinājumā ar pagājušo ceturksni ir tikai 2%.



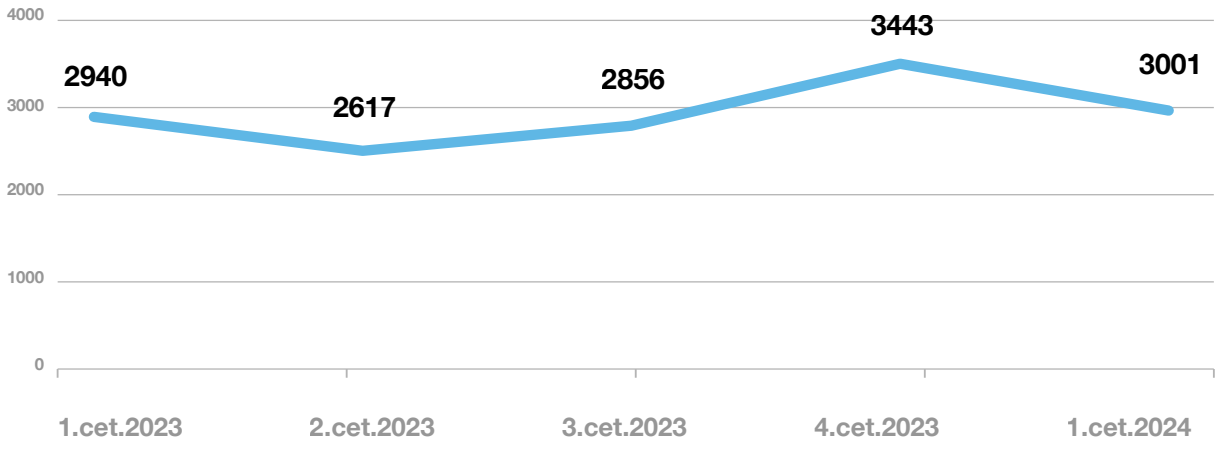
5. attēls. Apdraudēto unikālo IP adrešu skaits C4 kategorijā

Lielākā daļa C4 līmeņa apdraudējumu bija konfigurācijas nepilnības, ievērojamā skaitā ielaušanās mēģinājumi, krāpšanas mēģinājumi, ļaundabīgs kods un DDoS uzbrukumi augstas un vidēji augstas prioritātes iestādēs. Reģistrētas arī kompromitētas iekārtas un informācijas vākšana.

Konfigurācijas nepilnības (*Accessible-ftp, Ntp-version, Ssl-poodle, Dns-open-resolver, Open-telnet* u.c.) fiksētas vairāku pašvaldību un valsts iestāžu, augstskolu, elektronisko sakaru komersantu un citu organizāciju iekārtās un sistēmās. Savukārt ielaušanās mēģinājumi – vairāku pašvaldību un valsts iestāžu, kā arī veselības aprūpes un finanšu iestāžu, augstskolu un citu organizāciju iekārtās un sistēmās. Krāpšanas mēģinājumi fiksēti dažās valsts un pašvaldību iestādēs.

C5 jeb mēreni apdraudējumi ar indikatīvi nelielu ietekmi uz komerciālo sektoru, valsts un pašvaldību iestādēm veido 0,86% jeb 3001 apdraudēta unikāla IP adrese/gadījums no visiem kategorizētajiem apdraudējumiem.

2024. gada 1. ceturksnī C5 kategorijā reģistrēto apdraudēto unikālo IP adrešu skaits ir samazinājies par 13% salīdzinājumā ar pagājušo ceturksni; salīdzinot ar 2023. gada 1. ceturksni pieaugums ir 2%. C5 kategorijā TOP 3 apdraudējuma veidi bija ļaundabīgs kods, ielaušanās mēģinājumi un konfigurācijas nepilnības. Kiberapdraudējumi reģistrēti gan publiskā, gan privātā sektora dažādu iestāžu, organizāciju un komersantu iekārtās un sistēmās.



6. attēls. Apdraudēto unikālo IP adrešu skaits C5 kategorijā

CERT.LV EKSPERTU KOMENTĀRS

Lai arī uzbrukumi notiek viļņveidīgi, jārēķinās, ka Latvija turpinās būt Krievijas politiski motivētu kiberuzbrucēju mērķis, ņemot vērā Latvijas stingro nostāju pret Krievijas agresiju Ukrainā un atbalstu Ukrainai transatlantiskajā integrācijā. CERT.LV komanda nepagurusi strādā pie tā, lai Latvija un Eiropa transatlantiskajā komandā būtu gatava aizsargāt savu kibertelpu pret jebkuru potenciālo kiberuzbrucēju un jebkura scenārija gadījumā, veicinot Latvijas gatavību pretstāvēt 24/7 režīmā, kas ir efektīvākais kiberuzbrucēju atturēšanas līdzeklis.

2. TOP kiberincidenti un apdraudējumi: atbalsts un rekomendācijas to novēršanā

Veicinot IT drošību Latvijā un stiprinot kibernoturību, 2024. gada 1. ceturksnī tika turpināta CERT.LV aktīva sadarbība ar valsts un pašvaldību institūcijām, bankām, elektronisko sakaru komersantiem un citām organizācijām un kiberdrošības ekosistēmas partneriem dažādas bīstamības incidentu risināšanā.

IT drošības incidents - kaitīgs notikums vai nodarījums, kura rezultātā tiek apdraudēta informācijas tehnoloģiju integritāte, pieejamība vai konfidencialitāte.

Ziņošana par incidentiem, sadarbība un informācijas apmaiņa joprojām ir būtiski efektīvas kiberdrošības priekšnoteikumi. CERT.LV turpina regulāri informēt valdības pārstāvjus, valsts institūciju vadītājus un kiberdrošības speciālistus par notikumiem Latvijas kibertelpā.

Tāpat CERT.LV turpina nodrošināt ikmēneša notikumu apkopošanu un analīzi, sniedzot lēmumu pieņēmējiem informāciju, kas nepieciešama, lai savlaicīgi prognozētu un novērstu valsts iekšējo un ārējo apdraudējumu, kā arī uzlabotu valsts kritiskās infrastruktūras aizsardzību un noturību.

Tā kā kiberuzbrukumi nepārtraukti attīstās, lai sabiedrību informētu par jauniem drošības apdraudējumiem un iespējamiem pretpasākumiem, CERT.LV regulāri sniedz ikmēneša pārskatu "Kiberlaikapstākļi" par būtiskākajiem notikumiem kibertelpā TOP 5 kategorijās, publicējot pārskatu tīmekļa vietnes cert.lv sadaļā "Ziņas".

CERT.LV ir valstī lielākais kiberapdraudējumu datu un informācijas apkopotājs, kas automatizēti apstrādā un analizē vairākus miljonus ienākošo signālu mēnesī.

CERT.LV komandas atbalsts incidentu izmeklēšanā		
15-20 manuāli risināti incidenti katru dienu	Vairāk nekā 6,5 miljoni kiberdrošības telemetrijas signālu mēnesī	Atbalsts ikvienam, bet prioritāri: pamatpakalpojumu un digitālo pakalpojumu sniedzējiem, kritiskās infrastruktūras turētājiem un valsts iestādēm

Būtiskākie kiberincidenti un apdraudējumi, kas izgaismo 1. ceturksnī novērotās tendences, aplūkoti turpinājumā - 2.1. līdz 2.6. apakšnodaļās.

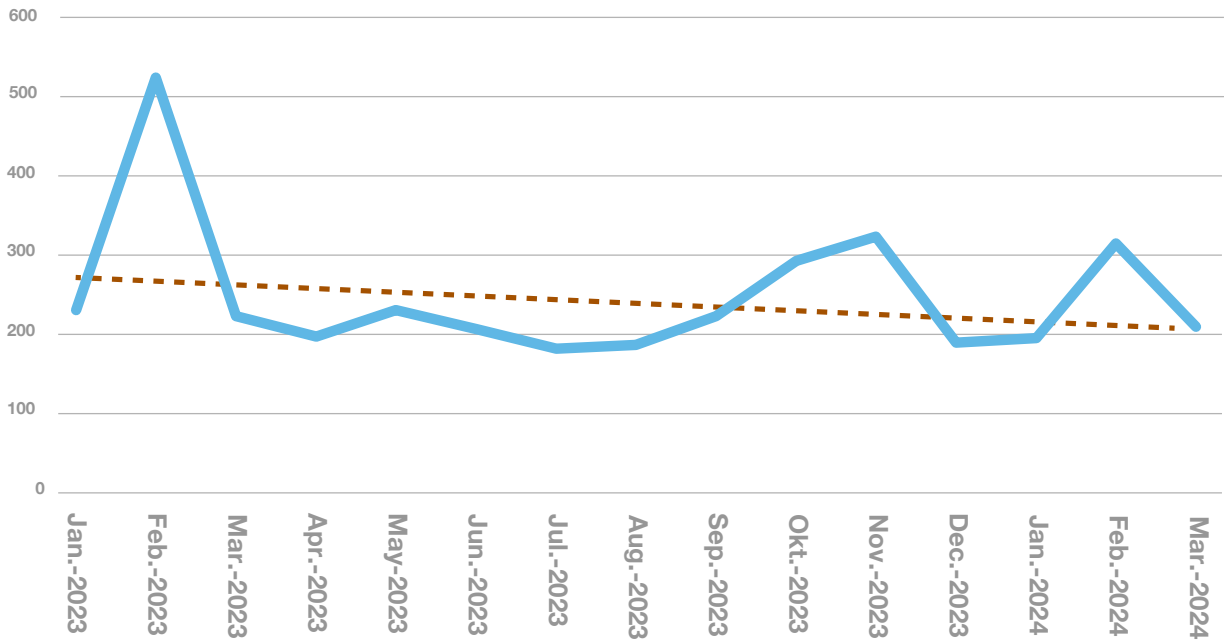
2.1. Krāpšana

CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits apdraudējumu veidā "Krāpšana" ir samazinājies salīdzinājumā ar pagājušo ceturksni un 2023. gada 1. ceturksni.

Pārskata periodā privātpersonas visvairāk tika ietekmētas ar dažādā veida krāpšanas un pikšķerēšanas aktivitātēm, lai izkrāptu kredītkaršu datus un iegūtu piekļuvi privātpersonu un uzņēmumu bankas kontiem.

Pikšķerēšanas kampaņas aizvien "strādā'" kā labi ieeļļots mehānisms, jo piemānīt cilvēku ir vieglāk nekā IT sistēmu, kura regulāri tiek atjaunināta un pasargāta. Turklāt CERT.LV un SKDS veiktā iedzīvotāju aptauja atklāj, ka 21% upuru iekrīt krāpnieku izliktajās lamatās tieši steigas un neiedziļināšanās dēļ.

Krāpnieki arvien gudrāk iedarbojas uz emocijām, piepildot potenciālā upura gaidas vai liekot rīkoties impulsīvi. Neuzmanība vai zināšanu trūkums par jauniem krāpniecības veidiem upurim var izmaksāt ļoti dārgi. Pie CERT.



7. attēls. Apdraudēto unikālo IP adrešu skaits

LV ir vērsušies vairāki simti šāda veida krāpšanas upuru, kas zaudējuši no dažiem desmitiem līdz vairākiem desmitiem tūkstošu eiro. Lielākās summas zaudējuši tie, kas paši apstiprinājuši internetbankas piekļuvi.

Kiberuzbrucēja primārais mērķis ir piekļuve upura internetbankai, pierunājot ievadīt/apstiprināt aktivizācijas kodus, lai aktivizētu krāpnieku pieslēgumu internetbankai, vai arī uzstādīt upura datorā vai tālrunī attālinātas piekļuves rīkus, visbiežāk – "AnyDesk", lai iespējotu krāpnieku piekļuvi upura ierīcēm.

Kā, piemēram, kliedzošs gadījums noticis februārī ar kādu personu no Kuldīgas, kurai izkrāpti 160 000 eiro. Personai zvanīja krāpnieki, kuri uzdevušies par bankas un policijas darbiniekiem, nosūtot viltus apliecību ar Valsts policijas priekšnieka foto. Viņi pieprasīja instalēt "AnyDesk" lietotni, pārliecinot upuri, ka viņa bankas kontos notiekot krāpnieciskas darbības, tāpēc nauda ir jāpārskaita vai jānosūta viņiem, lai nauda būtu drošībā. Persona apstiprināja bankas lietotāja datus un PIN kodus, kā rezultātā no saviem un darbavietas kontiem pārskaitīja aptuveni 150 000 eiro, turklāt pakomātā ievietoja vēl 10 000 eiro skaidrā naudā.

Krāpšanas shēmas nemitīgi tiek uzlabotas un pielāgotas aktualitātēm sabiedrībā, piemēram, ikgadējā pārmaksāto nodokļu atgūšana vai ienākumu deklarāciju iesniegšana VID; romantiskā krāpšana un šantāža Valentīna dienas aizsegā u.c.

Upurus krāpnieki visbiežāk uzrunā krievu valodā, bet arvien vairāk fiksēta arī labas un precīzas latviešu valodas lietošana. Krāpnieki izliekas par dažādu Latvijas valsts iestāžu pārstāvjiem vai dažādu uzņēmumu (piemēram, "Google" u.c.) palīdzības dienestiem. Joprojām krāpnieki uzdodas par Valsts policijas un Valsts ieņēmumu dienesta pārstāvjiem, kā arī aktīvi uzdodas par banku pārstāvjiem, norādot uz nelikumīgām darbībām vai neapstiprinātiem pārskaitījumiem no potenciālā upura konta.

CERT.LV EKSPERTU KOMENTĀRS

Krāpnieki negrib, lai jūs atvērtu vaļā datoru un aplūkotu informāciju lielajā ekrānā. Viņi grib, lai Jūs visu darītu telefonā, kura ekrāns ir mazs, tāpēc domēna vārdi netiek rūpīgi apskatīti. Turklāt pilnās adreses ekrānos daļēji ir apslēptas, lai ietaupītu vietu. Tieši viedtālruņu vidē krāpniekiem nereti veicas vislabāk – cilvēki noklikšķina uz saņemtās saites. Apstākļi, kas paaugstina kļūdīšanās iespējamību - steiga, nogurums, neparasta situācija, procedūru neesamība vai to nepārzināšana, mazs ekrāns - mazina analītisku pieeju situācijai un palielina iespējamību, ka uzbrukums netiks atpazīts.

Aizvien aktuālas ir arī viltus tirdzniecības platformas internetā. Tāpat "garnadži" aicina apmeklēt kurjerpakalpojumu (piemēram, "Omniva", "Latvijas Pasts" u.c.) sniedzēju vietnes, lai it kā precizētu piegādes adresi, veiktu piegādes apmaksu par it kā aizkavētu sūtījumu, apmaksātu muitu vai veiktu citas darbības.

Joprojām aktuāls ir krāpšanas veids, kur sūtītājs, uzdodoties par īsziņas saņēmēja bērnu, raksta par it kā salūzušu telefonu, aizmirstu maku vai iekļūšanu ceļu satiksmes negadījumā, lūdz viņam steidzami pārskaitīt naudu.

Smikšķerēšanas un pikšķerēšanas nolūks ir panākt, lai persona, atverot nosūtītajā ziņā esošo saiti, lejupielādētu ļaunatūru vai veiktu citu sev kaitīgu darbību.

Smikšķerēšana ir kiberuzbrukuma veids, kurā tiek izmantoti teksta paziņojumi, piemēram, SMS vai ziņas "WhatsApp". Pikšķerēšana ir identisks uzbrukums, visbiežāk sūtot ziņas uz elektronisko pastu.

Finansiāli motivētos uzbrukumos turpina izmantot smikšķerēšanas un pikšķerēšanas kombināciju, kā arī dažādas krāpnieciskas investīciju platformas. Pret uzņēmumiem turpinās darījuma sarakstes kompromitēšanas uzbrukumi, piekļūstot uzņēmuma e-pasta sarakstei un reālos darījumos piesūtot viltus rēķinus ar mainītiem maksājumu rekvizītiem.

Pikšķerētāji mēģina panākt, lai persona izpaustu savu personīgo informāciju, noklikšķinātu uz ļaunprātīgas saites vai atvērtu inficētu e-pasta vēstules pielikumu. Uzbrukuma ieroču arsenālā visbiežāk ir e-pasta vēstules no šķietami uzticama avota, aktīvi izmanto arī īsziņas, ziņas sociālajos medijos un telefona zvanus.

Telefonkrāpnieki sākuši aktīvāk izmantot mākslīgā intelekta rīkus, veicot robotzvanus, un sarunas laikā cenšoties no zvana adresāta izvilināt privātu informāciju, piemēram, personas datus, internetbankas pieejas un citu informāciju. Krāpniecisko zvanu veikšanai tiek izmantotas iepriekš internetā ierakstītas īstu cilvēku balsis, kas tiek apstrādātas ar īpašu mākslīgā intelekta programmatūru, radot imitētas balsu versijas.

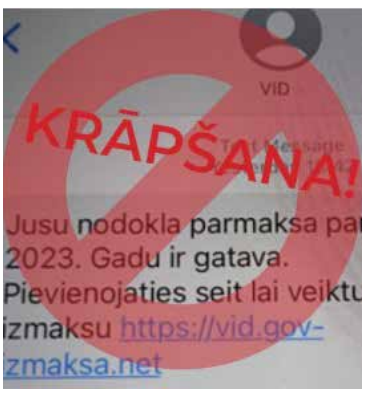
Tā kā daudzviet pasaulē šogad notiks vēlēšanas, tajā skaitā Eiroparlamenta vēlēšanas, pastiprināta uzmanība tiks pievērsta dezinformācijas kampaņu apkarošanai. Kiberdrošības pasākumi būs ļoti svarīgi, lai pasargātu no dezinformācijas un manipulācijām.

CERT.LV EKSPERTU KOMENTĀRS

Mākslīgā intelekta (MI) progress rada riskus un bažas par dziļviltojumiem, kurus varēs izmantot gan labiem, gan arī ļauniem mērķiem, lai destabilizētu sabiedrību. MI veidotie attēli, video, kurā izmantotas balss klonēšanas programmatūras, būs viena no "karstākajām" tendencēm šogad gaidāmajās Eiroparlamenta vēlēšanās. Vēlētājam būs jāspēj izvērtēt ne tikai politiķu solījumus, bet arī to, vai runātājs, kas redzams ierīces ekrānā, patiešām ir īsta persona vai MI radīts prasmīgs viltojums.

Pārskata periodā izplatītākās TOP 5 krāpšanas shēmas

Krāpnieku galvenā ēsma pavasarī – ienākumu deklarācijas: Krāpnieki seko līdzi aktualitātēm, izmanto to savā labā un arvien aktivizējas brīdī, piemēram, kad iedzīvotājiem aktuāla kļūst ikgadējā pārmaksāto nodokļu atgūšana.



Februārī un martā krāpnieki iedzīvotājiem masveidā sūtīja viltus īsziņas un e-pastus Valsts ieņēmumu dienesta (VID) vārdā, rakstot, ka sagatavots nodokļu pārmaksas dokuments par iepriekšējo gadu. Šai īsziņai/e-pastam tiek pievienota krāpnieciska saite, kas nesakrīt ar VID oficiālo vietņu adresi.

CERT.LV atgādina, ka neviena valsts institūcija un to pārstāvji e-pasta ziņojumos vai telefonsarunās nemudinās uz tūlītēju rīcību un neaicinās dalīties

ar bankas konta pieejas vai maksājumu karšu datiem. Par zvana vai ziņas leģitimitāti jāpārliecinās, apmeklējot iestādes tīmekļa vietni un sazinoties, izmantojot vietnē norādīto telefona numuru.

Smikšķerēšana dažādu kurjerdienestu vārdā, izplatot aicinājumu apmeklēt šo pasta pakalpojumu sniedzēju vietnes, lai precizētu piegādes adresi, apmaksātu muitu vai veiktu citas darbības.

Ziņojumos iekļautās saites ved uz kādu no saišu īsināšanas servisiem (urlz.com, u.to, lnkd.in, az3.in, linkr.it, inx.lv un citiem), kas pārvirza potenciālo upuri uz krāpnieku izveidotu vietni. To noformējums atdarina izmantotā servisa mājaslapas izskatu.

Viltvārži "Latvijas Pasts" vārdā masveidā sūtīja īsziņas ar melīgu informāciju par kavētām vai nepareizi norādītām piegādēm. Šāda īsziņa satur bīstamu saiti, kur upuris tiek mudināts sniegt personīgos datus krāpniecības vietnē.

Aktivizējušies uzbrukumi, izmantojot vietnes ss.lv un "Facebook Marketplace", kur pircēji tiek aizvedināti uz krāpnieciskām vietnēm.

Jauns krāpniecības vilnis ar viltus darba piedāvājumiem: Pārskata periodā konstatēti datu izvilināšanas mēģinājumi ziņapmaiņas platformā "WhatsApp", kur viltvārži uzdodas par uzticamu organizāciju, piemēram "WorkingDay Global" vai "Alliance Recruitment" darbiniekiem. Krāpnieki aicina potenciālos darbiniekus uz interviju, lai izvilinātu viņu internetbankas pieejas datus. CERT.LV aicina iedzīvotājus būt piesardzīgiem, nekavējoties pārtraukt sarunu un bloķēt šādus numurus, un nekādā gadījumā neizpaust personas datus, elektronisko maksāšanas līdzekļu datus un citu personīga rakstura informāciju.

Romantiskā krāpšana jeb jauns veids, kā šantažēt upurus: Februārī aktivizējās romantiskie krāpnieki, kas izmanto uzticēšanos, lai izspiestu naudu vai iegūtu upura kailfoto šantāžai. Nolūkā piesaistīt uzmanību, šie krāpnieki izveido pievilcīgus profilus "Facebook", "Instagram" vai "Tinder", un "lūdz" aizdot naudu, vai ieguldīt kriptovalūtā, vai ieguldījumu kontos. Vienā gadījumā izspiesta nauda vairāk nekā 2000 eiro, bet citā gadījumā naudas vietā pieprasītas sociālo mediju paroles, ko kāds iedzīvotājs nosūtīja un zaudēja piekļuvi saviem sociālo mediju profiliem.

Kādas pazīmes var liecināt par romantisko krāpšanu un kā no tās izvairīties, plašākai auditorijai videoformātā noderīgus ieteikumus sniedz CERT.LV kiberdrošības speciāliste: https://www.youtube.com/watch?v=Sv1Ka0oX9Po&t=105s.

Ir novērota jauna tendence izkrāpt bankas piekļuves informāciju tiesvedības datu monitoringa vietnes elieta.lv vārdā, kur ziņas saņēmēju apsūdz "Facebook Marketplace" krāpšanā. Kiberuzbrukumâ tiek izmantota smikšķerēšana jeb krāpniecisku īsziņu sūtīšana, lai persona, atverot nosūtītajā ziņā esošo saiti, lejupielādētu ļaunatūru vai veiktu citu sev kaitīgu darbību. Kā atpazīt krāpniecisku īsziņu jeb smikšķerēšanas mēģinājumu, skaidro CERT.LV kiberdrošības speciālists: https://jauns.lv/raksts/zinas/595637-video-patiesiba-par-meliem-uzmanies-vid-iszinas-nesuta-bet-krapnieki-gan.

IETEIKUMI DROŠĪBAI

Lai pasargātu visus Latvijas iedzīvotājus, uzņēmumus un organizācijas no kiberkrāpniekiem, CERT.LV aicina ikvienu personu ievērot piesardzības principus un preventīvas darbības:

- Pārbaudiet avotus un datu precizitāti: esiet piesardzīgi un kritiski izvērtējiet saņemtās ziņas patiesumu un sūtītāja e-pasta adresi un saturu, rūpīgi pievēršot uzmanību arī valodas kļūdām un stilam.
- Pirms atvērt saiti, izpētiet un pārliecinieties, ka tā ir droša un uzticama: novietojot kursoru virs saites, iespējams aplūkot vietnes adresi, uz kuru šī saite aizvedīs. Veiciet elektroniskos maksājumus tikai drošās interneta vietnēs. Pie interneta adreses pārlūkā ir jābūt atslēgas simbolam vai tai jāsākas ar https://.
- Neuzticieties svešiem ziņojumiem un neievadiet savus personas datus: ja jums ir šaubas par kādu informāciju, zvaniet uz attiecīgās organizācijas oficiālo tālruni un pārbaudiet to.
- Papildu aizsardzībai izmantojiet divu faktoru autentifikāciju: tas pasargās no konta pārņemšanas, pat ja uzbrucējs būs ieguvis jūsu paroli.
- Nav jāpakļaujas krāpnieku prasībām jūsu viedierīcēs instalēt attālinātas piekļuves programmatūru. Nepieļaujiet, ka krāpnieks var rīkoties ar jūsu ierīci un identitāti!
- Ziņojiet par krāpnieku aktivitātēm un ļaundabīgām vietnēm, pārsūtot kaitīgos e-pastus uz cert@cert.lv. Instrukcija, kā pareizi pārsūtīt: https://cert.lv/lv/kontakti/ka-parsutit-kaitigus-e-pastus
- Izmantojiet CERT.LV un NIC.LV nodrošinātu efektīvu bezmaksas aktīvo aizsardzību – https://dnsmuris.lv/, lai pasargātu sevi un darbiniekus no krāpnieciskām vietnēm.

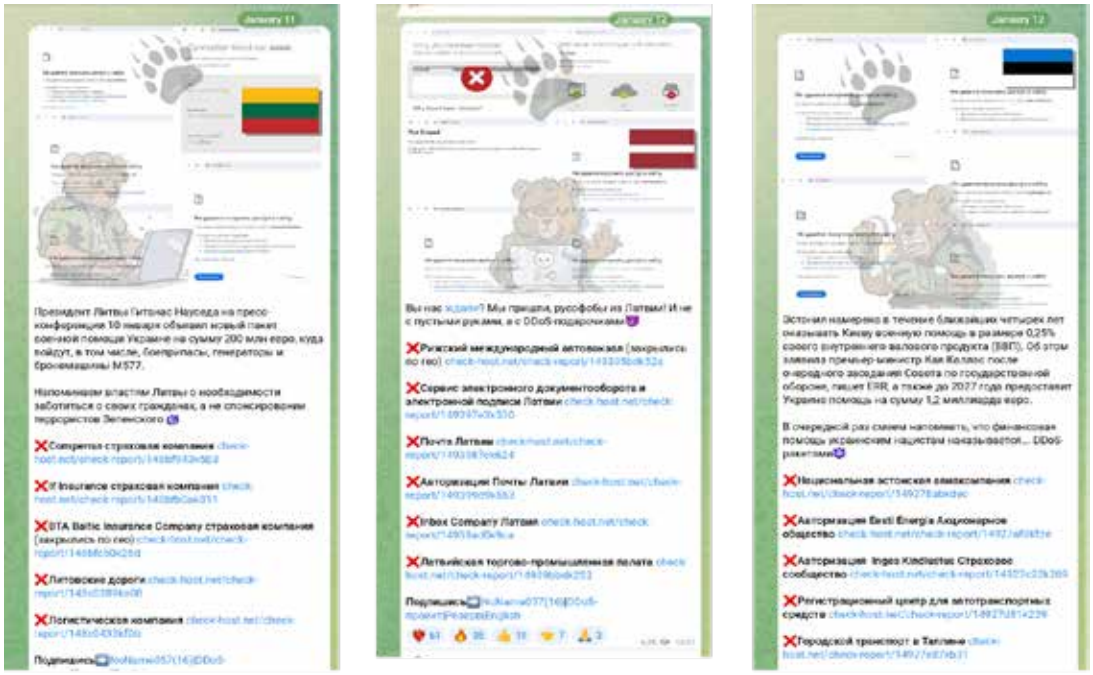
2.2. Pakalpojuma pieejamība (DDoS)

Politiski motivēti pakalpojumu atteices uzbrukumi (DDoS), ko veic Krievijas haktīvistu grupējumi, turpinās viļņveidīgi un mērķēti pret valsts pārvaldi un specifisku nozaru uzņēmumiem. Pārskata periodā DDoS uzbrukumi tika vērsti pret vairākiem desmitiem interneta pakalpojumu sniedzēju un nozīmīgu valsts sektora pakalpojumu sniedzēju tīmekļa vietņu. Pateicoties labi sagatavotām daudzpakāpju aizsardzības sistēmām un procesiem, vairumā gadījumu šie uzbrukumi neietekmēja resursu darbību vai arī to ietekme bija īslaicīga un nenozīmīga.

DDoS mērķis – pārpludināt mājaslapas serverus ar milzīga apjoma pieprasījumiem no ārpuses, cenšoties panākt, lai mājaslapas serveri netiktu galā ar šiem pieprasījumiem, un lapa vienkārši nebūtu pieejama publiski.

Politiski motivēti DDoS veicēji - kibernoziedznieki ir Krievijas spēka struktūrās integrēti izpildītāji, kuri pilda dotos uzdevumus. Viņu mērķis ir noslogot interneta infrastruktūru Ukrainas atbalstītājiem NATO valstīs, arī Latvijā. Tā, piemēram, marta vidū daudzu Igaunijas valsts iestāžu tīmekļa vietnes skāra līdz šim Igaunijā lielākais DDoS uzbrukumu vilnis. Atbildību par uzbrukumiem lielākoties uzņēmušies prokremliskie haktīvistu grupējumi.

CERT.LV novērojumi par situāciju kibertelpā rāda, ka aktīvi uzsaukumi Krievijas agresiju atbalstošo haktīvistu "Telegram" kanālos veikt DDoS uzbrukumus konkrētās valsts infrastruktūrai sekoja pēc Ukrainas prezidenta Volodomira Zelenska oficiālajām vizītēm 11. janvārī – Lietuvā, 12. janvārī – Latvijā un Igaunijā. Uzsaukumos iekļautā informācija nav tieši sasaistāma ar V. Zelenska vizīti, tomēr zīmīgi, ka tie notikuši uzreiz pēc tās. Pēc CERT.LV esošās informācijas notikušie DDoS uzbrukumi Latvijā bija bez ietekmes – interneta resursu darbības traucējumi Latvijas kibertelpā netika novēroti.



8. attēls. Ekrānšāviņi no uzsaukumiem "Telegram" kanālos krievu valodā

Lai arī uzbrukumi notiek viļņveidīgi, jārēķinās, ka politiski motivēta uzbrucēju pastiprināta interese par Latvijas resursiem saglabāsies. Attiecīgi sistēmu uzturētājiem proaktīvi jārūpējas par resursu atjaunināšanu, jāstiprina savas kiberdrošības pārvaldība un jāseko līdzi drošības ieteikumiem.

CERT.LV EKSPERTU KOMENTĀRS

DDoS uzbrukumi ir kā lietusgāze, kas parāda vājās vietas noteces sistēmā. Latvija ir iemācījusies labāk izturēt kiberuzbrukumus, un šāda kibernoturība ir viena no mūsu priekšrocībām salīdzinājumā ar citām valstīm. Runājot par prognozēm, DDoS uzbrukumi, visticamāk, tiks veiksmīgāk pielāgoti, kā rezultātā varētu pieaugt uzbrukumu skaits ar jūtamu ietekmi. Pieaugs mākoņpakalpojumu sniedzēju serveru izmantošana DDoS uzbrukumiem. Tāpat DDoS uzbrukumu intensitāti varētu palielināt IoT ierīces, jo tām biežāk mēdz būt zemāks aizsardzības līmenis, un tās ir vienkāršāk kompromitējamas. Turpināsies arī politiski motivēti DDoS uzbrukumi.

Pārskata periodā CERT.LV sadarbībā ar FIRST *(Forum of Incident Response Security Teams)* izplatīja aicinājumu elektronisko sakaru komersantiem, kritiskās infrastruktūras uzturētājiem un pamatpakalpojumu sniedzējiem pilnveidot BGP *(Border Gateway Protocol)* konfigurāciju, ievērojot labo praksi, lai stiprinātu BGP sesiju aizsardzību. Aicinājums attiecas arī uz citām Latvijas iestādēm un organizācijām, kas savā infrastruktūrā uztur BGP.

Pērn FIRST fiksēja divus šādus gadījumus, kad pret divām organizācijas BGP sesijām tika īstenots sekmīgs DDoS uzbrukums (TCP 179 ports), un abas sesijas tika pārtrauktas. IT drošības organizācija "Shadowserver" un "Shodan" serviss apkopojušas informāciju par +300 000 BGP 179 porta sesijām, kas pakļautas riskam un varētu kļūt par mērķi līdzīgiem uzbrukumiem.

Latvijā konstatēti ap 150 šādi internetā eksponēti BGP servisi. Vienlaicīgi uzbrukumi šiem servisiem varētu radīt nopietnas sekas un globālu "haosu internetā".

Pārskata periodā CERT.LV no savas puses ir izsūtījusi brīdinājumus visām iestādēm un organizācijām, kurām TCP 179 ports ir eksponēts internetā un kas atrodamas "Shadowserver" un "Shodan" sarakstos. Plašāk: https://cert.lv/lv/2024/01/ddos-uzbrukumi-bgp-sesijam

IETEIKUMI DROŠĪBAI

Efektīvai kiberhigiēnai un kibernoturībai jebkuras organizācijas ietvaros ir būtiska loma cīņā gan pret finansiāli, gan pret politiski motivētiem kiberuzbrukumiem. CERT.LV ir apkopojusi sagatavošanās darbus, kas jāizpilda, stiprinot kibernoturību pret potenciāliem DDoS uzbrukumiem, lai mazinātu vai novērstu šāda uzbrukuma ietekmi, kā arī aicina sekot līdzi labās prakses vadlīnijām. Katrai organizācijai jāizvērtē uzskaitīto punktu prioritāte un jāveic ieviešana, ņemot vērā savas infrastruktūras specifiku. Plašāk: https://cert.lv/lv/2022/08/ieteikumi-ddos-ietekmes-mazinasanai

CERT.LV aicina sazināties ar CERT.LV komandu gadījumos, ja ir nepieciešams atbalsts incidenta izmeklēšanā, seku novēršanā un prevencijas plānošanā, zvanot uz 67085888 vai rakstot uz cert@cert.lv.

2.3. Ievainojamības un konfigurācijas nepilnības

Līdzīgi kā iepriekšējos ceturkšņos, arī 2024. gada 1. ceturksnī izplatījās kritiskas ievainojamības, bet tas, kas padarīja šo ceturksni neparastu, bija jaunatklāto ievainojamību skaits un to atklāšanas biežums.

CERT.LV regulāri veic visaptverošu CVE monitoringu, kas ir sasaistāms ar eksponētiem servisiem/iekārtām. 1. ceturksnī CERT.LV proaktīvi izplatīja 13 brīdinājumus par dažādām jaunatklātām kritiskām ievainojamībām, tostarp individuāli apziņoja ievainojamo sistēmu turētājus, kā arī atbalstīja incidentu analīzē un novēršanā, sniedzot koordinētus norādījumus un ieteikumus kiberdrošības pārvaldības stiprināšanai.

Janvārī izgaismojās vairākas kritiskas ievainojamības, kas ļauj kiberuzbrucējiem izmantot attālinātu koda izpildi (*Remote Code Execution* jeb RCE), lai iekļūtu ievainojamajā sistēmā. Šīs ievainojamības ietver arī tādas, kas dod iespēju neautentificētam vai neautorizētam lietotājam piekļūt sistēmai un nesankcionēti nolasīt sistēmā glabāto informāciju, un pēc tam, iespējams, mēģināt izpildīt RCE.

Februārī atklāta kritiska ievainojamība *MS Exchange Server* programmatūrā (CVE-2024-21410), kas sniedz neautentificētam uzbrucējam iespēju iegūt paaugstinātas jeb privileģētas piekļuves tiesības. Tāpat konstatētas divas

Par ievērojamākajām ievainojamībām un ieteikumiem to novēršanai CERT.LV ar elektronisko sakaru komersantu starpniecību regulāri informē lietotājus arī tīmekļa vietnē: https://www.esidross.lv/informacija-par-apdraudejumiem/

ievainojamības *Fortinet FortiSIEM* programmatūrā (CVE-2024-23108 un CVE-2024-23109), kas uzbrucējam ļauj apiet autentifikācijas validāciju un neautentificējoties veikt nesankcionētu komandu izpildi, izmantojot tam speciāli sagatavotus API pieprasījumus.

Martā atklātas vairākas kritiskas ievainojamības *VMware* programmatūrā. Ievainojamības (CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255) sniedz uzbrucējam iespēju veikt koda izpildi uz iekārtas, kura uztur *VMware* virtuālo mašīnu. Tāpat augsta riska ievainojamība atklāta *Cisco Secure Client* programmatūrā, kas izpildās gadījumos, kad tiek izmantota tīmekļa spraudņa paplašinājuma funkcija. Ievainojamība CVE-2024-20337 ir saistīta ar nepietiekamu lietotāja ievades datu validāciju. Uzbrucējs var izmantot šo ievainojamību, pārliecinot lietotāju VPN sesijas izveides laikā noklikšķināt uz viltotas saites.

Kritisko ievainojamību saraksts 2024. gada 1. ceturksnī

CVE	Ietekmētie produkti	Apraksts
CVE-2023-48795	*SSH*	SSH protokola ievainojamība, kura skar OpenSSH paplašinājumu funkcijas. Šīs ievainojamības izmantošana ļauj uzbrucējam pazemināt drošības līmeni lietotāja iekārtā vai arī to pilnībā atslēgt. Vairāk: https://cert.lv/lv/2024/01/kritiska-ssh-protokola-ievainojamiba-cve-2023-48795
CVE-2023-51467	*Apache OFBiz*	Kritiska "nulles dienas" ievainojamība Apache OFBiz atvērtā koda risinājumā, kas paredzēts uzņēmuma resursu plānošanai (Enterprise Resource Planning jeb ERP). To izmanto, piemēram, Atlassian Jira. Vairāk: https://cert.lv/lv/2024/01/kritiska-apache-ofbiz-ievainojamiba-cve-2023-51467
CVE-2023-46805 **CVE-2024-21887**	*Ivanti Connect Secure un Ivanti Policy Secure*	Apvienojot abas ievainojamības (autentifikācijas apiešana un komandu injekcija web komponentēs), uzbrucējam ir iespējams neautentificējoties izpildīt patvaļīgas komandas ievainojamās sistēmās.
CVE-2024-0402	*GitLab*	Vairākas ievainojamības Gitlab CE/EE (Community un Enterprise Edition) programmatūrā, to starpā arī kritiska ievainojamība, kas ietekmē visas versijas no 16.0 līdz 16.5.8, 16.6 līdz 16.6.6, 16.7 līdz 16.7.4, un 16.8 līdz 16.8.1. Ievainojamību var izmantot brīdī, kad tiek veidota jauna darba virsma (workspace), un tā ļauj autentificētiem lietotājiem veidot jaunas datnes ar GitLab programmatūru nesaistītās lokācijās. Vairāk: https://cert.lv/lv/2024/01/atklatas-vairakas-ievainojamibas-gitlab-programmatura
CVE-2024-21410	*Microsoft Exchange*	Kritiska (CVSS vērtējums 9.8) ievainojamība Microsoft Exchange Server programmatūrā. Ievainojamība sniedz neautentificētam uzbrucējam iespēju iegūt paaugstinātas piekļuves tiesības (privilege escalation), un tiek aktīvi izmantota uzbrukumos. Vairāk: https://cert.lv/lv/2024/02/kritiska-ievainojamiba-ms-exchange-server-programmatura
CVE-2024-23108 **CVE-2024-23109**	*Fortinet FortiSIEM*	Divas kritiskas ievainojamības Fortinet FortiSIEM programmatūrā, kas uzbrucējam sniedz iespēju apiet autentifikācijas validāciju un neautentificējoties veikt nesankcionētu komandu izpildi, izmantojot tam speciāli sagatavotus API pieprasījumus. Vairāk: https://cert.lv/lv/2024/02/atklatas-kritiskas-ievainojamibas-fortinet-fortisiem-programmatura-cve-2024-23108-un-cve-2024-23109
CVE-2023-22527	*Confluence*	Kritiska ievainojamība Confluence Data Center un Server programmatūrā, kas ļauj neautentificētam uzbrucējam veikt attālinātā koda izpildi (RCE). CVSS jeb kopējā ievainojamības punktu skaitīšanas sistēmas 10 ballu skalā šīs ievainojamības vērtējums ir 10. Ietekmētas novecojušās Confluence Data Center un Server 8 versijas pirms 2023. gada 5. decembra, kā arī 8.4.5 versija. Vairāk: https://cert.lv/lv/2024/01/kritiska-ievainojamiba-confluence-data-center-un-server-cve-2023-22527
CVE-2024-20337	*Cisco Secure Client*	Augsta riska ievainojamība, kas izpildās gadījumos, kad tiek izmantota tīmekļa spraudņa paplašinājuma funkcija. Vairāk: https://cert.lv/lv/2024/03/augsta-riska-ievainojamiba-cisco-secure-client-programmatura
CVE-2024-22252 **CVE-2024-22253** **CVE-2024-22254** **CVE-2024-22255**	*VMware*	Vairākas kritiskas ievainojamības VMware programmatūrā, kas sniedz uzbrucējam iespēju veikt koda izpildi uz iekārtas, kura uztur VMware virtuālo mašīnu. Vairāk: https://cert.lv/lv/2024/03/atklatas-vairakas-kritiskas-ievainojamibas-vmware-programmatura

Lielākā daļa uzbrukumu tiek veikti, izmantojot publiski zināmas ievainojamības, nevis jaunatklātas ievainojamības (zero-day), tāpēc savlaicīgai ievainojamu sistēmu apzināšanai un ievainojamību lāpīšanai (patching) ir potenciāls būtiski uzlabot kiberdrošības situāciju.

CERT.LV EKSPERTU KOMENTĀRS

Neapšaubāmi - jaunatklātas ievainojamības ir aktuāla tēma, taču tā mēdz aizēnot faktu, ka liela daļa kiberuzbrucēju izmanto publiski sen zināmās ievainojamības, kurām izstrādātājs ir izlaidis "ielāpu", taču lietotājs nav veicis atjauninājumus. Neizpildot svarīgus atjauninājumus, kibernoziedznieki var brīvi iekļūt sistēmā, piekļūt konfidenciālai informācijai vai izraisīt citas negatīvas sekas.

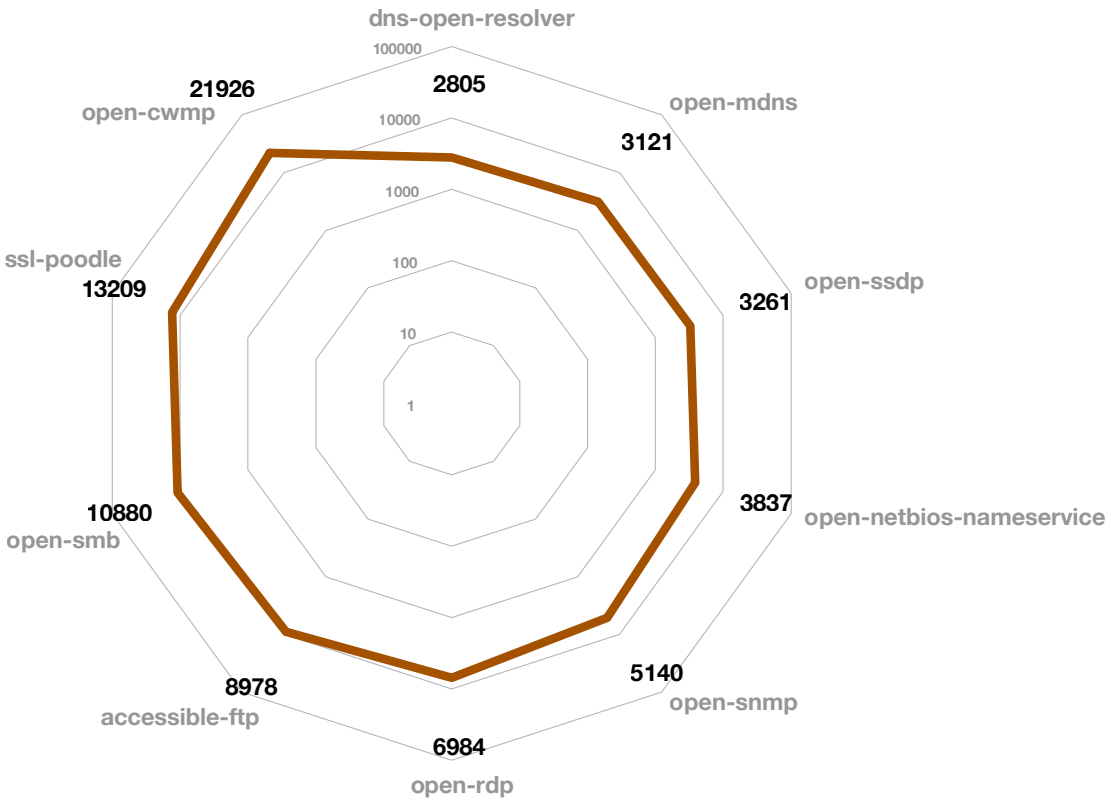
Konfigurācijas nepilnību TOP 10

2024. gada 1. ceturksnī **konfigurācijas nepilnību topa līderis ir *Open-cwmp*** - pārvaldības protokols, kas tiek izmantots, lai nodrošinātu individuālu iekārtu, piemēram, maršrutētāju vai VoIP telefonu pieslēgšanos pie telekomunikāciju pakalpojumu sniedzēja nodrošinātā tīkla. Lai šim pārvaldības rīkam novērstu neautorizētas piekļuves riskus, tiek rekomendēts ierobežot piekļuves tiesības, piemēram, izmantojot VPN.

2. vietā ierindojas *SSL-poodle*, kas pēdējo pāris gadu laikā nav bijis augstāk par 4. vietu. *SSL-poodle* saistīta ar iespēju "atvērt/uzlauzt" SSL 3.0 šifrētu tīkla plūsmu, tādējādi tiekot vaļā no šifrēšanas un iegūstot iespēju lasīt tīkla plūsmu. Ja uzbrucējs pārtver ierīces datu paketes, teorētiski tās var tikt atšifrētas.

3. vietu ieņem *Open-smb*, kas līdz šim ilgstoši turējās topa otrajā vietā. 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, uzbrucējiem ir iespēja piekļūt iekšējā tīkla iekārtām un inficēt tās, piemēram, ar izspiedējvīrusu.

Dinamiskā kiberdrošības ainava prasa patstāvīgu modrību, savlaicīgus programmatūras atjauninājumus, kā arī ievainojamību atklāšanas rīku uzlabošanu, jo kibernoziedznieki nemitīgi pielāgo un uzlabo savu taktiku. CERT.LV aicina sekot līdzi izstrādātāju norādījumiem un nevilcinoties atjaunināt programmatūras uz jaunāko pieejamo versiju. Ar visiem aktuālajiem brīdinājumiem var iepazīties tīmekļa vietnē www.cert.lv.

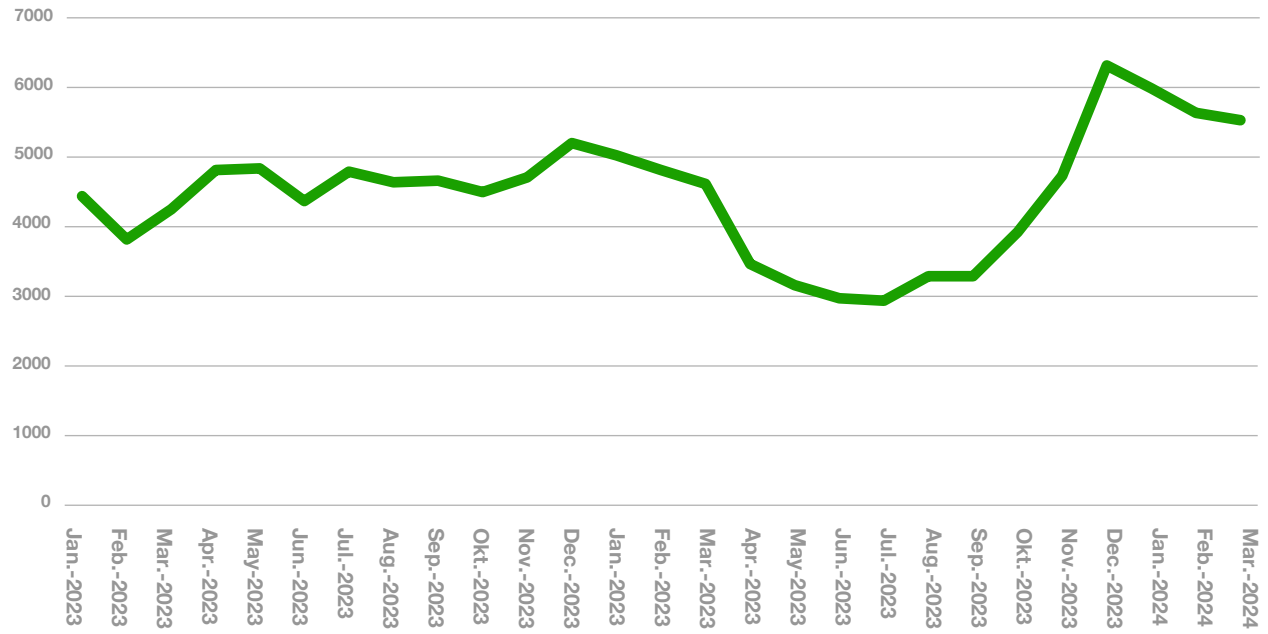


9. attēls. Apdraudēto unikālo IP adrešu skaits 1. ceturksnī – konfigurācijas nepilnību TOP 10

2.4. Ļaundabīgs kods

2024. gada 1. ceturksnī CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits ar ļaundabīgu kodu ir audzis par 22%, salīdzinājumā ar šo pašu periodu pirms gada. Turklāt ar šo apdraudējuma veidu šī gada janvārī reģistrētas 6272 unikālas IP adreses, kas ir otrs augstākais rādītājs pēdējo trīs gadu laikā (vairāk bija tikai pērn, decembrī - 6647).

Ļaunatūras tiek izplatītas galvenokārt diviem mērķiem – lai izvilinātu datus vai gūtu peļņu. Atverot ļaundabīgo pielikumu, iekārta tiek inficēta ar ļaunatūru, kas ievāc lietotājvārdus, paroles, kriptovalūtu maciņu un to piekļuves informāciju u.tml., lai nosūtītu to uz uzbrucēja kontrolētu serveri.



10. attēls. Apdraudēto unikālo IP adrešu skaits

Sistēmu uzlaušana un inficēšana notiek, pielietojot šādas metodes:

- Pikšķerēšana;
- Publiski zināmu ievainojamību ļaunprātīga izmantošana – versiju ievainojamības un jaunatklātas ***(zero-day)*** ievainojamības;
- Nekorektas konfigurācijas rezultātā tīmeklī eksponēto servisu ļaunprātīga izmantošana – noklusējuma autentifikācijas piekļuves dati, paroļu uzlaušana ar pilno pārlasi ***(brute-force)***, versiju ievainojamības;
- Inficēti datu nesēji - USB zibatmiņas;
- Pirātiskas programmatūras uzstādīšana;
- Nopludinātas un viegli uzminamas lietotāju paroles;
- Automatizētie uzbrukumi.

Galvenie ļaunatūras tipi pārskata periodā:

- Lietotāju datu zadzēji;
- ***Bot-net*** jeb zombēti datori;

- Izspiedējvīrusi;
- Attālinātās kontroles ***trojāni*** - mērķēti uz datu izgūšanu vai tālāko infrastruktūras kompromitēšanu.

Pārskata periodā lietotāju datu zadzēju ļaunatūra tika mērķēta uz nedroši, lokāli glabāto autentifikācijas datu un paroļu zagšanu, proti, paroļu iegūšanu no tīmekļa pārlūka vai nešifrētiem failiem. Šāda veida ļaunatūra tiek izplatīta kā ļaundabīgs tīmekļa pārlūka spraudnis vai kā izpildfails, pievienots pie pikšķerēšanas e-pasta vēstules.

Tāpat pārskata periodā informācijas izgūšanai dažādu iestāžu vārdā kampaņveidīgi tika izplatītas e-pasta vēstules ar kaitīgiem pielikumiem. Piemēram, marta nogalē krāpnieki Centrālās statistikas pārvaldes (CSP) vārdā masveidā izsūtīja ļaundabīgas e-pasta vēstules valsts iestāžu darbiniekiem. Vēstules pielikumā esošais datorvīruss bija paredzēts sensitīvas informācijas zagšanai uz upura iekārtas. Sūtītāja e-pasta adrese bija viltota, imitējot reālu CSP darbinieku. Arī vēstules saturs, šķietami informējot par veidlapas iesniegšanu CSP, izskatījās ticams un, iespējams, bija pārkopēts no kādas iepriekš sūtītas CSP e-pasta vēstules.

11. attēls. Piemērs ar brīdinājumu par ļaundabīgu e-pasta vēstules pielikumu

CERT.LV EKSPERTU KOMENTĀRS

Ļoti liels skaits adresātu martā saņēma šos CSP e-pastus tieši DMARC (spoofing aizsardzības) neesamības dēļ. Lai pasargātu citus saņēmējus un sava uzņēmuma vai organizācijas reputāciju, būtiski ir nodrošināt iespēju citiem pārliecināties par saņemtā e-pasta autentiskumu, ja tas izsūtīts jūsu uzņēmuma vai organizācijas vārdā, kā arī liegt iespēju trešajām pusēm izsūtīt šādus e-pastus.

CERT.LV aicināja iedzīvotājus saglabāt modrību un, saņemot šādu e-pasta vēstuli, nekādā gadījumā nevērt vaļā tās pielikumu. Savukārt e-pasta serveru uzturētājiem CERT.LV iesaka pārskatīt e-pasta servera DMARC konfigurāciju un pārliecināties, ka e-pasta vēstules, kas ir sūtītas it kā jūsu iestādes vai organizācijas vārdā, bet no cita e-pasta servera, attiecīgi tiek norādītas kā neleģitīmas.

Tāpat nav samazinājies gadījumu skaits, kad ar viltus reklāmu maldināti lietotāji paši ir instalējuši viltus mākslīgā intelekta spraudņus tīmekļa pārlūkā. Peļņas gūšanas nolūkā tika izplatīti šifrējošie izspiedējvīrusi, kuru uzbrukuma rezultātā dati upura iekārtā tika nošifrēti, un datu atgūšanai tika pieprasīta izpirkuma maksa.

Kompromitēti e-pasti vai lietotņu konti tika izmantoti, lai tālāk izplatītu ļaunatūru. Piemēram, tika konstatēti vairāki gadījumi, kad no kompromitētiem e-pastiem izplatīja *Agent Tesla* ļaunatūru, izsūtot viltus rēķinus.

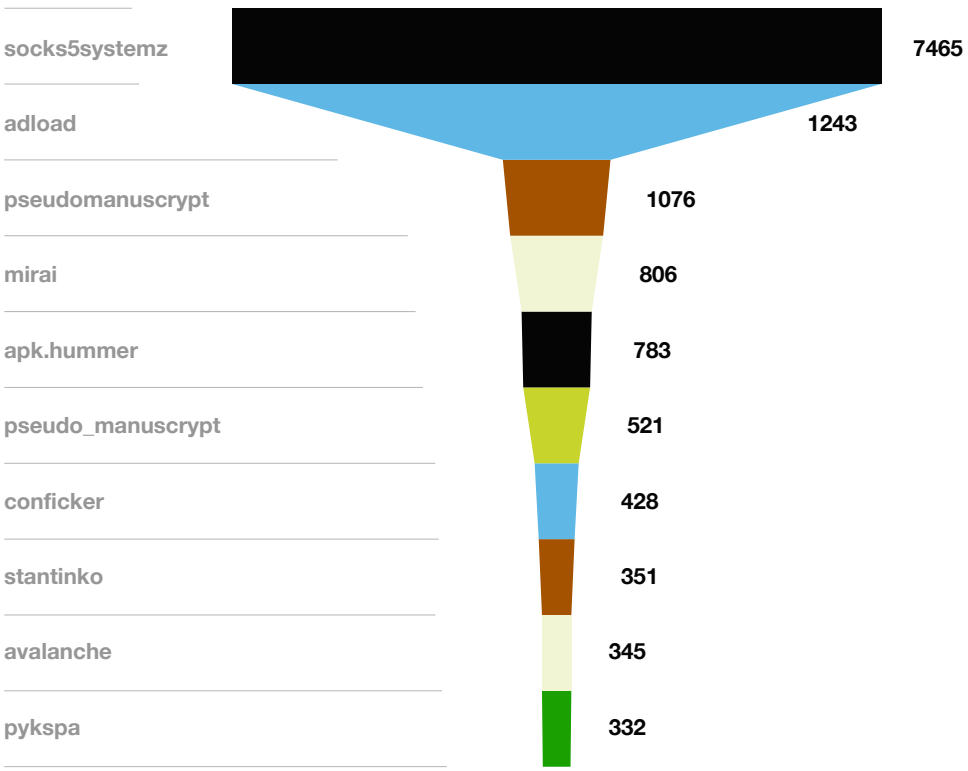
Ļaundabīgu kodu jeb ļaunatūru TOP 10

Ļaunatūru TOP 10 saraksta augšgalā 2024. gada 1. ceturksnī būtiskas izmaiņas nav notikušas - pirmās trīs vietas joprojām ieņem ***Socks5systemz***, ***Adload un Pseudomanuscrypt***.

1. vietā - ļaunatūra *Socks5systemz*, kas inficē iekārtas un pārvērš tās par pāradresācijas ***proxy*** jeb starpniekserveriem, savukārt ļaundari tos varētu izmantot, lai padarītu grūtāku viņu nelegālo un kaitīgo darbu izsekošanu. Tādējādi ar ***Socks5systemz*** inficēta ierīce tiek neautorizēti pārņemta no trešo personu puses un ar lielu varbūtību tiek iesaistīta nelegālo darbību atbalstīšanā.

2. vietā ierindojusies ļaunatūra *Adload*, kas zog upuru pārlūkmeklētāju datus un ievieto viltus/krāpnieciskas reklāmas upura interneta pārlūkā. Ja MAC ierīcei ir konstatēta ***Adload*** ļaunatūra, nepieciešams veikt pilnu datora pārbaudi ar atjauninātu antivīrusu programmu.
3. vietā kā papildu pārbaudījums iedzīvotāju modrībai ir **ļaunatūra *Pseudomanuscrypt***. Tas ir spiegošanas ***trojāns***, kurš spēj neautorizēti piekļūt un eksfiltrēt datus no inficētās ierīces, tai skaitā lietotņu autentifikācijas u.c. datus, kā arī spēj veikt inficētās sistēmas ekrānšāviņus, skaņas ierakstīšanu ar mikrofonu un citas darbības.

Vērojama arī *Mirai* aktīva izplatīšanās, kas inficē un iekļauj robotu tīklos lietu interneta ***(IoT)*** iekārtas, lai izmantotu tās tālākiem uzbrukumiem un citām pretlikumīgām darbībām.

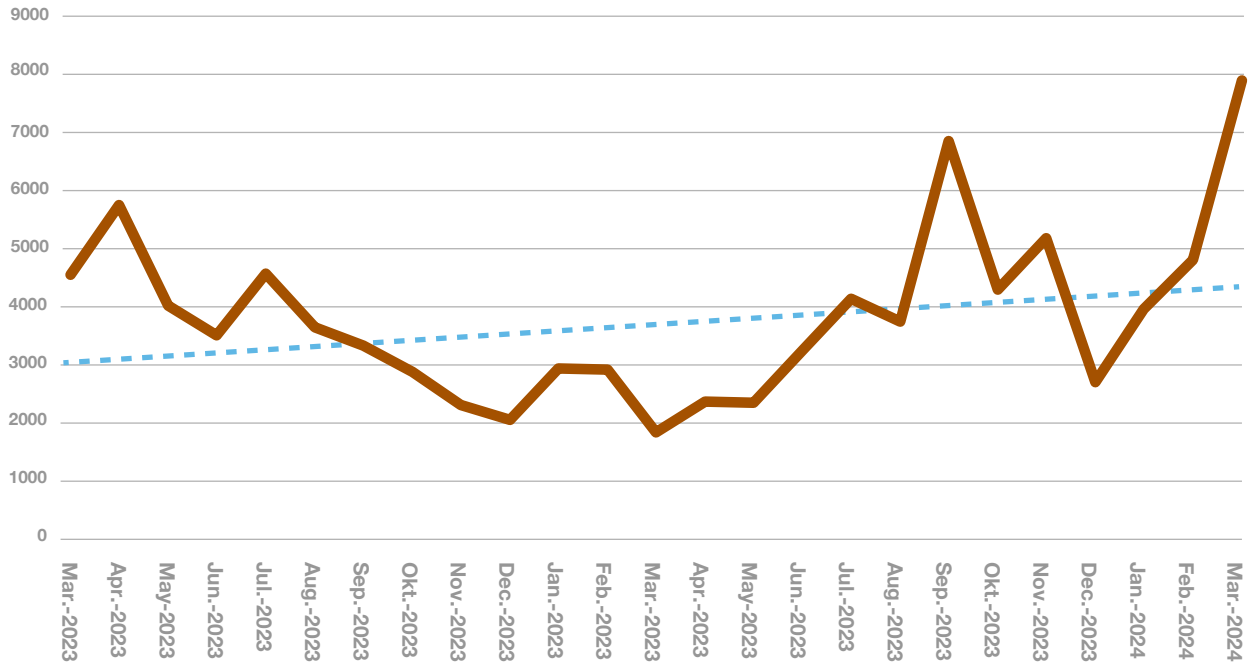


12. attēls. Apdraudēto unikālo IP adrešu skaits 1. ceturksnī – ļaunatūru TOP 10

2.5. Ielaušanās mēģinājumi

CERT.LV reģistrētie dati rāda, ka 1. ceturkšņa beigās kiberuzbrucēju ielaušanās mēģinājumi apdraudēja gandrīz 800 unikālas IP adreses, kas ir augstākais rādītājs pēdējo divu gadu laikā.

Ielaušanās mēģinājumu skaits kopš gada sākuma ir palielinājies par 118%, salīdzinājumā ar 2023. gada pirmajiem trim mēnešiem.



13. attēls. Apdraudēto unikālo IP adrešu skaits

Informācija par ielaušanās mēģinājumiem tika saņemta visa 1. ceturkšņa garumā ievērojamā intensitātē. Šie uzbrukumi veikti, lielākajā daļā gadījumu izmantojot paroļu minēšanu (*brute-force*) pret dažādiem elektronisko sakaru komersantiem, valsts un pašvaldību iestādēm, kā arī privāto sektoru. Uzbrucēji ķērās arī pie sen zināmām konfigurācijas nepilnībām plaši lietotos produktos. Fiksētie kiberuzbrukumi nav radījuši būtisku vai paliekošu ietekmi uz resursiem.

Visbiežāk neautorizēta piekļuve tīmekļu serverim un tā failu neautorizēta modifikācija notiek, izmantojot neatjaunotas satura vadības sistēmas (CMS) versiju un to spraudņu versiju ievainojamības. Līdz ar to tieši CMS un to spraudņu novēlota atjaunošana ir tīmekļa serveru kompromitēšanas dominējošais iemesls. Turklāt biežāk par citām tiek kompromitētas uz "WordPress" bāzes veidotas tīmekļa vietnes, kas ir skaidrojams ar to, ka "WordPress" ir visbiežāk izmantotais CMS.

Kiberuzbrucēju interese nav mazinājusies par attālinātajam darbam izmantotajām tehnoloģijām, tādām kā RDP (*Remote Desktop Protocol*), VPN (*Virtual Private Network*) un tiešsaistes sanāksmju un tērzēšanas platformām.

Redzama tendence, ka pirms uzbrukumiem tiek veikta izpēte, tiek meklētas organizācijas resursa vājās vietas, veikti ielaušanās mēģinājumi. Uzbrukums tiek mērķēts tieši caur "vājāko" ķēdes posmu.

Izmantojot jaunatklātas ievainojamības, kibernoziedznieki uzstājīgi meklēja iespējas iekļūt uzņēmumu un organizāciju iekšējos tīklos, lai nesankcionēti piekļūtu sensitīvai informācijai vai nošifrētu iekārtas un pieprasītu maksu par datu atgūšanu. Piemēram, janvārī tika saņemts ziņojums par šifrējošā izspiedējvīrusa uzbrukumu pret kādu grāmatvedības ārpakalpojumu uzņēmumu . Par datu atbloķēšanu kibernoziedznieki pieprasīja veikt izpirkuma maksu 8000 eiro apmērā.

IETEIKUMI DROŠĪBAI

Lai pasargātu organizāciju no izspiedējvīrusiem, ir svarīgi veikt drošības pasākumus - veidot drošas datu rezerves kopijas, izmantot pretvīrusu programmas, pārskatīt attālinātās piekļuves tiesības, nodrošināt visu ārējā perimetrā eksponēto resursu uzturēšanu atbilstošā drošības līmenī un izvairīties no aizdomīgu e-pasta vēstuļu vai saišu atvēršanas.

CERT.LV uzsver nepieciešamību konfigurēt drošu e-pasta vēstuļu izsūtīšanu un saņemšanu, kā arī aicina veikt iekārtu konfigurāciju atbilstoši labās prakses vadlīnijām. Tāpat arī svarīgi veikt sistēmu ievainojamību novēršanu, sekojot līdzi atjauninājumiem, kā arī turpināt veicināt lietotāju izglītošanu.

2.6. Kompromitētas iekārtas un datu noplūdes

Pārskata periodā iekārtu kompromitēšanas gadījumi skāra gan privātpersonas, gan privātā un publiskā sektora organizācijas. Uzbrukumu veikšanai tika izmantotas gan e-pasta vēstules ar ļaundabīgiem pielikumiem no jau kompromitētiem kolēģu vai sadarbības partneru kontiem, gan izmantoti trūkumi dažādu IKT resursu aizsardzībā, kas izpaudās kā vājas paroles un novecojis programmnodrošinājums ar vairākus gadus publiski zināmām ievainojamībām. Kompromitēti ir arī maršrutētāji nelielos uzņēmumos vai individuālās mājsaimniecībās.

Kiberuzbrukumu mērķis - izgūt datus, manipulēt ar maksājumu informāciju, panākot maksājumu veikšanu uz uzbrucēju bankas kontiem, vai nošifrēt iekārtas, lai pieprasītu izpirkuma maksu par datu atgūšanu un, iespējams, nenopludināšanu.

Paroļu pārvaldība: Fiksēti gadījumi, kad datora paroles tika glabātas nešifrētā veidā, lokāli uz inficēta datora, līdz ar to ierīces inficēšanas gadījumā uzbrucēji guva pieeju pie vairākiem lietotāju kontiem, kuriem nebija aktivizēta divfaktoru autentifikācija. Īpaši bīstami ir gadījumi, kad nešifrētas paroles tiek uzglabātas administratoru datoros, kuriem ir augstu privilēģiju piekļuve infrastruktūrā.

Reģistrēti arī gadījumi, kad inficētais dators tika izmantots kā koplietošanas darbstacija, līdz ar to, inficējot vienu ierīci, uzbrucēju rīcībā nonāca vairāku personu autentifikācijas dati. Papildus tam nereti kompromitēti e-pasti vai lietotņu konti tiek izmantoti, lai tālāk izplatītu ļaunatūru.

CERT.LV ir rosinājusi iekļaut daudzfaktoru autentifikāciju kā obligātu minimālo kiberdrošības prasību jaunās normatīvo aktu iniciatīvās. CERT.LV iesaka ikvienam, un it īpaši valsts un pašvaldību iestāžu darbiniekiem, iespējot daudzfaktoru autentifikāciju, kas nepieļautu kontu nozagšanu. Ja tiek izmantota daudzfaktoru autentifikācija, un kāds ļaundaris tomēr iegūst paroli, tas nevar piekļūt tiešsaistes kontam, ja vien nav pieejams arī otrais autentifikācijas faktors (upura telefons vai drošības atslēga).

Kompromitēti e-pastu konti: Kiberuzbrukums, kam ir nopietnas sekas, uzņēmumam vai iestādei bieži sākas ar darbinieka konta piesavināšanos. Joprojām novērojami gadījumi, kad pēc e-pasta kontu uzlaušanas uzbrucēji izveidoja e-pasta filtrus, lai pārtvertu un pārvirzītu interesējošā e-pasta vēstules krāpšanas nolūkā.

Kompromitēti lietotāju sociālo mediju konti: Informācija par kompromitētiem sociālo mediju kontiem tiek saņemta ievērojamā intensitātē. Lielā skaitā fiksēti gadījumi ar kompromitētiem “Instagram” un “Facebook” kontiem, kur piekļuve iegūta, izmantojot sociālo inženieriju. Izplatītākā metode - lietotājam nosūta ziņu no profila, kura nosaukums ir dažādas “Facebook” Administrator, “Meta” Administrator vai “Instagram” Blue Badge variācijas. Lietotājs tiek informēts par platformas noteikumu pārkāpumu, un, lai nodrošinātu turpmāku piekļuvi kontam, nepieciešams veikt darbības sūtītāja ziņā norādītajā saitē. Savukārt saitē nosaukums līdzinās attiecīgajai “Meta” platformai, kur jāievada lietotāja dati, kas tiek pārsūtīti krāpniekiem.

Kompromitēti tīmekļa serveri: Kiberuzbrucēji veic pikšķerēšanas satura izvietošanu vai arī izmanto tīmekļa serveri kā prettiesiski iegūto datu kolektoru. Praktiski katrā gadījumā, kad uzbrucējiem ir iespēja veikt neautorizētu tīmekļa servera modifikāciju serverī, tiek ievietoti vairāki ļaundabīgi čaulas skripti, ar kuru palīdzību uzbrucējiem ir iespējas kontrolēt kompromitētus tīmekļu serverus un caur tiem attālināti izpildīt komandas. Nereti uzbrucēji ar ievainojama tīmekļa servera starpniecību piekļūst arī citiem resursiem, piemēram, izgūst datubāzes, kuras satur personu datus.

Visbiežāk novērotie "klupšanas akmeņi", kurus CERT.LV identificēja kā būtiskus traucējumus, kas liedz pašai mērķa iestādei laicīgi un efektīvi uzraudzīt savu infrastruktūru un reaģēt uz potenciāliem incidentiem, ir šādi:

- Nav centralizēta auditācijas pierakstu uzkrāšana un analīze;
- Tīkla segmentācijas un IT infrastruktūras inventarizācijas neesamība;
- Nepareizi konfigurēta vai neeksistējoša SIEM (Security Information and Event Management) sistēma;
- Nepareizi konfigurēta vai neeksistējoša lietotāju tiesību pārvaldība un izpildāmo failu politika.

TOP incidenti pārskata periodā

Mērķēta pikšķerēšanas kampaņa pret funkcionālā apģērba un militārā ekipējuma ražošanas uzņēmumu: Kampaņa izveidota profesionāli no Krievijā uzturēta servera - atsūtīts viltus rēķins no reālas sadarbības kompānijas, pareizā darbības jomā; mērķis – izkrāpt e-pasta piekļuves datus. Pēc CERT.LV rīcībā esošās informācijas neviens no uzņēmuma darbiniekiem nav uz šo pikšķerēšanas kampaņu uzķēries. Par kampaņu tika ziņots CERT.LV, un tās indikatori ievietoti CERT.LV aktīvās aizsardzības pakalpojumā DNS ugunsmūrī. CERT.LV sniedza konsultācijas uzņēmuma kiberdrošības stiprināšanai.

Kādā kultūras biedrībā krāpnieciskā veidā tika pārņemts biedrības "Facebook" konts, kā rezultātā dažādās reklāmās ar nelielām summām no kontam piesaistītās kartes noņemti gandrīz 1000 eiro. Uzlaužot "Facebook" kontu, krāpnieki nomaina ne tikai paroles, bet arī atgūšanās e-pasta adreses, lai apgrūtinātu īpašniekiem kontu atgūšanu. CERT.LV rekomendēja cietušajiem par notikušo operatīvi ziņot "Facebook" atbalsta dienestam, lai uzsāktu konta atgūšanas procesu.

No kompromitēta e-pasta konta nosūtītas 10 000 pikšķerēšanas e-pasta vēstules: Uzbrucējiem pietiek kompromitēt tikai vienu e-pasta kontu, lai sasniegtu visus pārejos organizācijas darbiniekus. Piemēram, martā kāda Latvijas augstskola cieta lielā pikšķerēšanas uzbrukumā, jo kiberuzbrucēji bija ieguvuši piekļuvi viena studenta e-pastam un nosūtīja no tā ap 10 000 pikšķerēšanas e-pasta vēstules pārējiem augstskolas studentiem un darbiniekiem. CERT.LV sniedza iestādei nepieciešamo atbalstu, veicinot incidenta ietekmes pārvarēšanu.

IETEIKUMI DROŠĪBAI

- Izmantojot "WordPress" vai cita veida atvērtā koda CMS, izvēlēties automātisko atjauninājumu iespēju vai veikt regulārus atjauninājumus. Rūpīgi izvērtēt uzstādītos spraudņus un to nepieciešamību.
- Uzturot augstas nozīmības sistēmas vai tādas, kurās tiek glabāta informācija lielā apjomā, kas ir grūti atjaunojama, obligāti izmantot ārējo rezerves kopiju uzturēšanu.
- Uzturot resursus, it īpaši informatīvus un/vai kur minētas konkrētas personas un tām piesaistītā informācija, ko iespējams izmantot jebkāda veida ļaundabīgos nolūkos, piemēram, pikšķerēšanā, norādot jau pieejamu informāciju, aicināt vai, kur tas iespējams, pieprasīt uzglabāt žurnālfailus, kas satur informāciju par piekļuvi šiem resursiem un to saglabāšanu/lejupielādi, ja informācija tiek nodrošināta dokumentos ar lejupielādes iespēju.
- Plānot un organizēt regulāras darbinieku apmācības un zināšanu pārbaudi vismaz reizi gadā. Regulāri informēt darbiniekus par biežāk iespējamajiem kiberapdraudējumiem. Ieteicams sekot līdzi CERT.LV sociālo mediju kontiem un vietnei cert.lv, kur ikvienam pieejama informācija par aktualitātēm kiberdrošības jomā.
- Veikt paroļu uzglabāšanu šifrētā veidā, piemēram, izmantojot paroļu pārvaldnieku.
- Izmantot divu faktoru autentifikāciju visur, kur vien tas iespējams.
- Saņemot e-pastu no personām, ar kurām tiek veikta regulāra komunikācija, pārbaudīt, vai tiek izmantots kāds no e-pasta kontiem, kuri figurē regulārajā komunikācijā. Sistēmu administratoriem ieteicams izmantot DMARK, SPF un DKIM tehnoloģijas.
- Uzturot sistēmas, kurās pieejama iekšējās lietošanas informācija, regulāri monitorēt eksponētos servisus, it īpaši pie sistēmu atjauninājumu veikšanas.
- Tīmekļa vietnēm, kurās iespējams norēķināties ar maksājumu kartēm, veikt vietnes drošības auditu, ideālā gadījumā arī PCI sertifikāciju.

3. Kiberapdraudējumu prevencija

3.1. DNS ugunsmūris: aktīvā aizsardzība

DNS UGUNSMŪRIS - aktīvās aizsardzības pakalpojums individuālu lietotāju un organizāciju pasargāšanai no krāpniecisku vietņu apmeklēšanas, aizsargājot to ierīces no krāpnieciskās kampaņās izmantotām ļaundabīgām saitēm, krāpnieciskām vietnēm, kaitīga satura un vīrusiem, kā arī nodrošinot valstī vienotu ierobežojamo domēnu zonu apstrādi un izplatīšanu. Pakalpojumu bez maksas nodrošina CERT.LV un NIC.LV.

Plašāk: https://dnsmuris.lv/

Latvijā regulāri notiek kampaņveidīgas krāpnieciskās aktivitātes – gan viltus vietnes bankas kontu, e-pasta vai sociālo tīklu piekļuves datu izkrāpšanai, gan ļaunatūru izplatīšanai kibertelpā. CERT.LV novēro šādas kampaņas un operatīvi ievieto šo kampaņu indikatorus DNS ugunsmūrī, lai tā lietotājus pasargātu no identificētajiem apdraudējumiem.

DNS ugunsmūris nodrošina aktīvu aizsardzību, kā, piemēram, ļaunatūras lejupielādes bloķēšanu, tādējādi novēršot lietotāju piekļūšanu bīstamajiem resursiem un pārvirzot tos uz brīdinājuma vietni. Arī gadījumos, kad ļaunatūra jau ir inficējusi kādu iekārtu, DNS ugunsmūris sniedz iespēju ātrāk identificēt šādas iekārtas, kas sistēmu administratoriem dod iespēju operatīvi veikt seku novēršanu.

Pārskata periodā kopskaitā ģenerētais brīdinājumu skaits DNS ugunsmūra ietvaros ir gandrīz 1,2 miljoni, savukārt no ļaundabīgu vietņu apmeklēšanas DNS ugunsmūra lietotāji tika pasargāti vairāk nekā pusmiljons reižu. Divu gadu laikā DNS ugunsmūra pakalpojuma lietošana pieaugusi aptuveni 5 reizes, mēnesī apstrādājot ap 1,5 miljoniem DNS pieprasījumu.

Kopējo rezultātu ietekmē vairāki faktori - robotizēta domēna pārbaude, automātiska domēnu pārbaude, ko veic ugunsmūri vai maršrutētāji, kā arī cilvēka darbības rezultātā izsauktie domēni, bieža domēnu izsaukšana kompromitētā iekārtā vai aktīva koda ***persistences*** rezultātā.

Nozīmīgākās aktīvas aizsardzības epizodes pārskata periodā:

- 1 129 brīdinājumi par viltus EDS lapu aktivitātēm;
- 2 053 brīdinājumi par “Latvijas Pasts” tēla izmantošanu viltus vietnes kampaņās;
- 62 831 brīdinājums par ***Rasberry Robin*** vīrusa aktivitāti;
- 1 373 brīdinājumi, kas saistīti ar ***Balada*** ļaunatūru.

CERT.LV piedāvā iespēju uzņēmumiem un iestādēm, kas paši uztur savus DNS rekursīvos serverus, izmantot CERT.LV uzturētās DNS RPZ (***Response Policy Zone***), kas satur CERT.LV identificēto bīstamo resursu sarakstus. Papildus CERT.LV uztur arī kompetento iestāžu veidotos sarakstus, kuros iekļauti resursi, kam atbilstoši normatīvajiem aktiem Latvijā, jāierobežo piekļuve elektronisko sakaru tīklos. CERT.LV izveidojis atsevišķu DNS RPZ zonu katras kompetentās iestādes sarakstam. CERT.LV sadarbojas ar šo sarakstu veidotājiem, tai skaitā, pirms informācijas atjaunošanas pārbauda resursu pieraksta pareizību un unificē resursu sarakstus. Ar RPZ zonu sarakstu var iepazīties šeit: https://cert.lv/lv/elektronisko-sakaru-komersantiem/sadarbiba-ar-cert-lv#dnsrpz

IETEIKUMI DROŠĪBAI

Lai efektīvi pasargātu ikvienu no krāpniecisku un ļaundabīgu vietņu apmeklēšanas, izmantot CERT.LV nodrošināto aizsardzību - DNS ugunsmūri. Informēt Valsts policiju par krāpnieku aktivitātēm un ļaundabīgām vietnēm un ziņot CERT.LV, pārsūtot kaitīgos e-pastus uz cert@cert.lv (instrukcija, kā pareizi pārsūtīt: https://cert.lv/lv/kontakti/ka-parsutit-kaitigus-e-pastus).

3.2. Sensoru tīkls

SENSORU TĪKLS - agrās brīdināšanas sistēma (ABS) iestādēm, kurās tas ir uzstādīts, ļauj laicīgi pamanīt un atpazīt radušos apdraudējumus, kā arī savlaicīgi reaģēt uz tiem, papildus nodrošinot daudzpusīgāku priekšstatu par apdraudējumu spektru valsts un pašvaldību iestādēs.

ABS jeb sensoru tīkla izveides mērķis ir nodrošināt iestāžu atbildīgajiem un CERT.LV iespējas laicīgi identificēt esošos apdraudējumus iestādēm. Tas tiek nodrošināts, analizējot iestādes tīkla plūsmas kopiju, izmantojot speciāli izveidotos notikumu noteikumus ***(signature)*** un statistiskās datu analīzes metodes.

Pārskata periodā CERT.LV turpināja ABS sistēmas uzturēšanu un paplašināšanu. Tāpat tika pilnveidota sensoru programmu nodrošinājuma darbība.

ABS ik mēnesi fiksē vidēji 6000 augstas prioritātes (ar augstu bīstamības potenciālu) incidentus valsts, pašvaldību un kritiskās infrastruktūras (KI) iestādēs. Pārskata periodā ABS ģenerēto brīdinājumu skaits kopskaitā ir gandrīz 718 miljoni.

Pārskata periodā ABS visvairāk identificētie *apdraudējumi*

Apdraudējumi	Janvāris	Februāris	Marts
Ar datorvīrusiem saistīti brīdinājumi	52355	28487	277
Brīdinājumi par krāpniecību	157	272	2257
Ar pikšķerēšanu saistīti brīdinājumi	5672	18135	2174
Ar ļaunprātīgām vietnēm saistīti brīdinājumi	7813	14036	30073
Ar robottīklu, krāpniecību un vīrusu indikatoriem saistīti brīdinājumi	44406	20217	10833

3.3. Pasākumi incidentu novēršanai

Pārskata periodā valsts un pašvaldību iestāžu atbildīgajiem par IT drošību, kā arī pamatpakalpojumu sniedzējiem, digitālo pakalpojumu sniedzējiem un kritiskās infrastruktūras pārstāvjiem e-pastā tika izsūtīti kopskaitā 8 paziņojumi/ brīdinājumi ar aicinājumu nekavējoties veikt programmatūras atjaunināšanu:

- **5. janvārī** tika izsūtīts brīdinājums par ***Ivanti*** programmatūrā atklātu kritisku attālināta koda izpildes ievainojamību (CVE-2023-39336);
- **11. janvārī** - brīdinājums par kritiskām ievainojamībām ***Ivanti*** programmatūrā ***Ivanti Connect Secure un Ivanti Policy Secure (***CVE-2023-46805 un CVE-2024-21887);
- **15. janvārī** - brīdinājums par ***Juniper*** sistēmas ievainojamību (CVE-2024-21591);
- **29. janvārī** - brīdinājums par atklātām kritiskām ievainojamībām ***Jenkins*** programmatūrā (CVE-2024-23897 un CVE-2024-2389);
- **6. februārī** - brīdinājums par atklātām kritiskām ievainojamībām **QNAP** programmatūrā (CVE-2023-45025 un CVE-2023-47568).
- **7. februārī** - brīdinājums par vairākām ievainojamībām ***Fortinet*** **FortiSIEM** programmatūrā (CVE-2024-23108 un CVE-2024-23109);

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

- **21. februārī** - brīdinājums par atklātu kritisku ievainojamību ***ConnectWise ScreenConnect;***
- **11. martā** - brīdinājums par **QNAP** iekārtu ievainojamībām.

3.4. Koordinēta ievainojamību atklāšana (CVD)

CERT.LV turpināja darbu pie koordinētas ievainojamību atklāšanas ziņojumu reģistrēšanas platformas cvd.cert.lv (CVD) attīstības un popularizēšanas, pildot koordinētas ievainojamību atklāšanas procesa koordinētāja un vidutāja, kā arī platformas izstrādātāja, uzturētāja un pārziņa lomu.

CVD platformas darbība tika uzsākta 2023. gada martā. Tajā ir publicēta informācija par iestādēm, kuras brīvprātīgi iesaistījušās koordinētas ievainojamību atklāšanas procesā un noteikušas resursus, uz kuriem ievainojamību ziņošana attiecināma.

Koordinēta ievainojamību atklāšanas platforma (CVD) - nodrošina iespēju pētniekam reģistrēt ziņojumu par novēroto ievainojamību, kā arī visiem iesaistītajiem (iestādei, pētniekam un CERT.LV) iepazīties ar iesniegto informāciju, savā starpā sazināties un sekot līdzi ievainojamību novēršanas gaitai.

Plašāk: https://cvd.cert.lv/

Platformā tiek reģistrēti ievainojamību ziņojumi un ar to apstrādi saistītā komunikācija starp iesaistītajām pusēm. Šāda ziņošanas prakse dod iespēju CERT.LV savlaicīgi uzzināt par ievainojamībām un pilnvērtīgi koordinēt ievainojamību izpēti un to novēršanu, tā efektīvāk organizēt pasākumus Latvijas kibertelpas aizsardzībai.

Uz pārskata perioda beigām platformā cvd.cert.lv bija reģistrēti:

- Drošības pētnieki – 42 (kopš iepriekšējā ceturkšņa beigām skaits pieauga par 5);
- Aktīvas iestāžu programmas – 7 (skaits pieauga par 3);

Uz pārskata perioda beigām platformā reģistrēti 24 ievainojamību ziņojumi, tostarp:

- CERT.LV klientūras ievainojamības – 16 (skaits pieauga par 3);
- Uz konkrētām iestāžu programmām reģistrētās ievainojamības – 8 (skaits pieauga par 1).

26. martā IT drošības seminārā "Esi drošs" CERT.LV vadītāja Baiba Kaškina pasniedza iestāžu pārstāvjiem un pētniekiem pateicības rakstus par dalību CVD platformā.

CVD platformas attīstība

Turpinās darbs pie CVD platformas darbības attīstības, ieviešot pētnieku reitingu un profila informācijas pārvaldīšanas iespēju pētniekiem. Tiek ieguldīts darbs jaunu dalībnieku iesaistē, tajā skaitā Nacionālās kiberdrošības likuma (NKDL) subjektu uzrunāšana un jaunu pētnieku, piemēram, studentu, iesaiste. Lai sekmētu efektīvāku ziņojumu apstrādi, CERT.LV aicina platformā reģistrēties visas iesaistītās puses, tādējādi paātrinot un padarot caurspīdīgāku saziņu un informācijas apmaiņu.

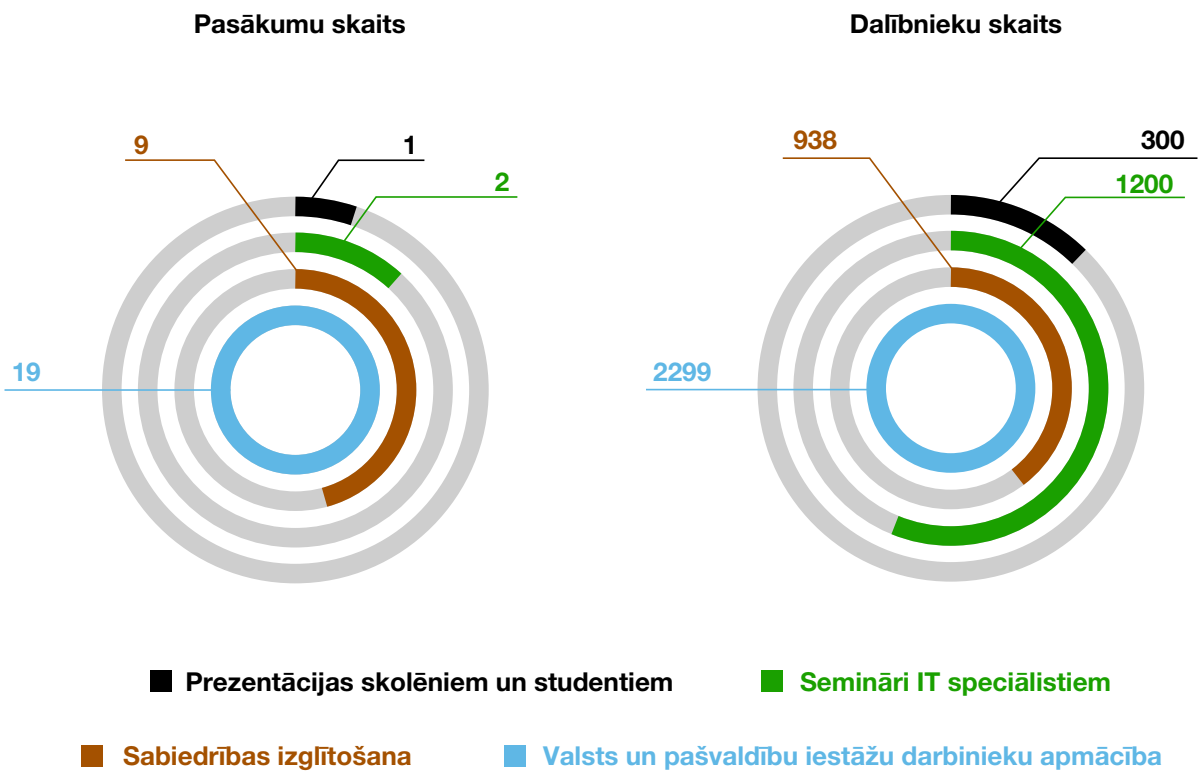
4. Komunikācija ar sabiedrību

4.1. Apmācības un izglītojošie pasākumi

Pārskata periodā CERT.LV komanda veica aktīvu darbu sabiedrības izglītošanai, gan organizējot, gan piedaloties dažādos tematiskos semināros, informējot par aktualitātēm kiberdrošības jomā, kā arī veicinot kiberhigiēnas labo praksi.

Papildus ierastajiem darbinieku izglītošanas semināriem par kiberdrošību vairākās iestādēs tika novadīta Kiberdrošības incidentu izmeklēšanas spēle *(Cybersecurity Breach Investigation Tabletop Exercise)*.

2024. gada 1. ceturksnī, iesaistoties 31 izglītojošā pasākumā, CERT.LV par IT drošību izglītoja 4 737 dalībniekus.



14. attēls. Izglītojošo pasākumu un apmācīto cilvēku skaits 1. ceturksnī

CERT.LV organizētie izglītojošie pasākumi IT drošības speciālistiem

26. martā CERT.LV organizēja IT drošības semināru "Esi drošs" valsts un pašvaldību iestāžu atbildīgajiem darbiniekiem par IT drošību, pamatpakalpojumu sniedzējiem, digitālo pakalpojumu sniedzējiem, kā arī citiem interesentiem, kuri darbojas IT drošības jomā.

Semināra ietvaros tika aplūkotas tādas tēmas kā NIS2 direktīva un Nacionālās kiberdrošības likums, informatīvais materiāls iestāžu vadītājiem par kiberdrošības veicināšanu, elektroniskās identifikācijas un uzticamības pakalpojumu kopīgais un atšķirīgais, drošības apmācību pieredzes stāsti, apmācību programmas izstrāde, koordinētas ievainojamību atklāšanas procesa jaunumi u.c. tēmas. Tāpat tika prezentēts CERT.LV pētījums par lietotāju drošību skaitļos un praktiskiem risinājumiem drošības uzlabošanai.

Semināru klātienē apmeklēja 140 dalībnieki, tiešsaistē sekoja līdzi vairāk nekā 900 dalībnieku. (Ieraksts: https://cert.lv/lv/2024/03/it-drosibas-seminars-esi-dross-26-marta)

Galda izspēles mācības par kiberdrošības incidentu izmeklēšanu: Pārskata periodā CERT.LV organizēja vairākas teorētiskās mācības, kurās CERT.LV speciālistu vadībā tika izspēlēta kiberdrošības incidentu izmeklēšanas spēle (*Cybersecurity Breach Investigation Tabletop Exercise*) vairākās organizācijās. Kopskaitā no visām organizācijām spēlē piedalījās 139 dalībnieki.

Kiberdrošības incidentu izmeklēšanas spēli sagatavojusi Eiropas Savienības Kiberdrošības aģentūra ENISA, lai veicinātu izpratni par kiberdrošību jomas nespeciālistiem, savukārt latviešu valodā to tulkojusi un pielāgojusi CERT.LV komanda.

CERT.LV prezentācijas par IT drošību sabiedrības izglītošanai

Nozīmīgākie pasākumi 1. ceturksnī:

6. februārī Drošāka interneta dienas ietvaros Ventspils Digitālais centrs organizēja Ventspils iedzīvotājiem un citiem interesentiem lekciju, kurā CERT.LV iepazīstināja klausītājus ar kiberhigiēnas pamatprincipiem.

13. februārī CERT.LV vadīja darbnīcu **"Drošība tavā ierīcē"** SSE Riga organizētajā ikgadējā **vakara skolā žurnālistiem**. Darbnīcas ietvaros CERT.LV informēja dalībniekus par drošākas ierīces izvēli, ražotāju piedāvātajiem rīkiem un iespējām, sociālo tīklu un dažādu servisu pieslēgumu drošību, rezerves kopijām, mākoņpakalpojumiem, kā arī par drošu iekārtas nomaiņu un datu dzēšanu.

23. februārī Latgales reģionālajā **seminārā par visaptverošu valsts aizsardzību** CERT.LV pārstāvis informēja dalībniekus par aktuālajiem kiberdrošības jautājumiem. Pasākuma mērķis bija sekmēt sabiedrības iesaisti valsts aizsardzībā.

28. februārī CERT.LV piedalījās Izglītības un zinātnes ministrijas organizētajā konferencē par skolu digitalizāciju, sniedzot prezentāciju "Datordrošības ieteikumi skolēnu datoriem". Konference tika organizēta ES Atveseļošanās fonda projekta "Digitālās plaisas mazināšana sociāli neaizsargātajām grupām un izglītības iestādēs" ietvaros ar mērķi izzināt izglītības tehnoloģiju lomu un attīstības iespējas, vienlīdzīgu un iekļaujošu mācīšanās iespēju nodrošināšanai ikvienam skolēnam. Pasākums pulcēja izglītības ekspertus, pašvaldību digitalizācijas vadītājus, skolu izglītības tehnoloģiju mentorus un pedagogus, lai spriestu par nākotnes izglītības tendencēm un dalītos labās prakses piemēros saistībā ar digitalizācijas procesu plānošanu un ieviešanu skolās un pašvaldībā, kuru mērķis ir pārvarēt šķēršļus un nodrošināt iekļaujošas mācīšanās iespējas visiem skolēniem.

5. martā kvalifikācijas celšanas pasākumā personas datu aizsardzības speciālistiem tika sniegta prezentācija, kurā dalībnieki tika informēti par aktualitātēm kibertelpā, kas ietekmē personas datu drošību.

4.2. Sabiedrības informēšana un kiberhigiēnas veicināšana

CERT.LV turpināja informēt sabiedrību par kiberdrošības riskiem, kiberhigiēnas veicināšanu un labajām praksēm, kā arī citām aktualitātēm Latvijas kibertelpā. 1. ceturksnī ar 324 publikācijām plašsaziņas līdzekļos potenciālais skatījumu skaits bija 13,42 miljoni.

Pārskata periodā lielāko mediju interesi izraisīja aktuālā situācija Latvijas kibertelpā, kā arī IT drošības seminārs "Esi drošs".

CERT.LV arī turpina tulkot un portālā **www.esidross.lv** publicēt OUCH! ikmēneša izdevumus (informācijas drošības biļetens, ko sagatavo SANS institūts).

Pārskata periodā portālā esidross.lv publicētie raksti:

- QR kodi jeb kvadrātkodi OUCH! 01/2024
- Auksts aprēķins un psiholoģiski "triki" = romantiskā krāpšana
- Identitātes zādzība: novēršana, atpazīšana un apturēšana OUCH! 02/2024
- Ziņojumapmaiņa: ko drīkst un ko nedrīkst darīt OUCH! 03/2024

Ikmēneša pārskats "Kiberlaikapstākļi"

CERT.LV turpina apkopot ikmēneša pārskatu "Kiberlaikapstākļi" par aizvadīta mēneša spilgtākajiem notikumiem kibertelpā TOP 5 kategorijās – krāpšana, ļaunatūras un ievainojamības, piekļuves atteices uzbrukumi, ielaušanās un datu noplūde, kā arī lietu internets. Pārskati publicēti tīmekļa vietnes www.cert.lv sadaļā "Ziņas":

- **Janvāris:** https://cert.lv/lv/2024/02/kiberlaikapstakli-janvaris
- **Februāris**: https://cert.lv/lv/2024/03/kiberlaikapstakli-februaris
- **Marts**: https://cert.lv/lv/2024/04/kiberlaikapstakli-marts#Krapsana

5. Stratēģiskā sadarbība Latvijā

Pārskata periodā CERT.LV speciālisti cieši sadarbojas ar Latvijas Republikas Zemessardzes Kiberaizsardzības vienību, kas IT drošības krīzes vai apdraudējuma situācijā sadarbībā ar CERT.LV varētu sniegt atbalstu valstij un privātajam sektoram. Pārskata periodā svarīgākā sadarbība notika, piedaloties kiberdrošības mācību *LOCKED SHIELDS* plānošanā un Latvijas komandas sagatavošanā mācībām.

CERT.LV turpina organizēt Informācijas tehnoloģiju un Informācijas sistēmu drošības ekspertu grupas (DEG) sanāksmes, kas notiek katra mēneša otrajā ceturtdienā. DEG ir brīvprātīga Informācijas tehnoloģiju un Informācijas sistēmu drošības ekspertu grupa ar mērķi veicināt IT/IS drošību, sekmēt drošības apziņas kultūru Latvijas Republikā un sniegt atbalstu CERT.LV. Sanāksmēs tiek apspriestas gan kiberdrošības aktualitātes, gan sekmēta grupas dalībnieku zināšanu un pieredzes apmaiņa.

CERT.LV cieši sadarbojas ar Aizsardzības ministrijas Nacionālās kiberdrošības politikas koordinācijas nodaļu un savas kompetences ietvaros aktīvi piedalījās Nacionālās kiberdrošības stratēģijas īstenošanā.

Turpinās sadarbība ar Latvijas Interneta asociāciju (LIA), kas izglīto sabiedrību par iespējamajiem riskiem un draudiem interneta vidē, veicinot drošu interneta lietošanu un nodrošinot ziņojumu līniju ziņošanai par bērnu seksuālu izmantošanu atainojošu materiālu apriti internetā. (LIA Drošāka interneta centra ziņojumu pārskatu skatīt 7. nodaļā).

5.1. Kibernoziedzības novēršana un apkarošana

Sadarbība ar kritiskās infrastruktūras (KI) turētājiem

Turpinās sadarbība ar KI turētājiem, gan uzraugot situāciju kibertelpā, gan sniedzot konsultācijas un atbalstu KI kibernoturības stiprināšanai un dažādu sektoru sadarbības pilnveidošanai. CERT.LV aktīvi koordinē sensoru un DNS RPZ uzstādīšanu iestādēs un uzņēmumos, lai veicinātu ātrāku KI apdraudējumu identificēšanu un efektīvāku to novēršanu.

Atbalsts Latvijas valsts tiesībsargājošajām iestādēm

Pārskata periodā CERT.LV sniedza atbalstu Latvijas valsts tiesībsargājošajām iestādēm kibernoziedzības incidentu izmeklēšanā, veicot padziļinātu izpēti un sagatavojot atbildes Valsts policijai par vairākiem drošības incidentiem.

CERT.LV akcentē nepieciešamību turpināt Latvijas sabiedrības izpratnes vecināšanu par kibertelpu un kibernoziegumu riskiem tajā, lai stiprinātu sabiedrības noturību pret kiberzubrukumiem, mazinātu to ietekmi un sekmētu to novēršanu. Īpaša uzmanība ir jāpievērš preventīvām metodēm un iniciatīvām, kas ļautu bloķēt ar noziedzīgu mērķi radītas vai noziedzīgām darbībām izmantotas interneta vietnes, šo iniciatīvu atzīšanu un iedzīvināšanu, pilnveidojot arī iesaistīto institūciju sadarbību un atbildīgo institūciju reaģēšanas ātrumu.

Drošības testi un izvērtējumi

2024. gada 1. ceturksnī CERT.LV komanda veica vēlēšanu sistēmas pilno drošības testu, kopskaitā trīs sistēmām, no kurām sarežģītākās sistēmas tests ir pabeigts, savukārt atlikušo divu sistēmu testi vēl ir procesā un tiks pabeigti 2. ceturkšņa sākumā.

Resursiem, kuros tika veikti ielaušanās testi, tika identificētas 4 vidēja un 3 zema riska ievainojamības. Kritiskas ievainojamības netika identificētas.

Resursu turētājiem un izstrādātājiem tika iesniegti pārskati par testu rezultātiem un sniegtas rekomendācijas nepilnību novēršanai. Pēc nepilnību novēršanas tiks veikti atkārtoti testi, lai pārliecinātos par sistēmu gatavību vēlēšanām. CERT.LV uzstāja uz nepieciešamību veikt iepriekšējo vēlēšanu pieredzē balstītus un reālās slodzes apstākļiem

pielāgotus slodzes testus. Sistēmu turētāji ir ieplānojuši visaptverošus slodzes testus iesaistītajām komponentēm pirms vēlēšanu sistēmu nodošanas ekspluatācijā.

Draudu medību operācijas

Proaktīvu kiberuzbrucēju klātbūtnes meklēšanu jeb draudu medību operācijas CERT.LV sadarbībā ar partnervalstīm Latvijai svarīgās infrastruktūras sistēmās veic kopš 2022. gada.

Par kibertelpas kā stratēģiski nozīmīgas vides lomu jau tiek runāts vairākus gadus – tai, kara apstākļos, tiek piešķirta vienlīdz stratēģiska nozīme kā zemei, jūrai, gaisam un kosmosam. Tas kļuvis īpaši svarīgi laikā pēc Krievijas pilna mēroga iebrukuma Ukrainā, jo arī Krievijas bruņotie spēki atklāti runā par kibertelpu kā karadarbības vidi.

Draudu medību operāciju rezultātā izdevies būtiski stiprināt Latvijas kritiskās infrastruktūras un digitālo pakalpojumu kibernoturību. Šo operāciju rezultātā vairākkārtīgi ir izdevies identificēt un veiksmīgi likvidēt citu valstu kiberoperāciju vienību klātbūtni Latvijas infrastruktūrā. Līdz 2023. gada beigām analizētas vairāk nekā 100 000 iekārtas 25 organizācijās. CERT.LV draudu medību operācijas notiek ar mērķi identificēt kiberapdraudējumu klātbūtni Latvijai svarīgās infrastruktūras sistēmās.

CERT.LV ieskatā Latvijas "jaunā kiber doktrīna" ir būtiska kiberaizsardzības spēju kāpināšana, tai skaitā ar sabiedrotajām valstīm, attīstot savas spējas un pretstāvēšanas kapacitāti, lai novērstu jebkura uzbrukuma iespējamību. Sniedzot savu ieguldījumu NATO kolektīvajā aizsardzībā, CERT.LV turpina draudu medību operācijas ciešā sadarbībā ar Kanādas Bruņoto spēku kiberpavēlniecību.

Pārskata periodā CERT.LV speciālisti kopā ar Kanādas kiberpavēlniecības pārstāvjiem pabeidza darbu pie *Threat Hunt Playbook* – draudu medību rokasgrāmatas pirmā izdevuma. Paredzams, ka rokasgrāmata tiks nepārtraukti papildināta un pilnveidota. Informācija par izdarīto, kas ir ievērojams sasniegums draudu medību jomā pasaulē, tiks nodota arī citiem partneriem.

Rokasgrāmatas pirmais izdevums 22. martā tika svinīgi prezentēts Tallinā esošajā NATO CCDCoE. CERT.LV draudu medību rokasgrāmatas praktiskais pielietojums tiks veicināts praktisku apmācību ciklā, kuras tiks organizētas Rīgā un būs pieejamas Latvijas un ārvalstu partneriem.

CERT.LV komanda ir līdere draudu medību operāciju organizēšanā un vadīšanā ES, sniedzot savu ieguldījumu NATO kolektīvajā aizsardzībā, veicinot starptautisko normu piemērošanu kibertelpā un veidojot uzticamu sabiedroto loku, kas spēj gan sniegt savstarpēju atbalstu kiberdraudu izvērtējumā, gan ātri apmainīties ar informāciju un labajām praksēm.

Sadarbības tikšanās, sanāksmes un konsultācijas kiberdrošības jomā

- Turpinās aktīva iesaiste Centrālās vēlēšanu komisijas (CVK) Vēlēšanu darba grupā, sniedzot rekomendācijas drošai vēlēšanu sistēmu izstrādei un uzturēšanai. CERT.LV eksperti regulāri piedalījās Vēlēšanu IT darba grupas sanāksmēs, sniedzot rekomendācijas saistībā ar sistēmu drošības aspektiem un testēšanu. CERT.LV arī sniedza savu redzējumu par IT riskiem CVK saistībā ar Eiropas Parlamenta 2024. gada vēlēšanu nodrošināšanu.
- Iesaiste Nacionālā koordinācijas centra vadītajā Starpinstitucionālajā darba grupā, kuras mērķis - veicināt informācijas apmaiņu starp valsts pārvaldes iestādēm un organizācijām par aktivitātēm un pasākumiem dažādās kiberdrošības jomās, lai sekmētu efektivitāti un sadarbību.
- Pārskata periodā tika veikta likumprojektu/iniciatīvu izskatīšana, tostarp 2 reizes izskatīti Eiropas Savienības līmeņa un 5 reizes Latvijas līmeņa likumprojekti, kā arī organizētas sanāksmes ar Latvijas līmeņa likumprojektu virzītājiem atsevišķu problēmjautājumu vai komentāru pārrunāšanai.

- 2. februārī CERT.LV uzņēma vizītē Latvijas Republikas aizsardzības ministru Andri Sprūdu, lai pārrunātu aktivitātes, kas tiek īstenotas Latvijas kiberspēju un kiberpārvaldības stiprināšanai.

- 4. martā CERT.LV vizītē uzņēma Valsts prezidentu Edgaru Rinkēviču, lai iepazīstinātu ar CERT.LV komandas darbu un līdz šim paveikto Latvijas kibertelpas drošības stiprināšanā. Vizītes ietvaros Valsts prezidents apmeklēja gan CERT.LV operāciju centru un industriālo kontroles iekārtu laboratoriju, gan iepazinās ar CERT.LV Incidentu risināšanas komandu un guva padziļinātāku ieskatu CERT.LV ikdienas darbā. E. Rinkēvičs īpaši atzinīgi novērtēja CERT.LV īstenotās veiksmīgās kiberdraudu meklēšanas operācijas kopā ar sabiedrotajiem.

5.2. CERT.LV atbalsts DDUK sekretariāta darbā

CERT.LV aktīvi piedalās Digitālās drošības uzraudzības komitejas (DDUK) darbā, tās ietvaros sniedzot atbalstu kvalificētu elektroniskās identifikācijas pakalpojumu sniedzēju un uzticamu sertifikācijas pakalpojumu sniedzēju uzraudzībā, kā arī veic Latvijas uzticamības saraksta (LV TSL – *LV trust list*) uzturēšanu. Papildus CERT.LV eksperti ir iesaistījušies topošās eIDAS 2.0 regulas projekta izskatīšanā, kā arī tā ietekmes uz DDUK plānotajiem darbiem novērtēšanā.

5.3. Izglītība un jauniešu kiberprasmju uzlabošana

CERT.LV piedalās Saldus tehnikuma administrācijas organizētajā darba grupā kvalifikācijas "Kiberdrošības tehniķis" standarta izstrādei, daloties ar savu pieredzi un sniedzot savu redzējumu par speciālistiem nepieciešamajām zināšanām, iemaņām un prasmēm, lai nodrošinātu, ka kvalifikācijas ieguvēji jau mācību laikā apgūst darbam nepieciešamās zināšanas un kļūst par augsti novērtētiem speciālistiem.

Latvijas kiberdrošības izaicinājums

Aizsardzības ministrijas Eiropas Savienības kiberdrošības jautājumu nodaļa organizē Eiropas mēroga kiberdrošības sacensību jauniešiem "Eiropas kiberdrošības izaicinājums 2024" (ECSC) Latvijas nacionālo atlasi. Latvija Eiropas kiberdrošības izaicinājumā piedalās pirmo reizi. Aktivitāte notiek Aizsardzības ministrijas NCC-LV koordinētā projekta ietvarā.

Lai nodrošinātu sekmīgu Latvijas komandas dalību ECSC sacensībās Itālijā, būtiska ir kiberdrošības kompetenču kopienas dalībnieku, īpaši augstskolu un privātā sektora uzņēmumu, iesaiste nacionālās atlases praktiskajā organizēšanā un atbalsta sniegšanā.

CERT.LV piedalās ECSC nacionālās atlases tīmekļa vietnes izveidošanā, kā arī nacionālās atlases nodrošināšanai nepieciešamās infrastruktūras un uzdevumu kopas sagatavošanas darbos.

Latvijas kiberdrošības izaicinājums 2024 norisināsies trīs kārtās:

- **1. kārta — 2024. gada 8. marts;**
- **2. kārta — 2024. gada 3.-4. aprīlis;**
- **3. kārta — 2024. gada 7.-8. maijs.**

Rezultāti tiks apkopoti un uzvarētāji paziņoti pēc 3. kārtas.

Eiropas kiberdrošības izaicinājums (ECSC)

Ikgadējās starptautiskās kiberdrošības sacensības, kuras organizē ES Kiberdrošības aģentūra (ENISA) sadarbībā ar dalībvalstīm un citiem partneriem.

Plašāk:
https://kibiz.lv/#about

6. Starptautiskā sadarbība

CERT.LV turpina pārstāvēt Latvijas intereses un stiprināt sadarbību ar citu valstu kiberdrošības incidentu novēršanas vienībām un starptautiskām organizācijām. Pārskata periodā CERT.LV darbinieki sniedza savu redzējumu un ieguldījumu dažādās darba grupās, daloties ar pieredzi un labo praksi, sniedzot konsultācijas un atbalstu, kā arī uzstājās ar prezentācijām starptautiskās konferencēs un semināros. Turpinājās arī darbinieku jaunu prasmju apgūšana un kvalifikācijas celšana, piedaloties starptautiskās mācībās.

Sadarbība ar CSIRTs tīklu, ENISA, Eiropas Savienības institūcijām un NATO

CERT.LV regulāri piedalās NIS (Tīklu un informācijas drošības) direktīvas *CSIRTs Network (CSIRT tīkls)* sadarbības tīkla sanāksmēs. *CSIRTs Network* darbu koordinē ENISA - Eiropas Savienības Kiberdrošības aģentūra, kas sniedz ieguldījumu ES politikā kiberdrošības jomā.

Pārskata periodā CERT.LV piedalījās *CSIRTs Network* darba grupā *Maturity*, kura rūpējas par ES dalībvalstu CSIRT komandu brieduma līmeņa paaugstināšanu.

Tāpat CERT.LV speciālisti turpināja aktīvi līdzdarboties ENISA organizētajās darba grupās:

CSIRTs Network (CSIRT tīkls)

Eiropas Savienības dalībvalstu kiberdrošības incidentu novēršanas institūciju tīkls nodrošina sadarbību starp kiberdrošības incidentu novēršanas vienībām Eiropas Savienībā. Tīkla sanāksmes notiek 3 reizes gadā, un tās organizē konkrētajā brīdī Eiropas Savienības Padomes prezidējošā valsts sadarbībā ar ENISA. Reizi gadā sanāksmē notiek arī apvienotās sesijas kopā ar NIS direktīvas Sadarbības grupu CyCLONe.

Plašāk:
https://csirtsnetwork.eu/
https://www.enisa.europa.eu/topics/incident-response/cyclone

- ***Coordinated Vulnerability Disclosure (CVD) Task Force*** – norit darbs pie ES līmeņa koordinētas ievainojamību atklāšanas politikas vadlīniju veidošanas;
- ***EU Cybersecurity Index*** – tiek izstrādāta kiberdrošības indeksa vērtības aprēķina metodoloģija dalībvalstu kiberdrošības novērtēšanai; turpinās darbs pie *EU Cybersecurity Index* platformas attīstīšanas;
- ***CSIRT Services Framework*** – tika turpināts darbs, izstrādājot vienotu ietvaru CERT komandu dalībnieku lomām, kompetencēm un prasmēm. Pārskata periodā tika veikta CERT komandu tipu noteikšanas metodoloģijas izstrāde, kas sekmētu veicamajiem uzdevumiem nepieciešamo lomu un kompetenču identificēšanu.

***CSIRT Network Situation Update* sanāksmes:** Pārskata periodā turpinājās regulāra dalība sanāksmēs, kuru mērķis ir veikt informācijas apmaiņu par aktuālo kibertelpā starp CSIRT tīkla biedriem.

Eiropas Komisijas EHDS (*European Health Data Space*) regulas darba grupa: CERT.LV speciālisti sniedza savu ieguldījumu darba grupā, kuras mērķis ir veicināt pacientu elektronisko datu pieejamību un iesaistīto pušu sadarbību Eiropas līmenī. Pārskata periodā darba grupa izvērtēja regulas saikni ar Mākslīgā intelekta aktu, Datu pārvaldības aktu un Vispārīgo datu aizsardzības regulu.

Regulāra CERT.LV ekspertu dalība Eiropas Kiberdrošības produktu sertifikācijas grupas ECCG *(European Cybersecurity Certification Group)* sanāksmēs, tajā skaitā divās tiešsaistes sanāksmēs martā, pārstāvot Latvijas intereses un sniedzot savu redzējumu par problemātiskiem jautājumiem, kas skar ES mākoņpakalpojumu sertificēšanas shēmas (EUCS) tālāku virzību uz priekšu ES valstīs.

ENISA organizētās mācības *CYBER EUROPE 2024:* Mācības norisināsies 19.-20. jūnijā, tiešsaistē. Latviju pārstāvēs Aizsardzības ministrija un CERT.LV, kā arī dalībnieki no enerģētikas nozares un datu centriem.

Sadarbība FIRST ietvaros

Turpinājās regulāra dalība *FIRST Membership Committee* (Jauno biedru uzņemšanas komitejas) sanāksmēs, lai apspriestu turpmākos noteikumus biedru uzņemšanā un piesaistīšanā, kā arī SIM3 modeļa pielietošanu komandu sertifikācijas procesā.

FIRST ir kiberdrošības organizācija, kas apvieno CERT, CSIRT, PSIRT, SOC komandas un citus kiberdrošības profesionāļus no visas pasaules.

2024. gada aprīlī FIRST biedri ir no 107 valstīm.

CERT.LV vadītāja Baiba Kaškina, turpinot pildīt *FIRST Membership Committee* priekšsēdētājas pienākumus, piedalījās jauno biedru pieteikumu izskatīšanā, kā arī veicināja biedru uzņemšanas procesa uzlabošanu.

Sadarbība TF-CSIRT ietvaros

Pārskata periodā CERT.LV ir viena no 47 Eiropas TF-CSIRT/*Trusted Introducer* sertificētām komandām (kopienā ir 515 komandas), kas apliecina CERT.LV komandas augsto brieduma un sagatavotības līmeni.

TF-CSIRT/Trusted Introducer ir Eiropas reģiona CERTu organizācija, kas apvieno incidentu reaģēšanas komandas no visiem sektoriem. Trusted Introducer serviss uztur uzticamu CERT vienību reģistru un veic vienību akreditāciju un sertifikāciju atbilstoši komandas demonstrētajam brieduma līmenim.

CERT.LV ir sertificēta Trusted Introducer komanda kopš 2016. gada 1. septembra.

Sertifikācijas uzturēšanai ik pēc trīs gadiem jāveic re-sertifikācijas process. 2022. gada 28. oktobrī, TF-CSIRT sanāksmē Viļņā, Lietuvā, tika paziņots, ka CERT.LV ir veiksmīgi re-sertificēta uz nākamajiem 3 gadiem (attiecīgi nākamais re-sertifikācijas process plānots 2025. gadā).

Sertifikācijas pamatā ir SIM3: *Security Incident Management Maturity Model* pieeja, kas vērtē organizācijas briedumu, skatoties uz organizatoriskiem, cilvēkresursu, izmantoto tehnisko rīku un procesu parametriem un to pielietojumu kvalitatīvai organizācijas darbības nodrošināšanai, primāri vērtējot incidentu risināšanas procesa briedumu.

Pārskata periodā CERT.LV turpināja darbu vairākās TF-CSIRT darba grupās.

Projekta Joint Threat Analysis Network īstenošana

CERT.LV komanda turpināja darbu pie projekta *Joint Threat Analysis Network* (turpmāk – JTAN projekts) īstenošanas. Kopējais JTAN projekta mērķis ir izveidot vienotu apdraudējumu analīzes tīklu. Tīkls būtu atvērts Eiropas CSIRT sadarbības grupai, kuras galvenā uzmanība pievērsta tehnisko, operatīvo un stratēģisko draudu izlūkošanas informācijas apmaiņai un analīzei.

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.

CERT.LV turpina *Graphoscope* risinājuma izstrādes darbus atbilstoši plānam. Pārskata periodā CERT.LV novirzīja papildu resursus projekta īstenošanai, piedalījās ikmēneša attālinātās JTAN projekta sanāksmēs, kurās projekta partneri informē par individuāliem projekta uzdevumiem un rezultātiem. Galvenās *Graphoscope* iezīmes:

GRAPHOSCOPE rīks paredzēts, lai korelētu datus no dažādiem datu avotiem un parādītu tos vizuālā formā.

- atbalsts daudziem datu avotiem un vienkārša sistēmas uzstādīšana;
- tīmeklī bāzēta saskarne, kas nav atkarīga no iepriekš instalētām datubāzēm;
- saskarne nodrošina elastīgus filtrus, atvieglojot liela apjoma datu analīzi.

Atbilstoši līgumam ar Eiropas Komisiju Nr. INEA/CEF/ICT/A2020/2373165, kas tika apstiprināts un uzsākts 2021. gada 1. jūlijā *2020 CEF Telecom Call – Cybersecurity* uzsaukumā, JTAN projekta īstenošana turpināsies līdz 2024. gada 30. jūnijam.

Citas starptautiskās aktivitātes

Pārskata periodā CERT.LV pārstāvji piedalījās vairākās starptautiska mēroga konferencēs un semināros, kā arī uzņēma vairākas ārvalstu delegācijas un piedalījās sanāksmēs ar ārvalstu delegāciju pārstāvjiem Latvijā. Būtiskākās aktivitātes:

No 16. līdz 17. janvārim Briselē, Beļģijā norisinājās NIS direktīvas *22. CSIRTs Network* sanāksme, kurā CERT.LV eksperti piedalījās ar savu ekspertīzi un pieredzi, nodrošinot efektīvu informācijas apmaiņu un sadarbību ar Eiropas Savienības CSIRT kopienu.

No 26. februāra līdz 1. martam Spānijā konferencē *Open Cyber Security Conference* uzstājās CERT.LV kiberdrošības speciālisti - Rūdolfs Ķelle ar prezentāciju *Prototyping a Network Intrusion Detection System: A Deep Dive into CERT.LV's IACS Lab for Safeguarding Critical Infrastructures* un Kārlis Svilans ar prezentāciju *Defending From the Beast in the East - Multinational Threat Hunting Operations*.

No 19. līdz 20. martam Prāgā, Čehijā konferencē *Prague Cyber Security Conference 2024* CERT.LV kiberdrošības eksperts Kristiāns Teters piedalījās paneļdiskusijā *Cloud Sovereignty or Cloud Solidarity? Finding Common Approach to Cloud Security* un dalījās pieredzē par aktuālo situāciju mākoņpakalpojumu drošības jomā un Latvijas pieredzi ar kiberdrošības prasībām mākoņpakalpojumu sniedzējiem, kā arī pozīciju mākoņpakalpojumu sertificēšanas jomā.

21. martā CERT.LV komanda kopā ar Kanādas bruņoto spēku pārstāvjiem viesojās pie NATO Kopējā kiberaizsardzības izcilības centra (CCDCoE) Tallinā, Igaunijā. Vizītes mērķis bija Draudu medību operāciju rokasgrāmatas prezentēšana un sadarbības pārrunāšana Draudu medību mācību kursa izveidē.

Turpinās regulāra CERT.LV ekspertu piedalīšanās *EU CyberNet* projekta ikmēneša sanāksmēs.
Projekta mērķis - 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.

Turpinās regulāra CERT.LV darbinieku dalība Ziemeļvalstu un Baltijas valstu drošības operāciju centra (*Nordic-Baltic SOC*) izveides koordinācijas darbā.

7. LIA Drošāka interneta centra ziņojumu pārskats

Latvijas Interneta asociācijas (LIA) Drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.01.2024. līdz 31.03.2024. ir saņēmusi un izvērtējusi 416 ziņojumus. No tiem 91 ziņojuma saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 18 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 32 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 164 ziņojumi, 25 ziņojumu saturs nav bijis pretlikumīgs, 71 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 53 ziņojumi par naida runu un bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 14 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kuru atrašanās vieta bija ārpus Latvijas, ir ievietoti INHOPE asociācijas datubāzē un iesniegti attiecīgās INHOPE valsts ziņojumu līnijai turpmāko darbību veikšanai, lai dzēstu nelegālo saturu no publiskas aprites.

Pārskata periodā no Latvijā uzturētajiem 91 ziņojuma par bērnu seksuālu izmantošanu saturošiem materiāliem 91 ziņojuma saturs ir dzēsts no publiskas aprites internetā.

LIA Drošāka interneta centra ziņojumu līnijas saņemtie ziņojumi no 01.01.2024. - 31.03.2024.

	Jan-24	Feb-24	Mar-24	Q1
Erotisks/ pornogrāfisks saturs bez izvietotiem brīdinājumiem	10	6	2	**18**
Pedofilija/ mazgadīgo prostitūcija/ bērnu seksuālu izmantošanu saturoši materiāli	30	12	49	**91**
Vardarbīga rakstura materiāli	1	1	2	**4**
Cieņas/ goda aizskaršana	14	7	11	**32**
Naida kurināšana/ rasisms	4	3	4	**11**
Finanšu krāpniecība	69	52	43	**164**
Konsultācijas/ padomi	35	22	14	**71**
Citi	7		18	**25**
KOPĀ:	**170**	**103**	**143**	**416**

Ziņojumi nosūtīti Valsts policijai	19	10	24	53
Ziņojumi nosūtīti INHOPE asociācijai	5	4	5	14
Kopā nosūtīti izskatīšanai	**24**	**14**	**29**	**67**

8. Nākamajā ceturksnī plānotie pasākumi

Svarīgākie virzieni un pasākumi 2024. gada 2. ceturksnī:

NIS2 un NKDL ieviešana: Sagatavošanās pasākumi, lai CERT.LV ir gatava sekmīgi turpināt darbu, kad tiks uzsākta NIS2 direktīvas piemērošana un tiks apstiprināts Nacionālās kiberdrošības likums (NKDL). Sekmējot Kiberdrošības pārvaldes reformas mērķu sasniegšanu, CERT.LV turpinās darbu pie jauno normatīvo aktu skaidrošanas, lai atbalstītu CERT.LV klientūru jauno prasību ieviešanā.

SOC izveide un attīstība: Turpinot mērķtiecīgi uzsāktās aktivitātes Drošības operāciju centra (SOC) attīstībā, plānots sākt sadarbību ar pirmajiem klientiem un sektoriem. Ir uzsākts aktīvs darbs ar vairāku valsts iestāžu infrastruktūras pievienošanu CERT.LV Drošības operāciju centram.

Pakalpojumu attīstība: CERT.LV turpinās attīstīt un popularizēt pakalpojumus (DNS ugunsmūri, pikšķerēšanas uzbrukumu simulāciju, koordinētu ievainojamību atklāšanu u.c.), lai nodrošinātu maksimālu aizsardzību valsts un pašvaldību iestāžu IKT resursu drošībai.

Draudu medību operācijas: CERT.LV turpinās stiprināt savu lomu kā līdere draudu medību operāciju organizēšanā un vadīšanā ES, veicinot stratēģisko sadarbību valsts un starptautiskā līmenī. Ciešā sadarbībā ar Kanādas Bruņoto spēku kiberpavēlniecību turpināsies draudu medību operācijas, sniedzot ieguldījumu NATO kolektīvajā aizsardzībā.

Sabiedrības izglītošana: CERT.LV eksperti turpinās informēt lēmumu pieņēmējus par situāciju kibertelpā. Ik mēnesi CERT.LV turpinās apkopot un publicēt kibertelpas būtiskāko notikumu pārskatu "Kiberlaikapstākļi" sabiedrības informēšanai. Dalība kiberkopienas pasākumos:

- **6. aprīlī** Rīgā kiberdrošības seminārā "No draudiem līdz izmeklēšanai", ko organizē *She Can Do IT* sadarbībā ar CERT.LV, ar savām zināšanām dalīsies CERT.LV kiberdrošības ekspertes Daina Ozoliņa un Dana Ludviga.

CERT.LV turpina aktīvi uzraudzīt kibertelpu, risināt un koordinēt incidentus, informēt un izglītot sabiedrību, veicinot stratēģisku sadarbību valsts un starptautiskā mērogā.

- **8. aprīlī** Rīgā CERT.LV eksperte Dana Ludviga piedalīsies studentu korporācijas "Imeria" rīkotajā viesu vakarā ar prezentāciju "Kiberdrošības aktualitātes, draudi un risinājumi".
- **11. aprīlī** Rīgā Baltic Security Conference paneļdiskusijā "Mākslīgā intelekta ietekme uz drošību" piedalīsies CERT.LV kiberdrošības eksperts Jānis Džeriņš. Papildus šajā konferencē CERT.LV tiks pārstāvēts ar stendu, kur plašākai sabiedrībai būs iespēja iepazīties ar CERT.LV piedāvātajiem pakalpojumiem.
- **13.–17. maijā** Digitālās nedēļas ietvaros LVRTC sadarbībā ar CERT.LV un NIC.LV 16. maijā organizēs vebināru "Kiberdrošа uzņēmuma anatomija digitālajā vidē" uzņēmējiem.

Starptautiskās sadarbības veicināšana: CERT.LV eksperti turpinās pārstāvēt Latvijas intereses un stiprināt sadarbību ar citu valstu kiberdrošības incidentu novēršanas vienībām un starptautiskām organizācijām, sniedzot konsultācijas un atbalstu, kā arī uzrunājot auditoriju dažādās konferencēs un semināros.

- **16.–17. aprīlī** Tiranā, Albānijā norisināsies seminārs *Effective CERT Constituency Building*, tā ietvaros CERT.LV vadītāja Baiba Kaškina sadarbībā ar *e-Governance Academy* pārstāvjiem vadīs tematiskas sesijas par būtiskiem publiskā un privātā sektora efektīvas sadarbības aspektiem kiberdrošības ekosistēmas izveidē, kā arī piedāvās savu redzējumu un risinājumus.

- **16.-17. aprīlī** Tallinā, Igaunijā CERT.LV pārstāvji prezentēs DDUK paveikto uzticamības pakalpojumu uzraudzības jomā FESA (*Forum of European Supervisory Authorities for Trust Service Providers*) un ENISA ECATS (*European Competent Authorities for Trust Services Expert Group*) ekspertu darba grupās, kā arī sniegs ieskatu par kiberdrošības situāciju uzticamības pakalpojumu jomā Latvijā.
- **13.–15. maijā** Kopenhāgenā, Dānijā notiks TF-CSIRT sanāksme, kurā CERT.LV kiberdrošības eksperte Sanita Vītola dalīsies ar CERT.LV pieredzi, izveidojot un iedzīvinot koordinētas ievainojamību atklāšanas procesu un platformu, kā arī CERT.LV pārstāvji vadīs CERT komandu starptautisko sabiedrisko attiecību darba grupas (*CERTS PR Working Group*) tikšanos. Darba grupas mērķis ir veicināt pieredzes apmaiņu sabiedrības izglītošanas un informēšanas jautājumos starp CERTu kopienas dalībniekiem.
- **22. maijā** Briselē, Beļģijā noritēs pieredzes apmaiņas tikšanās starp CERT.LV un CERT.BE. Šajā sanāksmē tiks apspriesti draudu medībās izmantotie rīki, incidentu reaģēšanas darba grupas darbības specifika, kā arī potenciālās CERT.LV un CERT.BE sadarbības iespējas nākotnē.
- **22.–23. maijā** Ģentē, Beļģijā notiks *23. CSIRTs Network* sanāksme, kas pulcēs kopā Eiropas CSIRT komandas un CERT-EU.
- **9.–14. jūnijā** Fukuokā, Japānā konferencē *36th Annual First Conference* uzstāsies CERT.LV kiberdrošības eksperts Rūdolfs Ķelle ar prezentāciju *From Laboratory to Grid: Advancing IACS Incident Response and Cyber Resilience.*

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, kā arī organizēt informatīvus un izglītojošus pasākumus gan valsts iestāžu darbiniekiem, gan IT drošības profesionāļiem, gan citiem interesentiem.

Saziņa ar CERT.LV:

Tālrunis: +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