Latvijas universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

2023 C1

Publiskais pārskats par CERT.LV uzdevumu izpildi

2023. gada 1. ceturksnis (01.01.2023. – 31.03.2023.)

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

Saturs

Kopsavilkums

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

Visa pārskata perioda garumā bija vērojami periodiski intensīvi Krievijas agresiju atbalstošu haktīvistu veikti piekļuves lieguma jeb DDoS uzbrukumi gan pret valsts pārvaldes iestādēm, gan pret finanšu, enerģētikas un transporta sektoru uzņēmumiem, taču tie lielākoties neradīja nekādu ietekmi uz mērķētajiem resursiem vai arī ietekme bija neliela.

9. janvārī notikušais incidents VAS "Latvijas Valsts radio un televīzijas centrs" (turpmāk - LVRTC) datu centrā, vienā no centrālajiem Latvijas sakaru infrastruktūras mezgliem, izraisīja plašus sakaru traucējumus, t.sk. mobilo sakaru nepieejamību dažos operatoru tīklos. Incidenta cēlonis nebija ārēja ietekme, bet gan kļūme plānotu iekšējo darbu laikā. Elektropiegāde tika atjaunota apmēram 20 minūšu laikā, bet lietotāji pakalpojumu problēmas izjuta ievērojami ilgāk. Incidents demonstrēja centrālo LVRTC datu centra lomu un rezerves risinājumu nepietiekamību.

Konstatēti ilgstoši mērķētu uzbrukumu mēģinājumi pret vairākām valsts iestādēm. Sekmīgi uzbrukumi nav atklāti, tehniskās pazīmes norāda uz Ķīnas uzbrucēju grupu *Mustang Panda*. Uzbrukumi tiek veikti ar e-pastu starpniecību, pielietojot Ukrainas atbalsta tematiku, uzbrucējam izliekoties par Ukrainas, NATO vai NATO dalībvalsts aizsardzības vai ārlietu resora darbinieku. Ķīnas uzbrucēju aktivitātes pret Latvijas mērķiem iepriekš ir novērotas ļoti reti. Iespējams, ka Ķīnai ir palielinājusies interese par Latviju, un Ķīnas uzbrukumi kļūs biežāki.

Sadarbībā ar ārvalstu partneriem no NATO tika turpināts veikt vairāku Latvijas IKT sistēmu ievainojamību pārbaudes un draudu medību operācijas, lai uzlabotu spēju atturēt apdraudējumus un reaģēt uz uzbrucēju darbībām. Draudu medības sniedz labāku izpratni par uzbrukumiem un

veicina sabiedroto komandu sadarbības spēju uzlabošanu un pieredzes apmaiņu, lai efektīvāk aizsargātu sistēmas, balstoties uz iegūto informāciju.

Aktualizējoties datu drošības jautājumam mobilajās ierīcēs saistībā ar sociālās lietotnes *TikTok* izmantošanu, CERT.LV rekomendēja īpaši iestāžu valdījumā esošās mobilās ierīces pārvaldīt centralizēti un iestādes drošības politikā paredzēt aizliegumu uzstādīt jebkādu lieku programmatūru, kas nav nepieciešama iekārtas darbībai vai arī darba pienākumu veikšanai, paredzot izņēmumus, kuri tiek pamatoti un izskaidroti, atsevišķu darbinieku līmenī.

Pārskata periodā tika reģistrētas 363 255 unikālas apdraudētas IP adreses, kas ir par nepilnu 1% vairāk nekā iepriekšējā ceturksnī un par 210% vairāk nekā šajā pašā periodā pirms gada. Izplatītākie apdraudējumi:

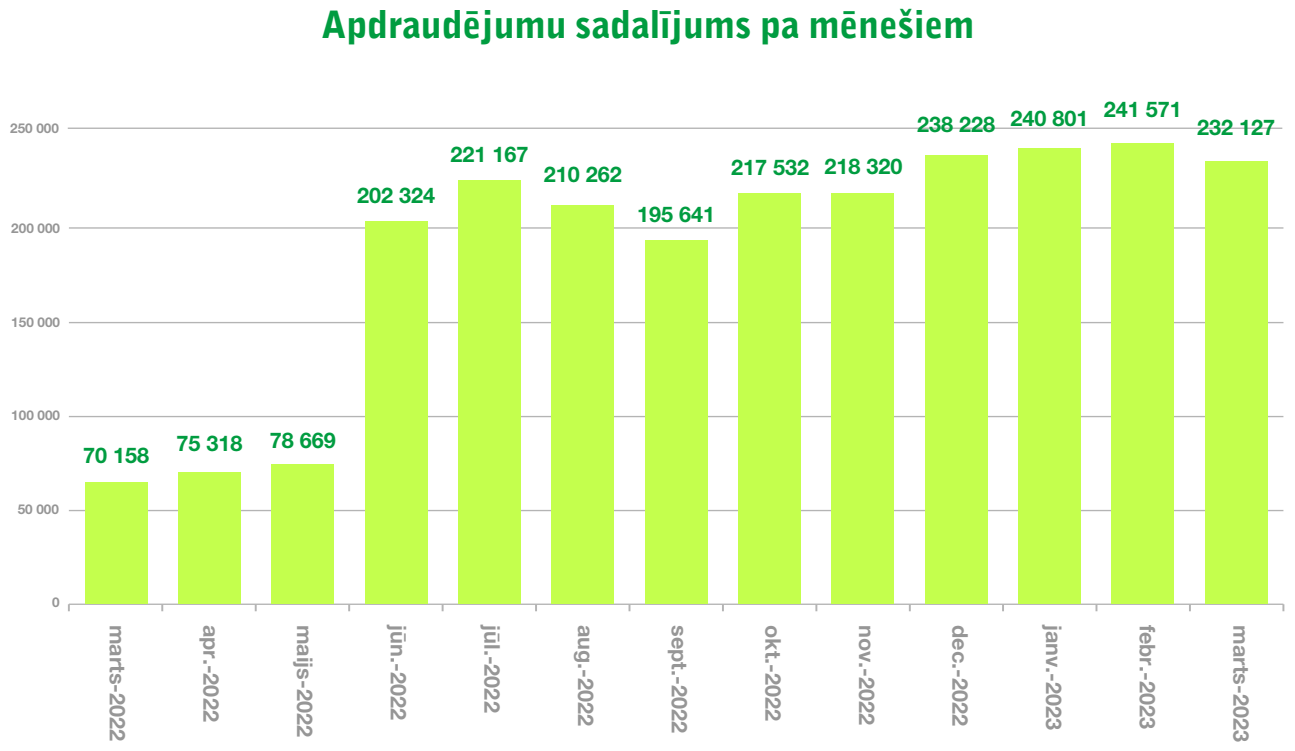
- konfigurācijas nepilnības (78 811 unikāla IP adrese) ar kritumu par 19% pret iepriekšējo periodu;
- ļaundabīgs kods (11 091 unikāla IP adrese) ar kritumu par 2%;
- pakalpojuma pieejamība (1002 unikālas IP adreses) ar kritumu par 65%.

30. martā norisinājās CERT.LV organizētais IT drošības seminārs *Esi drošs*, kas paredzēts valsts un pašvaldību iestāžu atbildīgajiem par IT drošību un citiem interesentiem. Semināra dalībnieki tika iepazīstināti ar jaunākajām normatīvo aktu iniciatīvām kiberdrošības jomā, koordinētas ievainojamību atklāšanas procesu valsts pārvaldē un CERT.LV izveidotās ievainojamību ziņošanas platformas cvd.cert.lv iespējām, Valsts elektroniskā sakaru pakalpojuma centra sniegtajām iespējām, domēna vārdu ilgtspējīgu izmantošanu, jaunu talantu atklāšanas iespējām kiberdrošībā un mobilo iekārtu drošu izmantošanu. Pasākumu klātienē apmeklēja 100, bet attālināti vēroja vairāk nekā 800 dalībnieki.

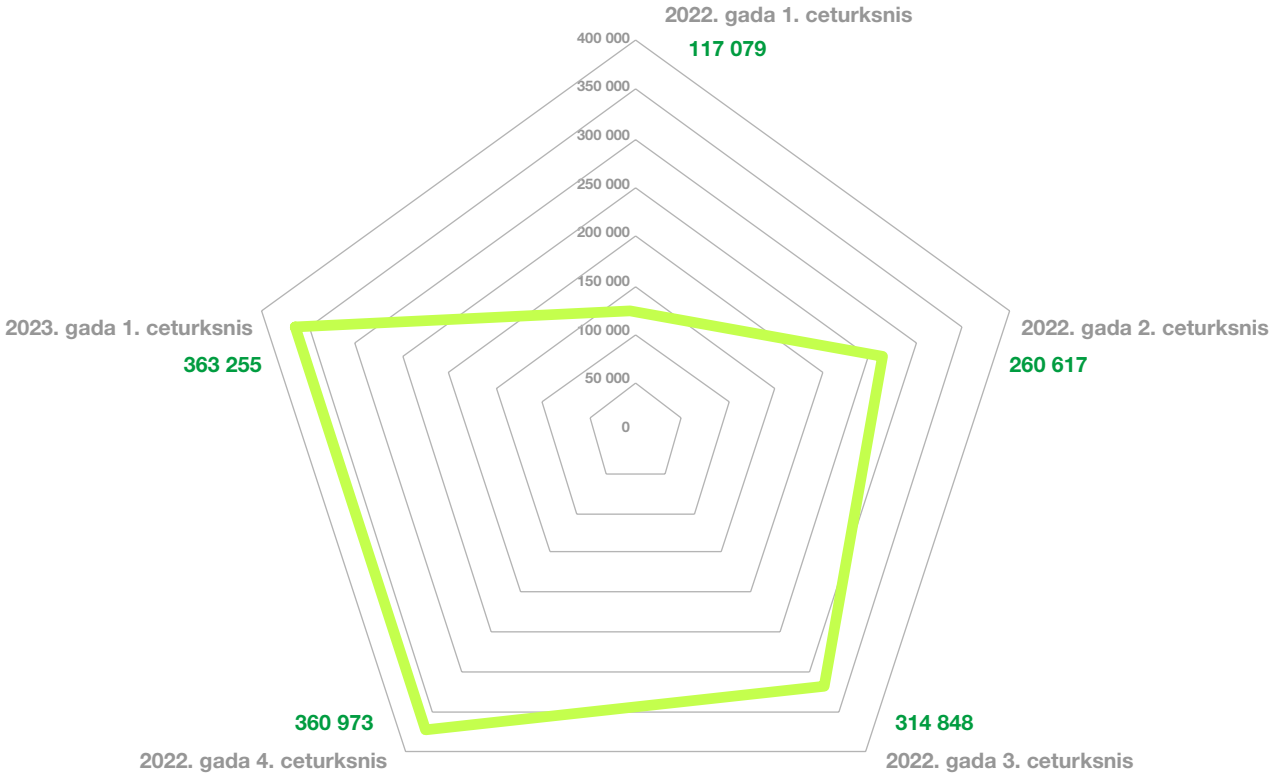
Pārskata periodā CERT.LV par IT drošību izglītoja 4430 cilvēkus, iesaistoties 20 izglītojošos pasākumos.

1. Vienota atainojuma uzturēšana par elektroniskās informācijas telpā notiekošajām darbībām

Ik mēnesi CERT.LV apkopo informāciju par apdraudētajām Latvijas IP adresēm. Lai sniegtu pilnvērtīgāku Latvijas kibertelpas pārskatu un nodrošinātu datu starptautisku salīdzināmību, CERT.LV apdraudējumu uzskaitei izmanto starptautiski lietotu incidentu taksonomiju (eCSIRT.net projekta izveidotā taksonomija, kas nosaukta par *Reference Security Incident Taxonomy*). Taksonomija ir formalizēts veids kā CERT.LV apkopo, sadala kategorijās un reprezentē par apdraudējumiem iegūto tehnisko informāciju. Statistikā visi CERT.LV reģistrētie apdraudējumi tiek



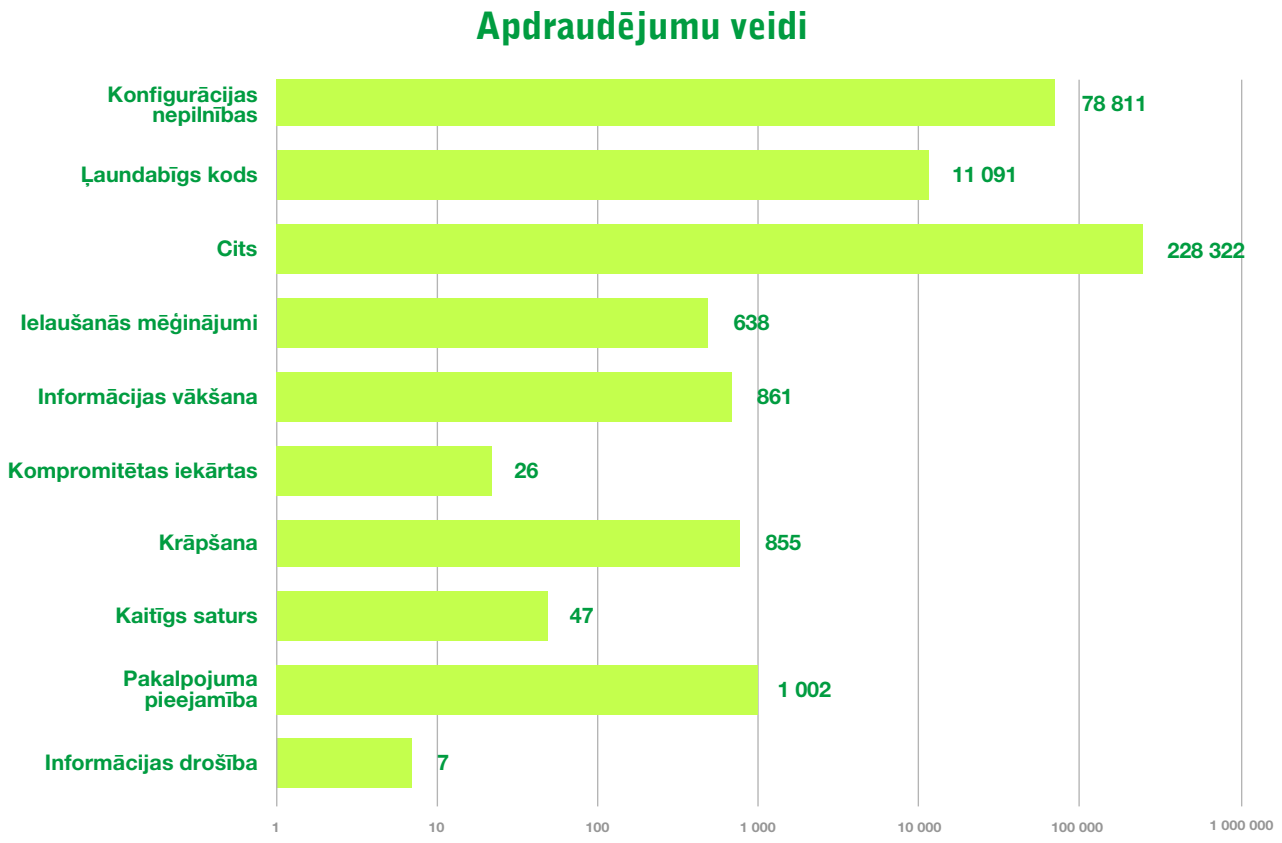
1. attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa mēnešiem 12 mēnešu griezumā.



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

uzskaitīti vienkopus, sadalot tos pa apdraudējumu veidiem (piemēram, ļaunatūra, ielaušanās, krāpšana), kā arī pa ļaunatūru (piemēram, *Confiker*, *Zeus*, *Mirai*) un konfigurācijas nepilnību (piemēram, *Opendns*, *Openrdp*) tipiem.

2023. gada 1. ceturksnī tika reģistrētas 363 255 unikālas apdraudētas IP adreses, kas ir par nepilnu 1% vairāk nekā iepriekšējā ceturksnī un par 210% vairāk nekā šajā pašā periodā pirms gada. Kopš

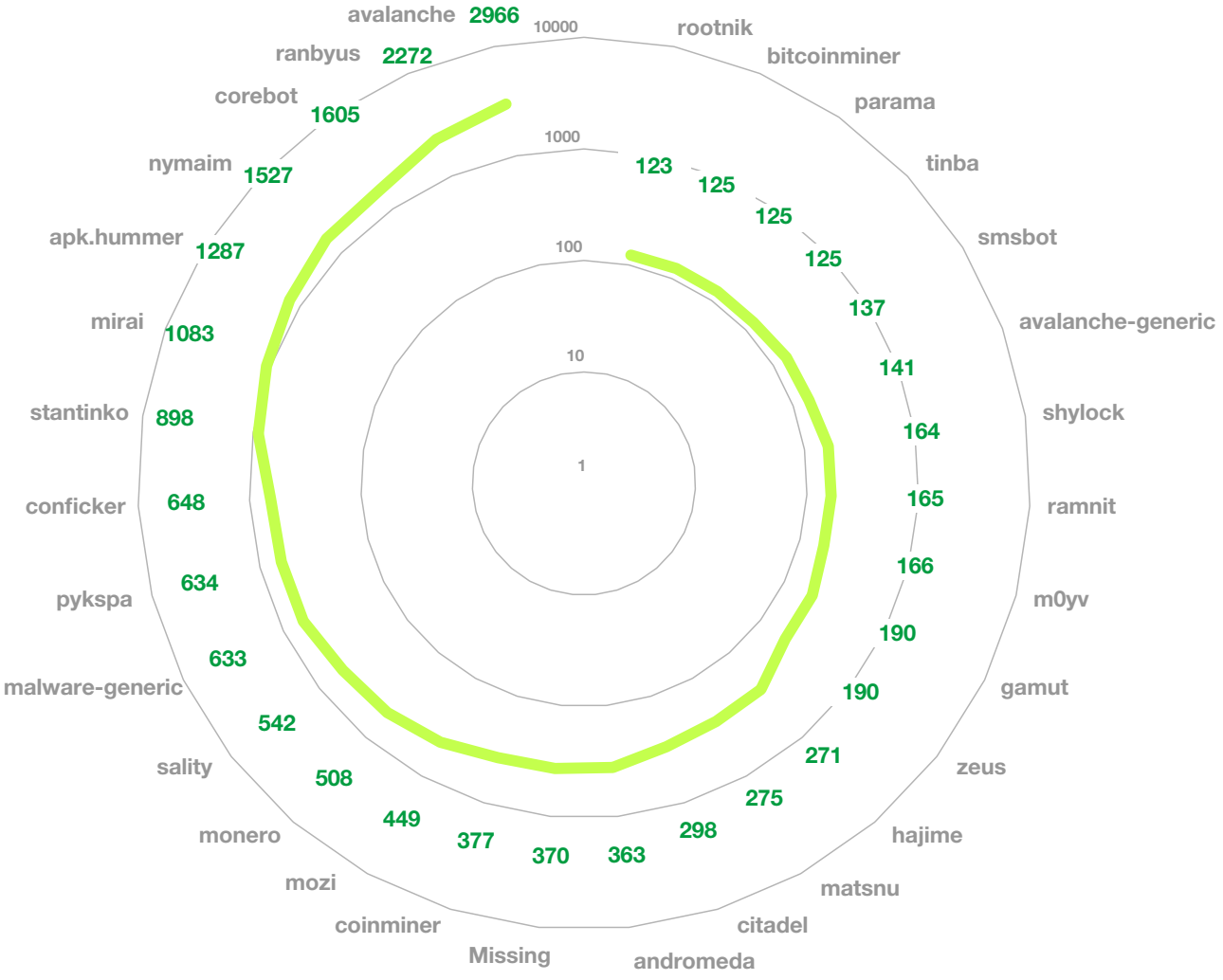


3. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2023. gada 1. ceturksnī pa apdraudējumu veidiem.

pagājušā gada vidus apdraudējumu līmenis Latvijas kibertelpā ir būtiski audzis. To ietekmējusi karadarbība Ukrainā un Krieviju atbalstošu haktīvistu, kā arī valsts sponsorētu grupējumu darbības.

Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (78 811 unikāla IP adrese) ar kritumu par 19% pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs kods (11 091 unikāla IP adrese) ar kritumu par 2%, bet trešais – pakalpojuma pieejamība (1002 unikālas IP adreses)

Unikālo IP adrešu skaits – ļaundabīgs kods



4. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2023. gada 1. ceturksnī ar apdraudējuma veidu – ļaundabīgs kods.

ar kritumu par 65%. Pakalpojuma pieejamības uzbrukumu intensitāte samazinājās uz ceturkšņa beigām, Krieviju atbalstošu haktīvistu grupējumiem pārvirzot uzmanību uz mērķiem Lietuvā.

Ļaunatūras topa pirmo vietu ieņem ļaunatūra *Avalanche,* kas no inficētajām iekārtām ievāc paroles un citu sensitīvu informāciju, lai to nosūtītu uz saimniekserveri, kā arī lejupielādē inficētajā iekārtā papildu ļaunprogrammatūras.

Otrajā vietā ierindojas ļaunatūra *Ranbyu*. Šī infekcija ievāc lietotāja izmantotās paroles un finanšu informāciju. Visbiežāk ļaunatūru *Ranbyus* iekārtā lejupielādē kāda cita tur jau esoša ļaunatūra, piemēram, *Andromeda/ Gamarue* vai *Matsnu*.

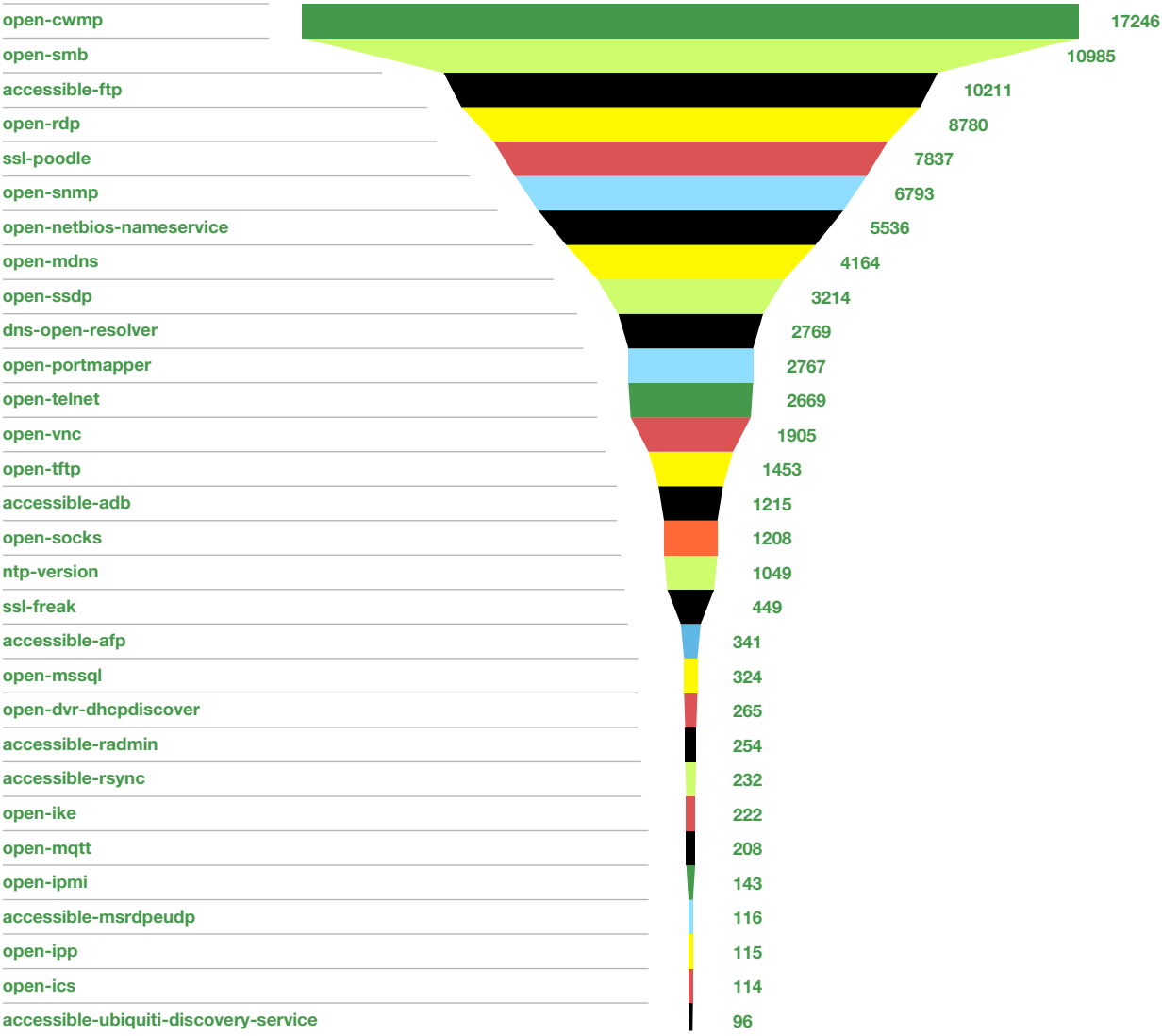
Trešajā vietā ir ļaunatūra *Corebot*, kuras uzdevums ir identificēt lietotāju aktivitātes, kas saistītas ar finansēm, pārtvert ievadīto informāciju un novilcināt tālākas lietotāju darbības, simulējot ielādes animāciju un aicinot ievadīt papildu datus. Tas sniedz uzbrucējiem laiku, lai pārtvertu sesiju un veiktu finanšu darbības upura vārdā.

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

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

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

Unikālo IP adrešu skaits – konfigurācijas nepilnības



5. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2023. gada 1. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

Pilnvērtīgākam kibersituācijas novērtējumam CERT.LV 2020. gadā ir uzsākusi *Apvienotās Karalistes Nacionālā kiberdrošības centra (NCSC)* izveidotās apdraudējumu matricas lietošanu. Matricā ievietotie apdraudējumi tiek grupēti pēc tā, cik nozīmīga ir skartā iestāde vai uzņēmums un/vai cik plašu sabiedrības daļu apdraudējums ietekmē, kā arī pēc tā, cik būtiskas sekas attiecīgais apdraudējums radīs. Apvienojot visus faktorus, apdraudējumi tiek iedalīti 6 kategorijās:

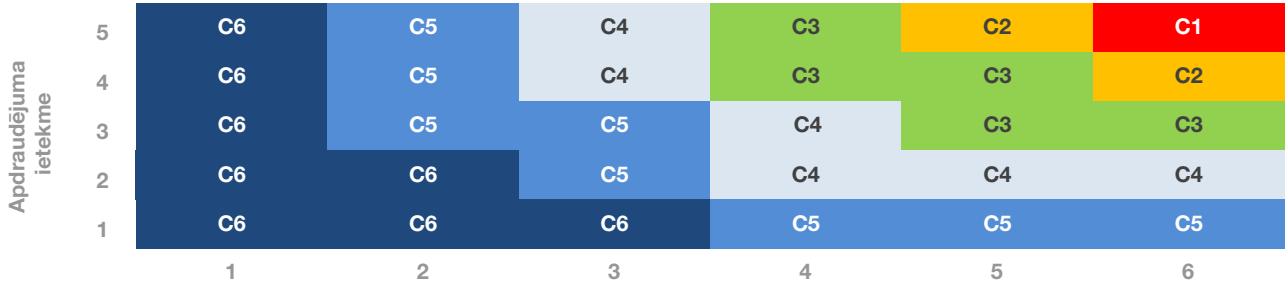
C1	Nacionāla līmeņa apdraudējums, ietekmēta pamatpakalpojumu sniegšana, apdraudēta ekonomiskā vai politiskā stabilitāte.
C2	Augstas nozīmes apdraudējumi, ietekmētas valsts iestādes, nacionālā infrastruktūra.
C3	Nozīmīgi apdraudējumi, plaša ietekme uz komerciālo sektoru, valsts un pašvaldību iestādēm.
C4	Būtiski apdraudējumi, vidēja ietekme uz komerciālo sektoru, valsts un pašvaldību iestādēm.
C5	Mēreni apdraudējumi, neliela ietekme uz komerciālo sektoru, valsts un pašvaldību iestādēm.
C6	Ikdienas apdraudējumi, ietekmē atsevišķus indivīdus, nenozīmīga ietekme uz uzņēmumiem vai valsts un pašvaldību iestādēm.

Vairāk nekā 98% apdraudējumu ietilpst maznozīmīgu apdraudējumu kopā (C6) un ir saistīti ar individuālu lietotāju iekārtām vai plaši izplatītiem ikdienišķiem, automatizētiem uzbrukumu mēģinājumiem uzņēmumiem vai valsts un pašvaldību iestādēm.

Nacionāla līmeņa apdraudējumi (C1) un augstas nozīmes apdraudējumi (C2) pārskata periodā nav reģistrēti.

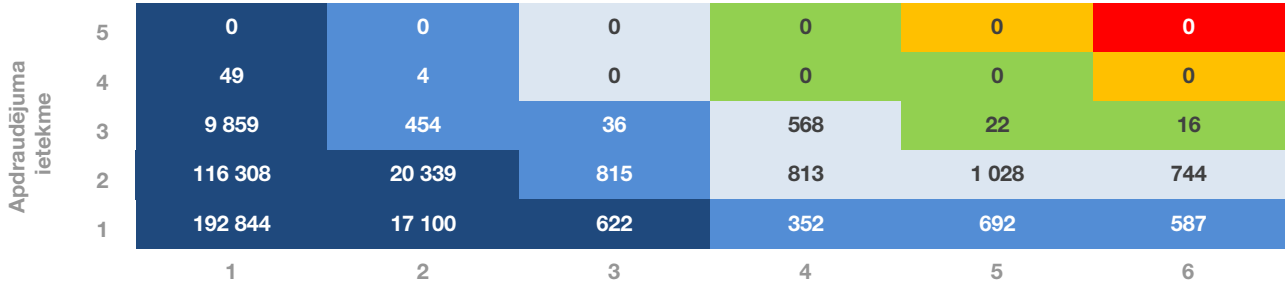
Nozīmīgi plašas ietekmes apdraudējumi (C3) veido 0,01% (38 unikālas apdraudētas IP adreses/gadījumi) no visiem kategorizētajiem apdraudējumiem. 63% šo apdraudējumu bija ļaundabīgs kods (Tieslietu ministrijā, Valsts ieņēmumu dienestā, AS *Rīgas siltums* un vairākās pašvaldībās), bet 37% veidoja pakalpojumu pieejamības incidenti.

Apdraudējumu matrica



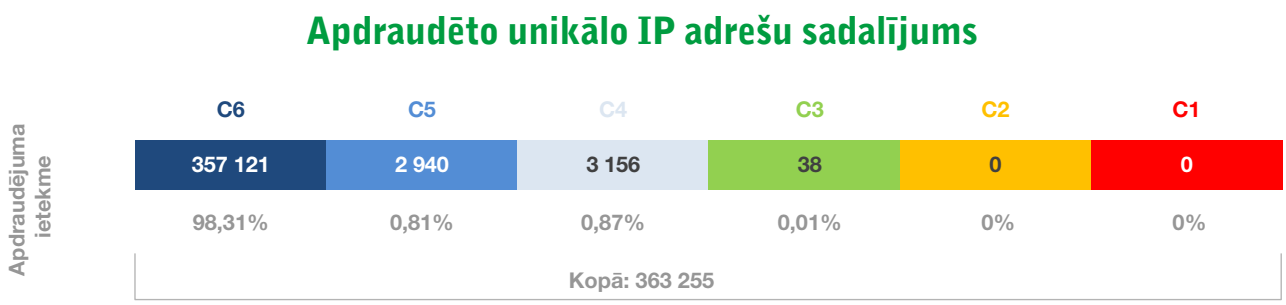
6. attēls – Apdraudējumu matricas sadalījums kategorijās.

Apdraudēto unikālo IP adrešu izvietojums



7. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu izvietojums matricā 2023. gada 1. ceturksnī valsts un pašvaldību institūcijās.

Lielākā daļa C4 līmeņa apdraudējumu (būtiski apdraudējumi ar vidēju ietekmi) jeb 20% bija pakalpojuma pieejamības incidenti augstas un vidēji augstas prioritātes iestādēs, 12% bija krāpšanas mēģinājumi, bet 9% - konfigurācijas nepilnības (*Open-socks, Accessible-ftp, ssl-poodle* u.c.).



8. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu sadalījums apdraudējumu kategorijās pēc apdraudējuma ietekmes (matrica) 2023. gada 1. ceturksnī.

Lai sekmētu kopējo kiberdrošību valstī, CERT.LV sadarbībā ar augstākā līmeņa domēna .LV reģistra uzturētāju (NIC) ir izstrādājusi DNS RPZ (*Domain Name Service Response Policy Zone*) jeb DNS ugunsmūri (*DNS firewall*). DNS mūris ik dienu tiek papildināts ar Latvijas iedzīvotāju un kiberdrošības ekspertu sniegto informāciju par kiberuzbrucēju aktivitātēm Latvijas kibertelpā un sniedz iespēju aizsargāt lietotājus no ļaundabīga satura internetā. Šis risinājums bez maksas ir pieejams jebkuram Latvijas iedzīvotājam, uzņēmumam un organizācijai. Informācija par darbību un uzstādīšanu: https://dnsmuris.lv/

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

CERT.LV sadarbojās ar valsts un pašvaldību institūcijām, bankām, interneta pakalpojumu sniedzējiem un citām organizācijām dažādas bīstamības incidentu risināšanā. Visos tālāk aplūkotajos incidentos uzbrukumu mēģinājumi bijuši nesekmīgi un zaudējumi nav radīti, ja vien nav norādīts citādi.

2.1 Krāpšana

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

Pārskata periodā tika novērota jauna tendence pikšķerēšanas uzbrukumos, kuros izmanto krāpnieciskus telefona zvanus – zvans tiek uzsākts lauzītā latviešu valodā, uzstājīgi piedāvājot pāriet uz krievu valodu. Uzbrucējiem acīmredzami ir pieeja cilvēkresursiem, kas nelielā apjomā apguvuši latviešu valodu. Zvani latviešu valodā varētu palielināt krāpniecības efektivitāti, tuvākajā nākotnē nodarot lielākus zaudējumus Latvijas tautsaimniecībai.

Turpinājās klasiski pikšķerēšanas uzbrukumi, izmantojot e-pastu, kas mērķēti pret Latvijas auditoriju, t.sk. izmantojot *VAS Latvijas Pasts*, portāla inbox.lv un lielāko Latvijas banku identitāti. Sociālajā tīklā *Telegram* tika konstatēti viltus kanāli, kas uzdevās par vairākām Latvijas bankām (piemēram, *Swedbank* un *Luminor*), bet kam ar šīm bankām nebija nekāda sakara. Ļaunprātīgas aktivitātes šajos kanālos netika konstatētas.

Martā, kas sakrīt ar periodu, kad iedzīvotāji var sākt iesniegt Valsts ieņēmumu dienestā (turpmāk - VID) gada ienākumu deklarāciju, lai atgūtu pārmaksāto iedzīvotāju ienākuma nodokli, sāka izplatīties krāpnieciskas īsziņas VID vārdā par nodokļu atmaksu ar saiti uz banku pikšķerēšanas vietni (galvenokārt *SEB*, bet saņemta informācija arī par *Luminor* un portālu latvija.lv). Nodokļu atmaksas temats figurēja arī pikšķerēšanas e-pastu kampaņā bankas *Citadele* vārdā.

Gan pret iedzīvotājiem, gan valsts iestādēm tika vērsta pikšķerēšanas kampaņa, kurā Pilsonības un migrācijas lietu pārvaldes (PMLP) vārdā e-pasta saņēmēji tika aicināti aizpildīt pielikumā pievienotu aptaujas anketu par Ukrainas pilsoņiem, kas uzturas Latvijā. Līdzīga kampaņa tika novērota arī Polijā.

Turpinājās krāpnieciskas aktivitātes, krāpniekiem uzdodoties par Valsts policiju un draudot ar sodu par pretlikumīgām darbībām. Arī krāpnieciski investīciju piedāvājumi joprojām bija aktuāli, un kāds iedzīvotājs cieta zaudējumus aptuveni 2500 eiro apmērā, iegādājoties kriptovalūtu un veicot investīcijas krāpnieciskā platformā.

CERT.LV novēroja vairākus krāpniecības mēģinājumus, kuros ļaundari izlikās par reāliem uzņēmumu vai iestāžu darbiniekiem un lūdza grāmatvedību/vadību atjaunot informāciju par konkrētā darbinieka algas kontu, nomainot to pret citu. Līdzīgas krāpniecības periodiski ir tikušas novērotas arī iepriekš.

Tika saņemta virkne ziņojumu par krāpnieku aktivitātēm, kurās izmantoti sabiedrībā atpazīstamu uzņēmumu zīmoli. Krāpnieki gan imitēja portālu un izvietoja maldinošu informāciju, gan publicēja viltus loterijas un reklāmas sociālajos tīklos. Uzbrucēju mērķis bija iedzīvotāju datu iegūšana. CERT.LV aicināja pirms jebkādu datu ievades pārbaudīt vietņu adreses un pārliecināties, vai atbilstošā loterija eksistē, pārbaudot informāciju uzņēmuma oficiālajā tīmekļa vietnē.

Kāds vērīgs iedzīvotājs CERT.LV ziņoja, ka konstatēts reģistrēts domēna vārds pmlp-gov-lv[.]online, kas var steidzīgākus un nevērīgākus Latvijas iedzīvotājus maldināt, izliekoties par Pilsonības un migrācijas lietu pārvaldi (PMLP). Šādu domēna vārdu ļaundari var izmantot uzbrukumos, viltojot PMLP identitāti, piemēram, veicot pikšķerēšanas uzbrukumus. Domēna vārds konfigurēts tā, ka spēj saņemt un izsūtīt e-pasta vēstules. Uzbrukumi pagaidām nav konstatēti.

2.2. Pakalpojuma pieejamība

Pārskata periodā tika novēroti vairāki liela apjoma pakalpojumu atteices uzbrukumi (DDoS) – koordinēti uzbrukumi pret banku, enerģētikas, transporta un valsts sektoriem no Krievijas Federāciju (KF) atbalstošu haktīvistu puses, kas radīja īslaicīgus traucējumus. To novēršanai tika pieslēgti papildu aizsardzības risinājumi. Koordinēti izmantoti vairāki uzbrukumu veidi (gan tīkla, gan lietojumprogrammu/aplikāciju līmenī), traucējumi lietotājiem lielākoties netika konstatēti. Uzbrukumi nav sasaistāmi ar kādiem vēsturiski nozīmīgiem datumiem vai aktuāliem notikumiem.

Pakalpojumu nepieejamību radīja arī vairākas ievērojamas tehniska rakstura problēmas, piemēram:

- Portāla latvija.lv atjaunināšanas darbi aizņēma ievērojami ilgāku laiku nekā sākotnēji plānots.
- 9. janvārī notikusī avārija LVRTC datu centrā, vienā no centrālajiem Latvijas sakaru infrastruktūras mezgliem, izraisīja plašus sakaru traucējumus, t.sk. mobilo sakaru nepieejamību dažos operatoru tīklos. Problēmu iemesls nav saistīts ar ārēju ietekmi, bet radās kļūme plānotajos darbos LVRTC iekšējos elektrotīklos, kā rezultātā izslēgusies datucentrā esošā aparatūra. Elektropiegāde atjaunota apmēram 20 minūšu laikā, lietotāji pakalpojumu problēmas izjutuši ievērojami ilgāk, jo iekārtas nav paredzētas pēkšņai izslēgšanai un pakalpojums neatjaunojas uzreiz pēc elektropiegādes atjaunošanas. Incidents demonstrēja centrālo LVRTC datu centra lomu un rezerves risinājumu nepietiekamību.
- Tika novēroti vairāku valsts iestāžu tīmekļa vietņu darbības traucējumi. Šīs tīmekļa vietnes tiek uzturētas Tīmekļvietņu vienotajā platformā. Tika konstatēts, ka platformas un tajā izvietoto vietņu darbību ietekmēja viena resursa atjaunošana no rezerves kopijas.
- Stundu tika traucēta resursa eveseliba.gov.lv darbība. Resurss piedzīvoja kiberuzbrukumu laikā, kad tika veikti arī plānoti iekšējie darbi, tāpēc nebija iespējams precīzi novērtēt uzbrukuma radīto ietekmi.

Uz pārskata perioda beigām DDoS uzbrukumu intensitāte mazinājās, uzbrukumiem vairs nenotiekot katru dienu. Uzbrucēju uzmanība tika pārvirzīta uz mērķiem Lietuvā.

2.3. Ļaundabīgs kods

Pārskata periodā tika saņemti ziņojumi par mēģinājumiem inficēt iekārtas, izmantojot ļaundabīgus e-pasta pielikumus, kā arī par nošifrētām iekārtām, uzbrucējiem izmantojot ievainojamības neatjauninātās sistēmās.

Tika saņemts ziņojums no kāda uzņēmuma par darbiniekiem masveidā iesūtītu kaitīgu e-pastu, kura pielikumā tika pievienots vīrusu saturošs attēls (.IMG fails). Uzņēmuma izmantotais antivīruss kaitīgo saturu neatpazina, taču uzņēmuma iekšējā drošības politika noteica .IMG failu bloķēšanu, kas nodrošināja potenciālā kaitējuma novēršanu. E-pasta pielikumā ieslēptā ļaunatūra tika identificēta kā *TrojanCryxos*, kas inficētajā iekārtā lejupielādē citas ļaunatūras, tai skaitā šifrējošos izspiedējvīrusus.

Īsi pirms 14.februāra (Valentīndienas) vairākas iestādes Latvijā saņēma mērķētas e-pasta vēstules ar *Google Drive* saiti, kas saturēja *.rar* arhīva failu, kas savukārt saturēja inficētu *.exe* izpildāmo failu. Neviens no CERT.LV identificētajiem saņēmējiem uzbrukumā necieta.

Kāds uzņēmums cieta šifrējošā izspiedējvīrusa *Royal Ransomware* uzbrukumā, vīrusam paplašinot mērķa iekārtu klāstu ar uzsvaru uz virtuālo mašīnu ESXi serveriem. CERT.LV izsūtīja brīdinājumus par ievainojamību CVE-2021-21974, kas tika izmantota *Royal Ransomware* uzbrukumos. Uzņēmums izmantoja ASV Kiberdrošības un infrastruktūras drošības aģentūras (CISA) februāra sākumā publicētos ieteikumus šifrēto VMware ESXi serveru atgūšanai.

Kādā citā uzņēmumā grāmatvedības datorā tika sašifrēti visi faili, kā arī tika konstatēts, ka visi servera faili ir šifrēti. Lai arī uzņēmumā izmantotā attālinātā piekļuve (RDP) tiek aizsargāta pret paroļu minēšanas uzbrukumiem (*brut-force*), pārējās uzņēmuma izmantotās tehnoloģijas uzskatāmas par

novecojušām, un tām netiek nodrošināts atbilstošs drošības līmenis un drošības ielāpi (*Windows XP* un *Windows Server 2003*). Uzņēmums vērsās ar iesniegumu policijā.

2.4. Ielaušanās mēģinājumi

Ielaušanās mēģinājumi 91% gadījumu veikti, izmantojot paroļu minēšanu (*brute-force*). Uzbrukumi vērsti galvenokārt pret dažādiem interneta pakalpojumu sniedzējiem. Pēc CERT.LV rīcībā esošās informācijas šie uzbrukumi nav bijuši sekmīgi.

Konstatēti ilgstoši uzbrukumu mēģinājumi (mērķēta pikšķerēšana) pret vairākām valsts iestādēm. Sekmīgi uzbrukumi nav konstatēti. Uzbrukumu tehniskās pazīmes norāda uz Ķīnas uzbrucēju grupu. Uzbrukumi tiek veikti ar e-pastu starpniecību, pielietojot Ukrainas atbalsta tematiku, uzbrucējam izliekoties par Ukrainas, NATO vai NATO dalībvalsts aizsardzības vai ārlietu resora darbinieku. Visbiežāk e-pasta vēstules uzbrucēji sūta no *Gmail*, *Yahoo* un citiem mākoņpakalpojuma e-pasta servisiem, tātad netiek lietotas oficiālo iestāžu e-pasta adreses. Ķīnas uzbrucēju aktivitātes pret Latvijas mērķiem iepriekš ir novērotas ļoti reti. Iespējams, ka Ķīnai ir palielinājusies interese par Latviju, un Ķīnas uzbrukumi kļūs biežāki.

2.5. Kompromitētas iekārtas un datu noplūdes

23. februārī Krievijas agresiju atbalstošiem haktīvistiem izdevies sekmīgi veikt uzbrukumu pret kādas valsts iestādes uzturētu projekta tīmekļa vietni, nopludinot gandrīz 10 000 datubāzes ierakstu. Izmeklēšanas gaitā secināts, ka tas uzturēts, neievērojot vispārējas drošības prasības gan attiecībā uz projektu, gan korporatīvā tīkla uzturēšanu kopumā.

Kopš 2023. gada februāra uz darba devēja iekārtām ASV federālajā valdībā un Eiropas Komisijā aizliegta *TikTok* lietotnes izmantošana. Līdzīgus ierobežojumus ieviesušas vairākas

Eiropas Savienības dalībvalstis. Arī Latvijas publiskajā sektorā vairākas ministrijas ir aizliegušas darbiniekiem izmantot TikTok lietotni, ja vien tas nav nepieciešams tiešo darba pienākumu pildīšanai.

CERT.LV ir izplatījis rekomendācijas par *TikTok* izmantošanu (https://cert.lv/lv/2023/03/par-tiktok-izmantosanu). CERT.LV ieskatā iestādes valdījumā esošās mobilās ierīces jāpārvalda centralizēti un drošības politikā jābūt noteiktam aizliegumam uzstādīt jebkādu lieku programmatūru, kas nav nepieciešama iekārtas darbībai vai arī darba pienākumu veikšanai. *TikTok* izmantošana sniedz iespēju uzrunāt jauniešu auditoriju, kas daļai valsts iestāžu varētu būt būtiski. Lai nezaudētu šo komunikācijas kanālu, iespējams, iestāžu un atsevišķu darbinieku līmenī būtu nepieciešams paredzēt izņēmumus, tos pamatojot un izskaidrojot.

2.6. Ievainojamības

Izsūtīti brīdinājumi vairākām pašvaldībām, kuru tīmekļa vietņu uzturēšanai tiek izmantota *Joomla* satura vadības sistēma, jo šīs vietnes tika identificētas kā apdraudētas un izmantotā programmatūras versija saturēja ievainojamību CVE-2023-23752, kas ļāva neautorizētam uzbrucējam piekļūt gala iekārtai, kas nodrošina tīmekļa pakalpojumus (*webservices*), kā arī noteiktos apstākļos veikt attālināto koda izpildi (RCE). CERT.LV aicināja vietņu uzturētājus uzstādīt atjauninājumus.

Izsūtīti brīdinājumi par *Fortigate* ievainojamību iestāžu pārvaldītajās IP adresēs. Ievainojamība sniedza uzbrucējam attālinātas koda izpildes iespēju. Iestādes tika aicinātas uzstādīt atjauninājumus.

Izsūtīti brīdinājumi par ievainojamību CVE-2021-21974, kas skāra VMware ESXi virtualizācijas servisu. Šī ievainojamība tika aktīvi izmantota šifrējošā datorvīrusa *ESXiArgs* izplatīšanai. CERT.LV aicināja atjaunināt šos serverus, līdz atjauninājumu uzstādīšanai ierobežojot servisam piekļuvi no interneta.

Publicēts brīdinājums par kritisku *Microsoft Outlook* "nulles dienas" ievainojamību CVE-2023-23397, kas kopš pagājušā gada tiek aktīvi izmantota arī no Krievijas APT grupējumu puses. Saskaņā ar *Microsoft* rīcībā esošo informāciju minētā ievainojamība izmantota ne tikai uzbrukumos Ukrainas resursiem, bet arī pret vairākām organizācijām Eiropā, to vidū arī valsts iestādēm un kritiskās infrastruktūras resursiem. Uzbrucējs var izgūt lietotāja paroles Net-NTLMv2 jaucējvērtību (*hash*), kura var tikt izmantota tālākos uzbrukumos, nosūtot lietotājam speciāli sagatavotu e-pasta vēstuli. Lietotāja iesaiste uzbrukuma procesā nav nepieciešama jeb uzbrukums var būt veiksmīgs arī tad, ja lietotājs inficēto e-pastu neatver.

2.7. Atbildīga ievainojamību atklāšana

Pārskata periodā tika saņemti daži maznozīmīgi ziņojumi. Sākot no 2023. gada 30. marta, Latvijas valsts un pašvaldību iestāžu IKT resursu ievainojamību ziņojumu reģistrēšanai un apstrādei pieejama CERT.LV izveidotā Ievainojamību ziņošanas platforma cvd.cert.lv.

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

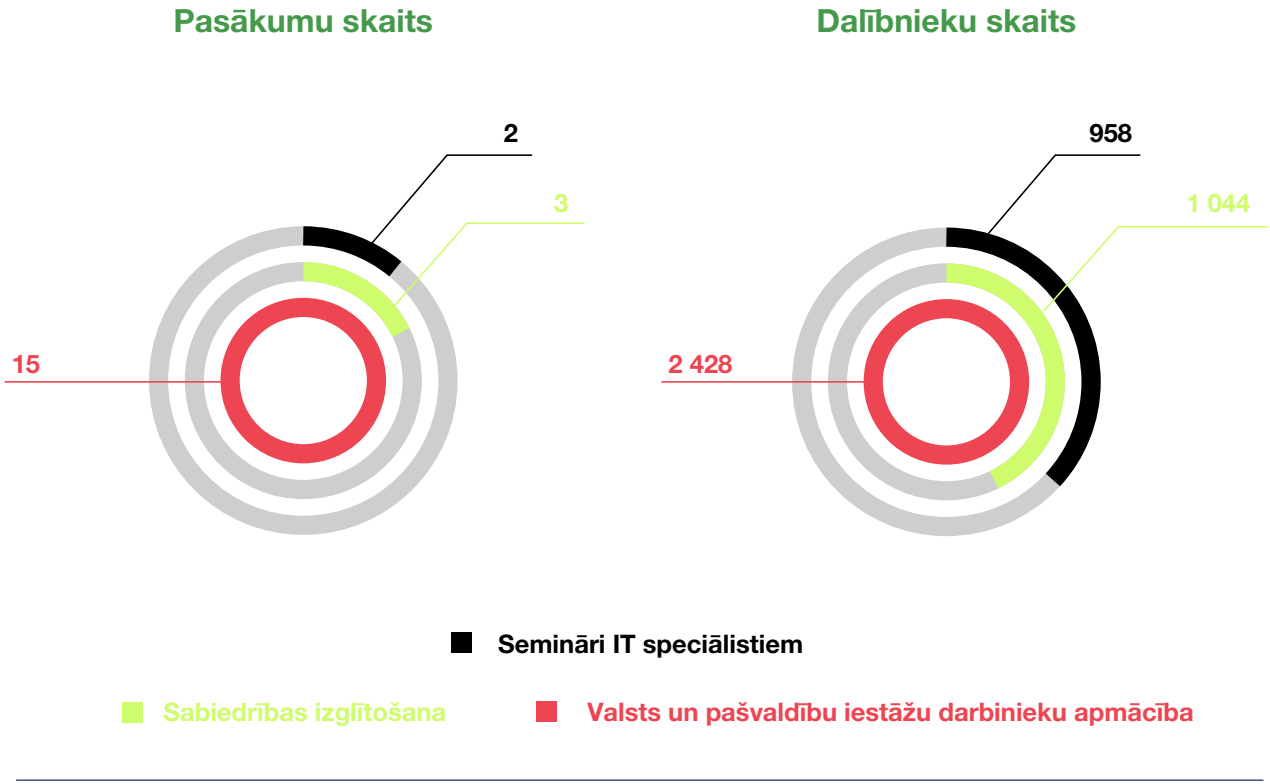
10. martā CERT.LV piedalījās augsta līmeņa ekspertu konferencē *Digitālais briedums un kibernoturība Latvijas ilgtspējai*, kuru organizēja biedrība *Latvijas Formula 2050* sadarbībā ar partneriem. CERT.LV uzsvēra, ka aizvadītais gads ir bijis līdz šim intensīvākais, bet reizē ļāva pārliecināties par Latvijas kibertelpas briedumu, kibertelpas dalībniekiem apliecinot spēju ātri pielāgoties un efektīvi sadarboties, tādējādi stiprinot kibertelpas noturību. CERT.LV norādīja arī uz Latvijas lieliski nodemonstrētajām spējām vadīt pasaules līmeņa kiberoperācijas. (https://www.youtube.com/watch?v=opKp6wuKY5Y)

22. martā CERT.LV piedalījās Valsts policijas Kibernoziegumu apkarošanas pārvaldes organizētajā starptautiskajā konferencē par aktualitātēm kibernoziegumu apkarošanā un izmeklēšanā, sniedzot prezentāciju par to, kā ģeopolitisko notikumu ietekmē mainījušās apdraudējumu tendences Latvijas kibertelpā. Konferencē tika apspriestas jomas tendences, inovācijas un izaicinājumi, īpašu uzmanību pievēršot sadarbības veicināšanai starp partneriem kibernoziegumu apkarošanai.

30. martā norisinājās CERT.LV organizētais IT drošības seminārs *Esi drošs*, kas paredzēts valsts un pašvaldību iestāžu atbildīgajiem par IT drošību un citiem interesentiem. Semināra dalībnieki tika iepazīstināti ar jaunākajām normatīvo aktu iniciatīvām kiberdrošības jomā, koordinētas ievainojamību atklāšanas procesu valsts pārvaldē un CERT.LV izveidotās ievainojamību ziņošanas platformas cvd.cert.lv iespējām, Valsts elektroniskā sakaru pakalpojuma centra sniegtajām iespējām, domēna vārdu ilgtspējīgu izmantošanu, jaunu talantu atklāšanas iespējām kiberdrošībā un mobilo iekārtu drošu izmantošanu. Pasākumu klātienē apmeklēja 100 dalībnieki, bet attālināti vēroja vairāk nekā 800 dalībnieki. (https://cert.lv/lv/2023/03/it-drosibas-seminars-esi-dross-marta)

Reaģējot uz intensīvo finanšu krāpnieku aktivitāti, *Luminor* banka sadarbībā ar CERT.LV izveidoja informatīvu video materiālu, kurā sabiedrība tiek aicināta izmantot CERT.LV un NIC

Izglītojošo pasākumu un apmācīto cilvēku skaits



9. attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2023. gada 1. ceturksnī

izveidoto un uzturēto bezmaksas rīku DNS ugunsmūris, lai pasargātu sevi un sev tuvos no krāpniecisku vai ļaundabīgu vietņu apmeklēšanas (https://www.facebook.com/LuminorLVA/posts/pfbid02woN5uzvecdy3QmMGpBcWUM4onBKtYfsp2JyFSvXJNbNNFedrwBz3uA3eRop6bEaKl).

Pārskata periodā CERT.LV par IT drošību izglītoja 4430 cilvēkus, iesaistoties 20 izglītojošos pasākumos.

Ikgadējā Baltijā vadošā kiberdrošības konference *Kiberšahs 2023* (CyberChess) norisināsies šī gada 4.-5. oktobrī. Diena pirms konferences, 3.oktobris, tiks veltīta semināriem un praktiskajām darbnīcām kiberdrošības jomas ekspertiem un interesentiem. Paralēli konferences norisei divu dienu garumā tiek plānotas arī *Capture the Flag (CTF)* sacensības. Šogad konferencei *Kiberšahs* pievienosies arī *Baltic domain days 2023*, lai apvienotu spēkus kiberdrošības jautājumu aktualizēšanā.

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

Sadarbības tikšanās, konsultācijas un prezentācijas:

- Tika sagatavoti komentāri par *Latvijas Kiberdrošības stratēģijas 2023.-2026. gadam* ieviešanas plāna uzdevumiem.
- Jaunā redakcijā komentēšanai tika saņemts Nacionālais kiberdrošības likums. Tika sniegtas rekomendācijas pilnvērtīgākai likuma redakcijas salāgošanai ar NIS2 direktīvas prasībām.
- Tika sniegti komentāri par Vides aizsardzības un reģionālās attīstības ministrijas izstrādāto MK noteikumu Nr. 597 *Informācijas sistēmu vispārējās tehniskās prasības* projektu, papildinot sadaļas, kas skar IS aktivitāšu kiberdrošības izvērtēšanu.
- Izskatīšanai tika saņemti labojumi MK noteikumu Nr. 442 *Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām* punkta *5.[1]* redakcijā, kas pieļauj datu glabāšanu NATO dalībvalstīs, tādējādi iestādēm/skolām ir iespēja izmantot *Google* nodrošinātos pakalpojumus.
- Dalība MK noteikumu Nr. 94 *Publisko elektronisko sakaru tīklu drošības prasības* izstrādes darba grupā. Noteikumi tika pieņemti 2023. gada 28. februārī.
- Sanāksmes ar Vides aizsardzības un reģionālās attīstības ministriju un citām iesaistītajām pusēm par koplietojamajiem skaitļošanas un datu glabāšanas

resursiem, veidojot Latvijas mākoņskaitļošanas federēto infrastruktūru. Tika pārrunāta e-pakalpojumu pieejamības nodrošināšana un nepieciešamie kontroles mehānismi tās uzraudzībai.

- Tika pabeigta koordinētas ievainojamību atklāšanas ziņojumu reģistrēšanas platformas izstrādes pirmā kārta. Platformas izstrāde tika uzsākta, balstoties uz Ministru kabineta apstiprināto Aizsardzības ministrijas sagatavoto informatīvo ziņojumu *Par koordinētas ievainojamību atklāšanas procesa ieviešanu valsts pārvaldē*, ar kuru ir uzsākta koordinētu ievainojamību atklāšanas procesa (turpmāk – CVD) ieviešana valsts pārvaldē, paredzot iespēju iestādēm brīvprātīgi iesaistīties CVD. Platforma nodrošinās iespēju pētniekam reģistrēt ziņojumu par novērotajām ievainojamībām iestāžu resursos, kā arī visiem iesaistītajiem (iestādei, pētniekam un CERT.LV) izvērtēt iesniegtos ziņojumus un sekot ievainojamību novēršanas gaitai. Pārskata periodā tika atvērta iestāžu pārstāvju un drošības pētnieku reģistrēšanās platformā.
- Aizsardzības ministrijas uzdevumā sagatavoti 9 sākotnējie izvērtējumi valsts informācijas sistēmu attīstības aktivitātēm (6 dažādi aktivitāšu iesniedzēji) un 1 atkārtots izvērtējums, bet 3 valsts informācijas sistēmu aktivitātēm tika izskatītas attīstības aktivitāšu iesniedzēju atbildes uz CERT.LV izvērtējumos iekļautajām rekomendācijām.
- 17. janvārī dalība Saeimas Sociālo un darba lietu komisijas sēdē, kurā tika apspriesti digitālās drošības riski un to novēršana attiecībā uz bērnu drošību internetā.
- 30. martā sanāksme Ekonomikas ministrijā par nepārtrauktas darbības nodrošinājumu tirdzniecības uzņēmumiem traucētas interneta pieejamības gadījumā.

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

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

CERT.LV starptautiskā sadarbība pārskata periodā:

- CERT.LV aktīvi piedalījās NIS (Tīklu un informācijas drošības) direktīvas CERTu tīkla darba grupā *Cyber Weather*, kura apkopoja informāciju par būtiskākajiem kiberincidentiem un reizi ceturksnī izstrādāja kiberlaikapstākļu pārskatu Eiropai. Tomēr 19. CERTu tīkla sanāksmē, kas notika 21. martā Lisabonā, Portugālē, *Cyber Weather* tika pieņemts lēmums par grupas darbības izbeigšanu, lai novērstu apkopojamās informācijas dublēšanu.
- Turpinājās darbs FIRST SIG darba grupā *CSIRT Services Framework*, izstrādājot vienotu ietvaru CERT komandu dalībnieku lomām, kompetencēm un prasmēm. Pārskata periodā turpinājās CERT komandu tipu noteikšanas metodoloģijas izstrāde, kas sekmētu veicamajiem uzdevumiem nepieciešamo lomu un kompetenču identificēšanu.
- Dalība FIRST *Membership Committee* (Jauno biedru uzņemšanas komitejas) sanāksmēs, lai apspriestu turpmākos noteikumus biedru uzņemšanā un piesaistīšanā, kā arī SIM3 modeļa izmantošanu. CERT.LV vadītāja Baiba Kaškina turpināja darbu kā FIRST *Membership Committee* priekšsēdētāja (*chair*), piedaloties jauno biedru pieteikumu izskatīšanā un veicinot biedru uzņemšanas procesa uzlabošanu.
- Dalība *EU CyberNet* projektā kā vienam no partneriem un piedalīšanās ikmēneša sanāksmēs. Projekta mērķis ir stiprināt kiberdrošības ekspertīzi un attīstīt to ne tikai Eiropas Savienībā, bet arī ārpus tās robežām (www.eucybernet.eu). Dalība projektā sniedz iespēju CERT.LV ekspertiem iesaistīties dažādos projektos, stiprināt savas zināšanas un kapacitāti.
- Dalība ENISA Eiropas kiberdrošības indeksa (*EU Cybersecurity index*) darba grupā, kurā tiek izstrādāta kiberdrošības indeksa vērtības aprēķina metodoloģija dalībvalstu

kiberdrošības novērtēšanai. Pārskata periodā pēc sākotnējā prototipa testēšanas darba grupa turpināja attīstīt *Cybersecurity index* platformas nākamo versiju.

- Dalība ENISA vadītajā darba grupā *Coordinated Vulnerability Disclosure (CVD) Task Force*, kurā norit darbs pie ES līmeņa koordinētas ievainojamību atklāšanas politikas vadlīniju veidošanas.
- 22. februārī CERT.LV vadīja kārtējo TF-CSIRT starptautisko CERT komandu sabiedrisko attiecību speciālistu darba grupas (CERTS PR *Working Group*) sanāksmi, kurā grupas pārstāvji dalījās pieredzē, sniedza grupas biedriem nepieciešamo atbalstu, kā arī apmainījās ar informāciju par aktuāliem novērojumiem kibertelpā, organizētajām kampaņām un jaunākajiem rīkiem komunikācijas procesu uzlabošanā.
- No 28. februāra līdz 3. martam CERT.LV pārstāvis apmeklēja Kosovu, lai dalītos pieredzē ar Kosovas kolēģiem un sniegtu atbalstu Kosovas Nacionālā kiberdrošības centra izveidē.
- 22. martā CERT.LV uzņēma pārstāvjus no Kopējā kiberaizsardzības izcilības centra (CCDCOE) un Kanādas Bruņoto spēku Latvijas Kaujas grupas štāba. CERT.LV dalījās iegūtajā unikālajā pieredzē par to, kā sadarbībā ar partneriem tiek veiktas draudu meklēšanas operācijas, lai identificētu pretinieku klātbūtni Latvijas kritiskās infrastruktūras sistēmās.

Sadarbība konkrētu incidentu risināšanā aplūkota pārskata 2. punktā.

6. Projekta Joint Threat Analysis Network īstenošana

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

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

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

2023. gada 1.ceturksnī CERT.LV turpināja darbu pie Grafoskopa izstrādes, tā attīstīšanas un pilnveidošanas, papildinot rīku ar jaunām funkcijām un uzlabojot esošās, tai skaitā publicēta jaunākā rīka versija *GitHub* platformā. Pārskata periodā CERT.LV piedalījās attālinātās JTAN projekta sanāksmēs, kurās projekta partneri informēja par saviem projekta uzdevumiem un rezultātiem.

2023. gada 29. martā notika CERT.LV organizētais Grafoskopa praktiskais seminārs, kurā dalībnieki tika iepazīstināti ar Grafoskopu un tā arhitektūru, mijiedarbību ar ārējiem datu avotiem un veidiem, kā šo rīku lietot. Tāpat seminārā tika demonstrēts, kā Grafoskopu uzstādīt, un parādīti tā pamata iestatījumi, kā arī savienošanās ar jaunu datu avotu.

Šajā pārskata periodā tika pieņemts lēmums, ka JTAN projektā plānotā ārpakalpojumu sniedzēja piesaiste nebūs nepieciešama, izstrādes darbus veiks CERT.LV un citu partneru speciālisti.

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

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

7. Citi normatīvajos aktos noteiktie pienākumi

- Tika turpināts darbs pie CERT.LV un augstākā līmeņa domēna .LV uzturētāja (NIC) izstrādātā DNS RPZ (*Domain Name Service Response Policy Zone*) jeb DNS ugunsmūra (*DNS firewall*) projekta īstenošanas. DNS mūris ik dienu tiek papildināts ar Latvijas iedzīvotāju un kiberdrošības ekspertu sniegto informāciju par kiberuzbrucēju aktivitātēm Latvijas kibertelpā un sniedz iespēju aizsargāt lietotājus no ļaundabīga satura internetā.

  DNS mūra darbības ietvaros ir bijuši jau daudzi gadījumi, kuros nostrādājusi aktīvā aizsardzība, pasargājot lietotājus no ļaundabīga satura un iekārtas no inficēšanas. Pārskata periodā lietotāji tika pasargāti no vairāku viltus lapu apmeklējumiem, maksājumu karšu datu zādzībām, viltus kurjerkompāniju tīmekļa vietņu apmeklējuma, kā arī tika liegts inficētām iekārtām sazināties ar vīrusu kontroles serveriem.

  Daļu no DNS PRZ pakalpojuma var izmantot bez līguma slēgšanas un autorizēšanās jebkurš interneta lietotājs. Lai to izmantotu, jālieto NIC rekursīvie DNS serveri. Tīmekļa vietnē https://dnsmuris.lv pieejamas ērti lietojamas instrukcijas DNS ugunsmūra aktivizēšanai.

  CERT.LV sadarbojas arī ar citām iestādēm, kuru uzdevums ir veidot bloķējamo vietņu sarakstus, un iekļauj šos sarakstus DNS ugunsmūrī, lai interneta pakalpojumu sniedzējiem, izvēloties izmantot DNS RPZ, būtu iespēja vienuviet iegūt visu informāciju par filtrējamajiem resursiem.

  Pārskata perioda laikā lietotāji tika pasargāti 83 243 reizes. Dažas no nozīmīgākajām aktīvās aizsardzības epizodēm (bloķētās vietnes):

  - Viltus banku tīmekļa vietnes: 938;
  - Apturēti paroļu pārsūtīšanas mēģinājumi uz kontrolserveriem: 1063;
  - Ar vīrusu saistītām aktivitātēm bloķētie pieprasījumi: 8433.

- Saskaņā ar MK 2015. gada 3. februāra sēdes protokolā Nr. 6 27. §, ar kuru pieņemts zināšanai informatīvais ziņojums *Par kompetento un atbildīgo iestādi, kura nodrošinās kvalificētu un kvalificētu paaugstinātas drošības elektroniskās identifikācijas pakalpojumu sniedzēju uzraudzību*, noteikto CERT.LV Digitālās drošības uzraudzības komitejas (DDUK) ietvaros turpināja uzraudzīt uzticamības pakalpojumu sniedzējus un kvalificētus elektroniskās identifikācijas pakalpojumu sniedzējus.

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

Latvijas Interneta asociācijas Drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.01.2023. līdz 31.03.2023. ir saņēmusi un izvērtējusi 593 ziņojumus. No tiem 356 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 15 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 20 ziņojumos konstatēta personas goda un cieņas aizskaršana, 10 ziņojumi saņemti par naida runu un 6 ziņojumos konstatēti vardarbīgi materiāli. Par finanšu krāpšanas mēģinājumiem internetā saņemti 84 ziņojumi, 47 ziņojumu saturs nav bijis pretlikumīgs, 55 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 187 ziņojumi par naida runu un bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 77 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kuru atrašanās vieta bija ārpus Latvijas, ir ievietoti INHOPE asociācijas datu bāzē un iesniegti attiecīgās INHOPE valsts ziņojumu līnijai turpmāko darbību veikšanai, lai dzēstu nelegālo saturu no publiskās aprites. Pārskata periodā no Latvijā uzturētajiem 186

ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem 184 ziņojumi ir dzēsti no publiskas aprites un 2 ziņojumu saturs atrodas dzēšanas procesā sadarbībā ar Valsts policiju un interneta pakalpojumu sniedzējiem.

2023. gada 22. maijā.

CERT.LV misija ir veicināt informācijas tehnoloģiju (IT) drošību Latvijā.

Galvenie CERT.LV uzdevumi ir uzturēt un aktualizēt informāciju par IT drošības apdraudējumiem, sniegt atbalstu valsts institūcijām IT drošības jomā, sniegt atbalstu IT drošības incidentu novēršanā jebkurai fiziskai vai juridiskai personai, ja incidentā iesaistīta Latvijas IP adrese vai .LV domēns, organizēt informatīvus un izglītojošus pasākumus gan valsts iestāžu darbiniekiem, gan IT drošības profesionāļiem, gan citiem interesentiem.

Saziņa ar CERT.LV:

Telefons: +371 67085888

E-pasts: cert@cert.lv

Tīmekļa vietne: www.cert.lv

Sekot CERT.LV aktualitātēm:

www.twitter.com/certlv

www.facebook.com/certlv

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija