Latvijas universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

2023 C3

Publiskais pārskats par CERT.LV uzdevumu izpildi

2023. gada 3. ceturksnis (01.07.2023. – 30.09.2023.)

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

Saturs

Kopsavilkums 4

1. Vienota atainojuma uzturēšana par kibertelpā notiekošajām darbībām 6

2. Atbalsts kiberdrošības incidentu novēršanā un koordinēšanā 16

- 2.1. Krāpšana 16
- 2.2. Pakalpojuma pieejamība (DDoS) 18
- 2.3. Ļaundabīgs kods 19
- 2.4. Ielaušanās mēģinājumi 20
- 2.5. Kompromitētas iekārtas un datu noplūdes 20
- 2.6. Ievainojamības 22
- 2.7. Atbildīga ievainojamību atklāšana 24

3. Pētnieciskais darbs, apmācību un izglītojošu pasākumu organizēšana kiberdrošības jomā *24*

4. Atbalsts valsts institūcijām kibertelpas drošības sargāšanā, noziedzīgu nodarījumu un likumpārkāpumu atklāšanā *26*

5. Sadarbība ar starptautiski atzītām kiberdrošības incidentu novēršanas institūcijām *27*

6. Projekta Joint Threat Analysis Network īstenošana *30*

7. Citi normatīvajos aktos noteiktie pienākumi *31*

8. Atskaite par Latvijas Interneta asociācijas Drošāka interneta centra ziņojumu līnijas darbību *32*

Kopsavilkums

Kiberapdraudējumu līmenis Latvijas kibertelpā 2023. gada 3. ceturksnī joprojām ir augsts, arī salīdzinājumā pret šo pašu periodu pagājušajā gadā, taču kiberdrošības situācija vērtējama kā stabila.

CERT.LV seko līdzi Krievijas hakeru grupējumu pakalpojumu atteices uzbrukumu (DDoS) virzībai. Pārskata periodā DDoS aktivitātes bija vērstas galvenokārt pret valsts iestādēm, kā arī finanšu, transporta un enerģētikas nozaru uzņēmumiem, bet uzbrukumu mērķu infrastruktūras bija gatavas uzbrukumus atvairīt, un tie neradīja jūtamu ietekmi uz pakalpojumu pieejamību. Arī turpmāk tiek prognozēta augsta DDoS intensitāte pret Latvijas resursiem. Krievijas hakeru grupējumi veic uzbrukumus, balstoties uz retoriku, ka tie turpināsies, kamēr turpināsies atbalsts Ukrainai.

Pārskata periodā Krievijas atbalstīti haktīvistu grupējumi ir veikuši plaša mēroga kiberuzbrukumus valsts iestāžu resursiem Latvijā, piemēram, ir novēroti pikšķerēšanas uzbrukumi e-pasta sistēmu lietotājiem valsts pārvaldē. Tomēr līdz šim tie nav radījuši būtisku ietekmi valsts un kritiskās infrastruktūras sektorā.

Pret Latvijas iedzīvotājiem tika vērsts liels apjoms komerciāli motivētu krāpniecisku aktivitāšu, kurās uzbrucēji, gan izmantojot īsziņas, gan krāpnieciskus telefona zvanus, un uzdodoties par valsts iestāžu vai organizāciju, tostarp arī Valsts policijas un CERT.LV darbiniekiem, centās iegūt internetbankas piekļuves datus. Vairāki iedzīvotāji krāpniecības neatpazina un zaudēja finanšu līdzekļus.

Pārskata periodā tika reģistrētas 336 220 unikālas apdraudētas IP adreses, kas ir tikai par 0,1% vairāk nekā iepriekšējā ceturksnī, toties par 7% vairāk nekā šajā pašā periodā pirms gada. 2023. gada 3. ceturksnī izplatītākie bija šādi apdraudējumi:

- **konfigurācijas nepilnības** (71 489 unikālas IP adreses) ar kritumu par 6% salīdzinājumā pret iepriekšējo ceturksni un par 39% mazāk nekā šajā pašā periodā pirms gada;
- **ļaundabīgs kods** (6962 unikālas IP adreses) ar kritumu par 1% salīdzinājumā pret iepriekšējo ceturksni un par 33% mazāk nekā šajā pašā periodā pirms gada;
- **ielaušanās mēģinājumi** (1200 unikālas IP adreses) ar pieaugumu par 90% salīdzinājumā pret iepriekšējo ceturksni un par 31% vairāk nekā šajā pašā periodā pirms gada.

CERT.LV kopā ar augstākā līmeņa domēna .LV reģistra uzturētāju (NIC) turpina uzturēt DNS RPZ (*Domain Name Service Response Policy Zone*) jeb DNS ugunsmūra pakalpojumu. DNS ugunsmūris bez maksas ir pieejams ikvienam Latvijas iedzīvotājam un organizācijai. Ik dienu DNS ugunsmūris tiek papildināts ar krāpnieciskām saitēm, ko iesūtījuši kiberdrošības speciālisti, iedzīvotāji un identificējusi CERT.LV komanda, tādējādi pasargājot no uzbrukuma DNS ugunsmūra lietotājus. Pārskata perioda laikā lietotāji tika pasargāti **40 837** reizes. Nozīmīgākās aktīvās aizsardzības epizodes:

- bloķētas viltus lapas, kur lietotāji saņēma īsziņu (SMS) veidā: 731;
- bloķēta lietotāja pārvirze uz kaitīgām lapām: 8 945;
- viltus bankas lapu bloķētie pieprasījumi datu izkrāpšanai: 104.

Pārraugot Latvijas kibertelpas notikumu attīstību, reizi mēnesī CERT.LV apkopoja un analizēja datus par svarīgākajiem notikumiem “Kiberlaikapstākļi” formātā, lai informētu sabiedrību par norisēm piecās kiberapdraudējumu kategorijās.

Pārskata periodā CERT.LV eksperti par kiberdrošību izglītoja 2112 cilvēkus, iesaistoties 20 izglītojošos pasākumos un profesionālās diskusijās. Tika sniegta informācija plašsaziņas līdzekļiem, attiecīgi ar 255 publikācijām, sasniedzot vairāk nekā 13 000 auditoriju.

Notika aktīvs darbs pie starptautiskās kiberdrošības konferences *CyberChess 2023* organizēšanas pēdējās fāzes. Konferences norise paredzēta 2023. gada 4. - 5. oktobrī.

CERT.LV turpina pildīt savu misiju un sadarbībā ar partneriem rāda efektīvu pretstāvi šī brīža ģeopolitiskajiem un hibrīdkara apstākļu izaicinājumiem, stiprinot drošības infrastruktūras attīstību, lai aizsargātu un nodrošinātu Latvijas iedzīvotājiem svarīgu resursu pieejamību.

1. Vienota atainojuma uzturēšana par kibertelpā notiekošajām darbībām

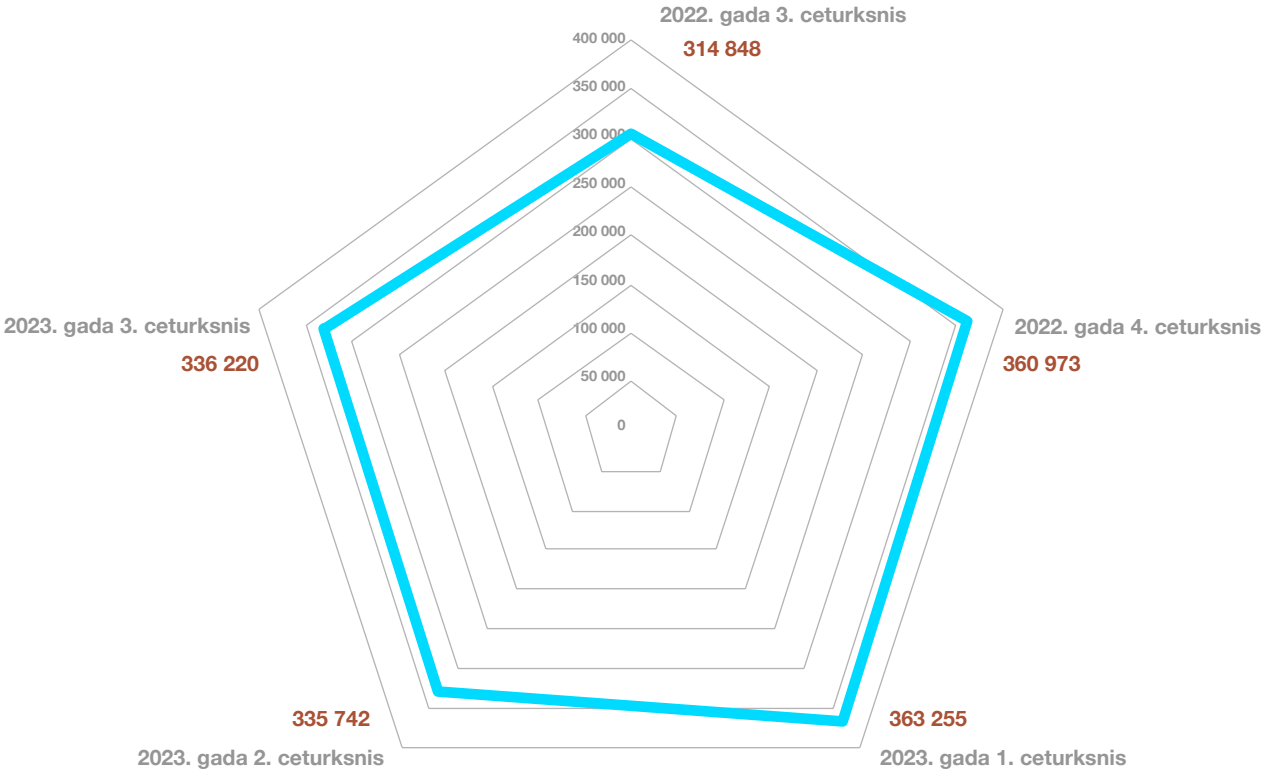
Ik mēnesi CERT.LV apkopo informāciju par apdraudētajām Latvijas IP adresēm. Lai sniegtu pilnvērtīgāku Latvijas kibertelpas pārskatu un nodrošinātu datu starptautisku salīdzināmību, CERT.LV apdraudējumu uzskaitei izmanto starptautiski lietotu incidentu taksonomiju (*Reference Security Incident Taxonomy*).

Taksonomija ir formalizēts veids kā CERT.LV apkopo, sadala kategorijās un reprezentē par apdraudējumiem iegūto tehnisko informāciju. Statistikā visi CERT.LV reģistrētie apdraudējumi tiek uzskaitīti vienkopus, sadalot tos apdraudējumu veidos (piemēram, ļaunatūra, ielaušanās, krāpšana), kā arī pa ļaunatūru (piemēram, *Confiker*, *Zeus*, *Mirai*) un konfigurācijas nepilnību (piemēram, *Opendns*, *Openrdp*) tipiem.

2023. gada 3. ceturksnī tika reģistrētas 33 6220 unikālas apdraudētas IP adreses, kas ir par 0,1% vairāk nekā iepriekšējā ceturksnī un par 7% vairāk nekā šajā pašā periodā pirms gada.

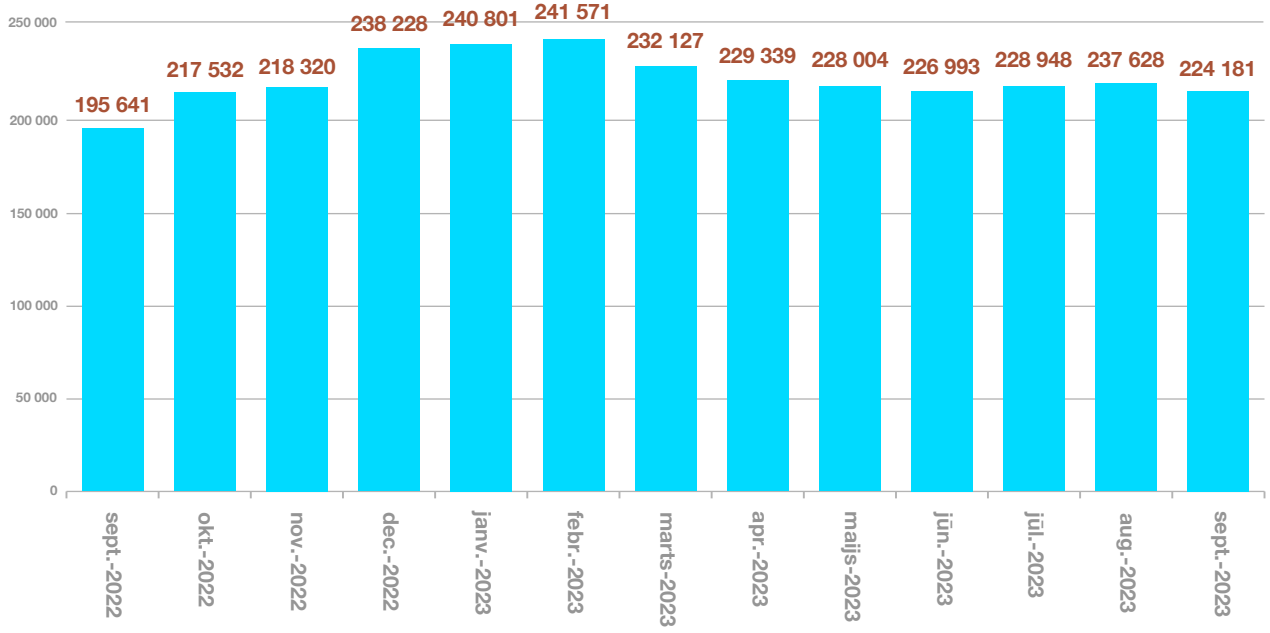
Kopš pagājušā gada vidus apdraudējumu līmenis Latvijas kibertelpā ir būtiski audzis, un saglabājas, augsts. Katra no ģeopolitiskajām un digitālajām pārmaiņām ir izaicinājums arī kibertelpas drošībai. To ietekmējusi karadarbība Ukrainā un Krieviju atbalstošu haktīvistu, kā arī valsts sponsorētu grupējumu darbības.

Apdraudējumu sadalījums pa ceturkšņiem



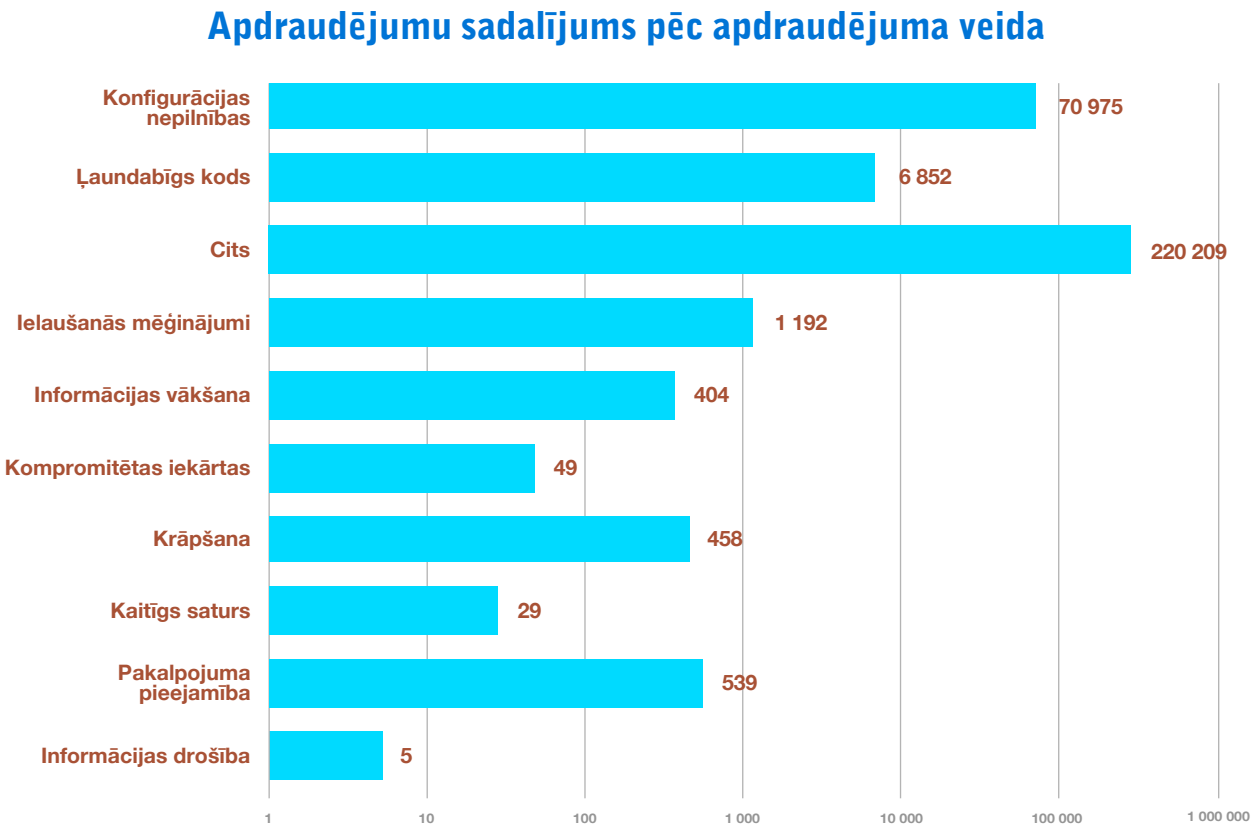
1 . attēls – CERT.LV reģistrētās apdraudētās IP adreses pa ceturkšņiem 2022. un 2023. gadā.

Apdraudējumu sadalījums 12 mēnešu griezumā



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

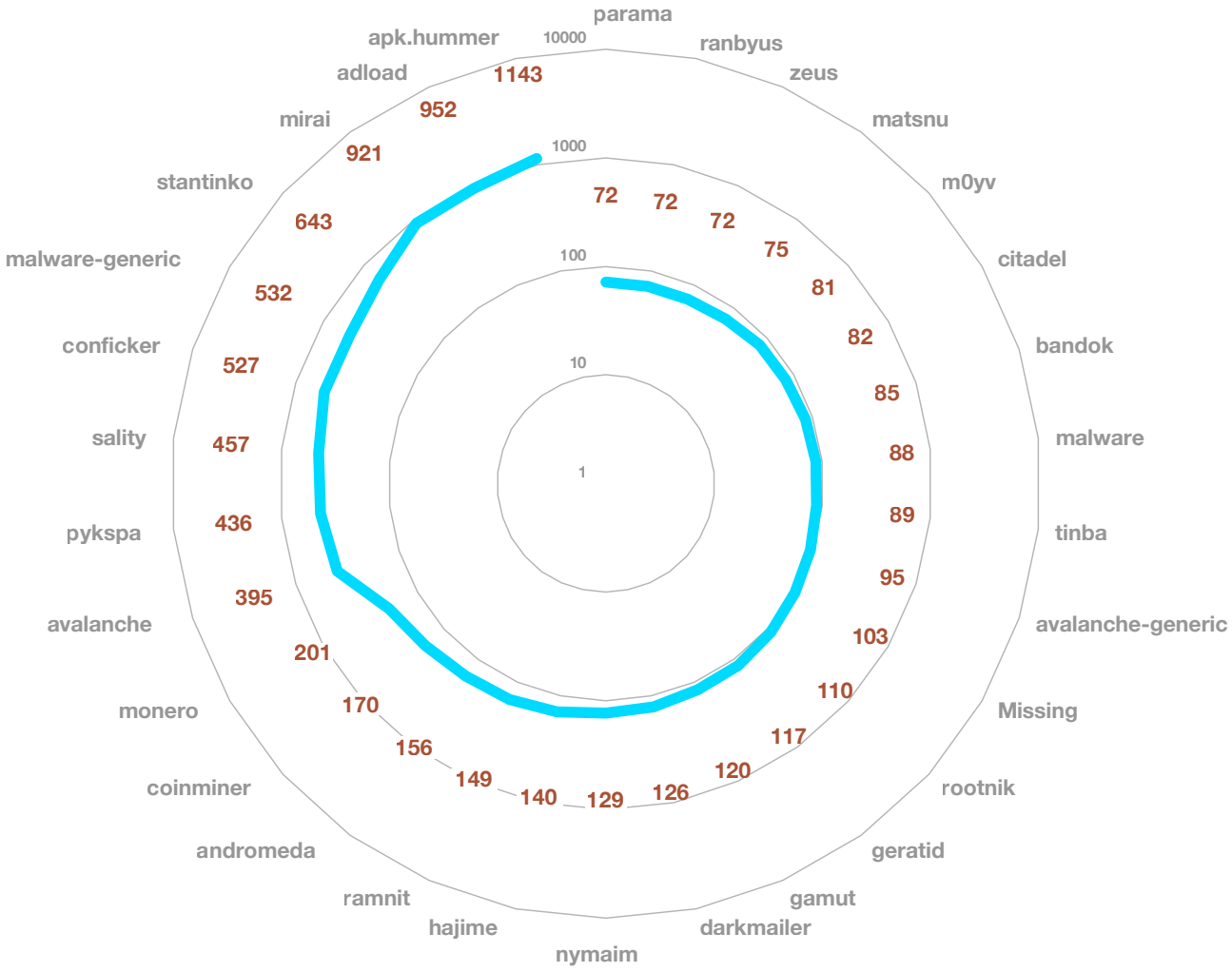
Pārskata periodā apdraudējumu līmenis bija stabils. Prognozes rāda, ka apdraudējumu intensitāte saglabāsies.



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

Pārskata periodā 1. vietu kā izplatītākais apdraudējums nemainīgi saglabā **konfigurācijas nepilnības** (70975 unikālas IP adreses), tomēr tas ir ar kritumu par 7% salīdzinājumā pret iepriekšējo ceturksni un par 40% mazāk nekā šajā pašā periodā pirms gada.

Ļaundabīgu kodu jeb ļaunatūru TOP 30



4. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2023. gada 3. ceturksnī ar apdraudējuma veidu – ļaundabīgs kods.

Otrs izplatītākais bija **ļaundabīgs kods** (6852 unikālas IP adreses) ar kritumu par 3% salīdzinājumā pret iepriekšējo ceturksni un par 34% mazāk nekā šajā pašā periodā pirms gada.

Savukārt 3. vietā ir "ielauzušies" – **ielaušanās mēģinājumi** (1192 unikālas IP adreses) ar iespaidīgu pieaugumu jeb par 89% vairāk salīdzinājumā pret iepriekšējo ceturksni un par 30% vairāk nekā šajā pašā periodā pirms gada.

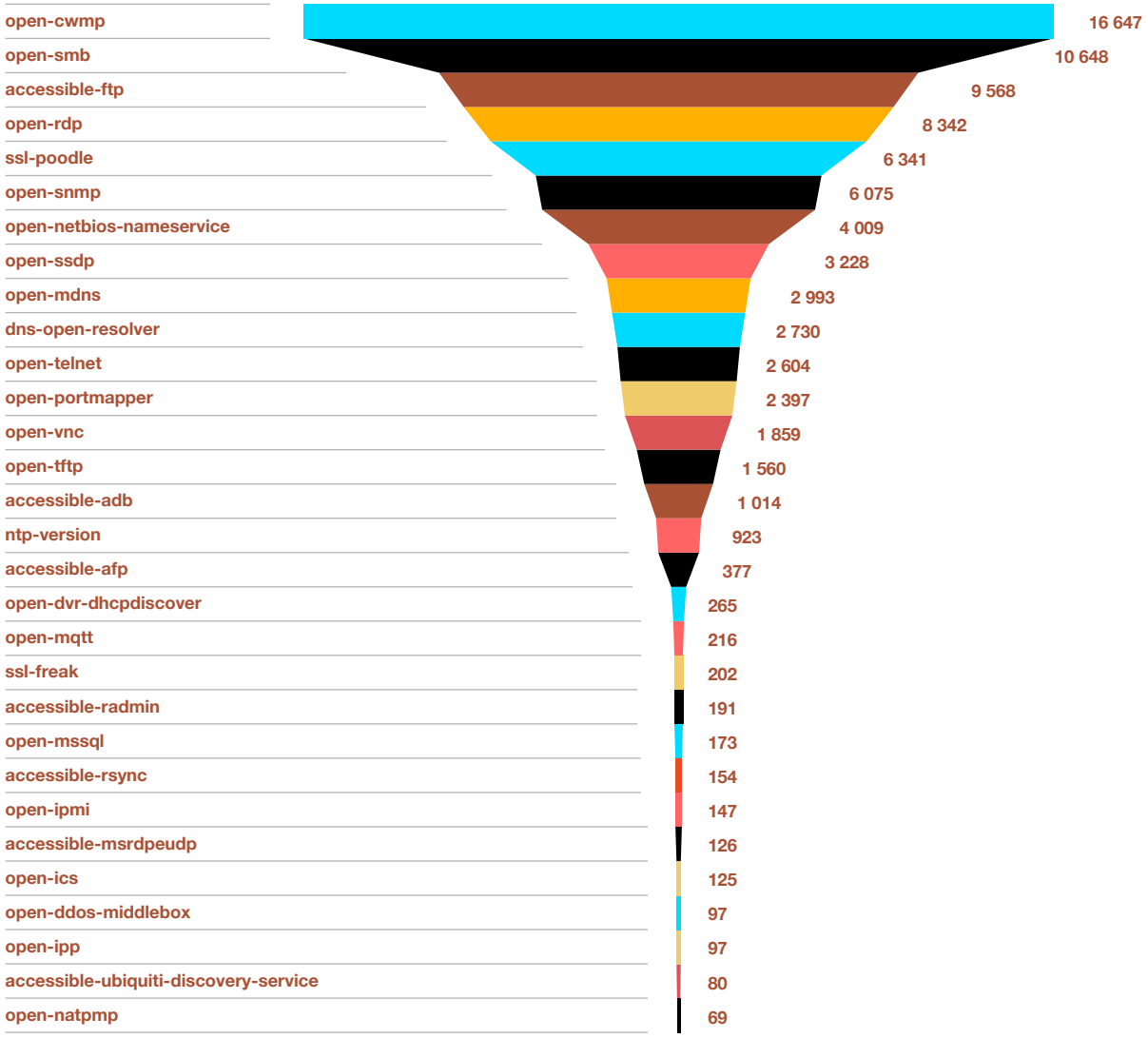
Pašreizējā ģeopolitiskajā situācijā un hibrīdkara apstākļos var pieņemt, ka ielaušanās mēģinājumu būtiskais pieaugums kibertelpā ir skaidrojams ar politiski motivētiem Krievijas hakeru uzbrukumiem un uzbrukumu mēģinājumiem, īpaši kas saistīti ar acīmredzamiem centieniem kompromitēt NATO un ES dalībvalstu kritisko infrastruktūru.

Ļaunatūras topa 1. vietu ieņem ļaunatūra *Apk.hummer*, kas iekārtās ar *Android* operētājsistēmu (planšetdatoros un viedtālruņos) demonstrē uznirstošas (*pop-up*) reklāmas un patstāvīgi lejupielādē dažādas lietotnes.

Savukārt topa jaunums ir ļaunatūra *Adload*, kas ir ierindojusies 2. vietā. *Adload* 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 – ļaunatūra *Mirai*, kas inficē un iekļauj robotu tīklos jeb *botnetos* lietu interneta (*IoT*) iekārtas, lai izmantotu tās tālākiem uzbrukumiem un citām pretlikumīgām darbībām. Par uzbrucēju upuriem parasti kļūst iekārtas, kuras pēc iegādes pieslēgtas internetam, nenomainot ražotāja uzstādītos iestatījumus – noklusēto lietotājvārdu un paroli. Lai pasargātu sevi no lieka riska un līdzcilvēkus no papildu apdraudējuma, tiek rekomendēts pirms jebkuras jaunas iekārtas pieslēgšanas internetam rūpīgi izvērtēt, vai konkrētajai iekārtai šis pieslēgums tiešām ir nepieciešams. Ja tomēr ir, tad jāparūpējas par iekārtas drošību, nomainot noklusēto paroli.

Konfigurācijas nepilnību TOP 30



5. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2023. gada 3. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

Konfigurācijas nepilnību topa pieciniekā 1. vietu joprojām ieņem *Open-cwmp*. CWMP ir pārvaldības protokols, kas tiek izmantots, lai nodrošinātu individuālu iekārtu, piemēram, maršrutētāju vai VoIP telefonu pieslēgšanos pie telekomunikāciju pakalpojumu sniedzēja nodrošinātā tīkla. Lai šim pārvaldības rīkam novērstu neautorizētas piekļuves riskus, tiek rekomendēts ierobežot piekļuves tiesības, piemēram, izmantojot VPN.

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

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

Apdraudējumu matrica pēc nozīmības un ietekmes

Pilnvērtīgākam kiberdrošības situācijas novērtējumam CERT.LV lieto Apvienotās Karalistes Nacionālā kiberdrošības centra (NCSC) izveidoto apdraudējumu matricu.

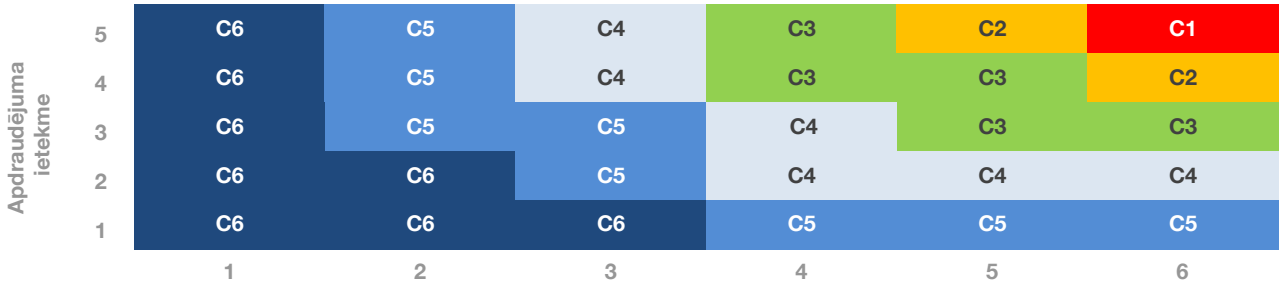
Matricā ievietotie apdraudējumi tiek grupēti pēc tā, cik nozīmīga ir skartā iestāde vai uzņēmums un/vai cik plašu sabiedrības daļu apdraudējums ietekmē, kā arī pēc tā, cik būtiskas sekas attiecīgais apdraudējums radīs.

Apvienojot visus faktorus, apdraudējumi tiek iedalīti 6 kategorijās:

C1	Nacionāla līmeņa apdraudējums, ietekmēta pamatpakalpojumu sniegšana, apdraudēta ekonomiskā vai politiskā stabilitāte.
C2	Augstas nozīmes apdraudējumi, ietekmētas valsts iestādes, nacionālā infrastruktūra.

C3	Nozīmīgi apdraudējumi, plaša ietekme uz komerciālo sektoru, valsts un pašvaldību iestādēm.
C4	Būtiski apdraudējumi, vidēja ietekme uz komerciālo sektoru, valsts un pašvaldību iestādēm.
C5	Mēreni apdraudējumi, neliela ietekme uz komerciālo sektoru, valsts un pašvaldību iestādēm.
C6	Ikdienas apdraudējumi, ietekmē atsevišķus indivīdus, nenozīmīga ietekme uz uzņēmumiem vai valsts un pašvaldību iestādēm.

Apdraudējumu matrica



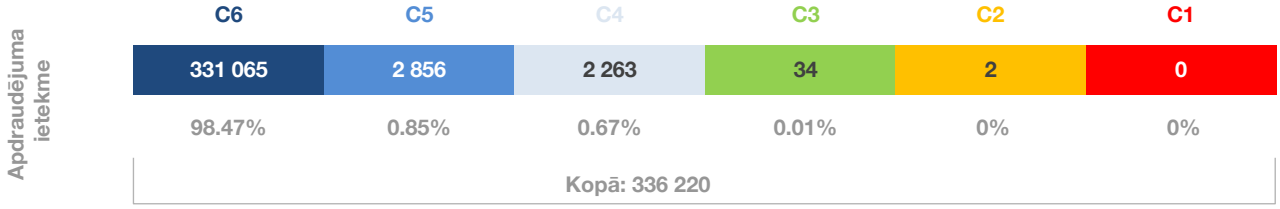
6. attēls – Apdraudējumu matricas sadalījums kategorijās.

Apdraudēto unikālo IP adrešu sadalījums

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

Nacionāla līmeņa apdraudējumi (C1) pārskata periodā nav reģistrēti. Augstas nozīmes apdraudējumu (C2) kategorijā reģistrētas divas apdraudētas IP adreses. Apdraudējums saistīts ar kompromitētām iekārtām kādā valsts iestādē.

Apdraudēto unikālo IP adrešu sadalījums

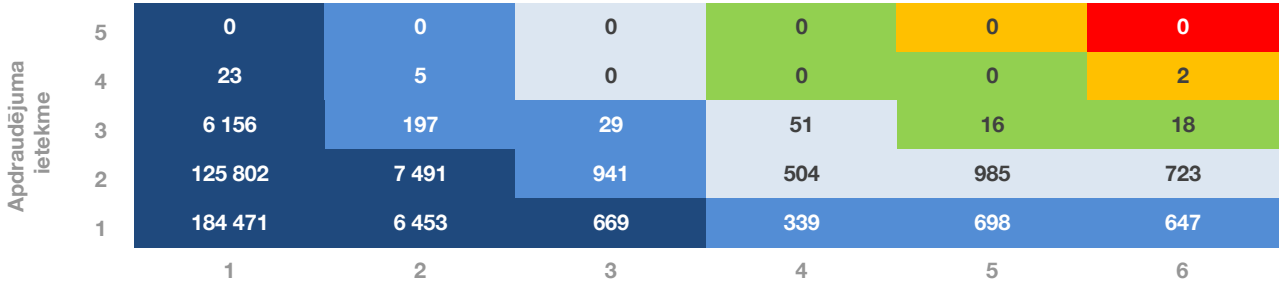


7. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu sadalījums apdraudējumu kategorijās pēc apdraudējuma ietekmes (matrica) 2023. gada 3. ceturksnī.

Nozīmīgi plašas ietekmes apdraudējumi (C3) veido 0,01% (34 unikālas apdraudētas IP adreses/gadījumi) no visiem kategorizētajiem apdraudējumiem. No tiem 29 apdraudējumi bija ļaundabīgs kods, savukārt pakalpojumu pieejamības incidenti bija pieci.

Būtiski apdraudējumi ar vidēju ietekmi (C4) veido 0,67% (2263 unikālas apdraudētas IP adreses/gadījumi) no visiem kategorizētajiem apdraudējumiem. 228 gadījumos jeb 10% no kopskaitā

Apdraudēto unikālo IP adrešu izvietojums



8. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu izvietojums matricā 2023. gada 3. ceturksnī valsts un pašvaldību institūcijās.

reģistrētajiem apdraudējumiem bija konfigurācijas nepilnības (Accessible-ftp, ntp-version, Ssl_poodle u.c.), 86 gadījumi tika reģistrēti kā krāpšanas incidenti, bet pārējo daļu veidoja ielaušanās mēģinājumi, ļaundabīgs kods, kompromitētas iekārtas, pakalpojuma pieejamības, informācijas vākšanas un citi incidenti augstas un vidēji augstas prioritātes iestādēs.

Lai sekmētu kopējo kiberdrošību valstī, CERT.LV sadarbībā ar NIC ir izstrādājusi DNS RPZ (*Domain Name Service Response Policy Zone*) jeb *DNS* ugunsmūri (*DNS firewall*). DNS ugunsmūris ik dienu tiek papildināts ar Latvijas iedzīvotāju un kiberdrošības ekspertu sniegto informāciju par kiberuzbrucēju aktivitātēm Latvijas kibertelpā, sniedzot iespēju aizsargāt lietotājus no ļaundabīga satura internetā. Šis risinājums bez maksas ir pieejams jebkuram Latvijas iedzīvotājam, uzņēmumam un organizācijai.

Vairāk informācijas par darbību un uzstādīšanu: https://dnsmuris.lv/.

2. Atbalsts kiberdrošības incidentu novēršanā un koordinēšanā

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

2.1 Krāpšana

Latvijā nemainīgi augsts krāpniecības kampaņu skaits

Apkopotie dati atklāj, ka 2023. gada 3. ceturksnī, iedzīvotāji turpināja masveidā saņemt ziņas no krāpniekiem, tika novērotas vairākas krāpniecības kampaņas, tostarp viltus zvani un īsziņas.

Iedzīvotāji jūlija mēnesī turpināja saņemt piedāvājumus ar mudinājumiem veikt investīcijas viltus platformās. Vairāki cietušie vērsās pie CERT.LV tikai tad, kad nauda krāpnieciskajās platformās jau bija iemaksāta.

Viltvārži turpināja sūtīt krāpnieciska rakstura īsziņas it kā VAS "Latvijas Pasts" vārdā, pieprasot upurim ievadīt maksājumu karšu datus īsziņā iekļautajā adresē, lai it kā veiktu maksājumu par atkārtotu piegādi. Tāpat augustā bija ievērojams skaits krāpnieciska rakstura īsziņu, kurās viltvārži, uzdodoties par platformu elieta.lv, ar īsziņu informēja upuri par it kā paredzēto tiesas sēdi un mudināja atvērt pievienoto saiti papildu informācijai. Sekojot pievienotajai saitei, krāpniecības upuri nonāca viltus tīmekļa vietnē, kas vizuāli līdzinājās VISS vienotās pieteikšanās modulim. Tajā ievadot internetbankas piekļuves datus, tie automātiski tika pārsūtīti krāpniekam. Iegūtie dati bieži tika izmantoti, lai paralēli pieslēgtos internetbankai un, ja upuris ievadīja savu Smart-ID PIN2 kodu, veiktu naudas pārskatījumu.

Augustā aktivizējās krāpnieki, kas zvanīja un izlikās par dažādu iestāžu vai organizāciju darbiniekiem, tostarp Valsts policijas un CERT.LV pārstāvjiem, tādējādi mēģinot izvilināt datus vai pierunāt uzstādīt attālinātās piekļuves programmas.

Tika saņemti vairāki ziņojumi no iedzīvotājiem par viltus pircējiem, kas uzrunā savus upurus *Facebook Marketplace* platformā. Saziņas lietotnē uzbrucēji nosūtīja pārdevējam ziņu, it kā izrādot interesi par preci un apgalvojot, ka preces piegādei un apmaksai izmantos piegādes pakalpojumu sniedzējus. Pārdevējam tika nosūtīta viltus "Omniva Latvija" vai "DPD Latvija" vietnes saite, kurā krāpniecības upurus aicināja ievadīt maksājumu kartes datus (arī CVV kodu) maksājuma saņemšanai par preci.

Līdzīgi kā jūlijā un augustā, tā arī septembrī tika novērots nemainīgi liels krāpnieciska rakstura īsziņu un e-pasta vēstuļu skaits, kas nosūtīts šķietami valsts iestāžu, tiesas vai uzņēmumu (SIA "Rimi Latvia", VAS "Latvijas Pasts", "DPD Latvija", "UPS" u.c.) vārdā. Atverot krāpnieciskas īsziņas tekstā pievienoto saiti, upuris tika aicināts ievadīt maksājumu kartes datus. CERT.LV rīcībā esošā informācija liecina, ka uzbrukumi ir bijuši veiksmīgi, un krāpniekiem ir izdevies izkrāpt naudas līdzekļus no Latvijas iedzīvotājiem.

Plaša mēroga kiberuzbrukumi pret valsts iestāžu resursiem

Septembrī Krievijas atbalstīti haktīvistu grupējumi veica plaša mēroga kiberuzbrukumus valsts iestāžu resursiem Latvijā. Tika novēroti pikšķerēšanas uzbrukumi e-pasta sistēmu lietotājiem valsts pārvaldē, bet līdz šim tie nav radījuši būtisku ietekmi valsts un kritiskās infrastruktūras sektorā.

CERT.LV aicināja pārliecināties, ka e-pasta sistēmās ir uzstādīta daudzfaktoru autentifikācija, un tās nav bez īpašas vajadzības pieejamas no interneta.

2.2. Pakalpojuma pieejamība (DDoS)

Politiski motivēti Krievijas hakeru uzbrukumi Latvijā

Krievijas militārā agresija pret Ukrainu ir mainījusi apdraudējumu ainu Eiropā. CERT.LV rūpīgi seko līdzi Krievijas hakeru grupējumu DDoS mērķiem. Novērojumi rāda, ka šajā sarakstā parādās gandrīz visas NATO dalībvalstis, tomēr Latvija, Lietuva, Igaunija, Polija un Čehija – daudz regulārāk.

Pārskata periodā Krievijas agresīvo režīmu atbalstošo haktīvistu grupējumu aktivitātes bija vērstas galvenokārt pret valsts iestādēm, kā arī finanšu, transporta un enerģētikas nozaru uzņēmumiem, bet mērķu infrastruktūras pārsvarā bija gatavas uzbrukumus atvairīt, un tie neradīja ietekmi uz resursu darbību.

4. septembrī notika vairāki agresīvi piekļuves atteices uzbrukumi lielam skaitam Latvijas mērķu. Starp skartajiem resursiem bija gan vairākas ministrijas, valsts iestādes un resursi, gan mediju platformas. Šoreiz uzbrukumu sarežģītība un jauda bija augstāka nekā vienkāršiem piekļuves atteices uzbrukumiem. Vairāki resursi bija īslaicīgi nepieejami.

Tuvākajā laikā prokrievisko hakeru aktivitātes intensitāte nemazināsies

Pašreizējā ģeopolitiskajā situācijā un hibrīdkara apstākļos starp kibertelpas aktualitātēm jūlijā tika izgaismota ziņa par Krievijas atbalstītās hakeru grupas *NoName* atjaunināto *DDoSia* pakalpojumatteices uzbrukuma rīku kopu.

Krieviju atbalstošie grupējumi ir apvienojušies, lai veiktu kopīgus uzbrukumus visām Baltijas valstīm. Uzbrukumi veidoti, galvenokārt balstoties uz retoriku, ka Baltijas valstis atbalsta Ukrainu, tāpēc tās ir jāsoda. Daži no uzbrukumu mērķiem saņēma e-pasta vēstules, kurās norādīts, ka kiberuzbrukumi turpināsies, kamēr turpināsies atbalsts Ukrainai.

Pateicoties sekmīgai sadarbībai ar Latvijas tiesībsargājošajām iestādēm, CERT.LV savas kompetences ietvaros nodrošina Latvijas valsts iestādēm un visai kiberdrošības kopienai datos balstītu apsteidzošu informāciju par prokrievisko hakeru izvēlētajiem mērķiem un metodēm, lai spētu efektīvi aizsargāt valsts resursus. Tas ir ļāvis savlaicīgi reaģēt, nodrošinot valstij un sabiedrībai būtisko resursu aizsardzību gan stiprinot noturību pret DDoS uzbrukumiem sadarbībā ar nozares partneriem, gan veicot apsteidzošas CERT.LV vadītas "draudu medību" operācijas, nepieļaujot uzbrucējiem gūt priekšrocības.

Kopumā situācija vērtējama kā stabila. CERT.LV turpina aktīvi uzraudzīt Latvijas kibertelpu un iespējamos apdraudējumus.

2.3. Ļaundabīgs kods

Neitralizēta ļaunatūras Qakbot infrastruktūra

Augustā starptautiskā kiberoperācijā *Duck Hunt*, kas notika ASV, Francijā, Vācijā, Nīderlandē, Lielbritānijā, Rumānijā un Latvijā, veiksmīgi tika neitralizēta ļaunatūras *Qakbot* infrastruktūra, kuru kibernoziedznieki izmantoja datu vākšanas, izspiešanas un finanšu krāpšanas darbību veikšanai. No Latvijas kiberoperācijā iesaistījās Valsts policija, LU MII SigmaNet laboratorija un CERT.LV.

Ļaunatūru *Qakbot*, sauktu arī par *Qbot* un *Pinkslipbot*, kontrolēja kibernoziedznieku organizācija, kuras lokā bija arī liels skaits Krievijas izcelsmes hakeru. *Qakbot* tika izmantota nolūkā uzbrukt kritiskajai infrastruktūrai visā pasaulē, izplatot mēstules un inficējot upuru datorus.

2.4. Ielaušanās mēģinājumi

Kiberuzbrucēji uzlauž Facebook kontus

Pārskata periodā tika saņemti vairāki ziņojumi par uzlauztiem *Facebook* kontiem gan no privātpersonām, gan iestādēm.

Augusta vidū tika uzlauzts Valmieras drāmas teātra *Facebook* konts, ar mērķi izkrāpt finanšu līdzekļus. Kaut arī nedēļu vēlāk kontu izdevās atgūt, šī incidenta rezultātā teātrim tika izkrāpti 1000 eiro.

Daļā gadījumu par virtuālo krāpnieku upuriem kļuva *Facebook* kontu īpašnieki, kuri administrē savam kontam piesaistītas vairākas *Facebook* lapas. Dažos gadījumos iedzīvotāji ziņoja, ka ir saņēmuši ļaundaru sūtītas ziņas no uzlauztiem *Facebook* kontiem. Šo kiberuzbrucēju mērķis bija paplašināt kompromitēto kontu tīklu, lūdzot kompromitētā *Facebook* konta īpašnieka draugiem telefona numurus un prasot atkopšanās kodus, kas tiek nosūtīti uz šiem numuriem, lai pārņemtu kontroli pār kontiem, pievienojot tos krāpnieku pārvaldītām ierīcēm.

CERT. LV stingri rekomendē nodrošināt papildu drošību, gan aktivizējot divfaktoru autentifikāciju (2FA) *Facebook* un e-pasta kontiem, gan nomainot paroles uz drošām un unikālām.

2.5. Kompromitētas iekārtas un datu noplūdes

Uzlauzta kāda valsts iestādes projekta mājaslapa

Jūlijā tika uzlauzta kādas valsts iestādes projekta mājaslapa, un tīmekļa serverī tika konstatēti nesankcionēti izvietoti faili. CERT.LV informēja iestādi par incidentu un sniedza rekomendācijas tālākai rīcībai, lai labāk novērtētu incidenta ietekmi, kā arī lai saglabātu pierādījumus tālākai incidenta analīzei. Incidents no iestādes puses tika operatīvi novērsts.

Nesankcionēta datu izgūšana no datubāzes

25. jūlijā tika saņemts ziņojums par tumšā tīmekļa (*darknet*) vietnēs un hakeru diskusiju forumos pieejamu informāciju par kāda datu centra datubāzēm. Uzsākot incidenta izmeklēšanu, CERT.LV konstatēja, ka datu izgūšana notikusi, izmantojot SQL injekciju. Datu noplūde notikusi jau 2022. gada septembrī.

Šajā datubāzē, pretēji labajai praksei, informācija par parolēm u.c. tika glabāta nešifrētā veidā, tādējādi apdraudot sistēmu uzturēšanas drošību.

CERT.LV sniedza informāciju un ieteikumus incidenta novēršanai. Ilgtermiņā labākais risinājums ir sistēmas datu migrācija uz mūsdienīgu arhitektūru, ko iespējams uzturēt un atjaunināt.

Ievainojamības ļauj iegūt neautorizētu piekļuvi paroļu jaucējvērtībām

CERT.LV saņēma informāciju par ievainojamībām kāda uzņēmuma nodrošinātās tīmekļa vietnes attālinātās industriālo procesu vadības un kontroles sistēmas (SCADA) autentifikācijas mehānismā. Šīs ievainojamības ļāva uzbrucējiem iegūt neautorizētu piekļuvi SCADA lietotāju paroļu jaucējvērtībām (*hash value*), ar kuru palīdzību varēja veikt sekmīgu autentifikāciju uzņēmuma klientu SCADA sistēmās no interneta, iegūstot pilnu piekļuvi.

CERT.LV eksperti vairākkārt ir uzsvēruši arvien pieaugošo industriālās kontroles sistēmu drošības nozīmi un nepieciešamību tās pienācīgi aizsargāt. Īpaši jāņem vērā riski, kas saistīti ar Krievijas agresiju un acīmredzamiem centieniem kompromitēt NATO un ES dalībvalstu kritisko infrastruktūru.

CERT.LV aktīvi iesaistījās incidenta risināšanā, brīdināja uzņēmumu par atklātajām drošības nepilnībām, no kurām kritiskākās ir novērstas. Turpinās aktīva sadarbība ar uzņēmumu pilnīgai SCADA piekļuves sistēmu ievainojamību novēršanai.

Veikta dezinformācijas kampaņa pret manabalss.lv

Reaģējot uz Krievijas agresiju atbalstošo haktīvistu grupu publicēto informāciju *Telegram* kanālos par it kā iegūtiem personu datiem no manabalss.lv pilsonisko iniciatīvu projekta, CERT.LV sadarbībā ar manabalss.lv organizēja koordinētu izmeklēšanu un veica datu analīzi.

Publiskotā uzbrucēju informācija, izmantojot *Telegram*, šķietami liecināja, ka no portāla ir izgūti dati (tika publiskots cilvēku saraksts ar vārdiem un uzvārdiem, kuri it kā ir balsojuši par iniciatīvu, lai nepagarinātu uzturēšanās atļaujas valodas prasībām neatbilstošajiem Krievijas pilsoņiem). Izvērtējot apstākļus, tika secināts, ka šī ir haktīvistu dezinformācijas kampaņa, jo kiberuzbrukums nebija noticis, un cilvēku saraksts nekorelēja ar tiem, kas tiešām bija balsojuši. Vienlaicīgi konstatēts, ka publiskotais saraksts ar vārdiem nebija nejaušs, tajā bija iekļauti gan dažādu valsts iestāžu darbinieku vārdi, gan arī cilvēki, kas aktīvi pauduši atbalstu Ukrainai dažādās platformās.

2.6. Ievainojamības

MikroTik ievainojamība

Jūlijā starptautiskie kiberdrošības eksperti ziņoja, ka kritiska "super administratora" privilēģiju eskalācijas ievainojamība var pakļaut riskam vairāk nekā 900 000 *MikroTik RouterOS* maršrutētājus, ļaujot uzbrucējam pārņemt pilnu kontroli pār iekārtu un palikt nepamanītam.

Šī ievainojamība (CVE-2023-30799) ļauj uzbrucējiem, kam pieejams administratora konts, palielināt savas privilēģijas līdz *super-admin* līmenim, izmantojot ierīces *Winbox* vai *HTTP* saskarni. Lai izmantotu ievainojamību, uzbrucējam ir jābūt administratora kontam, ko nav grūti iegūt – *MikroTik RouterOS* nav aizsargāts pret brutāla spēka uzbrukumiem un izmanto noklusējuma lietotāju *admin*. Savukārt *super-admin* kontam ir augstākas privilēģijas un piekļuve *RouterOS* operētājsistēmai; uzbrucēji var to izmantot, tai skaitā, lai noslēptu savas darbības konkrētajā ierīcē.

CERT.LV informēja sabiedrību par konkrēto ievainojamību un veicamajām darbībām savu iekārtu aizsargāšanai.

Barracuda e-pastu vārtejas ierīcēm joprojām pastāv kompromitēšanas riski

Pārskata periodā ASV Federālais izlūkošanas birojs (FBI) izplatīja brīdinājumu, mudinot izolēt vai aizvietot jau iepriekš kiberuzbrukumos cietušās *Barracuda Email Security Gateway* (*ESG*) iekārtas un uzsverot, ka Ķīnas Tautas Republikas kiberuzbrucēji turpina uzbrukumus. Joprojām pastāv kompromitēšanas risks, jo ļaunatūra tikusi izveidota tā, lai saglabātu klātbūtni mērķa uzņēmumos vai organizācijās pat pēc atjauninājumu veikšanas.

Vasaras sākumā arī CERT.LV izplatīja brīdinājumu par atklāto ievainojamību (CVE-2023-2868) *Barracuda ESG* risinājumā. Ievainojamība sniedz uzbrucējiem iespēju veikt attālinātu koda izpildi. Tā jau tika izmantota uzbrukumos, kuros vairāki cietušie ir arī Latvijā.

Lai noskaidrotu pašreizējo situāciju un efektīvākos soļus draudu novēršanai, CERT.LV aktīvi komunicē ar kiberuzbrukumā cietušajām organizācijām.

Jauni drošības atjauninājumi Microsoft Exchange 2019 un 2016 serveros

Augustā "Microsoft" publicēja drošības atjauninājumus, kas novērsa vairākas kritiskas ievainojamības šajos serveros. Viena no tām bija privilēģijas eskalācijas ievainojamība, bet virkne citu sniedza uzbrucējiem iespēju veikt attālinātā koda izpildi (RCE) ievainojamajā sistēmā.

CERT.LV aicināja iedzīvotājus un organizācijas nekavēties ar atjauninājumu uzstādīšanu.

"Apple" "nulles dienas" ievainojamības

Septembrī tehnoloģiju gigants "Apple" publicēja ārkārtas drošības atjauninājumus telefoniem, datoriem un pulksteņiem, lai novērstu divas "nulles dienas" ievainojamības, kas jau tikušas izmantotas, aktivizējot telefonos *Pegasus* spiegprogrammatūru. Atklātās ievainojamības ļāva uzbrucējiem telefonos ar 16.6 versijas programmatūru, neprasot lietotāja apstiprinājumu, instalēt programmas, izmantojot *iMessage*.

CERT.LV rekomendēja “Apple” produktu lietotājiem atbildīgi sekot līdzi atklātām ievainojamībām un nekavēties ar atjauninājumu uzstādīšanu.

2.7. Atbildīga ievainojamību atklāšana

Pārskata periodā tika saņemts ziņojums par starpvietņu skriptēšanas *XSS* (*cross site scripting*) ievainojamību kādas valsts iestādes *Jira* resursā. *XSS* ievainojamība sniedz uzbrucējam iespēju izpildīt patvaļīgu kodu citu lietotāju aplūkotajās tīmekļa vietnēs, piemēram, pārvirzot lietotāju uz kaitīgu vietni, kā arī izvairīties no vietņu piekļuves drošības mehānismiem. Resursa uzturētājs tika informēts par saņemto ziņojumu un nepieciešamajiem soļiem apdraudējuma novēršanai.

Tika saņemts ziņojums par kādas valsts iestādes resursu, kurā tika norādīts, ka konfigurācijas nepilnība atklāj informāciju par *Jira* iestatījumiem. Resursa uzturētājs tika informēts, kā arī resursam tika liegta piekļuve no interneta.

3. Pētnieciskais darbs, apmācību un izglītojošu pasākumu organizēšana kiberdrošības jomā

Papildu ierastajiem darbinieku izglītošanas semināriem par kiberdrošību, tika novadītas vairākas lekcijas un apmācības iestāžu un kritiskās infrastruktūras uzņēmumu darbiniekiem par specifiskām, iestāžu un uzņēmumu izvēlētām tēmām, piemēram, mākslīgā intelekta rīku drošu izmantošanu, aktuālajiem apdraudējumiem un datu drošību u.c.

26. septembrī CERT.LV piedalījās *ESET SECURITY DAYS 2023* konferencē, kurā sniedza prezentāciju par kiberdrošības situāciju Latvijā, kā arī piedalījās paneļdiskusijā “21. gadsimta

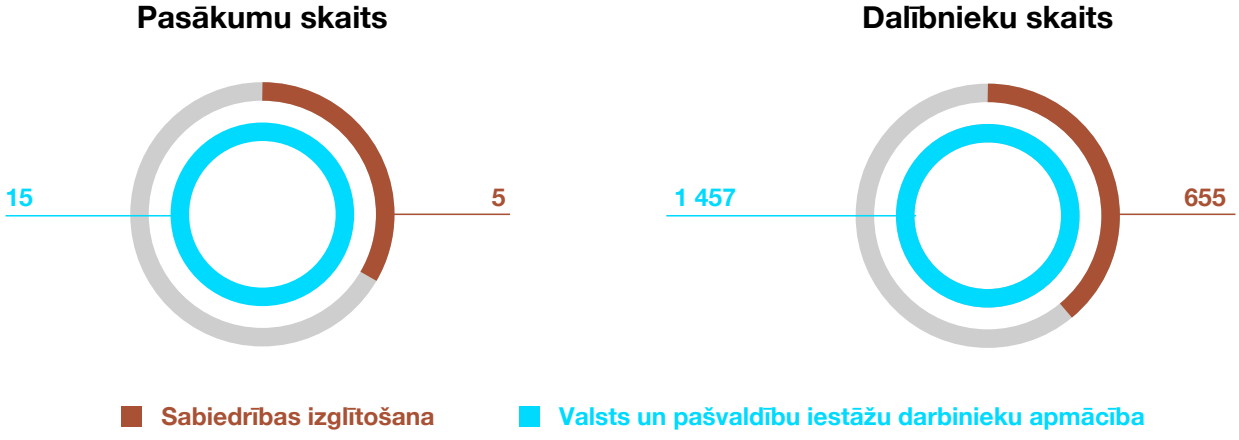
informācijas telpas aktualitātes – personas dati, to aizsardzība, mākslīgais intelekts". Vairāk informācijas: https://www.eset.com/lv/eset-security-day/

28. septembrī notika LVRTC organizētais pasākums "Kibernakts 2023", kurā CERT.LV sniedza informāciju par kiberuzbrucēju mērķiem un izmantotajām metodēm prezentācijā "Pikšķerēšana / Lavīnas sākums". Vairāk informācijas: https://www.lvrtc.lv/kibernakts-2023/

29. septembrī Latvijas Datortīklu skolas IT konferencē CERT.LV sniedza prezentāciju "Kā ātri zaudēt daudz datus – izspiedējvīrusu uzbrukumi biznesam", informējot dalībniekus par potenciālajiem kiberapdraudējumiem un rekomendācijām, kā pasargāt savu uzņēmumu.

CERT.LV darbojās kā nacionālais partneris, sniedzot atbalstu SANS institūtam *SANS CEE Cyber Tournament 2023* kiberdrošības sacensību organizēšanā un popularizēšanā. 14. - 15. septembrī noritēja sacensību atlases kārta, bet 28. - 29. septembrī notika fināls. Sacensības noritēja CTF

Izglītojošo pasākumu un apmācīto cilvēku skaits



9. attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2023. gada 3. ceturksnī

(*Capture the Flag*) formā un bija paredzētas kiberdrošības profesionāļiem un interesentiem no Centrālās un Austrumeiropas valstīm, lai sniegtu iespēju pilnveidot prasmes un popularizētu kiberdrošību kā karjeras izvēli.

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

Sadarbības tikšanās, konsultācijas un prezentācijas kiberdrošības jomā:

- Dalība jaunu Ministru kabineta noteikumu izstrādē par datu centriem un drošības operāciju centriem (SOC). Pārskata periodā noritēja darbs pie noteikumu satura. CERT.LV gatavoja papildinājumus prasībām datu centru auditoriem.
- CERT.LV sniedza komentārus Aizsardzības ministrijai par valsts vietotā interneta apmaiņas punkta (GLV-IX) darbību reglamentējošajiem Ministru kabineta noteikumiem, kā arī piedalījās noteikumu saskaņošanas sanāksmēs.
- Notika tikšanās ar Vides aizsardzības un reģionālās attīstības ministriju par projekta "Datu izplatīšanas un pārvaldības platforma (DAGR)" noteikumiem. Projekta mērķis ir informācijas apmaiņas un sadarbspējas uzlabošana valsts pārvaldē, kā arī datu pieejamības nodrošināšana ar garantētiem piekļuves laikiem. Īstenojot projektu, valsts pārvaldei tiks nodrošinātas iespējas apkopot potenciāli visu valsts iestāžu datus vienotā datu izplatīšanas platformā, kuru datu patērētāji varēs izmantot, lai izgūtu reāla laika datus no avotu sistēmām.
- Tika sniegts komentārs Aizsardzības ministrijai par informācijas tehnoloģiju sistēmu izvietošanu Elektronisko iepirkumu sistēmā (EIS), lai noskaidrotu nepieciešamību veikt izmaiņas Ministru kabineta noteikumos vai saistītajos dokumentos un šo izmaiņu potenciālo ietekmi.

- CERT.LV eksperti piedalījās Finanšu ministrijas darba grupā, apspriežot ministrijas virzītā prioritārā audita tvērumu 2024. gadam. "Informācijas un komunikāciju tehnoloģiju (IKT) pārvaldības un drošības vadības audits" uzdevumi ir novērtēt ministriju un iestāžu IKT pārvaldības organizēšanu, nepieciešamo resursu plānošanu, uzskaiti, sagādi, ieviešanu, izmantošanu, uzturēšanu, koplietošanu, optimizēšanu. Papildu tiks vērtēta arī IKT drošības vadības sistēma un ar to saistītie procesi un procedūras.

Koordinēta ievainojamību atklāšana

Turpinājās darbs pie koordinētas ievainojamību atklāšanas ziņojumu reģistrēšanas platformas (cvd.cert.lv) attīstības. Platformas izstrāde tika uzsākta, balstoties uz Ministru kabineta apstiprināto Aizsardzības ministrijas sagatavoto informatīvo ziņojumu "Par koordinētas ievainojamību atklāšanas procesa ieviešanu valsts pārvaldē", ar kuru ir uzsākta koordinētu ievainojamību atklāšanas procesa (turpmāk – CVD) ieviešana valsts pārvaldē, paredzot iespēju iestādēm brīvprātīgi iesaistīties CVD.

CVD platforma 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 ievainojamību novēršanas gaitai.

Uz pārskata perioda beigām platformā bija reģistrējušies 29 iestāžu/uzņēmumu atbildīgie par koordinātas ievainojamību atklāšanas ziņojumu apstrādi un 34 drošības pētnieki. Platformā reģistrētas 4 programmas, kurās var reģistrēt ievainojamību ziņojumus.

5. Sadarbība ar starptautiski atzītām kiberdrošības incidentu novēršanas institūcijām

CERT.LV starptautiskā sadarbība pārskata periodā:

- Turpinājās darbs FIRST SIG darba grupā *CSIRT (Computer Security Incident Response Team*) *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 vadītajā darba grupā *Coordinated Vulnerability Disclosure (CVD) Task Force*, kurā norit darbs pie ES līmeņa koordinētas ievainojamību atklāšanas politikas vadlīniju veidošanas.

- Dalība ENISA Eiropas kiberdrošības indeksa (*EU Cybersecurity Index*) darba grupā, kurā tiek izstrādāta kiberdrošības indeksa vērtības aprēķina metodoloģija dalībvalstu kiberdrošības novērtēšanai.

- 13. - 14. jūlijā notika sadarbības tikšanās ar Igaunijas CERT kolēģiem, lai pārrunātu aktuālos notikumus katras valsts kibertelpā, kā arī apmainītos ar pieredzi incidentu risināšanā un sabiedrības informēšanā un izglītošanā.

- Laikā no 19. līdz 20. septembrim CERT.LV piedalījās NATO CCDCoE organizēto mācību *Locked Shields 24* sākotnējā plānošanas konferencē Tallinā. Ar šo konferenci sākās jaunais mācību cikls, kas noslēgsies 2024. gada aprīlī ar mācību norisi. No CERT.LV mācības atbalsta eksperti gan *WhiteTeam*, gan *GreenTeam*, nodrošinot mācību organizēšanu un vērtēšanu, savukārt Kiberaizsardzības vienība mācībās

piedalās gan mācību izspēlē, veidojot Latvijas *BlueTeam*, gan sniedzot atbalstu *GreenTeam* un *RedTeam*, nodrošinot mācību organizēšanu un izspēles norisi.

- 22. septembrī CERT.LV piedalījās Eiropas Kiberdrošības produktu sertifikācijas grupas ECCG (*European Cybersecurity Certification Group*) sanāksmē Briselē, kur sniedza savu redzējumu par topošo ES mākoņpakalpojumu sertificēšanas shēmas projektu, kā arī aizpildīja anketu par sertifikācijas shēmu ieviešanas jautājumiem ES valstīs, sniedzot informāciju par Latviju.
- 25. septembrī Stokholmā, Zviedrijā, notika 70. TF-CSIRT sanāksme, kuras ietvaros CERT.LV vadīja CERT komandu starptautisko sabiedrisko attiecību darba grupas (*TF-CSIRT PR Working Group*) tikšanos. Darba grupas mērķis ir veicināt pieredzes apmaiņu sabiedrības izglītošanas un informēšanas jautājumos starp CERTu kopienas dalībniekiem.
- 25. – 26. septembrī Leonā, Spānijā notika 21. *CSIRTs Network Meeting*, pulcējot Eiropas Savienības CSIRT/CERT komandas. CERT.LV sniedza ziņojumu par savas darbības aktualitātēm, informējot arī par vadītajām starptautiskajām draudu medību operācijām. Sanāksmes laikā tika pārrunātas Eiropas Savienības normatīvā regulējuma aktualitātes, tajā skaitā diskusijas par prasībām, kas iestrādātas *Cybersolidarity Act*. Notika dalīšanās ar aktuālo informāciju kiberdrošības incidentu jomā. Sanāksmes otrajā dienā norisinājās arī sadarbības sesija ar *CyCLONe*.
- Dalība ENISA organizēto mācību *Cyber Europe 2024* plānošanas darbnīcās, tai skaitā plānošanas grupā un scenārija izstrādāšanas grupā, arī sniedzot ieguldījumu sabiedrisko attiecību plānošanā.
- Dalība NATO Transformācijas pavēlniecības organizēto mācību *Cyber Coalition* plānošanas sanāksmē. *Cyber Coalition* ir NATO nozīmīgākās ikgadējās kolektīvās kiberdrošības mācības, kas ir vienas no lielākajām pasaulē.
- Regulāra dalība *CSIRT Network Situation Update* sanāksmēs, kuru mērķis ir veikt informācijas apmaiņu par aktuālo kibertelpā starp CSIRT tīkla biedriem.

Sadarbība konkrētu incidentu risināšanā aplūkota pārskata 2. nodaļā.

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 . Tīkls būtu atvērts Eiropas CSIRT sadarbības grupai, kuras galvenā uzmanība pievērsta tehnisko, operatīvo un stratēģisko draudu izlūkošanas informācijas apmaiņai un analīzei.

2023. gada 3. ceturksnī CERT.LV tupināja *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.

Graphoscope 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 *Graphoscope* iezīmes:

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

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

7. Citi normatīvajos aktos noteiktie pienākumi

- Tika turpināts darbs pie CERT.LV un NIC izstrādātā DNS RPZ (*Domain Name Service Response Policy Zone*) jeb DNS ugunsmūra (*DNS firewall*) projekta īstenošanas. DNS ugunsmūris 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 ugunsmūra 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 noslēgšanas un autorizēšanās jebkurš interneta lietotājs. Lai to izmantotu, jālieto NIC rekursīvie DNS serveri. Tīmekļa vietnē dnsmuris.lv pieejamas ērti lietojamas instrukcijas DNS ugunsmūra aktivizēšanai.

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

- Pārskata perioda laikā DNS ugunsmūra lietotāji tika pasargāti **40 837** reizes. Nozīmīgākās aktīvas aizsardzības epizodes bija šādas:
  - bloķētas viltus lapas, kuras lietotāji saņēma īsziņu (SMS) veidā: 731
  - bloķēta lietotāja pārvirze uz kaitīgām lapām: 8945
  - viltus bankas lapu bloķētie pieprasījumi datu izkrāpšanai: 104

- 29. augustā Saldus tehnikumā CERT.LV piedalījās sanāksmē ar Latvijas Informācijas un komunikācijas tehnoloģijas asociāciju, Latvijas Elektrotehnikas un elektronikas rūpniecības asociāciju, Nozaru ekspertu padomi un Drošības profesionāļu asociāciju un tehnikuma vadību, lai pārrunātu izglītības programmas attīstības iespējas un turpmāko sadarbību.
- CERT.LV eksperti Digitālās drošības uzraudzības komitejas (DDUK) ietvaros sniedza atbalstu kvalificētu elektroniskās identifikācijas pakalpojumu sniedzēju un uzticamu sertifikācijas pakalpojumu sniedzēju uzraudzībā.

8. Atskaite par Latvijas Interneta asociācijas Drošāka interneta centra ziņojumu līnijas darbību

Latvijas Interneta asociācijas Drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.07.2023. līdz 30.09.2023. ir saņēmusi un izvērtējusi 364 ziņojumus. No tiem 156 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 5 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 18 ziņojumos konstatēta personas goda un cieņas aizskaršana, 5 ziņojumi saņemti par naida runu un 1 ziņojumā konstatēti vardarbīgi materiāli. Par finanšu krāpšanas mēģinājumiem internetā saņemti 112 ziņojumi, 25 ziņojumu saturs nav bijis pretlikumīgs, 42 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 87 ziņojumi par naida runu un bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 87 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kuru atrašanās vieta bija ārpus Latvijas, ir ievietoti INHOPE asociācijas datu bāzē un iesniegti attiecīgās INHOPE valsts ziņojumu līnijai turpmāko darbību veikšanai, lai dzēstu nelegālo saturu no publiskas aprites.

Pārskata periodā no Latvijā uzturētajiem 65 ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem 64 ziņojumi ir dzēsti no publiskas aprites un 1 ziņojuma saturs atrodas dzēšanas procesā sadarbībā ar Valsts policiju un interneta pakalpojumu sniedzējiem.

2023 .gada 16. oktobrī

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

Galvenie CERT.LV uzdevumi ir uzturēt un aktualizēt informāciju par IT drošības apdraudējumiem, sniegt atbalstu valsts institūcijām IT drošības jomā, sniegt atbalstu IT drošības incidentu novēršanā jebkurai fiziskai vai juridiskai personai, ja incidentā iesaistīta Latvijas IP adrese vai .LV domēns, 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