Latvijas universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

2022 C3

Publiskais pārskats par CERT.LV uzdevumu izpildi

2022. gada 3. ceturksnis (01.07.2022. – 30.09.2022.)

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

Saturs

Kopsavilkums

Sākotnēji tika prognozēts, ka augusta otrajā pusē varētu saasināties kiberuzbrukumu intensitāte saistībā ar plānoto Padomju armijas karavīriem veltītā pieminekļa demontāžu, taču pieminekļa nojaukšanas dienā, 25. augustā, Latvijas kibertelpā uzbrukumu aktivitāte bija vērojama daudz zemāka nekā 11. augustā pēc Saeimas lēmuma Krieviju atzīt par terorismu atbalstošu valsti. Atsevišķos *Telegram* kanālos, kas saistīti ar Krievijas agresiju atbalstošu haktīvistu grupējumiem, tika novēroti aicinājumi uzbrukt Latvijas medijiem, kas nodrošināja translāciju no Uzvaras parka. Latvijas kibertelpā tika izmantoti atbilstoši aizsardzības risinājumi un nopietni traucējumi netika novēroti.

Ja iepriekšējos mēnešos bija būtiski pieaudzis CERT.LV saņemto ziņojumu skaits par piekļuves atteices jeb DDoS uzbrukumiem gan publiskajam, gan privātajam sektoram, tad septembrī bija novērojama šo ziņojumu apjoma samazināšanās. Tas varētu būt skaidrojams gan ar Krievijas saspīlēto iekšējo situāciju, gan ar Krievijas agresīvo politiku atbalstošo haktīvistu pievēršanos citiem mērķiem, piemēram, Lietuvā (Kaļiņingradas blokāde) un ASV (uzbrukumi lidostu tīmekļa vietnēm).

Vairāki pārskata periodā saņemtie incidentu ziņojumi iezīmēja paviršu attieksmi pret Ministru Kabineta noteikumiem Nr. 442 *Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām* un kiberdrošības labo praksi. Paļaujoties uz pieņēmumu, ka infrastruktūra tiek uzturēta atbilstoši sagatavotajai dokumentācijai, un neveicot praktiskas pārbaudes, tiek radīti labvēlīgi apstākļi incidentiem ar būtiskām sekām, kā arī tiek būtiski samazināta mērķa iestāžu spēja šādus incidentus identificēt, izmeklēt un novērst.

Pārskata periodā tika reģistrētas 314 848 unikālas apdraudētas IP adreses, kas ir par 20% vairāk nekā iepriekšējā ceturksnī un par 217% vairāk nekā šajā pašā periodā pirms gada. Izplatītākie apdraudējumi:

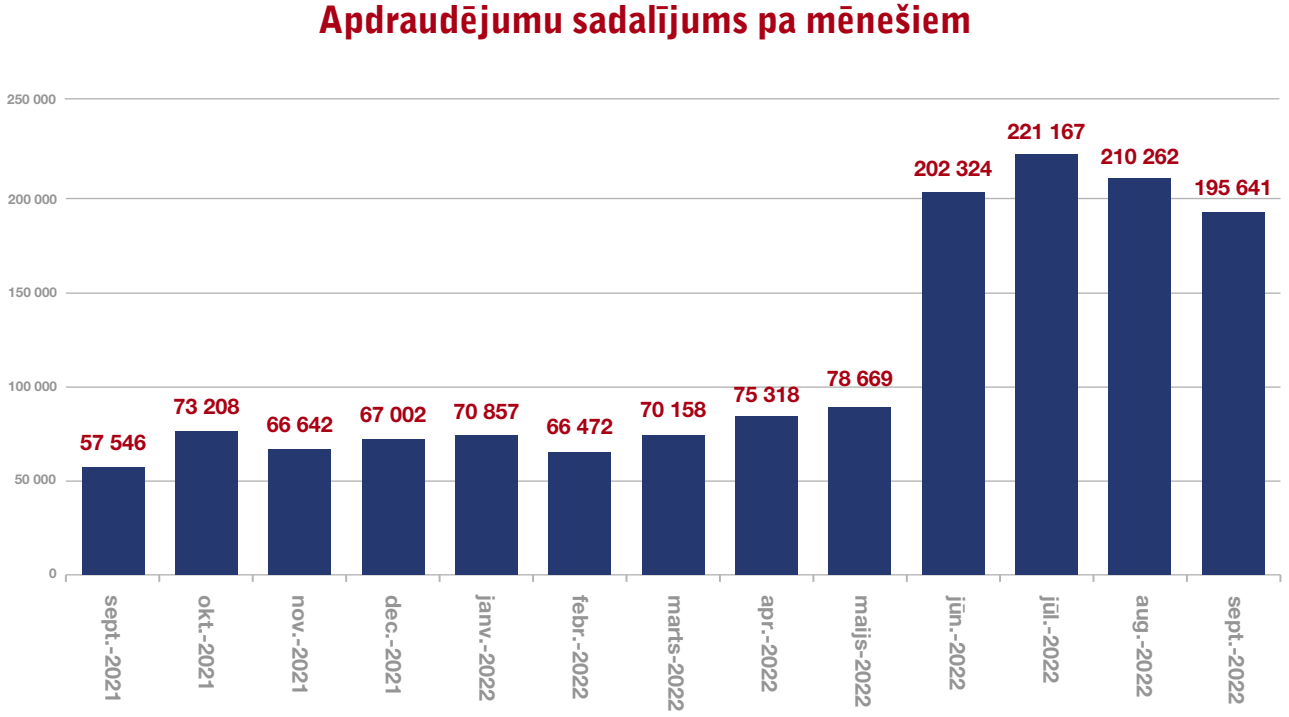
- konfigurācijas nepilnības (118 123 unikālas IP adreses) ar kritumu par 5% pret iepriekšējo periodu;
- bija ļaundabīgs kods (10 424 unikālas IP adreses) ar pieaugumu par 5%;
- pakalpojuma pieejamība (2125 unikālas IP adreses) ar kritumu par 20%.

Pārskata periodā CERT.LV par IT drošību izglītoja 3349 cilvēkus, iesaistoties 18 pasākumos.

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

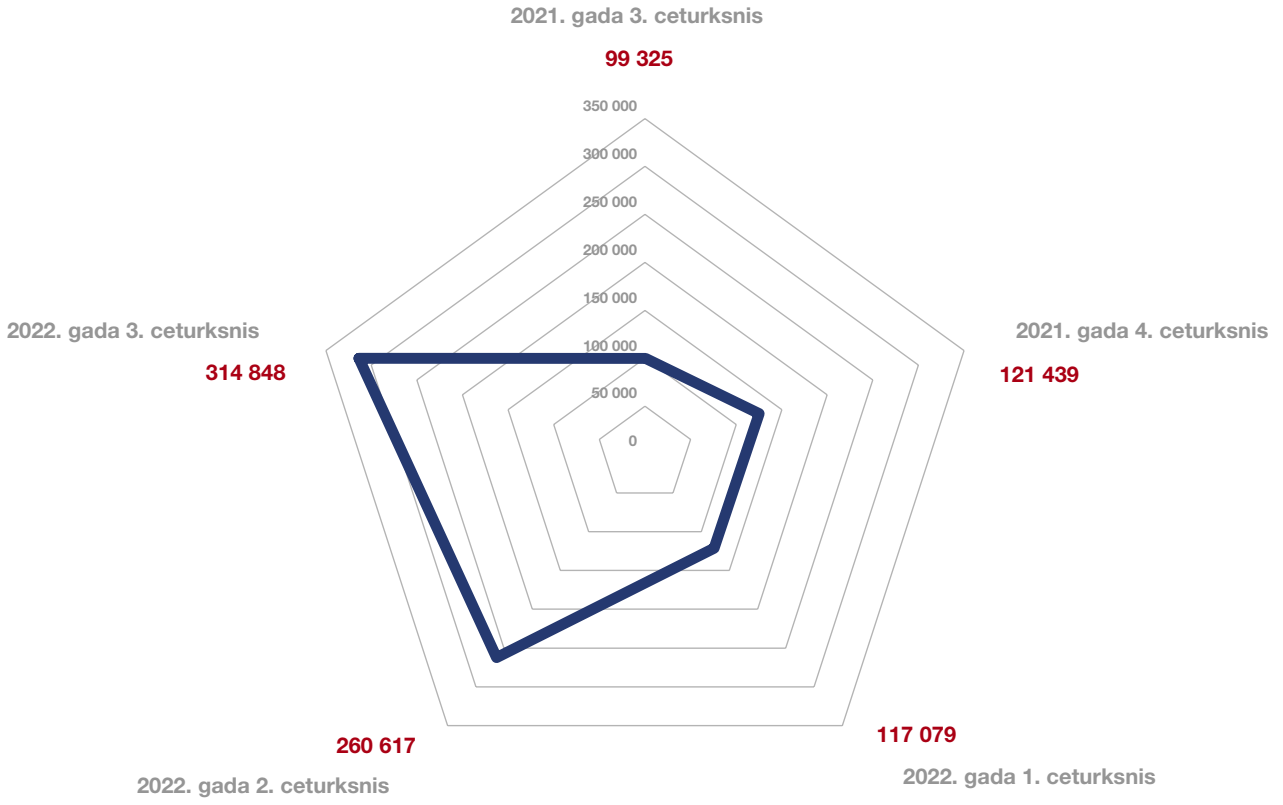
1. Vienota atainojuma uzturēšana par elektroniskās informācijas telpā notiekošajām darbībām

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



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

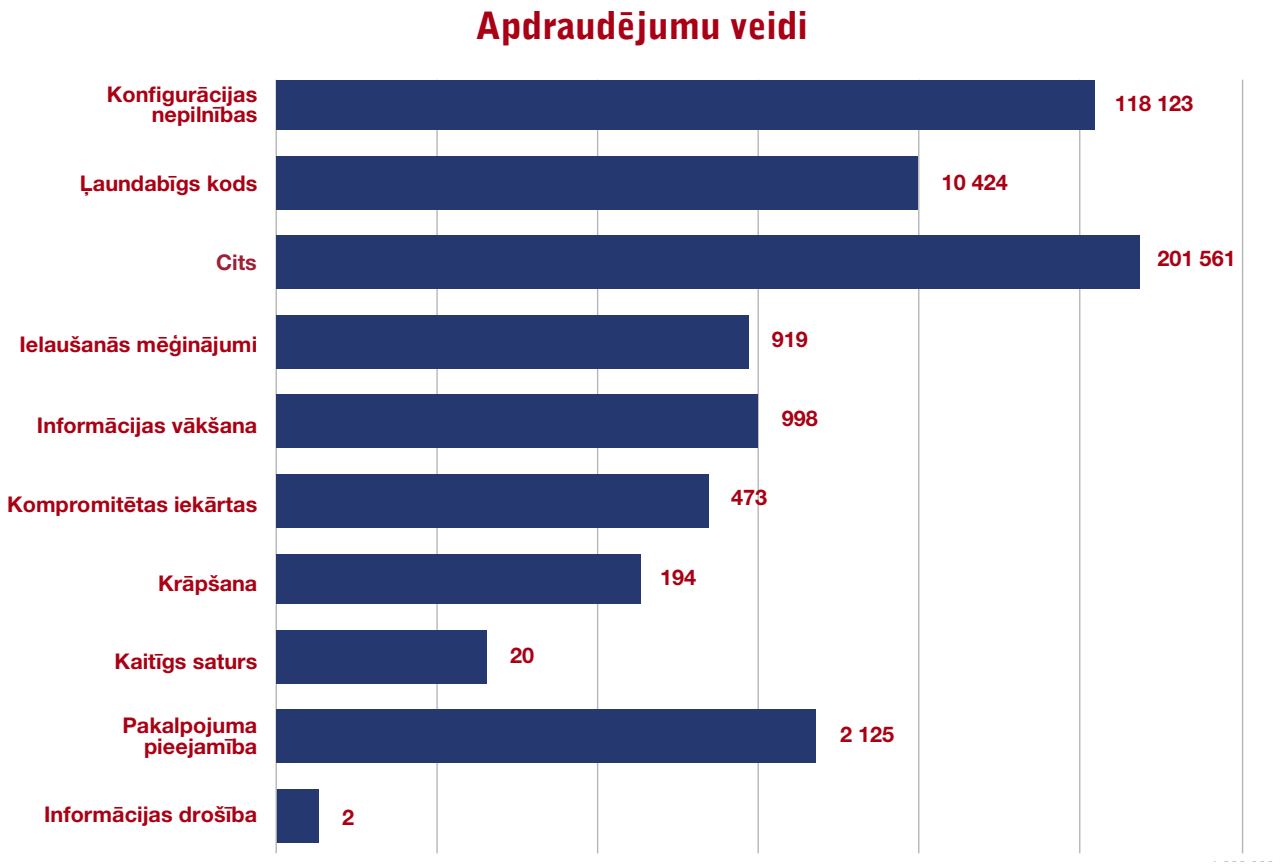
Apdraudējumu sadalījums pa ceturkšņiem



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

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.

2022. gada 3. ceturksnī tika reģistrētas 314 848 unikālas apdraudētas IP adreses, kas ir par 20% vairāk nekā iepriekšējā ceturksnī un par 217% vairāk nekā šajā pašā periodā pirms gada. Augstais

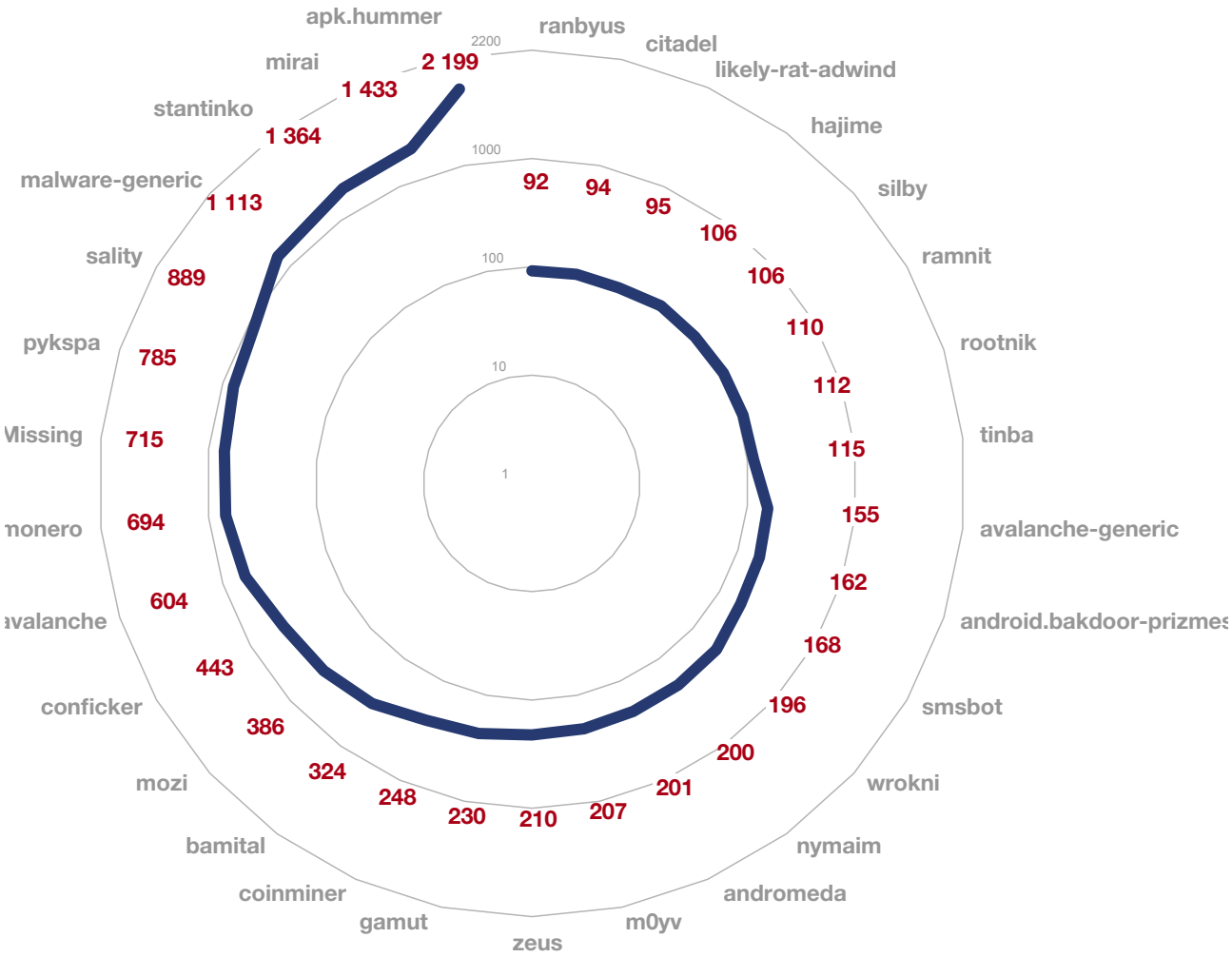


3. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2022. gada 3. ceturksnī pa apdraudējumu veidiem.

apdraudēto IP adrešu apjoms skaidrojams ar apjomīgajiem konfigurācijas nepilnību rādītājiem, kas saņemti no sadarbības partneriem un norāda uz potenciāli ievainojamām iekārtām Latvijas interneta tīklā.

Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (118 123 unikālas IP adreses) ar kritumu par 5% pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs

Unikālo IP adrešu skaits – ļaundabīgs kods



4. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2022. gada 3. ceturksnī ar apdraudējuma veidu – ļaundabīgs kods.

kods (10 424 unikālas IP adreses) ar pieaugumu par 5%, bet trešais – pakalpojuma pieejamība (2125 unikālas IP adreses) ar kritumu par 20%.

Augstais konfigurācijas nepilnību apjoms skaidrojams ar augstajiem rādītājiem tādās datu kategorijās kā *Accessible-SSL, Accessible-ssh, Accessible-smtp* u.c., par kurām informāciju apkopo un piegādā CERT.LV sadarbības partneri, bet kuras nenorāda uz tūlītēji bīstamām iekārtām. Informācija tiek apkopota, lai vērstu uzmanību uz potenciālu apdraudējumu, kas var rasties, ja iekārtas pieejamība internetā ir nejauša, tā nav aizsargāta ar drošu paroli vai šāda iekārta tiek aizmirsta un netiek pienācīgi atjaunināta.

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

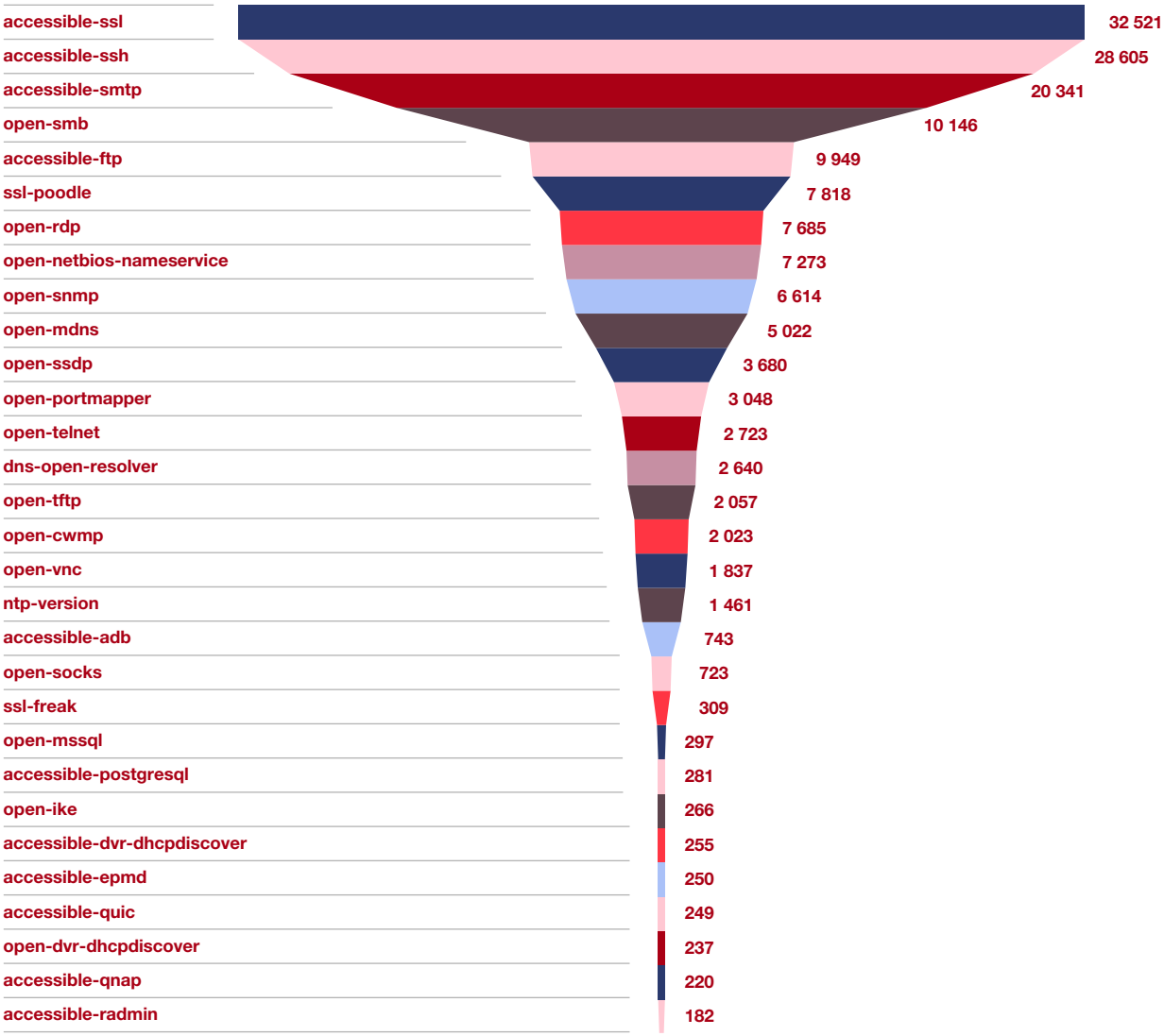
Otro vietu ieņem ļaunatūra *Mirai*, kas apdraud neatbilstoši aizsargātas lietu interneta (*IoT*) iekārtas. Visbiežāk inficēti tiek viedie televizori, interneta maršrutētāji, novērošanas kameras vai citas līdzīgas iekārtas, kas pēc iegādes tiek pieslēgtas internetam, nenomainot ražotāja iestatīto lietotājvārdu un paroli. Šīs iestatītās jeb noklusējuma paroles ir plaši zināmas, un to izmantošana pakļauj iekārtas paaugstinātam uzbrukuma riskam.

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

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

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

Unikālo IP adrešu skaits – konfigurācijas nepilnības



5. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2022. gada 3. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

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

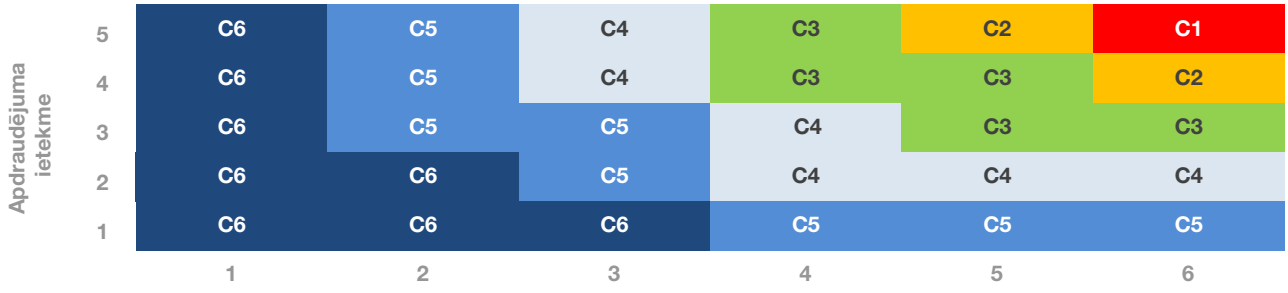
Pilnvērtīgākam kibersituācijas novērtējumam CERT.LV 2020. gadā ir uzsākusi *Apvienotās Karalistes Nacionālā kiberdrošības centra (NCSC)* izveidotās apdraudējumu matricas lietošanu. Matricā ievietotie apdraudējumi tiek grupēti pēc tā, cik nozīmīga ir skartā iestāde vai uzņēmums un/vai cik plašu sabiedrības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

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

Gandrīz 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.

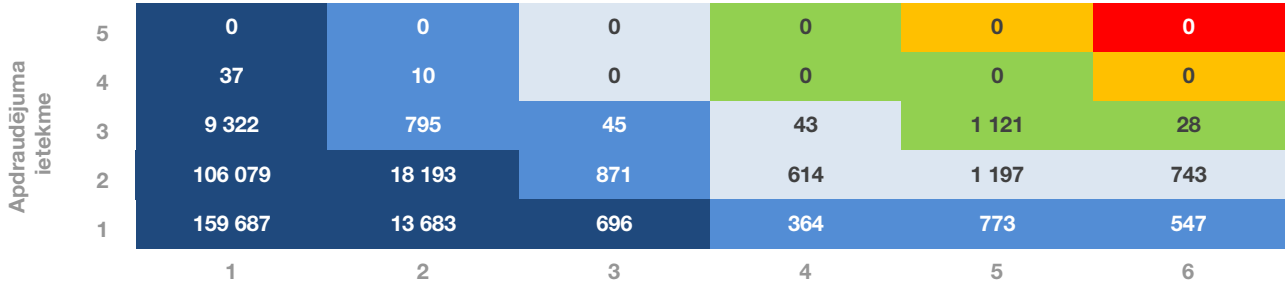
Nacionāla līmeņa apdraudējumi (C1) un augstas nozīmes apdraudējumi (C2) pārskata periodā nav reģistrēti.

Apdraudējumu matrica



6. attēls – Apdraudējumu matricas sadalījums kategorijās.

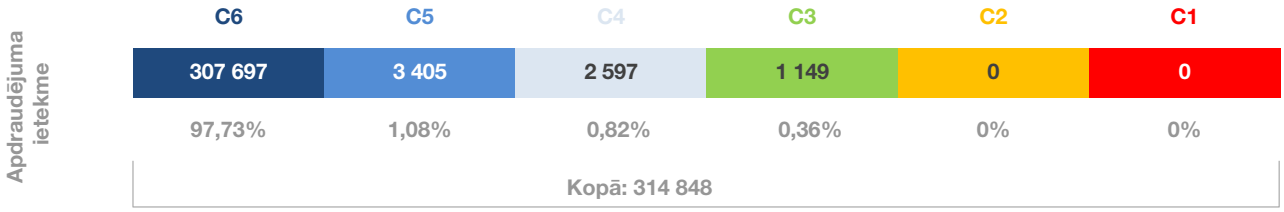
Apdraudēto unikālo IP adrešu izvietojums



7. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu izvietojums matricā 2022. gada 3. ceturksnī valsts un pašvaldību institūcijās.

Nozīmīgi plašas ietekmes apdraudējumi (C3) veido 0,36% (1149 unikālas apdraudētas IP adreses/gadījumi) no visiem kategorizētajiem apdraudējumiem. 97% šo apdraudējumu veido pakalpojuma pieejamības incidenti, 2% ļaundabīgs kods, bet 1% kompromitētas iekārtas un atsevišķi informācijas drošības incidenti.

Apdraudēto unikālo IP adrešu sadalījums



8. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu sadalījums apdraudējumu kategorijās pēc apdraudējuma ietekmes (matrica) 2022. gada 3. ceturksnī.

Lielākā daļa C4 līmeņa apdraudējumu (būtiski apdraudējumi ar vidēju ietekmi) jeb 77% bija konfigurācijas nepilnības (*Accessible-ssl*, *Accessible-smtp, Accessible-ssh, Open-rdp* u.c.), bet 14% pakalpojuma pieejamības (DDoS) incidenti, kas novēroti augstas un vidēji augstas prioritātes iestādēs. Konfigurācijas nepilnības fiksētas vairākos uzņēmumos un valsts iestādēs, kā arī augstskolās un pašvaldībās. Pakalpojuma pieejamības incidenti fiksēti vairākās valsts iestādēs, pašvaldībās, finanšu institūcijās un pie interneta pakalpojumu sniedzējiem.

Lai sekmētu kopējo kiberdrošību valstī, CERT.LV sadarbībā ar NIC.LV ir izveidojusi un uztur 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 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 NIC.LV uzturētajā DNS ugunsmūrī https://dnsmuris.lv, tādējādi pasargājot no uzbrukuma DNS ugunsmūra lietotājus. DNS ugunsmūris bez maksas ir pieejams ikvienam Latvijas iedzīvotājam un uzņēmumam.

Pārskata periodā uzbrucēji kampaņveidīgi centās izkrāpt maksājumus vai izvilināt Latvijas iedzīvotāju maksājumu karšu un internetbankas piekļuves datus. Mērķa sasniegšanai uzbrucēji izmantoja sociālo inženieriju, nosūtot upuriem pikšķerēšanas e-pastus Valsts policijas, Eiropola, Latvijas Pasta vai banku vārdā, un draudēja ar sodu par pretlikumīgām darbībām, bankas konta bloķēšanu vai sūtījuma nepiegādāšanu, ja e-pasta saņēmējs nesekos e-pastā iekļautajai saitei un neievadīs prasīto informāciju. Atsevišķos gadījumos e-pastu saņēmēji tika aicināti krāpniekiem nosūtīt arī pases datus. E-pastu ticamības palielināšanai tajos pretlikumīgi tika izmantota Latvijas valsts simbolika (ģerbonis) un dažādu valsts amatpersonu identitātes. Krāpnieciskajiem e-pastiem izmantotas e-pastu adreses, kas nebija saistītas ar institūcijām, par kurām krāpnieki uzdevās, un nebija līdzīgas institūciju oficiālajām adresēm. Arī pikšķerēšanas jeb datu izkrāpšanas vietņu adreses skaidri norādīja uz to, ka vietnes nav saistītas ar konkrētajām institūcijām.

Pēc ilgāka pārtraukuma CERT.LV redzeslokā atgriezās arī krāpniecības, kurās uzbrucēji cenšas iegūt maksājumu karšu datus, uzdodoties par privātpersonām, un norāda, ka vēlas iegādāties preci, apmaksai un piegādei izmantojot kurjerpakalpojumus (DPD, *Omniva*). Pārdevējs maksājuma saņemšanai tiek aicināts ievadīt kartes datus (ieskaitot CVV kodu) krāpnieku norādītajā viltotajā kurjerkompānijas vietnē.

Maksājumu karšu datus uzbrucēji centās izvilināt arī, piesolot naudas pārskaitījumu Inbox.lv lietotājiem, kā arī WhatsApp vārdā izsūtot e-pastus par laimestu, kura saņemšanai nepieciešams ievadīt maksājumu kartes datus e-pastā norādītajā krāpnieciskajā vietnē.

Uzbrucēji izmantoja sociālo tīklu sniegtās iespējas un iedzīvotāju vēlmi iegūt papildu ienākumus. Portālos *Facebook*, *Instagram* un *YouTube* tika ievietotas reklāmas, kurās Latvenergo un Swedbank vārdā tika izteikti aicinājumi veikt investīcijas, izmantojot reklāmās norādītās viltus platformas. Krāpnieki aicināja upurus uzstādīt savās iekārtās arī *AnyDesk* programmatūru, kas sniedz uzbrucējiem kontroli pār iekārtu, iespēju pieslēgties tai un sekot visām darbībām, iegūstot personas datus un citu svarīgu informāciju. CERT.LV ir saņēmusi ziņu no viena cietušā par zaudējumiem 150 USD apmērā.

Lai aicinātu iedzīvotājus investēt, izmantojot viltus platformas, krāpnieki veica arī telefona zvanus. Kāda Latvijas iedzīvotāja šādā incidentā cieta zaudējumus 2000 EUR apmērā un nodeva uzbrucēju rīcībā savus personas datus, bet kādā citā incidentā finansiālo zaudējumu apjoms sasniedza 40 000 EUR, jo upuris pieteicās arī vairākiem kredītiem.

Tika saņemti ziņojumi par vairākiem mērķētiem pikšķerēšanas uzbrukumiem, kuri tika veikti, lai iegūtu darbinieku e-pasta piekļuves datus. E-pastus ar aicinājumu nomainīt paroles krāpnieku norādītajā viltus vietnē saņēma gan vairākas valsts iestādes, gan privātā sektora uzņēmumi.

E-pastus organizāciju vadītāju vārdā saņēma vairākas iestādes. Uzbrucēji centās izkrāpt maksājumus, uzsākot sarunu ar jautājumu par konta atlikumu un aicinot veikt steidzamu maksājumu vairāku desmitu tūkstošu apmērā uz uzbrucēju kontrolētu bankas kontu.

Tika saņemti ziņojumi par savdabīgu kampaņu, kurā virkne pašvaldību saņēma e-pastu ar aicinājumu sekot PSRS vēlēšanu norisei.

2.2. Pakalpojuma pieejamība

Sākotnēji tika prognozēts, ka augusta otrajā pusē varētu saasināties kiberuzbrukumu intensitāte saistībā ar plānoto Padomju armijas karavīriem veltītā pieminekļa demontāžu, taču pieminekļa nojaukšanas dienā, 25. augustā, Latvijas kibertelpā uzbrukumu aktivitāte bija vērojama daudz zemāka nekā 11. augustā pēc Saeimas lēmuma Krieviju atzīt par terorismu atbalstošu valsti. Atsevišķos *Telegram* kanālos, kas saistīti ar Krievijas agresiju atbalstošu haktīvistu grupējumiem, tika novēroti aicinājumi uzbrukt Latvijas medijiem, kas nodrošināja translāciju no Uzvaras parka. Latvijas kibertelpā tika izmantoti atbilstoši aizsardzības risinājumi, un nopietni traucējumi netika novēroti.

Ja iepriekšējos mēnešos bija būtiski pieaudzis CERT.LV saņemto ziņojumu skaits par piekļuves atteices jeb DDoS uzbrukumiem gan publiskajam, gan privātajam sektoram, tad septembrī bija novērojama šo ziņojumu apjoma samazināšanās. Tas varētu būt skaidrojams gan ar Krievijas saspīlēto iekšējo situāciju, gan ar Krievijas agresīvo politiku atbalstošo haktīvistu pievēršanos citiem mērķiem, piemēram, Lietuvā (Kaļiņingradas blokāde) un ASV (uzbrukumi lidostu tīmekļa vietnēm).

Nesekmīgi DDoS uzbrukumi pārskata periodā tika novēroti pret Saeimu un virkni citu valsts iestāžu, kā arī pret vairākām finanšu institūcijām, bet īslaicīga nebūtiska uzbrukumu ietekme tika novērota vairākām valsts un pašvaldību iestāžu tīmekļa vietnēm un Pasažieru vilciena tīmekļa vietnei.

Pārskata perioda sākumā vairāku dienu garumā piekļuves atteices uzbrukumu ietekmē īslaicīgus darbības traucējumus piedzīvoja *Mobilly* sniegtie pakalpojumi. Savukārt jūlija beigās īslaicīgi tika traucēta pieeja Korupcijas novēršanas un apkarošanas biroja (KNAB) resursiem, bet augustā apjomīga DDoS uzbrukuma ietekmē vairāku stundu garumā nebija pieejama ziņu aģentūras LETA tīmekļa vietne.

Pārskata perioda sākumā intensīva 12h ilga kiberuzbrukuma rezultātā bija traucēta arī *eParaksts* pakalpojumu izmantošana.

Biežākais DDoS ietekmes mazināšanas risinājums bija piekļuves liegšana no ārzemēm jeb ģeobloķēšana. CERT.LV sagatavoja un publicēja tīmekļa vietnē www.cert.lv rekomendācijas DDoS ietekmes mazināšanai (https://cert.lv/lv/2022/08/ieteikumi-ddos-ietekmes-mazinasanai).

Uz pārskata perioda beigām DDoS uzbrukumu intensitāte mazinājās, taču uzbrukumi turpināja notikt katru dienu.

2.3. Ļaundabīgs kods

Pārskata periodā tika saņemta informācija par vairākām viltotu e-pastu kampaņām dažādu uzņēmumu un organizāciju vārdā. E-pastos tika izplatīta, galvenokārt, ļaunatūra, kas paredzēta informācijas ievākšanai no inficētās iekārtas (*Lokibot, AgentTesla*). Viltotu e-pastu aprites mazināšanai CERT.LV rekomendēja SPF, DMARK un DKIM ieviešanu. Tas sniegtu iespēju gan veikt ienākošo e-pastu pārbaudi, gan ļautu citiem e-pastu saņēmējiem pārliecināties, vai e-pasts tiešām tiek sūtīts no konkrētā uzņēmuma vai arī tas ir atzīmējams kā neuzticams. Pielikumā visbiežāk ir .iso vai .zip arhīva fails, atsevišķos gadījumos *MS Excel* dokuments ar ļaundabīgu *Macros* funkcionalitāti.

2.4. Ielaušanās mēģinājumi

Ielaušanās mēģinājumi 86% gadījumu veikti, izmantojot paroļu minēšanu (*brute-force*). Uzbrukumi veikti galvenokārt pret dažādiem interneta pakalpojumu sniedzējiem. CERT.LV rīcībā esošā informācija liecina, ka šie uzbrukumi nav bijuši sekmīgi.

Tika saņemts ziņojums no kādas valsts iestādes par paroļu minēšanas mēģinājumiem, lai piekļūtu kancelejas *MS Exchange* e-pasta serverim. CERT.LV rekomendēja daudzfaktoru (MFA) autentifikācijas ieviešanu un IP adrešu ierobežošanu.

No vairākām valsts iestādēm tika saņemta informācija par iestāžu resursu skenēšanu ar nolūku iegūt informāciju par ievainojamībām. Visas pamanītās darbības bijušas nesekmīgas.

2.5. Kompromitētas iekārtas un datu noplūdes

Vairāki uzņēmumi cieta šifrējošo izspiedējvīrusu uzbrukumos. Vairumā gadījumu sašifrēta tika QNAP datu uzglabāšanas sistēma, kura netika savlaicīgi atjaunināta un bija pakļauta *DeadBolt* šifrējošā vīrusa inficēšanas riskam. Vienā no incidentiem cietušais uzņēmums apsvēra iespēju maksāt pieprasīto izpirkuma maksu, jo dati bija svarīgi biznesa turpināšanai, bet rezerves kopijas bija novecojušas. CERT.LV rekomendēja nemaksāt un brīdināja, ka samaksa negarantē datu atgūšanu un palielina risku atkārtoti kļūt par izspiedējvīrusa mērķi.

Kādā valsts iestādē tika identificēta inficēta iekārta. Izmeklēšanā tika konstatēts, ka lietotājs sekojis kādai interneta reklāmai un lejupielādējis saturu, kas bija izpildāmais jeb .exe fails, kuru lietotājs atvēris, tādējādi inficējot datoru. CERT.LV norādīja uz nepieciešamību pilnveidot iekšējās drošības politiku, ierobežojot lietotāju iespējas lejupielādēt un izpildīt .exe failus. Konkrētā ļaunatūra netika identificēta kā plaši izplatītu saimi pārstāvoša.

Tika kompromitēts kāda uzņēmuma darbinieka e-pasts. Uzņēmums informēja klientus un sadarbības partnerus par incidentu un aicināja ignorēt e-pastus, kas saņemti no inficētās adreses ar tematu: “CITĀTA PIEPRASĪJUMS (JAUNS PASŪTĪJUMS)”. CERT.LV sniedza rekomendācijas e-pasta drošības stiprināšanai un domēna datu noplūdes monitoringam.

Tika saņemta informācija par kādas pašvaldības tīmekļa vietnes kompromitēšanu. Incidents notika, uzbrucējiem izmantojot ievainojamību novecojušā foruma modulī. Uzbrucēji bija veikuši failu

modifikāciju, lai pārvirzītu apmeklētājus uz uzbrucēju norādītu tirdzniecības vietni. Tīmekļa vietne tika operatīvi atjaunota no rezerves kopijas, paroles nomainītas, novecojusī komponente atslēgta.

Tika konstatēta vairāku valsts iestāžu pārvaldībā esošu resursu kompromitēšana. Nodarītais kaitējums nebija būtisks, jo ietekmētas tika maznozīmīgas tīmekļa vietnes, taču šie incidenti norāda uz trūkumiem IKT resursu pārvaldībā, kas var rezultēties arī ar nopietniem incidentiem. Novārtā atstāti, neatjaunināti, no publiskā interneta pieejami resursi (testa vides, novecojuši projekti) palielina potenciālo uzbrukuma laukumu.

Veicot pārbaudes kādas valsts iestādes infrastruktūrā, netika apstiprināta ļaunatūras klātbūtne, taču tika secināts, ka infrastruktūras uzturēšanā tiek pārkāptas MK noteikumu nr. 442 prasības, kas pakļauj iestādi būtiskam datu izgūšanas riskam.

2.6. Ievainojamības

Jūlija ielāpu otrdienā *Microsoft* publicējis atjauninājumus, kas novērsa kopumā 84 dažādas ievainojamības un drošības nepilnības. To vidū viena bija arī *nulles dienas* ievainojamība (CVE-2022-22047), kas tika aktīvi izmantota reālos kiberuzbrukumos, savukārt četras citas ievainojamības tika raksturotas kā kritiskas. CERT.LV aicināja pēc iespējas ātrāk uzstādīt atjauninājumus.

Tika sagatavots brīdinājums, kas attiecās uz tiem, kuru pārvaldībā ir *MS Exchange* serveri. Tika atklāta jauna un kritiska *0-day Microsoft Exchange* ievainojamība. CERT.LV aicināja pārbaudīt, vai pārvaldībā esoša sistēma nav kompromitēta.

CERT.LV aicināja nekavējoties atjaunināt *Windows* žurnalēšanas sistēmu (*Common Log File System*), uzstādot *Microsoft* publicētos atjauninājumus. Tie novērsa jaunatklātu un uzbrukumos aktīvi izmantotu kritisku ievainojamību CVE-2022-37969.

CERT.LV brīdināja par aktivitātēm un novērojumiem kibertelpā, kas saistīti ar *Log4Shell* un liecina par to, ka šī ievainojamība joprojām ir uzbrucēju pastiprinātas intereses objekts un tiek izmantota arī valstu sponsorētos uzbrukumos. Tika ziņots, ka uzbrucēji pastiprināti meklē neaizsargātus *VMware Horizon* un UAG (*Unified Access Gateway*) serverus, lai ar ievainojamības palīdzību iegūtu stabilas starta pozīcijas tālākiem uzbrukumiem.

Tika konstatētas konfigurācijas nepilnības kādas valsts iestādes infrastruktūrā, kas no publiskā tīkla sniedza piekļuvi visiem lokālajiem datoriem. Iestāde tika informēta, piekļuve tika aizvērta.

2.7. Atbildīga ievainojamību atklāšana

Tika saņemts ziņojums par starpvietņu skriptēšanas (XSS) ievainojamību kādas valsts iestādes mājaslapā. Par ievainojamību tika informēts iestādes par IT drošību atbildīgais.

Tika saņemta informācija par ilgstoši nenovērstu starpvietņu skriptēšanas ievainojamību kāda uzņēmuma tīmekļa vietnē. CERT.LV uzsāka ievainojamības novēršanas koordināciju.
Tika saņemts ziņojums par publiskajā tīklā eksponētu *Jira* servisu. Tika informēti infrastruktūras uzturētāji.

Saņemts atbildīgas ievainojamību atklāšanas ziņojums par kādas valsts iestādes *Apache* serveru atrašanos publiskajā tīklā. Informācija tika nosūtīta atbildīgajai personai.

Tika saņemta informācija par virkni neatbilstību kādas valsts iestādes resursos. Tika konstatēts vecs programmnodrošinājums, SQL injekciju apdraudējums ar piekļuvi visiem darbinieku datiem, ieskaitot paroles nešifrētā formātā. Uzturētāji tika informēti, uzsākta ievainojamību novēršana.

Tika saņemts ziņojums par iespēju izgūt kāda uzņēmuma citu klientu personīgos datus, patvaļīgi mainot īsziņā atsūtītās saites parametra vērtību. Vietnes uzturētājs tika informēts.

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

Cita veida sadarbība ar dažādām iestādēm ir norādīta atskaites 4. un 7. punktā.

3. Pētnieciskais darbs, izglītojošo pasākumu organizēšana un mācības informācijas tehnoloģiju drošības jomā

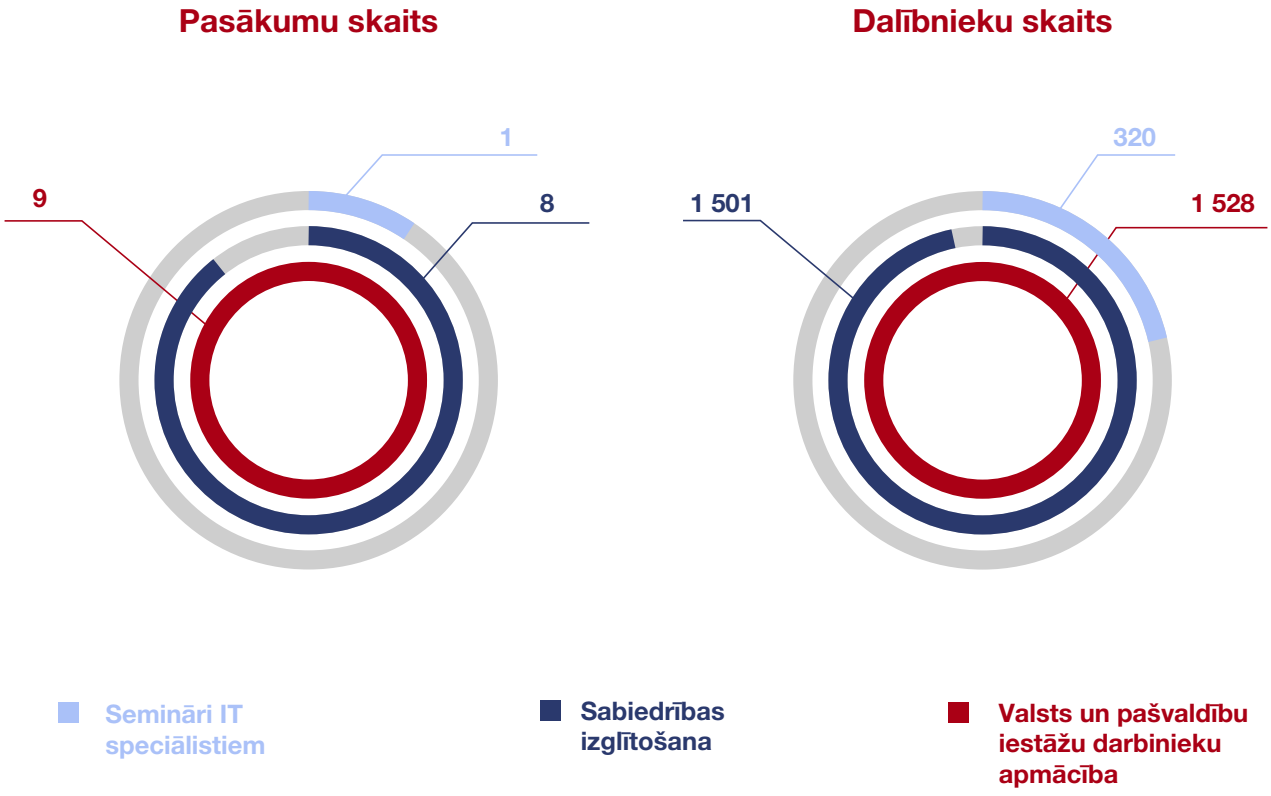
8. jūlijā CERT.LV pārstāvis lekšlietu ministrijas vizionāru seminārā sniedza prezentāciju par aktuālajiem apdraudējumiem kibertelpā, kas potenciāli varētu ietekmēt iekšlietu nozari.

Sadarbībā ar Latvenergo tapa izglītojošs video materiāls par krāpniecībām internetā. Izglītojošais video tika izveidots kā atbilde uz krāpnieku aktivitātēm sociālajā tīklā *Facebook* un platformā *YouTube*. Krāpnieki ar maldinošām reklāmām, kurās pretlikumīgi tika izmantots gan Latvenergo zīmols, gan Latvijas Valsts Prezidenta tēls, centās reklamēt viltus investīciju platformas.

Gatavojoties Saeimas vēlēšanām, tika novadīti semināri par kiberdrošību gan nacionālo, gan reģionālo mediju redaktoriem, aplūkojot gan potenciālos apdraudējumus, kas varētu skart pašus medijus, gan apdraudējumus, kas varētu skart vēlēšanu procesu.

14. septembrī CERT.LV piedalījās LVRTC rīkotajā pasākumā "*Kibernakts22. Kiber(ne)realitāte*.", kura ietvaros norisinājās augsta līmeņa ekspertu diskusija par aktuālajiem notikumiem kibertelpā, par novērotajām izmaiņām, atziņām, secinājumiem un ieteikumiem tālākai rīcībai (https://www.lvrtc.lv/kibernerealitate/).

Izglītojošo pasākumu un apmācīto cilvēku skaits



9. attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2022. gada 3. ceturksnī

20. septembrī CERT.LV pārstāvis piedalījās 9. pašvaldību forumā *Pašvaldība – digitālās sabiedrības veidotāja*, kurā sniedza prezentāciju par kiberdrošības pielāgošanu jaunajiem apstākļiem, kā arī piedalījās diskusijā par drošības un komunikācijas aspektiem pašvaldību pārvaldībā (https://www.zzdats.lv/pasvaldibu-forums-2022/).

29. septembrī Latvijas Universitātes jubilejas konferencē *Laikmeta izaicinājumi: vide, drošība, iekļautība*, kurā universitātes pārstāvji – mācībspēki, pētnieki, studenti – un nozaru eksperti

dalījās viedokļos par aktuālajiem ilgtspējas, drošības, digitalizācijas un iekļautības izaicinājumiem, CERT.LV pārstāvis sniedza prezentāciju *Kibertelpas (l/j)aunumi* par aktuālajiem digitālajiem apdraudējumiem.

Tika sniegts atbalsts Aizsardzības ministrijai informatīvu video materiālu sagatavošanā par pikšķerēšanu, smikšķerēšanu, vikšķerēšanu un izspiedējvīrusiem. Materiāli tiks izmantoti sabiedrības informēšanai Eiropas Kiberdrošības mēneša ietvaros.

Pārskata periodā CERT.LV par IT drošību izglītoja 3349 cilvēkus, iesaistoties 18 izglītojošos pasākumos.

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

Sadarbības tikšanās, konsultācijas un prezentācijas:

- CERT.LV aktīvi piedalījās vēlēšanu drošības darba grupā, lai atbilstoši sagatavotos rudenī gaidāmajām Saeimas vēlēšanām, kā arī tikās ar EDSO vēlēšanu novērotājiem, lai atbildētu uz jautājumiem par vēlēšanu IT sistēmu gatavību.
- Pārskata periodā notika tikšanās ar Latvijas Republikas Valsts kontroli par Revīzijas un metodoloģijas departamenta 2022. gada 26. jūlija lietderības revīzijas Nr.2.4.1-38/2020 *Vai varam paļauties uz informācijas sistēmu pieejamību un e-pakalpojumu saņemšanu?* ziņojumu, kā arī tikšanās ar Aizsardzības ministriju un VARAM par veicamajām darbībām ziņojumā ietverto uzdevumu izpildei.
- Turpinājās koordinētas ievainojamību atklāšanas ziņojumu reģistrēšanas platformas izstrāde, kas tika uzsākta, balstoties uz Ministru kabineta apstiprināto Aizsardzības ministrijas izstrādāto informatīvo ziņojumu *Par koordinētas ievainojamību atklāšanas*

procesa ieviešanu valsts pārvaldē, ar kuru ir uzsākta koordinētu ievainojamību atklāšanas procesa (turpmāk – KIAP) ieviešana valsts pārvaldē, paredzot iespēju iestādēm brīvprātīgi iesaistīties KIAP. CERT.LV ir paredzēta vidutāja un koordinatora loma. Oktobra beigās plānots atvērt platformu iestāžu pieteikumiem, piedāvājot iespēju reģistrēt resursus, kurus pētniekiem atļauts testēt. 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.

- CERT.LV piedalījās Aizsardzības ministrijas gatavotās Latvijas Kiberdrošības stratēģijas 2023.-2026. gadam koncepcijas izveidošanā un turpina aktīvu dalību stratēģijas izstrādē, piedaloties sanāksmēs, komentējot un papildinot darba dokumentus.
- Tika sniegti komentāri Aizsardzības ministrijai par Nacionālo kiberdrošības likumu, kuru Aizsardzības ministrija virzīs publiskai apspriešanai 2022. gada pēdējā ceturksnī.
- 1. jūlijā Ekonomiskās sadarbības un attīstības organizācijas (OECD) Parlamentārā tīkla sanāksmē Rīgā CERT.LV pārstāvis uzstājās ar prezentāciju par IKT risku un ievainojamību pārvaldību.
- 5. jūlijā dalība Latvijas Finanšu nozares asociācijas vadītās Krāpšanas ierobežošanas darba grupas sēdē, lai pārrunātu krāpniecisku mājaslapu pieejamības un pikšķerēšanas uzbrukumu ierobežošanas iespējas. Darba grupas mērķis ir veikt stratēģiskus koordinācijas pasākumus sektora līmenī un apzināt iespējamos pasākumus plašākā mērogā, lai ierobežotu krāpšanas, kuru ietvaros paši banku klienti autorizē piekļuvi saviem līdzekļiem.
- 8. augustā CERT.LV piedalījās topošo MK noteikumu projekta *Noteikumi par publisko elektronisko sakaru tīklu un tajos izmantoto iekārtu, programmatūru un ārpakalpojumu drošības prasībām, kompetentajām iestādēm drošības prasību piemērošanas uzraudzībai un to funkcijām uzraudzības jomā* iesūtīto iebildumu izskatīšanā savas kompetences ietvaros.

- 5. septembrī dalība sanāksmē ar Aizsardzības ministriju un Izglītības un zinātnes ministriju par Ministru kabineta noteikumu Nr. 442 prasību piemērošanu attiecībā uz mākoņpakalpojumu izmantošanu izglītības iestāžu datu glabāšanai.
- Ar septembri CERT.LV noslēdza savu darbību projektā par valkājamo ierīču drošību (*WearSec*). Projekta ietvaros tika sagatavota publikācija *NordSec 2022* konferencei, kas 30. novembrī notiks Islandē, kā arī reģistrēts Latvijas patents par *Bluetooth* datu ierakstu un analīzi. Projekta ietvaros veiktā pētījuma prezentācija tika iekļauta 4.-5. oktobrī notiekošās CERT.LV organizētās konferences *CyberChess 2022* tehniskajā sadaļā *CyberShock*.

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 divās NIS (Tīklu un informācijas drošības) direktīvas CERTu tīkla darba grupās:
  - *Cyber Weather* darba grupā, kura regulāri apkopo informāciju par būtiskākajiem kiberincidentiem un reizi ceturksnī izstrādā kiberlaikapstākļu pārskatu Eiropai. Pārskata periodā CERT.LV pārstāve Madara Krutova darbojas kā šīs darba grupas līdzpriekšsēdētāja.
  - *Maturity* darba grupā, kura rūpējas par ES dalībvalstu CSIRT komandu brieduma līmeņa paaugstināšanu.
- No 25. jūnija līdz 1. jūlijam CERT.LV pārstāvji piedalījās FIRST konferencē, kas notika Dublinā, Īrijā. CERT.LV pārstāvis konferences laikā piedalījās vairākās FIRST

Membership Committee (Jauno biedru uzņemšanas komitejas) sanāksmēs, lai apspriestu turpmākos noteikumus biedru uzņemšanā un piesaistīšanā, kā arī SIM3 modeļa izmantošanas pirmā gada rezultātus. CERT.LV vadītāja Baiba Kaškina turpināja darbu kā *FIRST Membership Committee* līdzpriekšsēdētāja (*co-chair*), piedaloties jauno biedru pieteikumu izskatīšanā un veicinot biedru uzņemšanas procesa uzlabošanu. Tā kā otrs līdzpriekšsēdētājs tika ievēlēts FIRST valdē, B.Kaškina kļuva par grupas priekšsēdētāju.

- Turpinājās darbs FIRST SIG darba grupā *CSIRT Services Framework*. Tika izstrādāts vienots ietvars CERT komandu dalībnieku lomām, kompetencēm un prasmēm. Pārskata periodā identificēta nepieciešamība noteikt CERT komandu tipus, kas sekmētu veicamajiem uzdevumiem nepieciešamo lomu un kompetenču identificēšanu.

- 30. jūlijā attālināta sanāksme ar Maurīcijas nacionālo CERT komandu CERT-MU, lai labāk iepazītos un varētu atbalstīt šīs komandas uzņemšanu *Trusted Introducer* CERT komandu kopienā.

- Dalība ENISA vadītajā darba grupā *Coordinated Vulnerability Disclosure (CVD) Task Force*, kurā norit darbs pie ES līmeņa koordinētas ievainojamību atklāšanas politikas vadlīniju veidošanas.

- CERT.LV pārstāvis sadarbībā ar citu ES dalībvalstu ekspertiem piedalījās *ENISA Foresight project 2030* seminārā. Semināra laikā tika izstrādāti maksimāli reālistiski apdraudējumu scenāriji, kuri tiks izmantoti, modelējot nākotnes kiberdrošības izaicinājumus un potenciālos risinājumus.

- Dalība ENISA Eiropas kiberdrošības indeksa (*EU Cybersecurity index*) darba grupā, kurā tiek izstrādāta kiberdrošības indeksa vērtības aprēķina metodoloģija dalībvalstu kiberdrošības novērtēšanai. Pārskata periodā tika izstrādāts vērtējuma anketas pilotprojekts un sniegts atbalsts Aizsardzības ministrijai anketas atbilžu aizpildīšanā. 2023. gadā, balstoties uz dalībvalstu iesniegto anketas rezultātu izpēti, tiks sagatavota ES kiberdrošības indeksa anketa, kas turpmāk tiks izmantota valstu kiberdrošības līmeņa novērtēšanai.

- 28.-29. septembrī TF-CSIRT 67. sanāksmē Viļņā, Lietuvā, CERT.LV pārstāvis sniedza prezentāciju par situāciju un apdraudējumu aktualitātēm Latvijas kibertelpā.
- Turpinājās aktīva dalība enerģētikas informācijas apmaiņas un sadarbības grupā *Energy ISAC Camelot*, lai veicinātu informācijas apmaiņu un sekmētu enerģētikas sektora kiberdrošību.
- Dalība EU *CyberNet* projektā kā vienam no partneriem un piedalīšanās ikmēneša sanāksmēs. Projekta mērķis ir stiprināt kiberdrošības ekspertīzi un attīstīt to ne tikai Eiropas Savienībā, bet arī ārpus tās robežām (www.eucybernet.eu). Dalība projektā sniedz iespēju CERT.LV ekspertiem iesaistīties dažādos projektos, stiprināt savas zināšanas un kapacitāti.
- 17. augustā kopā ar Aizsardzības ministrijas pārstāvjiem tikšanās ar Dānijas kolēģiem, lai pārrunātu pieredzi kiberdrošības centra izveidē un starptautiskas sadarbības organizēšanu.
- Pārrunas ar Luksemburgas CERT komandu par apvienoto dalību NATO CCDCoE organizētajās kiberdrošības mācībās *Locked Shields 2023*.

Sadarbība konkrētu incidentu risināšanā aplūkota pārskata 2. punktā.

6. Projekta Joint Threat Analysis Network īstenošana

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

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

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

2022. gada 3.ceturksnī CERT.LV turpināja darbu pie *Grafoskopa* izstrādes, tā attīstīšanas un pilnveidošanas. Pārskata periodā CERT.LV piedalījās attālinātās JTAN projekta sanāksmēs, kurās projekta partneri informēja par saviem projekta uzdevumiem un rezultātiem. Attiecībā uz JTAN projekta iepirkumu notiek diskusijas par iepirkuma saturu un iespējamajām prasībām.

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

- Lai sekmētu kopējo kiberdrošību valstī, CERT.LV sadarbībā ar NIC.LV ir izveidojusi un uztur 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.

  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.

Pārskata perioda laikā lietotāji tika pasargāti 19518 reizes. Daži no nozīmīgākajām aktīvās aizsardzības epizodēm:

- Bloķētas viltus loterijas ar krāpšanu saistītās lapās eu.gotbstgifts.click: 6463;
- Viltus bankas lapu bloķētie pieprasījumi: 695;
- Viltus kurjerkompāniju lapas: 865;
- Vīrusu kontrolserveri, no vēstulēm, kas tika izsūtītas no uzlauztiem e-pastu kontiem vai kontiem, kur tika viltots izsūtītājs: 651.

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

► 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. DDUK eksperti turpināja darbu dažādās ES līmeņa ekspertu darba grupās – eIDAS 2 regulas tapšanā, FESA, u.c.

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 01.07.2022. līdz 30.09.2022. ir saņēmusi un izvērtējusi 844 ziņojumus. No tiem 633 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 9 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 22 ziņojumos konstatēta personas goda un cieņas aizskaršana, 17 ziņojumi saņemti par naida runu. Par finanšu krāpšanas mēģinājumiem internetā saņemti 61 ziņojums, 65 ziņojumu saturs nav bijis pretlikumīgs, 37 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 592 ziņojumi par naida runu un bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 53 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kuru atrašanās vieta bija ārpus Latvijas, ir ievietoti INHOPE asociācijas datu bāzē un iesniegti attiecīgās INHOPE valsts ziņojumu līnijai turpmāko darbību veikšanai, lai dzēstu nelegālo saturu no publiskas aprites.

Pārskata periodā no Latvijā uzturētajiem 633 ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem 632 ziņojumi ir dzēsti no publiskas aprites un 1 ziņojuma saturs atrodas dzēšanas procesā sadarbībā ar Valsts policiju un interneta pakalpojumu sniedzējiem.

2022. gada 11. novembrī.

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