Latvijas universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

2022 C4

Publiskais pārskats par CERT.LV uzdevumu izpildi

2022. gada 4. ceturksnis (01.10.2022. – 31.12.2022.)

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 4

1. Vienota atainojuma uzturēšana par elektroniskās informācijas telpā notiekošajām darbībām 6

2. Atbalsta sniegšana informācijas tehnoloģiju drošības incidentu novēršanā vai novēršanas koordinēšana 15

2.1. Krāpšana 15

2.2. Pakalpojuma pieejamība 17

2.3. Ļaundabīgs kods 18

2.4. Ielaušanās mēģinājumi 19

2.5. Kompromitētas iekārtas un datu noplūdes 19

2.6. Ievainojamības 20

2.7. Atbildīga ievainojamību atklāšana 21

3. Pētnieciskais darbs, izglītojošo pasākumu organizēšana un mācības informācijas tehnoloģiju drošības jomā **22**

4. Atbalsts valsts institūcijām valsts drošības sargāšanā, noziedzīgu nodarījumu un likumpārkāpumu atklāšanā **25**

5. Sadarbība ar starptautiski atzītām informācijas tehnoloģiju drošības incidentu novēršanas institūcijām **27**

6. Projekta Joint Threat Analysis Network īstenošana **30**

7. Citi normatīvajos aktos noteiktie pienākumi **31**

8. Institūta papildu pasākumu veikšana – atskaite par Latvijas Interneta asociācijas Net-Safe Latvia Drošāka interneta centra ziņojumu līnijas darbību **33**

Kopsavilkums

Kopumā situācija Latvijas kibertelpā, lai arī intensīva, bija 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 kritiskās infrastruktūras uzņēmumiem, taču vairumā gadījumu tie neradīja ietekmi vai arī ietekme bija neliela. Veiksmīgi sadarbojoties VAS "Latvijas Valsts radio un televīzijas centrs", SIA "Tet" un CERT.LV, valsts un kritiskās infrastruktūras IKT resursiem tiek nodrošināta augsta noturība pret DDoS uzbrukumiem.

Sadarbībā ar ārvalstu partneriem no NATO tika turpināts veikt pārbaudes un draudu medības vairākās Latvijas Republikas kritiskās informācijas sistēmās, lai uzlabotu spēju atturēt apdraudējumus un reaģēt uz uzbrucēju darbībām. Draudu medības sniedza labāku izpratni par uzbrucējiem un veicināja sabiedroto komandu sadarbības spēju uzlabošanu un pieredzes apmaiņu, lai efektīvāk aizsargātu sistēmas, balstoties uz kopīgi iegūto informāciju.

Savukārt no vairākiem uzņēmumiem tika saņemti incidentu ziņojumi par iejaukšanos biznesa sarakstē. Uzņēmumi, apmaksājot sadarbības partneru vārdā atsūtītus viltus rēķinus un veicot pārskaitījumus uz krāpnieku norādīto bankas kontu, cieta ievērojamus zaudējumus, kuru kopējais apjoms pārsniedz 500 tūkstošus eiro.

Pārskata periodā tika reģistrētas 360 973 unikālas apdraudētas IP adreses, kas ir par 15% vairāk nekā iepriekšējā ceturksnī un par 197% vairāk nekā šajā pašā periodā pirms gada. Izplatītākie apdraudējumi:

- konfigurācijas nepilnības (91 407 unikālas IP adreses) ar kritumu par 23% pret iepriekšējo periodu;

- ļaundabīgs kods (11 351 unikāla IP adrese) ar pieaugumu par 9%;
- pakalpojuma pieejamība (2902 unikālas IP adreses) ar pieaugumu par 37%.

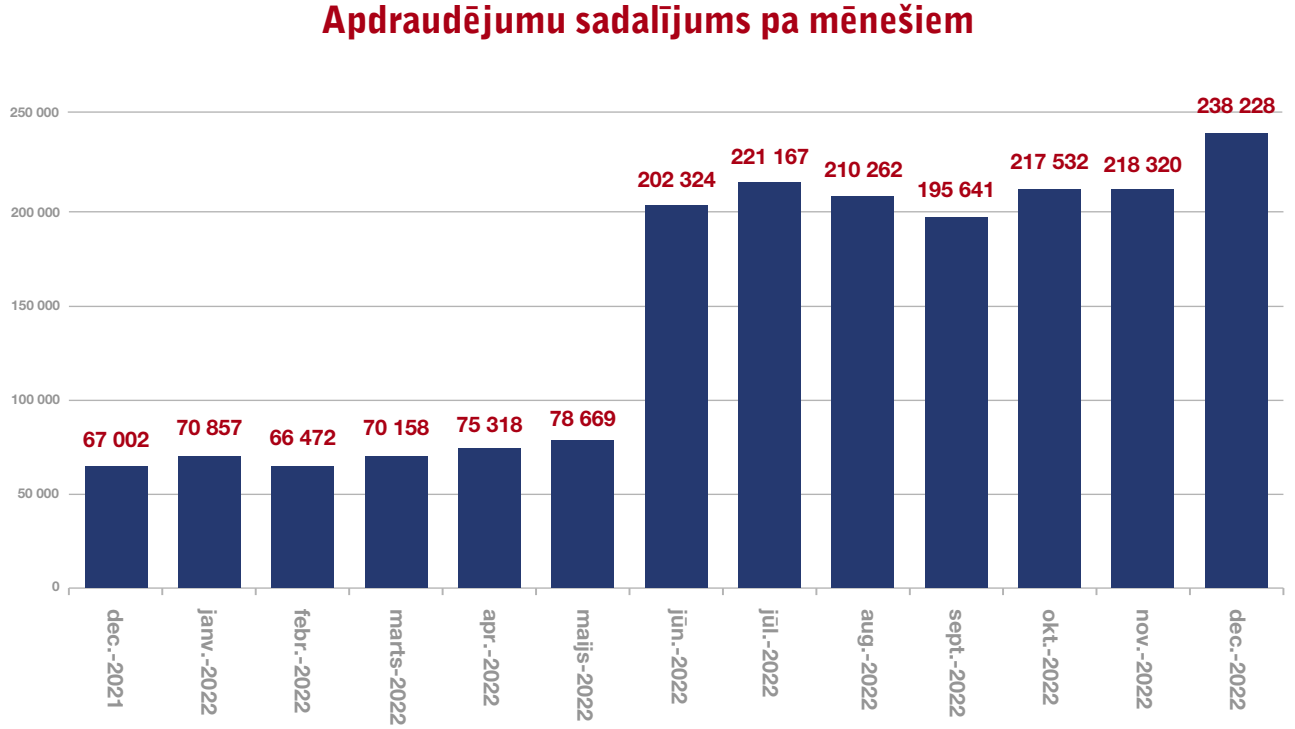
4.-5. oktobrī Eiropas Kiberdrošības mēneša ietvaros tika organizēta starptautiskā IT drošības konference ***Kiberšahs 2022***, kuras ietvaros divās paralēlsesijās tika aplūkoti stratēģiski politiskie kiberdrošības jautājumi Latvijā un Eiropā, kā arī veikta padziļināta tehnisku kiberdrošības tēmu izpēte un praktiskās demonstrācijas. Konferenci klātienē vēroja gandrīz 300 kiberdrošības ekspertu, bet pasākuma tiešraide piesaistīja vairāk nekā 3000 skatītāju no vismaz 30 pasaules valstīm.

Pārskata periodā CERT.LV par IT drošību izglītoja 8380 cilvēkus, iesaistoties 33 izglītojošos pasākumos.

Apdraudējuma līmenis Latvijas kibertelpā pārskata periodā bijis augsts, taču situācija tika veiksmīgi kontrolēta, CERT.LV sadarbībā ar partneriem turpina uzraudzīt tajā notiekošo.

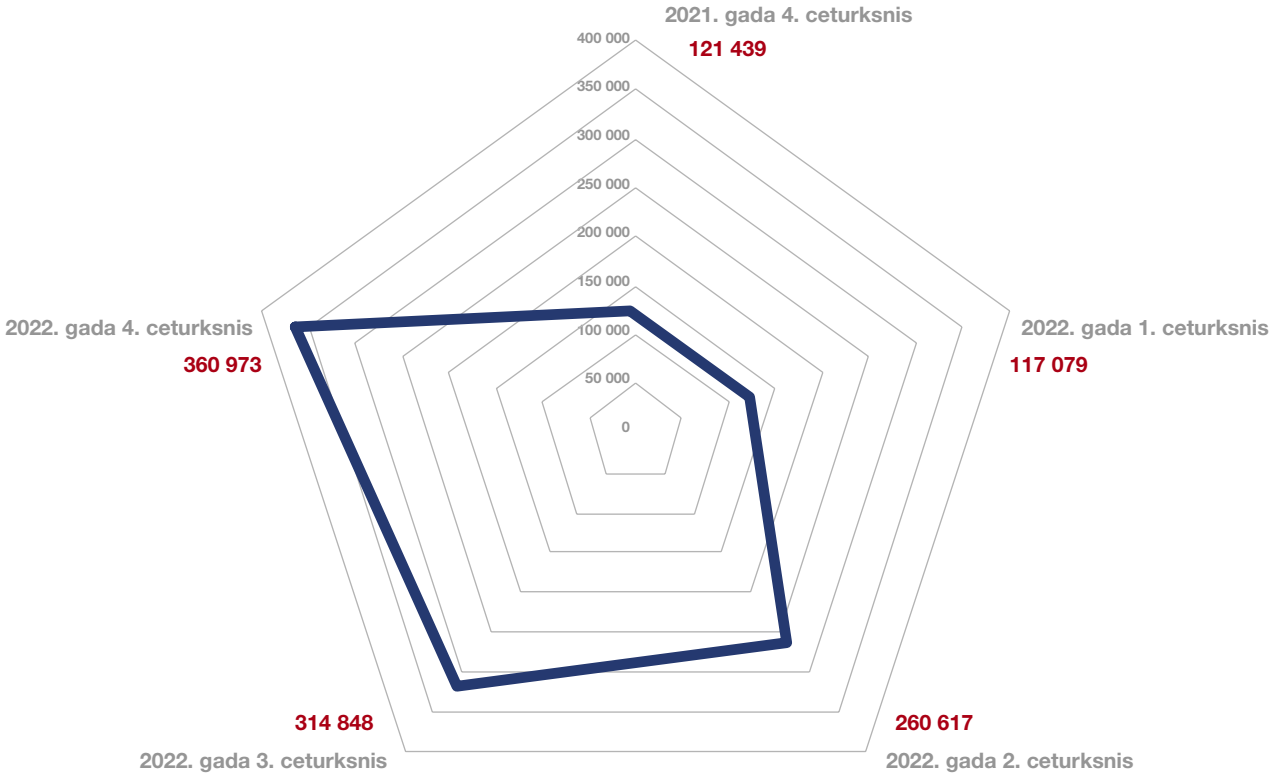
1. Vienota atainojuma uzturēšana par elektroniskās informācijas telpā notiekošajām darbībām

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 uzskaitīti vienkopus, sadalot



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

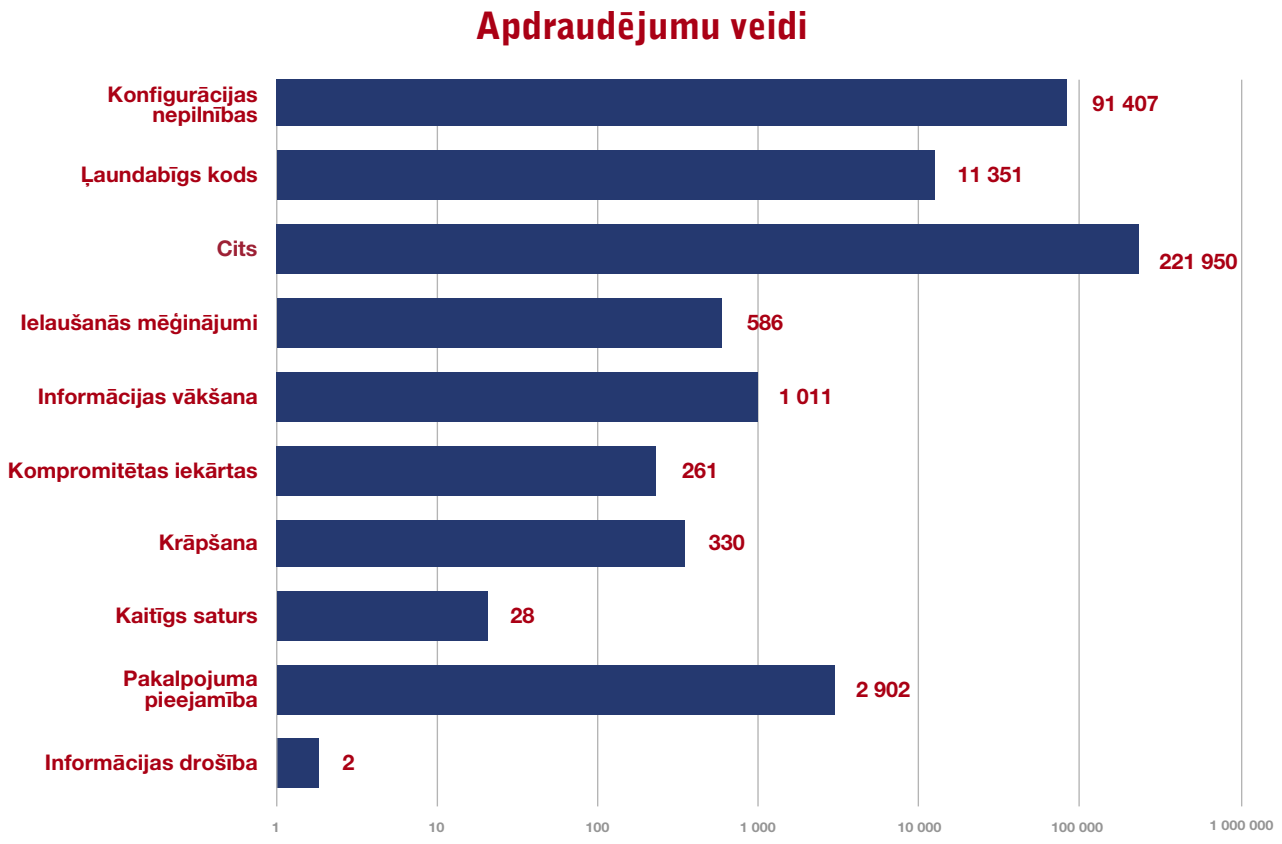
Apdraudējumu sadalījums pa ceturkšņiem



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

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 4. ceturksnī tika reģistrētas 360 973 unikālas apdraudētas IP adreses, kas ir par 15% vairāk nekā iepriekšējā ceturksnī un par 197% vairāk nekā šajā pašā periodā pirms gada. Augstais apdraudēto IP adrešu apjoms skaidrojams ar intensīvajiem piekļuves lieguma jeb DDoS uzbrukumiem un kāpumu reģistrētās ļaunatūras apjomā.

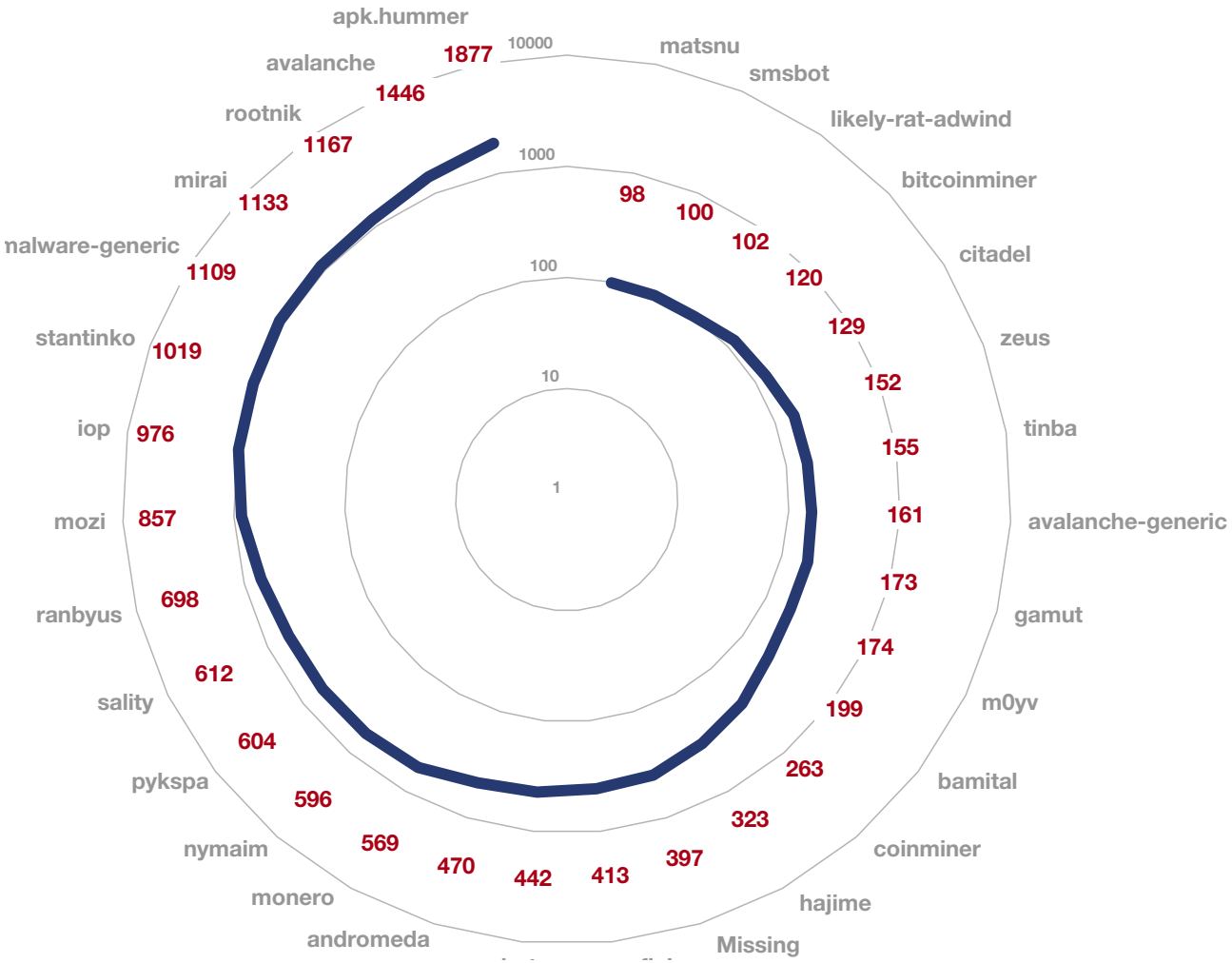


3. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2022. gada 4. ceturksnī pa apdraudējumu veidiem.

Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (91 407 unikālas IP adreses) ar kritumu par 23% pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs kods (11 351 unikāla IP adrese) ar pieaugumu par 9%, bet trešais – pakalpojuma pieejamība (2902 unikālas IP adreses) ar pieaugumu par 37%.

Kritums konfigurāciju nepilnību apjomā skaidrojams ar to, ka no statistikas tika izslēgti no sadarbības partneriem saņemtie dati, kas tiešā veidā nenorāda uz apdraudētām iekārtām, bet iekļauj gadījumus,

Unikālo IP adrešu skaits – ļaundabīgs kods



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

kuros iekārtas tikai noteiktos apstākļos varētu radīt apdraudējumu (*Accessible-ssh, Accessible-smts, Accessible-ssl* u.tml.). Savukārt pieaugošā pakalpojumu pieejamības jeb DDoS uzbrukumu intensitāte skaidrojama ar *Killnet* un citu līdzīgu haktīvistu grupējumu aktivitātēm.

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

Trešajā vietā ierindojas ļaunatūra *Rootnik*, kas veic modifikācijas iekārtās ar *Android* operētājsistēmu, lai iegūtu saknes (*root*) piekļuves tiesības iekārtai, tādējādi iegūstot kontroli pār šo iekārtu.

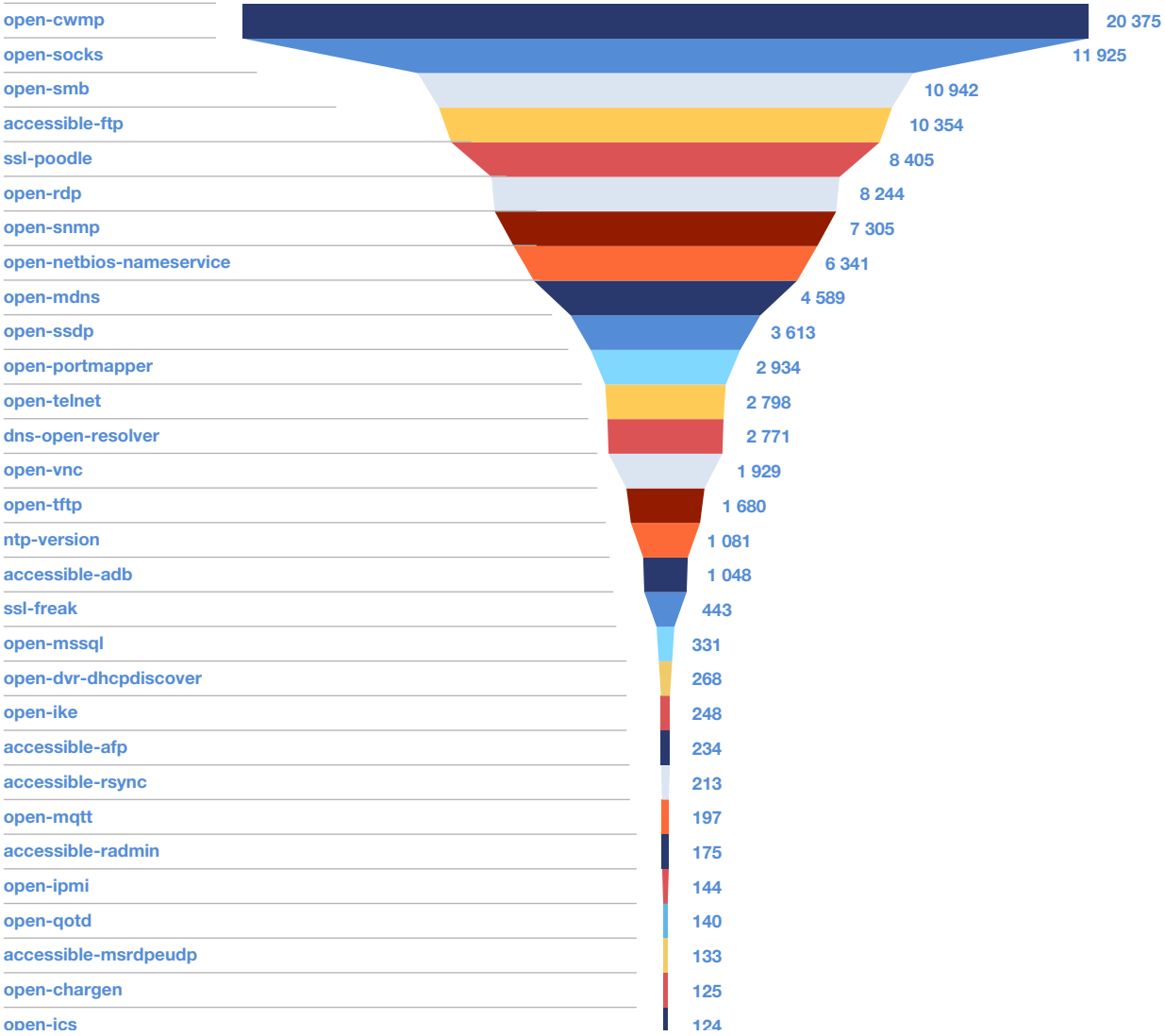
Pirmo vietu konfigurācijas nepilnību topā ieņem *Open-cwmp*. CWMP ir pārvaldības protokols, kas tiek izmantots, lai nodrošinātu individuālu iekārtu, piemēram, maršrutētāju vai VoIP telefonu, pieslēgšanos pie telekomunikāciju pakalpojumu sniedzēja nodrošinātā tīkla (interneta). Lai šim pārvaldības rīkam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

Otrajā vietā ierindojas *Open-socks*. No publiskā interneta pieejamie SOCKS starpniekserveri ar nepietiekamu aizsardzību tiek pakļauti dažādu uzbrukumu riskam, piemēram, uzbrucēji var pārtvert caur šo serveri sūtīto informāciju.

Trešo vietu ieņem *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.

Pilnvērtīgākam kibersituācijas novērtējumam CERT.LV kopš 2020. gada izmanto *Apvienotās Karalistes Nacionālā kiberdrošības centra (NCSC)* izveidoto apdraudējumu matricu. Matricā ievietotie

Unikālo IP adrešu skaits – konfigurācijas nepilnības



5. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2022. gada 4. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

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.

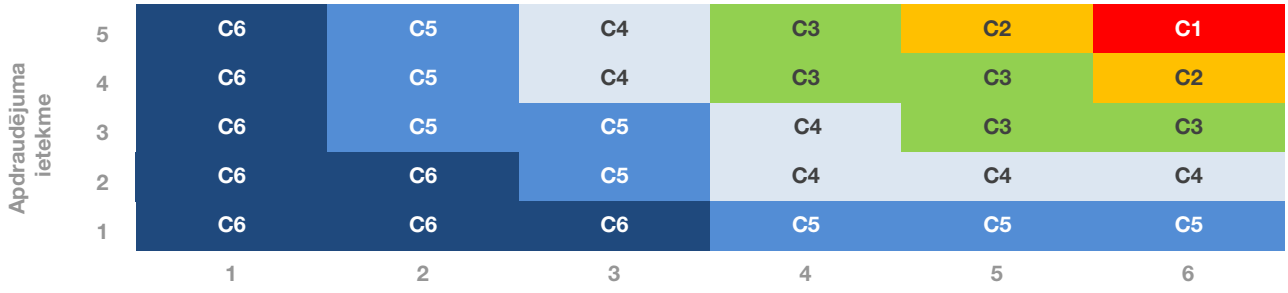
Gandrīz 98% apdraudējumu ietilpst maznozīmīgu apdraudējumu kopā (C6) un ir saistīti ar individuālu lietotāju iekārtām vai plaši izplatītiem ikdienišķiem, automatizētiem uzbrukumu mēģinājumiem uzņēmumiem vai valsts un pašvaldību iestādēm.

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

Nozīmīgi plašas ietekmes apdraudējumi (C3) veido 0,14% (503 unikālas apdraudētas IP adreses/gadījumi) no visiem kategorizētajiem apdraudējumiem. 90% šo apdraudējumu veido pakalpojuma pieejamības incidenti, 7% ļaundabīgs kods vairākās pašvaldībās, veselības aprūpes iestādēs un interneta pakalpojumu sniedzējos, bet 3% kompromitētas iekārtas un krāpšanas incidenti.

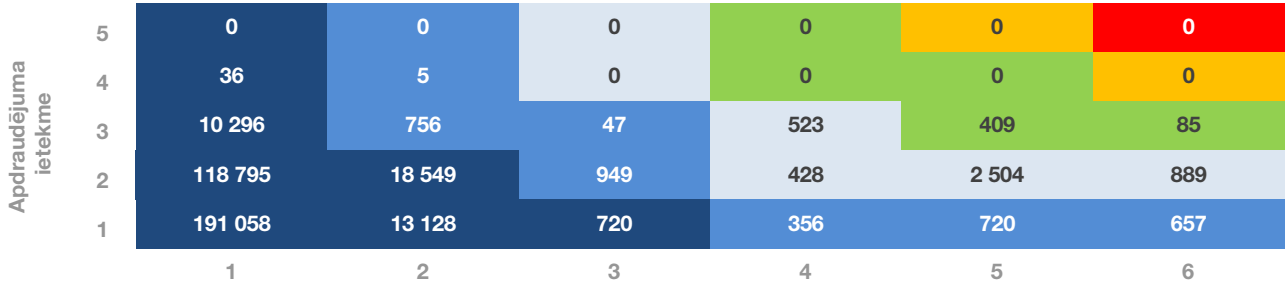
Lielākā daļa C4 līmeņa apdraudējumu (būtiski apdraudējumi ar vidēju ietekmi) jeb 47% bija pakalpojuma pieejamības incidenti augstas un vidēji augstas prioritātes iestādēs, 10% bija

Apdraudējumu matrica



6. attēls – Apdraudējumu matricas sadalījums kategorijās.

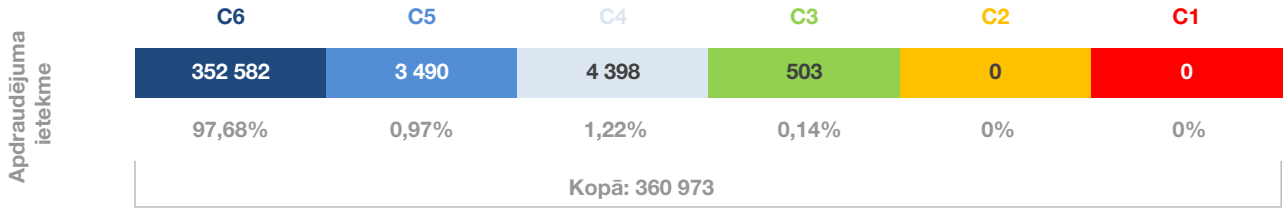
Apdraudēto unikālo IP adrešu izvietojums



7. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu izvietojums matricā 2022. gada 4. ceturksnī valsts un pašvaldību institūcijās.

konfigurācijas nepilnības (*Open-socks, Accessible-ftp, ssl-poodle* u.c.), bet 2% - ielaušanās mēģinājumi, ļaundabīgs kods, kompromitētas iekārtas un krāpšanas incidenti.

Lai sekmētu kopējo kiberdrošību valstī, CERT.LV sadarbībā ar NIC.LV ir izstrādājis DNS RPZ (*Domain Name Service Response Policy Zone*) jeb DNS ugunsmūri (*DNS firewall*). DNS mūris ik dienu tiek



8. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu sadalījums apdraudējumu kategorijās pēc apdraudējuma ietekmes (matrica) 2022. gada 4. ceturksnī.

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 tika novērota tendence vairākām pikšķerēšanas vietnēm izmantot vienu domēnu. Tas ļāva viegli identificēt šādus domēnus kā kaitīgus, taču nebija iespējams tos bloķēt, jo konkrētie domēni tika izmantoti arī daudzu leģitīmu vietņu uzturēšanai.

Šajā ceturksnī uzbrucēji uzdevās par banku pārstāvjiem un, sūtot e-pastus un veicot telefona zvanus, centās iegūt internetbanku piekļuves informāciju. Savukārt VAS "Latvijas Pasts" vārdā tika izplatītas krāpnieciskas īsziņas, ar kurām saņēmēji tika aicināti ievadīt maksājumu karšu datus viltus vietnē. Bankas karšu datus krāpnieki centās iegūt arī ar retāk pielietotu metodi, izplatot izdrukātas vēstules pa pastu. Maksājumu izkrāpšanas mēģinājumi tika veikti ar Valsts policijas vārdā izsūtītu e-pasta vēstuļu palīdzību. Krāpnieki nevilcinājās izmantot arī mūsdienu tehnoloģijas un viltot Valsts policijas telefona numuru, lai izkrāptu personīgu informāciju. Krāpnieki centās iegūt arī e-pastu piekļuves datus, uzdodoties par e-pasta pakalpojuma sniedzēju atbalsta dienestu.

Oktobrī īpaši aktīvi bija krāpnieki, kas ar viltus loteriju palīdzību centās izvilināt no iedzīvotājiem datus. Iegūtos vārdus un telefona numurus krāpnieki izmantoja, lai zvanītu iedzīvotājiem, uzdodoties par banku, un biedētu ar pretlikumīgām darbībām kontā, tādējādi cenšoties iegūt internetbankas piekļuves informāciju.

Ar viltus īsziņu starpniecību, uzdodoties par VAS "Latvijas Pasts", krāpnieki aicināja iedzīvotājus doties uz viltus vietni un ievadīt tajā maksājumu karšu datus, lai veiktu sūtījuma vai muitas nodokļa apmaksu. E-pasti tika sagatavoti labā latviešu valodā un izsūtīšanai tika izmatota e-pasta adrese, kas imitēja VAS "Latvijas Pasts" oficiālo e-pasta adresi.

Veselības ministrijas vārdā izsūtītajās viltus fiziskajās vēstulēs iedzīvotāji tika aicināti pieteikties kompensāciju izmaksai par vakcināciju pret Covid-19. Lai pieteiktos viltus kompensācijai, iedzīvotāji tika aicināti doties uz krāpnieku izveidotu vietni un ievadīt tajā savu maksājumu karšu datus.

Visa pārskata perioda garumā uzbrucēji Valsts policijas vārdā izplatīja viltus e-pasta vēstules, kurās saņēmējiem draudēja ar paraugprāvu par iesaisti bērnu pornogrāfijas apritē. Vēstulē tika piedāvāts izvairīties no tiesu darbiem, samaksājot sodu vairāku tūkstošu apmērā. Līdzīgas kampaņas tika novērotas arī citās Eiropas Savienības valstīs.

Savukārt viltojot Valsts policijas oficiālo telefona numuru, krāpnieki zvanīja Latvijas iedzīvotājiem un krievu valodā apgalvoja, ka kāds mēģina pieteikt kredītu zvana saņēmēja vārdā, un aicināja sniegt personīga rakstura informāciju, lai zvanītāja vārdiem "izvairītos no nepatikšanām".

Krāpnieki bez uzmanības neatstāja arī uzņēmumus un valsts iestādes. Vairāki grāmatveži saņēma e-pastu it kā vadītāja vārdā ar jautājumu par konta atlikumu un aicinājumu veikt maksājumu uz krāpnieku norādītu kontu. Tika saņemti arī četri incidentu pieteikumi, kuros uzņēmumi cieta no iejaukšanās biznesa sarakstē. Saņemot e-pastā rēķinu it kā no sadarbības partnera, uzņēmumi veica rēķina apmaksu uz uzbrucēju norādīto bankas kontu. Kopējais viltoto rēķinu radītais zaudējumu apjoms šajos incidentos pārsniedz 500 tūkstošu eiro.

2.2. Pakalpojuma pieejamība

Visa pārskata perioda laikā bija vērojami periodiski intensīvi DDoS uzbrukumi gan pret valsts pārvaldes iestādēm, gan kritiskās infrastruktūras uzņēmumiem, taču vairumā gadījumu tie neradīja ietekmi vai arī ietekme bija nebūtiska. Veiksmīgi sadarbojoties VAS "Latvijas Valsts radio un televīzijas centrs", SIA "Tet" un CERT.LV, valsts un kritiskās infrastruktūras IKT resursiem tiek nodrošināta augsta noturība pret DDoS uzbrukumiem. Biežākie uzbrucēju mērķi bija Tīmekļvietņu vienotā platforma (TVP), SIA "Tet" infrastruktūra, finanšu institūcijas un īslaicīgi arī enerģētikas sektors.

1.oktobrī, kad Latvijā notika 14. Saeimas vēlēšanas, tika konstatēti īslaicīgi pārtraukumi Centrālās vēlēšanu komisijas (CVK) sistēmu darbībā, taču tie nebija saistīti ar ārēju ietekmi. Vairāki traucējumi, kas nebija ilgāki par desmit minūtēm, elektroniskajā tiešsaistes vēlētāju reģistrā bija saistīti ar sistēmas drošības iestatījumu parametriem, kas, iecirkņu darbiniekiem aktīvi lietojot šo sistēmu, reaģēja kā DDoS uzbrukuma gadījumā – liedzot piekļuvi. Nepilnības sistēmas darbībā tika operatīvi novērstas.

30. novembrī, pēc ārlietu ministra E. Rinkēviča aicinājuma sniegt atbalstu Ukrainai, tika novēroti intensīvi DDoS uzbrukumi no Krieviju atbalstošo haktīvistu puses. Galvenie mērķi bija valsts iestādes un finanšu institūcijas. Lielākā daļa šo uzbrukumu tika veiksmīgi atvairīti. Tikai atsevišķos gadījumos bija novērojama īslaicīga resursu lēndarbība, taču visiem resursiem tika nodrošināta leģitīmu apmeklētāju piekļuve.

Nebūtiski pieejamības traucējumi tika konstatēti DDoS uzbrukuma laikā VAS "Latvijas dzelzceļš" tīmekļa vietnei, Dobeles pašvaldībai, Sabiedrisko pakalpojumu regulēšanas komisijai, Latvijas Bankai un CERT.LV. Vienā no uzbrukumiem uz 10 minūtēm pieejamība tika traucēta Tīmekļvietņu vienotajai platformai.

Vairākos gadījumos, lai nodrošinātu Latvijas iedzīvotāju piekļuvi valsts iestāžu un citiem būtiskiem resursiem, DDoS uzbrukumu ietekmes mazināšanai uz laiku tika izmantota ģeobloķēšana Baltijas valstu līmenī, kas ierobežoja piekļuvi uzbrukumu skartajiem resursiem tikai no Baltijas valstu IP adresēm.

2.3. Ļaundabīgs kods

Pārskata periodā tika saņemti ziņojumi galvenokārt par mēģinājumiem inficēt iekārtas, izmantojot ļaundabīgus e-pasta pielikumus. Šajās e-pasta vēstulēs saņēmēji tika aicināti veikt pielikumā norādīto preču piegādi, bet pielikums arhīva (.zip) formātā saturēja ļaunatūru. Tā tika paredzēta sensitīvas informācijas (lietotājvārdi, paroles u.tml.) ievākšanai.

Vismaz piecās izglītības iestādēs, kā arī vairāku uzņēmumu un valsts iestāžu tīklos tika konstatēta *RaspberryRobin* ļaunatūras klātbūtne. Minētais vīruss izplatās galvenokārt ar inficētu ārējo datu nesēju starpniecību, tādējādi īpaši apdraudot koplietošanas datorus, piemēram, lielajās mācību auditorijās. *RaspberryRobin* lielākoties apdraud iekārtas ar Windows operētājsistēmu un spēj izveidot sarežģītu un savstarpēji saistītu ļaunatūru ekosistēmu, lejupielādējot inficētajā iekārtā arī citas ļaunatūras. Ļaunatūra potenciāli tiek saistīta ar *Evil Corp* grupējumu, kas uztur saikni ar Krievijas valdību.

Tika reģistrēti arī vairāki *Gozi* vīrusa izplatīšanas gadījumi platformā *E-klase*. Vīruss tiek izmantots, lai iegūtu sensitīvu informāciju no inficētajiem datoriem, kā arī spēj sniegt uzbrucējam pilnu kontroli pār inficēto iekārtu.

No vairākiem uzņēmumiem tika saņemti ziņojumi par šifrējošā izspiedējvīrusa uzbrukumu. Vienā no gadījumiem uzņēmums spēja atjaunot darbību un datus, jo tam bija pieejamas datu rezerves kopijas. Citā gadījumā uzņēmuma datu rezerves kopijas tika veidotas, taču datu atjaunošana nebija iespējama, jo arī rezerves kopijas cieta uzbrukumā. Novecojuša, neatjaunināma programmnodrošinājuma izmantošana palielina risku uzņēmumam ciest šāda veida uzbrukumos.

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.

Oktobrī mērķētu pikšķerēšanas uzbrukumu piedzīvoja vairāki darbinieki no kādas ministrijas. Tie saņēma viltus e-pastu it kā no Polijas pārstāvniecības Eiropas Savienībā ar aicinājumu iepazīties ar Baltijas valstu nostāju attiecībā uz Krievijas agresiju. Uzbrukums, iespējams, veikts Krievijas atbalstītas kiberoperācijas *Gamaredon* ietvaros ar mērķi piekļūt sensitīvai informācijai. Ministrijas darbinieki kaitīgos e-pastus neatvēra.

2.5. Kompromitētas iekārtas un datu noplūdes

Tika fiksētas ar *Ngrok* programmatūras lietošanu saistītu aktivitāšu pazīmes kādā valsts uzņēmumā. Attiecīgā programmatūra tiek izmantota, lai nodrošinātu attālinātu piekļuvi infrastruktūrai. Lai arī leģitīma, šī programmatūra ir populāra kiberuzbrucēju vidū, jo sniedz iespējas piekļūt infrastruktūrai, neskatoties uz izmantotajiem aizsardzības pasākumiem. Incidenta izmeklēšanas procesā tika konstatēts, ka attiecīgās aktivitātes saistītas ar valsts uzņēmuma sadarbības partnera pārstāvja darbībām. Turpinās incidenta izmeklēšana.

Ar *Ngrok* izmantošanu saistītas aktivitātes fiksētas arī kādā valsts iestādē. Izpētē tika konstatēts, ka šīs aktivitātes saistāmas ar valsts iestādes pakļautībā esošas institūcijas IP adresi. *Ngrok* aktivitātes konstatētas arī vēl vismaz trīs citās organizācijās publiskajā sektorā. Tiek veikta incidentu izmeklēšana.

Tika saņemts ziņojums par aizdomīgām darbībām, kas tika veiktas no kādas pašvaldības IP adresēm. Incidenta izmeklēšanas rezultātā tika konstatēts, ka minētās pašvaldības tīmekļa vietne tikusi kompromitēta, un uzbrucēji to izmantoja, lai veiktu ievainojamību meklēšanu citos tīmekļa resursos. Uzturētāji tika informēti, apdraudējums tika novērsts.

Kādas reģionālās mācību iestādes tīmekļa vietnē tika ievietots kaitīgs saturs, kas pārvirzīja apmeklētājus uz pikšķerēšanas vietni. Uzbrucēji bija izmantojuši ievainojamības novecojušajā satura vadības sistēmā, kas tika izmantota vietnes uzturēšanai. Atbildīgie par vietnes uzturēšanu tika informēti, vietne tika atjaunināta, kaitīgais saturs dzēsts.

Telegram kanālos Krievijas agresīvo politiku atbalstošie haktīvisti publicēja informāciju par veiksmīgiem uzbrukumiem Latvijas tīmekļa resursiem, īstenojot arī datu noplūdi. Iepazīstoties ar pierādījumam publicētajiem dokumentiem, tika konstatēts, ka tie saturēja publisku informāciju un bija brīvi pieejami iestāžu mājaslapās.

1.decembrī savā Telegram kanālā haktīvistu grupējums Killnet publicēja informāciju par veiksmīgu uzbrukumu Valsts darba inspekcijai. Šī uzbrukuma rezultātā tika kompromitēta inspekcijas darbinieces e-pasta kastīte. Lai mazinātu incidenta ietekmi, darbinieces VPN un e-pasta piekļuve tika ierobežota. Par notikušo tika informēta arī Labklājības ministrija un Valsts sociālās apdrošināšanas aģentūra. Iestādē tika uzsākta draudu medību operācija. Izpētes darbs tiek turpināts.

2.6. Ievainojamības

Tika sagatavots brīdinājums *Fortinet* lietotājiem par kritisku ievainojamību (CVE-2022-40684), kas sniedza uzbrucējam iespēju veikt izmaiņas administratora panelī, neizmantojot administratora autentifikācijas validāciju. CERT.LV aicināja pārbaudīt žurnalēšanas pierakstus, lai pārliecinātos, ka iekārtas nav tikušas kompromitētas, kā arī uzstādīt atjauninājumus un ierobežot piekļuvi administrācijas panelim.

CERT.LV publicēja brīdinājumu par OpenSSL ievainojamībām (CVE-2022-3602 un CVE-2022-3786), aicinot pārbaudīt izmantotās sistēmas, vai tajās netiek lietota OpenSSL 3.0.x bibliotēka, un sekot OpenSSL publicētajām rekomendācijām.

SPNEGO drošības mehānisma ievainojamība (CVE-2022-37958) sniedza uzbrucējam iespēju,

neautentificējoties veikt attālinātu koda izpildi. CERT.LV aicina pārskatīt Microsoft drošības ieteikumus un uzstādīt nepieciešamos atjauninājumus.

Tika atklāta jauna kritiska Microsoft Exchange ievainojamība, kas sniedza uzbrucējiem iespēju, apvienojot 2022. gada laikā atklātās ievainojamības CVE-2022-41080 un CVE-2022-4108, padarīt Microsoft ieteikto risinājumu ProxyNotShell ievainojamības ietekmes mazināšanai par neefektīvu un veikt attālinātu koda izpildi. CERT.LV aicināja uzstādīt atjauninājumus un sekot Microsoft ieteikumiem.

Tika konstatēts, ka publiski pieejamā valsts iestādes tīmekļa resursā ir iespējota atkļūdošana, kas atklāj sensitīvu informāciju. Uzturētājs tika informēts un aicināts nomainīt visus piekļuves datus, kā arī pārbaudīt, vai nav notikušas nesankcionētas pieslēgšanās resursam.

Kādā valsts iestādes vietnē bija iespējams XML XEE injekcijas uzbrukums, kura rezultātā uzbrucējs varētu izgūt datus un potenciāli veikt arī attālinātu koda izpildi. Uzturētājs tika informēts, apdraudējums tika novērsts.

2.7. Atbildīga ievainojamību atklāšana

Pārskata periodā tika saņemti daži maznozīmīgi ziņojumi.

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

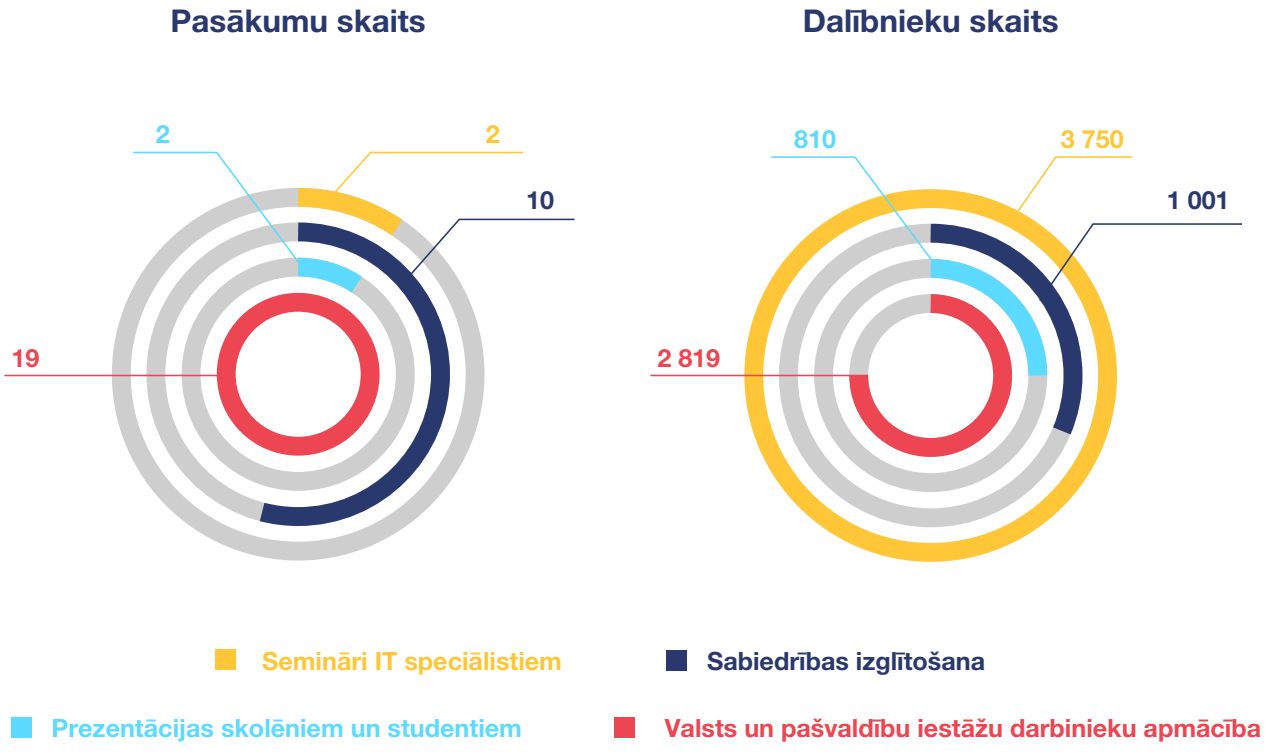
Oktobrī jau desmito gadu tika atzīmēts Eiropas Kiberdrošības mēnesis. Iniciatīvas mērķis ir veicināt Eiropas Savienības (ES) iedzīvotāju un uzņēmumu izpratni par kiberdrošību, sniedzot informāciju par aktuālākajām kiberaizsardzības metodēm. Šogad īpaša uzmanība tika pievērsta tieši pikšķerēšanas un šifrējošo vīrusu uzbrukumiem. Šo tēmu labākai izpratnei Aizsardzības ministrija sadarbībā ar CERT.LV, Valsts policiju un Kiberaizsardzības vienību oktobra ietvaros publicēja 4 izglītojoši informatīvus video, kuros nozares eksperti izklāstīja uzbrukumu būtību, biežāk sastopamās ļaundaru viltības un ieteikumus, kā sevi pasargāt.

Video:

- "Kas ir pikšķerēšana?" https://www.youtube.com/watch?v=leiy14qgClM&t=2s
- "Kas ir vikšķerēšana?" https://www.youtube.com/watch?v=S4p2MKjp2UE
- "Kas ir smikšķerēšana?" https://www.youtube.com/watch?v=JrJF7mzl9iE&t=1s
- "Kas ir izspiedējvīrusi?" https://www.youtube.com/watch?v=23yyZRG_ds8&t=1s

4.-5. oktobrī notika starptautiskā IT drošības konference *Kiberšahs 2022*, kuru organizēja CERT.LV sadarbībā ar Latvijas Interneta asociāciju, Aizsardzības ministriju, SIA Latvijas Mobilais Telefons, SIA WeAreDots (dots.), SIA Tet, SIA Cyber Circle, CybExer Technologies OU un CTF Tech. Konference norisinājās divās paralēlsesijās: Kiberšaha sesija tika veltīta stratēģiski politiskiem kiberdrošības jautājumiem Latvijā un Eiropā, savukārt Kiberšoka tehniskā sesija sniedza dalībniekiem iespēju padziļināti sekot līdzi daudz tehniskāku kiberdrošības jautājumu izpētei un praktiskām demonstrācijām. (https://cert.lv/lv/2022/09/konferences-kibersahs-2022-tiesraide)

Izglītojošo pasākumu un apmācīto cilvēku skaits



9. attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2022. gada 4. ceturksnī

Jau trešo gadu paralēli konferencei norisinājās arī tiešsaistes kiberdrošības sacensības *Capture The Flag* (CTF). Dalībniekiem 30 stundu laikā bija operatīvi jāspēj atrisināt 28 dažādus tehniskos uzdevumus, kas saistīti ar viedajām tehnoloģijām, sākot ar "viedo māju" un līdz pat "viedajai gaisa telpai". Sacensībās piedalījās 36 komandas gan no Latvijas, gan citām Eiropas valstīm, taču goda pjedestālu dalīja Latvijas pārstāvji.

Konferenci klātienē vēroja gandrīz 300 kiberdrošības ekspertu, bet pasākuma tiešraide piesaistīja vairāk nekā 3000 skatītāju no vismaz 30 pasaules valstīm.

6. oktobrī CERT.LV piedalījās studentu un jauno profesionāļu biznesa iespēju festivālā *Icebreakers'22*, kur diskutēja par kiberincidentiem un riskiem, kas saistīti ar datu drošību. (https://www.youtube.com/watch?v=JUrrreRv7-E).

26. oktobrī CERT.LV piedalījās SIA *Tet* organizētajā digitālās drošības forumā *CyberShield*, sniedzot prezentāciju *Has cyber security landscape changed since Russian aggression – report from trenches* un piedaloties paneļdiskusijā par nākotnes kiberapdraudējumiem *Cyber attack vectors-2023: thinking of the future.* (https://www.youtube.com/watch?v=ORSB0Qf3TNk).

14. decembrī tika organizēts IT drošības seminārs *Esi drošs*, kurā tika aplūkotas kiberdrošības aktualitātes gada griezumā, darbinieku apmācības, efektīva ielaušanās testu veikšana, rīcība kiberkrīzes situācijā un DNS RPZ izmantošana. Semināra tiešraidei sekoja 450 skatītāji. (https://cert.lv/lv/2022/11/it-drosibas-seminars-esi-dross-decembri).

15. decembrī CERT.LV sadarbībā ar NIC.LV sniedza prezentāciju *Kā uzņēmējiem viegli (ne) pazaudēt naudu kibertelpā?* Limbažu novada Uzņēmēju forumā, stāstot par riskiem un biežāk pieļautajām kļūdām attiecībā uz kiberdrošību.

CERT.LV pārstāvji piedalījās arī divu raidierakstu tapšanā. Viens no raidierakstiem tika izveidots sadarbībā ar Sargs.lv un tika veltīts atskatam uz gada notikumiem Latvijas kibertelpā (https://www.sargs.lv/lv/podkasti/2022-12-21/podkasts-ka-mainijusies-latvijas-kiberdrosibas-vide-kops-krievijas-iebrukuma), bet otrs tapa Riga Security Forum 2022 ietvaros, un aplūkoja drošu datu savienojamību nākotnes 5G/6G tīklos (https://open.spotify.com/episode/1xaLLGXt37TPHHJEbPpZWN).

Pārskata periodā CERT.LV par IT drošību izglītoja 8380 cilvēkus, iesaistoties 33 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 un 14. Saeimas vēlēšanu dienā. 1. oktobrī CERT.LV pastiprināti sekoja notikumiem kibertelpā. Būtiski incidenti netika novēroti. Dalība darba grupas sanāksmē pēc vēlēšanām, lai apkopotu un pārrunātu vēlēšanu laikā identificētos trūkumus un sagatavotu rekomendācijas procesu uzlabošanai.
- Dalība visaptverošas valsts aizsardzības ieviešanas uzraudzības un koordinācijas darba grupas sakaru un komunikācijas nodrošinājuma apakšgrupas sanāksmēs, savas kompetences ietvaros, izvērtējot grupā apstrādājamos dokumentus - sakaru nozares krīzes plānu, u.c.
- CERT.LV piedalījās vairākās sanāksmēs ar Aizsardzības ministriju, kurās pārrunāja *Latvijas Kiberdrošības stratēģijas 2023.-2026. gadam* prioritāros virzienus un uzdevumus.
- Oktobrī notika tikšanās ar Aizsardzības ministriju, Vides aizsardzības un reģionālās attīstības ministriju un Finanšu nozares asociāciju par eID līdzekļu izmantošanu, lai veiktu drošu autentifikāciju e-pakalpojuma izmantošanai.
- Dalība vairākās sanāksmēs, kurās ar Satiksmes ministriju, Finanšu nozares asociāciju (FNA), telekomunikāciju operatoriem / elektronisko sakaru komersantiem, Valsts policiju, Sabiedrisko pakalpojumu regulēšanas komisiju un Finanšu kapitāla un tirgus komisiju tika pārrunātas iespējas izmantot CERT.LV un NIC.LV izveidoto un uzturēto DNS RPZ un tika pārrunāti Elektronisko sakaru likumā veicamie grozījumi. Sanāksmes mērķis bija izskatīt iespējas apkarot krāpšanas, kas saistītas ar banku sektora klientiem. Aplūkotas tika telefonkrāpniecības, investīciju krāpšanas un citas krāpnieciskas aktivitātes internetā.

- Novembrī notika tikšanās ar Aizsardzības ministriju, Finanšu ministriju, Finanšu nozares asociāciju un Latvijas Banku par iespējām izslēgt finanšu sektoru no Nacionālā kiberdrošības likuma tvēruma, lai novērstu normatīvajos aktos iekļauto prasību dublēšanos vai pretrunas. Finanšu institūcijām būs piemērojami Eiropas Parlamenta un Padomes regula par finanšu sektora digitālās darbības noturību (DORA regula) nosacījumi par informācijas un komunikācijas tehnoloģiju risku pārvaldības pasākumiem, ar IKT saistītu incidentu pārvaldību un IKT saistītu incidentu paziņošanu, kā arī digitālās darbības noturības testēšanu u.c.

- Sadarbībā ar Aizsardzības ministriju tika sniegti komentāri Vides aizsardzības un reģionālās attīstības ministrijas sagatavotajam MK noteikumu projektam *Informācijas sistēmu vispārējās tehniskās prasības*.

- 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. 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 pilnveidota platformas dokumentācija un uzsākta platformas testēšana.

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 pārstāvis darbojas kā šīs darba grupas līdzpriekšsēdētājs.
  - *Maturity* darba grupā, kura rūpējas par ES dalībvalstu CSIRT komandu brieduma līmeņa paaugstināšanu.
- 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.

- CERT.LV piedalījās vairākās sanāksmēs, kas saistītas ar Eiropas kiberdrošības platformas *MeliCERTes* projekta noslēgumu, sniedzot atgriezenisko saiti par platformas izmantošanu un piedaloties diskusijās par projekta tālākas attīstības iespējām.
- Dalība ENISA Eiropas kiberdrošības indeksa (*EU Cybersecurity index*) darba grupā, kurā tiek izstrādāta kiberdrošības indeksa vērtības aprēķina metodoloģija dalībvalstu kiberdrošības novērtēšanai. Pārskata periodā ENISA tika iesniegta anketa *Launch of pilot data gathering phase via EU Survey*. CERT.LV pārstāvis piedalījas ENISA *Cybersecurity index* platformas testēšanā un rekomendāciju sagatavošanā par nepieciešamajiem uzlabojumiem.
- Dalība ENISA vadītajā darba grupā *Coordinated Vulnerability Disclosure (CVD) Task Force*, kurā norit darbs pie ES līmeņa koordinētas ievainojamību atklāšanas politikas vadlīniju veidošanas.
- Dalība Eiropas Komisijas EHDS (*European Health Data Space*) regulas darba grupā. Regulas mērķis ir veicināt pacientu elektronisko datu pieejamību un iesaistīto pušu sadarbību Eiropas līmenī. Darba grupa izvērtēja regulas saikni ar Mākslīgā intelekta aktu, Datu pārvaldības aktu un Vispārīgo datu aizsardzības regulu..
- Turpinājās dalība enerģētikas informācijas apmaiņas un sadarbības grupā *Energy ISAC Camelot*, lai veicinātu informācijas apmaiņu un sekmētu enerģētikas sektora kiberdrošību.
- Aizsardzības ministrijai tika iesniegti komentāri par Latvijas pozīciju ziņojumam par ES Kibernoturības aktu (*Cyber Resilience Act*), ar kura palīdzību, definējot kiberdrošības prasības iekārtām un programmnodrošinājumam, tiek pausti centieni aizpildīt robus Eiropas esošajā kiberdrošības regulējumā.
- Oktobrī notika tikšanās ar ENISA vadību Rīgā, lai pārrunātu turpmāko sadarbību.
- Oktobrī notika tikšanās ar META pārstāvjiem, lai pārrunātu sadarbības un incidentu atklāšanas un risināšanas procedūru uzlabošanas iespējas.

- Oktobrī notika tikšanās ar ASV vēstniecības pārstāvjiem, lai pārrunātu sadarbību kiberdrošības veicināšanā.
- Oktobra beigās CERT.LV uzņēma Moldovas delegāciju, lai iepazīstinātu ar CERT.LV darbību un dalītos pieredzē par nacionālās kibervides stiprināšanu.
- No 28. novembra līdz 2. decembrim CERT.LV pārstāvji piedalījās NATO ACT (*Allied Command Transformation*) kiberdrošības mācībās *Cyber Coalition 22.* Mācību mērķis bija stiprināt partneru spējas aizsargāt savu infrastruktūru, kā arī veicināt sadarbību.
- Decembra sākumā notika dalība NATO CCDCoE (*Cooperative Cyber Defence Centre of Excellence*) kiberdrošības mācībās *Crossed Swords 2022*, kas norisinājās Tallinā, Igaunijā. *Crossed Swords* ir tehniskās sarkano komandu mācības, kurās šogad tika eksperimentēts ar ofensīvo kiberoperāciju integrēšanu modernā karadarbībā ar mērķi pilnveidot sadarbību. Mācības apvienoja 120 dalībniekus no 24 valstīm.
- Gatavošanās dalībai NATO CCDCoE 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 4.ceturksnī CERT.LV turpināja darbu pie *Grafoskopa* izstrādes, tā attīstīšanas un pilnveidošanas, papildinot rīku ar jaunām funkcijām un uzlabojot esošās. Pārskata periodā CERT.LV piedalījās attālinātās JTAN projekta sanāksmēs, kurās projekta partneri informēja par saviem projekta uzdevumiem un rezultātiem. Daži no partneriem prezentēja arī jaunus rīkus un funkcionalitātes. Attiecībā uz JTAN projekta iepirkumu progress pagaidām ir diezgan lēns cilvēkresursu trūkuma dēļ, ko radījusi globālā situācija un ar to saistītie incidenti Latvijas kibertelpā.

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

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

7. Citi normatīvajos aktos noteiktie pienākumi

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

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

  Pārskata perioda laikā lietotāji tika pasargāti 75 309 reizes. Daži no nozīmīgākajām aktīvās aizsardzības epizodēm (bloķētās vietnes):

  - Viltus investīcijas, kuras piedāvā telefonkrāpnieki: 3599;
  - Investīciju tīmekļa vietnes, kurās tiek izmantota Latvijas simbolika: 7818;
  - Viltus loterijas un ar krāpšanu saistītas vietnes: 1672;
  - Viltus banku vietnes datu izkrāpšanai: 410;
  - VAS “Latvijas Pasts” vārdā izplatīti krāpnieciski mēģinājumi iegūt maksājumu karšu datus: 183.

  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. CERT.LV pārstāvis FESA (ES/EEZ eIDAS uzraudzības iestāžu federācija) gadskārtējā rudens sesijā 5.-6. oktobrī sniedza pārskatu par DDUK aktualitātēm uzticamības pakalpojumu sniedzēju uzraudzībā, kā arī par to, ka pārskata periodā nav notikuši incidenti, kas skar uzticamības pakalpojumu sniedzējus vai arī to sniegtos uzticamības pakalpojumus. Notika Latvijas uzticamības saraksta (LV TSL) informācijas atjaunošana.

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 01.10.2022. līdz 31.12.2022. ir saņēmusi un izvērtējusi 433 ziņojumus. No tiem 220 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 11 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 21 ziņojumā konstatēta personas goda un cieņas aizskaršana, 5 ziņojumi saņemti par naida runu. Par finanšu krāpšanas mēģinājumiem internetā saņemti 66 ziņojumi, 45 ziņojumu saturs nav bijis pretlikumīgs, 65 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 43 ziņojumi par naida runu un bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 174 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 220 ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem 218 ziņojumi ir dzēsti no publiskas aprites un 2 ziņojumu saturs atrodas dzēšanas procesā sadarbībā ar Valsts policiju un interneta pakalpojumu sniedzējiem.

2023. gada 11. janvārī.

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, 2023

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija