Latvijas universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

2022 C1

Publiskais pārskats par CERT.LV uzdevumu izpildi

2022. gada 1. ceturksnis (01.01.2022. – 31.03.2022.)

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

Jau kopš janvāra vidus Latvijas kibertelpā bija jūtama paaugstināta aktivitāte, kas būtiski pieauga līdz ar kara sākumu Ukrainā. Kopumā situācija ir stabila. Sekmīgi uzbrukumi valsts un kritiskās infrastruktūras sektorā ir notikuši, bet līdz šim nav radījuši būtisku tūlītēju ietekmi un sekas. Taču tas var mainīties ilgtermiņā, jo pastāv iespēja, ka vidēs, kuras tika pakļautas incidentiem, var tikt veiktas destruktīvas darbības, iespējams, ir noplūduši dati un autentifikācijas līdzekļi, kā arī uzbrucēji var censties realizēt iestādes vai uzņēmuma tēla graušanas aktivitātes. Jāatzīmē, ka gandrīz visi iespējamie apdraudējumi, izņemot tēla graušanu, ir novēršami, ja incidentam pakļautās iestādes ievieš IT drošības pasākumus, kā to paredz Ministru kabineta noteikumi nr. 442 *Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām*.

Pārskata periodā tika reģistrētas 117 079 unikālas apdraudētas IP adreses, kas ir par 4% mazāk nekā iepriekšējā ceturksnī un par 18% mazāk nekā šajā pašā periodā pirms gada. Izplatītākie apdraudējumi:

- konfigurācijas nepilnības (65 996 unikālas IP adreses) ar kritumu par 3% pret iepriekšējo periodu;
- ļaundabīgs kods (8 907 unikālas IP adreses) ar kritumu par 22%;
- informācijas vākšana (1 439 unikālas IP adreses) ar kritumu par 13%.

Lai arī kopējā informācijas vākšanai pakļauto IP adrešu apjomā bija vērojams kritums, septiņas reizes audzis informācijas vākšanai pakļauto IP adrešu skaits vidēji augstas un augstas prioritātes iestādēs, salīdzinot ar iepriekšējo pārskata periodu. Būtiski pieauga arī kopējā incidentu apstrādes

intensitāte, saņemto ziņojumu skaitam palielinoties par 23% un nozīmīgu plašas ietekmes apdraudējumu (kategorija C3) apjomam palielinoties par 78%.

Kopš kara sākuma būtiski augusi uzbrukumu intensitāte pret Latvijas valsts iestādēm un kritiskās infrastruktūras uzņēmumiem. Būtiski pieaudzis nelielu pakalpojumu atteices uzbrukumu skaits, kā arī tīklu skenēšana – programmatūras versiju un ievainojamību meklēšana. Jāņem gan vērā, ka uzbrucēju galvenais fokuss ir vērsts pret Ukrainu, bet Latvijas kibertelpā lielā daļā gadījumu veiktas aktivitātes, lai iegūtu informāciju par vieglāk kompromitējamiem mērķiem, kā arī radītu tīklā "troksni" uzmanības novēršanai, lai fonā realizētu plānotu uzbrukumu pret jau izpētītu mērķi ar augstu kompromitēšanas iespējamību.

Līdzšinējie kiberuzbrukumi ir bijuši veiksmīgi, galvenokārt, gadījumos, kad mērķa iestāde nav pienācīgi rūpējusies par savu IKT infrastruktūru un ignorējusi labās prakses principus. Novēroti tikai atsevišķi kiberuzbrukumi, kuru izpildījums vērtējams kā tehniski sarežģīts.

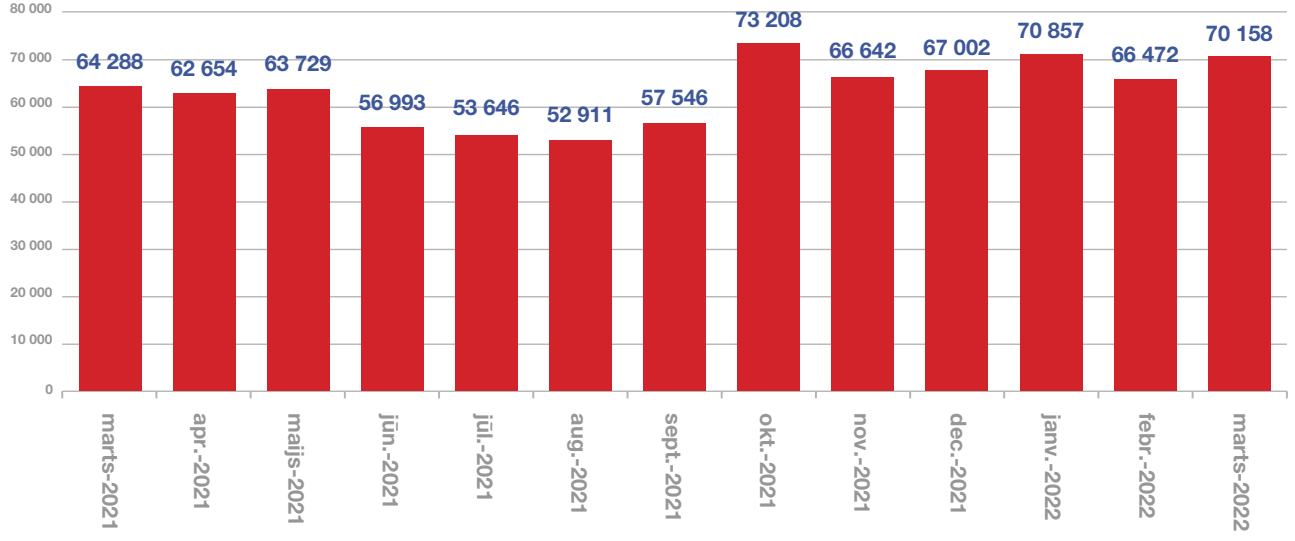
Ņemot vērā, ka kiberuzbrukumi ir plaši pielietojami pret dažādiem mērķiem, pret Ukrainu vērsts uzbrukums ar nezināmu (0-day) ievainojamību plaši izplatītā programmatūrā var tikt izmantots arī pret mērķiem Latvijā, tāpēc svarīga ir apdraudējumu informācijas apmaiņa gan ar Ukrainas kolēģiem, gan visiem sabiedrotajiem. CERT.LV aktīvi piedalās informācijas apmaiņā ar uzticamu starptautisko sabiedroto kopienu gan sniedzot, gan saņemot informāciju, kā arī nodrošina aktuālās informācijas apriti vietējo ekspertu kopienā.

Pārskata periodā CERT.LV par IT drošību izglītoja 4 797 cilvēkus, iesaistoties 41 izglītojošā pasākumā.

1. Elektroniskās informācijas telpā notiekošo darbību atainojums

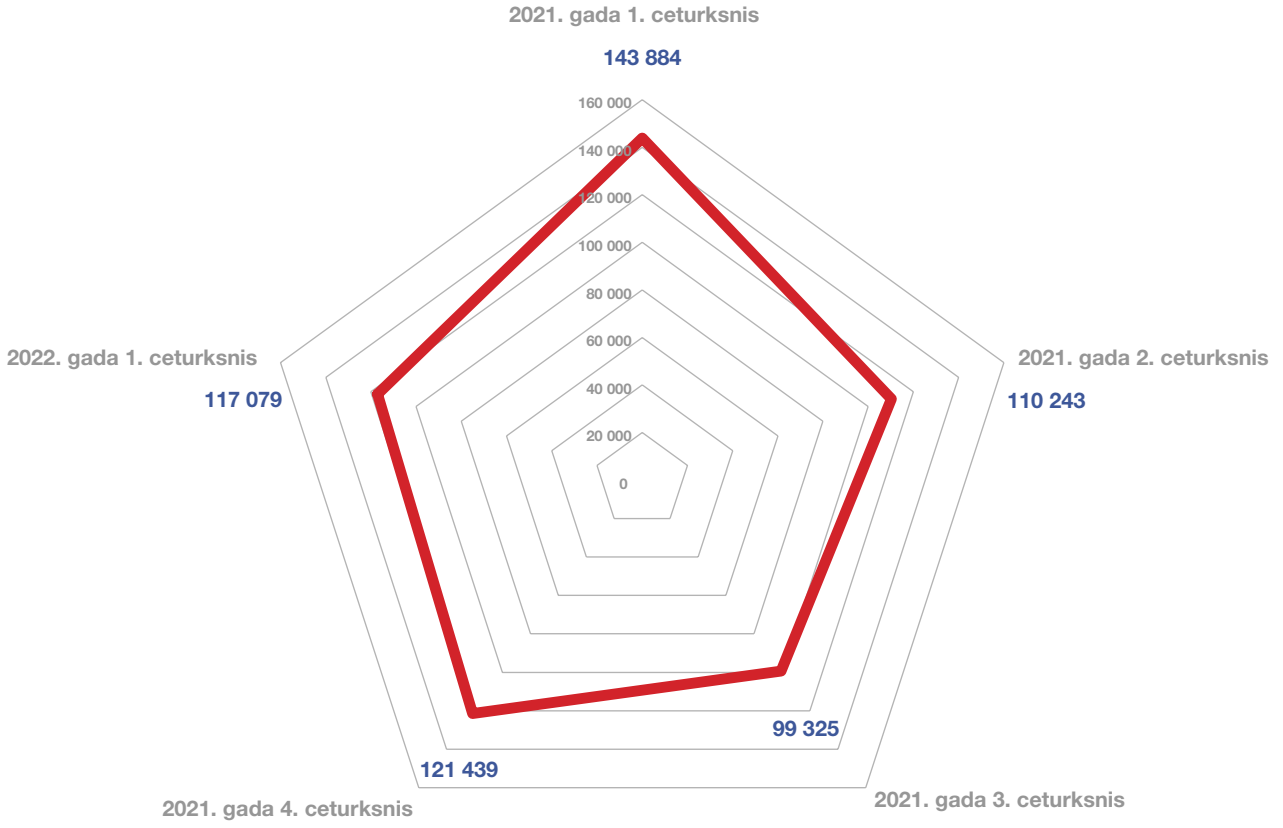
Ik mēnesi CERT.LV apkopo informāciju par apdraudētajām Latvijas IP adresēm. Lai sniegtu pilnvērtīgāku Latvijas kibertelpas pārskatu un nodrošinātu datu starptautisku salīdzināmību, CERT.LV apdraudējumu uzskaitei izmanto starptautiski lietotu incidentu taksonomiju (eCSIRT.net projekta izveidotā taksonomija, 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 tos pa apdraudējumu veidiem (piemēram, ļaunatūra, ielaušanās, krāpšana), kā arī pa ļaunatūru (piemēram, *Confiker*, *Zeus*, *Mirai*) un konfigurācijas nepilnību (piemēram, *Opendns*, *Openrdp*) tipiem.

Apdraudējumu sadalījums pa mēnešiem



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

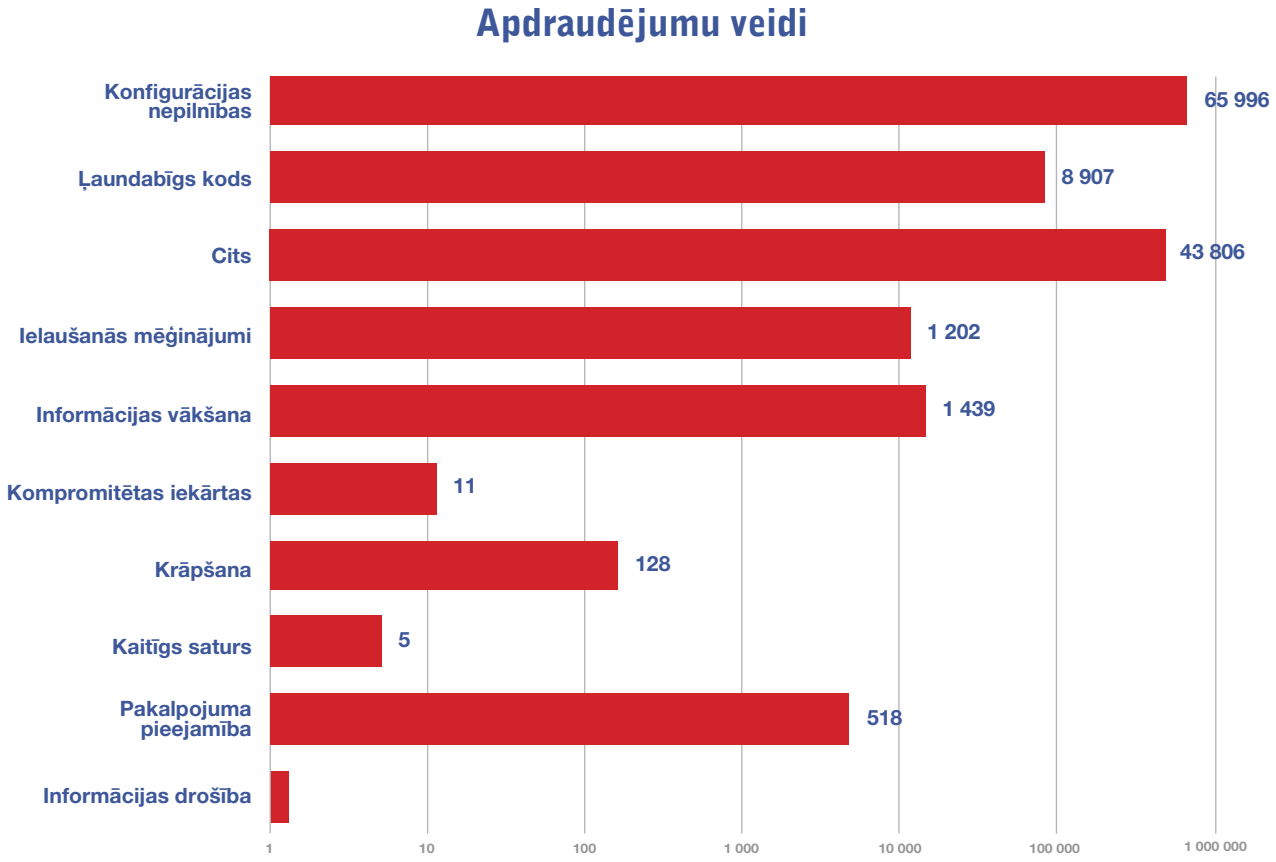
Apdraudējumu sadalījums pa ceturkšņiem



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

CERT.LV pārskata periodā ik mēnesi apkopoja informāciju vidēji par 68 000 ievainojamu unikālu IP adrešu.

2022. gada 1. ceturksnī tika reģistrētas 117 079 unikālas apdraudētas IP adreses, kas ir par 4% mazāk nekā iepriekšējā ceturksnī un par 18% mazāk nekā šajā pašā periodā pirms gada. Lai arī kopējā apdraudēto IP adrešu apjomā bija vērojams kritums, būtiski pieauga incidentu apstrādes

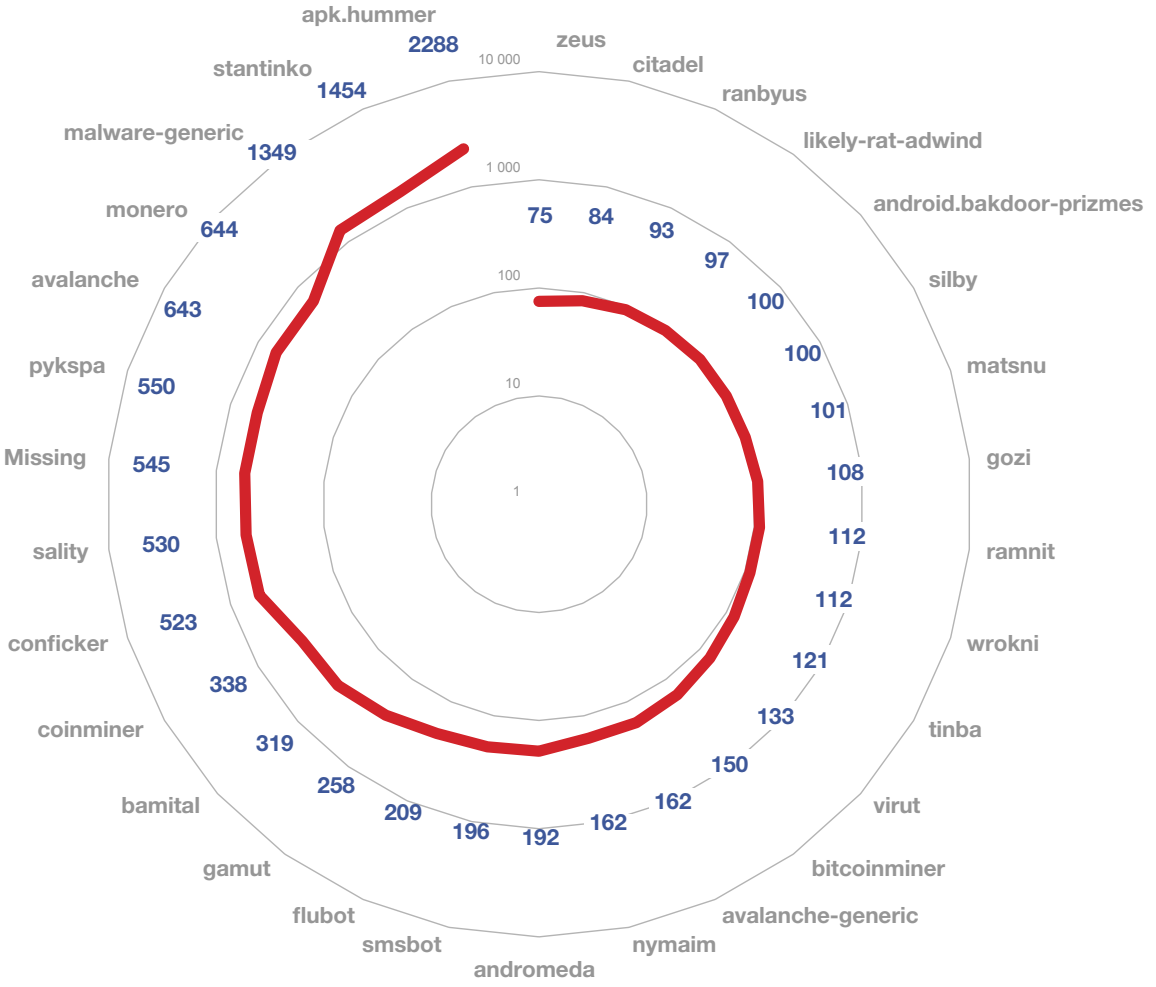


3. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2022. gada 1. ceturksnī pa apdraudējumu veidiem.

intensitāte, saņemto ziņojumu skaitam palielinoties par 23% salīdzinājumā ar šo pašu periodu pirms gada, bet nozīmīgu plašas ietekmes apdraudējumu (kategorija C3) apjomam palielinoties par 78%.

Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (65 996 unikālas IP adreses) ar kritumu par 3% pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs kods (8 907 unikālas IP adreses) ar kritumu par 22%, bet trešais – informācijas vākšana (1 439 unikālas IP adreses)

Unikālo IP adrešu skaits – ļaundabīgs kods



4. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2022. gada 1. ceturksnī ar apdraudējuma veidu – ļaundabīgs kods.

ar kritumu par 13%. Lai arī kopējā informācijas vākšanai pakļauto IP adrešu apjomā bija vērojams kritums, septiņkāršojies informācijas vākšanai pakļauto IP adrešu skaits vidēji augstas un augstas prioritātes iestādēs, salīdzinot ar iepriekšējo pārskata periodu.

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 saglabā 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.

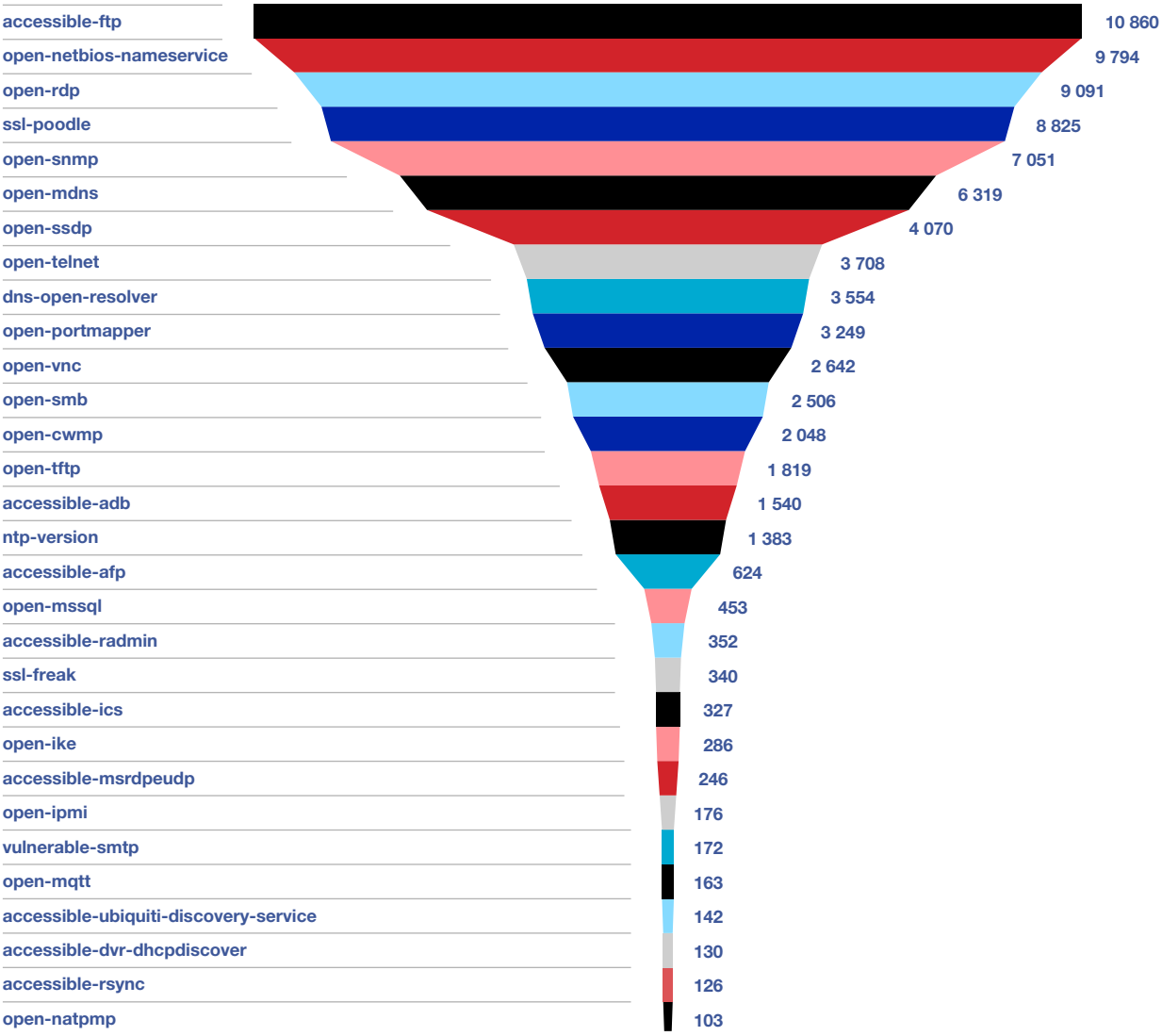
Trešo vietu ieņem *Monero*. Ļaunatūra veic kriptovalūtas *Monero* (uz privātumu orientēta kriptovalūta, kas ieguvusi popularitāti kriminālajās aprindās) ieguvi, izmantojot iekārtas resursus, lietotājam to nezinot. Nesaudzīgi izmantojot iekārtas jaudu, var bīstami noslogot iekārtu vai pat to neatgriezeniski sabojāt.

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

Otro vietu ieņem *Open NetBIOS Nameservices*. Lietojumprogrammas izmanto *NetBIOS* saziņai lokālajā tīklā, attiecīgi pieejas atvēršana no interneta nav lietderīga. Padarot *NetBIOS* pieejamu no interneta, to iespējams izmantot DDoS uzbrukumu veikšanai pret trešajām pusēm, kā arī tas sniedz papildu informāciju uzbrucējiem par serveri vai tīklu, kas ļauj labāk sagatavoties tālākiem uzbrukumiem.

Trešajā vietā atrodas *OpenRDP*. RDP ir attālās piekļuves risinājums, kas bieži tiek izmantots arī uzbrukumos. Ja netiek ievērota labā prakse un netiek ierobežota piekļuve RDP servisam, piemēram, ierobežojot IP adreses, kurām atļauts pieslēgties, vai nosakot piekļuvi caur VPN,

Unikālo IP adrešu skaits – konfigurācijas nepilnības



5. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2022. gada 1. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

uzbrucējs var pārņemt kontroli pār neatbilstoši konfigurētām iekārtām, kurās attālinātās piekļuves porti ir brīvi atvērti uz internetu un nav uzstādīta pietiekami droša piekļuves parole.

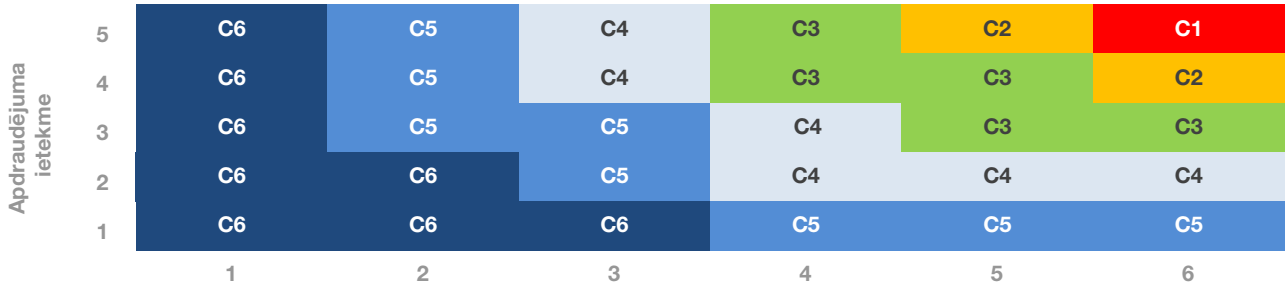
Pilnvērtīgākam kibersituācijas novērtējumam CERT.LV 2020. gadā ir uzsākusi *Apvienotās Karalistes Nacionālā kiberdrošības centra (NCSC)* izveidotās apdraudējumu matricas lietošanu. Matricā ievietotie apdraudējumi tiek grupēti pēc tā, cik nozīmīga ir skartā iestāde vai uzņēmums un/vai cik plašu sabiedrības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

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

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

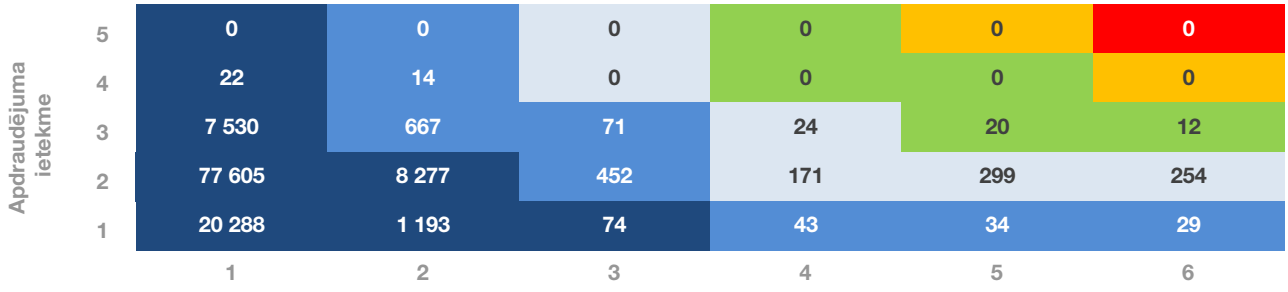
Nacionāla līmeņa apdraudējumi (C1) un augstas nozīmes apdraudējumi (C2) pārskata periodā nav reģistrēti. Nozīmīgi plašas ietekmes apdraudējumi (C3) veido 0,03% (32 unikālas apdraudētas IP adreses/gadījumi) no visiem kategorizētajiem apdraudējumiem. 84% šo apdraudējumu veido ļaundabīgs kods (*Android.Hummer, Tinba, Monero* u.c.), bet 9% informācijas vākšanas uzbrukumi jeb skenēšana, lai ievāktu informāciju par izmantotajām iekārtām un potenciālajām ievainojamībām.

Apdraudējumu matrica



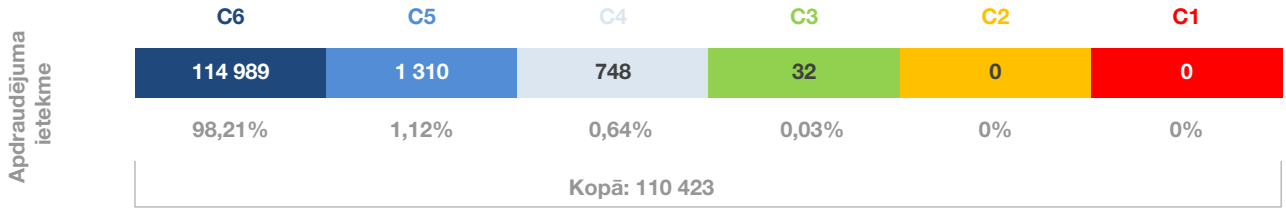
6. attēls – Apdraudējumu matricas sadalījums kategorijās.

Apdraudēto unikālo IP adrešu izvietojums



7. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu izvietojums matricā 2022. gada 1. ceturksnī valsts un pašvaldību institūcijās.

Lielākā daļa C4 līmeņa apdraudējumu (būtiski apdraudējumi ar vidēju ietekmi) bija konfigurācijas nepilnības (*Accessible-ftp*, *NTP-Version, SSL-Poodle*, u.c.), pakalpojuma atteices (DDoS) uzbrukumi, kā arī ielaušanās un pikšķerēšanas mēģinājumi, kas novēroti augstas un vidēji augstas prioritātes iestādēs – virknē valsts iestāžu, kā arī vairākās pašvaldībās un augstākās izglītības iestādēs.



8. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu sadalījums apdraudējumu kategorijās pēc apdraudējuma ietekmes (matrica) 2022. gada 1. ceturksnī.

CERT.LV būtiskākie proaktīvās rīcības pasākumi apdraudējumu mazināšanai:

- tika palielināta publiskā sektora aizsardzība, gan veicinot informācijas apmaiņu un izmantojot jaunus komunikācijas kanālus, gan iestādēs izmantojot CERT.LV un NIC uzturēto DNS ugunsmūri;
- tika organizēti ārkārtas informatīvie semināri par aktuālajiem apdraudējumiem kibertelpā;
- sadarbībā ar Aizsardzības ministriju iestādēm/uzņēmumiem tika izplatīts pārbaudes saraksts, kurā apkopoti kontroljautājumi par kiberdrošību paaugstinošām izpildāmajām darbībām;
- veikta regulāra informācijas apmaiņa par aktuālajiem apdraudējumu indikatoriem gan ar Latvijas, gan starptautisko ekspertu kopienu.

Lai mazinātu kopējo apdraudēto IP adrešu skaitu valstī, CERT.LV kopā ar Latvijas Interneta asociācijas (LIA) Net-Safe Latvija Drošāka interneta centru ir izveidojuši iniciatīvu *Atbildīgs interneta pakalpojumu sniedzējs*, kuras ietvaros tiek parakstīts saprašanās memorands ar ieinteresētajiem interneta pakalpojumu sniedzējiem (IPS), lai tie varētu informēt savus klientus

par viņu iekārtās konstatētajiem apdraudējumiem. Atbildīgo IPS skaits līdz pārskata perioda beigām saglabājās bez izmaiņām – 13.

Iniciatīvas *Atbildīgs interneta pakalpojumu sniedzējs* ietvaros ar interneta pakalpojumu sniedzēju starpniecību lietotājiem tiek nosūtīta ne tikai informācija par apdraudējumiem, kas konstatēti viņu lietotajās iekārtās, bet arī rekomendācijas šo apdraudējumu novēršanai (pieejamas arī angļu valodā).

2. Atbalsts informācijas tehnoloģiju drošības incidentu novēršanā vai to novēršanas 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

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.

Krāpnieki centās iegūt, galvenokārt, iedzīvotāju maksājumu karšu datus, kā arī internetbankas, e-pasta un sociālo tīklu piekļuves informāciju. Krāpniecībās tika izmantoti loģistikas kompāniju (DHL, DPD u.c.) kā arī VAS *Latvijas pasts* zīmoli, lai pārliecinātu krāpnieciskās ziņas saņēmēju ievadīt maksājumu kartes datus krāpnieku norādītajā vietnē samaksas saņemšanai par pārdotu preci vai sūtījuma piegādes apmaksai.

Krāpnieki uzdevās arī par dažādām Latvijā populārām bankām un banku vārdā izsūtīja krāpnieciskus e-pastus un īsziņas, aicinot iedzīvotājus ievadīt internetbankas piekļuves datus viltus vietnēs. Dažās no šīm krāpniecībām tika pamanīta inovatīva pieeja krāpniecisko vietņu izveidē – iedzīvotāju uzticības veicināšanai tika izmantoti latviskoti domēna vārdi ar mīkstajiem un garajiem burtiem, piemēram, manabanka-drošība.com.

Sociālo tīklu kontu lietotājvārdu un paroļu iegūšanai krāpnieki sociālajos tīklos izplatīja intriģējošas vai biedējošas viltus ziņas (daļa bija saistītas ar karu Ukrainā), kuru izvērstai aplūkošanai lietotāji tika aicināti "autorizēties", ievadot savu piekļuves informāciju viltus vietnēs. E-pastu un sociālo tīklu kontu aizsardzībai CERT.LV aicināja iedzīvotājus izmantot vairāku faktoru autentifikāciju, kas apgrūtinātu kontu pārņemšanu, pat ja uzbrucējs uzzinātu paroli.

9. februārī tika saņemta informācija par plašu krāpnieciskas ziņas izplatību lietotnē *Signal*. It kā *Signal* vārdā tika paziņots par laimestu, kura iegūšanai ziņojuma saņēmēji tika aicināti ievadīt maksājuma kartes datus krāpnieciskā vietnē. Ticamības palielināšanai vietnē tika simulēta komentāru sadaļa ar atsauksmēm no lietotājiem, kas jau saņēmuši laimestus. CERT.LV saņemtajos incidenta pieteikumos *Signal* ziņas tika sūtīta no numuriem ar valsts kodu "+7" (*Countries Sharing +7 country code*: Abkhazia, Kazakhstan, Russia), izmantotie pilsētu/ mobilo operatoru kodi norādīja uz Krievijas mobilo operatoru *BeeLine*. CERT.LV aicināja, saņemot negaidītus paziņojumus īsziņās vai mobilajās lietotnēs (*Whatsapp, Signal, Telegram* u.c.), kas satur saiti, un, iespējams, steidzina uz rīcību, saiti vaļā nevērt un savus datus nevadīt, par šādiem sūtījumiem informēt CERT.LV, kā arī bloķēt sūtītāju.

Dienu pēc Krievijas iebrukuma Ukrainā, vairāku iestāžu darbinieki Latvijā saņēma krāpnieciskus e-pastus angļu valodā, kuros tika aicināti izteikt atbalstu kādai no militārajā konfliktā iesaistītajām pusēm – Ukrainai vai Krievijai. Atbalsta paušanai ziņas saņēmēji tika aicināti balsot, ievadot maksājuma karšu datus krāpnieku izveidotā vietnē un pērkot balsis. CERT.LV rīcībā nav informācijas par to, vai kāds no e-pasta adresātiem ievadīja savus datus šajā vietnē, bet institūcija saņēma ziņojumus par vairāk nekā 150 šādiem e-pastiem. Iedzīvotāji tika aicināti būt modri, jo šādās krīzes situācijās darbojas krāpnieki, kas ir gatavi izmantot cilvēku vēlmi palīdzēt.

Martā tika novērota apjomīga pikšķerēšanas kampaņa, kas tika vērsta pret valsts un pašvaldību iestāžu darbiniekiem un valsts kapitālsabiedrībām. Krāpnieku mērķis bija izvilināt e-pasta kontu lietotājvārdus un paroles. CERT.LV ir saņēmusi informāciju par vairāk nekā 5 000 šādu e-pastu. Uzbrukumā tika izmantota kompromitēta Argentīnas valsts iestādes e-pasta kastīte, un nereti datu izkrāpšanai izveidotās viltus vietnes tika pielāgotas e-pasta saņēmēja izmantotajam e-pasta pakalpojumam, kā rezultātā konstatēti arī atsevišķi veiksmīgi uzbrukumi. Aktuālās situācijas kontekstā CERT.LV aicināja iestādes, kurās krāpnieciskos e-pastus neapturēja mēstuļu filtri un tie nonāca līdz darbiniekiem, veikt darbinieku e-pasta paroļu nomaiņu, kā arī uzstādīt vairāku faktoru autentifikāciju (2FA, MFA), ja tas vēl nav izdarīts.

Tika konstatēti aktīvi mērķēti uzbrukumi, izsūtot pikšķerēšanas e-pastus vairākiem publiskā sektora darbiniekiem, lai iegūtu informāciju par iestādēs izmantotajām iekārtām un programmatūru. Uzbrukumi bija nesekmīgi.

2.2. Pakalpojuma pieejamība

Būtiski pieauga uzbrukumu intensitāte pret Latvijas valsts iestādēm un kritiskās infrastruktūras uzņēmumiem. Intensīvi piekļuves atteices uzbrukumi (DDoS) tika vērsti pret finanšu institūcijām un vairāku valsts iestāžu tīmekļa vietnēm, atsevišķos gadījumos izraisot īslaicīgus vietņu darbības traucējumus, taču būtisku ietekmi neradot. DDoS uzbrukumus piedzīvoja arī atsevišķi mediji Latvijā un mediju kompānijas citās Eiropas valstīs, kas liecina par koordinētu uzbrucēju aktivitāti, taču pagaidām vairāk ar mērķi novērst uzmanību un *radīt troksni*.

17. janvārī tika konstatēts mēģinājums mērķtiecīgi pārslogot Centrālās laboratorijas informācijas tehnoloģiju (IT) sistēmas, kas radīja īslaicīgus piekļuves traucējumus mājaslapas informācijai un pieraksta iespējām tīmekļa vietnē, vēstīja laboratorijas pārstāvji. Uzbrukuma rezultātā veidojās pārslodze zvanu centrā. Uzbrukumu gan izdevās operatīvi novērst, un pēc laboratorijas sniegtās informācijas lietotāju dati netika skarti.

24. februārī, vienlaicīgi ar Krievijas iebrukumu Ukrainā, tika konstatēti Viasat uzturētā satelīta interneta pakalpojuma KA-SAT darbības traucējumi, kas vairāk nekā 10 000 klientiem dažādās Eiropas valstīs, tostarp arī Ukrainā, pārtrauca sakarus. Uzbrucēji iekļuva tīklā, izmantoja aizmirstu un ar vāju autentifikāciju aizsargātu VPN kontu, un kompromitēja satelīta sakaru klientu gala iekārtu atjaunināšanas servisu, izsūtot ļaundabīgu atjauninājumu un gala iekārtas padarot neizmantojamas. Latvijā skarts viens privātā sektora klients. CERT.LV aicina rūpīgi uzraudzīt izmantojamo infrastruktūru un rūpēties par atbilstošiem drošības pasākumiem (https://cert.lv/lv/2022/02/cert-lv-ieteikumi-saasinoties-geopolitiskajai-situacijai-eiropa-un-pieaugot-kiberdraudiem).

24. februārī līdzīgā laika nogrieznī tika novēroti darbības traucējumi gan SIA *Tet* digitālās TV, gan SIA *Bite Latvija* GO3 digitālās TV pakalpojumu darbībā, īslaicīgi apgrūtinot pakalpojuma saņemšanu vairākiem desmitiem tūkstošu klientu. Abi pakalpojumu sniedzēji spēja atjaunot pakalpojumu pieejamību 1-2 stundu laikā. Incidents, iespējams, vērtējams kā atbilde uz vairāku Krievijas televīzijas kanālu apraides aizliegšanu Latvijā, kaut arī Tet incidenta izmeklēšana ārēju iejaukšanos neapstiprināja.

Martā CERT.LV vērsa iedzīvotāju un uzņēmumu uzmanību uz nepieciešamību rast alternatīvus risinājumus tādu produktu un pakalpojumu izmantošanai, kuri saistīti ar Krieviju vai tās propogandas ruporiem, piemēram, mail.ru, vkontakte.ru vai 1C grāmatvedības programmatūrai. Sankcijas pret Krieviju un atsevišķām ar to saistītām personām var atstāt ietekmi uz šo kompāniju pakalpojumu pieejamību, kā arī šīs kompānijas apzināti vai neapzināti var tikt izmantotas kiberuzbrukumu veikšanai. Ja pāreja uz alternatīvu pakalpojumu nav iespējama, CERT.LV aicināja izvērtēt potenciālos riskus un veikt to ietekmes mazināšanas pasākumus, lai novērstu iespējamos piegādes ķēdes uzbrukumus un citus apdraudējumus. Pārskata periodā CERT.LV arī vairākkārtēji saņēma jautājumus no valsts iestādēm par *Kaspersky* izmantošanas drošību un aicināja iestādes meklēt alternatīvus risinājumus, ņemot vērā Latvijas valsts drošības iestāžu ieteikumus.

2.3. Ļaundabīgs kods

Masveidā tika saņemti ziņojumi par ļaundabīgu e-pastu vilni, kurā krāpnieki izlikās par uzņēmuma *Baltic Express LV* pārstāvi. E-pasta saņēmējs tika aicināts pārbaudīt pielikumā pievienotos piegādes dokumentus. E-pasta pielikums saturēja *LokiBot* vīrusu, kas paredzēts sensitīvas informācijas ievākšanai.

Marta noslēgumā tika novērotas divas apjomīgas ļaunatūras izplatīšanas kampaņas, kas tika vērstas pret Latvijas iedzīvotājiem. Vienā no kampaņām par ļaunatūras izplatīšanas platformu uzbrucēji izvēlējās plaši lietoto risinājumu *E-klase*. Izmantojot *E-klase* pasta sūtījumā iekļautu saiti vai pielikumu, tika izplatīts *Gozi* vīruss, kas, nonākot datorā, uzbrucējiem nosūtīja datorā izmantotos lietotājvārdus un paroles, kā arī sniedza uzbrucējiem pilnu kontroli pār iekārtu. Uzbrukumu grūti atpazīstamu padarīja tas, ka ļaundabīgo sūtījumu upuri saņēma no pazīstamiem sūtītājiem, kuru datori bija inficēti, kā arī ziņojums bija tematiski atbilstošs un sagatavots labā latviešu valodā. CERT.LV rīcībā esošā informācija liecina, ka inficētos sūtījumus saņēmuši vismaz 15 000 *E-klase* lietotāju. CERT.LV sadarbībā ar E-klasi veica incidenta izpēti.

Otra ļaunatūras izplatīšanas kampaņa tika vērsta pret uzņēmumiem, galvenokārt, enerģētikas sektorā. Ar saiti vai pielikumu e-pastos tika izplatīta *Qakbot* (*Qbot*) ļaunatūra, kas paredzēta paroļu un citas sensitīvas informācijas ievākšanai no inficētās iekārtas. Lai pārliecinātu e-pasta saņēmējus atvērt kaitīgo saiti un lejupielādēt vīrusu saturošo dokumentu, tika norādīts, ka saite satur informāciju par izmaiņām normatīvajā regulējumā un it kā ved uz likumi.lv. Viens no saņēmējiem ļaundabīgo sūtījumu atvēra, inficējot savu iekārtu. CERT.LV veica incidenta analīzi un sniedza rekomendācijas.

2.4. Ielaušanās mēģinājumi

Būtiski augusi uzbrukumu intensitāte pret Latvijas valsts iestādēm un kritiskās infrastruktūras uzņēmumiem. Novērota aktīva tīklu skenēšana – programmatūras versiju un ievainojamību meklēšana – gan finanšu sektorā, gan valsts pārvaldē. Aktivitātēm, kas vērstas pret finanšu sektoru, indikatori sakrīt ar Ukrainā ziņotajiem un ir novēroti visās Baltijas valstīs. Valsts iestādes un kritiskās infrastruktūras turētāji tika aicināti atļaut piekļuvi savām infrastruktūrām tikai no Latvijas IP adresēm. Papildu aizsardzības nodrošināšanai iestāžu un pakalpojumu sniedzēju infrastruktūrā tika uzstādīti CERT.LV sensori un DNS ugunsmūris. CERT.LV redzeslokā nonākušie uzbrukumi neradīja būtiskus apdraudējumus finanšu sektoram. CERT.LV uztur aktīvu un produktīvu sadarbību ar finanšu sektoru.

Februāra sākumā tika novēroti aktīvi mērķēti uzbrukumi vairākām valsts iestādēm. Līdzīgi uzbrukumi notikuši arī citās Eiropas valstīs. Saņemta informācija par veiksmīgiem uzbrukumiem citās ES valstīs. Valsts iestāžu darbiniekiem tika sūtītas e-pasta vēstules no kompromitētiem ārvalstu kolēģu e-pasta kontiem. Sūtījumi saturēja it kā paziņojumu par izmaiņām darba laikos un kaitīgu HTML pielikumu. Visā uzbrukuma realizēšanas ķēdē izmantoti tikai leģitīmi domēni (domēni uzturēja tādus servisus kā *Jira, Confluence* u.tml.), kas padarīja sarežģītu apdraudējumā iesaistīto vietņu bloķēšanu. Uzbrukuma mērķis – iekļūt infrastruktūrā un ievākt informāciju.

Marta sākumā virkne valsts iestāžu resursu piedzīvoja uzbrukumu mēģinājumus ar paroļu minēšanu un centieniem veikt koda injekcijas, taču visi šie uzbrukumu mēģinājumi tika veiksmīgi atvairīti.

Pastiprināta ievainojamību meklēšana un *taustīšanās* tika novērota arī privātajā sektorā. Aktīviem uzbrukumu mēģinājumiem tika pakļauti privātā sektora uzņēmumi, kas sniedz ar IT saistītus pakalpojumus. Tāpēc CERT.LV aicināja ražotājus un pakalpojumu sniedzējus cītīgi sekot līdzi atjauninājumiem, lai novērstu iespējamus piegāžu ķēžu uzbrukumus.

Kādā valsts iestādē pēc DNS ugunsmūra uzstādīšanas tika konstatēti un novērsti uzbrucēju mēģinājumi kompromitēt darbinieku tīklu.

2.5. Kompromitētas iekārtas un datu noplūdes

Tika konstatēta uzbrucēju klātbūtne kādā IT produktu izstrādes uzņēmuma tīklā. Uzņēmuma produktus izmanto klienti dažādos sektoros. CERT.LV uzskata, ka uzņēmums nav primārais mērķis, bet tiek izmantots kā līdzeklis, lai iekļūt klientu infrastruktūrā vai nu ar atjauninājumu starpniecību, vai arī izmantojot tīkla savienojumus uz klientu iekštīkliem, kas izveidoti izstrādāto risinājumu apkalpošanai. CERT.LV sniedza uzņēmumam atbalstu incidenta analīzē un rekomendācijas IT drošības pilnveidošanai.

Tika konstatētas uzbrucēja pazīmes kāda uzņēmuma iekšējā tīklā. Incidentu izraisīja kompromitēts serveris, kas uzņēmuma infrastruktūrā tika uzturēts nesankcionēti un ilglaicīgi netika pamanīts. CERT.LV novērojumi liecina, ka daudzās iestādēs un uzņēmumos netiek veikta pienācīga tīkla uzraudzība, lai savlaicīgi konstatētu nesankcionētu iekārtu klātbūtni, kā arī attālinātajai piekļuvei tiek izmantoti nedroši risinājumi. CERT.LV vairākkārt ir nācies konstatēt arī gadījumus, kad tīkla uzraudzības sistēmu iegāde un uzstādīšana ir veikta, bet darbam ar tām nav paredzēts kompetents personāls un nav izstrādātas atbilstošas rīcības procedūras.

Februārī notika veiksmīgs šifrējošās ļaunatūras uzbrukums, kura rezultātā kādā valsts iestādē tika kompromitētas vairākas iekārtas. Sekmīga uzbrukuma iemesli ir drošības prasību un labās prakses neievērošana, kas noveda arī pie apgrūtinātas incidenta izmeklēšsnas. Laicīgi izpildot CERT.LV rekomendācijas un Ministru kabineta noteikumus par kārtību, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām, incidents nebūtu noticis un ievērojami uzlabotos sistēmas noturība pret darbības traucējumiem un datu drošība. Iestāde nebija arī informējusi CERT.LV par uzbrukumā iesaistītās publiskās IP adreses saistību ar iestādes tīklu, kas būtu ļāvis saņemt CERT.LV rīcībā esošo informāciju par konstatētajām nepilnībām un apdraudējumiem, ļaujot laicīgi novērst incidentu. CERT.LV iesniedza iestādei incidenta pārskatu un rekomendācijas incidenta ietekmes novēršanai un IT drošības situācijas uzlabošanai.

Tika saņemta informācija par vairākām kompromitētām pašvaldību tīmekļa vietnēm. Uzbrucēji izmantoja vietnes nesankcionētai reklāmu demonstrēšanai vai ļaunatūras izplatīšanai, piemēram,

cenšoties pārliecināt apmeklētājus lejupielādēt savās iekārtās *Android* ļaunatūru *FluBot*, kas paredzēta sensitīvas informācijas iegūšanai, SMS izsūtnei un zvanu veikšanai no iekārtas bez lietotāja iesaistes. Vienā no gadījumiem tika konstatēts, ka vietnē izmantotās tehnoloģijas ir būtiski novecojušas un drošības līmenis neatbilst labajai praksei, tāpēc pašvaldība pieņēma lēmumu vietni slēgt. Pārējos gadījumos kaitīgais saturs no vietnēm tika dzēsts un drošības nepilnības novērstas.

Tika kompromitēta kādas valsts iestādes tīmekļa vietne. Uzbrukuma rezultātā vietnē tika nesankcionēti ievietota/ mainīta informācija. Sekmīga uzbrukuma iemesls bija IT drošības pasākumu neatbilstība labajai praksei (novecojusi, neatjaunināta sistēma u.tml.), kā arī trūka atbilstoša kontrole pār izmantojamajiem resursiem un atbildību sadalījumu. Žurnalēšanas pierakstu neesamība būtiski apgrūtināja incidenta analīzi.

2.6. Ievainojamības

Janvāra sākumā nepilnības *Microsoft Exchange Server 2016* un *Exchange Server 2019* programmnodrošinājumā izraisīja traucējumus e-pastu piegādē. Problēma neradīja drošības riskus, lai arī bija saistīta ar nepilnībām komponentē, kas veic pārbaudes ļaundabīga satura atklāšanai sūtītajos ziņojumos. Tika saņemta informācija par vairākām valsts iestādēm, kuras bija skārusi konkrētā nepilnība.

7. februārī CERT.LV izsūtīja brīdinājuma e-pastus valsts un pašvaldību iestāžu par IT drošību atbildīgajām personām, kā arī KI, PPS un DPS pārstāvjiem par kritiskām ievainojamībām *CISCO Small Business RV* sērijas maršrutētājos un VPN vārtejās, aicinot pēc iespējas ātrāk uzstādīt atjauninājumus. Kritiskākā no ievainojamībām – CVE-2022-20699 (CVSS 10.0) – ļāva uzbrucējiem attālināti bez autentifikācijas veikt koda izpildi SSL VPN vārtejas iekārtā.

9. martā CERT.LV publicēja brīdinājumu un izsūtīja brīdinājuma e-pastus par jaunu *Linux* ievainojamību, dēvētu arī par *Dirty Pipe* (CVE-2022-0847; 7.8/10), kuru iespējams viegli izmantot, lai arī nepriviliģēts lietotājs iegūtu pilnas *root* tiesības. Ievainojamība ļāva nepriviliģētam lietotājam

ievadīt un pārrakstīt datus arī tikai lasāmos (*read-only*) failos. CERT.LV aicināja nekavējoties uzstādīt atjauninājumus.

CERT.LV tīmekļa vietnē tika publicēti arī brīdinājumi par *PolKit* ievainojamību (CVE-2021-4034), kas ļāva uzbrucējiem iegūt *root* tiesības *Linux* distributīvos, un par *Microsoft* publicēto 71 labojumu, tostarp arī svarīgai *Windows SMBv3* (*Server Message Block*) protokola ievainojamībai (CVE-2022-24508; 8.8/10), kas sniedza iespēju uzbrucējam veikt attālināto koda izpildi.

2.7. Atbildīga ievainojamību atklāšana

Tika saņemts ziņojums par SQL injekcijas ievainojamību kādas organizācijas mājaslapā. Ievainojamība sniegtu uzbrucējam iespēju piekļūt vietnes datubāzei. Vietnes uzturētāji tika informēti, ievainojamība tika operatīvi novērsta.

Tika saņemts arī ziņojums par ievainojamībām, kas ļāva piekļūt nepubliskai informācijai vairākās valsts iestāžu tīmekļa vietnēs. Tika uzsākta ievainojamo resursu uzturētāju informēšana.

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

Cita veida sadarbība ar dažādām iestādēm ir norādīta atskaites 7. un 12.punktā.

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

No 21. līdz 25. martam Latvijā norisinājās ikgadējā informatīvi izglītojošā kampaņa *Digitālā nedēļa 2022*. Dažādos pasākumu formātos uzņēmumi un iedzīvotāji tika aicināti attīstīt digitālās prasmes biznesam un nodarbinātībai, aktīvāk izmantot tehnoloģijas un pakalpojumus, vienlaikus pievēršot uzmanību digitālajai identitātei, drošībai un kritiskajai domāšanai. 24. marts bija veltīts kritiskās domāšanas attīstībai un drošībai kibertelpā. Šīs dienas centrālais pasākums bija CERT.LV organizētais IT drošības seminārs *Esi drošs*, kurā tika aplūkotas tādas tēmas kā kiberdrošības aktualitātes ģeopolitiskā saspīlējuma apstākļos, valsts un pašvaldību vietņu ievainojamību ziņošana, piegāžu ķēžu uzbrukumi. Tāpat tika prezentēts CERT.LV pētījums par iedzīvotāju paradumiem internetā. Pasākumu tiešsaistē vēroja vairāk nekā 1 000 dalībnieki.

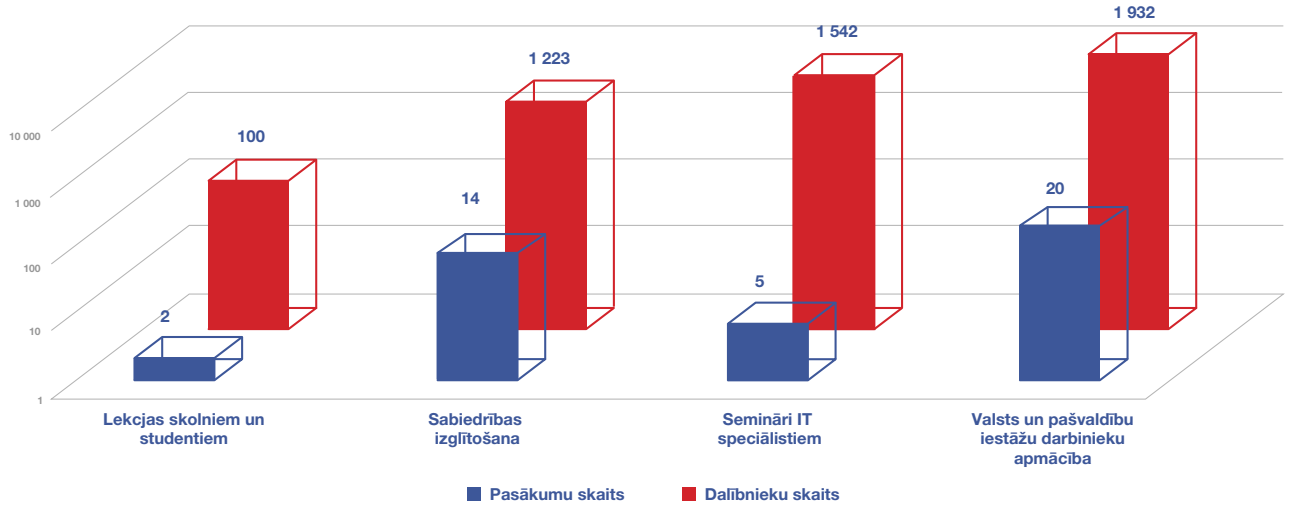
19. janvārī CERT.LV piedalījās *Rīgas Tehniskās universitātes* organizētajā *(IE)SPĒJA: medijpratība* vieslekcijā, stāstot studentiem par to, kas ir kiberdrošība, kāpēc tas ir svarīgs aspekts valsts kopējā drošībā, kādi mēdz būt kiberapdraudējumi un kādas ir CERT.LV funkcijas.

22. februārī krīžu un konsultāciju centra *Skalbes* rīkotajā seminārā par atbalsta iespējām noziedzīgos nodarījumos cietušajiem, kas notika *Eiropas dienas cietušajiem 2022* ietvaros, CERT.LV sniedza prezentāciju par kiberincidentiem, to veidiem un izpausmēm, kā arī rīcību kiberincidenta gadījumā (https://www.facebook.com/events/699581394537929).

Februāra beigās un marta sākumā CERT.LV sadarbībā ar Aizsardzības ministriju organizēja informatīvos seminārus par aktuālo situāciju un apdraudējumiem kibertelpā.

8. martā, atsaucoties Ārlietu ministrijas un Aizsardzības ministrijas aicinājumam, CERT.LV organizēja tiešsaistes informatīvo semināru Ukrainas krīzē atbalstu sniedzošām nevalstiskajām organizācijām, aplūkojot dažādus kiberdrošības aspektus.

Izglītojošo pasākumu un apmācīto cilvēku skaits



9. attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2022. gada 1. ceturksnī

9. martā CERT.LV sadarbībā ar Latvijas Informācijas un komunikācijas tehnoloģijas asociāciju (LIKTA) organizēja semināru LIKTA un Latvijas atvērto tehnoloģiju asociācijas (LATA) biedriem, kurā sniedza informāciju par aktuālajiem apdraudējumiem Latvijas kibertelpā.

29. martā CERT.LV eksperts piedalījās Finanšu un kapitāla tirgus komisijas organizētā diskusijā, kuras mērķis bija pievērst Latvijas finanšu sektora iestāžu vadības, IS drošības vadītāju un auditoru uzmanību sektora kiberdrošības riskiem un to pārvaldībai, jo līdz ar pieaugošo finanšu sektora atkarību no informācijas tehnoloģijām, pieaug arī riski un kibernegadījumu ietekme uz nozari.

Pārskata periodā CERT.LV par IT drošību izglītoja 4 797 cilvēkus, iesaistoties 41 izglītojošā pasākumā.

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

Sadarbības tikšanās, konsultācijas un prezentācijas:

- Savas kompetences ietvaros CERT.LV pēc Aizsardzības ministrijas pārstāvju lūgma piedalījās valsts informācijas sistēmu attīstības projektu pieteikumu novērtēšanā pēc Ministru kabineta 2021. gada 31. augusta noteikumos Nr. 597 *Valsts informācijas sistēmu attīstības projektu uzraudzības kārtība* ietvertajām prasībām, kas skar plānotās aktivitātes IKT drošības jautājumus.
- CERT.LV pārrunāja ar Aizsardzības ministriju potenciālo MK noteikumu nr. 442 *Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām* nākotnes struktūru, kā arī pilnveidošanai un papildināšanai nepieciešamo.
- CERT.LV turpināja piedalīties Aizsardzības ministrijas veidotajā darba grupā ar mērķi izstrādāt MK noteikumus Elektronisko sakaru likuma 8. panta 1. un 2. daļām par elektronisko sakaru tīklu drošību un tās uzraudzību.
- CERT.LV sadarbībā ar Aizsardzības ministriju sagatavoja un iesniedza Vides aizsardzības un reģionālās attīstības ministrijai (VARAM) rekomendācijas veicamajiem grozījumiem MK noteikumos nr. 421 *Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības*, lai izvairītos no drošības prasību dublēšanās, kas jau ir iekļautas *Informācijas tehnoloģiju drošības likumā* un MK noteikumos nr. 442 *Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībā,* aicinot MK noteikumus nr. 421 fokusēt uz datu centru fiziskās drošības un pieejamības prasībām, kā arī sertifikācijas un atbilstības jautājumiem.
- CERT.LV turpināja projekta par valkājamo ierīču drošību norises vadību.

- Dalība darba grupā, kuras uzdevums ir sadarbībā ar elektronisko sakaru komersantiem un Centrālo statistikas pārvaldi veikt Ministru kabineta noteikumu pilnveidošanu mobilo operatoru klientu datu apkopošanai oficiālās statistikas vajadzībām.
- Balstoties uz Ministru kabineta apstiprināto Aizsardzības ministrijas izstrādāto informatīvo ziņojumu, kas paredz valsts pārvaldē ieviest vienotu procesu, kādā ikviens iedzīvotājs var ziņot par ievainojamībām valsts un pašvaldību uzturētās informācijas sistēmās, CERT.LV uzsāka darbu pie koordinētas ievainojamību atklāšanas ziņojumu reģistrēšanas platformas izstrādes, procesa apraksta izveides un ziņošanas vadlīniju sagatavošanas.

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 trijās 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.
  - *TOR Review* darba grupā, kas pārskata CERTu tīkla statūtus un nolikumu, atbilstoši tos aktualizējot.

- CERT.LV vadītāja Baiba Kaškina turpināja darbu kā *FIRST Membership Committee* (Jauno biedru uzņemšanas komitejas) līdzpriekšsēdētāja (*co-chair*), piedaloties jauno biedru pieteikumu izskatīšanā un veicinot biedru uzņemšanas procesa uzlabošanu.
- Turpinājās darbs FIRST darba grupas *CSIRT Services Framework* darbā, lai izstrādātu vienotu ietvaru CERT komandu dalībnieku lomām, kompetencēm un prasmēm.
- Turpinājās aktīva dalība enerģētikas informācijas apmaiņas un sadarbības grupā *Energy ISAC Camelot*, lai veicinātu informācijas apmaiņu un sekmētu enerģētikas sektora kiberdrošību.
- Dalība ENISA Eiropas kiberdrošības indeksa (*EU Cybersecurity index*) darba grupā, kurā tiek izstrādāta kiberdrošības indeksa vērtības aprēķina metodoloģija dalībvalstu kiberdrošības novērtēšanai. Sadarbojoties ar Aizsardzības ministriju, tika izskatīti sagatavotie darba dokumenti un nosūtīti priekšlikumi dokumentu pilnveidošanai. Tiek plānota Latvijas pārstāvju tikšanās ar ENISA, lai pārrunātu metodoloģijas pielietojumu un iespējas sagatavot indeksa aprēķinam nepieciešamos datus.
- 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.

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 1. ceturksnī CERT.LV turpināja darbu pie Grafoskopa attīstīšanas un pilnveidošanas, kā arī projekta ietvaros uzsāka darbu pie iepirkuma plāna un prasību izstrādes. Pārskata periodā CERT.LV piedalījās attālinātās JTAN projekta sanāksmēs, kurās projekta partneri prezentēja savus projekta uzdevumus.

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. Projekta Cyber Exchange īstenošana

Turpinājās 2018. gada 1. novembrī CERT.LV uzsāktā *2017 CEF Telecom Cyber Security* uzsaukumā apstiprinātā projekta *Cyber Exchange* (līguma ar Eiropas Komisiju Nr. INEA/CEF/ICT/A2017/1528866) (turpmāk – *Cyber Exchange*) īstenošana.

Projekta mērķis ir stiprināt starptautisku sadarbību starp nacionālajām un valdības CSIRT/CERT organizācijām. *Cyber Exchange* projekts ir kā atbilde arvien pieaugošajiem draudiem kiberdrošības jomā, īpašu akcentu vēršot uz nepieciešamo pārrobežu sadarbību cīņā pret tiem. Latvija ir viena no 10 Eiropas valstīm, kas piedalās projektā. Projekta pamata aktivitāte ir pieredzes apmaiņas vizīšu organizēšana – Latvijas CERT.LV pārstāvjiem viesojoties pie citu projekta dalībvalstu CSIRT/CERT komandām vai uzņemot vizītē kolēģus no citām CSIRT komandām.

2022. gada 1. ceturksnī projekta ietvaros CERT.LV piedalījās attālinātā projekta sanāksmē, kurā tika apspriesti projekta noslēguma darbi un plānota klātienes sanāksme Horvātijā 2022. gada jūnijā un citas savstarpējās vizītes. 2022. gada aprīlī CERT.LV plānota tehniskā vizīte Heraklionā, Grieķijā.

Projektu plānots īstenot līdz 2022. gada 30. jūnijam.

8. 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.
  Projekta ietvaros ir bijuši jau daudzi gadījumi, kuros nostrādājusi aktīvā aizsardzība, pasargājot lietotājus no ļaundabīga satura un iekārtas no inficēšanas. Pārskata periodā

lietotāji tika pasargāti no vairāku viltus lapu apmeklējumiem, maksājumu karšu datu zādzībām, viltus kurjerkompāniju tīmekļa vietņu apmeklējuma, kā arī tika liegts inficētām iekārtām sazināties ar vīrusu kontroles serveriem.
Daļu no DNS PRZ pakalpojuma var izmantot bez līguma slēgšanas un autorizēšanās jebkurš interneta lietotājs. Lai to izmantotu, jālieto NIC.LV rekursīvie DNS serveri. Tīmekļa vietnē dnsmuris.lv pieejamas ērti lietojamas instrukcijas DNS ugunsmūra aktivizēšanai.

- CERT.LV guva iespēju papildināt apkures katlu inženieru un montieru apmācības centra sertifikācijas materiālu saturu, pievienojot informāciju par iekārtu izmantošanu tiešsaistē un riskiem, kas ar to saistīti.

- 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 darbu uzticamības pakalpojumu sniedzēju uzraudzībā, par ko tika iesniegta ikgadējā atskaite Eiropas Komisijai par 2021.gadā paveikto. Kvalificētu elektroniskās identifikācijas pakalpojumu uzraudzības jomā tika izskatīts VAS LVRTC kvalifikācijas saglabāšanas pieteikums un VAS LVRTC tika saglabāts kvalificēts paaugstinātas drošības elektroniskās identifikācijas pakalpojuma sniedzēja statuss, kā arī tika saglabāts kvalificēts paaugstinātas drošības elektroniskās identifikācijas līdzekļa statuss, visiem iepriekš pieteiktajiem VAS LVRTC elektroniskās identifikācijas līdzekļiem.

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

Latvijas Interneta asociācijas Drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.01.2022. līdz 31.03.2022. ir saņēmusi un izvērtējusi 7 691 ziņojumus. No tiem 7 144 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 15 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 16 ziņojumos konstatēta personas goda un cieņas aizskaršana, 156 ziņojumi saņemti par naida runu un 5 ziņojumi par vardarbību atainojošiem materiāliem. Par finanšu krāpšanas mēģinājumiem internetā saņemti 87 ziņojumi, 199 ziņojumu saturs nav bijis pretlikumīgs, 69 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 6 835 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 170 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 6 974 ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem 6 966 ziņojumi ir dzēsti no publiskas aprites un 8 ziņojumu saturs atrodas dzēšanas procesā sadarbībā ar Valsts policiju un interneta pakalpojumu sniedzējiem.

2022. gada 2. maijā.

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

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

Saziņa ar CERT.LV:

Telefons: +371 67085888

E-pasts: cert@cert.lv

Tīmekļa vietne: www.cert.lv

Sekot CERT.LV aktualitātēm:

www.twitter.com/certlv

www.facebook.com/certlv

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija