Latvijas universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

2021 C4

Publiskais pārskats par CERT.LV uzdevumu izpildi

2021. gada 4. ceturksnis (01.10.2021. – 31.12.2021.)

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

2021. gada 4. ceturksnī CERT.LV kibertelpā novēroja lielu apjomu kritisku ievainojamību, jaunu pieeju zvanītāja numura viltošanā krāpnieciskajos telefona zvanos, kā arī piegāžu ķēžu uzbrukumu aktualizēšanos.

Pārskata periodā tika reģistrētas 121 439 unikālas apdraudētas IP adreses, kas ir par 22% vairāk nekā iepriekšējā ceturksnī, bet par 24% mazāk nekā šajā pašā periodā pirms gada.

Pārskata periodā Latvijas interneta telpā izplatītākie apdraudējumi:

- konfigurācijas nepilnības (68 221 unikāla IP adrese) ar kritumu par 3% pret iepriekšējo periodu;
- ļaundabīgs kods (11 421 unikāla IP adrese) ar kritumu par 9%;
- informācijas vākšana (1657 unikālas IP adreses) ar kritumu par 18%.

Lielākā daļa krāpniecību bija vērstas uz iedzīvotāju maksājuma karšu piekļuves datu, finanšu līdzekļu, kā arī e-pasta piekļuves datu iegūšanu. Uzbrucēji sūtīja iedzīvotājiem krāpnieciskus e-pastus un īsziņas, uzdodoties, galvenokārt, par banku pārstāvjiem vai e-pasta pakalpojumu sniedzējiem. Krāpniecībās tika izmantotas arī sūtījumu piegādes kompānijas *Omniva*, *DPD* un *Latvijas Pasts*, lai, iespējams, pirmssvētku noskaņās, izvilinātu iedzīvotāju maksājumu karšu datus.

Uzņēmumi piedzīvoja iejaukšanos biznesa sarakstē ar zaudējumiem 200 000 eiro apmērā, un izspiedējvīrusu uzbrukumus, kuru rezultātā sašifrēta tika ne tikai serveros glabātā informācija, bet arī datu rezerves kopijas. Cietušie uzņēmumi apsvēra iespēju maksāt izpirkumu. CERT.LV rīcībā nav informācijas par to, vai izpirkums tika samaksāts.

Arī Latviju skāra piegāžu ķēžu uzbrukumi gan kompromitētas *JavaScript* bibliotēkas formā, kas ietekmē dažādu informācijas tehnoloģiju produktu drošu izmantošanu, gan kiberuzbrukumi pret Latvijas uzņēmumiem, kas ražo risinājumus globālajam tirgum.

Pārskata periodam bija raksturīgs ievērojams kritisku ievainojamību apjoms, kas pakļāva uzbrukumu riskam gan valsts, gan privātā sektora sistēmas. Aizsardzību apgrūtināja strauji mainīgā informācija par ievainojamības ietekmes mazināšanu, tai skaitā par atjauninājumu efektivitāti.

Vairāku valsts iestāžu informācijas sistēmu darbības traucējumus izraisīja tehniskas dabas traucējumi, atsevišķos gadījumos tie apturēja sistēmu darbību uz vairākām stundām.

6.-7. oktobrī Eiropas Kiberdrošības Mēneša ietvaros CERT.LV rīkoja tehnisko tiešsaistes konferenci kiberdrošības profesionāļiem *Kiberšoks 2021*, kurā starptautiski novērtēti eksperti dalībniekiem sniedza padziļinātu ieskatu plašā ar kiberdrošību saistītu jautājumu klāstā. Pasākumā piedalījās 923 dalībnieki no 53 valstīm.

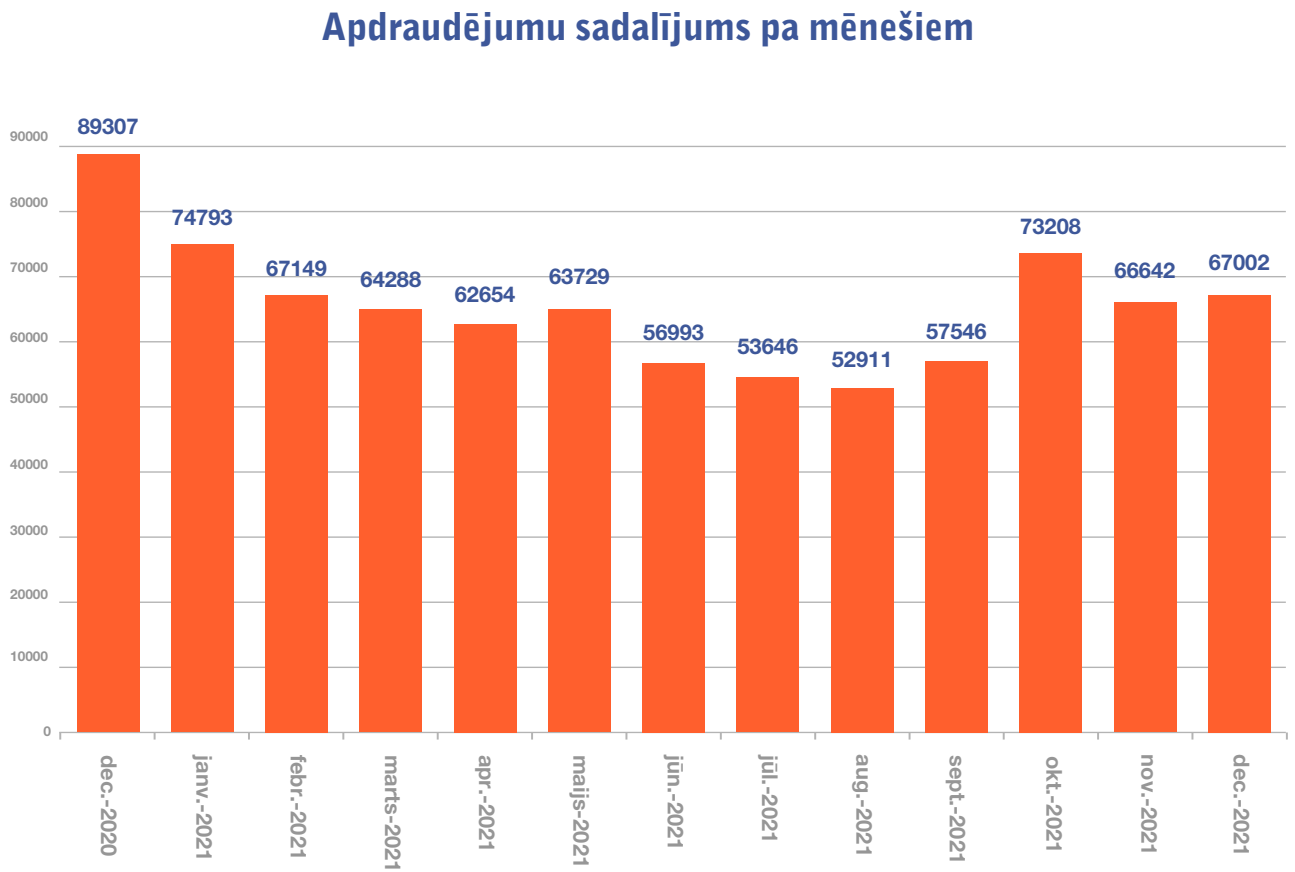
Pārskata periodā CERT.LV par IT drošību izglītoja 5414 cilvēkus, iesaistoties 38 izglītojošos pasākumos.

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

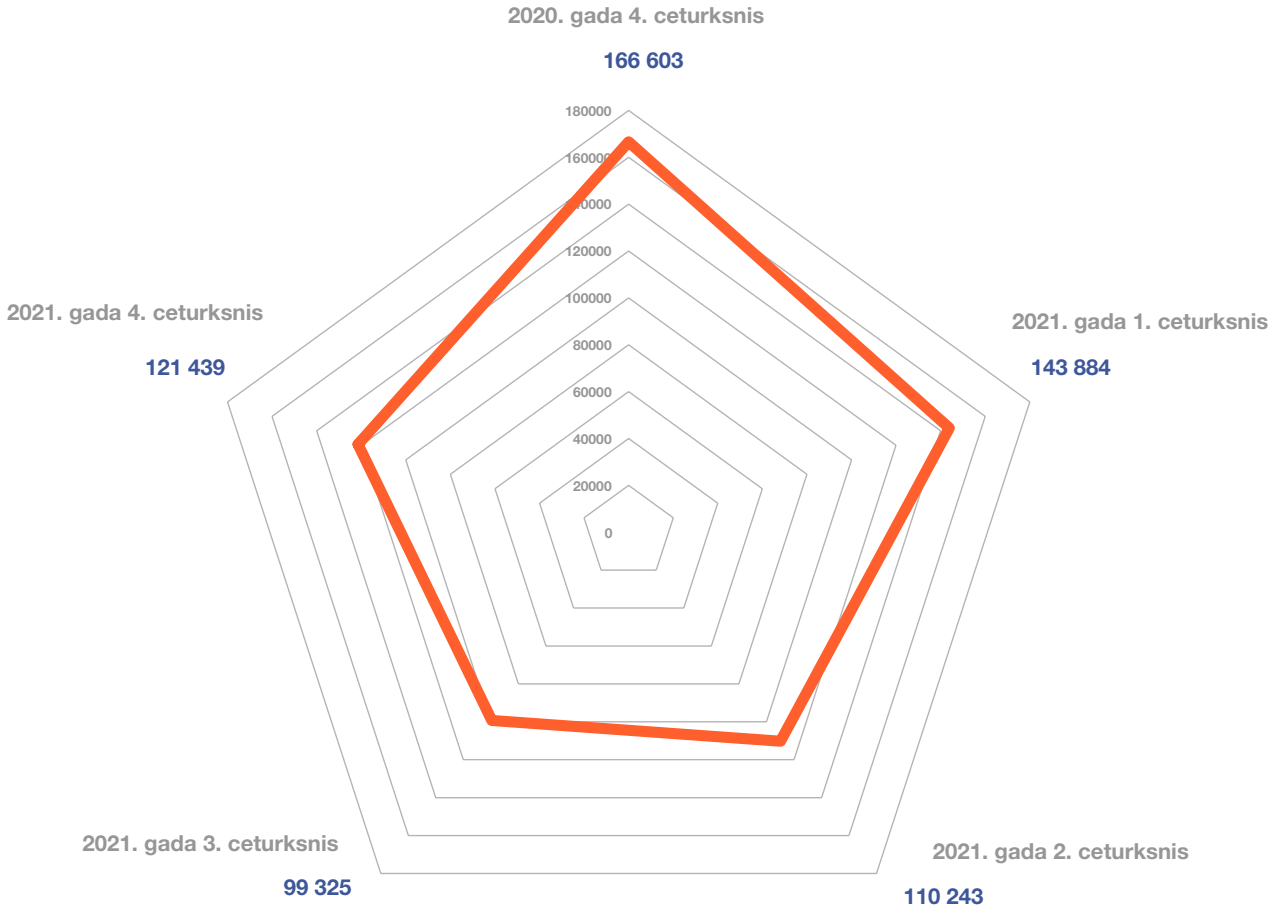
uzskaitīti vienkopus, sadalot tos pa apdraudējumu veidiem (piemēram, ļaunatūra, ielaušanās, krāpšana), kā arī pa ļaunatūru (piemēram, *Confiker*, *Zeus*, *Mirai*) un konfigurācijas nepilnību (piemēram, *Opendns*, *Openrdp*) tipiem.

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



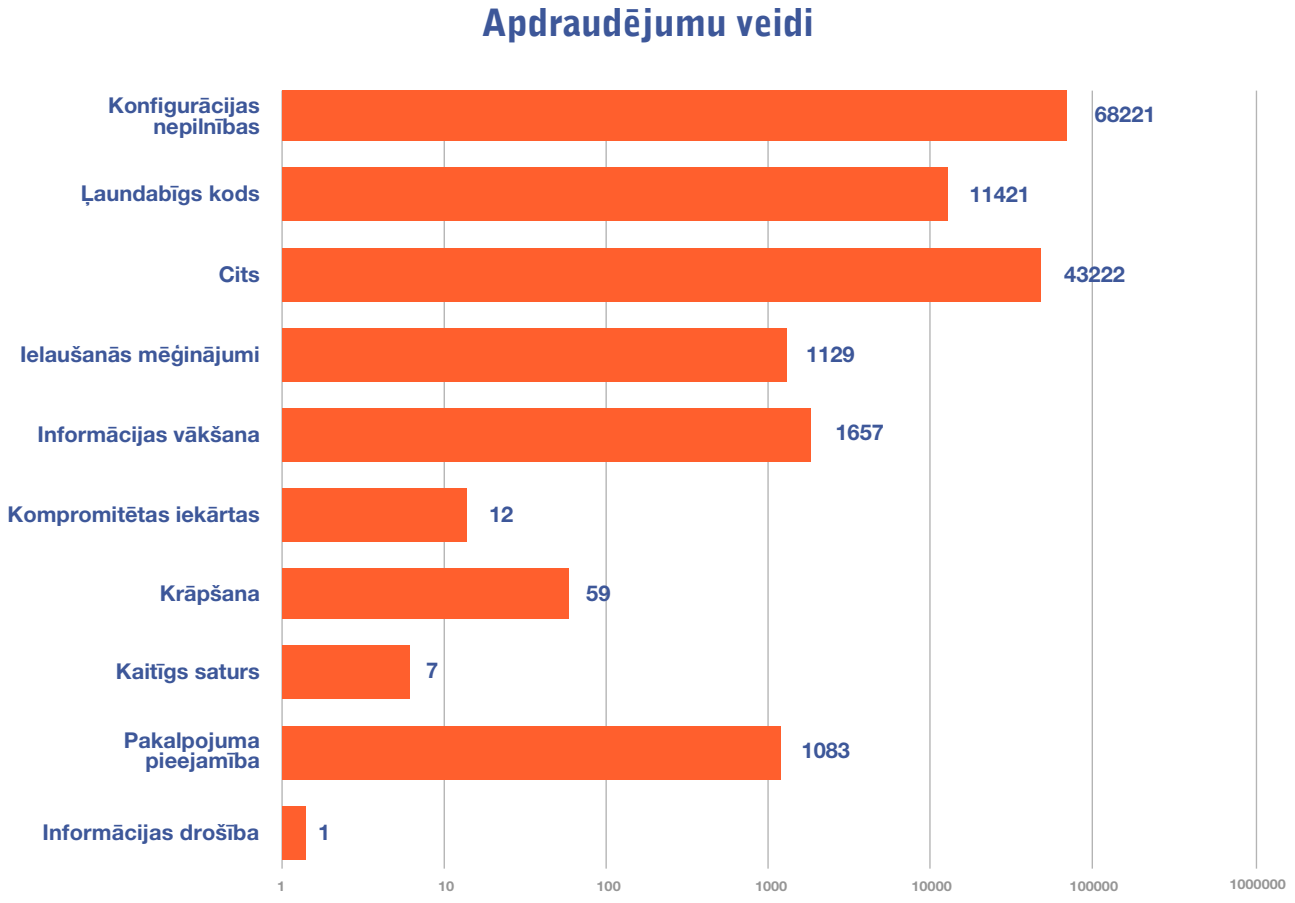
1. attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa mēnešiem 12 mēnešu griezumā.

Apdraudējumu sadalījums pa ceturkšņiem



2. attēls – CERT.LV reģistrētās apdraudētās IP adreses pa ceturkšņiem 2020. un 2021. gadā.

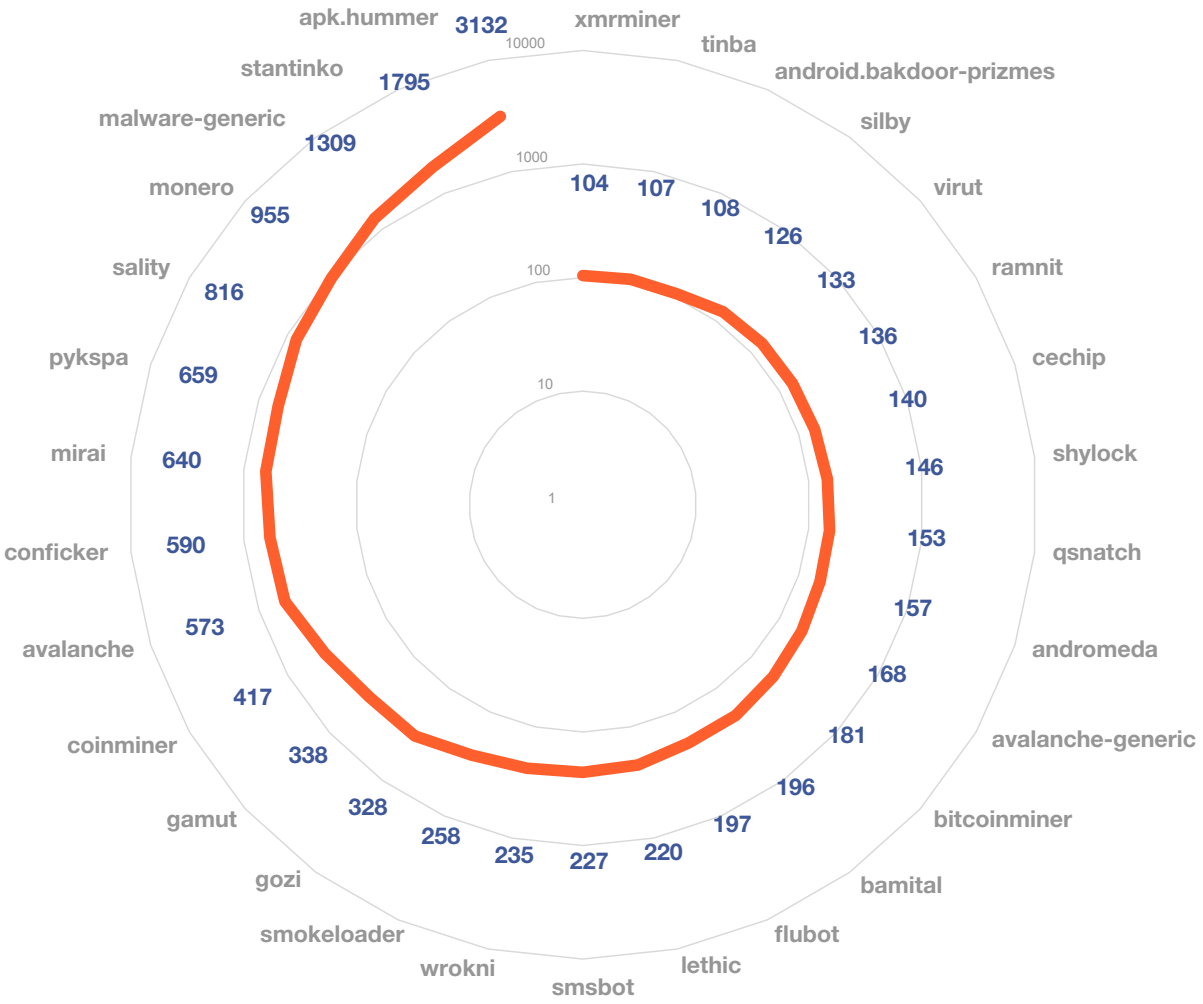
2021. gada 4. ceturksnī tika reģistrētas 121 439 unikālas apdraudētas IP adreses, kas ir par 22% vairāk nekā iepriekšējā ceturksnī, bet par 24% mazāk nekā šajā pašā periodā pirms gada. Kāpums skaidrojams ar pieaugumu apdraudējumu kategorijā Cits, kas satur informāciju par konsultācijām, melnajos sarakstos iekļautajām IP adresēm u.tml.



3. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2021. gada 4. ceturksnī pa apdraudējumu veidiem.

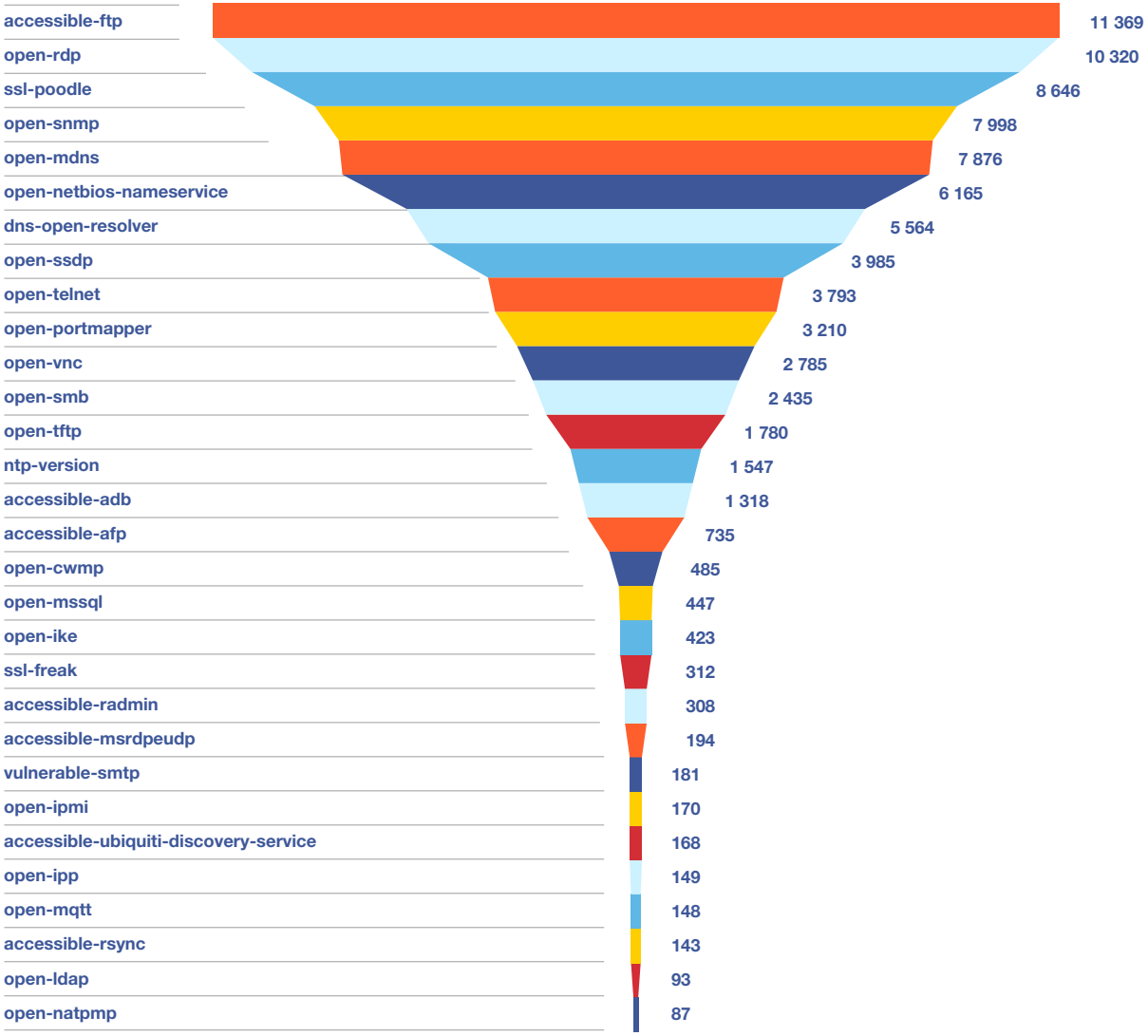
Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (68 221 unikāla IP adrese) ar kritumu par 3% pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs kods (11 421 unikāla IP adrese) ar kritumu par 9%, bet trešais – informācijas vākšana (1657 unikālas IP adreses) ar kritumu par 18%, kuru izraisīja īslaicīgs samazinājums ienākošo datu apjomā.

Unikālo IP adrešu skaits – ļaundabīgs kods



4. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2021. gada 4. ceturksnī ar apdraudējuma veidu – ļaundabīgs kods.

Unikālo IP adrešu skaits – konfigurācijas nepilnības



5. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2021. gada 4. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

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 *Moneроminer*. 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 augšgals paliek nemainīgs. 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.

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

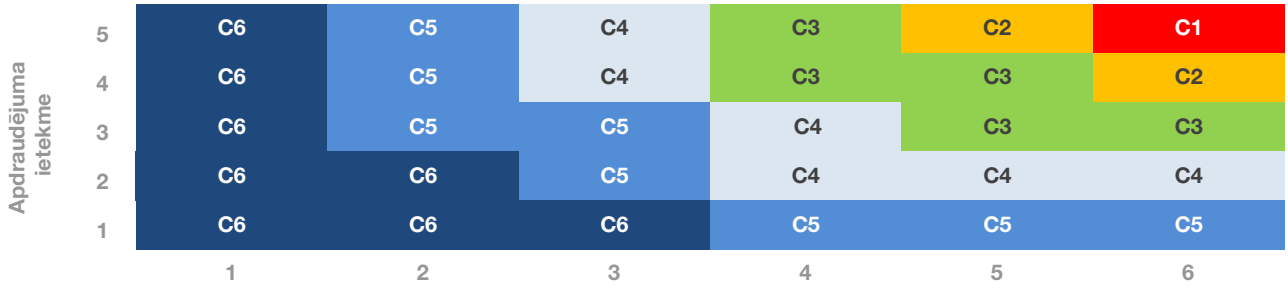
Trešo vietu ieņem konfigurācijas nepilnība *SSL-Poodle*, kas pakļauj iekārtu *POODLE* (*Padding Oracle On Downgraded Legacy Encryption*) uzbrukumam, sniedzot uzbrucējiem iespēju pārtvert šifrētu datu plūsmu, piemēram, lietotājvārdus, paroles, sīkdatnes u.c., un izlikties par iekārtas lietotāju.

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.

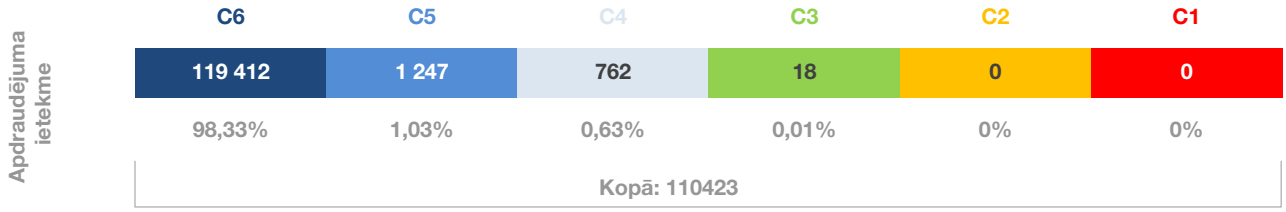
Apdraudējumu matrica



6. attēls – Apdraudējumu matricas sadalījums kategorijās.

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.

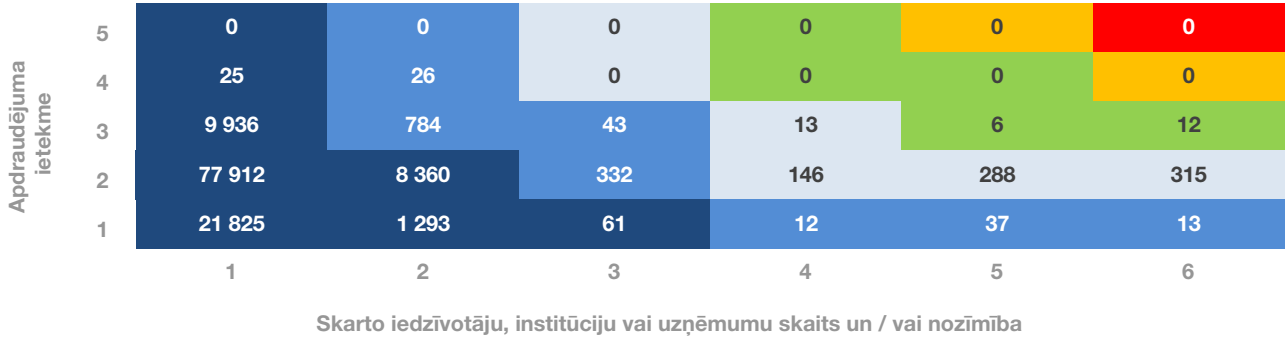
Apdraudēto unikālo IP adrešu sadalījums



7. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu sadalījums apdraudējumu kategorijās pēc apdraudējuma ietekmes (matrica) 2021. gada 4. ceturksnī.

Nacionāla līmeņa apdraudējumi (C1) un augstas nozīmes apdraudējumi (C2) pārskata periodā nav reģistrēti. Nozīmīgi plašas ietekmes apdraudējumi (C3) veido 0,01% (18 unikālas apdraudētas IP adreses/gadījumi) no visiem kategorizētajiem apdraudējumiem. 95% šo apdraudējumu veido ļaundabīgs kods (*Android.Hummer*, *Tinba*, *Sality*, *Stantinko* u.c.), bet 5% pakalpojuma pieejamības atteices jeb DDoS uzbrukumi augstas prioritātes iestādēs.

Apdraudēto unikālo IP adrešu izvietojums



8. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu izvietojums matricā 2021. gada 4. 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, ielaušanās mēģinājumi un ļaundabīgs kods (*Android.Hummer*, *Monero*, *Rootnik* u.c.), kas novēroti augstas un vidēji augstas prioritātes iestādēs – virknē pašvaldību un augstākās izglītības iestāžu.

Lai mazinātu kopējo apdraudēto IP adrešu skaitu, 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.

Lielākā daļa krāpniecību bija vērstas uz iedzīvotāju maksājuma karšu piekļuves datu, finanšu līdzekļu, kā arī e-pasta piekļuves datu iegūšanu. Uzbrucēji sūtīja iedzīvotājiem krāpnieciskus e-pastus un īsziņas, kā arī veica krāpnieciskus telefona zvanus, visbiežāk uzdodoties par banku pārstāvjiem vai e-pasta pakalpojumu sniedzējiem. Vairāki uzņēmumi cieta no iejaukšanās biznesa sarakstē (BEC), ciešot kopējos zaudējumus gandrīz 200 000 eiro apmērā.

Krāpnieku uzmanības lokā bija nonācis *Latvijas Pasts*. Uzbrucēji vairākās kampaņveidīgās aktivitātēs uzņēmuma vārdā izplatīja gan krāpnieciskus e-pastus ar draudiem par aizturētiem sūtījumiem, gan loterijas, cenšoties izvilināt iedzīvotāju maksājumu karšu datus un citu personīgu informāciju. Iespējams, šis uzņēmums tika izvēlēts, pateicoties tam, ka tuvojās pirmssvētku periods un dāvanu iegādes laiks.

Preču piegādes tematika figurēja arī krāpniecības mēģinājumos, kas bija vērsti pret pārdevējiem, kuri informāciju par preču pārdošanu ievietoja sludinājumu portālos. Uzdodoties par ieinteresētiem pircējiem un izmantojot *WhatsApp* saziņas platformu, krāpnieki izteica vēlmi iegādāties preci, it kā izmantojot kurjerkompānijas pakalpojumus, un aicināja pārdevējus maksājuma saņemšanai ievadīt karšu datus viltotās *Omniva*, *DPD* un vēlāk arī *Latvijas Pasts* vietnē, atklājot krāpniekiem gan CVV kodu, gan kartē pieejamo atlikumu. Daļa iedzīvotāju krāpnieciskās vietnes adresi rūpīgi aplūkoja tikai pēc datu ievadīšanas, tādējādi kļūstot par krāpniecības upuriem. Krāpnieki izmantoja pielāgotas tīmekļa vietņu adreses (domēnus), kas bija līdzīgas oriģinālo vietņu adresēm, lai maldinātu iedzīvotājus. CERT.LV rīcībā nav informācijas par zaudējumu apjomu.

Iespējams, tālākai izmantošanai krāpnieciskos nolūkos, uzbrucēji centās pārņemt *WhatsApp* kontus, lūdzot pārsūtīt sešciparu kodu, kuru it kā kļūdas pēc nosūtījuši uz ziņas saņēmēja telefona numuru. Tā kā ziņa tika saņemta no kontaktu sarakstā iekļautām personām, daļa iedzīvotāju kodus pārsūtīja, zaudējot piekļuvi savam *WhatsApp* kontam. Līdzeklis aizsardzībai pret šādu uzbrukumu būtu divu faktoru autentifikācijas izmantošana.

Krāpnieciskas īsziņas un e-pastus iedzīvotāji saņēma arī dažādu banku vārdā. Galvenokārt ziņas tika sūtītas plašam saņēmēju lokam, arī tiem, kas nebija konkrētās bankas klienti. Krāpnieki mēģināja iegūt iedzīvotāju datus, panākot šo datu ievadīšanu krāpnieciskās vietnēs, vai pārliecinot ziņas saņēmēju par nepieciešamību lejupielādēt ziņai pievienoto ļaundabīgo datni, kas parasti saturēja informāciju (paroles u.c.) ievācošu vīrusu, piemēram, *AgentTesla*. E-pastu serveris, kas atbalsta mūsdienu standartus (piem., DMARC izmantošana), šādus krāpnieciskus e-pastus automātiski atfiltrēja un tie gala lietotājus nesasniedza.

Maksājumu karšu informāciju krāpnieki no iedzīvotājiem mēģināja iegūt arī, izsūtot e-pastus ar aicinājumu pieteikties *Bitcoin* atlikumam, pierakstoties krāpnieciskā kriptovalūtas apmaiņas servisā.

Tika saņemta ziņa par uzbrukumu, kurā krāpnieki izmantoja NFT (*Non-fungible Tokens*), kas digitālajā vidē reprezentē kādu mākslas darbu vai artefaktu, piemēram, īpašu ieroci virtuālajā spēlē. Uzbrucēji uzrunāja spēlētājus, izmantojot *Discord* saziņas platformu, un norādīja uz fiktīvu problēmu, kuru piedāvājās palīdzēt atrisināt, tādējādi piekļūstot spēlētāju personīgajiem identifikatoriem. Tie ļāva turpināt komunicēt šo spēlētāju vārdā un izplatīt krāpnieciskus aicinājumus veikt drīzumā publicējamu jaunu NFT iegādi. Ziņotais kopējais zaudējumu apjoms (pārsvarā spēlētājiem ārpus Latvijas) sastādīja 300 tūkstošus eiro.

Tika novērota arī aktīva iedzīvotāju komentēšana un dalīšanās ar brīdinājumu sociālajos tīklos par mobilo iekārtu apdraudējumu, kas bija aktuāls pirms 20 gadiem – saņemot krāpniecisku zvanu un ievadot kombināciju #9, zvanītājs iegūst piekļuvi zvana saņēmēja iekārtai. Šo aktivitāti varētu skaidrot ar nepieciešamību paaugstināt iedzīvotāju izpratnes līmeni par aktuālajiem apdraudējumiem.

2.2. Pakalpojuma pieejamība

Pārskata periodā pakalpojuma atteices jeb DDoS uzbrukumi galvenokārt bija vērsti pret telekomunikāciju pakalpojumu sniedzējiem.

4. oktobrī tika saņemta informācija par darbības traucējumiem Latvijas Nacionālās bibliotēkas (LNB) Datu centrā. Tika traucēta darbība lielai daļai Kultūras informācijas sistēmu centra (KISC). CERT.LV pieejamā informācija neliecina par ārēju ietekmi uz LNB Datu centra pakalpojumu pieejamību.

10. oktobrī tika saņemts ziņojums par darbības traucējumiem kādas valsts iestādes uzturētajā platformā, Valsts kancelejas uzturētajā *Valsts un pašvaldību iestāžu tīmekļvietņu vienotajā platformā.* Tehniska kļūme uz laiku apturēja visu platformā izvietoto tīmekļa vietņu darbību.

Decembra sākumā darbības traucējumus piedzīvoja Saeimas tiešsaistes platforma *e-Saeima*, kas nodrošina Saeimai iespēju strādāt attālināti. Pārbaužu rezultātā tika konstatēts, ka darbības traucējumus nav radījusi ārēja ietekme, bet gan sistēmas atjauninājumi.

Ilgstoši DDoS uzbrukumi traucēja kādas skolas darbu. Līdzīgi ziņojumi no citām mācību iestādēm tika saņemti jau mācību gada sākumā. Ar šādiem izaicinājumiem saskaras arī mācību iestādes citviet Eiropā.

Sabiedrības un mediju interesi izraisīja oktobra sākumā piedzīvotā *Facebook* un ar to saistīto produktu (*Instagram* un *WhatsApp)* nepieejamība, kas ilga vairāk nekā 5 stundas. *Facebook* globālajā digitālajā telpā, tajā skaitā arī Latvijas iedzīvotājiem, kalpo ne tikai par saziņas platformu, bet tiek plaši izmantots arī kā pierakstīšanās rīks citās vietnēs un tiešsaistes pakalpojumos, piemēram, tirdzniecības vietnēs vai viedtelevīzijā. Kompānija publiski pauda, ka problēmas radīja kļūme konfigurācijā, un nav pamata domāt, ka būtu ietekmēti vai kompromitēti lietotāju dati.

2.3. Ļaundabīgs kods

Vairāki uzņēmumi cieta šifrējošo izspiedējvīrusu uzbrukumos. Tika nošifrēti serveri un ārējie diski, kā arī uzbrukumos bojātas datu rezerves kopijas. Nevienā no gadījumiem projekta *nomoreransom.org* ietvaros nebija pieejama atšifrēšanas atslēga. Zināms, ka dažu uzņēmumu izmantotajās iekārtās pirms kāda laika bija ievainojamības, kuras, iespējams, uzbrucēji izmantojuši,

lai iegūtu piekļuvi uzņēmumu iekšējam tīklam. Atsevišķos gadījumos vīrusa izplatību veicināja nepārdomāts IT infrastruktūras plānojums. Uzņēmumi apsvēra iespēju maksāt izpirkuma maksu. Viens no uzņēmumiem vēlāk ziņoja par atkārtotiem mēģinājumiem piekļūt tam pašam serverim.

Uzdodoties par uzņēmumu *SIA BRE* un *SIA MEKO un KO* darbiniekiem, uzbrucēji masveidā izsūtīja e-pastus ar *LokiBot* vīrusu pielikumā. Vīruss tika maskēts kā .zip datne un bija paredzēts paroļu izgūšanai no datorā izmantotajām programmmām un interneta pārlūkiem, kā arī kriptovalūtu maciņu un to piekļuves informācijas meklēšanai.

Saņemti ziņojumi par aktīvu ļaunatūras *QakBot* izplatīšanas kampaņu, izmantojot *MS Excel* dokumentus. Dokumenti ar kaitīgu saturu tika nosūtīti upuriem kā e-pasta pielikumi, par pamatu izmantojot iepriekš notikušu saraksti, kas iegūta no jau kompromitētām iekārtām. Par uzbrukuma mērķiem tika izvēlēti akadēmiskā, aizsardzības un privātā sektora pārstāvji. *QakBot* ir banku trojānis, kas paredzēts bankas piekļuves datu un maksājumu informācijas iegūšanai, kā arī spēj izplatīt izspiedējvīrusus.

Novērota *TP-Link* maršrutētāju un *Hikvision* kameru aktīva iesaiste robotu tīklos (*botnet*). Kompromitētās iekārtas tika izmantotas, lai veiktu uzbrukumus uz *WordPress* bāzētām tīmekļa vietnēm.

2.4. Ielaušanās mēģinājumi

Ielaušanās mēģinājumi 98% gadījumu veikti, izmantojot paroļu minēšanu (*brute-force*). Uzbrukumi veikti galvenokārt pret dažādiem interneta pakalpojumu sniedzējiem, dažām valsts iestādēm, kā arī atsevišķām pašvaldībām un privāto sektoru. Pēc CERT.LV rīcībā esošās informācijas šie uzbrukumi nav bijuši sekmīgi.

2.5. Kompromitētas iekārtas un datu noplūdes

Tika kompromitēta populārā *JavaScript UA-Parser-JS NMP* bibliotēka, realizējot plašas ietekmes piegāžu ķēdes integritātes uzbrukumu (*supply chain attack*). Bibliotēka tiek plaši izmantota dažādos IT risinājumos lietotāja pārlūkprogrammas, operētājsistēmas, iekārtas tipa un modeļa atpazīšanai. Uzbrukuma rezultātā miljoniem *Linux* un *Windows* iekārtu tika inficētas ar ļaunatūru, kas paredzēta paroļu pārtveršanai un nesankcionētai iekārtas resursu izmantošanai kriptovalūtu ieguvē. Šo *JavaScript* bibliotēku izmanto *Facebook*, *Microsoft*, *Amazon, Instagram, Google, Slack, Mozilla, Discord, Elastic* un daudzas citas kompānijas. CERT.LV aicināja sekot norādēm un pārbaudīt, vai sistēma nav kompromitēta, ja projektā tiek izmantota šī bibliotēka.

Vairāki iedzīvotāji sociālajos tīklos norādīja, ka ir saņēmuši brīdinājumus no *Apple* par uz sevi mērķētiem valstu sponsorētiem kiberuzbrukumiem. Tas saistīts ar ASV aktīvo vēršanos pret ofensīvo kiberrīku kompānijām *NSO Group*, *Candiru*, kā arī Krievijas *Positive Technologies* un Singapūras *Computer Security Initiative Consultancy PTE*. Kompānijas iekļautas ASV melnajā sarakstā kā personu un korporāciju privātumu un drošību apdraudošas.

Kādā valsts iestādē tika konstatētas kompromitēšanas pazīmes un ļaunatūras klātbūtne. Neskatoties uz savlaicīgiem CERT.LV brīdinājumiem, uzbrukums pamanīts novēloti – mēnesi pēc ievainojamības publicēšanas un pēc neuzmanīgas uzbrucēja rīcības. Incidents ietekmēja iestādes nodrošinātā risinājuma integrācijas iespējas, taču neradīja tiešu ietekmi uz tā funkcionalitāti. Turpinās darbs pie incidenta izpētes, lai pārliecinātos, ka nav nodarīts plašāks kaitējums.

Kādā valsts iestādē pēc atjauninājumu uzstādīšanas, tika konstatēta neatbilstoša lietotāju tiesību konfigurācija. Veicot izpēti, tika noskaidrots, ka incidents ir lokāla mēroga un radies, kļūdas pēc uzstādot nepareizos atjauninājumus, kuros netika saglabāta pieejas tiesību konfigurācija.

Mediju un sabiedrības uzmanību piesaistīja vairāki dažādās valstīs izdoti derīgi COVID19 vakcinācijas sertifikāti ar fiktīvām identitātēm – Ādolfs Hitlers, multiplikācijas filmu varoņi u.tml. Tika paustas bažas par iespējamu sertifikāta ievainojamību vai noplūdušām sistēmu privātajām

atslēgām. Ekspertu veikto pārbaužu rezultātā tika konstatēts, ka sertifikātu integritāte nav ietekmēta. Tika atklāti vairāki kanāli (Polijā, Ziemeļmaķedonijā, Vjetnamā), kas sniedza iespēju radīt neleģitīmus sertifikātus un kuru darbības pamatā bija negodprātīga medicīnas darbinieku rīcība. Tika konstatēts arī, ka sertifikātu anulēšanas mehānisms Eiropas Savienībā bija izstrādāts dizaina dokumentos, taču nebija pilnībā implementēts. Lai šo problēmu ierobežotu un identificētu liela mēroga neleģitīmu sertifikātu lietošanu, nepieciešams papildināt esošo risinājumu ar visaptverošu žurnalēšanu un žurnalēšanas ierakstu auditēšanu, taču tas, iespējams, konfliktēs ar leģitīmiem privātuma argumentiem.

Tika kompromitēti vairāku iestāžu un uzņēmumu e-pastu konti. No kompromitētajiem kontiem uzbrucēji veica tālākus pikšķerēšanas uzbrukumus, izsūtot e-pasta vēstules upura kontaktiem.

2.6. Ievainojamības

Ceturksni iezīmēja vairākas kritiskas ievainojamības. Oktobra sākumā tika atklāta kritiska ievainojamība (CVE-2021-41773) *Apache* serveros, kas sniedza uzbrucējiem iespēju piekļūt failiem, kā arī veikt attālinātu koda izpildi. Novembra vidū tika atklāta kritiska ievainojamības (CVE-2021-3064, CVE-2021-3063) ugunsmūra *Palo Alto Networks GlobalProtect* portāla un vārtejas saskarnēs. Ievainojamības sniedza iespēju uzbrucējiem veikt patvaļīgu attālinātu koda izpildi, iegūstot piekļuvi ievainojamajai sistēmai (sensitīvai konfigurācijas informācijai, piekļuves datiem utt), kā arī, sagatavojot atbilstošu tīkla pieprasījumu, izraisīt kļūdu un apturēt iekārtas darbību. CERT.LV apziņoja ievainojamo sistēmu turētājus valsts sektorā.

Tām uz pēdām mina kritiska ievainojamība, kas ietekmēja *Microsft Exchange* serverus (CVE-2021-42321). Ievainojamība ļāva veikt attālinātu koda izpildi uz ievainojamajām iekārtām. CERT.LV izsūtīja brīdinājumus valsts un pašvaldību iestāžu par IT drošību atbildīgajiem ar aicinājumu uzstādīt atjauninājumus.

Decembra beigās globālo kibertelpu saviļņoja ziņa par kritisku ievainojamību plaši izmantotajā *Apache Java Logging* bibliotēkā *Log4j* (CVE-2021-44228). Ievainojamības ietekmes vērtējums

tika noteikts 10 no 10 (augstākajā mērā kritiska). Ievainojamība sniedza uzbrucējiem iespēju veikt attālinātu koda izpildi (RCE) ievainojamajā iekārtā. Ietekmēts tika plašs produktu klāsts: *Elasticsearch, Apache Struts / Solr / Druid / Flink, Kafka, Webex, Confluence, JIRA, Jitsi, Oracle* u.c. Īsā laikā pēc ievainojamības atklāšanas tika konstatēta tās aktīva izmantošana uzbrukumos, to skaitā šifrējošo izspiedējvīrusu izplatīšanai. Situāciju sarežģīja biežā informācijas maiņa par dažādu paņēmienu, tajā skaitā atjauninājumu, efektivitāti ievainojamības ietekmes mazināšanā. Latvijā pagaidām nav konstatēti ar *Log4j* saistīti nopietni incidenti, taču jau no decembra sākuma ir novēroti uzbrukumu mēģinājumi gan pret publisko, gan privāto sektoru. CERT.LV turpina uzraudzīt situāciju un seko līdzi aktuālajai informācijai.

Pārbaudot *Log4j* skartās iestādes, tika konstatēts, ka kādas iestādes uzturētā sistēma satur novecojušu bibliotēkas versiju. Konkrētā bibliotēka nav apdraudēta, jo vēl nesatur *Log4j*, taču vecuma un tehniskā atbalsta trūkuma dēļ (izstrādātāja atbalsts pārtraukts 2015. gadā) satur citas ievainojamības un apdraudējumus (iespējama koda attālināta izpilde, izmantoti novecojuši šifrēšanas algoritmi), kurus nav iespējams novērst, jo versijai vairs netiek nodrošināti atjauninājumi. Jaunāku tehnoloģiju neizmantošana tiek pamatota ar nespēju nodrošināt savietojamību ar citām ārējām sistēmām.

Kādā valsts iestādē tika konstatēta novecojusi tīmekļa vietne, kura, iespējams, satura dēļ atstāta infrastruktūrā un nav atjaunināta, līdz ar ko satur ievainojamības. Uzturētājs tika informēts. Šādi gadījumi publiskajā sektorā periodiski atkārtojas un ir recepte nepatikšanām.

2.7. Atbildīga ievainojamību atklāšana

CERT.LV pārskata periodā saņēma ziņojumus par starpvietņu skriptēšanas (XSS) ievainojamību vienā valsts iestādes un vienā sakaru pakalpojumu sniedzēja tīmekļa vietnē. XSS ievainojamība sniedz uzbrucējiem iespēju veikt patvaļīgu *JavaScript* izpildi, izdarot izmaiņas tīmekļa vietnes saskarnē, izgūstot informāciju no lietotāja pārlūka vai pārsūtot lietotājus uz citu, ļaundabīgu tīmekļa vietni. Par ievainojamību tika informēti vietņu uzturētāji.

Tika saņemts ziņojums par programmatūrā iešūtu publisko DNS atslēgu kādu serveru *admin* lietotājam. Iešūtā atslēga nav ne nomaināma, ne dzēšama. Šim atslēgu pārim ir publiski pieejama arī privātā atslēga, attiecīgi iekārtām var piekļūt ar SSH, ar admin kontu bez autorizācijas. Pieteicējam tika lūgta precizējoša informācija.

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 4. un 5. punktā.

3. Pētnieciskais darbs, izglītojošo pasākumu organizēšana, mācības IT drošības jomā un sabiedrības informēšanā

2021. gada oktobris bija jau 9. ikgadējais Eiropas Kiberdrošības mēnesis, kurš pulcē ES iedzīvotājus, dalībvalstis, struktūrvienības un organizācijas, privātā sektora un akadēmisko aprindu pārstāvjus, lai popularizētu veselīgus kiberdrošības ieradumus. Visā Eiropā un ārpus tās mēneša ietvaros tika rīkoti pasākumi tiešsaistē, to skaitā mācības, konferences, viktorīnas, prezentācijas un valsts mēroga kampaņas, kuru mērķis bija uzlabot izpratni par kiberriskiem un dalīties ar informāciju par jaunākajām vadlīnijām un veidiem šo risku mazināšanai.

6.-7. oktobrī Eiropas Kiberdrošības Mēneša ietvaros CERT.LV rīkoja tehnisko tiešsaistes konferenci kiberdrošības profesionāļiem *Kiberšoks 2021*, kurā starptautiski novērtēti eksperti dalībniekiem sniedza padziļinātu ieskatu plašā ar kiberdrošību saistītu jautājumu klāstā, prezentācijās iekļaujot arī reāllaika demonstrācijas. Pasākumā piedalījās 923 dalībnieki no 53 valstīm. Paralēli konferencei norisinājās arī CTF (*Capture the Flag*) sacensības, kurās dažādiem kiberdrošības izaicinājumiem pretī stājās 31 komanda. (https://cybershock.lv/)

21. oktobrī *Eiropas Kiberdrošības mēneša* ietvaros *SIA Tet* rīkoja kiberdrošības forumu *CyberShield*, kura mērķis ir pievērst sabiedrības un uzņēmēju uzmanību virtuālajai drošībai, iedzīvinot kiberhigiēnas labāko praksi, analizējot aktuālākās tendences kibertelpā un aicinot ikvienu būt vērīgiem un ieguldīt enerģiju savu digitālo prasmju pilnveidē. CERT.LV pārstāvis forumā sniedza pārskatu par Latvijas un globālās kibertelpas aktualitātēm. (https://www.tet.lv/uznemumiem/vairak/forums-cybershield)

5. novembrī CERT.LV sadarbībā ar NIC.LV (.lv domēnu reģistru) piedalījās *Zemgales uzņēmējdarbības centra* organizētajā seminārā uzņēmējiem *IT risinājumi biznesa attīstībai*, kurā iepazīstināja klausītājus ar ieteikumiem, kā atpazīt kiberuzbrukumus, un kā pasargāt gan savu uzņēmumu, gan domēna vārdu digitālajā vidē.

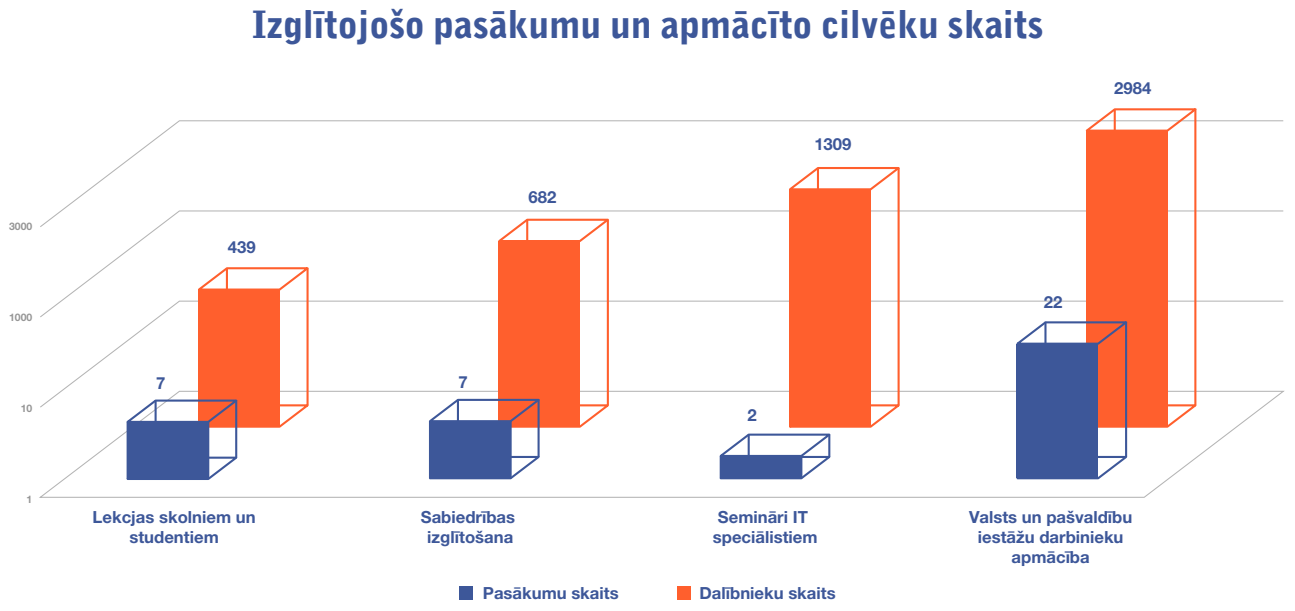
No 26.novembra pēc Aizsardzības ministrija iniciatīvas CERT.LV organizēja piecus kiberdrošības seminārus Latvijas Republikas Saeimas deputātiem un viņu palīgiem par informācijas drošības pamatprincipiem un labo praksi.

2. decembrī Latvijas Informācijas un komunikācijas tehnoloģijas asociācijas (LIKTA) ikgadējā konferencē tika pasniegta balva *Platīna pele*. Balva tiek pasniegta vairākās kategorijās un tās mērķis ir apzināt veiksmīgākos Latvijā radītos digitālos risinājumus, novērtēt izcilākos projektu autorus un izstrādātājus, kā arī veicināt izpratni par jēgpilnu tehnoloģiju pielietojumu – sabiedrībā, biznesā, pārvaldē un izglītībā. CERT.LV pārstāvis piedalījās kategorijas *Labākā kiberdrošības pratības iniciatīva* pretendentu vērtēšanā. Balvu šajā kategorijā šogad ieguva *Finanšu nozares asociācija* par informatīvo kampaņu drošības attālināto finanšu pakalpojumu izmantošanas veicināšanai *Neuzķeries! Esi gudrāks par krāpniekiem!*

8. decembrī CERT.LV organizēja IT drošības semināru valsts un pašvaldību iestāžu atbildīgajām personām par IT drošību, pamatpakalpojumu sniedzējiem, digitālo pakalpojumu sniedzējiem, kā arī citiem interesentiem, kuri darbojas IT drošības jomā. Seminārā tika aplūkotas tādas tēmas kā kritiskās infrastruktūras darbības nepārtrauktības plānošana, kiberdrošības krīzes plāns un krīzes simulācijas, rezerves kopiju pareiza izveide un glabāšana, domēnu vārdi administratīvi teritoriālās reformas kontekstā, spēles izmantošana kiberdrošības apmācībās un atskats uz 2021. gada kiberdrošības notikumiem. Pasākumam tiešsaistē pieslēdzās 386 dalībnieki. (https://cert.lv/lv/2021/11/it-drosibas-seminars-esi-dross-decembri)

CERT.LV pārstāvji piedalījās arī vairākos ar karjeru un izaugsmi saistītos pasākumos, stāstot jauniešiem par zināšanām un prasmēm, kas nepieciešamas, darbojoties kiberdrošības jomā, un potenciālajiem izaicinājumiem kibervidē.

Pārskata periodā CERT.LV par IT drošību izglītoja 5414 cilvēkus, iesaistoties 38 izglītojošos pasākumos.



9. attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2021. gada 4. ceturksnī

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

Sadarbības tikšanās, konsultācijas un prezentācijas:

- CERT.LV piedalījās Aizsardzības ministrijas informatīvā ziņojuma *Par valsts kiberdrošības pārvaldības uzlabošanu* sagatavošanā, kurš valsts kibertelpas stiprināšanai un ar kiberdrošību saistītu jautājumu koordinācijas nodrošināšanai, jo īpaši jaunā Eiropas Savienības regulējuma (NIS2 direktīvas) kontekstā, paredz Nacionālā kiberdrošības centra izveidi.
- Dalība Ministru kabineta noteikumu, kas saistīti ar *Elektronisko sakaru likumu*, veidošanas darba grupā, kurā CERT.LV savas kompetences ietvaros sniedza komentārus par vēlamo rezultātu topošo Ministru kabineta noteikumu sakarā.
- CERT.LV sagatavoja priekšlikumus un iesniedza Aizsardzības ministrijai saistībā ar Latvijas kiberdrošības stratēģijas izstrādi 2023.-2026. gadam.
- CERT.LV turpināja projekta par valkājamo ierīču drošību norises vadību. Sadarbībā ar LUMII Mākslīgā intelekta laboratoriju un Elektronikas un datorzinātņu institūtu (EDI) tika turpināta tehniskā prototipa koncepta izstrāde.
- Dalība sanāksmē par sagaidāmajām drošības prasībām komersantiem, lai pieslēgtos *Atvieglojumu vienotās informācijas sistēmai*.

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

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

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 tika iecelta par šīs darba grupas līdzpriekšsēdētāju.
  - *Maturity* darba grupā, kura rūpējas par ES dalībvalstu CSIRT komandu brieduma līmeņa paaugstināšanu.
  - *TOR Review* darba grupā, kas pārskata tīkla statūtus un nolikumu, atbilstoši tos aktualizējot.
- 10.-12. novembrī CERT.LV pārstāvji piedalījās *15th CSIRTs Network meeting* Ļubļanā, Slovēnijā, aktīvi diskutējot par jaunākajām likumdošanas iniciatīvām.
- 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.
- Dalība ENISA Eiropas kiberdrošības indeksa (*EU Cybersecurity index*) darba grupā, kurā tiek izstrādāta kiberdrošības indeksa vērtības aprēķina metodoloģija dalībvalstu

kiberdrošības novērtēšanai. Tika sniegti komentāri par dalībvalstu izskatīšanai nodoto indeksa indikatoru aprēķina metodoloģiju.

- 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.

- Turpinājās aktīva dalība enerģētikas informācijas apmaiņas un sadarbības grupā *Energy ISAC Camelot*, lai veicinātu informācijas apmaiņu un sekmētu enerģētikas sektora kiberdrošību.

- Dalība NATO CCDCoE ikgadējo tehnisko sarkano komandu kiberdrošības mācību *Crossed Swords 2021* galējā plānošanā, darbs pie mācību vides tehnisko elementu izstrādes, mācību izpildes koordinācija, industriālo vadības sistēmu uzbrukuma scenārija vadīšana. Mācības paredzētas ne tikai ielaušanās testētāju, digitālās kriminālistikas un apdraudējumu ekspertu tehnisko prasmju pilnveidei, bet arī vadītprasmju papildināšanai. CERT.LV pārstāvis piedalījās arī mācību izspēlē, kas notika 7.-9. decembrī, vadot vienu no mācību komandām. Mācībās piedalījās gandrīz 100 dalībnieki no 21 valsts.

- Gatavošanās dalībai NATO CCDCoE organizētajām kiberdrošības mācībām *Locked Shields 2022*. Uzsākta partneru uzrunāšana kopīgas komandas veidošanai.

- 1. oktobrī dalība ENISA rīkotajās Eiropas CERTu tīkla mācībās CyberSOPex 2021, lai paaugstinātu dalībnieku gatavību reaģēt liela apjoma pārrobežu incidenta gadījumā.

- 10. novembrī CERT.LV vadīja TF-CSIRT starptautisko CERT komandu sabiedrisko attiecību speciālistu darba grupas (*CERTS PR Working Group*) sanāksmi, kuras ietvaros CERTu pārstāvji informēja par aktuālajiem izaicinājumiem kiberdrošības izpratnes veicināšanas jomā, dalījās pieredzē par kampaņu organizēšanu un sniedza ieteikumus veiksmīgākas komunikācijas organizēšanai.

- 29.11. – 03.12. dalība NATO organizētajās kiberdrošības mācībās *Cyber Coallition 2021*. Mācību mērķis ir veicināt sadarbību - alianses dalībnieku un partneru veiktās aktivitātes tika vērstas uz kopīgu mērķu sasniegšanu, lai tādējādi pilnveidotu spējas novērst un atvairīt apdraudējumus kibertelpā un sniegtu ieguldījumu alianses izaugsmē. Mācībās piedalījās 1000 dalībnieki, kas pārstāvēja 30 NATO sabiedrotos, vairākus partnerus un Eiropas Savienību.
- 3. decembrī dalība Eiropas Kiberdrošības kompetences centra (*European Cyber security Competence Centre, ECCC*) sanāksmē par SOC (*Security Operation Centres*) idejas tālāku virzību, lai veicinātu Eiropas līmeņa informācijas apmaiņu par aktuālajiem apdraudējumiem kibertelpā saskaņā ar ES Kiberdrošības stratēģiju.
- 7. decembrī dalība ENISA organizētajā sanāksmē par apvienotās kiberdrošības vienības (*Joint Cyber Unit*, *JCU*) veidošanu. Valstu pārstāvji piedalījās diskusijā, daloties pieredzē, informējot par līdz šim izmantotajiem rīkiem un uzsāktajiem projektiem, lai sekmētu vienības izveidi ar skaidri definētiem uzdevumiem un darbības principiem. Vienības mērķis ir sekmēt koordinētu Eiropas līmeņa atbildes reakciju apjomīga kiberdrošības apdraudējuma gadījumā.

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.

2021. gada 4. ceturksnī CERT.LV turpināja darbu pie *Grafoskopa* izstrādes, tā attīstīšanas un pilnveidošanas. 2021. gada 9. decembrī tika publicēta *Grafoskopa* atvērtā koda licence, lai arī citi projekta partneri varētu rīku testēt, novērtēt un sniegt priekšlikumus uzlabojumiem. Rīks publiski pieejams https://github.com/cert-lv/graphoscope. Pārskata periodā CERT.LV piedalījās attālinātās JTAN projekta sanāksmēs.

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 Excange 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 desmit 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.

2021. gada 4. ceturksnī projekta ietvaros CERT.LV darbinieks pieredzes apmaiņas vizītē devās uz Poliju, kur 3 dienu laikā tika apskatīta un analizēta pikšķerēšanas incidentu automatizācija, kā arī iepazīti citi incidentu automatizācijas rīki un CERT.PL pieredze kiberdrošības incidentu apstrādē. Vizītes rezultātā tika uzlabotas attiecības starp CERT.LV un CERT.PL komandām, kas ir ļoti noderīgi gan ikdienas sadarbībai, gan kopīgu projektu un aktivitāšu īstenošanai.

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, kredītkaršu datu zādzībām, viltus kurjerkompāniju tīmekļa vietņu apmeklējuma, kā arī tika liegts inficētām iekārtām sazināties ar vīrusu kontroles serveriem. Kopējais bloķēto domēnu skaits:
  - Oktobrī – 120934
  - Novembrī – 117671
  - Decembrī - 228368

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.

- Saruna ar Jēkabpils Agrobiznesa koledžu par mācību programmas izveidi kiberdrošības speciālistu apmācībai un potenciālo CERT.LV speciālistu iesaisti.
- Tika uzstādīts jauns publiskais pirmā līmeņa (*Stratum 1*) NTP laika serveri. Serveris saņem precīzu laiku no GPS un tajā iebūvēts oscilators, kura kļūda ir ne vairāk kā 1.6s gada laikā. Līdz ar jauno serveri CERT.LV nodrošina kopā 3 publiskos NTP serverus, no kuriem 2 ir pirmā līmeņa un viens - otrā līmeņa serveris. Visi serveri ir pievienoti Latvijas NTP serveru kopai "lv.pool.ntp.org". CERT.LV rekomendē izmantot šo kopu kā precīzā laika avotu.
- 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 sertificētu uzticamības pakalpojumu sniedzēju darbību, kā arī sniedza prezentāciju Lietuvas eIDAS uzraudzības iestādes organizētajā konferencē *DigiT Baltic 2021* par DDUK kā eIDAS uzraudzības iestādi Latvijā.

9. 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 01.10.2021. līdz 31.12.2021. ir saņēmusi un izvērtējusi 3162 ziņojumus. No tiem 2973 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 5 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 17 ziņojumos konstatēta personas goda un cieņas aizskaršana, 2 ziņojumi saņemti par naida runu un 4 ziņojumi par vardarbību atainojošiem materiāliem. Par finanšu krāpšanas mēģinājumiem internetā saņemti 49 ziņojumi, 74 ziņojumu saturs nav bijis pretlikumīgs, 38 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 2785 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 14 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 2785 ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem 2738 ziņojumi ir dzēsti no publiskas aprites un 47 ziņojuma saturs atrodas dzēšanas procesā sadarbībā ar Valsts policiju un interneta pakalpojumu sniedzējiem.

2022. gada 2. februārī

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