Latvijas Universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

Līdzfinansē Eiropas Savienības Eiropas
infrastruktūras savienošanas instruments

# Publiskais pārskats par CERT.LV uzdevumu izpildi

## 2020

2020. gada 1. ceturksnis (01.01.20120 – 31.03.2020.)

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*

2020. gada 1. ceturksnī tika reģistrētas 204 508 unikālas apdraudētas IP adreses, kas ir par nepilniem 2% vairāk nekā iepriekšējā ceturksnī un par 6% vairāk nekā šajā pašā periodā pirms gada.

Pārskata periodā Latvijas interneta telpā izplatītākie apdraudējumi:

- konfigurācijas nepilnības (112 354 unikālas IP adreses) ar kāpumu 1% pret iepriekšējo periodu;
- otrs izplatītākais bija ļaundabīgs kods (18 586 unikāla IP adrese) a kāpumu 12%;
- bet trešais - ielaušanās mēģinājumi (2510 unikālas IP adreses) ar kāpumu 28%.

Lai arī pārskata periodā fiksēti atsevišķi ļaunatūras izplatīšanas mēģinājumi un huligāniska rakstura maldinošu informāciju izplatošas kampaņas WhatsApp lietotnē, kopumā kiberdrošības apdraudējuma līmenis COVID-19 pandēmijas apstākļos vērtējams kā mērens, ar apdraudējuma paaugstināšanos attālā darba raksturīgajām tehnoloģijām un attālā darba un infrastruktūras vadības apstākļiem, kas skaidrojams ar lielu mājās strādātāju skaita palielināšanos, kam tiek pielāgoti arī konkrēti kiberuzbrukumi.

Pārskata periodā aktīvi turpinājās gan uz Smart-ID lietotājiem vērstas krāpnieciskas aktivitātes, gan pikšķerēšanas kampaņas dažādu Latvijā operējošu banku klientiem (Citadele, Swedbanka, SEB). Lielākajā daļā krāpniecības incidentu, kuros cietuši Smart-ID klienti, ir secināms, ka klients neizprot pakalpojuma loģiku un funkcijas, kas, savukārt, paver iespējas noziedzniekiem manipulēt ar klientu un sekmīgi izkrāpt finanšu līdzekļus no Smart-ID iespējotiem banku kontiem. Piemēri sekmīgiem krāpniecības paņēmieniem: a) Krāpnieki sazinās ar klientu, uzdodoties par Smart-ID tehnisko atbalstu un pārliecina izpildīt konkrētas darbības, lai pārņemtu kontu; b) pikšķerēšanas kampaņas, kuru ietvaros klients pats nodod Smart-ID autentifikācijas līdzekļus krāpniekiem, neizprotot nedz to, ka notiek pikšķerēšanas uzbrukums, nedz paša Smart-ID pakalpojuma būtību. CERT.LV uzskata, ka finanšu iestādes nav pietiekami skaidrojušas klientiem Smart-ID pakalpojuma loģiku.

Pārskata perioda galvenā iezīme bija ārkārtas stāvokļa izsludināšana valstī un ar to saistītā nepieciešamība nodrošināt iespēju darbiniekiem veikt darbu attālināti.

Gan iestādes, gan uzņēmumi saskārās ar būtiskiem lēmumiem, kas saistīti gan ar infrastruktūras attālinātas pieejamības nodrošināšanu, gan ar iespējām nodrošināt atbilstošas iekārtas un risinājumus katram individuālam darbiniekam. Pieaugums IP adrešu apjomā, kurās konstatētas iekārtas ar *OpenRDP* ievainojamību, norāda uz neatbilstoši konfigurētu iekārtu izmantošanu ar attālināto pieslēgumu. Šādas iekārtas, bez atbilstošas aizsardzības, pakļauj gan individuālo lietotāju, gan infrastruktūru, kurai tās attālināti pieslēdzas, uzbrukumu un rezultātā arī datu zudumu riskam.

Ar ārkārtas situāciju saistītā iedzīvotāju apziņošana daļā iedzīvotāju radīja satraukumu un neizpratni izvēlēto metožu un ziņojumu sagatavošanas dēļ. Iedzīvotājiem likās aizdomīgas gan īsziņās saņemtās ej.uz saites, kas slēpj patieso galamērķi un netika asociētas ar valsts pārvaldi, gan CSDD izsūtītie PDF dokumenti, kas ir arī uzbrucēju vidū plaši izmantots ļaunatūras izplatīšanas paņēmiens, gan fakts, ka apziņošanai bija nepieciešamas vairākas dienas, kamēr tā sasniedza visus adresātus.

Meklējot informāciju gan par ārkārtas stāvokli, gan COVID-19 izplatību, lietotāji saskārās ar sarežģījumiem uzticama informācijas avota izmantošanā – SPKC tīmekļa vietnes darbībā bija vērojami traucējumi. CERT.LV sadarbībā ar tīmekļa vietnes uzturētāju veica situācijas analīzi,

secinot, ka tehniskā informācija nesatur uzbrukuma pazīmes. Tika veikti optimizācijas darbi vietnes noslodzes sadalīšanai un veiktspējas uzlabošanai.

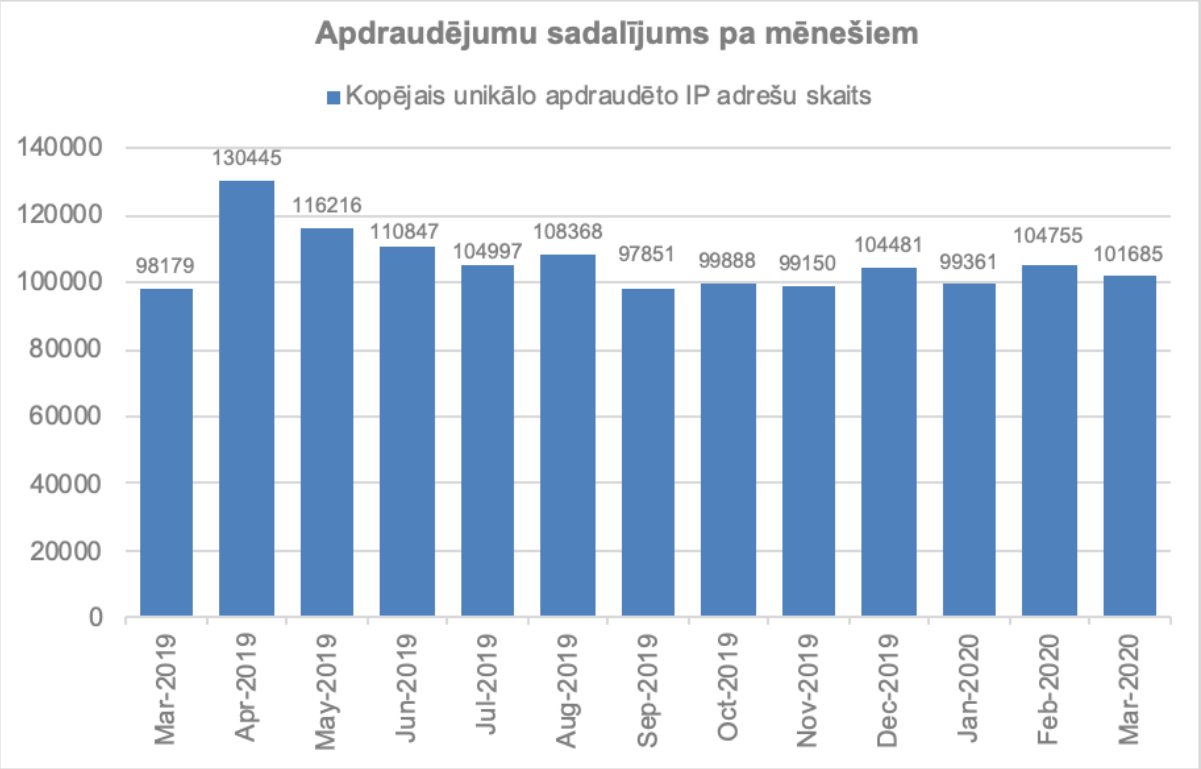
Novēroti arī e-veselības un e-klases darbības traucējumi, kas saistīti ar leģitīmu palielinātu noslodzi.

Pārskata periodā CERT.LV par IT drošību izglītoja 3324 cilvēkus, iesaistoties 39 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 tagad 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 infekciju (piemēram, *Confiker*, *Zeus*, *Mirai*) un ievainojamību (piemēram, *Opendns*, *Openrdp*) tipiem.

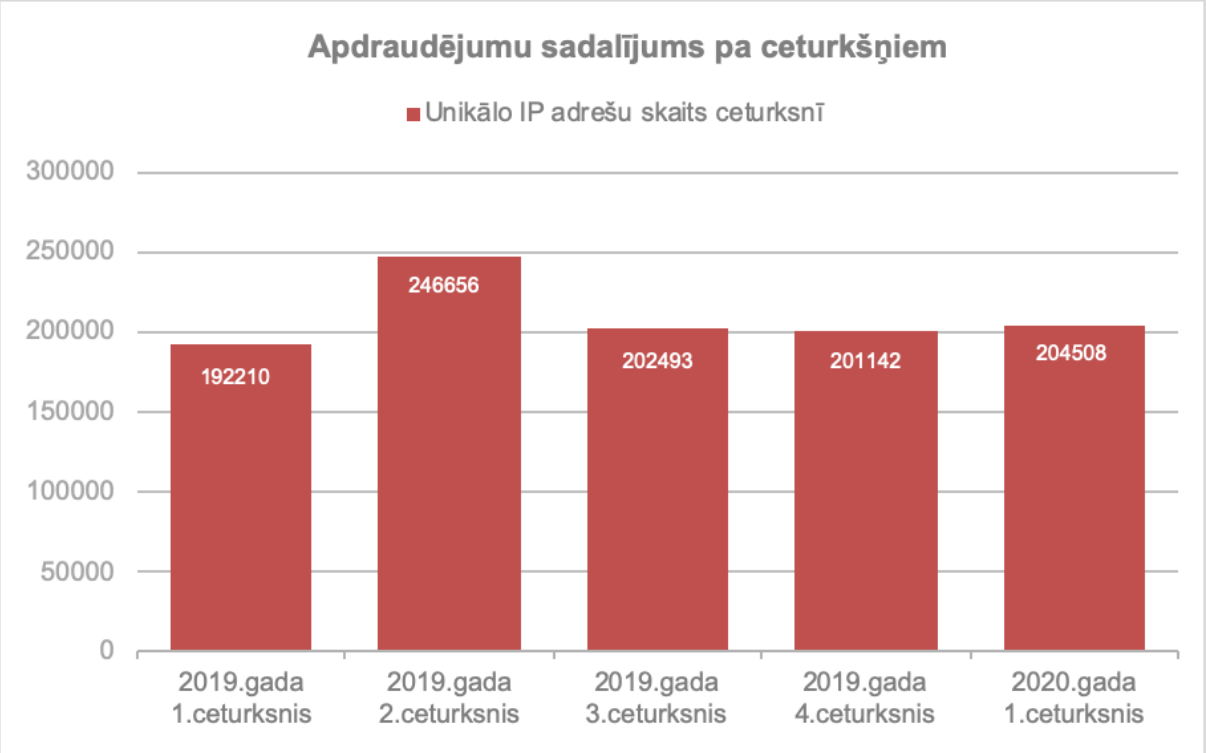
CERT.LV pārskata periodā ik mēnesi apkopoja informāciju par 100 000 – 105 000 ievainojamu unikālu IP adrešu.



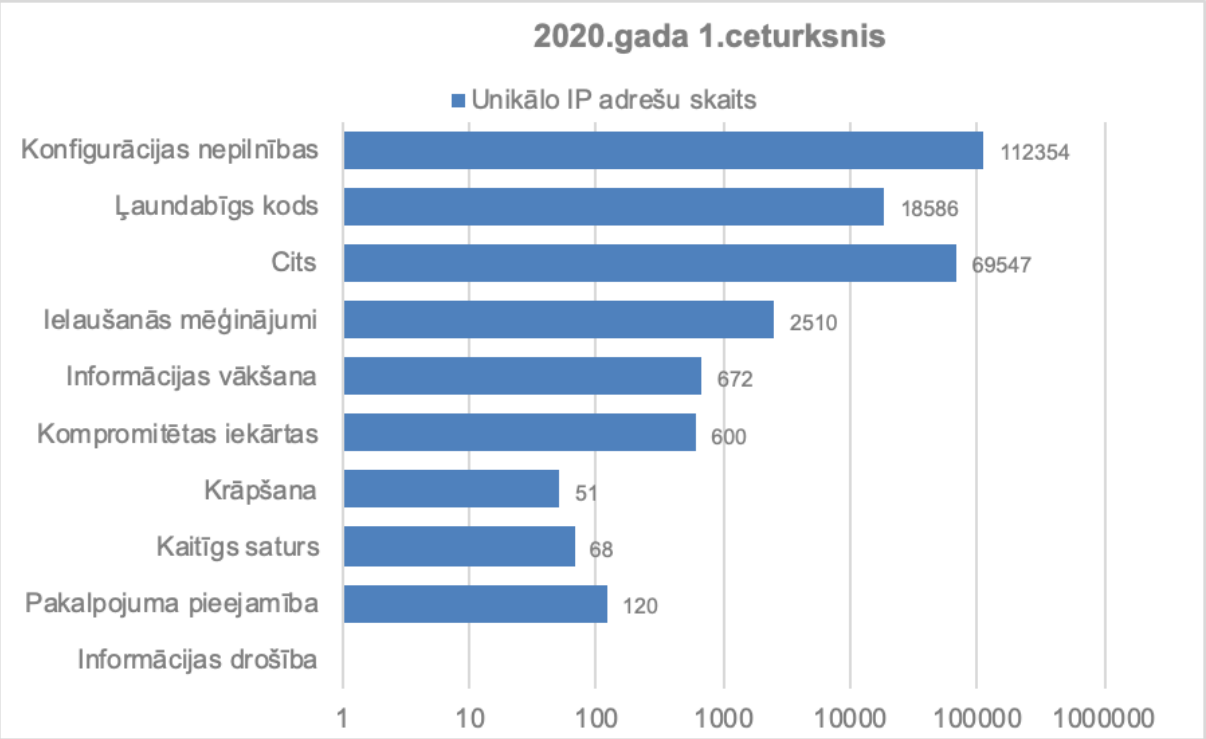

1.attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa mēnešiem 12 mēnešu griezumā.

2020. gada 1. ceturksnī tika reģistrētas 204 508 unikālas apdraudētas IP adreses, kas ir par nepilniem 2% vairāk nekā iepriekšējā ceturksnī un par 6% vairāk nekā šajā pašā periodā pirms gada.

Pārskata periodā nav vērojamas būtiskas izmaiņas mēnesī reģistrēto apdraudēto IP adrešu daudzumā.

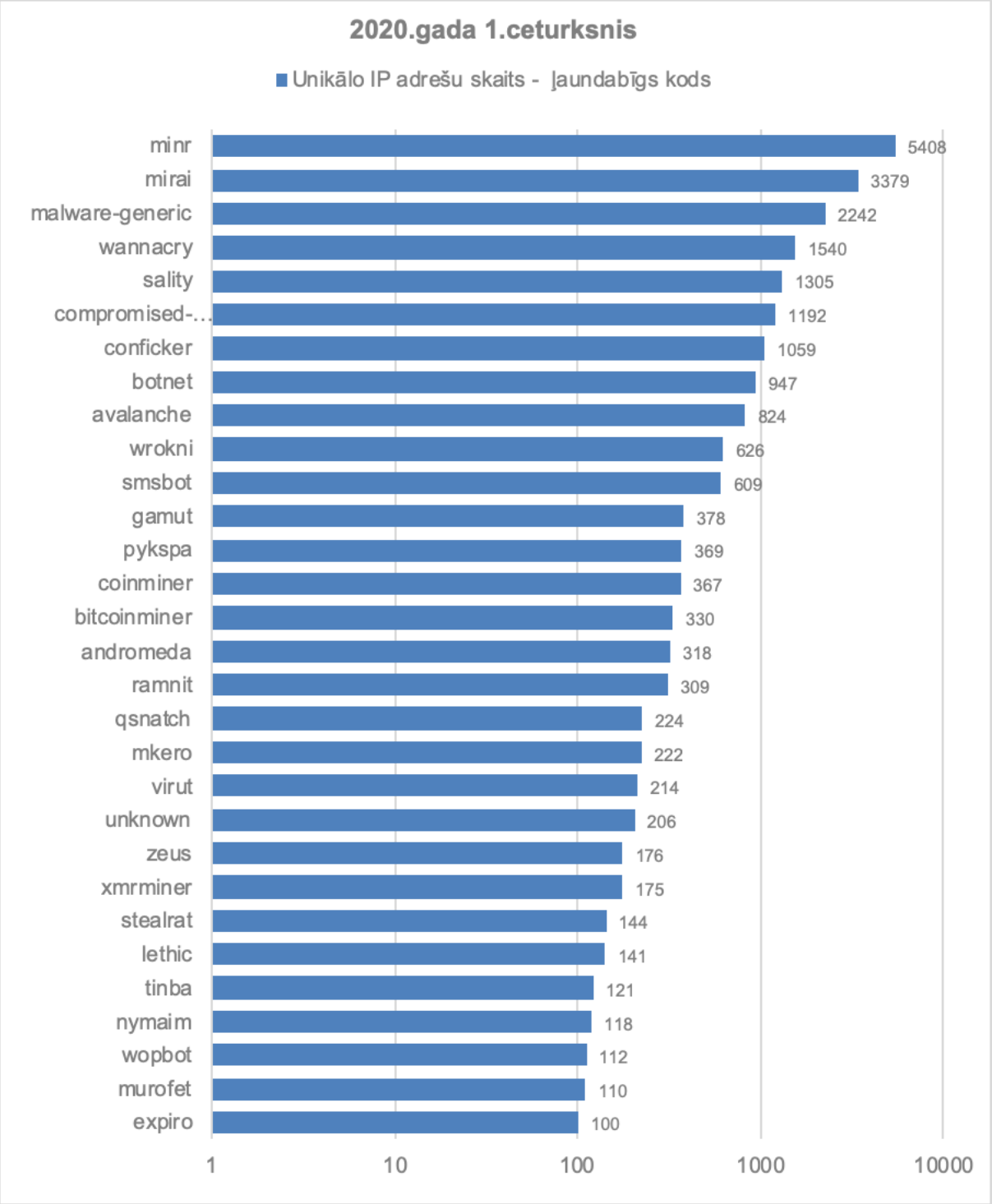



2.attēls – CERT.LV reģistrētās apdraudētās IP adreses pa ceturkšņiem 2019. un 2020. gadā.




3.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2020. gada 1. ceturksnī pa apdraudējumu veidiem.

Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (112 354 unikālas IP adreses) ar kāpumu 1% pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs kods (18 586 unikālas IP adreses) a kāpumu 12%, bet trešais - ielaušanās mēģinājumi (2510 unikālas IP adreses) ar kāpumu 7%.

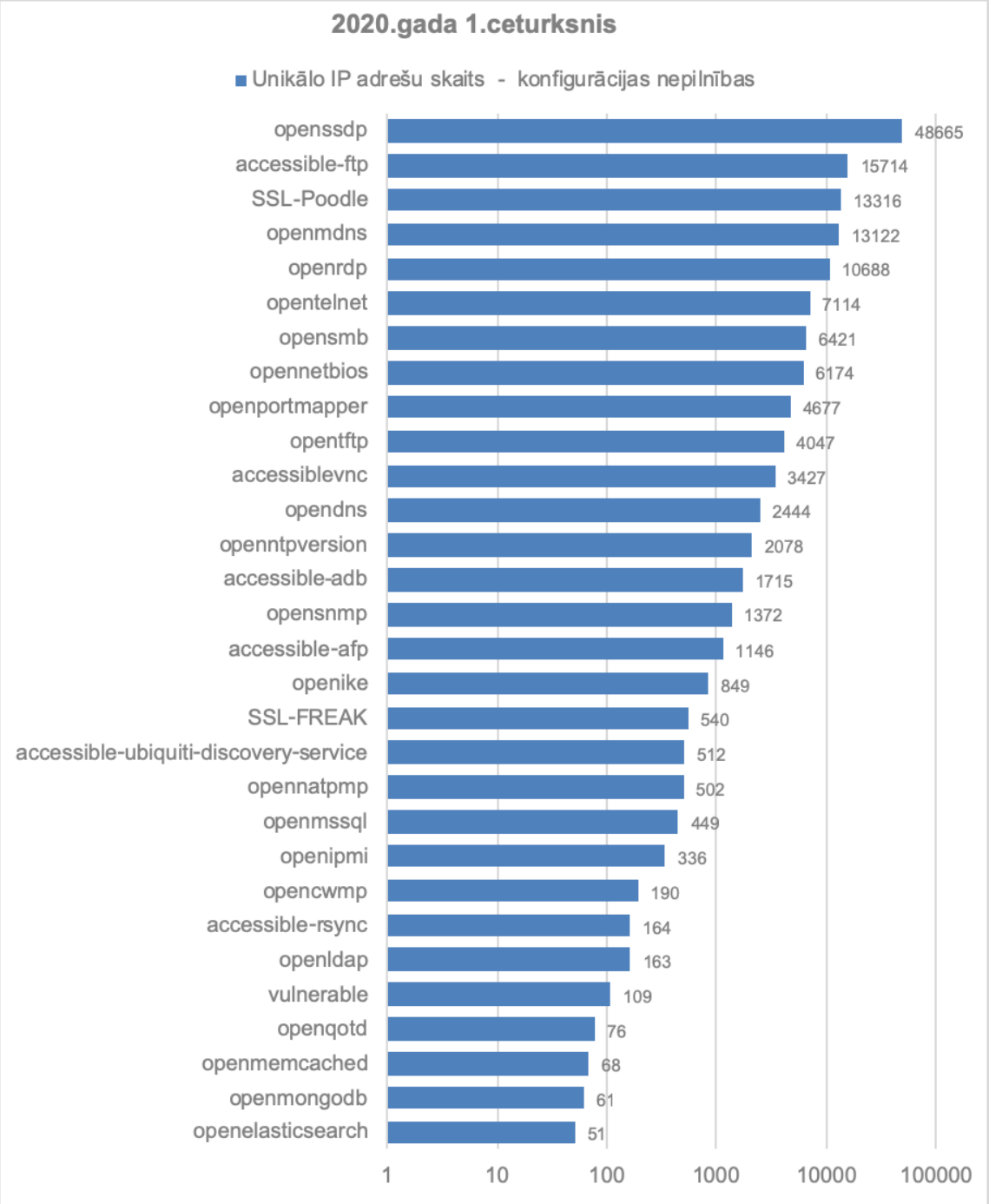



4.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2020. gada 1. ceturksnī ar apdraudējuma veidu - ļaundabīgs kods.

Ļaunatūras topā ir atgriezušies kriptovalūtas ieguves rīki. Viens no šādiem rīkiem – *Minr* ļaunatūra, kas šajā ceturksnī ir arī topa jaunpienācēja – ierindojas topa pirmajā vietā. Kriptovalūtas ieguves jeb "rakšanas" rīki bieži vien tiek ievietoti uzlauztās tīmekļa vietnēs un noslogo apmeklētāja iekārtu, nesankcionēti izmantojot iekārtas jaudu kriptovalūtas ieguvei,

tādejādi pakļaujot iekārtu pārslodzes riskam. Šo rīku popularitāte, iespējams, skaidrojama ar prognozēto *bitcoin* (BTC) vērtības kāpumu maijā un ar to saistītajām gaidāmajām tirgus izmaiņām.

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

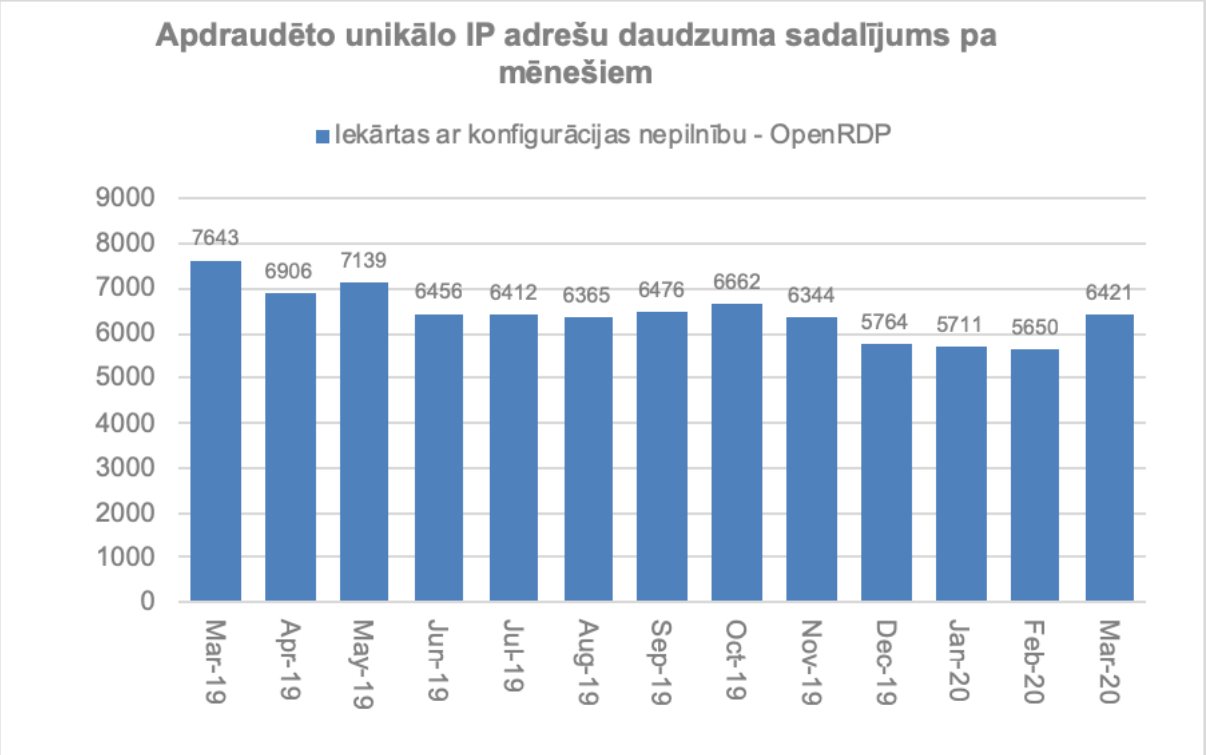



5.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2020. gada 1. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

Pirmo vietu konfigurācijas nepilnību topā ieņem *OpenSSDP* – iekārtas ar nedrošu konfigurāciju, kas var tikt izmantotas apjomīgos piekļuves atteices (DoS) uzbrukumos. *Simple Service Discovery Protocol* (SSDP) ir iebūvēts daudzās tīkla iekārtās, lai tās veiklāk varētu „atrast" viena otru un savstarpēji sazināties. Neliels šīs ievainojamības apjoma pieaugums vērojams martā. Iespējams, tas saistīts ar ārkārtas stāvokļa izsludināšanu valstī, kas mudinājis iedzīvotājus sekot aicinājumam palikt mājās un meklēt alternatīvus darba un atpūtas risinājumus, pieslēdzot tīklam līdz šim novārtā atstātas un nepienācīgi aizsargātas iekārtas.

Arī konfigurācijas nepilnība *OpenRDP* pārskata periodā joprojām atrodas topa augšgalā. Tā bieži tiek izmantota, lai piekļūtu iekārtām un tās sašifrētu. 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 pietiekami uzstādīta droša piekļuves parole.

Lai arī šādu gadījumu mazināšanai CERT.LV veica regulāru neatbilstoši konfigurēto iekārtu īpašnieku apziņošanu, un vairāku mēnešu garumā bija vērojams stabils *OpenRDP* ievainojamību samazinājums, martā, visticamāk saistībā ar attālinātā darba organizēšanas nepieciešamību valsts mērogā, atkal vērojams ievainojamo iekārtu kāpums – pieaugums 14% salīdzinājumā ar februāri (5.1. att.).



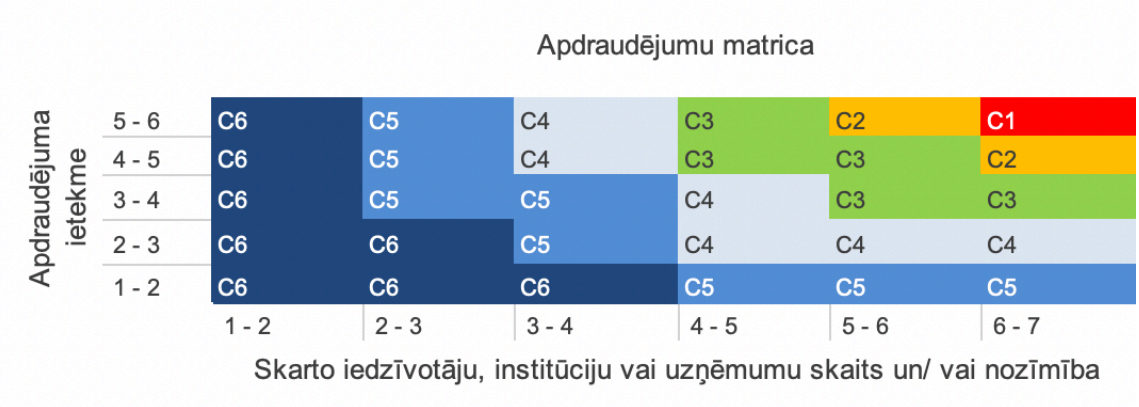

5.1.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2020. gadā ar konfigurācijas nepilnību *OpenRDP*.

Pilnvērtīgākam kibersituācijas novērtējumam CERT.LV pirmajā ceturksnī ir uzsācis Apvienotās Karalistes Nacionālā kiberdrošības centra (NCSC) izveidotās apdraudējumu matricas adaptāciju. 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 abus faktorus, apdraudējumi tiek iedalīti 6 kategorijās:

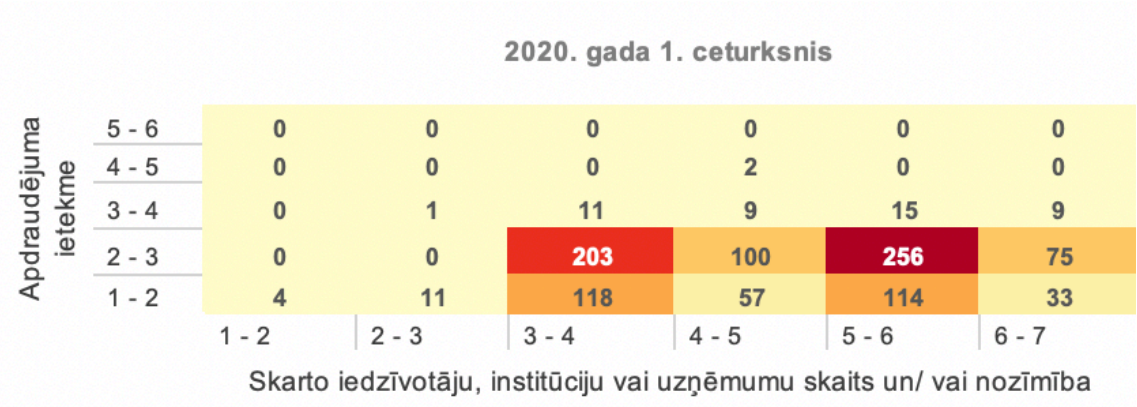
C1 – nacionāla līmeņa apdraudējums, ietekmēta pamatpakalpojumu sniegšana, apdraudēta ekonomiskā vai politiskā stabilitāte;

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.

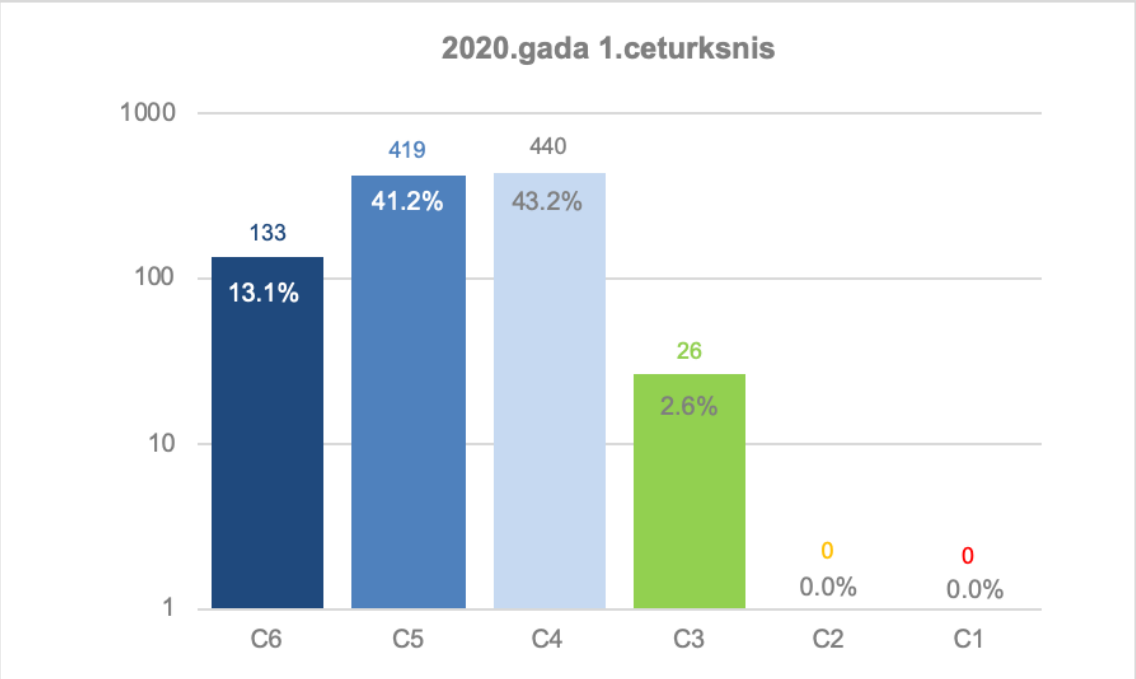
Jāuzsver, ka matrica šobrīd vēl ir ieviešanas stadijā un turpinās incidentu kategorizēšana pēc to nozīmīguma, kā arī skarto IP adrešu kategorizēšana pēc to piederības.




6. attēls – Apdraudējumu matricas sadalījums kategorijās.




7. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu izvietojums matricā 2020. gada 1. ceturksnī valsts un pašvaldību institūcijās.




8. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu sadalījums apdraudējumu kategorijās [1] pēc apdraudējuma ietekmes (matrica) 2020. gada 1. ceturksnī valsts un pašvaldību institūcijās.

7. un 8. attēlā redzams daļas no incidentiem, kas notikuši februārī un martā valsts un pašvaldību iestādēs, sadalījums pēc to svarīguma.

50% apdraudējumu ietilpst mērenu vai maznozīmīgu apdraudējumu kopā (C5 un 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 2,6% (26 unikālas apdraudētas IP adreses/gadījumi) no visiem kategorizētajiem apdraudējumiem. Kategoriju veido:

- Galvenokārt *Minr* ļaunatūra (kriptovalūtu ieguves rīks), kuras darbība fiksēta vairāku pašvaldību un uzņēmumu IP adresēs. Konkrētais apdraudējums tiek fiksēts, lietotājam apmeklējot ar ļaundabīgo kodu *Minr* aprīkotu-inficētu tīmekļa vietni, kuras apmeklējuma laikā lietotāja iekārta tiek nesankcionēti izmantota kriptovalūtas ieguvei, iespējams, pārslogojot iekārtas resursus.
- Kā arī *Emotet* ļaunatūras (sensitīvas informācijas vākšanai un citu ļaunatūru izplatīšanai), *Andromeda* ļaunatūras (citu ļaunatūru izplatīšanai, parasti informācijas ieguves nolūkos), *Conficker* ļaunatūras (novecojusi, viegli "ārstējama" ļaunatūra, kas ietekmē Windows iekārtas – lai arī nenodara būtisku kaitējumu, norāda uz ievainojamu, neatjauninātu iekārtu esamību) *Mkero* mobilās ļaunatūras (veic lietotāja parakstīšanu uz maksas servisiem) un *WannaCry* šifrējošā izspiedējvīrusa, kura izplatība joprojām turpinās, kaut arī tā postošo ietekmi lielā mērā ir apturējušas tiesībsargājošās iestādes, kaitīgā koda klātbūtne tika konstatēta atsevišķās pašvaldībās un uzņēmumos.

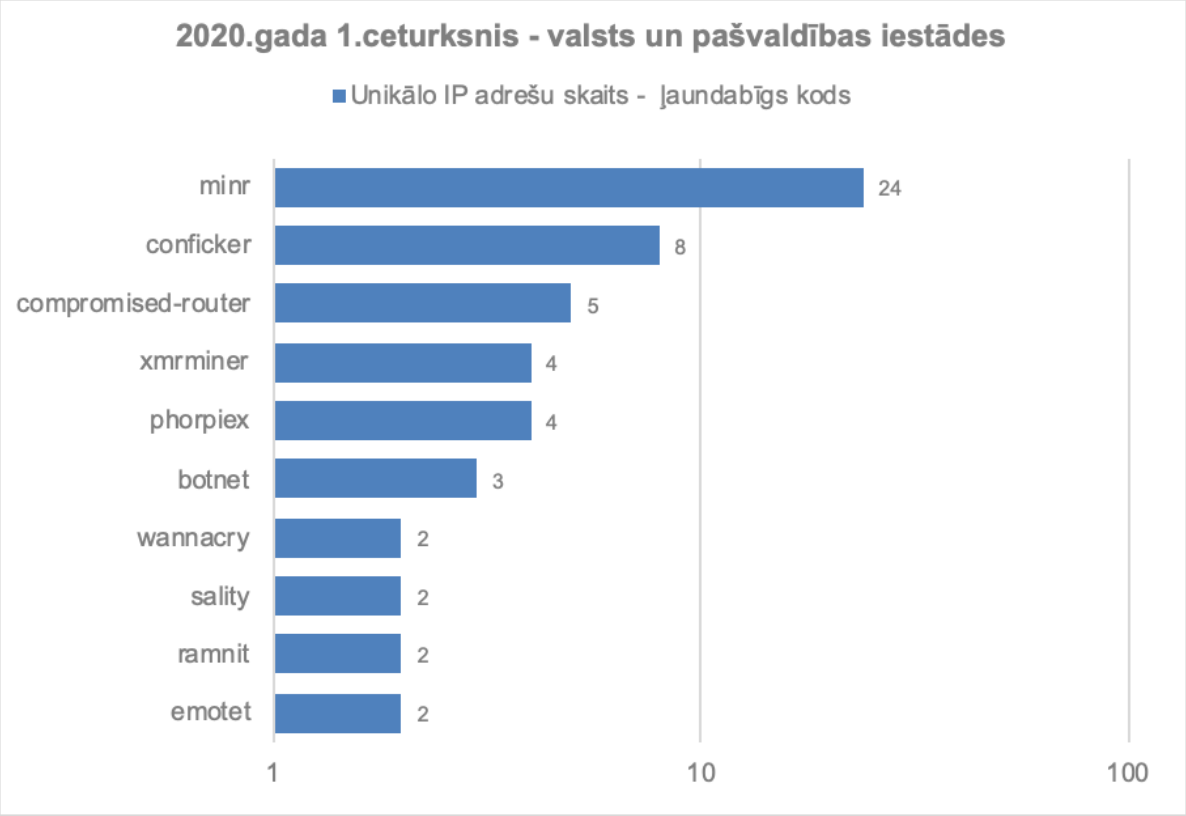
Lai samazinātu kopējo apdraudēto IP adrešu skaitu, CERT.LV kopā ar Latvijas Interneta

[1] Tiek apkopota informācija par valsts iestādēm, valsts kapitālsabiedrībām, pašvaldībām, pašvaldību kapitālsabiedrībām un citām valsts iestādēm (Ģenerālprokuratūra, NEPLP u.c.).

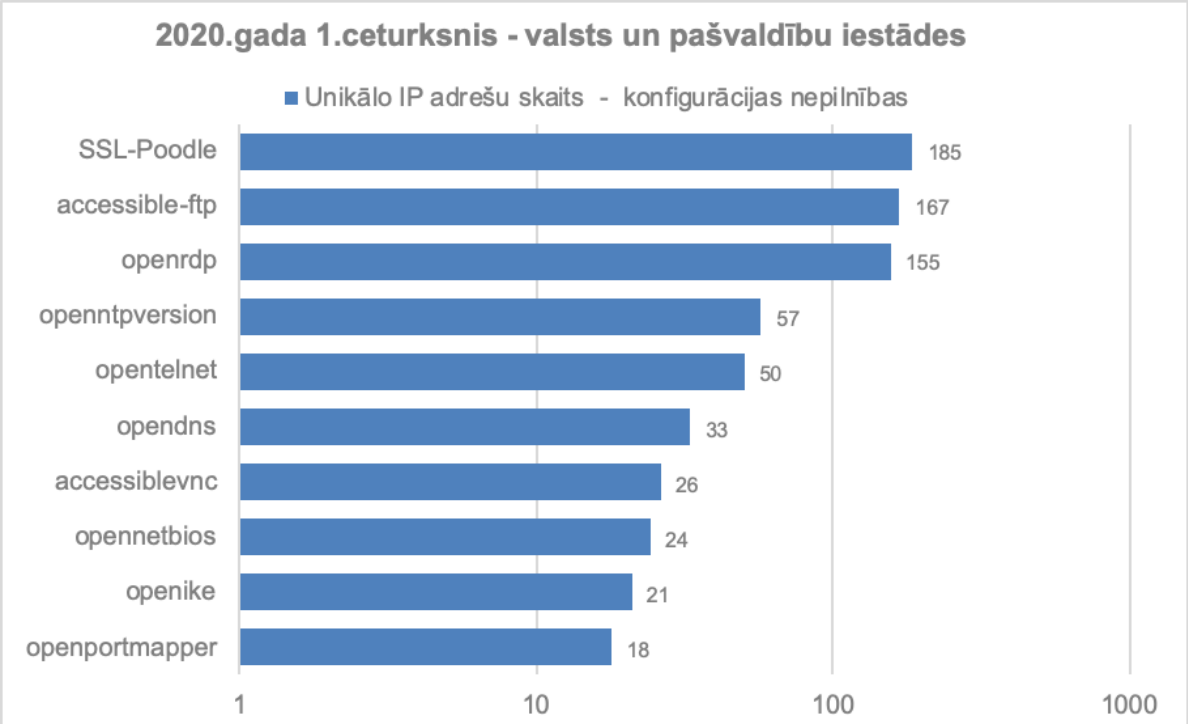
asociācijas (LIA) Net-Safe Latvija Drošāka interneta centru ir izveidojuši saprašanās memorandu, kas tiek slēgts ar interneta pakalpojumu sniedzējiem (IPS), kas vēlas pievienoties iniciatīvai „Atbildīgs interneta pakalpojumu sniedzējs" un informēt savus klientus par to iekārtās konstatētajiem apdraudējumiem. Atbildīgo IPS skaits līdz pārskata perioda beigām saglabājās bez izmaiņām – 13.

## 2. Atbalsts informācijas tehnoloģiju drošības incidentu novēršanā vai to novēršanas koordinēšanā.

CERT.LV apkopo informāciju no valsts un pašvaldību institūcijām par to izmantotajām IP adresēm un tīmekļa vietnēm, lai CERT.LV varētu operatīvāk reaģēt šo iestāžu IT drošības incidentu gadījumos. CERT.LV informē valsts un pašvaldību institūcijas, ja viņu IP adreses uzrādās kādā no ziņojumiem kā apdraudētas.




9.attēls - CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2020.gada 1.ceturksnī ar apdraudējuma veidu – Ļaundabīgs kods.




10.attēls - CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2020.gada 1. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

CERT.LV uzskaita arī kompromitēto un izķēmoto tīmekļa vietņu gadījumus. Pārskata periodā tika fiksētas 25 kompromitētas un izķēmotas tīmekļa vietnes. 23 gadījumos izķēmotās vietnes uzturēšanai tika izmantota Linux operētājsistēma, 1 gadījumā – Windows, bet par vienas vietnes operētājsistēmu nav informācijas. Neviena no izķēmotajām vietnēm pēdējā gada laikā nav izķēmota atkārtoti.

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

## Krāpšana

Tika saņemta informācija par krāpniecisku kampaņu, kas vērsta pret Smart-ID lietotājiem ar mērķi piekļūt lietotāju kontiem. Krāpnieciskos nolūkos lietotājiem tika izsūtīti e-pasti it kā Smart-ID tehniskā atbalsta vārdā. E-pastā tika paziņots par kritiskām kļūdām lietotāja Smart-ID kontā, un lietotājs aicināts sazināties ar tehniskā atbalsta dienestu pa e-pastā norādīto tālruni.

Turpinājās maldinošas reklāmas sociālajos tīklos, kurās tika izmantotas Latvijā pazīstamas personas, lai aicinātu ieguldīt naudu kriptovalūtā. Reklāmas novirzīja lasītāju uz vietnēm, kas vizuāli atgādināja kādu no populārajiem ziņu portāliem.

Kāds Latvijas iedzīvotājs, pēc iepazīšanās ar reklāmas materiāliem Facebook, nolēma iesaistīties valūtu tirdzniecībā, izmantojot reklamēto platformu Dream Equity MT4 terminal, nepārbaudot pie Finanšu un kapitāla tirgus komisijas (FKTK), vai attiecīgā kompānija ir tiesīga darboties Latvijā. Pēc pieteikuma aizpildīšanas ar lietotāju sazinājās "menedžeris", tika pieprasītas un nosūtītas dažādu dokumentu kopijas, uzinstalēta uz datora papildu programmatūra, kas ļautu finanšu konsultantam asistēt darbībās ar investīciju platformu, tika uzsākta investēšana. Lai arī sākotnēji darījumi bija šķietami veiksmīgi, kādā brīdī lietotāja

kontā bija negatīva bilance, un finanšu konsultants mudināja veikt aizņēmumus, "jo lielākus, jo labāk", lai labotu situāciju. Tika ņemti kredīti bankā, bet, kad banka atteicās piešķirt papildu līdzekļus, tika veikti aizņēmumi no paziņām, taču arī šīs summas tika zaudētas. Lietotāja konts platformā tika nobloķēts. Pēc "konsultanta" jautājuma par tālāko rīcību un lietotāja atbildes par papildu finanšu neesamību, komunikācija ar platformas pārstāvjiem pārtrūkusi. Lietotājs krāpnieciskajā platformā zaudēja vairāk kā 60 000 eiro. Ar vēlmi atgūt izkrāptos līdzekļus, lietotājs vērsies pie internetā uzietas juridisko pakalpojumu kompānijas EGIDA, kas norādījusi, ka ir pieredze līdzīgās lietās, un solījusi palīdzēt līdzekļus atgūt. Pēc sadarbības ar "juristiem" un "valūtas kontroles pārstāvjiem", kā arī maksām par pakalpojumiem, konvertācijām, pārvedumiem lietotājs atskārtis, ka arī šī ir krāpniecība. Kopumā tika pazaudēti vairāk nekā 70 000 eiro. Lietotājs vērsies ar iesniegumu policijā.

Marta otrajā pusē daļa Latvijas iedzīvotāju saņēma krāpnieciskus šantāžas e-pastus, šoreiz latviešu valodā. Tajos apgalvots, ka ļaundaris par lietotāju ievācis kompromitējošu informāciju, lietotājam apmeklējot pieaugušajiem domātas vietnes. Tika draudēts šo kompromitējošo materiālu izsūtīt draugiem, ģimenei un kolēģiem. CERT.LV informēja sabiedrību, ka nekādu safilmēto materiālu patiesībā nav.

Martā masveidā WhatsApp lietotnē tika izplatītas viltus ziņas par it kā kritisku drošības problēmu, kuru kāds var izmantot, atsūtot video. WhatsApp lietotāji tika aicināti saņemto ziņu pārsūtīt tālāk. Tādas pašas ziņas spāņu un angļu valodās runājošās valstīs tika izplatītas nedēļu pirms kampaņas nonākšanas Latvijas informatīvajā telpā.

No iedzīvotājiem tika saņemta informācija arī par aizdomīgām ziņām WhatsApp lietotnē, kurās apgalvots, ka valdība plāno izmaksāt 350 EUR visiem iedzīvotājiem, kuri nepametīs savu dzīvesvietu līdz 14.aprīlim. Lai pieteiktos pabalstam, WhatsApp ziņā tika iekļauta saite uz formu, kas jāizpilda. Atverot saiti, parādījās attēls ar pērtiķi, kurš rāda aizskarošu žestu. Šīs ziņas uzskatāmas par huligānismu, taču, CERT.LV atgādina, ka izmantotā metode var tikt pielietota arī uzbrukumam ar daudz postošākām sekām lietotāja iekārtai vai personīgai informācijai.

Marta beigās CERT.LV redzeslokā nonāca informācija par krāpnieciskiem e-pastiem ar nosaukumu "Uzmanību Svarīga informācija", kas tika izsūtīti "Latvijas administrācijas" vārdā no e-pasta adreses: admin@kartinitut.ru. E-pasta vēstulē bija norādīta saite, kas veda uz vietni, kurā krievu valodā tika reklamētas ātras peļņas iespējas.

Tika saņemti vairāki ziņojumi par biznesa sarakstes kompromitēšanas (BEC) uzbrukumiem. Kāds uzņēmums ziņoja par neveiksmīgu mēģinājumu izkrāpt maksājumu uz kontu Itālijā, izmantojot vadītāja vārdā izsūtītu vēstuli grāmatvedības personālam. Savukārt divos citos gadījumos uzbrucējs veiksmīgi kompromitēja upuru e-pasta kontus, tādejādi nodrošinot sev iespēju sekot uzņēmumu biznesa sarakstei un atbilstošajā brīdī nosūtīt e-pastu, kas informē sadarbības partneri par rekvizītu (bankas konta) maiņu. Abos gadījumos uzņēmumi cietuši finansiālus zaudējumus, par kuru apmēru CERT.LV nav informācijas. Uzņēmumiem ieteikts vērsties ar iesniegumu policijā.

Iestājoties ārkārtas stāvoklim valstī, iedzīvotāju apziņošanai tika izsūtītas informatīvas īsziņas, kuras saturēja saīsinātās ej.uz saites. Daudzos iedzīvotājos šīs saites radīja bažas par saņemto ziņu leģitimitāti. Jautājumi tika uzdoti, gan sazinoties ar CERT.LV, gan publicējot jautājumus sociālajos tīklos, piemēram, Twitter, un aicinot apstiprināt izplatīto īsziņu leģitimitāti.

Bažas iedzīvotājos radīja arī apziņošanas ietvaros CSDD klientiem izplatītais PDF dokuments, kas ir arī uzbrucēju vidū plaši izmantots ļaunatūras izplatīšanas paņēmiens.

## Pikšķerēšana jeb svarīgo datu izkrāpšana

Janvāra sākumā Citadeles vārdā krāpnieki izplatīja SMS ar krāpniecisku saiti. Banka aicināja kritiski izvērtēt ziņas, kas saņemtas bankas vārdā, īpaši, ja tajās lūgts atvērt kādu saiti vai ievadīt datus. Tāpat banka atgādināja, ka ar PIN kodiem, autorizācijas kodiem, parolēm, kartes numuriem, derīguma termiņiem un CVV kodiem tiek apstiprinātas tikai pašu iniciētas darbības.

Februārī CERT.LV saņēma virkni ziņojumu par krāpnieciska rakstura SMS it kā SEB bankas vārdā. SMS tika iekļauta saite, kas veda uz viltus SEB bankas vietni. Krāpniecības mērķis - iegūt lietotāja pieejas datus interneta bankai.

Tika saņemti ziņojumi par pikšķerēšanas kampaņu, kas tika vērsta pret pašvaldību darbiniekiem un bija paredzēta e-pasta piekļuves datu izkrāpšanai. Pikšķerēšanas e-pastā nebija iekļauta saites uz krāpniecisku vietni, bet bija izteikts aicinājums atbildēt uz saņemto e-pastu, iekļaujot atbildē e-pasta piekļuves informāciju.

Marta otrajā pusē tika izplatīta viltus ziņa sociālā tīkla Facebook piekļuves datu izkrāpšanai. Uzmanības piesaistīšanai viltus ziņā tika apgalvots, ka Daugavpilī reģistrēti vairāk nekā 150 COVID-19 nāves gadījumi. Ziņas turpinājumā lietotājs tika aicināts apmeklēt saiti, kurā it kā iespējams identificēt mirušos, un pārliecināties, vai to vidū nav kāds pazīstams cilvēks vai ģimenes loceklis. Lai piekļūtu informācijai – tika lūgts autentificēties, izmantojot Facebook lietotāja profilu. Ziņas sūtītāju mērķis bija iegūt Facebook piekļuves datus. CERT.LV atkārtoti aicināja iedzīvotājus kritiski izvērtēt ziņojumu saturu, un informācijai par vīrusa izplatību un citiem ar to saistītiem jaunumiem sekot līdzi tikai oficiālās informācijas vietnēs, piemēram, www.spkc.gov.lv.

Marta sākumā Swedbank vārdā tika izplatītas krāpnieciska rakstura īsziņas. Īsziņās saņēmēji tika aicināti atvērt interneta saiti, kura tālāk tos novirzīja uz viltus Swedbank vietni ar mērķi – izgūt lietotāja interneta bankas piekļuves datus.

Nedēļu vēlāk Swedbank vārdā tika izsūtītas arī krāpnieciska rakstura e-pasta vēstules angļu valodā. Tajās apgalvots, ka uz e-pasta saņēmēja bankas kontu pārskaitīta būtiska naudas summa no ārzemēm, bet maksājums, drošības nolūkos, ticis apturēts. Lai skatītu maksājuma detaļas – e-pasta vēstules saņēmējs tika aicināts atvērt e-pastā norādīto saiti. Atverot saiti, interneta lietotājs tika pārvirzīts uz vietni krievu valodā, kurā tika aicināts iesaistīties krāpnieciskā finanšu shēmā.

Marta sākumā darbinieki vairākās valsts un pašvaldību iestādēs masveidā saņēma pikšķerēšanas e-pastus it kā Microsoft vārdā, kuros apgalvots, ka steidzami nepieciešams verificēt e-pasta kontu, pretējā gadījumā tā darbība tiktu pārtraukta. E-pastā, kurš uzrakstīts sliktā latviešu valodā, tika norādīta arī saite verifikācija veikšanai. Verifikācijas gadījumā, krāpnieku rokās nonāca darbinieka e-pasta piekļuves dati.

No ārvalstu kolēģiem tika saņemta informācija par iespējamu mērķētu uzbrukumu kādas valsts iestādes darbiniekiem. Tika identificēts viens iestādes darbinieks, kas saņēmis atbilstoši noformētu e-pastu. E-pasts nesaturēja kaitīgas saites vai pielikumus.

## Pakalpojuma pieejamība (DDoS)

Pēc medijos izskanējušās ziņas par pirmo COVID-19 upuri kaimiņvalstī Igaunijā, Slimību profilakses un kontroles centra (SPKC) tīmekļa vietnē tika novēroti darbības traucējumi. CERT.LV sadarbībā ar tīmekļa vietnes uzturētāju veica situācijas analīzi, kuras rezultātā

apkopotā tehniskā informācija nesaturēja uzbrukuma pazīmes, bet liecināja par periodiski nepietiekamu veiktspēju, kas radusies palielinātā apmeklējumu skaita rezultātā. CERT.LV sadarbībā ar tīmekļa vietnes uzturētāju veica optimizācijas darbus vietnes noslodzes sadalīšanai un veiktspējas uzlabošanai.

Sakarā ar ārkārtas situāciju valstī, kā rezultātā tika atceltas klātienes mācības, pastiprinātu noslodzi piedzīvoja e-klase. Šī noslodze radīja periodiskus resursa darbības traucējumus. Leģitīmi darbības palēninājumi tika vēroti arī e-veselība portālā, gan saistībā ar vietnes veiktspēju, gan portāla latvija.lv veiktspējas traucējumiem, nodrošinot lietotāju autorizācijas procesu.

## Ļaundabīgs kods

Kādā publiskā pasākumā viesiem - uzņēmumu pārstāvjiem - tika izsniegtas zibatmiņas ar reklāmas materiāliem un vīrusu, kas nesankcionēti izveidoja "sētas durvis" (*backdoors*) upura datorā. CERT.LV aicināja būt piesardzīgiem gan ar nezināmas izcelsmes, gan ar šķietami zināmas izcelsmes zibatmiņu ievietošanu savās iekārtās.

Latvijas Universitātes vārdā februārī masveidā tika izsūtīti inficēti e-pasti ar *LokiBot* vīrusu pielikumā. Minētais vīruss paredzēts paroļu un sensitīvas informācijas zagšanai no upura iekārtas. E-pasts šķietami izsūtīts no admin@lu.lv un tematā norādīts - PIEDĀVĀJUMA PIEPRASĪJUMS (Latvijas Universitāte) EUI894/BU4600.

Marta pirmajā pusē vairāki Latvijas uzņēmumi un pašvaldības saņēma aizdomīgus e-pastus no kompromitēta e-pasta konta, kas piederēja kādam Latvijā reģistrētam uzņēmumam. E-pasta pielikums saturēja ļaunatūru lietotājvārdu un paroļu zagšanai. E-pasta vēstulēs latviešu valodā tika apgalvots, ka uzņēmums interesējas par produktu iegādi no e-pasta saņēmēja, un pielikumā pievienots precīzs produktu saraksts. CERT.LV sazinājās ar uzņēmumu, kura vārdā tika izsūtīti e-pasti, un informēja par notikušo. CERT.LV arī sniedza uzņēmumam ieteikumus, kā izvairīties no līdzīgiem incidentiem nākotnē.

Martā tika saņemti vairāki ziņojumi no Latvijā reģistrētiem uzņēmumiem, kas cietuši šifrējošo izspiedējvīrusu uzbrukumos, kā rezultātā liegta pieeja uzņēmumiem svarīgiem datiem. CERT.LV sazinājās ar uzņēmumiem un sniedza ieteikumus datu atgūšanai/ pierādījumu savākšanai tālākai incidenta analīzei.

Pasaules Veselības organizācijas (World Health Organisation – WHO) vārdā tika izsūtītas mēstules it kā ar jaunāko informāciju par COVID-19, taču patiesībā tās saturēja pielikumu ar ļaunatūru. Mēstules sagatavotas angļu valodā, un to noformējumā nesankcionēti izmantots arī WHO oficiālais logo. E-pasts šķietami izsūtīts no healthcaressupport@who.com un tā tematā norādīts – ATTENTION!!!/COVID-19/CASE-REPORT/SAFETY-MEASURES. CERT.LV publicēja brīdinājumu savos sociālo tīklu kontos, un aicināja iedzīvotājus neuzķerties uz krāpniecības, kā arī sekot COVID-19 jaunumiem WHO oficiālajā vietnē – www.who.int.

CERT.LV uzmanības lokā nonāca arī daži incidenti, kas saistīti ar COVID-19 izplatības karti un izmantoja cilvēku bailes un vēlmi uzzināt jaunāko informāciju par potenciālo draudu apmēru un tuvumu. Piedāvātā lietotne izmantoja leģitīmas vietnes vizualizācijas datus apvienojumā ar lietotāja sensitīvo datu (lietotājvārdi, paroles, maksājumu informācija) ieguves funkcionalitāti (*AZORult* ļaunatūru).

CERT.LV analizēja Latvijā uzturētu C2 (*comand & control*) serveri. Tas tika izmantots, lai izplatītu un kontrolētu komerciālu ļaunatūru – trojas vīrusu ar šifrējošo komponenti.

Izmantojot šo vīrusu, uzbrucējs ieguva pilnīgu kontroli pār upura iekārtu un varēja izlemt, vai veikt iekārtas šifrēšanu izpirkuma pieprasījumam, vai nē.

## Ielaušanās mēģinājumi

Līdz ar organizāciju pārslēgšanos attālinātā darba režīmā, martā tika novērota palielināta botu aktivitāte, kas meklē ievainojamas, neatbilstoši konfigurētas un/ vai ar vājām parolēm aizsargātas - tīmeklī pieslēgtas iekārtas. Kā iespējamie mērķi šiem botiem bija darba devēja steigā izsniegta, nepietiekami droši konfigurēta iekārta, vai personīgais dators, kas pēkšņi tiek izmantots darbam.

Martā tika saņemti divi ziņojumi par uzbrukumiem mācību iestāžu infrastruktūrai. Ņemot vērā attālināto mācību nodrošināšanas nepieciešamību un informāciju no citu valstu CERT vienībām par uzbrucēju pastiprinātu interesi attiecībā uz izglītības iestādēm, notikumiem, kas saistīti ar izglītības iestādēm, tika pievērsta pastiprināta uzmanība.

Tika saņemts ziņojums no kādas veselības aprūpes iestādes par aizdomīgām darbībām iestādes serverī. Lai arī izpētes procesā tika konstatēts, ka izmaiņas radījušas iekšējas tehniskas nepilnības, kas tika novērstas, pārskata periodā, balstoties uz veselības iestāžu būtisko lomu un saņemtajiem ziņojumiem no citu valstu CERT vienībām, pastiprināta uzmanība tika pievērsta arī incidentiem, kas saistīti ar veselības aprūpes iestādēm.

Tika saņemts ziņojums par aktīviem uzbrukuma mēģinājumiem kādas valsts iestādes resursam. Aplikācijas līmeņa uzbrukumi tika veikti no vienas IP adreses, cenšoties dažādos veidos (SQL injection, directory traversal, code injection) piekļūt servera parolēm, konfigurācijas datiem un injicēt dažādus izpildāmos kodus. Uzbrukumi veiksmīgi atvairīti.

## Kompromitētas iekārtas un datu noplūdes

Janvāra sākumā tika saņemta informācija par atvērtām direktorijām un iespēju piekļūt personas datiem kāda uzņēmuma tīmekļa vietnē. Resursa uzturētājs tika informēts par personas datu noplūdes risku un atslēdza direktorijām publisko pieeju. Par incidentu tika informēta arī DVI.

Janvāra beigās tīmeklī tika publiskoti vairāk nekā 500 000 kompromitētu serveru, maršrutētāju un lietu interneta (IoT) "gudro" iekārtu piekļuves dati. Saraksts saturēja iekārtu IP adreses, lietotājvārdus un paroles attālinātai iekārtu kontrolei (*Telnet service*). Sarakstu nopubliskoja kāds piekļuves atteices (DDoS) uzbrukumiem paredzētas infrastruktūras uzturētājs. CERT.LV veica nopludinātā kompromitēto serveru, maršrutētāju un lietu interneta (IoT) iekārtu saraksta pārbaudi. Tika konstatēts, ka no visām sarakstā uzskaitītajām iekārtām tikai nepilnas 100 atradās Latvijā. Izpētes rezultātā tika noskaidrots, ka publiskotā informācija par sarakstā minētajām apdraudētajām iekārtām (IP adresēm) ir novecojusi. Sarakstā iekļautās IP adreses no partneru ziņojumiem bija nonākušas CERT.LV redzes lokā jau 2018. gadā. Uz izpētes brīdi, iespējams, CERT.LV informatīvās apziņošanas rezultātā, paroles ir tikušas nomainītas, vai arī iekārtas atslēgtas no interneta.

Tika saņemta informācija par vairāku pašvaldību darbinieku e-pasta kontu kompromitēšanu. No kompromitētajiem kontiem tika izsūtīti e-pasti gan pašvaldībām, gan citiem kontaktiem. Izsūtīti tika gan pikšķerēšanas e-pasti, gan kaitīgas datnes - ļaunatūra, kas paredzēta paroļu un citas sensitīvas informācijas zādzībai. E-pasta konti, visticamāk, tikuši kompromitēti, lietotājiem atverot līdzīgu e-pastu. CERT.LV sniedza iestādēm rekomendācijas tālākai rīcībai.

Saņemta ziņa no kāda lietotāja par viņa vārdā izveidotu viltus e-pasta kontu. Izmantojot šo viltus e-pasta kontu, lietotāja darba devējam tika nosūtīta no lietotāja Facebook profila lejupielādēta tur publicēta agresīva satura fotogrāfija.

Tika kompromitēta kādas pašvaldības informatīvā vietne, ievietojot vietnes kodā *iframe* skriptu uzbrukuma bez apmeklētāju iesaistes (*drive-by*) veikšanai. Vietnes uzturētāji tika informēti, vietnes kods un spraudņi tika atjaunināti, novēršot uzbrukumam izmantoto ievainojamību.

No starptautiskajiem sadarbības partneriem tika saņemta informācija par kāda medija tīmekļa vietnes kompromitēšanu, ievietojot vietnē ārvalstu banku klientu datu izkrāpšanai paredzētu saturu. Vietnes uzturētāji tika informēti, kompromitētā novecojusī WordPress satura vadības sistēma atjaunināta.

## Ievainojamības

Janvāra beigās viens no lielākajiem tīkla aparatūras ražotājiem Citrix publicēja ielāpus kritiskas ievainojamības CVE-2019-19781 novēršanai. Ievainojamība ļāva uzbrucējam, neveicot autentifikāciju, realizēt patvaļīga koda izpildi ievainojamajā sistēmā. Globālā pieredze liecināja, ka ievainojamība tika aktīvi izmantota uzbrukumos, pakļaujot sistēmas šifrējošā izspiedējvīrusa *Sodinokibi* (pazīstams arī kā *REvil*) uzbrukumam, kurš ne tikai padara datus nepieejamus, lai pieprasītu izpirkuma maksu par datu atgūšanu, bet pirms tam šos datus nokopē, lai uzbrucējs varētu draudēt ar datu publiskošanu, ja netiks samaksāta izpirkuma maksa.

CERT.LV veiktās pārbaudes atklāja arī vairākas nozīmīgas ievainojamas sistēmas Latvijā, kuru turētāji tika apzināti un brīdināti. Ievainojamības tika veiksmīgi novērstas, ievainojamības ļaunprātīgas izmantošanas gadījumi Latvijā netika fiksēti.

Februārī publiski tika paziņota MS Exchange e-pasta servisa ievainojamība (CVE-2020-0688), kas ļāva izpildīt patvaļīgu kodu (RCE) ar sistēmas līmeņa tiesībām, ja ir iegūta pieeja jebkura līmeņa e-pasta kontam uz šī servera. Ievainojamība bija viegli ekspluatējama un guva popularitāti uzbrucēju vidū. CERT.LV veica Latvijā izmantoto serveru pārbaudi, kurā konstatēja aptuveni 120 ievainojamus serverus. Uzturētāji tika informēti par ievainojamajiem serveriem un ieteicamajiem soļiem uzbrukuma draudu novēršanai.

No sadarbības partneriem tika iegūta informācija par ievainojamību virtuālā privātā tīkla (VPN) tehnoloģijā. Tika apzināti un apziņoti VPN lietotāji, kuru izmantotās tehnoloģijas pakļautu infrastruktūru ievainojamības ļaunprātīgas izmantošanas riskam, to skaitā arī kādā valsts iestādē. Pēc apziņošanas ievainojamība iestādē tika novērsta.

## Atbildīga ievainojamību atklāšana

Pārskata periodā tika saņemti daži maznozīmīgi ziņojumi.

## CERT.LV pasākumi incidentu novēršanā:

- Informācija par pikšķerēšanas kampaņām un būtiskām ievainojamībām tika tika nosūtīta valsts un pašvaldību iestāžu atbildīgajām personām par IT drošību.
- Informācija par jaunatklātiem apdraudējumiem un ievainojamībām tiek publicēta arī CERT.LV sagatavotajās ziņās un sociālā tīkla Twitter kontā (@certlv).

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

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

13. janvārī CERT.LV pārstāvji piedalījās Finanšu nozares asociācijas organizētā nozares un citu iesaistīto organizāciju pārstāvju sanāksmē par potenciālu izglītojošas kampaņas organizēšanu iedzīvotājiem par drošību, lietojot finanšu pakalpojumus interneta vidē.

14. janvārī CERT.LV pārstāvis tikās ar Latvijas Informācijas un komunikācijas tehnoloģiju asociācijas (LIKTA) un VAS Latvijas Valsts radio un televīzijas centra (LVRTC) pārstāvjiem, lai apspriestu Eiropas Digitālās nedēļas pasākumu norisi un iesaisti tajos. Tika plānoti izglītojoši tiešsaistes semināri par e-paraksta izmantošanu un kiberdrošību darbavietā, kā arī diskusiju pasākums "Kibernakts".

15. janvārī CERT.LV pārstāvis piedalījās Aizsardzības ministrijas rīkotā seminārā iestāžu, uzņēmumu un nevalstisko organizāciju vadītājiem, politiķiem un akadēmiskās vides pārstāvjiem par visaptverošu valsts aizsardzības sistēmas veidošanu un valsts aizsardzības stiprināšanu, sekmējot starpnozaru sadarbību. CERT.LV iepazīstināja dalībniekus ar situāciju Latvijas kibervidē un modernajiem kiberapdraudējumiem.

30. janvārī CERT.LV pārstāvis piedalījās ikgadējā Latvijas atvērto tehnoloģiju asociācijas (LATA) konferencē, prezentācijā "Atvērto datu iniciatīvas Latvijā un piemēri pasaulē" aplūkojot dažādus atvērto datu projektus un aicinot izvērtēt šādu projektu drošības aspektus.

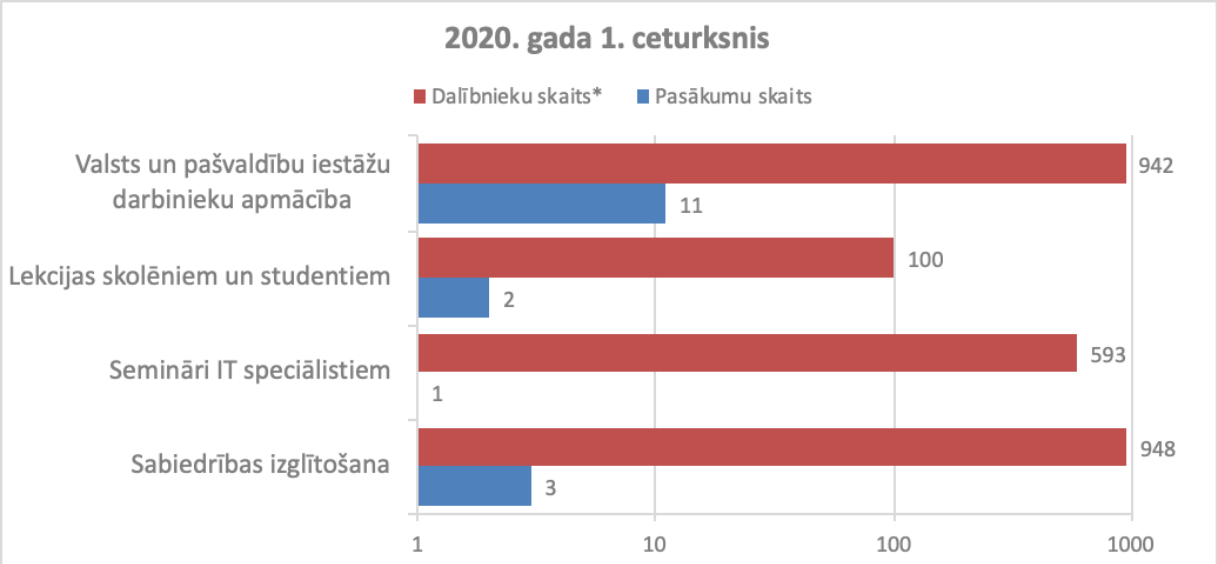
11. februārī CERT.LV pārstāvis piedalījās projekta SkeptiCafe, kas ir zinātnes un kritiskās domāšanas popularizēšanas "kafejnīca" – domubiedru vakars, ietvaros organizētā diskusijā par to "Ko internets tev nestāsta? Jeb indivīda un valsts digitālā drošība".

11. februārī CERT.LV pārstāvis kopā ar NIC.LV pārstāvi piedalījās Rīgas Centrālās bibliotēkas filiālbibliotēkas "Pūce" organizētā "Drošāka interneta dienas" pasākumā, kurā skolēnus iepazīstināja ar domēnvārdiem, pikšķerēšanu un citiem ar interneta drošu lietošanu saistītiem aspektiem.

24. martā CERT.LV organizēja attālinātu semināru "Esi drošs" valsts un pašvaldību atbildīgajām personām par IT drošību un citiem interesentiem. Seminārā tika aplūkoti dažādi ar attālinātā darba organizēšanu saistīti jautājumi un drošības aspekti. Seminārs tika pārraidīts tiešsaistē gan CERT.LV tīmekļa vietnē, gan sociālajā tīklā Facebook, sniedzot iespēju skatītājiem pasākuma laikā arī uzdot jautājumus. Pasākumam tiešsaistē sekoja gandrīz 600 skatītāju.

26. martā CERT.LV pārstāvis piedalījās Eiropas Digitālās nedēļas ietvaros organizētā attālinātā informatīvā pasākumā "Mazā Kibernakts", kuru organizēja LVRTC. Arī šis pasākums bija veltīts attālinātā darba jautājumiem un ar to saistītiem izaicinājumiem, ieskaitot dažādus kiberuzbrukumu riskus, dokumentu parakstīšanu un bērnu pieskatīšanu, izmantojot digitālās tehnoloģijas. Pasākumu varēja vērot sociālajā tīklā Facebook un vietnē lmt.straume.lv.

Pārskata periodā CERT.LV par IT drošību izglītoja 3324 cilvēkus, iesaistoties 39 izglītojošos pasākumos.




11.attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2020. gada 1. ceturksnī

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

**Sadarbības tikšanās, konsultācijas un prezentācijas:**

- CERT.LV pārstāvis tikās ar VARAM, lai pārrunātu iespējamos grozījumus fizisko personu elektroniskās identifikācijas likumā, balstoties uz Finanšu nozares asociācijas (FNA) iesniegtajiem jautājumiem un priekšlikumiem.
- CERT.LV tikās ar DVI pārstāvjiem, lai vienotos par abu organizāciju sadarbības mehānismiem.
- Pēc ārkārtas situācijas izsludināšanas valstī un akūtas nepieciešamības organizēt daudzu iestāžu darbu attālināti, CERT.LV saņēma virkni jautājumu par attālinātās komunikācijas rīku izvēli un to atbilstību drošības prasībām. Lai veicinātu informētu lēmumu pieņemšanu un IT drošības līmeni, CERT.LV veica populārāko attālinātās komunikācijas rīku analīzi, izvērtējot tos gan no datu drošības aspekta, gan piedāvātās funkcionalitātes, izcelsmes valsts, konstatētajām ievainojamībām u.c. parametriem. Ar pētījuma rezultātiem detalizēti tika iepazīstinātas galvenās sadarbības organizācijas un citi sadarbības partneri Latvijā un pasaulē.

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:**

- 20. – 23. janvārī Rīgā notika CERT.LV un NATO Apvienotā kiberaizsardzības izcilības centra (CCDCoE) organizētās ikgadējās kiberdrošības mācības "Crossed Swords", kuras šogad kopā pulcēja vairāk nekā 120 tehnisko ekspertu, nacionālo Kiberpavēlniecību, speciālo vienību un militārās policijas pārstāvjus no 26 valstīm. "Crossed Swords" no tīri tehniskām sarkanā karoga komandas mācībām attīstījušās par unikālu un kompleksu ofensīvo kiberoperāciju treniņu programmu, kas apvieno dažādas tehniskās prasmes ar kinētisko spēku komponenti, un aptver vairākus ģeogrāfiskos atrašanās punktus vienlaicīgi. Mācību galvenais uzsvars tika likts uz starpvalstu un starpdisciplināro sadarbību pilna spektra ofensīvas kiberoperācijas realizācijā.
- 21. janvārī NIS direktīvas CERTu tīkla ietvaros notika CERT komandu savstarpējais audits (peer review). CERT.LV pārstāvis viesojās Ļubļanā un veica auditu SI-CERT – Slovēnijas nacionālajai CERT komandai.
- 24. janvārī CERT.LV pārstāvis piedalījās FIRST 2020 konferences programmkomitejas sanāksmē, kuras laikā tika izstrādāta plānotās konferences programma.
- No 24. janvāra līdz 2. februārim CERT.LV pārstāvji piedalījās TF-CSIRT/FIRST simpozijā Malagā, kurā sniedza prezentāciju "Pastelyzer — the Paste Analyzer". Prezentācijā tika aplūkots CERT.LV izstrādāts rīks "Pastelyzer", kas paredzēts sensitīvu datu (lietotājvārdi, paroles, maksājumu karšu dati u.c.) noplūžu konstatēšanai. Izstrādātā rīka kods no 2020. gada janvāra ir padarīts publiski pieejams GitHub repozitorijā. Uz pārskata perioda beigām tika saņemta informācija, ka CERTu komūnā rīks jau tiek izmantots, kā arī saņemti pirmie ieteikumi rīka attīstīšanai un uzlabošanai. Papildus turpinājās arī darbs tematiskajās darba grupās. CERT.LV aktīvi piedalījās darba grupā "TF-CSIRT Future working group".
- 2. – 6. februārī CERT.LV pārstāvis vadīja vieslekciju maģistra programmas studentiem BTH (Belkinge University of Technology), Zviedrijā.
- 11. – 13. februārī CERT.LV pārstāvis piedalījās NIS direktīvas CERTu tīkla sanāksmē Stokholmā, un sniedza divas prezentācijas. Papildus turpinājās arī darbs tematiskajās darba grupās un CERT.LV aktīvi piedalījās divās no tām: "Cyber Weather" darba grupā, kura regulāri apkopo informāciju par būtiskākajiem kiberincidentiem un reizi ceturksnī izstrādā kiberlaikapstākļu pārskatu Eiropai, un "Maturity" darba grupā, kura rūpējas par ES dalībvalstu CSIRT komandu brieduma līmeņa paaugstināšanu.
- 2. martā CERT.LV pārstāvis FESA, ENISA 19th Article sanāksmē Luksemburgā prezentēja uzticamības pakalpojumu sniedzēju uzraudzību Latvijā.
- 2. – 5. martā CERT.LV pārstāvis piedalījās NATO CCDCoE "Executive Cyber Seminar" un vadīja vieslekciju.
- Pārskata periodā CERT.LV pārstāvis piedalījās ar kiberdrošības mācību "Cyber Europe" saistītām aktivitātēm. Mācības tika paredzētas 2020.gada jūnijā, taču pandēmijas ietekmē tās tiek plānots pārcelt uz 2021.gada martu.

- Pārskata periodā COVID-19 pandēmijas ietekmē kopš ārkārtas situācijas izsludināšanas brīža NIS direktīvas CERTu tīkla ietvarā tika uzsākta aktīva informācijas apmaiņa par incidentiem, kas saistīti ar COVID-19 tēmu un kiberdrošību veselības nozarē. Ik nedēļu tika apkopota situācija visās Eiropas valstīs un gatavots pārskats lēmumu pieņēmējiem NIS Cooperation grupā, kā arī citās grupās. Latvija šajā procesā aktīvi piedalījās un informēja partnerus par kibertelpas aktualitātēm un tendencēm.

Sadarbība konkrētu incidentu risināšanā aplūkota pārskata 2. punktā.

# 6. Projekta "Improving Cyber Security Capacities in Latvia" īstenošana

Turpinās 2018. gada 1.septembrī CERT.LV uzsāktā 2017 CEF Telecom-Cyber Security uzsaukumā apstiprinātā projekta "Improving Cyber Security Capacities in Latvia" (līguma ar Eiropas Komisiju Nr. INEA/CEF/ICT/A2017/1528784) (turpmāk – ICSC projekts) īstenošana.

Darbs turpinās visās sešās projektā definētajās darba pakās:

- 14. janvārī Briselē norisinājās MeliCERTes – Cybersecurity Core Service Platform – līdz šim koordinējošā konsorcija organizētā pēdējā sanāksme, kurā notika izstrādātās platformas funkcionalitātes pārskatīšana un vērtēšana. Tajā piedalījās CERTu tīkla un CEF projekta pārstāvji no dažādām Eiropas valstīm. Kopš 2019. gada decembra MeliCERTes platformas uzturēšanu un tālāku attīstīšanu īsteno jauns konsorcijs, kuru pārstāv Polijas, Austrijas, Luksemburgas, Slovākijas, Igaunijas CERTi un Deloitte. ICSC projekta ietvaros CERT.LV turpinās iesaisti MeliCERTes platformas tālākas izstrādes un testēšanas aktivitāšu atbalstam.
- Publiskota "Deep Analysis System" beta versija. Sistēma, instalēšanas instrukcija un lietotāju rokasgrāmata pieejami: https://github.com/cert-lv/pastelyzer/. 2020. gada janvāra beigās, piedaloties TF-CSIRT konferencē Malagā, Spānijā, CERT.LV prezentēja sistēmu arī plašākai CERTU kopienai, aicinot uz sadarbību CERTu komandas tālākai sistēmas attīstīšanai. Vairākas komandas atsaukušās aicinājumam un darbs pie sistēmas turpinās. Paredzams, ka plašākai sabiedrībai komunikācija par pieejamo sistēmu un tās funkcionalitāti notiks 2020. gada vasarā.
- Turpinājās darbs pie sabiedrību izglītojošas kampaņas "Kiberdrošība darbavietā" – pārskata periodā noslēdzās iepirkumu abas kārtas. Sākotnēji plānotais kampaņas norises laiks bija 2020. gada 1./2. ceturksnis, šobrīd, izsludinātā ārkārtas stāvokļa dēļ, paredzamas nobīdes. Kampaņas īstenošanas laiks tiks precizēts, ārkārtas stāvoklim beidzoties.

# 7. Projekta "Cyber Exchange" īstenošana

Turpinās 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 – Sadarbības projekts CyberExchange) īstenošana.

Projekta mērķis ir stiprināt starptautisku sadarbību starp nacionālajām un valdības CSIRT/CERT organizācijām. CyberExchange 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.

2020. gada 1. ceturksnī projekta ietvaros bija plānota CERT.LV pieredzes apmaiņas vizīte pie CERT.AT, taču COVID-19 vīrusa izplatības ierobežošanai noteikto ceļojumu ierobežojumu dēļ, vizīte tika atcelta. Arī citas pieredzes apmaiņas vizītes šobrīd ir atceltas, un tiks īstenotas pēc ārkārtas situācijas atcelšanas.

# 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. Projekts sniedz iespēju aizsargāt lietotājus no ļaundabīga satura internetā, kas saistīts ar kiberdrošības institūcijām jau zināmiem incidentu identifikatoriem (domēna vārdi, IP adreses u.c.). Daļu no DNS PRZ pakalpojuma var izmantot arī bez līguma slēgšanas un autorizēšanās jebkurš interneta lietotājs. Lai to izmantotu, jālieto NIC.lv rekursīvie DNS serveri. Šo iespēju CERT.LV aktīvi popularizēja mājas lietotājiem ārkārtas stāvokļa laikā.
- Tika organizētas un īstenotas tikšanās ar pamatpakalpojumu sniedzēju statusu ieguvušajām organizācijām, lai informētu organizācijas par jaunajiem pienākumiem, kas izriet no Informācijas tehnoloģiju drošības likuma un Ministru kabineta noteikumiem Nr.442, kā arī lai sniegtu informāciju par CERT.LV nodrošinātajiem pakalpojumiem.
- CERT.LV sniedza rekomendācijas un atbalstu pirmajai Latvijas komerciālajai CERT komandai CyberCircle Trusted Introducers biedra statusa pieteikumam, kas martā tika arī apstiprināts.
- 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 pārskata periodā veica atbilstošas konsultatīvās funkcijas.

# 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 01.01.2020. līdz 31.03.2020. ir saņēmusi un izvērtējusi 1481 ziņojumus. No tiem 1335 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 3 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 26 ziņojumos konstatēta personas goda un cieņas aizskaršana, 2 ziņojumi saņemti par naida runu un 1 ziņojums par vardarbību atainojošiem materiāliem. Par finanšu krāpšanas mēģinājumiem internetā saņemti 26 ziņojumi, 16 ziņojumu saturs nav bijis pretlikumīgs, 72 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 1267 ziņojumi par bērnu seksuālu izmantošanu saturošiem

materiāliem, kas tiek uzturēti uz serveriem Latvijā. 7 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 1328 ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem 1312 ziņojumi ir dzēsti no publiskas aprites un 16 ziņojumu saturs atrodas dzēšanas procesā sadarbībā ar Valsts policiju un interneta pakalpojumu sniedzējiem.

Sagatavotājs – Līga Besere,
tālrunis 67085888
e-pasts liga.besere@cert.lv