CERT.LV
Kiberincidentu novēršanas institūcija

Latvijas kiberdrošības un CERT.LV tehnisko aktivitāšu 2025. gada pārskats

TLP:CLEAR

Satura rādītājs

Ievads

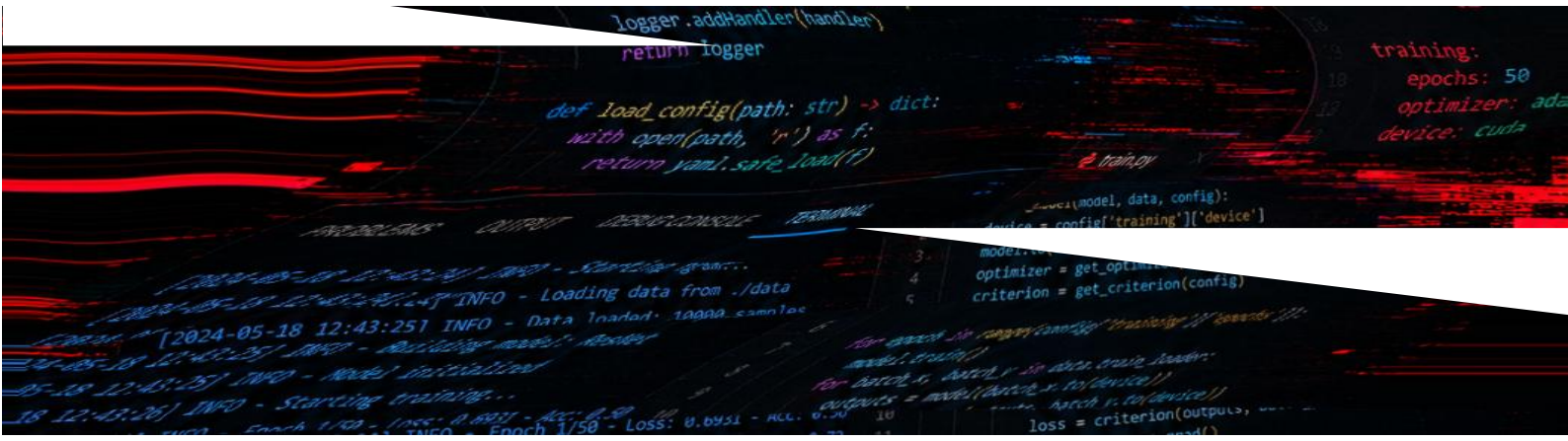
Pārskata mērķis ir sniegt Latvijas kiberdrošības pārvaldniekiem un speciālistiem operacionāli pielietojamu informāciju, analītiķiem izmantojamu apkopojumu par aizvadītā gada notikumiem Latvijas un Ziemeļeiropas reģiona kibertelpā, kā arī kiberdrošības situācijas attīstības prognozes tuvākai nākotnei.

CERT.LV komanda 2025. gadā par prioritāti noteica kritiskās infrastruktūras kiberdrošības stiprināšanu un reģionālu kiberdrošības spēju celšanu - visos Latvijas novados un valstspilsētās, pievēršot īpašu uzmanību novadu domēm, enerģētikas, satiksmes, veselības aprūpes, viedās pilsētas vadības elementiem un citu būtisku pakalpojumu sniedzējiem, to informācijas tehnoloģiju un operacionālo tehnoloģiju vidēm, lai stiprinātu valsts nacionālajai drošībai un sabiedrībai nozīmīgu pakalpojumu sniedzēju sistēmu noturību un drošību. Noteiktos mērķus sasniedzam, ieviešot un nodrošinot visaptverošu CERT.LV pakalpojumu un atbalsta mehānismu kopumu, kas to saņēmējiem ir pieejams bez atsevišķas maksas. Tas ļauj sasniegt reāllaikam pietuvinātu, datos balstītu kiberdrošības notikumu apstrādi un reaģēšanu infrastruktūras turētāju vidēs. Nacionālās kiberdrošības likuma subjektiem ieviešot CERT.LV pakalpojumus, reaģēšanas laiks sarežģīta kiberincidenta gadījumā samazināts no 6 mēnešiem līdz 1 dienai vai pat tuvinās reāllaika apdraudējuma novēršanai.

Par prioritāri izmantojamiem kiberdrošības pakalpojumiem esam noteikuši agrās brīdināšanas sensoru sistēmu (ABS), draudu medību operācijas - proaktīvu kiberapdraudējumu un iespējamas kiberuzbrucēju klātbūtnes pazīmju meklēšanu, un drošības operāciju centra (SOC) pakalpojumu. Citu CERT.LV nodrošināto pakalpojumu izmantošana tiek rekomendēta, pamatojoties uz Nacionālā kiberdrošības likuma subjekta informācijas sistēmu un sniegto pakalpojumu kritiskumu, kiberdrošības brieduma līmeni un piemērojamajām normatīvo aktu prasībām.

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

- **kibeapdraudējumu analīze;**
- **kiberuzbrukumu spektra kartēšana;**
- **kiberincidentu risināšana;**
- **ielaušanās testi un kontrolētu uzbrukumu veikšana;**
- **draudu medību operācijas;**
- **ieteikumi kiberdrošības uzlabošanai un kiberuzbrukuma virsmas mazināšanai.**



Kopsavilkums

Digitālās pasaules drošība turpina strauji mainīties - kiberapdraudējumi kļūst arvien dinamiskāki, bet to novēršana - sarežģītāka. Kibernoziedznieki plaši un sekmīgi izmanto mākslīgā intelekta iespējas, sociālo inženieriju un identitāšu ļaunprātīgu izmantošanu, par uzbrukuma mērķiem izvēloties gan indivīdus, gan organizācijas ar nepietiekamu kiberdrošības praksi un pārvaldības līmeni. Vienlaikus joprojām tiek īstenoti mērķēti, rūpīgi plānoti kiberuzbrukumi, kuros izmantoti īpaši izstrādāti rīki un sarežģītu, savstarpēji saistītu tehniku un taktiku ķēde.

Ilgstoši veiksmīgi pielietotais kiberuzbrukumu scenārijs sastāv no vairākiem loģiski savienotiem posmiem. Tas ietver gan sarežģītu, gan dažkārt vieglākā ceļa ielaušanās taktiku, pastāvīgas piekļuves nodrošināšanu, ilgstošu klātbūtni infrastruktūrā, veiklu izvairīšanos no aizsardzības risinājumiem un plašu pārvietošanos datortīklā jeb sānu kustību. Uzbrukuma noslēguma posmā parasti seko tā kulminācija – datu eksfiltrēšana jeb "nopludināšana" vai infrastruktūras pilnīga iznīcināšana. Šādu uzbrukumu pamatā bieži ir ievērojams finansējums un profesionālu kibernoziedznieku kolektīvs darbs.

Lai gan šāds labi pārdomāts "perfektais noziegums" joprojām ir iespējams, tas arvien biežāk kļūst par izpētes un digitālās izmeklēšanas rokasgrāmatu piemēru. Vienlaikus aizvien biežāk novērojama salīdzinoši jauna tendence - strauji, dažkārt oportūnistiski uzbrukumi ar ātru "notikuma vietas" pamešanu. Šo zibuzbrukumu mērķis ir īsā laikā ielauzties, iegūt pieejamos datus un pēc iespējas ātrāk pārtraukt aktivitāti, neatstājot pēdas. Uzbrucējiem pieņemama ir arī tikai daļēja mērķa sasniegšana, paļaujoties uz veiksmi, jo galvenais ir rīkoties ātri un ar iespējami zemām izmaksām.

Lai gan spēles noteikumi nekad nav pilnībā vienlīdzīgi un uzbrucējiem pietiek ar vienu ievainojamību, kamēr infrastruktūras aizsargiem jāidentificē un jānovērš visas iespējamās nepilnības - **tomēr jāatzīst, ka arī aizsargiem ir pieejama tā pati informācija, rīki un iespējas ieviest aizsardzības pasākumus. Tāpēc arvien mazāk paliek attaisnojumu šo pasākumu neesamībai.**

Bieži vien ar jēdzienu "kiberdrošība" vispirms asociējas augsti kvalificēta IKT speciālistu komanda, rūpīgi izstrādāta dokumentācija, procedūras un ekskluzīvs, ļoti dārgs tehnoloģiskais aprīkojums. Lai gan daļēji šāds priekšstats ir pamatots, pārskata gadā novērotā situācija sniedz arī labu ziņu – pie kiberdrošības pamatiem var strādāt jebkurš, turklāt sākt iespējams jau tagad. Labs sākums ir pilnībā iespējams arī bez ievērojamiem finanšu līdzekļiem un augsti kvalificētas komandas. Protams, drošība rada izmaksas, taču tās neesamība ilgtermiņā maksās daudz dārgāk.

CERT.LV tehnisko aktivitāšu 2025. gada pārskatā analizētie notikumi skaidri parāda, ka daudzos gadījumos incidentu būtu iespējams novērst vēl pirms tā iestāšanās. Lai to panāktu, darbs vienmēr sākas ar sevi un atbildīgu attieksmi:

- kritiskā domāšana, izvērtējot riskus mūsdienu steigā;
- pašdisciplīna, jo reti drošākā izvēle ir ērtākā;
- pacietība biežajā paroļu nomaiņā un daudzfaktoru autentifikācijas lietošanā;
- kiberhigiēnas ievērošana ne tikai darba vidē, bet arī privāti mājās;
- sapratne un sadarbība ar līdzcilvēkiem un IKT drošības personālu, jo mēs visi kolektīvi stiprinām valsts kopējo kiberdrošības pozīciju.

Organizācijā vai uzņēmumā kiberdrošības pamati un plānošana sākas ar savas digitālās saimniecības apzināšanu un sakārtošanu. Pirms jaunu tehnoloģisko risinājumu, automatizācijas vai mākslīgā intelekta risinājumu ieviešanas ir nepieciešama skaidra izpratne par to, kādi informācijas resursi, datorsistēmas, lietotāji, piekļuves tiesības, datu plūsmas un programmatūra jau pastāv organizācijas vidē. Efektīvu

kiberdrošību nevar sākt ar modernu tehnoloģiju pievienošanu videi, kas atrodas ārpus strukturētas kontroles. Nesakārtojot un nepārzinot savu digitālo saimniecību, jebkurš jauns risinājums palielinās sarežģītību, nevis drošību.

Tāpēc kiberdrošības plānošanas pirmais solis ir pašreizējās situācijas inventarizācija: resursu uzskaite, piekļuves tiesību pārskatīšana, kritisko sistēmu noteikšana, atbildīgo personu identificēšana un atbildības jomu sadalījums. Šāds sākums ir ne tikai vienkāršs, bet arī praktiski nozīmīgs, jo vairumā gadījumu tas jau agrīni palīdz atklāt iespējamos riskus organizācijā. Tas ļauj kiberdrošību veidot kā pārvaldāmu procesu, nevis kā no realitātes atrautu tehnoloģisku paralēlo pasauli.

Tehnisko aktivitāšu pārskats ietver ne tikai incidentu aprakstus, bet arī iespējami detalizētu analīzi un praktiskus ieteikumus, kas ir reāli ieviešami izmantotajās sistēmās.

Pārskata galvenais mērķis ir sniegt iespēju mācīties no pieļautajām kļūdām, izdarīt secinājumus un ieviest uzlabojumus ikdienas darba vidē. To var izmantot ne tikai kā informācijas avotu, bet arī kā pamatu labās prakses vadlīniju ieviešanai.

Pārskatā sniegta detalizēta informācija par šādām 2025. gada notikumu kategorijām:

Finansiāli motivēti uzbrukumi: aplūkoti kiberapdraudējumi, kuru galvenais mērķis ir finansiāla labuma gūšana, izmantojot lietotāju uzticēšanos, tehniskas ievainojamības vai maldinošas shēmas. Sadaļā skaidrota šo uzbrukumu ietekme un sniegti praktiski ieteikumi risku mazināšanai un finanšu drošības stiprināšanai.

Citu valstu organizēti kiberuzbrukumi Latvijai (APT): analizēti augsti organizēti un tehniski sarežģīti kiberuzbrukumi, kas tiek īstenoti ilgtermiņa mērķu sasniegšanai, stratēģiskas informācijas iegūšanai vai ietekmes palielināšanai.

Pakalpojumatteices uzbrukumi (DDoS): raksturoti uzbrukumi, kuru mērķis ir traucēt digitālo pakalpojumu pieejamību, pārslogojot sistēmas, tīklus vai tiešsaistes resursus.

Ievainojamību apkopojums: aplūkotas būtiskākās publiski zināmās ievainojamības, kas var ietekmēt organizāciju informācijas sistēmu drošību un radīt riskus neatļautai piekļuvei, datu noplūdei vai pakalpojumu darbības traucējumiem.

CERT.LV Ielaušanās testi un kontrolētu uzbrukumu veikšana (Red Teaming): raksturotas kontrolētas un likumīgas kiberdrošības pārbaudes, kuru mērķis ir novērtēt organizācijas spēju identificēt, apturēt un reaģēt uz reāliem uzbrukuma scenārijiem.

CERT.LV SOC pakalpojuma rezultāti: pārskats par Drošības operāciju centra (SOC) pakalpojumu, kas centralizēti apkopo drošības telemetriju no klienta infrastruktūras un sasaista tās notikumus ar visu CERT.LV pieejamo apdraudējumu indikatoru un zināšanu kopu.

OSINT iegūtie rezultāti un ieteikumi: aplūkota publiski pieejamas informācijas izmantošana, lai identificētu iespējamos drošības riskus, informācijas noplūdes un organizācijas digitālās klātbūtnes ievainojamos punktus.

Kiberdrošības draudu meklēšanas operācijas jeb draudu medības: draudu medībās novērtē vispārējo informācijas un komunikāciju tehnoloģijas (IKT) un infrastruktūras kiberdrošības līmeni. Tiek atklātas un analizētas ļaunprātīgas darbības, identificēta uzbrucēja klātbūtne, analizēta taktika, paņēmieni un izmantotās procedūras.

2025. gada galvenie rādītāji

2982 (+28%)

Manuāli apstrādāto kiberincidentu skaits (2025.g. vs 2024.g.)

1,32 milj.(+164%)

Identificēto apdraudēto iekārtu skaits (2025.g. vs 2024.g.)

1986 (+54%)

Krāpšanas gadījumu skaits;

kvantitatīvi dominējošais incidentu veids

(2025.g. vs 2024.g.)

76 (+41%)

Pieejamības traucējums jeb DDoS uzbrukumu skaits

(2025.g. vs 2024.g.)

~2,2 milj. (+20%)

Tik reižu CERT.LV DNS ugunsmūra uzturētie saraksti bloķēja piekļuvi ļaunprātīgām vietnēm

(2025.g. vs 2024.g.)

>13,1 milj.

Kaitīgo domēna vārdu DNS pieprasījumi kopumā 2025.gadā

82

CERT.LV veiktajos **27** IT sistēmu drošības testu ietvaros identificētās ievainojamības

15436

Nosūtīto e-pastu skaits pikšķerēšanas uzbrukumu simulācijās; atvērti **4 859** e-pasti jeb 32%; gandrīz **1/5** ievadīja datus

~42 tūkst.

Gala iekārtu skaits ar CERT.LV SOC nodrošinātu redzamību kopumā 55 NKDL subjektu infrastruktūrās (dati uz 2025.g. beigām)

23 milj.

SOC reģistrēto trauksmes ziņojumu skaits, tostarp 1871 manuāli izveidota lieta, 23 incidenti (dati uz 2025.g. beigām)

~16,4 tūkst.

Kopš 2022.gada draudu medībās anlizēto gala iekārtu skaits **40** NKDL subjektu infrastruktūrās

20%

Tik no visām analizētajām organizācijām kopš 2022.gada draudu medībās atklāta APT klātbūtne

1. Finansiāli motivēti uzbrukumi

Krāpšana - jaunumi un aktualitātes

Pēc privātpersonu zaudējumu apjoma visaugstākais rādītājs ir viltus investīciju krāpšanai. Šajās shēmās iedzīvotāji tiek pierunāti veikt ieguldījumus akciju, atvasinātu finanšu instrumentu un kriptovalūtu tirdzniecībā. Patiesībā krāpnieki nekādus reālus ieguldījumu portfeļus neveido, bet piesavinās upuru pārskaitīto naudu.

Gada laikā viltus investīciju reklamēšanā novērots straujš mākslīgā intelekta (MI) ģenerētu video izmantošanas pieaugums. Tajos tiek izmantoti populāru politiķu un citu sabiedrībā atpazīstamu personu tēli. Viltus reklāmu video un audio kvalitāte ir ievērojami uzlabojusies, taču maldinošais pamata saturs palicis nemainīgs:

- inovatīvs peļņas gūšanas veids;
- liels mantojums no nesen mirušas personas, kura it kā nopelnījusi ievērojamus līdzekļus investīciju platformā;
- slepena metode, kas sola peļņu līdz 10 000 EUR mēnesī;
- jebkuru aktuālu notikumu ciniska izmantošana viltus vietņu reklamēšanai, tostarp pazīstamu personu nāves vai skaļu nelaimes gadījumu piesaukšana.

Labi apmaksātās un ļoti intensīvi izplatītās viltus reklāmas visbiežāk tiek izvietotas Facebook un Google Ads platformās. Šo platformu reklāmu kontroles rīki tiek izmantoti auditorijas pielāgošanai. Iedzīvotāji šādas reklāmas ierauga, gan meklējot internetā populārus atslēgvārdus, gan apmeklējot tīmekļa vietnes ar iekļautiem reklāmas laukumiem.

Pēc krāpnieku reklamētās vietnes apmeklēšanas sākotnēji aktīvi uzbrukumi, piemēram, pārlūkprogrammai, parasti nenotiek - lietotājs tiek aicināts aizpildīt pieteikuma formu. Patiesais uzbrukums tiek īstenots ar sociālās inženierijas metodēm, proti, intensīviem tālruņa zvaniem, kuru mērķis ir pārliecināt upuri par ieguldījumu drošību un lielām peļņas iespējām.

Zvani tiek veikti no dažādu valstu tālruņu numerācijas apgabaliem, izmantojot gan standarta tālruņu tīklus, gan WhatsApp lietotni. Krāpnieki zvana bieži un uzstājīgi, cenšoties pārliecināt upuri, ka pieteikuma formas aizpildīšana ir pietiekams pamats obligātai investīciju veikšanai.

Lai veicinātu iedzīvotāju uzticēšanos viltus reklāmām, tiek kopēti zināmu Latvijas mediju vizuālie tēli - LSM.lv, delfi.lv, tvnet.lv, jauns.lv un citi. Vairums reklāmās tiek izmantoti nejauši ģenerēti domēnu vārdi dažādās zonās. Populārākie ir .sbr, .lat, .info, .world, .online. Atrasti arī vairāki .lv domēna izmantošanas gadījumi, kad nosaukumi veidoti fonētiski līdzīgi mediju nosaukumiem.

Vairāki no upuriem ne tikai ir veikuši ieguldījumus viltus platformās, bet arī samaksājuši krāpniekiem, kuri, uzdodoties par “konsultantiem” vai “advokātiem”, pret papildu atlīdzību solīja ieguldījumus “atgūt”. Šie incidenti apliecina, ka investīciju krāpnieki turpina pielāgot savas metodes un izmanto cilvēku uzticēšanos un vēlmi atgūt jau zaudēto naudu.

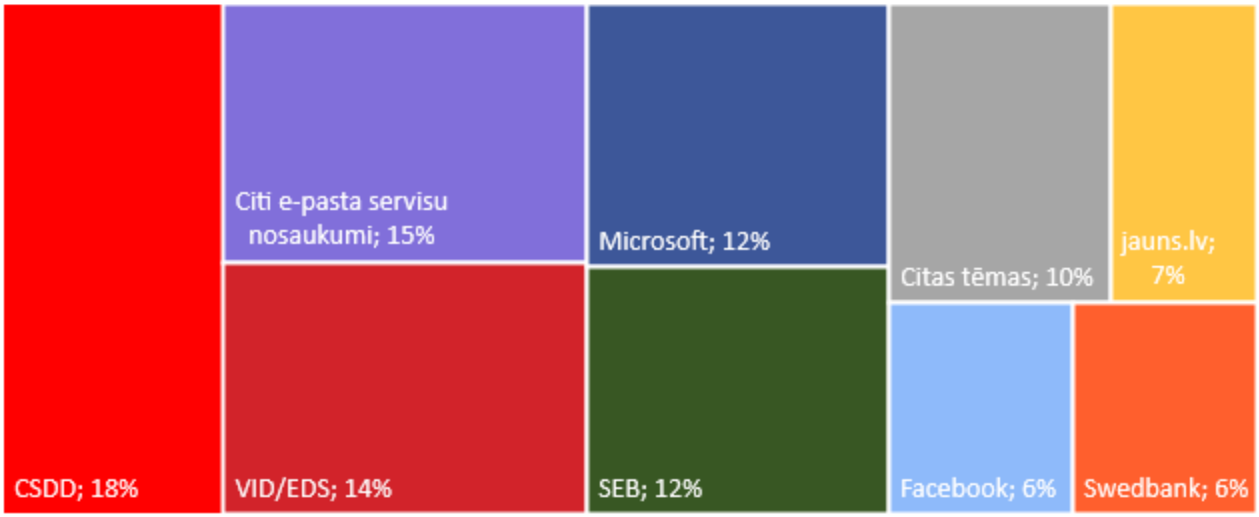
Pikšķerēšanas uzbrukumi

2025. gadā tika novērotas intensīvas krāpniecisku tālruņa zvanu (vikšķerēšana), viltus SMS (smikšķerēšana), e-pastu (pikšķerēšana) kampaņas. Galvenie riski bija saistīti ar autentifikācijas datu zādzību un nesankcionētu piekļuvi lietotāju kontiem.

Krāpnieki izmantoja pārkāpumu un soda naudu tematiku, piemēram, izsūtīja viltotus paziņojumus CSDD vārdā par it kā fiksētiem ātruma pārkāpumiem, kā arī "Mobilly" stāvvietu apmaksas un VID nodokļu atmaksas paziņojumus. Plaši izplatīti bija arī viltus ziņojumi "Latvijas Pasts" un citu kurjerpastu vārdā, kā arī dažādas viltus ziņas, kas imitēja finanšu iestāžu paziņojumus.

Izplatītākās krāpniecības kampaņas un tematika

(% daļa no kopējā CERT.LV apstrādāto pikšķerēšanas ziņojumu skaita 2025. gadā)



Krāpnieku aktivitāte viltoto paziņojumu izplatīšanā pārsvarā tika novērota darba dienu vakaros un nedēļas nogalēs, kā arī pirms un svētku dienu laikā, cerot uz upuru modrības mazināšanos.

Katrā kampaņā tika izmantoti vairāki desmiti domēna vārdu, no kuriem tikai nedaudzi atradās .lv zonā. Attāla līdzība ar oriģinālo iestādes nosaukumu tika fonētiski papildināta ar tādiem vārdiem kā "csn", "csd", "pieeja", "vld", "parkapums", "pazinojums", "citadele", "swed" u.c. Savukārt, izsūtot krāpnieciskas ziņas "Latvijas Pasts" aizsegā, uzbrucēji mēdza izmantot arī lietuviešu vārdu "pastas" un igauņu vārdu "posti".

CERT.LV speciālisti aktīvi apzināja iespējamos reģistrētos pikšķerēšanas domēna vārdus un ierobežoja piekļuvi tiem, iekļaujot šos domēnus DNS ugunsmūra (dnsmuris.lv) RPZ servera sarakstos.

Viltoti rēķini

Pārskata periodā izkrāptas lielas naudas summas, ielaužoties vairākos Latvijas un ārvalstu sadarbības partneru uzņēmumu e-pasta sistēmās. No visiem ziņotajiem zaudējumiem lielākais zaudējumu apmērs vienam uzņēmumam pārsniedza 500 000 EUR.

Lai piekļūtu uzņēmumu e-pastiem, uzbrucēji izmantoja standarta metodes:

- pikšķerēšanu;
- datu zagšanas ļaunatūru paroļu iegūšanai;
- cietušā e-pasta serverī ievietotu filtru, kas pārsūta sarakstes kopijas uzbrucējiem;
- upurim līdzīga domēna vārda iegādi pēc biznesa sarakstes par apjomīgu darījumu identificēšanas - ar tīmekļa vietnes atdarinājuma izvietošanu vai bez tās;
- krāpnieku modificētu un pārsūtītu e-pastu, kurā maksājuma saņēmēja konts aizstāts ar uzbrucēja kontrolētu kontu.

Pēc naudas saņemšanas uzbrucēji dažkārt turpina iejaukties sarakstē, aizbildinoties ar maksājumu apstrādes problēmām, kamēr nozagtā nauda tiek pārskaitīta, izmantojot dažādas noziedzīgi iegūtu līdzekļu legalizācijas shēmas.

Tipiskākie uzlauzto e-pastu lietotāji ir grāmatveži un uzņēmuma vadības darbinieki. Vairākos gadījumos uzbrucējiem nav traucējis iejaukties maksājumu veikšanas procesā arī tad, ja grāmatvedību nodrošinājis ārpakalpojuma sniedzējs.

Būtisks secinājums - grāmatvedības un struktūrvienību vadītāju amati ir pozīcijas, kuru e-pasti jāaizsargā īpaši rūpīgi.

Ieteikumi

Obligāti jālieto vairāku faktoru autentifikācija. Vēlams izmantot pret pikšķerēšanu noturīgu metodi, piemēram, FIDO2, WebAuthn, vai Passkey.

Jebkura norēķinu kontu maiņa jāapstiprina ar elektroniski parakstītu dokumentu, nepieciešamības gadījumā veicot arī papildu saskaņošanu telefoniski.

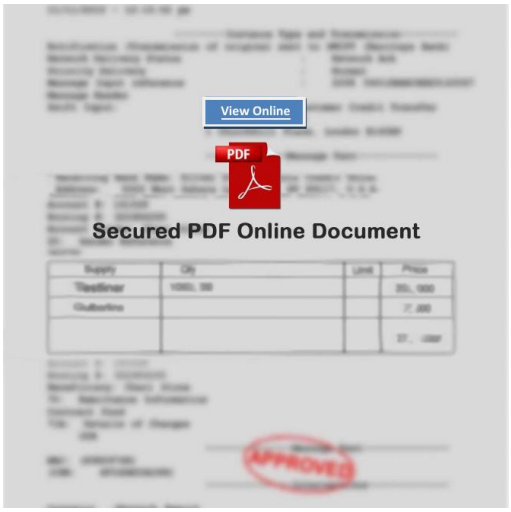
Papildu aizsardzībai ieteicams izmantot specializētu dublikātu meklēšanas pakalpojumu, kas nodrošina uzņēmuma domēna vārda vai nosaukuma izmantošanas monitoringu.

Microsoft 365 pikšķerēšana

Izmantojot viltotas vēstules zināmu sadarbības partneru vārdā, uzbrucējiem vairākkārt izdevies piekļūt pārtikas un kokrūpniecības uzņēmumu darbinieku Microsoft 365 kontiem.

Piekļuve pārņemta kontiem, kuros kā otrais autentifikācijas faktors tika izmantots OPT kodu kalkulators.

Uzbrukumos izmantota MITM ("man-in-the-middle") tehnika, ar kuru tika pārtverts upura divu faktoru autentifikācijas (2FA) sesijas marķieris ("token").



Uzbrukuma norises etapu ķēde

- Cietušais saņem e-pastu ar aicinājumu izvērtēt dokumentu, kas saistīts ar kādu projektu.
- Dokuments (parasti PDF vai DOCX formātā) izvietots partneru Microsoft Sharepoint serverī, leģitīmi un bez aizdomu radīšanas.
- Dokumentā ievietota saite uz ārēju tīmekļa resursu, kas atver Microsoft 365 autentifikācijas dialogu. Vietne vizuāli nav atšķirama no oficiālā Microsoft 365 autentifikācijas dialoga loga, jo starpniekserveris attēlo oriģinālo Microsoft saturu.
- Cietušais ievada paroli un Microsoft Authenticator lietotnes OTP kodu, tādējādi apstiprinot Microsoft 365 sesijas izveidi starp uzbrucēju un Microsoft vietni.
- Savienojuma sesija ar starpniekserveri un cietušo tiek pārtraukta.
- Uzbrucēji piekļūst cietušā Microsoft 365 kontam un veic pikšķerēšanas dokumenta ievietošanu upura SharePoint vai OneDrive platformā.

- Uzbrucēji izsūta pikšķerēšanas e-pastu visiem cietušā adrešu grāmatā esošajiem kontaktiem.

Noziedznieki iegūst ne tikai visu uzbrukumā skartā Microsoft 365 konta e-pasta saturu, bet arī dokumentus un datus no uzņēmuma OneDrive/SharePoint koplietošanas resursiem.

Izmeklēto incidentu analīze neuzrāda masveida failu kopēšanu vai dzēšanu; uzbrucēji primāri nodarbojušies ar jaunu pikšķerēšanas e-pastu izsūtīšanu. Ilgstoša konta kompromitēšana var novest pie būtiskām un neprognozējamām sekām, tostarp komercnoslēpuma un personas datu noplūdes.

Uzbrucēju pieslēgumi lielākoties veikti, izmantojot VPN pakalpojumus, kas izvietoti ASV un ES valstīs.

Lai gan Microsoft 365 kontiem tehniski ir pieejams netipisku pieslēgumu un pēkšņas lietotāja IP adreses maiņas monitorings, šī funkcionalitāte nav iekļauta Microsoft Entra ID bāzes līmeņa licencē.

Cietušie uzņēmumi šāda veida incidentus konstatējuši tikai pēc ārējo partneru ziņojumiem par netipisku e-pastu saņemšanu, ko nevar uzskatīt par pieņemamu un pietiekamu monitoringa vai drošības metodi.

Ieteicams izveidot papildu žurnālfailu analīzes un detektēšanas kārtulas, kas brīdinātu par netipisku e-pastu plūsmu vai pieslēgumiem no ārvalstu IP adresēm.

Realizētie kiberuzbrukumi uzskatāmi parāda, ka SMS un kodu kalkulatora risinājumos balstīti divu faktoru autentifikācijas mehānismi nav pilnībā droši pret tehniski pilnvērtīgiem pikšķerēšanas uzbrukumiem. Šos OTP mehānismus ieteicams aizstāt ar pret pikšķerēšanu drošiem divu faktoru autentifikācijas veidiem:

- fiziski pieejamām autentifikācijas ierīcēm, kas izmanto FIDO2/WebAuthn protokolus;
- biometrisko autentifikāciju ar iekārtas TPM moduli;
- PIN kodu, kas savienots ar iekārtas TPM moduli, piemēram, “Windows Hello for Business”.

Izspiedējvīrusi

Pārskata gadā konstatēti deviņi izspiedējvīrusu uzbrukumi, tostarp četri apjomīgi, kas tika īstenoti, nošifrējot vairākus desmitus serveru un datoru. Lai gan realizētais uzbrukumu skaits nav liels, šie joprojām ir bīstamākie uzbrukumi ar kritisku kaitējumu IT un datorsistēmām.

Piekļuves metodes (MITRE ATT&CK: T1133)

Izspiedējvīrusu incidentos ielaušanās un izplatīšanās visbiežāk notiek, izmantojot nepietiekami vai nepareizi nokonfigurētu attālinātās darbvirsmas rīku Microsoft RDP (“Microsoft Remote Desktop”). Lietotāju paroles tiek iegūtas ar pilnās pārlases metodi vai datu zagšanas ļaunatūras palīdzību.

Lai gan paroļu pilnās pārlases uzbrukumi ir viegli pamanāmi serveru žurnālfailos, praksē to uzraudzība bieži tiek veikta nepietiekami. Bieži konstatēti gadījumi, kad paroļu pārlases uzbrukumi turpinās vairākus mēnešus pēc kārtas.

Analīze atklāja, ka ikvienā incidentā RDP serviss bijis pieejams no jebkurām publiskajām IP adresēm un bez tīkla līmeņa pirmsautentifikācijas aizsardzības.

RDP pakalpojuma porta maiņa no noklusējuma TCP 3389 uz nestandarta portu (piemēram, TCP 3999), pret šī veida uzbrukumiem neaizsargā, jo tīkla skeneri ātri un efektīvi spēj identificēti tieši RDP servisu.

Tāpat uzņēmumu īpašnieki ne vienmēr pietiekami labi pārzina sava tīkla uzbūvi, tāpēc bieži nav informēti par publiskajā tīmeklī pieejamu RDP pakalpojumu.

VPN vārteju un citu tīkla iekārtu ievainojamības

Pārskata gadā tika atklātas daudzas būtiskas ievainojamības tīkla iekārtās, tostarp arī Latvijā populāro ražotāju Fortinet (CVE-2025-25257, CVE-2025-58034, CVE-2025-59718, CVE-2025-64446 u.c.) un Ivanti (CVE-2025-22457, CVE-2025-0282, CVE-2025-4428) ievainojamības.

Tika atklāti gadījumi, kuros uzbrucēji kompromitēto tīkla iekārtu konfigurāciju maina tā, lai atļautu piekļuvi RDP un VPN servisiem publiski no visas pasaules.

Tā kā izspiedējvīrusu izplatītāju uzmanības lokā ir minēto izstrādātāju iekārtas, regulāri jāveic sistēmu un programmatūras atjauninājumi.

Ievainojama tīmekļa vietņu programmatūra

Nesankcionētai piekļuvei serveru infrastruktūrā tiek izmantotas laicīgi neatjaunotas satura vadības sistēmas un vietnes, kas veidotas ar novecojušiem programmēšanas ietvariem.

Incidentos izmantotas Telerik (CVE-2019-18935: Remote Code Execution via Insecure Deserialization in Telerik UI) un WordPress ievainojamības. Publiski pieejamo resursu nepārtraukta uzraudzība un atjaunināšana ir obligāta visā informācijas sistēmas izmantošanas laikā.

Kompromitētajās datorsistēmās izmantotie rīki

Paroļu ieguve

Lai nodrošinātu piekļuvi lokālajiem resursiem, kas atrodas iekšējā datortīklā, uzbrucēji uzlauztajās iekārtās uzstāda dažādu paroļu izgūšanas rīku komplektu, primāri Mimikatz (https://github.com/gentilkiwi/mimikatz MITRE ATT&CK: S0002) ar PowerShell atvasinājumu.

Pārējie atrastie rīki:

Saite	Nosaukums
(https://www.nirsoft.net/utils/bullets_password_view.html)	BulletsPassView.exe
(https://www.nirsoft.net/utils/network_password_recovery.html)	netpass.exe
(https://www.nirsoft.net/utils/password_sniffer.html)	SniffPass.exe
(https://www.nirsoft.net/utils/wireless_key.html)	WirelessKeyView.exe
(https://www.nirsoft.net/utils/dialupass.html)	dialupass.exe
(https://www.nirsoft.net/utils/internet_explorer_password.html)	iepv.exe
(https://www.nirsoft.net/utils/mailpv.html)	mailpv.exe
(https://www.nirsoft.net/utils/mspass.html)	mspass.exe
(https://www.nirsoft.net/utils/opera_password_recovery.html)	OperaPassView.exe
(https://www.nirsoft.net/utils/pst_password.html)	PstPassword.exe
(https://www.nirsoft.net/utils/router_password_recovery.html)	RouterPassView.exe
(https://www.nirsoft.net/utils/pspv.html)	pspv.exe
(https://www.nirsoft.net/utils/remote_desktop_password.html)	rdpv.exe
(https://www.nirsoft.net/utils/vnc_password.html)	VNCPassView.exe

Rīks	Apraksts	Primārais MITRE ATT&CK
BulletsPassView.exe	Atklāj paroles aiz *** maskas pārlūku formās	**T1555.003 – Credentials from Web Browsers**
netpass.exe	Izgūst Windows saglabātās tīkla paroles	**T1555.004 – Windows Credential Manager**
SniffPass.exe	Pārtver paroles no tīkla plūsmas	**T1040 – Network Sniffing**
WirelessKeyView.exe	Izgūst saglabātās Wi-Fi atslēgas/paroles	**T1016.002 – Wi-Fi Discovery**
dialupass.exe	Izgūst Dial-up/RAS/VPN ierakstu lietotājvārdu/paroli/domēnu	**T1555 – Credentials from Password Stores**
iepv.exe	Izgūst Edge / IE saglabātās paroles	**T1555.003 – Credentials from Web Browsers**
mailpv.exe	Izgūst e-pasta klientu kontu paroles	**T1555 – Credentials from Password Stores**
mspass.exe	Izgūst IM lietotņu paroles	**T1555 – Credentials from Password Stores**
OperaPassView.exe	Izgūst Opera pārlūka saglabātās paroles no wand.dat	**T1555.003 – Credentials from Web Browsers**
PstPassword.exe	Izgūst Outlook PST faila paroli	——
RouterPassView.exe	Izgūst ISP, maršrutētāja admin. un Wi-Fi paroles no rūtera rez.kopijas faila	**T1552.001 – Credentials In Files**
pspv.exe	Izgūst paroles no Windows paroļu glabātuves un IE/Outlook Express/MSN Explorer	**T1555 – Credentials from Password Stores**
rdpv.exe	Izgūst Microsoft RDP rīka saglabātās paroles no .rdp failiem	**T1552.001 – Credentials In Files**
VNCPassView.exe	Izgūst VNC paroles reģistra no HKCU un “all users”	**T1552.002 – Credentials in Registry**

Risinājums: AppLocker (vai analogs), centralizēti žurnālfaili, SOC.

Privilēģiju eskalācija

Lai iegūtu SYSTEM līmeņa piekļuves tiesības, izmantots rīks “PrintSpoofer” (https://github.com/itm4n/PrintSpoofer), taču vairumā gadījumu lietotājiem datoros jau ir bijušas administratora līmeņa privilēģijas, rezultātā uzbrucējam papildus privilēģiju eskalācija nav bijusi nepieciešama.

Tīkla savienojuma izveide un uzturēšana ar C&C serveri

Identificēts kontroles tīkla tuneļa rīks NGROK (ngrok.exe https://ngrok.com), kas izmantots, lai pārvirzītu RDP savienojumu caur nestandarta portiem. Tādējādi mēģināts mazināt IDS/IPS sistēmu spēju šos savienojumus atklāt.

Iekštīkla skenēšana

Uzbrucēji lokālā datortīkla izlūkošanai un izpētei izmanto aktīvo ierīču atklāšanas rīkus, piemēram, Angry IP Scanner (https://github.com/angryip/ipscan/releases).

Sānu (laterālā) kustība iekštīklā

Ugunsmūra iestatījumu maiņa: Lai atvieglotu pārvietošanos iekštīklā, ar komandrindas netsh.exe veic Windows Defender Firewall modifikāciju, pievienojot jaunu kārtulu (nosacījumu), kas ļauj veikt RPD pieslēgumus portam 3389 no jebkuras avota IP adreses.

NTLM SMB savienojumi: Jau iepriekš vairākkārt minētais RDP ir uzbrucēju primārais izvēles rīks. Izmeklēšana atklāja, ja tā izmantošana nav iespējama, kā alternatīvu noziedznieki lieto "Pass the Hash" un "Pass the Ticket" metodes savienojumu izveidei. Konkrētāk, ar "Mimikatz" rīku izgūtas NTLM jaucējvērtības, ar kurām no jauna izveidotas Kerberos autentifikācijas biļetes.

Antivīrusu programmu atslēgšana: Izspiedējvīrusu gadījumā pirms šifrējošās ļaunatūras izplatīšanas un izpildes tiek atslēgta sistēmas pretvīrusu programma un citi aizsardzības risinājumi. Identificētas šādas izspiedējvīrusu saimes:

- INC Ransomware;
- Lab Ransomware;
- Sil3ncer Ransomware;
- Proton/Shinra Ransomware;
- Sarcoma Ransomware.

Izspiedējvīrusu uzbrukumos bieži izmanto RAAS ("ransomware-as-a-service") modeli, kur izspiedējvīrusu infrastruktūru uztur viena noziedzīga grupa, bet reālos uzbrukumus veic citi. Izpirkuma samaksāšanas gadījumā tas tiek sadalīts starp iesaistītajām pusēm.

Vienā incidentā cietušais uzņēmums samaksāja uzbrucēju prasīto izpirkumu un datus atguva. Izpirkuma samaksa negarantē datu atgūšanu, sistēmu pilnīgu atjaunošanu vai to, ka nozagtie dati netiks tālāk izmantoti vai publiskoti. Samaksa vienlaikus finansē turpmāku noziedzīgu darbību un palielina risku, ka organizācija tiks atkārtoti mērķēta. CERT.LV neatbalsta izpirkuma maksāšanu.

Rezerves kopijas: Trijos incidentos uzbrucēji sabojāja gan produkcijas datus, gan to rezerves kopijas, kas ir viens no galvenajiem datu atjaunošanas mehānismiem pēc tehniskas avārijas. Izspiedējvīrusu gadījumā uzbrucēju mērķis nav tikai aktuālie dati. Prioritāte ir arī atrast rezerves kopiju glabātuves un pārvaldības kontus, lai liegtu atjaunošanu un pārņemtu kontroli. Tāpat datu kopijas (arī automātiski sinhronizētās mākonī, datu centrā) var tikt pārrakstītas ar jau šifrētiem failiem. Tādēļ ar regulāru kopēšanu vien nepietiek - rezerves datiem un pārvaldības kontiem jābūt nošķirtiem. Svarīgi, ja sistēmas administratoram ir pilnas pieejas datu kopijas glabāšanas vietai, tās nav pasargātas no izspiedējvīrusu bojājumiem.

Fiksēti gadījumi, kad rezerves kopijas pēc uzbrukuma paliek neskartas, taču tas ne vienmēr nozīmē labu datu kopiju pārvaldību, bieži uzbrucēji vienkārši nav paspējuši sasniegt attiecīgo vidi vai nav pareizi identificējuši atjaunošanas infrastruktūru. Vienā incidentā organizācijas datus izglāba nevis klasiskās rezerves kopijas, bet failu servera momentuzņēmumi ("snapshot"). Tomēr momentuzņēmumi neaizstāj pilnvērtīgas rezerves kopijas, tie nav universāls ilgtermiņa aizsardzības mehānisms pret dzēšanu, bojāšanu vai kompromitētu pārvaldības vidi. Risinājums: Laba rezerves kopiju pārvaldības prakse ir dokumentēta procedūra, datu svarīguma kategorizēšana, skaidra secība un termiņš, kādā atjaunot kritiskās funkcijas. Rezerves kopijām jābūt nošķirtām no ikdienas darba vides, aizsargātām pret nesankcionētu piekļuvi un pārvaldītām ar paaugstinātas kontroles administratoru kontiem. Regulāri jāpārbauda kopiju integritāte, pieejamība un praktiska atjaunošanas spēja.

Datu noplūdes: lai cietušos piespiestu sadarboties, izspiedēju grupējumi var draudēt publiskot vai pārdot nozagtos datus, lai palielinātu spiedienu samaksāt izpirkuma maksu. Šāda rīcība konstatēta vienā incidentā, kurā nozagtie dati tiešām tika publicēti tumšajā tīmeklī jeb Darknet.

2. Citu valstu organizēti kiberuzbrukumi Latvijai (APT) un to ietekme uz informācijas sistēmām

APT (Advanced Persistent Threat) apdraudējumi ir vieni no sarežģītākajiem kiberdrošības incidentu veidiem, jo tos raksturo augsts tehniskais izpildījums, ilgstoša darbība un stratēģiskie mērķi.

APT kiberapdraudējumus parasti īsteno labi finansēti un tehniski spējīgi kiberuzbrucēji, kas visbiežāk ir politiski, ekonomiski vai stratēģiski motivēti un darbojas ar valsts atbalstu. Visu nepieciešamo tehnisko līdzekļu un aprīkojuma pieejamība ļauj uzbrucējiem ne tikai kompromitēt atsevišķas informācijas sistēmas daļas, bet arī ilgstoši un nepamanīti izzināt iekšējās infrastruktūras uzbūvi, iegūt priviliģētu lietotāju tiesības un slēptu pārvaldību, un pārvietoties starp infrastruktūras ierīcēm vairākos tīkla segmentos.

Trešo valstu izlūkdienesti bieži ir koordinatori vai pilna darbības cikla uzturētāji, tādēļ to var dēvēt arī par spiegošanu digitālajā vidē. Vērojams arvien straujāks tehnisko spēju pieaugums organizētā kibernoziedzībā un arvien ciešāks trešo valstu atbalsts un iesaiste kiberoperāciju ofensīvās. Tas izteikti vērojams Krievijā, kur varas vertikāle cieši integrēta ar organizēto noziedzību. APT izmeklēšanas un novēršanas gadījumos būtiska ir sadarbība ar valsts drošības iestādēm.

Latvijas kiberdrošībai lielākais apdraudējums ir Krievijas organizētās noziedzības grupas. Krievijas atbalstītie APT grupējumi veic kiberuzbrukumu ofensīvas ne tikai pret Latviju, bet arī ES un NATO dalībvalstīm kopumā. Krievija pēdējo 2-3 gadu laikā ir arvien plašāk izvērsusi aizsega uzņēmumu tīklu, kas reģistrē un uztur it kā likumīgus IT pakalpojumu sniedzējus, mitināšanas kompānijas un nelielus elektronisko sakaru komersantus. Tikmēr īstenībā šie uzņēmumi darbojas kā čaulas kompānijas Krievijas izlūkdienestu un valdības atbalstītām kiberoperāciju ofensīvām (angliski “bulletproof hosting”).

Arvien biežāk ir vērojama ar Ķīnas Tautas Republiku (ĶTR) saistītu uzbrucēju aktivitāte. To tehniskais fokuss pamatā ir vērsts uz tīkla iekārtām. Īstenotā kompromitēšanas gadījumā tālāk tiek veikti mēģinājumi iegūt plašu kontroli cietušās iestādes iekštīkla infrastruktūrā.

Vairāku gadu garumā APT ir nerimstošs drauds Latvijas informācijas sistēmām. APT uzbrucēju grupas ir īpaši bīstamas, tām ir ievērojami resursi, taktikas un tehniskās metodes pastāvīgi mainās un tiek īpaši pielāgotas upuru infrastruktūrām. Kaut arī APT grupējumi bieži uzbrukumos izmanto arī jaunas vai pat līdz šim nezināmas programmatūras ievainojamības, tomēr joprojām uzbrucējiem pietiek ar iespēju izmantot konfigurācijas kļūdas un salīdzinoši vecas ievainojamības. Tāpēc infrastruktūras īpašniekiem ir jāsaglabā pastāvīga modrība, jāveic pilna IT saimniecības uzraudzība un jāievēro drošības un labas pārvaldības prakses.

2.1. Nozīmīgākie incidenti: metodes, rīki un indikatori

2025. gadā izmeklētajos APT uzbrukumos ir secināms, ka tie gandrīz nekad nav nejauši, jo savlaicīgi pirms uzbrukuma sākuma tiek veikta rūpīga mērķa informācijas sistēmu infrastruktūras un to piegādes ķēdes (izstrādātāju) aktīva un pasīva izpēte. Šāda izlūkošana jeb nolasīšana (“enumerācija”) palīdz apzināt mērķa ārējā perimetra ierīces, tehnoloģijas un publiskā tīmeklī eksponētos servisus, piemēram, ugunsmūri, VPN vārtejas un tīmekļa serveri.

Izlūkošana ilgst vairākus mēnešus. Tā tiek veikta pakāpeniski, skenējot atsevišķus mērķa organizācijas IP apgabalus. Ārējā perimetra skenēšanai tiek izmantotas arī Latvijas IP adreses no, piemēram, uzlauztām Android operētājsistēmas ierīcēm vai robottīkliem (“botnet”) pievienotiem mājas un nelielu uzņēmumu maršrutētājiem. Kā būtiska Krievijas kiberuzbrucēju taktikas izmaiņa ir noteikti pieminama ORB (Operational

Relay Boxes) jeb starpnieksistēmu tīkla aktīva izveide, kas sastāv no kompromitētām vai nopirktām sistēmām kiberuzbrukumu mērķa valstī.

Latvijas IP adreses lietojis CERT.LV redzes lokā par kiberuzbrukumiem nonākušais uzņēmums "Stark Industries Solutions LTD".

Izlūkošana ārējā perimetra ierīcēs un servisos notiek ne tikai ievainojamību konstatēšanā, bet arī pikšķerēšanas uzbrukumos iegūtu piekļuves datu izmēģināšanā. Tāpat novērots, ka bez pikšķerēšanas uzbrukumiem piekļuves dati var būt nopirkti vai iegūti citā veidā, piemēram, no datu zadzēju vīrusiem vai lietotājvārdu/paroļu datubāzēm. Tas nozīmē, ka uzbrucējs sākotnējo piekļuvi veic, vienkārši ielogojoties ar derīgu lietotāja vārdu un paroli, tādējādi iegūstot neautorizētu piekļuvi e-pasta kontiem, RDP, VPN lietotājiem un citiem pakalpojumiem.

Kāda incidenta analīze atklāja, ka uzbrukums aizsākās ar ļaundara identificētu organizācijas "Microsoft Exchange Web Services" (EWS) API punktu - https://pasts.***. lv/EWS/Exchange.asmx, kura piekļuve uzņēmuma Aktīvajā Direktorijā izmantoja NTLM autentifikāciju un nebija ierobežota ar VPN.

Var secināt, ka uzbrucējs izmeklēšanas etapā ir atradis veidu, kā organizācijas e-pastā apiet 2FA. Ievadot derīgus NTLM autentifikācijas datus (lietotājvārdu un paroli), uzbrucējs iegūst tiesības sadarboties ar EWS funkcionalitāti, tādējādi iegūstot brīvu pieeju e-pasta kontam bez obligātā otrā faktora koda ievadīšanas.

Situāciju bīstamāku padarīja apstāklis, ka uzbrucēja rīcībā vecākā informācijas tehnoloģiju administratora kontam ar derīgajiem NTLM pieejas datiem bija paplašinātas pieejas tiesības (piederība grupai "View-Only Organization Management"). Izmantojot EWS funkcionalitāti, varēja nolasīt "Microsoft Exchange" lietotāja parametrus, ļaujot uzbrucējiem autentificēties un izgūt konkrētā lietotāja e-pasta saturu.

Piekļuve organizācijas e-pastam nedeva uzbrucējiem iespēju nodrošināt ne pastāvīgu pieeju, ne tālāku pārvietošanās turpināšanu iekštīklā. Taču konkrētais uzbrukums ļāva no darbinieka e-pasta satura iegūt vairākus derīgus VPN lietotāja piekļuves datus. Tas, savukārt, nodrošināja gan pastāvīgu pieeju iekštīklā, gan iespēju noskaidrot organizācijas iekšējās informācijas sistēmas un meklēt tālākās iespējas privilēģiju paaugstināšanai.

APT darbības analīzes rezultāti uzrādīja šādas noziedzīgo grupējumu raksturīgas darbības pēc sākotnējās piekļuves un pastāvīgās pieejas izveidošanas:

- Pēc pastāvīgās pieejas izveides vairāku dienu atturēšanās no jebkādām aktivitātēm;
- Klusuma posma noslēgumā uzbrucējs pakāpeniski veic iekštīkla izlūkošanu (nolasīšanu);

- Iekštīkla nolasīšanas posmam raksturīga “SYN” tipa skenēšana, meklējot ierīces ar šādiem atvērtiem portiem: 445 (SMB), 22 (SSH), 80 (HTTP), 443 (HTTPS), 3389 (RDP), 5985 (WinRM) un 5986 (WinRM HTTPS);
- “Kerberos” RC4 (0x17) algoritma šifrētu biļetenu (TGS) ieguve ar mērķi veikt privilēģiju eskalāciju, iegūstot AD servisa lietotāja paroli;
- Darbstaciju lokālo administratoru paroļu (t.sk. LAPS) iegūšana un izmantošana sānu (laterālās) kustības veikšanai;
- Piekļuve SMB koplietotām mapēm ar kompromitēto lietotāju NTLM piekļuves datiem (t.sk. “Pass the Hash” metodi) vai izmantojot anonīmo pieteikšanos (“Anonymous logon”);
- Piekļuve iekštīkla ierīcēm ar RDP protokolu, izmantojot kompromitēto lietotāju NTLM piekļuves datus (t.sk. “Pass the Hash” metodi);
- Windows reģistra vienību (SAM, SECURITY un SYSTEM) izgūšana no identificētiem priviliģētiem lietotājiem (administratoriem, IT atbalsta darbiniekiem) izmantojot RemoteRegistry pakalpojumu.

Atrasti gadījumi, kad APT grupējumi izmitina kontroles serveru (Command and Control) infrastruktūru Latvijas reģiona IP apgabalā, piemēram, ar Ķīnu saistīts APT grupējums “APT41” daļu “KEYPLUG” ļaunatūras mitināja Latvijas IP adresē. Atklāti trīs ļaunatūras “KEYPLUG” servera programmatūras paraugi.

Datortīkla plūsmas šifrēšanai ar komandserveri (C&C) visas trīs bināro failu versijas izmanto “WolfSSL”. Secināts, ka binārie faili servera puses komunikācijai ar klientiem izmanto “QUIC” tīkla protokolu, precīzāk, pilda “QUIC listener” funkciju (UDP protokola ports 443). Visticamāk, QUIC izmantošana saistīta ar iebūvētu tīkla plūsmas šifrēšanu un iespēju tuneli ārēji interpretēt kā HTTP/3 datu plūsmu uz UDP 443 portu. Šāda pieeja samazina atklāšanas iespējamību un apgrūtina tīkla uzraudzību.

2.2. CERT.LV izmeklēšanā konstatētie ar APT grupējumiem saistītie informācijas sistēmu incidenti

Tehniskā informācija notikumu hronoloģiskā secībā

Izmeklēto APT grupējumu aktivitātes atbilstoši “MITRE ATT&CK” uzbrukuma matricai:

Sākotnējā piekļuve	
T1190	publiski eksponēto ierīču/servisu ievainojamību izmantošana
T1078	derīgu kontu vai akreditācijas datu izmantošana nesankcionētai piekļuvei
T1133	ārējas attālinātās piekļuves pakalpojuma, piem., VPN izmantošana iekļūšanai mērķa vidē

Izmeklētā APT darbības rokraksts iezīmē šī grupējuma priekšroku pieejas nodrošināšanai, izmantojot vai nu jaunu VPN lietotāju veidošanu, vai jau esošu ar derīgiem piekļuves datiem. Novērota izvairīšanās no pastāvīgas pieejas izveides ar tehniskiem risinājumiem un mehānismiem.

Taču identificēti arī gadījumi, kad APT grupējums veido pastāvīgo pieeju, instalējot kompromitētā sistēmā VPN klientus, piemēram, “SoftEther VPN”, kas ar kontroles serveri izveido šifrētu datu kanālu.

Pastāvīgā pieeja	
T1505	Serveru programmatūras komponentes
T1505.003	Web Shell: tīmekļa serverī izvietota ļaunprātīga komponente pastāvīgas piekļuves uzturēšanai un komandu izpildei

Tīmekļa čaulas joprojām ir viens no izplatītākajiem veidiem, kā uzreiz pēc sākotnējās piekļuves posma APT grupējumi izveido pastāvīgo pieeju uz kompromitētām perimetra vai tīmeklī eksponētām ierīcēm. Tīmekļa čaulas bieži tiek izmantotas kā rezerves variants neautorizētās pieejas nodrošināšanai gadījumos, kad neizdodas izveidot citus pastāvīgās pieejas mehānismus. Tādēļ noziedzīgie grupējumi regulāri uzreiz ievieto vairākas tīmekļa čaulas.

Privilēģiju eskalācija	
T1078.002	Derīgu domēna kontu izmantošana nesankcionētai piekļuvei, noturībai, privilēģiju paaugstināšanai vai aizsardzības apiešanai.
T1078.003	Derīgu lokālo kontu izmantošana tiem pašiem mērķiem kompromitētajā sistēmā (tajā skaitā no LAPS jeb “Local Administrator Password Solution” risinājuma).

Windows reģistru datu kopņu izgūšana, lai veiktu aktīvās direktorijas kontu jaucējsummu un lokālo administratoru kontu paroļu izgūšanu. APT uzbrukumos grupējumi veic reģistra SECURITY, SAM un SYSTEM kopņu eksportu. SECURITY kopne satur sistēmas šifrēšanas atslēgas, arī tādas, kas nepieciešamas SAM kopnē glabāto lokālo administratoru paroļu atšifrēšanai. Turklāt SECURITY kopne satur sistēmas LSA (Local Security Authority) datus, no kuriem iespējams iegūt domēna lietotāju paroļu jaucējfunkciju vērtības.

Atrastas liecības par procesiem, kas tiek darbināti reģistru kopņu eksporta laikā. Tas pierāda ļoti ticamu iespēju, ka uzbrukumos izmantots publiski pieejams rīks secretsdump.py (daļa no “Impacket” rīku komplekta). Lietojot secretsdump.py, uzlauztajā ierīcē uz īsu laiku raksturīga “RemoteRegistry” servisa aktivizēšana, kā arī nr.3 tipa jeb tīkla autentifikācija no uzbrucēja ierīces, izmantojot kompromitētos piekļuves datus. Pēc eksporta izgūtie Windows reģistri tiek novietoti direktorijā C:\Windows\Temp\.

Aktīvās direktorijas vidē kompromitēts domēna konts ar tiesībām lasīt LAPS lokālo administratoru pārvaldības risinājuma paroles veic visu šo pieejas datu (paroļu) izgūšanu. Tas uzbrucējam dod lokālā administratora privilēģijas jebkurai domēnam pievienotai Windows iekārtai. (MITRE ATT&CK: T1078.003)

Uzbrucējs ar kompromitētu AD kontu nolasa LAPS paroles, fragments no Domēna kontroliera žurnālfaila “Security”:

Laiks	datorvārds	Pieprasītāja lietotājvārds	ziņa
2025-MM-DD HH:MM:SS	<target_host>	<Requestor_username>	Control Access : Local Administrator password of Computer <target_host> was read by clicking attribute editor tab of AD Users & Computers by <Requestor_username>

Pastāvīgā pieeja	
T1558.003	Kerberoasting: uzbrucējs ar derīgu TGT pieprasa pakalpojuma biļetes SPN kontiem, pēc tam mēģina šifrēto daļu atkodēt bezsaistē pakalpojuma konta paroles iegūšanai.
T1558.004	AS-REP Roasting: uzbrucējs iegūst AS-REP atbildes kontiem, kuriem ir atslēgta Kerberos iepriekš autentifikācija, un pēc tam mēģina bezsaistē atšifrēt saņemtos datus paroles atklāšanai.

Minētā uzlaušanas tehnika ir efektīva "Kerberos" servisa biļeteniem (TGS) ar vāju RC4 algoritma šifrēšanu, kā arī NTLM 1.0 versijas autentifikācijai.

Gan RC4, gan NTLMv.1 ir novecojuši algoritmi, kas uzbrucējiem ļauj jaucējsummas salīdzinoši vienkārši atšifrēt, iegūstot paroles tīrā tekstā. Turklāt, ja domēnā ir atļauta RC4 šifrēšana, uzbrucēji var izmantot jau iepriekš izgūto NTLM jaucējsummu "Kerberos" TGT biļetena pieprasīšanai.

Sānu (laterālā) kustība	
T1550.002	Pass the Hash: nozagtu NTLM paroļu jaucējvērtību (bez nepieciešamības zināt pašu paroli) izmantošana nesankcionētai autentifikācijai un sānu (laterālai) kustībai – visbiežāk RDP, WINRM, SMB.
T1021.001	Remote Desktop Protocol (RDP): attālinātas piekļuves izmantošana, pieslēdzoties vai pārvietojoties starp sistēmām ar RDP (sānu kustība kompromitētā vidē).
T1021.002	SMB/Windows Admin Shares: attālināta piekļuve un darbību veikšana, izmantojot SMB un administratīvos koplietojumus, piemēram, ADMIN$, C$ vai IPC$, bieži failu kopēšanai vai komandu izpildei citās sistēmās.

Aizsardzības pasākumi pret APT aktivitātēm

Organizācijai jāapzina tīmeklī eksponētās ierīces un servisi, jāizveido un jāuztur saraksts, kas atvieglinās apkalpošanas procesu nākotnē. Jānodrošina regulāra atjaunināšana un jāīsteno padziļināts drošības monitorings. Pieeja publiski pieejamiem servisiem pēc iespējas jāierobežo, izmantojot VPN, IP adrešu balto sarakstu un citus piekļuves kontroles mehānismus. Īpaša uzmanība jāpievērš servisiem, kas izmanto LDAP vai aktīvās direktorijas autentifikāciju, to eksponēšana publiskā tīmeklī palielina piekļuves datu kompromitēšanas un nesankcionētas piekļuves risku.

Tā kā pēc noklusējama Microsoft Exchange "ActiveSync" un "Exchange Web Services" neatbalsta divu faktoru autentifikāciju, šo servisu publiska eksponēšana tīmeklī rada iespēju uzminēt paroles vai apiet otro faktoru un piekļūt e-pastu saturam. Ieteicamās darbības:

- regulāri veikt paroļu rotāciju;
- ja iespējams, veikt ar organizāciju saistītu datu noplūžu monitoringu;
- paroles un otrais faktors ir slepeni dati, kas jāpārsūta dažādos saziņas kanālos un nekad nav jāiekļauj vienā ziņojumā.
- ja iespējams, aicinām izmantot e-pasta šifrēšanu, piemēram, ar PGP atslēgām.

Ieteikumi administratoriem

- Atslēgt vai līdz minimumam samazināt NTLM izmantošanu, pilnībā pārejot uz modernākiem autentifikācijas protokoliem, piemēram, Kerberos. Obligāti atspējot "NTLM v1" un "RC4" autentifikācijas šifrēšanas algoritmus. Tāpat jāpārliecinās, ka Kerberos autentifikācijas protokols pārslēgts no novecojuša šifrēšanas algoritma RC4_HMAC_MD5 uz AES128 vai AES256;
- Ar grupu politiku ierobežot "ANONYMOUS LOGON" izmantošanu;
- Veikt konstantu paroļu rotēšanu un obligāti likvidēt "koplietošanas" kontus, proti, katram lietotājam jābūt savam kontam un profilam;
- Pieturēties pie minimālo tiesību piešķiršanas principa arī attiecībā uz IT sistēmu administratoriem un IT atbalsta darbiniekiem. Piemēram, ierobežot SPN ("Service Principal Name") tiesības domēna lietotājiem, ierobežot tiesības lasīt LAPS paroles u.c.;
- VPN savienojumu ierobežot līdz vienai vienlaicīgai sesijai;
- VPN pieslēgumiem izveidot atļauto sarakstu, t.i., IP adreses, no kurām drīkst slēgties klāt pie VPN;
- RDP pieslēgumus nodrošināt no atsevišķi izveidota administrēšanas starpniekservera ("jumphost"), aizliegt tiešos RDP savienojumus starp darbstacijām.

Kādas organizācijas incidenta piemērs

Kiberdrošības pārvaldības daļas saņēma kiberincidenta pieteikumu. Uz 12 lietotāju datoriem apmēram vienā laikā pretvīrusu sistēma Windows Defender uzrādīja brīdinājumu par neraksturīgām darbībām operētājsistēmā, karantīnā ievietojot iespējamo kaitīgo procesa datni.

Uzņēmums sniedza papildu informāciju par nesankcionētu autorizēšanos VPN tīklā, izmantojot administratoru VPN piekļuves datus. Administratora kontiem bija iespējota divu faktoru autentifikācija (2FA). Turklāt šajā gadījumā 2FA nozīmē daļu no paroles. Katram lietotājam parole sastāv no 4 ciparu PIN koda, kuram seko 6 ciparu (mainās katras x sekundes) kombināciju no 2FA autentifikācijas lietotnes.

Tika saņemta papildu informācija par nesankcionētu iekštīkla skenēšanu no IP adresēm, kas piešķirtas uzbrucējam pēc VPN autentifikācijas.

CERT.LV uzsāka incidenta izmeklēšanu, lai noskaidrotu:

- kādā veidā tiks veikti VPN savienojumi, izmantojot uzņēmuma lietotāju, tostarp administratoru, VPN autentifikācijas datus;
- kādas bija uzbrucēju darbības iekštīklā pēc sākotnējās piekļuves;
- kāds bija sākotnējās piekļuves veids;
- kādi pasākumi jāveic incidenta seku mazināšanai un novēršanai.

Kopsavilkums

Incidenta izmeklēšanas rezultāti atklāja uzbrucēja darbības sākumu vismaz no 2024. gada 18. novembra. Pēc žurnālfailu ierakstiem, laikā no 2024. gada 18. novembra līdz 2025. gada. 9. janvārim uzbrucējs izlūkoja IT infrastruktūras ārējo perimetru, lai noteiktu redzamos pakalpojumus (servisus) no ārējā tīkla. Uzbrucēja mērķis bija identificēt sākotnējās uzbrukuma iespējas.

Uzbrukuma sākotnējai fāzei raksturīga nolasīšana (“enumerācija”), kad kiberuzbrucējs cenšas identificēt iestādes publiski eksponētos nedroši konfigurētos vai ievainojamos pakalpojumus (servisus), kurus kompromitējot var ielauzties iekšējā tīklā.

Skenēšana minētajā laika posmā iekļāva e-pasta servisus, OWA (Outlook Web Access) un VPN vārtejas, kā arī citus pakalpojumus.

Laikā no 2024. gada 11. decembra līdz 2024. gada 28. decembrim novēroti vairāki mēģinājumi uzminēt VPN lietotājus, ar kuriem autentificēties uzņēmuma galvenajā VPN vārtejā. Uzbrukumu mēģinājumi veikti no IP adreses 136.0.185.54, kura pieder mitināšanas (“hosting”) pakalpojuma sniedzējām “Stark Industries Solutions Ltd.”. Šis pakalpojuma sniedzējs ir vairākkārt nonācis CERT.LV redzeslokā ar nelikumīgām aktivitātēm saistītu pakalpojumu sniegšanu un Krievijas valsts atbalstītām kiberoperācijām.

No 19. decembra līdz 30. decembrim atklāti vairāki īstenoti pieslēgumi pie vairāku uzņēmuma darbinieku e-pastiem. Kaut arī žurnālfaili neuzrādīja uzbrucēju publiskās IP adreses, pēc detalizētas izmeklēšanas HTTP pieprasījumos atrastais “User-Agent” identifikators norādīja tīmekļa pārlūku (piemēram, Firefox, Chrome, Edge) un datorsistēmu (Windows, Mac, Linux), no kuras pieprasījumi ir veikti. Šie pieprasījumi neatbilst lietotāju ikdienas darbības modelim, tādēļ vērtējami kā uzbrucēju aktivitāte.

Viens no uzlauztajiem e-pasta kontiem pieder uzņēmuma lietotāja atbalsta nodaļas personālam. Pēc piekļuves iegūšanas, uzbrucējam bija pilna redzamība e-pasta saturā, tajā skaitā izsūtītajiem un saņemtajiem e-pastiem. CERT.LV šajos e-pastos atrada nedroši uzglabātu aizsargājamu informāciju – vēstulēs nosūtītus vairāku darbinieku VPN piekļuves datus, turklāt vienkopus atradās gan PIN kods, gan QR kods (otrais autentifikācijas faktors, 2FA). Ar šo informāciju uzbrucējam ir viss nepieciešamais 2FA lietotāja profila uzstādīšanai, lai veiktu sekmīgas VPN autentifikācijas ar uzņēmuma darbinieku VPN kontiem. Šādas nosūtītas e-pasta vēstules bija četriem dažādiem uzņēmuma darbiniekiem. Tieši ar šo darbinieku VPN kontiem uzbrucējs veica pirmos pieslēgumus 2025. gada janvāra sākumā.

E-pastā atradās arī vēstules ar saitēm uz vairākiem uzņēmuma iekštīklā svarīgiem resursiem, kuri tiešā veidā saistīti ar administrēšanas un cita veida darba pienākumiem. Vēstules atklātā tekstā saturēja lietotājvārdu un paroli, ar kuru autentificēties šiem resursiem. VPN administrēšanā visai lietotāju atbalsta nodaļai bija viens koplietots konts ar lietotājvārdu, bez autentificēšanās papildu mehānismiem. Šāda prakse apgrūtina izmeklēšanas iespējas, jo daudz sarežģītāk noteikt, kurš darbinieks tieši ir veicis autentifikāciju. Pieslēdzoties ar minētajiem pieejas datiem, var pārvaldīt jebkuru uzņēmuma darbinieku (t.sk. IT drošības nodaļas un administratoru) VPN kontus - rediģēt, dzēst, izveidot, iegūt autentificēšanās datus.

Laika posmā no 09.01.2025. līdz 03.03.2025. atrastas VPN sesijas, kurās uzbrucējs veicis izlūkošanu (nolasīšanu) vairākiem iekšējā tīkla segmentiem, koplietošanas katalogiem un servisiem. Notika mēģinājumi izgūt darbstaciju sistēmas akreditācijas datus no reģistru ierakstiem (“RegDump”), lai piekļūtu paaugstinātu privilēģiju lietotāju kontiem. uzņēmuma informāciju par notikumiem uz CERT.LV nosūtīja 2025. gada 3. martā.

No 2025. gada 14. janvāra fiksēta aktīvās direktorijas (AD) lietotāju kontu izmantošana, kas apliecina, ka uzbrucējs sekmīgi ieguvis lietotāju paroļu jaucējsummas (NTLM hash). Analizētajos artefaktos (digitālo pēdu nospiedumi) novērota tendence atkārtoti nolasīt resursus ar jauniegūtajiem lietotāju kontiem. Šajā dokumentā visas minētās darbstacijas, serveri un lietotāju konti jāuzskata par kompromitētiem.

2025. gada februāra beigās novērots administratora pieslēgums pie RADIUS servera pārvaldības pakalpojuma. Padziļinātā izpētē tika konstatēts, ka pieslēgums noticis no iekšējās VPN apakštīkla IP adreses, bet sākotnējais VPN savienojums izveidots no “Stark Industries Solutions Ltd.” publiskās IP adreses. Pēc divām

dienām uzbrucējs izveidoja sekmīgus VPN pieslēgumus ar administratora VPN lietotāja konta pieteikšanās datiem.

Kopš incidenta sākuma CERT.LV ir sniedzis vairākas rekomendācijas tūlītējai seku mazināšanai. Visi ieteikumi atrodami sadaļā "Vispārīgie ieteikumi".

Balstoties uz incidenta izmeklēšanas procesā iegūtiem datiem, CERT.LV ar augstu varbūtību šo uzbrukumu saista ar kādu Krievijas valsts atbalstītu grupējumu, iespējams, ar specdienestiem GRU/SVR. Vairāk informācijas skatīt sadaļā "sasaiste jeb atribūcija".

Incidenta norise

Ārējā Tīkla Segmenta nolasīšana (enumerācija)

HTTP Servisu nolasīšana

Laika posmā no 2024. gada 18. novembra līdz 2025. gada 19. janvārim tika veikta ārējā segmenta HTTP servisu meklēšana un testēšana no IP adreses 136.0.185.54 (AS44477). Tika skenēti šādi resursi:

- e-pasta sistēmas;
- surogātpasta aizsardzības risinājuma ārējais interfeiss;
- dokumentu vadības sistēma;
- "Citrix Gateway" vārteja un citi resursi.

VPN lietotāju minēšana

Tika identificēti 17 lietotāju autentificēšanās mēģinājumi no IP adreses 136.0.185.54 (AS44477), taču nenotika neviens veiksmīgs autentificēšanās mēģinājums. Ieskats tabulā zemāk:

Datums, laiks	Nosaukums	Avots	Mērķis	Lietotāja vārds
Dec 11, 2024, 4:56:03 PM	Login Failed	136.0.185.54		
Dec 11, 2024, 4:56:20 PM	Login Failed	136.0.185.54		
Dec 18, 2024, 2:55:49 PM	Login Failed	136.0.185.54		
Dec 23, 2024, 6:59:07 AM	Login Failed	136.0.185.54		
Dec 23, 2024, 6:59:25 AM	Login Failed	136.0.185.54		
Dec 23, 2024, 6:59:42 AM	Login Failed	136.0.185.54		
Dec 24, 2024, 11:25:32 AM	Login Failed	136.0.185.54		
Dec 24, 2024, 11:25:46 AM	Login Failed	136.0.185.54		
Dec 24, 2024, 11:25:59 AM	Login Failed	136.0.185.54		
Dec 24, 2024, 11:26:12 AM	Login Failed	136.0.185.54		
Dec 24, 2024, 11:26:24 AM	Login Failed	136.0.185.54		
Dec 24, 2024, 11:26:37 AM	Login Failed	136.0.185.54		
Dec 24, 2024, 11:26:53 AM	Login Failed	136.0.185.54		
Dec 24, 2024, 11:27:25 AM	Login Failed	136.0.185.54		
Dec 24, 2024, 11:27:53 AM	Login Failed	136.0.185.54		

Dec 28, 2024, 12:40:43 PM	Login Failed	136.0.185.54		
Dec 28, 2024, 12:40:49 PM	Login Failed	136.0.185.54		

Sākotnējā piekļuve

Pēc e-pasta servisa žurnālfailu analīzes, konstatēta nedroša konfigurācija.

Pirmkārt, autorizācija no publiskā tīmekļa bez VPN tieši pasta serverī.

Otrkārt, iestatīta bāzes (“basic”) autentifikācija, kas izmanto tikai aktīvās direktorijas lietotāja vārdu un paroli bez otrā faktora (vairāk informācijas skatīt sadaļā “*.lv 2FA apiešana”).

Secināts, ka uzbrucēju sākotnējā piekļuve uzņēmuma infrastruktūrā ar lielu varbūtību notika, autentificējoties pasta serverī ar “basic” metodi un derīgiem aktīvās direktorijas lietotāju pieteikšanās datiem (tabulā zemāk). Pašlaik nav zināms veids, kādā uzbrucēji ieguva uzskaitīto lietotāju aktīvās direktorijas paroles.

Veicot pasta servera IIS servera žurnālfailu izpēti, atrasta anomālija lietotāja aģentā “Microsoft+Office/16.0+(Windows+NT+10.0;+Microsoft+Outlook+16.0.15427;+Pro”, tā izmantošana sakrīt ar bāzes pieteikšanās tipa Nr.8 (“basic, logon type 8”) autentifikāciju pasta serverī. Incidenta brīdī žurnālfailos nebija iespējota autentifikācijas procesa ārējo IP adrešu reģistrēšana, tādēļ nav iespējams noteikt anomāliju sākotnējo publisko IP adresi.

Pēc ielaušanās e-pastā, uzbrucēji veica saturu izpēti, atrodot derīgus lietotāju VPN akreditācijas datus.

IIS žurnālfailu saraksts ar īstenotajiem bāzes autentifikācijas piekļuves mēģinājumiem pasta serverī ar “Microsoft+Office/16.0+(Windows+NT+10.0;+Microsoft+Outlook+16.0.15427;+Pro” lietotāja aģentu:

Laiks	Tips	Saite
Dec 30, 2024 @ 11:37:26	GET	/autodiscover/autodiscover.svc
Dec 30, 2024 @ 07:28:51	GET	/autodiscover/autodiscover.svc
Dec 21, 2024 @ 16:30:49	GET	/autodiscover/autodiscover.svc
Dec 21, 2024 @ 16:30:49	GET	/autodiscover/autodiscover.svc
Dec 21, 2024 @ 13:14:37	GET	/autodiscover/autodiscover.svc
Dec 21, 2024 @ 13:14:37	GET	/autodiscover/autodiscover.svc
Dec 21, 2024 @ 12:27:36	GET	/autodiscover/autodiscover.svc
Dec 21, 2024 @ 12:27:36	GET	/autodiscover/autodiscover.svc
Dec 20, 2024 @ 02:05:57	GET	/autodiscover/autodiscover.svc
Dec 20, 2024 @ 02:05:57	GET	/autodiscover/autodiscover.svc
Dec 19, 2024 @ 20:36:14	GET	/autodiscover/autodiscover.svc
Dec 19, 2024 @ 20:36:14	GET	/autodiscover/autodiscover.svc
Dec 19, 2024 @ 11:34:23	GET	/autodiscover/autodiscover.svc

“QRadar” ieraksti par augstāk minēto lietotāju īstenotajām bāzes autentifikācijām EID 4624 (“base auth, logon type 8”):

Datums	Statuss	ID	Tips
2024-12-30 11:37:31 AM	Login Success	4624	8
2024-12-30 7:29:2 AM	Login Success	4624	8
2024-12-21 4:30:58 PM	Login Success	4624	8
2024-12-21 1:14:42 PM	Login Success	4624	8
2024-12-21 12:27:50 PM	Login Success	4624	8
2024-12-20 2:6:12 AM	Login Success	4624	8
2024-12-19 8:36:26 PM	Login Success	4624	8
2024-12-19 11:34:25 AM	Login Success	4624	8

Administratora lietotāja e-pasts

Tika analizēti visi e-pastu konti ar fiksētiem pieslēgšanās mēģinājumiem no uzbrucēja izmantotā “user-agent”. Kā jau iepriekš tika pieminēts, izmeklēšanā atrasta sensitīvas informācijas uzglabāšana administratora e-pastā.

Administratora pastkastē tika atrasta visa nepieciešamā informācija, lai veiktu VPN pieslēgumus un piekļūtu uzņēmuma iekštīklam. Lai arī sūtītā informācija atbilst lietotāju atbalsta dienesta darba pienākumiem, identificētas būtiskas drošības nepilnības — e-pasta vēstulēs vienlaicīgi iekļauts PIN un QR kods (attēls zemāk). Šāda informācijas nodošana vienā komunikācijas kanāla vienā sūtījumā ir IS drošības un labās prakses pārkāpums

Rezultātā, pēc iekļūšanas e-pastā, uzbrucējam bija pieejama visa nepieciešamā informācija VPN savienojumu izveidošanai citu lietotāju vārdā.

Administratora pastkastes saturā atradās saites, lietotājvārdi un paroles uz vairākiem svarīgiem servisiem uzņēmuma iekštīklā. Visiem RADIUS serveriem izmantoti ne tikai vieni piekļuves dati (lietotājvārds: admin; parole: admin123), bet arī administrēšanas konts, visticamāk, bijis vairākiem administratoriem koplietošanā. Piesakoties RADIUS serverī, uzbrucējs var pārvaldīt VPN lietotājus uzņēmuma darbiniekiem, sistēmu administratoriem un IT drošības nodaļai.

Pēc uzņēmuma sistēmu administratoru teiktā, lietotājam nav “OWA” (Outlook Web Access) piekļuves tiesības, e-pasta piekļuve notiek tikai pēc sekmīgas VPN autentifikācijas. Izmeklēšana parāda, ka apgalvojums nav patiess un neatbilst faktiskajai situācijai, jo papildu uzbrucēja aģentam “Microsoft+Office/16.0+(Windows+NT+10.0;+Microsoft+Outlook+16.0.15427;+Pro”, uzņēmuma servera IIS žurnālfailos konstatēta arī piekļuve ar netipisko lietotāja aģentu “Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64;+rv:105.0)+Gecko/20100101+Firefox/105.0”. Tas ir tīmekļa pārlūka “Firefox” identifikators. Administratora datorā šāds pārlūks nav instalēts.

Pretēji apgalvojumam, ka administratoram nav piekļuve “OWA”, darbinieka datorā “Edge” tīmekļa pārlūka vēsturē konstatētas šāda veida leģitīmas autorizācijas ar lietotāja aģentu

“Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/131.0.0.0+Safari/537.36+Edg/131.0.0.0”.

Izmeklējot administratora darba datoru, nav konstatēta inficēšanās ar ļaunatūru vai citi dati par neautorizētu piekļuvi ierīcei. Secinājums, ka lietotāja piekļuves dati iegūti kādā vēl pagaidām nenoskaidrotā veidā.

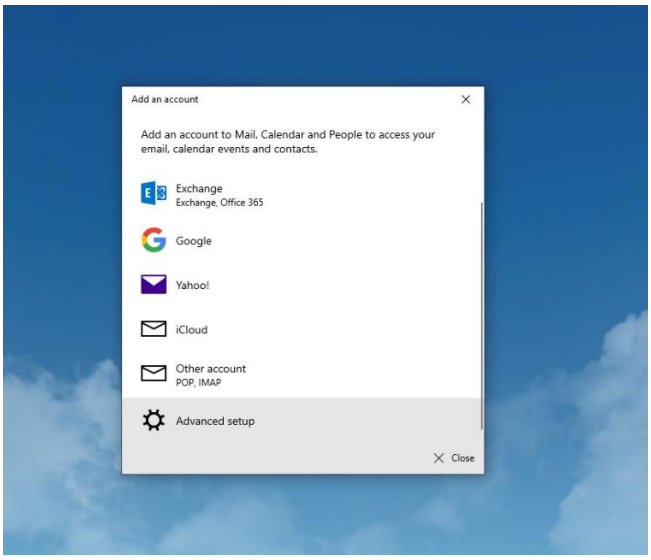
Servera divu faktoru autentifikācijas apiešana

CERT.LV pieprasīja kontu izveidi e-pasta servera testēšanai, lai novērtētu pasta sistēmas autentifikācijas un autorizācijas darbību. Lai nodrošinātu reālās situācijas apstākļus, testu kontiem tika piešķirtas identiskas piekļuves tiesības kā kompromitētajam lietotājam.

Pārbaudē secināts, ka ir iespējams apiet vairāku faktoru autentifikāciju, lai piekļūtu e-pastam.

Situācijas precīzai atkārtošanai, ar testa kontu cert_lv@*.lv veikti šādi soļi:

1. Windows darbstacijā tika atvērta e-pasta programmatūra “Mail”;
2. Izvēlēta paplašinātā uzstādīšanas opcija “Advanced Setup”;



3. Nākamajā solīt izvēlēts Exchange ActiveSync;
    a. Exchange ActiveSync izmanto HTTP bāzes autentifikāciju (“basic auth”);
    b. Tai nav vairāku faktoru autentifikācijas (2FA);
    c. Atkārtoti var pārliecināties ar testu: *.lv/Microsoft-Server-ActiveSync
4. Tālāk nepieciešamo datu ievade;
    a. E-pasts;
    b. Parole;
    c. AD lietotāja vārds;
    d. AD domēns;
    e. E-pasta servera nosaukums;

5. Pēc autentifikācijas tiek parādīts paziņojums, ka iekārtai ir jāatbalsta iestādes domēna politika. To apstiprinot, tiek likts iespējot “Bitlocker” un nomainīt lietotāja paroli, pēc tam e-pasti tiek pilnībā sinhronizēti;

6. Piekļuve e-pastam un saturam nodrošināta, apejot 2FA autentifikāciju;

Šādi tika tehniski pierādīta iespēja piekļūt mārketinga e-pastiem, apejot divu faktoru autentifikāciju. Konstatēts, ka šādu piekļuvi iespējams iegūt, izmantojot tikai aktīvās direktorijas lietotāja paroli.

Uzbrucēja darbības iekšējā tīklā

09.01.2025. laikā no 15:52 līdz 15:57 noticis viens pieslēgums no IP adreses 136.0.185.54 (AS44477 – "Stark Industries Solutions Ltd."). Plkst. 15:52 tika pārtraukta lietotāja aktīvā VPN sesija, kas tika uzsākta no Latvijas IP, tāpēc netika fiksēts uzbrucēja sesijas uzsākšanas notikums (tabula zemāk). Pieņēmums, ka šāda pieslēgšanās pārtver lietotāja aktīvo sesiju.

Plkst. 15:57 fiksēts QRadar notikums: "Session disconnected. Session Type: SSL, Duration: 0h:04m:50s", kas liecina par uzbrucēja sesijas pārtraukšanu. Tas notika, jo lietotāja atkārtoti pieslēdzas pie VPN. Secināts, ka tās dienas pieslēgumos uzbrucējs neveica ļaunprātīgas darbības.

Sākuma laiks	Beigu laiks	Avota IP
09.01.2025 15:52	09.01.2025 15:57	136.0.185.54
14.01.2025 15:01	14.01.2025 15:02	136.0.181.164
14.01.2025 14:49	14.01.2025 14:49	136.0.239.215
14.01.2025 14:51	14.01.2025 14:51	136.0.239.215
14.01.2025 14:54	14.01.2025 14:54	136.0.239.215
14.01.2025 15:10	14.01.2025 16:40	136.0.181.164
15.01.2025 14:39	15.01.2025 16:52	136.0.181.164
17.01.2025 10:44	17.01.2025 11:25	136.0.181.164
17.01.2025 11:25	17.01.2025 16:58	136.0.181.164
26.02.2025 09:43	26.02.2025 10:58	136.0.181.164
26.02.2025 10:58	26.02.2025 12:56	136.0.181.164
26.02.2025 13:39	26.02.2025 18:47	188.214.39.10
27.02.2025 11:23	27.02.2025 20:18	188.214.39.10
28.02.2025 09:42	28.02.2025 14:01	94.131.104.27
28.02.2025 14:02	28.02.2025 14:05	94.131.104.27
03.03.2025 11:32	04.03.2025 00:49	94.131.104.27

14.01.2025. no IP adresēm 136.0.181.164 un 136.0.239.215 (AS44477 – "Stark Industries Solutions Ltd.") notikušas vairākas sekmīgas VPN autentifikācijas, kas veiktas, izmantojot šādus lietotājus:

- datorlietotāja nr.1 sesija laikā no 15:01 līdz 15:02, šo var uzskatīt par savienojuma testēšanu;
- datorlietotājs nr.2 veica trīs īsas VPN sesijas. Secināts, ka šajās sesijās uzbrucēji testē pieslēgšanos VPN;

- datorlietotāja nr.3 sesijas laikā no 15:10 līdz 16:40, kurā notiek tīkla skenēšana.

Ar VPN lietotāju nr.3 veikts vairākums darbību, kur sesiju ietvaros tika izmeklēti un nolasīti divi tīkla segmenti. Abos meklētas iekārtas, kas atbild uz SMB TCP portu 445. Papildus veikta NTLM autentifikācija plkst. 15:21 ar uzņēmuma lietotāju, pirms kuras identificēti vairāki paroļu minēšanas gadījumi ar diviem neeksistējošiem lietotājiem.

2025. gada 15. janvārī notika atkārtota pieslēgšanās ar VPN no IP 136.0.181.164 (AS44477 – "Stark Industries Solutions Ltd."), sākot ar plkst. 14:39:03 līdz 16:52:12. VPN sesijas ietvaros tika veikta SYN tipa skenēšana, meklējot 445 (SMB) un 22 (SSH) portus šādos septiņos apakštīklos.

Sesijas laikā uzbrucējs ieguva 20 Kerberos servisa biļetenus ("service ticket"):

Laiks	ID	Šifrēšana
15:02:37	4769	0x17
15:03:19	4769	0x17
15:03:50	4769	0x17
15:04:31	4769	0x17
15:05:01	4769	0x17
15:05:32	4769	0x17
15:06:46	4769	0x17
15:07:07	4769	0x17
15:07:28	4769	0x17
15:07:49	4769	0x12
15:08:21	4769	0x12
15:08:41	4769	0x12
15:09:02	4769	0x12
15:09:23	4769	0x12
15:09:46	4769	0x12
15:10:02	4769	0x12
15:10:25	4769	0x17
15:11:18	4769	0x17
15:11:49	4769	0x17
15:11:59	4769	0x17

Servisa biļetenu ieguve ir daļa no "kerberoasting" (MITRE ATT&CK: T1558.003), "silver ticket" (T1558.002) un "pass-the-ticket" (T1550.003) uzbrukuma, kura izpildei ir nepieciešams uzlauzt servisa konta paroli. Vairumu

biļetenu ieguva, izmantojot RC4 (0x17) algoritmu. Pēc noklusējuma biļeteni tiek šifrēti ar AES, taču uzbrucēji izmanto RC4, kuru ir vieglāk uzlauzt. Šajā situācijā iesaistītie servisa konti bija divi standarta aktīvās direktorijas lietotāji. Standarta ikdienas lietotāju izmantošana servisu vajadzībām ir slikta prakse vāju un viegli uzlaužamu paroļu dēļ. Jāpiemin, ka uzbrucējs šos divus lietotājus ieguva pašus pirmos. Papildus tika iegūts biļetens lietotājam, kurš, savukārt, ir aktīvās direktorijas iebūvēts administrators.

Uzbrukuma sesijas ietvaros notika SMB servisa izmeklēšana. No skenēšanā iegūtiem rezultātiem vairākām iekārtām izpildīja SMB koplietošanas datņu nolasīšanu (enumerāciju), izmantojot uzņēmuma lietotāju, kura konteksta ietvaros ieguva tīkla koplietošanas datņu informāciju un saturu. Izmantojot Windows notikuma 5140 ID, iegūts saraksts ar nestandarta tīkla datnēm, kurām piekļuva uzbrucējs.

2025. gada 17. janvārī identificētas divas ar uzbrucēja lietotāju izveidotas VPN sesijas, abas uzsāktas no IP adreses 136.0.181.164 (AS44477 – “Stark Industries Solutions Ltd.”). Pirmā sesija uzsākta 10:44:35, kuras laikā veikta apjomīga HTTPS, SMB, RDP servisu un iekārtu meklēšana ar ICMP protokolu. Skenēšana notika iekšējos tīkla segmentos.

Uzbrukuma ietvaros notika piekļuve vairākām koplietošanas mapēm.

Otra sesija tika uzsākta 11:25:58, tajā netika veikta tīkla skenēšana. Uzbrucējs manuāli meklēja informāciju SMB tīkla mapēs, pārsvarā par vienu konkrētu iekārtu. Vairums SMB pieprasījumu mērķēja uz “CA” tīkla mapi (vairāk informācijas skatīt “QRadar” sarakstā), taču notika papildu pieprasījumi uz “GPO_SKRIPTI” un citām mapēm.

2025. gada 26. februārī fiksēta atkārtota pieslēgšanās ar VPN, izveidotas vairākas sesijas no IP 136.0.181.164 (AS44477 – “Stark Industries Solutions Ltd.”). Novērots, ka pirmās VPN sesijas ietvaros (09:43:53 - 10:58:07) veikta 7 apakštīklu skenēšana. Otrās VPN sesijas (10:58:11 - 12:56:23) laikā tīklu segmentu skenēšanas apjoms ir ievērojami plašāks.

Šajā laikposmā fiksēta uzņēmuma AD lietotāju izmantošana no uzbrucēju darbstacijas DESKTOP-****. Pamanīta nesekmīga autentifikācija lietotājam, veikta koplietošanas katalogu nolasīšana (enumerācija). Izgūtas lokālo administratoru LAPS paroles 4100 datoru iekārtām.

Novērotajā VPN sesijā ar izdalīto adresi atkārto tendenci un veic tīkla skenēšanu. Tāpat tiek izmantots uzņēmuma AD lietotāja konts pieslēgumiem no iekārtas, fiksēta koplietošanas katalogu nolasīšana.

2025. gada 27. februārī VPN pieslēguma laikā plkst. 11:23:56 - 20:18:10 no publiskās IP adreses 188.214.39.10 (ar papildus izdalīto iekštīkla adresi), notika vairāki autentificēšanās mēģinājumi (tostarp, arī nesekmīgi) ar gala lietotājiem un Administrator.

Uzbrucējs paralēli turpina veikt tīkla segmentu un koplietošanas katalogu nolasīšanu.

2025. gada 28. februārī no IP adreses 94.131.104.27 (AS44477 – “Stark Industries Solutions Ltd.”) uzsāktas divas VPN sesijas ar gala lietotāju (ar papildu izdalīto iekštīkla adresi, sesijas 09:42:01 - 14:01:34 un 14:02:36 - 14:05:34), kurās veikta vairāku tīklu segmentu nolasīšana.

VPN sesijās fiksētas autorizācijas ar vairākiem lietotājiem, tajā skaitā admin, un bijuši nesekmīgi autentifikācijas mēģinājumi ar vienu gala lietotāja kontu.

2025. gada 3. martā ar gala lietotāja kontu izveidots VPN savienojums (publiskā IP 94.131.104.27, ar izdalītu VPN apakštīkla IP), kurā nolasīti vairāki tīkla segmenti, tajā skaitā arī tie, kas jau iepriekš tikuši aplūkoti.

Tāpat kā iepriekšējos novērojumos, meklētas iekārtas, kas atsauktos uz servisiem ar TCP portiem 5986 (winrm https), 3389 (rdp), 5985 (winrm), 445 (smb). Paralēli uzbrucējs cenšas autentificēties ar vairākiem gala lietotājiem un "Administrator" lietotāja kontiem, visi mēģinājumi nesekmīgi.

Novērotās augstāk minētās aktivitātes liecina, ka ir iespējama autentifikācija, izmantojot NTLM jaucējsummu, piemēram, lietojot programmatūru xfreerdp. Pieslēgšanās no uzbrucēju ierīcēm ar NTLM autentifikācijas tipiem "logon type 3" un "logon type 10" manīta vairākas reizes, un tā ticami norāda uz "Pass the Hash" uzbrukuma metodes izmantošanu. Piemēram, uzbrucējs lieto gala lietotāja NTLM piekļuves datus, lai veidotu RDP sesiju ar kādu iekārtu, kas, savukārt, izveido žurnālfailu notikumus EID (Event ID) 4648 un 4624 "logon type 10".

Turklāt to apstiprina RDP autentifikācijas pēdu nospiedumi:

- "Security eid" 4778 (sesija atjaunota);
- eid 4779 (sesija pabeigta);
- iekārta, no kuras pieslēdzas, un tās iekštīkla IP adrese;
- uz citu iekārtu.

Drošības (Security) žurnālfails:

27.02.2025 11:04	**4779**	**Microsoft-Windows-Security-Auditing**	**Security**	**904**	**RDP disconnecting**	**RDP-Tcp**	**4**	**LogonId: 0x570EA73**
27.02.2025 11:03	4778	Microsoft-Windows-Security-Auditing	Security	904	RDP reconnecting	RDP-Tcp	4	LogonId: 0x570EA73
27.02.2025 11:03	4624	Microsoft-Windows-Security-Auditing	Security	904	Successful logon		10	LogonId: 0x3E2447CE

Ir zināmi vairāki datori, kuros izpildīta sekmīga autentifikācija no uzbrucēja iekārtām. Izpildītie pieslēgumi redzami "Qradar" ierakstos VPN sesiju laika posmos un Windows žurnāla notikumos "Security EventID 4624".

Isaistītas 72 iekārtas, kuras jāuzskata par kompromitētām!

Uzņēmuma infrastruktūra, tajā skaitā izmeklēšanā iesaistītās iepriekš uzskaitītās iekārtas, tika analizētas, tāpat daļa no iekārtām ātri tika integrēta CERT.LV SOC pakalpojumā.

Atsevišķa diska klona analīze tika veikta vairākām darbstacijām.

Izmeklēšanā netika konstatēti dati vai pazīmes, kas norādītu uz pastāvīgas ļaunatūras esamību. Atrastās uzbrucēju darbības un nedrošās administrēšanas prakses ir apkopotas nākamajās sadaļās.

Attālināta kritisko reģistra kopņu izguve

2025. gada 3. martā CERT.LV saņēma informāciju no uzņēmuma par Windows Defender pretvīrusu platformas atrastām ļaunatūras pazīmēm 12 infrastruktūras iekārtās laikā 27.02.2025. - 28.02.2025. Kaitnieciskās darbības antivīrusa sistēmā tika marķētas kā Behavior:Win32/RegDump.SA un ievietotas karantīnā katrā ierīcē.

CERT.LV speciālisti veica notikumu padziļinātu analīzi iekārtās, kurās rīks jau iepriekš uzstādīts Draudu Medību projekta ietvaros. Izpētīts, ka Windows Defender ievietoja karantīnā datnes, kuras sākotnēji atradās kāda datora mapē C:\Windows\Temp\, konkrētāk tā bija datne C:\Windows\Temp\eNpvgsaP.tmp. Antivīrusa trauksmi izsauca nevis datne, bet process "svchost.exe -k localService -p -s RemoteRegistry PID:17568". Datne "eNpvgsaP.tmp" ar MD5 jaucējfunkcijas vērtību "10e749a64320fab88094a2bd65d74208" attiecināma uz Windows reģistra SECURITY kopnes struktūru "eNpvgsaP.tmp: MS Windows registry file, NT/2000 or above".

- Cache;
- Policy: SECURITY\Policy\Secrets satur sistēmas šifrēšanas atslēgas, tajā skaitā SAM kopnes paroles atšifrēšanai nepieciešamās. Turklāt šī kopne satur sistēmas LSA ("Local Security Authority") datus, no kuriem ir iespējams iegūt domēna lietotāju paroļu jaucējfunkciju vērtības;
- RXACT.

Iepriekš identificētais raksturo "Impacket secretsdump.py" darbību. "Impacket" ir "Python" rīku kopa darbam ar tīkla protokoliem, tostarp tīkla pakešu veidošanai un nosūtīšanai. Tā var izpildīt autentifikācijas uzbrukumus, attālināti piekļūt sistēmām, izmantojot SMB protokolu, kā arī izmantot citus papildu rīkus, piemēram, NTLM jaucējvērtību un paroļu izgūšanai paredzēto "secretsdump". Lai apietu paroli un pārņemtu kontroli pār sistēmu un pārvietotos uz citām iekārtām, uzbrucējs centīsies iegūt NTLM jaucējvērtību bez tiešas paroles minēšanas, to sauc par "Pass the Hash" uzbrukumu.

Windows servisa "RemoteRegistry" aktivizēšana var būt viena no "secretsdump.py" darbību sastāvdaļām. Papildus tiek saglabātas Temp mapes failā ar 8 simbolu nosaukumu (piemēram, C:\Windows\Temp\eNpvgsaP.tmp) iegūtās SAM un SYSTEM reģistra kopnes datnes[1].

Izmantojot rīku "impacket-secretsdump", no reģistra kopnes SECURITY var iegūt lietotāju paroļu jaucējsummu vērtības, attiecīgi iesaistīto lietotāju un darbstaciju konti jāuzskata par kompromitētiem, tiem obligāti nepieciešams mainīt paroles!

Papildus tika konstatēts, ka 2025. gada 3. martā rīks "secretsdump" izmantots kādā gala iekārtā, to apliecina Windows Defender antivīrusa reģistrētais "Behavior:Win32/RegDump.SA" notikums par datni "C:\\Windows\\Temp\\mPzmKvkC.tmp". Sākotnēji sarakstā šāda iekārta netika uzrādīta.

Pēc Windows Defender brīdinājumiem papildus drošības stiprināšanai CERT.LV izolētā laboratorijas vidē pārbaudīja, kādu informāciju no darbstacijām uzbrucējs potenciāli var iegūt ar rīka "impacket-secretsdump" lietošanu pret reģistra kopnēm katrā incidentā iesaistītajā uzņēmuma iekārtā.

Rezultāti liecina, ka par kompromitētiem jāuzskata visi lietotāji un konti – domēna, lokālie, iekārtu un servisu konti – tādēļ tiem obligāti jāveic paroļu maiņa.

[1] Avots: https://www.synacktiv.com/en/publications/lsa-secrets-revisiting-secretsdump

Uzņēmuma infrastruktūrā atrasta nedokumentēta gala iekārta, kuras audita ierakstu procesu secību analīzē konstatēts tīkla autentifikācijas pieslēguma tips Nr.3 (“Logon Type 3”) ar lokālā administratora kontu pie visām incidentā iesaistītajām iekārtām. Kā noskaidrots, visās iekārtās iepriekš minētais lietotājs ir lokālā administratora konts, taču katrā iekārtā ar atšķirīgu paroli, ko pārvalda ar LAPS jeb Microsoft Local Admin Password Solution. Tika arī saņemti trauksmes ziņojumi no Microsoft Defender risinājuma.

Detalizēts žurnālfailu apskats par augstāk aprakstīto uzbrukumu

No audita žurnāla “Sysmon_Operational” ierakstiem noskaidrotā procesu secība:

1. PID 824;

```
C:\\WINDOWS\\system32\\services.exe
HKLM\\System\\CurrentControlSet\\Services\\RemoteRegistry\\Start
```

2. Process, kas MS Defender žurnālfailā norādīts kā ļaundabīgs: “PID 17568 C:\WINDOWS\system32\svchost.exe -k localService -p -s RemoteRegistry”;
3. Microsoft Defender trauksme;
4. Attālinātā reģistra vērtība atspējota (Remote registry disabled);
5. Žurnālfails no “Sysmon” audita datiem “wmiprvse.exe PID 13168 -> svchost.exe PID 17568”;
6. Microsoft Defender trauksme (Sysmon - uztpomco.sys md5 79534331d05dfd0f747e1c129f9607e3, daļa no Defender MSERT procesa);
7. Defender žurnālfails;
8. Žurnālfails “System”, reģistra vērtība pārslēdzas iepriekšējā statusā jeb “Remote registry” tiek atslēgts;
9. Audita datu “Sysmon” beigas, turpinājumā žurnālfails “Security”;
10. Ar lokālā administratora lietotāju notiek tīkla autentifikācija;
11. Windows pakalpojumu pārvaldnieks tika izmantots, lai ar lokālā administratora kontu izveidotu attālināto reģistru “Remote Registry service”.

Ņemot vērā iepriekš izklāstīto informāciju, “RemoteRegistry” procesu uzsāka lokālais administrators ar tīkla autentifikācijas tipu Nr.3 (Type3), konkrētāk, pieteikšanās procesu uzsāk lokālais administrators iekārtā A no attālinātās iekārtas B (Remote Host). CERT.LV secināja, ka iekārta B attālināti veica autentifikāciju 13 uzņēmuma iekārtās.

Pēc Sysmon audita datiem, Microsoft Defender reakcija sakrīt ar “RemoteRegistry” procesa aktivizēšanu – “C:\WINDOWS\system32\svchost.exe -k localService -p -s RemoteRegistry”:

Lokālā administratora veiktās operācijas ar pakalpojumu pārvaldnieku sakrīt ar incidenta laiku.

Pārbaudot visas iekārtas, serviss “RemoteRegistry” tika atslēgts. Incidentā iesaistītajās iekārtās automātiski sākotnējos (pēc katras pārstartēšanas) procesos nav konstatētas ļaundabīgas pazīmes.

Lokālā iekārtu administratora konta paroļu ieguve 2025. gada. 26. februārī

CERT.LV padziļinātās analīzes turpinājumā tika meklētas tās lietotāju grupas, kuras var nolasīt LAPS pārvaldīto lokālo administratoru kontu paroles. Atrastās domēna grupas “Lietotāju Administrator” (IT atbalsta daļas lietotāju administratori) piederīgie pēc noklusējuma var nolasīt paroles visiem datoru administratoriem aktīvajā direktorijā.

Šajā Aktīvās direktorijas organizāciju vienībā (OU) atradās visas iekārtas, kurās veikta reģistra izguve ar rīku “Impacket secretsdump” ar LAPS pārvaldnieka lietotāju.

CERT.LV pārbaudīja aktīvās direktorijas grupu politikas un konstatēja, ka ar LAPS tiek pārvaldīti vairāki lokālo administratoru konti.

Izmeklējot "AD Audit" platformas žurnālfailus un analizējot datus, tika konstatēts, ka 2025. gada 26. februārī kāds gala lietotājs pieprasīja visu 72 incidentā iesaistīto iekārtu paroles. Papildus redzams, ka nolasīšana veikta no jau iepriekš pieminētā uzbrucēja iekārtas B. Rezultātā tika iegūtas paroles ne tikai incidentā iepriekš iesaistītajām 13 iekārtām, bet visiem pieejamajiem AD lokālā administratora kontiem attiecīgajā OU. Kopējais iekārtu skaits ir 4100.

Attālināta piekļuve uzņēmuma iekārtām no privātām un ārpus domēna ierīcēm

Pēc uzņēmuma ierīču izpētes, konstatēti RDP pieslēgumi organizācijas datoram kādam organizācijas datoram no privātas, centrāli nepārvaldītas iekārtas. Noskaidrots, ka ierīce ir darbinieka privātā datorā instalēta virtuāla darbstacija, kas paredzēta attālinātiem pieslēgumiem uzņēmuma iekštīklā.

Papildus konstatēts, ka cita darbinieka rīcībā nodotai uzņēmuma ierīcei ir regulāri RDP pieslēgumi no vēl kādas domēnam nepievienotas iekārtas.

Pozitīvais aspekts: attālinātai piekļuvei, izmantojot RDP protokolu, netika izmantota trešo pušu programmatūra bez pietiekamas žurnalēšanas.

Negatīvais aspekts: pēc uzņēmuma tīklā aktīvo ierīču atlases ar "Qradar" filtru "WHERE Machine Identifier LIKE 'DESKTOP-%" tika atrastas vairākas aktīvas iekārtas, kuru identifikatori neatbilst uzņēmuma nosaukumu standartam. Daļa no tām nav pievienotas aktīvai direktorijai un netiek centralizēti pārvaldītas.

Apgrūtinātu incidentu izmeklēšanu un papildu riskus uzņēmuma infrastruktūrai rada konstatētais fakts, ka uzbrucēji neautorizētai piekļuvei (t.sk. ar RDP protokolu) uzņēmuma tīklā izmantoja domēnam nepievienotu ierīci ar nestandarta nosaukumu, kā arī to, ka šīs ierīces netika centralizēti monitorētas, atjaunotas un pārvaldītas. Līdz ar to jāveic ierīču atkārtota inventarizācija, jāizvērtē darbinieku nepieciešamība privāto ierīču lietošanai uzņēmuma iekštīklā.

Ieteikums par attālināto RDP piekļuvi darbstacijām ir pieturēties pie jau esošās procedūras, savienojumus veicot ar īpaši tam paredzētu starpniekiekārtu ("jumphost"). Tiešie RDP pieslēgumi no vienas darbstacijas uz citām darbstacijām jāaizliedz.

Uzņēmuma attālinātās pieejas risinājums

Uzņēmuma infrastruktūrā VPN pakalpojumu nodrošina šādas platformas:

- "Cisco" izstrādātā "Adaptive Security Appliance". Lietotāji ir sadalīti vairākās grupās, pēc kurām tiek noteikts pieejas tiesību līmenis un piešķirtas attiecīgas iekštīkla IP adreses.
- "Citrix Gateway" drošas attālinātās piekļuves risinājums serverī, paredzēts uzņēmuma iekštīklā atdalītu, ierobežotu tiesību lietotājiem, kuriem netiek izsniegts VPN konts.

VPN izveidošanas un piekļuves datu nodošanas procedūra: pēc konta izveidošanas, tehniskā atbalsta nodaļa nosūta lietotājam otrā faktora kvadrātkodu ("QR kodu") vienā saziņas kanālā (parasti tas ir e-pasts). Savukārt, četru ciparu PIN kodu citā saziņas kanālā – SMS uz darbinieka kartiņā norādīto tālruņa numuru.

Uzņēmuma VPN pieslēgšanās strādā tā, ka lietotājiem otrais mainīgais faktors ir jāievada pēc paroles ievadīšanas, respektīvi, parole sastāv no 4 ciparu PIN koda kopā ar 6 cipariem, kurus izsniedz otrais faktors. Tas nozīmē, ka visiem darbiniekiem VPN parole mainās ik pēc 30 sekundēm, kad mainās otrā faktora kods.

Sistēmu ievainojamības

Izmeklēšana atklāja 2023. gadā neveiksmīgu mēģinājumu sistēmā "Citrix NetScaler ADC" un "Gateway" izmantot kritisku ievainojamību "CVE-2023-4966", kas ļauj uzbrucējam iekārtas atmiņā piekļūt šifrētai informācijai TLS savienojumos. Taču padziļināta "Citrix Netscaler" analīze neatrada kompromitēšanas pazīmes.

Iekārtas pēdējo reizi atjauninātas 2023. gada 25. novembrī uz versiju "NetScaler NS13.0: Build 92.19.nc", kas pasargā no "CVE-2023-4966".

Ir iespēja, ka kopš ievainojamības publicēšanas līdz atjauninājuma uzstādīšanai (18.10.2023. - 25.11.2023.) iekārta ir tomēr bijusi kompromitēta, taču tam nav iegūti pierādījumi. Pilnvērtīgu analīzes veikšanu apgrūtina fakts, ka žurnāla faili tiek glabāti ļoti īsu periodu. Piemēram, pieejas žurnāla faili ("access log") tiek glabāti par pēdējām 7 dienām – vecākā ieraksta datums 25.03.2025. plkst.21:09:09 un "messages" – 01.02.2025. plkst. 16:00:00. Savukārt, sistēmā "Qradar" šie auditēšanas ieraksti netiek iesūtīti, piemēram, netiek uzrādīti rezultāti meklējot Qradar pēc vajadzīgajiem atslēgvārdiem. Tā vietā pieejams tikai "Connection Terminate" notikums no IP adreses. GET/POST pieprasījumi tiek reģistrēti sistēmas iekšienē.

RADIUS apraksts

Autentifikācijai tiek izmantoti četri RADIUS serveri. Tie arī veic pieteikšanās datu pārbaudi un pilnu pieslēgumu žurnalēšanu:

1. LietotājuA_RADIUS;
2. Administrator_RADIUS;
3. Citrix_RADIUS;
4. LietotājuB_RADIUS.

VPN kontu administrēšana notiek no minētajiem serveriem. Atbilstošajai grupai piederīgajiem administratoriem ir SSH pieejas uz RADIUS serveriem. Attiecīgi, lietotāja atbalsta nodaļas darbiniekiem ir tīmekļa pieejas pie šiem serveriem, lai rediģētu VPN kontus un atjaunotu lietotāju piekļuves datus.

Jāpiebilst, ka incidenta laika posmā visiem lietotāju atbalsta dienesta darbiniekiem bija vienādi RADIUS serveru administratoru piekļuves dati – lietotājs "admin" ar paroli "admin123". Tas neļauj pilnvērtīgi izmeklēt pieslēgumus pie tīmekļa pārvaldības portāla.

RADIUS serveros ir visa nepieciešamā informācija, tostarp PIN un Secret. Ar abu kombināciju var izveidot QR kodus, lai veiktu attālinātās pieejas savienojumus ar jebkura uzņēmuma darbinieka VPN kontu.

Janvāra žurnālfailos (sk. zemāk) nav redzamas pārlases uzbrukuma ("brute-force") pazīmes pieslēgumos no publiskām IP adresēm. Tas nozīmē, ka uzbrucējs jau ir ieguvis gan lietotāja 4 ciparu PIN un QR kodus vai Secret.

Administratoru pieslēgšanās RADIUS serveriem

No žurnālfaila ierakstiem 26.02.2025. 09:43:48 uzbrucējs izmantoja gala lietotāja VPN pieslēgumu ar piešķirtu iekštīkla IP adresi, no kuras neilgi pēc tam veikta tīmekļa pārlūka autentifikāciju ar kontu "admin" pie administratora RADIUS servera. Pēc divām dienām 2025. gada 28. februārī jau sekoja pieslēgums no publiskās IP adreses, autentificējoties ar galvenā tīkla administratora VPN kontu.

Novēroti arī citi gan sekmīgi, gan nesekmīgi mēģinājumi autentificēties ar pārējo administratoru pieteikšanās datiem.

Secinājums, ka uzbrucējs ar pieeju administratora e-pasta saturam, datus vēstulēs varēja izmantot un arī izmantoja VPN savienojumu veidošanai ar citu lietotāju pieteikšanās datiem. Pēc tam uzbrucējs e-pasta saturā atrada saites uz RADIUS serveriem, administratora serveri, ieguva atbalsta nodaļas lietotājvārdu un paroli. Pēc pieslēgšanās pārvaldības serverim uzbrucējs izguvis visu nepieciešamo informāciju tālākai VPN autentifikācijai ar uzņēmuma administratora pieteikšanās datiem.

Uzbrucēja identificēšana (atribūcija)

Uzbrucēja izmantotās taktikas, tehnikas un procedūras mērķētas pēc MITRE ATTACK[2] .

Uzbrukuma īstenošanai no mitināšanas pakalpojuma sniedzēja "Stark Industries Solutions Ltd." izmantotas trīs IP adreses, AS44477. Tās izmantoja IT infrastruktūras ārējā perimetra izlūkošanai (T1595) un VPN autentificēšanās mēģinājumiem ar vairākiem lietotājiem (T1133).

Jāpiebilst, ka uzbrucējs pārdomāti izvēlējās Latvijas reģiona IP adreses ar nolūku tīkla plūsmai žurnālfailos neizcelties uz pārējo fona ar citām leģitīmām Latvijas IP adresēm. Tāpat pastāvīgās pieejas ("persistence") nostiprināšanai gadījumā, kad cietusī iestāde atklāj incidentu un veic novēršanas darbības, tādas kā, piemēram, atļauj VPN pieslēgumu tikai no Latvijas reģiona IP adresēm. Tas norāda, ka uzbrucējs priekšlaicīgi ir veicis sagatavošanās darbus uzbrukumam.

"Stark Industries Solutions Ltd." (AS44477) vairākkārt nonācis CERT.LV redzeslokā un tiek uzskatīts par noziedzīgu darbību piesedzošu ("bulletproof") mitināšanas pakalpojuma sniedzēju, kurš nodrošina Krievijas atbalstītas kiberoperācijas pret Latviju, NATO un citām valstīm, kas sniedz atbalstu Ukrainai.

CERT.LV ir informācija par vairāku uzņēmuma lietotāju datu noplūdēm, kuru cēlonis ir informācijas zadzēju ļaunatūras. Tās mēdz izmantot sākotnējās piekļuves iegūšanai, datus bieži pārdod citam uzbrucējam ar atšķirīgiem mērķiem un ekspertīzes līmeni. Vairākām izcelsme cieši saistīta ar Krieviju.

CERT.LV nav informācijas, ka zināmās datu noplūdes būtu sasaistāmas ar incidenta notikumiem un to cēloņiem, taču aktivitāte norāda uz Krievijas interesi par uzņēmumu jau ilgākā laika periodā. Zemāk tabulā apkopoti informācijas zadzēji no kompromitētiem uzņēmuma lietotājiem.

Kad uzbrucējs sekmīgi bija veicis VPN autentifikāciju, tika identificētas vairākas darbības ar nolūku nostiprināt savu klātbūtni un izplatīties tālāk infrastruktūrā. Skripts "Secretsdump.py" ir daļa no "Impacket" rīku kolekcijas, lai izgūtu LSA Secrets, SAM datubāzi, NTDS.dit, un citus autentifikācijas datus (T1003). Šādas darbības identificētas vairāku valstu kritiskajās infrastruktūrās, un tās tiek sasaistītas ar Krievijas Militārās izlūkošanas dienesta (GRU) vienību "29155".

Turklāt "secretsdump.py" izmantošana ir novērota kopā ar "Raspberry Robin" ļaunatūru. CERT.LV identificējis inficēšanos ar ļaunatūru "Raspberry Robin" vairākās iestādēs. Augsta varbūtība, ka uzbrukumi saistīti ar Krievijas valsts atbalstītiem grupējumiem.

[2] https://attack.mitre.org

Tika novērota arī manipulēšana ar operētājsistēmas reģistra datiem, iegūti vairāku lietotāju dati no reģistra kopnēm (T1003.002). Arī šādas darbības ir agrāk pamanītas un saistītas Krievijas valsts APT grupējumu APT29 jeb Midnight Blizzard pēc Microsoft klasifikācijas.

Novērotas darbības ar mērķi apgrūtināt incidenta izmeklēšanas procesu. Liela apjoma iekšējā tīkla skenēšana veikta, visticamāk, lai pārpildītu žurnālfailiem pieejamo vietu un lai žurnālfailu rotācijas dēļ pierādījumi vairs nebūtu pieejami.

CERT.LV ar augstu varbūtību šo uzbrukumu saista ar kādu Krievijas valsts dienestu (iespējams, GRU un/vai SVR) atbalstītu grupējumu, balstoties uz faktiem:

- uzbrucēja lietotā infrastruktūra ir vairākkārt saistīta ar Krievijas valsts atbalstītām operācijām;
- izmantotās tehnikas un procedūras sakrīt ar iepriekš atklātiem Krievijas dienestu atbalstītiem incidentiem;
- cietušā kompromitēšana sakrīt ar Krievijas ģeopolitiskajiem plāniem.

Kompromitēšanas indikatori (IOC)

IP adreses:

- 94.131.104.27 (Autonomās sistēmas numurs - AS 44477; Piederība – "Stark Industries Solutions Ltd."; reģions - Latvija);
- 136.0.185.54 (Autonomās sistēmas numurs - AS 44477; Piederība – "Stark Industries Solutions Ltd."; reģions - Latvija);
- 136.0.181.164 (Autonomās sistēmas numurs - AS 44477; Piederība – "Stark Industries Solutions Ltd."; reģions - Latvija).

Ieteikumi

Vienīgā un drošākā atkopšanās pēc notikušā incidenta ir MS Windows infrastruktūras izveide pilnībā no jauna.

Incidenta ietekmes mazināšanai pēc iespējas ātrāk jāveic šādas darbības:

- Nomainīt domēna kontrolierī "KRBTGT" konta paroli divas reizes. Šī darbība var izraisīt kādu atsevišķu pakalpojumu nepieejamību, tādēļ jāgatavojas restartēt servisu vai pat serverus, lai visi Kerberos iepriekš izsniegtie biļeteni (TGT) būtu deaktivizēti. Attiecīgās skartās iekārtas/servisi/lietotāji autentificēsies atkārtoti, t.i., pieprasīs jaunu Kerberos biļetenu no KDC. Paredzams, ka var tikt ietekmēti tādi servisi kā "Sharepoint", "Skype for Business" un cita AD SSO autentifikāciju izmantojoša programmatūra. Starp abām "KRBTGT" konta paroles maiņas reizēm jānogaida vismaz 10 stundas. **Svarīgi** – "KRBTGT" konta parole jānomaina divas reizes visos domēnos, kas atrodas attiecīgajā domēna mežā ("Domain Forest"). Ja tas netiek izdarīts, uzbrucējiem ir atstāts iespējamais atpakaļceļš. Labā prakse ir mainīt "KRBTGT" konta paroli vismaz reizi 180 dienās, pat ja nav informācijas par notikušu incidentu. Microsoft instrukcija "KRBTGT" konta paroles maiņai pieejama šeit:https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-resetting-the-krbtgt-password;
- Nepieciešams mainīt visu servisa lietotāju (kam iestatīts SPN) paroles;
- Visus šajā atskaitē pieminētos kontus (lietotāju, servisu, darbstaciju, serveru) nepieciešams atspējot ("disable") un noņemt piederību visās pieejas tiesību grupās. Pēc tam jānomaina attiecīgo kontu paroles visās ietekmētajās sistēmās, un tikai kad tas paveikts, var kontus iespējot ("enable"). Papildu drošībai

aicinām šos kontus izveidot no jauna ar citu nosaukumu, jo uzbrucējam, visticamāk, ir izveidota zināšanu bāze par uzņēmuma infrastruktūras uzbūvi;

- Pārinstalēt 72 uzbrukumā skartās darbstacijas;
- Serverus pārbaudīt ar atjauninātu antivīrusa programmatūru;
- Pārliecināties, ka pretvīrusu risinājums pārbauda arī iekārtai pievienotos ārējos datu nesējus;
- Ja ir pieejama aktīvās direktorijas rezerves kopija, ieteikums atjaunot uz tādu versiju, par kuru ir pārliecība par kompromitēšanas pazīmju neesamību. CERT.LV veiktā izmeklēšana parāda, ka uzbrucēja darbības sākušās vismaz ar 2024. gada 18. novembri. Pēc kopijas atkopšanas noteikti nomainīt visas lietotāju/servisu/iekārtu kontu paroles, "KRBTGT" kontam paroli maina divreiz ar vismaz 10h intervālu. Plānojot atkopšanu, jāņem vērā dzēsto ierakstu jeb "tombstone" periods. Vairāk informācijas skatīt Microsoft dokumentācijā par aktīvās direktorijas atkopšanu;
- Pārliecināties, ka papildu žurnalēšanas rīks "Sysmon" ir uzstādīts un konfigurēts visās infrastruktūras iekārtās. Izmeklēšanā tika konstatēts, ka incidenta dienā vairākās iekārtās Sysmon nestrādāja, un vairākās iekārtās tas nebija uzstādīts;
- Ierobežot piekļuvi "Exchange Autodiscover" galapunktiem pēc IP adresēm (VPN, valsts, utt.);
- Ugunsmūra, starpniekservera ("proxy") vai DNS līmenī bloķēt tīkla plūsmu uz apšaubāmiem "autodiscover" domēniem, piemēram, "autodiscover.ru", "autodiscover.cn", "autodiscover.xyz" u.c.;
- Nodrošināt, ka e-pasta klienti neizmanto neatbilstošus vai novecojušus "Autodiscover" mehānismus;
- Atspējot "Basic Authentication" e-pasta serveros (vairāk informācijas skatīt šeit: https://learn.microsoft.com/en-us/powershell/module/exchange/set-authenticationpolicy);
- VPN lietotāju pieslēgumu ierobežot līdz vienai vienlaicīgai sesijai;
- Nomainīt divu faktoru autentificēšanos principu, kur katram lietotājam izsniegts lietotājs/parole, otrais faktors pieprasīts pēc "lietotājvārds:parole" kombinācijas ievadīšanas;
- Uzskaitīt visas leģitīmās uzņēmuma darbinieku IP adreses, izveidot atļauto sarakstu ar IP adresēm, kuras drīkst slēgties pie VPN (piemēram, apvienojot reģionu un interneta pakalpojuma sniedzēju);
- Nekavējoties bloķēt pieslēgumus no Stark Industries Solutions Ltd.", AS44477 piederošajiem tīkla adrešu apgabaliem (saraksts šeit: https://ipinfo.io/AS44477);
- Dzēst RADIUS servera pārvaldības konta nosaukumu "admin" un izveidot atsevišķu pieeju katram administratoram darba pienākumu pildīšanai;
- Lokālo administratora paroļu pārvaldības risinājuma "LAPS" kontiem mainīt paroli, ir nepārprotami pierādījumi, ka dati nonākuši uzbrucēja rīcībā (Incidenta izmeklēšanas aktīvajā fāzē CERT.LV informēja uzņēmuma atbildīgās personas par šo faktu);
- Maksimāli samazināt NTLM izmantošanu vai pilnībā pāriet uz modernāku Kerberos autentifikācijas protokolu.
- Atspējot NTLM v1 autentifikāciju;
- Pārliecināties, ka Kerberos autentifikācijā netiek izmantots novecojis "RC4-HMAC" šifrēšanas algoritms;
- Ievērot labo praksi servisa lietotāju izveidē (noņemt domēna standarta lietotājiem servisa lietotājus. Iestatot domēna lietotājus par servisa lietotājiem, palielinās "Kerberoasting" uzbrukuma risks);
- Ierobežot "ANONYMOUS LOGON" izmantošanu ar šādām grupu politikām:
    - "Network access: Let Everyone permissions apply to anonymous users" - ("disable") labā prakse aprakstīta šeit: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/network-access-let-everyone-permissions-apply-to-anonymous-users

- “Network access: Restrict anonymous access to Named Pipes and Shares” - (“enable”) labā prakse aprakstīta šeit: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/network-access-restrict-anonymous-access-to-named-pipes-and-shares
- “Network access: Named Pipes that can be accessed anonymously” labā prakse aprakstīta instrukcijā šeit: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/network-access-named-pipes-that-can-be-accessed-anonymously
- “Network access: Shares that can be accessed anonymously” labā prakse aprakstīta instrukcijā šeit: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/network-access-shares-that-can-be-accessed-anonymously
- Atkārtot iekārtu inventarizāciju;
- Apsvērt apturēt darbinieku privāto ierīču izmantošanu darbam uzņēmuma iekštīklā;
- Attālināto RDP piekļuvi darbstacijām veikt pēc procedūras no īpaši paredzētās savienojumu starpnieka iekārtas (“jumphost”), aizliegt tiešas RDP pieejas starp darbstacijām.

Kāda cita uzņēmuma tīmekļa vietnes incidents

Situācijas apraksts: 2025. gada 3. aprīlī tika saņemta informācija, ka kāda uzņēmuma vietne ir kompromitēta. Vietne tiek uzturēta uz koplietošanas servera.

Būtiski izmeklēšanas procesa notikumu datumi:

- **05.03.2025.** no tīmekļa vietnes mitināšanas pakalpojuma sniedzēja ika saņemti šādi dati: žurnālfaili, inficētās vietnes arhīvs, inficētās vietnes rezerves kopija;
- **07.03.2025.** no tīmekļa vietnes mitināšanas pakalpojuma sniedzēja saņemtas vēsturiskas rezerves kopijas, sākot ar 18.02.2025.;
- **12.03.2025.** uzsākta uzņēmuma mājas lapas analīze uzturētāja serverī (“Ubuntu” 18.04.06 LTS). Šajā serverī tiek uzturētas vairākas citas mājaslapas. Pēc servera analīzes netika iegūti pierādījumi par servera kompromitēšanu;
- Politiskais konteksts: vietnes saturs saistīts ar Latvijas valsts aizsardzības nozari.

Izpētes laikā CERT.LV konstatēja vairākas ļaunprātīgas tīmekļa čaulas (webshells), kas ļauj uzbrucējam apiet autentifikācijas metodes un iegūt kontroli pār tīmekļvietni vai serveri. Dažos gadījumos tīmekļa čaulas “Gecko” funkcionalitāte nodrošina ne tikai sistēmas datņu pārlūkošanu, bet arī WordPress pārvaldību – lietotāju pievienošanu, pārvaldības “cPanel” atiestatīšanu un citas darbības. Žurnālfailu analīzē konstatēti tīmekļa čaulu pieprasījumi no 2024. gada maija. Pēc CERT.LV apkopotās informācijas un tālāk veiktās izpētes secināts, ka uzbrucējiem bija iespēja veikt tīmekļa vietņu failu sistēmas modifikāciju un failu ievietošanu vismaz sākot ar 2025. gada. 18. februāri. CERT.LV ir pieejama informācija par CMS programmatūras versiju – “Drupal 6.26” – drošības atjauninājumu atbalsts tai beidzās 2014. gada februārī. “Drupal 6.26” ir vairākas ievainojamības, piemērām, SQL injekcija (SA-CORE-2014-005), kuras īstenošanas gadījumā uzbrucējs var pilnībā pārņemt kontroli pār tīmekļvietni. Ņemot vērā, ka ražotāja atbalsts šai versija pārtraukts 2014. gada februārī, pastāv augsta varbūtība, ka tīmekļvietne bijusi kompromitēta laikā posmā no 2014. gada līdz

2024. gada maijam, kas ir pieejamo žurnālfailu sākuma datums. Tīmekļa čaulas metadati ir modificēti, tāpēc nav iespējams noteikt konkrētu laiku, kad tie ir nonākuši uz sistēmas.

Tomēr, izpētot saistīto moduļu un bibliotēkas, kuru mapēs atradās tīmekļa čaulas, versijas, un, ņemot vērā, ka paša CMS programmatūras Drupal versija bija novecojusi, ļoti iespējams, ka ir tikušas izmantotas virkne ievainojamību, lai augšupielādētu tīmekļa čaulas un veiktu attālinātas darbības. Daudzās tīmekļa čaulas un Drupal versijas vecums ir pamats aizdomām par vairākiem dažādiem uzbrucējiem. Žurnālfailu laika ierobežojuma dēļ nav pieejami digitālie pēdu nospiedumi (artefakti), un līdz ar to nevar ne pilnībā izsekot uzbrucēju darbības sistēmā, ne arī precīzi noteikt uzbrukumu datumu.

Tā kā lielākajai daļai tīmekļa čaulu bija vairāki savstarpēji vienojoši atribūti (“gecko.php, style.php, kebogi.php, najyka.pjp, style.php”), ir pamats domāt, ka attiecīgās tīmekļa čaulas ir saistītas ar vienu uzbrucēju grupējumu. Turklāt vienīgā IP adrese, konkrēti, 185.175.44.233, kas parādījusies vairākās šajās tīmekļa čaulās, ir tālāk saistīta ar krieviski komunicējošo “magbo.cc”, kas ir nelikumīgi iegūtu piekļuvju pārdošanas pakalpojums. Ņemot vērā iepriekš minētos faktus un papildu apstākli, ka uzlauztās vietnes satura dēļ kompromitēšana varētu būt notikusi Krievijas ģeopolitiskajās interesēs, tad ar lielu iespējamību šo uzbrukumu var saistīt ar kādu Krievijas intereses pārstāvošu uzbrucēju.

Divas citas tīmekļa čaulas (“bypafgss.php, css.php”) tika identificētas ar vairākiem atribūtiem, kas norāda par iespējamu Ķīnas saistību, piemēram, hieroglifi, ķīniešu servisu kodējums, “Github” konts ķīniešu valodā. Kaut arī šie fakti un uzlauztās vietnes saturs saskan ar Ķīnas ģeopolitiskajām interesēm, tomēr zema iespējamība, ka uzbrukumu veicis Ķīnas atbalstīts uzbrucējs. Vairākos vēsturiskos incidentos novērots, ka Krievijas valsts atbalstīti uzbrucēji izmanto Ķīnas izstrādātas tīmekļa čaulas, lai maldinātu uzbrucēja profilēšanas procesu. CERT.LV nesaista indikatorus ar kādu konkrētu uzbrucēju grupējumu.

No 2025. gada 20. marta uzlauztā vietne tiek mitināta pie cita uzturētāja. Tā kā pie atrastajām tīmekļa čaulām piekļuve ir nesekmīga, var pieņemt, ka tās ir likvidētas.

Tehniskā informācija par tīmekļa vietni un citi dati

Informācija par uzlauzto vietni:

```
name = System
description = Handles general site configuration for administrators.
package = Core - required
version = VERSION
core = 6.x
; Information added by drupal.org packaging script on 2012-05-02
version = “6.26”
project = “drupal”
datestamp = “1335977158”
```

Incidenta izmeklēšana un rezultāti

Norises laiks no 2014. gada (iespējamais sākuma datums) līdz 2024. gada 12. maijam, detalizēta notikumu laika līnija no pieejamajiem datiem.

- 12-05-2024 04:44 Pirmais pieprasījums pēc vienas tīmekļa čaulas “gecko.php”:
- 13-05-2024 02:39 Pirmais pieprasījums pēc nākamās tīmekļa čaulas “kebogi.php”:
- 13-05-2024 - 28-02-2025 Regulāri pieprasījumi pēc “gecko.php” un “kebogi.php”:
- 30-09-2024 injekciju mēģinājumi:
- 18-10-2024 injekciju mēģinājumi “Baiduspider/2.0”:
- 23-02-2025 08:04 pirmais GET pieprasījums pēc “bypafgss.php” tīmekļa čaulas, kam plkst. 08:28 seko pirmais POST pieprasījums:
- 28-02-2025 05:49 pirmais ārpus “Sigmanet” starpniekservera pieprasījums tīmekļa čaulai no Krievijas reģiona IP adreses (185.175.44.233):
- 03-03-2025 14:27 atkārtots pieprasījums:
- 05-03-2025 vairāki atkārtoti pieprasījumi:
- Fakti par pieslēgumu no Krievijas reģiona IP adreses 185.175.44.233:

IP: 185.175.44.233;

ASN: AS50340;

Valsts: RU;

Domēns: magbo.cc.

- 28-02-2025 meklējot pēc “User-Agent”, atrasti pieprasījumi uz “kebogi.php” datumos 28-02-2025 un 03-03-2025, kas identiski sakrīt ar citu *.lv pieprasījumu https://*.lv/lv/__p19b:
- 03-03-2025 atkārtoti pieprasījumi.

Tīmekļa čaulas “Gecko” analīze

Trijās uzlauztās vietnes datnēs atrasta tīmekļa čaula “Gecko”:

- oldphp538/home/*/public_html/profiles/liaa/modules/email_registration/translations/gecko.php;
- oldphp538/home/*/public_html/files/*/content/gecko.php;
- oldphp538/home/public_html/files/*/imagecache/News_block_image/gecko.php

Izmeklēšana veikta vairākās rezerves kopijās, pirmo reizi tīmekļa čaula parādās 2025. gada 24. februārī.

Koda analīze parāda, ka sekmīgas autentificēšanās gadījumā uzbrucējs izpilda datni no vietnes:
http://www.qkl2048[.]com/tools/gekcko.txt
virustotal.com apraksts:
https://www.virustotal.com/gui/file/9a657974a87e40cb21f30cd3d4c350f07620617f310cfcab5471c88c5914cd66/details

Atmaskots skripts:
https://www.unphp.net/decode/*

Publiski pieejamā informācija norāda, ka tika izmantots “MadExploits” radīts aizmugures piekļuves (“backdoor”) rīks. Vairāk informācijas skatīt šeit: https://github.com/MadExploits/Gecko/.

Rīka funkcionalitāte ir plaša, tā spēj nodrošināt sistēmas ne tikai datņu pārlūkošanu, bet arī pievienot platformas “WordPress” lietotāju, atiestatīt pārvaldības paneli “cPanel” u.c. darbības.

Pilns skripts pieejams šeit: https://github.com/MadExploits/Gecko/blob/main/gecko-new.php

Izpētot detalizētāk domēnu "qkl2048.com/tools/gekcko.txt", ļaunatūras ķēdē konstatēta iespējama inficēta Google Chrome paplašinājuma lejupielāde.

Iesaistīti vairāki lietotāja aģenti ar publisku IP adresi 185.175.44.233, reižu skaits: 4.

Tīmekļa čaulas "style.php" analīze

Arī šajā gadījumā, līdzīgi kā "gecko.php", tiek pieprasīta tā pati datne.

alfa-shell: https://github.com/nicxlau/alfa-shell/blob/master/alfa-deobfuscated.php

Šīs tīmekļa čaulas funkcionalitātes apraksts:

- servera failu pārlūkošana, augšupielāde, lejupielāde, rediģēšana un dzēšana;
- servera konsoles komandas izpilde, dodot pilnu piekļuvi sistēmai;
- datubāžu piekļuve, dažādas darbības ar saturu, tostarp datu dublēšana, izgūšana;
- servera failu nolasīšana, piemēram, PHP iestatījumi, kuri var atklāt neizpaužamu konfigurāciju;
- arhīvu failu izveidošana, atpakošana un pārvaldīšana ZIP vai TAR formātā.

Iesaistītie lietotāju aģenti (*user-agents*): Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36;

Reižu skaits: 256.

Tīmekļa čaulas "Bypafgss.php" analīze

Atšķirībā no iepriekšējām čaulām, šai sākums ir "<?php /* PHP Encode by https://Www.PHPJiaMi.Com/" kas satur domēnu "PHPJiaMi.com", kas ir Ķīnas uzturēts PHP nokodēšanas un atkodēšanas tiešsaistes rīks. Tā kā tīmekļa čaulas saturs ir būtiski maskēts, nav iespējams noskaidrot tās funkcionalitāti.

Iesaistīti vairāki lietotāju aģenti ("user-agents") ar daudz dažādām IP adresēm.

Tīmekļa čaulas WSO "tbakrn.php" analīze

Publiski zināmajai tīmekļa čaulai "WSO" (web shell by oRb, https://github.com/mIcHyAmRaNe/wso-webshell) pieejamas vairākas versijas un variācijas, bet uzlauztajā vietnē injicēta versija 4.2.5. Šīs tīmekļa čaulas versijas funkcionalitāte izpilda:

- servera failu augšupielāde, rediģēšana, dzēšana un pārvietošana;
- attālināta komandu izpilde, nodrošinot pilnu piekļuvi sistēmai;
- piekļuve un izmaiņu veikšana SQL datubāzēs;
- paroles aizsardzība un šifrēšana neautorizētas piekļuves ierobežošanai.

Dati par iesaistītiem lietotāju aģentiem žurnālfailos nebija pieejami.

Dati par iesaistītām IP adresēm žurnālfailos nebija pieejami.

Tīmekļa čaulas "Kebogi.php" analīze

Maskēto skripta datņu saturs un izpildāmās komandas atšķiras, taču maskēšanas paņēmiens visām ir viens. Jāpiebilst, ka datņu izveidošanas sistēmas laiks ir dažāds.

Nav iespējams noteikt, kādas tieši komandas tiek izpildītas, jo tās norādītas sīkdatņu (“cookie”) parametrā.

Iesaistīti vairāki lietotāju aģenti no IP adreses 185.175.44.233, 10 reizes.

Tīmekļa čaulas “Najyka.php” analīze

Šīs datnes jaucējvērtība “c42ea979ed982c02632430e9e98a66d6” pirmo reizi parādās 2021. gada rakstā par platformas “Wordpress” spraudņiem “Vulnerable Kaswara Modern WPBakery”: https://jetpack.com/resources/vulnerable-kaswara-modern-wpbakery-plugin/.

Analizētajā incidentā atmaskotais PHP skripts norāda, ka tālāk izpildīšanai tiek sagaidīta “base64” kodēta datne, kuras MD5 jaucējsumma ir “c42ea979ed982c02632430e9e98a66d6”, taču tāda nav atrodama ne publiski pieejamā informācijā, ne žurnālfailos. Datnē izmantots gandrīz identisks “Vulnerable Kaswara Modern WPBakery” kods.

Dati par iesaistītiem lietotāju aģentiem žurnālfailos nebija pieejami.

Dati par iesaistītām IP adresēm žurnālfailos nebija pieejami.

Saistītie papildu konstatējumi

Meklētāja robots “Baiduspider”, pieprasījumi veikti: 18.10.2025. plkst. 00:25:39 un 09.11.2025. plkst. 05:55:37:

Izpildot komandu “grep -E “POST .*9217””, netiek uzrādīti nekādi rezultāti, tāpēc var pieņemt, ka šis elements nav izmantots. Vai arī nav tādu žurnālfailu, kas pierādītu tā izmantošanu.

Iesaistīts viens lietotāju aģents (“User-Agent”), 4 reizes.

Tīmekļa čaulas “css.php” analīze

Informācija par tīmekļa čaulu atklāja tās funkcionalitāti un papildu datus, kā arī vairākus iesaistītos lietotāju aģentus (“user-agents”).

Izmeklēšanas versija par sākotnējo piekļuvi

Iepriekš tika norādīts, ka par vietnes bāzi izmantota platformas “Drupal” versija 6.26, kura kopš 2016. gada 24. februāra netiek atbalstīta un nesaņem drošības atjauninājumus. Vairākiem moduļiem un bibliotēkām izmantotas vecākas versijas. Konkrētai Drupal versijai ir vairākas ievainojamības ar riska un bīstamības pakāpēm, daudzu īstenošana var rezultēties ar pilnīgu uzbrucēju kontroli pār serveri.

Piemēri:

1. Drupal kodola SQL injekcija “SA-CORE-2014-005” - kritiskā ievainojamība ļauj neautentificētiem uzbrucējiem veikt SQL injekcijas Drupal datubāzē, manipulējot ar pieprasījumiem, kas saistīti ar vietnes URL parametriem. Tā ļauj izpildīt patvaļīgus SQL vaicājumus, kas var novest pie sensitīvu datu noplūdes, lietotāju kontu pārņemšanas vai pat pilnīgas vietnes kontroles iegūšanas.
   Risks: izpildīta ievainojamība uzbrucējam ļauj izmainīt administratora paroles, izveidot jaunus augsti priviliģētus kontus vai izpildīt ļaunprātīgu PHP kodu serverī, radot nopietnus drošības draudus un sistēmas kompromitēšanu.
2. Failu augšupielādes ievainojamība CVE-2011-3402 ir “Drupal” failu augšupielādes funkcija, kas bez pārbaudes ļauj uzbrucējiem augšupielādēt kaitnieciskus failus. Nepareizas konfigurācijas gadījumā

uzbrucēji var augšupielādēt PHP failus, piemēram, tīmekļa čaulas, lai izpildītu koda izpildes uzbrukumus serverī.

Risks: Uzbrucējs var augšupielādēt failus ar PHP koda saturu, kuru izpilde serverī sniedz pilnu piekļuvi;

3. Starpvietņu skriptēšanas (Cross-site Scripting, XSS) ievainojamība CVE-2012-2183 ļauj uzbrucējiem ievadīt ļaunprātīgu "JavaScript" kodu vietnes ievades laukos, ko var izmantot ne tikai lietotāju maldināšanai, bet arī ļaunprātīgiem mērķiem, piemēram, administratīvām piekļuvēm vai failu augšupielādes manipulācijām.

   Risks: izmantojot ievainojamību kopā ar citiem trūkumiem, tā uzbrucējam palīdz iegūt piekļuvi vai manipulēt ar administratīvo paneli, lai augšupielādētu ļaunprātīgus failus.
4. SQL injekcijas ievainojamība CVE-2011-2981 ļauj uzbrucējiem manipulēt ar SQL vaicājumiem, iegūstot piekļuvi datubāzēm vai serverim. Ievainojamību var izmantot, lai iegūtu piekļuvi administratoru lietotāju sesijām un failu augšupielādes pārvaldīšanai.

   Risks: SQL injekcija uzbrucējiem ļauj piekļūt vietnes datiem, manipulēt ar lietotāju sesijām un izpildīt ļaunprātīgu kodu.
5. Privilēģiju paaugstināšanas ievainojamība CVE-2011-3026 ļauj uzbrucējiem palielināt piekļuves tiesības - no ierobežota lietotāja uz sistēmu administratoru. Tas sniedz uzbrucējam iespējas veikt sistēmas pārvaldnieka darbības, piemēram, konfigurēt sistēmu.

   Risks: no ierobežotu tiesību lietotāja uzbrucējs kļūst par administratoru, tad augšupielādē ļaunprātīgus failus, kas ļauj pārvaldīt servera konfigurāciju un iegūt pilnīgu kontroli pār sistēmu.
6. Starpvietņu pieprasījumu viltošanas (CSRF) ievainojamība CVE-2012-3360 ļauj uzbrucējiem veikt darbības vietnē no lietotāja sesijas un nemanīti sūtīt ļaunprātīgus pieprasījumus, kas var novest pie ļaunprātīgu failu augšupielādes vai servera konfigurācijas maiņas.

   Risks: CSRF ievainojamība atļauj vietnē veikt darbības, kas, izmantotas kopā ar citām ievainojamībām, uzbrucējam dod piekļuvi serverim un ļauj augšupielādēt kaitnieciskus failus.
7. Nepietiekamas piekļuves kontroles ievainojamība CVE-2011-3824 ļauj lietotājiem ar ierobežotām piekļuves tiesībām veikt tādas darbības, kas parasti bija pieejamas tikai virsadministratoriem, piemēram, piekļūt administratīvajiem iestatījumiem un augšupielādēt ļaunprātīgus failus.

   Risks: nepareiza piekļuves kontrole ļāva uzbrucējiem veikt darbības, kas standarta lietotājam nav pieejamas.

Tīmekļa čaulās atrastas vairākas bibliotēkas un moduļi: e-pasta reģistrācija ("email_registration"), detalizēta sistēmas informācija ("system"), satura veidošana un augšupielāde ("upload").

Incidenta saistīšana ar konkrētu grupējumu jeb "atribūcija"

Kaut arī identificētajās tīmekļa čaulās ir dažādība, atrasti pierādījumi par savstarpējo saistību. Pirmkārt, "gecko.php" un "style.php" tīmekļa čaulas datnes veic pieprasījumus uz vienu un to pašu domēnu "qkl2048.com", lai saņemtu nākamā uzbrukuma etapa tīmekļa čaulas.

Otrkārt, vienīgā IP adrese ar pieprasījumiem uz datni "gecko.php" bija 185.175.44.233 (AS50340 - RU), no tās pašas IP adreses arī uz "kebogi.php" datni (kurai ir vairākas līdzības ar "najyka.pjp"). Tāpēc ticams, ka šīs četras datnes saistītas ar vienu uzbrucēju.

Kopsavilkums par visām identificētajām tīmekļa čaulām:

Čaulas nosauk.	Datne	SHA256	Saite	Līdzīgas tīmekļa čaulas	Komentārs
Gecko	oldphp538/home/*/public_html/files/*/imagecache/News_block_image/gecko.php,	8e7334db6056355563a58980bb153eb7f72d830fcbd208f189b1613c0f0712a3	https://github.com/MadExploits/Gecko/	https://github.com/ItsMeAlf404/B	Sekmīga uzbrukuma gadījumā, tiku lejupielāda

	oldphp538/home/*/public_html/files/*/content/gecko.php, oldphp538/home/*/public_html/profiles/liaa/modules/email_registration/translations/gecko.php		blob/main/gecko-new.php	ackdoor/blob/main/awokpass.php	tīmekļčaula, kas atrodas Saite sadaļā, no qkl2048[.]com/tools/gekcko.txt
WSO	/*/public_html/modules/system/tbakrn.php	b462036676f01913cb9ed6380599f85b78bfea0d739429c4da359afe526503fd	https://github.com/Josexv1/wso-webshell	https://github.com/mIcHyAmRaNe/wso-webshell, https://github.com/ndbrain/WSO	Daļa no koda sakrīt identiski ar Josexv1/wso-webshell Github saturu. https://github.com/phpFileManager/WSO githubā saturs ir Krievu valodā
Bypafgss	/*/public_html/sites/all/modules/cck/includes/bypafgss.php	33d83b7c170efe509a502c5c1f3d18cbed951529cb9b9670cdb3193e67f650c9	N/A	N/A	Satur kodu <?php /* PHP Encode by https://Www.PHPJiaMi.Com/ */error_reporting(0);ini_set("display_errors", 0);, kas ir manīts vairākās YARA signatūrās internetā.
Kebogi	/*/public_html/modules/system/kebogi.php	9f8ed58495a4334b8d375915a3ea8a8034807173d2a620c0358e19ee413212cd	N/A	N/A	Līdzības najyka.php
Najyka	/*/public_html/modules/system/najyka.php	6ce3f9091e481b01ed6949657b5228e7d6dca9f7bdc32f4e4033621ed1da16e8	N/A	N/A	Līdzības kebogi.php, kods gandrīz identisks ar tīmekļčaulu, kas minēta šeit: https://jetpack.com/resources/vulnerable-kaswara-modern-wpbakery-plugin/
cn-2.php / CSS.php	federac/public_html/old_files/css/css.php	9b6ea86ffbec62b45b12824ae56f2781ac736243cce8122b24f0c9b678546c70	https://github.com/H4K6/webshell/blob/main/dama/cn-2.php	N/A	Visas tīmekļa čaulas, kas pieejamas šeit: https://github.com/H4K6/webshell/blob/main/dama/ ir ļoti līdzīgas. Valoda liecina, ka izveidotājs ir CN, pēdējo reizi atjaunināts 2020
Style	/home/*/public_html/misc/farbtastic/style.php				

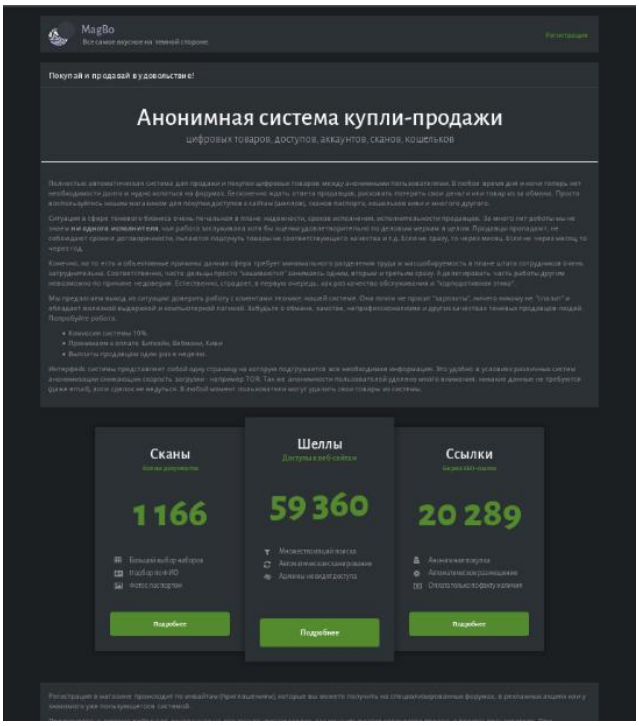
Datnes “style.php” nākamais etaps “ALFA Shell” ir atrodams tikai vienā publiskā “github” koda bāzē profilam ar reģistrācijas e-pasta adresi fedhrm@gmail.com:

Jacob Kuuhaku fedhrm@gmail.com; https://github.com/nicxlau/alfa-shell

IP: 185.175.44.233; ASN: AS50340; valsts: RU; domēns: magbo.cc

Atverot domēnu “magbo.cc”, apmeklētājs tiek novirzīts uz šādu vietni: http://magbocc3wzx4ysz6slun7pquhg7obesiwwtgymsggybkjfc53lav2pyd.onion/

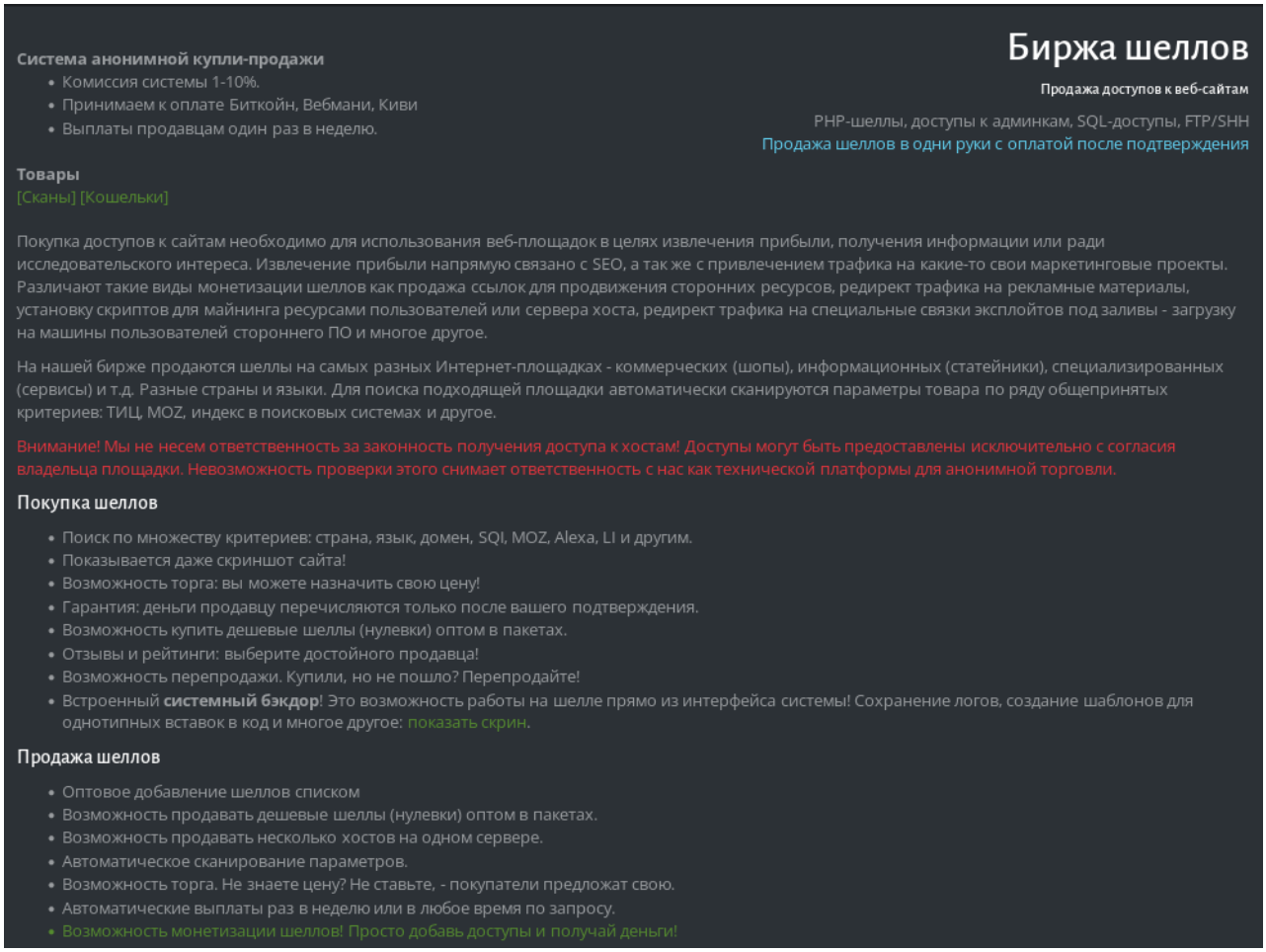
Magbo.cc ir Krievijā izstrādāta anonīma “digitālo preču, piekļuves, kontu, skenēšanas, maku” pirkšanas un pārdošanas sistēma. Tīmekļvietnē aprakstīts, ka var nopirkt piekļuves vietnēm, precīzāk, tīmekļa čaulām. Liels uzsvars uz lietotāju anonimitāti – kriptovalūtu pirkumi bez pircēja/pārdevēja datiem un darījuma žurnāliem.



Kaut arī “MagBO” vietnē ir brīdinājums (att. zemāk) neveikt nelegālas darbības, faktiskā rīcība liecina par tieši pretējo – šis serviss darbojas ar tiešu nolūku veikt kaitnieciskas darbības ar nelikumīgi iegūtām piekļuvēm.

Внимание! Публикуемые материалы преследуют цель предупредить незаконные действия в сфере IT и предостеречь пользователей от действий мошенников. Мы категорически не рекомендуем использовать эту информацию для нарушающего закон извлечения прибыли и предупреждаем о серьезной административной и уголовной ответственности за подобные действия! Мы не несем ответственности за последствия и принятия конкретными читателями решений об использовании данной информации. Все материалы несут исключительно информационный характер.

Papildu informācija par tīmekļa čaulu iegādi pieejama saitē: http://magbocc3wzx4ysz6slun7pquhg7obesiwwtgymsggybkjfc53lav2pyd.onion/about/shells



Tīmekļa čaula “tbakrn.php” ir tikai viens variants no ļoti plaši izplatītās WSO saimes, kurai ir publiski pieejamas vairākas versijas dažādās valodās, tajā skaitā krieviski (https://github.com/Josexv1/wso-webshell). Tomēr “tbakrn.php” saturā bija vairākas koda sadaļas, kas identiski sakrīt ar atrasto “Github” kodu krātuvē profilā “Josexv1”, saitē: https://github.com/Josexv1/wso-webshell. Tīmekļa čaulās “bypafgss.php” un “css.php” ir vairāki atribūti, kas liecina par iespējamu saistību ar Ķīnu. “bypafgss.php” ir ticis kodēts ar ķīniešu PHP kodēšanas servisu, savukārt, “css.php” ir gandrīz identisks publiskajā internetā atrodamai tīmekļa čaulai, kuras izveidotāja profils ar reģistrētu e-pasta adreses domēnu “qq.com” jeb Tencen QQ – Ķīnā plaši izmantotu tūlītējās saziņas platformu.

https://github.com/H4K6 Saistīta e-pasta adrese: akiritsu 240799357@qq.com

Pamatojoties uz visu tīmekļa čaulu (“gecko.php”, “style.php”, “kebogi.php”, “najyka.pjp”, “style.php”) vairākiem savstarpēji saistītiem atribūtiem, var uzskatīt, ka visas saistītas ar vienu uzbrucēju grupējumu. Turklāt vienīgā iesaistītā IP adrese 185.175.44.233 ir tālāk saistīta ar krieviski komunicejošo “magbo.cc”, kas ir nelikumīgi iegūtu piekļuvju pārdošanas pakalpojuma platforma. Ņemot vērā izmeklēšanā atrasto un uzlauztās mājas lapas saturu, tās kompromitēšana varētu būt Krievijas valsts interesēs.

Kaut arī divās citās tīmekļa čaulās (“bypafgss.php” un “css.php”) identificēti vairāki atribūti, kas norāda uz iespējamu saistību ar ĶīnU (ķīniešu hieroglifi, Ķīnas kodēšanas serviss, Github konts ķīniešu valodā), un zināms apstāklis, ka uzlauztās vietnes saturs par Latvijas Valsts aizsardzību skar Ķīnas ģeopolitiskās intereses, tomēr

ir zema ticamība uzbrukuma saistībai ar Ķīnas atbalstītiem grupējumiem. Tāpat zema iespējamība, ka tas ir Krievijas atbalstīts grupējums, kas, balstoties uz CERT.LV vēsturisko izmeklēšanas pieredzi, izmanto Ķīnas izstrādātas tīmekļa čaulas ar mērķi maldināt noziedznieka profilēšanas un iesaistes (atribūcijas) procesu.

Ieteikumi

- Izveidot tīmekļa vietni uz jaunas Drupal platformas, vēlama 10. versija vai tāda, kas saņem drošības atjauninājumus.
- Esošo tīmekļvietni nepieciešams izveidot no jauna ar atjaunotiem moduļiem un bibliotēkām. Satura un failu kopēšanu no iepriekšējās vietnes veic, stingri izvērtējot nepieciešamību.
- Pārskatīt PHP konfigurāciju, neatļaut augšupielādi failiem ar paplašinājumu "*.php".
- Ieviest Drupal platformas vairāku faktoru autentifikācijas moduli (Two-Factor Authentication (TFA) Module / Login Security Module / Authy Two-Factor Authentication / Google Authenticator).
- Pēc vietnes migrēšanas pie mitināšanas pakalpojumu sniedzēja Cloudflare, visi pieprasījumi uz vietni tiks veikti no Cloudflare starpniekserveru ("proxy") IP adresēm, nevis no sākotnējā klienta IP. Tas nozīmē, ka standarta žurnalēšanas konfigurācijā (piemēram, "Nginx" vai "Apache") netiks uzrādīta apmeklētāja reālā IP adrese, bet gan Cloudflare IP adrese.
- Cloudflare automātiski pievieno HTTP galveni "CF-Connecting-IP", kurā atrodas klienta reālā IP adrese.
- Tīmekļa servera konfigurācijas failā pievieno šādus parametrus: "Nginx: real_ip_header CF-Connecting-IP" un "Apache: RemoteIPHeader CF-Connecting-IP".
- Ņemot vērā, ka resursu inventarizācijas sarakstā ir arī cita mājaslapa, tad CERT.LV piedāvā veikt izmeklēšanu un analīzi arī šim resursam.
- Savas infrastruktūras aizsargāšanai iesakām izmantot CERT.LV pakalpojumus, sīkāk var iepazīties: https://cert.lv/lv/pakalpojumi.
- CERT.LV iesaka izvērtēt, vai organizācijas pakalpojumi atrodas aizsargājamo resursu sarakstā, to var noskaidrot sazinoties ar Aizsardzības Ministriju.

Kompromitēšanas indikatori (IOC)

- 33d83b7c170efe509a502c5c1f3d18cbed951529cb9b9670cdb3193e67f650c9 [bypafgss.php]
- b462036676f01913cb9ed6380599f85b78bfea0d739429c4da359afe526503fd [tbakrn.php]
- 9f8ed58495a4334b8d375915a3ea8a8034807173d2a620c0358e19ee413212cd [kebogi.php]
- 6ce3f9091e481b01ed6949657b5228e7d6dca9f7bdc32f4e4033621ed1da16e8 [najyka.php]
- 8e7334db6056355563a58980bb153eb7f72d830fcbd208f189b1613c0f0712a3 [gecko.php]
- b8e9014514b8327f0424470d6157a499ab0b7187c8c22ba9d96fe46f84807149 [style.php]
- 9b6ea86ffbec62b45b12824ae56f2781ac736243cce8122b24f0c9b678546c70 [css.php]
- http://www.qkl2048[.]com/tools/gekcko.txt
- 185.175.44.233

3. Pakalpojumu atteices uzbrukumi (DDoS)

DDoS uzbrukumus, turpinot iepriekšējo gadu raksturīgās iezīmes, galvenokārt veic prokrieviski haktīvistu grupējumi un valstiski atbalstīti uzbrucēji. Abu līdzīgais vienojošais mērķis ir radīt jebkāda veida un mēroga destrukciju. DDoS uzbrukumi neprasa augstas tehniskās prasmes, bet spēj radīt plašu pakalpojumu nepieejamību, ietekmēt iedzīvotāju ikdienu, radīt sabiedrības rezonansi un mediju uzmanību.

NATO un ES dalībvalstis, tajā skaitā Latvija, ir galvenie mērķi DDoS uzbrukumiem. Tos bieži veicina politiskās aktivitātes, kuras regulāri tiek uztvertas kā simboliska pretestība pret Krievijas agresiju. Tādēļ šīs valsts atbalstīti uzbrucēji cenšas izraisīt pakalpojumu atteices uzbrukumus Latvijas valsts un pašvaldību, finanšu, veselības iestāžu, transporta nozares un e-pakalpojumu resursiem, lai radītu spiedienu, provocētu plašu trauksmi un destabilizētu sabiedrību.

Salīdzinot ar iepriekšējiem gadiem, jaunā tendence ir arvien vairāk veiktu DDoS uzbrukumu no Latvijas IP adresēm. Indikatori norāda, ka šīs adreses lielākoties ir kompromitētas ierīces, piemēram, viedierīces, IoT jeb dažādas ierīces, kas ir pieslēgtas internetam vai lokālajam tīklam. Tās tiek pārveidotas par robottīklu (*botnet*) elementiem un izmantotas jau kā DDoS uzbrukumu dalībnieki, radot noslodzi cietušā resursiem. Iemesls novērotajam jaunumam, iespējams, ir ģeolokācijas ierobežojumi (pieejas aizliegums no ārvalstu IP adresēm) un esošie aizsardzības mehānismi.

3.1. Incidentu piemēri

Uzbrukums kādai tīmekļa sistēmai (MITRE ATT&CK: T1498.001)

2025. gada 3. martā saņemts incidenta pieteikums par lēnu sistēmas darbību. Analīze parādīja, ka tīmekļa vietnei uzbruka trīs IP adreses 45.131.103.207, 45.131.102.49 un 45.131.101.183 veicot vairāk nekā miljons failu pārlases pieprasījumus. Lai arī incidents netiek klasificēts kā DDoS ar mērķi nobloķēt sistēmu, tas ietekmēja vietnes darbības stabilitāti pārslogotās datubāzes dēļ.

Citas tīmekļa platformas nepieejamība (MITRE ATT&CK: T1498.001)

2025. gada 2. novembrī reģistrēta citas tīmekļa platformas nepieejamība, ko ietekmēja vairāku pieprasījumu kopums no dažādu valstu IP adresēm. Daļa no iesaistītajiem DDoS aģentiem ir tīkla maršrutētāji. Lai arī 160 transakcijas/sek. nav augsta uzbrukumu intensitāte, tā spēja vietnei izsaukt PHP darbību izpildes funkcionalitāti, tādējādi pārslogojot sistēmu un padarot to nepieejamu.

Top 10 ASN (interneta pakalpojuma sniedzēju identifikatori), no kuru resursiem notika uzbrukums:

2 "AS2514 NTT PC Communications, Inc."
2 "AS31898 Oracle Corporation"
2 "AS3320 Deutsche Telekom AG"
2 "AS44056 Trytek LLC"
2 "AS53667 FranTech Solutions"
3 "AS202561 High Speed Telekomunikasyon ve Hab. Hiz. Ltd. Sti."
3 "AS214677 DELUXHOST"
3 "AS394684 GOLD DATA USA INC"
3 "AS396982 Google LLC"

3 "AS51167 Contabo GmbH"
3 "AS8075 Microsoft Corporation"
6 "AS45326 Broad Band Telecom Services Ltd"
13 "AS14061 DigitalOcean, LLC"

Uzbrukums vēl kādai vietnei no Latvijas reģiona iekārtām (MITRE ATT&CK: T1499.003, T1499.003)

2025. gada 29. aprīlī vēl kādai vietnei notika DDoS uzbrukums, kas veikts lielākoties no Latvijas reģiona IP adrešu apgabala. Īpaši jāizceļ, ka DDoS uzbrukums notika L7 jeb lietotnes līmenī, no aģentiem vienlaikus izsūtot milzīgu skaitu HTTP GET/POST pieprasījumu. Tīkla plūsma izraisīja īslaicīgus pieejamības traucējumus, kas rezultējās tīmekļa resursa nepieejamībā. Incidenta analīze atklāja, ka DDoS uzbrukumu aģenti ir inficētas Android iekārtas. Visiem pieprasījumiem bija raksturīgs "user-agent": Dart/3.6 (dart:io) ieraksts.

Uzbrukumā bija iesaistītas inficētas Android iekārtas no Latvijas IP adresēm.

DDoS uzbrukumi lietotnes jeb L7 līmenī (MITRE ATT&CK: T1499.003)

Tīmekļa resurss sākotnēji tiek izpētīts, meklējot saites, kuru izsaukšana visvairāk noslogotu sistēmu. Attiecīgi, sūtot vairākus pieprasījumus, resurss vai vietne tiek pārslogota līdz nepieejamībai. Biežākie vektori ir tīmekļa vietņu funkcionalitātes kā mājaslapas meklētājs vai citas izpildes darbības, piemēram, pdf failu ģenerēšana.

Piemēri:

Veids	Metode	Domēns	IP	Ports	Parametri
http2	GET	www.*.lv		443	/stati/?cs=$_1
http2	GET	www.*.lv		443	/jaunumi/page/$_2/
http2	GET	www.*.lv		443	/arhivs/?yr=20$_5&mo=
http2	GET	www.*.lv		443	/lv/search?q=$_1
http2	GET	www.*.lv		443	/lv/jaunumi?title=$_1

DDoS uzbrukumi no kompromitētām iekārtām (MITRE ATT&CK: T1584.005)

Tiek izmantots inficētu iekārtu robottīkls ("botnet"), lai veiktu DDoS uzbrukumus. IP adrešu informācija parāda, ka uzbrukums veikts no vairākām Latvijas reģiona IP adresēm.

Lai arī norādītās IP adreses nav lietotāju gala iekārtas, taču novērota likumsakarība ir to pielāgojums mobilajam tīmeklim. CERT.LV šajā laikposmā saņēma informāciju, ka minētās IP adreses marķētas kā "Vo1d" vai "BadBox 2.0" inficētas iekārtas.

Veiktie pieprasījumi uzskatāmi parāda, ka iekārtas izmantotas kā starpnieki ("proxy"):

GET /api/all-operational-changes/lv HTTP/1.1

user-agent: Dart/3.6 (dart:io)

accept-encoding: gzip

authorization: **************

host: www.*.lv

X-Forwarded-For: 77.219.5.96

DDoS uzbrukumos tiek izmantoti arī maršrutētāji, ko parāda uzbrukums kādai tīmekļa platformai:

{"ip":"","services":{"transport_protocol":"TCP","extended_service_name":"MIKROTIK_WINBOX","service_name":"MIKROTIK_WINBOX","port":7575}
}

{"ip":"","services":{"transport_protocol":"TCP","extended_service_name":"MIKROTIK_BW","service_name":"MIKROTIK_BW","port":2000}}

{"ip":"","services":{"transport_protocol":"TCP","extended_service_name":"MIKROTIK_WINBOX","service_name":"MIKROTIK_WINBOX","port":7575}
}

{"ip":"","services":{"transport_protocol":"TCP","extended_service_name":"MIKROTIK_BW","service_name":"MIKROTIK_BW","port":2000}}

{"ip":"","services":{"transport_protocol":"TCP","extended_service_name":"MIKROTIK_WINBOX","service_name":"MIKROTIK_WINBOX","port":7575}
}

{"ip":"","services":{"transport_protocol":"TCP","extended_service_name":"MIKROTIK_BW","service_name":"MIKROTIK_BW","port":2000}}

{"ip":"","services":{"transport_protocol":"TCP","service_name":"MIKROTIK_WINBOX","extended_service_name":"MIKROTIK_WINBOX","port":2112}
}

{"ip":"","services":{"transport_protocol":"TCP","service_name":"MIKROTIK_WINBOX","extended_service_name":"MIKROTIK_WINBOX","port":8291}

{"ip":"","services":{"transport_protocol":"TCP","extended_service_name":"MIKROTIK_BW","service_name":"MIKROTIK_BW","port":2000}}

{"ip":"","services":{"transport_protocol":"TCP","service_name":"MIKROTIK_BW","extended_service_name":"MIKROTIK_BW","port":2000}}

{"ip":"","services":{"transport_protocol":"TCP","extended_service_name":"MIKROTIK_WINBOX","service_name":"MIKROTIK_WINBOX","port":511}}

{"ip":"","services":{"transport_protocol":"TCP","service_name":"MIKROTIK_BW","extended_service_name":"MIKROTIK_BW","port":2000}}

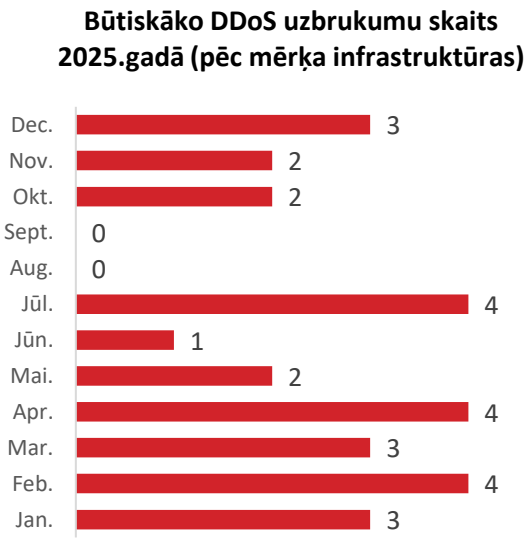
3.2. Aizsardzības pasākumi

Aizsardzībai pret DDoS uzbrukumiem ir 2 veidu mehānismi:

- **Satura servēšana** - biežāk pieprasītā satura novietošana starpatmiņā (kešatmiņā), kas atvieglo datubāzes noslodzi.
- **Automātisku apstrāžu mazināšana** - ieviest lietotāju pārbaudi uz resursu ietilpīgu funkciju izpildi, kas mazina sistēmas pārslodzes risku automātiski izsauktu meklēšanas vai PDF ģenerēšanas gadījumos.

Papildu kompleksos risinājumus nodrošina Interneta pakalpojuma sniedzēji.

Atsevišķas svarīgākās sistēmas var novietot CDN (Content Delivery Network) aiz DDoS aizsardzības.



4. Ievainojamību apkopojums

Programmatūras ievainojamības ir loģiskās kļūdas programmatūras kodā. Informācijas sistēmām tās rada kiberuzbrukumu vektorus, kurus var izmantot gan neautorizētai piekļuvei, gan pieejamības ietekmei, attiecīgi apdraudot to konfidencialitāti un integritāti vai traucējot informācijas sistēmas funkcionalitāti.

Mūsdienās kiberuzbrukumos programmatūras ievainojamības pārsvarā tiek izmantotas sākotnējās piekļuves un privilēģiju eskalācijas etapos. Ievainojamību ļaunprātīga izmantošana sākotnējās piekļuves nodrošināšanai praksē ir tīmeklī brīvi eksponētas iekārtas, publiski atvērtas pārvaldības konsoles, nejauši eksponēti servisi vai perimetra ("edge") iekārtas un citas nekorekti konfigurētās ierīces.

Tīmeklī eksponēta un ievainojama iekārta rezultātā kļūst par vārteju ("gateway") organizāciju korporatīvajos iekštīklos, ļaujot uzbrucējiem pārvarēt ārējo perimetru jau pašā sākumā un pāriet nākamajā fāzē, turpinot izvērst kiberuzbrukumu jau infrastruktūras iekšienē. Līdz ar to, gan informācijas sistēmas administratoriem, gan kiberdrošības personālam jāveic izmantoto programmatūras versiju un ievainojamību monitorings, pievēršot īpašu uzmanību internetā eksponētām iekārtām.

4.1. Nozīmīgāko incidentu piemēri

Kritiska lokālā (on-premises) SharePoint servisa ievainojamība CVE-2025-53770, kas ļauj neautentificētam uzbrucējam izpildīt attālinātu kodu ar parametra "__VIEWSTATE" "deserializācijas" nepilnību. Uzbrukums ir īstenots, kad augšupielādē .aspx datni jeb tīmekļa čaulu ("webshell") – ļaundabīgu skriptu, kurš paredzēts attālināto komandu izpildei, izmantojot HTTP protokolu.

Izmeklēšana atklāja uzbrukuma gaitu, tās sākums ir internetā eksponēts lokālais SharePoint serveris ar ievainojamību, kuru uzbrucēji izmantoja, ievietojot ļaundabīgu tīmekļa čaulu "spinstall0.aspx" ar attālināto Powershell koda izpildi, ko apliecina notikuma žurnālfails ar ID 4100.

Uzbrukumā uz kompromitētās ierīces tika izveidoti šādi faili:

- Program Files/Common Files/microsoft shared/Web Server Extensions/16/TEMPLATE/LAYOUTS/spinstall0.aspx (jaucējvērtība 92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514);
- Windows/Microsoft.NET/Framework64/v4.0.30319/Temporary ASP.NET Files/root/b96e96c3/cdbb1652/App_Web_spinstall0.aspx.9c9699a8.gznym_h2.dll (jaucējvērtība c7f7e1b7cf009d738a49e54fb1f3e131067e5510dc1005a7974688a155c841e);
- Windows/Microsoft.NET/Framework64/v4.0.30319/Temporary ASP.NET Files/root/b96e96c3/cdbb1652/spinstall0.aspx.9c9699a8.compiled (jaucējvērtība 62e6ed4930d3a7ee52d1a99297d1a265e28a6a439d52d9ee9b0fe3f83d6d487a).

Analizējot ievietoto ļaunatūras failu, konstatēts, ka uzbrukuma mērķis ir kompromitēto iekārtu atslēgu (machineKey) vērtības, ko tīmekļa izstrādes ietvars "ASP.NET" lieto "FormsAuthentication" un citu datu parakstīšanai un šifrēšanai. Tas ļauj turpināt attālinātu kodu izpildi pat pēc sākotnējās tīmekļa čaulas dzēšanas, nodrošinot pilnīgu servera kontroli un iespēju nemanāmi pārvietoties iekšējā tīklā.

Pēc atslēgu iegūšanas uzbrucēji var autentificēties kā jebkurš lietotājs un pārņemt iekārtas kontroli pat pēc paroles maiņas. Šajā situācijā vienīgais veids, kā pasargāt infrastruktūru, ir veikt iekārtas atslēgas nomaiņu jeb rotāciju.

Ļaunatūras izpildes process noritēja pēc šādas secīgas hierarhiskas (“parent/child”) shēmas:

- C:\Windows\System32\inetsrv\w3wp.exe;
    - C:\Windows\System32\cmd;
        - šifrēta “base64 PowerShell” komanda.

Žurnālfailu analīze atklāja uzbrucēju izmantotās IP adreses: 107.191.58.76, 154.47.21.168, 80.89.77.121, 84.15.222.129, 104.238.159.149, 80.89.76.3 un 78.84.21.118.

Attālināto pakalpojumu risinājuma “Ivanti Cloud Services Appliances” produkta ievainojamības CVE-2024-8190 (direktorijas ceļa manipulācija, “Path Traversal”) un CVE-2024-8963 (operētājsistēmas komandu injekcija, “OS Command Injection”) ļauj uzbrucējam veikt attālinātu koda izpildi. Konkrēti, CVE-2024-8190 atļauj piekļūt ievainojamam failam “DateTimeTab.php”, kam, savukārt, ar “http POST” metodi bez validēšanas var ievietot ļaundabīgu argumentu (CVE-2024-8963). Abu CVE kombinācija ļauj uzbrucējiem veikt attālināto koda izpildi pret tīmeklī eksponētu, ievainojamu “Ivanti Cloud Services Appliances” serveri. Ievainojamās ierīces izmeklēšanā atrasts žurnālfaila “messages” fragments, kas parāda uzbrucēju izpildītās komandas.

Pēc ievainojamības izmantošanas uzbrucēji izveido “NetCat” reverso čaulu (“ReverseShell”) uz mērķa IP adresi.

Pēc ievainojamības izmantošanas un pastāvīgās pieejas (“persistence”) nodrošināšanas, uzbrucēji veica iekštīkla skenēšanu, lai identificētu sānu (laterālās) kustības mērķus. Konkrētajā incidentā, pateicoties cietušā informācijas sistēmas infrastruktūrā strādājošam EDR risinājumam, kibernoziedznieki tika pamanīti un uzbrukums veiksmīgi novērsts.

Sākotnēja piekļuve tiek nodrošināta arī ar salīdzinoši vecām ievainojamībām, piemēram, CVE-2019-18935 jeb “Progress Telerik UI for ASP.NET AJAX”. Specifiski, šajā konkrētajā kiberuzbrukuma gadījumā ilgu laiku neatjaunināta, tāpēc ievainojama ierīce tika netīšām eksponēta tīmeklī ugunsmūra konfigurācijas kļūdas dēļ. Tas apstiprina nepieciešamību regulāri veikt programmatūras atjauninājumus arī tikai iekštīklam paredzētiem pakalpojumiem, protams, sevišķi rūpīgi sekojot līdzi tīmeklī eksponētām ierīcēm. Serverī ar šo ievainojamību tika ievietotas vairākas tīmekļa čaulas, kas saņēma komandas no IP adreses 178.18.254.229:

- C:/Windows/Temp/1754175431.6374192.dll (jaucējvērtība b989b09332422e938e8510d7e2cc7a7e75f4eec9b140c44511cc1254e6fc3ad9);
- C:/Windows/Temp/1754175473.6844523.dll (jaucējvērtība 2a9386e864cd299eedc6efce355caf8c5f4ade927a06471a4f5de4ff5c179d59);
- C:/Windows/Temp/1754175900.6890523.dll (jaucējvērtība 1b36f06740aab7ab7f385d1ca77f4e6bafcda3bdee40da6021f8e38bbc39e55e);
- C:/Windows/Temp/1754512465.837927.dll (jaucējvērtība b989b09332422e938e8510d7e2cc7a7e75f4eec9b140c44511cc1254e6fc3ad9);
- C:/Windows/Temp/1754512702.1202972.dll (jaucējvērtība 1b36f06740aab7ab7f385d1ca77f4e6bafcda3bdee40da6021f8e38bbc39e55e).

Tālākās uzbrucēju darbības bija privilēģiju eskalācija un sānu (laterālā) kustība ar nolūku šifrēt kompromitēto infrastruktūru (skat. sadaļu “Finansiāli motivēti uzbrukumi”).

Tīmeklī eksponēts attālinātās piekļuves RDP pakalpojums un ugunsmūru konfigurācijas nepilnības

Vairāki incidenti 2025. gadā tika konstatēti ar tīmeklī eksponētu grafisko attālinātās pārvaldības RDP, VNC, X11 pakalpojumu Aktīvās direktorijas ekosistēmas ierīcēm. Incidentu galvenais iemesls - darba datoriem nebija ieslēgti vai pareizi konfigurēti iekārtas ("host") ugunsmūri. Darbinieki, strādājot attālināti no mājas biroja, pieslēdza organizācijas datorus mājas tīmekļa ierīcēm, kas piešķīra šiem datoriem publiskās IP adreses, tādējādi atklājot attālināto servisu portus internetā. Tas spilgti parāda, kaut arī organizācijas pārvaldītās ierīces tika pasargātas ar korporatīvā tīkla ("network") ugunsmūra risinājumu, tās nav aizsargātas ārpus organizācijas vides bez pareizas gala iekārtas ugunsmūra konfigurācijas.

Tīmeklī atvērti attālinātas pārvaldības pakalpojumi tiek nekavējoties pakļauti paroļu minēšanas uzbrukumiem. Vairākos incidentos uzbrucējiem izdevās atminēt lokālo noklusējuma lietotāju vai servisu darbības kontu paroles. Cietušo infrastruktūrā pārsvarā īstenota slikta prakse, servisu darbībai deleģējot lietotāja kontus ar vājām parolēm.

Pēc uzbrucēja izpildītas autentificēšanās, gandrīz visos gadījumos turpinājumā bija mēģinājums šifrēt ierīci. Konstatēti gadījumi, kad uzbrucēji mērķtiecīgi veica Latvijas IP adrešu apgabala skenēšanu, (piemēram, no IP 139.135.50.22) uz atvērtiem RDP servisiem ar paroļu atkārtotas izmantošanas uzbrukuma jeb "password stuffing" metodi. Konsolidētā sarakstā apvienotas derīgas lietotāju paroles tirgotas tumšajā tīmeklī ("darknet") vai saziņas platformas "Telegram" atbilstošajos kanālos.

Ievainojamu robottīklam pievienotu maršrutētāju izmantošana uzbrukumiem Latvijas infrastruktūrai

ASV Federālās izmeklēšanas birojs 2025. gada 7. maijā publicēja rakstu par tīkla aparatūras ražotāju "Linksys" un "CISCO" rūteru plašu kompromitēšanu, pievienojot tos robottīklam, izmantojot versiju ievainojamības. Abu ražotāju tīkla maršrutētājiem ir publiski zināmas kritiskas ievainojamības, tajā skaitā CVE-2025-34037, CVE-2018-0171, CVE-2017-6736, kuras ļauj veikt attālināto koda izpildi. Neautorizētas piekļuves incidentu izmeklēšanā konstatēts, ka no Latvijas reģiona IP adresēm veikti pieslēgumi ievainojamu rūteru "Linksys" tīmeklī eksponētiem pārvaldības portiem (TCP 8080).

Papildu informācijai saraksts ar iekārtām, kurām beidzies ražotāja atbalsts ("End-of-Life"):

- https://www.ic3.gov/CSA/2025/250507.pdf;
- https://www.ic3.gov/PSA/2025/PSA250820.

Attēlā: Maršrutētāja pārvaldības konsole (fragments)

Robottīklam pievienota “Linksys” rūtera raksturīgās pazīmes (signatūras) ir tīmeklī eksponēts pārvaldības ports TCP 8080 un raksturīgi tehniskās informācijas “http” ziņojumi . Izveidots iespējami kompromitēto maršrutētāju saraksts, kurš validēts, pamatojoties uz reālu incidentu datiem. Ierīces izmantotas, lai konfidenciālai informācijai piekļūtu ar neautorizēti iegūtiem autorizācijas datiem (piemēram, no datu zagšanas ļaunatūras).

Iepriekš minētais parāda, ka tīmeklī eksponētās, ievainojamās iekārtas var tikt izmantotas uzbrukumiem trešās puses infrastruktūrai. Turklāt, izmantojot kompromitētas perimetra (edge) ierīces, mērķa valsts vidē kibernoziedznieki veido savu infrastruktūru, lai veiktu kiberuzbrukumus no šīs valsts IP apgabala, tādējādi apejot ugunsmūru iestatīto reģionu bloķēšanas filtru.

Ir pieejama informācija par kompromitēšanas indikatoriem 12 “Linksys” maršrutētājos, kas izmantoti uzbrukumos pret Latvijas IS infrastruktūru (dati aktuali no 2025. gada jūnija līdz augustam).

4.2. Raksturīgākās tendences 2025. gadā

Iekārtu ražotāju un izstrādātāju “Fortinet”, “Citrix” un “Ivanti” produktos 2025. gadā tika novērotas vairākas kritiskas ievainojamības:

- “Fortinet” produktos vairāk nekā 20;
- “Citrix” programmatūras ievainojamība “CitrixBleed2” (CVE-2025-5777);
- “Ivanti” produktiem nulles dienas (“0 day”) ievainojamības CVE-2025-4427 un CVE-2025-4428, konkrēti, “Ivanti EPM” produktā 13.

Kaut arī augstāk minētās ievainojamības aktīvi izmantotas kiberuzbrukumos visā pasaulē, tomēr Latvijā netika konstatēti saistīti incidenti.

Lielais vairums izmantotās ievainojamības joprojām saistītas ar tīmekļa satura platformas “WordPress” pārvaldību saistītiem spraudņiem.

Konstatētas aktīvi izmantotas vietnes, kurām regulāri nesankcionēti mainīts saturs. Tām vairākus gadus netika atjauninātas tehnisko komponenšu versijas.

Kompromitētas tīmekļa vietnes bieži tiek izmantotas, lai izplatītu sociālās inženierijas ļaunatūru (viltus CAPTCHA), kā “ClickFix” un “ClearFake”.

Profilaktiskie un aizsardzības pasākumi

- Tīkla segmentēšana, tīmeklī eksponēto iekārtu inventarizācijas saraksts, regulāra izvērtēšana par nepieciešamību tās eksponēt internetā. Ja eksponēšana tīmeklī nepieciešama, regulāri nodrošināt visus iekārtas atjauninājumus.
- Pārliecināties par pareizi izmantotu un konfigurētu ugunsmūru risinājumiem. Nodrošināt konfigurāciju, kas piekļuvi pārvaldības un kontroles portiem (SMB, RDP, WinRM u.tml.) atļauj tikai no domēna iekštīkla.
- Uzturot tikai iekštīkla lietošanai paredzētas sistēmas, regulāri pārskatīt eksponētos servisus, īpaši pēc ugunsmūra konfigurācijas vai sistēmas atjaunināšanas veikšanas.
- Servisu darbības nodrošināšanai izmantot domēna lietotājus grupā “Group Managed Service Accounts”.
- Lietojot “WordPress” vai citas atvērtā koda CMS, konfigurācijā izvēlēties automātiskos atjauninājumus. Pārskatīt uzstādītos spraudņus un regulāri izvērtēt to nepieciešamību.

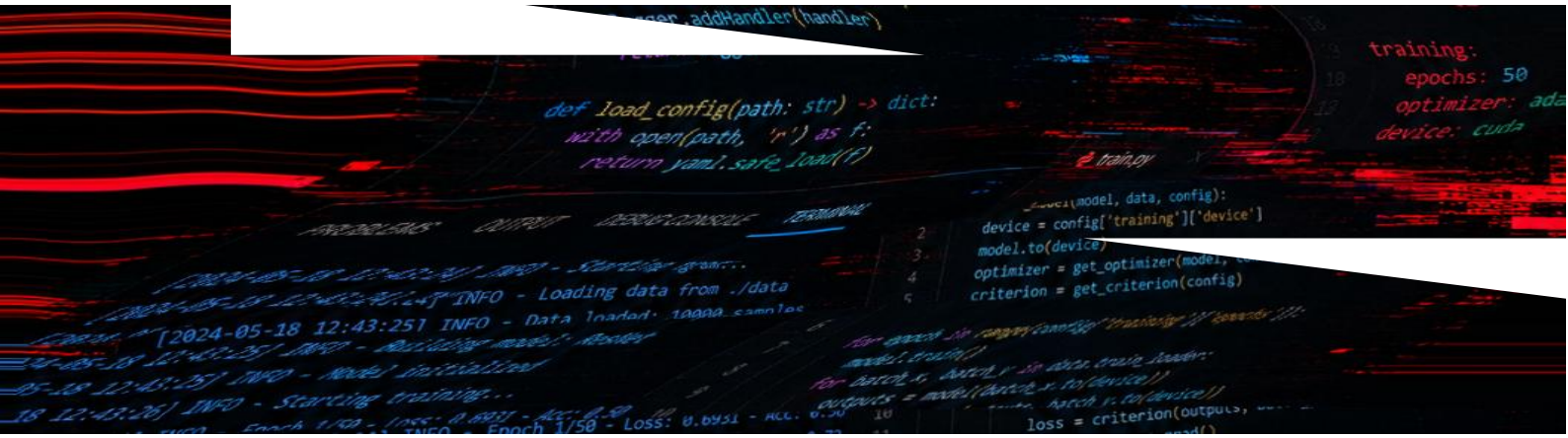
Kompromitēšanas indikatori (IOC)

Vadībā un kontrolē tika izmantotas šādas ievainojamības:

- CVE-2024-8963;
- CVE-2019-18935;
- CVE-2025-5377;
- RDP paroļu atkārtota izmantošana jeb “password stuffing”

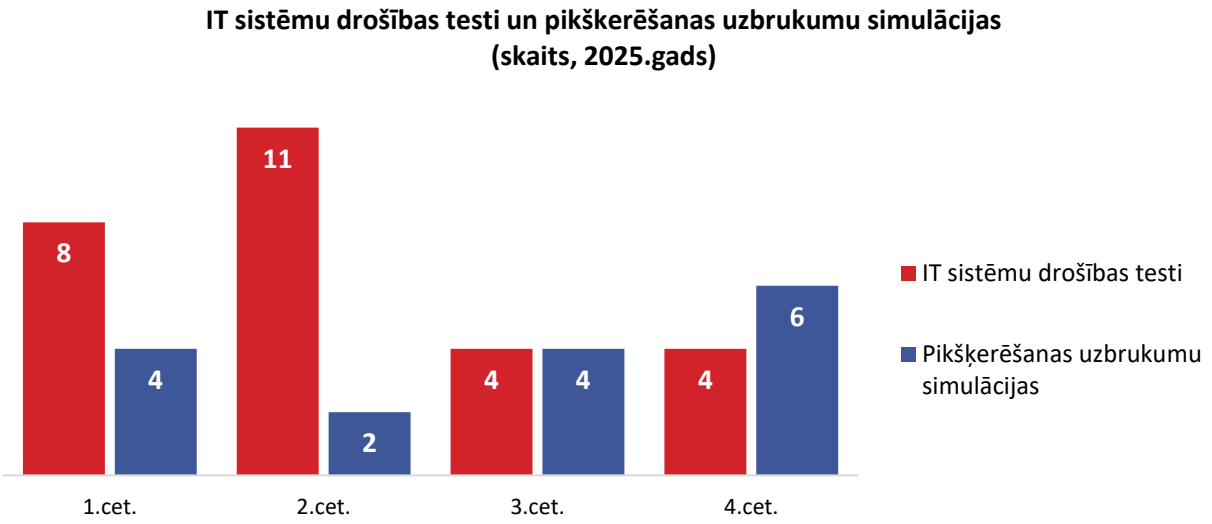
Ļaunatūra:

- CVE-2025-53770, tīmekļa čaula, jaucējvērtība 92bb4ddb98eeaf11fc15bb32e71d0a63256a0ed826a03ba293ce3a8bf057a514;
- CVE-2025-53770 tīmekļa čaula, jaucējvērtība c7f7e1b7cf009d738a49e54fb1f3e131067e5510dc1005a7974688a155c841e;
- CVE-2025-53770, tīmekļa čaula, jaucējvērtība 62e6ed4930d3a7ee52d1a99297d1a265e28a6a439d52d9ee9b0fe3f83d6d487a;
- CVE-2019-18935, tīmekļa čaula, jaucējvērtība b989b09332422e938e8510d7e2cc7a7e75f4eec9b140c44511cc1254e6fc3ad9;
- CVE-2019-18935, tīmekļa čaula, jaucējvērtība 2a9386e864cd299eedc6efce355caf8c5f4ade927a06471a4f5de4ff5c179d59;
- CVE-2019-18935, tīmekļa čaula, jaucējvērtība 1b36f06740aab7ab7f385d1ca77f4e6bafcda3bdee40da6021f8e38bbc39e55e;
- CVE-2019-18935, tīmekļa čaula, jaucējvērtība b989b09332422e938e8510d7e2cc7a7e75f4eec9b140c44511cc1254e6fc3ad9;
- CVE-2019-18935, tīmekļa čaula, jaucējvērtība 1b36f06740aab7ab7f385d1ca77f4e6bafcda3bdee40da6021f8e38bbc39e55e.



5. IT sistēmu drošības testi un kontrolētu uzbrukumu veikšana (Red Teaming)

CERT.LV 2025. gadā kopumā īstenoja **16** pikšķerēšanas uzbrukumu simulācijas un **27** IT sistēmu drošības testus.



5.1. Pikšķerēšanas uzbrukumu simulācija

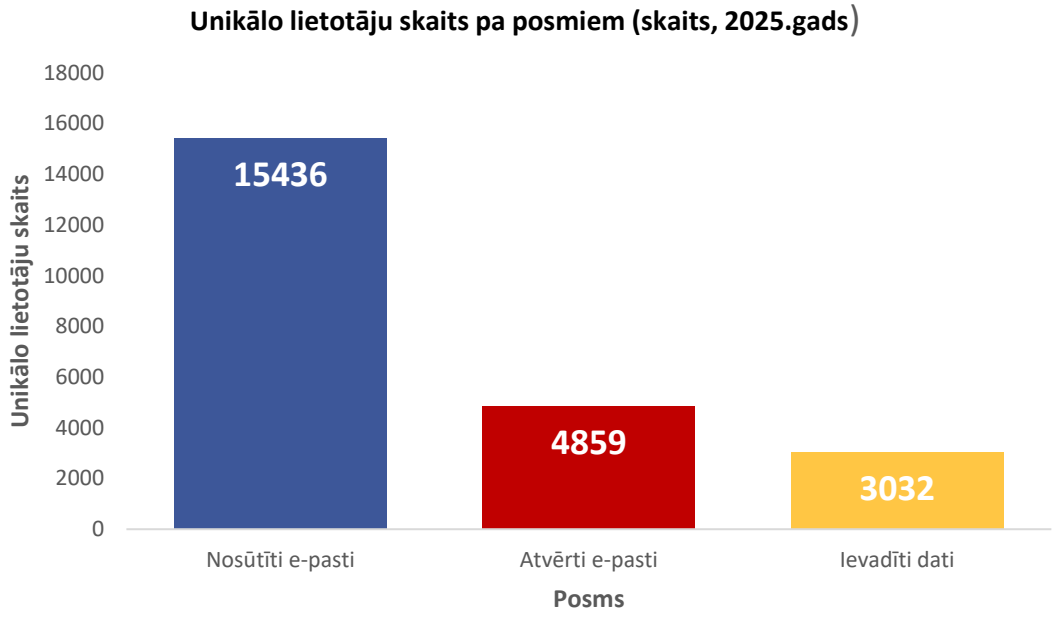
CERT.LV 2025. gadā īstenoja **16 pikšķerēšanas simulācijas kampaņas**, lai novērtētu darbinieku modrību pret kiberdrošības apdraudējumiem un lai identificētu virzienus, kuros nepieciešama papildu izglītošana.

Kampaņu mērķis bija iegūt aizsargājamus, sensitīvus lietotāju datus (e-pastu, lietotājvārdu, paroli) vai panākt e-pasta pielikumu lejupielādēšanu un ļaunatūras failu izpildīšanu uz savas darbstacijas. Kopumā tika nosūtīti 15 436 e-pasti, no kuriem atvērtas tika 4 859 e-pasta vēstules jeb 31,48%. Katras kampaņas beigās iestādei tika sniegta atskaite par rezultātiem un ieteikumi uzlabojumiem.

Rezultāti

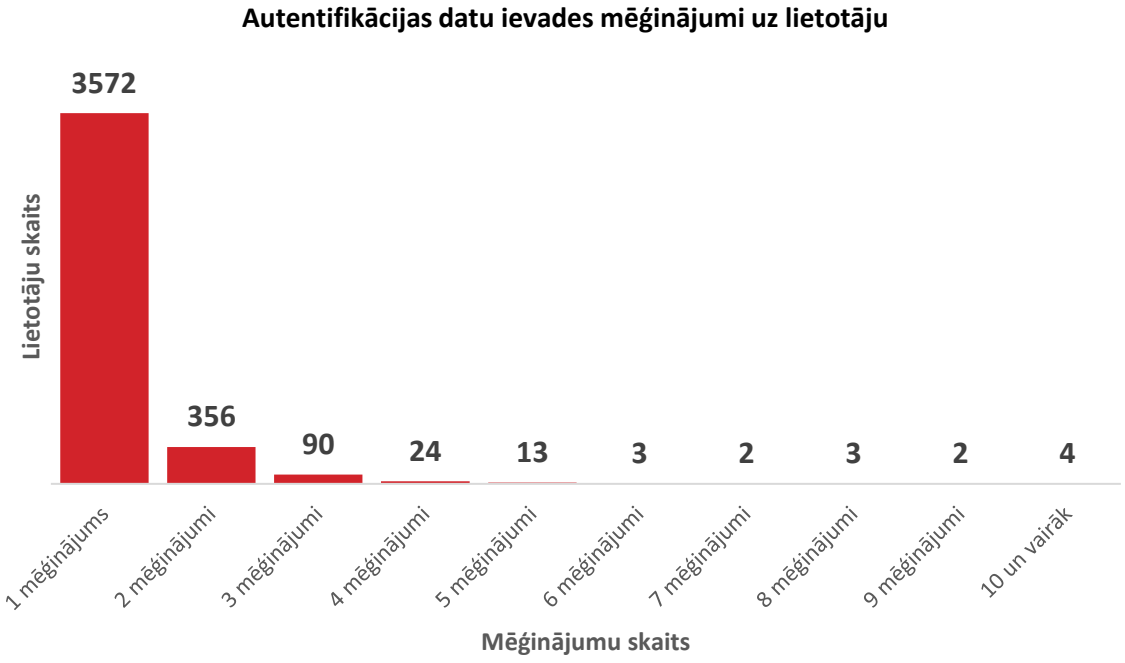
Analīzes rezultātā izveidots lietotāju skaita sadalījums pa unikālo apmeklējumu posmiem:

- Kampaņu norisē izsūtīti **15 436 e-pasti**;
- **Atvērtas** tika **4 859 e-pasta vēstules jeb 31,48%;**
- No atvērtajām vēstulēm **3 032 gadījumos tika ievadīti autentifikācijas dati** (kolonnu diagrammā nav iekļauti dati par darbiniekiem, kas atsevišķās kampaņās pikšķerēšanas vietnē nospieda uz pogas viltus AD autentifikācijas logā).



Datu ievades mēģinājumi

Pikšķerēšanas uzbrukuma simulācija pret 3 572 darbiniekiem tika īstenota, sasniedzot izvirzītos mērķus, proti, ievadīti akreditācijas dati vai nospiesta AD autentifikācijas poga. Grafikā attēlotajos ievades mēģinājumos ir tādi lietotāji, kas ierakstīja savus datus vairākas reizes. Tas notika pat pēc paziņojuma loga (rādīts katru reizi pēc paroļu iesūtīšanas) par pikšķerēšanas kampaņu, un informāciju, ka šī ir CERT.LV organizēta simulācija, papildus skaidrojot, kā atpazīt šādas kampaņas un kā no tām izvairīties. Rezultāti liecina, ka paziņojuma saturs ne vienmēr tiek pilnībā uztverts un daudzi darbinieki joprojām nepievērš pietiekamu vērtību tam, kur tiek ievadīti savi dati (10% gadījumu nosūtot atkārtoti).



Novērojumi un ieteikumi

Kopumā secinājumi un ieteikumi saglabājas nemainīgi. Liela daļa lietotāju joprojām nespēj sekmīgi atpazīt īstus e-pastus no uzbrucēju sūtītiem pikšķerēšanas e-pastiem. Tādēļ **aicinām iestādes regulāri apmācīt darbiniekus pikšķerēšanas e-pastu atpazīšanā.**

Atsevišķas organizācijas cenšas pasargāt vadības līmeņa darbiniekus, tos neiekļaujot kampaņu mērķu sarakstā vai pielāgojot tiem acīmredzami atpazīstamu pikšķerēšanas saturu. **Aicinām no šādas pieejas izvairīties, jo ļoti bieži tieši vadītāji kļūst par mērķi uzbrukumos, kuru nolūks ir iegūt datus ar augstu nozīmi amata pienākumu un piekļuves tiesību dēļ.**

Tāpat notiek mērķēti uzbrukumi, kuros saturs tiek pielāgots ne tikai konkrētai iestādei, bet arī konkrētam darbiniekam. Svarīgi ņemt vērā, ka šīs mācības ir treniņi, kas nerada nekādus zaudējumus, bet palīdz organizācijai identificēt vājās vietas, pie kurām nepieciešams strādāt.

Dažās kampaņās organizācijas lūdz iesniegt pikšķerēšanas "slazdos" iekritušo darbinieku sarakstu, lai pret viņiem vērstu kādas sankcijas, piemēram, piespiedu apmācības. **Arī no šādas pieejas aicinām izvairīties, jo apmācības jānodrošina visiem darbiniekiem regulāri, lai stiprinātu viņu zināšanas un praktiskās iemaņas.**

5.2. APT simulācija un mērķēta uzbrukuma simulācija klienta infrastruktūrai

Organizācijas vispārīgo gatavību reāla uzbrukuma gadījumā pārbauda APT jeb mērķēta uzbrukuma simulācijās. Jau šobrīd kritiskās infrastruktūras pārvaldītājiem ir vairākas prasības un pienākumi, kas jāievēro infrastruktūras pārvaldībā.

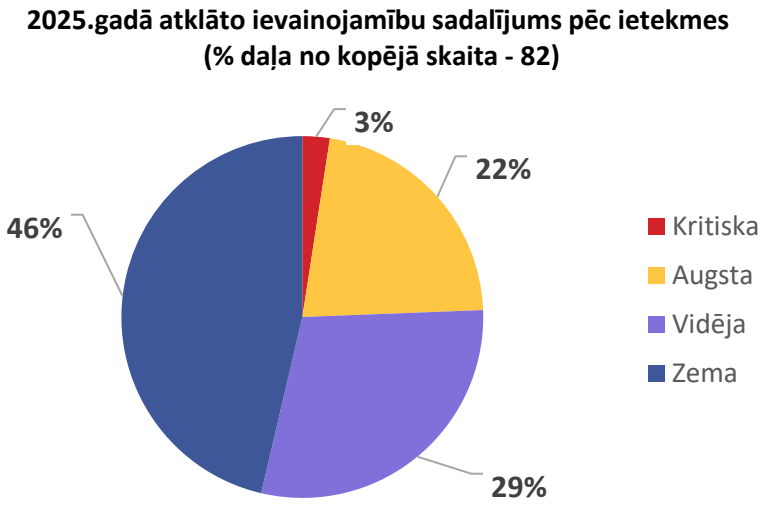
Pilnu uzbrukuma simulāciju 2025. gadā izlases kārtā CERT.LV veica kādā uzņēmumā, kas kritiskās infrastruktūras uzturētājiem nodrošina automatizācijas pakalpojumu un industriālu iekārtu komponenšu piegādi.

Saskaņotas simulācijas gaitā tika identificētas vairākas kritiskas ievainojamības, kas ļautu uzbrucējiem pilnībā pārņemt uzņēmuma infrastruktūru un kontroli aptuveni 30 Latvijas pilsētās. Sadarbībā ar uzņēmumu joprojām norit darbs pie identificēto nepilnību novēršanas.

5.3. IT sistēmu drošības testi

Drošības testu mērķis ir identificēt sistēmu ievainojamības, drošības apdraudējumus un nepilnības, lai novērstu iespējamos kiberuzbrukumus un datu noplūdes.

CERT.LV 2025. gadā veica **27 drošības testus**, kuru gaitā tika **atklātas 82 ievainojamības**, tostarp kritiskas un augstas ietekmes, kas tika novērstas pirms to iespējamās izmantošanas kiberuzbrukumos.



Būtiskākie secinājumi

Uzņēmuma e-pakalpojums:

- Iespējams nomainīt lietotāju datus un izveidot pieteikumu citai personai;
- Neautentificēta piekļuve aizsargājamai lietotāju informācijai;
- Iespēja izveidot vairākus iesniegumus vienam lietotājam;
- Iespēja apstiprināt nepilnīgu iesniegumu;
- Tīmekļa pakalpojumu "MS IIS" failu atlasīšana izmantojot "~" simbolu.

Uzņēmuma informācijas sistēma:

- Publiski pieejams .git programmu kodu platformas profils;
- Vairākas SQL injekcijas;
- Patvaļīga failu lasīšana;
- Iespējama privilēģiju eskalācija ar sesijas mainīgo iestatīšanu;
- XML ievainojamība XXE;
- Vairākas starpvietņu skriptēšanas (XSS) ievainojamības;
- Piekļuve visu lietotāju e-pastiem;
- Piekļuve augšupielādētiem failiem bez autentifikācijas;
- Publiski pieejami PowerShell faili.

Uzņēmuma slēgtā vide: Failu izgūšana no slēgtā tīkla.

Uzņēmuma informācijas sistēma:

- Paroles atjaunošanas saiti iespējams nosūtīt uz ļaunprātīgu vietni;
- Starpvietņu pieprasījuma viltošana (CSRF) profila dzēšanas pieprasījumā;
- E-veikalā iespējams mainīt cenu produktiem un piegādei;
- E-veikalā iespējams apiet maksāšanas procesu;
- Piekļuve citu lietotāju izrakstītajiem rēķiniem;
- Piekļuve citu lietotāju izveidotiem pieteikumiem.

6. SOC pakalpojuma rezultāti un galvenās tendences

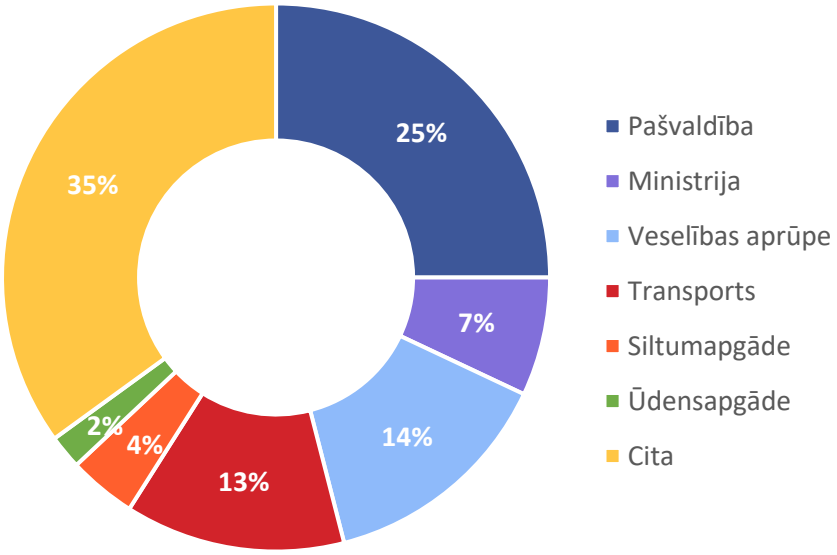
CERT.LV SOC pakalpojums centralizēti apkopo drošības telemetriju no klienta infrastruktūras, nosaka notikumu savstarpējās sakarības un sasaista tos ar visu CERT.LV pieejamo apdraudējumu indikatoru un zināšanu kopu.

CERT.LV SOC pakalpojums neaprobežojas tikai ar tehnoloģiju, būtisku pievienoto vērtību sniedz cilvēki – SOC analītiķu komanda. Izmantojot īpašu programmnodrošinājumu un pieejamos datus, reaģēšanas un analītikas vienība savlaicīgi novērš kaitējumu – identificē, brīdina un aptur kiberincidentu vai apdraudējumu.

6.1. SOC darbības rezultāti

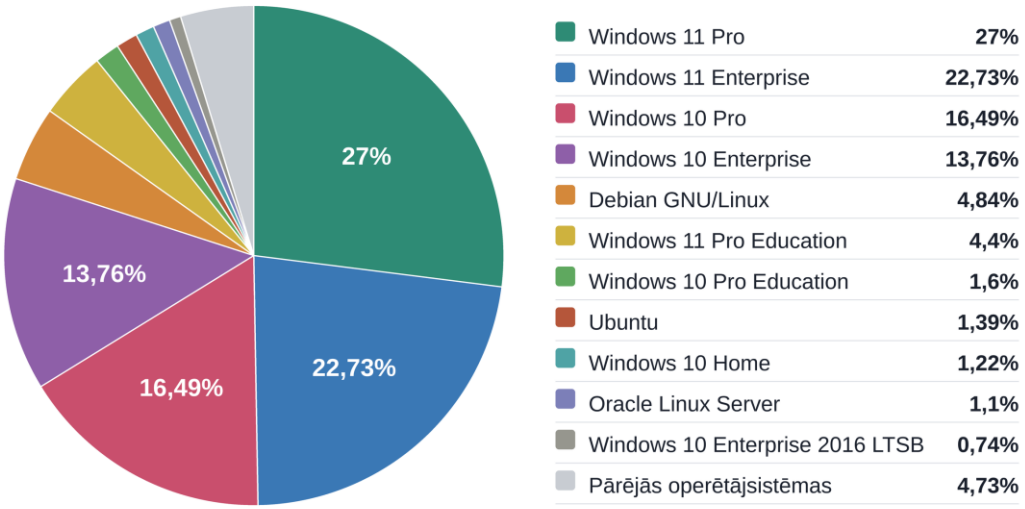
Dažādu nozaru organizācijas, kas nodrošina plašu pakalpojumu klāstu, ieviesušas un lieto SOC risinājumu. Vairāk pārstāvētas ir pašvaldības, ministrijas, veselības aprūpes iestādes un citas publiskā sektora iestādes.

Sadalījums ar organizāciju sektoriem, kas izmanto CERT.LV SOC (%)

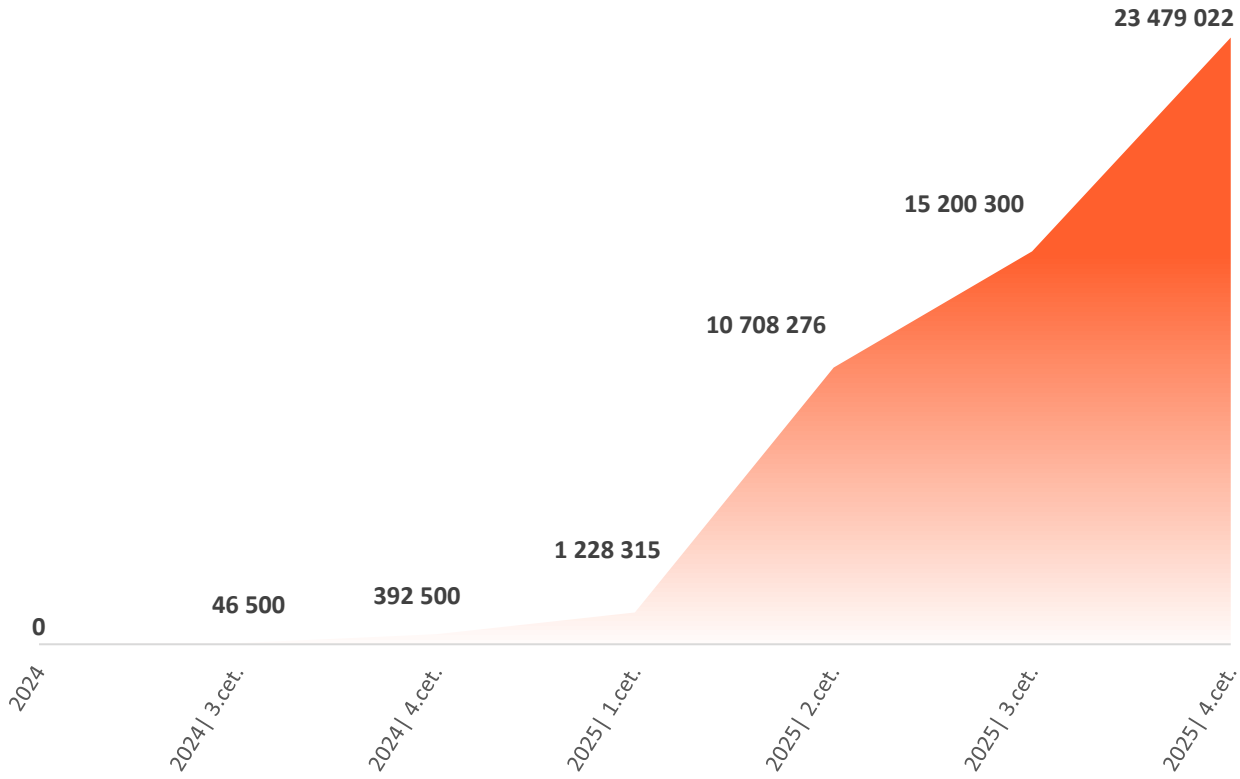


- **SOC pakalpojums ieviests** vai uzsākta tā ieviešana **55** klientiem.
- Pārskata periodā kopumā nodrošināta 41 534 iekārtu, tostarp serveru un darbstaciju, pārskatāmība.
- SOC pakalpojuma pārskata sanāksmes un **28 aktīvo SOC klientu jautājumu pārrunas 2025. gada laikā notika 47 reizes**. Sanāksmēs pārrunā konstatētos kiberincidentus, apdraudējumus, klienta izmantotās prakses un rekomendācijas kiberdrošības uzlabošanai.

Gala iekārtās visvairāk izmantota Microsoft Windows 11 Pro operētājsistēma



CERT.LV SOC reģistrēto drošības trauksmes ziņojumu dinamika (2024-2025)



Apstrādāto pieteikumu skaits: incidenti, trauksmes, viltus trauksmes, draudu atklāšana un novēršana

Kritisko trauksmju skaits	**72 K**
Augsta kritiskuma trauksmju skaits	1051 K
Manuāli izveidoto lietu skaits	1871
Viltus pozitīvo lietu skaits	1848
Kiberincidentu skaits	23

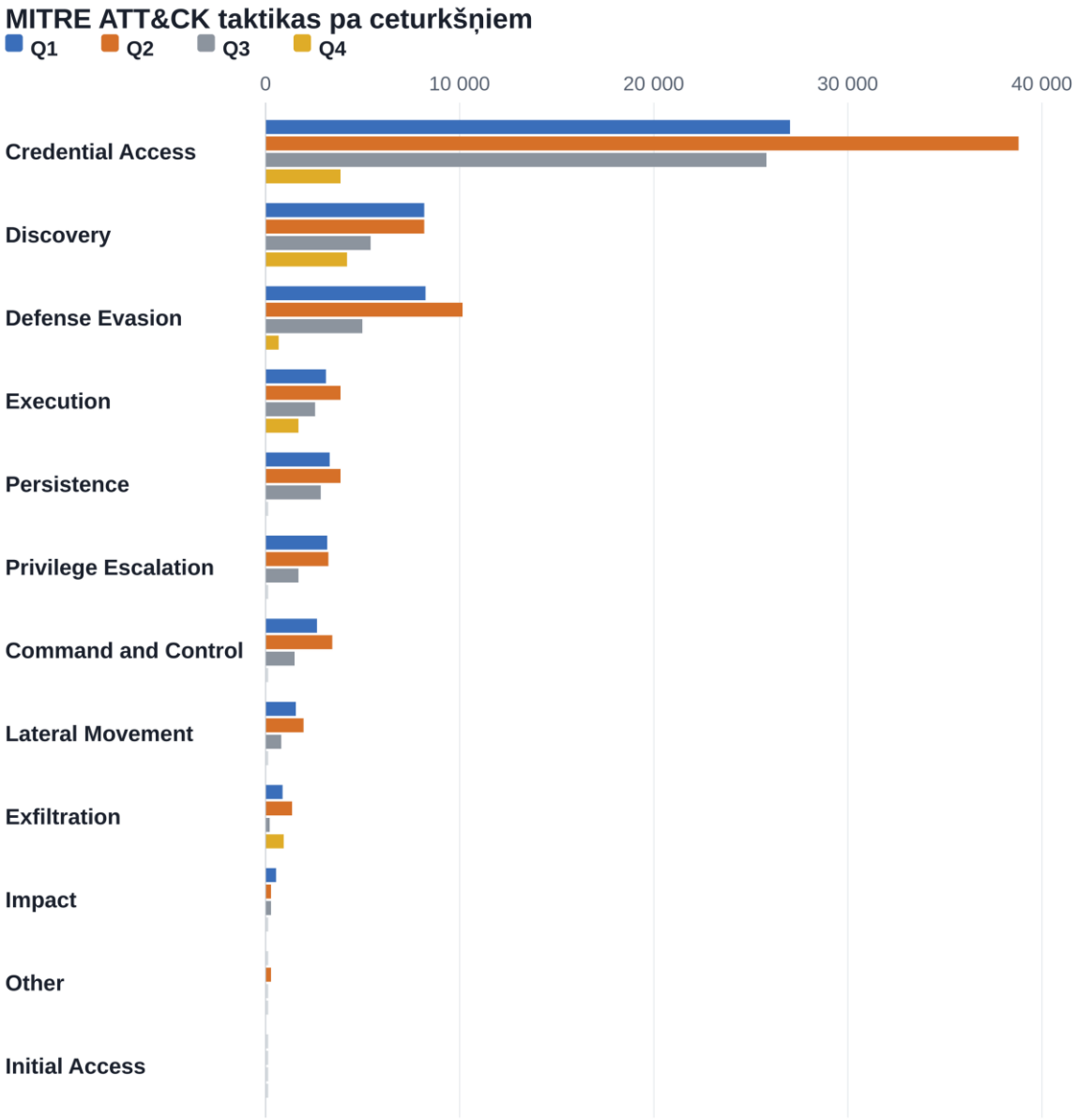
Lai efektīvi pamanītu kiberincidentus un apdraudējumus, nepieciešams mazināt trauksmju paziņojumu fona troksni.

SOC pakalpojumā novērots liels viltus trauksmju skaits, kuru galvenie iemesli ir šādi novērojumi klientu infrastruktūrā:

- Gala iekārtu konfigurācija nav standartizēta (viendabīga), trūkst pilnas inventarizācijas - iekārtas, programmatūra un cits inventārs (tehniskie pamatlīdzekļi).
  Ieteikums: izveidot pilnu inventarizāciju, infrastruktūru pārvaldīt centralizēti. Windows gadījumā visas iekārtas pievienot aktīvajai direktorijai;
- Nav atļauto programmatūru saraksts ar kontroles (t.sk. ierobežojošo) režīmu.
  Ieteikums: izveidot atļauto programmatūras sarakstu, ieviest kontroles risinājumu (SRP, AppLocker, WDAC, App Control for Business u.c.) jebkurai izpildītajai programmatūrai un failiem;
- Netiek kontrolēti pārlūku spraudņi.
  Ieteikums: centralizēti kontrolēt pārlūku spraudņu uzstādīšanu un izmantošanu;
- Nav viltus “captcha” aizsardzības.
  Ieteikums: atslēgt iespēju lietotājiem lietot “Win + R” komandu izpildīšanas rīku (lai nepieļautu komandu iekopēšanu);
- Netiek uzraudzīta USB zibatmiņu lietošana un no tām izpildīto failu kontrole.
  Ieteikums: pārvaldīt organizācijā lietotās zibatmiņas, izpildītos failus un ieslēgt antivīrusa pārbaudi, centrālo pārvaldību, atjaunināšanu;
- Publiskā tīmeklī eksponētas gala iekārtas ar izslēgtu lokālo ugunsmūri.
  Ieteikums: ieslēgt un atbilstoši konfigurēt lokālo ugunsmūri lietotāju gala iekārtās;
- Pārāk plaša dažādība tādu rīku lietošanā (t.sk. novecojušu versiju, iebūvēto jeb “LoL”), kurus parasti izmanto uzbrucēji, piemēram, “PSEXEC”, “WMI”, “VBS”, “PS1” u.c.
  Ieteikums: lietot viena tipa skriptus, piemēram, digitāli parakstītus “PowerShell”, grupu politikā atļaut tikai parakstīto izpildi;
- Nav ieslēgta žurnālierakstu veidošana, trūkst dokumentācijas un procedūru.
  Ieteikums: ieslēgt notikumu reģistrēšanu žurnālfailos, dokumentēt un uzraudzīt skriptu izmantošanu;
- Vairāku attālinātās piekļuves rīku (t.sk. novecojušas versijas) izmantošana lietotāju atbalstam: AnyDesk, Teamviewer u.c.
  Ieteikums: izmantot vienu risinājumu katram uzdevumam – komandrindai, darba virsmai, lietotāju atbalstam. Ieviest labas pārvaldības praksi – viena, nodalīta darbstacija ar atbilstošu lokālā ugunsmūra konfigurāciju.

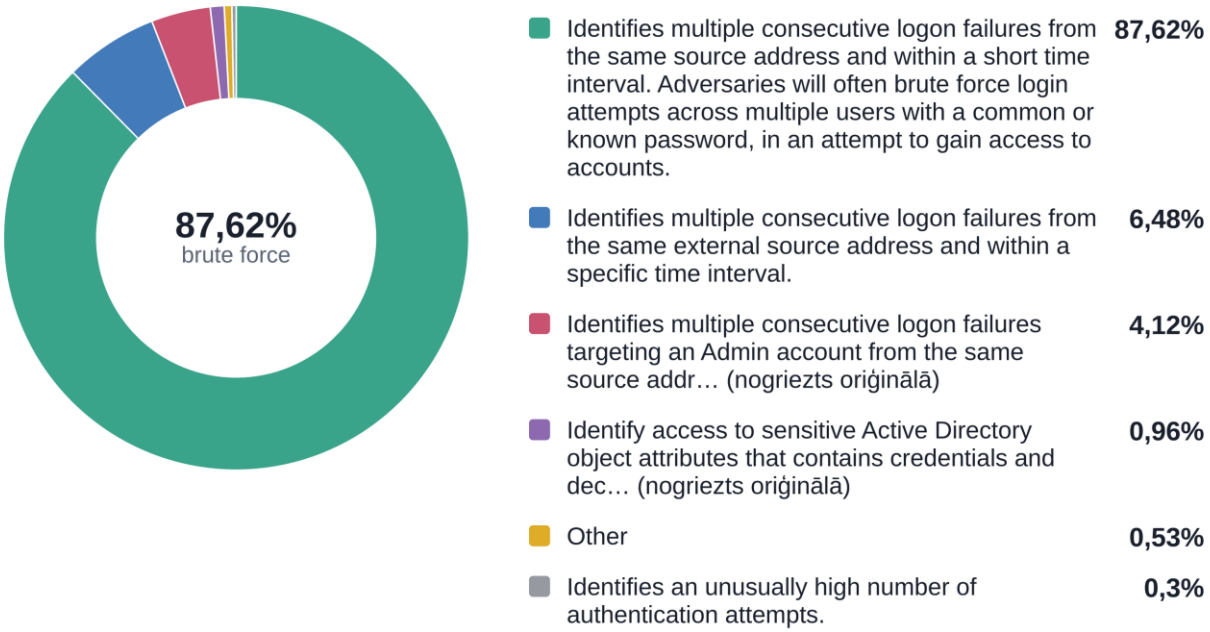
Notikumu statistika pēc MITRE ATT&CK ietvara

"Elastic" drošības platforma lieto MITRE ATT&CK ietvaru, lai trauksmju notikumi sniegtu kontekstu un izpratni par tā brīža uzbrukuma etapu, uzbrucēja aktivitātes virzienu un galamērķi.



Notikumos visbiežāk konstatētā taktika ir piekļuve akreditācijas datiem ("credential access"), kurai seko aizsardzības apiešana ("defense evasion") un tālāk atklāšana ("discovery"). Tas nozīmē, ka pārsvarā notikumi ir fiksēti uzreiz nākamajā etapā pēc sākotnējās piekļuves.

Akreditācijas datu piekļuves notikumu statistika



Aizsardzības apiešana jeb izvairīšanās no drošības kontroles (“defense evasion”) ir uzbrucēja taktika, kuras mērķis ir paslēpt ļaunprātīgas darbības un izvairīties no atklāšanas uzbrukuma laikā.

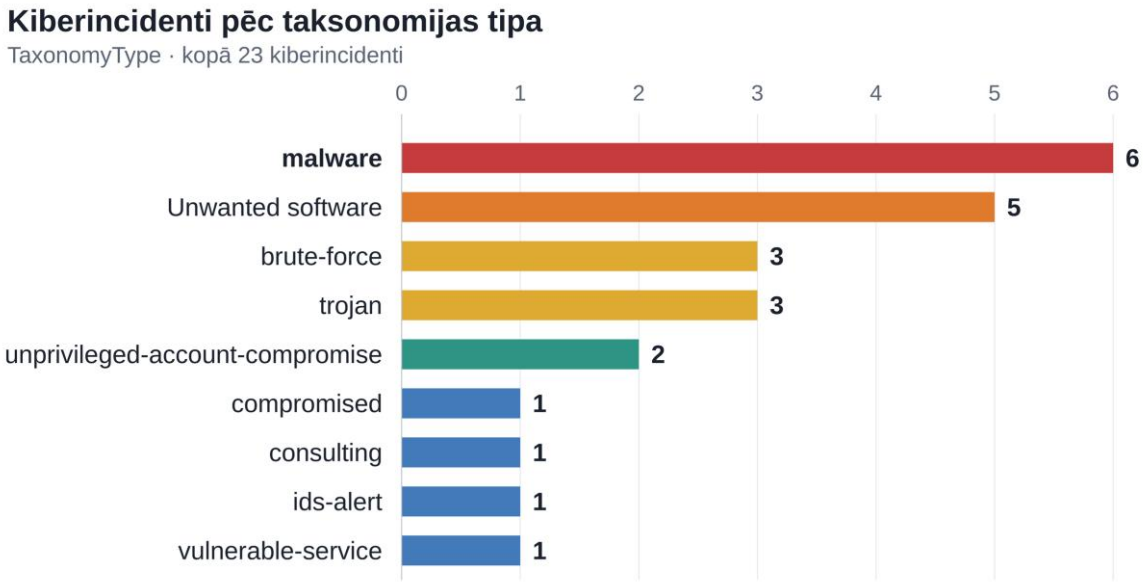
Populāri aizsardzības apiešanas paņēmieni ir drošības programmatūras atinstalēšana vai atspējošana, kā arī skriptu maskēšana un šifrēšana. Uzbrucēji ļaunprātīgi izmanto arī operētājsistēmas iebūvētus uzticamus izpildfailus (“LoL”) un procesus, lai slēptu un maskētu savu rīcību.

Atklāšana (“discovery”) ir metode, kuras mērķis ir iegūt zināšanas par sistēmām un iekšējo tīklu. Uzbrucējs šajā etapā izpēta tuvākos resursus ap viņa ieejas punktu, novēro vidi un izpēta infrastruktūru, lai izlemtu par izdevīgāku tālāko rīcību.

Tiek izzināts, kādas sistēmas varētu tikt pakļautas kontrolei, un kas no cietušā pieejamajiem resursiem dotu labumu uzbrucēja galvenajam mērķim. Praksē novērots, ka bieži tiek izmantoti iebūvētie operētājsistēmas rīki (“LoL”).

6.2. Konstatētie kiberincidenti

SOC reaģēšanas komandas konstatēto incidentu apkopojums un sadalījums pa kategorijām zemāk kolonnu diagrammā:



Aizsargājamu datu zagļu galvenais "kaujas" lauks ir tīmekļa pārlūkprogrammas, jo uzbrucēji iemanījušies veikli apiet tajos iebūvēto aizsardzību. Tāpēc gala iekārtu kompromitēšanas gadījumos vienmēr ieteikts mainīt visas lietotāja paroles.

Dominējošie sākotnējās piekļuves vektori

- Pārlūku spraudņi
- Viltus "CAPTCHA"
- No tīmekļa lejupielādēti un aktivizēti izpildāmie faili
- Izpildīti faili no zibatmiņām
- Pikšķērēšana
- Tīmeklī eksponētas iekārtas

Citi nozīmīgi kiberincidenti

Visi konstatētie incidenti notikuši Windows operētājsistēmās – gan darbstacijās, gan serveros. Apkopota tehniskā informācija un negadījumu konteksta ieteikumi.

- Iekārtā izpildīta "Elements Browser (Adware)" nevēlama reklāmu programmatūra. Ļaunatūra noņemta, veikta pretvīrusu skenēšana, ieteikts apsvērt programmatūras kontroles risinājumu (piemēram, AppLocker).
- Uzņēmumā pamanīta ļaunatūras "Lumma Stealer" aktivitāte, iekārta pārinstalēta. Kompromitēšana notika viltus mājaslapā ar "Fake Capcha" un "Win + R" izpildes logu. Ieteikts standarta lietotājam atslēgt "Win + R" izpildes rīku.
- Uzņēmumā nelegāls programmatūras aktivēšanas rīks "KMS Activator", iekārta pārinstalēta.
- Izmeklēts aizdomīgs uzdevuma pārvaldnieka "scheduled task" elements, kas izpilda failu "MPENTS~1.DLL". Ieteikts iekārtu pārinstalēt.

- Konstatēta rīka “Gsocket” aktivitāte. Iemesls - tīmeklī eksponēts serveris “moodle.*.lv” izmanto novecojušu “Moodle” versiju, atrastas vairākas tīmekļa čaulas. Ieteikts atjaunināt serveri un, ja iespējams, aizvērt publisku pieeju.
- Vairākiem klientiem nostrādāja SOC trauksme “Disabling Lsa Protection via Registry Modification”, novērota nedroša konfigurācija, ieteikts pārbaudīt LSA aizsardzību.
- Vairākiem klientiem novēroti mēģinājumi uzlauzt lietotāju kontus (*brute force*). Iemesls ir datoru pieslēgšana no korporatīvā uz publisko tīklu, kur notikusi iekārtas eksponēšana tīmeklī, jo nav iespējots lokāls ugunsmūris.
- Chrome pārlūkprogramma lejupielādē zemas reputācijas izpildāmo datni 8march.exe, Windows Defender bloķē, nenotiek tālāka aizdomīga rīcība. Ieteikts veikt papildu skenēšanu.
- lejupielādēta nevēlama programmatūra “downloader.exe”, kas uzstāda Yandex tīmekļa pārlūku un citu saistītu programmatūru. Dators pārinstalēts.
- Novērota izpildāmu failu un ļaunatūras izpilde no zibatmiņas, ieteikums kontrolēt zibatmiņas, izmantot tikai zināmās.
- Gandrīz visiem klientiem konstatēta nevēlamu (t.sk. ar darba pienākumiem nesaistītu) programmatūru nekontrolēta izpilde, ieteikums ieviest atļauto programmatūras sarakstu un kontroles risinājumus (piemēram, AppLocker).
- Vairākās iekārtās nevēlama programmatūra “Multiprotect_Console_License_Manage, tva_LAPS_UI”.
- Nelegāls programmatūras aktivēšanas rīks “AutoKMS”, ieteikts iekārtu pārinstalēt, ieviest AppLocker.
- Krievijā izstrādātā BitTorent aģentu “MediaGet” izmantošana, ieteikts programmatūru dzēst un izglītot lietotāju par tās kaitīgumu.
- Ļaunatūra “productkey”, no tīmekļa lejupielādētas un izpildītas dažādas datorspēles, jāievieš programmatūras kontrole.
- Inficēta vietne ar viltus “capcha”, kompromitēšana ar datu zadzēja ļaunatūru, kas apturēta, taču ieteikts uz laiku bloķēt visus iesaistītā lietotāja kontus un mainīt paroles.
- Konstatētas ļaunatūras atstātas pēdas uzdevumu pārvaldniekā, dators pārinstalēts.
- No zibatmiņas izpildīts auto diagnostikas rīks, jāievieš programmatūras kontrole.
- Nevēlama programmatūra “PatchSetup_A19.exe”, jāievieš programmatūras kontrole.
- Konstatēta ļaunatūra “Windows.Trojan.Guloader”, atverot kaitīgu pielikumu no e-pasta.
- Inficēta vietne ar viltus *capcha*.
- Ielaušanās mēģinājumi ar paroļu pārlasi (*brute force*), netīša datora eksponēšana tīmeklī bez lokāla ugunsmūra, jānokonfigurē gala iekārtas ugunsmūris.

Kompromitēšanas indikatori (IOC):

- #ioc s5.nybh[.]ru
- #ioc 37.wugh[.]ru
- #ioc zkg[.]lv
- #ioc https://elevatedeverydayeats[.]com
- #ioc: files.catbox.moe/cqyd3f[.]aaf
- #sha256:f138e29a75d6371cdaf7516ae34a2cdec8c098f6b72e2ed220dceb5cda3ee75e

- #ioc 107.174.33.15
- #ioc https: //greasyfork.org/en/scripts/7226-tw-gold-jobs-finder-more-languages

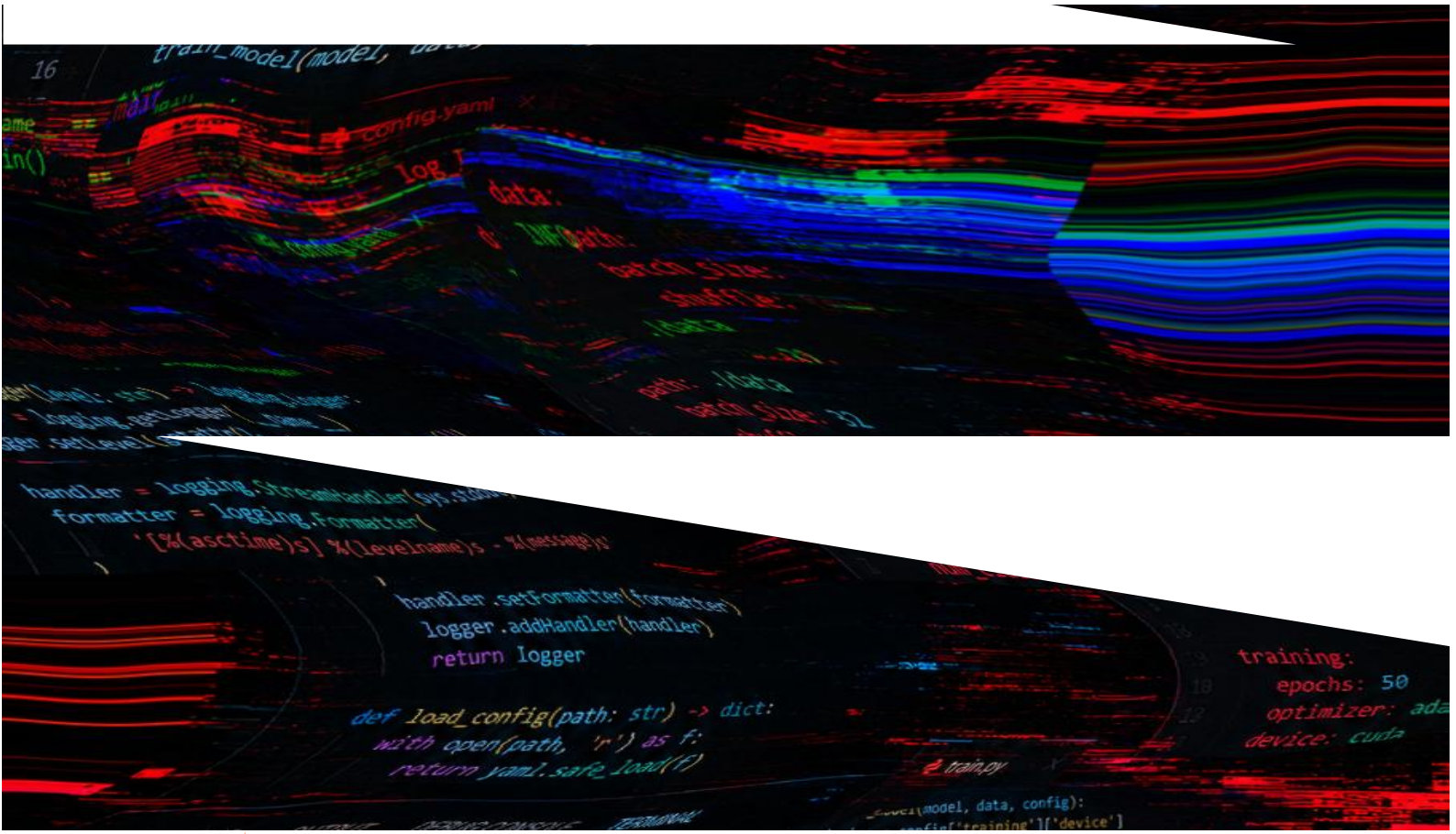
Kopsavilkums

CERT.LV SOC pakalpojums ir klienta infrastruktūras sargs, rūpēšanās par drošību, labām pārvaldības praksēm un aizsargāšana no iespējamiem uzbrukumiem.

Klienta datu drošībai un kiberincidentu un apdraudējuma skaita samazināšanai CERT.LV konsultē par labas infrastruktūras pārvaldības praksi un ieviešanu.

Klienta sākotnējais uzdevums ir pilna savu iekārtu un programmatūras inventarizācija, tālāk pilnībā ieviests Drošības operāciju centra (SOC) pakalpojums, visbeidzot – atrasto trūkumu novēršana. Rezultātā tiek būtiski paaugstināts drošības līmenis un mazinātas uzbrucēja iespējas sasniegt savu mērķi.

Infrastruktūras pārvaldībā ļoti svarīgi nepieļaut lietotājiem izpildīt neatļautu programmatūru (t.sk. no USB zibatmiņām), patvaļīgi instalēt pārlūku spraudņus, izpildīt dažādas konsoles komandas un eksponēt gala iekārtas tīmeklī bez lokāla ugunsmūra.



7. OSINT rezultāti un ieteikumi

OSINT (Open Source Intelligence) jeb atvērto avotu izlūkošanas procesā tika konstatēts, ka 2025. gada laikā turpinājās ļaunprātīgas kiberdarbības, kas saistāmas ar trešo valstu valdību atbalstītiem uzbrucēju grupējumiem. CERT.LV OSINT/CTI mērķis ir sniegt operacionālu informāciju un aizsardzībai nepieciešamās rekomendācijas, lai veiktu preventīvus pasākumus, kuri pēc iespējas vairāk apturētu potenciālus kiberincidentus.

Ņemot vērā Krievijas valdošā režīma stratēģiskās intereses, pārskata gadā konstatētie ar Krieviju saistītu vai tās atbalstītu grupējumu kiberuzbrukumi pret Rietumvalstīm, tostarp Latviju, bija prognozējami.

Galvenokārt tika konstatēti ideoloģiski motivētu hakeru jeb haktīvistu organizēti uzbrukumi, tostarp DDoS uzbrukumi un citas operācijas starptautiskās informācijas telpas ietekmēšanai. Vienlaikus novēroti arī mērķēti uzbrukumi Latvijas valsts institūcijām ar nolūku kompromitēt nacionāli nozīmīgas sistēmas, iegūt piekļuvi tām un saglabāt ilgtermiņa klātbūtni. Detalizētāki piemēri aprakstīti sadaļā "APT uzbrukumi".

CERT.LV jau iepriekš ir identificējusi uzņēmuma "Stark Industries Solutions Ltd." (tagad "PQ Hosting Plus S.R.L") infrastruktūru, kas ir Krievijas valdības atbalstīts čaulas IT pakalpojumu sniedzējs. Iepriekš bieži novērots, ka tās pakalpojumi izmantoti haktīvistu aktivitātēs, taču vairāki incidenti pierāda, ka Krievijas valdības atbalstīti kibernoziedznieku grupējumi izmanto Eiropas reģiona IT pakalpojuma sniedzēju pakalpojumus savu uzbrukumu īstenošanai.

Baltijas reģionā arī Ķīnas Tautas Republika (ĶTR) turpina izvērst aktivitātes savu interešu īstenošanā. Tās piecu gadu plāna mērķi zinātniskajā izpētē un tehnoloģiju attīstībā atbilst novērotiem uzbrukumiem Latvijā. Lai gan akadēmiskā nozare joprojām ir viens no galvenajiem mērķiem ĶTR valdības atbalstītiem uzbrucēju grupējumiem, ir novēroti mēģinājumi uzlauzt Latvijas valstī nozīmīgas sistēmas (piemērs: ievainojamību apkopojums CVE-2025-53770). Vairāki kiberdrošības uzņēmumi, piemēram, Microsoft, PaloAlto, identificēja tos pašus indikatorus arī Latvijā, un ar lielu iespējamību tos sasaista (atributē) ar ĶTR izcelsmes uzbrucēju grupējumiem "Linen Typhoon", "Volt Typhoon" un "Storm-2603"[3].

Ķīnas reģiona aktivitātes fokuss arī iepriekš konstatēts tieši uz sabiedrības datu drošību. Konkrēti, ir programmatūras pakalpojumus sniedzošs uzņēmums, kas 2024. gadā cieta incidentā, kura rezultātā notika vēsturē lielākā datu noplūde Latvijā. Nepareizu datu platformas servera "Elastic" konfigurāciju un nejaušu eksponēšanu publiskā tīmeklī izmantoja kāds uzbrucēju grupējums, kas automatizēti izguva (eksfiltrēja) lielu datu kopu. Tā saturēja sabiedrības datus – vārdus, uzvārdus, adreses, e-pasta adreses un citu informāciju. Incidenta izmeklēšanā analizēja serveri, no kura uzbrucēji veica ielaušanās darbības uzņēmuma infrastruktūrā. Tika identificētas pazīmes, piemēram, Šanhajas reģionālie iestatījumi un vairāku programmatūru komentāri Ķīniešu valodā, kas ar vidēju varbūtību apliecina uzbrucēja aktivitātes ĶTR interesēs.

Abu valstu atbalstītie uzbrucēju grupējumi izmanto dažādu taktiku, tehniku un procedūras (TTP), lai īstenotu savus galvenos mērķus. Ļaunatūra kā pakalpojums ("MaaS"), it īpaši datu zagšanā, ir plaši izmantota tehnika, lai iegūtu potenciālo upuru autentificēšanās datus sākotnējai piekļuvei. Noziedzīgu darbību piesedzošus ("bulletproof hosting") IT pakalpojumu uzņēmumus izmanto, lai veiktu izlūkošanu pirms DDoS un citiem kiberuzbrukumiem pret mērķiem Latvijā. Turklāt Latvijas reģionā arī atrasti IT čaulas uzņēmumi, kas sniedz

[3] Atsauce: https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities

nelegālu operāciju pakalpojumus Krievijas un ĶTR valstu atbalstītiem grupējumiem savās kiberoperācijās (detalizētāki piemēri - sadaļā "APT Uzbrukumi"). Iesaistītais konkrētais serveris pildīja komandkontroles ("C2") servera funkciju ļaunatūrai "KEYPLUG", kura, ļoti iespējams, saistīta ar ĶTR izcelsmes uzbrucēju grupējumu APT41 jeb "Wicked Panda"[4].

7.1. Čaulu IT pakalpojumu sniedzēji

CERT.LV pirms vairākiem gadiem identificēja Krievijas valdības atbalstītu čaulas IT pakalpojuma uzņēmumu "Stark Industries Solutions Ltd". Pakalpojuma sniedzējs iepriekš bija plaši novērots DDoS uzbrukumos ne tikai pret mērķiem Latvijā, bet arī Eiropas Savienībā. Eiropas Savienības sankcijas 2025. gada maijā pret šo pakalpojuma sniedzēju un tās īpašniekiem rezultējās ar šī uzņēmuma sadalīšanos vairākās citās čaulu kompānijās. Ar lielu pārliecību var uzskatīt, ka "Stark Industries Solutions Ltd." turpina sniegt pakalpojumus Krievijas valdības atbalstītām kiberoperācijām no citām kompānijām, tajā skaitā:

- "PQ Hosting Plus S.R.L" (AS44477), bijušais "Stark Industries Solutions Ltd.";
- "WorkTitans B.V." (AS213999 / AS209847);
- "THE.Hosting" (AS209847);
- "UFO Hosting" (AS33993).

CERT.LV iesaka uzskatīt augstāk minētos autonomo sistēmu ("AS") numurus par kaitnieciskiem un veikt nepieciešamās izmaiņas ugunsmūra konfigurācijās, lai bloķētu visu komunikāciju no attiecīgajiem IP adrešu apgabaliem.

IP adreses, kas identificētas kiberoperācijās pret Latvijas reģiona IS:

IP	AS	Komentārs	Mēnesis
94.131.104.27	AS44477	Uzbrucēja IP	Februāris
136.0.185.54	AS44477	Uzbrucēja IP	Februāris
136.0.181.164	AS44477	Uzbrucēja IP	Februāris
77.91.102.162	AS44477	Iesaistīta incidentā	Februāris
45.142.213.182	AS44477	Ielaušanās mēģinājumi	Marts
45.12.129.78	AS44477	NodeStealer informācijas zadzēja C2	Aprīlis
94.131.104.221	AS44477	Skenēšanas aktivitāte	Jūnijs
103.231.73.45	AS44477	Ielaušanās mēģinājumi	Jūlijs
103.231.73.251	AS44477	Ielaušanās mēģinājumi	Jūlijs
45.142.215.124	AS44477	Ielaušanās mēģinājumi	Jūlijs
103.231.73.114	AS44477	Ielaušanās mēģinājumi	Jūlijs
45.142.213.94	AS44477	Ielaušanās mēģinājumi	Jūlijs

[4] Atsauce: https://hunt.io/malware-families/keyplug.

Krievijā bāzēts noziedzīgu darbību piesedzošs (“bulletproof hosting, BPH”) pakalpojuma sniedzējs “Aeza Group” piedāvā uzbrucējiem un draudu grupējumiem nepieciešamo infrastruktūru, kas veic šifrējošā vīrusa uzbrukumus vai izplata datu zadzēja ļaunatūru. Šīs kompānijas infrastruktūru izmanto tādi datu zagļi kā “Meduza”, “Lumma”, “Redline”. Aizdomās turēts šifrēšanas vīruss “BianLian”.

Uzņēmumam “Aeza Group” 100% apmērā pieder “Limited Liability Company”.

“Limited Liability Company” sastāvā ietilpstošās organizācijas:

- Aeza Group LLC (RU) (AS216246);
- Aeza International Ltd. (UK branch) (AS210644);
- Aeza Logistic LLC (Russia-based subsidiary);
- Cloud Solutions LLC (Russia-based subsidiary) (AS214231).

2025. gada novembrī tieši puse no “Aeza International” IP adrešu prefiksiem tiek maršrutēti caur uzņēmumu “Aurologic GmbH” (AS30823), kas pierāda tehnisko nepieciešamību pēc vācu uzņēmuma pakalpojumiem augšupielādes plūsmas nodrošināšanai.

Daļa ASV resursu pārlikti uz “Smart Digital Ideas DOO” (AS215829) 2025. gada jūlija sankciju dēļ.

Laika posmā no 2024. gada jūlija līdz 2025. gada jūlijam 7.5% no visiem identificētajiem pirmā līmeņa komandkontroles (“Tier 1 C2”) serveriem bija saistīti ar “Aeza International Ltd”. Daļēji iesaistīts arī haktīvistu grupējums “DDoSia”.

Visus iepriekš uzskaitītos autonomo sistēmu (AS) apgabalus var uzskatīt par kaitnieciskiem, tāpēc CERT.LV iesaka veikt nepieciešamās izmaiņas ugunsmūru konfigurācijās, lai bloķētu ienākošo komunikāciju plūsmu no visiem iesaistītajiem IP adrešu apgabaliem.

7.2. Informācijas zadzēji

Datu zadzēji jeb zagšanas ļaunatūra ilgu laiku ir būtiska mākoņskaitļošanas pakalpojuma MaaS (“Malware as a service”) sastāvdaļa. Lai arī trešo valstu valdību atbalstīti noziedzīgie grupējumi ir attīstījuši savus tehniskos uzbrukumu rīkus, ir pierādījumi, ka sākotnējai piekļuvei izmantoti datu zagšanas risinājumi. Ļoti iespējams, ka sākotnējo pieeju un datu zagšanu veikuši dažādi grupējumi, starp kuriem noticis pagrīdes informācijas tirdzniecības darījums.

Uzbrukumos Latvijas reģiona cietušajiem sākotnējās pieejas etapā visbiežāk izmanto tādus pakalpojumus kā tīmekļa pārlūka e-pasts, iekšējā programmu koda “git” platforma, ārējā tīmeklī eksponētas datubāzes, neieslēgta divu faktoru autentifikācija. Privātās iekārtas – bez biznesa līmeņa drošības aprīkojuma un centrālas pārvaldības – joprojām tiek izmantotas darba vajadzībām. Tas rada lielus draudus, jo kompromitēt lietotāja privāto iekārtu ar informācijas zadzēju ir vienkāršāk, attiecīgi, uzbrucējam vieglāk piekļūt datora autentificēšanās datiem, iegūstot sākotnējo piekļuvi pie organizācijas vai uzņēmuma.

Jau 2024. gadā bija informācija, ka Krievijas izcelsmes APT grupējums izmanto informācijas zadzēju "Rhadamanthys"[5] . Jaunākie kiberizlūkošanas rezultāti ar lielu iespējamību apliecina, ka Krievijas valdības atbalstīto grupējumu arsenālā ir arī informācijas zadzēju ļaunatūras "Redline" un "Lumma".

Microsoft kiberizlūkošanas nodaļas izpēte parāda, ka starptautisko mērķu vidū otrajā vietā ir akadēmiskā nozare[6].

Izmeklēšanas rezultāti (skatīt zemāk tabulā) atklāj, ka Latvijas mācību iestādēs ir plaši izmantoti datu zadzēju paveidi "StealC" un "Vidar".

Identificētas 47 ārpus Latvijas IP adreses, kas izmantotas zagto datu nopludināšanā (eksfiltrēšanā) komandkontroles "C2" serveriem:

IP	Valsts	AS	Datu zadzējs
101.2.180.53	LK	AS18001 Dialog Axiata PLC.	Redline
103.114.64.176	IN	AS133661 Netplus Broadband Services Private Limited	Redline
109.221.178.196	FR	AS3215 Orange	Redline
117.211.143.154	IN	AS9829 National Internet Backbone	Redline
182.183.24.184	PK	AS17557 Pakistan Telecommunication Company Limited	Redline
83.185.36.11	SE	AS1257 Tele2 SWIPnet	Redline
89.211.144.32	QA	AS8781 Ooredoo Q.S.C.	Redline
88.97.224.206	GB	AS212655 YouFibre Limited	Redline
45.150.2.155	NL	AS35224 PLINQ BV	Redline
5.158.33.30	PT	AS12353 Vodafone Portugal - Communicacoes Pessoais S.A.	Redline
212.62.97.65	SA	AS43766 Mobile Telecommunication Company Saudi Arabia Joint-Stock company	Redline
184.22.149.42	TH	AS133481 AIS Fibre	Lumma
186.78.146.233	CL	AS7418 TELEFONICA CHILE S.A.	Lumma
212.216.162.22	IT	AS3269 TIM	Lumma
217.233.70.235	DE	AS3320 Deutsche Telekom AG	Lumma
46.11.227.94	MT	AS15735 GO p.l.c.	Lumma
72.143.239.98	CA	AS812 ROGERS-COMMUNICATIONS	Lumma
77.219.81.167	SE	AS1257 Tele2 SWIPnet	Lumma
77.38.35.6	SI	AS3212 Telemach Slovenija d.o.o.	Lumma
80.216.144.197	SE	AS1257 Tele2 SWIPnet	Lumma
89.18.201.238	FR	AS136787 PacketHub S.A.	Lumma
90.130.216.37	SE	AS1257 Tele2 SWIPnet	Lumma
104.28.216.221	PK	AS13335 CLOUDFLARENET	Lumma

[5] Atsauce: https://flashpoint.io/blog/russian-apt-groups-cyber-threats
[6] Atsauce: https://blogs.microsoft.com/on-the-issues/2024/11/12/expanding-accountguard-to-counter-growing-cyber-threats-in-africa

106.51.165.180	IN	AS24309 Atria Convergence Technologies Pvt. Broadband ISP INDIA	Lumma
113.168.192.128	VN	AS45899 VNPT Corp	Lumma
116.91.209.137	PH	AS14593 SPACEX-STARLINK	Lumma
145.90.158.99	NL	AS1103 SURF B.V.	Lumma
84.214.178.205	NO	AS25400 Telia Norge AS	StealC
45.84.139.60	DE	AS62240 Clouvider Limited	StealC
94.31.117.98	DE	AS60294 Deutsche Glasfaser Wholesale GmbH	StealC
178.165.204.48	AT	AS25255 Hutchison Drei Austria GmbH	StealC
89.46.10.193	DE	AS207137 PacketHub S.A.	Vidar
102.115.60.24	MU	AS23889 MauritiusTelecom	Vidar
102.117.103.57	MU	AS23889 MauritiusTelecom	Vidar
102.117.113.237	MU	AS23889 MauritiusTelecom	Vidar
102.117.202.212	MU	AS23889 MauritiusTelecom	Vidar
102.117.253.160	MU	AS23889 MauritiusTelecom	Vidar
102.117.29.212	MU	AS23889 MauritiusTelecom	Vidar
102.117.34.215	MU	AS23889 MauritiusTelecom	Vidar
102.91.4.122	NG	AS29465 MTN NIGERIA Communication limited	Vidar
202.142.118.27	IN	AS132115 INDINET SERVICE PRIVATE LIMITED	Vidar
138.199.7.239	NL	AS212238 Datacamp Limited	Acreed
212.104.229.247	LK	AS45356 Mobitel Pvt Ltd	Acreed
212.104.231.103	LK	AS45356 Mobitel Pvt Ltd	Acreed
217.210.53.93	SE	AS3301 Telia Company AB	Acreed
2.38.151.3	IT	AS30722 Vodafone Italia S.p.A.	Acreed
188.81.39.7	PT	AS3243 Servicos De Comunicacoes E Multimedia S.A.	Rhadamanthys

Lielākajai daļai iepriekš aprakstīto datu zadzēju aizsākumu pēdas meklējamas Krievijā, vairums pārdotas tumšā tīmekļa (krievu valodā) tirgotavās. Ir arī izņēmumi, piemēram, zagšanas ļaunatūras “Atlantida” un “AtomicMac” vairāki parametri liecina par Ķīnas reģiona izcelsmi. Savukārt, “Acreed”, “AZORult clone” un “Rhadamanthys” nevar atrast tādus parametrus, kas liecinātu par saistību ar Krieviju vai Ķīnu.

Informācijas zagšanas ļaunatūra tiek izplatīta ne tikai ar pikšķerēšanas uzbrukumiem, bet arī integrēta pirātiskā programmatūrā, kas lejupielādēta ar vienlīmeņa koplietošanas platformas “torrent” starpniecību. Tās biežākās lejupielādēšanas mapes ir “C:\Users**\AppData\Local\Temp\” un “C:\Users**\AppData\Roaming\”, bet var atrasties arī citos diskos un vietās, kā “C:\Users**\Downloads\”, “C:\Users**\Desktop\”, “E:\”, “F:\”.

Ieteikums: CERT.LV aicina visas organizācijas uzstādīt divu faktoru autentifikāciju visām IT sistēmām, kur vien tas ir iespējams. Obligāti ieslēgt autentificēšanās mēģinājumu reģistrēšanu žurnālfailos un ieviest aizdomīgu aktivitāšu identificēšanas mehānismu.

7.3. Aktivitātes enerģijas un ūdens apgādes jomā

Nozīmīgs notikums 2025. gadā Baltijas valstīs bija pievienošanās Eiropas enerģijas infrastruktūrai, atslēdzoties no Krievijas un Baltkrievijas elektrības apgādes tīkla "BRELL". Vairāki Ukrainas piemēri rāda, ka enerģijas infrastruktūra ir būtisks kiberuzbrukumu mērķis gan aktīvas karadarbības laikā, gan pirms tās. Īstenoti uzbrukumi enerģijas apgādes infrastruktūrai var radīt katastrofālas sekas valsts sabiedrībai. Tāpēc CERT.LV veica izpēti par 2025. gadā izpildītajiem kiberuzbrukumiem starptautiskajā enerģijas infrastruktūrā, lai definētu galvenos kritērijus uzbrukumu novēršanai un identificētu nepieciešamos pasākumus preventīvās aizsardzības nodrošināšanai.

2025. gada aprīlī ĶTR valdības atbalstīti APT grupējumi "UNC5221", "UNC5174" un "CL-STA-0048" veica uzbrukumus pret programmatūru "SAP NetWeaver Visual Composer" mērķiem Lielbritānijā, ASV un Saūda Arābijā, izmantojot ievainojamību CVE-2025-31324 attālinātā koda izpildei. Kiberdrošības pētnieki no uzņēmumiem "Mandiant" un "PaloAlto" šos grupējumus saista ar ĶTR Iekšējās drošības ministriju vai ar privātajiem uzņēmumiem tās pakļautībā. Kaut arī šo uzbrucēju aktivitāte Latvijā nav identificēta, tomēr tas parāda nepieciešamību zināt par ārējā tīklā eksponētām iekārtām un pakalpojumiem un nodrošināt laicīgu programmatūras atjaunināšanu.

Kiberaizsardzības uzņēmums "BitDefender" ir ziņojis par jaunu augsta līmeņa uzbrucēju grupējumu "Curly COMrades", kura darbības liecina par iespējamo saistību ar Krievijas valdību un tās stratēģiskajām interesēm. Lai arī uzbrucējs lielākoties ir veicis uzbrukumus pret valsts iestādēm Gruzijā, mērķu sarakstā ir arī Moldovas enerģijas apgādes kompānija. Uzbrucēja galvenais mērķis ir iegūt ilgstošu piekļuvi korporatīvā vidē, veikt autentifikācijas un citu iekšējās informācijas noplūdi ("eksfiltrēšanu"). Taktikas mērķa īstenošanai ir dažādas, piemēram, NTDS un LSASS eksfiltrēšana, savukārt, attālināto piekļuvi un pastāvīgo pieeju īsteno ar vairākiem starpniekserveriem ("proxy", "Resocks", "Stunnel", "SOCKS5", "CurlCat", "RuRat" u.c.). Uzbrucēja aktivitāte Latvijā nav manīta, tomēr vairāki no izmantotajiem rīkiem ir identificēti CERT.LV analizētajos incidentos. **Preventīvs aizsardzības pasākums ir programmatūras kontroles risinājums, piemēram, "AppLocker".**

Šifrējošā vīrusa uzbrukumā 2025. gada 25. oktobrī cieta Zviedrijas elektroapgādes uzņēmums "Svenska Kraftnät", kuru īstenoja finansiāli motivētais uzbrucēju grupējums "Everest Ransomware Group". Enerģijas apgādes uzņēmumi ir iekārojams mērķis, jo strādā ar ievērojamiem naudas līdzekļiem. Uzbrucēja aktivitāte Latvijā nav manīta.

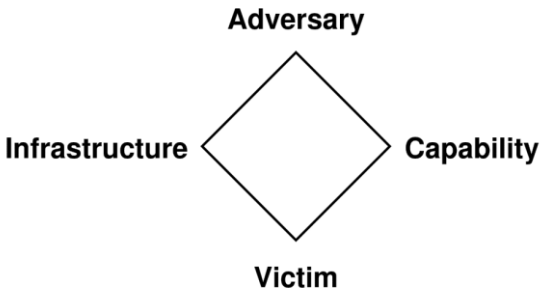
Tehnoloģiju uzņēmums "Forescout" veica izpēti par Krievijas haktīvistu grupējuma "TwoNet" uzbrukumu metodoloģiju pret operacionālo tehnoloģiju (OT) vidi. OT ir ierīces vai sistēma, kas uzrauga vai pārvalda ražošanas vai infrastruktūras tehnoloģiskos procesus. "Forescout" izveidoja "medus podu" jeb speciālu mānekļa sistēmu, kas imitē īstu serveri, šajā gadījumā fiktīva ūdens apgādes apakšstacija. Ar noklusējuma autentificēšanos datiem uzbrucējs piekļuva pie iekārtas un veica datubāzes izpēti. Tad izveidoja jaunu lietotāju, ar kuru pieteicās sistēmā un, izmantojot ievainojamību CVE-2021-26829, veica iekārtu degradējošas izmaiņas konfigurācijā. Arī šis uzbrucēju grupējums Latvijā nav manīts. Gada garumā CERT.LV ir identificējusi vairākas gan privātas, gan uzņēmumu OT iekārtas, kas eksponētas publiskā tīmeklī, tādējādi radot milzīgu risku. Uzlauztu privātu OT iekārtu gadījumā tas var būt cilvēku veselības vai dzīvības risks, piemēram, gāzes apkures katla atslēgšana. Uzņēmuma gadījumos OT iekārtas pārņemšana vai bojāšana var izraisīt biznesa apturēšanu. Diemžēl arvien vairāk iekārtu tiek eksponētas publiskā tīmeklī – videokameras, apkures katli un citas ar iebūvētu pārvaldības funkcionalitāti. **Noklusējuma autentificēšanos datu atstāšana ir viens no visbiežāk sastopamiem sākotnējas piekļuves veidiem, vienmēr jānomaina rūpnīcas iestatītā pārvaldības parole.**

Haktīvistu aktivitātes Latvijas reģionā nav mazinājušās, piekļuves aizlieguma (DDoS) uzbrukumi 2025. gadā turpinājās pret vairākām timekļa vietnēm. Bieži šie uzbrukumi ir kā reakcija uz publiskām ziņām vai intervijām, kas apliecina Latvijas atbalstu Ukrainai. Vairākas reizes 2025. gadā manītas haktīvistu ziņas par kādu kompromitētu Latvijas resursu, no kura iegūta konfidenciāla informācija. CERT.LV izmeklējis katru šādu gadījumu un konstatējis, ka visās reizēs haktīvisti izplatījuši nepatiesu informāciju. Paredzams, ka arī turpmāk turpinās izplatīties maldinoši paziņojumi par it kā uzlauztām sistēmām un datu noplūdēm gadījumos, kad haktīvistiem izdodas iegūt publiski eksponētu autentifikācijas paneļu ekrāna attēlus.

Ieteikums: CERT.LV rekomendē pārliecināties, ka publiskajā tīmeklī netiek eksponētas tādas sistēmas, kurām nav nepieciešama ārējā interneta pieeja. Nepieciešamības gadījumā censties to nodrošināt ar VPN risinājumu. Tādā veidā samazināsies iespējamais sākotnējās piekļuves vektori. Papildus jāpārliecinās, ka visa programmatūra tiek laicīgi atjaunināta, īpaši publiskā tīmeklī pieejamām iekārtām, kā arī jābūt iespējotai divu faktoru autentifikācijai.

7.4. Citu valstu atbalstītie kiberuzbrukumi

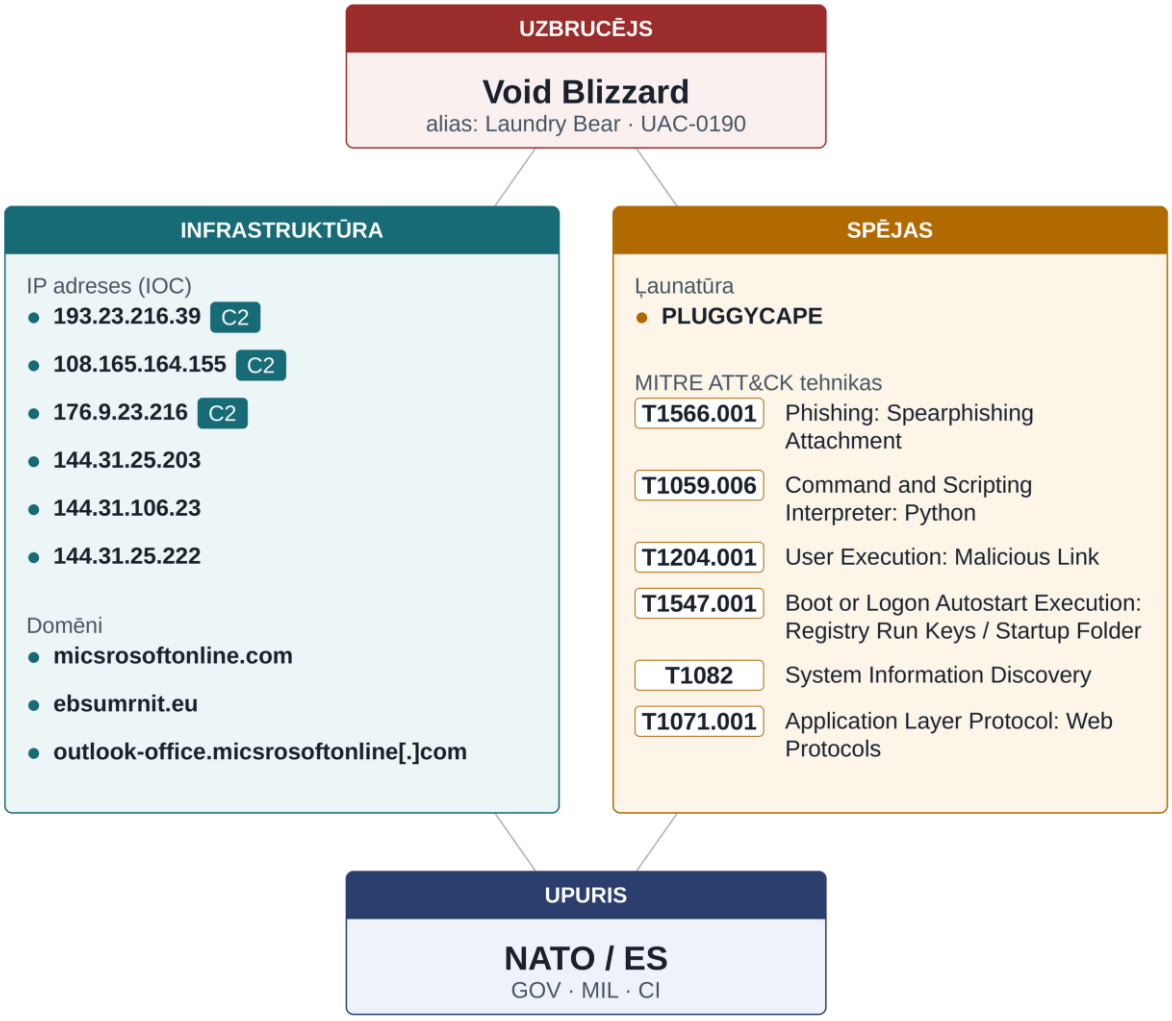
Kiberuzbrukumi Latvijas reģiona objektiem vai citas noziedzīgo grupējumu aktivitātes tiek kategorizētas, izmantojot kiberizlūkošanā pieņemto "Dimanta" modeli. Tas attēlo uzbrucēju spējas, izmantoto infrastruktūru un mērķus:



Pastāvīgo draudu grupējums APT (Advanced Persistent Threat) "Void Blizzard" (dēvēts arī par "Laundry Bear" vai "UAC-0190") ar lielu iespēju ir Krievijas valdības atbalstīts, tas darbojas vismaz kopš 2024. gada aprīļa.

Plaša mēroga kiberizlūkošanas kampaņas veiktas pret Ukrainas bruņotajiem spēkiem un valsts iestādēm. Grupējums izmantoja saziņas lietotnes "Singal" un "WhatsApp", lai piegādātu "PLUGGYAPE" un citu ļaunatūru.

Notiek aktivitātes arī pret NATO un ES valstu aizsardzības, transporta, veselības sektoriem, kā arī žurnālistiem. Kaut arī CERT.LV nav pierādījumu par uzbrukumu mēģinājumiem Latvijā, ļoti ticami ir pikšķerēšanas uzbrukumi tuvā nākotnē. **Paredzams, ka tie, visticamāk, notiks leģitīma ES/NATO konferenču, semināru, darba grupu u.c. pasākumu aizsegā. CERT.LV aicina informēt par aizdomīgiem uzaicinājumiem uz ES vai NATO pasākumiem no neoficiālām e-pasta adresēm.**



Augsti kvalificēts pastāvīgo draudu grupējums "APT28" (zināms arī ar nosaukumiem "BlueDelta", "Fancy Bear", "FightingUrsa", "Forest Blizzard", "Iron Twilight", "Pawn Storm", "Sednit", "Sofacy", "Strontium", "TAG-75" un "Tsar Team") ar augstu varbūtību ir Krievijas militārās izlūkošanas (GRU) organizēts.

Tas specializējas kiberizlūkošanā pret NATO un ES valstīm, izmanto plašu ļaunatūru klāstu, piemēram, "Dridex", "Vawtrak", "Gootkit", "TorrentLocker" un "HOOKEDGE".

Tika novērots arī "webhook.site" komandkontroles C2 komunikācijai un datu nopludināšanai.

Uzbrukumos izmanto mērķētu pikšķerēšanu, izveidojot pastāvīgo pieeju un pārvietojoties tālāk cietušā iekštīklā. Sākotnējās piekļuves iegūšanai mēdz izmantot arī informācijas zadzējus.

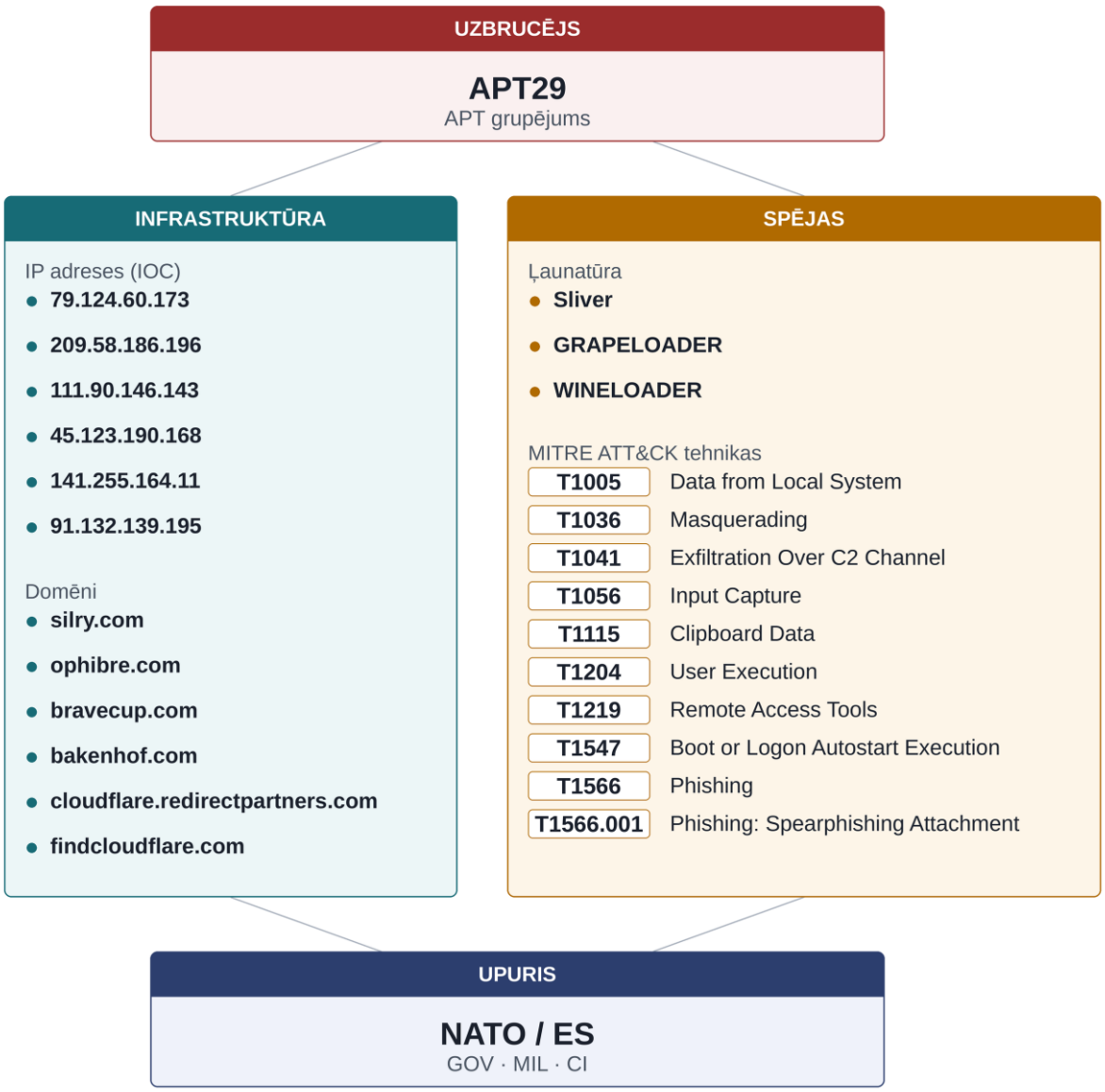
Tīkla aktivitāte uz domēnu "webhook.site" var būt leģitīma, ja to prasa darba vajadzības, pretējā gadījumā nepieciešama izmeklēšana.

Draudu grupas "APT28" uzbrukumu mēģinājumi Latvijā īstenoti pret valsts iestādēm.

Tehniski attīstīts pastāvīgo draudu grupējums "APT29" (pazīstams arī kā "BlueBravo", "Cozer", "Cozy Bear", "Cozy Duke", "CozyCar", "EuroAPT", "Group 100", "Midnight Blizzard", "Minidionis", "NOBELIUM", "Office Monkeys", "RUS2", "SeaDuke", "The Dukes" un "UNC2452"), ļoti ticams, ir izveidots vai citādi saistīts ar Krievijas ārējās izlūkošanas dienestu "SVR", kas specializējas izlūkošanā pret NATO un ES valstīm.

Uzbrukumos izmanto mērķētu pikšķerēšanu, izveido pastāvīgo pieeju un pārvietojas tālāk cietušā iekštīklā. Sākotnējās piekļuves iegūšanai mēdz izmantot informācijas zadzējus.

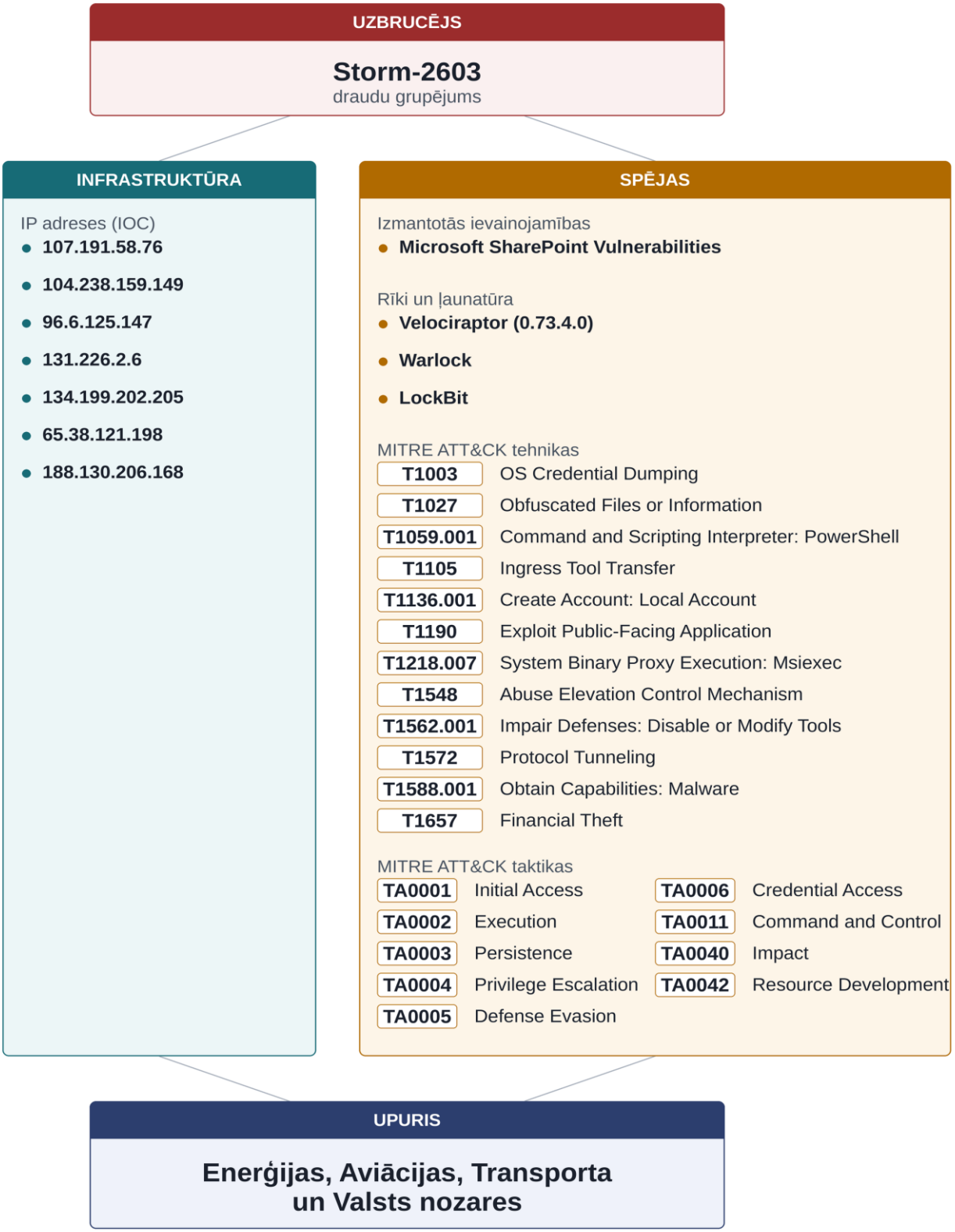
Grupējums veicis uzbrukumu mēģinājumus Latvijas valsts iestādēm (attēls zemāk):



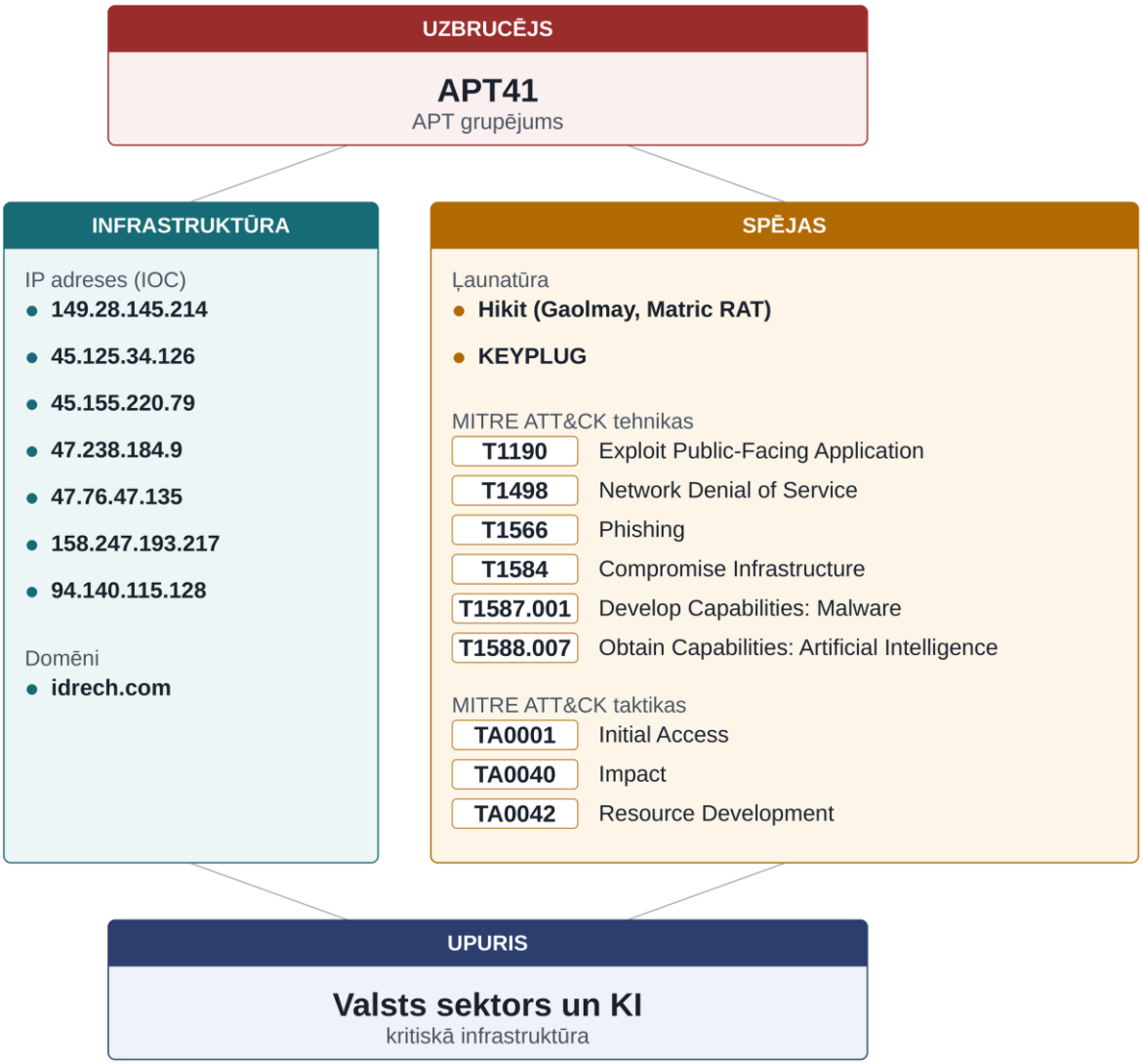
2025. gadā pret vienu no Latvijas valsts iestādēm tika īstenots kiberuzbrukums. Izmeklēšanas rezultāti norāda uz augsti kvalificētu kiberuzbrucēju un sarežģītu operacionālo darbību. Secināts, ka cietušā izvēle, uzbrukuma rokraksts un izvirzītie mērķi atbilst Krievijas valdības stratēģiskajām interesēm. Uzbrucējs nosaukts par "Unclassified-RU_1", jo nav iegūti pierādījumi par saistību ar kādu zināmu uzbrucēju grupējumu. Uzbrucējs, visticamāk, izmantoja informācijas zadzēju, lai ar iegūtajiem autentificēšanās datiem piekļūtu lietotāju e-pastam. Uzbrukums turpinājās cietušā infrastruktūrā ar VPN autentifikāciju, izplatoties tālāk iekštīklā ar "Impacket" rīku kopu, lai izgūtu autentificēšanās datus no "LSA Secrets", "SAM" un "NTDS.dit" datubāzēm. Pamanīta manipulācija ar operētājsistēmas reģistru, rezultātā iegūti vairāku lietotāju dati.

APT ar nosaukumu "Storm-2603" ar lielu varbūtību ir Ķīnas valdības atbalstīts kibergrupējums. 2025. gadā novēroti plaši Microsoft SharePoint ievainojamību CVE-2025-49704, CVE-49706, CVE-2025-53770 un CVE-2025-53771 izmantošanas mēģinājumi. Tāpat varēja novērot, ka pastāvīgas pieejas nodrošināšanā tika

izmantots kiberizmeklēšanas rīks. Kompromitētajās infrastruktūrās novēroti šifrējošie vīrusi “Warlock” un “LockBit”. Grupējums veica uzbrukumu mēģinājumus kritiskai infrastruktūrai arī Latvijā.



Pastāvīgo draudu grupējums "APT41" (pazīstams arī kā "RedGolf", "BRONZE ATLAS", "Barium", "Blackfly", "Brass Typhoon", "Earth Baku", "Red Kelpie", "Wicked Panda" un "Winnti Group"), ļoti iespējams, ir Ķīnas valdības atbalstīts uzbrucēju grupējums, kas vēsturiski veic kiberizlūkošanu un citas operācijas pret kritisko infrastruktūru valsts sektoros ASV un Taivānā. Tehniskie artefakti nesen pamanīti arī Latvijā. Komandkontroles ("C2") komunikācijai bieži izmanto "Cloudflare" tīkla pakalpojumu "CDN". Grupējums izmantojis Latvijas IT pakalpojuma sniedzēju infrastruktūru komandkontroles nodrošināšanai.

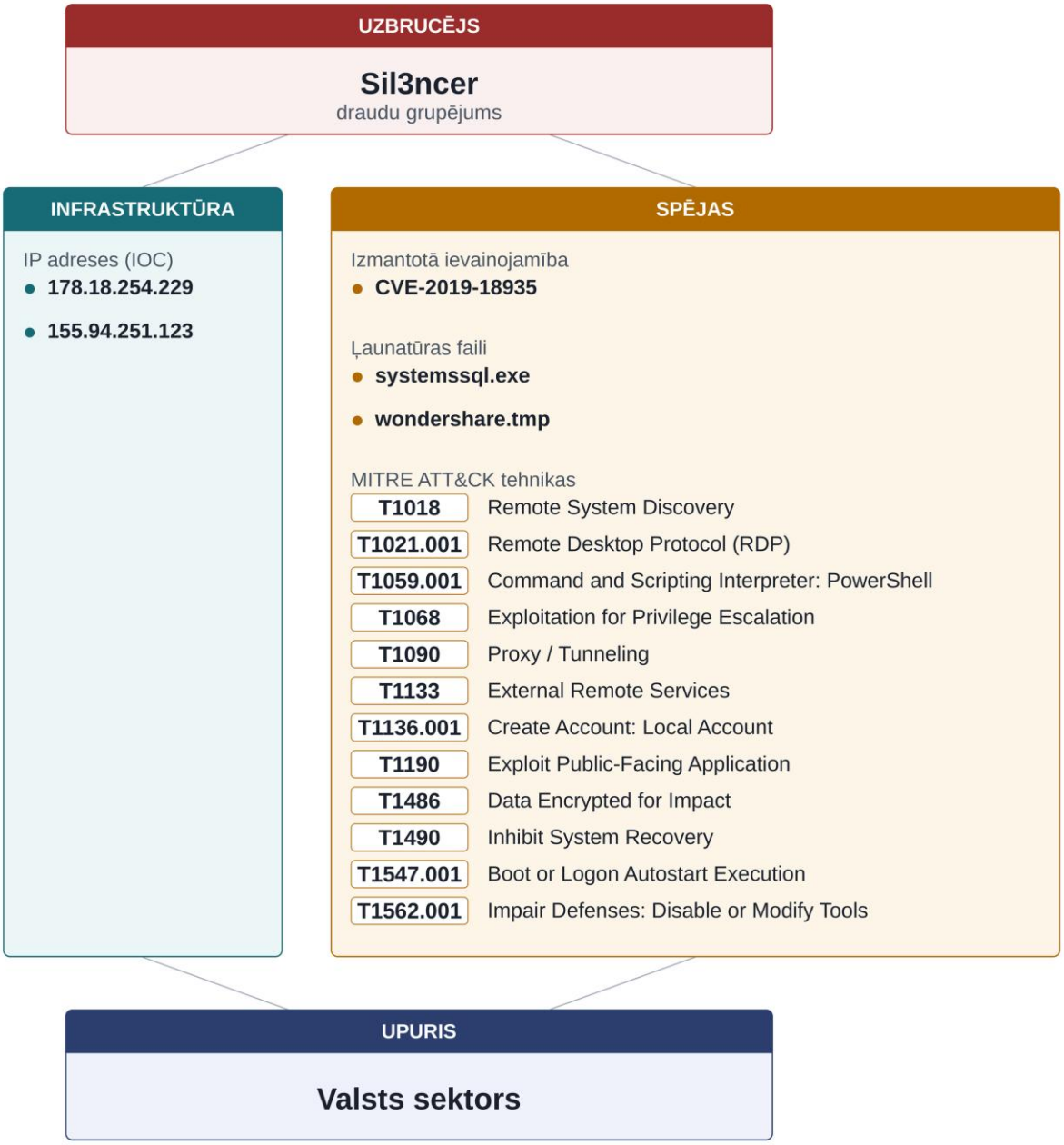


APT ar nosaukumu "Mustang Panda" (zināms arī kā "RedDelta", "BRONZE PRESIDENT", "DarkPeony", "HoneyMyte", "Red Lich", "TA416", "Twill Typhoon", "UNC6384" un "Vertigo Panda"), visticamāk, ir Ķīnas valdības atbalstīts grupējums, kas labi zināms ar kiberizlūkošanas un citām kritiskās infrastruktūras operācijām valsts sektoros Āzijas un Eiropas reģionā. Bieži pikšķerēšanas kampaņās izmanto aktuālos ģeopolitiskos notikumus un sociālo inženieriju. Liela interese par valsts ārlietu iestādēm. Grupējums zināms ar uzbrukuma mēģinājumiem pret Latvijas valsts iestādēm.

APT ar nosaukumu "Famous Sparrow" (pazīstams arī kā "RedMike", "Earth Estries", "GhostEmperor", "Salt Typhoon", "UNC2286" un "UNC5807") ar augstu iespējamību ir Ķīnas valdības atbalstīts grupējums, kas veic kiberizlūkošanu pret NATO un ES valstīm. Primāri fokusējas uz kritisko infrastruktūru, galvenokārt telekomunikācijas pakalpojumu sniedzējiem un valsts sektoru. Iecienīta Citrix produktu ievainojamību izmantošana, attālinātai piekļuvei lieto "AnyDesk" grafiskās pārvaldības risinājumu. Pikšķerēšanas e-pastos bieži lieto "protonmail.com" domēna adreses. Grupējums veicis uzbrukumu mēģinājumus pret Latvijas valsts iestādēm un akadēmisko nozari.

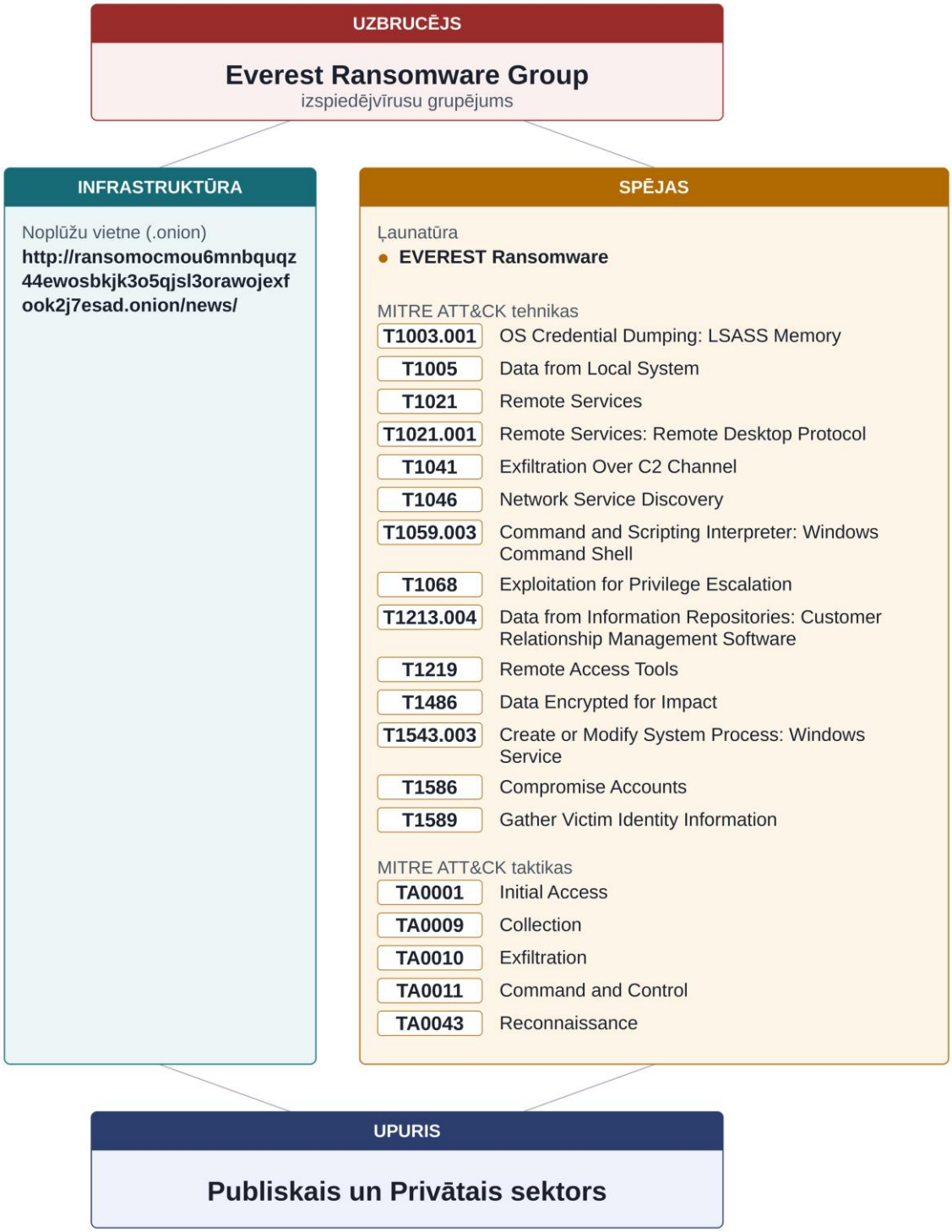
7.5. Finansiāli motivētie grupējumi

Uzbrucēju grupējums “Sil3ncer” ir finansiāli motivēts, mērķē uz publiski eksponētiem servisiem, piemēram, “Telerik UI”. Pēc sākotnējās piekļuves izveido lietotāju ar administratora tiesībām, turpinot ar šifrējošā vīrusa izplatīšanu (failu paplašinājums “.sil3ncer”). “Sil3ncer” veicis uzbrukumu mēģinājumus valsts iestādēm Latvijā.



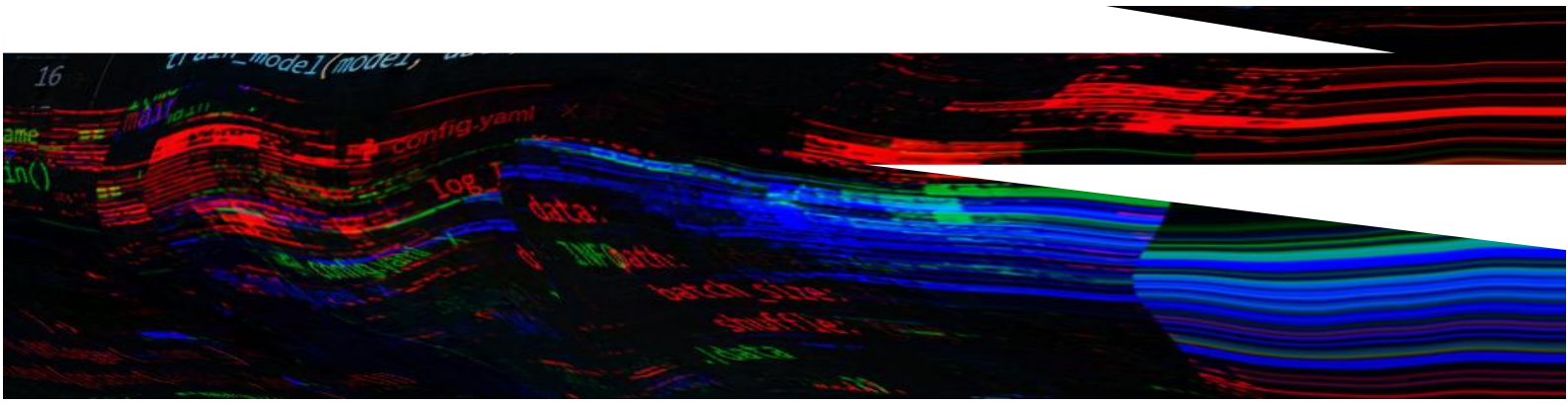
Finansiāli motivēts grupējums “Sarcoma” ir pazīstams ar izspiešanas metodi, kur upurim tiek draudēts ar nozagtās (eksfiltrētās) informācijas publisku nopludināšanu nemaksāšanas gadījumā. Primārais mērķis ražošanas nozare, Latvijā īstenoti uzbrukumu mēģinājumi uzņēmumiem privātajā sektorā.

Finansiālu mērķu vadīta uzbrucēju grupa “Everest Ransomware Group” mērķē uz nozīmīgiem uzņēmumiem ar apjomīgu apgrozījumu, piemēram, “Under Armour”, “ASUS”, “Iberia Airlines” u.c., plaši izmantojot programmatūras ievainojamības. Ļoti aktīvi darbojas globālu uzņēmumu kompromitēšanā un datu šifrēšanā. Darbība Latvijā vēl nav novērota.


UZBRUCĒJS
Everest Ransomware Group
izspiedējvīrusu grupējums
INFRASTRUKTŪRA
Noplūžu vietne (.onion)
http://ransomocmou6mnbquqz44ewosbkjk3o5qjsl3orawojexfook2j7esad.onion/news/
SPĒJAS
Ļaunatūra
EVEREST Ransomware
MITRE ATT&CK tehnikas
T1003.001 OS Credential Dumping: LSASS Memory
T1005 Data from Local System
T1021 Remote Services
T1021.001 Remote Services: Remote Desktop Protocol
T1041 Exfiltration Over C2 Channel
T1046 Network Service Discovery
T1059.003 Command and Scripting Interpreter: Windows Command Shell
T1068 Exploitation for Privilege Escalation
T1213.004 Data from Information Repositories: Customer Relationship Management Software
T1219 Remote Access Tools
T1486 Data Encrypted for Impact
T1543.003 Create or Modify System Process: Windows Service
T1586 Compromise Accounts
T1589 Gather Victim Identity Information
MITRE ATT&CK taktikas
TA0001 Initial Access
TA0009 Collection
TA0010 Exfiltration
TA0011 Command and Control
TA0043 Reconnaissance
UPURIS
Publiskais un Privātais sektors

Ieteikumi

- Iepriekš minētos autonomās sistēmas (AS) IP adrešu apgabalus uzskatīt par kaitnieciskiem un bloķēt tīkla komunikāciju ugunsmūra konfigurācijā. Rezultātu var sasniegt arī izmantojot CERT.LV pakalpojumu "MISP", kuru ieviešot tiks iegūta piekļuve pie identificētajiem kaitnieciskajiem IP adrešu apgabaliem;
- Pārliecināties, ka publiskā tīmeklī netiek eksponētas iekārtas un sistēmas, pārliecināties par programmatūras savlaicīgu atjaunināšanu;
- Lietotājiem (t.sk. administratoriem) iespējota divu faktoru autentifikācija, iespējota žurnālu ierakstu veidošana par visiem pieteikšanās mēģinājumiem un ieslēgts aizdomīgu darbību meklēšanas mehānisms;
- Publiska tīmekļa eksponēšanas nepieciešamības gadījumā, pakalpojumu nodrošināt ar VPN;
- Viedo funkcionālo iekārtu (piemēram, videokameras, apkures katli u.c.) pārvaldības paneļus neeksponēt publiskā tīmeklī, obligāti nomainīt ražotāja noklusējuma paroli;
- Pārliecināties, ka ir izveidots un aktuāls saraksts vai dokumentācija par uzņēmumā izmantoto programmatūru;
- Regulāri veikt rezerves kopijas, tās glabāt ārpus uzņēmuma ikdienas darba datortīkla vai pārkopēt citā nodalītā un standarta lietotājiem nepieejamā tīkla segmentā;
- Pārskatīt un aktualizēt uzņēmuma darba nepārtrauktības plānu;
- Domēna īpašniekiem/turētajiem ieteicams ieviest automātisku pārslēgšanos uz rezerves DNS serveri ("DNS Failover"), lai primārā DNS pakalpojuma sniedzēja avārijas gadījumos būtu nodrošināta aizsardzība (atsaucoties uz 2025. gada novembra "Cloudflare" incidentu);
- Valsts, pašvaldību iestādēm un NIS2 subjektiem ieteicams izmantot CERT.LV SOC pakalpojumu, kas nodrošina individuāli pielāgotu kiberdrošības uzraudzību reāllaikā. CERT.LV SOC identificē, izmeklē un novērš apdraudējumus un kiberincidentus. Plašāk: https://cert.lv/lv/pakalpojumi#12-drosibas-operaciju-centra-pakalpojums



8. Kiberdrošības draudu medību operācijas

Kopš 2022. gada CERT.LV veic Latvijā plaša mēroga draudu medību operācijas. Tās notiek CERT.LV vadībā sadarbībā ar NATO sabiedroto valstu partneriem, galvenokārt Kanādas bruņotajiem spēkiem un kiberdrošības centru. Sadarbība īstenota arī ar ASV kiberpavēlniecību, Beļģijas bruņotajiem spēkiem, Polijas bruņotajiem spēkiem, CERT.EU un Eiropas Savienības kiberdrošības aģentūru (European Union Agency for Cybersecurity, ENISA). Draudu medību aizsākšanas pamats bija CERT.LV notikumu novērojumi Latvijas kibertelpā, kā arī reģiona ģeopolitiskā situācija.

Draudu medības ir kiberaizsardzības operāciju veids (termins angliski "threat hunting"), kuras mērķis novērtēt vispārējo informācijas un komunikāciju tehnoloģijas (IKT) infrastruktūras kiberdrošības līmeni, kā arī atklātu, uzraudzītu un analizētu ļaunprātīgas darbības. Identificējot uzbrucēja klātbūtni, draudu medību dalībnieku uzdevums ir analizēt uzbrukumu taktiku, paņēmienus un izmantotās procedūras. Operāciju prioritāte ir identificēt citu valstu (piemēram, Krievijas un Ķīnas) atbalstītu kiberoperāciju jeb padziļināto pastāvīgo draudu (APT) klātbūtni. CERT.LV 2025.gadā veica visaptverošas IKT draudu medības 14 organizācijās, gandrīz visās tika konstatētas lielāka vai mazāka apmēra nepilnības infrastruktūras konfigurācijā vai pārvaldībā.

Draudu medības ir CERT.LV pakalpojums, kuru var pieprasīt valsts un pašvaldību iestādes, kritiskās infrastruktūras un būtisko pakalpojumu sniedzēji (https://cert.lv/lv/pakalpojumi). Kaut arī draudu medības pamatā ietver kiberaizsardzības operācijas klienta organizācijā, vienlaikus pēc katra projekta iespējām CERT.LV sadarbībā ar klientu nodrošina objektīvu skatījumu uz organizācijas IKT infrastruktūru un kopējo kiberdrošības līmeni. To panāk ar iestādes gala iekārtu analīzi, meklējot gan ļaunprātīgu darbību pazīmes, gan labās un sliktās IKT pārvaldības prakses, gan vājās vietas infrastruktūrā. Procesa gaita rūpīgi reģistrēta, protokolēta un dokumentēta, sniedzot rekomendācijas klienta IKT administratoriem un drošības pārvaldniekiem. Mērķis ir efektīva nepieciešamo izmaiņu veikšana un labo prakšu ieviešana, lai ilgtermiņā stiprinātu organizācijas kiberdrošību.

Uzbrukuma tehniku identificēšanai, klasificēšanai un strukturētai analīzei izmantots MITRE ATT&CK ietvars: https://attack.mitre.org/matrices/enterprise/.

Secinājumi un atradumi no kiberdrošības draudu medību operācijām 2025. gadā

Uzbrucēji ļoti bieži ļaunprātīgi izmanto leģitīmu sistēmu administratoru piekļuves, kontus un ikdienā lietotus administrēšanas rīkus. Kompromitēts vai apzināti iesaistīts administrators var kļūt par daļu no uzbrucēja infrastruktūras, nodrošinot piekļuvi, noturību, konfigurāciju maiņu un darbību slēpšanu. Šādu risku būtiski palielina administratoru vieglprātība, nepietiekama disciplīna, pārmērīga noslodze un personāla trūkums, kā rezultātā tiek pieļautas novēlotas atjaunināšanas, tiek piešķiras pārmērīgas privilēģijas ikdienas lietotājiem, koplietoti konti, nepietiekama žurnālfailu uzraudzība un citi drošības kompromisi. Šādos apstākļos administratori, pat bez ļaunprātīga nolūka, faktiski kļūst par uzbrucēju darbību veicinātājiem. Vienlaikus arī sākotnēji nekaitīgi administrēšanas rīki var tikt izmantoti kā LOTL ("living off the land") paņēmieni vai ļaunatūras sastāvdaļa.

Galvenais secinājums: klientu IKT infrastruktūrās atkārtoti konstatēta nepietiekami centralizēta un nekonsekventa pārvaldība. Bieži izmantotas novecojušas, ievainojamas vai ražotāja vairs neatbalstītas operētājsistēmas, lietojumprogrammas un iekārtu dziņi jeb "draiveri". Darba iekārtās atrasta nevēlama, pirātiska, ar darba pienākumiem nesaistīta vai apšaubāmas izcelsmes programmatūra, tostarp spēles, failu apmaiņas, attālinātās piekļuves un lietotāja aktivitāti imitējoši rīki. Vairākās vidēs lietotājiem un servisu

kontiem bija pārmērīgas tiesības, savukārt neaktīvie konti netika savlaicīgi atspējoti. Paroles un citi piekļuves dati glabāti atklātā tekstā, komandu vēsturē, skriptos, kontu aprakstos un citās nedrošās vietās. Konstatēta arī nekontrolēta attālinātās piekļuves rīku izmantošana, kas palielina uzbrukuma virsmu un apgrūtina incidentu izmeklēšanu. Daļa iekšējo pakalpojumu, pārvaldības paneļu un RDP servisu bija nevajadzīgi publiski eksponēti internetā. Gala iekārtu ugunsmūri, DNS filtrēšana, pretvīrusu aizsardzība, XDR un žurnālfailu uzkrāšana vairākos gadījumos bija nepilnīga vai nevienmērīga. Darbstacijās un ārējos datu nesējos glabāta konfidenciāla infrastruktūras informācija, sertifikāti un citi dati, kuru noplūde var palīdzēt uzbrucējam orientēties vidē.

Galvenie uzlabojumi jāveic inventarizācijā, atjauninājumu pārvaldībā, piekļuves tiesībās, programmatūras kontrolē, tīkla segmentācijā, žurnālfailu centralizācijā un regulārā drošības uzraudzībā.

8.1. Detalizēti tehniskie konstatējumi draudu medību ietvaros

Ļaunatūra

Draudu medību operāciju laikā tika konstatēti kompromitēšanas gadījumi ar ļaunatūrām "RemcosRAT" (T1219) un "XWorm" (TA0001, T1091), kur abu kampaņveidīga izmantošana plaši novērota 2025. gada beigās (https://www.malwarebytes.com/blog/threat-intel/2025/11/we-opened-a-fake-invoice-and-fell-down-a-retro-xworm-shaped-wormhole). Standarta antivīrusa risinājumi sākumā šo ļaunatūru neievēroja un nebloķēja. Tā saucamais "RAT" jeb "Remote Access Trojan" incidenta gadījumā nodrošina attālinātu piekļuvi kompromitētajām iekārtām.

Sākotnējā piekļuve. Tipiski ļaunatūru "XWorm" piegādā ar pikšķerēšanas e-pastiem, taču šajā gadījumā izpilde notika no kompromitēta USB datu nesēja (T1091), kurš sākotnēji pirms tam ievietots privātā iekārtā, tādējādi pavairojoties ar datu nesējiem. Šādā veidā ļaunatūra darbojas kā "datortārps", izplatoties starp dažādiem tīkliem. Inficētajā USB datu nesējā tika izveidots fails "678876789765.CMD", kas neveic automātisku izpildi, t.i., nenotiek nekādas darbības pēc USB zibatmiņas pievienošanas datoram. Uzbrucēji paļaujas, ka lietotājs neuzmanības dēļ izpildīs ļaunatūras failu.

Pastāvīgo pieeju (persistenci) ļaunatūra "XWorm" īstenoja ar operētājsistēmas uzdevuma pārvaldnieka "Windows Task Scheduler" (T1053) jaunu izveidotu plānoto notikumu, nosaukumā nejauši simboli "Othyzbjwm". Ņemot vērā, ka kompromitētajam lietotājam nebija datora administratora privilēģijas, izveidotais notikums izpildījās ar standarta lietotāja tiesībām. Šāds pastāvīgās pieejas mehānisms reizi 20 minūtēs izpildīja ļaunatūras izveidoto failu publiskajā lietotāja mapē "C:\users\public\othyzbjwm.url". Šis fails ir ļaunprātīga saīsne uz izpildāmu (.exe) datni "C:\Users\Public\Libraries\Othyzbjwm.exe", kas izmantoja leģitīmu tīmekļa vietni "Pastebin" (T1102), lai iegūtu informāciju par aktuālo kontroles serveri. Kontroles serveris atradās populārā mitināšanas pakalpojuma sniedzēja "DigitalOcean" tīklā, saziņai izmantojot TCP protokola 8912 portu. Ļaunatūras izpildes gaitā tika papildus novērota spraudņa "XWorm" izvietošana GZIP formātā sistēmas reģistra datnē "HKCU\SOFTWARE\<KLIENTA_ID>" (T1547.001). Reģistra vērtības nosaukums ir spraudņa jaucējfunkcijas vērtība, saturā ir izpildāms fails. Kad ļaunatūra saņems kontroles servera komandu izpildīt spraudni, tā izmantos šīs reģistra vērtības.

Indikatori

- MD5: 166ac66d27052926e1f8dedd6cdaa1c8;
- MD5: b967ccad9189b23601c3673d7f9207b8;
- Datne: C:\users\public\othyzbjwm.url;

- Datne: C:\Users\Public\Libraries\Othyzbjwm.exe;
- URL: https[:]//pastebin[.]com/raw/3XznTkFA;
- Windows uzdevumu pārvaldnieka "Task Scheduler" ieraksts: \Othyzbjwm;
- Domēns: www[.]hulduo88[.]com;
- IP: 167.71.255[.]27;
- MD5: ac409e8856618c3597647440d5d2ddc7;
- Datnes nosaukums: RemoteDesktop.dll;
- Reģistra atslēga: HKCU\SOFTWARE\6E1D9460E74AA120B160941F284C09563BA5E75BCEDC2006CB750793CE5BC3BB.

Tālākās izpildes fāze. Incidenta turpinājumā "XWorm" izmantots nākamās ļaunatūras "RemcosRAT" lejupielādei un izpildei. Šo maksas ļaunatūru izmanto attālinātās piekļuves nodrošināšanai, tās mērķis ir veikt ļaunprātīgas darbības, piemēram, starpliktuves, taustiņu kombinācijas un sistēmas piekļuves datu ieguve. Ļaunatūras papildu funkcija ir palikt neredzamai un izvairīties no atrašanas pretvīrusu risinājumiem (AV, EDR u.c.). Ļaunatūras darbības laikā tika novērota iebūvēto leģitīmo "LoL" izpildāmo failu izmantošana (T1036):

- "PowerShell", T1059.001;
- "wscript.exe" (JScript un VBScript izpildei), T1059.005;
- "cmd.exe" (.bat failu izpildei).

Windows notikumu žurnāls identificēja PowerShell izpildi ar dažādiem formātu kodēšanas mehānismiem nolūkā komandas padarīt nesalasāmas. Apskatot "PowerShell" skriptu digitālos parakstus (signatūras), slēpšanai tika izmantots, visticamāk, risinājums "Invoke-Obfuscation" vai līdzīgas funkcionalitātes alternatīva (https://github.com/danielbohannon/Invoke-Obfuscation).

Ļaunatūras izpildes laikā notika vairāki savienojumi pie kontroles servera IP adresēm, saziņai šajā gadījumā izmantojot TCP protokola 5321 portu. Kontroles servera mitināšanu nodrošināja "Cheapy.host LLC" pakalpojuma sniedzējs, kas nav tiešā veidā saistīts ar kādu APT grupējumu.

Indikatori

- Datne: C:\Users\Public\StableMarket.bat
- Datne: C:\Users\lietotajs\aoc.bat
- Datne: C:\Users\lietotajs\AppData\Local\Temp\otkrqd.js
- Datne: C:\Users\lietotajs\AppData\Local\Temp\Incisalia.bat
- Datne: C:\Users\lietotajs\AppData\Local\Temp\luywsu.vbs
- Datne: C:\Users\lietotajs\AppData\Local\Temp\vpcekogz.vbs

Ieteikumi ļaunatūru ierobežošanai

Pretvīrusa (AV) un EDR risinājumu konfigurācijas pārskatīšana, jo daudzos gadījumos AV identificē kaitīga skripta failu izpildi "Temp" direktorijā, taču to bloķēšana nav iespējota. Ļaunatūras bieži izmanto pagaidu "Temp" mapes, lai veiktu kaitniecisku failu izpildi. Ja AV risinājums paredz aizdomīgu izpildes aizliegšanas iestatījumu, to ieteicams iespējot.

USB datu nesēju pārvaldība ir preventīvs risinājums privātu zibatmiņu lietošanas risku mazināšanai. To var īstenot dažādos veidos, viens variants ir Windows aktīvās direktorijas grupu politikas konfigurācija, kur tiek definēti konkrēti atļautie USB sērijas numuri.

Draudu medībās vairākos tīklos tika atrastas citas mazākas nozīmes ļaunatūras paliekas un digitālie artefakti. Piemēram, lietotāji mēģināja uzstādīt leģitīmu videokonferences programmatūru, to lejupielādē netīšām no kaitnieciskas vietnes ļaundabīgā pakotnē "InstallPack_Zoom_c4b08.exe", kas maskējas par "Zoom" programmatūru. Atrastas arī vairākas pikšķerēšanas uzbrukumu pēdas, piemēram, automātiskās palaišanas "Autoruns" ieraksts ar ķīniešu simboliem un plašu atpazīstamību ļaunatūru koplietošanas vietnēs. Avots, visticamāk, ir pikšķerēšanas rezultātā lejupielādēts ".zip" arhīvs ar inficētu "*.xlsx" datni saturā.

Šie atrastie digitālie pēdu nospiedumi — maldinošu failu lejupielāde un pikšķerēšanā atvērtas datnes – ir netīša lietotāju rīcība, nevis mērķēta APT aktivitāte. Taču bieži šāda tipa programmas tiek lietotas mērķa iekārtas piekļuves nodrošināšanai (T1176).

8.2. Citi identificētie konstatējumi lietotāju darbībās

Gada rezultātu analīze parāda dažādas nevēlamas prakses un darbības lietotāju uzvedībā. Tās var iedalīt trīs grupās:

1. Darbinieki, kas pienākumu pildīšanai izmanto visu brīvi pieejamo programmatūru. Kad esošā lietotne neveic kādu uzdevumu, bez konsultēšanās un izvērtēšanas lejupielādē citu aizdomīgu programmatūru no pagrīdes avotiem. Šādus risinājumus saviem spēkiem darbinieki veic, kad vai nu trūkst atbilstošas lietotnes vai licences, vai IT administratoru atbalsts. Praksē tā ir dažādu rīku izmantošana, piemēram, "CuteWriter", "PDF Architect" satur reklāmvīrusus un citu ļaunatūru. Ķīnā izstrādāta biroja programmatūra "WPS Office", kas var saturēt dažādus riskus. Windows vai Microsoft Office nelegālu aktivācijas rīku izmantošana, nevis oficiāla licenču iegāde;
2. Darbinieki, kas izmanto dažādas programmas aktīva darba simulēšanai, piemēram, "mousejiggler.exe";
3. Darbinieki, kas organizācijas iekārtas izmanto privātām aktivitātēm, kā datorspēlēm ("Steam", "Roblox", "PUBG"), ar darbu nesaistītām tīmekļa vietnēm (azartspēles) un citu lieku izklaides programmatūru (piemēram, "Felix the cat", kas pa laikam "staigā" datora ekrānā).

Neatbilstoša prakse novērota arī lietotājiem ar paaugstinātām tehniskajām privilēģijām jeb IT sistēmu administratoriem.

Draudu medībās pastiprināta uzmanība tika pievērsta "Microsoft Exchange" e-pasta pakalpojumam. Publiski pieejams "Microsoft Exchange" autentifikācijas panelis nodrošina uzbrucējiem tiešu un vienmēr pieejamu automatizētu paroļu pārlases uzbrukumu vietu (T1110.003). Ja nav ieviesti efektīvi aizsardzības pasākumi, ir būtiski paaugstināts risks, ka kibernoziedznieki spēs kompromitēt kāda lietotāja kontu un to izmantot tālākos uzbrukumos. Papildu risks rodas, kad mērķa infrastruktūrā joprojām tiek izmantots autentifikācijas mehānisms "NTLMv2", tādos gadījumos pārtverti autentifikācijas dati var ļaut uzbrucējam pārvietoties cietušā infrastruktūrā vai tikt izmantoti citos uzbrukumos (T1550.002).

Lokāli uzturēts "Microsoft Exchange" serveris pēc noklusējuma eksponē vairākas saites (/ews, /autodiscover, /rpc, /owa), tādēļ iespējami vairāk jāliedz pieeja bloķējot no ārpuses vai jāatver piekļuve caur VPN tuneli. Ja to nav iespējams darīt biznesa nodrošināšanas dēļ, "Microsoft Exchange" serveri jānovieto aiz reversā starpniekservera (reverse-proxy), kas sniedz plašāku aizsardzību un iespējas stingrāk sekot līdzi aizdomīgiem pieslēgumiem.

Draudu medībās konstatēti dažādi attālinātās pārvaldības rīki un viena standarta trūkums. Organizācijas periodiski maina attālinātas piekļuves risinājumus vai izmanto vienlaicīgi vairākus, tas liedz attālināto piekļuvi

pārvaldīt, analizēt incidentus vai izvērtēt pieslēgšanās leģitimitāti. Iekārtas kompromitēšanas gadījumā dažādie rīki sniedz arī uzbrucējam vairākas rīcības alternatīvas, lai infrastruktūrā pārvietotos (laterālā kustība) un veiktu privilēģiju eskalāciju. Drošības personālam ir būtiski apgrūtināta uzbrucēja darbību atklāšana un izsekošana, ko paildzina nesistemātiski žurnālfailu ieraksti vai to trūkums. Centrāli nepārvaldīti risinājumi patvaļīgi var ieviest izmaiņas datora lokālā ugunsmūra iestatījumos. Ņemot vērā iepriekš minētos iemeslus, CERT.LV šādu praksi uzskata par nedrošu. Klientu infrastruktūrā atrastie attālinātās kontroles rīki, kuri nenodrošina žurnalēšanu, centralizētu pārvaldību un atjauninājumus:

- Bomgar SCC (Bomgar Secure Customer Chat);
- PsExec;
- RustDesk;
- TeamViewer;
- Anydesk u.c.

Kādā organizācijā tika konstatēti vairāk nekā 15 dažādu attālināto piekļuves rīku izmantošana. Attālināto piekļuves risinājumu atjauninājumu neveikšana vai viena rīka dažādu versiju izmantošana arī liecina par centralizētās pārvaldības trūkumu un iekšējo procedūru trūkumu.

Konstatēts gadījums, kad attālinātas pārvaldības “Intel Active Management Technology (AMT)” konsole tika eksponēta publiskajā tīmeklī:

Lai informācijas sistēmās un infrastruktūrā paplašinātu redzamību un stiprinātu attālinātas piekļuves pārvaldību, organizācijām ir ieteikts samazināt lietoto attālinātās piekļuves dažādību, izvēloties vienu konkrētu risinājuma komplektu. Piemēram, ieviešot vienu pamata rīku attālinātas piekļuves nodrošināšanai un vienu rezerves risinājumu (ja nepieciešams). Sekot līdzi un veikt atjauninājumus. CERT.LV iesaka izmantot operētājsistēmu iebūvētos risinājumus.

Vairākās analizētajās infrastruktūrās konstatēti ilgstoši nelietoti Aktīvās direktorijas (AD) lietotāju konti ar pēdējo pierakstīšanos pirms gada un vairāk. No tiem vairāki privileģēti lietotāji ar paaugstinātām piekļuves un pārvaldības tiesībām. Atrasti arī tādi AD konti, kuru aprakstā teikts, ka izveidoti uz laiku (piemēram, praktikantiem), taču faktiski joprojām ir strādājoši. Identificēti aktīvi konti, kuriem pieteikšanās nekad nav notikusi. Atrasta AD lietotāju mape "OU=Outsource", kurā konstatēts liels skaits neaktīvu AD kontu, kas, visticamāk, paredzēti ārējo resursu vai trešo pušu piekļuvei. Vienā no analizētajām infrastruktūrām bija vairāk nekā 200 šādu novecojušu, bet joprojām aktīvu AD lietotāju kontu.

Neaktuāli un iespējoti AD lietotāju konti rada papildus drošības riskus vairāku iemeslu dēļ, piemēram:

- bijušo darbinieku vai trešās puses konti var joprojām iegūt sensitīvu informāciju saistībā ar organizāciju;
- tie var tikt izmantoti kā uzbrukuma vektors, kompromitēšanas gadījumā novest pie tālākām neautorizētām aktivitātēm tīklā.

Ņemot vērā visu minēto, infrastruktūras administratoriem nepieciešams veikt regulāru AD kontu pārskatīšanu, auditu un veikt neaktīvo kontu atspējošanu vai dzēšanu.

Aktīvās direktorijas lietotāju pārvaldība piedāvā iespēju iestatīt automātisku konta atspējošanas datumu, piemēram, jauna īslaicīga praktikanta lietotāja izveidošanas brīdī iestatīt arī automātisku beigu derīguma termiņu.

8.3. Klientu IKT infrastruktūrā veikto draudu medību detalizēti konstatējumi un secinājumi

CERT.LV veica visaptverošas draudu medības uzņēmuma informācijas un komunikāciju tehnoloģiju (IKT) infrastruktūrā ar nolūku novērtēt vispārējo drošības apdraudējumu situāciju un identificēt jau kompromitētas sistēmas. Par prioritāti identificēt citu valstu (Krievija, Ķīna u.c.) atbalstītas kiberoperācijas (APT).

Šajā nodaļā sniegts detalizēts dažādu IKT infrastruktūru incidentu, drošības nepilnību un ieteikumu apraksts. Tā kā organizācijās identificētas arī līdzīgas problēmas, atsevišķi incidenti, secinājumi un ieteikumi var daļēji pārklāties.

Pozitīvie novērojumi

- Lietotāju iekārtu un serveru datorparks uzņēmumā tiek pārvaldīts centralizēti, kas tīkla administratoriem ļauj operatīvi un efektīvi reaģēt uz neplānotiem infrastruktūras darbiem. Piemēram, CERT.LV draudu medību projektam ātra tehnisko rīku uzstādīšanu apmēram 730 iekārtu lielā infrastruktūrā. Centralizēta pārvaldība ir būtiska arī gadījumos, kad ātri jāreaģē IT drošības incidentā. Taču ir svarīgi apzināties centralizācijas lielo atbildību un plašo ietekmes potenciālu. Būvējot un uzturot šādu infrastruktūru, jāpārliecinās par drošības zonu segmentāciju un mikro segmentāciju, ieskaitot arī Windows Aktīvās direktorijas struktūrās. Segmentācijas mērķis ir iespējami vairāk ierobežot kompromitētas sistēmas, kā arī nelojāla darbinieka vai uzbrucēja spējas neierobežoti un nepamanīti pārvietoties infrastruktūrā.
- Atzinība uzņēmuma IKT administratoriem par savlaicīgu un izsmeļošu atbilžu sniegšanu uz CERT.LV uzdotajiem jautājumiem Draudu medību kontekstā, kas veicināja operatīvu izmeklēšanas norisi.
- IKT pārvaldības personāla iesaiste un proaktīvā rīcība palīdzēja papildus atklāt iespējamos incidentus.
- Iekārtu analīzē konstatēts, ka uz visām Windows operētājsistēmas darbstacijām ir uzstādīta šobrīd jaunākā pieejamā "Windows 11" versija. Šis ir atzinīgi novērtējams IKT administratoru veikums, jo "Windows 10" versijai atbalsts beidzies 2025.gada oktobrī. Atzinība uzņēmuma IKT administratoriem par

savlaicīgu atbilžu sniegšanu uz CERT.LV uzdotajiem jautājumiem Draudu medību kontekstā, kā arī spēju savlaicīgi nodrošināt visus nepieciešamos papildu datus.

- Atzinība Uzņēmuma IKT administratoriem par savlaicīgu un izsmeļošu atbilžu sniegšanu uz CERT.LV uzdotajiem jautājumiem Draudu medību kontekstā, kas veicināja operatīvu izmeklēšanas norisi.
- Tehniskā personāla iniciatīva automatizēta paroļu atgādinātāja rīka izmantošanā.
- Lokālo administratoru paroļu pārvaldnieka LAPS ("Local Administrator Password Solution") lietošana.
- Detalizēta un aktuāla dokumentācija par programmatūru, u.c. resursiem uzņēmuma infrastruktūrā.
- Potenciāli kaitīgu darbību (piemēram, iejaukšanās "lsass.exe" procesā) atpazīšanas rīks "VI Sophos".
- Atzinība uzņēmuma IKT administratoriem par savlaicīgu un izsmeļošu atbilžu sniegšanu uz CERT.LV uzdotajiem jautājumiem Draudu medību kontekstā, kas veicināja operatīvu izmeklēšanas norisi.
- Tehniskā personāla iniciatīva automatizēta paroļu atgādinātāja rīka izmantošanā.
- Lokālo administratoru paroļu pārvaldnieka LAPS ("Local Administrator Password Solution") lietošana.
- Detalizēta un aktuāla dokumentācija par programmatūru, u.c. resursiem uzņēmuma infrastruktūrā.
- Potenciāli kaitīgu darbību (piemēram, iejaukšanās "lsass.exe" procesā) atpazīšanas rīks "VI Sophos".

Negatīvie novērojumi

- Uzņēmuma infrastruktūrā vairākkārt novērota novecojusi un ievainojama programmatūra, ieskaitot serveru operētājsistēmu versijas. Šādu programmatūru izmantošana būtiski palielina kompromitēšanas riskus, tādēļ nepieciešams nekavējoties uzstādīt atjauninājumus.
- Organizācijas infrastruktūrā novērota potenciāli kaitīga, ar darba pienākumiem nesaistīta programmatūra (t.sk. pārlūkprogrammu spraudņi) un lietotnes no ES / NATO nedraudzīgām valstīm – tas liecina par programmatūras kontroles politikas (Applocker / SRP u.c.) nepilnīgu konfigurāciju.
- IKT administratoru ikdienas darbā izmantotas vairākas nevēlamas prakses, kas ne tikai apdraud infrastruktūras drošību, bet arī sarežģī incidentu izmeklēšanu, apgrūtinot leģitīma lietotāja aktivitāšu nošķiršanu no uzbrucēja darbībām. Piemēram, vāju paroļu uzglabāšana atklātā tekstā, ievainojama programmatūras lietošana, nekonsekventa versiju pārvaldība, nepilnīga programmatūras kontroles politika ("AppLocker" vai analogs risinājums).
- Vairākos gadījumos organizācijas iekārtas tiek izmantotas darbinieku privātām vajadzībām, kas rada risku kaitīgu failu lejupielādē un tālāku izplatīšanos iestādes tīklā.
- Vairākās iekārtās pamanīta novecojusi programmatūra un operētājsistēmas.
- Atklāti tīkla plūsmas pieprasījumi uz aizdomīgiem resursiem un tādu tīmekļa vietņu apmeklēšana, kas nav nepieciešama darba pienākumu veikšanai. Ieteikums izmantot preventīvus pasākumus, kā tīmekļa filtru ("web filter") un ugunsmūra iestatījumus ar stingru tīkla drošības politiku ne tikai ienākošajiem, bet arī izejošiem savienojumiem. Publiskā tīmeklī brīvi pieejami lokālie pakalpojumi "Microsoft Exchange" e-pasts un "Gitlab" programmu koda pārvaldības platforma. Jebkuru resursu izvietojot publiskā tīmeklī tiek būtiski palielināts potenciālais uzbrukuma laukums, tādēļ kritiski jāizvērtē nepieciešamība atvēršanai internetā un visi iespējamie riski.
- Atsevišķām Microsoft Exchange lietotāju pastkastītēm ir piešķirtas, iespējams, pārāk plašas piekļuves tiesībās, proti, citiem lietotājiem ir tiesības lasīt/modificēt/dzēst pasta saturu.
- Iekārtā ar nosaukumu "win10.*.lv" atrastas aktīvās direktorijas drošības novērtējuma atskaites, jāizvērtē šo failu nepieciešamību atrasties minētajā iekārtā.
- Dažās "Windows" iekārtās ir strādājošs noklusējuma pārvaldības konts "Administrator", labās prakses vadlīnijas iesaka izveidot nestandarta priviliģēto lietotāju, atspējojot iebūvēto sistēmas pārvaldnieku.

- IKT administratoru ikdienas darbā izmantotas vairākas nevēlamas prakses, kas ne tikai apdraud infrastruktūras drošību, bet arī sarežģī incidentu izmeklēšanu, apgrūtinot leģitīma lietotāja aktivitāšu nošķiršanu no uzbrucēja darbībām. Piemēram, vāju paroļu uzglabāšana atklātā tekstā, ievainojama programmatūras lietošana, nekonsekventa versiju pārvaldība, nepilnīga programmatūras kontroles politika ("AppLocker" vai analogs risinājums).
- Vairākos gadījumos organizācijas iekārtas tiek izmantotas darbinieku privātām vajadzībām, kas rada risku kaitīgu failu lejupielādē un tālāku izplatīšanos iestādes tīklā.
- Vairākās iekārtās pamanīta novecojusi programmatūra un operētājsistēmas.
- Publiskā tīmeklī eksponēti svarīgi pakalpojumi, radot būtiskus drošības riskus.
- Palielināti riski, izmantojot programmatūru izstrādātu ārpus Eiropas Savienībai un NATO draudzīgām valstīm, kā Krievija un Ķīna.
- IKT administratoru ikdienas darbā izmantotas vairākas nevēlamas prakses, kas ne tikai apdraud infrastruktūras drošību, bet arī sarežģī incidentu izmeklēšanu, apgrūtinot leģitīma lietotāja aktivitāšu nošķiršanu no uzbrucēja darbībām. Piemēram, vāju paroļu uzglabāšana atklātā tekstā, ievainojama programmatūras lietošana, nekonsekventa versiju pārvaldība, nepilnīga programmatūras kontroles politika ("AppLocker" vai analogs risinājums).
- Vairākos gadījumos organizācijas iekārtas tiek izmantotas darbinieku privātām vajadzībām, kas rada risku kaitīgu failu lejupielādē un tālāku izplatīšanos iestādes tīklā.
- Vairākās iekārtās pamanīta novecojusi programmatūra un operētājsistēmas.
- Publiskā tīmeklī eksponēti svarīgi pakalpojumi, radot būtiskus drošības riskus.
- Palielināti riski, izmantojot programmatūru izstrādātu ārpus Eiropas Savienībai un NATO draudzīgām valstīm, kā Krievija un Ķīna.

Draudu medību rezultāti, novērojumi un secinājumi

Novecojusi operētājsistēma "Ubuntu"

Draudu medību ietvaros konstatēta iekārta ar novecojušu operētājsistēmu "Ubuntu 14.04", kas nodrošina kādas tīmekļa vietnes pakalpojumu.

Novecojusī "Ubuntu" versija nesaņem drošības atjauninājumus kopš 2019. gada aprīļa, konkrētāk, standarta atbalsts pārtraukts 02.04.2019., pagarinātais atbalsts apturēts 2024.gada aprīlī. Nekavējoties nepieciešams atjaunot servera operētājsistēmu uz aktuālo "Ubuntu" 24.04 LTS.

Novecojusi operētājsistēma "Windows Server"

Infrastruktūrā identificēti 14 operētājsistēmas "Microsoft Windows" serveri ar "2012R2 Standard" versiju, kurai 2023.gada 10.oktobrī beidzies ražotāja pamata atbalsts, t.i., netiek nodrošināti drošības atjauninājumi.

Jāpiebilst, ka operētājsistēmai "Server 2012 R2" vēl ir pieejama paplašinātā drošības atjauninājumu maksas programma (ESU), kurā ietilpst kritiskie un svarīgie drošības atjauninājumi līdz pat trīs gadiem pēc pagarinātā atbalsta beigām.

Novecojušu operētājsistēmu atrašanās infrastruktūrā būtiski paaugstina iespējamos drošības riskus, jo ražotājs neizlabo un nenovērš jebkuras jaunatklātās ievainojamības, kuras var tikt izmantotas ļaunprātīgiem mērķiem. CERT.LV iesaka pēc iespējas ātrāk atjaunot serverus uz pašlaik aktuālo "Windows Server" versiju 2022 vai 2025.

Konstatētas arī novecojušas Windows darbstaciju versijas. Novecojusi operētājsistēma nesaņem jaunatklāto ievainojamību labojumus, tādēļ būtiski palielinās kompromitēšanas, privilēģiju paaugstināšanas un ļaunatūras izpildes risks.

Novecojusi programmatūra "pgAdmin"

Programmatūra "pgAdmin" ir populāra "PostgreSQL" datubāzes izstrādes un pārvaldības vide, kuru var lietot kā tīmekļa pārlūkā, tā atsevišķā lietotnē. Izmeklēšanas laikā konstatēta novecojušu "pgAdmin" versiju lietošana vairākās iekārtās, no tām četros datoros vecāka par "8.3" – būtiskākā deserializācijas ievainojamība "CVE-2024-2044" ar CVSS riska rādītāju 9.9 no 10 (kritiski). Gadījumos, kad programmatūru izpilda iekārtā neaizsargātā tīkla zonā (piemēram, publiskā tīmeklī), uzbrucējs var veikt attālinātu koda izpildi. Risks mazinās, izmantojot programmatūras noklusējuma iestatīto eksponēšanu uz atgriezenisko IP adresi 127.0.0.1.

Iekārta ar "pgAdmin" versiju 8.5 pakļauta ievainojamībai "CVE-2024-4215", kas ļauj uzbrucējam apiet daudzfaktoru autentifikāciju. Risku mazinošs faktors, ka ievainojamības izmantošanai jāzina lietotāja vārds un parole.

Jāveic programmatūras atjaunināšana uz pašlaik aktuālo 8.13 versiju: https://www.pgadmin.org/download/.

Novecojusi programmatūra "SoapUI"

Atvērtā koda lietojumprogrammatūras testēšanas rīks "SoapUI" tiek izmantots SOAP un REST saskarnes plaša spektra automatizētai testēšanai. Izmeklēšanā identificētas vairākas iekārtas ar novecojušu programmatūru "SoapUI", versija 5.4.0 pakļauta "Log4J" ievainojamībām "CVE-2021-44228" un "CVE-2021-45046" attālināta koda izpildi.

Pamanītas iekārtas ar "SoapUI" 5.7.1 un vecākām versijām, kas pakļautas ievainojamībai "CVE-2024-7565" (ļaunprātīgas attālinātas piekļuves risks).

Kaut arī abos gadījumos ievainojamības darbībai ir nepieciešamas lietotāju darbības, piemēram, ļaunprātīgas tīmekļa vietnes vai datnes atvēršana, stingri ieteicams izmantot jaunāko "SoapUI" versiju 5.7.2. (https://www.soapui.org/downloads/soapui/) ar izlabotiem trūkumiem.

Novecojis Intel draiveris

Vairākās iekārtās tika konstatēts novecojis Intel tīkla adaptera draiveris ar ievainojamību "CVE-2015-2291", sīkāka informācija un uzlabojuma apraksts pieejams saitē: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00051.html

Novecojis Dell draiveris

Vienā iekārtā tika konstatēts novecojis DELL BIOS draiveris ar ievainojamību "CVE-2021-21551", sīkāka informācija un uzlabojuma apraksts pieejams saitē: https://www.dell.com/support/kbdoc/en-us/000186019/dsa-2021-088-dell-client-platform-security-update-for-an-insufficient-access-control-vulnerability-in-the-dell-dbutil-driver

Novecojis atvērtā koda tīmekļa serveris "Apache"

Tika novērota novecojusi un ievainojama “Apache” versija “2.2”, kura vairs nesaņem ražotāja drošības atjauninājumus un kura pakļauta vairākām ievainojamībām, kā “CVE-2017-15710”, “CVE-2017-9798” un “CVE-2017-9788”. Ieteikums nekavējoties veikt atjaunināšanas darbus.

Novecojusi 7-Zip programmatūra

Pārbaudot uzstādītās programmatūras, vairākās iekārtās atrastas novecojušas 7-Zip failu arhivēšanas programmatūras versijas, kuras pakļautas augsta riska ievainojamībai. Vecākā ir 2019. gadā izstrādātā versija “19.00”.

2025. gada janvārī tika publicēta augsta riska “7-Zip” ievainojamība “CVE-2025-0411, 7-Zip Mark-Of-The-Web Bypass”, kuru aktīvi izmanto kiberuzbrukumos, piemēram, ļaunatūras “SmokeLoader” izplatīšanā. Ievainojamība ļauj uzbrucējam apiet Windows operētājsistēmas “Mark-of-the-Web” (MoTW) aizsardzību. Respektīvi, kad lietotājs atver ļaundabīgu “7z” arhīvu, arhivētajiem failiem netiek nodots “MoTW” tīmekļa lejupielādes marķējums, rezultātā tie netiek pārbaudīti ar “Windows SmartScreen”. Rezultātā var tikt izpildīts kods ar aktīvā lietotāja tiesībām.

Pārbaudē netika konstatēti ar šo ievainojamību saistītu arhīvu lejupielāde un atvēršana.

Ieteikums iespējami ātrāk veikt “7-Zip” atjaunināšanu uz atskaites rakstīšanas brīdī aktuālo versiju “26.01”.

Novecojusi programmatūra

Konstatētas vairākas iekārtas ar uzstādītu “Barracuda Network Access Client” novecojušām versijām, kas pakļautas kritiskai ievainojamībai “CVE-2021-42711” (https://nvd.nist.gov/vuln/detail/cve-2021-42711). Tā ļauj ikvienam nepriviliģētam lietotājam iegūt augstākās “SYSTEM” līmeņa tiesības. Ieteikums nekavējoties veikt atjaunināšanas darbus.

Novecojusi datubāžu vadības sistēma

Pārskatot infrastruktūrā izmantoto programmatūru, konstatētas iekārtas ar novecojušu, ievainojamu un ražotāja neatbalstītu atvērtā koda datubāžu vadības sistēmu “PostgreSQL”. Versiju piemēri “11.0.1.18310”, “13.0.1.20314”, kā arī “14.0.17.25050”, kas vēl tiek atbalstīta, bet sen neatjaunota. Aicinām nekavējoties pārskatīt minētās “PostgreSQL” versijas un veikt to atjaunošanas darbus.

Novecojusi failu apmaiņas FTP protokola programmatūra

Analīzes laikā atrastas novecojušas FTP programmatūras “FileZilla” gan klienta, gan servera versijas, kas rada vairākus riskus. Pāris piemēri, klienta versija 3.59.0 pakļauta ievainojamībai “CVE-2022-29620”, kas ļauj uzbrucējam izgūt SSH vai FTP paroles atklātā tekstā. Versija 3.63.1 pakļauta DLL aizvietošanas (“DLL hijacking”) ievainojamībai (sīkāk saitē: https://www.exploit-db.com/exploits/51267).

Aicinām nekavējoties pārskatīt minētās programmatūras versijas un veikt tās atjaunošanas darbus uz šobrīd aktuālajām versijām no oficiālās FileZilla tīmekļa vietnes.

Novecojusi datubāze

Konstatēta novecojusi un ievainojama atvērtā koda datubāzes “MongoDB” versija 5.0.8.0., kurai ir vairākas augstas un kritiskas ievainojamības. Piemēram, ievainojamība “CVE-2024-1351” MongoDB serverī ļauj izlaist TLS sertifikātu pārbaudi, rezultātā tiek pieņemts nepārbaudīts sertifikāts un uzbrucējs izveido neuzticamu TLS savienojumu ar “MongoDB” serveri. Sīkāka informācija par ievainojamībām saitē:

https://www.cvedetails.com/vulnerability-list/vendor_id-12752/product_id-25450/version_id-1786745/Mongodb-Mongodb-5.0.8.html

Ieteikums iespējami ātrāk veikt "MongoDB" atjaunošanu uz aktuālo versiju.

Novecojusi finanšu programma

Iekārtā atrastā programma "c:\akmens\akmens.exe" tika kategorizēta kā trojas zirga vīruss, izmeklēšanā būtisks apdraudējums sistēmai netika atrasts. Datne "akmens.exe" saistīts ar novecojušu SEB bankas finanšu programmatūru. Kaut arī tās izstrādātājs ir leģitīms, programmatūra vairs netiek lietota un ir ievērojami novecojusi, tāpēc to ieteicams no sistēmas noņemt.

Citas novecojušas lietojumprogrammas

Vairākās iekārtās atrasta novecojusi programmatūra, dažas to versijas vairs nesaņem ražotāja drošības atjauninājumus vai satur bīstamas ievainojamības. Ieteikums iespējami ātrāk infrastruktūrā veikt programmatūras versiju uzskaiti un nekavējoties ieplānot atjaunināšanas darbus. Dzīvescikla beigu ("end of life") programmatūra vai bez ražotāja atbalsta ("end of support") jāaizstāj ar tādu, kas saņem ražotāja drošības atjauninājumus.

Aicinām atbildīgo personālu par IKT drošību izvērtēt "CuteWriter" atrašanos datoros un nepieciešamību darba pienākumu veikšanai. Rekomendējam programmu dzēst un izmantot organizācijā atļauto programmatūru, kā arī pārliecināties, ka iekārtās nav uzstādīti nevēlami tīmekļa pārlūka paplašinājumi.

Apšaubāmas reputācijas lietotnes

Izmeklēšanas laikā vairākās iekārtās atklāta dažāda nevēlama vai problemātiska programmatūra. Uzņēmuma un ar to saistīto organizāciju datortīklos tika atrastas aizdomīgas, zemas reputācijas lietojumprogrammas no draudu reputācijas pārbaudes platformas "VirusTotal". Rezultāts neliecina par kaitniecisku failu, bet sniedz ieskatu par tā potenciālo bīstamību pēc reputācijas koeficienta.

Lai arī minētās programmas nenozīmē ierīču kompromitēšanu, to klātbūtne liecina par lietotāju spēju lejupielādēt un lietot bīstamas, nelicencētas programmas. Tas, savukārt, norāda uz neieslēgtu vai slikti konfigurētu programmatūras kontroles politiku (AppLocker/SRP/ACB), kas var rezultēties ļaunatūras vai nevēlamu lietojumprogrammu izpildīšanā organizācijas datoros.

Nevēlama programmatūra, sistēmas tīrīšanas rīks

Vairākos datoros atrasts sistēmas apkopes rīks "CCleaner", kuru nevar saukt par kaitniecisku, taču stingri jāizvērtē tā atrašanās iekārtās. Lieku risku rada 2017. gadā notikušais piegādes ķēdes uzbrukums pret "CCleaner". Kaut arī "CCleaner" pārsvarā tiek izmantota datora darbības optimizēšanai, bijuši gadījumi, kad tā izdzēš lietotājam vajadzīgus failus. Par izstrādātāja bezatbildību liecina pamācība produkta mājaslapā, kur "CCleaner" instalēšanai ieteikts bloķēt iebūvēto aizsardzību "Windows Defender". CERT.LV iesaka izmantot citas metodes datora darbības optimizēšanai, piemēram, "Disk Cleanup", automātiskās palaišanas jeb "Startup" pārvaldību, kā arī sistēmas labošanas rīkus "SFC" un "DISM". Izveidot atļauto programmatūras sarakstu un ieviest darbstacijās stingru grupu politiku ar "AppLocker" vai analogiem risinājumiem.

Nevēlama programmatūra "Steam"

Datorspēļu izplatīšanas platforma “Steam” un vienlaicīgi sociālais tīkls var kļūt par datora inficēšanas avotu. Uzlaužot kādas spēles izstrādātāju, no tā konta var izplatīt ļaunatūru, ko citi Steam lietotāji nenojaušot var lejupielādēt kopā ar datorspēli. Turklāt datorspēles nav saistītas ar darba pienākumu pildīšanu. Lielu papildu risku visai infrastruktūrai rada identificētais gadījums, kad lietotājs izmantoja “Steam” iekārtā ar priviliģētām (administratora) tiesībām. Programmatūra nekavējoties jādzēš no darbinieku iekārtām, jāizveido vai jāaktualizē atļauto lietojumprogrammu saraksts.

Nevēlama programmatūra “Opera Browser”

Ir iekārtas, kurās izmanto tīmekļa pārlūkprogrammu “Opera Browser”, kurai ir iebūvēta VPN funkcionalitāte. Šis tīmekļa pārlūks uzskatāms par nevēlamu, jo izstrāde saistīta ar Ķīnas Tautas Republiku. Nepieciešams dzēst pārlūku “Opera” no minētās iekārtas, kā arī uzlabot programmatūras kontroles politiku (AppLocker) uzņēmuma infrastruktūrā.

Nevēlama programmatūra “Roblox”

Četrās iekārtās atrasti populāras datorspēles “Roblox” artefakti. Aicinām atbildīgo personālu par IKT drošību izvērtēt “Roblox Studio” un “Roblox Player” nepieciešamību darba pienākumu veikšanai un atrašanos šajos datoros.

Nevēlama programmatūra “Move Mouse”

Programmatūra “MoveMouse” tiek izmantota reālas datorpeles darbības simulēšanā, ko var izmantot dažādiem nolūkiem, taču galvenais ir lietotāja klātbūtnes imitēšana. Identificētas deviņas iekārtas, kurās tika izpildīta šī programmatūra, nepieciešams izvērtēt tās nepieciešamību darba vajadzībām. Tā kā “MoveMouse” galvenā funkcija ir iekārtas noturēšana nomodā, datora ekrāns vienmēr ir atbloķēts. Tas, savukārt, rada neautorizētas piekļuves risku, kad šāda iekārta atstāta bez uzraudzības, jo piekļuvei nav nepieciešama parole. Labā prakse vienmēr veikt ekrāna bloķēšanu (taustiņu saīsne “Win+L”).

Nevēlama programmatūra “CuteWriter”

Kādā iekārtā tika konstatēta PDF datņu rediģēšanas lietojumprogramma “CuteWriter.exe”, kas bieži tiek izplatīta kopā ar reklāmu programmatūru (“adware”). Arī “CuteWriter” instalācijas procesa laikā tiek uzstādīti dažādi nevēlami tīmekļa pārlūka spraudņi.

Nelabvēlīga vai pirātiska programmatūra

Draudu medībās izpildīto programmatūru pārbaudē vienā iekārtā konstatēta iespējami ļaundabīga datne “WinMp3Packer64bit.exe” (izstrādātājs “Chris Close 2006”), kas pēc apraksta ir rīks MP3 failu rediģēšanai un saspiešanai. Datne, iespējams, nonākusi iekārtā kā daļa no citas programmatūras.

Izpildāmo datņu automātiskas startēšanas ierakstu izpētē vienā iekārtā identificēta programmatūra “Presto! PageManager” versija “9.39.20”, kuru izstrādājis Taivānā reģistrēts uzņēmums “Newsoft Technology Corporation”. Nosaukums: “Presto! PageManager v.9.39.20”, atrašanās: “C:\Program Files (x86)\NewSoft\Presto! PageManager 9.39”.

Nepieciešams pārbaudīt programmatūras nepieciešamību darba vajadzībām, to ierobežojot ar programmatūras kontroles politikas risinājumu. Ārpus ES/NATO izstrādātas programmatūras instalēšana no drošības viedokļa var būt riskanta vairāku iemeslu dēļ. Svarīgākais, ka šo valstu uzņēmumi tiek pakļauti stingrai valsts kontrolei un var būt spiesti sadarboties ar tādām valdības aģentūrām kā Krievijas drošības

dienestu (FSB), kura var likt īstenot spiegošanu un datu noplūdi (eksfiltrāciju). Vairākos gadījumos šo valstu izcelsmes programmatūra bijusi iesaistīta kiberdrošības incidentos, datu zādzībās un ļaunatūras izplatīšanā.

Pirātiska Microsoft programmatūras aktivizācija

Vairākās iekārtās konstatēts, ka lietotāji "Admin" un "Administrator" izpildījuši PowerShell skriptu no vietnes "get[.]activated.win" ar mērķi nelegāli bez maksas ļaut izmantot Microsoft produktus. Šādi rīki un skripti bieži satur mānīgu nosaukumu, lai izplatītu ļaunatūru, tas būtiski palielina kā iekārtas, tā visas infrastruktūras kompromitēšanas riskus. CERT.LV aicina par IKT drošību atbildīgās personas papildināt ugunsmūra un/vai starpniekservera aizliegumu sarakstu, ievietojot minēto domēnu. Izvērtēt konkrēto lietotāju nepieciešamību izmantot Powershell darba pienākumu veikšanai.

Microsoft Windows nelegāls aktivizācijas rīks

Digitālo pēdu nospiedumu "Amache" analīze parādīja, ka iekārtās izmantots nelegāls "MS Windows" licences aktivizēšanas rīks "KMSSS.exe", kuru aizsardzības risinājums "Windows Defender" ievietoja karantīnā. Rīks izmantots ar administratora kontu, tas ir īpaši bīstami, jo "KMSSS.EXE" iestrādātas ļaunatūras gadījumā, tā nekavējoties tiktu pie visaugstākajām "SYSTEM" privilēģijām. Šādos rīkos bieži tiek iebūvēta ļaunatūra. Situācija parāda, ka lietotāji spēj lejupielādēt un izpildīt nevēlamas programmas, tas, savukārt, liecina par programmatūras kontroles politikas trūkumu ("AppLocker" vai analogs risinājums).

Licencēšanas atslēgu ģenerēšanas programmatūra

Vienai iekārtai novēroti divi brīdinājumi par "HackTool:Win32/Keygen" un "HackTool:Win32/ Keygen!MSR" rīkiem, kas paredzēti programmatūras atslēgu ģenerēšanai un pirātiskas programmatūras nelegālai licencēšanai. Šie brīdinājumi norāda uz pirātisku programmatūru iekārtā ar nosaukumu "5GM6P". Pirātiska programmatūra bieži tiek izplatīta kopā ar ļaunatūru. Pēc "Microsoft XDR" pieejamajiem datiem secināts, ka "5GM6P" ir privāta iekārta iekļauta "Intune" pārvaldības platformā. Rezultātā detalizētāku informāciju par izsauktajiem brīdinājumiem iegūt nevar. Aktīvs apdraudējuma statuss liecina, ka apdraudējumi netika apturēti.

Nevēlama "Torrent" programmatūra

Lai arī uz iekārtām failu koplietošanas protokola "torrent" programmatūra vairs nav atrodama, vēstures dati liecina par izmantošanu tādu failu lejupielādei, kas, iespējams, nav nepieciešami darba pienākumu pildīšanai. "Torrent" datnes mēdz mānīgi norādīt citu failu saturu vai nosaukumu, lai izplatītu ļaunatūru un nelicencētu programmatūru. Šādu failu lejupielāde var būtiski palielināt kā iekārtas, tā visas infrastruktūras kompromitēšanas riskus.

Lavasoft Web Companion Assistant

Tā tiek pozicionēta kā lietotāju tīmekļa aizsardzības rīks, taču realitātē tā patvaļīgi maina pārlūka iestatījumus, injicē reklāmas un ievāc lietotāja datus. "LavaSoft" izstrādājums parasti izplatās lietotājam nezinot, jo tiek iekļauts citu programmu instalācijas pakotnēs. "LavaSoft" uzskatāms par nevēlamu un to ieteicams noņemt no sistēmas.

Lai izvairītos no nevēlamu programmu lejupielādes un izpildes, vēlams ieviest programmatūras kontroles risinājumu ("AppLocker" vai analogu).

Diska veiktspējas rīks

Datne “crystaldiskmark-8.0.4-installer_pdff-h1.exe”, kas ir instalācijas pakotne diska veiktspējas mērīšanas rīkam “CrystalDiskMark”. Ņemot vērā programmatūras uzvedību un lejupielādes avotu “SoftSonic”, to ieteicams no sistēmas noņemt.

Nevēlams PHP izstrādes vides rīks

Iekārtā atrasta tīmekļa vietņu PHP izstrādes vides “JetBrains PhpStorm” programmatūra, kas lejupielādēta no failapmaiņas torentu vietnes “rutracker[.]org”.

Potenciāli nevēlama programmatūra “PDF Architect”

Vairāki brīdinājumi par “pdfforge GmBH” izstrādāta PDF dokumentu rediģēšanai paredzētā rīka “PDF Architect 9” instalācijas pakotni “architect-setup.exe”. Tas tika bloķēts kā apdraudējums “PUABundler:Win32/Playanext” saistībā ar citas programmatūras uzstādīšanu. Iemesls trauksmes brīdinājumiem bija “PDF Architect” uzstādīšanas laikā lejupielādētas papildus datnes, piemēram, citi “pddforge GmBH” izstrādājumi – pārlūkprogrammu un virtuālo disku integrācijas. Aicinām izvērtēt minētā rīka nepieciešamību darba vajadzībām.

PDFsam Enhanced 7

Konstatēta .PDF datņu rediģēšanas programmatūra “PDFsam Enhanced 7”, kas bieži tiek izplatīta kopā ar reklāmas ļaunatūru (“adware”), proti, instalēšanas procesā paralēli uzstādīti, dažādi nevēlami tīmekļa pārlūka paplašinājumi.

Ieteikums par IKT drošību atbildīgajam personālam izvērtēt “PDFsam Enhanced 7” atrašanos iekārtā un nepieciešamību darba pienākumu veikšanai. Programmu no iekārtas dzēst un izmantot tikai iestādē atļauto risinājumu.

Mouse Jiggler

Programmatūra tiek izmantota reālas datorpeles darbības simulēšanā, ko var izmantot dažādiem nolūkiem, taču galvenais ir lietotāja klātbūtnes imitēšana. Identificētas sešas iekārtas, kurās tika izpildīta šī programmatūra, nepieciešams izvērtēt tās nepieciešamību darba vajadzībām. Tā kā “Mouse Jiggler” galvenā funkcija ir iekārtas noturēšana nomodā, datora ekrāns vienmēr ir atbloķēts. Tas, savukārt, rada neautorizētas piekļuves risku, kad šāda iekārta atstāta bez uzraudzības, jo piekļuvei nav nepieciešama parole. Labā prakse vienmēr veikt ekrāna bloķēšanu (taustiņu saīsne “Win+L”).

Battlegrounds

Pārskatot iekārtu automātisko procesu startēšanu līdz ar iekārtas ieslēgšanu, identificēts draiveris “xhunter1.sys” un serviss “ucldr_battlegrounds_gl.exe”, kurus parakstījis uzņēmums “Wellbia.com Co., Ltd.”, pazīstams ar tiešsaistes datorspēļu pretkrāpšanās (“anti-cheat”) programmatūras izstrādi. Kādā iekārtā identificētas datnes saistītas ar datorspēli “Battlegrounds”. Ieteikums nekavējoties dzēst programmatūru un uzlabot lietotņu kontroles politiku.

zetupd.exe

Divās iekārtās tika atrasts izpildfails “zetupd.exe”, kura saistīta ar Krievijā ražotu astroloģijas programmatūru “AstroZet” (https://astrozet.net/). Lai arī tas nav apliecinājums par kādu konkrētu ierīču kompromitēšanu, tas nozīmē, ka lietotāji spēj lejupielādēt un lietot bīstamas un nelicencētas programmas. Tas, savukārt, norāda par vāji konfigurētu vai trūkstošu programmatūras kontroles politiku (“AppLocker” vai analogu risinājumu).

Felix The Cat

Datora programma ar animētu kaķa tēlu, kas paredzēta lietotāju izklaidei. Piesaista uzmanību ar animācijām, tiešsaistes saitēm un satura kopīgošanas funkcijām. Programmas funkcionalitāte līdzinās ļaunatūras darbības pazīmēm, ko norāda arī draudu analīzes vietne “VirusTotal”. Šāda veida programmatūru izmantošana ir riskanta, jo datnes mēdz mānīgi norādīt failu saturu un nosaukumu, ko izmanto ļaunatūras un nelicencētas programmatūras izplatīšanai. Tādu failu lejupielāde būtiski palielina kā iekārtas, tā visas infrastruktūras kompromitēšanas riskus.

Yandex

Programmatūra “YandexPackLoader” ir saistīta ar “Yandex” pārlūkprogrammu, ko izmanto tās pārvaldības komponenšu ielādēšanai. Infrastruktūrā atrastas divas iekārtas ar “Yandex” programmatūru, kas izstrādāta Krievijā ar tās valdības atbalstu. Šāda veida programmatūras izmantošana paaugstina datu privātuma un drošības riskus.

Tīmekļa pārlūks “Atom”

Analoģiski augstāk minētajam, Krievijas uzņēmuma “Mail.Ru” izstrādāti tīmekļa pārlūki “Atom” atrasti divās iekārtās. Tās izmantošana nav ieteicama paaugstinātu datu privātuma un drošības risku dēļ.

WPS Office

Ķīnas uzņēmuma “KingSoft” produkts “WPS Office” paredzēts darbam ar dokumentiem. 2024. gadā tika atklātas kritiskās ievainojamības, kuras aktīvi izmantoja uzbrucēji. Valsts Drošības Dienesta ieteikums ir izmantot programmatūru tikai no ES, NATO un partneru valstīm. Nekādā gadījumā neizmantot programmatūru no izcelsmes valsts Krievija vai Ķīna.

Free Download Manager

Programmatūra, kas paredzēta datņu lejupielādei no tīmekļa, tā atbalsta “torrent” datņu lejupielādes, kā arī tā nodrošina starpniekservera (proxy) funkcionalitāti. Šāda veida programmatūra rada papildus riskus iestādes infrastruktūras drošībai. Lai arī programma nav ļaundabīga, ar to var tikt lejupielādētas, piemēram, “torrent” datnes. Turklāt iebūvētā starpniekservera (“proxy”) funkcionalitāte rada draudus iestādes ugunsmūrim.

ScreenRec

Programmatūra paredzēta iekārtas ekrāna ierakstīšanai, visbiežāk datorspēļu vai apmācības materiālu veidošanai video formātā. Tomēr tā var tikt izmantota arī ļaunprātīgi, lai bez lietotāja ziņas ierakstītu ekrānu un video nodotu trešajām pusēm.

Dropbox

Mākoņkrātuves pakalpojums, kas ļauj lietotājiem tiešsaistē glabāt, koplietot un sinhronizēt failus. Tiešā viedā programmatūra nerada draudus, taču to var izmantot konfidenciālas informācijas nodošanai trešajām pusēm lietotājām gan tīšuprāt, gan neapzināti.

Wargaming Platform

Iekārtās konstatēta Baltkrievijas uzņēmuma "Wargaming Platform" (wargaming.net) tiešsaistes datorspēļu platforma, kur ir iespējams spēlēt dažādas militārās stratēģijas spēlēs (piemēram, "World of Tanks"). Aicinām par IKT drošību atbildīgās personas nekavējoties dzēst programmu un uzlabot lietotņu kontroles risinājumu ("AppLocker" vai analogu).

Citas datorspēles un saistītā programmatūra

Izmeklēšanā, analizējot iekārtās izpildīto programmatūru, konstatētas citu datorspēļu un tiešsaistes spēļu vai to lejupielādes platformu izmantošana. Aicinām par IKT drošību atbildīgās personas nekavējoties dzēst programmu un uzlabot lietotņu kontroles risinājumu ("AppLocker" vai analogu).

WebCompanionInstaller

Iekārtās izpildītas datnes "WebCompanionInstaller.exe" (pilna atrašanās "\users* \appdata\roaming\lavasoft\web companion\application\ webcompanioninstaller.exe"), programmatūra paredzēta lietotāju aizsardzībai pret dažādiem kiberdraudiem gan tīmekļa vietnēs, gan interneta lejupielādēs. Tā bieži tiek izplatīta ar iebūvētu papildu nevēlamu programmatūru ("PUP") vai reklāmprogrammatūru ("adware"). Drošības platforma "Virustotal" šo datni ar rezultātu 12/17 atzīmē kā potenciāli bīstamu. Padziļināta iekārtas analīzes neuzrādīja ļaunatūru vai inficēšanās pazīmes, tomēr aicinām par IKT drošību atbildīgās personas programmu dzēst un uzlabot lietotņu kontroles risinājumu ("AppLocker" vai analogu).

Tīkla skenēšanas programmatūra

Konstatēta šāda tīkla skenēšanas programmatūras izmantošana iestādes infrastruktūrā: "Ipscan", "Nmap", "Advanced IP Scanner". Kaut arī tās izmanto tīkla administrēšanas darbos, tomēr šos rīkus uzbrucēji var tik izmantot ļaunprātīgi, veicot iestādes tīkla izpēti un ievainojamību meklēšanu. Ieteikums ierobežot šo rīku izmantošanu lietotājiem, kas neveic iestādes tīkla uzturēšanu.

Tīkla iekārtu "MikroTik" ekspluatācijas datnes

Iekārtās izmeklēšanas laikā atrastas vairākas ar uzbrukumiem "MikroTik" maršrutētāju operētājsistēmai "RouterOS" saistītas datnes. Tās satur skriptus, kas nolasa "MikroTik" ierīces lietotājvārdus un paroles. Skripti izmanto 2018. gadā atklāto ievainojamību "CVE-2018-14847", kas ietekmē visus "MikroTik" maršrutētāju operētājsistēmu "RouterOS" versijas vecākas par "6.42". Saziņā ar administratoriem tika noskaidrots, ka rīkus izmantoja leģitīmiem testiem. Kaut arī šāda pārbaude vērtējama pozitīvi, pēc rīku izmantošanas tos no darba iekārtas jādzēš. Testus vēlams veikt no atsevišķas, nodalītas iekārtas, piemēram, virtuālās mašīnas.

Windows IIS serveri bez satura

Veicot izmeklēšanu, identificētas 12 iekārtas ar aktīvu "Microsoft IIS" pakalpojumu, taču ar tukšu izvietoto tīmekļa vietni bez satura. Iekārtām iestatīta noklusējuma dokumentu direktorija "C:\inetpub\wwwroot" bez failiem saturā. Nepieciešams izvērtēt šādu servisu izvietošanas nepieciešamību. Kiberdrošības labā prakse ir uzbrukuma virsmas samazināšana, tādēļ ieteikums slēgt liekās tīmekļa vietnes.

LinPEAS rīka izmantošana

Linux "Privilege Escalation Awesome Script" jeb "LinPEAS" ir atvērtā koda rīks. Tas pārbauda dažādas konfigurācijas un drošības iestatījumu Linux sistēmās ar nolūku atrast iespējamās vājās drošības vietas, kas varētu ļaut iespējamam uzbrucējam iegūt augstākas priviliģētas piekļuves tiesības. Pēc Linux iekārtu komandrindas vēstures pārbaudes, konstatēta "LinPEAS" rīka skripta "linpeas.sh" izpilde 13 iekārtās.

Apšaubāmas reputācijas lietotnes

Izmeklēšanas laikā vairākās iekārtās atklātas dažāda nevēlama vai problemātiska programmatūra. VI datortīklā atrastas aizdomīgas, zemas reputācijas lietojumprogrammas no draudu reputācijas pārbaudes platformas "VirusTotal". Rezultāts neliecina par kaitniecisku failu, bet sniedz ieskatu par tā potenciālo bīstamību pēc reputācijas koeficienta.

Piemēri:

SHA1	Nosaukums	Direktorija	Reputācijas koef.
a7f24583dd93c03ba44f644a75f99ad4322e33a2	rserver3.exe	c:\windows\syswow64\rserver30\rserver3.exe	9/71
b9fca8774bdc3df737fa930255e2924e7ddf738a	gpg4win-4.0.0.exe	d:\users*\downloads\gpg4win-4.0.0.exe	3/69
545359cd68d0ee37f4b15e1a22c2c9a5fda69e22	setup-lightshot.exe	c:\users*\downloads\setup-lightshot.exe	6/72
ff85f30308754f402eb6ee1e94b38f23ed33b36c	LaunchPad.exe	c:\users*\desktop\a.zÄ⍰lÄ«te\launchpad.exe	3/72
ce215dd4e5cba017903a7749235c36808280bbf9	RemoteDeployment_x86.exe	c:\program files (x86)\lansweeper\service\deployers\remotedeployment_x86.exe	5/71

Lai arī minētās programmas nenozīmē ierīču kompromitēšanu, to klātbūtne liecina par lietotāju spēju lejupielādēt un lietot bīstamas, nelicencētas programmas. Tas, savukārt, norāda uz neieslēgtu vai slikti konfigurētu programmatūras kontroles politiku (AppLocker/SRP/ACB), kas var rezultēties ļaunatūras vai nevēlamu lietojumprogrammu izpildīšanā organizācijas datoros.

Nevēlami tīmekļa pārlūka spraudņi

Uzņēmuma infrastruktūrā izmantotajās iekārtās atrasti liels skaits dažādu tīmekļa pārlūkprogrammas "Chrome" paplašinājumu, no kuriem, visticamāk, vairums nav nepieciešams darba pienākumu veikšanai. Identificētie paplašinājumi saistīti ar datorspēlēm, video straumēšanu, "Torrent" tīkliem, kriptovalūtu maciņiem, VPN risinājumiem, attālinātu iekārtas kontroli un vēl daudzi citi. Šāda prakse rada papildu riskus organizācijas kiberdrošībai, jo pārlūku spraudņiem ir plašas piekļuves tiesības, piemēram, pilnai interneta

pārlūkošanas vēsturei, paroļu pārvaldībai un pat vietņu satura manipulācijām. Šādi paplašinājumi var būt sākotnēji izstrādāti kā ļaunprātīgi vai tikt uzlauzti, liela daļa spraudņu ievāc un nosūta lietotāja datus trešajām pusēm.

CERT.LV aicina rūpīgi izvērtēt tīmekļa pārlūka paplašinājumu izmantošanas nepieciešamību, darba vajadzībām nevajadzīgos dzēst no lietotāju iekārtām.

Aktīvajai direktorijai pievienotās Windows operētājsistēmās var centralizēti pārvaldīt "Google Chrome" paplašinājumus ar grupu politikas administrēšanas veidni (ADMX), ko lejupielādē no Google tīmekļvietnes. Konfigurācijā var norādīt atļauto spraudņu sarakstu, kurus iepriekš IT administrators pārbaudījis.

Papildu informācija par konfigurēšanu sniegta sadaļā "Vispārīgie ieteikumi".

Ievainojama programmatūra "Greenshot"

Operētājsistēmai "Windows" izstrādāts atvērtā koda ekrāna attēlu uzņemšanas rīks "Greenshot" piedāvā lietotājiem ne tikai fiksēt ekrāna attēlus, bet arī veikt to rediģēšanu. Izmeklēšanas laikā vairākās iekārtās atrasta "Greenshot" versija ievainojama ar "CVE-2023-34634", kad ļaunprātīgas datnes atvēršana izpilda arī ļaunatūru.

Programmatūras izstrādātāji kļūdu nav izlabojuši, kas liecina par sliktu kiberdrošības praksi. Lai arī ievainojamību īstenot var ar lietotāja iesaisti (atverot datni), ieteicams šādu programmatūru neizmantot. Ekrāna uzņēmumu izveidei ieteicams izvēlēties citu alternatīvu, bet labā prakse ir lietot Windows iebūvēto lietojumprogrammu "Izgriešanas rīks" (aktivizē ar taustiņu saīsni "Win + Shift + S"), kas samazina izmantoto programmatūru daudzumu un arī uzbrukuma virsmu.

Nepārvaldīti tūlītējas ziņojumapmaiņas risinājumi

Draudu medību laikā kāda uzņēmuma iekārtās notika programmatūras analīze, tika meklēta gan pašlaik aktīva, gan vēsturiski izpildīta programmatūra. Infrastruktūrā konstatētas šādas izmantotas tūlītējās ziņojumapmaiņas lietojumprogrammas: "Skype", "WhatsApp", "Signal", "Facebook", "TwitchClient", "Telegram (izcelsmes valsts Krievija).

CERT.LV iesaka izveidot stingru ziņojumapmaiņas politiku ar konkrētiem izmantošanas noteikumiem. Pārliecināties par "Telegram" nepieciešamību darba pienākumiem. Pārbaudīt arī "Skype", "WhatsApp", "Signal", "Facebook" un "TwitchClient" izmantošanas pamatojumu.

"Telegram" gadījumā iesakām neizmantot produktus, kas izstrādāti Eiropas Savienībai un NATO nedraudzīgās valstīs. Detalizēta informācija sniegta sadaļā "Vispārīgie ieteikumi".

Nedroša piekļuves datu glabāšana

Linux operētājsistēmā

Veicot operētājsistēmas "Linux" komandrindas "bash" vēstures pārbaudi, trim iekārtām "ftp2", "www.*.lv", "test" tika konstatēta paroles glabāšana atklātā tekstā. Ieteikums izmantot paroļu maskēšanu (obfuskāciju) vai terminālī ievadīt paroles, nesaglabājot vēsturi, kas var atklāt lietotās paroles, API atslēgas vērtības un citu sensitīvu informāciju. Ierakstu vēsturi var atslēgt, piemēram, iestatot sistēmas vides argumentus "HISTSIZE" un "HISTFILESIZE" vērtību "0".

Linux komandrindas (bash) vēstures pārbaudē (.bash_history), tika atrastas vairākas paroles atklātā tekstā. Tas var radīt privilēģiju palielināšanas un noturēšanas iespējamību potenciāliem uzbrucējiem. Ieteikums terminālī vai skriptos lietot paroles paslēpšanas mehānismus vai nesaglabāt izpildīto komandu vēsturi, kas var atklāt lietotās paroles, API atslēgu vērtības un citu sensitīvu informāciju. Nesaglabāt vēsturiskos komandu ierakstus var panākt, iestatot sistēmvides argumentus HISTSIZE un HISTFILESIZE vērtību "0".

Ieteikums glabāt piekļuves datus aizsargātos vides mainīgajos ("environment variables") vai lokālās paroļu krātuvēs (piemēram, Windows akreditācijas datu pārvaldniekā, macOS atslēgu krātuvē vai citā paroļu pārvaldniekā), nolasot piekļuves datus tikai skripta izpildes laikā. Papildu ieteikums atiestatīt "administrator", un citu iesaistīto lietotāju piekļuves datus.

Windows operētājsistēmā

Citā gadījumā analizējot Powershell vēsturi, konstatēta paroles lietošana atklātā tekstā. Tas palielina uzbrukumu virsmu, radot uzbrucējiem privilēģiju paaugstināšanas un noturēšanas iespējas. Zinot konkrēto paroli, uzbrucējs var piekļūt "vCenter Server" sistēmai kaitniecisku darbību veikšanai.

Kādā iekārtā administratora lietotājs izpildīja komandu: "Connect-VIServer -server vmware4.*.lv -user root -pass asdasd".

Ieteikums terminālī vai skriptos lietot paroles paslēpšanas mehānismus vai nesaglabāt izpildīto komandu vēsturi, kas var atklāt lietotās paroles, API atslēgu vērtības un citu sensitīvu informāciju. Nesaglabāt vēsturiskos komandu ierakstus var panākt, iestatot sistēmvides argumentus HISTSIZE un HISTFILESIZE vērtību "0".

Konkrētajā "VMware PowerCLI" kontekstā var izmantot "ViCredentialStore" vai citas Powershell iespējas, piemēram, "Get-Credential" paroli prasītu ievadīt vai nu atsevišķi interaktīvā veidā, vai nolasīt no droša piekļuves datu pārvaldnieka "Windows Credential Manager".

PowerShell gadījums

Kādā uzņēmumā, analizējot Powershell komandu izpildes vēsturi, tika atrastas paroles atklātā tekstā. Ieteikums veikt to maiņu, lai novērstu neautorizēto piekļuvi. Piemēram, kādā iekārtā lietotājs "Administrator" izpildīja komandu: "ktpass -princ HTTPS/* -mapuser krb5eso -pass admin1234 -ptype KRB5_NT_PRINCIPAL -in c:\temp\dat.keytab -out c:\tas\dat.keytab".

Tālākā Windows Powershell komandu vēstures analīzē atrasta "Graylog" servisa "API" atslēga atklātā tekstā. Uzbrucējam tas var nodrošināt iespēju piekļūt Graylog sistēmai un veikt kaitnieciskas darbības.

Paroļu un API atslēgu pieejamība atklātā tekstā palielina uzbrukumu virsmu un rada uzbrucējam privilēģiju paaugstināšanas un pastāvīgās pieejas iespējas. Piemēram, lietotājs "admin" izpildīja komandu: "msiexec.exe /i graylog.msi SERVERURL=https://g2a1e.*.lv:9000/api APITOKEN= qwerty123 TAGS=server", avots: "C:\Users\ *\AppData\ Roaming\ Microsoft\Windows\ PowerShell\ PSReadLine\ ConsoleHost_history.txt"

Ieteikums, ievadot paroles atslēgas (tokenus) terminālī vai skriptos, izmantot paroļu paslēpšanas mehānismus vai nesaglabāt izpildīto komandu vēsturi, kas var atklāt lietotās paroles, API atslēgu vērtības un citu sensitīvu informāciju. Powershell gadījumā var izmantot, piemēram, "Read-Host" ar parametru "-AsSecureString". Šādi lietotājam manuāli jāievada parole, taču tā neparādīsies izpildīto komandu vēsturē.

Zemas reputācijas domēnu pieprasījumi

Draudu medībās notika iekārtu tīmekļa pārlūkprogrammu vēstures analīze, atrastas apmeklētas zemas reputācijas mājaslapas un tādi domēni, kas vēsturiski iesaistīti pikšķerēšanas kampaņu aktivitātēs vai ļaunatūras izplatīšanā.

Kaitīgā domēna vārds
yourmanloverfind.top
dqryzb.top
garrafaoutsins.top
bp57w6ntskf7.top
topnotchdating.top
kilimanjarospot.top
winrewardnewcash.top
elementalhammer.top
tdspa.top
pullerkwazoku.top
ednvh.top
fenrawrye.live
freelivechat08.buzz
mynextlove.xyz
qvsep.xyz
dateguys.online
eu.got-to-be.net
fouwaboozi.com
gloamtazab.com
toapodazoay.com
worldfreshjournal.com

Iesakām ieviest stingrāku tīmekļa lietošanas politiku ar preventīviem risinājumiem, piemēram, pārlūka spraudnis "Ublock Origin Lite" (https://github.com/uBlockOrigin/uBOL-home) ir atvērta pirmkoda risinājums, kas, izmantojot dažādus nevēlamu domēnu avotus, brīdina lietotāju par bīstamu vietņu apmeklēšanu. Šos domēnus var ievietot iestādes ugunsmūra vai starpniekservera aizliegtajos sarakstos.

Tā kā tika analizēta iekārtu tīmekļa pārlūkprogrammu vēsture, atrastas sešas iekārtas ar pornogrāfiska rakstura meklēšanu vai vietņu apmeklēšanu:

Kā minēts iepriekš, arī šajā gadījumā iesakām ieviest stingrāku interneta izmantošanas politiku, šāda veida domēnus ievietojot iestādes ugunsmūra vai starpniekservera melnajos sarakstos.

Savukārt, sarakstus var papildināt, piemēram, ar datiem no "Github" vai citiem projektiem:

- https://github.com/blocklistproject/Lists;
- https://github.com/Bon-Appetit/porn-domains.

Autentifikācija ar lokālo administratora lietotāju

Vairākās iekārtās konstatēta autentificēšanās ar iebūvēto administratora kontu, ko Windows labās prakses vadlīnijas iesaka atspējot. Administratora tiesību nepieciešamības gadījumā ieteicams izmantot Windows nestandarta lietotāju, kam ir piešķirtas administratora tiesības.

Publiski eksponēts "GitLab" pakalpojums

Atvērtā koda projektu pārvaldības platforma "GitLab" izmantota, lai veiktu programmatūru pirmkoda glabāšanu un uzturēšanu. Izmeklēšanā atklāts, ka "GitLab" instance iekārtai "autodiscover.*.lv" ir pieejama tīmeklī. Publiski eksponēti pakalpojumi ir pakļauti uzbrucēju darbībām, kas var radīt drošības riskus, turklāt jebkura servisa izvietošana internetā palielina uzbrukuma laukumu. Labā prakses vadlīnijas iesaka šādus pakalpojumus izvietot lokāli, no ārpuses piekļūstot ar VPN tuneli. Stingrs ieteikums iestatīt daudzfaktoru autentifikāciju.

Publiski eksponēts "Microsoft Exchange" pakalpojums

Ziņojumapmaiņas platforma "Microsoft Exchange" nodrošina e-pastu, kalendāru u. c. biznesa sadarbības pakalpojumus. Izmeklēšanā konstatēts, ka iekārtas "epasts.*.lv" publiskā tīmeklī pieejama "Microsoft Exchange" instance. Internetā eksponēti pakalpojumi ir pakļauti uzbrucēju darbībām, kas var radīt drošības riskus un palielina uzbrukuma iespējas. Labā prakse ir izvietot šādus servisus lokāli vai izmantojot VPN tuneli. Tāpat, nepieciešams iestatīt daudzfaktoru autentifikāciju.

Piekļuves tiesības "MS Exchange" lietotāju pastkastēm

Tā kā draudu medības atklāja "Microsoft Exchange" instances pieejamību no publiskā tīmekļa, tika veikta padziļināta servera "EXCH2016.*.lv" audita pierakstu analīze, jo nevar izslēgt neleģitīmu pieslēgumu iespējamību. "MS Exchange" audita pierakstu analīze nekonstatē neautorizētas pieslēgšanās gadījumus, tomēr vairākām lietotāju pastkastītēm (noklusējuma vai pašu izveidotajām mapēm) atrastas, iespējams, pārāk plašas piekļuves tiesības – citi autentificēti vai neautentificēti lietotāji var lasīt/modificēt/dzēst saturu. Kibernoziedznieks potenciāli var iegūt pieeju slepenai organizācijas informācijai un autentifikācijas datiem (ja e-pastā pārsūtīta paroles atklātā tekstā), rezultātā uzbrucējam dodot priviliģēta lietotāja tiesības un iespēju pārvietoties tālāk organizācijas IKT infrastruktūrā.

Lietotāju grupu "Default" vai "Anonymous" jebkuras pieejas tiesības (izņemot "No permissions" vai "None") ir rūpīgi jāizvērtē, jo "Default" grupa tiek attiecināta uz jebkuru autentificētu lietotāju, savukārt, "Anonymous" tiek attiecināta pilnīgi uz jebkuru (t.sk. viesu) lietotāju.

CERT.LV iesaka atbildīgajam personālam par IKT drošību pārbaudīt faktisko situāciju, t.i., vai konfigurācija atbilst lietotāju darba pienākumu veikšanai. Ja piešķirtās tiesības ir pārāk plašas, tās nepieciešams noņemt vai iestatīt noklusējuma vērtības, piemēram, "Default – None" un "Anonymous – None".

Datnes ar būtisku infrastruktūras informāciju

Izmeklēšanā identificēts, ka Aktīvas Direktorijas drošības novērtējuma (ievainojamības, konfigurācija, nepilnības, u.c.) rīka "PingCastle" izveidotās atskaites pieejamas iekārtā "win10.*.lv", mapē "C:\PingCastle\3_2_0_1\ad_hc_*.lv.html". Iekārtas kompromitēšanas gadījumā uzbrucējs piekļūtu kritiski svarīgai informācijai par domēna uzbūvi un konfigurāciju, ko tālāk var izmantot ļaunprātīgiem nolūkiem. Ieteikums atskaites no iekārtas vai nu dzēst, vai nodrošināt lasīšanas tiesības ierobežotam darbinieku lokam pienākumu pildīšanas vajadzībām.

DNS konfigurācija

Izmeklēšanā identificētas 56 iekārtas ar, iespējams, kļūdainu DNS konfigurāciju, kur publisks DNS serveris iestatīts 25 iekārtām kā primārais un 31 iekārtai kā sekundārais serveris. Labā prakse iesaka visām iekārtām iestatīt iekšējo DNS serveri.

Plašāk ieteikumi drošības stiprināšanai sniegti sadaļā "Vispārīgie ieteikumi".

Iespējami uzbrukumi un ievainojamību skenēšana

Žurnālfailu ierakstu atlasē pēc nesekmīgajiem autentifikācijas mēģinājumiem tika apkopoti pieteikšanās jeb ielogošanās mēģinājumi no ārvalstu IP adresēm. Riska faktors īstenotas autentifikācijas gadījumā, ka uzbrucējs tiek pie iespējas nolasīt vai labot datus, vai pat administratora privilēģijām. Pozitīvais secinājums, ka sekmīgie autentifikācijas gadījumi nav atrasti.

Autentifikāciju žurnālfailu analīzē redzami tādi detalizēti dati kā nesekmīgo pieteikšanās mēģinājumu skaits.

Nepieciešams pēc būtības izvērtēt nesekmīgās autentifikācijas lokālajā tīklā - neraksturīgs laiks, mēģinājumu skaits, lietotāja vārds utt. Nevēlama prakse ir publiski eksponēti serveri un VPN neizmantošana.

Nedroša infrastruktūras pārvaldība

Dažādu pārvaldības rīku izmantošana īstenotas kompromitēšanas gadījumā sniedz uzbrucējam plašas iespējas lietot tās pašas lietojumprogrammas, lai pārvietotos tālāk infrastruktūrā vai izplatītu ļaunatūru. Tāpat, IKT drošības personālam ir ievērojami grūtāk izsekot uzbrucēja digitālajām pēdām. Dažās darbstacijās konstatētā "Sysinternals PsExec" lietošana norāda uz iepriekš aprakstīto nevēlamo administrēšanas praksi.

CERT.LV aicina atbildīgo personālu izvērtēt nepieciešamību administrēšanā izmantot "PsExec" rīku uzskaitītajās iekārtās. Iesakām papildus izveidot stingru attālinātās piekļuves izmantošanas politiku.

Nedroša Linux operētājsistēmas pārvaldība

Vienā Linux iekārtā novērota "bash" sistēmas "chmod" komandrindas nepamatota "777" parametra izmantošana, kas rada vairākus drošības riskus, bet galvenais ir pilnas faila modificēšanas un izpildes tiesības visiem iekārtas lietotājiem.

Iekārtas kompromitēšanas gadījumā uzbrucējs var failu nolasīt, pārkopēt (eksfiltrēt), modificēt vai ievietot tajā un pēc tam izpildīt kaitnieciskas komandas. Piemērs, iekārtā ar nosaukumu "spkcmoodle" izpildīta komanda "chmod -R 777 /var/www/moodledata/*".

Ieteikums ierobežot piekļuvi, balstoties uz lietotājiem vai grupām ar attiecīgo nepieciešamību piekļūt konkrētiem failiem un direktorijām – minimālas pieejas tiesības darba pienākumu izpildīšanai.

Programmatūru ievainojamības

Programmatūra no ES nedraudzīgām valstīm

Krievijā (RU) un Ķīnā (CH) izstrādātas programmatūras instalēšana no drošības viedokļa var būt riskanta vairāku iemeslu dēļ. Svarīgākais, ka šo valstu uzņēmumi tiek pakļauti stingrai valsts kontrolei un var būt spiesti sadarboties ar tādām valdības aģentūrām kā Krievijas drošības dienestu (FSB), kura var likt īstenot spiegošanu un datu noplūdi (eksfiltrāciju).

Vairākos gadījumos šo valstu izcelsmes programmatūra bijusi iesaistīta kiberdrošības incidentos, datu zādzībās un ļaunatūras izplatīšanā. Lietotņu piemēri: Yandex un mail.ru (RU), WPS Office (CN).

Valsts Drošības Dienesta ieteikums ir izmantot programmatūru tikai no ES, NATO un partneru valstīm. Nekādā gadījumā neizmantot programmatūru no izcelsmes valsts Krievija vai Ķīna.

Windows servisu izveides rīks

Trešo pušu rīka “NSSM” (“Non-Sucking Service Manager”) funkcija ir nodrošināt datora operētājsistēmā konkrētas programmatūras iestatīšanu servisa režīmā. Papildu “NSSM” funkcionalitāte ir servisa statusa pārbaude un automātiska kļūdu apstrāde, maksimāli nodrošinot pakalpojuma pieejamību. Uzbrucēji ļoti bieži izmanto “NSSM” pastāvīgās pieejas nodrošināšanai, uzstādot ļaunatūru kā servisu, lai noturētos sistēmā pēc iekārtas restarta. Draudu rīkotāji ar “NSSM” var modificēt iekārtā jau esošus leģitīmus servisus, pielāgojot tos saviem nolūkiem.

Cita trešo pušu rīka “SrvAny” funkcija ir nodrošināt datora operētājsistēmā konkrētas programmatūras iestatīšanu servisa režīmā. Papildu “SrvAny” funkcionalitāte ir servisa statusa pārbaude un automātiska kļūdu apstrāde, maksimāli nodrošinot pakalpojuma pieejamību. Uzbrucēji ļoti bieži izmanto “SrvAny” pastāvīgās pieejas nodrošināšanai, uzstādot ļaunatūru kā servisu, lai noturētos sistēmā pēc iekārtas restarta. Draudu rīkotāji ar “SrvAny” var modificēt iekārtā jau esošus leģitīmus servisus, pielāgojot tos saviem nolūkiem.

Lai arī šīs programmas neliecina par ierīču kompromitēšanu, to klātbūtne norāda lietotāju spēju lejupielādēt un lietot bīstamas, nelicencētas programmas. Tas, savukārt, norāda uz programmatūras vāju konfigurētu kontroles politikas trūkumu vai vāju konfigurāciju.

CERT.LV ir informācija par šī rīka aktīvu izmantošanu Krievijas atbalstītā grupējuma “APT29” kiberoperācijās, tāpēc “NSSM” lietošanai tiek pievērsta pastiprināta uzmanība.

Nevēlami pārlūka spraudņi

Uzņēmuma infrastruktūras ierīcēs tika atrasti vairāki tīmekļa pārlūka paplašinājumi, kuri ne vienmēr ir kaitnieciski, taču to nepieciešamība administratoriem kārtīgi jāizvērtē. Paplašinājumiem ir piekļuve lietotāja datiem un pārlūkošanas vēsturei, tāpat tos var izmantot nesankcionētu darbību veikšanai, piemēram, konfidenciālas informācijas nopludināšanai. Spraudņu lejupielādei no trešo pušu vietnēm jābūt aizliegtai.

Atsauktie draiveru sertifikāti

Draiveru sertifikātu atsaukums var rasties vairāku iemeslu dēļ, visbiežākie ir drošības apsvērumi, ja tajos tiek atklātas ievainojamības vai ļaunprātīgs kods.

Uzbrucēji bieži izmanto draiverus, lai uzstādītu un izplatītu ļaundabīgu programmatūru, ietekmētu sistēmu darbību, atslēgtu aizsargmehānismus vai citādi bojātu sistēmas.

Draiveri lielākoties darbojas ar augstākām privilēģijām nekā standarta lietotāja programmatūra. Ieteikums pārskatīt draiveru nepieciešamību, iespēju robežās veicot to atjaunināšanu.

Papildu ieteikums iestatīt ievainojamu draiveru bloķēšanu (“Microsoft Vulnerable Driver Blocklist”) reģistra atslēgā “VulnerableDriverBlocklistEnable”, sīkāka informāciju saitē: https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/design/microsoft-recommended-driver-block-rules

Pretvīrusu programmatūra

Infrastruktūrā atrasti vairāki pretvīrusu pakalpojumu risinājumi, par to liecina vairāki artefakti jeb digitālie pēdu nospiedumi. Galvenais, visvairāk izplatītais pretvīrusa risinājums ir “Windows Defender”. Dažās iekārtās atklāti citi aktīvi pretvīrusu risinājumi, kā “Malwarebytes”, “McAfee”, “Eset”, “BitDefender”, “COMODO Internet Security” un “AO Kaspersky Lab”. Ieteikums izmantot tikai vienu antivīrusa programmatūras risinājumu, kas uzstādīts un centrāli pārvaldīts visās Windows iekārtās. Jāizvairās no produktiem, kuru izcelsme ir ārpus Eiropas Savienībai draudzīgo valstu saraksta.

Datorspēles

Uzņēmuma infrastruktūrā Draudu medību laikā konstatētas vairākas datorspēļu lietotnes. Lai arī datorspēles pēc būtības nav kaitnieciskas, tās nav nepieciešamas darba pienākumu pildīšanai, tām nav jāatrodas organizācijas iekārtās. Digitālo pēdu "Amcache" nospiedumos atrastās datorspēles norāda, ka tās bijušas uzstādītas un darbinātas.

Par datorspēlēm liecina arī izņēmumu nosacījumi Windows ugunsmūrī.

Neaktīvi autostarta ieraksti

Automātiska starta ierakstu pārvaldes rīks "Autoruns" vairākkārt atradis programmatūru, kas ir konfigurēta automātiska izpildes (palaišanas) režīmā arī pēc sistēmas pārstartēšanas, izslēgšanas vai lietotāja pieteikšanās. Ieraksti ir aktīvi, taču sekmīgi nedarbojas, jo izpildfails vairs sistēmā neeksistē (kļūda "File not found").

Vēsturiski konfigurētie automātiskie iestatījumi, visticamāk, palikuši pēc izpildfaila noņemšanas no sākotnējās mapes. Ieteikums **izdzēst** visus neaktīvos "Autoruns" ierakstus.

Ieteikumi

Plašāk ieteikumi drošības stiprināšanai sniegti sadaļā "Vispārīgie ieteikumi".

Papildu ieteikums infrastruktūras uzraudzībai:

- **Ieviest iekārtu un programmatūras pārvaldības risinājumu "Microsoft Configuration Manager"** (saīsinājumā "ConfigMgr"), iegūstot infrastruktūrā pilnvērtīgu kontroli un centralizētu pārvaldību. Tas aizstātu pašlaik operētājsistēmas Uzdevumu pārvaldniekā ("scheduled tasks") lietotos skriptus un citus izpildfailus. Pārvaldības platforma "ConfigMgr" (iepriekšējais nosaukums "System Center Configuration Manager" jeb "SCCM") nodrošina detalizētu žurnālfailu ierakstu veikšanu un uzraudzību, bieži palīdzot identificēt un atrisināt infrastruktūras problēmas, pirms tās kļūst par reālu incidentu.
- **Ļoti vēlams ieteikums izmantot CERT.LV ABS sensora pakalpojumu**, lai CERT.LV varētu nodrošināt nepārtrauktu datu plūsmas anomāliju analīzi, ļaunatūras aktivitāšu atpazīšanu un brīdinājumu nosūtīšanu atbildīgajiem speciālistiem. Sīkāka informācija par pakalpojumu saitē: https://cert.lv/lv/pakalpojumi#6-informacijas-tehnologiju-drosibas-apdraudejumu-agras-bridinasanas-sistema

CERT.LV veica visaptverošas draudu medības Uzņēmuma informācijas un komunikāciju tehnoloģiju (IKT) infrastruktūrā ar nolūku novērtēt vispārējo drošības apdraudējumu situāciju un identificēt jau kompromitētas sistēmas. Par prioritāti identificēt citu valstu (Krievija, Ķīna u.c.) atbalstītas kiberoperācijas (APT).

Programmatūras problēmas

Tīkla auditēšanas programmatūra

Kādā uzņēmumā un ar to saistītajās iestādēs tika konstatēta dažāda veida tīkla auditēšanas programmatūra, kuru uzbrucējs var izmantot izlūkošanas fāzē papildus informācijas iegūšanai par tīkla uzbūvi. Iespējams, šo programmu atrašanās sistēmās ir leģitīma, administratori veikuši vai nu ar ielaušanās testus, vai ievainojamību skenēšanu. Nepieciešams noskaidrot zemāk redzamo programmas nepieciešamību.

Dažāda failapmaiņas programmatūra

Uzņēmuma infrastruktūrā konstatēta dažāda veida programmatūra, kuru izmanto failu apmaiņai starp darbstacijām – "FileZilla", "WinSCP" un "FAR". Kaut arī tās nav kaitnieciskas, tomēr stingrs ieteikums lietot vienu risinājumu visā Uzņēmuma datortīklā, lai mazinātu uzbrucēja iespējas izmantot plašu rīku klāstu ļaunprātīgu darbību veikšanai. Turklāt viena rīka standarts būtiski paātrina uzbrucēja atpazīšanu ielaušanās gadījumos.

Windows ugunsmūra konfigurācija

Windows ugunsmūris jeb "Windows Defender Firewall with Advanced Security" (WFAS) ir būtisks lokālās darbstacijas drošības elements. Ir zināms, ka ugunsmūra primārā funkcija ir bloķēt nevēlamu vai kaitniecisku ienākošo tīkla plūsmu. Taču situācijās, kad darbstacija jau ir uzlauzta vai inficēta, svarīgs ugunsmūra uzdevums neatļaut uzbrucējam vai ļaunatūrai izejošo tīkla plūsmu. Tādējādi uzbrukums var tikt ierobežots vai pat apturēts vienas darbstacijas ietvaros. Svarīgi pieminēt, ka pareizi konfigurēts ugunsmūris liedz vai būtiski apgrūtina uzbrucēja pārvietošanos iekštīklā starp dažādām darbstacijām. Sīkāka informācija nodaļas beigās sadaļā "Vispārīgie ieteikumi, Windows ugunsmūra konfigurācija".

Windows ugunsmūra (WFAS) priekšrocības

- Ērta centralizēta pārvaldība, izmantojot domēna kontroliera grupu politiku;
- Integrēts Windows operētājsistēmā bez papildus maksas;
- Funkcionalitāte "Connection Security Rules" ir Kerberos autentifikācija pirms atļaut izveidot savienojumu. Autentificēt var atsevišķi lietotāju vai tikai darbstaciju, vai abus vienlaicīgi;
- IPsec savienojuma šifrēšana.

Pēc visu Windows darbstaciju un serveru ugunsmūra nosacījumu ("rules") analīzes, veikti šādi secinājumi un ieteikumi, sadalīti divās grupās. Personalizētie – specifiski katrai organizācijai draudu medību beigu rezumējumā.

Vispārīgie – attiecināmi visiem tālāk uzskaitītajiem gadījumiem:

1. Lietojumprogrammai vai lietotnei (*.exe, *.dll) gandrīz visos gadījumos atļauti ienākošā tīkla plūsma visiem TCP un UDP protokolu portiem, daudzos gadījumos, atļauti arī visi tīkla protokoli. Rodas vairāki riski, būtiskākie piemēri ir aizvietojot leģitīmu "*.exe" ar ļaunatūru, tai tiks atļauti visi ienākošā tīkla savienojumi. Apgrūtināta ikdienas pārvaldība un incidentu izmeklēšana.
   Ieteikums. Darbstacijas pareizas ugunsmūra konfigurācijas ieviešanā ir vairākas līdzvērtīgi pareizas metodes, taču svarīgākais ir rīkoties pakāpeniski un procesu sadalīt etapos. Vispirms sašaurināt atļautās tīkla plūsmas darbību, ierobežojot secīgi protokolu, tad portu vai diapazonu. Pēc tam norādīt konkrēta *.exe, servisa vai lietotnes atļauto portu vai diapazonu un, ja iespējams, norādīt savienojuma avota IP adresi vai apgabalu. Vēlams izmantot "Connection Security rules", īpaši šo ieteicams lietot sistēmu administratoriem pārvaldības darbiem.
2. Papildu ieteikums par "Connection Security Rules" ir veikt rūpīgu analīzi un testus, sākt ar nelielu izmēģinājuma darbstaciju grupu. Pat minimāla konfigurācijas nesakritība var bloķēt leģitīmus savienojumus. Obligāti jānodrošina rezerves plāns, piemēram, komandrinda ar laika izpildi, kas atslēdz ugunsmūra nosacījumu.
3. Neierobežoti atļauta visa izejošā tīkla plūsma pēc noklusējuma. Ieteikums limitēt analoģiski punktā Nr.1.
4. Jāieslēdz ugunsmūra savienojumu ierakstu žurnāls ("Windows Firewall Log").

5. Lokālā vai centralizētā grupu politikā jāiespējo notikumu žurnāla savienojuma objektu ieraksti (sadaļa “Advanced Audit Policy Configuration”).
6. Pēc žurnālu ierakstu ieslēgšanas punktos Nr.4 un Nr.5, Windows ugunsmūrī atrastie aizdomīgie nosacījumi ietvers ne tikai savienojumu IP adreses un portus, bet lietotņu nosaukumus. Tas kalpos notikumu vēstures izmeklēšanai vai apliecinās lietotnes pašreizējo eksistenci, ļaujot izvērtēt tās nepieciešamību un veikt atinstalēšanu vai ugunsmūra nosacījuma pielāgošanu.

Windows ugunsmūra nosacījuma izveidošanas fakts parāda, ka programmatūras uzstādīšanas vai izmantošanas brīdī lietotājam bijušas administratora privilēģijas (ugunsmūra izņēmumus nav iespējams izveidot standarta lietotājiem).

Paroļu uzglabāšana atklātā tekstā

Komandrindas Powershell vēstures analizē konstatētas paroles atklātā tekstā. Ieteikums veikt sarakstā minēto lietotāju paroļu maiņu, lai novērstu iespējamu neautorizētu piekļuvi. Turklāt atrastās paroles saturiski nav pietiekami drošas un neatbilst drošai paroļu veidošanas politikai.

Detalizētie novērojumi un ieteikumi

1. Tīmekļa servera platformas “Microsoft IIS” funkcionalitāte. Mēdz būt gadījumi, kad kādam vēsturiskam vai testa servisam ir iespējots “IIS”, kurš ir funkcionējošs, taču neizmantots. Labā prakse to atinstalēt vai atslēgt neizmantotās funkcijas, izvērtējot “IIS” nepieciešamību uz iekārtām. Ja “IIS” darbība ir nepieciešama un tīkla savienojumi leģitīmi, tad jāpārliecinās par to pārvaldību un pārraudzīšanu tīkla iekārtu līmenī.
2. Programma darbstacijas attālinātai kontrolei un ekrāna koplietošanai “Screen Share”, plašāka informācija vienota standarta ieteikumos.
3. Programma audio izklaidei “Spotify”, plašāka informācija ieteikumos par darbam nesaistītu lietotņu izmantošanu.
4. Datorspēļu platforma “Steam”, plašāka informācija ieteikumos par darbam nesaistītu lietotņu izmantošanu.
5. Ķīnas uzņēmuma izstrādāta videonovērošanas programma “EyeCloud”, plašāka informācija ieteikumos par ārpus ES un NATO ražotu programmatūras izmantošanu.
6. Failu apmaiņas rīks “Torrent”, plašāka informācija ieteikumos par darbam nesaistītu lietotņu un “torrent” izmantošanu.
7. “Dell” tīkla serveris var izraisīt nesankcionētus, nepārvaldītus savienojumus ārpus organizācijas monitoringa. Papildus ievainojamību riskus rada iekārtas neatjaunošana. Plašāka informācija par vispārīgām rekomendācijām.
8. Virtualizācijas platformas var izraisīt nesankcionētus, nepārvaldītus savienojumus un citas tehniskās darbības ārpus organizācijas monitoringa. Ieteikums izmantot virtualizācijas pakalpojumus uz esošām šim mērķim paredzētām iekārtām vai izveidot nodalītu testa vidi.
9. “VLC” audiovizuālo materiālu atskaņošanas rīks, kas nav kaitnieciska programma, taču jāievēro ieteikumi par 1) vienota standarta izmantošanu 2) centralizētu, regulāru VLC atjaunināšanu.
10. Saziņas lietotne “WhatsApp” pakļauj datoru nulles dienas jeb “zero-day” ievainojamībām ar iesūtītu ļaunatūru, turklāt “beta” versiju izmantošana rada papildu nestabilitātes riskus. Ieteikums lietot vienu saziņas platformu, sīkāk par vienota standarta ieviešanu un centralizēti pārvaldītiem atjauninājumiem.

11. “Mikrotik” izstrādāts tīkla pārvaldības rīks “Winbox” var uzbrucējam ļaut tikt pie tīkla infrastruktūras pārvaldības un paplašinātas informācijas iegūšanas ne tikai par datortīklu, bet pievienotajām iekārtām un servisiem. “Winbox” atļauj iespēju saglabāt tīkla iekārtu adreses un administratoru lietotāju paroles, kuras var eksportēt teksta formātā. Ieteikums tīkla pārvaldības un monitoringa rīkus lietot nodalītā pārvaldības tīklā un atsevišķā pārvaldības datorā. Plašāka informācija sadaļā par iekārtu pārvaldības labajām praksēm, administratīvo darbstaciju un lietotāju nodalīšanu.
12. Nezināmas funkcionalitātes izpildfails “winuix”, netika atrasts ražotājs un darbības apraksts. Plašāka informācija meklējama atskaites ieteikumu sadaļā par lietojumprogrammām pēc būtības un atbilstības.
13. Trešās puses ekrāna ieraksta un video montāžas rīks “Wondershare”. Sīkāka informācija par vienotu standarta izmantošanu un labo praksi operētājsistēmas iebūvēto rīku izmantošanā (izgriešanas rīks jeb “Snipping Tool”).
14. SSH klienta rīks “Xshell”, kas nav centralizēti pārvaldīts, uzbrucējam dod iespēju izveidot SSH pieslēgumus, tuneļus, starpniekservera “proxy” u.c. funkcionalitāti kaitnieciskām darbībām. Bezmaksas “Xshell” lietošana atļauta mājas vajadzībām, uzņēmumiem noteikta maksas licences iegāde. Sīkāk ieteikumos par vienota standarta izveidi, nodalītu administrācijas vidi un monitoringu.
15. Pārvaldības risinājums “LANDesk” var izmantot kaitnieciskām darbībām ar plašām kontroles un konfigurācijas iespējām, ja uzbrucējs iegūst pieeju šim rīkam. Sīkāka informācija ieteikumos par vienotu standartu, pārvaldības labajām praksēm un nodalītu administrēšanas vidi.

Iejupielādēts kaitniecisks fails

Veicot vēsturiski lejupielādēto failu izpēti, atrasts fails ar nosaukumu “InstallPack_Zoom_c4b08.exe”, kas sākotnēji izskatās pēc “Zoom” video sapulces platformas instalācijas, taču faktiski satur vairākas kaitnieciskas pazīmes. Faila jaucējvērtība “VirusTotal” uzrādīja reputācijas rezultātu 53/72, atzīstot failu par kaitniecisku reklāmas ļaunatūru. Pie faila lietotāju aizveda saite “zoom-us.ru”, kas nešaubīgi ir pikšķerēšanas pazīme, atdarinot oficiālo “Zoom” vietni “zoom.us”.

Fails netika izpildīts, tā rāda “Amcache” rezultāti, taču nepieciešams izveidot drošības politiku, kas vai nu liedz lietotājiem lejupielādēt failus no nezināmām vietnēm, vai jāizmanto programmatūras kontroles risinājums (“AppLocker” vai analogs risinājums). Papildu ieteikums izmantot CERT.LV DNS ugunsmūri, kas aizsargātu organizāciju no šādām pikšķerēšanas vietnēm. Vairāk informācijas sadaļā “Vispārīgi ieteikumi”.

Iespējami uzbrukumi un ievainojamību skenēšana

Žurnālfailu ierakstu atlasē pēc nesekmīgajiem autentifikācijas mēģinājumiem tika apkopoti pieteikšanās jeb ielogošanās mēģinājumi no ārvalstu IP adresēm. Riska faktors īstenotas autentifikācijas gadījumā, ka uzbrucējs tiek pie iespējas nolasīt vai labot datus, vai pat administratora privilēģijām. Pozitīvais secinājums, ka sekmīgie autentifikācijas gadījumi nav atrasti.

Tika novērotas šādas riskantas prakses:

- publiski eksponēti serveri;
- VPN neizmantošana;
- uzbrucējam sniegta iespēja izmantot nepārtrauktu paroļu pārlasīšanu jeb minēšanu (“brute force”).

Nedroša infrastruktūras pārvaldība

Nedroša Linux operētājsistēmas pārvaldība

Vienā Linux iekārtā novērota "bash" sistēmas "chmod" komandrindas nepamatota "777" parametra izmantošana, kas rada vairākus drošības riskus, bet galvenais ir pilnas faila modificēšanas un izpildes tiesības visiem iekārtas lietotājiem. Iekārtas kompromitēšanas gadījumā uzbrucējs var failu nolasīt, pārkopēt (eksfiltrēt), modificēt vai ievietot tajā un pēc tam izpildīt kaitnieciskas komandas.

Piemēram, vienā iekārtā izpildīta komanda "sudo chown 777 *" un citā iekārtā izpildīta komanda "cd /var/www/api/ ; chmod -R 777 ./storage/ ; chown -R www-data:www-data ./*".

Ieteikums ierobežot piekļuvi, balstoties uz lietotājiem vai grupām ar attiecīgo nepieciešamību piekļūt konkrētiem failiem un direktorijām – minimālas pieejas tiesības darba pienākumu izpildīšanai.

Detalizētāki novērojumi un ieteikumi

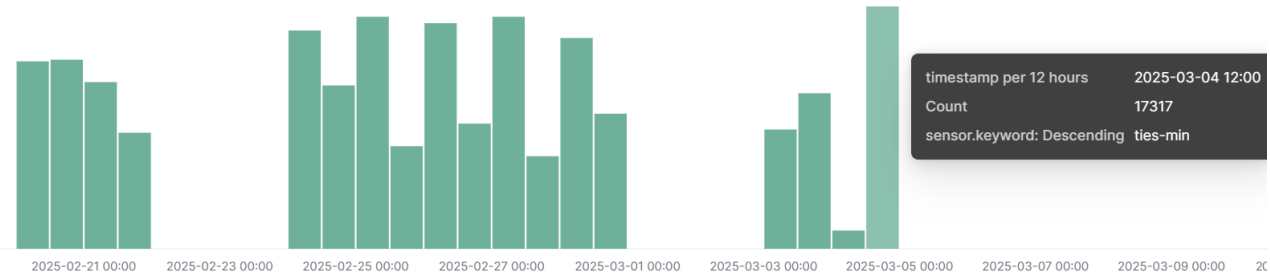
1. Tīmekļa servera platformas "Microsoft IIS" funkcionalitāte. Mēdz būt gadījumi, kad kādam vēsturiskam vai testa servisam ir iespējots "IIS", kurš ir funkcionējošs, taču neizmantots. Labā prakse ir to atinstalēt vai atslēgt neizmantotās funkcijas, izvērtējot "IIS" nepieciešamību uz iekārtām. Ja "IIS" darbība ir nepieciešama un tīkla savienojumi leģitīmi, tad jāpārliecinās par to pārvaldību un pārraudzīšanu tīkla iekārtu līmenī.
2. Ķīnas uzņēmuma "Hikvision" izstrādāta programmatūra "SADP" skenē datortīklā videonovērošanas iekārtas. Tas var apgrūtināt tīkla monitoringu un ieteicams neizmantot Ķīnā ražotu programmatūru . Alternatīvs risinājums ir izpildīt "SADP" domēnam nepievienotā datorā, pēc tam programmu dzēst, datoru pārinstalēt vai atjaunot no iepriekš izveidotas kopijas.
3. Programma audio izklaidei "Spotify", plašāka informācija ieteikumos par darbam nesaistītu lietotņu izmantošanu.
4. Programmnodrošinājuma komplekts "Tildes Birojs" (vārdnīca, pareizrakstības rīki, diakritiskās zīmes) ir neaktuāls, plašāka informācija par novecojušas programmatūras izmantošanu.
5. Failu apmaiņas rīks "Torrent", plašāka informācija ieteikumos par darbam nesaistītu lietotņu un "torrent" izmantošanu.
6. Videoierakstu un datu kolektors, par kuru nav pieejama detalizēta informācija. Plašāka informācija sniegta ieteikumos par programmu atbilstību pēc būtības.
7. Saziņas rīks "Cisco Jabber", plašāka informācija sniegta par vienota standarta izmantošanu.
8. Tīmekļa pārlūka "Apple Safari" komponente. Centralizēti nepārvaldīts pārlūks rada risku uzstādīt neatļautus paplašinājumus, novecojušu versiju, apiet organizācijas interneta drošības politikas. Plašāka informācija sniegta par vienota standarta izmantošanu un atļauto lietotņu kontroli ("AppLocker" vai analogu).
9. Saziņas lietotne "WhatsApp" pakļauj datoru nulles dienas jeb "zero-day" ievainojamībām ar iesūtītu ļaunatūru, turklāt "beta" versiju izmantošana rada papildu nestabilitātes riskus. Ieteicams lietot vienu saziņas platformu. Plašāk informācija sniegta par vienota standarta ieviešanu un centralizēti pārvaldītiem atjauninājumiem.
10. Tīkla monitoringa rīks "WhatsUp Gold WhatsConnected" var ļaut uzbrucējam iegūt paplašinātu informāciju par infrastruktūru. Ieteicams tīkla pārvaldības un monitoringa risinājumus lietot atdalītā pārvaldības tīklā no atsevišķas darbstacijas. Papildu informācija sniegta ieteikumos par iekārtu pārvaldības labo praksi un administratīvo darbstaciju lietošanu.

11. Nestandarta Windows žurnālfailu un datu kolektora risinājums apgrūtina pārredzamību un rada risku nodot informāciju uzbrucēja rīcībā. Ieteikums ieviest Windows žurnalēšanas standartu visām sistēmām, izmēģinājumiem izveidojot nodalītu testa vidi.
12. Trešo pušu Windows konfigurācijas rīks "Wintoys" var izsaukt nevēlamas izmaiņas vai radīt sistēmas nestabilitāti. Sīkāka informācija ieteikumos par centrālo pārvaldību un vienota standarta ieviešanu.
13. Failu arhivēšanas rīks "Winzip" ir centralizēti nepārvaldīta trešās puses programma, kas datorlietotāja sistēmu pakļauj arhivētas ļaunatūras uzbrukuma riskiem. Sīkāka informācija par vienota standarta izmantošanu un centrālu atjauninājumu pārvaldību.
14. Datorspēle "Datorspēle World of Tanks", plašāka informācija ieteikumos par darbam nesaistītu lietotņu izmantošanu.

Kompromitētās iekārtas

Agrīnās brīdināšanas sensora (ABS) datos tika novērotas konstanti TCP tīkla savienojumi no iestādes ierīces uz IP 45.9.148.140:80. IP adrese 45.9.148.140:80 pieder Nīderlandes "NiceIT-NL" mitināšanas pakalpojuma sniedzējam un saistīta ar "CoinMiner" ļaunatūru, kuras kods satur viltus "Chrome" tīmekļa instalācijas failu "chrome.exe, md5sum 3231c01e0b747ace61771e7450a59494".

Tā kā tīkla savienojumi (kopā 209575) no ierīces uz IP 45.9.148.140:80 notika laikā no 20.02.2025 līdz 04.03.2025, var secināt, ka ierīce ar IP *.*.*.130 tika inficēta ar "CoinMiner" kopš 20.02.2025.



Augsta iespēja, ka lietotājs patvaļīgi instalēja programmatūru no nedrošiem resursiem, tas parāda nepieciešamību ieviest ierobežojumus instalēt programmatūru organizācijas darbstacijās.

Plānotais sistēmas uzdevums ar virsadministratora privilēģijām

Iekārtā konstatēts plānotais uzdevums, kas izpilda primitīvu skriptu "Pauze" ar pārmērīgi augstām tiesībām – ID (S-1-5-18) – Windows lokālās sistēmas identifikators. Rezultātā uzdevums tiek izpildīts ar augstākajām (SYSTEM) tiesībām. Lai arī uzdevumam iestatīta "RunLevel" vērtība "LeastPrivilege", uzdevums tiks izpildīts ar sistēmas administratora privilēģijām.

Reizi stundā izpildīts skripts ar atrašanās vietu "C:\temp\pauze.bat". Datne nesatur tādu kodu, kur būtu nepieciešamas sistēmas līmeņa tiesības:

```
@echo off
echo "Take a break!"
timeout 15
```

Šādi skripti jāizpilda ar mazāko tiesību principu, šajā gadījumā "UserID" laukā iestatot "S-1-5-32-545" (standarta lietotājs jeb "Standard Users Group") vai arī "Author". Papildus jāpārbauda skripta datnes

piekļuves tiesības, ja modificēšana atļauta citiem lietotājiem, tas var tikt un tiks izmantots uzbrucēja kaitniecisko komandu izpildīšanā.

Aizdomīgas izcelsmes programmatūras izpildīšana

Pretvīrusa programmatūras brīdinājuma signālus radīja 20 identificētas izpildāmas datnes ar nosaukumiem slāvu alfabētā jeb kirilicā. Pieņēmums, ka to izcelsmes valsts ir Krievija, nosaukumi zemāk:

```
01 - Многоаспектная методика СМИЛ (566 вопросов).exe;
01 - Профориентационная методика Дж.Голланда.exe;
02 - Многоаспектная методика СМИЛ (388 вопросов).exe;
02 - Ориентировочная анкета направленности Б.Басса.exe;
03 - Модифицированный 8 цветовой тест М.Люшера.exe;
03 - Тест К.Томаса реагирование в конфликтных ситуациях.exe;
04 - Методика САН (Самочувствие Активность Настроение).exe;
04 - Модифицированный портретный тест Л.Сонди.exe;
05 - 16 факторный личностный опростник Р.Кеттелла.exe;
05 - Опросник уровня агрессивности Б.Басса-Дарки.exe;
06 - Методика УСК (Уровень Субъективного Контроля).exe;
06 - Многофакторная личностная методика ММРI(2).exe;
07 - Характерологический опросник Айзенка вариант В.exe;
07 - Характерологический опросник К.Леонгарда.exe;
08 - Многоаспектная методика ММРI (Мини-Мульт).exe.
08 - Тест А.Ассингера агрессивность в отношениях.exe;
09 - Методика Ч.Спилбергера-Ханнина уровень тревожности.exe;
09 - Статический критерий Ф Фишера.exe;
10 - Опросник Йовайши профориентационная методика.exe;
11 - Психогеометрическая методика ПГТ.exe.
```

Vienā piemērā izpildāmā datne ar nosaukumu “02 - Ориентировочная анкета направленности Б.Басса.exe” un SHA256 jaucējfunkcijas vērtību “4e4c73895bfb1bf952b15fdf7517d0e637 649424fcd1212396ba7d4600b26c6e” platformā “VirusTotal” 30 no 74 antivīrusa pakalpojuma sniedzējiem to atzīst par ļaunatūru.

Lai arī pati datne nav vīruss, tas ir nelabvēlīgs izpildfails. Ir ieteicams izvairīties no šādu datņu izpildes, kā arī ieviest programmatūras kontroles risinājumu (“AppLocker” vai analogu).

Tīmekļa vietne ar SQL injekciju

Iekārtā identificēta tīmekļa vietnes lietotne, kurā iespējams veikt SQL injekciju, veicot POST pieprasījumu tīmekļa lapai “http://*.lv/ login_ex.asp”. SQL injekcijai pakļautā datne “C:\inetpub\wwwroot\Expert\login_ex.asp” satur lietotāja parametru izmantošanu SQL vaicājumā. Lietotāja parametri “username” un “password” netiek pareizi apstrādāti.

Izpildot SQL injekciju, jebkurš vietnes apmeklētājs var apiet autentifikāciju un sensitīvu datu izguvi. Pamats uzskatīt, ka konkrētā tīmekļa vietne nav pieejama internetā, par ko nepieciešams papildus pārliecināties. Šādas ievainojamības jāizlabo, kaut arī vietne atrodas iekšējā tīklā. Jebkura ievainojamība uzbrucējiem atvieglo sensitīvu datu izguvi.

Novecojis Kerberos biļetenu šifrēšanas algoritms

Windows domēna kontrolieru auditēšanas ierakstos novērots, ka vairākos Kerberos biļetenu apmaiņas pieprasījumos tiek izmantota “RC4-HMAC” šifrēšana algoritms, kas ir pakļauts vairākām ievainojamībām. Pāreja uz AES128 vai AES256 algoritmiem ir ieteikta kopš “Windows Server 2008” versijas. Ja izmanto “RC4-HMAC” algoritmu, infrastruktūra tiek pakļauta Kerberoasting uzbrukumam, kad iegūst lietotāja paroli no Kerberos biļetena.

Tehniskajam personālam nepieciešams izpētīt novecojuša “RC4-HMAC” izmantošanas iemeslus un iespēju to mainīt uz AES paaudzi (vēlams AES256).

Neaktīvi lietotāji

Pēc lietotāju kontu pārskatīšanas identificēti vairāki “*_ADM” lietotāji, kas nav pieteikušies sistēmā vismaz gadu un vairāk. Par IKT drošību atbildīgajam personālam jāpārskata lietotāju saraksts un neizmantotos kontus jādzēš, sīkāka informācija saitē: https://learn.microsoft.com/en-us/services-hub/unified/health/remediation-steps-ad/regularly-check-for-and-remove-inactive-user-accounts-in-active-directory

Microsoft XDR brīdinājumi

Pārskatot drošības platformas “Microsoft XDR” pieejamo informāciju par ļaunatūru, konstatēti vairāki brīdinājumi, kuri izcēlušies vairākās “Microsoft Intune” pārvaldītajās iekārtās.

Attālinātas piekļuves programmatūra

Pārskatot iekārtās izpildīto programmatūru konstatēts, ka infrastruktūrā tiek izmantoti dažādi attālinātās piekļuves rīki “Anydesk”, “Teamviewer”, “PSexec”. Kompromitēšanas gadījumā tie dod uzbrucējam plašas rīku izmantošanas iespējas, lai tālāk pārvietotos infrastruktūrā. IKT drošības personālam vairāku risinājumu lietošana būtiski apgrūtina uzbrucēja izsekošanu.

Vairākās iekārtās konstatēts attālinātās pārvaldības rīks “Bomgar SCC” (Bomgar Secure Customer Chat).

PsExec rīka izmantošana incidentu izmeklēšanas gadījumus padara sarežģītus, jo leģitīmas darbības no uzbrucēju darbībām gandrīz nav atšķiramas. Atsauce uz Microsoft uzbrukuma laukuma samazināšanas (“Attack Surface Reduction”) ieteikumiem saitē: https://learn.microsoft.com/en-us/defender-endpoint/attack-surface-reduction-rules-reference#block-process-creations-originating-from-psexec-and-wmi-commands

Atsauce uz uzbrucēja “PsExec” izmantošanu “Mitre Attack” izpildes tehniku:

https://attack.mitre.org/software/S0029/

https://attack.mitre.org/techniques/T1569/002/

Par IKT drošību atbildīgajam personālam nepieciešams izvērtēt šīs programmatūras atrašanos uz minētajām iekārtām. Labās prakses vadlīnijas iesaka attālinātai pārvaldībai izvēlēties tikai vienu centralizēti pārvaldāmu rīku. CERT.LV iesaka izmantot Microsoft iebūvētos risinājumus, piemēram, “Remote Desktop Connection”.

Pagaidu direktorijās instalētas programmas

Pārskatot iekārtās izpildīto programmatūru vēsturi, novērots, ka infrastruktūrā dažas tiek izpildītas no operētājsistēmas pagaidu direktorijas “C:\Temp”, kas kompromitēšanas gadījumā var tikt nepamanīti izmantotas uzbrucēja programmatūras izpildīšanā. Biežāk sastopamie riski, kad programmatūra vai citi dati tiek izvietoti “Temp” direktorijā:

- Temp mapei un apakšmapēm bieži ir plašas rakstīšanas tiesības, kas ļauj neautorizētiem lietotājiem un procesiem modificēt tajās esošās datnes. Tas, savukārt, var tikt izmantots ļaunprātīgi – uzbrucējs leģitīmos izpildfailus var aizvietot ar ļaunatūru sistēmas privilēģiju paaugstināšanas nolūkā. Papildu informācija par šo uzbrukuma tehnikas veidu saitē: https://attack.mitre.org/techniques/T1574/005/

- DLL ielādes pārtveršana (“DDL Hijacking”), kad uzbrucējs var izveidot ļaunprātīgu DLL bibliotēku ar tādu pašu nosaukumu kā leģitīmai datnei temp direktorijā. Izmantojot to, kādā secībā Windows operētājsistēma veic leģitīmas programmatūras DLL datņu meklēšanu, var ielādēt un izpildīt uzbrucēja kaitniecisko kodu. Papildu informācija par šī uzbrukuma tehniku: https://attack.mitre.org/techniques/T1574/

Vērts pieminēt, ka antivīrusa programmatūras šīm direktorijām skenēšanas procesā bieži samazina prioritāti, kas var ļaut uzbrucējam izvairīties no atklāšanas.

Aicinām par IKT atbildīgo personālu izskatīt iespējas programmas pārvietot citā mapē, piemēram, lietotāja vai programmu failu direktorijā. Ir situācijas, kad nav iespējams izvairīties no programmu glabāšanas pagaidu direktorijās. Šādos gadījumos ieteikums pastiprināti uzraudzīt jaunu datņu izveidi “Temp” mapē – īpaši ar tādiem paplašinājumiem kā “doc”, “docx”, “pdf”, “xls”, “rtf”, “exe”, “scr”, “lnk”, “pif”, “cpl”, “zip”. Windows domēnā šādu notikumu uzraudzībai var izmantot “Sysmon” rīka notikumu kodu Nr.11 (“Event ID 11”). Var lietot Windows sistēmā iebūvēto notikumu pārvaldnieka ID Nr. 4663 (“Windows Event Log Event ID 4663”), tādā gadījumā vispirms nepieciešams grupu politikā iespējot “Object Access” auditēšanu.

Starpniekservera žurnālfaila rotācijas trūkums

Starpniekservera “Squid” piekļuves auditēšanas pieraksti tiek saglabāti vienā failā “/var/squid/logs/access.log”, kura apjoms analīzes brīdī sasniedza 250GB. Lielais faila izmērs izskaidrojams ar visu jauno pierakstu pievienošanu klāt esošajam “access.log” failam. Šis žurnālfails satur svarīgu informāciju par piekļuves laikiem, IP adresēm, izmantotajiem protokoliem u.c., dati ir noderīgi tīkla aktivitātes novērošanai un dažādu notikumu izpētei. Konkrētā žurnālfaila izmērs padara lejupielādi un analīzi par ļoti laikietilpīgu un resursu prasīgu procesu. Turklāt paši senākie ieraksti vairs var nebūt aktuāli.

Ieteikums ieviest žurnālfailu rotāciju, arhivējot tos pēc konkrēta laika perioda vai faila izmēra sasniegšanas, turpinot pierakstu veikšanu jaunā failā. Tas ievērojami samazinātu faila apjomu, nepieciešamības gadījumā nodrošinot analīzes procesu vienkāršāku un efektīvāku, kā arī uzlabojot pārvaldības procesu un ietaupot sistēmas resursus.

Nedroša datu glabāšana ārējos datu nesējos

Windows notikumu žurnālfailos (“Event Logs”) konstatēta informācija par pirātisku programmatūru aktivizēšanas rīkiem, kas atrodas ārējos datu nesējos. Nav pazīmju par programmatūras izpildīšanas notikumu.

Ieteikums ieviest ierobežošanu un monitoringu ārējiem datu nesējiem. Izglītot lietotājus par kaitējumu, ko var radīt pirātiska un iespējami ļaunprātīga programmatūra.

TightVNC

Vairākās iekārtās konstatēts attālinātās piekļuves rīks TightVNC un ar to saistīts aktīvs serviss “tvnserver.exe”, kas izmanto portus TCP 5800 un TCP 5900. Pārbaudot izpildāmās datnes jaucējvērtības, noskaidrotas ievērojami novecojušas versijas - 2.5.2 un 2.8.8, izstrādātas attiecīgi 2012. un 2017. gadā.

Novecojusi programmatūra var tikt pakļauta draudu riskiem, “TightVNC” ievainojamība “CVE-2023-27830” ļauj uzbrucējiem iegūt paaugstinātas tiesības, tā ietekmē visas versijas pirms 2.8.75 (versija 2.8.8 izlaista pirms 2.8.75). Ievainojamība “CVE-2024-42049” ietekmē visas versijas pirms 2.8.84, kas uzbrucējiem ļauj

veikt piekļuvi aizsargājamai informācijai vai iegūt kontroli pār "TightVNC" serveri. Nepieciešams programmatūru atjaunot uz aktuālu versiju.

Papildus jābūt skaidrībai par atļauju "TightVNC" izmantot infrastruktūrā. Iespējams, ir nepilnīgi konfigurēta vai trūkstoša programmatūras kontroles politika. Ja rīka atrašanās infrastruktūrā nav pamatota, to nepieciešams no sistēmām dzēst.

Novecojušas paroles

Paroles vecākas par 6 mēnešiem ir astoņiem lietotāju kontiem, no tiem pieci atrodas AD grupā "lietotaji" ("OU, Organizational Unit"). Trim paroles nav mainītas vismaz pēdējo piecu gadu laikā, senākā ir 2018. gadā. Nepieciešams kontus pārskatīt un, atkarībā no lomām, veikt paroļu maiņu drošības risku mazināšanai.

Papildus jāizvērtē spēkā esošā paroļu politika. Jaunākās vadlīnijas vairs tik aktīvi neuzstāj 30-90 dienu nomaiņu, jo lietotāji bieži tās speciāli veido vienkāršākas. Svarīgi ir papildu pasākumi ilgstošas vienas paroles drošākai lietošanai:

- parolēm jābūt unikālām, lietotājiem jāzina riski ar vienas lietošanu vairākos pakalpojumos. Noplūdes gadījumā var tikt skarti visi pakalpojumi, kuros lietota viena parole;
- nepieciešamas skaidras un reāli ieviestas prasības parolēm attiecībā uz simbolu skaitu un sarežģītību. Pašlaik labā prakse ir fokuss uz paroles garumu nevis sarežģītību, turklāt garas frāzes ir vieglāk iegaumēt nekā simbolu kombinācijas;
- administratoriem paaugstināto tiesību dēļ tāpat ieteikts paroles mainīt biežāk;
- biežāka nomaiņa attiecas arī uz paaugstināta riska (piem., ārpakalpojuma u.c.) kontiem, kas parasti autentificējas no citas vides. Nepieciešama skaidra procedūra par VPN, administratīvās starpniekservera ("jumphost") izmantošanu;
- daudzfaktoru autentifikācijas lietošana;
- paroļu noplūdes monitorings.

Atkarībā no sekmīgas rekomendāciju ieviešanas, paroles standarta lietotājiem var tikt lietotas ilgāk. Ja šie papildus drošības elementi nav ieviesti, ilgstoša vienas paroles lietošana ir riskanta – tā var tikt atminēta, noplūst un citādi kļūt bīstama. Paliekot pie biežākas paroļu maiņas stratēģijas, jānosaka tās minimālais vecums un vēsture ("Enforce password history"), lai nenotiktu atkārtota izmantošana.

Aktīvās direktorijas (AD) pārbaude pēc Microsoft drošības vadlīnijām

Analizējot AD konfigurāciju pēc Microsoft drošības vadlīnijām (https://www.microsoft.com/en-us/download/details.aspx?id=55319) noskaidrots, ka pašreizējā konfigurācija lielākoties neatbilst rekomendācijām. Esošās konfigurācijas reģistra vērtības, kas apzīmē specifiskus iestatījumus, tika salīdzinātas pret vadlīnijās ieteiktajām vērtībām, kopā pārbaudot 222 atslēgu ierakstus.

Lielākā daļa no Microsoft ieteiktās konfigurācijas nav veikta vispār, t.i., reģistrā neeksistē attiecīgā iestatījuma ieraksts.

Konfigurācija novērota tikai 3 drošības iestatījumiem, taču tie nesakrīt ar vadlīnijās ieteiktajiem.

Drošības stiprināšanas nolūkos CERT.LV iesaka pārskatīt esošās aktīvās direktorijas konfigurāciju, iespējami to pietuvinot Microsoft vadlīnijām.

Mobilie tīkla adapteri

Pārskatot aktīvos tīkla interfeisus, trijās iekārtās konstatēta mobilā tīkla adaptera izmantošana. IKT atbildīgajam personālam jāizvērtē to izmantošana, jo paralēls mobilais pieslēgums ar organizācijas datortīklu var apiet iestādes ugunsmūri un citus uzraudzības, pārvaldības, drošības risinājumus. Iekārtas kompromitēšanas gadījumā tas var radīt papildu drošības draudus visai iestādes infrastruktūrai.

Publiski pieejams autentifikācijas panelis

Draudu medībās analizēti publiskā tīmeklī pieejami uzņēmuma resursi, rezultātā identificēts serveris ar aktīvu IIS servisu portā TCP 443. Ieteikums IKT atbildīgajam personālam izvērtēt paneļa publisku pieejamību internetā, jo uzbrucēji var veikt lietotāju paroļu pārlases uzbrukumu. Īpašs risks, ja nav iestatīta kontu nobloķēšanas (lockout) politika.

Datu noplūdes

Draudu medību ietvaros CERT.LV izmeklēja publiski pieejamās datu noplūdes ar iesaistītu kādas organizācijas domēna vārdu. Konstatēti vairāki lietotāji, kuri organizācijas e-pastu izmanto, visticamāk, ar privātām vajadzībām saistītiem pakalpojumiem. Piemēram, kāds e-pasts, kas bija reģistrēts vietnēs "golfs.lv", "pienaloterija.lv", "travelnews.lv", "Myheritage" u.c. Lai arī vairums noplūdes notikušas pirms vairākiem gadiem un paroles, visdrīzāk, ir nomainītas, tomēr ieteikums informēt iesaistīto e-pastu lietotājus, jo viņu dati uzskatāmi par kompromitētiem – piekļuves nopērkamas pagrīdes tirgū vai pat iegūstamas bez maksas. Tāpat nevar izslēgt kādas nopludinātās paroles izmantošanu, lai pieslēgtos organizācijas e-pasta kontam. Attiecīgi visiem sarakstā minētajiem lietotājiem jānomaina piekļuves e-pasta konta dati.

Par IKT drošību atbildīgajam personālam regulāri jāatgādina darbiniekiem kiberhigiēnas labā prakse: organizācijas e-pasts ir paredzēts tikai ar darba pienākumiem saistītai saziņai un profesionālām vajadzībām. Darba e-pasta izmantošana privātu kontu, piemēram, "YouTube", "Spotify", interešu forumu, sociālo tīklu, interneta veikalu u.c. lietošanai nav pieļaujama.

Tāpat darbiniekiem regulāri jāatgādina paroļu lietošanas politika, kā arī jānodrošina apmācības par drošu paroļu izveidi un paroļu pārvaldnieku izmantošanu.

Aktīvās direktorijas (AD) servisa konti

Konstatēta standarta lietotāja "user.admin" kontam piesaistīts SPN (Service Principal Name). Tā nav labā prakse, jo bieži ir tā, ka servisa kontiem reti maina paroles, pakļaujot tos "Kerberoasting" uzbrukumiem. Tas nozīmē, ka jebkurš domēna lietotājs var pieprasīt SPN Kerberos biļetenu un bezsaistē uzlauzt jaucējsummu paroles iegūšanai.

Microsoft Exchange analīze

Draudu medībās analizēta Microsoft Exchange lietotāju kontu konfigurācija. Uzmanība vērsta uz pārāk plašu privilēģiju piešķiršanu e-pasta mapēm, piemēram, mapes "/inbox" piekļuve atļauta visiem iestādes lietotājiem. Apskatīts arī scenārijs, kad e-pastu mapes tiek koplietotas ar citiem tādiem lietotājiem, kas nav mapes īpašnieki.

Infrastruktūrā identificētas vairākas e-pasta mapes ar plašām privilēģijām, taču, spriežot pēc nosaukumiem, liela daļa koplietotas ar nolūku.

Nepieciešams pārliecināties par piekļuvi “Default” un “Anonymous” lietotājiem. Ja tās nav nepieciešamas, koplietošana jānoņem.

Citā medību procesā tika analizēta Microsoft Exchange lietotāju kontu konfigurācija. Uzmanība pievērsa pārāk plaša privilēģiju piešķiršana lietotāju e-pastu kontu mapēm. Tika apskatītas arī e-pastu mapes koplietošana ar lietotājiem, kas nav mapes īpašnieki.

Publiski eksponēts Microsoft Exchange tīmekļa pakalpojums “EWS” var kļūt par vienkāršu uzbrukuma vektoru. Uzbrucēji izmanto EWS, lai iegūtu nesankcionētu piekļuvi uzņēmuma e-pasta sistēmām, kas var rezultēties biznesa e-pasta kompromitēšanā. Īstenotā uzbrukumā noziedznieki manipulē ar uzņēmuma darbiniekiem vai piegādātājiem, lai izkrāptu finansiālus līdzekļus vai sensitīvu informāciju, kas ļautu uzbrucējiem iegūt tālāku piekļuvi infrastruktūrai, piemēram, iegūstot e-pastos pārsūtītu piekļuves datu informāciju. Tā kā šajā gadījumā nav ieviesta divu faktoru autentifikācija, tie pakļauti paroļu minēšanas uzbrukumiem. Ieteikums izvietot visus šāda veida pakalpojumus iekšējā tīklā vai nodrošināt piekļuvi, izmantojot VPN.

Rīka “NTDSAudit” izmantošana

Aktīvās direktorijas auditēšanas rīka “NTDSAudit” izmantošana var būt leģitīma, taču arī to var izmantot uzbrucēji, lai veiktu lietotāju kontu jaucējvērtību izgūšanu (“hash dumping”).

Rīka “Lynis” izmantošana

Draudu medību ietvaros kādā iekārtā konstatēts “/home/old_locals/user/lynis”, kas ir atvērtā koda rīks Unix tipa operētājsistēmu pārbaudei drošības stiprināšanai. To bieži izmanto uzbrucēji pēc sākotnējās piekļuves, lai noteiktu sistēmas vājās vietas un veiktu tālākos uzbrukumus, piemēram, privilēģiju paaugstināšanu. Par IKT drošību atbildīgajam personālam jāizvērtē rīka nepieciešamība un jādzēš, ja tas vairs nav nepieciešams.

Publiski pieejamā informācija

CERT.LV draudu medību ietvaros veica atvērto avotu izlūkošanu OSINT (Open-Source Intelligence), tajā skaitā informācijas vākšanu par datu noplūdēm un pieejamajiem pakalpojumiem, kuros ir iesaistīts uzņēmuma domēna vārds.

Identificēts publiski eksponēts domēns “autodiscover.*.lv”, īstenotas autentifikācijas gadījumā, uzbrucējs var piekļūt tādai informācijai kā:

- iekšējai un ārējai Exchange serveru informācijai;
- pieejamām autentifikācijas metodēm;
- vispārīgai informācijai par iestādēs iekšējo infrastruktūru.

Nepieciešams ierobežot “Autodiscover” piekļuvi no ārējā tīkla, atstāt pieeju tikai konkrētiem lietotājiem no iekštīkla. Nepieciešams atspējot novecojušas autentifikācijas metodes (“Basic, NTLM”), jānodrošina daudzfaktoru autentifikācija un jāpārliecinās par pieprasījumu žurnalēšanu.

Identificēts kāds domēns, kas, visticamāk, izmantots VPN pakalpojumam.

Tam identificēts apakšdomēns, kas atver programmatūras "Tomcat" noklusējuma lapu. Kaut arī "Tomcat" konfigurācija papildus informācijas detaļas atklāj no lokālā servera, ieteikums publiski neeksponēt tīmekļa lapas izstrādes laikā.

Atrasts arī kāds apakšdomēns, kas, visticamāk, tiek izmantots programmatūras izstrādes pārvaldībai. Jebkurā gadījumā ieteikums to neeksponēt publiski, atļaut piekļuvi tikai no iekšējā tīklā vai sekmīgas VPN autentifikācijas.

Par identificēto domēnu "terminal.*.lv" saņemta informācija no atbildīgā personāla, ka tas ir RDP tīmekļa pakalpojums, kas tiek izmantots grāmatvedības vajadzībām. Resurss savienots ar Aktīvo Direktoriju, kam atļauts NTLM autentifikācijas mehānisms, apraksts: "Type: 3 - NETWORK LmPackageName: NTLM V2", avota IP adrese: 136.0.190.154.

Pagaidu risinājums būtu atļaut piekļuvi pie RDP servisa tikai pēc sekmīgas VPN autentifikācijas. Aicinām IKT atbildīgo personālu izvērtēt nepieciešamību pakalpojumu atklāt publiskā tīmeklī, jo uzbrucēji autentifikācijas formas var izmantot lietotāju paroļu pārlases uzbrukumiem. Tāpat atgādinām, ka NTLM autentifikācijas metodes ir novecojušas un tās jāaizstāj ar "Kerberos" protokolu (avots: https://learn.microsoft.com/en-us/windows/whats-new/deprecated-features).

Pakalpojums "Google Play Games"

Pārbaudot izpildāmo datņu automātiskas startēšanas ierakstus, iespējots "Google Play Games" pakalpojums un Windows uzdevumu pārvaldnieka regulārais uzdevums "Google Play Games Notifier". Pakalpojums nodrošina dažādas datorspēles "Android", "ChromeOS" un "Windows" iekārtās, sīkāk: https://developer.android.com/games/pgs/overview

Nepieciešams pārbaudīt pakalpojuma nepieciešamību darba uzdevumu veikšanai.

Nevēlama VPN programmatūra

Uzstādīta VPN programmatūra "Express VPN", tā kā šī ir vienīgā tāda iekārta, nepieciešams pārbaudīt šī VPN pakalpojuma nepieciešamību. Datnes atrašanās vieta un izpildes laiks "Prefetch" ierakstos:

- 2025-05-15 07:12:03.38, c:\program files (x86)\expressvpn\expressvpn-ui\expressvpn.exe;
- 2025-05-15 07:12:23.39, c:\program files (x86)\expressvpn\expressvpnd\windows\openvpn.exe.

Citi notikumi

SSH savienojumi ar ārējiem resursiem

Analizējot lietotāju izpildītās komandas, tika konstatēta attālinātā protokola SSH ("Secure Shell") lietošana vairākās iekārtās. Ieteikums pārbaudīt vairākas konstatētās komandas.

Izpildītās komandas:

- Issh support@uznemums.lv;
- ssh -p 2022 lietotajs@uznemums.lv;
- ssh -J admin@uznemums.lv admins@uznemums.lv;
- ssh -J asa@uznemums.lv er@uznemums.lv;
- ssh root@uznemums.lv.

Izpildītajās komandās tika konstatēti:

- savienojumi ar ārējām IP vai domēniem;
- lietotāju "root" un "support" kontu izmantošana;
- nestandarta porta "2022" izmantošana;
- starpnieksavienojuma "ProxyJump" izmantošana (ssh -J).

Konstatēta iebūvētā sistēmas lietotāja "root" konta izmantošana SSH pieslēgumiem. Lietotājam "root" ir visaugstākās tiesības sistēmā, tā kompromitēšanas gadījumā uzbrucējs var iegūt neierobežotu piekļuvi iekārtai.

Labā prakse nosaka stingri ierobežot iebūvētos lietotāju kontus (piemēram, "root", "administrator", "guest"), tādā veidā apgrūtinot uzbrucēja iespējas piemeklēt sistēmai atbilstošus piekļuves datus paroļu pārlases uzbrukumu laikā.

Ieteikums izveidot atsevišķu lietotāju ar ierobežotām privilēģijām ikdienas darbiem, pārslēdzoties uz "root" tikai nepieciešamības gadījumā. Pārliecināties par SSH servera konfigurāciju, lai tiktu bloķēti pieslēgumi no "root" lietotājiem vai ierobežot piekļuvi tikai no noteiktām IP adresēm.

Papildu ieteikums: pārliecināties, ka augstāk minētie ārējie resursi ir pazīstami un darbības ir autorizētas, un nepieciešamas darba pienākumu veikšanai.

Ārējas IP adrese Windows "TrustedHosts" sarakstā

Pārbaudot "PowerShell" komandu vēsturi, iekārtā "*.Uznemums.lv" (iesaistītie lietotāji "admin", "ad_admin") izpildīta komanda "Set-Item wsman:\localhost\client\trustedhosts -Value *IPadrese*" Šī komanda pievieno Windows attālinātās pārvaldības ("Remote Management, WinRM") uzticamo iekārtu sarakstam Beļģijas ārējo IP adresi.

Ieteikums apstiprināt darbības leģitimitāti un noskaidrot iemeslus. Ja operācija ir atpazīstama, bet savienojumu izmantošana vairs nav nepieciešama, ieteicams ierakstu dzēst no uzticamo iekārtu saraksta.

Publiski pieejams pārvaldības panelis

Publiski pieejams cPanel/Webmail autentifikācijas panelis.

Pētot publiski pieejamos kāda uzņēmuma resursus, identificēts tiešsaistes e-pasta pakalpojums "Webmail" un tīmekļa vietņu pārvaldības "cPanel" autentifikācijas panelis, kas publiski pieejams tīmekļa adresē.

Aicinām par IKT atbildīgo personālu izvērtēt pakalpojumu publisku pieejamības nepieciešamību publiskā tīmeklī. Draudu rīkotāji tos var izmantot lietotāju paroļu pārlases uzbrukumos, īpaši trūkstoša kontu bloķēšanas ("lockout") vai divu faktoru autentifikācijas gadījumos.

Novecojušu pakalpojumu publiska eksponēšana pakļauj tos dažādiem uzbrukumiem, izmantojot jaunatklātas vai esošas ievainojamības, kas var rezultēties līdz pilnai servera kompromitēšanai.

Novecojuši tīmekļa vietnēs risinājumi

Kādā tīmekļa vietnē pētīti izmantotie tehnoloģiskie risinājumi un versijas ar mērķi identificēt ievainojamības. Risinājumi ar potenciālām ievainojamībām:

- JavaScript bibliotēka "FancyBox 3.2.10" (CVE-2025-3662);

- programmēšanas valoda “PHP iespējamā versija 5.6.40” (CVE-2019-9641, CVE-2017-8923).

Vietnes spraudnis “FancyBox” ievainojamība “CVE-2025-3662” atrodama versijās pirms “3.3.6”, tā ļauj veikt neautentificētu starpvietņu skriptēšanu (“Unauthenticated Stored XSS”).

Ievainojamībai ir publiski pieejams koncepcijas pierādījums (“PoC, “proof-of-concept”), kas atvieglo tās izmantošanu. Ieteikums spraudni atjaunināt uz aktuālo versiju, sīkāk par ievainojamību: https://wpscan.com/vulnerability/4cda12f0-3c23-44ad-80ea-db2443ebcf82/

Darbstacijai atvērts ports

Darbstaciju tīkla konfigurācijas pārbaudē datorā identificēts atvērts TCP 80 ports ar augstākajām “NT AUTHORITY\SYSTEM” privilēģijām, kas parasti tiek izmantots HTTP pakalpojumam. Jaucējvērtība “MD5, d41d8cd98f00b204e9800998ecf8427e” sniedz norādes par tā saistību ar programmatūru “Android CTS (Compatibility Test Suite)”.

Ieteicams pārbaudīt pakalpojuma nepieciešamību un to atslēgt. Termināla komanda “netsh http show servicestate” uzrāda vairāk informācijas par servisu.

Potenciāli uzbrukumi un skenēšana

Identificēta aizdomīga aktivitāte domēna lietotāja kontam, kurš autentificējies “Microsoft Exchange” e-pasta serverī no dažādām aizdomīgām IP adresēm. Pieprasījumi tika veikti, izmantojot ikdienas darbam neraksturīgu “exchangelib/5.5.0+(python-requests/2.32.3) “User-Agent”” galveni. Tā atbilst tādiem rīkiem kā “PyMailSniper” (https://github.com/foofus-sph1nx/PyMailSniper), kas tiek izmantoti pastkastīšu satura un koplietoto mapju nolasīšanai. Daļa pieprasījumu veikti tīmekļa adresei “https://mail.*.lv/ews/exchange.asmx” no vairākām IP adresēm. Iegūtie 200 statusa kodi apliecina veiksmīgu autentifikāciju “Exchange Web Services (/EWS/Exchange.asmx)” autentifikācijas pieprasījumiem ar domēna lietotāju.

Šādas aktivitātes liecina par nesankcionētu e-pastu lejupielādēšanu no dažādiem virtuāliem privātiem serveriem (Virtual Private Server, VPS), kuri lielākoties izmitināti pie pakalpojumu sniedzēja “Stark Industries Solutions Ltd.” (AS44477), kurš saistīts ar Krievijas valdības atbalstītiem grupējumiem.

CERT.LV ir pieejama informācija, ka šī lietotāja autentifikācijas dati ir iekļauti datu noplūdēs sākot ar 2021. gada 12. oktobri, izmantotā parole “admin123”. Jaunākie ieraksti redzami 2025. gada 17. jūlijā ar paroli “admin1234”. Ierakstos minēts arī lietotājvārds ar NetBIOS domēna vārdu, kas liecina par informācijas zagšanas ļaunatūru, taču tā netika atrasta lietotāja darba datorā.

Saziņā ar administratoriem noskaidrots, ka lietotāja e-pasts, iespējams, nav pilnībā kompromitēts, jo konts 2022. gadā ticis pārcelts uz “Microsoft 365” mākoni, kur nepieciešama daudzfaktoru autentifikācija. Jebkurā gadījumā ir nepieciešams veikt drošības pasākumus un pārliecināties, ka kontam nav piekļuve Exchange tīmekļa pakalpojumam EWS. Ir iespēja, ka konts pārcelts, bet EWS piekļuves ir palikušas nemainītas. Papildus nepieciešams atrast un pārinstalēt visas iekārtas, kuras lietotājs izmantojis e-pasta piekļuvei. Ieskaitot privātās darbstacijas un viedierīces, kas potenciāli var būt inficētas ar ļaunatūru.

Publiski eksponētas iekārtas ar RDP pakalpojumu

Identificēta iekārta “dators.*.lv” ar internetā eksponētu attālinātās piekļuves pakalpojumu “RDP”. Atkārtojot vēl šādu iekārtu meklējumus, tīmeklī tika atrasti vēl vairāki TLS sertifikāti, kas atbilst “Uznemums” iekārtām (CN=*-pc.*.lv). Visas, visticamāk, saistītas ar eksponētiem RDP servisiem.

Šāda veida konfigurācijas kļūdas tipiski tiek pieļautas maršrutētājos, kurus piedāvā interneta pakalpojuma sniedzējs. Tiem kāds no tīkla kabeļa "RJ45" portiem nokonfigurēts publiskā tīmekļa režīmā, kas izmantošanas gadījumā darbstaciju eksponē internetā bez ugunsmūra. Tā kā bieži nav iespējots lokālais datora ugunsmūris, darbstacija tiek pakļauta dažāda veidu kiberuzbrukumiem, galvenokārt paroļu minēšanai un ievainojamību izmantošanas mēģinājumiem. Jaunatklātas ievainojamības gadījumā iekārtas var tikt pakļautas tūlītējiem uzbrukumiem.

Šāda tipa RDP lietotāja paroles minēšanas gadījumi konstatēti 2025. gada 25. maijā iekārtai "pc.*.lv", galvenie mērķi bija lietotāji "Administrator" un "Admin". Eksponētās iekārtas var kļūt par galveno ieejas punktu uzņēmuma iekštīklā un datoru infrastruktūrā. Ieteikums mainīt ugunsmūra konfigurāciju, kas liedz eksponēt iekārtas pakalpojumus uz visiem interfeisiem. Sniegt tehnisko atbalstu un konsultācijas lietotājiem, kuri darba iekārtas izmanto attālinātam darbam.

Kriptovalūtas ieguves programmatūra

Kādā iekārtā identificēta kriptovalūtas ieguves programmatūra "XMRig", kas uzstādīta kā daļa no "Tari Universe" rīka (https://www.tari.com/). Papildus "XMRig" instalēts anonīmas saziņas tīkls "TOR", kas nepieciešams programmatūras darbībai. "Tari Universe" ir programmatūra, kas pievieno iekārtu decentralizētam kriptovalūtas ieguves tīklam, tā darbības laikā tiek izmantoti datora skaitļošanas resursi, lai iegūtu kriptovalūtu.

Ieteikums programmatūru aizliegt, jo būtiski tērēti uzņēmuma resursi (elektrība, aparatūras jauda), turklāt izmantošanas riskus palielina bieži nezināmie izcelsmes avoti. Programmatūras darbība var tikt izmainīta ļaunprātīgām darbībām un "TOR" izpildāmās datnes bieži izmantotas uzbrukumos komandkontroles (C2) nodrošināšanai, un ilgtermiņa piekļuvei.

Citu dažādu rīku izmantošana

Draudu medību procesā identificēta vairāku nevēlamu programmu izmantošana. Piemēram, "RusVPN", "Kaspersky Network Agent", "Proton VPN", "uTorrent", attālinātās pārvaldības rīks "Psexec", kā arī videospēles un programmatūra ar operētājsistēmas kodola līmeņa kodu.

Ieteikums kontrolēt programmatūras instalēšanu ar centralizētu risinājumu, kas uzstāda atļauto programmatūru. Papildu ieteikums ierobežot datņu izpildi pēc atrašanās mapes, piemēram, ja instalācijas fails ir koplietotā mapē, tad lietotāji to var izpildīt tikai no konkrētās koplietotās mapes. Tādā veidā ierobežotu gadījumus, kuros lietotāji izpilda nevēlamas datnes no "Downloads" vai "Desktop" direktorijām.

Sertifikātu datnes

Sertifikāta ".pfx" paroles glabāšana atklātā tekstā atrasta divās iekārtās skripta saturā vai PowerShell izpildīto komandu vēsturē. Ikviens ar tiesībām lasīt skriptus un žurnālfailus var iegūt paroli, tas rada būtisku apdraudējumu visu šīs paroles aizsargāto sertifikātu drošībai.Konstatēti vairāki skripti ar paroli saturā. Glabājot ".pfx" sertifikātu paroles atklātā tekstā, tiek atklātas to ietvertās privātās atslēgas. Tādēļ visi sertifikāti ir jāuzskata par kompromitētiem un ir jāaizstāj ar jauniem.

Sistēmas līmeņa tiesības bez paroles ievadīšanas

Pārskatot Linux komandrindas terminālī vēsturiski izpildītās komandas, vairākās iekārtās atrasta izpildīta komanda, kas lietotājam piešķir neierobežotas ("root") tiesības bez paroles ievadīšanas. Šāda konfigurācija rada papildu drošības riskus, jo būtiski atvieglo uzbrucējam privilēģiju paaugstināšanas iespējas.

Ieteikums pārskatīt esošos "/etc/sudoers" un "/etc/sudoers.d/*" ierakstus datnēs un attiecīgi dzēst "NOPASSWD" konfigurāciju. Nepieciešamības gadījumā atļaut lietotājiem izpildīt bez paroles tikai konkrētas komandas. Vēlams ieviest monitoringu un brīdinājumu ziņojumus par "/etc/sudoers" rediģēšanas gadījumiem.

Drošības testu pēdu nospiedumi

Pārskatot "Windows Defender" pretvīrusa auditēšanas ierakstus, konstatēts brīdinājums par atrastu speciāli izveidotu, nekaitīgu EICAR testa datni direktorijā "C:\Users*\Downloads". Šajā mapē padziļinātā iekārtas analīzē atrastas vairākas datnes, visticamāk, saistītas ar dažādiem drošības testiem, piemēram, pikšķerēšanas kampaņām.

Ieteikums par IKT drošību atbildīgajam personālam pārskatīt failu nepieciešamību atrasties iekārtā un pārliecināties par to izmantošanu darba pienākumu veikšanā.

Pornogrāfiska rakstura mājaslapu apmeklēšana

Draudu medību ietvaros analizēta tīmekļa pārlūkprogrammu vēsture. No kādas iekārtas bieži tiek apmeklētas zemas reputācijas mājaslapas ar pornogrāfisku saturu un meklētas datorspēļu video pamācības. Papildus novērots, ka lietotājs, iespējams, mēģinājis uzstādīt virtuālo platformu "VirtualBox" ar Windows 11 operētājsistēmu, lai varētu konfigurēt "Andorid" emulatoru ar "Bluestacks", un, visticamāk, spēlēt "AFK Journey" spēles mobilo versiju.

Šādu mājaslapu apmeklēšana ir bīstama, jo tajās bieži izvietota ļaunatūra. Ieteikums ieviest stingrāku tīmekļa izmantošanas politiku ar preventīviem risinājumiem, piemēram, pārlūka spraudņi aizdomīgu resursu bloķēšanai, kā "Ublock Origin Lite" (https://github.com/uBlockOrigin/uBOL-home). Tas ir atvērta pirmkoda risinājums, kas, izmantojot dažādus nevēlamu domēnu sarakstus, brīdina lietotāju par bīstamu vietņu apmeklēšanu. Ir pieejami arī publiski saraksti ar domēniem, kurus var ievietot iestādes ugunsmūrī vai starpniekserverī tīmekļvietņu satura apmeklēšanas kontrolei.

Kompromitēšanas gadījums

Draudu medībās konstatēts, ka uzņēmuma iekārta ir kompromitēta. Tajā konstatēti faili un žurnalēšanas ieraksti, kas liecina par inficēšanos ar ļaunatūru "XWorm" un "RemcosRAT".

2025. gada 5. novembris noteikts kā sākotnējais sistēmas kompromitēšana datums, kad ļaunatūru neatpazina sistēmas pretvīrusa programmatūra "McAfee". Tas turpinājās līdz 2025. gada 20. novembrim, kad to pretvīrusa programmatūra atpazina izdzēsa ļaunatūru. Visas darbības incidenta ķēdē izpildītas ar uzņēmuma gala lietotāju.

Pēc Uzņēmuma administratoru sniegtās informācijas noskaidrots, ka lietotājam nav aktīvās direktorijas administratoru tiesības.

Pēc pieejamās informācijas uzbrucēja tālāka pārvietošanās uzņēmuma tīklā netika identificēta.

Tehniskā Analīze

Ļaunatūra izplatīta ar USB zibatmiņu, kas sistēmai tika pievienota "2025-11-05 17:38:42 UTC". Kāds lietotājs pievienoja zibatmiņu, kurai tika piešķirts disks "E:\", tad novērota faila "E:\678876789765.CMD" izpilde. Pēc tam tiek izveidots pastāvīgas klātbūtnes mehānisms ar Windows uzdevumu pārvaldnieka plānoto notikumu "\Othyzbjwm", kas reizi 20 minūtēs izpilda failu "c:\users\public\othyzbjwm.url". Tas ir saīsnes "URL" tipa

fails, kas norāda uz izpildāmu datni “C:\Users\Public\Libraries\Othyzbjwm.exe”, kura MD5 jaucējfunkcijas vērtība (166ac66d27052926e1f8dedd6cdaa1c8) identificēta antivīrusa žurnālfailos. Platforma “VirusTotal” šo datni atpazīst kā trojas zirga vīrusu, visu minēto darbību secība un failu nosaukumi atbilst ļaunatūras “XWorm” izpildei (678876789765.CMD).

Ļaunatūras izveidotais uzdevumu plānotāja ieraksts:


```
"Time": "20251105-174229",
"Entry Location": "Task Scheduler",
"Entry": "\\Othyzbjwm",
"Enabled": "enabled",
"Category": "Tasks",
"Profile": "System-wide",
"Description": "",
"Signer": "",
"Company": "",
"Image Path": "c:\\users\\public\\othyzbjwm.url",
"Version": "",
"Launch String": "\"C:\\\\Users\\\\Public\\\\Othyzbjwm.url\" ",
"MD5": "B967CCAD9189B23601C3673D7F9207B8",
"SHA-1": "DD0AF402D54A86C20995994D6FA88667B59E3366",
"PESHA-1": "DD0AF402D54A86C20995994D6FA88667B59E3366",
"PESHA-256": "A525A1F912CCFDECC19F19FC4024FCC14BB7B22F122244321D723B6416214B4F",
"SHA-256": "A525A1F912CCFDECC19F19FC4024FCC14BB7B22F122244321D723B6416214B4F",
"IMP": ""
```


Sākotnējā piekļuve šāda tipa ļaunatūrai parasti tiek nogādāta ar pikšķerēšanas e-pastu. Saņemtajos e-pasta žurnālfailos nav pazīmes, ka pikšķerēšanas mērķis ir lietotāja darba e-pasts. Pēc administratoru sniegtās papildu informācijas noteikts, ka pievienotā USB zibatmiņa ir darbinieka privātā ierīce. Visticamākais sākotnējās kompromitēšanas cēlonis ir inficēts darbinieka privātais dators, pārnesot ļaunatūru privātajā USB zibatmiņā.

Veicot “XWorm” ļaunatūras analīzi, identificēti papildu indikatori - domēns “www[.]hulduo88[.]com” un IP adrese “167.71.255[.]27”. Tie atrodas pakalpojuma sniedzēja “Cheapy.host LLC” tīklā, kas vēsturiski saistīts ar tīkla skenēšanu, tīmekļa vietņu uzbrukumiem un kiberuzbrukumu simulācijas rīka “Cobalt Strike” komunikāciju nodrošināšanu. Datus ļaunatūra iegūst no teksta koplietošanas vietnes “Pastebin” (https[:]//pastebin[.]com/raw/3XznTkFA). Identificētā IP adrese pieder “DigitalOcean, LLC” infrastruktūrai, internetā pieejamā informācija norāda uz IP adreses dalību robotu tīklā, kas nodrošina “XWorm” ļaunatūras komandkontroles (C2) saziņu. Saziņa ar IP adresi (TCP ports 8912) atrasta administratoru dotajā ugunsmūra žurnālfailā. Pirmais savienojums identificēts 2025-11-05T17:42:40.000 UTC un pēdējais 2025-11-06T05:09:31.000 UTC.

Meklējot pēc datuma un laika (2025-11-05 21:25:32 UTC), identificēti vairāki PowerShell žurnālfailu notikumi, kuri atbilst attālinātās piekļuves rīka “Remcos” ļaunatūras izpildei. Pēc izpildes tika identificēta reģistra vērtības izveide “HKEY_USERS\\S-1-5-*-3255\\ Software\\ A35375309304E86FA6F3\\ 6E1D9460E74AA120B160941F284C 09563BA5E75BCEDC2006CB750793CE5BC3BB”. Šī reģistra vērtība satur “RemoteDesktop.dll” failu ar MD5 jaucējfunkcijas vērtību “ac409e8856618c3597647440d5d2ddc7”. Faila saturs ir “XWorm” ļaunatūras spraudnis, kas ļauj uzbrucējam attālināti kontrolēt sistēmu.

Tālākā darbībā 2025-11-05 23:22:17 UTC notika vairāku failu izpilde mapē “C:\Users*\AppData\Local\Temp\”. Faili tika izpildīti ar Windows iebūvēto programmatūru “wscript.exe”,

darbības atrastas pretvīrusu risinājuma “McAfee” žurnālfailā “AccessProtectionLog.txt”. “McAfee” paziņo, ka datņu izpilde tiktu bloķēta, ja konfigurācijā būtu iespējota skriptu bloķēšana no lietotāju “Temp” direktorijas. Taču funkcionalitāte nebija iespējota, izpildot skriptus:

- C:\Users*\AppData\Local\Temp\otkrqd.js;
- C:\Users*\AppData\Local\Temp\Incisalia.bat;
- C:\Users*\AppData\Local\Temp\luywsu.vbs.

Pēc to izpildes notiek faila “C:\users*\aoc.bat” izveide, kas veic saziņu ar kontroles serveri (C2) IP adresi 196.251.69[.]233. Līdzīgi savienojumi notiek 2025. gada 6. novembrī, kad izpildīts skripts “C:\Users*\AppData\Local\Temp\vpcekogz.vbs”. Pēc šiem savienojumiem ļaunatūra neveic papildu darbības līdz brīdim, kad 2025-11-20 02:07:14 UTC to izdzēš pretvīrusu sistēma.

McAfee žurnālfailos atrodama informācija par datnes Othyzbjwm.exe dzēšanu 20. novembrī.

Uzbrukuma izcelsmes noteikšana (atribūcija)

Uzbrucēja darbībās tika izmantotas vairāku tipu komerciālas ļaunatūras: “XWorm”, “Remcos” un “Cobalt Strike”. Izmantotā infrastruktūra, lai nodrošinātu komandkontroles (C2) saziņu, ir vēsturiski saistīta ar tīmekļa vietņu uzbrukumiem un skenēšanu.

Šāda tipa ļaunatūras visbiežāk izmanto finansiāli motivēti uzbrucēji. Apkopojot visus zināmos un konstatētos faktorus (infrastruktūru, mērķi un uzbrucēja spējas un rokrakstu), nevar noteikt saistību (atribūciju) ar konkrētu kibernoziedznieku grupējumu.

Turklāt uzbrukumā redzama tikai sākotnējās piekļuves daļa, kas neatspoguļo pilnu informāciju par uzbrucēju un izmantotajām metodēm. Rezultātā uzbrukumu var attiecināt (atribūtēt) komerciāli motivētam kiberuzbrukumu grupējumam, kas nav saistīts ar citu valstu (Krievija, Ķīna) atbalstītiem grupējumiem.

Ieteikumi

- Lai gan ļaunatūra vairs nav aktīva, lai pilnībā likvidētu tās saturu, ir nepieciešama iesaistītās iekārtas pārinstalēšana. Tikai tā var gūt pilnu pārliecību, ka draudi ir novērsti. Turklāt atkārtotās draudu medībās šie atradumi neietekmēs citu nesaistītu notikumu izmeklēšanu.
- Jāpārskata “McAfee” pretvīrusa programmatūras konfigurācija, jo vairāki ļaunatūras izpildīti skripti no lietotāja “Temp” direktorijas tika atpazīti kā kaitnieciskas datnes, taču netika bloķēti.
- Izmeklēšanas gaitā saņemta informācija, ka izmantotā iekārta paredzēta vienam lietotājam. Padziļinātā izpētē konstatēts, ka tajā atrodas vairāku lietotāju dati, liecinot par vairāku aktīvu lietotāju klātbūtni. Papildus to apliecina arī Windows notikumu žurnāls, kurā redzami citu lietotāju notikumu ieraksti. Šādai praksei ir vairāki riski, viens piemērs ir citu lietotāju piekļuves datu atrašanās Windows kešatmiņā. Ja uzbrucējam izdodas piekļūt sistēmai, tas varētu iegūt vairāku lietotāju piekļuves datus. Turklāt vairāku lietotāju vienlaicīgas darbības incidentu izmeklēšanu apgrūtina un palēnina.
- Tā kā kompromitēšanas cēlonis ir privāta USB zibatmiņa, jānodrošina organizācijas iekārtām tikai uzticamu USB zibatmiņu pievienošana. To ir iespējams realizēt ar Windows grupu politikas iestatījumiem.

Nedroša infrastruktūras pārvaldības prakse

Atklāta teksta paroles aktīvās direktorijas (AD) lietotāju kontu aprakstos

Veicot aktīvās direktorijas lietotāju analīzi, identificētas 49 lietotāju paroles kontu aprakstos tīrā tekstā, t.i., tipisku paroļu simbolu virknes. Liela daļa šo lietotāju konti ir iespējoti. Tā ir ļoti nedroša prakse, jo atvieglo un palielina iespēju uzbrucējiem iegūt piekļuves datus, kas var būt pamats tālākiem uzbrukumiem. Identificētās paroles bija ļoti vienkāršas, dažkārt iekļautas populāros paroļu sarakstos, ko bieži izmanto uzbrucēji, piemēram, "Qwerty123". Ieteikums piekļuves datus nomainīt un neuzglabāt kontu aprakstos, kā arī atspējot neizmantotos lietotājus. Pārskatīt paroļu veidošanas politiku, nepieļaujot vienkāršu paroļu lietošanu.

Nešifrēta attālinātās piekļuves protokola izmantošana

Veicot komandrindas Powershell vēstures pārbaudi, konstatēta attālinātās piekļuves "Telnet" izmantošana 7 dažādās iekārtās. Aplūkojot izpildītās "Telnet" komandas, konstatēts:

- Telnet pieslēgums ārēja resursa "powershellgallery[.]com" 443 portu;
- Telnet savienojumi pie ārējās IP * portiem 21, 80, 8080;
- Telnet savienojumi iekšējā tīklā uz SCCM portiem 8530 un 8531, kā arī portiem 22, 25, 443;
- Telnet savienojums pie diviem uzņēmuma e-pasta domēniem.

Nav ieteicams lietot "Telnet", jo sūtītie dati, arī paroles, tiek pārraidīti nešifrēti atklātā veidā, tādējādi uzbrucējiem sniedzot vieglas piekļuves iespējas. Ieteikums pārbaudīt uzskaitītās aktivitātes, kā arī nepieciešams izvērtēt "Telnet" nepieciešamību, apsverot alternatīvas, piemēram, droši šifrētas attālinātās piekļuves SSH protokolu.

Priviliģēti lietotāji

Pārskatot AD lietotāju piekļuves tiesības tika identificēti lietotāju un servisu konti ar, iespējams, pārmērīgi augstām piekļuves tiesībām, kas tikušas pārmantotas no citiem tiesību objektiem. Vairāki konti, piemēram – "Printeris" un "VeeamBack" servisa lietotāji — ar piederību dažādām grupām manto paaugstinātu piekļuvi, kas, visticamāk, pārsniedz minimāli nepieciešamo. Tas paaugstina dažādus infrastruktūras un domēna kompromitēšanas drošības riskus – neatļautu piekļuvi un pārvietošanos tīklā ("lateral movement").

Papildus jāizvērtē spēkā esošā paroļu politika. Jaunākās vadlīnijas vairs tik aktīvi neuzstāj 30-90 dienu nomaiņu, jo lietotāji bieži tās speciāli veido vienkāršākas.

Svarīgi ir papildu pasākumi paroles drošākai lietošanai:

- parolēm jābūt unikālām, lietotājiem jāzina riski ar vienas lietošanu vairākos pakalpojumos. Noplūdes gadījumā var tikt skarti visi pakalpojumi, kuros lietota viena parole;
- nepieciešamas skaidras un reāli ieviestas prasības parolēm attiecībā uz simbolu skaitu un sarežģītību. Pašlaik labā prakse ir fokuss uz paroles garumu nevis sarežģītību, turklāt garas frāzes ir vieglāk iegaumēt nekā simbolu kombinācijas;
- administratoriem paaugstināto tiesību dēļ tāpat ieteikts paroles mainīt biežāk;
- biežāka nomaiņa attiecas arī uz paaugstināta riska (piemēram, ārpakalpojuma u.c.) kontiem, kas parasti autentificējas no citas vides. Nepieciešama skaidra procedūra par VPN, administratīvās starpniekservera ("jumphost") izmantošanu;
- daudzfaktoru autentifikācijas lietošana;
- paroļu noplūdes monitorings.

9. Vispārīgie ieteikumi

Vispārīgas labās prakses lokālajiem sistēmu administratoru kontiem iesaka katrā iekārtā izmantot unikālu paroli, kas jāizveido ar paroļu ģeneratoru vai skriptu. Tādējādi liegts veidot paroles ar atšķirību vienā simbolā (burts/cipars/gads/mēnesis), piemēram, "Vasara2021", "Vasara2022 utt. Lokālo administratoru paroļu pārvaldībai ieteikts izmantot "Microsoft risinājumu "Local Administrator Password Solution" jeb "LAPS" (https://www.microsoft.com/en-us/download/details.aspx?id=46899).

Labā prakse ir uzglabāt vai pārsūtīt paroles šifrētā veidā, izmantojot paroļu pārvaldniekus, kuros var gan droši uzglabāt, gan ģenerēt jaunas, unikālas paroles. Ja piekļuves dati jānorāda kādā programmas kodā vai skriptā, tad vadlīnijas iesaka lietot paroļu glabātuvi ("Password Vault", "Keychain" u.c.).

Tā kā glabātuves ieviešana var būt laikietilpīgs process, ir daži īstermiņa pagaidu risinājumi. Piemēram:

- paroli glabāt atsevišķā teksta failā ar stingri ierobežotu pieeju tikai "SYSTEM\root" lietotājam, pašā skriptā piešķirot pieejas datus kā mainīgo ar norādi uz šo failu. Windows vidē lietot NTFS tiesības un, kur iespējams, faila līmeņa šifrēšanu;
- sertifikātu autentifikācija;
- domēna vidē Kerberos autentifikācija.

Administratoru papildu drošības mehānismi

- Ierobežot domēna administratorus, atļaujot pieslēgties tikai domēna kontrolieriem un, ja nepieciešams, atsevišķiem serveriem;
- Nepieļaut viena un tā paša domēna lietotāja piederību lokālā administratoru grupā vairākās iekārtās;
- Administratoriem stingri ieteicams izmantot nodalītas darbstacijas kontus dažādiem pārvaldības pienākumiem, piemēram, domēna kontrolierim viens lietotāja konts un atsevišķa darbstacija, serveriem cits konts, ikdienas darbiem – standarta lietotāja konts. Jāievēro minimālo nepieciešamo piekļuves tiesību princips. Piemēram, administratora vai Powershell izpildīšanas tiesības tikai tiem lietotājiem, kam nepieciešams, un tikai, kad nepieciešams. Vairāk informācijas par minimālo nepieciešamo piekļuves tiesību modeli ("Least-Privilege"): https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models;
- Tīkla administratoru kontiem izmantot "Protected Users" grupu, kas novērš paroļu jaucējvērtības ("hash") izgūšanu no sistēmas: https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group;
- Administratoriem darbā ar "Remote Desktop Protocol" aktivizēt "Restricted Admin Mode" režīmu - https://social.technet.microsoft.com/wiki/contents/articles/32905.remote-desktop-services-enable-restricted-admin-mode.aspx.

Programmatūras izvēle un konfigurācija

- Jāiepazīstas ar VDD sagatavotajiem ieteikumiem par informācijas tehnoloģiju produktu un pakalpojumu izvēli: https://vdd.gov.lv/uploads/materials/24/lv/it-drosibas-rekomendacijas.pdf;
- Nepieciešams izveidot vai pilnveidot atļautās programmatūras sarakstu un ieviest programmatūras pārvaldības politiku (AppLocker, SRP, ACB u.c.), kas darbojas sākot ar Windows 10 versiju lokālā vai mākoņpakalpojuma (Microsoft 365) infrastruktūrā. Pilnvērtīgākam tvērumam Microsoft iesaka visu risinājumu kombinēšanu;

- Pārliecināties par izslēgtu “AutoRun/AutoPlay” funkcionalitāti, lai iekārtas ārējā datu nesēja pievienošanas brīdī “AutoRun” komandas netiks automātiski izpildītas. Tas gan nepasargā no paša lietotāja uzklikšķināšanas uz kāda inficēta datu nesēja faila. Papildu informācija saitēs:
  https://www.stigviewer.com/stig/microsoft_windows_11/2024-06-10/finding/V-253387
  https://www.stigviewer.com/stig/microsoft_windows_11/2024-06-10/finding/V-253386
  https://www.stigviewer.com/stig/microsoft_windows_11/2024-06-10/finding/V-253388
  https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-autoplay
- Rīka “Sticky Keys” izslēgšana ar “PowerShell” komandām un grupu politiku:
  Set-ItemProperty -Path "HKCU:\Control Panel\Accessibility\StickyKeys" -Name "Flags" -Type String -Value "506"
  Set-ItemProperty -Path "HKCU:\Control Panel\Accessibility\ToggleKeys" -Name "Flags" -Type String -Value "58"
  Set-ItemProperty -Path "HKCU:\Control Panel\Accessibility\Keyboard Response" -Name "Flags" -Type String -Value "122"

Pretvīrusu risinājumi

- Izvēlēties vienu NATO, ES vai EEZ dalībvalstī izstrādātu pretvīrusu risinājumu visām Windows iekārtām. Pārliecināties par nepieciešamo atjauninājumu saņemšanu. “Windows Defender” izmantošanas gadījumā noteikti jāiespējo uzbrukuma virsmas samazināšanas (“Attack Surface Reduction”) nosacījumi: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-deployment?view=o365-worldwide;
- Antivīrusa risinājumā konfigurēt iekārtai pievienotu ārējo datu nesēju skenēšanu. Bieži noklusējuma iestatījums šai funkcionalitātei ir izslēgts. “Microsoft Defender” risinājuma izmantošanas gadījumā informācija saitē: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-advanced-scan-types-microsoft-defender-antivirus?view=o365-worldwide;
- “Microsoft Defender” iestatīt failu jaucējvērtību (“hash”) attēlošanu skenētajām datnēm, kas šaubu gadījumā sniedz iespēju pārbaudīt brīdinājumus ārējos resursos, piemēram, VirusTotal meklētājā. Konfigurēšana iespējama domēna grupu politikā “Computer Configurations\Administrative Templates\Windows Components\Microsoft Defender Antivirus\MpEngine\Enable file hash computation feature”.

Tīmekļa pārlūkprogrammas “Google Chrome” paplašinājumu kontrole

- Centralizēti pārvaldīt “Google Chrome” paplašinājumus ar aktīvās direktorijas grupu politiku administratīvo veidni “ADMX”;
- Ieteikums konfigurēt šādus “Google Chrome” grupu politiku iestatījumus:
  Configure extension installation allow list (atļautie paplašinājumi)
  Configure extension installation block list (bloķētie paplašinājumi)
  Extension install force list (obligāti uzstādāmie paplašinājumi)
- Papildu informācija: https://support.google.com/chrome/a/answer/187202?hl=en#zippy=%2Cwindows

Ierīču konfigurācija

- Regulāri atjaunot Microsoft Windows Server operētājsistēmas. Iekārtām ar "Server 2012 R2 Standard" versiju pāriet uz šobrīd aktuālo "Server 2022" vai "Server 2025".
  Microsoft programmatūras atbalsta informācija vietnē: https://learn.microsoft.com/lv-lv/lifecycle/products/
- Domēnā atslēgt novecojušos "Kerberos" protokola šifrēšanas algoritmus, izmantot tikai "AES" paaudzi ("AES128_HMAC_SHA1" un "AES256_HMAC_SHA1");
- Windows domēnā aizliegt NTLM autentifikāciju, pārejot uz "Kerberos" protokolu;
- Atslēdzot NTLM autentifikāciju, vispirms jāveic testi. Ir vecākas paaudzes sistēmas, piemēram RDP, Outlook u.c., kas joprojām izmanto "NTLM" autentifikāciju, tādējādi riskējot radīt darbības traucējumus. Testa režīmu var ieslēgt grupu politikas sadaļā "Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options" iestatījumā "Network Security: Restrict NTLM: Audit NTLM authentication in this domain". Pēc tam serveru auditēšanas žurnālu ierakstos "Applications and Services Log\Microsoft\Windows\NTLM\Operational" var novērot autentifikācijas pieprasījumus. Izņēmumus var iestatīt: "Network security: Restrict NTLM: Add server exceptions in this domain". Tikai pēc pārbaudes veikšanas var ieslēgt "Network Security: Restrict NTLM: NTLM authentication in this domain". Gadījumos, kad lielākā daļa servisu atkarīga no "NTLM" protokola, iesākumā var atspējot tikai ienākošo "NTLM" autentifikāciju "Network security: Restrict NTLM: Incoming NTLM traffic -> Deny All Accounts".

Infrastruktūras uzraudzība

- Regulāri veikt iekārtu skenēšanu gan no iekštīkla, gan publiskā tīmekļa, lai pārliecinātos, ka internetā netiek eksponēti nevajadzīgi pakalpojumi un porti. Ja darba vajadzībām "Microsoft Windows" iekārtā tomēr nepieciešama piekļuve no ārpuses (visbiežāk novērots "Remote Destop Protocol"), jāievieš drošības mehānismi;
- Automātiska lietotāju bloķēšana (account lockout) gadījumos, kad veikti vairākkārtīgi neveiksmīgi autentifikācijas mēģinājumi, instrukcijas: https://cert.lv/uploads/materiali/Windows-domain-account-lockout.pdf
  https://cert.lv/uploads/materiali/Local-Windows-account-lockout.pdf;
- Jāievieš atļauto IP adrešu saraksts, no kurām drīkst veikt pieslēgumus. Piemēram, tikai no Latvijas IP adrešu apgabaliem (https://www.nic.lv/lix) vai atļaut piekļuvi tikai no VPN iekštīkla, ievērojot mazāko nepieciešamo piekļuves tiesību principus;
- Atļaut izmantot "Remote Desktop Protocol" tikai ierobežotam lietotāju lokam, veicot drošu konfigurāciju un pieeju nodrošinot tikai iekštīklā;
- Iestatīt vismaz 14 simbolu paroli;
- paredzēt obligātu paroles maiņu reizi mēnesī;
- Izmantot divu faktoru autentifikāciju;
- Atļaut piekļuvi tikai no VPN tīkla, ievērojot mazāko nepieciešamo piekļuves tiesību principu;
- Regulāri pārbaudīt iestādes domēna lietotāju datus publiskās datu noplūdēs, piemēram, "HaveIbeenPwned": https://haveibeenpwned.com/DomainSearch;
- Droši konfigurēt gan serverus, gan darbstacijas pēc labās prakses vadlīnijām, piemēram, "STIG" (https://www.stigviewer.com/stigs), kur pieejamas rekomendācijas gan populārākajām operētājsistēmu versijām, gan konkrētai programmatūrai. Pieejams arī Microsoft izstrādāts rīku kopums "Windows Security Baselines", kas palīdz Windows administratoriem novērtēt domēnā

situāciju un konfigurēt atbilstoši labajai praksei (https://www.microsoft.com/en-us/download/details.aspx?id=55319);
- Iepazīties ar CERT.LV sagatavoto informāciju par kompromitēta Windows domēna atpazīšanu, risku mazināšanu un atgūšanos pēc uzbrukuma ("Mitigation/Hardening"): https://cert.lv/lv/2020/04/rekomendacijas-auditesanas-iestatijumiem-windows-domena-infrastruktura;
- Izskatīt CERT.LV sniegtos pakalpojumus un pieteikties pēc nepieciešamības, vairāk informācijas skatīt šeit: https://cert.lv/lv/pakalpojumi.

Centralizēta žurnālfailu ievākšana un uzturēšana

- Jānodrošina centralizēta audita ierakstu uzglabāšana un monitorings (SIEM), jāpārliecinās, ka laika zīmogs konfigurēts atbilstoši mītnes valsts laika zonai;
- Jāizveido aizdomīgu darbību automātiski brīdinājumi, jāsūta uz e-pastu un citām tūlītējās ziņojumapmaiņas platformām;
- Iepazīties ar CERT.LV izstrādātajām rekomendācijām auditēšanas iestatījumiem Windows domēna infrastruktūrā: https://cert.lv/lv/2020/04/rekomendacijas-auditesanas-iestatijumiem-windows-domena-infrastruktura;
- Ministru kabineta noteikumu Nr. 397 nodaļa 3.9. par žurnālfailu pārvaldību nosaka, ka subjektam jānodrošina informācijas sistēmu žurnālfailu un tīkla plūsmas žurnālfailu veidošanu. Nodaļā noteikts, kas iekļaujams žurnālfailos, kā arī noteiktas drošības prasības un žurnālfailu uzglabāšanas ilgums: A klases informācijas sistēmām un to darbību nodrošinošām operētājsistēmām, pakalpēm (servisiem), tīklu un serveru iekārtām – vismaz 18 mēnešus pēc ieraksta izdarīšanas; B klases informācijas sistēmām un to darbību nodrošinošām operētājsistēmām, pakalpēm (servisiem), tīklu un serveru iekārtām – vismaz 12 mēnešus pēc ieraksta izdarīšanas; C klases informācijas sistēmām un to darbību nodrošinošām operētājsistēmām, pakalpēm (servisiem), tīklu un serveru iekārtām – vismaz 6 mēnešus pēc ieraksta izdarīšanas;
- Veikt ne tikai Windows serveru un darbstaciju auditācijas pierakstu un monitoringu SIEM sistēmā, pārliecināties par datu saņemšanu arī no tīkla iekārtām, starpniekserveriem, VPN vārtejām un maršrutētājiem.

Windows ugunsmūra konfigurācija

Windows ugunsmūris jeb "Windows Defender Firewall with Advanced Security" (WFAS) ir būtisks lokālās darbstacijas drošības elements. Ir zināms, ka ugunsmūra primārā funkcija ir bloķēt nevēlamu vai kaitniecisku ienākošo tīkla plūsmu. Taču situācijās, kad darbstacija jau ir uzlauzta vai inficēta, svarīgs ugunsmūra uzdevums neatļaut uzbrucējam vai ļaunatūrai izejošo tīkla plūsmu. Tādējādi uzbrukums var tikt ierobežots vai pat apturēts vienas darbstacijas ietvaros. Svarīgi pieminēt, ka pareizi konfigurēts ugunsmūris liedz vai būtiski apgrūtina uzbrucēja pārvietošanos iekštīklā starp dažādām darbstacijām.

Windows ugunsmūra (WFAS) priekšrocības

- ērta centralizēta pārvaldība, izmantojot domēna kontroliera grupu politiku;
- integrēts Windows operētājsistēmā bez papildus maksas;
- funkcionalitāte "Connection Security Rules" ir Kerberos autentifikācija pirms atļaut izveidot savienojumu. Autentificēt var atsevišķi lietotāju vai tikai darbstaciju, vai abus vienlaicīgi;
- IPsec savienojuma šifrēšana.

Pēc visu Windows darbstaciju un serveru ugunsmūra nosacījumu ("rules") analīzes, veikti šādi secinājumi un izveidoti ieteikumi:

1. Lietojumprogrammai vai lietotnei (*.exe, *.dll) gandrīz visos gadījumos ienākošā tīkla plūsma visiem TCP un UDP protokolu portiem ir atļauta, daudzos gadījumos atļauti arī visi tīkla protokoli. Rodas vairāki riski, piemēram, aizvietojot leģitīmu *.exe ar ļaunatūru, tai tiks atļauti visi ienākošā tīkla savienojumi. Apgrūtināta ikdienas pārvaldība un incidentu izmeklēšana. Ieteikums. Darbstacijas pareizas ugunsmūra konfigurācijas ieviešanā ir vairākas līdzvērtīgi pareizas metodes, taču svarīgākais ir rīkoties pakāpeniski un procesu sadalīt etapos. Vispirms sašaurināt atļautās tīkla plūsmas darbību, ierobežojot secīgi protokolu, tad portu vai diapazonu. Pēc tam norādīt konkrēta *.exe, servisa vai lietotnes atļauto portu vai diapazonu un, ja iespējams, norādīt savienojuma avota IP adresi vai apgabalu. Vēlams izmantot "Connection Security rules", īpaši šo ieteicams lietot sistēmu administratoriem pārvaldības darbiem.
2. Papildu ieteikums par "Connection Security Rules" ir veikt rūpīgu analīzi un testus, sākt ar nelielu izmēģinājuma darbstaciju grupu. Pat minimāla konfigurācijas nesakritība var bloķēt leģitīmus savienojumus. Obligāti jānodrošina rezerves plāns, piemēram, komandrinda ar laika izpildi, kas atslēdz ugunsmūra nosacījumu.
3. Neierobežoti atļauta visa izejošā tīkla plūsma pēc noklusējuma. Ieteikums limitēt analoģiski punktā Nr.1.
4. Jāieslēdz ugunsmūra savienojumu ierakstu žurnāls ("Windows Firewall Log").
5. Lokālā vai centralizētā grupu politikā jāiespējo notikumu žurnāla savienojuma objektu ieraksti (sadaļa "Advanced Audit Policy Configuration").
6. Pēc žurnālu ierakstu ieslēgšanas punktos Nr.4 un Nr.5, Windows ugunsmūrī atrastie aizdomīgie nosacījumi ietvers ne tikai savienojumu IP adreses un portus, bet lietotņu nosaukumus. Tas kalpos notikumu vēstures izmeklēšanai vai apliecinās lietotnes pašreizējo eksistenci, ļaujot izvērtēt tās nepieciešamību un veikt atinstalēšanu vai ugunsmūra nosacījuma pielāgošanu.

Windows ugunsmūra nosacījuma izveidošanas fakts parāda, ka programmatūras uzstādīšanas vai izmantošanas brīdī lietotājam bijušas administratora privilēģijas (ugunsmūra izņēmumus nav iespējams izveidot standarta lietotājiem).

Universāls ceļvedis IKT vides sakārtošanai

Plāns ir veidots vidēja lieluma uzņēmuma vajadzībām, taču to var izmanot arī kā praktisku orientieri un ideju avotu mazām un lielām organizācijām.

1. Digitālās saimniecības uzskaite:

    1.1. Tehniskais inventārs - serveri (t.sk. datu centros izvietotie serveri), darbstacijas un portatīvie datori, tīkla iekārtas, perimetram ("edge") iekārtas, mākoņskaitļošanas risinājumi, mobilās ierīces, lietotnes, programmatūra, kā arī ārpakalpojumu ietvaros izmantotie IKT risinājumi;

    1.2. Informācija par katru resursu: par katru uzskaitīto inventāru jābūt zināmai šādai informācijai - īpašnieks vai atbildīgā persona, resursa nozīmīgums, versija un konfigurācijas statuss, ražotāja tehniskā atbalsta statuss, žurnālfailu pieejamība, resursa mērķis un loma, lietošanas nolūks, ārpakalpojuma sniedzēja atbildība zona un citi nozīmīgi tehniskie un organizatoriskie fakti.

2. Programmatūras pārvaldība un kontrole:

    2.1. Vadības saskaņota, autorizēta;

2.2. Skaidrs process jaunas programmatūras ieviešanai un apturēšanai;

2.3. Ieviesti un pārbaudīti programmatūras, lietotņu pārvaldības un kontroles risinājumi (piemēram, Microsoft AppLocker, ACB vai analogi).

3. Programmatūras un sistēmu atjaunošana:

3.1. Īpaša uzmanība jāpievērš un prioritāri jāatjaunina iekārtas un sistēmas, kas ir pieejamas no interneta, piemēram, VPN risinājumi, ugunsmūris u.c.;

3.2. Iekštīklā izmantot centralizētu atjaunojumu pārvaldību.

4. Identitātes un kontu pārvaldība:

4.1. Obligāta daudzfaktoru autentifikācija (MFA) e-pastam, VPN, administratoru kontiem, mākoņskaitļošanas platformām;

4.2. Administratora kontu nodalīšana;

4.3. Koplietotu kontu aizliegums (izņemot īpaši pamatotus gadījumus);

4.4. Organizācijas darba iekārtas tikai darbinieku lietošanai;

4.5. Vienots standarts paroļu pārvaldībai (piemēram, KeePass).

5. Žurnālfaili un pārredzamība:

5.1. Žurnālfailu iespējošana, centralizēta uzkrāšana un notikumu analīze;

5.2. **CERT.LV SOC pakalpojuma ieviešana** (https://cert.lv/lv/pakalpojumi);

5.3. Labās prakses izmantošana (jāizmanto iekārtu, programmatūras izstrādātāju drošības vadlīnijas un labās prakses) .

6. Rezerves kopiju nodrošināšana:

6.1. Jānodrošina regulāra būtisko sistēmu un datu rezerves kopēšana;

6.2. Regulāra atjaunošanas pārbaude;

6.3. Rezerves kopiju nodalīšana no ikdienas darba vides.

7. **Incidentu gatavība un novēršana** (https://cert.lv/lv/pakalpojumi).

7.1. Kiberdrošības draudu medības, uzlabojumu rīcības plāns un izpilde;

7.2. Kiberapdraudējumu simulācija, uzlabojumu rīcības plāns un izpilde;

7.3. Pikšķerēšanas uzbrukumu simulācija;

7.4. Personāla apmācība – jānodrošina regulāras, praktiskas un konkrēto darbinieku pienākumiem atbilstošas kiberdrošības apmācības.

Personāla apmācības un kiberdrošības kultūras veicināšana

- Visiem darbiniekiem un līgumdarbiniekiem veikt periodiskas apmācības, kas aptver pamata kiberdrošības tēmas (pikšķerēšana, biznesa e-pasta kompromitēšana, operacionālā drošība, paroļu drošība utt.) un veicina iekšējo drošības un kiberdrošības kultūru. Apmāciet lietotājus aizdomīgu e-pastu atpazīšanā;

- Pielāgojiet apmācību tīkla IT personālam, administratoriem un citiem atbildīgajiem darbiniekiem, pamatojoties uz organizācijai aktuāliem kiberdraudiem. Nodrošināt operacionālo tehnoloģiju (“OT”) personālam jomas specifisku kiberdrošības apmācību vismaz reizi gadā;
- Izglītot lietotājus par riskiem, uzglabājot neaizsargātas paroles;
- Nodrošināt personālam iekārtas tikai darba pienākumu veikšanai;
- Veikt darbinieku zināšanu pārbaudi, tostarp regulāras pikšķerēšanas simulācijas kampaņas, papildinot tās ar apmācībām un reāliem piemēriem. Iekļaut pikšķerēšanas simulācijās organizācijas vadību. Ieteikums izmantot CERT.LV pikšķerēšanas uzbrukumu simulācijas pakalpojumu;
- Kiberdrošības pārvaldniekiem vismaz reizi gadā ir jāapmeklē CERT.LV organizētas apmācības. Regulāri organizējiet darbinieku apmācības par aktuālajiem kibervides riskiem vismaz reizi gadā. CERT.LV piedāvā lekcijas, praktiskas kiberincidentu izspēles galda spēles un seminārus;
- Regulāri sekot CERT.LV tīmekļvietnei un sociālo mediju kontiem par aktualitātēm kibertelpā.

10. 2026./2027. gada kiberdrošības apdraudējuma prognoze Latvijai

10.1. Vispārējā draudu intensitāte

2026. gada garumā prognozējams draudu intensitātes pieaugums vai vismaz saglabāšanās augstā līmenī. Sagaidāms, ka 2026. gadā un turpmākajos gados galvenais apdraudējuma paātrinātājs būs mākslīgā intelekta (MI) izmantošana kiberuzbrukumu automatizācijā, kā arī ātrākā un kvalitatīvākā uzbrukumu komponentu sagatavošanā: ievainojamību izmantošanas rīki tiek izstrādāti arvien ātrāk pēc informācijas par ievainojamību vai programmatūras ielāpu publiskošanas (kritiskām ievainojamībām pat 24 stundu logā), bet par infrastruktūras sargāšanu atbildīgais personāls, procedūras un reaģēšanas spējas šo tempu bieži nespēj sasniegt.

Lai gan mākslīgā intelekta pielietojums tuvākajā laikā nerada principiāli jaunus apdraudējumus, tas neizbēgami veicinās lielāku incidentu skaitu ar uzbrucējiem labvēlīgu apsteidzošu efektu. Lai pretstāvētu šiem draudiem, ir kritiski svarīgi pārzināt savu infrastruktūru, uzturēt pilnvērtīgu tās inventarizāciju, interneta tīklā atstāt pieejamus tikai tādus servisus, kuriem pēc savas būtības ir pamatoti jābūt plaši pieejamiem, drošības pārbaudes un nocietināšana (hardening) veicama pilnīgi visiem interneta tīklā pieejamajiem servisiem, daudzfaktoru autentifikācija ir obligāta visiem interneta tīklā pieejamajiem autentifikācijas moduļiem.

Tāpat jānodrošina pilnvērtīga auditācijas pierakstu uzglabāšana un apstrāde, lai spētu identificēt un novērst incidentus - SOC / SIEM spējām jākļūst par obligāti pieejamām, jāpilnveido programmatūras versiju un ielāpu pārvaldība, kā arī vispārējā kiberdrošības tehnisko ierobežojumu politika valsts iestāžu, kiberdrošības likuma subjektu un kritiskās infrastruktūras turētāju tīklos, piemēram, atļauto lietotņu saraksta uzturēšana, tīkla segmentācija un mazāko privilēģiju lietošanas prakse.

CERT.LV turpinās jau sekmīgi uzsākto darbu pie Latvijas kiberdrošības apdraudējuma spektra kartēšanas, Kiberdrošības draudu medību, SOC, ABS un citu pakalpojumu (https://cert.lv/lv/pakalpojumi) attīstības, kā arī arvien ciešākas Latvijas kiberdrošības kopienas iesaistes apdraudējumu atklāšanā, piemēram, CVD (https://cvd.cert.lv) platformas ietvaros, lai arvien ātrāk un efektīvāk identificētu apdraudējumu un veicinātu tā novēršanu, padarot Latviju par neparocīgu mērķi kiberuzbrucējiem.

Nozaru specifiskie riski

Nozare	2026./2027. gada riska raksturojums
Valsts pārvalde un vēlēšanu infrastruktūra	Paaugstināta uzmanība sagaidāma saistībā ar vēlēšanu procesiem. Turpināsies Latvijai nedraudzīgu valstu (APT) un organizētās noziedzības grupu izlūkošana un pikšķerēšana pret ministrijām, pašvaldībām un valstij nozīmīgiem uzņēmumiem.
Enerģētika un OT/rūpnieciskās vadības sistēmas	Ar Krieviju saistīti grupējumi turpinās kartēt OT vidi; publiski internetā eksponētas un nedroši konfigurētas OT pārvaldības saskarnes paliks galvenais sākotnējās piekļuves vektors. Latvijai jāveido apsteidzošas spējas - CERT.LV to jau dara, novērsti vairāki desmiti ievainojamību, kuru izmantošana varēja novest pie incidenta. Subjektiem jāveicina atbildīgāka tehnoloģiju ieviešana un ārpakalpojumu uzraudzība.
Elektronisko sakaru un telekomunikāciju nozare	"Salt Typhoon" tipa Ķīnas un Krievijas kiberspiegošanas kampaņas pret telekomunikāciju operatoriem ES jau skārušas vismaz 3 dalībvalstis — augsta varbūtība uzbrukumiem ar apsteidzošas pozicionēšanās nolūku paplašināties uz Baltijas operatoriem.

Nozare	2026./2027. gada riska raksturojums
Finanšu sektors	Turpināsies finansiāli motivētu grupējumu izspiešanas kampaņas; pieaugs sarežģītāku un daudz ticamāku, MI ģenerētu krāpšanas shēmu apjoms.
Veselības aprūpe un pašvaldības	Ierobežoti IT resursi, operacionālais modelis un novecojusi infrastruktūra padara šīs nozares neproporcionāli neaizsargātas pret kiberuzbrukumiem, kas var rezultēties gan datu noplūdēs, gan infrastruktūras sabotāžas incidentos. CERT.LV viena no nākamā gada prioritātēm būs pievērst šīm iestādēm papildu uzmanību.

Uzbrukumu vektori un metodes

- **Identitāte kļūst par jauno perimetru:** pieaugošs fokuss uz akreditācijas datu zādzību (lietotājvārdi, paroles, piekļuves atslēgas), daudzfaktoru (MFA) apiešanas tehnikām un servisa/API kontu ļaunprātīgu izmantošanu. Mākoņpakalpojumu noklusētā konfigurācija ne vienmēr ir droša - ir svarīgi ieviest papildu kontroles - piemēram, atslēgt nevajadzīgo funkcionalitāti (“device code authentication”), nocietināt pakalpojumus pret nesankcionētu piekļuvi. Incidentus veicinās arī pavirša risinājumu izstrāde un akla uzticēšanās MI rīku sagatavotiem risinājumiem, izstrādātāju pavirša programmatūras koda un koda versiju kontroles sistēmu pārvaldība. Piemēram, ik gadu notiek vairāki būtiski incidenti dēļ nedroši eksponētām GIT instancēm, kurās pieejami programmatūras izstrādes materiāli, pirmkods, API atslēgas, utt.
- **"Malware-as-a-Service" / "Phishing-as-a-Service" un MI demokratizācija:** gatavu uzbrukuma rīkkopu pieejamība pazemina tehnisko kompetences slieksni; MI rīki paātrina pikšķerēšanas satura lokalizāciju un ticamību.
- **Piegādes ķēdes un uzticēto pakalpojumu izmantošana:** svarīgi savlaicīgi identificēt piegādes ķēdes apdraudējumu - pakalpojumu, aprīkojuma un programmatūras kontekstā. Dažādu čaulas kompāniju, "bulletproof hosting", kompromitētu mājas un mazā biznesa iekārtu un leģitīmu mākoņpakalpojumu ļaunprātīga izmantošana uzbrucēju operācijās turpinās veicināt arvien sarežģītāku atribūcijas procesu un uzbrukuma pēdu slēpšanu. Piegādes ķēdes drošības apdraudējums turpinās būt aktuāls arī no kompromitētu vai nedroši pārvaldītu ārpakalpojumu sniedzēju sniegtajiem pakalpojumiem, tāpēc jāpievērš īpaša uzmanība piekļuves un integritātes kontrolēm, kuras var ietekmēt ar ārpakalpojuma starpniecību - attālināta pārvaldība (RDP, VNC, utt), VPN piekļuves, programmatūras integrācija, u.c.
- **Novecojušas, neatjauninātas internetā eksponētas sistēmas:** VPN vārtejas, ugunsmūri, maršrutētāji, tīmekļvietnes (WEB), API saskarnes, e-pasta sistēmas un RDP paliks visbiežāk izmantotais sākotnējās piekļuves vektors. Uzbrucējs vienmēr prioritizēs tādu sistēmu kompromitēšanu, kuras uztur pati mērķa iestāde, nevis ārpakalpojuma datu centrs. Tas tādēļ, ka no mērķa iestādes uzturētas sistēmas ir lielāka iespējamība pēc pirmā sekmīgā uzbrukuma pārvietoties dziļāk infrastruktūrā. Atbilstoši šai hipotēzei ir apzināti jāplāno aizsardzības politika.

Hibrīdo un fizisko draudu dimensija

Gan 2026., gan 2027. gadā sagaidāma turpmāka kiberdraudu un fizisko/hibrīdo draudu konverģence Baltijas jūras reģionā: zemūdens kabeļu un cauruļvadu sabotāžas mēģinājumi, GPS/navigācijas traucēšana un Krievijas "ēnu flotes" kuģu aizdomīga darbība turpināsies paralēli kiberizlūkošanai, kas kartē to pašu infrastruktūru. NATO iniciatīvas ("Baltic Sentry", "Nordic Warden") jau uzrādījušas rezultātus, taču reģiona atkarība no jūras dibena infrastruktūras pieaug straujāk nekā aizsardzības spējas.

Hakeru aktīvisms un DDoS

DDoS uzbrukumi saglabāsies kā skaitliski biežākais, taču zemas tehniskās sarežģītības incidentu veids. Uzbrukumu intensitāte cieši korelēs ar politiskiem notikumiem — publiskots atbalsts Ukrainai vairumā gadījumu izraisa tūlītēju pro-Krievijas hakeru aktīvistu reakciju; līdzīga dinamika iespējama arī saistībā ar notikumiem Tuvajos Austrumos.

Kopsavilkuma prognožu tabula

Dimensija	2025. gada bāzlīnija	2026./2027. gada prognoze
Kopējā incidentu intensitāte	Straujš pieaugums visā reģionā	Turpmāks pieaugums vai augsta līmeņa saglabāšanās; MI paātrina uzbrukuma ciklu.
Dominējošais draudu tips	Krāpšana/DDoS (apjoms), APT (ietekme)	Identitātes/piekļuves uzbrukumi kā galvenais vektors; DDoS turpinās kā fona troksnis.
Krievijas draudi	Dominējošais valstiskais apdraudējums	Turpinās kā primārais draudu avots; augsts eskalācijas potenciāls.
Ķīnas draudi	Pieaugoša, iepriekš nenovērtēta aktivitāte	Prasa pastiprinātu uzmanību 2026. un 2027. gadā; fokuss uz telekomunikācijām, akadēmisko vidi.
Fiziskā/hibrīdā dimensija	Zemūdens kabeļu incidenti, ēnu flote	Turpināsies paralēli kiberizlūkošanai; NATO spējas uzlabosies, bet nesasniegs pilnu pārklājumu.

10.2. Ieteikumi un darbības fokusa virzieni

Balstoties uz iepriekš aprakstītajām tendencēm, Latvijas valsts iestādēm, pašvaldībām, kritiskās infrastruktūras un privātā sektora organizācijām ieteicams:

Obligātais minimums (jāsasniedz visiem)

- Daudzfaktoru autentifikācija (MFA) visiem attālinātās piekļuves, e-pasta, jebkurai internetā pieejamai autentifikācijas pakalpei, VPN un administratoru kontiem — vēlams ar phishing-noturīgām metodēm (FIDO2/WebAuthn/Passkey), nevis SMS/OTP, bet, ja tomēr ir kaut kāda MFA implementācija, tas vienalga ir labāk, nekā ja tās nav vispār.
- Pilna IT resursu inventarizācija un regulāra ievainojamību pārvaldība ar īsu ielāpu ieviešanas ciklu — īpaši internetā eksponētām sistēmām.
- Centralizēta žurnālfailu uzkrāšana un uzraudzība (SIEM/SOC), ar spēju identificēt un izolēt skartās sistēmas automatizēti vai pietuvināti reāllaikam.
- Privileģēto kontu pārvaldība (PAM), administratora un ikdienas lietotāja kontu nodalīšana, minimālo nepieciešamo tiesību princips.
- Microsoft AD infrastruktūras un darbstaciju centralizēta pārvaldība, vēlams ar Microsoft native rīkiem.

Nozaru un infrastruktūras līmenī

- OT/rūpniecisko vadības sistēmu (enerģētika, ūdensapgāde, siltumapgāde) segmentācija no korporatīvā IT tīkla un pārvaldības saskarņu izņemšana no publiskā interneta.
- Paplašināti, mērķēti IT sistēmu drošības testi (t.sk. Red Teaming / Purple Teaming) kritiskās infrastruktūras un vēlēšanu infrastruktūras subjektiem.
- Piegādes ķēdes riska pārvaldība — pastiprināta uzmanība trešo pušu IT pakalpojumu sniedzējiem, kas var kalpot kā netiešs piekļuves ceļš uzbrucējiem.

Reģionālās un starptautiskās sadarbības līmenī

- Aktīva dalība NATO un ES koordinētajās iniciatīvās (CERT.LV nacionālā un starptautiskā sadarbība, NATO Locked Shields mācības, "Baltic Sentry"/"Nordic Warden" tipa fiziskās infrastruktūras aizsardzības mehānismi).
- Indikatoru un draudu izlūkošanas datu (IOC/CTI) apmaiņas trupmāka padziļināšana ar partnervalstīm.
- Latvijas un Kanādas sadarbības attīstīšana kiberaizsardzības un kiberdraudu medību starptautisko apmācību jomā.
- Sabiedrības informēšana par krāpšanas un pikšķerēšanas riskiem, jo šis apdraudējuma veids skar visplašāko iedzīvotāju loku.

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

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

gan citiem interesentiem.

Saziņa ar CERT.LV:

Tālrunis: +371 67085888

E-pasts: cert@cert.lv

Tīmekļa vietne: cert.lv

Sekot CERT.LV aktualitātēm:

@cert.lv