Kiberdrošības situācija Latvijā

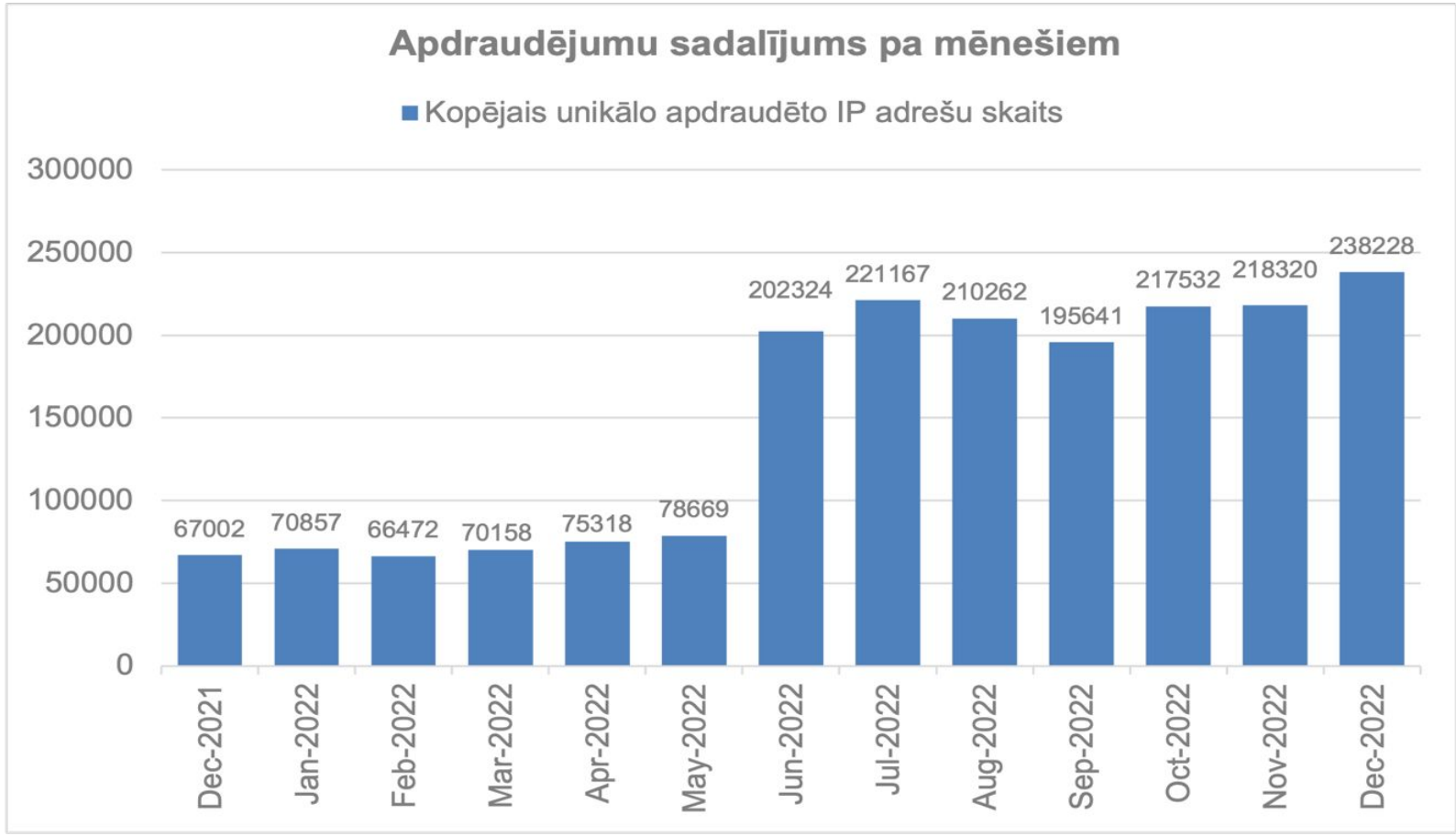
ESET SECURITY DAY LATVIA

26.09.2023. - Varis Teivāns

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

2022.gads Latvijas kibertelpā

- **Incidentu pieaugums – 40%**
- **Valsts sektoram uzbrukumu apjoms – x4**
- **Ievainojamību meklēšana – x7**



Jaunāko APT uzbrukumu laika nogrieznis

Sākotnējās piekļuves mēģinājumi un realizācija
Pakalpojumu sniedzēji, Valsts un Kritiskā infrastruktūra
Maijs 2021

Strauji palielinās aktivitāte
Gulošo (jau kompromitēto) aģentu aktivizēšana
Janvāris 2022 - Maijs 2022

Vairāk kā ducis kompromitētu mērķu
Pakalpojumu sniedzēji, Valsts un Kritiskā infrastruktūra
Marts 2022 - Septembris 2022

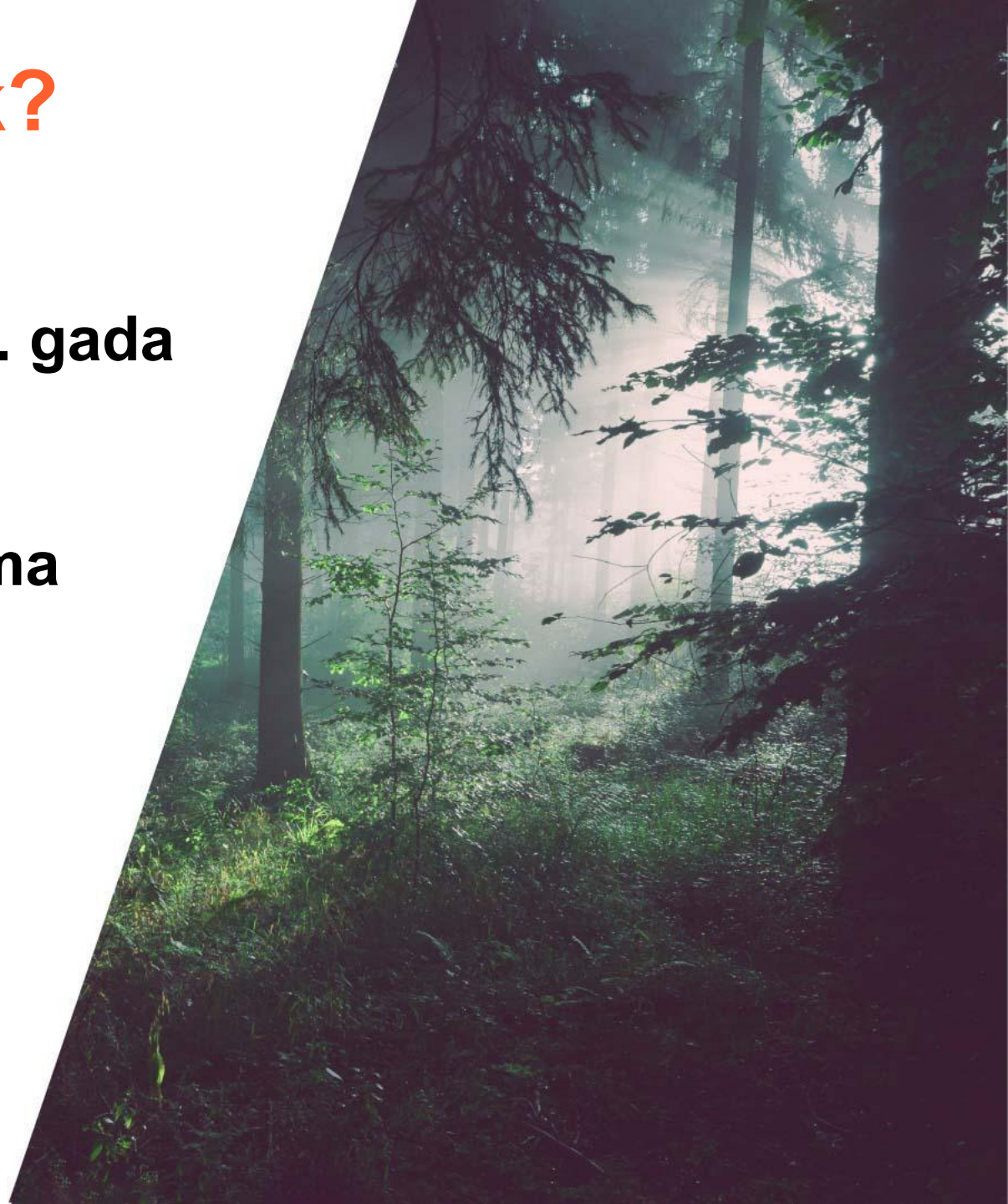
CERT.LV draudu medības
Mar 2022 - šim brīdim

Aktīva uzbrucēja pretdarbība
RED vs BLUE
Apr 2022 - tagad

Kas Latvijai uzbrūk?

Krievija realizē plaša mēroga kiberoperācijas vismaz kopš 2007. gada (Agent-BTZ, Turla, …)

Latvijā kiberdrošības apdraudējuma līmenis noteikts kā augsts kopš 2022. gada janvāra.



Kiberoperācijas pret LV

Krievija

Ķīna

Baltkrievija?

Krievijas kiberoperāciju piemēri e-pastā

From MINISTRY OF DEFENSE OF UKRAINE <military-of-ukraine@web-mail.website> ☆ Reply Reply All Forward More

Subject **Providing additional military assistance to the defenders of Ukraine** 17.05.22 14:12

To

Šis ir ārējs e-pasts, lūdzu pievērsiet uzmanību avota autentiskumam.

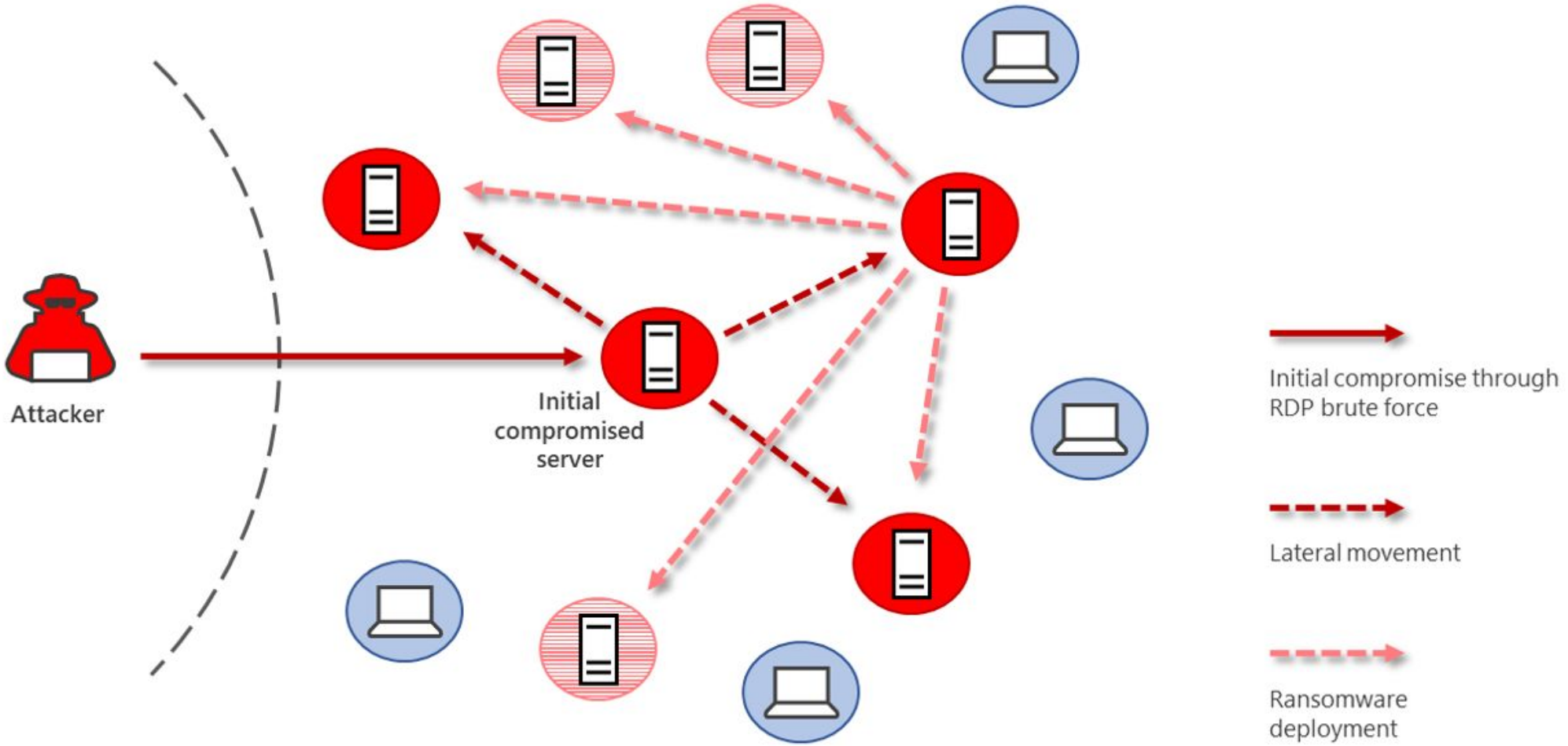
In connection with the ongoing military aggression of the Russian Federation against the civilian population of Ukraine, I ask you, as an official representative of the state, a friend of our country, to contact the Minister of National Defense - Commander of the Armed Forces, to consider providing additional military and humanitarian assistance to the defenders of Ukraine.

Deputy Commander for Armaments -
Head of the Technical Department
Major General (MG) Yevgeny Gerasimenko

MINISTRY OF DEFENSE OF UKRAINE
6, Povitroflotskyi Sq., Kyiv

1 attachment: Military assistance of Ukraine.htm 180 KB Save

Sākotnējās piekļuves un kontroles izvēršanas piemērs



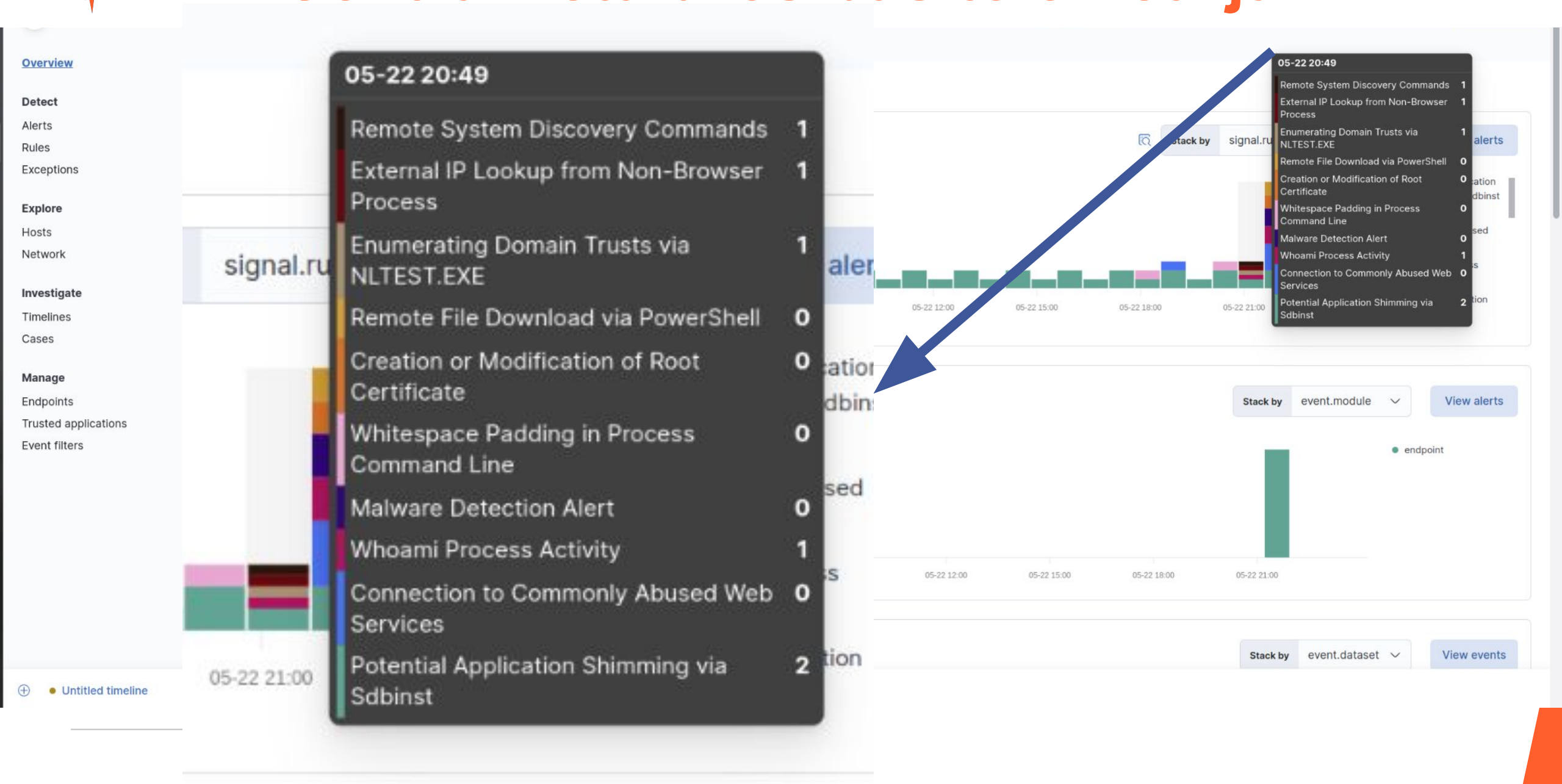
Gatavība sākotnējās uzbrukuma fāzes / piekļuves pamanīšnai un reakcijai

CERT.LV

RECON

whoami
ipconfig /all
nslookup -type=SRV ldap._tcp.dc._msdcs.//domain
curl http://ifconfig.me
net use
net view
ping 8.8.8.8
arp -a
nltest /domain_trusts
nbtstat -n
tasklist /svc

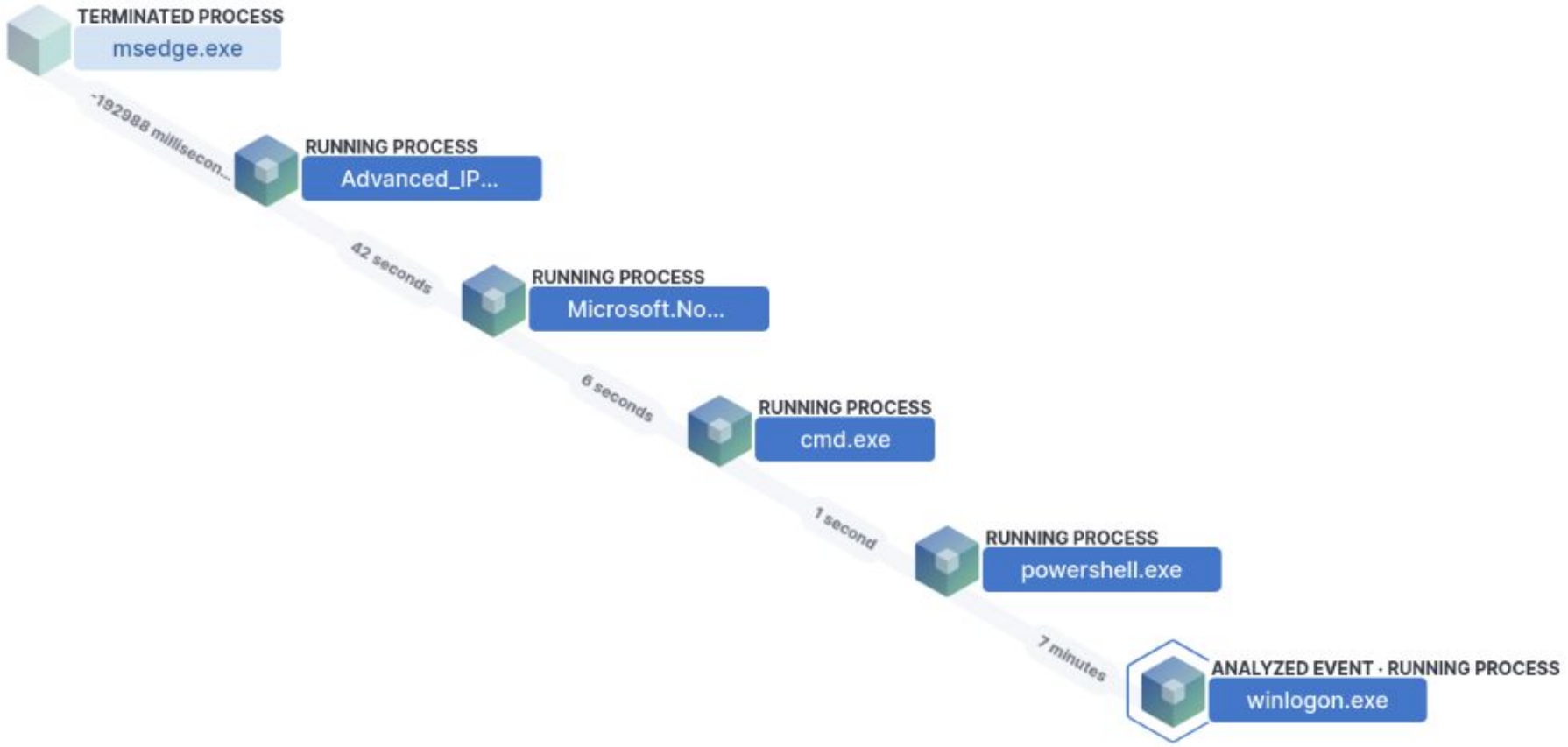
Centralizēta drošības telemetrija



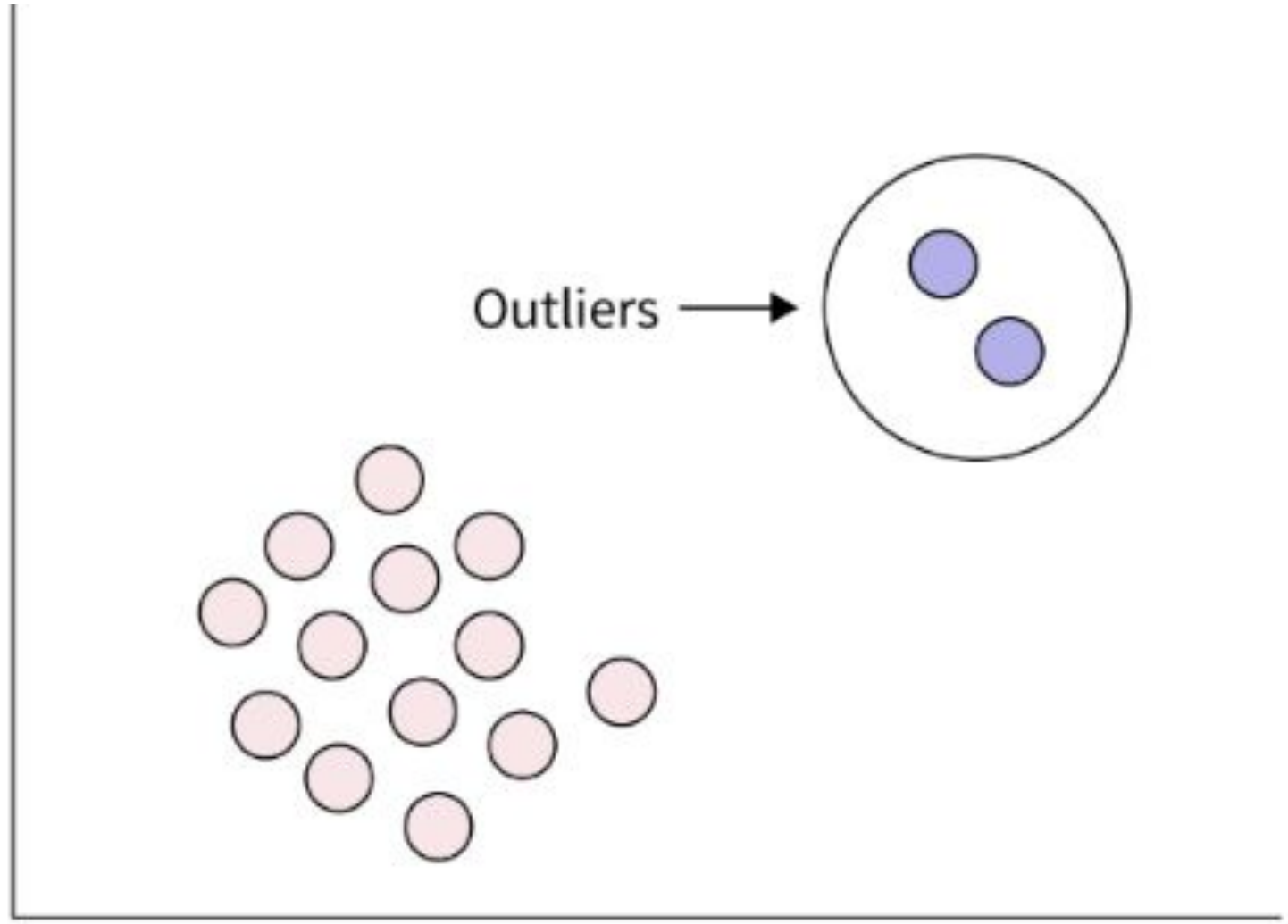
Centralizēta drošības telemetrija
Uzbrucējs ir pliks…

All Process Events

Process Name	Timestamp
msedge.exe	May 24, 2023 @ 16:58:50.355
Advanced_I...	May 24, 2023 @ 16:55:37.367
Microsoft.N...	May 24, 2023 @ 16:56:19.677
cmd.exe	May 24, 2023 @ 16:56:25.762
powershell....	May 24, 2023 @ 16:56:27.053
ANALYZED EVE... winlogon.exe	May 24, 2023 @ 17:03:49.527



Sākotnējās piekļuves fāzē vienmēr būs “izlecēji” un tie ir jāpamana



Virzība uz nobriedušas kiberaizsardzības līmeni

Uzbrucēja TTPs simulācija

JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:CLEAR | Product ID: AA23-129A

May 9, 2023

Communications Security Establishment | Centre de la sécurité des télécommunications
Canadian Centre for Cyber Security | Centre canadien pour la cybersécurité
National Cyber Security Centre
Australian Government Australian Signals Directorate | ACSC Australian Cyber Security Centre
National Cyber Security Centre

Hunting Russian Intelligence "Snake" Malware

SUMMARY

The Snake implant is considered the most sophisticated cyber espionage tool designed and used by Center 16 of Russia's Federal Security Service (FSB) for long-term intelligence collection on sensitive targets. To conduct operations using this tool, the FSB created a covert peer-to-peer (P2P) network of numerous Snake-infected computers worldwide. Many systems in this P2P network serve as relay nodes which route disguised operational traffic to and from Snake implants on the FSB's ultimate targets. Snake's custom communications protocols employ encryption and fragmentation for confidentiality and are designed to hamper detection and collection efforts.

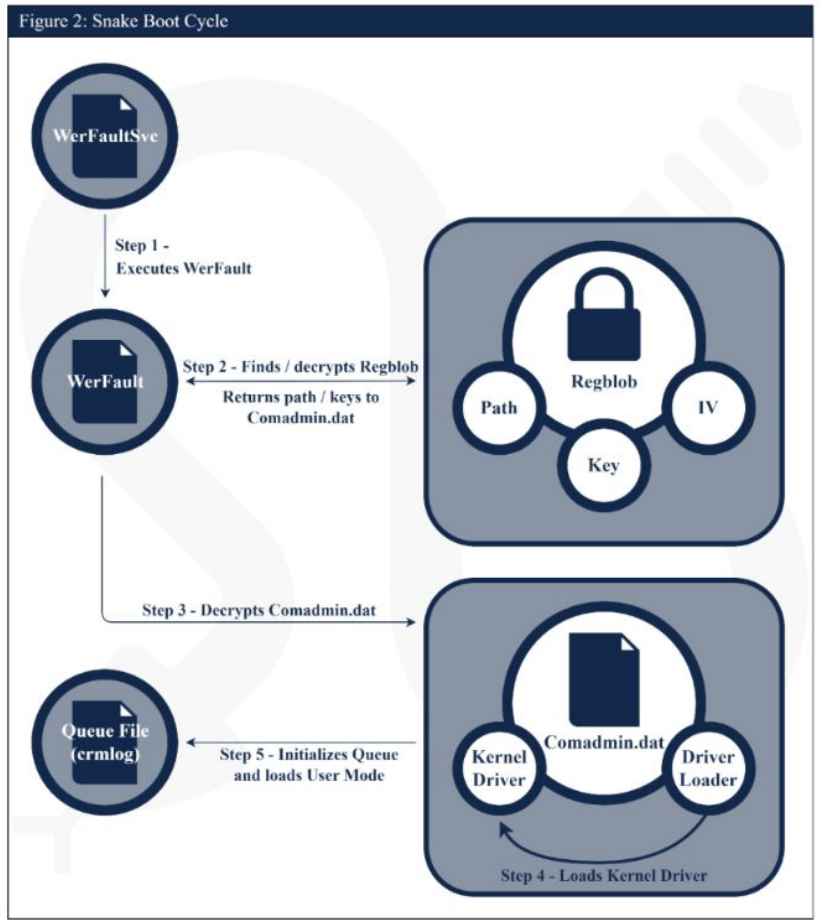
We have identified Snake infrastructure in over 50 countries across North America, South America, Europe, Africa, Asia, and Australia, to include the United States and Russia itself. Although Snake uses infrastructure across all industries, its targeting is purposeful and tactical in nature. Globally, the FSB has used Snake to collect sensitive intelligence from high-priority targets, such as government networks, research facilities, and journalists. As one example, FSB actors used Snake to access and exfiltrate sensitive international relations documents, as well as other diplomatic communications, from a victim in a North Atlantic Treaty Organization (NATO) country. Within the United States, the FSB has victimized industries including education, small businesses, and media organizations, as well as critical infrastructure sectors including government facilities, financial services, critical manufacturing, and communications.

This Cybersecurity Advisory (CSA) provides background on Snake's attribution to the FSB and detailed technical descriptions of the implant's host architecture and network communications. This CSA also addresses a recent Snake variant that has not yet been widely disclosed. The technical information and mitigation recommendations in this CSA are provided to assist network defenders in

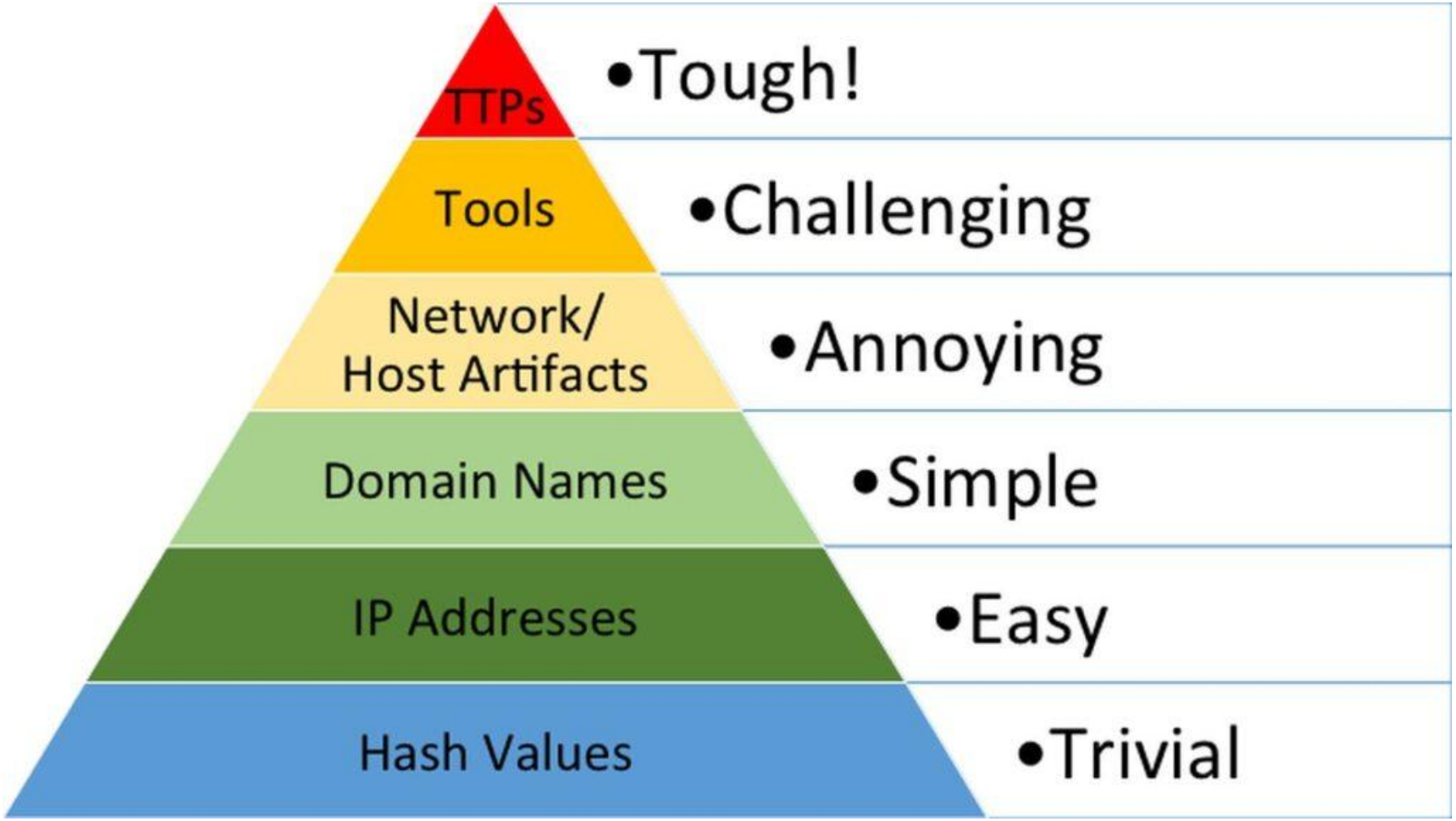
Persistence Mechanism

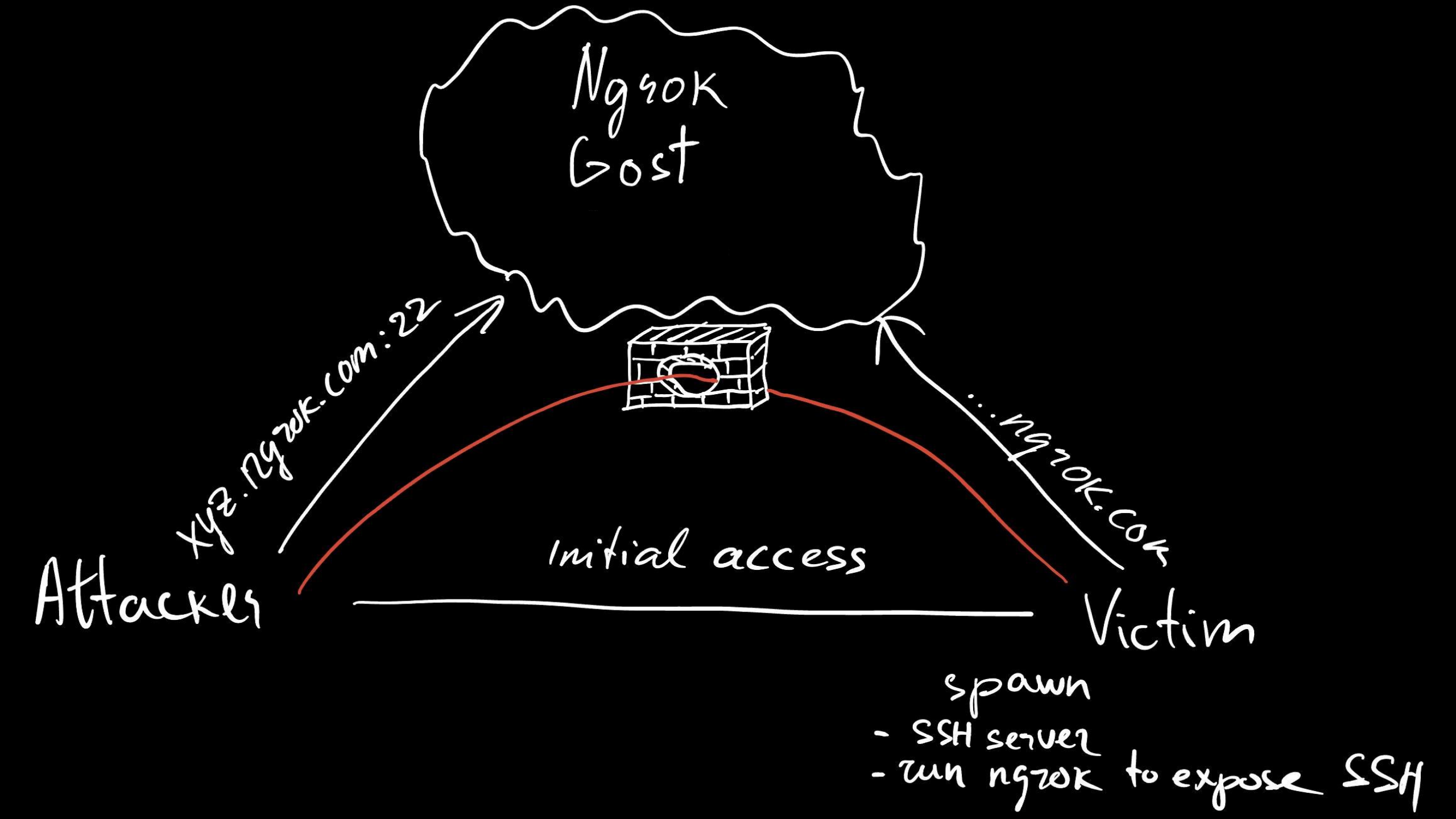
The Snake version primarily discussed in this advisory registers a service to maintain persistence on a system. Typically, this service is named "WerFaultSvc," which we assess was used to blend in with the legitimate Windows service WerSvc. On boot, this service will execute Snake's WerFault.exe, which Snake developers chose to hide among the numerous valid Windows "WerFault.exe" files in the %windows%\WinSxS\ directory. Executing WerFault.exe will start the process of decrypting Snake's components and loading them into memory.[11]

Figure 2: Snake Boot Cycle



Spēja rekonstruēt uzbrukuma detaļas, rīku, taktiku un procedūru identificēšana

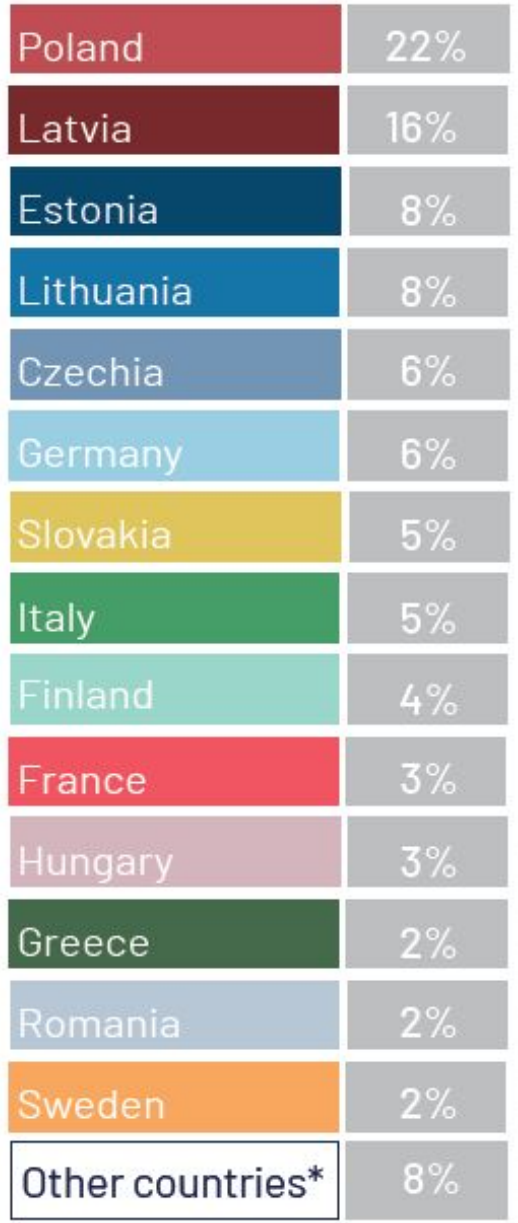



Ngrok
Gost
xyz.ngrok.com:22
...ngrok.com
Initial access
Attacker
Victim
spawn
- SSH server
- run ngrok to expose SSH

Kam visvairāk uzbrūk Eiropas savienībā?

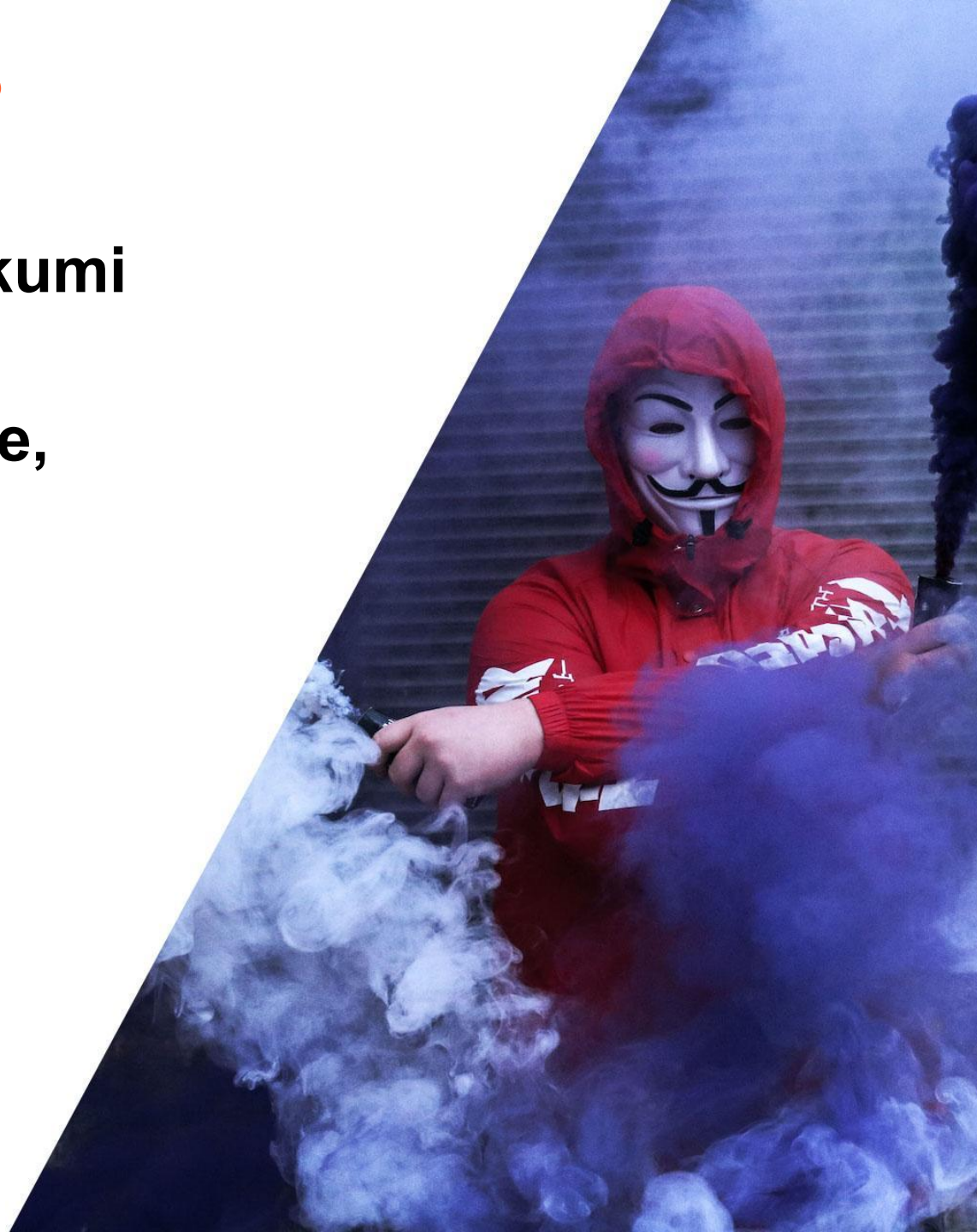
CERT-EU apskats:

RUSSIA'S WAR ON UKRAINE: ONE YEAR OF CYBER OPERATIONS



Kas Latvijai uzbrūk?

- Piekļuves lieguma – DDoS uzbrukumi
- Citas haktīvistu aktivitātes (deface, phishing, data leaks, InfoOps)
- RU dienestu atbalstītas kiberoperācijas - Cadet Blizzard, Ghostwriter, Gamaredon, Turla…
- Komerciāli motivēti uzbrukumi

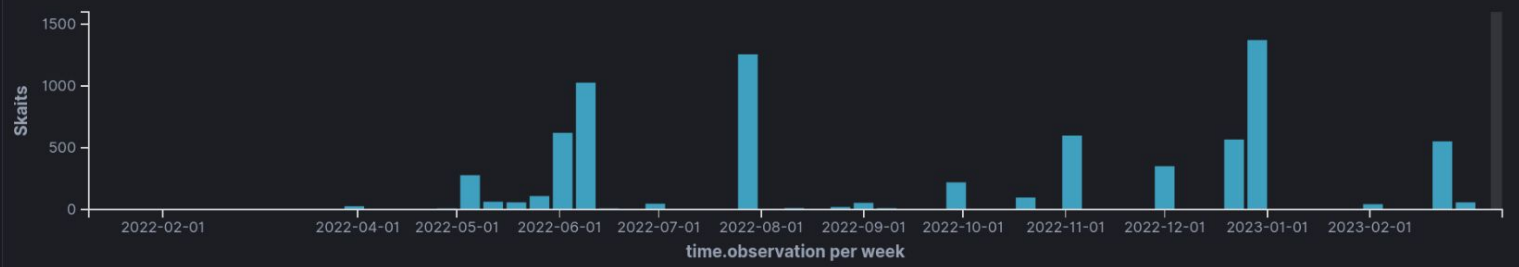


DDoS noturība - KI

Total count

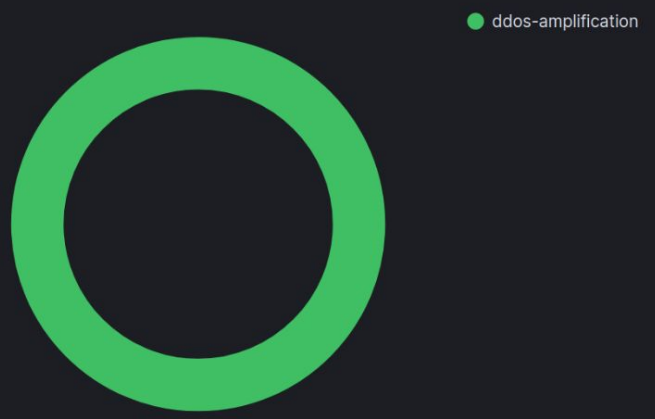
7547
Count

Time histogramm

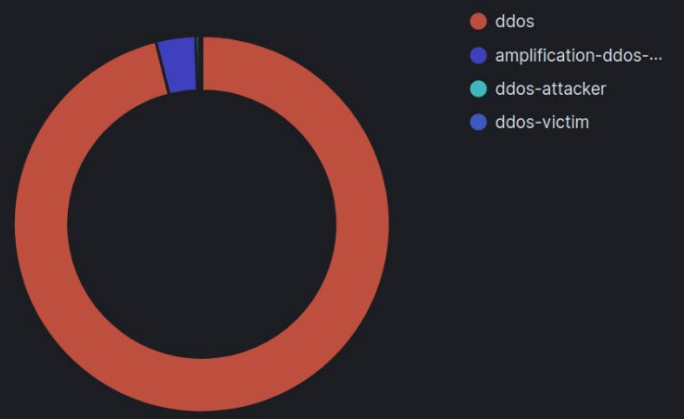


	Count
	7251
	257
	39

Top malware.name



Top classification.identifier



	Count
	7251
Events	257
	23
	16

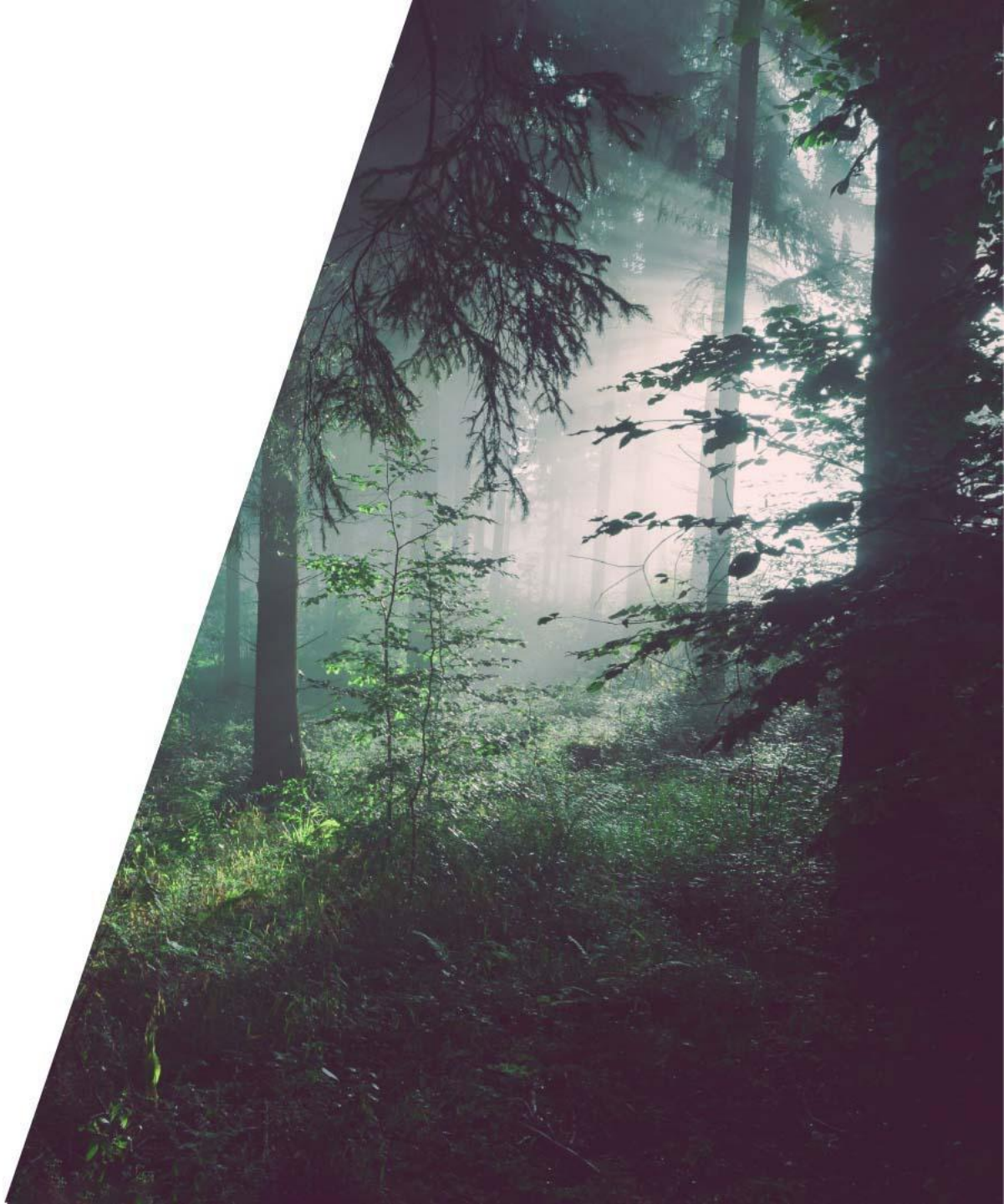
Categorisation matrix

≥ 5 and < 6	0	0	0	0	0	0
≥ 4 and < 5	0	0	0	0	0	0
≥ 3 and < 4	0	0	0	2438	2296	88
≥ 2 and < 3	0	0	0	288	2001	122
≥ 1 and < 2	0	0	0	0	63	251

DDoS noturība

Esam cienījami pretstāvējuši apjomīgākajiem un ilgstošākajiem DDoS uzbrukumiem pateicoties:

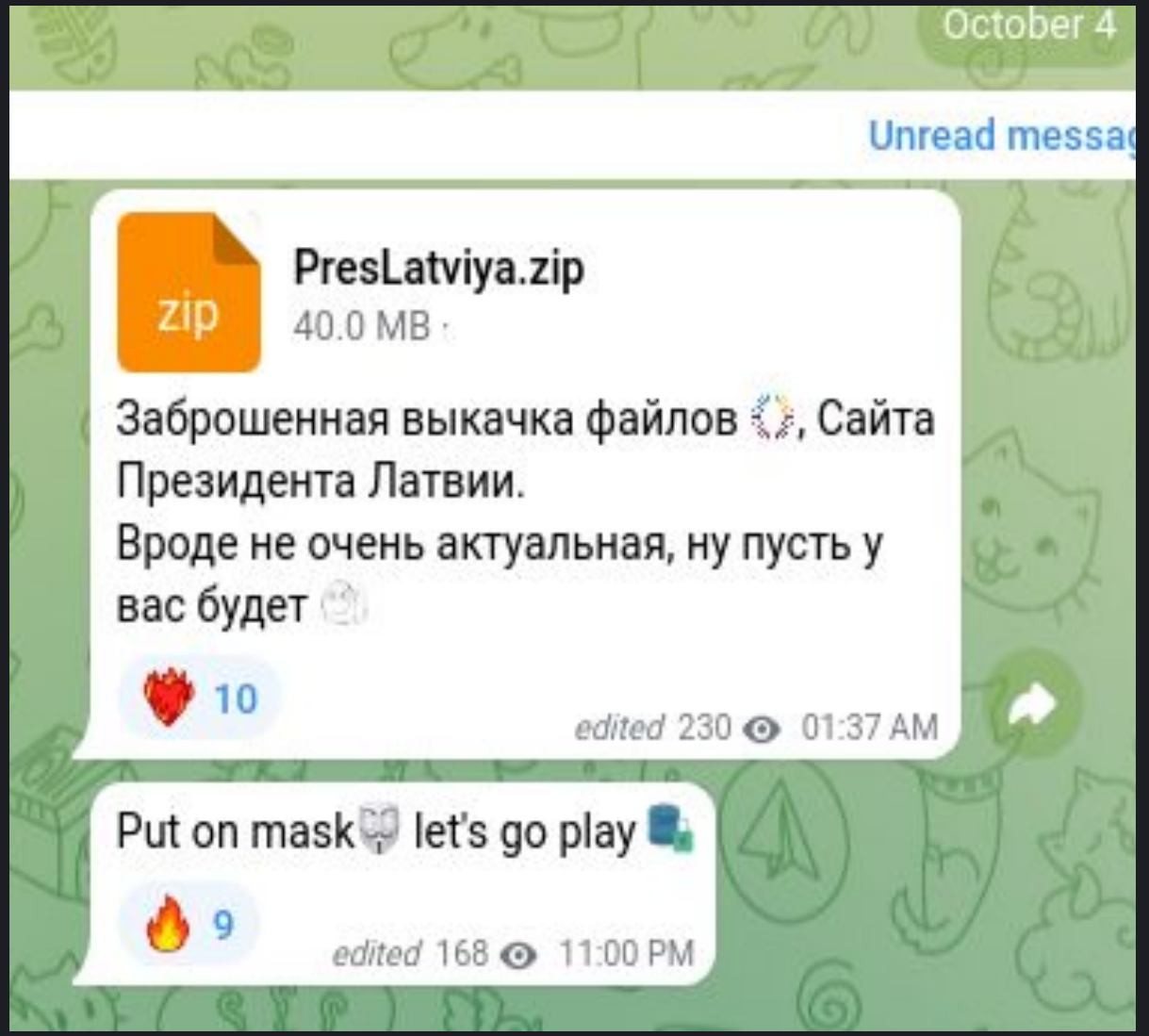
… un daudziem citiem partneriem!



Krievijas agresiju atbalstošais PR - haktīvisti

krievu haktīvistu PR :)

```
┌──(kali㉿kali)-[~/Desktop/Выкачка]
└─$ ls
03072017-lemums_degviela.pdf
2011-gada-parskats_budzeta-izpilde.xls
20130611_1994_2004tzo.doc
20160406kandidatu_atlases_nolikums.doc
201607_nolikums.doc
201607_pazinojums_par_lemumu_degviela.doc
201608_nolikums.doc
201608_pazinojums_par_lemumu.doc
20160908_nolikums-az_2.docx
20160927_noteikumi.doc
20161007pazinojums_par_lemumu.doc
20161011_noteikumi-1_0.doc
20161122_noteikumi_0.doc
201611_noteikumi_0.doc
20161214_gleznu_kopijaspazinojums_par_lemumu.doc
20161214_pazinojums_par_lemumu_0.doc
20161214_rotajumi_pazinojums_par_lemumu_0.doc
20170309_finansu_pied_forma_i.xlsx
20170309_nolikums.doc
201706_atk_finansu_piedavajuma_forma_1_dala.xlsx
201706_atk_finansu_piedavajuma_forma_2_dala.xlsx
201706_finansu_piedavajuma_forma_1_dala-1.xlsx
201706_nolikums.doc
201708_nolikums.docx
201709_davanu_vitrinas_nolikums.doc
201711.doc
201715_lemums.doc
201716_nolikums.doc
201716_pielikumi.zip
201717_lemums.doc
201717_nolikums.doc
201718_lemums.doc
201720_nolikums.doc
201721_nolikums-1.doc
356EBC_27_0.woff2
fikseto_balss_sakaru_pakalp_nolikums.docx
finansu-piedavajuma-forma.docx
iepirkuma-pielikumi-i-dala.zip
iepirkuma-pielikumi-ii-dala.zip
ievas-silinas-intervija-rigas-aprinka-avizei-kodols-20.08.2019.1.pdf
lemums_interneta_pieslegums.pdf
lemums_par_iepirkuma_partrauksanu.pdf
lemums_ziedi.doc
lvpk_2017_10_nolikums.docx
nolikums_garderobe.doc
nolikums_word_ar_grozijumiem_0.docx
noteikumi1.doc
noteikumi_degviela.doc
pazinojums_par_lemumu_181116_edinasana_0.doc
tehniska-piedavajuma-forma.docx
tehniska-specifikacija.doc
vpk_2015_zino_110416.docx
web.config
```



krievu haktīvistu PR :) “uzbrukums” manabalss.lv

Антифашисты Прибалтики 🇱🇻🇱🇹 ...

Огромная благодарность группе NoName за прекрасно проведенную операцию по взлому сервера нацистского шабаша на Manabals с голосованием за депортацию русских стариков!

К сожалению, не получилось деанонимизировать все 10 000 нацистов, но часть из них всё-таки удалось выцепить. Все полученные списки будут переданы в СК РФ с просьбой привлечь указанных лиц к ответственности за издевательство над гражданами РФ на территории Латвии, за возрождение и реабилитацию нацизма и покушению на геноцид по национальному признаку.

Здесь мы опубликуем малую часть ставших известными нам фамилий, исключительно чтобы продемонстрировать - мы знаем про вас всё. Мы знаем кто вы, где вы и мы не простим вам преступления вашего неонацистского режима. Враг будет уничтожен. Победа будет за нами!

Agnese Kurša
Aigars Stārks
Aija Vlasa
Aivars Krivmans
Aleksandrs Šverns
Aleksejs Zubrickis
Anda Ulme

Telegram: Contact @antifalivland

Renars Arnicans
Arturs Kriviss
Linda Curika
Andris Dzintars
Jane Doe
Vineta Mekone
Elina Lange
Simona Lucatniece
Una Aleksandra Bērziņa – Čerenkova
Tomass Pildegovičs
Ieva Viese-Vigula
Liina Lumiste
Māris Andžāns
Nora Biteniece
Jānis Uplejs
Elizabete Auniņa
Nika Aleksejeva
Ēriks K. Selga
Sanda Svetoka

Pašorganizētas grupas…?

: vk.link

: wagner2022.ru, wagnercentr.ru → 24. jūnijs 2023

Noņemtie mērķi

: www.skm.pkp.pl, metro.waw.pl, www.rbinternational.com.pl

: www.pts.se

: www.danishshipping.dk, www.moviatrafik.dk

: e-journal.iea.gov.ua, zno.testportal.com.ua

: www.evofenedex.nl

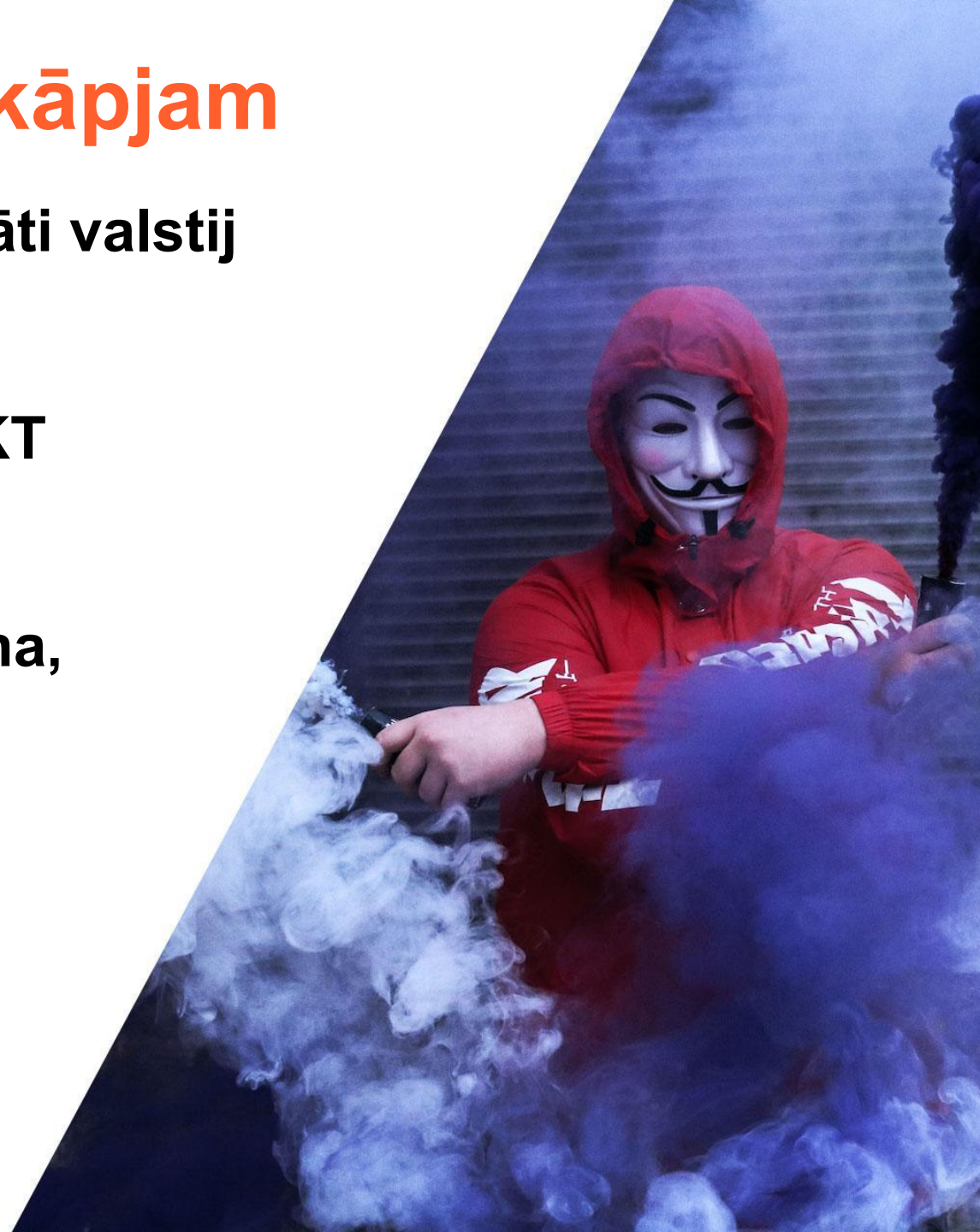
: www.port.brussels

: www.northseaport.com, www.brussels-charleroi-airport.com

Kļūdas, secinājumi un virzība uz nobriedušas kiberaizsardzības līmeni

Grābekļi, uz kuriem kāpjam

- Nepārdomāti centralizēti un izstrādāti valstij un sabiedrībai nozīmīgi IKT resursi
- Piegādes ķēžu drošība - privātais IKT pakalpojumu sektors sevi nesargā
- Atturīga mākoņpakalpojmu ieviešana, kur to varētu darīt
- Nepietiekama kompetence valsts pārvaldes iestādēs - jāiegulda personāla izaugsmē



Briedums un kibernoturība

- Spējam ātri pielāgoties un mobilizēties
- Strādājam nelielās, taču efektīvās komandās
- Mēs pazīstam viens otru
- Mēs uzticamies un viens otram pierādām, ka varam uzticēties
- Mums ir Kiberaizsardzības vienība Zemessardzē un mobilizēties spējīgas ekspertu grupas

Sadarbība ar tiesībsargājošām iestādēm

- Sadarbības līgumi un normatīvo aktu pamats
- Kopīgas veiksmīgas operācijas
- CERT.LV dalās ar informāciju par incidentu izmeklēšanas rezultātiem
- Kopīgs darbs pie Latvijā identificētu kaitīgu resursu izpētes un to neitralizēšanas

Valsts soļi brieduma veicināšanā

- Pieņemta jaunā Kiberdrošības stratēģija (2023-2026)
- Kiberdrošības likums (ITDL vietā)
- Nacionālā Kiberdrošības centra veidošana
- MK442 pārstrāde
- Uzraudzības sistēmas izveide

Mēs esam “tā” noturība!

- **Mikrotik**
- **ziedot.lv**
- **Edge Autonomy**
- un daudzi citi, kurus varam saukt par Latvijas *“Nokia”*

Latvija vada kiberoperācijas pasaules ekspertu līmenī

Visu izšķir attieksme!

20 000 galaiekārtu infrastruktūra pilnā gatavībā 2 - 4 stundu laikā

VS

3 500 galaiekārtu infrastruktūra pilnā gatavībā 2 mēnešu laikā

Vairāk kā 50 000 sistēmas

Latvija vada kiberoperācijas pasaules ekspertu līmenī

CERT @certlv · Feb 28

For more than a year CERT.LV is leading a threat hunt operation in close collaboration with the highly professional colleagues from US @US_CYBERCOM and CAN @CanadianForces @cybercentre_ca to strengthen the cyber resilience of critical infrastructure & ICT services

> **U.S. Embassy Riga** @USEmbassyRiga · Feb 28
>
> Ambassador Robinson welcomed Maj. Gen. William Hartman, Commander of the Cyber National Mission Force of @US_CYBERCOM, to the Embassy today. 🇺🇸 works closely with 🇱🇻#Latvia and other Allies to strengthen capabilities and counter threats in cyberspace. #StrongerTogether

CERT @certlv · Mar 2

Jūtamies pagodināti par iespēju dalīties ar Kosovas kolēģiem Latvijas pieredzē par nacionālās kiberdrošības pilnveidošanu.

We are honored to have this opportunity to share Latvia's experience on improving national cyber security with our Kosovo colleagues.

> **Sense** @Sense_CRC · Mar 1
>
> Day one of the workshop was focused on sharing good practices for national cybersecurity coordination, and we had the privilege of learning from the experiences of Latvia. We thank @bkaskina from @certlv and Elina Viksne for the great presentations. twitter.com/sense_crc/stat...

Canada in Latvia @CanadaLatvia · Mar 8

Cyber experts from the @CanadianForces @cybercentre_ca are proud to work closely with their exceptional Latvian counterparts @certlv to counter threats and enhance capabilities. Cooperation makes both our countries more secure. #StrongerTogether

> **CERT** @certlv · Feb 28
>
> For more than a year CERT.LV is leading a threat hunt operation in close collaboration with the highly professional colleagues from US @US_CYBERCOM and CAN @CanadianForces @cybercentre_ca to strengthen the cyber resilience of critical infrastructure & ICT services

Kā pasargāties?

- Agrās brīdināšanas sensoru tīkls
- DNS ugunsmūris (dnsmuris.lv)
- CERT.LV SOC (draudu telemetrija)
- CERT.LV draudu medības
- CERT.LV ielaušanās testi / audits
- CERT.LV darbinieku izglītošnas semināri
- Kiberdrošības kopienas info apmaiņas platforma (mm.cert.lv)

CERT.LV

Paldies!

Varis Teivāns

https://www.cert.lv

certlv

certlv