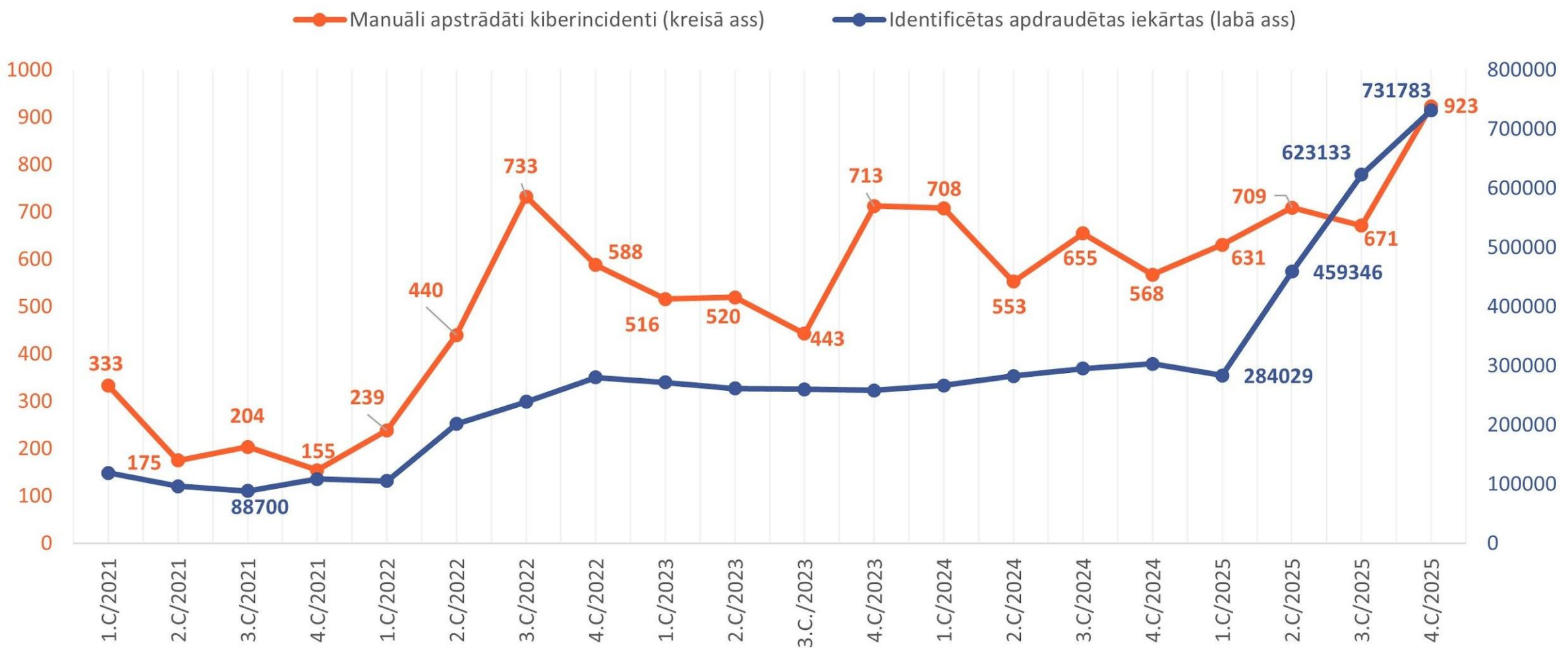
Situācija Latvijas kibertelpā un ko es varu darīt savā labā?

Baiba Kaškina

08.04.2026

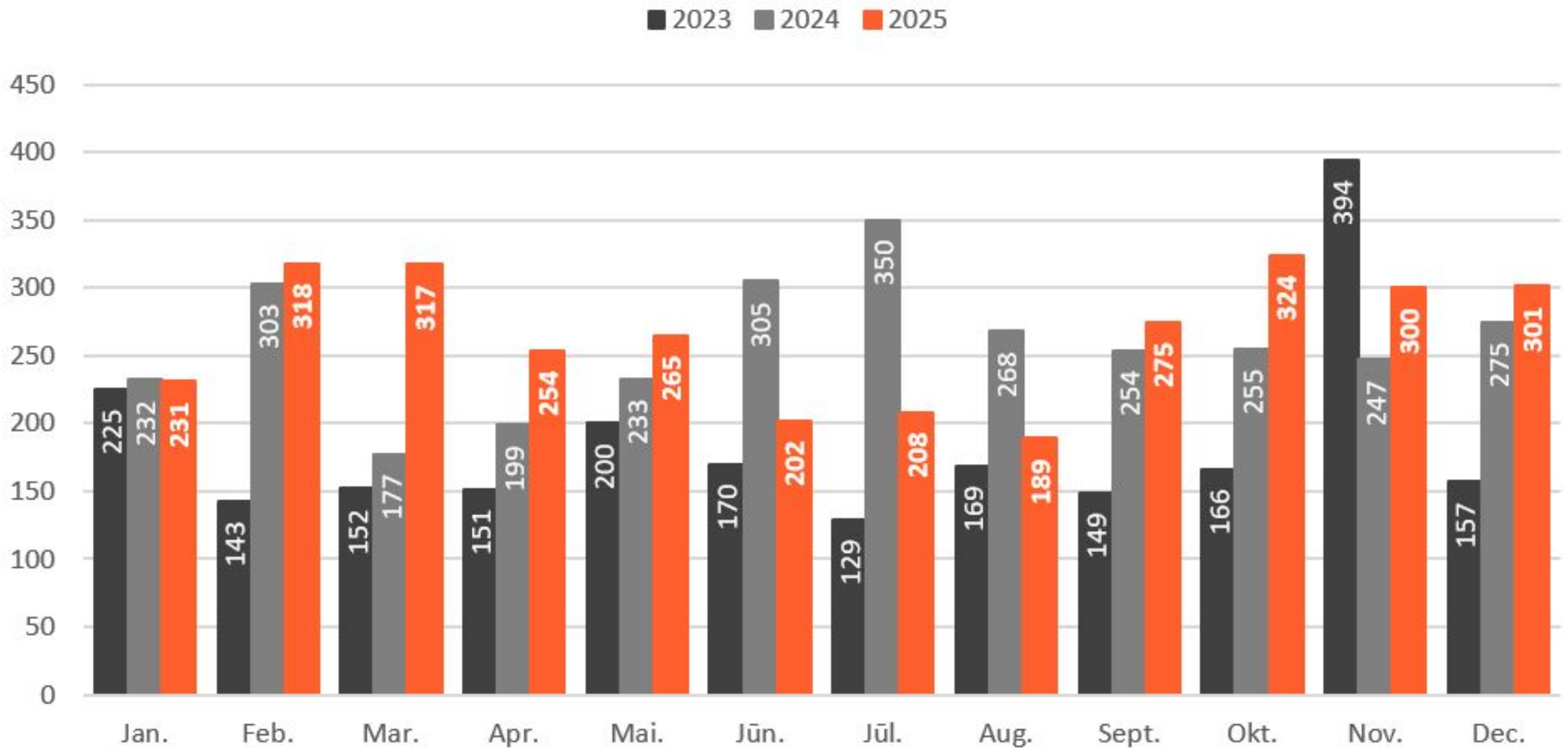
CERT.LV
Kiberincidentu novēršanas institūcija

Digitālā apdraudējumu realitāte Latvijā



Kiberincidentu dinamika

(skaits mēnešu dalījumā)



Patvertņu izveidei un aprīkošanai novirzīs 22 miljonus eiro ES fondu naudas

Dalīties:

Patvertne Kuldīgā, Rātskunga ielā 2 Inga Ozola / Latvijas Radio

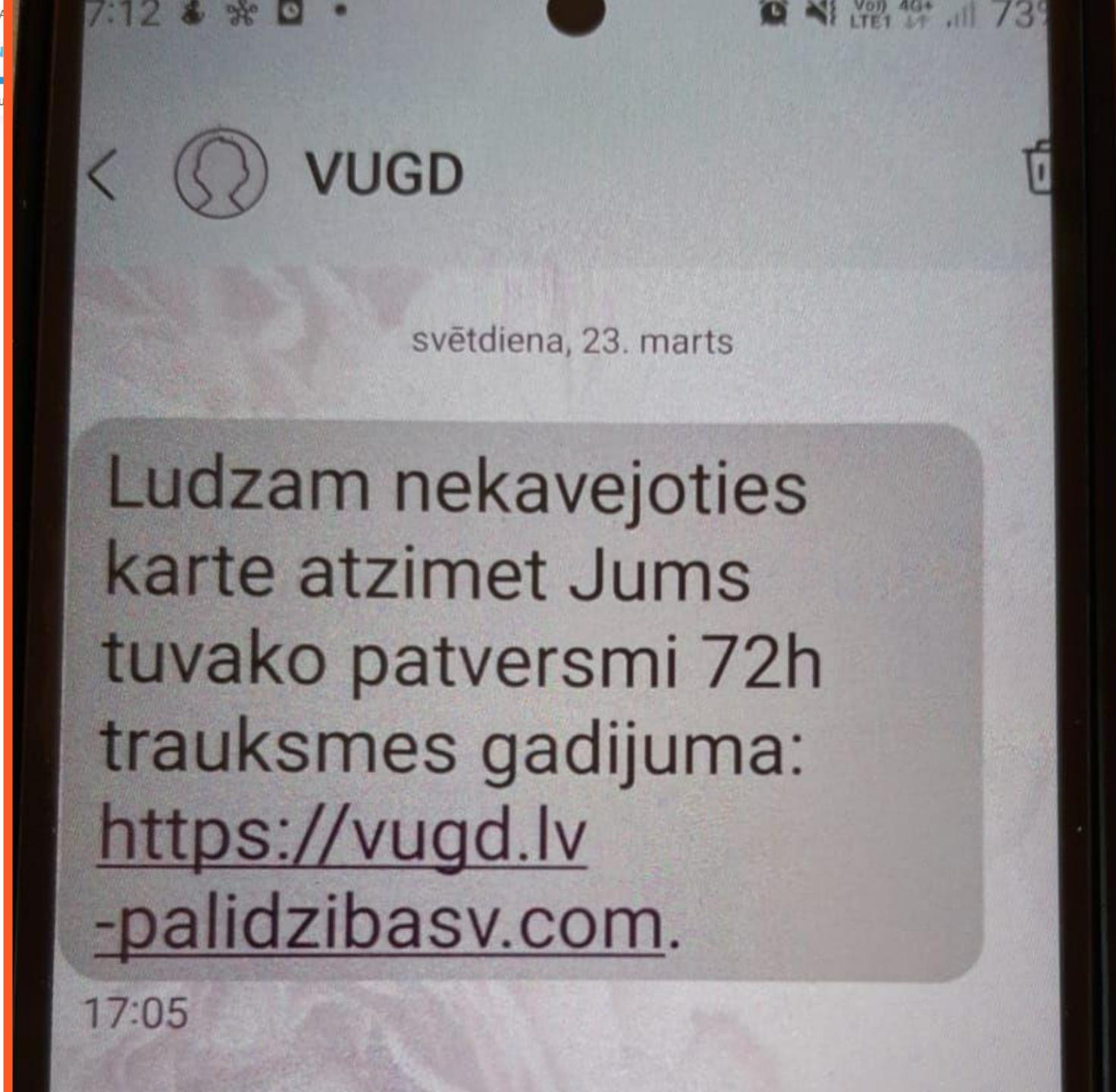
19. februāris, 9:14 | Latvijā | **Autori:** LSM.lv Ziņu redakcija

Lai Latvijā straujāk virzītos uz priekšu ar patvertņu izveidošanu un pielāgošanu, Eiropas Savienības Fondu tematiskā komiteja vienojusies šim nolūkam novirzīt 22 miljonus eiro no Eiropas reģionālās attīstības (ERAF) fonda. Trešdien pašvaldībām izvērtēšanai nosūtīts priekšlikums par iespējamo finansējuma sadali.

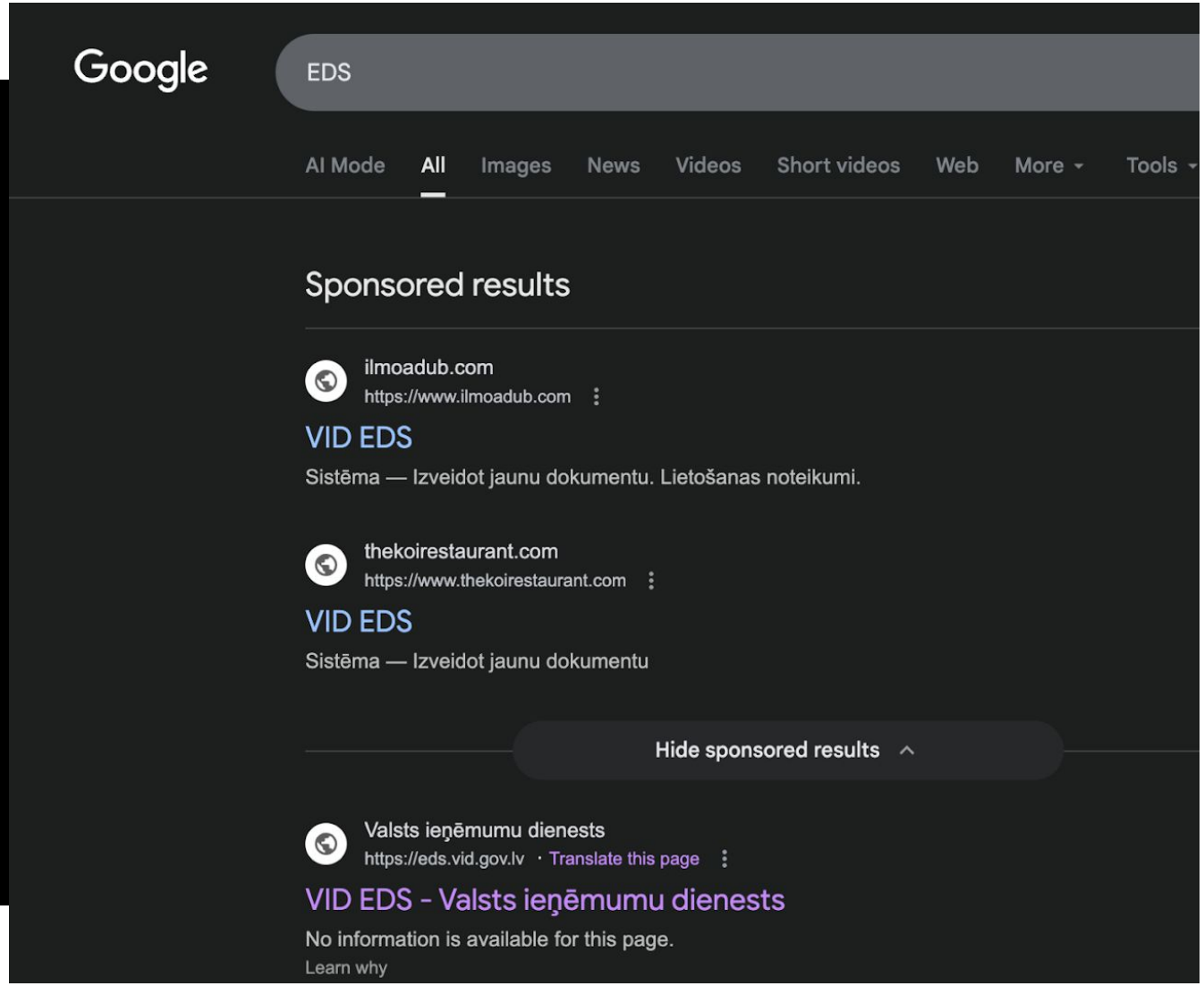
Iecerēts, ka esošais piedāvājums ļaus atbilstoši III kategorijas patvertnei pielāgot un aprīkot vismaz 500 valsts un pašvaldības īpašumā esošus objektus.

Valsts plāno regulējumu patvertņu izveidošanai, pielāgošanai un izmantošanai
11. februāris, 14:51

Lai par Eiropas finansējumu nodrošinātu patvertnes iespējami lielākam cilvēku skaitam, Valsts ugunsdzēsības un glābšanas dienests (VUGD) veicis patvertņu kategorizēšanu, izmantojot vairākus kritērijus, tostarp iedzīvotāju blīvumu apdzīvotajā vietā, patvertnes atrašanās vietu pašvaldībā.




VID-Dekl
Text Message • SMS
šodien, 18:48
2025 gada nodoklu lidzekli ir aprekinati un gaida apsitrinajumu to atpirksanai, parskatiet seit https://dekl.vdslstema.info


Google
EDS
AI Mode
All
Images
News
Videos
Short videos
Web
More
Tools
Sponsored results
ilmoadub.com
https://www.ilmoadub.com
VID EDS
Sistēma — Izveidot jaunu dokumentu. Lietošanas noteikumi.
thekoirestaurant.com
https://www.thekoirestaurant.com
VID EDS
Sistēma — Izveidot jaunu dokumentu
Hide sponsored results
Valsts ieņēmumu dienests
https://eds.vid.gov.lv · Translate this page
VID EDS - Valsts ieņēmumu dienests
No information is available for this page.
Learn why

Uzbrucēji

Krievijas un Ķīnas TR izcelsmes grupējumu aktivitāte joprojām augsta

KRIEVIJA:

- **Cadet Blizzard**
- **DEV-0586**
- **Gamaredon**
- **Turla, APT28**
- **GreyScale**
- **GhostWriter**

ĶĪNA:

- **Volt Typhoon**
- **Mustang Panda**
- **Sparrow Door**
- **Linen Typhoon**
- **Violet Typhoon**
- **Storm-2603**

Mērķi: kritiskā infrastruktūra un OT sistēmas (enerģētika, ūdens, siltums)

Atbildes reakcija: DDoS uzbrukumi no NoName057(16) u.c.

APT28 Targeted European Entities Using Webhook-Based Macro Malware

Ravie Lakshmanan Feb 23, 2026

Malware / Threat Intelligence

The Russia-linked state-sponsored threat actor tracked as APT28 has been attributed to a new campaign targeting specific entities in Western and Central Europe.

The activity, per S2 Grupo's LAB52 threat intelligence team, was active between September 2025 and January 2026. It has been codenamed **Operation MacroMaze**. "The campaign relies on basic tooling and the exploitation of legitimate services for infrastructure and data exfiltration," the cybersecurity company said.

The attack chains employ spear-phishing emails as a starting point to distribute lure documents that contain a common structural element within their XML, a field named "INCLUDEPICTURE" that points to a webhook[.]site URL that hosts a JPG image. This, in turn, causes the image file to be fetched from the remote server when the document is opened.

Put differently, this mechanism acts as a beacon akin to a tracking pixel that triggers an outbound HTTP request to the webhook[.]site URL upon opening the document. The server operator can log metadata associated with the request, confirming that the document was indeed opened by the recipient.

Trending News


Anthropic Finds 22 Firefox Vulnerabilities Using Claude Opus 4.6 AI Model


ThreatsDay Bulletin: DDR5 Bot Scalping, Samsung TV Tracking, Reddit Privacy Fine and More


Cisco Confirms Active Exploitation of Two Catalyst SD-WAN Manager Vulnerabilities


ClawJacked Flaw Lets Malicious Sites Hijack Local OpenClaw AI Agents via

Massive cyberattack on Polish power system in December failed, minister says

By **Reuters**

January 13, 2026 1:06 PM GMT+2 · Updated January 13, 2026

Newly appointed Polish Minister of Energy, Milosz Motyka attends a government reshuffle announcement in Warsaw, Poland, July 23, 2025. REUTERS/Kuba Stezycki Purchase Licensing Rights

WARSAW, Jan 13 (Reuters) - Poland's power system faced its largest cyberattack in years in the last week of December that also followed a different pattern, the country's energy minister said on Tuesday.

IMAGE: EUGENE CHYSTIAKOV VIA UNSPLASH

Alexander Martin

January 14th, 2026

Cybercrime News News Briefs

Cyberattack forces Belgian hospital to transfer critical care patients

A reported ransomware attack on AZ Monica hospital in Belgium has led to operations being canceled and forced the Red Cross to transfer seven patients requiring critical care to other hospitals.

In a statement on Tuesday, AZ Monica confirmed experiencing "a serious disruption" to its IT systems. To halt the attack, it said it proactively shut down all servers for its campuses in Deurne and Antwerp, causing massive disruption to care.

The hospital credited the Red Cross with assisting the transfer of critical patients to other hospitals, as their status was unstable and their safety could not be guaranteed. Other patients "remain safely in the hospital and are receiving the necessary care."

"Due to this situation, no scheduled surgeries are possible today. We have informed all patients. The Emergency Department is operating at reduced capacity," the hospital warned.

CERT.LV

Tendences & Taktikas


#1 KRĀPNIECĪBA

KRĀPŠANAS GADĪJUMU STATISTIKA ČETRĀS LIELĀKAJĀS BANKĀS

(01.01.2025.–31.12.2025.)

FINANŠU NOZARES ASOCIĀCIJA

14 031 342 €

Novērsto krāpšanas gadījumu apmērs

12 219 719 €

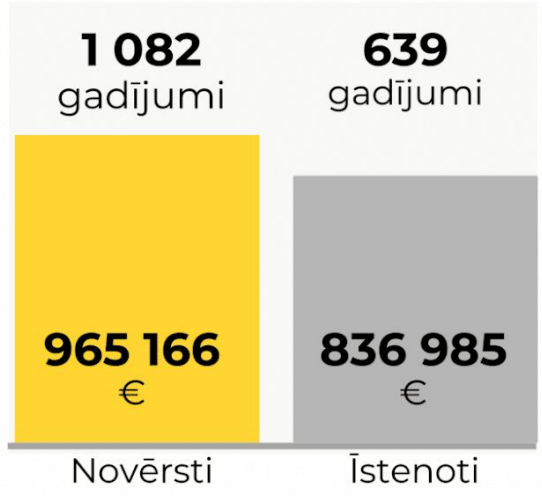
Izkrāpto līdzekļu apmērs banku klientiem, pašiem apstiprinot maksājumu

TELEFONKRĀPŠANAS

(iekļauti visi trešo pušu veiktie neautorizētie maksājumi)

INVESTĪCIJU KRĀPŠANAS

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



CITA VEIDA KRĀPŠANAS

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

Cilvēki pārdod īpašumus un atdod dārglietas – krāpnieku guvums sasniedz 23 miljonus

23,7 miljoni eiro – tik daudz 2025. gadā krāpnieki izkrāpa Latvijas iedzīvotājiem, kas ir būtisks pieaugums salīdzinot ar 2024. gadu, kad zaudējumi bija 16 miljoni eiro, portāls "tv3.lv" uzzināja Valsts policijā.

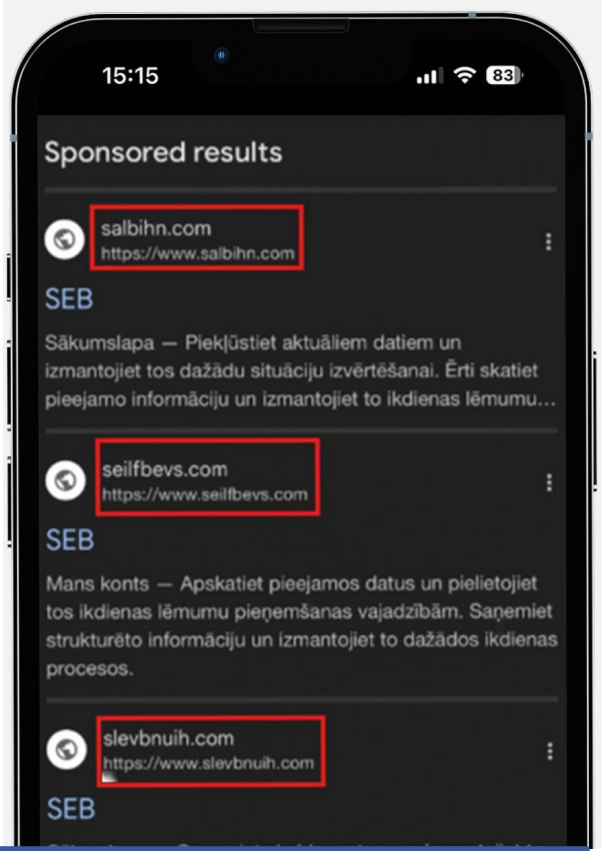
3

FOTO: SEBASTIAN KAHNERT, DPA/PICTURE-ALLIANCE

Jaunākais

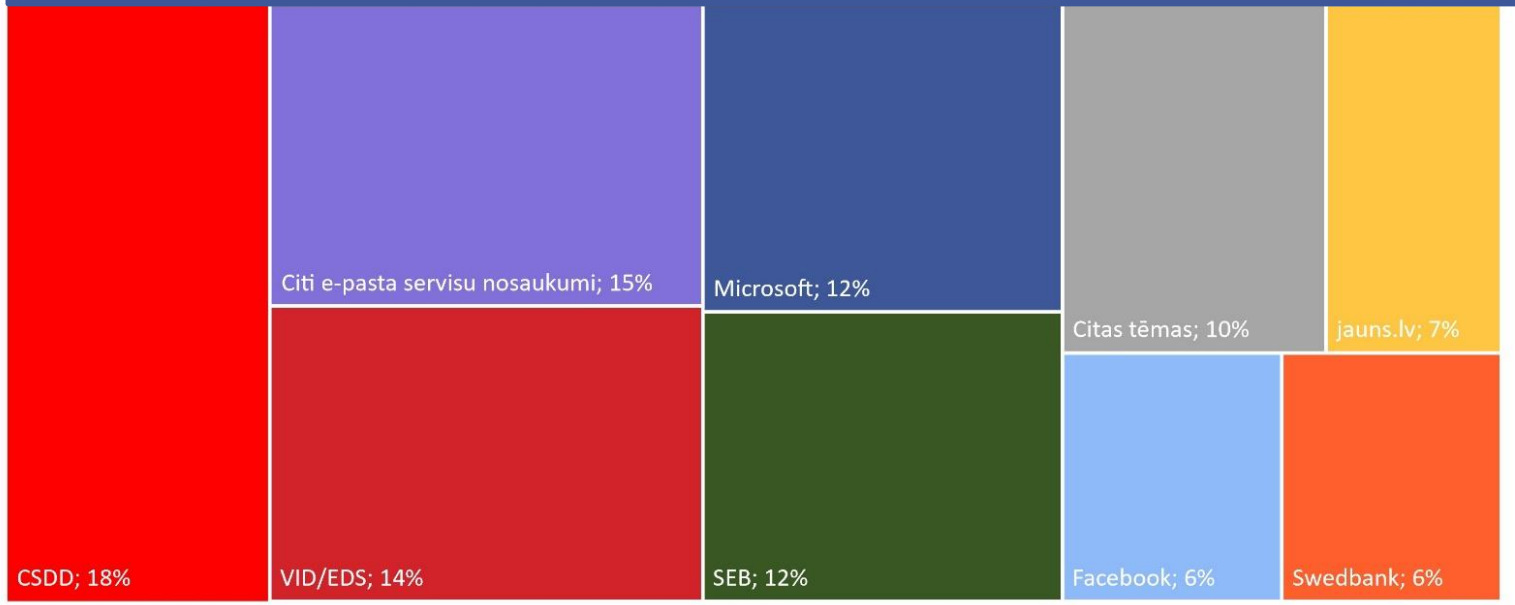
11:36 TENISS Kā pēdējās "Australian Open" pusfinālu sasniedz...
11:26 ĀRVALSTĪS Pētījums: kopējais karā Ukrainā kritušo un...
11:11 AIZJŪRU SLAVENĪBAS Aktrises Denīzes Ričardsas bijušais vīr...
11:10 HOKEJS Balcers un Veckaktiņš asistē savu komandu vārtu...
11:05 ĀRVALSTĪS Putins izvairās no mobilizācijas, bet karavīru...
11:04 VESELĪBA Mazā rokasgrāmata rūpēm par ādu sala laikā
11:00 NHL Dalīna nakts Toronto – pirmais "hat trick," divas...
10:58 ĀR K
10:43 SA br
10:27 AU m
10:25 SI ie
10:07 NH N
10:01 SA pa

Veiksmīgi piekoptās taktikas:



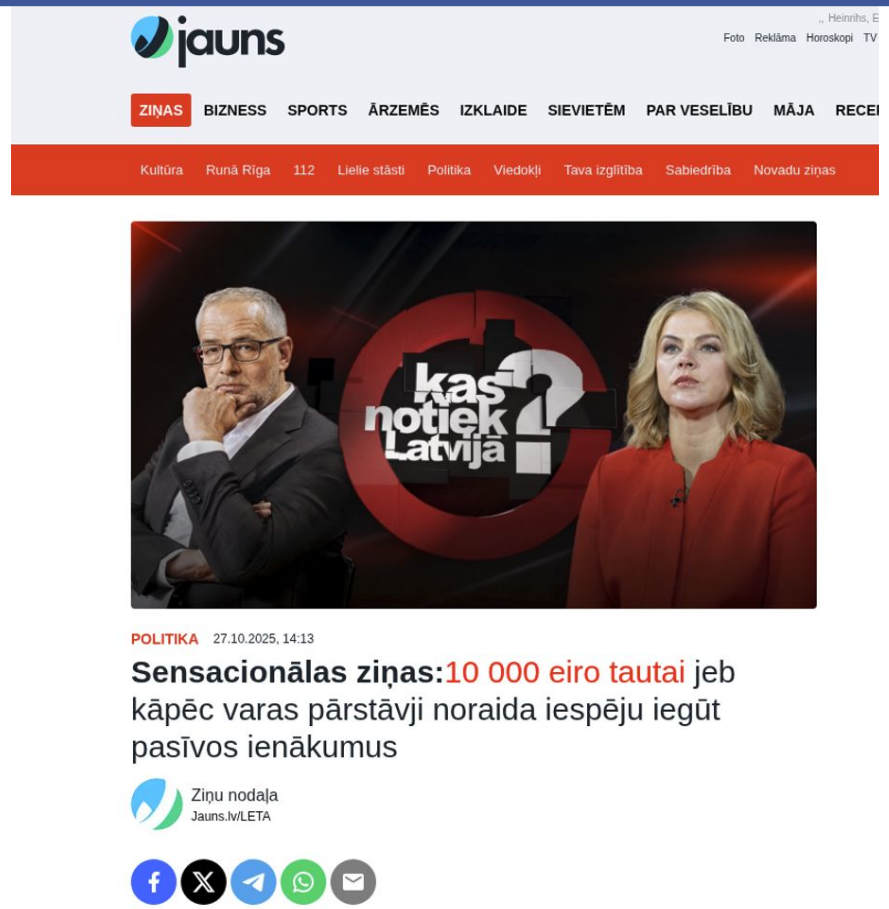
Zīmolu imitējošas krāpnieciskas Google reklāmas

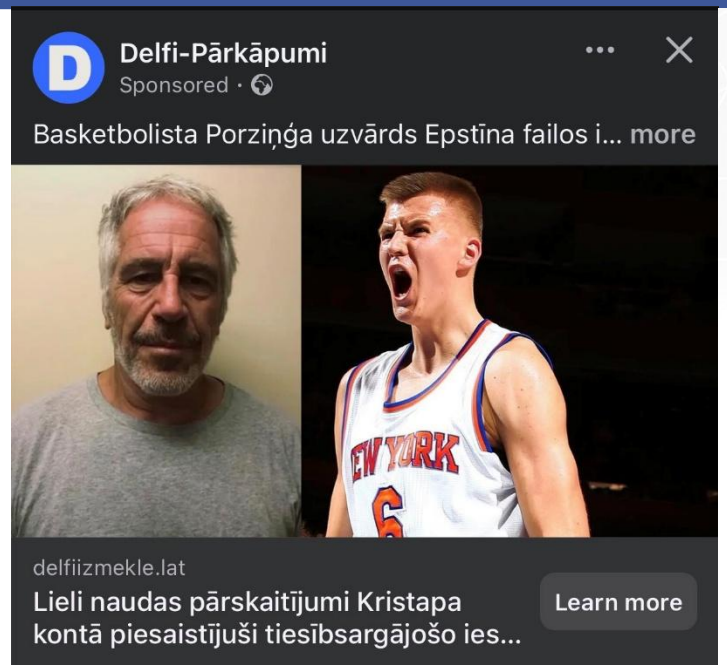
Krāpniecības kampaņas zināmu valsts un komerciestāžu vārdā



Veiksmīgi piekoptās taktikas:

Viltus investīciju piedāvājumi ar “ziņu portālu” masku (*delfi.lv, jauns.lv, grani.lv, TV3, u.c.*)

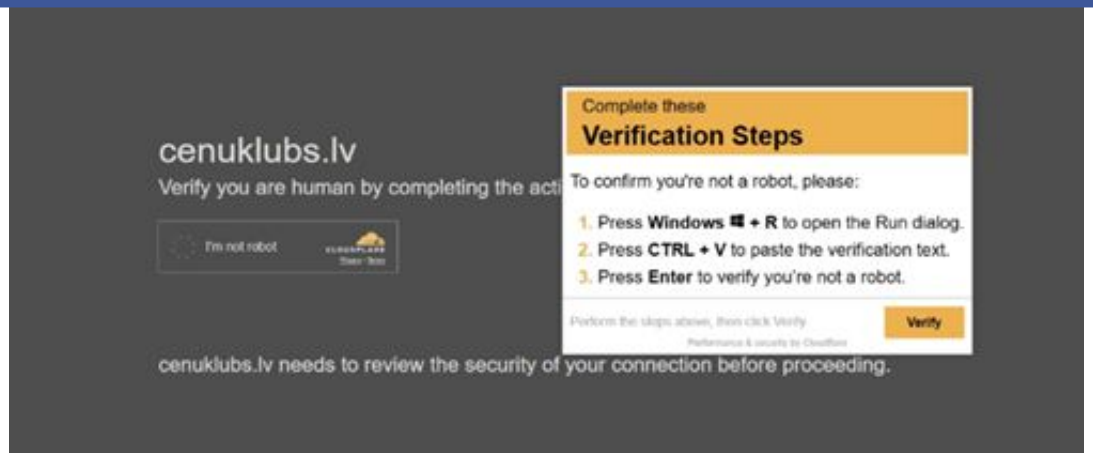


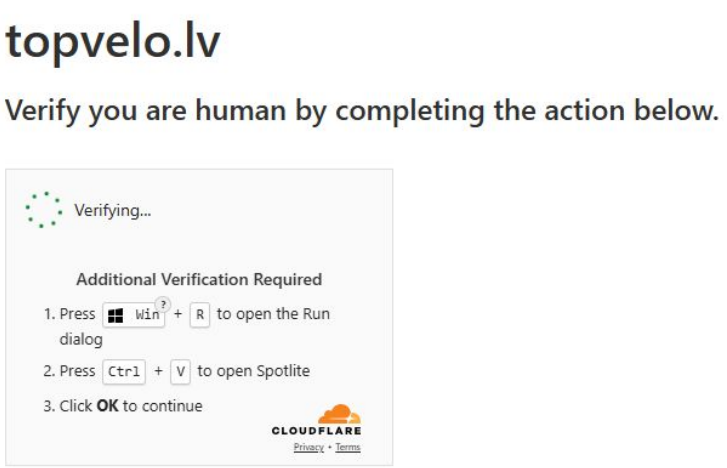


#2 IEVAINOJAMĪBAS & ĻAUNATŪRAS

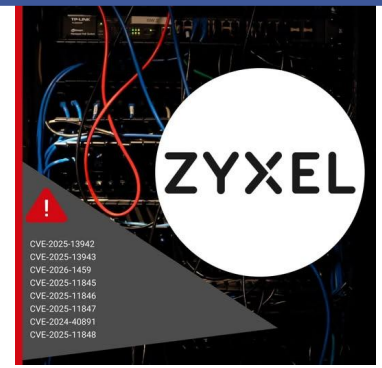
Veiksmīgi piekoptās taktikas:

ClickFix un infostealer uzbrukumu eskalācija





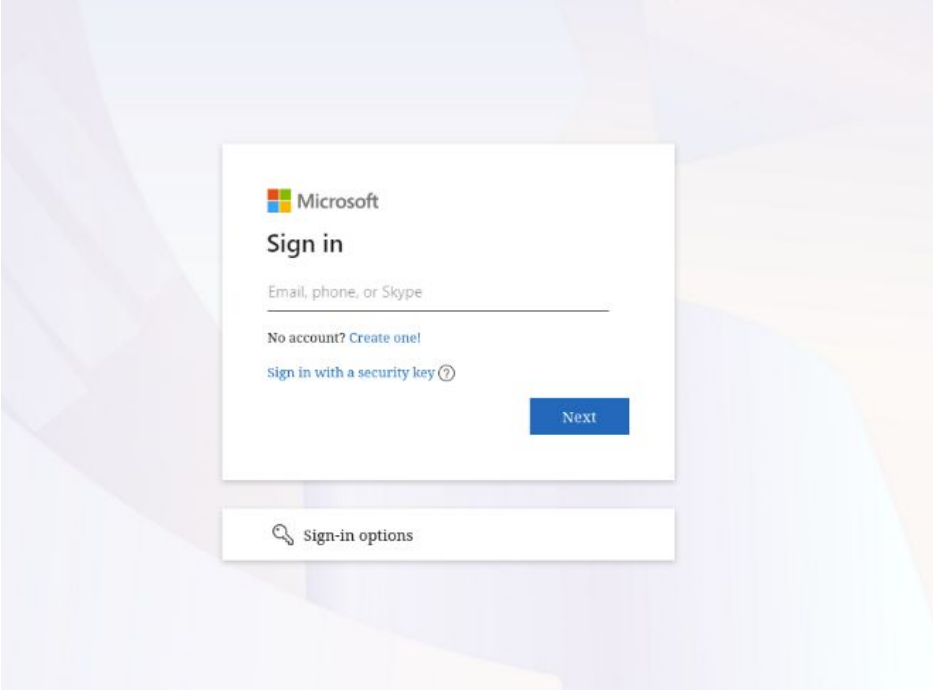
Aktīvi izmantotas kritiskas ievainojamības



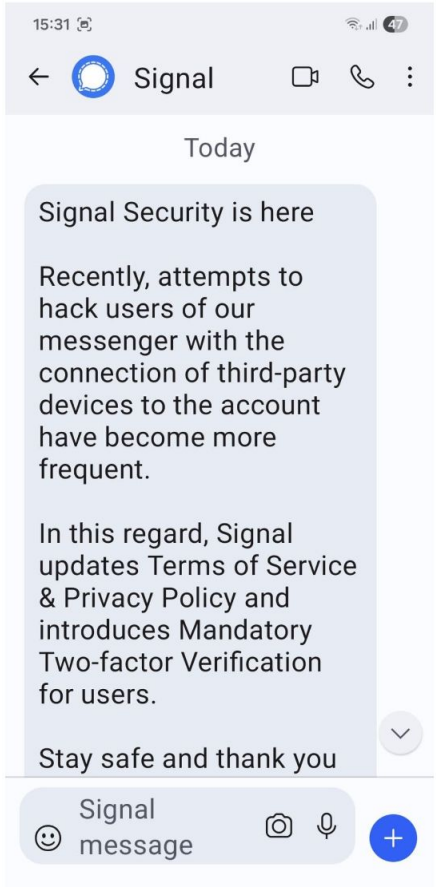
#3 PIEKĻUVES PĀRŅEMŠANA & DATU IZMANTOŠANA

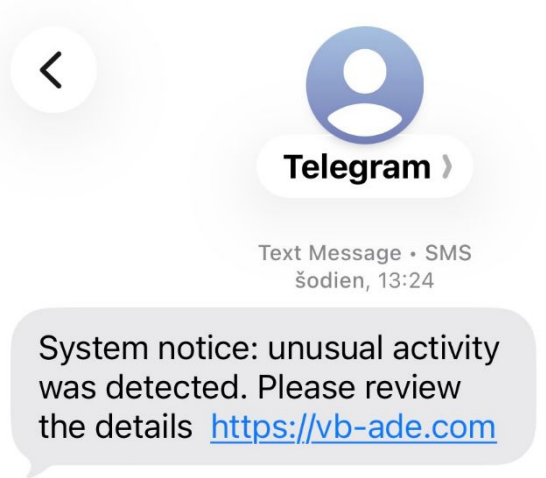
Veiksmīgi piekoptās taktikas:

Microsoft un Amazon kontu pārņemšana



Saziņas kanālu pārņemšana





Izspiedējvīrusu pieaugošā izplatība

Secinājumi

- Uzbrukumi kļūst **hibrīdi**: tie vienlaikus izmanto gan tehnoloģiskas, gan cilvēkfaktora ievainojamības;
- Noturība jāveido **daudzslāņaina:** tehnoloģiskā, operacionālā, organizatoriskā un cilvēkfaktora līmenī;
- **Ātrums** ir kritisks faktors: gan uzbrucēju reakcijā, gan aizsardzības pusē.

Ko es varu darīt savās organizācijas labā?

1. **Apzināt** un **uzraudzīt** savu infrastruktūru (SOC, monitorings)
2. **Gatavoties** krīzes situācijām un piedalīties mācībās
3. **Izglītot** darbiniekus
   - Vispārīgā izglītošana
   - Pikšķerēšanas simulācijas
   - Spēles

Darbības nepārtrauktības izaicinājums

Mērķis:
Praktiskā veidā drošā vidē pārbaudīt, cik gatava ir iestāde reaģēt uz kiberincidentiem un ar tiem saistītām krīzes situācijām.

Pieteikšanās: rakstot uz events@cert.lv
norādot iestādes nosaukumu, kontaktpersonu, dalībnieku skaitu un vēlamo laiku!

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

Jautājumi?

cert@cert.lv

https://www.cert.lv