]{iberuzbrukumu @izkulise$

Dana Ludviga

11.09.2025

CERT.LV
Kiberincidentu novēršanas institūcija

Uzbrucēju tipi:

Uzbrucēju tipi

<!-- Latvijā aktīvākā daļa -->

- **Valsts sponsorēti aktieri** *(APT - Advanced Persistent Threat)*
- **Finansiāli motivēti grupējumi**
  - **BEC grupējumi**
  - **Izspiedējvīrusu bandas**
  - **Piekļuves nodrošinātāji** *(IAB - Inital Access Brokers)*
- **Haktīvisti**

- Kiberhuligāni *(Script kiddies)*
- Iekšējais drauds
- Un citi

Valsts sponsorēti draudu aktieri

(APT - Advanced Persistent Threats)

Raksturojums: Labi organizētas un profesionālas grupas, kas darbojas kādas valsts interesēs. Darbs ir ilgtermiņa, precīzi mērķēts, slepens. Izmanto kompleksus uzbrukumus, bieži apvienojot spiegošanu, sabotāžu un izlūkošanu.

Motivācija: Politiska, militāra, izlūkošanas interese. Retāk finansiāla motivācija.

Tipiska uzvedība: Ilgstoša mērķa monitorēšana. Atslēgvārds slepenība, izmanto *"dzīvo zem radara"* paņēmienus. Kompleksi rīki un progresīvas taktikas, taču mērķis nav uzreiz radīt haosu, bet iegūt informāciju kuru tālāk var izmantot saviem stratēģiskiem mērķiem. Īstajā mirklī aktivizējas un rīkojas destruktīvi.

Piemēri:

Cadet Blizzard / DEV-0586: saistīta ar Krievijas izlūkdienestiem, mērķē uz valsts iestādēm Eiropā, taču pēdējā laikā novērojama interese arī par privāto sektoru tehnoloģiju izstrādes un tehnoloģiju apkalpošanas jomā.

Volt Typhoon un **Mustang Panda**: Atšķirībā no Krievijas APT šiem ir lielāks fokuss uz militāro un ārlietu nozari, kā arī mērķiem, kuru nosaukumā ir atslēgvārdi: **akadēmija, institūts, universitāte, augstskola, laboratorija.** Taču mērķē arī uz tīkla iekārtām (arī mājsaimniecībās).

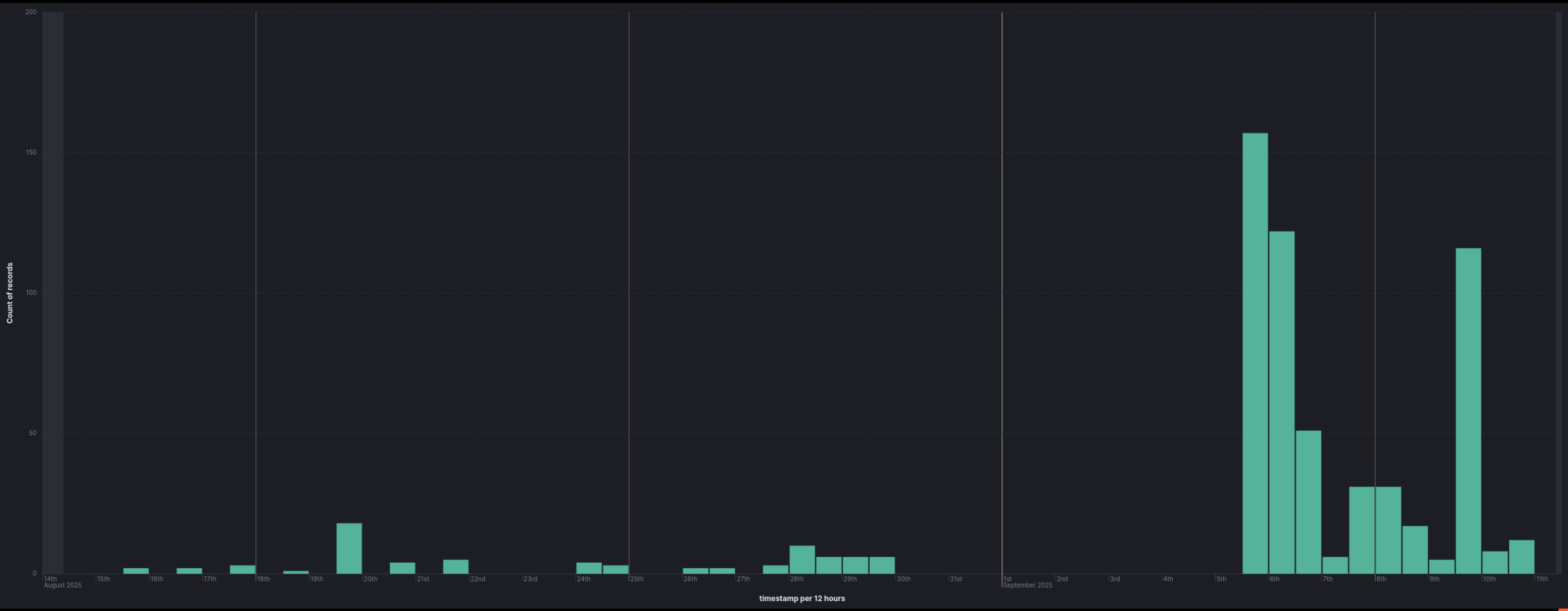
Finansiāli motivētie krāpnieki

Raksturojums: Organizētas draudu aktieru grupas no visas pasaules, kuru galvenais mērķis ir ātri iegūt un “atmazgāt” naudu. Viņus **parasti** neinteresē politika vai ideoloģija, viņi darbojas kā nelieli “IT uzņēmumi” ar sadalītām lomām: izstrādātāji, infrastruktūras uzturētāji, naudas “atmazgātāji” un starpnieki.

Motivācija: Naudas iegūšana pēc iespējas ātrāk un ar minimālu risku.

Tipiska uzvedība: Parasti uzbrūk uzņēmumiem, bankām, e-komercijas platformām vai privātpersonām. Izmanto dažādas metodes no izspiedējvīrusiem, pikšķerēšanas līdz pat BEC, investīciju krāpniecība, u.tml.

Dnsugunsmūris statistika:



Apakštips: BEC grupējumi

BEC - Business email compromise

Raksturojums: Tehniski ne tik advancēti grupējumi taču ar stiprām sociālās inženierijas, OSINT un naudas “atmazgāšanas” prasmēm. Interesē tikai biznesa sarakste. Nemēģina lauzties tālāk, jo nav nepieciešamības.

Motivācija: Finansiāla

Tipiska uzvedība: Uzmanīgi lasas citreiz arī filtrē un pārsūta sev interesējošo sarakstes daļu. Krāpniecība ir ilgtermiņa, pacietīgi seko sarakstei un iejaucas tikai īstajā brīdī.

Apakštips: Izspiedējvīrusu bandas

(Ransomware groups)

Raksturojums: Organizētas, tehniski prasmīgas grupas, kas veic datu šifrēšanu un izspiešanu par naudu. Darbojas kā biznesa vienība ar dažādām lomām.

Motivācija: Finansiāla

Tipiskā uzvedība: Šifrē datus uzņēmumos vai iestādēs. Pieprasa izpirkumu (kriptovalūtu). Nereti veic “double extortion”. Atsevišķām bandām ir savi ētikas kodeksi. Labprāt maksā par piekļuves informācijas izpaušanu sava mērķa darbiniekiem (iekšējais drauds).

CERT.LV

TVNET > Financenet > Nozares

Kiberuzbrukumā noplūduši alkohola ražotāja "Amber Beverage Group" dati

Foto: Schutterstock.com

Alkoholisko dzērienu ražotājs "Amber Beverage Group" piedzīvojis šifrējošā izspiedējvīrusa uzbrukumu, kas rezultējies uzņēmuma datu noplūdē, apstiprināja informācijas tehnoloģiju drošības incidentu novēršanas institūcijas "Cert.lv" pārstāvji.

TVNET > Bizness > TechBiz > Internets

"Jelgavas tipogrāfija" cietusi kiberuzbrukumā

TVNET / LETA

2025. gada 4. jūnijs 14:14

Noklausies

Jelgavas tipogrāfija FOTO: PAULA ČURKSTE / LETA

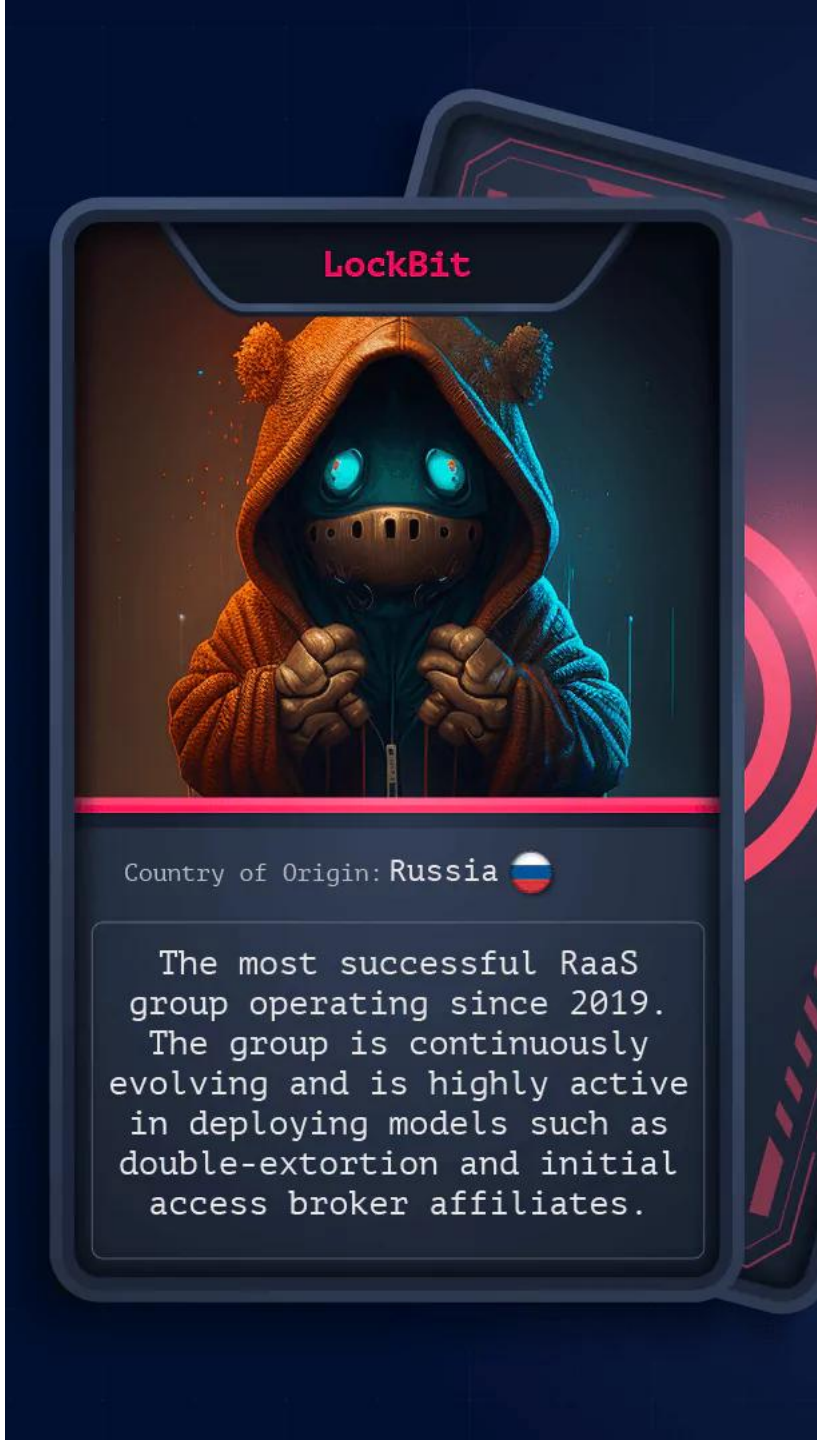
SIA "Jelgavas tipogrāfija" šonedēļ ir cietusi no kiberuzbrukuma, aģentūrai LETA pastāstīja uzņēmuma valdes priekšsēdētājs Māris Matrevics.

Piemērs

LockBit - “digitālais izspiedējs” no Krievijas, kas mērķē uz uzņēmumiem visā Eiropā, tajā skaitā Latviju, izpilda “double extortion” stratēģiju.

Aktīvi piekopj RaaS *(Ransomware-as-a-Service)* darbības modeli:

- LockBit operatori izstrādā un uztur vīrusu, infrastruktūru, platformu, DLS *(Dedicated leak sites)*.
- Partneri (*affiliates*) veic uzbrukumus dažādās valstīs, operatoriem maksājot procentus no izpirkuma.



Apakštips: Piekļuves nodrošinātāji

IAB - Initial Access Broker

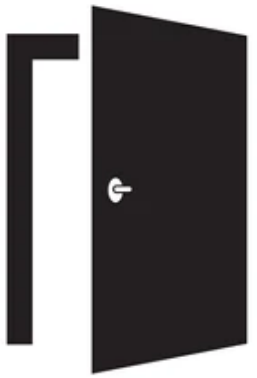
Raksturojums: Profesionāla uzbrucēju grupa, kuru galvenais "produkts" ir piekļuve uzņēmumu un organizāciju sistēmām. Viņi darbojas kā starpnieki, ielaužas infrastruktūrā un pārdod šo piekļuvi citiem uzbrucējiem - izspiedējvīrusu grupām, APT, u.tml.

Motivācija: Finansiāla, peļņa no kompromitētas piekļuves pārdošanas

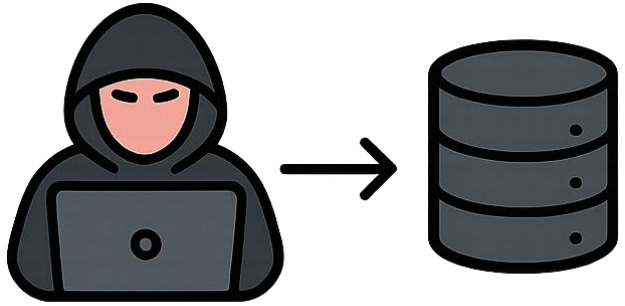
Tipiska uzvedība: Izmanto ievainojamību ekspluatāciju, *bruteforce*, pikšķerēšanu un ļaunatūru, u.tml. Nereti iegūst administratora tiesības, izveido *backdoor* vai kontus turpmākai izmantošanai. Publicē piedāvājumus *DarkNet* forumos vai pārdod to privāti.

Piemērs (rīki)

Raspberry Robin - Rīks tārps (worm) kas parasti tiek izpaltīts ar USB un ārējo disku, e-pasta pielikumu vai kompromitētu mājaslapu palīdzību. Kad tas inficē datoru tad izveido savienojumu ar C2 un izpilda norādes. Iegūtā piekļuve tiek pārdota *DarkNet.*



RedLineStealer - Finansiāli motivēts IAB operātors, kas specializējas infromācijas zādzībā (lietotājvārdi, paroles, pārlūkprogrammā saglabātie dati, kriptovalūtu maki, sistēmas informāciju, IP adreses, utt.)
Piedāvā MaaS *(Malware as a service)* pakalpojumu.
Ļaunatūra izplatās caur pikšķerēšanas e-pastiem, ļaunprātīgām lejupielādēm, pirātiskām programmām.



Haktīvisti
(Hacktivists)

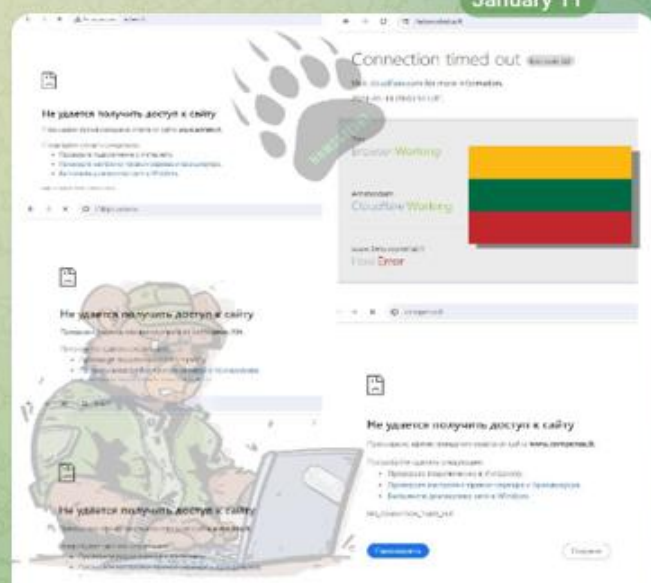
Raksturojums: Politiski vai ideoloģiski motivēti draudu aktieru grupējumi, kas vēlas sūtīt ziņu, protestēt vai atmaskot.

Motivācija: Ideoloģija, protesti pret valdību, uzņēmumiem vai institūcijām, cilvēktiesību jautājumi.

Uzvedība: Publiski demonstrē uzbrukumus - datu noplūdes, Ddos, mājaslapu *"defacement"*. Ir aktīvi sociālajos tīklos, vēlas publicitāti. Izmanto sabiedrības uzmanību, lai ietekmētu lēmumu pieņēmējus.
Ne vienmēr meklē finansiālu ieguvumu.
Pēdējā laikā manāma sadarbība ar APT.

Piemērs: KillNet un NoName057(16)

January 11



Президент Литвы Гитанас Науседа на пресс-конференции 10 января объявил новый пакет военной помощи Украине на сумму 200 млн евро, куда войдут, в том числе, боеприпасы, генераторы и бронемашины M577.

Напоминаем властям Литвы о необходимости заботиться о своих гражданах, а не спонсировании террористов Зеленского 😈

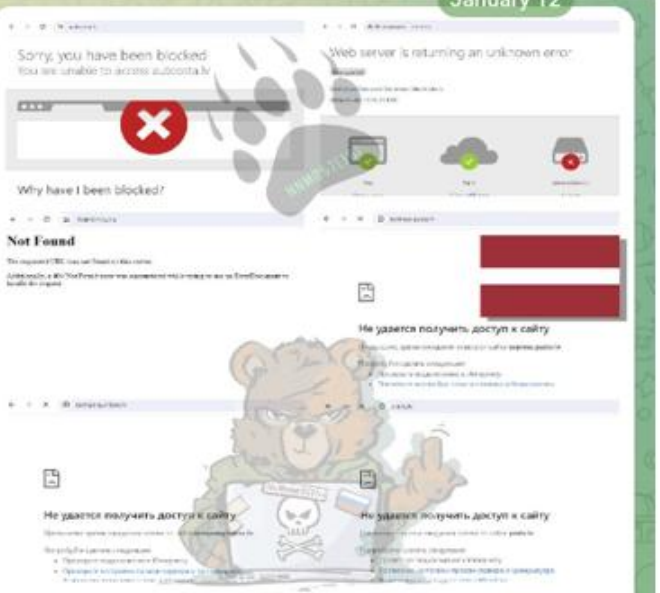
❌**Compensa страховая компания** check-host.net/check-report/148bf943k5b3

❌**If Insurance страховая компания** check-host.net/check-report/148bfb0ak311

❌**BTA Baltic Insurance Company страховая компания** (закрылись по гео) check-host.net/check-report/148bfc50k25d

❌**Литовские дороги** check-host.net/check-

January 12



Вы нас ждали? Мы пришли, русофобы из Латвии! И не с пустыми руками, а с DDoS-подарочками😈

❌**Рижский международный автовокзал** (закрылись по гео) check-host.net/check-report/149395bdk52a

❌**Сервис электронного документооборота и электронной подписи Латвии** check-host.net/check-report/149397e3k530

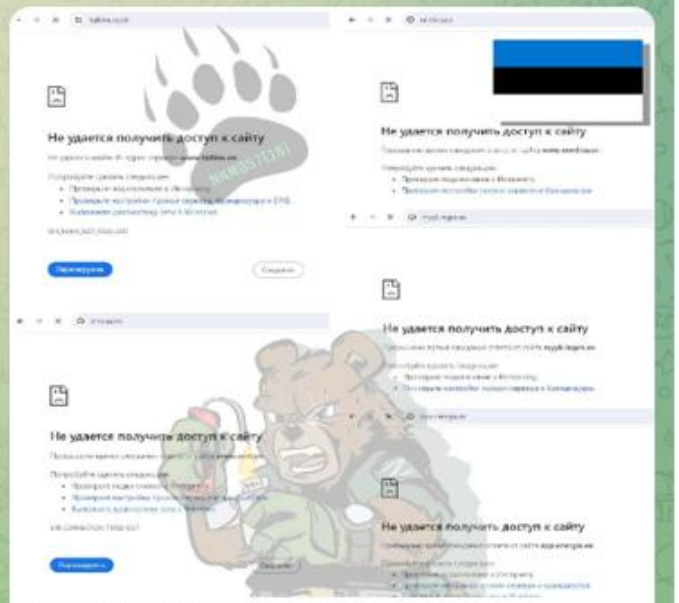
❌**Почта Латвии** check-host.net/check-report/1493987ck624

❌**Авторизация Почты Латвии** check-host.net/check-report/149399d9k553

❌**Inbox Company Латвия** check-host.net/check-report/14939ad0k9ca

❌**Латвийская торгово-промышленная палата** check-host.net/check-report/14939bbdk252

January 12



Эстония намерена в течение ближайших четырех лет оказывать Киеву военную помощь в размере 0,25% своего внутреннего валового продукта (ВВП). Об этом заявила премьер-министр Кая Каллас после очередного заседания Совета по государственной обороне, пишет ERR, а также до 2027 года предоставит Украине помощь на сумму 1,2 миллиарда евро.

В очередной раз смеем напомнить, что финансовая помощь украинским нацистам наказывается... DDoS-ракетами😈

❌**Национальная эстонская авиакомпания** check-host.net/check-report/149278abkdec

❌**Авторизация Eesti Energia Акционерное общество** check-host.net/check-report/14927af8kfde

❌**Авторизация Inges Kindlustus Страховое сообщество** check-host.net/check-report/14927c22k269

Kiberhuligāni
(*Script kiddies*)

Raksturojums: jauni, maz pieredzējuši uzbrucēji, nereti izmanto citu uzlaušanas rīkus, “lejupielādē gatavus skriptus vai malware” bez dziļas izpratnes. Melnajā tīmeklī spēlējas ar Phishing as a service, Ddos as a service un citām platformām.

Motivācija: vēlas izcelties, jautrība, piedzīvojuma meklējumi, garlaicības dēļ.

Tipiska uzvedība: Izmanto viegli pieejamus “hack tools”, AI palīdzību. Rīkojas nepārdomāti, bieži atstājot pēdas. Mērķis: vietējie serveri, spēļu konti, mazi uzņēmumi, u.c.

Iekšējais drauds

CyberChess

October 29-30, 2025

Riga, Latvia

CERT.LV
National Cybersecurity Centre of Latvia
Ministry of Defence Republic of Latvia
Institute of Mathematics and Computer Science University of Latvia
ISACA Latvia Chapter
Latvian Internet Association
ECCC European Cybersecurity Competence Centre
NCC-LV Latvia Cybersecurity Coordination Centre
Co-funded by the European Union
European Cyber Security Month
tet
eset Cybersecurity
Bitdefender
Recorded Future
CYBERCIRCLE
CLOUDFLARE
VMRAY
zscaler
Cisco Distributor
SILENT PUSH
paloalto Networks
lmt
squalio
Latvia State Radio and Television Center
Mattermost
ICANN
CLICO
ALSO The Technology Provider
Canada
MODAT
CYBER UNIT
DATORIKI
altacom
BLACK HILLS Information Security

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

CERT.LV

Liec mūri pret krāpnieku dūri!

@cert.lv