Nulles dienas ievainojamības un to ietekme uz perimetra iekārtu drošību

Gints Mālkalnietis

09.12.2025

CERT.LV
Kiberincidentu novēršanas institūcija

Ko uzbrucēji vēlas iegūt?

Draudu dalībnieka (TA) motīvs:

- **Nauda** (Kibernoziedzība)
- **Sensitīva informācija un dati** (Kiberizspiegošana)
- **Popularitāte** (Haktīvisms)
- **Iekšējās propagandas veicināšana** (Dezinformācija)

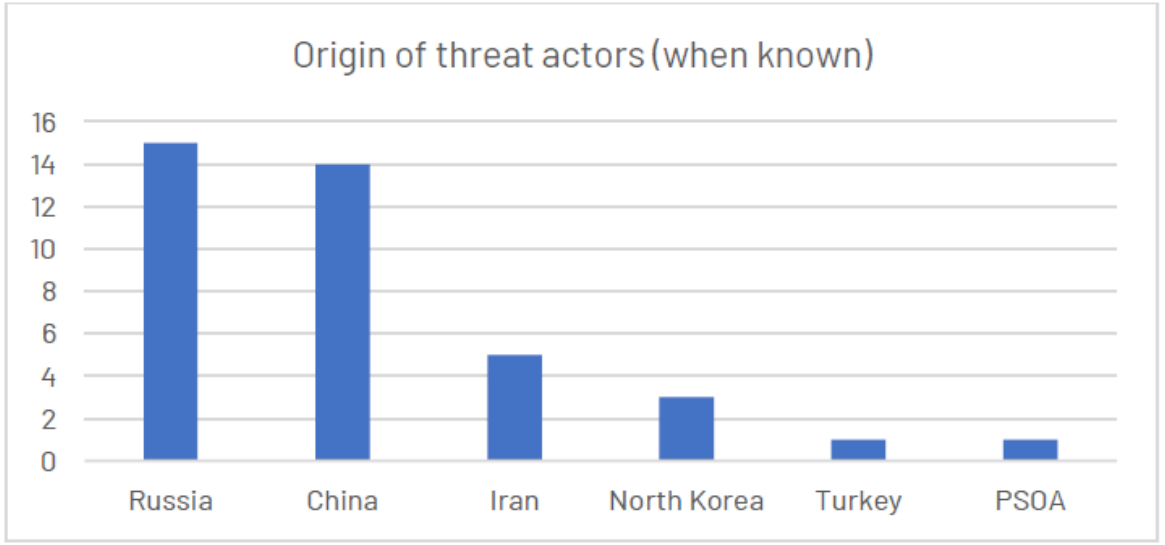
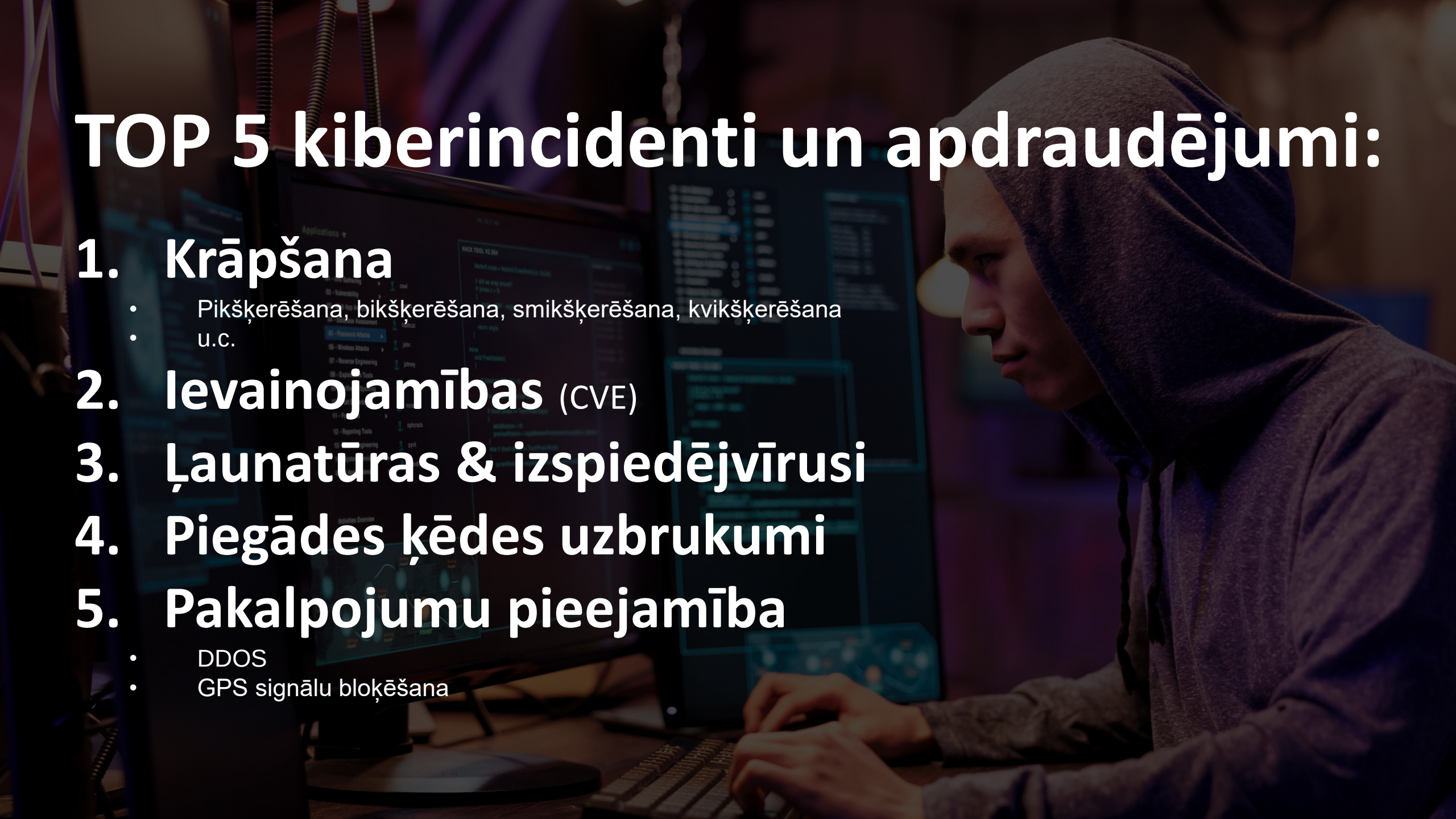


Figure 3 - Origin of threat actors

CERT. EU Threat landscape report 2023

PSOA = private sector offensive actor

https://cert.europa.eu/publications/threat-intelligence/tlr2023/



TOP 5 kiberincidenti un apdraudējumi:

1. **Krāpšana**
   - Pikšķerēšana, bikšķerēšana, smikšķerēšana, kvikšķerēšana
   - u.c.
2. **Ievainojamības** (CVE)
3. **Ļaunatūras & izspiedējvīrusi**
4. **Piegādes ķēdes uzbrukumi**
5. **Pakalpojumu pieejamība**
   - DDOS
   - GPS signālu bloķēšana

2. Ievainojamības

- Nulles dienas ievainojamības
- Zināmās ievainojamības

CVE (*Common Vulnerabilities and Exposures*) - standartizēta sistēma, kas paredzēta dažādu programmatūras un aparatūras produktu drošības ievainojamību identificēšanai un nosaukšanai.

Incidentos izmantotās ievainojamības

CVE-2025-53786

CVE-2019-18935

CVE-2025-53770

Izspiedējvīrusi

Noticis kiberuzbrukums kultūras nozares informācijas sistēmām - PAPILDINĀTA INFORMĀCIJA

Atskaņot tekstu

Publicēts: 08.08.2025.

Izspiedējvīrusi

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.

Ransomware operatoru izvēle

CISCO

CVE-2023-20269
Cisco Adaptive Security Appliance and Firepower Threat Defense Unauthorized Access Vulnerability
CVE-2020-3259 **Cisco ASA and FTD Information Disclosure Vulnerability**
CVE-2020-3153 **Cisco AnyConnect Secure Mobility Client for Windows Uncontrolled Search Path Vulnerability**
CVE-2020-3433 **Cisco AnyConnect Secure Mobility Client for Windows DLL Hijacking Vulnerability**

Ransomware operatoru izvēle

Fortinet

CVE-2025-24472 Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability
CVE-2024-55591Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability
CVE-2024-21762 Fortinet FortiOS Out-of-Bound Write Vulnerability
CVE-2019-6693 Fortinet FortiOS Use of Hard-Coded Credentials Vulnerability

Ransomware operatoru izvēle

Palo Alto Networks

CVE-2024-9474
Palo Alto Networks PAN-OS Management Interface OS Command Injection Vulnerability
CVE-2024-0012
Palo Alto Networks PAN-OS Management Interface Authentication Bypass Vulnerability
CVE-2024-3400
Palo Alto Networks PAN-OS Command Injection
CVE-2020-2021**Palo Alto Networks PAN-OS Authentication Bypass Vulnerability**

Ransomware operatoru izvēle

CISCO

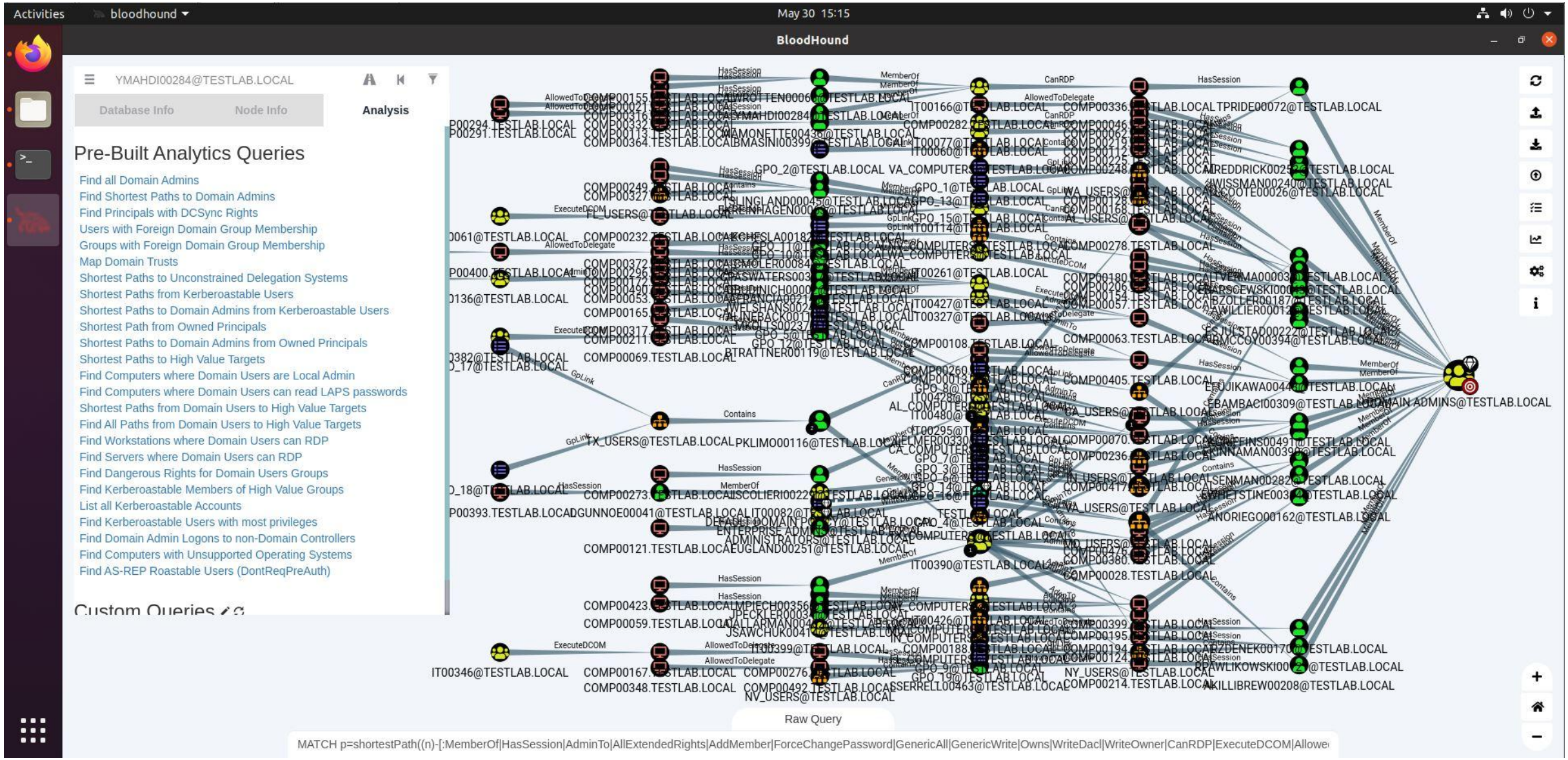
CVE-2023-20269
Cisco Adaptive Security Appliance and Firepower Threat Defense Unauthorized Access Vulnerability
CVE-2020-3259 **Cisco ASA and FTD Information Disclosure Vulnerability**
CVE-2020-3153 **Cisco AnyConnect Secure Mobility Client for Windows Uncontrolled Search Path Vulnerability**
CVE-2020-3433 **Cisco AnyConnect Secure Mobility Client for Windows DLL Hijacking Vulnerability**

No 0-dienas ievainojamībām nav pasargāts neviens ražotājs!

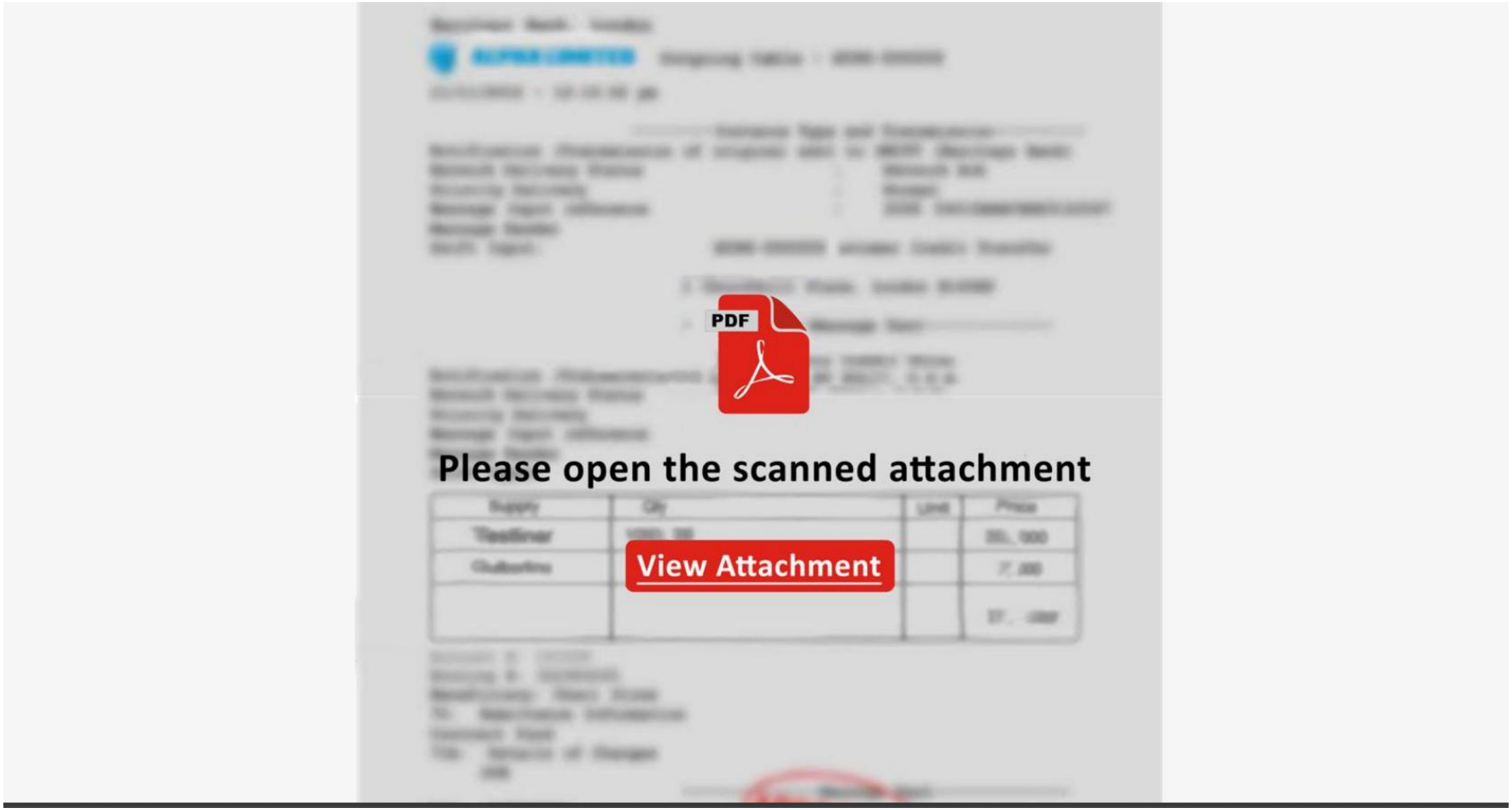
Plāns – samazināt uzbrucēju iespējas!

1. Atslēdzam neizmantotos servisus
2. Izdzēšam no iekārtu konfigurācijas paroles un kontus ko neizmantojam
3. Neizmantojam AD administratora piekļuves tiesību kontus LDAP/Radius servisiem
4. Ierobežojam ar IP/firewall filtriem iekārtu loku no kurām var veikt konfigurācijas izmaiņas
5. Segmentācija – dažādas piekļuves tiesības pie iekštīkla.
6. Monitorings – vienmēr!

Aktivitātes datortīklā



Office365 phishing



Visiem ir apnikušas paroles!

Standard FIDO

Simple, secure and cost-effective multi-factor authentication keys

View Standard FIDO Keys

Biometric FIDO

Biometric multi-factor authentication keys make passwordless logins possible

Explore Biometric FIDO Keys

NFC FIDO Keys

Multi-factor authentication keys featuring NFC and USB connectivity

Explore NFC FIDO Keys

iOS Security Keys

MFA security keys specifically designed for use with Apple devices

View iOS Security Keys

Vairāku slāņu piekļuves kontrole

1. Piekļuvi no perimetra iekārtas uz iekštīklu **ierobežojam** visos maršrutētājos, ne tikai pašā iekārtā
2. Atļaujam piekļuvi tikai nepieciešamajiem **servisiem**
3. Par **plānotajiem konfigurācijas maiņas** darbiem brīdinām kolēģus
4. **Pārbaudām** kas sanācis! Gan no iekštīkla, gan ārējām IP.
5. Veidojam pārbaudes skriptus, **procedūras**, lai automatizētu un vienkāršotu atkārtotas darbības.

3.9. Žurnālfailu pārvaldība

3.9. Žurnālfailu pārvaldība

58.1. informācijas sistēmas ieslēgšanu un izslēgšanu;
58.2. kontu izveidi, grozīšanu vai dzēšanu, kontu piekļuves tiesību izmaiņām;
58.3. kontu piekļuvi informācijas resursiem, tostarp neveiksmīgiem piekļuves mēģinājumiem;
58.4. datu pievienošanu, izmaiņām, dzēšanu un datu atlasi;
58.5. tehnisko resursu konfigurāciju izmaiņām;
58.6. informācijas sistēmas paziņojumiem, brīdinājumiem un citiem IKT notikumiem, kas varētu liecināt par kiberincidentu vai citu apdraudējumu informācijas sistēmas vai informācijas resursa drošībai.

Ieteikumi žurnālfailu apstrādei

1. **Neglabājiet** visus iespējamos žurnālfailus **maksimāli** ilgi!
2. Konfigurējiet datorsistēmu auditācijas pierakstus tā, lai tajos **būtu atrodama** nepieciešamā informācija
3. Neglabājiet žurnālfailus tikai **vienā vietā**!
4. Syslog, rsync, Logstash, Graylog, Beats utt.
5. Arī žurnālfailu glabātavām jāveido **rezerves kopijas**!
6. Pamēģiniet žurnālfailos kaut ko **atrast**! Vai jūsu izvēlētā sistēma indeksē pareizos laukus? Vai visi žurnālfaili ir izveidoti ar vienlīdz precīzu laika zīmogu? Cik senus žurnālfailus jūs spējat operatīvi pārmeklēt?

60.Tīkla plūsmu pieraksti:

Tīkla plūsmas žurnālfailos ietver informāciju par datu nosūtīšanas un saņemšanas notikumiem. Tīkla plūsmas žurnālfailos fiksē vismaz šādu informāciju:
60.1. notikuma laiku, kas sinhronizēts ar augstas precizitātes tīkla laika protokola (NTP) serveri;
60.2. datu nosūtītāja (avota) un saņēmēja (galamērķa) IP adreses;
60.3. avota un galamērķa izmantotos tīkla aplikācijas līmeņa protokolus (piemēram, HTTP, HTTPS, FTP);
60.4. ja attiecināms, avota unikālo identifikatoru (MAC adrese);
60.5. izmantoto tīkla transporta protokolu (piemēram, TCP, UDP);
60.6. pārsūtīto datu apjomu.

Tīkla plūsmu anomāliju kontrole

1. Ikdienas **monitorings** – iekārtu darbības profila izveide
2. Administratoru sesijas no **netipiskām IP**
3. Lielu **datu apjomu** pārsūtīšanas detekcija
4. Savienojumi starp **netipiskām iekārtām**
5. Ārēju **pakalpojumu sniedzēju** piekļuve netipiskos vai nesaskaņotos laikos
6. **TRAUKSMES –** saņemiet un apskatiet tās nekavējoties, nevis pēc 24 stundām!

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