Institute of Mathematics and Computer Science University of Latvia

CERT.LV
Information Technologies Security Incident Response Institution

Ministry of Defence Republic of Latvia

2023 Q4

Report on the implementation of CERT.LV tasks

2023 | Q4 (01.10.2023. – 31.12.2023.)

Summary

The situation in the Latvian cyberspace in Q4 2023 was intense but stable. The volume of compromised unique IP addresses was similar to the previous quarter and the same period last year. There were no dramatic fluctuations in the volume of compromised IP addresses, which shows that Latvia's cyberspace protection measures are effective and adequate.

Statistics on the types of threats to unique IP addresses in Q4 show that ***configuration flaws*** **are still the most common threat**, but their share has slightly decreased compared to the previous quarter and to the same period a year ago. *Malicious code* comes in second place, with a surprising 62% increase compared to Q3. In third place is *intrusion attempts*, also up 19% on the previous quarter and up 65% on the same period a year ago.

In Q4 2023, 335 143 unique endangered IP addresses were registered on CERT.LV. This is 0.32% less than in the previous quarter and 7% less than a year ago. The active protection DNS firewall provided by CERT.LV and NIC.LV (the registry of the top-level domain .LV) reached a new record – its (unique) users were protected from malicious links, viruses and malicious websites 467 888 times. This is an increase of 1046% compared to Q3 and 521% compared to the same period a year ago. The DNS firewall handles around 1.5 million DNS requests each month.

Analysis of the data shows that **current attacks continue to involve the use of malware** to gain access to equipment and systems of public and private sector employees, including the active use of emails with remote access files as attachments. Network compromises in the public and private sectors have increased with the spread of encrypting ransomware viruses, which encrypt data on the victim's machine and demand a ransom to recover it.

Given the current geopolitical tensions and the threat of hybrid warfare, it can be assumed that the **significant increase in hacking attempts in cyberspace** is due to politically motivated Russian hacking attacks and targets. This can be assumed in particular with hacking attempts, that were related to apparent efforts to compromise the security of critical infrastructure of NATO and EU Member States.

In late 2023, especially in the pre-Christmas period, **a large number of commercially motivated phishing campaigns** were aimed at the Latvian population. The fraudsters used text messages, fraudulent telephone calls or impersonation of employees of public authorities and other organisations, including sending photographs with a fake police officer's identity cards as an attempt to false identity and credibility proof while trying to retrieve people's personal information or internet banking credentials. As usual, at the end of the year, accountants of companies and organisations were also targeted by fraudsters, who were sending notifications for allegedly unpaid invoices. Artificial Intelligence (AI) solutions are widely used by members of organised crime groups to prepare and send messages and to carry out fraud with fake caller IDs – several people did not recognise the fraudsters' schemes and, for example, lost their finances by installing fraudulent software on their devices or by taking part in the schemes offered by fraudsters.

Active distributed denial-of-service (DDoS) attacks by hacktivist groups supporting the aggressive Russian regime were periodically observed against State and local authorities and state-owned companies, as well as companies in the financial, transport, energy, postal and telecommunications sectors. However, the targeted infrastructures were prepared to stand up against the attacks and the availability of the services or resources concerned was not affected.

Russia remains the main source of cyber threats, exploiting the political situation to attack targets by targeting political issues, such as the rise of issues such as nationality and residence permits.

But whereas previously politically motivated attacks were aimed at disrupting systems, Q4 saw a shift in tactics towards cyber espionage and Kremlin influence operations.

CERT.LV continues to strengthen its role as a leader in organising and conducting threat hunting operations in the European Union - developing and strengthening strategic cooperation not only at the national but also the international level, contributing to NATO's collective European defence, developing and improving threat hunting methodologies, and organising experience sharing events with partner organisations in allied countries.

In fulfilling its mission, CERT.LV continues to promote cybersecurity and be a trusted opinion leader in Latvian cyberspace.

CERT.LV stresses that cyber hygiene is essential at both governmental and commercial sector organizations. Sufficient knowledge of cyber-hygiene principles allows protection of Latvian and allied cyberspace from various cyber-attacks. To achieve this goal, it is important to strengthen the resilience of critical infrastructure to cyber threats and the ability to restore services as quickly as possible after incidents. This includes also the situation of hybrid warfare. To add CERT.LV recommends keeping an eye on the opportunities and threats presented by the development of artificial intelligence.

CERT.LV continues to actively inform the Latvian public about cybersecurity risks and cyber hygiene best practice. During the reporting period, **CERT.LV experts participated in 55 educational events, educating 16 144 participants on IT security, which is almost 8 times more than in the previous quarter.** The CyberChess 2023 conference was a success, bringing together more than 500 participants from 18 countries in Riga and attracting around 6000 live views from 39 countries.

With 376 media publications, up 47% compared to the previous quarter as a total, 16.5 million views were generated.

The report contains information accessible in the public domain which does not contain information regarding the results achieved by CERT.LV that include limited access information. The report is for informational purposes only.

Contents

1. Cybersecurity Threats in Cyberspace: Statistics and Trends

CERT.LV compiles information on endangered Latvian IP addresses every month. For threat accounting, CERT.LV works with an internationally used incident taxonomy. During the reporting period, all threats recorded by CERT.LV are listed in one place, broken down into threat types (e.g., malware, intrusion, fraud), as well as types of malware and configuration vulnerabilities.

Taxonomy – a formalised way for CERT.LV to collect, categorise and represent technical information about threats..

In Q4 2023, 335 143 compromised unique IP addresses were recorded on CERT.LV, which is 0.32% less than in Q3 and 7% less than in the same quarter last year.

Overall, Q4 was a busy but stable quarter. The total number of threats and incidents has changed little over the last three quarters of 2023. As expected, the story of threat motives remains the same: the challenges to our cybersecurity are geopolitical and digital change, as well as war in Ukraine and the activities of pro-Russia hacktivists, including state-sponsored groups, as well as seasonal factors such as Black Friday shopping fever and the year-end pre-holiday period, characterised by fake shops and lotteries, and when we need to be more vigilant against phishing campaigns and fraudulent emails asking for payment for undelivered parcels or for customs release costs.

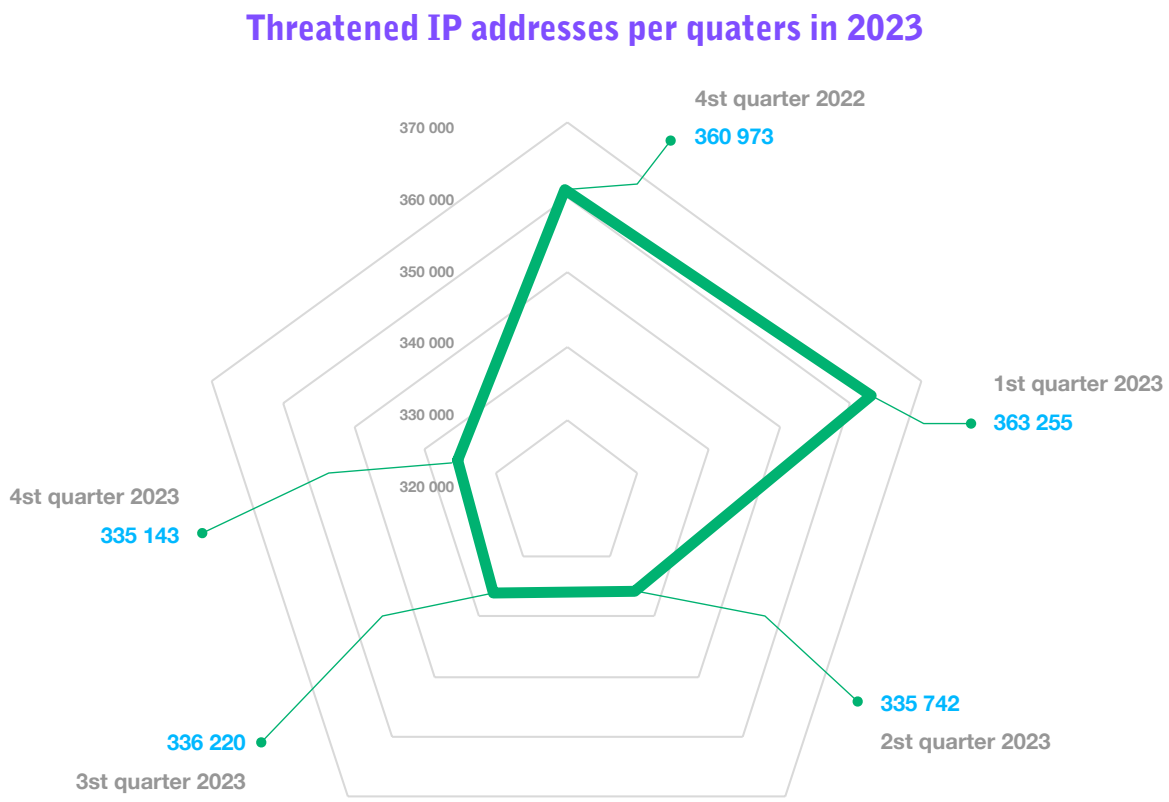


Figure 1 - Registered threatened unique IP addresses per quarter in 2023

During the reporting period, the threat level was stable and there were no dramatic fluctuations in the volume of endangered IP addresses. This signals that the frequency and impact of attacks have decreased quarter-on-quarter.

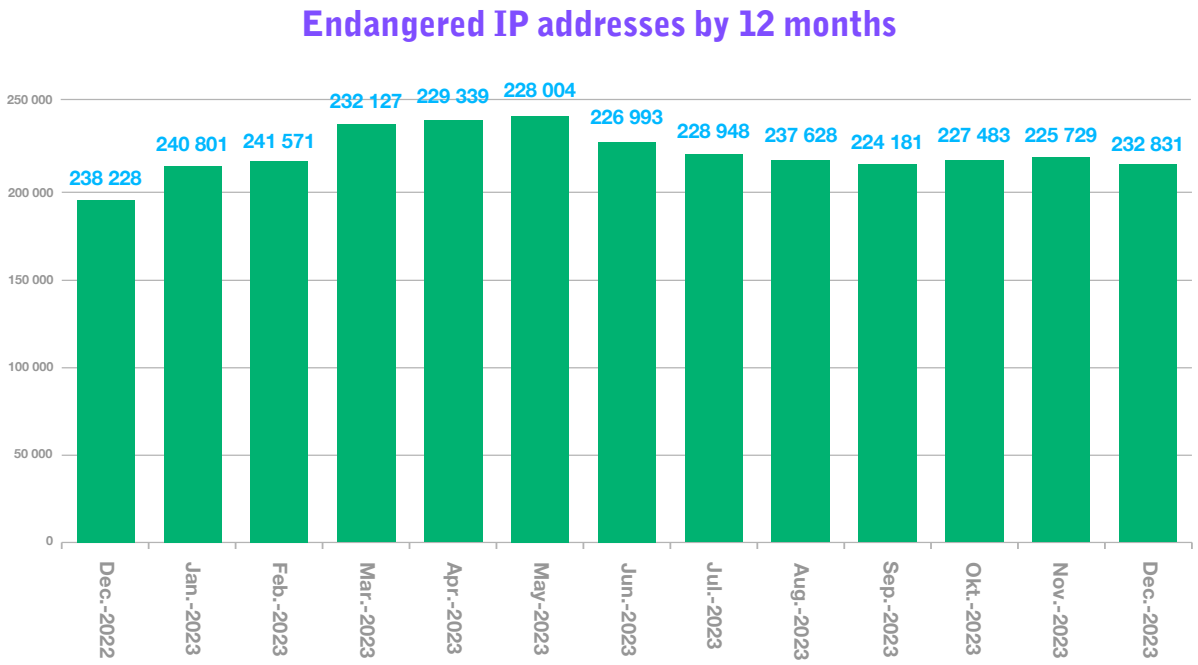


Figure 2 - Unique endangered IP addresses by 12 months

In Q4 2023, the most common threat type was **configuration flaws** (68 978 unique IP addresses), with a drop of 3% compared to Q3 and 25% less than in the same period a year ago.

In 2nd place was **malicious code** (11 075 unique IP addresses), surprising with an increase of 62% from Q3 but down 2% from the same period a year ago.

Meanwhile, i**ntrusion attempts** (969 unique IP addresses) remain in 3rd place with an increase of 19% compared to Q3 and 65% more than in the same period a year ago..

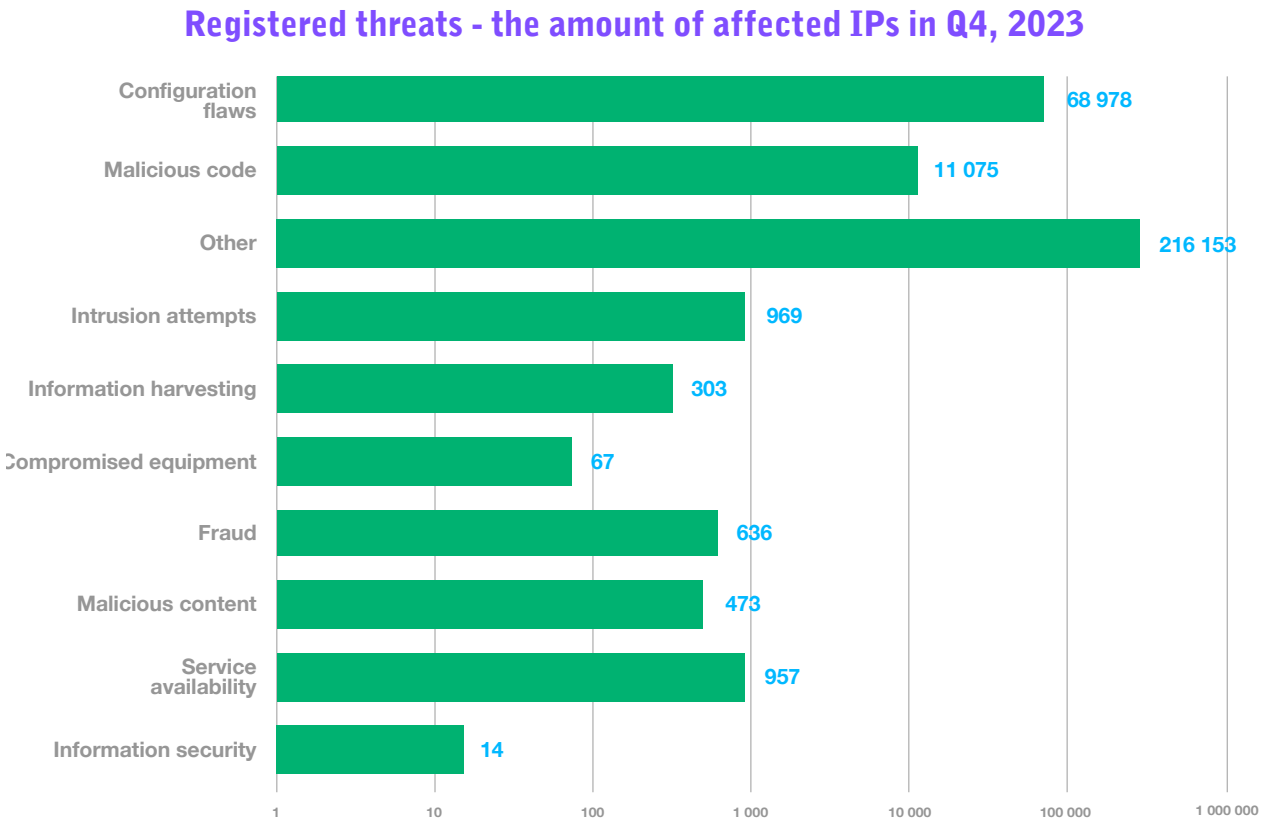


Figure 3 -Threatened unique IP addresses by CERT.LV by type of threats in Q4, 2023

Compared to the same period a year ago, the number of unique endangered IP addresses in Q4 2023 showed a significant increase in four types of threats: intrusion attempts, fraud, malicious content and information security. In contrast, there were declines in six threat types: configuration flaws, malicious code, information harvesting, compromised equipment, service availability, and in the other category.

In the current geopolitical situation and hybrid warfare, it can be assumed that the significant increase in intrusion attempts in cyberspace is due to politically motivated Russian hacking and attack attempts, especially those related to apparent efforts to compromise critical infrastructure of NATO and EU Member States.

Also, in Q4, a large number of commercially motivated fraudulent activities were directed against Latvian citizens, in which attackers attempted to retrieve internet banking access data using SMS messages, fraudulent phone calls and impersonating employees of State authorities, including the State Police, courts, SRS, CERT.LV and other organisations such as Latvijas Pasts, Citadele banka AS, and Google. Several citizens did not recognise the fraud and lost significant financial resources by installing remote access software on their computers.

As could have been expected, the number of threats at the end of the year increased relatively more in December, when several fraudulent campaigns were detected. The pre-holiday period saw an increase in fraudulent online shops trying to lure gullible shoppers with unbelievably low prices for well-known branded products, as well as fake advertisements circulating on social networks, where supposedly well-known companies offer people to buy returned parcels or suitcases abandoned at the airport for a small fee, thereby scamming people out of their payment card details. As usual, the end of the year also saw an increased focus on accountants in companies and organisations, who are particularly busy at this time of year. Fraudsters sent notifications of a supposedly unpaid invoice on time or requested an urgent payment on behalf of a manager, hoping that the signs of forgery in the received email would not be spotted in the rush.

The last months of the year were fraught with significant vulnerabilities. The prompt installation of updates to address vulnerabilities was necessary for a wide range of protection tools used in companies, for email servers and for mobile

CERT.LV Expert Commentary

Russia was the source of the majority of cyber threats in the reporting period, with targets chosen according to political developments, such as the rise of citizenship and residence permit issues. However, while politically motivated attacks were initially launched to disrupt systems, Q4 saw a shift in tactics towards cyber espionage and Kremlin influence operations. For example, the bomb threat email campaign sent to Latvian schools, kindergartens, courts and local governments was most likely a Russian-organised influence operation against the Latvian public.

Active distributed denial-of-service (DDoS) attacks by hacktivist groups supporting the aggressive Russian regime were periodically observed, mainly targeting State and local government institutions and capital companies, as well as financial, transport, energy, postal and telecommunications companies, but the targeted infrastructures were ready to repel the attacks and they had no impact on the availability of the services or resources concerned..

The good news is that no successful attacks with a significant impact on the public and critical infrastructure sector have been detected so far. CERT.LV, contributing to NATO's collective defence of Europe, as a strong leader in conducting threat hunting operations in European cyberspace, successfully identified and neutralised both politically (Russian, Belarusian, Chinese) and commercially motivated attackers from targeted infrastructure during the reporting period.

The bad news is that Russia remains the main threat to Latvia and NATO and is one of the most active cyber aggressors, using a variety of methods to influence politics, the economy and public opinion of other countries. The current geopolitical situation is expected to further increase cybersecurity risks worldwide. There are concerns that cyber-attacks will increase, especially in countries where sanctions against Russia are in place. In addition, Western countries face two major challenges: in addition to Russia's war in Ukraine, Israel's war with the terrorist organisation Hamas is also a cause for concern and could escalate into a wider regional conflict.

phones. Attackers did not hesitate to exploit these vulnerabilities to infect devices that were not updated and take control of them.

In order to protect Latvian cyberspace and allies from cyber-attacks, during the reporting period CERT.LV emphasised the importance of effective cyber hygiene at the national and enterprise level, the resilience of critical infrastructure cybersecurity and the ability to restore services after incidents, including in hybrid warfare, as well as the opportunities and threats presented by the development of artificial intelligence.

TOP3 Malicious Codes or Malware

In Q4 2023, the **#1** malware in the Top is the newcomer ***Socks5systemz***, which infects machines and turns them into redirection ***proxies*** or proxies that could be used by bad actors to make it harder to track their illegal and malicious activities. Thus, a device infected with ***Socks5systemz*** is taken over unauthorised by third parties and is more likely to be involved in supporting illegal activities..

#2 is the ***Adload*** malware, which steals victims' browser data and inserts fake/fraudulent ads on the victim's web browser. If ***Adload*** malware is detected on a MAC device, a full scan of the computer with an up-to-date antivirus program is required.

#3 – ***Pseudomanuscrypt*** malware is an espionage Trojan that is able to gain unauthorised access to and exfiltrate data from the infected device, including keyboard keystrokes, clickboard data, app authentication data, and is also able to take screenshots of the infected system, record sound with a microphone and more.

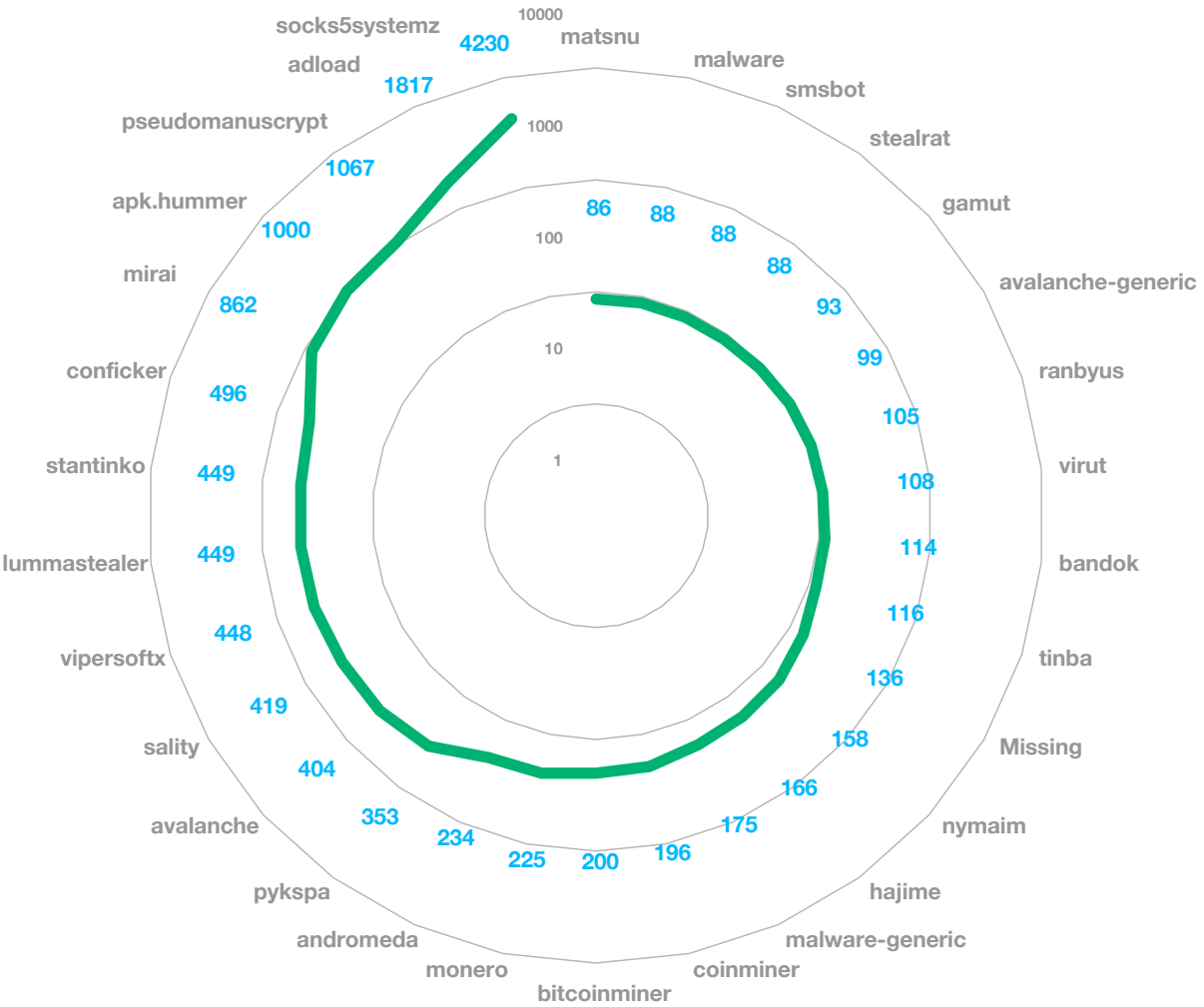


Figure 4 -Total number of CERT.LV registered thraetened unique IP addresses in Q4, 2023 with type of threat – maliciou code

TOP 30 Configuration Flaws

In Q4 2023, the **#1** configuration flaw is ***Open-cwmp***, a management protocol used to allow individual devices such as routers or VoIP phones to connect to a network provided by a telecommunications service provider. To prevent unauthorised access risks to this management tool, it is recommended to restrict access rights, e.g., by using a VPN.

#2 is invariably ***Open-smb***. Vulnerability indicates that the equipment in question has an open port to the public internet, which is used by the SMB protocol to access files and equipment on the internal network. By compromising the SMB protocol, attackers are able to gain access to the internal network devices and infect them with, for example, a ransomware virus..

#3 goes to ***Accessible-ftp***. The FTP data transfer protocol does not provide encryption of the data to be transferred, unless additional protection in the form of TLS or SSL protocol (FTPS, respectively) is used. This configuration flaw exposes sensitive information and access data to the risk of leakage.

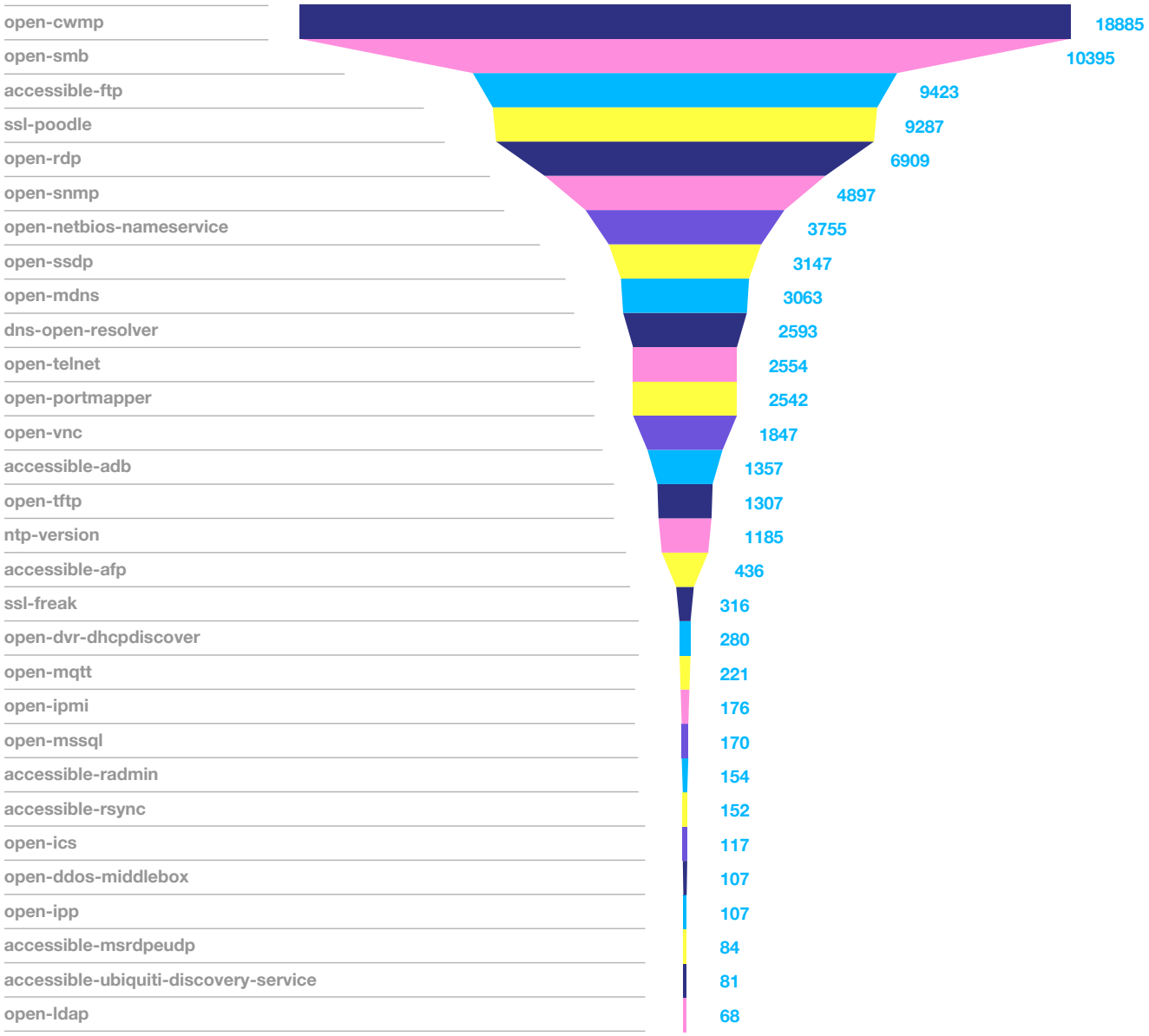


Figure 5 - Number of threatened unique IP addresses registered by CERT.LV in Q4, 2023 with type of threat – configuration flaw

Distribution of unique endangered IP addresses in the matrix during the reporting period

For a more complete monthly assessment of the cybersecurity situation, CERT.LV uses the threat matrix developed by the UK National cybersecurity Centre (NCSC). Threats in the matrix are grouped according to the importance of the affected institution/company, the extent to which the threat affects the general public, and the significant impact the threat will have.

Combining all the factors, the threats are divided into 6 categories:

C1	National threat, basic services affected, economic or political stability threatened.
C2	High-level threats, national institutions, national infrastructure affected.
C3	Major threats, widespread impact on commercial sector, national and local authorities.
C4	Major threats, medium impact on commercial sector, national and local authorities.
C5	Moderate threats, minor impact on commercial sector, national and local authorities.
C6	Everyday threats, impact on individuals, not significant impact on businesses or public and local authorities.

Figure 6 - Threat matrix categorisation

No national level threats (C1) were recorded during the reporting period. The majority, 98%, fall into the minor threat category (C6) and are related to individual user devices or widespread, mundane, automated attack attempts against businesses or State and local authorities.

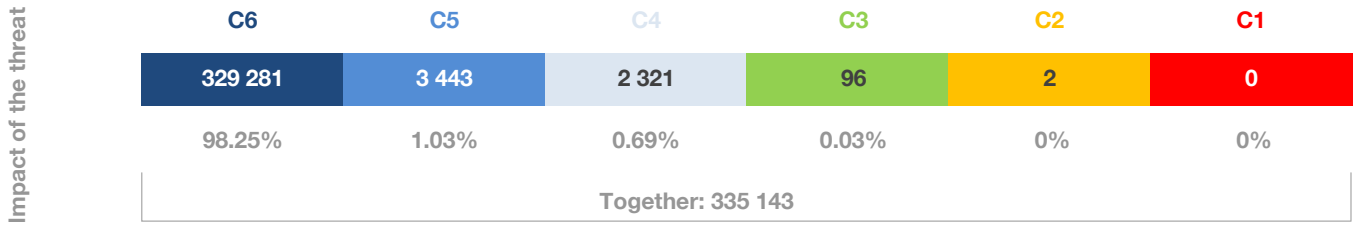


Figure 7 - Categorisation of unique endangered IP addresses by impact of the threat in Q4

Two IP addresses have been recorded in the high threat (C2) category, associated with a single incident on 31 October 2023. The incident is related to a ***Barracuda*** vulnerability (CVE-2023-2868) which led to compromised equipment in a public authority. Testing showed that the compromised equipment was located in an isolated environment and that no large-scale data extraction by the attacker was performed and no other internal equipment was affected..

Significant comprehensive threats (C3) represent 0.03% or 96 unique endangered IP addresses/incidents of all categorised threats, an increase of 62 unique endangered IP addresses compared to the previous quarter. Most of these threats, or almost 80%, are malicious code in a number of internal devices and systems of local governments, healthcare and educational institutions and electronic communications providers.

Impact of the threat						
5	0	0	0	0	0	0
4	28	5	0	0	14	2
3	10 313	243	56	67	54	28
2	127 744	7 524	929	506	1 013	735
1	176 033	6 551	1 088	372	738	1 100
	1	2	3	4	5	6

Number and/or importance of affected population, institutions or enterprises

Figure 8 - Categorisation of unique endangered IP addresses in the matrix in Q4ī

Significant threats with medium impact (C4) account for 0.69% (2321 unique endangered IP addresses/ events) of all categorised threats. Most of the C4 threats were configuration flaws (***Accessible-ftp, Ntp-version, Dns-open-resolver***, etc.), but intrusion attempts, fraud incidents, malicious code in high and medium priority institutions (several local governments and public institutions, universities and other organisations) were also observed.

2. TOP Cyber Incidents and Threats: Support and Recommendations to Prevent them

In order to promote IT security in Latvia and strengthen resilience to cybercrime, in Q4 2023 CERT.LV continued its active cooperation with State and local government institutions, banks, electronic communications merchants and other organisations and cybersecurity ecosystem partners in addressing incidents of varying severity.

Cyber-attacks against public institutions, organisations and critical infrastructure service providers are a serious threat that could negatively impact the security of citizens, institutions and businesses, as well as pose a threat to providers of essential services and digital services, thereby affecting national security, financial stability and even undermining economic growth.

Incident reporting, cooperation and information sharing remain essential prerequisites for effective cybersecurity. CERT.LV continues to keep government representatives, heads of State institutions and cybersecurity experts regularly informed about developments in Latvian cyberspace. CERT.LV also continues to provide monthly event aggregation and analysis, providing decision-makers with the information they need to timely predict and prevent internal and external threats, as well as to improve the protection and resilience of the country's critical infrastructure

CERT.LV is the country's largest aggregator of cyber threat data and information, automatically processing and analysing several million incoming signals per month

The key cyber incidents and threats highlighting the trends observed in Q4 are discussed below in subsections 2.1 to 2.6.

CERT.LV team support in incident investigations		
15–20 manually handled incidents per day	More than 6.5 million cybersecurity telemetry signals per month	Support for everyone, but the priority being: basic and digital service providers, critical infrastructure holders and public authorities

2.1. Fraud

Fraud campaigns remain high and continue to increase

Q4 2023 has seen a steady increase in the number of fraudulent text messages, emails and calls, with fraudsters posing as representatives of various public authorities, organisations and companies. The number and variety of methods is growing, with techniques becoming more sophisticated and the Latvian language no longer being an obstacle for fraudsters. The main goal of fraudsters is to gain access to social network accounts (*Facebook, Google, Instagram*) or to retrieve personal data and access to online banking by asking the victim to confirm a fraudulent transaction by logging in.

In Q4, there were widespread incidents of phishing, where citizens were sent a fake text message purporting to be from the courts or police with a fraudulent link attached. In order to gain people's trust, fraudsters also sent a photo of a fake police officer's identity card on communication apps as a way of allegedly proving their identity.

In October, a large number of applications were received from people looking for work who had been contacted by fraudsters claiming to be from the HR department of a company. After lengthy contact, it was found that the fraudsters had aimed to obtain the victim's bank account details and had been successful in several casess.

As could have been expected, the number of fraud cases, including fraudulent webshops, increased at the end of the year, especially in November and even more so in December. Several fraudulent campaigns were also recorded in early December, in which attackers posed as representatives of postal service providers, the police, the State Revenue Service, Google and other companies in order to persuade people to disclose their online banking access details. Accountants of companies and organisations were also targeted.

As an additional test of citizens' vigilance, cybercriminals' innovative approach to fraudulent phone calls was implemented using fake caller IDs – pretending to be a bank – and spoofing citizens' online banking credentials. By authorising the fraudster's online banking activity, the fraudster is able to cause significant monetary losses to the victim, even if they do not have any funds in their account. The fraudster can apply for several lines of credit and consequently scam the victim out of money that they do not actually have.

Top 5 most common fraud schemes during the reporting period

Fraudsters impersonating law enforcement authorities: impersonating the State Police, fraudsters inform about allegedly illegal activities on a bank account or a desire to illegally arrange a loan in the name of the recipient of the call. To build trust, fraudsters often work in teams and involve a 'colleague' during the phone call to build trust and reinforce the idea that the situation is real.

Impersonating bank employees: one of the most popular methods used by fraudsters. Fraudsters inform their victim that fraudulent activity is taking place on the account and that there is an urgent need to remedy the situation by asking the person to disclose access details. For example, one trend: fraudsters impersonated a bank employer and asked to open a bank account and then share the data. This was done through phone calls, text messages, fake websites and online advertisements that visually resembled the communication material used by the bank. CERT.LV is aware of a case where a fraudster actually created a bank account for a victim at the same time as the victim was going through the process of creating the account and thought they were approving their own actions; they actually approved the fraudster's actions and created a bank account in their own name but could not access it himself/herself because the access **had been passed** to the fraudster.

Fake financial supervisors: during the reporting period, cases of fraudsters posing as representatives of the Data State Inspectorate, the SRS or the financial regulator were recorded. In order to obtain personal data and access to a bank account, fraudsters report a cryptocurrency account supposedly opened in the name of the recipient of the message, where illegal transactions are supposedly taking place..

Phishers impersonating Google, Netflix, booking.com: fraudsters often impersonate employees of local and international companies, for example using the Google brand, to report suspicious activity or connections to a Google account. Fraudsters tried to convince victims to download remote management software such as AnyDesk or TeamViewer to gain access to their money.

Fraudsters impersonating Latvijas Pasts VAS, DPD and Omniva: an impersonation of Latvijas Pasts VAS was recorded on Facebook, where scammers created a page called Latvijas Pasts Express, offering to buy allegedly undelivered parcels. The name

CERT.LV Expert Commentary

Fraudsters have significantly improved their methods of psychological attack or social engineering. The most significant changes are in the methods of sending messages, which are becoming more efficient, using artificial intelligence (AI) to prepare and send messages. The development of AI presents both opportunities and threats, and cyber fraud can be expected to continue to increase in frequency and intensity.
In cyber fraud, organised criminal groups are most likely to work in large groups, making the extensive use of innovations and new information technology solutions to harm people. The bad news is that AI is used to create fake websites, images and audio files that mislead people, thereby exfiltrating the victim's online banking details, social networking profile credentials or other information. Many people fall for these scams because they are credible and the websites designed to spoof access data are very well-designed, mimic the original sites and also use the Latvian language. Nevertheless, the good news is that sound investment in AI can also result in better protection capabilities and better tools to fight threats

of Latvijas Pasts VAS was also used in fraudulent text messages and emails in an attempt to mislead people into providing additional information for delivery or paying customs duties. Impersonation of private sector courier service providers DPD and Omniva was also a popular fraud scheme. By setting up fake websites, visually very similar to the websites of these companies, citizens were scammed out of their bank card details and defrauded of their money.

SAFETY RECOMMENDATIONS AND ADVICE

To protect yourself from phishing attacks, CERT.LV urges people to be vigilant and, when receiving text messages or emails, not to enter bank or personal details in links sent by strangers before you have verified their authenticity. Also, pay particular attention to:

- **the sender's contact details (e.g., email address in the *From*: field);**
- **links in the text – whether they lead to the relevant website;**
- **files attached to the email and their extensions – what letters appear to the right of the filename after the last period. If the last letters are .iso, .exe, .img, .rar or .zip, it is better not to open the attachment.**

2.2. Distributed Denial-of-Service (DDoS)

During the reporting period active distributed denial-of-service (DDoS) attacks by hacktivist groups supporting the aggressive Russian regime were periodically observed, mainly targeting State and local government institutions and State capital companies, as well as financial, transport, energy, postal and telecommunications companies, but the targeted infrastructures were ready to repel the attacks and they had no impact on the availability of the services or resources concerned.

Although the overall situation is stable, one of the most aggressive cyber-attacks took place on 14 November and again on 22 November, when the hacktivist group Killnet circulated information on the Telegram platform calling for service 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 assessed as negligible, i.e., there was no impact or it was temporary.

CERT.LV provided recommendations for improving active protection solutions and procedures.

SAFETY RECOMMENDATIONS AND ADVICE

CERT.LV has summarised the preparations that should be made in anticipation of a DDoS attack in order to mitigate or prevent the impact of such an attack. Each institution, company and organisation should assess the priority of the items listed and implement them taking into account the specificities of their infrastructure.

More information: https://cert.lv/lv/2022/08/ieteikumi-ddos-ietekmes-mazinasanai

2.3. ulnerabilities and Configuration Deficiencies

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 networksi.

When identifying compromised devices in Latvian cyberspace, it was found that the number of compromised devices in the public sector and of local authorities was noticeably lower compared to the previous year, probably due to rather quick and active communication from CERT.LV about potential threats.

At the same time, there were many newly discovered critical vulnerabilities in Q4. CERT.LV notified the holders of the vulnerable systems and provided support in incident analysis and remediation. CERT.LV provided alerts on vulnerabilities and updates, providing coordinated guidance and recommendations.

CERT.LV Expert Commentary

Critical vulnerabilities provide attackers with the ability to perform remote code execution (RCE) by gaining access to a vulnerable system.

Critical vulnerabilities include those that allow an unauthenticated or unauthorised user to gain access to a system. Such a user could potentially read information stored in the system in an unauthorised manner and then potentially seek to execute an RCE. CERT.LV encourages following the developers' recommendations and immediately update the software to the latest available version.

TOP 6 vulnerabilities during the reporting period

***Exim vulnerabilities*:** On 2 October, CERT.LV alerted Exim email server hosts to several vulnerabilities, including CVE-2023-42115, which is related to external authorisation and allows attackers to perform remote code execution (RCE). All Exim users were advised to follow the developers' recommendations and update software to the latest available versionu.

More: https://cert.lv/lv/2023/10/exim-ievainojamibas

Critical WinRAR vulnerability: On 20 October, CERT.LV provided an alert of a critical vulnerability in WinRAR software, CVE-2023-38831, which is being actively exploited by APT (*advanced persistent threat*) groups to compromise devices and networks. All software versions up to 6.23 were affected. The WinRAR vulnerability allows attackers to execute arbitrary code if a user attempts to view an innocuous file in a ZIP archive, and a number of other conditions must be met. CERT.LV called for an infrastructure-wide software update to version 6.24 as a matter of urgency.

More: https://cert.lv/lv/2023/10/kritiska-winrar-ievainojamiba-cve-2023-38831

Critical vulnerability in several QNAP products: On 6 November, CERT.LV issued an alert about a critical vulnerability in several QNAP products. The vulnerability, CVE-2023-23368, which opens the door to remote code execution by attackers and affects several QNAP (QTS, QuTS hero and QuTScloud) products, is very serious and rated 9.8 on the CVSS scale (1–10). Critical vulnerabilities have been observed in several QNAP products over the last few years and were exploited in ransomware attacks against institutional and corporate resources in Latvia. CERT.LV urged not to delay the installation of updates for QNAP products..

More: https://cert.lv/lv/2023/11/kritiska-ievainojamiba-vairakos-qnap-produktos

Critical OwnCloud vulnerability (CVE-2023-49103): On 30 November, CERT.LV issued an alert about a vulnerability in OwnCloud – its solution component graphapi version 0.2.0 to 0.3.0 was found to have a critical vulnerability CVE-2023-49103 with a CVSS score of 10.0 on a scale of 1 to 10. The vulnerability allows an unauthenticated user to access phpinfo configuration information and read the values of system environment variables such as administrator

password, licence keys, email server credentials and other sensitive information. CERT.LV informed about the necessary actions and called for attention to other significant OwnCloud vulnerabilities.

More: https://cert.lv/lv/2023/11/kritiska-owncloud-ievainojamiba-cve-2023-49103

Critical vulnerabilities in Zyxel NAS devices: On 1 December, CERT.LV warned of several vulnerabilities in Zyxel NAS (network-attached storage) devices, including three critical vulnerabilities that allow an unauthenticated attacker to execute system commands at the operating system level. These vulnerabilities affect the NAS326 and NAS542 devices and exploitation of the vulnerabilities could lead to unauthorised access, leakage of sensitive system information or allow an attacker to completely take over the affected Zyxel NAS devices. CERT.LV informed about the necessary updates and urged not to delay installation.

More: https://cert.lv/lv/2023/12/kritiskas-ievainojamibas-zyxel-nas-ierices

Critical SSH protocol vulnerability: In late December, CERT.LV identified more than 10 000 unique devices exposed on the public network and exposed to the critical vulnerability CVE-2023-48795. This is an SSH protocol vulnerability affecting OpenSSH extension functions. Exploitation of this vulnerability allows an attacker to lower the security level of a user's device or to disable it completely. This vulnerability can be exploited in a Terrapin attack (prefix truncation attack) and affects various products such as OpenSSH versions older than 9.6, Dropbear versions before 2022.83 and many other products that support SSH server functionality.

CERT.LV encourages reviewing all equipment that hosts an SSH service accessible over the internet, disable unused SSH services and update the installation of necessary software updates for the equipment.

More: https://cert.lv/lv/2024/01/kritiska-ssh-protokola-ievainojamiba-cve-2023-48795

CERT.LV regularly informs internet users about the most significant vulnerabilities and recommendations for their remediation via electronic communications service providers. More information on the threats is available at: https://www.esidross.lv/informacija-par-apdraudejumiem/

2.4. Malicious Code

Malware distribution in Q4 2023 continued to be mainly for two purposes: to exfiltrate data or for profit. Emails with malicious attachments were distributed in a campaign to extract information on behalf of banks, institutions and companies. Upon opening the attachment, the device was infected with malware that collects usernames, passwords, cryptocurrency wallet and access information, etc., to send it to a server controlled by the attacker.

Looking at the trends for 2023, in general, in terms of malware activity and information technology security incidents, it can be concluded that system hacks and infections occurred using the following methods:

- phishing;
- exploitation of publicly known vulnerabilities – versioning vulnerabilities and zero-day vulnerabilities;
- misconfiguration; abuse of exposed web services – default authentication credentials, brute-force password cracking, versioning vulnerabilitie;
- infected storage media – USB sticks;
- installation of pirated software;

- leaked and easily guessed user passwords;
- automated attacks.

The main types of malware in the reporting period

- user data hijackers;
- *Bot-net* or zombified computers;
- ransomware;
- remote-control *Trojans* targeting data mining or further infrastructure compromise.

The most common user data-jacking malware has been found to target insecure, locally stored authentication data 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 email.

The reporting period also saw an increase in the number of cases where users deceived by fake advertising have installed fake AI plug-ins in their web browser themselves. For example, there were cases of malicious *AiGoogle* plugins designed to steal access data to *Facebook* accounts.

Encryption ransomware was distributed for profit, attacking the victim's device, decrypting the data and demanding a ransom to recover it. Encryption virus attacks were experienced in both the private and public sectors.

In addition, compromised emails or app accounts are often used to further spread malware. For example, several cases of *Agent Tesla* malware being spread from compromised emails by sending fake invoices were identified.

There were also cases where, after hacking email accounts, attackers set up email filters to intercept and redirect correspondence of interest to themselves. These actions were carried out for fraudulent purposes, e.g., by intercepting the emails of customers of the hacked company, invoices were sent to customers with changed bank details.

Banking Trojans such as *Ranbyus, Corebot, Tinba* are the leading malware activity in the Latvian IP address range. The *RaspberryRobin* malware is still relatively active and is mostly spread from device to device with infected USB sticks, e.g., the presence of *RaspberryRobin* malware was detected in the networks of several public institutions during the reporting period.

Cases of malware that had been running undetected in the infrastructure for several years were also detected. For example, *Windows* servers were identified as having been compromised as long ago as in early 2021 using the then-new CVE-2021-26855 vulnerability and infected with the remote control malware *SparrowDoor*.

In 2023, including the reporting period, there was a strong presence of botnet activity in Latvia. It was found that some brute-force (via password guessing) and DDoS attack devices located in the Latvian IP area were infected and included in the *Mirai* and *Gamut* malware botnets. The *socks5systemz* and *SystemBc* botnets were also actively spreading. Moreover, *socks5systemz* was ranked 1st in the malware TOP30 list in Q4.

CERT.LV Expert Commentary

It is important to note that during the reporting period, it was not the exploitation of newly discovered vulnerabilities that most often led to encrypted systems, but the insufficient protection of resources. Weak passwords and outdated software with vulnerabilities publicly known for several years, which could have been remedied by a timely software update, were the main vectors of initial infection. In some cases, poor IT infrastructure design was an additional contributing factor in the spread of the virus.

2.5. Intrusion Attempts

Information on intrusion attempts was received throughout Q4 at a significant rate. These attacks were carried out in most cases through brute-force attacks against various electronic communications companies, State and local authorities and the private sector. According to the information available to CERT.LV, these attacks were not successful.i.

The attackers were most interested in technologies used for remote working, such as Remote Desktop Protocol (RDP), Virtual Private Network (VPN) and online meeting and chat platforms. Cybercriminals, using various types of attacks, including newly discovered vulnerabilities, persistently sought to penetrate the internal networks of companies and organisations to gain unauthorised access to sensitive information or to encrypt devices and demand a fee for data recovery. Attackers also exploited long-known configuration flaws in widely used products.

SAFETY RECOMMENDATIONS AND ADVICE

CERT.LV points out that effective cyber hygiene within any organisation plays a key role in combatting both commercially motivated and politically motivated, including Russian, cyber-attacks in the Latvian cyberspace. As a primary solution to combat intrusion attempts and attacks using emails with malicious attachments, such as an attached RDP connection initialization file, CERT.LV stresses the need to configure secure sending and receiving of emails, and recommends configuring devices according to best practices, as well as continuing to promote user education, and preventing system vulnerabilities by keeping up to date with updates.

More information and recommendations are available on the website::
https://cert.lv/lv/2020/05/e-pastu-drosiba-aizsardziba-pret-ienakoso-e-pastu-viltosanu
https://cert.lv/lv/2020/05/e-pastu-drosiba-aizsardziba-pret-izejoso-e-pastu-viltosanu

2.6. Compromised Devices and Data Leaks

During the reporting period, individuals and businesses, as well as national and local authorities, were affected by compromised equipment. The attacks were carried out using emails with malicious attachments from already compromised accounts of colleagues or business partners, as well as weaknesses in the protection of various ICT resources, such as weak passwords and outdated software with vulnerabilities that have been publicly known for years. Routers in small businesses or individual households were also compromised.

Cyber-attacks aim to extract data, manipulate payment information, causing payments to be made to the attackers' bank accounts, or encrypt equipment in order to demand a ransom for data recovery and possibly non-leakage.

Cases have been documented where computer passwords were stored unencrypted, locally on an infected computer, so that if the device were infected, attackers would gain access to multiple user accounts for which two-factor authentication was not 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.

TOP incidents in the reporting period

Several Latvian companies were victims of business email compromise (BEC), in which attackers accessed a company's or business partner's email account to send fake invoices with altered bank details to the parties. CERT.LV encouraged companies to contact their business partner whenever changes are made to financial data, using other communication channels such as a phone call, to ensure that the information is correct.

Signs of Ngrok-related activity were detected in high and medium priority institutions. The software in question is used to provide remote access to infrastructure. Although legitimate, this software is popular among cybercriminals as it allows access to infrastructure by circumventing security measures. In all cases, CERT.LV investigated the incidents.

During the reporting period, CERT.LV received a large number of complaints from individuals and companies about hacked accounts on the Facebook platform. When hacking a Facebook account, fraudsters change not only passwords but also recovery email addresses to make it more difficult for account owners to recover their accounts. CERT.LV recommended that victims promptly report the incident to Facebook Support in order to start the account recovery process.

In November, information was received about an encrypting ransomware attack against a group of companies in the car and motorcycle trade. The ransomware attack encrypted the company's servers and databases, as well as data backups. The data encryption was carried out to extort money – the cybercriminals demanded a ransom in cryptocurrency to unlock the data.

CERT.LV provided the company with the necessary support to help overcome the impact of the incident.

CERT.LV Expert Commentary

When compiling information on compromised websites, it can be observed that unauthorised access to a web server and unauthorised modification of its files are most often carried out through vulnerabilities in CMS and their plug-ins. In addition, there was a trend that websites based on WordPress were more frequently compromised than others. However, this trend is due to the fact that WordPress is the most commonly used CMS. For example, the SocGholish and Balada Injector malware JavaScript injections were detected, which means that the web servers contained files of these malware, so that the websites executed the attackers' code in addition to their own legitimate code.

Attackers have been observed compromising a web server by deploying phishing content or using the web server as a collector of illegally obtained data or as a control server for a phishing campaign. In virtually every case where attackers are able to make unauthorised modifications to a web server, a number of webshell or malicious shell scripts are inserted which allow attackers to control compromised web servers and remotely execute commands through them.

Often, attackers can also access other resources through a vulnerable web server, for example by retrieving databases containing personal data. In some cases, attackers, including politically motivated attackers, have carried out website hacks.

An encryption virus is malware that encrypts files and systems and demands a ransom to recover them (*ransomware*).

SAFETY RECOMMENDATIONS AND ADVICE

To protect an organisation from ransomware, it is important to take precautions such as backing up data securely, using antivirus software, reviewing remote access rights, ensuring that all resources exposed to the external perimeter are maintained at an appropriate security level and avoiding opening suspicious emails or links. Cybersecurity experts never recommend paying a ransom as this does not guarantee a positive outcome. CERT.LV called for multi-factor authentication to be used wherever possible as an important mechanism to protect devices and accounts. Preventive cybersecurity compliance, precautions and preparedness against attacks through well thought out and sensible defence plans are critical.

3. Cyber Threat Prevention

3.1. DNS Firewall: Active Protection

In order to contribute to the overall security of the country and to effectively prevent cyber threats, work continues on the development and promotion of the active protection service DNS Firewall developed by CERT.LV and NIC.LV.

The DNS Firewall is updated daily with malicious domains submitted by Latvian citizens and identified by the CERT.LV team, thus protecting the users of the DNS Firewall from cyber threats. This active protection solution is available free of charge to every Latvian citizen, company and organisationi.

During the reporting period, CERT.LV continued its effective cooperation with electronic communications merchants and companies, such as LMT, Tet. As a result of the cooperation, partners receive a list of harmful domains from CERT.LV using CERT.LV DNS RPZ zone transfer.

DNS Firewall

CERT.LV's active protection service, DNS Firewall, effectively protects every internet user in Latvia free of charge, by protecting their devices from malicious links used in fraudulent campaigns, fraudulent websites, harmful content and various viruses, as well as by ensuring a nationwide uniform processing and distribution of restricted domain zones.

More: https://dnsmuris.lv/

The most significant episodes of active protection in the reporting period:


blocked fake pages received by users in the form of SMS – **751 times;**


blocked user redirection to malicious pages – **5 067 times;**


blocked requests for data scams from fake banking pages – **343 times.**

At the end of the year, the saturated information flow, when online shops run various discount promotions during the November Black Friday or pre-Christmas period, is exploited by fraudsters who create fake copies of online shops' websites to obtain sensitive information from citizens – name, address, password, payment card details, etc. Statistics on the DNS firewall indicate that a large number of fake online shops and virus-spreading websites were also generated every month in Q4 2023.

CERT.LV Expert Commentary

During the reporting period, the DNS Firewall experienced many instances where active protection worked, protecting users from malicious content and devices from being infected – from visiting multiple fake pages, from having payment card details stolen, from visiting fake courier company websites, and by preventing infected devices from communicating with virus control servers. The number and intensity of these types of attacks will increase in the future as technology, the digital environment and cryptocurrencies evolve, and as the opportunities offered by artificial intelligence (AI) are exploited.

In Q4 2023, users of the DNS Firewall (unique) were protected from cyber threats 467 888 times, which is 1046% more than in Q3 2023 and 521% more than in the same period a year ago. The DNS firewall handled around 1.5 million DNS requests each month.

SAFETY RECOMMENDATIONS AND ADVICE

CERT.LV encourages everyone to be vigilant and strongly recommends always verifying the authenticity and recognisability of the link or sender: critically assess the sender's contacts, websites, and recognise untrustworthy attachments in emails and other communication platforms, and immediately inform CERT.LV and the State Police of any incidents.

More information on the key security advantages and benefits of activating the DNS Firewall, as well as easy-to-use instructions for activating it, are available on the CERT.LV website: https://dnsmuris.lv/.

3.2. Sensor Network

The purpose of the EWS or sensor network is to enable authorities to identify threats to their institutions in good time. This is done by analysing a copy of the institution's network traffic using specially designed event rules (*signature*).

On average, the EWS detects 6000 high-priority (high potential threat) incidents per month in national, local and critical infrastructure (CI) institutions.

During the reporting period, CERT.LV continued to maintain and expand the EWS system.

Sensor Network

The Early Warning System (EWS), or sensor network, allows the institutions where it is installed to detect, identify and respond to emerging threats in a timely manner, in addition to providing a more comprehensive view of the threat spectrum in national and local authorities.

Total number of alerts generated by EWS during the reporting period

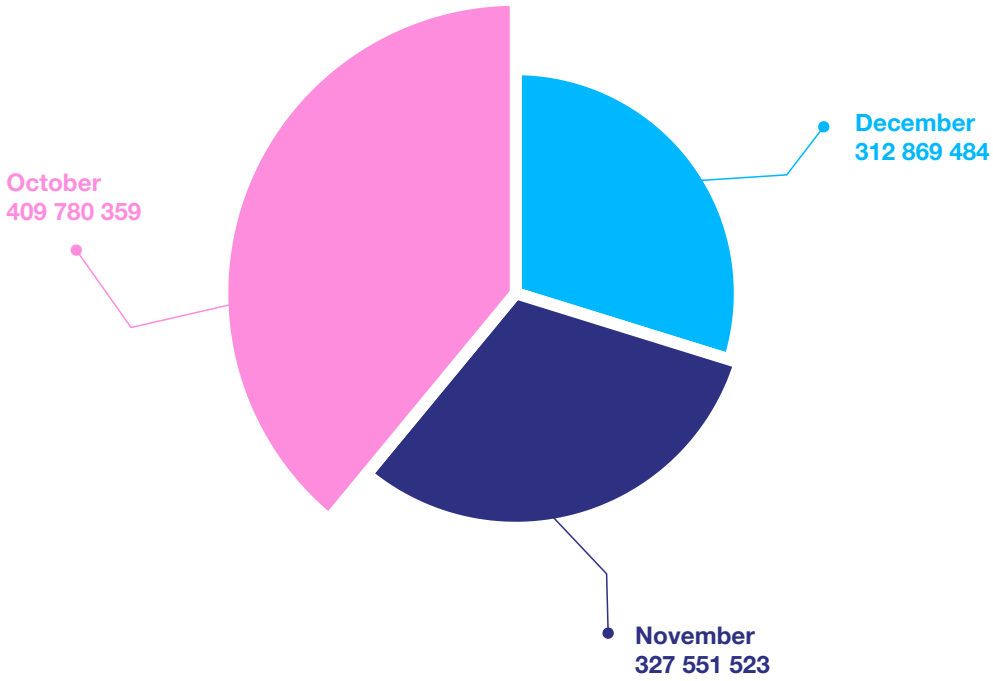


Figure 8 - Number of alerts generated by EWS in Q4 (multiple alerts may be associated with one incident, and some alerts may be unrelated to incidents).

Most identified threats by EWS during the reporting period

Threatsi	October	November	December
Various suspicious activities	7 306	5 392	2 733
Various alerts on APT indicators	1 277	1 869	1 560
Malware related alertsi	213	177	135
Phishing related alerts	2 991	3 033	2 341
Malware related botnet alertsi	99 597	96 192	10 0541
Warnings from public aggregators on signs of compromise	9 171	4 094	3 93
Fraudulent activities	217	519	1 526

3.3. Measures to Prevent Incidents

During the reporting period, *WinRAR* vulnerability alerts and alerts about fake emails distributed on behalf of the *State Security Service* were sent to IT security officers of State and local authorities, as well as to core service providers, digital service providers and critical infrastructure representatives. The alert included indicators of malicious emails and encouraged authorities to restrict access to harmful resources. CERT.LV also encouraged people to report if they had received the fake emails.

Information on newly discovered threats and vulnerabilities is also published on the CERT.LV website and on the X (@certlv) and Facebook (@cert.lv) social network accounts.

3.4. Coordinated Vulnerability Disclosure (CVD)

CERT.LV continued its focused work on the development and promotion of the coordinated vulnerability disclosure reporting platform cvd.cert.lv (CVD), acting as coordinator and facilitator of the coordinated vulnerability disclosure process, as well as developer, maintainer and manager of the platform.

The CVD platform was launched in March 2023. It publishes information on institutions that have voluntarily engaged in a coordinated vulnerability disclosure process and identified resources to be covered by vulnerability reporting. The Platform registers vulnerability reports and the related communication between the parties involved. This reporting practice enables CERT.LV to learn about vulnerabilities in a timely manner and to fully coordinate vulnerability research and remediation, thus more effectively organising measures to protect the security of the Latvian cyberspace.

CVD.CERT.LV

The Coordinated Vulnerability Disclosure (CVD) platform enables a security researcher to log a report of an observed vulnerability, as well as all involved (the institution, the security researcher and CERT.LV) to review the submitted information, communicate with each other and track the progress of the vulnerability remediation.

More: https://cvd.cert.lv/

At the end of the reporting period, the following were registered on cvd.cert.lv:

- security researchers – 37;
- active programmes – 4;
- responsible representatives of institutions/companies – 28.

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

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

Promoting the good practice of coordinated and responsible IT security vulnerability disclosure, during the reporting period CERT.LV specialists continued to promote the CVD platform by addressing the target audience at several outreach events and at the Esi drošs (Be Safe) seminar, as well as by inviting security researchers to report vulnerabilities in services in the CERT.LV domain. In 2024, CERT.LV will continue to invite public administrations to publish their institutional programmes on the platform and security researchers to report discovered vulnerabilities.

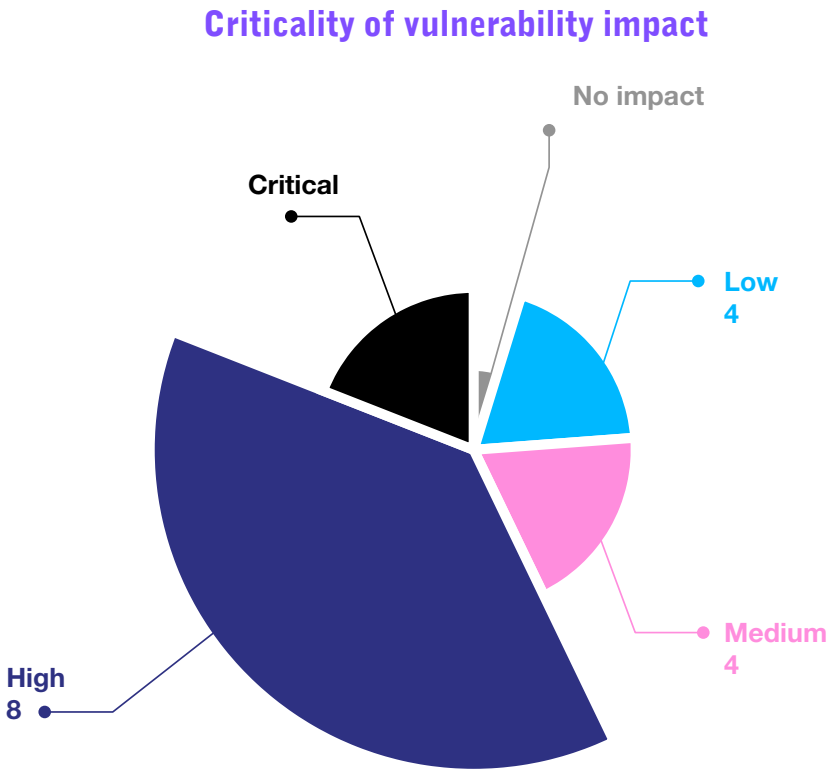


Figure 10 - Criticality of vulnerability impact in Q4

The CVD platform was developed on the basis of the information report "On the Implementation of a Coordinated Vulnerability Disclosure Process in State Administration" prepared by the Ministry of Defence and approved by the Cabinet of Ministers, providing for the possibility for institutions to voluntarily engage in the implementation of a coordinated vulnerability disclosure process in public administration.

4. Communication with the Public

4.1. Training and Educational Events

The CERT.LV team actively worked to educate the public by organising and participating in various thematic seminars, informing about current cybersecurity issues and promoting cyber hygiene best practices. In addition to the usual employee awareness seminars on cybersecurity, several lectures and training sessions were held for employees of institutions and critical infrastructure companies on specific topics selected by the institutions and companies.

In Q4 2023, CERT.LV educated 16 144 participants on IT security through 55 educational events, which is almost 8 times more than in the previous quarter.

Educational Events Organised by CERT.LV for IT Security Specialists

On 4 and 5 October, during European Cybersecurity Month, the **10th** edition of the **international cybersecurity conference CyberChess 2023** took place in Riga. The participants were given the opportunity to hear from world and Baltic cybersecurity professionals in one place, as well as to interact with each other in an informal atmosphere, in order to add to their knowledge and create new and common ideas

Educational and informative events in Q4, 2023

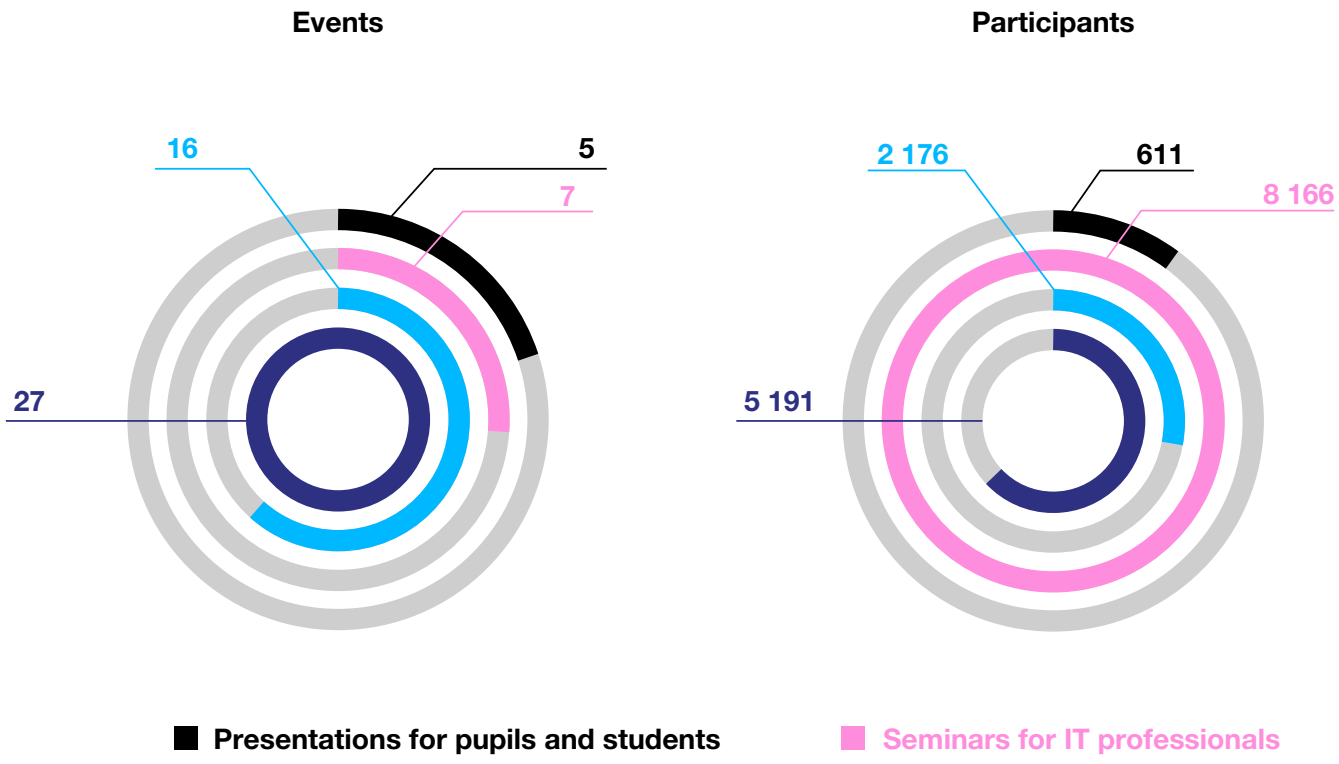


Figure 11 - Number of events and audience reached in Q4, 2023


CyberChess
2023
Cybersecurity Conference
October 4 - 5
Riga, Latvia
CyberChess
2023


through public-private cooperation
Questions: menti.com
Code: 4622 9931
MR. RICHARD BROWNE
MR. INGMĀRS PŪKIS
MR. FLORIAN PENNINGS


2023

in the field of cybersecurity. This year's conference brought together more than 500 participants and experts from 18 countries, while the live webcast attracted around 6000 views from 39 countries. The programme included more than 60 keynote speeches and discussions by local and international experts in three sessions: strategic-political, technical and domain names. A recording of the conference is available at: www.cyberchess.lv.

For the fourth year running alongside the conference, CyberChess 2023 **also hosted Capture The Flag (CTF)**, an online cybersecurity competition that allowed participants to face a variety of cybersecurity challenges in categories such as cryptography, network analysis, forensics, binary code and more. Several technical workshops were organised on the day before the conference, which also gave cybersecurity professionals the opportunity to improve their practical knowledge in areas such as cyber incident investigation, cyber-attack analysis and improving cyber defences.

Tabletop exercises on cybersecurity incident investigation: during the reporting period, CERT.LV experts organised several workshops prior to the annual conference CyberChess 2023. In one of them, a *Cybersecurity Breach Investigation Tabletop Exercise* was played under the guidance of CERT.LV, where participants interactively explore and analyse the course of an attack, what indicators point to an attack and how to get to the culprit. The game has been developed by the *European Union Agency for Cybersecurity (ENISA*) to raise awareness of cybersecurity among non-specialists, and translated and adapted into Latvian by the CERT.LV team. The game was also played at an event organised by the *Ventspils Digital Centre*, as well as at distance learning training for teachers organised by *Riga Technical University*.

On 12 December, CERT.LV organised an **IT security seminar *Esi drošs* (Be Safe)** for IT security officers of State and municipal authorities, key service providers, digital service providers, as well as other interested parties working in the field of IT security. The seminar covered topics such as cybersecurity news for the year, services provided by CERT.LV, establishing a SOC (Security Operations Centre) using open source tools, technological solutions for cybersecurity training, safe use of artificial intelligence, etc. More than 450 participants followed the seminar onlineu. (Recording: https://cert.lv/lv/2023/11/it-drosibas-seminars-esi-dross-decembri)

CERT.LV Presentations on IT Security for Public Education

Key events in Q4

On 26 October, the Baltic Centre for Media Excellence organised the event **Media Literacy Day: Why teach and learn?** as part of UNESCO's Global Media and Information Literacy Week. The event was organised to stimulate discussion, debate and dialogue on the importance of teaching media literacy to young people and to provide teachers and other employees with practical methods for teaching media literacy. CERT.LV participated in the discussion on the need for media literacy, stressing that media literacy is an essential part of everyone's cybersecurity.

On 27 October, CERT.LV Manager Baiba Kaškina took part in a discussion on careers in cybersecurity at **CyberShield 2023**, a forum organised by the Latvian technology company Tet as part of European Cybersecurity Month. The forum brought together local and international cybersecurity experts and industry professionals, providing a comprehensive overview of the latest cybercrime trends, cybersecurity challenges and technologies.

On 1 November, an international conference dedicated to the 30th anniversary of the State Revenue Service (SRS) **"SRS 30. Transformation and Sustainability"** took place, where a CERT.LV expert took part in a discussion on current security challenges.

On 3 November, the Students' Council of the Faculty of Computing of the University of Latvia organised a CTF competition. The aim was to introduce CTF to first-year students from various higher education institutions, as well as other interested parties, and to draw attention to the cybersecurity industry and its topicality in the format of an educational and entertaining competition. Before the competition, CERT.LV representative gave students an overview of cybersecurity and presented the current situation in Latvian cyberspace, as well as talked about the principles of Red Team/Blue Team and discussed aspects of the CTF.

On 23 November, representatives of CERT.LV participated in a **seminar organized by the Ventspils Digital Centre** for entrepreneurs and their employees, where they presented recommendations on how to identify cyber attacks and protect your company and domain name in the digital environment.

4.2. Public Awareness and Promotion of Cyber Hygiene

CERT.LV continued to inform the public about cybersecurity risks, cyber hygiene promotion and best practices, as well as other topical issues in Latvian cyberspace. With 376 media publications, up 47% on the previous quarter, 16.5 million views were generated.

During the reporting period, the current situation in Latvian cyberspace, especially at the end of the year, the threat letters sent to schools and the safe use of mobile apps attracted the most media attention.

CERT.LV also continues to translate and publish the monthly OUCH! (Information Security Newsletter produced by the SANS Institute) on www.esidross.lv.

Articles published at esidross.lv during the reporting period:

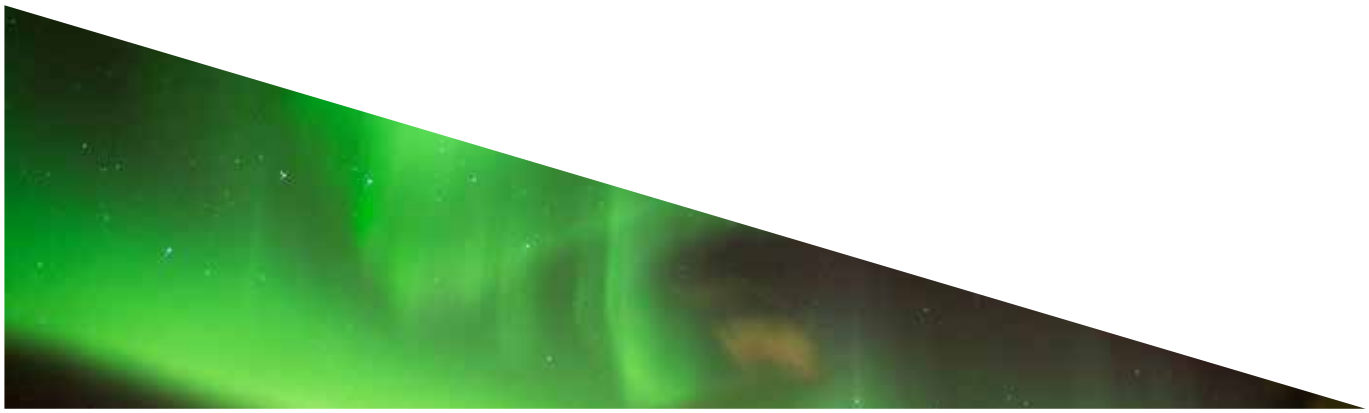
- The Power of the Passphrase. OUCH! 12/2023;
- Safe and smart online shopping: how to avoid scammers' traps?
- 'Black on White' – a single platform for reporting cases of misinformation;
- I'm Hacked, Now What? OUCH! 11/2023;
- The Power of Updating OUCH! 10/2023.

CERT.LV also continued to collect information on major cyber incidents at the end of each month by developing and publishing a report, Cyber Weather, in the News section of the website www.cert.lv.

Cyber Weather Report

CERT.LV offers a monthly overview for cyber weather watchers of the last month's highlights in cyberspace in the TOP 5 categories – scams, malware and vulnerabilities, denial-of-service attacks, intrusions and data leaks, and the Internet of Things.

October: https://cert.lv/lv/2023/11/kiberlaikapstakli-oktobris
November: https://cert.lv/lv/2023/12/kiberlaikapstakli-novembris
December: https://www.cert.lv/lv/2024/01/kiberlaikapstakli-decembris



5. Strategic Cooperation in Latvia

During the reporting period, CERT.LV representatives actively participated in the work of the **National Information Technology Security Council**, which aims to coordinate the planning and implementation of tasks and activities related to information technology security in Latvia.

CERT.LV specialists closely cooperated with the National Armed Forces **Cyber Defence Unit** of the Republic of Latvia, which in the event of an IT security crisis or threat, in cooperation with CERT.LV, could provide support to the state and the private sector. During the reporting period, the most important cooperation took place in the planning of the Locked Shields cybersecurity exercise and in the preparation of the Latvian team for the exercise.

CERT.LV also continued to organise the **Information Technology and Information Systems Security Expert Group (DEG) meetings**, which take place on the second Thursday of every month. The DEG is a voluntary group of Information Technology and Information Systems Security experts with the aim of promoting IT/IS security, fostering a culture of security awareness in the Republic of Latvia and providing support to CERT.LV. The meetings are held to discuss cybersecurity issues and to facilitate the exchange of knowledge and experience among the members of the group.

CERT.LV closely cooperated with the National Cyber Security Policy Coordination Division of the Ministry of Defence, and within its competence actively participated in the implementation of the National Cyber Security Strategy.

Cooperation with the Latvian Internet Association (LIA), which educates the public about potential risks and threats in the internet environment, continues to promote safe internet use and safe internet content (see Chapter 7 for an overview of LIA Safer Internet Centre reports).

5.1. Preventing and Combatting Cybercrime

Cooperation with critical infrastructure (CI) holders

Cooperation with CI holders continues, both in monitoring the situation in cyberspace and in providing advice and support to strengthen the cyber resilience of CIs and to improve cross-sectoral cooperation. CERT.LV actively coordinates the installation of sensors and DNS RPZs in institutions and enterprises to facilitate the faster identification of CI threats and more effective prevention.

Support to Latvian national law enforcement authorities

During the reporting period, CERT.LV provided support to Latvian law enforcement authorities in the investigation of cybercrime incidents, preparing responses to the State Police on several incidents.

In October, when hundreds of Latvian schools and kindergartens received threatening emails about

CERT.LV emphasises the need to continue raising awareness of the Latvian public about cyberspace and the risks of cybercrime in order to strengthen the resilience of society to cyber-attacks, mitigate their impact and contribute to their prevention. Particular attention should be paid to preventive methods and initiatives to block websites created for criminal purposes or used for criminal activities, to the recognition and implementation of these initiatives, and to improving the cooperation between the institutions involved and the speed of response by the responsible authorities.

potential security risks, as well as identical threatening emails distributed to courts and municipalities, CERT.LV teamed up with the State Police to conduct a coordinated investigation and, together with law enforcement authorities, analysed the email and IP addresses and infrastructure used to send the threatening emails.

In addition, comments were provided on IP and email addresses potentially linked to criminal offences, on the use of internet resources, on possible unauthorised access to email and invoice fraud, and an analysis of a phishing site.

Security tests and assessments

In Q4 2023, a total of 7 security tests were carried out, including on a server in a public limited company, on five different resources in an institution, and on an institution's website.

Reports on the results of the tests were provided to the resource holders and recommendations were made to remedy the deficiencies.

Also, during the reporting period, 8 (4 initial and 4 resubmissions) applications for the evaluation of the State Information Systems (SIS) were received, of which three were agreed and five were given recommendations before resubmission.

Threat hunting

During the reporting period, threat hunting operations aimed at safeguarding the Latvian Critical Infrastructure, continued in close cooperation with the Cyber Command of the Canadian Armed Forces. CERT.LV specialists also continued to work on the development and improvement of threat hunting methodological materials and the organisation of experience exchange events.

The CERT.LV team is a leader in organising and conducting threat hunting operations in the European Union, contributing to NATO's collective defence of Europe, promoting the application of international norms in cyberspace and building a trusted circle of allies capable of both mutual support in cyber threat assessment and the rapid exchange of information and best practices.

Cooperation events, meetings and consultations in the field of cybersecurity

- Active involvement in the Central Election Commission's (CEC) Election Working Group, providing recommendations for the development and maintenance of secure electoral systems. CERT.LV experts regularly participated in the meetings of the Election IT Working Group, providing recommendations on security aspects of systems and testing. CERT.LV also provided its perspective on IT risks to the CEC in the context of securing the 2024 European Parliament elections.
- Involvement in the work of the Inter-institutional Working Group led by the National Coordination Centre, which aims to facilitate the exchange of information between public administrations and organisations on activities and measures in different areas of cybersecurity in order to promote efficiency and cooperation.
- During the reporting period, draft laws/initiatives were examined, including 9 European Union and 8 Latvian draft laws, as well as meetings with Latvian drafters to discuss specific issues or comments.

5.2. CERT.LV Support to the DDUK Secretariat

CERT.LV actively participates in the work of the Digital Security Monitoring Committee (DDUK), providing daily support in the monitoring of qualified electronic identification service providers and trusted certification service providers.

5.3. Education and Improvement of Youth Cyber Skills

CERT.LV participates in the working group organised by the Saldus Technical School administration for the development of the standard for the qualification “Cybersecurity Technician”, sharing its experience and providing its vision on the knowledge, skills and competences required by specialists to ensure that the holders of the qualification are in demand and highly valued specialists in the labour market.

The European Union Cyber Security Division of the Ministry of Defence organises the Latvian national selection of the European Cyber Security Challenge 2024 (ECSC), a pan-European cybersecurity competition for young people. To ensure the successful participation of the Latvian team in the ECSC, the involvement of members of the cybersecurity competence community, in particular universities and private sector companies, in the practical organisation and support of the national selection, is essential.

CERT.LV provides support in the development of the ECSC national selection website, as well as in the preparation of the infrastructure and task set required for the national selection.

6. International Cooperation

During the reporting period, CERT.LV continued to represent Latvia's interests and strengthen cooperation with other countries' cybersecurity incident response teams and international organisations. CERT.LV employees also provided their vision and input to various working groups, sharing experience and best practices, providing advice and support, as well as making presentations at international conferences and seminars. Employees also continued to learn new skills and improve their qualifications through international training.

Cooperation with the CSIRTs network, ENISA, European Union institutions and NATO

CERT.LV regularly participates in the network meetings of the NIS (Network and Information Security) directive CSIRTs Network. The work of the CSIRTs Network is coordinated by ENISA, the European Union Agency for Cybersecurity, which contributes to EU policy on cybersecurity.

During the reporting period, CERT.LV participated in the CSIRTs Network Maturity Working Group, which is dedicated to improving the maturity level of EU Member States' CSIRTs Network teams.

CERT.LV experts also continued to actively participate in working groups organised by ENISA:

- ***Coordinated Vulnerability Disclosure (CVD) Task Force*** – work is underway on the development of EU-level guidelines for a coordinated vulnerability disclosure policy;
- ***EU Cybersecurity Index*** – a methodology for calculating the value of the cybersecurity index is being developed to assess the cybersecurity of Member States. During the reporting period, after testing an initial prototype, the Working Group continued to develop the EU Cybersecurity Index platform;
- ***CSIRT Services Framework*** – continued work on developing a common framework for roles, competencies and skills of CERT team members. During the reporting period, the development of a methodology for defining the types of CERT teams was carried out, which would facilitate the identification of roles and competences required for the tasks to be performed.

CSIRTs Network

The network of Computer Security Incident Response Teams of the Member States of the European Union ensures cooperation between cybersecurity incident response teams in the European Union. The Network meetings take place three times a year and at the moment are organised by the country holding the Presidency of the Council of the European Union in cooperation with ENISA. Joint sessions with the NIS Directive Cooperation Group CyCLONe also take place once a year.

More:
https://csirtsnetwork.eu/
https://www.enisa.europa.eu/topics/incident-response/cyclone

CSIRT Network Situation Update **sanāksmes:** regular participation in meetings aimed at exchanging information on current developments in cyberspace between CSIRT Network members continued during the reporting period.

European Commission EHDS (European Health Data Space) Regulation Working Group: CERT.LV experts contributed to a working group aimed at promoting the availability of electronic patient data and cooperation between stakeholders at the European level. During the reporting period, the working group assessed the Regulation's relationship with the Artificial Intelligence Act, the Data Governance Act and the GDPR.

Regular participation of CERT.LV experts in the European Cybersecurity Certification Group (ECCG) meetings, including the EU Certification Week in Malaga, Spain, from 20 to 23 November, representing Latvian interests and providing their vision on the future EU Cloud Certification Scheme project, as well as on other issues regarding the implementation of ICT product cybersecurity certification in EU countries.

ENISA-organised training CYBER EUROPE 2024: CERT.LV experts participated in the final planning conference of the training, which took place during the reporting period from 13 to 15 November in Athens, Greece. During the

final conference, Member States not only agreed on technical and operational level incidents but also decided to test international cooperation within the CSIRT Network and CyCLONe (European Cyber Crisis Liaison Organisation Network).

NATO exercise CYBER COALITION: from 27 November to 1 December 2023, CERT.LV experts participated in the NATO exercise CYBER COALITION 2023, which took place online and included both technical and procedural exercises. The main objectives of the 2023 exercise were to enhance Allies' resilience to cyber-attacks and their ability to conduct joint response operations in cyberspace.

NATO CYBER COALITION

The largest annual collective cybersecurity exercise organised by NATO, which is one of the largest in the world. It aims to improve cooperation and coordination in the field of cybersecurity among Allies.

Cooperation within FIRST

Regular participation in the FIRST Membership Committee meetings continued to discuss future rules for membership and recruitment, as well as the use of the SIM3 model.

CERT.LV Manager Baiba Kaškina, who continues to serve as Chair of the FIRST Membership Committee, participated in the review of new member applications and contributed to improving the membership application process.

FIRST

Cybersecurity organisation bringing together CERTs, CSIRTs, PSIRTs, SOC teams and other cybersecurity professionals from around the world. At the beginning of 2024, FIRST has members from 106 countries.

Cooperation within TF-CSIRT

CERT.LV has been a certified *Trusted Introducer* team since 1 September 2016.

During the reporting period, CERT.LV is one of 47 TF-CSIRT/Trusted Introducer certified teams in Europe (there are 495 teams in the community), which confirms the high level of maturity and preparedness of the CERT.LV team.

To maintain the certification, a re-certification process is required every three years. On 28 October 2022, at the TF-CSIRT meeting in Vilnius, Lithuania, it was announced that CERT.LV has been successfully re-certified for the next 3 years (accordingly, the next re-certification process is planned for 2025).

The certification is based on SIM3: Security Incident Management Maturity Model approach, which assesses the maturity of an organisation by looking at organisational, human resources, technical tools and processes used and their application to ensure the quality of the organisation's operations, primarily assessing the maturity of the incident handling process.

TF-CSIRT/Trusted Introducer

TF-CSIRT is the organisation for CERTs in the European region, bringing together incident response teams from all sectors. The Trusted Introducer service maintains a trusted register of CERTs and accredits and certifies teams according to their demonstrated level of maturity.

During the reporting period, CERT.LV continued its work in several TF-CSIRT working groups.

Implementation of the Joint Threat Analysis Network project

The CERT.LV team continued its work on the implementation of the Joint Threat Analysis Network project (hereinafter – JTAN project).

The leading partner of the project is CERT.PL, the Polish Information Technology Security Incident Response Team,

Implementation of the Joint Threat Analysis Network

The overall objective of the project is to create a Joint Threat Analysis Network. The network would be open to a European CSIRT cooperation group focusing on the exchange and analysis of technical, operational and strategic threat intelligence.

which operates within the Naukowa i Akademicka Sieć Komputerowa (NASK) institute. Partners from Austria, France, Estonia, Luxembourg, Romania and Slovakia are also participating in the JTAN project.

In Q4 2023, CERT.LV continued the development of the Graphoscope solution as planned. During the reporting period, CERT.LV allocated additional resources to the implementation of the project, and participated in monthly remote JTAN project meetings, where project partners are briefed on individual project tasks and results.

Graphoscope

A tool designed to correlate data from different data sources and display them in a visual form.

Key features of Graphoscope:

- support for multiple data sources and easy system setup;
- a web-based interface that does not depend on pre-installed databases;
- the interface provides flexible filters to facilitate the analysis of large volumes of data.

According to the contract with the European Commission No. INEA/CEF/ICT/A2020/2373165, which was approved and launched on 1 July 2021 under the *2020 CEF Telecom Call – Cybersecurity*, the implementation of the JTAN project will continue until 30 June 2024.

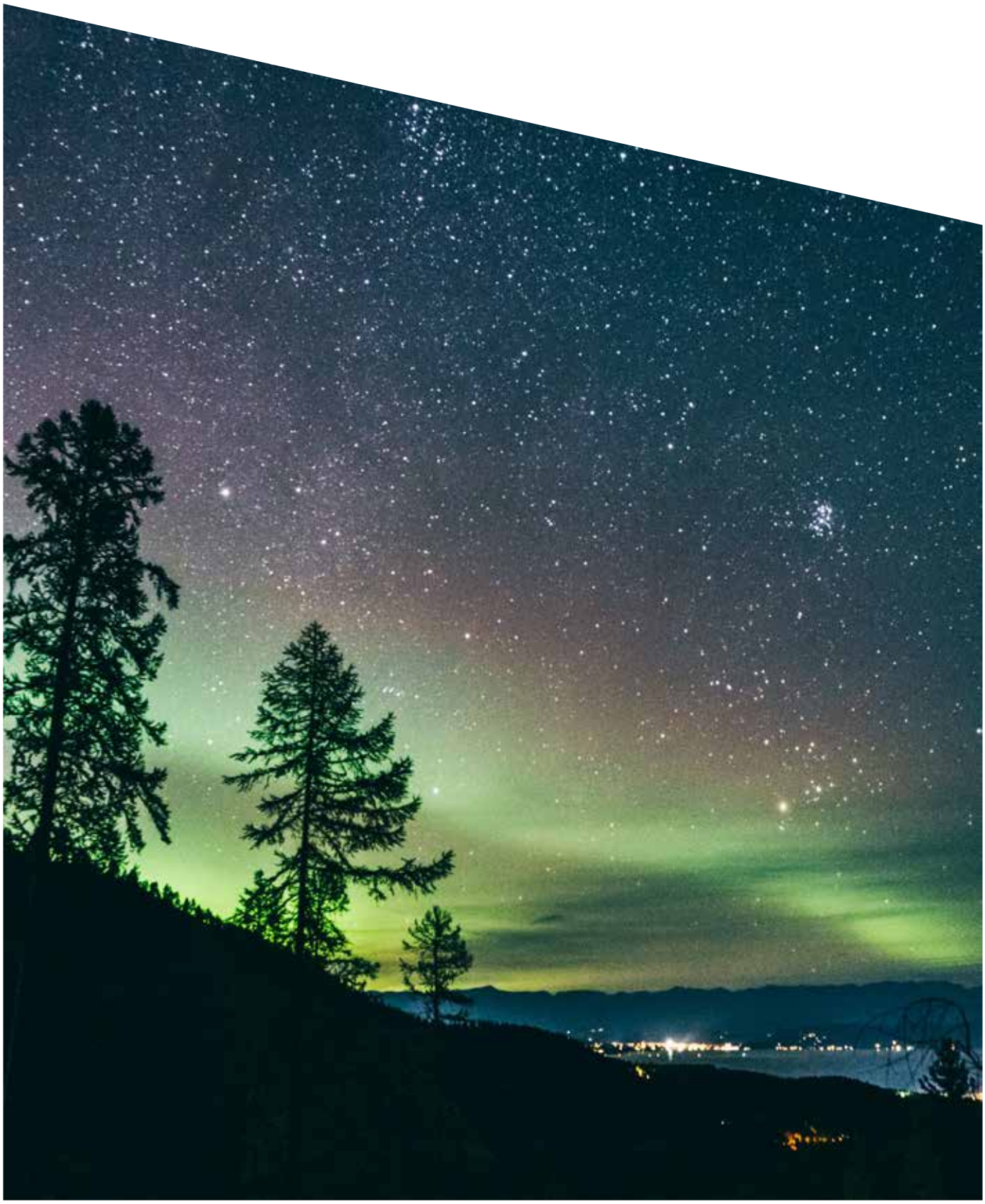
Other international activities

During the reporting period, CERT.LV representatives participated in several international conferences and seminars, as well as hosted several foreign delegations and participated in meetings with representatives of foreign delegations in Latvia. Key activities:

- **On 5 October,** as part of European Cybersecurity Month, an informal meeting of the European Cybersecurity Competence Centre (ECCC) National Coordination Centres (NCCs) was held in Riga, where its leaders and experts from six EU Member States – Latvia, Estonia, Lithuania, Luxembourg, Finland and Sweden – shared their experience on issues related to the implementation of cybersecurity projects. It is planned that such meetings will be held in the future, both in Latvia and in other EU Member States. The functions of the Latvian National Coordination Centre (NCC-LV) are implemented by the Ministry of Defence in cooperation with CERT.LV and the Central Finance and Contracting Agency.
- **From 28 October to 4 November,** a CERT.LV representative participated in the RISE South Korea conference with the presentation Heated Cyberspace in Latvia 2022–2023, as well as visited the South Korean national CERT KrCERT/CC. The conference was attended by about 120 participantsi.
- **From 8 to 10 November,** Riga hosted representatives of cybersecurity organisations from Kosovo and Macedonia. During the meeting, the CERT.LV team, together with colleagues from the Ministry of Defence and the National Armed Forces Cyber Defence Unit, presented the Latvian cybersecurity ecosystem, CERT.LV activities and shared their experience and best practices on strengthening national cybersecurity. The visit was organised by *DCAF (Geneva Centre for Security Sector Governance*).
- **From 12 to 22 November,** a CERT.LV representative participated in two international workshops to promote cybersecurity capacity building in different regions. One of them was CSIRT Technical and Operational Development in Latin America and the Caribbean, held in the Dominican Republic. At the workshops, a CERT.LV representative spoke about aspects of coordinated vulnerability reporting, CERT.LV's practices and approach in this area, as well as the overall situation in the Latvian cyberspace. The second workshop, Workshop on the International Legal Framework for Cybersecurity and EU Cybersecurity Law, was held in Montenegro, where the CERT.LV representative participated in discussions on both the implementation of good governance principles and the opportunities for effective cooperation between the private and public sectors in the field of cybersecurity.

Regular participation of CERT.LV experts in monthly meetings of the EU CyberNet project. The project aims to strengthen and develop cybersecurity expertise not only within the EU, but also beyond its borders (www.eucybernet.eu). Participation in the project provides an opportunity for CERT.LV experts to engage in various projects, strengthening their knowledge and capacity.

Regular participation of CERT.LV employees in the coordination of the Nordic-Baltic SOC (Nordic-Baltic Security Operations Centre).



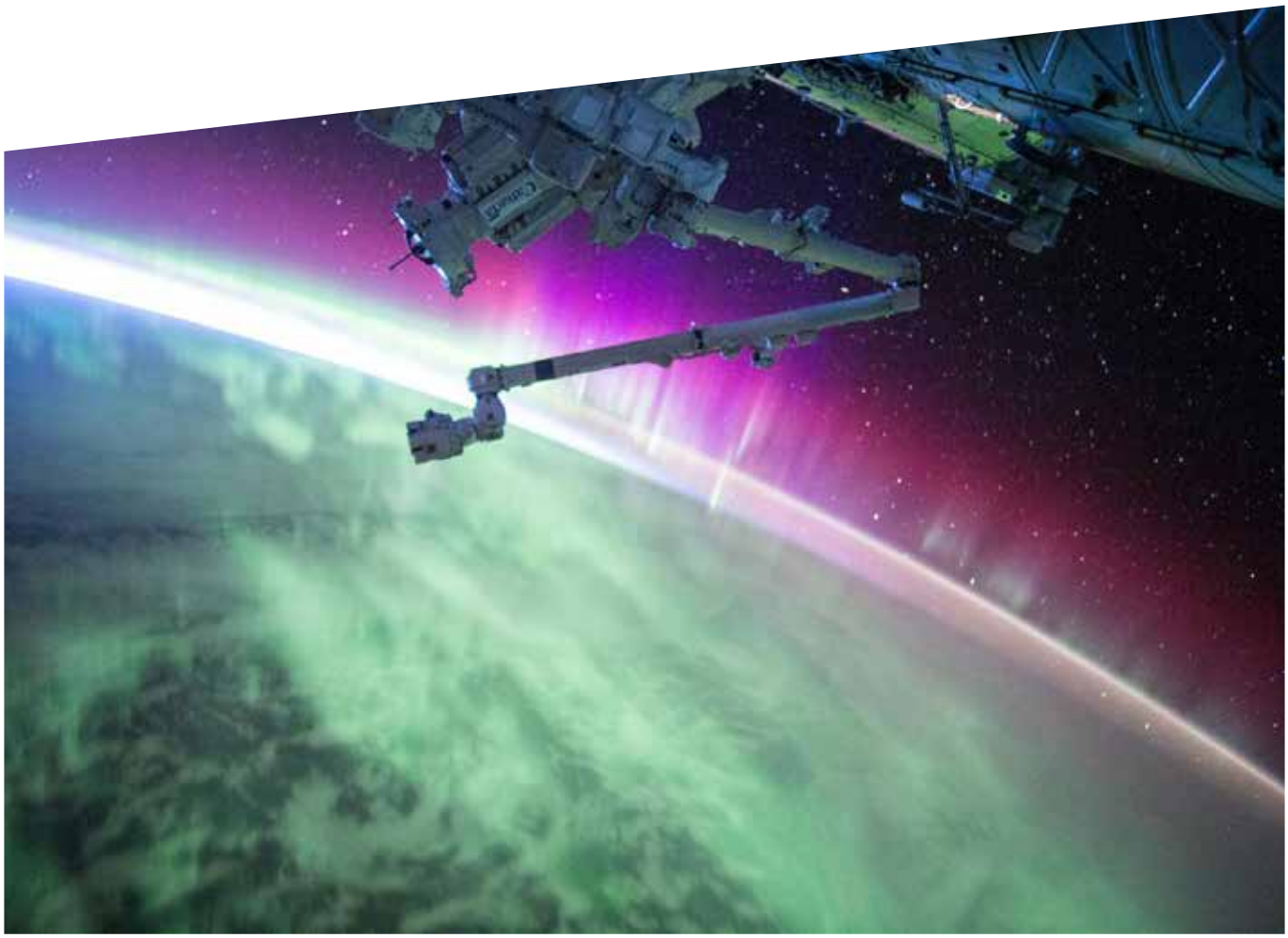
7. LIA Safer Internet Centre Report

The Latvian Internet Association Safer Internet Centre Report Line (RL) has received and evaluated 487 reports between 01.10.2023 and 31.12.2023. Of these, 195 reports contained child sexual abuse material, 8 reports contained pornography without an age restriction warning, 35 reports contained defamation and slander, 11 reports contained hate speech and 4 reports contained violent material.

There were 124 reports of attempted financial fraud on the internet, 54 of which were not illegal in content, and 56 of which resulted in recommendations to whistleblowers to resolve the problem.

80 reports of hate speech and child sexual abuse material hosted on servers in Latvia were sent to the National Police. 120 reports of child sexual abuse material originating outside Latvia have been entered into the INHOPE Association's database and submitted to the relevant INHOPE country reporting line for follow-up action to remove illegal content from the public domain.

During the reporting period, of the 71 reports of child sexual abuse material maintained in Latvia, 70 have been deleted from public circulation and 1 is in the process of deletion in cooperation with the State Police and electronic communications companies.



8. Events Planned for the Next Quarter

The CERT.LV team will continue to effectively monitor the situation in cyberspace, coordinate and resolve incidents, as well as inform and educate the public, developing and strengthening strategic cooperation not only at the national but also at the international level.

By maintaining active cooperation with state and local government institutions, electronic communications companies and other organisations and partners, CERT.LV will continue its work in addressing and supporting incidents of varying severity. It will also organise meetings, consultations and presentations, providing professional support to State and local authorities in safeguarding national cybersecurity.

In order to define the priority areas of CERT.LV activities for 2024, the following main events and activities are planned for Q1:

Development and promotion of services

CERT.LV will continue its focused work on the development and promotion of the active protection service – DNS Firewall, the development of new active protection services, as well as the improvement and development of Sensor Network services for the detection of a common and sectoral threat level, providing maximum benefit to national security from the processed information.

Also, in Q1, targeted activities will be launched to establish and develop Security Operations Centres (SOCs), or CERT.LV, as part of a comprehensive, centralised model for strengthening cybersecurity in the country.

In order to facilitate the identification of vulnerabilities in the ICT resources of Latvian State and local government institutions and their reporting on the vulnerability reporting platform (cvd.cert.lv.), it is planned to address representatives of institutions registered on the platform and encourage them to register their programmes with resources to be tested, as well as to create a rating table for security researchers.

Continuation of threat hunting operations

CERT.LV will continue to strengthen its role as a leader in organising and conducting threat hunting operations in the European Union. Developing and strengthening strategic cooperation not only at the national but also at international level, contributing to NATO's collective European defence, developing and improving threat hunting methodologies, and organising experience sharing events with partner organisations in allied countries.

Promoting the visibility and reputation of CERT.LV's technical authority

CERT.LV experts will continue to regularly inform decision-makers about developments in the Latvian cyberspace. By providing information to the public and giving the opportunity to look back at the most important events in cyberspace in the TOP5 categories, CERT.LV will publish a monthly Cyber Weather Report on its website.

CERT.LV experts will continue to promote and organise Cybersecurity Tabletop Exercises. Mock exercises with companies and organisations in the financial, health, education and public services sectors are planned for Q1. CERT.LV experts will also offer tailor-made exercises, which discuss the most relevant issues, examples of cyber-attacks, procedures or areas of responsibility according to the client's needs, followed by a summary and recommendations.

Participation of CERT.LV experts in cybersecurity community events is planned, as well as regular and effective messaging with the cybersecurity community to raise public awareness of cybersecurity and cyber hygiene aspects.

- In March, CERT.LV plans to organise the annual IT security seminar Esi drošs (Be Safe) for IT security officers of State and local authorities, as well as for other interested parties.

- CERT.LV is an associate partner of the NCC-LV project implemented by the Ministry of Defence (MoD). CERT.LV will implement the tasks assigned within the project framework (e.g., Cybersecurity Challenge, conference CyberChess 2024), actively participate in the work of the Latvian cybersecurity community established by NCC-LV and provide support for the implementation of the MoD project activities.

Developing and promoting international cooperation

CERT.LV experts will continue to represent Latvia's interests and strengthen cooperation with other countries' cybersecurity incident response teams and international organisations by providing advice and support, making presentations at conferences and sharing experience.

- The 22nd CSIRTs Network Meeting of the NIS Directive will take place in Brussels, Belgium from 16 to 17 January, where CERT.LV experts will share their expertise and experience, ensuring effective information exchange and cooperation with the CSIRTs Network community.

- From 26 February to 1 March, CERT.LV cybersecurity experts will present Prototyping a Network Intrusion Detection System: A Deep Dive into CERT.LV's IACS Lab for Safeguarding Critical Infrastructures and Defending From the Beast in the East – Multinational Threat Hunting Operations at the Open Cyber Security Conference in Spain.

Implementation of the NIS2 Directive in Latvia

In support of the objectives of the Cybersecurity Governance Reform, work will be invested in the clarification of new legislation and the preparation of guidance to support CERT.LV's clientele in the implementation of the new requirements.

15 January 2024

CERT.LV mission is to promote information technology (IT) securityin Latvia.

Main objectives of CERT.LV are: to update information about IT security threats; to provide support to state institutions regarding national IT security; to provide support regarding IT security incidents to every private end user or legal entity, if the incident involves a Latvian IP address or .LV domain; to conduct research, orgnaize educational events and trainings in the field of information technologies security.

Contact CERT.LV:

Telephone: +371 67085888

E-mail: cert@cert.lv

Web: www.cert.lv

Follow CERT.LV:

www.twitter.com/certlv

www.facebook.com/certlv

© CERT.LV, 2024

CERT.LV
Information Technologies
Security Incident
Response Institution