CERT.LV ACTIVITY REPORT

Q3 2024

CERT.LV
Cyber Incident Response Institution

Institute of Mathematics and Computer Science University of Latvia

Ministry of Defence Republic of Latvia

The Activity Report for Q3 2024 contains publicly available information and does not include information about CERT.LV activities that contain classified information. The report is for informational purposes only.

Contents

Summary

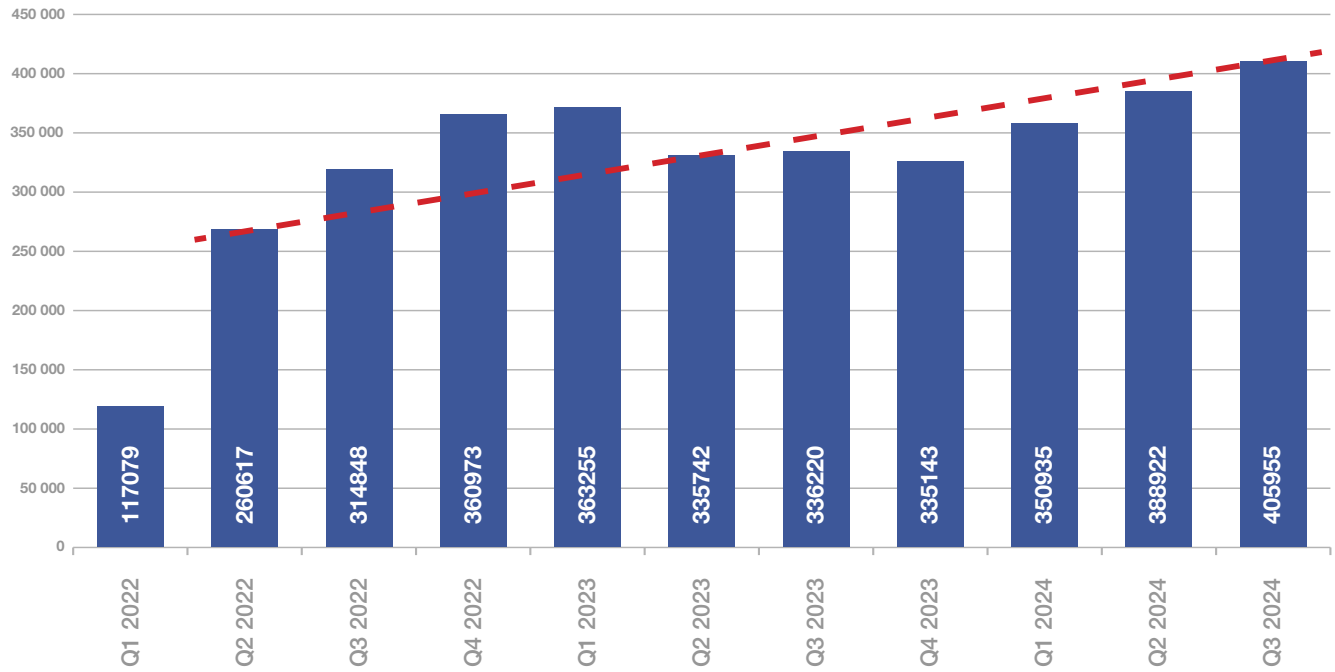
Geopolitical and ideological conflicts continue to be strong drivers of cyber attacks. Since the Russian invasion of Ukraine, the level of cyber threats in Latvia has increased significantly. The support of Latvia to Ukraine and the continuation of Russian aggression means that a high cyber threat dynamic is maintained, which underlines the need for constant vigilance and improved defence solutions.

Since the beginning of 2022, public and private sector organisations have been reporting incidents and vulnerabilities more frequently and requesting support from CERT.LV more often, reflecting an increasing level of trust between public and private sector organisations.

The historically high level of 405 955 unique IP addresses being compromised indicates a significant increase in cyber threats and activity.

In Q3 2024, the number of reports recorded increased by 4.4% compared to the previous quarter and by 21% compared to the same period last year. Latvia demonstrates a high level of cyber resilience.

Cyber threat dynamics by quarter

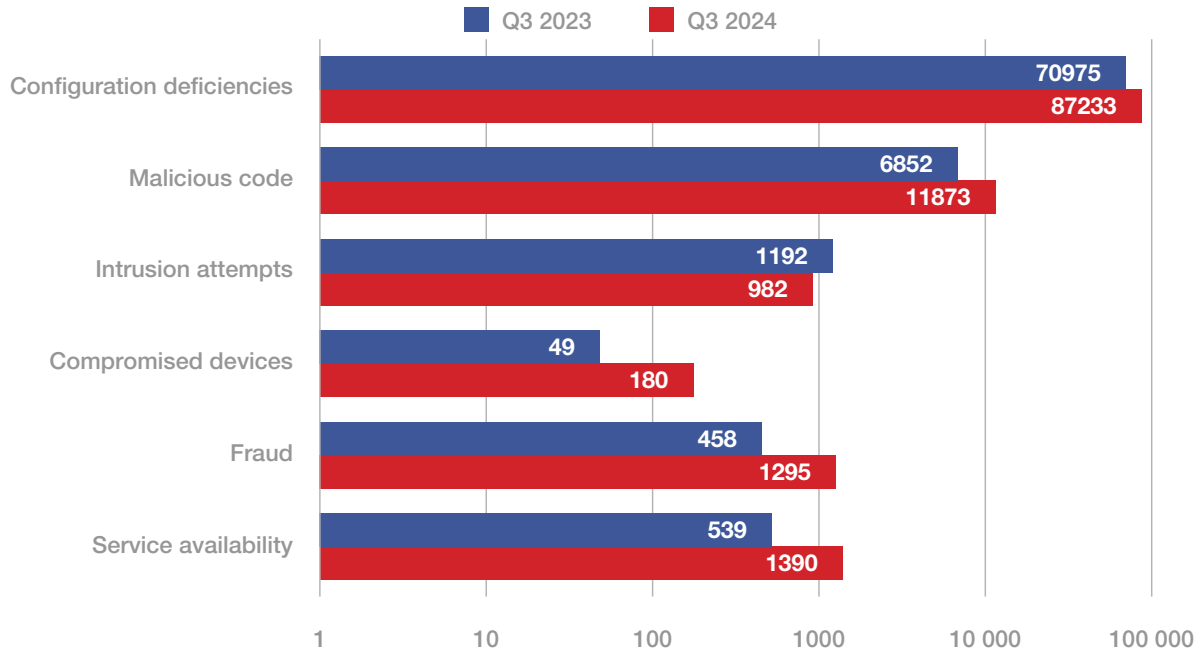


In Q3 2024, the most common types of threats were configuration deficiencies, malicious code, service availability and fraud.

Compared to the same period a year ago, only the number of intrusion attempts decreased in the reporting period, while the following threat types showed the largest increase:

- compromised devices (+267%),
- fraud (+183%),
- service availability (+158%),
- malicious code (+73%).

Breakdown of threats by type*



*Comparison of the number of unique IP addresses compromised in Q3 2023 and Q3 2024 by threat type. The graph excludes IP addresses with threat types "Other", "Information security", "Harmful content", "Information gathering".

The trend of the development of cyber threats in the future remains high. CERT.LV is actively monitoring the situation and the potential threats.

CERT.LV services to public and private sector organisations are expanding. From 1 September 2024, with the entry into force of the National Cybersecurity Law (NCSL) in Latvia, the cyber incident response body CERT.LV will become part of the National Cybersecurity Centre. The NCSL extends the scope of the law to a wider range of organisations, thus increasing the number of CERT.LV constituents who have to comply with the new requirements but can also receive the services offered by CERT.LV. As the main operational cyber security organisation in Latvia, CERT.LV offers a wide range of services to strengthen cyber resilience: https://cert.lv/lv/pakalpojumi

1. Top cybersecurity threats in Latvia: statistics and trends

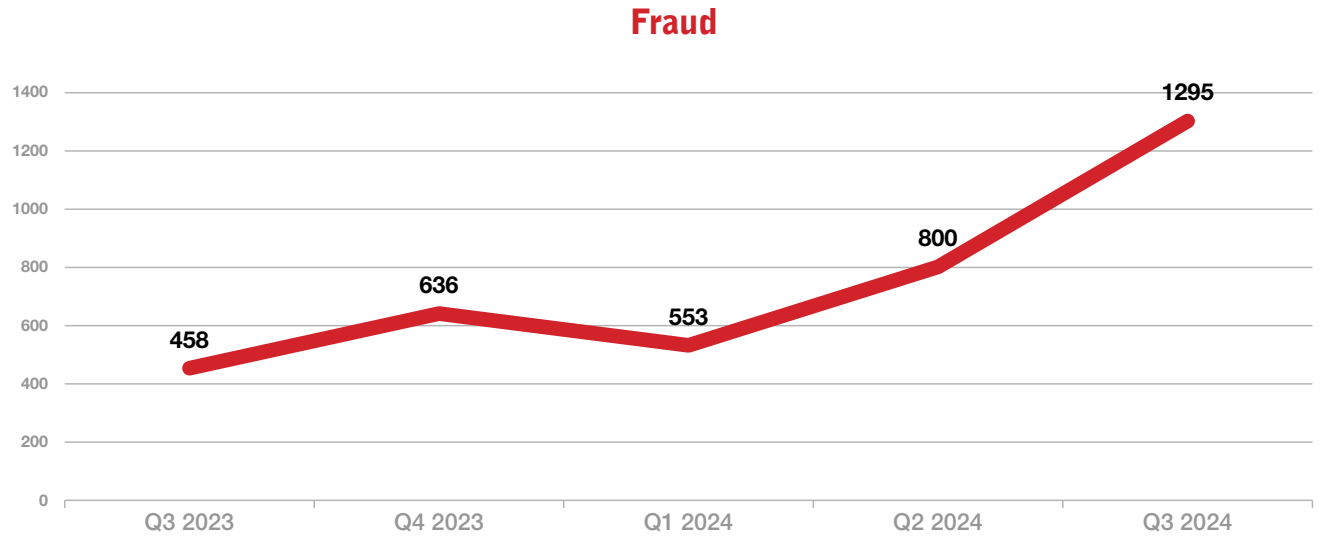
Cybersecurity threats by importance and impact

During the reporting period, 3 high-profile cyber-attacks on public institutions were recorded, but they did not have any lasting impact on society. Significant threats with a broad impact on the commercial sector, State and local government authorities account for 0.23% or 926 compromised unique IP addresses of all categorised threats. This is 13 times more than in Q2 and 27 times more than a year ago. Significant threats with a medium impact account for 0.61% or 2466 unique IP addresses being compromised. The increase compared to the previous quarter is 2%, and compared to Q3 last year, the increase is 9%.

Social engineering-based fraud is on the rise

The number of compromised unique IP addresses registered by CERT.LV has increased by 62% compared to the previous quarter and by 183% compared to Q3 last year. This indicates increased cyber activity and greater risk for internet users. To mitigate the risk, it is important to continue educating the public and promoting good cyber hygiene practices.

Manipulative measures to extract data and compromise integrity are becoming more sophisticated. The most common schemes are phishing, smishing, targeted phishing, compromising email correspondence, fake calls involving imitation of the human voice, fake websites and profiles on social networks to distribute fake lotteries and surveys, etc. Scams in the Latvian language are on the rise. Messages are sent on behalf of public authorities, couriers and financial service providers. Often people are scammed due to carelessness and poor cyber hygiene practices, since this increases the risks of fraud.

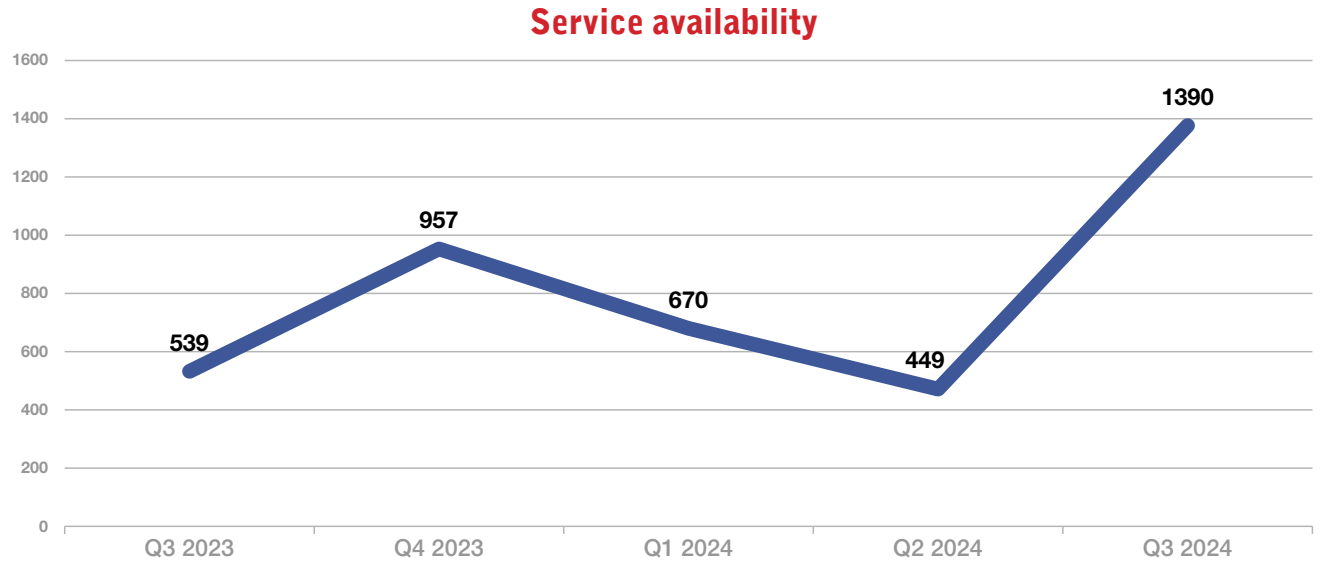


Fraud tactics are sophisticated but preventive measures are simple: start with a secure password manager, two-factor authentication (2FA), regular updates and a DNS firewall. And always treat suspicious calls, emails and messages with caution. Think critically about every request to share your personal information. Stay vigilant and be responsible regarding digital security and your activities online!

Politically motivated service attacks

The 210% increase in the number of compromised unique IP addresses recorded by CERT.LV compared to the previous quarter and the 158% increase compared to Q3 last year shows a significant increase in the number and intensity of service attacks.

Latvia continues to face a high cyber threat from Russia and hacktivists supporting Russia. DDoS attacks against Latvia continue, targeting public authorities, critical ICT infrastructure and service providers.



The Russian-sponsored cyber-attacks in Latvia are primarily aimed at undermining support for Ukraine and strengthening national security by provoking a clash of ideological values caused by the conflict between Ukraine and Russia in the geopolitical environment.

In July 2024, a statement by Latvian President Edgars Rinkēvičs to the media from the NATO summit in Washington about Western arms supplies to Ukraine sparked a wide discussion in hacktivist groups on the Telegram. On 12 July, widespread denial-of-access attacks were carried out against electronic communications companies. The number of requests was up to 200 times higher than normal, causing temporary disruptions to websites. The cyber-attacks were mainly prevented by geo-blocking.

In the second half of August 2024, intensive and tailored DDoS attacks were observed at the national level against internet resources in the public and transport sector, as well as against some resources in the private sector. As a result of the attacks, some resources experienced disruptions – slowness or, in some cases, intermittent unavailability. Overall, the attacks are considered to be significant. Information obtained from the Latvian State Radio and Television Centre shows that the attackers profiled the performance of the sites and adjusted the parameters of the attacks to target certain functionalities of the pages. Cyber attackers dynamically adapted and activated new attack sources. Attacks with different targets and intensities continued throughout the week. The reason for these attacks can be linked to the Latvian aid package to Ukraine, which was approved on 13 August – the transfer of 30 equipped vehicles to Ukraine.

Overall, the situation in the Latvian cyberspace remains stable; CERT.LV, in cooperation with partners, continues to actively monitor the security of cyberspace, centralised DDoS protection solution has been reinforced further. CERT.LV stresses the need for system maintainers to be vigilant and proactive in their targeted efforts to strengthen cybersecurity management and resilience, as the number of attempted cyber-attacks is continually on the rise.

Vulnerabilities and configuration deficiencies

CERT.LV regularly performs comprehensive monitoring, studying the CVE (Common Vulnerabilities and Exposures) landscape, which can be linked to exposed services/facilities.

In Q3 2024, CERT.LV proactively distributed alerts to users on 16 newly discovered critical CVE vulnerabilities, providing coordinated guidance on updates and installation.

According to the FIRST CVSS methodology, vulnerabilities with a score between 9.0 and 10 are the most critical ones, indicating that they have high exploitation potential and pose significant risks to systems and data. Many are related to web vulnerabilities, which are often a prime target for attackers seeking unauthorised access.

The use of vulnerabilities in web management systems, firewalls, VPNs and routers is an ongoing trend. Misconfigured services continue to pose significant risks.

It is important to patch vulnerabilities rated as 'high' or 'critical' immediately to protect the organisation from potential attacks. In many cases, vulnerabilities that fall into these categories can be a more accessible entry point for attackers looking to hack into systems and gain access to data. Such attacks can cause financial losses, damage an organisation's reputation, or even result in fines. However, vulnerabilities with lower scores should not be ignored as they often serve as a foothold in the latter stages of a cyber-attack.

Challenges can also be caused by a faulty software update, as was the case on 19 July 2024 when many users around the world experienced problems with the Windows operating system. This was caused by a buggy update to the CrowdStrike anti-virus software, which knocked out more than 8.5 million computers. The IT disruption affected airports, rail and healthcare industries, hotels, media, banks and many other organisations around the world. CrowdStrike software is not widely used in Latvia, so the impact was minimal. CERT.LV experts recommend that you always check for updates before installing them.

Effective and prioritised vulnerability patching can prevent a large number of incidents, or at least make them significantly more difficult to execute.

They still account for the majority of all the threats in Latvian cyberspace recorded by CERT.LV. In addition, the number of attacks continues to grow, showing an upward trend and reaching the highest level in the last two years – 87 233 compromised unique IP addresses. The majority of cyber-attacks are still carried out using publicly known vulnerabilities, so early identification and patching of configuration deficiencies can significantly improve the cybersecurity situation.

Cyber attackers target the easiest targets first, so don't put off security updates. CERT.LV encourages following the instructions of the developers to promptly update the software and operating systems to the latest available version. All current alerts are also posted by CERT.LV online on www.cert.lv.

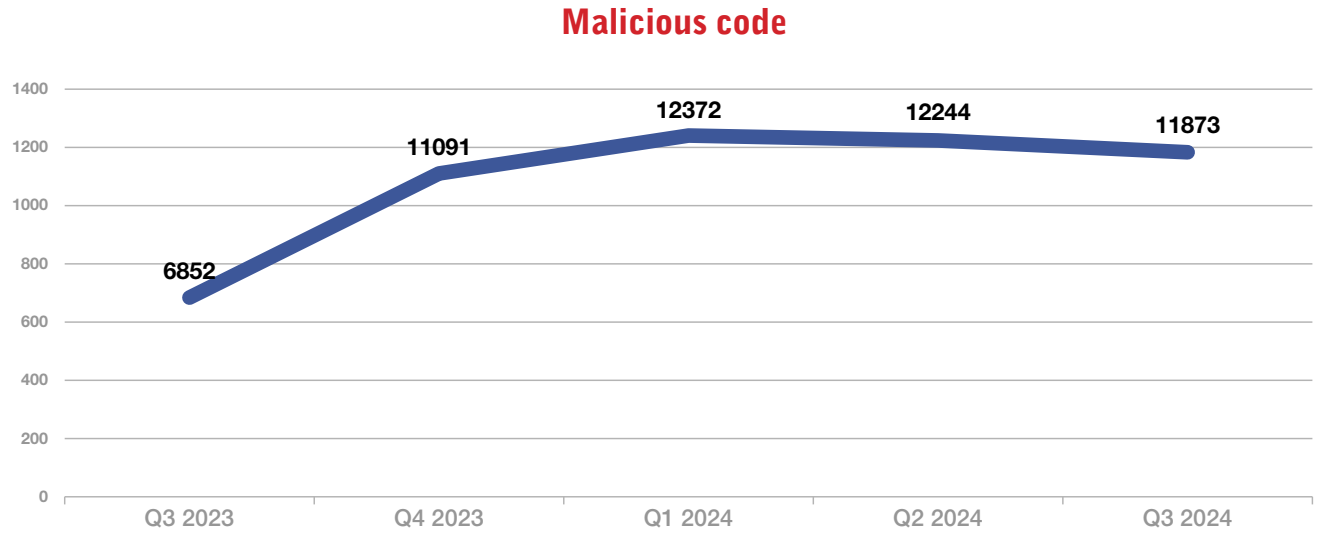
The spread of malicious code threatens data integrity

The number of unique IP addresses compromised by malicious code in Latvian cyberspace remains high. Although there is a slight decrease in Q3 2024 compared to the previous quarter, the 73% increase compared to Q3 2023 indicates a long-term increase in the prevalence of malicious code.

The slight decrease compared to the previous quarter could indicate a temporary improvement or more effective protection mechanisms, but the overall trend is still upwards.

Top 5 most common methods used to hack and infect systems:

- **Phishing emails;**
- **Exploitation of publicly known vulnerabilities;**
- **Abuse of services exposed to the web due to incorrect configuration: default authentication credentials, brute-force password cracking, version vulnerabilities;**
- **Leaked user credentials;**
- **Automated attacks.**



During the reporting period, the main types of malware were user data theft tools, bot-nets, ransomware and remote control Trojans to extract data or compromise infrastructure.

Malware is mainly spread for two purposes: to retrieve data or to make a profit.

Social engineering, through phishing, encourages users to download malware. Malware embedded in online advertisements also widens the attack surface. In addition, cyber attackers continue to use techniques such as password-protected archives and deceptive HTML phishing pages. So-called watering-hole attacks compromise websites to infect visitors, and supply chain attacks target business partners to infiltrate larger networks. User data theft tools and malware that steal personal data are becoming increasingly sophisticated and are a serious concern – these trends are likely to continue.

When the user opens a malicious attachment, the device is infected with malware that collects usernames, passwords, cryptocurrency wallets, and their access credentials, among other things, in order to send these to attacker-controlled infrastructure.

Attacks are sometimes opportunistic, targeting the data or infrastructure that has the greatest impact on victims' activities. Cybercriminals can either steal directly from victims or make money from information stolen from victims. In addition, cybercriminals are increasingly working together in organised groups, making them a force to be reckoned with.

Phishing remains the preferred method of cybercriminals, and they refine their strategies through social media and popular email marketing platforms. Cybercriminals are increasingly turning to social media and communication platforms such as WhatsApp or LinkedIn to circumvent corporate defences. Personal accounts, which are generally less secure than corporate accounts, are particularly vulnerable. This approach is likely to continue in the future.

Data theft malware targets low-security, locally stored authentication data and passwords, i.e., it retrieves passwords from web browsers or unencrypted files. This type of malware is distributed as a malicious web browser plugin or as an executable file attached to a phishing e-mail.

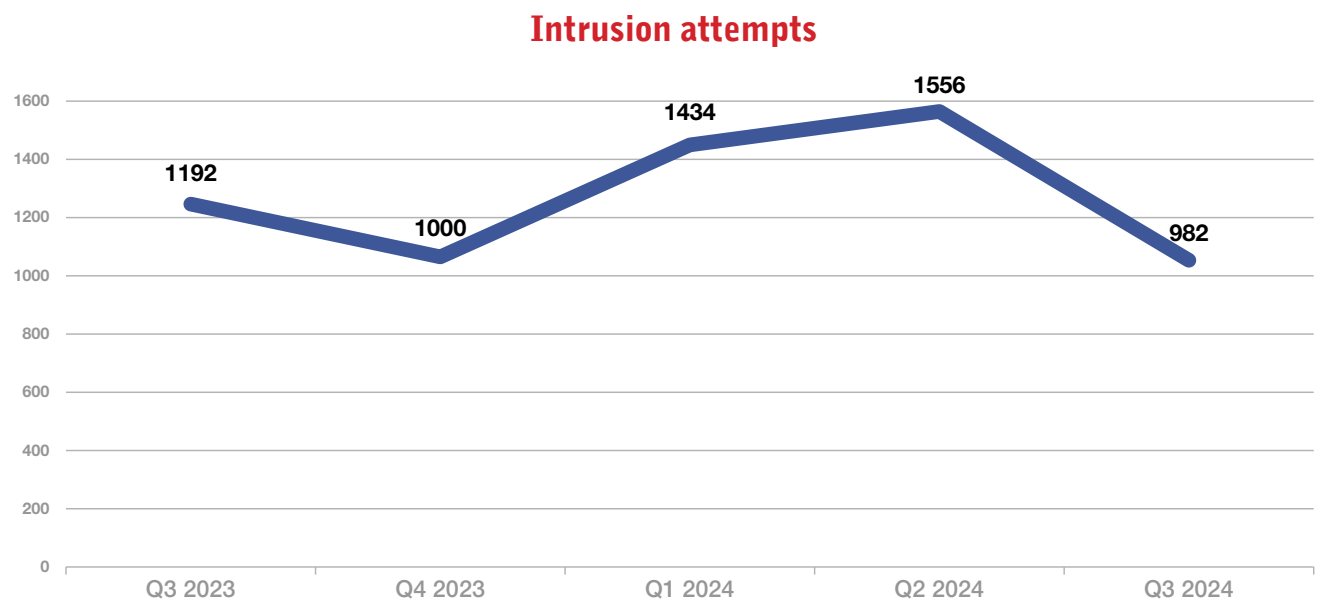
Cyber attacks against companies have increased significantly. Compromised emails or app accounts are actively used to spread malware.

Phishing emails are more likely to contain malicious attachments with an .html extension, including phishing schemes where the malicious attachment contains instructions that prompt the user to execute commands by pasting them into the Windows runtime window.

Ransomware attacks against businesses are becoming increasingly audacious and financially disruptive. During the reporting period, Amber Beverages Group, a manufacturing company, experienced an encrypting ransomware attack which resulted in a leak of company data. Criminal proceedings have been initiated by the State Police and CERT.LV continues to provide support.

Intrusion attempts

The 37% decrease in the number of compromised unique IP addresses recorded by CERT.LV in the reporting period compared to Q2 reflects improved protection measures and a more effective response to cyber threats.
The 18% decrease compared to Q3 2023 indicates long-term improvements in cybersecurity.



While the previous quarter marked the highest level in two years, the current decrease could indicate changing threat dynamics and a possible decrease in the intensity of attacks.

The majority of cases involve brute-force attacks against various electronic communications companies, State and local government authorities and the private sector.

In parallel, long-known configuration weaknesses in widely used products are exploited. Cybercriminals also work hard to penetrate the internal networks of organisations, exploiting newly discovered vulnerabilities to gain unauthorised access to sensitive information or to encrypt data on devices and extort money for the recovery of data.

In addition, the human factor remains a major cybersecurity risk, as people are easily fooled by, for example, phishing techniques that can compromise otherwise well-protected systems.

The risks of compromising equipment are increasing

In Q3 2024, the 267% increase in the number of compromised unique IP addresses recorded by CERT.LV, compared with Q3 last year, shows a significant increase in the number and intensity of attacks, with a consequent increase in the risks of accounts and websites being compromised.

The most common methods of hacking systems are:

- **phishing emails;**
- **publicly known / newly disclosed vulnerabilities;**
- **exposed services – default authentication credentials, brute-force password cracking, versioning vulnerabilities;**
- **weak password management and absence of 2FA;**
- **supply chains;**
- **automated attacks;**
- **compromised social network accounts of users.**

During the reporting period, there were cases of compromised devices, which affected individuals as well as private and public organisations. Supply chain attacks remain a threat that is also used as a way to convey a political message.

As in April and May 2024, a supply chain compromise attack was reported in September against a TV channel rebroadcast in Latvia. On 20 September, a video prepared by cyber-attackers praising Russian imperialism appeared for a few minutes on the interactive television content of the Latvian communications operator Balticom. Preliminary investigations indicate that a cyber attack took place on the servers of an intermediary service provider outside Latvia. Balticom estimates that around 2% of Balticom's interactive television customers may have been affected. CERT.LV stresses that this is the second such attack against the same content provider, which also affected Balticom's content on 9 May this year, and it is likely that the supply chain of the service has been compromised again and that the intermediary has not implemented preventive measures; its credibility should therefore be assessed.

2. Cyber threat prevention

Effectiveness of DNS firewall

Campaigns on fraudulent activity – both redirections to fake sites to scam bank accounts, email or social network access data, and distribution of malware in cyberspace – are a regular occurrence in Latvia. CERT.LV monitors such activities and promptly inserts campaign indicators into the DNS firewall, protecting its users from identified threats and redirecting them to the alert site.

If malware has already infected a device, the CERT.LV DNS firewall enables identification of such devices more quickly, allowing system administrators to promptly clean up the consequences.

In Q3 2024, DNS firewall users were protected from visiting malicious sites more than 103 414 times by redirecting the end-user to the CERT.LV alert site.

With the entry into force of the NCSL, electronic communications service providers from 1st September 2024 are obliged to use the CERT.LV DNS firewall, which automatically blocks harmful internet resources, thus protecting all Latvian internet users in a centralised way.

The effectiveness of Early Warning Systems (EWS)

The IT Security Early Warning System is a service provided by CERT.LV that analyses traffic anomalies and identifies signs of cyber-attacks in the service recipient's infrastructure.

In Q3 2024, the total number of alerts generated by the EWS in State, local government and ICT critical infrastructure institutions was approximately 1.83 billion – an increase of 26% compared to Q2. This increase was mainly due to warnings related to large-scale phishing and computer viruses.

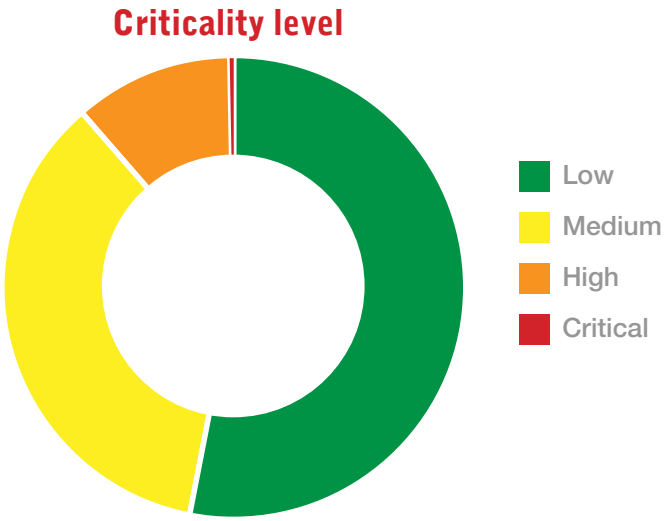
Development of the Security Operations Centre (SOC)

Developed with the aim for CERT.LV to obtain near-real-time visibility of the happenings in Latvian cyberspace – SOC service centrally collects security telemetry from the customer's infrastructure, and correlates events in the customer's infrastructure with the set of threat indicators and knowledge available to CERT.LV. This allows identification, warning, stopping and preventing a cyber threat or cyber incident.

The SOC service offers various significant advantages, such as the processing and temporary storage of the customer's security telemetry data in the CERT.LV infrastructure keeping it in the territory of Latvia.

At the end of the reporting period, the SOC monitored 1774 devices in the customer infrastructure, recording more than 46 000 security telemetry alerts, 104 of which were critical. The majority of these were low-level alerts (more than 24 000).

The targeted activities to develop CERT.LV SOC services and on-board new customers continued. With the NCSL, range of subjects has expanded. Cooperation with providers of essential and critical services to facilitate more effective protection against cyber threats was prompted.



Coordinated Vulnerability Disclosure (CVD)

CERT.LV continues its work on the development and promotion of the CVD reporting platform cvd.cert.lv, playing the role of coordinator and facilitator of the coordinated vulnerability disclosure process, as well as being the developer, maintainer and manager of the platform.

In Q3 2024, the number of security researchers (+5%) and the number of vulnerability reports (+15%) registered on the CVD platform increased.

The CVD platform, launched in 2023, enables institutions that have voluntarily engaged in a coordinated vulnerability disclosure process and have identified the resources that can covered by vulnerability reporting, to publish these on the platfrom. 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 fully coordinate vulnerability research and remediation, thus more effectively organising measures to protect Latvia's cyberspace.

3. Strategic partnerships in Latvia

Threat hunting operations

CERT.LV is a leader in conducting cybersecurity threat hunting operations in the European Union. Proactive cyber threat hunting operations have been conducted since 2022 with the aim of identifying the presence of cyber threats in ICT infrastructure systems important to Latvia.

The analysis of CERT.LV threat hunting operations show that the presence of foreign APTs, including politically motivated and other commercially motivated cyber-attackers supported by Russia and China, was identified in approximately 25% or 8 organisations' facilities and has been since successfully neutralised.

Other significant threats were also discovered, which the target organisations were able to address through data-driven decision-making thanks to the reports received after the threat hunting was concluded.

Cyber threat hunting operations led by CERT.LV are conducted in close cooperation with the Canadian Armed Forces Cyber Command.Threat hunting operations are important for enhancing Latvia's cyber defence capabilities contributing to further development of their own capabilities while contributing to strengthening counter-insurgency capacity to prevent any cyber-attack from occurring.

During the reporting period, theoretical and practical materials were developed for the upcoming international Threat Hunting Workshop to be held in October of this year in cooperation with the Canadian Armed Forces Cyber Command and NATO CCDCOE.

Security Tests

CERT.LV experts discovered and remediated a number of significant vulnerabilities in critical infrastructure and service delivery organisations, as well as trained the cyber hygiene skills of their employees by conducting 14 large-scale IT security tests as well as conducted simulations of cyber threats and phishing attacks.

Cooperation with ICT critical infrastructure holders

Cooperation with ICT critical infrastructure holders continued, both in terms of monitoring the situation in cyberspace and providing advice and support to strengthen cyber resilience and improve cross-sectoral cooperation. CERT.LV is actively installing IT Security Early Warning Systems (EWS) and DNS RPZs in institutions and enterprises to facilitate faster identification and the more effective prevention of threats to critical ICT infrastructure.

Work continues on improving the CERT.LV service framework, both by developing new solutions for service provision and by improving the procedures related to service provision.

In recent years, CERT.LV has observed an increasing number of attacks aimed at compromising industrial control systems.

For example, CERT.LV was informed about a situation where a large farmer in Latvia, fell victim to a cyber-attack. The automation system of a grain dryer on his farm was not sufficiently protected, and, system was accessed (allegedly by Russian-linked attackers), the parameters were changed, and the grain started to burn. As we are talking about the spoiling of many tens of tonnes of grain, this is a major problem, not only for the farmer concerned, but even at the national level.

Similar type of risks affects also energy and transport companies of all kinds. As a response to this CERT.LV is offering a service – the Industrial Automation and Control Systems Security Lab. Lab allows testing the security of operational technology (OT) equipment, software and the communication protocols used to perform security tests on real devices and provide support to companies and organisations in these sectors.

CERT.LV recommends that critical infrastructure organisations implement user behaviour analytics – a process that allows automatic detection of behavioural anomalies in networks, devices or accounts. Behavioural analytics is essential for detecting malicious actors, who often use so-called "living off the land" (LOTL) techniques. LOTL techniques allow an attacker to carry out malicious activities using tools or programs in the target environment and evade detection. State-sponsored groups such as Volt Tyhoon often use LOTL techniques to gather information.

By using CERT.LV SOC service protection solutions, anomalous activities can be detected by comparing event logs with daily activities. Organisations should also consider threat hunting operations as a proactive measure to detect malicious actors using LOTL techniques.

Contribution to the development of cybersecurity policies

In order to strengthen cybersecurity in Latvia and to implement the requirements of the revised European Union Network and Information Systems Security Directive (NIS2), the National Cybersecurity Law (NCSL) entered into force on 1 September.

On 1 September 2024, the new National Cybersecurity Law entered into force in Latvia

A new institution, the National Cybersecurity Centre, was launched to act as a single point of contact for cybersecurity issues. Centre will also monitor the implementation of national cybersecurity requirements, as well as develop national cybersecurity policy initiatives. The functions of the centre will be performed by the Ministry of Defence in cooperation with CERT.LV, while the monitoring authority for ICT critical infrastructure will be the Constitutional Protection Bureau.

In the context of the implementation of the NCSL, CERT.LV took preparatory measures to prepare for the new tasks once the NIS2 Directive is applied and the new regulation enters into force. CERT.LV is in the process of adapting internal and external documentation and making other preparations.

CERT.LV continues to make a valuable contribution to the sectoral policy framework. Work continues on the clarification of new legislation and the preparation of guidelines to support NCSL subjects in implementing the new requirements.

During the reporting period, the review of draft laws/initiatives was carried out. This included one EU and 15 Latvian draft legislative initiatives.

Cybersecurity challenge for young people in Latvia

CERT.LV is actively involved in promoting cybersecurity skills among young people in Latvia, both by supporting the preparation of the National Cybersecurity Challenge competition and by participating in the preparation of the Latvian team for the European Cybersecurity Challenge 2024 (ECSC 2024) to be held in Turin, Italy, from 8 to 11 October 2024.

By taking part in the cybersecurity challenge, young people have the opportunity to test and put into practice their knowledge and skills in various areas of cybersecurity. Event enables also meeting and building closer cooperation with representatives from other EU Member States.

The Latvian team will participate in the European Cyber Security Challenge for the first time. National Cybersecurity Challenge 2024 ensured the selection of candidates for the Latvian team. The national selection was organised by the Ministry of Defence in cooperation with CERT.LV, the University of Latvia and the Cyber Defence Unit of the National Guard. It was supported by the Latvian National Coordination Centre for Cybersecurity Excellence (NCC-LV) and the European Cybersecurity Competence Centre and co-funded by the European Union (EU).

The annual event in 2024 is organised by the EU Cybersecurity Agency (ENISA) in cooperation with the Italian Cybersecurity Agency and the Cybersecurity National Laboratory (CINI). More information: https://ecsc2024.it/.

4. Communication with the public

During the reporting period, the CERT.LV team was active in educating the public by organising and participating in various thematic seminars, providing information about current cybersecurity developments and promoting cyber hygiene best practices.

In Q3 2024, CERT.LV implemented **17 educational events** on IT security and current trends, training a total of **7787 participants** across Latvia.

CERT.LV continues to provide its clientele with a hands-on Cyber Incident Investigation Mock Trial, where participants are given a unique opportunity to take on the role of a cyber detective and interactively investigate and analyse the progress of a cyber-attack on a multinational company. One of the central tasks of the mock trial is to identify the culprit responsible for the cyber-attack and discuss its consequences.

CERT.LV also supported the Ministry of Defence in organising information seminars for representatives of industries subject to the new National Cybersecurity Law (NCSL). During the reporting period, sectoral seminars were organised for representatives of telecommunications and ICT, energy, water supply, transport, medical and pharmaceutical, food production and wholesale, postal, courier, waste management and other sectors, as well as for representatives of state administration and local governments.

CERT.LV continues to inform the public about cybersecurity risks, cyber hygiene promotion and best practices, as well as other topical issues in Latvian cyberspace, including the monthly Cyber Weather review of the monthly highlights in the TOP 5 categories.

5. International cooperation

CERT.LV continues representing Latvia and building partnerships with cyber incident response teams and National Cybersecurity Centres from other countries. Partnerships are built also with international organisations, including the CSIRTs network, ENISA, FIRST, EU institutions, NATO, and other security partners in the Euro-Atlantic region and in international security overall, providing advice and support through various working groups, and consistently working with the public at international conferences.

We are proud! In May 2024, a GOVCERT.LU expert conducted a SIM3 Peer Review of CERT.LV, and the Peer Review report submitted at the end of July confirms that the CERT.LV team received the highest rating, EXPERT.

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

- **Coordinated Vulnerability Disclosure Task Force** – work is underway to gather EU-level coordinated vulnerability disclosure experience and practices;
- **EU Cybersecurity Index** – work continues on developing the EU Cybersecurity Index platform.

CSIRT Network Situation Update meetings: regular participation in meetings aimed at exchanging information on the current situation in cyberspace between CSIRT Network members continues.

European Commission European Health Data Space (EHDS) 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 General Data Protection Regulation.

During the reporting period, CERT.LV participated in the European Cybersecurity Certification Group (ECCG) meetings, including meetings representing Latvia's interests and providing its perspective on problematic issues concerning the further progress of the EU Cloud Certification Scheme (EUCS) in EU countries, as well as other issues concerning the implementation of the cybersecurity certification of ICT products in EU countries.

The Cyber Europe 2024 training organised by ENISA took place from 19 to 20 June, with the primary audience being the energy sector and secondary audiences being public administration and data centres. In September, CERT.LV was involved in the preparation of the After Action Report. The evaluation meeting of the training is planned for November 2024.

NATO CCDCOE organised the exercise Crossed Swords 2024: in Q3, CERT.LV participated in the planning cycle of the exercise Crossed Swords 2024, providing support to the organisers (White Team) in the development of the Information Operations Game scenario.

Cyber Coalition exercise organised by NATO: in Q3, CERT.LV participated in the Cyber Coalition national planning conference, where the National Armed Forces informed attendees about this year's exercise scenario, Latvia's chosen scenario directions and challenges, and cooperation between the civilian and military spheres.

Cooperation within FIRST

Regular participation in FIRST Membership Committee meetings continued to discuss future rules for membership admission and recruitment, membership categories, and the application of the SIM3 model in the team certification process. CERT.LV Manager Baiba Kaškina, while continuing as Chair of the FIRST Membership Committee, participated in the review of new member applications and contributed to the improvement of the membership process.

Cooperation within TF-CSIRT

CERT.LV is one of 42 TF-CSIRT/Trusted Introducer certified teams in Europe. At the end of the reporting period, there are 526 teams in the community, which demonstrates the high level of maturity and preparedness of the CERT.LV team. CERT.LV continues to work in several TF-CSIRT working groups.

We are proud! CERT.LV is a TF-CSIRT Trusted Introducer certified IT security incident response team of the highest level.

Certification is based on the SIM3 standard and parameter levels defined by TI/TF-CSIRT. The certification is based on SIM3: The 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. Successful certification demonstrates the professionalism of the team and the orderliness of the processes. The certificate is issued for three years, after which a re-audit is required to maintain the certification.

From 25 to 27 September, the 72nd TF-CSIRT meeting took place in Prague, Czech Republic, with CERT.LV experts Dana Ludviga presenting The Rise and Impact of DNS Firewall in Latvia – From Idea to Mandatory Measure, and Egils Stūrmanis presenting Twelve Years Experience of Cybersecurity Awareness Raising in Latvia.

Other key events during the reporting period:

On 9 July, at the United Nations in New York, USA, CERT.LV Manager Baiba Kaškina represented Latvia at a thematic discussion on strengthening resilience in cyberspace. Event was organised by the Permanent Mission of Latvia to the UN in cooperation with the missions of Bahrain and Colombia, as well as the UN think tank UNIDIR. The event was opened by Rolands Heniņš, Undersecretary of State – Policy Director, Ministry of Defence of the Republic of Latvia and Director of National Cyber Security Centre.

From 22 to 23 August in Arhus, Denmark, the Nordic-Baltic CyberSkills Think Tank meetings were attended by representatives of both the Ministry of Defence and CERT.LV. CERT.LV expert Sanita Vītola took part in the discussions and talked about Latvian initiatives to improve cybersecurity education. More information: https://cyberbridgeforum.com/

On 12–13 September in Tallinn, Estonia, at the Nordic Baltic Security Summit, CERT.LV Manager Baiba Kaškina shared CERT.LV's vision on strategies and best practices for strengthening cyber resilience during the panel discussion The Role of Education and Social Awareness in Building Resilient Cyber Security.

On 19 September, the ENISA-organised conference ThreatHunt 2030 took place in Athens, Greece. CERT.LV representatives were also present. The conference focused on future cybersecurity threats and how the European Union and Member States can best anticipate, identify, prevent and respond to future cybersecurity challenges.

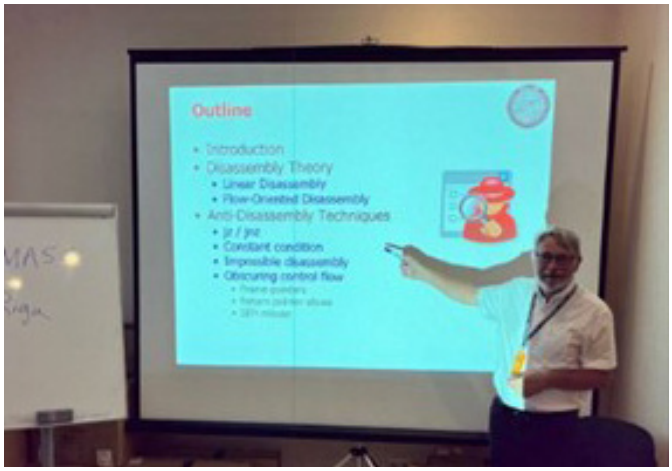
CERT.LV representatives participated remotely in the **24th CSIRT Network meeting in Budapest, Hungary, from 23 to 24 September** to ensure a successful exchange of information and closer cooperation with EU cyber incident response teams.

CERT.LV expert Daina Ozoliņa participated in **the cybersecurity event organised by Korea CERT in Seoul, South Korea, from 23 to 27 September**. The aim of the event was to bring together cyber incident responders from the Asia-Pacific region, Europe and America. The programme included a TRANSITS-I course on organisational, operational, legal and technical aspects of cybersecurity, with a strong focus on experiences from different countries and regions, and discussions where D. Ozoliņa presented CERT.LV initiatives – threat hunting, the DNS firewall, the CVD platform, as well as participation in international exercises. Ozoliņa also participated in the Table-Top exercise on a ransomware attack (incident handling, coordination and communication).

CERT.LV continues to participate in the coordination of the Nordic-Baltic SOC (Nordic-Baltic Security Operations Centre).

Latvia hosts a high-level training course for cybersecurity professionals

In August 2024, a successful 2-week training course – Malware Analysis Short Course – was conducted by the Canadian Armed Forces Cyber Command with Royal Military College of Canada in cooperation with CERT.LV.



The participants gained theoretical knowledge as well as practical experience and important skills that will be useful in their daily work to combat cyber threats, thus strengthening the country's overall cyberspace defence. The training is a valuable step in the joint cooperation between Latvia and Canada.

CERT.LV continues promoting cybersecurity and being a trusted opinion leader in Latvian cyberspace.

CERT.LV's mission is to foster IT security in Latvia.

The main tasks of CERT.LV are to maintain and update information on IT security threats, provide IT security support to government institutions, assist in the clean-up of IT security incidents affecting any natural individual or legal entity if the incident involved a Latvian IP address or was in the .LV domain, and organise information and education events for the employees of government agencies, IT security professionals, and other interested parties.

Contact CERT.LV:

Phone: +371 67085888

E-mail: cert@cert.lv

Website: www.cert.lv

Follow CERT.LV news on:


www.twitter.com/certlv


www.facebook.com/certlv

CERT.LV
Cyber Incident
Response Institution