# Q1 2025
# In Latvian cyberspace

**Period: 01.01.2025. – 31.03.2025.**

CERT.LV
Cyber Incident
Response Institution

# Q1 2025 in Latvian cyberspace

## SUMMARY

In the first months of 2025, the cyber threat landscape in Latvia and around the world continues to evolve with increasing intensity, complexity and strategic direction. Cyber-operations are no longer just one-off attacks or attempts to profit – they are increasingly targeted, persistent and aligned with broader geopolitical and economic objectives.

With continued large-scale cyber-attacks against Latvia, the threat level remains high since Russia's full-scale invasion of Ukraine in 2022. Against the backdrop of the threat of Russian aggression, the start of 2025 clearly demonstrates Latvia's cyber resilience and ability to effectively defend our cyberspace.

Cyber espionage and financially motivated attacks have mainly targeted important institutions and organisations in the financial, law enforcement, education, healthcare and telecommunications sectors, as well as state and local government authorities and critical infrastructure. These attacks are intended to extract sensitive data, destabilise operations, undermine public confidence and create strategic pressure.

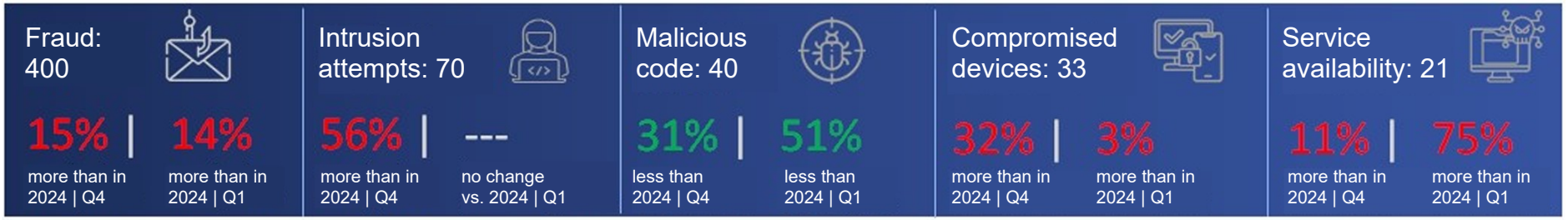
Given the potential aggressive plans and rhetoric of Russia towards the EU and the Baltic States, the threat dynamics are expected to remain high in the future. Interest in Latvian infrastructure from Chinese and Belarusian-backed cyber attackers has not diminished.

**The number of cyber incidents (631) in the reporting period increased** by 11% compared to the previous quarter, but is 11% lower than in Q1 2024.

**The volume of alerts automatically processed and sent (284 029) is high,** but stable year-on-year.

**The intensity of cyber threats remains high** and the trends observed call for further improvements in preventive security measures and the effectiveness of the response.

### Top 5 most common threat types and number of cyber incidents in the reporting period



# 1. Cyber security Threats in Cyberspace: Statistics and Trends

In Latvian cyberspace, the intensity of cyber threats has been high since Russia's full-scale invasion of Ukraine in 2022, and the dynamics are expected to remain high in the future.

The increasing intensity, sophistication and relentless ingenuity of cyber attackers encourages every organisation to counter this with appropriate technological solutions, which in turn boosts technical capabilities, the demand for data-driven cyber security services, and strengthens public and private sector response capabilities. Security Operations Centre services and regular IT system security are becoming common practice. The challenges are contributing to significant developments in strengthening our cyber security, without allowing Latvia to be perceived as an easy target.

In response to the growing scale and complexity of cyber threats, from 1 January 2025 we have improved our statistical approach – from now on, unique cyber incidents are counted rather than unique IP addresses compromised. This approach more accurately reflects the scale and impact of threats; comparability with historical data is maintained.

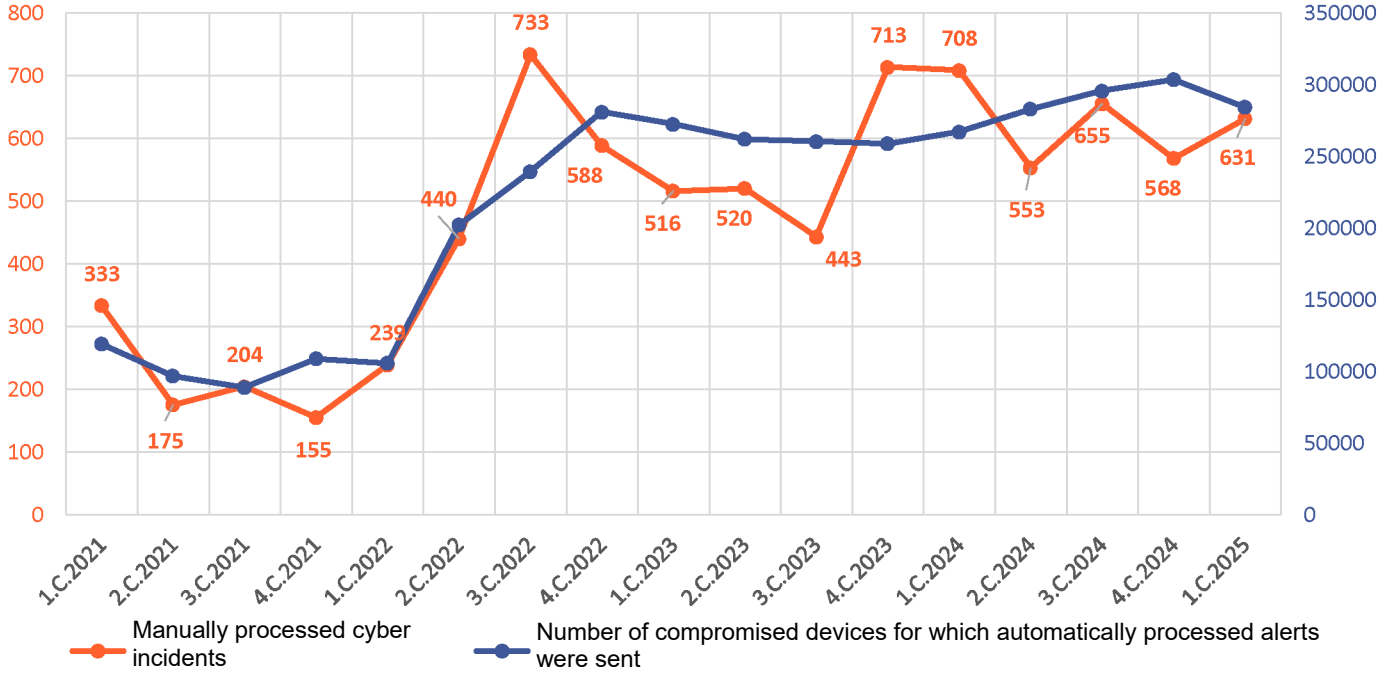



**Figure 1. Dynamics of the cyber incident and equipment threat curve (numbers by quarter; 2021–2025)**

## The volume of automatically processed alerts is high but stable

In Q1 2025, the number of alerts[1] processed automatically reached 284 029, a 6% decrease compared to the previous quarter, but a 6% increase compared to Q1 2024. This means that the volume remains stable year-on-year and the identification of threats and the sending of alerts are improving.

Quantitatively, the majority (83%) of automatically processed alerts were due to configuration deficiencies and remained at the same level year-on-year.

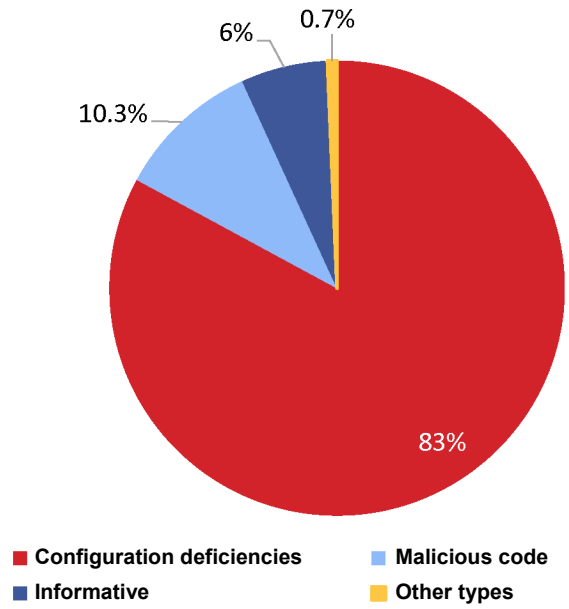



**Figure 2. Automatically processed threat alerts (percentage of the total in Q1 2025)**

This points to system and network security weaknesses, mainly due to human error or insufficient security standards, such as:

- leaving service ports unprotected,
- using unencrypted data transmission,
- practicing weak access control,
- failing to ensure proper version control of devices and the services they maintain.

### Vulnerability management recommendations

- Regularly conduct a comprehensive inventory of equipment and systems for a complete picture of the infrastructure to spot obsolete or vulnerable equipment early.
- Reduce security risks by avoiding unnecessary exposure of IT resources on the public internet. Ensure access is only through secure solutions using MFA or encryption.
- Keep up-to-date with software updates; ensure all systems have the latest security patches.
- Implement centralised update management to ensure continuous monitoring of all systems in the organisation.
- Conduct regular vulnerability scans to identify weaknesses and reduce risks from known vulnerabilities.

[1] Using the telemetry data available in CERT.LV, the end-user was informed about the threat to the device by means of information delivered via Internet Service Providers.

## The number of cyber incidents manually handled by CERT.LV is increasing

In the reporting period, 631 cyber incidents[2] were recorded, an increase of 11% compared to the previous quarter, but a decrease of 11% compared to Q1 last year. The increase could be due to new types of attacks and the development of Artificial Intelligence (AI), which facilitates and accelerates fraud, intrusions and automated attacks. During the reporting period, the month of February recorded the 3rd highest number of incidents in the last three years.

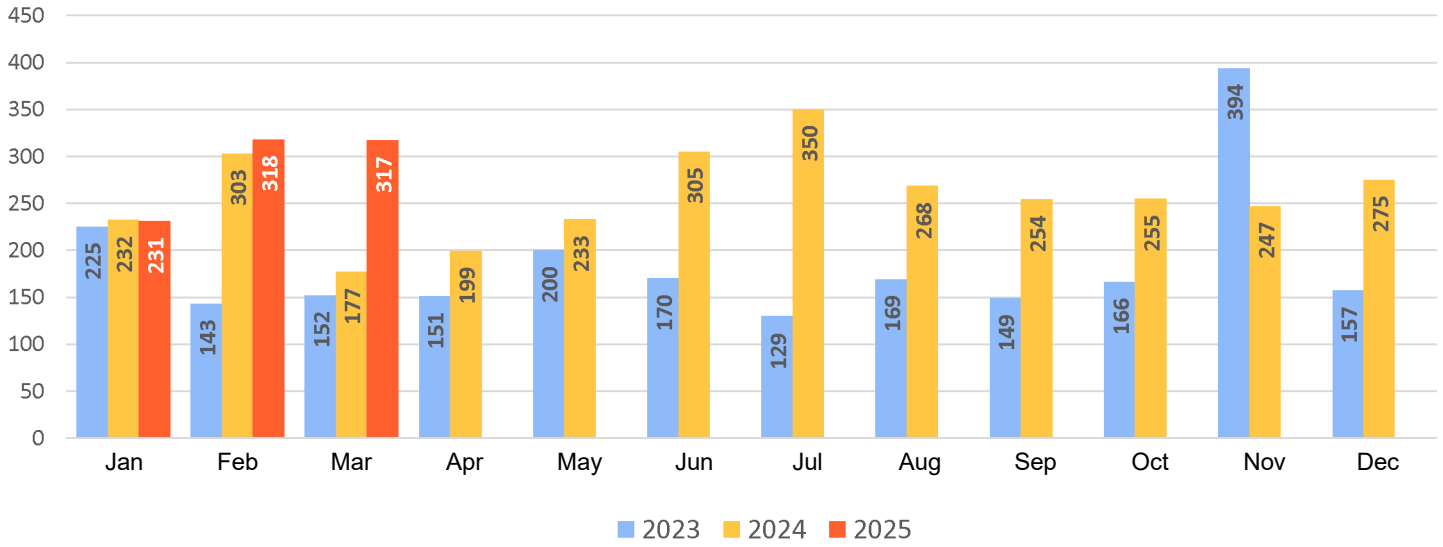



**Figure 3. Cyber incident dynamics (number of months; period: 2023–2025)**

## Cyber Weather

Monthly overview of the most prominent cyber incidents and threats in Latvia in TOP 5 categories

An overview in easy-to-read language: current events in cyberspace, threat analysis and useful tips on how to stay one step ahead of potential cyber threats.

**Find out more:**

- January
- February
- March

[2] Incidents that compromised processed data or the availability, authenticity, integrity or confidentiality of services offered by or accessible through network and information systems.

# 2. Most common cyber threats in the reporting period: analysis and recommendations on how to tackle them

- **Fraud** (400 cyber incidents) – the biggest threat and growing rapidly.
- **Intrusion attempts** (70 cyber incidents) – increasingly innovative methods and their challenges have not diminished during the year.
- **Malicious code** (40 cyber incidents) – decreasing but still dangerous.
- **Compromised equipment, service availability and information security** – cyber incidents are on the rise with the increasing intensity of attacks.

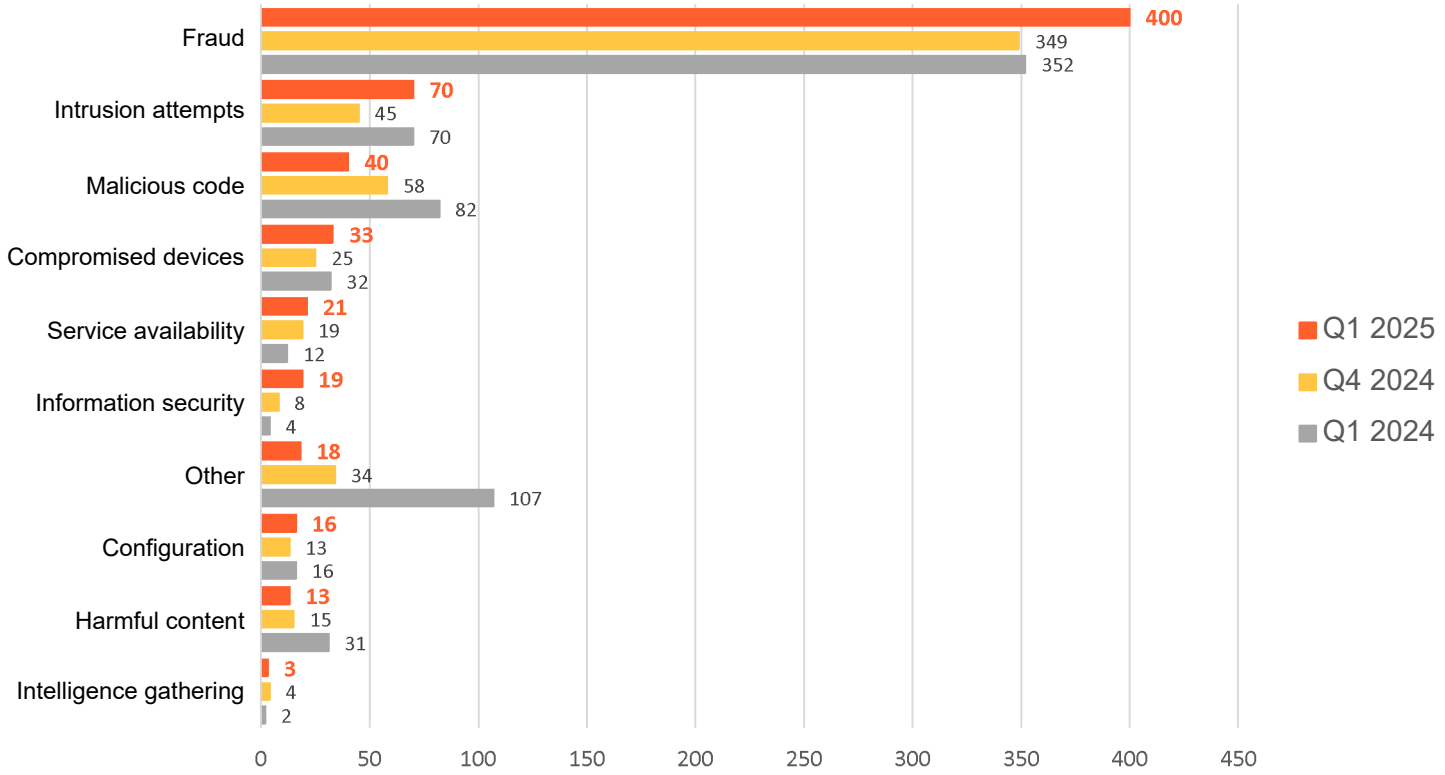



**Figure 4. Comparison of cyber incidents by type**

## Service availability attacks

(+11% vs Q4 2024 and +75% vs Q1 2024) are increasingly used to affect national resources – websites of the unified web platform, financial institutions, mobile operators and some parts of the private sector.

During the reporting period, the financial sector was the target of the most DDoS attacks.

## Intrusion attempts

with an increase of 56% compared to the previous quarter, this indicates more aggressive attacks against systems, but the number remained stable year-on-year. Configuration deficiencies and vulnerabilities in systems, outdated software, weak passwords and lack of multi-factor authentication, phishing, vulnerabilities in remote access devices (RDP, VPN, SSH), automated attacks and botnets were the most significant security risks exploited in intrusion attempts.

Hostile state-sponsored and politically motivated cyber-attacks against Latvia's public institutions, financial sector and critical infrastructure mainly use targeted phishing, malware, DDoS attacks and infrastructure sabotage. Russian-backed hacking groups target critical infrastructure, state institutions and large enterprises. **Main objectives: intelligence and data collection, promotion of social tensions and sabotage of critical infrastructure. There is also interest in Latvia's ICT infrastructure from cyber attackers linked to China and Belarus.**

**Fraud** (+15% vs Q4 2024 and +14% vs Q1 2024) continues to grow, indicating a high threat level.

Several commercially motivated fraud campaigns were recorded during the reporting period, which were generated through the skilful use of AI and social engineering to access personal data and information.

**Phishing campaigns targeting Latvian citizens using the names of well-known organisations were particularly common.**

Figure 5 below shows that the largest percentage of the total number of phishing reports processed by CERT.LV was related to the use of SEB Bank's name for phishing purposes.

Various other phishing topics were detected 34 times, while phishing of less popular web-based email services was detected 27 times.

**The main motive of fraudsters is profit, but the number of cases where such attacks are carried out for espionage purposes is increasing.**

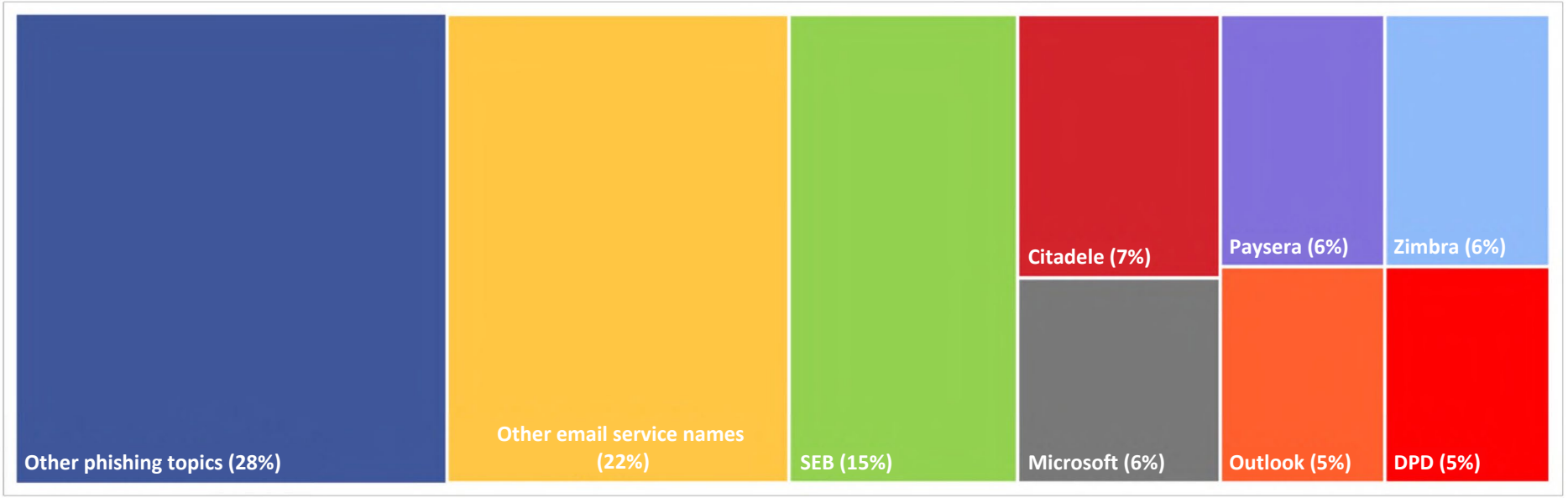



**Figure 5. Most common phishing campaigns using the names of known organisations**

(percentage of total number of phishing messages processed by CERT.LV in Q1 2025)

**CERT.LV reminds that governmen institutions and their representatives will not urge immediate action in emails or phone calls and will not share bank account access or payment card data.**

**The legitimacy of the call or message should be verified by visiting the official website of the institution and contacting the telephone number provided there.**

## RECOMMENDATIONS FOR ORGANISATIONS TO EDUCATE EMPLOYEES:

- Train users to recognise suspicious emails (fake senders, urgent requests) and how to check email headers and content.
- Block specific file types in email attachments (.exe, .js, .vbs, etc.)
- Regularly (at least once a year) educate staff on current cyber risks and cyber security best practices. CERT.LV offers lectures, games and seminars.
- Conduct knowledge testing of employees, including regular assignment simulation campaigns, supplemented by training and real phishing examples. Include the management of the institution in phishing simulations, as managers are often the targets of attacks. It is recommended to use the CERT.LV phishing attack simulation service.

## Malware is distributed mainly for two purposes: to exfiltrate data or to gain profit.

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.

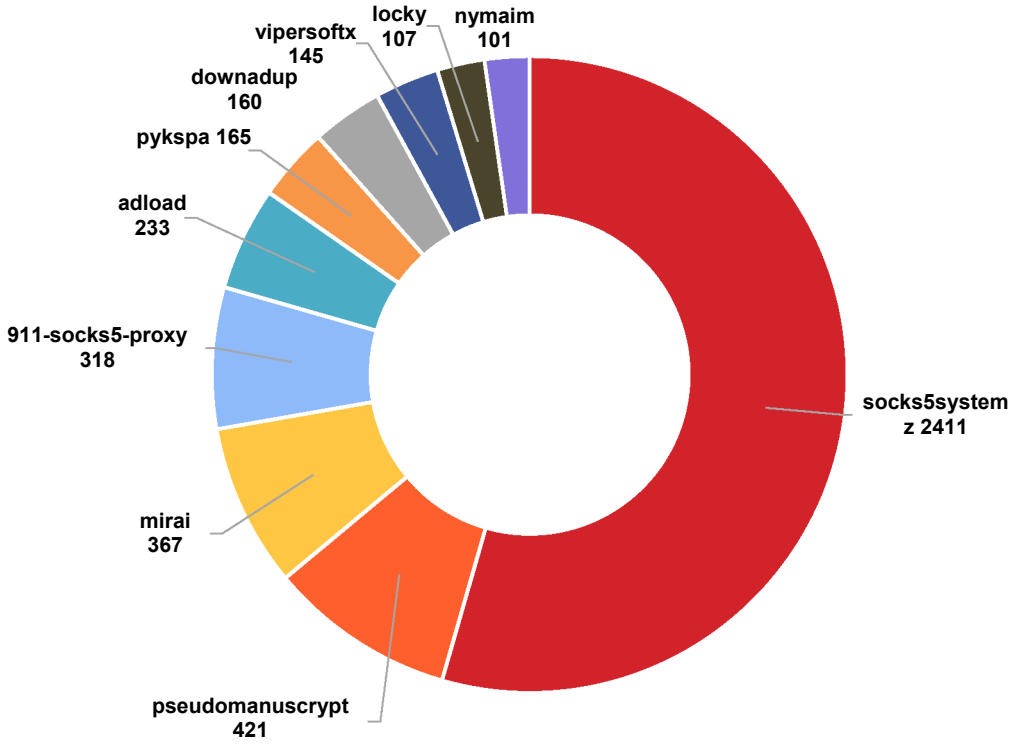



Figure 6. Top 10 malware; number in Q1 2025

### The most common types of malware:

- **User data hijackers**
- **Botnets**
- **Ransomware**
- **Remote control trojans for data extraction and infrastructure compromise**

In most cases, data theft malware targets low-security, 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 email – trends that are likely to continue.

***Socks5systemz* once again proves its resilience in the cyber world – a constant leader in the TOP 10 list of malwares for several years.** It infects machines, turning them into redirection proxies, which can in turn be used by malicious actors to make it harder to track their illegal and harmful 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.

# Key trends and findings

## The art of manipulation in cyberspace: social engineering and fraud

- **Phishing and personalised cyber-attacks:** the use of known organisation names and AI to create trusted, targeted emails, text messages and fake websites is increasing significantly.
- **Voice cloning and phone scams:** the threat of AI being used to clone voices to persuade victims to make payments or disclose sensitive information is increasing.
- **Hybrid romance and investment scams:** social networks and AI are increasingly sophisticated to create fake identities and investment platforms, causing significant financial losses to romantic victims.
- **Compromised email accounts and fake invoices:** compromised employee email accounts are used to distribute malicious attachments, send fake invoices, causing financial losses to organisations.

## Targeted attacks against the state and public sector are intensifying

- **Targeted phishing:** targeted phishing with malicious attachments against state and local government authorities. Previously compromised email accounts are often used to enhance the credibility of the attack.
- **Politically motivated cyber-attacks:** public administrations and critical infrastructure remain high-risk targets. Activities related to cyber-attacks supported by other countries (APTs) have been observed.

## Malicious code and ransomware: a growing problem in cyberspace

- **Increase in ransomware:** attacks observed, especially in the healthcare sector. Data encryption paralyses organisations, with attackers demanding ransom for data recovery.
- **Malware sophistication:** malware used to steal data is becoming more technically sophisticated and harder to detect.

## Emerging threats: compromised devices and communication apps

- **Insufficiently protected devices:** the number of compromised devices is increasing, signalling weaknesses in network segmentation and device security policies and procedures.
- **Threats to communication platforms:** attempts to take over users' Signal and WhatsApp accounts to access sensitive communications. Attacks are linked to Russian-backed attackers who are constantly improving their tactics.

- The growing threat of cyber-attacks underlines the need to reinforce cyber security training for staff, in particular on social engineering and phishing recognition.
- It is important to introduce multi-factor authentication and review access control mechanisms at all levels of the system.
- Network segmentation, device control and monitoring need to be strengthened, especially for IoT devices.

**Working in synergy, CERT.LV's DNS firewall, SOC operations, threat hunting, security tests, phishing simulations and training effectively strengthen organisations' cyber defences – proactively protecting, detecting vulnerabilities, improving cyber literacy and increasing threat preparedness.**

## DNS firewall

In Q1 2025, the total number of malicious domain name DNS requests within the DNS firewall service was **713 548**. Cyber-attacks repelled by all CERT.LV zones prevented users from visiting malicious sites **476 855** times, an increase of **4%** compared to the previous quarter.

CERT.LV welcomes the involvement of citizens who identify and forward fraudulent emails to cert@cert.lv. The reports are compiled and the malicious domain names are placed in an active protection tool – DNS firewall – which is available free of charge to everyone in Latvia, and a **mobile app for DNS firewall is also available.**

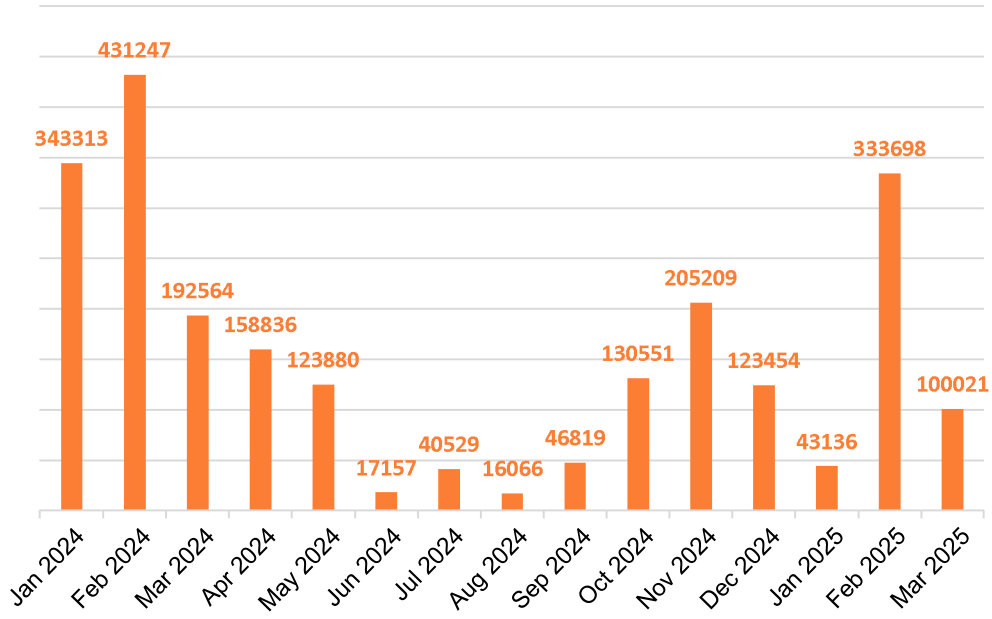



**Figure 7. Cyber attacks repelled in all CERT.LV zones**

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

| Alerts | Quantity |
|---|---|
| The use of the "DELFI" image in advertising campaigns for fraudulent cryptocurrency investment platforms | 33 777 |
| Fake shops selling medical services and goods | 22 126 |
| AgentTesla malware | 4931 |
| Use of "Rimi Latvia" image in fake website campaigns | 1505 |
| Use of "Latvijas Pasts" image in fake website campaigns | 1070 |
| Use of "DPD Latvija" image in fake website campaigns | 891 |
| Use of "Swedbank" image in fake website campaigns | 836 |
| Use of "SEB banka" image in fake website campaigns | 834 |
| Fraudulent campaigns to take over WhatsApp accounts | 761 |
| Use of "Citadele banka" image in fake website campaigns | 631 |

## Security Operations Centre (SOC)

Since 2024, when the CERT.LV SOC service was launched for institutions, a total of **8409 devices (servers and workstations) have gained visibility** as of the end of Q1 2025.

**During the reporting period, the number of endpoint devices has increased by 3119** (59% increase compared to the previous quarter), with a consequent increase in the number of security alerts (absolute number increased by more than 851 000).

**More than 1.2 million security alerts were registered. 181 manual files were created** in the processing of security alerts. In 77% of the cases, customers were contacted to request additional information, to inform about a cyber threat or a cyber incident.

**Four cyber incidents detected.** In all cases, malware was detected with the aim of stealing information from employee workstations. No further impact of malware on the infrastructure has been detected.

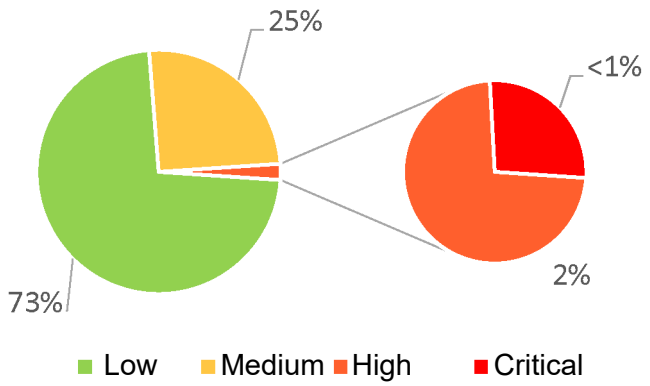



**Figure 8. Security alerts recorded by SOC in Q1 2025 (percentage by criticality level)**

## Cyber security threat hunting operations

Between 2022 and the end of Q1 2025, **cyber security threat hunting operations have analysed 155 000 endpoint devices** (+5000 in the reporting period) in various public sector bodies and ICT critical infrastructure companies. In **~20%** of the cases, the presence of advanced persistent threat (APT), mostly linked to Russia and conducting a wide range of cyber operations, was detected in the infrastructure. Activity by Chinese-linked groups was also observed.

**The Latvian-Canadian cyber security partnership continues:** the Threat Hunting training course was developed and we shared our experience with cyber security professionals from more than 25 NATO Member States. Participants had the opportunity to strengthen their threat hunting capabilities and expand their knowledge of the latest cyber defence strategies. The successful implementation of the training not only strengthened the cyber security resilience of the participating organisations, but also set a new direction for future cooperation initiatives and international cyber security training.

## IT system security tests and phishing attack simulations

In Q1 2025, CERT.LV Cyber security Testing Team conducted **eight** IT system security tests in various public sector institutions and ICT critical infrastructure organisations, as well as **four** phishing attack simulation campaigns, promoting and strengthening staff protection against social engineering attacks and mitigating human factor risks. In addition, CERT.LV also carried out a number of out-of-round security checks on public sector websites. In total, the security tests identified **32** vulnerabilities, of which **three** were critical and **five** high-risk. Thanks to the tests, they were proactively addressed.

## Coordinated Vulnerability Disclosure (CVD)

CSD reporting practices help to learn about vulnerabilities earlier, coordinate vulnerability research and prevention, and organise protection measures more efficiently. In Q1 2025, the number of Security Researchers on the CVD platform increased by **15**, which is **67%** more than in the previous quarter. Between March 2024 and March 2025, **124 vulnerability reports** were registered, an increase of **44** in the reporting period.

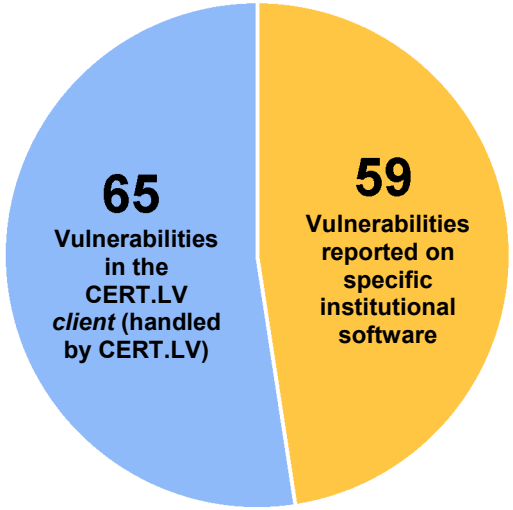



**Figure 9. 124 vulnerability reports; period: 01.03.2024–01.03.2025.**

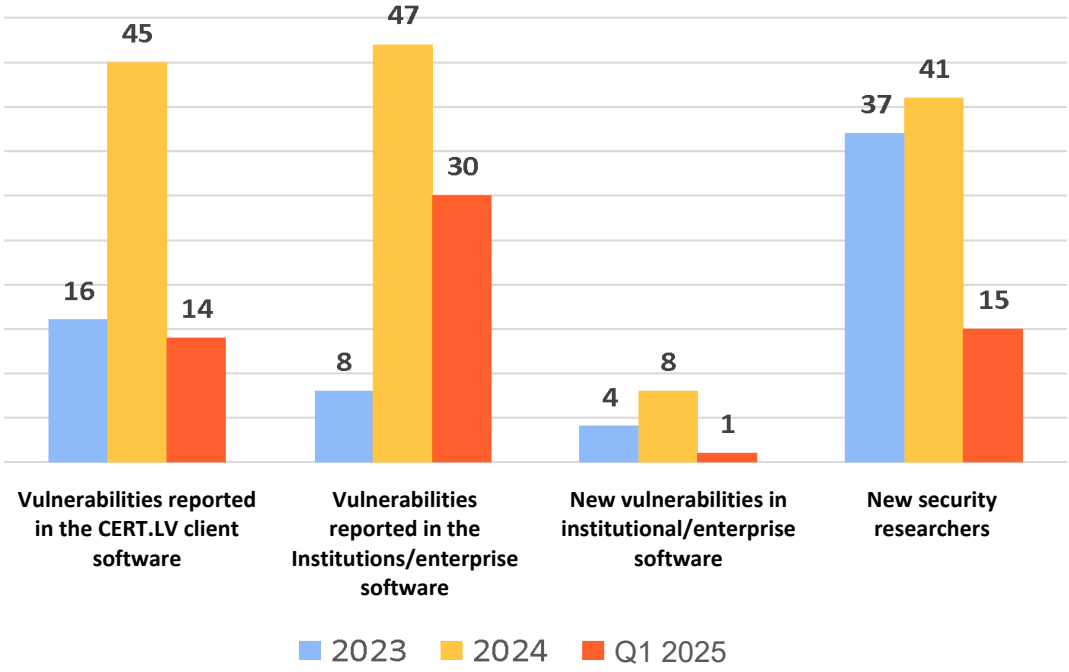



**Figure 10. CVD platform: Number of vulnerability reports in Latvia**

CERT.LV offers a wide range of cyber security services to effectively protect organisations' ICT infrastructure and strengthen their cyber resilience.
Protect and strengthen your cyberspace today with CERT.LV's expertise and guidance: **https://cert.lv/lv/pakalpojumi**
If you would like to receive CERT.LV services, please contact **cert@cert.lv**