2025 Q2

IN LATVIAN CYBERSPACE

PERIOD: 01.04.2025 - 30.06.2025

CERT.LV
Cyber Incident Response Institution

Institute of Mathematics and Computer Science University of Latvia

Ministry of Defence Republic of Latvia

Summary

In Q2 2025, Latvia's cyberspace saw a significant increase in cyber threats and vulnerabilities, confirming trends that have been in place for a long time. It is not just the intensity and complexity of attacks that is on the rise: it is also the ability of attackers to adapt, which in turn encourages the development of appropriate tech security solutions, spurring demand for data-driven services and for better response capability in the public and private sectors.

During the reporting period, a significant **increase in the number of cyber incidents was recorded in Latvia**, with 709 cases (+12% relative to Q1 2025, +28% relative to Q2 2024). Much of this increase is due to the human factor, a rising dependency on digital technology, device vulnerabilities, as well as the rise in the malicious use of generative artificial intelligence (AI) models.

The number of vulnerable devices identified increased significantly, to 459 346 (+62% compared to Q1 this year, and Q2 last year), which indicates the growing use of automated scanning and vulnerabilities. At the same time, this can be explained by the addition of large sources of telemetry data to CERT.LV.

Top 5 reporting-period cyber threats in terms of quantity:

Threat type: number of incidents	Change relative to Q1 2025	Change relative to Q2 2024
Fraud: 460	+15%	+46%
Malicious code: 45	+12%	+7%
Break-in attempts: 31	-56%	-33%
Compromised devices: 25	-24%	-32%
Service availability disruptions: 21	0%	+250%

The sharp rise in fraud reflects a continuously intense level of fraudulent campaign activity aimed at the public that involves assuming the identities of government institutions and well-known companies. New attack vectors: smart TVs, voice spoofing, double extortion. There is an increase in business e-mail compromise (BEC) and encrypting ransomware virus activity. Global-scale login data leaks (from Google, Facebook, Apple, and others) have taken place that increase the likelihood of cyberattacks in Latvia.

DDoS attacks remained intense with seasonal peaks, especially around holidays and politically important events; however, these are mostly fought off automatically. Meanwhile, no cyber incidents or cyber threats that could indicate any external attempts to influence this year's elections were detected in Latvian cyberspace during, before, or after the elections. This points to the effectiveness of the preventive cybersecurity measures taken by CERT.LV.

The intensity and complexity of cyberattacks that pose a high risk for the general public, businesses and institutions is increasing in Latvian cyberspace. Cyberattacks directly and indirectly affect people's financial assets, and the impact of these attacks is becoming increasingly tangible. A negative trend like this can affect the level of trust in digital services among the public.

In order to strengthen cyber resilience in the country, one must ramp up public education and cyber hygiene efforts, improve the technical security capabilities of organisations, and foster the use of AI and data telemetry in security. CERT.LV services, such as its Security Operations Centre, threat hunting, security testing, and training, play a strategically important role in mitigating the threats and are essential for strengthening the country's resilience in the field of cybersecurity. If Latvia is to avoid gaining the reputation of an 'easy target', it must demonstrate resilience and strategic vigilance based on its capacity to identify threats and act on them in time.

We are proud of Latvia's successes, as for the third year in a row, the Latvian team maintained its global top-five position in NATO's extensive Locked Shields exercise, ranking 4th this year. Its special achievement is 1st place in the Cyber Security and International Law category, showing that even a small country can be a major player in global.

1. Cybersecurity threats: statistics and trends

The intensity of cyber threats aimed at Latvia increased in Q2 2025 compared to before the 2022 Russian invasion of Ukraine. The variety of threats is rising, and so is their technical and psychological complexity.

Since the beginning of 2025, Latvian cyberspace has seen a **sharp increase in the number of manually processed cyber incidents**. The peak of 733 cyber incidents was in Q3 2022, with another spike in Q3–Q4 2023, and then again in Q2 2025, with **709 cyber incidents** recorded[1]: an **increase of 12%** quarter-on-quarter and 28%, year-on-year. This increase correlates with the global escalation of cyber threats and growing digital dependency among the general public, as well as the human factor. The rise of AI plays a significant role here, as it simplifies and speeds up fraud, intrusion and automated attacks.

The number of threatened devices identified by CERT.LV (459,346) **rose by 62%** compared to both Q1 this year, and Q2 last year. This trend suggests the growing use of automated scans and the exploitation of vulnerabilities. Configuration gaps account for most of the vulnerabilities: 93%. This points to weaknesses in the system and network security, mainly caused by the human factor and insufficient security standards. The increase can also be explained by the addition of data sources to CERT.LV telemetry data in Q2.

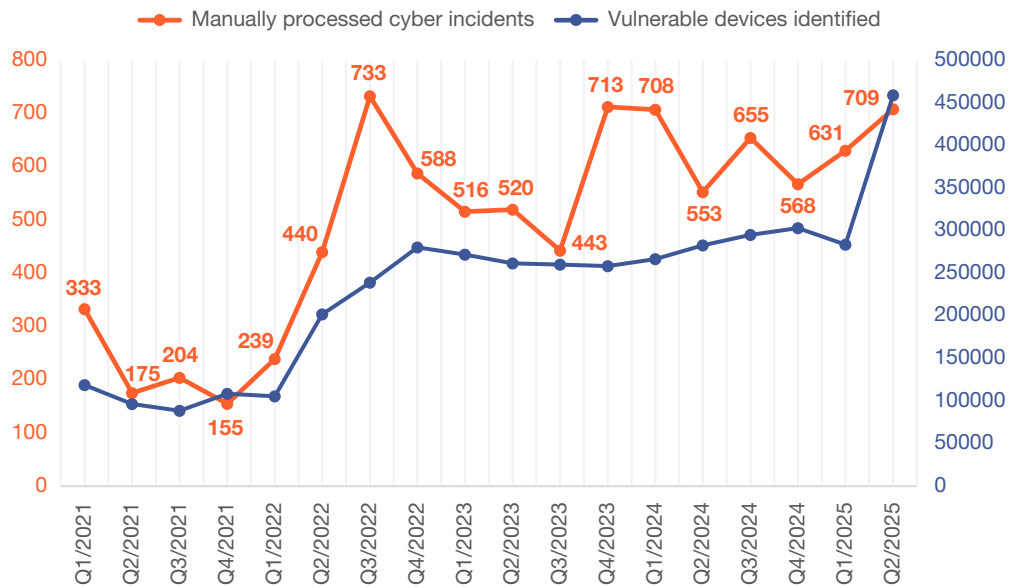

Figure 1. Number of devices exposed to cyber incidents and identified, by quarter

Key risks:

- **The amount of attempted fraud, in particular phishing campaigns** aimed at the general public, in which the scammers claim to represent government agencies, is on the rise.
- **Human factor as key vulnerability** (e.g., not using 2FA, clicking on phishing links): the human factor is a major weakness in society at large and in organisations, and it can affect the situation with cybersecurity.

1 Events that threatened data processed or the availability, authenticity, integrity, or confidentiality of services offered by or accessible through network and information systems..

- **Businesses are increasingly threatened by encrypting ransomware attacks and business e-mail compromise (BEC) attacks**, which cause financial damage and threaten their reputation.
- **Targeted DDoS attacks against critical and important service infrastructure** within the context of particular seasons and current events among the general public and in international politics. Q2 saw a significant increase (250%) in these, partly due to the addition of data sources to CERT.LV telemetry. However, the number and intensity of such attacks implies targeted attempts at continuing the use of DDoS as a means of ideological protest or undermining public trust in government digital services.
- **Increasing role of AI in cyber threats and disinformation.** There is a major trend involving the rapid expansion of the use of AI in Russian cyber operations, whereby it is becoming increasingly difficult to detect content produced by AI. Given Russia's confrontational foreign policy, as well as the information influence campaigns and operations it has carried out in recent years, there is a growing risk that AI technology could be used to target public opinion in Latvia or carry out more sophisticated cyberattacks.
- **The use of vulnerabilities, including those associated with the Internet of Things (IoT) and automation, is gaining momentum.** These threats affect the public as well as private sectors.

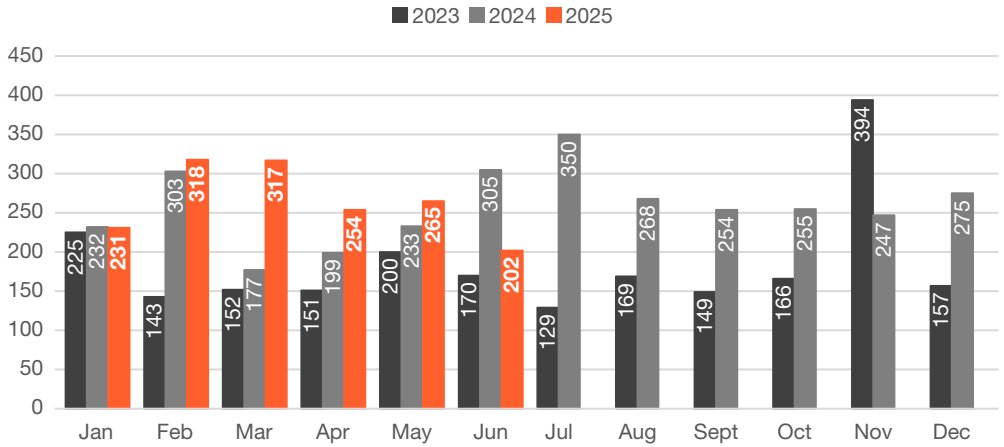

Figure 2. Cyber incident trends (monthly breakdown)

The intensity of cyber threats in Latvia remains consistently high every month. They typically have the capacity to adapt and use topics relevant to various audiences in order to achieve greater effect. The monthly **"Kiberlaikapstākļi"** ("Cyber Weather") overview highlights the 5 most prominent cyber threats in various categories (only in Latvian).

CERT.LV offers a monthly plain-language report of the critical events in Latvian cyberspace through top-5 categories, for those interested in the "cyber weather". The latest cyberspace events, threat analysis, and useful tips for the reporting period: APRIL | MAY | JUNE

2. Top reporting-period cyber threats and key events

In Q2 2025, Latvia's cyberspace saw a significant increase in cyber incidents caused by cyber threats of a number of types, marking trends that have been present for a long time.

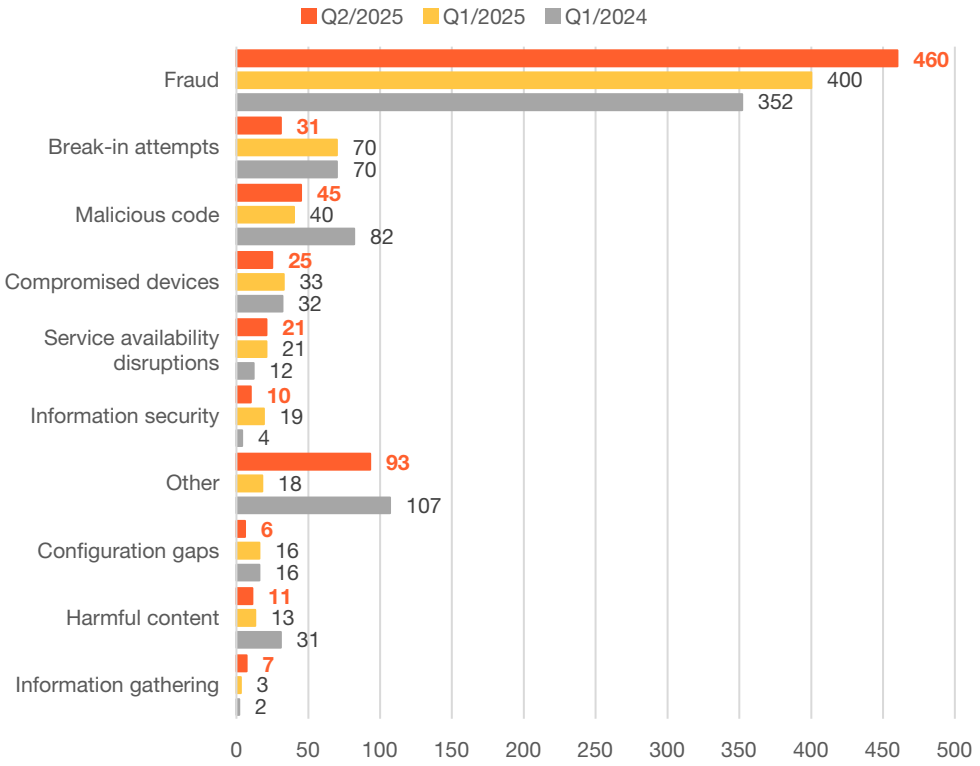

Figure 3. Quantitative comparison of cyber incident type

Ongoing presence of fraudulent activities and phishing campaigns; rising psychological manipulation quality

Intensive phishing campaigns were observed, with scammers impersonating government institutions (especially CSDD and SRS), banks (SEB and Swedbank in particular), postal delivery companies (especially Latvijas Pasts, FedEx), e-mail services (especially Microsoft Outlook), and tech companies (especially Meta). The most prominent form these campaigns took was text messages about traffic offences or unpaid fines, claiming to be from the Road Traffic Safety Directorate (CSDD) and trying to extort data and money. State Police data show that this year, more than 100 people have believed these fake CSDD text messages, with a total of 174,523 euros stolen from them .

Overall, we observe that scammers are using more and more innovative solutions, adapting their fraud techniques to particular seasons or popular trends among the public. For example, they exploited the topic of municipal elections in June, sending text messages about "annulled votes".

Fake investment and cryptocurrency schemes continue, advertised by imitating popular websites (delfi.lv, diena.lv and jauns.lv). A "double extortion" tactic was also observed, in which a fake lawyer offered the victim "assistance" in recovering their money, and defrauded them of even more.

New psychologically manipulative phone scams were recorded: scammers make multiple calls in a row to gradually undermine the victim's vigilance and direct them towards actions that may lead to disclosing their personal data or granting access to their accounts without the victim realising it. The use of generative AI to mimic voices and more easily manipulate people's emotions and trust is rising.

There were instances observed of scammers using randomly generated "eParaksts mobile" personal identity numbers/user numbers to make unauthorised purchases in the online shop, shop.banknote.lv. It has been noted that scammer activity tends to increase during public holidays, as they send fake notifications claiming, for example, that the recipient has to renew a supposedly expired "eParaksts mobile" certificate, or fake text messages with links appearing to be from the State Social Insurance Agency online service address.

2 Source: https://www.vp.gov.lv/lv/jaunums/noziedznieki-ar-iszinam-csdd-varda-sogad-izkrapusi-simtiem-tukstosus-eiro

A new wave of scams aimed at smart TVs (especially those running Android OS) was observed. As part of these attacks, scammers took targeted steps to trick users, for example, into installing malicious apps that ask for personal data. A few of such cases were recorded in Latvia, indicating that this type of fraud has seen success.

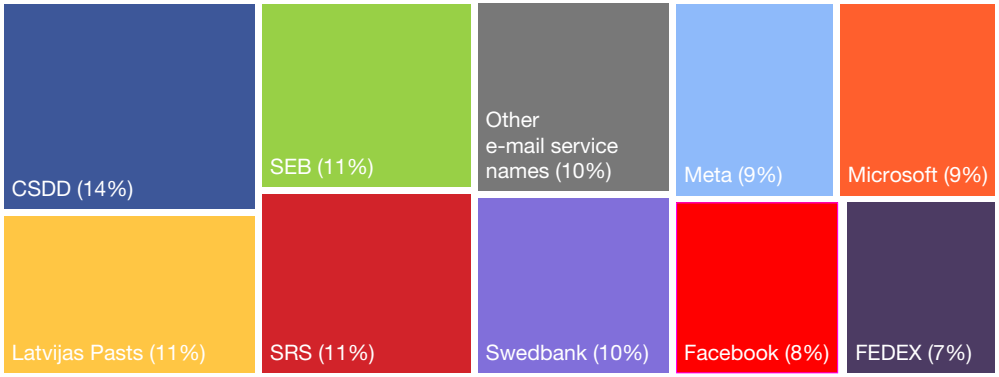

Figure 4. Top phishing campaigns assuming names of well-known organisations (as a share of total phishing reports processed by CERT.LV in Q2 2025)

Business e-mail compromise (BEC) incidents rising

As part of targeted cyberattacks, a couple of companies received multiple invoices with fake account numbers, and having paid them, suffered significant financial damage. The gaining of access through the leaked e-mail credentials of a company manager emphasises the critical importance of 2FA: not using 2FA is a critical vulnerability.

Growing encrypting ransomware virus risks

Ransomware virus attacks are an increasingly serious threat to Latvian companies, capable of paralysing their work and causing extensive financial losses. Furthermore, the spread of the 'Ransomware-as-a-Service' (RaaS) model makes these attacks accessible to a larger group of criminals. A dangerous ransomware virus of the Mallox subtype, which operates under RaaS, affected two companies in the agricultural sector. The 'Jelgavas tipogrāfija' printing house also suffered an encrypting ransomware virus attack: the company has an annual turnover of 17 million euros, and the losses it suffered could amount to a quarter of that amount as it was forced to suspend its operations because its data were encrypted.

Fluctuating global politics event-related DDoS attack trends persist

In April 2025, a cyber incident was observed involving a DDoS attack that briefly disrupted access to a political party's website and e-mail server. During the May holidays, DDoS attacks against government assets rose by 40%, with particularly intense attacks against those in the financial sector. Notably, on 9 May, a DDoS attack was launched against the website of the Museum of the Occupation, but was unsuccessful. DDoS attacks did not leave a lasting impact overall, with most of them being thwarted automatically.

As part of its preparations for the municipal elections that took place on 7 June, CERT.LV proactively implemented a number of preventive measures, improving its capacity to respond to potential cyber threats. No cyber incidents or cyber threats that could indicate any external attempts to influence this year's elections were detected in Latvian cyberspace during, before, or after the elections.

Data theft malware more advanced and harder to detect

Here, the predominant vector comprised vulnerable websites based on the WordPress content management system and infected with malware. The public was also actively warned about the spread of fake-CAPTCHA malware intended to steal personal data on infected websites, with several victims recorded in Latvia.

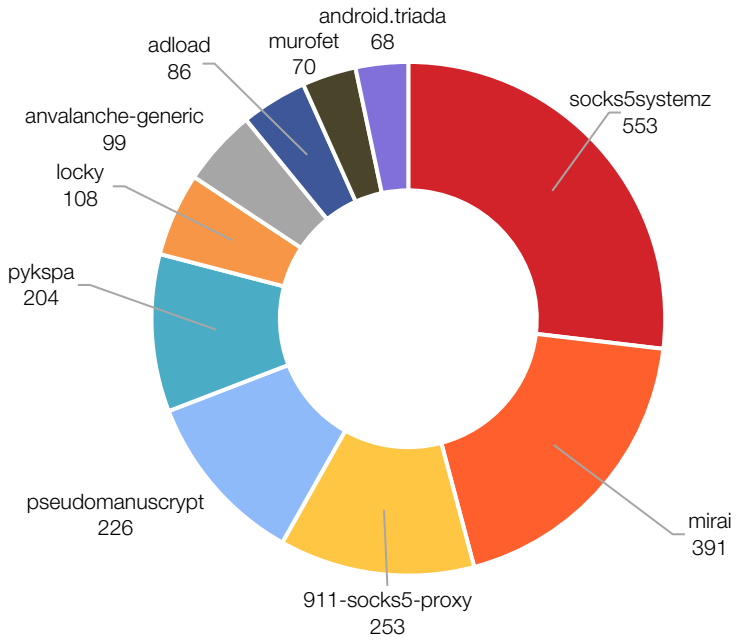

Figure 5. Top 10 malware in Q2 2025, by number

Rising vulnerability use

In the international context, the activities of the APT28 group, sponsored by the Russian state, which exploited XSS vulnerabilities in popular e-mail servers (Roundcube, Zimbra, etc.) to steal confidential data and attack the e-mail accounts of government agencies and defence industry organisations, mainly in Ukraine and Eastern Europe, stand out for their potential impact. These are high-level cyber intelligence operations with potentially serious national security implications, especially in relation to the support of Ukraine. Latvian organisations that do not update their e-mail servers in time are also exposed to this risk.

Large access data leak incident with high risk, also for Latvia's residents whose data may have been compromised

The web's biggest data breach ever was discovered: access data for more than 16 billion accounts on popular services such as Google, Facebook, Apple, Telegram, and others were published. The data can be used to break into accounts, commit fraud, etc. Much of the data may have been obtained via data-theft malware, and are likely to have been collected from many sources over a long period. CERT.LV urges all users to take proper security measures (use a unique password for every website, set up 2FA wherever possible, refrain from opening suspicious links, and install updates).

Risks created by IoT and automation devices expected to increase significantly

IoT devices that are smart and connected to the internet often become the weak link in network security and an easy target for building up botnets, which are later used in large-scale DDoS attacks. The predominance of automatic bot traffic (studies show that more than 50% of internet traffic is created by bots, 37% of which are malicious) signals a new cybersecurity era, in which defence systems must be capable of tackling AI threats.

Main conclusions

Latvia's cyberspace has seen both a qualitative and a quantitative increase in cyber incidents, threats and vulnerabilities that affect the reputation and operational continuity of organisations. Cyberattacks directly and indirectly affect people's financial assets, and the impact of these attacks is becoming increasingly tangible as the spread of tech in everyday life continues. A negative trend like this can affect the level of trust in digital services among the public.

The human factor remains the central source of risk. Critical thinking, cyber hygiene and public awareness are still insufficient, which makes organisations vulnerable to social engineering and scamming attacks. It is necessary to bolster the technical security of organisations, as well as cyber hygiene and the critical thinking of individuals.

Meanwhile, one must also build the public's resilience to disinformation and activities aimed at influencing information. The capacity of the government for the early identification of influence operations and maintaining a dialogue with the public becomes a critical security guarantee.

Another important element is the use of real-time telemetry, security testing, and the implementation of AI technologies in the cybersecurity of organisations. Russia's aggression is likely to also continue in cyberspace: demonstrating resilience and taking preventive action will be vital in pursuing a strategy of deterrence, making sure that Latvia does not appear to be an easy target.

3. CERT.LV services: monitoring, protection and testing

CERT.LV services, including the DNS firewall, support resolving incidents, Security Operations Centre (SOC), cyber threat hunting, security testing, education and training activities for the public, as well as other services, are an essential asset for mitigating risks and building resilience to increasingly intense and sophisticated cyber threats.

DNS firewall

In Q2 2025, as part of the DNS firewall service:

- **The number of malicious domain name DNS requests** reached 2,532,552, a 255% quarter-on-quarter increase, and 219%, year-on-year. A very large number of requests for SEB, Swedbank, and various infected WordPress pages stands out in particular, though in most cases, there is virtually no actual human activity clicking on these pages, and they are likely to have been automated requests – for example, by firewalls or proxy systems that regularly check domain reputation.

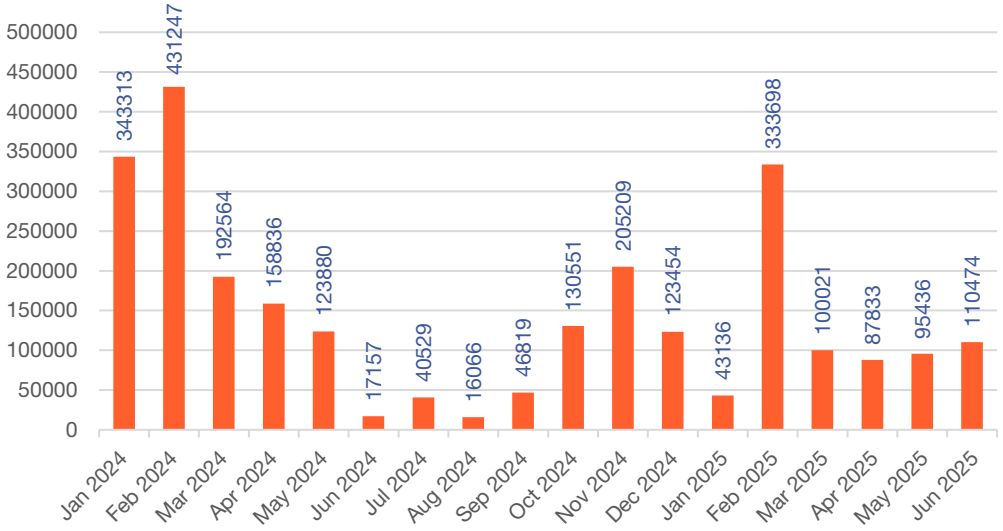

Figure 6. Cyber attacks repelled across all CERT.LV zones

- **The cyberattacks repelled across all CERT.LV zones prevented users** from visiting malicious websites 293,743 times, which is38% less compared to Q1, and 2% less than in Q2 last year. The reasons for the decrease could be seasonal or related to particular periods, with a cyclic drop that may flip in the next quarter. The number of attacks defended against also has a direct correlation with the number of active fraud campaigns.

Major active defence episodes during the reporting period

Warnings	Quantity
Vulnerable websites based on the WordPress content management system and infected with malware.	**24 874**
Fake online shops using well-known brand names.	**23 357**
Advertising of gambling through infected websites.	**8 115**
Use of Jauns.lv branding in fraudulent cryptocurrency investment platform advertising campaigns.	**6 207**
Use of Latvijas Pasts branding in fake website campaigns.	**6 120**
Use of DELFI branding in fraudulent cryptocurrency investment platform advertising campaigns.	**4 284**
Use of State Revenue Service branding in fake website campaigns.	**2 249**
Fraudulent payday loan websites.	**1 875**
Use of DIENA branding in fraudulent cryptocurrency investment platform advertising campaigns.	**1 727**
Use of CSDD branding in fake website campaigns.	**1 522**

Threat early warning system

The IT Security Threat Early Warning System (EWS) is a CERT.LV service that analyses traffic anomalies and identifies signs of cyberattacks in the service recipient's infrastructure. At the end of the reporting period, the number of alerts generated by EWS was about **1.7 billion**.

The most common high-priority cyber threat alerts by CERT.LV Signature Group were related to computer viruses, phishing and potentially malicious websites, as well as to botnets, scams and virus indicators.

Every month, ABS records an average of **6000** high-priority cyber threats (incidents with high danger potential) in national and municipal-government, and ICT-critical infrastructure.

Security Operations Centre (SOC)

Between 2024, when the provision of the CERT.LV SOC service began for institutions, and the end of Q2 2025, **visibility was achieved for a total of 33,828 devices** (servers and workstations). In Q2, the number of end devices increased by **25,419, about 75% of the total, with a resulting** rise in the number of security alerts.

More than 10 million security alerts were registered during the reporting period, almost 9 times more than in Q1. This spike in the number of security alerts detected by SOC is mainly due to the increased visibility achieved in the infrastructure of new clients.

As a result of processing the security alerts, 375 cases were manually opened in Q2. In 172 (46%) of these, the clients were contacted to obtain additional information and inform them about a cyber threat or a cyber incident.

1 cyber incident detected: malware in the Windows activation tool aimed at stealing data via an employee workstation. The workstation was reinstalled, and user passwords were changed; no further impact of malware has been noted in the infrastructure.

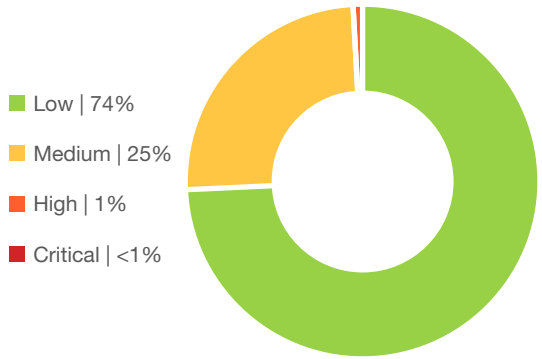

Figure 7. Security alert level: security alerts recorded by SOC in Q2 2025 (percentage share of total)

Cyber threat hunting operations

Between 2022 and the end of the reporting period, a total of **160,000** ICT infrastructure end devices of essential and significant service providers, as well as government agencies, were analysed as part of cyber threat hunting operations. In Q2 2025, the number of end devices **increased by 5000**.

Cybersecurity cooperation between Latvia and Canada continues, which is particularly important given the political situation in the region and potential threats from third countries. A month-long threat hunting operation with an expanded presence of allies led by CERT.LV came to an end.

IT system security tests and phishing attack simulation campaigns

During the reporting period, CERT.LV performed **11 IT system security tests**, 10 of which were for systems associated with elections. **2 phishing attack simulation campaigns** were carried out, improving the skills of the staff of the institutions in identifying social engineering attacks and mitigating human factor-associated risks.

Coordinated vulnerability detection (CVD)

The CVD reporting practices facilitate the earlier discovery of vulnerabilities, helping coordinate their investigation and elimination, while achieving better efficiency in organising security measures.

As of the end of the reporting period (30.06.2025), the following was recorded on the CVD platform overall:

- Security researchers: 114 active (increase of 21 in Q2)
- New institution programmes: 13

As of the end of the reporting period, a total of 215 vulnerability reports (increase of 55 in Q2) were recorded, including:

- Vulnerabilities among CERT.LV clients: 103 (increase of 28 in Q2)
- Vulnerabilities reported in institution programmes: 112 (increase of 27 in Q2)

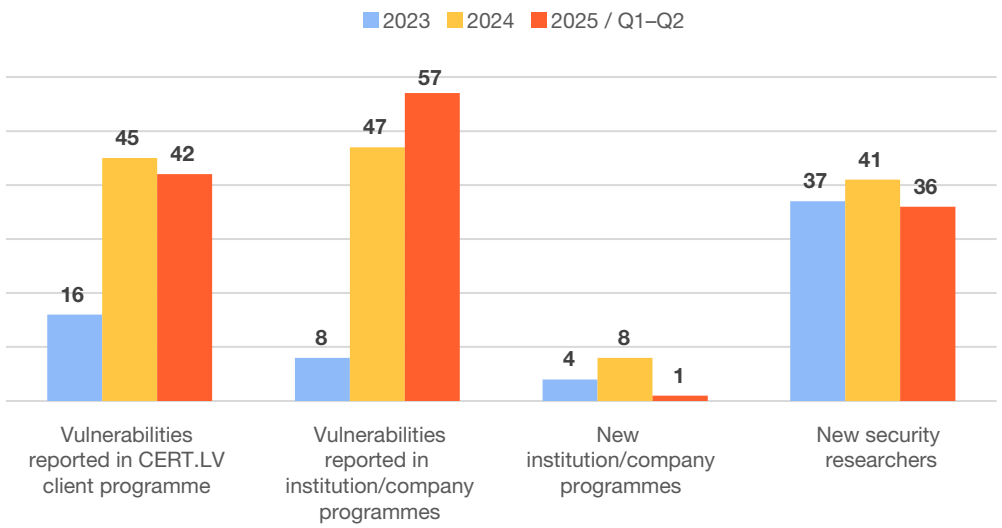

Figure 8. CVD platform: Number of vulnerability reports in Latvia

CERT.LV offers a broad range of cyber security services that effectively protect the ICT infrastructure of organisations and bolster their cyber resilience.
Protect and secure your cyberspace today with the expertise and advice of CERT.LV: https://cert.lv/lv/pakalpojumi
If you would like to receive a CERT.LV service, please write to us at cert@cert.lv

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.

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

Contact CERT.LV:

Phone: +371 67085888

E-mail: cert@cert.lv

Website: cert.lv

Follow CERT.LV news on:

@cert.lv