CERT.LV ACTIVITY REVIEW

Q2 2024

CERT.LV
Information Technologies Security Incident Response Institution

Institute of Mathematics and Computer Science University of Latvia

Ministry of Defence Republic of Latvia

Latvia faces a persistently high level of cyber threats driven by financial, political, and ideological motives. The cyber threat landscape is evolving with increasingly sophisticated attacks that exploit human error and technological weaknesses. Attackers skillfully use phishing, targeted malware, and weak authentication mechanisms to breach defenses.

In Q2 2024, CERT.LV registered 388,922 threatened unique IP addresses, which was the highest number in two years. Quarter-on-quarter, the increase is 11%, and 16%, year-on-year.

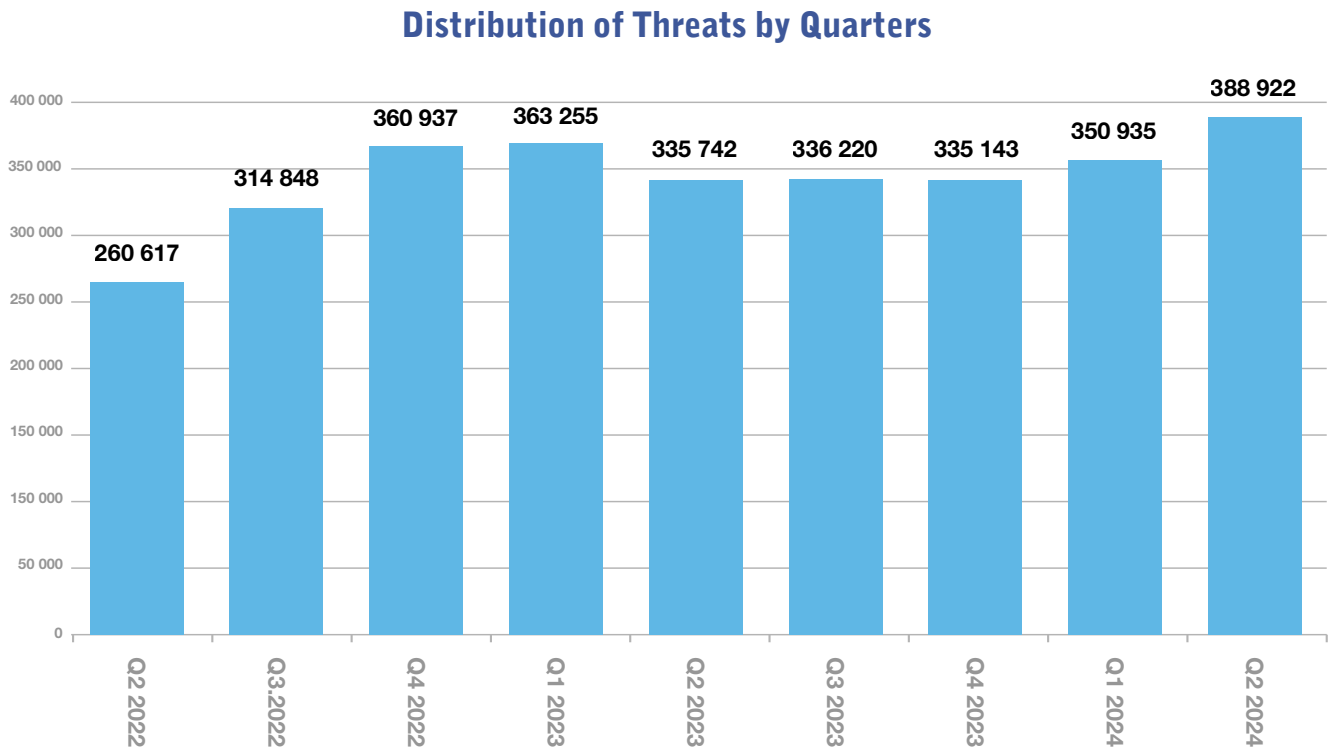

Figure 1. Distribution of Threats by Quarters

At the same time, the cyberspace situation is considered stable, and cyberspace itself, well-protected. Latvia's information and communication technology (ICT) infrastructure is increasingly resilient to cyberattacks: so far, these have not had a significant or lasting impact on the public, its security, and essential services. We can be proud of our excellent cybersecurity professionals. However, we should not rest on our laurels, as changes in cybersecurity are constant, making it necessary to look for and implement new measures that improve cyber resilience.

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

Biggest cybersecurity threats: statistics and trends

During the reporting period, one major cyberattack was recorded at a governmental institution, where VPN without two-factor authentication was used. However, the attack did not have a lasting effect on the public. Significant threats with an extensive impact on the private sector, and on national and municipal authorities, account for 0.02% of all

categorised threats, which is almost half the level of Q1, but 75% more than in Q2 last year. Meanwhile, significant, medium-impact threats represent 0.65% of all categorised threats: the number of threatened IP addresses is 11% higher than in Q1 and 16% higher than in Q2 last year.

Compromised devices, malicious code, and break-in attempts were the kinds of threats that saw the highest increase in activity in Q2 2024. The number of attempted break-ins continues to rise, reaching its highest level in the last two years, with an increase of 56% since the beginning of the year, and more than doubling since Q2 last year. From a geopolitical perspective, this can be explained by Russia-sponsored cyberattacks and efforts to compromise the critical ICT infrastructure of NATO and EU member states, which have been unwavering in their support for Ukraine's people in their fight against Russia.

> **"The current threat level has not decreased in any area, but we have learnt to handle threats a lot better.** Automated solutions deter many attacks, providing some relief for us and other institutions. However, we continue to work diligently to address ongoing challenges."
>
> Baiba Kaškina, head of CERT.LV

The findings of CERT.LV threat hunting operations are concerning, as almost a quarter of public sector institutions suffered, more or less, from cyberattacks linked to operations sponsored by other countries (including Russia). Cyber attackers supported by hostile countries, including Russia, used a variety of intrusion techniques to gain access to critical government and ICT infrastructure assets, including authentication spoofing, exploiting publicly known vulnerabilities, compromising websites, compromising VPN and e-mail gateways, phishing, and targeted delivery of malware via e-mail. Such trends point to the necessity to ramp up security efforts and educate the public about potential cyber threats.

This underscores the necessity of monitoring compliance with the country's minimum cybersecurity requirements and ensuring the availability of effective cybersecurity services. Additionally, the processing of ICT security telemetry is crucial to providing high-quality support for the public sector's technical and human resources, enabling them to counter growing cyber threats and meet current challenges.

CERT.LV offers a broad range of services for the controllers of critical ICT infrastructure, including phishing attack simulations, cyber threat simulations, early warning systems, CERT.LV MISP (malware-related information sharing platform), threat hunting operations, as well as the services of the CERT.LV Security Operations Centre (SOC).

During the reporting period, CERT.LV made significant enhancements to the framework of its services, developing new solutions and refining related procedures. To learn more about the free services provided by CERT.LV, please, visit https://www.cert.lv/pakalpojumi.

Notably, on 20 June 2024, the Latvian Parliament passed the National Cyber Security Law (NCSL), taking a significant, major step towards strengthening cybersecurity in Latvia and complying with the requirements of the revised European Union (EU) Network and Information Security Directive (NIS2). NIS2 aims to achieve a uniformly high level of cybersecurity across the EU. CERT.LV continues its efforts to clarify the new legislation and is preparing guidelines to support the entities subject to NCSL in implementing its new requirements.

COMMENT BY CERT.LV EXPERTS

There are a few trends affecting the situation with cybersecurity in Latvia, including the increasing incidence of ransomware and data-stealing viruses, malicious cyber operations sponsored by other countries, and the growing cyber threats to critical ICT infrastructure. The dynamic nature of cyber threats requires constant vigilance and adaptation, given the advancing integration of AI in offensive and defensive cyber operations. The potential vulnerabilities in the internet of things also create increasing risks as the space for cyber-attacks expands. In working to achieve good cyber hygiene practices, every organisation must emphasise strong password policies, multi-factor authentication, and regular software updates. Sharing information and cooperating with international partners (NATO, EU, EU CSIRT, CyCLONe, ENISA, etc.) are essential in countering new cyber threats.

Scale of fraud picking up pace

In Q2 2024, the number of unique IP addresses registered by CERT.LV as exposed to 'Fraud' threats rose by 45% compared to Q1 this year and 70% compared to Q2 last year, with at least 1 million euros defrauded every month.

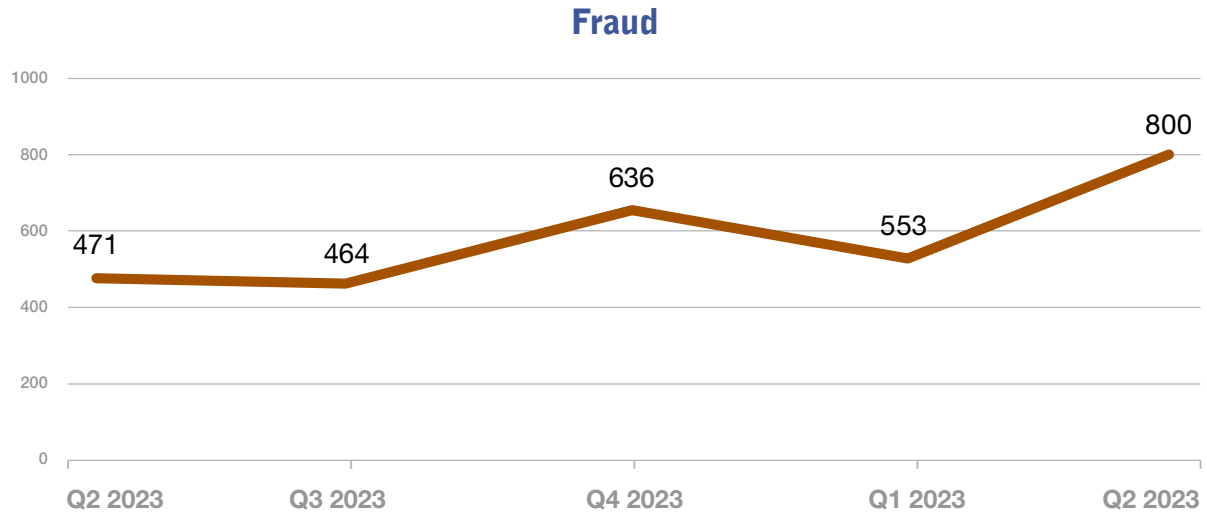

Figure 2. Unique IP addresses exposed to fraud threats

The 3 most common types of fraud are vishing, phishing, and SMS phishing. In most cases, large quantities of text messages and e-mails are sent with fake links, embedded QR codes, or malicious attachments disguised as invoices, pretending to come from various government agencies, courier services, and financial institutions. Scammers keep up to date with the latest events and step up their activities by using them, an example highlighting this is: timing fraudulent activities with deadlines for the submission of tax returns. Fake calls and compromised business correspondence have become a serious problem affecting many businesses and private individuals. User carelessness and poor cyber hygiene increase the risks of fraud.

CERT.LV promptly includes indicators of fraudulent activity in its DNS firewall to prevent users from accessing malicious sites and instead redirects them to a warning page. Even if malware has already infected a device, the DNS firewall makes it possible to identify such devices in time, enabling system administrators to mitigate the damage and promptly clean up the consequences.

CERT.LV urges people to be vigilant, to think critically about every request to share personal details, and to use the DNS firewall for their own protection: CERT.LV and NIC.LV provide this active defence tool free of charge.

Service availability

Waves of denial-of-service (DDoS) attacks, including cyberattacks by Russia and hacktivists supporting it that target government agencies and businesses operating in certain sectors continued but were successfully repelled, in many cases automatically. Compared to Q2 2023, the number of DDoS attacks almost halved. This is not a coincidence Latvia has developed strong defenses, making itself a challenging and unattractive target for cyberattacks.

However, the difficulty of the task has not diminished, as the Baltic region faces its own particular challenges due to higher risks of cyberattacks orchestrated by hostile states. Ideologically or politically-motivated cyber attackers integrated with the power structures of Russia persist in their interest in Latvian assets. Their aim is to overload the internet infrastructure of Ukraine's supporters in NATO and EU member states (including Latvia). Accordingly, system controllers must continue to develop and improve DDoS protection mechanisms, and follow the advice of cybersecurity experts.

It is essential to prevent the involvement of Latvia's ICT infrastructure in cyberattacks, as Russian-linked telecommunications companies are deliberately buildingpresence in Latvia and other EU member states.

Security experts warn that to conduct their attacks, cyber entities in hostile countries often use the devices of private individuals, such as Wi-Fi and IoT devices. Cybercriminals are constantly on the lookout for vulnerable network devices, using both manual and automated tools for detecting these. Hijacked network devices then can be used to conduct DDoS attacks.

The most common DDoS attacks take place using remotely controlled devices that have been taken over by the cyber attacker. The cyber attacker can also use hijacked network devices to cover its tracks or launch attacks from IP addresses in the target country. The latter method is particularly effective because malicious traffic coming from a local ISP's network is not as easy to detect as malicious traffic coming from a network abroad.

Shortly before the European Parliament (EP) elections, Telegram accounts of Russia's supporters spread calls to disrupt the election process in Latvia and other EU member states, even if without success. In Latvia's cyberspace, the EP elections took place without incidents. There were no incidents observed in Latvia that were targetting election systems or election security.
A cyberattack before the Midsummer holidays disrupted the Smart-ID electronic identification and signature tool, disrupting users ability to use Smart-ID application. The cyberattack against Smart-ID only temporarily affected the general availability of the service, but did not compromise the security of user data. This cyberattack once again demonstrated the importance for diversifying the available authentication solutions to the public. In this case, bank customers were able to use other available authentication tools like eParaksts mobile and code calculators.

Vulnerabilities and flaws in configurations

This is an ever-present risk, which is affected by newly discovered critical vulnerabilities, incorrectly configured IT systems, and supply chain attacks. In Q2, CERT.LV issued 16alerts on newly discovered critical vulnerabilities and exposures (CVE), which included directly informing the controllers of the vulnerable systems, and supported incident analysis and clean-up, providing coordinated instructions and recommendations for the better management of cybersecurity. Most cyberattacks still use publicly known vulnerabilities rather than unknown, recently discovered vulnerabilities, therefore early identification and remediation of deficiencies in configurations can significantly improve the cybersecurity posture of an organization.

The number of configuration flaws continued to rise during the reporting period, reaching its highest level in the last 22 months. They still account for the majority of all of the threats in Latvian cyberspace recorded by CERT.LV.

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

Malicious code

In Q2 2024, the number of unique IP addresses threatened with malicious code and registered by CERT.LV slightly decreased compared to the previous quarter, but rose by 74% year-on-year.

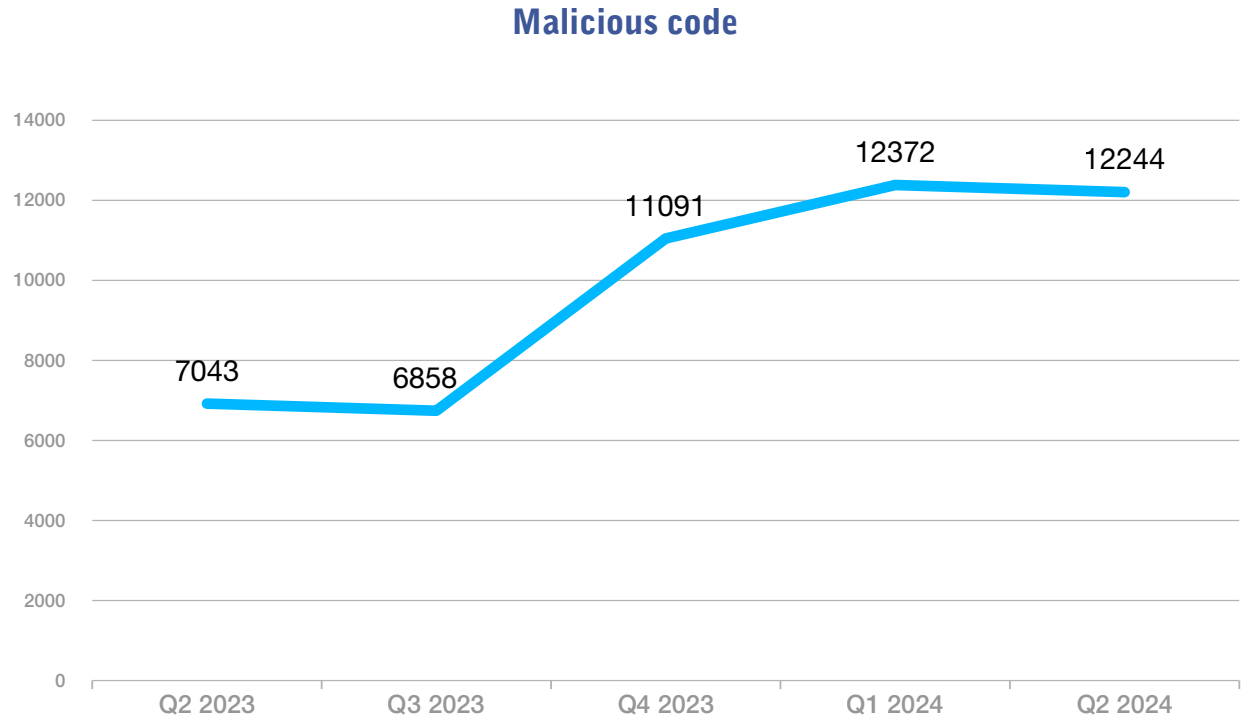

Figure 3. Unique IP addresses exposed to malicious code threats

The most common methods used to hack into and infect systems are: phishing, exploiting publicly known vulnerabilities, abuse of services exposed to the web due to incorrect configuration (default authentication credentials, brute-force password cracking, version vulnerabilities), infected storage media (USB flash drives), leaked and easy-to-guess user passwords, etc.

The main types of malware during the reporting period were: user data theft tools, botnets, ransomware, remote control malware aimed at the retrieval of data or compromising of infrastructure.

The number of unique IP addresses in Latvian cyberspace facing threats remains alarmingly high. Malware is primarily deployed for two key purposes: data theft and financial gain. When a user opens a malicious attachment, their device becomes infected, allowing the malware to harvest sensitive information such as usernames, passwords, cryptocurrency wallets, and access credentials. This data is then transmitted to infrastructure controlled by the attackers. In most cases, 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.

The amount of fraud schemes against companies increased significantly, ranging from sending fake invoices and requests to change bank account details in order to get them to pay the attacker, to phishing e-mails aimed at pursuing the attackers' financial goals. Compromised e-mails and app accounts are used to spread malware.

Break-in attempts

During the reporting period, cyber intrusion attempts affected more than 1500 unique IP addresses, reaching the height over last two years. The number of attempted break-ins have risen by 56% since the beginning of the year, more than doubling since Q2 last year.

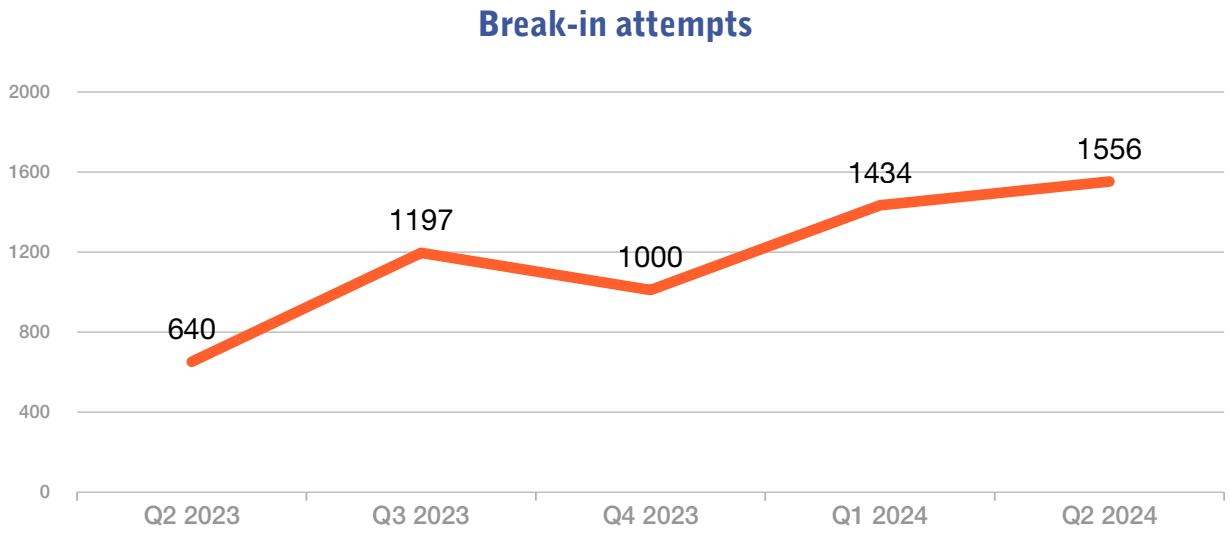

Figure 4. Unique IP addresses exposed to break-in attempts

The majority of cases involved brute-force password cracking aimed at telecommunications companies, some national and local agencies, as well as private businesses.

Break-in attempts also exploit long-known configuration weaknesses in commonly used products. Cyber criminals also work hard to penetrate into the internal networks of organisations, exploiting newly discovered vulnerabilities to gain unauthorised access to personal data and sensitive information, to encrypt data on devices and extort money for the recovery of the data.

One cyberattack on a governmental institution recorded during the reporting period was carried out where VPN gateway software that did not use the two-factor authentication. The cyberattack had no permanent effects. Its limited duration prevented the attackers from taking additional actions to investigate or compromise the network. This cyber incident once again stresses the necessity of two-factor authentication. The CERT.LV early warning system also detected this type of cyberattack against another government agency, but it was not successful.

Compromised devices and data leaks

During the reporting period, there were cases of compromised devices, which affected individuals, as well as private and public organisations. The most common methods used to break into systems were: phishing, exploiting publicly known vulnerabilities, malicious use of services exposed to the web due to improper configuration, installation of pirated software, leaked, easily guessed passwords that are stored in an unencrypted form, automated cyberattacks, and user social media accounts compromised through social engineering.

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

1) lack of centralised data collection and analysis of audit trails;

2) absence of network segmentation and IT infrastructure inventory;

3) incorrectly configured or non-existent SIEM system;

4) incorrectly configured or non-existent user rights management and executable file policies.

Cases have been documented in which computer passwords were stored unencrypted locally on an infected computer, so if the device was infected, the attackers would gain access to multiple user accounts for which two-factor authentication had not been activated.
Organisations often face increasingly sophisticated cyber threats. Cyberattacks against companies are designed to break into their systems undetected and steal the information the intruders need. So they try to behave as

inconspicuously as possible in order to continue stealing information for as long as possible. Phishing attacks are also frequently used by the cyber units of Russian special services to gain access to the e-mail accounts and computer networks of various institutions.

Cyberattacks using the so-called supply chain method went up during the reporting period. In April and May, there were reports of attacks aimed at compromising the supply chain of TV channels broadcast in Latvia. These cybersecurity incidents clearly demonstrate the importance of supply chain security. CERT.LV would like to stress that these were not cyber-attacks intended against Latvia's ICT infrastructure as such, instead these can be interpreted as being a part of Russia's hybrid war. Such provocations are likely to continue in the future, and we need to be prepared for them.

A political party's website was compromised shortly before the European Parliament elections in Latvia. The cyberattack resulted in the leaking of the site's content management system administrator data, including access passwords. CERT.LV supported the investigation within the scope of its competence and found out that the victim's computer was used to retrieve passwords for accessing the server hosting the party's website. The website was temporarily unavailable, but its content was not distorted. There is no reason to believe that the cyberattack was linked to the elections.

Preventing cyber threats

DNA firewall effectiveness: In Q2, the DNS firewall service handled more than 1 million requests, protecting the service's users from malicious websites. Every detected threat indicator goes into a centralised active protection infrastructure to protect all Latvian citizens and organisations using the free protection provided by CERT.LV and NIC.LV.

Early-warning sensor network (ABS) effectiveness: Every month, ABS records an average of 6000 high-priority incidents in governmental, local municipality and ICT-critical infrastructure. In Q2, the number of warnings generated by ABS almost doubled compared to the first quarter. This increase was mainly due to very large-scale phishing campaigns, in which the attackers pretended to work on behalf of the State Revenue Service (SRS) and the Latvijas Pasts postal service, breaking all previous records during the reporting period. This is largely due to the fact that spring marks the beginning of the annual income tax return submission period to the SRS, leading to an increase in emails about tax overpayments The rise in online shopping has led to scammers impersonating Latvijas Pasts, and falsely claiming that the recipient needs to update their delivery address. Such fake messages were being sent almost daily.

Coordinated vulnerability detection (CVD) platform: Q2 was particularly productive in the continued development of the CVD platform: the number of security researchers rose by 57%, while the number of vulnerabilities recorded in specific software used by official institutions increased by a factor of five, and the number of reports of vulnerabilities among CERT.LV clients tripled.

Strategic partnerships in Latvia

Security tests: CERT.LV closely cooperated with the Central Election Commission, the State Chancellery, and other institutions involved in the election process, performing penetration tests on all systems involved in conducting the European Parliament (EP) elections. There were no incidents observed in Latvia that could be directly linked to election systems or overall election security.

Threat hunting operations: With more than 140,000 devices in 31 organisations analysed by the end of the reporting period, Latvia is the European Union's leader in organising and conducting threat hunting operations. Results of these operations show, that for a quarter (8) of the organisationsthe presence of a foreign Advanced Persistent Threat (APT) actor was identified with high confidence. The attacker's access was successfully removed. Threat hunting operations allowed discovery of additional significant threats, with information presented to the target organizations, these were then able to address these threats effectively through data-driven decisions.

At the end of the reporting period, CERT.LV concluded an threat hunting surge operation with representatives of the Canadian Armed Forces Cyber Operator, the Canadian Centre of Cyber Security, and the Latvian Armed Forces. This surge strengthened and supported the continually ongoing threat hunting work. A few allied countries were present during the surge to learn from the successful cooperation between Latvia and Canada and to possibly adopt the good practices to potentially implement this in their own fields of responsibility.

During the surge, further attesting to the strategic importance of the cooperation between Latvia and Canada, there were several visits by high-level officials from Canada: Canada's Ambassador to NATO D. Angell, Canadian Defence Attaché to NATO Vice-Admiral Bishop, Commander of the Canadian Cyber Force Rear Admiral Carosielli, and Commander of the Canadian Armed Forces mission in Latvia, Colonel V.G. Kirstein.

Training and educational activities

During the reporting period, CERT.LV reached 10,742 participants via 52 educational events, improving the knowledge and skills of individual users and entire organisations in ensuring the security of their data and systems. This was achieved both via traditional seminars – lectures as well as by delivering *Cybersecurity Breach Investigation Tabletop Exercises*.

International cooperation

CERT.LV continues representing Latvia and building partnerships with cyber incident response teams from other countries and 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:

- The 71st annual TF-CSIRT meeting took place in Copenhagen, Denmark, on 13-15 May, where CERT.LV expert Sanita Vītola spoke about the Coordinated Vulnerability Reporting platform and its success in Latvia, while Kristiāna Mūze-Feldberga discussed Latvia's experience in organising the annual international CyberChess conference.
- On 22 May, a CSIRT Network meeting took place in Ghent, Belgium, where CERT.LV expert Aleksejs Veremejenko talked about Latvia's work in the design, development and improvement of the Graphoscope. The Graphoscope tool, developed as part of an EC-co funded project JTAN is aimed at helping analysts to correlate data from different sources and display them in a clear visual form.
- As part of its participation in FIRST, CERT.LV's experts joined the 36th annual FIRST conference FIRSTCON24 in Fukuoka, Japan, which took place on 9–14 June. Head of CERT.LV Baiba Kaškina gave opening remarks as the chair of the Membership Committee. During the conference, CERT.LV expert Rūdolfs Ķelle talked about his experience and encouraged the sharing of best practices in strengthening the security of operational networks, giving a presentation entitled 'From Laboratory to Grid: Advancing IACS Incident Response and Cyber Resilience'. Meanwhile, CERT.LV expert Bernhards Blumbergs offered the presentation 'Distributed Web Mining Approach for Contextual Cyber Threat Intelligence Acquisition'. It was based on research that Blumbergs carried out as part of a Japan international postdoctoral fellowship (JSPS).

- The global national CERT meeting took place on 14–15 June in Fukuoka, Japan, where CERT.LV experts Armīns Palms and Rūdolfs Ķelle delivered a talk on the active protection service provided by CERT.LV, the DNS firewall, and its advantages and benefits for the user.

Participation in international cybersecurity exercises:

- Locked Shields is NATO's largest cyber defence exercise, with several thousand participants from the more than 40 countries taking part in 2024. This year CERT.LV experts participated in the Locked Shields 2024 exercise planning cycle, providing support to the organisers (White Team) in writing strategic communication and media incidents of the game, preparing the Info Range of the game's environment, conducting the exercise, and assessing it.

- CERT.LV experts also participated in the main exercise forming a joint Latvian-NATO team on 22-26 April, performing tasks in the technical team (especially threat hunting and situation assessment) and in the strategic communication and legal teams. This year, Latvian-NATO joint team won 1st place in this exercise. The CERT.LV team is very proud of this achievement, as it is a confirmation of outstanding performance as cybersecurity professionals!

- On 19-20 June, ENISA hosted the Cyber Europe 2024 exercise, addressing the topics of energy sector resilience and challenging thousands of participants closely associated with cybersecurity. The Cyber Europe exercise, conducted by ENISA and organised in conjunction with CERT.LV and other participants from the EU, is designed to test our readiness to face cyber threats in a wide range of sectors. This exercise provides an opportunity for the participants to handle complex situations involving business continuity and crisis management.

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, to provide IT security support to government institutions, to 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 to 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
Information Technologies
Security Incident
Response Institution