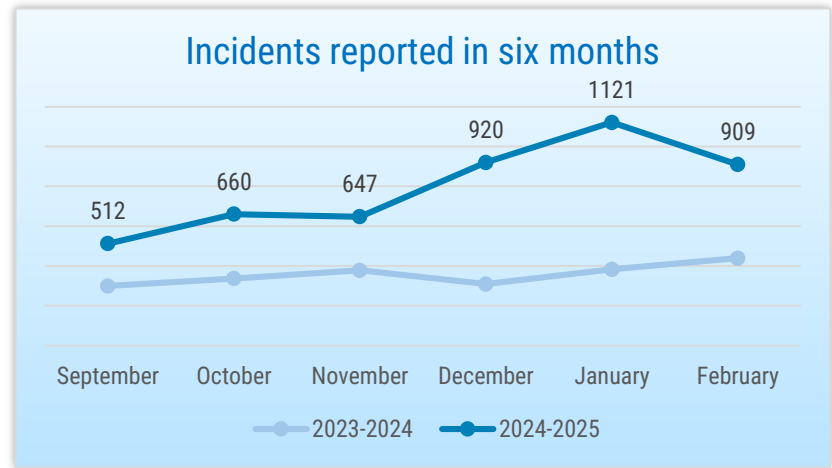




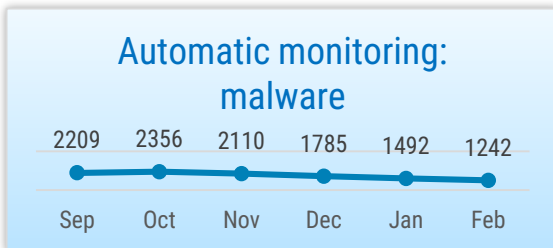
SITUATION IN CYBERSPACE

FEBRUARY 2025

- In February, we recorded 909 incidents with an impact, which is a higher indicator than the average in the last six months.
- The services of the IT and Development Centre of the Ministry of the Interior were disrupted for two consecutive days, affecting the emergency services and the police. A company operating in Tallinn fell victim to a ransomware attack.
- We organised the NB8 CIIP Summit, where Nordic and Baltic experts discussed how to provide better support to critical service providers in promoting cybersecurity. In RIA's blog, we wrote about passwords, the Signal app, and the possibilities and dangers of DeepSeek.
- A New York-based NGO called New York Blood Center Enterprises was hit by a ransomware attack. Malware was planted in the UK online shop of Casio. The Australian government banned products created by Kaspersky Lab.



Incidents reported to CERT-EE that had an impact on the confidentiality, integrity, or availability of data or information systems.



Devices in Estonian cyberspace infected with malware detected by automatic monitoring. CERT-EE notifies network owners of infections.



Phishing sites still account for the largest proportion of incidents recorded by CERT-EE.



Situation in Estonian cyberspace

In February, several services experienced disruptions.

Due to an error that occurred during a system change, there were errors in the operation of Elisa's Mobile-ID on 3 February between 2.10 p.m. and 3.17 p.m. On 24 February, Telia's Mobile-ID service was not working between 8.36 p.m. and 9.16 p.m. The reason for the outage is unknown.

The website login.alexela.ee experienced interruptions between 11.03 a.m. and 11.35 a.m. on 3 February and from 11.21 p.m. on 3 February until 2.57 p.m. on 4 February. As a result, users were unable to log in to the app or pay at Alexela petrol stations using their mobile app. Cash and card payments worked. The incident was caused by an outage in a server managed by a partner.

For two consecutive days, there were failures in the services of the IT and Development Centre of the Ministry of

the Interior. On 19 February, the emergency number 112 and the emergency call handling system SOS2 were disrupted between 12.58 p.m. and 1.35 p.m. As a result, the wait time for taking some emergency calls was longer than usual. The incident was caused by a malfunction in the SOS2 database due to a failed system change.

On 20 February, neither the border control information system PIKO nor the automated border control system (ABC gates) were functioning between 8.15 a.m. and 9.25 a.m. This outage was also caused by a failed software upgrade that disrupted the operation of the database.

On 11 February, ransomware was used for encrypting data in a server of a company operating in Tallinn.

Attackers penetrated the system through a remote desktop application (RDP) protected by a weak password. As we noted in our latest Cyber Security Yearbook regarding last year,

attackers penetrated almost one in three systems through remote desktop applications that used weak passwords and lacked additional security measures, such as a VPN, two-factor authentication, IP-based restrictions, logging, and monitoring.

February was once again rife with different types of scams, but the biggest losses were caused by investment fraud. Investment fraud offers victims a seemingly excellent investment opportunity, promising a low-risk or risk-free investment and a guaranteed return. Generally, the victims are asked to transfer money to a dubious cryptocurrency platform and shown how their investments keep growing. They will then be asked to transfer a new amount and the same sequence of actions will be repeated. At some point, the victim will want to withdraw the money, but this is not possible. We have seen losses amounting to tens of thousands of euros.



Activities of the Estonian Information System Authority

Experts from the Nordic and Baltic countries discussed how to offer better support to critical service providers in promoting cybersecurity at the NB8 CIIP Summit in Tallinn on 5–7 February.

In recent years, cyber attacks have hit critical service providers (banks, telecoms, hospitals, water and energy companies), and therefore, it is important to proactively address cyber threats. This is why representatives from cybersecurity centres in Finland, Sweden, Norway, Denmark, Iceland, Latvia, and Lithuania were invited by RIA to convene and exchange information on current common cyber threats, share experiences on organising work more efficiently, and look for ways to work even more closely together, which is particularly useful in times of crisis.

One of the most common ways of hacking into corporate and institutional networks and stealing information is to use an account and password of an employee.

We described the process in greater detail and the possible measures for protection in the [blog](#) of the Information System Authority.

We wrote a brief overview of the opportunities and risks of the Chinese AI DeepSeek-R1.

DeepSeek has reportedly been able to train its language model more cheaply compared to Western counterparts, and also requires far fewer and less powerful chips. The main concerns about using the DeepSeek-R1 model are related to censorship and data dissemination and use in China. RIA discusses it in greater depth in its [blog](#).

As some articles have recently drawn attention to the security of the Signal messaging application, we discussed it in greater detail in our [blog](#). In RIA's opinion, Signal continues to be safe to use. The application uses an open-source end-to-end encryption protocol and allows the verification of the integrity of the communication chain.

On 13 February, the traditional RIA CyberMeetUp event took place – this time with Märt Hiitamm (Head of the Analysis and Prevention Department of RIA), Kristo Timberg (Managing Director of Hansab AS), and Anto Kallas (Head of the Information Security Department of the Health and Welfare Information Systems Centre). Recordings of all the past events can be [watched here](#). The next event will take place on 20 March.

We would like to remind you that Microsoft will end its official support for a number of key software products in October. Starting from 14 October, there will be no security updates, new features, or technical support for Windows 10. Read RIA's [blog](#) for more information on software that will become obsolete this year and the risks of using outdated software.

The RIA Cyber Security Yearbook is now also available in English and can be consulted [here](#).



International situation

A New York NGO called New York Blood Center Enterprises **was hit by a ransomware attack, after which it took weeks to restore the operations of the centre fully.** It is a large chain of blood centres that collects blood from donors and supplies more than 400 hospitals in 17 states. As a result of the incident, donor appointments for blood donations had to be postponed or cancelled in several locations.

Cybersecurity firm Trend Micro published a report describing a malware campaign by Russian hackers against the public and private sector institutions in Ukraine. The campaign was discovered in September 2024, and according to Trend Micro, the attackers exploited a vulnerability in the popular archiving software 7-Zip. The targets were sent an email mimicking the Ukrainian government or private companies; the email contained an attachment that infected computers with malware when opened. This way, the attackers

managed to penetrate the network of a Ukrainian automotive company, a public transport company, a regional pharmacy chain, and a water supply company, among others.

Malware was embedded in the UK online store website of electronics manufacturer Casio, which collected the credit card details of customers. Security vulnerabilities in the popular online shopping software Magento were likely used to compromise the software. The scheme was as follows: after selecting the products and proceeding to checkout, customers were directed to a fake web page where they unsuspectingly entered their card details. An error message was then displayed and the customers were redirected to the correct payment page, but the card details had already fallen into the hands of the criminals. At least 16 other online shops were infected with the same malware.

AppSOC, a US-based company that deals with the security and governance issues of artificial intelligence, evaluated the security of the aforementioned popular DeepSeek-R1 model against a total of 6,400 tests based on various parameters and found that DeepSeek lacks several important security controls. One of the more serious shortcomings highlighted was the willingness of DeepSeek to create malware or viruses.

The Australian government has banned all products and web services from Kaspersky Lab in its systems based on an analysis claiming that the company poses a significant security risk to the country. The United States banned Kaspersky's products in government systems in 2017 and extended the ban to all US companies and consumers in 2024. The German government also discourages its companies from using Kaspersky products.