TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

December 2024

#cyberweather

Cyber weather gives you an update on the key information security incidents and phenomena of the month.

The product is primarily targeted at those who work with information security issues at different levels of organisations. Cyber weather gives readers a quick overview of recent and upcoming events in the field of cyber security.

Cyber weather can be:  calm  worrying  serious

Cyber weather, December 2024

Data breaches and leaks

- In December, we received reports about data breach attempts targeting network edge devices. If successful, these attempts may result in ransomware infections, for example.
- Cryptocurrrency accounts were hacked with the help of phishing messages sent in the name of different crypto services.

Scams and phishing

- Scammers are trying to steal online banking details with fake messages sent in the name of authorities. Advertising space in search engines has been bought for spoofed websites.
- Scams employing QR codes are often enabled by malicious scanning applications. It is still smart to ensure that the code has not been tampered with or covered with a sticker.

Malware and vulnerabilities

- Numerous reports about ransomware received in December.
- Individual reports about Lumma Stealer infections in computers.
- Vulnerability (CVE-2025-0282) in Ivanti Connect Secure already exploited. Updates must be installed immediately.

Automation and IoT

- IOCONTROL malware detected in several Israeli and US automation systems. The authors of the malware are believed to work for the Iranian state. [4]
- The location histories and owner details of electric vehicles stored unprotected on public servers have revealed the exact routes and stops of private individuals but also those of politicians and police vehicles, for example. [5]

Network performance

- Damage to submarine telecommunications cables did not have a significant impact on Finnish telecommunications.
- A few denial-of-service (DoS) attacks causing short service interruptions by flooding an online form.

Spying

- Cyber attacks against Ukraine continued. In December, disturbances were reported in a population information register.
- For example, Russia-linked APT groups Turla and Sandworm have been active in Ukraine.

NCSC-FI's tips and recommendations for improving cyber security preparedness:

The US cyber security agency CISA maintains a website called #StopRansomware. The website contains excellent up-to-date information on ransomware.[6]

ENISA, the European Union's cyber security agency, has published the final report of a Europe-wide cyber exercise. Around 5,000 people from all over Europe took part in the exercise, approximately 50 of them from Finland. The NCSC-FI was responsible for the national planning and implementation of the exercise. [7]

The NCSC-FI organised a webinar on the requirements laid down in the Cyber Resilience Act (CRA) to explain which products are covered by the Act and to give tips to help organisations prepare for the Act in advance. A recording of the webinar will be made available to share the information with those who missed the event. [8], [9]

Overview of cyber security in December

- There was a slight decrease in the number of ransomware reports towards the end of 2024
  - All reported cases concerned different variants of ransomware.
  - Network edge devices are still used to access services and systems. Vulnerabilities, flaws in processes and configuration errors expose organisations to attacks. Regular exercises help organisations prepare for various cyber incidents. We discussed this in an article in March 2024. [10]
  - Backups helped many organisations recover from a ransomware attack last year.
  - Organisations should also analyse outgoing traffic from their internal networks because in some cases the activation or installation of ransomware can be detected and prevented based on outgoing traffic.
- As in November, telecommunications cables were damaged in December
  - On 25 December, the NCSC-FI received reports about several damages to electricity transmission and telecommunications cables in the Gulf of Finland. The NCSC-FI began special monitoring of the incidents.
  - The events have not affected Finland’s security of supply, and most of the damaged cables have already been repaired. Finland is well prepared for various disturbances in electricity transmission and telecommunications. Different sectors of society work in close cooperation to prepare for disruptions and disturbances, and the authorities and companies practice the procedures together regularly.

Cyber security trends
in the past 12 months