TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

February 2023

#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, February 2023

Data breaches and leaks

- PowerApps phishing campaigns continued to cause a considerable number of data breaches. MFA is an easy method of protecion against the phenomenon.
- Criminals actively monitor information released about vulnerabilities and try to exploit them for data breaches.

Scams and phishing

- Rent-related scams tried to lure victims to transfer rent money to criminals' accounts.
- According to Finance Finland, phishing campaigns to steal online banking details caused people in Finland to lose 10 million euros in 2022.

Malware and vulnerabilities

- A ransomware campaign exploiting a VMWare ESXi vulnerability spread aggressively at the beginning of February in many countries.
- Patch Tuesday brought along patches to numerous vulnerabilities, including zero-day vulnerabilities.

Automation and IoT

- The NCSC-FI published instructions on key cyber security controls in industrial automation.

Network performance

- One significant disturbance occurred in public communications services in February.
- The number of reported denial-of-service attacks has decreased significantly compared to the volumes towards the end of 2022.
- Some of the attacks had a minor impact on service availability.

Spying

- The European Union Agency for Cybersecurity (ENISA) and the CERT of the EU institutions, bodies and agencies (CERT-EU) jointly published a report to alert on sustained activity by particular threat actors.
- ENISA and CERT-EU strongly encourage all public and private organisations in the EU to follow the recommendations put forward in the publication.

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

The NCSC-FI published new instructions on cyber threats concerning local mobile networks and the management of risks. The instructions provide information to organisations that are considering local mobile networks.

The European Cybersecurity Competence Centre's National Coordination Centre Finland (NCC-FI) began operations in early 2023 at the Finnish Transport and Communications Agency Traficom.

Operational continuity in the social and healthcare sector relies increasingly on cyber security. In Finland, cooperative efforts to improve cyber security in the sector are ongoing on many fronts, including the information sharing networks facilitated by the NCSC-FI.

Overview of cyber weather in February

- After the calm beginning of the year, report volumes have increased to their normal levels. The NCSC-FI continues to receive reports on a wide range of issues.
- Towards the end of February, we received numerous reports about a new scam luring SMS recipients to transfer rent money to criminals.
- The Western Uusimaa District Court ordered the person suspected of hacking into the patient records of the psychotherapy centre Vastaamo to be remanded.
- The number of reported denial-of-service attacks has continued to decrease.
- The vulnerability in VMWare ESXi is being actively exploited, and the exploits have had significant effects abroad.
  - In Finland, the NCSC-FI has so far only received reports about individual cases where the vulnerability has been exploited.

Cyber security trends
in the past 12 months