TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

December 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, December 2023

Data breaches and leaks

- The number of reported data breaches fell to the median level of 2023, but the number of serious data breaches increased in December.
- In several cases, systems and confidential information had been accessed with the help of hacked main user credentials.

Scams and phishing

- At the very beginning of December, we saw thousands of scam messages made in the name of MyTax (OmaVero), promising tax refunds.
- There were a lot of job offer scams in the WhatsApp messaging service.
- Signature services were used as a pretext for phishing.

Malware and vulnerabilities

- An exceptional number of reports about the Akira ransomware (6 reports in December).
- Many vulnerabilities in Atlassian products that allowed remote execution of arbitrary code have been fixed.
- Ivanti’s VPN product had two exploited zero-day vulnerabilities.

Automation and IoT

- Ukraine's security service SBU said it found hacked IoT video cameras in Ukraine that have been used for military intelligence purposes.

Network performance

- In December, there were no malfunctions in general communications services.
- Denial-of-service attacks were reported in various sectors. Most of them had no impact on the functioning of services.
- HSL publicly reported denial-of-service attacks on New Year's Eve that affected services.

Spying

- The Callisto group, which is linked to Russia, has tried to spy on targets in Western countries by sending targeted phishing messages to individuals' private e-mails. This circumvents the information security controls used by organisations.
- Callisto is also known as Star Blizzard and Coldriver.

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

Multi-factor authentication also protects user credentials in the network infrastructure and can prevent, for example, the success of a brute force attack. Check out our instructions for multi-factor authentication.

The NCSC-FI has opened applications for financial support for the implementation of modern information security solutions and innovations. Financial support can be applied for by micro-businesses and small and medium-sized businesses. Apply by 1 March 2024 at 16:15.

Traficom is preparing a recommendation on the cybersecurity risk management measures of the NIS2 directive.

Overview of cyber weather in December

- Exploitation of known vulnerabilities in data breaches continued, which was reflected in the number of ransomware cases reported to us
  - Most of the reports were about the Akira ransomware. Akira has been found to be still exploiting the Cisco network device vulnerability (CVE-2023- 20269), which enables a *brute force* attack. The success of the attack can be prevented by enabling multi-factor authentication in Cisco's VPN service.
- At the beginning of January, Ivanti published two critical vulnerabilities that affect two of its different products. Vulnerabilities have already been exploited. Numerous domestic organisations need to react to vulnerabilities immediately.
  - Based on the surveys made by the NCSC-FI, there are several hundred vulnerable servers in Finland. Software updates that fix vulnerabilities are currently not available, but quick fixes that prevent the exploitation of vulnerabilities have been published.
  - Even if measures to limit the effects of vulnerabilities are implemented, it is still necessary to analyse the system in case of a data breach that may have already occurred.
  - According to data security company Volexity, exploitation of vulnerabilities has been observed since early December 2023.

1 mo.

Cyber security trends
in the past 12 months

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Data breaches and leaks	🌦	🌦	⛈	⛈	🌩	⛈	🌧	⛈	🌦	🌩	⛈	⛈
Scams and phishing	🌧	🌧	⛈	⛈	🌧	🌧	🌧	⛈	⛈	🌩	🌧	🌧
Malware and vulnerabilities	🌦	🌧	🌧	☀	🌧	🌦	⛈	🌧	🌧	🌩	🌩	🌩
Automation & IoT	☀	☀	☀	☀	🌦	🌧	🌦	☀	☀	🌧	🌦	🌧
Network performance	🌦	🌦	🌧	🌧	🌧	🌧	☀	🌧	🌧	⛈	🌧	🌦
Spying	🌧	🌩	🌧	🌧	🌧	🌧	🌧	🌧	🌧	🌧	🌧	🌧