TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

April 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, April 2023

Data breaches and leaks

- In terms of data breaches and leaks, April was similar to March.
- Major phenomena in Finland continued to include breaches compromising corporate email accounts (M365) and social media accounts.

Scams and phishing

- Scam calls from spoofed numbers have caused the rightful holders of the numbers used in scams a lot of trouble and inconvenience. Scams have employed the numbers of both businesses and private individuals.
- April saw new aggressive phishing campaigns to obtain online banking and payment card details. Themes employed included tax returns and messages sent in the name of banks and the OmaPosti service.

Malware and vulnerabilities

- We have once again reminded people about the importance of updates and advised Apple device users to install patches for critical vulnerabilities.
- The number of reports about malware and vulnerabilities decreased compared to March.

Automation and IoT

- Every now and then, we receive reports of digital services and devices marketed to the employees of organisations. These products are often cloud-based and easy to deploy without the support of the organisation's own IT department.
- However, the deployment of digital services and devices should always be controlled.

Network performance

- Seven significant disturbances in public telecommunications services in April.
- Three of them were caused by power supply issues.
- Finland joined NATO on 4 April 2023. The day also brought along denial-of-service attacks, with a total of 7 reported cases.

Spying

- Polish authorities published a report on a widespread espionage campaign linked to cyber threat actor APT29.
- According to the report, the campaign aimed at collecting information from e.g. diplomatic entities in NATO and EU member states using spear phishing.

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

The NCSC-FI is currently surveying the state of software security in Finland. In addition to surveying the current situation, we are hoping to collect information on pain points and good practices that could help us support companies and other organisations. Respond to the survey!

The NCSC-FI, the Finnish National Bureau of Investigation and Elisa held a joint presentation on the cooperation between Traficom and Finnish telecommunications operators to prevent caller ID spoofing at the information security event RSA Conference at the end of April in the United States.

According to a thesis project carried out for the NCSC-FI, a practice facilitating the reporting of vulnerabilities is not yet widely adopted in Finland. The practice is based on RFC 9116, recommending that organisations always publish their contact details for vulnerability reports in the same place.

Overview of cyber weather in April

- Phishing campaigns targeting corporate email accounts and resulting in compromised accounts seem to change themes weekly. During the past month, we have seen at least secure email-themed campaigns and messages fraudulently representing Adobe and Microsoft OneDrive. In almost all the cases reported to us, accounts could have been protected by using multi-factor authentication.
- In April, Traficom and the Finnish Security and Intelligence Service (Supo) held a joint information session reviewing the current cyber security threat level, which remains heightened. Attackers are increasingly interested in Finnish organisations. The number of targeted attacks has increased, in particular.
- As the summer and summer holiday season are approaching, various invoicing scams are also becoming more common. The NCSC-FI has lately received several reports of attempted invoice fraud from companies across Finland. All organisations should train their staff – including seasonal and summer employees – on their invoicing practices to protect themselves against CEO and invoice fraud.

1 mo.

Cyber security trends
in the past 12 months

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

TOP 5 cyber threats in the near future (6–24 months)

1. 🔄

Threat level in Finland’s cyber environment remains heightened.

The number of targeted attacks has increased. The heightened threat level increases the importance of preparedness in organisations.

2. 🔄

Economic and political phenomena are reflected in cyber security.

The phenomena may affect the digital environment quickly, and their impact on cyber security may be difficult to predict.

3. 🛡

Organisations should prepare for AI-related challenges.

Organisations should try to identify challenges that artificial intelligence may cause and prepare for them by training their staff, for example.

🛡 **New**

🔄 **Updated**

Symbols

4. 🔄

The information security and continuity of supply and service chains are increasingly critical.

To ensure cyber security, organisations need to understand their own supply chains. Most organisations are more or less dependent on outsourced digital services.

5. 🔄

Cyber security depends on experts and cyber security skills are important for all of us!

The need for cyber security experts is diversifying. As new regulations and cyber security meld into a part of the daily functions of companies, the need for experts increases further.