TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

October 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, October 2023

Data breaches and leaks

- In October, we issued a yellow alert regarding highly active and widespread M365 phishing and data breaches.
- In October, we received a few notifications where malware was sent as a ZIP file along with a Teams meeting invitation.

Scams and phishing

- Attempts were made to scam online banking IDs with a tax refund theme.
- Credential phishing faked as security mail increased so much that a yellow alert was issued about it.
- At the end of October, an extensive text message campaign was used to try and scam the rent money meant for November.

Malware and vulnerabilities

- Several critical vulnerabilities were published in October, many of which had already been exploited.
- A modem or router is the gateway to our home network, and securing it is important when criminals search the network manually or automatically for vulnerabilities.

Automation and IoT

- Neither security nor the availability of updates seem to play an essential role in Black Friday deals.
- The United States authorities published guidelines for the use of open source code in OT environments.
- The APT group has developed its capabilities to affect the automation systems of critical infrastructure.

Network performance

- There were 16 major disruptions in public communications services in October.
- The hacktivist group NoName057(16) has targeted tens of organisations in Finland with denial-of-service attacks during the fall.
- Application-level denial-of-service attacks have had an impact on some organisations.

Spying

- Various vulnerabilities are actively exploited in cyber spying.
- In October, for example, there were reports of exploiting vulnerabilities in the WinRAR compression tool, Atlassian Confluence, Roundcube email servers and Jetbrains TeamCity for spying purposes.

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

The Tietoturva 2023 information security seminar was held on Thursday 12 October 2023. The recording of the seminar and the presentation materials are on our website.

Traficom and National Emergency Supply Agency's new report provides information on the current state and development needs of software development.

We published a new guide for securing home networks and routers.

The recording of the result review webinar of the Ketjutonttu campaign held on 5 October 2023, as well as the final report, are on our website.

We published a new guide on ensuring the data security of stand-alone workstations.

Overview of cyber weather in October

- Several critical vulnerabilities were released in October.
  - It is always good to update systems and devices as soon as possible!
- On 20 October 2023, we issued a serious alert about the wave of data breaches of Microsoft 365 accounts, in which the passwords of the Microsoft 365 environment have been phished with fake e-mails. The phishing utilised a secure mail theme, which increased the credibility of the fake messages. The campaign had an extraordinary number of victims.
  - The alert was removed as inactive on 8 November 2023.
- At the beginning of October, Traficom's regulation came into force, which obliges telecommunications operators to reject calls from abroad that are faked as Finnish numbers, including mobile numbers. Consequently, the number of notifications about scam calls from fake numbers has decreased in October.

1 mo.

Cyber security trends
in the past 12 months

	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct
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. 🛡

Serious vulnerabilities are being exploited faster and faster

In addition to installing an update that fixes the vulnerability, it is often necessary to investigate whether the vulnerability has already been exploited before installing.

3. 🔄

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.

🛡 **New**

🔄 **Updated**

Symbols

4.

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.

5. 🔄

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

As new regulations and cyber security meld into a part of the daily functions of companies, the need for different experts increases further. Additionally, from the point of view of risk management and continuity, ensuring sufficient competence during all seasons is important for organisations.