TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

January 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, January 2024

Data breaches and leaks

- M365 account breaches increased at the start of the year. The cause of the breaches was, for example, secure email themed phishing messages.
- We received several reports about logging in attempts to VPN services, and part of these attempts led to the Akira ransomware investigation.

Scams and phishing

- Email account breaches moved from one organisation to another via secure email themed phishing messages.
- Scam text messages pretending to be from the police threatened with speeding fines.
- Scam messages pretending to be from OmaVero continued in substantial quantities in January.

Malware and vulnerabilities

- Ivanti’s products have critical abused vulnerabilities.
- Cisco Anyconnect vulnerability has been used as the entry point for the Akira ransomware.
- Five bulletins were published in January and two at the start of February regarding critical vulnerabilities.

Automation and IoT

- Kyberala murroksessa (Cyber sector in transition) seminar opened the current state of cyber regulation.
- Malware that infects IoT devices remains popular with cybercriminals year after year. Criminals create new botnets with new features, especially based on Mirai's source code.

Network performance

- There were 3 disruptions in public communications services in January.
- Denial-of-service attacks done by hacktivists continued.
- Organisations prepare, protect themselves and fight denial-of-service attacks with a good routine.

Spying

- Microsoft told about the attack done by Midnight Blizzard on its cloud services.
- Other Microsoft’s customer organisations were also the target of the attack.
- The attacker's goal was to search for information, for example, from the e-mails of decision-makers and cyber security experts.

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

Kyberala murroksessa (Cyber sector in transition) seminar was held on 23 January 2024. The recording of the seminar will be published as soon as possible on Traficom's YouTube channel. Presentation materials have been published on the program page of the seminar.

The application for financial support for the implementation of modern information security solutions and innovations in small and medium-sized enterprises is open until 1 March 2024. A total of 1.5 million euros is being applied for. A maximum of 60,000 euros per project can be granted.

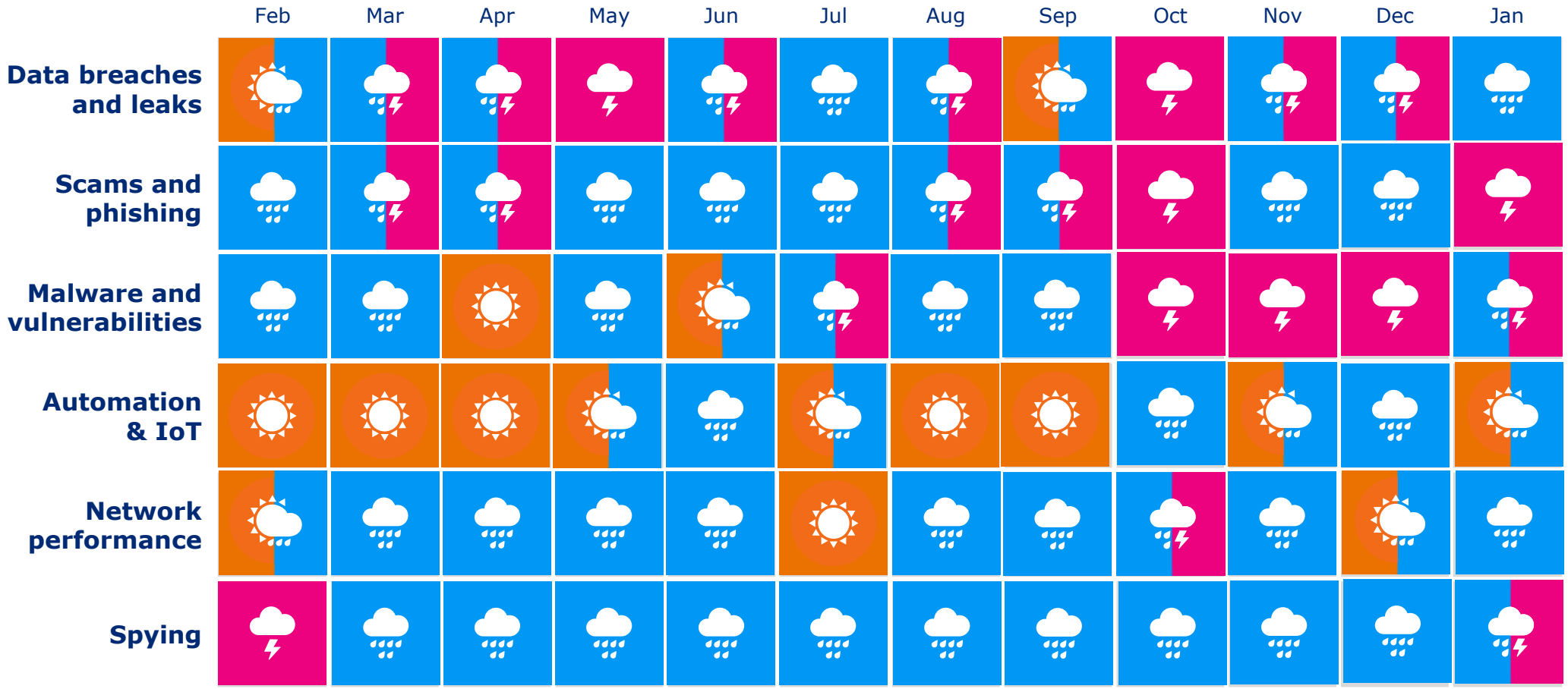
We published the Information Security Now! article *Cooperation between the authorities ensures secure elections*. The National Cyber Security Centre Finland is involved in supporting the Ministry of Justice and other election authorities in preparing and preparing for national elections.

The weak data security of smart devices will be controlled by regulation from 1 August 2024, when mandatory data security requirements will be applied to wireless devices.

Overview of cyber weather in January

- Denial-of-service attacks will also continue in 2024. Tens of domestic organisations have been listed as targets of denial-of-service attacks by pro-Russian hacktivist groups from the beginning of 2024.
  - In the beginning of the year, there were completely new targets on the lists from, for example, the municipal and education sectors.
  - Last year, especially finance, logistics and transport and state administration operators were popular targets.
- Several critical vulnerabilities have been published in the first half of the year.
  - For example, critical vulnerabilities concerning Ivanti products, which are also widely used in Finland, have been published since the beginning of the year.
- The active sharing of information by organisations increases the ability of other organisations to protect themselves from digital threats. A cyber threat encountered by one organisation today may be encountered by another tomorrow. Open and up-to-date information sharing reduces the effects and costs of threats. Learning from others is also cost-effective, when others do not have to reinvent a solution already in use elsewhere.

Cyber security trends
in the past 12 months



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.