Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

June 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, June 2023

Data breaches and leaks

- Breaches compromising corporate e-mail accounts have continued to be high during the first half of the year compared to 2022.
- Reports on social media account breaches have continued to be high.

Scams and phishing

- Phishing sites are more increasingly being hidden behind QR codes.
- Personal data, whether stolen or leaked out, are used for many kinds of offences, such as more personal, tailored phishing to steal online banking details.

Malware and vulnerabilities

- Zyxel patched a critical vulnerability in its online file storage, vulnerabilities have already been reported.
- The NCSC-FI has got the right to issue CVEs, i.e. to be a CVE Numbering Authority (CNA).

Automation and IoT

- IoT solutions may stop working unexpectedly, which may cause considerable problems for a user.
- A single customer's ability to affect the service provider or fix the problem is minimal.
- There may be difficult ethical questions related to the decision to discontinue the service.

Network performance

- Three significant disturbances in public telecommunications services in May.
- Port operators targeted again by DoS attacks.
- An operator's DNS provided to corporate customers was targeted by a DoS attack.

Spying

- Malware spread through USB sticks are on the rise again also in cyber espionage.
- Information security researchers report several cases where malware spread by infected USB sticks have been exploited for data collection and gaining control of targets.

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

The NCSC-FI has been authorized to be a CNA (CVE Numbering Authority) to assign CVE IDs to vulnerabilities.

The NCC-FI has opened its first application for funding support for the deployment of cyber security solutions and innovations in small and medium-sized enterprises (SMEs).

We published a new guideline on how to implement an e-mail exercise.

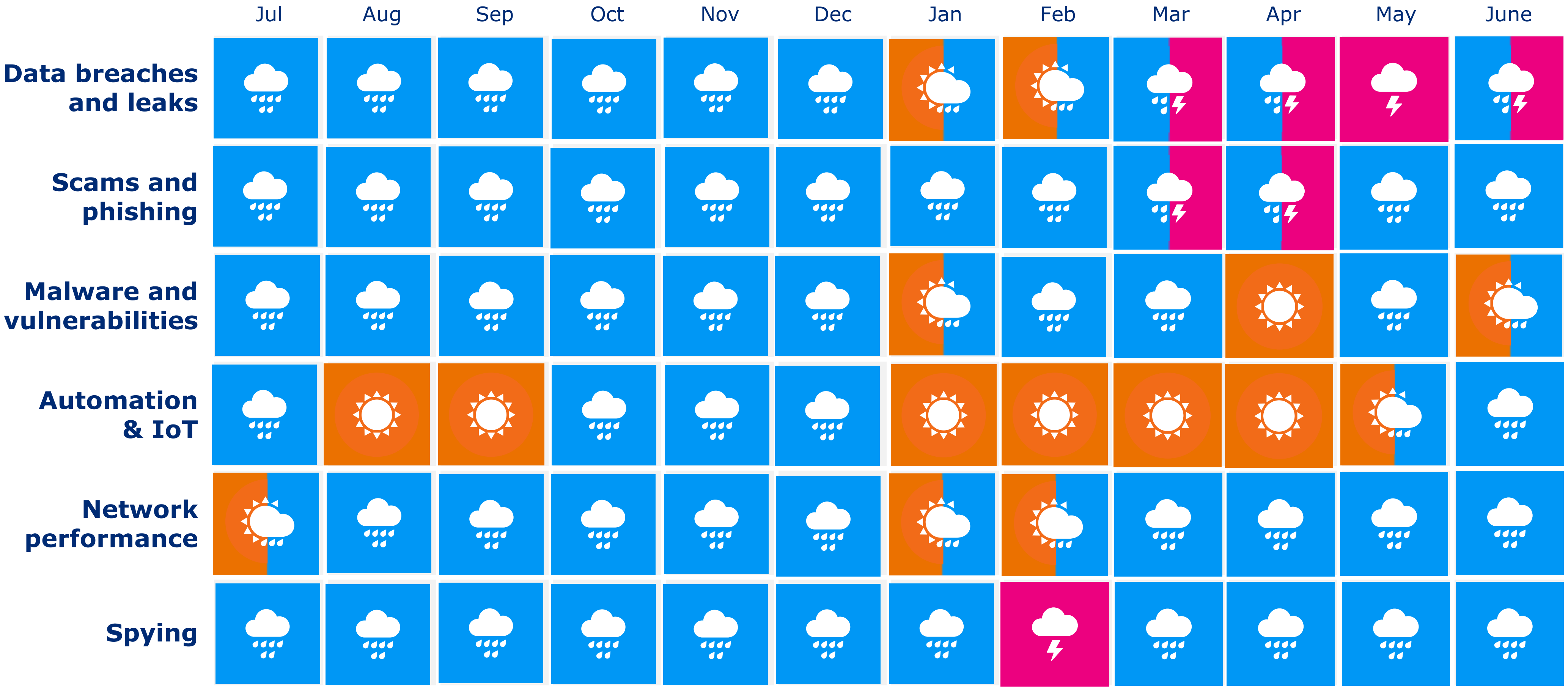
Preparations for the Post-Quantum Crypto is ongoing also in Finland.

Overview of cyber weather in June

- In June, cases where vulnerabilities in Zyxel have been exploited were also reported in Finland. At international level the vulnerability has been actively exploited and, for example, the botnet Mirai has reportedly targeted Zyxel's firewalls.
  - In its release, Zyxel thanks the NCSC-FI for the help in finding the vulnerability.
- A zero-day vulnerability in the MOVEit file transfer software was internationally widely exploited. There were not many cases in Finland as, according to our knowledge, the system is not widely used.
- M365 phishing is becoming quicker. At the moment, the time between a successful phishing event (were the user enters the codes) and exploitation of it is at its fastest only minutes.
  - More than 100 hijacked M365 account breaches were reported to the NCSC-FI during the second quarter of the year.

1 mo.

Cyber security trends
in the past 12 months



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