Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

June 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 June 2024

Data breaches and leaks

- June was relatively peaceful in terms of data breaches and leaks.
- Facebook accounts were breached using IKEA themed phishing messages that were targeting the confirmation codes.
- M365 account breaches were reported especially toward the end of the month. Accounts were breached using, for example, phishing messages that “shared a file”.

Scams and phishing

- Scams threatening with a fine from Traficom appeared at a new, slightly different than before, URL ”trafcom.info”.
- In June, tax refund-related scam messages began to appear again pretending to be from the tax authorities.

Malware and vulnerabilities

- June was calm in terms of malware and vulnerabilities.
- We received a few reports of attempts to spread the Vultur malware via text messages.

Automation and IoT

- Operators' devices in the headlines: In the United States, 600,000 routers broke as a result of an attack. In Finland, due to the expiration of some modem certificates, unprotected devices are not allowed to enter the network.
- A very serious flaw in the FreeRTOS operating system of, e.g. small automation devices can cause problems for a long time.

Network performance

- There were 10 disruptions in public communications services in June.
- In June, a few denial-of-service attacks were reported, but the reported occurrences had no significant effect on services.

Spying

- TeamViewer, known for its remote management solution, reported a data breach in its corporate network that has been blamed on Midnight Blizzard (Nobelium, APT29). It is known that the breach did not extend to customer connections or the production environment.
- Microsoft has sent alerts to customers who may have been affected by the data breach linked to Midnight Blizzard that took place during the winter.

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

We published a new guideline on quantum-safe algorithms and transitioning to them.

We reminded you to be prepared for the increasing number of invoicing and CEO scams during the summer. The most effective way to protect yourself from invoicing scams is to verify the matter in unclear cases by telephone and using the original invoicer's contact information. It is important to remind summer employees, and also those who have been employed longer, what is the right way to handle incoming invoices in your organisation.

On 27 June 2024, the Government appointed the Advisory Board for Network Security for a new term of office. The task of the Advisory Board for Network Security is to monitor the development of communications networks and technology and the application practice of legislation concerning network security, and to support decision-making by authorities. The term of office of the Advisory Board is from 1 July 2024 to 31 December 2027.

In June 2024, Traficom approved two communities as trusted flaggers, specifically against illegal content targeting children and young people on the Internet. The status was granted to Save the Children Finland and Somis Enterprises Oy that offers the Someturva service.

Overview of cyber security in June

- Tens of thousands of searches were conducted without cause through the consulting company's systems in the spring, for example in the registers of the authorities. The attacker is suspected to have conducted searches using the breached usernames of the auto repair shop and towing service.
  - This is a so-called supply chain attack.
  - The observation and management of a supply chain attack is important not only for the continuity of one's own operations, but also because they affect the reputation and trust of the organisation greatly in the network. The victim of a supply chain attack is both the supplier and the customer. Managing the situation often requires transparency and cooperation from the parties involved.
  - Phishing can be used to carry out supply chain attacks.
- The NCSC-FI has recently received several reports of various Microsoft 365 user account phishing attempts targeting organisations. Some of the phishing has led to an e-mail account data breach.
  - Phishing is done with different, often topical themes. Sometimes, even topics that the target is waiting to be contacted about can be utilized in phishing, in which case the identification of phishing requires especial vigilance.
  - Check out our guide Do this in the event of a Microsoft 365 account breach.

1 mo.

Cyber security trends
in the past 12 months

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