TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

February 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, February 2024

Data breaches and leaks

- Login attempts targeting network devices and M365 account breaches continued. In several M365 cases, AiTM fishing was used for the breach.
- In social media account hacks, a ransom was demanded from the account owners to restore the account.

Scams and phishing

- Over 80 sender IDs are already protect against scams. Each protected sender ID reduces the means of criminals to scam people in the name of authorities and companies.
- There are still a lot of scary SMS scam messages about traffic violations or unpaid car taxes, even without a credible sender ID.

Malware and vulnerabilities

- Ivanti's vulnerabilities show the criticality of data security for network edge devices.
- The US cyber security authority CISA told about the Ivanti data breach.
- At the beginning of March, a vulnerability bulletin was published about a critical vulnerability in the JetBrains TeamCity software.

Automation and IoT

- A smart gift can be an unfortunate surprise - check out the information security features of the product before making a purchase decision.
- The failure of automation used on farms can have serious consequences. Ransomware in the computer controlling the feeding of the farm threatened the well-being of farm animals.

Network performance

- There were 2 disruptions in public communications services in February.
- At the beginning of February, hacktivists targeted a record number of domestic organisations with denial-of-service attacks.

Spying

- US authorities disrupted an attack network formed from hacked Ubiquiti EdgeRouter devices.
- According to authorities, the devices were used, among other things, for forwarding and collecting login information stolen in APT28 actor campaigns and for routing attack traffic.

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

Together against text message scams - more than 80 sender IDs are already protected.

Internet platforms and other digital services have new obligations when the application of the EU's Digital Services Act started on 17 February 2024. The purpose of the new Act is to reduce illegal content and increase the transparency of services.

Overview of cyber weather in February

- Microsoft 365 phishing reared its head again in February. The spoofed secure email messages contained links that led to a phishing site asking for your username and password.
  - The NCSC-FI recommends all Microsoft 365 clients to communicate internally about the threats of phishing messages.
  - The phishing sites have used advanced adversary-in-the-middle automation (AitM) which can in some cases bypass multi-factor authentication (MFA).
    - The forced introduction of multi-factor authentication works as an efficient protection method and basis for other protection methods against phishing campaigns.
- CEO scams and other invoicing frauds have also been in circulation in February.
  - Organisations should provide employees, not forgetting summer employees and interns, with clear instructions on the organisation's invoicing practices and safe verification practices, and they should always be adhered to.
  - You can verify the authenticity of suspicious messages by calling the sender by phone.

1 mo.

Cyber security trends
in the past 12 months

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