TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

March 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, March 2024

Data breaches and leaks

- The data breach phenomenon of the month was email phishing and data breaches targeting organisations.
- We have continued to receive notifications about scans targeting network edge devices and exploitation and breach attempts of vulnerabilities.

Scams and phishing

- Vehicle tax themed SMS scams phished online banking credentials in the name of Traficom.
- In addition to all banks, Posti, OmaKanta and MyTax have been the subject of phishing messages.

Malware and vulnerabilities

- Linux-distribution's XZ Utils file compression program versions 5.6.0 and 5.6.1 contain harmful code that allows unauthorized access, creating a backdoor into the system.

Automation and IoT

- Connectivity Standards Alliance (CSA) responsible for the Matter protocol has published a cybersecurity label for IoT products and agreed on the reciprocal recognition of the labels with Singapore's Cyber Security Authority (CSA).
- Additionally, the Federal Communications Commission of the United States has published a voluntary cybersecurity label for IoT products.

Network performance

- There were 3 disruptions in public communications services in March.
- Hacktivists targeted Finland with DoS attacks again at the end of March.
- Regardless of findings, the attacks had no significant effects.

Spying

- Several countries reported additional information regarding APT31's cyber spying.
- APT31, which is connected to China, was said to have used hacked Swedish routers in attacks against different countries and sought to obtain information from British politicians' emails.
- The National Bureau of Investigation told that ATP31's connection to the parliament data breach in 2020–2021 has been confirmed.

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

The report by Traficom and the National Emergency Supply Agency regarding Ai-based cybersecurity solutions has been published.

Traficom continues the 5G cybersecurity hacking event series with a new Hack the Networks event in May 2024. Sign up for the hackathon by 14 April 2024!

The Information security in 2023 report evaluated the threat level to remain heightened in 2024 as well.

Overview of cyber weather in March

- During March, organisations have been bothered by both DoS attacks and data breach attempts. Criminals have targeted, for example, various network edge devices.
- After the vulnerability of the XZ Utils software package, which became public at the turn of March and April, was revealed, users were advised to remove the tainted update as an initial measure. Currently, potential exploits are being searched for, updates to fix the issue are being published, and the case is being investigated extensively.
  - So far, critical vulnerability exploitations have not emerged.
  - Criminals used several years to prepare the critical vulnerability of the XZ Utils software package for exploitation, and the attack has been described as one of the most advanced supply chain attacks discovered to date.
  - Read more about the XZ Utils software package case in our Weekly review 14/2024.
- As a part of The National Cyber Security Centre Finland's weekly review, we started to publish a section titled Recently reported scams at the end of March. In the section, we collect examples of active scams that have been reported to us.

Cyber security trends
in the past 12 months