TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber Weather

April 2022

#cyberweather

Cyber weather gives you an update on the key information security incidents and phenomena of the month. We want to give our readers an overview of what has happened in the field of cyber security during the past month. The situation can be:

calm

worrying

serious

Cyber weather, April 2022

Data breaches and leaks 🌧

- Email accounts of some cities and municipalities have been hacked and used to send large amounts of phishing messages.
- Social media accounts are still being targeted by data breaches and their attempts.

Scams and phishing ⛈

- Fenton scams sent thousands of false job offers and tried to lure people into investing in a pyramid scheme.
- The Wallpaperga scam messages trick victims to click on a link to cancel a subscription subject to a fee.

Malware and vulnerabilities 🌧

- The NCSC-FI has once again received a few reports about the malware Emotet.
- There is another active campaign spreading the mobile device malware FluBot via SMS.

Automation and IoT 🌧

- Several signs indicate that cyberattacks against automation systems will become more widespread.
- A manufacturer of smart lighting systems went bankrupt – users no longer able to adjust their lights.

Network performance 🌧

- Eight major faults.
- Network performance continues at normal level, and the situation is good.
- Denial-of-service attacks against central government sparked discussion.

Spying 🌧

- The number of cyberattacks in Ukraine has increased manifold during the war. Attacks have also targeted industrial automation.
- Numerous APT groups continued their espionage against Western countries in April. The groups take advantage of the war in Ukraine, for example.

TOP 5 Cyber Threats — Major Long-term Phenomena

1 🔄

Economic and political phenomena are reflected in cyber security. Digitality cuts across all activities of organisations, and changes in the international security situation have a major impact on continuity and risk management in organisations.

2 🛡

Insufficient exchange of information leads to poorer situational awareness of cyber security. A cyber threat encountered by one organisation today may be encountered by others tomorrow.

3

Unpatched vulnerabilities open a route to the organisation for criminals. Criminals are quick to exploit vulnerabilities. Vulnerabilities mean devices and services connected to the internet with poor information security and insufficient protection and maintenance.

Symbols

New 🛡

Updated 🔄

4

Cyber security depends on experts, and cyber security skills are important for all of us!

Increasingly diversified cyber security expertise is needed: there is a growing need for experts as new regulation is adopted and cyber security becomes an integral part of daily operations in businesses and organisations.

5

Access rights – the keys to an organisation.

Access control is important in any organisation. Credentials can be stolen via different kinds of attacks, and credentials in the wrong hands may have a major impact on an organisation’s activities.