TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber Weather

February 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, February 2022

Data breaches and leaks 🌧

- Savonia University of Applied Sciences reported having been targeted by a cyber attack.
- The municipal sector was targeted by a rather large phishing campaign that resulted in several successful data breaches.

Scams and phishing 🌧

- Scams on online marketplaces have continued active.
- Criminals are using new tricks to steal user credentials for social media accounts.

Malware and vulnerabilities 🌧

- Malware have been used in attacks against Ukrainian organisations.
- Linux kernel has a highly critical vulnerability that enables privilege escalation, i.e. gaining a higher level of access than intended.

IoT 🌧

- Several critical vulnerabilities were found, for example, in an integration platform used for the management and remote monitoring of IoT systems.

Network performance 🌧

- Network performance is currently good in Finland.
- A denial-of-service (DoS) attack had a major impact on the services of a bank.
- Overall, the DoS trend continues its steady fluctuations.

Spying 🌧

- Several data wiper malware, phishing and DoS attacks have been discovered in Ukraine after the Russian attack against the country.
- The United States reported major espionage operations targeting its defence industry and media sector.
- The Iranian threat group MuddyWater is actively conducting cyber espionage in many sectors.

TOP 5 Cyber Threats — Major Long-term Phenomena

1 🛡

Economic and political phenomena are reflected in cyber security. The phenomena may affect the digital environment quickly, and their impact on cyber security may be difficult to predict.

2 🛡

Leadership and risk management. Rapid changes in operating environments test organisations' ability to manage risks concerning cyber security. The management in organisations is responsible for ensuring the effectiveness of risk management.

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.