TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

# Cyber Weather

January 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

TRAFICOM

1.3.2022

# Cyber weather, January 2022

## Data breaches and leaks

- Facebook Messenger is being actively used for phishing Facebook user credentials.
- January was otherwise quiet: the number of data breach reports was low.

## Scams and phishing

- Messages with fake invoices and secure mail notifications have been used to phish credentials for hundreds of user accounts. Some accounts have been hijacked.
- Online sales platforms are used to lure users to give their credit card details to criminals.

## Malware and vulnerabilities

- The critical alert on the Log4shell vulnerability has been lifted after two months.
- The FluBot alert has been removed because telecommunications operators' filtering measures have been successful.

## Automation

- More than half of IoT devices in healthcare are vulnerable.
- Vulnerabilities detected in Tesla cars. The responsible action of reporting vulnerabilities is not self-evident.
- New sections added to the book Automaation tietoturva ('Information security in automation', available in Finnish).

## Network performance

- Five major disruptions in public communications services in January.
- Several denial-of-service (DoS) attacks reported at the end of January.
- Another new record in Finland: a DoS attack measured at 379 Gbps.

## Spying

- Finnish diplomats have also been targeted using the Pegasus spyware that can infiltrate mobile devices.
- Increased tension between Ukraine and Russia has led to cyberattacks in the area.

17 January 2022

TRAFICOM

# **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.