TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

# Cyber Weather

March 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

21.4.2022

# Cyber weather, March 2022

## Data breaches and leaks

- There have been numerous data breaches and breach attempts targeting the social media accounts of private individuals.

## Scams and phishing

- Scam messages have been sent in the name of the police in Finland and elsewhere in Europe.
- CEO scam campaigns are targeting all organisations from hobby clubs to listed companies.

## Malware and vulnerabilities

- Numerous reports about messages containing a link to the OneDrive file sharing service.
- Several reports about attempts to spread the Emotet malware via email in Finland.

## Automation and IoT

- Industrial automation monitoring reports show improvement in cyber security capabilities.

## Network performance

- Seven major disruptions.
- Disruptions have been caused by power cuts, hardware malfunctions and modifications.
- Increase in the number of reports about denial-of-service attacks in various sectors.

## Spying

- Cyberattacks and their attempts by operators associated with Russia are being detected in Ukraine and Western countries.
- The FBI disrupted the use of a botnet consisting of infected routers for malicious activities. The botnet was suspected to be controlled by the APT Sandworm.

TRAFICOM

21.4.2022

# **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.