TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

# Cyber Weather

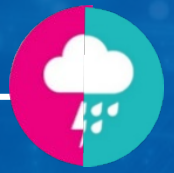
March 2021

**#cyberweather** 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
Finnish Transport and Communications Agency
National Cyber Security Centre

# Cyber weather March 2021



## Data breaches and leaks

- The Exchange situation has stabilised and subsided somewhat after early March.
- Some of the data stolen from Facebook in 2019 has been published, including data from Finnish users.

## Scams and phishing

- OmaPosti-themed text messages continue to pester people daily.
- Scam phone calls from technical support continue to torment Finns – mostly in English, but sometimes in broken Finnish, too.

## Malware and vulnerabilities

- The BazarLoader malware is being spread via e-mail. The campaign is also known as “BazarStrike”
- OmaPosti-themed text messages lead to malware in some cases.

## Automation and IoT

- The background systems of network device manufacturer Ubiquiti have suffered a significant data breach.

## Network performance

- Five significant disturbances.
- Recurring disturbances in identifying users of national digital health services.
- Disturbing remote teaching environments by using denial-of-service attacks is not harmless fun; such actions will lead to a criminal investigation.

## Spying

- According to the Finnish Security Intelligence Service, the cyber attack against the Finnish Parliament was caused by an APT31 operation.
- Many APT groups linked to China have been active around the world in recent times.

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

# TOP 5 cyber threats — **Major long-term phenomena**

## 1 ↑

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

## 2 →

**Using various cyber attack methods for extortion is becoming commonplace and threatening business continuity.** More and more cyber attacks in which tens of thousands of euros are still small change will be seen in Finland.

## 3 ↓

**Phishing** is extremely common and potentially difficult for the target to identify. This is also exploited in the context of targeted attacks and spying.

↑ *increase*

↓ *decrease*

→ *no change*

*Yellow* = new/updated*

## 4 →

**Inadequate management of cyber risks and muddled division of responsibility in service management.** Information security suffers as a result of deficiencies in the anticipation of the impact of cyber threats and insufficiently defined roles in the context of service management.

## 5 →

**Deficiencies in log data** pose a risk to many organisations. The inadequate collection, monitoring and storage of log data results in an inability to detect and investigate anomalies.

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre