Finnish Transport and Communications Agency
National Cyber Security Centre

# Cyber Weather

October 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

22.11.2022

# Cyber weather, October 2022

## Data breaches and leaks

- A large number of Zalando accounts were hacked. The hackers may have used previously leaked lists of user IDs and passwords.
- The energy, industry, media and education sectors were highlighted among targets of data breaches and attempted breaches.

## Scams and phishing

- Extortion scams with a police theme have continued in even higher volumes than before. Fraudulent charges are used to swindle money out of victims in Finland and elsewhere in Europe.

## Malware and vulnerabilities

- Observations of the malware Emotet have been reported abroad.
- A few reports about ransomware. In September, we reported that the number of ransomware in Finland has increased.

## Automation and IoT

- The management of vulnerabilities in medical devices must be improved.

## Network performance

- Two significant disruptions in public communications services.
- The number of denial-of-service (DoS) attacks is on the rise.
- Of all DoS attack reports in 2022, 25% were received in October.

## Spying

- State actors are exploiting known and previously unknown vulnerabilities.
- According to Microsoft, the Microsoft Exchange ProxyNotShell vulnerability has presumably been exploited since August in an operation by a state actor.

# **TOP 5 cyber threats** – near future (6–24 months)

## 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

**Cyber threat level in Finland has increased.**

The increase in malicious traffic and the rise in the threat level make preparedness even more important in organisations.

## 3

**Weaknesses in ordinary control measures still cause the majority of information security incidents.**

For example, access rights management, keeping software up to date and good information security cultre are at the core of cyber security.

**Symbols**

*New*

*Updated*

## 4

**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. Efficient sharing of information improves cyber security for all.

## 5

**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.

TRAFICOM

22.11.2022