Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber Weather

December 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

19.1.2023

Cyber weather, December 2022

Data breaches and leaks

- Hijacking of social media accounts is still commonplace.
- A vulnerability in Microsoft Exchange is being actively exploited to inject ransonware into systems.

Scams and phishing

- The use of .fi domain names is still a rare exception in phishing campaigns to steal banking details. Most fraud still use international domains.
- CEO fraud attempts have been frequent, but most attempts are fortunately unsuccessful.

Malware and vulnerabilities

- Reports of ransomware have increased.
- Several vulnerability reports were issued in December, informing about numerous patches to critical vulnerabilities in different products.

Automation and IoT

- Continuity in the functioning and maintenance of medical implants is ethically important. If a manufacturer goes bankrupt, the cyber security of patients could also be compromised.

Network performance

- Two significant disturbances in public telecommunications services in December.
- Denial-of-service (DoS) attacks are increasingly frequent.
- 25% of all DoS attack reports in 2022 were submitted in December.

Spying

- Espionage campaigns aim to circumvent mechanisms designed to alert users.
- Key infiltration routes used by APT actors include vulnerabilities in VPN solutions and other network traffic products.

TRAFICOM

19.1.2023

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

19.1.2023