TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber Weather

November 2021

#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

3.1.2022

Cyber weather, November 2021

Data breaches and leaks

- The Digital and Population Data Services Agency has published an electronic guide on the Suomi.fi web service for organisations affected by a data breach or data leak.
- A Danish wind turbine manufacturer and operator reported its IT systems were breached.

Scams and phishing

- The number of SMS scams has soared.
- In addition to banking details, phishers have been after the user credentials and emails of university students and staff.

Malware and vulnerabilities

- The actively exploited Log4j vulnerability requires administrators to take immediate action.
- FluBot malware campaigns have been active in Finland. The campaigns have used text messages with parcel delivery and voice mail themes.

IoT and automation

- Strategies and guidelines on cyber security in IoT and automation are becoming more and more common, which is a sign of increasing awareness about the importance of the topic.

Network performance

- Six major disruptions were reported. The cases involved system changes and software errors.
- Hacked servers were used for denial-of-service (DoS) attacks.
- The Hospital District of Helsinki and Uusimaa reported being targeted by a DoS attack.

Spying

- Iranian operators have become increasingly interested in the IT industry and internet service providers.
- A North Korean group tried to spy on information security researchers.
- Various network devices are continuously targeted and used as tools in cyber espionage campaigns.

TRAFICOM

3.1.2022

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 internet with poor information security and insufficient protection and maintenance.

2

User credentials are valuable information in organisations Maintaining control over user credentials is important in any organisation. Credentials can be stolen via different kinds of attacks, and their loss may have a major impact on an organisation's activities.

3

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.

Symbols

New

Updated

4

Cloud services are new to many organisations, and attackers are often best experts in the information security of clouds. Organisations are rapidly migrating to cloud services but often do not understand their own environment and its capabilities well enough.

5

The information security of supply and service chains is becoming more and more critical. To ensure cyber security, organisations need to understand their own supply chains.

TRAFICOM

3.1.2022