TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber Weather

July 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

Cyber weather, July 2021

Data breaches and leaks

- Several reports about breached .fi websites.
- Extra care should be taken with social media accounts because they are often used by criminals.

Scams and phishing

- Bank scam campaigns have remained active.
- There have been numerous attempts to phish for online banking credentials and payment details in the name of all Finnish banks. The campaigns employ both email and text messages.

Malware and vulnerabilities

- The FluBot malware epidemic is subsiding, but malware numbers fluctuate from month to month.
- Several critical vulnerabilities were detected in July – patches should be installed as soon as possible.

Automation

- Information security is the greatest worry of IoT product developers.
- The first ISO standard on IoT security and privacy is out for international consultation. The draft is available for reading and comments free of charge.

Network performance

- Various modifications and configuration errors caused disturbances.
- Different disturbances also occurred in VoLTE services.
- The number of reported denial-of-service attacks was low but included valuable examples and lessons for other organisations to learn from.

Spying

- Western countries are accusing China of large-scale cyber espionage.
- The surveillance software of the Israeli company NSO Group has been used to spy on journalists and activists.
- APT29/NOBELIUM actively spies on governments and related organisations.

TRAFICOM

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

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

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.

Symbols

New

Updated

4

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.

5

Remote work is here to stay, and so are the associated risks. Devices' remote access services open to the internet expose organisations to data breaches. Administrators should make sure that teleworkers' devices are secured and firewall settings appropriate.

TRAFICOM