TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber Weather

August 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

Cyber weather, August 2022

🌧

Data breaches and leaks

- We have received numerous reports about attempts to log in to the information systems of Finnish organisations.
- Reports of domains and social media accounts of small enterprises being hijacked.

🌧

Scams and phishing

- Phishing for online banking details mainly employs text messages (smishing), while subscription traps have switched from text messages to email.
- Traficom Regulation 28 aiming to prevent caller ID spoofing has helped reduce the number of technical support scam calls.

🌧

Malware and vulnerabilities

- Ransomware observations reported by Finnish organisations and organisations operating in Finland.
- It is still important to install updates. Vulnerabilities are exploited quickly once they are discovered.

☀

Automation and IoT

- Cybersecurity Label seminar on 29 September focuses on future mandatory security requirements for IoT products in the EU.
- Researchers discovered vulnerabilities in nearly all examined IoT interfaces in 4G/5G networks.

🌧

Network performance

- Three major disruptions in mass communications services.
- Denial-of-service attacks increased in August.
- The number of DoS attacks reported to the NCSC-FI doubled compared to summer months.

🌧

Spying

- Data wiper malware detected in at least 25 countries during the first half of the year.
- APT actors still very interested in organisations’ cloud services and log in credentials.

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

4.10.2022