TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber Weather

July 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, July 2022

Data breaches and leaks

- Web servers that have vulnerabilities or have not been properly kept up to date are constantly being hacked.
- The Finnish News Agency STT and Wärtsilä were targeted by a data breach and became victims of ransomware.

Scams and phishing

- The logos of the Finnish Police and names of police personnel have been used in scam messages threatening with legal action and demanding a ransom.
- Phishing attempts to steal online banking details employ a wide range of scam messages sent via SMS and email.

Malware and vulnerabilities

- Only a few malware infections were reported in July.
- A severe vulnerability in Samba and a critical vulnerability in VmWare required quick installation of patches.

Automation and IoT

- Cyber criminals try to find new and creative ways to access isolated automation systems.
- Password cracker programs can contain trojans!

Network performance

- A disturbance with the rating A (affecting more than 300,000 users) occurred on the channel Yle TV1 on a weeknight.
- Only two major disturbances in communications networks.
- Only a few denial-of-service attacks in Finland.

Spying

- An operator associated with the Iranian government has destroyed information systems of the Albanian central governemnt.
- Attackers associated with the North Korean government have been active.
- An operator associated with the Russian intelligence service has continued its hacking attempts.

TOP 5 Cyber Threats — Major Long-term Phenomena

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 🛡

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.

3

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.

Symbols

🛡 *New*

🔄 *Updated*

4

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.

5

Access rights – the keys to an organisation.

Access control is important in any organisation. Credentials can be stolen via different kinds of attacks, and credentials in the wrong hands may have a major impact on an organisation's activities.

TRAFICOM

18.8.2022