Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

July 2020

#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

Cyber weather, July 2020

🌧

Data breaches and leaks

- Observations of hacked Finnish PulseSecure and Netscaler servers and vulnerable BIG-IP servers.
- Rise in the number of Office 365 data breaches after the more quit period during the summer.

🌧

Scams and phishing

- Phishing is a tool actively and increasingly used by professional criminals for on-line scams.
- Telephone scams are back after quarantine break. There are hundreds of thousands of incoming scam calls in Finland.

🌧

Malware and vulnerabilities

- Ransomware actors auction stolen data in order to make money with the data.
- In July, critical vulnerabilities were disclosed and vulnerabilities against network devices were actively exploited.

🌧

Automation

- US authorities warned of the increased threat of cyber attacks against automation systems.
- Automation system vulnerabilities are found increasingly often.

☀

Network performance

- Only three serious disruptions in public communications services.
- DigiCert revoked several certificates on 11 July, which also affected many Finnish services.
- The DoS attack situation was calm in Finland in July.

🌧

Spying

- The EU has taken the first ever active counter-measures related to cyber attacks directed against the EU member states by imposing sanctions.
- The aim of the targeted attacks is not only spying but also influencing and financing a nuclear weapon programme.

Top 5 cyber threats - Major Long-Term Phenomena

1 ⬆

Extensive ransomware threatens business continuity. Damages for individual incidents have gone up to tens of millions of euros.

2 ⬇

Phishing is very common, and it may be difficult for the recipient of a message to discover a scam. This is also exploited in targeted attacks and spying.

3 ⬇

Vulnerabilities are exploited rapidly, thus requiring quick updates. Equipment and services for which no attention is paid to information security are left open on the internet, and both protection measures and maintenance are incomplete.

⬆ *increase*

⬇ *decrease*

➡ *no change*

4 NEW

Poor cyber risk management and unclear distribution of responsibilities for service management. Cyber threat impacts can not be anticipated and unclear distribution of responsibilities for service management affect the information security.

5 NEW

Insufficient log data is a risk in many organisations. They are not able to observe or investigate incidents due to insufficient collection, monitoring or storing of log data.

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre