TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber Weather

June 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 June 2022

Data breaches and leaks

- O365 phishing has occurred as before even in June.
- A data breach in a police database took place in China and data of one billion people ended up in the wrong hands.

Scams and phishing

- Phishers are after online banking access codes in the name of almost all Finnish banks.
- Scam messages are being sent in the name of the National Police Board of Finland.

Malware and vulnerabilities

- A vulnerability in a Microsoft tool enables attacks using malicious Microsoft Office documents.

Automation and IoT

- Not even aware users are always able to protect their smart devices if the vulnerability is in the manufacturer's cloud service.
- Severe vulnerabilities are continuously found in automation environments, and they are being increasingly exploited also in cyber operations.

Network performance

- Six major disturbances detected in networks. However, they did not have any major impact.
- As regards Denial-of-Service (DoS) attacks, the current situation in Finland is calm.

Spying

- The Soft Cell campaign has extended its target from telecommunications operators to the finance sector and to the public administration.
- The APT actors exploit the Follina vulnerability.
- Home and small enterprise routers are still targeted by APT actors.

TOP 5 Cyber Threats — Major Long-term Phenomena

1 🛡

Economic and political phenomena are reflected in cyber security.

The phenomena may affect the digital environment quickly, and their impact on cyber security may be difficult to predict.

2 🛡

Leadership and risk management.

Rapid changes in operating environments test organisations’ ability to manage risks concerning cyber security. The management in organisations is responsible for ensuring the effectiveness of risk management.

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

18.7.2022