TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber Weather

August 2021

#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

TRAFICOM

16 September 2021

Cyber weather, August 2021

Data breaches and leaks

- The domain name Vastaamohaku.com was registered at the end of August, but it was taken down a few days later.
- We received several reports of user accounts being breached as a result of phishing.

Scams and phishing

- Phishing campaigns concerning banking credentials are becoming increasingly credible.
- Attackers are using search engine results and ads to lure victims on phishing sites instead of the correct e-services.

Malware and vulnerabilities

- We removed the alert on Android malware on 17 August.
- The PrintNightmare vulnerability is still an active issue.
- The Atlassian Confluence vulnerability is being actively exploited.

Automation

- Many severe vulnerabilities that attackers are actively trying to exploit.
- ETSI has released a technical specification for assessing the security of consumer IoT devices.

Network performance

- Four major disruptions.
- Hacked Confluence servers used for DoS attacks.
- Autumn is approaching and will bring along attacks on learning environments. Remind school-aged children that interference with information networks is a crime.

Spying

- Chinese operators have for years tried to hack telecommunications operators' systems in Asia with methods similar to those used in the Hafnium operation.
- In a campaign this spring, attackers tried to install Cobalt Strike malware on devices via email. In Europe, the campaign targeted at least Slovakia.

TRAFICOM

16 September 2021

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.

3 months

TRAFICOM

16 September 2021