TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber Weather

September 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, September 2021

Data breaches and leaks

- In early September, the Finnish listed company Adapteo announced a data breach against its systems.
- Firewall administrator credentials of Finnish organisations were on sale on a hacker forum.

Scams and phishing

- There have been numerous attempts to phish for online banking credentials and payment details in the name of all Finnish banks via email and text messages.
- Fake links to bank websites and My Kanta Pages have been also been used among search engine results to lure victims to fraudulent sites.

Malware and vulnerabilities

- We published a new web page that provides information on the most common malware observations in the Autoreporter system.
- A vulnerability in Microsoft's autodiscover feature was exploited.

IoT and automation

- The NCSC-FI at Traficom and the Cyber Security Agency of Singapore announced their collaboration on the mutual recognition of IoT cyber security labels.
- New IoT vulnerabilities were discovered, and the number of vulnerabilities in industrial automation systems is on the rise.

Network performance

- Two major network performance disruptions occurred in Finland.
- Facebook's problems also affected the use of Instagram and WhatsApp for several hours.
- Denial-of-service attacks had a moderate impact on service availability in September.

Spying

- The ProxyShell attack poses a threat to on-premises Microsoft Exchange servers.
- Germany and the EU are accusing Russia of the 'Ghostwriter' campaign.
- According to the Finnish Security and Intelligence Service, Finland is continually targeted by cyber espionage attempts.

TRAFICOM

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