TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber Weather

June 2021

#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

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather June 2021

☀ Data breaches and leaks

- Data leaks may sometimes be unintentional or caused without external intrusion.
- Remember to be careful with backup copies, data duplication plays a key role.

🌧 Scams and phishing

- Active phishing campaigns continued in the name of banks. According to the police, financial losses from online scams have amounted to millions of euros this year.
- The FluBot campaign was highly active in June.

🌧 Malware and vulnerabilities

- The Norwegian Axiell AS was targeted by a ransomware attack.
- The Kaseya supply chain attack affected hundreds of organisations.
- Malware spread by SMS have also been very active.

🌧 Automation and IoT

- A critical vulnerability has been discovered in Bosch IP cameras. A patch has been released.
- Several actors have published instructions to help organisations to prepare for cyber threats more systematically.

🌧 Network performance

- In June, 14 major disruptions were observed in public communications services.
- Storms and service breaks caused the number of disruptions to be higher than in previous months (2 in April and 3 in May).
- Extortion messages with a DoS theme.

🌧 Spying

- Western information security authorities said Russian military intelligence is behind the wide brute force campaign.
- Asian countries were frequently featured in news about cyber espionage.

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.

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre