TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber Weather

October 2021

#cyberweather

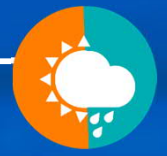
Cyber weather gives you an update on the key information security incidents and phenomena of the month. We want to give our readers an overview of what has happened in the field of cyber security during the past month. The situation can be:

calm worrying serious

TRAFICOM

16 September 2021

Cyber weather, October 2021



Data breaches and leaks

- Twitch experienced a data breach in which critical data about the service was leaked.
- An Argentinian government information system was breached and the personal data of tens of millions of citizens ended up in the hands of criminals.

Scams and phishing

- Campaigns to steal online banking details were extremely active in October.
- In addition to email scams, fake text messages are used to lure victims.

Malware and vulnerabilities

- The QakBot malware is being spread actively.
- “Information Security Now!” article: Dependency confusion exposes companies to attacks.

IoT and automation

- Strategies and guidelines on cyber security in IoT and automation are becoming more and more common, which is a sign of increasing awareness about the importance of the topic.

Network performance

- 10 major disruptions
- Some of the disruptions were caused by various changes to networks or configuration errors.
- Municipalities reported DoS attacks targeting school addresses. The attacks have also had an indirect impact on other services.

Spying

- Cyber spies have been interested in telecommunications operators: the LightBasin group has hacked the systems of numerous telecommunications operators across the world.
- NOBELIUM used IT service providers’ administrator credentials to infiltrate the systems of their customer organisations.

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

User credentials are valuable information in organisations Maintaining control over user credentials is important in any organisation. Credentials can be stolen via different kinds of attacks, and their loss may have a major impact on an organisation's activities.

3

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.

Symbols

New

Updated

4

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.

5

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.

3 months

TRAFICOM

16 September 2021