TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber Weather

May 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 May 2021

Data breaches and leaks

- The number of reported Office 365 data breaches began to increase at the beginning of summer.
- Several significant data breaches involving ransomware have been reported abroad.

Scams and phishing

- SMS scams infected mobile phones in Finland. The FluBot malware, which has spread aggressively, also steals banking credentials.
- Extortion scams using messages in Finnish became more active towards the end of the month.

Malware and vulnerabilities

- Malware campaigns targeting mobile devices have been active.
- On 4 June, we issued a yellow alert on FluBot.
- Microsoft's monthly updates included patches for 55 vulnerabilities.

Automation and IoT

- The ransomware infection in Colonial Pipeline's office network also affected production systems.
- A recording of Traficom's webinar on IoT security requirements is now available.

Network performance

- In May, only three major disruptions occurred in Finland.
- The Salesforce outage was due to human error.
- In May, the number of DoS attacks reported to us decreased, but the attacks were among the largest in history.

Spying

- The APT29 group has emailed targeted malicious messages to a large number of recipients.
- The NSA of the United States is accused of spying on public officials and politicians in Germany, France, Sweden and Norway via Denmark in 2012–2014.

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

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 network 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 ↓

Phishing is extremely common and potentially difficult for the target to identify. This is also exploited in the context of targeted attacks and spying.

↑ *increase*

↓ *decrease*

→ *no change*

Yellow = new/updated*

4 →

Inadequate management of cyber risks and muddled division of responsibility in service management. Information security suffers as a result of deficiencies in the anticipation of the impact of cyber threats and insufficiently defined roles in the context of service management.

5 →

Deficiencies in log data pose a risk to many organisations. The inadequate collection, monitoring and storage of log data results in an inability to detect and investigate anomalies.

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre