TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber Weather

September 2020

#cyberweather gives you an update on the key information security incidents and phenomena of the month. This product is primarily intended for use by information security officers. 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, September 2020

Data breaches and leaks

- Higher than normal number of reports of breaches targeting Finnish websites received by NCSC-FI.
- Large number of ransomware attacks against healthcare industry actors detected around the world.
- Office 365 security breaches continued.

Scams and phishing

- Thousands of text messages have been sent in Posti's name leading to subscription traps, phishing and malware.
- The details of dozens of victims were found via the phishing site, which were used to stop the security breaches.

Malware and vulnerabilities

- Emotet is actively spreading via email attachments, including in Finland.
- The Zerologon vulnerability is also being actively exploited. Ensure that all domain controllers are up to date.

Automation

- A Microsoft study found vulnerabilities in 71% of automation system networks.
- According to Kaspersky, the first half of 2020 saw Northern European automation systems face the smallest number of attacks.

Network performance

- A total of nine significant disruptions, of which three caused by summer storm Aila. Most other disruptions were due to power supply malfunctions or maintenance errors.
- Relatively few DoS attacks detected in Finland, but the number of threats is on the rise.

Spying

- Microsoft reported a campaign by the APT28 group aiming to collect passwords from the employees of a range of organisations.
- Various services that are free to use or offer free trials can be used as command-and-control channels to hide malicious activity.

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

TOP 5 Cyber Threats — Major Long-term Phenomena

1 ➡

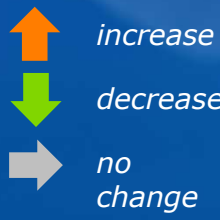
Ransomware attacks with wide-ranging effects pose a threat to the continuity of business operations. Individual attacks have caused damage worth tens of millions of euros.

2 ➡

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

3 ➡

Vulnerabilities are being exploited at a fast pace, which requires speedy updates. Devices and services are left exposed to the internet, with insufficient attention paid to data security, administration and protective measures.



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