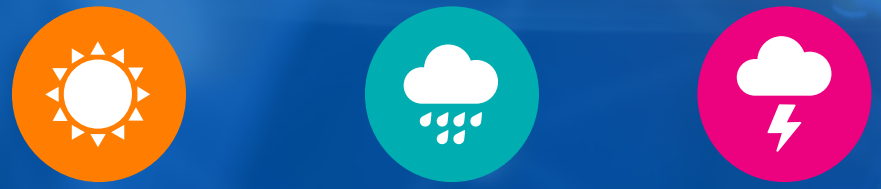
TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber Weather

February 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 for February 2021

Data breaches and leaks

- The French National Cybersecurity Agency (ANSSI) published a report on data breaches targeting Centreon software
- We published two articles related to the prevention and detection of lateral movement

Scams and phishing

- OmaPosti-themed scam text messages sent to Finns daily.
- Scammers phished for credit card details, claiming to need them for tax refund purposes.

Malware and vulnerabilities

- Red alert 1/21: Exchange server vulnerabilities
- The BazarStrike campaign saw attempts to distribute malware via spam email

Automation and IoT

- Dragos published an annual report on information security in the context of industrial automation.
- Remotely managed automation and IoT services show signs that user-friendliness is being prioritised at the expense of information security.

Network performance

- Five major disturbances in public communications services. Relatively minor effects.
- Finnish telecommunications operator targeted by a massive denial-of-service attack. The attack resulted in a significant slowdown of internet traffic for customers, lasting for about one hour.

Spying

- Microsoft reported that APT group Hafnium, which has links to China, exploited the zero-day vulnerabilities found in Exchange email servers in order to steal data.
- Foreign intelligence services have used network routers owned by Finnish companies and individuals for cyber espionage purposes.

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

TOP 5 Cyber Threats — **Major Long-term Phenomena**

1

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

2

The use of various types of cyber attacks for the purposes of extortion is becoming more common, posing a threat to the continuity of business operations. Individual attacks have caused damage worth tens of millions of euros.

3

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

increase

decrease

no change

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