TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

January 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, January 2021

Data breaches and leaks

- Staffing agency Eilakaisla suffered a data breach and a ransomware attack.
- Vastaamo patient records were once again shared in multiple places in January.

Scams and phishing

- Bank credentials are being phished for using false search engine results.
- A Finnish-language porn ransom campaign became active again. Ransom messages continue to be sent out in English as well.

Malware and vulnerabilities

- The Emotet botnet was shut down as a result of international police cooperation.
- An OmaPosti-themed widespread mobile malware distribution campaign spread via SMS has been very active.

Automation and IoT

- NAT Slipstreaming v2.0: New attack variant can expose all internal network devices to the internet.
- National Cyber Security Centre Finland promotes the adoption of SBOM with a blog post.

Network performance

- Six major disruptions in general communications services.
- A global disruption in team communications service Slack.
- Denial-of-service attacks impacted Finland as well in January. We would like to thank everyone who have submitted reports!

Spying

- Information security and vulnerability researchers are of interest to state-backed operators.
- Data stolen in connection with the European Medicines Agency data breach were leaked online in modified form.
- Germany issued a warning that the threat group APT31 is mapping opportunities to breach Western political organisations.

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