TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber Weather

October 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 for October 2020

Data breaches and leaks

- NCSC-FI continued to receive reports of Office 365 incidents.
- Psychotherapy centre Vastaamo and its customers targeted by extortionists following a data breach Patient and personal data was leaked online.
- See the https://tietovuotoapu.fi/en/ website for support and advice.

Scams and phishing

- Phishing scammers have attempted to steal Office 365 login credentials using extremely believable Zoom meeting invitations.
- The COVID-19 pandemic is again apparent in so-called porn scams, donation scams, Nigerian letter frauds and several kinds of phishing campaigns.

Malware and vulnerabilities

- The healthcare sector has been targeted by ransomware attacks.
- Malware for Android devices is being distributed in Posti's name.

Automation and IoT

- A threat report published by Nokia found that a third of all detected malware targeted IoT devices.
- This is up 17 percentage points on the previous year, which attests both to an increase in the number of IoT devices as well as their poor information security.

Network performance

- Only three significant disturbances in Finnish communications services.
- Global disturbances in Microsoft and Slack services.
- NCSC-FI received reports of denial-of-service attacks with major impacts on the targeted services.

Spying

- Norway accused Russia of mounting a cyber attack against its Parliament earlier this autumn.
- According to the Finnish Security Intelligence Service (Supo), the role of cyber espionage has grown in relative importance during the coronavirus pandemic. Supo further pointed out that Russia and China have a particular interest in Finland in this context.

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

TOP 5 Cyber Threats — Major Long-term Phenomena

1 ↑

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.

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.

↑ *increase*

↓ *decrease*

→ *no change*

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre