TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber Weather

August 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, August 2020

Data breaches and leaks

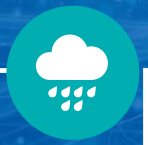
- Norwegian parliament targeted by data breach.
- Data stolen from over 900 breached Pulse Secure VPN servers published on the internet.
- Number of Office 365 breaches on the rise due to successful phishing attacks.

Scams and phishing

- No limits to the audacity of scammers: Services that supposedly help return money stolen in scams designed to scam victims again.
- Phishing actively utilised by professional criminals.

Malware and vulnerabilities

- EMOTET spreading in Finland and elsewhere — yellow alert issued by NCSC-FI.
- Number of critical vulnerabilities, updates recommended without delay.

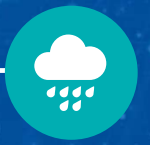


Automation

- Information security researchers found hunderds of thousands of vulnerable printers on the internet.
- First official standard on information security of consumer IoT devices published.

Network performance

- Only four notable disruptions affecting public communications services.
- Disruption affecting CenturyLink on 30 August had a global impact.
- Internet censorship in Belarus.
- Only few DoS attacks in Finland, but threats on the increase.



Spying

- Targeted commissioned attacks pose a particular threat to information critical to business operations, but state administration and diplomatic targets may also be victims of made-to-order attacks.
- Some cyber attackers targeting government bodies are motivated by money.

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.

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