TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

December 2020

#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, December 2020

Data breaches and leaks

- Versions of the SolarWinds management tool affected by the backdoor in use in Finland
- Office 365 accounts continue to be targeted by active breach attempts

Scams and phishing

- A large number of subscription trap, phishing and malware scams distributed by SMS
- Notices of arrival used for phishing, with payday loans taken out by scammers in the victim's name

Malware and vulnerabilities

- Backdoor discovered in the SolarWinds management tool used for spying and data breaches
- Following a month of little activity, Emotet malware on the rise again in Finland

Automation and IoT

- Discovery of new attack and spreading methods used by the Gitpaste worm
- Deficiencies observed in updates to vulnerable automation systems, as long supply chains increase reaction times and make identification more difficult

Network performance

- Only two major disturbances in public communications services
- Global disturbance in Google's services made working impossible for many and disabled IoT devices
- DoS attacks targeted service providers, VPN solutions and more

Spying

- Autumn 2020 saw the Finnish Parliament targeted by a cyber attack, which compromised the information security of email accounts, including accounts belonging to MPs
- In the USA, ministries, agencies and technology companies were breached by hackers using a backdoor added to the SolarWinds Orion platform

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 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