TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

April 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

Cyber weather April 2021

Network performance ☀

- Office 365 data breaches still occur but the number of reported incidents has decreased in 2021.

Spying 🌧

- Smishing attacks are becoming more and more common: SMSs are used to phish for banking credentials, lure recipients into subscription traps and spread malware.
- Sextortion campaigns were less active in April but have picked up again.

Malware and vulnerabilities 🌧

- A patch has been published for the Pulse Connect Secure VPN vulnerability and should be installed immediately.
- FluBot and FakeCop/FakeSpy malware are being spread by SMS.

Data breaches and leaks 🌧

- The vulnerabilities BadAllock and NAME:WRECK are affecting hundreds of millions of embedded systems.
- Electric cars and their charging points are becoming increasingly common, but there is little talk about the cyber security of charging points.

Scams and phishing 🌧

- Only two major disruptions occurred in Finland in April.
- Microsoft’s cloud services experienced two major disruptions.
- Approximately a half of DoS attacks reported to us in April concerned schools or remote learning environments.

IoT and automation 🌧

- The severe Pulse Connect Secure vulnerability may have been exploited for state-sponsored espionage.
- The United States and the United Kingdom are accusing Russian foreign intelligence of hacking the supply chain of the SolarWinds Orion platform

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

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

1 ⬆

Unpatched vulnerabilities open a route to the organisation for criminals. Criminals are quick to exploit vulnerabilities. Devices and services are left exposed to the internet with insufficient attention paid to security, protection and maintenance.

2 ➡

Using various cyber attack methods for extortion is becoming commonplace and threatening business continuity. More and more cyber attacks in which tens of thousands of euros are still small change will be seen in Finland.

3 ⬇

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

4 ➡

Inadequate management of cyber risks and muddled division of responsibility in service management. Information securitysuffers 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