TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber Weather

December 2021

#cyberweather

Cyber weather 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

21.1.2022

Cyber weather, December 2021

Data breaches and leaks

- Several reports about hijacked social media accounts or attempts to hijack accounts.
- Multi-factor authentication should be used on all social media platforms, where possible.

Scams and phishing

- Online selling sites and marketplaces attract scammers.
- Pop-up messages pressure victims into new kinds of subscription traps.
- The number of various telephone scams has increased.

Malware and vulnerabilities

- Critical Log4shell vulnerability in the Apache Log4j component.
- Millions of text messages filtered in Finland to tackle the FluBot campaign.

IoT and automation

- A bill on consumer smart devices has been introduced in the UK. The law would ban easy-to-guess default passwords and require that customers are told how long security updates are available for the device.
- Researchers set up cyber traps to investigate the factors motivating attacks against IoT devices.

Network performance

- Four major disruptions in public communications services in November.
- Disruptions in AWS services.
- Denial-of-service attacks affected e.g. ICT service providers.

Spying

- Microsoft seized a set of NICKEL-operated websites and disrupted an espionage operation targeting 29 countries.
- Attempts to spy mobile devices made the headlines again.
- APT31 has abused hacked home routers to route malicious traffic.

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. Vulnerabilities mean devices and services connected to the internet with poor information security and insufficient protection and maintenance.

2

User credentials are valuable information in organisations Maintaining control over user credentials is important in any organisation. Credentials can be stolen via different kinds of attacks, and their loss may have a major impact on an organisation's activities.

3

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.

Symbols

New

Updated

4

Cloud services are new to many organisations, and attackers are often best experts in the information security of clouds. Organisations are rapidly migrating to cloud services but often do not understand their own environment and its capabilities well enough.

5

The information security of supply and service chains is becoming more and more critical. To ensure cyber security, organisations need to understand their own supply chains.

TRAFICOM

21.1.2022