TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber Weather

May 2022

#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

28.6.2022

Cyber weather May 2022

Data breaches and leaks

- Social media accounts have been targeted by data breaches or their attempts.
- Successful phishing attempts have resulted in breaches in Office 365 accounts. The breached accounts have been used to send messages.

Scams and phishing

- Thousands of text messages with fraudulent order confirmations have been sent in the name of the desktop wallpaper service Wallpaper and the game service Dorgames.
- Phishing for online banking details in the name of the Tax Administration.

Malware and vulnerabilities

- The infrastructure spreading the FluBot malware is no longer active, and the alert on FluBot has been removed.
- New guidelines help organisations who have become a victim of ransomware.

Automation and IoT

- The German cyber security authority BSI has published an information security certificate for consumer smart devices.
- Criminal activity can be concealed by exploiting IoT systems that are excluded from normal information security controls.

Network performance

- In May, network performance in Finland was very good.
- Denial-of-service attacks were reported, but there were no major impacts.

Spying

- APT41, or Winnti, has tried to spy on industrial companies all over the world.
- Groups reportedly associated with Russia have continued active operation in Europe, and cyberattacks are still taking place in Ukraine, too.

TRAFICOM

28.6.2022

TOP 5 Cyber Threats — Major Long-term Phenomena

1

Economic and political phenomena are reflected in cyber security.

Digitality cuts across all activities of organisations, and changes in the international security situation have a major impact on continuity and risk management in organisations.

2

Insufficient exchange of information leads to poorer situational awareness of cyber security.

A cyber threat encountered by one organisation today may be encountered by others tomorrow.

3

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.

Symbols

New

Updated

4

Cyber security depends on experts, and cyber security skills are important for all of us!

Increasingly diversified cyber security expertise is needed: there is a growing need for experts as new regulation is adopted and cyber security becomes an integral part of daily operations in businesses and organisations.

5

Access rights – the keys to an organisation.

Access control is important in any organisation. Credentials can be stolen via different kinds of attacks, and credentials in the wrong hands may have a major impact on an organisation’s activities.

TRAFICOM

28.6.2022