TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber Weather

November 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

Cyber weather, November 2022

Data breaches and leaks

- The number of data breach reports continues its steady rise. Growth from October to November was 12% and from September to November 27%.
- Increasing volumes of ransomware and wipers disguised as ransomware across the world.

Scams and phishing

- Police-themed scams and other forms of extortion remain a problem.
- The number of attempted payroll scams has increased.
- Black Friday in November sparked numerous scams.

Malware and vulnerabilities

- The United States cyber security authority CISA has a Shields Up website that includes a list of exploited vulnerabilities and instructions for vulnerability management.

Automation and IoT

- Growing cyber threats in industrial environments. The number of ransomware incidents has increased in the autumn.
- IoT devices exposed to old vulnerabilities because of neglected updates.

Network performance

- Two significant disturbances in public telecommunications services in November.
- Based on reports, November was the second most active month in terms of DoS attacks. The number of reports has been higher only in October.
- Some attacks have temporarily affected the availability of services.

Spying

- Cyber espionage and sabotage campaigns associated with the war in Ukraine continue.
- Information security researchers report Mustang Panda activity during the year.

TRAFICOM

12/19/2022

TOP 5 cyber threats – near future (6–24 months)

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

Cyber threat level in Finland has increased.

The increase in malicious traffic and the rise in the threat level make preparedness even more important in organisations.

3

Weaknesses in ordinary control measures still cause the majority of information security incidents.

For example, access rights management, keeping software up to date and good information security cultre are at the core of cyber security.

Symbols

New

Updated

4

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. Efficient sharing of information improves cyber security for all.

5

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.

TRAFICOM