TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

January 2023

#cyberweather

Cyber weather gives you an update on the key information security incidents and phenomena of the month.

The product is primarily targeted at those who work with information security issues at different levels of organisations. Cyber weather gives readers a quick overview of recent and upcoming events in the field of cyber security.

Cyber weather can be:  calm  worrying  serious

Cyber weather, January 2023

Data breaches and leaks

- A wave of phishing attacks has resulted in successful breaches of individual Microsoft Office 365 accounts. **Multi-factor authentication** has also prevented breaches!
- Social media accounts are still being targeted by active data breach campaigns.

Scams and phishing

- "Hi mom" SMS scams attempt to win the target's trust. Take a look at our instructions on how to protect your accounts!
- "Is it you in this video?" A scam circulating via Facebook Messenger steals the account holder's credentials.

Malware and vulnerabilities

- Malware report volumes have been low in the first months of the year.
- A vulnerability report was published in 2021 regarding the software VMWare ESXi. It is highly recommended to update the software or ensure that the vulnerable service cannot be accessed from the Internet.

Automation and IoT

- EU has taken action on the information security of smart devices. New non-compliant smart products can be withdrawn from the EU market as from 1 August 2024.
- Information security deficiencies have been detected in webcams sold in Finland. We remind all users of the importance of secure use and security settings.

Network performance

- Five significant disturbances in public communications services in January.
- The number of reported denial-of-service attacks reduced towards the end of the year, but some attacks did affect services.

Spying

- Social media is used to prepare phishing attacks.
- The UK cyber security authority has reported attacks against academia, state organisations, non-governmental organisations, think tanks, politicians, journalists and activists, among others.

NCSC-FI's tips and recommendations for improving cyber security preparedness:

It is important to patch the vulnerability in VMWare ESXi as soon as possible or to ensure that the vulnerable service cannot be accessed from the Internet. Because the campaign has been so extensive, it can be expected that servers with unpatched vulnerabilities have been breached.

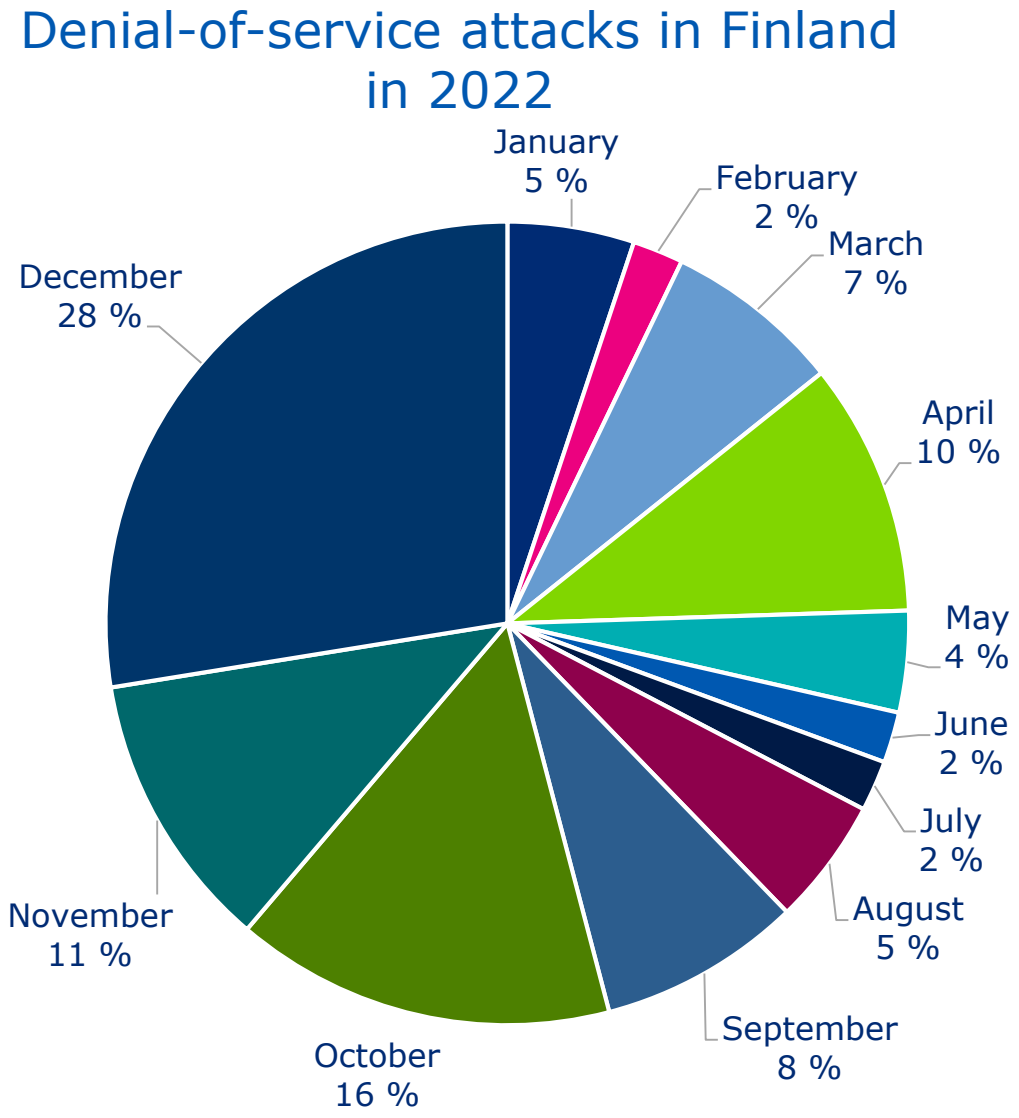
A password manager helps you store and use your passwords for different online services. Using the password manager to create strong passwords for different accounts keeps you better protected against the criminal use of leaked passwords.

The Finnish Transport and Communications Agency Traficom has granted support for the development of information security to first companies. The objective of the support is to improve the level of information security in companies and thereby make the whole society better equipped against cyber security threats.

Based on the NCSC-FI's observations, the default level of information security in modern devices is often poor. As from 1 August 2024, devices that do not meet information security requirements can be withdrawn from the market under the EU Radio Equipment Directive. To prepare for future rules, manufacturers, importers and vendors must immediately ensure that their products are sufficiently secure.

Overview of cyber weather in January

- In terms of information security incidents, January was quieter than the previous year, and no significant individual incidents with wide impacts were observed.
- However, January was marked by denial-of-service (DoS) attacks inspired by Killnet and other hacktivist groups.
- In addition to Europe and the United States, DoS attacks also targeted the websites of Finnish organisations, such as the Hospital District of Helsinki and Uusimaa. The number of reported attacks was still 71% lower than in December 2022.



Cyber security trends
in the past 12 months