TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

September 2024

#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

Monthly numbers

1 year.

Traficom's NCSC-FI's national attack surface mapping service (Hyöky) turned one year old in September! The service is aimed at municipalities and public administration organisations, but its subscription possibility is being extended to organisations that are critical to security of supply. [1, 14]

100/100

In the global cybersecurity index compiled by the International Telecommunication Union (ITU), Finland received a full score, ranked at level 1. [2]

1.

The Finnish Transport and Communications Agency Traficom has approved the first cryptography product to protect NATO classified information for the Insta SafeLink cryptography product solution. [3]

Cyber weather, September 2024

Data breaches and leaks

- The reported amount of data breaches has continued on the same, calm level.
- Dropbox themed M365 phishing and data breaches caused by it are the biggest single category.
- In comparison to last year, the number of ransomware attacks has been lower.

Scams and phishing

- SMS scams pretending to be from Traficom lessened when the SMS Sender ID protection registration entered into force at the end of September.
- Scams pretending to be from the Finnish Patent and Registration Office led to a phishing site that looked like the Suomi.fi identification site.

Malware and vulnerabilities

- Lumma Stealer malware has been spread in a new way since August.
- Two critical vulnerabilities have been found in Red Hat OpenShift.
- Vulnerabilities in the CUPS printing system allow arbitrary code execution.

Automation and IoT

- Criminals make great use of remote access software [4] installed on the systems of industrial automation users.
- According to security company Claroty, 55% of industrial automation environments connected to the internet have at least four different remote access software in them [5].

Network performance

- In September, two disruptions were detected in public communications networks.
- Domestic organisations reported denial-of-service attacks more actively than in the previous year.
- There were disturbances in the financial sector, which also gained visibility in the media. Nordea told the disturbances were partly due to denial-of-service attacks [6].

Spying

- U.S. authorities conducted a shutdown operation on a large botnet connected to China. [7]
- APT operators make use of botnets to, among other things, obscure the origin of malicious network traffic or make it difficult to detect it.

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

Under the NIS2 Directive, organisations will be obliged to report significant information security incidents to the supervisory authority. We published an article with tips on how to develop deviation management processes in organisations. [8]

Organisations must continue to prepare for denial-of-service attacks in various ways. Hactivists' application-level denial-of-service attacks and the now emerging carpet bombing technology are good examples of the attackers' efforts to continuously develop their methods.

The constant change in the operating environment sets expectations and demands for preparedness in both organisations and society at large. Regular exercise activities in preparation can be used to improve society's cyber resilience and operational reliability. The NCSC-FI participates in numerous exercises each year and supports cyber training for security of supply organisations as an authority service. [9]

Overview of cyber security in September

- In September, there was a slight increase in the number of cybersecurity cases after the calm summer months.
- Otherwise, there has been some rainy weather due to the recent denial-of-service attacks on Finnish organisations, as well as various phishing and scam campaigns.
  - In early autumn, the NCSC-FI has seen even more reports of denial-of-service attacks. Nordea, among others, has said that the recent disruptions were partly caused by denial-of-service attacks. So far, the effects have been limited in other cases. [10, 11]
  - In particular, Dropbox themed M365 code phishing has been active in early autumn. Numerous M365 account data breaches have been reported to the NCSC-FI as a result of Dropbox phishing. [12]
  - Text message scams pretending to be from Traficom are reflected in the police's national situational picture of fraud offences. According to the police, the combined criminal benefit of the scam cases in September alone was over 560,000 euros. The same phenomenon has been seen in the situational picture earlier in the summer, but in the autumn the phenomenon has seen growth, according to the police. [13]
- In addition, we observed more than usual activity of two different botnets in Finland.
  - The newer Quad7 botnet takes over especially Asus and TP-Link branded routers for home use. Observations have also been made on the Mirai botnet, which has been operating for several years. [14]

Cyber security trends
in the past 12 months