TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

November 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

Microsoft 365 phishing campaigns were especially active in November. The campaigns relied on Dropbox-themed messages, in particular.

It took less than two weeks to fix the C-Lion1 submarine communications cable. Damages to other cables than submarine cables can be detected and fixed in just hours.

Cyber weather, November 2024

Data breaches and leaks

- M365 accounts were actively breached with Dropbox-themed phishing messages leading to AiTM phishing sites.
- A few reports were received about online services that made data publicly available unnecessary widely and openly.

Scams and phishing

- S-Bank, OP, MyKanta and Danske Bank were popular among scammers in November.
- A significant share of scams phishing for online banking details still employ SMS.

Malware and vulnerabilities

- Services and control panels openly visible to the public internet have been reported to service owners.
- Attempts were made to exploit a vulnerability in Fortinet's old FortiEMS versions and FortiManager.

Automation and IoT

- Black Friday reminded us about the importance of continuity in security features and updates in online shopping. [1]
- A new version and Finnish translation of the automation system information security standard IEC 62443-2-1 has been released. [2]
- SANS has published a report on the state of OC/ITS cyber security. [3]

Network performance

- Six disturbances were reported in public communications networks in November.
- Broken telecommunications cables were fixed quickly. Networks continued to function despite the breakages.
- Denial-of-service (DoS) attacks have decreased towards the end of the year.

Spying

- Cyber espionage regularly exploits zero-day vulnerabilities.
- In November, reports were received abroad about a vulnerability in Fortinet's VPN software exploited by a Chinese actor, for example.

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

Data breaches utilising the adversary-in-the-middle (AiTM) technique can be detected and prevented by activating passwordless authentication and enforcing stricter Conditional Access policies for M365 services. [4, 5]

The NCSC-FI published tips for webshop administrators on how to detect and prevent digital skimming and what to do if they detect skimming. Digital skimming means stealing payment card data from the customers of an online store. [6]

Nato's Cyber Coalition exercise was organised in late November and early December. The cyber exercise is part of the continuous collaborative efforts of national authorities and their international partners to prepare for occurrences that affect the whole society. [7]

The guide Preparing for incidents and crises was published on the Suomi.fi website. Aimed at all residents in Finland, the guide includes a section on how to prepare for cyber attacks and incidents. The guide was drawn up by the Ministry of the Interior in cooperation with the Digital and Population Data Services Agency and a wide network of operators. [8]

Overview of cyber security in November

- November proved the importance of preparedness as Finland faced two very different anomalies in our digitally-enabled society. At the beginning of the week from 18 to 24 November, there was news of a submarine telecommunications cable (C-Lion1) breaking between Finland and Germany, and later in the week a strong storm hit Finland from the south. [9]
  - On 19 November, Traficom together with other authorities and Cinia, the owner of the C-Lion1 cable, organised a briefing on the damage to the submarine cable. The break in the cable has had no visible impact on Finland's IT connections to the world, and the security of supply of society has not been compromised. The National Bureau of Investigation is investigating the cable breakage.
  - During Storm Jari in November, tens of thousands of households in Finland were without electricity. Long power cuts can cause problems with mobile connections, for example.
  - Overall, the resilience of Finnish society is at a good level. Despite this, disruptions can have relatively short-lived local effects on telecommunications.
- The greyest month of the year was also tinged with scams and phishing campaigns in the name of banks. A significant share of scams phishing for online banking details still employ SMS.
  - Cases reported to the NCSC-FI also included Dropbox-themed M365 phishing attempts, some of which resulted in data breaches.
  - We have also received regular reports about information security incidents concerning hotel and travel booking services. Some of them have resulted in financial losses. For example, there are various active Booking.com-themed scams in Finland. We published an Information Security Now! article about the issue in early November. [10]
- In terms on DoS attacks, the situation has calmed down at the end of the year, and reports about disruptions caused by DoS attacks have been fewer than in the autumn.

Cyber security trends
in the past 12 months