TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

August 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, August 2023

Data breaches and leaks

- The abuse of the vulnerability in the Citrix Netscaler that was published during the summer was visible in data breaches in August. Taking advantage of the vulnerability seemed to be very quick and automated.
- Otherwise, the amount of notices have decreased to reflect the so-called normal level of the beginning of the year.

Scams and phishing

- Phishing in August has been very active.
- The messages sent by the hotel service booking.com are used for phishing for payment card details.
- Online banking details are phished both with a topical tax returns theme as well as with a text message disguised as a message from the postal services.

Malware and vulnerabilities

- The Citrix Netscaler vulnerability in July led to several data breaches in Finland.
- Updates should be installed as soon as possible when they become available.
- U.S. Authorities tell of preventing the operating of a Qakbot malware with an international operation.

Automation and IoT

- The circulation for comment for the harmonised standards of the data security regulation of the EU's Radio Equipment Directive (RED) has started.

Network performance

- There were nine significant disturbances in public telecommunications services in August.
- Power cuts caused a part of these disturbances.
- Regarding denial-of-service attacks, August was peaceful and the noticed occurrences did not have major effects on services.

Spying

- Targeted phishing can also happen via Teams.
- According to a Microsoft report, one campaign utilised phishing messages sent through Teams whose goal was to hijack the target's user account. In the messages, they appeared as IT support or as a representative of the information security team.

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

National Cyber Security Centre Finland has released a new tool to ease the planning of cyber exercises.

We published a guide on how to delete your information from the Yango taxi service.

The information security seminar Tietoturva 2023 will be held on 12 October 2023. You can watch the seminar for free online. Sign up now!

The open results review of the Ketjutonttu project will be held on 5 October 2023.

Traficom has published a web page regarding seafaring cyber security matters.

Overview of cyber weather in August

- During August, there were a lot of secure e-mail themed scam messages. Additionally, attempts were made again in the name of well-known operators such as the Police, Posti and Tax authority to swindle information and money from the recipients of the messages.
- In August we saw the very quick and automated exploitation campaign of the over the network exploited Citrix Netscaler vulnerability. The exploitation enabled leaving a backdoor (webshell) to the program and it stayed there even after updating the program.
- At the start of September, a hacktivist group announced they had attacked several European cyber security authorities.
  - National Cyber Security Centre Finland at the Finnish Transport and Communications Agency Traficom was one of the announced targets.
  - The effect of denial-of-service attacks is usually temporary in the service functionality. They have often been compared to a traffic jam or a protest carried out online, the goal of which is to create news.

Cyber security trends
in the past 12 months