TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

May 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, May 2023

Data breaches and leaks

- Report volumes concerning breaches compromising social media accounts increased almost 300 per cent in relation to the average from the beginning of the year.
- Reports on M365 data breaches also continued to increase in the beginning of the month. In late May, however, a slight improvement was observed.

Scams and phishing

- Tenacious scammers send text messages and make follow-up phone calls.
- More and more telephone scam calls are made using spoofed numbers. Traficom Regulation 28 obligates telecommunications operators to prevent caller ID spoofing from 2 October onwards.

Malware and vulnerabilities

- A zero-day vulnerability was detected in the MOVEit file transfer software. Exploitation has been detected in Finland and abroad.
- A zero-day vulnerability was identified in Barracuda ESG appliances.
- Vulnerabilities in Zyxel firewall and VPN devices. Exploitation has been detected in Finland and abroad.

Automation and IoT

- We published an Information Security Now! article with the title "Data breach against an industrial system supplier requires the supplier's clients to take swift action".

Network performance

- Four significant disturbances in public telecommunications services in May.
- Port operators targeted by DoS attacks.
- Especially application-level attacks have recently impacted for example the operation of websites.

Spying

- US authorities published a report on the Snake malware used by the cyber threat actor Turla.
- The report provides guidelines on how to detect the malware in infected systems.
- The authorities also conducted a removal operation of the malware from some of the infected systems.

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

New requirements for strong electronic identification that will enter into force in the summer of 2023 make the use of electronic services even more secure than before. The aim of the new requirements is to ensure that the user can check even more easily than before which service they are logging in to.

We published an article where organisations are reminded to also prepare for information security incidents targeted at suppliers. We ask that especially all industrial environment owners prepare for the possibility that a supplier critical for your own production is targeted by a data breach.

A new version of Kybermittari along with new supporting material is available on our website. Updates in the new version include features that make it easier to use the tool, to report observations to support decision making and the repeatability of the assessment. Register for summer and autumn presentation and training events!

Overview of cyber weather in May

- In May there was a considerable increase in reports concerning social media account breaches.
- At the end of last month double scams were also observed. In these scams a person is contacted several times via text message or phone calls. Scammers try to convince the target that their account is at risk and urges them to transfer the money to a secure account.
- Reports on M365 phishing increased in May but towards the end of the month a slight improvement was observed.
  - According to NCSC-FI’s knowledge, in approximately 60 organisations at least one M365 email account has been compromised since April.

Cyber security trends
in the past 12 months