TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

November 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, November 2023

Data breaches and leaks

- Ransomware attacks caused by data breaches were especially targeted at industrial sectors in November. In most cases, the Akira and LockBit cybercriminal groups were behind the incidents.

Scams and phishing

- An extensive text message campaign at the beginning of November tried to trick people to send rent money into the wrong bank account.
- The owners of Facebook pages were intimidated with closing the pages for various reasons. The scammer tried to hijack the pages for themselves.
- Online bank ID phishing scared people with unknown payments and account closures.

Malware and vulnerabilities

- We have received several reports of ransomware detections.
- Cisco devices had several critical vulnerabilities that required immediate updating.
- We mapped the Citrix Bleed vulnerability (CVE-2023-4966) and contacted several organisations.

Automation and IoT

- A political agreement was reached on the EU Cyber Resilience Act (CRA).
- Unitronic's programmable logic controllers (PLC) have also been hacked in Finland. The controllers are used from water treatment plants to small power plants. The attacks have been successful due to, among other things, weak default passwords.

Network performance

- There were seven major disruptions in public communications services in November.
- Hacktivists also targeted Finland with denial-of-service attacks in November.
- Organisations have not reported significant service effects regarding denial-of-service attacks.

Spying

- Finnish Security and Intelligence Service warned again about the use of network devices intended for consumer use in cyber espionage in November.
- Weakly protected and vulnerable devices connected to the Internet are broken into as part of the attack infrastructure, and by exploiting them, it becomes more difficult to detect a cyber attack.

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

Since the summer, it has been noticeable that cybercriminals have accelerated their ability to exploit the vulnerabilities that have become public. Updates must be taken care of every day of the year, including the coming Christmas holidays.

Backup mnemonic form 3 – 2 – 1. Take at least 3 backups, store them in at least 2 different formats and locations, and keep at least 1 backup offline.

We published a new guideline Security is a matter for the entire organisation - tips for planning personnel security training.

Data security development support for 24 companies - all subsidies of a maximum of 100,000 euros were distributed.

Overview of cyber weather in November

- November's trends included the use of known vulnerabilities in data breaches and ransomware attacks.
  - In November, numerous critical vulnerabilities were announced, requiring immediate update or restrictive measures from administrators.
  - The ransomware Akira has been found to be exploiting the Cisco network device vulnerability (CVE-2023-20269) in Finland as well.
- Ransomware actors often seek to encrypt or destroy backups as well. In this way, criminals make it significantly more difficult for companies to recover organically. So keep at least 1 backup offline.
- E-mail accounts are among the favourite targets of criminals. Sensitive information should be sent by encrypted e-mail and stored elsewhere than in the e-mail box.

Cyber security trends
in the past 12 months