TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

May 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

Cyber weather May 2024

Data breaches and leaks

- The City of Helsinki Education Division was the target of an extensive data breach.
- Tens of thousands of unauthorized searches were made to the authorities' registers as a result of the data breach targeting the customer organisation.
- It is estimated that criminals have acquired hundreds of thousands of instances of personal data.

Scams and phishing

- There has been a new Microsoft Planner phishing theme in M365 account breaches.
- At the end of May, an extensive SMS scam campaign was launched, threatening people with an unpaid fine claiming to be from Traficom. The link led to online banking details phishing.

Malware and vulnerabilities

- Thousands of Finnish IP addresses are included in the 911 S5 botnet.
- Online banking details are stolen with the new Android malware.
- Check Point Quantum Gateway vulnerability was exploited.

Automation and IoT

- Politically motivated hackers around the world targeted attacks on industrial control systems.
- Data breaches occurred e.g. to weakly protected programmable logic controllers and industrial routers.
- The safety controls of automation systems should be checked regularly.

Network performance

- There were 10 disruptions in public communications services in April.
- Only a few denial-of-service attacks were reported during the month and their effects remained mild.

Spying

- Poland reported of a campaign targeting its government in which harmful emails had been sent to the targets. The perpetrator was estimated to be the APT28 group linked to Russian military intelligence.
- On the other hand, in Germany it was reported that APT28 was spying on Social Democratic Party emails in a breach that began in 2022.

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

Mitigating cyber threats with limited resources - a guideline for civil society has been published.

Traficom has prepared a draft recommendation to NIS-supervisory authorities on cybersecurity risk management measures. The draft recommendation also sets out basic security practices. Cyber hygiene practices provide the foundation for an organisation's cyber security.

Unupdated network edge devices are still heavily exploited in data breaches. Organisations should ensure that these products are deployed with security in mind and that updates are always up-to-date.

The National Coordination Centre (NCC-FI) organises a free two-part training on the presentation and application of cybersecurity proposals in the Digital Europe programme on 18 June and 28 June 2024. Sign up!

Overview of cyber weather in May

- The 911 S5 botnet, which was closed in May 2024, provided criminals with access to compromised IP addresses and related devices owned by individuals and businesses. Thousands of Finnish IP addresses were also included.
  - Free, illegal VPN services were packaged in pirated video games and software that victims downloaded to their devices. When the download was complete, the VPN app and the proxy backdoor installed on their devices without the victims knowing, and they unknowingly became part of the 911 S5 botnet.
- The data breaches and leaks that have occurred in Finland over the past month have been unusually extensive.
- The theme of the Microsoft Planner scheduling and task sharing app is used in phishing by sharing a PDF file with a link to the phishing page.
  - The NCSC-FI was notified of 53 phishing attacks on Microsoft 365 email accounts. Of those, 25 led to a data breach of a Microsoft 365 email account.

Cyber security trends
in the past 12 months