TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

July 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, July 2024

Data breaches and leaks

- M365 account breaches darkened the sunny summer weather. The number of breaches increased in July compared to previous months. Especially AiTM attacks were used in attempted account breaches.
- In total, the number of data breach reports was halved during the summer in comparison to the start of the year.

Scams and phishing

- A scammer claims to be calling from the bank and frightens the victims by telling of suspicious bank transfers abroad. The scammer asks for online banking credentials for the “refund account”.
- In text messages, the scammer intimidates victims with a "fine going into debt recovery" by the names TRAFCOM and TRAFCORN, similar to those of the authorities.

Malware and vulnerabilities

- The CrowdStrike disruption on 19 July activated opportunists: CrowdStrike's name was used to fish for information and distribute malware that was claimed to fix problems caused by the update.
- A critical vulnerability was found in the Cisco Secure Email Gateway (formerly IronPort).

Automation and IoT

- Disrupting wireless burglary protection and camera surveillance systems is technically easy. In the United States, police have warned that the phenomenon is on the rise. Part of the reason for this growth is probably the proliferation of surveillance cameras in homes.

Network performance

- There were nine disturbances in public telecommunications services in July.
- DoS attacks were also reported during the summer, but the service effects have been non-existent.
- Not all denial-of-service attacks can be linked to hacktivists.

Spying

- The APT45 (Andariel), a cyberthreat operative linked to North Korea, has used ransomware programs against U.S. healthcare providers to earn money for the state.
- The targets of APT45’s espionage include the defence industry, aviation, and nuclear-related organisations.

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

We published the guide "Social media accounts in order, tips for the safe use of social media." The guide is suitable for both individuals and those updating their company's social media.

Some ransomware programs have also tried to find and destroy their target's backup copies. For the most important backups, it is recommended to follow the 3-2-1 rule: keep at least **three** backups in **two** different locations and keep **one** of these copies completely offline.

The Digital Europe programme's funding application training is held on 27 August 2024. The application training will present funding calls for the cyber security work programme of the Digital Europe Programme and, under the guidance of experienced experts, will go through concrete advice and tips on how to prepare high-quality applications for the Digital Europe Programme.

Overview of cyber security in July

- July was very calm and the summer holiday season was also noticeable in the overview.
- An update to the CrowdStrike security product caused a glitch that prevented Windows devices using that product from booting. The disruption caused downtime in several services worldwide, affecting payments, air traffic, train traffic, health care and media houses, among others. There were also organisations in Finland that were affected either directly or indirectly through the supply chain.
- We received several reports of various Microsoft 365 user account phishing attempts targeting organisations during July. Some of the phishing led to an e-mail account data breach.
- Various scam messages were also sent during July. Criminals also move with the times and at the end of the month tax refund-themed scam messages began to become more common, because tax refunds will become topical for many from August onwards.
- Denial-of-service attacks targeted various organisations, particularly the central government, during July.

TOP 5 cyber threats in the near future (6–24 months)

1. 🔄

Serious vulnerabilities are being exploited faster and faster

In addition to installing an update that fixes the vulnerability, it is often necessary to investigate whether the vulnerability has already been exploited before installing.

2. 🛡

Ransomware - Significant threat to organisations

Over the past year, several organisations in Finland have fallen victim to ransomware, and their number is also growing globally.

3. 🔄

The information security and continuity of supply and service chains are increasingly critical.

To ensure cyber security, organisations need to understand their own supply chains. Most organisations are more or less dependent on outsourced digital services.

🛡 New

🔄 Updated

Symbols

4. 🔄

Organisations should prepare for AI-related challenges.

Organisations should try to identify challenges that artificial intelligence may cause and prepare for them by training their staff, for example.

5. 🛡

Importance of protecting telecommunications infrastructure emphasised

It is important to protect telecommunications and information system infrastructure both abroad and at home, both because of incidents and natural phenomena and because of deliberate disturbances caused by outsiders.

1 mo.

Cyber security trends
in the past 12 months

	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul
Data breaches and leaks	⛈	🌦	🌩	⛈	⛈	🌧	🌧	🌧	🌩	🌩	🌦	🌦
Scams and phishing	⛈	⛈	🌩	🌧	🌧	🌩	🌦	🌧	🌩	🌩	🌧	🌧
Malware and vulnerabilities	🌧	🌧	🌩	🌩	🌩	⛈	🌧	🌧	🌩	🌧	🌦	🌦
Automation & IoT	☀	☀	🌧	🌦	🌧	🌦	🌧	☀	⛈	🌧	🌧	🌦
Network performance	🌧	🌧	⛈	🌧	🌦	🌧	🌧	🌦	🌧	🌧	🌧	🌦
Spying	🌧	🌧	🌧	🌧	🌧	⛈	🌧	🌧	🌧	🌧	🌧	🌧