TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

# Cyber weather

September 2025

# Cyber weather, September 2025

## Data breaches and leaks

- Compromised Microsoft 365 accounts are often used to quickly send out large volumes of new phishing messages.
- In some cases, M365 breaches are prolonged: attackers remain in the environment, observing activity for months before using the victim's credentials to commit invoice fraud.
- Data breaches have also been carried out by exploiting vulnerabilities in edge devices, such as firewalls and VPN solutions.

## Scams and phishing

- Scam call blocking won the 2025 crime prevention award. By blocking spoofed calls, millions of scam calls have been successfully prevented.
- Data breaches of Microsoft M365 email accounts continued to increase. In September, a severe alert was issued about M365 phishing. Phishing-based data breaches remain the most common way to gain unauthorised access to company systems.

## Malware and vulnerabilities

- At the end of September, operations at several airports across Europe were paralysed following a ransomware infection. As an indirect consequence, flights from Finland were delayed and rerouted.
- Critical vulnerabilities in Cisco ASA and FTD products have also been exploited in attacks worldwide.

## Automation and IoT

- The United States Federal Highway Administration urged authorities to inspect road digital infrastructure for hidden components, such as concealed radios. Such devices could potentially be used to disrupt or spy on road operations.
- In Europe, the Cyber Resilience Act (CRA) and the NIS2 Directive establish strong frameworks for addressing these types of cyber threats originating from supply chains.

## Network performance

- Several Finnish organisations were targeted by denial-of-service (DoS) attacks. Thanks to good preparedness and active countermeasures, there were no significant impacts on service availability.
- The effects of DoS attacks can also be seen in services that are not directly targeted. Shared resources may become overloaded, causing disruptions to multiple services simultaneously.

## Spying

- The activity of Iran-linked threat actors in Europe has reportedly increased. One APT group was reported to have attempted to infiltrate telecommunications operators' systems through recruitment scams, while another sought information from organisations in the satellite sector and the defence industry. Targets in these campaigns included entities in the United Kingdom, France, Sweden and Denmark.

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

Phishing targeting Microsoft 365 accounts has remained active. Due to the sharp increase in case numbers and the resulting risk, the NCSC-FI issued an alert about the phenomenon.

A denial-of-service attack can disrupt business operations and become a recurring nuisance without sufficient anticipation. Preparedness includes pre-attack planning, such as administrative and technical measures, active response during an attack and appropriate follow-up actions afterwards. You can read more about the topic in the Information Security Now! article "Anticipation is the best defence against denial-of-service attacks" (in Finnish).

The NCSC-FI's weekly reviews now feature a new section dedicated to malware. The malware review is designed especially for readers who are not yet very familiar with malware.

# Overview of cyber security in September

The onset of autumn brought rainy skies also in the field of cybersecurity. September was moderately active in terms of incident numbers, with notable cases attracting media attention both in Finland and abroad.

- In Finland, denial-of-service attacks began to appear in the threat landscape after mid-September. Many of these attacks deliberately targeted websites and organisations likely to draw public attention. The resulting disruptions were, however, mostly short-lived. For many organisations, denial-of-service attacks have become relatively routine, and recovery is often swift.
- Phishing and data breaches targeting Microsoft 365 accounts continued their upward trend, prompting the issuance of an alert.

A large-scale cyberattack disrupted operations at several European airports starting on 19 September.

- A ransomware attack targeting Collins Aerospace, a company providing check-in and boarding services, affected passenger transport at airports including Brussels, Berlin and Heathrow.
- The attack caused flight delays and cancellations. Some airlines successfully implemented alternative methods to serve passengers — in some cases, boarding passes were even issued manually.
- Overall, the attack impacted airport operations for about a week, with the most severe disruptions occurring in the first few days. As late as 9 October, Berlin Brandenburg Airport’s website was still reporting disturbances caused by the cyberattack.

# Cyber security trends
in the past 12 months

1 kk