

TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

September 2026

Cyber weather

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 cybersecurity.

Cyber weather can be:



calm



worrying



serious



Overview of cyber weather

September 2026

Rain and storms at the network edge

The cybersecurity situation in Finland in September was characterised particularly by scams, website breaches and critical vulnerabilities in network edge devices. Scams once again took many forms, with CEO fraud attempts observed almost daily. Breaches of Finnish WordPress sites and the distribution of malware using the ClickFix technique continued. In addition, several critical vulnerabilities under active exploitation were disclosed in September, affecting products from Cisco, F5, Check Point and GitLab, among others.

At the end of September, the NCSC-FI issued a severe alert about vulnerabilities in Citrix NetScaler ADC and Gateway products that have been exploited in several data breaches in Finland. In this case, patching alone is not sufficient: organisations must also examine their environments for signs of compromise.

Lightning strikes edge devices abroad

- Zero-day vulnerabilities in Citrix NetScaler devices were exploited globally from the beginning of September. Targets included public sector and financial organisations in Europe and North America.
- Norway experienced several large-scale denial-of-service attacks in late August and September. A pro-Russian hacktivist group claimed responsibility for some of the attacks.
- No similar activity has been observed in the other Nordic countries, but Denmark raised its cyber threat assessment for destructive cyberattacks to high in September.



Hail shower of the month

The quantum transition is coming – are you ready?

At the end of January, the NCSC-FI published a guidance website on the threat posed by quantum computers to current encryption methods. As a follow-up, the NCSC-FI has now published a short presentation on transitioning to quantum-safe cryptography. Its four clear slides outline the key issues that organisational management should consider when preparing for the quantum transition.

Advances in quantum computing are changing the security assumptions underlying current encryption methods. The quantum threat particularly concerns data that must remain confidential far into the future, such as personal data, health data, trade secrets and non-disclosable government information.

Quantum threat does not begin on Q-day

- The quantum threat is sometimes described using the term **Q-day**, which refers to the point at which quantum computers become capable of breaking widely used classical asymmetric encryption methods in practice.
- However, Q-day is not a clear dividing line before which the threat does not exist. A significant part of the quantum threat involves attackers collecting encrypted data before Q-day and storing it for decryption at a later date. This is known as the harvest now, decrypt later strategy.

NCSC-FI's tips and recommendations for improving cybersecurity preparedness



The NCSC-FI issued its first severe alert of the year. The alert concerned critical vulnerabilities in Citrix NetScaler ADC and Gateway products disclosed in late September.



Credential phishing is a common method used to compromise organisations' Microsoft 365 user accounts. An article published on our website explains how Microsoft 365 credential phishing and account takeovers unfold, how to detect and contain a data breach, and what technical security measures organisations can take to reduce the risk of user accounts being compromised.



Threat modelling enables organisations to identify security risks in software and systems as early as the development stage and systematically integrate security into software development. We published a set of materials and accompanying training courses on our website to help organisations get started with threat modelling and practise applying it.

Cyber weather phenomena

In this section,
we review developments and trends
in key cybersecurity phenomena.



Cyber weather

September 2026



Data breaches and leaks

The number of data breach reports increased by 81.5% in September compared with the previous month. Attackers exploited software vulnerabilities in data breaches, while ransomware attacks particularly targeted small businesses.



Malware

During the reporting period, several Finnish websites were observed distributing malware using the ClickFix technique.

Malicious packages and malware were distributed through GitLab.



Vulnerabilities

As many as eight vulnerability advisories were issued during September.

The number of vulnerabilities being exploited has increased, and attackers are exploiting them more rapidly.



Scams and phishing

According to a recent report by Finance Finland, banks prevented more than half of all attempted scams in the first half of the year. Nevertheless, the number of scam attempts increased by almost a third compared with the same period the previous year.



Automation and IoT

Research findings on vulnerabilities in electric vehicle charging systems were presented at the VehicleSec '26 and WOOT '26 conferences. Attackers could exploit these vulnerabilities for financial gain or to disrupt charging. Videos of the presentations were released in September.



Network performance

During September, a few hacktivist-motivated denial-of-service attacks targeting Finnish organisations were observed.



Cyber weather

September 2026 1/2



Data breaches and leaks

- Software vulnerabilities continued to be exploited in many data breaches. More than half of these incidents involved the exploitation of vulnerabilities in WordPress websites.
- Ransomware attacks particularly targeted small businesses. Attackers gained access to systems by exploiting vulnerabilities or using VPN credentials without multi-factor authentication.
- The number of Microsoft 365 account breaches increased sharply towards the end of the month



Malware

- During September, the NCSC-FI received several reports of Finnish websites distributing malware or malicious code using the ClickFix technique. The websites had often been compromised by exploiting WordPress vulnerabilities.
- The NCSC-FI received observations and reports of malicious repositories being distributed through GitLab. However, these were quickly removed.



Vulnerabilities

- Citrix NetScaler vulnerabilities were particularly prominent among the vulnerability advisories issued in September.
- As vulnerabilities are being exploited at an increasingly rapid pace, it is more important than ever for organisations to understand their own network environments and attack surfaces, and to apply security updates promptly, particularly to network edge devices.
- In addition to applying updates, organisations should often also check whether vulnerabilities have already been exploited before patching.



Cyber weather

September 2026 2/2



Scams and phishing

- According to a recent report by Finance Finland, banks prevented more than half of all attempted scams in the first half of the year. Nevertheless, the number of scam attempts increased by almost a third compared with the same period the previous year.
- In addition to traditional phishing and investment scams, criminals attempt to use stolen online banking credentials to open new banking and mobile phone services and obtain loans and hire purchase agreements.
- The report's key message is that scams are becoming increasingly common and the methods used are evolving rapidly.



Automation and IoT

- The risks associated with charging infrastructure are not limited to data breaches.
- Software flaws in electric vehicle chargers can cause charging to continue when it should stop or result in charging costs being billed to someone else. Security weaknesses in older communication protocols can allow attackers to discharge vehicle batteries or charge vehicles without authorisation.
- In Finland, the Cybersecurity Act imposes requirements on charging point operators if they are sufficiently large or their operations are otherwise considered critical.

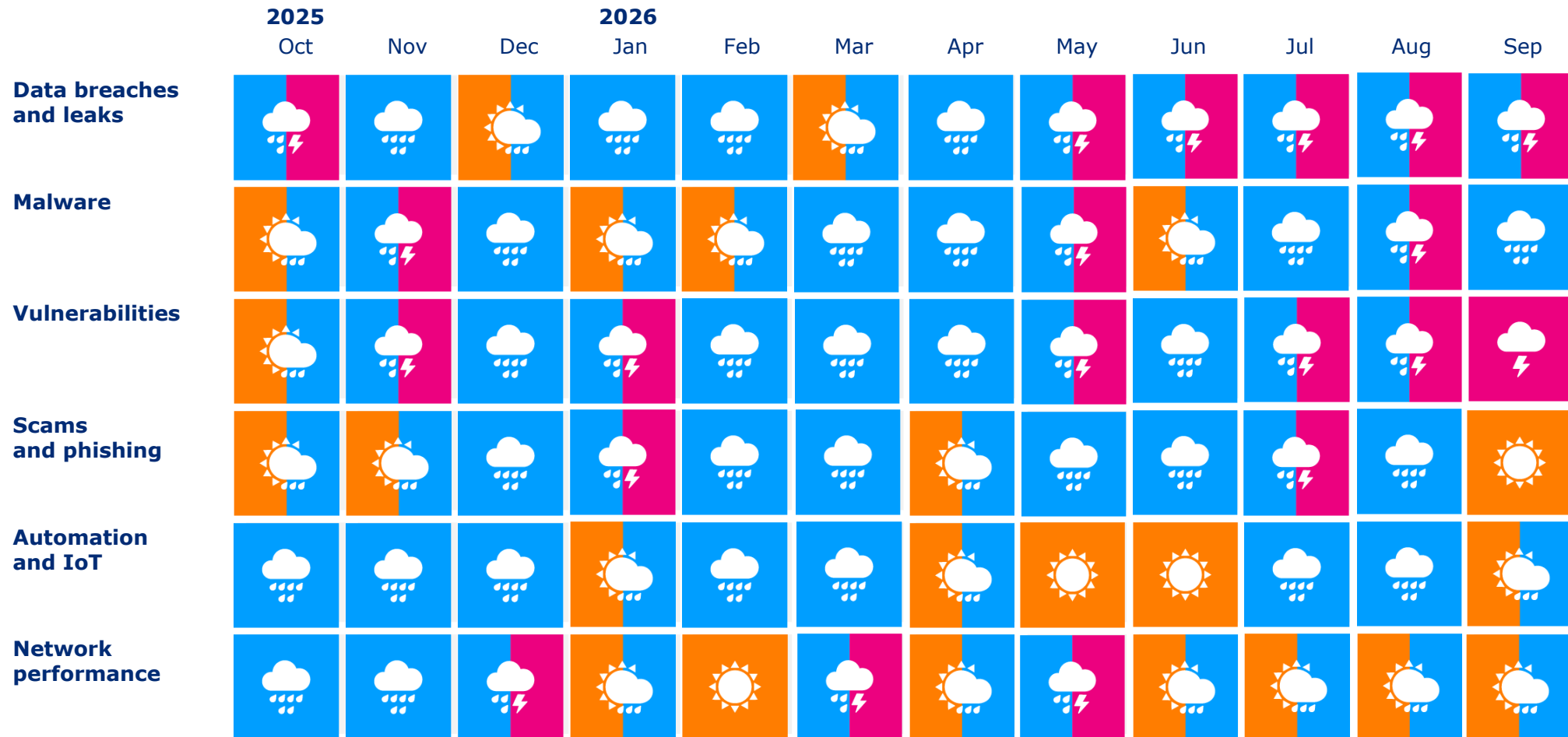


Network performance

- During September, a few hacktivist-motivated denial-of-service attacks targeting Finnish organisations were observed. Some individual attacks had minor impacts at most, causing brief service outages.
- Europol's Operation PowerOFF works with international law enforcement partners to shut down commercially available services used to carry out denial-of-service attacks. As part of the operation, authorities seek to disrupt the operation and use of these services.



Cyber weather in the past 12 months



Cyber weather forecast

The cyber weather forecast provides a summary based on previous observations and an indicative assessment of cyber threats and their likely developments in the coming months.



Cyber weather forecast

Cyber threats remain at a typical level

October has started with unsettled cyber weather, and conditions are likely to remain much the same throughout the month. The Citrix storm that emerged in late September is not yet over, and its effects will be monitored during October. Opportunistic exploitation of the vulnerability may continue. Scams are likely to continue bringing rainy conditions, with scattered showers expected in the form of website breaches.

The reporting obligations under the Cyber Resilience Act began to apply on 11 September 2026, so October will bring the first experiences of manufacturers' reporting practices.

For users, this means more up-to-date information on vulnerabilities affecting their devices.



The cyber weather forecast provides a summary based on previous observations and an indicative assessment of the cyber threat situation. It should not be used as the sole basis for preparedness – organisation-specific information and analysis must also be considered.



Worrying

The volume and severity of cyber threats are at a typical level.

However, the threat landscape can change rapidly — including in a negative direction.



TOP 5 cyber threats in the near future

1 Serious vulnerabilities are being exploited 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 the patch.

2 The increasing use of AI requires risk management

Organisational preparedness and active risk management measures are essential as the use of artificial intelligence increases rapidly.

3 Information security and continuity of supply and service chains

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

4 Protecting critical infrastructure is essential

The rapidly evolving cyber landscape affects the protection of critical infrastructure.

5 Ransomware is a significant threat to organisations

The number of ransomware incidents continues to increase globally.