TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

# Cyber weather

April 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, April 2024

## Data breaches and leaks

- The Palo Alto critical vulnerability CVE-2024-3400) resulted in several data breaches and data breach attempts. We received c. 15 notifications, due to which we avoided serious harm.
- In April, M365 user accounts were breached with DropBox themed phishing messages. Part of the breaches used the AiTM technique.

## Scams and phishing

- Android phones are the target of malware being spread through scam messages presenting as being from a collection agency. Phone calls and text messages that look like they have been sent by Kredinor direct you to install an "antivirus program" on your phone, but it is in fact malware that steals online banking details.
- Phishing sites have been created that use .fi in the domain name presenting as, for example, The Finnish Patent and Registration Office.

## Malware and vulnerabilities

- Alert 1/2024: A vulnerability (CVE-2024-3400) in a Palo Alto GlobalProtect product that is widely used in organisations was being actively exploited.
- After the amount of notifications made to NCSC-FI decreased, the Warning was removed on 7 May 2024.

## Automation and IoT

- Consumer products have had significant cybersecurity problems. In some cases, consumers have been dissatisfied with the communications about them. Poor crisis communications is a significant reputation and business risk for a company.
- Planning and practising crisis communications is central for business continuity management.

## Network performance

- There were 9 disruptions in public communications services in April.
- Denial-of-service attacks orchestrated by hacktivists have targeted Finland during April.
- Other denial-of-service attacks have not been reported to have had significant effects.

## Spying

- Observations connected to Sandworm were present in several publications.
- Malware used by the operator as a backdoor was detected in countries such as  Ukraine and Estonia.
- In Ukraine, the operator was reportedly preparing attacks on local energy, water and heat production.

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

M365 data breaches utilize the AiTM phishing technique increasingly. We published a guide where we go over the progression, recognition and protection against AiTM phishing.

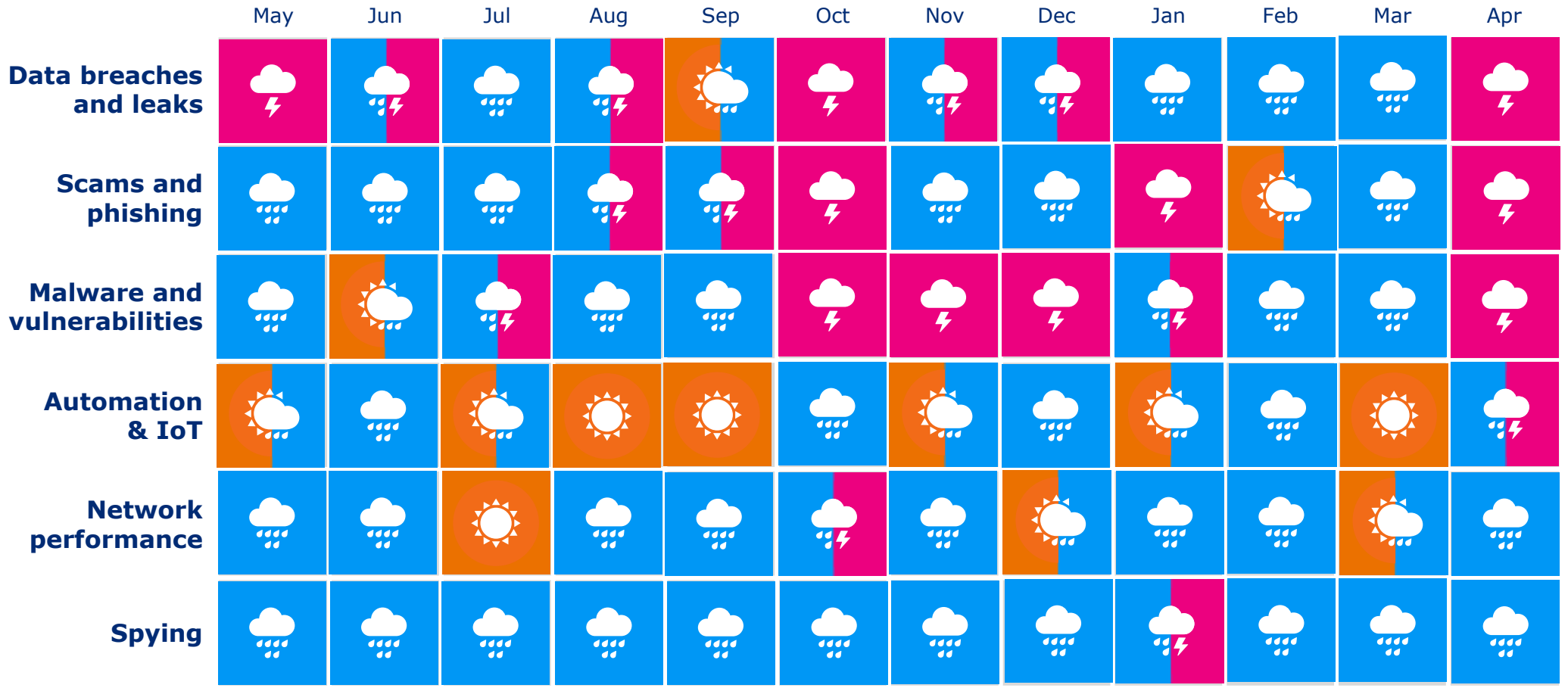
Criminals have asked for ransom for returning the breached user accounts. You should never pay the ransom because it supports the continuation of crime and ransom activities.

Read in our new blog post the tips for fighting against the operational conditions of Mirai and many other malware variants.

# Overview of cyber weather in April

- We published a Warning 1/2024 on 18 April 2024 regarding the data breaches targeting Palo Alto GlobalProtect products.
  - Palo Alto GlobalProtect Gateway, and GlobalProtect Portal that is used to manage the Gateway, are products which organisations use, for example, for safe VPN remote work solutions.
  - The situation turned out to be calmer than was anticipated, and the Warning was removed on 7 May 2024.
- Fitsec has published a way to decrypt the Akira malware and is offering its assistance to victims of Akira on its website.

# Cyber security trends
in the past 12 months



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

## 1.

**Threat level in Finland's cyber environment remains heightened.**

The number of targeted attacks has increased. The heightened threat level increases the importance of preparedness in organisations.

## 2.

**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.

## 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.

**Cyber security depends on experts and cyber security skills are important for all of us!**

As new regulations and cyber security meld into a part of the daily functions of companies, the need for different experts increases further. Additionally, from the point of view of risk management and continuity, ensuring sufficient competence during all seasons is important for organisations.