TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

July 2023

#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 2023

Data breaches and leaks

- In July the amount of reports decreased to reflect the levels of the start of the year.
- The decrease was steady regarding both social media account breaches as well as breaches directed toward company emails.

Scams and phishing

- Scam messages avoid email filters by hiding the phishing links behind a QR code.
- Online banking details were phished throughout the summer by intimidating people using the name of banks or the suomi.fi service.

Malware and vulnerabilities

- Several critical vulnerabilities have been made public in July.
- NCSC-FI has done mapping work of critical software vulnerabilities in July. So far, not a single organisation in Finland has reported any confirmed exploitations.

Automation and IoT

- The US will introduce a new voluntary smart device cyber security certification and marking program "U.S. Cyber Trust Mark" in the year 2024.
- The need for device updates must be monitored during the holiday season as well by utilising the risk-based vulnerability control

Network performance

- There were six significant disturbances in public telecommunications services in July.
- President Biden’s visit did not cause malfunctions on websites.

Spying

- A Storm-0558 operator connected to China breached the email accounts of organisations of central government in western countries after gaining access to an encryption key with which it could create falsified Microsoft account login details. Additionally, this attack utilised a deficiency in the confirmation of these details.

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

We published a new guide where we give advice on the information secure use of a phone.

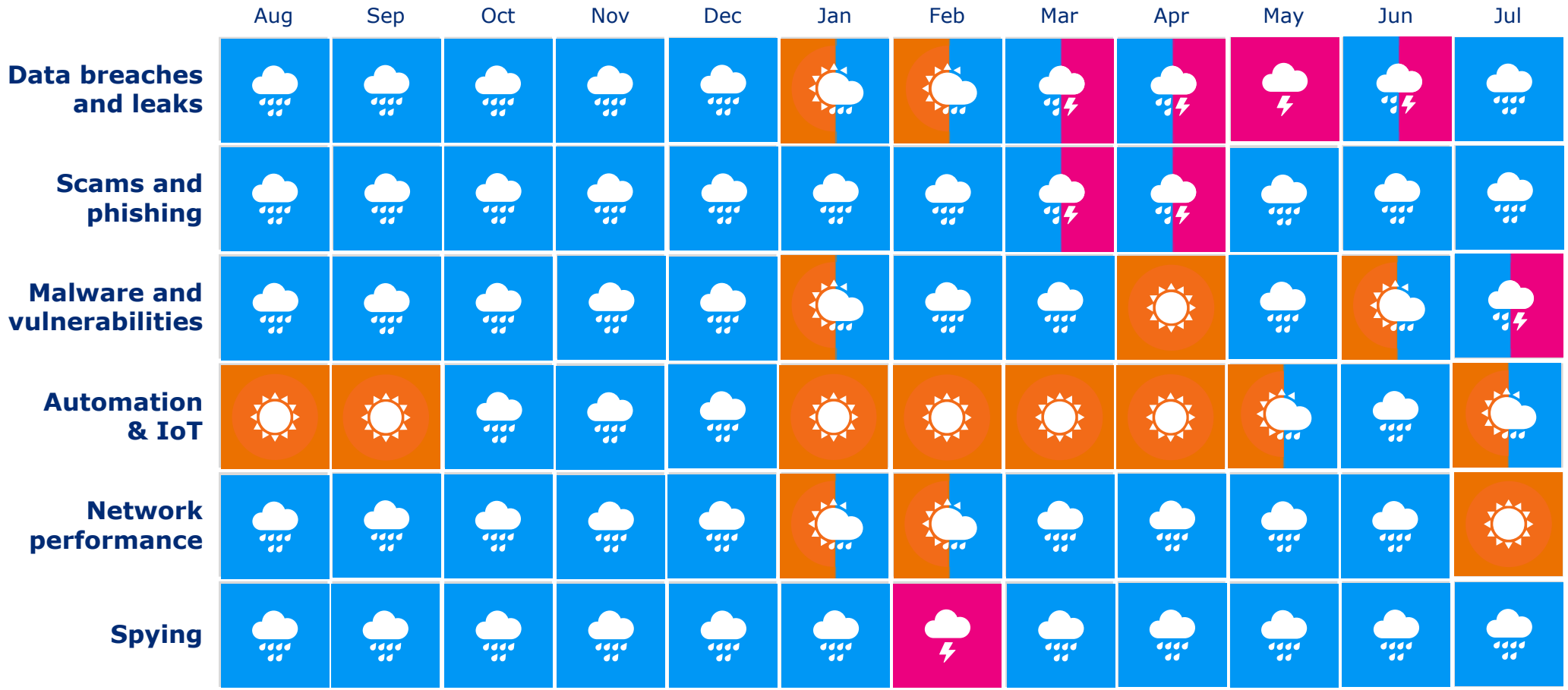
We shared our tips for an information secure summer.

We advised in our Information Security Now! article how to avoid an eSIM scam and how to identify one.

Overview of cyber weather in July

- Several updates to critical products also widely used in Finland were published in July. NCSC-FI mapped the situation immediately in Finland once the vulnerability was made public and contacted over a hundred organisations regarding the vulnerabilities.
  - So far not a single organisation in Finland has reported exploitations regarding these vulnerabilities.
- It is recommended to take care of the updates of devices and systems during the holiday season as well.

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.

Political and economic phenomena are reflected in cyber security.

The phenomena may affect the digital environment quickly, and their impact on cyber security may be difficult to predict.

3.

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.

New

Updated

Symbols

4.

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.

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.