TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

June 2020

#cyberweather gives you an update on the key information security incidents and phenomena of the month. We want to give our readers an overview of what has happened in the field of cyber security during the past month. The situation can be:

☀ calm

🌧 worrying

⚡ serious

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber Weather, June 2020

Data breaches and leaks

- Wide-ranging hacking campaigns targeting email accounts observed in Finland.
- Data breaches and breach attempts into customer loyalty systems.

Scams and phishing

- Frequent phone calls from scammers pretending to be technical support.
- CEO scams and other forms of billing fraud are on the increase during the summer holiday season.

Malware and vulnerabilities

- A number of critical vulnerabilities affecting e.g. Palo Alto Networks and F5 VPN solutions as well as Citrix's Application Delivery Controller (ADC), Gateway and SD-WAN WANOP products.

Automation

- EKANS malware attacks targeted Honda and the ENEL Group.
- June also saw the publication of notable automation and IoT studies.

Network performance

- A total of 12 notable disruptions, of which three caused by summer storm Päivö.
- The multi-year downward trend in the number of notable disruptions appears to have given way to a slight increase.
- June saw only relatively few DoS attacks.

Spying

- Social media platforms can be exploited in order to distribute malicious messages and attachments.
- Organisations' network systems and secure connection solutions are attractive targets for attackers looking for weaknesses or attempting to steal data.

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

TOP 5 Cyber Threats — Major Long-term Phenomena

1 ➡

Phishing
is extremely common and potentially difficult for the target to identify. This is also exploited in the context of targeted attacks and spying.

2 ⬆

Vulnerabilities are being exploited at a faster pace, which requires speedy updates. Devices and services are left exposed to the internet, with insufficient attention paid to data security, administration and protective measures.

3 ⬇

Ransomware attacks with wide-ranging effects pose a threat to the continuity of business operations. Individual attacks have caused damage worth tens of millions of euros.

⬆ *increase*

⬇ *decrease*

➡ *no change*

4 ➡

When the **division of responsibility** among service providers, contractors and buyers is muddled, cyber security suffers. Deficiencies in log monitoring make detecting threats more difficult.

5 ➡

Organisations are unable to manage cyber risks.
Risks are underestimated as a result of an inability to assess the impact of threats on business operations. Aspects of recovery plans are inadequate.

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre