TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

November 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, November 2020

Data breaches and leaks

- Several ministries targeted by data breaches in Estonia.
- Office 365 security breaches continued, with breached email mailboxes used to send phishing messages.

Scams and phishing

- Frequent scam phone calls, SMS fraud perpetrated in Posti's name and O365-themed phishing scams.
- Wangiri phone call scams on the rise again, now from +212 numbers.
- Phishing is an important tool for criminals perpetrating targeted data breaches.

Malware and vulnerabilities

- The number of detected Emotet incidents has decreased, and the warning related to them has been removed.
- Old vulnerabilities of Fortinet VPN technologies have been exploited.
- Secure email messages sent in the name of banks have been used to spread malware.

Automation and IoT

- Disruptions in AWS impacted robot vacuum cleaners and other devices around the world.
- Criminals used IoT devices located in Finland to route network traffic related to credit card fraud.
- The Gitpaste worm can also infect IoT devices.

Network performance

- A slightly higher than usual number of network disruptions.
- NCSC-FI received reports of denial-of-service attacks with major impacts on the targeted services.
- Reports were also filed regarding extortion messages related to the denial-of-service attacks.

Spying

- The cyber security company FireEye was targeted by a data breach perpetrated by a state actor. The attack was aimed at securing information related to customer relationships the company has with governments.
- A number of actors have carried out cyber espionage attacks against organisations developing COVID vaccines.
  - Targets included the European Medicines Agency.

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

TOP 5 Cyber Threats — Major Long-term Phenomena

1 ➡

The use of various types of cyber attacks for the purposes of extortion is becoming more common, posing a threat to the continuity of business operations. Individual attacks have caused damage worth tens of millions of euros.

2 ➡

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

3 ➡

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

4 ➡

Inadequate management of cyber risks and muddled division of responsibility in service management.
Information security suffers as a result of deficiencies in the anticipation of the impact of cyber threats and insufficiently defined roles in the context of service management.

5 ➡

Deficiencies in log data pose a risk to many organisations. The inadequate collection, monitoring and storage of log data results in an inability to detect and investigate anomalies.

increase

decrease

no change

Yellow = new/ updated content*

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre