TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

April 2020

#cyberweather gives you an update on the key information security incidents and phenomena of the month. This product is primarily intended for use by information security officers. 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

Cyber weather April 2020

Data breaches and leaks 🌧

- The number of Office 365 data breaches has risen to the same level as it was in the beginning of the year.
- O365 credentials obtained by phishing are also used for other data breaches.

Scams and phishing 🌧

- The victim’s real personal data, account details, e-mail and SMS are used in advanced scams.
- The hijacked account is used together with the password reset functionality in order to steal passwords of several services.

Malware and vulnerabilities ⛈

- During the month, there have been many critical vulnerabilities, new exploits and services susceptible to attacks.
- Do not neglect critical updates especially if the service is open to the Intenet.

Automation 🌧

- The National Cyber Security Centre Finland’s (NCSC-FI) annual report on unprotected automation equipment on Finnish data networks is under way.
- Devices that are not properly updated, such as industrial automation devices or medical devices, have been infected by known malware.

Network performance 🌧

- The number of performance incidents was higher than usual and the performance incidents had widespread effects.
- Disruption in Telia’s internet connections on 25 April affected many functions of the society.
- April was calm as far as denial-of-service attacks are concerned.

Spying 🌧

- Themes related to coronavirus, such as vaccine research and other research, may be subject to spying.
- The decision-making of states and its preparation are also traditional targets that are also topical during the pandemic period.

Top 5 cyber threats - significant longer-term phenomena

1

Vulnerabilities are exploited more rapidly, necessitating speedy updates. Devices and services whose information security has not been addressed and whose security measures and maintenance are inadequate are left connected to the network.

2

Phishing is very common, and detecting the fraud may be difficult for the phishing message recipient. This is also exploited in targeted attacks and spying.

3

Ransomware attacks with extensive impacts put business continuity at risk. The damage caused has amounted to tens of millions of euros in individual cases.

4

Unclear division of responsibilities between the service provider, subcontractors and customer undermines information security management. Shortcomings in log monitoring make detecting threats difficult.

5

Organisations are unable to manage their cyber risks. Risks are underestimated as organisations are unable to anticipate the impacts of the threats on their operations. Shortcomings in recovery plans.