TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

May 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 May 2020

Data breaches and leaks

- The number of Office 365 data breaches is currently comparable to that observed in early 2020.
- Actors in the municipal sector were targeted by a data breach and a breach attempt.
- Outside Finland, several high-performance computing environments have been targeted by data breaches.

Scams and phishing

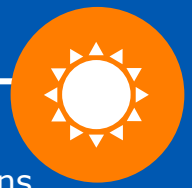
- Text message scams sent in Posti's name contain malware that infects mobile devices.
- CEO scams and other forms of billing fraud are on the increase as the summer holiday season approaches.

Malware and vulnerabilities

- Ransomware actors are auctioning stolen data with the aim of profiting from it.

Automation

- A Finnish critical infrastructure system was targeted by a ransomware attack.
- Automation systems have also faced repeated attacks in the context of conflicts among states.



Network performance

- Only three significant disruptions
- Broken optical fibre in Pasila caused widespread disruption to rail transport on 7 May.
- May saw only relatively few DoS attacks.

Spying

- A warning has been issued regarding attempts by the Sandworm group to infiltrate vulnerable Exim email servers starting from August 2019, and possibly earlier.
- Critical infrastructure systems are tempting targets for infiltration by APT groups.

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.