TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Cyber weather

March 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 March 2020

Data breaches and leaks

- The number of reported Office 365 data breaches is decreasing slightly.
- Customer loyalty systems were targeted by multiple data breaches. Finns' information was among the stolen data.

Scams and phishing

- Corona-related scams saw attempts to sell non-existent protective masks and testing kits.
- No phishing calls claiming to be from technical support were made after 24 March.

Malware and vulnerabilities

- Make sure that remote work arrangements don't pose a risk to your company network's information security.
- A substantial amount of COVID-19-related malicious content is being spread on the internet.

Automation

- The number of automation environments open to the internet is on the rise. Great care should be taken when opening remote administration connections.

Network performance

- Communications networks have withstood the additional strain caused by the move home from offices and schools.
- Some DoS attacks have had indirect effects on e.g. remote connections.

Spying

- Cyber spies are taking advantage of the coronavirus pandemic.
- Outdated systems may also attract APT groups.

Top 5 cyber threats – Major long-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.

Corona Extra

The National Cyber Security Centre has compiled a separate coronavirus-themed cyber weather report, which sheds light on the cyber security aspects of the pandemic. It is published as part of the regular cyber weather report, but will not be a permanent feature.

Corona Cyber Weather, March 2020

Data breaches and leaks

- Possible late updates expose systems to data breaches and leaks.
- The social and healthcare services sector is a target for criminals globally due to its critical role during the pandemic.

Scams and phishing

- So far, NCSC-FI has received relatively few reports of scams or phishing exploiting the corona pandemic.
- Corona-themed spam messages are being sent to both individuals and companies.

Malware and vulnerabilities

- There have been reports of ransomware in hospitals and laboratories in several countries.
- Criminals may also target other essential societal actors.

Automation

- Possible late updates and modifications may expose systems to data breaches and the spread of malware.
- In the context of automation, it is also crucial to take into account the availability of personnel for installations, updates and other necessary actions.

Network performance

- While remote work arrangements have become more common, Finland's communications networks have the necessary capacity to accommodate the increasing numbers of remote workers and online transactions.

Spying

- Actors engaged in spying are also exploiting the virus as part of their attacks.
- The World Health Organisation (WHO) has been targeted by a number of advanced cyber attack campaigns.

TOP 5 Corona Cyber Threats — Major Long-term Phenomena

1

Vulnerabilities aren't patched quickly enough in cases in which the resources available to service providers or organisations are diminished. NCSC-FI has for a long time observed criminals exploiting vulnerabilities increasingly quickly.

2

Corona-themed phishing and scam attempts are likely to become more common and diverse as the epidemic spreads in Finland. Providing personnel with adequate instructions is key when combatting this threat.

3

Ransomware attacks with wide-ranging effects are a significant threat, particularly for essential actors. Criminals are likely to assume that the virus pandemic makes organisations more likely to and capable of paying the ransom.

4

Staff shortages are possible in the coming weeks as the number of infections increases. Organisations that have not yet done so should plan to ensure the availability of competent personnel, both remotely and in person.

5

Denial of service attacks. Busy websites make easy targets for criminals. If information is not made available through official channels, people may look for it elsewhere on the internet or social media, increasing the likelihood of falling prey to scams and misinformation.

How to improve your own cyber security

1

Keep your devices updated. Computers or other devices usually remind users of available updates through desktop notifications. Don’t delay installing any suggested updates.

2

Use different passphrases for different systems. It is not advisable to use the same login details at work as you do for online shops or personal email accounts, for example.

3

Check which services and applications you are actually using. If you’re not using an application, it is advisable to delete it. Also make sure that the privacy settings of your social media accounts are set so as to suit your needs.

4

Use trusted and secure networks. If you are using wireless networks (WLAN, WiFi) while working remotely, make sure that they are password protected. Instead of unfamiliar networks, it is better to use your phone’s internet connection. Whenever possible, prefer WLAN over mobile connections so as to avoid causing mobile network congestion.

5

Make backup copies. It is advisable to transfer your data to a backup device periodically. This enables you to recover it in case your device is damaged. You won’t lose your photos if your phone is broken, for example.