Metropolitan Stock Exchange of India Limited

Circular No: MSE/IT/8991/2020 May 5, 2020

Cyber Security advisory: Precautionary measures in COVID-19 outbreak

In the wake of nationwide Lockdown to contain the Covid-19 pandemic, Government of India has requested organisations (Government/Private) to use of "work from home" facility. This has resulted in unprecedented increase of dependency on digital means and resulting in many operations that may be under remote monitoring mode.

A cyber-attack on critical sector organisations to access to their devices, data or the Internet could be devastating in present case. In a worst-case scenario, broad-based cyber-attacks could cause widespread infrastructure failures that take entire communities or cities offline, obstructing healthcare providers, public systems and networks. The most common scams and possible attacks are as follows:

Social Engineering Attacks

Phishing emails with links claiming to have important updates on Coronavirus from World Health Organisation (WHO). The links, if clicked may lead the devices being infected with malware/ransom ware.

Ransom ware Attacks

An attacker may target increase use of remote login credentials to organizational resources.
Ex: Android apps titled 'CovidLock' which claims to provide access to a map that details real-time virus tracking and information. Once installed, the app asks for various permissions which it claims are needed to be able to deliver notifications and installs ransom ware which can you the access to your phone by forcing a change in the phone's lock screen password.

Phishing Attacks

Users working with home systems for official work could fall for "free" access to obscure websites or pirated shows, opening the door to likely malware and attacks.
Ex: Covid-19/CORONA Virus themed phishing email which claims to be from Income Tax or RBI announcing 'new tax refund programme' to deal with the outbreak with malicious link. Once clicked, it requests the victim for their financial and tax information, bank details and PII.

Precautionary measures to be taken to prevent cyber-attack:

1. Ensure you are using secure Wi-Fi connection. Avoid the use of public Wi-Fi.
2. Change default password on you home Wi-Fi router to prevent hackers accessing your network.
3. In case of working in public place use a privacy screen and tether using a 3G/4G connection instead of an untrusted Wi-Fi hotspot.
4. Ensure your system antivirus is in place and fully updated.
5. Only use authorised software /trusted source to share files. Refrain from using personal email or 3rd party services unless reliably informed otherwise.
6. Do not click on links or download attachments from unknown sources.
7. Use strong passwords/passphrases to login to your personal desktops/laptops.
8. Lock your screen when not in use.

9. Use separate logins for home system for work purpose.
10. Ensure not to reuse passwords across the web.
11. Do not download apps from untrusted and unfamiliar sites.
12. Pay close attention to the permissions requested by an app and think twice before you grant access to sensitive information such as your address book or access to your photo library.
13. Remember to back up all important files regularly. Disk encryption is an option available in most operating systems. In many cases it is optional that can be enabled as and when required.
14. Don't click on COVID-19 related messages with attachments. Don't forward them to family or friends.
15. Be wary of websites that start "Coronavirus" or "Covid." E.g. do not install or click on apps like "coronavirusapp.site." which supposedly tracks virus outbreaks. Downloading such applications will infect your systems/phones with ransom ware.
16. Seek legitimate information from authentic government, university, hospital and news sites with names you know.

The Government of India National Critical Information Infrastructure Protection Centre, a unit of NTRO has issued a cyber-security advisory on precaution of CII in COVID-19 is enclosed as **Annexure A.**

Members are requested to take a note of the same.

For any clarifications, please contact InfoSec Team by sending an email to InfoSec@msei.in.

For and on behalf of
Metropolitan Stock Exchange of India Limited

Mr. Kundan Zamvar
Vice President – IT & CISO

Encl.: As above