NSE Clearing

Circular

Department: Cyber & Information Security Team	
Download Ref No: NCL/CIS/44247	Date: April 29, 2020
Circular Ref. No: 01/2020	

All Members,

Cyber Security Advisory: COVID-19 based Cyber Attacks

Novel Coronavirus, originated in December 2019 is a viral disease spread worldwide.

It has been reported that Threat Actors are using the COVID-19 pandemic as a cyber-attack vector for their own notorious gains. Cyber criminals are taking advantage of victims increased craving for information about the Novel Coronavirus due to fear and uncertainty associated with it as the outbreak of the disease is progressing worldwide.

In regards with the above and the ICT threat received from regulators, all members are hereby notified and requested to undertake appropriate actions as applicable to their environment. A brief description and immediate steps to be taken are mentioned below.

1. Attack Tactics and Procedures

a. The Threat actors employ references related to COVID-19 in phishing attacks to steal information and drop additional malware.

b. Threat actors devise following strategies to target victims with scams or malware campaigns:

i. Use of Legitimate corporate branding in the name of COVID-19 to send malware to victims.

ii. Using names of trusted organizations in phishing attacks in order to attain credibility and to lure victims to further open attachment

iii. Using promotional code

iv. Coronavirus Maps

v. "COVID19" as discount codes used by different hacking groups to promote their goods (malicious malware or exploit tools) for financial gain sold over dark net

vi. Trojan being delivered via Android app that lures victims offering Coronavirus safety mask upon installation.

vii. Coronavirus tracker App that takes away access of android microphone and camera once installed.

2. Key precautions and recommendations

a. The majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence design thoughtful security awareness campaigns that stress on the avoidance of clicking on links and attachments in email which can establish an essential pillar of defence.

b. Allow remote access to the organization's network strictly with two-factor authentication.

c. Systems should be deployed with antivirus and a malware protection program and ensure that the signatures are always up to date.

d. Apply strict application whitelisting, block unused ports, turn off unused services, and monitor outgoing traffic to prevent infections from occurring.

e. Check all services and devices for remote access for updates of firmware and security patches. Internet-facing open ports of remote-control services are a key target for attacks.

f. Disable use of Macros in Microsoft office.

g. For additional details on COVID-19 malware families and recommendations, please refer the advisory issued by CERT-In attached as Annexure A.

3. Reference Links

a. http://www.cert-in.org.in

4. Disclaimer

a. The information contained in this notice has been extracted from regulatory sources and has been published only as guidance to members. As the future course of events with regards to this threat are not known, members are advised to keep a close watch on their systems to identify timely detection and remediation of this threat.

b. Members shall act upon this notice at their own discretion after conducting appropriate impact/risk analysis to their specific environment.

c. Please note that the other exploit kits are also widely in circulation and available for download for free on the Internet and there are possibilities of attack vectors other than this threat which may exist/emanate. It is critical to perform a self-assessment against these zero-days/ exploit kits released in the wild in a controlled environment.

d. This notice is for informational purpose only.

For and on behalf of

Chief Information Security Officer

NSE Clearing Limited

Toll Free No	Telephone No	Email ID
1800–266–0053	+91–22–26598100| Extn:24043	soc_im@nse.co.in