NATIONAL COMMODITY & DERIVATIVES EXCHANGE LIMITED

Circular to all members of the Exchange
Circular No. : NCDEX/RISK- 001/2020
Date : April 15, 2020
Subject : Cyber Security Advisory Covid-19 Pandemic

There has been an increase in the number of cyberattacks on personal computer networks and routers since professionals were asked to work from home in the wake of the COVID-19 outbreak. Many organizations are being encouraged by their management to work from home to help stop the spread of coronavirus. However, switching to remote working could create cyber security problems.

Cyber criminals are exploiting the Covid-19 outbreak as an opportunity to send phishing emails claiming to have important updates or encouraging donations, and they at times impersonate trustworthy organizations to do this.

With most employees working from home, enterprise VPN servers have now become increasingly vulnerable and their security and availability must be the focus for IT teams. It is therefore very important that the VPN service is patched and updated regularly.

We take this opportunity to advise market participants that in view of the present circumstances (Covid-19 and Lockdown) wherein most people are working from home, to keep themselves aware of various advisories (particularly cyber security related) as and when issued by CERT and NCIIPC.

Please Note: CERT (Computer Emergency Response Team)

NCIIPC (National Critical Information Infrastructure Protection Centre)

For your ready reference, we have compiled in the attached advisory the guidelines issued by CERT-IN on their website, for your information and necessary action.

Source - **https://www.cert-in.org.in/**

1.0 CERT-In Advisory CORONAVIRUS PANDEMIC [COVID-19] BASED CYBER ATTACKS

Original Issue Date: March 23, 2020

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 cyberattack 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.

Attack stages - Primary set of attacks:

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

Tactics and attack procedures involved post initial phase of attacks:

Threat actors devise following new strategies to target victims with scams or Malware

- Use of legitimate corporate branding in the name of COVID-19 to send malware to victims
- Using names of trusted organizations in phishing attacks in order to attain credibility and to lure victims to further open attachment
- Using promotional code Coronavirus Maps
- "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
- Trojan being delivered via Android app that lures victims offering Coronavirus safety mask upon installation. Coronavirus tracker App that takes away access of android microphone and camera once installed.

Malware families related to covid-19:

- AGENT TESLA
- TRICKBOT
- LOKIBOTEMOTET
- TRICKYMOUSE
- VICIOUS PANDA
- CAMPAIGN AZORULT
- CRIMSON RAT
- COVIDLOCK

Best Practice and Recommendations

1. The majority of the infections are primarily introduced via phishing emails, malicious adverts on websites, and third-party apps and programs. Hence, thoughtfully designed security awareness campaigns that stress the avoidance of clicking on links and attachments in email, can establish an essential pillar of defense.
2. Allow remote access to the organization's network strictly with two-factor authentication.
3. Systems having antivirus and a malware protection program on it and making sure they are always up to date with latest signatures.
4. Administrators applying strict application whitelisting, blocking unused ports, turning off unused services, and monitoring outgoing traffic to prevent infections from occurring.
5. Checking 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.
6. Disable use of Macros in Microsoft office. COVID-19 used VBA Macros as an initial step for targeting victims.

2.0 CERT-In Advisory CIAD-2020-0008

Cyber security during covid-19 outbreak

Issue Date: March 26, 2020
Updated: March 30, 2020

Description

Many organizations are being encouraged its staff to work from home to help stop the spread of corona virus. Switching to remote working because of the covid-19 can create cyber security problems for employers and employees. There is an increase in the number of cyber attacks on computers, routers and unprotected home networks used by employees who have switched to remote working due to the spread of covid-19.

Cyber criminals are exploiting the covid-19 outbreak as an opportunity to send phishing emails claiming to have important updates or encouraging donations, impersonating trustworthy organizations.

With most employees working from home, enterprise VPN servers have now become paramount to a company's backbone, and their security and availability must be the focus going forward for IT teams. It is important that the VPN service is patched and up-to-date because there will be way more scrutiny against these services.

Security best practices

- Change default passwords on your home Wi-Fi router to prevent hackers accessing your network
- Use strong and unique passwords on every account and device - consider using two-factor authentication (2FA).
- Update VPNs, network infrastructure devices, and devices being used to remote into work environments with the latest software patches and security configurations.
- Only use software your company would typically use to share files. Refrain from using your personal email or 3rd party services unless reliably informed otherwise.
- Avoid accessing the corporate network through third-party services that use intermediate servers and take over the responsibility for authorization and authentication issues.
- Network segmentation and access right differentiation are both required. It is recommended that even remote user activity is covered by the organization's perimeter security tools.
- Check the availability and duration of logging remote user actions. Ensure that remote sessions automatically time out after a specified period of inactivity and that they require re-authentication to gain access.
- Remind employees of the types of information that they need to safeguard. This often includes information such as confidential business information, trade secrets, protected intellectual property and other personal information.
- Do not allow sharing of work computers and other devices. When employees bring work devices home, those devices should not be shared with or used by anyone else in the home. This reduces the risk of unauthorized or inadvertent access to protected company information.
- "Remember password" functions should always be turned off when employees are logging into company information systems and applications from their personal devices.

- Consider Mobile Device Management (MDM) and Mobile Application Management (MAM). These tools can allow organizations to remotely implement a number of security measures, including data encryption, malware scans, and wiping data on stolen devices.

References

Practical steps to work from home securely
https://workfromhome.globalcyberalliance.org

Work from home - Best practices
https://www.dsci.in/sites/default/files/DSCI-WorkfromHomeAdvisory-1.pdf

3.0 Source - CERT-In Advisory CIAD-2020-0010

Secure usage of Zoom video conferencing application

Issue Date: March 30, 2020

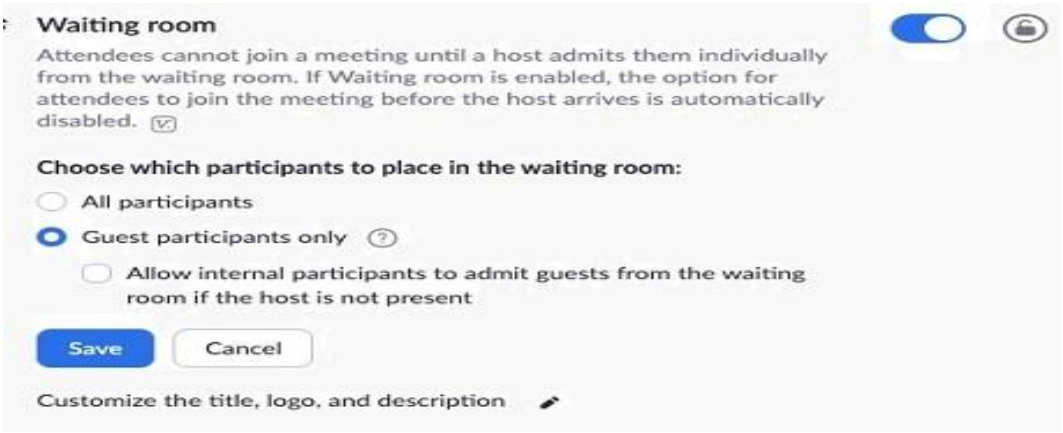
Description

Many organizations have allowed its staff to work from home to stop the spread of Coronavirus disease (COVID-19). Online communication platforms such as Zoom, Microsoft Teams and Teams for Education, Slack, and Cisco WebEx etc. are being used for remote meetings and webinars.

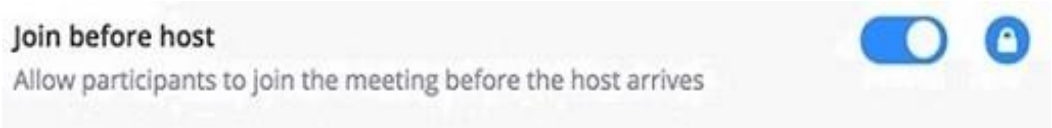
Zoom is a popular video conferencing platform. Insecure usage of the platform may allow cyber criminals to access sensitive information such as meeting details and conversations. Following measures are advised for increasing the security of Zoom meetings and reducing risks-

- Keep your Zoom software patched and up-to-date.
- Always set strong, difficult-to-guess and unique passwords (make your password at least eight characters long and use at least three of the following types of characters: lowercase letters, uppercase letters, numbers, symbols) for all meetings and webinars. This is especially recommended for any meetings where sensitive information may be discussed.

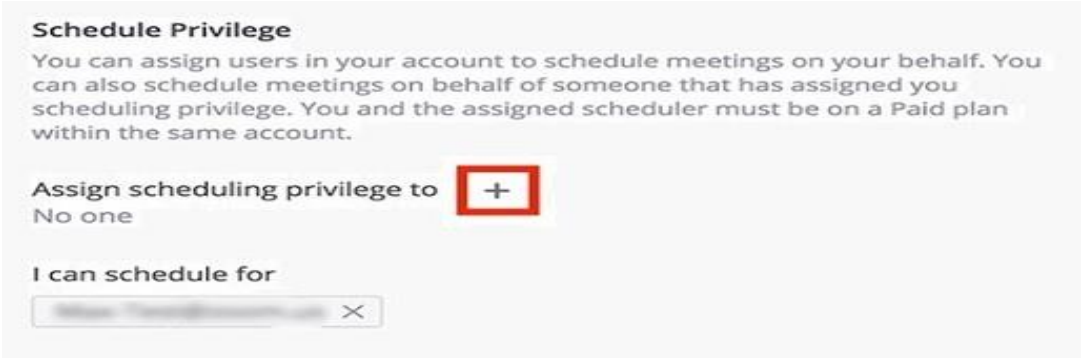
- Enable "Waiting Room" Feature so that the call manager will have a better control over participants. All participants can join a virtual "Waiting Room", but they will be approved by call manager to be part of the actual meeting.



Disable Join Before Host Feature: The "Join Before Host" option lets others to continue with a meeting in the absence of an actual host, but with this option enabled, the first person who joins the meeting will automatically be made the host and will have full control over the meeting. Alternatively, "Scheduling Privilege" may be given to a trusted participant to host the meeting



In the absence of an actual host.



- If not required, restrict/disable file transfers.
- From settings and controls, ensure removed participants are unable to re-join meetings. If not required, limit Screen Sharing to the Host only.
- Lock the meeting session once all your attendees have joined.
- Restrict the call record feature "Allow Record" to trusted participants only.

References

- ✓ https://blog.checkpoint.com/2020/03/26/whos-zooming-who-guidelines-on-how-to-use-zoom-safely/
- ✓ https://it.cornell.edu/zoom/keep-zoom-meetings-private
- ✓ https://www.foxbusiness.com/technology/securely-host-zoom-meeting
- ✓ https://www.forbes.com/sites/zakdoffman/2020/01/28/new-zoom-roulette- security-warning-your-video-calls-at-risk- from-hackers-heres-what-you-do/#591e905d734

For and on behalf of
National Commodity & Derivatives Exchange Limited

Umesh Gurav
Vice President - Enterprise Risk and Governance

For further information / clarifications, please contact

1. Customer Service Group on toll free number: 1800 26 62339
2. Customer Service Group by e-mail to : askus@ncdex.com