Cyber Crime Information – **149**

Feb 02nd, 2022

Subject: Malicious Executable Files distributed during Video Conferences (VCs)

Threat Summary

The Covid-19 pandemic created a massive surge in the use of video conferencing platforms (for video telephony and online chats), which has raised understandable concerns about risk and security. Cybercriminals are targeting such platforms where virtual meetings are held by government organizations, educational institutions and businesses, etc.

Fig. 01 – Video Conferencing Platforms

Cybercriminals continuously developing techniques for covert attendance in video conferences to perpetrate further cyber crimes as the need for such platforms to interface with browsers also creates opportunities for inadvertent vulnerabilities that hackers can exploit.

Modus Operandi

- Cybercriminals gain access of virtual meetings/classes by compromising the email addresses belonging to the target organization(s) / participants.
- Once inside a meeting, cybercriminals drop malicious executable file(s) disguised as a related important document to trick users into opening/running it, which generally implement some malware program, trojan, etc.
- After installation, the executable file initiates malicious activities in the system and infects victims' devices with various malware, allowing cybercriminals to remotely access victim's system.
- Espionage efforts aimed at government organizations and businesses also take place by accessing the shared data in the meetings or record the whole meetings.

Suggestions

- Scrutinize the source of the file(s) posted during virtual meeting or classes before downloading.
- Multi-factor authentication feature (such as password based entry) may be included to verify that only authorized members participate in a meeting. Hosts may also keep track of who is joining the meeting.
- Ensure that video conferencing platform uses encryption, follows industry best practices for patching & updating, and uses a reputable cloud service provider.
- Organizations may implement protection that downloads all files in a sandbox and inspects them for malicious content.
- Avoid clicking on the links shared during virtual meetings/classes without confirming the source(s) as it might be a phishing links.
- Avoid opening e-mails or messages sent from unknown senders. Do not click on any link sent on such mails.
- Government officials may utilize video conferencing tools developed by CDAC, CDOT and NIC. For sharing documents CDAC's Samvad and NIC's Sandes app may be used.
- Avoid sharing meeting details on public platforms (social media, group emails, etc.).
- Utilize waiting rooms or lobbies feature where participants can wait before they're allowed to join the meeting.
- Report any such incidents on the ***cybercrime.gov.in*** portal and follow ***@CyberDost*** on Twitter to know more about safety tips.

Regards,

Indian Cyber Crime Coordination Centre
CIS Division, MHA
011-23438207