Zoom

Cyber Risks & Best Practices

Zoom, a remote conferencing service, has seen a significant increase with organizations shifting to remote work environments as a result of COVID-19. The surge in usage has gained the attention of cyber actors, who attempt to exploit vulnerabilities and take advantage of inadvertent missteps. Below are common issues that have increased with the rise of Zoom usage, as well as tips to ensure protection and security.

Cyber Threats & Risks

- **Automated Zoom Conference Finder:** a tool that can discover up to 100 public meetings per hour, allowing uninvited people to join the meeting
- **Zoombombing:** an uninvited person who joins the Zoom meeting and posts offensive imagery or plays sounds and video for the purpose of disruption
- **Malicious Zoom Domains:** a drastic increase in phishing domains pretending to be legitimate Zoom meeting links, but instead install malware or steal user credentials
- **End-to-end Encryption Issues:** this feature is available, but relies on adhering to specific parameters, and how Zoom generates and stores encryption keys is concerning
- **Leaked Credentials for Webinar Users on Windows:** Zoom converts Windows file paths, i.e. where a file is stored on a computer, to clickable links, which leaks user names and hashed passwords
- **Unauthorized Access for Webinar Users on Mac OS:** microphone and webcam access can be controlled by an unauthorized party, or used to eavesdrop, through malicious code injection
- **Recorded Videos on the Cloud:** videos can be accessed and downloaded through unsecured links or found on the Cloud even after being deleted

Steps to Mitigate Cyber Risk

- Only invite attendee(s) that are supposed to be in the meeting
- Discourage sharing meeting links on public-facing platforms
- Auto generate the meeting ID. DO NOT use the personal meeting room ID
- Disable *Embed Password in Meeting Link for One-click Join* under Account Settings
- Require a complex password to join, and share it with invitees separately from the meeting invite
- Enable the *Waiting Room* feature, which allows hosts to see participants in a virtual staging area
- Disable the *Allow Removed Participants to Rejoin* function
- Lock your meeting once all participants have joined
- Restrict screen sharing by making screen share capabilities administrator/host only
- Do not discuss or share anything that is highly sensitive
- Do not post photos of your Zoom meetings
- Be cautious of Zoom phishing email scams. Threat actors are spoofing emails from Zoom and Zoom meeting links
- Continuously update Zoom for newly released security features

ANTHONY J. FERRANTE
Global Head of Cybersecurity
Senior Managing Director
+1 202 312 9165
ajf@fticonsulting.com

JORDAN RAE KELLY
Head of Cybersecurity, Americas
Senior Managing Director
+1 202 312 9140
jordan.kelly@fticonsulting.com

KYUNG KIM
Head of Cybersecurity, APAC
Senior Managing Director
+82 2 2190 3727
kyung.kim@fticonsulting.com

JOSHUA BURCH
Head of Cybersecurity, EMEA
Senior Managing Director
+44 20 3727 1854
joshua.burch@fticonsulting.com

FTI Consulting is an independent global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities.©2020 FTI Consulting, Inc. All rights reserved. **www.fticonsulting.com**

FTI CONSULTING | CYBERSECURITY