WHAT IS ZOOMBOMING?

The novel COVID-19 virus has spawned a wave of cyberattacks, including new tactics that are targeting businesses and individuals and are posing new security challenges. One, “Zoombombing,” involves hackers hijacking sessions on Zoom, a popular video conferencing service, to display offensive content, direct participants to harmful sites, or share malicious files.[1] As many schools and businesses transition to working from home, Zoom and other video conferencing applications have become critical in allowing classes and meetings to be conducted remotely, and thus have become an attractive target for hackers.

WHAT ARE THE RISKS?

The Zoombombing trend started when companies began reporting that their Zoom conferences had been interrupted by uninvited participants joining the meeting and displaying offensive content, like pornography or racial slurs. On March 17th, Chipotle was forced to end a public Zoom meeting after a participant began broadcasting pornography to hundreds of attendees[2] and New York City schools recently banned Zoom from their online classrooms after several Zoombombing incidents.[3] What began as a few internet trolls looking to harass meeting goers has now become a coordinated and organized effort. Attackers are gathering in the tens of thousands on chatrooms like Discord, message boards like 4Chan and Reddit, and even social media sites like Twitter and Instagram to share Zoombombing raid plans and Zoom meeting codes.[4]

Easy-to-guess file naming conventions make it easy to search the internet for recorded meetings, meeting transcripts export private messages between participants, and the iOS version of the app shares data with Facebook even if the user does not have a Facebook account.   These concerns can be mitigated however by restricting access to recorded meetings to only trusted viewers and reviewing mobile app permissions and privacy settings to make sure data is not shared with third parties.

Successful Zoombombing attacks can have several consequences. If the attacker shares offensive content, this can be damaging to a business’s reputation and credibility or can be counterproductive if the host is forced to end the meeting as a result. If the attacker goes unnoticed by the host or other participants, they may listen in on the conversation to steal sensitive company information or export this information from the meeting chat. The attacker may use the meeting chat feature to share malicious links to phishing and spam sites or use the file transfer feature to spread malware and infect unknowing participants.

[1] *https://techcrunch.com/2020/03/17/zoombombing/*
[2] *https://www.nytimes.com/2020/03/20/style/zoombombing-zoom-trolling.html*
[3] *https://thenextweb.com/security/2020/04/06/nyc-classrooms-cancel-zoom-after-trolls-make-zoombombing-a-thing/*
[4] *https://www.nytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html*
[5] *https://www.nytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html*

In addition to the security risks posed by Zoombombing, there are several privacy concerns aired in the press, associated with the application itself. For example, the press states that Zoom's original claim that it offers "end-to-end" encryption is misleading. Although Zoom calls are secured with encryption, the encryption it uses is actually TLS or transport encryption, the same encryption technique used to secure connections to HTTPS websites. This is different from end-to-encryption because it means that Zoom has access to the video and audio content from meetings.[6] A representative from Zoom has stated, "Currently, it is not possible to enable E2E encryption for Zoom video meetings. Zoom video meetings use a combination of TCP and UDP. TCP connections are made using TLS and UDP connections are encrypted with AES using a key negotiated over a TLS connection."

Additionally, participants must call in using computer audio rather than calling in with a phone to take advantage of the encryption. Zoom has since changed the language on the security page of their website to more accurately reflect their encryption practices. The company has also stated in its privacy policy that it does not monitor or access meeting recordings and transcripts, nor does it sell user data to third parties or use it for advertising.[7]

HOW DO I PROTECT MYSELF?

You can make your meetings safer by following some simple steps:

- Generate a random meeting ID that is specific to each meeting and don't use your personal meeting ID for meetings
- Disable the "Join before host" setting so that attackers can't join the meeting before you can stop them
- Disable screen sharing and file transfer so that attackers can't display offensive content or share malware
- Enable the "Waiting Room" feature so that you can vet participants as they come in before allowing access
- Once all meeting participants have joined, lock the meeting so that no one else can come in
- If an uninvited guest joins the meeting, lock them out and disable the "Allow Removed Participants to Rejoin" setting so they can't come back in
- Designate and assign "Co-Hosts" that can help manage participants and monitor for suspicious activity
- Enable the "Require Encryption for 3rd Party Endpoints" setting to secure the meeting for all participants

Zoom has also addressed security concerns in its latest release of the software, which came out on April 7th. This version enforces the use of passwords on all meetings, does not display the meeting ID in the page's toolbar (which used to be visible if someone posted a screenshot of their meeting), and includes a security icon that allows users to access all security settings in one place.[8] Please ensure you are using the latest version of the software to take advantage of the new security features.

CONCLUSION:

As the COVID-19 crisis continues, we expect to see cyber threat actors taking advantage of the situation with new campaigns and techniques to exploit vulnerable systems. While we all adjust to the new normal, it is important to be aware of the cybersecurity risks and apply the necessary measures to protect against these kinds of attacks. Global Guardian is a managed security service that can help protect home and business computer systems from cyberattacks. If you have been the victim of a Zoombombing attack or are looking for solutions to better secure your remote workforce, please contact Global Guardian today.

[6] *https://theintercept.com/2020/03/31/zoom-meeting-encryption/*
[7] *https://zoom.us/privacy*
[8] *https://www.ibtimes.com/zoom-announces-new-security-changes-response-hacks-zoom-bombing-incidents-2955269*