So What's All This About Zoom?

Anton Janik, Jr.
ajanik@mwlaw.com
(501) 688.8888

04/10/2020

For the time being, many Americans are at home due to the COVID-19 virus, but they are continuing to work, learning to homeschool and socializing with friends thanks to virtual platforms. Although there are a variety of applications and platforms, Zoom has landed on top and is quickly becoming a household name. However, as principally a video meeting platform for large-scale enterprises, educational institutions and government bodies that already had their own IT departments, Zoom was not built for the purpose of being an open social platform, leaving the company ill-prepared to moderate user behavior on its platform.[1]

Last week, reports began surfacing that various state Attorneys General, including New York, Connecticut and Florida, were investigating Zoom's security practices after "Zoombombing" incidents occurred in public meetings on the company's platform. During these incidents, hackers crash into a public meeting and share graphic content to the meeting users. These incidents have escalated enough to prompt the Federal Bureau of Investigation to issue a warning that hijackers may face fines and even jail time.

So how can users protect themselves against these types of invasions?

Use the most recent version of the remote access/meeting application: In January, Zoom updated the security to their software where passwords were added as a default setting. The ability to randomly scan for meetings to join was also disabled.

Manage meeting invitations: When setting a meeting[2], only provide the meeting link to specific attendees via a direct channel, such as email. Do not share links in social media posts and comments. If you are hosting a public meeting, use a randomly generated meeting specific ID[3] rather than using yourpersonal meeting ID[4] that is associated with your account. (In fact, because your personal meeting room is your permanently reserved meeting room which is accessed by your personal meeting ID, best practices would have you to never share your personal meeting ID, since that is a direct access link to any meeting you are hosting. Thus, an invite sent out with your personal meeting ID this week could potentially also be used by the recipient to drop in on any other meeting you host at any other time. Recently, images have popped up on Twitter showing British Prime Minister Boris Johnson in a private cabinet meeting conducted on Zoom, with the meeting ID prominently displayed.[5])

Make meetings private: Access to private meetings can be provided either by requiring a password[6] or by utilizing the waiting room feature[7] to manually control the admittance of guests.

Manage screen sharing: Restrict screen sharing[8] to prevent uninvited attendees from taking control of your screen.

Manage participants: Zoom identifies multiple ways a host can restrict attendees in a meeting, such as setting up additional two factor authentication[9], removing unwanted participants[10], holding attendees audio and visual capabilities and disabling private chat, among others[11].

In addition to providing, extensive online trainings and tutorials, Zoom has also offered webinar trainings[12] and free and interactive live training webinars on a daily basis[13]. CEO Eric S. Yuan also hosts a webinar each Wednesday at 12 PM CST to "Ask Eric Anything" in a live format. Questions are submitted via email prior to the meeting.

Zoom published a blog entitled "How to Keep Out Uninvited Guests" on March 20, ten days prior to the FBI-issued warning about teleconference hijacking[14]. However, blog posts are not an appropriate response to AG investigations[15], shareholder class action suits[16], government bans of the application[17] and user privacy concerns regarding the issues within Zoom's security infrastructure.

But what exactly are these issues and what is Zoom doing about them?

Inadequate encryption: Zoom investor Michael Drieu filed a class action suit in San Francisco federal court on April 6, claiming the company concealed issues in the application's software encryption. Zoom claimed to offer "end-to-end" encrypted meetings, meaning that only the attendees can access the meetings. Additionally, as reported by Citizen Lab on April 3, Zoom has claimed the application uses "AES-256" encryption where possible, but Citizen Lab discovered in its investigation that in each Zoom meeting, a single "AES-128" key was used to encrypt audio and video. Citizen Lab also verified that this key was sufficient to decrypt Zoom packets intercepted in Internet Traffic[18] and appear to be generated by Zoom servers.

Zoom's Response: Zoom published a blog post on April 1, clarifying the facts around its encryption measures.[19] Refreshingly, before any explanation came the following apology: "In light of recent interest in our encryption practices, we want to start by apologizing for the confusion we have caused by incorrectly suggesting that Zoom meetings were capable of using end-to-end encryption." In this blog, Zoom also expressly stated "[it] has never built a mechanism to decrypt live meetings for lawful intercept purposes, nor do we have means to insert our employees or others into meetings without being reflected in the participant list." Zoom responded that enterprise customers have the option to run certain versions of connectors within the customer's own data center to directly manage decryption and translation process. Zoom further hinted that a solution for additional control of keys would be available later this year.

Routing Information Through Servers Outside the U.S.: Speaking of encryption and Zoom's servers, tests run by the University of Toronto's Citizen Lab for a call between users in the United States and Canada showed that the key to encrypt and decrypt that call was routed through a Zoom server located in Beijing–even though all meeting users were located outside of China.[20]

Zoom Response: In its urgency to add server capacity as usage exploded over the last few weeks, it had added two servers in China to a whitelist of permitted call-routing servers. However, when it brought those servers online, Zoom "failed to fully implement our usual geo-fencing best practices."[21] (Generally, a geo-fence is used to prevent data from one geographical area, like the United States, from crossing over into another geographical area, like China. Such data is ordinarily geo-fenced because different countries have different approaches to data privacy.) Zoom admitted that by whitelisting those two servers in China, they "potentially enable[d] non-Chinese clients to — under extremely limited circumstances — connect to them (namely when the primary non-Chinese servers were unavailable)."[22] Zoom further admitted that, as Citizen Lab reported, "it is possible certain meetings were allowed to connect to systems in China, where they should not have been able to connect." Zoom reported that they have now corrected this issue.

Citizen Lab also reported that Zoom owns three companies in China and employs 700 persons there.[23] Several sources point out that China's cybersecurity laws require that encryption keys be turned over to the Chinese government, which may allow China the ability to access to that content at will.[24]

Unauthorized disclosure of personal information to Facebook: On March 30,a class action lawsuit was filed in the Northern District of California for providing users' personal data to third parties, including

Facebook, without prior disclosures. Zoom's iOS application gave Facebook the user's customer and device information, including IP addresses and the device's unique advertising identifier, regardless of whether the Zoom user had a Facebook account. These identifiers are used to target users for advertising purposes. The law suit also alleges that Zoom was paid for sharing user data.[25]

Zoom's Response: Zoom acknowledged its data sharing practices and removed the feature after being made aware on March 25 that the Facebook SDK was collecting device information unnecessary for the provision of Zoom's services.[26] "On March 27th, we took action to remove the Facebook SDK in our iOS client and have reconfigured it to prevent it from collecting unnecessary device information from our users."[27] This change requires users to update to the latest version of the application.

Zoom has communicated its "commitment to ensuring that the safety, privacy, and security of [its] platform is worthy of the trust of all [its] users…"[28] So, what else can we expect from Zoom?[29]

- Launch of a Chief Information Security Officer and Advisory Board to share ideas and collaborate on privacy, security and technology issues and best practices from industry leaders
- A comprehensive security review of the Zoom platform lead by outside advisor, Alex Stamos, the former Chief Security Officer of Facebook
- A shift in engineering resources to focus on safety and privacy issues rather than feature development
- A transparency report detailing requests for data, records and content
- An enhancement of Zoom's current bug bounty program

While Zoom is conducting corrective action to ensure the safety, privacy and security of its platform, the FBI recommends exercising due diligence and caution in your cybersecurity efforts. If you were or become a victim of a teleconferencing hijacking, or any cybercrime, report it to the FBI's Internet Crime Complaint Center.

---

[1] "[W]e did not design the product with the foresight that, in a matter of weeks, every person in the world would suddenly be working, studying, and socializing from home. We now have a much broader set of users who are utilizing our product in a myriad of unexpected ways, presenting us with challenges we did not anticipate when the platform was conceived." https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/

[2] https://support.zoom.us/hc/en-us/articles/201362183-How-do-I-invite-others-to-join-a-meeting-

[3] https://www.youtube.com/watch?v=XhZW3iyXV9U&feature=youtu.be&t=27

[4] https://support.zoom.us/hc/en-us/articles/203276937-Using-Personal-Meeting-ID-PMI-?zcid=1231

[5] https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/ and https://twitter.com/AmichaiStein1/status/1244998914773827586

[6] https://support.zoom.us/hc/en-us/articles/201362603-Host-and-Co-Host-Controls-in-a-Meeting?zcid=1231

[7] https://blog.zoom.us/wordpress/2020/02/14/secure-your-meetings-zoom-waiting-rooms/?zcid=1231

https://www.youtube.com/watch?reload=9&v=ntaT7KEcids&feature=youtu.be

[8] https://support.zoom.us/hc/en-us/articles/201362153-How-Do-I-Share-My-Screen-

[9] https://support.zoom.us/hc/en-us/articles/360033559832-Meeting-and-Webinar-Passwords-?zcid=1231

[10] https://support.zoom.us/hc/en-us/articles/115005759423-Managing-participants-in-a-meeting?zcid=1231

[11] https://support.zoom.us/hc/en-us/articles/115005759423?zcid=1231

[12] https://blog.zoom.us/wordpress/2020/03/11/free-zoom-training-customer-training-success/

[13] https://support.zoom.us/hc/en-us/articles/360029527911-Live-Training-Webinars?zcid=1231

[14] https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

[15] https://www.cnbc.com/2020/04/03/zoom-probed-by-three-states-for-potential-privacy-violations.html

[16] https://www.bloomberg.com/news/articles/2020-04-08/zoom-sued-for-securities-fraud-over-privacy-security-flaws

[17] https://www.bbc.com/news/technology-52200507

[18] https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/

[19] https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/

[20]https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/

[21] https://blog.zoom.us/wordpress/2020/04/03/response-to-research-from-university-of-torontos-citizen-lab/

[22] https://blog.zoom.us/wordpress/2020/04/03/response-to-research-from-university-of-torontos-citizen-lab/

[23] https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/

[24] https://www.chinalawblog.com/2019/11/chinas-new-cryptography-law-still-no-place-to-hide.html

[25] https://www.cbsnews.com/news/zoom-app-personal-data-selling-facebook-lawsuit-alleges/

[26] https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/

[27] https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/

[28] https://blog.zoom.us/wordpress/2020/04/08/update-on-zoom-90-day-plan-to-bolster-key-privacy-and-security-initiatives/

[29] https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/