Keep Zoombombing cybercriminals from dropping a load on your meetings

Posted: April 14, 2020 by Philip Christian
Last updated: April 13, 2020

While shelter in place has left many companies struggling to stay in business during the COVID-19 epidemic, one company in particular has seen its fortunes rise dramatically. Zoom, the US-based maker of teleconferencing software, has become the web conference tool of choice for employees working from home (WFH), friends coming together for virtual happy hour, and families trying to stay connected. Since March 15, Zoom has occupied the top spot on Apple's App Store. Only one week prior, Zoom was the 103rd-most popular app.

Even late-night talk show hosts have jumped on the Zoom bandwagon, with Samantha Bee, Stephen Colbert, Jimmy Fallon, and Jimmy Kimmel using a combination of Zoom and cellphone video to produce their respective shows from home.

What is Zoombombing?

Since the call for widespread sheltering in place, a number of security exploits have been discovered within the Zoom technology. Most notably, a technique called Zoombombing has risen in popularity, whether for pure mischief or more criminal purpose.

Zoombombing, also known as Zoom squatting, occurs when an unauthorized user joins a Zoom conference, either by guessing the Zoom meeting ID number, reusing a Zoom meeting ID from a previous meeting, or using a Zoom ID received from someone else. In the latter case, the Zoom meeting ID may have been shared with the Zoombomber by someone who was actually invited to the meeting or circulated among Zoombombers online.

The relative ease by which Zoombombing can happen has led to a number of embarrassing and offensive episodes.

In one incident, a pornographic video appeared during a Zoom meeting hosted by a Kentucky college. During online instruction at a high school in San Diego, a racist word was typed into the classroom chat window while another bomber held up a sign that said the teacher “Hates Black People.” And in another incident, a Zoombomber drew male genitalia on screen while a doctoral candidate defended his dissertation.

Serious Zoombombing shenanigans

The Zoombombing problem has gotten so bad that the US Federal Bureau of Investigations has issued a warning.

That said, it’s the Zoombombs that no one notices that are most worrying, especially for Zoom’s business customers. Zoombombers can discreetly enter a Zoom conference and capture screenshots of confidential screenshares and record video and audio from the meeting. While it’s not likely for a Zoom participant to put up a slide with their username and password, the information gleaned from a Zoom meeting can be used in a phishing or spear phishing attack.

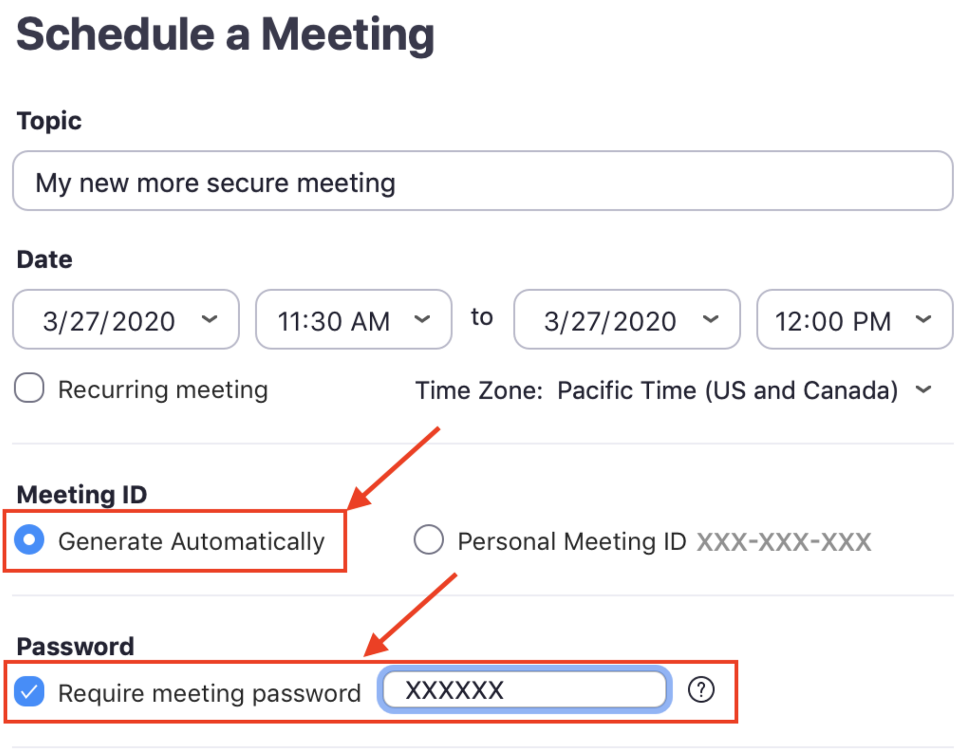
As of right now, there hasn’t been a publicly disclosed data breach as a result of a Zoombomb, but the notion isn’t far-fetched.

Numerous organizations and educational institutions have announced they will no remote learning. And Elon Musk's SpaceX has banned Zoom, noting "significant privacy and security concerns" in a company-wide memo.

"Most Zoombombing incidents can be prevented with a little due diligence on the part of the user," Malwarebytes Head of Security John Donovan said. "Anyone using Zoom, or any web conference software for that matter, is strongly encouraged to review their conference settings and minimize the permissions allowed for their conference attendees."

"You can't walk into a high school history class and start heckling the teacher. Unfortunately, the software lets people do that if you're not careful," he added.

For their part, Zoom has published multiple blog posts acknowledging the security issues with their software, changes the company has made to shore up security, and tips for keeping conferences private.



Schedule a Meeting

Topic

My new more secure meeting

Date

3/27/2020 11:30 AM to 3/27/2020 12:00 PM

□ Recurring meeting

Time Zone: Pacific Time (US and Canada)

Meeting ID

● Generate Automatically ○ Personal Meeting ID XXX-XXX-XXX

Password

☑ Require meeting password XXXXXX

Set your meeting ID to generate automatically and always require a password.

Keep your Zoom meetings secure

1. **Generate a unique meeting ID.** Using your personal ID for meetings is like having an open-door policy—anyone can pop in at any time. Granted, it's convenient and easy to remember. However, if a Zoombomber successfully guesses your personal ID, they can drop in on your meetings whenever they want or even share your meeting ID with others.

2. **Set a password for each meeting.** Even if you have a unique meeting ID, an invited participant can still share your meeting ID with someone outside your organization. Adding a password to your meeting is one more layer of security you can add to keep interlopers out.

3. **Allow signed-in users only.** With this option, it won't matter if Zoombombers have the meeting ID—even the password. This setting requires everyone to be signed in to Zoom using the email they were invited through.

4. **Use the waiting room.** With the waiting room, the meeting doesn't start until the host arrives and adds everyone to the meeting. Attendees in the waiting room can't communicate with each other while they're in the waiting room. This gives you one additional layer of manual verification, before anyone can join your meeting.

5. **Enable the chime when users join or leave the meeting.** Besides giving you a reason to embarrass late arrivals, the chime ensures no one can join your meeting undetected. The chime is usually on by default, so you may want to check to make sure you haven't turned it off in your settings.

6. **Lock the room once the meeting has begun.** Once all expected attendees have joined, lock the meeting. It seems simple, but it's another easy way to keep Zoombombing at bay.

7. **Limit screen sharing.** Before the meeting starts, you can restrict who can share their screen to just the host. And during the meeting, you can change this setting on the fly, in case a participant ends up needing to show something.

A special note for IT administrators: As a matter of company policy, many of these Zoom settings can be set to default. You can even further lock down settings for a particular group of users with access to sensitive information (or those with a higher learning curve on cybersecurity hygiene). For more detailed information, see the Zoom Help Center.

exists.

No matter which web conferencing software you use, take a moment to learn its settings and make smart choices about the data you share in your meetings. Do this, and you'll have a safe and happy socially-distanced gathering each time you sign on.

SHARE THIS ARTICLE

COMMENTS

Ghostery hat Kommentare blockiert, die durch Disqus erstellt werden.

RELATED ARTICLES

A week in security (April 13 – 19)

April 20, 2020 - A roundup of the previous week's security news, including phishing scams, coronavirus scams, Apple scams, and more.

CONTINUE READING

No Comments

Mass surveillance alone will not save us from coronavirus

April 15, 2020 - As governments roll out enormous data collection programs to limit coronavirus, we should remember that mass surveillance alone will not save us.

Lock and Code S1Ep4: coronavirus and responding to computer viruses with Akshay Bhargava

April 13, 2020 - We cover the week's security headlines plus talk with Malwarebytes CPO Akshay Bhargava about the similarities in responding to computer viruses vs. real-life pandemics in episode 4 of Lock and Code.

CONTINUE READING

No Comments

Online credit card skimming increased by 26 percent in March

April 8, 2020 - With confinement measures imposed in many countries, online shopping has soared and with it, credit card skimming, which increased by 26 percent in March.

CONTINUE READING

No Comments

Coronavirus Bitcoin scam promises “millions” working from home

March 26, 2020 - We look at a set of Coronavirus Bitcoin scam emails promising vast sums of cryptocash that can be made working from home—but drains users accounts instead.

CONTINUE READING

No Comments

ABOUT THE AUTHOR

Philip Christian

Cybersecurity writer at Malwarebytes. Types his missives on a manual typewriter.

Contributors

Threat Center

Glossary

Scams

Write for Labs

Malwarebytes LABS

HEADQUARTERS

Malwarebytes

3979 Freedom Circle, 12th Floor

Santa Clara, CA 95054

FOLLOW US

EULA Privacy Accessibility Terms of Service

Language English