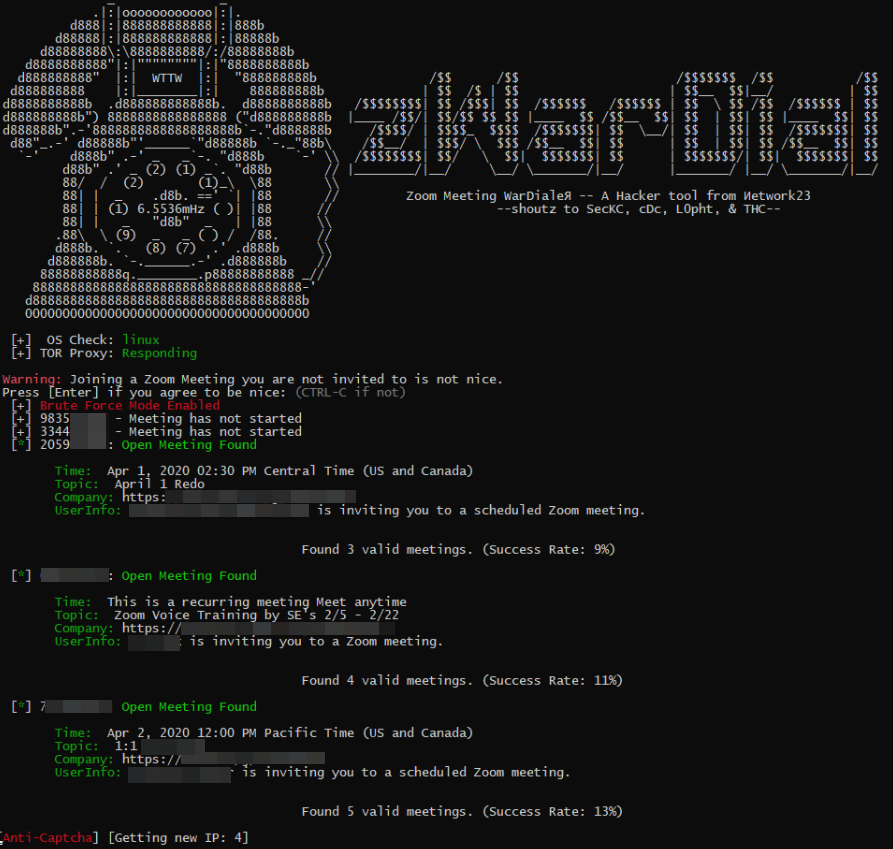
**‘War Dialing’ Tool Exposes Zoom’s Password Problems**

As the Coronavirus pandemic continues to force people to work from home, countless companies are now holding daily meetings using videoconferencing services from **Zoom**. But without the protection of a password, there’s a decent chance your next Zoom meeting could be “Zoom bombed” — attended or disrupted by someone who doesn’t belong. And according to data gathered by a new automated Zoom meeting discovery tool dubbed “**zWarDial**,” a crazy number of meetings at major corporations are not being protected by a password.

[](https://krebsonsecurity.com/wp-content/uploads/2020/04/zwardial-red1.png)

*zWarDial, an automated tool for finding non-password protected Zoom meetings. According to its makers, zWarDial can find on average 110 meetings per hour, and has a success rate of around 14 percent.*

Each Zoom conference call is assigned a Meeting ID that consists of 9 to 11 digits. Naturally, hackers have figured out they can simply guess or automate the guessing of random IDs within that space of digits.

Security experts at **Check Point Research** [did exactly that last summer](https://research.checkpoint.com/2020/zoom-zoom-we-are-watching-you/), and found they were able to predict approximately four percent of randomly generated Meeting IDs. The Check Point researchers said enabling passwords on each meeting was the only thing that prevented them from randomly finding a meeting.

Zoom responded by saying it was enabling passwords by default in all future scheduled meetings. Zoom also said it would block repeated attempts to scan for meeting IDs, and that it would no longer automatically indicate if a meeting ID was valid or invalid.

Nevertheless, the incidence of [Zoombombing](https://techcrunch.com/2020/03/17/zoombombing/) has skyrocketed over the past few weeks, even prompting an alert by the FBI on how to secure meetings against eavesdroppers and mischief-makers. This suggests that many Zoom users have disabled passwords by default and/or that Zoom’s new security feature simply isn’t working as intended for all users.

New data and acknowledgments by Zoom itself suggest the latter may be more likely.

Earlier this week, KrebsOnSecurity heard from [Trent Lo](https://www.twitter.com/surbo), a security professional and co-founder of [SecKC](https://www.seckc.org/), Kansas City’s longest-running monthly security meetup. Lo and fellow SecKC members recently created **zWarDial**, which borrows part of its name from [the old phone-based war dialing programs](https://www.youtube.com/watch?v=zb1r_uKOew4) that called random or sequential numbers in a given telephone number prefix to search for computer modems.

Lo said zWarDial evades Zoom’s attempts to block automated meeting scans by routing the searches through multiple proxies in [Tor](https://en.wikipedia.org/wiki/Tor_(anonymity_network)), a free and open-source software that lets users browse the Web anonymously.

“Zoom recently said they fixed this but I’m using a totally different URL and passing a cookie along with that URL,” Lo said, describing part of how the tool works on the back end. “This gives me the [Zoom meeting] room information without having to log in.”

Lo said a single instance of zWarDial can find approximately 100 meetings per hour, but that multiple instances of the tool running in parallel could probably discover most of the open Zoom meetings on any given day. Each instance, he said, has a success rate of approximately 14 percent, meaning for each random meeting number it tries, the program has a 14 percent chance of finding an open meeting.

Only meetings that are protected by a password are undetectable by zWarDial, Lo said.

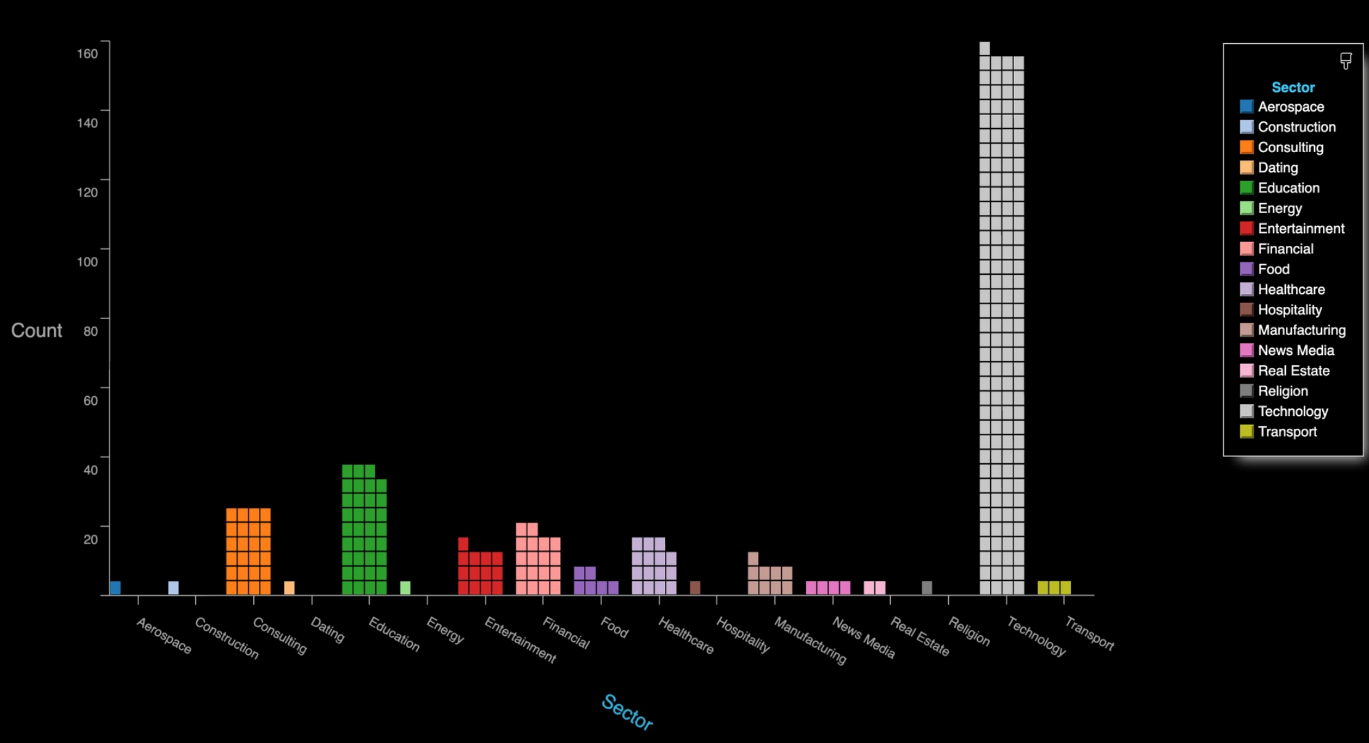
“Having a password enabled on the meeting is the only thing that defeats it,” he said.

Lo shared the output of one day’s worth of zWarDial scanning, which revealed information about nearly 2,400 upcoming or recurring Zoom meetings. That information included the link needed to join each meeting; the date and time of the meeting; the name of the meeting organizer; and any information supplied by the meeting organizer about the topic of the meeting.

The results were staggering, and revealed details about Zoom meetings scheduled by some of the world’s largest companies, including major banks, international consulting firms, ride-hailing services, government contractors, and investment ratings firms.

KrebsOnSecurity is not naming the companies involved, but was able to verify dozens of them by matching the name of the meeting organizer with corporate profiles on LinkedIn.

By far the largest group of companies exposing their Zoom meetings are in the technology sector, and include a number of security and cloud technology vendors. These include at least one tech company that’s taken to social media warning people about the need to password protect Zoom meetings!

[](https://krebsonsecurity.com/wp-content/uploads/2020/04/zwardialmeetingsbyindustry.png)

*The distribution of Zoom meetings found by zWarDial, indexed by industry. As depicted above, zWarDial found roughly 2,400 exposed meetings in less than 24 hours. Image: SecKC.*

**A GREMLIN IN THE DEFAULTS?**

Given the preponderance of Zoom meetings exposed by security and technology companies that ostensibly should know better, KrebsOnSecurity asked Zoom whether its approach of adding passwords by default to all new meetings was actually working as intended.

In reply, Zoom said it was investigating the possibility that its password-by-default approach may fail under certain circumstances.

“Zoom strongly encourages users to implement passwords for all of their meetings to ensure uninvited users are not able to join,” the company said in a written statement shared with this author.

*Under certain circumstances, users unaffiliated with an account owner or administrator may not have had passwords switched on by default at the time that change was made.*

“Passwords for new meetings have been enabled by default since late last year, unless account owners or admins opted out,” the statement continues. “We are looking into unique edge cases to determine whether, under certain circumstances, users unaffiliated with an account owner or administrator may not have had passwords switched on by default at the time that change was made.”

The acknowledgment comes amid a series of security and privacy stumbles for Zoom, which has seen its user base grow exponentially in recent weeks. Zoom founder and chief executive **Eric Yuan** said in a recent blog post that the maximum number of daily meeting participants — both paid and free — has grown from around 10 million in December to 200 million in March.

That rapid growth has also brought additional scrutiny from security and privacy experts, who’ve found plenty of real and potential problems with the service of late. TechCrunch’s **Zack Whittaker** has a fairly comprehensive breakdown of them [here](https://techcrunch.com/2020/03/31/zoom-at-your-own-risk/); not included in that list is [a story he broke earlier this week](https://techcrunch.com/2020/04/01/zoom-doom/) on a pair of zero-day vulnerabilities in Zoom that were publicly detailed by a former NSA expert.

Zoom CEO Yuan acknowledged that his company has struggled to keep up with steeply growing demand for its service and with the additional scrutiny that comes with it, saying in a blog post that for the next 90 days all new feature development was being frozen so the company’s engineers could focus on security issues.

**Dave Kennedy**, a security expert and founder of the security consultancy [TrustedSec](https://www.trustedsec.com/), penned a lengthy thread on Twitter saying while Zoom certainly has had its share of security and privacy goofs, some in the security community are unnecessarily exacerbating an already tough situation for Zoom and the tens of millions of users who rely on it for day-to-day meetings.

“What we have here is a company that is relatively easy to use for the masses (comes with its challenges on personal meeting IDs) and is relatively secure,” Kennedy [wrote](https://twitter.com/HackingDave/status/1245536000819986432). “Yet the industry is making it out to be ‘this is malware’ and you can’t use this. This is extreme. We need to look at the risk specific applications pose and help voice a message of how people can leverage technology and be safe. Dropping zero-days to the media hurts our credibility, sensationalizes fear, and hurts others.”

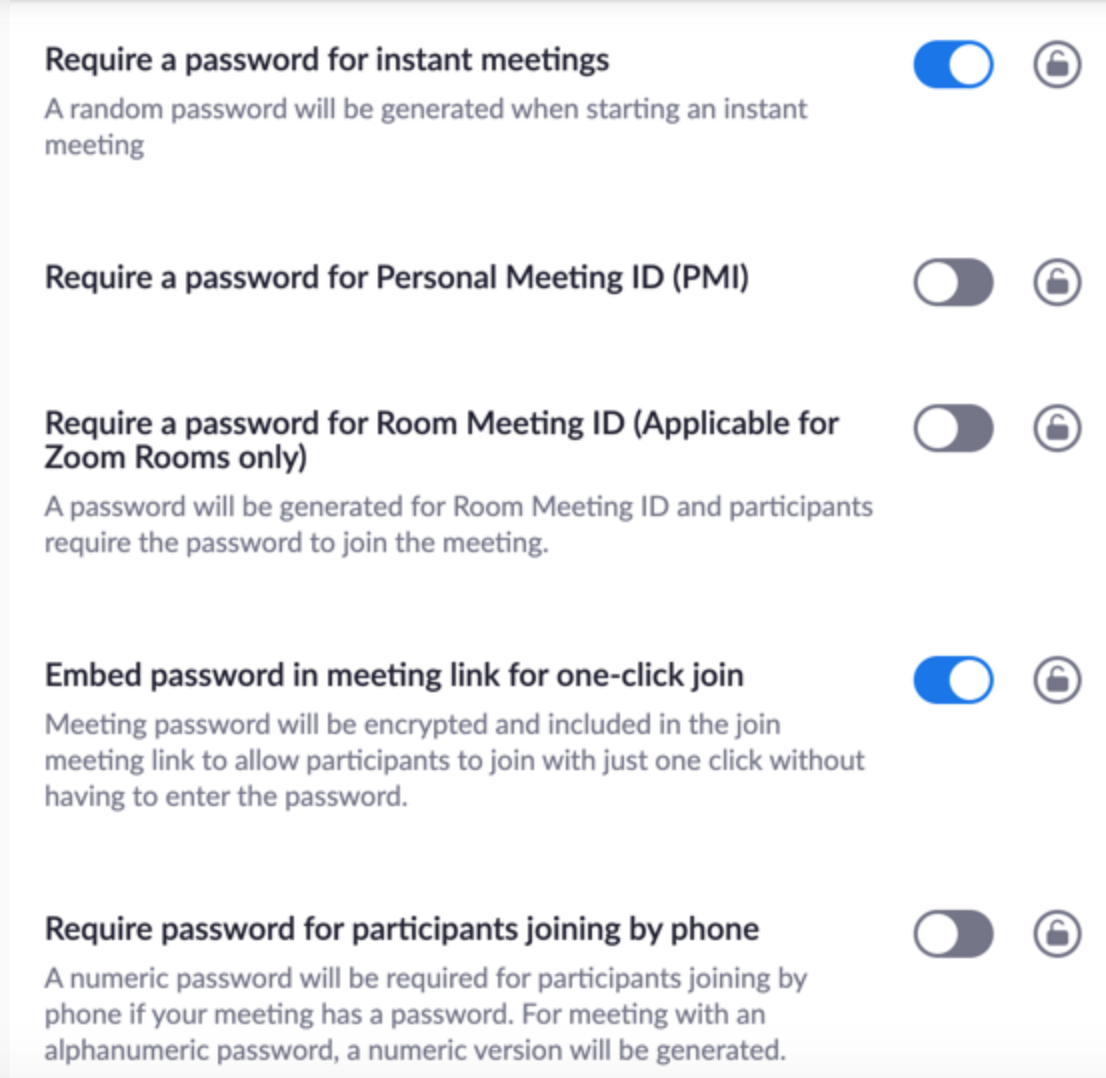
“If there are ways for a company to improve, we should notify them and if they don’t fix their issues, we should call them out,” he continued. “We should not be putting fear into everyone, and leveraging the media as a method to create that fear.”

Zoom’s advice on securing meetings is [here](https://support.zoom.us/hc/en-us/articles/360033331271-Account-Setting-Update-Password-Default-for-Meeting-and-Webinar). SecKC’s Lo said organizations using Zoom should [avoid posting the Zoom meeting links on social media](https://twitter.com/bry_campbell/status/1244994026413137920), and always require a meeting password when possible.

“This should be enabled by default as a new customer or a trial user,” he said. “Legacy organizations will need to check their administration settings to make sure this is enabled. You can also enable ‘Embed password in meeting link for one-click join.’ This prevents an actor from accessing your meeting without losing the usability of sharing a link to join.”

In addition, Zoom users can disable “Allow participants to join the meeting before the host arrives.”

“If you have to have this feature enabled at least enable “notify host when participants join the meeting before them,” Lo advised. “This will notify you that someone might be using your meeting without your knowledge. If you must keep your meeting unprotected you should enable ‘Mask phone number in the participant list.’ Using the waiting list feature will prevent unwanted participants from accessing your meeting but it will still expose your meeting details if used without a password.”



*Some of the security settings available to Zoom users. These and others can be found at https://www.zoom.us/profile/settings/*