SPACE INVADERS: THE NETWORKED TERRAIN OF ZOOM BOMBING

By Brian Friedberg, Gabrielle Lim, and Joan Donovan, PhD

tasc | Technology and Social Change Project

HARVARD Kennedy School
SHORENSTEIN CENTER
on Media, Politics and Public Policy

Table of Contents

EXECUTIVE SUMMARY

Within days of the virtual meeting platform Zoom becoming a household name, news spread that meetings were being hijacked by uninvited guests. The practice was quickly dubbed Zoom bombing.

Zoom bombing is a novel form of raiding or bombing, a common type of coordinated online attack. In this report, we examine how Zoom bombing works, the sociotechnical systems that enabled it, and the networked terrain of the attacks. Zoom bombing illustrates that networked participatory technology is often used in malicious or mischievous ways its creators and clients did not — but should have — foreseen.

When workers across the US first began staying home in order to flatten the COVID-19 curve in early March, 2020, a huge proportion of them began using Zoom. This rapid explosion in popularity was met with pre-existing sociotechnical conditions that created the perfect environment for Zoom bombing: lax security settings in the software, inadequate training for new users who inaccurately assumed the software was more private than it was, bored teenagers home from school, social proclivities toward trolling, and easy outlets for the bombs to go viral. Therefore, Zoom bombing isn't technically "hacking," but rather a misuse of Zoom's core functionality. It is a sociotechnical exploit that combines sociocultural and technical conditions to deliver a threat.

We trace Zoom bombs through their life cycle across multiple platforms and show how the phenomenon morphed from a low-stakes gag to a coordinated effort to cause real social harm by spreading noxious and hateful content to unexpecting audiences.

This paper explains what Zoom bombings is, who Zoom bombers and their targets are, where and how they coordinate, execute and share attacks, and how press attention on the phenomenon has changed the information ecosystem. We seek to shed light on these processes to offer a comprehensive and nuanced explanation of the vulnerabilities that drive Zoom bombing and to offer suggestions for how the makers of communication technologies can better anticipate these kinds of misuses to protect their users.

INTRODUCTION

As social distancing measures and stay-at-home orders rolled out around the world in response to COVID-19, people tried to replicate real-world connections online. Millions turned to Zoom, a web video conferencing platform, which saw its user base jump from 10 to 200 million in a month.[1] This exponential growth created an opportunity for a novel kind of mayhem: "Zoom bombing," whereby people disrupt online meetings, often with offensive and provocative content, to evoke lulz or cause genuine harm.

The phenomenon was born of boredom, and began as a kind of prank. Take the case of the YouTuber twomad. "aite start dming me your zoom classes/karate/ church whatever. i'll be live in around 30 mins,"[2] he tweeted in April, indicating the popular internet personality would invade Zoom meetings sent to him by his followers, and broadcast the results live.[3] The tweet was met with glee from his followers. A beloved young troll known for his outlandish sketches and awkward online encounters, twomad's YouTube channel currently boasts 1.13 million subscribers, and his antics are popular meme fodder in Generation Z spaces. For several weeks, twomad would pop into unsuspecting online classes using links and passwords provided on Twitter and Discord, disrupting the confused participants to the delight of his audience. "TWOMAD JUST INVADED MY FUCKING ZOOM MEETING,"[4] boasted a follower on Twitter, and many other social media users proudly displayed examples of twomad in their virtual classrooms.

---

1   "A Message to Our Users," *Zoom*, last modified April 1, 2020, https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/.

2   twomad, Twitter post, April 21, 2020, 11:46 a.m., https://twitter.com/twomad/status/1252624700687048706.

3   twomad, "Invading Random Online College Classes 2...." April 21, 2020, Video, 8:36. https://youtu.be/ocCKMSy_4So.

4   da plate, Twitter post, May 4, 2020, 1:14 p.m., https://twitter.com/whoakden/status/1257358067022381056.

This is a more lighthearted example of the phenomenon referred to as Zoom bombing. Many students stuck at home and adjusting to online classes necessitated by COVID-19 see a Zoom disruption by an internet celebrity like twomad as playful entertainment. On social media, they and others share short video clips, screenshots and memes of these Zoom bombs as small bits of comedy in an otherwise dark and disorienting time. However, online pranks rarely remain as innocent as they begin. As Zoom meetings become increasingly popular and Zoom bombs go viral, more and more people recognize the disruptive possibility of exploiting Zoom's lax default privacy settings. This has sparked a coordinated effort to use Zoom bombs to cause real social harm by spreading noxious and hateful content to unexpecting audiences.

Zoom bombing has since hit Narcotics Anonymous gatherings, virtual classes, and even government meetings. While much of the focus has been on Zoom itself, the campaigns are carried out using multiple platforms and are the product of sociocultural and technical conditions. This paper seeks to shed light on these processes and offers a more comprehensive and nuanced explanation of the vulnerabilities that drive Zoom bombing.

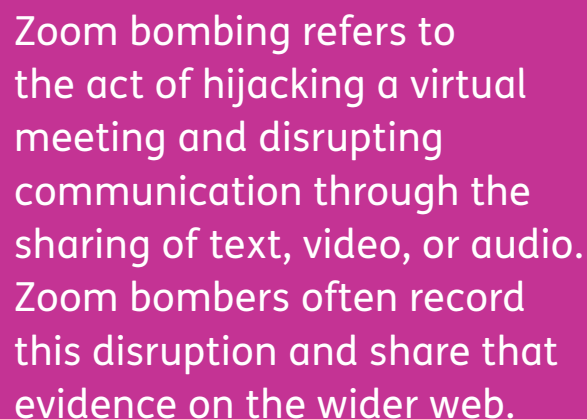*This is a thumbnail image for a twomad YouTube recording of Zoom bombings.*

Part 1:

EXPLAINING THE SOCIOTECHNICAL SYSTEM

What Is Zoom Bombing?

Zoom bombing refers to the act of hijacking a virtual meeting and disrupting communication through the sharing of text, video, or audio. Zoom bombers often record this disruption and share that evidence on the wider web. This form of behavior is commonly referred to as "raiding" or "bombing" online, taking the term from organized attacks carried out in video games, itself a reference to the military exercise. While "raiding" implies the coordination of groups of individuals to carry out these attacks, Zoom bombing may refer to individual actions that disrupt teleconferences as well as those done en mass. Sometimes these raids are just for fun, but also for more targeted reasons, including disruption of business activities and identity-based attacks on marginalized groups.

The term Zoom bombing was popularized by reporter Josh Constantine on March 17, 2020, after his publication *TechCrunch*'s "Work from Home Happy Hour" Zoom call was raided by anonymous individuals sharing offensive content.[5] After this initial reporting, use of the term spread to other press outlets and on social media. "Zoom bombing" is now used commonly to refer to attacks being carried out on schools, businesses, nonprofits and support groups who have been forced to move online because of social distancing requirements enacted to combat COVID-19.

> Zoom bombing refers to the act of hijacking a virtual meeting and disrupting communication through the sharing of text, video, or audio. Zoom bombers often record this disruption and share that evidence on the wider web.

5   Josh Constine, "Beware of 'ZoomBombing': screen sharing filth to video calls," *TechCrunch*, March 17, 2020, https://techcrunch.com/2020/03/17/ZoomBombing/.

While teleconferencing and remote meeting technology has been widely available and used by multiple sectors for decades, the rapid adoption of Zoom as a platform for remote meetings created an unprecedented surge in their user base, and unforeseen vulnerabilities.

Counter to much popular sentiment during the dawn of the phenomenon, Zoom bombing isn't technically "hacking," but rather a misuse of Zoom's core functionality. Zoom bombers use three functions of the platforms for their disruptive raids: video and audio sharing, screen sharing, and chat. Instead of sharing their audio visual content via webcam as is standard in a Zoom meeting, bombers would use their live video feed to broadcast offensive materials. Screen sharing allows users to broadcast content on their own computer to the group, and hijackers often queue up images or video to then widely broadcast to the groups. Bombers also exploit the chat feature by posting offensive words or phrases. They often, but not always, use third-party recording software or external cameras to capture the Zoom bomb and later share that recording widely.

Ultimately, Zoom bombing is a sociotechnical exploit, in that it combines sociocultural and technical conditions to deliver a threat.[6] Sociocultural and technical conditions, while not necessarily vulnerabilities on their own, when combined lead to unique exploits that can be taken advantage of by threat actors. The Zoom bombing phenomenon takes advantage of three different sociocultural and technical conditions: the application's lax default privacy settings, as opposed to a bug in the traditional cybersecurity sense; cultural proclivities that drive the activity, such as pranking and trolling culture, racism and misogyny, and widespread expectations of privacy; and the sudden and rapid need for millions of people to use a technology with which they were not that familiar. Goerzen et al. describe these combinations as "sociotechnical exploits," while other scholars have also identified the importance of understanding the social layer and the potential harms that can arise when combined with the technical layer.[7]

Because Zoom bombing is emergent from technical and sociocultural conditions, understanding why Zoom bombing exists requires an explanation of both layers. From the technical layer, Zoom's default privacy settings are extremely lax. Until recently, meetings were not automatically password protected, all attendees could freely share their screens, claim host role (which comes with more administrative privileges), chat to all other attendees, turn on their audio and video at will, and use the whiteboard feature, which allows attendees to draw over a shared screen. These features when combined with the social layer — such as the hosts' unfamiliarity with the web conferencing software, their assumptions

---

6   Matt Goerzen, Elizabeth Anne Watkins, Gabrielle Lim, "Entanglements and Exploits: Sociotechnical Security as an Analytic Framework," presented at the 9th USENIX Workshop on Free and Open Communications on the Internet (FOCI), Santa Clara, CA, August 2019, https://www.usenix.org/conference/foci19/presentation/goerzen.

7   David V. Gioe, Michael S. Goodman, and Alicia Wanless, "Rebalancing cybersecurity imperatives: patching the social layer," *Journal of Cyber Policy* 4, no. 1 (April 26, 2019): 117-137, https://www.tandfonline.com/doi/full/10.1080/23738871.2019.1604780.

that privacy was assured, and the desire of individuals and groups to engage in provocative behavior to elicit negative reactions — allowed trolling communities and teenage pranksters to wreak havoc on many a Zoom meeting.

Related Sociotechnical Behavior

Unexpected, malicious, or mischievous misuse of communication systems are common occurrences when new technology is adopted wide scale, resulting in unintended consequences, unforeseen vulnerabilities, and new forms of social disruption. So while the practice of Zoom bombing is novel, there is a long history of manipulating audiovisual and communication technology for mischief that predates the wide-scale adoption of the internet. For example, photobombing,

While the practice of Zoom bombing is novel, there is a long history of manipulating audiovisual and communication technology for mischief that predates the wide scale adoption of the internet.

which involves an individual inserting themselves into a photo being taken by others, may have been first recorded in 1853.[8]

The closest historical association with Zoom bombing, however, is manipulation of the phone systems. In the late 1970s, a loose coalition of hackers found ways to exploit vulnerabilities in telecommunication systems. This series of techniques, dubbed "phone freaking," allowed hackers to use signal and tone generation to gain access to systems not intended for them.[9] Telephone Denial of Service (TDoS) is a related phenomenon, sometimes referred to as "phone bombing," wherein individuals overwhelm a call line to prevent legitimate users from gaining access to telecommunication systems.

While Zoom bombing employs technical means, like denial of service, it is an intrinsically social activity and bears similarity to the insertion of instigative comments into online forums to elicit reactions. It is analogous to the raiding and bombing of comment sections. Initially introduced in 1998 by *The Rocky Mountain News*, comment sections were a new way for publishers to encourage engagement from audiences seeking their news online.[10] On news sites and blogs, users were able to create usernames or post anonymously, sharing their thoughts and impressions of an article. Many large news sites and microblogging services embraced this new form of interactivity during the 2000s.

---

8   Phil Edwards, "This 1853 image might show the first photobomb," *Vox*, September 25, 2015, https://www.vox.com/2015/9/25/9397733/first-photobomb.

9   Phil Lapsley, "Exploding the Phone," New York, USA, Grove Atlantic, 2014, https://groveatlantic.com/book/exploding-the-phone/.

As comment sections gained ubiquity in online publications, however, they were often hijacked by bad actors.[11] The feminist online publication *Jezebel* famously penned a letter demanding their parent company *Gawker* take action to eliminate harassment in the comments.[12] Raiding comment sections was also coordinated by far right groups seeking to spread their messaging to more mainstream audiences in the early 2010s.[13] Given the difficulty of filtering out toxic content in comment sections and the fact they represented just a small part of audience interaction overall, sites began scaling comment sections back in 2013. By 2018, most major publications declared open comment sections dead, though some publications like *The New York Times* continue to operate heavily moderated comment sections.[14]

Zoom bombing also bears many similarities to the act of raiding servers and streams in online gaming. By exploiting text, audio, emoticons, and in-game behavior, raiders disrupt gameplay with distracting content. These raids are coordinated off platform in chat groups and produce copycat efforts based on their success. Troll raids can involve simple mockery, sexual humor, or more harmful content like racism, sexism, or homophobia. In massively multiplayer games, trolls may undertake raiding campaigns for comedic purposes, such as with events in Second Life,[15] or as a way to advance racial profiling, as when Anonymous employed Nazi imagery in the MMO Habbo Hotel in what came to be known as the Pool's Closed campaign.[16] When trolls disrupt popular video game streamers on platforms like Twitch, they're intending to provoke reactions and gain attention from small internet celebrities, and will often repost clips of those disruptions on other platforms like YouTube. Some platforms, like Twitch, have adjusted their moderation practices to prevent trolling activity that violates terms of service, like the promotion of hate speech.[17]

The social behaviors used in Zoom bombing are rooted in the desire to explore, exploit, and sometimes hack new technology. When it comes to Zoom bombing, these urges found a uniquely fertile environment in which to express themselves, because of the speed with which a new telecommunication product was

11   Klint Finley, "A Brief History of the End of the Comments," *Wired*, October 8, 2015, https://www.wired.com/2015/10/brief-history-of-the-demise-of-the-comments-timeline/.

12   Peter Sterne, "Gawker turns off images in comments," *Politico*, August 12, 2014, https://www.politico.com/media/story/2014/08/gawker-turns-off-images-in-comments-002651.

13   Charlie Warzel, "How The Alt-Right Manipulates The Internet's Biggest Commenting Platform," *Buzzfeed News*, June 5, 2018, https://www.buzzfeednews.com/article/charliewarzel/how-the-alt-right-manipulates-disqus-comment-threads.

14   Keith A. Spencer, "Why comments sections must die," *Salon*, November 17, 2018, https://www.salon.com/2018/11/17/why-comments-sections-must-die/.

15   Stephanie Mercier Voyer, "Esteban Winsmore Has Resuscitated Second Life Through Trolling," *Vice*, December 2, 2013, https://www.vice.com/en_ca/article/jmkbay/esteban-winsmore-has-resuscitated-second-life-through-trolling.

16   "Pool's Closed," Know Your Meme, accessed April 27, 2020, https://knowyourmeme.com/memes/pools-closed.

17   Julia Alexander, "Twitch is temporarily suspending new creators from streaming after troll attack," *The Verge*, May 28, 2019, https://www.theverge.com/2019/5/28/18643167/twitch-artifact-suspend-new-users-trolls-attack-v.

adopted, the wide range of users forced to use it, and Zoom's lax default privacy settings. Zoom bombing is therefore a consequence of the combination of these sociocultural and technical conditions.

This report details the convergence of these conditions to illustrate how multi-platform campaigns are conducted — specifically when coordination, execution, and dissemination take place on different platforms — and how media manipulation, whether motivated to hurt or just for the lulz, can ultimately lead to changes in the information ecosystem.

Who Are the Zoom Bombers?

Although attributing the coordination, execution, and dissemination of a Zoom bomb is a difficult exercise, due to the anonymity provided by the platforms used, two general groups stand out for their participation: Gen Z students and online trolling communities. This section details their engagement, as well as the cultural and historical dimensions of these groups.

Gen Z Students

Members of Generation Z are commonly referred to as "Zoomers," a term popularized in the mid 2010s to contrast Gen Z with their grandparents' generation, the baby boomers.[18] Given the unprecedented shelter in place happening globally, many high school and college students are faced with the new reality of learning remotely at home. In the US, many of these classes are happening via Zoom or Google Classroom. This sudden shift to remote learning is subverting classroom dynamics, and creating unforeseen difficulties for educators. The young, extremely online set has a far larger toolkit than many of their parents or teachers, use many more communication and networking apps than older generations, and have far

This is Zoomer Wojack, a popular internet meme symbolizing Generation Z.

greater tech savvy. Among some younger internet users, who are often bored and looking for social activity of any kind, the sharing of Zoom links to encourage raids

---

18   "Words We're Watching: 'Zoomer.'" n.d. Accessed May 18, 2020, https://www.merriam-webster.com/words-at-play/words-were-watching-zoomer-gen-z.

has become a gamified pastime and a way to build social capital within their online communities. For maximum impact, sharing Zoom links with trolling communities is a quick way to get results.

Trolls

Trolling communities are loosely affiliated networks of pseudonymous individuals who start arguments and share offensive content to sow chaos in online communication. Much of the work of trolling is "spreading grisly or disturbing content, igniting arguments, or engendering general bedlam."[19] The degree of chaos ranges from pure jokes to organized harassment of individuals. Gabriella Coleman describes hackers, here phone freaks, as "fusing technological spelunking with mischief." On the more harmful end of the spectrum, much of the online harassment targets people of color, women, trans, and non-binary individuals. While not all trolls use hate speech, many do to cause a reaction or to spread racist ideology. The alt right, for example, grew out of trolling communities online, long since desensitized by offensive content that most internet users don't encounter on a daily basis. For communities hardened on sharing gore, horrific pornography and racism, Zoom bombing is a low-lift effort.

Brigading, a form of coordinated harassment, and trolling behavior have been used as tools of bad actors since the origin of message boards and other means of pseudonymous posting. Trolls rarely use their real names to engage in raids or brigading, and these groups have long cultural traditions of casting off screen names or accounts once they complete a campaign. Some of this is "identity tourism," a term coined by the media scholar Lisa Nakamura to describe the ways in which the internet allows users to "try on" various racialized and gendered identities.[20] Nakamura also connects organized racist and gendered harassment online to the troll practice of "griefing," which she describes as "the purposeful use of digital affordances to destroy another user's pleasure or freedom of movement" in group communication online. Zoom bombing can be seen as a form of griefing at scale, particularly when intentionally breaking up what were thought to be safe, enclosed social environments online.[21]

Zoom bombing campaigns have also drawn a significant amount of attention from the press. That attention is one of the goals of this kind of trolling, as communications scholar Whitney Phillips has pointed out when describing the cultural impact of trolling. She notes that small groups of anonymous actors are able to influence mass media in an ongoing asymmetrical warfare across social platforms.[22]

---

19   Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (London, UK, Verso Books, 2014), 19.

20   Lisa Nakamura, "Race In/For Cyberspace: Identity Tourism and Racial Passing on the Internet," 1995, https://pdfs. semanticscholar.org/3531/da9329d2b7158bd697e1aa8ef073f78de6fb.pdf.

21   Lisa Nakamura, "Putting Our Hearts Into It," in *Diversifying Barbie And Mortal Kombat*, eds. Yasmin B. Kafai, Gabriela T. Richard, and Brendesha M. Tynes, (Pittsburgh: Carnegie Mellon, ETC Press, 2016), 35-47. https://press.etc.cmu.edu/ index.php/product/diversifying-barbie-and-mortal-kombat-intersectional-perspectives-and-inclusive-designs-in-gaming/.

22   Whitney Phillips, *This Is Why We Can't Have Nice Things* (Cambridge, MA: MIT Press, 2015), https://mitpress.mit.edu/ books/why-we-cant-have-nice-things.

While Zoom bombing is a new example of this phenomenon, it is consistent with the antagonistic relationship between online culture and more formal media establishments. In some trolling communities, press coverage serves as "trophies," proof of their impact on mainstream discourse.

Despite the innocuous or mischievous nature of many Zoom bombing campaigns, we have encountered many examples of hard racism or white supremacist terminology in recorded Zoom bombs, some of which were shared on social media. White supremacists have a long history of organizing digitally, as Jessie Daniels has traced, including using private message boards to coordinate hate campaigns and engage in online disinformation tactics like "cloaked websites," where misleading site titles expose users to extreme racist materials unknowingly.[23] While some of the Zoom bombing examples we observed often employ charged racist and gendered words and imagery, we find little evidence of direct involvement of organized white nationalist groups in these campaigns.

Ultimately, trolls use offensive internet language and memes as weapons against the unexpecting, and revel in the trauma of those targeted. Although ascertaining which of these trolls hold sincere racist views and who are only using it to cause a reaction is near impossible, it almost doesn't matter, as the end result is the same: the spread of hate speech and imagery. While more organized white supremacists and Neo-Nazis may be involved in trolling campaigns, the use of racism as a tool of trolls doesn't necessitate formal engagement with hate movements. The use of offensive language and imagery is simply a tactic to quickly and easily shock, as is seeking out groups to raid.

> Ultimately, trolls use offensive internet language and memes as weapons against the unexpecting, and revel in the trauma of those targeted.

Who Are the Targets of Zoom Bombers?

Although an exact number is difficult to ascertain due to the inconsistent reporting of Zoom bombing occurrences and the lack of a transparency report from the company, the most prevalent targets of Zoom bombing are likely to be classrooms and public meetings with lax privacy settings. The latter includes a wide variety of targets, such as Alcoholics Anonymous gatherings, yoga classes, and government meetings. What they all have in common are assumptions of privacy, a lack of time and training in using Zoom's features, and, to varying degrees, the desire to increase participation among attendees.

Because of the rapid adoption of Zoom, many users were unaware of the platform's default privacy settings, which at the time that coronavirus was first sending the world indoors made meetings publicly available without a password and gave attendees a wide range of privileges, such as screen sharing, audio and video streaming, and the ability to change other attendees' names. As there was little time to prepare for the sudden adoption of Zoom, formal training was likely inconsistent, limited, or in some cases, non-existent. Educators from across the United States have criticized the transition to online teaching, citing poor resources and limited training. In some cases, the hosts of these meetings wanted to increase participation and ensure as many people as possible could attend. By making access and participation easier, however, these meetings were left unsecured and open for attack. While these conditions would not have been considered technical vulnerabilities in the traditional computer security sense, when combined, they resulted in an ideal target for Zoom bombing.

Although the activity typically consists of mild pranks and mere annoyance, highly coordinated and persistent campaigns that employ racist, sexist, and other offensive content have the potential to cause harm. Within the chat application Discord, where some of the raids were being coordinated, users expressed the desire to target women or minorities specifically. Speaking to *The Hollywood Reporter*, members of Alcoholics Anonymous, who rely on face-to-face meetings for support, spoke of repeatedly being targeted and harassed.[24] One member noted that the raids had turned darker and more disturbing, while another shared how such activity led some in the group to seek out alcohol again. What's more, these often traumatizing events were then shared across YouTube, TikTok, and Reddit, further violating the victims' privacy and desire to stay anonymous.[25]

---

24   Chris Gardner, "Pornography, Racial Slurs and Coordinated Attacks: How Zoom-Bombers Are Wreaking Havoc on Virtual 12-Step Meetings," *The Hollywood Reporter*, April 7, 2020, https://www.hollywoodreporter.com/rambling-reporter/how-zoombombers-are-wreaking-havoc-virtual-12-step-meetings-1288719.

25   Michael Kan, "Were You Zoom-Bombed? Video of It May Now Be on YouTube, TikTok for All to See," *PC Mag*, April 2, 2020, https://www.pcmag.com/news/were-you-zoom-bombed-video-of-it-may-now-be-on-youtube-tiktok-for-all-to.

Part 2:

MAPPING THE NETWORKED TERRAIN

Where Are Attacks Coordinated?

While an individual acting alone can create a large disturbance, coordinated raids of Zoom meetings have become a social activity traversing the networked terrain of multiple platforms and webspaces. Raiders coordinate by sharing links to Zoom meetings targets and other operational and logistical details regarding the execution of an attack. This section covers some of the online spaces where this coordination takes place, namely Discord, 4chan, Reddit. Additionally, we suggest many Zoom bombings are being coordinated privately, outside of our ability to investigate — on private chat applications like WhatsApp, Signal, Snapchat, Telegram, and in direct messages. It is even harder to prevent or assign blame for attacks organized in such private spaces.

Discord

Discord, released in 2015, is a free social application, designed for video gaming communities to communicate online. Users can communicate with text, image, video, and audio in a chat channel and host their own servers where larger groups can meet. In some ways, it is comparable to Slack, but tailored for gamers. While the coordination capabilities of the platform were designed for gamers seeking companionship and collaboration in online games, many people have used it for additional, and sometimes nefarious, purposes. Discord hosts various groups, from artists to designers, and even educators, but is perhaps best known as the epicenter of many meme and trolling communities.

Discord came to national attention after it was revealed that white nationalist groups were using the platform to organize, including coordinating the deadly Unite the Right rally of 2017.[26] Activists and researchers infiltrated these groups and were able to leak the chat logs to antifascist investigators at *Unicorn Riot*. In response, Discord banned many white nationalist, Nazi, and alt right groups and

---

26   Megan Farokhmanesh, "White supremacists who used Discord to plan Charlottesville rally may soon lose their anonymity," *The Verge*, August 7, 2018, https://www.theverge.com/2018/8/7/17660308/white-supremacists-charlottesville-rally-discord-plan.

symbols. However, the platform continues to be used by organized doxers, racists, misogynists, and transphobes.

In our research, we have observed several Discord servers where people share Zoom links, and many new servers created solely for coordinating Zoom bombings. Using names like "Zoom support," these servers were set up recently to take advantage of the Zoom bombing phenomenon. Discord servers created for trolling purposes are hardly new, though these dedicated Zoom groups are a result of the popularization of Zoom bombing online. By using names mentioning Zoom, and using server tags related to Zoom and bombing, the server administrators made their groups searchable on search engines like disboard.org, hoping to attract more users to share links and engage in raids.
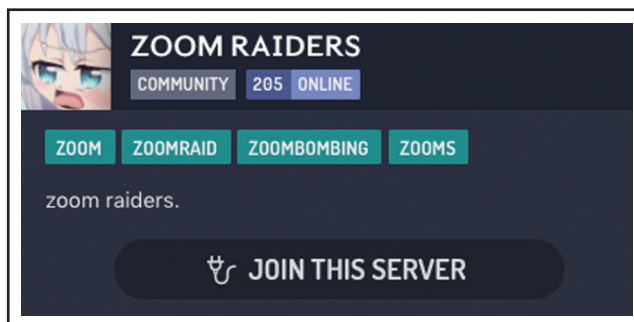
This is one example of a public Zoom raiding Discord sever accessed via disboard.org.

As social media users and journalists began pointing this practice out, Discord took some action against the large servers used to coordinate bombings. In response, the server administrators adapted, renaming some groups to hide their true purpose, while still using identifying tags, as seen in the "Bible Study with Kanye West!" group. Smaller, more focused groups formed, like those devoted to harassing marginalized populations via Zoom. These have names like "LGBTQ-Friendly Zoom" to signal the servers are dedicated to harassing sexual minorities.
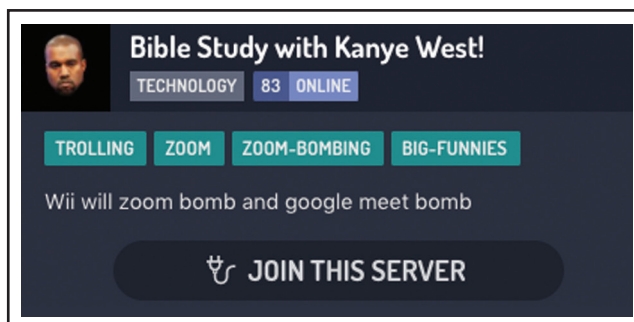

This is another example of a public Zoom raiding Discord sever accessed via disboard.org.

In these groups, users collect publicly available Zoom links found on Twitter, Facebook, and the open web. Some links are automatically gathered by web scraping bots and auto posted in these servers, and others are dropped in manually. By sharing Zoom links, users can pick and choose which meetings to invade. In these groups, trolls decide what content is used for trolling, and what is not — many, for example, draw the line at sharing images depicting the abuse of minors. However, racist, homophobic, and misogynistic language is usually fair game.

In late March, and early April, 2020, Discord removed several groups used to coordinate Zoom bombing. "This activity clearly violates Discord's Terms of

Service, and we removed the servers as soon as we were made aware of them,"[27] the company said in a statement to *PC Magazine* on March 31. Much of the pressure on platforms to act on terms of service (ToS) violations comes from critical press, but press attention delights trolls. They see negative press attention as a trophy and sign of victory. Articles such as the one pictured to the right are commonly shared within Zoom bombing Discord servers. It is clear from our research that Discord is a favorite place to coordinate and celebrate Zoom raids.
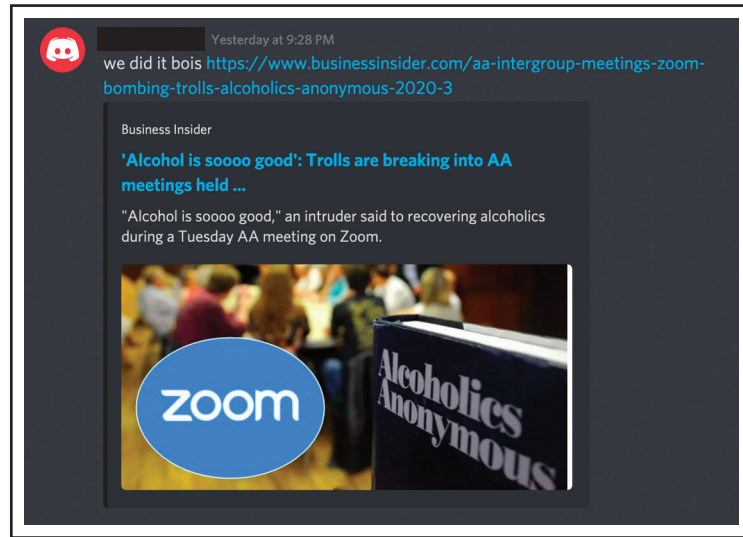
This is a post from a Discord server celebrating critical press coverage of a Zoom raid.

4chan

4chan is an anonymous English-language image-sharing website originally created for anime fandoms. Launched in 2003, the site hosts boards dedicated to music, literature, comics, video games, and fitness. 4chan has a long association with hacktivist and trolling communities, and has been used to launch everything from consumer pranks to the Anonymous movement of the late 2000s. The anonymity of the site (you don't have to register to post) provides cover for all manner of agents, activists, and trolls. It now also hosts

far more notorious communities, including the "politically incorrect" board, which is a hotbed of racist and misogynistic content, and the "random" board, where revenge porn is a popular commodity. The far-right Qanon conspiracy theory grew out of 4chan in 2017. After being invaded by organized white nationalists in the mid 2010s, far-right ideology and terminology became a norm on 4chan, and it was an influential space in the growth of the alt-right.
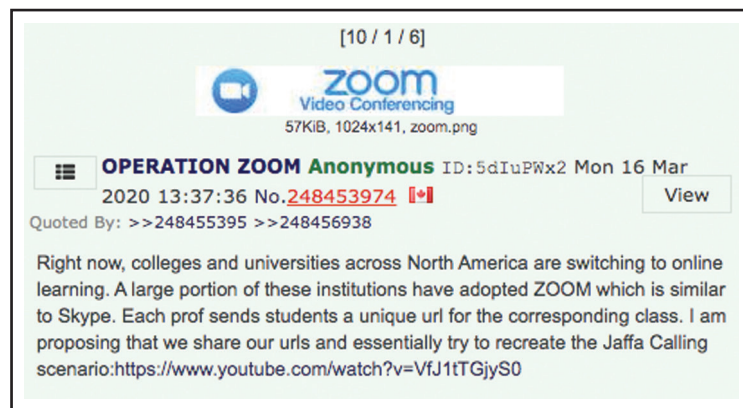
This is an example of a 4chan post attempting to organize Zoom raids.

27   Michael Kan, "Students Conspire in Chats to 'Zoom-Bomb' Online Classes, Harass Teachers," *PC Magazine*, March 31, 2020, https://www.pcmag.com/news/students-conspire-in-chats-to-zoom-bomb-online-classes-harass-teachers.

Zoom links are typically shared in ephemeral boards that are not archived. However in the course of our research we were able to save some of these posts. Although we found Zoom links being shared on 4chan, it is not the primary place where these attacks are coordinated. 4chan users were largely seen reacting to ongoing Zoom bombing campaigns as they were reported on social media and in the press. In addition, these may be removed by site moderators as they violate 4chan's terms of service regarding coordinated harassment.

Reddit

Reddit is a popular news sharing and discussion platform founded in 2005. All manner of interest groups use Reddit to share information and tips, and host political discussions. In some subreddits, like Teenagers, users have shared Zoom links for potential bombing. However, this content is usually quickly removed by site moderators as it clearly violates ToS. In fact, the majority of conversations about Zoom on Reddit occur among the adult user base. They share experiences of being Zoom bombed, and tips for how to prevent it from happening to others. The use of Reddit to coordinate is likely a marginal part of Zoom bombing, as active community moderation tends to remove links fairly quickly.

This is an example of a Reddit post soliciting readers to raid a Zoom class.

Where Are Attacks Shared?

Once a Zoom raid has been coordinated and executed, the video recording is often uploaded to the open web, becoming popular content on YouTube, TikTok, Instagram, and other social media platforms. While Zoom allows for a host to record a meeting, which alerts all participants via an automated message, there are many available workarounds for those looking to record a meeting unannounced. Cell phone cameras are the easiest way to record a Zoom meeting, and there is no way to prevent an individual from grabbing footage this way. Using free or paid third-party software like Bandicam or OBS Studio, users may directly capture streaming audio and video and record these to a file. Video recordings of Zoom bombings may then be edited, compressed, and uploaded to any number of video hosting or streaming platforms. As the demand for such videos grew, well-

known content creators began soliciting links to videos on social media.[28] In this section we cover the platforms used for dissemination.

YouTube

On YouTube, the world's largest video sharing platform, video recordings by Zoom bombers are popping up every day. Some users create "best of" clip compilations, sharing highlights from other videos originally hosted on other platforms. These typically use titles like "zoombombing compilation" or "best of online class trolling." Wracking up thousands of views, many of these trolling compilations do not feature direct hate speech, and depict more social disruption than offensive actionable content. YouTube's enforcement of its ToS against hate speech has kept the most offensive content from being recirculated. At the time of writing, it appears YouTube has deranked or removed Zoom bombing content from its platform after a wave of critical press.

TikTok

Popular video-sharing platform TikTok is also host to many short clips of Zoom bombings. Like YouTube, much of this content is more benign than some of the more egregious cases reported by educators, and where hate speech was used. The sharing of these short videos, like receiving press coverage, is a sign of victory for successful bombers. TikTok users have also taken to uploading their own reactions in "duet" format where they comment on Zoom bombings that have been recorded. On TikTok, these videos are shared using hashtags like #zoombomb for maximum visibility.

Instagram

Instagram users have also shared short clips of Zoom bombings, much like on TikTok, and some people have created accounts that specialize in sharing Zoom bombing clips. Like TikTok, these are shared with hashtags related to the terms Zoom, raid, and troll.

Twitch

Twitch, a video streaming site popular with gamers, has seen its share of Zoom bombing content, too. Some Twitch users have live streamed Zoom raids to their audiences. The platform has since removed some of the worst offenders, and generally has strongly enforced ToS for hate speech and coordinated harassment.

---

28   "Invading Random Online College Classes…." Youtube Video, 14:02, twomad https://www.youtube.com/watch?v=FJzMm-Cmfqk.

Twitter & Facebook

For the last few months, Twitter and Facebook have been a hotbed of conversation about Zoom bombing. Like Reddit, the userbase on Twitter and Facebook skews adult in age, and many of those people are sharing experiences they've had getting Zoom bombed and offering tips for avoiding being bombed, and some users are sharing images or short videos of the raids themselves. The term has quickly become part of our common online language, and the majority of the conversation about Zoom bombing on Twitter and Facebook is not driven by trolls. Some video clips of Zoom bombs were shared on these platforms, though many were hosted on other sites like YouTube and TikTok.

What Are the Changes to the Information Ecosystem?

Since being coined by *TechCrunch*, the term Zoom bombing has become ubiquitous in popular press coverage and on social media. According to the global news search engine Factiva, there were 2,938 English-language articles published containing the words "Zoom bomb", "Zoom bombing", or "Zoom Bombing" during March and April of 2020. Major US outlets like *The New York Times*,[29] *The Washington Post*,[30] and *CNN*[31] all featured stories on the phenomenon as more users began adopting the technology out of necessity. Much of the early coverage was describing the phenomenon, criticizing Zoom for its apparent security flaws, and teaching users how to avoid being bombed themselves. In tech sector reporting, there were many articles critical of Zoom's security and privacy, prompting CEO Eric Yuan to issue a statement addressing the many concerns with his platform.[32]

After the term Zoom bombing was established and normalized, some outlets reoriented reporting by looking deeper into the phenomenon, specifically on the coordination and sharing of Zoom bombing campaigns, and the additional life these videos have on YouTube and TikTok.[33] Despite some changes implemented by the platform, Zoom continued to be the target of critical press for both Zoom bombing and its myriad security and privacy issues.

29   Taylor Lorenz, "'Zoombombing': When Video Conferences Go Wrong," *The New York Times*, April 7, 2020, https://www.nytimes.com/2020/03/20/style/zoombombing-zoom-trolling.html.

30   Nick Anderson, "'Zoombombing' disrupts online classes at University of Southern California," *The Washington Post*, March 25, 2020, https://www.washingtonpost.com/education/2020/03/25/zoombombing-disrupts-online-classes-university-southern-california/.

31   Dakin Andone, "FBI warns video calls are getting hijacked. It's called 'Zoombombing'," *CNN*, April 2, 2020, https://www.cnn.com/2020/04/02/us/fbi-warning-zoombombing-trnd/index.html.

32   "A Message to Our Users," *Zoom*, last modified April 1, 2020, https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/.

33   Michael Kan, "Were you Zoom-Bombed? Video of It May Now Be on YouTube, TikTok for All to See." *PC Magazine*, April 2, 2020, https://www.pcmag.com/news/were-you-zoom-bombed-video-of-it-may-now-be-on-youtube-tiktok-for-all-to.

The identity-based attacks of many Zoom bombings also prompted an outcry from many civil society groups that campaign against abuse and hate online. Organizations like the Color of Change, the National Hispanic Media Coalition, the National LGBT Task Force, the Anti Defamation League, Equality Labs and others called on Zoom to address the hate and exploitation on its platform. Many of these groups pointed out that Zoom bombings employed defamatory language and tended to target marginalized groups specifically.[34]

Various levels of government have also responded. The Department of Justice issued a press release warning would-be Zoom bombers that they could be charged with state or federal crimes, and that these charges are punishable by fines and imprisonment.[35] To further drive home the point, the U.S. Attorney for Eastern Michigan warned, "You think Zoom bombing is funny? Let's see how funny it is after you get arrested. If you interfere with a teleconference or public meeting in Michigan, you could have federal, state, or local law enforcement knocking at your door." A Zoom bombing teen in Connecticut has already been arrested and charged with committing fifth-degree computer crime, fifth-degree conspiracy to commit a computer crime, and breach of peace.[36]

To avoid Zoom bombs, several school districts moved away from Zoom shortly after adopting it as a platform of choice for their teachers. The New York City Department of Education in early April advised principals not to use Zoom,[37] banning it completely in NYC.[38] Similarly, Nevada's Clark County[39] and individual schools in Los Angeles[40] have banned the app's use.

Other governments and government agencies have also limited or banned the use of Zoom, though that is likely due to a mix of security concerns that go beyond Zoom bombing.[41] For example, the Australian Defense Force, the Taiwanese government, and NASA have banned its use. While the Australian Defense Force

34   Shannon Bond, "Racial Slurs And Swastikas Fuel Civil Rights Pressure On Zoom," *NPR*, April 10, 2020, https://www.npr.org/2020/04/10/831379995/racial-slurs-and-swastikas-fuel-civil-rights-pressure-on-zoom.

35   "Federal, State, and Local Law Enforcement Warn Against Teleconferencing Hacking During Coronavirus Pandemic," Department of Justice, last modified April 3, 2020, https://www.justice.gov/usao-edmi/pr/federal-state-and-local-law-enforcement-warn-against-teleconferencing-hacking-during.

36   "Teen arrested after 'Zoom bombing' high school classes," *Associated Press*, April 8, 2020, https://apnews.com/ba16a1c1f4f6cdfa62d680f497461609.

37   Lauren Feiner, "NYC education department tells principals to stop using Zoom, citing privacy concerns," *CNBC*, April 6, 2020, https://www.cnbc.com/2020/04/06/nyc-doe-tells-principals-to-switch-from-zoom-to-google-and-microsoft.html.

38   Zack Whittaker, "New York City bans Zoom in schools, citing security concerns," *TechCrunch*, April 5, 2020, https://techcrunch.com/2020/04/05/zoom-new-york-city-schools/.

39   Alexis Egeland, "Clark County schools ban Zoom app over security concerns," *Las Vegas Review Journal*, April 1, 2020, https://www.reviewjournal.com/local/education/clark-county-schools-ban-zoom-app-over-security-concerns-1997093/.

40   Anna Kemenetz, "Schools Ditch Zoom Amid Concerns Over Online Learning Security," *NPR*, April 6, 2020, https://www.npr.org/sections/coronavirus-live-updates/2020/04/06/828087551/schools-ditch-zoom-amid-concerns-over-online-learning-security.

41   Brandon Vigliarolo, "Who has banned Zoom? Google, NASA, and more," *Tech Republic*, April 9, 2020, https://www.techrepublic.com/article/who-has-banned-zoom-google-nasa-and-more/.

was Zoom bombed by a comedian, it's likely other security concerns, such as the company's misleading statements about encryption and the location of its servers, are a large concern to these groups.[42]

Response from Zoom and Other Tech Companies

Following increased scrutiny from the media, civil society, and the government, Zoom and Discord have made adjustments to their respective platforms. Zoom, which had already instituted a feature freeze in order to focus on security, changed some of the default settings.[43] At the time of this writing, it has enabled waiting rooms and meeting passwords as a default, introduced a "Report a User" button, removed the meeting ID from the title bar, and added a security icon to adjust security settings such as "Lock meeting."[44]

Discord, meanwhile, has removed over 350 servers dedicated to Zoom bombing, in addition to taking down content and banning users.[45] Its community guidelines now also forbid "Organizing and participating in raids or other forms of harassment," warning that users engaging in this behavior may be removed along with the content.[46] Similarly, Facebook, Instagram, and Reddit have also taken down content related to Zoom bombing.[47]

---

43   Tom Warren, "Zoom announces 90-day feature freeze to fix privacy and security issues," *The Verge*, April 2, 2020, https://www.theverge.com/2020/4/2/21204018/zoom-security-privacy-feature-freeze-200-million-daily-users.

44   "90-Day Security Plan Progress Report: April 15," Zoom, last updated April 15, 2020, https://blog.zoom.us/wordpress/2020/04/15/90-day-security-plan-progress-report-april-15/.

CONCLUSION

In an interview with *NPR*, Zoom founder Eric Yuan admitted he had underestimated the threat of harassment, and that he "never thought about this seriously."[48] In a bid to make Zoom as easy as possible for as many types of individuals and organizations to use, the company traded security and privacy for increased market share, and in doing so failed to plan for the ways its platform could be misused. For example, Zoom removed the 40-minute meeting limit for their free "Basic" accounts for tens of thousands of schools around the world at the outbreak of the pandemic.[49] Zoom's Chief Financial Officer, Kelly Steckelberg also noted that the push to learn and work from home had provided Zoom with "the opportunity to get more people exposed to Zoom."[50] Despite this explosion of interest from groups and individuals who had not used this kind of tech before, the company did not recognize that a closer attention to security and privacy was essential. Move fast, break things — a motto coined by Facebook's CEO Mark Zuckerberg and operationalized by Silicon Valley entrepreneurs — appears to have struck again.[51]

Furthermore, Zoom bombing illustrates how networked participatory technology, in practice, is rarely defined by its narrow intended use cases. As with previous trolling campaigns, online harassment, and influence operations, specific sociocultural and technical conditions that on their own would not necessarily be vulnerabilities, can combine to deliver unique threats. This entanglement of once disparate groups raises serious privacy, security, and legal concerns over how such platforms ought to be governed, developed, and adopted.

As such, instead of assuming a narrow set of use cases intended for a singular client type (i.e. enterprise users with existing IT resources), companies like Zoom should reevaluate their design, implementation, and roll-out to encompass a more inclusive set of users. This may slow down the pace of delivering new

48   Shannon Bond, "Zoom CEO Tells NPR He Never Thought 'Seriously' About Online Harassment Until Now," *NPR*, April 8, 2020, https://www.npr.org/sections/coronavirus-live-updates/2020/04/08/829330707/zoom-ceo-tells-npr-he-never-thought-seriously-about-online-harassment-until-now.

49   "Zoom for Online Learning Updates: Expanded Access for Schools," Zoom, last updated March 29, 2020, https://blog.zoom.us/wordpress/2020/03/29/how-to-use-zoom-for-online-learning/.

50   Rani Molla, "Microsoft, Google, and Zoom are trying to keep up with demand for their now free work-from-home software," *Vox Recode*, March 11, 2020, https://www.vox.com/recode/2020/3/11/21173449/microsoft-google-zoom-slack-increased-demand-free-work-from-home-software.

51   Hemant Taneja, "The Era of "Move Fast and Break Things" Is Over," *Harvard Business Review*, January 22, 2019, https://hbr.org/2019/01/the-era-of-move-fast-and-break-things-is-over.

Zoom bombing illustrates how networked participatory technology, in practice, is rarely defined by its narrow intended use cases. As with previous trolling campaigns, online harassment, and influence operations, specific sociocultural and technical conditions that on their own would not necessarily be vulnerabilities, can combine to deliver unique threats.

features, but would raise and hopefully address important issues, such as harassment and privacy, that will affect their user base. In doing so, companies like Zoom may be able to anticipate how their platforms will be used and abused, leading to products designed to protect users from the get go. In addition, calls for Zoom to release a transparency report are worth highlighting.[52] Not only would such a report detail how the company handles its users' data and requests from state agencies, but the company could aggregate and release how many instances of harassment have been reported to them and what it has done to address the issue. Zoom's regular and public updates on its ongoing security changes is a good start.[53]

Lastly, Zoom bombing exemplifies the evolving nature of information operations and how campaign coordination, execution, and dissemination can involve multiple platforms, services, and targets. Proposed measures to counter such threats therefore require an understanding of the entire life cycle, the social and technical layers, and how users — as well as the "bad actors" — may adapt to changes made by the platforms involved, the government, and each other. Tactics may be ephemeral, but social-layer vulnerabilities are not. Longstanding sociopolitical cleavages may at a later date be co-opted again for nefarious purposes. The consequences, however, depend on how they get remixed with existing or emergent technologies, and how society responds.

---

52   Jay Peters, "Advocacy group calls for Zoom to release a transparency report," *The Verge*, March 19, 2020, https://www.theverge.com/2020/3/19/21186152/zoom-transparency-report-access-now-advocacy-group.

53   "90-Day Security Plan Progress Report: May 6," Zoom, accessed May 11, 2020, https://blog.zoom.us/wordpress/2020/05/07/90-day-security-plan-progress-report-may-6/.

ABOUT THE AUTHORS

Brian Friedberg

Brian Friedberg is the Senior Researcher of the Technology and Social Change Research Project at the Shorenstein Center on Media, Politics and Public Policy at Harvard Kennedy School. Blending academic research and open source intelligence techniques, Brian is an investigative ethnographer, focusing on the impacts alternative media, anonymous communities and unpopular cultures have on political communication and organization.

Gabrielle Lim

Gabrielle Lim is a Researcher at the Technology and Social Change Project at Harvard Kennedy's Shorenstein Center, as well as a fellow with Citizen Lab at the Munk School, University of Toronto. Her research focuses primarily on information controls and security.

Joan Donovan

Joan Donovan, PhD, is the Research Director of Harvard Kennedy's Shorenstein Center and the Director of the Technology and Social Change Research Project. Her research specializes in Critical Internet Studies, Science and Technology Studies, and the Sociology of Social Movements.

ACKNOWLEDGMENTS

tasc

Technology and
Social Change
Project

HARVARD Kennedy School
SHORENSTEIN CENTER
on Media, Politics and Public Policy