'Zoombombing' research shows legitimate meeting attendees cause most attacks

February 3 2021

Credit: Unsplash/CC0 Public Domain

Most zoombombing incidents are "inside jobs" according to a new study featuring researchers at Binghamton University, State University of New York.

As the COVID-19 virus spread worldwide in early 2020, much of our lives went virtual, including meetings, classes and social gatherings.

The videoconferencing app Zoom became an online home for many of these activities, but the migration also led to incidents of "zoombombing"—disruptors joining online meetings to share racist or obscene content and cause chaos. Similar apps such as Google Meet and Skype also saw problems.

Cybersecurity experts expressed concerns about the apps' ability to thwart hackers. A new study from researchers at Binghamton University and Boston University, however, shows that most zoombombing incidents are "inside jobs."

Assistant Professor Jeremy Blackburn and Ph.D. student Utkucan Balci from the Department of Computer Science at Binghamton's Thomas J. Watson College of Engineering and Applied Science teamed up with Boston University Assistant Professor Gianluca Stringhini and Ph.D. student Chen Ling to analyze more than 200 calls from the first seven months of 2020.

They found that the vast majority of zoombombing are not caused by attackers stumbling upon meeting invitations or "bruteforcing" their ID numbers, but rather by insiders who have legitimate access to these meetings, particularly students in high school and college classes. Authorized users share links, passwords and other information on sites such as Twitter and 4chan, along with a call to stir up trouble.

"Some of the measures that people would think stops zoombombing—such as requiring a password to enter a class or meeting—did not deter anybody," Blackburn said. "Posters just post the password online as well.

"Even the waiting rooms in Zoom aren't a deterrent if zoombombers name themselves after people who are actually in the class to confuse the teacher. These strategies that circumvent the technical measures in place are interesting. It's not like they're hacking anything—they're taking advantage of the weaknesses of people that we can't do anything about."

Because almost all targeting of Zoom meetings happens in real time (93% on 4chan and 98% on Twitter), the attacks seem to happen in an opportunistic fashion. Zoombombing posts cannot be identified ahead of time, so hosts have little or no time to prepare.

"It's unlikely that there can be a purely technical solution that isn't so tightly locked up that it becomes unusable," Blackburn said. "Passwords don't work—that's the three-word summary of our research. We need to think harder about mitigation strategies."

Because of the worldwide reach of the internet, the research team found that the problem is not restricted to just one country or time zone.

"We found zoombombing calls from Turkey, Chile, Bulgaria, Italy and the United States," Balci said. "It's a globalized problem now because of the circumstances of COVID."

Examining the dark corners of the internet has been Blackburn's main research for the past decade, but as anonymity breeds antisocial behavior and hate, there are—sadly—always new topics to consider.

"When we start turning over rocks, it's amazing what crawls out from under them," he said. "We're trying to look for one problem, but we'll also find five other problems under there that are somehow related, and we have to look at that, too."

One big drawback to this kind of study is having to do both quantitative

and qualitative analyses on vile hate speech. It even has to be published with a warning so that readers can brace themselves for what's ahead.

Blackburn and Balc both said that the camaraderie and open conversations at Blackburn's lab keeps everyone on an even keel.

"We do our best to make sure everybody is not taking it too personally," Blackburn said. "If you don't look at the content, you can't really do research about it, but if you look at the content too much or too deeply—you stare into the abyss a bit too long—you might fall into it. It's hard walking that line."

Balci added: "Sometimes I don't want to look at Twitter too much because the content is too overwhelming. It might depress me. However, from a research perspective, I'm curious about why these things happen. I just need to look at it in a more objective way."

The research, "A First Look at Zoombombing," was published by the IEEE Symposium on Security and Privacy (Oakland), 2021.

More information: A First Look at Zoombombing, arXiv:2009.03822 [cs.CY] arxiv.org/abs/2009.03822

Provided by Binghamton University