SITUATIONAL INFORMATION REPORT
FEDERAL BUREAU OF INVESTIGATION
Tradecraft Alert
BOSTON DIVISION

Reports of Teleconferencing and Online Classroom Hijacking in the FBI Boston AOR, as of March 2020

As large numbers of people turn to video-teleconferencing (VTC) platforms to stay connected in the wake of the COVID-19 crisis, reports of VTC hijacking (also called "Zoom-bombing") are emerging nationwide. The FBI has received multiple reports of conferences being disrupted by pornographic and/or hate images, and threatening language.

Within the FBI Boston Area of Responsibility (AOR), two schools in Massachusetts reported the following incidents:

- In late March 2020, a Massachusetts-based high school reported that, while a teacher was conducting an online class using the teleconferencing software Zoom, an unidentified individual(s) dialed into the classroom. This individual yelled a profanity and then shouted the teacher's home address in the middle of instruction.
- A second Massachusetts-based school reported, in late March 2020, a Zoom meeting being accessed by an unidentified individual. In this incident, the individual was visible on the video camera and displayed swastika tattoos.

As partners across the AOR transition to online lessons and meetings, FBI Boston recommends diligence in your cybersecurity efforts. The following steps can be taken to mitigate teleconference hijacking threats:

- Do not make meetings or classrooms public. In Zoom, there are two options to make a meeting private; require a meeting password or use the waiting room feature and control the admittance of guests.
- Do not share a link to a teleconference or classroom on an unrestricted publicly available social media post. Provide the link directly to specific people.
- Manage screensharing options. In Zoom, change screensharing to "Host Only."
- Ensure users are using the updated version of remote access/meeting applications. In January 2020, Zoom updated their software. In their security update, the teleconference software provider added passwords by default for meetings and disabled the ability to randomly scan for meetings to join.[1]
- Lastly, ensure that your organization's telework policy or guide addresses requirements for physical and information security.

[1] (U) Online article| Palmer, Danny | "Zoom fixes security flaw that could have let hackers join video conference calls" | *ZDNet.com* | 28 January 2020 | https://www.zdnet.com/article/zoom-fixes-security-flaw-that-could-have-let-hackers-join-video-conference-calls/, accessed 27 March 2020

Report instances of teleconference hijacking or cyber crimes to the Internet Crime Complaint Center at www.ic3.gov. If you receive a specific threat during a teleconference, please report it to the FBI via https://www.fbi.gov/tips, 1-800-CALLFBI (225-5324), or call FBI Boston at 857-386-2000.

Warning: This is an information report, not finally evaluated intelligence. It is being shared for informational purposes but has not been fully evaluated, integrated with other information, interpreted, or analyzed. Receiving agencies are cautioned not to take actions based solely on this raw reporting unless the information is independently verified.