Homeland Security

27 April 2020

(U//FOUO) Cyber Mission Center and Counterintelligence Mission Center

(U//FOUO) COVID-19: Advanced Persistent Threat Actors Likely View Zoom Platform Vulnerabilities as Attractive Opportunity to Threaten Public and Private Sector Entities

(U//FOUO) Scope. This *Article* provides federal, state, local, and private sector executives and network defenders insight into likely nation-state advanced persistent threat (APT) cyber actors exploiting the Zoom video- and teleconference platform in light of widespread public and private sector use during the COVID-19 pandemic.[a] This *Article* does not distinguish between the commercial and government versions of Zoom. This *Article* is the latest in a series of products on COVID-19 cyber threats, but differs in scope by focusing specifically on a technology tool that enables virtual collaboration.[b,c,d,e,f] The information cutoff date for this *Article* is 15 April 2020.

(U//FOUO) Prepared by the DHS Intelligence Enterprise (DHS IE) Cyber Mission Center (CYMC) and Counterintelligence Mission Center (CIMC). Coordinated with CBP, CISA, CWMD, FEMA, ICE, S&T, TSA, USCG, USSS, CIA, DIA, Department of Energy, Department of State, Department of the Treasury, FBI, NASIC, NGA, NIC, and NSA.

(U//FOUO) **APT actors likely will identify new or use existing vulnerabilities in Zoom to compromise user devices and accounts for further exploitation of corporate networks. This judgment includes critical infrastructure entities using Zoom.** We base this judgment on recent public exposure of Zoom's numerous vulnerabilities. While vendors regularly publish patches for vulnerabilities, reports indicate there are instances in which users and organizations delay updates. The patching process is undermined by APT actors who often capitalize on delays and develop exploits based on the vulnerability and available patches. We also base this judgment on reported Chinese access to Zoom servers. China's access to Zoom servers makes Beijing uniquely positioned to target US public and private sector users of the platform; however, we assume China's unique position does not prevent other nation-states from using Zoom vulnerabilities to achieve their objectives.

» (U) Several Zoom vulnerabilities have been publicized, including a vulnerability in the Zoom desktop conferencing application that allows an attacker to hijack various components of Zoom sessions, for which Zoom[USPER] has provided a patch; vulnerabilities in Zoom Client for Meetings that enable root access, as well as unprompted camera and microphone access; Zoom installing a hidden web server designed to circumvent pop-ups that removes password prompts; and using default settings to generate codes to join a meeting, easily leading to "zoombombing," according to an internationally distributed US news source, a Canada-based

[a] (U) APT actors are sophisticated cyber actors, typically state-sponsored, capable of gaining unauthorized access to a computer network and remaining undetected for an extended period.
[b] (U//FOUO) *Homeland Intelligence Article* titled "Nation-State Cyber Actors Likely to Conduct COVID-19-Themed Spear-Phishing Against Homeland Targets", published on 27 March 2020, serial number is IA-43452-20.
[c] (U//FOUO) *Homeland Intelligence Article* titled "Cyber Actors Almost Certainly View Growing Telework During the Novel Coronavirus Pandemic as an Opportunity to Exploit Enterprise Networks", published on 30 March 2020, serial number is IA-43325-20.
[d] (U//FOUO) *Homeland Intelligence Article* titled "Malicious Cyber Actors Likely See Opportunity to Target Virtual Private Network Vulnerabilities as More People Telework Due to COVID-19", published on 8 April 2020, serial number is IA-43472-20.
[e] (U//FOUO) Homeland Intelligence Article titled "COVID-19: Cybercriminals Almost Certainly Will Continue to Target US Public Using Economic Relief Themes and Scams," published on 15 April 2020; serial number is IA-43603-20
f (U//FOUO) Homeland Intelligence Today Article titled "(U//FOUO) Cyber Targeting of US Public Health and Healthcare Sector Likely to Increase During Pandemic," published on 15 April 2020; serial number is IA-43541-20.

research laboratory, a technology blog, and two vulnerabilities published on the National Institute for Standards and Technology (NIST) website.[1,2,3,4,5]

» (U) As of 15 April 2020 two zero-day exploits for Zoom that allow actors arbitrary code execution affecting Zoom on Windows and Apple operating systems were being sold for $500,000, according to a global research and advisory firm and an information security and technology news publication.[6,7,g] We are unable to confirm whether these zero-day exploits are related to already discovered and patched vulnerabilities. However, even if there are patches available for these vulnerabilities, organizations are slow or unwilling to install patches, as there are risks that a patch may disrupt other dependent systems, and installing patches may incur downtime for business operations, according to a cybersecurity company.[8]

» (U) APT cyber actors often use newly released software patches to develop exploits and access networks that have not yet upgraded with vendor released patches, according to an NSA cybersecurity advisory.[9] For example, APT actors as of October 2019 were exploiting common vulnerabilities in popular US virtual private network products to gain access to unprotected networks, according to the same source.

» (U) Zoom claims the application has end-to-end encrypted meetings; however, the company in its April 2020 blog clarified that Zoom does not currently implement end-to-end encryption as the cybersecurity industry understands the term, according to a Canada-based research laboratory and Zoom's company blog.[10,11]

» (U) Though Zoom is headquartered in the United States, the main Zoom application appears to be developed by three companies in China, which employ at least 700 workers, according to a Canada-based research laboratory providing strategic policy and legal engagement on information technologies, human rights and global security.[12] Additionally, tests conducted by the same research laboratory observed keys for encrypting and decrypting meetings were transmitted to servers in Beijing.[13] This raises concerns due to China's 2016 Cybersecurity Law, which compels foreign firms to hand over important intellectual property assets, such as source code, to Chinese authorities, and China's 2017 National Intelligence Law (Article 7), which mandates all organizations and citizens to support, assist, and cooperate with Chinese national intelligence efforts, according to an international online news source covering the Asia-Pacific region and a prominent American news source.[14,15]

(U//FOUO) **Malicious cyber actors likely view Zoom users as targets of opportunity to exploit a broad range of public and private sector entities including critical infrastructure.** We base this judgment on the extensive publicity surrounding Zoom's confidentiality issues and sudden popularity with users in a broad range of sectors adapting to the pandemic stay-at-home orders. This judgment is underpinned by the assumption that the unidentified cyber actors gained unsolicited access to ongoing Zoom conference sessions with ease, and that malicious actors can duplicate those efforts and use their accesses to facilitate additional malicious activities.

[g] (U) Zero-day exploits are custom-built exploits targeting systems running with vulnerabilities that have not yet been patched by a hardware or software vendor.

» (U) US schools in March 2020 reported that while teachers were conducting online classes on Zoom, unidentified cyber actors "zoombombed" the sessions, according to two US press reports and a report from the FBI's Boston Division.[16,17,18,h]

» (U) Researchers in April 2020 discovered over 500,000 Zoom accounts being sold and shared on the dark web and underground forums, according to an information security and technology news publication.[19] The accounts include users from banking and educational institutions, according to the same source.

» (U) Zoom from its foundation in 2011 to December 2019 grew to 10 million users, and within the first three months of 2020 saw a twenty-fold increase in usage to 200 million daily users, according to a Zoom company blog.[20]

» (U) Entities within a broad range of sectors—including commercial facilities, defense industrial base, financial services, government facilities, healthcare and public health, information technology, and state and local sectors—have reportedly used Zoom in some capacity, according to a company that leverages machine learning to discover and understand millions of companies worldwide and a Washington, DC-based radio station covering breaking news, information, and analysis for the people who support the missions of federal agencies.[21,22]

(U) Outlook

(U//FOUO) Zoom's sudden immense growth and use across both public and private sector entities in combination with its highly publicized cybersecurity issues creates a vulnerable, target-rich environment that APT actors likely see value in exploiting to achieve nation-state objectives against the Homeland, which could include disruption, espionage, or financial gain. Successful compromise of a critical infrastructure entity could inflict economic loss on at least the targeted organization, and if left undetected, preposition the cyber actors for future operations. Any organization currently using—or considering using—Zoom should evaluate the risk of its use.

(U) Intelligence Gap – APT Network Exploitation

(U//FOUO) We lack indicators showing sophisticated cyber actors accessing Zoom and compromising user devices to gain access to victim networks. APT actors could access a victim's network via Zoom is by exploiting vulnerabilities that allow them to access a user's account with stolen credentials or hijack a conference session. The actor also could leverage Zoom's integrated file transfer feature to deliver malware, such as a backdoor or other malicious executables. This root privilege escalation from Zoom to user device would enable the APT actor to further exploit the victim's corporate network.

(U) Reporting Computer Security Incidents

(U) To report a computer security incident, please contact CISA at 888-282-0870; or go to https://forms.us-cert.gov/report. Please contact CISA for all network defense needs and complete the CISA Incident Reporting System form. The CISA Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to CISA. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

(U) To report this incident to the Intelligence Community, please contact your DHS I&A Field Operations officer at your state or major urban area fusion center, or e-mail DHS.INTEL.FOD.HQ@hq.dhs.gov. DHS I&A Field Operations officers are forward deployed to every US state and territory and support state, local, tribal, territorial, and private sector partners in their intelligence needs; they ensure any threats, incidents, or suspicious activity is reported to the Intelligence Community for operational awareness and analytic consumption.

[h] (U) Zoombombing is a new form of trolling in which an unwanted or unwelcome participant uses Zoom's screen sharing feature to interrupt and disrupt meetings and classes.

(U) Source Summary Statement

(U//FOUO) This *Article* is based on 19 articles from a body of open-source reporting that includes an FBI press release, media reporting, the NIST website, a DoD cybersecurity advisory, technology news websites, a radio station's news coverage, cybersecurity firm reporting, a research advisory firm, and information from Zoom's website.

(U//FOUO) APT actors likely will identify new or use existing vulnerabilities in Zoom to compromise user devices and accounts for further exploitation of corporate networks. This judgment includes critical infrastructure entities using Zoom. We have **moderate confidence** in this assessment based on 15 reports citing various Zoom vulnerabilities. Of these reports, 14 are from credible news sources, a Canadian research laboratory, a technology-based news website, the NIST website, a DoD cybersecurity advisory, research advisory firm, and a cybersecurity company; one source is Zoom's company blog whose reliability cannot be determined, as there is a possible conflict of interest. Indicators show malicious actors compromising a Zoom user and subsequently gaining privileged access on a victim's device, which further allows actors to escalate privilege and move laterally on the victim's network. The 15 sources are dated from June 2017 to April 2020.

(U//FOUO) Malicious cyber actors likely view Zoom users as targets of opportunity to exploit a broad range of public and private sector entities including critical infrastructure. We have **moderate confidence** in this assessment based on seven reports of unidentified cyber actors targeting Zoom. Six reports are from credible for-profit and non-profit news sources, a highly credible FBI press release, and a reputable software company, while one report is from Zoom's company blog, whose reliability cannot be determined, as there is a possible conflict of interest. The seven sources are dated from March 2020 to April 2020.

[1] (U); USA Today; "Zoom Issues: People Hijacking Streams, Possible Security Flaws; 01 APR 2020; https://www.usatoday.com/story/tech/2020/04/01/zoom-demand-zooms-but-problems-coronavirus-drives-stay-home-video-chats-zoom-has-issues-beyond-deman/5102150002/; accessed on 02 APR 2020. Source is a reputable internationally-distributed US newspaper with a history of credible reporting.

[2] (U); Citizen Lab; "Move Fast and Roll Your Own Crypto a Quick Look at the Confidentiality of Zoom Meetings"; 03 APR 2020; https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/; accessed on 7 APR 2020. Source is a Canada-based research laboratory, based at University of Toronto that provides strategic policy and legal engagements for information technologies, human rights and global security and is considered reliable.

[3] (U); Tenable; "Remotely Hijacking Zoom Clients"; 03 DEC 2018; https://medium.com/tenable-techblog/remotely-exploiting-zoom-meetings-5a811342ba1d; accessed on 14 APR 2020.

[4] (U); NIST; "CVE-2020-11469"; 2020; https://nvd.nist.gov/vuln/detail/CVE-2020-11469; accessed on 14 APR 2020.

[5] (U); NIST; "CVE-2020-11470"; 2020; https://nvd.nist.gov/vuln/detail/CVE-2020-11470; accessed on 14 APR 2020.

[6] (U); Gartner; "Zoom Security Response; DOI UNK; accessed on 16 APR 2020; pg 4; Source is a global research and advisory firm; source is considered reliable.

[7] (U); Bleeping Computer; "Exploit for Zoom Windows Zero-day Being Sold for $500,000; 15 APR 2020; https://www.bleepingcomputer.com/news/security/exploit-for-zoom-windows-zero-day-being-sold-for-500-000/; accessed on 16 APR 2020; Source is a news source for information security and technology issues. Source is considered reliable.

[8] (U); Delta Risk; "We Don't Need No Stinking Patches: Why Organizations Don't Patch; 07 AUG 2019; https://deltarisk.com/blog/we-dont-need-no-stinking-patches-why-organizations-dont-patch/; accessed on 16 APR 2020; Source is a cybersecurity company providing Security Operations Center-as-Service and security services; Source is considered subject-matter expert and is reliable.

[9] (U); DoD; "NSA Cybersecurity Advisory: Malicious Cyber Actors Leveraging VPN Vulnerabilities for Attack; Check VPN Products for Upgrade;" 7 OCT 2019; https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1982939/nsa-cybersecurityadvisory-malicious-cyber-actors-leveraging-vpn-vulnerabilitie/; Source is considered an expert on cybersecurity issues and highly reliable.

[10] (U); Citizen Lab; "Move Fast and Roll Your Own Crypto a Quick Look at the Confidentiality of Zoom Meetings"; 03 APR 2020; https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/; accessed on 7 APR 2020. Source is a Canada-based research laboratory, based at University of Toronto that provides strategic policy and legal engagements for information technologies, human rights and global security and is considered reliable.

[11] (U); Zoom; "The Facts Around Zoom and Encryption for Meetings/Webinars" 01 APR 2020; https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/; accessed on 7 APR 2020.

Source is Zoom's company blog; however, we are unable to determine the veracity of Zoom's blog posting, as there is a possibility that the source is obscuring facts.

[12] (U); Citizen Lab; "Move Fast and Roll Your Own Crypto a Quick Look at the Confidentiality of Zoom Meetings"; 03 APR 2020; https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/; accessed on 7 APR 2020. Source is a laboratory based at University of Toronto that provides strategic policy and legal engagement on information technologies, human rights and global security and is considered reliable.

[13] (U); Citizen Lab; "Move Fast and Roll Your Own Crypto a Quick Look at the Confidentiality of Zoom Meetings"; 3 APR 2020; https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/; accessed on 7 APR 2020. Source is a Canada-based research laboratory, based at University of Toronto that provides strategic policy and legal engagements for information technologies, human rights and global security and is considered reliable.

[14] (U); The Diplomat; "China's Cybersecurity Law: What You Need to Know"; 1 June 2017; https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/; accessed on 7 APR 2020. Source is an international online news source covering Asia-Pacific region and a prominent American news source and is considered reliable.

[15] (U); CNBC; "Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice"; 4 MAR 2019; https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html; accessed on 7 APR 2020. Source is a prominent American news source and is considered reliable.

[16] (U); Los Angeles Times; "USC, school districts getting 'Zoom-bombed' with racist taunts, porn as they transition to online meetings"; 25 MAR 2020; https://www.latimes.com/california/story/2020-03-25/zoombombing-usc-classes-interrupted-racist-remarks; accessed on 30 MAR 2020; Source is a daily California-based newspaper with a history of credible reporting.

[17] (U); Chalkbeat; "Teachers across New York City are getting a lesson in 'Zoombombing'"; 24 MAR 2020; https://chalkbeat.org/posts/ny/2020/03/24/teachers-across-new-york-city-are-getting-a-lesson-in-zoombombing/; accessed on 30 MAR 2020; Source is a nonprofit news organization of unknown reliability or credibility that reports on education issues in local American communities.

[18] (U); FBI; "FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic"; 30 MAR 2020; https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic; accessed on 31 MAR 2020; Source is a reliable federal law enforcement agency.

[19] (U); Bleeping Computer; "Over 500,000 Zoom Accounts Sold on Hacker Forums, the Dark Web"; 13 APR 2020; https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/; accessed on 15 APR 2020; Source is a news source for information security and technology issues. Source is considered reliable.

[20] (U); Zoom; "A Message to Our Users"; 01 APR 2020; https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users; accessed on 07 APR 2020. Source is Zoom's company blog; however, we are unable to determine the veracity of Zoom's blog posting, as there is a possibility that the source is obscuring facts.

[21] (U); Enlyft; "Companies Using Zoom"; 2020; https://enlyft.com/tech/products/zoom; accessed on 15 APR 2020; Source is a company that leverages machine learning to discover and understand millions of companies worldwide.

[22] (U); Federal News Network; "For CIOs, the Decision to Limit the Use of Zoom Isn't a Big Deal"; 08 APR 2020; https://federalnewsnetwork.com/cybersecurity/2020/04/for-some-cios-the-decision-to-limit-the-use-of-zoom-isnt-a-big-deal/; accessed on 15 APR 2020; Source is a DC-based radio station with a history of credible reporting.