WHITE PAPER | COVID-19 VTC Exploitation

April 3, 2020

Health Sector Cybersecurity Coordination Center (HC3) | HC3@HHS.GOV

Executive Summary

The Coronavirus pandemic has resulted in increased telework, enabled largely by video-teleconferencing (VTC) services such as Zoom, WebEx, and others. This swell in usage has created an unusually large target for malicious hackers. Attacks include call interruption/disruption (aka "Zoom-bombing"), using fake web addresses to entice unsuspecting conference attendees to download malicious software, and exploiting multiple newly discovered zero-day vulnerabilities. VTC technologies are frequently used in the healthcare industry, and we advise healthcare organizations to respond appropriately.

Introduction

Popular online VTC technologies have seen a significant rise in use in recent months. Zoom has reportedly enjoyed an increase of over 2 million monthly active users in the first three months of 2020. Cisco, with VTC products such as WebEx and Telepresence, claims that customers spent over 5 billion minutes in virtual meetings in the first two weeks of March.[1 & 2] Healthcare organizations frequently use VTC technologies for regular business communications, and for telehealth and telemedicine delivery.[3 & 4] Cyberattacks may degrade or disrupt healthcare operations and may lead to leaks of personally identifiable information (PII) and protected health information (PHI). The primary categories of attacks we will cover in this paper include social engineering via the use of fake domains and exploitation of software vulnerabilities.

Exploitation

In recent weeks, there have been a number of ongoing attacks and newly-discovered exposures including two zero-day vulnerabilities, malicious domain registrations, and teleconference session hijacking. The Coronavirus pandemic and subsequent expansion of telework requirements has resulted in an increased use of Zoom and other VTC platforms. Consequently, fake domain registrations have spiked, especially those containing 'zoom,' which have a considerably greater potential in phishing unsuspecting users.[5] Check Point has noted that more than 1,700 new Zoom-related domains were created in the first three months of 2020 with approximately 25% registered at the end of March (see figure A).[6]

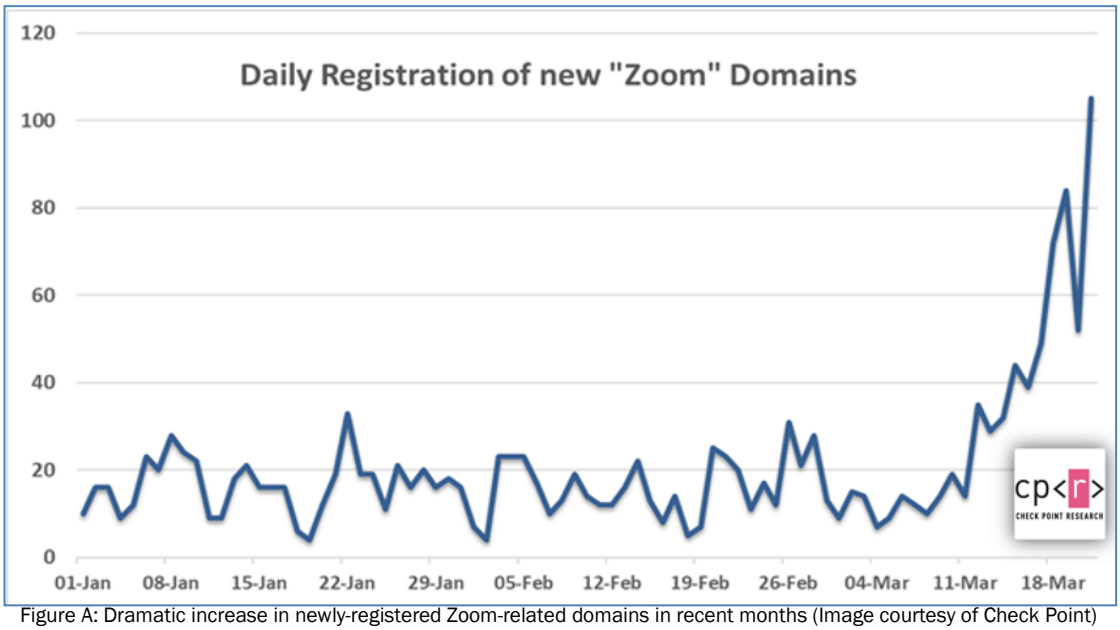

Figure A: Dramatic increase in newly-registered Zoom-related domains in recent months (Image courtesy of Check Point)

Fake domains are effective because legitimate Zoom meeting invitations include a link to the meeting (see Figure B). Similar to phishing campaigns, invites contain fake links that are designed to look legitimate and can entice a user to click the link and initiate a cyberattack to capture personal information or download malware for further compromise.[7 & 8]

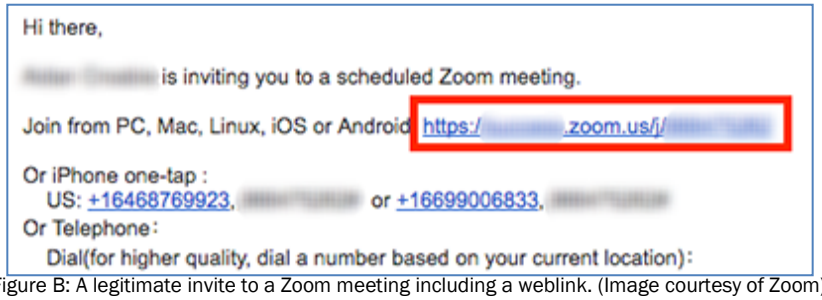

Figure B: A legitimate invite to a Zoom meeting including a weblink. (Image courtesy of Zoom)

Exacerbating the potential for attacks are several recently discovered zero-day vulnerabilities. One security researcher proved recently that Zoom's macOS application facilitated root-level attacks on an already-compromised system.[9] A second vulnerability allowed access to a victim's camera and microphone. Other security researchers found and verified a zero-day vulnerability in the Zoom Windows client, which may enable an attacker to steal a user's Windows credentials. These vulnerabilities were quickly patched. [10] Other major online VTC tools have had security concerns as well.

In early March 2020, Cisco released an advisory warning that its WebEx software was vulnerable to remote code execution (RCE) attacks. RCEs are particularly egregious in that they allow an attacker to execute malicious code on a victim system, which enables them with range of follow-up options to cause additional harm.[11] In late 2019, GoToMeeting was found to be susceptible to hacking (since resolved),[12] which like other VTC clients may be insecurely configured by users to enable ease of use.

Such configurations can open the door to abuse. "Zoom-bombing" is an additional attack seeing a recent surge in popularity, and is not limited to Zoom users.[13] Online communities such as Discord, Twitter, Reddit and various hacking message forums are being used to organize these efforts.[14] Attackers, usually motivated by trolling and pranks, take advantage of misconfigured meeting settings on a variety of cloud VTC sessions (e.g. Zoom, Cisco WebEx, Google Hangouts Meet, GoToMeeting, etc.), that allow anyone to join meetings, enabling an attacker to broadcast their own video, audio, and to share their screens with the rest of the meeting participants. Consequently, this has spurred a recent increase in zoom-bombing, with session hijackers sharing undesirable video and images such as pornography, hate symbols, and other disturbing imagery.[15] Finally, the compliance-impacting encryption measures of Zoom have been recently questioned by security researchers and various technology media outlets. Zoom posted a blog response about their encryption capabilities and announced in early April that they are pausing in their feature-development efforts to address security in their product.[16]

Conclusion

The existing threats to videoconference technologies creates many potential issues when left unresolved. Disruption of real-time communications can affect telemedicine and telehealth services as well as prevent collaboration of medical expertise in a timely manner. Several mitigations are necessary for healthcare and public health organizations to protect their stakeholders from harm while using these critically important applications.

Mitigations/Remediation

- Pay special attention to any voice or video conferencing software or other remote collaboration tools for the duration of the Coronavirus pandemic as these present an enticing target for malicious cyber threat actors
- Ensure all users are utilizing the most up-to-date teleconference software. Apply all operating system and application patches aggressively. For vulnerability management programs, ensure proper prioritization of systems and patches.
- Conference managers should be especially careful when authorizing participants/attendees to join a meeting and selectively specifying who can share their camera, microphone, or screen.[17]
- Configure password protection for ALL conferences and protect those passwords accordingly.
- Do not configure conferences to be available to the public, unless necessary. Do not post about conferences on unrestricted social media posts, unless necessary.
- Assume that information shared in a VTC conference will be disseminated beyond the authorized attendees.
- Limit access and maintain positive physical control of your devices. Strongly consider using separate accounts on your personal computer, with root or administrative access used only when necessary.
- Encourage users to use extreme caution when using any weblink posted to a VTC meeting.
- Report cybercrime, including teleconference hijacking, to the FBI's Internet Crime and Complaint Center (ic3.gov)[18]

Endnotes

[1] Novet, J. (February 26, 2020). Zoom Has Added More Videoconferencing Users This Year Than in All Of 2019 Thanks To Coronavirus, Bernstein Says. CNBC. Accessed April 1, 2020 at: https://www.cnbc.com/2020/02/26/zoom-has-added-more-users-so-far-this-year-than-in-2019-bernstein.html

[2] Bursztynsky, J. (March 17, 2020). Cisco CEO: Customers Spent 5.5 Billion Minutes in Virtual Meetings This Month Due to Coronavirus. CNBC. Accessed April 1, 2020 at: https://www.cnbc.com/2020/03/17/cisco-ceo-says-5point5-billion-minutes-of-webex-meetings-due-to-coronavirus.html

[3] Cisco. (n.d.) Clinicians: Get Started with Telehealth. Cisco WebEx. Accessed April 1, 2020 at: https://www.webex.com/webexremotehealth.html

[4] Zoom. (n.d.) Zoom for Healthcare. Zoom. Accessed April 1, 2020 at: https://zoom.us/docs/doc/Zoom%20for%20Healthcare.pdf

[5] Check Point. COVID-19 Impact: Cyber Criminals Target Zoom Domains. Check Point Software Technologies Ltd. Accessed April 1, 2020 at: https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains/

[6] Vijayan, J. (March 30, 2020). Researchers Spot Sharp Increase in Zoom-Themed Domain Registrations. Dark Reading. Accessed March 31, 2020 at: https://www.darkreading.com/vulnerabilities---threats/researchers-spot-sharp-increase-in-zoom-themed-domain-registrations/d/d-id/1337443

[7] Lakshmanan, R. (March 30, 2020). COVID-19: Hackers Begin Exploiting Zoom's Overnight Success to Spread Malware. The Hacker News. Accessed March 30, 2020 at: https://thehackernews.com/2020/03/zoom-video-coronavirus.html

[8] CISOMAG. (March 31, 2020). Cybercriminals Target Zoom Domains to Distribute Malware. CISOMAG. Accessed March 31, 2020 at: https://www.cisomag.com/cybercriminals-target-zoom-domains-to-distribute-malware/

[9] O'Donnell, L. (April 1, 2020). Two Zoom Zero-Day Flaws Uncovered. Threat Post. Accessed April 1, 2020 at: https://threatpost.com/two-zoom-zero-day-flaws-uncovered/154337/

[10] Yuan, E. (April, 1, 2020). A Message to Our Users. Zoom Blog. Accessed April 1, 2020 at: https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/

[11] Cisco. (March 4, 2020). Cisco Webex Network Recording Player and Cisco Webex Player Arbitrary Code Execution Vulnerabilities. Cisco. Accessed March 31, 2020 at: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200304-webex-player

[12] O'Donnell, D. (November 12, 2019). GoToMeeting is Found to be Potentially Susceptible to Hacking. Notebook Check. Accessed April 1, 2020 at: https://www.notebookcheck.net/GoToMeeting-is-found-to-be-potentially-susceptible-to-hacking.442684.0.html

[13] Gatlan, S. (March 30, 2020). FBI Warns of Ongoing Zoom-Bombing Attacks on Video Meetings. Bleeping Computer. Accessed March 30, 2020 at: https://www.bleepingcomputer.com/news/security/fbi-warns-of-ongoing-zoom-bombing-attacks-on-video-meetings/

[14] https://www.zdnet.com/article/the-internet-is-now-rife-with-places-where-you-can-organize-zoom-bombing-raids/

[15] Cimpanu, C. (April 2, 2020). The Internet is Now Rife with Places Where You Can Organize Zoom -Bombing Raids. ZDNet. Accessed April 2, 2020 at: https://www.cbsnews.com/news/zoom-bombing-calls-hacked-racial-slurs-pornography/

[16] Gal, O. (April, 1, 2020). The Facts Around Encryption for Meetings/Webinars. Zoom Blog. Accessed April 1, 2020 at: https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/

[17] Herscovici, O. (n.d.) Who's Zooming Who? Guidelines on How to Use Zoom Safely. Check Point Software Technologies Ltd. Accessed April 2, 2020 at: https://blog.checkpoint.com/2020/03/26/whos-zooming-who-guidelines-on-how-to-use-zoom-safely/

[18] Setera, K. (March 30, 2020). FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic. FBI Boston. Accessed March 30, 2020 at: https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic