SECURONIX™

Securonix Threat Research:

Securing Your Remote Workforce - Detecting Teleconferencing Tools Attacks in the Work-From-Home (WFH) World - Part 2

Oleg Kolesnikov, Kayzad Vanskuiwalla, Aditya TS
Securonix Threat Research Team
Last Updated: June 8, 2020

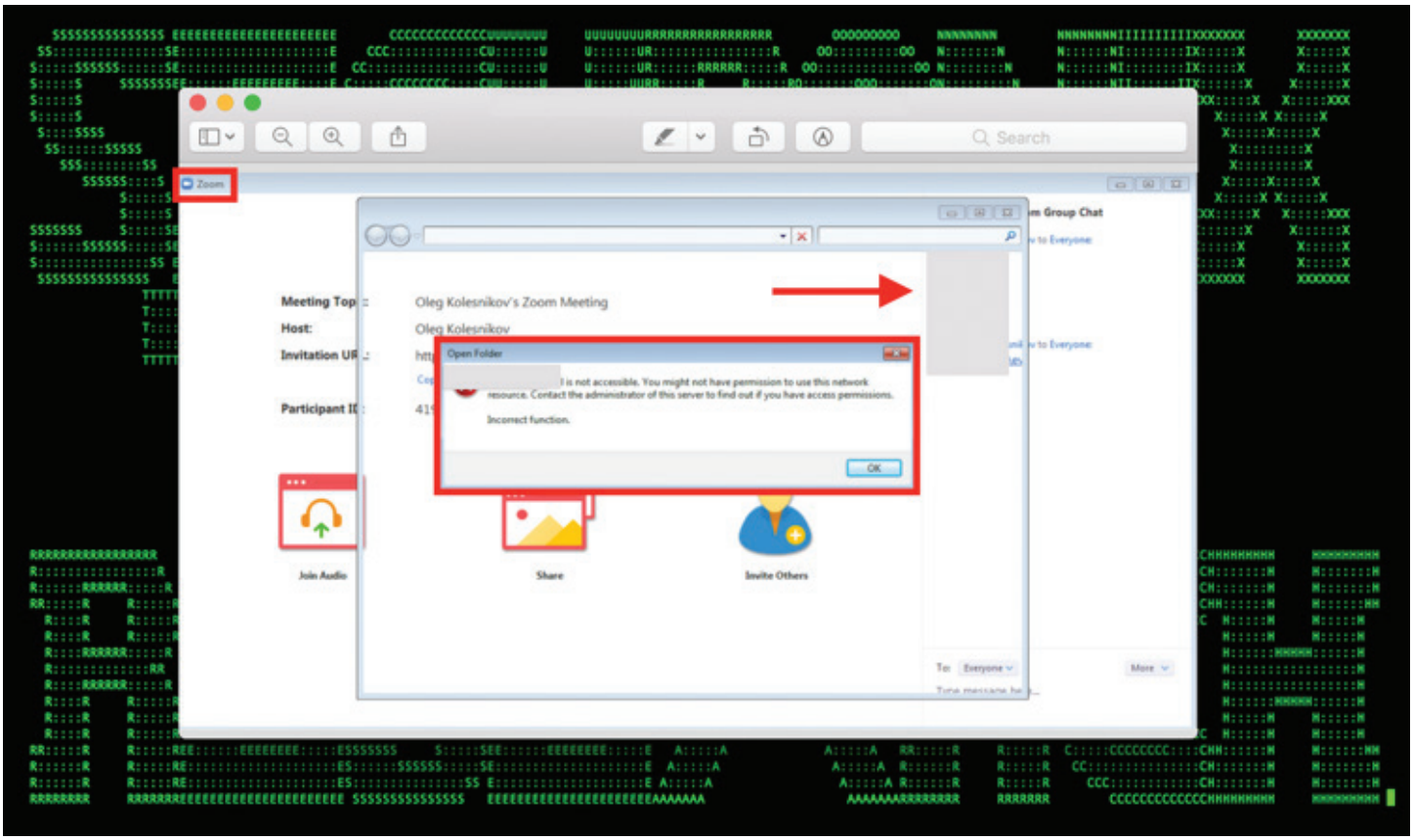

Figure 1: Remote Work/Teleconferencing Tools (Zoom) UNC Path Vulnerability Exploitation - I

The Securonix Threat Research team has recently been observing a number of new attacks/security issues reported involving different remote workforce teleconferencing applications (TA), including Zoom, Cisco Webex, and Microsoft Teams. Some examples of the attacks/exploits reported include Zoom UNC path exploits [1], Zoom and Webex phishing [6], new high-profile Zoom zero-day exploits [2], Cisco Webex remote code-execution (RCE) [3, 5] vulnerability, Microsoft Teams GIF subdomain/account takeover [7], and a number of other attacks/issues (see below).

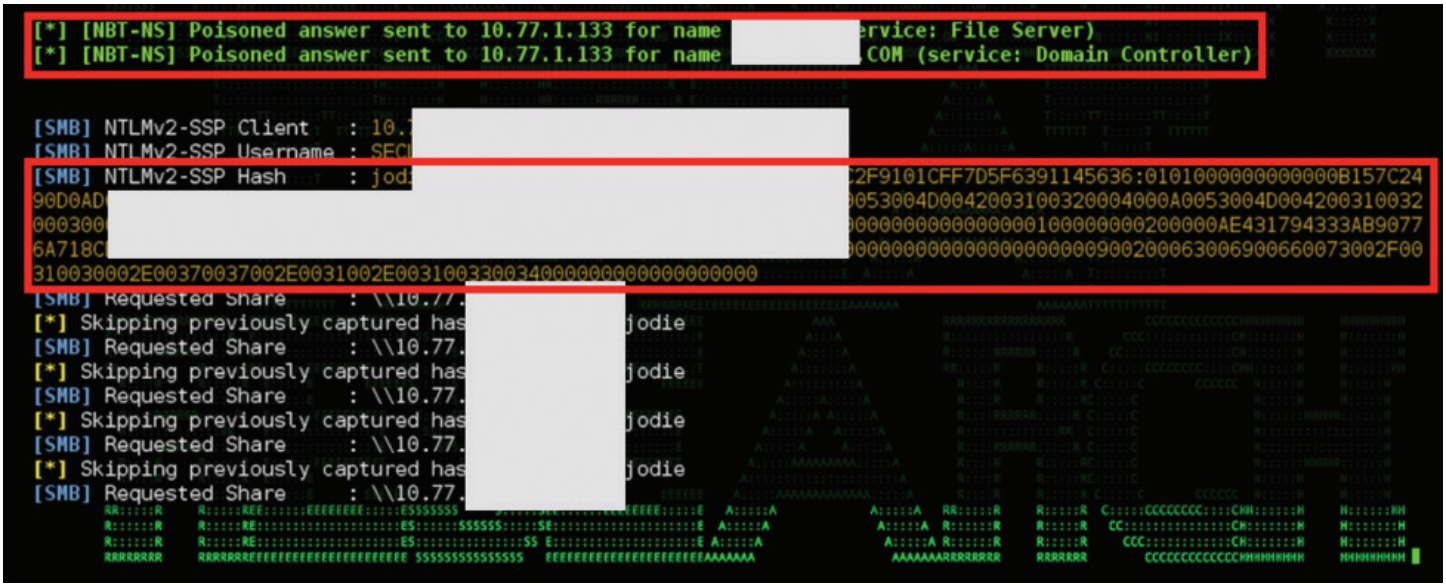

Figure 2: Remote Work/Teleconferencing Tools (Zoom) UNC Path Vulnerability Exploitation – II

The Securonix Threat Research Team has been actively investigating and closely monitoring these cyberattacks/security issues to help organizations better protect themselves in light of the global shift to remote workforce/teleconferencing work. Below is a summary of some of the key details with our recommendations, including some details about the recommended log/data sources and priority use cases that you can use to improve your remote workforce TA monitoring, including Zoom, Webex, and others.

Summary

1.1 What parts of your organization these recommendations might these be helpful for?

Security operations/SOC, IT operations, and insider threat teams.

1.2. What are some of the relevant cyberattack types to consider?

Some examples of the relevant attack vectors to consider from a security detection perspective include:

Figure 3: Example - Cracked Zoom Credentials for Sale

- TA credential dumps/combolists available from the dark web and leveraged by attackers in attempts to reuse the same compromised credentials across the organization. Example: Over 500k compromised Zoom accounts were sold on hacker forums (see https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/ and Figure 3).
- TA UNC exploits. Example: Zoom UNC exploit (see https://www.pcworld.com/article/3535373/report-hackers-can-steal-windows-credentials-via-links-in-zoom-chat.html).
- TA phishing/credential harvesting landing pages. Example: Cisco Webex and Zoom phishing (see https://www.proofpoint.com/us/threat-insight/post/remote-video-conferencing-themes-credential-theft-and-malware-threats).
- Fake TA/update. Example: Spoofed Cisco critical updates (see https://threatpost.com/cisco-critical-update-phishing-webex/154585/).
- Client-side RCE vulnerabilities including both known and zero-days. Example: Cisco Webex ARF/WRF RCE [3].
- Other TA exploits. Example: Microsoft Teams subdomain takeover-based credential stealing [7].

and others.

1.3 What are some of the recommended log/data sources to monitor in order to increase the chances of detecting these and other relevant cyberattack variants as part of remote workforce/WFH monitoring?

Some of the relevant log/data sources we recommend include:

- Strongly Recommended: Remote user monitoring log sources to detect attempts to leverage credentials related to compromised Zoom/Webex accounts (credential reuse), including proxy and VPN server logs. Examples include Zscaler, Pulse Secure*, Cisco, Citrix, Palo Alto Networks, Microsoft Office 365, and others.

Note: In order to enable the proper visibility, consider reviewing your VPN and proxy servers to ensure your teleconferencing traffic is routed through your corporate network.

- Strongly recommended: EDR/remote workforce workstation logs to detect attempts to target TA executables. Examples include Windows event logs, Carbon Black*, Tanium*, Sysmon, and others.
- Recommended: NTA/pcap metadata for your remote workforce traffic. Examples include Corelight, Zeek, and others.
- Optional: *Teleconferencing API polling logs to detect insecure use of teleconferencing apps. Examples include Zoom API, Webex API, and others.

Note: Due to how the logging is implemented in most of the TAs, including Zoom, the required details are typically only available through the API, so for this to work, you'll typically need to implement a polling app to obtain the logs such as call parameters, security settings used during calls (viz. password protection, and others). See https://github.com/cisco-ie/webex-api-client, https://github.com/phantomcyber/phantom-community-projects/tree/master/Apps/phzoom

Service	Basic Functionality	1 – E2E Encryption	2 – Testable Encryption	3 – MFA	4 – Invitation Controls	5 – Minimal 3rd Party Sharing	6 – Secure Deletion	7 – Public Source Code Shared	8 – Certified Service (FedRAMP / NIAP)
Amazon Chime™[i]	a, b, c, d, e	N	Y	Y	Y	N	Client – Y Server – Y	N	None
Cisco Webex®[ii]	a, b, c, d, e	Y[1]	Y	Y[1, 2]	Y[1]	Y	Client – Y Server – N[3]	N	FedRAMP
Dust	a	Y	N[3]	N	Y	N	Client – Y Server – Y	N	None
Google G Suite™[iii]	a, b, c, d, e	N	Y	Y[1]	Y[1, 4]	Y	Client – Y Server – Y[2]	N	FedRAMP
GoToMeeting®[iv]	a, b, c	Y[1]	Y	N	Y[1]	Y	Client – Y Server – N[3]	N	None
Jitsi Meet®[v]	a, b, c, d, e	Y[4]	Y	N	Y	N	Client – N[3] Server – N[3]	Y	None
Mattermost™[vi]	a, b, c, e	N	Y	Y[2]	Y[4]	N	Client – Y Server – N	Y	FedRAMP
Microsoft Teams®[vii]	a, b, c, d, e	Y[4]	Y	Y	Y	Y	Client – Y[1] Server – Y[1]	N	FedRAMP
Signal®[viii]	a, b, d	Y	Y	Y	Y	Y	Client – Y Server – Y	Y	None
Skype for Business™[ix]	a, b, c, d, e	Y[4]	Y	Y	Y	Y	Client – Y[1] Server – Y[1]	N	FedRAMP
Slack®[x]	a, b, c, d, e	N	Y	Y	Y	Y[1]	Client – Y[1] Server – Y[1]	N	FedRAMP
SMS Text	a, d	N	N	N	N	N	Client – Y Server – N	N	None
WhatsApp®[xi]	a, c, d	Y	Y	Y	Y	Y	Client – Y Server – Y	N	None
Wickr®[xii]	a, b, c, d, e	Y	Y	Y	Y	Y	Client – Y Server – Y	Y	FedRAMP
Zoom®[xiii]	a, b, c, d, e	Y[1, 4]	Y	Y[1]	Y	Y	Client – Y Server – N[3]	N	FedRAMP

Table of Assessments against Criteria

Legend: Y = Yes, N = No; (a) text chat, (b) voice conferencing, (c) video conferencing, (d) file sharing, (e) screen sharing.

Figure 4: National Security Assessment of the Collaboration Services for Telework (June 2020 Update)

2.1 Some Teleconferencing Tool Attack Examples - Highlights

- Some of the attacks observed involved attackers attempting to re-use the credentials of various TA that were made available as part of numerous malicious combolists/dumps on the dark web (see Figure 3). For instance, in one of the dumps, over 500k Zoom credentials were sold for about $1k [11].
- Another relevant attack vector observed is the Zoom UNC exploit that enables attackers to steal credentials and execute binaries from a local system using a specially crafted link. This can then be leveraged, e.g., to steal credential using variants of SMBRelay, running commands without a prompt from the Windows default download directory, etc. (see Figures 1 and 2).
- In addition to the exploits and vulnerabilities above, there are also reports of new high-profile $500k+ Zoom zero-day exploits up for sale online [2]. While the details of the new zero-day exploits are not publicly known at the moment, based on the limited details available, as well as some of the other critical RCEs we've analyzed that impact Zoom, there is a good chance that the new zero-day exploits involve some form of client-side attack vector similar to the original ZoomOpener 'zoom.com/attacker.zoom.us' or related modalities (this is to be confirmed), e.g. the original Zoom RCE URI) from a few months ago involved targeting a Zoom webserver component running locally: http://localhost:19421/launch?action=launch&domain=assetnotehackszoom.com/attacker.zoom.us&usv=66916&uuid=-7839939700717828646&t=1553838149048 [9, 10]. If this assumption is correct, while directly targeting the local webserver might no longer be feasible in some of the latest patched versions of Zoom, it might still be possible to exploit some other vectors associated with the opener/handler input processing functions. So, based on our experience, monitoring processes for different types of links used to initiate teleconferencing sessions can likely be helpful in proactively detecting many of the current and future variants of the attacks reported.
- In addition to Zoom, there has been reports of several other TA exploits and vulnerabilities, including Microsoft Teams and Webex. The Webex vulnerabilities involved client-side RCE in Cisco Webex using specially crafted ARF and WRF recording files [3, 5]. The Microsoft Teams exploit involved a form of a subdomain hijacking followed by stealing JWT cookies via a specially crafted chat message containing an image (no clicking needed). [7]
- While some of the software security issues have already been patched by the vendors in the latest versions of the TA products, for some of the issues above, attackers might still be able to perform malicious activity against some of the older versions of the client software, and also take advantage of some of the fundamental weaknesses and stolen credentials, so it is important to implement some of the recommended detection use cases (see below) including monitoring TA process and network activity.

- **Update June 8, 2020:** The National Security Agency has recently released a great security assessment providing some helpful insights related to the security of commercially available telework tools (see Figure 4). We strongly recommend that you consider the assessment as part of your defense-in-depth strategy in order to help better secure your WFH/remote workforce leveraging collaboration services [12].

3.1 Detection - Sample Spotter Search Queries

Please find below some examples of the trivial Spotter queries to assist with initial threat hunting/ identifying some possible attack vectors based on the details above.

Note: Because of the rapidly changing attack landscape, the recommendation is not to rely on static indicators of attack (IOA)/queries and to implement the use cases/predictive indicators for the best possible protection (see Section 3.2).

Sample Spotter Queries

Helping with initial threat hunting for rare target processes or domains accessed by TAs:

rg_functionality = “Endpoint Management Systems” AND baseeventid=3 AND (sourceprocessname=”Zoom.exe” OR sourceprocessname=”Zoominstaller.exe” OR sourceprocessname=”Teams.exe” OR sourceprocessname=”SkypeBackgroundHost.exe” OR sourceprocessname=”Skype Meetings App.exe” OR sourceprocessname=”SkypeApp.exe” OR sourceprocessname=”SkypeBridge.exe” OR sourceprocessname=”webexteams.msi” OR sourceprocessname=”webexapp.msi” OR sourceprocessname=”ptSrv.exe” OR sourceprocessname=”WEBEXA~1.EXE” OR sourceprocessname=”webexAppLauncher.exe” OR sourceprocessname=”webex.exe” OR sourceprocessname=”atmgr.exe” OR sourceprocessname=”wbxreport.exe” OR sourceprocessname=”webexmta.exe” OR sourceprocessname=”webexAppLauncherLatest.exe” OR sourceprocessname=”ptupdate.exe” OR sourceprocessname=”atcliun.exe” OR sourceprocessname=”ptOlEx.exe” OR sourceprocessname=”ptoneclk.exe” OR sourceprocessname=”g2mupdate.exe” OR sourceprocessname=”g2mupload.exe” OR sourceprocessname=”G2MInstaller.exe” OR sourceprocessname=”g2mcomm.exe” OR sourceprocessname=”g2mlauncher.exe” OR sourceprocessname=”g2mstart.exe”) AND (destinationhostname NOT CONTAINS “zoom.us” OR destinationhostname NOT CONTAINS “cloudfront.net” OR destinationhostname NOT CONTAINS “lync.com” OR destinationhostname NOT CONTAINS “teams.microsoft.com” OR destinationhostname NOT CONTAINS “teams.microsoft.com” OR destinationhostname NOT CONTAINS “msedge.net” OR destinationhostname NOT CONTAINS “compass-ssl.microsoft.com”

OR destinationhostname NOT CONTAINS “statics.teams.microsoft.com” OR destinationhostname NOT CONTAINS “compass-ssl.microsoft.com” OR destinationhostname NOT CONTAINS “hangouts.google.com” OR destinationhostname NOT CONTAINS “broadcast.skype.com” OR destinationhostname NOT CONTAINS “quicktips.skypeforbusiness.com” OR destinationhostname NOT CONTAINS “skypemaprdsitus.trafficmanager.net” OR destinationhostname NOT CONTAINS “skypeforbusiness.com” OR destinationhostname NOT CONTAINS “secure.skypeassets.com” OR destinationhostname NOT CONTAINS “skype.com”) | RARE limit=50 accountname sourceprocessname destinationprocessname destinationhostname

rg_functionality = “Endpoint Management Systems” AND baseeventid=3 AND (destinationprocessname=”Zoom.exe” OR destinationprocessname=”Zoominstaller.exe” OR destinationprocessname=”Teams.exe” OR destinationprocessname=”SkypeBackgroundHost.exe” OR destinationprocessname=”Skype Meetings App.exe” OR destinationprocessname=”SkypeApp.exe” OR destinationprocessname=”SkypeBridge.exe” OR destinationprocessname=”webexteams.msi” OR destinationprocessname=”webexapp.msi” OR destinationprocessname=”ptSrv.exe” OR destinationprocessname=”WEBEXA~1.EXE” OR destinationprocessname=”webexAppLauncher.exe” OR destinationprocessname=”webex.exe” OR destinationprocessname=”atmgr.exe” OR destinationprocessname=”wbxreport.exe” OR destinationprocessname=”webexmta.exe” OR destinationprocessname=”webexAppLauncherLatest.exe” OR destinationprocessname=”ptupdate.exe” OR destinationprocessname=”atcliun.exe” OR destinationprocessname=”ptOlEx.exe” OR destinationprocessname=”ptoneclk.exe” OR destinationprocessname=”g2mupdate.exe” OR destinationprocessname=”g2mupload.exe” OR destinationprocessname=”G2MInstaller.exe” OR destinationprocessname=”g2mcomm.exe” OR destinationprocessname=”g2mlauncher.exe” OR sourceprocessname=”g2mstart.exe”) AND (destinationhostname NOT CONTAINS “zoom.us” OR destinationhostname NOT CONTAINS “cloudfront.net” OR destinationhostname NOT CONTAINS “lync.com” OR destinationhostname NOT CONTAINS “teams.microsoft.com” OR destinationhostname NOT CONTAINS “teams.microsoft.com” OR destinationhostname NOT CONTAINS “msedge.net” OR destinationhostname NOT CONTAINS “compass-ssl.microsoft.com” OR destinationhostname NOT CONTAINS “statics.teams.microsoft.com” OR destinationhostname NOT CONTAINS “compass-ssl.microsoft.com” OR destinationhostname NOT CONTAINS “hangouts.google.com” OR destinationhostname NOT CONTAINS “broadcast.skype.com” OR destinationhostname NOT CONTAINS “quicktips.skypeforbusiness.com” OR destinationhostname NOT CONTAINS “skypemaprdsitus.trafficmanager.net” OR destinationhostname NOT CONTAINS “skypeforbusiness.com” OR destinationhostname NOT CONTAINS “secure.skypeassets.com” OR destinationhostname NOT CONTAINS “skype.com”) | RARE limit=50 accountname sourceprocessname destinationprocessname destinationhostname

Identifying unusual TA in use on your network (Note: Example based on Palo Alto Network Firewall): resourcegroupname = “Palo Alto Firewall” and deviceeventcategory = “internet-communications-and-telephony” | stats devicecustomstring3
Possible attempts at phishing from a freemail domain against multiple recipients via the same requesturl:
rg_functionality = Email / Email Security and (emailsenderdomain contains “gmail” or emailsenderdomain contains “yahoo” or emailsenderdomain contains “hotmail”) and requesturl not null and (requesturl CONTAINS “zoom.us” OR requesturl CONTAINS “cloudfront.net” OR requesturl CONTAINS “lync.com” OR requesturl CONTAINS “teams.microsoft.com” OR requesturl CONTAINS “teams.microsoft.com” OR requesturl CONTAINS “msedge.net” OR requesturl CONTAINS “compass-ssl.microsoft.com” OR requesturl CONTAINS “statics.teams.microsoft.com” OR requesturl CONTAINS “compass-ssl.microsoft.com” OR requesturl CONTAINS “hangouts.google.com” OR requesturl CONTAINS “broadcast.skype.com” OR requesturl CONTAINS “quicktips.skypeforbusiness.com” OR requesturl CONTAINS “skypemaprdsitus.trafficmanager.net” OR requesturl CONTAINS “skypeforbusiness.com” OR requesturl CONTAINS “secure.skypeassets.com” OR requesturl CONTAINS “skype.com”) | TOP limit=30 DISTINCT(emailsenders) requesturl

rg_functionality = Email / Email Security and (emailsenderdomain contains “gmail” or emailsenderdomain contains “yahoo” or emailsenderdomain contains “hotmail”) and requesturl not null and (requesturl CONTAINS “zoom.us” OR requesturl CONTAINS “cloudfront.net” OR requesturl CONTAINS “lync.com” OR requesturl CONTAINS “teams.microsoft.com” OR requesturl CONTAINS “teams.microsoft.com” OR requesturl CONTAINS “msedge.net” OR requesturl CONTAINS “compass-ssl.microsoft.com” OR requesturl CONTAINS “statics.teams.microsoft.com” OR requesturl CONTAINS “compass-ssl.microsoft.com” OR requesturl CONTAINS “hangouts.google.com” OR requesturl CONTAINS “broadcast.skype.com” OR requesturl CONTAINS “quicktips.skypeforbusiness.com” OR requesturl CONTAINS “skypemaprdsitus.trafficmanager.net” OR requesturl CONTAINS “skypeforbusiness.com” OR requesturl CONTAINS “secure.skypeassets.com” OR requesturl CONTAINS “skype.com”) | TOP limit=30 DISTINCT(emailsubject) requesturl

rg_functionality = Email / Email Security and (emailsenderdomain contains “gmail” or emailsenderdomain contains “yahoo” or emailsenderdomain contains “hotmail”) and requesturl not null and (requesturl CONTAINS “zoom.us” OR requesturl CONTAINS “cloudfront.net” OR requesturl CONTAINS “lync.com” OR requesturl CONTAINS “teams.microsoft.com” OR requesturl CONTAINS “teams.microsoft.com” OR requesturl CONTAINS “msedge.net” OR requesturl CONTAINS “compass-ssl.microsoft.com” OR requesturl CONTAINS “statics.teams.microsoft.com” OR requesturl CONTAINS “compass-ssl.microsoft.com” OR requesturl CONTAINS “hangouts.google.com” OR requesturl CONTAINS “broadcast.skype.com” OR requesturl CONTAINS “quicktips.skypeforbusiness.com” OR requesturl CONTAINS “skypemaprdsitus.trafficmanager.net” OR requesturl CONTAINS “skypeforbusiness.com” OR requesturl CONTAINS “secure.skypeassets.com” OR requesturl CONTAINS “skype.com”) | TOP limit=30 DISTINCT(emailrecipient) requesturl

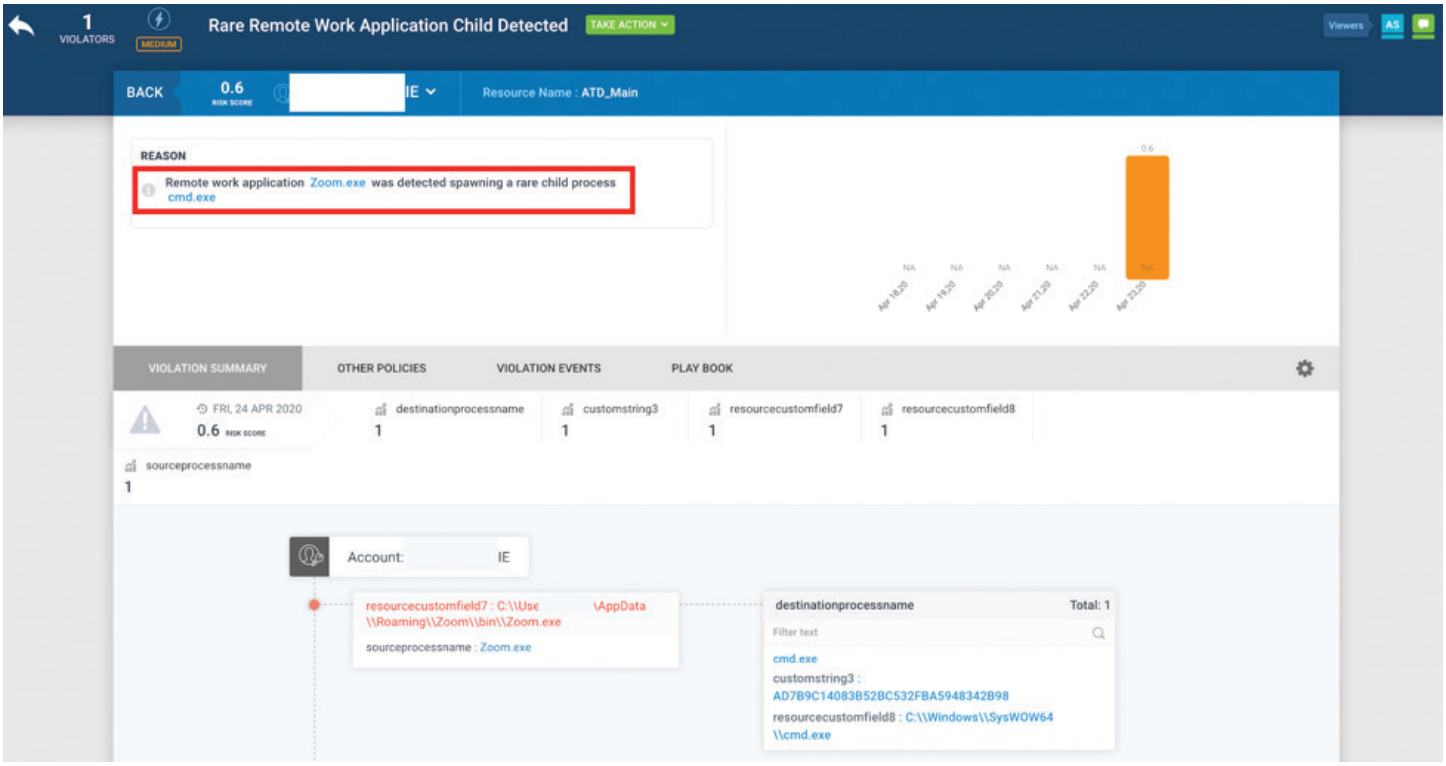

Figure 5: Remote Work/Teleconferencing Tools (Zoom) Attack Detection Example - I

3.2 Securonix Detection – Some Examples of Securonix Predictive Indicators

Here is a summary of some of the relevant use cases recommended to increase the chances of detecting and mitigating the teleconferencing app attacks observed early (high-level):

- Unusual processes spawned by teleconferencing apps.
- Unusual network connections used by teleconferencing apps.
- Potentially insecure teleconferencing app meeting configurations in use e.g. password-less (leverages teleconferencing app API logs).
- Potential compromised credential reuse users involved in suspicious account/authentication activity - geolocation, landspeed, MFA activity.
- Potential compromised credential reuse users involved in suspicious cloud activity - collaboration, cloud mail forwarding rule changes, anomalous aggregation of data from external sources, etc.

- Possible phishing URL redirects to rare unauthorized teleconferencing visual similarity domains from URL shorteners.
- Suspicious files created via phishing emails from TAs URLs via email.
- Unusual teleconferencing app use on a network.

and others

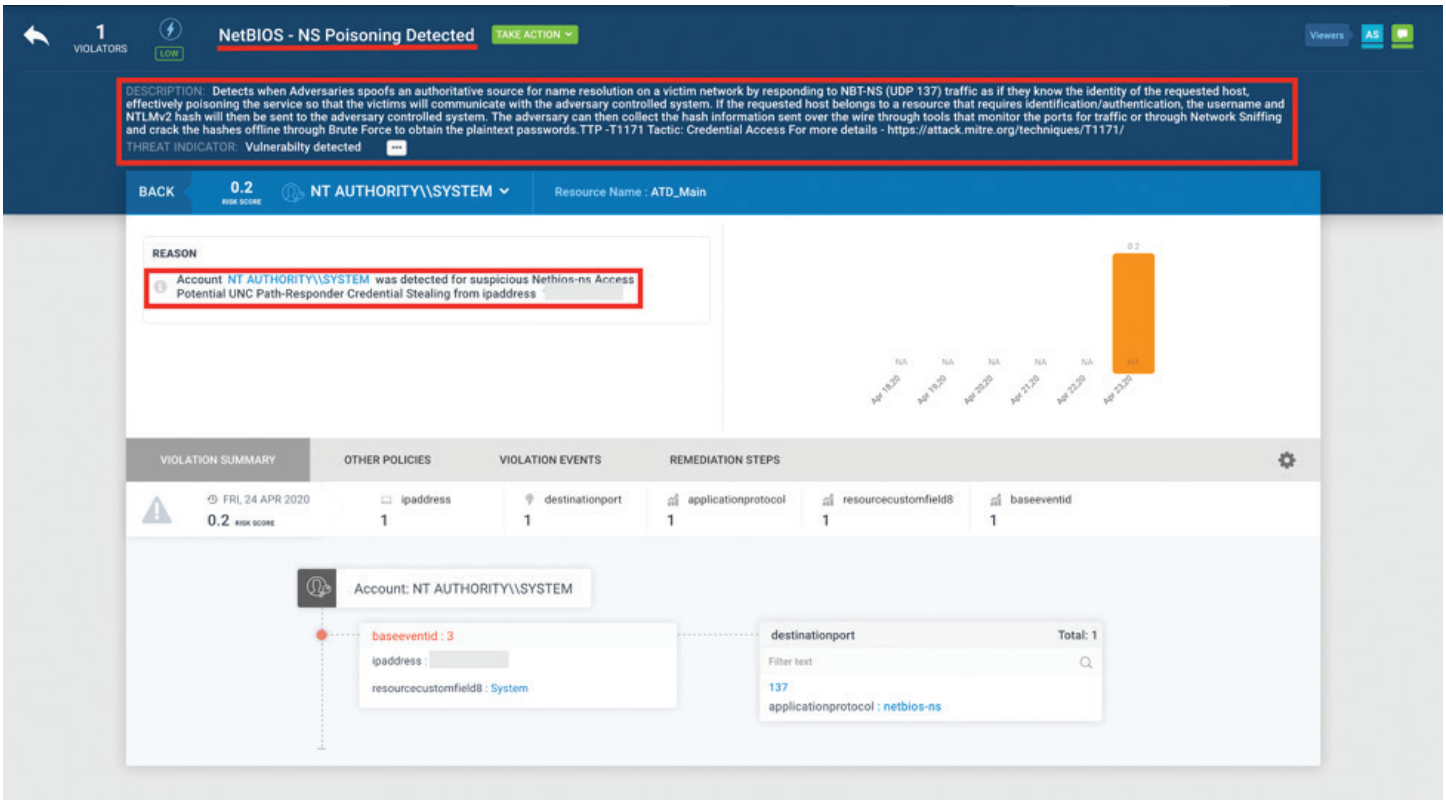

Figure 6: Remote Work/Teleconferencing Tools (Zoom) Attack Detection Example – II

Some examples of the detection of these real-world attacks in practice in the Securonix Labs are shown in Figures 5 and 6.

References

1. Mitch. Zoom UNC Path Injection Exploits. https://twitter.com/_g0dmode.
2. SecureworldExpo. Zoom 0-Day Exploits. https://www.secureworldexpo.com/industry-news/zoom-cybersecurity-zero-day-exploits
3. Cisco. Cisco Webex Player Security Advisory. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-player-Q7Rtgvby.
4. HackerOne. Slack HTTP Request Smuggling. https://hackerone.com/reports/737140
5. NIST. Cisco WebEx Player RCE. https://nvd.nist.gov/vuln/detail/CVE-2020-3127.
6. Proofpoint. Remote Video Conferencing-themed Credential Theft. https://www.proofpoint.com/us/threat-insight/post/remote-video-conferencing-themes-credential-theft-and-malware-threats
7. Omer Tsarfati. Beware of the GIF: Account Takeover Vulnerability in Microsoft Teams. https://www.cyberark.com/threat-research-blog/beware-of-the-gif-account-takeover-vulnerability-in-microsoft-teams/.
8. Patrick Wardle. Zoom Webcam Hijacking. https://objective-see.com/blog/blog_0x56.html
9. Assetnote. Zoom Zero Day Followup. https://blog.assetnote.io/bug-bounty/2019/07/17/rce-on-zoom/
10. Jonathan Leitschuh. Zoom Zero Day. https://medium.com/bugbountywriteup/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75c83f4ef5
11. Lawrence Abrams. Over 500,000 Zoom accounts sold on hacker forums, the dark web. https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/
12. NSA. Selecting and Safely Using Collaboration Services for Telework-Update. https://media.defense.gov/2020/Jun/03/2002310067/-1/-1/0/CSI-SELECTING-AND-USING-COLLABORATION-SERVICES-SECURELY-LONG-20200602.PDF.

About Securonix

The Securonix platform delivers positive security outcomes with zero infrastructure to manage. It provides analytics-driven next-generation SIEM, UEBA, and security data lake capabilities as a pure cloud solution, without needing to compromise.

Contact Securonix

www.securonix.com

info@securonix.com | (310) 641-1000

0620


SECURONIX™