Information Security
Class Project
Exploiting Zoom

Jake Derkowski & Katerina Moutafis

April 28, 2020

Contents

1 Problem Statement

Zoom is a web conferencing software that has risen exponentially in popularity since the COVID-19 pandemic. The newly found reliance upon Zoom from the majority of instituions and companies gave rise to a new and vulnerable target for hackers to exploit [1].

The vulnerability focused on in this deliverable is the UNC Path vulnerability. This vulnerability has already been discovered, and an attempt at a patch was released by Zoom as of April 2, 2020 [2]. This attack uses a Universal Naming Convention path, along with another vulnerability in the Windows Operating System. When a Windows client clicks on a UNC path, the client automatically tries to authenticate to the web server at that path, thus sending Windows login credentials. Zoom automatically rendered these links as clickable within the chat function of the application, and did nothing to stop a user from clicking a link sent to them by a malicious actor.

2 Implemented Solution

To replicate this exploit, a lab workstation was used along with 2 virtual machines running on VMWare Workstation 15 Pro. The Kali Linux VM was the attacker machine and the Windows 10 VM was the victim. It is important to note that the vulnerability outlined in this document is only a vulnerability for Windows Clients.

While running the tool, Responder, the attacker machine will send a malicious link to the victim via Zoom chat, and when the victim clicks on it, the attacker is able to capture the victim's Windows login credentials, since Windows clients will attempt to authenticate to an SMB server at the link. For sake of this experiment, Hashcat is used to crack the NTLMv2 password hash [3].

2.1 Technical Infomation

Machines & Operating Systems

	OS Version	RAM	Hard Drive/Storage
Host Machine	Windows 10 Pro v. 1909	80GB	500GB Hard Drive & 1TB SSD
Windows VM	Windows 10 Enterprise Evaluation v. 1909	3.73GB	60GB
Kali Linux VM	2020.1	2GB	80GB

Software & Versions:

VMWare Workstation 15 Pro	Version 15.5.2
Zoom for Windows	Version 4.6.8
Zoom for Linux	Version 3.5.361976.0301
Responder	Version 3.0.0.0
Wireshark	Version 3.2.1
Hashcat	Version 5.1.0

[1]

[1]Refer to Appendix figures 1 - 3 for more information.

3 Repeatable Methodology

These instructions are limited to the software versions that were used in this experiment. Installers for these versions will be provided for the means of replication.

3.1 Environment

The following procedure is the process taken in creating the environment that is to be used in performing this experiment.

1. Download Vmware 15 evaluation version:
   `https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html`
   (a) Go to the downloaded file
   (b) Run the installer, and use all default options
   (c) There will be a prompt for a product-key once installed, continue to the evalution version.
2. Download 7zip:
   `https://www.7-zip.org/download.html`
   (a) Run the 7-zip executable file
   (b) Use all of the default settings
3. Download Kali Linux 64-bit, version 2020.1 for VMware:
   `https://images.offensive-security.com/virtual-images/kali-linux-2020.1-vmware-amd64.7z`
4. Download the Windows 10 evaluation ISO
   `https://www.microsoft.com/en-us/software-download/windows10ISO`
   (a) Scroll down to find Windows 10, select `ISO` option, then provide the necesary personal information in order to continue with the installation.
   (b) once this file has been downloaded, we will open VMware to use the ISO in creating the virutal machine.

Kali Virutal Machine

1. Navaigate to where you downloaded the Kali Vmware file
2. The downloaded file with have the `7z` extension, and will need to be decompressed using the 7zip program. Note the directory in which it is extracted to.
3. Open Vmware15, in the menu toolbar:
   click `File` → `open...` → extracted Kali folder → open the file with the `.vmx` extension. You will now have a fully functional Kali virtual machine.
4. To begin using Kali, click the play button located near to top, left corner of the window.

Installing Zoom

1. install the Zoom from the attached folder – Zoom version 3.5.361976.0301
2. move the .deb file from your host machine to the virtual kali
3. type the following commands to install Zoom
   (a) `sudo apt update`
   (b) `sudo apt install gdebi -y`
   (c) `sudo gdebi-gtk`
4. in the gdebi GUI, File → Open → select the Zoom .deb file
5. Then click install this package
6. Zoom is now ready to be used on the Kali machine.

Windows 10 Virtual Machine

1. In the VMware menu bar: File → New Virtual Machine... → Custom(advanced) → next → I will install the operating system later → Select Microsoft Windows, Windows 10x64 → next → Select UEFI, then next → 2 processors, 2 cores → next → 2048 mb of memory, next → NAT network, next → use the default/recommended settings for the controller types → SCSI, for the virtual machine disk type → Create a new Virtual Disk → 60 Gb for disk size, split into multiple file → next → finish

2. We have now set the confiuration up for the virtual machine, now to install the machine, we can right-click on the machine's tab, go to settings → click CD/DVD. On the right hand side of the window, you will see an option for `ISO`, select this option and then niaviage to the Windows ISO file that has been downloaded.

3. To finish the installation, "Play" the guest machine from the menu bar, and then follow the installation wizard.

4. Once this has been completed, shut down the Windows guest, open the settings as we did earier, and navaigate to the CD/DVD again. Uncheck the boxes "Connected" and "Connect at power on"

5. You now have a fully functional Windows 10 evalution Virtual machine.

Installing Zoom for Windows

1. Move the given Zoom installer from the host to the Windows virtual machine

2. Double click the executable installer, making sure not to agree to any updates during the installation

3. Zoom is now ready to be used.

3.2 Attacks

Zoom Exploit

These are the procedural steps in conduction the Zoom exploit. It is important to verify that all correct software versions have been installed correctly.

1. Start up the Kali and Windows 10 virtual machine in Vmware, and open the Zoom application.
2. Begin a Zoom meeting on the Kali Linux machine, this will be the meeting host.
3. From the Windows machine, join the meeting this meeting using the meeting ID and the password displayed.
4. This invitation can be sent via email, copied, or sent as an URL
5. Admit the Target to the meeting from the waiting room
6. Open terminal on the Kali box
7. Run Responder program: `sudo responder -I eth0`
   (a) IP of the listener should be the Kali's IP (**Figure 4**)
8. Using the Zoom chat feature, establish communication between Host and Guest and create a dialogue.
9. When appropriate, send the UNC link to the Guest (**Figure 5)**
10. Guest clicks link, hash appears in terminal (**Figure 6**)
11. Save the hash value into a file

Password Attack

The success of the following procedure is dependant on the target's password strength. If the Target has a secure password (not found in popular wordlists) then more resources will be needed in order to crack. It is possible for the captured hash to be of a password that is too strong to crack.

1. Run the Kali virtual machine in Vmware
2. We must move the wordlist to the home directory in order to perform the password cracking.
3. Copy a wordlist to this directory using the following command:
   `sudo cp /usr/share/hashcat/wordlists/rockyou.txt.gz`
4. Decompress the wordlist: `gzip -d rockyou.txt.gz`
5. Execuate the hashcat program (**Figure 7**):
   `hashcat -m 5600 CapturedHash rockyou.txt --force`
6. Sit back and wait for the computer to crack
7. If hashcat exhausts it's resources before it crack the password, a new wordlist can be used for the attack.

[2]

[2]Special thanks to the Collision Inteligence and Lawerence Systems youtube channel (sources 3 & 4)

4 Results and Analysis

The grabbing of the username and password hash was successful in this environment and set up. After the victim clicks the link in the chat, the NTLMv2 username, password hash, and IP Address and Computer name appear in the terminal. Ability to retrieve this information is very dangerous, as it can be used to do further exploits. This experiment was actually run on a network we built for another class, and we ended up being able to add a user to the domain with administrative privileges.

Wireshark was also run during the experiment to see if any further information could be gathered.The following results are consistent with the results obtained in the video, Looking at Zoom Security with Wireshark and Talking Zoom Privacy [5].It is clear from the PCAP file that was obtained, that Zoom is using TLSv1.2, and it appears that the Linux host we collected the PCAP file from only interfaces with the Zoom servers prior to the attack, meaning we cannot obtain any information about IP addresses until the experimental attack occurs.When a client joins the meeting, a TLS Handshake occurs. After the handshake occurs, all data being passed through Zoom is encrypted, but the Client continues to only communicate with the Zoom server.

It is recommended to check for Zoom updates before each use, and always update when prompted. However, this is not a complete solution. The two following versions of Zoom did not patch this vulnerability. The first update disabled sending hyperlinks and all types of files via chat entirely, but the vulnerability remained. If the attacker was to simply get the target to search the payload link in a web browser their goal would still be achieved. The following version re-enabled file sharing using the chat function, but disabled UNC links appearing like hyperlinks. Instead, the full link would just be sent in plaintext and the vulnerability could still be exploited in the same way as the previous version.

It took Zoom several attempts before they were able to successfully patch this UNC vulnerability. On April 27th, 2020, Zoom released version 5.0.0 which addresses the main weaknesses that we have discussed in this report [8]. This new version has added AES encryption in all data transist and fixed the bugs within the chat feature,

plus securing and localizing each meeting to add security and limit unwanted users for gaining meeting information. Zoom's many updates shows that it is not giving up so easily and will continue to evolve as the attacks do.

5 Team Member Contribution

5.1 Jake Derkowski

- Initial research for the UNC path vulnerability and others
- Created exploit videos
- Set up testing environment
- Wrote Repeatable Methodology, Sources, & part of Results and Analysis sections of final report
- Collected Wireshark data
- Ran experiment during class Zoom meeting
- Embedded link in Image for testing patch
- Narrated slides 5-11 in final video
- Converted final writeup of project into LaTeX format, along with screenshots

5.2 Katerina Moutafis

- Initial research for the UNC path vulnerability and others
- Researched other forms of UNC path injections to attempt to break the patch
- Researched Zoom's E2E encryption for presentation
- Attempted UNC path traversal to break patch
- Attempted to send broken word documents to break patch
- Created slideshow
- Analyzed Wireshark data
- Wrote Problem Statement, Implemented Solution, & other half of Results and Analysis sections of final report

6 Appendix

Technical Information

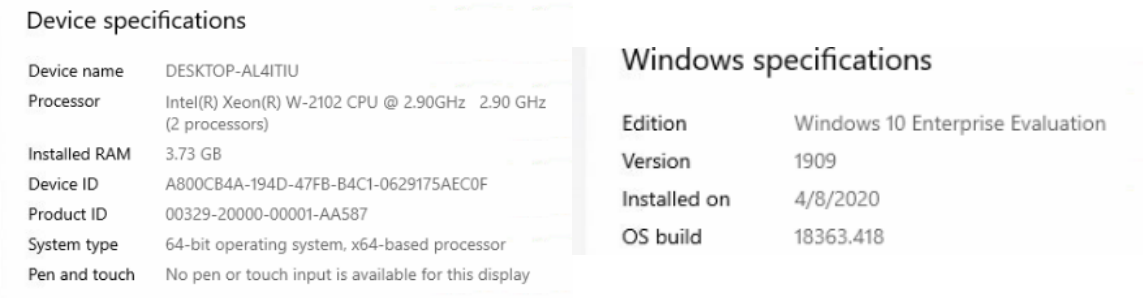


Figure 1: Windows 10 Specifications

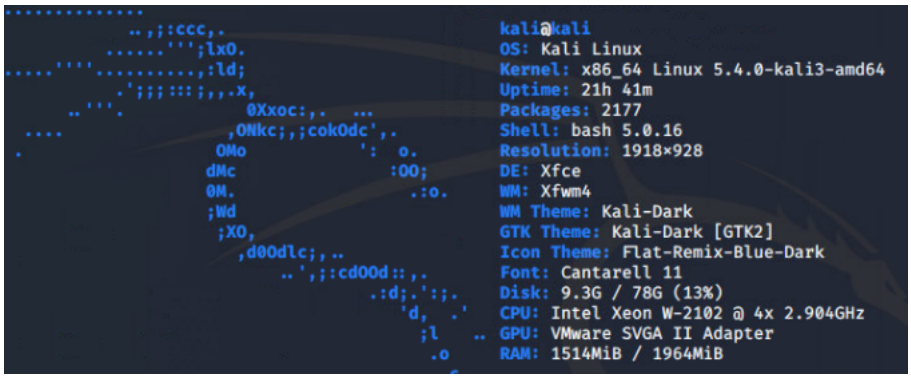
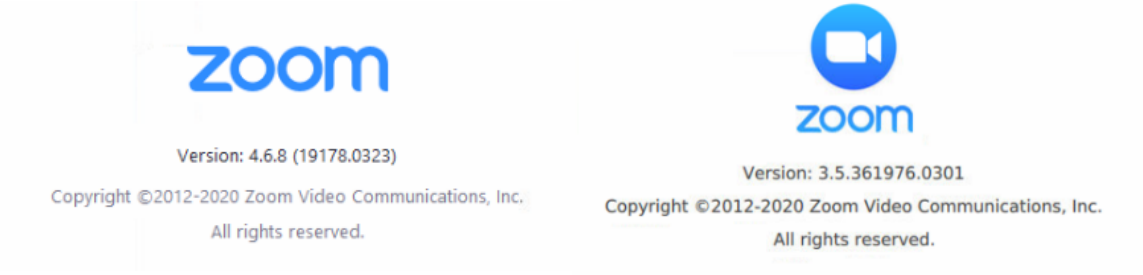


Figure 2: Kali system specifications



(a) Windows 10

(b) Kali 2020.1

Figure 3: Zoom Versions

Attack Screenshots

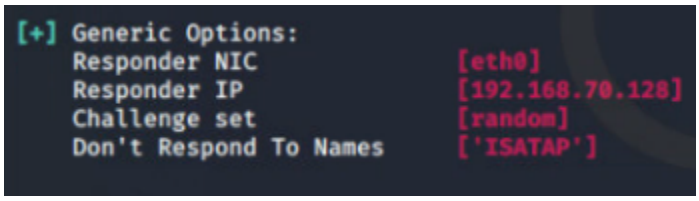


Figure 4: Responder IP address

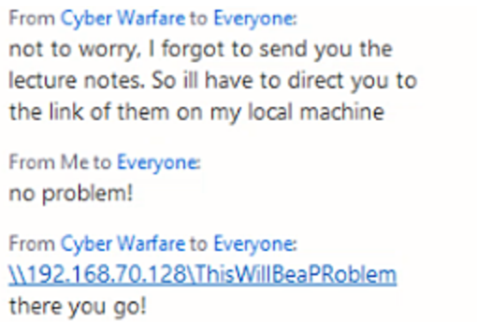


Figure 5: Guest perspective of chat

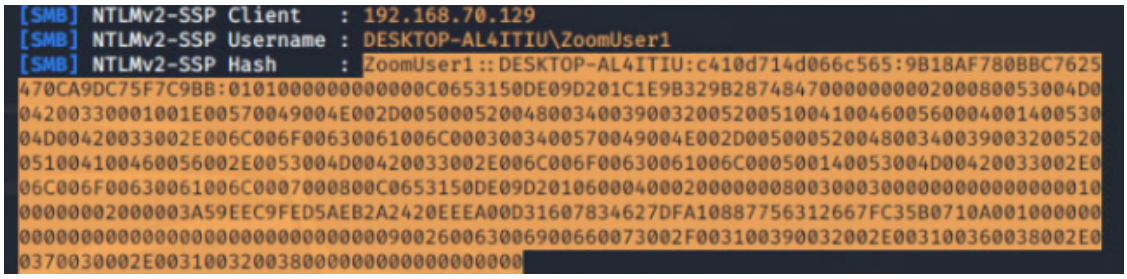


Figure 6: Responder captured hash successfully

Figure 7: Using hashcat

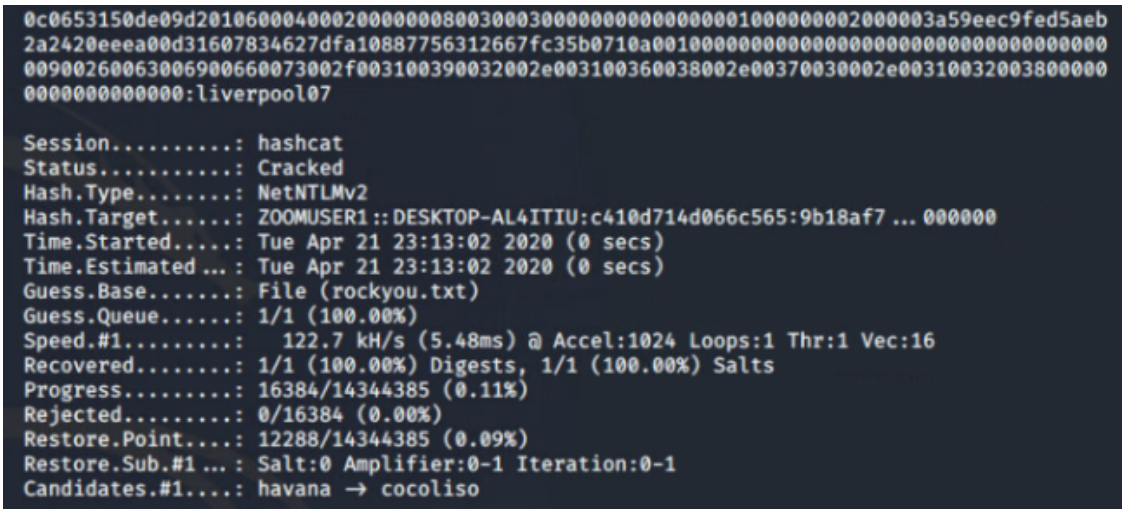


Figure 8: Password: **liverpool07**

7 Reference IEEE

[1] "How to Prevent Zoom-Bombing", PCMAG. [Online].
Available: https://www.pcmag.com/how-to/how-to-prevent-zoom-bombing.
[Accessed: 28-Apr-2020].

[2] K. Fosaaen, C. Wass, K. Robertson, and J. Jensen,
"10 Places to Stick Your UNC Path", NetSPI Blog, 16-Apr-2020. [Online].
Available: https://blog.netspi.com/10-places-to-stick-your-unc-path/#REDIR.
[Accessed: 27-Apr-2020].

[3] W. Hurer-Mackay, "LLMNR and NBT-NS Poisoning Using Responder",
4ARMED Cloud Security Professional Services, 06-Jun-2016. [Online].
Available: https://www.4armed.com/blog/llmnr-nbtns-poisoning-using-responder/.
[Accessed: 27-Apr-2020].

[4] From Zoom to Domain Controller (less than 15min).
Collision - Intelligence Labs, 2020.

[5] Looking at Zoom Security with Wireshark and Talking Zoom Privacy.
Lawrence Systems / PC Pickup, 2020

[6] portal.msrc.microsoft.com. [Online].
Available: https://portal.msrc.microsoft.com/en-US/security-guidance/
advisory/CVE-2020-0796. [Accessed: 27-Apr-2020].

[7] L. Abrams, "Zoom Lets Attackers Steal Windows Credentials, Run
Programs via UNC Links", BleepingComputer, 03-Apr-2020. [Online].
Available: https://www.bleepingcomputer.com/news/security/zoom-lets-
attackers-steal-windows-credentials-run-programs-via-unc-links/.
[Accessed: 23-Apr-2020].

[8] "New updates for Windows", Zoom Help Center. [Online].
Available: https://support.zoom.us/hc/en-us/articles/201361953-New-
updates-for-Windows.
[Accessed: 28-Apr-2020].