CYBERCONTAINMENT 1 -ZOOM : HERO OR VILLAIN ?-

Arch0nte

04/2020

Introduction: Zoom, what's that ? 2

1° Privacy issues 3

2° Security issues 5

Conclusion 6

Bibliography 7

What is Zoom?

Surprisingly, Zoom is not only a supervillain fighting against the Flash (https://en.wikipedia.org/wiki/The_Flash_(season_2)) but also a remote conferencing service company founded in 2009 which employed around 2.000 full time employees in 2019.

Figure 1: Not the Zoom we'll talk about

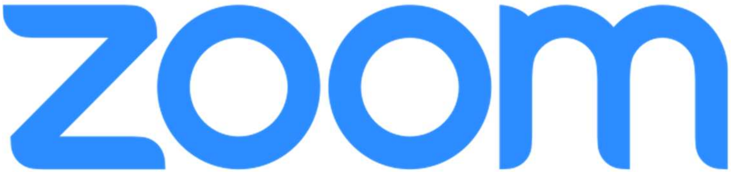

Figure 2: The Zoom we're going to talk about

Zoom came under the spotlight during the current coronavirus lockdown because of the necessity to develop a way to work remotely and a lot of companies but also governments [1] decided to opt for this solution.

With several offers depending on how many people you need to organize a conference with, how long it needs to be available, a cloud service and an actual end-user support, Zoom imposed itself as a must-use for companies and Universities in a matter of days. So, they are providing a service which is exactly what companies and governments need right now, in a situation of quasi-monopole. This brought a lot of scrutiny and, in a matter of days, some pretty serious problems were found by researchers. This is my summary of these problems plus my personal take ☺

Privacy Issues

Several issues emerged in less than 2 weeks, compiled by the EFF in an excellent blogpost [2].

Some quick definitions: the host of a conference is the organizer of that conference and the administrator is the person managing the Zoom server (either a Zoom employee if you use Zoom servers or, if you have your own implementation, a member of the staff of your company).

To sum up:

- The host of a conference can spy on the attendees while screen-sharing, seeing if their Zoom window is active or not
- Administrators have detailed reports compiled in dashboards of user activity including the time spent in conferences [3]
- If a call is recorded in Zoom, administrators can access its content
- For any call currently happening, an administrator of the local Zoom can join, without warning or permission
- For any meeting in progress, or that has happened, admins can access information about the operating system, IP address, location data and device information of each participant, in addition to the information you already gave them when you created your account (name, address, phone number, email, …).

These, are worth knowing before holding your top-secret business meeting, or worse, your National Emergency Meeting (like Mr. Johnson expertly did … I sincerely sympathize with the GCHQ folks trying to extinguish that bushfire ^^).

Another problem, is dubious marketing. Zoom pretends that it uses “end to end encryption” and that’s … not exactly true [4]. It’s more of a mid to mid encryption. End to end means that from your computer to your interlocutor’s computer, the entire feed is cyphered and no one can read it. In the case of Zoom, the feed is encrypted from one Zoom access to another. That means that from your computer to Zoom, the security is just a TLS encryption (the same as an https page) which means that someone on the outside can’t read that audio or video feed **but** Zoom can.

Let’s draw a sketch to show you better:

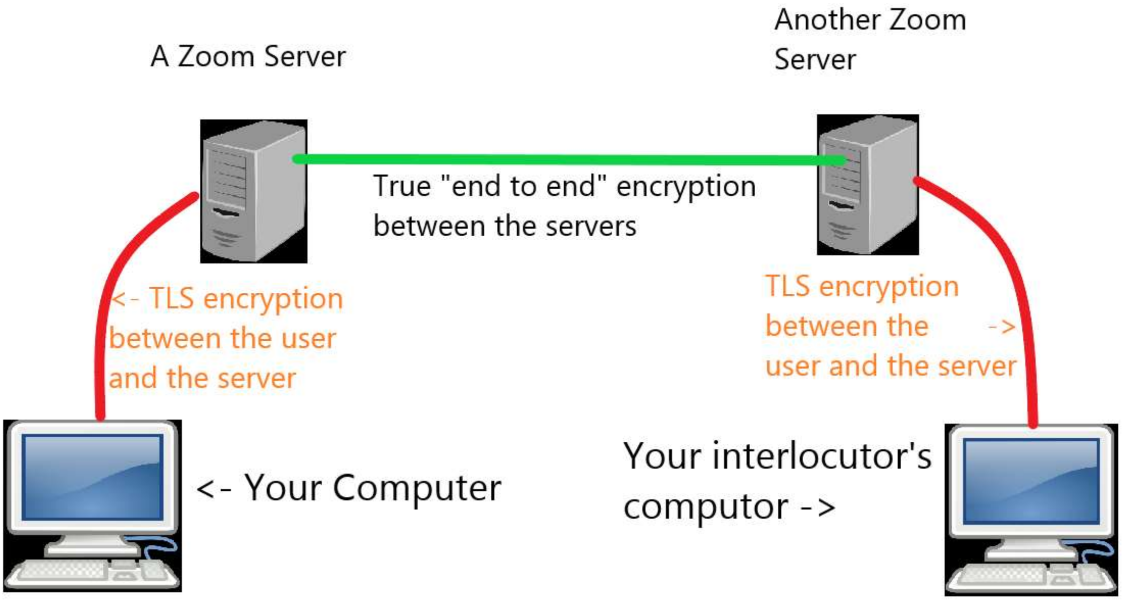
A Zoom Server
Another Zoom Server
True "end to end" encryption between the servers
<- TLS encryption between the user and the server
TLS encryption between the user and the server ->
<- Your Computer
Your interlocutor's computor ->

Figure 3: A wonderful sketch made on Paint3D which shows why I decided to study cybersecurity and not art.

In addition, up to the 28th of March, on its iOS version, Zoom gave away your personal information directly to our favourite Big Brother, Facebook [5]. These were of course added to the file of data that Facebook hoards like a dragon with compulsive hoarding.

On the point of Facebook tracking you and knowing more about you than even you do, you can act! Here are some tools I personally recommend for improved privacy ;)

- EFF's Privacy Badger: https://privacybadger.org/
- Mozilla's Facebook Container : https ://www.mozilla.org/fr/firefox/facebookcontainer/

If you want to know more about privacy online and defend your rights online, you can look at other projects and what you can do to help here : https://www.eff.org/

Now that you have enhanced your privacy, let's go back to Zoom's problems not linked to choices or design from their team but to security flaws ☺

Security Issues

Zoom has a history of security problems like this vulnerability [6] which allowed an attacker to force any user visiting the malicious website into a Zoom call with his camera active. I won't go into the technical details here because 1° this is a post for people of all technical levels ☺ 2° The article is already extremely good! I really recommend you read it thoroughly.

Another vulnerability, more recently, came in the form of the IDs of conference not being generated randomly which could allow attackers (really really motivated attackers ^^') to access a call if it wasn't protected by a password [7].

Fortunately, these have been patched but a new critical one emerged just last week!

Originating from a tweet by a member of the UK infosec community [8] and confirmed today by renowned hackers [9], this vulnerability is present in the Zoom clients for Windows and macOS and is called a 'UNC path injection'.

All the attacker needs to do is send a crafted unsafe url (a clickable link) and convince people to click on it in the Zoom conference chat. This link will be automatically converted by Zoom and Windows will attempt to connect to the address the attacker gave to download something from it.
In doing so, your username and password will be sent to the attacker's server!
Well, not exactly, your password will be 'hashed' this means that there is theoretically no way to find what your password is … If it's complex enough. If it's short, or too simple in its construction (something like "password" or "mypassword") the "hash" will be broken in a matter of seconds.

One of my next posts will certainly be about Hashing so if you want to know more about it, I'll soon write something ☺

On the bright side, Zoom has, up until now, been quite quick at patching security problems so we can only hope they keep that approach in the future, where, I am certain, more vulnerabilities are going to be discovered.

A quick update on the UNC path injection, it was patched during the 24h between the time I wrote this article and it's publication ^^

Conclusion

First of all, this is not a call to arms against Zoom or anything in that vein. Any software has his flaws and (almost) every company online has a dubious policy on privacy and data protection. I just want to inform people so they know about the technology they are using.

Then, if you have any returns or questions, feel free to email me at archonte@minet.net or to @me on Discord (you can find me via the HackademINT server).

Finally, I'd like to thank anyone who took the time to read my post ☺

Bibliography

[1]: https://www.infosecurity-magazine.com/news/uk-government-zoom-despite-mod/

[2]: https://www.eff.org/deeplinks/2020/03/what-you-should-know-about-online-tools-during-covid-19-crisis

[3]: https://www.youtube.com/watch?v=bGGms1ksUhQ

[5]: https://www.vice.com/en_us/article/z3b745/zoom-removes-code-that-sends-data-to-facebook

[4]: https://theintercept.com/2020/03/31/zoom-meeting-encryption/

[6]: https://medium.com/bugbountywriteup/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75c83f4ef5

[7]: https://blog.checkpoint.com/2020/01/28/check-point-research-finds-vulnerabilities-in-zoom-video-communications-inc/

[8]: https://twitter.com/_g0dmode/status/1242131019026874369

[9]: https://twitter.com/hackerfantastic/status/1245133371262619654

Images

Figure 1 : https://i.pinimg.com/236x/53/b4/6c/53b46c0daf7005e4df9c8e5d087f78dd.jpg

Figure 2 : https://commons.wikimedia.org/wiki/File:Zoom_Communications_Logo.svg

Figure 3 : Me, and my tremendous artistic skills xD