Date: April 5th, 2020
Reference: C-N-112

CERT-IL's Recommendation on how to use the "Zoom" application safely

Introduction

1. In light of the corona virus epidemic, many organizations turned to remote work methods (WFH).
2. Many of them uses collaboration on-line applications, the most popular on-line application is "Zoom".
3. This document contains recommendations for safer usage of the application.

Details

1. The extended usage of the "zoom" application made attackers keener to find methods of attacking it, resulting in exploiting Zoom users as the attack surface.
2. The attacks range between vandalism to denial of service, through attempts to attack the system's users and obtain their credentials or even install a malware on the users' computers.
3. There are different concerns regarding the software:
    a. The ability of attackers to barge into a conversation, uninvited and disrupt the whole conversation (Zoom Bombing).
    b. Reports of a vulnerability that allows the attacker to send a link to a remote server using SMB protocol. An activation of this link makes the operating system try and connect with the server, thus allowing the user's identification details, which are automatically moving to the server, to be caught by the attacker. In fact, this vulnerability is part of the operating

system's default behavior and it exists when a link is being sent through office etc. and it is not connected to the usage of "Zoom" specifically.

c. Reports regarding the encryption of the software and the degree of it. Reports were published that the software is not encrypted from end to end as promised by its manufactures. The company issued a clarification that only when all the parties of a conversation use updated client software **and the conversation is not recorded**, only then the entire conversation is encrypted. But if part of the users uses different interfaces, from a phone call to recording the conversation, the encryption is not end to end.

4. Other subjects that are not part of the software:
   a. Usage of domains that includes "zoom" to conduct phishing attacks etc.
   b. Usage of malicious software that imposes as a zoom client and that encourages the users to install it.

Recommendations

1. In order to avoid intruders from barging and disrupting a "zoom" conversation it is recommended to use the following steps:
   a. Publish the upcoming conversation with internal organization platforms and not public ones.
   b. Make sure the conversation password feature is enabled.
   c. Lock the conversation after all the relevant users joined, as to not allow anyone uninvited to join later.
2. In order to **prevent users' credentials from being leaked** the next steps are recommended:
   a. Avoiding opening any links that are suggested during the conversation by any user.
   b. Updating the windows OS client to version 4.6.9, that prevents opening such links. (a link is attached below)

   c. Setting the firewall to deny outbound traffic in port 445 (SMB).

3. In order to **avoid data leakage** from zoom meeting, the next steps are recommended:
   a. Limit the conversations only to updated clients that use computers or smart phones and do not record the conversation.
   b. Restrict the classification of the conversation, thus even if a leakage occurred, it will not be classified.
4. It is recommended to install the application only from **formal application stores** like Google play and App store or from the manufacturers' official site.
5. It is recommended to obtain information about the application only from **well-known and official sites.**

Sources

- https://zoom.us/security
- https://blog.zoom.us/wordpress/2020/03/27/best-practices-for-securingyour-
- virtual-classroom/
- https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf
- https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryptionfor-
- meetings-webinars/
- https://support.zoom.us/hc/en-us/articles/201361953-New-Updates-for-
- Windows

Best regards,

CERT-IL
team@cyber.gov.il