DATE OF BRIEF – 02 APRIL 2020

ZOOM APPLICATION SECURITY CONCERNS

The COVID-19 Pandemic outbreak has most countries going into lock down and many organisations have rapidly transitioned their workforce to remote working from home arrangements. This rapid shift has forced an increased reliance on remote meeting service providers such as Zoom and WebEx. Consequently, Zoom's widespread use, has now generated increased focus a on Zoom's security vulnerabilities, and privacy and data collection practices. Recently some very serious vulnerabilities have been identified within the Zoom platform that could allow an attacker remote exploit and take over users computer session and also Zoom meeting sessions.

In response, Zoom made some critical changes this week.

Identified Threat and Impact

Two new zero-day vulnerabilities have been discovered by security researchers in Zoom's macOS client version:

1. The web conferencing platform's vulnerabilities could give local, unprivileged attackers root privileges, and allow them to access a victims' microphone and camera.
2. When using the Zoom client, meeting participants can communicate with each other by sending text messages through a chat interface. The Zoom client is vulnerable to UNC path injection in the client's chat feature that could allow attackers to steal the Windows credentials of users who click on the link.

Also of concern is Zoom's privacy policy which stated it would collect, store, and share data with advertiser's, which could potentially include "the content contained in cloud recordings, instant messages, files and whiteboards" shared on the platform. This included videos and transcripts shared with third party vendors such as Google and Facebook.

Background and Key Findings

Zoom's privacy policy began to draw widespread attention more than a week ago for provisions about its storage and use of customer data. At the time, Zoom said it would collect, store, and share data with advertiser's that potentially includes "the content contained in cloud recordings, instant messages, files and whiteboards" shared on the platform. This included videos and transcripts.

Amid this scrutiny, Zoom made some critical changes to that policy this week. The company website now says in bold, italic lettering "Zoom does not sell customer content to anyone or use it for any advertising purposes,"— a welcome change in policy.

It is worth noting that the privacy policy itself, appears to only deal with the tip of the iceberg. An investigation by *Vice Motherboard* published Friday found the Zoom iOS app

Threat Assessment	
Threat Classification?	User session take over via malicious meeting invitation.
What is the risk rating of the threat?	High risk.
What is the target industry vertical?	Affects all industries using Zoom Video Conferencing.
How is the attack delivered?	Malicious meeting link via email or instant messages.
How to confirm a compromise?	Random users joining the meeting, controlling of your computer and webcam remotely.
What is the best action of remediation?	Links shared could be malicious. Action precautions before clicking links.
Are there any Indicators of Compromise available?	No
Protective measures?	Keep the Zoom meeting private with a password and only allow known users

HIGH	MEDIUM	LOW
TLP: RED ALERT	TLP: AMBER ALERT	TLP: GREEN ALERT

Mitigations

To exploit the discussed vulnerabilities, attackers need to trick the users to click on malicious links that pretend to be a Zoom meeting invite or general Zoom access link. Once the user clicks the link a payload within the link will exploit all relevant vulnerabilities and compromise the users' computer and/or account.

To mitigate against this, users of Zoom should be made aware that links can be shared within Zoom that could be malicious and to use their better judgement by only clicking on known or trusted links.

Conclusion

Zoom appears to have privacy concerns in terms of how they collect and distribute customer data and information collected as part of the subscription to their products and services. The system has had various security vulnerabilities and issues identified in the past which have not yet been completely resolved by the organisation and as a result, the company is now losing the confidence of its users.

Zoom appears to have lacked transparency and communication with its customers, users and the wider security industry by not building a more secure product. Due to this, there have been a few class-action lawsuits raised against the organisation to address the privacy and security issues highlighted in threat reports over the past few months.