PrivacyLok Whitepaper

Overview

If one were to objectively look at what has transpired over the last year and a half, believe it or not, there have been some things that have transpired very quickly as a result of COVID19. Probably one of the best examples of this is that of the Remote Workforce. While there is nothing new about this concept, the magnitude by which it has occurred can be deemed almost jaw breaking.

Many people believed that it would be at least four to five years down the road till we saw almost everybody Work From Home (WFH) at a near 99% level. But all of this happened in just a matter of three-month timespan.

With this considerable transition, remote employees had no choice other than to react positively to this new norm and embrace newer ways of engaging with colleagues, using Video Conferencing as the de facto standard to get daily job tasks done.

The Cyber Threats Posed By Video Conferencing

Because this has become the primary tool used by the Remote Workforce today, it has naturally become a top choice of prey for the Cyberattacker. Some of the most bombarded tools have been that of the Zoom platform, especially with its notorious "Zoombombing." But all of the other major Video Conferencing platforms have taken a hit, and varying tools such as Skype, WebEx, Microsoft Teams, etc. While they may not have necessarily been "bombed" like Zoom, they too fell victim to other kinds of security breaches, such as the following:

- The unauthorized access into Private Meetings:

  This typically occurs when a Cyberattacker breaks into a secure meeting and interferes with the flow of it. This is what "Zoombombing" is all about. In these instances, pornographic images or other offensive materials will be displayed, or the Cyberattacker will interject totally meaningless audio sounds and/or profane speech in efforts to sabotage the meeting completely. This is particularly the case in Virtual Classrooms.

- Breaking into the chat features:

  Even despite using the most robust of passwords, the Cyberattacker still has a way of breaking into the major Video Conferencing Platforms' chat sessions as just reviewed. When this happens, he or she then tries to impersonate a legitimate employee. Once this foothold has been gained, they will then attempt to launch a Phishing attack on the participants in the meeting by attaching malicious documents (typically those of the .XLS and .DOCX file formats), or sending links over directing the participants to a fake website.

- The heisting of login credentials:

  Once the Cyberattacker has broken through the Video Conferencing Platform's defense perimeters, one of the most prized possessions that the Cyberattacker will go after are the passwords of the company. These are often hijacked when they move laterally across the IT and Network Infrastructure, and once they have got their loot, they will then attempt to sell this on the Dark Web for a rather nice profit.

- Data Exfiltration:

  Apart from the hijacking of passwords, the vulnerabilities in these major Video Conferencing Platforms can also serve as a backdoor for the Cyberattacker to enter and steal other mission-critical data, such as the Personal Identifiable Information (PII) datasets of your employees and customers, theft of Intellectual Property, etc.

How To Overcome These Cyber Threats – The PrivacyLok

Now, there is a way to circumvent all of the Cyber Threats just described and even more. The engineering team at Strike Force Technologies, Inc. has created and designed a revolutionary new product called the "PrivacyLok." It offers protective mechanisms that are far more encompassing than what the other Video Conferencing Platforms can ever provide to its end users.

Here is what Privacy Lok currently has to offer:

1) Camera Locking:

   This has been of the most significant issues with Zoombombing. For example, from nowhere out of the blue, a Cyberattacker could take control over the camera on your wireless device and ruin your meeting. But with this feature, your camera is locked, and any transmitted images are thus encrypted.

2) Keyboard Protection:

   Malicious-based Keyloggers have always been a threat, but with chat mechanisms now in full swing, this problem has become even more proliferated. With this feature in Privacy Lok, any attempt to take over your keyboard will be detected and thwarted off.

3) Clipboard Protection:

   Generally speaking, whenever you copy an item (such as image, content, or any other form of replicable data), it is temporarily stored in a special section in the RAM (which is known as the "Clipboard") until you paste that item somewhere else. This is a functionality used very commonly, and the Cyberattacker is fully aware of this, especially when it comes to confidential information and data. However, this is a security issue that is still extremely overlooked. Yet, the Strike Force team has realized the grave importance of protecting this and has developed a particular procedure for encrypting that information and data until it is pasted. As a result, if the Cyberattacker were to hijack the RAM, there is not much that they can do with the content because of the garbled state that it is in.

4) Microphone Protection:

   With this, any conversations you are having with your co-workers via Video Conferencing remains private and secure.

5) Audio Input/Output Locking:

   As mentioned before in this whitepaper, with Zoombombing, the Cyberattacker can all of a sudden join a Private Meeting and make remarks which are offensive by nature. But with the specific locking mechanism available in Privacy Lok, your audio streams are completely protected, thus avoiding this kind of threat vector from even occurring at all.

6) Anti-Screen Scraping:

   Once again, with Zoombombing, if a Cyberattacker can break through your Video Conferencing Platform, just about anything derogatory can be displayed in the middle of your meeting by taking advantage of the screen sharing functionality. Or worst yet, they could take screenshots of any private information and data that you are sharing. But with this Anti Scraping feature available in PrivacyLok, this Cyber Threat becomes almost nonexistent.

7) Anti-Click Jacking:

   One of the biggest Cyber threats that has evolved since COVID19 is that of covert, malicious objects that are placed onto legitimate and authentic websites. The root cause of this is typically that of poor source code and/or API security. With this particular functionality, you are alerted if any of these objects exist before you click anything on the website that you are visiting.

What Is The Next Step?

Obviously, it will be to protect whatever Video Conferencing Platform that you are using with the PrivacyLok. This solution is very affordable, particularly for the SMB. It only costs $39.95 per year with an annual subscription, with special pricing available for larger businesses.

For more information, please contact us at: www.privacylok.com.