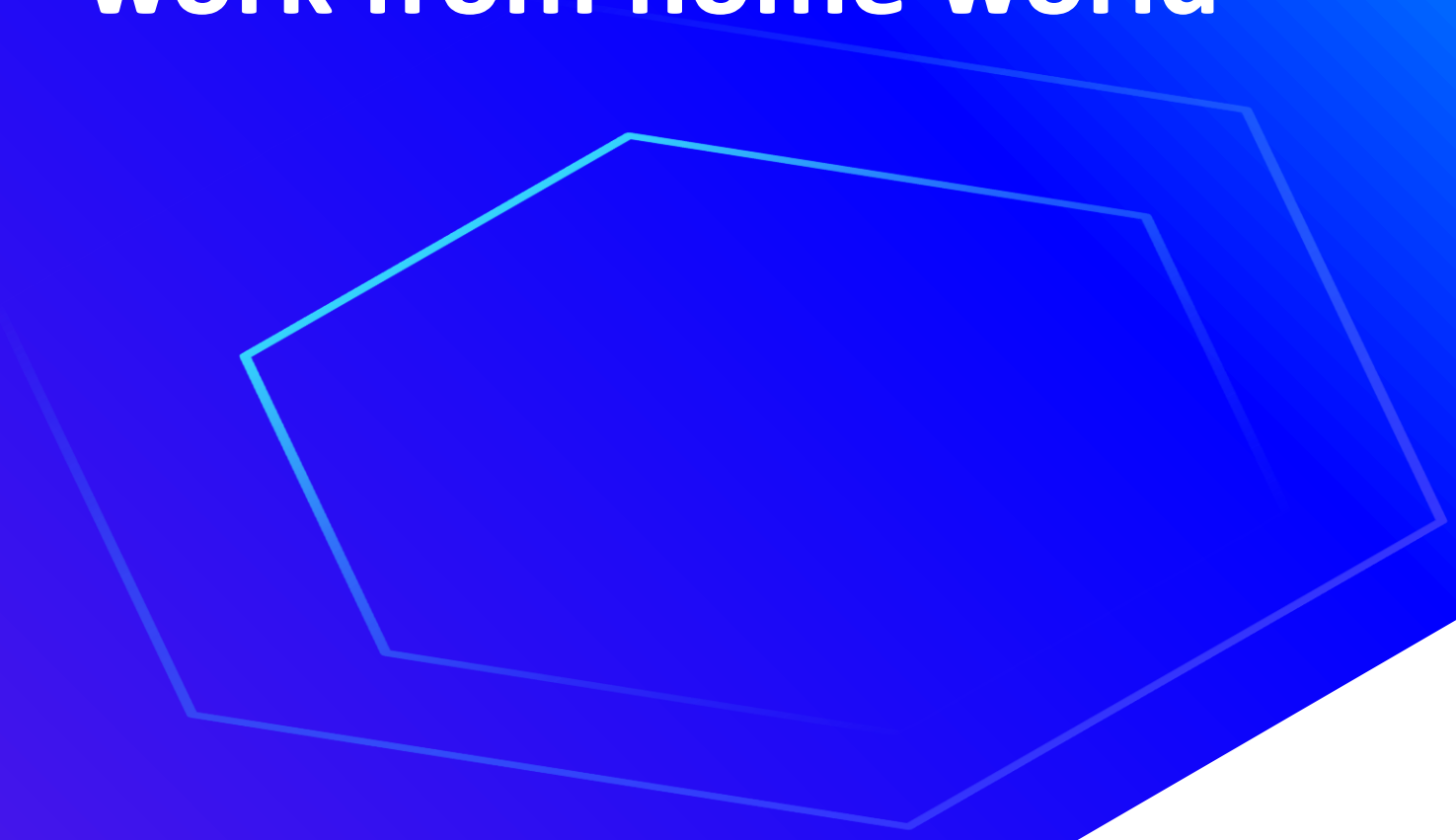
Security vulnerabilities in the new Enterprise **work from home world**



CybrHawk
Transforming Cybersecurity

CybrHawk.com

Table of contents

INTRODUCTION

As the number of remote employees continues to exponentially increase, collaboration applications such as Slack, Zoom, Microsoft Teams, and WebEx grow in importance. Zoom, for example, added 2.2 million monthly active users in January **and February 2020**, **dwarfing their entire monthly** active user number from all of 2019. Microsoft Teams added 44 million daily active users as of March 18, with Slack adding 7,000 paying customers from February to March 18 of 2020.

This growth in user counts is stress-testing digital **such as increased outages and reduced fidelity** from massive user growth as more enterprises tell their employees to work from home.

collaboration applications—many of which were not originally crafted to handle such an enormous spike in usage over such a short time frame. Practically every communication tool faces new problems.

On top of increased usage, these applications must also now contend with a higher risk of vulnerabilities being exploited.

Threat actors often decide to investigate applications for exploits based on which targets would be most **profitable, investing extensive amounts of time** into vulnerability research to increase their **ROI**. **Digital collaboration tools fulfill both these** criteria, largely because many of these software companies are not structured to quickly patch zero-days or other security vulnerabilities.

Contrast this with Microsoft Office and Adobe Flash—applications that have been targeted for the past 20 years—two vendors that have veritable armies of developers focused on patching vulnerabilities.

Threat actors have already taken steps to exploit the weak security posture of collaboration applications. While "**Zoombombing**" makes the news, the more dangerous risk is that hackers gain footholds through phishing attacks designed to look like Zoom invitations, an info-stealer to grab all Zoom users in a domain, a **UNC path injection** that allows for passwords to be stolen, or even scraping all information through an unpatched vulnerability. Slack has also been the subject of several CVEs, and it's incredibly easy for an attacker **to exfiltrate all a Slack user's workspaces, chat messages, files, and history once they get into a Device.**

GROWING MARKET SHARE = GROWING TARGET

Collaboration application spending has skyrocketed over the past few years, reaching $31 billion in 2019 and predicted to exceed $48 billion by 2024. Within this category are applications focused on **file sharing, enterprise social networks, and team collaboration like Slack, Zoom, WebEx, and Microsoft Teams.**

Team collaboration apps allow distributed workforces to collaborate through chat and video conferencing, breaking down communication barriers and empowering workers located around the world to communicate in real or near-real time. These applications have seen explosive growth in the first few months of 2020 with the COVID-19 pandemic driving hundreds of thousands of knowledge workers to become remote employees practically overnight.

This growing market share is a double-edged sword. As more people log into collaboration applications, more threat actors seek to use these apps to exfiltrate confidential data or steal payment information. This makes collaboration applications such as Zoom and Slack higher security risks than they have historically been.

There are a few reasons behind this higher risk, including a lack of focus on application security, an increased risk of browser-based attacks, and a higher possibility of success with social engineering attacks.

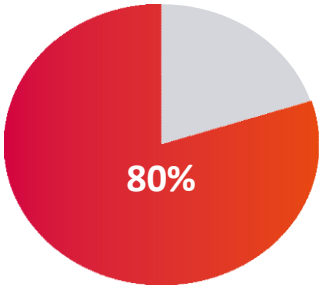
Zoom added 2.2 million **users in the first two** months of 2020

Source: CNBC

COLLABORATION APPS CAN'T PATCH VULNERABILITIES FAST ENOUGH

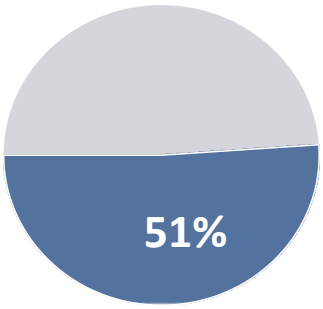
Adversaries only spend their time building exploits for tools that are widely used so they can get the best ROI for their efforts. Threat actors are by and large financially motivated—except in the case of rare, targeted, nation-state type attacks—which means that they mostly will not seek out exploits for applications that do not have a broad user base. They are instead targeting the largest pool of ways to break into an enterprise, which is why they have historically weaponized Microsoft Word documents and Adobe PDF files.

This common targeting of Word and PDF files means that Microsoft and Adobe (and vendors of similar size) have literal armies of security experts patching holes in their software products. They have these security personnel because they have gone through substantial pain over the last 10 to 20 years from threat actors exploiting vulnerabilities that it is vital for these vendors to release patches as fast as possible. As a result, Microsoft and Adobe applications have been hardened against many exploits.



of successful attacks are new or unknown zero days

Source: Ponemon Institute



of companies claim they have a cybersecurity skills shortage

Source: CSO Online

Collaboration applications are not yet structured in the same way as Adobe and Microsoft with regards to patching software vulnerabilities. Part of the problem is that these applications have not been targeted yet because they have not reached critical mass in terms of users to be attractive from an ROI perspective. The other issue is that there is a severe shortage of security experts worldwide, and in addition there are not enough tools to **quickly and efficiently find the flaws in collaboration** applications (such as fuzzers).

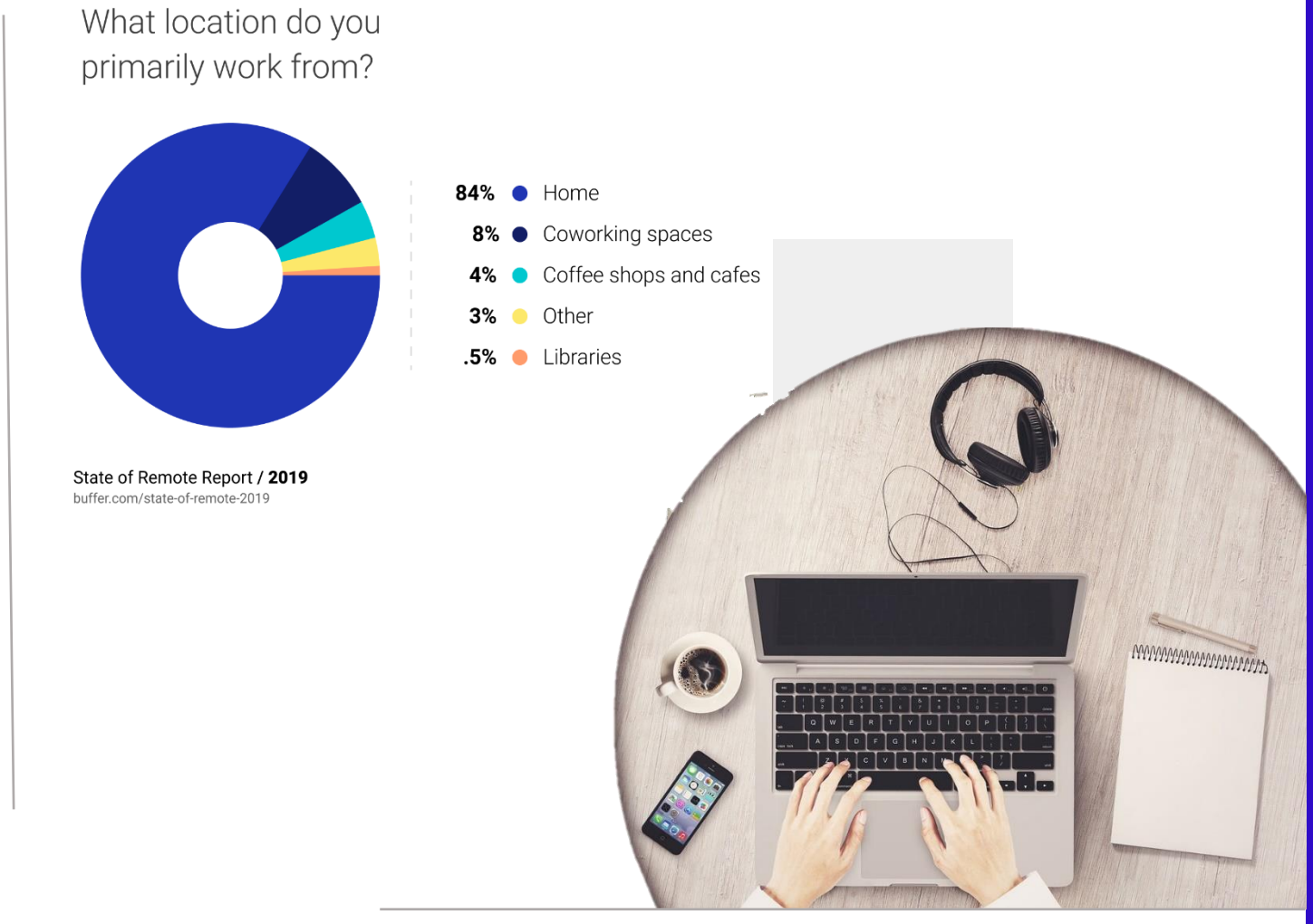
Exploiting these tools can lead to RCE (remote code execution), which basically allows the adversary to run their malicious code on the machine that is running the collaboration application. In the case of Slack, there was a recent exploit that allowed the adversary to completely exfiltrate messages, contact lists, and every other form of data tied to the messaging application. Zoom in the last two weeks had several zero days reported; including one where a UNC path could expose Windows passwords and one that enabled attackers to install malware on infected machines.

HIGHER RISK OF BROWSER-BASED ATTACKS

Coupled with risky patching processes is a much higher risk of **browser-based attacks**, especially for applications that are accessible via a browser such as WebEx, Go to Meeting, and Zoom. Video conferencing and collaboration tools such as these require their own code to be loaded into the browser to support their functionality. As these application vendors are not yet heavily invested in secure coding, they increase the browser's attack surface. This can result in an attacker abusing the loaded code to eventually remotely execute code on behalf of the browser.

The high risk of vulnerability via the web browser should give any IT security professional pause.

Browser attacks such as drive-by downloads and browser-based phishing are a high risk with collaboration apps. This is especially true given how exposed many of these applications are to threat actors, and the increase in work from home employees.



Countering the Security Risk of Collaboration Applications

INCREASED RISK OF SUCCESSFUL SOCIAL ENGINEERING ATTACKS

Phishing emails are the most common malware delivery mechanism in use today. Collaboration applications, especially messaging tools such as Slack and Microsoft Teams, provide new avenues for phishing messages to be delivered and acted upon. Video conferencing apps especially run the risk of being used for social engineering. With collaboration tools often lacking basic security protocols, such as two-factor authentication for password protection and not fully encrypting traffic in certain cases, social engineering risks are dramatically higher. A successful attack in this context could result

in credential stealing on a remote employee's machine and, if the user is an admin, then the attacker could further their goals in a more streamlined manner.

1,700 domains containing the word "Zoom" have been created since January 2020

-Check Point Research

How to Reduce the Security Breach of Corporate remote users

Collaboration applications are not going away any time soon. As more people work from home, and do so more frequently, these applications will grow in importance and add even more users than before. This presages a corresponding increase in security risk, which CISOs and other security executives need to account for.

CybrHawk solutions to prevent security risks:

Cloud Security: To provide stability and protection to cloud based resources, with multiple layers of protection. Whether in a private cloud security, high availability, data security, and regulatory compliance.

O365 & GSuite Monitoring: CybrHawk detects and responds to advanced threats targeting your Office 365 and GSuite SaaS application and helps you comply with regulatory mandates like PCI, HIPAA, and SOX. You will be able to get 50+ alerting rules upon setup, Comprehensive monitoring, alerting rules for user and access authentication, resource sharing, mail and file operations, mobile device administration, and detailed reporting.

Dark Web Monitoring: Ensure your Digital Security covers the deep dark roots of internet, CybrHawk Dark Web Monitoring allows you to Auto Hunt for Security Threat, Collet and Index Data, Search, Analyze and Visualize, and get Comprehensive Reports.

Memory & Process Injection Detection: Harpoon Security defense against changes to memory and process injection by blocking malware and ransomware before they launch an attack.

CONCLUSION

For all their importance in the enterprise, the reality is that collaboration applications are often not ready for prime time. Slack, Zoom, Microsoft Teams, WebEx, GoToMeeting, and other collaboration tools all have their security vulnerabilities and will continue to be exploited now and in the future. These are often consumer- grade applications that are ill-suited to the vast number of corporate entities currently using them for critical communications.

These applications need to be protected more **effectively against the worst cyberattacks. This is what CybrHawk excels at**, including automatic hardening of remote endpoints that enables work from home employees to access the collaboration apps they need to do their work.

Contact us for more information!

Email: sales@cybrhawk.com
Tel.: 954-669-1960
Web: www.cybrhawk.com

CybrHawk
Transforming Cybersecurity