AVANAN

THE MICROSOFT TEAMS SECURITY REPORT

Table Of Contents

The Microsoft Teams Security Report

What you need to know when securing Microsoft Teams for usage in an enterprise environment

Background: Microsoft Teams is the Business App of Choice. Hackers Know This.

As firms and workers across the globe went remote, it was Microsoft Teams that saw the bulk of growth for chat and collaboration.

The growth has been exponential and stunning. Teams usage in December 2020 is estimated to be 115 million daily users, growing from 32 million in early March 2020. After what appeared to be an early pandemic rivalry with Slack, Teams quickly became the de-facto communication and collaboration app for anyone using Office 365. Now, 91 of the U.S.'s 100 largest companies use Teams. Twenty organizations with more than 100,000 users use it, with major organizations like Coca-Cola, Pfizer and Accenture, to name a few.

The success of Microsoft Teams has also made it ripe for hackers. In fact, as this year of explosive growth comes to an end, we've begun to see and learn how hackers are targeting this platform for data, personal and corporate information, and as a jumping-off point for other attacks.

For this whitepaper, Avanan analyzed nearly 200 enterprise customers for two months. In doing so, we were able to uncover current hacking activities and trends in Teams, as well as assess the overall cybersecurity risk involved in using the service.

- Microsoft Teams has quickly become the go-to application for remote work, accelerating dramatically in usage over the last year
- As Teams is still relatively new, much is unknown about how it operates and how hackers will approach it
- Avanan worked with Microsoft to apply the Avanan layers of security on top of Teams, and analyzed close to 200 enterprise customers over two months to uncover current hacking activities in Microsoft Teams and the cybersecurity risk involved in its usage
- Despite inherent trust, hacking activity in Teams is apparent
- Teams attackers also appear to act differently than email-based attacks
- Malware, impersonation and east-west attacks are the most popular attack types
- Recommendation: Businesses that use Teams need to secure it from DLP, malicious files and links
- Recommendation: CISOs should educate their end-users on secure usage of Teams. They should communicate the policy and provide end-user training on security related matters like inviting external users, configuration when creating a new channel, and more

As business continues to expand from email to collaboration and chat apps, it is incumbent upon firms to secure this platform in the same way they do email and to place the same attention into securing collaboration and chat.

In this whitepaper, we will discuss the inherent vulnerabilities within Teams; how hackers have begun to exploit these vulnerabilities; the great unknowns of a platform that remains in its infancy; and how you can take action to protect yourself and your organization from Teams becoming a liability.

Part 1: Vulnerabilities and Attacks Found in Microsoft Teams

The first, and perhaps most important, thing to know about Microsoft Teams is that, by default, it is not protected. Unlike Exchange Online that comes with EOP as a default layer, Teams does not have any default security protections. That means that everything you share, from files to company data, general and personal information—it all goes unscanned. Only if you purchase an E5 license or if you add the ATP (now renamed as Microsoft Defender for Office 365), are the following scanning capabilities are added for Teams:

- Safe attachments in Teams
- Safe Links in Teams

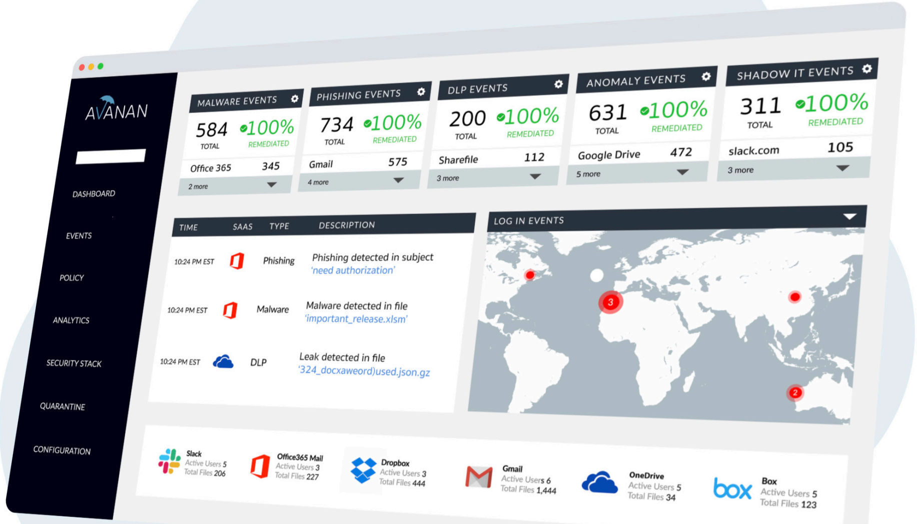
Threat 1: Cross-Site Scripting Vulnerability

When it comes to Data Loss Prevention in Teams, customers are also required to have an E5 license.

After analyzing nearly 200 enterprise Teams environments for two months and reviewing several reports from other sources, we have summarized several Teams-specific attacks that have been used by hackers in recent months.

In December, a zero-click vulnerability was uncovered in the Teams environment. The flaw was uncovered by a gamer, who noticed it in the 'teams.microsoft.com' domain. Leveraging cross-site scripting vulnerability, an attacker could send a particular message to any Teams channel or user, and launch an exploit that runs silently, giving the attacker full access to devices and Teams environment, and continuing to auto-propagate as a worm to other channels from one compromised account to the next. The effectiveness of this attack is that it does not require the end-user to click or open anything.

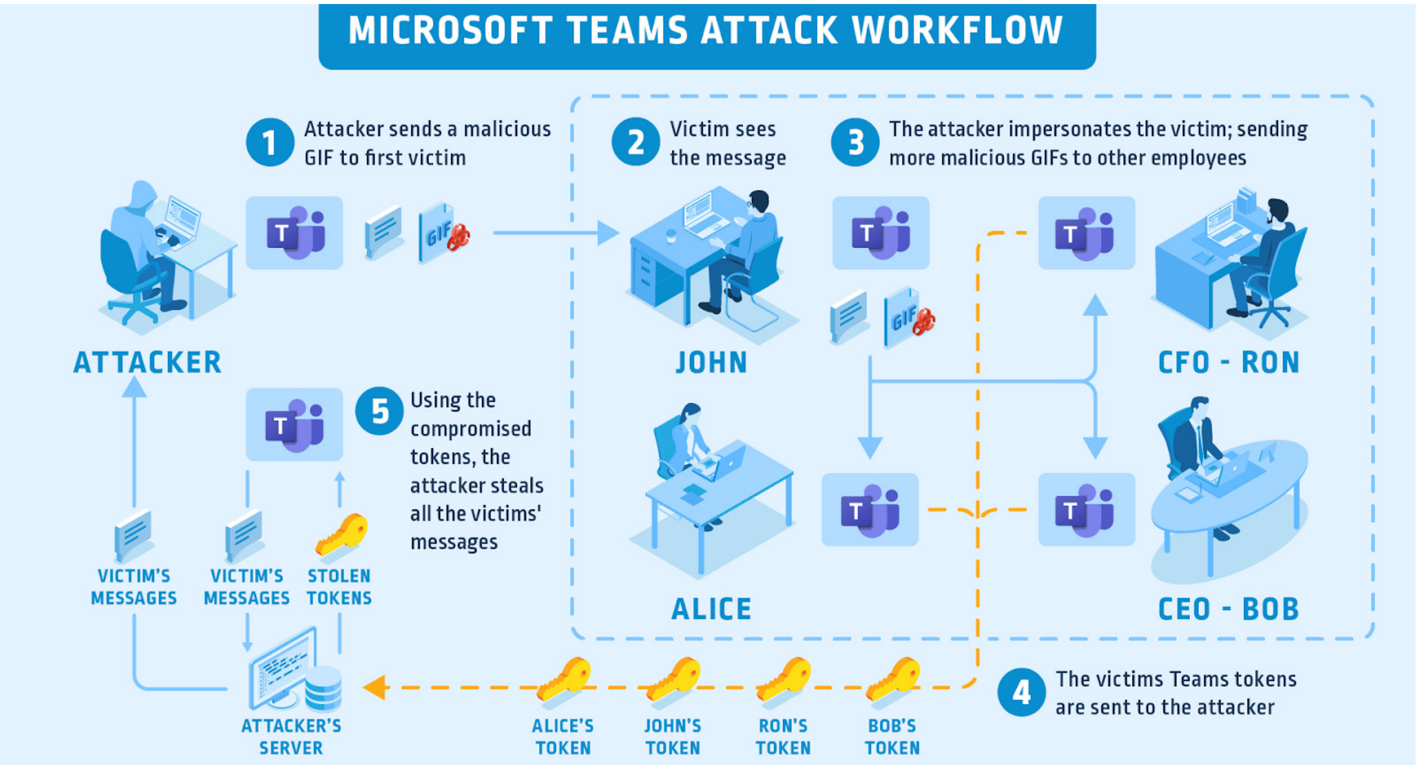
Avanan security analysts tested this shortly after it was published, and verified it was fixed by Microsoft.



TIME	SAAS	TYPE	DESCRIPTION
10:24 PM EST		Phishing	Phishing detected in subject 'need authorization'
10:24 PM EST		Malware	Malware detected in file 'important_release.xlsm'
10:24 PM EST		DLP	Leak detected in file '324_docxaweord)used.json.gz

Threat 2: The Cat GIF Vulnerability

Another threat that was uncovered leveraged a viral cat GIF, taking advantage of end-users sharing the GIF with other colleagues.


MICROSOFT TEAMS ATTACK WORKFLOW
1 Attacker sends a malicious GIF to first victim
2 Victim sees the message
3 The attacker impersonates the victim; sending more malicious GIFs to other employees
ATTACKER
JOHN
CFO - RON
ALICE
CEO - BOB
5 Using the compromised tokens, the attacker steals all the victims' messages
VICTIM'S MESSAGES
VICTIM'S MESSAGES
STOLEN TOKENS
ATTACKER'S SERVER
ALICE'S TOKEN
JOHN'S TOKEN
RON'S TOKEN
BOB'S TOKEN
4 The victims Teams tokens are sent to the attacker
GIF

Courtesy of CYBERARK: Microsoft Teams GIF Attack Workflow

In this attack, first discovered by CyberArk, a malicious GIF was uploaded to a Teams channel. Clicking on it would lead to the hackers harvesting the user's session token, allowing the hacker to impersonate a legitimate employee. As the GIF is shared internally, the hackers are gaining access to additional accounts, gaining access to all Teams content and login credentials and leveraging the compromised accounts to attack additional

Threat 3: Partner Compromise Attack

This attack was found by the Avanan platform in a financial institution that is an Avanan customer. The financial institution was working with a partner organization, and the two companies communicated on a shared Teams channel. This is one of the key benefits of Teams—multiple companies can join and collaborate instantly.

What our analysts found was that the partner organization had an account that was compromised for almost one year, unbeknownst to either company.

And unlike traditional spray-and-pray campaigns we see in compromised email accounts, this hacker acted differently on Teams. For that year, the hacker did not contribute once in the channel. Instead, the hacker listened, collected data and waited for an opportunity. This is a new revelation. In order to evade detection in this new medium, hackers would rather wait for when they can make the biggest impact with the least possible detection.

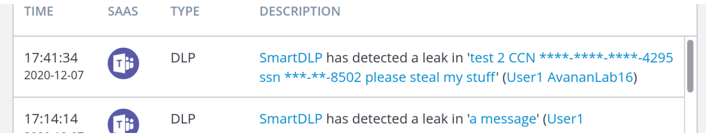
When an opportunity arrived and sharing a file was part of a natural chat conversation, the hacker shared a zip file, which included a version of a malware kit designed for desktop monitoring and configured to install silently upon clicking the file. This Remote Access Trojan would have given the attacker full access to monitor and control the victim's desktop. Avanan caught this malware by running the file in a sandbox and quarantined it from access by other end-users.

Threat 4: Sharing sensitive data with internal and external end-users

An Avanan customer that is one of the largest hospitals in the United-States has added Avanan's Microsoft Teams protection in the past couple of months.

The most common security event in this environment is DLP. We found that doctors share patient medical information practically with no limits on the Teams platform. Medical staff generally know the security rules and risk of sharing information via email, but ignore those when it comes to Teams. In their mind, everything can
be sent.

In one extreme case, we identified a Teams channel with roughly 250 end-users, many of which with email addresses external to the hospital's domain, where sensitive information is shared continuously. In one case medical information, procedures and family circumstances of a minor, was shared together with her name and social security number.

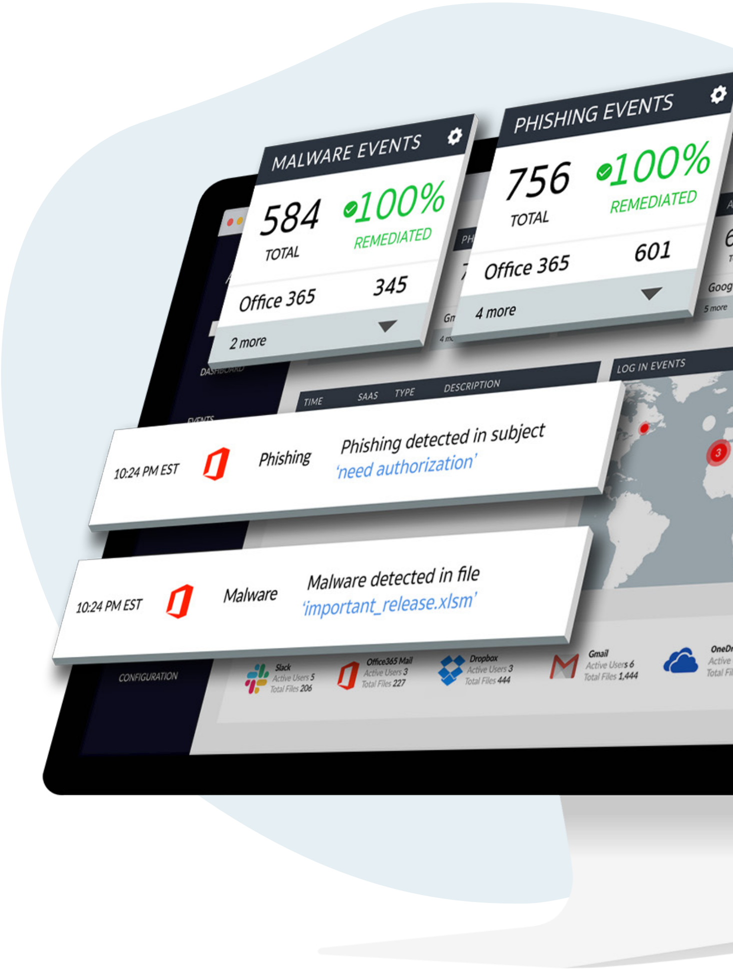


TIME	SAAS	TYPE	DESCRIPTION
17:41:34 2020-12-07	T	DLP	SmartDLP has detected a leak in 'test 2 CCN ****-****-****-4295 ssn ***-**-8502 please steal my stuff' (User1 AvananLab16)
17:14:14	T	DLP	SmartDLP has detected a leak in 'a message' (User1

Those responsible for making life-saving decisions tend to undermine the importance of IT Security and data privacy, and sharing information at the speed and flexibility possible in Teams is a tool we want our doctors to have. At the same time, this extreme case demonstrated that they also need more guidance on usage of the platform to understand what information and with whom they can share, and they need to know that it is monitored just like email is.

Threat 5: FakeUpdates Attack

In one recent report, the FakeUpdates attack, which offers "security recommendations" for hackers to make it easier for its malware to get past ATP scanners, has spread to Teams. Now, this group placed malicious fake ads, hoping that users would click it to install an update. In at least one attack, this group purchased an ad that led to a payload download that extracted a PowerShell script to gain more malicious content. It also installed a legit copy of Microsoft Teams to keep victims in the dark.



10:24 PM EST Phishing Phishing detected in subject 'need authorization'

10:24 PM EST Malware Malware detected in file 'important_release.xlsm'

Part 2: Teams Platform Risks

When companies use Teams, they assume it is internal and unmonitored. Accordingly, the end-user behavior we identified during this analysis observed free sharing of all data. End-users freely share files, data, spreadsheets and sensitive information—often without thinking. Pretty much everything that makes a business run is shared on Teams. That's part of what makes Teams so attractive to businesses.

But it is not always very clear who the users are within a specific channel, especially with channels that may include hundreds of participants. Often companies invite external organizations and individuals into the environment— to new users, it is not always clear when external users are included in a channel.

- With one click, sensitive information can be forwarded outside the organization, either by user error, insider threat or hackers that compromised an account

- External members might be added to a channel and team members may not realize that there are external members on a certain channel, and share information that might not be applicable or appropriate

- Partner's end-user accounts could be compromised while the organization has no control over the security of their partner

- Channels created by partners do not allow visibility to the channel for the organization, via admin or API. Accordingly, the company cannot know what has been shared on these channels and the data goes unaudited

Being a new platform to the enterprise environment, Avanan recommends providing the employees with both guidelines and security training for safe usage of Teams.

The Malicious Content Problem

Microsoft Teams by default does not provide effective security for malicious content:

- Links in the chat are not scanned at all

- Files are scanned because they are actually saved to OneDrive, but only for known signature and at a very low frequency, leaving even known malware available for download for possibly hours

Customers that purchase Microsoft ATP will get more protection for Microsoft Teams, specifically:

- URL protection with Safe Links
- Malicious file protection with Safe Attachments

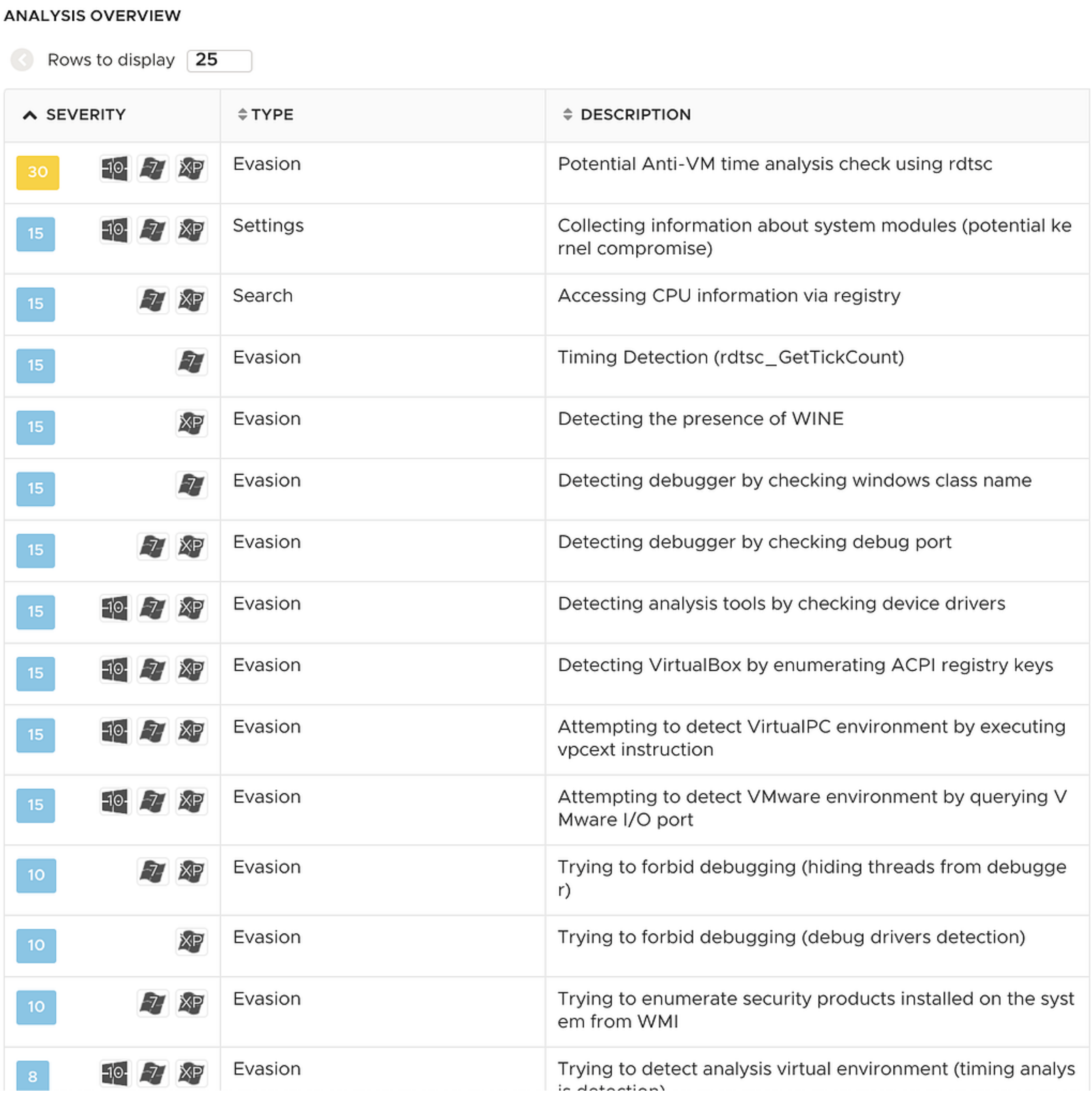
But the general problem that we have seen in email is that the Microsoft ATP layers are not effective enough, especially for targeted attacks, as hackers have access to the Microsoft layers and craft the attack to bypass it. As stated above, in Teams the attacks we have seen are extremely targeted, therefore making ATP even less effective then it is for email.

In the example of the Partner Compromise Attack, the financial institution did have Microsoft ATP running. The hacker had compromised a partner organization for over a year, and observed the inter-organizational chat. When the time was right, the hacker responded to a request for flies with the following text:

"Some of these were large, so I zipped them. Lmk if you have trouble and I can resend."

The hacker then responded with a zipped folder with multiple files, including many that were legitimate and pertinent to the conversation, so there would be no way for the recipient to know that they were about to become a victim. Only one file was a hacked version of desktop monitoring software, configured to install silently upon clicking the file. This Remote Access Trojan would have given the attacker full access to both monitor and control the victim's desktop.

ATP scans files in an asynchronous fashion. It's possible that a malicious file would be available for multiple minutes. Because the scan is actually triggered and done in OneDrive, we found that this protection isn't reliable and fast enough for Teams, which relies on instant action.



ANALYSIS OVERVIEW

Rows to display 25

SEVERITY		TYPE	DESCRIPTION
30	10 7 XP	Evasion	Potential Anti-VM time analysis check using rdtsc
15	10 7 XP	Settings	Collecting information about system modules (potential kernel compromise)
15	7 XP	Search	Accessing CPU information via registry
15	7	Evasion	Timing Detection (rdtsc_GetTickCount)
15	XP	Evasion	Detecting the presence of WINE
15	7	Evasion	Detecting debugger by checking windows class name
15	7 XP	Evasion	Detecting debugger by checking debug port
15	10 7 XP	Evasion	Detecting analysis tools by checking device drivers
15	10 7 XP	Evasion	Detecting VirtualBox by enumerating ACPI registry keys
15	10 7 XP	Evasion	Attempting to detect VirtualPC environment by executing vpcext instruction
15	10 7 XP	Evasion	Attempting to detect VMware environment by querying VMware I/O port
10	7 XP	Evasion	Trying to forbid debugging (hiding threads from debugger)
10	XP	Evasion	Trying to forbid debugging (debug drivers detection)
10	7 XP	Evasion	Trying to enumerate security products installed on the system from WMI
8	10 7 XP	Evasion	Trying to detect analysis virtual environment (timing analysis detection)

Reported issues when running the file in the Avanan Sandbox

- Our analysts then wanted to know if ATP would have detected it, had it ran the file in time. In this case, the file was not detected by ATP even if it had scanned it in time. This hacker indeed crafted a Trojan that would bypass the ATP scanning.
- This attack, Avanan analysts believe, represents the future of Teams attacks. There are a number of steps in this attack that work perfectly in a Teams environment.
- Starting from a Microsoft 365 compromise account. The same credentials that are used to log into Microsoft email is used to login into Teams. Hackers have spent years compromising Microsoft 365 accounts using traditional phishing methods. Once they have those credentials, they can walk right into Teams.
- Leveraging the inherent trust end-users put in Teams. There's no reason to think that someone isn't who they say they are. Users respond freely to messages and download files without a second thought.

The East-West Problem

According to a recent study, in 96% of compromised Microsoft 365 accounts, hackers demonstrated attempts for lateral movement in Microsoft 365, namely attempts to spread to new targets within the organization. Hackers are specifically using Microsoft 365 for lateral movement.

Microsoft Teams is part of the larger Microsoft 365 suite. It is built specifically to glue some of the other tools like OneDrive and make all of them interoperable and easily accessible.

As much as it fosters collaboration and productivity, it's also a gold mine for hackers. If the hacker compromises an account via email, they can then easily try to spread inside the organization and to partners via Teams, SharePoint and OneDrive. In their next hop, the compromise can start in Teams and move to email. Because the login credentials are shared and also because the suite is so tightly woven, it's fairly easy to infiltrate just one and get access to all the rest. By leveraging this technique, hackers spread from partner to partner, as explained in the attack above.

Teams is the ultimate East-West vector. An external actor can be invited, create a free legitimate account and go hunting. Or they can compromise an account, not participate in chats but use Teams to scour the organization for goods.

The Partner Problem

There are several ways external users can join your Teams channels:

- Being a member of a partner account in which both organizations share vital identity information
- Via an email invite that requires a join-request approval
- Via a Teams code that requires no interaction

If you have partner accounts, your users can join channels that your partners create. But that brings up a significant visibility problem:

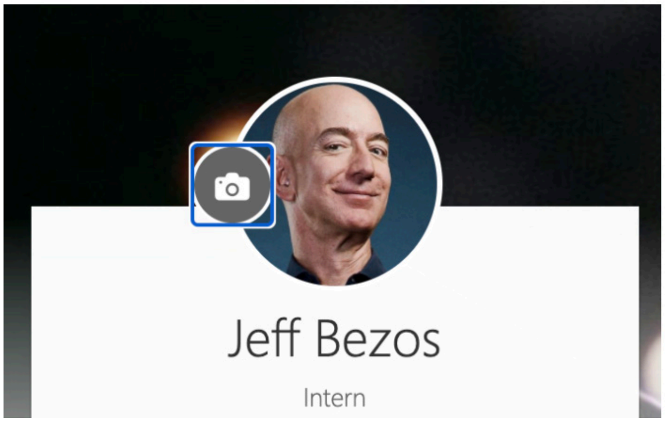
- *The Partner's Partner Problem*: Partners can add their own partners and it becomes a web of external users, and your end-users will have limited ability to separate who they should actually be interacting with. Is that user a member of the partner organization? Or someone else entirely?
- *Hidden Data*: The channels' content is hidden to your organization's administrators and security tools. If malicious content was sent to your employees, or if your employees leak sensitive data, you will not be able to know

With no forensics or easy ability to suss out who is who, it's difficult to protect your organization from this channel. Even an above-the-board interaction with a partner organization can quickly spiral into something malicious.

The Impersonation Problem

One issue we have seen is that when joining with a Teams code, it is possible for an external user to join a group using a free Teams account and a name/ identity of their choice, created at the time of the invite. While it is normally recommended to limit this capability, most organizations allow these features to remain open for the sake of web shares and webinars that require non-Microsoft users to join conference calls and sales meetings.

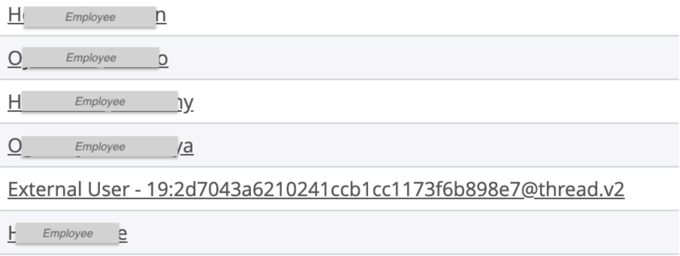
There is an apocryphal story of the company that, for the sake of a birthday prank, changed the photo and public name of every employee Teams accounts to that of the CEO. While funny for the day, it became such a regular occurrence that made it difficult to trust any Teams request or conversation in the organization. Even within Avanan, we saw this happen.



Jeff Bezos doesn't work for Avanan and with someone so recognizable, it can be a fun joke.

Any Teams user can change their name and photo. You cannot see their email address, and therefore there is no "locked identity" that prevents them from impersonating another employee.

Even if you have admin access, via the admin console or API, for external users, you would see they are external but get a cryptic name that will not indicate who the user is or their organization.



H Employee n

O Employee o

H Employee ny

O Employee ya

External User - 19:2d7043a6210241ccb1cc1173f6b898e7@thread.v2

H Employee e

In the attack at the global financial firm described above, the compromised account used the image and name of another user that, in fact, was still an active member of the other inter-organizational groups. From the point of view of the financial firm, these two accounts appeared identical. It's nearly impossible to figure out if an external user is legitimate or not, because there aren't any tools to accurately do so. Then the real user/account builds their reputation with your end-users through their regular interaction, and the external hacker account eventually leverages that to carry out an attack. Even the best anti-phishing trained user will know not to click on links and files.

A partner account can be compromised. Hackers will "invite" themselves and create an account with the same name and picture. Then hackers will wait in the weeds for as long as needed, in one case a year, before striking.

Part 3: The Unknowns of Microsoft Teams

What's perhaps most concerning about Teams is the unknown. Despite rapid adoption, it is still a new platform. An example for some of the unknown risks is the cross-site scripting attack explained in 'Threat-1' above. In that specific attack, Microsoft was very fast to fix and avoid a very harmful zero-click attack on its users.

But what about the vulnerabilities we still don't know about? The platform is just three years old, with most of its users starting in 2020, which means that for all we know about the risks inherent to Teams, there's still much unknown about how end-users will operate in Teams and how hackers will take advantage of it.

Some of the statistics around adoption did demonstrate that we are only at the early stages of usage:

- According to an Avanan analysis, only 25% of Microsoft 365 users actually use Teams on a daily basis. Another study found that 60% of users have less than one interaction a week. The end-users are still learning and experimenting

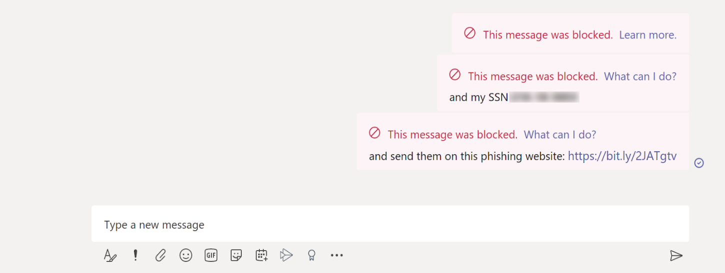
- At the same time, 11% of organizations already invite external collaborators

- Based on the type of data end-users share, we estimate that almost all end-users believe that Teams is internal-only and completely safe

This combination of a new platform with new users that are uneducated on using it securely, with hackers that see the growth and are looking for new ways to hack into organizations, provides the ideal environment for new attacks to come. As Teams continues to take off, hackers will continue to innovate, figure ways to obfuscate the attack and find ways to compromise accounts and steal information.

Part 4: How Avanan Analyzed Teams

Avanan was among the first Microsoft partners to leverage the API for Teams while it was still in beta, and to gain access to the 'action API' that allows quarantining content from end-users. For the purpose of this document, the Avanan security analysts looked at data from roughly 200 enterprise customers that are using Avanan Teams Security module, and analyzed data over a period of two months. By applying our award-winning security layers for email security on Teams, our platform was able to flag malicious files and links, detect sensitive content, compromised accounts, insider threats and unsecure configurations.

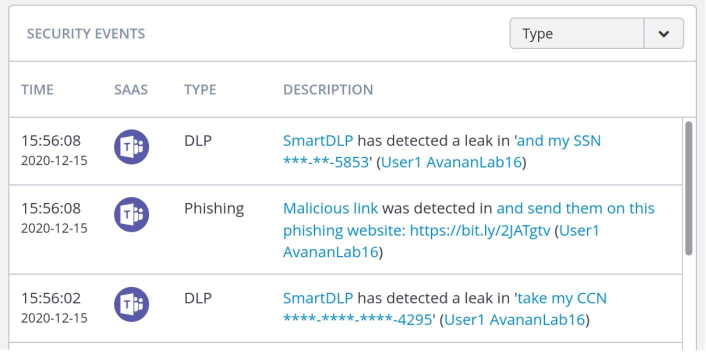


This message was blocked. Learn more.

This message was blocked. What can I do?
and my SSN [redacted]

This message was blocked. What can I do?
and send them on this phishing website: https://bit.ly/2JATgtv

Additionally, it's all recorded as events in the Avanan console, meaning you can analyze Teams events just as you would email:



SECURITY EVENTS

TIME	SAAS	TYPE	DESCRIPTION
15:56:08 2020-12-15	T	DLP	SmartDLP has detected a leak in 'and my SSN ***-**-5853' (User1 AvananLab16)
15:56:08 2020-12-15	T	Phishing	Malicious link was detected in and send them on this phishing website: https://bit.ly/2JATgtv (User1 AvananLab16)
15:56:02 2020-12-15	T	DLP	SmartDLP has detected a leak in 'take my CCN ****-****-****-4295' (User1 AvananLab16)

Avanan is the only company that has this robust offering of Teams protections. It is derived from our mission to secure every line of communication.

Part 5: Conclusion

Business now takes place on Microsoft Teams. Chat, setting meetings, video-conferencing, file sharing—it's all on Teams. While initially it is primarily designed for internal to internal communication, more and more organizations also use it for communication with their partners.

After two months of analyzing nearly 200 enterprise Teams environments, Avanan was able to identify multiple attacks and vulnerabilities in the service, such as:

- The Cross-Scripting Vulnerability
- The Cat GIF Vulnerability
- The Partner Compromise Vulnerability
- The Fake Updates Vulnerability

We've also identified multiple popular types of attack, such as:

- Malware
- Impersonation
- East-West Attack

All these vulnerabilities possess serious risk for end-users. Users are still figuring out how to best use Teams, and surely hackers will adapt with them. This is why we estimate that even more risk comes in the form of the unknown.

As work shifts to Teams, it is incumbent upon businesses that use Teams to secure it from these threats. The best way to think of this problem is to adopt a whole-of-business security, protecting every application where business is conducted.

AVANAN

Avanan is a cloud email security platform that pioneered and patented a new approach to prevent sophisticated attacks. It uses APIs to block phishing, malware, and data leakage in the line of communications traffic. This means Avanan catches threats missed by Microsoft while adding a transparent layer of security for the entire suite that also protects other collaboration tools like Slack. The solution has been recognized as the top-rated cloud email security solution by customers and can replace the need for multiple tools that surround email and file sharing.

See how Avanan can transform your security avanan.com/demo