Global Financial Institution's Microsoft Teams Account Compromised by Malware

Posted by Michael Landewe on November 25, 2020

- Tweet
-

Summary

- A compromised Microsoft Teams account at a partner organization fooled users at a global financial institution into sharing insider information.
- After exfiltrating data via the compromised account, the attacker escalated the attack by sharing a Remote Access Trojan (RAT) to members of the group that was *specifically* designed to bypass Teams protections.
- **This attack bypasses both the default and Advanced Threat Protection (ATP) Teams protections but was caught by Avanan.**
- This is a new methodology that shows how hackers are starting to use different tactics to target Teams over email.
- As Microsoft Teams usage rapidly expands, Avanan analysts expect this type of malware attack to gain widespread prominence.

New Attack Proves Teams Attacks Are Targeted

When a Microsoft 365 account is compromised, one of the first things hackers check for is if the person has a Teams account. Hackers consider this a high-value account, given the free-flowing of information and data.

Currently, Avanan secures Microsoft Teams for about 150 of its enterprise customers. Last week, Avanan's security analysts observed a compromised Teams account and noticed that **hackers are exploiting Teams differently than they do email**. Instead of typical spray and pray tactics, hackers infiltrating Teams accounts are thoughtful and patient, waiting for the right moment to strike.

Avanan analysts have identified this approach as a harbinger of Teams attacks to come—and in the case of one large, global financial institution, it was enough to *almost* bring it to its knees.

This specific malware attack used Microsoft Teams as a vector to install a remote control trojan from a compromised Teams account.

A malicious payload was sent via a Teams chat from a compromised partner organization and was *specifically designed* to both bypass built-in protections and fool the user into opening the malicious file.

Though this attack bypassed both EOP and ATP, it was caught and stopped by Avanan.

The Attack Leveraged Teams to Include a Silent Installer of Remote Monitoring Software

This attack involves two companies. The Avanan customer is a global financial firm—and then there's a partner organization that they work with.

Based on our analysis, an account in the partner organization was compromised for almost one year, and the hacker listened in on an inter-organizational Teams chat. Over the course of the year, the malicious actor did not contribute in that group channel. This is the antithesis of typical spray-and-pray modus operandi when an email account gets compromised.

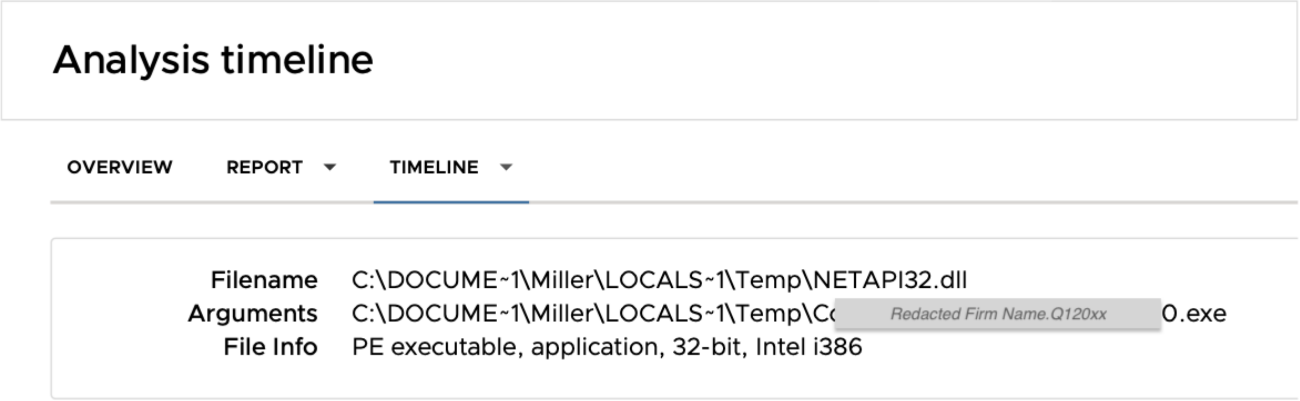
And then the opportunity for the hacker came. The attacker responded to a team-wide request for some files with the message:

> “some of these were large, so I zipped them. Lmk if you have trouble and I can resend.”

The file included an easily-obtainable 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.

Had the file reached the user, she would have opened the file and installed the malware with no local alert or message that anything was wrong.

Because the message included multiple files, including legitimate, pertinent documents, the recipient would have been none the wiser.



Analysis timeline

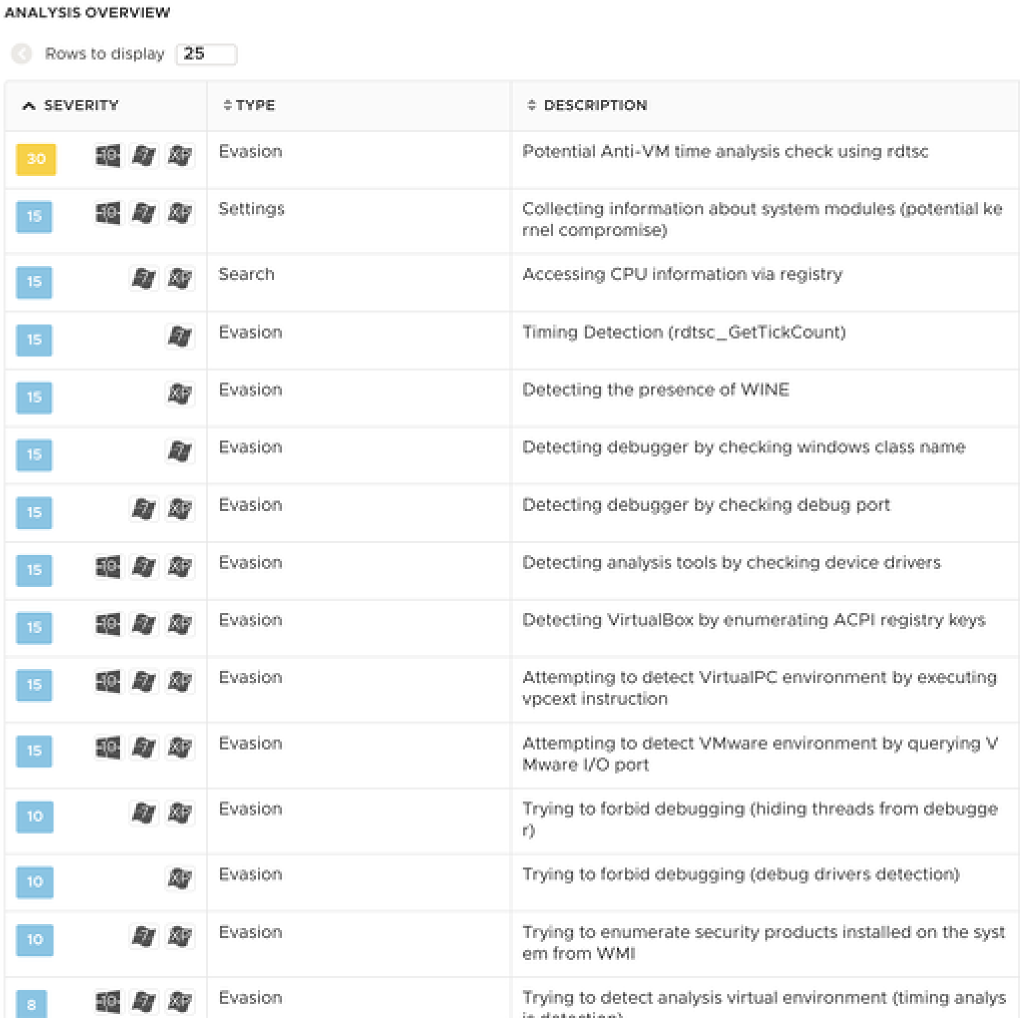
Filename	C:\DOCUME~1\Miller\LOCALS~1\Temp\NETAPI32.dll
Arguments	C:\DOCUME~1\Miller\LOCALS~1\Temp\Co Redacted Firm Name.Q120xx 0.exe
File Info	PE executable, application, 32-bit, Intel i386

The Trojan Software Was Designed to Bypass Built-in Teams Protections

The RAT was designed to bypass Microsoft malware filters.

Most organizations rely on the default, signature-based protection for Microsoft Teams, but this firm had also upgraded to the additional Advanced Threat Protection subscriptions. With the ATP upgrade, files that are shared via Teams may be scanned by sandboxing filters when they are uploaded to the associated ShareFile/OneDrive directory.

It is clear, though, that the attacker had assumed such defenses, as the Trojan included a variety of methods to detect both sandboxing tools and Windows desktop protections. (The sandboxing tools used by Avanan use these methods as indicators of attack.)



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 analys

When tested against Advanced Threat Protection (both the email and file-share scanning tools), this Trojan went undetected. **Unbeknownst to the attacker, the Avanan system identified and blocked the malicious file, protecting the user and outing the compromised account.**

This is The New Teams Attack

While attacks that use Microsoft Teams as a vector are currently less common than email-borne attacks, there are some lessons to be learned from Slack-based attacks, which became ubiquitous in 2019.

- **Compromising a Teams account is 'easy'.** Attackers are already very adept at compromising Microsoft 365 accounts using traditional email phishing methods. The same credentials work for Teams.

- **Attacks that use Teams or Slack as a vector are silent and stealthy, designed to avoid detection**. Because of the inherent trust that users grant to Teams or Slack messages, attackers are very careful about potential discovery. Slack and Teams are the preferred internal East-West vector for attackers to spread inside the organization.
- **Malware or phishing URLs are specifically targeted to bypass built-in protections.** Once inside an organization, an attacker (normally) knows what technology is being used to protect it. An attack that uses Teams as a vector will have already been tested against Microsoft filters.

Learn More: Teams Security

This Single Incident is Highly Scalable into a Widespread Campaign

When Slack first became the most commonly used collaboration tool, small attacks found in isolated organizations soon became widespread.

Microsoft Teams is now, by far, the most-used internal collaboration tool, as usage of the service grew exponentially during the COVID-19 pandemic. Teams now has 115 million daily active users, nearly one hundred million more than the latest Slack usage numbers. As Teams usage continues to increase, Avanan expects a significant increase in these sorts of attacks.

Because Teams is used in a variety of organizations that host scores of sensitive information, there is vast opportunity for data exfiltration. Microsoft announced that 91 of the Fortune's 100 companies use Teams, including major pharmaceutical companies like Pfizer and a number of financial institutions. This type of attack would cause significant damage.

This attack demonstrates that hackers are beginning to understand and better utilize Teams as a potential attack vector. If Teams campaigns follow the trajectory of Slack-based attacks, we foresee large-scale Teams-based campaigns in 2021.

Subscribe to Our Attack Briefs for More Research

- Tweet
-

Topics: