Attackers Leveraging Microsoft Teams Defaults and Quick Assist for Social Engineering Attacks

linkedin.com/pulse/attackers-leveraging-microsoft-teams-defaults-quick-assist-p1u5c

ConnectWise

ConnectWise

A platform of software & services built for TSPs. Follow us for product updates, company news, business advice and more.

Published Jan 31, 2025

+ Follow

By: Blake Eakin

During January the CRU observed incidents in which phishing was carried out by sending Teams messages to users from an external Microsoft 365 tenant. In this way, they masqueraded as members of the victim organization's internal IT help desk and instructed the victims to set up Microsoft Quick Assist in order to provide the attackers with access to their machine. Once initial access was accomplished, the attackers used a varied arsenal of tools to attain footholds, move laterally, and elevate privileges.

A similar campaign was observed by Sophos in November and December of 2024, which they track as STAC5777. The same attack vector was also covered by Microsoft around May 2024, attributed to what they track as Storm-1811. Both of these reports mention the attacks leading to Black Basta ransomware, however, the follow-on activity leading to ransomware deployment has differed between what was reported by Microsoft in May and what was observed by us and Sophos since November.

> We are releasing this report to emphasize monitoring and mitigation of this attack vector and provide additional observations of the tools and techniques used.

Initial Access

The attackers sent messages to victims via Teams with a display name of Help Desk. Teams logs all showed the messages coming from different accounts across incidents, but consistently from the same IP addresses of either 78.46.67[.]201, as also reported by Sophos, or 2a01:4f8:120:53f6[::]2, which appears to just be the IPv6 address of the same host. Other reporting outlines a technique of flooding victims with phishing emails and then initiating Teams chats as Help Desk suggesting they are there to remediate the issue.

The attackers initiate a voice chat with the victims and instruct them to open Quick Assist and enter a PIN granting them remote access to the victim machine. From here the attackers download two files from an Amazon S3 bucket that we observed as kb052117-01.bpx and kb052123-02.bpx, which were then combined into the zip archive file pack.zip.

Persistence and Command and Control

Attackers set the registry key HKCU\SOFTWARE\TitanPlus with a list of Command and Control (C2) addresses and ports. In some cases they are formatted normally, and in others the '.' Characters are replaced with 'B' and ':' is replaced with 'A'. Then they looked specifically for CrowdStrike Falcon running in the task list.

They extracted pack.zip into %temp% using the native tar utility, followed by using the expand utility to extract a cab file into %LocalAppdata%\Microsoft\OneDrive. This is the native folder for OneDrive and some of its utilities, however the attackers extracted several

additional dll files and a settingsbackup.dat file there, where they would not normally be found. Then they manually ran the OneDriveStandaloneUpdater.exe binary with the -Embedding option to initiate dll sideloading of malicious payloads.

This behavior was well covered by Sophos in their report, but the payloads were also explored by researchers at Walmart as Back.Connect. They also suggested possible ties to Qakbot, which Microsoft reported being used by Storm-1181. In both reports exploring the malicious payloads used in this manner, they mentioned them coming from a sideload of winhttp.dll. We did not directly observe this, but did see the use of a wscapi.dll file that suspiciously had an original file name of ieui.dll, but had a code signing certificate with a subject name of Farfield Computing Systems Inc. The malicious payload set persistence in the Startup directory with OneDriveUpdate.lnk.

On the beachhead hosts that the attackers gained initial access on we observed these actions being manually executed via a cmd session. They would repeat these steps on several other machines in the environment to establish further footholds except by using a batch script. Instead of %LocalAppdata%\Microsoft\OneDrive the files would be extracted into C:\Windows\System32\LogFiles\OneDriveUpdate.

In one incident, when the attackers gained access to a server running MS-SQL they logged into the database and enabled xp_cmdshell. Through this access they changed the passwords for several administrator accounts that they then used throughout the rest of the incident. This also provided them a further method of possible persistence.

On some hosts the RMM tools Level and Atera were installed. The URL for downloading the Atera installer showed an integratorLogin email of cynthia.guerrero@stock[.]com[.]py, a domain used by a Paraguayan super market. This suggests they may be using compromised accounts and infrastructure to further develop their own.

Lateral Movement and Discovery

The attackers used many different methods for lateral movement including RDP, SMB, WMI, WinRS, remote scheduled tasks, and WinRM. They were observed tampering with the HKLM\System\CurrentControlSet\Control\Terminal Server\fDenyTSConnections and HKLM\System\CurrentControlSet\Control\Lsa\DisableRestrictedAdmin registry keys in order to ease remote access by setting both of their values to 0.

We were able to identify some of the various tools used for lateral movement, such as winrm-fs a tool for file management using WinRM. We also observed the use of impersonate, a token impersonation tool, to not only impersonate tokens, but also to execute commands for facilitating lateral movement onto domain controllers, like using the net command to ensure accounts were active on the targeted DCs.

The attackers did use Psexec during an incident, but it was only used to execute commands locally rather than remotely. A discovery tool called eviltree was also observed that can be used for searching across nested directory structures for keywords or regex.

Defense Evasion

On several machines, before installing their backdoor, we observed the attackers make use of a tool to disable SentinelOne on victim endpoints. We identified the executable and driver combination to be what has previously been reported as Stonestop and Poortry. However, unlike previous reporting, this version of the EDR killing malware was specifically targeted towards SentinelOne.

It was delivered in a zip archive containing a batch file named run.bat, an InnoSetup installer named k2bP.exe, and a driver named nbwdv.sys. The run.bat file drives the whole operation by first impairing and disabling the Windows Time Service and setting the system date to 2012 before executing k2bP.exe.

It does this because the certificate for the nbwdv.sys driver is expired. Setting the system time somewhere during the valid dates for it and impeding the Windows Time Service effectively allows them to bypass expiration checks for the certificate.

The controller binary k2bP.exe communicates with the driver through a handle it opens to the hardcoded path \??\fqg0Et4KlNt4s1JT and calls to the DeviceIOControl API. It initiates communication with the driver using the IOCTL code 0x2236544 and passes it the id “7N6bCAoECbItsUR5-h4Rp2nkQxybfKb0F-wgbJGHGh20pWUuN1-ZxfXdiOYps6HTp0X”.

During execution, k2bP.exe goes about enumerating all the files in the C:\Program Files\SentinelOne directory recursively and deleting any files with a .exe extension using IOCTL value 0x2236800. Then it reviews the names of all the running processes and kills any related to SentinelOne using IOCTL 0x2236740 along with the corresponding process id to kill. After all this work is done it will idle, looking for a directory named ‘stop’ in its current working directory. If it finds this directory (or just any file named stop) then it will delete the directory and stop running. Otherwise it runs indefinitely.

ATT&CK Techniques

Initial Access

T1566.003 Spearphishing via Service

T1566.004 Spearphishing Voice

Execution

T1059.003 Windows Command Shell

T1059.001 PowerShell

T1053.005 Scheduled Task

T1569.002 Service Execution

T1047 Windows Management Instrumentation

Persistence

T1098 Account Manipulation

T1547.001 Registry Run Keys / Startup Folder

T1136.002 Domain Account

T1574.001 DLL Search Order Hijacking

T1574.002 DLL Side-Loading

Privilege Escalation

T1134.001 Token Impersonation/Theft

Defense Evasion

T1562.001 Disable or Modify Tools

T1112 Modify Registry

Discovery

T1087.002 Domain Account

T1069.002 Domain Groups

T1033 System Owner/User Discovery

Lateral Movement

T1570 Lateral Tool Transfer

T1021.001 Remote Desktop Protocol

T1021.002 SMB/Windows Admin Shares

T1021.006 Windows Remote Management

Command and Control

T1219 Remote Access Software

IOCs

IPs

Command and Control:

185.190.251[.]16

207.90.238[.]52

89.185.80[.]86

38.180.25[.]3

45.8.157[.]199

5.181.3[.]164

Teams Phishing:

2a01:4f8:120:53f6:0[::]2

78.46.67[.]201

Teams Phishing Accounts

admin_911@stmgnyl.onmicrosoft[.]com

DDDr@freeagentnetwork913.onmicrosoft[.]com

admin_0123@remicristian.onmicrosoft[.]com

ConnectWise Cyber Research

46,708 followers

+ Subscribe

To view or add a comment, sign in

More articles by ConnectWise

- Apr 1, 2025
  ### Fake File Converters on the Rise
  By: Bryson Medlock and Al Calleo Since February, the CRU has seen a notable increase in attacks involving fake online…
  28
  2 Comments

- Mar 11, 2025
  ### Patch Tuesday March 2025
  On March 12, 2025, Microsoft released its latest batch of security updates as part of Patch Tuesday, addressing 56…
  16

- Mar 10, 2025
  ### Large-Scale Malvertising Campaign Targets Nearly One Million Devices
  By: Bryson Medlock In December 2024, a significant cybersecurity incident unfolded, affecting close to one million…
  25
  1 Comment

- Mar 5, 2025

  Emerging Ransomware Tactics: Black Basta and Cactus Groups

  By Bryson Medlock Recent investigations have unveiled evolving methodologies employed by the Black Basta and Cactus…

  27

- Feb 26, 2025

  Recent Observations from ClickFix Campaigns

  By Blake Eakin The ClickFix initial access technique, where victims are social engineered into executing malicious code…

  19

- Feb 24, 2025

  New PayPal Scam Bypasses Email Security

  By Bryson Medlock A recent phishing campaign has emerged, exploiting PayPal's "New Address" verification emails to…

  31

- Feb 12, 2025

  Patch Tuesday | February 2025

  Every month on the second Tuesday, Microsoft and other vendors release security software patches in what has become…

  28

- Feb 11, 2025

  Key cybersecurity predictions for 2025

  By Bryson Medlock As we start a new year, it is important to examine recent developments and trends in order to stay…

  42

- Feb 4, 2025

  PoC Exploit Released for Patched Active Directory Vulnerability CVE-2025-21293

  By: Bryson Medlock A vulnerability patched in Microsoft’s January 2025 Patch Tuesday security updates now has a…

  37

- Jan 29, 2025

  Threat Actors Exploiting SimpleHelp RMM

  Security researchers have identified active exploitation of vulnerabilities in SimpleHelp's Remote Monitoring and…

  26

  1 Comment

See all articles

Insights from the community

- Technical Support

  How can network security monitoring identify and respond to social engineering attacks?

- Network Security

  Your team member has compromised network integrity. How will you prevent future social engineering attacks?

- Cybersecurity

  How can you ensure your SOC detects social engineering attacks?

- Telecommunications Engineering

  How can you protect your voice platform from social engineering attacks?

- Systems Engineering

  How can you detect and prevent operating system attacks?

- Workplace Safety

  How can you prevent cyber attacks in the workplace?

- Warehouse Operations

  What are the best ways to secure your WMS against social engineering attacks?

- Operating Systems

  How can you build resilience against cyber attacks in Operating Systems?

Others also viewed

Explore topics