Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

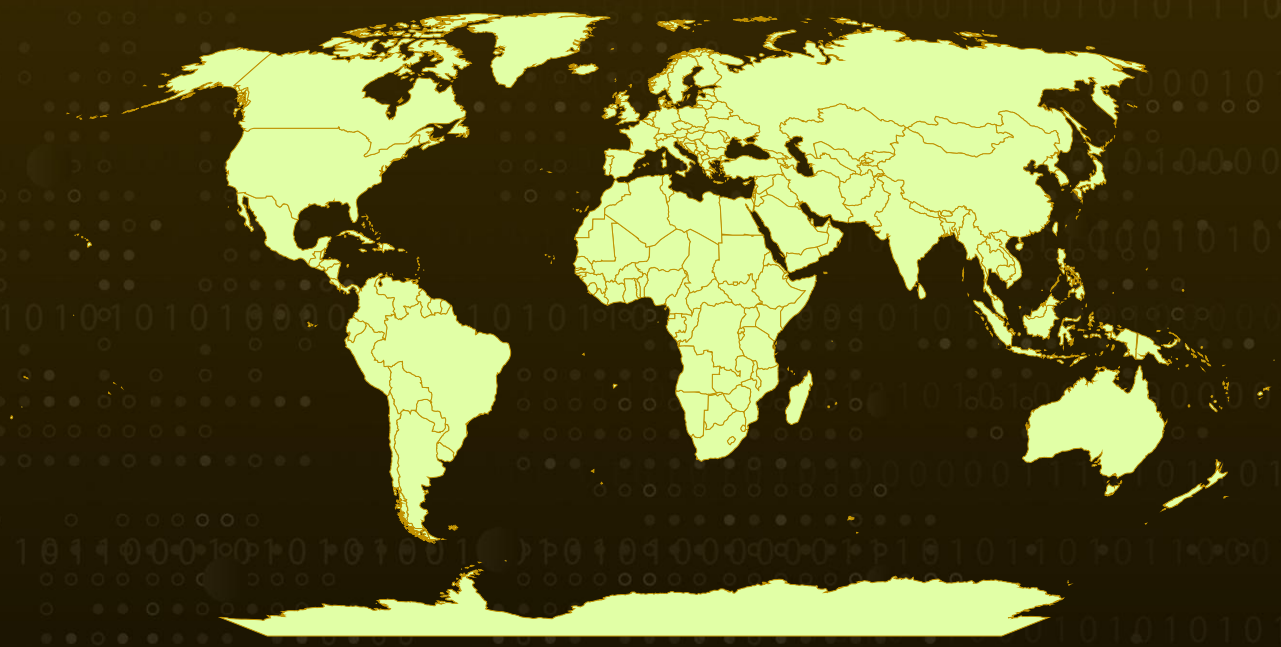
Microsoft Teams Social Engineering Delivers A0Backdoor Malware

Date of Publication	Admiralty Code	TA Number
March 11, 2026	A1	TA2026064

Summary

First Seen: August 2025
Targeted Regions: Worldwide
Targeted Platforms: Windows
Targeted Industries: Financial Services, Healthcare
Malware: A0Backdoor
Attack: A sophisticated social-engineering campaign is targeting financial and healthcare organizations by abusing trust in internal IT support channels. Attackers flood victims with spam emails before contacting them on Microsoft Teams while posing as helpdesk staff, convincing them to grant remote access through Windows Quick Assist. They then deploy a signed installer that abuses DLL sideloading to deliver A0Backdoor, showing how attackers increasingly leverage trusted tools to quietly infiltrate enterprise environments.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Targeted Non-Targeted

Attack Details

#1

Threat actors have been approaching employees at financial and healthcare organizations through Microsoft Teams, posing as internal IT support to trick them into granting remote access via Windows Quick Assist. The deception ultimately leads to the deployment of a newly identified malware called A0Backdoor. The campaign typically begins with an email bombing phase, where the victim's inbox is flooded with a large number of harmless spam messages to create confusion and disrupt normal communication. Taking advantage of the chaos, the attackers quickly contact the target through Teams, offering to help resolve the email issue they themselves triggered. The operation primarily focuses on high-value personnel such as executives, senior managers, finance teams, legal staff, and other employees with access to sensitive corporate data.

#2

During the interaction, victims are persuaded to launch Windows Quick Assist, a legitimate built-in remote support tool that allows screen sharing and device control. Once access is granted, attackers deploy malicious MSI installer packages hosted on Microsoft personal cloud storage using tokenized download links. These installers are created using Advanced Installer and disguised to resemble legitimate Microsoft components. To appear trustworthy, the MSI files are digitally signed with publicly trusted certificates, including one issued to MULTIMEDIOS CORDILLERANOS SRL, which appear to rotate periodically, likely to avoid revocation or detection.

#3

Inside the installer, most bundled DLL files retain legitimate Microsoft signatures, helping the package look authentic. However, one key componenthostfxr.dll, a .NET hosting library normally signed by Microsoft, has been replaced with a malicious version signed with the same non-Microsoft certificate as the installer. This enables a DLL sideloading technique in which a legitimate executable, CrossDeviceService, unknowingly loads the malicious library. The malicious DLL contains encrypted payload data and employs several anti-analysis techniques, including excessive thread creation through the CreateThread API to disrupt debugging environments. After performing sandbox and timing checks, the shellcode decrypts and launches the A0Backdoor payload.

#4

Once active, A0Backdoor moves its code into a new memory region and decrypts its internal routines, including its command-and-control configuration. It then gathers system and user details using Windows APIs. For communication, the malware relies on a covert DNS tunneling technique, sending DNS MX queries containing encoded metadata within subdomains to trusted public resolvers like 1.1.1.1 and 8.8.8.8. By embedding commands within DNS requests, the malware can quietly receive instructions while blending in with normal network traffic, allowing attackers to maintain persistent and stealthy control over compromised systems. These traits closely resemble the activity patterns of Blitz Brigantine (Storm-1811 / STAC5777) and align with the Black Basta social-engineering playbook, while suggesting the group continues to refresh its tooling to better evade enterprise security defenses.

Recommendations

Restrict or Remove Quick Assist: Disable Windows Quick Assist enterprise-wide where it is not operationally required. Where it must remain, enforce policies that restrict who can initiate and accept remote sessions, and log all Quick Assist connection events for SOC monitoring.

Implement User Awareness Training on Teams-Based Social Engineering: Deploy immediate and targeted training emphasizing that the IT helpdesk will never initiate unsolicited contact via Microsoft Teams. Mandate that employees verify any unexpected IT contact through a secondary, pre-established channel such as a known helpdesk phone number before granting any form of remote access.

Monitor for Anomalous DNS MX Query Patterns: Deploy detection rules for unusually high volumes of DNS MX queries from endpoints, particularly those directed to public recursive resolvers (1.1.1.1, 8.8.8.8) with high-entropy subdomains. Standard workstations rarely generate MX record lookups; any such activity should trigger an alert for investigation.

Monitor for DLL Sideloading via CrossDeviceService: Create detection logic for CrossDeviceService.exe or similar legitimate Microsoft binaries loading DLLs (particularly hostfxr.dll) that are not signed by Microsoft. Hash-based or certificate-based validation of loaded libraries can identify sideloading attempts in real time.

Enforce Code-Signing Certificate Validation: Implement policies that validate code-signing certificate chains before allowing MSI or DLL execution. Alert on execution of binaries signed with recently revoked certificates, as this campaign relies on timestamped signatures that preserve trust even after revocation.

Deploy Network Segmentation and Zero-Trust Controls: Segment networks to limit lateral movement following an initial compromise through remote access tools. Enforce least-privilege access and require multi-factor authentication for privileged actions, reducing the impact of compromised senior-level accounts.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.003: Spearphishing via Service
Execution	T1204: User Execution	T1204.001: Malicious Link
Persistence	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
Defense Evasion	T1553: Subvert Trust Controls	T1553.002: Code Signing
	T1656: Impersonation	
	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
		T1027.002:Software Packing
		T1027.009: Embedded Payloads
	T1497: Virtualization/Sandbox Evasion	
	T1622: Debugger Evasion	
	T1140: Deobfuscate/Decode Files or Information	
	T1480: Execution Guardrails	T1480.001:Environmental Keying
Discovery	T1082: System Information Discovery	
	T1033: System Owner/User Discovery	

Tactic	Technique	Sub-technique
Command and Control	T1071: Application Layer Protocol	T1071.004: DNS
	T1572: Protocol Tunneling	
	T1102: Web Service	
	T1105: Ingress Tool Transfer	
	T1132: Data Encoding	T1132.002: Non-Standard Encoding
Resource Development	T1588: Obtain Capabilities	T1588.003: Code Signing Certificates
Impact	T1667: Email Bombing	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	0c99481dcacda99014e1eeef2e12de3db44b5db9879ce33204d3c65469e969ff, 26db06a2319c09918225e59c404448d92fe31262834d70090e941093e6bb650a
Domains	fsdgh[.]com, my[.]microsoftpersonalcontent[.]com

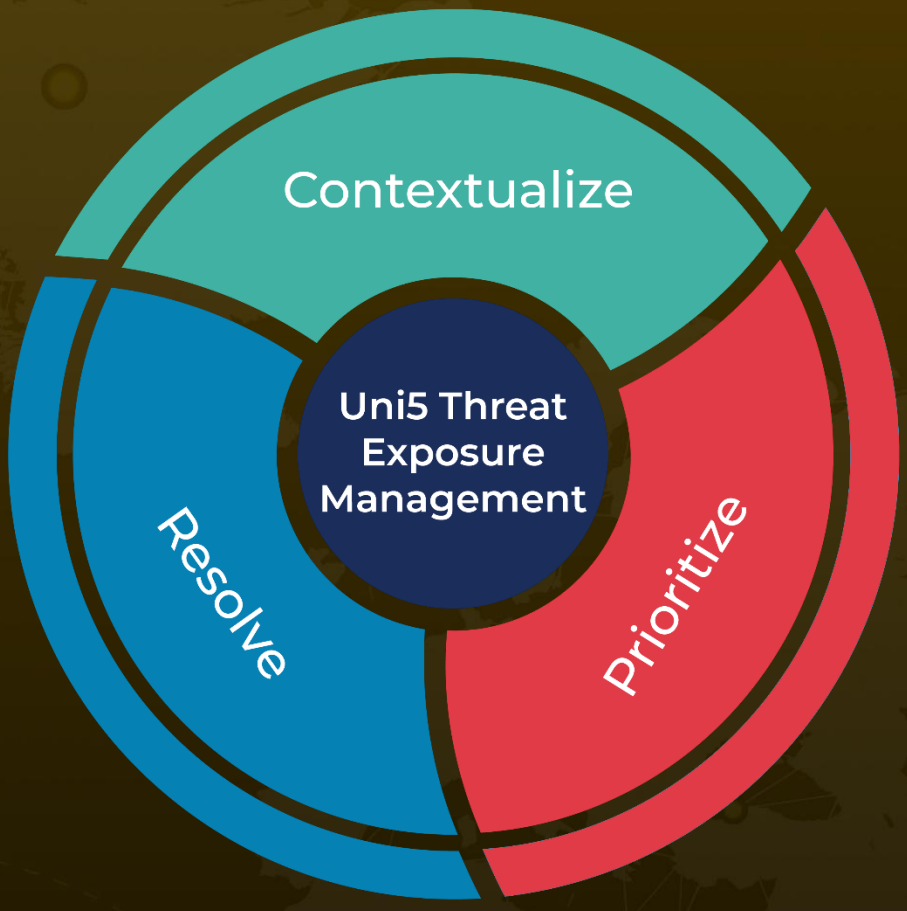
References

https://www.bluevoyant.com/blog/new-a0backdoor-linked-to-teams-impersonation-and-quick-assist-social-engineering

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 11, 2026 • 02:00 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com