Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

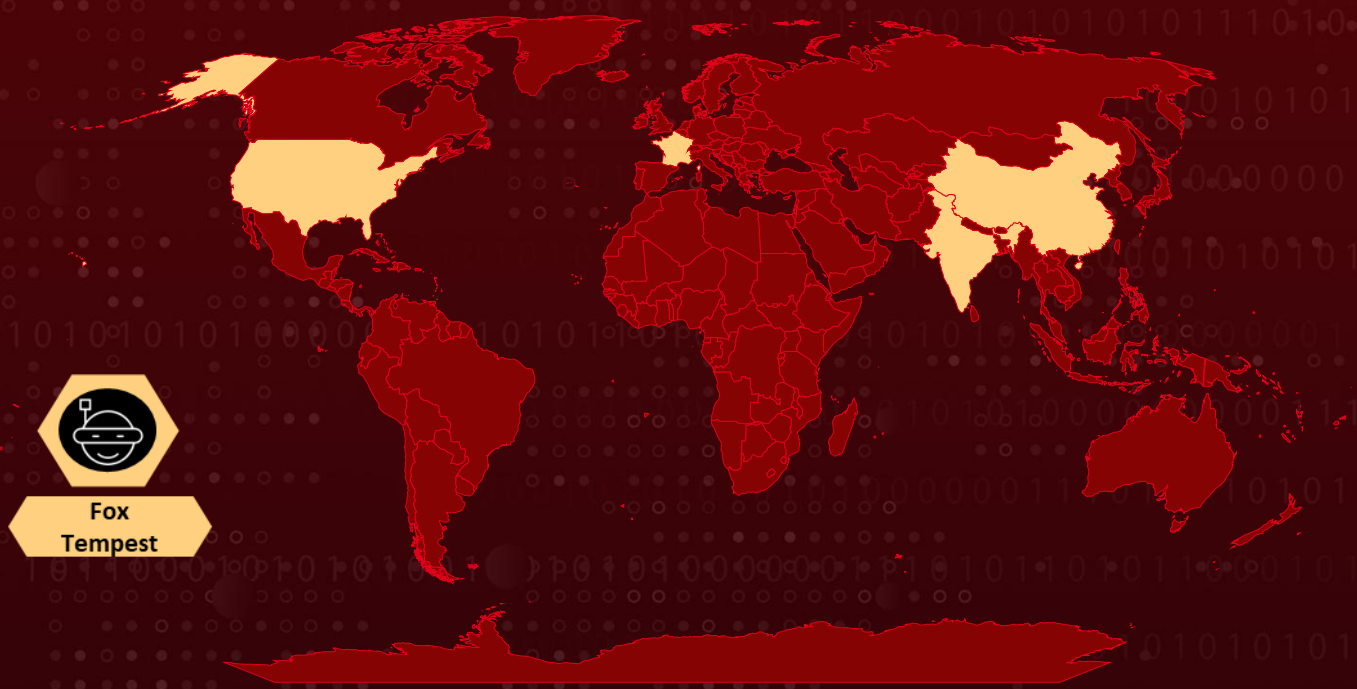
72-Hour Window of Trust: Fox Tempest's Abuse of Microsoft Artifact Signing

Date of Publication	Admiralty Code	TA Number
May 22, 2026	A1	TA2026142

Summary

First Seen: May 2025
Targeted Regions: United States, France, India, China
Targeted Platform: Windows
Targeted Products: AnyDesk, Microsoft Teams, PuTTY, Webex (impersonated as lures)
Targeted Industries: Healthcare, Education, Government, Financial Services
Threat Actor: Fox Tempest
Attack: Fox Tempest is a financially motivated threat actor that operated a malware-signing-as-a-service (MSaaS) offering branded as SignSpace. The service abused Microsoft Artifact Signing to issue short-lived, fraudulently obtained code-signing certificates valid for 72 hours, allowing customer-supplied malware and ransomware to masquerade as legitimately signed Windows software such as AnyDesk, Microsoft Teams, PuTTY, and Webex.

Attack Regions



Attack Details

#1

Fox Tempest is a financially motivated threat actor that does not directly compromise victims; instead, it operates a malware-signing-as-a-service capability that downstream ransomware and commodity malware operators consume to gain initial access against end-user environments. Customers of Fox Tempest, including Vanilla Tempest, Storm-0501, Storm-2561, and Storm-0249, distribute the resulting fraudulently signed binaries through legitimately purchased advertisements, malvertising, and SEO poisoning that redirect victims searching for popular enterprise tools such as AnyDesk, Microsoft Teams, PuTTY, and Webex to attacker-controlled download pages. Because the installers are signed with short-lived Microsoft-issued code-signing certificates obtained through Microsoft Artifact Signing and valid for only 72 hours, they appear to originate from a trusted publisher and bypass reputation, allow-list, and publisher-trust controls that would otherwise flag unsigned or unknown executables. To obtain the certificates, Fox Tempest is assessed to have used stolen identities based in the United States and Canada to defeat the identity validation processes required by Artifact Signing.

#2

Once a victim executes the trojanized installer, such as the malicious MSTeamsSetup.exe deployed in the Vanilla Tempest case study, the fraudulently signed binary launches a follow-on payload from the Fox Tempest-enabled distribution catalog. Observed payloads include the Oyster backdoor (also known as Broomstick), Lumma Stealer, and Vidar. Oyster is a modular, multistage implant that establishes persistent remote access, initiates command-and-control communications, collects host-level information, and enables the delivery of additional payloads, while blending into normal enterprise activity by virtue of its legitimate-looking signed parent installer. The Vanilla Tempest attack chain depicts scheduled tasks being created as part of the Oyster deployment, supporting persistent execution across reboots.

#3

Following the establishment of initial access, downstream operators have been observed conducting hands-on-keyboard activity within victim environments. Microsoft Defender for Endpoint detections cited in the source reporting include user accounts created under suspicious circumstances, new groups added suspiciously, and new local administrator accounts created using Net commands, indicating credential and privilege manipulation consistent with preparation for lateral movement and broader environment compromise.

#4

The downstream impact of Fox Tempest-enabled access is overwhelmingly ransomware deployment. In observed Vanilla Tempest engagements, the same Oyster-led intrusion chain culminated in the deployment of Rhysida ransomware within the victim environment. Cryptocurrency analysis associated with Fox Tempest has identified clear links to ransomware affiliates responsible for deploying multiple prominent ransomware families, including Rhysida, INC, Qilin, Akira, and BlackByte, with observed proceeds in the millions of dollars. The resulting attacks have impacted healthcare, education, government, and financial services organizations across the United States, France, India, and China, demonstrating that Fox Tempest functions as a vital trust-laundering operator within the broader cybercrime ecosystem.

Recommendations

Do Not Rely on Code Signing as a Standalone Trust Control: Layer Authenticode signature verification with behavioral analytics, EDR telemetry, and execution restrictions, because a valid Microsoft-issued certificate alone is no longer a reliable indicator of software trustworthiness given the fraudulent issuance through Artifact Signing observed in this campaign.

Enable Tenant-Wide Tamper Protection: Activate tenant-wide tamper protection in Microsoft Defender for Endpoint to prevent attackers who achieve initial execution via Fox Tempest-signed payloads from disabling Defender or modifying antivirus exclusions, and enable DisableLocalAdminMerge to block GPO-based exclusion tampering.

Deploy SmartScreen-Enabled Browsers: Standardize on Microsoft Edge or other browsers supporting Microsoft Defender SmartScreen to block known malicious download pages, malvertising, and SEO-poisoned search results that redirect to counterfeit AnyDesk, Teams, PuTTY, and Webex installers.

Validate Application Allow-Listing with Behavioral Validation: Augment Windows Defender Application Control or similar allow-listing solutions so that newly observed signed binaries are not automatically trusted on the basis of a valid signature alone, and require behavioral validation or hash-based approval for execution.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1583: Acquire Infrastructure	T1583.001: Domains
		T1583.003: Virtual Private Server
		T1583.008: Malvertising
	T1585: Establish Accounts	T1585.001: Social Media Accounts
		T1585.003: Cloud Accounts
	T1586: Compromise Accounts	
	T1587: Develop Capabilities	T1587.002: Code Signing Certificates
	T1608: Stage Capabilities	T1608.006: SEO Poisoning
Initial Access	T1189: Drive-by Compromise	
Execution	T1204: User Execution	T1204.002: Malicious File
Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1136: Create Account	T1136.001: Local Account
Defense Evasion	T1553: Subvert Trust Controls	T1553.002: Code Signing
	T1036: Masquerading	T1036.005: Match Legitimate Resource Name or Location
Discovery	T1082: System Information Discovery	
Credential Access	T1555: Credentials from Password Stores	

Tactic	Technique	Sub-technique
Command and Control	T1071: Application Layer Protocol	
	T1105: Ingress Tool Transfer	
Impact	T1486: Data Encrypted for Impact	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	signspace[.]cloud
SHA1	dc0acb01e3086ea8a9cb144a5f97810d291020ce, 7e6d9dac619c04ae1b3c8c0906123e752ed66d63
SHA256	f0668ce925f36ff7f3359b0ea47e3fa243af13cd6ad9661dfccc9ff79fb4f1cc, 11af4566539ad3224e968194c7a9ad7b596460d8f6e423fc62d1ea5fc0724326, f0a6b89ec7eee83274cd484cea526b970a3ef28038799b0a5774bb33c5793b55
Telegram Channel	EV Certs for Sale by SamCodeSign
Telegram Username	arbadakarba2000

References

https://www.microsoft.com/en-us/security/blog/2026/05/19/exposing-fox-tempest-a-malware-signing-service-operation/

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 Demo of **HivePro**.

REPORT GENERATED ON

May 22, 2026 • 06:00 AM

More at www.hivepro.com