INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-20 13:50 UTC

Microsoft Dismantles Fox Tempest's Certificate Mill: How a Legitimate Signing Service Became Ransomware Infrastructure

THREAT CAMPAIGN | HIGH | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0344
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Microsoft Azure Artifact Signing (formerly Trusted Signing); Windows OS code-signing trust chain; malware impersonating Microsoft Teams, AnyDesk, PuTTY, Webex; organizations targeted by Rhysida, Akira, INC, Qilin, and BlackByte ransomware
Published	2026-05-19T17:47:31
Discovery Source	Rss

Executive Summary

Microsoft's Digital Crimes Unit dismantled Fox Tempest, a criminal service that abused Microsoft's Azure Artifact Signing platform to issue over 1,000 fraudulent code-signing certificates to ransomware operators including Rhysida, Akira, INC, Qilin, and BlackByte. Signed malware impersonating Microsoft Teams, AnyDesk, PuTTY, and Webex bypassed Windows code-signing trust controls, allowing ransomware payloads to appear as legitimate software to endpoints and security tools. Microsoft seized the signspace[.]cloud domain, took hundreds of virtual machines offline, and filed a federal civil lawsuit, but organizations that executed any of these signed payloads before the takedown remain at risk of active ransomware compromise.

Technical Analysis

Fox Tempest operated a malware-signing-as-a-service (MSaaS) platform by exploiting the low identity-verification threshold of Azure Artifact Signing's Public Trust Certificate profile. This profile allowed threat actors to obtain Microsoft-rooted, Authenticode-valid signatures without adequate subscriber vetting, directly abusing CWE-346 (Origin Validation Error), CWE-290 (Authentication Bypass by Spoofing), and CWE-347 (Improper Verification of Cryptographic Signature). Signed payloads impersonated Microsoft Teams, AnyDesk, PuTTY, and Webex, passing Windows SmartScreen and Authenticode trust checks. MITRE ATT&CK techniques observed: T1553.002 (Code Signing), T1036.005 (Match Legitimate Name or Location), T1036.001

(Invalid Code Signature), T1588.003 (Obtain Capabilities: Code Signing Certificates), T1588.004 (Obtain Capabilities: Digital Certificates), T1583.001 (Acquire Infrastructure: Domains), T1204.002 (User Execution: Malicious File), T1486 (Data Encrypted for Impact), and T1195 (Supply Chain Compromise). No CVE has been assigned; the root issue is a policy and vetting gap in the signing service, not a software vulnerability. Microsoft revoked the fraudulent certificates and took the signing infrastructure offline. Organizations should treat any recently executed signed binary impersonating the above applications as potentially compromised until verified.

Action Checklist

1. Containment: Block the signspace[.]cloud domain at DNS, proxy, and firewall layers immediately. Isolate any endpoint that executed a signed binary impersonating Microsoft Teams, AnyDesk, PuTTY, or Webex within the past 90 days pending forensic review. Per NIST IR-4, activate your incident response plan if any ransomware-affiliated IOCs are confirmed in your environment.
2. Detection: Query endpoint detection logs for Authenticode-signed binaries with certificate issuers referencing Azure Artifact Signing or Microsoft Trusted Signing where the signing account is not an internally approved publisher. Search EDR telemetry for T1036.005 indicators: binaries named teams.exe, anydesk.exe, putty.exe, or webex.exe executing from non-standard paths (e.g., %TEMP%, %APPDATA%, user-writable directories). Correlate against SIEM logs for process creation events from these binaries. Apply NIST SI-4 (System Monitoring) and AU-6 (Audit Record Review) to prioritize log review. Reference CIS 8.2 for audit log collection coverage validation.
3. Eradication: Revoke trust in any internally issued code-signing certificates that used the Azure Artifact Signing Public Trust Certificate profile if your organization operates a certificate issuance infrastructure. Remove all identified malicious binaries from endpoints. Review and update application allowlisting rules (NIST SI-3, Malicious Code Protection) to require publisher identity validation beyond certificate chain alone; certificate thumbprint matching is required. Apply NIST SI-7 (Software, Firmware, and Information Integrity) to audit executable integrity on affected hosts.
4. Recovery: Re-image any endpoint confirmed to have executed a Fox Tempest-signed payload. Validate that CrowdStrike, Defender, or your AV platform has updated signatures covering the revoked certificate hashes before restoring to production. Monitor for Rhysida, Akira, INC, Qilin, and BlackByte post-compromise behaviors (lateral movement, Volume Shadow Copy deletion, large outbound transfers) for 30 days post-remediation per NIST IR-5 (Incident Monitoring). Confirm signspace[.]cloud is blocked and verify no DNS resolution is occurring across all egress points.
5. Post-Incident: Conduct a lessons-learned review focused on three control gaps: (1) code-signing trust policy, evaluate whether your application control solution validates certificate thumbprints, not just chain validity (addresses CWE-347); (2) software inventory coverage, confirm CIS 2.1 (Software Inventory) captures all executables, including those delivered via user-initiated downloads impersonating approved tools; (3) publisher verification process, establish an internal approved-publisher list and enforce it via NIST SI-7 (Software, Firmware, and Information Integrity) integrity verification tooling. Apply NIST IA-5 (Authentication and Identification) controls to any signing credentials your organization controls.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to executive leadership, legal counsel, and external IR retainer immediately if any endpoint confirmed to have executed a Fox Tempest-signed payload shows evidence of lateral movement, credential harvesting (e.g., LSASS access via Sysmon Event ID 10), Volume Shadow Copy deletion, or large outbound data transfers exceeding your DLP thresholds — these behaviors indicate active Rhysida, Akira, INC, Qilin, or BlackByte ransomware deployment, triggering breach notification obligations under GDPR, HIPAA, and applicable U.S. state data breach statutes if PII or PHI is present on affected systems.
Recovery Notes	Re-image all confirmed-compromised endpoints from a known-good baseline rather than attempting in-place remediation, as Fox Tempest-signed payloads delivering Rhysida, Akira, INC, Qilin, or BlackByte ransomware may have established persistence mechanisms (scheduled tasks, registry run keys, WMI subscriptions) that survive binary removal alone. Before returning any system to production, validate that Microsoft Defender or your AV platform has ingested the updated revocation data for Fox Tempest-issued Azure Artifact Signing certificates and confirm signspace[.]cloud is unresolvable from all restored endpoints and egress points. Maintain elevated monitoring for all five ransomware affiliate TTPs — particularly VSS deletion (vssadmin delete shadows), credential dumping (LSASS access), and bulk SMB file access — for a minimum of 30 days post-recovery, as ransomware operators frequently maintain secondary access footholds or pre-position encryption routines ahead of the primary deployment event.
Forensic Artifacts	Authenticode signature metadata extracted via sigcheck.exe or Get-AuthenticodeSignature from binaries in %TEMP%, %APPDATA%, %LOCALAPPDATA%, Downloads, and Desktop directories — specifically the Issuer field referencing Azure Artifact Signing or Microsoft Trusted Signing with a Subject that does not match legitimate Microsoft Corporation or the real AnyDesk GmbH, PuTTY, or Cisco Webex publisher identities, enabling identification of Fox Tempest-fraudulent certificates distinct from legitimate vendor signatures. | Windows Prefetch files (C:\Windows\Prefetch\TEAMS.EXE-*.pf, ANYDESK.EXE-*.pf, PUTTY.EXE-*.pf, WEBEX.EXE-*.pf) providing first- and last-execution timestamps and referenced DLL paths for impersonating binaries, even after the binaries themselves have been deleted — parse with WinPrefetchView or PECmd from Eric Zimmerman's toolkit. | AmCache.hve registry hive (C:\Windows\AppCompat\Programs\Amcache.hve) and SYSTEM hive AppCompatCache (ShimCache) entries for the impersonating binary names, capturing SHA-1 hashes and first-execution timestamps that can be correlated against Fox Tempest certificate validity periods to establish whether execution occurred before or after Microsoft's revocation action. | Windows DNS Client Operational event log (Microsoft-Windows-DNS-Client/Operational) and host-based firewall logs for resolution attempts or blocked connections to signspace[.]cloud — the Fox Tempest infrastructure domain — providing evidence of C2 callback attempts by Rhysida, Akira, INC, Qilin, or BlackByte staging payloads downloaded via the fraudulent signing service. | Volume Shadow Copy enumeration output (vssadmin list shadows) and Windows System Event Log entries for VSS service state changes (Event ID 7036) combined with Sysmon Event ID 1 process creation records for vssadmin.exe, wbadmin.exe, or WMIC with 'shadowcopy delete' arguments — the presence of VSS deletion activity is a high-confidence indicator that a ransomware affiliate progressed beyond initial access to active encryption staging on the affected host.

Per-Action IR Details

Containment — Block the signspace[.]cloud domain at DNS, proxy, and firewall layers immediately. Isolate any endpoint that executed a signed binary impersonating Microsoft Teams, AnyDesk, PuTTY, or Webex within the past 90 days pending forensic review. Per NIST IR-4, invoke your incident handling capability now if any ransomware-affiliated IOCs are confirmed in your environment.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: On Windows endpoints without EDR, run the following PowerShell to identify binaries matching the impersonation targets executed from non-standard paths within 90 days: Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4688 -and $_.Message -match 'teams.exe|anydesk.exe|putty.exe|webex.exe'} | Where-Object {$_.Message -notmatch 'Program Files'}. For DNS blocking on a budget, add signspace[.]cloud to the Windows hosts file (C:\Windows\System32\drivers\etc\hosts) pointing to 0.0.0.0 and configure pi-hole or pfSense DNS resolver block lists at the perimeter. Document all isolated endpoints with a chain-of-custody timestamp before any remediation action.

Evidence: Before isolating endpoints, capture: (1) full memory dump of any process associated with the impersonating binary using ProcDump (sysinternals) — e.g., procdump.exe -ma — to preserve in-memory ransomware staging artifacts from Rhysida, Akira, INC, Qilin, or BlackByte payloads; (2) Windows Security Event Log Event ID 4688 (Process Creation) filtered on teams.exe, anydesk.exe, putty.exe, webex.exe with full command-line logging enabled; (3) DNS query logs or Windows DNS Client event log (Microsoft-Windows-DNS-Client/Operational) for any resolution of signspace[.]cloud; (4) Prefetch files from C:\Windows\Prefetch\ for the impersonating binary names to establish first- and last-execution timestamps; (5) AmCache.hve and ShimCache (SYSTEM hive AppCompatCache) entries for the impersonating executables to confirm execution history even if binaries have since been deleted.

Detection — Query endpoint detection logs for Authenticode-signed binaries with certificate issuers referencing Azure Artifact Signing or Microsoft Trusted Signing where the signing account is not an internally approved publisher. Search EDR telemetry for T1036.005 indicators: binaries named teams.exe, anydesk.exe, putty.exe, or webex.exe executing from non-standard paths (e.g., %TEMP%, %APPDATA%, user-writable directories). Correlate against SIEM logs for process creation events from these binaries. Apply NIST SI-4 (System Monitoring) and AU-6 (Audit Record Review) to prioritize log review. Reference CIS 8.2 for audit log collection coverage validation.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST AU-3 (Content of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Without EDR, deploy Sysmon with a configuration that captures Event ID 1 (Process Create) and Event ID 7 (Image Load) — use the SwiftOnSecurity Sysmon config as a baseline and add rules filtering on Image paths containing \Temp\, \AppData\, or \Downloads\ for teams.exe, anydesk.exe, putty.exe, webex.exe. To inspect Authenticode certificate metadata without EDR, run: Get-AuthenticodeSignature -FilePath | Select-Object -ExpandProperty SignerCertificate | Format-List Subject,Issuer,Thumbprint — flag any result where Issuer contains 'Microsoft Identity Verification Root Certificate Authority' or 'Trusted Signing' but the Subject does not match your internal approved publisher list. Write a YARA rule targeting the certificate serial numbers associated with Fox Tempest-issued certs once Microsoft publishes the revocation list, and scan with YARA against all executables in user-writable directories.

Evidence: Before concluding detection scope: (1) Extract Authenticode signature metadata from all binaries in %TEMP%, %APPDATA%, %LOCALAPPDATA%, Downloads, and Desktop paths using sigcheck.exe (Sysinternals) with output to CSV — sigcheck.exe -c -s — and filter for issuers referencing Azure Artifact Signing or Trusted Signing with non-internal publisher subjects; (2) Pull Windows Application and Services Logs > Microsoft > Windows > CodeIntegrity > Operational (Event ID 3033, 3034, 3077) to identify binaries that triggered code integrity failures or warnings prior to execution; (3) Review browser download history (Chrome: %LOCALAPPDATA%\Google\Chrome\User Data\Default\History SQLite DB; Edge: %LOCALAPPDATA%\Microsoft\Edge\User Data\Default\History) for downloads of files named teams, anydesk, putty, or webex from non-official domains in the 90-day window; (4) Check Windows Defender scan history logs at C:\ProgramData\Microsoft\Windows Defender\Support\MPLog-*.log for detections or scan skips on Authenticode-signed files; (5) Query Sysmon Event ID 7 (ImageLoad) for DLLs loaded by the impersonating process to

identify ransomware-specific modules or injected code.

Eradication — Revoke trust in any internally issued code-signing certificates that used the Azure Artifact Signing Public Trust Certificate profile if your organization operates a signing pipeline. Remove all identified malicious binaries from endpoints. Review and update application allowlisting rules (NIST SI-3, Malicious Code Protection) to require publisher identity validation beyond certificate chain alone — certificate thumbprint matching is required. Apply D3-SFA (System File Analysis) to audit executable integrity on affected hosts.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-3 (Malicious Code Protection), NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-3 (Configuration Change Control), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 2.3 (Address Unauthorized Software)

Compensating: For teams without enterprise application control, use Windows Defender Application Control (WDAC) or AppLocker (available on Windows 10/11 Pro and Enterprise at no cost) to enforce publisher rules requiring exact certificate thumbprint match rather than chain trust alone — in WDAC policy XML, set the element with a specific TBS hash value rather than a root-trust rule. To remove Fox Tempest-signed binaries at scale without EDR, run: Get-ChildItem -Path C:\Users -Recurse -Include teams.exe,anydesk.exe,putty.exe,webex.exe -ErrorAction SilentlyContinue | Where-Object {(Get-AuthenticodeSignature $_.FullName).SignerCertificate.Issuer -match 'Trusted Signing'} | Remove-Item -Force. Verify removal with a post-deletion hash audit using Get-FileHash. Run ClamAV with an updated database against user-writable directories on Linux-adjacent or cross-platform systems in the environment.

Evidence: Before eradicating binaries: (1) Collect full binary copies of all identified Fox Tempest-signed malicious executables to a forensic evidence store with SHA-256 hash documentation — use: Get-FileHash -Algorithm SHA256; (2) Export the full certificate chain from each malicious binary using certutil -dump or sigcheck -i to capture the Fox Tempest-issued certificate serial number, thumbprint, and validity period for IOC sharing and internal revocation records; (3) Capture registry run key persistence entries that the ransomware affiliates (Rhysida, Akira, INC, Qilin, BlackByte) commonly use — HKCU\Software\Microsoft\Windows\CurrentVersion\Run, HKLM\Software\Microsoft\Windows\CurrentVersion\Run — and document any entries referencing the impersonating binary paths; (4) Export scheduled task XML definitions from C:\Windows\System32\Tasks\ and query via schtasks /query /fo LIST /v for tasks pointing to user-writable paths or referencing the impersonating binary names; (5) Capture Volume Shadow Copy status with vssadmin list shadows before eradication to determine if ransomware pre-staged VSS deletion, preserving evidence of attempted or completed shadow deletion.

Recovery — Re-image any endpoint confirmed to have executed a Fox Tempest-signed payload. Validate that CrowdStrike, Defender, or your AV platform has updated signatures covering the revoked certificate hashes before restoring to production. Monitor for Rhysida, Akira, INC, Qilin, and BlackByte post-compromise behaviors (lateral movement, Volume Shadow Copy deletion, large outbound transfers) for 30 days post-remediation per NIST IR-5 (Incident Monitoring). Confirm signspace[.]cloud is blocked and verify no DNS resolution is occurring across all egress points.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-5 (Incident Monitoring), NIST CP-10 (System Recovery and Reconstitution), NIST SI-3 (Malicious Code Protection), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Without CrowdStrike or enterprise AV management, verify Microsoft Defender signature currency via PowerShell on each restored endpoint: Get-MpComputerStatus | Select-Object AntivirusSignatureLastUpdated,AntivirusSignatureVersion — confirm the signature date is post-Microsoft's revocation action for Fox Tempest certificates. To monitor for Rhysida, Akira, INC, Qilin, and BlackByte lateral movement post-restoration without SIEM, deploy Sysmon Event ID 3 (Network Connect) and configure alerts for SMB connections (port 445) originating from newly restored endpoints to non-standard destinations. Monitor for VSS deletion attempts using Windows System Event Log Event ID 7036 filtered on VSS service state changes, and alert on execution of

vssadmin.exe, wbadmin.exe, or wmic with shadowcopy delete arguments via Sysmon Event ID 1. Confirm DNS blocking by running Resolve-DnsName signspace.cloud from each restored endpoint and verifying it returns no valid IP.

Evidence: Before returning any endpoint to production: (1) Confirm clean re-image by validating OS build hash against a known-good baseline — document with Get-ComputerInfo | Select-Object OsName,OsVersion,OsBuildNumber; (2) Run a full sigcheck scan of the restored system's Program Files and user-accessible directories to confirm no Fox Tempest-issued Authenticode signatures remain: sigcheck.exe -c -r -s C:\Users > post_reimage_sigcheck.csv; (3) Verify network egress logs (firewall or proxy) show zero DNS resolution or HTTP/S connection attempts to signspace[.]cloud from the restored endpoint for a minimum 72-hour observation window before sign-off; (4) Confirm VSS snapshot availability post-recovery with vssadmin list shadows to ensure ransomware staging did not complete shadow deletion during the dwell period; (5) Capture a baseline Autoruns snapshot (autoruns.exe -a * -c > baseline_autoruns.csv) immediately post-reimage to enable future delta comparison if the endpoint shows re-infection indicators during the 30-day monitoring window.

Post-Incident — Conduct a lessons-learned review focused on three control gaps: (1) code-signing trust policy — evaluate whether your application control solution validates certificate thumbprints, not just chain validity (addresses CWE-347); (2) software inventory coverage — confirm CIS 2.1 (Software Inventory) captures all executables, including those delivered via user-initiated downloads impersonating approved tools; (3) publisher verification process — establish an internal approved-publisher list and enforce it via NIST SI-7 (Software, Firmware, and Information Integrity) integrity verification tooling. Apply D3-CH (Credential Hardening) to any signing credentials your organization controls.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST SI-7 (Software, Firmware, and Information Integrity), NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-2 (Flaw Remediation), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: To build an approved-publisher list without enterprise tooling, generate a reference CSV of thumbprints from all legitimate installed executables using sigcheck.exe -c -s C:\Program Files > approved_publishers_baseline.csv and review against known-good vendor thumbprints documented on vendor websites. For ongoing integrity monitoring, deploy osquery with a file_events query against user-writable paths to detect new Authenticode-signed executables that do not match the approved thumbprint baseline. For signing credential hardening without a PAM solution, rotate any Azure Artifact Signing service principal credentials immediately, enforce MFA on the associated Azure AD account, restrict signing pipeline service principals to the minimum required Azure RBAC role, and audit the Azure Activity Log for any unauthorized certificate issuance events under the Trusted Signing resource provider. Write a Sigma rule targeting process creation events where Image matches known impersonation names but ParentImage does not match the legitimate installer path, and deploy via Windows Event Forwarding to a central log collector.

Evidence: For the lessons-learned record: (1) Compile the full timeline of Fox Tempest-signed binary execution events from Prefetch, AmCache, and Security Event Log 4688 records across all affected endpoints to establish initial access dwell time; (2) Document all certificate thumbprints and serial numbers from recovered malicious binaries and cross-reference against Microsoft's published revocation data to confirm complete eradication scope; (3) Preserve browser download history artifacts and any phishing or social engineering artifacts (emails, chat messages referencing fake Teams/AnyDesk/PuTTY/Webex installers) that established the initial delivery vector — store in case management system with chain of custody; (4) Export the Azure Activity Log (if the organization uses Azure Artifact Signing) covering the 90-day window to confirm whether any internal service principals were enumerated or misused by Fox Tempest-affiliated actors; (5) Document the detection gap — specifically, the time delta between first execution of a Fox Tempest-signed binary and first alert — to quantify the detection latency that CWE-347 (Improper Verification of Cryptographic Signature) introduced into the environment's trust model.

Detection Guidance

Primary detection focus: Authenticode-signed binaries whose certificate chain terminates in Microsoft's Azure Artifact Signing (formerly Trusted Signing) intermediate CA, where the subscriber identity does not match an internally approved publisher list. Key indicators: (1) Binaries named to match Microsoft Teams, AnyDesk, PuTTY, or Webex executing from user-writable paths (%TEMP%, %APPDATA%, Downloads, Desktop), flag via EDR process creation logs. (2) Outbound DNS or HTTP connections to signspace[.]cloud, query proxy, DNS resolver, and firewall logs. (3) Windows Event Log: Event ID 8003 or 8004 from source MSISERVER, or AppLocker/WDAC audit events showing signed-but-not-whitelisted binaries. (4) Signtool or certificate inspection revealing issuer 'Microsoft ID Verified CS EOC CA 01' or related Azure Artifact Signing intermediates on unexpected binaries. (5) EDR behavioral alerts consistent with T1486 (ransomware encryption activity), T1036.005 (masquerading), or credential access following execution of any of the named impersonation payloads. IOC cross-reference: signspace[.]cloud (seized but monitor for DNS lookups indicating pre-takedown infections still beaconing). Apply NIST AU-6 review cadence and SI-4 monitoring controls to prioritize these log sources. CIS 8.2 audit log coverage should extend to endpoint process execution and DNS query logs.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`signspace[.]cloud`	Primary infrastructure domain operated by Fox Tempest for the malware-signing-as-a-service platform; seized by Microsoft DCU	HIGH

Framework Mappings

MITRE-ATTACK

- **T1588.004** — Digital Certificates
- **T1486** — Data Encrypted for Impact
- **T1553.002** — Code Signing
- **T1588.003** — Code Signing Certificates
- **T1583.001** — Domains
- **T1204.002** — Malicious File
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1195** — Supply Chain Compromise
- **T1036.001** — Invalid Code Signature

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan

- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **IR-4** — Incident Handling
- **AT-2** — Literacy Training and Awareness
- **SC-13** — Cryptographic Protection

NIST-CSF-2

- **RS.MI-01** — Incidents are contained

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.23** — Information security for use of cloud services

CIS-V8

- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1588.004	Digital Certificates	Resource-Development
T1486	Data Encrypted for Impact	Impact
T1553.002	Code Signing	Defense-Evasion
T1588.003	Code Signing Certificates	Resource-Development
T1583.001	Domains	Resource-Development
T1204.002	Malicious File	Execution
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1195	Supply Chain Compromise	Initial-Access
T1036.001	Invalid Code Signature	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/cybercrime-service-d...	T3

Source	URL	Tier
Azure Artifact Signing (formerly Trusted Signing)	https://azure.microsoft.com/en-us/products/artifact-signing	T1
Malware Using Microsoft Trusted Certificates Found in Wild	https://www.ampcuscyber.com/shadowopsintel/malware-signed-with-micr...	T3
Artifact Signing Account with Public Trust Certificate Profile and ...	https://learn.microsoft.com/en-us/answers/questions/5855805/artifac...	T1
Code signing on Windows with Azure Artifact Signing - Sine Machine	https://melatonin.dev/blog/code-signing-on-windows-with-azure-trust...	T3

Generated 2026-05-20 13:50 UTC by TJS Security Command Center