INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-30 19:07 UTC

Fox Tempest Dismantled: Microsoft-Signed Malware-as-a-Service Operation

THREAT ACTOR | CRITICAL | CVSS 9.0

SCC Item ID	SCC-TAC-2026-0021
Type	Threat Actor
Severity	CRITICAL
CVSS Base Score	9.0
Affected Products	Microsoft code signing infrastructure; organizations targeted via Rhysida ransomware, Lumma Stealer, and Vidar deployments
Published	2026-05-29
Discovery Source	Gemini

Executive Summary

Microsoft disrupted Fox Tempest, a cybercriminal operation that fraudulently obtained Microsoft code-signing certificates and resold them to threat actors deploying Rhysida ransomware, Lumma Stealer, and Vidar infostealer. The signed malware bypassed endpoint security controls on thousands of machines before takedown, enabling ransomware attacks on hospitals and critical infrastructure alongside large-scale credential theft. Microsoft has revoked the fraudulent certificates, but organizations must audit their environments for prior compromise and harden certificate validation processes immediately.

Technical Analysis

Fox Tempest operated 'OpFauxSign' from approximately May 2025 through May 2026, fraudulently obtaining Microsoft Artifact Signing certificates and selling them to downstream threat actors for $5,000-$9,000 each. The fraudulent certificates satisfied Windows Authenticode trust chain validation (CWE-295: Improper Certificate Validation; CWE-347: Improper Verification of Cryptographic Signature), allowing malicious binaries to appear legitimately signed and bypass EDR tools and Windows Smart App Control. Downstream payloads included Rhysida ransomware (T1486: Data Encrypted for Impact), Lumma Stealer and Vidar infostealers (T1555: Credentials from Password Stores), delivered via phishing (T1566) and user execution (T1204). Fox Tempest obtained signing certificates through fraudulent means (T1588.003: Code Signing Certificates), applied them to embedded malicious code (T1553.002: Code Signing; CWE-506: Embedded Malicious Code), and exfiltrated data via encrypted channels (T1041: Exfiltration Over C2 Channel). No CVE is assigned; the attack vector is trust-chain abuse rather than a software vulnerability. Microsoft revoked all identified fraudulent certificates as part of the takedown. No vendor patch applies, remediation is detection- and policy-based.

Action Checklist

1. Step 1: Containment, Query your EDR and AV platforms for binaries signed by Microsoft certificates issued between May 2025 and May 2026 that have since been revoked. Isolate any hosts where revoked-certificate binaries executed. Cross-reference Microsoft's published revocation list from their May 19, 2026 security blog (Tier 1 source: https://www.microsoft.com/en-us/security/blog/2026/05/19/exposing-fox-tempest-a-malware-signing-service-operation/). Block execution of binaries with revoked Authenticode signatures at the endpoint policy layer.
2. Step 2: Detection, Search Windows Event Logs for Event ID 8028 (SmartScreen blocked a revoked certificate) and Event ID 4688 (process creation) where the signing certificate subject matches Fox Tempest-associated certificate thumbprints published by Microsoft. Query your SIEM for Lumma Stealer and Vidar behavioral indicators: outbound POST requests to randomized domains over 443/80, access to browser credential stores (AppData\Local\Google\Chrome\User Data\Default\Login Data), and Rhysida ransomware artifacts including .rhysida extension and dropped ransom notes. Reference MITRE ATT&CK T1555 and T1486 detection guidance. Apply CIS 8.2 (Collect Audit Logs) to confirm logging is active across endpoints.
3. Step 3: Eradication, Remove any identified malicious binaries signed with revoked Fox Tempest certificates. For hosts with confirmed Rhysida, Lumma, or Vidar activity: reimage from a known-clean baseline rather than attempting in-place cleanup. Rotate all credentials on affected systems per NIST AC-2 (Account Management) and D3-CRO (Credential Rotation). Revoke and reissue any API keys, service account tokens, or certificates stored on compromised hosts. Apply D3-CH (Credential Hardening) to reduce reuse risk.
4. Step 4: Recovery, Verify no revoked-certificate binaries remain in startup locations, scheduled tasks, or service entries (NIST SI-4, D3-SICA: System Init Config Analysis). Confirm EDR telemetry shows no further suspicious signed-binary execution. Monitor for reinfection indicators over 30 days: anomalous outbound connections, credential-store access patterns, and new scheduled tasks created by non-administrative accounts. Validate that Windows certificate revocation checking (CRL/OCSP) is enforced and not bypassed at the endpoint or network proxy level.
5. Step 5: Post-Incident, Conduct a gap review against NIST CM-7 (Least Functionality) and AC-6 (Least Privilege) to restrict which processes can install or execute newly signed software. Implement application allowlisting (NIST SI-7: Software, Firmware, and Information Integrity) to prevent unsigned or newly signed binaries from executing without explicit approval. Review CIS 2.1 (Software Inventory) and CIS 2.3 (Address Unauthorized Software) compliance, Fox Tempest succeeded in part because signed malware was treated as implicitly trusted. Establish a process to ingest Microsoft certificate revocation notices as a threat intelligence feed.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to senior IR leadership, legal counsel, and executive stakeholders if any host with confirmed Lumma Stealer or Vidar activity is found to have stored PHI, PII, financial data, or privileged credentials — Fox Tempest-facilitated credential theft triggers HIPAA breach notification (45 CFR §164.400), state privacy law obligations, and potential SEC disclosure requirements if a publicly traded entity is affected; also escalate if Rhysida ransomware activity is confirmed on any operational technology or healthcare system, given the threat actor's documented targeting of hospitals and critical infrastructure.
Recovery Notes	Before returning any host to production, validate the full Authenticode chain for all executables in startup paths, scheduled tasks, and installed services against Microsoft's current CTL (Certificate Trust List) using 'certutil -verify -urlfetch ' — do not rely solely on EDR verdicts, as Fox Tempest-signed binaries were specifically designed to pass signature validation. Monitor all recovered hosts and associated user accounts for 30 days post-eradication using behavioral baselines focused on credential-store access, outbound POST volume to new domains, and shadow copy deletion attempts, given Lumma/Vidar's known capability to persist via harvested credentials and enable secondary Rhysida ransomware deployment. Any detection of .rhysida file extension creation, vssadmin shadow deletion, or bulk file modification on a recovered host during the monitoring window should trigger immediate re-isolation and a full reimaging cycle.
Forensic Artifacts	Authenticode signature metadata for all binaries executed during May 2025–May 2026: extract via 'sigcheck -c -h -s' (Sysinternals) and cross-reference thumbprints against Microsoft's Fox Tempest revocation list — this directly maps which binaries on your estate were Fox Tempest-signed and bypassed endpoint controls | Windows Prefetch and Amcache entries (C:\Windows\Prefetch*.pf and C:\Windows\AppCompat\Programs\Amcache.hve) for Rhysida dropper, Lumma Stealer, and Vidar executables — these persist execution evidence even after the malicious binaries have been deleted post-infection | Browser credential store access timestamps and shadow copies of %LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data, \Cookies, \Web Data, and equivalent Firefox (logins.json, key4.db) and Edge paths — Lumma Stealer and Vidar specifically target these files and leave file-access timestamp artifacts that establish the credential theft timeline | Volume Shadow Copy metadata and Windows Event ID 4688 command-line logs for 'vssadmin delete shadows', 'wmic shadowcopy delete', and 'bcdedit /set recoveryenabled No' — Rhysida consistently deletes shadow copies as a pre-encryption step, and this artifact sequence establishes the ransomware execution timeline with forensic precision | Network proxy and DNS logs for outbound POST requests to high-entropy domains over ports 443 and 80 originating from Fox Tempest-signed process names during the exposure window — Lumma Stealer and Vidar use this C2 communication pattern, and correlating process name, signing certificate thumbprint, and destination domain establishes the full infection-to-exfiltration chain

Per-Action IR Details

Step 1: Containment — Query your EDR and AV platforms for binaries signed by Microsoft certificates issued between May 2025 and May 2026 that have since been revoked. Isolate any hosts where revoked-certificate binaries executed. Cross-reference Microsoft's published revocation list from their May 2026 security blog (Tier 1 source: microsoft.com/en-us/security/blog/2026/05/19/exposing-fox-tempest-a-malware-signing-service-operation/). Block execution of binaries with revoked Authenticode signatures at the endpoint policy layer.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy (CSF RS.MA-01: Execute IR plan, contain, mitigate)

Controls: NIST IR-4 (Incident Handling), NIST SI-3 (Malicious Code Protection), NIST CM-7 (Least Functionality), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Without EDR, use Sysinternals Sigcheck to enumerate signed binaries on hosts: 'sigcheck -c -h -s C:\Windows\System32 > sigcheck_output.csv' then filter output against the Fox Tempest revoked thumbprint list from Microsoft's advisory. Automate across the estate with a PowerShell loop: 'Get-AuthenticodeSignature -FilePath | Where-Object {$_.Status -eq "Revoked"}'. For network-level blocking, configure Windows Defender Application Control (WDAC) or Software Restriction Policies to deny execution of binaries with revoked Authenticode signatures — no SIEM required.

Evidence: Before isolating hosts, capture: (1) Prefetch files from C:\Windows\Prefetch\ for any revoked-certificate binaries to establish first/last execution timestamps; (2) Shimcache and Amcache registry entries at HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache and C:\Windows\AppCompat\Programs\Amcache.hve to confirm binary execution even if the file has been deleted; (3) Windows Event Log Security channel for Event ID 4688 filtered on processes with revoked Authenticode signatures; (4) $MFT and $UsnJrnl entries for Fox Tempest-signed binary file creation timestamps to establish the initial compromise window.

Step 2: Detection — Search Windows Event Logs for Event ID 8028 (SmartScreen blocked a revoked certificate) and Event ID 4688 (process creation) where the signing certificate subject matches Fox Tempest-associated certificate thumbprints published by Microsoft. Query your SIEM for Lumma Stealer and Vidar behavioral indicators: outbound POST requests to randomized domains over 443/80, access to browser credential stores (AppData\Local\Google\Chrome\User Data\Default\Login Data), and Rhysida ransomware artifacts including .rhysida extension and dropped ransom notes. Reference MITRE ATT&CK T1555 and T1486 detection guidance. Apply CIS 8.2 (Collect Audit Logs) to confirm logging is active across endpoints.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis (CSF DE.AE-02, DE.AE-03, DE.AE-07: Analyze adverse events, correlate sources, integrate CTI)

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

Compensating: Without a SIEM, deploy Sysmon with a config that captures ProcessCreate (Event ID 1), FileCreate (Event ID 11), and NetworkConnect (Event ID 3) events. Use the following PowerShell to hunt Lumma/Vidar credential-store access: 'Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" | Where-Object {$_.Message -like "*Login Data*"}'. For Rhysida, hunt .rhysida file extension creation: 'Get-WinEvent -FilterHashtable @{LogName="Microsoft-Windows-Sysmon/Operational"; Id=11} | Where-Object {$_.Message -like "*.rhysida*"}'. Apply the publicly available Sigma rule for T1486 (sigma-rules repo: ransomware_file_encryption) converted to Evtx query format for offline log analysis with tools like Chainsaw or Hayabusa.

Evidence: Capture before full triage: (1) Sysmon Event ID 3 (NetworkConnect) records showing outbound POST connections from processes matching Fox Tempest-signed binary names to high-entropy randomized domains — characteristic of Lumma Stealer and Vidar C2 beaconing; (2) VSS shadow copy metadata to determine if Rhysida deleted volume shadow copies via vssadmin or wmic (Event ID 4688 with command-line 'vssadmin delete shadows'); (3) Browser credential store file access timestamps at %LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data and equivalent Firefox/Edge paths, cross-referenced with process access tokens (Sysmon Event ID 10, ProcessAccess); (4) Windows Application Event Log entries for SmartScreen Event ID 8028 confirming revoked-certificate execution attempts that were blocked versus those that were not.

Step 3: Eradication — Remove any identified malicious binaries signed with revoked Fox Tempest certificates. For hosts with confirmed Rhysida, Lumma, or Vidar activity: reimage from a known-clean baseline rather than attempting in-place cleanup. Rotate all credentials on affected systems per NIST AC-2 (Account Management) and D3-CRO (Credential Rotation). Revoke and reissue any API keys, service account tokens, or certificates stored on compromised hosts. Apply D3-CH (Credential Hardening) to reduce reuse risk.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication (CSF RS.MA-01: Remove threat from environment, verify eradication)

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST IA-5 (Authenticator Management), NIST SI-2 (Flaw Remediation), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: For teams without enterprise credential management, use the following sequence: (1) Run 'net user /domain' and 'Get-ADUser -Filter {LastLogonDate -lt (Get-Date).AddDays(-45)}' to identify and disable dormant accounts that Lumma/Vidar may have harvested and could be replayed; (2) Force password reset for all accounts present on confirmed-compromised hosts via 'Set-ADAccountPassword' in bulk PowerShell; (3) For API keys and service tokens, enumerate credential files with: 'Get-ChildItem -Recurse -Include *.env,*.config,*.json | Select-String -Pattern "(api_key|token|secret|password)"' on affected hosts before reimaging; (4) Reimaging is non-negotiable for Rhysida-confirmed hosts — infostealer-only hosts (Lumma/Vidar) may be considered for forensic retention before wipe if legal hold applies.

Evidence: Before reimaging, capture full disk images of confirmed Rhysida hosts using a write-blocked imaging tool (FTK Imager free tier or dc3dd) to preserve encrypted file artifacts, ransom note contents, and Rhysida dropper persistence mechanisms. Document all scheduled tasks, services, and Run key entries created by Fox Tempest-signed binaries: 'schtasks /query /fo LIST /v > schtasks_pre_eradication.txt' and 'reg export HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run run_keys.reg'. Capture a memory image (WinPmem) on hosts with active Lumma/Vidar processes before termination — infostealer malware frequently holds decrypted credential material in heap memory that is unrecoverable post-reimage.

Step 4: Recovery — Verify no revoked-certificate binaries remain in startup locations, scheduled tasks, or service entries (NIST SI-4, D3-SICA: System Init Config Analysis). Confirm EDR telemetry shows no further suspicious signed-binary execution. Monitor for reinfection indicators over 30 days: anomalous outbound connections, credential-store access patterns, and new scheduled tasks created by non-administrative accounts. Validate that Windows certificate revocation checking (CRL/OCSP) is enforced and not bypassed at the endpoint or network proxy level.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery (CSF RC: Execute recovery plan, restore systems, verify integrity, communicate)

Controls: NIST SI-4 (System Monitoring), NIST CM-6 (Configuration Settings), NIST CP-10 (System Recovery and Reconstitution), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without EDR, validate CRL/OCSP enforcement via Group Policy: confirm 'HKLM\SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot\DisableRootAutoUpdate' is set to 0 and that no proxy is configured to strip OCSP responses. Use Autoruns (Sysinternals) to enumerate all startup locations, scheduled tasks, and services and filter output by 'VirusTotal' column for revoked-certificate binaries: 'autorunsc -a * -c -h -v -vt > autoruns_output.csv'. Monitor for Lumma/Vidar reinfection using a cron-scheduled osquery query checking for new processes accessing Chrome Login Data: 'SELECT name, path, cmdline FROM processes WHERE cmdline LIKE "%Login Data%"'.

Evidence: Post-recovery, retain and monitor: (1) Baseline Autoruns output from all recovered hosts as a configuration snapshot for 30-day delta comparison; (2) DNS query logs for 30 days post-recovery, specifically for high-entropy domain lookups consistent with Lumma/Vidar DGA-style C2 (query length >20 chars, no established reputation) — use passive DNS logging via Windows DNS debug logs or Pi-hole if enterprise DNS logging is unavailable; (3) Windows Security Event ID 4698 (scheduled task created) and 4702 (scheduled task updated) for any new tasks created by non-SYSTEM, non-administrative accounts post-recovery; (4) Certificate store audit logs confirming Fox Tempest thumbprints are present in the 'Untrusted Certificates' store: 'certutil -store Disallowed'.

Step 5: Post-Incident — Conduct a gap review against NIST CM-7 (Least Functionality) and AC-6 (Least Privilege) to restrict which processes can install or execute newly signed software. Implement application allowlisting (NIST SI-7: Software, Firmware, and Information Integrity) to prevent unsigned or newly signed binaries from executing without explicit approval. Review CIS 2.1 (Software Inventory) and CIS 2.3 (Address Unauthorized Software) compliance — Fox Tempest succeeded in part because signed malware was treated

as implicitly trusted. Establish a process to ingest Microsoft certificate revocation notices as a threat intelligence feed.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity (CSF GV, ID: Lessons learned, update policies, improve detection, share intelligence)

Controls: NIST CM-7 (Least Functionality), NIST AC-6 (Least Privilege), NIST SI-7 (Software, Firmware, and Information Integrity), NIST RA-3 (Risk Assessment), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 2.3 (Address Unauthorized Software)

Compensating: Implement WDAC (Windows Defender Application Control) in audit mode first using the Microsoft-recommended base policy, then enforce. For teams without commercial allowlisting tools, the free WDAC Wizard (from Microsoft) generates enforceable XML policies without licensing cost. To ingest Microsoft certificate revocation as a TI feed, write a weekly PowerShell script that queries the Microsoft Security Response Center (MSRC) API for certificate revocation advisories and automatically imports revoked thumbprints into the 'Disallowed' certificate store via 'certutil -addstore Disallowed '. Subscribe to the Microsoft Security Update Guide RSS feed as a zero-cost revocation alerting mechanism.

Evidence: For the lessons-learned review, compile: (1) A timeline correlating the Fox Tempest certificate issuance window (May 2025–May 2026) against your software installation logs (Windows Event ID 11707: product installed) to identify all signed software deployed during the exposure window that has not yet been investigated; (2) Application Compatibility Telemetry or Inventory logs showing all Authenticode-signed binaries executed during the window, exportable via 'Get-AppLockerFileInformation -EventLog -LogPath "Microsoft-Windows-AppLocker/EXE and DLL"'; (3) Documentation of which hosts had CRL/OCSP checking disabled or bypassed by SSL-inspecting proxies — this is a root-cause control gap that directly enabled Fox Tempest malware to execute without revocation alerts firing.

Detection Guidance

Primary detection pivot is Authenticode certificate validation status. Query endpoints and EDR telemetry for binaries that: (1) carry Microsoft Artifact Signing certificate chains issued May 2025-May 2026, and (2) appear on Microsoft's revocation list published with the Fox Tempest disclosure. Windows Event ID 4688 (process creation with full command line logging enabled) combined with certificate thumbprint matching is the most reliable host-based signal. For Lumma Stealer: look for processes accessing browser SQLite credential databases (Login Data, Cookies) outside of the browser process itself, and outbound encrypted traffic to short-lived domains with high entropy names. For Vidar: similar browser-store access patterns plus access to cryptocurrency wallet directories. For Rhysida ransomware: mass file rename events with .rhysida extension, VSS deletion (vssadmin.exe delete shadows), and dropped HTML ransom notes. Network-layer indicators include C2 beaconing patterns documented in Microsoft's May 19, 2026 Fox Tempest disclosure blog (https://www.microsoft.com/en-us/security/blog/2026/05/19/exposing-fox-tempest-a-malware-signing-service-operation/). Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) cadence to ensure these log sources are reviewed on a defined schedule. D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) are applicable countermeasures for ongoing detection.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	`[See Microsoft Security Blog 2026-05-19 for full IOC list]`	Microsoft published certificate thumbprints and binary hashes associated with Fox Tempest-signed malware in the Tier 1 disclosure. Retrieve directly from source to ensure accuracy.	HIGH
DOMAIN	`[See Microsoft Security Blog 2026-05-19 for C2 infrastructure indicators]`	C2 domains associated with Lumma Stealer, Vidar, and Rhysida deployments are listed in Microsoft's threat intelligence disclosure. Do not rely on third-party reproductions for IOC accuracy.	HIGH

Framework Mappings

MITRE-ATTACK

- **T1588.003** — Code Signing Certificates
- **T1555** — Credentials from Password Stores
- **T1486** — Data Encrypted for Impact
- **T1041** — Exfiltration Over C2 Channel
- **T1204** — User Execution
- **T1553.002** — Code Signing
- **T1566** — Phishing

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **SC-8** — Transmission Confidentiality and Integrity
- **SC-17** — Public Key Infrastructure Certificates
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A02:2021** — Cryptographic Failures
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **3.10** — Encrypt Sensitive Data in Transit
- **6.3** — Require MFA for Externally-Exposed Applications
- **8.2** — Collect Audit Logs

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **DE.CM-01** — Networks and network services are monitored

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(d)** — Person or Entity Authentication

ISO-27001-2022

- **A.5.29** — Information security during disruption

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1588.003	Code Signing Certificates	Resource-Development
T1555	Credentials from Password Stores	Credential-Access
T1486	Data Encrypted for Impact	Impact
T1041	Exfiltration Over C2 Channel	Exfiltration
T1204	User Execution	Execution
T1553.002	Code Signing	Defense-Evasion
T1566	Phishing	Initial-Access

Sources

Source	URL	Tier
Microsoft Takes Down Group Operating Ransomware ...	https://www.infosecurity-magazine.com/news/microsoft-takes-down-fox...	T3
Microsoft Takes Down Malware-Signing Service Behind ...	https://thehackernews.com/2026/05/microsoft-takes-down-malware-sign...	T3

Source	URL	Tier
Exposing Fox Tempest: A malware-signing service operation	https://www.microsoft.com/en-us/security/blog/2026/05/19/exposing-f...	T1
Microsoft dismantles Fox Tempest cybercrime platform tied ...	https://industrialcyber.co/ransomware/microsoft-dismantles-fox-temp...	T3
Microsoft disrupts cybercrime operation that hid behind ...	https://www.cybersecuritydive.com/news/microsoft-disrupts-cybercrim...	T3

Generated 2026-05-30 19:07 UTC by TJS Security Command Center