INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-13 16:28 UTC

Microsoft Threat Intelligence Reports on Storm-1175's Rapid Medusa Ransomware Deployment

THREAT CAMPAIGN | HIGH

SCC Item ID	SCC-CAM-2026-0173
Type	Threat Campaign
Severity	HIGH
Affected Products	Various, organizations in healthcare, education, finance, and professional services sectors; specific vulnerable products not enumerated in source data
Published	2026-04-11
Discovery Source	Gemini

Executive Summary

Storm-1175, a financially motivated threat group, is deploying Medusa ransomware within 24 hours of public vulnerability disclosures, targeting organizations in healthcare, education, finance, and professional services. The compressed attack timeline eliminates the patch window most organizations rely on for protection, meaning unpatched systems can be encrypted before remediation is even scheduled. Business risk includes operational shutdown, data exfiltration for double-extortion leverage, and sector-specific regulatory exposure.

Technical Analysis

Storm-1175 is exploiting both zero-day and recently disclosed N-day vulnerabilities at high velocity, achieving initial access and full ransomware deployment within a 24-hour window following public vulnerability disclosure. Mapped MITRE ATT&CK techniques indicate a multi-stage intrusion chain: T1190 (Exploit Public-Facing Application) for initial access; T1078 (Valid Accounts) suggesting credential abuse or account takeover post-access; T1059 (Command and Scripting Interpreter) for execution; T1083 (File and Directory Discovery) for pre-encryption reconnaissance; T1486 (Data Encrypted for Impact) as the ransomware payload delivery; and T1567 (Exfiltration Over Web Service) indicating double-extortion data staging prior to encryption. The ransomware family is Medusa. No specific CVEs, affected product versions, CVSS scores, or confirmed IOCs are available in the source data at this fidelity level. Attribution is attributed to Microsoft Threat Intelligence coverage; however, primary Microsoft Security Blog posts or CISA advisories were not directly consulted in this review. Source quality is secondary/broad coverage (score: 0.64). Analysts should treat specific technical claims as unconfirmed pending primary source verification, particularly verification from CISA Advisory AA25-071A or

an official Microsoft Security Blog post on Storm-1175.

Action Checklist

1. Step 1: Containment. Immediately audit all internet-facing systems for unpatched vulnerabilities disclosed within the last 30 days, prioritizing healthcare, finance, education, and professional services infrastructure. Isolate any systems that cannot be patched within 24 hours. Monitor CISA's Known Exploited Vulnerabilities (KEV) catalog and advisories for confirmed Storm-1175 or Medusa-specific attack indicators.
2. Step 2: Detection. Review endpoint and SIEM logs for indicators of the mapped ATT&CK chain: T1190 exploitation attempts against public-facing applications, T1078 anomalous account usage (off-hours logins, new service accounts, lateral movement), T1059 unusual scripting interpreter invocations (PowerShell, cmd, bash), and T1083 large-scale file system enumeration. No confirmed Medusa IOCs (hashes, IPs, domains) are available from the current source data; cross-reference with Ransomware-as-a-Service threat feeds and CISA Advisory AA25-071A (Medusa Ransomware, published March 2025) for known indicators.
3. Step 3: Eradication. Apply all critical and high severity patches for internet-facing systems on an accelerated schedule. In the absence of specific CVE data from current sources, treat any vulnerability disclosed in the prior 30-day window as a candidate for exploitation. Enforce application allowlisting to block unauthorized scripting interpreter use aligned with T1059 behavior.
4. Step 4: Recovery. After patching, validate system integrity against known-good baselines before restoring to production. Monitor for T1567 exfiltration patterns (unusual outbound data transfers to cloud storage or web services) for at least 72 hours post-remediation. Confirm backup integrity and verify backups are stored offline or immutably to resist encryption.
5. Step 5: Post-Incident. Review patch SLA policies against the 24-hour exploitation window Storm-1175 demonstrates. Organizations relying on monthly patch cycles are structurally exposed to this actor. Evaluate whether emergency patch procedures exist for critical internet-facing systems and test those procedures. Map detection coverage gaps against T1078, T1059, T1083, T1567, and T1486 in your SIEM and EDR.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior IR leadership, legal counsel, and sector-specific regulatory contacts (HHS/OCR for HIPAA-covered healthcare entities, appropriate financial regulators for finance-sector organizations) if any evidence of T1486 ransomware encryption activity, T1567 data exfiltration to external destinations, or confirmed Storm-1175 TTPs is identified on systems containing PHI, PII, or financial records — each of these conditions independently triggers breach notification assessment obligations with statutory timelines.

Recovery Notes	Before returning any patched internet-facing system to production, validate that no web shells, rogue service accounts (Event ID 4720), or unauthorized scheduled tasks introduced during the Storm-1175 intrusion window remain present — patch application does not remove post-exploitation persistence mechanisms already installed. Maintain continuous outbound traffic monitoring for T1567 exfiltration patterns for a minimum of 72 hours post-remediation, as Medusa operators may have staged exfiltrated data for upload prior to containment. Given Medusa's double-extortion model, treat any confirmed exfiltration event as a breach notification trigger regardless of whether encryption occurred, and engage legal counsel to assess notification obligations under applicable sector regulations (HIPAA, GLBA, state breach notification statutes).
Forensic Artifacts	Web server access logs (IIS: %SystemDrive%\inetpub\logs\LogFiles\W3SVC**.log; Apache/Nginx: /var/log/apache2/access.log or /var/log/nginx/access.log) — preserved before log rotation — containing HTTP 200 responses to anomalous URI patterns, large POST body sizes, or URL-encoded/Base64 payload strings indicative of T1190 exploitation of the specific internet-facing service targeted by Storm-1175 | Sysmon Event ID 1 (Process Create) logs showing parent-child process chains where internet-facing service executables (w3wp.exe, java.exe, nginx worker processes) spawned cmd.exe, powershell.exe, wscript.exe, or cscript.exe — direct forensic evidence of web shell execution (T1059) following T1190 initial access | Windows Security Event Log entries for Event ID 4720 (user account created), 4728/4732 (security group membership changes), 4624 with LogonType 3 (network logon) or LogonType 10 (remote interactive), and 4776 (NTLM credential validation) within the 24-hour window following the exploited vulnerability's public disclosure date — documents Storm-1175 T1078 credential-based lateral movement | Registry export of HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, HKLM\SYSTEM\CurrentControlSet\Services, and HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, plus output of `schtasks /query /fo CSV /v` — captures Medusa ransomware persistence mechanisms and any Storm-1175 backdoor installation that survives initial containment | Full memory image (WinPmem/LiME) and network capture (tcpdump/Wireshark) of outbound connections to cloud storage provider IP ranges and hostnames from affected hosts during the exploitation and pre-encryption window — documents T1567 exfiltration staging, which is a prerequisite for Medusa's double-extortion model and the primary evidence artifact for breach notification assessment

Per-Action IR Details

Step 1: Containment — Immediately audit all internet-facing systems for unpatched vulnerabilities disclosed within the last 30 days, prioritizing healthcare, finance, education, and professional services infrastructure. Isolate any systems that cannot be patched within 24 hours. No specific patch ID is available from current source data; monitor the Microsoft Security Blog and CISA KEV catalog for Storm-1175-specific advisories.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST RA-5 (Vulnerability Monitoring and Scanning), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: For teams without enterprise vulnerability scanners: run `nmap -sV --script vulners -p 80,443,8080,8443,3389,22,445 ` to enumerate exposed services and version strings, then cross-reference output against CISA KEV at https://www.cisa.gov/known-exploited-vulnerabilities-catalog filtered to the last 30 days. For Windows hosts, run `Get-HotFix | Where-Object {$_.InstalledOn -lt (Get-Date).AddDays(-30)}` to surface machines missing recent patches. Use `ss -tlnp` or `netstat -ano` on Linux/Windows to confirm which services are externally exposed. If a system cannot be patched in 24 hours, apply a host-based firewall rule blocking inbound access to the

vulnerable port until patching is complete — on Linux: `iptables -I INPUT -p tcp --dport -j DROP`; on Windows: `New-NetFirewallRule -DisplayName 'Storm1175-Block' -Direction Inbound -LocalPort -Protocol TCP -Action Block`.

Evidence: Before isolating any system, capture a full netstat snapshot (`netstat -ano > netstat_baseline.txt`), running process list (`tasklist /svc > proclist.txt` on Windows or `ps auxf > proclist.txt` on Linux), and active network connections with process mapping using `Get-NetTCPConnection | Select-Object LocalAddress,LocalPort,RemoteAddress,RemotePort,State,OwningProcess` on Windows. Preserve Windows Security Event Log (EVTX) from the affected host — specifically filter for Event ID 4624 (successful logon) and Event ID 4625 (failed logon) within the prior 72 hours to establish whether Storm-1175 lateral movement (T1078) preceded your containment window. Capture IIS/Apache/Nginx access logs from the prior 30 days before any rotation occurs, as Storm-1175 initial access via T1190 will leave HTTP 200 responses to anomalous URI patterns against the exploited service.

Step 2: Detection — Review endpoint and SIEM logs for indicators of the mapped ATT&CK chain: T1190 exploitation attempts against public-facing applications, T1078 anomalous account usage (off-hours logins, new service accounts, lateral movement), T1059 unusual scripting interpreter invocations (PowerShell, cmd, bash), and T1083 large-scale file system enumeration. No confirmed Medusa IOCs (hashes, IPs, domains) are available from the current source data; cross-reference with Ransomware-as-a-Service threat feeds and the CISA Medusa advisory (AA25-071A, published March 2025) for known indicators.

NIST Phase: Detection Analysis

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

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Deploy Sysmon (using SwiftOnSecurity config at minimum) to capture Event ID 1 (Process Create), Event ID 3 (Network Connection), and Event ID 11 (File Create) if no EDR is present. For T1059 detection without a SIEM, run this PowerShell query against Sysmon logs: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 1 -and $_.Message -match 'powershell|cmd|wscript|cscript'} | Select-Object TimeCreated, Message | Export-Csv sysmon_scripting.csv`. For T1078 off-hours logon detection, query Windows Security log: `Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4624} | Where-Object {$_.TimeCreated.Hour -lt 6 -or $_.TimeCreated.Hour -gt 22} | Select-Object TimeCreated, Message`. For T1083 file enumeration (a pre-encryption Medusa behavior), hunt for abnormally high volumes of Sysmon Event ID 11 from a single process within a short window — a two-person team can parse this with `Group-Object` in PowerShell. Apply the Sigma rule `win_susp_powershell_enc_cmd.yml` (from the SigmaHQ repository) locally using `sigma convert` to generate native Windows Event Log queries. Cross-reference behavioral findings against IOCs published in CISA Advisory AA25-071A.

Evidence: For T1190 exploitation evidence: collect web server access logs (IIS: `%SystemDrive%\inetpub\logs\LogFiles\`, Apache/Nginx: `/var/log/apache2/access.log` or `/var/log/nginx/access.log`) and filter for HTTP 4xx/5xx sequences followed by HTTP 200s against unusual URI paths, large POST bodies, or encoded payloads (URL-encoded characters, Base64 strings in URI) consistent with exploitation attempts against the specific vulnerable service. For T1078 credential abuse: query Windows Security Event ID 4720 (account creation), 4728/4732 (group membership changes), and 4776 (NTLM authentication) — Storm-1175 operators are known to create rogue service accounts post-access. For T1059 scripting activity: Sysmon Event ID 1 with parent-child process relationships showing the exploited internet-facing service (e.g., `w3wp.exe`, `java.exe`, `nginx`) spawning `powershell.exe`, `cmd.exe`, or `wscript.exe` is a high-confidence indicator of web shell execution or post-exploitation scripting. For T1083 enumeration: Sysmon Event ID 11 volume spikes across `C:\Users\`, `C:\ProgramData\`, and network shares from a single process context preceding any encryption activity.

Step 3: Eradication — Apply all critical and high severity patches for internet-facing systems on an accelerated schedule. In the absence of specific CVE data from current sources, treat any vulnerability disclosed in the prior 30-day window as a candidate for exploitation. Enforce application allowlisting to block unauthorized scripting interpreter use aligned with T1059 behavior.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST CM-7 (Least Functionality), NIST IR-4 (Incident Handling), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 2.3 (Address Unauthorized Software)

Compensating: For T1059 application allowlisting without enterprise tooling: enable Windows Software Restriction Policies (SRP) or AppLocker (available on Windows Server and Windows 10/11 Enterprise/Education) to block execution of `powershell.exe`, `wscript.exe`, `cscript.exe`, and `mshta.exe` from non-standard paths (i.e., anything outside `%SystemRoot%\System32\`). On Linux, use `auditd` rules to alert on `execve` syscalls for `/bin/bash`, `/usr/bin/python3`, and similar interpreters invoked by web server process UIDs (e.g., `www-data`, `apache`): `auditctl -a always,exit -F arch=b64 -S execve -F uid=33 -k webshell_exec`. To detect and remove web shells dropped by Storm-1175 during the exploitation phase (a prerequisite for T1059 post-exploitation scripting), scan web root directories with `grep -rn 'eval\|base64_decode\|system(\|exec(\|passthru\|shell_exec' /var/www/html/ > webshell_candidates.txt` or use the free NeoPI tool against IIS/Apache web roots. Verify patch status post-application using `wmic qfe list brief` (Windows) or `rpm -qa --last | head -20` / `dpkg -l` (Linux) filtered against the CISA KEV 30-day window.

Evidence: Before executing eradication, preserve a full memory image of any suspected compromised internet-facing host using WinPmem (Windows, free) or LiME kernel module (Linux) — Medusa operators establish persistence mechanisms (scheduled tasks, registry run keys, new service accounts) that exist in memory and on-disk prior to encryption and must be documented before reimaging. Capture `reg export HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run persistence_run.reg` and `schtasks /query /fo CSV /v > scheduled_tasks.csv` to document Storm-1175 persistence artifacts. Export the Windows Security Event Log in its entirety before patching overwrites forensic state. On Linux, capture `/etc/crontab`, `/var/spool/cron/`, and `/etc/systemd/system/` for any backdoor service units or cron jobs installed during the intrusion window.

Step 4: Recovery — After patching, validate system integrity against known-good baselines before restoring to production. Monitor for T1567 exfiltration patterns (unusual outbound data transfers to cloud storage or web services) for at least 72 hours post-remediation. Confirm backup integrity and verify backups are stored offline or immutably to resist encryption.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CP-9 (System Backup), NIST AU-11 (Audit Record Retention), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 3.4 (Enforce Data Retention), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: For integrity validation without enterprise FIM: use `Get-FileHash` in PowerShell against critical system binaries and web application files compared to a pre-incident hash baseline (if unavailable, compare against a clean reference system of the same patch level). On Linux, use `aide --check` if AIDE was configured pre-incident, or `debsums -c` (Debian/Ubuntu) / `rpm -Va` (RHEL/CentOS) to verify package file integrity against RPM/DEB manifests. For T1567 exfiltration monitoring without a SIEM: capture outbound traffic to known cloud storage endpoints (OneDrive, Dropbox, Mega.nz, AWS S3) using `tcpdump -i eth0 -w recovery_monitor.pcap 'host storage.googleapis.com or host api.dropboxapi.com or host mega.nz'` and review with Wireshark, filtering for large TLS sessions (>10MB) to these destinations. For backup integrity: test restore of a critical backup to an isolated VM — do not assume backup validity. Verify that backup media or cloud snapshots are immutable by confirming object-lock or WORM settings are enabled; Medusa operators specifically target and encrypt accessible backup repositories before triggering ransomware.

Evidence: During the 72-hour monitoring window post-remediation, capture and retain all outbound NetFlow or firewall connection logs, specifically flagging connections from previously compromised hosts to cloud storage hostnames or IP ranges not present in historical baselines — this documents T1567 exfiltration attempts that may occur even after patching if a secondary implant or scheduled task survived eradication. Preserve Sysmon Event ID 3 (Network Connection) logs filtered to `initiated=true` from the recovered hosts for the full monitoring window. Document backup repository access logs — Medusa's double-extortion model requires data exfiltration confirmation prior to encryption,

so unusual backup server read activity in the 24-48 hours preceding any detected encryption event is a key forensic indicator of pre-encryption staging.

Step 5: Post-Incident — Review patch SLA policies against the 24-hour exploitation window Storm-1175 demonstrates. Organizations relying on monthly patch cycles are structurally exposed to this actor. Evaluate whether emergency patch procedures exist for critical internet-facing systems and test those procedures. Map detection coverage gaps against T1078, T1059, T1083, T1567, and T1486 in your SIEM and EDR.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-2 (Flaw Remediation), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST RA-5 (Vulnerability Monitoring and Scanning), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For coverage gap assessment without enterprise SIEM/EDR: download and run the free ATT&CK Navigator (local browser-based, no server required) and map your current Sysmon + Windows Event Log + firewall log collection against T1078, T1059, T1083, T1567, and T1486 — visually identify which techniques have zero log sources generating detectable telemetry. For each gap identified, locate the corresponding Sigma rule in the SigmaHQ GitHub repository (search by ATT&CK technique ID) and convert to a native Windows Event Log query using `sigma convert -t windows-eventlog`. To test emergency patch procedures: conduct a tabletop exercise using a recent CISA KEV entry as the scenario — specifically simulate the Storm-1175 pattern of a new CVE appearing in the KEV catalog and measure actual time-to-patch against the 24-hour exploitation window this actor demonstrates. Document the delta as a residual risk finding. Subscribe to the CISA KEV RSS feed and Microsoft Security Response Center (MSRC) security update notifications to reduce the detection-to-awareness gap for newly disclosed vulnerabilities.

Evidence: Compile the complete incident timeline documenting: (1) the timestamp of public vulnerability disclosure for each CVE targeted, (2) the timestamp of first exploitation indicator in logs, (3) the timestamp of organizational awareness, and (4) the timestamp of containment action — this four-point delta analysis quantifies your actual exposure window against Storm-1175's documented 24-hour weaponization cadence and is the primary evidence artifact for both the lessons-learned report and any regulatory notification obligations. Retain all SIEM/log queries, Sysmon configurations, firewall rule change records, and patch deployment receipts as evidence of due diligence for potential HIPAA breach notification (healthcare sector) or SEC cyber incident disclosure (finance sector) requirements. Archive the CISA AA25-071A advisory and any Microsoft Threat Intelligence blog posts referencing Storm-1175 as contemporaneous threat intelligence corroborating the incident classification.

Detection Guidance

No confirmed Medusa or Storm-1175 IOCs are available from the source data at this fidelity level. Detection should focus on behavioral indicators aligned to the MITRE technique chain. Query SIEM for: (1) T1190, spike in exploit-pattern web requests against public-facing applications shortly after vulnerability disclosures; (2) T1078, account activity anomalies including new service account creation, credential use from unexpected geolocations, or authentication outside business hours; (3) T1059, PowerShell or scripting engine invocations with encoded commands, especially from non-admin processes; (4) T1083, high-frequency file system enumeration by a single process across multiple directories in a short window; (5) T1486, rapid file extension changes consistent with encryption, shadow copy deletion commands (vssadmin, wbadmin), or volume shadow service termination; (6) T1567, large outbound data transfers to cloud storage endpoints (Mega, OneDrive, Google Drive) prior to encryption activity. Cross-reference with CISA Advisory AA25-071A (Medusa Ransomware) for known IOC sets published by CISA. Note: CISA AA25-071A was published March 2025; verify currency at cisa.gov before operational use.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1059** — Command and Scripting Interpreter
- **T1190** — Exploit Public-Facing Application
- **T1486** — Data Encrypted for Impact
- **T1567** — Exfiltration Over Web Service
- **T1083** — File and Directory Discovery

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **IR-4** — Incident Handling
- **IR-5** — Incident Monitoring

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

HIPAA-SECURITY

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

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities

CIS-V8

- **7.3** — Perform Automated Operating System Patch Management

- **7.4** — Perform Automated Application Patch Management

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1059	Command and Scripting Interpreter	Execution
T1190	Exploit Public-Facing Application	Initial-Access
T1486	Data Encrypted for Impact	Impact
T1567	Exfiltration Over Web Service	Exfiltration
T1083	File and Directory Discovery	Discovery

Sources

Source	URL	Tier
One-day, n-day, and zero-day vulnerabilities explained - Field Effect	https://fieldeffect.com/blog/1-day-0-day-vulnerabilities-explained	T3
Zero-day vulnerability - Wikipedia	https://en.wikipedia.org/wiki/Zero-day_vulnerability	T3
Understanding Zero-Day Vulnerabilities, Exploits and Attacks	https://it.tenable.com/source/zero-day	T3
Zero-day vulnerabilities: how they work and how to stop them	https://www.vectra.ai/topics/zero-day	T3
What Is a Zero-Day Attack? Risks, Examples, and Prevention - Palo ...	https://www.paloaltonetworks.com/cyberpedia/zero-day-attacks-explai...	T3

Generated 2026-04-13 16:28 UTC by TJS Security Command Center