INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-11 06:11 UTC

BASANAI Ransomware Identified as New MedusaLocker-Family Variant

THREAT CAMPAIGN | **HIGH** | CVSS 8.1

SCC Item ID	SCC-CAM-2026-0165
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	8.1
Affected Products	Windows-based systems (file-encrypting malware; specific OS versions unconfirmed)
Published	2026-04-10
Discovery Source	Gemini

Executive Summary

BASANAI is a newly identified ransomware variant linked to the MedusaLocker family, a ransomware-as-a-service operation active since 2019. The variant encrypts files on Windows systems and operators claim to exfiltrate data before encrypting it, creating dual pressure through both operational disruption and threatened data exposure. BASANAI was identified in threat intelligence reporting in early 2026; independent technical validation from CISA, NIST, or MITRE has not yet been confirmed. Confidence in the variant's distinct status is low-to-medium pending independent sandbox analysis and primary-source technical documentation.

Technical Analysis

BASANAI is classified as a MedusaLocker-family ransomware variant (family confidence: medium; distinct variant status confidence: low-to-medium). It targets Windows-based systems, encrypts files using methods consistent with MedusaLocker lineage, appends a unique file extension to encrypted files, and drops a ransom note named 'README.txt'. Operators claim to perform data exfiltration prior to encryption (T1041), consistent with double extortion tradecraft. Known propagation vectors for MedusaLocker variants include phishing emails (T1566), exposed RDP services (T1021.001), valid account abuse (T1078), and vulnerability exploitation. Post-compromise behaviors include inhibiting system recovery (T1490), encrypting files (T1486), and enumerating file and directory contents (T1083). Relevant CWEs: CWE-311 (Missing Encryption of Sensitive Data, applied inversely as victim data encrypted without consent) and CWE-506 (Embedded Malicious Code). No CVE identifier is assigned. No specific patch exists; mitigation is defensive hardening and detection. BASANAI-specific technical details are unconfirmed from primary sources. Behaviors described (file extension appending, README.txt ransom note, claimed exfiltration) are inferred from MedusaLocker family patterns and

require independent sandbox analysis for validation.

Action Checklist

1. Containment: Identify and isolate Windows endpoints with exposed RDP (port 3389) from the internet. Disable or restrict RDP where not operationally required. Block inbound RDP at the perimeter firewall and enforce Network Level Authentication (NLA) where RDP must remain enabled. This addresses T1021.001, a primary MedusaLocker propagation vector.
2. Detection: Search endpoint logs and EDR telemetry for mass file rename or extension change events on Windows systems, creation of 'README.txt' in multiple directories, high-volume file I/O activity from a single process, and outbound data transfers to unknown external IPs (T1041). Query SIEM for T1566 indicators: suspicious email attachments or links targeting Windows users. No confirmed BASANAI-specific IOCs are available at this time; apply MedusaLocker family behavioral patterns as a baseline.
3. Eradication: No BASANAI-specific patch exists. Harden attack vectors: enforce MFA on all remote access and VPN, patch internet-facing systems against known vulnerabilities used by MedusaLocker-family operators, and audit for unauthorized valid accounts (T1078). Remove any identified malicious executables per EDR quarantine procedures.
4. Recovery: Restore encrypted files from offline or immutable backups only after confirming the compromised endpoint is fully reimaged or forensically cleared. Validate backup integrity before restore. Monitor restored systems for recurrence of file encryption behavior and anomalous outbound traffic. Do not pay ransom without legal and law enforcement consultation.
5. Post-Incident: Conduct a gap assessment against NIST CSF PR.AC (Access Control) and PR.AT (Awareness and Training) controls. Review email filtering, RDP exposure, backup immutability, and endpoint detection coverage. Report the incident to the FBI Internet Crime Complaint Center (IC3) at ic3.gov and CISA at cisa.gov/report if operational impact occurred. Document findings to satisfy incident response policy and any applicable breach notification obligations.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior IR leadership and legal counsel if: (1) any evidence corroborates MedusaLocker operators' double-extortion data exfiltration claim (sustained outbound transfers pre-encryption visible in NetFlow), which triggers breach notification assessment under applicable regulations (HIPAA, GDPR, state statutes); (2) encryption activity is observed spreading laterally beyond the initially identified endpoint via SMB (T1021.002) or RDP (T1021.001), indicating active propagation; or (3) the responding team lacks the capability to perform forensic disk imaging before reimaging, as loss of evidence may compromise law enforcement cooperation and legal proceedings.

Recovery Notes	Restore only to endpoints that have been fully reimaged from a known-good OS image — do not attempt in-place disinfection of BASANAI-encrypted systems, as MedusaLocker variants do not have a publicly available decryptor and residual persistence mechanisms may survive partial remediation. Validate restored systems against a configuration baseline using CIS-CAT Lite (free) before reconnecting to the production network, with particular focus on RDP disabled or NLA-enforced, no unauthorized local administrator accounts, and Sysmon deployed for 30-day post-recovery monitoring. Monitor all restored endpoints and any systems that share network segments with previously infected hosts for recurrence of VSS deletion activity (vssadmin delete shadows executed via cmd.exe or PowerShell) and mass FileCreate events for a minimum of 30 days, as MedusaLocker-affiliated operators have been observed re-entering environments through retained valid credentials.
Forensic Artifacts	Windows Security Event Log (Event IDs 4624 Type 10, 4625, 4648, 4720, 4732, 1102) on all Windows endpoints — captures MedusaLocker's RDP brute-force initial access, credential-based lateral movement (T1078), unauthorized account creation, and the characteristic post-encryption log clearing behavior | Sysmon Event ID 11 (FileCreate) logs showing mass creation of ransom note files (README.txt or BASANAI variant-specific filename) across multiple directory paths within a compressed time window, establishing the encryption event timeline | Windows Registry hive exports (HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run) from compromised endpoints, capturing MedusaLocker-family persistence mechanisms that survive user logoff | Network flow or perimeter firewall logs covering 72 hours pre-encryption, filtered for sustained outbound TCP connections to non-RFC1918 addresses from the compromised host — primary evidence for or against MedusaLocker operators' double-extortion data exfiltration (T1041) claim, which drives breach notification obligation analysis | VSS snapshot inventory captured via 'vssadmin list shadows' output at time of detection, documenting MedusaLocker's characteristic inhibit-system-recovery action (MITRE T1490) by confirming shadow copy deletion, which establishes both the threat actor's TTPs and the scope of unrecoverable encrypted data requiring backup restoration

Per-Action IR Details

Containment — Identify and isolate Windows endpoints with exposed RDP (port 3389) from the internet. Disable or restrict RDP where not operationally required. Block inbound RDP at the perimeter firewall and enforce Network Level Authentication (NLA) where RDP must remain enabled. This addresses T1021.001, a primary MedusaLocker propagation vector.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 12.2 — Establish and Maintain a Secure Network Architecture (IG2/IG3, referenced for perimeter segmentation context)

Compensating: Run 'netstat -an | findstr :3389' on each Windows host or use 'nmap -p 3389 --open ' from a jump host to enumerate exposed RDP. Immediately apply a Windows Defender Firewall inbound rule via PowerShell: 'New-NetFirewallRule -DisplayName Block-RDP-Inbound -Direction Inbound -LocalPort 3389 -Protocol TCP -Action Block'. For hosts where RDP must remain active, enforce NLA via Group Policy: Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Require NLA. Document each isolated host with timestamp and responsible analyst per NIST 800-61r3 §3.3 isolation requirements.

Evidence: Before isolating, capture: Windows Security Event Log Event ID 4624 (Logon Type 10 = RemoteInteractive) and Event ID 4625 (failed logon) filtered to source IPs outside known-good ranges, indicating brute-force or

credential-stuffing against RDP consistent with MedusaLocker initial access patterns. Export firewall connection logs (Windows Filtering Platform, Event IDs 5156/5157) showing established inbound TCP:3389 sessions. Preserve NetFlow or perimeter firewall logs showing source IPs and session durations for all inbound RDP connections in the 72 hours preceding detection — MedusaLocker operators often maintain persistent RDP access before deploying ransomware. Capture 'qwinsta' output and 'net session' output to enumerate active RDP sessions at time of containment.

Detection — Search endpoint logs and EDR telemetry for: mass file rename or extension change events on Windows systems, creation of 'README.txt' in multiple directories, high-volume file I/O activity from a single process, and outbound data transfers to unknown external IPs (T1041). Query SIEM for T1566 indicators: suspicious email attachments or links targeting Windows users. No confirmed BASANAI-specific IOCs are available at this time; apply MedusaLocker family behavioral patterns as a baseline.

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

Compensating: Deploy Sysmon with SwiftOnSecurity config to capture Event ID 11 (FileCreate) and Event ID 1 (ProcessCreate). Detect mass file rename activity (BASANAI encryption behavior) using this PowerShell query on collected Sysmon logs: 'Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" | Where-Object {$_.Id -eq 11} | Group-Object {$_.Properties[0].Value} | Where-Object {$_.Count -gt 200} | Sort-Object Count -Descending'. For README.txt ransom note drops, run: 'Get-ChildItem -Path C:\ -Recurse -Filter "README*.txt" -ErrorAction SilentlyContinue'. Monitor outbound exfiltration (T1041) with Wireshark or Windows Packet Capture (netsh trace) filtering on sustained outbound connections to non-RFC1918 addresses on ports 443/80 from processes other than known browsers. For T1566 (phishing), parse Windows Defender/Microsoft 365 quarantine logs or review Outlook .pst files with free tool MailXaminer or native PowerShell message trace if Exchange is on-premises.

Evidence: Capture before or concurrent with detection actions: Sysmon Event ID 1 (ProcessCreate) showing the BASANAI executable lineage — MedusaLocker variants typically execute from user-writable paths such as %APPDATA%, %TEMP%, or C:\Users\Public; Sysmon Event ID 11 (FileCreate) showing mass creation of ransom notes (README.txt or variant-specific filename) across multiple directories in compressed time window; Windows Security Event ID 4663 (Object Access — file rename/write) on shares and local drives showing the encrypting process renaming files to an unrecognized extension appended by BASANAI; Sysmon Event ID 3 (NetworkConnect) showing sustained outbound TCP connections preceding the encryption event, consistent with MedusaLocker double-extortion exfiltration behavior (T1041) before payload detonation; Windows Application Event Log entries from VSS (Volume Shadow Copy Service) showing deletion events (vssadmin delete shadows) — MedusaLocker family consistently destroys VSS snapshots to prevent recovery.

Eradication — No BASANAI-specific patch exists. Harden attack vectors: enforce MFA on all remote access and VPN, patch internet-facing systems against known vulnerabilities used by MedusaLocker-family operators, and audit for unauthorized valid accounts (T1078). Remove any identified malicious executables per EDR quarantine procedures.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST IA-5 (Authenticator Management), NIST AC-2 (Account Management), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.3 (Perform Automated Operating System Patch Management)

Compensating: Audit for T1078 (Valid Accounts) abuse — the MedusaLocker access-as-a-service model frequently leverages purchased RDP credentials or brute-forced local accounts. Run: 'net localgroup administrators' on all Windows hosts and compare against a known-good baseline; flag any account not in the approved list. Query Windows Security Event Log for Event ID 4720 (account created) and Event ID 4732 (member added to security-enabled local

group) in the past 30 days. For MFA enforcement without enterprise tooling, deploy Microsoft Authenticator with Azure AD free tier for VPN/RDP MFA, or configure Duo Security free tier (up to 10 users). For malicious executable removal without EDR, hash all executables in %APPDATA%, %TEMP%, and C:\Users\Public using 'Get-FileHash -Algorithm SHA256' and submit to VirusTotal via free API or manual upload; quarantine matches by moving to a restricted directory and disabling execution via icacls. Patch prioritization for MedusaLocker-family operators should include CVE-2021-34527 (PrintNightmare), CVE-2020-0787 (BITS elevation), and ProxyShell/ProxyLogon variants if Exchange is present — these are documented exploitation vectors for affiliated IABs.

Evidence: Before eradication, preserve: full disk image or at minimum forensic copy of %APPDATA%\Roaming, %TEMP%, C:\Users\Public, and C:\ProgramData for the suspected BASANAI executable and any dropper components — MedusaLocker variants are frequently delivered as a single PE binary; Windows Registry export of HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run for persistence mechanisms (MedusaLocker variants commonly establish Run key persistence); Windows Security Event Log Event ID 4648 (logon using explicit credentials) showing lateral movement from the initially compromised host to other endpoints using harvested credentials (T1078); memory dump of the encrypting process (if still active) using ProcDump: 'procdump.exe -ma ' to support later YARA analysis against MedusaLocker family signatures; Windows Security Event ID 1102 (audit log cleared) — MedusaLocker-affiliated operators frequently clear event logs post-encryption to hinder IR.

Recovery — Restore encrypted files from offline or immutable backups only after confirming the compromised endpoint is fully reimaged or forensically cleared. Validate backup integrity before restore. Monitor restored systems for recurrence of file encryption behavior and anomalous outbound traffic. Do not pay ransom without legal and law enforcement consultation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST CP-9 (System Backup), NIST CP-10 (System Recovery and Reconstitution), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 11.1 (Establish and Maintain a Data Recovery Process — IG1/IG2/IG3), CIS 11.2 (Perform Automated Backups — IG1/IG2/IG3)

Compensating: Verify backup integrity before restore using hash comparison: compute SHA-256 of backup files at the time of backup creation and recompute at restore time — mismatch indicates tampering or corruption. For immutable backup validation without enterprise tooling, confirm the backup target (e.g., external drive, NAS) was offline or write-protected during the incident window by reviewing backup device connection logs or physical custody records. Post-restore, deploy Sysmon on recovered systems and monitor Event ID 11 (FileCreate) for recurrence of mass file operations within the first 72 hours. Use Autoruns (Sysinternals) on each recovered endpoint to confirm no MedusaLocker persistence mechanisms (Run keys, scheduled tasks, services) survived the reimage. Monitor outbound traffic on restored systems with 'netstat -b 5' logged to a file every 5 minutes for 48 hours to detect C2 reconnection attempts or resumed exfiltration (T1041) if the adversary retained any access.

Evidence: Before initiating recovery, document and preserve: the full encrypted file listing (file paths, extensions, timestamps) using 'Get-ChildItem -Recurse | Where-Object {$_.Extension -match ""} | Export-Csv' as evidence of encryption scope for breach notification assessment; all ransom note (README.txt) file paths and contents as evidence of the threat actor's identity claims and data exfiltration assertions — MedusaLocker operators claim to exfiltrate data before encryption, which may trigger breach notification obligations under HIPAA, GDPR, or state statutes regardless of whether ransom is paid; VSS snapshot status via 'vssadmin list shadows' to confirm MedusaLocker's characteristic shadow copy deletion occurred (supports scope of impact documentation); network flow logs covering the pre-encryption window showing data volumes transferred to external IPs to assess whether double-extortion data exfiltration claim is substantiated.

Post-Incident — Conduct a gap assessment against NIST CSF PR.AC (Access Control) and PR.AT (Awareness and Training) controls. Review email filtering, RDP exposure, backup immutability, and endpoint detection coverage. Report the incident to the FBI Internet Crime Complaint Center (IC3) at ic3.gov and CISA at cisa.gov/report if operational impact occurred. Document findings to satisfy incident response policy and any applicable breach notification obligations.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-6 (Incident Reporting), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST AU-11 (Audit Record Retention), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 17.4 (Establish and Maintain Security Awareness for Network Infrastructure — IG2/IG3, for RDP/phishing awareness training gap)

Compensating: Conduct the NIST CSF PR.AC gap assessment using the free CISA Cyber Hygiene (CyHy) scanning service to validate external RDP exposure is fully remediated post-incident. For PR.AT (Awareness and Training) gaps identified through this incident — specifically MedusaLocker's documented use of phishing (T1566) as an initial access vector — deploy free KnowBe4 or Proofpoint Security Awareness Training free tier for targeted phishing simulation. Document the lessons-learned session output using CISA's free Cyber Incident Reporting template. For breach notification assessment, apply the HHS breach notification decision tool (if healthcare data is involved) or state AG notification requirements based on the confirmed or suspected data exfiltration claim made by MedusaLocker operators — the double-extortion claim alone may trigger notification obligations under some jurisdictions even without confirmed exfiltration. Retain all IR artifacts (logs, disk images, ransom notes, network captures) for a minimum of 3 years per NIST AU-11 (Audit Record Retention) to support any subsequent law enforcement or legal proceedings.

Evidence: Compile and preserve for post-incident record: the complete incident timeline reconstructed from Windows Event Logs (Security, System, Application), Sysmon logs, and network flow data covering initial access through encryption — this timeline supports both internal lessons learned and any FBI IC3 or CISA report submission; documented evidence of the MedusaLocker operator's double-extortion data exfiltration claim (ransom note contents, any threat actor communication) alongside network flow analysis results that either corroborate or refute the exfiltration assertion — this distinction materially affects breach notification obligation analysis; gap assessment results against CIS Controls v8 IG1 safeguards (specifically CIS 6.3 MFA, CIS 7.3 OS patching, CIS 11.1 backup recovery) as a documented baseline for remediation prioritization; MITRE ATT&CK technique mapping covering the full observed kill chain (T1021.001 RDP initial access, T1078 valid accounts, T1486 data encrypted for impact, T1041 exfiltration over C2, T1490 inhibit system recovery via VSS deletion) to support threat intelligence sharing with CISA and FBI.

Detection Guidance

No confirmed BASANAI-specific IOCs (hashes, IPs, domains, C2 infrastructure) are available from primary sources at this time. Apply MedusaLocker family behavioral detection baselines. Key detection signals: (1) Endpoint, mass file extension changes on Windows file systems, creation of 'README.txt' across multiple directories, high CPU/disk I/O from an unknown or unsigned process, and shadow copy deletion commands (vssadmin.exe delete shadows, wmic shadowcopy delete) indicating T1490. (2) Network, anomalous outbound data transfers prior to encryption onset (T1041), RDP authentication failures or successful RDP logins from unusual source IPs (T1021.001). (3) Email gateway, phishing indicators consistent with T1566: malicious attachments, credential-harvesting links, or macro-enabled documents. EDR behavioral rules for file encryption activity and ransom note creation should be enabled if not already active. YARA and Sigma rules for BASANAI are not yet available in public threat intelligence repositories; monitor MITRE ATT&CK, CISA alerts, and established threat intelligence feeds for updated indicators as analysis matures.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`README.txt`	Ransom note filename dropped in encrypted directories — consistent with MedusaLocker family pattern; BASANAI-specific confirmation pending	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1041** — Exfiltration Over C2 Channel
- **T1566** — Phishing
- **T1490** — Inhibit System Recovery
- **T1486** — Data Encrypted for Impact
- **T1021.001** — Remote Desktop Protocol
- **T1078** — Valid Accounts
- **T1083** — File and Directory Discovery

NIST-800-53R5

- **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
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

NIST-CSF-2

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

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(5)(i)** — Security Awareness and Training
- **164.312(e)(1)** — Transmission Security

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.8.24** — Use of cryptography

CIS-V8

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1041	Exfiltration Over C2 Channel	Exfiltration
T1566	Phishing	Initial-Access
T1490	Inhibit System Recovery	Impact
T1486	Data Encrypted for Impact	Impact
T1021.001	Remote Desktop Protocol	Lateral-Movement
T1078	Valid Accounts	Defense-Evasion
T1083	File and Directory Discovery	Discovery

Sources

Source	URL	Tier
What Are the Types of Ransomware? - Akamai	https://www.akamai.com/glossary/what-are-the-types-of-ransomware	T3
5 Most Common Types of Ransomware | CrowdStrike	https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/type...	T3
Ransomware - FBI	https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-fra...	T1
Understanding File-Based Attacks - Upwind Security	https://www.upwind.io/feed/understanding-file-based-attacks	T3
Ransomware Attacks and Types – How Encryption Trojans Differ	https://usa.kaspersky.com/resource-center/threats/ransomware-attack...	T3

DISCLAIMER

Generated 2026-04-11 06:11 UTC by TJS Security Command Center