INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-23 19:02 UTC

Aur0ra Ransomware: Stealthy Encryption and Double-Extortion Strain

THREAT CAMPAIGN | **HIGH** | CVSS 8.1

SCC Item ID	SCC-CAM-2026-0359
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	8.1
Affected Products	Windows endpoints (specific versions unconfirmed); broad targeting implied by ransomware strain classification
Published	2026-05-22
Discovery Source	Gemini

Executive Summary

CYFIRMA researchers have identified Aur0ra, a newly discovered ransomware strain that deliberately avoids renaming encrypted files to delay detection by security tools and users. The ransomware combines file encryption with reported data exfiltration (double-extortion model) and communicates with victims through a Tor-based portal. Organizations running Windows endpoints face potential operational shutdown, data loss, and public extortion if defenses fail to catch this strain before encryption completes.

Technical Analysis

Aur0ra is a Windows-targeting ransomware strain identified by CYFIRMA. Its primary evasion characteristic is the absence of filename modification or new extension appending post-encryption, a technique that bypasses detection logic relying on file rename events or extension allowlists. This maps to CWE-311 (Missing Encryption of Sensitive Data used offensively), CWE-506 (Embedded Malicious Code), and CWE-200 (Exposure of Sensitive Information). MITRE ATT&CK techniques observed or implied: T1486 (Data Encrypted for Impact), T1041 (Exfiltration Over C2 Channel), T1027 (Obfuscated Files or Information), T1490 (Inhibit System Recovery), and T1562 (Impair Defenses). The double-extortion component involves reported exfiltration prior to encryption, with a Tor-based victim portal used for ransom negotiation, consistent with current ransomware operational patterns. No specific Windows version targeting has been confirmed. No CVE is associated. Attribution is unconfirmed. **Source Status:** This item originated from secondary intelligence aggregation. Technical details beyond the initial CYFIRMA summary remain unverified; validation against primary CYFIRMA reporting is required before IOC-level operational decisions.

Action Checklist

1. Containment: Isolate any Windows endpoints exhibiting unusual CPU or disk I/O spikes, unexpected process launches, or outbound Tor traffic. Block Tor exit node IP ranges and .onion resolution at perimeter and end-user device firewalls (CIS Controls 4.4, 4.5; NIST SC-7 Boundary Protection). Disable SMB lateral movement paths on segments not requiring file sharing.
2. Detection: Audit endpoint logs for mass file read/write operations without corresponding rename events, which is the signature evasion behavior of Aur0ra. Query EDR telemetry for T1486 indicators: high-volume file open/write sequences with unchanged extensions. Monitor for T1041 patterns: unexpected outbound connections to Tor infrastructure. Enable volume shadow copy deletion alerts mapped to T1490. Ensure event logging and audit record review are active per NIST AU-2 and AU-6; confirm CIS Control 8.2 (Collect Audit Logs) is active across all Windows endpoints.
3. Eradication: No vendor patch applies; Aur0ra is not CVE-linked. Eradication depends on removing the malware binary and restoring from clean backups. Verify no persistence mechanisms survive (scheduled tasks, startup entries) per NIST SI-7 (Software, Firmware, and Information Integrity). Confirm shadow copies were not deleted before attempting VSS-based recovery.
4. Recovery: Restore encrypted files from verified offline or immutable backups only. Before reconnecting systems, validate endpoint integrity: scan with updated signatures, confirm no lateral movement occurred using local account audit logs per NIST AU-6. Rotate all credentials accessible on affected endpoints per NIST IA-4 (Credential Management), as exfiltration is claimed. Monitor restored systems for 72 hours for recurrence.
5. Post-Incident: Review detection gaps exposed by the no-rename evasion technique and update EDR rules to trigger on file content change without metadata change. Assess whether backup immutability and air-gap posture meet NIST CP-9 (System Backup) and CP-10 (Information System Recovery and Reconstitution) requirements. Evaluate exfiltration path to determine whether data loss notification obligations apply. Strengthen least-privilege access per NIST AC-6 (Least Privilege) and CIS Control 5.4 to limit blast radius of future ransomware execution.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership, legal counsel, and executive notification immediately if: network flow analysis confirms outbound data transfer exceeding 1GB to non-corporate IPs (triggering double-extortion breach notification assessment), more than 3 endpoints show simultaneous encryption activity (indicating active lateral spread beyond initial patient zero), or any domain controller or backup infrastructure is confirmed affected — each condition independently meets the threshold for regulatory breach notification evaluation and potential law enforcement engagement.

Recovery Notes	Restore only from backups with a verified creation timestamp predating the earliest Aur0ra execution artifact identified in the MFT or Sysmon logs, and hash-validate every backup archive before mounting to prevent restoring a compromised snapshot. Because Aur0ra's double-extortion model means encryption and exfiltration may have occurred on different timelines, treat credential rotation as a prerequisite to network reconnection — not a post-reconnection task — given that harvested credentials may enable re-entry independent of the ransomware binary. Monitor restored endpoints for 72 hours minimum using Sysmon Event ID 11 volume baselines and outbound connection logging, with particular attention to any re-emergence of Tor-bound traffic on ports 9001/9030/9050 that would indicate a surviving persistence mechanism or re-infection from an unidentified lateral movement path.
Forensic Artifacts	MFT ($MFT) export showing mass file modification timestamps without corresponding rename records — this is the definitive forensic signature of Aur0ra's in-place encryption evasion technique, distinguishing it from standard ransomware that produces paired write/rename MFT entries | Sysmon Event ID 11 (FileCreate) burst logs from C:\Users*\Documents, Desktop, Downloads, and mapped network drives showing hundreds of file overwrites per minute with unchanged extensions — the no-rename pattern is anomalous against any legitimate application baseline | Windows Security Event ID 4648 (Logon with Explicit Credentials) and Sysmon Event ID 10 (ProcessAccess targeting lsass.exe) from the 24-hour window before encryption onset, documenting credential harvesting that enabled Aur0ra's claimed exfiltration component | Network perimeter or host-based firewall logs (Windows Filtering Platform Event ID 5156) showing outbound connections to Tor guard node IP ranges on ports 9001/9030, timestamped to establish the C2 check-in timeline relative to encryption start and exfiltration volume | Ransom note files (scan all encrypted directories for newly created .txt/.html files dropped by Aur0ra) containing the Tor .onion portal URL — preserve as legal hold evidence, extract the onion address as a network IOC for blocking, and submit to threat intel feeds for correlation with known Aur0ra infrastructure

Per-Action IR Details

Containment — Isolate any Windows endpoints exhibiting unusual CPU or disk I/O spikes, unexpected process launches, or outbound Tor traffic. Block Tor exit node IP ranges and .onion resolution at the perimeter firewall per CIS 4.4 (Implement and Manage a Firewall on Servers) and CIS 4.5 (Implement and Manage a Firewall on End-User Devices). Disable SMB lateral movement paths on segments not requiring file sharing.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-4 (Information Flow Enforcement), 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: Use Windows Firewall with Advanced Security (netsh advfirewall) to block outbound TCP 9001/9030 (Tor relay ports) and deny all outbound to known Tor guard node IP ranges published at dan.me.uk/torlist. Disable SMB (TCP 445) laterally via Group Policy or: `Set-SmbServerConfiguration -EnableSMB2Protocol $false` on non-file-server endpoints. For network-level Tor blocking without a commercial firewall, deploy pfSense with the pfBlockerNG package using the Emerging Threats Tor ruleset (free). Use `netstat -ano` on suspect endpoints to identify active .onion-bound connections before isolation to preserve the C2 indicator.

Evidence: Before isolating, capture: (1) full memory dump using WinPmem or ProcDump targeting any process with active outbound TCP connections on ports 9001/9030/9050/9150; (2) Windows Security Event Log Event ID 5156 (Windows Filtering Platform permitted connection) filtered for destination IPs correlating to Tor guard nodes; (3) Prefetch files from C:\Windows\Prefetch\ for any recently executed unknown binaries, as Aur0ra's launcher will appear here before encryption begins; (4) `netstat -ano` output timestamped at moment of detection, preserving the Tor relay

IP for threat intel; (5) VSS snapshot inventory via `vssadmin list shadows` to confirm shadow copies exist before isolation prevents further deletion.

Detection — Audit endpoint logs for mass file read/write operations without corresponding rename events, which is the signature evasion behavior of Aur0ra. Query EDR telemetry for T1486 indicators: high-volume file open/write sequences with unchanged extensions. Monitor for T1041 patterns: unexpected outbound connections to Tor infrastructure. Enable volume shadow copy deletion alerts mapped to T1490. Reference AU-2 (Event Logging) and AU-6 (Audit Record Review, Analysis, and Reporting) to ensure these event types are captured and reviewed. CIS 8.2 (Collect Audit Logs) must be confirmed active across all Windows endpoints.

NIST Phase: Detection Analysis

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

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

Compensating: Deploy Sysmon with the SwiftOnSecurity config (minimum) and enable Event ID 11 (FileCreate) — Aur0ra's in-place encryption will generate mass Event ID 11 entries with unchanged extensions in rapid succession, detectable as >500 file write events in under 60 seconds. Use this PowerShell query against the Sysmon log: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 11} | Group-Object -Property {$_.Properties[0].Value} | Where-Object {$_.Count -gt 200}`. For VSS deletion detection, enable Windows Security auditing of `vssvc.exe` and alert on Sysmon Event ID 1 (Process Create) where CommandLine contains `Delete Shadows` or `resize shadowstorage`. For Tor C2 detection without SIEM, use Wireshark with display filter `tcp.dstport == 9001 || tcp.dstport == 9030` or deploy Zeek on a network tap to log conn.log entries for those ports.

Evidence: Preserve before any remediation: (1) Sysmon Event ID 11 logs showing file writes without extension changes — the absence of rename events (Sysmon Event ID 23 or file delete/rename sequences) alongside mass writes is Aur0ra's evasion signature; (2) Windows Security Event Log Event ID 4663 (Object Access — file system) filtered for WriteData access on user document directories (C:\Users*\Documents, Desktop, etc.) without corresponding rename operations; (3) Sysmon Event ID 1 showing parent-child process relationships of the suspected Aur0ra binary spawning cmd.exe or PowerShell for VSS deletion (T1490); (4) Windows Security Event ID 7045 or Sysmon Event ID 13 (RegistryEvent) for any new service or Run key persistence entries created during the encryption window; (5) DNS query logs (Windows DNS debug log or Zeek dns.log) for any .onion resolution attempts, which indicate the double-extortion C2 check-in.

Eradication — No vendor patch applies; Aur0ra is not CVE-linked. Eradication depends on removing the malware binary and restoring from clean backups. Verify no persistence mechanisms survive (scheduled tasks, startup entries) using D3-SICA (System Init Config Analysis) and D3-SFA (System File Analysis). Confirm shadow copies were not deleted before attempting VSS-based recovery.

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 CM-6 (Configuration Settings), CIS 2.3 (Address Unauthorized Software)

Compensating: Run `schtasks /query /fo LIST /v > schtasks_audit.txt` and `reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` plus the corresponding HKCU key to enumerate all persistence points — compare against a known-good baseline from a clean endpoint of the same build. Use Autoruns (Sysinternals, free) with VirusTotal integration enabled to flag the Aur0ra binary hash across all autostart locations. For binary identification without EDR, submit the suspected executable to a YARA scan using a rule targeting in-place encryption behavior (high-entropy file writes with no rename): look for ransom note strings and Tor onion address patterns in the binary using `strings.exe` from Sysinternals. Confirm VSS status with `vssadmin list shadows` — if shadows are absent, document this as evidence of T1490 execution before proceeding to backup-based recovery.

Evidence: Capture before wiping: (1) Full disk image of the affected endpoint using FTK Imager Lite (free) or `dd` equivalent, preserving the encrypted file corpus and the Aur0ra binary in original state for later decryptor analysis if one becomes available; (2) Export all scheduled tasks from `C:\Windows\System32\Tasks\` and registry Run keys (HKLM

and HKCU) to document Aur0ra's persistence mechanism — ransomware families commonly use `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` for re-execution on reboot; (3) Copy the Aur0ra binary (do not execute) and compute SHA-256 hash for threat intel sharing — submit to VirusTotal and cross-reference with CYFIRMA's published IOCs; (4) Windows Event Log Event ID 104 (System log cleared) or Event ID 1102 (Security log cleared) to determine if Aur0ra attempted log wiping; (5) MFT ($MFT) export via a forensic tool to confirm in-place encryption — the MFT will show file modification timestamps without corresponding rename records, validating the no-rename evasion technique.

Recovery — Restore encrypted files from verified offline or immutable backups only. Before reconnecting systems, validate endpoint integrity: scan with updated signatures, confirm no lateral movement occurred using local account audit logs per D3-LAM (Local Account Monitoring). Rotate all credentials that were accessible on affected endpoints per D3-CRO (Credential Rotation), as exfiltration is claimed. Monitor restored systems for 72 hours for recurrence.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST CP-9 (System Backup), NIST CP-10 (System Recovery and Reconstitution), 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)

Compensating: Validate backup integrity before restore by computing SHA-256 hashes of backup archives and comparing against pre-incident hash records — do not restore from any backup created after the earliest estimated compromise timestamp. For credential rotation without a PAM tool, use the Active Directory bulk password reset script: `Get-ADUser -Filter * -SearchBase 'OU=Affected,DC=domain,DC=com' | Set-ADAccountPassword -Reset -NewPassword (ConvertTo-SecureString -AsPlainText 'TempP@ss!' -Force)`, then force change at next logon. For lateral movement validation on a budget, run `net session` and review Windows Security Event ID 4624 (Logon) Type 3 (network logon) events on neighboring endpoints from 48 hours prior to containment — filter for accounts present on the encrypted host. Use ClamAV with a freshly updated signature database for the post-restore malware scan before network reconnection.

Evidence: Before reconnecting to the network: (1) Windows Security Event ID 4624 filtered for Logon Type 3 (network/SMB) originating from the compromised host's IP within the 72-hour pre-containment window — documents whether Aur0ra used SMB for lateral spread; (2) Windows Security Event ID 4648 (Logon with explicit credentials) on the affected host, identifying any credential harvesting activity that fed the claimed exfiltration; (3) Review LSASS access events — Sysmon Event ID 10 (ProcessAccess) targeting lsass.exe — to confirm whether credentials were dumped (common precursor to double-extortion exfiltration); (4) Network flow logs or Windows Firewall logs for large outbound data transfers (>100MB) to non-corporate IPs in the 24 hours before encryption was detected, corroborating Aur0ra's exfiltration claim; (5) Backup system access logs confirming the selected restore point predates the earliest Sysmon or MFT timestamp associated with Aur0ra activity.

Post-Incident — Review detection gaps exposed by the no-rename evasion technique and update EDR rules to trigger on file content change without metadata change. Assess whether backup immutability and air-gap posture meet CP-9 (System Backup) requirements. Evaluate exfiltration path to determine whether data loss notification obligations apply. Strengthen least-privilege access per AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) to limit blast radius of future ransomware execution.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST CP-9 (System Backup), NIST AC-6 (Least Privilege), NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Develop a Sigma rule targeting Aur0ra's no-rename evasion behavior: correlate Sysmon Event ID 11 (FileCreate) volume spikes against the absence of Event ID 23 (FileDelete/rename) within the same 30-second window on the same host — this behavioral detection catches in-place encryption regardless of binary hash. Publish the rule to

the SigmaHQ community for broader defense. For backup immutability without enterprise storage, configure Windows Server Backup to write to a network share with a dedicated write-once service account, then disable that account between backup windows. Implement tiered local admin control using LAPS (Microsoft Local Administrator Password Solution, free) to eliminate shared local admin credentials that allowed lateral movement. Document the Tor C2 IOCs and exfiltration method in a structured threat report formatted for STIX/TAXII sharing with sector ISACs.

Evidence: For the lessons-learned report and regulatory assessment: (1) Compile the full timeline from MFT timestamps and Sysmon logs showing first execution to last encrypted file write — this establishes the dwell time and encryption window for breach notification calculations; (2) Extract network flow records documenting outbound data volume and destination IPs during the pre-encryption period to quantify exfiltration scope for data loss notification obligations (GDPR 72-hour clock, HIPAA 60-day clock, state breach laws); (3) Document all user accounts with local administrator rights on affected endpoints at time of incident — the blast radius directly correlates to privilege scope, supporting the AC-6 remediation; (4) Preserve the ransom note (typically dropped as .txt or .html in each encrypted directory) for legal hold, law enforcement referral, and Tor portal URL extraction; (5) Capture the before/after EDR rule configuration diff showing the detection gap that allowed Aur0ra's no-rename technique to bypass alerting — required for insurer documentation and audit evidence.

Detection Guidance

Primary behavioral indicator: mass file writes with no corresponding rename or extension-append events. Standard ransomware detection signatures will miss this evasion. Query EDR for processes writing to large numbers of files within short timeframes where source and destination filenames are identical. Supplement with entropy analysis on file content: encrypted files show high entropy regardless of unchanged filenames. Monitor for T1490 activity, specifically vssadmin.exe or wmic.exe invocations deleting shadow copies. Flag outbound connections to Tor infrastructure (port 9001, 9030, or known Tor guard node IPs) per T1041. Watch for T1562 indicators: security tool process termination or log clearing. If SIEM is deployed, build a correlation rule combining high-volume file I/O + shadow copy deletion + Tor egress within the same time window and host. Hash-based and domain-based detection require primary CYFIRMA source validation. Once IOC details are published, update signature and block lists accordingly.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`Tor-based victim portal — specific .onion address not confirmed in available reporting`	Victim communication portal used for ransom negotiation; block Tor infrastructure broadly pending specific IOC confirmation	LOW

Framework Mappings

MITRE-ATTACK

- **T1562** — Impair Defenses
- **T1490** — Inhibit System Recovery
- **T1486** — Data Encrypted for Impact
- **T1041** — Exfiltration Over C2 Channel
- **T1027** — Obfuscated Files or Information

NIST-800-53R5

- **AC-6** — Least Privilege
- **AU-9** — Protection of Audit Information
- **CM-6** — Configuration Settings
- **SI-4** — System Monitoring
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(6)(ii)** — Response and Reporting
- **164.312(e)(1)** — Transmission Security

NIST-CSF-2

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

ISO-27001-2022

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

SOC2-TSC

- **CC7.4** — Responds to identified security incidents

CIS-V8

- **8.2** — Collect Audit Logs

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1562	Impair Defenses	Defense-Evasion
T1490	Inhibit System Recovery	Impact
T1486	Data Encrypted for Impact	Impact
T1041	Exfiltration Over C2 Channel	Exfiltration
T1027	Obfuscated Files or Information	Defense-Evasion

Sources

Source	URL	Tier
What is Ransomware | Attack Types, Protection & Removal - Imperva	https://www.imperva.com/learn/application-security/ransomware/	T3
What Is Ransomware? | IBM	https://www.ibm.com/think/topics/ransomware	T3
Ransomware: How to prevent and recover (ITSAP.00.099)	https://www.cyber.gc.ca/en/guidance/ransomware-how-prevent-and-reco...	T3
Ransomware: Types, Examples & Removal Tactics - Fortinet	https://www.fortinet.com/resources/cyberglossary/ransomware	T3
Ransomware Attacks of the COVID-19 Pandemic: Novel Strains ...	https://www.computer.org/csdl/magazine/it/2023/05/10308425/1RMfMbcj1YI	T3

Generated 2026-05-23 19:02 UTC by TJS Security Command Center