INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-06 18:47 UTC

Emerging RaaS Operation Reports Record Affiliate Growth via Aggressive Revenue Sharing

THREAT CAMPAIGN | HIGH

SCC Item ID	SCC-CAM-2026-0421
Type	Threat Campaign
Severity	HIGH
Affected Products	Organizations globally across multiple sectors; no specific product or version implicated
Published	2026-06-05
Discovery Source	Gemini

Executive Summary

A new ransomware-as-a-service operation is attracting affiliates at an unusually high rate by offering above-market revenue splits, drawing operators away from established groups and expanding the pool of actors available to conduct attacks. Larger affiliate networks translate directly to more intrusion attempts across more sectors, increasing the statistical likelihood that any organization becomes a target. While specific group attribution and verified metrics are unavailable, the structural pattern is consistent with how previous high-growth RaaS programs preceded significant victim volume increases.

Technical Analysis

This item describes a structural shift in the RaaS ecosystem rather than a specific vulnerability or exploit chain. No CVE, CWE, or technical indicators are associated. The operational model follows the standard RaaS pattern: a core developer group maintains ransomware build infrastructure, encryption tooling, and victim negotiation portals; affiliates independently conduct intrusions and deploy payloads, typically via initial access through phishing (T1566), valid account abuse (T1078), and financial extortion (T1657), followed by inhibit system recovery (T1490), service stop (T1489), and data encryption (T1486). The threat is the expansion of the affiliate tier, not a new technical capability. Increased affiliate count raises targeting frequency and sector diversity without requiring the core group to develop novel tradecraft. No group name, victim data, ransom figures, or technical indicators were included in available sources. Claims of record growth are unverified.

Action Checklist

1. Step 1: Exposure Assessment. Audit commonly exploited internet-facing entry points: VPN endpoints, RDP services, exposed email gateways, and unpatched public-facing applications. Verify MFA is enforced on all remote access per CIS 6.4 and CIS 6.3.
2. Step 2: Detection. Enable and review logging across endpoint, identity, and network layers per NIST AU-2 and CIS 8.2. Hunt for behavioral indicators consistent with mapped techniques: anomalous logon activity (T1078), mass file rename events (T1486), Volume Shadow Copy deletion (T1490), and bulk service termination (T1489). Query SIEM for vssadmin, wbadmin, bcdedit, and net stop commands in process execution logs.
3. Step 3: Hardening. Restrict administrator privileges to dedicated accounts (CIS 5.4, NIST AC-6). Disable dormant accounts within 45 days (CIS 5.3). Enforce MFA for all administrative and remote access (CIS 6.5, CIS 6.4). Apply D3-MFA and D3-CH (credential hardening) countermeasures. Rotate credentials for any service accounts exposed to internet-facing systems (D3-CRO).
4. Step 4: Backup and Recovery Validation. Verify that offline, immutable backup copies exist and are inaccessible from production network segments. Test restoration procedures. Confirm backup jobs are completing and audit logs protecting backup infrastructure per NIST AU-9. Review NIST CP controls for backup scope and frequency.
5. Step 5: Post-Incident Posture. Conduct tabletop exercise simulating a RaaS intrusion scenario against your environment. Map gaps against MITRE ATT&CK techniques T1566, T1078, T1490, T1489, T1486, T1657. Review IR playbooks for ransomware scenarios. Assess whether separation of duties (NIST AC-5) prevents a single compromised account from enabling both lateral movement and backup deletion.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to senior leadership, legal counsel, and cyber insurer if any of the following are confirmed: (1) evidence of active T1486 encryption or T1490 VSS deletion in progress; (2) discovery that a service or admin account shared between production and backup systems has been compromised; (3) ransomware note or encrypted files discovered in any environment segment containing PII, PHI, or PCI data triggering breach notification obligations under applicable state law, HIPAA, or PCI DSS; or (4) the organization lacks offline backup copies and cannot demonstrate a viable RTO — at that point the capability gap itself is a material risk requiring executive decision.
Recovery Notes	Following any confirmed RaaS intrusion, do not restore from backup until a full forensic triage confirms the initial access vector (T1078 credential compromise, T1566 phishing, or unpatched internet-facing application) has been closed — restoring to an environment with the same vulnerability reinstates the affiliate's access path. Monitor restored systems for 30 days using Sysmon and Windows Security Event logging at elevated verbosity (Event IDs 4624, 4625, 4648, 4688, 7045), specifically watching for re-appearance of the same lateral movement and VSS-deletion command patterns that characterized the original intrusion. Rotate all credentials organization-wide — not just the confirmed compromised accounts — because RaaS affiliates routinely harvest credential databases (NTDS.dit, SAM hive) during dwell time and sell or retain access for secondary intrusions.

Forensic Artifacts	Windows Security Event Log — Event IDs 4624 (Logon Type 3/10 for network and remote interactive logons), 4625 (failed logons), 4648 (explicit credential use), 4720/4722/4728 (account creation and group changes): these trace T1078 Valid Accounts abuse, the predominant RaaS affiliate initial access and lateral movement method | Sysmon Event ID 1 (Process Create) logs showing execution of vssadmin.exe, wbadmin.exe, bcdedit.exe, and net.exe with arguments targeting backup and recovery infrastructure: direct forensic evidence of T1490 (Inhibit System Recovery) execution by the ransomware payload or pre-encryption script | File system metadata on encrypted volumes — last-modified timestamps, file extension patterns (e.g., bulk uniform extension appended to files), and MFT ($MFT) entries capturing the encryption event window: establishes encryption start time for T1486 (Data Encrypted for Impact) and narrows the dwell-time window investigators must analyze | Windows System Event Log — Event IDs 7045 (new service installed) and 7036 (service state change): RaaS affiliates and their deployed ransomware binaries commonly install persistence via new services and terminate AV/backup services (T1489) immediately before encryption; these events bracket the pre-encryption phase precisely | Network flow logs or Windows Firewall logs from the 72 hours preceding confirmed encryption — specifically lateral movement indicators such as sequential SMB connections (port 445) from a single internal host to multiple destinations, RDP hops between internal hosts, and outbound connections to known RaaS C2 infrastructure or data exfiltration endpoints: required to establish the full intrusion timeline and determine whether double-extortion data exfiltration (T1657) preceded encryption

Per-Action IR Details

Step 1: Exposure Assessment — Audit internet-facing entry points most frequently exploited by RaaS affiliates: VPN endpoints, RDP services, exposed email gateways, and unpatched public-facing applications. Verify MFA is enforced on all remote access per CIS 6.4 and CIS 6.3.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR capability and hardening posture before incidents occur

Controls: CIS 6.3 (IG1/IG2/IG3) — Require MFA for Externally-Exposed Applications, CIS 6.4 (IG1/IG2/IG3) — Require MFA for Remote Network Access, CIS 7.1 (IG1/IG2/IG3) — Establish and Maintain a Vulnerability Management Process, AC-17 — Remote Access, AC-3 — Access Enforcement

Compensating: Run `nmap -sV -p 3389,1194,443,25,110,143 ` to enumerate exposed services. For RDP exposure, execute `netstat -ano | findstr :3389` on each host and cross-reference with firewall rules. Use Shodan CLI (`shodan host `) to confirm external visibility. For VPN MFA gaps, review authentication logs manually: on Windows NPS servers, query Event ID 6272 (Network Policy Server granted access) and 6273 (access denied) in Event Viewer under Applications and Services Logs > Microsoft > Windows > Network Policy Server.

Evidence: Before remediating, document the current exposed-service inventory: capture `nmap` output to a timestamped file, export firewall rule sets, and pull the last 30 days of VPN authentication logs (Windows NPS Event IDs 6272/6273 or equivalent vendor auth logs) and RDP login logs (Windows Security Event ID 4624 with Logon Type 10 for remote interactive) to establish a baseline of which accounts authenticated without MFA — this baseline is critical for later identifying RaaS affiliate initial access accounts.

Step 2: Detection — Enable and review logging across endpoint, identity, and network layers per NIST AU-2 and CIS 8.2. Hunt for behavioral indicators consistent with mapped techniques: anomalous logon activity (T1078), mass file rename events (T1486), Volume Shadow Copy deletion (T1490), and bulk service termination (T1489). Query SIEM for vssadmin, wbadmin, bcdedit, and net stop commands in process execution logs.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Monitoring systems, identifying attack indicators, and correlating evidence across sources

Controls: AU-2 — Event Logging, AU-3 — Content Of Audit Records, AU-6 — Audit Record Review, Analysis, And Reporting, AU-12 — Audit Record Generation, CIS 8.2 (IG1/IG2/IG3) — Collect Audit Logs

Compensating: Deploy Sysmon with SwiftOnSecurity's config (github.com/SwiftOnSecurity/sysmon-config) to capture Event ID 1 (Process Create) for `vssadmin.exe delete shadows`, `wbadmin.exe delete catalog`, `bcdedit.exe /set {default} recoveryenabled No`, and `net stop` targeting backup/AV services. Without SIEM, use PowerShell: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4688} | Where-Object {$_.Message -match 'vssadmin|wbadmin|bcdedit'}` on each endpoint. For mass file rename detection (T1486), run `Get-ChildItem -Recurse -Path C:\Users | Where-Object {$_.Extension -match '\.[a-z0-9]{4,8}$'} | Sort-Object LastWriteTime -Descending | Select-Object -First 100` to spot bulk extension changes consistent with ransomware encryption.

Evidence: Preserve these artifacts BEFORE tuning or clearing logs: (1) Windows Security Event Log entries — Event ID 4624 (Logon Type 3/10 for lateral movement and remote access), Event ID 4625 (failed logons indicating credential stuffing), Event ID 4648 (explicit credential use indicating Pass-the-Hash or Pass-the-Ticket); (2) Sysmon Event ID 1 logs showing process lineage for any `cmd.exe` or `powershell.exe` spawned by unexpected parent processes (e.g., `msiexec.exe`, web server processes); (3) Volume Shadow Copy state — run `vssadmin list shadows` immediately and export output, as RaaS affiliates using T1490 will delete these early in the encryption phase; (4) Windows Event ID 7045 (new service installed) and 7036 (service state changes) from the System log for T1489 bulk service termination.

Step 3: Hardening — Restrict administrator privileges to dedicated accounts (CIS 5.4, NIST AC-6). Disable dormant accounts within 45 days (CIS 5.3). Enforce MFA for all administrative and remote access (CIS 6.5, CIS 6.4). Apply D3-MFA and D3-CH (credential hardening) countermeasures. Rotate credentials for any service accounts exposed to internet-facing systems (D3-CRO).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: Limiting blast radius and preventing further compromise while maintaining operational continuity

Controls: AC-6 — Least Privilege, AC-2 — Account Management, CIS 5.3 (IG1/IG2/IG3) — Disable Dormant Accounts, CIS 5.4 (IG1/IG2/IG3) — Restrict Administrator Privileges to Dedicated Administrator Accounts, CIS 6.4 (IG1/IG2/IG3) — Require MFA for Remote Network Access, CIS 6.5 (IG1/IG2/IG3) — Require MFA for Administrative Access, AC-5 — Separation Of Duties

Compensating: Run `net user /domain` and `Get-ADUser -Filter {LastLogonDate -lt (Get-Date).AddDays(-45)} -Properties LastLogonDate` to identify dormant accounts for disabling. For privilege restriction without PAM tooling, create a GPO that denies local logon rights (`Deny log on locally`) to domain admin accounts on non-DC systems. Audit service account exposure with `Get-ADServiceAccount -Filter *` and cross-reference with systems in the internet-facing inventory built in Step 1. Force a Kerberos TGT reset for all service accounts using `Set-ADUser -Identity -ChangePasswordAtLogon $true` as the minimum credential rotation action.

Evidence: Before rotating credentials or modifying account state, export a full snapshot of Active Directory: `Get-ADUser -Filter * -Properties * | Export-Csv AD_snapshot_$(Get-Date -Format yyyyMMdd).csv`. This baseline is forensically critical — RaaS affiliates using T1078 (Valid Accounts) frequently create new accounts or modify existing ones during dwell time, and a pre-hardening snapshot allows investigators to diff against post-incident state. Also collect `Get-WinEvent -LogName Security | Where-Object {$_.Id -in @(4720,4722,4728,4732,4756)}` (account creation and group membership changes) covering the prior 90 days.

Step 4: Backup and Recovery Validation — Verify that offline, immutable backup copies exist and are inaccessible from production network segments. Test restoration procedures. Confirm backup jobs are completing and audit logs protecting backup infrastructure per NIST AU-9. Review NIST CP controls for backup scope and frequency.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Restoring systems to normal operation and verifying integrity before returning to production

Controls: AU-9 — Protection Of Audit Information, AU-4 — Audit Storage Capacity, AU-11 — Audit Record Retention, CIS 3.4 (IG1/IG2/IG3) — Enforce Data Retention

Compensating: For teams without enterprise backup platforms, validate offline backup isolation by physically or logically disconnecting the backup storage device and confirming production systems cannot reach it via `ping` or `Test-NetConnection`. Use `robocopy /MIR /LOG` to a write-once NAS or external drive with `icacls` permissions set to deny write access from production service accounts. Verify backup integrity by restoring a sample of critical files to an isolated VM — RaaS operators specifically target backup agents (Veeam, Backup Exec, Windows Backup) via T1490, so confirm backup agent service accounts do not share credentials with production accounts.

Evidence: Before validating backup health, capture the current state of backup infrastructure as forensic evidence: (1) run `vssadmin list shadows` and document all existing shadow copy versions and their associated volumes; (2) check backup agent logs (e.g., Veeam `C:\ProgramData\Veeam\Backup\`, Windows Server Backup event log under Applications and Services Logs > Microsoft > Windows > Backup) for any unexpected deletion events or authentication failures that could indicate a prior affiliate reconnaissance or pre-positioning activity targeting backup infrastructure; (3) export firewall rules governing backup server network segment access to confirm isolation has not been silently modified.

Step 5: Post-Incident Posture — Conduct tabletop exercise simulating a RaaS intrusion scenario against your environment. Map gaps against MITRE ATT&CK techniques T1566, T1078, T1490, T1489, T1486, T1657. Review IR playbooks for ransomware scenarios. Assess whether separation of duties (NIST AC-5) prevents a single compromised account from enabling both lateral movement and backup deletion.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons learned, playbook improvement, and capability gap identification to reduce recurrence

Controls: AC-5 — Separation Of Duties, AU-6 — Audit Record Review, Analysis, And Reporting, CIS 7.2 (IG1/IG2/IG3) — Establish and Maintain a Remediation Process, CIS 7.1 (IG1/IG2/IG3) — Establish and Maintain a Vulnerability Management Process

Compensating: Structure the tabletop around the RaaS affiliate kill chain: phishing (T1566) or credential purchase → VPN/RDP access (T1078) → internal reconnaissance (`net view`, `nltest /dclist`) → lateral movement to backup server → VSS deletion (T1490) → service termination (T1489) → encryption (T1486) → ransom negotiation (T1657). Use free Sigma rules from the SigmaHQ repository (search tag `ransomware`) to test whether your current log sources would fire on each phase. Document each phase where detection gaps exist and assign a responsible owner and 30-day remediation deadline. For playbook gaps, CISA's free Ransomware Response Checklist (available at cisa.gov) provides a validated baseline — note this URL should be human-verified as current.

Evidence: The tabletop output itself becomes a forensic-readiness artifact: document which ATT&CK technique phases your current tooling cannot detect, which accounts have combined rights enabling both lateral movement and backup access (a direct T1490 enabler), and the current Recovery Time Objective (RTO) measured during the restoration test in Step 4. This gap register establishes a pre-incident baseline that regulators and cyber insurers may require following an actual RaaS event, and it anchors future post-incident lessons-learned sessions to measurable improvement rather than anecdotal assessment.

Detection Guidance

No IOCs are available for this item. Detection must rely on behavioral indicators mapped to the associated MITRE techniques. Monitor for: (1) mass file rename or extension change events on file servers, indicator of T1486 encryption activity; (2) execution of vssadmin delete shadows, wbadmin delete catalog, or bcdedit /set recoveryenabled no, indicator of T1490 recovery inhibition; (3) net stop or sc stop commands targeting backup, AV, or database services in bulk, indicator of T1489; (4) logon events using valid accounts at unusual hours or from unexpected source IPs, indicator of T1078 valid account abuse; (5) phishing email delivery with weaponized attachments or credential-harvesting links, indicator of T1566. Per NIST AU-6 and CIS 8.2, ensure

audit log collection is active across endpoint EDR, Windows Security Event logs (Event IDs 4625, 4648, 4688, 7045), and network flow data. Per D3-LAM, monitor local account activity for privilege escalation patterns. Per D3-UAP, alert on permission changes granting broad file system access to non-standard accounts.

Framework Mappings

MITRE-ATTACK

- **T1490** — Inhibit System Recovery
- **T1566** — Phishing
- **T1078** — Valid Accounts
- **T1657** — Financial Theft
- **T1489** — Service Stop
- **T1486** — Data Encrypted for Impact

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-6** — Configuration Settings
- **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
- **164.312(e)(1)** — Transmission Security

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.24** — Use of cryptography

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1490	Inhibit System Recovery	Impact
T1566	Phishing	Initial-Access
T1078	Valid Accounts	Defense-Evasion
T1657	Financial Theft	Impact
T1489	Service Stop	Impact
T1486	Data Encrypted for Impact	Impact

Sources

Source	URL	Tier
What Is Ransomware-as-a-Service (RaaS)? | IBM	https://www.ibm.com/think/topics/ransomware-as-a-service	T3
Analysis of Modern Ransomware & RaaS Operations - Sealpath	https://www.sealpath.com/blog/ransomware-raas-operations-guide/	T3
Complete Guide to Ransomware as a Service (RaaS) - TierPoint	https://www.tierpoint.com/blog/cybersecurity/ransomware-as-a-service/	T3
What Is RaaS - Ransomware-as-a-Service? - Sophos	https://www.sophos.com/en-us/cybersecurity-explained/ransomware-as-...	T3
New Ransomware-as-a-Service (RaaS) Groups to Watch in 2025	https://flashpoint.io/blog/new-ransomware-as-a-service-raas-groups-...	T3

Generated 2026-06-06 18:47 UTC by TJS Security Command Center