INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-13 18:56 UTC

RaaS Operator Exposed: OPSEC Failure Reveals 'The Gentlemen' Affiliate Model and Organizational Structure

THREAT ACTOR | MEDIUM | CVSS 5.0

SCC Item ID	SCC-TAC-2026-0017
Type	Threat Actor
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	None specified, organizational/operational exposure, not a product vulnerability
Published	2026-05-13T16:47:46
Discovery Source	Rss

Executive Summary

A ransomware-as-a-service group called 'The Gentlemen' has suffered an operational security failure that exposed internal details about its affiliate recruitment model, revenue-sharing structure, and targeting patterns. No specific organization has been named as a victim, but the leaked intelligence gives defenders rare visibility into how this group recruits partners and executes campaigns. Security teams can use this exposure to establish threat actor profiling baselines, affiliate attribution confidence, and detection coverage against this group's known techniques.

Technical Analysis

Source: Dark Reading (T3, single news-tier source, no corroborating primary-tier confirmation from CISA, MITRE, or NVD at analysis time). Confidence: medium. Recommended action: Implement detection coverage for mapped techniques immediately (low implementation risk); defer high-cost infrastructure changes pending additional corroboration.

The exposure involves an OPSEC failure attributed to 'The Gentlemen' RaaS operation, surfacing internal affiliate model details, payout structures, and organizational hierarchy. No CVE or product vulnerability is associated. Referenced CWEs, CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor) and CWE-522 (Insufficiently Protected Credentials), reflect the nature of the group's internal failure, not a vendor flaw.

Mapped MITRE ATT&CK techniques associated with this group's known tradecraft include: T1486 (Data Encrypted for Impact), T1566 (Phishing), T1078 (Valid Accounts), T1133 (External Remote Services), T1041 (Exfiltration Over C2 Channel), T1021 (Remote Services), T1589 (Gather Victim Identity Information), T1583 (Acquire Infrastructure), T1562 (Impair Defenses), T1083 (File and Directory Discovery), and T1587.001 (Develop Capabilities: Malware). The affiliate model and high payout structure are consistent with patterns observed in other prominent RaaS ecosystems. No patch, CVE remediation, or vendor advisory applies.

Action Checklist

1. Profiling, Add 'The Gentlemen' as a tracked threat actor in your TIP or SIEM. Tag all associated MITRE techniques (T1486, T1566, T1078, T1133, T1041, T1021, T1562, T1083, T1589, T1583, T1587.001) and set alert rules against them.
2. Detection, Hunt for behavioral patterns consistent with this group's tradecraft: phishing delivery (T1566), use of valid or stolen credentials (T1078), external remote service abuse (T1133), and data encryption activity (T1486). Review endpoint and authentication logs for anomalous lateral movement via remote services (T1021).
3. Exposure Review, Audit internet-facing remote access services (VPN, RDP, cloud management consoles). Confirm MFA is enforced on all external access points. Review credential hygiene for service accounts and privileged users; T1078 and T1133 are primary initial-access vectors for this group.
4. Intelligence Enrichment, Cross-reference any existing IOCs or historical incidents in your environment against known RaaS affiliate TTPs. If your sector matches the opportunistic targeting pattern reported (no specific sectors named in source, treat as broad), increase monitoring sensitivity on backup systems and file servers.
5. Post-Incident Controls Review, Use this exposure to evaluate gaps in your ransomware-specific playbooks. Confirm backup integrity and offline copy availability. Validate that impair-defenses detections (T1562) are tuned, affiliates commonly disable logging and AV before encryption.

IR / Forensic Enrichment

Triage Priority	STANDARD
Escalation Criteria	Escalate to urgent if any T1562 indicators (audit log cleared, Windows Defender disabled, VSS shadow copies deleted) are detected on file servers or backup infrastructure, or if authentication anomalies consistent with T1078/T1133 are identified on external-facing services, as these represent active affiliate staging activity that precedes ransomware deployment and may trigger breach notification obligations if PII/PHI is resident on affected systems.
Recovery Notes	Because The Gentlemen's affiliate model targets backup infrastructure before encryption (T1490), recovery validation must begin with an offline, air-gapped restore test of critical system backups before declaring any incident resolved — do not trust VSS shadow copies as the sole recovery path. Post-recovery, maintain elevated monitoring on file servers, backup hosts, and authentication infrastructure for a minimum of 30 days, specifically watching for reinfection via residual access (T1078 credential reuse by a second affiliate) or delayed payload execution. Update your ransomware playbook to reflect the affiliate-specific TTP cluster (T1566 → T1078/T1133 → T1021 → T1083 → T1562 → T1486) as a sequential kill chain detection hypothesis for future threat hunts.

Forensic Artifacts	Windows Security Event Log (Event IDs 4624, 4625, 4648, 4768, 4769, 4771) from domain controllers and VPN/RDP gateways — The Gentlemen affiliates' reliance on T1078 and T1133 will produce authentication events with mismatched logon types (Type 3/10) from external source IPs or service accounts accessing file and backup servers interactively | Sysmon Event IDs 1 (Process Creation), 3 (Network Connection), 11 (FileCreate), and 13 (RegistryEvent) from file servers and backup hosts — T1486 encryption activity produces characteristic mass FileCreate events with renamed extensions, and T1562 produces Sysmon Event ID 4 (service state changed) when logging or AV is disabled by the affiliate | Windows Application and System Event Logs for Event IDs 7036 (service stopped) and 7040 (service start type changed), plus Security Event ID 1102 (audit log cleared) and System Event ID 104 (System log cleared) — these are the primary forensic indicators of T1562 impair-defenses execution that The Gentlemen affiliates use immediately before deploying the ransomware payload | VSS shadow copy inventory and backup repository access logs — query vssadmin list shadows and review Windows Security Event ID 4663 (file object access) on backup share paths for access by accounts other than the designated backup service account, as T1490 inhibit-system-recovery activity will appear here before or concurrent with T1486 encryption | Email gateway delivery logs and Microsoft 365 Unified Audit Log (MailItemsAccessed, FileDownloaded operations) — The Gentlemen's T1566 phishing delivery and T1589 victim research activity will leave inbound message metadata (sender domains, attachment hashes, URL redirectors) that can be correlated against the affiliate's infrastructure built via T1583 and T1587.001 to establish initial access timeline

Per-Action IR Details

Profiling — Add 'The Gentlemen' as a tracked threat actor in your TIP or SIEM. Tag all associated MITRE techniques (T1486, T1566, T1078, T1133, T1041, T1021, T1562, T1083, T1589, T1583, T1587.001) and set alert rules against them.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing threat actor tracking and detection rule baselines before active compromise

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-4 (System Monitoring), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For teams without a commercial TIP: create a structured threat actor profile file (JSON or Markdown) in a shared repo and load The Gentlemen's 11 technique IDs into Sigma rules targeting Windows Security, Sysmon, and authentication logs. Use the MITRE ATT&CK Navigator (free, browser-based) to generate a heatmap of T1486/T1566/T1078/T1133/T1021/T1562 for visual briefing to leadership. Reference Sigma rule categories: process_creation, network_connection, registry_event, and file_event.

Evidence: Before finalizing the profile, collect any existing threat intelligence hits from your environment: query your SIEM or log aggregator for historical matches against The Gentlemen's known technique cluster — specifically, any prior alerts on T1078 (account reuse from credential sources), T1133 (external-facing RDP/VPN authentication events), and T1562 (Windows Defender or logging service stop/disable events). Document which affiliate-linked IOCs, if any, appear in your historical incident tickets or threat feeds.

Detection — Hunt for behavioral patterns consistent with this group's tradecraft: phishing delivery (T1566), use of valid or stolen credentials (T1078), external remote service abuse (T1133), and data encryption activity (T1486). Review endpoint and authentication logs for anomalous lateral movement via remote services (T1021).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Behavioral threat hunting using known affiliate TTPs to surface precursor activity before ransomware payload delivery

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM/EDR: (1) For T1566 phishing precursors, parse email gateway logs or Microsoft 365 Unified Audit Log for inbound messages with URL redirectors or attachment types (.html, .iso, .lnk, .zip) targeting privileged users. (2) For T1078/T1133, run: Get-EventLog -LogName Security -InstanceId 4624,4625,4648 | Where-Object {$_.Message -match 'Logon Type.*3|10'} to surface remote interactive and network logons — filter for off-hours or geographically anomalous source IPs against VPN and RDP gateway logs. (3) For T1486 early indicators, deploy Sysmon Event ID 11 (FileCreate) with filters on rapid file rename events in user home directories and file servers, which precede encryption. (4) For T1021 lateral movement, query Windows Security Event ID 4648 (explicit credential use) and 4778/4779 (session reconnect/disconnect) across domain controllers.

Evidence: Capture before hunting: export Windows Security Event Log (Event IDs 4624, 4625, 4648, 4768, 4769, 4771) from all authentication infrastructure (DCs, VPN concentrators, RDP gateways) for the trailing 30-day window; preserve Sysmon logs (Event IDs 1, 3, 11, 13) from file servers and backup hosts; snapshot email gateway delivery logs filtering on attachments or links received by IT, finance, and executive mailboxes; and pull authentication records from cloud management consoles (Azure AD Sign-in logs, AWS CloudTrail) for any service account activity during non-business hours.

Exposure Review — Audit internet-facing remote access services (VPN, RDP, cloud management consoles). Confirm MFA is enforced on all external access points. Review credential hygiene for service accounts and privileged users — T1078 and T1133 are primary initial-access vectors for this group's affiliate model.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Reducing attack surface by hardening initial-access vectors documented in The Gentlemen's affiliate playbook prior to a targeting event

Controls: NIST AC-17 (Remote Access) — implied from AC family scope, NIST IA-5 (Authenticator Management) — implied from IA family scope, NIST CM-7 (Least Functionality) — implied from CM family scope, NIST SI-2 (Flaw Remediation), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 5.3 (Disable Dormant Accounts)

Compensating: For teams without enterprise PAM tools: (1) Run the following PowerShell to identify service accounts without MFA flagged in AD: Search-ADAccount -PasswordNeverExpires | Select-Object Name,SamAccountName,LastLogonDate — review any account with PasswordNeverExpires=True and recent logon activity as a T1078 risk. (2) Use nmap or Shodan Monitor (free tier) to enumerate externally visible RDP (TCP 3389), VPN (UDP 500/4500, TCP 443), and SSH (TCP 22) endpoints and compare against your authorized asset inventory. (3) For RDP exposure, run: netstat -an | findstr :3389 on each server and cross-reference against CIS 1.1 asset inventory. (4) Disable any service account interactive logon rights via GPO (Deny log on locally / Deny log on through Remote Desktop Services) for accounts that do not require them.

Evidence: Before making changes, document the current exposure baseline: screenshot or export your firewall/NAT rule set showing all inbound rules for TCP 3389, TCP 443 (split-tunnel VPN), and management console ports; export the Active Directory report of all accounts with 'Password Never Expires' and 'Last Logon' within 90 days; and capture current MFA enrollment status from your identity provider (Azure AD MFA Status report, Duo enrollment report, or equivalent) to establish a before-state for audit evidence under NIST AU-9 (Protection of Audit Information).

Intelligence Enrichment — Cross-reference any existing IOCs or historical incidents in your environment against known RaaS affiliate TTPs. If your sector matches the opportunistic targeting pattern reported (no specific sectors named in source — treat as broad), increase monitoring sensitivity on backup systems and file servers.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Integrating threat actor intelligence to improve detection fidelity and prioritize monitoring on high-value targets consistent with RaaS affiliate objectives

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

Compensating: For teams without a commercial threat intelligence platform: (1) Query AlienVault OTX (free) and OpenCTI (open source) for any published IOCs associated with 'The Gentlemen' RaaS group and export as a STIX bundle or CSV for local correlation. (2) On backup servers (Windows Server Backup, Veeam free tier hosts), enable auditing on the backup repository share via GPO (Audit Object Access → Success and Failure) and review Windows Security Event ID 4663 (object access attempt) and 4656 (handle requested) for any access from accounts other than the designated backup service account — RaaS affiliates using T1083 will enumerate backup paths before T1490 (inhibit system recovery) actions. (3) On file servers, deploy Sysmon Event ID 11 with a ProcessAccess filter to detect mass file open/rename operations consistent with encryption staging.

Evidence: Before increasing monitoring sensitivity, preserve a forensic baseline snapshot: use osquery (free) to run SELECT * FROM file WHERE path LIKE '/backup/%' OR path LIKE 'C:\\Backup\\%' and capture file count, sizes, and last-modified timestamps on backup repositories — this establishes an integrity baseline to detect T1490 deletion or T1486 encryption of backup sets; also export the current VSS shadow copy inventory via vssadmin list shadows and hash the output to detect future tampering.

Post-Incident Controls Review — Use this exposure to evaluate gaps in your ransomware-specific playbooks. Confirm backup integrity and offline copy availability. Validate that impair-defenses detections (T1562) are tuned — affiliates commonly disable logging and AV before encryption.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Using threat actor OPSEC exposure as a forcing function to update ransomware playbooks, validate recovery capability, and harden T1562 detection before an active engagement

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-3 (Malicious Code Protection), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-5 (Response to Audit Logging Process Failures), NIST AU-9 (Protection of Audit Information), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without enterprise EDR: (1) Deploy Sysmon Event IDs 4 (Sysmon service state change) and Windows Security Event ID 7045 (new service installed) plus Event ID 4719 (system audit policy changed) to detect The Gentlemen affiliates' T1562 pattern of disabling Windows Event Log service or audit policy before encryption; create a Sigma rule for: EventID 1102 (audit log cleared) and EventID 104 (System log cleared). (2) Validate AV protection state via PowerShell: Get-MpComputerStatus | Select-Object AMServiceEnabled,RealTimeProtectionEnabled,AntivirusEnabled — schedule this as a daily Task Scheduler job and log output to a protected share. (3) For backup integrity, run: wbadmin get versions to confirm the most recent backup completed and cross-check with a test restore of a single non-critical file to verify recoverability — document the test result and timestamp as evidence for NIST CP (Contingency Planning) compliance.

Evidence: Before finalizing playbook updates, capture current detection coverage gaps as documented evidence: export your SIEM or Windows Event Forwarding subscription list to confirm Event IDs 1102, 4719, 7036 (service stopped), and 7040 (service start type changed) are being collected from all endpoints; verify that Windows Defender tamper protection status is logged (Microsoft-Windows-Windows Defender/Operational log, Event ID 5013 for tamper protection trigger); and document the last successful offline backup date with hash verification as the recovery baseline for your ransomware playbook.

Detection Guidance

No confirmed IOCs are available from this item. Detection should focus on behavioral coverage of mapped ATT&CK techniques.

Priority detection areas:

- T1566 (Phishing): Email gateway logs, flag suspicious attachment types and lookalike sender domains. Correlate with endpoint process creation following email open events.

- T1078 / T1133 (Valid Accounts / External Remote Services): Authentication logs, alert on logins from unusual geographies, off-hours access to VPN or RDP, and credential reuse across systems.

- T1562 (Impair Defenses): EDR/AV logs, alert on security tool process termination, service disabling, or log clearing events (Windows Event ID 1102, 104).

- T1486 (Data Encrypted for Impact): File system monitoring, mass file rename events, extension changes consistent with ransomware staging, shadow copy deletion (vssadmin delete shadows).

- T1041 / T1083 (Exfiltration / File Discovery): NetFlow or proxy logs, large outbound data transfers to unfamiliar destinations; file enumeration activity on shared drives.

Note: All detection recommendations are based on mapped ATT&CK techniques from source data. No actor-specific signatures, IOCs, or confirmed tooling are available from this single-source news item.

Framework Mappings

MITRE-ATTACK

- **T1587.001** — Malware
- **T1566** — Phishing
- **T1078** — Valid Accounts
- **T1133** — External Remote Services
- **T1041** — Exfiltration Over C2 Channel
- **T1021** — Remote Services
- **T1589** — Gather Victim Identity Information
- **T1583** — Acquire Infrastructure
- **T1562** — Impair Defenses
- **T1083** — File and Directory Discovery
- **T1486** — Data Encrypted for Impact

NIST-800-53R5

- **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
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems

- **AC-3** — Access Enforcement
- **CM-7** — Least Functionality
- **AU-9** — Protection of Audit Information
- **CM-6** — Configuration Settings
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **SC-28** — Protection of Information at Rest
- **IR-4** — Incident Handling

OWASP-TOP10-2021

- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **5.2** — Use Unique Passwords
- **6.3** — Require MFA for Externally-Exposed Applications
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(a)(1)** — Access Control
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(d)** — Person or Entity Authentication

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.8.8** — Management of technical vulnerabilities

SOC2-TSC

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1587.001	Malware	Resource-Development
T1566	Phishing	Initial-Access

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1133	External Remote Services	Persistence
T1041	Exfiltration Over C2 Channel	Exfiltration
T1021	Remote Services	Lateral-Movement
T1589	Gather Victim Identity Information	Reconnaissance
T1583	Acquire Infrastructure	Resource-Development
T1562	Impair Defenses	Defense-Evasion
T1083	File and Directory Discovery	Discovery
T1486	Data Encrypted for Impact	Impact

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/threat-intelligence/gentlemen-raas-gang...	T3
K000157317: BIND vulnerability CVE-2025-8677 - MyF5 | Support	https://my.f5.com/manage/s/article/K000157317	T3
CVE-2025-4615 PAN-OS: Improper Neutralization of Input in the ...	https://security.paloaltonetworks.com/CVE-2025-4615	T3
Reducing the Significant Risk of Known Exploited Vulnerabilities	https://www.cisa.gov/known-exploited-vulnerabilities	T1
A security vulnerability has been identified that affects games and ...	https://www.reddit.com/r/Unity3D/comments/1nwsu97/a_security_vulner...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-05-13 18:56 UTC by TJS Security Command Center