INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-23 06:39 UTC

New Ransomware Group 'The Gentlemen' Scales Rapidly, Signals Operational Maturity

THREAT ACTOR | HIGH | CVSS 7.5

SCC Item ID	SCC-TAC-2026-0008
Type	Threat Actor
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Not specified, sector targeting not confirmed in available source data
Published	2026-04-22T16:51:55
Discovery Source	Rss

Executive Summary

A new ransomware group called 'The Gentlemen' is expanding quickly and shows signs of operating under a ransomware-as-a-service model, meaning it likely has access to professional-grade attack tools and a network of affiliates. No confirmed victims, targeted sectors, or ransom figures have been published at this stage; reporting is early and attribution confidence is low. Organizations should treat this as an emerging threat worth monitoring, particularly those with internet-facing infrastructure or known exposure to RaaS-style intrusion vectors.

Technical Analysis

No CVE, CWE, or confirmed technical indicators of compromise are associated with this report. The Gentlemen appear to operate under a RaaS model based on behavioral characteristics observed by researchers at this stage of reporting. MITRE ATT&CK techniques mapped to this group's probable methodology include: T1057 (Process Discovery), T1486 (Data Encrypted for Impact), T1082 (System Information Discovery), T1021 (Remote Services), T1133 (External Remote Services), T1588.002 (Tool Procurement), T1560 (Archive Collected Data), T1567.002 (Exfiltration to Cloud Storage), T1078 (Valid Accounts), T1567 (Exfiltration Over Web Service), T1490 (Inhibit System Recovery), T1489 (Service Stop), and T1059 (Command and Scripting Interpreter). These techniques are consistent with a double-extortion RaaS playbook: initial access via valid accounts or external remote services, internal reconnaissance, data staging and exfiltration, then encryption with recovery inhibition. No confirmed encryptor, negotiation portal, leak site URL, or affiliate indicators have been published. The CVSS score of 7.5 present in the source data is a data artifact with no associated vulnerability; it is not applicable to this threat actor profile. Primary sourcing is a single T3 news article from Dark Reading. Additional URLs encountered during ingestion referenced CSP header content unrelated to this threat

actor and are not included in the source list.

Action Checklist

1. Monitor: Add 'The Gentlemen' as a tracked threat actor in your threat intelligence platform and subscribe to updates from Dark Reading, CISA, and MITRE ATT&CK for new IOCs, TTPs, or victim sector disclosures as reporting matures.
2. Detection: Hunt for MITRE T1133 and T1078 indicators - review authentication logs for unusual use of valid accounts, external remote service logins (VPN, RDP, Citrix) from anomalous geolocations or off-hours access patterns, and new service account creation without change tickets.
3. Hardening: Audit internet-facing remote access infrastructure (RDP, VPN concentrators, external-facing SMB). Disable or restrict T1133-mapped services not in active use. Enforce MFA on all external access paths consistent with NIST SP 800-53 IA-2.
4. Recovery Resilience: Verify that backup systems are offline or immutable and that restoration procedures have been tested recently; RaaS operators routinely target T1490 (inhibit system recovery) by deleting shadow copies and disabling backup agents before deploying encryptors.
5. Post-Discovery: Document the current threat actor profile gap in your risk register. Schedule a re-evaluation once a second credible source confirms sector targeting, IOCs, or victim data. Do not treat early-stage reporting as confirmed threat intelligence without corroboration.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to incident commander and executive leadership if: (1) any T1133/T1078 hunting query returns a confirmed match tied to an unrecognized external IP or unauthorized service account; (2) 'vssadmin list shadows' returns zero results on a production Windows server with no documented VSS policy change; or (3) a second credible source (CISA advisory, ISAC bulletin, or MITRE ATT&CK group page update) confirms The Gentlemen's sector targeting overlaps with your organization's industry vertical, at which point the triage priority should be immediately re-evaluated as 'immediate' and breach notification assessment for PII/PHI data exposure should be initiated per applicable regulatory requirements.
Recovery Notes	Post-containment, prioritize restoring internet-facing systems from verified clean backups only after confirming VSS integrity and backup agent health were not compromised during any undetected dwell period. Monitor re-enabled external access services (VPN, RDP) for 30 days post-hardening using enhanced logging at the authentication layer, specifically watching for T1078 re-use of any credentials that were active during the exposure window — those credentials should be considered potentially compromised and rotated before service restoration. Maintain the actor tracking entry in the risk register on a 30-day re-evaluation cadence until MITRE ATT&CK or CISA publish a confirmed profile with IOCs, at which point conduct a full retrospective hunt against the 90-day log baseline established during preparation.

Forensic Artifacts	Windows Security Event Log — Event IDs 4624 (logon type 10, RemoteInteractive), 4625 (failed logon), 4720 (account created), 4728/4732 (group membership changes): primary evidence source for T1078 valid account abuse and T1133 external remote service initial access consistent with RaaS affiliate tradecraft | VPN concentrator authentication logs (Cisco ASA, Palo Alto GlobalProtect, Fortinet SSL-VPN raw syslogs): preserve full session records including source IP, geolocation, authentication method, and session duration to identify credential-based initial access attempts before confirmed IOC publication | VSS and backup agent state artifacts — 'vssadmin list shadows' output, Windows System Event ID 7036 (service state changes) for VSS and backup agent services, and registry key 'HKLM:\SYSTEM\CurrentControlSet\Services\VSS': primary indicators of T1490 (Inhibit System Recovery) pre-encryption staging, which RaaS operators including emerging groups execute before deploying encryptors | Active Directory replication metadata and tombstone objects — run 'repadmin /showchanges' and query AD for accounts modified or created in the past 90 days without corresponding change management records: RaaS affiliates commonly create or hijack service accounts for persistence (T1078.002) before lateral movement to backup infrastructure | Firewall and perimeter session logs for inbound TCP 3389 (RDP), TCP 445 (SMB), and SSL-VPN ports from external CIDR ranges: establishes a baseline of external exposure and provides evidence of reconnaissance or access attempts against the T1133-mapped attack surface that The Gentlemen's affiliates are most likely to exploit given the RaaS operational model described in source reporting

Per-Action IR Details

Monitor — Add 'The Gentlemen' as a tracked threat actor in your threat intelligence platform and subscribe to updates from Dark Reading, CISA, and MITRE ATT&CK for new IOCs, TTPs, or victim sector disclosures as reporting matures.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing threat intelligence feeds and actor tracking as a precondition to effective detection and response

Controls: NIST IR-4 (Incident Handling) — Maintain capability to ingest and act on emerging threat actor intelligence, NIST SI-5 (Security Alerts, Advisories, and Directives) — Subscribe to external organizations for ongoing security alerts and advisories on The Gentlemen as reporting matures, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — Incorporate emerging RaaS actor intelligence into vulnerability and risk prioritization workflows

Compensating: Without a commercial TIP, create a dedicated tracking file (CSV or Obsidian note) for 'The Gentlemen' actor profile. Set Google Alerts for the actor name plus 'ransomware.' Subscribe to the free CISA Known Exploited Vulnerabilities RSS feed and bookmark the MITRE ATT&CK Groups page. Use OpenCTI (free, open-source) to ingest MITRE ATT&CK STIX bundles and tag actor-linked TTPs. Assign one analyst to review Dark Reading and BleepingComputer weekly for new attribution or IOC disclosures.

Evidence: At this preparation stage, no active forensic evidence collection is triggered. However, establish a baseline now: export current VPN authentication logs (covering the past 90 days), Active Directory account creation records (Event ID 4720), and a snapshot of all currently enabled external remote access service configurations (RDP enabled hosts via 'Get-ItemProperty HKLM:\System\CurrentControlSet\Control\Terminal Server'), so anomalies introduced after actor IOC publication can be detected against a known-good baseline.

Detection — Hunt for MITRE T1133 and T1078 indicators: review authentication logs for unusual use of valid accounts, external remote service logins (VPN, RDP, Citrix) from anomalous geolocations or off-hours access patterns, and new service account creation without change tickets.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Correlating authentication anomalies and external remote service abuse consistent with RaaS initial access tradecraft attributed to T1133 and T1078

Controls: NIST SI-4 (System Monitoring) — Monitor authentication events and remote access services for indicators consistent with T1133 (External Remote Services) and T1078 (Valid Accounts) abuse, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — Perform targeted review of VPN, RDP, and Citrix authentication logs for geolocation anomalies and off-hours access patterns, NIST IR-5 (Incident Monitoring) — Track and document all authentication anomalies identified during hunting as candidate incidents pending corroboration, CIS 8.2 (Collect Audit Logs) — Ensure VPN concentrator, Windows Security Event Log, and Citrix access logs are collected and retained to support T1133/T1078 hunting

Compensating: Without SIEM: Run the following PowerShell on domain controllers to surface new service accounts created in the past 30 days without a corresponding change ticket timestamp window: 'Get-ADUser -Filter {whenCreated -ge ((Get-Date).AddDays(-30))} -Properties whenCreated,Description | Where-Object {$_.Description -notmatch "ticket"}'. For VPN/RDP geolocation anomalies, export authentication logs and run them through the free tool 'GeoIP2' (MaxMind free tier) or parse with a bash one-liner against an IP geolocation CSV. Deploy Sysmon with the SwiftOnSecurity config and filter on Event ID 3 (Network Connection) for RDP (port 3389) and SMB (port 445) originating from external IPs. Use the Sigma rule 'win_susp_failed_logon_source.yml' from the SigmaHQ repository to hunt Windows Security Event ID 4625 (failed logons) clustered by source IP.

Evidence: Before concluding analysis, preserve: Windows Security Event Log entries for Event ID 4624 (successful logon, logon type 10 = RemoteInteractive) and 4625 (failed logon) filtered to external source IPs; VPN authentication logs from the concentrator (Cisco ASA, Palo Alto GlobalProtect, Fortinet SSL-VPN — export raw syslogs, do not rely on dashboard summaries); Citrix NetScaler access logs at '/var/nslog/ns.log' filtered for authentication events; Active Directory event ID 4720 (account created) and 4728/4732 (member added to security/local group) from domain controllers; and firewall session logs showing RDP (TCP 3389) or SMB (TCP 445) inbound connections from non-approved external CIDR ranges.

Hardening — Audit internet-facing remote access infrastructure (RDP, VPN concentrators, external-facing SMB). Disable or restrict T1133-mapped services not in active use. Enforce MFA on all external access paths consistent with NIST SP 800-53 IA-2.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment: Reducing attack surface by disabling or restricting external remote services that represent the primary initial access vector for RaaS affiliates operating under The Gentlemen's model

Controls: NIST IA-2 (Identification and Authentication — Organizational Users) — Enforce MFA on all external-facing access paths including VPN, RDP gateways, and Citrix to counter T1078 credential abuse, NIST CM-7 (Least Functionality) — Disable or restrict RDP, SMB, and other remote services on internet-facing assets not required for documented business operations, NIST SC-7 (Boundary Protection) — Enforce network boundary controls to block direct inbound RDP (TCP 3389) and SMB (TCP 445) from the internet at the perimeter firewall, CIS 4.4 (Implement and Manage a Firewall on Servers) — Implement host-based firewall rules on all servers to block inbound RDP and SMB from non-management CIDR ranges, CIS 6.3 (Require MFA for Externally-Exposed Applications) — Require MFA on all externally-exposed remote access services to reduce T1078 valid account abuse impact, CIS 6.4 (Require MFA for Remote Network Access) — Require MFA for all remote network access, directly countering RaaS affiliate credential-based initial access

Compensating: To identify exposed RDP/SMB: run 'nmap -p 3389,445,1433 --open -iL internet_facing_hosts.txt' from an external vantage point (use a cloud VM if no external scanner exists). To disable RDP on Windows hosts where not required: 'Set-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Terminal Server" -Name fDenyTSConnections -Value 1'. To block inbound RDP at the Windows firewall: 'netsh advfirewall firewall add rule name="Block RDP Inbound" protocol=TCP dir=in localport=3389 action=block'. For MFA on RDP without commercial tooling, deploy Duo Security free tier (up to 10 users) or configure Windows NPS with RADIUS to require certificate-based authentication. For SMB, enforce signing via GPO: Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > 'Microsoft network server: Digitally sign communications (always)' = Enabled.

Evidence: Before making changes, snapshot the current state for change validation and potential evidence preservation: export 'netstat -ano' output from all internet-facing hosts to document active listening services; capture registry key 'HKLM:\System\CurrentControlSet\Control\Terminal Server\fDenyTSConnections' value; export current firewall rules via 'netsh advfirewall export firewall_baseline.wfw'; and record all currently active VPN user sessions from

the concentrator management interface before any account disablement actions are taken.

Recovery Resilience — Verify that backup systems are offline or immutable and that restoration procedures have been tested recently; RaaS operators routinely target T1490 (inhibit system recovery) by deleting shadow copies and disabling backup agents before deploying encryptors.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Verifying backup integrity and immutability as a precondition to recovery capability against RaaS operators who pre-stage T1490 actions to eliminate recovery options before encryption

Controls: NIST CP-9 (System Backup) — Verify backup copies are stored offline or in immutable storage, and that backup integrity is validated through test restores, specifically against T1490 shadow copy deletion and backup agent tampering, NIST SI-7 (Software, Firmware, and Information Integrity) — Verify integrity of backup agents and backup software binaries on protected systems to detect T1490-stage tampering prior to encryptor deployment, NIST IR-4 (Incident Handling) — Incorporate T1490 pre-encryption staging detection into the incident handling playbook as an early ransomware indicator, CIS 7.2 (Establish and Maintain a Remediation Process) — Validate that backup restoration SLAs are documented and tested, with priority given to systems most exposed to RaaS lateral movement paths

Compensating: To check for existing VSS deletion (a T1490 indicator of prior compromise): run 'vssadmin list shadows' on all Windows servers — zero results on a system with no recent Group Policy change is a red flag. To verify backup agent integrity: check the Windows Services list for backup agent services (e.g., Veeam Backup Agent: 'VeeamAgentSvc'; Windows Server Backup: 'wbengine') using 'Get-Service | Where-Object {$_.Name -match "backup|veeam|backup exec"}' and confirm running state and binary hash against vendor-published values. For immutability verification without enterprise backup: confirm S3 Object Lock status via AWS CLI 'aws s3api get-object-lock-configuration --bucket ' or verify offline media is physically disconnected. Test restore: perform a documented file-level restore from the most recent backup of one critical system and record the RTO achieved.

Evidence: Before any recovery validation steps, collect: output of 'vssadmin list shadows' from all Windows hosts (absence of shadow copies on recently modified systems may indicate prior T1490 staging); Windows System Event Log entries for Event ID 7036 (service state change) filtered on backup-related services to detect agent disablement; registry key 'HKLM:\SYSTEM\CurrentControlSet\Services\VSS' to verify VSS service configuration has not been altered; and backup server access logs to detect unauthorized authentication or configuration changes to backup jobs that could indicate pre-encryption backup sabotage by a RaaS affiliate already present in the environment.

Post-Discovery — Document the current threat actor profile gap in your risk register. Schedule a re-evaluation once a second credible source confirms sector targeting, IOCs, or victim data. Do not treat early-stage reporting as confirmed threat intelligence without corroboration.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Documenting intelligence gaps and scheduling structured re-evaluation as part of the lessons-learned and risk posture update process when confirmed attribution and IOC data are unavailable

Controls: NIST IR-8 (Incident Response Plan) — Update the IR plan and risk register to reflect the identified gap in confirmed threat intelligence for The Gentlemen, and schedule a structured re-evaluation trigger tied to second-source corroboration, NIST RA-3 (Risk Assessment) — Document the residual risk associated with low-confidence early-stage reporting on The Gentlemen actor in the organizational risk register, with explicit acknowledgment of attribution uncertainty, NIST SI-5 (Security Alerts, Advisories, and Directives) — Establish a structured cadence for reviewing CISA, MITRE ATT&CK, and sector-specific ISACs for corroborating intelligence on The Gentlemen before elevating response posture, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — Integrate the actor tracking re-evaluation milestone into the vulnerability management cycle so that confirmed sector targeting triggers a reassessment of exposure priority

Compensating: Without a GRC platform, create a plain-text or spreadsheet risk register entry for 'The Gentlemen — Emerging RaaS Actor' with fields: date first observed, source (single-source, unconfirmed), confidence level (LOW), re-evaluation trigger (second credible source confirms sector targeting or IOC publication), and assigned owner. Set a calendar reminder for 30-day review. Use a simple traffic-light status: RED = confirmed targeting, AMBER =

single-source (current status), GREEN = no credible reporting. Link the entry to the VPN/RDP hardening actions taken under the containment step so the risk register reflects compensating controls already applied.

Evidence: Document as record artifacts for the risk register entry: a timestamped export of the original Dark Reading or source advisory text; the list of hardening actions taken (VPN audit results, MFA enforcement status, RDP exposure scan output from the containment step); the current 'vssadmin list shadows' and backup verification outputs from the recovery resilience step; and a written attestation of the single-source, low-confidence status of current reporting on The Gentlemen, signed by the responsible analyst or IR lead, to establish an auditable baseline for future re-evaluation against NIST IR-6 (Incident Reporting) documentation requirements.

Detection Guidance

No confirmed IOCs are available for The Gentlemen at this reporting stage. Detection should focus on behavioral patterns consistent with the mapped ATT&CK techniques. Key signals: (1) T1078/T1133, authentication events from valid accounts at unusual times or locations, failed-then-succeeded login sequences, new VPN or RDP sessions from residential or Tor-exit IPs; (2) T1082/T1057, process enumeration commands (tasklist, net group, wmic) executed by non-admin accounts or scripting interpreters; (3) T1560/T1567.002, large archive creation events (7zip, WinRAR) followed by outbound data transfers to cloud storage endpoints (Mega, Dropbox, file.io); (4) T1490/T1489, vssadmin delete shadows, bcdedit recovery mode changes, or service-stop sequences targeting backup agents (Veeam, VSS, Windows Backup). Log sources: Windows Security Event Log (event IDs 4624, 4625, 4648, 4672), Sysmon (process creation, network connections), EDR telemetry, and firewall egress logs. No specific YARA rules or network signatures have been published as of this report.

Framework Mappings

MITRE-ATTACK

- **T1057** — Process Discovery
- **T1486** — Data Encrypted for Impact
- **T1082** — System Information Discovery
- **T1021** — Remote Services
- **T1133** — External Remote Services
- **T1588.002** — Tool
- **T1560** — Archive Collected Data
- **T1567.002** — Exfiltration to Cloud Storage
- **T1078** — Valid Accounts
- **T1567** — Exfiltration Over Web Service
- **T1490** — Inhibit System Recovery
- **T1489** — Service Stop
- **T1059** — Command and Scripting Interpreter

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-17** — Remote Access

- **AC-3** — Access Enforcement
- **CM-7** — Least Functionality
- **IA-2** — Identification and Authentication (Organizational Users)
- **AC-20** — Use of External Systems
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **CM-6** — Configuration Settings
- **SI-4** — System Monitoring
- **SI-3** — Malicious Code Protection
- **SI-7** — Software, Firmware, and Information Integrity
- **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.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.8.24** — Use of cryptography

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1057	Process Discovery	Discovery
T1486	Data Encrypted for Impact	Impact
T1082	System Information Discovery	Discovery
T1021	Remote Services	Lateral-Movement
T1133	External Remote Services	Persistence
T1588.002	Tool	Resource-Development
T1560	Archive Collected Data	Collection

Technique ID	Technique Name	Tactic
T1567.002	Exfiltration to Cloud Storage	Exfiltration
T1078	Valid Accounts	Defense-Evasion
T1567	Exfiltration Over Web Service	Exfiltration
T1490	Inhibit System Recovery	Impact
T1489	Service Stop	Impact
T1059	Command and Scripting Interpreter	Execution

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/threat-intelligence/gentlemen-rapidly-r...	T3
Content Security Policy (CSP) Not Implemented - Invicti	https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/c...	T3
Content Security Policy (CSP) Not Implemented - Vulnerabilities	https://www.acunetix.com/vulnerabilities/web/content-security-polic...	T3
Missing content security policy header - issue with chrome and firefox	https://stackoverflow.com/questions/45944031/missing-content-securi...	T3
Vulnerable Missing Content Security Policy (CSP) #9790 - GitHub	https://github.com/roundcube/roundcubemail/issues/9790	T3

Generated 2026-04-23 06:39 UTC by TJS Security Command Center