INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-11 07:44 UTC

The Gentlemen Ransomware Group Emerges as Second Most Active Threat Actor by Victim Count

THREAT ACTOR | HIGH

SCC Item ID	SCC-TAC-2026-0024
Type	Threat Actor
Severity	HIGH
Affected Products	Multiple sectors, specific targets not confirmed from available source data
Published	4 hours ago
Discovery Source	Serper

Executive Summary

A ransomware group calling itself 'The Gentlemen' has been reported by Krebs on Security as second most active by victim count. The group appears to be expanding rapidly, suggesting active affiliate recruitment or accelerated operations across multiple sectors. Organizations in any industry face elevated risk of targeted ransomware extortion, with potential for data encryption, operational disruption, and double-extortion exposure.

Technical Analysis

The Gentlemen is a ransomware threat actor ranked second by victim count per Krebs on Security reporting. Three MITRE ATT&CK techniques are associated with this group based on accessible source data: T1489 (Service Stop), T1486 (Data Encrypted for Impact), and T1190 (Exploit Public-Facing Application). No CVE identifiers, specific malware families, confirmed IOCs, or detailed TTPs are available from the accessible source material. The group's rapid rise suggests either aggressive affiliate recruitment under a ransomware-as-a-service (RaaS) model or consolidation of existing criminal infrastructure. Full technical analysis is limited by source accessibility; the originating Krebs on Security article was not fully retrievable for deeper extraction. Caution: technical details here are bounded by what accessible source data confirms; no inferred specifics have been added.

Action Checklist

1. Step 1: Containment. Audit internet-facing systems for exposure, prioritizing public-facing applications (aligned with T1190). Verify that perimeter controls block unauthorized inbound connections to administrative interfaces and remote access services (NIST AC-17, Remote Access; CIS 4.4, Implement and Manage a Firewall on Servers).
2. Step 2: Detection. Review endpoint and SIEM logs for service-stop events (T1489) and mass file modification or encryption activity (T1486). Query for unexpected termination of backup, security, or database services. Monitor for large-scale file rename or extension-change patterns (NIST AU-6, Audit Record Review, Analysis, and Reporting; CIS 8.2, Collect Audit Logs; D3-LAM, Local Account Monitoring; D3-SFA, System File Analysis).
3. Step 3: Eradication. No specific patch or malware family is confirmed from available data. Harden public-facing application attack surface by applying current vendor patches and reviewing externally exposed services for unnecessary exposure. Disable or restrict accounts not needed for operations (NIST AC-6, Least Privilege; CIS 4.7, Manage Default Accounts on Enterprise Assets and Software; D3-UAP, User Account Permissions).
4. Step 4: Recovery. Validate integrity of backup systems and confirm backups are offline or immutable and not accessible from production networks. Test restoration procedures. Monitor post-incident for re-encryption attempts or persistence mechanisms (NIST AU-9, Protection of Audit Information; CIS 3.4, Enforce Data Retention).
5. Step 5: Post-Incident. Review MFA enforcement on all remote access and administrative accounts, as RaaS groups commonly gain initial access via credential compromise and public-facing exploits. Document control gaps identified during this review (NIST AC-17, Remote Access; 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; D3-MFA, Multi-factor Authentication; D3-CRO, Credential Rotation).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior IR leadership, legal counsel, and executive stakeholders if active encryption is detected on production systems, if PII or PHI is confirmed within the encrypted or exfiltrated dataset (triggering breach notification obligations under HIPAA, state breach laws, or GDPR), or if the organization lacks the internal capability to isolate affected systems within 2 hours of confirmed ransomware activity.
Recovery Notes	Before restoring any system from backup, verify that the backup predates the earliest evidence of threat actor presence in authentication and endpoint logs — RaaS affiliates including The Gentlemen's expected affiliates typically maintain dwell time of days to weeks before deploying ransomware, meaning backups created during that window may contain active malware or attacker-staged tools. Rebuild compromised systems from validated clean images rather than restoring in-place where feasible, and rotate all credentials — domain admin, service accounts, VPN, and externally-exposed application accounts — before bringing restored systems back online. Monitor restored systems intensively for 30 days post-recovery using Sysmon, Windows Event ID 4688 process creation logging, and network flow monitoring for C2 beaconing patterns, as re-infection via undetected persistence is the most common cause of secondary ransomware incidents.

Forensic Artifacts	Windows Security Event Log (Event IDs 4624, 4625, 4648, 4688, 4720, 7036) from all domain controllers, RDP gateways, and VPN concentrators for the 30-day pre-detection window — these logs contain the authentication trail of affiliate initial access via credential compromise or brute force, consistent with RaaS affiliate tradecraft targeting exposed remote access services | VSS shadow copy deletion records: Windows Security Event ID 4688 filtered on vssadmin.exe, wmic.exe with 'shadowcopy delete' arguments, and bcdedit.exe with 'recoveryenabled no' — deliberate shadow copy destruction immediately preceding encryption is a near-universal ransomware pre-encryption step and establishes timeline of attack execution | Ransom note files (README.txt, HOW_TO_DECRYPT.txt, or The Gentlemen-branded variants) collected with full filesystem metadata (creation time, MFT entry, parent directory) — note content typically includes actor-specific Tor negotiation portal URLs and wallet addresses that support attribution, law enforcement referral, and cross-victim correlation via open-source ransomware tracking resources such as Ransomlook or ID Ransomware | Memory acquisition (WinPMEM or DumpIt output) from at least one confirmed-compromised host captured before reboot or eradication — in-memory forensics can reveal injected ransomware payload, C2 beacon configuration, and stolen credentials that are not present in disk artifacts, particularly relevant given RaaS affiliates' use of fileless or living-off-the-land execution techniques aligned with T1059 and T1055 | Network flow logs and proxy/firewall logs showing outbound connections in the 72 hours preceding encryption onset — RaaS double-extortion operations including The Gentlemen's expected model require data exfiltration prior to encryption (T1048, T1567), producing anomalous outbound data volume to cloud storage endpoints (Mega, Rclone targets) or actor-controlled infrastructure that is visible in perimeter logs and proxy categorization data

Per-Action IR Details

Step 1: Containment — audit internet-facing systems for exposure, prioritizing public-facing applications (aligned with T1190); verify that perimeter controls block unauthorized inbound connections to administrative interfaces and remote access services (NIST AC-17 — Remote Access; CIS 4.4 — Implement and Manage a Firewall on Servers)

NIST Phase: Containment

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

Controls: NIST AC-17 (Remote Access), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Run 'netstat -ano' on Windows hosts or 'ss -tlnp' on Linux to enumerate all listening services and correlate PIDs to processes. Use nmap from a jump host to external-scan your own perimeter: 'nmap -sV -p 22,3389,445,5985,8080,8443,9090 ' to identify exposed admin interfaces. Apply Windows Firewall rules via PowerShell: 'New-NetFirewallRule -DisplayName "Block RDP External" -Direction Inbound -Protocol TCP -LocalPort 3389 -RemoteAddress Internet -Action Block'. For Linux, enforce iptables drop rules on ports 22 and 3389 from non-management subnets.

Evidence: Before modifying any firewall rules, capture current state: export 'netsh advfirewall show allprofiles' and 'netstat -ano > baseline_connections.txt' on Windows. On Linux, run 'iptables -L -n -v > iptables_baseline.txt' and 'ss -tlnp > open_ports_baseline.txt'. Preserve router/firewall flow logs and perimeter NAT tables showing inbound connection attempts to RDP (3389), WinRM (5985/5986), SMB (445), and web admin panels — The Gentlemen, consistent with RaaS affiliate tradecraft, commonly leverage exposed RDP and VPN endpoints as initial access vectors aligned with T1190 and T1133.

Step 2: Detection — review endpoint and SIEM logs for service-stop events (T1489) and mass file modification or encryption activity (T1486); query for unexpected termination of backup, security, or database services; monitor for large-scale file rename or extension-change patterns (NIST AU-6 — Audit Record Review, Analysis, and Reporting; CIS 8.2 — Collect Audit Logs; D3-LAM — Local Account Monitoring; D3-SFA —

System File Analysis)

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity config and query Event ID 1 (Process Create) for 'net.exe stop' or 'sc.exe stop' targeting VSS, Veeam, Backup Exec, or Windows Defender services — command pattern: 'Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" | Where-Object {$_.Message -match "net stop|sc stop|vssadmin delete"}'. Use Sigma rule 'ransomware_mass_file_rename.yml' (available in SigmaHQ repository) against Windows Security Event ID 4663 (Object Access) filtered on FileExtensionChange. For Linux, run: 'inotifywait -m -r -e modify,create,moved_to /data /home --format "%T %w%f" --timefmt "%Y%m%d-%H%M%S" >> /var/log/filewatch.log &' to detect mass modification in real time. Query Windows Security Event ID 7036 (Service Control Manager) for services entering stopped state in rapid succession.

Evidence: Capture before any remediation: Windows Security Event Log filtered on Event ID 7036 (service state changes) and 4663 (file access auditing) from the 72 hours preceding detection. Export VSS shadow copy inventory via 'vssadmin list shadows' — ransomware groups including RaaS affiliates consistently delete shadow copies (T1490) immediately before encryption, so absence of recent shadows is a key indicator. Collect Sysmon Event ID 11 (FileCreate) logs showing bulk creation of ransom note files (typically dropped as README.txt, HOW_TO_DECRYPT.txt, or actor-branded variants). Preserve Windows Event ID 4688 (Process Creation) entries for wmic.exe, vssadmin.exe, bcdedit.exe, and powershell.exe with encoded command arguments, all consistent with The Gentlemen's expected pre-encryption kill-chain.

Step 3: Eradication — no specific patch or malware family is confirmed from available data; harden public-facing application attack surface by applying current vendor patches and reviewing externally exposed services for unnecessary exposure; disable or restrict accounts not needed for operations (NIST AC-6 — Least Privilege; CIS 4.7 — Manage Default Accounts on Enterprise Assets and Software; D3-UAP — User Account Permissions)

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Enumerate all local administrator accounts on Windows endpoints: 'Get-LocalGroupMember -Group "Administrators" | Export-Csv local_admins.csv'. Disable accounts not needed: 'Disable-LocalUser -Name '. For domain environments without enterprise tooling, run: 'Get-ADUser -Filter {Enabled -eq $true -and LastLogonDate -lt (Get-Date).AddDays(-45)} | Select Name,LastLogonDate | Export-Csv stale_accounts.csv' to identify dormant accounts that ransomware affiliates may have compromised for persistence. Audit for newly created local accounts (indicator of affiliate backdoor staging) via Event ID 4720 (User Account Created). Run 'net share' and 'Get-SmbShare' to enumerate and remove unnecessary SMB shares that ransomware uses for lateral propagation via T1021.002.

Evidence: Before disabling accounts or removing persistence, image affected systems or capture memory with WinPMEM ('winpmem_mini_x64.exe output.raw') to preserve evidence of injected processes, in-memory credentials, and C2 beaconing activity. Export Windows Security Event Log Event ID 4624 (Logon) and 4648 (Explicit Credential Use) for the 14-day period preceding detection, filtered on LogonType 3 (Network) and LogonType 10 (RemoteInteractive), to identify the account(s) used for initial access and lateral movement. Collect scheduled task exports ('schtasks /query /fo CSV /v > scheduled_tasks.csv') and registry run key dumps ('reg export HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run run_keys.reg') before eradication — The Gentlemen affiliates are expected to deploy persistence mechanisms consistent with T1053 and T1547 to maintain access across reboots.

Step 4: Recovery — validate integrity of backup systems and confirm backups are offline or immutable and not accessible from production networks; test restoration procedures; monitor post-incident for re-encryption

attempts or persistence mechanisms (NIST AU-9 — Protection of Audit Information; CIS 3.4 — Enforce Data Retention)

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-9 (Protection Of Audit Information), NIST AU-11 (Audit Record Retention), CIS 3.4 (Enforce Data Retention)

Compensating: Verify backup integrity before restoration by checking cryptographic hashes of backup archives: 'Get-FileHash -Algorithm SHA256 -Path | Export-Csv backup_hashes.csv' and compare against hashes recorded at backup creation time. Confirm backup media or repositories are isolated: verify no active SMB, NFS, or iSCSI connections from production hosts to backup targets using 'Get-NetTCPConnection | Where-Object {$_.RemotePort -in 445,2049,3260}'. For post-recovery monitoring, deploy Sysmon Event ID 11 (FileCreate) alerting on known ransomware extension patterns (configure via Sysmon config TargetFilename matching '*.encrypted', '*.locked', or actor-specific extensions if identified) and run as a scheduled task with output to a monitored log path. Use osquery to continuously monitor for re-emergence of malicious scheduled tasks: 'SELECT name, path, enabled FROM scheduled_tasks WHERE path NOT IN (SELECT path FROM scheduled_tasks WHERE name LIKE "%Microsoft%")'.

Evidence: Before initiating restoration, document the full encrypted file inventory: 'Get-ChildItem -Recurse -Path | Where-Object {$_.Extension -match "encrypted|locked|[a-z0-9]{5,8}"} | Export-Csv encrypted_files.csv' — this inventory supports insurance claims, regulatory notification obligations, and potential decryption if a decryptor becomes available for The Gentlemen's tooling. Capture ransom note file contents and file metadata (creation timestamp, parent process if determinable from Sysmon logs) as these notes frequently contain actor-specific wallet addresses or negotiation portal URLs useful for attribution and law enforcement referral. Preserve the VSS deletion command history (Event ID 4688 for vssadmin.exe and wmic.exe) as evidence of deliberate backup destruction supporting potential criminal referral.

Step 5: Post-Incident — review MFA enforcement on all remote access and administrative accounts, as RaaS groups commonly gain initial access via credential compromise and public-facing exploits; document control gaps identified during this review (NIST AC-17 — Remote Access; 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; D3-MFA — Multi-factor Authentication; D3-CRO — Credential Rotation)

NIST Phase: Post Incident

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

Controls: NIST AC-17 (Remote Access), NIST AC-7 (Unsuccessful Logon Attempts), 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 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For organizations without enterprise MFA infrastructure, implement free TOTP-based MFA on VPN and RDP using Duo Free tier (up to 10 users) or self-hosted Authelia with a reverse proxy. Enforce account lockout policy via GPO: 'Account lockout threshold: 5 attempts; lockout duration: 30 minutes' — directly counters the credential-stuffing and brute-force techniques used by RaaS affiliates for initial access. Conduct a credential exposure check using the free Have I Been Pwned API against organizational email domains: 'Invoke-RestMethod -Uri "https://haveibeenpwned.com/api/v3/breachedaccount/" -Headers @{"hibp-api-key"=""}' to identify accounts with credentials in known breach datasets that The Gentlemen affiliates may be purchasing or exploiting. Document all identified gaps in a formal lessons-learned report referencing NIST 800-61r3 §4 post-incident activity requirements.

Evidence: Compile the complete authentication log timeline from the incident window: Windows Security Event IDs 4625 (Failed Logon), 4624 (Successful Logon), and 4648 (Explicit Credential Use) across all domain controllers and VPN/remote access gateways — the initial access vector for RaaS affiliates is frequently visible as a spike in 4625 events followed by a successful 4624 LogonType 3 or 10 from an unexpected IP. Export this data with source IP geolocation for law enforcement referral. Preserve any C2 network IOCs extracted from memory dumps or proxy logs (destination IPs, domains, User-Agent strings) — if The Gentlemen's TTPs become better characterized through future reporting, these artifacts enable retrospective matching. Document the MFA gap inventory as a control-gap record supporting compliance remediation tracking under NIST AC-17 and applicable regulatory frameworks.

Detection Guidance

Detection for this threat is limited by the absence of confirmed IOCs or malware signatures in available source data. Focus detection on behavioral indicators aligned with confirmed MITRE techniques. For T1489 (Service Stop): alert on unexpected termination of backup agents, VSS (Volume Shadow Copy Service), endpoint protection services, and database processes; Windows Event IDs 7034, 7035, 7036, and 7045 are relevant. For T1486 (Data Encrypted for Impact): monitor for high-volume file modification events, bulk file renames, and appearance of ransom note files (e.g., README.txt, DECRYPT_FILES.html patterns); file integrity monitoring on critical data directories supports early detection (D3-SFA, System File Analysis). For T1190 (Exploit Public-Facing Application): review web application and network perimeter logs for anomalous inbound requests, authentication failures, or unexpected process spawning from web server processes. No confirmed IOC patterns, hashes, or C2 infrastructure are available from source data; treat any IOC-based hunting as hypothesis-driven until authoritative intelligence is published.

Framework Mappings

MITRE-ATTACK

- **T1489** — Service Stop
- **T1486** — Data Encrypted for Impact
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **CM-6** — Configuration Settings
- **SI-4** — System Monitoring
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **IR-4** — Incident Handling

NIST-CSF-2

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

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan

ISO-27001-2022

- **A.5.29** — Information security during disruption

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1489	Service Stop	Impact
T1486	Data Encrypted for Impact	Impact
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
	https://krebsonsecurity.com/	T3
Brian Krebs - SecureWorld News	https://www.secureworld.io/industry-news/author/brian-krebs	T3
Addressing Risks from Chris Krebs and Government Censorship	https://www.whitehouse.gov/presidential-actions/2025/04/addressing-...	T1
Brian Krebs - Wikipedia	https://en.wikipedia.org/wiki/Brian_Krebs	T3
Krebs on Security posts | daily.dev	https://app.daily.dev/sources/krebsonsecurity	T3

Generated 2026-06-11 07:44 UTC by TJS Security Command Center