INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-18 06:51 UTC

Ransomware Activity Remains Elevated with Emerging Groups and Extortion-Focused Tactics in Q1 2026

SECURITY ANALYSIS | HIGH

SCC Item ID	SCC-STY-2026-0066
Type	Security Analysis
Severity	HIGH
Affected Products	Various industries globally; manufacturing and construction sectors disproportionately targeted
Published	2026-04-16
Discovery Source	Gemini

Executive Summary

GuidePoint Security's Q1 2026 ransomware report documents sustained attack volumes of 150-200 victim posts per week on leak sites, with a measurable shift toward data theft and extortion over encryption, a tactical evolution that reduces attacker complexity while preserving financial leverage. Manufacturing and construction sectors absorb disproportionate impact, driven by operational technology dependencies and historically underdeveloped security programs. The emergence of new groups like 'The Gentlemen' signals continued RaaS ecosystem growth, lowering barriers to entry and expanding the threat actor pool available to target organizations across all sectors.

Technical Analysis

GuidePoint Security's Q1 2026 ransomware data captures a threat landscape in active tactical evolution. Leak site victim post rates, averaging 150-200 per week, reflect sustained high-volume operations across the RaaS ecosystem, with no indication of slowdown attributable to law enforcement disruptions from prior quarters.

The most operationally significant shift is the prioritization of data theft and extortion (T1657) over encryption-led attacks. Where traditional ransomware campaigns required actors to deploy, execute, and manage encryption payloads across victim environments, exfiltration-first models reduce dwell-time exposure, eliminate decryption negotiation complexity, and maintain equivalent leverage. Actors exfiltrate data via tools mapped to T1567.002 (Exfiltration to Code Repository or cloud storage services), then threaten publication on leak sites. This approach is harder to detect before leverage is established and reduces effectiveness of many recovery-focused defenses like backup validation and decryption key negotiation.

Initial access tradecraft continues to rely on valid account abuse (T1078) and reconnaissance against externally accessible infrastructure (T1590). Service disruption (T1489) and encryption (T1486) remain in the toolkit but appear selectively deployed where maximum operational disruption increases payout pressure, most relevant in manufacturing and OT-adjacent environments.

Manufacturing and construction sectors remain primary targets for structural reasons: OT/IT convergence creates environments where downtime tolerance is measured in hours, not days; legacy systems resist rapid patching cycles; and security maturity lags IT-native sectors. Deloitte's smart factory security analysis identifies segmentation failures between corporate IT and OT environments as a persistent structural gap that ransomware operators actively exploit.

'The Gentlemen' is flagged as an emerging actor in the Q1 2026 report. Specific TTPs, infrastructure, or victim patterns for this group are not available in the provided source material. Security teams should monitor threat intelligence feeds for emerging attribution data as this actor's operational profile develops.

Confidence note: Core trends described here are consistent with CISA ransomware advisories and established industry reporting. Specific statistics (150-200 posts per week) and actor attribution ('The Gentlemen') derive from the GuidePoint Security Q1 2026 report as described in secondary source data. The primary report was not directly reviewed. Figures should be validated against the published GuidePoint report before use in formal risk documentation.

Action Checklist

1. Step 1: Assess sector exposure. If your organization operates in manufacturing, construction, or any OT-adjacent environment, treat this report as directly applicable and prioritize accordingly.
2. Step 2: Audit data exfiltration controls. Review DLP policies, cloud storage egress rules, and monitoring coverage for T1567.002 patterns; exfiltration-first attacks will not trigger encryption-based alerts.
3. Step 3: Validate account hygiene. Audit privileged account inventories, enforce phishing-resistant MFA on all externally accessible systems, and review VPN/RDP exposure consistent with T1078 and T1590 tradecraft.
4. Step 4: Review OT/IT segmentation. Verify that network segmentation between operational technology and corporate IT environments is enforced and tested; flat networks in manufacturing environments are a documented enabler of ransomware lateral movement.
5. Step 5: Update threat register. Add 'The Gentlemen' as an emerging tracked actor; assign an owner to monitor emerging TTPs, infrastructure indicators, and victim patterns as intelligence matures.
6. Step 6: Test backup and recovery posture. Confirm that backups are offline or immutable, test restoration procedures, and document RTO/RPO against realistic ransomware scenarios including data-only extortion with no encryption event.
7. Step 7: Monitor GuidePoint Security Q1 2026 report. Obtain the primary report directly to validate the 150-200 weekly victim post figures and any published IOCs before using statistics in board-level risk reporting.

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate immediately to CISO and legal counsel if network monitoring detects confirmed outbound bulk data transfer to cloud storage endpoints (T1567.002) exceeding 1GB from any OT-adjacent host, any file server, or any host holding PII, PHI, or regulated data — this constitutes a potential extortion-triggering exfiltration event that may satisfy breach notification thresholds under GDPR Article 33, HIPAA §164.400, or applicable state privacy laws regardless of whether encryption occurs.
Recovery Notes	For extortion-first ransomware with no encryption event, recovery is primarily a data exposure and legal response rather than a systems restoration exercise — verify the integrity and isolation of backup repositories before assuming they are usable, and use 'vssadmin list shadows' and backup job audit logs to confirm threat actors did not tamper with recovery options during the pre-extortion dwell period. Monitor all previously compromised or at-risk accounts for re-authentication attempts for a minimum of 90 days post-containment, as ransomware groups frequently maintain persistent access via additional backdoors or valid accounts for re-extortion campaigns. Conduct a post-incident review specifically evaluating whether existing encryption-triggered alerting would have detected this attack at all, and update detection rules to cover exfiltration volume anomalies, Rclone/MEGAcmd process execution, and T1567.002 network patterns as the primary detection layer.
Forensic Artifacts	Proxy and firewall egress logs showing outbound sessions to mega.nz, Rclone CDN endpoints, GoFile, or anonymous file-sharing services — specifically look for sessions with cumulative transfer sizes exceeding 500MB from a single internal host within a 24-hour window, which is characteristic of ransomware group bulk staging behavior prior to extortion demand | Sysmon Event ID 1 (Process Creation) logs for rclone.exe, MEGAcmd.exe, 7z.exe, and WinRAR.exe with command-line arguments referencing network share paths or specific data directories — ransomware operators staging exfiltration frequently compress and chunk data before upload, leaving distinctive CLI argument patterns | Windows Security Event Log Event ID 4624 (Logon Type 3 and 10) from file servers and domain controllers showing lateral movement from IT subnets into OT-range hosts in the hours or days preceding any detected exfiltration activity — this establishes the lateral movement timeline consistent with T1078 and T1021 tradecraft used in manufacturing-targeted campaigns | VSS shadow copy inventory and deletion event logs — query Windows Event Log for Event ID 524 (VSS snapshot deleted) and PowerShell Event ID 4104 (Script Block Logging) for 'vssadmin delete shadows' or 'wmic shadowcopy delete' commands, which ransomware groups execute via T1490 to eliminate recovery options before issuing extortion demands | Active Directory replication metadata and NTDS.dit access timestamps — ransomware operators using T1003.003 (NTDS credential dumping) to harvest domain credentials for bulk access leave forensic traces in domain controller Security Event Log Event ID 4662 (Directory Service Object Access) and Event ID 7045 (New Service Installed) if they deploy dumping tools as temporary services

Per-Action IR Details

Step 1: Assess sector exposure — if your organization operates in manufacturing, construction, or any OT-adjacent environment, treat this report as directly applicable and prioritize accordingly

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR capability and prioritizing risk based on threat landscape relevance

Controls: NIST IR-8 (Incident Response Plan) — update plan to explicitly scope OT-adjacent environments and ransomware extortion-only scenarios, NIST RA-3 (Risk Assessment) — assess likelihood and impact specifically for manufacturing/construction OT exposure against GuidePoint Q1 2026 findings, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — confirm OT assets, SCADA endpoints, HMIs, and engineering workstations are

inventoried and tagged by criticality, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — scope vulnerability management program to include OT-adjacent systems that are frequently excluded from standard enterprise scanning

Compensating: Run a two-person asset discovery sweep using nmap ('nmap -sn 10.0.0.0/8 -oX assets.xml') against OT VLAN ranges and compare output against last known inventory. Use the free OT-specific asset profiling tool Dragos Community Edition or Claroty Free Tier where available. Document any unmanaged PLCs, HMIs, or engineering workstations discovered — these are the flat-network enablers cited in GuidePoint's sector analysis.

Evidence: Before scoping decisions are finalized, capture current network topology diagrams, firewall rule exports, and any existing IT/OT segmentation documentation. Pull the last 90 days of DHCP lease logs to identify OT-range hosts that communicated with corporate IT subnets — this baseline is critical for later lateral movement analysis if an incident is declared.

Step 2: Audit data exfiltration controls — review DLP policies, cloud storage egress rules, and monitoring coverage for T1567.002 patterns; exfiltration-first attacks will not trigger encryption-based alerts

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Expanding detection coverage to match attacker TTPs when encryption-based alerting is insufficient for exfiltration-first ransomware

Controls: NIST SI-4 (System Monitoring) — extend monitoring scope to cover T1567.002 (Exfiltration to Cloud Storage) via outbound traffic to Mega.nz, AWS S3, Google Drive, Dropbox, and Rclone endpoints, NIST AU-2 (Event Logging) — verify that proxy logs, firewall egress logs, and DNS query logs capture large outbound transfers to cloud storage providers associated with ransomware staging, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — establish a daily review cadence for anomalous outbound transfer volume, particularly off-hours bulk uploads exceeding 1GB, CIS 13.1 (Centralize Security Event Alerting) — consolidate proxy, DNS, and firewall egress logs to detect Rclone or MEGAcmd command patterns used by ransomware groups for T1567.002 staging

Compensating: Without a SIEM, deploy Zeek (Bro) on a network tap or SPAN port and write a custom script to alert on HTTP POST volumes exceeding a threshold to known cloud storage FQDNs (mega.nz, rclone.org CDN endpoints, amazonaws.com, storage.googleapis.com). On Windows endpoints, use Sysmon Event ID 3 (Network Connection) filtered for processes like rclone.exe, MEGAcmd.exe, or curl.exe making outbound connections to port 443 destinations on those domains. Query: 'Get-WinEvent -LogName Microsoft-Windows-Sysmon/Operational | Where {$_.Id -eq 3} | Where {$_.Message -match "mega.nz|rclone"}'

Evidence: Capture the following before modifying any egress rules: (1) Full proxy access logs for the past 30 days filtered on cloud storage FQDNs associated with T1567.002 tradecraft — mega.nz, put.io, Gofile; (2) DNS query logs for Rclone configuration domains and dynamic DNS providers commonly used as exfil staging; (3) NetFlow or firewall session logs showing cumulative outbound byte counts per source host over 24-hour windows — exfiltration-first groups stage data in large batches, leaving distinctive volume spikes that encryption-triggered alerts would never surface.

Step 3: Validate account hygiene — audit privileged account inventories, enforce phishing-resistant MFA on all externally accessible systems, and review VPN/RDP exposure consistent with T1078 and T1590 tradecraft

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Hardening authentication and access controls against valid account abuse (T1078) and reconnaissance-enabled credential targeting (T1590) prior to an incident

Controls: NIST AC-2 (Account Management) — audit all privileged accounts including service accounts, local admin accounts on OT engineering workstations, and VPN accounts not governed by IdP lifecycle management, NIST IA-5 (Authenticator Management) — enforce FIDO2 or certificate-based MFA on all VPN gateways, RDP jump hosts, and externally exposed management interfaces; SMS/TOTP is insufficient against SIM-swap and real-time phishing proxies used by ransomware initial access brokers, NIST AC-17 (Remote Access) — inventory all RDP-exposed surfaces; require all RDP to route through an MFA-enforced gateway and disable direct RDP (TCP/3389) exposure at the perimeter firewall, CIS 6.3 (Require MFA for Externally-Exposed Applications) — validate MFA enforcement on VPN, RDP gateways, webmail, and any cloud admin consoles accessible without VPN, CIS 5.3 (Disable Dormant Accounts) — identify and disable accounts inactive for 45+ days, with particular attention to contractor accounts and OT vendor remote access credentials that are frequently left active between site visits

Compensating: Run 'net user /domain' and 'Get-ADUser -Filter {Enabled -eq $true} -Properties LastLogonDate | Where {$_.LastLogonDate -lt (Get-Date).AddDays(-45)}' to enumerate stale privileged accounts. For RDP exposure, use Shodan Community (free tier) with query 'port:3389 org:"YOUR-ASN"' to validate external RDP surface. Deploy free MFA via Duo Free tier (up to 10 users) or enforce Windows Hello for Business on priority admin workstations as phishing-resistant credential options for small teams.

Evidence: Before revoking or modifying any accounts, export: (1) Windows Security Event Log Event ID 4624 (Successful Logon) and 4625 (Failed Logon) from VPN concentrators, RDP gateways, and domain controllers for the past 30 days — filter on Logon Type 3 (Network) and Type 10 (RemoteInteractive) for off-hours or foreign-IP originating sessions; (2) VPN authentication logs filtered for accounts that authenticated from residential ISP ranges or Tor exit nodes, consistent with T1078 initial access broker tradecraft; (3) Active Directory audit log Event ID 4720 (Account Created) and 4728 (Member Added to Security-Enabled Global Group) for the past 90 days to identify persistence accounts created post-compromise.

Step 4: Review OT/IT segmentation — verify that network segmentation between operational technology and corporate IT environments is enforced and tested; flat networks in manufacturing environments are a documented enabler of ransomware lateral movement

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Verifying containment architecture before an incident to limit blast radius of ransomware lateral movement across IT/OT boundaries

Controls: NIST SC-7 (Boundary Protection) — verify that firewall ACLs between OT VLANs and corporate IT are deny-by-default with documented exceptions; manufacturing ransomware groups exploit flat Layer 2 adjacency to pivot from IT to HMI/SCADA systems, NIST CM-7 (Least Functionality) — disable all unnecessary protocols between IT and OT zones, specifically SMB (TCP/445), WMI (TCP/135), and WinRM (TCP/5985/5986) which ransomware uses for lateral movement via T1021.002 and T1047, NIST CA-9 (Internal System Connections) — formally document and authorize all IT-to-OT connections; any undocumented connection discovered during this audit should be treated as a potential persistence mechanism, CIS 4.4 (Implement and Manage a Firewall on Servers) — enforce host-based firewall rules on OT engineering workstations to block inbound SMB and RPC from IT subnets even if network-level segmentation is bypassed

Compensating: Use nmap to actively validate segmentation: from a corporate IT host, run 'nmap -p 445,3389,5985,135 --open' — any responsive hosts represent a segmentation failure and a lateral movement path. Use Wireshark with a SPAN port on the IT/OT boundary switch to capture 24 hours of cross-segment traffic and identify undocumented flows. For host-level blocking, deploy Windows Firewall via Group Policy to deny inbound SMB and WMI from corporate IP ranges on all OT workstations running Windows-based HMI software.

Evidence: Before modifying firewall rules, capture: (1) A full export of current ACLs from all firewalls and managed switches governing IT/OT boundary traffic — this is your legal and operational baseline; (2) NetFlow or firewall session logs showing all IT-to-OT-subnet connections in the past 30 days, particularly any SMB (445), RPC (135), or RDP (3389) sessions which are the primary lateral movement protocols used by ransomware groups in manufacturing environments; (3) Switch ARP table snapshots from OT VLAN interfaces to identify any IT-subnet hosts that have Layer 2 adjacency to OT assets, indicating VLAN misconfiguration.

Step 5: Update threat register — add 'The Gentlemen' as an emerging tracked actor; assign an owner to monitor emerging TTPs, infrastructure indicators, and victim patterns as intelligence matures

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Updating threat intelligence baselines and improving detection posture based on emerging actor identification before a confirmed incident occurs

Controls: NIST IR-8 (Incident Response Plan) — update the threat actor section of the IR plan to include 'The Gentlemen' with their documented extortion-first model, distinguishing their TTPs from encryption-primary groups in detection and escalation criteria, NIST SI-5 (Security Alerts, Advisories, and Directives) — establish a formal feed subscription to GuidePoint Security, Recorded Future Free Community, and CISA Known Exploited Vulnerabilities for continuous 'The Gentlemen' TTP updates as intelligence matures, NIST PM-16 (Threat Awareness Program) — assign a named intelligence owner responsible for bi-weekly review of 'The Gentlemen' victim patterns, MITRE ATT&CK technique updates, and dark web leak site monitoring, CIS 7.1 (Establish and Maintain a Vulnerability Management

Process) — incorporate threat actor TTP mapping into vulnerability prioritization so that assets matching 'The Gentlemen' targeting profile (manufacturing, OT-adjacent, Windows-based) receive accelerated patching timelines

Compensating: Use free OSINT tooling to track 'The Gentlemen' infrastructure: monitor their leak site via Tor Browser manually on a weekly cadence using an isolated VM, and set up RSS monitoring via RansomWatch (open-source, GitHub) which aggregates ransomware group leak site posts. Subscribe to CISA's free TAXII feed and Abuse.ch ThreatFox for emerging IOCs. Create a shared threat register entry in a free tool such as MISP Community (self-hosted) or a structured markdown file in a private Git repo, with fields for last-updated date, confirmed TTPs (MITRE technique IDs), known infrastructure, and victim sector pattern.

Evidence: Before closing out this intelligence task, document the current baseline: (1) All publicly available 'The Gentlemen' victim posts from Q1 2026 leak site activity, with sector, geography, and claimed data volume — this establishes a targeting baseline for sector risk assessment; (2) Any infrastructure indicators (domains, IPs, file hashes) published in the GuidePoint Q1 2026 report or corroborating OSINT sources — these become detection signatures once verified; (3) The date of first observed 'The Gentlemen' activity in open sources, which establishes the dwell time baseline for any future forensic investigation if the actor is later found in your environment.

Step 6: Test backup and recovery posture — confirm that backups are offline or immutable, test restoration procedures, and document RTO/RPO against realistic ransomware scenarios including data-only extortion with no encryption event

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Validating recovery capability including the specific scenario where extortion-only ransomware produces no encryption event and traditional DR triggers may not fire

Controls: NIST CP-9 (System Backup) — verify that backup media is air-gapped or immutable (WORM storage, object lock enabled on S3/Azure Blob) and that ransomware groups cannot reach backup targets via the same compromised credentials used to access production systems, NIST CP-10 (System Recovery and Reconstitution) — conduct a full tabletop or live restoration test scoped specifically to the extortion-only scenario: no encrypted files, but confirmed data theft from file servers and SharePoint — what is the response, what is the legal trigger, and can operations continue?, NIST IR-4 (Incident Handling) — update incident handling procedures to include a decision branch for 'data theft confirmed, no encryption' that does not default to full system recovery but instead triggers legal/privacy counsel notification and evidence preservation, CIS 11.2 (Perform Automated Backups) — validate that backup jobs completed successfully for the past 30 days with no silent failures; ransomware groups frequently identify and delete or corrupt backup jobs weeks before launching extortion demands, CIS 11.4 (Establish and Maintain an Isolated Instance of Recovery Data) — confirm that at least one backup copy is logically and physically isolated from the primary domain — ransomware operators with Domain Admin access will target backup servers connected to the same AD forest

Compensating: For a 2-person team without enterprise backup infrastructure, use Veeam Community Edition (free, up to 10 workloads) with a detached USB or NAS target that is disconnected after each backup job via a scheduled task ('net use Z: /delete' post-backup script). Test restoration by actually restoring a critical file server to an isolated VM — do not assume backups work. For the extortion-only scenario, draft a one-page decision tree: if exfiltration is confirmed but no encryption occurred, what data was taken, does it trigger GDPR/HIPAA/state breach notification, and who is the legal contact?

Evidence: Before conducting recovery tests, capture: (1) Backup job logs for the past 90 days from your backup solution — look for any failed, skipped, or truncated jobs, which ransomware operators may have deliberately caused via T1490 (Inhibit System Recovery) weeks prior to extortion demand; (2) VSS snapshot inventory via 'vssadmin list shadows' on all file servers — ransomware groups routinely delete VSS copies as a precursor to extortion; (3) Active Directory delegation records showing which service accounts have write access to backup shares or NAS targets — these accounts are high-value targets for credential theft used to preemptively destroy recovery options.

Step 7: Monitor GuidePoint Security Q1 2026 report — obtain the primary report directly to validate the 150-200 weekly victim post figures and any published IOCs before using statistics in board-level risk reporting

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Validating threat intelligence source integrity before incorporating statistics into organizational risk posture and executive reporting

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives) — require that threat intelligence statistics used in executive or board reporting be sourced directly from the originating vendor publication, not secondary aggregators, to avoid misattribution or data drift, NIST IR-6 (Incident Reporting) — ensure that threat trend data incorporated into board risk reports accurately reflects the extortion-first tactical shift documented in GuidePoint's Q1 2026 findings, which changes the risk calculus from 'will we lose access to data' to 'is our data already exfiltrated', NIST PM-16 (Threat Awareness Program) — integrate verified GuidePoint Q1 2026 IOCs into the organization's threat awareness program and detection tooling only after direct source validation; unverified IOC ingestion from secondary sources introduces false positive risk and can degrade SIEM/EDR detection quality, CIS 7.2 (Establish and Maintain a Remediation Process) — use verified weekly victim post volume (150-200/week) as a quantitative input to risk-based remediation prioritization discussions with leadership, framing ransomware as an active and statistically probable threat rather than a theoretical one

Compensating: Retrieve the GuidePoint Q1 2026 report directly from GuidePoint Security's official website (guidepoint security.com/resources) — do not rely on news article summaries or third-party aggregator excerpts for statistics used in board reporting. For IOC validation before ingestion, use VirusTotal Community (free) and Abuse.ch ThreatFox to cross-reference any published file hashes, IPs, or domains against independent sources before adding to blocklists or detection rules. Maintain a source citation log (a simple spreadsheet) documenting report name, direct URL, retrieval date, and which statistics were used in which board presentations.

Evidence: No forensic evidence collection is required for this step as it is an intelligence validation and reporting hygiene action. However, document the retrieval metadata: (1) The direct URL from which the GuidePoint Q1 2026 report was obtained and the date retrieved — this establishes source provenance for any audit or regulatory inquiry about how the organization assessed the threat; (2) A record of which IOCs from the report were ingested into detection tools, which were rejected as unverifiable, and why — this demonstrates a defensible, reasoned intelligence program rather than uncritical IOC bulk ingestion.

Detection Guidance

Detection priority should shift toward exfiltration and staging behaviors rather than encryption events, given the tactical move toward data-theft-led extortion.

Log sources to prioritize:

- Cloud storage and SaaS egress logs: Look for anomalous upload volumes to services like Mega, OneDrive, Google Drive, or code repositories (T1567.002). Baseline normal upload behavior and alert on deviations exceeding defined thresholds.

- DNS and proxy logs: Identify connections to newly registered domains, domains with low reputation scores, or domains associated with known RaaS infrastructure. Short-lived domains used for staging and exfiltration are a common operational pattern.

- Authentication logs: Hunt for valid account usage at unusual hours, from unexpected geographies, or involving accounts not recently active. T1078 abuse often precedes exfiltration by days or weeks.

- EDR telemetry: Look for use of legitimate tools in exfiltration chains, archive utilities (7-Zip, WinRAR), file enumeration scripts, and cloud sync clients spawned from unexpected parent processes.

- OT/IT boundary traffic: For manufacturing and construction environments, monitor for lateral movement crossing the OT/IT boundary. Any IT-origin process communicating with OT assets warrants investigation.

Hunting hypotheses:

- Hypothesis 1: A valid account authenticates from a new IP range, then initiates large file transfers to an external cloud service within the same session.

- Hypothesis 2: An archive utility executes on a system that does not normally run compression tools, followed by outbound transfer.

- Hypothesis 3: Service disruption (T1489) attempts on OT-adjacent systems following authentication anomalies in corporate IT, indicating a pivot from IT toward operational systems.

IOC note: Specific indicators for 'The Gentlemen' are not available in the provided source material. Monitor GuidePoint Security publications and threat intelligence platforms (MISP communities, ISACs relevant to manufacturing) for emerging infrastructure and behavioral indicators as this group's operational profile develops.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`Pending — refer to GuidePoint Security Q1 2026 Ransomware Report for published indicators`	The GuidePoint Security Q1 2026 report is expected to contain behavioral indicators, infrastructure data, and potentially tooling associated with tracked groups including 'The Gentlemen'. Specific values were not available in the source material reviewed for this story.	LOW

Framework Mappings

MITRE-ATTACK

- **T1567.002** — Exfiltration to Cloud Storage
- **T1590** — Gather Victim Network Information
- **T1078** — Valid Accounts
- **T1489** — Service Stop
- **T1486** — Data Encrypted for Impact
- **T1657** — Financial Theft

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-6** — Configuration Settings
- **SI-4** — System Monitoring
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **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
T1567.002	Exfiltration to Cloud Storage	Exfiltration
T1590	Gather Victim Network Information	Reconnaissance
T1078	Valid Accounts	Defense-Evasion
T1489	Service Stop	Impact
T1486	Data Encrypted for Impact	Impact
T1657	Financial Theft	Impact

Sources

Source	URL	Tier
Top Industries Most Vulnerable to Cyberattacks in 2026	https://www.eccu.edu/blog/top-industries-most-vulnerable-to-cyber-a...	T1
Top Cybersecurity Threats in the Manufacturing Industry 2026	https://hoxhunt.com/blog/cyber-security-threats-in-manufacturing-in...	T3
How to face top 10 cyber threats to manufacturing industry	https://www.dataguard.com/blog/top-10-cyber-threats-to-manufacturin...	T3
Cybersecurity in the Manufacturing Industry - UpGuard	https://www.upguard.com/blog/cybersecurity-in-the-manufacturing-ind...	T3

Source	URL	Tier
Cybersecurity for Smart Factories in the Manufacturing Industry	https://www.deloitte.com/us/en/Industries/energy/articles/smart-fac...	T2

Generated 2026-04-18 06:51 UTC by TJS Security Command Center