CTI-The Gentlemen Ransomware

Erik Westhovens

May 2026

REPORT HEADER

Cyber Threat Intelligence Report

Subject: A Fast-Rising Ransomware Operation Built on Experienced Operators, Speed, and High-Impact Tradecraft

Audience: SOC, Incident Response, Threat Hunting, Vulnerability Management, Security Leadership

Date: May 2026

Author: Erik Westhovens

Management Summary

The Gentlemen is one of the most important emerging ransomware operations to watch in 2026 because it is behaving less like a new entrant and more like a mature criminal service already optimized for scale. Multiple sources indicate that the group surfaced in 2025 and accelerated sharply into 2026, rapidly climbing the victim rankings while maintaining a pace that is unusual for a supposedly young operation.

The strongest reason to take The Gentlemen seriously is not only its victim count but its operational profile. Available reporting indicates the group relies on experienced operators, likely including personnel or affiliates with prior ties to other ransomware ecosystems. Group-IB reported in March 2026 that the group was active since May 2025 and led by a former Qilin affiliate, while other reporting linked its rapid maturity to prior experimentation with established ransomware affiliate models. That background helps explain why the group already shows disciplined tradecraft, well-developed propagation methods, and strong understanding of how to dismantle enterprise defenses quickly.

The Gentlemen's strategy is built around speed, practical initial access, and high-pressure extortion. The group targets exposed internet-facing devices, moves quickly toward privileged access, disables or weakens security controls, laterally propagates through administrative mechanisms, steals data, and then applies ransomware at scale. The near-term risk to defenders is therefore not novelty for its own sake; it is the industrialization of capable operators who know how to turn weak perimeter exposure and identity gaps into rapid, organization-wide impact.

Key Takeaways

- The Gentlemen appears new, but its operational maturity strongly suggests experienced personnel or affiliates with earlier ransomware experience.
- The group is rising fast by combining aggressive growth incentives with proven tactics rather than depending on exotic tradecraft.
- Its most important strategic features are speed, flexible cross-platform ransomware capability, dual extortion, and fast movement from exposed edge devices to domain-wide impact.

Chapter 1

1. Why The Gentlemen Matters Now

The Gentlemen should be treated as a serious operational ransomware threat rather than as a fringe upstart.

The Gentlemen has moved rapidly from a newly observed ransomware name into one of the more active operations in the 2026 landscape. Check Point Research reported on April 20, 2026 that the group had claimed over 320 victims since mid-2025, with 240 of those attacks occurring in 2026 alone, making it the second most active ransomware group by victim count so far in 2026. S-RM similarly assessed on May 7, 2026 that the group had already claimed over 340 victims as of April 2026.

That pace matters because it changes how defenders should prioritize the group. Many ransomware brands appear suddenly and then fragment or disappear. The Gentlemen instead appears to be stabilizing and scaling. Cyble's March 2026 landscape reporting placed The Gentlemen among the top five most active ransomware actors globally for that month, reinforcing that this is not a one-region anomaly or a short-lived spike.

The group is especially concerning because its public growth profile does not match the normal learning curve of a truly inexperienced operation. The reporting points instead to a team or affiliate base that already understands access, privilege escalation, lateral movement, anti-forensics, and mass-impact deployment.

Assessment

- The threat is current, fast-growing, and already materially active in 2026.
- Victim-count growth is only one signal; the more important issue is how quickly the group reached operational maturity.
- Organizations should assume the group can move from foothold to enterprise-wide impact faster than many standard ransomware playbooks.

Chapter 2

2. Origins, Membership, and Why They Look Experienced

The group's background strongly suggests prior ransomware experience rather than organic growth from a novice team.

Open reporting does not support the view that The Gentlemen is simply a random new crew experimenting in public. Group-IB reported in March 2026 that the group was active since May 2025, had approximately 15 members, and was led by a former Qilin affiliate. That alone is significant because Qilin is an established ransomware ecosystem, and leadership with that background would help explain the group's fast operational maturity.

Cybereason reported in November 2025 that before creating their own ransomware-as-a-service platform, The Gentlemen operators had experimented with affiliate models used by other prominent ransomware groups. Cybereason also linked underground activity around the alias 'hastalamuerte' to early operational development and exploration of other ransomware software options before the group refined its own service model.

Taken together, these signals make the most defensible assessment that The Gentlemen likely emerged from experienced ransomware circles rather than from inexperienced criminals learning in real time. That matters because it means the group should be expected to improve quickly, recruit effectively, and reuse proven ideas from predecessor ecosystems instead of slowly discovering them through trial and error.

Why This Matters

- Leadership or affiliate overlap with earlier ransomware ecosystems is a central risk factor.
- Former-Qilin linkage matters because it suggests operational know-how rather than just branding speed.
- The group's maturity is best explained by experienced actors repackaging proven ransomware business and intrusion methods.

Chapter 3

3. Business Model and Growth Strategy

The Gentlemen appears to be scaling through an attractive affiliate model, practical tooling, and low-friction operator support.

The Gentlemen operates as a ransomware-as-a-service operation, but available reporting suggests it is not limited to a traditional polished affiliate panel model. Group-IB noted that the group distributes tools directly via Tox messenger without a conventional affiliate panel. S-RM also described a straightforward revenue-sharing model in which operators retain 10 percent and affiliates keep the remainder.

Check Point Research reported on April 20, 2026 that a 90/10 affiliate revenue split, compared with the more common 80/20 structure, is accelerating the group's growth by attracting experienced operators from competing programs. That point is strategically important because it helps explain both the group's rising victim volume and the quality of its tradecraft. A generous split attracts capable affiliates who bring their own access, experience, and victim pipelines.

The group also appears to market itself as operationally useful rather than merely loud. Reporting highlights features such as self-deletion, log wiping, concurrent execution, EDR bypass tooling, and custom utilities for lateral movement. In other words, The Gentlemen is not only selling encryption. It is selling a practical attack stack that helps affiliates move quickly from intrusion to pressure.

Strategic Features

- A favorable affiliate split can recruit experienced operators faster than brand reputation alone.
- The group appears to compete on usability, support, and operator effectiveness rather than only on locker availability.
- Tool distribution and operator support lower the barrier for affiliates to scale proven playbooks.

Chapter 4

4. Initial Access and Targeting Strategy

The Gentlemen's initial access strategy is practical, repeatable, and dangerous because it depends on common enterprise weaknesses.

Check Point Research assessed that The Gentlemen deliberately targets internet-facing devices, especially VPNs and firewalls, as entry points. Once inside, the group is reported to move quickly to broader network control and enterprise-wide encryption. Check Point further emphasized that the operation does not depend on exotic zero-days as its core access model; instead, it benefits from unpatched or misconfigured perimeter systems and weak post-compromise controls.

This is strategically important because it means many organizations are already exposed if they have weak patching discipline around edge infrastructure, insufficient MFA, or poor administrative segmentation. A ransomware operation does not need novel initial access if it has reliable access to vulnerable internet-facing devices and knows how to exploit the resulting identity and network trust relationships efficiently.

Victimology reporting suggests The Gentlemen has a notable concentration in Asia while remaining globally active. S-RM reported that Asia accounted for nearly 46 percent of observed cases, while the United States and Thailand recorded the highest number of individual victims. Manufacturing, technology, healthcare, professional services, and other continuity-sensitive sectors appear repeatedly in reporting, indicating the group values both operational pressure and data value.

Initial Access Assessment

- Edge-device exposure remains the key upstream enabler for this operation.
- The group benefits from organizations that still treat firewalls, VPNs, and remote access portals as second-tier patching priorities.
- Sector selection suggests a mix of opportunism and targeting toward organizations where downtime and disclosure both create strong leverage.

Chapter 5

5. Intrusion Strategy, Methods, and Tradecraft

The Gentlemen's methods reflect a mature post-compromise playbook centered on speed, control, and blast radius.

Cybereason's analysis of The Gentlemen's Windows locker and associated commands shows a ransomware operation designed for flexible deployment rather than one-size-fits-all execution. The group supports multiple encryption speeds, local and network encryption modes, silent execution, SYSTEM-level operation, mapped-share targeting, and PowerShell- and WMI-based propagation. It also uses anti-forensics measures such as log deletion, Defender exclusion changes, and self-deletion after execution.

Cybereason further documented execution behavior that included remote PowerShell commands to disable Microsoft Defender real-time monitoring, add exclusion paths, enable network discovery rules, enumerate cluster and local volumes, modify permissions with ICACLS, and remotely create processes through WMI. The built-in kill list for services and processes includes databases, backup tooling, virtualization components, and remote access utilities, reflecting a deliberate attempt to maximize encryption success and reduce recovery options.

Check Point's DFIR reporting adds an operational perspective: the group can move from established administrative access to domain-wide ransomware deployment through Group Policy within hours. That speed is one of the most important characteristics to emphasize. The Gentlemen's operators are not improvising at the end of the intrusion; they appear to be executing a rehearsed process designed to hit large parts of an environment before defenders can meaningfully react.

Methods and TTPs

- The group combines practical admin abuse, defense impairment, discovery, and broad propagation rather than relying on one standout trick.
- Its methods are dangerous because they are repeatable across many Windows-heavy enterprise environments.
- The combination of anti-forensics, security-tool impairment, and fast distributed execution increases both damage and investigation difficulty.

Chapter 6

6. Ransomware Capability and Platform Coverage

The Gentlemen is more dangerous because it offers flexible ransomware capability across multiple enterprise platforms.

Cybereason reported that The Gentlemen markets Windows, Linux, and ESXi locker capability, with configurable encryption depth and performance. The Windows locker uses XChaCha20 and Curve25519, supports fast and ultrafast modes, and can operate across local disks, mapped shares, and UNC paths. Group-IB further reported in March 2026 that the group was reportedly developing Linux and ESXi variants with AI assistance.

Cross-platform capability matters because it increases the likelihood of high operational impact in mixed enterprise environments. Windows endpoints, Linux systems, and virtualization infrastructure each present different recovery challenges. A ransomware group that can cover all three is better positioned to prevent clean fallback paths and to disrupt both business systems and supporting infrastructure.

This also reinforces that The Gentlemen is not a shallow single-binary threat. It is better understood as a service ecosystem that keeps improving locker functionality, propagation options, and persistence features in response to defender behavior.

Capability Assessment

- Cross-platform encryption increases business impact and complicates recovery sequencing.
- Flexible encryption speed options help affiliates balance stealth, time, and impact.
- Locker evolution suggests the group is actively investing in operational refinement.

Chapter 7

7. Victim Impact and Strategic Risk

The Gentlemen is strategically dangerous because it combines scale, speed, and operator experience in sectors where disruption hurts quickly.

Check Point's April 2026 reporting indicates the group may be larger than public leak-site counts suggest. During one incident response engagement, researchers observed a command-and-control server linked to a Gentlemen affiliate and identified a botnet of more than 1,570 likely corporate victims. That observation implies the public victim list is only part of the operational picture and that the group may have substantially more latent access than public disclosures reveal.

The strategic business risk is therefore not only the incident that has already detonated. It is the possibility that footholds are staged across multiple organizations awaiting later monetization. For defenders, that means leak-site counting alone underestimates exposure. The more important question is whether the organization would be easy for a capable affiliate to move through once initial access is obtained.

The group also appears willing to hit continuity-sensitive sectors such as manufacturing, technology, and healthcare. Check Point explicitly noted that healthcare is becoming a stronger target and that the group does not seem to observe the informal limits that some ransomware operators claim to apply to critical services. That increases the real-world risk of operational disruption, safety impact, regulatory scrutiny, and outsized executive pressure during incidents.

Risk Implications

- Public victim counts likely understate the scale of actual access and staging.
- Manufacturing, technology, and healthcare exposure should be treated as strategically important.
- The operation's willingness to pressure sensitive sectors raises both business and societal risk.

Chapter 8

8. Recommendations for Defenders

Defending against The Gentlemen is primarily a matter of disciplined hardening, identity control, and detection of post-compromise movement before encryption.

The first priority is hardening internet-facing infrastructure. VPNs, firewall management portals, and remote access gateways should be treated as top-tier exposure reduction priorities, with accelerated patching, access restriction, strong MFA, and external exposure review. Check Point's reporting is especially clear that these systems are the primary entry point for this operation.

The second priority is limiting what the group can do after entry. Domain admin pathways, unrestricted PowerShell remoting, over-permissive WMI usage, broad SMB reachability, and weak backup isolation all increase the blast radius of a successful intrusion. Monitoring should focus on credential validation, lateral movement, GPO abuse, mass service stoppage, security-tool impairment, and unusual WMI- or PowerShell-based remote execution.

The third priority is response readiness. Because The Gentlemen moves quickly, isolated backups, tested restoration processes, and well-rehearsed containment authority matter more than generic policy language. Organizations should also assume that data theft is part of the operating model, meaning legal, communications, and extortion decision processes need to be prepared before an incident begins.

Recommended Actions

- Prioritize patching and restricting internet-facing firewalls, VPNs, and remote access systems.
- Reduce post-compromise blast radius through identity controls, segmentation, and admin-channel hardening.
- Detect and respond to lateral movement and security-control impairment before ransomware deployment begins.

Chapter 9

9. Sources

Primary and high-value public sources used in this report.

1. Cybereason. License to Encrypt: The Gentlemen Make Their Move. November 18, 2025. https://www.cybereason.com/blog/the-gentlemen-ransomware

2. Check Point Research. The Gentlemen: A New Ransomware Threat Climbing the Charts Fast. April 20, 2026. https://blog.checkpoint.com/research/the-gentlemen-a-new-ransomware-threat-climbing-the-charts-fast/

3. Check Point Research. DFIR Report – The Gentlemen & SystemBC: A Sneak Peek Behind the Proxy. April 20, 2026. https://research.checkpoint.com/2026/dfir-report-the-gentlemen/

4. Group-IB. APAC Intelligence Insights Report, March 2026. https://www.group-ib.com/resources/research-hub/apac-intelligence-insights-report-march-2026/

5. Group-IB. APAC Intelligence Insights Report, February 2026. https://www.group-ib.com/resources/research-hub/apac-intelligence-insights-report-february-2026/

6. S-RM. Ransomware in focus: The Gentlemen. May 7, 2026. https://www.s-rminform.com/latest-thinking/ransomware-in-focus-meet-the-gentleman

7. Cyble. Threat Landscape March 2026: Ransomware Dominance, Access Brokers, Data Leaks, and Critical Exploitation Trends. April 20, 2026. https://cyble.com/blog/monthly-threat-landscape-march-2026/