halcyon | Ransomware Research Center

# The Gentlemen Ransomware Group is Scaling Faster Than Any Other Group on Record

## Summary

Halcyon is tracking a rapidly escalating splinter group from the prolific Qilin Ransomware-as-a-Service (RaaS) operation: The Gentlemen. Since it surfaced in mid-2025, the gang has claimed nearly 300 organizations across more than 66 countries and 20 industry verticals, becoming one of the fastest-scaling ransomware threats that we have tracked.

The Gentlemen appears to have formed following a payment dispute with Qilin ransomware. Halcyon estimates the core team to be roughly 20 members, many with prior experience in established ransomware ecosystems. The group demonstrated operational maturity from the beginning, with much of its growth driven by its generous offer to pay affiliates 90% of ransom proceeds combined with a multi-OS codebase under continuous development.

More than 200 of The Gentlemen's victim claims occurred between January and March 2026, making its volume second only to Qilin and ahead of established actors like ClOp, RansomHub, and LockBit. During the group's first five months, it listed the same number of victims that it took Akira twelve and Qilin eighteen months to reach.

The Gentlemen should be treated as a critical-priority threat to enterprise environments globally. Organizations running Fortinet edge devices, those heavily reliant on Active Directory, and entities in manufacturing, technology, and healthcare face the most elevated risk.

## Background

The Gentlemen previously operated as ArmCorp, a prolific affiliate of the Qilin ransomware program. The split between ArmCorp and Qilin was triggered by a payment dispute on 22 July 2025, when threat actor "hastalamuerte" filed a public complaint on the RAMP underground forum, alleging Qilin's operators owed roughly $48,000 in unpaid commission. A few days prior on 17 July 2025, the first The Gentlemen ransomware sample appeared on VirusTotal with the binary already embedding the URL for The Gentlemen's dedicated leak site, suggesting the separation was already underway before the dispute went public. By September 2025, the RaaS was being openly marketed on criminal forums, and victim data had started appearing on the leak site.

The Gentlemen operate a fully featured RaaS platform that equips affiliates with a complete attack toolkit. The 90% revenue share for affiliates is also among the highest in the current underground market, designed to draw experienced operators away from competitors. Most RaaS programs offer affiliates between 70% and 80% of ransom proceeds, with only RansomHub previously matching The Gentlemen's 90/10 split. The strategy appears to be working. Most infections observed in 2026 were carried out by affiliates rather than the core team, a clear sign the program has achieved meaningful scale.

Ransom negotiations happen over individual affiliate Tox IDs rather than through the central leak portal, keeping a buffer between the platform and its operators. This also serves as an advantage for affiliates as it prevents the operators from locking them out of ongoing negotiations. The group operates an X/Twitter account, in addition to their data leak site, where they publicly name victims, a pressure tactic aimed at driving payment through reputational damage.

Further demonstrating their operational depth, The Gentlemen's developers are systematically reverse-engineering samples from Babuk, Qilin, LockBit 5.0, and Medusa, cherry-picking the strongest encryption routines, code-obfuscation techniques, and EDR evasion methods to incorporate into their own codebase. The result is a deliberate composite engineering effort rather than a simple fork of any single predecessor.

## Initial Access

The Gentlemen's primary entry vector exploits CVE-2024-55591, a critical authentication bypass in FortiOS/FortiProxy that allows an unauthenticated attacker to bypass login controls. Once inside, attackers can escalate privileges, create administrator accounts, and establish persistent access to the network.

Researchers recently revealed that the operators maintain an inventory of approximately 14,700 FortiGate devices worldwide that they have already compromised, supplemented by nearly a thousand brute-forced FortiGate VPN credentials. This pre-positioned access stockpile is exceptionally large for a single ransomware operation and gives them the ability to conduct sustained attacks without needing to establish new footholds each time.

Beyond Fortinet exploitation, affiliates also gain entry through internet-facing RDP, SSL VPN endpoints, and remote management tools. Once inside, they rely on legitimate administrative utilities such as AnyDesk and PsExec for lateral movement, allowing malicious activity to blend into normal network operations.

The group's initial access strategy is not static. Internal communications leaked in May 2026 revealed that The Gentlemen are actively tracking and evaluating newer vulnerabilities, including CVE-2025-32433 and CVE-2025-33073, alongside continued exploitation of Cisco edge appliances, NTLM relay attacks, and harvested OWA/M365 credential logs. This signals a deliberate effort to diversify entry points beyond Fortinet infrastructure.

## Data Encryption

The Gentlemen ransomware is written in Go and targets Windows, Linux, NAS, and CSD environments, with a dedicated C-based locker for ESXi. A unique ephemeral key is generated per file to prevent bulk decryption if a single key is recovered. Files 1 MB or smaller are fully encrypted, while larger files undergo intermittent encryption targeting segments, a method that balances speed against impact. Execution requires a mandatory build-specific password argument, limiting automated analysis and adding a layer of access control for operators.

The command-line interface offers significant operational flexibility including the percentage of each file that is encrypted, speed modes ranging from default to ultrafast that target progressively smaller file portions, and path arguments to optimize targeting. By default, the Windows variant recursively traverses all local drive letters from A:\ through Z:\, while the Linux variant walks the filesystem from the specified root. An additional wipe flag on the Linux variant overwrites free disk space to obstruct recovery efforts.

Before encryption begins, The Gentlemen systematically prepares the target environments.

- **Windows:** Terminates processes and services associated with databases, backup solutions, virtualization platforms, and productivity applications; deletes shadow copies and the Recycle Bin contents; disables Windows Defender real-time protection while adding exclusions for its own binary.
- **Linux:** Removes trash and recycle bin contents; destroys filesystem snapshots including those used by NAS and virtualized environments; eliminates VMware virtual machine snapshots; Terminates virtualization and database services to maximize the number of accessible files
- **ESXi:** Shuts down virtual machines through a two-step process combining graceful shutdown attempts with forced termination, degrades caching, flushes disk buffers, and disables VM auto-recovery mechanisms.

The different variants perform anti-forensic actions to hinder investigation, including clearing logs, wiping command history, and removing other system artifacts. The Linux variant also establishes persistence so it can survive a reboot. On ESXi systems, the ransom note is displayed at login. All encrypted files are appended with a unique six-character extension and a README-GENTLEMEN.txt ransom note is dropped across affected directories.

## Victimology

The Gentlemen often target organizations where centralized identity systems and constant operational demands provide maximum leverage in ransom negotiations. Consistent among Russian-speaking cybercriminal groups, the operators have also enforced a strict ban on targeting Russia and the Commonwealth of Independent States.

Thailand is the most targeted country with 27 victims, followed by the United States, France, and Brazil. Only 7% of victims are US-based, a significant deviation from the broader ransomware ecosystem where roughly half of all victims are American organizations. This geographic outlier may suggest the affiliate base draws heavily from Southeast Asian and Latin American operators.

Victims span 66 countries across every continent, ranging from small and mid-market firms to sizeable entities in government, energy, and critical infrastructure. The top targeted sectors are IT services, construction, manufacturing, financial services, and healthcare.

## Key Vulnerability Factors

Several overlapping factors increase an organization's exposure:

- **Active Directory exploitation:** The group's most devastating deployment tactic hijacks AD Group Policy to detonate ransomware on every domain-joined host simultaneously. Flat AD designs with weak tier separation are especially exposed.
- **Virtualization targeting:** A purpose-built ESXi locker written in C targets hypervisors that may host dozens of critical workloads on a single machine.
- **Remote access abuse:** Internet-facing RDP, SSL VPN, and remote management tools form the primary entry points that affiliates exploit. Because the group relies on legitimate admin utilities like AnyDesk and PsExec, malicious traffic blends into normal operations.
- **Supply chain exposure:** Smaller vendors and suppliers that hold privileged network connections to larger partners but lack the budget for advanced defenses create additional cascading risk across interconnected business relationships.

## Comparative Landscape

The Gentlemen have scaled faster than nearly any modern ransomware operation on record. The group was responsible for 48 attacks in January 2026 and 91 in February 2026, nearly doubling month over month. The Gentlemen's growth trajectory is comparable to the early rise of LockBit 3.0, widely considered the highest benchmark for RaaS scaling.

The Gentlemen should not be evaluated as a standalone operation. Affiliates are tapping into a wider attack ecosystem, mixing initial access tools, post exploitation frameworks, and encryption payloads from multiple providers. The ongoing practice of borrowing from rival ransomware codebases reinforces the picture of an operation built to remain a persistent threat.

## Internal Leaks

On May 4, 2026, The Gentlemen's administrator publicly acknowledged on underground forums that an internal backend database had been compromised and leaked. The following day, an account began advertising the stolen data for $10,000 in Bitcoin, posting partial proof files that included server account credentials and password hashes. The leak was later fully published and exposed nine internal accounts, including zeta88, the handle tied to hastalamuerte and the core administrator of the RaaS program.

Leaked material offers a window into the group's daily operations with compromised VPN and Synology accounts constantly being shared and operators later coming in and picking them up for further exploitation. The internal channels also reveal how affiliates and operators shared tooling and techniques for disabling endpoint security, set up C2 infrastructure, coordinated intrusions in progress, and tracked payouts across campaigns clearly demonstrating a highly efficient operation.

The leaked chats also exposed negotiation details, including one case where The Gentlemen successfully collected $190,000 after opening with a $250,000 demand. In another case, the group reused data stolen from a UK software consultancy during negotiations with a separate Turkish victim, portraying the UK firm as the source of the breach and encouraging the Turkish company to pursue legal action against them.

In response to the leak, the administrator announced a full overhaul of the group's communication infrastructure, deployment of new storage systems, and several technical upgrades to the locker. The response suggests a group intent on hardening its operations and continuing to scale.

## Mitigations

- **Deploy Dedicated Anti-Ransomware Solution:** Deploy dedicated anti-ransomware defenses capable of detecting and stopping threats before encryption begins. Effective solutions should identify the behavioral patterns that precede a ransomware deployment including network scanning, credential harvesting, lateral movement via PsExec, AnyDesk, and PowerShell Remoting, and privilege escalation through tools like PowerRun. Solutions should also detect late-stage indicators such as GPO modification for domain-wide ransomware deployment, kernel-mode EDR/AV killing, and Volume Shadow Copy deletion [M1038] [M1040].
- **Perimeter and Edge Device Hardening:** Immediately patch CVE-2024-55591 on all FortiOS/FortiProxy appliances. The Gentlemen maintain a stockpile of approximately 14,700 already-compromised FortiGate devices, so any appliance left unpatched during the vulnerability window should be treated as potentially breached. Audit for indicators of prior exploitation and extend hardening to Cisco edge appliances and internet-facing RDP

endpoints, both of which appear in the group's leaked internal playbooks. Also monitor for CVE-2025-32433 and CVE-2025-33073, which the group is actively evaluating. Refer to CISA's Known Exploited Vulnerabilities (KEV) Catalog for prioritization.

- **Harden Active Directory and Group Policy:** Implement an AD tiering model, restrict write access to NETLOGON and SYSVOL shares, monitor for unauthorized GPO modifications and scheduled task creation, and alert on new domain admin account creation. Flat AD designs with weak tier separation are especially exposed to this group [M1026] [M1018].
- **Credential Hygiene and Identity Controls:** Deploy phishing-resistant multi-factor authentication (MFA) across all systems, with particular emphasis on FortiGate VPN, remote access, and privileged accounts [M1032]. The Gentlemen's leaked communications reveal active use of harvested OWA/M365 credential logs and brute-forced VPN credentials, so audit all third-party access and rotate any legacy or potentially exposed credentials immediately [M1018].
- **Backup Resilience and Recovery Testing:** Maintain immutable, offline backups isolated from domain-joined systems, and test restoration procedures regularly [M1053]. The Gentlemen specifically target NAS systems, Exchange servers, storage arrays, and backup infrastructure before encryption to prevent recovery. Knowing a backup exists is not the same as knowing it works.
- **Supply Chain Risk Governance:** The Gentlemen have demonstrated a willingness to pivot from one compromised organization to its clients, using stolen credentials and infrastructure documentation as a bridge. Establish baseline security requirements for critical vendors, software providers, and third-party service partners [M1013]. Actively monitor for breaches in third-party tools and platforms in use across organization [M1047].

## References


- *Group-IB - Hasta la vista, Hastalamuerte: An Overview of The Gentlemen's TTPs (April 2026)*
- *Check Point Research - DFIR Report: The Gentlemen & SystemBC (May 2026)*
- *Cybereason - License to Encrypt: The Gentlemen Make Their Move (2026)*
- *SOCRadar - Dark Web Profile: The Gentlemen Ransomware (February 2026)*
- *Fortinet FortiGuard - The Gentlemen Ransomware Threat Actor Profile (March 2026)*
- *Blackpoint Cyber - The Gentlemen Ransomware Threat Profile (November 2025)*
- *KPMG - CTIP: Gentlemen Ransomware (November 2025)*
- *Dark Reading - The Gentlemen Rapidly Rises to Ransomware Prominence (April 2026)*

- *Ransomware.live - The Gentlemen Group Tracking Data*
- *Thus Spoke...The Gentlemen - Check Point Research*

## Source Summary

This Alert is based on Halcyon observations, open-source information, and ongoing research. Findings reflect our current understanding of threat actor activity and may be updated as new evidence emerges. Assessments may be revised as additional evidence becomes available.

*The Halcyon Ransomware Research Center unites experts, drives smart policies, and delivers actionable intelligence to detect, disrupt, and defeat ransomware. Explore the Center's latest reports, analysis, and resources here.*