Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

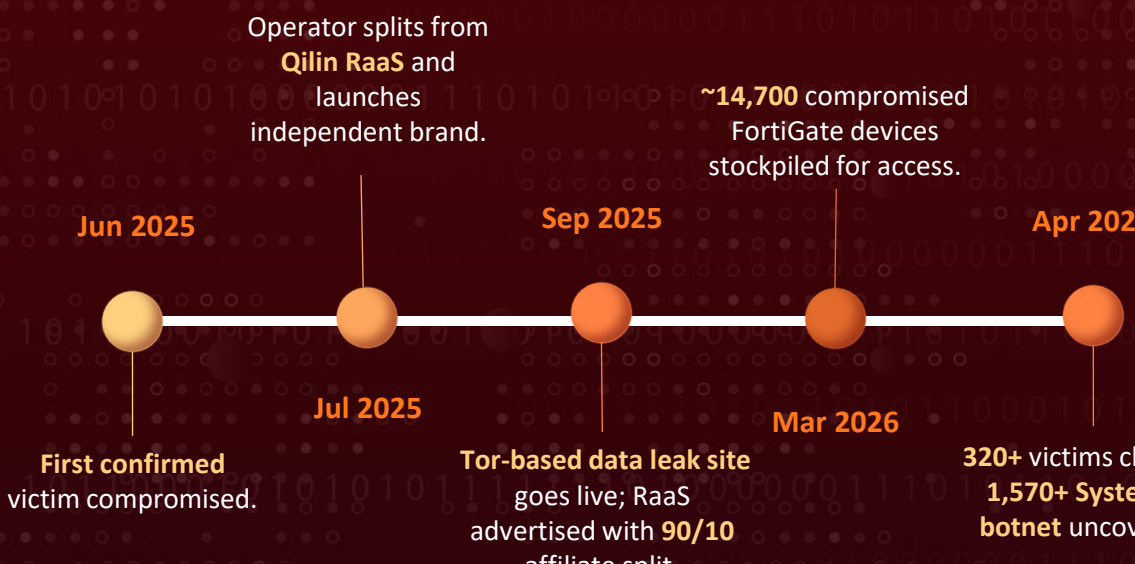
The Gentlemen Ransomware: A Rapidly Scaling RaaS Threat

Date of Publication	Admiralty Code	TA Number
April 24, 2026	A1	TA2026114

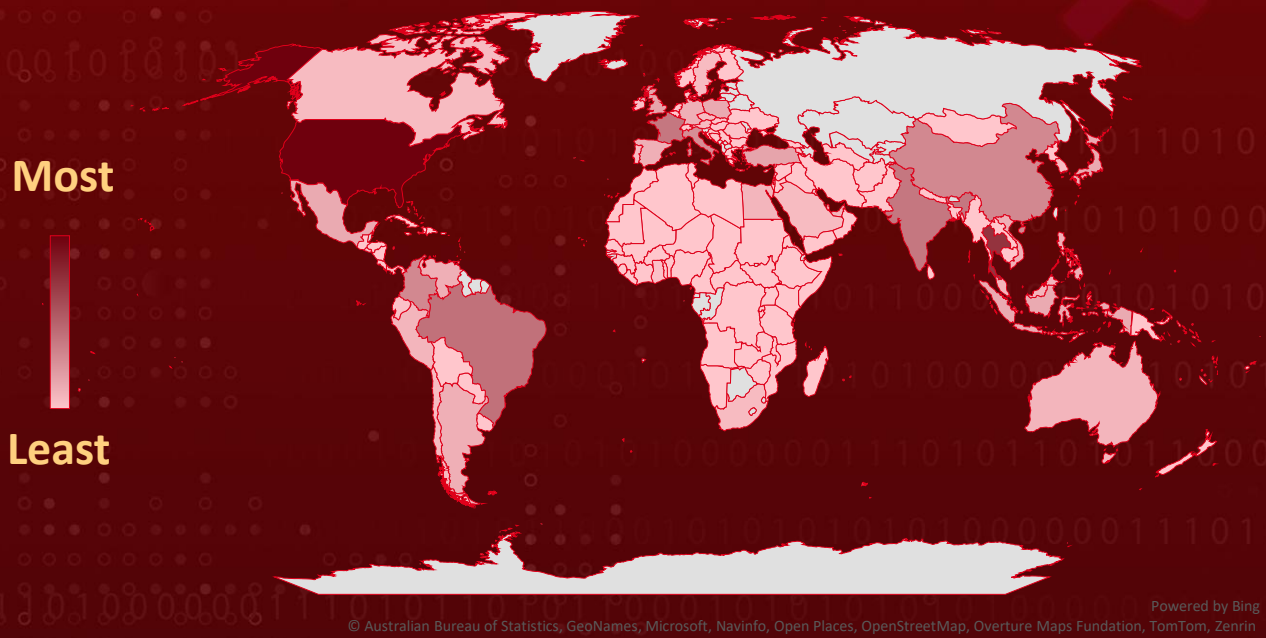
Summary

First Active: June 2025
Targeted Regions: Global (Except CIS countries)
Targeted Platforms: Windows, Linux, NAS, BSD, and VMware ESXi
Targeted Industries: Manufacturing, Technology, Healthcare, Retail, Business Services & Consulting, Transportation, Financial Services, Education, Government, Real Estate, Agriculture, Energy, Insurance, Pharmaceutical, Food Service, Media, Hospitality, Charitable Organizations, Telecommunications, Legal
Malware: The Gentlemen Ransomware, SystemBC
Attack: The Gentlemen is a Ransomware-as-a-Service (RaaS) operation that emerged in mid-2025 and has scaled rapidly, with affiliates publicly claiming more than 320 victims, the majority (approximately 240) concentrated in the first months of 2026. The group supplies affiliates with a multi-OS Go-based locker for Windows, Linux, NAS, and BSD, plus a dedicated C-based locker for ESXi, enabling coordinated attacks across heterogeneous enterprise estates. Affiliates have been observed combining the ransomware with SystemBC proxy malware and Cobalt Strike, establishing covert SOCKS5 tunnels, credential harvesting with Mimikatz, and domain-wide deployment through Group Policy, culminating in near-simultaneous encryption across victim environments and classic double-extortion pressure via a dedicated Tor leak site and a public X/Twitter account.

Ransomware Timeline



Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-55591	Fortinet FortiOS Authorization Bypass Vulnerability	Fortinet FortiOS	✓	✓	✓
CVE-2023-27532	Veeam Backup & Replication Cloud Connect Missing Authentication for Critical Function Vulnerability	Veeam Backup & Replication Cloud Connect	✗	✓	✓
CVE-2024-37085	VMware ESXi Authentication Bypass Vulnerability	VMware ESXi	✗	✓	✓
CVE-2025-7771	TechPowerUp ThrottleStop Privilege Escalation Vulnerability	TechPowerUp ThrottleStop	✓	✗	✗

Attack Details

#1

The Gentlemen is a Ransomware-as-a-Service (RaaS) operation that publicly surfaced in September 2025, though malware samples and forensic evidence trace development activity back to at least mid-July 2025, with its earliest confirmed victim, a Peruvian steel manufacturer, compromised as early as June 30, 2025. The operation is run by a Russian-speaking threat actor using the alias "hastalamuerte" (also tracked as LARVA-368), who previously led an affiliate crew called ArmCorp inside the Qilin RaaS program. After a public payment dispute with Qilin on the RAMP underground forum in July 2025, hastalamuerte formalized an already-planned departure and launched The Gentlemen as an independent brand, reusing proven tooling and infrastructure.

#2

The RaaS was formally advertised on underground forums on September 12, 2025 under the alias "Zeta88," promoting a minimal-infrastructure model (leak site plus Tox) and a cross-platform locker initially covering Windows and Linux, with NAS, BSD, and ESXi support added in later iterations. Consisting of roughly 20 members, the group offers affiliates an aggressive 90/10 revenue split, well above the industry norm of 80/20, along with full control over victim negotiations, which has fueled rapid recruitment of seasoned operators from competing programs.

#3

The group has scaled dramatically in under a year, growing from approximately 30 claimed victims across 17 countries in autumn 2025 to 48 by October 2025, roughly 130 by early February 2026, and over 320 publicly listed victims by April 2026, with 240 of those claimed in the first months of 2026 alone. Independent telemetry from a command-and-control server tied to an affiliate revealed a botnet of more than 1,570 likely corporate victims, indicating the true scale exceeds the leak-site count. Manufacturing, technology, healthcare, and financial services are the most impacted sectors, and the group shows no self-imposed restraint regarding hospitals or critical services. The heaviest geographic concentrations are the United States, Thailand, United Kingdom, Germany, Brazil, and France. Consistent with Russian-speaking ransomware norms, affiliate rules explicitly prohibit targeting organizations in Russia and other CIS states.

#4

Initial access is predominantly achieved through exploitation of internet-facing edge devices, most notably FortiGate appliances via CVE-2024-55591, an authentication bypass in FortiOS/FortiProxy. Operators maintain a curated database of roughly 14,700 already-compromised FortiGate devices and 969 validated brute-forced VPN credentials, enabling affiliates to skip the reconnaissance phase entirely. Infostealer-sourced credentials and exposed administrative panels serve as secondary vectors. Once inside, affiliates conduct structured reconnaissance using Advanced IP Scanner, Nmap, and Active Directory enumeration scripts, then pivot to defense evasion through a Bring-Your-Own-Vulnerable-Driver (BYOVD) technique abusing the ThrottleStop.sys driver (renamed ThrottleBlood.sys) to exploit CVE-2025-7771, granting kernel-level code execution.

#5

Custom utilities such as All.exe and Allpatch2.exe are deployed to terminate EDR and antivirus processes at the kernel, supplemented by PowerShell commands that disable Windows Defender, add broad path and process exclusions, and purge Defender support files. Lateral movement relies on living-off-the-land utilities including PsExec, WMI, WinRM, PowerRun.exe for UAC bypass and SYSTEM escalation, and remote scheduled tasks or services created across reachable hosts. Credentials are harvested from memory using Mimikatz, and AnyDesk is typically installed with a hardcoded password as a fallback remote access channel.

#6

Command-and-control is established through Cobalt Strike beacons and SystemBC SOCKS5 proxies using an RC4-encrypted protocol, while data exfiltration is performed over encrypted channels via WinSCP. The defining impact technique is the ransomware's built-in Group Policy deployment mode, which, once a Domain Controller is compromised, copies the locker to the NETLOGON share, creates a malicious GPO with an immediate scheduled task, and forces policy refresh to trigger near-simultaneous encryption across every domain-joined system.

#7

The Go-based locker targets Windows, Linux, NAS, and BSD environments, with a companion C-based variant for ESXi hypervisors. It requires a per-build password argument to prevent sandbox detonation and uses hybrid cryptography combining X25519 key exchange with XChaCha20 stream encryption, generating a unique ephemeral key per file. Configurable speed modes encrypt only 1 to 9 percent of large files for throughput while retaining destructive impact, and operators can optionally wipe free disk space to defeat forensic recovery. Before encryption, the malware terminates dozens of backup, database, virtualization, and security services, deletes shadow copies, clears Windows event logs, and removes prefetch and RDP artifacts.

#8

Following a double-extortion model, stolen data, often ranging from hundreds of gigabytes to multiple terabytes per victim, is staged before encryption and published on a Tor-based leak site if ransom demands go unmet, with negotiations conducted through Tox and Session messengers and additional public pressure applied via a branded social media account.

Recommendations

Patch Internet-Facing Services: Prioritize timely patching of any exposed VPN appliances, RDP gateways, and remote-access infrastructure, since affiliates of The Gentlemen rely heavily on opportunistic exploitation of exposed services and stolen credentials for initial access.

Harden and Monitor Domain Controllers: Treat Domain Controllers as the crown jewel of the ransomware kill chain. Restrict interactive and network logons, monitor for unusual ADMIN$ writes, abnormal RPC-launched binaries, and PowerShell sessions spawned under scheduled-task contexts on DCs.

Block and Detect Group Policy Weaponization: Alert on the creation of new GPOs, changes to NETLOGON or SYSVOL scheduled-task XML files, and bulk Invoke-GPUpdate or gpupdate /force activity. The --gpo path is the single most impactful deployment mechanism in this ransomware and must be detectable in near real time.

Hunt for SystemBC Proxy Activity: Instrument EDR and NetFlow for unexpected SOCKS5 traffic, particularly from corporate hosts that should never act as proxies. Outbound connections to 45[.]86[.]230[.]112 or anomalous encrypted tunnels from workstations to low-reputation hosts should be investigated as potential pre-ransomware staging.

Conduct Regular Data Backups and Test Restoration: Regularly backup critical data and systems, store them securely offline. Test restoration processes to ensure backup integrity and availability. In case of a The gentlemen ransomware attack, up-to-date backups enable recovery without paying the ransom.

Protect Windows Defender Tamper Controls: Enable Tamper Protection, restrict who can run Set-MpPreference, and alert on any execution of Set-MpPreference -DisableRealtimeMonitoring, Add-MpPreference -ExclusionPath 'C:\', or Add-MpPreference -ExclusionProcess , all are explicit behaviors of the Gentlemen locker.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1078: Valid Accounts	
	T1133: External Remote Services	
Execution	T1059: Command and Scripting Interpreter	T1059.003: Windows Command Shell
		T1059.001: PowerShell
	T1047: Windows Management Instrumentation	
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1569: System Services	T1569.002: Service Execution
	T1106: Native API	
	T1204: User Execution	T1204.002: Malicious File
Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
		T1053.003: Cron
	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
		T1037.004: RC Scripts
	T1543: Create or Modify System Process	T1543.003: Windows Service

Tactic	Technique	Sub-technique
Privilege Escalation	T1078: Valid Accounts	
Defense Evasion	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.004: Disable or Modify System Firewall
	T1070: Indicator Removal	T1070.001: Clear Windows Event Logs
		T1070.004: File Deletion
	T1036: Masquerading	T1036.004: Masquerade Task or Service
		T1036.005: Match Legitimate Name or Location
	T1564: Hide Artifacts	T1564.001: Hidden Files and Directories
	T1027: Obfuscated Files or Information	
Credential Access	T1003: OS Credential Dumping	
	T1555: Credentials from Password Stores	
Discovery	T1082: System Information Discovery	
	T1033: System Owner/User Discovery	
	T1087: Account Discovery	T1087.002: Domain Account
	T1482: Domain Trust Discovery	
	T1018: Remote System Discovery	
	T1135: Network Share Discovery	
	T1083: File and Directory Discovery	
	T1518: Software Discovery	T1518.001: Security Software Discovery

Tactic	Technique	Sub-technique
Lateral Movement	T1021: Remote Services	T1021.002: SMB/Windows Admin Shares
		T1021.001: Remote Desktop Protocol
		T1021.006: Windows Remote Management
	T1570: Lateral Tool Transfer	
Command and Control	T1090: Proxy	T1090.003: Multi-hop Proxy
	T1105: Ingress Tool Transfer	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1573: Encrypted Channel	T1573.002: Asymmetric Cryptography
Exfiltration	T1041: Exfiltration Over C2 Channel	
Impact	T1486: Data Encrypted for Impact	
	T1490: Inhibit System Recovery	
	T1489: Service Stop	
	T1491: Defacement	T1491.001: Internal Defacement
	T1657: Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	194[.]87[.]31[.]69, 91[.]107[.]247[.]163, 45[.]86[.]230[.]112
SHA256	992c951f4af57ca7cd8396f5ed69c2199fd6fd4ae5e93726da3e198e78bec0a5, 025fc0976c548fb5a880c83ea3eb21a5f23c5d53c4e51e862bb893c11adf712a, 22b38dad7da097ea03aa28d0614164cd25fafeb1383dbc15047e34c8050f6f67, 2ed9494e9b7b68415b4eb151c922c82c0191294d0aa443dd2cb5133e6bfe3d5d, 3ab9575225e00a83a4ac2b534da5a710bdcf6eb72884944c437b5fbe5c5c9235, 48d9b2ce4fcd6854a3164ce395d7140014e0b58b77680623f3e4ca22d3a6e7fd, 62c2c24937d67fdeb43f2c9690ab10e8bb90713af46945048db9a94a465ffcb8, 860a6177b055a2f5aa61470d17ec3c69da24f1cdf0a782237055cba431158923, 87d25d0e5880b3b5cd30106853cbfc6ef1ad38966b30d9bd5b99df46098e546c, 8c87134c1b45e990e9568f0a3899b0076f94be16d3c40fa824ac1e6c6ee892db, 91415e0b9fe4e7cbe43ec0558a7adf89423de30d22b00b985c2e4b97e75076b1, 994d6d1edb57f945f4284cc0163ec998861c7496d85f6d45c08657c9727186e3, 9f61ff4deb8afced8b1ecdc8787a134c63bde632b18293fbfc94a91749e3e454, a7a19cab7aab606f833fa8225bc94ec9570a6666660b02cc41a63fe39ea8b0ad, 51b9f246d6da85631131fcd1fabf0a67937d4bdde33625a44f7ee6a3a7baebd2, 2834114ff7e487c4ca3f50ca39f7d652dea1be98f885c388f01b6ff35309307b

TYPE	VALUE
SHA256	b67958afc982cafbe1c3f114b444d7f4c91a88a3e7a86f89ab8795ac2110d1e6, c46b5a18ab3fb5fd1c5c8288a41c75bf0170c10b5e829af89370a12c86dd10f8, c7f7b5a6e7d93221344e6368c7ab4abf93e162f7567e1a7bcb8786cb8a183a73, ec368ae0b4369b6ef0da244774995c819c63cffb7fd2132379963b9c1640ccd2, efaf8e7422ffd09c7f03f1a5b4e5c2cc32b05334c18d1ccb9673667f8f43108f, f736be55193c77af346dbe905e25f6a1dee3ec1aedca8989ad2088e4f6576b12, fc75ed2159e0c8274076e46a37671cfb8d677af9f586224da1713df89490a958, cc14df781475ef0f3f2c441d03a622ea67cd86967526f8758ead6f45174db78e, 078163d5c16f64caa5a14784323fd51451b8c831c73396b967b4e35e6879937b, fe1033335a045c696c900d435119d210361966e2fb5cd1ba3382608cfa2c8e68, 5dc607c8990841139768884b1b43e1403496d5a458788a1937be139594f01dca, 788ba200f776a188c248d6c2029f00b5d34be45d4444f7cb89ffe838c39b8b19, 1eece1e1ba4b96e6c784729f0608ad2939cfb67bc4236dfababbe1d09268960c
MD5	d65c293efb5e6d033c83b2ac472bf0cb, 42c062d6299ca9f76554441a29429404, efd5366eb7473d6f7fb97ec7ac59f09d, 8901ce810f999f79c51c4d4f6c93fe6b
SHA1	c12c4d58541cc4f75ae19b65295a52c559570054, c0979ec20b87084317d1bfa50405f7149c3b5c5f, df249727c12741ca176d5f1ccba3ce188a546d28, e00293ce0eb534874efd615ae590cf6aa3858ba4

TYPE	VALUE
Ransom Note Filename	README-GENTLEMEN.txt
Tor Leak Site	Tezwsse5czllksjb7cwp65rvnk4oobmzti2znn42i43bjdfd2prqqkad[.]onion
Tox ID	D527959A7BC728CB272A0DB683B547F079C98012201A48DD2792B84604E8BC29F6E6BDB8003F, F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EBBDF92CF9A9B84079F8F04060FF98D098E, D2CBA43A1AF6D965432AE11487726DB84D2945CF2CD975D7774B76B54AF052418AC2E59ADA69
File Path	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\GupdateU, /bin/.vmware-authd, /etc/rc.local.d/local.sh

Recent Breaches

https://lawson.co.th
https://coralina.gov.co
https://yikekj.com
https://eecegypt.com
https://iesmartsystems.com
https://championhomes.com.au
https://eurocreations.co.th
https://uniview.com
https://suma24.pl
https://philiplee.ie
https://jeancard.com
https://teleosvet.co.uk
https://jumbotransport.dk
https://martonagency.com
https://sluzia.com.br
https://bmtp.co.th

Patch Links

https://fortiguard.fortinet.com/psirt/FG-IR-24-535

https://www.veeam.com/kb4424

https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24505

References

https://research.checkpoint.com/2026/dfir-report-the-gentlemen/

https://www.broadcom.com/support/security-center/protection-bulletin/cross-platform-and-coordinated-the-gentlemen-raas-targets-windows-linux-and-esxi

https://www.group-ib.com/blog/hastalamuerte-gentlemen-raas-ttps/

https://hivepro.com/threat-advisory/fortinet-firewalls-under-siege-exploitation-of-critical-zero-day-cve-2024-55591/

https://hivepro.com/threat-advisory/fin7-affiliated-hackers-exploit-flaws-in-veeam-backup-servers/

https://hivepro.com/threat-advisory/vmware-esxis-fatal-flaw-cve-2024-37085-opens-doors-for-ransomware-havoc/

https://hivepro.com/threat-advisory/medusalocker-uses-throttlestop-sys-flaw-to-kill-av-on-windows/

https://hivepro.com/threat-advisory/the-gentlemen-ransomware-a-rising-global-cyber-threat/

https://x.com/KrakenLabs_Team/status/1983458109323362432

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

April 24, 2026 • 10:00 AM

More at www.hivepro.com