Dark Web Profile: The Gentlemen Ransomware

Published: 2026-02-12 · Archived: 2026-04-05 15:25:36 UTC

Despite its polished name, The Gentlemen Ransomware shows little interest in playing nice. First observed in 2025, the group quickly established itself as a capable and coordinated threat, operating across multiple regions and enterprise environments with notable speed.

This profile outlines who The Gentlemen are, how they operate, which organizations they target, and what defenders should know to reduce exposure to this ransomware threat.

Who Is “The Gentlemen” Ransomware?

The Gentlemen is an emerging ransomware threat group first observed in mid-to-late 2025. While some indicators suggest development activity as early as July 2025, The ransomware group was first clearly observed in active campaigns beginning in August 2025.

Despite its relatively recent appearance, the group has demonstrated a level of technical maturity and operational discipline more commonly associated with established ransomware operators. This has led researchers to assess that The Gentlemen may consist of experienced actors, potentially with ties to earlier ransomware ecosystems.

Threat actor card for The Gentlemen Ransomware

The group operates a **double-extortion model**. After gaining access to a victim’s network, the attackers exfiltrate sensitive data, encrypt systems, and threaten to publish stolen information on Dark Web leak sites if ransom demands are not met. This approach increases pressure by combining operational disruption with reputational and regulatory risk.

Technically, The Gentlemen Ransomware is primarily written in **Go**, with variants targeting **Windows, Linux, and ESXi environments**. Execution requires a password parameter, a control mechanism that helps prevent accidental deployment in unintended or analysis environments. This design choice reflects a deliberate, operator-driven deployment model rather than indiscriminate spreading.

Observed Ransomware-as-a-Service (RaaS) Activity

In September 2025, SOCRadar observed a Dark Web forum post advertising “The Gentlemen’s RaaS,” indicating that the group was actively recruiting partners through a structured ransomware program. The post

invited teams and individual operators to cooperate and outlined a clear affiliate-based model.

Dark Web forum post advertises The Gentlemen's RaaS (SOCRadar Dark Web News)

According to the advertisement, affiliates are offered **90% of ransom proceeds** and full control over victim negotiations, while the operators retain centralized control over infrastructure such as the data leak site. Communication is handled primarily through TOX, and the service infrastructure is intentionally kept minimal to reduce operational exposure.

The post describes a **cross-platform ransomware family**, supporting **Windows, Linux, NAS, BSD**, and a dedicated **ESXi locker**, with malware written in **Go** and **C**. Advertised features include hybrid encryption using **XChaCha20 and Curve25519**, password-protected builds, partial or full encryption modes, background execution, and automated network discovery. The ESXi variant is positioned as optimized for virtualized environments, with support for multithreaded encryption and controlled VM handling.

Further features of The Gentlemen's RaaS (SOCRadar Dark Web News)

What Are The Gentlemen Ransomware's Targets?

The Gentlemen Ransomware primarily targets **medium to large organizations** operating complex enterprise environments.

Geographically, The Gentlemen operates on a **global scale**, impacting organizations across **at least 17 countries**. The **United States** leads with **9 victims**, followed by **Brazil (7)** and **Thailand (6)**. European activity is also notable, with **France (5)** and the **United Kingdom (4)** affected, alongside multiple victims in **Indonesia, Colombia, and Vietnam**. This distribution highlights a preference for regions with mature enterprise infrastructure rather than a single geographic focus.

Top 10 countries targeted by The Gentlemen Ransomware

Manufacturing and technology are the most affected industries, with **13 known victims each**, reflecting the group's focus on environments that rely heavily on shared infrastructure and centralized identity management. **Healthcare** follows with **10 victims**, where service disruption and sensitive data significantly increase extortion leverage, while **financial services** account for **9 victims**, driven by regulatory exposure and the value of confidential customer information. Additional activity has been observed in education and other operationally dependent sectors, indicating flexible but deliberate targeting.

Top 10 industries targeted by The Gentlemen Ransomware

Overall, The Gentlemen's targeting strategy emphasizes **high-impact environments** where enterprise access, shared systems, and operational dependency allow the group to maximize the effectiveness of its double-extortion model.

Recent Attacks and Claims Linked to The Gentlemen Ransomware

Public leak-site reporting suggests The Gentlemen continued adding new victims into late 2025 and January 2026. Here are a few recent examples, based on the group's published victim claims as tracked by ransomware monitoring sources:

- In mid-January 2026, the group listed Dongguan HYX Industrial with a discovery date of **January 16, 2026**, indicating ongoing activity into the new year.
- Around the same period, Rogers Capital appeared as a claimed victim with a discovery date of **January 14, 2026**, showing that the group's targeting extends beyond industrial sectors into business and financial services.
- On **January 11, 2026**, Warka Bank for Investment and Finance was also listed, reinforcing the group's willingness to name organizations in regulated sectors where data exposure can add extra pressure during extortion.
- In late 2025, one post tied to Solumek included a notable data-theft claim – **"1.5 terabytes of data stolen"** – which aligns with The Gentlemen's broader double-extortion playbook.

What Are The Gentlemen Ransomware's Techniques?

The Gentlemen Ransomware uses a **streamlined but highly effective attack chain**, built around adaptive tooling and deep enterprise access. Below is a concise, step-by-step overview incorporating the group's most notable techniques.

The Gentlemen Ransomware attack chain

Initial Access:

The attackers gain entry by exploiting **internet-exposed services** or **compromised administrative credentials**, including exposed firewall and VPN management interfaces such as FortiGate appliances.

Reconnaissance:

After establishing a foothold, the group maps the environment using tools like **Advanced IP Scanner** and Active Directory queries to identify:

- Domain administrators
- Privileged accounts
- Network shares and critical servers

Privilege Escalation:

To obtain full control, The Gentlemen abuse legitimate utilities such as **PowerRun.exe** to bypass User Account Control (UAC) and execute processes with **SYSTEM-level privileges**.

Defense Evasion:

Defense evasion is a core strength of the group. Techniques include:

- **Bring Your Own Vulnerable Driver (BYOVD)** abuse using signed drivers

- Custom tools (e.g., All.exe with ThrottleBlood.sys) to terminate antivirus and EDR processes
- Adaptive tooling that changes based on the victim's security stack

Lateral Movement:

With elevated access, the attackers move laterally using **PsExec over SMB admin shares**, allowing them to execute commands across multiple systems while blending into normal administrative traffic.

Ransomware Deployment:

The ransomware is deployed centrally through **domain resources such as NETLOGON shares**, using **password-protected payloads** to prevent accidental execution and analysis. The group is capable of encrypting **Windows, Linux, and ESXi** environments.

Impact:

Before encryption, the malware:

- Terminates backup, database, virtualization, and security services
- Deletes logs and recovery artifacts

Encrypted files are appended with the **.7mtzhh** extension, and ransom notes named **README-GENTLEMEN.txt** are dropped across affected systems to initiate double-extortion pressure.

This focused, step-driven methodology highlights how The Gentlemen combine **legitimate tools, privileged access, and adaptive evasion** to execute high-impact ransomware attacks against enterprise environments.

What Are the Mitigation Tactics Against The Gentlemen Ransomware?

Defending against The Gentlemen Ransomware requires a focus on **preventing privileged abuse and early-stage detection**, rather than relying solely on signature-based protection.

Key mitigation strategies include:

- **Reducing attack surface** by securing internet-facing services and eliminating unnecessary external access
- **Enforcing strong identity controls**, including multi-factor authentication for all administrative accounts
- **Monitoring Active Directory activity**, especially mass account enumeration, GPO changes, and NETLOGON modifications
- **Hardening endpoints** against driver abuse and unauthorized service termination attempts
- **Restricting execution paths**, particularly user download and temporary directories commonly used for tool staging
- **Maintaining offline, tested backups** to ensure recovery options remain viable

Organizations should also prioritize **behavior-based detection** capable of identifying reconnaissance, defense evasion, and lateral movement well before encryption is triggered.

How Can SOCRadar Help?

SOCRadar can support defense against The Gentlemen Ransomware by providing targeted visibility across external exposure, underground activity, and ransomware operations.

- **Dark Web Monitoring** enables organizations to track The Gentlemen's leak sites, underground forums, and extortion activity, helping identify stolen data, victim listings, or brand mentions early in the extortion cycle.

SOCRadar's Dark Web Monitoring

- **Ransomware Group Tracking** provides ongoing insight into The Gentlemen's infrastructure, tooling, and targeting patterns, allowing security teams to anticipate shifts in tactics and respond proactively.

SOCRadar's Threat Actor Intelligence, The Gentlemen Ransomware details

- **Attack Surface Management (ASM)** identifies exposed VPNs, firewalls, and remote access services that ransomware operators commonly exploit for initial access, reducing entry points before they are abused.
- **Threat Intelligence Feeds** deliver actionable indicators of compromise and observed TTPs associated with The Gentlemen, enabling faster detection, threat hunting, and security control updates.

Together, these SOCRadar modules help organizations detect exposure earlier, reduce attack surface risk, and strengthen preparedness against advanced ransomware campaigns.

What Are the MITRE ATT&CK TTPs of The Gentlemen Ransomware?

Tactic	Technique ID	Technique Name
Initial Access	T1190	Exploit Public-Facing Application
	T1078	Valid Accounts
	T1078.002	Valid Accounts: Domain Accounts
Execution	T1059	Command and Scripting Interpreter
	T1059.001	Command and Scripting Interpreter: PowerShell
	T1059.003	Command and Scripting Interpreter: Windows Command Shell
Persistence	T1547	Boot or Logon Autostart Execution
	T1136	Create Account
Privilege Escalation	T1068	Exploitation for Privilege Escalation
Defense Evasion	T1562	Impair Defenses
	T1112	Modify Registry

	T1027	Obfuscated Files or Information
	T1484.001	Domain Policy Modification: Group Policy Modification
Discovery	T1046	Network Service Discovery
	T1087	Account Discovery
	T1087.002	Account Discovery: Domain Account
	T1482	Domain Trust Discovery
Lateral Movement	T1021	Remote Services
	T1021.001	Remote Services: Remote Desktop Protocol
	T1021.002	Remote Services: SMB/Windows Admin Shares
	T1021.004	Remote Services: SSH
Collection & Exfiltration	T1074	Data Staged
	T1074.001	Data Staged: Local Data Staging
	T1039	Data from Network Shared Drive
	T1048	Exfiltration Over Alternative Protocol
	T1048.001	Exfiltration Over Alternative Protocol: Unencrypted/Obfuscated Non-C2 Protocol
Command & Control	T1071	Application Layer Protocol
	T1071.001	Application Layer Protocol: Web Protocols
	T1219	Remote Access Software
Impact	T1486	Data Encrypted for Impact
	T1489	Service Stop
	T1552	Unsecured Credentials
