



THREAT PROFILE:

The Gentlemen Ransomware



TABLE OF CONTENTS

Executive Summary

2

Description

3

Previous Targets

- Previous Industry Targets
- Previous Victim HQ Regions

4

Data Leak Site

6

Known Tools

7

Observed Behaviors

- Windows

9

MITRE ATT&CK[®] Mappings

11

References

14

Executive Summary

First Identified:

2025

Operation style:

Ransomware-as-a-Service (RaaS)

Extortion method:

Double Extortion - where the operators encrypt victim data and exfiltrate sensitive data and threat to leak that data if the ransom is not paid.

Most frequently targeted industry:

- Industrials (Manufacturing)

Most frequently targeted victim HQ region:

- South America
- Asia

INITIAL ACCESS

Valid accounts, vulnerability exploitation (MITRE ATT&CK: T1078, T1190)

PERSISTENCE

Create account, create or modify system process, hijack execution flow (MITRE ATT&CK: T1136, T1543, T1574)

LATERAL MOVEMENT

Remote services, lateral tool transfer (MITRE ATT&CK: T1021, T1570)

Description

The Gentlemen Ransomware is an operation that first emerged in August 2025 and operates as a ransomware-as-a-service (RaaS). The group reportedly operates in the double extortion method, where the group encrypts victim data and exfiltrates sensitive data that can be held for ransom. The group threatens to leak the data via a data leak site if the ransom demand is not paid.

Researchers have reported that The Gentlemen operators have displayed sophistication in their attacks, adapting tactics mid-campaign, and strategic initial access methods rather than opportunistic. Additionally, the group appears to conduct significant reconnaissance on their victims by using custom tools designed to target specific security vendors.

The Gentlemen operators have been reported to create new accounts, modify system processes, and hijack execution flows for persistence. Additionally, the group has been reported to deploy the tool, AnyDesk, to maintain remote access to victim environments.

The group has been reported to modify critical registry settings that govern authentication and remote access protocols and rely on PsExec for lateral movement. Additionally, The Gentlemen group was reported to use the Group Policy Management Console and Group Policy Management Editor to attempt to deploy malicious configurations across the domain.

The Gentlemen operators utilized WinSCP for data exfiltration and used encrypted channels highlighting how the group likely prioritizes operational security.

Similar to many other ransomware operations, The Gentlemen deletes Shadow Copies, disables defensive measures, such as Windows Defender, and modifies firewall rules.

The Gentlemen has proved to be an adaptable and persistent threat to victim organizations.

Once the victims' environment is encrypted, The Gentlemen drops a ransom note "README-GENTLEMEN.txt" and each file is appended with a six character extension. Additionally, the ransomware changes the desktop wallpapers.

In September 2025, a user "Zeta88" was observed advertising The Gentlemen RaaS operation on the cybercriminal forum, RAMP. According to the user, the ransomware targets Windows, Linus, BSD, NAS, and ESXi environments using compact, efficient binaries. The ransomware reported encrypts files with hybrid cryptography, XChaCha20 with Curve25519, and generates a unique ephemeral key for each file.

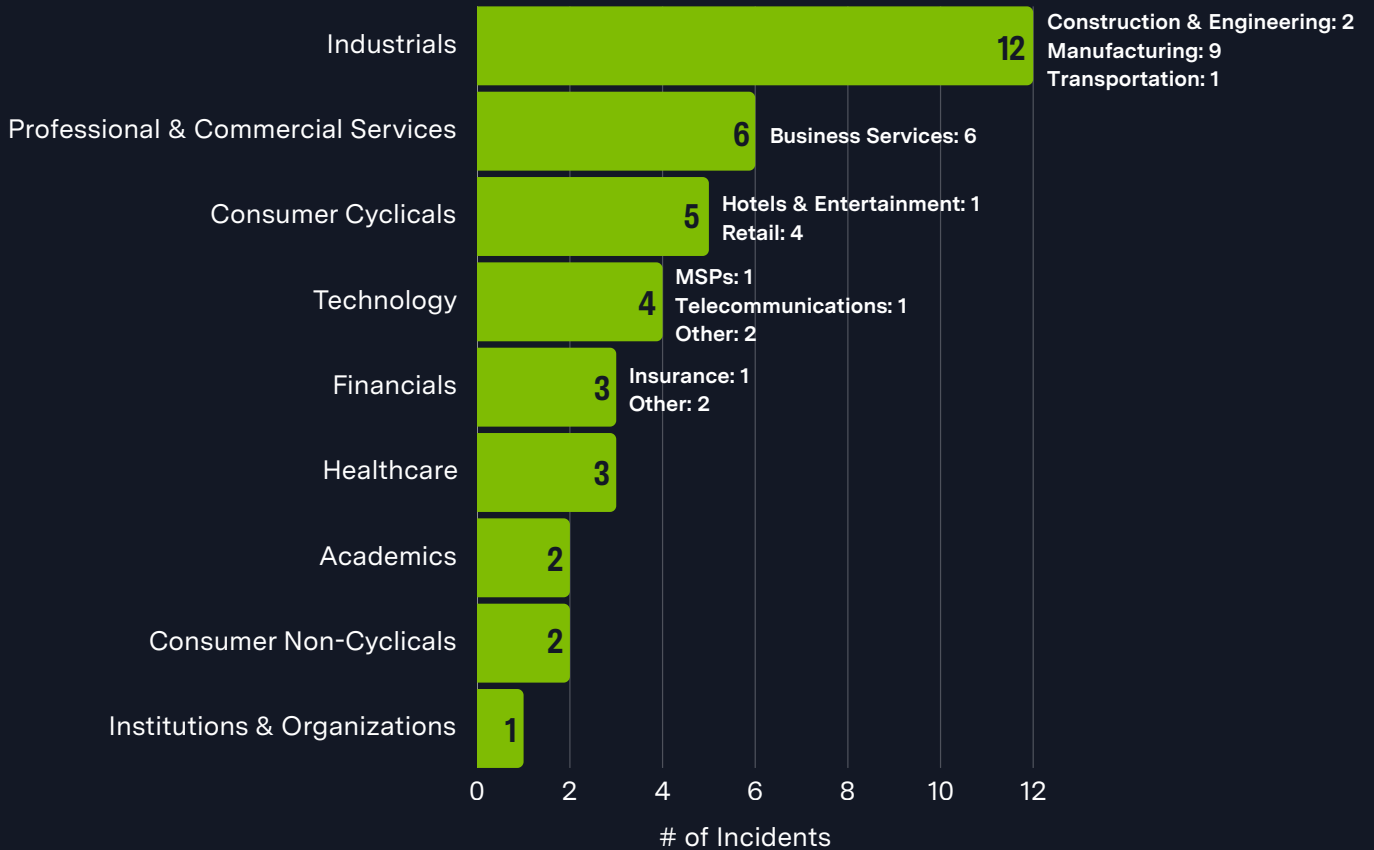
Additionally, the user stated that the ransomware can run multiple instances on the same machine without conflict, forcibly access locked folders, and contains an extended kill list to terminate processes and services.

While The Gentlemen operation recently appeared within the ransomware landscape, their tactics indicate the operators are likely experienced in ransomware operations. The group appears to be focused on extensive reconnaissance efforts, custom tooling to ensure successful attacks, and operational security to prevent identification.

It is likely that The Gentlemen is a persistent ransomware operation with a goal of conducting targeted, more customized attacks. It is very likely that ransomware will remain a pervasive threat to organizations worldwide over the next 12 months.

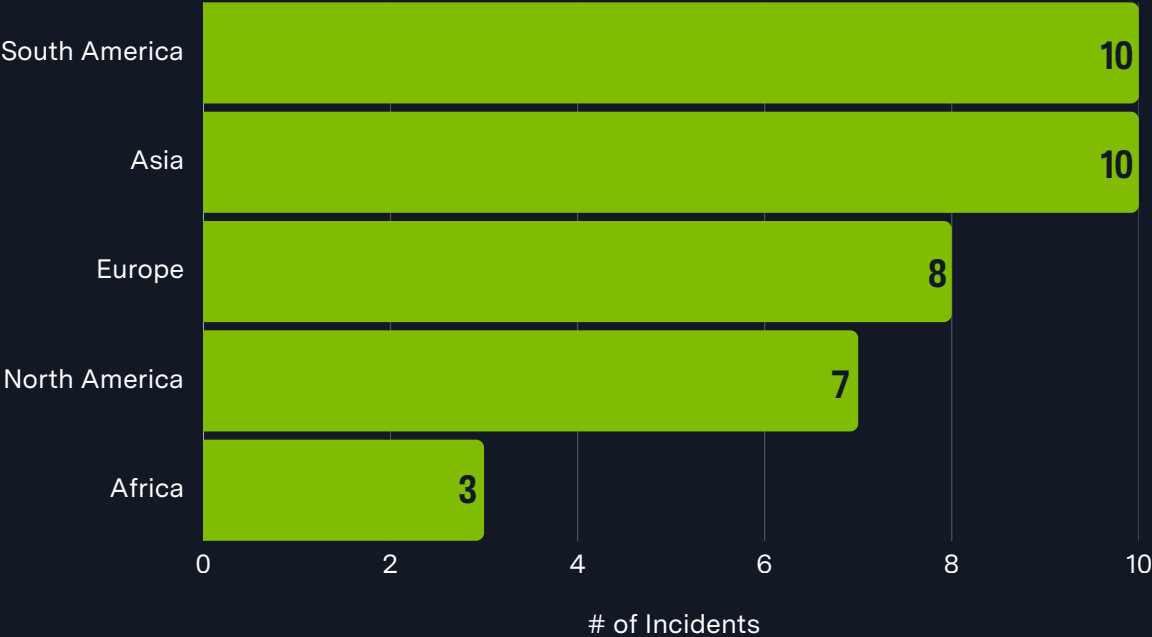
Previous Targets

Previous Industry Targets from 01 Aug 2025 to 30 Sept 2025



Previous Targets

Previous Victim HQ Regions from 01 Aug 2025 to 30 Sept 2025



Data Leak Site



Welcome to our blog!

Créée en 1991, la société [redacted] est une société française dont le siège social est situé en Ile-de-France, au cœur de l'Essonne. Initialement spécialisée dans la peinture anti-corrosion et autres prestations, [redacted] est professionnalisée dans la conception, la fabrication et la distribution de matériels de sécurité puis de coffrages pour le bâtiment (location [redacted] ventes, prestations de remise en état). [redacted] dispose d'un parc matériel de 52.000 m², de moyens de manutention et de soudure, d'un atelier pour le traitement de surface, ainsi que des ateliers pour l'entretien de matériels pour le BTP (grenailage / peinture). Forte de 30 années d'expérience et de collaboration avec les plus grands groupes du BTP, [redacted] su s'adapter aux nouvelles contraintes de production et de sécurité pour concevoir des produits plus performants, plus ergonomiques et plus respectueux de l'environnement.

Data

broyeurs de branches et de végétaux Saelen. Demandez une démonstration et découvrez les broyeurs Eliet, les tondeuses Walker et Messex, les rogneuses de souches Rayco, le matériel Re [redacted] les épandeurs à sel et sable Snowex. [redacted] votre fournisseur expert en machines u [redacted] entretien des espaces verts. HEIZOMAT FRANCE, fournisseur de solutions d'énergies renouvelables, propose des équipements répondant à tous les besoins de la filière [redacted] - broyeurs des plaquettes de bois de 30 à 80 cm de diamètre [redacted] - chaudières à bois [redacted] - déchiqueté entièrement automatisés [redacted] - filtre céramique ZERO particules fines. Entreprise en forte croissance, engagée pour la transition énergétique, dans le domaine de la biomasse énergie, propose et intègre des équipements répondant à tous les besoins de la filière [redacted]

Data

[redacted] service, and outsourcing organization. Our approach is to use our deep expertise in enterprise, extend enterprise solutions and outsourcing to help our clients create value for their customers and stakeholders. We use our industry and business-process knowledge, coupled with our awareness and understanding of emerging technologies, and new business and technology trends to design and implement solutions for our clients. We strive to help our clients improve their operational performance, deliver their products and services more effectively and efficiently, and grow their businesses in existing and new markets. We consider each of our clients unique, strive to design solutions exclusive to their business needs, and intend to help our clients move forward in every part of their businesses, from strategic planning to day-to-day operations.

Data

[http://tezwss5czllksjb7cwp65rvnk4oobmzti2znn42i43bjdfd2prqqkad\[.\]onion/](http://tezwss5czllksjb7cwp65rvnk4oobmzti2znn42i43bjdfd2prqqkad[.]onion/)

Associations

Zeta88

Zeta88 is a threat actor on the Russian-language criminal forum, RAMP, that has been observed advertising The Gentlemen RaaS operation. The exact relationship to the group remains unverified; it is likely that the user is a part of the core operation.

Known Tools

Advanced IP Scanner	A fast and powerful network scanner with a user-friendly interface. It can locate all computers on your wired or wireless local network and scan their ports.
All.exe	An AV killer that uses Throttlestop.sys to hijack kernel functions and enable the execution of kernel-mode-only routines from user mode.
Allpatch2.exe	A custom tool used to neutralize key security agent components by targeting and terminating relevant processes.
AnyDesk	A remote desktop application that provides remote access to computers and other devices.
cmd	A program used to execute commands on a Windows computer.
GPMC	Group Policy Management Console. A tool for centrally managing Group Policy Objects (GPOs) in Active Directory and can be abused to gain unauthorized access, deploy malware, and abuse GPOs to disable security settings, create backdoors, and steal data.
Group Policy Management Editor	A Windows administration tool for configuring system and user settings via Group Policy Objects (GPOs) and can be abused to gain persistence, disable security settings, and move laterally through a network.
net	A Windows utility that is used in command-line operations for control of users, groups, services, and network connections. It can gather system and network information, move laterally through SMB/Windows Admin Shares, and interact with services.
netsh	A scripting utility used to interact with networking components on local or remote systems.
nmap	An open-source utility for network discovery; it runs on all major computer operating systems and includes multiple tools that can be used to transfer data, compare scan results, and generate packets.
PowerRun	A legitimate tool that is frequently exploited for privilege escalation; it is designed to run programs with the highest system privileges and provides attackers with a way to bypass security controls and execute malicious actions.

Known Tools

PowerShell	A task automation and configuration management program that includes a command-line shell and the associated scripting language.
PsExec	A command-line utility that allows users to execute processes on remote systems; it is part of the Sysinternals suite and is frequently used by system admins for remote management tasks. The tool is also repeatedly abused by threat actors for lateral movement and remote execute.
PuTTY	A free and open-source terminal emulator, serial console and network file transfer application.
RDP	A protocol that provides a user with a graphical interface to connect to another computer over a network connection.
Taskkill	A legitimate Windows file that is used by malware to terminate processes on the victims' computer.
ThrottleStop.sys	A legitimate driver developed by TechPowerUp and used by the ThrottleStop app; the application is designed to monitor and correct CPU throttling issues, and is mostly used by gamers.
VssAdmin	A Windows service that allows taking manual or automatic backup copies of computer files or volumes..
WebDAV	Web Distributed Authoring and Versioning. An extension of the HTTP protocol that allows users to perform collaborative document authoring and management on a remote server, enabling remote file editing, updating, and organization.
wevutil	A command utility used primarily to register a provider on the computer and can be used to retrieve information about event logs and publishers.
WinSCP	A free and open-source SFTP, FTP, WebDAV, S3, and SCP client for Windows that can be used to exfiltrate files to a remote server.
WMIC	A utility that provides a command-line interface for Windows Management Instrumentation.

Observed Behaviors: Windows

Tactic	Commands Observed
Persistence	<pre>reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0 /v RestrictSendingNTLMTraffic /t REG_DWORD /d 0 /f reg add HKLM\System\CurrentControlSet\Control\Lsa /t REG_DWORD /v DisableRestrictedAdmin /d 0x0 /f reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v SecurityLayer /t REG_DWORD /d 1 /f "C:\Windows\System32\gpme.msc" /s /gpobject:"LDAP://<REDACTED>/cn<REDACTED>,cnpolicies,cnssystem,DC<R EDACTED>,DClocal"</pre>
Discovery	<pre>C:\Program Files (x86)\Advanced IP Scanner\advanced_ip_scanner.exe user admin.it /dom user administrator /dom user fortigate /dom group "domain admins" /dom group "Enterprise admins" /dom localgroup __vmware__ localgroup administrators nmap -sV -T4 -O -F -oX C:\Users\FORTIG~1\AppData\Local\Temp\zenmap- 7ii30x5l.xml --version-light <IP address></pre>
Defense Evasion	<pre>\$myuserprofile\$\Downloads\All.exe \$myuserprofile\$\Downloads\ThrottleBlood.sys Set-MpPreference -DisableRealtimeMonitoring \$true -Force Add-MpPreference -ExclusionProcess "C:\Windows\Temp\<REDACTED>" netsh firewall set service type remotedesktop mode enable</pre>
Collection	<pre>C:\programdata\data\<REDACTED>.pdf:zone.identifier:\$data C:\Windows\system32\davclnt.dll,DavSetCookie <IP Address> http://\ <REDACTED>// C:\Windows\system32\davclnt.dll,DavSetCookie <IP Address> http://\ <REDACTED>//share_EXT01 C:\Windows\system32\davclnt.dll,DavSetCookie <IP Address> http://\ <REDACTED>//c\$</pre>
Exfiltration	<pre>C:\ProgramData\data\INTERNAL\Summary<REDACTED> → "C:\ProgramData\WinSCP.exe"</pre>

Observed Behaviors: Windows

Tactic	Commands Observed
Impact	\\<REDACTED>.local\NETLOGON\<REDACTED>.exe --password <8-byte key> README-GENTLEMEN.txt

MITRE ATT&CK[®] Mappings

Reconnaissance

T1592: Gather Victim Host Information

Initial Access

T1078: Valid Accounts

.002: Domain Accounts

T1190: Exploit Public-Facing Application

Execution

T1059: Command and Scripting Interpreter

.001: PowerShell

.003: Windows Command Shell

T1129: Shared Modules

Persistence

T1136: Create Account

.001: Local Account

T1543: Create or Modify System Process

.003: Windows Service

T1574: Hijack Execution Flow

.001: DLL

Privilege Escalation

T1484: Domain or Tenant Policy Modification

.001: Group Policy Modification

Defense Evasion

T1014: Rootkit

MITRE ATT&CK[®]

Mappings

Defense Evasion

T1027: Obfuscated Files or Information

T1070: Indicator Removal

.001: Clear Windows Event Logs
.004: File Deletion

T1112: Modify Registry

T1562: Impair Defenses

.001: Disable or Modify Tools
.004: Disable or Modify System Firewall

Discovery

T1018: Remote System Discovery

T1046: Network Service Discovery

T1069: Permission Groups Discovery

.002: Domain Groups

T1087: Account Discovery

.002: Domain Account

T1482: Domain Trust Discovery

T1518: Software Discovery

Lateral Movement

T1021: Remote Services

.001: Remote Desktop Protocol
.002: SMB/Windows Admin Shares
.004: SSH

T1570: Lateral Tool Transfer

MITRE ATT&CK[®] Mappings

Collection	
T1005: Data from Local System	
T1039: Data from Network Shared Drive	
T1074: Data Staged	.001: Local Data Staging
Command and Control	
T1071: Application Layer Protocol	.001: Web Protocols
T1219: Remote Access Tools	.002: Remote Desktop Software
Exfiltration	
T1048: Exfiltration Over Alternative Protocol	.001: Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Impact	
T1486: Data Encrypted for Impact	
T1489: Service Stop	
T1490: Inhibit System Recovery	
T1657: Financial Theft	

References

- Chassignol, Florent (18 September 2025) SOS Ransomware: “The Gentlemen: the new ransomware of autumn 2025.” <https://sosransomware.com/en/ransomware-groups/the-gentlemen-the-new-ransomware-of-autumn-2025/>
- Hive Pro (2025, September 10) “The Gentlemen Ransomware: A Rising Global Cyber Threat.” <https://hivepro.com/threat-advisory/the-gentlemen-ransomware-a-rising-global-cyber-threat/>
- Santos, Jacob; Policarpio, Maristel; et. al. (2025, September 09) Trend Micro: “Unmasking The Gentlemen Ransomware: Tactics, Techniques, and Procedures Revealed.” https://www.trendmicro.com/en_us/research/25/i/unmasking-the-gentlemen-ransomware.html



Adversary Pursuit Group

