The Gentlemen Ransomware

Target Bio

Names/Alias: The Gentlemen Ransomware, The Gentlemen, thegentlemen
Affiliations: Zeta88, hastalamurete
Motivation: Financial gain
First Activity: June 30, 2025
Structure: Centralized
Country of Origin: Unknown
Targets: Manufacturing, technology, healthcare, financial services and education
Methodology: Double-extortion, ransomware
Most Recent Development: February 26, 2026 – Sando Tech (Japan)

BLUF

The Gentlemen Ransomware (often referred to as just 'The Gentlemen') is a Ransomware-as-a-Service (RaaS) group that utilizes a double-extortion attack model to target organizations, coercing them to purchase their stolen data back, lest it be posted publicly on the dark web. They primarily attack high impact areas like manufacturing, technology and healthcare to increase their success rate and payouts they receive.

Background

Despite less than a year of activity, The Gentlemen have continuously displayed an incredible level of skill and experience hacking various organizations [1][2][3][4][5][6][7]; This suggests that while the group itself is new, the members are likely a rebranded crew, or veteran hackers with prior experience in the field [1][2]. Thus far, the Gentlemen have targeted 17 different countries, focusing primarily on manufacturing, healthcare, and consumer services that host windows environments [1][3][4]. This this group distinguish themselves by adopting a highly methodical approach in their exploits, as opposed to most other RaaS groups opportunistic approach [1][2][7].

Summary (General Overview)

The Gentlemen are motivated solely by financial gain. They attack medium to large sized organizations and critical infrastructure sectors globally with a very high success rate [1][3][4][7]. Since their appearance in 2025, they have quickly become a major player in the RaaS community. They recruit new partners via forums posted on the dark web, the first of which was found in September 2025. These forums advertise that affiliates are offered 90% of ransom proceeds, full control over victim negotiations and guaranteed safety. [1][2][7]. Affiliates receive highly customizable pre-configured builds along with lockers for Windows, Linux, BSD, NAS, and ESXI environments. Per the forum's rules, any exfiltrated data must be uploaded to The Gentlemen's cloud resources in case demands are not met and publication is necessary [1][2]. The attack pattern they utilize is detailed and highly efficient; Gain initial access, perform recon and explore the network, evade defenses and escalate privileges, move laterally across the network**, and lastly,** exfiltrate the data and encrypt it. After this process, a ransom note (README -GENTLEMEN.txt) file is left, and negotiations ensue [1][2][3][4][6]7].

Details & References

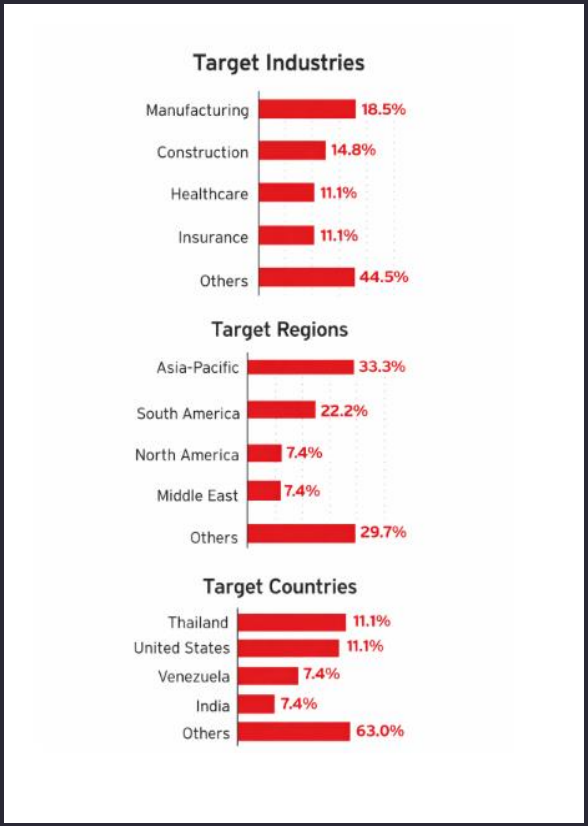
Analysis Summary

In less than a year, The Gentlemen have very quickly become a major threat to businesses and organizations worldwide. Because of their high levels of skill, experience, and adaptability, they opt for a highly detailed and precise attack methodology, as opposed to the more common opportunistic approach, distinguishing themselves from other RaaS groups in the industry [1][2][3][4][5][7].

Analyzing the attack history of The Gentlemen reveals that geographically speaking, they prefer to target regions with developed enterprise infrastructure and high-impact environments [1][4][7]. When it comes to organizational preference, their most frequent targets are manufacturing, technology, and healthcare companies across many different countries. Their focus on organizations with shared systems and operational-dependency maximizes the effectiveness of the double-extortion attack model they utilize, further emphasizing the experience level and operational awareness the group [1][3][7].

It can be expected that The Gentlemen will continue attacking organizations at the same rate as (if not faster than) last year with a continued focus on medium to large scale manufacturing, technology, and healthcare businesses. They will continue to be one of the most prominent RaaS groups, further developing their tools, connections, and TTP's, making them one of the most prominent threats to organizations across the globe.

To prevent attacks from The Gentlemen and other similar ransomware groups, organizations should address the common vulnerabilities these actors frequently exploit. This includes hardening internet-facing services by disabling unused firewall ports, enforcing privileged access controls through tiered administrative accounts, monitoring the use of administrative tools, restricting outbound data transfers by limiting SSH/SFTP to approved servers, controlling execution paths to prevent unauthorized code from running, and monitoring Group Policy Objects (GPOs) for unexpected changes [1][2][3][7]. These technical measures should be supported by a strong security framework, adherence to established best practices, and consistent employee awareness training.



Unmasking The Gentlemen Ransomware: Tactics,

References

[1] https://socradar.io/blog/dark-web-profile-the-gentlemen-ransomware/

[2] https://www.provendata.com/blog/gentlemen-ransomware/

[3] https://blackpointcyber.com/threat-profile/gentlemen-ransomware/

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

[5] https://assets.kpmg.com/content/dam/kpmgsites/in/pdf/2025/11/kpmg-ctip-gentlemen-ransomware-11-nov-2025.pdf.coredownload.inline.pdf

[6] The Gentlemen

[7] The Gentlemen: the new ransomware of autumn 2025