Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

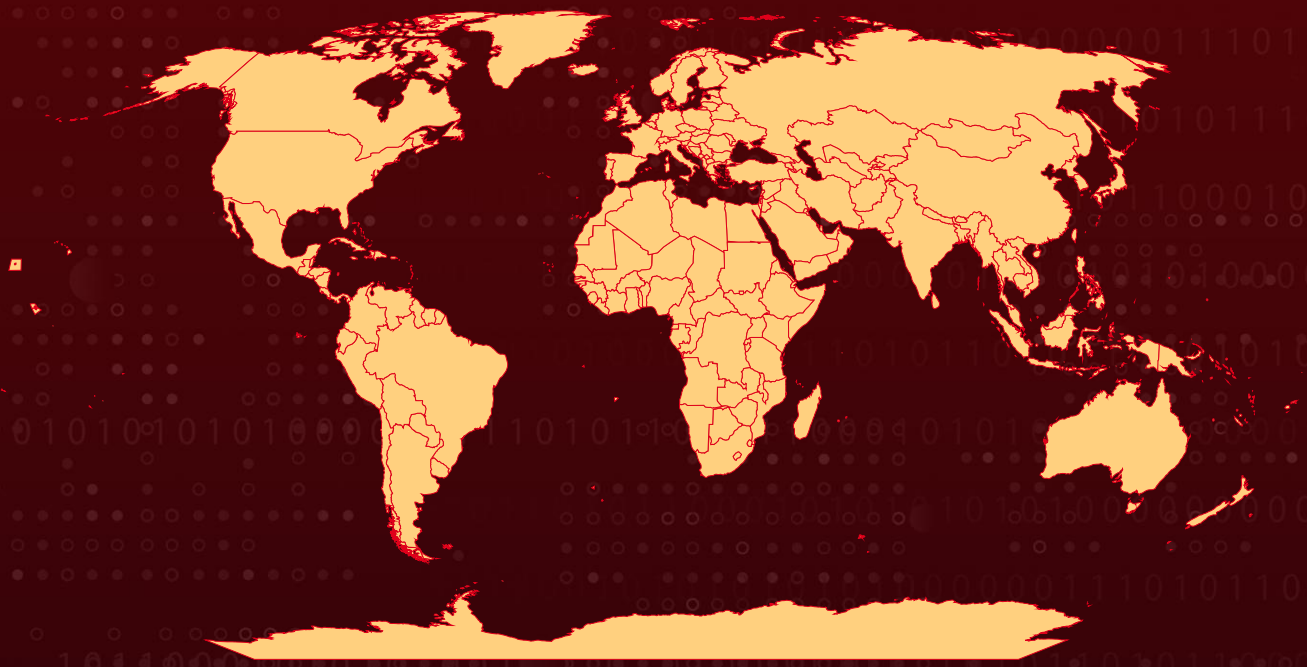
The Gentlemen Ransomware: A Rising Global Cyber Threat

Date of Publication	Admiralty Code	TA Number
September 10, 2025	A1	TA2025277

Summary

First Seen: August 2025
Targeted Countries: Worldwide
Targeted Industries: Manufacturing, Construction, Healthcare, Insurance, Consumer Services
Targeted Platforms: Windows
Malware: The Gentlemen
Attack: A newly identified ransomware group, The Gentlemen, is conducting highly adaptive attacks across more than 17 countries, targeting critical sectors like manufacturing, healthcare, and insurance. Their operations leverage legitimate tools, custom anti-AV software, and environment-specific malware to evade defenses and maintain persistence. This marks a shift toward more targeted ransomware strategies, urging organizations to adopt proactive detection and incident response measures.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1

The Gentlemen ransomware group, first profiled in August 2025, has rapidly emerged as a significant threat through highly tailored attacks targeting enterprise environments, particularly in sectors like manufacturing, construction, healthcare, and insurance across 17 countries. The group's operators demonstrate advanced capabilities, systematically compromising infrastructure by adapting their toolkit mid-campaign to bypass endpoint defenses and security software, indicating either a well-funded new entrant or a rebrand of experienced threat actors.

#2

Initial access was likely gained by exploiting internet-exposed services and privileged device accounts, most notably, they abused compromised FortiGate administration for deep network reconnaissance and lateral movement. The Gentlemen deploy a range of legitimate and malicious tools, leveraging signed driver abuse for defense evasion, custom anti-AV utilities, and living-off-the-land methods like PowerRun, PsExec, Nmap, and PuTTY for privilege escalation and remote access.

#3

The campaign features extensive group and account enumeration, Group Policy manipulation via privileged PowerShell and console tools, and highly customized payload delivery. Persistence and stealth are maintained using AnyDesk for remote access, registry modifications for survivability, and encrypted channels for data exfiltration, most notably via WinSCP. Data staging and exfiltration procedures are methodical, revealing strong operational security awareness.

#4

Once inside, The Gentlemen neutralize backup, security, and critical process operations to maximize impact. The ransomware is distributed via domain NETLOGON shares, employs password-protected payloads to evade automated analyses, and aggressively terminates backup, database, and AV services, deleting forensic logs and recovery files to impede incident response. Each victim system receives a "README-GENTLEMEN.txt" ransom note and files are appended with a ".7mtzhh" extension, signaling compromise. The Gentlemen represent a serious threat, using legitimate tools and tailored malware in methodical, customized attacks that mark a troubling evolution in ransomware sophistication.

Recommendations

Harden Privileged Accounts and Active Directory: Limit privileged account use through least privilege principles and Just-In-Time access. Audit Group Policy Objects regularly and monitor for abnormal authentication patterns that may signal compromise.

Defend Against Driver and Tool Abuse: Block unsigned or untrusted drivers and enforce an allowlist of approved drivers and administrative tools. Closely monitor for unauthorized use of remote access software such as AnyDesk.

Strengthen Endpoint and Network Security: Use EDR/XDR solutions to detect anti-AV tampering and monitor for suspicious encrypted transfers with tools like WinSCP. Segment networks and apply data loss prevention controls to reduce exfiltration risks.

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 an The Gentlemen ransomware attack, up-to-date backups enable recovery without paying the ransom.

Potential MITRE ATT&CK TTPs

TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
TA0010 Exfiltration	TA0040 Impact	TA0001 Initial Access	TA0002 Execution
T1046 Network Service Discovery	T1190 Exploit Public-Facing Application	T1078.002 Domain Accounts	T1078 Valid Accounts

T1059.003 Windows Command Shell	T1059.001 PowerShell	T1059 Command and Scripting Interpreter	T1018 Remote System Discovery
T1087.002 Domain Account	T1087 Account Discovery	T1069 Permission Groups Discovery	T1069.002 Domain Groups
T1482 Domain Trust Discovery	T1562.001 Disable or Modify Tools	T1562 Impair Defenses	T1014 Rootkit
T1112 Modify Registry	T1562.004 Disable or Modify System Firewall	T1027 Obfuscated Files or Information	T1484.001 Group Policy Modification
T1484 Domain or Tenant Policy Modification	T1219 Remote Access Software	T1021.002 SMB/Windows Admin Shares	T1021 Remote Services
T1021.001 Remote Desktop Protocol	T1021.004 SSH	T1074.001 Local Data Staging	T1074 Data Staged
T1039 Data from Network Shared Drive	T1071.001 Web Protocols	T1071 Application Layer Protocol	T1048 Exfiltration Over Alternative Protocol
T1048.001 Exfiltration Over Symmetric Encrypted Non-C2 Protocol	T1486 Data Encrypted for Impact	T1489 Service Stop	T1552 Unsecured Credentials

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	c12c4d58541cc4f75ae19b65295a52c559570054, c0979ec20b87084317d1bfa50405f7149c3b5c5f, df249727c12741ca176d5f1ccba3ce188a546d28, e00293ce0eb534874efd615ae590cf6aa3858ba4

Recent Breaches

www.kandeofund.com
www.pcchandraindia.com

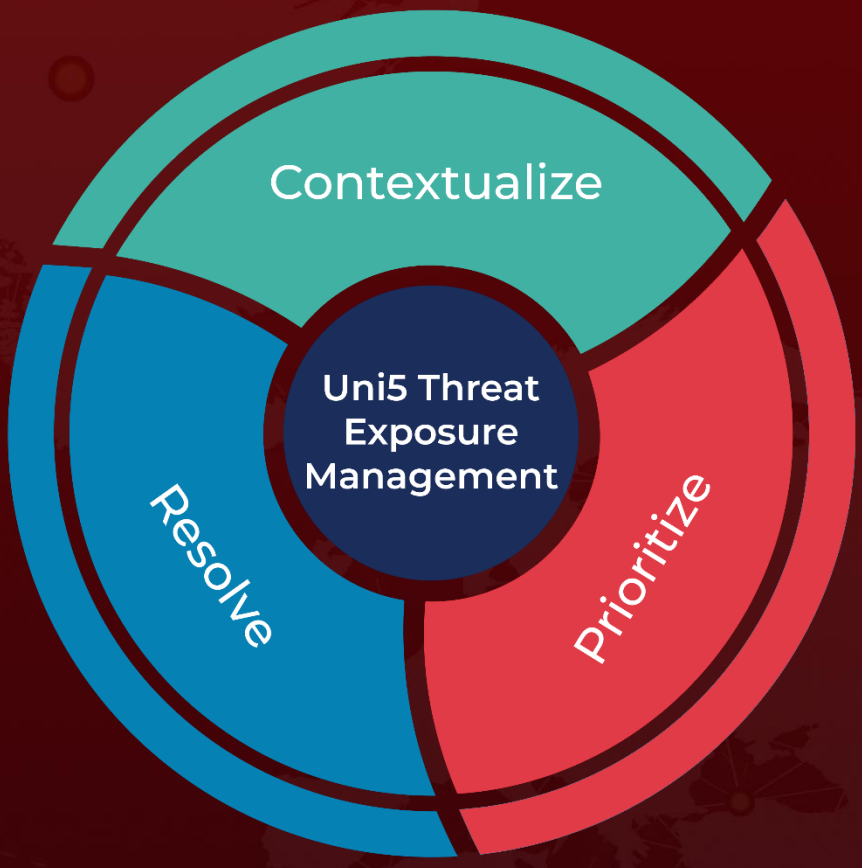
References

https://www.trendmicro.com/en_us/research/25/i/unmasking-the-gentlemen-ransomware.html

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 free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 10, 2025 . 7:30 AM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com