29 May 2026

TLP: WHITE

INTEL471

EMERGING THREATS

Gentlemen Ransomware

The Gentlemen ransomware operation emerged as a rapidly evolving ransomware threat observed throughout 2025, leveraging aggressive defense evasion techniques and multi-stage intrusion activity to compromise enterprise environments. Researchers have linked the group to campaigns targeting organizations across multiple regions across the globe including North America, Europe, and Asia, with observed victims spanning industries such as healthcare, manufacturing, technology, and professional services. The ransomware itself employs a double extortion model in which sensitive data is exfiltrated prior to encryption, allowing the attackers to pressure victims through both operational disruption and threats of public data exposure. It is worthy to note that the group demonstrates a high degree of operational maturity, utilizing stealth-focused tradecraft, remote administration tooling, and credential abuse techniques that closely resemble behaviors observed in other advanced ransomware ecosystems.

GENTLEMEN RANSOMWARE HUNT COLLECTION

https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:last_updated_desc,term:!('a89a84e3-505f-428d-ab34-9ebbc482d871'),touched:!t)

RELATED HUNT PACKAGES

Direct to IP Address in Execution of WebDav DLL via Rundll32 - Malicious Link or Exploitation

https://hunter.cyborgsecurity.io/research/hunt-package/d020807d-8833-460f-ac88-b004b74ecea4

File Writes with Single Character File Names and Execution Extension - Potential Malware Staging

https://hunter.cyborgsecurity.io/research/hunt-package/f20c5f61-c68a-446d-95c4-e227d3ac1078

Suspicious Execution of NetExec (NXC)

https://hunter.cyborgsecurity.io/research/hunt-package/5d3b649c-f8dd-4e77-a087-d8114795de43

Execute Payload as Trusted Installer

https://hunter.cyborgsecurity.io/research/hunt-package/d8160c37-219d-43c4-a975-90770d2e4437

Executable Run from SYSVOL or NETLOGON Director

https://hunter.cyborgsecurity.io/research/hunt-package/63043074-c4fe-456b-87b6-3a6fe5ca6933

Copyright © 2026 Intel 471, Inc. All Rights Reserved.

Remote Desktop Protocol (RDP) port manipulation

https://hunter.cyborgsecurity.io/research/hunt-package/015d7a14-0b42-42b9-8328-991738d64e56

Double File Extension - Potential Malware Execution

https://hunter.cyborgsecurity.io/research/hunt-package/E1FF5919-4CE6-4318-8C3F-55924D7AE4DC

Taskkill.exe executed multiple times in a short period

https://hunter.cyborgsecurity.io/research/hunt-package/219d9dd8-0ffb-4052-909e-8ba86a6db08c

Suspicious SOCKS Proxy Process Creation

https://hunter.cyborgsecurity.io/research/hunt-package/e1650196-ebc1-4dee-a65e-2fcaacf5255e

Process Commands Containing Single Character File Names With Execution Extension - Potential Malware Staging

https://hunter.cyborgsecurity.io/research/hunt-package/8d918fe0-b923-4dd7-8b15-d49ecd2f9e82

New Executable Created in SYSVOL or NETLOGON Directory

https://hunter.cyborgsecurity.io/research/hunt-package/7e2685a8-ddd3-4725-a84e-8b78e9311df4

Advanced IP Scanner Tool Utilization

https://hunter.cyborgsecurity.io/research/hunt-package/181b11a6-3391-4d98-aaab-a2544f03c2ef

RDP Enabled Via NETSH

https://hunter.cyborgsecurity.io/research/hunt-package/6322023c-8874-41f2-aa0b-c6600d47398c

Copyright © 2026 Intel 471, Inc. All Rights Reserved.

Scheduled Task Created

https://hunter.cyborgsecurity.io/research/hunt-package/aaa77f56-4a4c-4fdd-a6e3-156e1996d310

AnyDesk Silent Installation - Potential Malicious RMM Tool Installation

https://hunter.cyborgsecurity.io/research/hunt-package/11353A3B-797D-45BC-BA32-3D10F14EDC82

User Added to Default Privileged Windows Security Groups

https://hunter.cyborgsecurity.io/research/hunt-package/b6365ad5-0ccd-4426-97bc-b9484eb9579f

RDP Restricted Admin Mode Enabled - Registry Key Detection

https://hunter.cyborgsecurity.io/research/hunt-package/4cbffa4d-cbb5-45f2-86e4-591a065fc10e

AnyDesk Password Set Via CLI - Potential Malicious RMM Tool Installation

https://hunter.cyborgsecurity.io/research/hunt-package/8E0CF375-A8D7-46BD-B9B9-C7181B194706

Abnormal Execution of WebDav DLL via Rundll32 - Potentially Malicious Link or Exploitation

https://hunter.cyborgsecurity.io/research/hunt-package/062ae7c6-3e3d-401c-8797-1df3218f3e47

WinSCP Session Created - Possible Data Exfil

https://hunter.cyborgsecurity.io/research/hunt-package/acbe6ddb-8762-4af5-9d85-e644d7bcce44

Copyright © 2026 Intel 471, Inc. All Rights Reserved.

AnyDesk Service Installation - Potentially Malicious RMM Tool Installation

https://hunter.cyborgsecurity.io/research/hunt-package/4103B086-F093-4084-9125-15B9A6C872B8

Shadow Copies Deletion Using Operating Systems Utilities

https://hunter.cyborgsecurity.io/research/hunt-package/2e3e9910-70c1-4822-804a-ee9919b0c419

PowerShell Encoded Command Execution

https://hunter.cyborgsecurity.io/research/hunt-package/d2d3bbc2-6e57-4043-ab24-988a6a6c88db

Unusual Secrets Dump Processes - DonPAPI Activity

https://hunter.cyborgsecurity.io/research/hunt-package/e8b2ffcb-0f64-48c3-853e-5dd0a2be0eee

Windows Defender Tampering - Possible Malware Activity

https://hunter.cyborgsecurity.io/research/hunt-package/aa6e2535-e1e3-4f0f-80e4-68cc47fc2684

AnyDesk Execution from Abnormal Folder - Potential Malicious Use of RMM Tool

https://hunter.cyborgsecurity.io/research/hunt-package/93F71607-F35D-4AA6-AEC9-C2F8A62CBD8A

Copyright © 2026 Intel 471, Inc. All Rights Reserved.

THREAT SUMMARY

The Gentlemen ransomware operation emerged as a rapidly evolving ransomware threat observed throughout 2025, leveraging aggressive defense evasion techniques and multi-stage intrusion activity to compromise enterprise environments. Researchers have linked the group to campaigns targeting organizations across multiple regions across the globe including North America, Europe, and Asia, with observed victims spanning industries such as healthcare, manufacturing, technology, and professional services. The ransomware itself employs a double extortion model in which sensitive data is exfiltrated prior to encryption, allowing the attackers to pressure victims through both operational disruption and threats of public data exposure. It is worthy to note that the group demonstrates a high degree of operational maturity, utilizing stealth-focused tradecraft, remote administration tooling, and credential abuse techniques that closely resemble behaviors observed in other advanced ransomware ecosystems.

Over the past several months in 2026, the Gentlemen ransomware group has evolved from a relatively new operation into a more coordinated and technically sophisticated threat actor capable of conducting large-scale enterprise intrusions. Recent reported activity indicates the operators increased focus on weakening defensive tooling and establishing broad network visibility before encryption is executed, allowing them to maximize the impact of attacks and increase leverage during negotiations. The group's activity enables malicious actors to compromise domain infrastructure, steal sensitive organizational data, disable endpoint protections, and encrypt large portions of enterprise environments. Given the combination of stealth tactics, credential targeting, and widespread encryption capability, it is important to assess, understand, and prepare for this threat as it continues to evolve and expand globally.

Verity471 References:

Info Report: The Gentlemen ransomware, data extortion group internal chat leak reveals targeted entities

Info Report: The Gentlemen ransomware, data extortion group internal chat leak reveals tools and operational methods

Info Report: The Gentlemen ransomware, data extortion group internal chat leak reveals members and roles

Copyright © 2026 Intel 471, Inc. All Rights Reserved.

THREAT SYNOPSIS

At the outset, the Gentlemen ransomware operation has been observed leveraging compromised credentials (such as Cisco AnyConnect VPN, FortiClient VPN for example), exposed remote access services, and post-compromise tooling to establish initial access into victim environments. Researchers observed the group using legitimate administrative tools and living-off-the-land techniques to blend into normal enterprise activity while conducting reconnaissance and privilege escalation. During intrusion activity observed, the operators enumerate Active Directory environments, identify high-value systems, and target security tooling prior to ransomware deployment. It is also worthy to note that the group demonstrates an emphasis on defense evasion, with reports highlighting the abuse of tools and techniques designed to disable or interfere with endpoint protection solutions before encryption begins. The attackers have also been observed utilizing remote administration utilities and scripting frameworks to maintain access and facilitate lateral movement throughout compromised networks.

The ransomware deployment pathway involves broad encryption of local and network-accessible systems after the environment has been sufficiently prepared. Prior to encryption, the operators conduct data exfiltration activities to support double extortion operations, allowing them to threaten public release of sensitive information if ransom demands are not met. Reporting additionally highlights the use of credential dumping and privilege escalation methods that allow the attackers to gain elevated access and maximize encryption coverage across enterprise infrastructure. Once encryption begins, the ransomware impacts operational continuity by targeting critical systems and shared resources, while ransom notes are deployed to direct victims toward negotiation channels. The combination of credential abuse, stealth-focused intrusion activity, defense evasion, and mass encryption enables the Gentlemen ransomware group to compromise enterprise environments rapidly and create significant operational and financial disruption for affected organizations.

Copyright © 2026 Intel 471, Inc. All Rights Reserved.

MITRE CONTEXT

- MITRE Technique IDs:
  - T1112
  - T1543.003
  - T1059
  - T1053
  - T1090.003
  - T1219
  - T1059.001
  - T1078
  - T1048
  - T1133
  - T1134
  - T1105
  - T1566
  - T1562.004
  - T1136.002
  - T1021
  - T1212
  - T1570
  - T1555
  - T1021.001
  - T1018
  - T1204.001
  - T1036
  - T1074.001
  - T1027
  - T1572
  - T1562.001
  - T1555.004
  - T1071.001
  - T1218.011
  - T1490
  - T1127
  - T1078.003

Copyright © 2026 Intel 471, Inc. All Rights Reserved.

  - T1204.002
  - T1550.002

- MITRE Technique Names:
  - Windows Service
  - Command and Scripting Interpreter
  - Inhibit System Recovery
  - Masquerading
  - Disable or Modify System Firewall
  - Protocol Tunneling
  - Malicious File
  - External Remote Services
  - Rundll32
  - Remote Access Software
  - Malicious Link
  - Multi-hop Proxy
  - Exploitation for Credential Access
  - Pass the Hash
  - Access Token Manipulation
  - Disable or Modify Tools
  - Credentials from Password Stores
  - Lateral Tool Transfer
  - Obfuscated Files or Information
  - Remote System Discovery
  - PowerShell
  - Remote Desktop Protocol
  - Exfiltration Over Alternative Protocol
  - Trusted Developer Utilities Proxy Execution
  - Modify Registry
  - Web Protocols
  - Valid Accounts
  - Phishing
  - Local Data Staging
  - Local Accounts
  - Domain Account

Copyright © 2026 Intel 471, Inc. All Rights Reserved.

    - Ingress Tool Transfer
    - Scheduled Task/Job
    - Windows Credential Manager
    - Remote Services

- MITRE Tactic Names:
    - Discovery
    - Impact
    - Privilege Escalation
    - Initial Access
    - Command and Control
    - Exfiltration
    - Executio,
    - Collection
    - Lateral Movement
    - Persistence
    - Defense Evasion
    - Credential Access

Copyright © 2026 Intel 471, Inc. All Rights Reserved.

REFERENCES

1. https://www.trendmicro.com/en_us/research/25/i/unmasking-the-gentlemen-ransomware.html
2. https://www.huntress.com/blog/the-gentlemen-ransomware-defense-evasion-ttps
3. https://www.fortiguard.com/threat-actor/6387/the-gentlemen-ransomware
4. https://www.cybereason.com/blog/the-gentlemen-ransomware\u2028
5. https://www.halcyon.ai/ransomware-research-reports/threat-assessment-the-gentlemen-ransomware-group

STAY AHEAD OF THE THREAT

Looking to hunt these threats yourself? Join the HUNTER Community for free and get access to behavioral threat hunting content for your SIEM, EDR, NDR, and XDR platforms.

Get Your Free HUNTER Community Account

Copyright © 2026 Intel 471, Inc. All Rights Reserved.