Unmasking The Gentlemen Ransomware: Tactics, Techniques, and Procedures Revealed

Published: 2025-09-09 · Archived: 2026-04-05 16:22:50 UTC

Key takeaways

- The Gentlemen ransomware group launched a campaign involving advanced, highly tailored tools specifically designed to bypass enterprise endpoint protections.
- The campaign leveraged a combination of legitimate driver abuse, Group Policy manipulation, custom anti-AV utilities, privileged account compromise, and encrypted exfiltration channels.
- The group targeted multiple industries and regions, focusing heavily on a range of industries such as manufacturing, construction, healthcare, and insurance, with attacks spanning at least 17 countries.
- The Gentlemen show advanced capabilities by systematically compromising enterprise environments, using versatile tools from generic anti-AV utilities to targeted variants, highlighting serious threat to organizations despite security measures.
- The group also engineered ransomware deployment via privileged domain accounts and created evasion methods to persist against security controls.
- Trend Vision One™ detects and blocks the indicators of compromise (IOCs) described in this blog and equips customers with tailored hunting queries, threat intelligence, and actionable insights. Additional mitigation recommendations are outlined below.

Introduction

In August 2025, we investigated a new ransomware campaign orchestrated by The Gentlemen, an emerging and previously undocumented threat group. This threat actor quickly established itself within the threat landscape by demonstrating advanced capabilities through their systematic compromise of enterprise environments. By adapting their tools mid-campaign—shifting from generic anti-AV utilities to highly targeted, specific variants—the attackers demonstrate versatility and determination, posing a significant threat to organizations regardless of their security defenses.

The campaign’s attack chain exposed several highly sophisticated and concerning tactics. Notably, the threat actor exploited legitimate drivers for defense evasion, abused Group Policy Objects (GPO) to facilitate domain-wide compromise, and deployed custom malicious tools designed to disable security solutions present in the environment. The Gentlemen group demonstrated operational security practices by utilizing encrypted channels for data exfiltration via WinSCP and establishing redundant persistence mechanisms through both AnyDesk remote access software and modified registry settings.

Significance

The group's tactics, particularly their development of custom tools targeting specific security vendors, indicates an evolution in ransomware operations where attackers conduct extensive reconnaissance — resulting in tailored bypasses for the defenses they encounter. This approach represents a shift from opportunistic attacks; through systematic analysis of security software documentation, the threat actors combine this knowledge with the abuse of legitimate tools and vulnerable drivers to deploy environment-specific evasion techniques.

The Gentlemen's substantial victim count, coupled with the lack of prior threat intelligence suggests either a rebranding effort by experienced operators or the emergence of a well-funded new entrant within the ransomware ecosystem. By using threat intelligence on the group's methodologies, organizations can proactively identify their tools, tactics, and procedures (TTPs), implement targeted defensive measures, and prepare incident response plans aligned with these observed behaviors.

Victimology

The Gentlemen ransomware group has been targeting organizations across multiple sectors, with a particular focus on the Asia-Pacific region. The manufacturing industry has been the hardest hit, followed closely by construction, healthcare, and insurance. The group’s attacks on essential services such as healthcare highlights its disregard for critical infrastructure and its potential public safety implications. Key target countries include Thailand and the United States, with a total of 17 countries affected.

Initial Access

Although the exact initial access vector remains unconfirmed for this specific incident, our investigation suggests the threat actors likely exploited internet-facing services or compromised credentials to establish their initial foothold. The presence of

network reconnaissance tools (such as Advanced IP Scanner, shown below) early in the attack timeline, combined with evidence of systematic infrastructure mapping, indicates a calculated entry strategy rather than opportunistic exploitation. Following the initial compromise, the attackers carried out thorough reconnaissance via Advanced IP Scanner to gain knowledge of the network layout and identify valuable targets.

C:\Program Files (x86)\Advanced IP Scanner\advanced_ip_scanner.exe

Discovery

During the discovery phase, the threat actor examined Active Directory structures, focusing on domain administrators, enterprise administrators, and custom privilege groups such as *itgateadmin*.

One notable technique used by The Gentlemen involved the use of a batch script named *1.bat* to perform mass account enumeration, querying more than 60 user accounts across the domain infrastructure:

- *user admin.it /dom*
- *user administrator /dom*
- *user fortigate /dom*
- *group "domain admins" /dom*
- *group "Enterprise admins" /dom*
- *localgroup __vmware__*
- *localgroup administrators*
- *[additional net user commands]*

They also demonstrated extensive environmental awareness by querying local groups, including standard administrative groups and virtualization-specific groups such as *VMware*, indicating preparation for lateral movement across both physical and virtualized infrastructure components.

Defense Evasion

The group's initial defense evasion strategy centered on deploying *All.exe* in conjunction with *ThrottleBlood.sys*, leveraging a sophisticated technique previously documented in by other researchers in this report. This approach exploits a legitimate signed driver to perform kernel-level manipulation, effectively terminating security software processes by abusing Windows driver functionality. The tool operates by loading the vulnerable driver and using it to kill protected processes that would normally be shielded from termination:

- *$myuserprofile$\Downloads\All.exe → $myuserprofile$\Downloads\ThrottleBlood.sys*
-

Recognizing the limitations of this initial approach, the threat actors shifted tactics and began conducting detailed reconnaissance of the endpoint protection mechanisms in place. This allowed them to identify specific security controls and tailor their methods accordingly.

Next, they deployed *PowerRun.exe*, a legitimate tool frequently abused for privilege escalation. By leveraging *PowerRun.exe*, the attackers attempted to execute high-privilege operations, aiming to disable or terminate security-related services and processes.

Throughout this phase, the group demonstrated a targeted approach, adapting their techniques to the particular security solutions they encountered rather than relying solely on generic bypass methods.

After gathering sufficient information, the threat actors introduced an enhanced version of their defense evasion tool, *Allpatch2.exe*. This tool was specifically customized to neutralize key security agent components by targeting and terminating relevant processes. Their ability to modify evasion strategies based on the victim environment’s defenses highlights a high level of sophistication and adaptability.

Lateral Movement and Persistence

The threat actors leveraged PsExec for lateral movement, demonstrating proficiency in living-off-the-land techniques. They systematically weakened security controls by modifying critical registry settings that govern authentication and remote access protocols:

- *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*

To maintain persistent command-and-control (C&C) access, the threat actors relied on *AnyDesk*, creating a remote access channel resilient to traditional incident response actions. They further expanded their situational awareness by downloading, installing and executing *Nmap* for comprehensive internal network scanning:

- Downloaded NMAP: *C:\Users\fortigate\Downloads\nmap-7.97-setup.exe*
- *nmap -sV -T4 -O -F -oX C:\Users\FORTIG~1\AppData\Local\Temp\zenmap-7ii30x5l.xml --version-light <IP address>*

Critically, the *Nmap* output path revealed the compromise of a *FortiGate* administrative account, with network scans originating from this privileged context. This suggests the threat actors had compromised critical network security infrastructure, potentially granting them extensive visibility and control over network traffic. Our investigation confirmed that the *FortiGate* server was directly accessible from the internet, which likely served as the attackers' entry point into the network.

Additional evidence further indicates the possible use of *PuTTY* for Secure Shell (SSH)-based lateral movement, though the full scope of this tool's usage remains unclear.

Group Policy Manipulation

We've also observed the use of Group Policy Management Console *(gpmc.msc)* and Group Policy Management Editor *(gpme.msc)*, likely as part of an attempt to deploy malicious configurations across the domain:

- *"C:\Windows\System32\gpme.msc" /s /gpobject:"LDAP://<REDACTED>/cn<REDACTED>,cnpolicies,cnsystem,DC<REDACTED>,DClocal"*
-

The attacker also executed encoded PowerShell to identify critical domain infrastructure, with a particular focus on the Primary Domain Controller for potential high-impact operations:

- *C:\Windows\System32\cmd.exe → /Q /c powershell.exe -noni -nop -w 1 -enc IAAoAEcAZQB0AC0AQQBEAEQAbwBtAGEAaQBuACkALgBQAEQAQwBFAG0AdQBsAGEAdABvAHIA 1> \Windows\Temp\UDaYsR 2>&1*
  → ***(Get-ADDomain).PDCEmulator***
- *C:\Windows\System32\cmd.exe → /Q /c powershell.exe -noni -nop -w 1 -enc IABHAGUAdAAtAEEARABEAG8AbQBhAGkAbgAgAHwAIABTAGUAbABlAGMAdAAtAE8AYgBqAGUAYwB0ACAAUABEAEMARQBtAHUA 1> \Windows\Temp\IHQBeJ 2>&1*
  → ***Get-ADDomain | Select-Object PDCEmulator***

This level of Active Directory manipulation indicates preparation for domain-wide ransomware deployment or the establishment of persistent backdoor installation through GPO abuse.

Collection

The data staging portion of operation suggests what appears to be a methodical approach to information gathering. We found evidence suggesting possible data consolidation in *C:\ProgramData\data*, with hundreds of files being accessed. The presence of zone identifier streams could also indicate advanced collection methods, though alternative explanations cannot be ruled out:

- *C:\programdata\data\<REDACTED>.pdf:zone.identifier:$data*
- *[approximately 100 similar files]*

We observed several *WebDAV* connections to several internal resources throughout the compromise period. While these connections could potentially indicate an alternative data collection mechanism or preparation for distributed exfiltration, we would also like to note that *WebDAV* activity can also occur through legitimate business operations. Within the broader context of the compromise, however, these connections warrant scrutiny:

- *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$*
- *[approximately 50 different local networks and shares]*

Even though the timing and volume of these activities align with typical data staging behaviors observed in ransomware attacks, we present this analysis with moderate confidence pending additional forensic validation.

Exfiltration

Data exfiltration was likely carried out through *WinSCP*, a legitimate file transfer tool commonly abused by threat actors for its reliability and encryption capabilities. Our telemetry shows the transfer of sensitive internal documentation:

- *C:\ProgramData\data\INTERNAL\Summary<REDACTED> → "C:\ProgramData\WinSCP.exe"*
-

The choice of *WinSCP* suggests the attackers prioritized operational security, using encrypted channels to avoid detection by network monitoring solutions.

Impact

The ransomware was deployed throughout the domain's *NETLOGON* share, ensuring widespread distribution across all domain-joined systems. The payload was password-protected, likely to evade automated sandbox analysis:

- *\\<REDACTED>.local\NETLOGON\<REDACTED>.exe --password <8-byte key>*
-

Prior to encryption, the built-in Windows Defender was neutralized through PowerShell commands:

- *Set-MpPreference -DisableRealtimeMonitoring $true -Force*
- *Add-MpPreference -ExclusionProcess "C:\Windows\Temp\<REDACTED>"*

To ensure persistent access for negotiation and additional extortion activities, the following firewall rules were modified:

- *netsh firewall set service type remotedesktop mode enable*
-

Overall, the campaign highlights the threat actors' understanding of enterprise security architectures, demonstrated through adaptive countermeasures specifically tailored to overcome deployed security solutions, systematic data theft for double extortion, and the eventual successful deployment of ransomware using domain administrator privileges for maximum impact.

Ransomware analysis

The ransomware drops the following ransom note and appends the following extension:

- **README-GENTLEMEN.txt** - Ransom note containing victim ID and contact information
- **.7mtzhh** - File extension appended to each encrypted file

In terms of execution, the ransomware accepts specific parameters:

- **--password** (Required): 8-byte password parameter needed to execute the ransomware
- **--path** (Optional): Target path parameter for specifying custom encryption directory

The ransomware aggressively attempts to terminate key services commonly associated with backup, database, and security processes to maximize its impact:

net stop <service_name>*(.*)sql(.*), AcrSch2Svc, VSNAPVSS, MVarmor64, MVarmor, VeeamTransportSvc, VeeamDeploymentService, VeeamNFSSvc, AcronisAgent, QBIDPService, QBDBMgrN, QBCFMonitorService, OracleServiceORCL, MySQL, MSSQL, SAPHostExec, SAPHostControl, SAPD$, SAP$, postgresql, SAP, SAPService, GxFWD, GxVsshWProv, GXMMM, GxClMgr, MariaDB, GxCVD, GxClMgrS, GxVss, GxBlr, BackupExecRPCService, SQLAgent$SQLEXPRESS, BackupExecManagementService, BackupExecJobEngine, MSSQL$SQLEXPRESS, BackupExecDiveciMediaService, BackupExecAgentBrowser, SQLWriter, BackupExecAgentAccelerator, BackupExecVSSProvider, PDVFSService, SQLSERVERAGENT, WSBExchange, MSExchange\$, MSExchange, sophos, msexchange, docker, MSSQLSERVER, MSSQL*, Sql, vss, backup, veeam, memtas, mepocs, vmms*

Further, the threat systematically terminates processes using the following commands:

taskkill /IM <process_name>.exe /F*Veeam.EndPoint.Service.exe, mvdesktopservice.exe, VeeamDeploymentSvc.exe, VeeamTransportSvc.exe, VeeamNFSSvc.exe, EnterpriseClient.exe, DellSystemDetect.exe, avscc.exe, avagent.exe, sapstartsrv.exe, saposco.exe, saphostexec.exe, CVODS.exe, cvfwd.exe, cvd.exe, CVMountd.exe, tv_x64.exe, tv_w32.exe, pgAdmin4.exe, TeamViewer.exe, TeamViewer_Service.exe, SAP.exe, QBCFMonitorService.exe, pgAdmin3.exe, QBDBMgrN.exe, QBIDPService.exe, CagService.exe, vsnapvss.exe, raw_agent_svc.exe, cbInterface.exe, "Docker Desktop.exe", beserver.exe, pvlsvr.exe, bengien.exe, benetns.exe, vxmon.exe, bedbh.exe, IperiusService.exe, sqlceip.exe, xfssvccon.exe, wordpad.exe, winword.exe, visio.exe, thunderbird.exe, thebat.exe, Iperius.exe, psql.exe, postgres.exe,*

tbirdconfig.exe, synctime.exe, steam.exe, sqbcoreservice.exe, powerpnt.exe, cbVSCService11.exe, postmaster.exe, mysqld.exe, outlook.exe, oracle.exe, onenote.exe, ocssd.exe, ocomm.exe, ocautoupds.exe, SQLAGENT.exe, sqlwriter.exe, notepad.exe, mydesktopservice.exe, mydesktopqos.exe, mspub.exe, msaccess.exe, cbService.exe, sqlbrowser.exe, w3wp.exe, sql.exe, isqlplussvc.exe, infopath.exe, firefox.exe, excel.exe, encsvc.exe, Ssms.exe, DBeaver.exe, sqlservr.exe, dbsnmp.exe, dbeng50.exe, agntsvc.exe, vmcompute.exe, vmwp.exe, vmms.exe

Beyond service and process termination, the ransomware executes additional commands to impede recovery and forensic investigation:

- Deletes the Recycle Bin content: *cmd /C "rd /s /q C:\$Recycle.Bin"*
- Deletes Remote Desktop Protocol (RDP) log files: *cmd /C "del /f /q %SystemRoot%\System32\LogFiles\RDP**.*"*
- Deletes Windows Defender support files: *cmd /C "del /f /q C:\ProgramData\Microsoft\Windows Defender\Support*.*"*
- Deletes Prefetch files: *cmd /C "del /f /q C:\Windows\Prefetch*.*"*
- Adds C:\ to Windows Defender exclusion path: *powershell -Command "Add-MpPreference -ExclusionPath C:\ -Force"*
- Adds the {filename} of the ransomware to the Windows Defender exclusion process: *powershell -Command "Add-MpPreference -ExclusionProcess C:\Users\User\Desktop\{filename}.exe -Force*
- Disables Windows Defender real-time monitoring: *powershell -Command "Set-MpPreference -DisableRealtimeMonitoring $true -Force"*
- *wevtutil cl Security*
- *wevtutil cl Application*
- *wevtutil cl System*
- Deletes shadow copies:
- *wmic shadowcopy delete*
- *vssadmin delete shadows /all /quiet*

For final cleanup, the ransomware drops a batch script named after itself (e.g., *{filename}.exe.bat*). This script pings the local host for a brief delay, deletes the ransomware binary, and then deletes itself. This ensures comprehensive removal of its artifacts after the encryption routine is complete.

Conclusion

The Gentlemen ransomware campaign shows the rapid evolution of modern ransomware threats, blending advanced technical sophistication with persistent, targeted operations. This campaign is distinguished by its use of custom-built tools for defense evasion, its ability to study and adapt to deployed security software, and its methodical abuse of both legitimate and vulnerable system components to subvert layered enterprise defenses. By tailoring their tactics against specific security vendors, The Gentlemen have demonstrated an acute awareness of their targets' environments and a willingness to engage in in-depth reconnaissance and tool modification throughout the course of their operation.

The campaign's impact on critical infrastructure and use of double extortion techniques underscores the significant risk this threat actor poses to organizations. Their campaign illustrates the growing trend among ransomware operators to move beyond "one-size-fits-all" methods and toward highly customized attacks, raising the bar for detection, prevention, and incident response.

Organizations are strongly advised to review their security posture, focusing on proactive threat hunting for group-specific tools, tactics, and procedures, the strengthening of endpoint and network protections, and the continuous refinement of incident response strategies. Particular attention should be given to monitoring for anomalous administrative activity, the abuse of legitimate tools for lateral movement and privilege escalation, and early indications of defense evasion efforts targeting security solutions.

Defending against the Gentlemen attacks

Given the group's exploitation of internet-facing infrastructure and VPN appliances, Zero Trust controls are essential for preventing initial access and limiting blast radius. Organizations must eliminate direct RDP exposure to the internet, enforce multi-factor authentication for all administrative interfaces, and implement network segmentation between IT management tools and production systems. Enterprises should also implement virtual patching for known vulnerabilities in perimeter devices, particularly VPN concentrators and firewalls that THE GENTLEMEN has been observed targeting.

Essential access controls and monitoring include:

- Restricting domain controller share access and alerting on unauthorized NETLOGON modifications
- Auto-isolating devices showing indicators of driver-based attacks or anti-AV tool execution
- Implementing time-based access controls for privileged accounts with automatic de-escalation

- Monitoring for mass Active Directory queries and bulk group membership changes
- Deploying deception technologies on critical file shares to detect reconnaissance activities

The immediate priority is hardening endpoint security deployments against the group's documented process termination techniques. Organizations using Trend solutions should enable Tamper Protection with Anti-exploit Protection to prevent custom tools from terminating critical security processes. Additionally, password-protect agent uninstallation and activating Agent Self-Protection alongside Predictive Machine Learning in both pre-execution and runtime modes. These configurations specifically counter the group's attempts to disable security services before ransomware deployment.

Critical endpoint controls should include:

- Blocking execution from temporary and user download directories where attack tools are typically staged
- Monitoring service stop commands targeting security processes and alerting on mass termination attempts
- Implementing application control to restrict unauthorized remote access tools (RDP clients, file transfer utilities)
- Enforcing driver signature verification and alerting on vulnerable driver loading attempts
- Enabling behavioral detection for privilege escalation and credential dumping activities

Observed MITRE ATT&CK tactics, techniques, and procedures

Tactic	Technique	Description
Tactic	Technique	Description
Initial Access	T1190 - Exploit Public-Facing Application	Compromised FortiGate server and admin account via Nmap
	T1078.002 - Valid Accounts: Domain Accounts	Compromised domain accounts
Discovery	T1046 - Network Service Discovery	Nmap executed for service discovery
	T1018 - Remote System Discovery	Advanced IP Scanner used for network mapping
	T1087.002 - Account Discovery: Domain Account	Batch script querying multiple domain accounts
	T1069.002 - Permission Groups Discovery: Domain Groups	Enumeration of domain groups
	T1482 - Domain Trust Discovery	PowerShell commands used to identify PDC
Execution	T1059.003 - Command and Scripting Interpreter: Windows Command Shell	Used cmd.exe to execute different commands
	T1059.001 - Command and Scripting Interpreter: PowerShell	PowerShell commands used to deploy anti-av and ransomware
Defense Evasion	T1562.001 - Impair Defenses: Disable or Modify Tools	Stopped security services using Anti-AV tools
	T1014 - Rootkit	Deployed vulnerable driver for process termination
	T1112 - Modify Registry	Registry changes to weaken authentication
	T1562.004 - Impair Defenses: Disable or Modify System Firewall	Modified firewall settings for RDP access
	T1027 - Obfuscated Files or Information	Execution of base64 encoded PowerShell commands
Privilege Escalation	T1484.001 - Domain or Tenant Policy Modification: Group Policy Modification	GPO manipulation for domain-wide impact
Persistence	T1219 - Remote Access Software	Installed AnyDesk for remote access.

	T1112 - Modify Registry	Registry changes for persistence
Lateral Movement	T1021.002 - Remote Services: SMB/Windows Admin Shares	Used PSExec for lateral movement
	T1021.001 - Remote Services: Remote Desktop Protocol	Enabled RDP via registry modification
	T1021.004 - Remote Services: SSH	Used PuTTY for SSH movement
Collection	T1074.001 - Data Staged: Local Data Staging	Data staged in C:\ProgramData\data
	T1039 - Data from Network Shared Drive	WebDAV connections to internal shares
Command and Control	T1219 - Remote Access Software	AnyDesk used for C&C server
	T1071.001 - Application Layer Protocol: Web Protocols	WebDAV used for C&C server and data movement
Exfiltration	T1048.001 - Exfiltration Over Alternative Protocol: Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Data exfiltrated using WinSCP
Impact	T1486 - Data Encrypted for Impact	Ransomware deployed via NETLOGON share
	T1489 - Service Stop	Termination of security services

Proactive security with Trend Vision One™

Trend Vision One™ is the only AI-powered enterprise cybersecurity platform that centralizes cyber risk exposure management, security operations, and robust layered protection. This holistic approach helps enterprises predict and prevent threats, accelerating proactive security outcomes across their respective digital estate. With Trend Vision One, you're enabled to eliminate security blind spots, focus on what matters most, and elevate security into a strategic partner for innovation.

Trend Vision One™ Threat Intelligence

To stay ahead of evolving threats, Trend customers can access Trend Vision One™ Threat Insights, which provides the latest insights from Trend™ Research on emerging threats and threat actors.

Trend Vision One Threat Insights

- Emerging Threats: Dressed to Encrypt: The Gentlemen's Tailored Ransomware Campaign
-
- Trend Vision One Intelligence Reports (IOC Sweeping)
- Dressed to Encrypt: The Gentlemen's Tailored Ransomware Campaign

Hunting Queries

Trend Vision One customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post with data in their environment.

eventSubId: 106 AND processCmd: /--password\s+(\w{8})\b/ AND objectFilePath: .7mtzhh

eventSubId: 101 AND processCmd: /--password\s+(\w{8})\b/ AND objectFilePath: README-GENTLEMEN.txt

More hunting queries are available for Trend Vision One customers with Threat Insights Entitlement enabled.

Indicators of Compromise

SHA1	Detection name	Description
c12c4d58541cc4f75ae19b65295a52c559570054	Ransom.Win64.GENTLEMAN.THHAIBE	Ransomware
c0979ec20b87084317d1bfa50405f7149c3b5c5f	Trojan.Win64.KILLAV.THHBHBE	Initial KILLAV
df249727c12741ca176d5f1ccba3ce188a546d28	Trojan.Win64.KILLAV.THHBHBE	Patched KILLAV

e00293ce0eb534874efd615ae590cf6aa3858ba4	HackTool.Win32.PowerRun.THHBHBE	PowerRun

---