License to Encrypt: “The Gentlemen” Make Their Move

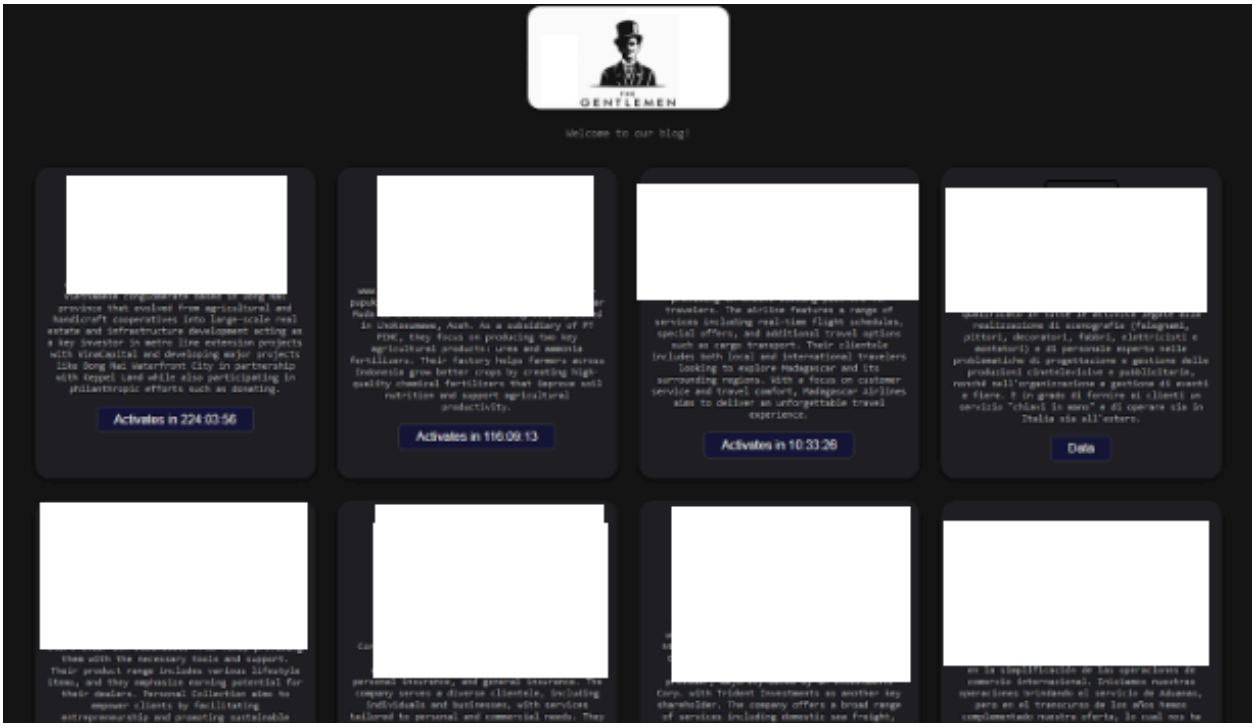
By Cybereason Security Services Team

Archived: 2026-04-05 12:55:44 UTC

Cybereason Threat Intelligence Team recently conducted an analysis of "The Gentlemen" ransomware group, which emerged around July 2025 as a ransomware threat actor group with relatively advanced methodologies. The Gentlemen group employs a dual-extortion strategy, not only encrypting sensitive files but also exfiltrating critical business data and threatening to publish it on dark web leak sites unless a ransom is paid. The group has demonstrated a unique approach by combining established ransomware techniques with newer strategies, making them quick to adapt to new attack vectors, allowing them to remain a persistent to evolving threat to organizations worldwide.

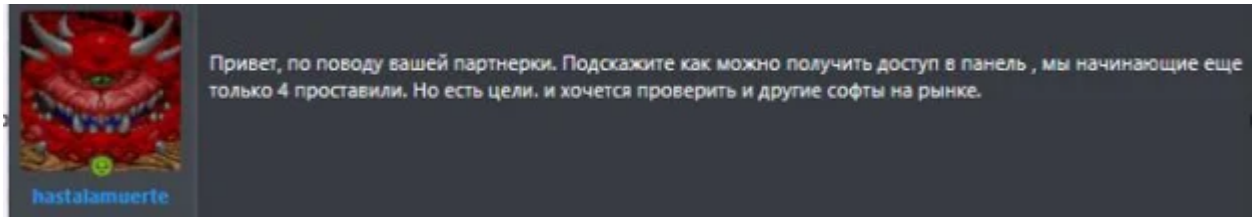
KEY points

Emergence of “The Gentlemen”: “The Gentlemen” ransomware group emerged around July 2025, and according to their data leak site activity, began the publication of 48 victims in September and October 2025.
They employ advanced dual-extortion tactics, encrypting data while also exfiltrating sensitive business information, threatening to release it unless a ransom is paid.



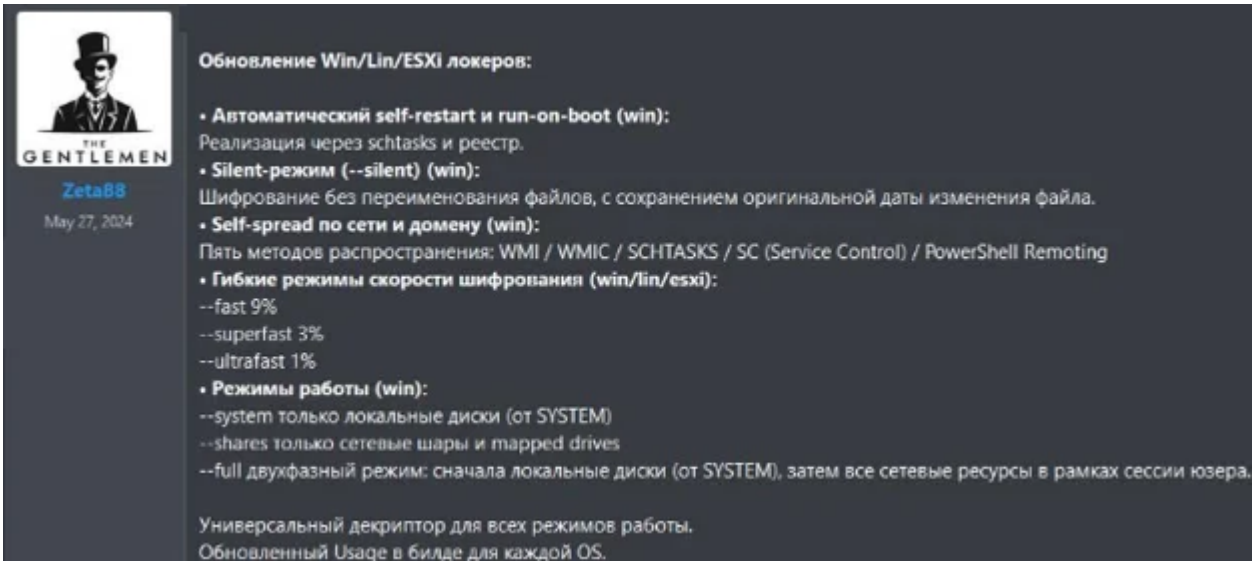
“The Gentlemen” DLS is Online

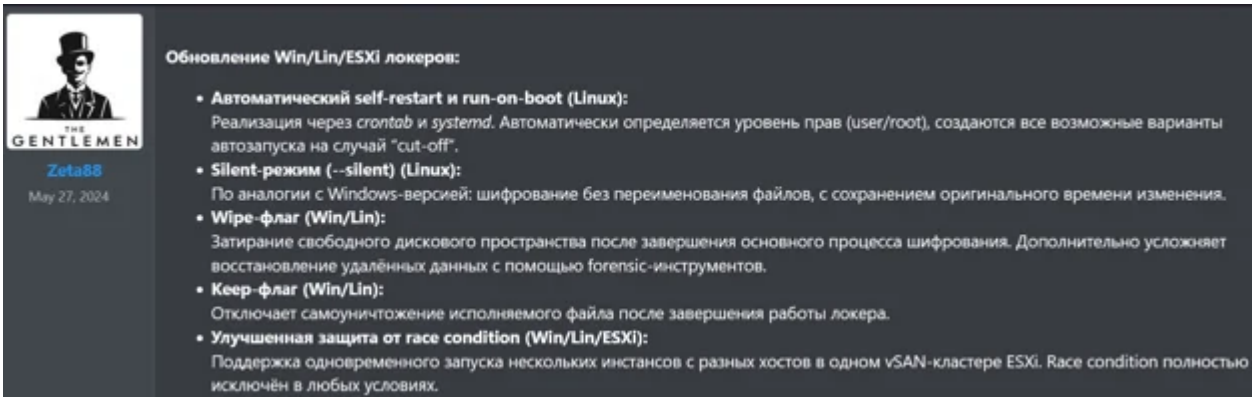
Development of RaaS and Affiliate Models: According to a statement from PRODAFT, before creating their own Ransomware-as-a-Service (RaaS) platform, “The Gentlemen” experimented with various affiliate models used by other prominent ransomware groups. This experience allowed them to refine their methods and eventually create their own RaaS operation.



Hastalamuerte (LARVA-368) was seeking access to the Qilin ransomware locker panel. They mention being new to the operations and express interest in exploring other ransomware software options on the market. This suggests that the user may have been considering or testing various RaaS platforms before eventually developing their own.

Latest Ransomware Update: The most recent update from The Gentlemen introduces advanced capabilities for automatic self-restart and run-on-boot functionality, enhancing their persistence on compromised systems. The ransomware also now supports flexible encryption speeds and distribution methods using WMI, PowerShell remoting, and other tools to propagate across networks. Additionally, it targets both local disks and network-shared drives, emphasizing the group's evolving approach to maintaining control and increasing the impact of their attacks.





The ransomware changelogs from the darknet forum

The group has released significant updates to its Win/Linux/ESXi locker variants, introducing improved automation, persistence, and encryption performance.

Persistence & Automation:
Implements automatic self-restart at run-on-boot, leveraging schtasks and registry entries.
Supports silent mode (-silent) for stealth execution.

Encryption Enhancements:
Encrypts both removable and mapped drives, while preserving original file modification dates.
Improved propagation techniques using WMI, SCHTASKS, SC (Service Control), and PowerShell Remoting.
Notable performance boost: encryption speed increased by 9–15%.

Execution Modes:
Can operate under SYSTEM privileges for full local disk access.
Supports dual operation: local + network encryption from the same session.

Target Scope:
Aimed at both physical and virtual Windows environments.
Support expanded for broader OS coverage.

Persistence & Privilege Escalation:
Now features automatic restart at boot on Linux via system-level autostart.
Capable of privilege escalation from user to root depending on configuration.

Silent Mode & Encryption:
Includes -silent execution mode for Linux systems.
Enhancements in file handling and timestamp preservation.
Uses a “wipe-after” mechanism to securely remove free disk space after encryption, complicating recovery.

Core-Locker Integration:
Modular architecture allows seamless execution post-encryption for cleanup tasks.

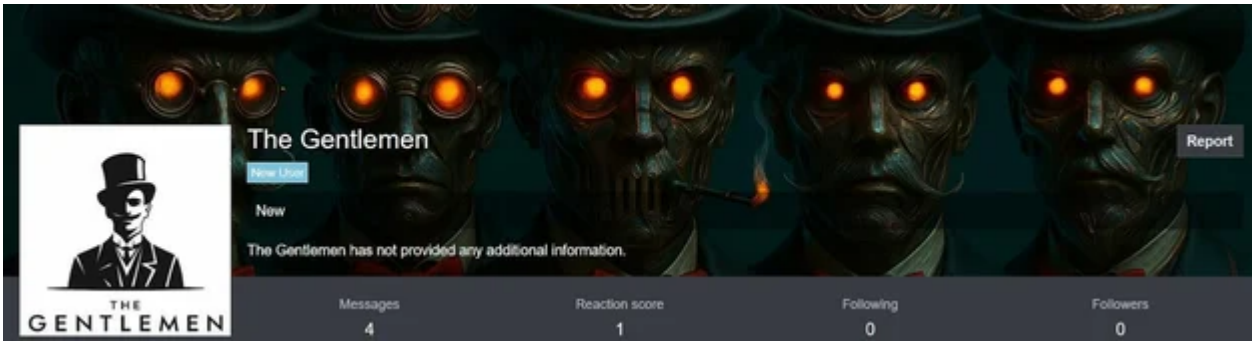
VMware/ESXi Focus:
Optimized for encrypting multiple ESXi instances across clustered hosts, including vSAN storage.
Improved concurrency to handle simultaneous operations across hypervisors.

The Gentlemen Ransomware-as-a-Service

On various cybercrime forums, “The Gentlemen” ransomware is promoted as an advanced Ransomware-as-a-Service (RaaS) solution, designed to offer highly configurable features tailored for a variety of attack scenarios. This RaaS program appeals to affiliates with its strong technical capabilities, providing them with versatile tools for large-scale deployments and efficient operations.

The Gentlemen ransomware combines advanced encryption techniques with dynamic propagation options, allowing operators to target and infect a broad range of systems, including Windows, Linux, and ESXi platforms. The service is continuously updated to adapt to new defense strategies, maintaining its relevance and effectiveness in a fast-evolving threat landscape.

Key capabilities include its powerful encryption mechanisms, specialized ESXi lockers, and persistent access features, including self-restart and run-on-boot functionality. Additionally, the group’s dual-extortion tactics—encrypting files while exfiltrating sensitive data for later release—are central to its operational strategy.



"The Gentlemen" accounts on dark web forums and X.

RaaS Capabilities:

Reliable Encryption: Uses XChaCha20 and Curve25519 for robust file encryption, ensuring secure data locking.

Configurable Attack Methods: The ransomware offers flexible encryption methods, allowing operators to adjust speed and thoroughness, optimizing attack outcomes.

ESXi Locker: A specialized locker designed for ESXi environments, providing asynchronous encryption and stealthy operations to avoid detection.

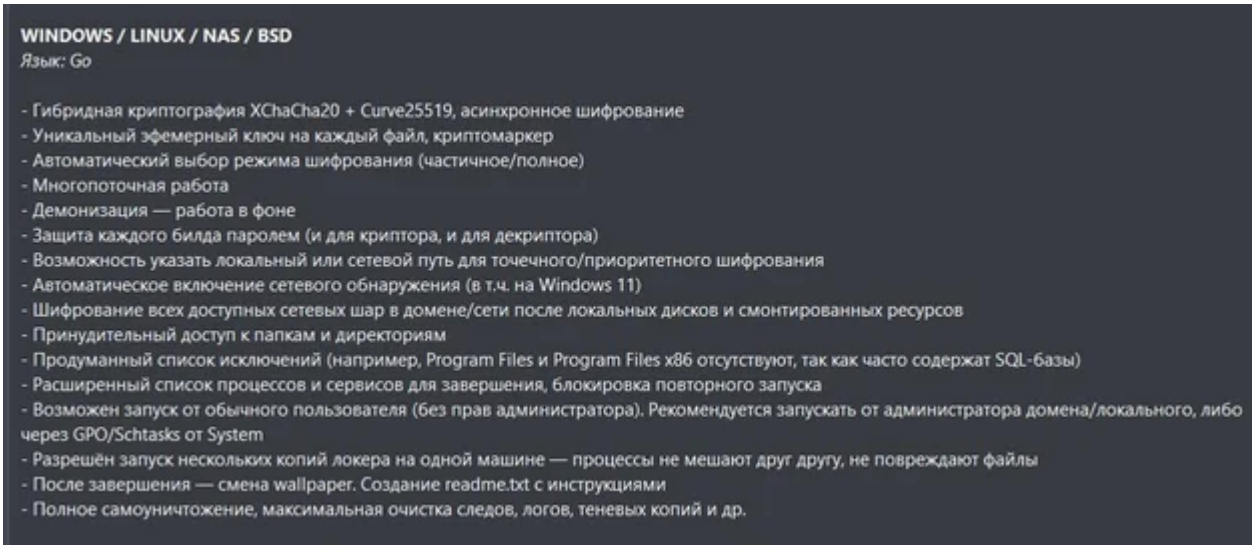
Dual-Extortion Tactics: Encrypts critical data while exfiltrating it for ransom demands. The group has published 47 victims on their dark web leak site within just two months of operation.

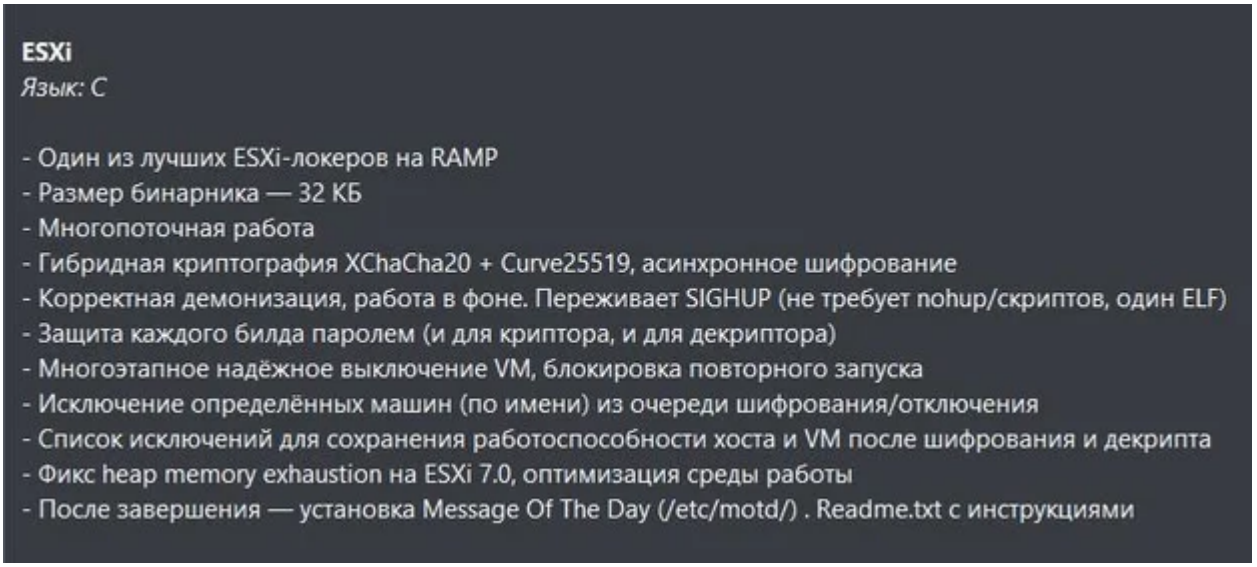
Persistence and Propagation: Employs self-restart and run-on-boot features to ensure continued access to compromised systems. The ransomware also spreads via WMI and PowerShell remoting, exploiting network-shared drives and credentials to expand its reach.

RaaS Model: Operates as a Ransomware-as-a-Service, allowing affiliates to deploy payloads while maintaining control over the infrastructure. The service includes customizable build options for affiliates and continuous support.

Below is detailed information on how The Gentlemen ransomware is offered as a Ransomware-as-a-Service (RaaS) and its key features.

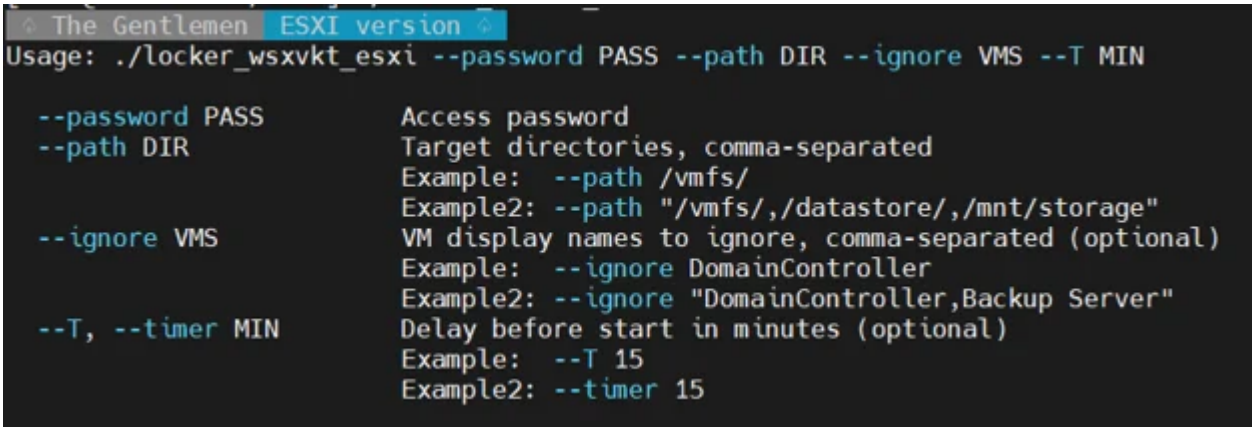
Briefly about the available functionality:



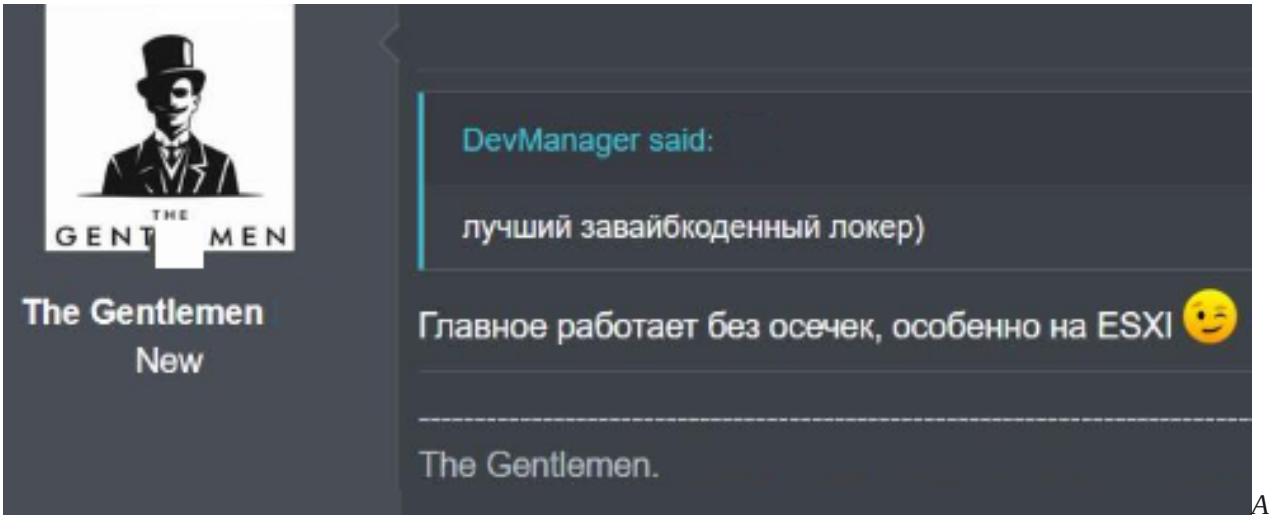


- **Reliable Encryption:** Uses XChaCha20 and Curve25519 for strong file encryption.
- **Configurable Encryption Modes:** Operators can adjust encryption methods for speed and depth, ensuring optimal performance.
- **Self-Persistence:** Ensures continued control over infected systems using self-restart and run-on-boot options.
- **Targeted Encryption:** Capable of encrypting specific directories or entire systems, including ESXi servers.
- **Dual-Extortion:** Exfiltrates sensitive data alongside encryption, threatening to release it unless the ransom is paid.
- **Network Propagation:** Uses WMI and PowerShell remoting to spread across local networks and gain access to additional systems.
- **Flexible Settings:** Offers a customizable build with both pre-configured and custom settings for affiliates to adapt their attack strategy.
- **Support for Affiliates:** The RaaS platform includes full support for negotiations and flexible control over ransom demands.
- **Geographic Restrictions:** Work is prohibited in Russia and CIS countries.

- **Data Collection:** Affiliates must upload encrypted data to a public cloud or approved resource, which will be displayed on the group's blog.
- **Security Features:** The program offers tools such as EDR-killer and the multi-chain system only to trusted affiliates.



"The Gentlemen" ESXI locker version



A forum user claimed that the locker used by "The Gentlemen" ransomware is written using 'vibecoding' techniques, while "The Gentlemen" seem to approve this statement.

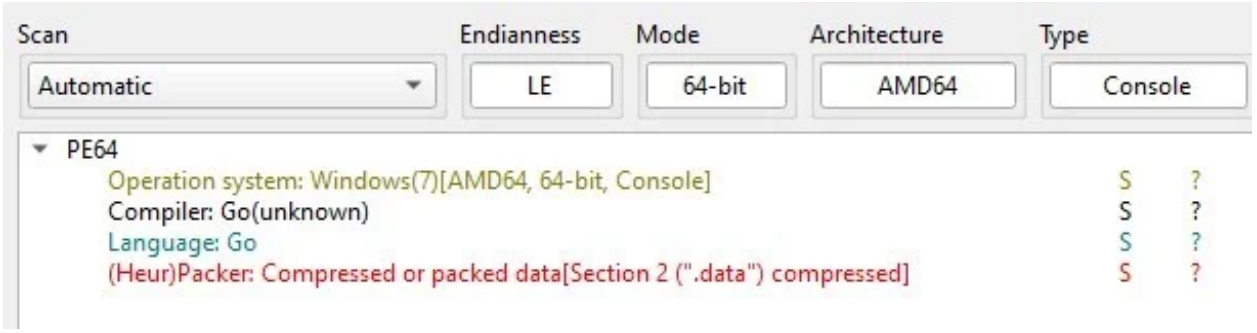
Technical Analysis

In this section, we performed an analysis of the ransomware executable file and observed the technique similarities with other ransomware groups that existed before.

The file hash is as follows:
3ab9575225e00a83a4ac2b534da5a710bdcf6eb72884944c437b5fbe5c5c9235

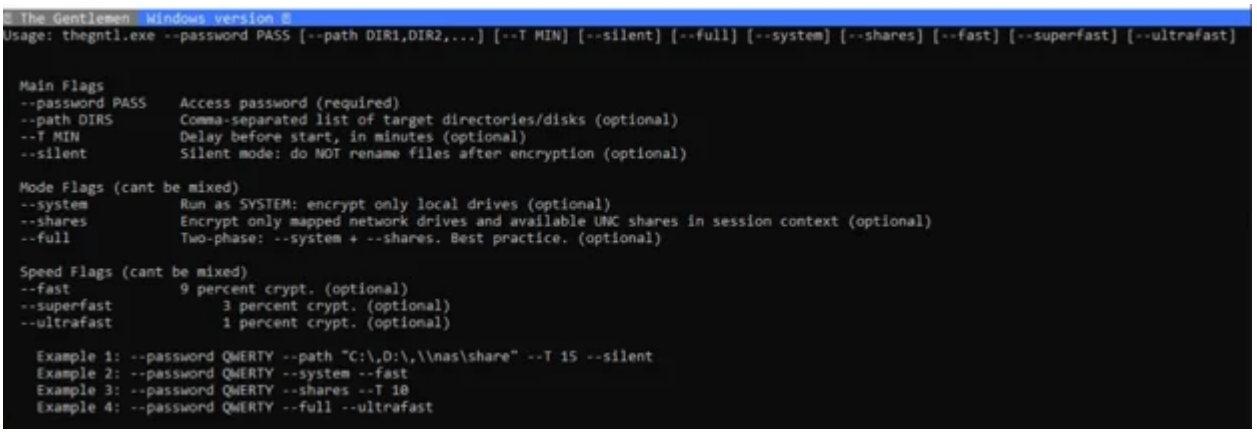
The Gentlemen (Windows, Go variant)

The file we analyzed is a 64bit Windows executable, written in Golang:



“Detect it Easy” analysis information

When launched, the ransomware executable provides an extensive help message, showing various options and flags available:



Windows Variant Command Line Options

The malware requires a “--password” argument to run the encryption routine. We assume that the argument is passed to the executable by a dropper or other kind of loader at the first step of infection.

The listed ransomware executable options are as follows:

Usage: %s --password PASS [--path DIR1,DIR2,] [--T MIN] [--silent] [--full] [--system] [--shares] [--fast] [--superfast] [--ultrafast]

Main flags:
--password PASS Access password (required)
--path DIRS Comma-separated list of target directories/disks (optional)
--T MIN Delay before start, in minutes (optional)
--silent Silent mode: do NOT rename files after encryption (optional) .

Mode flags:
--system (encrypt local drives as SYSTEM), --shares (map shares / UNC), --full (two-phase: system + shares).

Speed flags:
--fast (9% crypt), --superfast (3% crypt), --ultrafast (1% crypt).

Example invocations:

Example 1: --password QWERTY --path "C:\,D:\,\\nas\share" --T 15 --silent

Example 2: --password QWERTY --system --fast

Example 3: --password QWERTY --shares --T 10

Example 4: --password QWERTY --full --ultrafast .

A quick static analysis shows that the executable contains plaintext ransom note hardcoded:

```
.rdata:0000000000542D67                                         ; DATA XREF: .data:off_6BE180↓o
.rdata:0000000000542D93                 db 0Dh,0Ah
.rdata:0000000000542D95                 db 'Gentlemen, your network is under ou'
.rdata:0000000000542DB8 aRFullControlAl db 'r full control.',0Dh,0Ah
.rdata:0000000000542DC9                 db 'All your files are now encrypted and inaccessible.',0Dh,0Ah
.rdata:0000000000542DFD                 db 0Dh,0Ah
.rdata:0000000000542DFF                 db '1. Any mod'
.rdata:0000000000542E09 aIficationOfEnc db 'ification of encrypted files will make recovery impossible. ',0Dh
.rdata:0000000000542E46                 db 0Ah
.rdata:0000000000542E47                 db '2. Only our unique '
.rdata:0000000000542E5A aDecryptionKeyA db 'decryption key and software can restore your files. ',0Dh,0Ah
.rdata:0000000000542E90                 db '   Brute-force, RAM dumps, '
.rdata:0000000000542EAB aThirdPartyReco db 'third-party recovery tools are useless.',0Dh,0Ah
.rdata:0000000000542ED4                 db '   It’s a fundamental mathematical rea'
.rdata:0000000000542EFC aLityOnlyWeCanD db 'lity. Only we can decrypt your data.',0Dh,0Ah
.rdata:0000000000542F22                 db '3. Law enforcement, authorities, and “dat'
.rdata:0000000000542F4D aARecoveryCompa db 'a recovery” companies will NOT help you.',0Dh,0Ah
.rdata:0000000000542F79                 db '   They will only waste your time, ta'
.rdata:0000000000542F9E aKeYourMoneyAnd db 'ke your money, and block you from recovering your files – your bu'
.rdata:0000000000542FE1                 db 'siness will be'
.rdata:0000000000542FEF aLost4AnyAttemp db ' lost.',0Dh,0Ah
.rdata:0000000000542FF7                 db '4. Any attempt to restore systems, or refusal to negotiate, may l'
.rdata:0000000000543038                 db 'ead to i'
```

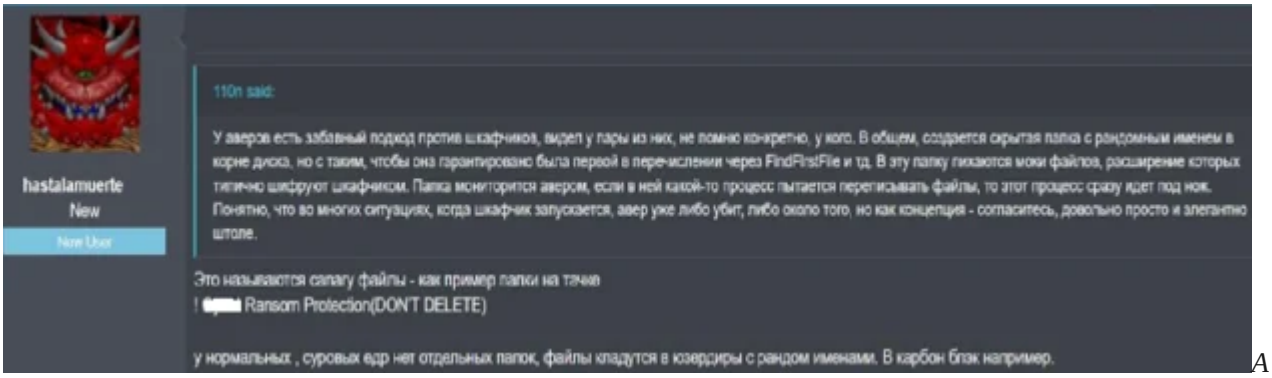
The Gentlemen Ransom Note

While performing the static analysis, we found a hardcoded string “ ! <...> Ransom Protection(DON’T DELETE)” in the sample:

```
}
puVar4 = (undefined8 *)FUN_00414440(&DAT_0051aaa0);
puVar4[1] = 0x26;
*puVar4 =
"crypto/sha256: invalid hash state sizeinvalid P256 compressed point encoding! -_ ~ Ransom Pr
otection(DON\'T DELETE)exec: environment variable contains NULmismatched count during itab tab
le copyout of memory allocating heap arena map/cpu/classes/gc/mark/assist:cpu-seconds/cpu/clas
ses/scavenge/total:cpu-seconds/memory/classes/profiling/buckets:bytesmspan.sweep: bad span sta
te after sweepruntime: blocked write on free polldescPowerRegisterSuspendResumeNotification"
;
auVar6._8_8_ = puVar4;
auVar6._0_8_ = &PTR_DAT_0056a940;
```

Decompiled code segment from the Gentlemen ransomware sample showing the embedded string “ ! <...> Ransom Protection(DON’T DELETE)”

After researching, Cybereason Threat Intelligence Team identified a forum post by a user “Hastalamuerte” that discussed the same marker present in “The Gentlemen” sample, while describing its relation to anti-ransomware functionality.



A forum post shared by a user operating under the alias “hastalamuerte” discusses the string “ ! <...> Ransom Protection(DON’T DELETE)” as an example of anti ransomware protection and bypass solutions.

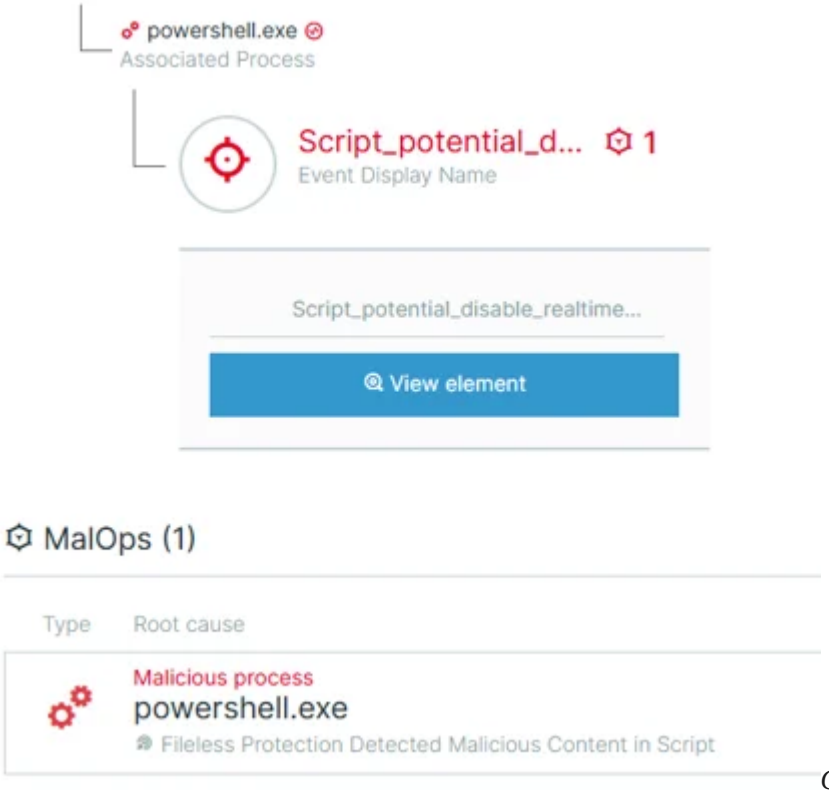
“The Gentlemen” PowerShell Operation

In this section we analyze the PowerShell commands executed by the ransomware.

The sample includes a PowerShell command designed to execute remotely via Invoke-Command:

```
Invoke-Command -ComputerName %s -ScriptBlock { Set-MpPreference -DisableRealtimeMonitoring $true; Ad
```

The command disables Windows Defender’s real-time protection and adds both directory (C:\) and process to the exclusions, a common tactic used by ransomware to evade detection before encryption.



Cybereason detection of malicious PowerShell command execution

Other commands executed by the ransomware include:

```
Write-Host " ♘ The Gentlemen " -BackgroundColor DarkGray -ForegroundColor White -NoNewline
```

This command prints the string "♘ The Gentlemen" to the console with custom colors, serving as a visual identifier or branding element for the ransomware during execution.

```
Get-NetFirewallRule -DisplayGroup "Network Discovery" | Enable-NetFirewallRule
```

This command enables Windows Firewall rules in the "Network Discovery" group, effectively opening discovery and file-sharing related ports.

```
AppData/Roaming/Microsoft/Windows/PowerShell/PSReadline/ConsoleHost_history.txt
```

This path points to the PowerShell PSReadLine history file (ConsoleHost_history.txt), which can contain a record of executed PowerShell commands and is a valuable forensic artifact for reconstructing attacker activity.

```
del /f /q %SystemRoot%\System32\LogFiles\RDP*\*.*
del /f /q C:\ProgramData\Microsoft\Windows Defender\Support\*.*
del /f /q C:\Windows\Prefetch\*.*
```

These commands are explicit anti-forensics actions that erase evidence of interactive access, endpoint protection telemetry, and application execution history, making post-incident investigation and timeline reconstruction far more difficult.

Cybereason detection of log removal

```
ping localhost -n 3 > nul & del
```

Malware removes itself from the system after execution.

```
$p = [WMICLASS]"\\\\%s\root\cimv2:Win32_Process"; $p.Create("%s")
```

This PowerShell snippet uses the WMI Win32_Process class to remotely create a process on \\<host>\root\cimv2, enabling adversaries to execute commands on other machines for lateral movement or distributed execution.

```
 $volumes=@();$volumes+=Get-WmiObject -Class
Win32_Volume|Where-Object{$_.Name -like '*:\*'}|Select-Object
-ExpandProperty
Name;try{$volumes+=Get-ClusterShare
dVolume|ForEach-Object{$_.SharedVolumeInfo.FriendlyVolumeName}}catch{};$volumes
```

This PowerShell snippet enumerates local drive volumes (Win32_Volume) and attempts to include Cluster Shared Volumes (Get-ClusterSharedVolume), collecting their names into $volumes, a routine used to discover all potential targets (local, clustered, and network-mounted volumes) before performing broad encryption or selective exclusion.

```
icacls <path> /grant *S-1-1-0:(OI)(CI)F
```

The ICACLS command in Windows is used to modify file and directory permissions. This command grants full control to the Everyone group (represented by the S-1-1-0 security identifier) for the specified folder and all its contents, including subfolders and files. The (OI) and (CI) flags ensure that the permissions apply to both files (Object Inherit) and subdirectories (Container Inherit).

Targeted Processes and Services

The Gentlemen ransomware contains a built-in kill list designed to stop critical services and processes before encryption. These include database engines, backup utilities, remote-access tools, and virtualization services components that could otherwise block file access or enable recovery.

Processes and services referenced:

sqlservr, MSSQL, MSSQL$SQLEXPRESS, SQLAGENT, SQLWriter, Ssms, postgres, postmaster, psql, postgresql, MySQL, mysqld, veeam, GxVss, vsnapvss, xfssvccon, qbdbMgrN, TeamViewer, MSExchange, vmms, and other processes and services.

Registry Keys Usage

The sample embeds multiple Windows registry references that point to both persistence and system-configuration manipulation. Notably, it contains HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run and HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run (common autorun locations used for persistence), HKLM\SYSTEM\CurrentControlSet\Control\Lsa (security/authentication-related settings), and HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters (server/SMB share configuration). It also references SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones, which may be read for localization/timestamp handling. Taken together, these registry touches indicate the malware programs for persistence, security policy interaction, and network-share behaviour modification in support of large-scale encryption.

Conclusion

Cybereason's analysis shows that "The Gentlemen" is a highly adaptive, fast-moving ransomware operation that blends mature ransomware techniques with RaaS features, dual-extortion, cross-platform (Windows/Linux/ESXi) lockers, automated persistence, flexible propagation, and affiliate support, allowing it to scale attacks and evade basic defenses quickly. Its rapid victim publication, powerful encryption (XChaCha20/Curve25519), EDR-evasion tactics and tooling for lateral movement make it a credible and persistent risk to organizations.

Recommendations:

- Follow and hunt "The Gentlemen" Locker affiliate activity in order to identify pre-ransomware behaviors
- Promote cybersecurity best practices such as multifactor authentication and patch management.
- Regularly backup files and create a backup process and policy: Restoring your files from a backup is the fastest way to regain access to your data
- Keep systems fully patched: Make sure your systems are patched in order to mitigate vulnerabilities
- If nefarious activity is detected, immediately involve Incident Response services to execute a thorough investigation and containment process in order to fully eliminate the threat actor from the infected network
- For Cybereason customers on the Cybereason Defense Platform:
    - Enable Anti-Malware and set the Anti-Malware > Signatures mode to Prevent, Quarantine, or Disinfect
    - Enable Anti-Ransomware (PRP), set Anti-Ransomware to Quarantine mode and enable shadow copy protection.
    - Enable Application Control
    - Enable Variant Payload Prevention with prevent mode on Cybereason Behavioral execution prevention.

IOC	IOC type	Description
3ab9575225e00a83a4ac2b534da5a710bdcf6eb72884944c437b5fbe5c5c9235	SHA256	Windows Ransomware Sample
51b9f246d6da85631131fcd1fabf0a67937d4bdde33625a44f7ee6a3a7baebd2	SHA256	Windows Ransomware Sample

Tactic	ATT&CK Technique (ID)

TA0002: Execution	T1059.001 – Command and Scripting Interpreter: PowerShell T1569.002 – System Services: Service Execution
TA0003-Persistence	T1547.001 – Registry Run Keys / Startup Folder
TA0005-Defense Evasion	T1070.004 – Indicator Removal on Host: File Deletion T1070.001 – Indicator Removal on Host: Clear Windows Event Logs T1562.001 – Impair Defenses: Disable or Modify Security Tools T1562 – Impair Defenses T1222 – File and Directory Permissions Modification T1218 – System Binary Proxy Execution (use of trusted Windows utilities such as vssadmin, wevtutil, and taskkill)
TA0007: Discovery	T1083 – File and Directory Discovery T1135 – Network Share Discovery T1018 – Remote System Discovery
TA0008: Lateral Movement	T1047 – Windows Management Instrumentation (WMI) T1021.002 – Remote Services: SMB/Windows Admin Shares
TA0040: Impact	T1486 – Data Encrypted for Impact T1489 – Service Stop T1490 – Inhibit System Recovery

About The Researcher

Mark Tsipershtein, Security Researcher

 Mark Tsipershtein, a security researcher at the Cybereason Security Research Team, focuses on research, analysis automation and infrastructure. Mark has more than 20 years of experience in SQA, automation, and security research.

Source: https://www.cybereason.com/blog/the-gentlemen-ransomware