TLP: CLEAR

Pesquisa de Cibersegurança

The Gentlemen - Análise do Grupo de Ransomware

heimdall
security research

Acesse nossa comunidade no WhatsApp, clicando na imagem abaixo!

heimdall
security research
A DIVISION OF ISH

Acesse a inteligência que produzimos sobre as Táticas, Técnicas e Procedimentos de determinados *Threat Actors*, análises de *malwares* emergentes no cenário de cibersegurança, análises de vulnerabilidades críticas e outras informações no *blog* da ISH Tecnologia, clicando na imagem abaixo.

ISH

ALERTA HEIMDALL! HTTP2 RAPID RESET_IMPACTOS E DETECÇÃO DA CVE-2023-44487

Falhas de negação de serviço (DoS) não são apenas interrupções técnicas. Elas representam riscos reais à continuidade do negócio, à confiança dos clientes e à reputação da marca. Nisto temos a vulnerabilidade CVE-2023-44487, conhecida como HTTP/2 Rapid Reset.

BAIXAR

ISH

ALERTA HEIMDALL! BABUK2 EM 2025: RETORNO LEGÍTIMO OU COPYCAT ESTRATÉGICO

O cenário de ransomware manteve-se ativo em 2024 e se estendeu para este ano de 2025, com diversos grupos realizando ataques a uma ampla gama de organizações, setores e com surgimento de novos grupos. Nesse contexto, temos o ransomware Babuk2.

BAIXAR

ISH

ALERTA HEIMDALL! A ANATOMIA DO RANSOMWARE AKIRA E SUA EXPANSÃO MULTIPLATAFORMA

O cenário de ransomware manteve-se ativo em 2024 e se estendeu para este ano de 2025, com diversos grupos realizando ataques a uma ampla gama de organizações, setores e ganhando bastante popularidade. Nesse contexto, temos o ransomware Akira.

BAIXAR

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1. INTRODUÇÃO EXECUTIVA

Este relatório fornece uma análise abrangente do grupo de *ransomware* "**The Gentlemen**", um ator de ameaça que emergiu em meados de 2025 e rapidamente se estabeleceu como uma operação de *Ransomware-as-a-Service* (**RaaS**) sofisticada e de alto volume. O grupo emprega um modelo de dupla extorsão, combinando a criptografia de sistemas com a exfiltração e ameaça de publicação de dados sensíveis.

Notável por sua maturidade técnica e abordagem metódica, *The Gentlemen* utiliza um arsenal de ferramentas personalizadas, explora ativamente vulnerabilidades de "*Bring Your Own Vulnerable Driver*" (**BYOVD**) e demonstra uma capacidade de adaptação em tempo real às defesas do ambiente de suas vítimas. Com um alcance global e um foco em setores críticos, o grupo representa uma ameaça significativa e crescente para organizações em todo o mundo.

2. PERFIL DO GRUPO E IDENTIDADE

The Gentlemen foi observado pela primeira vez em campanhas ativas por volta de agosto de 2025. O grupo cultiva uma identidade de marca polida, inspirada no filme de ***Guy Ritchie*** de mesmo nome, o que, juntamente com sua rápida ascensão e disciplina operacional, sugere que pode ser uma reformulação de operadores experientes ou uma nova equipe bem financiada.

Operando um modelo **RaaS**, o grupo recruta ativamente afiliados em fóruns da *dark web*, oferecendo uma **divisão de receita de 90%** e controle sobre as negociações com as vítimas, enquanto os operadores mantêm o controle centralizado da infraestrutura, como o site de vazamento de dados. As comunicações são gerenciadas principalmente através do *messenger* criptografado **Tox**, com um **ID** público divulgado para negociações.

3. VITIMOLOGIA E ALVOS

Até o momento, *The Gentlemen* já reivindicou **mais de 140 vítimas** em escala global, indicando expansão contínua de sua atividade. As ocorrências estão distribuídas internacionalmente, sem evidência pública de segmentação geográfica específica. Os Estados Unidos concentram o maior número de casos observados, seguidos por Tailândia, **Brasil**, Índia e França.

O direcionamento por setor indica maior incidência em ambientes onde a interrupção das operações pode gerar impacto relevante. Manufatura e tecnologia concentram o maior número de casos observados, seguidos por serviços financeiros e saúde.

Distribuição Geográfica Global

Figura 1 - Distribuição geográfica

Atividade do Grupo

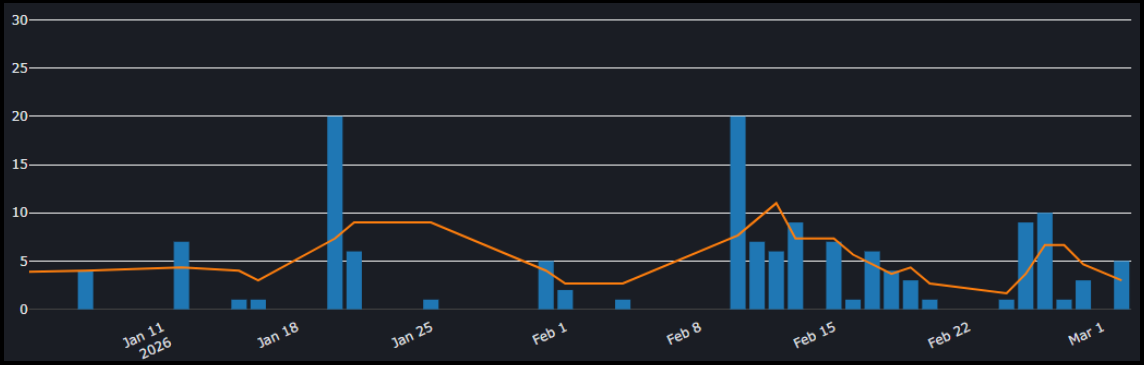

Figura 2 - The Gentlemen atividade

Posição	Top 5 Países Alvo	Top 5 Setores Alvo
1º	Estados Unidos	Manufatura
2º	Tailândia	Tecnologia
3º	Brasil	Serviços Financeiros
4º	Índia	Saúde
5º	França	Transportes/Logística

Tabela 1 - top alvos e setores

4. TÁTICAS, TÉCNICAS E PROCEDIMENTOS (TTPS)

O grupo *The Gentlemen* emprega uma cadeia de ataque simplificada, porém altamente eficaz, caracterizada por ferramentas adaptativas. Sua metodologia reflete uma mudança de ataques oportunistas para campanhas meticulosamente planejadas e direcionadas.

Acesso Inicial: O vetor de entrada principal é a exploração de serviços expostos à *internet*, como *appliances* de **VPN** e *firewall* (por exemplo, ***FortiGate***), ou o **uso de credenciais administrativas comprometidas**.

Reconhecimento e Descoberta: Uma vez dentro da rede, os operadores utilizam ferramentas como ***Advanced IP Scanner*** e ***Nmap*** para mapeamento de rede. Eles realizam uma extensa enumeração do ***Active Directory*** usando *scripts* em lote personalizados para identificar contas privilegiadas e a topologia do domínio.

Evasão de Defesa e Escalação de Privilégios: Esta é uma área de grande força para o grupo. Eles empregam uma técnica de *"Bring Your Own Vulnerable Driver"* (**BYOVD**), abusando de um *driver* legítimo e assinado (***ThrottleStop.sys***, renomeado para ***ThrottleBlood.sys***) que contém a vulnerabilidade **CVE-2025-7771** para obter privilégios em nível de *kernel* e terminar processos de soluções de segurança (**EDR/AV**). Ferramentas legítimas como **PowerRun.exe** são usadas para contornar o Controle de Conta de Usuário (**UAC**) e executar processos com privilégios de ***SYSTEM***.

Movimentação Lateral e Persistência: O movimento lateral é predominantemente alcançado usando **PsExec** sobre compartilhamentos administrativos **SMB**. A persistência é estabelecida através da instalação de software de acesso remoto

como o ***AnyDesk*** e modificações no registro para enfraquecer a autenticação e habilitar o **RDP**.

Exfiltração e Impacto: Antes da criptografia, dados sensíveis são coletados e exfiltrados usando canais criptografados, como **SFTP** via **WinSCP**, para evitar a detecção. O *ransomware*, escrito principalmente em **Go** com variantes para ***Windows***, ***Linux*** e **ESXi**, é então implantado de forma centralizada através de Objetos de Política de Grupo (**GPO**) e compartilhamentos ***NETLOGON***. O *malware* requer um parâmetro de senha para execução, uma medida anti-análise, e realiza a auto-exclusão após a conclusão para apagar seus rastros.

5. Capacidades do Binário

5.1 Comportamento em Runtime e Manipulação do Host

A análise dinâmica do artefato evidencia múltiplas capacidades ofensivas. A cadeia de processos gerada pela amostra revelou uma série de ações coordenadas para evasão de defesa, remoção de mecanismos de recuperação e maximização do impacto da criptografia.

Abaixo, as capacidades observadas são categorizadas conforme o ***framework*** **MITRE ATT&CK**.

T1562.001 - Impair Defenses: Disable or Modify Tools

O *ransomware* realiza a desativação do *Windows Defender* e adiciona exclusões para evitar detecção e bloqueio durante a execução.

```
powershell -Command "Set-MpPreference -DisableRealtimeMonitoring $true -Force"
powershell -Command "Add-MpPreference -ExclusionProcess
C:\Users\<user>\Desktop\gentle.exe -Force"
powershell -Command "Add-MpPreference -ExclusionPath C:\ -Force"
```

T1070.001 - Indicator Removal: Clear Windows Event Logs

O artefato executa a limpeza dos *logs* de eventos do *Windows*, removendo rastros da atividade maliciosa.

```
wevtutil cl Security
wevtutil cl Application
wevtutil cl System
```

T1490 - Inhibit System Recovery

São removidas cópias de sombra do sistema, impedindo a recuperação de arquivos.

```
wmic shadowcopy delete
vssadmin delete shadows /all /quiet
```

T1489 - Service Stop

O *ransomware* interrompe serviços críticos utilizando o comando **net stop <serviço>**, visando encerrar aplicações relacionadas a banco de dados, *backup*, virtualização e aplicações corporativas, desbloqueando arquivos em uso antes da criptografia.

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

T1562.001 - Terminate Processes

É realizado o encerramento forçado de processos por meio do comando **taskkill /IM <processo> /F**, com o objetivo de liberar arquivos em uso e maximizar o impacto da criptografia.

```
vmms.exe; vmwp.exe; vmcompute.exe; agntsvc.exe; dbeng50.exe; dbsnmp.exe; sqlservr.exe; encsvc.exe; excel.exe; firefox.exe; infopath.exe; isqlplussvc.exe; sql.exe; w3wp.exe; msaccess.exe; mspub.exe; mydesktopqos.exe; mydesktopservice.exe; notepad.exe; sqlwriter.exe; ocautoupds.exe; ocomm.exe; ocssd.exe; onenote.exe; oracle.exe; outlook.exe; mysqld.exe; powerpnt.exe; sqbcoreservice.exe; steam.exe; synctime.exe; tbirdconfig.exe; postgres.exe; thebat.exe; thunderbird.exe; visio.exe; winword.exe; wordpad.exe; xfssvccon.exe; bedbh.exe; vxmon.exe; benetns.exe; bengien.exe; pvlsvr.exe; beserver.exe; "Docker Desktop.exe"; raw_agent_svc.exe; vsnapvss.exe; CagService.exe; QBIDPService.exe; QBDBMgrN.exe; QBCFMonitorService.exe; SAP.exe; TeamViewer_Service.exe; TeamViewer.exe; tv_w32.exe; tv_x64.exe
```

T1070.004 - Indicator Removal on Host: File Deletion

O *ransomware* realiza a exclusão de arquivos e artefatos do sistema por meio do comando **del /f /q**, incluindo diretórios sensíveis (como *Prefetch*) e o próprio executável. O objetivo é dificultar a análise forense e remover vestígios da execução no *host* comprometido.

```
cmd /C "del /f /q C:\Windows\Prefetch\*.*"
cmd /C "del /f /q C:\Pro
```

Ao final do processo de criptografia, o *ransomware* cria e executa um *script* **.bat** responsável por remover o próprio executável do sistema. O *script* utiliza um pequeno atraso (**ping 127.0.0.1**) para garantir que o processo principal seja finalizado antes da exclusão.

```
@echo off
ping 127.0.0.1 -n 3 > nul
del /f /q "C:\Users\<user>\Desktop\gentle.exe"
del /f /q "%!~(MISSING)f0"
```

5.2 Lógica Interna e Mecanismos de Evasão

A análise do binário **THE GENTLEMEN** revelou um nível de sofisticação focado em impedir a análise automatizada e garantir a persistência silenciosa. Escrito em **Go**, o artefato utiliza estruturas complexas de *runtime* que, somadas à proteção comercial **VMProtect**, virtualizam funções críticas, elevando a dificuldade de sua análise.

5.2.1 Reconstrução de Memória e Desofuscação

Para contornar a camada de virtualização inicial, foi realizado um *process dump* em tempo de execução, resultando em um binário descompactado em memória que expandiu de **14MB** para **25MB**. Embora a ofuscação permaneça presente no artefato despejado, o uso do **GoReSym** possibilitou a extração de informações relacionadas ao *runtime* e a recuperação parcial de símbolos associados a componentes da biblioteca padrão. Essa etapa, embora não tenha simplificado totalmente a análise devido à complexidade das sub-rotinas customizadas, forneceu elementos auxiliares relevantes para a compreensão da estrutura interna do binário.

5.2.2 Mecanismo de Trava de Execução

Identificamos uma rotina crítica de validação. O *ransomware* implementa uma técnica de ***Malware Keying***, onde a carga útil permanece inerte a menos que receba um parâmetro específico via linha de comando.

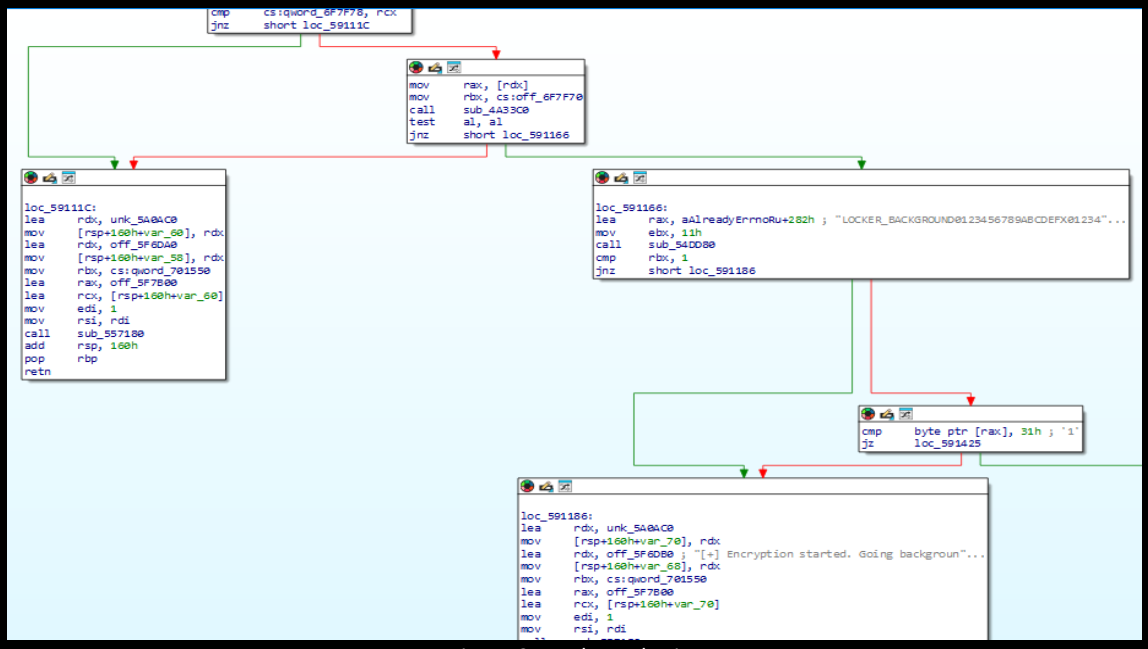

Figura 3 - Malware keying

A instrução **cmp qword_6f7f78, rcx** realiza uma comparação estrita **de 8 bytes**.

- **Fluxo Positivo:** Caso a senha coincida, o *malware* prossegue para a orquestração da carga útil.

```
C:\Users\[redacted]\Desktop>gentle.exe --password [redacted]
[+] Encryption started. Going background...
```

Figura 4 - Execução validada

- **Fluxo Negativo (Evasão):** Qualquer divergência resulta no salto condicional para uma rotina de encerramento imediato com a mensagem ***bad args***.

```
C:\Users\[redacted]\Desktop>gentle.exe --password 7Go2C10r
bad args
```

Figura 5 - Execução inválida

Este mecanismo é projetado especificamente para derrotar *Sandboxes* de Análise Automática, que tipicamente executam amostras sem argumentos, mantendo o comportamento malicioso oculto de sistemas de detecção perimetral.

5.2.3 Persistência Stealth via Variável de Ambiente

Após a validação da senha, o binário utiliza uma técnica de **Fork/Re-execução** para operar de forma invisível. É configurado a variável de ambiente **LOCKER_BACKGROUND=1**, no qual o processo pai lança uma cópia de si mesmo com esta *flag* ativa e encerra sua própria execução. O novo processo filho detecta a variável e assume a execução em segundo plano, desvinculando-se do console, permitindo a execução em *background*.

5.2.4 Implantação do README-GENTLEMEN.txt

A conclusão do ciclo de execução é marcada pela disseminação da nota de resgate, **README-GENTLEMEN.txt**. Este ficheiro atua como o componente central da fase de extorsão, sendo gerado dinamicamente para cada diretório afetado pelo processo de cifragem.

README-GENTLEMEN.txt - Notepad

File Edit Format View Help

```
3b7b4f2d33bdfb8a31b480d0eb2815cd = YOUR ID

Your network has been encrypted.
All encrypted files now have a new extension.

1) If you modify or rename encrypted files, our decryption software will NOT be able to restore them.
2) If you use any third-party recovery software, you may permanently damage your files (see item 1).
3) You need our unique decryption key and our software to restore your data. Your files cannot be decrypted without our key, not even with a qu
   Any attempts to brute-force or dump RAM will not help (locker binaries not contain the private key). Only we have the required key. Don't tr
4) Law enforcement, authorities, or data recovery companies will NOT be able to help you. Most of them will only take your money and waste your
5) Please note that attempts to restore the system may ultimately lead to a complete wipe of the system.

We have also downloaded sensitive/confidential data from your network, including NAS storage, Acronis cloud, etc.
If you do not contact us, or refuse to cooperate, your data will be published on our blog leak site and other hack forums, blogs, and social ne

BLOG link: http://tezwsse5czllksjb7cwp65rvnk4oobmzti2znn42i43bjdfd2prqqkad.onion/
Download Tor Browser: https://www.torproject.org/download/

TOX CONTACT - RECOVER YOUR FILES
Download TOX messenger: https://tox.chat/download.html
Contact us (add via TOX ID): F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EBBDF92CF9A9B84079F8F04060FF98D098E

Any other means of communication are fake and may be set up by third parties. Only use the methods listed in this note or on the specified webs
```

Figura 6 - Nota de Resgate

Composição e Estrutura de Dados

O conteúdo da nota é montado em tempo de execução, utilizando uma estrutura de dados organizada. O *malware* utiliza um *template* base que é preenchido com informações críticas para a negociação:

- **Identificador Único (UID):** O campo **YOUR ID** é populado, permitindo a sua identificação no painel do atacante.
- **Canais de Comunicação:** Instruções detalhadas para contacto via protocolo descentralizado **TOX** e *links* para o portal de fugas (*leak site*) na **rede Tor**.

Orquestração e Motores de Criptografia

A escrita da nota ocorre imediatamente após a conclusão da rotina de cifragem em cada pasta. Embora o processo seja executado de forma invisível, o binário implementa um motor híbrido de alta performance para garantir a velocidade do ataque:

- **Cifragem de Ficheiros:** Utiliza o algoritmo de fluxo **XChaCha20**, otimizado para alto desempenho em *software*.
- **Proteção de Chaves:** Implementa o protocolo **ECDH** (*Elliptic Curve Diffie-Hellman*) sobre a curva P-256, assegurando que apenas o detentor da chave privada do atacante possa reverter o processo.

6. Recomendações e Mitigação

Devido à força criptográfica do **ransomware The Gentlemen**, que utiliza um *design* de chave efêmera por arquivo, a recuperação sem a chave privada do operador é atualmente inviável. Portanto, a estratégia de defesa deve se concentrar na prevenção, detecção e resiliência.

- **Gerenciamento de Superfície de Ataque**: Audite e proteja rigorosamente todos os serviços voltados para a *internet*. Aplique o princípio de privilégio mínimo para contas de acesso remoto e implemente autenticação multifator (MFA) em todos os lugares possíveis.
- **Proteção de Endpoints:** Utilize uma solução de EDR capaz de detectar e bloquear técnicas de **BYOVD** e o abuso de ferramentas legítimas. Monitore a criação de serviços e tarefas agendadas suspeitas.
- **Segurança do Active Directory:** Monitore de perto as modificações nos **GPOs** e a atividade de contas privilegiadas. Limite o acesso a compartilhamentos como **NETLOGON**.
- **Backup e Recuperação:** Mantenha *backups offline* e imutáveis de dados críticos. Teste regularmente os procedimentos de restauração para garantir uma recuperação rápida em caso de incidente.

7. TABELA MITRE ATT&CK - THE GENTLEMEN RANSOMWARE

Esta tabela apresenta o mapeamento das Táticas, Técnicas e Procedimentos (TTPs) utilizadas pelo grupo **The Gentlemen**.

Tática	ID	Técnica	Procedimento / Observação
Acesso Inicial	T1190	Exploit Public-Facing Application	Exploração de serviços expostos (VPN/Firewall como FortiGate).
	T1078.002	Valid Accounts: Domain Accounts	Uso de credenciais administrativas comprometidas.
Execução	T1059.001	Command and Scripting Interpreter: PowerShell	Desativação do Windows Defender e execução de scripts de deploy.
	T1059.003	Command and Scripting Interpreter: Windows Command Shell	Execução de comandos via cmd.exe para limpeza de logs e exclusão de arquivos.
	T1204.002	User Execution: Malicious File	Execução do binário do ransomware (frequentemente via GPO ou manual).
Persistência	T1219	Remote Access Software	Instalação de software de acesso remoto como AnyDesk.
	T1112	Modify Registry	Modificações no registro para persistência e enfraquecimento de autenticação.
	T1543.003	Create or Modify System Process: Windows Service	Criação de serviços para manter acesso.
Escalação de Privilégios	T1068	Exploitation for Privilege Escalation	Técnica BYOVD abusando do driver ThrottleStop.sys (CVE-2025-7771).
	T1548.002	Abuse Elevation Control Mechanism: Bypass User Account Control	Uso de ferramentas como PowerRun.exe para obter privilégios de SYSTEM.
Evasão de Defesa	T1562.001	Impair Defenses: Disable or Modify Tools	Desativação do Real-time Monitoring do Defender e encerramento de processos de EDR/AV.
	T1014	Rootkit	Uso de driver vulnerável em nível de kernel para "cegar" soluções de segurança.
	T1070.001	Indicator Removal: Clear Windows Event Logs	Limpeza de logs de eventos via wevtutil.
	T1070.004	Indicator Removal on Host: File Deletion	Auto-exclusão do binário via script .bat e limpeza de Prefetch.
	T1027	Obfuscated Files or Information	Uso de VMProtect e ofuscação de runtime em Go; Malware Keying (parâmetro de senha).
	T1497.001	Virtualization/Sandbox Evasion: System Checks	Mecanismo de trava de execução (senha) para evitar análise em sandboxes.
Descoberta	T1046	Network Service Discovery	Uso de Nmap para mapeamento de serviços na rede.
	T1018	Remote System Discovery	Uso de Advanced IP Scanner para identificar hosts.
	T1087.002	Account Discovery: Domain Account	Enumeração do Active Directory via scripts em lote.
	T1069.002	Permission Groups Discovery: Domain Groups	Identificação de grupos privilegiados no domínio.
	T1482	Domain Trust Discovery	Identificação de controladores de domínio e topologia.
Movimentação Lateral	T1021.002	Remote Services: SMB/Windows Admin Shares	Uso de PsExec sobre compartilhamentos administrativos.
	T1021.001	Remote Services: Remote Desktop Protocol	Habilitação e uso de RDP para movimentação entre servidores.
Coleta	T1074.001	Data Staged: Local Data Staging	Compactação e organização de dados em diretórios locais antes da exfiltração.

Comando e Controle	T1219	Remote Access Software	Uso de AnyDesk como canal de C2 secundário.
	T1071.001	Application Layer Protocol: Web Protocols	Uso de protocolos web/SFTP para comunicação.
Exfiltração	T1048.003	Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol	Uso de WinSCP (SFTP) para envio de dados sensíveis.
Impacto	T1486	Data Encrypted for Impact	Criptografia híbrida (XChaCha20 + ECDH P-256) dos arquivos.
	T1489	Service Stop	Interrupção de serviços de banco de dados e backup (net stop).
	T1490	Inhibit System Recovery	Exclusão de Shadow Copies via vssadmin e wmic.
	T1491.001	Defacement: Internal Defacement	Alteração do papel de parede do sistema para notificação do resgate.

Tabela 2 - Mapeamento das TTPs

8. CONCLUSÃO

A análise do grupo ***The Gentlemen*** revela um ecossistema de ameaças que vai além da mera execução de um binário malicioso, consolidando-se como uma operação de ***Ransomware-as-a-Service*** de alta maturidade técnica e disciplina operacional. O grupo não apenas demonstra perícia no desenvolvimento de artefatos defensivos, mas também uma compreensão profunda da cadeia de ataque, desde o acesso inicial via exploração de serviços expostos até a exfiltração estratégica de dados sensíveis para dupla extorsão.

As **TTPs** empregadas evidenciam um foco agressivo na Evasão de Defesa e na Escalação de Privilégios. O uso da técnica de ***Bring Your Own Vulnerable Driver*** com o *driver* **ThrottleBlood.sys** (**CVE-2025-7771**) é um diferencial crítico, permitindo ao ator "cegar" soluções de EDR e antivírus em nível de *kernel*. Complementarmente, o binário implementa mecanismos de ***Malware Keying*** e execução furtiva via variáveis de ambiente (***LOCKER_BACKGROUND***), táticas projetadas especificamente para derrotar análises automatizadas em *sandboxes* e manter a persistência silenciosa durante a fase de impacto.

Para uma detecção e mitigação eficaz, as organizações devem adotar uma postura de defesa em profundidade que priorize a **detecção comportamental**, monitorando rigorosamente o **abuso de LOLBins** e **ferramentas administrativas legítimas** que o grupo utiliza em sua cadeia de ataque. A higiene de identidade, com MFA em todos os pontos e auditoria estrita de GPOs, torna-se a principal barreira contra a movimentação lateral. Diante da criptografia híbrida (**XChaCha20** + **ECDH P-256**) e da destruição sistemática de *Shadow Copies*, a resiliência de dados depende de ***backups offline***, testados regularmente para garantir a continuidade do negócio. Em última análise, a defesa contra o ***The Gentlemen*** exige que ferramentas convencionais sejam integradas a uma estratégia proativa de ***Threat Hunting***, capaz de identificar anomalias no uso de ferramentas nativas e neutralizar o impacto de um comprometimento que, dada a sofisticação do ator, torna-se cada vez mais inevitável.

REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **CTI Purple Team *by* ISH Tecnologia**
- VMProtect Software
- Trend Micro. "Unmasking The Gentlemen Ransomware: Tactics, Techniques, and Procedures Revealed".
- Cybereason. "License to Encrypt: “The Gentlemen” Make Their Move".
- SOCRadar. "Dark Web Profile: The Gentlemen Ransomware".
- Proven Data. "Gentlemen Ransomware: Tactical Analysis of a High-Velocity RaaS Operation".
- SOS Ransomware. "The Gentlemen: the new ransomware of autumn 2025".
- Ransomlook. "the gentlemen details".
- Ransomware.live. "Ransomware Statistics for Group: Thegentlemen".

AUTORES

Gustavo Jatene de Oliveira - Security Researcher

heimdall
security research
A DIVISION OF ISH