Alerta

Campaña

de Intrusión The Gentlemen (Storm-2697)

COLCERT AL – 20260719 - 103

TLP:CLEAR

Resumen Ejecutivo

The Gentlemen es un grupo de Ransomware-as-a-Service (RaaS) que surgió en julio de 2025 y escaló rápidamente hasta convertirse en una de las amenazas más sofisticadas de 2026. **Emplea una estrategia de doble extorsión:** exfiltra grandes volúmenes de datos sensibles antes de cifrar los sistemas de la víctima, con capacidad de cifrado multiplataforma sobre Windows, Linux y entornos virtualizados ESXi.

A fecha de abril de 2026 el grupo había reclamado **más de 200 víctimas en más de 50 países**, con predominancia de ataques al sector de manufactura, seguido de construcción, salud, finanzas y energía. De acuerdo a información de investigaciones el grupo representa cerca del 10% del volumen global de ataques de ransomware, como segundo actor más dañino del ecosistema después de Qilin.

El grupo se distingue por su capacidad de neutralizar defensas de nivel kernel mediante técnicas de Bring Your Own Vulnerable Driver (BYOVD), por la explotación sistemática de dispositivos perimetrales (en particular VPN Fortinet FortiGate a través del CVE-2024-55591) y por el uso de un locker multiplataforma escrito en Go con criptografía Curve25519 y XChaCha20. Se le atribuye una restricción operativa de no atacar objetivos en Rusia ni en países de la Comunidad de Estados Independientes (CEI), lo que sugiere un origen en Europa del Este.

Nivel de riesgo crítico: *El grupo mantiene actividad de intrusión activa y confirmada, con capacidad demostrada de comprometer el dominio completo de una organización y desplegar el cifrado en cuestión de minutos una vez alcanzados privilegios de administrador de dominio.*

NIVEL DE RIESGO

ALTO

Introducción

La inteligencia operativa asocia la infraestructura de soporte de esta amenaza al alias "hastalamuerte", perfilando posibles nexos tácticos con antiguos afiliados del ecosistema Qilin. **El incentivo económico es un factor multiplicador de este riesgo:** la organización ofrece una retención del 90% del rescate a quienes ejecutan las intrusiones, fomentando una rápida adopción y la descentralización de los ataques.

Esta delegación operativa permite la ejecución simultánea de múltiples campañas independientes, amplificando el nivel de amenaza a escala global. El patrón de compromiso de estos afiliados evidencia una dependencia crítica en la superficie de ataque externa y los dispositivos de borde. La explotación sostenida de vulnerabilidades perimetrales conocidas subraya una brecha estructural en las funciones de protección; esto demuestra de forma tangible que, incluso al establecer pruebas de concepto rigurosas para evaluar el filtrado de contenido y el bloqueo de malware en los firewalls, la efectividad del perímetro es fácilmente neutralizada si las organizaciones carecen de un ciclo estricto y continuo de gestión de parches.

Perfil del Actor

Identidad y alias

El grupo es identificado principalmente con el nombre The Gentlemen, denominación utilizada tanto por sus integrantes como por la comunidad especializada en inteligencia de amenazas (Threat Intelligence). En documentación técnica y reportes elaborados en español, también es común encontrar las traducciones "Los Señores" y "Los Caballeros", empleadas como variantes equivalentes para hacer referencia al mismo actor.

Asimismo, en diferentes análisis e investigaciones se han identificado los alias "hastalamuerte" y "zeta88", asociados presuntamente con operadores o afiliados vinculados a las actividades del grupo. Estos seudónimos han sido utilizados para identificar la participación de determinados individuos dentro de la infraestructura o las operaciones atribuidas a la organización.

Por otra parte, diversas fuentes hacen referencia a una entidad de soporte administrativo denominada The Gentlemen Data, la cual habría desempeñado funciones de apoyo relacionadas con la gestión o coordinación de ciertos aspectos operativos del grupo. De acuerdo con la información disponible, esta entidad es señalada como de presunto origen ruso; sin embargo, dicha atribución debe considerarse con cautela, ya que no existe confirmación pública e independiente que permita establecer de manera concluyente su procedencia o vinculación.

Atribución y origen

Hasta la fecha, la información disponible no atribuye a The Gentlemen un país de origen específico, no obstante, diversos análisis destacan que el grupo mantiene una política estricta de no ejecutar ataques contra Rusia ni contra los países miembros de la Comunidad de Estados Independientes (CEI), circunstancia que ha llevado a algunos investigadores a sugerir un posible origen o vínculo con Europa del este, adicionalmente, *algunas fuentes de inteligencia de amenazas sostienen que The Gentlemen habría surgido como una escisión (spin-off) del grupo Qilin en julio de 2025, presuntamente como consecuencia de desacuerdos relacionados con el reparto de ingresos entre sus integrantes.*

Según esas mismas fuentes, en mayo de 2026 el operador identificado con el alias "hastalamuerte", también motivado por discrepancias sobre la distribución de beneficios, habría filtrado de forma voluntaria bases de datos internas, paneles de administración y credenciales de acceso del grupo a diversas empresas de ciberseguridad, principalmente Group-IB. Asimismo, dichas fuentes afirman que la información filtrada habría revelado la existencia de vínculos de soporte mutuo entre The Gentlemen, un grupo de amenazas identificado como Phantom Mantis y células asociadas con la denominación LARVA-368, no obstante, estas afirmaciones provienen de fuentes de inteligencia de amenazas y, hasta el momento, no cuentan con una confirmación pública e independiente que permita verificarlas de manera concluyente.

Motivación, modelo de operación, sectores objetivo y alcance

The Gentlemen opera bajo un modelo de Ransomware as a Service (RaaS) con fines económicos, utilizando una estrategia de doble extorsión que combina la exfiltración de información confidencial con el cifrado de los sistemas de la víctima, condicionando la no publicación de los datos al pago del rescate, el modelo de reparto de beneficios asignaría el 90 % del rescate a los afiliados y, tras la filtración ocurrida en mayo de 2026, el grupo habría reforzado sus mecanismos de reclutamiento, exigiendo a los nuevos afiliados aportar al menos 1 GB de información previamente robada como prueba de capacidad operativa antes de habilitarles el acceso a las herramientas de compilación del ransomware.

El grupo concentra la mayor parte de sus ataques en el sector de manufactura, responsable de aproximadamente el 30 % de las víctimas identificadas, seguido por los sectores de construcción, salud, finanzas y energía. Hasta abril de 2026, The Gentlemen había reclamado públicamente más de 200 víctimas en más de 50 países, sin embargo, esta cifra representaría solo una parte de las organizaciones comprometidas, mientras que el acceso a un servidor de comando y control (C2) de un afiliado habría revelado una infraestructura con más de 1.570 organizaciones comprometidas que permanecían sin divulgar mientras se completaban las actividades de exfiltración de datos.

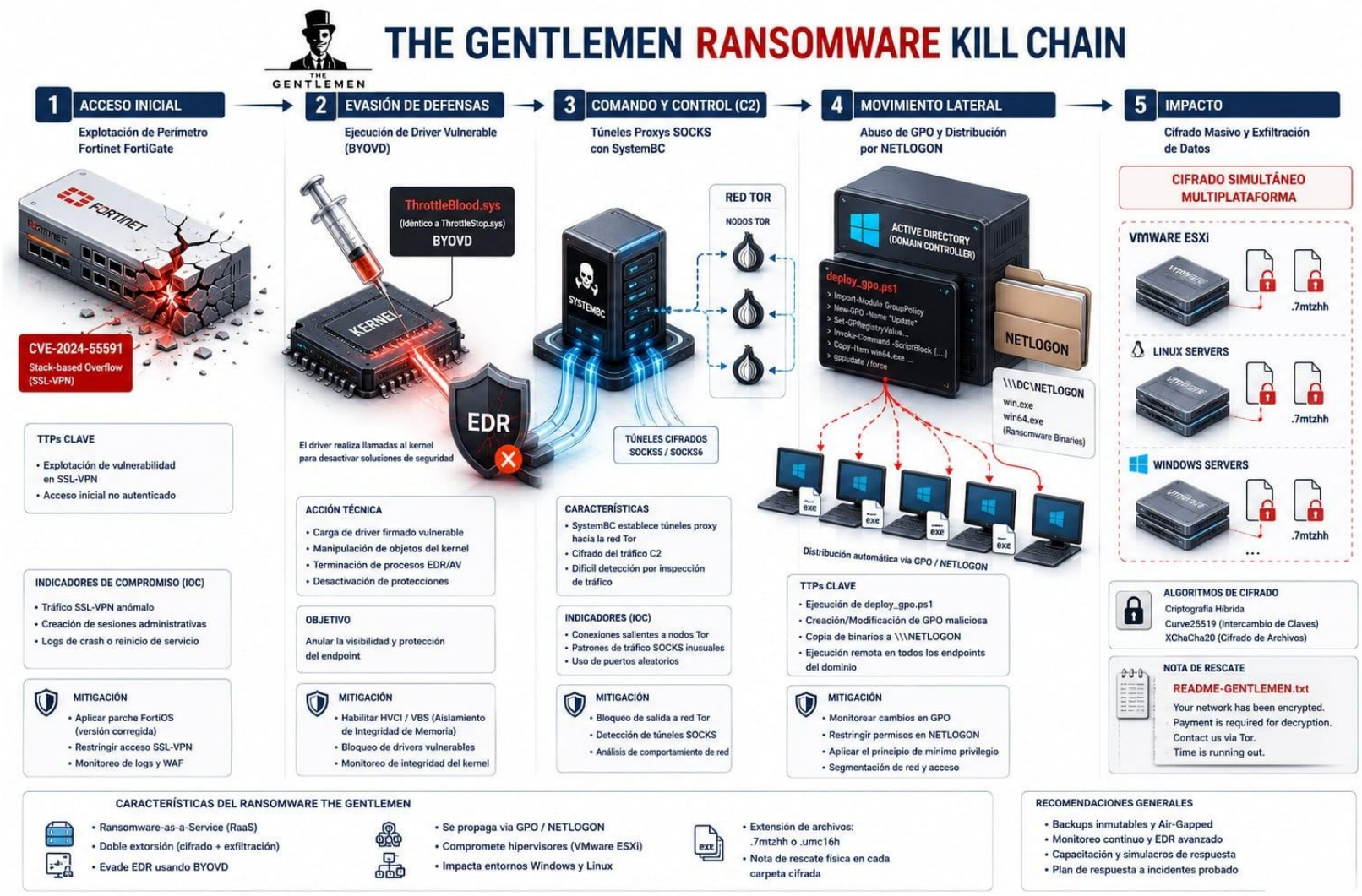
Técnicas y Tácticas — MITRE ATT&CK

A continuación se detalla el ciclo de ataque documentado, organizado por fases.

Técnica ID	Nombre	Táctica	Descripción Operacional
T1190	Exploit Public-Facing Application	Acceso Inicial	Explotación de aplicaciones y dispositivos expuestos a Internet, principalmente FortiOS/FortiProxy (CVE-2024-55591), así como otras vulnerabilidades reportadas en soluciones VPN y gateways empresariales para obtener acceso inicial.
T1078	Valid Accounts	Acceso Inicial	Uso de credenciales válidas obtenidas mediante phishing, malware infostealer o adquiridas a Initial Access Brokers (IAB) para autenticarse en VPN SSL, Citrix y portales SSO.
T1110	Brute Force	Acceso Inicial	Ejecución de campañas automatizadas de fuerza bruta contra servicios VPN SSL y RDP utilizando diccionarios de credenciales y contraseñas por defecto.
T1595	Active Scanning	Reconocimiento	Escaneo de servicios expuestos (RDWeb, Microsoft IIS y RDP) para identificar sistemas accesibles y posibles vectores de intrusión.
T1046	Network Service Discovery	Descubrimiento	Enumeración de servicios de red, servidores, bases de datos, sistemas VMware ESXi y dispositivos NAS mediante herramientas de escaneo y scripts automatizados.
T1087	Account Discovery	Descubrimiento	Enumeración de usuarios, grupos y objetos de Active Directory mediante SharpADWS para identificar cuentas con privilegios elevados.
T1003.001	LSASS Memory	Obtención de Credenciales	Volcado de la memoria del proceso LSASS para obtener credenciales y facilitar la escalada de privilegios hasta administrador de dominio.

Técnica ID	Nombre	Táctica	Descripción Operacional
T1068	Exploitation for Privilege Escalation	Escalada de Privilegios	Uso de la técnica Bring Your Own Vulnerable Driver (BYOVD) mediante un controlador vulnerable para obtener privilegios de kernel antes del despliegue del ransomware.
T1562.001	Disable or Modify Security Tools	Evasión de Defensas	Desactivación de soluciones EDR y antivirus mediante controladores vulnerables, modificación de Microsoft Defender, cambios en el registro y uso de herramientas legítimas para eliminar agentes de seguridad.
T1070	Indicator Removal on Host	Evasión de Defensas	Eliminación de registros de eventos, historial de PowerShell, caché de conexiones RDP y archivos Prefetch para dificultar el análisis forense.
T1497	Virtualization/Sandbox Evasion	Evasión de Defensas	Verificación de parámetros específicos de ejecución; el malware finaliza su ejecución si detecta un entorno automatizado o de análisis.
T1219	Remote Access Software	Persistencia	Implementación de herramientas legítimas de acceso remoto, como AnyDesk y BeyondTrust, para mantener acceso persistente a los sistemas comprometidos.
T1090	Proxy	Comando y Control	Uso de SystemBC para establecer túneles SOCKS y canalizar las comunicaciones entre los sistemas comprometidos y la infraestructura de comando y control (C2).
T1055	Process Injection	Comando y Control	Despliegue de implantes personalizados desarrollados en Go e inyección de cargas adicionales en memoria para mantener la comunicación con los operadores.
T1484.001	Group Policy Modification	Movimiento Lateral	Distribución del ransomware mediante Objetos de Directiva de Grupo (GPO) utilizando el recurso compartido NETLOGON de los controladores de dominio.
T1021	Remote Services	Movimiento Lateral	Uso de WMI, PowerShell Remoting (WinRM) y PsExec para ejecutar comandos y desplegar el ransomware en sistemas remotos del dominio.
T1053.005	Scheduled Task	Movimiento Lateral	Creación de tareas programadas para ejecutar simultáneamente el ransomware en todos los equipos unidos al dominio.
T1048	Exfiltration Over Alternative Protocol	Exfiltración	Exfiltración de información mediante WinSCP utilizando conexiones SFTP cifradas antes de iniciar el proceso de cifrado.
T1486	Data Encrypted for Impact	Impacto	Cifrado de archivos mediante un ransomware desarrollado en Go y C, empleando los algoritmos XChaCha20 y Curve25519 para afectar sistemas Windows, Linux, NAS y VMware ESXi.
T1490	Inhibit System Recovery	Impacto	Eliminación de instantáneas de volumen, copias de seguridad y detención de servicios críticos (MSSQL, MySQL, MongoDB y Veeam) para impedir la recuperación de los sistemas afectados.

Cyber kill chain



Indicadores de Compromiso (IoCs)

Categoría	Indicadores asociados	Descripción operacional
Dominios, URLs y servicios de comunicación	wmk77[.]com thegentlemen[.]cc tezwsse5czllksjb7cwp65rvnk4oobmzti2znn42i43bjdfd2prqqkad[.]onion x[.]com/TheGentlemen26 smp17[.]simplex[.]im/a#YeXZNiEHZesT2O7cz4vV3IPnjpstnC6ujF9pvjIOjJQ simplex[.]chat/downloads/ tox[.]chat/download.html torproject[.]org/download/	Infraestructura asociada a comando y control (C2), portal de filtración de datos (DLS), comunicación con víctimas, negociación de rescates y acceso a servicios de anonimización.
Hashes SHA-256 del ransomware y herramientas asociadas	3ab9575225e00a83a4ac2b534da5a710bdcf6eb72884944c437b5fbe5c5c923522b38dad7da097ea03aa28d0614164cd25fafeb1383dbc15047e34c8050f6f67025fc0976c548fb5a880c83ea3eb21a5f23c5d53c4e51e862bb893c11adf712a1334f0189a8e6dbc48456fa4b482c5726ab7609f7fa652fcc4c1a96f2334436f1eece1e1ba4b96e6c784729f0608ad2939cfb67bc4236dfababbe1d09268960c5dc607c8990841139768884b1b43e1403496d5a458788a1937be139594f01dca	Muestras del ransomware multiplataforma: cifrador principal Windows, variantes Go, lockers Linux y componentes dirigidos a NAS/hipervisores.

Categoría	Indicadores asociados	Descripción operacional
Hashes MD5	adf675ffc1acb357f2d9f1a94e016f52 de1a114a2c5552387a1bbb61501bf129	Variante del ransomware y herramienta asociada a desactivación de soluciones EDR.
Archivos ejecutables y artefactos maliciosos	win[.]exe win64[.]exe README-GENTLEMEN[.]txt ThrottleBlood[.]sys All[.]exe Allpatch2[.]exe deploy_gpo[.]ps1 kavrmvr[.]exe gentlemen[.]bmp gentlemen_system	Binarios, scripts y artefactos asociados al cifrado, nota de rescate, evasión de defensas, despliegue mediante GPO, eliminación de antivirus y modificación visual posterior a la infección.
Extensiones y artefactos de cifrado	.7mtzhh .umc16h	Extensiones aplicadas a archivos cifrados por variantes del ransomware.
Infraestructura IP prioritaria (C2/VPN/Proxy)	45[.]92[.]170[.]210 185[.]100[.]157[.]111 185[.]65[.]134[.]216 92[.]60[.]40[.]220 193[.]32[.]249[.]173 2a01:111:2053:900e:0:afd:ad4:4e1e	Direcciones asociadas a nodos VPN, proxies, tránsito de red, SystemBC y comunicaciones C2.
Infraestructura IP adicional observada	40[.]126[.]32[.]99 213[.]111[.]146[.]77 202[.]29[.]236[.]131 49[.]232[.]90[.]103 61[.]53[.]254[.]181 172[.]111[.]138[.]100 58[.]59[.]152[.]62 111[.]59[.]182[.]242 113[.]228[.]104[.]78 103[.]133[.]109[.]181 117[.]253[.]110[.]19 5[.]181[.]86[.]60 221[.]14[.]169[.]68 117[.]206[.]214[.]197 117[.]243[.]247[.]33 61[.]1[.]228[.]152 42[.]5[.]4[.]199 27[.]202[.]180[.]33 219[.]133[.]103[.]198 221[.]15[.]131[.]26 77[.]105[.]178[.]226 118[.]194[.]228[.]101 61[.]0[.]185[.]156 8[.]219[.]204[.]102 125[.]43[.]89[.]104 45[.]144[.]212[.]58 1[.]92[.]81[.]34 49[.]74[.]5[.]132 61[.]3[.]105[.]98 115[.]55[.]104[.]196 103[.]237[.]86[.]46 59[.]36[.]75[.]227 45[.]78[.]229[.]227 117[.]235[.]115[.]164 42[.]228[.]32[.]120 47[.]98[.]50[.]198 38[.]89[.]70[.]165 59[.]183[.]173[.]232 172[.]29[.]16[.]132	Direcciones IP identificadas en infraestructura, actividad sospechosa, phishing, Cobalt Strike, RATs y nodos de tránsito.

Categoría	Indicadores asociados	Descripción operacional
Servicios y puertos asociados	443/tcp 445/tcp SMBv1	Servicios utilizados como superficie de ataque, comunicación HTTPS e intrusión mediante SMB.
Vulnerabilidades explotadas o asociadas	CVE-2017-0143 CVE-2017-0144 CVE-2017-0145 CVE-2017-0146 CVE-2017-0147 CVE-2017-0148 CVE-2012-0002 CVE-2012-0152 CVE-2019-0708 MS17-010 MS12-020	Vulnerabilidades asociadas a explotación SMB (EternalBlue), RDP (BlueKeep/MS12-020) y ejecución remota en sistemas Windows.
Malware y herramientas relacionadas	WannaCry EternalBlue Amadey KTLVdoor SystemBC WinSCP PsExec WMI PowerShell Remoting SharpADWS Advanced IP Scanner NetScan	Malware, herramientas legítimas y utilidades empleadas para reconocimiento, movimiento lateral, exfiltración, persistencia y comunicación C2.

Recomendaciones Técnicas

Endurecimiento perimetral y protección de accesos externos

- Se recomienda aplicar de manera inmediata y con prioridad crítica los parches de seguridad disponibles en dispositivos Fortinet FortiGate/FortiOS/FortiProxy, con el objetivo de mitigar la explotación del CVE-2024-55591, vulnerabilidad reportada como vector de acceso inicial utilizado contra infraestructura VPN expuesta a Internet.
- Evaluar la aplicación de actualizaciones de seguridad asociadas a otras vulnerabilidades en dispositivos de borde y soluciones VPN, incluyendo CVE-2025-32433 y CVE-2025-33073, con el fin de reducir posibles vectores alternativos de intrusión.
- Implementar autenticación multifactor (MFA) obligatoria para todos los accesos remotos, priorizando mecanismos resistentes a phishing como FIDO2/WebAuthn, especialmente en servicios críticos como VPN SSL, portales RDWeb, consolas administrativas y plataformas de gestión en la nube.
- Restringir la exposición directa a Internet de servicios administrativos como RDP (3389/tcp) y SMB (445/tcp), permitiendo su acceso únicamente mediante canales VPN autenticados, con controles adicionales de segmentación y monitoreo.
- Deshabilitar completamente el protocolo SMBv1 en controladores de dominio, servidores y estaciones Windows, debido a su asociación con vulnerabilidades históricas de ejecución remota y propagación de malware.

Protección contra técnicas BYOVD y abuso de controladores vulnerables

- Para reducir el riesgo asociado a técnicas de Bring Your Own Vulnerable Driver (BYOVD), se recomienda habilitar Hypervisor-Protected Code Integrity (HVCI) y Virtualization-Based Security (VBS) en todos los sistemas Windows compatibles.
- Implementarse la lista de bloqueo de controladores vulnerables mediante Windows Defender Application Control (WDAC), prestando especial atención a controladores asociados a herramientas utilizadas para evasión defensiva, como ThrottleStop.sys/ThrottleBlood.sys.
- Se recomienda establecer mecanismos de monitoreo sobre la instalación, carga y ejecución de controladores del sistema, generando alertas ante drivers firmados pero identificados como vulnerables o utilizados para desactivar soluciones de seguridad.

Protección de Active Directory y prevención del movimiento lateral

Se recomienda restringir estrictamente los permisos de escritura sobre el recurso compartido NETLOGON en los controladores de dominio, permitiendo modificaciones únicamente a cuentas administrativas autorizadas y monitoreadas. Debe establecerse monitoreo continuo sobre modificaciones de Objetos de Directiva de Grupo (GPO) y ejecución de scripts sospechosos, especialmente aquellos con comportamiento similar a mecanismos automatizados de despliegue como deploy_gpo.ps1.

Se debe implementar detección sobre herramientas comúnmente utilizadas para movimiento lateral y administración remota, incluyendo:

- Ejecución no autorizada de PsExec.exe.
- Creación de procesos anómalos mediante wmiprvse.exe.
- Uso sospechoso de wsmprovhost.exe asociado a PowerShell Remoting.
- Actividad administrativa fuera de patrones habituales.

Además, se recomienda habilitar y centralizar registros avanzados de seguridad, incluyendo:

- Auditoría operacional de WMI mediante eventos 5857 y 5861.
- Registro de bloques de scripts de PowerShell mediante Event ID 4104.
- Supervisión de conexiones administrativas mediante WinRM (TCP 5985/5986), especialmente aquellas originadas desde estaciones de trabajo hacia controladores de dominio.

Resiliencia y protección de datos críticos

Las organizaciones deben mantener copias de seguridad críticas bajo esquemas resistentes al ransomware, incluyendo almacenamiento inmutable, desconectado de red (air-gapped) o protegido contra modificación por cuentas comprometidas.

Los respaldos deben incluir información esencial para la recuperación completa del entorno, como:

- Bases de datos.
- Configuraciones de sistemas críticos.
- Imágenes de máquinas virtuales.
- Infraestructura VMware ESXi y almacenamiento NAS.

Se recomienda realizar pruebas periódicas de restauración para validar que los mecanismos de recuperación funcionan correctamente y no dependen de infraestructura potencialmente comprometida.

Fuentes

- AhnLab. (2025, 10 de diciembre). Threats Behind the Mask of Gentlemen Ransomware – ASEC. https://asec.ahnlab.com/en/
- Bitdefender. (2026, 10 de marzo). Bitdefender Threat Debrief | March 2026. https://www.bitdefender.com/blog/labs/bitdefender-threat-debrief-march-2026/
- Cybereason. (2025, 18 de noviembre). License to Encrypt: “The Gentlemen” Make Their Move. https://www.cybereason.com/blog/threat-intelligence-report-thegentlemen-ransomware
- Cyfirma. (2026, 20 de marzo). Weekly Intelligence Report – 20 March 2026. https://www.cyfirma.com/uncategorized/weekly-intelligence-report-20-march-2026/
- Group-IB. (2025). Ransomware Ecosystem Report 2025-2026: The Rise of The Gentlemen. https://www.group-ib.com/resources/reports/
- Provendata. (2026). The Gentlemen Ransomware Analysis and Recovery. https://www.provendata.com/blog/gentlemen-ransomware/
- SOCRadar. (2026). Dark Web Profile: The Gentlemen Ransomware Group. https://socradar.io/dark-web-profile-the-gentlemen-ransomware/
- Trend Micro. (2026). Ransomware Status Report Q1 2026: The Evolution of BYOVD Tactics. https://www.trendmicro.com/vinfo/us/security/news/
- Check Point Research. (2026). The Gentlemen: The Rapid Rise of a Sophisticated New Ransomware Threat. https://research.checkpoint.com/2026/the-gentlemen-ransomware-rising-threat/
- Trend Micro. (2025). Unmasking The Gentlemen Ransomware: Tactics, Techniques, and Procedures Revealed. https://www.trendmicro.com/en_us/research/25/h/unmasking-the-gentlemen-ransomware.html
- Group-IB. (2026). Hasta la vista, Hastalamuerte: An Overview of The Gentlemen's TTPs and Affiliate Disputes. https://www.group-ib.com/resources/research/the-gentlemen-ransomware-ttps/
- Kaspersky GReAT. (2026). Not too gentle: Kaspersky warns of The Gentlemen ransomware group expanding operations with new malware. https://securelist.com/the-gentlemen-ransomware-backdoor/112345/
- AhnLab ASEC. (2025). New Gentlemen Ransomware Hits Corporations, Steals Confidential Data Before Locking Systems. https://asec.ahnlab.com/en/85234/