

Alerta ID:	111
Fecha del reporte:	18/06/2026
Entidad:	Todas las Entidades del Ecosistema Digital
Título:	The Gentlemen (Storm-2697): RaaS impulsado por infostealers, IA y un reparto del 90% a afiliados
Herramienta de detección	N/A
Activo involucrado:	Sectores de manufactura, tecnología, Servicios, Salud, Seguros, construcción
Tipo de alerta:	Alerta de Inteligencia de Amenazas (Threat Intelligence)
Nivel de riesgo:	ALTO / CRITICO

Resumen ejecutivo

The Gentlemen es una operación de Ransomware-as-a-Service (RaaS) que emergió hacia mediados de 2025 y que, en menos de un año, se ha consolidado como la segunda marca de ransomware más prolífica de 2026 por número de víctimas publicadas, solo por detrás de Qilin. Al 13 de junio de 2026 el grupo había listado 483 víctimas en su portal de filtraciones (DLS), 380 de ellas durante 2026, distribuidas en 66 países.

La relevancia de esta amenaza para el sector salud es doble. Primero, la salud figura de forma consistente entre los sectores más atacados por el grupo (cuarto sector con 44 víctimas listadas, según el conteo más reciente). Segundo, y más grave, los operadores han demostrado disposición a ejercer presión extorsiva utilizando contenido médico sensible de las víctimas, enviado desde buzones de correo comprometidos, lo que eleva el riesgo reputacional, legal y de protección de datos para cualquier entidad de salud afectada.

Un hecho determinante ocurrido en mayo de 2026 fue la filtración de los chats internos y datos de backend del propio grupo, atribuida a un insider o a un host comprometido. Ese material, analizado por KELA y otros equipos, expuso un núcleo de aproximadamente nueve miembros,



un modelo de afiliados que entrega el 90% del rescate al operador que ejecuta la intrusión, el uso operativo de modelos de inteligencia artificial (incluidos modelos de pesos abiertos sin filtros de seguridad) y un modelo de acceso construido casi en su totalidad sobre credenciales robadas por malware infostealer de uso común.

Conclusión para CSIRT Salud: la defensa frente a The Gentlemen no exige herramientas exóticas, sino disciplina operativa en parcheo de dispositivos perimetrales (con especial atención a FortiOS / CVE-2024-55591), tratamiento de las infecciones por infostealer como brechas con revocación inmediata de sesiones, endurecimiento de Active Directory frente a ZeroLogon y PetitPotam, y monitoreo continuo de credenciales filtradas y cookies de sesión en la dark web.

Perfil del actor y modelo de operación.

Cronología y posicionamiento

- **Aparición pública:** campana documentada por primera vez por Trend Micro en agosto-septiembre de 2025; Microsoft Threat Intelligence rastrea al operador como Storm-2697.
- **Volumen:** 483 víctimas acumuladas y 66 países afectados al 13/06/2026; aproximadamente el 10% de las víctimas de ransomware observadas a nivel global en 2026.
- **Distribución geográfica atípica:** solo cerca del 15% de las víctimas están en Estados Unidos (frente al 40-50% habitual en otras marcas). El resto se reparte entre Tailandia, Brasil, Reino Unido, Francia, India, Alemania, Italia, Japón, Taiwan y España.
- **Lógica de selección de objetivos:** los chats filtrados indican que se priorizaron países de “Tier 1 a 3” y América Latina, ponderando el dolor operativo sobre el ingreso bruto. El razonamiento explícito es que una empresa de servicios públicos de USD 20 millones puede pagar más rápido que una manufacturera de USD 200 millones si el cifrado realmente detiene el negocio.



Modelo de afiliados y aspectos financieros

El núcleo del grupo construye y mantiene el ransomware y el panel de negociación; los operadores externos (afiliados) ejecutan las intrusiones y conservan el 90% de cada rescate, un reparto notablemente generoso que se reparte típicamente entre 2 o 3 colaboradores por intrusión. Esta estructura abarata radicalmente el escalamiento de la marca.

Las negociaciones documentadas muestran demandas calibradas al techo de la póliza de ciberseguro de la víctima, usando datos de ingresos de fuentes como ZoomInfo. En un caso documentado, una demanda inicial de USD 250.000 se ajustó a USD 190.000 efectivamente recibidos. El blanqueo de fondos incluye cadenas de intercambio, conciencia explícita de puntajes AML, billeteras no custodiales y cobros OTC.

Uso de inteligencia artificial

La operación es abiertamente asistida por IA, lo que constituye uno de los casos mejor documentados de uso real de modelos de lenguaje en operaciones cotidianas de ransomware, más allá del discurso. El administrador (alias zeta88) afirmó haber “vibe-coded” el panel de negociación en tres días. El grupo discutió el uso de modelos de pesos abiertos “abliterated” (con las salvaguardas de alineamiento removidas), identificados por KELA como una variante derivada de Qwen 3.5, tanto para programación como para razonar sobre cientos de gigabytes de datos robados e identificar paneles de administración y rutas de acceso.

El análisis autónomo de datos robados mediante LLM auto alojado figura en los chats como un objetivo anunciado, no como una capacidad plenamente operativa al momento de la filtración. No obstante, marca una tendencia clara de adopción de IA ofensiva que CSIRT Salud debe vigilar.

Reutilización del manual de Black Basta

El grupo estudio la filtración de chats de Black Basta de febrero de 2025 y la trato como un manual de entrenamiento, copiando flujos de phishing y de abuso de buzones de correo en lugar de desarrollarlos desde cero, incluyendo técnicas de firma de código para hacer que los binarios parezcan legítimos.



Vectores de acceso inicial



El grupo concentra su energía en el acceso inicial, no en el cifrado. Los vectores observados y descritos en los chats son:

- **Explotación de servicios expuestos a Internet:** aprovechamiento de la vulnerabilidad de elusión de autenticación de FortiOS CVE-2024-55591, así como debilidades clásicas de Active Directory como ZeroLogon (CVE-2020-1472) y PetitPotam.
- **Credenciales robadas por infostealers:** es el hilo que une toda la operación. El equipo de acceso inicial utiliza de forma sistemática motores de búsqueda de logs de infostealer (por ejemplo, Snusbase y servicios equivalentes) para localizar credenciales corporativas válidas antes de lanzar el ataque, evitando la necesidad de exploits complejos.
- **Abuso de buzones OWA (Outlook Web Access) comprometidos:** cuando no hay exploit disponible, se usan credenciales válidas robadas de buzones OWA, tanto para descubrir accesos VPN como para enviar phishing desde cuentas internas de confianza que los destinatarios no tienen motivos para desconfiar.

Caso ilustrativo (cookies de sesión): RansomNews cruzó una muestra de víctimas de The Gentlemen contra el índice de infostealers alerts.bar y halló credenciales corporativas activas o tokens de sesión vigentes antes de su aparición en el DLS. En un caso, la firma logística filipina 2GO mostraba 6 accesos de empleados, 7 de clientes y 38 tokens de sesión activos ya expuestos. Las cookies de sesión robadas derrotan por completo el MFA basado en SMS y notificaciones push, razón por la cual el monitoreo de infostealers y dark web debe situarse en el mismo nivel de riesgo que la gestión de parches.

Tácticas, técnicas y procedimientos (cadena de ataque)



Con base en el análisis técnico de Trend Micro sobre la campana, complementado por Microsoft y Huntress, la cadena de ataque observada es la siguiente:



Descubrimiento

- Reconocimiento de red con Advanced IP Scanner y posteriormente Nmap (nmap -sV -T4 -O -F).
- Enumeración masiva de cuentas mediante un script por lotes (1.bat) que consulta más de 60 cuentas de dominio, incluyendo administradores de dominio, administradores de empresa y grupos privilegiados personalizados (p. ej. itgateadmin), así como grupos de virtualización (VMware).
- Identificación del PDC mediante PowerShell codificado en base64: (Get-ADDomain).PDCEmulator.

Evasión de defensas

- Abuso de driver legítimo vulnerable: despliegue de All.exe junto con ThrottleBlood.sys para terminar procesos protegidos a nivel kernel (técnica tipo “BYOVD” / AV killer).
- Herramientas anti-AV a medida: PowerRun.exe para escalamiento y, posteriormente, una versión mejorada y específica Allpatch2.exe adaptada para neutralizar los componentes del agente de seguridad presente en el entorno.
- Modificación de registro para debilitar autenticación (RestrictSendingNTLMTraffic, DisableRestrictedAdmin) y desactivación de Windows Defender (Set-MpPreference -DisableRealtimeMonitoring \$true; exclusiones de ruta y proceso).
- Limpieza de evidencia: wevtutil cl Security/Application/System, borrado de Prefetch, logs RDP y soporte de Defender.

Movimiento lateral, persistencia y exfiltración

- Movimiento lateral con PsExec (SMB) y habilitación de RDP vía registro; indicios de SSH con PuTTY.
- Persistencia y C2 mediante AnyDesk (acceso remoto resiliente a la respuesta a incidentes).
- Manipulación de GPO (gpme.msc / gpmmc.msc) para despliegue de configuraciones maliciosas en todo el dominio.



- Estancamiento de datos en C:\ProgramData\data y exfiltración cifrada mediante WinSCP; conexiones WebDAV a recursos internos.

Impacto

- Despliegue del cifrador a través del recurso compartido NETLOGON, garantizando distribución a todos los equipos unidos al dominio.
- Cifrador escrito en Go, multiplataforma (Windows, Linux, ESXi, NAS, BSD), con cifrado híbrido Curve25519 + XChaCha20 y autopropagación en redes Windows (documentado por Microsoft).
- Terminación masiva de servicios y procesos de respaldo, base de datos y seguridad (Veeam, SQL, Backup Exec, Acronis, sophos, vss, etc.) y eliminación de instantáneas: vssadmin delete shadows /all /quiet y wmic shadowcopy delete.
- Artefactos del cifrador: extensión de archivo .7mtzhh y nota de rescate README-GENTLEMEN.txt. El binario requiere el parámetro --password (clave de 8 bytes) para ejecutarse, lo que dificulta el análisis automatizado en sandbox.

Relevancia e impacto para el sector salud

Aunque la fuente primaria es un reporte de alcance global, el perfil del actor presenta varios puntos de contacto directos con el portafolio de entidades monitoreadas por CSIRT Salud:

- **Salud como sector objetivo recurrente:** Trend Micro sitúa a la salud entre los sectores más golpeados desde el origen de la campana, y los conteos de 2026 la mantienen en el cuarto lugar con 44 víctimas listadas.
- **Extorsión con datos médicos:** KELA observó a los operadores ejerciendo presión sobre una víctima mediante contenido médico sensible enviado desde un buzón personal comprometido. Para entidades de salud colombianas, un incidente de este tipo implicaría exposición de historia clínica y datos sensibles, con implicaciones bajo la Ley 1581 de 2012 y obligaciones de reporte.



- **Dependencia de FortiGate / FortiOS:** el vector CVE-2024-55591 y el compromiso de cuentas administrativas de FortiGate son centrales en la cadena de ataque. Varias entidades del portafolio operan dispositivos FortiGate expuestos, por lo que la superficie de exposición es directamente aplicable.
- **La exfiltración pesa más que el cifrado:** el apalancamiento real proviene cada vez más de los datos robados y de la lista de contactos de la víctima, no de los archivos cifrados. Disponer de respaldos no elimina el riesgo: se debe asumir robo de datos con independencia de si hubo cifrado.

Mapeo MITRE ATT&CK

Técnicas observadas y mapeadas con alta confianza a partir de los reportes de Trend Micro, Microsoft y Check Point:

Táctica	Técnica (ID)	Descripción observada
Acceso inicial	T1190	Explotación de FortiGate / CVE-2024-55591; servicios expuestos
Acceso inicial	T1078.002	Cuentas válidas de dominio (credenciales de infostealer / OWA)
Descubrimiento	T1046 / T1018	Nmap y Advanced IP Scanner para mapeo de red
Descubrimiento	T1087.002	Enumeración masiva de cuentas de dominio (1.bat)
Descubrimiento	T1482	Identificación del PDC vía PowerShell
Ejecución	T1059.001 / .003	PowerShell y cmd.exe para anti-AV y despliegue
Evasión	T1562.001	Deshabilitar/modificar herramientas de seguridad (anti-AV)
Evasión	T1014	Driver vulnerable (ThrottleBlood.sys) para terminar procesos
Evasión	T1112	Modificación de registro (NTLM, RestrictedAdmin)
Evasión	T1562.004	Modificación del firewall para acceso RDP
Evasión	T1027 / T1070.001	PowerShell base64; limpieza de logs (wevtutil)
Escalamiento	T1484.001	Manipulación de GPO para impactó en todo el dominio
Persistencia	T1219	AnyDesk como acceso remoto / C2



Táctica	Técnica (ID)	Descripción observada
Mov. lateral	T1021.002 / .001 / .004	Psexec (SMB), RDP y SSH (PuTTY)
Colección	T1074.001 / T1039	Estancamiento en ProgramData; WebDAV a recursos internos
Exfiltración	T1048.001	Exfiltración cifrada mediante WinSCP
Impacto	T1486	Cifrado de datos (cifrador Go vía NETLOGON)
Impacto	T1489 / T1490	Detención de servicios; borrado de instantáneas

Indicadores de compromiso (IOC)

Los siguientes indicadores provienen del análisis público de Trend Micro y Microsoft. Se recomienda su carga en FortiSIEM, FortiEDR, FortiAnalyzer, Trend Vision One / Apex One y plataformas de correo, validando previamente para evitar falsos positivos.

Hashes (SHA-1) y herramientas

Indicador (SHA-1)	Detección / Tipo
c12c4d58541cc4f75ae19b65295a52c559570054	Ransom.Win64.GENTLEMAN.THHAIBE (cifrador)
c0979ec20b87084317d1bfa50405f7149c3b5c5f	Trojan.Win64.KILLAV.THBBHBE (KILLAV inicial)
df249727c12741ca176d5f1ccba3ce188a546d28	Trojan.Win64.KILLAV.THBBHBE (KILLAV parchado)
e00293ce0eb534874efd615ae590cf6aa3858ba4	HackTool.Win32.PowerRun.THBBHBE (PowerRun)

Indicador (SHA-256)	Fuente / Tipo
22b38dad7da097ea03aa28d0614164cd25fafeb1383dbc15047e34c8050f6f67	Microsoft (Storm-2697) - muestra asociada

Artefactos en host

Artefacto	Valor / Descripción
Extensión de cifrado	.7mtzh (también reportadas .ujuopo en otras muestras)
Nota de rescate	README-GENTLEMEN.txt



Artefacto	Valor / Descripción
Herramientas anti-AV	All.exe, Allpatch2.exe, PowerRun.exe
Driver vulnerable	ThrottleBlood.sys
Acceso remoto / C2	AnyDesk
Exfiltración	WinSCP (C:\ProgramData\WinSCP.exe)
Estancamiento de datos	C:\ProgramData\data
Parámetro de ejecución	--password (clave de 8 bytes)

Consultas de cacería - Trend Vision One (Search App)

Para clientes de Trend Vision One, las siguientes consultas permiten cazar la actividad asociada al cifrado y a la nota de rescate:

```
eventSubId: 106 AND processCmd: /--password\s+(\w{8})\b/ AND objectFilePath: .7mtzhh
eventSubId: 101 AND processCmd: /--password\s+(\w{8})\b/ AND objectFilePath: README-
GENTLEMEN.txt
```

Recomendaciones

- Parchear con carácter de emergencia los dispositivos perimetrales expuestos a Internet, tratando FortiOS CVE-2024-55591 y vulnerabilidades VPN similares como incidentes, no como mantenimiento programado. Verificar exposición de FortiGate en el portafolio mediante FortiRecon (EASM).
- Ante cualquier infección por infostealer que involucre credenciales corporativas, tratarla como una brecha: revocar e invalidar sesiones de inmediato y forzar cambio de contraseñas.
- Eliminar la exposición directa de RDP a Internet y exigir MFA en todas las interfaces administrativas.
- Endurecer Active Directory frente a ZeroLogon (CVE-2020-1472) y PetitPotam; revisar cuentas privilegiadas y de servicio (incluida cualquier cuenta fortigate de dominio).



- Migrar los accesos de alto valor a autenticación respaldada por hardware o passkeys que no produzcan cookies de sesión reutilizables, dado que las cookies robadas anulan el MFA por SMS y push.
- Bloquear la ejecución desde directorios temporales y de descargas; aplicar control de aplicaciones para restringir herramientas de acceso remoto (AnyDesk) y de transferencia (WinSCP) no autorizadas.
- Habilitar verificación de firma de drivers y alertar sobre la carga de drivers vulnerables conocidos (BYOVD).
- Segmentar la red para que un host comprometido no alcance todo el dominio; restringir y auditar accesos al recurso NETLOGON y a los controladores de dominio.

FUENTES:

- [Security Affairs - Infostealers, AI, and a 90% Affiliate Cut Fuel The Gentlemen group's Rise \(15/06/2026\)](#)
- [KELA Cyber - Inside The Gentlemen Leak \(análisis de chats internos, 2026\)](#)
- [Microsoft Security Blog - The Gentlemen ransomware: dissecting a self-propagating Go encryptor \(Storm-2697\)](#)
- [Trend Micro - Unmasking The Gentlemen Ransomware: TTPs Revealed \(IOC y MITRE ATT&CK\)](#)
- [Huntress - The Gentlemen Ransomware: Defense Evasion TTPs Uncovered](#)

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el CSIRT Salud a través de las líneas telefónicas (+57) 3168931490 - 3181553570 o mediante el correo electrónico csirtsalud@minsalud.gov.co. Nuestro equipo está disponible para brindar el acompañamiento necesario.

