I. DATOS GENERALES:

Clase de alerta: Actualización Ataque Ransomware Gentlemen
Tipo de Incidente: Uso de tareas programadas SYSTEM para el cifrado y propagación en la red
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Actualización de Ataque Ransomware Gentlemen - Figura referencial

Microsoft Threat Intelligence ha publicado una nueva actualización sobre Ransomware Gentlemen, la cual incluye detalles de su flujo de ejecución, mecanismos de evasión de defensas, esquema de cifrado y técnicas de movimiento lateral. Entre los hallazgos más relevantes se destaca el uso de tareas programadas ejecutadas con privilegios de la cuenta SYSTEM para cifrar unidades locales con privilegios elevados, así como capacidades de auto propagación de tipo gusano (worm) dentro de una red.

III. INTRODUCCIÓN

El grupo Ransomware Gentlemen inició sus operaciones a mediados de 2025 como una organización cerrada, pero posteriormente adoptó el modelo Ransomware-as-a-Service (RaaS), alquilando el malware a otros actores de amenaza conocidos como

afiliados. Como parte de su expansión, llevó a cabo actividades de reclutamiento dentro del ecosistema cibercriminal, incluyendo el foro BreachForums, donde buscó incorporar pentesters maliciosos e intermediarios de acceso inicial (Initial Access Brokers - IABs).

Sus operaciones emplean una estrategia de doble extorsión, que combina el cifrado de los sistemas comprometidos con la exfiltración de información sensible, incrementando la presión sobre las víctimas para que paguen el rescate a cambio de la recuperación de los datos y la no divulgación de la información robada.

Microsoft cataloga a los responsables de administrar la plataforma RaaS de Ransomware Gentlemen bajo el identificador Storm-2697. Paralelamente, en foros clandestinos, un actor de amenaza presuntamente de origen ruso, conocido por los alias zeta88 y "hastalamuerte", se presenta como una figura de liderazgo vinculada a la gestión y coordinación de esta operación cibercriminal.

Ransomware Gentlemen desarrollado en Go y protegido mediante técnicas de ofuscación con Garble para evadir el análisis y dificultar la ingeniería inversa, el ransomware está diseñado para comprometer entornos Windows y maximizar el impacto de la operación mediante capacidades de movimiento lateral acelerado. El malware emplea un esquema criptográfico híbrido basado en Curve25519 y XChaCha20, permitiendo el intercambio seguro de claves y el cifrado eficiente de archivos, lo que reduce significativamente las posibilidades de recuperación de la información sin acceso a las claves criptográficas utilizadas durante el proceso de cifrado.

Las operaciones de Ransomware Gentlemen se han dirigido principalmente a organizaciones de los sectores manufacturero, industrial, tecnológico, financiero, salud, construcción e infraestructura crítica, con actividad observada en Europa, Asia-Pacífico y Sudamérica, especialmente en Reino Unido, Alemania, Brasil, Francia, India y Japón.

IV. VECTOR DE ATAQUE

Microsoft Threat Intelligence presenta un análisis detallado sobre el cifrador de Ransomware Gentlemen, que incluye: su usage prompt, flujo de ejecución, escalamiento de privilegios y persistencia empleando el uso de tareas programadas, el diseño del cifrado y las técnicas de movimiento lateral.

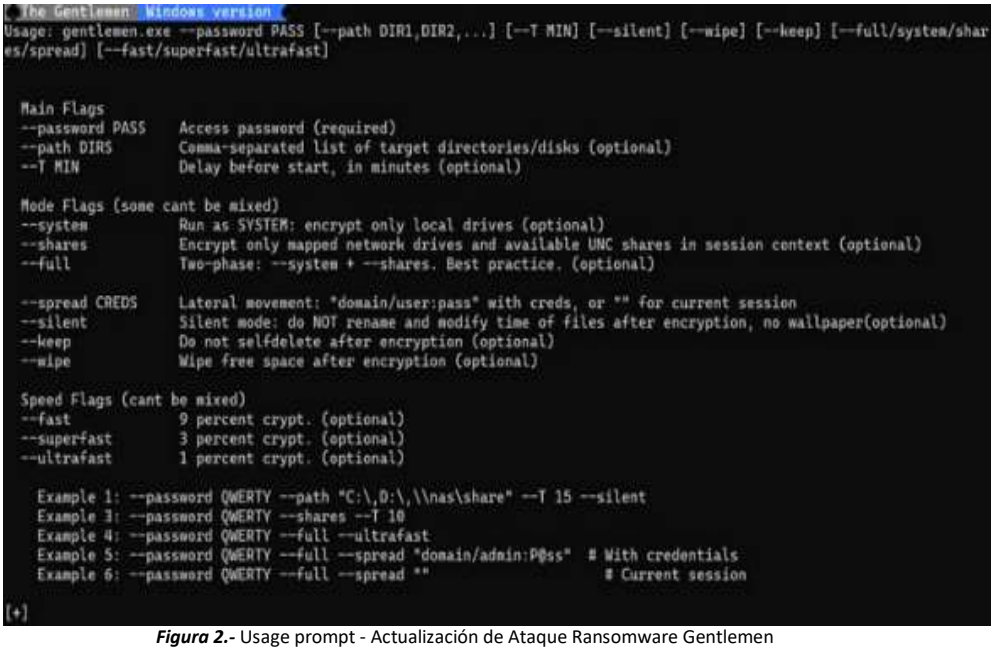

Figura 2.- Usage prompt - Actualización de Ataque Ransomware Gentlemen

Los operadores de Ransomware Gentlemen controlan el cifrador mediante parámetros de línea de comandos, en este punto requiere una contraseña para su ejecución junto a parámetros opcionales permiten al operador especificar el alcance del cifrado, la velocidad, el movimiento lateral y los comportamientos posteriores al cifrado.

El usage prompt de Ransomware Gentlemen recoge todos los parámetros disponibles, junto con sus descripciones y ejemplos

Parámetros de líneas de comandos	Descripción
--password <password>	Contraseña de acceso obligatoria (específica de la compilación)
--path <list of paths>	Lista de directorios de destino o rutas de archivos separados por comas
--T <minutes>	Delay en minutos antes de que comience el cifrado de archivos.
--silent	Modo silencioso. Desactiva el cambio de nombre de los archivos, la modificación de las marcas de tiempo tras el cifrado y la configuración del fondo de escritorio.
--system	Cifra los archivos como SYSTEM, centrándose únicamente en las unidades locales.

--shares	Cifra únicamente las unidades de red asignadas y los recursos compartidos UNC (Universal Naming Convention) disponibles.
--full	Cifrado en dos fases mediante el reinicio del proceso en dos procesos independientes: uno con el parámetro --system para las unidades locales y otro con el parámetro --shares para los recursos compartidos de red.
--spread <domain/user:password>	Habilitar la autopropagación. Aceptar credenciales para el movimiento lateral. Si no se proporcionan credenciales, se utiliza el token de la sesión actual para el movimiento lateral.
--ultrafast	Cifrar el 0,3 % por fragmento (aprox. 0,9 % en total para archivos grandes).
--superfast	Cifrar el 1 % por fragmento (aprox. 3 % en total para archivos grandes)
--fast	Cifrar el 3 % por fragmento (aprox. 9 % en total para archivos grandes)
--keep	Desactiva la autodestrucción una vez finalizada el cifrado del archivo
--wipe	Borrar el espacio libre en disco tras el cifrado

Tabla 1.- Parámetros de Usage prompt- Actualización de Ataque Ransomware Gentlemen

Pre-cifrado

Antes de su ejecución el malware valida el argumento ***--password*** comparándolo con una contraseña inmersa en el binario (en la muestra analizada por Microsoft la contraseña esperada era 9VoAvR7G). Si el valor no coincide, muestra el mensaje "bad args" y finaliza su ejecución. Este mecanismo actúa como una medida básica de autenticación para restringir el uso del cifrador a operadores autorizados; sin embargo, al basarse en una comparación estática, puede identificarse y eludirse mediante análisis del binario.

El parámetro ***--full*** parece ser el modo de funcionamiento previsto para el cifrado completo de los archivos en el dispositivo infectado. Su ejecución, hace que el malware genere dos procesos hijos de sí mismo:

- ***--system***, para cifrar volúmenes locales bajo una tarea programada con privilegios de SYSTEM.
- ***--shares***, para cifrar recursos compartidos de red.

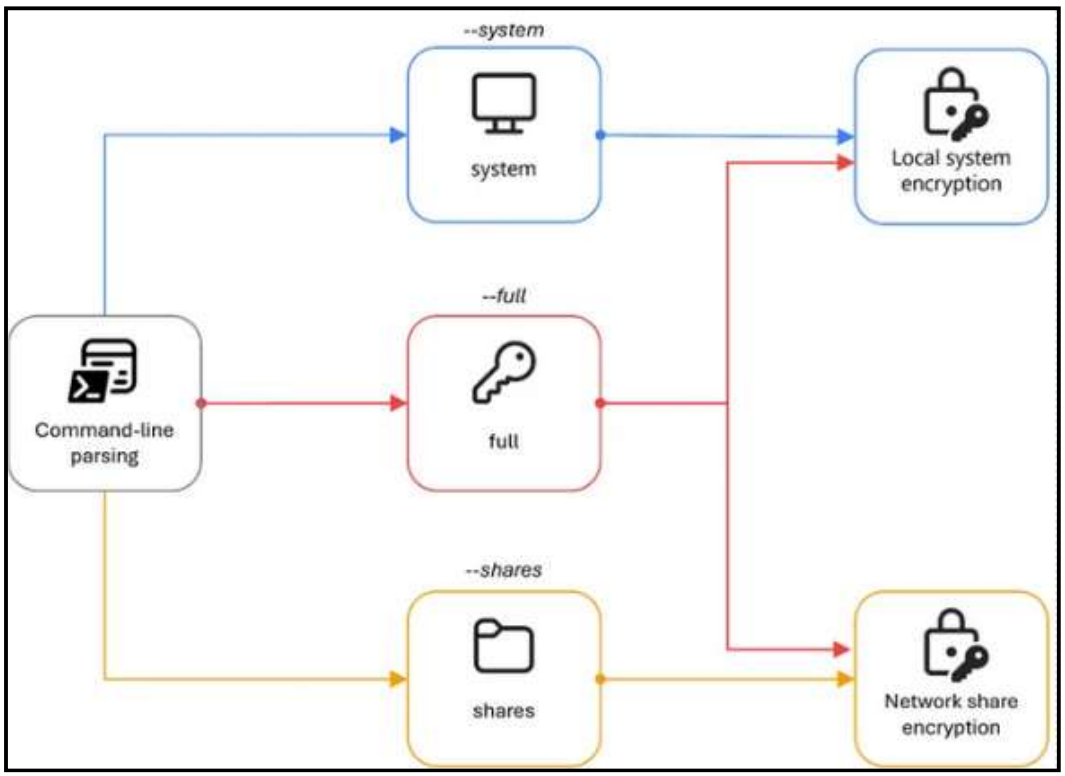

Figura 3.- Parâmetros de línea de comandos de modo de cifrado - Actualización de Ataque Ransomware Gentlemen

Escalamiento de Privilegios

Al utilizar el argumento **--system**, Ransomware Gentlemen crea la tarea programada temporal **gentlemen_system** para ejecutarse bajo la cuenta SYSTEM, eliminando cualquier tarea previa con el mismo nombre. La tarea puede activarse de inmediato o tras un retraso definido mediante el argumento ***--T***, permitiendo al malware operar con los máximos privilegios de Windows. Dentro de este contexto de tarea programada, el malware establece la variable de entorno LOCKER_BACKGROUND=1, utilizada como indicador interno para identificar que el proceso opera como un trabajador de cifrado en segundo plano con privilegios elevados

Persistencia

El cifrador puede garantizar su persistencia mediante dos mecanismos: tareas programadas y claves del Registro de Windows:

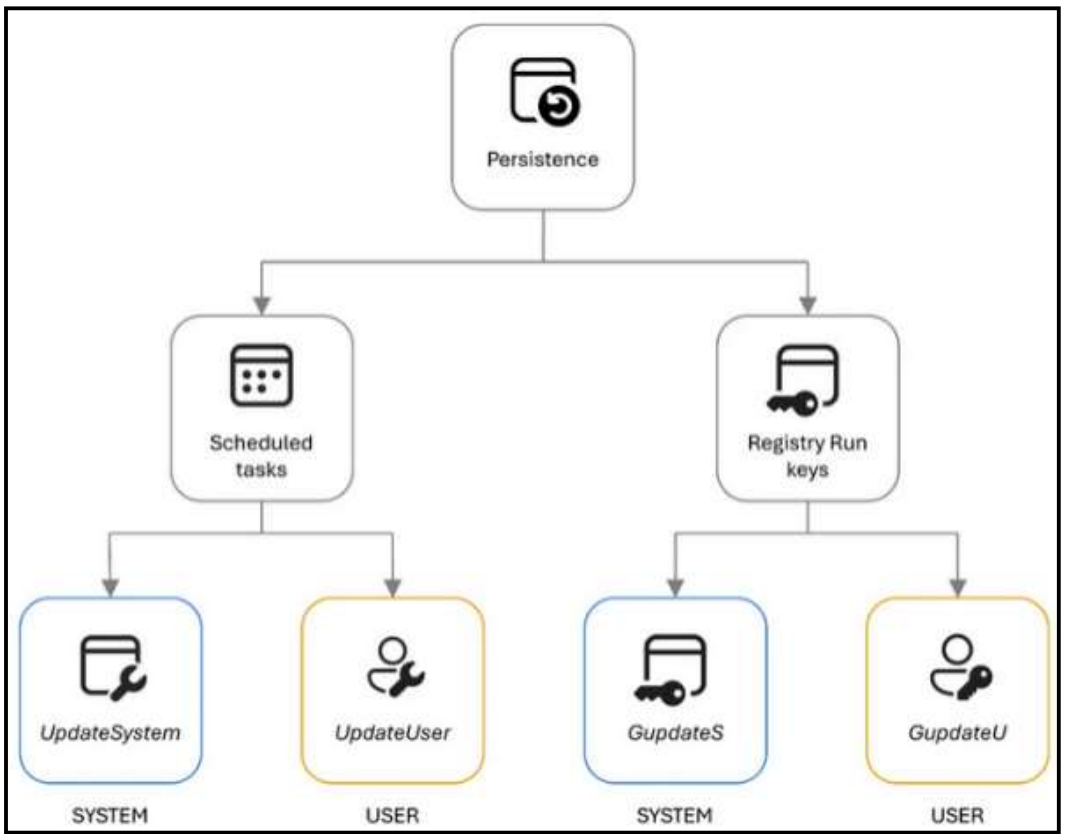

Figura 4.- El mecanismo de persistência - Actualización de Ataque Ransomware Gentlemen

- Uso de tareas programadas

Ransomware Gentlemen inicialmente elimina cualquier tarea existente de nombre **UpdateSystem** o **UpdateUser** para evitar conflictos o duplicidades. Posteriormente, crea ambas tareas programadas con el fin de permitir la ejecución automática del binario tras el reinicio del sistema.

La tarea **UpdateSystem** ejecuta el payload bajo la cuenta SYSTEM, mientras que **UpdateUser** lo ejecuta en el contexto del usuario que haya iniciado sesión. Este enfoque incrementa la probabilidad de que el ransomware continúe operando después de un reinicio, independientemente de si existe una sesión de usuario activa. Además, la ejecución bajo la cuenta SYSTEM permite que el malware disponga de los máximos privilegios disponibles en Windows cuando la tarea correspondiente es activada.

- De claves del Registro

Gentlemen Ransomware actualiza los valores de registro de:

GupdateS en HKEY_LOCAL_MACHINE (HKLM) proporciona persistencia en todo el dispositivo, lo que permite que el malware se ejecute al inicio para todos los usuarios y **GupdateU** en HKEY_CURRENT_USER (HKCU) proporciona persistencia a nivel de usuario dentro del perfil actual.

De esta forma, configura rutas de ejecución automática tanto a nivel del sistema como del usuario, incrementando la resiliencia de sus mecanismos de persistencia.

Recorrido de volúmenes y directorios

Para enumerar todos los volúmenes disponibles en el sistema, el malware ejecuta comandos de PowerShell que consultan Windows Management Instrumentation (WMI) con el fin de obtener todos los volúmenes montados con letra de unidad asignada. Asimismo, intenta identificar volúmenes compartidos de clúster (CSV).

Adicionalmente, realiza una rutina de enumeración secundaria recorriendo las letras de unidad de la A a la Z y verificando su existencia en el sistema. Este método permite identificar volúmenes que podrían no ser recuperados mediante consultas WMI, maximizando la visibilidad de posibles objetivos de cifrado.

Recorrido por recursos compartidos de red

Cuando se utiliza el parámetro ***--shares***, el malware amplía la búsqueda hacia recursos compartidos de red. Para ello, sondea las letras de unidad de la A a la Z con el objetivo de identificar unidades de red asignadas y acceder a los recursos compartidos disponibles para su posterior procesamiento.

Esquema criptográfico (Cifrado de archivos)

Ransomware Gentlemen utiliza un diseño criptográfico híbrido que combina la criptografía de curva elíptica Curve25519 con el cifrado de flujo XChaCha20 para lograr un cifrado por archivo eficiente y seguro.

Para cada archivo, el malware realiza la siguiente secuencia de operaciones:

- Genera un par de claves Curve25519 efímeras únicas, compuesto por una clave privada generada aleatoriamente y su clave pública correspondiente
- Calcula el secreto compartido de curva elíptica Diffie–Hellman (ECDH) entre la clave privada efímera y la clave pública integrada del operador.
- Utiliza el secreto compartido resultante como clave XChaCha20 y deriva el nonce a partir de los primeros 24 bytes de la clave pública efímera.
- Cifra el contenido del archivo utilizando XChaCha20 con esta combinación de clave y nonce.
- Añade la clave pública efímera codificada en Base64 al pie del archivo para permitir la posterior reconstrucción de la clave durante el descifrado.

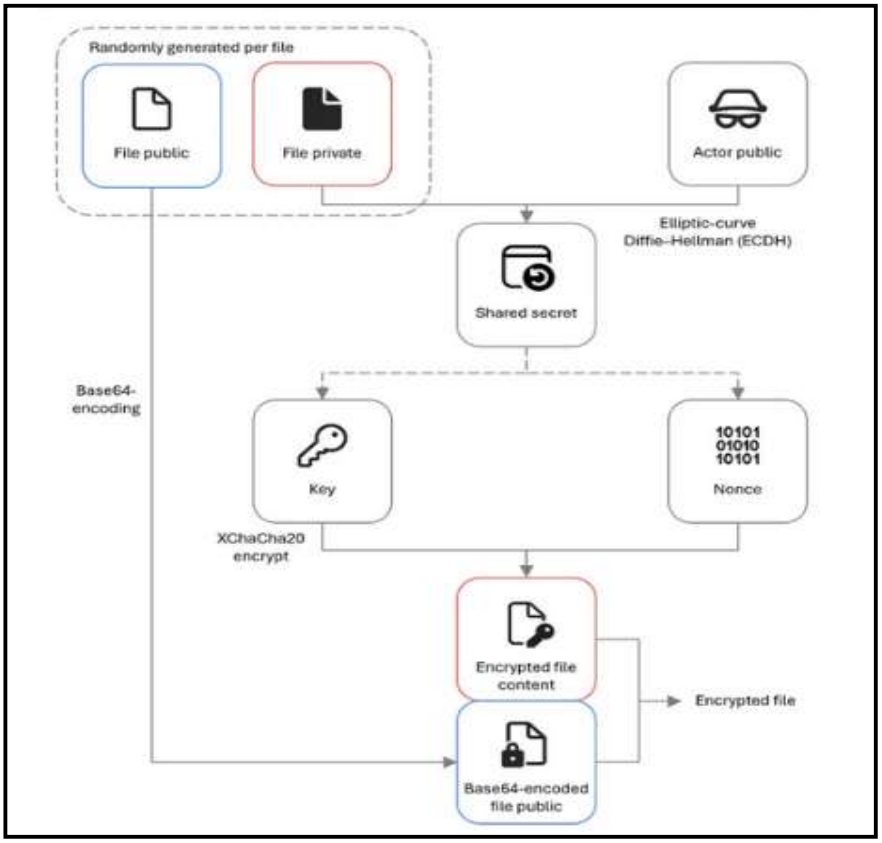

Figura 5.- El mecanismo de cifrado de archivos - Actualización de Ataque Ransomware Gentlemen

Auto-propagación

El parámetro ***--spread*** habilita la capacidad de auto propagación del malware, transformándolo en un gusano (worm) capaz de propagarse automáticamente por la red e instalar su cifrador en sistemas accesibles. Para el movimiento lateral, puede utilizar credenciales explícitas en formato **dominio/usuario:contraseña** o reutilizar el token de autenticación de la sesión actual.

V. IMPACTO

Categoría	Sistemas/Servicios Afectados
Sistemas Operativos	Microsoft Windows, Windows Server 2016, Windows Server 2019 y otras versiones de Windows.
Recursos de Red	Unidades de red mapeadas, recursos compartidos SMB y recursos compartidos UNC.
Virtualización	Hyper-V, Docker y servicios asociados de virtualización.
Bases de Datos	Microsoft SQL Server, MySQL, MariaDB, PostgreSQL y Oracle.
Correo Electrónico	Microsoft Outlook, Thunderbird y Microsoft Exchange.
Aplicaciones de Oficina	Microsoft Excel, Word, PowerPoint, Access, OneNote, Visio y Publisher.
Sistemas de Respaldo	Veeam, Backup Exec, Acronis, Commvault y otras soluciones de respaldo.
Seguridad	Soluciones EDR, antivirus y herramientas de protección de endpoints.
Acceso Remoto	TeamViewer, AnyDesk y otras herramientas de administración remota.
Aplicaciones Empresariales	SAP y aplicaciones corporativas que mantengan archivos o bases de datos en uso.

Tabla 2.- Sistemas/Servicios Afectados - Actualización de Ataque Ransomware Gentlemen

VI. INDICADORES DE COMPROMISO

Indicadores de compromiso		
Indicador	**Tipo**	**Descripción**
22b38dad7da097ea03aa28d0614164cd25fafeb1383dbc15047e34c8050f6f67	SHA-256	Cifrador ransomware caballeros
078163d5c16f64caa5a14784323fd51451b8c831c73396b967b4e35e6879937b	SHA-256	binario PsExec

fe1033335a045c696c900d435119d210361966e2fb5cd1ba3382608cfa2c8e68	SHA-256	Fondo de pantalla para caballeros (archivo bitmap)
Nombre de archivo	README-GENTLE-MEN.txt	Nota de rescate depositada en cada directorio cifrado
Extensión	.umc16h	Extensión añadida a todos los archivos cifrados
Nombre de archivo	gentle-men.bmp	Fondo de pantalla depositado en %TEMP% tras el cifrado
Tarea programada	gentle-men_system	Tarea con privilegios SYSTEM creada para el cifrado elevado
Tarea programada	UpdateSystem	Persistencia: ejecuta el payload como SYSTEM al inicio
Tarea programada	UpdateUser	Persistencia: ejecuta el payload como usuario actual al inicio
Clave de registro	GupdateS (HKLM)	Persistencia autorun a nivel de sistema
Clave de registro	GupdateU (HKCU)	Persistencia autorun a nivel de usuario
Ruta de archivo	C:\Temp\psexec.exe	Binario PsExec depositado para movimiento lateral
Nombre de archivo	wipefile.tmp	Archivo temporal usado para borrar el espacio libre en disco
Variable de entorno	LOCKER_BACKGROUND=1	Señala ejecución del cifrado en segundo plano con privilegios completos
Password fija	9VoAvR7G	Contraseña de autenticación del operador específica de la compilación incluida en la muestra analizada

Tabla 3.- Indicadores de Compromiso - Actualización de Ataque Ransomware Gentlemen

VII. RECOMENDACIONES:

- Implementar autenticación multifactor (MFA) en accesos remotos y cuentas privilegiadas.
- Mantener sistemas operativos, aplicaciones y soluciones de seguridad completamente actualizados.

- Restringir la exposición de servicios remotos (RDP, VPN, SMB, SSH) a Internet.
- Aplicar el principio de mínimo privilegio y revisar periódicamente las cuentas administrativas.
- Implementar soluciones EDR/XDR con capacidades de detección y respuesta ante ransomware.
- Monitorear intentos de acceso no autorizados, movimientos laterales y uso anómalo de credenciales.
- Segmentar la red para limitar la propagación de amenazas.
- Realizar copias de seguridad periódicas, aisladas y verificadas mediante pruebas de restauración.
- Capacitar a los usuarios sobre phishing e ingeniería social.
- Mantener un plan de respuesta a incidentes y recuperación ante ransomware.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

MICROSOFT (2026). *The Gentlemen ransomware: Dissecting a self-propagating Go encryptor*. https://www.microsoft.com/en-us/security/blog/2026/05/28/the-gentlemen-ransomware-dissecting-a-self-propagating-go-encryptor/

FORTIGUARD LABS (2026). *The Gentlemen Ransomware*. https://www.fortiguard.com/threat-actor/6387/the-gentlemen-ransomware

CYBER SECURITY NEWS (2026). *Ransomware Uses System Scheduled Task to Encrypt Systems and Spread Automatically*. https://cybersecuritynews.com/ransomware-uses-system-scheduled-task/

TELCONET CSIRT (2026). *Ransomware The Gentlemen utiliza tareas programadas con privilegios SYSTEM para cifrar sistemas y propagarse de forma automática en la red*. https://csirt.tel-

conet.net/comunicacion/boletines-servicios/ransomware-the-gentlemen-utiliza-tareas-programadas-con-privilegios-system-para-cifrar-sistemas-y-propagarse-de-forma-automatica-en-la-red/

ECUCERT (2026). *Alerta de Seguridad AL-2026-009 – Ransomware Gentlemen*. https://www.ecucert.gob.ec/wp-content/uploads/2026/02/Al-2026-009-Ransomware-Gentlemen.pdf

ECUCERT (2026). *Alerta de Seguridad AL-2026-015 – Grupo Ransomware Gentlemen*. https://www.ecucert.gob.ec/wp-content/uploads/2026/05/Al-2026-015-Grupo-Ransomware-Gentlemen.pdf

ECUCERT (2026). *Alerta de Seguridad AL-2026-021 – Ransomware Gentlemen (Actualización)*. https://www.ecucert.gob.ec/wp-content/uploads/2026/05/Al-2026-021-Ransomware-Gentlemen-Actualizacion.pdf