I. DATOS GENERALES:

Clase de alerta: Ataque de Ransomware
Tipo de Incidente: Cifrado de activos digitales, exfiltración de información sensible y extorsión múltiple.
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Ransomware Gentlemen - Figura referencial

El Ransomware Gentlemen es un grupo de ransomware que continúa operando activamente bajo el modelo Ransomware-as-a-Service (RaaS)**.** La amenaza mantiene el esquema de doble extorsión, combinando el cifrado de información con la exfiltración de datos confidenciales, los cuales son utilizados como mecanismo de presión contra las organizaciones afectadas.

III. INTRODUCCIÓN

El Ransomware Gentlemen es un grupo de actores experimentados ransomware observado por primera vez en una campana activa en agosto de 2025, lanzando ataques altamente adaptativos y dirigidos en 17 países con un enfoque principalmente dirigido a empresas de fabricación, construcción, atención médica, seguros y servicios al consumidor, dirigidos contra entornos Windows.

Escrito en lenguaje Go (Goland) posee diferentes variantes para entornos Windows, Linux, NAS, BSD y ESXi. Entre sus características influye un cifrado hibrido usando XChaCha20 y Curve25519 que son algoritmos criptográficos, usado para el cifrado parcial o completo mediante la generación de una clave primaria para la encriptación de archivos.

Una vez que obtiene acceso al dispositivo víctima, los atacantes exfiltran datos confidenciales, cifran archivos del sistema (extension .7mtzhh) y amenazan con publicar la información robada en sitios de fugas en la Dark Web (DLS) sino cumplen con las demandas de pago del rescate de información, este modelo de robo de datos e información y la filtración de datos se lo conoce como doble extorsión.

En septiembre de 2025 a través de un sitio de la Dark Web se observó El Ransomware Gentlemen promocionarse como un servicio (RaaS), lo que indicaba que el grupo estaba reclutando socios equipos o personas que quieran cooperar y delinear un modelo en base a sus afiliados.

Durante enero de 2026 se registraron nuevos incidentes atribuidos al Ransomware Gentlemen en organizaciones industriales de China y en entidades del sector comercial y financiero en Mauricio (África), confirmando la continuidad de sus operaciones. Asimismo, se reportó un ataque contra una institución bancaria en Irak, lo que evidencia el interés del Ransomware Gentlemen en sectores regulados.

Adicionalmente, a finales de 2025 se documentó un incidente en una empresa industrial en Polonia, donde se reportó la exfiltración de aproximadamente 1,5 TB de información, consistente con tácticas de doble extorsión.

IV. VECTOR DE ATAQUE

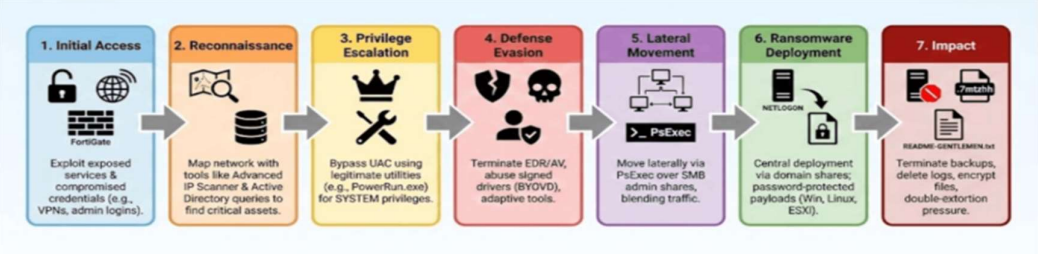

Figura 2.- Cadena de ataque de Ransomware Gentlemen

En resumen, el Ransomware Gentlemen, mantiene su cadena de ataque, partiendo:

Acceso inicial: los atacantes explotan servicios expuestos a Internet o hacen uso de credenciales administrativas compartidas, tales como interfaces de administración de firewalls y conexiones VPN expuestas, incluyendo dispositivos FortiGate.

Reconocimiento: se realiza mediante herramientas como Advanced IP Scanner y consultas a Active Directory, orientadas a la identificación de administradores de dominio y activos críticos.

Escalamiento de privilegios: utilización de PowerRun.exe para evadir el Control de Cuentas de Usuario (UAC) y ejecutar procesos con privilegios SYSTEM.

Evasión de defensas: empleo de herramientas como All.exe junto con el controlador ThrottleBlod.sys, destinadas a la finalización de procesos de antivirus y soluciones EDR.

Movimiento lateral: uso de PsExec para obtener acceso administrativo a través de SMB en otros sistemas de la red.

Despliegue del ransomware: implementación centralizada mediante recursos del dominio, como shares NETLOGON, utilizando payloads protegidos con contraseña para impedir su ejecución y análisis accidental.

Impacto: finalización de servicios de copias de seguridad, bases de datos, plataformas de virtualización y seguridad, seguida de la eliminación de registros y artefactos de recuperación.

Se cita el TTP utilizado:

Táctica	Técnica	Descripción
Acceso inicial	T1190 - Explotar una aplicación pública	Servidor FortiGate y cuenta de administrador comprometidos a través de Nmap
	T1078.002 - Cuentas válidas: Cuentas de dominio	Cuentas de dominio comprometidas
Descubrimiento	T1046 - Descubrimiento de servicios de red	Nmap ejecutado para el descubrimiento de servicios
	T1018 - Detección remota de sistemas	Escáner de IP avanzado utilizado para mapeo de red
	T1087.002 - Descubrimiento de cuenta: Cuenta de dominio	Script por lotes que consulta varias cuentas de dominio

Táctica	Técnica	Descripción
	T1069.002 - Descubrimiento de grupos de permisos: Grupos de dominios	Enumeración de grupos de dominios
	T1482 - Descubrimiento de confianza de dominio	Comandos de PowerShell utilizados para identificar PDC
Ejecución	T1059.003 - Intérprete de comandos y secuencias de comandos: Shell de comandos de Windows	Se utilizó cmd.exe para ejecutar diferentes comandos
	T1059.001 - Intérprete de comandos y scripts: PowerShell	Comandos de PowerShell utilizados para implementar antivirus y ransomware
Evasión de defensa	T1562.001 - Debilitar defensas: Deshabilitar o modificar herramientas	Servicios de seguridad detenidos que utilizan herramientas Anti-AV
	T1014 - Rootkit	Se implementó un controlador vulnerable para la terminación del proceso
	T1112 - Modificar el Registro	Cambios en el registro para debilitar la autenticación
	T1562.004 - Debilitar defensas: deshabilitar o modificar el firewall del sistema	Configuración de firewall modificada para el acceso RDP
	T1027 - Archivos o información ofuscados	Ejecución de comandos de PowerShell codificados en base64
Escalada de privilegios	T1484.001 - Modificación de la política de dominio o inquilino: Modificación de la política de grupo	Manipulación de GPO para impacto en todo el dominio
Persistencia	T1219 - Software de acceso remoto	Instalé AnyDesk para acceso remoto.
	T1112 - Modificar el Registro	Cambios en el registro para la persistencia
Movimiento lateral	T1021.002 - Servicios remotos: recursos compartidos de administración de SMB/Windows	Se utilizó PSExec para el movimiento lateral
	T1021.001 - Servicios remotos: Protocolo de escritorio remoto	RDP habilitado mediante modificación del registro
	T1021.004 - Servicios remotos: SSH	Se utilizó PuTTY para el movimiento SSH
Recopilación	T1074.001 - Datos en almacenamiento temporal: Almacenamiento temporal de datos locales	Datos almacenados en C:\ProgramData\data
	T1039 - Datos de una unidad compartida de red	Conexiones WebDAV a recursos compartidos internos
Comando y control	T1219 - Software de acceso remoto	AnyDesk utilizado para el servidor C&C
	T1071.001 - Protocolo de capa de aplicación: Protocolos web	WebDAV utilizado para el servidor C&C y el movimiento de datos

Táctica	Técnica	Descripción
Exfiltración	T1048.001 - Exfiltración mediante un protocolo alternativo: Exfiltración mediante un protocolo cifrado simétrico distinto de C2	Datos exfiltrados mediante WinSCP
Impacto	T1486 - Datos cifrados para mayor impacto	Ransomware distribuido a través del recurso compartido NETLOGON
	T1489 - Parada de servicio	Terminación de los servicios de seguridad

Tabla 1.- Cadena de ataque - Ransomware Gentlemen

V. INDICADORES DE COMPROMISO

Sitio de fugas dedicados (dls)
http://tezwsse5czllksjb7cwp65rvnk4oobmzti2znn42i43bjdfd2prqqkad[.]onion/

Tabla 2.- DLS - Ransomware Gentlemen

IP Address
104.86.182[.]8

Tabla 3.- Ip Address - Ransomware Gentlemen

Archivos Maliciosos
ThrottleBlood.sys (controlador vulnerable explotado) README-GENTLEMEN.txt (nota de rescate)
Extensión .7mtzhh en archivos cifrados

Tabla 4.- Archivos Maliciosos - Ransomware Gentlemen

Hashes
a88daa62751c212b7579a57f1f4ae8f8
408dd6ade80f2ebbc2e5470a1fb506f1
c0979ec20b87084317d1bfa50405f7149c3b5c5f
e00293ce0eb534874efd615ae590cf6aa3858ba4
7a311b584497e8133cd85950fec6132904dd5b02388a9feed3f5e057fb891d09
4c82fbafef9bab484a2fbe23e4ec8aac06e8e296d6c9e496f4a589f97fd4ab71
0002acdcbce29a01357d13dd7025b7b0d656763428b1297b950394fdd068a096
0008aaa853001623ba1e2084afbe27fed8faebad8755cb9584ce9f75b73c5a53
0019ee55db44a45c1d221e50e55d660eaeb24e1b1072087e1346903921cd8229
003381c91e50f1a2b8be7dc1a6bfaa5af12ffe4d617e4c43897f3e0d2800d0ef
0043a98418e2588dbb2a410574b6dec54a52608e83c7d4e08ea06d683f2c9913
005e8301b497a75484acfbc10a49d2e45b0bb090310972afc86d052dd3d1a339
006ac1771aaacf02c44cdcde5a2913a07a6c82f30e84b94eceb2100cc0ca0298
00a93232fb64496ab7c8b3b1a250a61e3ca936a7b797b0f2c7dc16d1c78a54bb

Hashes
00b6a47efb9049283473fe8296ee2488b790a3ba8133c4a7586aeaf9e685a9a7
00ce99391bba9ffeb9ae3baf206eea3be99d2e0cc433a9ce8a37e9f4e4f2bc5b
00e47ef59e8ce07ae591bb87f693f97955a8e2a52c32668153303943859aaaf6
00ed5f41cc3b8812c2c2cc7e3b733e19a3809076b14e4bb30c0b9f0668a1c1b1
00fd5303503ef3d91496fb14441061929fcc8651ba2abecacde86ff54ef06d07
010d6d3854182d0dfea4293eca8849906bf08718bb8781238af657f1fbde2f0a
019d420f4cc961d6a7c632e8be5f158eed94c84906dc61923e50c18724dba8af
01ee929fefc2c4fc999d231c7342996d228dce5e514a16a56abd81d3c533a8b8
023bbab9e147bbfad6e19b76f3f35bf44081c69c3c91e3d1587d3e639f7847c3
023cc6b05dd940ed3faabfa2fc1c1f6b49fc2a122a59ca2593ebf0884aea7017
0255f7d0611bdf9ae573628007a427931f8f8d04fdc857689785e63180a13fc6
026f058fe290063a612c44cac98ca9d4a2ebc6ed06e1d4c16c52d1169407f0dd
0272a75a97e742b13715a8fc69aa292760390822578500dcb73fcd5ca2b7c7e7
02ce33e0afb75d2fc969c555722d71487ce5b23a058845c94861e45866bc2f20
03391a28d58fe8a2eda9fd9302197ff086822a78cd717532962aa686844f3729
048cbd8e760a23edb4535193dcd1216cdc9ae223a9883a30ef07b9b346a07ea9
0a0cf5fdc45897e0905d0e13d2eac30e1c2804b41e2fc736df0a324e88d34746
0121141e055dc5d174d2d3079ff957db4d8b17f969134bb8ca61a491dd41b58d
0152552c9656b47fdb05dd30b8f535a7232884ee4c599780d3ee194d5c7fb923

Tabla 5.- Hashes - Ransomware Gentlemen

VI. IMPACTO

Sistemas Operativos Afectados	Tipo de Entorno
Windows	Servidores y Endpoints
Linux	Servidores
VMware ESXi	Infraestructura Virtual
BSD	Servidores
NAS (almacenamiento)	Dispositivos de Red/Backups

Tabla 6.- Sistemas Operativos Afectados - Ransomware Gentlemen

VII. RECOMENDACIONES:

- Restringir estrictamente los privilegios administrativos y auditar cambios en políticas de grupo (GPO).

- Monitorear el uso de herramientas de acceso remoto y administración fuera de horario o sin autorización.
- Bloquear la carga de controladores vulnerables y fortalecer mecanismos de protección del kernel.
- Implementar segmentación de red para limitar el movimiento lateral.
- Asegurar copias de seguridad offline o inmutables y validar periódicamente los procesos de restauración.

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:

ECUCERT (2025). Alerta de seguridad AL-2025-060 – Ransomware Gentlemen. https://www.ecucert.gob.ec/wp-content/uploads/2025/11/AL-2025-060-Ransomware-Gentlemen.pdf

SOC RADAR (2026). Dark Web Profile: The Gentlemen Ransomware. https://socradar.io/blog/dark-web-profile-the-gentlemen-ransomware/

DEVEL GROUP (2026). Emulación de adversarios: Ransomware The Gentlemen. https://devel.group/blog/emulacion-de-adversarios-ransomware-the-gentlemen/