I. DATOS GENERALES:

Clase de alerta: Ransomware
Tipo de Incidente: Actualizacion IOCs / TTP Gentlemen Ransomware
Nivel de riesgo: Alta

II. ALERTA

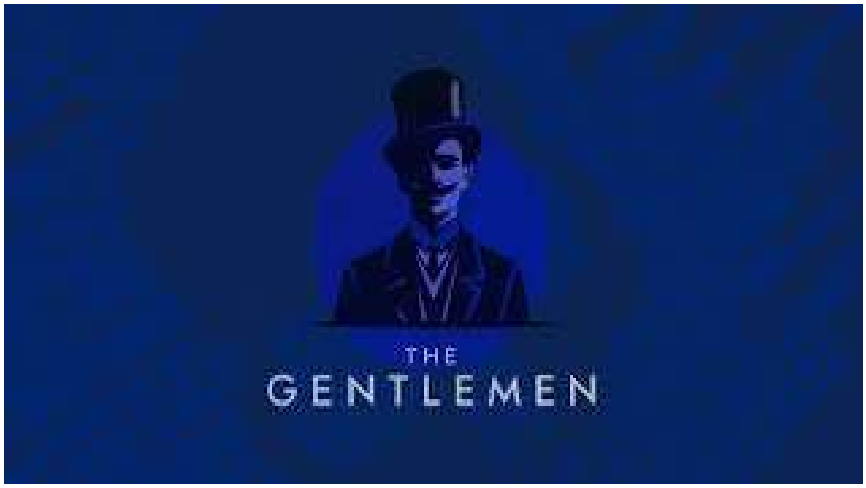

Figura 1.- Ransomware Gentlemen - Figura referencial

Actualización de IOCs y TTPs del Ransomware Gentlemen, activo y bajo el modelo Ransomware-as-a-Service (RaaS), mantiene el esquema de doble extorsión, combinando el cifrado de información, exfiltración de datos confidenciales, los cuales son utilizados como mecanismo de presión contra las organizaciones afectadas

III. INTRODUCCIÓN

Presente desde el 2025, Ransomware Gentlemen continúa a la actualidad operando activamente, expertos de ESET compañía global de ciberseguridad, reportan que en febrero de 2026 contabiliza un ataque en Argentina y en el mes de marzo en Chile, sumando ya las victimas de Brasil, Perú, Ecuador, Venezuela, Guatemala, República Dominicana, Costa Rica y Panamá.

Una breve reseña del Ransomware Gentlemen, fue 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.

El grupo se enfoca principalmente en la explotación de servicios remotos vulnerables expuestos a Internet, como RDWeb y SSL VPN, aprovechando en muchos casos credenciales débiles o configuraciones por defecto. Entre sus vectores de acceso inicial destaca la explotación de la vulnerabilidad CVE-2024-55591 en productos Fortinet (FortiOS/FortiProxy), la cual permite la omisión de autenticación y el compromiso total de dispositivos perimetrales.

IV. VECTOR DE ATAQUE

La siguiente tabla presenta una nueva actualización de las técnicas, tácticas y procedimientos (TTPs) asociados al Ransomware Gentlemen.

Táctica	Técnica ID	Nombre de la Técnica	Descripción del incidente
Acceso inicial	T1190	Exploit Public-Facing Application	Uso de vulnerabilidad en firewalls no pacheados
Ejecución	T1059.001	PowerShell	Scripts para deshabilitar defensas y propagar binarios
Persistencia	T1543.003	Windows Service	Instalación de RATs como servicios de sistemas ocultos
Evasión	T1562.001	Impair Defenses	Intentos de detener procesos de ESET/XDR
Acceso Credencial	T1003.001	LSASS Memory	Extracción de hashes y tickets Kerberos vía Mimikatz
Movimiento Lateral	T1021.004	SSH/RDP	Saltos entre el AD y las interfaces de los hipervisores.
Impacto	T1486	Data Encrypted for Impact	Cifrado masivo de máquinas virtuales en ESXi 6,5.

Tabla 1.- Técnicas y Tácticas de Ataque (TTPs) – Actualización - Ransomware Gentlemen

V. 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 2.- Sistemas Operativos Afectados - Ransomware Gentlemen

VI. INDICADORES DE COMPROMISO

Se detallan los nuevos indicadores a los que ya EcuCERT presento en anteriores documentos.

Ubicación del archivo	Nombre del archivo	HASH COMPLETO SHA-256	Función / Familia Maliciosa
\\?\C:\ProgramData\x64\	111.exe	912018AB3C6B16B39EE84F17745FF0C80A33CEE241013EC35D0281E40C0658D9	**NetWalker Ransomware:** Cifrado de archivos en staging.
\\?\C:\Users\administrator\Pictures\	111.exe	BD2C2CF0631D881ED382817AFCCE2B093F4E412FFB170A719E2762F250ABFEA4	**NetWalker Ransomware:** Copia adicional preparada para ejecucion.
\\?\C:\ProgramData\x64\	mimidrv.sys	BEE3D0AC0967389571EA8E3A8C0502306B3DBF009E8155F00A2829417AC079FC	**MimiKatz Driver:** Extracción de credenciales de la memoria LASS
\\?\C:\Users\administrator\Pictures\DCM\	in.exe	339D3458D730BF9107D5472BE935BC2CDF284C86ADE92D5F8AC4EE67EC0F0449	**Lypserat RAT:** Troyano de Acceso Remoto para persistencia C2.
\\?\C:\\Windows	VVSX2.exe	F3EA0CCCB12E574781866BEDFDA6A963238040915F82EC-DACE1619858C682E6	**Malware de Sistema:** Persistencia mediante suplantación de proceso.
\\?\C:\ProgramData\x64	mimilib.dll	D9770865EA739A8F1702A2651538F4F4DE2D92888D188D8ACE2C79936F9C2688	**MimiKatz Spooler:** Inyección de código mediante servicios de impresión.
\\?\C:\ProgramData\x64	ytvrbhvt.dll	96632F716DF30AF567DA00D3624E245D162D0A05AC4B4E7CBADF63F04CA8D3DA	**Payload Dinámico:** Librería de ejecución temporal detectada en Temp.

Tabla 3. Indicadores de Compromiso - Ransomware Gentlemen

VII. RECOMENDACIONES:

- Habilitar MFA especialmente en accesos remotos, VPN y cuentas privilegiadas, reduciendo significativamente el riesgo de accesos no autorizados.
- Mantener actualizados sistemas y aplicaciones, priorizando la remediación de vulnerabilidades críticas explotadas activamente.
- Implementar herramientas de detección y respuesta con capacidades de análisis de comportamiento para identificar actividades maliciosas en endpoints.
- Ejecutar respaldos periódicos y almacenarlos fuera de línea o en entornos segregados para evitar su compromiso.

- Supervisar continuamente servicios como VPN, RDP o RDWeb, y detectar intentos de acceso sospechosos.
- Implementar controles contra phishing y robo de credenciales, principal vector de acceso inicial.
- Configurar políticas que bloqueen comportamientos asociados a ransomware y robo de credenciales.
- Sensibilizar a los usuarios sobre phishing, enlaces maliciosos y buenas prácticas, reduciendo el riesgo del factor humano.
- Se desaconseja el pago, ya que incentiva la actividad delictiva y no garantiza la recuperación de la información.

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 (2026). AI-2026-009-Ransomware-Gentlemen. https://www.ecucert.gob.ec/wp-content/uploads/2026/02/AI-2026-009-Ransomware-Gentlemen.pdf

ECUCERT (2026). AI-2026-015-Ransomware-Gentlemen. https://www.ecucert.gob.ec/wp-content/uploads/2026/03/AI-2026-015-Grupo-Ransomware-Gentlemen.pdf

SC MEDIA (2026). The Gentlemen ransomware gang's inner workings leaked. https://www.scworld.com/brief/the-gentlemen-ransomware-gangs-inner-workings-leaked

IBM X-FORCE EXCHANGE (2026). Gentlemen ransomware – Threat Intelligence Report. https://exchange.xforce.ibmcloud.com/osint/guid:6ac6d555073d486aafea2b34d2755c04

INFOSECURITY MAGAZINE (2026). Ransomware affiliate exposes Gentlemen group operations. https://www.infosecurity-magazine.com/news/ransomware-affiliate-gentlemen/