Nro. Alerta:	AL-2025-060	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	26-nov-2025	Ransomware Gentlemen	Pág.: **1** of **9**

I. DATOS GENERALES:

Clase de alerta: Ataque de Ransomware

Tipo de Incidente: Cifrado de activos digitales y posible exfiltración de información sensible.

Nivel de riesgo: Alta

II. ALERTA

Figura 1. Ransomware Gentlemen- figura referencial

Ransomware Gentlemen es un grupo de ransomware emergente que opera bajo el modelo de *Ransomware-as-a-Service (RaaS)*. Su enfoque se basa en la doble extorsión: cifrado de archivos y amenaza de exposición pública de datos robados. Aunque su actividad ha sido principalmente internacional, se mantiene vigilancia ante posibles ataques en la región, incluyendo Ecuador.

III. INTRODUCCIÓN

Ransomware Gentlemen se caracteriza por cifrar los archivos de sus víctimas, alterando sus nombres al añadir una extensión aleatoria al final. Por ejemplo, un archivo como "1.jpg" puede transformarse en "1.jpg.7mtzhh", y "2.png" en "2.png.7mtzhh". Tras completar el cifrado, el malware deja una nota de rescate con el nombre "README-GENTLEMEN.txt", en la cual se exige un pago económico a cambio de la supuesta restauración de los datos comprometidos.

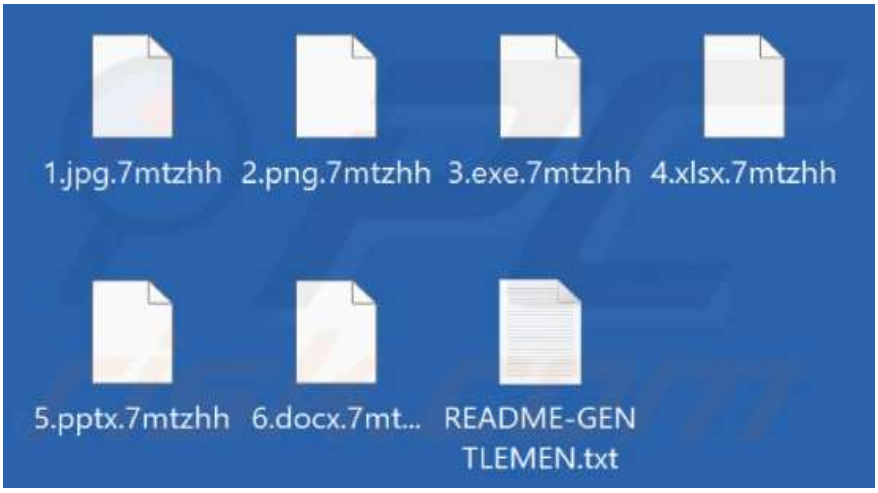
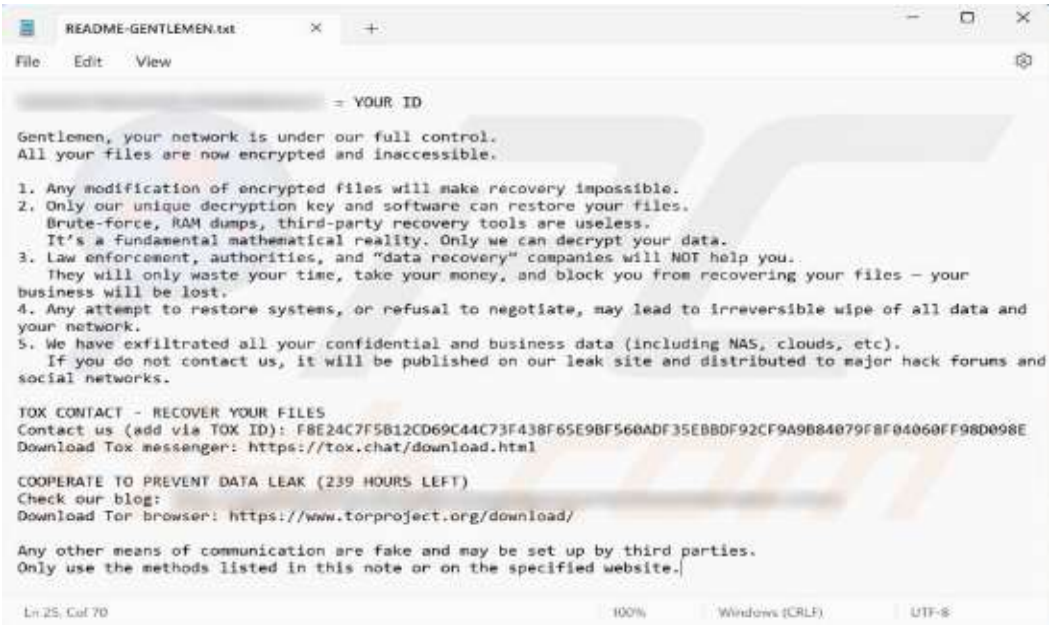


Figura 2. Archivos Cifrados - Ransomware Gentlemen

Este tipo de ataque está diseñado para generar presión sobre los usuarios afectados, buscando beneficios financieros mediante extorsión.


README-GENTLEMEN.txt

File Edit View

[redacted] = YOUR ID

Gentlemen, your network is under our full control.
All your files are now encrypted and inaccessible.

1. Any modification of encrypted files will make recovery impossible.
2. Only our unique decryption key and software can restore your files.
   Brute-force, RAM dumps, third-party recovery tools are useless.
   It's a fundamental mathematical reality. Only we can decrypt your data.
3. Law enforcement, authorities, and "data recovery" companies will NOT help you.
   They will only waste your time, take your money, and block you from recovering your files — your business will be lost.
4. Any attempt to restore systems, or refusal to negotiate, may lead to irreversible wipe of all data and your network.
5. We have exfiltrated all your confidential and business data (including NAS, clouds, etc).
   If you do not contact us, it will be published on our leak site and distributed to major hack forums and social networks.

TOX CONTACT - RECOVER YOUR FILES
Contact us (add via TOX ID): F8E24C7F5B12CD69C44C73F438F65E9BF560ADF35EBBDF92CF9A9B84079F8F04060FF98D098E
Download Tox messenger: https://tox.chat/download.html

COOPERATE TO PREVENT DATA LEAK (239 HOURS LEFT)
Check our blog:
Download Tor browser: https://www.torproject.org/download/

Any other means of communication are fake and may be set up by third parties.
Only use the methods listed in this note or on the specified website.

Ln 25, Col 70 100% Windows (CRLF) UTF-8

Figura 3. Nota de Rescate - Ransomware Gentlemen

La nota de rescate dejada por el Ransomware Gentlemen afirma que la red de la víctima ha sido completamente comprometida y que todos los archivos han sido cifrados. Advierte que cualquier intento de modificación o restauración sin la herramienta adecuada resultará en la pérdida permanente de los datos, indicando que solo los atacantes poseen la clave de descifrado necesaria.

Asimismo, se amenaza con consecuencias más graves si no se establece contacto. Según el mensaje, los actores maliciosos han exfiltrado datos sensibles y confidenciales de la organización y advierten que serán publicados en un sitio de filtraciones y distribuidos en foros como los conocidos sitios de fuga dedicados (DLS) de ciberdelincuencia y redes sociales si la víctima se niega a negociar o intenta restaurar los sistemas por su cuenta.

Como canal de contacto, se proporciona un identificador Tox, a través del cual la víctima debe comunicarse para iniciar el supuesto proceso de recuperación.

IV. VECTOR DE ATAQUE

TrendMicro empresa multinacional de ciberseguridad detalla el proceso de ataque del Ransomware Gentlemen.

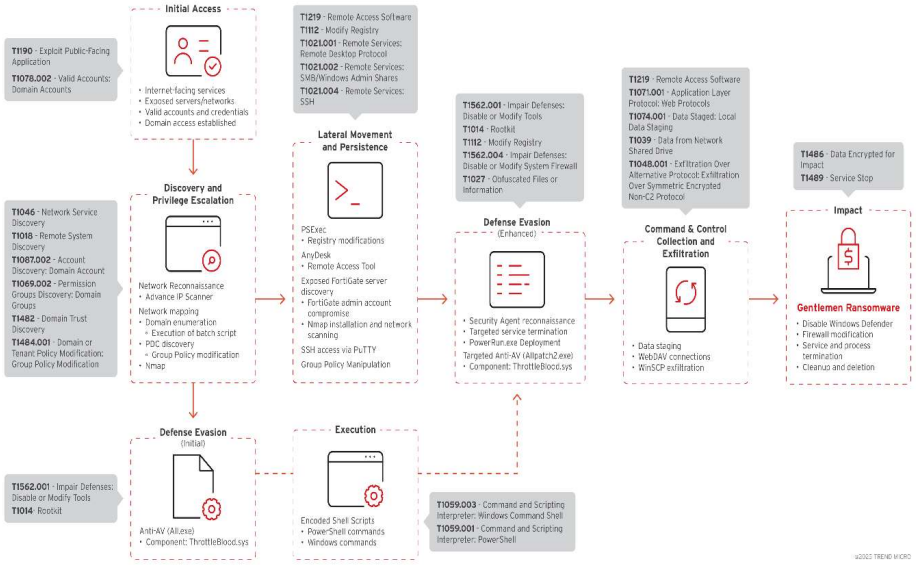


Figura 4. Cadena de Ataque - Ransomware Gentlemen

Se detallan las técnicas de ataque MITRE asociadas al Ransomware Gentlemen:

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
	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

Táctica	Técnica	Descripción
	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
Exfiltración	T1048.001 - Exfiltración mediante un protocolo alternativo: Exfiltración mediante un protocolo cifrado simétrico distinto de C2	Datos exfiltrados mediante WinSCP

Táctica	Técnica	Descripción
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. Técnicas, Tácticas y Procesos de ataque – 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

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

Tabla 3.- dls - Ransomware Gentlemen

IP Address
104.86.182[.]8

Tabla 4.- Ip Address - Ransomware Gentlemen

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

Tabla 5.- Archivos Maliciosos - Ransomware Gentlemen

Hashes
a88daa62751c212b7579a57f1f4ae8f8
408dd6ade80f2ebbc2e5470a1fb506f1
df249727c12741ca176d5f1ccba3ce188a546d28
c12c4d58541cc4f75ae19b65295a52c559570054
c0979ec20b87084317d1bfa50405f7149c3b5c5f
e00293ce0eb534874efd615ae590cf6aa3858ba4
7a311b584497e8133cd85950fec6132904dd5b02388a9feed3f5e057fb891d09

Hashes
4c82fbafef9bab484a2fbe23e4ec8aac06e8e296d6c9e496f4a589f97fd4ab71
0002acdcbce29a01357d13dd7025b7b0d656763428b1297b950394fdd068a096
0008aaa853001623ba1e2084afbe27fed8faebad8755cb9584ce9f75b73c5a53
0019ee55db44a45c1d221e50e55d660eaeb24e1b1072087e1346903921cd8229
003381c91e50f1a2b8be7dc1a6bfaa5af12ffe4d617e4c43897f3e0d2800d0ef
0043a98418e2588dbb2a410574b6dec54a52608e83c7d4e08ea06d683f2c9913
005e8301b497a75484acfbc10a49d2e45b0bb090310972afc86d052dd3d1a339
00694fdee131bb692add8f02da2ee2fc147ab2c09ecf7321fad3207976494939
006ac1771aaacf02c44cdcde5a2913a07a6c82f30e84b94eceb2100cc0ca0298
00a93232fb64496ab7c8b3b1a250a61e3ca936a7b797b0f2c7dc16d1c78a54bb
00b6a47efb9049283473fe8296ee2488b790a3ba8133c4a7586aeaf9e685a9a7
00ce99391bba9ffeb9ae3baf206eea3be99d2e0cc433a9ce8a37e9f4e4f2bc5b
00e47ef59e8ce07ae591bb87f693f97955a8e2a52c32668153303943859aaaf6
00ed5f41cc3b8812c2c2cc7e3b733e19a3809076b14e4bb30c0b9f0668a1c1b1
00fd5303503ef3d91496fb14441061929fcc8651ba2abecacde86ff54ef06d07
010d6d3854182d0dfea4293eca8849906bf08718bb8781238af657f1fbde2f0a
019d420f4cc961d6a7c632e8be5f158eed94c84906dc61923e50c18724dba8af
01bfc830626191cffe8b35a2e61b8545c38203674a4f8bf6805d89a50434ecf5
01ee929fefc2c4fc999d231c7342996d228dce5e514a16a56abd81d3c533a8b8
0208ef60699014a57b58eac363973dbe333b94aa430c1b1443f91615a941bfce
0238e0341dc7818d1a61f7f1017b659b7bc82f02e7945eaf9d0ab7889677b559
023bbab9e147bbfad6e19b76f3f35bf44081c69c3c91e3d1587d3e639f7847c3
023cc6b05dd940ed3faabfa2fc1c1f6b49fc2a122a59ca2593ebf0884aea7017
0255f7d0611bdf9ae573628007a427931f8f8d04fdc857689785e63180a13fc6
026f058fe290063a612c44cac98ca9d4a2ebc6ed06e1d4c16c52d1169407f0dd
0272a75a97e742b13715a8fc69aa292760390822578500dcb73fcd5ca2b7c7e7
02ce33e0afb75d2fc969c555722d71487ce5b23a058845c94861e45866bc2f20
03391a28d58fe8a2eda9fd9302197ff086822a78cd717532962aa686844f3729
03437abbfa60bc0e268ea8098a5e80585ee8b7842b470092471bc6434d39666c
048cbd8e760a23edb4535193dcd1216cdc9ae223a9883a30ef07b9b346a07ea9
0a0cf5fdc45897e0905d0e13d2eac30e1c2804b41e2fc736df0a324e88d34746
0121141e055dc5d174d2d3079ff957db4d8b17f969134bb8ca61a491dd41b58d
0152552c9656b47fdb05dd30b8f535a7232884ee4c599780d3ee194d5c7fb923

Tabla 6.- Hashes - Ransomware Gentlemen

VII. RECOMENDACIONES:

- Asegurar que los accesos elevados se otorguen únicamente bajo necesidad operativa, utiliza mecanismos de acceso temporal (Just-In-Time) y revisa regularmente las políticas de grupo para detectar modificaciones inusuales.

- Establecer políticas de uso controlado para herramientas administrativas remotas, como AnyDesk, y mantén un control estricto sobre los controladores permitidos dentro del entorno.

- Implementa herramientas avanzadas de detección y respuesta (EDR/XDR), vigila intentos de desactivación de software de seguridad y alerta sobre movimientos de archivos cifrados inusuales.

- Utiliza segmentación de red para dificultar la propagación del ataque e incorpora sistemas de prevención de fuga de datos (DLP) para monitorear actividades sospechosas de exfiltración.

- Realiza copias de seguridad con regularidad, almacénalas fuera de línea y efectúa simulacros de restauración para garantizar una recuperación oportuna ante un incidente de 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:

TREND MICRO. (2025). Unmasking the Gentlemen Ransomware. Trend Micro Research. https://www.trendmicro.com/en_us/research/25/i/unmasking-the-gentlemen-ransomware.html

HOOKPHISH. (2025). Ransomware Group “TheGentlemen” Hits Ecuacorriente S.A. HookPhish. https://www.hookphish.com/blog/ransomware-group-thegentlemen-hits-ecuacorriente-s-a/?utm_source

CYBERSECURITY NEWS. (2025). The Gentlemen Ransomware Group. https://cybersecuritynews.com/the-gentlemen-ransomware-group/

ASAASERADIO. (2025). The Gentlemen Ransomware Group Emerges With Dual Extortion Tactics and Driver Abuse. https://asaaseradio.com/the-gentlemen-ransomware-group-emerges-with-dual-extortion-tactics-and-driver-abuse/

PCRISK. (2025). Gentlemen Ransomware – Removal Guide. https://www.pcrisk.com/removal-guides/33845-gentlemen-ransomware

HIVE PRO. (2025). The Gentlemen Ransomware: A Rising Global Cyber Threat. https://hivepro.com/threat-advisory/the-gentlemen-ransomware-a-rising-global-cyber-threat/

WATCHGUARD. (2025). Gentlemen – Ransomware Tracker. https://www.watchguard.com/es/wgrd-security-hub/ransomware-tracker/gentlemen