I. DATOS GENERALES:

Clase de alerta: Ransomware
Tipo de Incidente: Compromiso de sistemas mediante técnicas de cifrado de información, exfiltración de datos y extorsión asociada
Nivel de riesgo: Alta

II. ALERTA

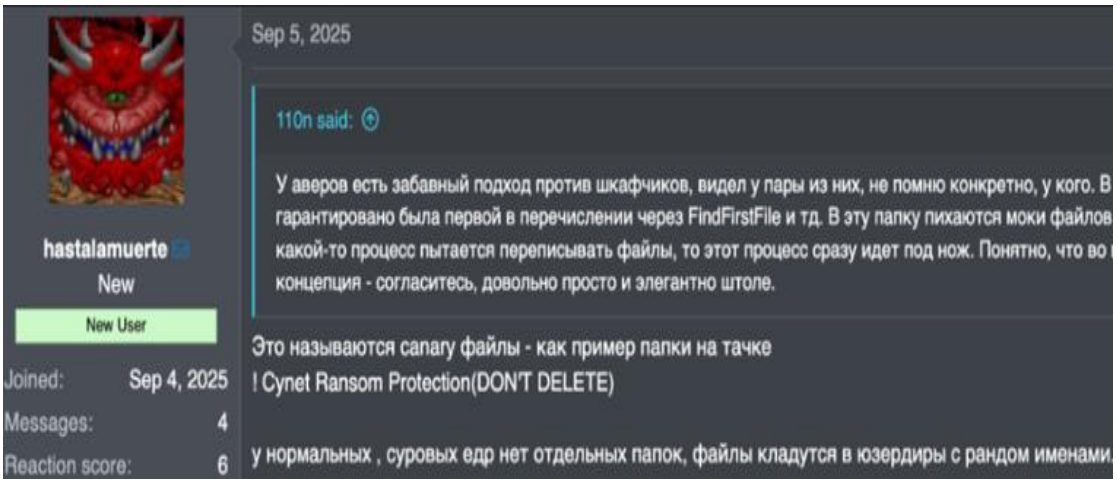

Figura 1.- Ransomware Gentlemen - Figura referencial

Un afiliado del grupo de Ransomware Gentleman, identificado como “hastalamuerte”, ha revelado detalles operativos del grupo, proporcionando información sobre sus tácticas, técnicas y procedimientos (TTP), así como evidenciando disputas internas entre los miembros del esquema RaaS.

III. INTRODUCCIÓN

La operación de Ransomware Gentleman, que surgió tras una disputa con el grupo Qilin ransomware, ha sido recientemente expuesta luego de que un afiliado y administrador de origen ruso, identificado como “hastalamuerte”, revelara información interna del grupo.

Entre los datos filtrados, se detalla que el actor proporcionaba a los afiliados recursos para facilitar intrusiones, incluyendo dispositivos comprometidos, herramientas de evasión de soluciones AV/EDR y scripts automatizados. No obstante, los problemas de

seguridad operativa dentro del grupo han generado preocupaciones entre sus miembros, evidenciadas en conflictos con otro actor de amenaza conocido como “Devman”, lo que sugiere una escalada de tensiones dentro del ecosistema de ciberdelincuencia. Tras este incidente, una investigación reciente de Group-IB (Empresa líder en ciberseguridad, inteligencia de amenazas y prevención de fraudes con sede en Singapur), proporcionaba el 19 de marzo una visión detallada sobre el funcionamiento de Ransomware Gentleman bajo el modelo de ransomware como servicio (RaaS), incluyendo su infraestructura, métodos de ataque y relaciones con afiliados.

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.

Adicionalmente, el grupo mantiene una base de datos de aproximadamente 14.700 dispositivos FortiGate comprometidos a nivel global y ha validado credenciales obtenidas mediante ataques de fuerza bruta para al menos 969 instancias de VPN. Asimismo, emplea técnicas avanzadas de evasión de defensas, como el método Bring Your Own Vulnerable Driver (BYOVD), con el fin de deshabilitar soluciones de seguridad EDR/AV a nivel del kernel.

IV. VECTOR DE ATAQUE

El análisis cubre en detalle los TTP (tácticas, técnicas y procedimientos) de Ransomware Gentleman, desde el acceso inicial hasta las fases de cifrado y extorsión de datos. El grupo emplea una variedad de técnicas, incluyendo la explotación de aplicaciones expuestas a Internet, ataques de fuerza bruta sobre credenciales, el uso de scripts en PowerShell y Python para la ejecución de payloads, así como el uso de tareas programadas para mantener persistencia.

Asimismo, los actores realizan robo de credenciales mediante técnicas de credential dumping del sistema operativo y la extracción de credenciales almacenadas en aplicaciones, como Veeam Backup & Replication**.**

Entre los principales vectores de ataque destacan el acceso inicial y los ataques de fuerza bruta.

Acceso inicial

Los actores maliciosos llevaron a cabo campañas de reconocimiento dirigidas a interfaces de administración de dispositivos FortiGate expuestas a Internet. Durante esta fase, explotaron la vulnerabilidad CVE-2024-55591, enviando solicitudes especialmente diseñadas a la consola del firewall.

Esta explotación no corresponde a un único fallo, sino a una cadena de vulnerabilidades críticas:

1. **Establecimiento de WebSocket sin autenticación:** permite crear una conexión sin validación previa.

2. **Abuso de parámetros especiales:** uso del parámetro local_access_token para evadir controles de sesión.

3. **Condición de carrera (race condition):** envío de solicitudes de autenticación antes del desafío del servidor.

4. **Ausencia de validación de credenciales:** el atacante puede autenticarse sin credenciales válidas, asignándose el perfil super_admin.

Como resultado, los atacantes logran la toma de control total del firewall con privilegios administrativos**.**

Con acceso de superadministrador, los actores:

- Crean cuentas backdoor (por ejemplo: *support_fortinet*, *badmin*, *forti-api*)
- Extraen la configuración del sistema (topología, credenciales y políticas)
- Establecen acceso persistente mediante SSL VPN
- Comprometen cuentas VPN existentes
- Ejecutan ataques Adversary-in-the-Middle (AiTM) para comprometer cuentas administrativas

Ataque de fuerza bruta

El equipo de inteligencia de Group-IB ha observado que afiliados de Ransomware Gentleman han comprometido aproximadamente 1.000 servicios VPN de Fortinet mediante ataques de fuerza bruta.

Estos ataques se basan en el uso de credenciales débiles o reutilizadas, lo que evidencia la falta de controles de seguridad robustos en los accesos remotos. A continuación, se muestra la lista de nombres de usuario y contraseñas habituales que los actores de amenaza utilizaban para llevar a cabo ataques de contra las VPN de Fortinet.

Usuario	Contraseñas
guest	guest
Admin	guestнепонятно
fortinet	password-whamola
test	password-whamola[.]net
vpnuser	fortinet-maritime!
admin	test-minus
forinetvpn	guest-пустая
fortinetsslvpn	test-минусвозможнонужносша
administrator	test-корпа
testtest	testtest-хз
user	guest-минус
testuser	test-непонятно
sslvpnuser	guestминус
support	test
vpnadmin	password
cli	Welcome1!
operator	123456
info	admin
vpnservice	P@ssw0rd
system	fortinet
scanner	0
sslvpn	1234
mail	4321
mailadmin	fortinetvpn
superadmin	8test
Fortinet	Welcome1
ldap	fortimanager_Access
admin1	info
	mail
	mailadmin
	p@ssw0rd
	p@ssword

	passw0rd
	password01
	password1
	postgres
	private
	public
	superadmin
	support
	svc_vpn
	sys
	systemadmin
	user
	voicemail
	vpnadmin
	vpnservice
	testtest
	vpnuser
	Password1
	systemadministrator
	training
	12345678
	user1
	fortigate
	john.doe
	testuser
	system
	123123
	secret
	guestHONEY
	Admin
	Administrator
	sslvpn
	123456789
	Fortinet
	1234567890
	ldap
	12345
	admin1

	123123123
	abcd1234
	admin123

Tabla 1.- Usuários y contraseñas maliciosas - Ransomware Gentlemen

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

Táctica	IDENTIFI-CACIÓN	Técnica	Procedimiento
Acceso inicial	T1190	Explotar una aplicación de cara al público	Explota la vulnerabilidad CVE-2024-55591 (omisión de autenticación en FortiOS/FortiProxy) mediante el envío de solicitudes WebSocket especialmente diseñadas para crear conexiones sin autenticación, abusar del parámetro local_access_token, explotar condiciones de carrera y obtener acceso de superadministrador sin validación de credenciales. Mantiene una base de datos de aproximadamente 13 400 dispositivos FortiGate explotados.
Acceso inicial	T1110.001	Fuerza bruta: Adivinación de contraseñas	Realiza ataques de fuerza bruta contra dispositivos VPN FortiGate utilizando un diccionario de nombres de usuario y contraseñas comunes.
Ejecución	T1059.001	Intérprete de comandos y scripts: PowerShell	Ejecuta scripts de PowerShell para habilitar el acceso web de Windows PowerShell (PSWA), deshabilitar las protecciones de Windows Defender, mover objetos de equipo de Active Directory entre unidades organizativas, actualizar objetos de directiva de grupo y administrar servicios.
Ejecución	T1059.006	Intérprete de comandos y scripts: Python	Implementa un script Python personalizado (user-passfort.py) para extraer credenciales de los archivos de configuración de Fortinet mediante patrones de expresiones regulares y ejecutar automáticamente NetExec (nxc) para realizar ataques de relleno de credenciales contra objetivos SMB.
Ejecución	T1053	Tarea/Trabajo programado	Crea tareas programadas mediante schtasks para ejecutar el script de exfiltración rclone.ps1 al iniciar el sistema con privilegios de SYSTEM y el nivel de ejecución MÁS ALTO, lo que garantiza la persistencia de las operaciones de robo de datos.
Persistencia	T1098	Manipulación de cuentas	Restablece las contraseñas de root de ESXi para mantener el acceso administrativo permanente a la infraestructura de virtualización. Incluye referencias a técnicas documentadas para los procedimientos de restablecimiento de contraseñas.
Persistencia	T1098.007	Manipulación de cuentas: Grupos	Agrega cuentas comprometidas o recién creadas a grupos predeterminados usando NetExec: nxc

		locales o de dominio adicionales	smb [destino] -u [usuario] -p [contraseña] -x 'net localgroup “nombre_grupo” [usuario] /add'
Persistencia	T1136.002	Crear cuenta: Cuenta de dominio	Crea cuentas de dominio con nombres como “MicrosoftSupporte” usando net user MicrosoftSupporte Password123 /add /domain, las agrega a los grupos “Administradores de dominio”, otorga acceso a Escritorio remoto y crea inicios de sesión SQL en bases de datos Veeam con privilegios db_owner.
Escalada de privilegios	T1484.001	Modificación de directiva de dominio o inquilino: Modificación de directiva de grupo	Modifica la directiva de grupo para habilitar los servicios SMB, configurar las reglas del Firewall de Windows para el uso compartido de archivos, mover los objetos de equipo de CN=Computers a las OU de destino y forzar las actualizaciones de GPO en todos los equipos del dominio mediante los comandos Invoke-GPUpdate y gpupdate /force.
Escalada de privilegios	T1068	Explotación para la escalada de privilegios	Investiga y comparte exploits, incluyendo la técnica de escalada de privilegios BadSuccessor, CVE-2025-32463 (escalada de privilegios en Linux) y CVE-2024-37085 (vulnerabilidad de ESXi). La evidencia sugiere la intención de utilizarlos en operaciones.
Evasión de defensa	T1112	Modificar el registro	Modifica las claves del registro para deshabilitar los productos de seguridad.
Evasión de defensa	T1562.001	Debilitar las defensas: Deshabilitar o modificar las herramientas.	Deshabilita Windows Defender mediante directivas de grupo y comandos de PowerShell, finaliza los procesos EDR utilizando técnicas BYOVD con controladores vulnerables y utiliza NetExec para deshabilitar la protección en tiempo real.
Evasión de defensa	T1036	Suplantación de identidad: Cambiar el nombre de las utilidades legítimas	Cambia el nombre del ejecutable RClone a "avastrclone.exe" para que parezca un software legítimo de Avast, enmascarando las actividades de exfiltración de datos y eludiendo la detección por parte de las herramientas de monitoreo de seguridad.
Evasión de defensa	T1070.001	Eliminación del indicador: Borrar los registros de eventos de Windows	Borra todos los registros de eventos de Windows usando wevtutil cl Security, wevtutil cl Application, wevtutil cl System, elimina los registros de RDP, los archivos de soporte de Defender, los archivos de Prefetch y el contenido de la Papelera de reciclaje para eliminar la evidencia forense.
Acceso con credenciales	T1003.004	Extracción de credenciales del sistema operativo: secretos de LSA	Extrae las claves de respaldo de DPAPI utilizando la herramienta dpapi.py de Impacket para obtener las claves maestras para descifrar las credenciales almacenadas.

Acceso con credenciales	T1555	Credenciales de almacenes de contraseñas	Extrae las credenciales de Veeam de la base de datos y el registro de PostgreSQL, descifra las contraseñas usando Veeam.Backup.Common.dll y explota la vulnerabilidad CVE-2023-27532.
Acceso con credenciales	T1557.001	Adversario en el medio	Fuerza la autenticación mediante métodos de coerción utilizando NetExec con el módulo coerce_plus para transmitir credenciales NTLM y eludir los controles de autenticación.
Evasión de defensa	T1222.001	Modificación de permisos de archivos y directorios	Modifica los permisos de archivo mediante icacls para otorgar acceso no autorizado a directorios y archivos protegidos.
Descubrimiento	T1087.002	Descubrimiento de cuentas: Cuenta de dominio	Enumera los equipos del dominio y prueba la conectividad utilizando PowerShell combinado con Test-Connection para identificar hosts en línea/fuera de línea y recuperar direcciones IPv4.
Descubrimiento	T1615	Descubrimiento de políticas de grupo	Descubre la configuración de directivas de grupo aplicadas mediante gpresult /r, comprueba el estado de replicación con repadmin /replsummary y repadmin /showrepl para comprender las configuraciones de seguridad del dominio e identificar los controles basados en directivas.
Movimiento lateral	T1021.002	Servicios remotos: Recursos compartidos de administración de SMB/Windows	Propaga malware a través de recursos compartidos administrativos SMB mediante NetExec y crea recursos compartidos de red abiertos con net share, otorgando acceso completo a todos.
Movimiento lateral	T1021.001	Servicios remotos: Protocolo de escritorio remoto	Se conecta a las máquinas de las víctimas a través de RDP usando mstsc /v:[objetivo] después de agregar cuentas controladas por el atacante al grupo Usuarios de Escritorio remoto a través de comandos SMB de NetExec.
Mando y control	T1572	Tunelización de protocolo	Utiliza Chisel para crear proxies SOCKS cifrados para la comunicación C2, con el fin de tunelizar el tráfico a través del puerto 443 y evadir la detección con bajas tasas de firmas antivirus.
Exfiltración	T1048	Exfiltración mediante protocolo alternativo	Extrae datos utilizando RClone con el protocolo SFTP configurado en archivos de configuración personalizados.
Impacto	T1490	Inhibir la recuperación del sistema	Detiene los servicios de copia de seguridad (Veeam, Acronis, BackupExec, etc.), las bases de datos (SQL, Oracle, MySQL, SAP, PostgreSQL) y los servicios de virtualización (vmms, vmwp, vmcompute) mediante net stop [service]. Elimina las copias de instantáneas con vssadmin delete shadows /all /quiet y wmic shadowcopy delete.
Impacto	T1486	Datos cifrados para mayor impacto	El ransomware Gentlemen cifra los datos del usuario.

Tabla 2.- 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 3.- Sistemas Operativos Afectados - Ransomware Gentlemen

VI. INDICADORES DE COMPROMISO

Tipo	Valor	Contexto
IP Address	194[.]87[.]31[.]69	Exfiltración de datos vía SFTP (puerto 2222)

Tabla 4. Indicadores de Red - Ransomware Gentlemen

Tipo	Hash
SHA256	51b9f246d6da85631131fcd1fabf0a67937d4bdde33625a44f7ee6a3a7baebd2
SHA256	3ab9575225e00a83a4ac2b534da5a710bdcf6eb72884944c437b5fbe5c5c9235
SHA256	2834114ff7e487c4ca3f50ca39f7d652dea1be98f885c388f01b6ff35309307b
MD5	d65c293efb5e6d033c83b2ac472bf0cb
MD5	42c062d6299ca9f76554441a29429404
MD5	efd5366eb7473d6f7fb97ec7ac59f09d
MD5	8901ce810f999f79c51c4d4f6c93fe6b

Tabla 5. - Hashes de Archivos - Ransomware Gentlemen

Tipo	Indicador
Nota de rescate	README-GENTLEMEN.txt
Extensión	.7mtzhh
Ejecutable	avastrclone.exe
Script	userpassfort.py
Builder	GLOCKER
Script	deploy.cmd
Script	rclone.ps1

Tabla 6.- Artefactos en el Sistema (Filesystem IoCs) - Ransomware Gentlemen

Tipo	Ruta
Temporal	C:\Windows\Temp\rclone.ps1
Programa	C:\ProgramData\AnyDesk.exe
Red	\.local\NETLOGON<nombre>.exe

Tabla 7.- Rutas del Sistema - Ransomware Gentlemen

Nombre
ThrottleBlood.sys
viragt64.sys

Tabla 8.- Drivers Maliciosos (BYOVD) - Ransomware Gentlemen

Tipo	Usuario	Contraseña
Backdoor	support_fortinet	—
Backdoor	badmin	—
Backdoor	forti-api	—
Dominio	MicrosoftSupporte	Password123
Local	oldadministrator	qc69t4B#Z0kE3

Tabla 9.- Cuentas Maliciosas - Ransomware Gentlemen

Campo	Valor
Nombre	SafeSync
Comando	powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -File C:\Windows\Temp\rclone.ps1
Trigger	ONSTART / SYSTEM / HIGHEST

Tabla 10.- Tarea Programada - 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). Al-2026-009-Ransomware-Gentlemen. https://www.ecucert.gob.ec/wp-content/uploads/2026/02/Al-2026-009-Ransomware-Gentlemen.pdf

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

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/