Nro. Alerta:	AL-2025-047	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	28-ago-2025	Ransomware Trigona	Pág.: **1** of **4**

I. DATOS GENERALES:

Clase de alerta: Incidente
Tipo de Incidente: Ransomware
Nivel de riesgo: Alta

II. ALERTA

Figura 1.- Ransomware Trigona - figura referencial

Se ha identificado una nueva variante del Ransomware Trigona dirigida a distribuciones Linux. Este malware presenta técnicas avanzadas de evasión y manipulación de archivos empleando ingeniería inversa, lo que incrementa significativamente su peligrosidad, dificulta su detección y mitigación.

III. INTRODUCCIÓN

Ransomware Trigona es una familia de ransomware activa desde junio de 2022, conocida por su enfoque de doble extorsión y su capacidad para atacar tanto sistemas Windows como Linux. Recientemente, se ha observado una evolución en sus tácticas, especialmente sobre Linux, donde emplea técnicas anti-forenses y el uso de herramientas como **r2ai.**

R2AI es la abreviatura de 2 términos, Radare2 e Inteligencia Artificial (IA), este apartado Radare2 es un framework de CLI de ingeniera inversa de código abierto y

análisis forense, con el objetivo de inspeccionar, analiza y manipular binarios (ejecutable, librerías, firmwares, etc) para entender su funcionamiento sin necesidad de tener el código fuente original.

IV. VECTOR DE ATAQUE

Ransomware Trigona gana su acceso inicial de múltiples maneras, mediante el uso de correos electrónicos de phishing dirigidos, ataques de fuerza bruta y explotación de vulnerabilidades en servicios y aplicaciones web o vulnerabilidades RDP.

Usa técnicas de ingeniería inversa, la descompilación, esto es el proceso de traducir código de bajo nivel (también llamado código maquina o binario) de vuelta a código de alto nivel (escritos en C, Java, C#, entre otros) que son legibles para los seres humanos. Todo esto con la modificación de código utilizando r2ai.

Actúa sobre distribuciones Linux modificando permisos de archivos críticos empleando el comando **chattr** (**Change Attribute**), utilizado para cambio de atributos especiales de archivos y directorios en sistemas de archivo ext2, ext3, ext4 y demás compatibles.

Este comando **chattr** permite añadir o eliminar la inmutabilidad con el parámetro o bandera(flag) "**i**", al ejecutar el comando **chattr +i** sobre el archivo malicioso impide que herramientas seguridad (antivirus, EDR) o administradores borren este archivo, con esto también facilita el cifrado de archivos posteriormente y lo que también le permite mantener su persistencia en el sistema víctima.

Ransomware Trigona puede cifrar archivos esenciales de Linux y alterar atributos del sistema para persistir y bloquear mecanismos de recuperación. El impacto abarca interrupción de servicios, pérdida de datos críticos y posibles demandas de rescate. La manipulación de flags y atributos complica la restauración y el análisis forense tras el incidente, aumentando el tiempo de recuperación y los costes para la organización.

V. IMPACTO

Sistemas Afectados
Windows Server 2016/2019, Linux (Debian, Ubuntu, CentOS)

Tabla 1.- Sistemas afectados - Ransomware Trigona

VI. INDICADORES DE COMPROMISO

Categoría	Indicador
Extensiones de archivo	.lockeda, .Trigona, .encrypted, .locked
Archivos sospechosos	turnoff.bat, DECRYPT-FILES.txt, autorun_only.hta

Hashes conocidos	SHA-256: c08a752138a6f0b... *(varía por muestra)*
Comandos maliciosos	/!autorum, /!lan, /erase, /full, /!local, /autorun_only
Direcciones TOR	http://trigona[.]onion, http://decrypt[.]trigona[.]onion
Procesos sospechosos	splashtop.exe, portscanner.exe, networkscanner.exe
Modificaciones en registro	Claves persistentes en HKCU\Software\Trigona o HKLM\System\Trigona
Comportamiento en red	Comunicación cifrada con servidores TOR, escaneo de puertos SMB

Tabla 2.- IoCs - Ransomware Trigona

VII. RECOMENDACIONES:

- Restricción de comandos críticos: Limitar el acceso al comando chattr y a herramientas de modificación de código como r2ai.
- Control de acceso: Implementar listas de control de acceso estrictas para proteger archivos y directorios sensibles.
- Auditorías regulares: Realizar auditorías periódicas de integridad de archivos y monitorear cambios inusuales en atributos de archivos.
- Actualización de sistemas: Mantener todos los sistemas y aplicaciones actualizados con los últimos parches de seguridad.
- Implementación de soluciones EDR: Utilizar soluciones de detección y respuesta en endpoints (EDR) compatibles con Linux para una supervisión continua.
- Educación y concienciación: Capacitar al personal sobre las amenazas de ransomware y las mejores prácticas de seguridad informática.

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:

SEGURIDADPY (2025). Trigona: evolución del ransomware y evasión avanzada en Linux. https://seguridadpy.info/2025/08/trigona-evolucion-del-ransomware-y-evasion-avanzada-en-linux-html/

HISPASEC UNA AL DÍA (2025). Trigona: evolución del ransomware y evasión avanzada en Linux. https://unaaldia.hispasec.com/2025/08/trigona-evolucion-del-ransomware-y-evasion-avanzada-en-linux.html

MALWARE.NEWS (2025). Linux Trigona: analysis with r2ai. https://malware.news/t/linux-trigona-analysis-with-r2ai/98299/1

CIBERNOTICIAS (2025). Trigona: evasión avanzada en sistemas Linux. https://cibernoticias.blog/2025/08/27/trigona-evasion-linux/

ECUCERT (2025). Alerta AL-2025-012: Trigona Ransomware. https://www.ecucert.gob.ec/wp-content/uploads/2025/03/AL-2025-012-TRIGONA.pdf