Nro. Alerta:	AL-2025-012	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	25-mar-2025	**TRIGONA RANSOMWARE**	Pág.: **1** of **9**

I. DATOS GENERALES:

Clase de alerta: Información

Tipo de incidente: Ransomware

Nivel de riesgo: Alto

II. ALERTA

El ransomware Trigona, inicialmente rastreado por Trend Micro como Water Ungaw, surgió en octubre de 2022. Sin embargo, los primeros binarios del ransomware se detectaron ya en junio del mismo año.

Trigona intenta extorsionar a sus víctimas con plazos intimidantes. Mediante una nota de rescate en formato *.HTA*, se les indica que ingresen su clave única para recibir instrucciones específicas. Posteriormente, se las dirige a un portal de pagos basado en TOR donde el grupo prefiere aceptar pagos en Monero (XMR).

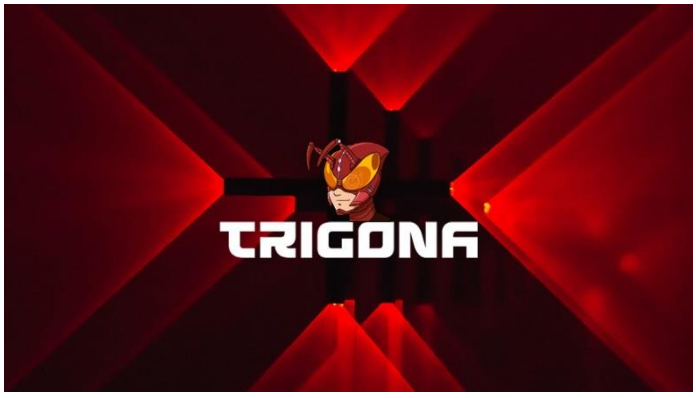

Figura 1.- Trigona
Fuente: https://www.bleepingcomputer.com/news/security/microsoft-sql-servers-hacked-to-deploy-trigona-ransomware/

III. INTRODUCCIÓN

Los métodos iniciales de distribución de las cargas útiles de Trigona varían según la campaña. Se ha observado su implementación mediante phishing selectivo y la

explotación de vulnerabilidades conocidas. Las primeras cargas útiles de Trigona basadas en Windows están escritas en Delphi y se centran en la evasión, así como en un cifrado eficiente y rápido. El cifrado de archivos se gestiona mediante una combinación de AES-256 (clave simétrica) y RSA-4112 (clave pública) en modo OFB (retroalimentación de salida).

Los datos de configuración del ransomware Trigona se integran en cada carga útil. Estos datos se cifran mediante múltiples capas de AES en modo CBC. Los archivos cifrados se modifican, añadiendo la extensión *._locked* a los archivos afectados. El malware intenta persistir mediante claves de ejecución del registro.

Además, el ransomware Trigona parece tener la capacidad de propagarse por SMB (Server Message Block). Esta capacidad se puede activar y desactivar en las generaciones actuales del ransomware Trigona. También admite argumentos adicionales de la línea de comandos.

Los siguientes comandos están disponibles en la generación actual de cargas útiles del ransomware Trigona. La mayoría se implementan en plataformas Windows y Linux.

- ***/!autorum* –** Omitir la entrada de registro de ejecución automática (persistencia)
- /!***lan*** – No intente cifrar archivos en recursos compartidos de red
- /!***local*** – No cifrar archivos locales
- /***autorun_only*** – Crear una entrada de registro para persistencia – sin cifrado
- ***/erase*** – Sobrescribir datos. Los primeros 512 KB son los predeterminados, pero esta opción se puede usar con el argumento /full.
- ***/full*** – Cifrado completo de archivos (a diferencia de los primeros 512 KB)
- ***/is_testing*** – Establece el indicador de prueba/depuración
- ***/p*** – Ruta especificada para el cifrado
- ***/path*** – Igual que /p – ruta especificada para el cifrado (recursivo)

- ***/r*** – Cifrar archivos en orden aleatorio
- ***/shdwn*** – Iniciar el apagado del sistema después del cifrado (shutdown.exe -f -s -t 00)
- ***/test_cid*** – Forzar el uso de la ID de computadora especificada (prueba)
- ***/test_vid*** – Forzar el uso de la identificación de la víctima especificada (prueba)

Los atacantes pueden usar la función /erase para simular la función de borrado. Esta opción se combina con /path o /full según lo considere oportuno. Esta opción hace que los archivos afectados sean irrecuperables.

Las notas de rescate de Trigona se guardan en el disco como how_to_decrypt.hta y funcionan como aplicaciones *.HTA* válidas. Al abrir la nota de rescate, se indica a las víctimas que copien la URL correspondiente (basada en TOR) y la clave de autorización.

IV. VECTOR DE ATAQUE:

El ransomware Trigona utiliza una amplia gama de métodos de infección y vectores de ataque, lo que le permite infiltrarse en una amplia gama de sistemas objetivo. Estos métodos suelen aprovechar vulnerabilidades y errores humanos, lo que los hace potentes y versátiles:

- **Explotación de vulnerabilidades de RDP**: los actores de Trigona con frecuencia apuntan a vulnerabilidades del Protocolo de Escritorio Remoto (RDP) sin parches y las utilizan como puerta de entrada para iniciar sus ataques.
- **Correos electrónicos de phishing**: Las campañas de correo electrónico engañosas representan otro de los vectores de ataque favoritos de Trigona. Estos correos electrónicos están diseñados para engañar a destinatarios

desprevenidos para que descarguen y ejecuten el ransomware mediante archivos adjuntos o enlaces maliciosos.

- **Ataques de fuerza bruta**: Los operadores de Trigona realizan ataques de fuerza bruta, especialmente dirigidos a credenciales débiles o predeterminadas para servidores RDP y SQL. Esta técnica proporciona acceso no autorizado a los sistemas, lo que facilita la propagación de ransomware.
- **Explotación de vulnerabilidades**: Trigona aprovecha la explotación de diversas vulnerabilidades en servicios y aplicaciones conectadas a Internet, particularmente aplicaciones web, como un medio para infiltrarse en las redes.

V. IMPACTO:

- Instalación de extensiones y software malicioso.
- Control total sobre el sistema comprometido
- Cifrado de la información

VI. INDICADORES DE COMPROMISO:

Hashes y archivos relacionados:

- 8cbe32f31befe7c4169f25614afd1778006e4bda6c6091531bc7b4ff4bf62376
  Archivo: Ransom.Win32.TRIGONA.YPDDZ

- 11b0e9673bbeb978aa9b95bcad43eb21bbe0bbaaf7e5a0e20d48b93d60204406
  Archivo: Ransom.Win32.TRIGONA.YXDDR

- eda603f4d469d017917f5d6affeb992fdf3b7971e49868ece8c38fb8e6f8b444
  Archivo: Ransom.Win32.TRIGONA.YXDDR

- c4529a061f205aaee46c219123d15059d2161df2bd7c7b738dd2a2c1ffd8d3ee
  Archivo: Ransom.Win32.TRIGONA.YXDDR

- 170fa5d29cdb562d41a054abf2a57ca29fc233805b59692a1a57ebf25449be7c
  Archivo: Ransom.Win32.TRIGONA.YXDDR
- f29b948905449f330d2e5070d767d0dac4837d0b566eee28282dc78749083684
  Archivo: Ransom.Win32.TRIGONA.THABOBC
- 197f4933680a611ad2234a22769bd079885f81956221ec0de172d5a19eab648e
  Archivo: Ransom.Win32.TRIGONA.YXDDR
- 1017fcf607a329bb6ad046181c3656b686906a0767fff2a4a3c6c569c2a70a85
  Archivo: Ransom.Win32.TRIGONA.YXDDR
- 761b78ddab55b4e561607ce5ce9d424a7aec4f1994aad988f0612b096cdd1d6d
  Archivo: Ransom.Win32.TRIGONA.YXDDR
- 097d8edb1762d7d3ded4360a9f5b4673a898937421f36853d2f5cde77e1bac93
  Archivo: Ransom.Win32.TRIGONA.YXDDR
- 4a06231957c53dee1a11ff3eb84caad082f18761aee49e72d79c7f1d32884e34
  Archivo: Ransom.Win32.TRIGONA.YXDDR
- fb128dbd4e945574a2795c2089340467fcf61bb3232cc0886df98d86ff328d1b
  Archivo: Ransom.Win32.TRIGONA.YMDBJ
- feb09cc39b1520d228e9e9274500b8c229016d6fc8018a2bf19aa9d3601492c5
  Archivo: disable-defender.exe
- f6440c5cfc1a0bf4fdc63124eef27f40be37af8f46d10aea9a645f5b084004e3
  Archivo: defoff.bat
- da0a235cd729d4aa6b209bfe1edefbeeca8fe2ae92d4e3830db7744c9393eadf
  Archivo: coba.bat
- 69f245dc5e505d2876e2f2eec87fa565c707e7c391845fa8989c14acabc2d3f6
  Archivo: mim.exe
- eeed7ce800a9714b65aaae4f1d61deb83d3f0cbcfd814372807b73c940d4bb8f

Archivo: meshagent.exe

- 4c181562c9a52be9a629522de7d46f04a490b29d673e8a2376e4cb65158c1be6
  Archivo: zam.bat

- 18f0898d595ec054d13b02915fb7d3636f65b8e53c0c66b3c7ee3b6fc37d3566
  Archivo: netscan.exe

- 1845fe8545b6708e64250b8807f26d095f1875cc1f6159b24c2d0589feb74f0c
  Archivo: IObitUnlocker.sys

URL

- 3x55o3u2b7cjs54eifja5m3ottxntlubhjzt6k6htp5nrocjmsxxh7ad[.]onion
  Descripción: Trigona TOR negotiation portal

- Hxxp[:]//6n5tfadusp4sarzuxntz34q4ohspiaya2mc6aw6uhlusfqfsdomavyyd[.]onion
  Descripción: Trigona leak site

- hxxs[:]//www.virustotal.com/gui/file/feb09cc39b1520d228e9e9274500b8c2290166fc8018a2bf19aa9d3601492c5
  Descripción: disable-defender.exe

- hxxs[:]//www.virustotal.com/gui/file/f6440c5cfc1a0bf4fdc63124eef27f40be37af8f46d10aea9a645f5b084004e3
  Descripción: defoff.bat

- hxxs[:]//www.virustotal.com/gui/file/da0a235cd729d4aa6b209bfe1edefbeeca8fe2ae92d4e3830db7744c9393eadf
  Descripción: coba.bat

- hxxs[:]//www.virustotal.com/gui/file/69f245dc5e505d2876e2f2eec87fa565c707e7c391845fa8989c14acabc2d3f6
  Descripción: mim.exe

- hxxs[:]//www.virustotal.com/gui/file/eeed7ce800a9714b65aaae4f1d61deb83d3f0cbcfd814372807b73c940d4bb8f
  Descripción: meshagent.exe

- hxxs[:]//www.virustotal.com/gui/file/4c181562c9a52be9a629522de7d46f04a490b29d673e8a2376e4cb65158c1be6
  Descripción: zam.bat

- hxxs[:]//www.virustotal.com/gui/file/18f0898d595ec054d13b02915fb7d3636f65b8e53c0c66b3c7ee3b6fc37d3566
  Descripción: netscan.exe

- hxxs[:]//www.virustotal.com/gui/file/1845fe8545b6708e64250b8807f26d095f1875cc1f6159b24c2d0589feb74f0c
  Descripción: IObitUnlocker.sys

DIRECCIONES IP

- 45.227.253[.]99
- 45.227.253[.]106
- 45.227.253[.]98
- 45.227.253[.]107
- 77.83.36[.]6

VII. RECOMENDACIONES:

La prevención de un ataque de ransomware Trigona comienza con la implementación de prácticas recomendadas de seguridad integrales. Estas estrategias sirven como escudo proactivo contra amenazas y ayudan a las organizaciones a desarrollar resiliencia.

- **Autenticación Multifactor (MFA)**: Implementar la MFA para todas las cuentas de usuario, especialmente para el acceso a escritorios remotos. Esta capa adicional de seguridad reduce significativamente el riesgo de acceso no autorizado mediante credenciales robadas o comprometidas.
- **Aplicación regular de parches de software**: Mantener todo el software, los sistemas operativos y las aplicaciones actualizados con los últimos parches de seguridad. Muchos ataques de ransomware se dirigen a vulnerabilidades conocidas, por lo que la gestión de parches es crucial.
- **Seguridad del correo electrónico**: Mejorar la seguridad del correo electrónico implementando filtros antispam robustos y capacitando a los empleados sobre las amenazas de phishing. Con frecuencia, el ransomware se infiltra en los sistemas a través de archivos adjuntos o enlaces maliciosos en correos electrónicos.
- **Control de acceso**: Implementar el principio de mínimos privilegios (PoLP), garantizando que los usuarios solo tengan el acceso mínimo necesario para sus roles. Esto reduce la superficie de ataque y limita el potencial de daño.
- **Segmentación de red**: Dividir las redes en segmentos para aislar los sistemas críticos del resto de la infraestructura. En caso de una brecha de seguridad, esto impide el movimiento lateral de los atacantes.
- **Copias de seguridad periódicas**: Mantener copias de seguridad seguras y sin conexión de sus datos y sistemas críticos. Estas copias de seguridad son indispensables para la recuperación sin pagar un rescate.
- **Copias de seguridad inmutables y con espacio de aire:** implementar copias de seguridad inmutables y con espacio de aire para garantizar que los datos no se vean afectados por ataques de ransomware.

- **Protección de puntos finales**: invertir en soluciones de seguridad de puntos finales sólidas que puedan detectar y prevenir malware, incluido 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:

https://www.sentinelone.com/anthology/trigona/

https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-trigona

https://unit42.paloaltonetworks.com/trigona-ransomware-update/

https://es.sentinelone.com/resources/sentinelone-vs-trigona-ransomware-prevention/

https://stonefly.com/blog/what-is-trigona-ransomware/

https://asec.ahnlab.com/en/61000/

https://www.bleepingcomputer.com/news/security/microsoft-sql-servers-hacked-to-deploy-trigona-ransomware/

https://www.linkedin.com/pulse/anatom%C3%ADa-de-un-compromiso-ransomware-trigona-merabytes-5owhf/