	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 095	Fecha: 22-04-2023
		Página 7 de 20

Componente que reporta	**CENTRO DE CIBERDEFENSA DEL EJÉRCITO DEL PERÚ**		
Nombre de la alerta	Servidores Microsoft SQL pirateados para implementar el ransomware Trigona		
Tipo de ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de subfamilia	C02
Clasificación temática familia	Código Malicioso		

Descripción

ANTECEDENTES:

El 19 de abril del 2023, a través del monitoreo y búsqueda de amenazas en el Ciberespacio, se tiene conocimiento que, los ciberdelincuentes están hackeando servidores Microsoft SQL (MS-SQL) mal protegidos y expuestos a Internet para implementar cargas útiles del ransomware Trigona y cifrar todos los archivos.

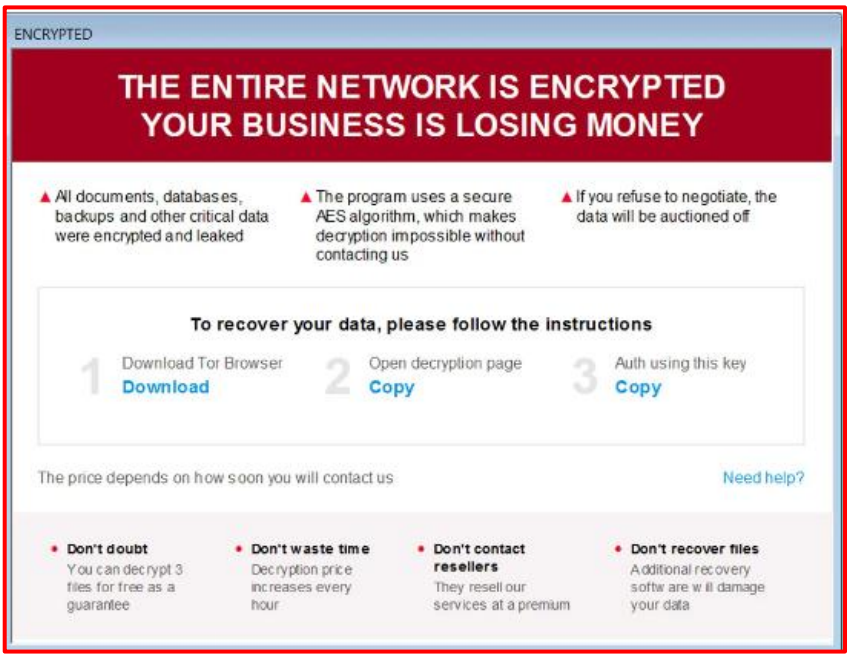
El ransomware Trigona, fue descubierta por primera vez en octubre de 2022 y es conocida por aceptar solo pagos de rescate en criptomoneda. Los ciberdelincuentes también afirman haber robado documentos confidenciales de su organización que posteriormente se agregarán a su sitio de fugas en la web oscura.

DETALLES:

Los servidores MS-SQL están siendo violados mediante ataques de fuerza bruta o de diccionario que aprovechan las credenciales de cuenta fáciles de adivinar. Después de conectarse a un servidor, los actores de amenazas implementan el malware denominado CLR Shell.

Este malware se usa para recolectar información del sistema, alterar la configuración de la cuenta comprometida y aumentar los privilegios a LocalSystem al explotar una vulnerabilidad en el Servicio de inicio de sesión secundario de Windows (que será necesario para iniciar el ransomware como servicio).

CLR Shell es un tipo de malware de ensamblaje CLR que recibe comandos de los actores de amenazas y realiza comportamientos maliciosos, de manera similar a los WebShells de los servidores web.



En la siguiente etapa, los atacantes instalan y lanzan un malware cuentagotas como el servicio "svcservice.exe", que utilizan para lanzar el ransomware Trigona como "svchost.exe". Luego configura el binario de ransomware para que se inicie automáticamente en cada reinicio del sistema a través de una clave de ejecución automática de Windows para garantizar que los sistemas se cifren incluso después de un reinicio.

Antes de cifrar el sistema e implementar notas de rescate, el malware deshabilita la recuperación del sistema y elimina las instantáneas de volumen de Windows, lo que hace que la recuperación sea imposible, sin la clave de descifrado.

Después de cifrar los archivos agrega la extensión. ”_locked” e incorpora la clave de descifrado cifrada, el ID de la campaña y el ID de la víctima (nombre de la empresa) en cada archivo bloqueado. También crea notas de rescate denominadas "how_to_decrypt.hta" en cada carpeta con información sobre el ataque, un enlace al sitio web de negociación de Trigona Tor y un enlace que contiene la clave de autorización necesaria para iniciar sesión en el sitio de negociación.

RECOMENDACIONES:

- Se recomienda mantener actualizado el servidor de base de datos Microsoft SQL.
- Realizar copias de seguridad (backup), especialmente de los archivos de gran interés institucional.
- Usar analizadores de virus y filtros de contenido en los servidores de correo electrónico, ya que es una forma inteligente de prevenir el ransomware. Estos programas reducen el riesgo de que llegue spam con archivos adjuntos maliciosos o enlaces infectados a su buzón.
- Con el fin de minimizar el impacto potencial de un ataque de ransomware exitoso, se recomienda restringir privilegios para que los usuarios solo tengan acceso a la información y los recursos necesarios para ejecutar funciones específicas.
- Evitar hacer clic en anuncios emergentes ya que suelen conducir a la descarga de software malicioso.

Fuentes de información	▪ hxxps://www.bleepingcomputer.com/news/security/microsoft-sql-servers-hacked-to-deploy-trigona-ransomware/