Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

RANSOMWARE TRIGONA DESENCADENA ALARMAS DE CIBERSEGURIDAD EN LA REGIÓN

31/ 01 / 2024

CONTENIDO

INTRODUCCIÓN

Trigona , conocido por su capacidad para cifrar archivos y dejar a las empresas locales en estado de emergencia, ha marcado un nuevo nivel de amenaza en el mundo digital. Su método distintivo de agregar la extensión "._locked" a los nombres de archivo ha desencadenado el caos en organizaciones de todos los tamaños, dejando a las víctimas en un estado de incertidumbre y temor.

RANSOMWARE TRIGONA DESENCADENA ALARMAS DE CIBERSEGURIDAD EN LA REGIÓN

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_01_31_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	31/01/2024
Es día cero (0 day):	No

RESUMEN

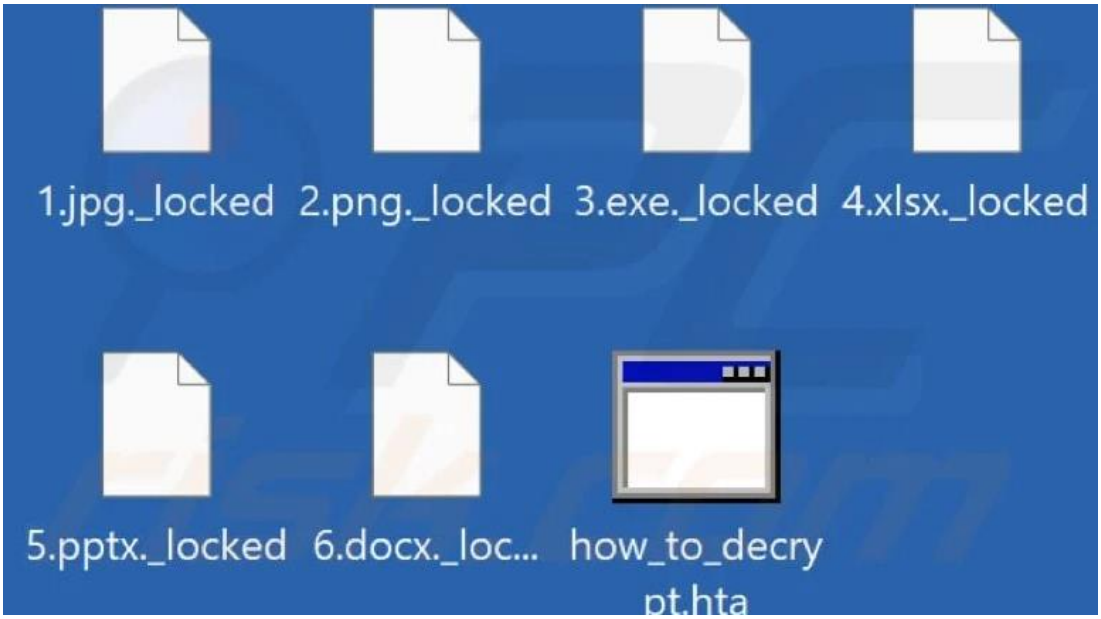
La región ha sido testigo de una serie de ataques cibernéticos devastadores con la llegada del ransomware Trigona, un peligroso virus que cifra archivos y ha dejado a las empresas locales en estado de emergencia. Este ransomware, conocido por agregar la extensión "._locked" a los nombres de archivo, ha desatado el caos en organizaciones de todos los tamaños.

Trigona opera mediante la encriptación de archivos esenciales, cambiando nombres como "1.jpg" a "1.jpg._locked" y "2.png" a "2.png._locked". Además, deja su marca característica al incorporar la clave de descifrado cifrada, el ID de la campaña y el ID de la víctima en cada archivo afectado.

La nota de rescate dejada por Trigona sumerge a las víctimas en un estado de incertidumbre y temor.

El comunicado insta a las víctimas a contactar a los atacantes lo antes posible para evitar un aumento en el costo del rescate, que aumenta por hora. Sin embargo, se destaca la peligrosa realidad de que, incluso después de pagar, no todas las víctimas reciben las herramientas de descifrado prometidas. Es un riesgo significativo y, por lo tanto, no se recomienda ceder ante las demandas de los ciberdelincuentes.

El ransomware se propaga rápidamente y puede afectar no solo a un equipo, sino también a otros conectados en una red local. Por lo tanto, se enfatiza la importancia de examinar minuciosamente los correos electrónicos antes de abrir enlaces o archivos adjuntos, especialmente aquellos enviados desde direcciones desconocidas o sospechosas.



La eliminación inmediata del ransomware de los sistemas es crucial, ya que cada minuto cuenta para evitar una mayor propagación y daño.

La llegada de Trigona ha dejado a la región en estado de alerta, destacando la necesidad crítica de prácticas de ciberseguridad sólidas. La resistencia contra estos ataques radica en la concienciación, la prevención proactiva y la adopción de medidas de seguridad avanzadas. Manténgase informado, protegido y vigilante en el mundo digital en constante evolución.

RECOMENDACIONES

- Asegúrese de que todos sus programas y aplicaciones estén actualizados. Los ciberdelincuentes a menudo explotan vulnerabilidades en software desactualizado.
- Utilice un firewall para bloquear todo el tráfico no autorizado hacia y desde tu ordenador.
- Utilice una Red Privada Virtual (VPN) cuando te conectes a redes públicas para asegurar tu conexión a Internet.
- Mantenga un registro de toda la actividad de la red. Esto puede ayudarle a detectar cualquier actividad sospechosa.
- Mantenga actualizados sus programas antivirus para proteger su sistema contra las últimas amenazas.
- Implemente la autenticación de dos factores siempre que sea posible para añadir una capa adicional de seguridad.
- Evite visitar sitios web no seguros o de reputación dudosa. Utilice la navegación segura en tu navegador para bloquear sitios web maliciosos.
- Realice copias de seguridad periódicas de los datos críticos y almacénelos en ubicaciones seguras e independientes. Esto facilitará la recuperación en caso de un ataque de ransomware.

NOTICIA COMPLETA

https://devel.group/blog/ransomware-trigona-desencadena-alarmas-de-ciberseguridad-en-la-region/

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20240131_01_TrigonaRansomware

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://www.devel.group/reporta-un-incidente