Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Lockbit 2.0 Ransomware

18/mayo/2022

Contenido

INTRODUCCIÓN

Mediante este boletín, mostramos información relevante sobre Lockbit 2.0 y sus métodos de infección junto a consejos para poder prevenir ser victima de este peligroso Ransomware.

LOCKBIT 2.0.

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

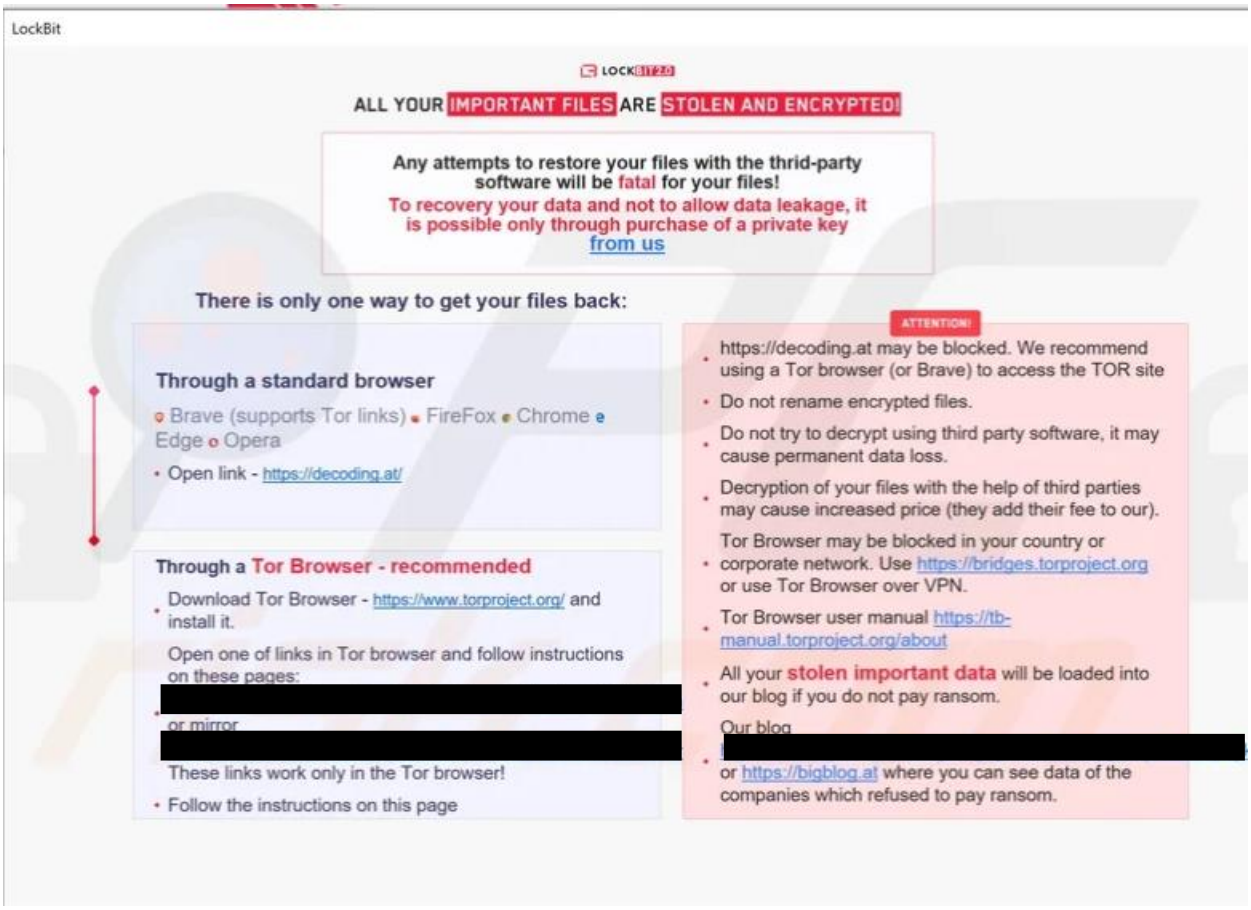
ID de alerta:	DSOC-CERT_2022_05_18
Clasificación de alerta:	Ransomware
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**WHITE**
Fecha de publicación:	05/18/2022
Es día cero (0 day):	NO

RESUMEN

Este programa malicioso está diseñado para encriptar datos y exigir rescates por el desencriptado. En otras palabras, este ransomware inutiliza los archivos y pide a las víctimas que paguen para restaurar el acceso/uso de sus datos.

Durante el proceso de encriptado, los archivos afectados se adjuntan con la extensión ".lockbit". Por ejemplo, un archivo como "1.jpg" aparecería como "1.jpg.lockbit", y así sucesivamente. Una vez finalizado este proceso, las notas de rescate se crean/muestran en el fondo del escritorio, la ventana emergente ("LockBit_Ransomware.hta") y el archivo de texto "Restore-My-Files.txt"

Captura de pantalla notificando que sus datos están encriptados:



Métodos de infección:

El ransomware y otro malware se distribuyen comúnmente a través de dudosos canales de descarga, por ejemplo, redes de intercambio de igual a igual (clientes Torrent, Gnutella, eMule, etc.), sitios web no oficiales y gratuitos de alojamiento de archivos (freeware) y otros descargadores de terceros.

Las herramientas de activación ilegal ("cracks") y las actualizaciones falsas son ejemplos principales de contenido que prolifera con malware. Las herramientas de "craqueo" pueden causar infecciones en lugar de activar productos con licencia.

Los archivos maliciosos pueden estar en varios formatos, por ejemplo, archivos (RAR, ZIP, etc.), ejecutables (.exe, .run, etc.), documentos PDF y de Microsoft Office, JavaScript, etc. Cuando los archivos se ejecutan, se ejecutan o se abren de otro modo, la cadena de infección se inicia.

Etapas del ataque:

Los ataques de LockBit pueden entenderse en aproximadamente tres etapas:

1. Explotar
2. Infiltrarse
3. Implementar

Etapa 1: Explotar las debilidades de una red. La brecha inicial es muy similar a otros ataques maliciosos. Una organización puede ser explotada por tácticas de ingeniería social como el phishing, que consiste en que los atacantes se hacen pasar por personal o autoridades de confianza para solicitar credenciales de acceso. Resulta igualmente viable el uso de ataques de fuerza bruta contra los servidores de la intranet y los sistemas de red de una organización. Si la red carece de una configuración adecuada, las sondas de ataque pueden tardar solo unos días en realizar su trabajo.

Una vez que LockBit entra en la red, el ransomware prepara el sistema para liberar su carga útil de cifrado en todos los dispositivos que pueda. Sin embargo, es posible que un atacante deba asegurarse de que se realicen algunos pasos adicionales antes de dar el golpe final.

Etapa 2: Infiltrarse más profundamente para completar la configuración del ataque si es necesario. A partir de aquí, el programa LockBit realiza toda la actividad por sí mismo. Está programado para utilizar lo que se conoce como herramientas de «posexplotación» para obtener privilegios escalonados y lograr el nivel de acceso necesario para lanzar los ataques. También está presente a través de un acceso ya disponible mediante un movimiento lateral para examinar la viabilidad del objetivo.

En esta etapa LockBit toma las medidas de preparación necesarias antes de implementar el cifrado del ransomware. Esto incluye la desactivación de los programas de seguridad y de cualquier otra infraestructura que pudiera permitir la recuperación del sistema.

El objetivo de la infiltración es imposibilitar la recuperación sin ayuda, o hacer que sea tan lenta que pagar el rescate exigido por el atacante sea la única solución práctica. Cuando la víctima está desesperada por que las operaciones vuelvan a la normalidad es cuando pagará el rescate.

Etapa 3: Implementar la carga de cifrado. Una vez que la red está lista para que LockBit se movilice por completo, el ransomware empezará a propagarse a través de cualquier máquina a la que pueda acceder. Como se ha mencionado anteriormente, LockBit no necesita gran cosa para completar esta etapa. Una sola unidad de sistema con alto nivel de acceso puede emitir comandos a otras unidades de la red para descargar LockBit y ejecutarlo.

La etapa del cifrado pondrá un «candado» en todos los archivos del sistema. Las víctimas solo podrán desbloquear sus sistemas con una clave personalizada creada por la herramienta de descifrado patentada de LockBit. El proceso también deja copias de un simple archivo de texto

de notas de rescate en cada carpeta del sistema. Este proporciona a la víctima instrucciones para restaurar su sistema e incluso incluye la amenaza de chantaje en algunas versiones de LockBit.

Una vez completadas todas las etapas, los siguientes pasos quedan a cargo de la víctima. Puede decidir comunicarse con el servicio de asistencia técnica de LockBit y pagar el rescate. Sin embargo, se aconseja no ceder a sus demandas. Las víctimas no tienen garantías de que los atacantes vayan a cumplir con su parte del trato.

Eliminación y Cifrado:

Si tu organización ya está infectada, la eliminación del ransomware LockBit por sí sola no te dará acceso a tus archivos. Deberás utilizar una herramienta para restaurar el sistema, ya que el cifrado requiere una «clave» para desbloquearlo. Como alternativa, puedes restaurar tus sistemas mediante la creación de una nueva imagen si ya has creado imágenes de copia de seguridad previas a la infección.

RECOMENDACIONES

Se recomiendan las siguientes acciones:

1. Implementa contraseñas seguras.
2. Activa la autenticación de varios factores.
3. Vuelve a evaluar y simplifica los permisos de las cuentas de usuario.
4. Borra las cuentas de usuario desactualizadas y no utilizadas.
5. Asegúrate de que las configuraciones del sistema sigan todos los procedimientos de seguridad.
6. Tener siempre preparadas copias de seguridad de todo el sistema e imágenes limpias de los equipo locales.
7. Configurar de manera adecuada su software Anti-phishing.
8. Si observa comportamiento anormal en uno de sus equipos, por favor aislarlo de la red inmediatamente y realizar una revisión profunda en el, los IOC le ayudaran a comprobar si su equipo esta infectado con Lockbit.

Noticia Completa

https://www.picussecurity.com/resource/lockbit-2.0-ransomware-ttps-used-in-emerging-ransomware-campaigns

https://latam.kaspersky.com/resource-center/threats/lockbit-ransomware

https://www.pcrisk.es/guias-de-desinfeccion/10926-lockbit-2-0-ransomware

Indicadores de Compromiso.

https://github.com/develgroup/SOC_IOCs/tree/main/20220506_01_LockBit

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