Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CISA emite recomendaciones para evitar el Ransomware MedusaLocker.

1/julio/2022

Contenido

INTRODUCCIÓN

A continuación, mostramos información de mucha utilidad para usted y su organización sobre MedusaLocker, sus vectores de ataque y los indicadores de compromiso.

Sugerimos prestar atención a las recomendaciones que acá se muestran, para que puedan ser aplicadas en su entorrno.

MEDUSALOCKER RANSOMWARE

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

ID de alerta:	DSOC-CERT_2022_07_01_01
Clasificación de alerta:	Noticia
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**WHITE**
Fecha de publicación:	07/01/2022
Es día cero (0 day):	NO

RESUMEN

La Oficina Federal de Investigaciones (FBI), la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA), el Departamento del Tesoro y la Red de Ejecución de Delitos Financieros (FinCEN) han publicado esta información para proporcionar información sobre el ransomware MedusaLocker. Observado recientemente en mayo de 2022, los actores de MedusaLocker dependen predominantemente de vulnerabilidades en el Protocolo de escritorio remoto (RDP) para acceder a las redes de las víctimas. Los actores de MedusaLocker encriptan los datos de la víctima y dejan una nota de rescate con instrucciones de comunicación en cada carpeta que contiene un archivo encriptado. La nota indica a las víctimas que proporcionen pagos de ransomware a una dirección de billetera Bitcoin específica. MedusaLocker parece operar como un modelo de Ransomware-as-a-Service (RaaS) basado en la división observada de los pagos de rescate. Los modelos típicos de RaaS involucran al desarrollador de ransomware y varios afiliados que implementan el ransomware en los sistemas de las víctimas. Los pagos del ransomware MedusaLocker parecen dividirse constantemente entre el afiliado, que recibe del 55 al 60 por ciento del rescate; y el promotor, que recibe el resto.

Detalles técnicos

Los actores del ransomware MedusaLocker a menudo obtienen acceso a los dispositivos de las víctimas a través de configuraciones vulnerables del Protocolo de escritorio remoto (RDP). Los actores también utilizan con frecuencia campañas de correo electrónico no deseado y phishing por correo electrónico, adjuntando directamente el ransomware al correo electrónico, como vectores de intrusión iniciales

El ransomware MedusaLocker utiliza un archivo por lotes para ejecutar el script de PowerShell invoke-ReflectivePEInjection. Este script propaga MedusaLocker a través de la red editando el EnableLinkedConnectionsvalor dentro del registro de la máquina infectada, lo que luego permite que la máquina infectada detecte hosts y redes conectados a través del Protocolo de mensajes de control de Internet (ICMP) y detecte el almacenamiento compartido a través del Protocolo de bloque de mensajes del servidor (SMB).

MedusaLocker entonces:

Reinicia el LanmanWorkstationservicio, lo que permite que las ediciones del registro surtan efecto.
Elimina los procesos de software forense, contable y de seguridad conocido.

Reinicia la máquina en modo seguro para evitar la detección por parte del software de seguridad.

Cifra los archivos de las víctimas con el algoritmo de cifrado AES-256; la clave resultante se cifra luego con una clave pública RSA-2048.

Se ejecuta cada 60 segundos, encriptando todos los archivos excepto aquellos críticos para la funcionalidad de la máquina de la víctima y aquellos que tienen la extensión de archivo encriptada designada.

Establece la persistencia copiando un ejecutable (svhost.exe o svhostt.exe) en %APPDATA%\Roamingdirectorio y programando una tarea para ejecutar el ransomware cada 15 minutos.

Intenta evitar las técnicas de recuperación estándar mediante la eliminación de copias de seguridad locales, la desactivación de las opciones de recuperación de inicio y la eliminación de instantáneas.

Los actores de MedusaLocker colocan una nota de rescate en cada carpeta que contiene un archivo con los datos cifrados de la víctima. La nota describe cómo comunicarse con los actores de MedusaLocker, por lo general proporciona a las víctimas una o más direcciones de correo electrónico en las que se puede contactar a los actores. El tamaño de las demandas de rescate de MedusaLocker parece variar según el estado financiero de la víctima según lo perciben los actores.

RECOMENDACIONES

- Implemente un plan de recuperación que mantenga y conserve múltiples copias de datos confidenciales o de propiedad y servidores en una ubicación segura, segmentada y separada físicamente (es decir, disco duro, dispositivo de almacenamiento o la nube).

- Implemente la segmentación de la red y mantenga copias de seguridad fuera de línea de los datos para garantizar una interrupción limitada de la organización.

- Realice copias de seguridad de los datos con regularidad y proteja con contraseña las copias de seguridad almacenadas sin conexión. Asegúrese de que las copias de los datos críticos no sean accesibles para su modificación o eliminación desde el sistema donde residen los datos.

- Instale, actualice periódicamente y habilite la detección en tiempo real del software antivirus en todos los hosts.

- Instale actualizaciones para sistemas operativos, software y firmware lo antes posible.

- Revise los controladores de dominio, los servidores, las estaciones de trabajo y los directorios activos en busca de cuentas nuevas o no reconocidas.

- Auditar cuentas de usuario con privilegios administrativos y configurar controles de acceso según el principio de mínimo privilegio.

- Deshabilite los puertos no utilizados.

- Considere agregar un banner de correo electrónico a los correos electrónicos recibidos desde fuera de su organización.

- Deshabilite los hipervínculos en los correos electrónicos recibidos.

- Hacer cumplir la autenticación multifactor (MFA).

- Considere instalar y usar una red privada virtual (VPN) para establecer conexiones remotas seguras.

Noticia Completa

https://www.cisa.gov/uscert/ncas/alerts/aa22-181a

IOC's

https://github.com/develgroup/SOC_IOCs/tree/main/20220630_01_MedusaLocker-Ransomware

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