Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CISA ha emitido una nueva advertencia sobre el ransomware Zeppelin.

11/Agosto/2022

Contenido

INTRODUCCIÓN

Mediante este boletín queremos compartir con usted el reciente reporte de CISA sobre el ransomware Zeppelin que generalmente accede a través de RDP, fallas en el firewall de SonicWall y phishing.

ZEPPELIN RANSOMWARE.

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

ID de alerta:	DSOC-CERT_2022_08_11_01
Clasificación de alerta:	Noticia
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	08/11/2022
Es día cero (0 day):	NO

RESUMEN

La Oficina Federal de Investigaciones (FBI) y la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) están lanzando este CSA conjunto para difundir los IOC y TTP conocidos del ransomware Zeppelin asociados con variantes de ransomware identificadas a través de investigaciones del FBI hasta el 21 de junio de 2022.

El FBI y CISA alientan a las organizaciones a implementar las recomendaciones en la sección Mitigaciones de este CSA para reducir la probabilidad y el impacto de los incidentes de ransomware.
El ransomware Zeppelin es un derivado de la familia de malware Vega basada en Delphi y funciona como ransomware como servicio (RaaS). Desde 2019 hasta al menos junio de 2022, los actores han utilizado este malware para apuntar a una amplia gama de empresas y organizaciones de infraestructura crítica, incluidos contratistas de defensa, instituciones educativas, fabricantes, empresas de tecnología y, especialmente, organizaciones en las industrias médica y de atención médica. Se sabe que los actores de Zeppelin solicitan pagos de rescate en Bitcoin, con cantidades iniciales que van desde varios miles de dólares hasta más de un millón de dólares.

Los actores de Zeppelin obtienen acceso a las redes de las víctimas a través de la explotación de RDP explotando las vulnerabilidades del firewall de SonicWall [T1190] y campañas de phishing. Antes de implementar el ransomware Zeppelin, los actores pasan de una a dos semanas mapeando o enumerando la red de la víctima para identificar enclaves de datos, incluido el almacenamiento en la nube y las copias

de seguridad de la red [TA0007]. Los actores de Zeppelin pueden implementar el ransomware Zeppelin como un archivo .dll o .exe contenido dentro de un cargador de PowerShell.
Antes del cifrado, los actores de Zeppelin filtran archivos de datos confidenciales de la empresa para venderlos o publicarlos en caso de que la víctima se niegue a pagar el rescate. Una vez que se ejecuta el ransomware, se agrega un número hexadecimal aleatorio de nueve dígitos a cada archivo cifrado como una extensión de archivo, por ejemplo, file.txt.txt. Se deja un archivo de nota con una nota de rescate en los sistemas comprometidos, con frecuencia en el escritorio (nota de ejemplo a continuación).

El FBI ha observado instancias en las que los actores de Zeppelin ejecutaron su malware varias veces dentro de la red de una víctima, lo que resultó en la creación de diferentes ID o extensiones de archivo para cada instancia de un ataque; esto da como resultado que la víctima necesite varias claves de descifrado únicas.

TÉCNICAS DE ATAQUE.

Acceso inicial		
Título de la técnica	**IDENTIFICACIÓN**	**Uso**
Explotar servicios remotos externos	T1133	Los actores de Zeppelin explotan RDP para obtener acceso a las redes de las víctimas.
Explotar Aplicación orientada al público	T1190	Los actores de Zeppelin explotan las vulnerabilidades en los sistemas orientados a Internet para obtener acceso a los sistemas.
Suplantación de identidad	T1566	Los actores de Zeppelin han utilizado el phishing y el spear phishing para obtener acceso a las redes de las víctimas.
Ejecución		
Título de la técnica	**IDENTIFICACIÓN**	**Uso**
Enlace malicioso	T1204.001	Los actores de Zeppelin engañan a los usuarios para que hagan clic en un enlace malicioso para ejecutar macros maliciosas.
Adjunto de archivo malicioso	T1204.002	Los actores de Zeppelin engañan a los usuarios para que hagan clic en un archivo adjunto malicioso disfrazado de publicidad para ejecutar macros maliciosas.
Persistencia		
Título de la técnica	**IDENTIFICACIÓN**	**Uso**
Modificar el proceso del sistema	T1543.003	Cifran las funciones operativas para preservar las funciones del sistema comprometidas.

Impacto		
Título de la técnica	**IDENTIFICACIÓN**	**Uso**
Datos cifrados para impacto	T1486	Los actores de Zeppelin tienen datos cifrados en los sistemas de destino o en una gran cantidad de sistemas en una red para interrumpir la disponibilidad de los recursos del sistema y de la red.

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 siempre que estén disponibles y el historial de cambios no indique vulnerabilidades o bugs críticos.

- 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.

- Hacer cumplir la autenticación multifactor (MFA).

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

- Examine el tráfico de red entrante y saliente, en busca de actividad sospechosa dentro de su red.

- Utilizar escritorio remoto solo cuando es necesario.

- Realizar capacitaciones de forma continua a su personal sobre detección y reporte de Phishing.

Noticia Completa

https://devel.group/cisa-ha-emitido-una-nueva-advertencia-sobre-el-ransomware-zeppelin/

IOC's

https://github.com/develgroup/SOC_IOCs/tree/main/20220811_01_Zeppelin

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