Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Boletín Informativo

.

03/mayo/2022

Contenido

RESUMEN

El siguiente boletín presenta información sobre nuevos ataques de ransomware reportados por analistas de Trend Micro, con la novedad de que también es capaz de escanear múltiples puntos finales en busca de la vulnerabilidad Log4j Log4shell utilizando el script Nmap NSE.

AvosLocker Ransomware

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

ID de alerta:	DSOC-CERT_2022_05_03
Clasificación de alerta:	RANSOMWARE
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**WHITE**
Fecha de publicación:	03/05/2022
Es día cero (0 day):	NO

Resumen

AvosLocker, una de las familias de ransomware más nuevas para llenar el vacío dejado por REvil , se ha relacionado con una serie de ataques dirigidos a infraestructura crítica en los EE.UU. incluidos los servicios financieros e instalaciones gubernamentales.

Un grupo basado en afiliados de ransomware como servicio (RaaS) descubierto por primera vez en julio de 2021, AvosLocker va más allá de la doble extorsión al subastar los datos robados a las víctimas en caso de que las entidades objetivo se nieguen a pagar el rescate.

Otras víctimas objetivo reclamadas por el cartel de ransomware se encuentran en Siria, Arabia Saudita, Alemania, España, Bélgica, Turquía, los Emiratos Árabes Unidos, el Reino Unido, Canadá, China y Taiwán, según un aviso publicado por el FBI en marzo de 2022.

Se cree que el punto de entrada para el ataque se facilitó al aprovechar un exploit para una falla de ejecución remota de código en el software ManageEngine ADSelfService Plus de Zoho (CVE-2021-40539) para ejecutar una aplicación HTML (HTA) alojada en un servidor remoto.

Esto incluye recuperar un shell web ASPX del servidor, así como un instalador para el software de escritorio remoto AnyDesk , el último de los cuales se usa para implementar herramientas adicionales para escanear la red local, finalizar el software de seguridad y eliminar la carga útil del ransomware.

Algunos de los componentes copiados en el punto final infectado son un script Nmap para escanear la red en busca de la falla de ejecución remota de código de Log4Shell (CVE-2021-44228) y una herramienta de implementación masiva llamada PDQ para entregar un script por lotes malicioso a múltiples endpoints.

De acuerdo con el aviso de seguridad cibernética, varias víctimas informaron vulnerabilidades de seguridad de Microsoft Exchange Server en las instalaciones como el vector probable de intrusión, incluidas las vulnerabilidades de Proxy Shell (CVE-2021-31207, CVE-2021-34523, CVE-2021-34473 y CVE -2021-26855).

Herramientas usadas por los atacantes:

- Netscan: Para buscar otros endpoints

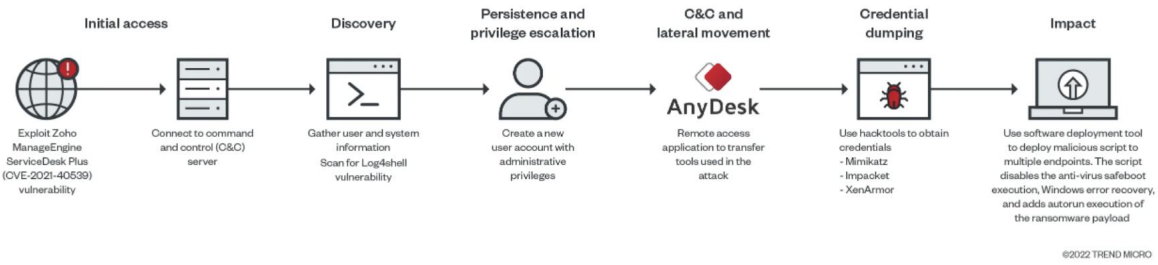
- Nmap (log4shell.nse): para buscar endpoints vulnerables de Log4shell

- Herramientas de hacking Mimikatz e Impacket: Para movimiento lateral

- Implementación de PDQ: para la implementación masiva de secuencias de comandos maliciosos en múltiples endpoints

- Aswarpot.sys: para deshabilitar soluciones de defensa. Notamos que puede deshabilitar una serie de productos antivirus, previamente identificados por los investigadores de Aon.

Cadena de Infección:



Recomendaciones

Se recomiendan las siguientes acciones:

1. Se recomienda implementar las mitigaciones mostradas en este documento.
2. Se recomienda contar con una plataforma SIEM y su debido monitoreo de alertas y amenazas.
3. Se recomienda que todos sus sistemas públicos cuenten con un doble factor de autenticación para el ingreso a las plataformas.
4. Se recomienda un monitoreo activo y escaneo publico periódico para la identificación de alguna falla externa dentro de los sistemas públicos de la corporación.

Links de referencia

Se adjuntan links de referencia en donde se puede obtener más información de terceros:

https://www.securitymagazine.com/articles/97300-avoslocker-ransomware-a-threat-to-critical-infrastructure

https://www.trendmicro.com/research/avoslocker

https://otx.alienvault.com/pulse/6271533a6e96d8f605d9ade5

Indicadores de compromiso

https://github.com/develgroup/SOC_IOCs/tree/main/20220503_01_AvosLocker

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