Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

PROLIFERAN ATAQUES DE ALPHV BLACKCAT RANSOWMARE EN LA REGIÓN

04 / Abril/2023

CONTENIDO

INTRODUCCIÓN

Se ha observado a un nuevo afiliado de ransomware ALPHV (también conocido como BlackCat ransomware), rastreado como UNC4466, dirigirse a instalaciones de Veritas Backup Exec expuestas públicamente y vulnerables a CVE-2021-27876, CVE-2021-27877 y CVE-2021-27878, para obtener acceso inicial a los entornos de las víctimas. Un servicio comercial de escaneo de Internet identificó más de 8.500 instalaciones de Veritas Backup Exec actualmente expuestas en Internet, algunas de las cuales aún pueden no estar parcheadas y ser vulnerables.

ALPHV BLACKCAT RANSOMWARE

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

ID de alerta:	DSOC-CERT_2023_04_13_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	13/04/2023
Es día cero (0 day):	No

RESUMEN

ALPHV surgió en noviembre de 2021 como un ransomware-as-a-service que algunos investigadores han afirmado es el sucesor del ransomware BLACKMATTER y DARKSIDE. Mientras que algunos operadores de ransomware implementaron reglas para evitar impactar infraestructuras críticas y entidades de salud, ALPHV ha seguido dirigiéndose a estas industrias sensibles.

UNC4466 (AlphV "BlackCat Ransomware) hace uso de ADRecon para obtener información de la red, cuentas y host del entorno de la víctima. ADRecon genera varios reportes en el entorno de Active Directory, incluyendo Trusts, sitios, subnets, políticas de contraseña y listados de cuentas de usuarios y computadoras.

Así mismo UNC4466 hace uso de Background Inteligen Transfer Service (BITS) para descarar herramientas adicionales tales como LAZAGNE, LIGOLO, WINSW, RCLONE, y finalmente el encriptador de AlphV Ransomware.

UNC4466 aprovecha túneles SOCKS5 para así poderse comunicar con el sistema comprometido en la red de la víctima. Esta técnica permite evitar o evadir las defensas de la red u otros controles preventivos de la red.

El actor de amenazas utilizó múltiples herramientas de acceso a credenciales, incluidas Mimikatz, LaZagne y Nanodump para recopilar credenciales de texto claro y material de credenciales.

En noviembre de 2022, UNC4466 utilizó el módulo de inyección MIMIKATZ Security Support Provider ('MISC::MemSSP'). Este módulo recopila credenciales en texto no cifrado a medida que se utilizan, manipulando el Servicio de servidor de autoridad de seguridad local (LSASS) en los sistemas víctimas. Este módulo crea un archivo llamado 'C:\Windows\System32\mimilsa.log'.

[Nanodump] también se usó para volcar la memoria LSASS. Al igual que los ejemplos que se muestran en la página GitHub de Helpsystems, el archivo de salida especificado era un archivo en el directorio 'C:\Windows\Temp'.

Durante las operaciones, UNC4466 toma medidas para evadir la detección. Además de borrar los registros de eventos, UNC4466 también usó el cmdlet Set-MpPrefernce integrado para deshabilitar la capacidad de supervisión en tiempo real de Microsoft Defender.

A partir de la fecha de esta publicación de blog, un servicio comercial de escaneo de Internet informó más de 8500 direcciones IP que anuncian el servicio "Symantec / Veritas Backup Exec ndmp" en el puerto predeterminado 10000, así como en el puerto 9000 y el puerto 10001. Si bien este resultado de búsqueda no identifica directamente los sistemas vulnerables, ya que las versiones de la aplicación no eran identificables, demuestra la prevalencia de instancias expuestas a Internet que podrían ser probadas por los atacantes.

NOTA IMPORTANTE

Es importante resaltar en esta nota que en el último año los atacantes han dirigido sus esfuerzos a cifrar máquinas virtuales dentro de hosts como VMWare Vcenter o ESXi, y los afiliados de ALPHV no son la excepción según lo evidenciado en ataques recientes en la región.

Por lo cual se les insta a tomar en cuenta todas las recomendaciones a nivel de mejores prácticas para estos recursos, ya que son de los objetivos principales de los atacantes media vez se encuentren a su disposición.

Existen múltiples vulnerabilidades críticas en VMWare ESXi que deben de ser parcheadas lo antes posible para evitar ejecución de código remoto en los sistemas afectados (CVE-2021-21974, CVE-2022-31696, CVE-2022-31697, CVE-2022-31698, y CVE-2022-31699). Adicional a esto asegurarse de restringir el acceso a estos recursos para las personas que lo requieren, con contraseñas complejas, doble factor de autenticación y de ser posible por medio de una plataforma de gestión de accesos privilegiados.

RECOMENDACIONES

- Identificación de los Indicadores de compromiso como direcciones IP y dominios maliciosos.
- 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.
- Mantenga actualizado todos los sistemas operativos, y software.
- Instale, actualice periódicamente y habilite la detección en tiempo real del software antivirus en todos los hosts.
- Audite las cuentas de usuarios con privilegios administrativos y configure los controles de acceso, con el principio de privilegios mínimos.
- Desactive los puertos no utilizados.
- Deshabilite las actividades y permisos de línea de comandos y scripting.
- Asegúrese de que todos los datos de copia de seguridad estén encriptados, sean inmutables
- Examine el tráfico de red entrante y saliente, en busca de actividad sospechosa dentro de su red.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20230413_01_AlphVBlackCat

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