Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Microsoft alerta sobre ataques de BlackCat ransomware a servidores Exchange

17/junio/2022

Contenido

INTRODUCCIÓN

Por medio del presente boletín, queremos brindarle a usted información relevante sobre los numerosos ataques de BlackCat ransomware ha realizado sobre servidores Exchange, favor tomar en cuenta la información y recomendaciones que se le brindan en este documento.

BlackCat Ransomware

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

ID de alerta:	DSOC-CERT_2022_06_17_01
Clasificación de alerta:	Ransomware
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**WHITE**
Fecha de publicación:	06/17/2022
Es día cero (0 day):	NO

Resumen

Microsoft dice que los afiliados del ransomware BlackCat ahora están atacando los servidores de Microsoft Exchange utilizando exploits dirigidos a vulnerabilidades sin parches.

En al menos un incidente que observaron los expertos en seguridad de Microsoft, los atacantes se movieron lentamente a través de la red de la víctima, robando credenciales y exfiltrando información para usarla en una doble extorsión.

Dos semanas después del compromiso inicial utilizando un servidor Exchange sin parches como vector de entrada, el actor de amenazas implementó cargas útiles de ransomware BlackCat en toda la red a través de PsExec.
“Si bien los vectores de entrada comunes para estos actores de amenazas incluyen aplicaciones de escritorio remoto y credenciales comprometidas, también vimos que un actor de amenazas aprovechó las vulnerabilidades del servidor de Exchange para obtener acceso a la red de destino”, dijo el equipo de inteligencia de amenazas de Microsoft 365 Defender.

Aunque no mencionó la vulnerabilidad de Exchange utilizada para el acceso inicial, Microsoft vincula a un aviso de seguridad de marzo de 2021 con orientación sobre cómo investigar y mitigar los ataques de ProxyLogon.

Además, aunque Microsoft no nombró al afiliado de ransomware que implementó el ransomware BlackCat en este estudio de caso, la compañía dice que varios grupos de ciberdelincuencia ahora son afiliados de esta operación de ransomware como servicio (RaaS) y lo están usando activamente en los ataques.

Uno de ellos, un grupo de ciberdelincuencia motivado financieramente, rastreado como FIN12, es conocido por implementar previamente ransomware Ryuk, Conti y Hive en ataques dirigidos principalmente a organizaciones de atención médica.
Sin embargo, como reveló Mandiant, los operadores de FIN12 son mucho más rápidos , ya que a veces se saltan el paso del robo de datos y tardan menos de dos días en descargar sus cargas útiles de cifrado de archivos en la red de un objetivo.

“Hemos observado que este grupo agregó BlackCat a su lista de cargas útiles distribuidas a partir de marzo de 2022”, agregó Microsoft .

"Se sospecha que su cambio a BlackCat desde su última carga utilizada (Hive) se debe al discurso público sobre las metodologías de descifrado de este último".

El ransomware BlackCat también está siendo implementado por un grupo afiliado rastreado como DEV-0504 que normalmente extrae datos robados mediante Stealbit, una herramienta maliciosa que la pandilla LockBit proporciona a sus afiliados como parte de su programa RaaS. DEV-0504 también ha utilizado otras variedades de ransomware a partir de diciembre de 2021, incluidas BlackMatter, Conti, LockBit 2.0, Revil y Ryuk.

Para defenderse de los ataques de ransomware BlackCat, Microsoft aconseja a las organizaciones que revisen su postura de identidad, supervisen el acceso externo a sus redes y actualicen todos los servidores Exchange vulnerables en su entorno lo antes posible.

Utilizado en cientos de ataques de ransomware

En abril, el FBI advirtió en una alerta relámpago que el ransomware BlackCat se había utilizado para cifrar las redes de al menos 60 organizaciones en todo el mundo entre noviembre de 2021 y marzo de 2022.
"Muchos de los desarrolladores y lavadores de dinero de BlackCat/ALPHV están vinculados a Darkside/Blackmatter, lo que indica que tienen amplias redes y experiencia con operaciones de ransomware", dijo el FBI en ese momento.

Sin embargo, es probable que el número real de víctimas de BlackCat sea mucho mayor dado que se enviaron más de 480 muestras en la plataforma ID-Ransomware entre noviembre de 2021 y junio de 2022.

Recomendaciones

1. No descargar documentos que sean enviados por remitentes desconocidos, o documentos que usted no solicito.

2. Mantenga su software Antivirus actualizado.

3. Instalar los parches y actualizaciones de sistema que sus servidores Exchange soliciten.

4. Solicitar a su SOC monitoreo directo sobre sus dispositivos potencialmente vulnerables.

5. Mantenga la autenticación de doble factor activa en todos los sistemas y dispositivos que permitan esta función.

6. Descargue los IOC y agregue los códigos Hash a sus respectivas consolas AV y EDR, Bloquear las direcciones IP que encontrara en los IOC.

Noticia Completa

https://diariopb.com/blackcat-ransomware-gang-apuntando-a-servidores-de-microsoft-exchange-sin-parches/

IOC's

https://github.com/develgroup/SOC_IOCs/tree/main/20220617_01_BlackCat-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