

CYBER **SECURITY** **NEWS**

SECURITY OPERATIONS CENTER

**GRUPO DE RANSOMWARE AFIRMA ROBAR 6 TB
DE DATOS DE CHANGE HEALTHCARE**

04 / 03 / 2024

CONTENIDO

INTRODUCCIÓN	3
RESUMEN	5
INDICADORES DE COMPROMISO	6
NOTICIA COMPLETA	6
CONTACTOS DE SOPORTE	7

INTRODUCCIÓN

El mundo digital enfrenta una nueva amenaza con el reciente ataque de ransomware perpetrado por el grupo BlackCat/ALPHV contra la plataforma de Change Healthcare, una pieza vital en el intercambio de pagos utilizado por miles de entidades de atención médica en los Estados Unidos. Este incidente no solo ha provocado una interrupción continua en los servicios de Change Healthcare, sino que también ha expuesto datos sensibles de millones de personas, incluyendo registros médicos y de seguros. Aunque las autoridades aún no han confirmado oficialmente la participación de BlackCat en el ataque, las agencias gubernamentales han advertido sobre la creciente amenaza que representa este grupo para el sector de la salud. Este incidente destaca la urgente necesidad de fortalecer las medidas de ciberseguridad en el ámbito de la salud y resalta la importancia de la colaboración entre sectores público y privado para hacer frente a estas amenazas cibernéticas.

GRUPO DE RANSOMWARE AFIRMA ROBAR 6 TB DE DATOS DE CHANGE HEALTHCARE
continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_04_03_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	CLEAR
Fecha de publicación:	04/03/2024
Es día cero (0 day):	No

RESUMEN

El grupo de ransomware BlackCat/ALPHV ha hecho una declaración oficial afirmando su responsabilidad en un ciberataque dirigido a Optum, una filial de UnitedHealth Group (UHG), lo que ha provocado una interrupción continua en la plataforma de Change Healthcare.

ALPHVBlogCollectionsApi

Change Healthcare - Optum - UnitedHealth

2/28/2024, 11:19:59 AM

UnitedHealth has announced that the attack is "strictly related" to Change Healthcare only and it was initially attributed to a nation state actor.

Two lies in one sentence.
Only after threatening them to announce it was us, they started telling a different story. It is true that the attack is centered at Change Healthcare production and corporate networks, but why is the damage extremely high?

Change Healthcare production servers process extremely sensitive data to all of UnitedHealth clients that rely on Change Healthcare technology solutions. Meaning thousands of healthcare providers, insurance providers, pharmacies, etc....

Also, being inside a production network one can imagine the amount of critical and sensitive data that can be found.

ALPHVBlogCollectionsApi


sensitive data being processed by the company.

The list of affected Change Health partners that we have sensitive data for is actually huge with names such as...

- Medicare
- Tricare
- CVS-CareMark
- Loomis
- Davis Vision
- Health Net
- MetLife
- Teachers Health Trust
- Tens of insurance companies and others

Anyone with some decent critical thinking will understand what damage can be done with such intimate data on the affected clients of UnitedHealth/UnitedHealth solutions as well, beyond simple scamming/spamming.

After 8 days and Change Health have still not restored its operations and chose to play a



Change Healthcare, la plataforma de intercambio de pagos más grande utilizada por más de 70,000 farmacias en los Estados Unidos, han sido afectadas por este incidente. Mientras tanto, UHG, la compañía de atención médica más grande del mundo en términos de ingresos se enfrenta a las consecuencias de este ataque.

Según BlackCat, se ha robado 6 TB de datos de la red de Change Healthcare, pertenecientes a una amplia gama de entidades de atención médica, aseguradoras y farmacias. Entre los datos robados incluyen registros médicos, de seguros, dentales, de pagos y reclamos, así como la información personal identificable (PII) de millones de personas, incluidos números de teléfono, direcciones, números de seguro social y direcciones de correo electrónico.

Optum ha confirmado que aún está trabajando para restaurar los sistemas afectados y que sus sistemas, junto con los UnitedHealthcare y UnitedHealth Group, no se han visto afectados por este incidente.

Aunque el vicepresidente de UnitedHealth Group, Tyler Mason, no ha confirmado la participación de BlackCat en el ataque, ha informado que el 90% de las más de 70,000 farmacias afectadas han cambiado

a nuevos procedimientos electrónicos para abordar los problemas causados por el ataque a Change Healthcare.

BlackCat también ha negado el uso de una falla crítica de ScreenConnect auth bypass (CVE-2024-1709) por parte de los afiliados que violaron la red de Change Healthcare.

Las agencias gubernamentales, como el FBI, CISA y el Departamento de Salud y Servicios Humanos (HHS), han advertido que los afiliados del ransomware de BlackCat se centran en organizaciones del sector de la salud en los Estados Unidos. Este incidente resalta la importancia de la seguridad cibernética en el sector de la salud y la necesidad de medidas proactivas para proteger los datos sensibles de los pacientes.

El Departamento de Estado de EE.UU. está ofreciendo una recompensa de hasta \$15 millones por información que ayude a identificar o localizar a los líderes de BlackCat y a las personas vinculadas a sus ataques de ransomware.

CYBERSECURITY ADVISORY

#StopRansomware: ALPHV Blackcat

Last Revised: February 27, 2024

Alert Code: AA23-353A

RELATED TOPICS: [CYBER THREATS AND ADVISORIES](#), [MALWARE](#), [PHISHING](#), [AND RANSOMWARE](#), [INCIDENT DETECTION](#), [RESPONSE](#), [AND PREVENTION](#)



ACTIONS TO TAKE TODAY TO MITIGATE AGAINST THE THREAT OF RANSOMWARE:

1. Routinely take inventory of assets and data to identify authorized and unauthorized devices and software.
2. Prioritize remediation of known exploited vulnerabilities.
3. Enable and enforce multifactor authentication with strong passwords.
4. Close unused ports and remove applications not deemed necessary for day-to-day operations.

INDICADORES DE COMPROMISO

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

NOTICIA COMPLETA

<https://devel.group/blog/grupo-de-ransomware-afirma-robar-6-tb-de-datos-de-change-healthcare/>

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>