Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

PRICESMART SE VE AFECTADO POR ALPHV

14 / 11 / 2023

CONTENIDO

INTRODUCCIÓN

Al menos 500 GB de información sensible habría sido exfiltrada de los servidores de la cadena de supermercados PriceSmart por parte de la organización cibercriminal de Ransomware ALPHV, según informó este domingo la firma especializada en rastreo de ataques informáticos FalconFeeds.io en su perfil de X (antes Twitter), así como el monitor de ransomware ThreatMon.

PRICESMART SE VE AFECTADO POR ALPHV

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

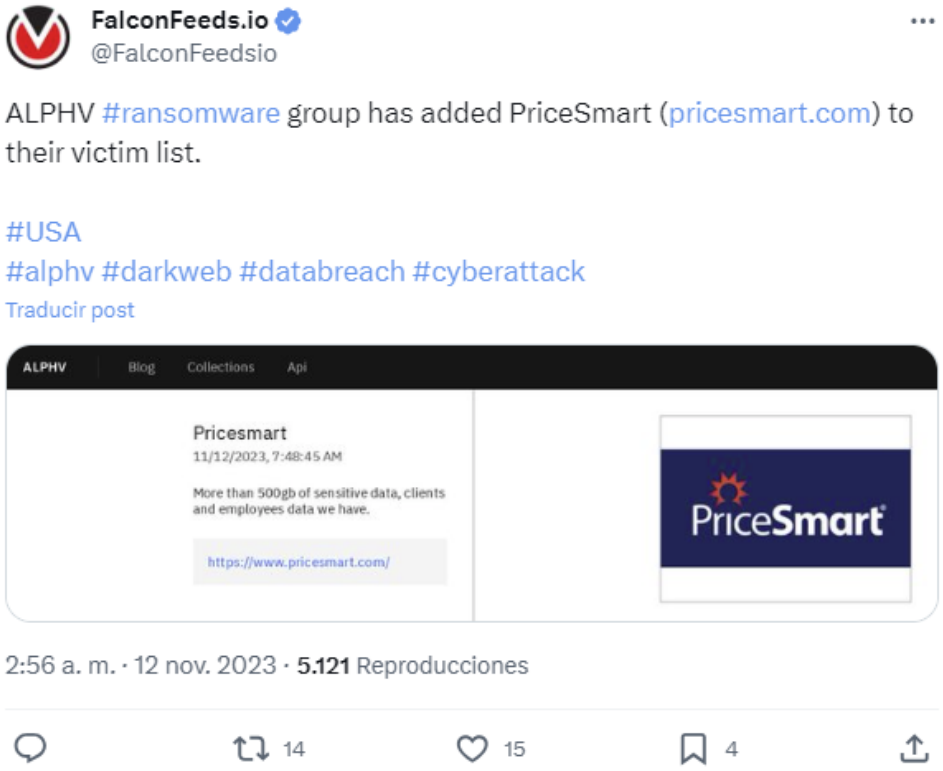
ID de alerta:	DSOC-CERT_2023_11_14_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	14/11/2023
Es día cero (0 day):	No

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.

Al menos 500 GB de información sensible habría sido exfiltrada de los servidores de la cadena de supermercados PriceSmart por parte de la organización cibercriminal de Ransomware ALPHV, según informó este domingo la firma especializada en rastreo de ataques informáticos FalconFeeds.io en su perfil de X (antes Twitter), así como el monitor de ransomware ThreatMon.

Los datos extraídos corresponderían a clientes de países del Caribe donde tiene presencia dicha empresa de compras por membresía, entre los que destacan Jamaica, Santa Lucía, Barbados, así como Trinidad y Tobago, entre otros, informó el medio de ese país 'Technology News from Trinidad and Tobago'.



Entre la información presuntamente obtenida por los piratas informáticos se incluye nombre de clientes, direcciones, números de teléfono, contraseña de la cuenta, detalles de los pedidos, ubicación y fecha de compra, método de pago, entre otros datos captados por transacciones a través de la página web de dicho comercio.

"Se insta a los usuarios de los portales de compras en línea de estas empresas a cambiar sus contraseñas de inmediato", indicó el portal trinitense, el cual dio a conocer que ALPHV, también conocido como Black Cat, habría comprometido a más de 60 organizaciones en el último mes.

La cadena de supermercados PriceSmart se ha pronunciado ante el indicente mediante un comunicado.

> En PriceSmart nos esforzamos por proteger siempre los intereses de nuestros Socios en todo lo que hacemos. Por lo tanto, queremos compartir con usted una actualización importante sobre un evento reciente de ciberseguridad que afectó algunos de nuestros sistemas internos.
>
> Aunque aún no hemos encontrado evidencia que indique robo de identidad o fraude relacionado con este evento, queremos asegurarnos de ofrecerle la información sobre el incidente, nuestra respuesta y las medidas que estamos tomando para ayudar a proteger su información personal.
>
> Somos conscientes de que un grupo actor de delitos informáticos afirmó haber extraído datos de nuestros sistemas y hemos estado trabajando con expertos líderes en ciberseguridad para recopilar rápidamente los hechos mientras trabajamos para garantizar que los datos de los Socios permanezcan protegidos.

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