Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CIBERATAQUE A OLEODUCTO CANADIENSE: ALPHV AMENAZA CON FILTRAR 190GB DE INFORMACIÓN SENSIBLE

14 / 02 / 2024

CONTENIDO

INTRODUCCIÓN

Varias instituciones prominentes han sido presuntamente víctimas de sofisticados ataques cibernéticos, lo que ha generado preocupaciones sobre la preparación en materia de ciberseguridad a nivel global. Desde Trans-Northern Pipelines hasta SouthState Bank, estas organizaciones se han visto afectadas, lo que subraya la urgencia de medidas de protección mejoradas en todos los sectores empresariales.

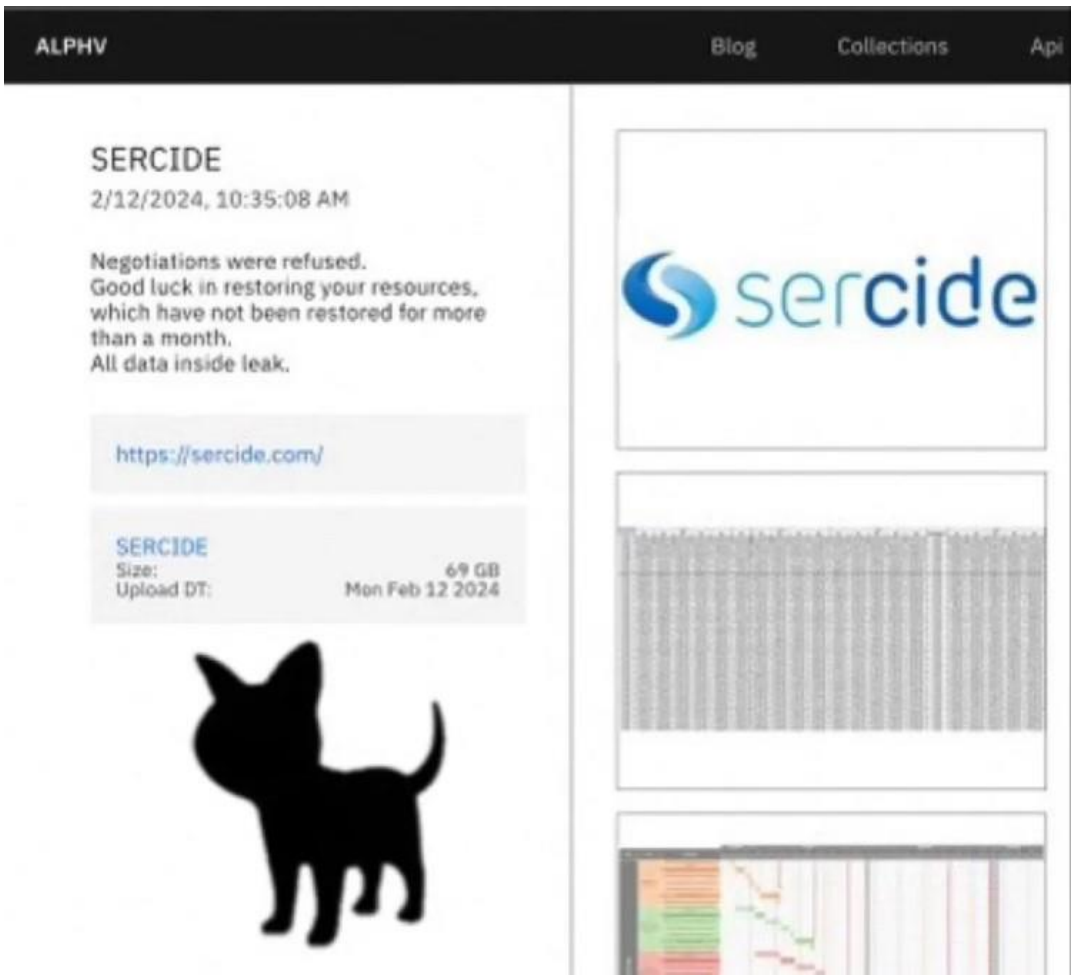
CIBERATAQUE A OLEODUCTO CANADIENSE: ALPHV AMENAZA CON FILTRAR 190GB DE INFORMACIÓN SENSIBLE

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

ID de alerta:	DSOC-CERT_2024_02_14_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	14/02/2024
Es día cero (0 day):	No

RESUMEN

El panorama de la ciberseguridad vuelve a sacudirse. Esta vez, el oleoducto canadiense Trans-Northern Pipelines se encuentra en medio de la tormenta tras ser presuntamente infiltrado por el grupo ALPHV/BlackCat. Los ciberdelincuentes afirman haber robado 190GB de datos "importantes", amenazando con filtrarlos si no reciben un pago.



Aunque ALPHV no ha especificado el contenido exacto de los datos robados, afirman que se trata de "información importante". Esto podría incluir:

Datos operativos del oleoducto: Fórmulas, diagramas, planes de mantenimiento, información sobre flujos y capacidad.

Información financiera y comercial: Contratos, acuerdos, datos de clientes y proveedores, secretos comerciales.

Datos personales: Información de empleados, contratistas y terceros relacionados con el oleoducto.

Trans-Northern Pipelines es una pieza clave de la infraestructura energética canadiense, operando kilómetros de tuberías en tres provincias. Una filtración de datos sensibles podría tener graves consecuencias:

Daños operativos: La publicación de información crítica podría facilitar futuros ataques o sabotajes al oleoducto.

Pérdidas económicas: La interrupción del servicio o la necesidad de implementar medidas de seguridad adicionales tendría un alto costo.

Daño reputacional: La filtración de información confidencial podría dañar la imagen de la empresa y sus socios.
Trans-Northern Pipelines ha confirmado que sufrió un incidente cibernético en noviembre de 2023, pero asegura que ya está contenido y no afecta las operaciones. Sin embargo, la investigación sobre las amenazas de ALPHV sigue en curso.

Este ataque es un recordatorio de la importancia de la ciberseguridad para las empresas e instituciones, especialmente aquellas que gestionan infraestructura crítica. Algunas medidas para reforzar la seguridad incluyen:

El caso de Trans-Northern Pipelines demuestra que nadie está a salvo de los ciberataques. Estar preparados y contar con medidas de seguridad sólidas es fundamental para minimizar los riesgos y proteger la información valiosa. Los atacantes exploraron archivos remotamente y utilizaron herramientas como MS Paint para revisar imágenes en sistemas remotos.

INDICADORES DE COMPROMISO

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

NOTICIA COMPLETA

https://devel.group/blog/ciberataque-a-oleoducto-canadiense-alphv-amenaza-con-filtrar-190gb-de-informacion-sensible/

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