Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

EL GRUPO RANSOMED.VC AFIRMA HABER HACKEADO “TODOS LOS SISTEMAS DE SONY”

26/09/2023

CONTENIDO

INTRODUCCIÓN

Un grupo de hackers de ransomware afirma haber hackeado “todos los sistemas de Sony” y están buscando compradores, con una fecha máxima del 28 de septiembre, que sería presumiblemente cuando lo publicarían.

GRUPO RANSOMED.VC

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

ID de alerta:	DSOC-CERT_2023_09_26_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	26/09/2023
Es día cero (0 day):	No

RESUMEN

Ransomed.vc solo ha estado operando desde septiembre, a pesar de algunos enlaces a foros y grupos anteriores. Sin embargo, en ese tiempo, el grupo ha acumulado una cantidad impresionante de víctimas, y Sony es una de ellas.

Ransomed.vc dijo en sus sitios de filtraciones, tanto en la web normal como en la red oscura, tomando una descripción directamente de Wikipedia: 'Sony Group Corporation, anteriormente Tokyo Telecommunications Engineering Corporation, y Sony Corporation, es una corporación multinacional conglomerada japonesa con sede en Minato, Tokio, Japón'.

"Hemos comprometido con éxito [sic] todos los sistemas de Sony. ¡No los rescataremos! Venderemos los datos. Debido a que Sony no quiere pagar. LOS DATOS ESTÁN A LA VENTA", añade el grupo, antes de declarar "LO ESTAMOS VENDIENDO".

El grupo incluye algunos datos de prueba de hackeo, pero en principio no son información especialmente convincente; parecen ser capturas de pantalla de una página de inicio de sesión interna, una presentación interna de PowerPoint que detalla los detalles del banco de pruebas y varios archivos de Java.

Ransomed.vc también ha publicado un árbol de archivos de toda la filtración, que parece tener menos de 6.000 archivos, aparentemente pequeños para “todos los sistemas Sony”. Aquí se incluyen “archivos de registro de compilación”, una amplia gama de recursos Java y archivos HTML.

Muchos de los archivos de ejemplo parecen presentar caracteres japoneses de forma destacada.

No se indica ningún precio para los datos, pero Ransomed.vc ha dejado los datos de contacto del servicio de mensajería Tox, así como los detalles de Telegram y correo electrónico.

El grupo también ha enumerado una “fecha de publicación” del 28 de septiembre de 2023. Si nadie compra los datos, esto es presumiblemente cuando Ransomed.vc los publicará al por mayor.

Al momento de escribir, Sony no ha hecho ninguna mención de un posible hackeo en sus sitios web.

Ransomed.vc parece ser tanto un operador de ransomware por derecho propio como una organización de ransomware-as-a-service; actualmente está anunciando la posibilidad de que ‘afiliados’ se registren.”

En el recuerdo de muchos sigue el devastador ataque informático que PlayStation Network sufrió en 2011, comprometiendo los nombres, direcciones y tarjetas de créditos de 77 millones de usuarios, por el que Sony pagó 15 millones de dólares en paquetes de compensaciones a los afectados.

RECOMENDACIONES

Si tiene una cuenta en PlayStation Network, se recomienda:

- Eliminar su tarjeta de crédito o débito de su cuenta
- Cambiar la contraseña de su cuenta
- Activar el factor de doble autenticación
- Al no conocer el momento del hackeo de Sony, y al existir la posibilidad de que se hayan comprometido los datos de la tarjeta, se recomienda monitorear las transacciones de su banca, o de confirmarse el hackeo se recomienda el cambio de tarjeta.

NOTICIA COMPLETA

https://devel.group/blog/el-grupo-ransomed-vc-afirma-haber-hackeado-todos-los-sistemas-de-sony/

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