

CYBER **SECURITY** **NEWS**

SECURITY OPERATIONS CENTER

**HACHEO AL ISSS DE EL SALVADOR:
CIBERINTELIGENCIASV EXPONE DATOS
SENSIBLES EN TELEGRAM**

06 / 09 / 2024

CONTENIDO

INTRODUCCIÓN	3
RESUMEN	6
CONTACTOS DE SOPORTE	8

INTRODUCCIÓN

El Instituto Salvadoreño del Seguro Social (ISSS) se enfrenta a una grave crisis de seguridad tras ser víctima de un ciberataque perpetrado por el grupo hacktivista CiberinteligenciaSV. En un acto de exposición masiva, el grupo robó y divulgó en Telegram una base de datos con 974,428 registros sensibles, dejando en evidencia la fragilidad de las medidas de seguridad del ISSS y generando alarma entre miles de salvadoreños cuya información personal podría estar comprometida.

HACKEO AL ISSS DE EL SALVADOR: CIBERINTELIGENCIASV EXPONE DATOS SENSIBLES EN TELEGRAM

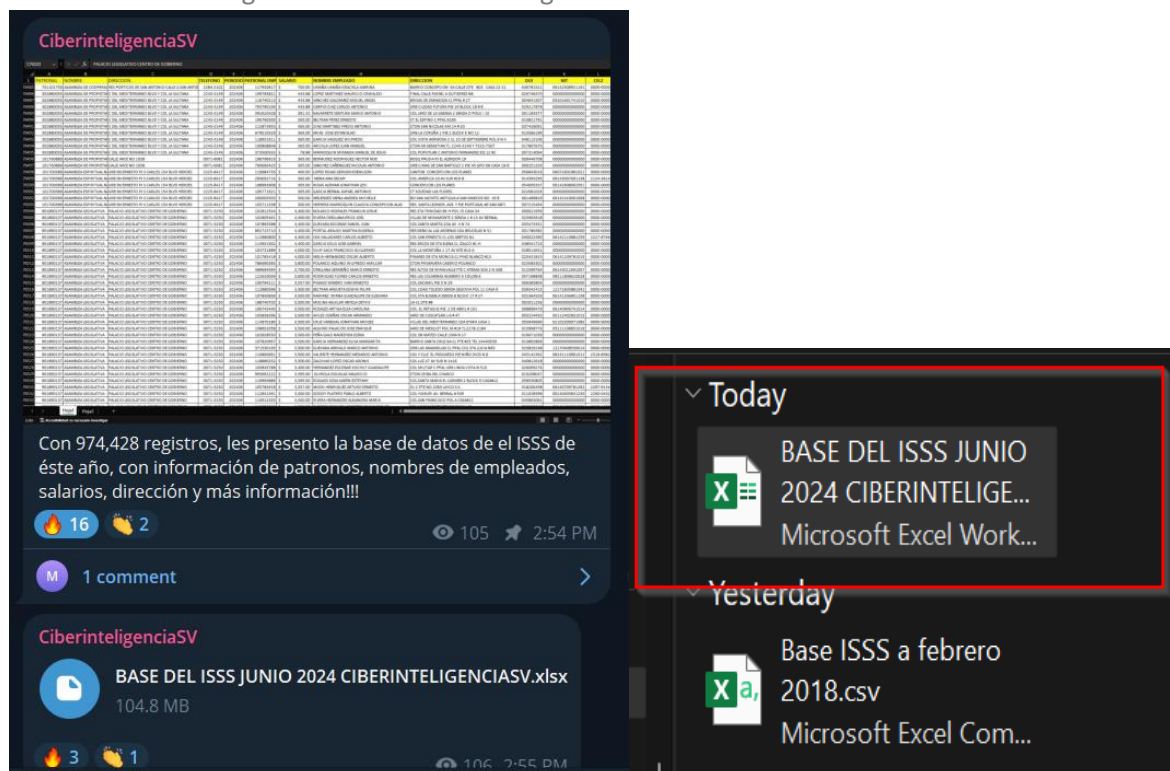
A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_09_06_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	CLEAR
Fecha de publicación:	06/09/2024
Es día cero (0 day):	No

RESUMEN

En un ataque cibernético sin precedentes, el grupo hacktivista CiberinteligenciaSV ha puesto en jaque al Instituto Salvadoreño del Seguro Social (ISSS) al robar y exponer su base de datos completa. Los datos, que incluyen información sensible de miles de personas, fueron compartidos hoy en la tarde en su grupo de Telegram, aunque la fecha exacta del ataque aún se desconoce.

El archivo divulgado, un Excel de 104.8 MB en formato .xlsx, contiene un total de 974,428 registros, evidenciando la magnitud de la brecha de seguridad.



The image shows a Telegram chat interface on the left and a Windows taskbar on the right. The Telegram chat is titled 'CiberinteligenciaSV' and contains a message from the same group: 'Con 974,428 registros, les presento la base de datos de el ISSS de éste año, con información de patronos, nombres de empleados, salarios, dirección y más información!!!'. Below the message is a file named 'BASE DEL ISSS JUNIO 2024 CIBERINTELIGENCIASV.xlsx' with a size of 104.8 MB. The Windows taskbar on the right shows two open files: 'BASE DEL ISSS JUNIO 2024 CIBERINTELIGENCIASV.xlsx' (Microsoft Excel Work...) and 'Base ISSS a febrero 2018.csv' (Microsoft Excel Com...).

Los datos, que incluyen información sensible de miles de personas, fueron compartidos hoy a las 12:55 p.m. en su grupo de Telegram, aunque la fecha exacta del ataque aún se desconoce.

El archivo divulgado, un Excel de 104.8 MB en formato .xlsx, contiene un total de 974,428 registros, evidenciando la magnitud de la brecha de seguridad. Los datos comprometidos podrían incluir información personal y médica de los afiliados al ISSS, lo que plantea serias preocupaciones sobre la privacidad y la seguridad de los afectados. Este incidente destaca nuevamente la vulnerabilidad de las instituciones públicas ante los ciberataques y la necesidad urgente de reforzar las medidas de seguridad para proteger la información crítica de los ciudadanos. Las autoridades aún no han emitido un comunicado oficial sobre el suceso, y se espera que la investigación continúe para determinar el alcance del ataque y los pasos a seguir. Recomendaciones: Es crucial que los usuarios del ISSS se mantengan atentos a cualquier actividad inusual en sus cuentas personales y consideren la posibilidad de cambiar sus contraseñas y monitorear sus estados financieros para detectar posibles usos indebidos de su información. Las instituciones, por su parte, deben fortalecer sus sistemas de seguridad y actualizar sus protocolos para prevenir futuros incidentes de esta naturaleza. Este caso refuerza la importancia de la ciberseguridad en la era digital y el impacto que puede tener un ataque en la vida de miles de personas.

Los datos comprometidos podrían incluir información personal y médica de los afiliados al ISSS, lo que plantea serias preocupaciones sobre la privacidad y la seguridad de los afectados.

Este incidente destaca nuevamente la vulnerabilidad de las instituciones públicas ante los ciberataques y la necesidad urgente de reforzar las medidas de seguridad para proteger la información crítica de los ciudadanos. Las autoridades aún no han emitido un comunicado oficial sobre el suceso, y se espera que la investigación continúe para determinar el alcance del ataque y los pasos a seguir.

Recomendaciones

Es crucial que los usuarios del ISSS se mantengan atentos a cualquier actividad inusual en sus cuentas personales y consideren la posibilidad de cambiar sus contraseñas y monitorear sus estados financieros para detectar posibles usos indebidos de su información. Las instituciones, por su parte, deben fortalecer sus sistemas de seguridad y actualizar sus protocolos para prevenir futuros incidentes de esta naturaleza.

Este caso refuerza la importancia de la ciberseguridad en la era digital y el impacto que puede tener un ataque en la vida de miles de personas.

NOTICIA COMPLETA

<https://devel.group/blog/hackeo-al-iss-de-el-salvador-ciberinteligenciasv-expone-datos-sensibles-en-telegram/>

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>