Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

HACKEO INÉDITO AL MINISTERIO DE EDUCACIÓN DE GUATEMALA: 529 GB DE DATOS EXPUESTOS POR RANSOMHUB

30/ 08 / 2024

CONTENIDO

INTRODUCCIÓN

El Ministerio de Educación de Guatemala ha sido blanco de un ciberataque sin precedentes, que expone graves fallos en la seguridad cibernética del país. El 21 de agosto de 2024, el grupo de ransomware RansomHub ejecutó un sofisticado hackeo, robando 529 GB de información sensible, incluidos archivos de compras y carpetas completas de los equipos comprometidos. A pesar de los esfuerzos por contener la crisis, los datos fueron revelados públicamente el 30 de agosto, generando preocupación y cuestionamientos sobre la protección de la información gubernamental. Este incidente resalta la necesidad urgente de fortalecer las medidas de seguridad en las instituciones públicas para evitar futuros ataques.

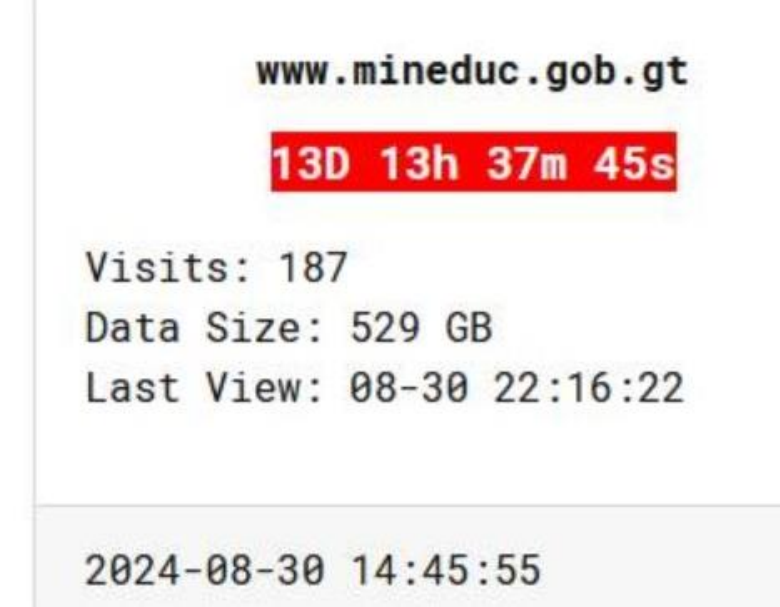
HACKEO INÉDITO AL MINISTERIO DE EDUCACIÓN DE GUATEMALA: 529 GB DE DATOS EXPUESTOS POR RANSOMHUB

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

ID de alerta:	DSOC-CERT_2024_08_30_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	30/08/2024
Es día cero (0 day):	No

RESUMEN

El Ministerio de Educación de Guatemala ha sido el objetivo de un ciberataque devastador, perpetrado por el grupo de ransomware conocido como RansomHub. El ataque, que tuvo lugar el 21 de agosto de 2024, resultó en la filtración de 529 GB de información confidencial, revelada públicamente el 30 de agosto de 2024.



Entre los datos expuestos, archivos de compras, y carpetas completas de los equipos comprometidos, se ha generado una ola de preocupación en la comunidad educativa y entre los empleados del Ministerio.


Sistema de Contabilidad Integrada Gubernamental
Ejecución de Gastos - Reportes - CUR de Ejecucion del Gasto
CUR del Gasto
Expresado en Quetzales
Unidad Ejecutora Igual a 325, Programa Igual a 16, Actividad Igual a 01, Subprograma Igual a 05, Clase Gasto Diferente 51E, Clase Gasto Diferente TRF, Clase Reg Diferente CYD
PAGINA : 1 DE 7
FECHA : 12/08/2024
HORA : 9:01:22
REPORTE: R00804107.rpt
EJERCICIO: 2024
ENTIDAD: 11130000.325.00 DIRECCIÓN DEPARTAMENTAL DE EDUCACIÓN GUATEMALA ORIENTE

pic_MINEDUCGT_2.png 82.38 KB

tal entity in charge of administering, supervising and coordinating the entire educational field in the department of Quetzaltenango

En respuesta a este grave incidente, el Ministerio de Educación de Guatemala emitió un comunicado oficial en el que se destaca lo siguiente:

1. Los datos sensibles de estudiantes y personal están protegidos, y se están evaluando los posibles daños en las aplicaciones informáticas.
2. Se implementaron medidas inmediatas para asegurar la continuidad de los programas de apoyo y la nómina de salarios.
3. Se trabaja meticulosamente para restablecer los sistemas y prevenir futuros ataques.
4. Se ha presentado la denuncia correspondiente ante las autoridades.

Ministerio de Educación

Comunicado Oficial del Ministerio de Educación de Guatemala

El Ministerio de Educación de Guatemala informa que la semana pasada se produjo un ataque cibernético a nuestros sistemas informáticos; no obstante, para tranquilidad de los usuarios y de la comunidad educativa, comunicamos lo siguiente:

1. Los datos sensibles de estudiantes y personal del Ministerio de Educación están resguardados en nuestra base de datos. Se están determinando los posibles daños que hayan sufrido las aplicaciones informáticas.

2. Se tomaron acciones inmediatas tras la detección del ataque, para proteger la ejecución de los programas de apoyo, la nómina de salarios y continuar con el normal funcionamiento de la institución.

3. Estamos trabajando de manera cuidadosa, para restablecer plenamente el funcionamiento de nuestros sistemas y evitar nuevos incidentes.

4. Por los hechos indicados se presentó la denuncia correspondiente.

   Agradecemos su comprensión y solicitamos que no se dejen sorprender por información falsa o de fuentes no oficiales.

Guatemala, 30 de agosto de 2024.

PBX: (502) 2411-9595 www.mineduc.gob.gt

A pesar de las afirmaciones del Ministerio sobre la seguridad de los datos más sensibles, la información filtrada y el tipo de documentos comprometidos indican una brecha significativa en la seguridad cibernética de la institución. Este ataque no solo pone en riesgo la privacidad de los involucrados, sino que también deja en evidencia las vulnerabilidades en la infraestructura tecnológica del gobierno guatemalteco.

El comunicado oficial del Ministerio hace un llamado a la calma, instando a la población a no caer en desinformación; sin embargo, el impacto de este ataque resuena más allá de lo comunicado, y plantea serias preguntas sobre la preparación y respuesta ante amenazas cibernéticas de esta magnitud.

Este caso subraya la urgencia de reforzar las defensas cibernéticas en las instituciones públicas del país, para evitar que ataques similares pongan en jaque la seguridad nacional.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20240405_1_RansomHub

NOTICIA COMPLETA

https://devel.group/blog/ataque-de-ransomware-revela-masivo-robo-de-datos-del-ministerio-de-educacion-de-guatemala/

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