

SECURITY

SECURITY OPERATIONS CENTER

GRUPO DE RANSOMWARE RANSOMHUB ATACA EMPRESA AVÍCOLA EN GUATEMALA

06/11/2024



CONTENIDO

INTRODUCCIÓN	3
RESUMEN	5
INDICADORES DE COMPROMISO	
NOTICIA COMPLETA	
CONTACTOS DE SOPORTE	7



INTRODUCCIÓN

Una reciente amenaza de ciberseguridad ha afectado a una importante empresa avícola en Guatemala, luego de que el grupo de ransomware RansomHub ejecutara un ataque y robara 300 GB de información sensible. Este grupo de cibercriminales, conocido por sus tácticas de "doble extorsión", no solo cifra los datos de sus víctimas, sino que también las amenaza con divulgar la información robada si no reciben el pago exigido. El incidente subraya la importancia de que las empresas en sectores críticos, como el alimentario, fortalezcan sus defensas ante el aumento de ciberataques sofisticados y de alto impacto en sus operaciones y en la seguridad de su información.



GRUPO DE RANSOMWARE RANSOMHUB ATACA EMPRESA AVÍCOLA EN GUATEMALA

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

ID de alerta:	DSOC-CERT_2024_11_06_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	CLEAR
Fecha de publicación:	06/11/2024
Es día cero (0 day):	No



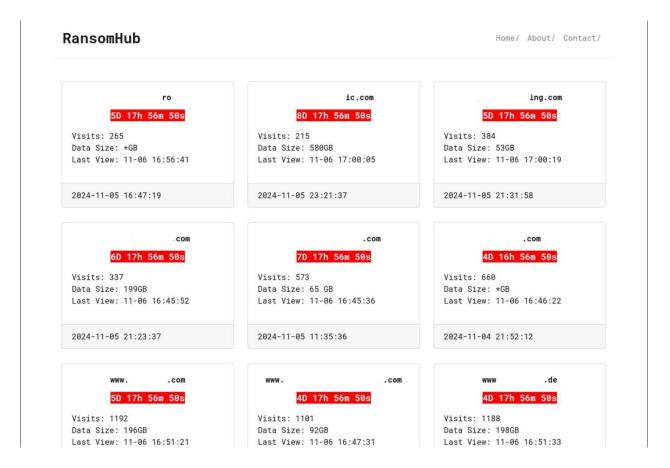
RESUMEN

El grupo de ransomware RansomHub ha lanzado un nuevo ataque, esta vez dirigido a una reconocida empresa avícola de Guatemala, robando aproximadamente 300 GB de información crítica. Aunque aún no se conoce la magnitud exacta del impacto, la pérdida de estos datos ha generado preocupaciones significativas sobre la seguridad de la información y la continuidad operativa de la empresa afectada.

¿Quién es RansomHub?

RansomHub es un grupo de cibercriminales especializado en ataques de "doble extorsión". Su metodología incluye cifrar los datos de sus víctimas y, además, amenazarlas con la publicación de información confidencial en caso de que no se realice el pago del rescate exigido. Este grupo utiliza diversos métodos para infiltrarse en las redes de sus objetivos, entre los que destacan el aprovechamiento de vulnerabilidades en sistemas expuestos a internet y ataques de phishing altamente dirigidos a empleados clave. Una vez dentro, buscan escalar privilegios y desplazarse lateralmente por la red para localizar y cifrar archivos sensibles.

RansomHub ha centrado sus ataques en sectores industriales, como el avícola, debido al alto valor de sus datos y al impacto significativo que una interrupción en sus operaciones puede generar en la cadena de suministro y en el servicio a clientes y proveedores.





Recomendaciones de Seguridad para Mitigar el Riesgo

Para protegerse contra los ataques de grupos de ransomware como RansomHub, es fundamental que las organizaciones refuercen sus defensas de ciberseguridad y adopten medidas preventivas. A continuación, algunas recomendaciones clave:

- Implementación de autenticación multifactor (MFA): Asegurar el acceso a cuentas con privilegios mediante autenticación multifactor reduce significativamente las posibilidades de que los atacantes puedan explotar cuentas administrativas o de usuarios críticos.
- 2. **Monitoreo y análisis de la red**: La supervisión constante de la actividad en la red puede ayudar a identificar patrones de comportamiento anómalos y potenciales amenazas en sus primeras etapas, permitiendo una respuesta temprana a intentos de intrusión.
- 3. **Respaldo y recuperación de datos**: Establecer copias de seguridad regulares y almacenarlas de forma aislada garantiza que, en caso de un ataque, los datos críticos puedan recuperarse sin necesidad de pagar un rescate.
- 4. **Actualización y parcheo de sistemas**: Mantener los sistemas operativos, aplicaciones y dispositivos actualizados con los últimos parches de seguridad es esencial para reducir el riesgo de que los cibercriminales aprovechen vulnerabilidades conocidas.
- 5. **Entrenamiento continuo al personal**: La concienciación sobre amenazas de ciberseguridad y el entrenamiento para identificar ataques de phishing pueden ser cruciales para evitar que los empleados caigan en tácticas de engaño utilizadas por grupos como RansomHub.

Conclusión

Este incidente destaca la importancia de una postura de ciberseguridad proactiva, especialmente en sectores como el avícola, que son fundamentales para la economía y que pueden enfrentar riesgos sustanciales en caso de interrupciones. A medida que grupos como RansomHub intensifican sus actividades, es crucial que las empresas guatemaltecas y de toda la región refuercen sus medidas de seguridad para protegerse de estos ciberataques y minimizar el impacto en sus operaciones.

INDICADORES DE COMPROMISO

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

NOTICIA COMPLETA

https://devel.group/blog/grupo-de-ransomware-ransomhub-ataca-empresa-avicola-en-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