Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

IMPORTANTE ADVERTENCIA CONJUNTA DE AGENCIAS DE SEGURIDAD SOBRE LA OPERACIÓN DE RANSOMWARE AKIRA

19 / 04 / 2024

CONTENIDO

INTRODUCCIÓN

Las agencias de seguridad han lanzado una advertencia conjunta sobre la operación de ransomware conocida como Akira, que ha causado estragos en más de 250 organizaciones y ha generado ganancias exorbitantes de aproximadamente $42 millones de dólares en pagos de rescate. Desde su surgimiento en marzo de 2023, Akira ha destacado por su capacidad para atacar diversas industrias en todo el mundo, mostrando una evolución constante en sus técnicas y estrategias.

IMPORTANTE ADVERTENCIA CONJUNTA DE AGENCIAS DE SEGURIDAD SOBRE LA OPERACIÓN DE RANSOMWARE AKIRA

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

ID de alerta:	DSOC-CERT_2024_04_19_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	19/04/2024
Es día cero (0 day):	No

RESUMEN

Una alerta conjunta emitida por el FBI, CISA, el Centro Europeo de Ciberdelincuencia (EC3) de Europol y el Centro Nacional de Seguridad Cibernética de los Países Bajos (NCSC-NL) ha puesto de manifiesto la alarmante actividad de la operación de ransomware Akira. Desde su surgimiento en marzo de 2023, este grupo ha perpetrado ataques a más de 250 organizaciones, generando ganancias cercanas a los $42 millones de dólares en pagos de rescate.

Creciente Amenaza

Akira ha ganado notoriedad al dirigirse a una amplia gama de industrias a nivel mundial. Incluso, para junio de 2023, habían desarrollado y desplegado un cifrador Linux para atacar las máquinas virtuales VMware ESXi, ampliamente utilizadas en organizaciones empresariales.

Demanda de Rescate

Los operadores de Akira están exigiendo rescates que oscilan entre los $200,000 y varios millones de dólares, dependiendo del tamaño de la organización comprometida. Los datos de negociación obtenidos revelan esta alarmante realidad.

Impacto Global
Desde marzo de 2023, Akira ha impactado tanto a empresas como a entidades de infraestructura crítica en América del Norte, Europa y Australia. Entre sus víctimas más recientes se encuentran Nissan Oceanía y la Universidad de Stanford, con miles de individuos afectados por violaciones de datos.

Consejos para la Defensa
Las agencias de seguridad han emitido recomendaciones para mitigar los riesgos asociados con los ataques de este grupo de ransomware. Se enfatiza la importancia de parchear vulnerabilidades, implementar autenticación multifactor (MFA) y mantener actualizado el software.

Llamado a la Acción
El FBI, CISA, EC3 y NCSC-NL instan a las organizaciones a implementar las medidas de mitigación propuestas para reducir la probabilidad e impacto de futuros incidentes de ransomware.

Conclusión
La amenaza representada por la operación Akira es significativa y en constante evolución. La colaboración entre agencias de seguridad y la adopción de prácticas de ciberseguridad robustas son fundamentales para protegerse contra este tipo de ataques.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20240419_1_AkiraRansomware

NOTICIA COMPLETA

https://devel.group/blog/importante-advertencia-conjunta-de-agencias-de-seguridad-sobre-la-operacion-de-ransomware-akira/

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