Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

RANSOMHUB LOGRA FILTRAR 487 GB DE INFORMACIÓN DE SOCIEDAD DE AHORRO Y CRÉDITO CONSTELACIÓN

05 / 04 / 2024

CONTENIDO

INTRODUCCIÓN

El panorama del ransomware se enfrenta a una nueva amenaza con la emergencia de un actor destacado: RansomHub. Este grupo ha llamado la atención al respaldar sus reclamos con filtraciones de datos, marcando su presencia con un ataque dirigido a la Sociedad de Ahorro y Crédito Constelación de El Salvador. Con la advertencia de filtrar 497 GB de información, incluyendo datos de clientes, RansomHub ha puesto en alerta a la comunidad de ciberseguridad. En esta noticia, exploraremos quién es RansomHub, cómo opera y los últimos desarrollos que subrayan su impacto en el mundo del ransomware.

RANSOMHUB LOGRA FILTRAR 487 GB DE INFORMACIÓN DE SOCIEDAD DE AHORRO Y CRÉDITO CONSTELACIÓN

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

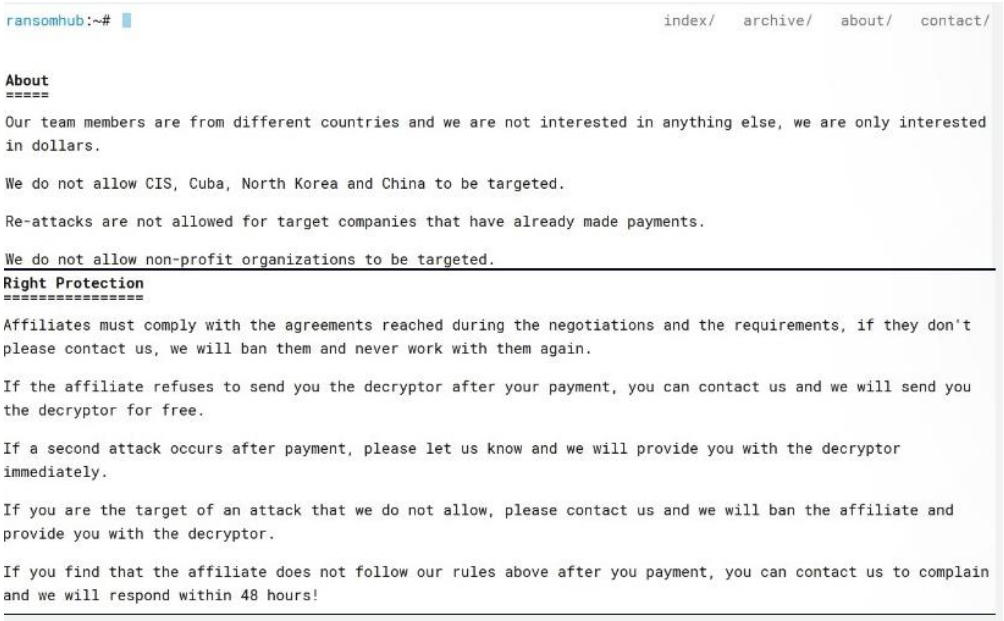
ID de alerta:	DSOC-CERT_2024_04_05_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	05/04/2024
Es día cero (0 day):	No

RESUMEN

En el paisaje del ransomware, ha surgido un nuevo actor amenazante: RansomHub. Destacándose por respaldar sus afirmaciones con filtraciones de datos, este grupo ha marcado su presencia con un ataque dirigido a la Sociedad de Ahorro y Crédito Constelación de El Salvador. Con la amenaza de filtrar 497 GB de información, incluyendo datos de clientes, RansomHub ha puesto en alerta a la comunidad de ciberseguridad.

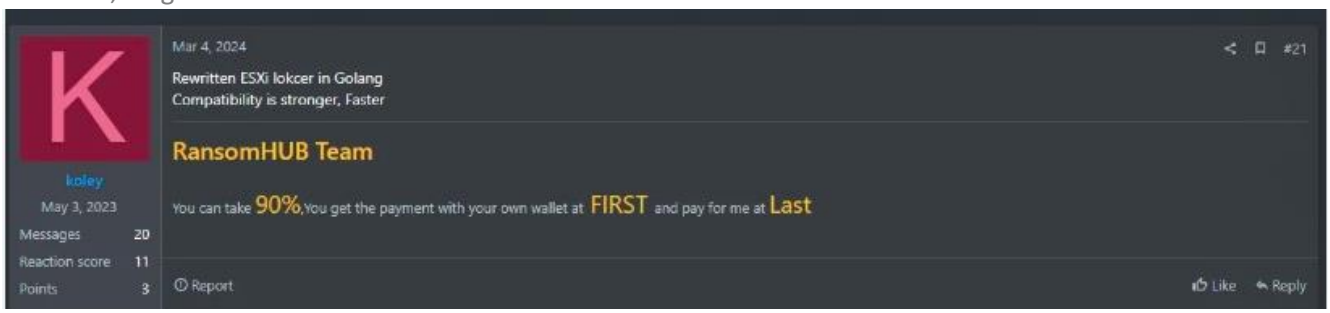
¿QUIÉN ES RANSOMHUB?

Según su página “Acerca de”, RansomHub está compuesto por hackers de diversas ubicaciones globales, unidos por el objetivo de obtener ganancias financieras. El grupo explicita que no ataca a países específicos ni a organizaciones sin fines de lucro. Funcionando como un grupo de ransomware en colaboración con afiliados, RansomHub se clasifica como un Ransomware como Servicio (RaaS).



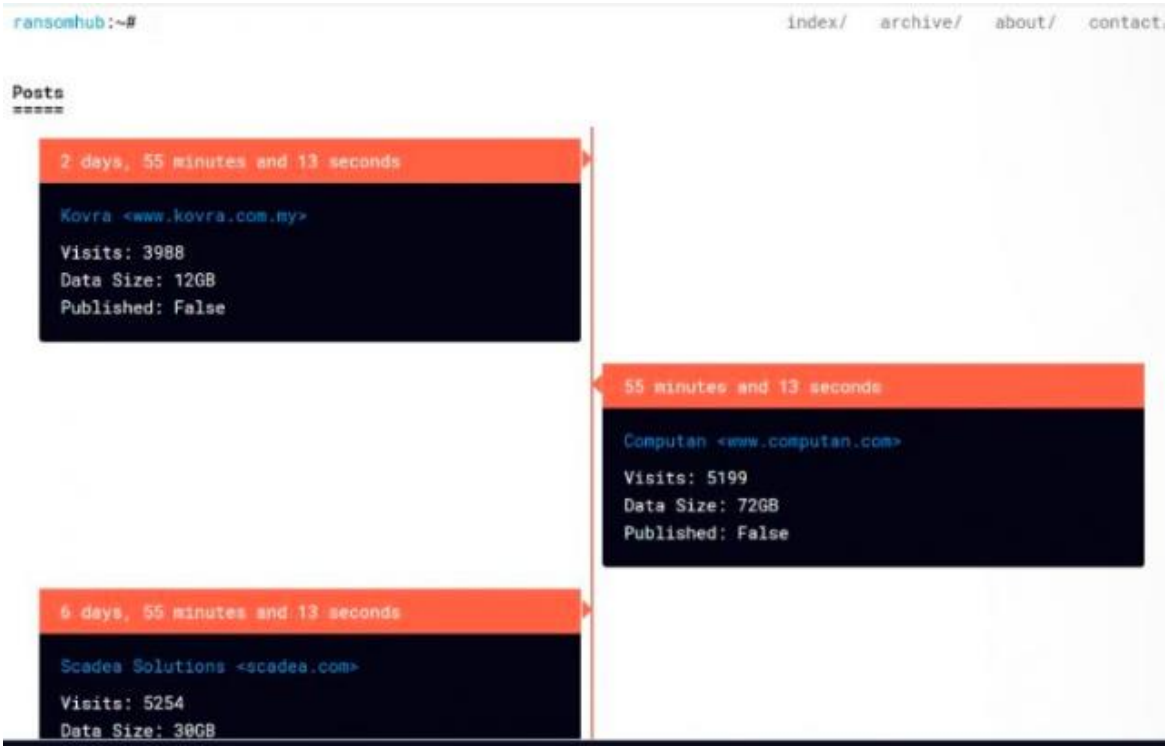
¿CÓMO OPERA?

RansomHub recluta principalmente a sus afiliados del foro RAMP, con una estructura que asigna el 90% de las ganancias a los afiliados y el 10% al grupo principal. Este enfoque, que contrasta con las prácticas comunes, ha ganado el reconocimiento en la comunidad de ransomware.



VICTIMOLOGÍA

En su sitio de filtración de datos, los propios afiliados de RansomHub manejan las publicaciones, sin seguir un patrón específico en las víctimas. Desde instituciones de atención médica hasta empresas manufactureras, una amplia gama de sectores se ve afectada por sus ataques.



ÚLTIMOS DESARROLLOS

El grupo también alberga datos de muestra de víctimas de las cuales no pudo recibir pago, disponibles para su descarga en su sitio web. Esta táctica agresiva de filtración de datos subraya la amenaza que representa RansomHub en el mundo del ransomware.

En resumen, la presencia de RansomHub exige una respuesta proactiva y coordinada de la comunidad de ciberseguridad. Su enfoque distintivo en la colaboración con afiliados y su táctica agresiva de filtración de datos lo convierten en una amenaza significativa que no debe subestimarse.

INDICADORES DE COMPROMISO

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

NOTICIA COMPLETA

https://devel.group/blog/ransomhub-logra-filtrar-487-gb-de-informacion-de-sociedad-de-ahorro-y-credito-contelacion/

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