Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

NUEVO RANSOMWARE SEXI: UNA AMENAZA PARA LOS SERVIDORES VMWARE ESXI

05 / 04 / 2024

CONTENIDO

INTRODUCCIÓN

En un golpe sorpresivo al mundo de la ciberseguridad empresarial, la firma de hosting IxMetro Powerhost se encuentra en el epicentro de un ataque devastador perpetrado por un nuevo y despiadado grupo de ransomware conocido como SEXi. La incursión en los servidores VMware ESXi de la empresa ha dejado a numerosos clientes en una situación de crisis, con sus datos cifrados y sus servicios inaccesibles. Este ataque no solo resalta la constante evolución de las amenazas cibernéticas, sino también la urgente necesidad de fortalecer las defensas digitales en un mundo cada vez más interconectado.

NUEVO RANSOMWARE SEXI: UNA AMENAZA PARA LOS SERVIDORES VMWARE ESXI

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

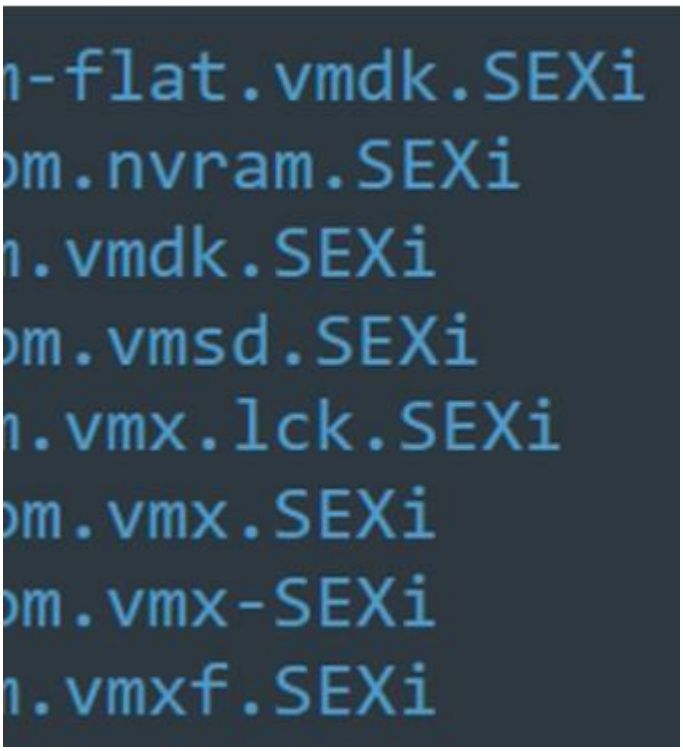
ID de alerta:	DSOC-CERT_2024_04_05_2
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	05/04/2024
Es día cero (0 day):	No

RESUMEN

El mundo digital se ve una vez más sacudido por un nuevo ataque cibernético, esta vez dirigido hacia la firma de hosting IxMetro Powerhost. Este proveedor de centros de datos y alojamiento ha sido blanco de un ataque perpetrado por una nueva banda de ransomware conocida como SEXi, dejando a su división chilena, IxMetro, en un estado de emergencia.

El Ataque

IxMetro Powerhost, una empresa con ubicaciones en Estados Unidos, Sudamérica y Europa informó a sus clientes sobre un ataque de ransomware que ocurrió durante la madrugada del sábado pasado. Los servidores VMware ESXi de la compañía, utilizados para alojar servidores privados virtuales (VPS) para clientes, fueron cifrados, dejando fuera de servicio los sitios web y servicios alojados en estos servidores.



Demanda del Rescate

La situación se vuelve aún más preocupante cuando se revela que los backups también han sido cifrados, dificultando enormemente la restauración de los servidores afectados. La banda de ransomware SEXi exige un rescate de dos bitcoins por cada víctima, lo que equivaldría a $140 millones de dólares. Sin embargo, el CEO de PowerHost, Ricardo Rubem, ha declarado que las agencias de seguridad recomiendan no negociar con los criminales, ya que la mayoría de las veces desaparecen después del pago.

El Ransomware SEXi

El ransomware, que añade la extensión .SEXi a los archivos cifrados, ha sido identificado por investigadores de seguridad como una nueva amenaza. Hasta el momento, se ha observado que los ataques se centran exclusivamente en servidores VMware ESXi, lo que explica el nombre 'SEXi', haciendo un juego de palabras

con 'ESXi'. Los archivos cifrados se acompañan de notas de rescate con instrucciones para contactar a los atacantes a través de la aplicación de mensajería Session.

Variantes Conocidas

Aunque no se ha podido obtener una muestra del cifrador SEXi, investigadores han identificado otras variantes, como SOCOTRA, FORMOSA y LIMPOPO, que utilizan un enfoque similar. Estas variantes también se basan en el código fuente filtrado del ransomware Babuk y han sido empleadas para cifrar archivos en servidores ESXi.

Conclusiones

La incursión del ransomware SEXi plantea serias preocupaciones sobre la seguridad cibernética en el mundo empresarial. Las empresas deben mantenerse alerta y fortalecer sus medidas de seguridad para protegerse contra estas amenazas emergentes. En un mundo donde la ciberdelincuencia evoluciona constantemente, la prevención y la preparación son fundamentales para mitigar los riesgos y proteger los activos digitales de las organizaciones.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/main/20240405_02_SEXiRansomware

NOTICIA COMPLETA

https://devel.group/blog/nuevo-ransomware-sexi-una-amenaza-para-los-servidores-vmware-esxi/

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