Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 124	Fecha: 27-05-2023 Página 4 de 22

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Ransomware contra sistemas de virtualización y Linux cada vez más comunes		
Tipo de ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	Red, Internet, Correo Electronico, Redes Sociales, etc.		
Código de familia	C	Código de subfamilia	C01
Clasificación temática familia	Intento de intrusión		

Descripción

Según el análisis de los investigadores de ciberseguridad de Trend Micro, los servidores Linux están "cada vez más bajo el fuego" de los ataques de ransomware, con un aumento del 75 % en las detecciones en el transcurso del último año 2022, ya que los ciberdelincuentes buscan expandir sus ataques más allá de los sistemas operativos Windows.

DETALLES:

- La popularidad del código abierto y la virtualización está en aumento, lo que significa que cada vez hay más servidores que ejecutan Linux o VMWare ESXi. Estos suelen almacenar una gran cantidad de información crítica que, si se cifra, puede paralizar al instante las operaciones de una empresa. Y, dado que la seguridad de los sistemas Windows ha sido tradicionalmente el centro de atención, el resto de los servidores están demostrando ser una presa fácil.

- En febrero del 2023, muchos propietarios de servidores VMware ESXi se vieron afectados por el brote de ransomware ESXiArgs. Aprovechando la vulnerabilidad CVE-2021-21974, los atacantes deshabilitaron las máquinas virtuales y cifraron los archivos .vmxf, .vmx, .vmdk, .vmsd y .nvram.

- El famoso grupo Clop, conocido por un ataque a gran escala contra los servicios vulnerables de transferencia de archivos Fortra GoAnywhere a través de la CVE-2023-0669, fue detectado en diciembre del 2022 usando, aunque con limitaciones, una versión para Linux de su ransomware. Esta se diferencia significativamente de su equivalente para Windows (carece de algunas optimizaciones y trucos defensivos), pero se adapta a los permisos y tipos de usuarios de Linux y se dirige específicamente a las carpetas de bases de datos de Oracle.

- El ransomware BlackCat, escrito en Rust, también puede deshabilitar y eliminar máquinas virtuales ESXi. En otros aspectos, el código malicioso difiere ligeramente de la versión de Windows.

- El ransomware Luna, que detectamos en el 2022, era originalmente una multiplataforma, capaz de ejecutarse en sistemas Windows, Linux y ESXi. Y, por supuesto, el grupo LockBit difícilmente pudo ignorar esta tendencia y también comenzó a ofrecer versiones para ESXi de su malware a los afiliados.

```
C:\Samples>luna.exe -help
How to use:
C:\Samples\luna.exe (Start encryption of all drives)
C:\Samples\luna.exe -file C:/test/test.txt (Encrypts test.txt in C:/test/ directory)
C:\Samples\luna.exe -dir C:/test/ (Encrypts C:/test/ directory)
```

- En cuanto a los ataques más antiguos estaban las campañas RansomEXX y QNAPCrypt, que afectaron en gran medida a los servidores Linux.

- Para penetrar en servidores Linux, generalmente hay que explotar vulnerabilidades. Los atacantes pueden convertir estas vulnerabilidades en armas dentro del sistema operativo, los servidores web y otras aplicaciones básicas, así como en las aplicaciones corporativas, las bases de datos y los sistemas de virtualización. Como demostró Log4Shell el año pasado, las vulnerabilidades en los componentes de código abierto requieren una atención especial. Después de una infracción inicial, muchas cepas del ransomware utilizan trucos o vulnerabilidades adicionales para elevar los privilegios y cifrar el sistema.

RECOMENDACIONES:

- Actualizar e instalar las vulnerabilidades de inmediato.
- Minimizar la cantidad de conexiones y puertos abiertos a Internet.
- Implementar herramientas de seguridad especializadas en servidores para proteger tanto el propio sistema operativo como las máquinas virtuales y los contenedores alojados en el servidor.

Fuentes de información	▪ hxxps://blog.segu-info.com.ar/2023/05/ransomware-contra-sistemas-de.html ▪ Análisis propio de fuentes abiertas.