CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Amenaza Cibernética

Fecha: **12/10/2022**

Problemática: **Nuevo método de eliminación de copia de seguridad**

Correlativo: **AA-0042**

Institución / Sector: **Instituciones Públicas y Privadas**

CONTEXTO

Recientemente se ha hecho pública una investigación sobre una nueva técnica utilizada por ciberdelincuentes que buscan la eliminación de instantáneas de volumen de máquinas virtuales. Según mencionan en la investigación se descubrió que la técnica utilizadas por los actores de amenazas aún podría estar en desarrollo y posiblemente la perfeccionen conforme el tiempo, lo que el impacto podría ser sumamente crítico.

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	Preventiva

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	Alta	Alta	Alta

SITUACIÓN

La información obtenida a raíz de la investigación realizada por el Centro Estratégico de Monitoreo – CEM, este nuevo ransomware utiliza las bibliotecas COM (Modelo de objetos componentes) de Windows como una solución de respaldo legítima para eliminar todas las instantáneas de volumen, lo que resulta en la incapacidad de restaurar desde la copia de seguridad o recuperar archivos anteriores o versiones de archivos. Este utiliza un servicio de Volume Shadow Copy que es una función integrada de Windows que permite la creación de copias de seguridad instantáneas de archivos informáticos o discos completos y, a menudo, facilita otras soluciones comerciales de copia de seguridad.

Esta técnica se descubrió en lo que parece ser una nueva muestra del ransomware HelloXD, esta familia de ransomware es conocida por los ataques de doble extorsión en los que roban los datos de las víctimas antes de cifrar los dispositivos.

RECOMENDACIONES

Recomendaciones generales aplicando Mittre:

- **Filtrar tráfico de red: El tráfico a las redes de anonimato conocidas y la infraestructura C2 se puede bloquear mediante el uso de listas de bloqueo y permisos de red. Cabe señalar que este tipo de bloqueo puede evitarse mediante otras técnicas como Domain Fronting.**
- **Prevención de intrusiones en la red: Los sistemas de detección y prevención de intrusiones en la red que usan firmas de red para identificar el tráfico de malware adversario específico se pueden usar para mitigar la actividad a nivel de red.**
- **Inspección SSL/TLS: Si es posible inspeccionar el tráfico HTTPS, las capturas se pueden analizar en busca de conexiones que parezcan estar al frente del dominio.**

En la medida de lo posible, las copias de seguridad deben mantenerse fuera de línea y completamente inaccesibles para el ransomware.

DICCIONARIO DE DATOS

Ataque de fuerza bruta: Procedimiento para averiguar una contraseña que consiste en probar todas las combinaciones posibles hasta encontrar la combinación correcta.
Ransomware: Malware cuya funcionalidad es «secuestrar» un dispositivo (en sus inicios) o la información que contiene de forma que, si la víctima no paga el rescate, no podrá acceder a ella.
Ciberdelincuente: Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos.
Parche de seguridad: Conjunto de cambios que se aplican a un software para corregir errores de seguridad en programas o sistemas operativos.

REFERENCIAS

1. https://blogs.vmware.com/security/2022/09/threat-report-illuminating-volume-shadow-deletion.html
2. https://blogs.vmware.com/security/2022/09/threat-research-new-method-of-volume-shadow-backup-deletion-seen-in-recent-ransomware.html
3. https://attack.mitre.org/techniques/T1090/

ÁREA PARA DEFINICIONES