

Modificación de memoria

¿Qué es la modificación de memoria?

La modificación de memoria, tal como Cyber Crucible utiliza el término, ocurre cuando las secciones ejecutables de la memoria de un proceso han sido modificadas de manera anormal. La ejecución normal de un proceso dado, sin manipulación externa, no desencadena estas modificaciones; son distintas de las operaciones normales de "memoria volátil" dentro de un proceso.

Una técnica común de modificación de memoria es el "process hollowing" (vaciado de procesos), donde un atacante inicia un proceso víctima en la máquina, a menudo comenzando en un estado suspendido, y cambia el código ejecutable para que en realidad ejecute el código de algún otro programa.

Tácticas relevantes de MITRE:

- [MITRE T1055](#) - Inyección de procesos, generalmente utilizada para ejecutar código malicioso dentro de un proceso objetivo mientras se permite que el proceso original continúe.
- [MITRE T1055-12](#) - Inyección de procesos mediante el reemplazo de código en un proceso, típicamente antes de que comience su ejecución.
- [MITRE T1559](#) - La comunicación entre procesos puede proporcionar control sobre el proceso objetivo desde el inyector una vez que se completa la inyección.
- [MITRE T1548](#) - El abuso del control de elevación puede permitir que un proceso que normalmente no tendría privilegios más altos sea escalado para obtener acceso a datos protegidos.

¿Cuáles son las consecuencias?

Las modificaciones de memoria pueden tener consecuencias muy similares a otras técnicas de inyección de procesos, pero son aún más evasivas. Dado que no hay creación de hilos remotos ni llamadas a funciones externas, a menudo puede ser muy difícil detectar las modificaciones de memoria, y aún más difícil atribuir las a un proceso en particular.

Un proceso cuya memoria ha sido modificada puede ser forzado a llevar a cabo actividad maliciosa que de otro modo no habría realizado. No se debe confiar en ningún proceso con memoria ejecutable que haya sido manipulada, ya que no es un evento normal en las comunicaciones o interacciones entre procesos.

¿Qué hace Cyber Crucible?

Cyber Crucible monitorea el estado de la memoria de un proceso a lo largo de su ciclo de vida. Si se considera que la memoria ha sido manipulada, el proceso se marca y se considera no confiable. En el momento en que ocurre un evento de extorsión, se toma una instantánea de la memoria para proporcionarla durante posibles investigaciones de respuesta a incidentes (IR).

La instantánea de memoria contiene la memoria ejecutable original, sin manipular, y cualquier "diferencia" ("diffs"), junto con sus desplazamientos ("offsets") dentro de la memoria del proceso. El análisis de estos volcados de memoria puede ser complicado, pero puede proporcionar evidencia sólida sobre los comportamientos del código malicioso.

¿Cómo puedo saberlo?

Cyber Crucible Indicates Responses with Modified Memory

Cyber Crucible indica respuestas con memoria modificada

La memoria modificada es más difícil y más efímera de rastrear que otros métodos de inyección de procesos. En su lugar, proporcionamos un valor booleano rápido para ver que la modificación ocurrió, y a partir de ahí, analizar las diferencias de memoria reales requiere una investigación más profunda.

Some raw memory

Memoria sin procesar

Disassembled memory

Memoria desensamblada

Recopilar la memoria es solo el primer paso; incluso después del desensamblado, el código puede estar muy ofuscado y ser difícil de leer. La buena noticia es que tenemos mucho con qué trabajar para este análisis cuando contamos con la memoria original, los metadatos asociados, el ejecutable original y las propias instrucciones del ejecutable modificado.

1. sí, 2.

Escenarios de ejemplo:

- [Escenario de capacitación - Modificación de memoria](#)

Revision #1

Created 2026-07-24 01:11:51 UTC by Dennis Underwood

Updated 2026-07-24 01:11:52 UTC by Dennis Underwood