

Modificação de Memória

O que é modificação de memória?

Modificação de memória, como a Cyber Crucible utiliza o termo, ocorre quando as seções executáveis da memória de um processo foram modificadas de formas anormais. A execução normal de um determinado processo, sem interferência externa, não desencadeia essas modificações – elas são distintas das operações normais de "memória volátil" dentro de um processo.

Uma técnica comum de modificação de memória é o process hollowing, na qual um atacante inicia um processo vítima na máquina, geralmente iniciando em estado suspenso, e altera o código executável para efetivamente executar o código de outro programa.

Táticas relevantes do MITRE:

- [MITRE T1055](#) - Injeção de processo, normalmente usada para executar código malicioso em um processo alvo, permitindo que o processo original continue.
- [MITRE T1055-12](#) - Injeção de processo por substituição de código em um processo, tipicamente antes que ele inicie a execução.
- [MITRE T1559](#) - A comunicação entre processos (Inter-Process communication) pode fornecer controle sobre o processo alvo ao injetor, uma vez concluída a injeção.
- [MITRE T1548](#) - O abuso de controles de elevação pode permitir que um processo que normalmente não teria privilégios mais altos seja escalado para obter acesso a dados protegidos.

Quais são as consequências?

As modificações de memória podem ter consequências muito semelhantes às de outras técnicas de injeção de processo, mas são ainda mais evasivas. Como não há criação de threads remotas nem chamadas a funções externas, muitas vezes é muito difícil detectar modificações de memória, e mais difícil ainda atribuí-las a um processo específico.

Um processo que teve sua memória modificada pode ser forçado a realizar atividades maliciosas que, de outra forma, não realizaria. Nenhum processo com memória executável adulterada deve

ser considerado confiável, pois isso não é uma ocorrência normal em comunicações ou interações entre processos.

O que a Cyber Crucible faz?

A Cyber Crucible monitora o estado da memória de um processo ao longo de todo o seu ciclo de vida. Se a memória for considerada adulterada, o processo é sinalizado e considerado não confiável. No momento em que ocorre um evento de extorsão, a memória é capturada em snapshot para ser fornecida durante possíveis investigações de resposta a incidentes.

O snapshot de memória contém a memória executável original, não adulterada, e quaisquer "diffs", com seus deslocamentos (offsets) dentro da memória do processo. A análise desses dumps de memória pode ser desafiadora, mas pode fornecer evidências sólidas sobre os comportamentos do código malicioso.

Como identificar?

Cyber Crucible Indicates Responses with Modified Memory

A Cyber Crucible Indica Respostas com Memória Modificada

A memória modificada é mais difícil e mais efêmera de rastrear do que outros métodos de injeção de processo. Em vez disso, fornecemos um valor booleano rápido para indicar que a modificação ocorreu, e, a partir daí, a análise dos diffs reais de memória requer uma investigação mais aprofundada.

Some raw memory

Memória bruta

Disassembled memory

Memória desmontada

Coletar a memória é apenas o primeiro passo; mesmo após a desmontagem, o código pode estar muito ofuscado e ser difícil de ler. A boa notícia é que temos muito com que trabalhar nessa análise quando dispomos da memória original, dos metadados associados, do executável original e das próprias instruções do executável modificado.

1. sim, 2.

Cenários de exemplo:

- [Cenário de Treinamento - Modificação de Memória](#)

Revision #1

Created 2026-07-24 05:10:06 UTC by Dennis Underwood

Updated 2026-07-24 05:10:06 UTC by Dennis Underwood