

O Que Acontece Quando a CC Detecta Ataques de Memória

Primeiramente, é muito importante observar que as alterações de memória ocorrem por vários motivos diferentes:

1. Ataques na memória (in-memory attacks)
2. Interação entre programas
3. Falhas de software (bugs)
4. Exploits

Portanto, uma injeção de processo ou técnica de alteração de memória utilizada, mesmo entre programas, não é necessariamente uma ação maliciosa.

Se um programa que sofreu um evento de memória provavelmente malicioso (ou seja, #1 ou #4 acima) estiver envolvido em uma resposta automatizada por parte da Cyber Crucible, ocorre uma atividade de coleta automatizada.

A parte da memória que foi alterada em um programa, bem como o estado "anterior", é salva em um formato estruturado da Cyber Crucible chamado .ccdif

Essa parte injetada ou alterada da memória é salva e fica disponível para download no portal web da Cyber Crucible.

Por Que Isso Não É Automaticamente Enviado ao Virustotal (etc.) para Análise?

Em algumas circunstâncias, o código malicioso utilizado em um ataque contém variáveis que são exclusivas de um ataque, especificamente relacionadas a uma vítima.

Enviar esse código malicioso a um mecanismo de análise público, como o Virustotal, representaria uma divulgação indesejada de informações que identificam a vítima à comunidade de segurança.

Por Que Seria Útil Enviar Esses Dados Binários ao Virustotal (etc.)?

Ferramentas de antivírus e EDR baseadas em assinaturas procuram por strings ou bytes de código observados em ataques anteriores. Mesmo que esse malware nunca tenha sido visto antes, com o tempo ele pode passar a ser conhecido pela comunidade de segurança. Essas ferramentas de varredura geralmente não precisam que o código esteja em um binário devidamente formatado para sinalizar uma associação com um malware conhecido.

Revision #1

Created 2026-07-24 05:46:43 UTC by Dennis Underwood

Updated 2026-07-24 05:46:43 UTC by Dennis Underwood