

A Cyber Crucible consegue impedir o movimento lateral de atacantes?

O mecanismo comportamental do produto e as metodologias de Zero Trust reúnem, de forma eficaz, evidências de movimento lateral.

Isso pode ser evidência de movimento lateral de processo para processo na própria máquina, ou pode ser a descoberta do ponto de entrada de um atacante no sistema a partir de um sistema remoto, durante a realização de uma Análise de Causa Raiz.

Programas e seus argumentos associados a métodos de injeção de processo e a processos “living off the land” que abrem outros processos são capturados e enviados à Cyber Crucible.

Devido à análise comportamental de processos em nível de kernel, não há processos com privilégios excessivos para observação e relato pela Cyber Crucible (incluindo outros drivers de kernel, ou até mesmo outras ferramentas de segurança de endpoint).

Respostas automatizadas de contra-extorsão ocorrem quando ações de extorsão de dados ou de criptografia de ransomware são iniciadas.

Por exemplo, aqui está um vídeo demonstrando o movimento lateral em uma máquina, utilizando técnicas em memória, e a exploração do Log4j. Observe que a suspensão automatizada do(s) processo(s) afetado(s) ocorreu após o início dos comportamentos de roubo de dados e de ransomware.

[rr-log4j-procinj-3mins.mp4](#)

Outro exemplo dessa dinâmica demonstra o uso, por um atacante, para abrir um shell do Windows. A observação capturou todas as evidências, mas a atividade foi suspensa assim que o shell do Windows começou a tentar atividades de extorsão de dados (neste caso, roubo de dados)

[rr-com-dll.mp4](#)

Por fim, a migração a partir de um navegador explorado também é observada, e, neste caso, o atacante nunca conseguiu se mover com sucesso a partir do navegador Chrome explorado, devido ao monitoramento do estado de memória do navegador:

[rr-untrusted-chrome.mp4](#)

Revision #1

Created 2026-07-24 05:37:47 UTC by Dennis Underwood

Updated 2026-07-24 05:37:47 UTC by Dennis Underwood