

A Cyber Crucible coleta chaves de criptografia?

A resposta mais curta é: “Não.”

Houve uma época em que o software da Cyber Crucible não impedia a criptografia de ransomware antes da criptografia. Em vez disso, coletava possíveis chaves de criptografia ou configurações e, em seguida, utilizava uma variedade de técnicas para descobrir o pacote de descriptografia adequado (incluindo as chaves) para descriptografar após um ataque de ransomware.

Do ponto de vista do que coletávamos, uma boa analogia seria uma câmera de vídeo que tirasse fotos de tudo o que pudesse ser uma chave para um cofre. Em seguida, um servidor faria os diversos cálculos para determinar a chave e as configurações corretas para o arquivo adequado. Cientistas da computação chamariam isso de aprendizado de máquina.

Antes de deixarmos para trás o antigo modelo de software “coletar tudo o que possa ser uma chave”, estávamos organizando automaticamente milhares de chaves e configurações de criptografia por máquina durante os ataques.

O módulo de software de análise criptográfica evoluiu agora para um módulo analítico comportamental adicional, que é utilizado como uma das fontes de dados para determinar se um software está tentando acessar indevidamente dados de identidade ou “dados de dados” para roubá-los ou criptografá-los.

Revision #1

Created 2026-07-24 05:49:30 UTC by Dennis Underwood

Updated 2026-07-24 05:49:30 UTC by Dennis Underwood