Por que capturar chaves de criptografia de ransomware deixou de ser uma defesa válida?

Resposta curta: A captura de chaves deixou de ser tecnicamente confiável em 2021. O ransomware moderno evita as bibliotecas de criptografia padrão do sistema operacional, portanto não há chaves para uma ferramenta defensiva interceptar — e mesmo quando as chaves são obtidas, muitas vezes não podem ser aplicadas.

Como o ransomware moderno contorna a captura de chaves

- **Bibliotecas personalizadas:** o código de criptografia é compilado diretamente no malware em vez de chamar bibliotecas do sistema operacional, de modo que as chaves são geradas e usadas inteiramente dentro do processo do próprio invasor — invisíveis para ferramentas que monitoram chamadas padrão.
- **Implementações exclusivas:** algumas variantes usam criptografia não padronizada, específica para cada execução. Mesmo uma chave capturada não pode ser aplicada, porque o próprio algoritmo é personalizado.
- **Cifras de fluxo (streaming ciphers):** construídas sobre um conceito fundamentalmente diferente do AES, são simplesmente imunes à captura de chaves AES.

A Cyber Crucible originalmente desenvolveu e patenteou a tecnologia de captura de chaves e, em seguida, apresentou a criptanálise que demonstrava seus limites na BSides Pittsburgh em 2021. Avançamos porque as evidências assim indicavam.

O problema de conformidade também

A captura de chaves exige o armazenamento centralizado das chaves de criptografia — criando um ponto único de falha e um alvo de alto valor. Um governo também poderia forçar o acesso por meio de uma intimação classificada ou de uma carta de segurança nacional, sem o seu conhecimento. Esse é um risco sério de soberania de dados, somado a uma defesa que já não funciona.

Revision #1
Created 2026-07-24 05:44:59 UTC by Dennis Underwood
Updated 2026-07-24 05:44:59 UTC by Dennis Underwood