Por que o antivírus tradicional não consegue impedir ataques de ransomware zero-day e sem arquivo (fileless)?

Resposta curta: As ferramentas de segurança baseadas em assinaturas dependem do reconhecimento de padrões de ataque conhecidos, mas os atacantes modernos testam deliberadamente suas ferramentas contra essas mesmas defesas antes de implantá-las e, cada vez mais, evitam completamente a criação de arquivos detectáveis. Essa combinação de ameaças mutantes e não reconhecidas com técnicas que operam apenas na memória tornou os métodos tradicionais de detecção muito menos confiáveis.

O Problema de Depender de Assinaturas Conhecidas

Os ataques zero-day são, por definição, novos ou alterados o suficiente para ficarem fora do que as ferramentas de segurança existentes já reconhecem. Os fornecedores há muito prometem melhorias na detecção dessas ameaças, mas os atacantes têm uma vantagem inerente: eles têm acesso aos mesmos produtos comerciais de segurança que os defensores utilizam. Antes de lançar uma campanha, os atacantes costumam testar seu malware contra ferramentas de detecção populares, refinando-o até que consiga passar despercebido. Isso transforma a detecção em um alvo em constante movimento, em vez de uma defesa fixa.

Técnicas Sem Arquivo (Fileless) Comprometem o Whitelisting

Os atacantes também deixaram de inserir executáveis maliciosos óbvios em um sistema. Em vez disso, eles sequestram aplicativos legítimos e confiáveis, já aprovados por ferramentas de whitelisting de aplicativos, executando atividades maliciosas por meio de processos que o software de segurança presume serem seguros. Quando essa abordagem sem arquivo é combinada com código que muta rapidamente, os ataques podem ser concluídos em uma janela de tempo muito

curta — às vezes dentro de meia hora — muito antes que uma equipe humana de resposta a incidentes possa realisticamente investigar.

Os Atacantes Apagam Seus Próprios Rastros

Em muitos casos, como o ataque ocorre na memória em vez de no disco, os atacantes eliminam registros, evidências e até sensores de segurança antes de finalizar sua operação. Isso é semelhante a um assaltante desativar câmeras de segurança e alarmes antes de cometer um crime: quando alguém procura por evidências, a visibilidade mais útil já foi destruída. Essa combinação de métodos de ataque imprevisíveis com evidências que se autoapagam é o motivo pelo qual a Cyber Crucible investiu esforços significativos na construção de uma abordagem automatizada e escalável — projetada para capturar os dados críticos necessários para tomar decisões precisas antes que os atacantes possam apagar os rastros, em vez de depender do reconhecimento de ameaças após o fato.

https://player.vimeo.com/video/1164197533?texttrack=pt

Assistir no Vimeo · Legendas: English, Français, Español, العربية

Revision #2
Created 2026-07-24 06:15:37 UTC by Dennis Underwood
Updated 2026-08-06 18:38:18 UTC by Dennis Underwood