Como a Análise Comportamental de Memória da CC difere da varredura de memória?

O Que É a Varredura de Memória?

A varredura de memória é a prática de pegar um bloco de memória, normalmente copiando-o para um local diferente no sistema para análise, e realizar a varredura para análise.

Fotografia vs Ação ao Vivo

Isso não é uma varredura ao vivo do programa enquanto ele se comporta, mas sim uma imagem instantânea do programa em um determinado momento. Pense nisso como uma fotografia, em comparação a uma transmissão ao vivo. O estado do programa pode ser drasticamente diferente de um momento para o outro, portanto, é mais útil como um exercício forense em um ambiente controlado. É menos útil em um ambiente não controlado, como o ambiente de um cliente. Quanto mais ocupada a máquina, ou quanto mais um programa estiver fazendo, mais difícil é obter uma imagem precisa do estado atual de um programa.

A Cyber Crucible começou com um uso intenso de varredura de memória, tentando tirar muitas "fotos" dos estados de memória dos programas. À medida que nos tornamos mais rápidos, encontramos múltiplos gargalos na velocidade com que os snapshots de memória podiam ser feitos, e em múltiplos programas.

Preocupações com o consumo de recursos de CPU ou GPU

Essa varredura de memória pode consumir muitos recursos e pode levar algum tempo para programas grandes. Quando a Cyber Crucible utilizava a varredura de memória, em vez do monitoramento inteligente do comportamento da memória, um núcleo inteiro da CPU era dedicado à varredura.

A Intel possui uma tecnologia inovadora chamada Intel TDT AMS, disponível em arquiteturas específicas baseadas em Intel com uma GPU Intel integrada.

Ela realiza a varredura da memória de um programa quando ele é iniciado pela primeira vez, utilizando a GPU para ajudar a não sobrecarregar a CPU. Além disso, a GPU tem melhor desempenho para o tipo de varredura realizada (mais sobre isso depois).

Metodologia de Varredura

A varredura de memória é realizada para procurar códigos ou "strings" específicos. Estes são frequentemente os mesmos elementos de dados que ferramentas de antivírus/EDR procuram em arquivos potencialmente maliciosos.

A varredura de memória, especificamente, é mais limitada do que algumas das buscas complexas que podem ser realizadas em um arquivo.

Portanto, a varredura, por padrão, procura por itens já conhecidos, como malwares mais antigos, mas é limitada em sua capacidade de fazê-lo.

A Cyber Crucible costumava varrer segmentos de memória em busca de material criptográfico, mas isso se mostrou muito limitado para ambientes modernos, e inventamos um método diferente para observar comportamentos, utilizando lógica baseada em kernel.

Metodologias Baseadas em Comportamento vs Varredura

A Cyber Crucible migrou de uma metodologia baseada em varredura para uma baseada em comportamento por alguns motivos.

Desvantagens da Varredura

A primeira é que uma imagem ao vivo precisava ser utilizada em todos os programas. Os snapshots eram realmente difíceis de completar mesmo para uma análise limitada, antes que

outro fosse necessário. Muita atividade dos programas estava sendo perdida, quase como ter uma câmera de vídeo operando a uma taxa de quadros muito baixa. Isso era agravado pela necessidade de monitorar todos os programas simultaneamente. Servidores ou estações de trabalho ocupadas, sem dúvida os computadores que mais precisavam de monitoramento e que eram mais importantes, acabavam com o menor percentual de vigilância realizada. Independentemente da empresa ou produto, as limitações tecnológicas eram evidentes e inviáveis.

A segunda é que, além do consumo de recursos, a varredura exige, por padrão, procurar por **algo conhecido**. Assim, a varredura de memória precisa ser baseada em assinaturas. Além disso, a varredura por assinatura deve ser um subconjunto limitado da varredura por assinatura mais completa encontrada na varredura de antivírus baseada em arquivos. Os atacantes já vêm evadindo as defesas baseadas em assinaturas de arquivos há anos; há muito pouca chance de os atacantes serem descobertos por um sistema baseado em assinaturas ainda menos capaz.

Vantagens da Análise Comportamental

O monitoramento de memória baseado em comportamento da Cyber Crucible não requer assinaturas e utiliza o acesso à memória do kernel para rastrear os comportamentos de todos os programas simultaneamente. Vamos detalhar isso.

Primeiro, o monitoramento comportamental significa que novos malwares, ou malwares que foram editados por atacantes para parecerem novos, podem ser facilmente descobertos em tempo real. A varredura baseada em assinaturas, seja de memória ou de arquivos, depende de já ter visto aquele malware específico anteriormente. Os atacantes vêm evadindo as defesas baseadas em assinaturas há anos, apesar de um conjunto completo de técnicas de varredura contra arquivos. As técnicas de varredura disponíveis contra a memória são um subconjunto disso, e são ainda menos eficazes.

Segundo, o novo monitoramento comportamental de memória da Cyber Crucible é capaz de permanecer em tempo real em todos os programas simultaneamente, durante toda a execução dos programas. A varredura de memória sofre de graves gargalos de recursos que só pioram à medida que mais programas são executados. Os atacantes normalmente executam dezenas de amostras de malware ao mesmo tempo, sobrecarregando a análise de varredura de memória devido à velocidade e ao número de programas a serem examinados simultaneamente, independentemente de ser um malware de dia zero ou antigo.

Revision #1
Created 2026-07-24 05:46:33 UTC by Dennis Underwood
Updated 2026-07-24 05:46:33 UTC by Dennis Underwood