Como posso investigar a causa raiz de um evento?

Existem três blocos de construção de análise disponíveis para você durante a investigação de um alerta.

Atualmente, é mais provável que um invasor conduza uma variedade de atividades em um sistema, usando uma combinação de técnicas na memória e sequestro de processos (injeção ou hollowing), do que executando um programa óbvio de “hacker.exe”.

Análise de Memória

O primeiro bloco de construção é encontrado na própria página de Resposta ou Incidente. A análise de memória acompanha os comportamentos do processo na memória durante a inspeção contínua de possíveis comportamentos de extorsão de dados (roubo ou criptografia).

Um estado de memória que indica provável adulteração é tipicamente indicativo de um problema.

Isso nem sempre é malicioso em si, pois práticas de programação inadequadas ou bugs de software também podem resultar na adulteração do estado de memória de um programa em execução.

63504385.png?width=680
Aqui vemos uma instância em que um processo do Adobe Acrobat exibe possíveis comportamentos de extorsão de dados após abrir um PDF baixado, e vemos que a memória do processo do Acrobat havia sido modificada. O processo Acrobat.exe no disco não foi afetado de forma alguma.

A análise forense da memória envolvida com o Acrobat.exe suspenso provavelmente indicará um problema de preocupação - possivelmente um exploit em uso, senão injeção de processo ou

hollowing de processo.

Para respostas de extorsão com um valor de Memória Modificada igual a Verdadeiro, há um ícone de download na coluna Análise de Causa Raiz para baixar o arquivo de Diferença de Memória (Memory Diff) da resposta:

63602693.png?width=680
O Arquivo de Diferença de Memória (Memory Diff File) é o código-fonte compilado do que foi injetado no programa. Provavelmente contém malware e/ou código de exploit, para que um analista de malware ou de segurança examine. Observe que este arquivo não contém o programa inteiro, apenas a parte que foi alterada por meio de um exploit ou técnica de ataque como injeção de processo. Saiba mais sobre este arquivo aqui.

Análise de Injeção de Processos

O primeiro indicador de que pode haver um evento de injeção de processo relevante para uma resposta automatizada é a coluna Threads Remotas Não Confiáveis para um Incidente/Resposta. Isso indica que a análise comportamental em nível de kernel revelou uma thread remota não confiável sendo observada com o processo conduzindo roubo de dados ou comportamento semelhante a ransomware.

63471635.png?width=680
Uma investigação mais aprofundada pode ser realizada na página de Injeção de Processos. O valor Verdadeiro em Threads Remotas Não Confiáveis é um bom indicador de que deve-se acessar essa página.

A coluna Análise de Causa Raiz também possui um ícone para redirecioná-lo automaticamente para a página de Injeções, mostrando apenas as injeções de processo relacionadas à resposta

63602703.png?width=680
Após clicar no ícone de injeções, você será direcionado para a página de Injeções de Processos, onde verá apenas as injeções de processo relacionadas à resposta:

63569930.png?width=680
Aqui, na página de Eventos de Injeção de Processos, vemos o caminho e os argumentos do processo injetor, e o caminho e os argumentos do processo injetado. Geralmente, os argumentos desempenham um papel muito importante na análise de memória ou indicam, por exemplo, quais comandos do PowerShell devem ser executados. Os IDs de processo também estão presentes, para ajudar a rastrear injeções iterativas realizadas à medida que um invasor pula de processo em processo, ou para consultar a análise de causa raiz na página de Criação de Processos.

63438879.png?width=680
Como sabíamos que o rundll32.exe era, na verdade, um fornecedor de antivírus? Continue lendo!

Análise de Criação de Processos

É muito raro que um invasor use apenas um processo durante seu ataque. Ele pode nem saber que as ferramentas que está usando estão gerando novos processos e utilizando diversas ferramentas administrativas no sistema infectado.

A página de Criação de Processos rastreia todos os processos que abrem outros processos (ou a si mesmos), os argumentos usados e os IDs de processo, ou Pids, para cada origem e destino.

Isso é realizado no nível do kernel, o que significa que nada é perdido.

Observação: a telemetria da Microsoft possui parte desses dados, mas não todos. Optamos por não usar essa fonte de dados, pois observamos que ela deixa de registrar eventos importantes ou é desativada por invasores durante um ataque.

O quão boa é nossa visibilidade?

Juntando tudo - uma investigação completa

O quão boa é nossa visibilidade, e quão rápido você pode realizar uma Análise de Causa Raiz? Confira este exemplo - um antivírus, com algumas das permissões mais altas em um sistema, foi observado tentando injetar código em nosso software Cyber Crucible. Esperamos que fosse para investigar nosso software, mas ainda assim entramos em modo de autoproteção (ou seja, isso fez com que nosso software rejeitasse a adulteração do antivírus... não há portas dos fundos que permitam acesso para edição ou uso de nosso software por terceiros externos).

Então, vamos começar aqui, com uma resposta automatizada:

63569937.png?width=680
Obviamente, o Cyber Crucible não é ransomware. Vemos aqui uma tentativa de injeção de processo envolvendo comportamento suspeito de thread remota, em conjunto com comportamentos semelhantes à extorsão de dados.

OK - vamos ver o que está acontecendo em Eventos de Injeção de Processos clicando no ícone de injeções. 5 segundos depois - já temos nossa resposta!

63471644.png?width=56463438879.png?width=680

Mas espere - rundll? Isso não é um hacker, é? Certamente, não é um programa hacker.exe. Vamos fazer alguma filtragem, para obter nossa resposta na página de Criação de Processos. Não temos uma captura de tela aqui, mas os IDs de processo estão disponíveis para todas as respostas e injeções de processo. Vamos voltar à página de respostas e clicar no ícone de criações de processo para nos levar à página de Criações de Processos e filtrar automaticamente a grade para mostrar as criações de processo relacionadas a esta resposta.

63537184.png63438886.png?width=680

Rápido e fácil, agora vemos que a “raiz” (sem trocadilhos) foi o WebRoot, um fornecedor de antivírus, que gerou um processo rundll32.exe para carregar uma das DLLs do WebRoot, que então tentou fazer *algo* com o software do Cyber Crucible, para forçá-lo a percorrer arquivos como uma ferramenta de roubo de dados.

Por que escolhemos mostrar este exemplo?

Temos inúmeros exemplos de técnicas de invasores, com níveis variados de competência por parte deles. Os antivírus alcançam um nível de permissões em um sistema que exige um nível muito alto de habilidade, tecnologia e preparação por parte dos invasores. O Cyber Crucible detectar comportamentos “semelhantes a hackers” de uma ferramenta de segurança convencional e, em seguida, interrompê-los automaticamente, demonstra alguns dos mais altos níveis de excelência em engenharia e segurança de nossa parte, sem se perder em exploits individuais ou técnicas específicas de invasores.

Revision #1
Created 2026-07-24 05:32:07 UTC by Dennis Underwood
Updated 2026-07-24 05:32:07 UTC by Dennis Underwood