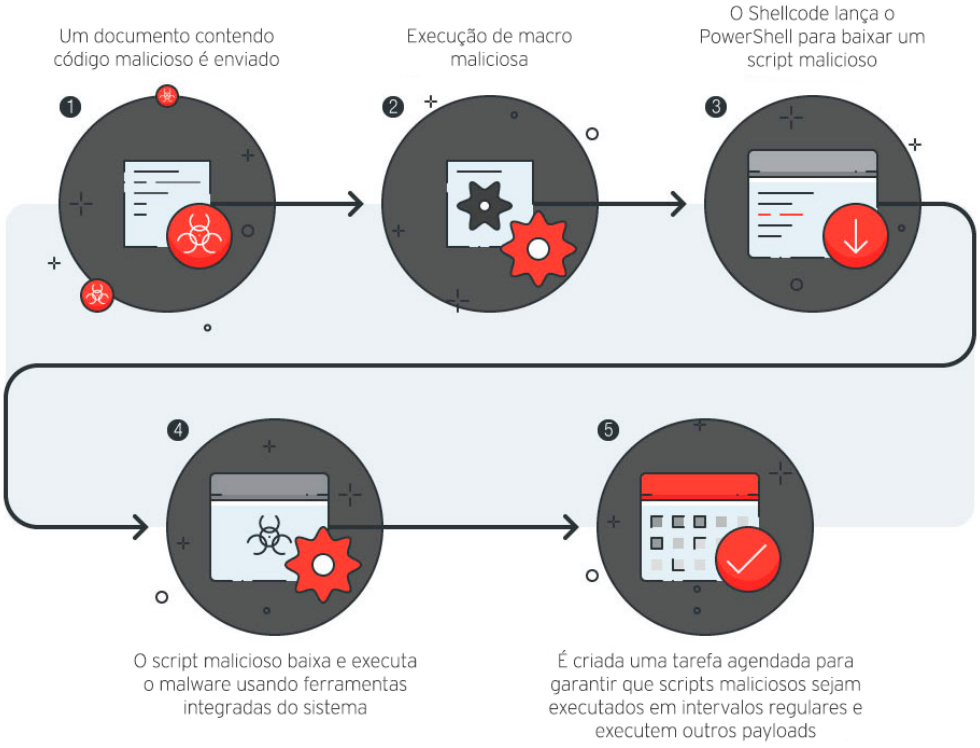
Riscos sob o radar

Entendendo as ameaças fileless

O que são ataques fileless?

Um ataque fileless é um tipo de atividade maliciosa em que um hacker tira proveito de aplicações já instaladas em uma máquina. Diferentemente de outros ataques em que o software malicioso é instalado em um dispositivo sem que o usuário saiba, os ataques fileless usam aplicações confiáveis, software existente e protocolos autorizados. Essencialmente, eles não precisam de malware para executar um ataque.



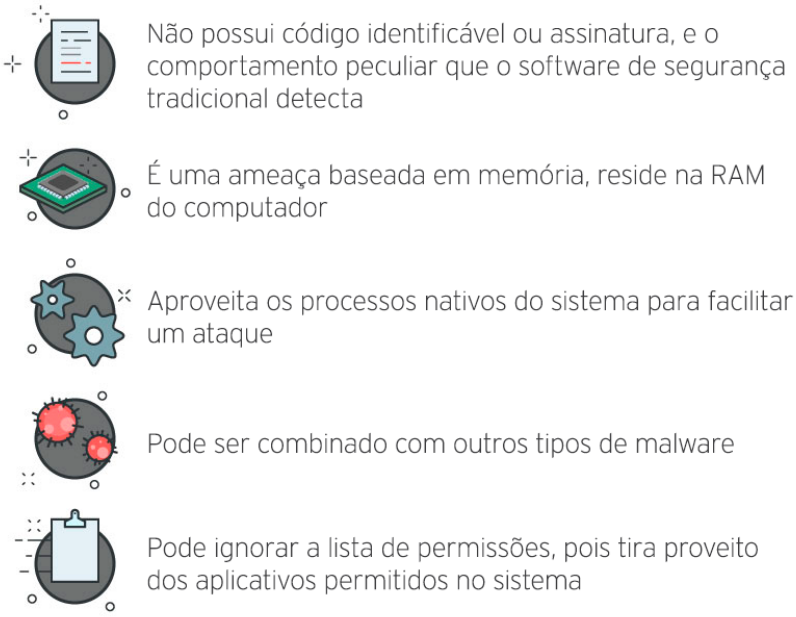
Uma cadeia de infecção típica de uma ameaça fileless que é lançada através da exploração de documentos, instala payloads e mantém persistência.

Um ataque pode ser iniciado por uma ação de um usuário, como clicar em um documento anexado incorporado com código contaminado, que depois usa outras aplicações instaladas na máquina. Estes ataques ocorrem na memória de acesso aleatório (RAM) de uma máquina e geralmente utilizam ferramentas nativas do Windows, como o PowerShell e o Windows Management Instrumentation (WMI), para executar comandos maliciosos. Essas aplicações conhecidas realizam tarefas do sistema em endpoints, o que os torna ideais para facilitar os ataques. As ameaças fileless também podem ser associadas a outros vetores de ataque, como o ransomware.

Uma vez que estas ameaças não carecem do download de arquivos maliciosos, a detecção e a prevenção delas podem ser desafiadoras. Entretanto, como a memória RAM mantém seus dados apenas quando a máquina está ligada, a infecção não deve mais estar ativa quando o computador for reiniciado. Contudo, isso não significa que os hackers não possam tirar proveito de outras fraquezas do computador ou mesmo executar outras técnicas para ter persistência. Por exemplo, um hacker pode continuar um ataque configurando scripts que são executados quando o sistema é reiniciado.

Os Fundamentos das Ameaças Fileless:

Características de um Ataque Fileless



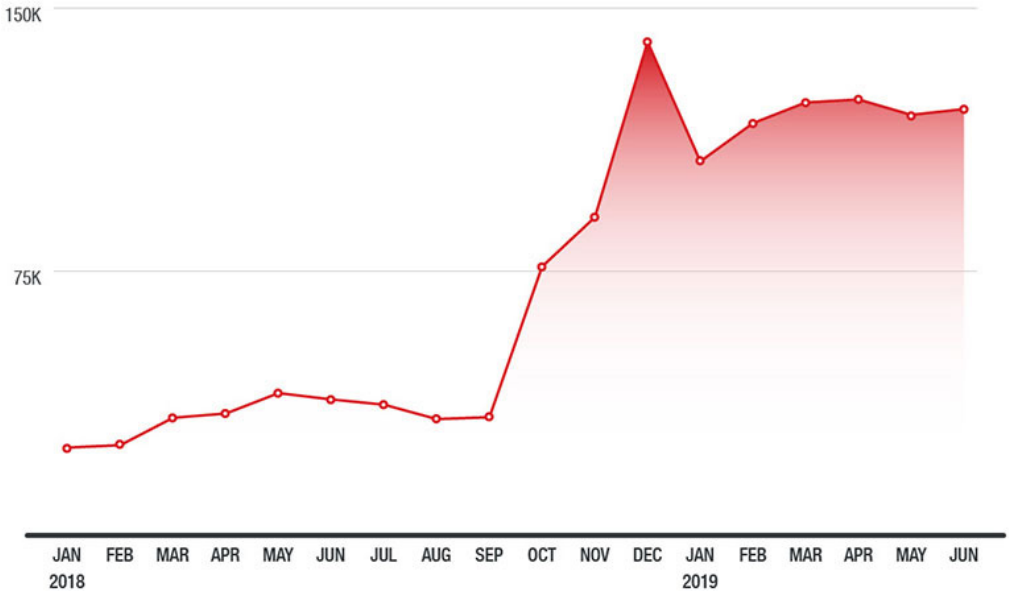
Como as ameaças fileless entram nos sistemas e como são detectadas?

Os ataques de malware geralmente envolvem arquivos maliciosos gravados em disco ou requerem interação para realizar suas intenções maliciosas. Essas características deixariam vestígios, de uma forma ou de outra, para uma análise pós-infecção. Como as ameaças fileless devem residir na memória, na maioria das vezes, elas não deixam pegadas após a execução. O payload malicioso ocorre na RAM, o que significa que nada é gravado no disco. Isso torna os ataques baseados em memória mais problemáticos e difíceis de detectar do que os malwares baseados em arquivos. No entanto, atividades deste tipo podem ser detectadas rastreando indicadores que não são baseados em arquivos, como eventos ou comportamentos específicos de execução.

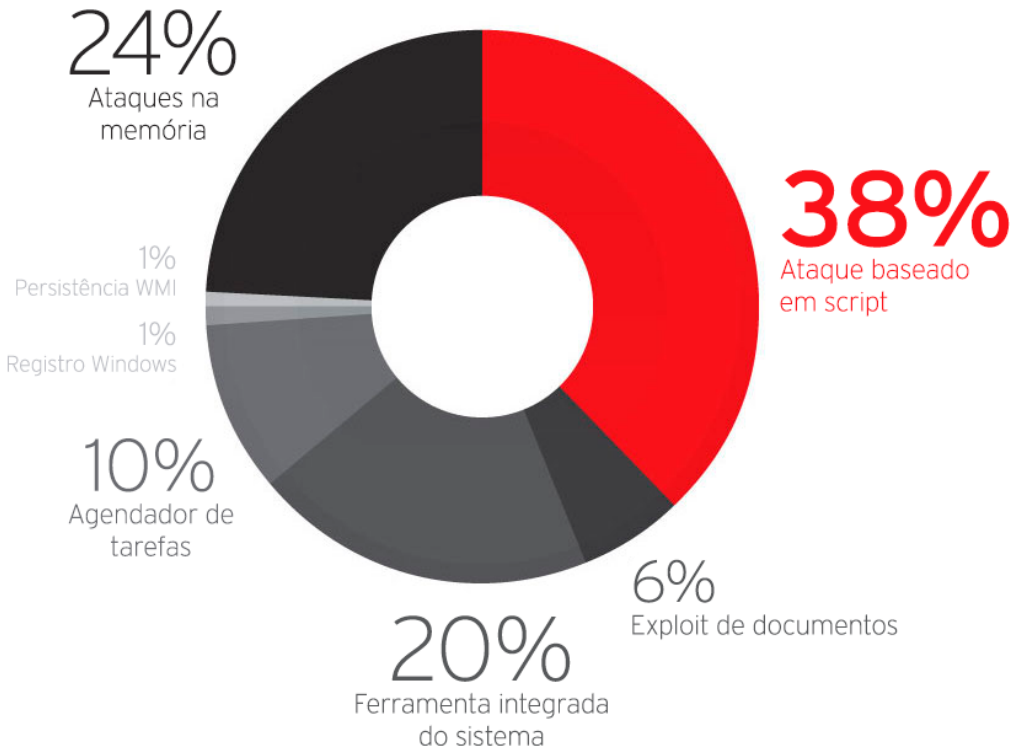
↑396%

em ameaças fileless
Jan de 2018 - Jun de 2019

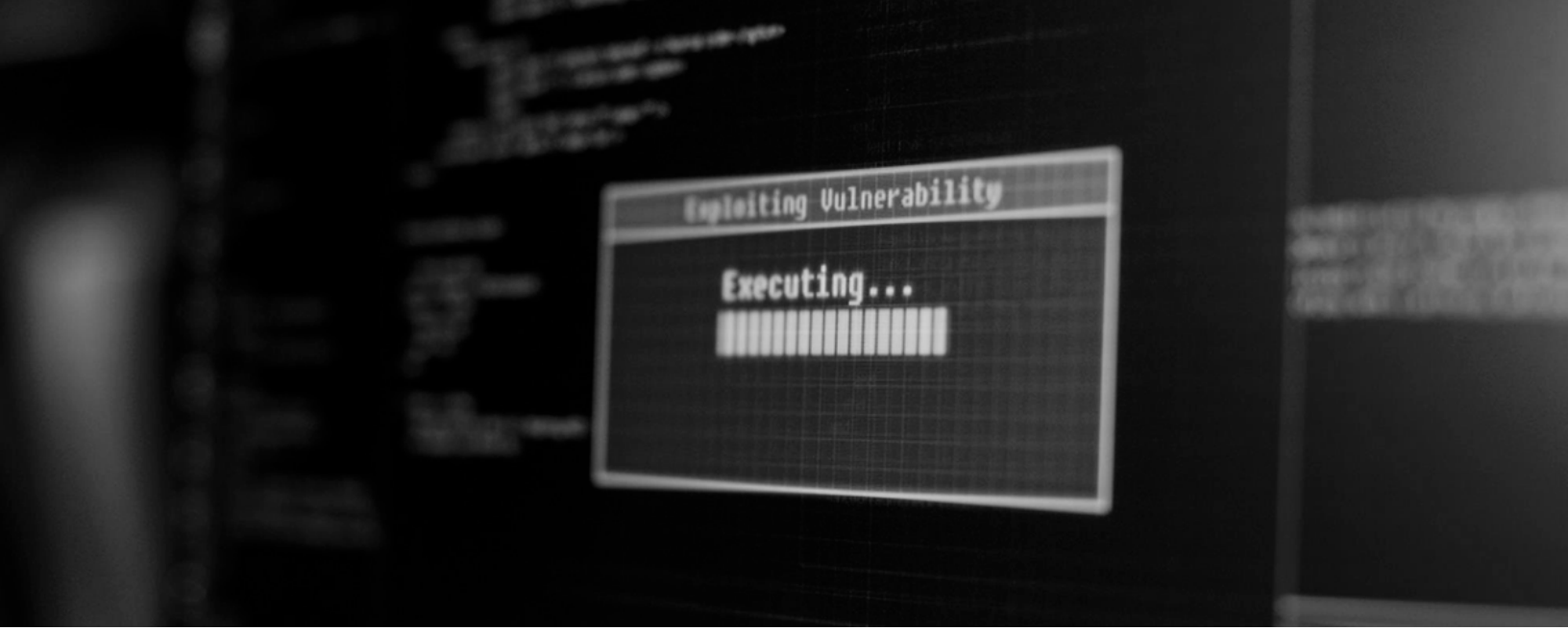
Estes ataques prosperam com discrição e sutileza, e os números mês a mês mostram que a ameaça é atraente para os criminosos. O rastreamento de detecções de ameaças fileless de 2018 até o primeiro semestre de 2019 mostra um aumento notável. O crescimento pode ser atribuído ao uso contínuo de diferentes técnicas fileless para evitar a detecção e as soluções convencionais da lista negra.



Comparação mensal de eventos fileless bloqueados, com base em dados da infraestrutura Trend Micro™ Smart Protection Network™ (janeiro de 2018 a junho de 2019)



Porcentagem de eventos fileless detectados (janeiro a junho de 2019)



Veja como as ameaças fileless funcionam e por quais técnicas se deve procurar:

Iniciando ataques por meio de exploits de documentos ou na memória

Um ataque fileless pode começar "tradicionalmente" por meio de código de macro malicioso (por exemplo, JavaScript ou VBScript) incorporado em arquivos, outros arquivos aparentemente normais e aplicações aprovadas, como documentos do Office (por exemplo, Microsoft Word e Excel) e PDFs. Atacantes tiram vantagem disso, permitindo que eles executem código com os mesmos privilégios que a aplicação em execução. As macros podem executar scripts e abusar de ferramentas legítimas como o PowerShell para iniciar, baixar ou executar códigos, scripts e payloads. Esses scripts também podem ter suas informações ofuscadas, o que torna a detecção de palavras-chave que acionam a execução um desafio para as organizações. Um ataque desta natureza também pode chegar aos sistemas por uma mensagem de spam ou phishing que induz o destinatário a clicar em um link malicioso, o que inicia o processo de infecção.

As ameaças fileless também podem empregar maneiras diferentes de executar a partir da memória. Um exemplo recente disso é o EternalBlue de exploração em memória, que tira proveito de uma vulnerabilidade no protocolo SMB 1 (Server Message Block 1). Um ataque também pode tirar proveito de processos legítimos por meio da injeção de DLL, o que força o carregamento de uma DLL (dynamic-link library) em um processo host, eliminando a necessidade de gravar a DLL no disco. Uma técnica como o process hollowing, que substitui algum código por uma função maliciosa, também pode ser empregada. Isso envolve a execução de código diretamente na memória e pode ser mantida em execução em segundo plano, mesmo após o fechamento do software.

Instalando malware via ferramentas ou scripts integrados ao sistema

Invasores podem abusar das ferramentas e utilitários de administração do sistema por infecções fileless. Em vez de se utilizar executáveis, os atacantes podem usar indevidamente as ferramentas que já estão no sistema de destino para conduzir seus ataques. Algumas dessas ferramentas são interfaces de linha de comando, como o **BITSAdmin** (Serviço de Transferência de Inteligência em Segundo Plano), usado para criar e baixar tarefas e monitorar o progresso; **CertUtil**, usado para serviços/gerenciamento de certificados; e **msiexec**, usado para instalar, modificar e executar aplicativos do Windows Installer.

Os ataques baseados em script são a ameaça mais comum deste tipo, com base em nossos dados (38% no primeiro semestre de 2019). Muitos ataques baseados em script usam scripts interpretados, pois são executados diretamente na linha de comando (via PowerShell, JavaScript, VBScript, WScript, mshta etc.) e podem levar à execução arbitrária de código. O PowerShell, por exemplo, consegue executar um comando oculto no sistema que pode ser definido dependendo do tempo planejado para o ataque. Desde então, muitos tipos de malware foram entregues sem download de arquivo malicioso através da execução de código na memória para ignorar a segurança baseada no endpoint.

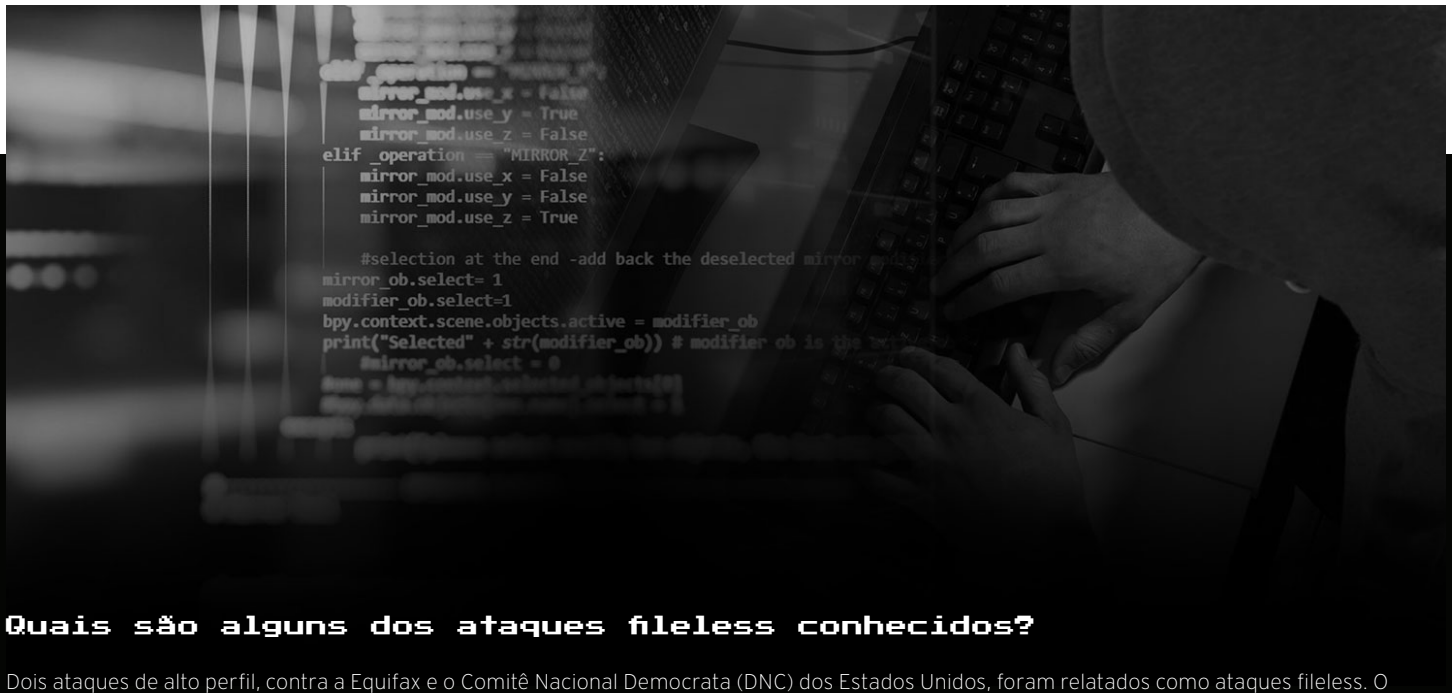
Muitas ameaças fileless abusam do PowerShell, em particular, uma vez que ele é um recurso interno de muitos sistemas operacionais Windows. A estrutura da Microsoft também é capaz de acessar APIs (interfaces de programação de aplicativos) que executam funções cruciais do sistema e de aplicativos. Também é atraente para os invasores porque não tem executável no disco, permitindo que eles entreguem payloads e comandos maliciosos executivos fileless. Os administradores de TI podem detectar melhor o uso indevido do PowerShell por meio da detecção comportamental, ou seja, discernir uma sessão do PowerShell executada através de uma ordem codificada na linha de comando.

Manutenção da persistência via Agendador de tarefas, Registro ou WMI

Frequentemente, violações causadas por ameaças fileless podem ser interrompidas assim que o usuário reiniciar o computador, já que o código malicioso reside apenas na memória. No entanto, agentes mal-intencionados já usam técnicas para garantir que estas infecções não confiem nos endpoints para sustentar um ataque. Os hackers têm a capacidade de fazer alterações sutis no registro do sistema plantando entradas e configurando scripts para serem executados mesmo após a reinicialização do sistema. O que torna isso particularmente digno de nota é que, por ter os próprios comandos de um sistema executando um ataque, isso pode não ser identificado em alguns esforços de monitoramento. Por um lado, o Registro do Windows também pode ser comprometido armazenando códigos maliciosos no registro com recursos de execução automática, para que os ataques sejam atualizados em segundo plano, mesmo após a reinicialização do computador. Um exemplo é a versão fileless do KOVTER, um malware em evolução, que foi visto anteriormente criando entradas de registro que carregam códigos maliciosos na memória sempre que uma máquina infectada era reiniciada ou arquivos em lote eram acionados.

O Agendador de tarefas, usado para permitir que programas com script sejam iniciados em um horário pré-determinado, também pode ser abusado para manter a persistência. Para ameaças assim, isso significa que as tarefas podem ser agendadas para execução. Os invasores podem até definir as tarefas para que se repitam e criar entradas de registro para re-infectar automaticamente os sistemas.

Códigos interpretados, como os do PowerShell ou um componente do Windows, como o Windows Management Instrumentation (WMI), geralmente usados pelas redes corporativas para automação de tarefas de administração do sistema, podem ser explorados para permitir a execução de scripts maliciosos, o que conseguiria afetar o endpoint sem gravação no disco. Os atacantes abusam disso para execução de código, movimento lateral e persistência. Eles podem usar repositórios WMI para armazenar scripts mal-intencionados periodicamente, usando ligações WMI. Notavelmente, iterações de malware de mineração de criptomoeda também foram vistas abusando do WMI por persistência.



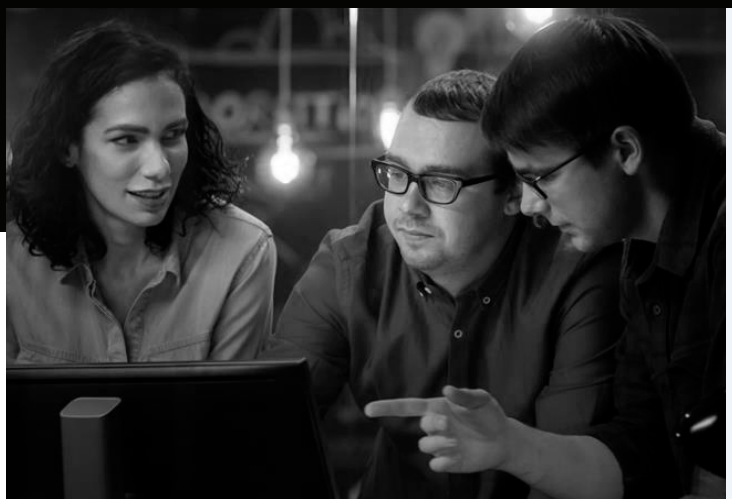
Quais são alguns dos ataques fileless conhecidos?

Dois ataques de alto perfil, contra a Equifax e o Comitê Nacional Democrata (DNC) dos Estados Unidos, foram relatados como ataques fileless. O último hack usou uma vulnerabilidade de injeção de comando na aplicação Apache Struts, enquanto o primeiro aproveitou o PowerShell e o WMI para ganhar uma posição nos sistemas.

Em 2017, um ataque fileless infectou instituições financeiras, empresas de telecomunicações e organizações governamentais em 40 países. A equipe de segurança de um banco descobriu o ataque através da cópia do Meterpreter, um componente em memória do Metasploit, na memória física de um controlador de domínio da Microsoft. Provavelmente, isso foi feito via PowerShell, para que ele fosse carregado na memória em vez de gravado no disco e comprometer os computadores que controlam caixas eletrônicos. Em outro incidente, hackers conseguiram infectar máquinas e roubar US$ 800.000. Embora não tenham encontrado nenhum vestígio de malware nos caixas eletrônicos ou na rede de back-end, eles encontraram dois arquivos contendo logs de malware no disco rígido do caixa eletrônico, possivelmente instalados e executados por módulos de administração remota.

Outras formas de crime cibernético também foram vistas utilizando técnicas fileless. A Trend Micro reportou um ransomware com algumas semelhanças com o WannaCry, que explora as mesmas vulnerabilidades. No entanto, a variante de malware, chamada UIWIX, é fileless – e executada na memória depois de explorar o EternalBlue. O ransomware conclui automaticamente se detectar uma máquina virtual ou sandbox, permitindo evitar a detecção.

Outra campanha usou infecção fileless em kits de exploits, como no caso do grupo de criminosos cibernéticos Lurk, que roubou mais de US$ 45 milhões de instituições financeiras. Os invasores também usaram ameaças fileless em campanhas envolvendo mineradores de criptomoeda visando servidores corporativos e estações de trabalho e backdoors que chegam por meio do procedimento de registro de inicialização automática. O mais recente, no momento da redação deste artigo, envolve o troiano Astaroth, que foi deixado na memória dos computadores infectados e abusou da disseminação da ferramenta de linha de comando da Windows Management Instrumentation Command-line (WMIC).



Como usuários e empresas podem se defender contra ameaças fileless?

Enfrentar o cenário em constante mudança e proteger contra ameaças emergentes e sofisticadas, como ataques fileless, pode ser assustador para organizações que não estão cientes das técnicas envolvidas. No entanto, as ameaças fileless podem ser defendidas, apesar da falta de um binário ou executável discreto. Além de manter os sistemas e o software atualizados, as organizações podem implementar o princípio do menor privilégio e empregar uma sandbox personalizada.

Melhores Práticas

As organizações devem adotar essas práticas recomendadas para se preparar melhor contra os riscos mencionados:

- **Proteja o uso do PowerShell.** Use seu próprio recurso de registro, que pode ajudar a examinar comportamentos suspeitos em um sistema. Os administradores de TI também devem considerar listar gatilhos para detecção que podem se basear em comandos em scripts maliciosos do PowerShell.
- **Fazer hardening dos sistemas via comandos do PowerShell.** O uso do Windows PowerShell pode ser protegido ainda mais contra códigos maliciosos, empregando comandos que envolvem políticas de execução (ou seja, definindo condições sob as quais um script pode ser executado) e o uso de ConstrainedLanguageMode (por exemplo, restringindo scripts que podem ser usados para invocar funções arbitrárias).
- **Empregar mecanismos de monitoramento de comportamento.** Ter a monitoração do comportamento no endpoint pode auxiliar na prevenção e limitação do vazamento de dados e a infecção por malware, monitorando anomalias na cadeia de processos e bloqueando comportamentos e rotinas maliciosos associados ao malware. Ele também monitora modificações incomuns em softwares e aplicativos como o PowerShell.
- **Reinicie o dispositivo de endpoint e altere as senhas.** Reiniciar a máquina deve interromper qualquer ataque fileless, pois ele só manterá os dados na memória RAM quando o dispositivo estiver ligado – se a ameaça fileless não empregar nenhuma técnica de persistência. Os usuários também devem alterar suas senhas.
- **Instale um software de segurança que forneça proteção em várias camadas.** Considere produtos de segurança que podem detectar e impedir ameaças fileless na memória e outras técnicas que podem expor os sistemas a infecções desta natureza.
- **Desative componentes desnecessários.** Desabilitar componentes subutilizados e desatualizados pode impedir que um invasor viole um sistema ou rede a partir de um componente não seguro.
- **Bloqueie possíveis pontos de entrada.** Os vetores de ataque de ameaças fileless podem incluir sites e URLs maliciosos, spam e componentes vulneráveis de terceiros, como plug-ins de navegador.
- **Desconfie de macros.** A rota segura é desativar macros nos documentos do Microsoft Office para impedir a execução de códigos não seguros. Se não puder ser evitado, altere as configurações para permitir apenas macros assinadas digitalmente.
- **Evite abrir arquivos de locais não confiáveis.** Os arquivos maliciosos ainda podem participar de uma infecção fileless por meio de payloads embedados ou baixados.

Soluções Trend Micro

As Smart Protection Suites da Trend Micro oferecem vários recursos, como *machine learning* de alta fidelidade e serviços de reputação na web que minimizam o impacto de ameaças persistentes e fileless. A proteção Trend Micro Apex One™ emprega uma variedade de recursos de detecção de ameaças, principalmente análises comportamentais que protegem contra scripts maliciosos, injeção, ransomware, ataques de navegador e memória relacionados a ameaças fileless. Além disso, o Apex One Endpoint Sensor fornece investigação e resposta em endpoints (EDR) com reconhecimento de contexto que monitora eventos e examina rapidamente quais processos ou eventos estão desencadeando atividades maliciosas. A solução Trend Micro Deep Discovery™ possui uma camada para inspeção de e-mail que pode proteger as empresas detectando anexos e URLs maliciosos. O Deep Discovery pode detectar os scripts remotos, mesmo que não estejam sendo baixados no endpoint físico.

Também é importante monitorar proativamente os endpoints e as redes. As ameaças fileless podem não ser tão visíveis quanto outros malwares, mas também têm a capacidade de deixar sinais reveladores aos quais as equipes de TI e segurança podem prestar atenção, como tráfego de rede suspeito (para comunicação de C&C e exfiltração de dados). Por exemplo, a sandbox personalizada da Trend Micro integrada no Deep Discovery™ através do Deep Discovery Analyzer, Deep Security™ e Apex One™ pode interceptar APIs e verificar cadeias de código destinadas a executar a técnica ou as rotinas de evasão de um malware.

A implementação do monitoramento de comportamento também ajuda no identificação e no bloqueio de comportamentos e rotinas anômalos associados a um malware, como um processo sequestrado invocaria o Prompt de Comando para executar um script do PowerShell. As soluções de endpoints da Trend Micro, como Trend Micro™ Security, Apex One e Worry-Free Business Security, incluem monitoramento de comportamento para detectar ameaças fileless baseadas em script. Isso ajuda as organizações a olhar para o comportamento malicioso e bloquear o malware antes que o comportamento seja executado. O Apex One também pode incluir um recurso de controle de dispositivo que pode impedir o acesso a mídias removíveis, como USB e unidades ópticas, impedindo que sejam vetores de ameaças fileless.