Resumo de solução

Proteção contra malware sem arquivo

No ***Relatório do McAfee® Labs sobre ameaças: novembro de 2015***, examinamos detalhadamente o malware sem arquivo e nos aprofundamos nos aspectos técnicos do Kovter, que evita detecções ao reduzir ou eliminar o armazenamento de quaisquer binários em disco, ocultando seu código no Registro de um host comprometido. Os autores de malware tornaram desafiadora a detecção ao utilizar técnicas como polimorfismo, implantação de monitoramentos, revogação de permissões e muito mais. Também em 2015, vimos atacantes aproveitando recursos como a Instrumentação de Gerenciamento do Windows (ou Windows Management Instrumentation) e o Windows PowerShell para comprometer endpoints sem jamais armazenar um binário em disco, assegurando que os ataques permaneçam difíceis de rastrear.

As infecções com base em memória e sem arquivo já são conhecidas há anos pelo setor de segurança. Muito embora sejam consideradas sem arquivo, famílias de malware anteriores instalavam um pequeno binário em disco na fase de ataque inicial, antes de passar para a memória principal do host comprometido. Porém, as últimas técnicas de evasão utilizadas por malware sem arquivo — Kovter, Powelike e XswKit, por exemplo — não deixam vestígio algum no disco, tornando mais difícil a detecção, que geralmente depende de arquivos estáticos no disco.

Existem três tipos comuns de malware sem arquivo:

- **Residente na memória**: esse tipo de malware sem arquivo utiliza o espaço de memória de um arquivo legítimo do Windows. Ele carrega seu código nesse espaço de memória e permanece residente até ser acessado ou reativado. Embora a execução ocorra dentro do espaço de memória do arquivo legítimo, há um arquivo físico em hibernação que inicia ou reinicia a execução. Consequentemente, esse tipo de malware não é completamente sem arquivo.
- **Rootkits**: alguns exemplares de malware sem arquivo ocultam sua presença por trás de uma interface de programação de aplicativos (API) em nível de kernel ou de usuário. Um arquivo está presente no disco, mas em modo oculto.
- **Registro do Windows**: alguns novos tipos de malware sem arquivo residem no Registro do sistema operacional Windows. Os autores de malware exploraram recursos como o cache de miniaturas do Windows, utilizado para armazenar imagens para a visualização de miniaturas do Windows Explorer. O cache de miniaturas atua como um mecanismo de persistência para o malware. O malware sem arquivo desse tipo precisa ainda entrar no sistema da vítima por meio de um binário estático. A maioria utiliza o e-mail como meio para atingir o sistema. Assim que o usuário clica no anexo, o malware grava o arquivo de carga completo, de forma criptografada, no Registro do Windows. Ele, então, desaparece do sistema excluindo a si próprio.

intel Security

Os autores de malware construíram habilmente as famílias de malware Kovter, Powelike e XswKit para executar ataques completamente sem arquivo ao Registro do Windows, sem deixar vestígio algum no sistema de arquivos. Embora o ambiente para a realização desses ataques seja preparado pela execução de código em um arquivo, o arquivo se destroi quando o sistema está pronto para a operação maliciosa.

Como a Intel Security ajuda na proteção contra o malware sem arquivo

A detecção completa de malware sem arquivo que não envolva um binário inicial pode ser complicada e frequentemente é necessário um trabalho investigativo por parte da organização de segurança. No entanto, assegurar que controles adequados estejam implementados para negar aos atacantes um ponto de entrada é fundamental para deter o malware sem arquivo.

McAfee Advanced Threat Defense

O **McAfee Advanced Threat Defense** é um produto para detecção de malware em múltiplas camadas que combina vários mecanismos de inspeção. Ao combinar múltiplos mecanismos que aplicam inspeção com base em assinaturas e em reputação, emulação em tempo real, análise completa de código estático e análise dinâmica em área restrita (sandbox), o McAfee Advanced Threat Defense oferece proteção contra o malware sem arquivo que inicialmente instala um binário no sistema-alvo.

- **Detecção com base em assinaturas**: detecta vírus, worms, spyware, bots, cavalos de Troia, estouros de buffer e ataques combinados. Sua base de conhecimentos abrangente é criada e mantida pelo McAfee Labs.
- **Detecção com base em reputação**: consulta a reputação dos arquivos utilizando o McAfee Global Threat Intelligence (McAfee GTI) para detectar ameaças recém-surgidas.
- **Análise estática e emulação em tempo real**: oferece emulação e análise estática em tempo real para localizar rapidamente malware e ameaças de dia zero não identificados por reputação ou técnicas com base em assinaturas.
- **Análise completa de código estático**: faz a engenharia reversa do código do arquivo para determinar todos os seus atributos e conjuntos de instruções e analisa completamente o código-fonte sem execução. Seus recursos de descompactação abrangentes abrem todos os tipos de arquivos compactados para a análise completa e classificação do malware, permitindo que a sua empresa entenda a ameaça representada pelo malware em questão.
- **Análise dinâmica em área restrita**: para os arquivos cuja segurança não possa ser determinada pelos mecanismos de inspeção acima, o McAfee Advanced Threat Defense pode executar o código do arquivo em um ambiente de tempo de execução virtual e observar o comportamento resultante. Ambientes virtuais podem ser configurados para corresponder aos ambientes host. O McAfee Advanced Threat Defense é compatível com imagens personalizadas dos sistemas operacionais (OS) Windows XP SP2 e SP3, Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows Server 2003, Windows Server 2008 (64 bits) e Android.

McAfee Threat Intelligence Exchange

É imprescindível dispor de uma plataforma de inteligência capaz de se adaptar, com o passar do tempo, para atender às necessidades do seu ambiente. O **McAfee Threat Intelligence Exchange** reduz significativamente a exposição a ataques de malware sem arquivo, graças à sua visibilidade sobre ameaças imediatas, como aplicativos ou arquivos desconhecidos em execução no ambiente.

- **Inteligência abrangente sobre ameaças**: personalize facilmente informações abrangentes sobre ameaças obtidas de fontes de dados de inteligência global sobre ameaças. Essas fontes podem ser o McAfee GTI ou canais de terceiros, com inteligência local sobre ameaças obtida de dados de eventos históricos e em tempo real fornecidos via endpoints, gateways e outros componentes de segurança.

- **Prevenção de execução e correção**: o McAfee Threat Intelligence Exchange pode intervir e impedir que aplicativos desconhecidos sejam executados no ambiente. Caso um aplicativo cuja execução tenha sido permitida seja posteriormente considerado malicioso, o McAfee Threat Intelligence Exchange pode desativar os processos em execução associados ao aplicativo em todo o ambiente, graças às poderosas capacidades de imposição de políticas e gerenciamento central do produto.
- **Visibilidade**: o McAfee Threat Intelligence Exchange pode rastrear todos os arquivos executáveis compactados e sua execução inicial no ambiente, bem como todas as alterações ocorridas a partir de então. Essa visibilidade sobre as ações de um aplicativo ou processo, desde a instalação até o momento presente, permite mais rapidez na resposta e na correção.
- **Indicadores de comprometimento**: importe hashes de arquivos notoriamente nocivos e imunize o seu ambiente contra essas ameaças conhecidas através da imposição de políticas. Caso algum dos indicadores de comprometimento seja acionado no ambiente, o McAfee Threat Intelligence Exchange pode eliminar todos os processos e aplicativos associados aos indicadores de comprometimento.

McAfee Web Gateway

Downloads de passagem e URLs maliciosos incorporados em e-mails de phishing são os principais métodos de ataque utilizados para entregar malware de sem arquivo. O **McAfee Web Gateway** é um produto sólido que reforça a proteção da sua empresa contra esse tipo de ameaça.

- **McAfee Gateway Anti-Malware Engine**: a análise de intenção sem assinaturas filtra o conteúdo malicioso do tráfego na Web em tempo real. A emulação e análise de comportamento protegem de forma proativa contra ataques de dia zero e ataques direcionados. O McAfee Gateway Anti-Malware Engine inspeciona os arquivos e impede que os usuários façam download se tais arquivos são maliciosos.
- **Integração com o McAfee GTI**: canais de inteligência em tempo real, com reputação de arquivos, reputação na Web e categorizações na Web do McAfee GTI, oferecem proteção contra as ameaças mais recentes, pois o McAfee Web Gateway impede tentativas de conexão a sites maliciosos conhecidos ou a sites que usam redes de anúncios maliciosos.

Além desses produtos da Intel Security, recomendamos duas classes adicionais de tecnologias de segurança.

- **Segurança de gateway de e-mail**: a maior parte do malware sem arquivo entra nos sistemas através de um anexo em uma mensagem de e-mail, portanto, um produto robusto de segurança de gateway de e-mail que faça varredura de todos os anexos quanto à presença de malware deve ser parte de uma defesa sólida contra esse tipo de ataque.
- **Firewall**: a tecnologia de firewall é fundamental para qualquer sistema de segurança. Um firewall pode detectar muitas ameaças no perímetro — antes que elas entrem na rede confiável. Como o malware sem arquivo entra nos sistemas através de binários estáticos, muitos desses ataques podem ser interrompidos antes que invadam sistemas dentro da rede confiável.

McAfee. Part of Intel Security.
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070 - São Paulo - SP - Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.intelsecurity.com