Proteção contra malware com base em scripts

Os autores de malware tornaram desafiadora a detecção ao utilizar técnicas como polimorfismo, implantação de monitoramentos, revogação de permissões e muitas outras.

Durante esta década, vimos atacantes aproveitando recursos como o Microsoft Windows Management Instrumentation (WMI) e o Windows PowerShell para comprometer endpoints sem jamais armazenar um binário em disco, assegurando que os ataques permaneçam difíceis de rastrear porque o código malicioso pode ser implantado diretamente no Registro de um host comprometido.

Infecções com base em scripts já existem há anos. 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 sistema.

Porém, as últimas técnicas de evasão utilizadas por malware de script não deixam vestígio algum no disco, tornando mais difícil a detecção, que geralmente consiste em localizar arquivos estáticos. Leia nossa análise detalhada sobre malware com base em scripts no *Relatório do McAfee Labs sobre ameaças: setembro de 2017*.

Existem três tipos comuns de malware com base em scripts:

- **Residente na memória:** esse tipo de malware 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.
- **Rootkits:** alguns exemplares de malware 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 tipos avançados de malware de script residem no Registro do Windows. Os autores de malware já exploraram recursos como o cache de miniaturas do Windows, utilizado para armazenar imagens para a visualização de miniaturas do Explorer. O cache de miniaturas atua como um mecanismo de persistência para o ataque. O malware desse tipo precisa ainda entrar no sistema da vítima por meio de um binário estático. A maioria utiliza e-mail como vetor de ataque para atingir o sistema. Assim que o usuário clica no anexo, o malware grava o arquivo de carga completo, de forma criptografada, em chaves do Registro do Windows. Ele, então, desaparece do sistema excluindo a si próprio.

Atualmente, os autores de malware já construíram habilmente as famílias de malware de script necessárias 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 exclui a si mesmo quando o sistema está pronto para a operação maliciosa.

Políticas e procedimentos para proteção contra malware com base em script

As mais recentes práticas recomendadas de defesa cibernética da McAfee incluem a adoção das seguintes estratégias gerais de mitigação de ameaças para redes e endpoints:

- A melhor maneira de proteger o seu sistema contra infecções por malware de script é bloqueá-las antes que elas aconteçam. A prevenção é a chave. O fator mais relevante na prevenção de qualquer tipo de infecção por malware em um computador é o usuário. Os usuários precisam estar cientes dos riscos de fazer download e instalar aplicativos que eles não compreendem ou nos quais não confiam. Além disso, o malware pode ser contraído inadvertidamente via download por usuários incautos durante a navegação.
- Aplique correções e atualizações de segurança aos seus aplicativos e ao sistema operacional.
- Mantenha os navegadores da Web e seus complementos atualizados e aplique as versões mais recentes de atualização e upgrade no antimalware dos endpoints e gateways de rede.

- Nunca utilize computadores que não sejam distribuídos e certificados pelo seu grupo de segurança de TI corporativa. O malware de script pode ser facilmente disseminado por ativos desprotegidos conectados à sua rede corporativa.
- Caso os usuários tenham privilégios de administrador local para instalar aplicativos por conta própria, instrua-os a instalar somente aplicativos de fornecedores conhecidos e com assinaturas confiáveis. É muito comum que aplicativos "inofensivos" oferecidos on-line contenham rootkits e outros tipos de malware de script.
- Evite downloads de aplicativos que não sejam da Web. Em grupos da Usenet, canais de IRC, programas de mensagens instantâneas ou redes P2P, a probabilidade de se fazer download de malware é muito grande. Links para sites vistos no IRC e em programas de mensagens instantâneas também levam, frequentemente, a downloads infectados.
- Implemente um programa de conscientização para prevenção de ataques de phishing. O malware é frequentemente distribuído por e-mails direcionados.
- Aproveite canais de Inteligência contra ameaças, aliados à sua tecnologia antimalware. Essa combinação o ajudará a melhorar o tempo de detecção das ameaças de malware, tanto as emergentes quanto as já conhecidas.

Como a McAfee ajuda na proteção contra malware com base em scripts

A detecção completa de malware de script 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 esse tipo de malware.

McAfee Endpoint Security

O McAfee Endpoint Security (ENS) proporciona uma estrutura de segurança colaborativa que reduz a complexidade dos ambientes de segurança de endpoint e oferece visibilidade sobre ameaças avançadas, como malware de script, acelerando a detecção e as respostas de correção. Sua arquitetura expansível oferece a equipes de segurança sobrecarregadas por múltiplas soluções uma estrutura que permite visualizar, responder e gerenciar facilmente o ciclo de vida da defesa contra ameaças.

O McAfee ENS introduz várias novas tecnologias e aperfeiçoamentos:

- **Real Protect.** Aplica técnicas de autoaprendizagem para identificar código malicioso com base em sua aparência, no que ele talvez faça (análise pré-execução) e no que ele faz (análise comportamental dinâmica) — sem assinaturas. O Real Protect é parte de uma estratégia de defesa eficaz contra o malware de script.

- **Contenção dinâmica de aplicativos.** Inclui a capacidade de conter uma única instância de um processo.
- **Integração com o McAfee Client Proxy.** O McAfee Endpoint Security pode ser combinado com a segurança multicamada do gateway de Web, a qual proporciona proteção em qualquer lugar onde o usuário esteja, eliminando a lacuna da proteção fora da rede ao conectar os endpoints ao serviço de nuvem do Web Gateway.
- **Módulo de firewall.** A próxima camada de proteção assegurada por uma estratégia de segurança proativa consiste em bloquear a comunicação entre o seu computador e os servidores controlados pelos criminosos cibernéticos.
- **Módulo de prevenção de ameaças.** As varreduras solicitadas agora incluem uma opção de varredura do Registro, útil para proteção contra malware de script. Os administradores podem criar regras personalizadas de proteção de acesso a serviços, que agora incluem serviços do Windows. A prevenção personalizada de explorações em aplicativos está disponível juntamente com as assinaturas de sistema de prevenção de intrusões fornecidas pela McAfee. Finalmente, uma proteção para aplicativos de Windows foi adicionada às regras de prevenção de explorações.

McAfee Advanced Threat Defense

O McAfee Advanced Threat Defense (ATD) 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 ATD oferece proteção contra o malware de script 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 (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 (sandbox):** para os arquivos cuja segurança não possa ser determinada pelos mecanismos de inspeção precedentes, o McAfee ATD 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.

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 ambiente. O McAfee Threat Intelligence Exchange (TIE) reduz significativamente a exposição a ataques de malware de script, graças à sua visibilidade sobre ameaças imediatas, como aplicativos ou arquivos desconhecidos em execução no ambiente.

- **Informações abrangentes contra ameaças:** personalize facilmente informações abrangentes contra ameaças obtidas de fontes de dados de inteligência global contra 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 TIE 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 TIE 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 TIE 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 TIE 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 script. O McAfee Web Gateway (MWG) é um produto sólido que reforça a proteção da sua empresa contra esse tipo de ameaça.

- **Gateway Anti-Malware Engine:** a análise de intenção sem assinaturas filtra o conteúdo malicioso do tráfego da 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 MWG impede tentativas de conexão a sites maliciosos conhecidos ou a sites que usam redes de anúncios maliciosos. Além desses produtos da McAfee, recomendamos duas classes adicionais de tecnologias de segurança.
  - **Segurança de gateway de e-mail:** a maior parte do malware de script 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 de script entra nos sistemas através de binários estáticos, muitos desses ataques podem ser interrompidos antes que invadam sistemas dentro da rede confiável.

McAfee
Together is power.

Av. Nações Unidas, 8.501 – 16º andar
Pinheiros – São Paulo – SP
CEP 05425-070, Brasil
+(11) 3711-8200
www.mcafee.com/br

3529_0917
SETEMBRO DE 2017