Resumo de solução

Proteção contra explorações no Adobe Flash

A plataforma de software e multimídia Adobe Flash é um formato bastante conhecido para apresentar conteúdos com base na Web, como jogos, sites, aplicativos, entre outros. Infelizmente, sua popularidade faz dele um alvo atraente para os criminosos cibernéticos, que exploram, de forma implacável, novas vulnerabilidades não corrigidas, prejudicando usuários desavisados.

Predominância das explorações no Adobe Flash

As explorações Flash são discutidas em detalhes no ***Relatório do McAfee Labs sobre ameaças: maio de 2015***. As explorações Flash começaram a aumentar dramaticamente a partir do último trimestre de 2014. Hoje, elas estão entre os principais alvos dos autores de explorações. O McAfee Labs acredita que existem diversos fatores que explicam essa tendência: o aumento constante no número de vulnerabilidades do Flash; a demora dos usuários em aplicar correções de software para essas vulnerabilidades; métodos novos e criativos para explorá-las; um aumento expressivo no número de dispositivos móveis que executam arquivos .swf do Flash; e a dificuldade em detectar as explorações Flash.

O Angler se destaca como o kit de exploração mais popular entre os kits que entregam explorações Flash. Esse kit potente, discutido em detalhes no ***Relatório do McAfee Labs sobre ameaças: fevereiro de 2015***, é um kit de ferramentas fácil de usar e pronto para uso, capaz de entregar uma ampla variedade de cargas através da exploração das vulnerabilidades.

Proteção contra as explorações Flash

Descubra algumas práticas e procedimentos úteis para se proteger contra as explorações Flash:

- Ative as atualizações automáticas do sistema operacional, ou faça download dessas atualizações regularmente para manter os sistemas operacionais corrigidos contra vulnerabilidades conhecidas.
- Configure o software antivírus para bloquear anexos com a extensão .swf.
- Defina as configurações de segurança do navegador em nível médio ou superior.
- Use um plug-in de navegador para bloquear a execução de scripts e iframes.
- Não instale plug-ins de navegador não confiáveis.

intel Security

- Tenha muito cuidado ao abrir anexos, principalmente aqueles que vêm com a extensão .swf.
- Nunca abra e-mails não solicitados ou anexos inesperados — mesmo que venham de pessoas conhecidas.
- Cuidado com esquemas de phishing com base em spam. Não clique em links de e-mails ou de mensagens instantâneas.
- Digite ou copie os URLs na barra de endereço do navegador e verifique o endereço em vez de clicar nos anúncios Web.
- Não clique em vídeos Flash em sites não confiáveis.

Saiba como a Intel Security pode ajudá-lo a se proteger contra as explorações Flash

McAfee Web Gateway

Anúncios enganosos, downloads de passagem e URLs maliciosos incorporados em sites confiáveis são apenas alguns dos métodos de ataque utilizados para empreender ataques que aproveitam as explorações Flash. 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 Global Threat Intelligence (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.

McAfee Application Control

O **McAfee Application Control** permite que a sua empresa controle quais aplicativos estão autorizados a ser executados no seu ambiente através de listas brancas dinâmicas e políticas de imposição para endpoints tanto conectados quanto desconectados. Garantir a proteção da sua organização contra aplicativos vulneráveis, como as instalações Flash antigas, é o segredo para combater a crescente tendência das explorações Flash.

- **Listas brancas dinâmicas:** permitem que sua organização gerencie de forma eficiente seus aplicativos relacionados em listas brancas, elaborando tais listas automaticamente conforme os sistemas são corrigidos e atualizados. O McAfee Application Control reduz a sua exposição às explorações Flash ao impedir que versões não corrigidas do Flash sejam executadas no seu ambiente.
- **Reputação de arquivos:** a integração com o McAfee GTI permite que o McAfee Application Control consulte canais em tempo real de tipos de arquivos válidos conhecidos, inválidos e desconhecidos, ajudando a sua empresa a ficar atenta a vulnerabilidades ou ataques de aplicativos que podem ter sido alterados.
- **Mantenha-se protegido, conectado ou desconectado:** imponha controles a servidores conectados ou desconectados, máquinas virtuais, endpoints e dispositivos de função fixa, como terminais de ponto de venda.

McAfee Vulnerability Manager
O **McAfee Vulnerability Manager** ajuda a sua organização a entender a extensão da exposição que pode ser causada pelas versões antigas do Flash instaladas no seu ambiente, e a tomar as medidas necessárias para reduzir essa exposição de forma eficaz.

- **Varredura abrangente de vulnerabilidades:** o McAfee Vulnerability Manager é um produto independente e altamente expansível para descoberta de host, gerenciamento de ativos, avaliação de vulnerabilidade e geração de relatórios sobre qualquer dispositivo conectado à rede. O McAfee Vulnerability Manager consegue avaliar a exposição do seu ambiente às explorações Flash ao fazer a varredura de sistemas que estão executando versões vulneráveis do Flash.
- **Geração de relatórios e correção flexíveis:** o McAfee Vulnerability Manager e o **McAfee Asset Manager** trabalham juntos para oferecer monitoramento automatizado e gerenciamento de varredura, correção, imposição e geração de relatórios. Isso ajuda a evitar demoradas simulações de emergências e processos específicos, a eliminar erros e a proteger mais sistemas de maneira eficiente.
- **Conheça a sua exposição:** o McAfee Asset Manager permite que a sua empresa saiba quais sistemas estão vulneráveis às explorações Flash pela correlação de varreduras de vulnerabilidade com varreduras de descoberta de host. Poder identificar em tempo real quais sistemas estão executando versões Flash vulneráveis significa perder menos tempo pensando se você está exposto e poder dedicar mais tempo à correção.

McAfee Threat Intelligence Exchange
É imprescindível dispor de uma plataforma de inteligência capaz de se adaptar para atender às necessidades do seu ambiente. O **McAfee Threat Intelligence Exchange** reduz significativamente a exposição a ataques, graças à sua visibilidade sobre ameaças imediatas, como aplicativos ou arquivos desconhecidos, que exploram as vulnerabilidades Flash no ambiente da sua organização.

- **Informações abrangentes sobre ameaças:** personalize facilmente informações abrangentes sobre ameaças obtidas de fontes de dados de inteligência global. Essas fontes podem ser o McAfee GTI ou canais de terceiros, com informações locais sobre ameaças obtidas 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 suas poderosas capacidades de imposição de políticas e gerenciamento central.
- **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 (IoCs):** importe hashes de arquivos nocivos conhecidos para que o McAfee Threat Intelligence Exchange imunize o seu ambiente contra esses arquivos notoriamente nocivos através da imposição de políticas. Caso algum dos indicadores de comprometimento (IoCs) seja acionado no ambiente, o McAfee Threat Intelligence Exchange pode eliminar todos os processos e aplicativos associados com o IoC.

McAfee VirusScan Enterprise

Com o **McAfee VirusScan® Enterprise** é fácil detectar e limpar o malware que explora as vulnerabilidades Flash para infiltrar seu ambiente. O McAfee VirusScan Enterprise utiliza o premiado mecanismo de varredura da McAfee para proteger os seus arquivos contra vírus, worms, rootkits, cavalos de Troia e outras ameaças avançadas.

- **Proteção proativa contra ataques:** integra tecnologia antimalware com prevenção de intrusões para proteção contra explorações que utilizam explorações de estouro de buffer direcionadas contra vulnerabilidades em aplicativos.
- **Detecção e limpeza de malware imbatíveis:** protege contra ameaças, como rootkits e cavalos de Troia, com análise comportamental avançada. Detém o malware utilizando técnicas como bloqueio de portas, nomes de arquivos, pastas/diretórios e compartilhamentos de arquivos, bem como rastreamento e bloqueio de infecções.
- **Segurança em tempo real com integração com o McAfee GTI:** protege contra ameaças conhecidas e emergentes em todos os vetores de ameaça — arquivos, Web, e-mail e rede — com o suporte da plataforma de inteligência sobre ameaças mais abrangente do mercado.

McAfee Global Threat Intelligence

O **McAfee Global Threat Intelligence (McAfee GTI)** é um serviço abrangente de inteligência sobre ameaças em tempo real com base na nuvem que permite aos produtos da McAfee bloquear ameaças cibernéticas em todos os vetores — arquivos, Web, mensagens e rede. Garanta proteção proativa contra explorações Flash e outras ameaças com os recursos abaixo:

- **Inteligência através da correlação de vetores:** reúne e correlaciona dados oriundos dos principais vetores de ameaça — arquivos, Web, e-mail e rede — para detectar ameaças mistas.
- **Plataforma abrangente de inteligência sobre ameaças:** coleta informações sobre ameaças de milhões de sensores em produtos McAfee distribuídos por clientes, como sistemas de prevenção de intrusões de rede, e-mail, Web e endpoint, além de dispositivos firewall.
- **Security Connected:** integrado com outros produtos de segurança da McAfee para proporcionar os dados mais amplos sobre ameaças, a mais minuciosa correlação de dados e a mais completa integração de produtos disponível no momento, para garantir proteção contra as explorações Flash.

McAfee VirusScan Mobile

O **McAfee VirusScan Mobile** é um sistema antimalware que faz varredura e limpeza de dados móveis, prevenindo corrupção decorrente de vírus, cavalos de Troia e outros tipos de código malicioso. O McAfee VirusScan Mobile protege seus dispositivos móveis nos pontos mais críticos de exposição, incluindo e-mails recebidos e enviados, mensagens de texto, anexos de e-mail e downloads da Internet.

- Detecção de ameaças em tempo real: bloqueie malware em e-mails, mensagens de texto e anexos sem atraso perceptível. O McAfee VirusScan Mobile procura uma variedade de ameaças maliciosas em menos de 200 milissegundos, proporcionando proteção automática e abrangente para smartphones.

A crescente predominância das vulnerabilidades Flash, que são aproveitadas pelos autores de malware, não mostra sinais de atenuação. A tecnologia da Intel Security é capaz de ajudar sua empresa a se proteger de forma proativa contra ameaças que buscam explorar essas vulnerabilidades.

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