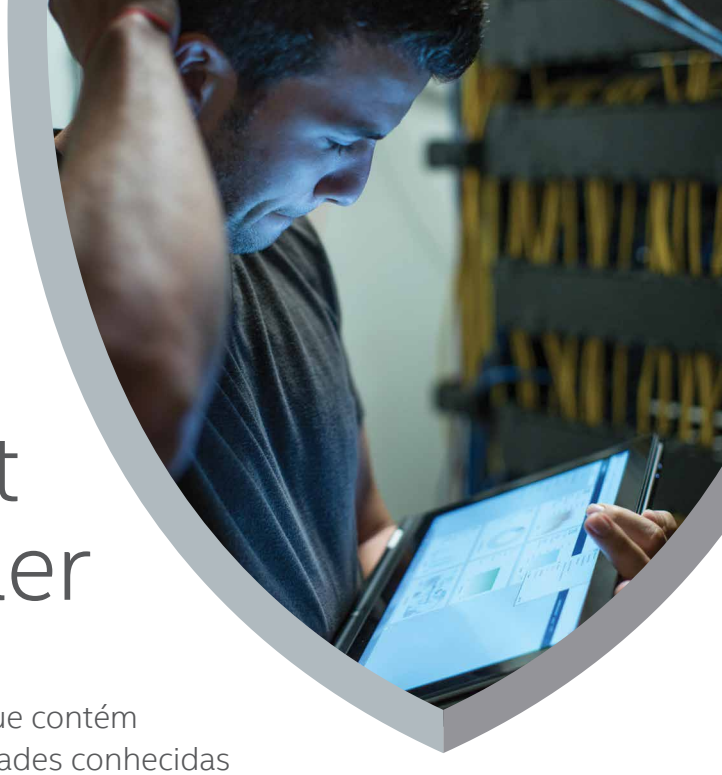
Resumo de solução



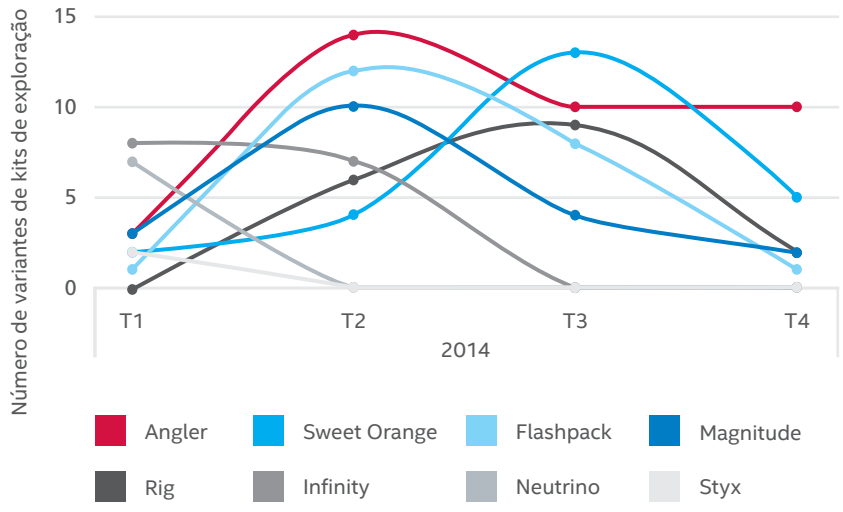
Como derrotar o kit de exploração Angler

Um kit de exploração é um pacote pronto de software que contém ataques predefinidos e fáceis de usar contra vulnerabilidades conhecidas e desconhecidas (de dia zero). Esses kits de ferramentas exploram vulnerabilidades no lado do cliente, visando tipicamente o navegador Web e aplicativos que podem ser acessados por meio do navegador Web. Os kits de exploração também rastreiam parâmetros de infecção e têm sólidas capacidades de controle.

O que é o kit de exploração Angler?

O kit de exploração Angler é discutido em detalhes no **Relatório de ameaças do McAfee® Labs: fevereiro de 2015**. O Angler cresceu em predominância e notoriedade no segundo semestre de 2014 devido a recursos como infecção sem arquivos (injeção em memória), máquina virtual e detecção de produtos de segurança, bem como sua capacidade de entregar uma ampla variedade de cargas, incluindo cavalos de Troia bancários, rootkits, ransomware, CryptoLocker e cavalos de Troia de backdoor. Além disso, o Angler não exige proficiência técnica para ser utilizado eficazmente e sua disponibilidade em mercados do submundo on-line resultou em seu grande crescimento:

Variantes entre os kits de exploração em 2014



Fonte: McAfee Labs, 2015

intel Security

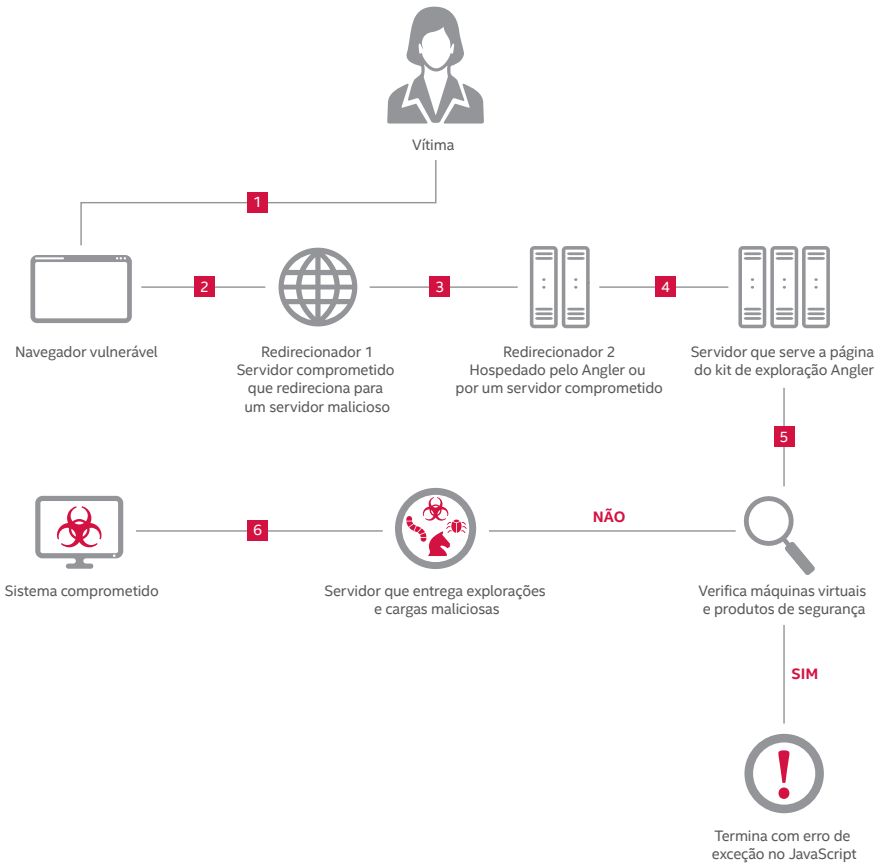
O Angler frequentemente altera seus padrões e cargas para contornar a capacidade dos produtos de segurança de detectar o kit de exploração ativo. O Angler executa várias ações evasivas para evitar detecção:

- Usa dois níveis de redirecionadores antes de chegar à página de destino.
- Os servidores Web comprometidos que hospedam a página de destino só podem ser visitados uma vez a partir de cada IP. Os atacantes estão, evidentemente, monitorando os hosts.
- Detecta a presença de máquinas virtuais e produtos de segurança no sistema.
- Faz chamadas falsas para dificultar engenharia reversa.
- Criptografa todas as cargas no download e as descriptografa na máquina comprometida.
- Utiliza infecção sem arquivos (instala-se diretamente na memória).

O kit de exploração Angler executa várias etapas para conseguir infectar os sistemas:

- A vítima utiliza um navegador vulnerável para acessar um servidor Web comprometido.
- O servidor Web comprometido redireciona para um servidor intermediário.
- O servidor intermediário redireciona para um servidor Web malicioso que hospeda a página de destino do kit de exploração.
- A página de destino verifica se há plug-ins vulneráveis (Java, Flash e Silverlight) e verifica suas informações de versão.
- Quando plug-ins ou um navegador vulnerável são encontrados, o kit de exploração fornece a carga apropriada e infecta a máquina.

Cadeia de infecção do kit de exploração Angler



Como se proteger contra o kit de exploração Angler

Veja a seguir algumas maneiras de proteger sistemas contra o kit de exploração Angler:

- Use um provedor de serviços de Internet que seja responsável em relação à segurança e que implemente procedimentos fortes contra spam e phishing.
- Ative atualizações automáticas ou faça download de atualizações do sistema operacional regularmente para manter os sistemas operacionais corrigidos contra vulnerabilidades conhecidas. Instale patches de outros desenvolvedores de software tão logo eles sejam distribuídos. Um computador com todas as correções instaladas e atrás de um firewall é a melhor defesa contra ataques de cavalos de Troia e spyware.
- Tenha atenção redobrada ao abrir anexos. Configure o seu software antivírus para examinar automaticamente todos os anexos de e-mail e de mensagens instantâneas. Certifique-se de que os programas de e-mail não abram anexos ou processem gráficos automaticamente e certifique-se de que o painel de visualização esteja desativado. 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.
- Use um plug-in de navegador para bloquear a execução de scripts e iframes.

Como a Intel Security pode ajudá-lo a se proteger contra o kit de exploração Angler

McAfee Web Gateway

Anúncios enganosos, downloads de passagem e URLs maliciosos incorporados em sites confiáveis são apenas alguns dos métodos de ataque utilizados para fornecer o kit de exploração Angler. O **McAfee Web Gateway** é um produto sólido que incrementa 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 a 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 dos mesmos caso sejam maliciosos.
- **Integração com o McAfee Global Threat Intelligence (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 VirusScan® Enterprise

Detectar e limpar malware do tipo fornecido pelo Angler é simples com o **McAfee VirusScan Enterprise**. 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**: proteção contra ameaças conhecidas e emergentes em todos os vetores de ameaças — arquivos, Web, e-mail e rede — com o suporte da plataforma de inteligência sobre ameaças mais abrangente do mercado.

McAfee Advanced Threat Defense

O **McAfee Advanced Threat Defense** é uma solução de 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 os kits de exploração predominantes, como o Angler e o malware por ele distribuído.

- **Detecção com base em assinaturas**: detecta vírus, worms, spyware, bots, cavalos de Troia, estouros de buffer e ataques combinados. Sua abrangente base de conhecimentos é criada e mantida pelo McAfee Labs e atualmente contém mais de 150 milhões de assinaturas, incluindo o Angler e suas variantes.
- **Detecção com base em reputação**: consulta a reputação dos arquivos utilizando a rede 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 engenharia reversa do código do arquivo para determinar todos os seus atributos e conjuntos de instruções e analisar completamente o código-fonte sem execução. Amplos recursos de descompactação permitem abrir todos os tipos de arquivos compactados, permitindo análise completa e classificação do malware para que a sua empresa compreenda a ameaça representada pelo malware em questão.
- **Análise dinâmica em área restrita**: executa o código do arquivo em um ambiente virtual em tempo de execução e observa o comportamento resultante. Ambientes virtuais podem ser configurados conforme os ambientes de host da sua empresa, com suporte para imagens personalizadas de sistema operacional Windows 7 (32/64 bits), Windows XP, Windows Server 2003, Windows Server 2008 (64 bits) e Android.

McAfee Network Security Platform

O **McAfee Network Security Platform** foi desenvolvido para realizar inspeções profundas no tráfego de rede. Ele reúne técnicas de inspeção avançadas, que incluem análise completa de protocolo, reputação de ameaças, análise de comportamento e análise avançada de malware para detectar e impedir ataques conhecidos e de dia zero na rede.

- **Defesa abrangente contra malware**: reúne reputação de arquivos do McAfee GTI, análise profunda de arquivos com detecção de JavaScript e análise avançada de malware, sem assinaturas, para detectar e deter ameaças de dia zero, malware personalizado e outros ataques furtivos.
- **Aproveita técnicas avançadas de inspeção**: inclui análise completa de protocolo, reputação de ameaças e análise de comportamento para detectar e prevenir ataques conhecidos e de dia zero na rede.
- **Integração com o McAfee GTI**: combina canais de geolocalização, reputação de IP e reputação de arquivos em tempo real com dados contextuais detalhados sobre usuários, dispositivos e aplicativos para respostas rápidas e precisas a ataques via rede.
- **Security Connected**: uma integração decisiva com o McAfee Advanced Threat Defense permite ao McAfee Network Security Platform enviar para o McAfee Advanced Threat Defense arquivos suspeitos encontrados no tráfego monitorado e permiti-los ou proibi-los, com base em descobertas do McAfee Advanced Threat Defense.

McAfee Threat Intelligence Exchange

É importante 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** reduz significativamente a exposição a esses tipos de ataque, graças à sua visibilidade sobre ameaças iminentes, como arquivos ou aplicativos desconhecidos em execução no seu ambiente.

- **Inteligência abrangente sobre ameaças**: personalize facilmente uma inteligência abrangente sobre ameaças obtida de fontes de dados de inteligência global. 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 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 inicial 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 TIE pode eliminar todos os processos e aplicativos associados com o IoC.

O predomínio crescente de kits de exploração fáceis de usar, como o Angler, nos faz acordar para o fato de que o cenário de ameaças está sempre mudando. A tecnologia da Intel Security pode ajudar a sua empresa a se proteger proativamente contra ameaças como o kit de exploração Angler, tanto no endpoint quanto na rede.

61738brf_angler-exploit-kit_0215

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