Resumo de solução

Proteção contra malware evasivo

Conforme detalhamos no Relatório do McAfee Labs sobre ameaças: junho de 2017, o malware evasivo disfarça-se para não ser detectado. Ele se esconde subvertendo ou acrescentando-se a aplicativos legítimos. Ele reconhece quando está sendo analisado em uma área restrita (sandbox) e atrasa sua execução, aguardando durante dias, semanas e até meses por uma oportunidade de atacar.

A criação de um programa de segurança para proteção contra malware evasivo deve se basear em três componentes fundamentais.

- **Pessoas**: os profissionais de segurança devem ser treinados para responder adequadamente aos incidentes de segurança e gerenciar devidamente a tecnologia de segurança atual. Os atacantes costumam utilizar engenharia social para infectar os usuários. Sem treinamento e conscientização interna, os usuários deixam janelas abertas para os atacantes.
- **Processo**: processos internos e estruturas claras precisam estar implementados para que os profissionais de segurança sejam eficientes. As melhores práticas de segurança (atualizações, backups, governança, inteligência, planos de resposta a incidentes e mais) são as chaves para uma equipe de segurança poderosa e eficaz.
- **Tecnologia**: a tecnologia respalda a equipe e os processos. Ela deve ser cultivada e aprimorada para que se adapte às novas ameaças.

Políticas e procedimentos decisivos para proteção contra malware evasivo

- A defesa mais importante contra infecções por malware são os usuários. Os usuários devem estar cientes do risco do download e instalação de aplicativos oriundos de fontes potencialmente arriscadas. Os usuários também devem aprender que o malware pode ser contraído inadvertidamente durante a navegação.
- Sempre mantenha os navegadores e seus complementos atualizados e aplique as versões mais recentes de atualização e upgrade dos endpoints e gateways de rede.
- Não permita, na rede confiável, sistemas que não sejam distribuídos e certificados pelo grupo de segurança de TI corporativa. O malware evasivo pode ser facilmente disseminado por sistemas desprotegidos conectados à rede confiável.

McAfee™
Together is power.

- O malware evasivo pode se esconder dentro de software legítimo previamente "troianizado" por um atacante. Para evitar um ataque bem-sucedido desse tipo, mecanismos rígidos de fornecimento e distribuição de software são altamente recomendáveis. É sempre bom ter um repositório central de aplicativos corporativos do qual os usuários possam fazer download de software aprovado.
- Em situações nas quais os usuários estejam autorizados a instalar aplicativos não previamente validados pelo grupo de segurança de TI, instrua os usuários a instalar somente aplicativos de fornecedores conhecidos e com assinaturas confiáveis. É muito comum que aplicativos "inofensivos" oferecidos on-line tenham malware evasivo incorporado.
- Evite downloads de aplicativos que não sejam da Web. Em grupos da Usenet, canais de IRC, programas de mensagens instantâneas ou sistemas 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 ataques de phishing.
- Aproveite canais de Inteligência contra ameaças, aliados a tecnologia antimalware. Essa combinação ajuda a acelerar a detecção de ameaças.

Como os produtos da McAfee podem protegê-lo contra malware evasivo

A McAfee oferece uma nova geração de recursos de segurança criados para combater as mais evasivas e modernas ameaças. Com base em poderosas análises de autoaprendizagem e ferramentas de contenção de aplicativos, as organizações podem revelar ameaças ocultas e bloqueá-las — muito mais rapidamente e com muito menos trabalho.

Essas capacidades são fornecidas através dos seguintes produtos da McAfee:

Real Protect

O Real Protect, parte do McAfee Endpoint Protection, combina análise estática pré-execução e análise comportamental pós-execução para bloquear mais malware do que qualquer solução com base em assinaturas ou somente estática; tudo integrado no ecossistema da McAfee. O Real Protect aplica avançadas técnicas de autoaprendizagem para identificar código malicioso com base em uma avaliação profunda de suas características estáticas (análise pré-execução) e no que ele faz (análise comportamental dinâmica) — tudo isso sem assinaturas. O Real Protect desmascara as mais recentes técnicas de ocultação para revelar as ameaças ocultas, de maneira que o malware de dia zero não tenha onde se esconder.

Contenção dinâmica de aplicativos

A contenção dinâmica de aplicativos (DAC), também parte do McAfee Endpoint Protection, protege "pacientes zero" contra novas infecções por malware de dia zero. Quando um endpoint detecta um arquivo suspeito, a DAC bloqueia imediatamente os comportamentos habituais do malware (como alterar o Registro, gravar em um diretório temporário ou excluir arquivos). Diferentemente de outras técnicas que retêm o arquivo (e o usuário) durante minutos por vez, a DAC permite que o arquivo suspeito seja carregado na memória sem permitir que ele faça determinadas alterações no endpoint ou que ele infecte outros sistemas enquanto está sob suspeita.

O Real Protect e a DAC estão integrados — entre si, com soluções de segurança de terceiros como SPLUNK, Avecto, ForeScout e com o McAfee Endpoint Protection — para oferecer uma defesa multicamada contra as ameaças mais evasivas. Eles capacitam a sua equipe de segurança a enfrentar todos os estágios do ciclo de vida da defesa contra ameaças — detecção, correção e proteção proativa — de uma maneira rápida e automatizada.

O Real Protect e a DAC podem ser aproveitados para:

- Revelar ataques desmascarando as técnicas de ocultação para ver mais ameaças de malware.
- Limitar o impacto de um ataque: contenha, isole e previna danos aos sistemas, seja antes da ocorrência de um ataque ou antes que este possa causar danos irreversíveis.
- Rastrear e adaptar-se: utilize defesas automatizadas e integradas para realizar uma gama mais ampla de operações de segurança sem ter de pensar nelas ou ativá-las manualmente.

Assista em vídeo uma demonstração de contenção de malware evasivo utilizando o Real Protect e a DAC.

Melhores prática de configuração da contenção dinâmica de aplicativos
As regras da DAC na política McAfee Default (padrão) são configuradas para apenas informar e, com isso reduzir os falsos positivos. A proteção adaptável contra ameaças oferece duas políticas de DAC predefinidas adicionais: McAfee Default Balanced e McAfee Default Security. Essas políticas definem regras recomendadas para bloqueio com base no perfil de segurança:

- McAfee Default Balanced oferece um nível básico de proteção e, ao mesmo tempo, minimiza falsos positivos em muitos instaladores e aplicativos não assinados comuns.
- McAfee Default Security proporciona uma proteção mais forte, mas pode produzir falsos positivos mais frequentes em instaladores e aplicativos não assinados.

Avalie o impacto das regras da DAC utilizando a política McAfee Default com regras definidas para reportar. Para determinar se devem ser definidas regras para bloquear, monitore os registros e relatórios. Após coletar a violação da DAC permitida (ID de evento 37280), configure exclusões da DAC ou reputações em nível corporativo antes de impor a politica McAfee Default Balanced.

A DAC pode excluir processos da contenção com base em nome, hash MD5, dados de assinatura e caminho. Se a sua organização assina ferramentas distribuídas internamente, adicione essas assinaturas como exclusões para reduzir os falsos positivos.

As regras da DAC têm controle de vazão, o que limita o número de eventos gerados a um por hora, por regra e por processo. O controle de vazão da DAC rastreia os processos por ID de processo. Quando um processo é reiniciado, o sistema operacional atribui a ele uma nova ID, o que zera o controle de vazão, embora o nome do processo seja o mesmo. Por exemplo, se o Processo A viola a regra A da DAC 100 vezes por hora, você recebe um evento por hora. Se o Processo A for reiniciado durante essa hora, o controle de vazão será zerado para o Processo A e você receberá um outro evento caso ele continue a violar a regra A da DAC. Se o Processo B violar a mesma regra A da DAC, você receberá um segundo evento (com detalhes do Processo B). Leia isto para obter mais informações sobre melhores práticas específicas de regras de DAC definidas pela McAfee.

Execute a ferramenta GetClean da McAfee nas imagens de base de distribuição em sistemas de produção para assegurar que arquivos limpos sejam enviados ao McAfee Global Threat Intelligence (GTI) para serem categorizados. Essa ferramenta garante que o McAfee GTI não forneça um valor de reputação incorreto para os seus arquivos. Para obter mais informações, consulte o Guia de produto do GetClean (PD23191).

McAfee Cloud Threat Detection

Melhore facilmente as proteções da McAfee para condenar malware avançado e expor ameaças evasivas aproveitando o McAfee Cloud Threat Detection (CTD). Obtenha acesso ao McAfee ePO Cloud, ative o McAfee CTD e integre-o com os seus produtos McAfee.

Para usar a capacidade McAfee CTD com os seus produtos de segurança McAfee, siga estas etapas:

- Ative o McAfee CTD no McAfee ePO Cloud.
- Ative o McAfee CTD na interface do seu produto de segurança McAfee e obtenha a chave de provisionamento.
- Use a chave de provisionamento para gerar uma chave de ativação na interface do McAfee ePO Cloud.
- Use a chave de ativação para ativar o seu produto de segurança McAfee.

As instruções detalhadas para obtenção da chave de provisionamento e ativação de um produto variam. Consulte o guia do produto para obter informações detalhadas sobre integração do McAfee CTD com o seu produto McAfee.

Quando os produtos integrados começarem a enviar ao McAfee CTD arquivos para análise, você poderá visualizar suas informações de utilização na página Subscriptions (Assinaturas) do McAfee ePO Cloud.

McAfee Active Response

- O McAfee Active Response foi criado para localizar e responder a ameaças avançadas. Quando utilizado em associação com canais de ameaças, como McAfee GTI, Dell SecureWorks ou ThreatConnect, ameaças evasivas podem ser procuradas e eliminadas antes que tenham a oportunidade de se espalhar.
- Coletores personalizados podem ser utilizados para construir ferramentas específicas para localizar e identificar indicadores de comprometimento associados a aplicativos troianizados.
- Gatilhos e reações podem ser criados pelo usuário para definir ações a serem executadas quando condições específicas forem satisfeitas. Por exemplo, quando hashes ou nomes de arquivo específicos são encontrados, uma ação de exclusão pode ocorrer automaticamente.

Leitura adicional

Neutralize Advanced Threats: Adapt Layered Defenses for Comprehensive Malware Protection (Neutralize ameaças avançadas: adapte defesas em camadas para uma proteção abrangente contra malware)

McAfee Security Advice Center: 10 principais formas de defender-se contra malware e cavalos de Troia

McAfee Endpoint Security: Perguntas frequentes

McAfee™
Together is power.

McAfee LLC
2821 Mission College Blvd.
Santa Clara, CA 95054 USA
www.mcafee.com/br