Resumo de solução

Proteção contra ameaças esteganográficas

A esteganografia — arte e ciência da ocultação de segredos — também pode ser utilizada para ocultar informações no mundo digital. Uma mensagem pode ser escondida dentro de uma imagem, faixa de áudio, clipe de vídeo ou arquivo de texto. Ela pode ser utilizada para fins legítimos, mas a esteganografia é mais frequentemente utilizada por malware.

Para evitar detecção, alguns exemplares de malware utilizam esteganografia digital para esconder seu conteúdo malicioso dentro de um arquivo de "fachada", aparentemente inocente. Essa técnica de evasão tira proveito de que a maioria das assinaturas antimalware detecta conteúdo malicioso no arquivo de configuração do malware. Com a esteganografia, o arquivo de configuração fica incorporado no arquivo de fachada. Além disso, o arquivo esteganográfico resultante pode ser descriptografado na memória principal, reduzindo ainda mais as possibilidades de detecção. Finalmente, é extremamente difícil detectar a presença de informações ocultas, como um arquivo de configuração, atualização de binário ou comando de bot, dentro de um arquivo esteganográfico. Infelizmente, o uso de esteganografia em ataques cibernéticos é fácil de implementar e difícil de detectar.

Políticas e procedimentos para proteção contra ataques esteganográficos

A McAfee recomenda que as organizações sigam as etapas abaixo para se proteger contra ameaças esteganográficas.

- **Reforce os mecanismos de entrega e distribuição de software para se proteger contra ameaças por parte de elementos internos.** É sempre uma boa ideia ter um repositório central de aplicativos corporativos confiáveis do qual os usuários possam fazer download de software aprovado, evitando a prática arriscada de deixar que os usuários façam download de software de fontes desconhecidas que possam conter código esteganográfico.

McAfee™
Together is power.

- **Observe atentamente as imagens.** Com a ajuda de software de edição de imagens, procure indícios de esteganografia, como leves diferenças de coloração nas imagens. Um grande número de cores duplicadas em uma imagem pode ser indício de um ataque esteganográfico.
- **Controle o uso de software de esteganografia.** A presença de software de esteganografia em qualquer sistema corporativo deve ser proibida, a menos que seja necessário para fins de negócios. Distribua esse tipo de software somente em um segmento de rede confinado.
- **Só permita assinaturas confiáveis.** Instale somente aplicativos com assinaturas confiáveis e de fornecedores confiáveis.
- **Configure antimalware para detectar binders.** O software antimalware deve ser configurado para identificar a presença de binders, os quais podem conter imagens esteganográficas.
- **Segmente a rede.** Caso um ataque esteganográfico seja bem-sucedido, arquiteturas de virtualização confiáveis, aliadas a uma segmentação de rede adequada, podem ser úteis para conter uma epidemia porque o processo de inicialização segura e verificável utilizado e o monitoramento contínuo do tráfego de rede ajudam a manter os aplicativos isolados.
- **Monitore o tráfego de saída.** Identifique a presença de ataques esteganográficos bem-sucedidos monitorando o tráfego de saída.

Como os produtos da McAfee podem proteger contra código esteganográfico em ataques de malware

McAfee Endpoint Security

Prevenção de ameaças

Certifique-se de que o McAfee Endpoint Security (ENS) esteja configurado para prevenir quaisquer ameaças conhecidas de malware que possam conter código esteganográfico:

- Mantenha o McAfee ENS completamente atualizado com o patch, a versão do DAT e o mecanismo de varredura mais recentes.
- Certifique-se de que todos os sistemas do seu ambiente estejam protegidos e atualizados.
- Configure a varredura em tempo real (ao acessar) para examinar todos os arquivos, na leitura e na gravação. Nunca desative a varredura na leitura, exceto ao configurar processos de baixo risco.
- As regras de exclusão de varredura devem ser minimizadas e utilizadas somente quando necessário. Em caso de suspeita de malware, certifique-se de desativar temporariamente quaisquer exclusões de varredura. Aprenda a configurar exclusões com o artigo KB88595 da base de conhecimentos.
- Compreenda as implicações de desempenho do uso de configurações de processos de alto risco/padrão/de baixo risco para limitar a exposição a ameaças esteganográficas em ambientes de uso intenso ou nos quais a segurança de hardware seja mínima. Saiba como melhorar o desempenho com o Endpoint Security KB88205.
- Configure o McAfee ENS para usar o recurso de reputação de arquivo McAfee Global Threat Intelligence (GTI). Essa tecnologia ajuda a fechar a lacuna entre ameaças de dia zero e detecções com base em assinaturas. Conheça as configurações recomendadas de reputação de arquivo do McAfee GTI em KB74983, com informações adicionais em KB53735.

- Configure regras de proteção de acesso do McAfee ENS para evitar a criação de arquivos autorun.inf.
- Use regras de proteção de acesso para evitar que ameaças desconhecidas sejam instaladas.

Controle da Web

O módulo de controle de Web do McAfee ENS baseia-se nos serviços de reputação e categorização de Web do McAfee GTI. O software infectado por esteganografia frequentemente se encontra em sites de distribuição de malware.

O módulo de controle de Web do McAfee ENS identifica sites — antes de você visitá-los — que hospedam ou estão infectados por malware, ou que incluem conteúdo inadequado.

Controle de Web da McAfee:

- Indica a segurança relativa dos sites utilizando cores e ícones:
  - Verde = seguro (risco muito baixo ou nenhum)
  - Amarelo = cuidado (algum risco)
  - Vermelho = atenção (risco grave)
  - Cinza = desconhecido (ainda não avaliado; cuidado)
  - McAfee Secure = testado diariamente em busca de vulnerabilidades para hackers
- É facilmente distribuído e configurado através do McAfee ePolicy Orchestrator.
- Oferece uma camada adicional de proteção de endpoint. Pode ser utilizado com Internet Explorer, Firefox e Chrome.
- Utiliza uma proteção antispam eficaz para impedir que e-mails maliciosos entrem nas redes.

Leia mais: Guia de produto do McAfee Endpoint Security - Utilização do controle de Web do ENS

Proteção adaptável contra ameaças

- Deixe que o McAfee Real Protect aplique técnicas de autoaprendizagem para identificar ameaças avançadas com base em suas características aparentes e no que elas podem fazer (análise pré-execução) e também com base no que elas realmente fazem (análise comportamental dinâmica) — tudo isso sem assinaturas. Saiba mais: Proteção adaptável contra ameaças — Real Protect
- Implemente a contenção dinâmica de aplicativos da McAfee e siga as melhores práticas recomendadas. Leia mais: KB87843.

McAfee VirusScan Enterprise

Os clientes que ainda não distribuíram o McAfee ENS mais recente devem assegurar que o McAfee VirusScan Enterprise (VSE) esteja configurado para prevenir quaisquer ameaças conhecidas de malware que possam conter código esteganográfico:

- Mantenha o McAfee VSE completamente atualizado com o patch, a versão do DAT e o mecanismo de varredura mais recentes.
- Certifique-se de que todos os sistemas do seu ambiente estejam protegidos e atualizados.
- Configure a varredura em tempo real (ao acessar) para examinar todos os arquivos, na leitura e na gravação. Nunca desative a varredura na leitura, exceto ao configurar processos de baixo risco.

- As regras de exclusão de varredura devem ser minimizadas e utilizadas somente quando necessário. Em caso de suspeita de malware, certifique-se de desativar temporariamente quaisquer exclusões de varredura. Aprenda a configurar exclusões com o artigo KB50998 da base de conhecimentos.
- Em ambientes de uso intenso ou nos quais a segurança de hardware seja mínima, use configurações para alto risco/padrão/processos de baixo risco para limitar a exposição a ameaças esteganográficas. Entenda esse recurso em KB55139 e aprenda a configurá-lo em KB58692.
- Configure o McAfee VSE para usar o recurso de reputação de arquivo McAfee Global Threat Intelligence (GTI). Essa tecnologia ajuda a fechar a lacuna entre ameaças de dia zero e detecções com base em assinaturas. Conheça as configurações recomendadas de reputação de arquivo do McAfee GTI em KB74983, com informações adicionais em KB53735.
- Configure regras de proteção de acesso do McAfee VSE para evitar a criação de arquivos autorun.inf.
- Use regras de proteção de acesso para evitar que ameaças desconhecidas sejam instaladas.

McAfee Application Control
O McAfee Application Control é uma maneira eficaz de bloquear código e aplicativos não autorizados, resultantes de ataques esteganográficos, em servidores, desktops corporativos e dispositivos de função fixa. O McAfee Application Control previne o comprometimento de arquivos e impede que os infectadores de arquivos se espalhem pela rede.

O McAfee Application Control ajuda a proteger duas áreas principais:

- **Proteção com base em arquivos:** defesa contra ataques com base em arquivos, característicos das ameaças esteganográficas. Esses ataques podem tentar executar novos aplicativos ou modificar os aplicativos atuais.
- **Proteção de memória:** defesa contra ataques com base em memória, os quais podem ocorrer pela Internet, pela rede ou de forma local, como resultado da execução de arquivos.

Proteção com base em arquivos
Os aplicativos que não constam na lista branca não estão autorizados nem protegidos. Por outro lado, os itens da lista branca estão autorizados e protegidos. Se um item não autorizado for introduzido em um endpoint (por exemplo, por meio de um download, acesso pela rede ou de forma local, via pen drive ou CD), ele poderá ser copiado para o endpoint ou modificado e movido de uma pasta para outra no endpoint, mas em momento algum poderá ser executado. Veja a seguir exemplos desses tipos de eventos.

Execução negada	Um aplicativo que não consta na lista branca tenta ser executado, mas é impedido de fazê-lo pelo McAfee Application Control.
Impedida instalação de ActiveX	O McAfee Application Control impede tentativas de instalação de controles ActiveX não autorizados.

Se um processo não autorizado (por exemplo, oriundo da execução de um arquivo malicioso em um endpoint remoto) ou um usuário não autorizado tentar modificar, renomear, mover ou excluir um arquivo incluído na lista branca e, portanto, protegido, o McAfee Application Control bloqueará essa modificação. Veja a seguir exemplos desses tipos de eventos.

Gravação do arquivo negada	O McAfee Application Control impede tentativas de modificação de um aplicativo da lista branca por parte de um processo não autorizado.
Impedida a modificação do pacote	O McAfee Application Control impede aplicativos que usam um pacote instalador com base em MSI de instalar, modificar ou remover utilizando um mecanismo não autorizado.

Leia mais: Melhores práticas com o McAfee Application Control

McAfee Advanced Threat Defense

O McAfee Advanced Threat Defense (ATD) detecta compactadores furtivos e altamente sofisticados, cargas criptografadas e malware de dia zero com uma abordagem inovadora e em camadas. Ele combina defesas automatizadas baseadas em assinaturas antimalware, reputação e emulação em tempo real a código estático e avançado e análise dinâmica de malware (sandboxing) para analisar o comportamento do malware.

Leia mais: Perguntas frequentes sobre o McAfee Advanced Threat Defense

Para leitura adicional

McAfee Security Advice Center: Proteção contra phishing

Dashboard do cenário de ameaças: O kit de exploração Sundown foi atualizado no final de 2016 e, segundo se descobriu, utilizava esteganografia para ocultar código de exploração.

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