Resumo de solução

Software legítimo “troianizado”

Evite infecções e limite a propagação com os produtos da Intel® Security

Os mecanismos utilizados para distribuição de software pela Internet podem ser convertidos em vetores de ataque de malware e vírus. Há uma nítida evolução entre o binder (agregador) malicioso original, exposto há uma década, e a distribuição sofisticada de software legítimo que é “troianizado” antes ou durante a fase de distribuição.

Independentemente da sofisticação do cavalo de Troia, as etapas fundamentais são as mesmas:

- Transformar o software em uma arma: inserir malware em um aplicativo entregável.
- Entrega: transmitir o software troianizado não detectado para o alvo.
- Exploração: acionar o código do cavalo de Troia e tentar permanecer não detectado.
- Instalação: estabelecer uma presença persistente e tentar se movimentar lateralmente.

A técnica de ataque mais recente baseia-se em um sofisticado mecanismo direto que injeta código em um download legítimo de maneira a permanecer não detectado. O princípio do ataque é mesclar o aplicativo original e o código malicioso.

Essa técnica de ataque pode utilizar dois componentes para localizar um ponto de entrada viável no alvo: um “ouvinte” que capture e modifique a solicitação de download HTTP e um binder que infecte e distribua os binários.

Os algoritmos atuais distribuem rotinas de infecção por malware e ataques de redirecionamento de rede sem modificar o código do aplicativo. Isso abre as portas para o uso de software comercial ou de código aberto como arma, podendo incluir arquivos executáveis com uma assinatura incorporada. O ataque será bem-sucedido se a assinatura não for verificada automática e completamente antes de qualquer tentativa de execução inicial.

Uma vez iniciado o aplicativo troianizado no alvo, um processo do binder cria seu próprio arquivo para executáveis incorporados adicionais, nos quais todo o código injetado é reconstruído para execução adicional, contornando todos os controles de segurança. Como o aplicativo original permanece intacto, o malware pode ser agregado a qualquer arquivo, com qualquer assinatura, e ainda assim ter êxito.

intel Security

Políticas e procedimentos

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

- Use uma rede privada virtual (VPN) ao se conectar a uma rede não confiável. Os administradores devem manter o software de segurança atualizado e contar com indicadores fortes de confiança em vez dos que podem ser forjados em um ataque. Os aplicativos devem ser assinados e verificados com uma cadeia de confiança. Análises forenses devem incluir correlação de hashes com fontes confiáveis.
- O software de segurança deve incluir análise dinâmica para sinalizar ações espúrias, independentemente de inspeções de binários iniciais, devido aos limites da varredura estática. Monitoramento comportamental, reputação de Web e de IP, varredura de memória e contenção de aplicativos são componentes valiosos de uma solução completa.
- Downloads de fornecedores devem ocorrem via conexões seguras e todo o código deve ser assinado. Isso reduz consideravelmente os ataques de interceptação. Os fornecedores de software devem incluir autovalidação em seus aplicativos, auditar regularmente seu código, utilizar ferramentas de análise estática de código e realizar avaliações independentes. É sempre bom ter um repositório central de aplicativos corporativos confiáveis e só permitir que os usuários façam download de instaladores aprovados desse repositório.
- O software antimalware deve ser configurado para identificar a presença de binders.
- Aplicativos de detecção e prevenção de intrusões no host devem ser utilizados para inspeções de pacotes que possam identificar cargas virais maliciosas.
- Utilize somente arquiteturas de virtualização confiáveis, combinadas com segmentação de rede adequada. As arquiteturas de virtualização confiáveis utilizam um processo de inicialização seguro e verificável. Uma segmentação de rede adequada pode monitorar o tráfego e manter os aplicativos isolados na eventualidade de uma exploração bem-sucedida. Essa combinação também previne a movimentação lateral do malware.
- Identifique a presença do malware entregue pelo software troianizado monitorando o tráfego de saída. É possível expor máquinas infectadas para remediação adicional pelo tráfego que estas tentam enviar à Internet.

Intel Security

Os produtos da Intel Security podem identificar software legítimo troianizado, identificar e bloquear ameaças de malware incorporadas, expor comprometimentos e responder rapidamente:

McAfee VirusScan® Enterprise 8.8 ou McAfee Endpoint Security 10

- Mantenha os arquivos DAT atualizados.
- Certifique-se de que o McAfee Global Threat Intelligence (McAfee GTI) esteja em uso; ele reconhece mais de 600 milhões de assinaturas de malware exclusivas.
- Crie regras de proteção de acesso para evitar a instalação e cargas virais de malware:
  - Consulte os artigos da base de conhecimentos sobre regras de proteção de acesso: KB81095 e KB54812.
  - Consulte as práticas recomendadas de configuração do McAfee VirusScan 8.8 Enterprise: PD22940.
  - Consulte as práticas recomendadas de configuração do McAfee Endpoint Security: KB86704.

McAfee Host Intrusion Prevention

- O McAfee Host Intrusion Prevention pode ajudar a prevenir a disseminação de malware. Utilizando assinaturas de IPS personalizadas, você pode criar regras para prevenir operações de arquivo geradas pelo malware (criação, gravação, execução, leitura, etc.).
- Ative a assinatura 3894 do McAfee Host Intrusion Prevention, Access Protection—Prevent svchost.exe executing non-Windows executables (Proteção de acesso — Impedir o svchost.exe de executar executáveis que não sejam do Windows).
- Ative as assinaturas 6010 e 6011 do McAfee Host Intrusion Prevention para bloquear injeções imediatamente.
- Dois tipos de sub-regra possibilitam isso:

1. Crie uma assinatura de IPS personalizada utilizando o mecanismo Files e uma sub-regra com os seguintes critérios:
   - Name: <insira o nome>
   - Rule type: Files
   - Operations: Create, Execute, Read, Write
   - Parameters: Include - Files - <caminho/nome do arquivo do malware>
     - O nome do arquivo precisa incluir um caminho. Se quiser especificar o caminho com caracteres curinga, comece o nome do arquivo com "**\" ou, se desejar substituir a letra da unidade por um caractere curinga, use "?:\" (por exemplo: "**\nomedoarquivo.exe" ou "?:\nomedoarquivo.exe").
     - Não é possível utilizar hashes MD5 com o parâmetro "Files"; somente caminho/nome do arquivo.
     - Você pode utilizar o tipo de unidade para limitar o caminho a uma unidade específica (por exemplo, disco rígido, CD-ROM, USB, rede, disquete).
   - Executables: pode ser deixado em branco, a não ser que você queira limitar a assinatura a processos específicos que realizem a operação de arquivo (por exemplo, explorer.exe, cmd.exe, etc.).
2. Crie uma assinatura de IPS personalizada utilizando o mecanismo Program e uma sub-regra com os seguintes critérios:
   - Name: <insira o nome>
   - Rule type: Program
   - Operations: Run target executable
   - Parameters: <deixar em branco>
   - Executables: pode ser deixado em branco, a não ser que você queira limitar a assinatura a um processo específico, como o executável de origem (por exemplo, caso você queira impedir que explorer.exe execute o executável especificado em Target Executable (por exemplo, notepad.exe)).
   - Target Executables: defina as propriedades do executável cuja execução você deseja impedir (por exemplo, se você deseja bloquear a execução do notepad.exe, especifique o caminho/nome do arquivo do executável). O executável pode ser definido utilizando-se um ou mais dos critérios (descrição do arquivo, nome do arquivo, impressão digital, assinador).

McAfee SiteAdvisor® Enterprise ou McAfee Web Protection

- Utilize as reputações dos sites para evitar aqueles que distribuem software troianizado ou para advertir os usuários sobre tais sites.

McAfee Threat Intelligence Exchange e McAfee Advanced Threat Defense

- Configuração de política do McAfee Threat Intelligence Exchange:
  - Iniciar com o modo de observação: conforme forem descobertos endpoints com processos suspeitos, usar tags do sistema para aplicar políticas de imposição do Threat Intelligence Exchange.
  - Limpar caso a reputação seja known malicious (sabidamente malicioso).
  - Bloquear caso a reputação seja most likely malicious (muito provavelmente malicioso) (bloquear unknown (desconhecido) seria uma proteção melhor, mas poderia aumentar demasiadamente a carga de trabalho administrativo inicial).
  - Submit files to McAfee Advanced Threat Defense (Enviar arquivos para McAfee Advanced Threat Defense) se o nível de reputação for unknown (desconhecido) ou abaixo.
  - Política do servidor McAfee Threat Intelligence Exchange: aceite reputações do McAfee Advanced Threat Defense para arquivos ainda não vistos pelo McAfee Threat Intelligence Exchange.
- Intervenção manual no McAfee Threat Intelligence Exchange:
  - Imposição de reputação de arquivos (sujeita ao modo de operação). Most likely malicious (Muito provavelmente malicioso): limpar/excluir.
  - Might be malicious (Provavelmente malicioso): bloquear.
- A reputação corporativa (organizacional) pode prevalecer sobre o McAfee GTI:
  - Você pode optar por bloquear um processo indesejado, por exemplo, um aplicativo incompatível ou vulnerável.
  - Marque o arquivo como might be malicious (provavelmente malicioso).
- Ou opte por permitir um processo indesejado para teste:
  - Marque o arquivo como might be trusted (provavelmente confiável).

McAfee Advanced Threat Defense

- Capacidades de detecção incluídas:
  - Detecção com base em assinaturas: as assinaturas mantidas pelo McAfee Labs chegam a mais de 600 milhões.
  - Detecção com base em reputação: McAfee GTI
  - Análise estática e emulação em tempo real: utilizada para detecção sem assinaturas
  - Regras YARA personalizadas
  - Análise completa de código estático: realiza engenharia reversa do código do arquivo para determinar atributos e conjuntos de funções e analisar completamente o código fonte sem executá-lo.
  - Análise dinâmica em área restrita (sandbox)
- Crie perfis do Analizer onde o software troianizado provavelmente será executado:
  - Sistemas operacionais comuns, Windows 7, Windows 8, Windows 10
  - Instalar aplicativos do Windows (Word, Excel) e ativar macros.
- Ofereça acesso à Internet ao perfil do analisador:
  - Muitas amostras executam um script de um documento Microsoft que cria uma conexão de saída e que pode ativar o malware. Oferecer conexão à Internet a um perfil do analisador aumenta as taxas de detecção.

McAfee Network Security Platform

- O McAfee Network Security Platform tem assinaturas em suas políticas padrão para detectar a rede TOR e que podem ser utilizadas para transferir arquivos associados a malware.
- Integração com o McAfee Advanced Threat Defense para novas variantes de ataques:
  - Configure a integração do McAfee Advanced Threat Defense na "política de malware avançado".
  - Configure o McAfee Network Security Platform para enviar arquivos .exe, do Microsoft Office, Java Archive e PDF para inspeção pelo McAfee Advanced Threat Protection.
  - Verifique se a configuração do McAfee Advanced Threat Protection está aplicada em nível de sensor.
- Atualize regras de detecção de retorno de chamada (para combater redes de bots).

McAfee Web Gateway

- Ative a inspeção do McAfee Gateway Anti-Malware.
- Ative o GTI para reputação de URL e de arquivo.
- Integração com o McAfee Advanced Threat Defense para análises em área restrita (sandbox) e detecção de ameaças de dia zero.

VirusTotal Convicter: intervenção automatizada

- O Convicter é um script Python disparado pelo sistema de resposta automatizada do McAfee ePolicy Orchestrator® (McAfee ePO) para fazer referência cruzada entre o VirusTotal e qualquer arquivo gerador de um evento de ameaça do McAfee Threat Intelligence Exchange.
- É possível alterar o script para fazer referência a outros intercâmbios de inteligência contra ameaças, como o GetSusp.
- Se o limite para confiança na comunidade for atingido, o script definirá automaticamente a reputação corporativa. Limite de condenação sugerido: 30% dos fornecedores e dois fornecedores principais devem concordar.
- Filtrar: Target file name does not contain (o nome do arquivo de destino não deve conter): McAfeeTestSample.exe.
- Esta é uma ferramenta gratuita, com suporte da comunidade (sem suporte pela Intel Security).

McAfee Endpoint Threat Defense and Response

- O McAfee Endpoint Threat Defense and Response encontra e responde a ameaças avançadas. Quando utilizado em associação com canais de ameaças do McAfee Labs, Dell SecureWorks ou ThreatConnect, ameaças novas podem ser procuradas e eliminadas antes que tenham a oportunidade de se espalhar.
- Coletores personalizados permitem construir ferramentas específicas para localizar e identificar indicadores de comprometimento associados a aplicativos troianizados.
- Gatilhos e reações são construídos pelo usuário para definir ações quando condições específicas são satisfeitas. Por exemplo, quando hashes ou nomes de arquivo são encontrados, uma ação de exclusão pode ser executada automaticamente.

Para leitura adicional

Best Practices for how to use McAfee Host Intrusion Prevention rules for a malware outbreak (Práticas recomendadas sobre como utilizar regras do McAfee Host Intrusion Prevention em uma epidemia de malware): KB84507

Esse artigo da base de conhecimentos oferece aos clientes informações detalhadas sobre o Trojan-Powelike: infecção e vetores de propagação: PD25582

SIEM Orchestration: Orchestration Triggers Signs of Malware Infection and Anomalous Behaviors (Orquestração de SIEM: a orquestração é acionada em caso de indícios de infecção por malware e comportamentos anômalos): PD24830

White paper: *Segurança além de assinaturas*

FAQs for Network Security Platform: Advanced Malware Detection (Perguntas frequentes sobre o Network Security Platform: detecção de malware avançado): KB75269

Guia de produto do McAfee Web Gateway: filtragem da Web: PD26339

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