Resumo de solução

Como deter cavalos de Troia backdoor

A ferramenta de administração remota (RAT) Adwind é um cavalo de Troia de backdoor baseado em Java que visa várias plataformas compatíveis com arquivos Java. O Adwind não explora vulnerabilidade alguma. Normalmente, para que uma infecção ocorra, o usuário precisa executar o malware clicando duas vezes em um arquivo .jar recebido como anexo de e-mail ou abrir um documento do Microsoft Word infectado. A infecção começará se o usuário tiver o Java Runtime Environment instalado. Uma vez que o arquivo .jar malicioso tenha sido executado com êxito no sistema-alvo, o malware instala-se sorrateiramente e conecta-se a um servidor remoto através de uma porta pré-configurada para receber comandos do atacante remoto e realizar mais atividades maliciosas.

Uma breve história

O Adwind é uma evolução da RAT Frutas. Frutas é uma RAT baseada em Java descoberta no início de 2013 e amplamente utilizada em campanhas de phishing por e-mail contra destacadas empresas de telecomunicações, mineração, governamentais e financeiras na Europa e na Ásia.

Desde o início do primeiro trimestre de 2015, o McAfee® Labs observa um aumento significativo em envios de arquivos .jar identificados como Adwind.

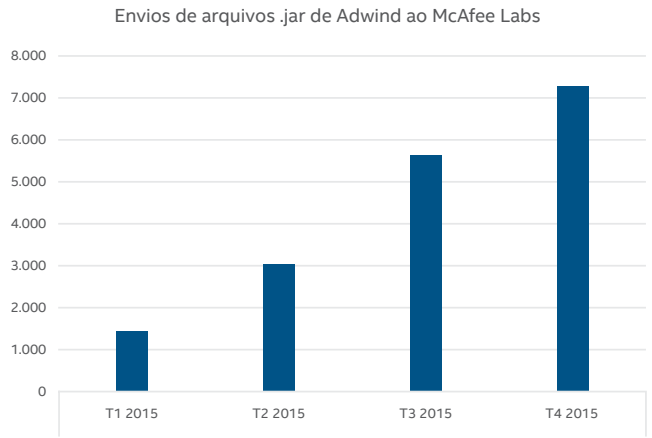

Figura 1. O número de envios de arquivos .jar de Adwind para o McAfee Labs cresceu de 1.388 no primeiro trimestre de 2015 para 7.295 no quarto trimestre de 2015, um aumento de 426%.

intel Security

Cadeia de infecção

O Adwind costuma ser propagado por meio de campanhas de spam que empregam anexos de e-mail contendo malware, páginas da Web comprometidas e downloads de passagem. Seu mecanismo de distribuição evoluiu. Antes, as campanhas de spam duravam dias ou semanas e seus e-mails tinham o mesmo assunto e o mesmo anexo. Essa consistência ajudava os fornecedores de segurança a detectar e a combater rapidamente as ameaças. Agora, porém, as campanhas de spam têm vida curta, com assuntos frequentemente variáveis e anexos cuidadosamente criados, o que permite ao Adwind evitar detecções.

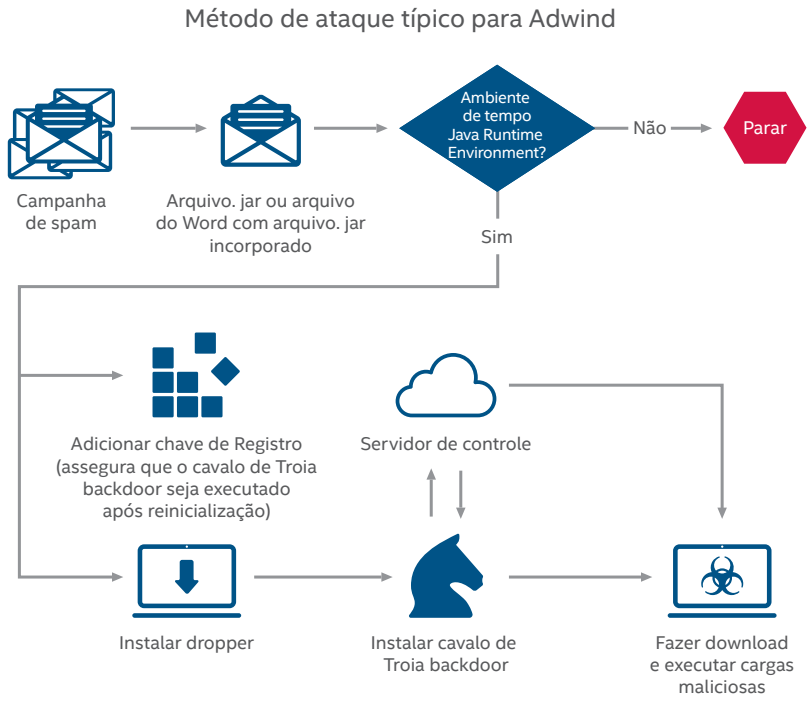

Figura 2. A cadeia de infecção do Adwind.

Vimos que o Adwind, depois que consegue infectar um sistema, registra pressionamentos de teclas, modifica e exclui arquivos, faz download e executa mais malware, captura telas, acessa a câmera do sistema, assume o controle do mouse e do teclado, atualiza-se e muito mais.

Como a Intel Security ajuda na proteção contra o Adwind e outros cavalos de Troia de backdoor

A tecnologia da Intel Security pode ajudar na proteção contra cavalos de Troia de backdoor, como o Adwind. Eis alguns dos produtos que podem ajudar a deter esse tipo de ataque.

McAfee® Threat Intelligence Exchange

É imprescindível 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 cavalos de Troia de backdoor, graças à sua visibilidade sobre ameaças imediatas, como aplicativos ou arquivos desconhecidos em execução no ambiente.

- **Informações abrangentes contra ameaças:** personalize facilmente informações abrangentes contra ameaças obtidas de fontes de dados de inteligência global contra ameaças. Essas fontes podem ser o **McAfee Global Threat Intelligence** (McAfee GTI) ou feeds de terceiros, com informações locais contra ameaças obtidas de dados de eventos históricos e em tempo real dos 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 poderosas capacidades de imposição de políticas e gerenciamento central do produto.
- **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:** importe hashes de arquivos notoriamente nocivos e imunize o seu ambiente contra essas ameaças conhecidas através da imposição de políticas. Caso algum dos indicadores de comprometimento seja acionado no ambiente, o McAfee Threat Intelligence Exchange pode eliminar todos os processos e aplicativos associados aos indicadores de comprometimento.

McAfee Advanced Threat Defense

O **McAfee Advanced Threat Defense** é um produto para detecção de malware em múltiplas camadas que combina vários mecanismos de inspeção. Os mecanismos fazem inspeção com base em assinaturas e em reputação, emulação em tempo real, análise completa de código estático e análise dinâmica em área restrita (sandbox) de objetos suspeitos para proteção contra o malware que inicialmente instala um binário no sistema-alvo.

- **Detecção com base em assinatura:** detecta vírus, worms, spyware, bots, cavalos de Troia, estouros de buffer e ataques combinados. A abrangente base de conhecimentos é criada e mantida pelo McAfee Labs.
- **Detecção com base em reputação:** consulta a reputação dos arquivos utilizando o McAfee GTI para detectar ameaças emergentes recém-surgidas.
- **Análise estática e emulação em tempo real:** oferece emulação e análise estática em tempo real para localizar rapidamente cavalos de Troia de backdoor e ameaças de dia zero não identificados por reputação ou técnicas com base em assinaturas.
- **Análise completa de código estático:** faz a engenharia reversa do código do arquivo para determinar todos os seus atributos e conjuntos de instruções, e analisa completamente o código-fonte sem execução. Seus recursos de descompactação abrangentes abrem todos os tipos de arquivos compactados para a análise completa e classificação do malware, permitindo que a sua empresa entenda a ameaça representada pelo malware em questão.
- **Análise dinâmica em área restrita (sandbox):** para os arquivos cuja segurança não possa ser determinada pelos mecanismos de inspeção precedentes, o McAfee Advanced Threat Defense pode executar o código do arquivo em um ambiente de tempo de execução virtual e observar o comportamento resultante. Ambientes virtuais podem ser configurados para corresponder aos ambientes host. O McAfee Advanced Threat Defense é compatível com imagens personalizadas dos sistemas operacionais Microsoft Windows XP (32 e 64 bits), Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows Server 2003, Windows Server 2008 (64 bits) e Android.

McAfee Network Security Platform

O **McAfee Network Security Platform** é um produto de segurança inteligente e exclusivo que descobre e bloqueia ameaças sofisticadas na rede. Com técnicas avançadas de emulação e detecção, este produto vai além da simples correspondência de padrões para defender seu sistema contra ataques indetectáveis com extrema precisão. Nossa abordagem aberta e integrada ao gerenciamento da segurança simplifica as operações de segurança combinando os canais em tempo real do McAfee GTI com dados contextuais detalhados sobre usuários, dispositivos e aplicativos para respostas rápidas e precisas a ataques via rede.

- **Defesas não baseadas em assinaturas:** ameaças avançadas e desconhecidas, como malware indetectável, ameaças persistentes avançadas (APTs), bots e ataques de dia zero frequentemente contornam defesas com base em assinaturas. O McAfee Network Security Platform conta com múltiplos mecanismos avançados que dispensam assinaturas para a proteção contra essas ameaças avançadas e desconhecidas. A detecção sem assinatura analisa comportamentos de conteúdos da Web, arquivos PDF, arquivos Flash e JavaScript em tempo real utilizando emulação.
- **McAfee Endpoint Intelligence Agent:** o McAfee Network Security Platform oferece correlação em tempo real de tráfego de endpoint por fluxo. O agente combina análise comportamental de fluxos de tráfego de rede com múltiplas fontes de inteligência de reputação. Essa tecnologia aproveita informações da rede e de cada host Windows para revelar relacionamentos entre executáveis de endpoint e fluxos de tráfego de rede, possibilitando identificar conexões de rede e executáveis maliciosos em tempo real. O agente incorpora um contexto de processo detalhado dos ataques, bloqueia comunicações maliciosas, evita a disseminação de malware avançado e, finalmente, coloca em quarentena e corrige sistemas host compometidos.

McAfee Web Gateway

Anúncios enganosos, downloads de passagem e URLs maliciosos incorporados em e-mails de phishing são alguns dos principais métodos de ataque utilizados para entregar cavalos de Troia de backdoor. O **McAfee Web Gateway** é um produto sólido que reforça a proteção da sua empresa contra esse tipo de ameaça.

- **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 Gateway Anti-Malware Engine inspeciona os arquivos e impede que os usuários façam download se tais arquivos são maliciosos.
- **Integração com o 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 conhecidos como maliciosos ou sites notórios por atuar como servidores de controle.

Além desses produtos da Intel Security, recomendamos uma classe adicional de tecnologia de segurança.

- **Segurança de gateway de e-mail:** a maioria dos cavalos de Troia de backdoor entra nos sistemas através de um anexo em uma mensagem de e-mail, portanto, um produto robusto de segurança de gateway de e-mail que faz varredura de todos os anexos quanto à presença de malware proporciona uma defesa sólida contra esse tipo de ataque.

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