Resumo de solução

Abuso de confiança

Aproveitando-se da confiança dos outros

O ditado “confiança não se dá, se conquista” soa bem verdadeiro; todos nós já vimos exemplos como esse na vida. Por outro lado, o que leva anos para se conquistar pode ser destruído em questão de segundos. A confiança nunca se definiu em um modelo estático, e tal característica tornou-se ainda mais evidente com a população mundial cada vez mais dependente da Internet.

O que é abuso de confiança?

A exploração da confiança é discutida em detalhes no **Relatório do McAfee Labs sobre ameaças: novembro de 2014**. No mundo on-line, partimos do pressuposto de que tudo que vemos é confiável, seja um aplicativo transferido por download para um dispositivo móvel, um anúncio aparentemente inofensivo em um site popular ou um e-mail de uma empresa com a qual trabalhamos. Os atacantes tiram proveito do princípio da confiança de diversas maneiras, tendo como seu principal objetivo a exploração de vítimas incautas. Seguem abaixo alguns tipos de ataques discutidos no relatório:

- **Anúncios enganosos:** quando os anúncios inofensivos no site de uma empresa são, na verdade, a origem do ataque a consumidores incautos, estes passam a questionar se sua confiança é justificada. **Redes de anúncios maliciosos, como a “Kyle and Stan”** distribuem malware através de “malvertisements” (malware disfarçados de anúncios) por meio de sites, como amazon.com, youtube.com e **em importantes redes de anúncio, como DoubleClick e Zedo**.
- **Malware assinado:** uma tática cada vez mais comum praticada pelos autores de malware é adquirir certificados de uma autoridade de certificação (CA) e tentar pegar carona na confiança de empresas estabelecidas no mercado ou fingir ser uma empresa verdadeira. Os atacantes exploram a confiança intrínseca que depositamos nas CAs. Recentemente, uma campanha maliciosa distribuiu variantes assinadas do cavalo de Troia CryptoWall por meio da rede de anúncios Zedo, o que teria **afetado usuários dos sites mais visitados segundo a classificação do Alexa**. A assinatura digital emitida para a “Trend” provavelmente estava tentando se passar pelo fornecedor de produtos de segurança Trend Micro, sendo este um exemplo perfeito de exploração da inocência por associação.
- **Imitação de aplicativos:** as marcas comerciais gastam uma quantidade considerável de tempo e energia para proteger seus clientes de produtos falsificados que se aproveitam da confiança consolidada da marca perante seus consumidores. Com aplicativos que oferecem funções que ultrapassam o mundo digital, não nos surpreende perceber que atacantes ousados têm recorrido à criação de aplicativos que são cópias baratas de programas legítimos e, em geral, populares.

intel Security

No último trimestre, a McAfee observou golpistas tentando distribuir um aplicativo que parecia ser o Adobe Flash Player 11. De acordo com a contagem de downloads da loja Google Play e da telemetria de detecção feita pelo McAfee Mobile Security, os golpistas tiveram êxito em enganar os usuários para que fizessem o download de sua cópia pirata.

- **Sideload de DLL:** os atacantes sabem que o código malicioso terá maiores chances de sucesso se conseguir pegar carona em um aplicativo confiável. O malware tem se aproveitado desse fator por vários anos, utilizando uma técnica de ataque conhecida como sideload de DLL. Essa técnica consiste em executar um aplicativo legítimo que executa código de uma DLL externa. Os atacantes fazem com que sua carga assuma o papel da DLL externa, fazendo com que o aplicativo limpo execute o código malicioso.

  No terceiro trimestre, o McAfee Labs observou ataques explorando o aplicativo Google Updater. Novas variantes da família do malware PlugX assumem o papel do goopdate.dll importado, mas o PlugX dá um passo além para ocultar suas ações. O módulo goopdate.dll não passa de um intermediário que lê o conteúdo de um arquivo de dados criptografado, (goopdate.dll.map), descriptografa-o na memória e transfere o controle da execução para esse código malicioso.

- **Sistema operacional e software de rede:** existem vários exemplos de ataques que abusam da confiança intrínseca e estabelecida entre os sistemas operacionais e software de rede. Alguns ataques se aproveitam do software que estabelece conexões seguras na Internet. Aplicativos insuspeitos confiam nas conexões transmitidas pelo sistema operacional que, por sua vez, confia no software de rede que supostamente estabeleceu conexões seguras. Outros ataques exploram vulnerabilidades intrínsecas aos sistemas operacionais ou software de rede. Muitas vezes, esses ataques se aproveitam de software de código aberto incorporado na pilha do sistema operacional ou do software de rede.

  A BERserk é uma vulnerabilidade de falsificação de assinatura **divulgada recentemente** que subverte a confiança de sistemas operacionais e software de rede. A BERserk permite que pessoas maliciosas realizem ataques de interceptação, possibilitando que falsifiquem assinaturas RSA e ignorem a autenticação a sites que usam SSL/TLS.

Soluções da McAfee

As tecnologias de segurança da McAfee podem ajudar você a se proteger contra ataques que buscam abusar da confiança que a sua empresa tem em suas operações cotidianas. Seguem abaixo alguns produtos da McAfee que permitem à sua empresa assegurar que seu modelo de confiança não seja explorado por supostos atacantes.

McAfee Application Control

É fundamental proteger a sua empresa e seus aplicativos legítimos contra códigos maliciosos, como a BERserk. O **McAfee Application Control** permite que a sua empresa controle quais aplicativos estão autorizados a ser executados no seu ambiente através de listas brancas dinâmicas e políticas de imposição para endpoints tanto conectados quanto desconectados.

- **Listas brancas dinâmicas:** permitem que sua organização gerencie de forma eficiente os aplicativos relacionados em listas brancas, elaborando tais listas automaticamente conforme os sistemas são corrigidos e atualizados. O McAfee Application Control reduz sua exposição à BERserk ao impedir a execução de aplicativos que invocam o código vulnerável de verificação de assinatura RSA.

- **Reputação de arquivos:** a integração com o McAfee Global Threat Intelligence permite que o McAfee Application Control consulte canais em tempo real de tipos de arquivos válidos conhecidos, inválidos e desconhecidos, ajudando a sua empresa a ficar atenta a vulnerabilidades como a BERserk.
- **Mantenha-se protegido, conectado ou desconectado:** imponha controles a servidores conectados ou desconectados, máquinas virtuais, endpoints e dispositivos fixos, como terminais de ponto de venda.

McAfee Email Gateway

Saber se um e-mail na caixa de entrada de um usuário é inofensivo ou malicioso é uma das principais preocupações das empresas. Os atacantes fazem uso do spear phishing para atrair vítimas incautas para iniciar o comprometimento por meio de malware incorporado ou URLs maliciosos. O **McAfee Email Gateway** oferece proteção contra esses tipos de ataques com diversos recursos:

- **ClickProtect:** elimine ameaças de URLs incorporados em mensagens de e-mail ao fazer varredura dos URLs no momento em que estes são clicados. A inspeção inclui verificação de reputação do URL e emulação proativa do McAfee Gateway Anti-Malware Engine.
- **Integração com o McAfee Advanced Threat Defense:** detecte malware evasivo e sofisticado com código estático avançado e análise dinâmica de arquivos suspeitos anexados ao e-mail, impedindo que arquivos maliciosos sequer alcancem a caixa de entrada.
- **Integração com o McAfee Global Threat Intelligence:** combina informações da rede local com a inteligência de reputação do McAfee Global Threat Intelligence, proporcionando a proteção mais completa disponível contra ameaças de entrada, spam e malware.

McAfee Global Threat Intelligence

O **McAfee Global Threat Intelligence (GTI)** é um abrangente serviço de informações sobre ameaças em tempo real com base na nuvem. Com ele, os produtos da McAfee podem bloquear ameaças cibernéticas em todos os vetores — arquivos, Web, mensagens e rede. Garanta proteção proativa contra abuso de confiança com os recursos abaixo:

- **Reputação de certificados:** consulte canais em tempo real de certificados válidos e inválidos para proteger sua empresa contra ameaças, como o malware assinado, que podem ser distribuídas por redes de anúncios maliciosos.
- **Reputação de arquivos:** proteja-se contra a imitação de aplicativos no desktop e fique atento a aplicativos que podem ser vulneráveis a ataques como BERserk. Consulte canais de arquivos válidos, inválidos e desconhecidos em tempo real para manter-se protegido.
- **Inteligência através da correlação de vetores:** reúna e correlacione dados de todos os principais vetores de ameaça e por todos eles — arquivos, Web, e-mail e rede — para detectar ameaças mistas, como redes de anúncios distribuindo malware assinado, e-mails de spear phishing de fontes aparentemente confiáveis e downloads de passagem hospedados em sites maliciosos ou sites “confiáveis” comprometidos.
- **Security Connected:** integração com outros produtos de segurança da McAfee para proporcionar os dados mais amplos sobre ameaças, a mais minuciosa correlação de dados e a mais completa integração de produtos disponível no momento, para garantir proteção contra ataques que abusam da confiança.

McAfee Vulnerability Manager

Ataques como a BERserk ilustram o cenário de ameaças em constante mudança que afeta o modelo de confiança. Saber se você está em risco e saber a extensão da sua vulnerabilidade a esses novos ataques pode ser uma tarefa assustadora. Aqui estão algumas formas em que o **McAfee Vulnerability Manager**, junto com o **McAfee Asset Manager**, pode ajudar a sua empresa a entender vulnerabilidades como a BERserk, e a tomar as medidas necessárias para corrigi-las de forma efetiva:

- **Varredura abrangente de vulnerabilidades:** o McAfee Vulnerability Manager é um produto independente altamente expansível para descoberta de host, gerenciamento de ativos, avaliação de vulnerabilidade e geração de relatórios sobre qualquer dispositivo conectado à rede. O McAfee Vulnerability Manager busca pela BERserk procurando sistemas que estão executando versões vulneráveis do Firefox, Chrome e outros produtos que invocam o código vulnerável de verificação de assinatura RSA.
- **Personalize varreduras para novas ameaças:** o Foundstone Scripting Language (FSL) Editor pode complementar as verificações predefinidas e atualizações para ameaças de dia zero e vulnerabilidades, como a BERserk, criando verificações e scripts personalizados para avaliar seu ambiente. A partir de 24 de setembro de 2014, o McAfee Vulnerability Manager passa a detectar sistemas vulneráveis à BERserk dentro de suas verificações predefinidas.
- **Geração de relatórios e correção flexíveis:** o McAfee Vulnerability Manager e o McAfee Asset Manager trabalham juntos para oferecer monitoramento automatizado e gerenciamento de varredura, correção, imposição e geração de relatórios. Isso ajuda a evitar demoradas simulações de emergências e processos específicos, a eliminar erros e a proteger mais sistemas de maneira eficiente.
- **Conheça a sua exposição:** o McAfee Asset Manager permite que a sua empresa saiba quais sistemas estão vulneráveis à BERserk pela correlação de varreduras de vulnerabilidade com varreduras de descoberta de host. Poder identificar em tempo real quais sistemas estão executando versões de aplicativos vulneráveis significa perder menos tempo pensando se você está exposto e poder dedicar mais tempo à correção.

McAfee Web Gateway

Anúncios enganosos, downloads de passagem e URLs maliciosos incorporados em URLs confiáveis são apenas alguns dos métodos de ataques usados para abusar da confiança. O **McAfee Web Gateway** reforçará 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 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 se tais arquivos são maliciosos. O McAfee Web Gateway é líder no mercado devido à sua capacidade de bloquear downloads de malware, graças à inspeção excepcional desse mecanismo.
- **Integração com o McAfee GTI:** a reputação de arquivos, reputação na Web e os canais de categorização na Web em tempo real 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 maliciosas.

McAfee SiteAdvisor® Enterprise

É desafiador manter-se um passo à frente do cenário de ameaças em constante mudança, principalmente quando tentamos proteger os usuários on-line contra ameaças, como o abuso de confiança, sem impor políticas rígidas que comprometam a experiência do usuário.

- **Fácil identificação de ameaças, como sites maliciosos que se passam por sites legítimos:** com um sistema de classificação baseado em um intuitivo código de cores, o **McAfee SiteAdvisor Enterprise** oferece uma camada extra de proteção no desktop. O McAfee SiteAdvisor Enterprise impede a conexão com sites maliciosos conhecidos e informa os usuários sobre o perigo.
- **Segurança aprimorada oferecida pelo McAfee GTI:** o McAfee GTI oferece informações de inteligência de ameaças em tempo real para o McAfee SiteAdvisor Enterprise, para que este avalie os sites com base nas informações mais recentes.

McAfee Threat Intelligence Exchange

O abuso de confiança se dá de diversas maneiras; 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 (TIE)** reduz de forma significativa a exposição a ataques graças a sua visibilidade sobre ameaças, como certificados maliciosos descobertos no seu ambiente.

- **Reputação de certificado:** a integração com o McAfee GTI permite que a sua empresa fique protegida em tempo real contra ataques que aproveitam o código malicioso assinado ao consultar canais em tempo real de certificados válidos e inválidos conhecidos. O McAfee TIE pode proteger seus endpoints contra certificados maliciosos através de políticas gerenciadas de maneira centralizada, que podem ser implementadas para proteger endpoints tanto conectados quanto desconectados.
- **Derrote o sideload de DLL, imitações de aplicativos e outros ataques:** uma tecnologia de ponta para a proteção de endpoints determina as decisões de execução de arquivos de acordo com uma lógica relacionada com o contexto do endpoint (atributos de ambiente, arquivo e processo), combinada com as informações coletivas sobre ameaças.
- **Indicadores de comprometimento:** importe hashes de arquivos inválidos conhecidos e certificados maliciosos conhecidos no McAfee TIE para imunizar seu ambiente contra esses arquivos inválidos conhecidos através da imposição de políticas. Se qualquer um dos indicadores de comprometimento (IoCs) é acionado no ambiente, o McAfee TIE pode eliminar todos os processos e aplicativos associados com o IoC.

McAfee VirusScan® Mobile Security

- **Derrote as imitações de aplicativos:** com o respaldo do McAfee GTI, o **McAfee VirusScan Mobile Security** pode derrotar imitações de aplicativos com malware quase em tempo real. Ele consegue detectar o malware em menos de 200 milissegundos sem interromper as operações sem fio ou a conectividade.

Proteger sua empresa contra adversários que buscam tirar proveito desse modelo de confiança dinâmico pode ser uma tarefa assustadora. As tecnologias de segurança da McAfee permitem que sua empresa proteja-se de forma proativa contra ataques que buscam abusar da confiança do usuário.

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