Resumo de solução

Proteção contra malware de macro

No ***Relatório do McAfee® Labs sobre ameaças: novembro de 2015***, examinamos detalhadamente o malware de macro, uma relíquia dos anos 1990 que agora está ressurgindo devido ao uso continuado de macros por empresas, bem como a crescente sofisticação dos ataques de engenharia social que estão propagando malware de macro novo e mais indetectável. Uma macro é um atalho utilizado para automatizar uma tarefa frequentemente executada. Trata-se de um fragmento de código incorporado dentro de um documento — tipicamente um documento do Microsoft Office — sendo normalmente escrito na linguagem de programação Visual Basic for Applications. Quando uma macro é gravada, na verdade se gera um programa em Visual Basic for Applications. Para combater o malware de macro, a Microsoft criou uma etapa com base em permissão, para ativar as macros, que serve como confirmação. Atualmente o Microsoft Office desativa todas as macros por padrão para que a execução de macros não seja possível sem a permissão do usuário. Essa medida esfriou os ânimos dos criadores de malware de macro e as macros maliciosas perderam influência. Contudo, no ano passado, atacantes tiraram proveito de malware de macro novo e mais indetectável, juntamente com engenharia social, para visar empresas persistentemente. O número de novas amostras de malware de macro está em seu nível mais alto em seis anos.

Atualmente, os atacantes de malware de macro aproveitam principalmente anexos de e-mails de phishing, bem como campanhas de spam, páginas da Web comprometidas e downloads de passagem para distribuir seu malware. Essas técnicas são muito mais sofisticadas do que nos anos 1990, quando o malware de macro surgiu pela primeira vez. Tornou-se bastante difícil para os usuários identificar essas campanhas porque elas são direcionadas, duram pouco tempo e contêm anexos cuidadosamente elaborados para evitar detecção.

Apresentamos algumas políticas e procedimentos recomendados para proteção contra ataques de malware de macro:

- Ative as atualizações automáticas do sistema operacional, ou faça download dessas atualizações regularmente para manter os sistemas operacionais corrigidos contra vulnerabilidades conhecidas.
- Use software Microsoft Office atualizado, que tem melhor proteção contra esses tipos de ataques.

intel Security

- Certifique-se de que a configuração padrão de segurança de macro em todos os produtos Microsoft Office esteja definida como alta.
- Configure o software antimalware para examinar automaticamente todos os anexos de e-mail e mensagens instantâneas. Certifique-se de que os programas de e-mail não abram anexos ou processem gráficos automaticamente, e desative o painel de visualização.
- Coloque as configurações de segurança do navegador em nível médio ou superior.
- Tenha muito cuidado ao abrir anexos, principalmente aqueles que vêm com a extensão .doc ou .xls.
- Nunca abra e-mails não solicitados ou anexos inesperados — mesmo que venham de pessoas conhecidas.
- Cuidado com esquemas de phishing com base em spam. Não clique em links de e-mails ou de mensagens instantâneas.
- Monitore pings inesperados para endereços IP como 1.3.1.2 ou 2.2.1.1 de computadores internos.
- Observe que documentos de informações sobre cobrança ou recibos não precisam de macros.
- Tenha cuidado ao lidar com documentos vazios que pedem aos usuários para ativar macros para permitir a visualização do conteúdo.

Como a Intel Security ajuda na proteção contra malware de macro

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 malware de macro. O **McAfee Web Gateway** é um produto sólido que reforça 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.
- **Integração com o McAfee Global Threat Intelligence (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 maliciosos conhecidos ou a sites que usam redes de anúncios maliciosos.

McAfee VirusScan® Enterprise

A detecção e limpeza de malware de macro é simples com o **McAfee VirusScan Enterprise**. O McAfee VirusScan Enterprise utiliza o premiado mecanismo de varredura do McAfee Labs para proteger os seus arquivos contra vírus, worms, rootkits, cavalos de Troia e outras ameaças avançadas. Proteja ainda mais sua empresa com a capacidade do McAfee VirusScan Enterprise de bloquear portas, nomes de arquivos, pastas, diretórios e compartilhamentos de arquivos, além de rastrear e bloquear infecções.

- **Proteção proativa contra ataques**: integra tecnologia antimalware com prevenção de intrusões para proteção contra explorações que utilizam explorações de estouro de buffer direcionadas contra vulnerabilidades nos aplicativos da Microsoft.
- **Detecção e limpeza de malware imbatíveis**: protege contra ameaças, como rootkits e cavalos de Troia, com análise comportamental avançada. Detém o malware utilizando técnicas como bloqueio de portas, nomes de arquivos, pastas/diretórios e compartilhamentos de arquivos, bem como rastreamento e bloqueio de infecções.

- **Segurança em tempo real com integração com o McAfee GTI**: proteção contra ameaças conhecidas e emergentes em todos os vetores de ameaça — arquivos, Web, e-mail e rede — com o suporte da plataforma de inteligência sobre ameaças mais abrangente do mercado.

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. Ao combinar múltiplos mecanismos de inspeção que aplicam inspeções com base em reputação e em assinaturas, emulação em tempo real, análise completa de código estático e análise dinâmica em área restrita (sandbox), o McAfee Advanced Threat Defense não apenas detecta documentos que empregam macros para entregar malware, mas também assegura detecção e proteção contra o malware transferido por download após a execução.

- **Detecção com base em assinaturas**: detecta vírus, worms, spyware, bots, cavalos de Troia, estouros de buffer e ataques combinados. Sua base de conhecimentos abrangente 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 malware de macro 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 acima, 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 (OS) Windows XP SP2 e SP3, Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows Server 2003, Windows Server 2008 (64 bits) e Android.

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 malware de macro, graças à sua visibilidade sobre ameaças imediatas, como aplicativos ou arquivos desconhecidos em execução no ambiente.

- **Inteligência abrangente sobre ameaças**: personalize facilmente informações abrangentes sobre ameaças obtidas de fontes de dados de inteligência global sobre ameaças. Essas fontes podem ser o McAfee GTI ou canais de terceiros, com inteligência local sobre ameaças obtida de dados de eventos históricos e em tempo real fornecidos via 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.

Além desses produtos da Intel Security, recomendamos duas classes adicionais de tecnologias de segurança.

- **Segurança de gateway de e-mail**: a maior parte do malware de macro 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 faça varredura de todos os anexos quanto à presença de malware deve ser parte de uma defesa sólida contra esse tipo de ataque.
- **Firewall**: a tecnologia de firewall é fundamental para qualquer sistema de segurança. Um firewall pode detectar muitas ameaças no perímetro — antes que elas entrem na rede confiável.

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