McAfee
Together is power.

Proteção de dispositivos IoT como defesa contra ataques

O ataque bem-sucedido de negação de serviço distribuída (DDoS) realizado contra a infraestrutura de DNS gerenciada da Dyn em outubro de 2016 foi assunto de uma análise detalhada no *Relatório do McAfee Labs sobre ameaças: abril de 2017*.

O ataque foi realizado utilizando o protocolo DNS, o que torna extremamente difícil para a tecnologia de segurança distinguir o tráfego legítimo do hostil. Para complicar o problema, os tráfegos de ataque ilegítimo e legítimo vêm de milhões de endereços IP do mundo todo.

Esse tipo de ataque DDoS está em alta, alimentado pela mal protegida infraestrutura da Internet das Coisas (IoT). O malware Mirai utilizado durante o ataque à Dyn explorou uma ampla variedade de dispositivos IoT mal protegidos, como gravadores de vídeo, impressoras, câmeras de vigilância, refrigeradores, termostatos, etc. Quando um dispositivo IoT era infectado, o malware espalhava a infecção para outros dispositivos IoT, formando uma "rede de bots" e utilizando seu poder de processamento agregado para executar o ataque DDoS.

Segundo a equipe de segurança da Dyn, dezenas de milhões de dispositivos IoT maliciosos fizeram parte da rede de bots com base no Mirai durante o pico do ataque.

Não há maneira fácil de determinar se um dispositivo de rede foi infectado ou o estágio da infecção, o qual pode variar desde as etapas iniciais de deflagração do código, movimentação lateral ou comunicação com servidores de controle, até o recrutamento da rede de bots para ataques DDoS coordenados. No entanto, você pode seguir recomendações de segurança que ajudam a proteger os seus dispositivos IoT e a sua rede confiável.

Como proteger dispositivos IoT

Os atacantes seguem o caminho de menor resistência para obter controle sobre os dispositivos IoT. Normalmente, através de credenciais fracas. Contudo, eles podem se adaptar a credenciais fortes e a outros controles de segurança. Esse é o padrão que vimos em muitos vetores de ataque.

A McAfee recomenda bloquear explorações conhecidas e futuras manobras semelhantes por parte dos atacantes. Siga estas três etapas para proteger os dispositivos IoT do momento em que são produzidos até serem aposentados:

Proteção de dispositivos IoT

1. Projete dispositivos IoT levando em consideração a segurança.

Os fabricantes de dispositivos IoT precisam incorporar segurança na arquitetura, nas interfaces e nos projetos de seus produtos. Estabeleça e teste capacidades e conceitos básicos de segurança, como compartimentalização de dados e código, comunicação entre partes confiáveis, proteção de dados em uso e estacionários e autenticação de usuários. No futuro, os produtos serão mais poderosos, armazenarão mais dados e terão mais funcionalidades. Isso significa que os produtos devem ser capazes de receber atualizações de segurança, bloqueio de recursos, validação de compilação, aprovação de software e configurações padrão que sigam as melhores práticas do setor.

Tudo começa pelo fabricante; a proteção futura é um trabalho de base. O hardware, o firmware, os sistemas operacionais e o software precisam ser projetados para entrar em um ambiente hostil e sobreviver. Os compradores de dispositivos IoT devem avaliar possíveis compras levando isso em consideração. O fabricante projetou e arquitetou o dispositivo IoT considerando a segurança?

2. Provisione e configure com segurança.

A maioria dos dispositivos IoT requer algum tipo de configuração e provisionamento na instalação. A identidade e a autenticação dos dispositivos são uma parte essencial desse processo de duas etapas. Configurações padrão apropriadas que sigam as melhores práticas de segurança são importantes e devem ser de fácil compreensão para os usuários. As regras não devem permitir senhas padrão e devem exigir que patches e atualizações sejam assinados, que os dados sejam criptografados e que as conexões Web sejam seguras. Para corporações, limitar o acesso à rede, aplicar patches prontamente e só permitir software aprovado contribuem em muito para manter os dispositivos IoT protegidos. Em aparelhos com tais capacidades, a implementação de software de segurança, como antimalware, sistemas de prevenção de intrusões e até mesmo firewalls locais, melhorarão a postura de defesa do dispositivo. A detecção e a telemetria também devem ser configuradas para detectar quando os sistemas estão sob ataque ou se estão funcionando de maneiras não previstas pela organização.

Políticas devem ser estabelecidas para privacidade, retenção de dados, acesso remoto, segurança de chaves e procedimentos revogatórios.

3. Aplique administração e gerenciamento adequados.

No caso de dispositivos pertencentes a consumidores, somente estes têm a palavra final sobre como o dispositivo é gerenciado. Os fabricantes e provedores de serviços on-line desempenham um papel no provisionamento, mas os proprietários devem reter o controle sobre o que os dispositivos farão. Provisionamento não é o mesmo que administração. Por exemplo, na instalação de câmeras domiciliares, faz sentido conectar-se ao fabricante para obter os mais recentes patches e talvez até mesmo configurar um armazenamento em nuvem. Porém, os consumidores não querem que as câmeras domiciliares sejam controladas pelos fabricantes. Os fabricantes não devem ter a capacidade de operar dispositivos sem a anuência dos compradores. Os proprietários devem preservar o poder de ligar e desligar seus produtos e escolher quais serviços on-line devem ser permitidos. Essa capacidade requer identificação e autenticação adequadas do usuário. Permitir uma senha padrão comum não é bom porque qualquer um pode assumir o papel de administrador. Imagine se o Microsoft Windows viesse com uma senha de login padrão em todos os sistemas. Seria um pesadelo em termos de segurança porque muitos usuários nunca mudariam a senha e os atacantes poderiam efetuar login como se fossem os usuários.

Os sistemas IoT precisam primeiro ser capazes de autenticar seus proprietários. A funcionalidade de gerenciamento também precisa ser ampliada para permitir que os proprietários estabeleçam limites, políticas de dados e parâmetros de privacidade que sejam mais restritivos que os de qualquer fornecedor terceiro. Atualizações de segurança assinadas devem ser instaladas automaticamente assim que forem disponibilizadas. Proprietários habilidosos devem poder configurar limites para conexões de entrada e saída, tipos de dados, portas e configurações de segurança. Logs que possam ser enviados a um sistema confiável ou visualizados localmente devem capturar erros, bem como atividades inesperadas e incomuns. Um sistema para notificações de aviso remoto, via e-mail ou mensagens de texto, é um recurso bem-vindo em alguns dispositivos. Finalmente, uma capacidade de redefinição (reset) é necessária em caso de comprometimento irrecuperável ou transferência de propriedade.

Procedimentos e políticas decisivas para proteção de dispositivos IoT

- **Pesquise o histórico de segurança do dispositivo IoT.** Antes de comprar um dispositivo IoT, verifique se ele ou a empresa que o oferece tiveram problemas. Basta uma rápida pesquisa na Internet. Uma pesquisa no site da FTC (Federal Trade Commission) revelará intervenções anteriores. Fazendo pesquisas básicas, você pode constatar que algumas empresas ignoram questões de segurança, enquanto outras são mais proativas.
- **Mantenha atualizado o software de todos os dispositivos IoT.** Essa simples prática recomendada pode eliminar as vulnerabilidades, especialmente as recém-descobertas e em destaque publicamente. Tenha um procedimento implementado para aplicação de patches e verifique se os patches foram aplicados corretamente.
- **Quanto aos dispositivos IoT que não podem ser corrigidos, elimine o risco.** Você pode conseguir isso fazendo uso de listas brancas de aplicativos, as quais bloqueiam sistemas e impedem a execução de programas não aprovados.
- **Segregue os dispositivos IoT das outras partes da rede** utilizando um firewall ou um sistema de prevenção de intrusões. Desative portas ou serviços desnecessários nesses sistemas para reduzir a exposição a possíveis pontos de infecção. A Mirai explora portas não usadas.
- **Use senhas fortes e diferentes do padrão.** Senhas padrão ou fracas são a principal ameaça aos dispositivos IoT. Adote bons hábitos em relação às senhas, como utilizar frases longas, caracteres especiais, combinação de maiúsculas e minúsculas e números. As senhas precisam ser fortes e difíceis de se adivinhar.
- **Aproveite as configurações de segurança da IoT.** Alguns dispositivos IoT oferecem configurações avançadas que você deve aproveitar ao máximo. Determinados produtos IoT podem oferecer redes separadas, semelhantes a uma rede Wi-Fi hóspede, juntamente com sua conexão principal. Este é apenas um recurso — muitos mais podem acompanhar outros produtos.

- **Conecte os dispositivos IoT utilizando Wi-Fi seguro.** Crie senhas fortes e use os protocolos de segurança mais recentes, como WPA2.
- **Restrinja o acesso físico aos dispositivos IoT.** A adulteração direta dos dispositivos também pode resultar em hacking de dispositivos IoT.
- **Desative o suporte a Universal Plug and Play (UPNP).** Muitos dispositivos são compatíveis com UPnP, o que os torna mais fáceis de descobrir na Internet e mais vulneráveis a infecções por malware. Desative esse recurso quando possível.
- **Desligue e religue os dispositivos IoT periodicamente.** O malware costuma ser armazenado em memória volátil e pode ser apagado desligando-se e religando-se o dispositivo.

Como a McAfee protege sistemas e redes contra ataques a dispositivos IoT

Além da lista precedente de melhores práticas decisivas em dispositivos IoT, os produtos da McAfee podem ajudar a minimizar os riscos de infecções de malware dentro dos dispositivos IoT e bloquear as atividades maliciosas das redes de bots. As seguintes configurações de produtos da McAfee podem ajudar a proteger sistemas e redes contra ataques oriundos de dispositivos IoT:

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 Enterprise 8.8: **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, 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 um executável especificado em Target Executable, como 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 malware 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 McAfee 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 o 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:
  - Detecção com base em assinaturas: o McAfee GTI contém mais de 600 milhões de assinaturas.
  - Detecção com base em reputação: McAfee GTI.
  - Análise estática e emulação em tempo real: utilizadas 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 analisador onde o malware provavelmente será executado:
  - Sistemas operacionais comuns, Windows 7, Windows 8, Windows 10
  - Instale aplicativos do Windows (Word, Excel) e ative as 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 ativa o malware. Oferecer conexão à Internet aos perfis 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 antimalware do McAfee Web Gateway.
- Ative o McAfee 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 McAfee).

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 GTI, 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 malware.
- 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

White paper: ***More Confidence, Safety, and Security in the Digital World*** (Mais confiança, proteção e segurança no mundo digital)

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

SIEM orchestration. How McAfee Enterprise Security Manager can drive action, automate remediation, and increase situational awareness (Orquestração de SIEM. Como o McAfee Enterprise Security Manager pode gerar ação, automatizar a correção e aumentar a conscientização situacional): **PD24830**

White paper: ***Secure Beyond the Signature*** (Segurança além de assinaturas)

FAQs for McAfee Network Security Platform: Advanced Malware Detection (Perguntas frequentes sobre o McAfee Network Security Platform. Detecção de malware avançado): **KB75269**

Guia de produto do McAfee Web Gateway. Filtragem da Web: **PD26339**

McAfee
Together is power.

Av. Nações Unidas, 8.501 – 16º andar
Pinheiros – São Paulo – SP
CEP 05425-070, Brasil
+(11) 3711-8200
www.mcafee.com/br