Resumo de solução

Proteção contra ladrões de senhas

Na medida em que dependemos cada vez mais de dispositivos eletrônicos pessoais e empresas levam informações valiosas para a nuvem, o valor das credenciais de acesso aumenta. Atualmente, os atacantes utilizam senhas roubadas nos estágios preliminares de praticamente todas as principais ameaças persistentes avançadas.

Os ladrões de senhas concentram-se na violação da segurança de redes e sistemas para a obtenção de credenciais de acesso crítico. As sólidas capacidades do ladrão de senhas Fareit fizeram dele o mais popular malware para roubo de senhas por mais de cinco anos. Desde sua descoberta em 2012, o Fareit continuou mudando para driblar as mais recentes tecnologias de defesa cibernética.

Inicialmente, o Fareit concentrava-se no roubo de credenciais de login de navegadores da Web para obter acesso a aplicativos, como os de acesso bancário, contas de e-mail ou para roubo de identidade. Desde então, o Fareit evoluiu e se tornou um ladrão de informações mais agressivo, que se esconde utilizando táticas de imitação, como alterar seu hash de arquivo a cada infecção. Em 2016 surgiu uma nova geração do malware de roubo de senhas Fareit que utilizava um ativo de rede infectado para realizar ataques de negação de serviço distribuída. Além disso, o Fareit é oferecido atualmente como um serviço do tipo “pague por infecção”, o que significa que os criminosos cibernéticos agora estão ganhando dinheiro com a distribuição de malware. Quanto mais infecções conseguem, mais eles ganham.

Os ataques de phishing que entregam ladrões de senhas como o Fareit estiveram entre os principais vetores de ataque inicial ao longo da década passada.

Políticas e procedimentos para proteção contra ataques de ladrões de senhas

A McAfee recomenda que as organizações sigam as etapas abaixo para se proteger contra ataques de ladrões de senhas:

- Os ladrões de senhas costumam ser distribuídos por malware, portanto, como medida de segurança padrão, sempre mantenha atualizados os produtos antimalware.
- O malware pode ser contraído por download por usuários incautos durante a navegação. Mantenha os navegadores e seus complementos atualizados para adicionar uma camada extra de proteção.

McAfee™
Together is power.

- Execute aplicativos como usuário com privilégios limitados em vez de direitos de administrador.
- Mantenha protegido o perímetro de rede. Firewalls podem impedir que atacantes externos obtenham acesso a aplicativos internos previamente comprometidos por ataques bem-sucedidos de ladrões de senhas.
- Use credenciais de autenticação corporativa (como as de proxies da Web para navegação na Internet, aplicativos de banco de dados, pastas compartilhadas, etc.) somente quando estiver utilizando ativos corporativos. Não permita, na rede corporativa confiável, sistemas que não sejam distribuídos e certificados pelo grupo de segurança de TI corporativa.
- Um malware contendo um ladrão de senhas pode estar incorporado em um software legítimo previamente troianizado por um atacante. Para evitar um ataque bem-sucedido desse tipo, mecanismos rígidos de fornecimento e distribuição de software são altamente recomendáveis. É sempre bom ter um repositório central de aplicativos corporativos do qual os usuários possam fazer download de software aprovado.
- Caso os usuários estejam autorizados a instalar aplicativos não previamente validados pelo grupo de segurança de TI, instrua-os a instalar somente aplicativos de fornecedores conhecidos e com assinaturas confiáveis. É muito comum que aplicativos "inofensivos" oferecidos on-line tenham ladrões de senhas ou outros tipos de malware incorporado.
- Evite downloads de aplicativos que não sejam da Web. Em grupos da Usenet, canais de IRC, clientes de mensagens instantâneas ou sistemas P2P, a probabilidade de se fazer download de malware é muito grande. Links para sites vistos no IRC e em programas de mensagens instantâneas também levam, frequentemente, a downloads infectados.
- Implemente um programa educativo para prevenir ataques de phishing. Os ladrões de senhas costumam ser distribuídos por phishing.

Se você acredita que seus sistemas foram comprometidos por um ladrão de senhas, algumas práticas recomendadas o ajudarão a conter a movimentação lateral da infecção:

- Reduza a superfície de ataque ativando a autenticação de dois fatores nos aplicativos que tiverem essa funcionalidade. Mesmo que o atacante tenha uma senha roubada, o segundo fator impedirá a infiltração.
- O uso de um firewall de endpoint restringirá a expansão das intrusões com senhas roubadas se o computador tiver um tráfego limitado de entrada e saída, imposto por regras de firewall.

Como os produtos da McAfee podem protegê-lo contra ataques de ladrões de senhas

McAfee VirusScan® Enterprise 8.8 ou McAfee Endpoint Security 10

- Mantenha o software antimalware do endpoint atualizado com o patch, a versão do DAT e o mecanismo de varredura mais recentes. Certifique-se de que o McAfee Global Threat Intelligence (McAfee GTI) esteja em uso.
- 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

Ferramentas de prevenção de intrusões não são eficazes para expor um ataque de ladrão de senhas bem-sucedido. Contudo, o McAfee Host Intrusion Prevention ajuda a evitar a movimentação lateral da carga do malware, a qual pode conter um ladrão de senhas.

- 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 ou 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, para impedir que explorer.exe execute um executável especificado em Target Executables, 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 bloquear aqueles que distribuem ladrões de senhas ou avisar os usuários sobre eles.

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 Advanced Threat Defense (Enviar arquivos para o Advanced Threat Defense) se o nível de reputação for Unknown (Desconhecido) ou abaixo.
  - Política do McAfee Threat Intelliqence Exchange Server: 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:
  - Opte 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: o "zoológico" de malware do McAfee Labs guarda mais de 600 milhões de assinaturas.
  - Detecção com base em reputação: McAfee GTI.
  - Análise estática e emulação em tempo real: utilizada para detecção de 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 de analisador onde o malware de roubo de senhas tem probabilidades de ser executado:
  - Sistemas operacionais comuns, como Windows 7, 8 e 10.
  - Instale aplicativos do Windows (Word, Excel) e ative as macros.
- Instaure um analisador para determinar o perfil do acesso à Internet:
  - Muitas amostras executam um script de um documento Microsoft que cria uma conexão de saída e ativa o malware. A instauração de um analisador permite determinar o perfil de uma conexão à Internet, aumentando 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 ladrões de senhas.

- 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 Defense.
  - Verifique se a configuração do McAfee Advanced Threat Defense 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.
- Você pode alterar o script para fazer referência a outros módulos do McAfee Threat Intelligence Exchange, 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 Active Response

- O McAfee Active Response encontra ameaças avançadas e responde a elas. 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 podem ser utilizados para construir ferramentas específicas para localizar e identificar indicadores de comprometimento associados a ladrões de senhas.
- Gatilhos e reações são criados pelo usuário para definir ações a serem executadas quando determinadas condições forem satisfeitas; por exemplo, quando hashes ou nomes de arquivo são encontrados, uma ação de exclusão pode ser executada automaticamente.

Para leitura adicional

Phishing Attacks Employ Old but Effective Password Stealer (Ataques de phishing empregam ladrão de senhas antigo, porém eficaz)

Perfil do vírus Fareit

Perfil do vírus Fareit

McAfee™
Together is power.

McAfee LLC
2821 Mission College Blvd.
Santa Clara, CA 95054 USA
www.mcafee.com/br