Como se proteger contra o ransomware

Evite as atuais ameaças de ransomware com a McAfee®

O ransomware é o malware que usa a criptografia assimétrica para sequestrar as informações de suas vítimas. Criptografia assimétrica (público-privada) é uma criptografia que utiliza um par de chaves para criptografar e descriptografar um arquivo. O par público-privado de chaves é gerado exclusivamente pelo atacante para a vítima, sendo a chave privada para descriptografar os arquivos armazenada no servidor do atacante. O atacante disponibiliza a chave privada para a vítima somente após o pagamento do resgate, embora isso não aconteça sempre — como visto nas últimas campanhas de ransomware. Sem acesso à chave privada, é praticamente impossível descriptografar os arquivos mantidos reféns em troca de um resgate.

Existem muitas variantes de ransomware. Frequentemente, o ransomware (e outros tipos de malware) é distribuído por meio de campanhas de spam em e-mail ou através de ataques direcionados. Os produtos da McAfee® empregam várias tecnologias que ajudam a prevenir o ransomware. Os seguintes produtos McAfee e as configurações associadas foram desenvolvidos para deter muitos tipos de ransomware.

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 sendo utilizado; ele contém mais de oito milhões de assinaturas de ransomware exclusivas.
- Crie regras de proteção de acesso para evitar a instalação de cargas virais de ransomware: consulte os artigos da base de conhecimentos sobre regras de proteção de acesso: **KB81095** e **KB54812**.

McAfee Host Intrusion Prevention

- **Assista o vídeo** sobre como configurar o McAfee Host Intrusion Prevention para evitar a carga viral do CryptoLocker.
- 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.

Regras do McAfee Host Intrusion Prevention

O McAfee Host Intrusion Prevention permite monitorar a criação, leitura, gravação, execução, exclusão, renomeação, modificação de atributos e criação de links físicos de arquivos. Especifique os tipos e caminhos de arquivo sobre os quais você deseja (ou não deseja) alertas e quaisquer executáveis que você queira incluir (fontes sabidamente nocivas) ou excluir (geradores notórios de falsos positivos). Essa regra tem o potencial de ser intrusiva, portanto, considere o uso da regra em modo de log/informativo por um período de experiência. Observe que as regras de proteção de arquivos exigem que você estabeleça o seu banco de dados de aplicativos confiáveis.

Rule: Cryptolocker—block EXE in AppData
Rule type: files
Operations: create, execute, write
Parameters:
- Include: Files: **\AppData*.exe
- Include: Files: **\AppData\Local*.exe
- Include: Files: **\AppData\Roaming*.exe

Executables: Include *.*

Observe que o exemplo seguinte omitiu muitas extensões de arquivo devido a restrições de espaço. Certifique-se de selecionar todas as extensões de arquivo relevantes para os seus aplicativos.

```
Rule {
tag “Blocking a Non-Trusted program attempt to write to protected data file extensions”
Class Files
Id 4001
level 4
files {Include “*\\*.3DS” “*\\*.7Z” “*\\*.AB4” “*\\*.AC2” “*\\*.ACCDB” “*\\*.ACCDE” “*\\*.ACCDR” “*\\**.ACCDT” “*\\*.ACR” “*\\*.ADB” “*\\*.AI” “*\\*.AIT” “*\\*.al” “*\\*.APJ” “*\\*.ARW” “*\\*.ASM” “*\\*.ASP” “*\\*.BACKUP” “*\\*. BAK” “*\\*.BDB” “*\\*.BGT” “*\\*.BIK” “*\\*.BKP” “*\\*. BLEND” “*\\*.BPW” “*\\*.C” “*\\*.CDF” “*\\*. CDR” “*\\*. CDX” “*\\*.CE1” “*\\*.CE2” “*\\*.CER” “*\\*.CFP” “*\\*.SRF” “*\\*.SRW” “*\\*.ST4” “*\\*.ST5” “*\\*.ST6” “*\\*.ST7” “*\\*. ST8” “*\\*.STC” “*\\*.STD” “*\\*. STI” “*\\*.STW” “*\\*.STX” “*\\*.SXC” “*\\*.SXD” “*\\*.SXG” “*\\*.SXI” “*\\*.SXM” “*\\*. SXW” “*\\*.TXT” “*\\*.WB2” “*\\*.X3F” “*\\*.XLA” “*\\*. XLAM” “*\\*.XLL” “*\\*. XLM” “*\\*.XLS” “*\\*.XLSB” “*\\*. XLSM” “*\\*.XLSX” “*\\*.XLT” “*\\*.XLTM” “*\\*. XLTX” “*\\*. XLW” “*\\*.XML” “*\\*.ZIP”}
Executable {Include “*”}
user_name{Include “*”}
directives files:writefiles:renamefiles:delete
}
```

- Regras de proteção de acesso: Você também pode usar regras de proteção de acesso para reforçar a regra do McAfee Host Intrusion Prevention com os versáteis caracteres curinga: **\Users**\AppData***.exe

Observação: Nas versões mais recentes do SYSCore fornecidas por versões atualizadas do McAfee VirusScan® Enterprise, do McAfee Agent, do McAfee Host Intrusion Prevention e do McAfee Data Loss Prevention, ** não funciona mais no início do campo “File or folder name to block” (Nome do arquivo ou pasta a ser bloqueado). Nas versões mais recentes, é preciso utilizar o seguinte formato:

```
C:\**\AppData\**.exe
```

Isso é feito para bloquear qualquer .exe aleatório na raiz e qualquer subdiretório de uma pasta chamada AppData em qualquer lugar da unidade C:.

As iterações possíveis de uma regra desse tipo são praticamente ilimitadas, portanto, pense bem em todas as implicações da regra. Você deve considerar todos os aspectos da regra, todas as entradas possíveis para seu funcionamento pretendido e também como configurar as regras como um todo (exemplo a seguir):

```
Process to include: *
Process to exclude: [deixar em branco]
File or folder name to block: <caminho ou diretório>
File actions to prevent: [Quaisquer ações que você queira (é recomendável começar com ações menos agressivas para minimizar possíveis dados ao endpoint)]
```

McAfee SiteAdvisor Enterprise ou McAfee Endpoint Security/Web Protection

- Utilize as reputações dos sites para evitar ou advertir os usuários sobre sites que distribuem ransomware.

McAfee Threat Intelligence Exchange e McAfee Advanced Threat Defense

- Configuração de política do McAfee Threat Intelligence Exchange:
  - Comece com o modo de observação — Conforme forem descobertos endpoints com processos suspeitos, use 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 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 Protection

- Capacidades de detecção incluídas:
  - Detecção com base em assinaturas — As assinaturas mantidas pelo McAfee Labs incluem mais de oito milhões de assinaturas de ransomware, como CTB-Locker, CryptoWall e suas variantes.
  - 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 Analizer onde o ransomware provavelmente será executado:
  - Sistemas operacionais comuns, Microsoft Windows 7, Microsoft Windows 8 e Microsoft Windows XP.
  - Instale aplicativos do Windows (Word, Excel) e ative macros.
- Ofereça acesso à Internet ao perfil do Analizer:
  - Muitas amostras executam um script de um documento Microsoft que cria uma conexão de saída e ativa o malware. Oferecer conexão à Internet a um perfil do Analizer aumenta as taxas de detecção.

McAfee Network Security Platform

- O McAfee Network Security Platform tem assinaturas em suas políticas padrão para:
  - Verificar se você tem a assinatura com id=0x4880f900 (específica para ransomware).
  - O McAfee Network Security Platform também tem assinaturas para identificar TOR, 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 (rede de bots).

McAfee Web Gateway

- Ative a inspeção do McAfee Gateway Anti-Malware.
- 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 uma referência cruzada entre um arquivo gerador de um evento de ameaça do McAfee Threat Intelligence Exchange e o VirusTotal.
- Observe que você pode 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 Active Response

O McAfee Active Response encontra e responde a ameaças avançadas. Quando utilizado em associação com canais de ameaças, como McAfee GTI, Dell SecureWorks ou ThreatConnect, ameaças novas — incluindo ransomware — 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 ransomware.
- 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 efetuada automaticamente.

Para leitura adicional

Protecting Against Ransomware (Proteção contra ransomware)

Esse artigo da base de conhecimentos oferece aos clientes as informações mais detalhadas sobre proteção contra ransomware em um ambiente McAfee.

Para informações detalhadas sobre as diversas variantes, sintomas, vetores atacados e técnicas de prevenção do ransomware CryptoLocker, assista os seguintes vídeos:

- **CrytpoLocker Malware Session (Sessão do malware CrytpoLocker)**
- **CryptoLocker Update (Atualização do CryptoLocker)**

Consultoria de ameaças do McAfee Labs: X97M/Downloader

Esse artigo oferece aos clientes uma análise detalhada de uma versão mais recente do ransomware.

Derrote o ransomware: proteja seus dados contra sequestros digitais

Resumo de solução de cinco páginas que descreve o que é o ransomware e como algumas das soluções da McAfee (mas não todas) ajudam a proteger contra ele.

Advice for Unfastening CryptoLocker Ransomware (Recomendações para se livrar do ransomware CryptoLocker)

Artigo de blog detalhado sobre o que o cliente deve fazer após um ataque de ransomware.

A volta do ransomware: novas famílias surgem com força total

Artigo do relatório do McAfee Labs sobre ameaças (página14), destacando o ransomware novo e sua evolução.

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