Resumo de solução

Derrote o ransomware: proteja seus dados contra sequestros digitais

O ransomware é o malware que usa a criptografia assimétrica para sequestrar as informações de suas vítimas. A criptografia assimétrica (pública-privada) utiliza um par de chaves para criptografar e descriptografar um arquivo. O par de chaves pública-privada é gerado exclusivamente pelo atacante visando a vítima, e a chave privada descriptografa os arquivos armazenados 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 quase impossível descriptografar os arquivos mantidos reféns.

Um panorama sobre o ransomware

Para uma visão técnica aprofundada sobre o ransomware, consulte o ***Relatório do McAfee Labs sobre ameaças: maio de 2015***. No *Relatório do McAfee Labs sobre ameaças: novembro de 2014*, previmos nove grandes ameaças para 2015. O McAfee Labs afirmou que: "O ransomware (vírus sequestrador) evoluirá em seus métodos de propagação, na criptografia e nos alvos visados". Houve um aumento enorme quase imediato na predominância do ransomware, além do surgimento de novas famílias, como a Teslacrypt, e mais mudanças em famílias já ativas, como CTB-Locker, CryptoWall e TorrentLocker.

A maioria das campanhas de ransomware começa com um ataque de phishing. Com o passar do tempo, elas se tornaram mais sofisticadas; hoje, muitas são especialmente elaboradas nos mínimos detalhes para a localização onde se encontram as vítimas visadas.

Novas tecnologias também foram adaptadas para fortalecer o ransomware:

- **Moeda virtual:** ao utilizar **moeda virtual** como método para pagamento de resgates, os atacantes não ficam expostos às transações bancárias tradicionais e à possibilidade de rastreamento das transferências.
- **Rede Tor (rede de anonimato):** com a **rede Tor**, os atacantes conseguem ocultar com mais facilidade a localização dos seus servidores de controle, que armazenam as chaves privadas das vítimas. A rede Tor viabiliza a manutenção da infraestrutura criminal por longo prazo, possibilitando, ainda, o aluguel da infraestrutura a outros atacantes, para que promovam campanhas afins.

intel Security

- **Ataques aos dispositivos móveis:** em junho de 2014, pesquisadores descobriram a primeira família de ransomware a criptografar dados em dispositivos Android.[1] Com a criptografia AES, a família Pletor bloqueia os dados armazenados no cartão de memória do telefone e conecta-se aos atacantes através da rede Tor, SMS ou HTTP.
- **Ataques direcionados aos dispositivos de armazenamento em massa:** em agosto de 2014, o Synolocker começou a direcionar seus ataques contra as estações de rack e disco de armazenamento conectado em rede (NAS) da Synology.[2] O malware explora as vulnerabilidades em versões não corrigidas dos servidores NAS para criptografar remotamente todos os dados armazenados nos servidores, utilizando tanto as chaves RSA de 2.048 bits quanto as chaves de 256 bits.

Proteção contra ransomware

Descubra a seguir algumas boas práticas e políticas para proteger melhor você e sua organização contra a ameaça do ransomware.

- **Sempre promova a conscientização dos usuários:** pelo fato de a maioria dos ataques de ransomware começar com e-mails de phishing, conscientizar o usuário é imprescindível e necessário. As estatísticas revelam que para cada dez e-mails enviados pelos atacantes, pelo menos um atingirá seu objetivo. Não abra e-mails ou anexos de remetentes desconhecidos ou não verificados.
- **Mantenha os patches do sistema atualizados:** muitas vulnerabilidades das quais o ransomware se aproveita podem ser corrigidas. Mantenha os patches atualizados para sistemas operacionais, Java, Adobe Reader, Flash e aplicativos. Tenha um procedimento de correção em vigor e verifique se os patches foram aplicados corretamente.
- **Tenha atenção redobrada ao abrir anexos:** configure o seu software antivírus para examinar automaticamente todos os anexos de e-mail e de mensagens instantâneas. Certifique-se de que os programas de e-mail não abram anexos ou processem gráficos automaticamente e certifique-se de que o painel de visualização esteja desativado. 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.

Como a Intel Security pode ajudá-lo a se proteger contra o ransomware

McAfee Web Gateway

Anúncios enganosos, downloads de passagem e URLs maliciosos incorporados em sites confiáveis são apenas alguns dos métodos de ataque utilizados para distribuir ransomware. O **McAfee Web Gateway** é um produto sólido que reforça a proteção da sua empresa contra esse tipo de ameaça.

- **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 Email Gateway
Saber se um e-mail na caixa de entrada de um usuário é inofensivo ou trata-se de um ataque de phishing para distribuir ransomware é uma das principais preocupações das empresas. O **McAfee Email Gateway** oferece proteção com diversos recursos contra esses tipos de ataques de phishing cada vez mais sofisticados.

- **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 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 GTI:** combina informações da rede local com a inteligência de reputação do McAfee GTI, proporcionando a proteção mais completa disponível contra ameaças de entrada, spam e malware.

McAfee Advanced Threat Defense
O **McAfee Advanced Threat Defense** é uma solução multicamada de detecção de malware, que combina vários mecanismos de inspeção com base em assinaturas e reputação, emulação em tempo real, análise completa de código estático e análise dinâmica em área restrita. O McAfee Advanced Threat Defense protege contra exemplares predominantes de ransomware, como o CTB-Locker, CryptoWall e outros.

- **Detecção com base em assinaturas:** detecta vírus, worms, spyware, bots, cavalos de Troia, estouros de buffer e ataques combinados. Sua abrangente base de conhecimentos é criada e mantida pelo McAfee Labs, e atualmente contém mais de 150 milhões de assinaturas, incluindo o CTB-Locker, CryptoWall e suas variantes.
- **Detecção com base em reputação:** consulta a reputação dos arquivos utilizando o serviço 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 e ameaças de dia zero não identificados por reputação ou técnicas com base em assinaturas.
- **Análise completa de código estático:** faz engenharia reversa do código do arquivo para determinar todos os seus atributos e conjuntos de instruções e analisar completamente o código-fonte sem execução. Amplos recursos de descompactação permitem abrir todos os tipos de arquivos compactados, permitindo análise completa e classificação do malware para que a sua empresa compreenda a ameaça representada pelo malware em questão.
- **Análise dinâmica em área restrita:** executa o código do arquivo em um ambiente virtual em tempo de execução e observa o comportamento resultante. Os ambientes virtuais podem ser configurados conforme os ambientes de host da sua empresa, e são compatíveis com imagens personalizadas dos sistemas operacionais Windows 7 (32 ou 64 bits), Windows XP, 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 para atender às necessidades do seu ambiente. O **McAfee Threat Intelligence Exchange** reduz significativamente a exposição a ataques, graças à sua visibilidade sobre ameaças imediatas, como aplicativos ou arquivos desconhecidos em execução no ambiente. O bloqueio de executáveis novos ou desconhecidos garante a proteção proativa contra ransomware.

- **Informações abrangentes sobre ameaças:** personalize facilmente informações abrangentes sobre ameaças obtidas de fontes de dados de inteligência global. Essas fontes podem ser o McAfee GTI ou canais de terceiros, com informações locais sobre ameaças obtidas 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 suas poderosas capacidades de imposição de políticas e gerenciamento central.
- **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 (IoCs):** importe hashes de arquivos nocivos conhecidos para que o McAfee Threat Intelligence Exchange imunize o seu ambiente contra esses arquivos notoriamente nocivos através da imposição de políticas. Caso algum dos indicadores de comprometimento (IoCs) seja acionado no ambiente, o McAfee Threat Intelligence Exchange pode eliminar todos os processos e aplicativos associados com o IoC.

McAfee VirusScan Enterprise
Com o **McAfee VirusScan® Enterprise** é fácil detectar e proteger contra ransomware. O McAfee VirusScan Enterprise utiliza o premiado mecanismo de varredura da McAfee para proteger arquivos contra vírus, worms, rootkits, cavalos de Troia e outras ameaças avançadas.

- **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 em aplicativos.
- **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:** protege 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 Network Security Platform

O McAfee Network Security Platform foi desenvolvido para realizar inspeções profundas no tráfego de rede. O McAfee Network Security Platform combina técnicas de inspeção avançadas — incluindo análise completa de protocolo, reputação de ameaça, análise de comportamento e análise avançada de malware — para detectar e prevenir ataques, como ransomware que tenta se comunicar através de protocolos de rede, como a rede Tor, IRC e outros.

- **Defesa abrangente contra malware:** reúne reputação de arquivos do McAfee GTI, análise profunda de arquivos com inspeção de JavaScript e análise avançada de malware, sem assinaturas, para detectar e deter ameaças de dia zero, malware personalizado e outros ataques furtivos.
- **Uso de técnicas avançadas de inspeção:** inclui análise completa de protocolo, reputação de ameaças e análise de comportamento para detectar e prevenir ataques conhecidos e de dia zero na rede.
- **Integração com o McAfee GTI:** combina canais de geolocalização, reputação de IP e reputação de arquivos em tempo real com dados contextuais detalhados sobre usuários, dispositivos e aplicativos para respostas rápidas e precisas a ataques via rede.
- **Security Connected:** uma integração decisiva com o McAfee Advanced Threat Defense permite ao McAfee Network Security Platform enviar para o McAfee Advanced Threat Defense aquivos suspeitos encontrados no tráfego monitorado e permiti-los ou proibi-los, com base em descobertas do McAfee Advanced Threat Defense.

Certificar-se de que os dados valiosos da sua organização não estão suscetíveis a sequestros digitais é uma tarefa difícil, especialmente com o ransomware tornando-se, cada vez mais, um vetor de ataque. A tecnologia da Intel Security pode ajudar sua empresa a se proteger de forma proativa contra ameaças, como o ransomware, tanto no endpoint quanto na rede.

1. **https://threatpost.com/android-ransomware-first-to-encrypt-data-on-mobile-devices/106535**
2. **http://forum.synology.com/enu/viewtopic.php?f=108&t=88770**

61980brf_ransomware_0615

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