Resumo de solução

Proteja sistemas de atendimento médico contra ransomware

O ransomware é um malware que geralmente emprega criptografia assimétrica para manter reféns as informações da vítima. 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.

Nos últimos anos o ransomware tem estado entre as maiores preocupações de todo profissional de segurança. Infelizmente, o ransomware é uma ferramenta de ataque cibernético simples e eficaz, utilizada para ganho monetário fácil. Ao longo do ano passado, vimos uma mudança nos alvos, de indivíduos para empresas, porque estas pagam resgates maiores. Recentemente, hospitais tornaram-se um alvo muito popular para os autores de ransomware. No *Relatório do McAfee Labs sobre ameaças: setembro de 2016*, analisamos os ataques de ransomware dos dois primeiros trimestres de 2016 contra hospitais e constatamos que foram ataques bem-sucedidos, relacionados e direcionados, embora não muito sofisticados. Discutimos também os desafios que o ransomware representa especificamente para hospitais, incluindo sistemas legados e dispositivos médicos com segurança deficiente, além da questão de vida ou morte relacionada à necessidade de acesso imediato à informação.

Políticas e procedimentos para proteção contra ransomware

O passo mais importante para proteger sistemas contra ransomware é estar ciente do problema e das maneiras pelas quais ele se dissemina. Veja a seguir várias políticas e procedimentos que os hospitais devem seguir para minimizar o sucesso dos ataques de ransomware:

- Tenha um plano de ação para a eventualidade de um ataque. Saiba onde se encontram os dados críticos e descubra se há algum método para infiltrá-los. Realize exercícios de continuidade dos negócios e recuperação de desastres com a equipe de gerenciamento de emergências do hospital para validar o ponto de recuperação e os objetivos de prazo.

intel Security

Esses exercícios podem revelar impactos sobre as operações do hospital que, de outra forma, não apareceriam durante um teste de backup normal. A maioria dos hospitais paga o resgate por não dispor de planos de contingência!

- Mantenha os patches do sistema atualizados. Muitas vulnerabilidades frequentemente aproveitadas pelo ransomware podem ser corrigidas. Mantenha os patches atualizados para sistemas operacionais, Java, Adobe Reader, Flash e aplicativos. Tenha um procedimento implementado para aplicação de patches e verifique se os patches foram aplicados corretamente.
- Para sistemas hospitalares legados e dispositivos médicos que não podem ser corrigidos, amenize o risco utilizando listas brancas de aplicativos, as quais bloqueiam os sistemas e impedem a execução de programas não aprovados. Segregue esses sistemas e dispositivos 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.
- Proteja os endpoints. Ative a proteção dos endpoints e aproveite seus recursos avançados. Em muitos casos, o cliente é instalado com apenas os recursos padrão ativados. Ao implementar alguns recursos avançados — por exemplo, “impedir executável de ser executado a partir da pasta Temp” — é possível detectar e bloquear um maior número de malware.
- Se possível, evite o armazenamento de dados confidenciais em discos locais. Peça aos usuários que armazenem os dados em unidades de rede seguras. Isso limita a indisponibilidade porque os sistemas infectados podem ser simplesmente recriados a partir de imagens.
- Use antispam. A maioria das campanhas de ransomware começa com um e-mail de phishing, que vem com um link ou um determinado tipo de anexo. Nas campanhas de phishing que compactam o ransomware em um arquivo .scr ou em outro formato de arquivo incomum, fica fácil configurar uma regra de spam para bloquear esses anexos. Se os arquivos .zip não são bloqueados, faça a varredura em pelo menos dois níveis no arquivo .zip em busca de possíveis conteúdos maliciosos.
- Bloqueie o tráfego e programas indesejados ou desnecessários. Se não houver necessidade do Tor, bloqueie o aplicativo e seu tráfego na rede. Frequentemente, bloquear o Tor impede que o ransomware obtenha sua chave pública RSA do servidor de controle, bloqueando assim o processo de criptografia do ransomware.
- Adicione segmentação de rede para dispositivos críticos necessários para o atendimento aos pacientes.
- Isole os backups. Certifique-se de que sistemas, armazenamento e fitas de backup estejam em um local que normalmente não é acessível pelos sistemas das redes de produção. Se as cargas virais dos ataques de ransomware se disseminarem lateralmente, elas poderão afetar os dados armazenados no backup.
- Utilize uma infraestrutura virtual para sistemas de registros médicos eletrônicos críticos que fique isolada do restante da rede de produção.
- Sempre promova a conscientização dos usuários. Como a maioria dos ataques de ransomware começa com e-mails de phishing, a conscientização dos usuários é fundamental. Estatísticas mostram que, para cada dez e-mails enviados por atacantes, pelo menos um é bem-sucedido. Não abra e-mails ou anexos de remetentes desconhecidos ou não verificados.

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

McAfee VirusScan Enterprise e McAfee Endpoint Security 10

- Com o McAfee VirusScan Enterprise (VSE) ou o McAfee Endpoint Security (ENS), implemente o seguinte:
  - Use o McAfee ePolicy Orchestrator (ePO) diariamente para distribuir DATs atualizados.
  - Certifique-se de que o McAfee Global Threat Intelligence (McAfee GTI) esteja ativado; o McAfee GTI contém mais de sete milhões de assinaturas de ransomware exclusivas.
  - Desenvolva regras de proteção de acesso para evitar a instalação e as cargas de ransomware; consulte os artigos da base de conhecimentos sobre regras de proteção de acesso KB81095 e KB54812.
  - Use a contenção dinâmica de aplicativos para impedir que aplicativos desconhecidos realizem atividades maliciosas.

McAfee Threat Intelligence Exchange

- Com o McAfee Threat Intelligence Exchange (TIE), configure as seguintes políticas:
  - Iniciar com o modo de observação.
  - Conforme forem descobertos endpoints com processos suspeitos, usar tags do sistema para aplicar políticas de imposição do McAfee TIE.
  - Limpar caso a reputação seja de sabidamente malicioso.
  - Bloquear caso a reputação seja de muito provavelmente malicioso (bloquear desconhecido seria uma proteção melhor, mas poderia aumentar demasiadamente a carga de trabalho administrativo inicial).
  - Enviar arquivos para McAfee Advanced Threat Defense (ATD) se o nível de reputação for desconhecido ou abaixo.
  - Política de servidor do TIE: aceitar reputações do McAfee ATD para arquivos ainda não vistos pelo McAfee TIE.
- Intervenção manual no McAfee Threat Intelligence Exchange:
  - Imposição de reputação de arquivos (sujeita ao modo de operação).
  - Muito provavelmente malicioso: limpar/excluir.
  - 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. Marcar o arquivo como provavelmente malicioso.
  - Fornecer dados de reputação de terceiros ao McAfee TIE via indicadores de comprometimento.

McAfee Advanced Threat Defense

- O McAfee Advanced Threat Defense tem as seguintes capacidades próprias de detecção:
  - Detecção com base em assinaturas: as assinaturas mantidas pelo McAfee Labs chegam a mais de 150 milhões, incluindo assinaturas do CTB-Locker, do CryptoWall e de suas variantes.
  - 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 do Analizer onde o ransomware provavelmente será executado:
  - Sistemas operacionais comuns, Windows 7, Windows 8 e Windows XP.
  - Instalar aplicativos do Windows (Word, Excel) e ativar macros.

- Ofereça perfis do Analizer exclusivos para sistemas operacionais distintos com acesso à Internet:
  - Muitas amostras executam um script de um documento do Microsoft Office que cria uma conexão para fora e ativa o malware. Oferecer um perfil do Analizer com conexão à Internet aumenta as taxas de detecção.

McAfee Application Control

- O McAfee Application Control oferece proteção com lista branca de aplicativos. Isso é ideal para proteger todos os tipos de dispositivos, especialmente:
  - Dispositivos estáticos, como equipamentos médicos.
  - Sistemas com sistemas operacionais legados que não recebem mais atualizações.
  - Servidores de aplicativos que oferecem um numero limitado de serviços.
  - Sistemas que não mudam com frequência.
- Instalação inicial
  - O McAfee Application Control faz uma varredura completa do sistema durante a instalação, e cria o inventário de endpoints e aplicativos a serem incluídos na lista branca.
- Modo de observação
  - Permite que os administradores rastreiem novos aplicativos instalados/iniciados, com a opção de mesclá-los na lista branca centralizada caso seja determinado que o aplicativo deve ser autorizado.
  - Auxilia o processo de inclusão em lista branca identificando novos atualizadores confiáveis para aplicativos dentro do ambiente.
  - Identifica métodos para atualização da lista branca, como processos, certificados, diretórios ou usuários aprovados.
- Modo de autoaprovação
  - Os usuários podem aprovar aplicativos não incluídos na lista branca. Isso proporciona flexibilidade e o mínimo de impacto sobre os negócios.
  - Os administradores podem rastrear de forma centralizada o conteúdo aprovado pelos usuários e aceitar ou revogar a autorização do aplicativo com base na reputação e nas políticas da organização.
- Imposição da lista branca
  - O sistema é completamente protegido contra aplicativos desconhecidos, incluindo aplicativos maliciosos, como ransomware.
  - Oferece uma notificação ao usuário final sobre o procedimento a ser seguido para aprovação de novos executáveis.

Leitura adicional

Comunidade do Intel Security Expert Center

- McAfee VirusScan Enterprise
- McAfee Endpoint Security
- McAfee Threat Intelligence Exchange
- McAfee Advanced Threat Defense
- McAfee Application Control

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