Por Michal Salat (*)

 Há algumas semanas atrás, o Hospital Universitário de Brno, na República Tcheca, que também é um centro de testes para o Coronavírus, enfrentou um ataque de ransomware que paralisou os seus computadores. O hospital seguiu procedimentos padrão e notificou a Agência de Segurança de Informações e Cibernética National Tcheca para ajudar na investigação, e os nossos Laboratórios de Ameaças ofereceram ajuda, apoiando o hospital e analisando o malware.

Os hospitais não são necessariamente mais suscetíveis a ataques de ransomware, no entanto, um ataque pode ter consequências severamente prejudiciais para eles, como a perda de registros de pacientes e atrasos ou cancelamentos de tratamentos. Como os hospitais realizam operações críticas e mantêm informações vitais sobre os pacientes, eles também têm maior probabilidade de pagar o resgate, o que os torna alvos atraentes para os autores das ameaças.

Declarações dos responsáveis por ransomware dizendo que não vão atacar os hospitais, durante a pandemia, estão colocando os holofotes absurdamente nos cibercriminosos como se fossem filantrópicos, porém provavelmente estão apenas evitando evidenciar qualquer um que ataque os serviços de emergência.

Como os hospitais podem se tornar mais resistentes a ataques de ransomware

Existem medidas que os hospitais podem adotar para fortalecer as suas defesas, protegendo os seus sistemas, dados de clientes e operações.

Mantendo o software atualizado

Em maio de 2017, a variedade do ransomware WannaCry atacou milhões de computadores em todo o mundo, infectando os dispositivos com êxito, abusando de uma vulnerabilidade para a qual a Microsoft havia emitido um patch há dois meses antes do ataque em massa. Milhões de pessoas e empresas não aplicaram a atualização, a qual os teria protegido contra uma infecção WannaCry. Os hospitais também foram atingidos pelo ransomware.

É absolutamente crucial manter todos os softwares e sistemas operacionais atualizados, o tempo todo. A Microsoft emite constantemente patches de emergência. Recentemente, a Microsoft lançou um patch de emergência para uma vulnerabilidade crítica do Windows 10 batizada de “EternalDarkness“, uma vulnerabilidade wormable que afeta o protocolo SMB, o qual é usado para compartilhar arquivos e é o mesmo protocolo explorado na disseminação do WannaCry, há três anos. A Microsoft solicitou aos usuários para tomarem medidas imediatas, quanto à aplicação da atualização. As instituições de saúde devem levar a sério essa chamada quanto à esta ação.

Limitando o acesso

Também é recomendável que os hospitais tentem suspender todos os serviços disponíveis diretamente na internet. Os administradores de TI devem considerar uma lista de permissões estrita, quando se tratar de arquivos executáveis, para que apenas aplicativos conhecidos e confiáveis possam ser executados nos computadores dos hospitais.

Realizando treinamento de higiene digital

Assim como os hospitais treinam as suas equipes, no que diz respeito às melhores práticas de higiene, os funcionários também devem receber treinamento e orientação regulares sobre higiene digital. A equipe do hospital deve estar ciente dos golpes e táticas atuais usados pelos cibercriminosos, pois o e-mail continua sendo um dos métodos mais populares utilizados pelos cibercriminosos. Os funcionários devem ter cuidado com os e-mails de remetentes desconhecidos e evitar clicar em qualquer link ou fazer o download de anexos, a menos que tenham 100% de certeza de que são genuínos.

Fazendo backup regular de todos os dados importantes

Se o backup dos arquivos for feito, o ransomware perderá muito do seu poder, pois os sistemas podem ser restaurados e os dados recuperados. Documentos importantes, incluindo registros de pacientes, devem ser copiados regularmente, para garantir que os hospitais sempre tenham uma versão limpa dos seus arquivos, caso sejam criptografados. É melhor salvar os dados, tanto na nuvem como armazená-los em um dispositivo físico, apenas por precaução. Além disso, ter uma imagem única com todas as configurações padrão é útil quando um PC precisa ser restaurado, para que volte a ter um bom estado.

Etapas a serem seguidas em caso de infecção por ransomware

Infelizmente, as coisas podem acontecer e, portanto, é importante saber o que fazer se o pior ocorrer.

Etapa 1: Isolar imediatamente os dispositivos infectados

A primeira coisa a fazer, se um PC com Windows for atacado por ransomware, é encontrar e desconectar todos os computadores com e sem fio infectados, além de outros dispositivos conectados à rede. Isso impedirá que o ransomware se espalhe e infecte ainda mais computadores, tablets e smartphones, tornando-os reféns.

Durante este procedimento, recomenda-se que as vítimas também desconectem tudo o que estiver conectado com os dispositivos ligados à rede, incluindo armazenamento externo.

Para completar esta etapa, as vítimas devem verificar se algo estava conectado com o PC infectado. Se sim, deve-se verificar se há mensagens de resgate nesses sistemas também.

Etapa 2: Coletando logs e criando uma imagem forense

Depois que a máquina estiver isolada e não puder causar mais danos ao ambiente da rede, deve ser feita uma imagem forense do sistema ativo para análise de monitoramento. Isso congelará todos os logs e eventos, e irá melhorar consideravelmente a capacidade da equipe para descobrir de onde veio o ataque e como ele se comportou.

Etapa 3: Identificando o tipo de ataque de ransomware

Em seguida, as vítimas devem descobrir com qual tipo de ransomware estão lidando. Esse conhecimento pode ajudar a encontrar uma solução. Para auxiliar na determinação do tipo de ransomware em uma máquina, recomendamos o uso de No More Ransom's Crypto Sheriff . Fornecida pelo Centro Europeu de Cibercrime da Europol, essa ferramenta prática verifica os arquivos criptografados pelo invasor e a nota de resgate. Se o Crypto Sheriff reconhecer a

criptografia e tiver uma solução, ele oferecerá um link para baixar o programa de descriptografia necessário. Fóruns de soluções de problemas e suporte técnico para PCs também podem ser pesquisados, para encontrar informações sobre a variante do ransomware que precisa ser removida. Mesmo que seja novo, pode haver um meio de oferecer correção ou algo que os membros do fórum estejam trabalhando na busca de uma resolução.

Algumas infecções por ransomware renomearão arquivos e suas extensões (por exemplo: .exe, .docx, .dll) após criptografá-los. Ao visitar fóruns técnicos para obter ajuda, os usuários podem procurar por nomes e extensões dos arquivos criptografados. Cada um pode ajudar a orientar as discussões sobre a variedade de ransomware, que precisa ser removida.

Esses fóruns são fontes úteis e disponibilizam informações adicionais:

- Bleeping Computer Forums
- Computer Hope Forum
- Microsoft Community
- Reddit (r/Ransomware)

Etapa 4: Removendo o ransomware

É importante se livrar do malware subjacente, que mantém o PC como refém. Existem opções de remoção de ransomware para Windows 7, 8 e 10:

1. Verificar se o ransomware foi excluído por conta própria (o que geralmente acontece)
2. Removê-lo com uma solução antivírus, como o Avast Antivirus
3. Remover o programa malicioso manualmente
4. Reinstalar o sistema a partir de uma imagem

As pessoas afetadas e os administradores de TI poderão encontrar etapas mais detalhadas em um guia da Avast. O passo a passo pode ser conferido aqui. Enquanto todos tentamos nos proteger do vírus, é importante também continuar protegendo os nossos dispositivos contra vírus cibernéticos. Na Avast, estamos comprometidos em interromper essas ameaças e continuamos vigilantes à medida que a situação evolui. Mantenha a segurança, pessoal!

(*) **Michal Salat** é Diretor de Inteligência de Ameaças da Avast.

Fonte: **Portal Hospitais Brasil**, em 29.05.2020