A extorsão digital Ransonware e a perícia digital e computação forense.

O recente episódio envolvendo o worm WannaCry aclarou de forma única a ameaça muito comum atualmente, a qual muitas empresas e pessoas já experimentaram de forma trágica. O ataque ransonware. O WannaCry foi massificado com uso de um exploit, aparentemente obtido da NSA.

O exploit explorava uma desatualização do sistema Windows, da Microsoft, que lançou informações sobre como se proteger contra o worm, incluindo a implantação do patch MS17010, atualização do Windows Defender, bem como a não utilização do SMBv1.

O ransonware criptografa o disco das vitimas e exige um resgate para o envio da chave necessária para recuperar os arquivos. Estima-se mais de 74 países afetados em 45 mil ataques. No Brasil, inúmeros órgãos públicos ficaram fora do ar. Estes eventos demonstram a importância de prevenção, mas principalmente, de respostas forenses adequadas. O que um time de resposta pode imaginar é que basta desconectar a máquina infectada, impedindo que se prolifere pela rede, infectando as demais, reduzindo o poder do ataque. Mas a questão é: Como saber qual máquina foi a gênese do worm em uma rede?

A computação forense em Ransonware é embrionária, mas já tem valores e consenso em alguns pontos. Uma iniciativa interessante é o script PowerShell que, sabendo que o ransonware sobrescreve na NTFS arquivos por versões cifradas, é capaz de responder quando um arquivo é gravado, enviando e-mail e demonstrando as unidades mapeadas, logo, destinado à detecção e contenção do ataque. Pode-se inclusive tentar matar o processo relativo ao worm. [1]

Outra trilha valiosa é lecionada por Chris Brewer, da Nuix, que infectando-se com o CryptVault, realizou análise de rede, sistemas de arquivos e processos, de modo a determinar o host de origem do ataque, valendo-se ferramentas como Wireshark, Regshow, Processes Monitor e NetworkMiner.[2]

Algumas orientações são importantes diante de um ataque. Inicialmente, deve-se determinar qual tipo e versão do ransonware atacou a rede. Por exemplo, em sendo CryptoLocker, já se tem roteiros de recuperação de dados. [3]

Posteriomente a) deve-se determinar o vetor inicial do ataque, b) deve-se estimar a origem do mesmo, ou seja, como ele chegou à rede, e-mails em anexo, compartilhamento de arquivos, exploits, executáveis ou ameaças externas; c) pode ser possível identificar o numero da carteira bitcoin no e-mail de resgate.

A perícia poderá examinar evidências digitais de sistemas comprometidos para levantar artefatos de origem e de conexões remotas e demais dados. Uma outra fase pode, dependendo do ransonware, resultar em um trabalho de decodificação dos arquivos. Comumente, porém, o perito poderá ajudar no processo de negociação, com redução do valor do resgate afim de recuperar arquivos críticos.

Por fim, minimizado o dano causado, a equipe de computação forense poderá atuar na remediação, juntamente com a equipe de segurança digital, atuando para evitar explorações no futuro e cuidando para que o ambiente esteja realmente limpo.

As recomendações adicionais de respostas para um ataque desta natureza são a) desconectar o dispositivo afetado da rede, evitando que ataque acesse as unidades compartilhadas; b) muito cuidado com ações impensadas, como tentativas de recuperação (adicionar drives) em ambientes ainda infectados ou cópia de arquivos; c) conheça quais as opções diante do ataque e d) conte com o apoio de uma consultoria em computação

forense especializada, sobretudo para a cópia bit-a-bit da unidade encriptada para eventualmente ser decodificada no futuro, caso nada seja possível ser feito no momento.

Um ataque de ransonware não precisa ser sobre dinheiro, podendo ser um ataque a uma delegacia de polícia ou órgão público para queima de provas, por exemplo. E se o atacante não quer dinheiro, os dados nunca mais serão recuperados (Como o ocorrido com Departamento de policia de Cocrell Hill, em caso recente.) Neste sentido, prevenção também é fundamental.

Portanto, contanto não se possa afirmar ser possível em todos os casos a recuperação integral dos arquivos, resta demonstrada que o papel do perito digital é indispensável na contenção, coletas e preservação das evidências, bem como na minimização do dano, com a possibilidade de identificação da origem do ataque, bem como de recuperação parcial ou futura dos dados.

Notas:

[1] http://www.freeforensics.org/2016/03/proactively-reacting-to-ransomware.html

[2] https://www.nuix.com/blog/ransomware-part-4-analyzing-results

[3] https://threatpost.com/forensics-method-quickly-identifies-cryptolocker-encrypted-files/103049/

José Antonio Milagre
Advogado. Perito em Informática. Mestre e Doutorando em Ciência da Informação pela UNESP, Coordenador da Pós-Graduação em Computação Forense pelo ESB – Brasília. Árbitro de tecnologia da CIAMTEC.br
E-mail: assessoria@josemilagre.com.br Website: www.direitodigital.adv.br