Como os “hackers” agiram no ataque ao Superior Tribunal de Justiça do Brasil?

Investigação, lições e como se proteger do ransomware

*José Antonio Milagre**

Um dos maiores ataques cibernéticos do país indisponibilizou serviços do Superior Tribunal de Justiça Brasileiro (STJ). Estima-se que o Ministério da Saúde também tenha sido atingido. Após ter dados críticos criptografados, os técnicos da corte encontraram um pedido de resgate.

Ao que identificado, o STJ foi vitimado por uma ameaça conhecidíssima, nada de “alta tecnologia”, mas um ataque de ransomware, “sequestro de dados”, códigos automatizados que ao infectarem máquinas, criptografam arquivos com diversas extensões, ou mesmo cifram o disco todo, exigindo o pagamento em bitcoins.

No caso do STJ, o ataque criptografou os arquivos, renomeando as extensões, aparentemente, para *. Sth888. Como prova de que podem reverter o conteúdo, pedem que a vítima envie qualquer arquivo menor que 900 KB e devolverão descriptografados.

Assim, bases de dados críticas, sistemas, servidores web e softwares são paralisados, causando indisponibilidade de serviços e grandes transtornos. No caso, até audiências foram paralisadas. Trata-se de uma ameaça onde o que não se falta são medidas “preventivas” para evitar que criminosos tenham sucesso com o golpe digital. (Já tratei inclusive deste tema no meu canal em: *Ransomware: Como evitar, remover, descriptografar e descobrir como foi infectado? 2020 José Milagre* *https://www.youtube.com/watch?v=EPJwP1rRsq8*).

Muitos poderiam pensar que um Tribunal estruturado e com um grande orçamento, jamais seria vítima de uma ameaça tão conhecida, para qual existem recursos preventivos diversos. Porém, a invasão ao STJ e a outros órgãos públicos nos faz refletir sobre alguns pontos:

a) Não importa o quão a empresa invista em infra-estrutura em seu ambiente, na nova forma de trabalho, home office, a vulnerabilidade pode estar no elo mais fraco da corrente, ou seja, as máquinas vulneráveis dos trabalhadores, que acessam a VPN ou rede da empresa;

b) Até mesmo ameaças conhecidas, se não tratadas com medidas técnicas e organizativas, podem impactar grandemente em dados e na disponibilidade de sistemas; Um exemplo de boa prática é a adoção de backups e o estabelecimento de um *disaster recovery plan*.

c) Uma estrutura de resposta a incidentes jamais será eficaz se não estiver formalmente constituída e preparada com antecedência, com processos claros para compreensão do incidente, se evolve dados pessoais ou se há a necessidade da perícia em informática, para que se possa identificar e apurar o modus operandi e a possível autoria.

Os criminosos podem responder, de acordo com a situação, dentre outros delitos, por invasão de dispositivo informático e também pelo delito de interrupção ou perturbação de serviço informático, ou de informação de utilidade pública, crimes previstos no Código Penal Brasileiro e Lei 12.737/2012 (Carolina Dieckman).

No entanto, no caso do ataque de ransomware, tão dificultoso quanto descriptografar os dados sem a chave de reversão (o que demandaria muito poder de processamento, diante da complexidade dos algoritmos), é a apuração da autoria ou dos responsáveis. A perícia digital e em informática lidará com origem incerta, além da dificuldade de apurar a conta de

destino do resgate, considerando que os criminosos recebem em criptomoedas e as transações na Blockchain podem não indicar muito sobre o recebedor.

Importante destacar, igualmente, que de acordo com a Lei Geral de Proteção de Dados, os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado, ou ilícito.

Mais que isso, deverão comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, em prazo razoável, indicando a descrição da natureza dos dados pessoais afetados, as informações sobre os titulares envolvidos, a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial, os riscos relacionados ao incidente e as medidas que foram ou que serão adotadas para reverter, ou mitigar os efeitos do prejuízo.

Logo, é dever do órgão apurar se existiu ofensa a dados pessoais e ser transparente a respeito, nos termos da legislação nacional de proteção de dados.

Ferramentas e kits que permitem que qualquer pessoa aplique o ransomware e se torne um criminoso, com alguns cliques, são facilmente encontradas na rede. Pacotes efetivos e "atualizados" são vendidos na deep web, inclusive com disparos de e-mails "*pishing*" e outras formas mais sofisticadas de infecção, como o carregamento do código a partir do navegador, com o acesso a um site infectado. Em sentido oposto, as técnicas de perícia em informática para rastreio da Blockchain em busca do destino do dinheiro produto de crime engatinham e as transações em criptomoedas para fins ilícitos constituem um grande desafio para peritos de informática e investigadores

digitais.

Deste modo, o ransomware, conquanto ameaça conhecida, continua em alta e muito efetiva, lesando de pequenos empresários e grandes cortes, sobretudo diante dos descuidos com proteção de dados e cópias de segurança, e como visto, a prevenção continua sendo a melhor forma de proteção contra este problema.

Prof. MSc. José Antonio Milagre, é perito em informática, advogado especialista em crimes cibernéticos e direito digital, Mestre e Doutorando em Ciência da Informação pela UNESP, Pesquisador do Nucleo de Estudos em Web Semântica e Análise de dados – NEWSDA-BR da Universidade de São Paulo (USP), Diretor do Instituto de Defesa do Cidadão na Internet – IDCI. Autor pela Editora Saraiva em co-autoria com o Professor Damásio de Jesus, dos livros e "Marco Civil da Internet: Comentários à Lei 12.965/2014" e "Manual de Crimes Informáticos". É colunista da Rádio Justiça/STF.

consultor@josemilare.com.br