Ataque cibernético mundial comprova a insegurança na internet

Desde a última sexta-feira (12/5), o planeta assiste alarmado um ataque mundial cibercriminoso, com a utilização de um vírus de "resgate", o chamado *ransomware*, que fez mais de 200 mil vítimas, espalhadas em ao menos 150 países no mundo (segundo o diretor do Serviço Europeu de Polícia – Europol, Rob Wainright), tendo se disseminado, em grande parte, por meio de e-mails infectados pelo vírus *WannaCry*.

O *ransomware* é um tipo de vírus que se aproveita de uma vulnerabilidade do sistema Windows (já corrigida, para quem atualizou o sistema, em 14 de março, segundo a Microsoft) e que sequestra, através da criptografia, os arquivos digitais salvos no computador da vítima, ou em sua rede, impedindo a vítima de acessá-los. O valor do "resgate" para a devolução ao acesso aos arquivos deve ser pago em bitcoins (moeda digital que dificulta o rastreamento da transação), cobrando-se em torno de US$ 300, por máquina.

No Brasil, o Tribunal de Justiça de São Paulo também sofreu ataques virtuais naquela data, seus funcionários foram orientados a desligarem os computadores e o seu site ficou fora do ar. Também tiraram sites do ar e/ou desligaram seus computadores: o Ministério Público de São Paulo, a Petrobras, o Instituto Nacional do Seguro Social (INSS), tribunais de Justiça em todo o país, o Itamaraty e o Instituto Brasileiro de Geografia e Estatística (IBGE).

Para se ter uma ideia dos riscos deste crime, naquele dia 12 de maio, somente no Reino Unido, pelo menos 16 hospitais públicos foram alvos destes ataques, que se utilizaram de *ransomware* gerando dificuldades ou impedindo o acesso aos prontuários dos pacientes, atrapalhando a logística das ambulâncias e de outros socorros, colocando, assim, diversas vidas em risco.

Pesquisa feita pela Trend Micro, empresa de segurança na internet, mostra que o crime de sequestro de dados/informações, com a utilização do *ransomware* não é novidade no mundo do cibercrime, uma vez que, nesta análise, do ano de 2016, de 300 empresas brasileiras, 51% delas já tinham sido vítimas do *ransomware*, sendo esse, o crime digital mais cometido no ano de 2016.

Os especialistas já indicavam desde 2015, ano das primeiras aparições deste crime, que, nos anos seguintes, esse tipo de ataque seria uma tendência na internet e bateria recordes, e depois do ataque em massa ocorrido, ficou patente que pouco ou nada foi possível fazer para evitar essa previsão.

Ao analisar todos os cibercrimes, no ano de 2016, o Brasil foi o quarto país que mais sofreu com estas atividades criminosas, que causaram um prejuízo de R$ 32 bilhões, segundo o relatório *Norton Cyber Security Insights*, enquanto que, no mundo, o valor do prejuízo foi de quase R$ 400 bilhões.

Pela lei brasileira, o cibercriminoso que pratica esta conduta, utilizando-se do vírus *ransomware* e pedindo o "resgate", responde pelo crime de extorsão, previsto no artigo 158 do Código Penal, com pena prevista de reclusão de 4 a 10 anos, e multa.

No caso do crime de extorsão com a utilização do *ransomware*, existe o constrangimento mediante grave

ameaça (da não recuperação dos dados), com o intuito de obtenção de vantagem econômica indevida, ou seja, o pagamento do “resgate”. Vale ressaltar que tal imputação independe do efetivo pagamento, já que é um crime formal, ou seja, não é necessária a produção do resultado para a sua consumação.

Portanto, para quem não acreditava na possibilidade de ocorrer um ataque virtual desta magnitude, fica o alerta de que não há segurança absoluta na internet, sendo necessário manter os sistemas operacionais, backups e antivírus sempre atualizados, a fim de minimizar os efeitos desta verdadeira guerra virtual.

Date Created
17/05/2017