

Por Thiago Madeira de Lima (*)

Vírus que "sequestram" dados dos usuários ameaçam a segurança de empresas em todo o mundo

Recentemente uma grande empresa de soluções de segurança divulgou um estudo que aponta o Brasil como um dos maiores propagadores de vírus do mundo. Somos o décimo país no ranking mundial e o primeiro na América Latina. Muito disso se deve aos hábitos dos usuários de internet no país, que costumam ser descuidados na hora de abrir e compartilhar informações, mesmo que manualmente.

Mais preocupante do que esse cenário, é o fato de que, nós brasileiros, somos a população mais exposta a um tipo de vírus que vem causando muitos transtornos em usuários domésticos e corporativos – os ransomwares.

Trata-se de uma categoria de malware – aplicações maliciosas que acessam sistemas clandestinamente – que, literalmente, sequestram os dados do computador infectado. O vírus criptografa, com códigos fortíssimos, todas as informações do usuário. Em seguida, cyber-criminosos cobram o resgate dos dados, normalmente via bitcoins ou outras operações não rastreáveis.

Apesar do recente crescimento de dificuldades ocasionadas pelos ransomwares – a incidência deste tipo de ataque aumentou 35% em 2015, de acordo com o mesmo estudo anteriormente citado – o problema não é novo. A primeira vez que um caso de sequestro de dados foi sinalizado foi em 1989.

Porém, foi somente na última década que o termo ganhou atenção especial, graças a um vírus conhecido como Gpcode. De lá para cá, uma infinidade de novos ransomwares foi criada no mundo da tecnologia, como o Simplocker, que afeta dispositivos Android, e o temido Cryptolocker, que ataca o sistema Windows.

O risco que essas ameaças representam, sobretudo às empresas, é imenso. Portanto, os dados e informações de uma empresa devem ser tratados como um ativo valioso. Medidas básicas de proteção como, manter os softwares atualizados, o firewall ativado e evitar clicar em e-mails e programas estranhos, podem ajudar a evitar uma grande dor de cabeça.

No entanto, a melhor prevenção contra os ransomwares ainda é o bom e velho backup. É importante conscientizar os gestores de negócios que a cópia periódica de arquivos importantes em um serviço de nuvem seguro garante que não haverá problemas maiores no caso de uma infecção do sistema físico da empresa.

Se prevenir contra vírus, especialmente ransomwares, pode ser determinante para a saúde de um negócio. A proteção ideal para dados e informações corporativas não requer um alto investimento. Com a oferta existente de serviços de nuvem e contando com um suporte de TI de confiança, não há razões para deixar o backup de lado.

(*) **Thiago Madeira de Lima** é diretor executivo da [Penso Tecnologia](#).

Fonte: [Migalhas](#), em 13.05.2016.