Autoridades dos EUA advertem bancas sobre surto de ransomware

As águas da navegação na Internet estão cada vez mais turbulentas. A World Wide Web, além dos perigos de *hackers*, está infestada de espécies maliciosas de softwares, chamados genericamente de *malwares*, como vírus, *worm*, *trojan horse*, *spyware*, *adware*, *scareware* e *ransomware*.

O *ransomware* é o *malware* da vez. Atualmente, é o preferido dos criminosos cibernéticos, porque é mais lucrativo e mais fácil de operar do que seus congêneres. *Ransomware* é uma espécie de sequestro, que é resolvido mediante pagamento de resgate (daí a palavra "ransom"). O criminoso bloqueia o acesso ao sistema de computação de uma organização e só desbloqueia após o pagamento. Às vezes recebe o resgate e não desbloqueia.

De acordo com um relatório recente da empresa de segurança Kaspersky Lab, no período de janeiro a setembro deste ano a taxa de ataques de *ransomware* aumentou de um a cada dois minutos para um a cada 40 segundos. E as variações de *ransomware* aumentaram para 32.091 no primeiro trimestre do ano. Até agora, no ano, foram detectadas cerca de 62 mil novas famílias de *ransomware*.

Isso significa que os criminosos cibernéticos não respeitam mais ninguém. A essa altura, nem mesmo os advogados (ou escritórios de advocacia) que poderão, um dia, ter de representá-los em algum tribunal.

O problema se tornou tão sério que, nesta semana, procuradores-gerais dos estados de Nova York, Texas, Pensilvânia, Maryland e Flórida, entre outros segundo o Jornal da ABA (*American Bar Association*) divulgaram informes à imprensa, quase que simultaneamente, advertindo sobre um surto de *ransomware* especial para advogados e escritórios de advocacia. Seccionais da ABA em alguns estados também divulgaram advertências.

Em nota, o procurador-geral do estado de Nova York advertiu as bancas que os criminosos estão enviando e-mails a advogados que se assemelham às comunicações oficiais de seu departamento. O e-mail, cujo assunto é "The Office of The State Attorney Complaint, se refere a uma suposta queixa de um cliente contra o advogado ou contra a banca.

O texto, que contém redação e termos costumeiros da advocacia, informa que uma queixa foi apresentada contra a banca e que ela tem 10 dias para protocolar uma resposta (*rebuttal*). "A queixa pode ser vista no link abaixo", diz o e-mail. "As respostas não podem exceder 15 páginas e podem se referir a documentos ou provas adicionais, que estarão disponíveis a pedido…".

A seccional da ABA do Texas também advertiu os advogados sobre um suposto e-mail da Procuradoria Geral do estado. O texto é igual e o link para ver a queixa é exatamente o mesmo do e-mail que circula em Nova York. O perigo está sempre em clicar no link.

A seccional da ABA de Maryland advertiu os advogados sobre o suposto e-mail da Procuradoria Geral e acrescentou uma outra armadilha: e-mails com o assunto "nos veremos no tribunal", enviados por algum outro advogado, cuja conta de e-mail foi invadida pelos criminosos cibernéticos. Assim, o advogado acredita que é um e-mail legítimo e clica no link para ver o documento. E tudo não passa de um *ransomware*

.

Ao contrário de outros *malwares*, o *ransomware* é um mal que não tem cura — nem mesmo um tratamento paliativo ou para prolongar a sobrevivência. É fatal. A única medida eficaz contra o *ransomware* é a prevenção.

Recomendações preventivas
Todos os sites que tratam do assunto recomendam não clicar no link e não abrir documentos anexados ao e-mail. O procurador-geral de Nova York recomenda deletar o e-mail e telefonar para o departamento para falar sobre o e-mail e checar se há, realmente, algum problema a ser resolvido.

Algumas mensagens trazem um número de telefone. A recomendação é nunca ligar para esse número, porque quem vai atender é um membro de uma quadrilha. É preciso buscar o número do suposto remetente do e-mail por outros meios. Da mesma forma, nunca se deve responder a esses e-mails.

O site CSO diz que é preciso treinar o pessoal de TI sobre *ransomware* (e outros *malwares*), porque, em muitos casos, eles não sentem o peso da responsabilidade de perder todos os dados, documentos e outros arquivos do escritório como o advogado e, por isso, são mais descuidados.

Os programas de proteção contra *malwares* devem ser atualizados frequentemente, porque podem ajudar a prevenir ataques de criminosos cibernéticos.

No entanto, a melhor medida é manter todos os arquivos e programas do sistema de computação do escritório em um HD externo ou na nuvem. Se tudo for sistematicamente atualizado, pelo menos será possível recuperar todo o ativo de computação do escritório.

Embora a convicção geral seja a de que o *ransomware* é um mal que não tem cura, o site No More Ransom, produzido por empresas de segurança, diz que pode haver uma ou outra ferramenta que decifre a criptografia de um ou outro *malware*. E sugere que chequem o site.

A Kaspersky Lab recomenda que nunca, em hipótese alguma, se pague o resgate. Os acontecimentos já mostraram que quem paga, provavelmente por desespero, sofrerá outro ataque de *ransomware* e, desta vez, o pedido de resgate será bem maior. Em vez disso, o ataque deve ser relatado às autoridades.

Para advertir os clientes
Todos esses ataques são mais comuns em países com moedas fortes, embora a moeda digital *Bitcoin* seja o principal meio de pagamento — e também se use transferências bancárias, serviços de voucher, etc.

Nos Estados Unidos, os cidadãos também são vítimas cotidianas de e-mails maliciosos. E o mais comum é o e-mail supostamente vindo de um tribunal que intima o cidadão para comparecer à corte ou servir como testemunha, no qual ele tem de clicar em um link (ou abrir um anexo) para ver o documento enviado pelo tribunal. Ao fazê-lo, se torna vítima de um *malware* ou de *phishing*.

Date Created
14/12/2016