ALERTA CIBERCRIME

23 de janeiro de 2019

Extorsão por *email*

1. Está em curso uma campanha criminosa de extorsão por via de correio eletrónico. O propósito criminoso de tal atuação é o de convencer vítimas a pagar quantias monetárias, em *bitcoins*, sob a ameaça de divulgação pública de dados, imagens ou informações pessoais das mesmas.
Trata-se de ações provenientes de múltiplos agentes, independentes uns dos outros que, replicando os vários modos de atuar, prosseguem interesses individuais, de lucro ilegítimo.

2. O processo fraudulento começa com a expedição, para destinatários previamente selecionados, de mensagens de correio eletrónico. Nessas mensagens, o remetente diz ser conhecedor da senha (*password*) de correio eletrónico do destinatário. Adianta que, por essa mesma razão, logrou aceder ao computador do mesmo.
Foi recolhida informação que permite concluir que os remetentes destas mensagens terão obtido os endereços de correio eletrónico das vítimas, e as correspondentes *password*, em listagens disponíveis na Internet. Tais listagens são resultantes de dados conseguidos em diversos ataques informáticos realizados no passado a diversos servidores.
Em geral, as *password* em causa são já antigas e não estão a ser utilizadas. Porém, o mero conhecimento das mesmas pelos agentes criminosos tem provocado inquietação nas vítimas.

3. Em regra, as mensagens referem explicitamente provir de um *hacker*. Os vários textos referem que tal *hacker* logrou introduzir no computador, ou *smartphone*, da vítima, programas informáticos maliciosos, ou "*malware*" (é frequente a referência a "*trojans*"). Com esta alusão, os autores das mensagens pretendem convencer as vítimas de que, efetivamente, tiveram acesso aos conteúdos guardados nos respetivos dispositivos. Por vezes, é mesmo mencionado o acesso a conteúdos de natureza íntima, sexual, e o registo de acesso a páginas na Internet dessa mesma natureza.

4. As mensagens dizem ainda, sempre, que o seu autor revelará o conteúdo da informação íntima a que teve acesso a pessoas incluídas na lista de contactos da vítima, caso não lhe seja efetuado um pagamento.
Em geral, a ameaça vem acompanhada de muita urgência, sendo concedido um prazo que varia entre 24 e 48 horas.

Quanto aos pagamentos solicitados, embora o sejam sempre em *bitcoins*, referem também sempre um valor em moedas com curso legal (foram registados pelo Gabinete Cibercrime exigências em euros, dólares americanos e libras esterlinas). Os montantes exigidos variam entre as centenas e os milhares de euros. As carteiras de *bitcoins* são também várias.
É ainda – e sempre –, feita a advertência de que as comunicações da vítima são monitorizadas e que, portanto, o recebimento e abertura da mensagem criminosa é do conhecimento do emissor da mesma.

5. Sublinha-se que as concretas mensagens deste tipo a que o Gabinete Cibercrime teve acesso terão, todas elas, sido expedidas para endereços de correio eletrónico disponíveis na Internet, em resultado de ataques informáticos ocorridos no passado – alguns deles há já vários anos. Por outro lado, as *password* indicadas às vítimas estão igualmente disponíveis na Internet e associadas a esses endereços. Em geral, as *password* eram já antigas e tinham sido substituídas.

6. Por outro lado, não se apurou, em caso algum, que os remetentes das mensagens tivessem efetivamente instalado "*malware*" nos computadores das vítimas. Ou seja, nos casos identificados, os remetentes destas mensagens procuraram explorar o desconhecimento das vítimas, invocando *intrusões* técnicas que efetivamente não realizaram – portanto, falsas.

7. Muitas das mensagens fraudulentas identificadas eram provenientes de servidores de *webmail* gratuitos. Noutros casos, as mensagens provinham de contas de correio eletrónico de terceiros, ilegitimamente acedidas com este específico e abusivo propósito.
Em geral, na expedição destas mensagens foram utilizadas ferramentas de anonimização, tendo em vista ocultar a origem da comunicação.

8. Sem prejuízo da recomendação de alteração da *password* de acesso à conta de correio eletrónico (que aliás deve fazer-se regularmente, por rotina), não há outra recomendação de segurança a fazer nestes casos: apenas ignorar a ameaça carreada pela mensagem, não respondendo ao seu remetente. Na verdade, nos casos identificados, estas mensagens são sucessivamente remetidas para muitos destinatários, a partir de informação disponível na Internet, não tendo o seu autor qualquer tipo de conhecimento das suas potenciais vítimas, nem qualquer tipo de acesso ao seu computador ou *smartphone*.
Nos casos registados, embora fosse *concedido* à vítima um prazo muito curto (de 24 ou 48 horas) para pagar um *resgate*, decorrido esse prazo nada aconteceu.