ALERTA CIBERCRIME

11 de fevereiro de 2021

Extorsão por *email* (divulgação de imagens de cariz sexual)

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 imagens ou informações pessoais das mesmas.
Trata-se de ações ilícitas, provenientes de agentes criminosos que procuram lucros ilegítimos.

2. O processo fraudulento começa com a expedição, para destinatários indiscriminadamente selecionados em bases de dados disponíveis na Internet, de mensagens de correio eletrónico. Nessas mensagens, o remetente diz que se infiltrou no dispositivo eletrónico da vítima, logrando aceder ao mesmo. Refere ainda que introduziu no computador, ou *smartphone*, da vítima, programas informáticos maliciosos, ou "*malware*" (é frequente a referência a "*trojans*", ou *cavalos de Troia*). Com esta alusão, o autor da mensagem pretende convencer a vítima de que assumiu o comando de todas as suas aplicações e funcionalidades (correio eletrónico, navegador de Internet, câmara fotográfica, etc.), tendo assim acesso aos conteúdos guardados nos seus dispositivos. Refere ainda que presenciou, por esta via, o acesso da vítima a páginas de cariz pornográfico na Internet, tendo gravado estes episódios.

3. As mensagens dizem ainda (sempre) que o seu autor revelará o conteúdo de 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 para pagamento que não ultrapassa as 48 horas.
Quanto aos pagamentos solicitados, embora o sejam sempre em *bitcoins*, referem por vezes moedas com curso legal (euros ou dólares americanos). Os montantes exigidos são da ordem das centenas de euros.
É ainda 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, bem como o serão eventuais comunicações com as autoridades de justiça criminal.

4. Ao contrário do que ocorreu com outras campanhas desta natureza, identificadas no passado, as mensagens da presente campanha a que o Gabinete Cibercrime teve acesso, são redigidas em português escorreito (no passado tinham sido identificadas mensagens dirigidas a cidadãos portugueses, mas normalmente redigidas em inglês ou traduzidas rudimentarmente por tradutores automáticos). Por outro lado, enquanto no passado as campanhas desta natureza eram indiscriminadamente dirigidas, para todo o mundo, para endereços de correio eletrónico disponíveis na Internet, neste caso, desta nova campanha, as mensagens visaram maioritariamente titulares de endereços de correio eletrónico de fornecedores de serviço de *webmail* com ligação a Portugal (sapo.pt, zonmail.pt, entre outros). Nalguns casos, visaram utilizadores de correio eletrónico de instituições públicas com domínios ".pt."
Como ocorreu em outras campanhas no passado, as mensagens identificadas nesta campanha provieram todas de fornecedores de serviço de *webmail*, baseados em diversíssimos países de diversas latitudes.

5. Importa sublinhar que não se apurou, em caso algum, que os remetentes das mensagens tivessem efetivamente instalado "*malware*" nos computadores das vítimas.
Por outro lado, também não foi identificado nenhum caso em que as supostas imagens comprometedoras, ou outros dados das vítimas, tenham sido reveladas. Nos casos registados, embora fosse *concedido* à vítima um prazo muito curto (até 48 horas) para pagar um *resgate*, a verdade é que decorrido esse prazo, nada aconteceu em nenhum dos casos.
Como se referiu, todas estas mensagens parecem ter sido expedidas para milhares de destinatários, de forma indiscriminada. Em nenhum dos casos o seu autor tinha qualquer conhecimento de quem era o destinatário da mensagem, nem sabia nada acerca do mesmo. Apenas pretendeu, fazendo "bluff", extorquir-lhe quantias monetárias. Se os destinatários destas mensagens não responderam às mesmas, o criminoso pura e simplesmente abandonou o assunto.
Ou seja, nos casos identificados, os remetentes destas mensagens procuraram apenas explorar o desconhecimento das vítimas, invocando *intrusões* técnicas que efetivamente não realizaram – portanto, falsas.

6. Sem prejuízo da recomendação, por mera precaução, de mudança regular das *password* de acesso aos dispositivos e às diversas contas, de correio eletrónico e outras, não há outra recomendação de segurança a fazer nestes casos: apenas ignorar a ameaça carreada pela mensagem, não respondendo ao seu remetente.