VÍRUS DA COVID-19 OU VÍRUS VIRTUAL?

Autores: Carla Ripoli Bedone e Lucie Antabi**

A expansão da criminalidade no âmbito cibernético não é uma novidade trazida pela pandemia do novo Coronavírus. A prática de delitos nesse contexto (denominados usualmente "*cibercrimes*") ocorrem desde o final do século XX, à medida que a *internet*[8] era aprimorada e alavancada em nível mundial. Pode-se afirmar que o que favorece o cometimento destes crimes é o anonimato, bem como a facilidade que tem o agente para praticar a infração. Muitas vezes perpetrados de sua própria residência, os autores utilizam-se de meios para mascarar sua verdadeira identidade, o que torna mais dificultosa a apuração da autoria.

Nesse contexto, se por um lado o isolamento social está ocasionando uma diminuição dos crimes patrimoniais do roubo e do furto, por exemplo, com a restrição do trânsito das pessoas nas ruas, por outro a prática de crimes cibernéticos vem sendo amplamente verificada. Isso porque as vítimas nesses casos se encontram massivamente confinadas em suas casas, o que naturalmente resulta em um acesso mais incidente à *internet* em tempos de pandemia. Assim, a vítima acaba por ficar mais vulnerável a ataques similares.

Segundo *site* da Polícia Federal, durante a crise pandêmica da Covid-19, os agentes "*utilizam campanhas falsas - compostas por meio de e-mails, links, mensagens por aplicativos, ligações telefônicas e outros canais – para obter dados bancários e informações pessoais*". [9]Os mecanismos utilizados consistem em: ***(i)*** **links** enviados por e-mail, SMS ou aplicativos de mensagens em nome de instituições bancárias, induzindo o indivíduo a preencher dados de cartões de crédito em formulários e fornecer dados de cartões de crédito e senha em ligações telefônicas; ***(ii) voucher*** **de auxílio emergencial,** em que são disparadas diversas mensagens por meio de aplicativos como *Whatsapp*, SMS, e-mails e até telefonemas, solicitando informações para cadastro dos beneficiários do auxílio emergencial aprovado pelo Governo Federal; ***(iii)*** **aplicativos maliciosos,** que solicitam informações ou se passam por órgãos do governo a fim de obter dados pessoais; ***(iv)*** **golpes usando o *Whatsapp***, com solicitações de empréstimos e transferências oriundas de contatos no referido aplicativo; e ***(v)*** boleto falsificado, com códigos de barras que podem ser facilmente alterados. [10]

Uma das vítimas de ataques cibernéticos neste contexto de pandemia foi a própria Organização Mundial da Saúde (OMS). Constatou-se que houve, neste período, um aumento de mais de duas vezes nos ataques cibernéticos contra a entidade, segundo um importante funcionário da organização. [11]

---

[8] Nos termos do artigo 5º, inciso I da Lei nº 12.965/2014 ("Marco Civil da Internet"), define-se "*internet*" como: *"o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes."*

[9]http://www.pf.gov.br/imprensa/noticias/2020/04-noticias-de-abril-de-2020/policia-federal-alerta-para-ameacas-ciberneticas e https://noticias.r7.com/brasil/pf-identifica-aumento-significativo-de-ameacas-ciberneticas-08042020

[10]http://www.pf.gov.br/imprensa/noticias/2020/04-noticias-de-abril-de-2020/policia-federal-alerta-para-ameacas-ciberneticas e https://noticias.r7.com/brasil/pf-identifica-aumento-significativo-de-ameacas-ciberneticas-08042020

[11]https://g1.globo.com/economia/tecnologia/noticia/2020/03/23/hackers-tentaram-invadir-sistemas-da-oms-em-meio-a-pandemia-de-covid-19.ghtml

Os *hackers* tentaram invadir o sistema da Organização, tendo o Vice-Presidente de segurança da informação da OMS declarado que ainda não foi possível descobrir a identidade dos autores, mas que a tentativa de invasão não foi bem sucedida. Os *hackers* intentaram, ainda, ativar um site malicioso que imita o sistema de e-mail interno da entidade. Ainda, alertou-se: *"as ações de hackers contra a organização e seus parceiros dispararam em meio à campanha do órgão global para combate ao coronavírus, que já matou mais de 15 mil pessoas no mundo."*[12]

Convém destacar que os agentes vêm se utilizando de *"Phishings"*, isto é, uma forma utilizada para enganar a vítima a revelar informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias, por meio do envio e-mails falsos ou direcionando a vítima a websites falsos.[13] Alguns exemplos de mensagens encaminhadas pelos agentes podem se constituir em *links* como "clique aqui para você receber seu auxílio do Estado", considerando que o Governo Federal disponibilizou o *auxílio emergencial*[14]; ou "clique aqui para ver se você está contaminado", tendo em vista que todos estão preocupados em saber se foram contaminados pela doença.

Ademais, há a divulgação de campanhas falsas em auxílio aos necessitados, no sentido de obter das pessoas que se filiam à ação dados bancários e informações pessoais. Esta é uma prática extremamente prejudicial não apenas para as vítimas que têm seus dados coletados, mas para as campanhas que são verdadeiras.

Pessoas que querem disponibilizar seus recursos financeiros para ajudar terceiros passarão a questionar a veracidade das campanhas, e, muitas vezes, por um medo absolutamente compreensível de terem seus dados coletados, acabarão deixar de fazer doações para ações que de fato existem.

Assim, no sentido de se prevenir destes ataques, a população deve se orientar por meio de fontes precisas e atualizadas, utilizando-se de *sites* e canais oficiais, a exemplo do Ministério da Saúde, Organização Mundial da Saúde, Portal Governo do Brasil, para verificar a veracidade da informação. Além disso, deve-se buscar também fortificar a segurança dos dispositivos, tendo em vista que atualmente é de extrema necessidade as pessoas se cercearem de cautela para que não sejam alvos dos agentes de crimes cibernéticos.

Conforme acima exposto, vivemos em tempos que exigem cuidados redobrados. Para lutar contra o vírus invisível da Covid-19 é necessário utilizar-se de álcool em gel, isolamento etc., e para combater o vírus anônimo dos *hackers*, imprescindível diligência redobrada ao navegar na rede.

***Carla Ripoli Bedone,** advogada criminalista atuante no escritório Fernando José da Costa Advogados. Pós-graduanda em Direito e Processo Penal pela Universidade Presbiteriana Mackenzie e graduada pela mesma instituição.

***Lucie Antabi**, advogada criminalista, atuante no escritório Fernando José da Costa Advogados, Pós-graduanda em Direito Penal Econômico pela FGV/SP e graduada pela FAAP/SP.

[12] https://g1.globo.com/economia/tecnologia/noticia/2020/03/23/hackers-tentaram-invadir-sistemas-da-oms-em-meio-a-pandemia-de-covid-19.ghtml-

[13] Definição conferida pelo *site:* https://www.avast.com/pt-br/c-phishing.

[14]https://gauchazh.clicrbs.com.br/coronavirus-servico/noticia/2020/04/golpistas-usam-auxilio-emergencial-para-tentar-obter-dados-sigilosos-de-vitimas-ck8qbrezu00pv01qwxlcw3at8.html