COVID-19 E O OPORTUNISMO CIBERNÉTICO

Danielle Jacon Ayres Pinto[1]

Não é novidade que situações limítrofes e de desestabilização da ordem causam uma quebra da sociabilidade e abrem espaços para novas possibilidade de infrações contra aqueles que são mais vulneráveis. Não seria diferente com a pandemia de um dos tipos de coronavírus, o COVID-19, declarada pela Organização Mundial da Saúde (OMS) em 2020.

Estamos assistindo situações que expõem os indivíduos ao perigo: presos fugindo em massa de cadeias, cidadãos se recusando a fazer testes, países se recusando a reconhecer a gravidade da doença, países fechando fronteiras e recusando receber cruzeiros deixando-os vagar pelos mares, voos cancelados e pessoas sem perspectivas de retorno a seus países de origem, uma incapacidade global de cooperação que vai na contramão do processo globalizante tão defendido e tantos outros obstáculos que mostram a dificuldade da sociedade em lidar com problemas de magnitude mundial.

Todavia, há um novo tipo de ameaça que o século XXI e as novas tecnologias trouxeram para situações limítrofes como a que se vive hodiernamente. São ameaças que não necessariamente agridem diretamente o indivíduo, mas sim, abusam de sua empatia, da solidariedade e, principalmente, do medo para extorquir informações, dados e dinheiro as pessoas.

Segundo o Centro Nacional de Cibersegurança de Portugal (CNCS) quatro tipos de ações praticadas na rede estão sendo utilizadas para cometer crimes nesse período de pandemia, e contra isso devemos estar atentos. São eles:

1) **As campanhas de engenharia social** – grupos estão se fazendo passar com organizações internacionais, ONG´s e outros tipos de entidades e através de email-s, sms ou mesmo as redes sociais criam campanhas falsas de informação para conseguir acesso aos dados dos usuários. Essa tática muito conhecida como *phishing* é prática comum no mundo virtual. O objetivo é fazer com que o indivíduo

[1] Pós-Doutora em Ciências Militares – ECEME, pesquisadora do Projeto Pró-Defesa IV - Ciência, Tecnologia e Inovação em Defesa: Cibernética e Defesa Nacional. Professora da Pós-Graduação em Relações Internacionais da UFSC e coordenadora do GEPPIC e GESED. Contato: djap2222@yahoo.com ou danielle.ayres@ufsc.br

clique em um link através dessas plataformas acima referidas e a partir disso tais grupos criminosos passam a ter acesso aos dados dos usuários ou até mesmo aos seus arquivos nos computadores e celulares. Normalmente a ideia é utilizar desses dados para cometer crimes no futuro ou mesmo para instalar vírus de computador que prejudiquem os usuários.

2) **SMS que pedem recursos financeiros** – O SMS (*Short Message Service*) é uma ferramenta comum para que empresas acessem os usuários oferecendo ou vendendo qualquer tipo de serviço via telefonia móvel (celulares). Tais serviços normalmente oferecem produtos que acabam por sair mais caro ao consumidor do que o informado, tornado tal prática algo sempre questionável junto aos usuários. Mas em tempos de pandemia e medo, não só esse tipo de expediente é utilizado através dos SMS. Grupos estão enviando mensagens de texto com falsas ofertas de vacinas contra o COVID-19, onde para usufruir de tal benesse o indivíduo deve fazer um depósito através do link enviado a ele. Daí, o medo e a auto-preservação falam mais alto, e mesmo sendo constantemente informado pela mídia tradicional sobre o cenário da pandemia, o indivíduo engana-se e acredita numa possível vacina e na necessidade de paga-la antecipadamente para que possa ter acesso. Quando percebe que é um golpe, efetivamente, já é tarde. Não é possível reaver o dinheiro e é muito difícil de conseguir rastrear quem foi o autor de tal ação criminosa.

3) **Campanhas falsa para recolha de donativos** – Nos últimos tempos está sendo comum ver campanhas para arrecadação de recursos para diversos motivos: pesquisadores que precisam de dinheiro para viajar, pessoas doentes que precisam de dinheiro para tratamento, etc. Todavia, apesar de todos os mecanismos para efetivamente comprovar a veracidade desses *Crowdsourcing* ainda existe um lapso digital que possibilita a fraude, assim, durante a pandemia de COVID-19 está sendo possível ver em países onde o problema já está a mais tempo ocorrendo a criação de campanhas falsas para arrecadação de recursos para compra de medicamentos, mantimentos ou outros tipos de utensílios essenciais para ultrapassar a pandemia com alguma segurança. A doação é feita normalmente por transferência bancaria ou depósito, o que permite o rastreamento para onde o dinheiro está indo, porém, o problema frente a esse golpe não é o destino do dinheiro em si, mas o cumprimento da promessa de utilizar dos recursos para os fins que foram

solicitados. Até que se descubra o que ocorreu, o dinheiro já se perdeu e o usuário dificilmente irá recuperá-lo.

4) **Aplicativos maliciosos** – Os aplicativos, em especial os voltados para celulares, passaram a ser o novo fenômeno do mundo digital. Quase todos os serviços digitais estão ligados a um aplicativo que através de uma interface amigável faz com que usuários comuns possam obter acesso as informações, orientar-se por ruas e estradas, comprar produtos, vender produtos, alugar casa, alugar quartos de hotéis e etc. Mas nessa época de pandemia os aplicativos passam a ter uma função mais social, são criados para informar e monitorar as pessoas, e nessa esteira, surgem os aplicativos verdadeiros e os falsos, que tem por objetivo obter vantagens ilícitas. Assim, aplicativos estão sendo criados e disponibilizados aos usuários como meio para se informar sobre a COVID-19, mas ao invés de fazerem isso o objetivo real de tais aplicações digitais é infectar o aparelho com um vírus e exigir um pagamento para que os dados dos usuários não sejam definitivamente corrompidos e para que ele possa voltar a ter acesso aos mesmos. Esse tipo de prática é conhecida como *Ransomware*, onde o objetivo é pedir um resgate para repor as informações dos aparelhos pessoais dos indivíduos que foram bloqueadas por grupos criminosos. Assim, utilizando da vontade de obter informação, da necessidade de monitoramento e da busca por precaução através de meios digitais, criminosos estão agindo para obter lucros através de ameaças que dificilmente podem ser revertidas, afinal a maioria das pessoas e instituições ainda não possuem backups de suas informações e arquivos essenciais.

Como então é possível precaver-se contra tais ações ilegais, principalmente em um período de exceção como o de uma pandemia?

A recomendação continua sendo a de ter cuidado com o que se acessa e que se baixa da internet. É preciso que as pessoas sejam ciosas de ler as condicionalidades de cada aplicativo, que busquem informações sobre a veracidade das campanhas de renomadas instituições e que evitem entrar em links que desconheçam completamente a fonte, mesmo que seu conteúdo seja de alto apelo emocional para situações extremas, como a atual pandemia de COVID-19.

Mas não só as pessoas são alvos desse novos oportunistas digitais, já há relatos de que hospitais estão sendo atacados ciberneticamente durante a pandemia, um deles segundo a reportagem

do site ZDNet, especializado em temas de tecnologia, é o Brno University Hospital na República Checa. O Hospital não informa qual tipo de ataque sofreu, mas foi obrigado a desligar por completo todo seu sistema de tecnologia e informação, sendo forçado a enviar pacientes para hospitais próximos e cessar atendimento emergenciais do COVID-19.

As possibilidades de ataques são muitas, as motivações são as mais diversas, e os cenários de crises como o atual os mais propícios para que criminosos explorem a boa vontade e a necessidade de indivíduos e instituições que possuem grande parte da sua vida ligada ao mundo digital. Frente a isso, precaução continua sendo a palavra de ordem para os indivíduos e as instituições, porém, os Estados precisam encarar tais situações como novas ameaças a sua percepção de defesa e soberania. Em situações pandêmicas e de alta carga de emocional para a sociedade, qualquer perturbação da ordem que não seja relacionado a doença, mas sim ao oportunismo de criminosos, deve ser tida como uma ameaça direta a soberania e a ordem do Estado, e como tal enfrentada com políticas públicas sérias e estruturais. A pandemia de COVID-19 é uma excelente oportunidade para se pensar novos protocolos digitais de proteção e como o Estado deve agir frente a tais ameaças.

As lições da pandemia de COVID-19 estarão num futuro próximo ligadas a muitas temáticas da saúde, mas também, servirá efetivamente de cenário para que todo os atores estatais e os próprios indivíduos possam se preparar cada vez mais para vida digital, *locus* comum da vida contemporânea, e tudo que ela envolve de assertivo e de ameaça.

Referências do texto e sites para se informar mais sobre possíveis ameaças digitais em época de COVID-19:

ONU Cybersecrutity - https://unite.un.org/services/information-security

Ministério da Defesa do Brasil - https://www.defesa.gov.br/

Homeland Security USA - https://www.dhs.gov/topic/cybersecurity

Agência da União Europeia para Cibersegurança - https://www.enisa.europa.eu/

Centro Nacional de Cibersegurança de Portugal - https://www.cncs.gov.pt/

Reportagem do ZDNet “Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak” publicada em 13/03/2020 - https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/

ZDNet – Sessão de Negócios e Tecnologia e Pandemia de COVID-19 https://www.zdnet.com/topic/coronavirus-business-and-technology-in-a-pandemic/