Impacto dos Ataques Cibernéticos Durante a Pandemia

Francisco Ivanilso S. Araujo[1], **Francisco Camilo de Lima Filho**[1], **Francisco Evenilson Liandro Pinheiro** [1], **Ana Kely Lopes Ferreira** [1] **Wladimir Araújo Tavares** [1]

[1]Campus Quixadá – Universidade Federal Ceará (UFC)
Caixa Postal 6001 – 63.900-000 – Quixadá – CE – Brasil

{ivanilson.soares, caamilolima,evenilsonlp wladimirufc}@gmail.com

{kely}@alu.ufc.br

Resumo. *Descreve-se neste trabalho uma análise das formas de ataques que estão acontecendo, ele descreve algumas técnicas que são mais utilizadas atualmente e possíveis formas de evitar os ataques. Com isso foi realizado um questionário para saber como os usuários se comportam em suas redes sociais. Salienta-se que o trabalho tem o objetivo relatar a ação dos hackers nas redes sócias e em grandes empresas.*

Abstract. *This work describes an analysis of the forms of attacks that are happening, it describes some techniques that are more used today and possible ways to prevent attacks. With this, a questionnaire was carried out to find out how users behave on their social networks. It should be noted that the work aims to report the action of textit hackers on partner networks and large companies.*

1. Introdução

Em meados dos anos de 1990 o famoso *hacker Kevin Mitnick* ajudou a popularizar a expressão "engenharia social", que é um dos ataque mais simples para se conseguir dados dos usuários. Sendo seu principal objetivo enganar algum individuo fazendo com que a vitima divulgue informação de sua empresa ou vida social.

No Brasil os ataques cibernéticos vem crescendo de forma alarmante, tendo em 2007 alcançado a marca de 205 milhões de ataques, segundo Douglas Rocha(2019), sendo equivalente a uma pessoa por ataque, vale ressalta que esses ataques são feitos em computadores pessoais, empresas e até em hospitais.

Em meado de março de 2020, o mundo conheceu a doença COVID-19, transmitida por um vírus da família coronavírus. O novo coronavírus (*SARS-CoV-2*) começou a sua disseminação em por volta de novembro de 2019 na cidade de Wuhan na China. Com isso, diversos chefes governamentais decidiram adotar o isolamento para tentar frear a onda de infectados para não causar o colapso dos hospitais, entretanto pessoas mal intencionadas começaram a realizar ataques de engenharia social e *Phishing*, que é um crime de enganar pessoas para compartilhar informações confidenciais fazendo com que seja possível conseguir efetuar o roubo de dados ou informações que podem ser usadas para conseguir dinheiro de suas vitimas.

Tendo em vista o avanço da pandemia pelo mundo e com grande parte da população em quarentena, começaram a agravar vários problemas entre a população como

ansiedade, depressão, desseminação de fake news. Essa situação tornou-se um ambiente fértil para que *hackers* desenvolvessem ações maliciosas através do envio de mensagens pelos aplicativos de rede social como *WhatsApp* e *Instagram* com o objetivo de fazer com que os portadores dos dispositivos realizassem a leitura do texto de distração e acessassem links no final do texto ou compartilhasse a mensagem para amigos e familiares.

Por exemplo, uma das mensagens que mais foi compartilhada nas redes sociais continha a seguinte frase, "A Netflix decidiu liberar o acesso a sua plataforma de filmes e séries pelo período de isolamento das pessoas, mas é por pouco tempo o cadastramento! Corre no site https://netflix-usa.net/?periodo-de-isolamento-gratis.". A mensagem não é prejudicial, mas o link contido no final da mensagem pode causar grande prejuízo e complicações para os usuários pois o link pode ser direcionada para páginas que iram solicitar dados do indivíduo fazendo com que o *hacker* atinga seu objetivo e comesse a manipular o usuário de diversas formas.

Neste trabalho, analisamos as respostas de um questionário simples com 8 perguntas sobre o cotidiano dos usuários em redes sociais: número de anúncios recebidos, compartilhamento de informações com amigos, acesso de sites desconhecidos, cuidado com as informações pessoais, recebimento de ligações de números desconhecidos e o conhecimento sobre o termo engenharia social. Essas informações foram levantadas para traçar um panorama da situação desse grupo de pessoas.

O trabalho será organizado da seguinte maneira. Na Seção 2, apresentamos os trabalhos relacionados. Na Seção 3, apresentamos as principais técnicas para a realização de ataques cibernéticos. Na Seção 4, apresentamos um breve relato da análise das respostas do questionário. Na Seção 5, tecemos algumas considerações finais sobre o tema.

2. Trabalhos Relacionados

Nesta seção, apresentamos alguns trabalhos relacionados com o tema de engenharia social.

Em [Krombholz et al. 2015], os autores fizeram um importante alerta sobre a grande ameaça dos ataques de engenharia social. Na visão dos autores, vários fatores contribuem para o agravamento do problema dos ataques de engenharia social entre eles: a política BYOD (Bring your own device) em que os funcionários utilizam seus próprios aparelhos, a diminuição da interação pessoal combinado com a abundância de ferramentas para comunicação (email, Skype, Dropbox, etc). Observe que a situação apresentada pelos autores foi levada ao limite durante a pandemia com a necessidade do trabalho remoto e com um grande número de pessoas usando essas ferramentas de comunicação pela primeira vez.

Em [Rocha 2019], o autor apresenta dados de ataques de phishing, *Spyware* sendo esses ataques feitos em computadores pessoais ou em computadores empresariais, com um único objetivo: conseguir dados para usar com uma vitima em potencial. Em seu trabalho é mostrado um pouco sobre as tecnologias utilizadas para a realização destes ataques e o mesmo mostra forma de prevenção para esses ataques.

Em [Wagner Monteverde 2020], os autores relatam o aumento de ataques cibernéticos devido a pandemia do COVID-19, sendo um cenário atípico pois a maioria da população está em isolamento social fazendo com que algumas pessoas fiquem ocio-

sas e com isso começam a buscar formas de distração e acabam caindo em armadilhas feitas por pessoal mal intencionadas que disponibilizam mensagens com links para algum beneficio com pouca probabilidade de realmente existir, fazendo com que o usuário coloque dados pessoais para ter acesso ao recurso.

Resumidamente os três artigos falam sobre ataques que já vem acontecendo a muito tempo no mundo, no entanto com a chagada da pandemia aumentou de maneira exponencial, fazendo com que a possibilidade da um individuo cair em alguma dessas armadilhas sem querer seja maior que nos últimos anos, porém os especialistas em ataques cibernéticos estão trabalhando para conscientizar as pessoas a não abrirem links desconhecidos.

3. Procedimentos e Métodos

Nessa seção será apresentado as técnicas mais utilizadas para a realização ataques cibernéticos em sistemas computacionais ou em pessoas por meio da tecnologia, algumas das técnicas apresentadas fazem a utilização de programas que foram criados com o objetivo de capturar dados, vale ressaltar que muitos desse programas não foram criados para serem usados da maneira que será apresentada.

3.1. Phishing

O *Phishing* é um termo composto por duas palavras, uma delas é *fishing* que significa pesca e o outro termo é *phreak* que foram usados para nomear os primeiros *hackers* de telefonia, porém outros estudos apontam outras origens deste nome. Diante disso, um estudo realizado pela Malwarebytes mostra que em 2013 cerca de 110 milhões de registros de clientes de cartões de créditos foram roubados de clientes da target.

Diante disso as redes sociais se tornaram um dos principais alvos dos ataques de *Phishing*, pois com a grande quantidade de informações e usuários que fazem a utilização dos aplicativos, o ataque a qualquer usuário desse rede pode acontecer a qualquer momento, vale ressaltar que o *Phishing* é um ataque considerado simples, perigoso e eficiente pois na maioria das vezes ele é realizado por meio da formulários para preencher informações pessoais que podem ser usadas de varias mameiras por quem tem seu domínio.

3.2. Spyware

O *Spyware* é um *Software* malicioso que tenta infecta o computador ou dispositivo móvel do individuo, tendo com objetivo coletar informações e até mesmos seus hábitos de navegar na internet, esse programa agi de forma sorrateira pois o mesmo é executado de forma silenciosa em segundo plano tendo acesso a permissões a recursos da maquina sem que o usuário saiba. Além disso, o programa pode ser instalado na sua máquina de várias maneiras, por meio de programas desconhecidos onde o usuário aceita todos os termos de instalação, por meio de trojan e Marketing enganoso.

No entanto, existe formas de prevenir a infecção por esse tipo de *Software* malicioso, que é não abrir e-mails desconhecidos, não baixar arquivos de sites que não sejam confiáveis e verificar se o link que foi disponibilizado irá ser direcionado para um *WebSite* confiável.

3.3. Ataques de engenharia social baseados em humanos

Os ataques de engenharia social, também são conhecidos por *no-tech hacking* pois estes ataque não fazem a utilização de tecnologia, mas utiliza de outras táticas que requerem uma interação pessoal para alcançar seus objetivos, tendo com tática a *Dumpster Diving*, sendo uma técnica que se baseia em vasculhar o lixo de pessoas ou organizações que na maioria das vezes utilizada para beneficio próprio, no entanto que se trata de lixo das grande empresas essa prática pode render muitas informações de caráter sensível ou até sigilosa, ou seja, descartar o lixo de forma incorreta é bastante preocupante.

Essa é uma das técnicas mais utilizada no *no-tech hacking*, pois quem comete esse delito busca ter acesso a organização sem ter que encontrar falhas em seus computadores, no entanto existe formas de se prevenir deste ataque, sendo a politica de descarte fazendo com que todos os documentos sejam triturados antes de serem descartados.

4. Resultados

Os resultados deste trabalho foi obtido por meio de um questionário contendo oito perguntas, no entanto foram utilizadas apenas quatro dessas perguntas para obter os resultados da pesquisa, sendo essa pergunta ligadas diretamente a formas de ataques que já foram citadas no artigo, com tudo o formulário teve um total de 73 respostas.

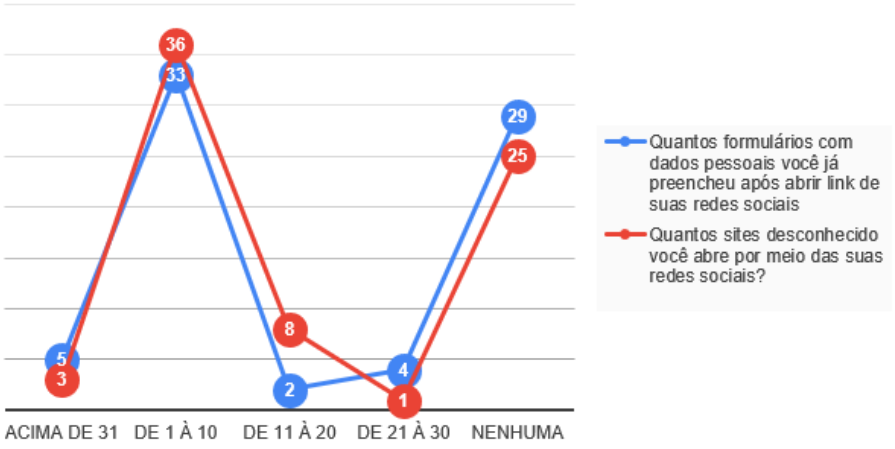

Figura 1. Comparativo de Duas Perguntas do Formulário

No questionário foi aplicado duas perguntas que se complementam, uma fala sobre a quantidade de anúncios que contem links desconhecidos que são abertos por meio de alguma rede social e a outra pergunta foi quantos formulários com dados pessoais foram preenchidos, visto isso os *hackers* podem fazer com que algum destes links sejam direcionados para o usuário com o objetivo de obter as informações pessoais ou até mesmo as de cartões de credito, na Figura 1 cerca de 36 pessoas abrem links desconhecidos e destas 33 resolvem preencher os formulários com os dados pessoais, sendo um dado alarmante pois caso estes formulários que foram disponibilizados tenham sido feitos por pessoas mal-intencionadas, as informações podem ser utilizadas para chantagem ou compra de produtos sem a autorização do usuário mandatário do recurso.

Na Figura 2 foi proposto duas perguntas que se complementavam, sendo uma delas a quantidade de ligações de números desconhecidos por dia e a quantidade de vezes

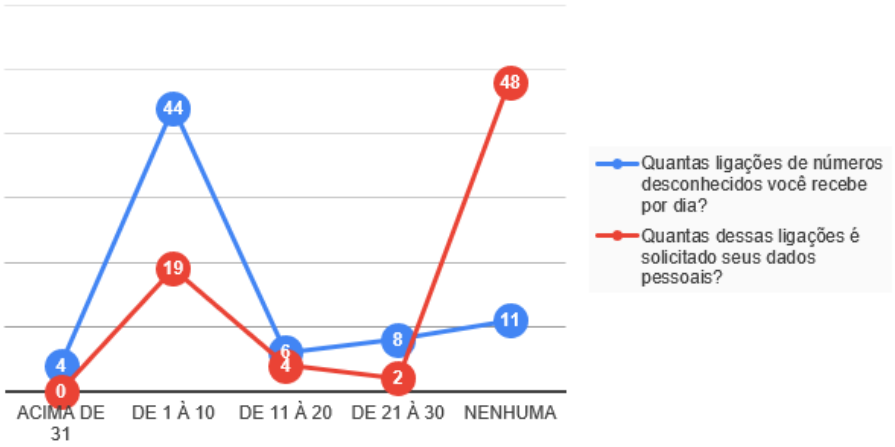

Figura 2. Comparativo de Duas Perguntas do Formulário

que nas ligações eram solicitados a confirmação de dados pessoais, visto isso pode se perceber que de 1 à 10 vezes por dia as pessoas recebem ligações, no entanto cerca de 19 pessoas confirmam seus dados em ligações desconhecidas esses dados chamam atenção pois apesar de apenas 73 pessoas terem respondidos e destas 19 realizarem a confirmação faz com que *hackers* que praticam engenharia social utilizem de seus conhecimentos para obterem dados para uso indevido.

5. Considerações Finais

Portanto, com as técnicas de invasão e obtenção de informações relatadas durante o artigo, pode-se perceber que a utilização desses meios para obtenção de informações de forma ilegal pode causar danos aos usuários, que podem ser devastadores pois vai depender do *hacker* que tem a posse das informações.

Vale ressaltar que no período da pandemia do COVID-19 houve um aumento exponencial dos ataques, no entanto as politicas publicas começaram a fazer divulgações e material para evitar que mais pessoas caiam em golpes, fazendo com que as pessoas sejam conscientizadas sobre suas ações, porém nem todas as conscientizações irão prevenir todos os ataques.

Caso algum desses ataques sejam realizado em âmbito corporativo, onde podem causar grande perdas financeiras, faz-se necessário o investimento em politicas de segurança bem definidas para prevenir algum possível ataque a organização.

Referências

Krombholz, K., Hobel, H., Huber, M., and Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, 22:113–122.

Malwarebytes (2019). Tudo sobre phishing.

Rocha, D. (2019). Engenharia social: Compreendendo ataques e a importÂncia da conscientizaÇÃo.

Wagner Monteverde, M. N. (2020). Pandemia da covid-19 ocasiona aumento de ciberataques, alertam especialistas.