COMPUTAÇÃO COGNITIVA NO ÂMBITO CORPORATIVO: uma perspectiva em segurança da informação

Samantha Morais Nunes
samanthamoraisnunes@gmail.com

Aluno concluinte do curso de pós-graduação em Segurança de Informação do Centro Universitário UNA.

Orientador: Guilherme Rodrigues Pereira

RESUMO

A utilização da computação cognitiva, através da solução *chatbot*, está cada vez mais comum no meio corporativo. Os *chatbots* são softwares que utilizam aprendizagem de máquina para simular um ser humano através de uma conversa, permitindo uma relação mais próxima com os clientes bem como melhoria na qualidade dos serviços como atendimento, marketing e vendas. Essa tecnologia está evoluindo a cada dia, segundo Gartner, em 2020 as pessoas irão conversar mais com os *bots*, o que demonstra o aumento na confiança em assistentes virtuais. Entretanto, ao ser posicionado como uma interface de interação com seus consumidores, o *chatbot* pode representar uma ameaça tanto para as organizações quanto para os usuários. Considerando esse cenário, foi realizada uma pesquisa para compreender quais ameaças à segurança de informação usuários e organizações estão suscetíveis. Durante o estudo foi possível identificar ameaças quanto ao comprometimento de informações dos usuários, ataques de negação de serviço, corrupção da inteligência artificial e engenharia social. Além disso, como o fator humano é considerado o ponto fraco da segurança de informação, foi realizado um estudo de caso para compreender quão bem-sucedido seriam ataques de engenharia social utilizando *chatbots*.

Palavras-chave: computação cognitiva, *chatbot*, engenharia social

1. INTRODUÇÃO

O mercado de aplicativos de mensagens está se desenvolvendo rapidamente. Segundo pesquisa da BI Intelligence (2016) as pessoas estão usando mais aplicativos de mensagens do que as redes sociais. Como pode ser observado no Gráfico 1, existem diversos aplicativos de mensagens, destacando-se o Whatsapp com mais de 900 milhões de usuários.

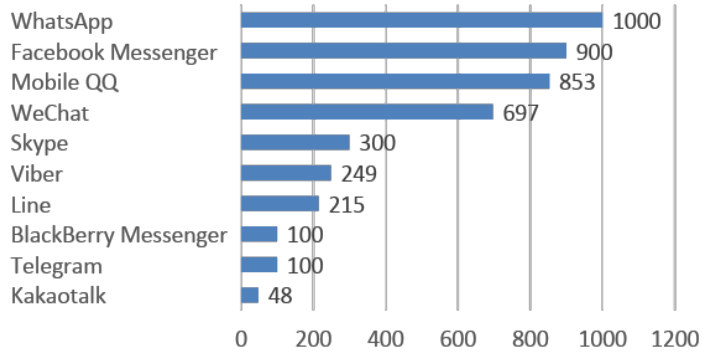

Gráfico 1 – Mais populares aplicativos de mensagens do mundo a partir de abril de 2016
Fonte: Statista

Impulsionado pelo crescimento do mercado de *Mobile Messaging*, os *chatbots*, que podem ser definidos como softwares que utilizam aprendizagem de máquina para simular um ser humano, respondendo automaticamente mensagens recebidas através de uma conversa, estão se tornando mais populares. Esse crescimento vem ocorrendo principalmente após o lançamento, pelo Facebook, de uma ferramenta de criação de *bots* dentro do *Facebook Messenger*, que agora é tratado como plataforma.

Com isso, a solução de *Chatbot* está sendo adotada por diversas organizações com o objetivo de estabelecer uma relação mais próxima com os clientes, abrindo oportunidades para marketing, vendas e atendimento ao consumidor. Além disso a utilização de *chatbots* pode, ao automatizar algumas tarefas, poupar tempo de uma pessoa e disponibilizar o serviço 24 horas, representando economia.

Essa tecnologia está trazendo muitos benefícios, no entanto pode também representar grande ameaça uma vez que a engenharia social que pode ser definida, de acordo com Huber, Kowalski e Nohlberg (2009), como a arte de explorar a confiança das pessoas para obter informações ou executar uma ação maliciosa em nome do atacante, pode ser aplicada também nesse contexto. Os engenheiros sociais e *phishers* estão acompanhando as evoluções tecnológicas, de acordo com Jagatic, Johnson, Jakobsson, and

Menczer (2005) é inevitável que as futuras gerações de ataques incorporem maiores elementos tornando-se mais eficazes e, portanto, mais perigosos para a sociedade.

Grande parte dos usuários estão cientes dos cuidados necessários e se mostram cautelosos para lidar com e-mails para que não se tornem vítima, mas esse mesmo cuidado não acontece quando se trata de redes sociais ou aplicativos de mensagens. Durante o estudo de Jagatic, Johnson, Jakobsson, and Menczer (2005) foi identificado que o contexto de uma rede social aumenta o sucesso de um ataque de *phishing*.

O *chatbot*, tecnologia estudada neste artigo, é desenhado para ser amigável e o mais semelhante possível à um humano de forma a estabelecer uma relação de confiança. Isso faz com que aumentem as chances de atacantes conseguirem que usuários disponibilizem informações, que podem ser utilizadas contra o próprio usuário ou organização, ou cliquem em links que aparentemente está no contexto da conversa, mas que podem conter um *malware*.

Além disso, as chances de ataques bem-sucedidos podem aumentar considerando que a ação seria automatizada, a base de usuários disponível é muito grande, como demonstrado na Figura 1, e que o ataque viria de um canal que grande parte das pessoas têm como confiável.

Outra questão que deve ser levada em consideração é que a utilização de inteligência artificial requer que uma rede neural seja treinada. Nesse contexto é importante analisar a melhor forma de armazenamento dos dados vindos dos usuários do *chatbot* para serem utilizados para o treinamento, bem como estabelecer um controle de acesso a essas informações.

Como o desempenho do *chatbot* melhora à medida que é treinado com base nos dados vindos dos usuários, existe a possibilidade de um atacante inserir dados para corromper a inteligência do *chatbot*, fazendo com que o mesmo compreenda como verdadeiro informações falsas prejudicando empresas e clientes.

Portanto, é importante conhecer as potenciais ameaças às quais usuários finais e empresas estarão suscetíveis ao utilizar *chatbots*. Dessa forma a presente pesquisa, buscando compreender esse cenário pela perspectiva da segurança de informação, poderá servir como base de conhecimento para pesquisas futuras e implementação de ações de prevenção.

Tendo em vista as questões discutidas, este artigo visa responder à pergunta problema: “Como a utilização da computação cognitiva, através de *chatbots*, pode representar uma ameaça para usuários e organizações na perspectiva da segurança de informação? ”.

1.1. Objetivo

A utilização de computação cognitiva, através de *chatbots* está proporcionando diversos benefícios para organizações e clientes, como por exemplo melhor qualidade de serviço ao permitir uma relação mais próxima. Entretanto, é importante que sejam consideradas as implicações, com relação à segurança da informação, que esta tecnologia pode trazer.

Considerando este cenário, este artigo tem como objetivo analisar como a utilização da computação cognitiva, através de *chatbots*, pode representar uma ameaça para usuários e organizações na perspectiva da segurança de informação e como objetivos específicos:

- Identificar os possíveis ataques que usuários e organizações estão suscetíveis ao utilizar *chatbots*.
- Compreender as ameaças que a utilização de *chatbots* pode representar, com relação à segurança de informação, para usuários e organizações.
- Analisar de que forma os possíveis ataques podem prejudicar os usuários e organizações com base nos resultados do estudo de caso.

1.2. Justificativa

O cenário de ameaças à segurança de informação está cada dia mais dinâmico. Os atacantes acompanham as evoluções tecnológicas de forma que novos elementos passem a fazer parte de seus ataques tornando-os mais eficazes e eficientes.

Sob essa ótica torna-se relevante compreender sobre as ameaças que áreas como a computação cognitiva, no caso deste estudo através de *chatbots*, podem trazer para a sociedade. Além de permitir o desenvolvimento da competência na área de segurança de informação e computação cognitiva, ao realizar a análise de ataques através de *chatbots*, será possível contribuir para pesquisas posteriores como base de conhecimento e implementações de ações para prevenção a ataques relacionados à *chatbots*.

1.3. Metodologia

Tomando como base a questão da pesquisa, dos objetivos gerais e específicos definidos, este artigo apresenta uma pesquisa quantitativa, com base em um estudo bibliográfico e análise de resultados obtidos através de estudo de caso realizado em ambiente real.

Com o objetivo de compreender sobre as ameaças que a utilização da computação cognitiva aplicada a interfaces de comunicação, através de *chatbots*, pode representar com relação à segurança de informação, foi realizado uma pesquisa sobre as possíveis ameaças que a utilização dessa tecnologia pode representar para organizações e usuários. Com base nessa pesquisa, foi selecionada, visto que o fator humano é considerado o ponto fraco da segurança de informação, a ameaça relacionada à engenharia social, para um estudo de caso com o objetivo de compreender quão bem-sucedido seriam esses ataques utilizando *chatbots*.

Foi realizado o levantamento bibliográfico sobre projetos na área de computação cognitiva, *social phishing* e engenharia social automatizada que foram a base para a construção do estudo de caso. Dessa forma foi possível desenvolver um fluxo contendo cinco fases, como pode ser observado na Figura 1, considerando um cenário de ataque de engenharia social, buscando analisar os resultados de cliques em links e obtenção de informações através de *chatbots*. A seguir serão discutidas cada uma das etapas da simulação de um ataque de engenharia social.

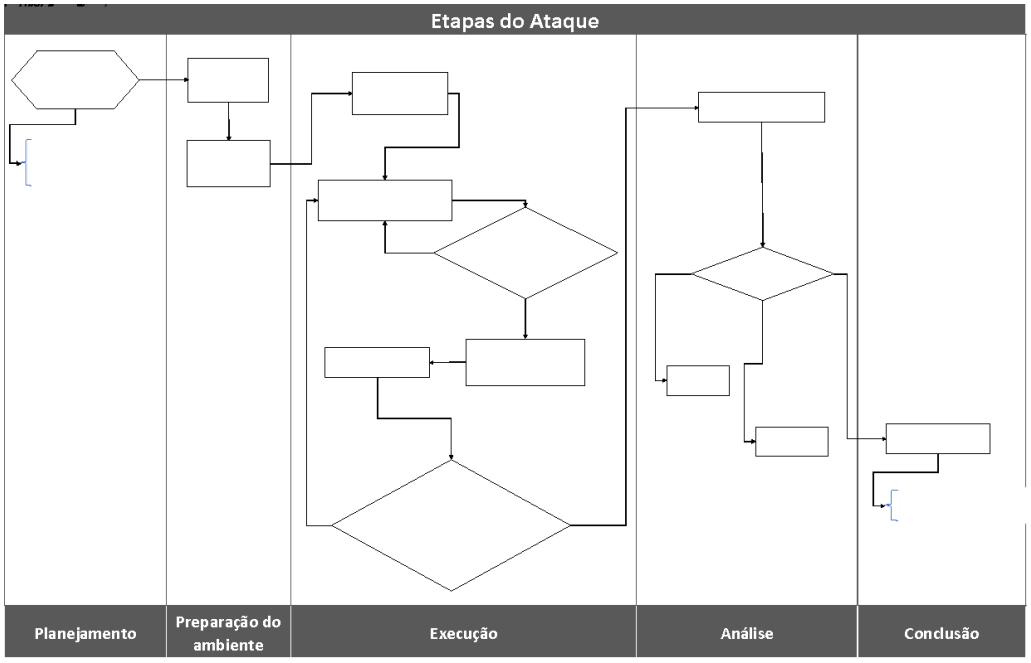

Figura 1 – Etapas da simulação de um ataque realizado como estudo de caso

Na etapa de Planejamento foram definidos os parâmetros, incluindo a escolha do objetivo, o perfil dos alvos e o canal de comunicação. O objetivo foi conseguir com que os usuários clicassem nos links enviados durante a conversa com o *chatbot*, bem como a obtenção de informações pessoais. Nesse contexto, o perfil escolhido foram pessoas que estão à procura de emprego, considerando que é um assunto atual.

Como podemos verificar na Figura 1, o *Whatsapp* tem a maior base de usuários, porém sua API (*Application Programming Interface*) ainda não está

aberta para a criação de *chatbots*, portanto o *Facebook Messenger*, que possui a segunda maior base de usuários, foi selecionado como canal de comunicação.

Na etapa de Preparação do Ambiente foi criado um *chatbot* através da plataforma *Chatfuel*. Esta plataforma foi selecionada por conta de sua praticidade em lidar com a inteligência artificial necessária para o funcionamento do *chatbot*. Foi criada uma página no *Facebook* chamada "Quem Indica", através da qual cada mensagem recebida seria automaticamente respondida pelo *chatbot*. A Figura 2 demonstra um exemplo de fluxo de navegação do *chatbot*.

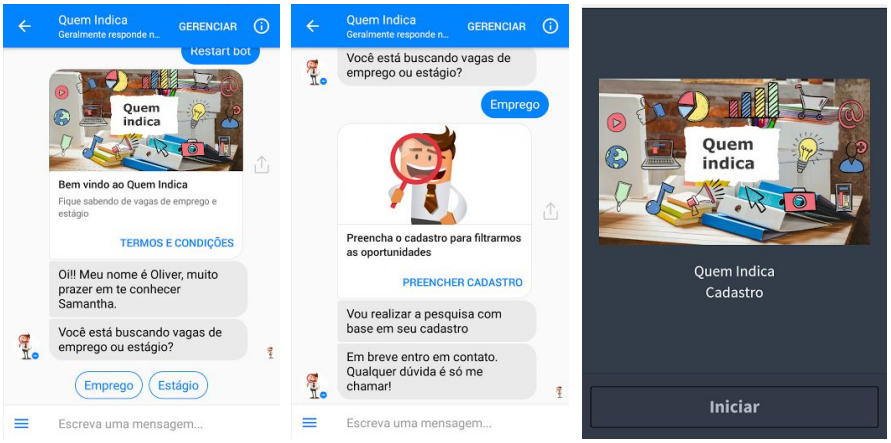

Figura 2 – Exemplo de fluxo de utilização do *chatbot*

Na etapa de Execução, a seleção dos alvos, com base no perfil definido, foi através dos grupos do *Facebook* relacionados a busca de novas oportunidades de emprego. Para se comunicar com as pessoas do grupo, foi criado um perfil falso de um usuário do *Facebook*, através do qual foi possível fazer parte de diversos grupos e realizar a divulgação do *chatbot*.

A partir do momento em que um usuário enviasse a primeira mensagem o *chatbot* iniciaria a conversa com a vítima. O fluxo implementado no *chatbot* foi desenhado para ser amigável de forma que fosse possível estabelecer uma relação de confiança para que os usuários não identificassem que se tratava de um *chatbot*.

Através da plataforma do *Facebook* já é possível ter acesso a algumas informações dos usuários, mas para obter outras informações, durante a conversa, foi solicitado aos usuários que clicassem em um link e preenchessem um cadastro. O formulário de cadastro foi desenvolvido com a utilização da plataforma *Typeform* que disponibiliza um painel com métricas, onde é possível verificar o total de usuários únicos que acessaram o formulário, bem como as informações preenchidas.

O formulário continha as solicitações de informações diversas como nome, e-mail, telefone, carteira de identidade, nome da última empresa que trabalhou

e cargo, além de informações sobre outras experiências e área pretendida para recolocação profissional. Com base nessas informações foram realizadas buscas de vagas de emprego disponíveis. Os links selecionados com as vagas, foram encurtados através do serviço *Google URL Shortner* para que pudesse ser verificado se o usuário clicou no link enviado.

Durante a etapa de Análise foi realizada a verificação dos resultados adquiridos com o *chatbot* que serão discutidos na seção Análise e Discussão dos Resultado deste artigo. Já na etapa de Conclusão a simulação de ataques foi finalizada com a exclusão do perfil falso e o *chatbot* despublicado.

2. REFERENCIAL TEÓRICO

Nesta seção, serão abordados os conceitos relacionados a inteligência artificial, *chatbots* e engenharia social.

2.1. Inteligência artificial

A inteligência artificial (IA) não tem uma definição simples, de acordo com Luger (2014) pode ser definida como um ramo da ciência da computação que se ocupa da automação do comportamento inteligente através do conjunto de diversos métodos, algoritmos e técnicas que possibilitam tornar um software mais inteligente. IA é um campo de pesquisa que não busca apenas compreender entidades inteligentes, mas também as construir, segundo Russell e Norvig (2013), podendo ser relacionada e aplicada a diversas outras áreas.

De acordo com Russell e Norvig (2013), o primeiro trabalho reconhecido na área foi realizado por Warrem Macculloch e Walter Pitts em 1943, em que os pesquisadores propuseram um modelo de neurônio artificial, que se caracterizava por estar “ligado” ou “desligado”, baseado em conhecimento e função dos neurônios no cérebro. Já em 1950 foi criado o primeiro computador de rede neural por Marvin Minsky e Dean Edmonds, ambos estudantes de Harvard. Ainda em 1950 Alan Turing, foi o primeiro a articular uma visão completa da IA em seu artigo “*Computing Machinery and Intelligency*”, com o Teste de Turing cujo objetivo é medir o desempenho de uma máquina e de um humano.

Esse teste, chamado de "*The Imitation Game*", de acordo com Luger (2014), consiste em colocar um humano e uma máquina em salas separadas, e um segundo humano como “interrogador”. Este interrogador não sabe qual entidade é a máquina e o objetivo é que através de perguntas possa distinguir a máquina do ser humano, caso isso não seja possível pode-se supor que a máquina possui inteligência.

A seguir serão apresentados os conceitos de aprendizado de máquina e computação cognitiva, e como estes campos estão relacionados à inteligência artificial (IA).

2.1.1 Aprendizagem de Máquina

Earley (2015) defende que o aprendizado de máquina se refere à utilização de algoritmos e metodologias que permitem, com a obtenção de dados, melhorar seu desempenho. Através desses algoritmos é possível detectar padrões, descobrir e classificar informações retornando os resultados relevantes para o usuário.

2.1.2 Computação cognitiva

A computação cognitiva tem o objetivo simular processos de pensamento humano através de algoritmos de aprendizagem (Marr, 2016). Tendo a inteligência artificial e aprendizagem de máquina como pilares, utiliza-se a mineração de dados, reconhecimento de padrões e processamento de linguagem natural, para se aproximar da forma como o cérebro humano funciona.

A computação cognitiva refere-se a sistemas que “aprendem e raciocinam” a partir de interações com os humanos, de forma a permitir que computadores e homens cooperem na tomada de decisões (Kelly, 2015). Isso quer dizer que a computação cognitiva se baseia no uso de aprendizagem de máquina, e que através da contínua alimentação com dados, o sistema se torna capaz de reconhecer padrões e, de acordo com Kelly e Hamm (2013), extrair informação de uma grande quantidade de dados. A ideia não é substituir o cérebro humano, mas potencializá-lo de forma que humanos e máquinas possam trabalhar de forma colaborativa na busca por melhores resultados.

O primeiro sistema cognitivo foi o IBM Watson, apresentado em 2011 através da participação no *Jeopardy*, uma competição de perguntas e respostas. IBM Watson conseguiu responder a perguntas simples e complexas demonstrando o poder do sistema cognitivo. Atualmente já existem outros como a Apple Siri, Microsoft Cortana, Google Now, e Amazon Echo, além do mensageiro inteligente do Google chamado Allo, que permite o processamento de texto e voz em linguagem natural e uma melhor classificação da informação, permitindo respostas mais assertiva (Luca, 2016).

Estes sistemas dependem de aprendizagem com base em algoritmos e redes neurais para processar a informação, que vão além do que a simples decifração, de acordo com Kelly (2015), quanto mais dados são submetidos ao sistema mais ele aprende, desenvolvendo a compreensão e tornando o

sistema mais preciso. Isso permite que o sistema possa identificar aspectos que antes eram invisíveis, com base em padrões e percepções em dados estruturados ou não.

O conceito de computação cognitiva está muito próximo ao da IA, mas podemos considerar, de maneira geral, que a computação cognitiva é uma arquitetura de subsistemas de IA utilizando várias metodologias de aprendizado de máquina, segundo Lynne Parker diretora da divisão de sistemas de informação da Fundação Nacional de Ciências dos Estados Unidos.

2.2. Chatbot

A computação cognitiva está ganhando cada vez mais atenção e sua aplicação pode ser vista em diversas áreas. Uma das que está se destacando é a computação cognitiva no âmbito corporativo com os *chatbots*.

Chatbot é um sistema de software, desenvolvido para simular um ser humano em uma conversa de acordo com Nunes (2016). Podem interpretar, compreender e prever ações dos usuários e ainda aprender novas informações com as metodologias de aprendizagem de máquina. O termo surgiu da junção das palavras provenientes do inglês *chatter*, que significa a pessoa que conversa, e da palavra *bot*, que é a abreviatura de *robot* que significa robô.

O objetivo é responder perguntas automaticamente de forma que os usuários não percebam que estão conversando com um software. Essa tecnologia não é recente, mas se tornou mais comum após o anúncio do *Facebook* sobre a disponibilização do serviço de *chatbot* na rede social para empresas (Nunes, 2016). Além do *facebook Messenger, os chatbots* podem ser disponibilizados através de diversos aplicativos de mensagens como *telegram, skype, slack* e outros.

2.3. Engenharia Social

No que se refere à segurança da informação o fator humano é o elo mais fraco como ressalta Mitnick (2002). A engenharia social pode ser definida como a ação de tentar obter informações ou influenciar alguém a realizar alguma ação apoiando-se na confiança de outras pessoas (Hardnagy, 2014). Nesse contexto, Hardnagy (2014) determina três metodologias principais:

- *Phishing* caracterizada pela prática de envio de e-mails aparentemente confiáveis, com o objetivo de influenciar ou obter alguma informação sensível;
- *Vishing* caracterizada pela prática de obter informações ou tentar influenciar uma ação através do telefone;
- *Impersonation* caracterizada pela prática de fingir ser outra pessoa com o objetivo de obter informação ou acessos não autorizados

O uso crescente de redes sociais e aplicativos de mensagens tanto para uso profissional quanto pessoal, faz com que os engenheiros sociais tentem uma nova vertente evoluindo seus ataques para obter informações valiosas tanto sobre os usuários quanto das organizações.

Através do *Phishing* um atacante tenta adquirir fraudulentamente informações confidenciais de uma vítima, representando um terceiro confiável, de acordo com o estudo de Jagatic, Johnson, Jakobsson, and Menczer (2005) ao explorar o contexto das redes sociais pode-se potencializar esses ataques. Esse estudo demonstrou que os utilizadores de redes sociais podem ter mais de quatro vezes mais probabilidades de se tornarem vítimas se o atacante for amigável.

Considerando o contexto de *chatbots,* um estudo de Huber, Kowalski e Nohlberg (2009) ilustra como as redes sociais podem ser utilizadas para engenharia social. Neste estudo foram realizados dois testes através de um bot, neste caso foi implementado um *bot* para conversar diretamente com as pessoas se passando por um estudante. No primeiro foi examinada a capacidade de coleta de informações e a segunda realizou o Teste de Turing no protótipo. Os resultados dos experimentos evidenciaram que a realização de engenharia social automatizada através de bots é eficiente e eficaz.

3. ANÁLISE E DISCUSSÃO DOS RESULTADOS

Com base no estudo realizado sobre computação cognitiva e *chatbots*, presente no Referencial Teórico, foi possível realizar uma análise e identificar os possíveis ataques que usuários e organizações estão suscetíveis ao utilizar *chatbots*, que serão discutidos a seguir.

Os *chatbots* utilizam os dados disponibilizados pelos usuários durante a conversa para aprender e aumentar sua capacidade de compreensão com o tempo. Com isso surge a preocupação sobre a segurança das informações de quem interage com *chatbots*, tanto sobre o armazenamento seguro quanto ao controle de quem pode ter acesso aos dados, visto que no caso de *chatbots* com interação por redes sociais, as informações ficam disponíveis nas *threads* de conversas.

Considerando que os *chatbots* são sistemas de inteligência artificial programados para responder de forma automática as mensagens enviadas pelos usuários, evoluindo seus métodos de conversação através do treinamento de sua rede neural com base nos dados gerados durante as conversas, existe a possibilidade de comprometer sua inteligência de forma a compreender como correta alguma informação errada. Um exemplo desse tipo de ataque ocorreu com a Tay, um *chatbot* criado pela *Microsoft* para se passar por uma adolescente americana e que interagia com os usuários através do *Twitter*. Em menos de 24 horas, sua inteligência artificial foi corrompida, passando a postar mensagens ofensivas. Esse tipo de ataque pode pôr em risco a imagem de uma organização, assim como pode também gerar danos financeiros, por exemplo se utilizado em *chatbots* de investimento financeiro, com o objetivo de manipular o mercado de ações, no qual seriam realizadas sugestões erradas para os clientes.

Ataques DoS, sigla para *denial of service*, tem como objetivo deixar um recurso do sistema indisponível, impedindo que os usuários possam ter acesso. No contexto de chatbots, de acordo com Mann (2016), é possível realizar um ataque DoS, demonstrado através da utilização de um metasploit (msf-fb-messenger-bot-dos), desenvolvido pelo autor. Segundo Mann (2016), a utilização desse metasploit é possível porque a API do *Facebook Messenger*, tem uma maneira de verificar que o Facebook está conectado com um *chatbot*, na qual as bibliotecas utilizadas não implementam segurança ou implementam de forma incorreta.

Finalmente, sobre a ameaça relacionada a engenharia social, as organizações devem manter seus colaboradores cientes sobre a utilização de *chatbots* com segurança. Essa tecnologia pode ser utilizada por atacantes, ao projetar um *chatbot* para iniciar conversas através de aplicativos de mensagens, e durante a conversa, obter informações sensíveis ou incentivar cliques em links.

O fator humano é frequentemente referenciado como o elo mais fraco da segurança da informação, como ressalta Mitnick (2002). No ambiente corporativo a falta da cultura de segurança da informação por parte dos colaboradores é destacada como um dos principais fatores em violações de dados pela CyberArk(2015) através do *Global Advanced Threat Landscape Survey 2015*, como pode ser observado no Gráfico 2 abaixo.

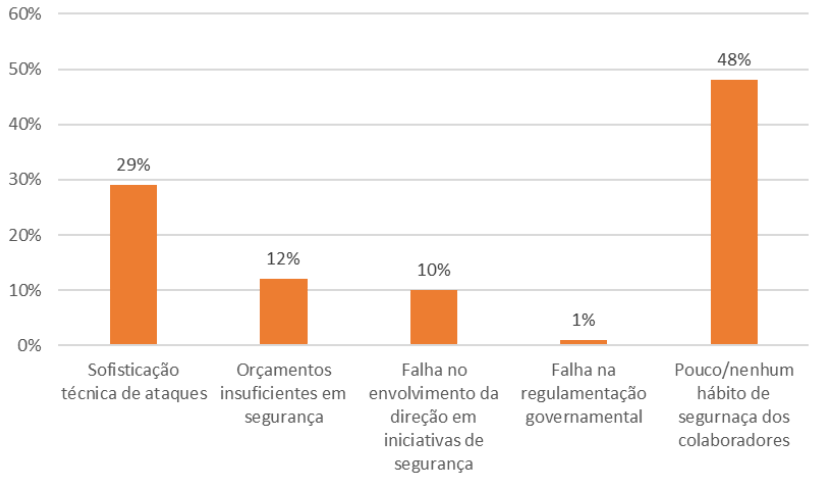

Gráfico 2 – Principais fatores de violações de dados
Fonte: Global Advanced Threat Landscape Survey 2015

Os criminosos cibernéticos estão a cada dia aprimorando seus métodos. Portanto entende-se que a aprendizagem de máquina pode ser utilizada para potencializar e sofisticar ataques de engenharia social, e tendo em vista o crescimento de sua utilização pelo meio corporativo, é uma das tendências presente no relatório de previsões sobre ameaças em 2017 pela McAfee Labs (2016).

Portanto, dentre as ameaças identificadas, a que se refere à engenharia social foi selecionada para um estudo de caso em que, através da simulação de um cenário real, foi possível compreender quão bem-sucedido seria este tipo de ataque realizado através de *chatbots*. A seguir serão discutidos os resultados obtidos através do estudo de caso.

3.1. Resultados do estudo de caso

Conforme discutido na seção Metodologia, foi criado, através da ferramenta *chatfuel*, um *chatbot* publicado no *Facebook* chamado Quem Indica, cujo objetivo é a busca de vagas de empregos com base em informações disponibilizadas pelos usuários. Para que o resultado refletisse um cenário real, foram realizados comentários em posts de pessoas em grupos de busca de emprego com um perfil falso do Facebook criado para o teste, como demonstrado na Figura 4 abaixo.

Figura 4 – Divulgação do *Chatbot*

A partir do momento que o usuário envia uma mensagem, automaticamente passa a ser atendido pelo *chatbot*, como demonstrado na Figura 5 abaixo.

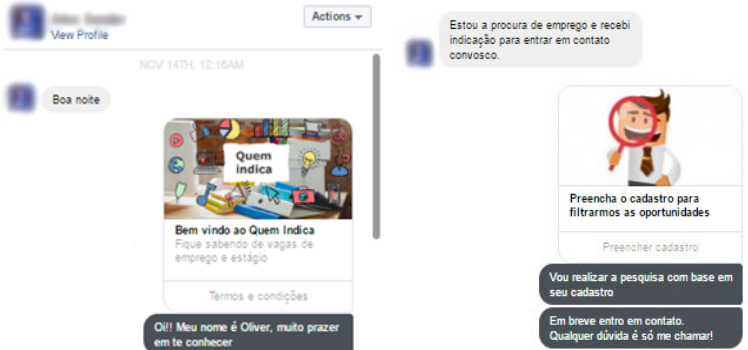

Figura 5 – Interação de usuários do facebook com o *chatbots*

O *chatbot* ficou habilitado por doze dias, período no qual foi possível estabelecer conversa com dezoito pessoas. Do total de pessoas, 78% são do sexo feminino e 22% do sexo masculino, com idades variando entre 17 e 43 anos.

Analisando a taxa de cliques nos links enviados no contexto da conversa, considerando o fluxo de navegação proposto para simular ataques de engenharia social, foram obtidos 100% de cliques no primeiro link enviado solicitando cadastro do perfil profissional.

Das pessoas que interagiram com o *chatbot*, 78% delas preencheram o cadastro de perfil profissional, com base no qual foi realizada uma pesquisa sobre a vaga pretendida e enviado um novo link com sugestões de vagas no perfil indicado. Ao enviar a url encurtada, com a utilização do *Google URL Shortner*, foi possível identificar se o usuário clicou no link enviado. Com base nos resultados obtidos a taxa de cliques foi de 71%.

Com relação às informações solicitadas no cadastro profissional, a única questão que nem todos os usuários preencheram foi o número da carteira de identidade, em que somente seis pessoas disponibilizaram a informação. As demais informações como nome, e-mail, telefone, última empresa na qual trabalhou e cargo, entre outras foram preenchidas por todos.

Com base nos resultados obtidos podemos identificar que o fato do *chatbot* ter sido construído de forma a se apresentar mais amigável e o fato desse sistema fazer parte da plataforma do facebook pode ter influenciado para aumentar sua credibilidade, de forma que os usuários se sentem mais confortáveis em disponibilizar informações pessoais e clicar em links. Além disso, ações que auxiliam na identificação de engenharia social como endereço de e-mail suspeito ou erros de escrita, não se aplicam quando se trata de redes sociais e aplicativos de mensagens, pois não são exibidos e-mails, apenas o nome da página do *chatbot*, enquanto que erros de digitação e palavras abreviadas são considerados normais em conversas.

Com o intuito de realizar uma comparação, através do *MailChimp*, ferramenta para envio de *newsletter*, foi enviado um e-mail no contexto do serviço de busca de vagas, para todos os usuários que preencheram o

cadastro, neste caso quatorze pessoas. Esta ferramenta possui um painel com as métricas de quantidade de e-mails abertos e cliques em links, através do qual foi possível verificar que dos quatorze e-mails enviados, apenas quatro foram abertos e houve apenas um clique dentre os diversos links disponibilizados no corpo do e-mail através de botões para aumentar o incentivo, enquanto que com a utilização do *chatbot*, de dezoito contatos existentes houveram dezoito cliques, como pode ser observado no Gráfico 3 abaixo.

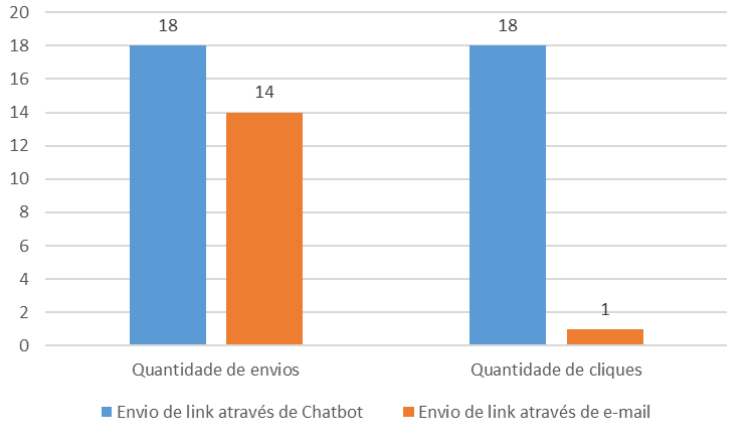

Gráfico 3 – Comparação entre envio de links através de *chatbots* e e-mail

Com base nos resultados discutidos nesta seção, identificamos que para o presente estudo de caso, considerando um cenário de ataque de engenharia social, o *chatbot* seria bem-sucedido, e neste caso mais eficiente do que através de e-mail.

4. CONSIDERAÇÕES FINAIS

A utilização da computação cognitiva pode ser uma revolução e trazer diversos benefícios, no entanto sua utilização, por ser uma área que está se expandindo rapidamente para o meio corporativo, tendo como exemplo o uso de *chatbots*, que pode trazer para as organizações e cliente ameaças ainda desconhecidas.

Através da pesquisa bibliográfica foi possível verificar que a utilização de *chatbots* pode abrir portas para diversos tipos de ataques como vazamento de informações disponibilizadas pelos usuários, ressaltando questões quanto à forma de armazenamento dos dados e controle de acesso. Outra questão é com relação à possibilidade de comprometer a inteligência artificial, através da disponibilização de dados com o objetivo de fazer com que o *chatbot* compreenda como correta alguma informação errada. Além disso ataques de DoS também são possíveis como demonstrado em Mann (2016) e por último, o

ataque relacionado a engenharia social, para o qual foi realizado o estudo de caso.

Com base nos resultados obtidos com o estudo de caso sobre a engenharia social, foi possível demonstrar que em um cenário de ataque com a utilização de um *chatbot* seria bem-sucedido.

A utilização de aprendizagem de máquina pode potencializar e sofisticar ataques de engenharia social, sendo uma das tendências presentes no relatório de previsões sobre ameaças em 2017 pela McAfee Labs (2016). No caso da aplicação dos ataques através de *chatbots*, como discutido anteriormente, tem grandes chances de serem bem-sucedidos. Além disso considerando o meio de comunicação sendo redes sociais ou aplicativos de mensagens, ações comuns para detecção de ataques de engenharia social como endereço de e-mail e erros encontrados no texto não se aplicam neste caso. Em conversas através de *chatbots* não são exibidos e-mails e erros de digitação e palavras abreviadas fazem parte da comunicação através de redes sociais e aplicativos de mensagens.

Portanto é necessário que tanto organizações quanto usuários estejam atentos quanto ao tipo de informação que está sendo solicitada através do *chatbot* e links enviados para evitar danos causados por ataques, que muitas vezes podem causar danos irreparáveis.

REFERÊNCIAS

BAKER, Mike. Whats the risk? 3 things to know about chatbots and cybersecurity. 2016. Disponível em: <http://www.darkreading.com/vulnerabilities---threats/whats-the-risk-3-things-to-know-about-chatbots-and-cybersecurity/a/d-id/1326912> Acesso em: 24 nov. 2016

BI Intelligence. Messaging apps are now bigger than social networks. BI Intelligence. set. 2016. Disponível em:< http://www.businessinsider.com/the-messaging-app-report-2015-11> Acesso em: 5 nov. 2016.

CyberArkGlobal. Advanced Threat Landscape Survey 2015. Disponível em< http://www.dit.co.jp/products/cyberark/pdf/survey-cyberarks-2015-global-advanced-threat-landscape-09-30-15.pdf> Acesso em: 2 dez 2016.

EARLEY, Seth. Machine Learning and Cognitive Computing. IEEE IT Professional. 2015

HARDNAGY, Christopher. The Social Engeneering Framework. 2014. Disponível em: < http://www.social-engineer.org/framework/general-discussion> Acesso em: 5 nov. 2016

HUBER, Markus; KOWALSKI, Stewart; NOHLBERG, Marcus; TJOA, Simon. 2009. Towards Automating Social Engineering Using Social Networking Sites. Proceedings of the 2009 International Conference on Computational Science and Engineering - Volume 03 (CSE '09), Vol. 3. IEEE Computer Society, Washington, DC, USA, 117-124.

JAGATIC, Tom; JOHNSON, Nathaniel; JAKOBSSON, Markus; MENSZER, Filippo. Social Phishing. Indiana University, Bloomington. December 12, 2005

KELLY, John E. Computing, cognition and the future of knowing How humans and machines are forging a new age of understanding. IBM Research and Solutions Portfolio. 2015

KELLY, John E; HAMM, Steve. Smart Machines: IBM's Watson and the Era of Cognitive Computing. 2013

LUCA, Cristina De. Conquistas de aprendizado de máquina do Google já estão ao alcance de todos. 2016. Disponível em: < http://cio.com.br/tecnologia/2016/12/04/conquistas-de-aprendizado-de-maquina-do-google-ja-estao-ao-alcance-de-todos/> Acesso em: 6 de dez 2016

LUGER, George F. Inteligência Artificial. 6° edição. São Paulo. Pearson Educação do Brasil, 2014. p.1-13

MANN, David. How to kill a bot with 10 http requests. 2016. Disponível em: < https://chatbotsmagazine.com/how-to-kill-a-bot-with-10-http-requests-ca7eb57c2ad1#.ck8mppgm9> Acesso em: 30 nov. 2016.

MARR, Bernard. What Everyone Should Know About Cognitive Computing. mar 2016. Disponível em:< http://www.forbes.com/sites/bernardmarr/2016/03/23/what-everyone-should-know-about-cognitive-computing/#4a7cd24b5d6e>. Acesso em: 5 nov. 2016.

McAfee Labs Previsões sobre ameaças em 2017. 2016. Disponível em <http://www.mcafee.com/br/resources/reports/rp-threats-predictions-2017.pdf> Acesso em:3 de dez 2016

MITNICK, Kevin e SIMON, William. A arte de enganar. John Wiley & Sons. 2002

MOREIRA, Isabela. A Microsoft criou uma robô que interage nas redes sociais - e ela virou nazista. 2016. Disponível em: < http://revistagalileu.globo.com/blogs/buzz/noticia/2016/03/microsoft-criou-uma-r

obo-que-interage-nas-redes-sociais-e-ela-virou-nazista.html> Acesso em: 30 nov. 2016

NUNES, Emily Canto. Chatbot: o que são os robôs conversadores? nov 2016. Disponível em:< https://iq.intel.com.br/chatbot-o-que-sao-os-robos-conversadores> Acesso em: 5 nov. 2016.

RUSSELL, Stuart; NORVIG, Peter. Inteligência artificial; Tradução Regina Célia Simille. Rio de Janeiro. Elsevier. 2013. p.1-40

SASSE, Martina A; BROSTOFF, Sacha; WEIRICH, Dirk. Transforming the “Weakest Link”: A Human-Computer Interaction Approach for Usable and Effective Security. 2001. Department of Computer Science, University College London