UNIVERSIDADE FEDERAL DO ACRE

CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

Engenharia Social: um estudo de caso sobre técnicas que podem expor o usuário de internet a uma condição de sequestro eletrônico - Ransomware.

RIO BRANCO
2019

LUCAS DA SILVA CRUZ

Engenharia Social: um estudo de caso sobre técnicas que podem expor o usuário de internet a uma condição de sequestro eletrônico - *Ransomware*.

Projeto de monografia apresentado como exigência parcial para obtenção do grau de bacharel em Sistemas de Informação da Universidade Federal do Acre.

Orientadora: Drª Laura Costa Sarkis
Coorientador: PhD Hermann Atila Hrdlicka

RIO BRANCO
2019

Ficha catalográfica elaborada pela Biblioteca Central da UFAC

C889e Cruz, Lucas da Silva, 1990-

Engenharia social: um estudo de caso sobre técnicas que podem expor o usuário de internet uma condição de sequestro eletrônico - Ransomware/ Lucas da Silva Cruz; orientadora: Drª. Laura Costa Sarkis e Coorientador: PhD Hermann Atila Hrdlicka.– 2019.

76 f.: il. ; 30 cm.

Monografia (Graduação) – Universidade Federal do Acre, Centro de Ciências Exatas e Tecnológicas, Curso de Sistemas de Informação. Rio Branco, 2019.

Inclui referências bibliográficas e apêndices.

1. Segurança da informação. 2. Engenharia Social. 3. Spear Phishing Ransomware. I. Sarkis, Laura Costa (orientadora). II. Hrdlicka, Hermann Atila (Coorientador). III. Título.

CDD: 004

Bibliotecária: Nádia Batista Vieira CRB-11º/882.

TERMO DE APROVAÇÃO

LUCAS DA SILVA CRUZ

Engenharia Social: um estudo de caso sobre técnicas que podem expor o usuário de internet a uma condição de sequestro eletrônico - *Ransomware*.

Esta monografia foi apresentada como trabalho de conclusão de Curso de Bacharelado em Sistemas de Informação da Universidade Federal do Acre, sendo aprovado pela banca constituída pelo professor orientador e membros abaixo mencionados.

Compuseram a banca:

Profª. Orientadora, Drª Laura Costa Sarkis
Curso de Bacharelado em Sistemas de Informação

Prof. Membro da banca, Me. Wilker Luiz Gadelha Maia
Curso de Bacharelado em Sistemas de Informação

Prof. Membro da banca, Dr. André Luiz Nasserala Pires
Curso de Bacharelado em Sistemas de Informação

Rio Branco, Fevereiro de 2019

“Para minha família”

“Quando algo é importante o suficiente, você realiza mesmo que as chances não estejam a seu favor.”
- Elon Musk

AGRADECIMENTOS

Primeiramente a Deus que permitiu que tudo isso acontecesse, ao longo de minha vida, e não somente nestes anos como universitário, mas que em todos os momentos é o maior mestre que alguém pode conhecer.

À Prof.ª. Dr. ª Laura Costa Sarkis, integrante do quadro docente, na estimada entidade Universidade Federal do Acre que me acolheu fruto de uma transferência de outra instituição. Ao meu coorientador Prof. PhD. Hermann Atila Hrdlicka, do quadro da Universidade Federal da Paraíba onde dei início a minha formação, pelo paciente trabalho de orientação, coorientação, endossamento e revisão da redação. Agradeço a todos os *professores* por proporcionarem o conhecimento não apenas racional, mas a manifestação de caráter e afetividade da educação no processo de *formação profissional*, pela dedicação a mim destinada, não somente pelo ensino, mas pela aprendizagem concedida.

A palavra mestre, nunca fará justiça a dedicação dos professores que mesmo sem nominá-los, terão os meus eternos agradecimentos.

Aos meus pais, Antônio Carlos Saraiva da Cruz e Edna da Silva Cruz, pelo amor, incentivo e apoio incondicional e aos meus Irmãos Mateus da Silva Cruz e Sara Kelita da Silva Cruz que me deram forças para terminar essa etapa.

A Laila Assad por ter me ajudado e apoiado a todo momento dando condições de concluir (obrigado pelo notebook e pelas revisões de ortografia) e a todos que de forma direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

LISTAS DE FIGURAS

SUMÁRIO

RESUMO

A presente pesquisa diz respeito a um estudo de segurança da informação com ênfase na Engenharia Social. A proposta é analisar o comportamento dos usuários que utilizam redes sociais, nesse sentido, busca-se verificar como a Engenharia social está sendo utilizada para ações de sequestro eletrônico de dispositivos. O resultado do estudo de caso apresenta gráficos que indicam, se as pessoas que frequentam as redes sociais, apesar de todos os alertas e utilização de mecanismos de bloqueio de conteúdo, ainda estão vulneráveis a ataques que podem resultar em sequestros eletrônicos fruto de ações de engenharia social. Apresentam-se resultados, tais como: qual a porcentagem de pessoas da amostra que podem ser alvos de ataques cibernéticos, idade, grau de escolaridade entre outros elementos dentro do contexto de usuários de plataformas sociais. No trabalho, expõe-se ainda, sugestões de estratégias que podem ser adotadas para evitar estes tipos de ataques.

Palavras-chave: Segurança da Informação, Engenharia Social, Spear Phishing, Ransomware.

ABSTRACT

The present research concerns an information security study with an emphasis on Social Engineering. The proposal is to analyze the behavior of users who use social networks, in this sense, it is sought to verify how social engineering is being used for actions of electronic device sequestration. The outcome of the case study shows graphs that indicate whether people attending social networks despite all alerts and use of content blocking mechanisms are still vulnerable to attacks that may result in electronic hijackings as a result of engineering actions Social. Results are presented, such as the percentage of people in the sample who may be targets of cyber-attacks, age, and educational level among other elements within the context of users of social platforms. In the paper, it is also presented suggestions of strategies that can be adapted to avoid these types of attacks.

Keywords: Information Security, Social Engineering, Spear Phishing, Ransomware

1 INTRODUÇÃO

Com a popularização da internet, as pessoas geram a todo momento dados de inúmeros conteúdos de seu cotidiano, o que a torna um indivíduo altamente disponível, termo que pode ser associado a uma área da informática em relação a disponibilidade de serviços, pois está passível de ser observado praticamente em tempo real em suas ações diárias.

De acordo com a pesquisa da *HootSuite* e *We Are Social* (WE ARE SOCIAL, 2018) existem quase 4,2 bilhões de usuários de internet em todo o mundo e em outubro de 2018, houve um aumento de 7% em relação ao ano de 2017. Só no Brasil, o número de pessoas conectadas chega a 116 milhões, destes, cerca de 94,2% são usuários constantes de aplicações web, além de regularmente existir a troca de mensagens entre plataformas sociais (IBGE, 2016).

Segundo ainda pesquisa feita pela *HootSuite* e *We Are Social* (WE ARE SOCIAL, 2018), cerca de 3,4 bilhões de pessoas no mundo usaram as mídias sociais em setembro de 2018, um aumento de 10% em relação a setembro de 2017.

Em consonância com estes dados, a *Norton Cyber Security Report* mostra que no Brasil em 2017, o prejuízo com ataques cibernéticos é de 62 Milhões de vítimas, além de ser estimado uma perda financeira de quase R$ 83 Bilhões (cotação do dólar em 27 de julho de 2018) ficando atrás apenas da China com quase R$246 Bilhões de prejuízo com ataques de hackers (SYMANTEC, 2018).

Pesquisas elaboradas por Gross e Acquisti (2005) e Yang e colab.(2012) revelam que ao examinar uma certa vulnerabilidade das informações privativas, existe a possibilidade da realização de ataques contra a privacidade através da inferência de informações colhidas. Estes autores afirmam que mediante a busca das informações disponibilizadas pelos usuários nas plataformas de redes sociais é possível descobrir várias outras informações não informadas por eles, ampliando ainda mais, a capacidade de gerar situações passíveis de serem rodeadas por características, que trazem confiança para o usuário ser vítima.

As empresas de tecnologias aplicadas às redes sociais apresentam aos seus usuários forma de ter o resguardo dos dados pessoais, entretanto a falta de gerência dos usuários, acaba por fornecer a um público duvidoso, inúmeras informações que quando analisadas de forma mal-intencionada, podem tornar-se em um cenário ideal para aplicar técnicas de sequestro de dados e extorsão do usuário.

Os usuários de plataformas de redes sociais têm em suas mãos a capacidade de administrar suas informações prestadas com certa constância por meio de aplicações sociais. Em muito dos casos, quem utiliza essas plataformas desconhece ou até mesmo não se atenta a necessidade de que ocorra um bom senso, bem como uma boa gerência das informações nesse meio virtual. Assim como, ocorre nas empresas, as pessoas precisam compreender que a informação deve ser preservada e deve sempre ser vista como um elemento de alto valor de mercado.

O usuário é classificado como vítima em potencial quando o mesmo possui características de pessoa apta a interagir com elementos que o direcione para armadilhas personalizadas. A pessoa em questão pode ser o alvo principal ou até mesmo apenas o mecanismo para ter acesso a níveis acima, quando a proposta é obter informações sigilosas acerca da empresa na qual trabalha.

Com o exposto, este trabalho apresenta um estudo de caso que busca demonstrar que usuários de redes sociais podem ser vítimas de roubo de dados até mesmo, enquanto colaboram com uma inofensiva pesquisa de opinião. O escopo deste trabalho compreende um estudo de softwares que geram sequestro de dispositivos, conhecidos popularmente com o termo em inglês: *Ransomware*.

Estes softwares se apresentam como arquivos camuflados, executando operações de bloqueio total do aparelho, criptografando o mesmo e pode ter como única forma de recuperação dos dados, os pagamentos de resgates.

1.1 PROBLEMA DA PESQUISA

Atualmente as plataformas de redes sociais possuem inúmeras formas de gerenciar as informações que o usuário presta e avalia a disponibilidade delas para outras pessoas, mas raramente é tomada as devidas precauções acerca de a que público devem ser disponibilizadas as fotos, conversas, compartilhamentos e as curtidas de autoria do usuário. Esta falta de cuidado, torna possível através dessas informações, a criação do perfil do usuário e de sua vida diária. Este perfil pode ser utilizado por criminosos e isto pode acarretar em sequestro eletrônico de informações do usuário.

A ação dos infratores gera indisponibilidade do equipamento, o qual na maioria das vezes, possui vasta informações do usuário, o que faz com que seja necessária a recuperação destas informações. Comumente, o mecanismo de resgate é feito por uso de tecnologias de pagamentos online com auxílio de moedas digitais e carteiras criptografadas com as transações, ocorrendo através de rede *P2P* que concede uma carga de anonimidade entre as transações, denominado *BITCOINS* (NAKAMOTO, 2008).

Diante do exposto, faz-se o seguinte questionamento: Quais as precauções a se tomar no uso de redes sociais, a fim de minimizar a chance de ser vítima de um sequestro eletrônico?

1.2 OBJETIVOS DA PESQUISA

Os objetivos da pesquisa estão apresentados nas seções 1.2.1 e 1.2.2.

1.2.1 OBJETIVO GERAL

Apresentar um estudo de caso, demonstrando como usuários de redes sociais podem ser vítimas de sequestro eletrônico utilizando a técnica de *Spear Phishing* e disponibilizar medidas preventivas que podem ser adotadas para diminuir as chances de ações deste tipo de sequestro.

1.2.2 OBJETIVOS ESPECÍFICOS

Visando apresentar meios para orientar o usuário, o assunto elenca um número vasto de requisitos e dentre alguns deles possui os objetivos específicos:

- Apresentar os elementos que integram a segurança da informação com ênfase em aplicações sociais.
- Expor características da engenharia social aplicado às plataformas sociais.
- Explicar como a análise comportamental é obtida por usuários mal-intencionados, visando cenários para executar a ação de sequestro eletrônico.
- Identificar pontos de como práticas atuais dos usuários, contrastam no quesito do compartilhamento de informação sensível.
- Apresentar um estudo de caso resultado da técnica *Spear Phishing* sendo analisado qual decisão que o usuário apresentou quando

interagiu com esse tipo de ação.

- Expor soluções eficazes para combater o processo de sequestro eletrônico por meio de redes sociais.

1.3 JUSTIFICATIVA

As aplicações e plataformas de redes sociais dentro do cenário global é visto como parte do cotidiano da navegação e tem efeito motivador para que usuários se mantenham conectados na internet. Com esta necessidade criada, surge quem quer se aproveitar das informações disponibilizadas pelo usuário. Visando se aproximar, o criminoso executa procedimentos de captura dos dispositivos da vítima e a expõe a diversas ameaças virtuais e para finalizar pode solicitar pedidos de resgates.

A proposta desses criminosos virtuais é direcionar ataques bem-sucedidos em troca de ganhos monetários ou mesmo notoriedade, dentro da comunidade no qual está inserido. Quando se trata de aplicações sociais, um campo maior é visado, pois o ataque é semelhante ao sequestro físico, desta forma, o usuário deve compreender que sua chance de ser vítima, diminui se for feito o uso de políticas de segurança (SIMON; MITNICK, 2003).

A engenharia social proporciona ataques de várias formas, os mais comuns utilizam vias virtuais. Uma das técnicas utilizadas para se sequestrar dados sensíveis do usuário é através do sequestro eletrônico por meio de utilização de *exploits* ou *phishing scam*; O pedido de resgate é feito através de e-mail anônimos com pagamentos por vias de moedas digitais (*bitcoins*), desta forma não é possível enxergar a origem ou destino do beneficiado. Um fator complicador neste tipo de ação é que à medida que ocorre uma tentativa de mitigar tal ação, aumenta a quantidade de variantes de aplicações de sequestro, tornando necessário a tomada de medidas de precauções constantes para minimizar a possibilidade desses ataques.

De acordo com um estudo do *Norton Cyber Security Insights* houve um aumento de cibercrimes no Brasil da ordem de US$10,3 Bilhões no ano de 2016

para US$ 22,5 bilhões no ano de 2017 (SYMANTEC, 2018). Constatou-se também que no Brasil, cada vez mais, o usuário sofre golpes de *phishing*, que é a atividade maliciosa mais detectada por empresas de segurança.

Com o alarmante aumento de cibercrimes cometidos em usuários de redes sociais é necessário gerar alertas sobre como a ingerência de informações destas plataformas deve ser evitada, tendo em vista que criminosos podem em algum momento ter acesso aos armazenamentos dos dados de grande valia aos usuários.

1.4 ORGANIZAÇÃO DA PESQUISA

Esta pesquisa além deste capítulo, compõe-se de mais três capítulos, assim distribuídos:

No capítulo 2 são elencados os conceitos que fundamentam a monografia apresentando elementos inerente ao tema da pesquisa como engenharia social, *Phishing Scam, exploit,* estenografia*, malware* e *bitcoin.*

No capítulo 3 são descritos e analisados pontos inerentes a pesquisa, tais como a preparação, análise e resultados do questionário, bem como, as ferramentas utilizadas, o ambiente simulado e os seus resultados.

O capitulo 4 apresenta as considerações finais, medidas preventivas para minimizar o efeito de ser alvo do que é sugerido no tema da pesquisa juntamente com sugestões para trabalhos futuros.

Por fim são apresentadas as questões abordadas durante a pesquisa, dentro da plataforma online de formulário do *Google* necessárias para identificação do perfil do entrevistado presente no apêndice A.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são apresentados os assuntos principais do escopo deste Trabalho de Conclusão de Curso. Na seção 2.1 é apresentada a engenharia social que trata das técnicas de abordagem que são utilizadas para os cibercrimes serem cometidos. Na seção 2.2 trata de técnicas e personalização de ataques com utilização de iscas orientadas com base na engenharia social. Na seção 2.3 apresenta argumentos sobre o conceito de exploit que é utilizado através das falhas de hardware e software. A seção 2.4 explicita a técnica de camuflagem de dados de termo denotado estenografia. A seção 2.5 aborda o conceito de malware, além da apresentação da aplicação da pesquisa que é o Ransomware com o uso da estenografia. E na última seção é apresentado o conceito de bitcoin que foi identificado como sendo o recurso utilizado para efetivar transações de resgastes.

O sequenciamento das seções se deu com a proposta de apresentar cada etapa identificada que gera o processo de sequestro eletrônico desde o momento de identificação do alvo até a conclusão da ação maliciosa.

2.1 ENGENHARIA SOCIAL

A Engenharia Social possui como ideia norteadora, dentro de um contexto de segurança da informação, o rastreio e a ludibriação psicológica de pessoas para executar ações ou mesmo torna-se efetiva a disponibilidade de informações confidenciais. O termo também é associado a um conjunto de técnicas cujo objetivo é a obtenção de informações relevantes a respeito de um determinado indivíduo ou organização. Segundo Ulbrich e Valle (2009), as informações com dados sensíveis são provenientes quase sempre de pessoas próximas ao alvo, se encaixa como espionagem, é então quando se figura o termo Engenharia Social.

Esse tipo de abordagem é uma forma utilizada para identificar alvos suscetíveis a armadilhas, tornando-os até mesmo, potenciais vítimas de sequestro eletrônico, dado que se for possível traçar o perfil do usuário com algumas informações, existe a chance de obtenção de sucesso em pedido de regastes por pessoas mal-intencionadas.

Os usuários de plataforma sociais compartilham informações que ao serem analisadas por usuários mal-intencionados pode haver a adoção de arquivos contendo instruções que analisam a possibilidade de existência de um *exploit*[1]. Estes tipos de softwares são camuflados, com uso de estenografia.

Quem faz uso das técnicas de Engenharia Social foca em determinar o comportamento de seus alvos e compreender melhor seus *"modus operandi",* monitoramento de horários, hábitos e círculos sociais, colhendo o maior número de informações possíveis, nesse sentido, traça um perfil e posteriormente pode acionar ações de ataque sistemático neste perfil.

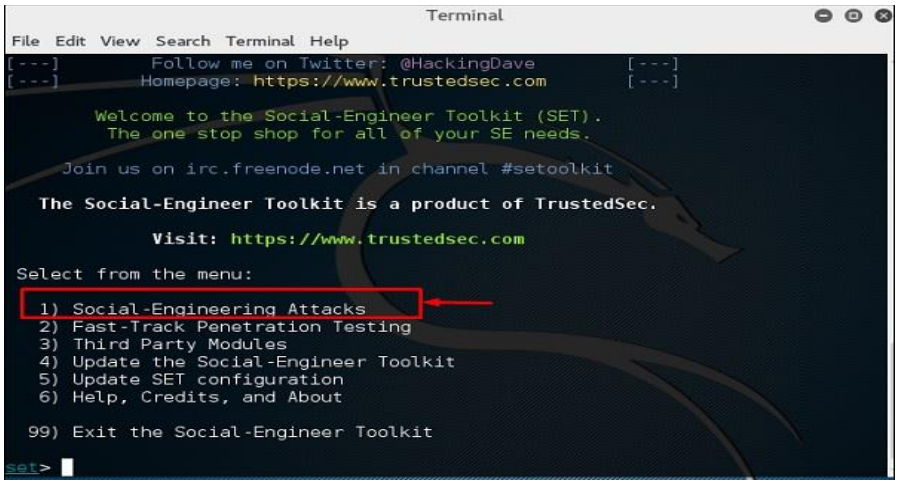
2.2 FERRAMENTAS DE ENGENHARIA SOCIAL

Para a criação de um perfil específico é necessário a presença de

[1] Termo em inglês que faz referência a softwares maliciosos com instrução direcionado para falhas.

ferramentas que ampliem o rastreio de informações, a fim de detalhar com maior precisão as informações da pessoa. Mesmo ciente que para a engenharia social o fator humano é levado em consideração mais que qualquer outra técnica, a presença de elementos que potencializam a efetividade da engenharia é muito bem vista, quando se trata de gerenciar informações do alvo específico.

Figura 1 - Imagem do Programa Social Enginner ToolKit

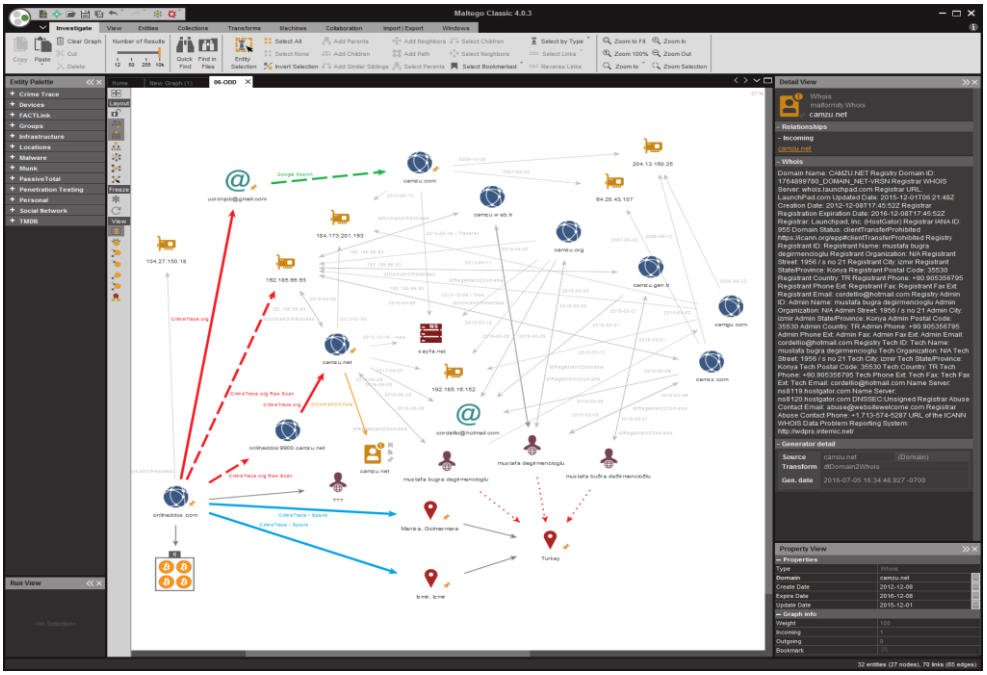


Fonte: Própria.

Dentre algumas ferramentas, destacam-se o *Maltego, Social Engineer Toolkit*, este último presente, em distribuições nativas do *Kali Linux*[2] (Figura 1) que possui um arsenal de técnicas para aplicar dentro de um contexto que se aplica a engenharia social. Dentre essas técnicas, apresenta-se a utilização de páginas clones, bem com estratégias de ataques MITM[3] que se enquadra na parte de criação de ambientes que venham gerar confiança.

[2] Kali Linux – Distribuição Linux com ferramentas para atuação na área de segurança de informação como visto em https://kali.org.
[3] MITM – Abreviatura de palavra estrangeira do inglês Man In The Middle, homem do meio, que é uma técnica utilizada para escutar transmissões e garimpar dados entre essas transações.

Figura 2 - Maltego, software de engenharia social



Fonte: Mensk (GLEB ESMAN, [s.d.]).

Outro software, o Maltego (Figura 2) possui a capacidade de criar o cenário apresentador, a possibilidade de identificar atores com descrição que caracterizam aquele indivíduo, além de gerar ligações entre os mesmos. Este software pode aprimorar os rastreios e a gerencia das informações dos usuários, bem como seus relacionamentos com outros atores, visando indicar possibilidades para aplicar as outras técnicas de engenharia social. (PATERVA,2019)

2.3 PHISHING SCAM

O *Phishing Scam* é apresentado para designar tentativas de obtenção de informação pessoal utilizando técnicas que oferecem aproximação do atacante para com o alvo, sem que o mesmo o identifique, ao ponto de interferir no procedimento do criminoso dentro do contexto da informática (BALTZAN, 2016).

Figura 3 - Tela de Phising Scam recebido por e-mail

Fonte: CanalTech (ULTRADOWNLOADS, 2012)

A palavra é derivada de o termo em inglês pescar – *phishing*, devido a forma de como é feita a captura dos dados, tendo em vista que existe a necessidade da utilização de uma isca como exemplo na (Figura 3), não havendo a necessidade da sua utilização em um alvo especifico.

O termo surgiu em meio a comunidades hackers do Estados Unidos. Em 1996, este termo foi utilizado em um fórum para identificar a forma de angariar contas de um serviço de e-mail na época chamado AOL[4].

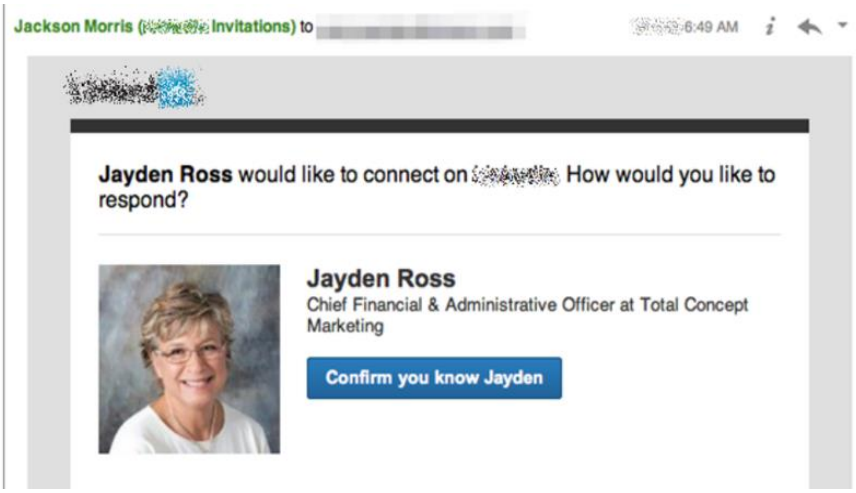
Para conseguir efetivar a ação muitas dessas iscas são construídas a partir da análise do alvo com informações adquiridas pela engenharia social, neste caso, a aprimoração dessa atividade tem o termo *Spear Phishing*.

[4] AOL é acrônimo da empresa americana América On Line provedor de serviço de internet.

2.3.1 SPEAR PHISHING

Ao passo que o *Phising Scam* é utilizado sem ter um alvo especifico, quando ocorre a busca de um alvo em específico dar se a o termo em inglês *Spear Phishing* para identificar uma personalização dessa técnica. O usuário pode ser o alvo final ou apenas o meio para o rastreio e geração de coleta de informações sensíveis, aumentando a probabilidade de sucesso na obtenção dos dados.

Figura 4 - Tela de spear phishing direcionando para captura de dados.



Fonte*:* TechWorld (DUNN, [s.d.])

Como exemplo a (Figura 4) representa um convite com informações que solicita a validação de um relacionamento pessoal numa rede social, o texto em inglês "*Confirm you Know Jayden*[5]" em questão, representado por um botão irá encaminhar o usuário a outro serviço que possa ocorrer procedimentos de captura de informações.

A definição para um ataque sistemático direcionado para uma única pessoa ou empresa tendo por base o termo *Spear Phishing* (FEDERAL BUREAU INVESTIGATION, 2009) seria ao equivalente a pesca com arpão, na qual definido o alvo, não é levado em consideração, outros alvos para se fisgar.

Neste tipo de ataque, conseguir o controle da máquina é o resultado final, pois as etapas que levam o usuário a este resultado, vai desde

[5] Tradução: "Confirma que conhece Jayden"

questionamentos até mesmo a sugestão pelo atacante de arquivos camuflados com instruções não cientes pelo lado do alvo, uma vez identificado qual *exploit*[6] é funcional no ambiente do usuário, que leva a condição do atacante a uma elevação de privilégios que pode orientar a tomada de decisões da máquina de forma remota.

2.4 EXPLOIT

Hardware e software são construídos seguindo especificações e preocupações dentro da narrativa de engenharia de software ou mesmo em engenharia da computação, na qual cada etapa oferece todo aporte necessário para confecção de uma aplicação ou de um dispositivo livre de falhas.

A ideia de gerar um produto final seja software ou hardware sem qualquer problemas futuros é algo que dificilmente ocorre, já que com o uso de engenharia reversa, técnica utilizada para desconstruir uma aplicação ou dispositivo, afim de observar possíveis falhas, possui e facilita a identificação de fatores críticos nas aplicações para a criação de pequenas partes de código que se utilizam dessas brechas deixadas para elevar privilégios dentro de uma aplicação, geralmente construído por *hacker* ou entusiastas de engenharia reversa.

Existem falhas que não são divulgadas dentro das comunidades Hackers são chamados “0-*day*” (dia zero) onde a posição da falha é tão crítica que existe a necessidade da recriação de todo o projeto da aplicação ou do dispositivo para que ocorra a correção do problema. Para aqueles que possuem os “0-*days”* o nível de influência na comunidade, bem como a característica que elevam o conceito da pessoa detentora desse *exploit* (SYMANTEC, 2018).

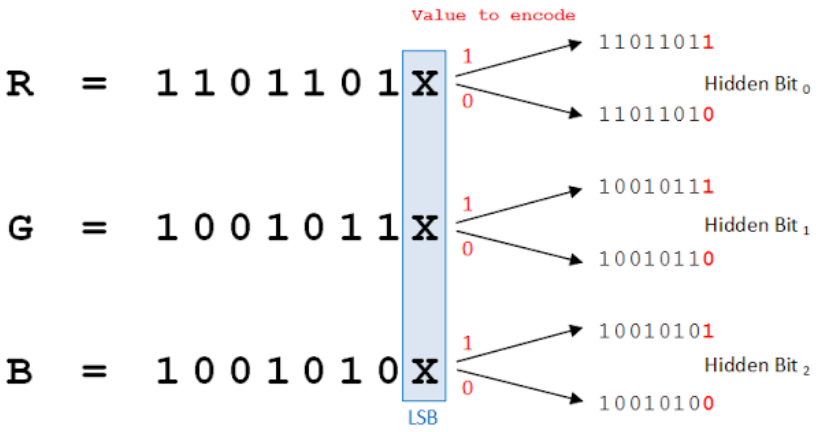
[6] Exploit software que utiliza de brecha em programas originais com erro não corrigidos pelas fabricantes.

2.5 ESTENOGRAFIA

O conceito de estenografia é esconder uma mensagem dentro de outra ou mesmo informações dentro de objetos, que podem ser: arquivos de vídeos, músicas ou imagens. A técnica utilizada para camuflar aplicações visando o transporte, parte de um princípio simples: Existe um mensageiro que possui a necessidade de enviar uma mensagem para um receptor sem que ocorra a compreensão da real mensagem por quem faz o transporte quando este não possui a confiança de quem envia (POLLON, 2006) sem que o usuário que venha manipular o arquivo venha ter conhecimento.

A operação de camuflagem depende em certos momentos de software específico para ocorrer a mescla das aplicações entre as diversas aplicações existente, dentro da distribuição *linux Kali*, o *"steghide"* é utilizado amplamente para executar essa operação, podendo utilizar a técnica em arquivos de áudio e imagem (HETZL, 2002).

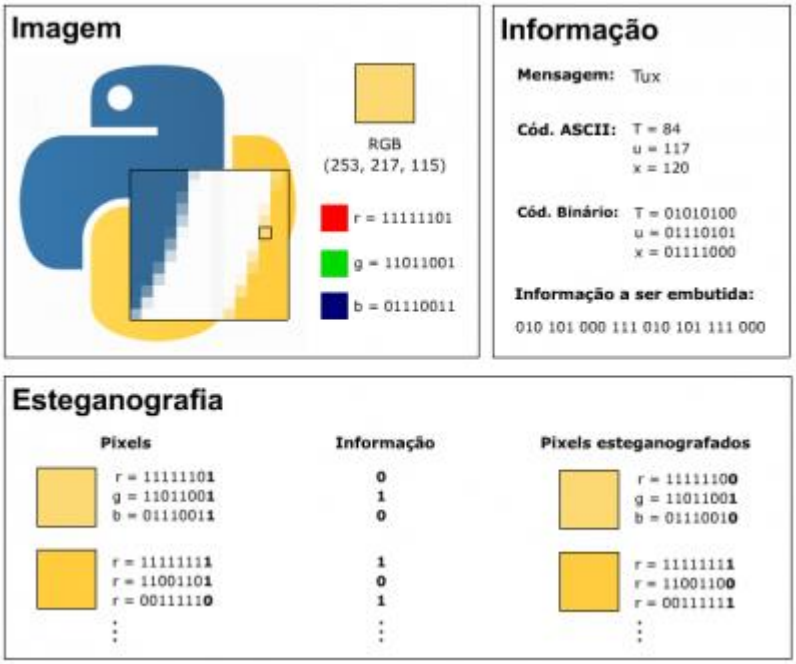
Figura 5 - Representação do último bit significante para utilização da estenografia.



Fonte: KitPloit (BLACK, [s.d.])

Existem diversas formas de aplicar a estenografia, a utilizada de forma mais eficiente é a *"Least Significant Bit"* que de acordo com Fortini (1998) como apresentado na figura 5, vem tratando da busca do bit com menor significância para inserir um bit contendo informação nova o que resulta na inserção de conteúdo dentro de um outro que detinha uma forma original.

Figura 6 - Funcionamento de estenografia com uso de texto e imagem



Fonte: Viva O Linux (“Esteganografia utilizando steghide [Artigo]”, [s.d.])

A Figura 6 apresenta como ocorre o funcionamento da estenografia LSB, onde a *string*[7] "Tux" é acoplada em uma imagem com o logotipo da linguagem Python sendo possível enviar a imagem para outro usuário com essa informação a mais, junto com a imagem em questão.

2.6 MALWARE

O software malicioso faz a construção do termo *malware (malicious software)* que vem sendo empregado para programas desenvolvidos especificamente para executar operações ou gerar comportamento malicioso em um computador. Uma vez que a aplicação instalada na máquina possibilita inúmeras ações que vão desde rastrear informações pessoais ao ponto de tomar certas atitudes na máquina alvo, como passar pelo usuário devidamente autenticado, conseguindo até obter acesso a níveis de privilégios e gerando possibilidades de controle remoto do equipamento.

[7] String termo utilizado para definir palavra em linguagem de programação.

O emprego dessa aplicação geralmente é utilizado para obter vantagens financeiras, coleta de informações sigilosas ou apenas por vandalismo ou auto promoção pessoal (CERT, 2018).

2.7 RANSOMWARE

Ransomware é um termo em inglês que significa aplicação de resgate e que se trata de um subtipo de *malware* do tipo cavalo de troia, que foca em instalação de aplicações com intuito de deixar um acesso remoto para o atacante, possuindo como principal ação, bloquear o acesso aos arquivos ou sistemas e liberando apenas com o pagamento de um resgate por um valor especificado (DA SILVA, 2017).

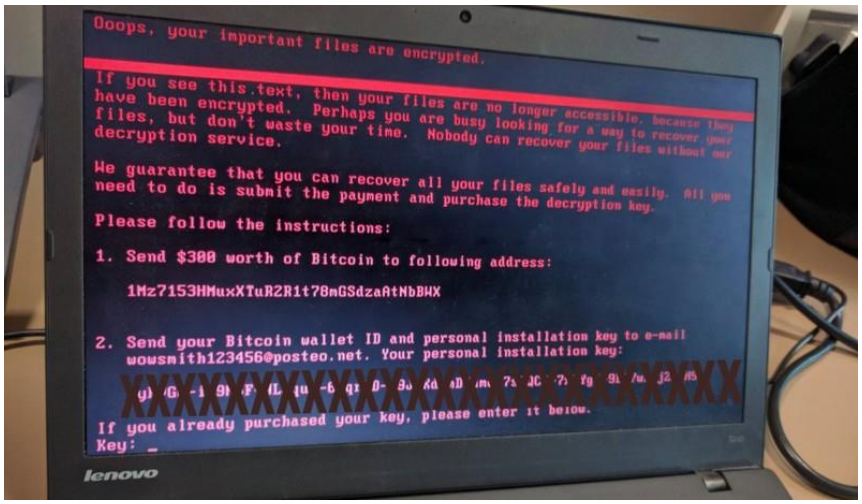
Figura 7 - Tela de entrada do ransoware que se apresentava como um Cassino

Fonte: Q-CASINO.COM (Malware Example, [s.d.])

Apesar de estar presente nos noticiários atualmente, *Ransomware* não é um conceito novo, este conceito é datado desde 1980, com o codinome Casino, que era um vírus de DOS que copiava dados da memória RAM e do sistema de arquivo FAT, apagando todo o conteúdo do HD, mas não exigia o usuário desembolsar resgate. ao passo que somente liberava se o usuário contasse num jogo estilo caça-níquel que se exibia na tela como visto na (Figura 7) (DA SILVA, 2017)

Ao longo de quase 11 anos os *Ransomwares* tiveram inúmeras variantes que se apresentavam nas mais diversas plataformas, utilizando novas formas de criptografia, inúmeras formas de instalação e técnicas de terrificar o usuário, além do principal, solicitar resgates. Atualmente as variantes que estão sendo amplamente divulgadas com noticiários de ataques em massas, são as *Petrywrap (*Figura 8), *Wannacry e Cryptlocker* [8](DA SILVA, 2017) .

Figura 8 - Petrywrap aplicado a um notebook



Fonte: https://www.windowscentral.com

A propagação de um *Ransomware* pode ocorrer induzindo a vítima a executar o programa local para dar abertura a uma ação remota ou local de instalação de aplicação que restringe o usuário a utilizar os seus dados.

Outra possibilidade de propagação se dá através do uso de *exploit* de vulnerabilidades conhecidas e não corrigidas, forçando que as empresas que mantêm essa vulnerabilidade, informe patch de segurança para corrigir tais problemas, como exemplo recente, tem-se a versão modificada e disponibilizada do famoso *CCLEANER*[9] *(*utilitário para limpeza de registro e dados do computador) que teria infectado 2,2 milhões de usuários e os criminosos tiveram a sua disposição informações como: nome do computador, lista de programas instalados e processos em execução, além de endereços MAC de adaptadores de rede da máquina, dentre outros dados (BRUMAGHIN, 2017)

[8] Variantes de *ransomware* com especificações diferente, mas com a mesma ação principal de sequestro eletrônico de dispositivos.
[9] *Software* produto da empresa Piriform. Fonte: https://www.ccleaner.com/pt-br

2.7.1 ESTENOGRAFIA PARA UMA VARIANTE DE RANSOMWARE: SYNCCRYPT

A Estenografia possui a capacidade de camuflar e acrescentar a possibilidade de ampliar o potencial do uso da técnica em outras situações uma delas dentro da narrativa *Ransoware*.

Esta camuflagem vem sendo possível com a presença de uma técnica chamada de *SyncCrypt,* como visto o código de criação na figura 9. O intuito é que uma vez que se apresenta para usuários de sistemas operacionais *"Windows"*, ele venha executar algumas regras que no ambiente Windows são costumeiramente de auto executar com um clique apenas.

Eles são espécies de macros orientados para execução como objeto ActiveX, o uso deles tem sido desencorajado por constantes falhas no quesito segurança (VOLTOLINI, 2014), geralmente é distribuído como uso de anexo de correio eletrônico contendo arquivos de script para *Windows* (WSF).

Figura 9 - Exemplo de código, WSF, do SyncCrypt

```
var oShell = new ActiveXObject("WScript.Shell");
appdir = oShell.ExpandEnvironmentStrings("%temp%"), downloc = appdir + "\\" + makeid(), appdir +=
"\\BackupClient";
var u1 = "https://image.ibb.co/mxRqXF/arrival.jpg",
    u2 = "http://sm.uploads.im/X8IOl.jpg",
    u3 = "http://185.10.202.115/images/arrival.jpg";
try {
    download(u1, downloc + ".jpg") && download(u2, downloc + ".jpg") && download(u3, downloc + ".jpg") ?
    WScript.Quit(0) : exp(downloc, appdir)
} catch (err) {
    WScript.Quit(0)
}
fs = new ActiveXObject("Scripting.FileSystemObject"), fs.DeleteFile(downloc + ".jpg"), fs.DeleteFile(downloc + ".zip"),
desktop = oShell.ExpandEnvironmentStrings("%userprofile%"), desktop += "\\desktop" ;
var d = new Date,
    time = msToTime(d.getTime() - 6e4 * d.getTimezoneOffset()); - 1 != version().indexOf("Windows XP") && (time +=
    " /ru SYSTEM"), oShell.Run('schtasks /CREATE /F /TN sync /TR  "' + appdir + '\\sync.exe -e \\"' + desktop + '\\"" /sc
    once /st ' + time), WScript.Echo("This file version is not compatible with your Windows machine. Please update your
    system.") ; <
/script> <
/job>
```

Fonte: BleppingComputer (ABRAMS, 2017)

O arquivo de *script*[10] por sua vez em seu código, força o usuário a fazer o *download* de uma imagem com um arquivo do tipo .zip com executáveis para operação padrão de todo *Ransomware*. Este criptografa

[10] *Script* e o termo utilizado na informática para apresentar um conjunto de instruções.

todos os dados usando AES além de acrescentar uma terminação “kk” em todos os arquivos da vítima. Além de prover um arquivo do tipo .html contendo as informações para recuperação dos arquivos afetados pela ação dessa variante de *Ransomware* (ABRAMS, 2017).

O *SyncCrypt* pode ser customizado o que dificulta em recuperar os dados e evitar de acontecer a contaminação por este *malware* mas a forma de se apresentar no ato da infecção e bastante compreendida pela heurística de muitas aplicações de antivírus que observa quando o usuário faz transferência de arquivos para seu computador bloqueando a ação de *“download”* remoto dos arquivos (ABRAMS, 2017).

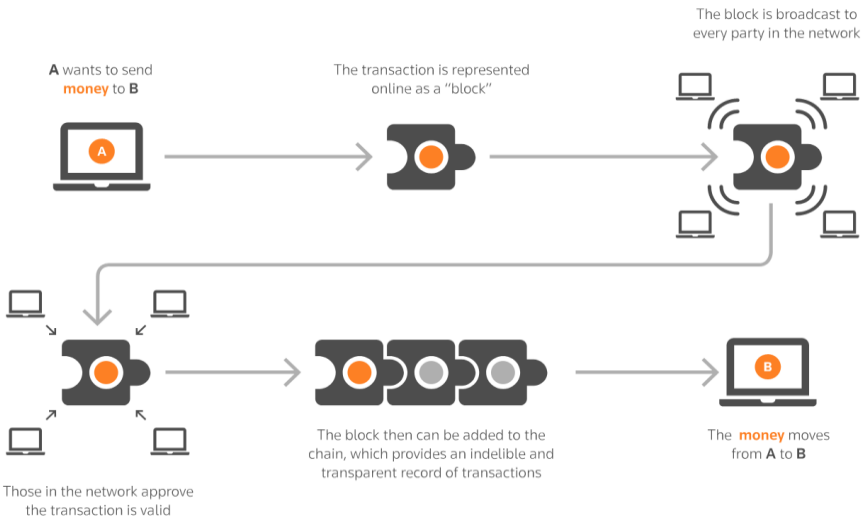
2.8 BITCOIN

O *Bitcoin* é um conceito de moeda virtual que atualmente está sendo utilizado em larga escala, já possuindo valores comerciais que variam com o decorrer do tempo, por conta da demanda de *Bitcoin*.

A estrutura do *Bitcoin* se resume a operações, nas quais o usuário cria uma carteira virtual e pode transacionar para outra carteira, sem que nenhum dado pessoal venha ser compartilhado ou informações a respeito da transação sobrevivam para que seja investigada posteriormente pela polícia

Os únicos dados mantidos são registros públicos, essas transações são atrelados a um livro razão que mantem informações acercas de todas as transações guiado na forma de encadeamento de blocos que sugere o termo em inglês para nomina-lo por *blockchain*, de transferência de *Bitcoin* da carteira "A" para a carteira "B" que, no entanto, podem estar sob pseudônimos (NAKAMOTO, 2008), como pode-se visualizar na figura 10.

Figura 10 - Transação de bitcoin com o conceito da blockchain e suas validações



Fonte: Blockchain/Bitcoin ("Are you ready for blockchain?", [s.d.])

A razão pela qual os criminosos se utilizam deste método para receber a maioria dos resgates, se dá pelo simples fato do *BITCOIN* ser descentralizado, ou seja, não depende de uma instituição financeira, banco de operações e agências governamentais para que ela venha ocorrer, dificultando o rastreio dos participantes e de suas trocas, sugerindo uma forma de facilitar em questões como de lavagem de dinheiro (NAKAMOTO, 2008).

O procedimento utilizado para rastrear o dono da carteira virtual depende diretamente da quantidade de vezes que se pode observar o endereço de *ip*[11] da origem ou do receptor, possuindo rastros replicados ou outras informações na internet. Para criminosos que aplicam sequestro eletrônico, a utilização do *Bitcoin* como forma de pagamento, favorece manter o anonimato por parte do autor da ação, dificultando gerar indiciados por algum crime (CONTI e colab., 2018).

A aplicação prática do *Bitcoin* no contexto do *Ransomware* se dá pela adoção como forma de pagamento oficial para resgatar a máquina e possibilitar a recuperação da informação. Ocorrendo o repasse, ainda corre-se o risco de não acontecer a concretização do fornecimento das informações para recuperar a máquina alvo (CONTI; GANGWAL; RUJ, 2018).

[11] Internet Protocol – Protocolo de internet

2.9 SEQUESTRO ELETRÔNICO: PONTO DE VISTA LEGAL

Acerca do sequestro eletrônico a punição de quem pratica tal ação é prevista em lei com a devida interpretação jurídica de cada caso. Com a dificuldade que se tem para identificar infratores que utilizam da tecnologia para efetuar ações de sequestro eletrônico, do ponto de vista legal a depender da concretização do ato, quem executar tais ações de sequestro acaba por se enquadrar em questões de extorsão, ameaça e invasão podendo incorrer ao menos em três tipos penais, previsto em lei:

- Extorsão, prevista pelo artigo 158 do Código Penal:

Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa:
Pena - reclusão, de quatro a dez anos, e multa.
§ 1º - Se o crime é cometido por duas ou mais pessoas, ou com emprego de arma, aumenta-se a pena de um terço até metade.
§ 2º - Aplica-se à extorsão praticada mediante violência o disposto no § 3º do artigo anterior.
§ 3º Se o crime é cometido mediante a restrição da liberdade da vítima, e essa condição é necessária para a obtenção da vantagem econômica, a pena é de reclusão, de 6 (seis) a 12 (doze) anos, além da multa; se resulta lesão corporal grave ou morte, aplicam-se as penas previstas no art. 159, §§ 2º e 3º, respectivamente.
(BRASIL, 1940, on-line)

- Ameaça, prevista pelo artigo 147 do Código Penal:

Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave:

Pena - detenção, de um a seis meses, ou multa.

Parágrafo único - Somente se procede mediante representação.

(BRASIL, 1940, on-line)

- Invasão de dispositivo informático, prevista pelo artigo 154-A do Código do Processo Penal (2012):

Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita"

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou

> o controle remoto não autorizado do dispositivo invadido:
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
>
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
>
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
>
> I - Presidente da República, governadores e prefeitos;
>
> II - Presidente do Supremo Tribunal Federal;
>
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal;
>
> IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal
>
> (BRASIL, 2012, on-line)

Existem elementos de lei no campo jurídico que dá vista a efeito de condenação a indivíduos que venha a praticar o ato do sequestro eletrônico. Esta pesquisa busca alertar como a ingerência das informações em plataforma sociais podem possibilitar ações que podem ter condenações no campo jurídico.

Vale salientar na questão jurídica acerca do processo de execução desses procedimentos que até o próprio, o Marco Civil da Internet, reunido pela lei 12.965/2014, que reforça quais são os princípios de garantia da privacidade, intimidade, proteção de dados, sigilo das comunicações, segurança e responsabilização dos agentes na Internet (artigos 3º, 7º, 10°) repudia e apresenta critérios de penalidade (BRASIL, 2014, on-line). Desta forma é desencorajado veementemente a execução de atividades que possam vir a ser enquadradas como crimes virtuais.

3 ESTUDO DE CASO

Neste capítulo será apresentado levantamento seguido de aferição de comportamento, dividido em cinco tópicos, na seção 3.1 descreve-se o projeto que apresenta técnicas de engenharia social para coleta dos dados, na seção 3.2 é demonstrado o questionário que serviu de ferramenta coletora, as ferramentas de apoio utilizadas no estudo de caso são apresentadas na seção 3.3, enquanto que a seção 3.4 descreve como se deu a coleta e análise dos dados, os resultados da pesquisa são expostos na seção 3.5.

3.1 PROCEDIMENTOS METODOLÓGICOS - PROJETO

O projeto foi realizado através da utilização de técnicas de engenharia social aplicadas dentro de um modelo de questionário para usuários, onde além dos resultados coletados, o ambiente servirá também como ambiente para teste da temática abordada neste trabalho.

O questionário irá conflitar questões acerca da postura do internauta frente a gestão das suas informações em âmbito de redes sociais, paralelamente ocorrerá a coleta das informações. Enfatizando que não são armazenadas informações que visem identificar nominalmente o usuário.

A aplicação da proposta visa demonstrar que até em ambientes controlados, existe a possibilidade de aplicar a injeção remota de arquivos e identificar a quantidade de usuários que quando surpreendidos com um *download* despretensioso, recusam o recebimento do arquivo, mesmo que este esteja relacionado ao tema base da pesquisa que o usuário aceitou se submeter.

Figura 11 - Código da página contendo formulário dentro de um ambiente de teste

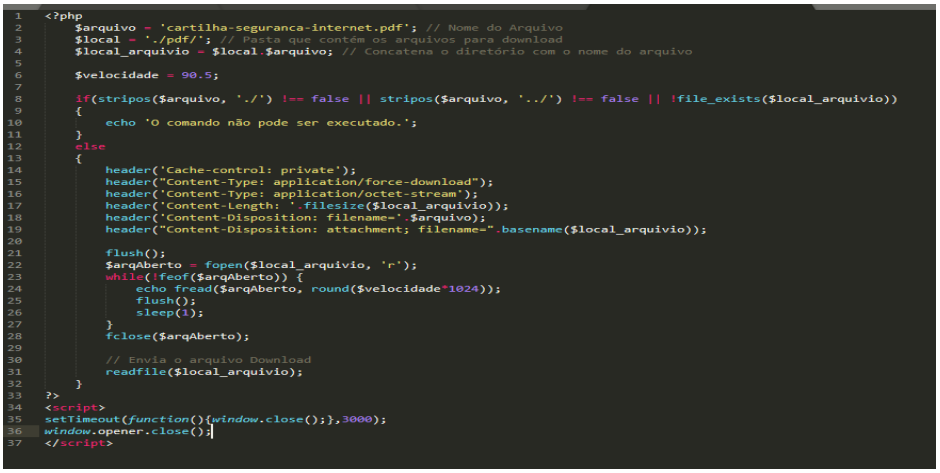
```
<?php
//include("pdf.php");
//echo "<script>window.open('https://goo.gl/forms/3fiw1s0XnxsCNqtA2');</script>";

?>
<style>
    iframe {
    border: 0;
    height: 100%;
    left: 0;
    position: absolute;
    top: 0;
    width: 100%;
}
</style>
<iframe src="https://goo.gl/forms/3fiw1s0XnxsCNqtA2" allowfullscreen></iframe>
<script>setTimeout(function() {
  window.open('/pdf.php');
}, 10000);
</script>
```

Fonte: Própria

A figura 11 retrata como foi disponibilizado o formulário online feito no *Google Forms*[12] e indexado dentro de uma página que partilhava fora dos domínios da empresa detentora do produto. Foram utilizados a *metatag iframe* do *html,* que se trata de uma chamada especifica para criação de um janela que aponta para outra pagina o termo *iframe* e um sintaxe prevista na linguagem de marcação de *hypertexto*, para anexar o formulário para que pudessem ser apresentados em primeiro plano no domínio https://sshlock.com.br, este domínio foi desativado após a pesquisa, e ocultamente, ocorria o procedimento de envio de arquivos e rastreio de informação.

[12] Google Forms é uma plataforma proprietária da Google para geração de formulários online.

Figura 12 - Código da página que força o envio do arquivo “malicioso” com limitador de velocidade



```php
<?php
    $arquivo = 'cartilha-seguranca-internet.pdf'; // Nome do Arquivo
    $local = './pdf/'; // Pasta que contém os arquivos para download
    $local_arquivio = $local.$arquivo; // Concatena o diretório com o nome do arquivo

    $velocidade = 90.5;

    if(stripos($arquivo, './') !== false || stripos($arquivo, '../') !== false || !file_exists($local_arquivio))
    {
        echo 'O comando não pode ser executado.';
    }
    else
    {
        header('Cache-control: private');
        header("Content-Type: application/force-download");
        header('Content-Type: application/octet-stream');
        header('Content-Length: '.filesize($local_arquivio));
        header('Content-Disposition: filename='.$arquivo);
        header("Content-Disposition: attachment; filename=".basename($local_arquivio));

        flush();
        $arqAberto = fopen($local_arquivio, 'r');
        while(!feof($arqAberto)) {
            echo fread($arqAberto, round($velocidade*1024));
            flush();
            sleep(1);
        }
        fclose($arqAberto);

        // Envia o arquivo Download
        readfile($local_arquivio);
    }
?>
<script>
setTimeout(function(){window.close();},3000);
window.opener.close();
</script>
```

Fonte: Própria

O usuário ao acessar o site com o questionário, em um determinado momento era sugerido o recebimento de um arquivo no formato PDF[13] com um conjunto de instruções e demandado para o navegador do usuário um conjunto de instrução para limitar a velocidade da transação, exemplo na figura 12.

O limite de velocidade foi proposto para gerar uma condição para capturar a reação do usuário para enxergar a tomada de decisão em dar continuidade em receber o arquivo ou não.

Com o título sugestivo apresentado que remetia a instruções sobre segurança dentro de uma cartilha, o servidor que hospedava o ambiente de teste recebia em paralelo a informação da aceitação ou recusa do arquivo pelo usuário.

Tal procedimento veio com a ideia de questionar a proposta levantada pela pesquisa, dado que dentro de uma narrativa, ideias dos usuários sobre segurança na web são na prática observadas por eles? Estão de fato atentos ao que recebem em seus computadores quando estão online? Seus sistemas de segurança são adequados para alertá-los sobre recebimento de arquivos, imagens estranhas ao ambiente de seus computadores? O resultado obtido tem o propósito de avaliar se de fato os usuários estão mais protegidos ou se ainda são muito suscetíveis a ataques virtuais maliciosos que podem proporcionar sequestros eletrônicos. Em nossa avaliação, o aceite de um arquivo sem conhecimento de seu teor, pode viabilizar esta ação.

Seguindo a proposta do questionário, cujos resultados são apresentados

[13] PDF – Portable Document File, arquivo de documento portátil.

na seção 3.2, a coleta das informações vem com intuito de analisar o perfil do usuário, sendo aplicada a públicos diversos, a fim de gerar uma variância no momento que se é avaliado o nível de segurança que a pessoa possui, estando a frente de situações diárias em plataformas sociais.

A captura da informação do lado do servidor se houver o recebimento do arquivo vazio teve a proposta de gerar um questionamento para o entrevistado sem a necessidade de perguntar explicitamente, levando-se em consideração a tomada de atitude não pratica.

O ato de receber ou não o arquivo é presente quando o usuário se submete a uma experiência de um ataque real, no qual com base nas suas respostas irá configurar em um possível sequestro eletrônico. Por procedimentos similares serem reproduzidos quanto ao envio do arquivo de forma abrupta.

3.2 QUESTIONÁRIO

A técnica utilizada para a coleta de dados foi feita através de questionário online, com alcance de 107 usuários até o fechamento da pesquisa, composta por 21 perguntas objetivas que foram separadas por seções.

Estas perguntas versavam sobre a identificação do perfil, a proximidade que cada pessoa tem com a tecnologia e aplicações sociais e para finalizar, com busca do padrão de comportamento dos usuários, frente a algumas situações que se apresentam no cotidiano do usuário na internet. Dessa forma, o questionário apresenta uma visão ampla com um nível de alcance, além do domicílio da pesquisa, rastreando comportamentos necessários para respaldar a pesquisa.

O questionário desenvolvido, encontra-se no Apêndice A, com a ciência da orientadora e do coorientador, verificando a possibilidade de criar eixos para selecionar o pesquisado e identificar com mais afinco elementos resultantes com maior grau de proximidade com a temática do projeto/pesquisa, a condução internamente gerada durante a pesquisa, em relação a proximidade com a Internet, não apresentou fenômenos que viesse interferir nos resultados.

3.3 FERRAMENTAS DE APOIO UTILIZADA

Para que o projeto tivesse a profundidade devida, houve a necessidade de apoio em algumas ferramentas que pudessem auxiliar, desde o engajamento de participantes para o questionário, bem como a coleta de respostas e além de traçar o perfil do usuário que teve contato com o portal que abrigava o formulário.

Como a proposta tinha como fundamento a criação de um formulário que servisse também como ambiente para testar a temática da monografia foi utilizado a plataforma de formulário, *Google Forms* online que foi inserida dentro de uma página, utilizando a técnica de *tag* de marcação para IFRAME, com recursos previamente orientados a identificar o perfil do usuário para disponibilizar dados demográficos.

Para o ambiente teste foi desenvolvido uma página com instruções em *JavaScript* para forçar o envio do arquivo PDF, bem como, gerar um efeito limitador de velocidade da ação de download, esse já concedendo ações para que o próprio navegador limita-se receber o arquivo em questão.

Para efeito de engajamento de público foi disponibilizado o *link* https://sshlock.com.br, este domínio foi desativado após a pesquisa, que durante o projeto foi criado para facilitar o compartilhamento do acesso, sem a ideia de usar encurtadores de links ou semelhante.

Na distribuição dos links, os replicadores eram orientados a informar que a coleta de dados era anônima, que no caso, não era possível nominar quem fez qual resposta às questões elencadas na pesquisa.

3.4 SIMULAÇÃO SPEAR PHISING, “CARTILHA DE SEGURANÇA .PDF”

A entrevista possuía uma última questão a ser respondida sendo observado a atitude que o entrevistado teria diante de uma narrativa simulada de sequestro eletrônico com a utilização da engenharia social e com características de personalização do ataque direcionado *Spear Phishing*.

Durante a fase do questionário que estava em processo, o usuário foi submetido a receber um arquivo contendo possíveis informações sobre segurança. Como o argumento do questionário girava em torno do elemento segurança poderia ser questionável a aceitação de um arquivo de forma forçada pelo site em questão.

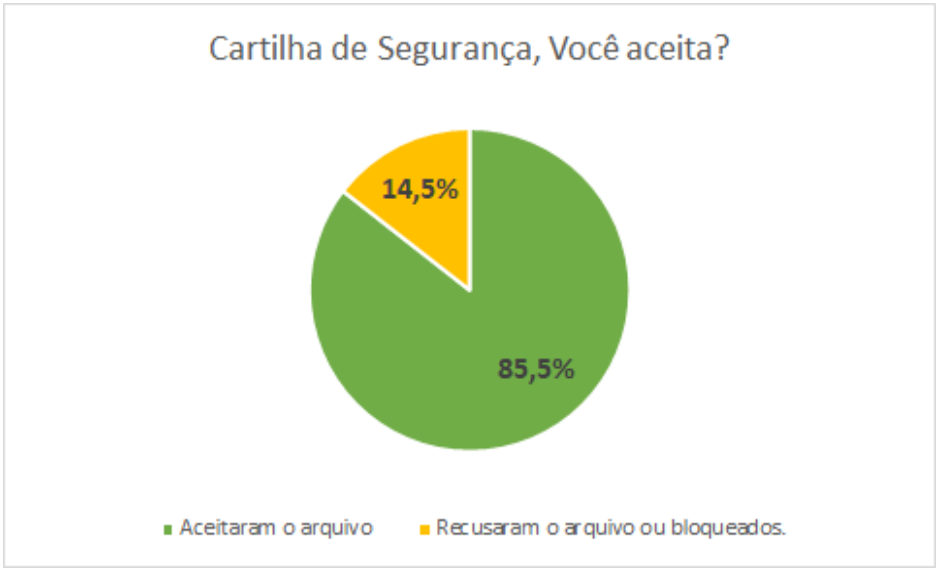
O posicionamento do usuário seria questionado por algumas vezes acerca das ações que estava a presenciar. A necessidade de controle da velocidade do envio de arquivo era um elemento fundamental para evitar que mesmo que tivesse conexão com velocidade superior a outros entrevistados o mesmo seria forçado a ter um limite para então gerar um campo de igualdade entres os entrevistados. Onde mais tarde todos viesse ter sido alvo de um procedimento para que ocorresse a captura da recusa do arquivo e assim fosse possível existir um tempo de reação por parte do entrevistado.

O acolhimento do arquivo com o nome “cartilha-seguranca.pdf”, só estava sendo coletado internamente, como mais uma resposta ao tópico apresentado no questionamento, sem que fosse necessário criar uma pergunta.

E para um movimento na contramão da pesquisa, mesmo ocorrendo de acordo com a figura 13, uma massiva parte dos usuários se apresenta com características que possuíam regras a serem empregadas ao receber arquivos.

Cerca de 85,5% dos usuários receberam o arquivo imposto refletindo algo contraditório com o resultado dos questionamentos acerca de recebimento de arquivos.

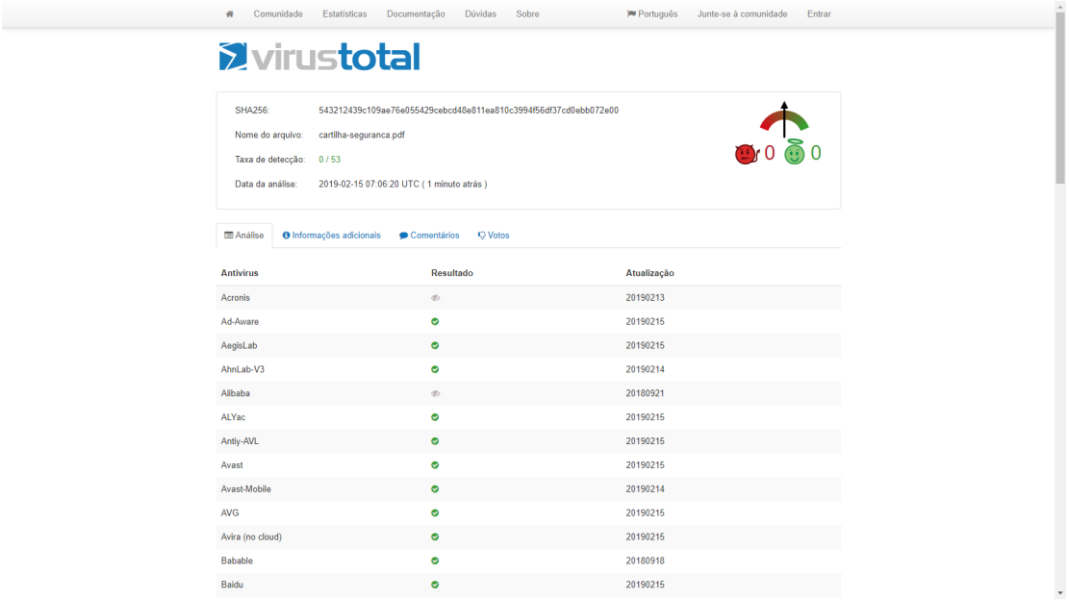
Figura 13 - Gráfico usuários que receberam o arquivo



Fonte: Própria

O arquivo em questão com formato conhecido, *portable document file* ou conhecido com a abreviatura de PDF, não possuía conteúdo algum internamente e foi criado apenas com conteúdo randômico de caracteres para apresentar tamanho de 20 megabytes.

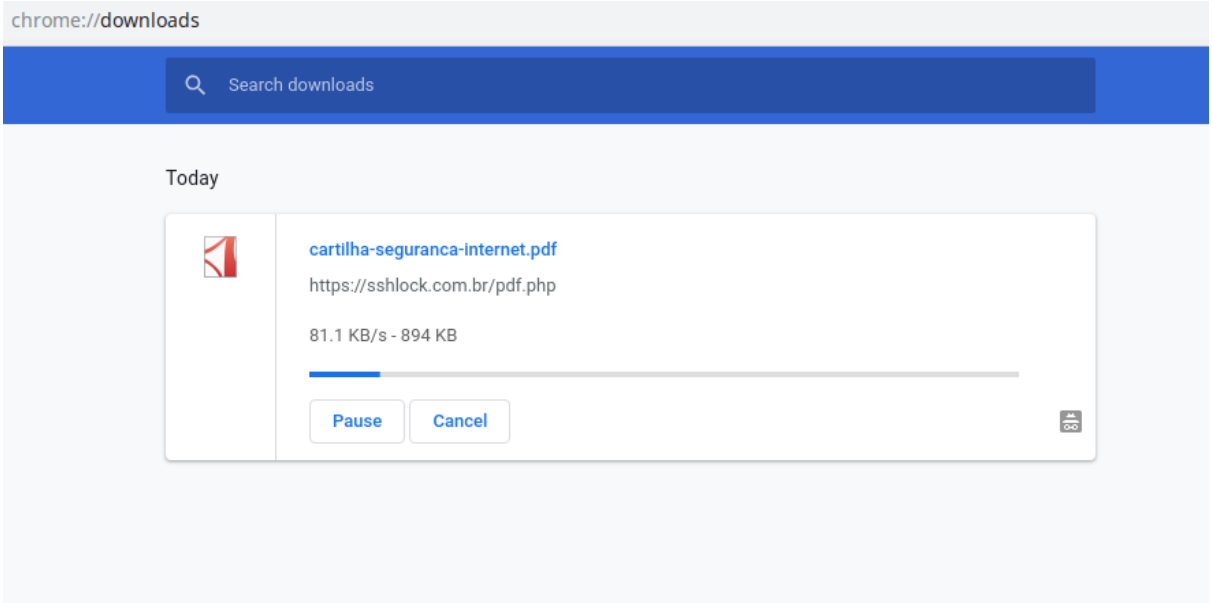
Figura 14 – Arquivo analisado para identificar nível de perigo para o usuário.



Fonte: Vírus Total analise.(VIRUSTOTAL, 2019)

O arquivo foi submetido para análise no VirusTotal [14]para identificar se existia algum perigo para o entrevistado como resposta da analise pode ser vista na figura 14 acima e o relatório da analise sendo disponibilizado no link https://www.virustotal.com/pt/file/543212439c109ae76e055429cebcd48e811ea810c3994f56df37cd0ebb072e00/analysis/1550214380/

Figura 15 - Como era apresentado na tela do entrevistado o download forçado



Fonte: Própria

Com auxílio da linguagem *javascript eram* apresentadas regras para o navegador limitar a velocidade do recebimento do arquivo, como pode ser visto na figura 15. O objetivo é verificar como seria a tomada de decisão do usuário quando estava recebendo o arquivo.

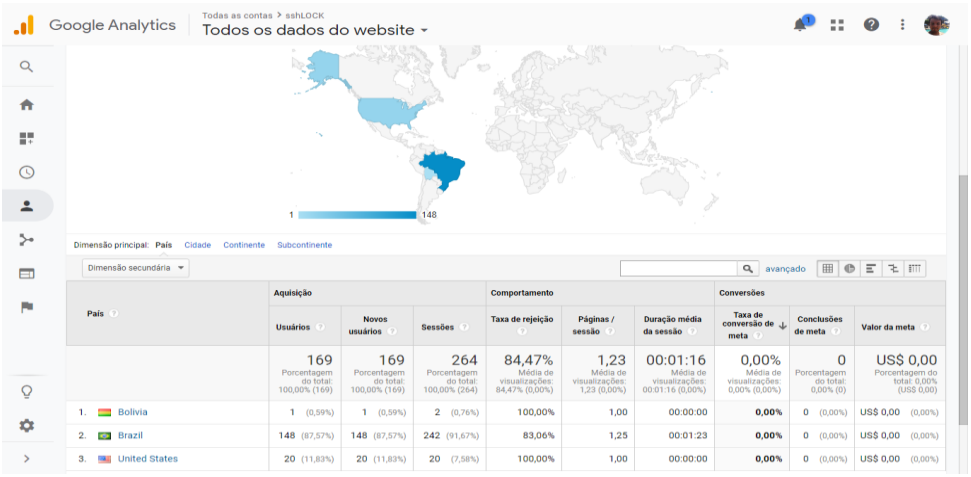
Os outros 14,5%, presente na representação da figura são usuários que possuem proteções ativas em seus navegadores que impossibilitam de participar da pesquisa, juntamente com entrevistados que recusaram o recebimento do arquivo, pois em algum momento, os serviços de bloqueio presente nos navegadores quando submetidos em um determinado momento a uma ação semelhante questiona o usuário se permitir para trazer comodidade o ato de desabilitar tal recurso, mas não o fazem.

[14] Empresa/aplicação que analisa arquivos e verifica dentre uma vasta lista de antivírus se o arquivo possui alguma anotação como sendo vírus sendo uma aplicação reconhecida mundialmente.

3.5. COLETA E ANALISE DE DADOS

A pesquisa foi realizada com o usuário de mecanismo do *Whatsapp*[15], o que gerou uma abrangência além do local da residência da pesquisa. O endereço https://sshlock.com.br, este domínio foi desativado após a pesquisa, site criado para o projeto, foi a peça chave que apresentava aos usuários o questionário e foi compartilhado para um grupo de pessoas que eram orientados a compartilhar para contatos, seguindo a orientação de que se tratava de um questionário, no qual a coleta de dados mesmo que conseguindo a informação demográfica, não cria condição ou característica internamente de identificar quem respondeu as informações de regiões.

Figura 16 - Relatório demográfico dos usuários da página/questionário.



Fonte: Própria

Tal procedimento foi disponibilizado com o propósito de apresentar que as informações colhidas partiam de outros lugares, além do domicílio da pesquisa e a amostra do questionário foi composta por 21 questões e 107 pessoas responderam, a localização dessas pessoas se subdividiram em 3 países: Brasil, Estados Unidos e Bolívia, e ao todo distribuídos em 32 cidades apresentado na (Figura 16).

A coleta de dados foi orientada em 4 sessões, a primeira sessão contendo 3 perguntas para identificar o perfil do pesquisado. A segunda sessão com 3 perguntas para compreender a proximidade com uso da internet e aplicações sociais, bem como

[15] Whatsapp aplicação de mensagem instantânea

o tempo gasto e se caso a pessoa respondesse que não utilizava, era finalizado o questionário. A terceira sessão com 7 perguntas envolvendo múltipla escolha e seleção múltipla, visando identificar o comportamento do internauta frente a algumas situações que fazem parte do cotidiano de quem utiliza a internet. E a quarta sessão com 8 perguntas de escala linear com regras, que se o valor 1, fosse escolhido, a pessoa discordava completamente da frase apresentada e 5 correspondendo ao concordo completamente.

Nas seções de 3.5 a 3.6 são apresentados em gráficos os resultados da entrevista correspondentes às questões da pesquisa apresentadas no Apêndice A.

3.5 CONHECIMENTO DO PÚBLICO ALVO

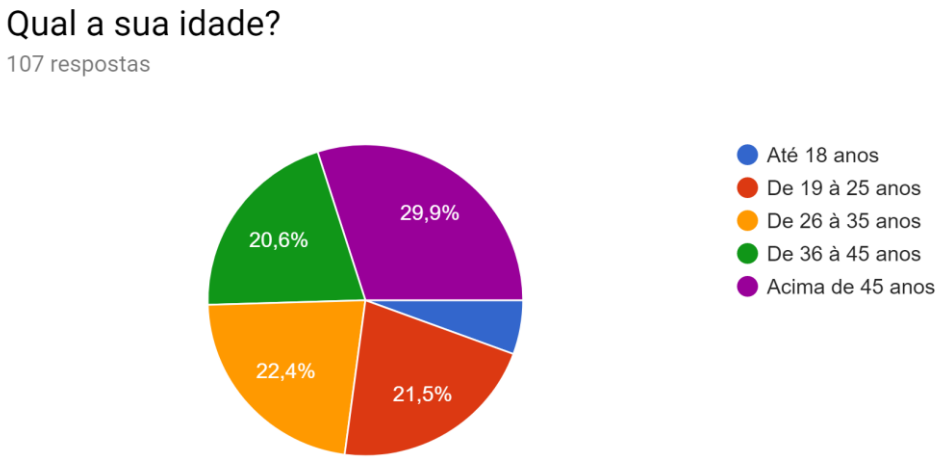
Na primeira seção de perguntas da pesquisa foi disponibilizada três perguntas para identificação dos alunos, foi questionado sexo, idade e escolaridade atual. Com base nos pós aquisição obteve-se as seguintes respostas:

Figura 17 - Gráfico da coleta acerca da identidade de gênero

Fonte: Própria.

Com base na figura 17 foi identificado que o público que possui maior representatividade nesta pesquisa foi de usuários do sexo masculino, sendo observado que em relação ao tema de segurança de informação o público masculino mostrou ser o mais interessado neste tema. A visão a ser passada inicialmente, era apenas de apresentar o arranjo de existência da presença de homens e mulheres.

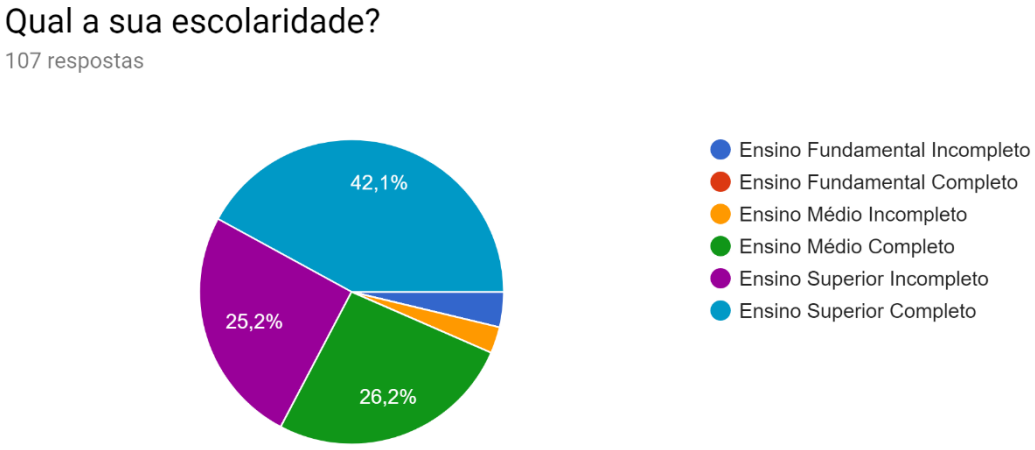
Figura 18 - Gráfico representando a idade dos entrevistados



Fonte: Própria

De acordo com a figura 18, percebe-se que a questão conseguiu gerar um grupo que alcançasse todas os 5 grandes grupos etários, apresentando uma grande presença de pessoas da faixa etária acima de 45 anos, com exatos 29,9% que se veem estimulados frente a plataformas sociais. Os adultos mais jovens, os quais tem como características estarem mais intimamente ligados a tecnologia aparecem na segunda posição, de 19 a 25 anos com 21,5%, seguidos pelas pessoas de 26 a 35 anos com 22,4% e das pessoas de 36 a 45 anos com 20,6%. Em termos gerais, observa-se que a quantidade de pessoas com mais de 26 anos que se interessam por segurança da informação é bem significativa.

Figura 19 - Gráfico apresentando a escolaridade dos entrevistados



Fonte: Própria

Na figura 19, observa-se que o grau de interesse com o tema proposto é de 42,1% de usuários com ensino superior completo, seguido pelo ensino médio completo 26,2% e superior incompleto com 25,2%.

Conclui-se que a maioria que se identifica com questões acerca de segurança compreende os usuários com grau de instrução igual e acima do ensino médio completo.

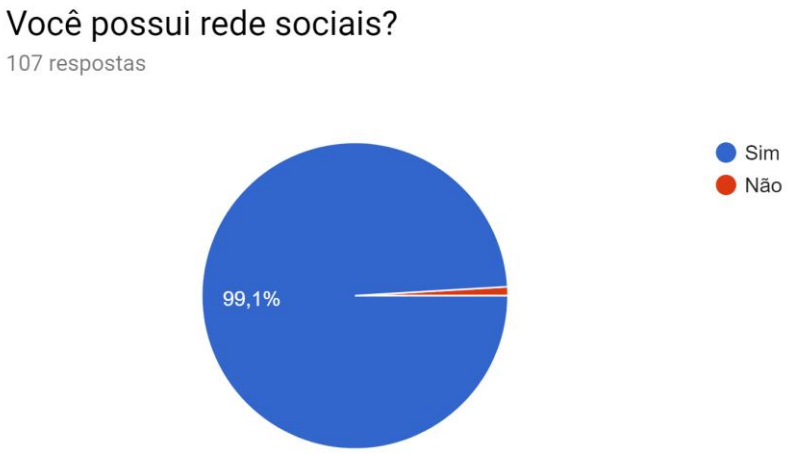
3.6 DESCRIÇÃO E ANÁLISE DE DADOS COLETADOS

No questionamento da pesquisa quanto ao comportamento dos usuários dentro das plataformas sociais e a abordagem de questões sobre segurança da informação para compreender algumas etapas que auxilia na definição de suscetibilidade para traçar um perfil vulnerável.

Obteve-se os seguintes resultados:

Figura 20 - Gráfico representando quantidade de entrevistados

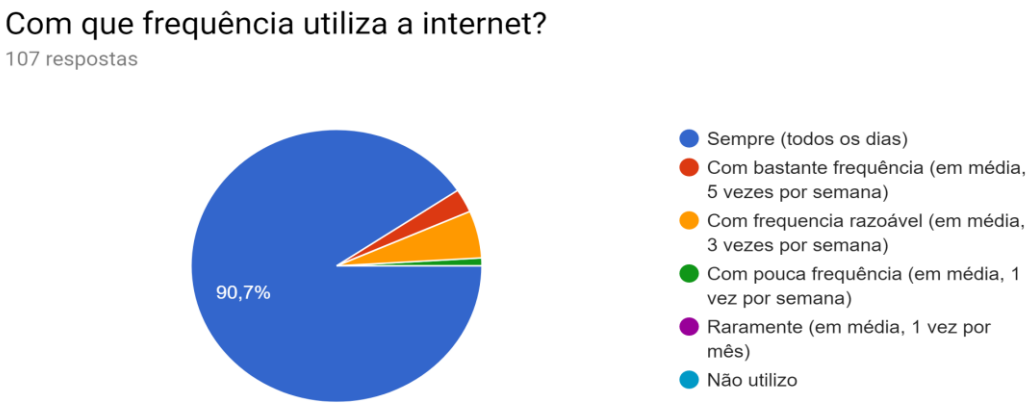
que possui rede sociais



Fonte: Própria

Na figura 20 é possível identificar que o público que utiliza redes sociais dentro de um universo de mais de 100 entrevistados, cerca de 99,1% possui redes sociais. Neste caso, pode-se relatar que a busca por compreender o cotidiano do usuário, coletou um grupo bastante específico de usuários de redes sociais, nesse sentido, o contexto de engenharia social pode ser aplicado, por efetivamente os entrevistados estarem presente neste meio.

Figura 21 - Gráfico apresentando frequência dos usuários na internet de acordo com a entrevista



Fonte: Própria

Na figura 21 foi possível identificar que cerca de 90,7% dos usuários se mantém conectados todos os dias, neste caso a quantidade de informações que o

usuário consome e ao mesmo tempo disponibiliza é bastante alto. Tornando a sua conectividade como elemento importante do seu dia a dia, da mesma forma, como qualquer atividade corriqueira que possa ser estimulada

Muitas vezes, as informações disponibilizadas oferecem características de posicionamento global, situação emocional, conquistas particulares e algumas vezes ocorrem descrições em tempo real de tomada de decisões. Informações sensíveis que são disponibilizadas sem um devido controle, proporciona nestes casos, uma falsa sensação de liberdade e segurança, pois o usuário tem o pensamento que está compartilhando apenas com pessoas íntimas.

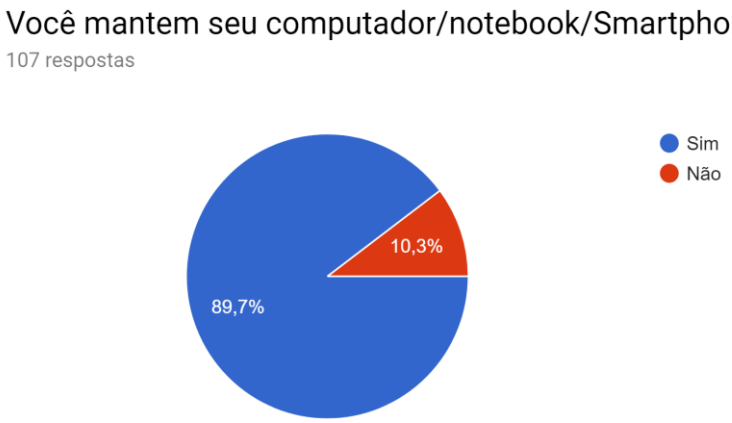
Figura 22 - Gráfico apresentando tempo que os entrevistados permanecem conectado à internet

Fonte: Própria

Seguindo com relação a frequência do uso da internet, como visto na figura 22 foi questionado em média quanto tempo por dia a pessoa permanece conectado e para surpresa 48,6% relatou que mais de 5 horas e o tempo que se passa seguido de um grupo de 1 a 3 horas que é considerado normal em relação a outros usuários que passam acima de 3 horas.

O tempo gasto de forma exacerbada revela que muitas vezes, o uso de aplicações sociais estimula o que era reflexo de comportamento e ações humanas agora possuindo um novo campo para ser expressado.

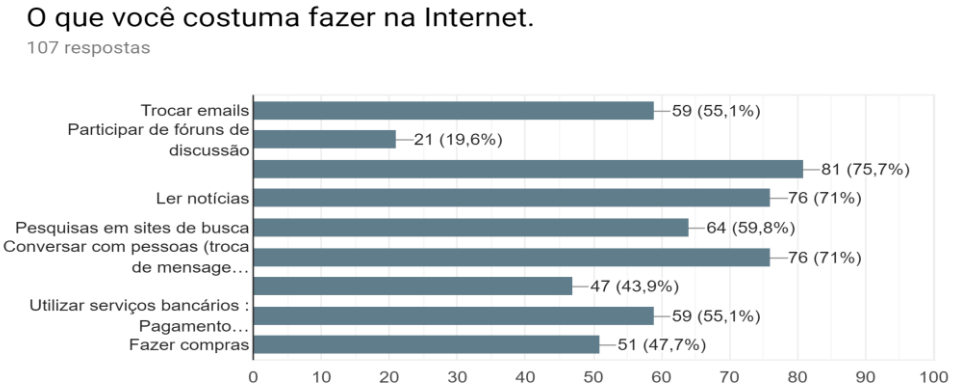
Figura 23 - Gráfico que apresenta quem mantem equipamentos utilizado entre os entrevistados



Fonte: Própria.

Na figura 23 é apresentado o resultado do questionamento sobre as ferramentas que os usuários utilizam para se conectar à internet, se são atualizadas com frequência. Os resultados obtidos foi que 89,7% mantinham seus equipamentos atualizados, muitas vezes forçados pelos próprios aplicativos ou incentivados por terceiros, em contraponto 10,3% não atualizavam com frequência seus equipamentos, por simplesmente desconhecer a abordagem e o meio para se fazer o procedimento.

Figura 24 - Gráfico que representa a distribuição dos entrevistados em relação ao que costuma fazer na internet.



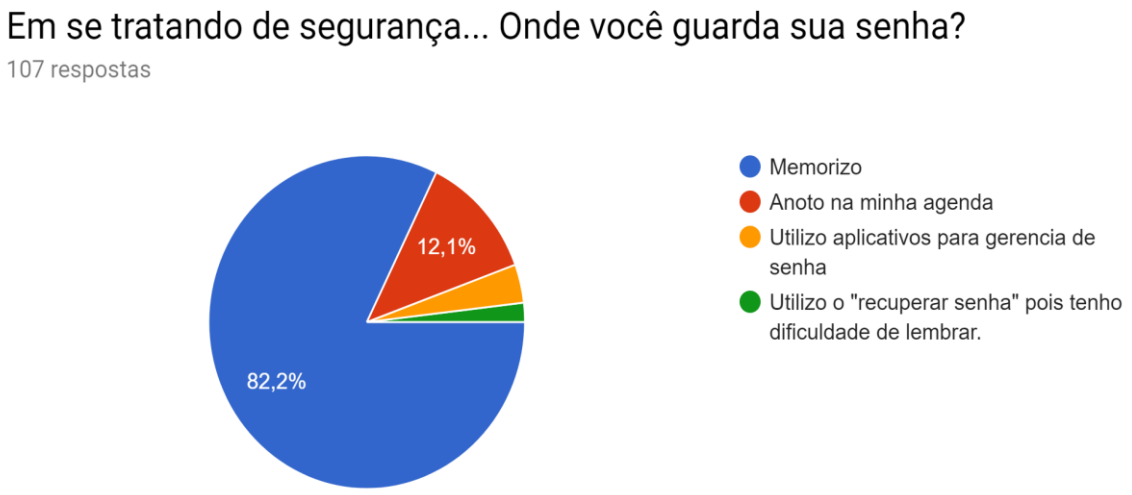
Fonte: Própria

O cotidiano dos entrevistados foi questionado e apresentado na figura 24, a pesquisa se voltou a misturar tópicos de forma aleatórios e outros temas com

prioridade na pesquisa para identificar dentro do grupo de entrevistados a porcentagem dos mesmos que utilizam os tópicos com informação sensível. Cerca de 59 dos entrevistados responderam que utilizam para serviços bancários e trocar e-mail pela internet e cerca de 51 disseram que utilizam para “Fazer Compras”. Estes tópicos destacados são os considerados relevantes para pesquisa, pois fazem parte do acesso a níveis de privilégios que possibilitem perdas substanciais e até financeiramente.

O que demonstra que existe uma parte significativa dos participantes da pesquisa que utilizam serviços financeiros, portanto existe a presença de informações sensíveis que merecem atenção a questões de segurança que podem levar a sequestros de dispositivos eletrônicos dos usuários para aproveitar-se destas informações.

Figura 25 - Gráfico que representa a distribuição dos entrevistados em relação aonde guarda senha



Fonte: Própria

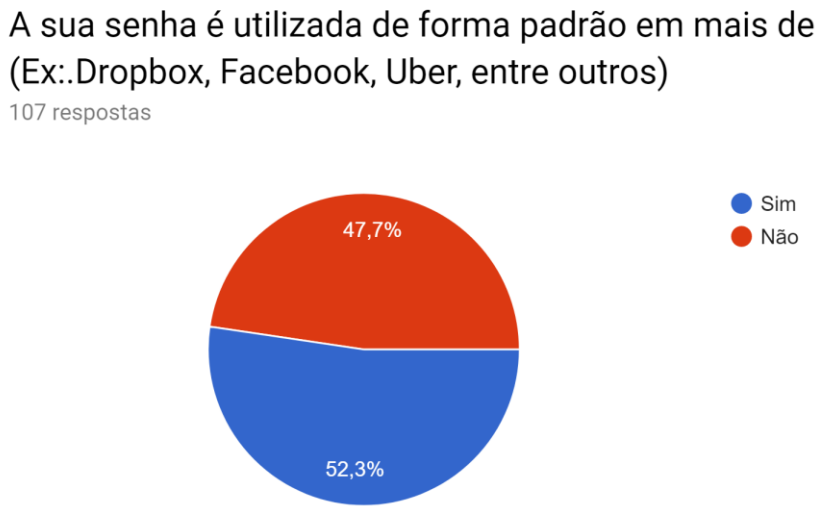
Na figura 25 foi questionado qual o procedimento que o usuário tem em relação a armazenamento da senha, associado a qualquer tipo de serviço, verificou-se que a maioria faz a opção por memorizar a senha, como principal forma de ter sempre em mãos a sua chave de acesso, 82,2 % dos entrevistados e 12,1% adota a forma manual de guardar a senha através de agenda físicas.

Existe um número pequeno de usuários que utilizam programas de terceiros para armazenar e um pequeno grupo que utiliza o serviço de “recuperar senha” para

sempre está renovando a cada acesso, o que pode não ser algo positivo, tendo em vista que a senha está sendo disponibilizada para um gestor, este fato faz com que se tenha garantias que este gestor esteja protegido de ações que venham expor as senhas.

A validação da segurança através do serviço de recuperar senha em algumas aplicações utiliza a técnica de autenticação de 2 fatores ou duas etapas que é o uso de outros locais ou equipamentos para gerar *tokens* ou mesmo um serviço de segunda senha para acessar. Em certos momentos o *login* concedido através dessa técnica, gera uma carga a mais de privacidade, o que torna necessário que o usuário possua um equipamento próximo, por exemplo ‘o celular’, para que ocorra o envio de código para autenticação por serviço de mensagem de texto.

Figura 26 - Gráfico que representa a distribuição dos entrevistados em relação ao uso da mesma senha para mais de um serviço



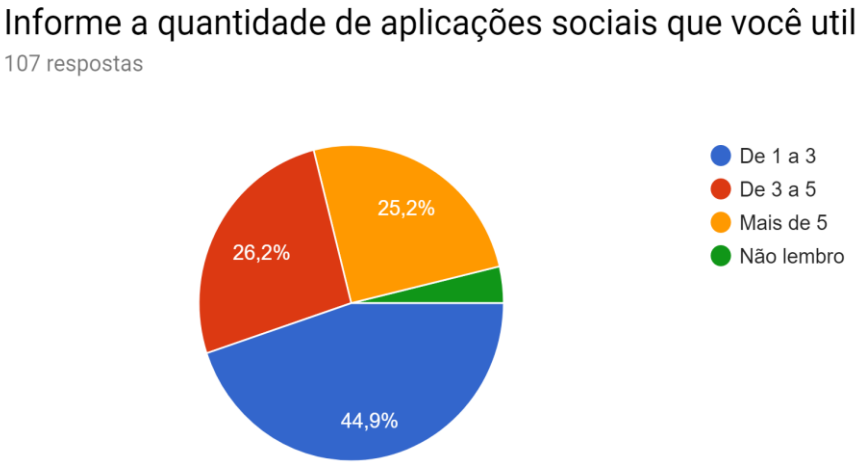
Fonte: Própria

A senha é uma peça chave para ter acesso a aplicações sociais e ter uma chave que abre todas as portas, não é uma estratégia correta quando se deseja a valorização da privacidade. Quando foi questionado se a senha era utilizada de forma padrão em mais de um serviço, os resultados obtidos foram os expostos na figura 26, nos quais cerca de 52,3% dos 107 entrevistados relataram que utilizam a senha de forma padrão em mais de uma aplicação. O que pode ser um grande problema, caso esta senha seja descoberta.

Este tipo de problema é algo mais comum do que se imagina pois quando

ocorre um vazamento a primeira atitude por parte do usuário mal-intencionado é acabar testando esta senha em outras aplicações. Além do que, tal descoberta de senha acaba por figurar em fóruns e grupos, que compartilham esses dados extraídos de forma ilegal em ambientes que geralmente compreendem espaços de difícil rastreio como ***deepweb*** ou ***darknet***[16]. Desta forma, deve-se ter bastante cuidado ao se utilizar senha única para mais de um serviço.

Figura 27 - Representa a quantidade de redes sociais que os usuários utilizam



Fonte: Própria.

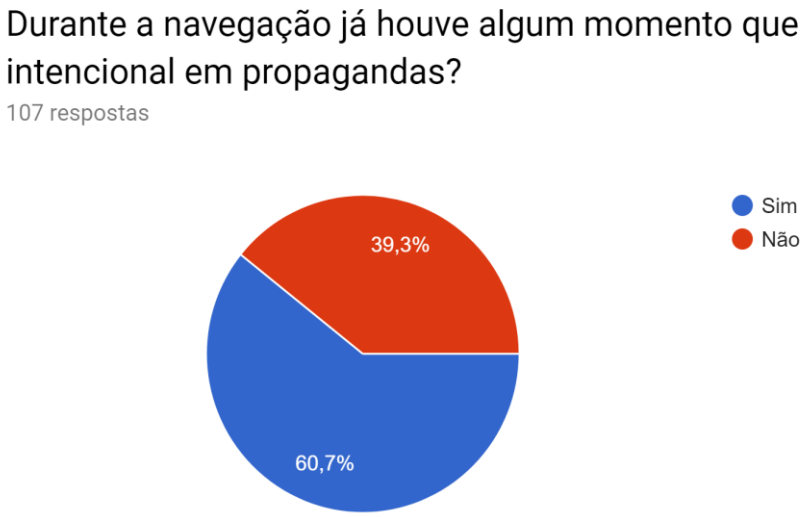
Ao intensificar sobre a questão do posicionamento de segurança e ciente que existe um grande número de pessoas que utilizam a mesma senha em várias aplicações foi questionado a quantidade de aplicações sociais que o pesquisado costuma utilizar e o resultado foi um número bastante expressivo, de acordo com a figura 27, compreendido de 1 a 5 aplicações.

Se levar em consideração o questionamento sobre utilizar a mesma senha para mais de um serviço e a quantidade de aplicações utilizadas pelo usuário, caso haja a descoberta desta senha, o acesso a várias informações confidenciais do usuário, poderão ser disponibilizadas.

Figura 28 - Gráfico identificando se o usuário de forma intencional já clicou em

[16] Termos utilizado para identificar uma parte da internet que possui serviço de criptografia e redirecionamento de navegação para manter anonimidade dos usuários e dos serviços acessados não sendo rastreados pelos serviços de buscas como Google por exemplo.

propagandas durante sua navegação.



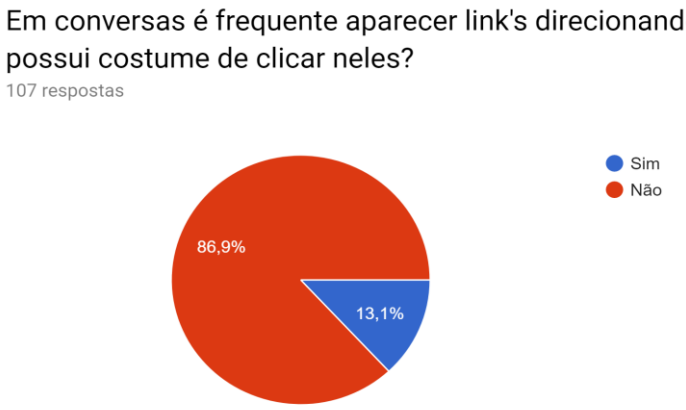
Fonte: Própria

De acordo com a figura 28, cerca de 60,7% relataram que durante navegação clicaram de forma intencional em propagandas que em algum momento tiveram interesse. Casos dos quais se enquadram, uma oferta tentadora de passagens áreas ou pacotes promocionais, decorrendo em grande perigo, uma vez que o usuário pode estar sendo direcionado para uma armadilha gerada por pessoas mal-intencionadas.

Um dos cenários existentes utilizados para promover ações de ataques direcionados personalizados é o *spear phishing* e a personalização de iscas, que podem se apresentar como propagandas em páginas, não seguras, para atrair os usuários com apresentação de elementos que pertencem ao cotidiano dos mesmos.

Figura 29 - Gráfico do posicionamento do usuário

Diante de um link de fonte desconhecida.



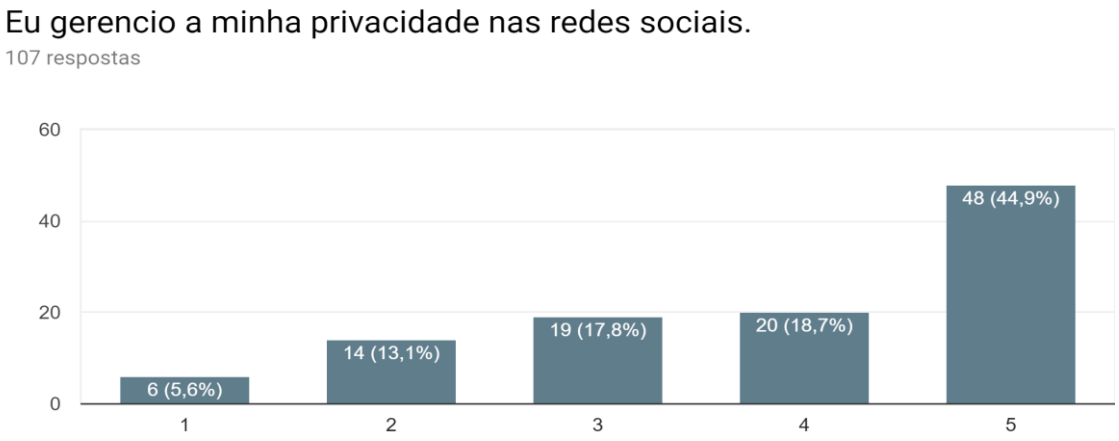
Fonte: Própria

Outra forma de apresentar situações que podem levar o usuário a ser direcionado para ambientes desprotegidos e o compartilhamento de endereços infectados foi apresentado e quando perguntados, cerca de 86,9% dos entrevistados relataram que não possuem o costume de clicar em links que são apresentados durante troca de conversas, como pode ser visto na figura 29, o que demonstra que os usuários possuem cuidado para não serem direcionados a links, mesmo estando em conversas com pessoas consideradas confiáveis.

Toda e qualquer plataforma social possui configurações que possibilita ao usuário dar a visibilidade que deseja. A personalização vai desde a apresentação de dados pessoais, como níveis de acesso a algumas informações, podendo selecionar quais tipos de dados são compartilhados entre os usuários da sua rede, o que auxilia na manutenção da privacidade dos clientes.

Disponibilizando uma regra linear onde de 1 a 5, onde 1 discorda completamente e 5 concorda com a afirmação, no que se refere ao nível de proximidade com o tema gerenciamento de privacidade em plataformas sociais gerou os seguintes resultados com base na figura 30 para a afirmação “Eu gerencio minha privacidade nas redes sociais”, cerca de 44,9% concorda com esta afirmativa.

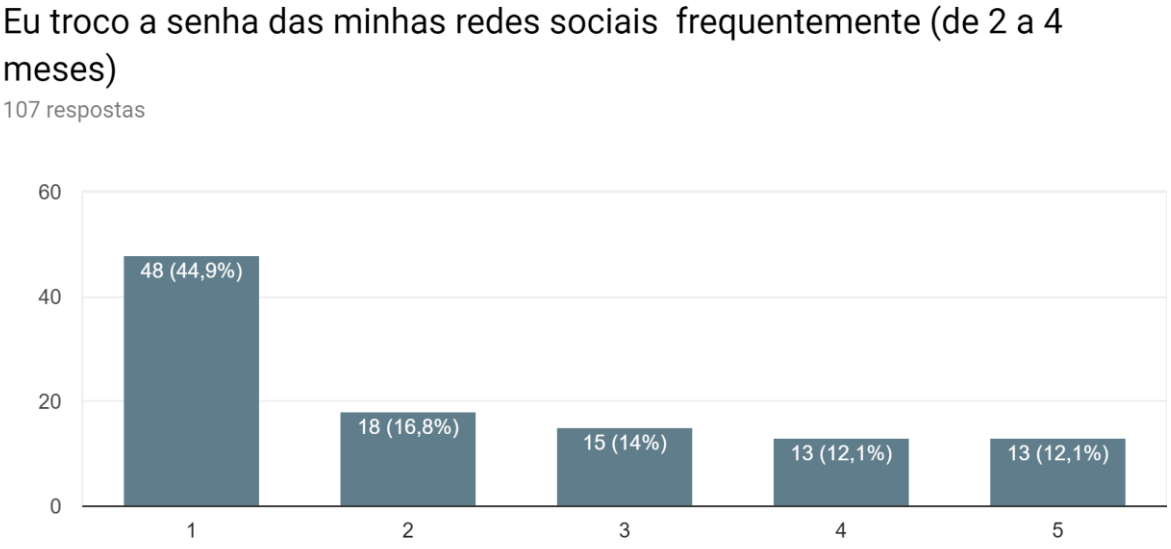
Figura 30 – Gráfico sobre privacidade em redes sociais



Fonte: Própria

Com este nível de aceitação, o tema é relevante entre os entrevistados e a proposta de gerenciamento de privacidade em redes sociais é algo corriqueiro. A presença de empresas que disponibilizem produtos que ofertem um maior acesso a personalização do nível de acesso, acaba por conquistar grupos como estes submetidos a estes questionamentos.

Figura 31 – Gráfico com a frequência da troca de senhas em redes sociais.



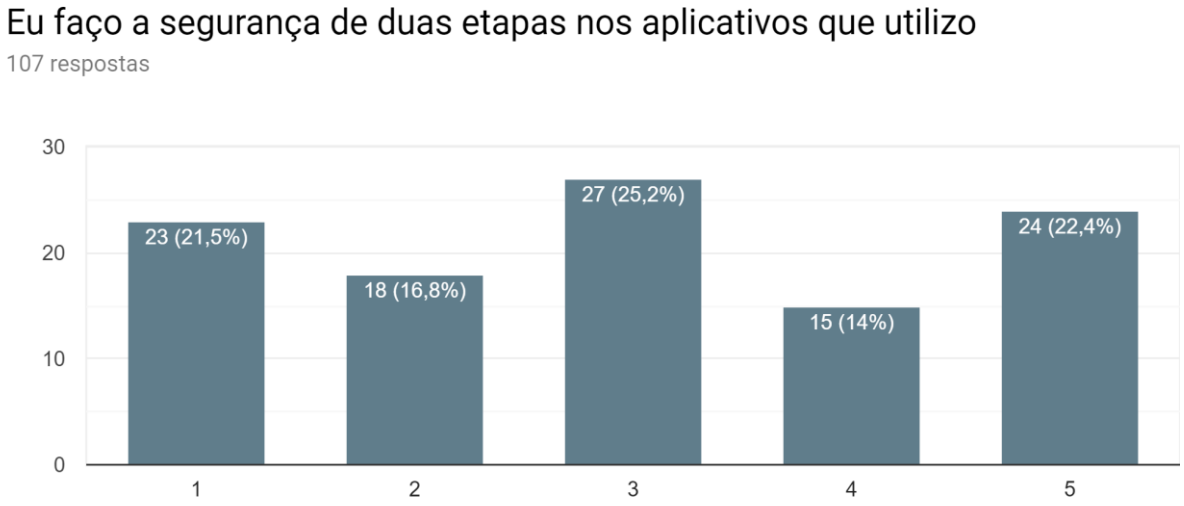
Fonte: Própria

Em relação a questão de senhas foi ainda questionado, se os usuários

possuíam costume de trocar as suas palavras de passe com certa frequência. De acordo com o resultado do questionamento, cerca de 44,9%, conforme figura 31 relatou que não efetuam tal operação, o que demonstra que não existe uma manutenção frequente em relação a senha.

A escolha em discordar do tempo de validade da senha, termina por causar um efeito cascata, uma vez que em questionamentos anteriores sobre se a senha estava presente em mais de uma plataforma e o fato de a troca da senha não ser frequente, pode acarretar no caso de uma quebra do sigilo desta, um grande transtorno para o seu usuário, já que este pode ter vários dados importantes expostos.

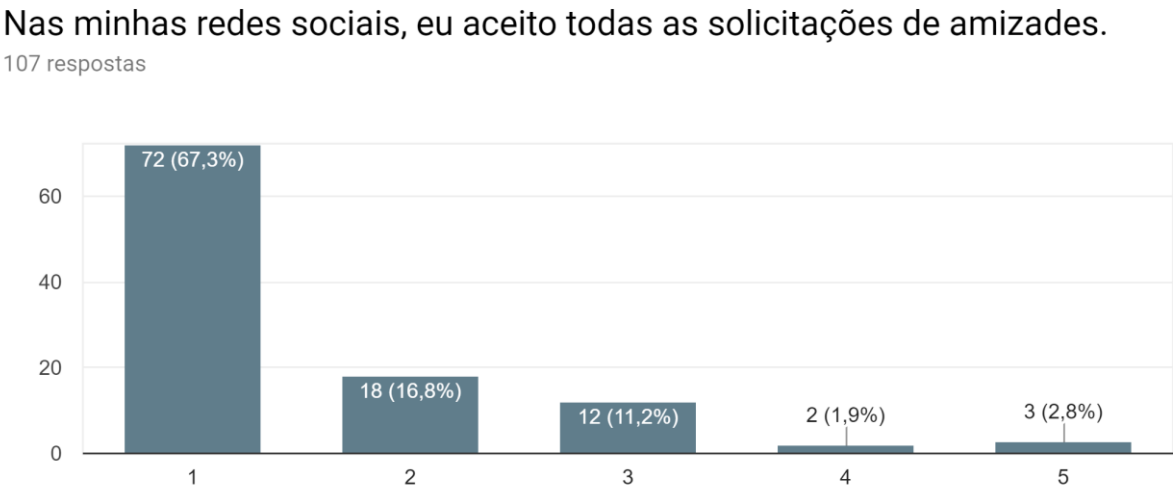
Figura 32 - Sobre a segurança em duas etapas.



Fonte: Própria

Foi apresentado, de acordo com a figura 32, a seguinte afirmação “Eu faço a segurança de duas etapas nos aplicativos que utilizo” e dentre as outras afirmações essa se apresentou com respostas bastantes distribuídas entre as opções de 1 a 5, que correspondem a “discordo plenamente” e a “concordo plenamente”, respectivamente. O resultado remete a compreender que o usuário ainda possui dúvidas em relação ao serviço de autenticação de duas etapas nos aplicativos. Tendo em vista que as “duas etapas” ou “autenticação de dois fatores” podem existir, mas necessita que as plataformas possuam uma melhor abordagem com usuários para relatar a devida necessidade de ativar tal serviço que implementa uma camada de segurança maior para o usuário.

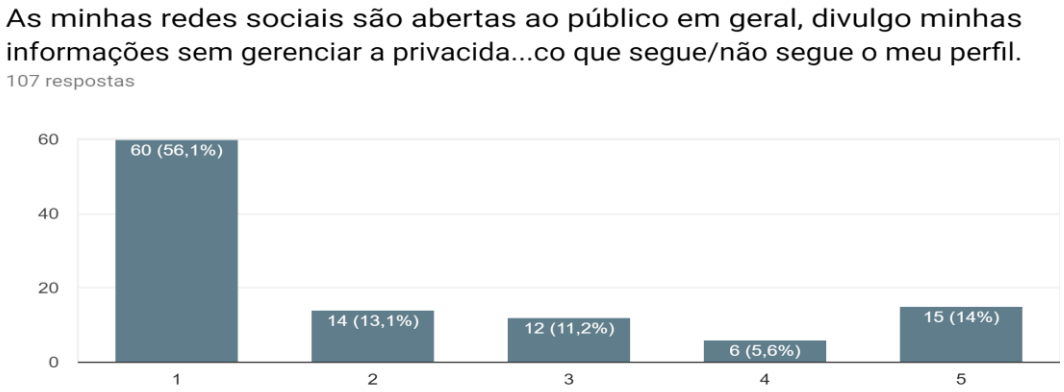
Figura 33 - Gráfico apresentando sobre o aceite de solicitação de amizade



Fonte: Própria

De acordo com a figura 33, cerca de 67,3% dos entrevistados relataram que não aceitam toda e qualquer solicitação de amizade. O que auxilia em atrasar a forma de interação de pessoas de má índole com propostas de rastrear, se utilizando de engenharia social, informações do usuário.

Figura 34 - Gráfico apresentando sobre privacidade das plataformas sociais

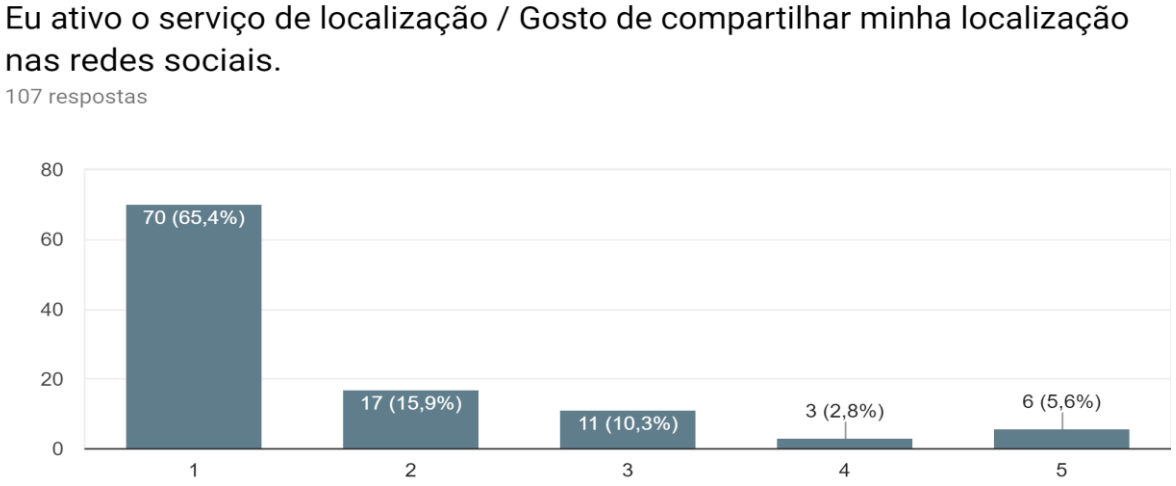


Fonte: Própria.

A figura 34 remete o seu contexto, a uma afirmação anterior sobre gerenciamento de privacidade, pois de acordo com o gráfico apresentado nesta figura, a afirmação sobre disponibilizar as informações de forma pública é negada (discordam) por cerca 56,1% dos participantes da pesquisa.

Uma vez que houve um grande número de entrevistados relatando que gerencia sua privacidade, cerca de 44,9%. A presença de indicativos que as informações dos usuários de plataforma sociais poderiam se encaminhar também na gestão da inserção de conteúdos nas redes sociais é salutar.

Figura 35 - Sobre geolocalização em plataformas sociais.



Fonte: Própria

A afirmação abordada na figura 35 teve como indicativo a utilização de serviços de geolocalização, uma vez que o usuário disponibilize este tipo de elemento, ele é armazenado na base de dados das aplicações e existe a possibilidade de apresentar históricos.

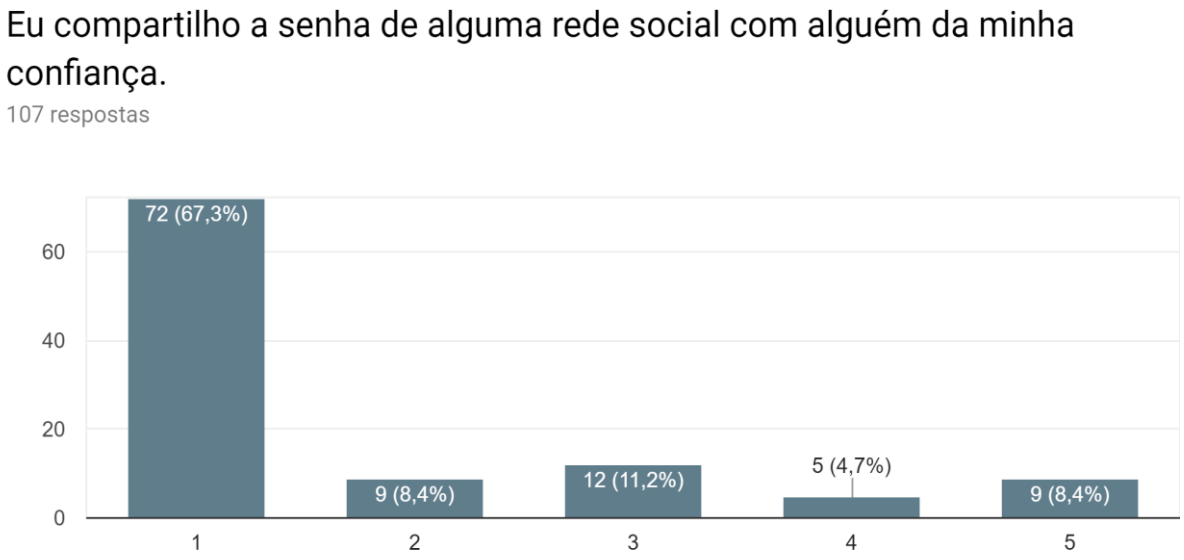
Em se tratando de segurança da informação, uma vez que o usuário mal-intencionado consegue obter chave de acesso às plataformas e identifica históricos de localização, consegue um grau maior de informação para traçar o perfil do usuário com base nas preferências ou mesmo na identificação do momento em que o usuário está ativo com seus equipamentos.

O usuário também pode ser alvo de *phishing* direcionado e personalizado com a presença de elementos de geolocalização que deixam mais próximos locais reais que o usuário já tenha visitado. O resultado é o usuário ser alvo de *spear phishing*, ou de ataques do formato *MITM*, *man in the middle*, que utiliza técnicas de escuta para intermediar transações e filtrar dados sensíveis ao estar em contato com essas redes

personalizadas para aquisição de mais dados sensíveis.

Cerca de 65,4% das pessoas durante a pesquisa relataram discordar da afirmação, o que diminui a possibilidade de acontecer ações com formatos mais abrangentes e sofisticadas, mas não impossibilita que a somatória dos índices 3, 4 e 5 não venham ser vítimas dessas ações.

Figura 36 - Gráfico representando entrevistados que compartilham senha.

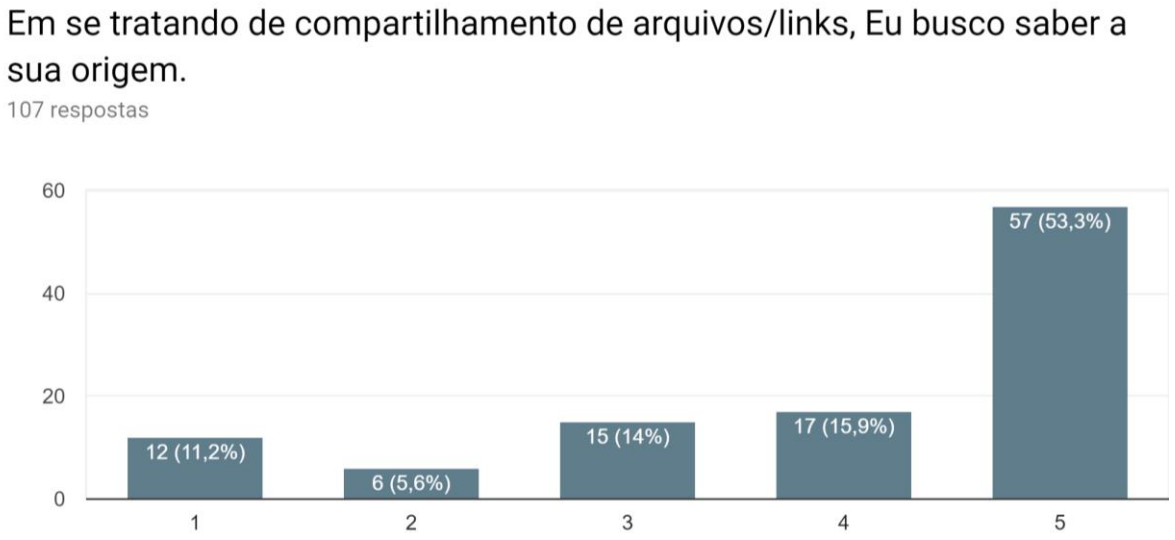


Fonte: Própria

A senha é a forma como o usuário se autentica entre as plataformas de redes sociais, compartilhá-la é algo que deve ser desestimulado de acordo com o grupo de entrevistados.

De acordo com a figura 36, mesmo que ocorra um número grande de pessoas (67,3%) que discordam da afirmação que compartilha a senha da rede social com outra pessoa da sua confiança, ainda assim, existe uma distribuição dos entrevistados que concorda com a ideia de compartilhamento de senha, tal atitude é complexa, dado que a pessoa de confiança pode não possuir as mesmas preocupações com segurança que a detentora da senha. O que pode gerar perspectivas futuras de quebra de sigilo da senha.

Figura 37 - Sobre a ciência da origem dos links.



Fonte: Própria

Com a proposta de identificar, se dentro de um ambiente controlado, uma plataforma social ou mesmo um mensageiro instantâneo, quando é apresentado a compartilhamento de arquivos ou link, se o usuário busca saber a origem da geração da ação. De acordo com a figura 37, um grande número relatou que busca saber a origem para identificar, se é algo seguro ou se trata de um potencial perigo para quem é destinado.

Cerca de 53,3% relataram que concordam com a prática de identificar a origem, mas existe um número razoável de entrevistados que não se importam muito com isto, a faixa de 1 a 2, representando cerca de 16,8% dos entrevistados.

Ao ser feita uma análise mais rigorosa, pode-se enfatizar que existem muitos entrevistados suscetíveis ao *Ransomware*, pois não possuem a preocupação de verificar a origem do compartilhamento recebido, considerando a faixa de 1 a 4, apresentada na figura, tem-se 46,7% dos entrevistados.

3.7 RESULTADO DA PESQUISA

Esta seção descreve os resultados obtidos, através da análise final dos questionários relacionada com o resultado do ambiente de teste. E traz algumas medidas preventivas para minimizar a ação de sequestro eletrônico por vias da engenharia social.

3.7.1 ANÁLISE

A realização da pesquisa quantitativa se deu pela utilização do mecanismo de coleta de dados online utilizando a plataforma *Google Forms.* Tal mecanismo foi apresentado para um grupo pequeno de usuários de mensageiro instantâneo *WhatsApp*, e de plataformas sociais. Estes usuários foram colocados em condições de voluntários para efetivar o procedimento de compartilhamento da pesquisa, o que possibilitou um maior alcance do número de entrevistados presentes em diversas localidades geográficas.

O procedimento de compartilhamento do *link* da pesquisa para pessoas próximas possibilitou que a técnica de engenharia social fosse aplicada, tendo em vista que, a interação final que gerava a participação na entrevista foi possível ocorrer com base no elemento de confiança gerado a partir dos voluntários.

Em um ataque especializado a confiança e a base para orquestrar o direcionamento de propostas sendo observado e levado em consideração os perfis de usuários gerado através da análise do perfil do alvo. Tudo com intuito de permitir a falsa sensação de segurança dentro de um padrão aceitável do usuário alvo do ataque.

Dentro de uma busca de possíveis alvos, os usuários mal-intencionados se utilizam da possibilidade de conquistar a confiança e a partir disto acionar mecanismos

que possibilitem mais informações sigilosas. A engenharia social, neste caso foi utilizada para tornar possível a geração do primeiro contato com o entrevistado.

A quantidade de entrevistados durante a pesquisa foi vista como um número satisfatório para extração de dados. Obedecido o critério da coleta ser anônima para evitar o comprometimento da pesquisa, de acordo com que foi acertado com os entrevistados.

Em relação ao alcance da pesquisa em questões demográficas, ela percorreu por diversas localizações, assumindo um conglomerado de 3 países, sendo dois da América do Sul e um da América do Norte. A comprovação deste fato pode ser feita através dos rastros coletados pelo *Google Analytics*. Estes dados não possuem fins de associar ou identificar os entrevistados e sim o de verificar o alcance da pesquisa.

A pesquisa quantitativa foi construída em cima de 21 questionamentos sendo eles de múltiplas escolhas e outros de escolha linear onde 1 era discordo completamente e 5 concordo completamente. Todos os questionamentos orientados por questões, afim de obter informações possíveis para construção de uma persona.

Os questionamentos abordados na pesquisa possibilitaram rastrear o máximo de entrevistados com proximidade ao público que utiliza internet focado em plataformas sociais. Em um determinado momento da pesquisa quando ocorreu o questionamento acerca de quantas horas o entrevistado passava conectado à internet e acerca se o usuário possui ou não redes sociais, presentes no apêndice A, foi criado uma rota de saída para que esses entrevistados que não tivessem proximidade com internet, não viessem gerar informações aleatórias que alterassem de forma significativa a qualidade dos dados gerados uma vez que o foco era alimentar a base com um grupo que tivesse afinidade com a internet.

A presença de técnicas de engenharia social na abordagem dos entrevistados gerou um acesso de confiança entre a pesquisa e o entrevistado, o que possibilitou a presença dos entrevistados em todos os levantamentos, mesmo que não fosse colocado restrição de obrigatoriedade de respostas, a pesquisa acerca de questionamento sobre segurança em sua plenitude foi respondida por todos eles.

Para que houvesse a extração do público alvo foram necessários questionamentos sobre o uso da internet para eventos pessoais, como por exemplo o uso de plataformas sociais, tendo em vista que a presente pesquisa vem com a proposta de enxergar uma lacuna sobre segurança da informação aplicada a este

núcleo.

A proposta da pesquisa era questionar se a ingerência da informação era passível de rastrear o perfil do usuário, a fim de colocá-lo em uma situação que poderia ter seus dados ou dispositivos capturados. A questão de confiança era a peça chave das informações, uma vez que se o questionário fosse enviado por pessoas muito próximas facilitaria a montagem do ambiente de teste da pesquisa.

O ambiente de teste, o próprio questionário, executou instruções para que ocorresse a sugestão de arquivo para quem estava sendo entrevistado. Essa sugestão era aplicada com intuito de confirmar se o usuário estava confiante no ambiente em que estava ao passo de ser posto em questionamentos sem perguntas com a sua resposta sendo a aceitação ou não do arquivo sugerido. Com base na recusa do arquivo foi guardada a quantidade de usuários que recusaram e o número utilizado para extrair da quantidade que responderam o questionário.

A base de resposta do questionário mostrou que a maioria do público se apresenta com informações o suficiente acerca de questões de segurança de informação e como se portar na web, entretanto, mostraram-se bastante contraditórios quando foi analisado a quantidade de usuários, pelo lado do ambiente de teste, que aceitaram o recebimento do arquivo.

Levando-nos a concluir que a proposta dessa pesquisa foi validada, tendo em vista que uma simples carga de confiança para chegar até o usuário, mais a aplicação de técnicas de engenharia social possibilita que sejam utilizadas técnicas de obtenção de informação, tornando possível criar a ação de captura com o uso de envio sem solicitação de arquivos para o usuário. Estes arquivos podem se apresentar como itens camuflados com instruções que podem elevar privilégios para terceiros, que podem remotamente sequestrar o conteúdo do dispositivo do usuário.

A aceitação desses arquivos configurava que o entrevistado em questão estava infectado, no caso do arquivo da pesquisa ofertado ao entrevistado, este não possuía quaisquer ações, instruções ou informações que viesse a comprometer os dispositivos deles.

Seguindo o contexto apresentado no referencial teórico a camuflagem não foi necessária, pois não existiria a necessidade de apresentar essa etapa ao entrevistado sendo apenas a analise observada diante da decisão que o usuário viesse a tomar pela aceitação ou não de um arquivo sugestivo. A técnica de camuflagem de arquivos

com a possibilidade de execução de instruções quando o mesmo recebe em seus dispositivos é constantemente apresentada a todos os usuários de forma cotidiana na internet.

O arquivo criado possuía 20 (vinte) megabytes de conteúdo nulo com a proposta de ser um arquivo com título especifico e sugestivo acerca do tema apresentado aos entrevistados “Cartilha de Segurança” traçado a hipótese desse arquivo que dentro do nível de confiança obtido pela pesquisa fosse possível de passar pelo filtro de aceitação do usuário questionado de forma instintiva, se permitia a conclusão do download do arquivo.

Como resultado final da pesquisa, é possível observar que existe a necessidade de criar ações de conscientização, com a ideia de experimentação de como pode se apresentar uma possível ameaça para o usuário, pois mais importante que venha ser, a teoria deve vir acompanhada com a prática, pois ambas são decisivas para aumentar as chances de evitar comprometimento de informações pessoais estando elas ou não em dispositivos pessoais.

3.7.2 MEDIDAS PREVENTIVAS

A pesquisa possibilitou vislumbrar a tomadas de decisão dos usuários frente a aplicação da técnica de *Spear Phishing*, além do que se constatou, que o compartilhamento entre pessoas próximas dos entrevistados, acarretou em um aumento de confiança no acesso ao link da pesquisa e levava o usuário em um determinado momento a interagir com o questionamento do aceite ou não do arquivo, sem conteúdo algum apenas para avaliação da tomada de decisão do usuário, mas que poderia ser um *spear phishing scam*, se utilizado por pessoas mal-intencionadas.

Todos os dias os usuários da internet são submetidos a eventuais situações semelhantes, desta forma é necessário manter a vigilância a todo passo a ser dado no ambiente *web.* Algumas sugestões foram elencadas para auxiliar na mitigação de ataques de *spear phishing* são elas:

- Questionar a fonte da origem do arquivo ou link compartilhado (CERT.BR, 2018);
- Utilizar plataformas de busca para rastrear o link em busca de mais informações

sobre o ambiente que você está sendo convidado a utilizar existe uma plataforma chamada Relatório de Transparência, criado pela Google, que faz este procedimento sendo indicado como uma boa ferramenta para este fim (GOOGLE, 2018);

- Utilizar aplicações de antivírus que se comunicam com navegadores para analisar o link em questão e se o mesmo se encontra em lista negras que são constantemente atualizadas, por diversas empresas em todo mundo (CERT.BR, 2018);
- Em se tratando de aplicações sociais, verificar o serviço de configuração, assim como a parte reservada a privacidade para personalizar que tipo de informação deseja ter caráter público (BELLO, 2011);
- Criar políticas próprias de segurança quanto ao nível de aceitação de arquivos e links gerado pelas pessoas de seu ciclo de convivência (CERT.BR, 2018).
- Manter um serviço de backup sempre em operação, observado a necessidade de uma cópia total do sistema ou apenas a disponibilização de pastas em serviços de backup online, bem como a disponibilidade das mesmas em outros dispositivos de armazenamento (CERT.BR, 2018).
- Uma vez sendo alvo de sequestro eletrônico, executar procedimentos de retorno do backup, juntamente com a formatação do ambiente infectado, além da análise de dispositivos utilizados como memórias secundárias da presença de elementos que possam retornar à ação do *malware*, antes da formatação (CERT.BR, 2018).
- Não efetuar pagamento de resgaste pois existe a chance de não haver a recuperação dos dados (CERT.BR, 2018).

4 CONSIDERAÇÕES FINAIS E RECOMENDAÇÕES

E finalizando esta monografia, foram feitas a seguir as considerações e recomendações finais. Descrevendo sobre a conclusão do objeto de estudo que pode auxiliar na pesquisa realizada.

4.1. CONSIDERAÇÕES FINAIS

O intuito desse trabalho é apresentar como hoje a engenharia social é aplicada em ações de pessoas mal-intencionadas para obter informações sensíveis em potencial. Possibilitando o ato de sequestro eletrônico, sendo este aplicável quando o arquivo sugerido venha camuflado para reais intenções com determinadas instruções para execução do ato, uma vez que o usuário venha tomar decisão que possibilite a conclusão do feito. Dentro dos objetivos específicos e da metodologia escolhida para essa pesquisa pode-se afirmar que o objetivo principal foi atingido.

Seguindo a linha de raciocínio da pesquisa, a proposta trouxe que com base no rastreio de uma quantidade relativa de informações que o usuário venha a disponibilizar nas redes sociais ou nas diversas aplicações de compartilhamento de informações, como: instagram, facebook, twitter, foursquare[17], torna-se possível quando identificado os limites que contornam o perfil do mesmo, ser estabelecido formas de produzir ações para obter acesso aos dispositivos dos usuários.

A pesquisa vem como um alerta para quais medidas devem-se inferir com base na observação da forma como ocorre o processo de sequestro eletrônico, percebendo as falhas que poderão ser utilizadas contra o usuário e as medidas que podem ser tomadas para contra-atacar esses tipos de ações, visando um posicionamento para o ganho de segurança na internet.

Nesta pesquisa, apresentamos primeiramente as características da Engenharia Social que é apontada no contexto de segurança da informação, como um ponto chave na aproximação dos usuários para verificar o seu comportamento, buscando conhecer seu cotidiano.

Analisando as tomadas de decisão por parte dos usuários foi constatado que mesmo que o comportamento coletivo se apresente com elementos cercados de segurança e ações preventivas, quando o mesmo é apresentado a uma possível armadilha ocorre indicações contrárias, ao posicionamento exposto durante as entrevistas. Na análise do ambiente de teste constatou-se a alta taxa de aceitação da proposta de *phishing*. O que traz um alerta, pois mesmo o usuário detendo o máximo de informação sobre o tema de segurança, na prática, ele desconhece o comportamento correto em ações deste tipo.

Como uma solução imediata para corrigir ação de phishing é dar atenção a atualização das aplicações nativas do usuário, bem como a atenção especial com respeito a atualizações do sistema operacional. Existe também a necessidade de manter os *drivers*[18] dos dispositivos físicos também atualizados para minimizar a chance de ter falhas sendo exploradas por *exploit*. O uso de software de análise em tempo real para prevenção de vírus localmente aumenta a expectativa de um ambiente seguro.

---

[17] Plataforma de rede sociais cada qual com o seu diferencial acerca da informação gerida na mesma.
[18] Driver e o que faz simplifica a tarefa da aplicação atuando como um tradutor entre o dispositivo físicos e as aplicações logicas ou o sistema operacional.

Quanto aos enquadramentos da pesquisa, salienta-se que, por se tratar de um estudo de caso específico os resultados embora possuam uma abrangência nacional, tomando como base a identificação territorial dos entrevistados, aplicam-se apenas para o objeto de estudo, não podendo ser empregado para interpretações de outras organizações.

A pesquisa possibilitou valiosas interações com conhecimento obtidos durante o curso vale salientar as matérias que estimularam a pesquisa sendo elas matéria acerca de Segurança da Informação instruída durante o momento na Universidade Federal do Acre onde foi gerado o desperta para essa questão.

Em questionamentos acerca de engenharia social houve proximidade com informações obtidas através de matérias como Teoria Geral de Sistemas (UFAC) e Sistemas de apoio a Gestão (UFPB) que ambas trouxeram conhecimento a um nível maior de complexidade do uso da engenharia social onde chegava ao passo de espionagem industrial tema esse discutido também na matéria de Segurança da Informação.

Em se tratando de conhecimentos acerca de exploit, ataques de MITM e informações acerca de bitcoins foi juntamente com matéria de Redes de Computadores e Gerencia de Redes (UFAC).

E no desenvolvimento web que facilitou a geração da página que continha o questionário foi com o conhecimento adquirido durante o Estágio Supervisionado (UFAC) onde foi desenvolvido o mesmo na linguagens de programação web.

E acerca da matéria de Ética e Legislação aplicada a Informática (UFAC) que possibilitou enxerga questões jurídicas, como indicações de onde buscar informação, acerca de alguns pontos que poderiam nortear em que se enquadrava essa pratica acerca de sequestro eletrônico.

4.2. RECOMENDAÇÕES

A pesquisa teve como objetivo identificar as tomadas de decisão dos usuários frente a aplicação de uma variante da técnica de *Spear phishing*, que trata de foco direcionado e personalizado de ataque. Nesse sentido sugere-se:

- Desenvolvimento de softwares que consigam identificar quais os nichos de vítimas mais propensos a ataques de engenharia social com dados obtidos a partir de coletas de dados feitos junto a estas vítimas; ou

- Desenvolvimento de softwares que consigam simular ataques de vários formatos para serem testados por usuários para compreender padrões e como melhorar na tomada de decisão frente a essas ações.

- Desenvolvimento de softwares para elencar os possíveis passos de quem pode está sujeito a um cibercrime, tendo como base as ações que o usuário disponibiliza em suas redes sociais, na internet, quais tipos de serviços (compras, bancários) e dispositivos de segurança são utilizados em seus equipamentos.

REFERÊNCIAS

ABRAMS, L. **SyncCrypt Ransomware Hides Inside JPG Files, Appends .KK Extension**. Disponível em: <https://www.bleepingcomputer.com/news/security/synccrypt-ransomware-hides-inside-jpg-files-appends-kk-extension/>. Acesso em: 5 nov. 2018.

Are you ready for blockchain? Disponível em: <https://www.thomsonreuters.com/en/reports/blockchain.html>. Acesso em: 22 fev. 2019.

BALTZAN, P. **Tecnologia Orientada para Gestão - 6ed**. [s.l.] McGraw Hill Brasil, 2016.

BELLO, C. D. Visibilidade, vigilância, identidade e indexação: a questão da privacidade nas redes sociais digitais. **Logos**, v. 18, n. 1, 18 nov. 2011.

BLACK, L. **LSB-Steganography - Python program to steganography files into images using the Least Significant Bit**. Disponível em: <http://www.kitploit.com/2018/02/lsb-steganography-python-program-to.html>. Acesso em: 21 fev. 2019.

BRASIL. **Lei N° 2848**. . 7 dez. 1940.

BRASIL. **Lei Nº 12.737**. . 30 nov. 2012, p. 1.

BRASIL. **Lei N° 12.965**. . 23 abr. 2014.

BRUMAGHIN, E. **CCleanup: A Vast Number of Machines at RiskCisco Talos Intelligence**, 2017. Disponível em: <http://blog.talosintelligence.com/2017/09/avast-distributes-malware.html>. Acesso em: 5 nov. 2018

CERT, N. B. **Cartilha de Segurança -- Códigos Maliciosos (Malware)**. Disponível em:

<https://cartilha.cert.br/malware/>. Acesso em: 5 nov. 2018.

CERT.BR. **Cartilha de Segurança para Internet**. Informativo. Disponível em: <https://cartilha.cert.br/>. Acesso em: 16 fev. 2019.

CONTI, M.; GANGWAL, A.; RUJ, S. **On the economic significance of ransomware campaigns: A Bitcoin transactions perspective**. Computers & Security, v. 79, p. 162–189, 1 nov. 2018.

DA SILVA, C. L. A. **Três décadas de ransomware: uma linha do tempo da nova praga digital**, 2017. Disponível em: <https://www.codigofonte.com.br/artigos/tres-decadas-de-ransomware-uma-linha-do-tempo-da-nova-praga-digital>. Acesso em: 13 dez. 2018

DUNN, J. E. **Phishing attacks: is it time to take employee training more seriously?** Disponível em: <https://www.techworld.com/security/phishing-attacks-is-it-time-take-employee-training-more-seriously-3644608/>. Acesso em: 21 fev. 2019.

Esteganografia utilizando steghide [Artigo]. Disponível em: <https://www.vivaolinux.com.br/artigo/Esteganografia-utilizando-steghide>. Acesso em: 21 fev. 2019.

FEDERAL BUREAU INVESTIGATION. **Spear Phishing**. Disponível em: <https://www.fbi.gov/news/stories/2009/april/spearphishing_040109>. Acesso em: 13 dez. 2018.

FORTINI, M. **Least Significant Bits (LSB) insertion**. Disponível em: <http://www.lia.deis.unibo.it/Courses/RetiDiCalcolatori/Progetti98/Fortini/lsb.html>. Acesso em: 5 nov. 2018.

GLEB ESMAN. **Connecting the Dots: Tracking Identity of DDOS-for-Bitcoins criminal service operator with Maltego, Splunk and DomaintoolsMensk Technologies Inc**, [s.d.]. Disponível em: <http://www.mensk.com/tracking-identity-of-ddos-for-bitcoins-criminal-service-operator-with-maltego-splunk-and-domaintools/>. Acesso em: 21 fev. 2019

GOOGLE. **Google Transparency Report**. Disponível em: <https://transparencyreport.google.com/>. Acesso em: 16 fev. 2019.

GROSS, R.; ACQUISTI, A. **Information Revelation and Privacy in Online Social Networks (The Facebook case)**. p. 11, 2005.

HETZL, S. **Steghide - Manual**. Disponível em: <http://steghide.sourceforge.net/documentation/manpage.php>. Acesso em: 5 nov. 2018.

IBGE. **IBGE - Agência de Notícias | PNAD Contínua TIC 2016: 94,2% das pessoas que utilizaram a Internet o fizeram para trocar mensagens**. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/20073-pnad-continua-tic-2016-94-2-das-pessoas-que-utilizaram-a-internet-o-fizeram-para-trocar-mensagens>. Acesso em: 5 nov. 2018.

Malware Example: Q CASINO.COM. [s.l: s.n.] Disponivel em: <https://archive.org/details/malware_Q-CASINO.COM> Acesso em:13 fev 2019.

NAKAMOTO, S. **Bitcoin: A Peer-to-Peer Electronic Cash System**. p. 9, 2008.

PATERVA. **Showcase**. Disponível em:

<https://www.paterva.com/web7/docs/use_cases.php>. Acesso em: 13 fev. 2019.

POLLON, V. **Esteganografia: a arte de ocultar arquivos dentro de arquivos - Vande…**, 2006. Disponível em: <https://pt.slideshare.net/tchelinux/esteganografia>. Acesso em: 5 nov. 2018

SIMON, W. L.; MITNICK, K. D. **A Arte De Enganar**. [s.l.] MAKRON, 2003.

SYMANTEC, N. **2017 Norton Cyber Security Insights Report - Global Results**. p. 30, 2018.

ULBRICH, H. C.; VALLE, J. D. **UNIVERSIDADE HACKER - H4CK3R: DESVENDE TODOS OS SEGREDOS DO SUBMUNDO DOS HACKERS**. [s.l.] Digerati (livros), 2009.

ULTRADOWNLOADS. **O que é Phishing Scam? - Hacker**. Disponível em: <https://canaltech.com.br/hacker/O-que-e-Phishing-Scam/>. Acesso em: 21 fev. 2019.

VIRUSTOTAL. **Virus Total - Analise cartilha de segurança pdf**. Disponível em: <https://www.virustotal.com/pt/file/543212439c109ae76e055429cebcd48e811ea810c3994f56df37cd0ebb072e00/analysis/1550214380/>. Acesso em: 21 fev. 2019.

VOLTOLINI, R. **Controles ActiveX desatualizados serão bloqueados pelo Internet Explorer**. Disponível em: <https://www.tecmundo.com.br/internet-explorer/60201-controles-activex-desatualizados-bloqueados-internet-explorer.htm>. Acesso em: 15 fev. 2019.

WE ARE SOCIAL. **Digital in 2018 Global Overview**, 2018. Disponível em: <https://www.slideshare.net/wearesocial/digital-in-2018-global-overview-86860338?ref=https://wearesocial.com/blog/2018/01/global-digital-report-2018>. Acesso em: 5 nov. 2018

YANG, Y. et al. **Stalking online: on user privacy in social networks**. Proceedings of the second ACM conference on Data and Application Security and Privacy - CODASKY ’12. **Anais**... In: THE SECOND ACM CONFERENCE. San Antonio, Texas, USA: ACM Press, 2012Disponível em: <http://dl.acm.org/citation.cfm?doid=2133601.2133607>. Acesso em: 14 dez. 2018

APÊNDICE A

Sua segurança na internet como anda?

O questionário dura menos de 2 minutos e suas respostas serão tratadas de forma totalmente anônima.

*Obrigatório

1. **Qual a sua idade?** *
   Marcar apenas uma oval.

- ◯ Até 18 anos
- ◯ De 19 à 25 anos
- ◯ De 26 à 35 anos
- ◯ De 36 à 45 anos
- ◯ Acima de 45 anos

2. **Qual sua identidade de gênero?** * *Marcar apenas uma oval.*

- ◯ Feminino
- ◯ Masculino
- ◯ Prefiro não dizer
- ◯ Outro

3. **Qual a sua escolaridade?** *
   Marcar apenas uma oval.

- ◯ Ensino Fundamental Incompleto
- ◯ Ensino Fundamental Completo
- ◯ Ensino Médio Incompleto
- ◯ Ensino Médio Completo
- ◯ Ensino Superior Incompleto
- ◯ Ensino Superior Completo

4. **Você possui rede sociais?** * *Marcar apenas uma oval.*

- ◯ Sim
- ◯ Não *Após a última pergunta desta seção, vá para "Obrigado pela sua participação.."*

5 **Com que frequência utiliza a internet?** * *Marcar apenas uma oval.*

- ◯ Sempre (todos os dias)
- ◯ Com bastante frequência (em média, 5 vezes por semana)
- ◯ Com frequencia razoável (em média, 3 vezes por semana)
- ◯ Com pouca frequência (em média, 1 vez por semana)
- ◯ Raramente (em média, 1 vez por mês)
- ◯ Não utilizo *Após a última pergunta desta seção, vá para "Obrigado pela sua participação.."*

6. **Em geral, quanto tempo por dia você permanece conectado à Internet?** * *Marcar apenas uma oval.*

- ◯ Até 1 hora
- ◯ De 1 a 3 horas
- ◯ De 3 a 5 horas
- ◯ Mais de 5 horas
- ◯ Não utilizo. *Ir para "Obrigado pela sua participação.".*

Continuação da pesquisa

7. **Você mantem seu computador/notebook/Smartphone atualizado?** * *Marcar apenas uma oval.*

- ◯ Sim *Após a última pergunta desta seção, ir para a pergunta 7.*
- ◯ Não *Após a última pergunta desta seção, ir para a pergunta 7.*

8. **O que você costuma fazer na Internet.**

Pode escolher mais de uma alternativa. *Marque todas que se aplicam.*

- [ ] Trocar emails
- [ ] Participar de fóruns de discussão
- [ ] Navegar pelos sites de seu interesse
- [ ] Ler notícias
- [ ] Pesquisas em sites de busca
- [ ] Conversar com pessoas (troca de mensagens instantâneas)
- [ ] Fazer downloads (séries, filmes, músicas, etc.)
- [ ] Utilizar serviços bancários : Pagamento, Transferência
- [ ] Fazer compras

9. **Em se tratando de segurança... Onde você guarda sua senha?** * *Marcar apenas uma oval.*

   - ◯ Memorizo
   - ◯ Anoto na minha agenda
   - ◯ Utilizo aplicativos para gerencia de senha
   - ◯ Utilizo o "recuperar senha" pois tenho dificuldade de lembrar.

10. **A sua senha é utilizada de forma padrão em mais de um serviço? (Ex:.Dropbox, Facebook, Uber, entre outros)** * *Marcar apenas uma oval.*

    - ◯ Sim
    - ◯ Não

11. **Informe a quantidade de aplicações sociais que você utiliza** * *Marcar apenas uma oval.*

    - ◯ De 1 a 3
    - ◯ De 3 a 5
    - ◯ Mais de 5
    - ◯ Não lembro

12. **Durante a navegação já houve algum momento que clicou de forma intencional em propagandas?**
    Marcar apenas uma oval.

    - ◯ Sim
    - ◯ Não

13. **Em conversas é frequente aparecer link's direcionando para sites. Você possui costume de clicar neles?** *
    Marcar apenas uma oval.

    - ◯ Sim
    - ◯ Não

Privacidade e Segurança - Tópicos

Com base nas frases indique se concorda com elas.

14. **Eu gerencio a minha privacidade nas redes sociais.** * *Marcar apenas uma oval.*

	1	2	3	4	5	
Discordo Totalmente	◯	◯	◯	◯	◯	Concordo Totalmente

15. **Eu troco a senha das minhas redes sociais frequentemente (de 2 a 4 meses)** *
Marcar apenas uma oval.

	1	2	3	4	5	
Discordo Totalmente	◯	◯	◯	◯	◯	Concordo Totalmente

16. **Eu faço a segurança de duas etapas nos aplicativos que utilizo** * *Marcar apenas uma oval.*

	1	2	3	4	5	
Discordo Totalmente	◯	◯	◯	◯	◯	Concordo Totalmente

17 **Nas minhas redes sociais, eu aceito todas as solicitações de amizades.** * *Marcar apenas uma oval.*

	1	2	3	4	5	
Discordo Totalmente	◯	◯	◯	◯	◯	Concordo Totalmente

18. **As minhas redes sociais são abertas ao público em geral, divulgo minhas informações sem gerenciar a privacidade ou limitar o publico que segue/não segue o meu perfil.** *
Marcar apenas uma oval.

	1	2	3	4	5	
Discordo Totalmente	◯	◯	◯	◯	◯	Concordo Totalmente

19. **Eu ativo o serviço de localização / Gosto de compartilhar minha localização nas redes sociais.** *
Marcar apenas uma oval.

	1	2	3	4	5	
Discordo Totalmente	◯	◯	◯	◯	◯	Concordo Totalmente

20. **Eu compartilho a senha de alguma rede social com alguém da minha confiança.** * *Marcar apenas uma oval.*

1	2	3	4	5

Discordo Totalmente	◯	◯	◯	◯	◯	Concordo Totalmente

21. **Em se tratando de compartilhamento de arquivos/links, Eu busco saber a sua origem.** *
Marcar apenas uma oval.

	1	2	3	4	5	
Discordo Total	◯	◯	◯	◯	◯	Concordo Totalmente

Obrigado pela sua participação.

VIDEO - Dicas de segurança nas redes social.