ACADEMIA MILITAR DAS AGULHAS NEGRAS
ACADEMIA REAL MILITAR (1811)
CURSO DE CIÊNCIAS MILITARES

Lucas Fernando Peña Farias

ANÁLISE DA INFLUÊNCIA DO USO DE REDES SOCIAIS POR CADETES PARA A SEGURANÇA DA INFORMAÇÃO NA AMAN EM 2021

Resende
2022

	APÊNDICE III (TERMO DE AUTORIZAÇÃO DE USO DE DIREITOS AUTORAIS DE NATUREZA PROFISSIONAL) AO ANEXO B (NITCC) ÀS DIRETRIZES PARA A GOVERNANÇA DA PESQUISA ACADÊMICA E DA DOUTRINA NA AMAN	**AMAN 2022**

TERMO DE AUTORIZAÇÃO DE USO DE DIREITOS AUTORAIS DE NATUREZA PROFISSIONAL

TÍTULO DO TRABALHO: ANÁLISE DA INFLUÊNCIA DO USO DE REDES SOCIAIS POR CADETES PARA A SEGURANÇA DA INFORMAÇÃO NA AMAN EM 2021
AUTOR: LUCAS FERNANDO PENA FARIAS

Este trabalho, nos termos da legislação que resguarda os direitos autorais, é considerado de minha propriedade.

Autorizo a Academia Militar das Agulhas Negras a utilizar meu trabalho para uso específico no aperfeiçoamento e evolução da Força Terrestre, bem como adivulgá-lo por publicação em revista técnica da Escola ou outro veículo de comunicação do Exército.

A Academia Militar das Agulhas Negras poderá fornecer cópia do trabalho mediante ressarcimento das despesas de postagem e reprodução. Caso seja de natureza sigilosa, a cópia somente será fornecida se o pedido for encaminhado por meio de uma organização militar, fazendo-se a necessária anotação do destino no Livro de Registro existente na Biblioteca.

É permitida a transcrição parcial de trechos do trabalho para comentários e citações desde que sejam transcritos os dados bibliográficos dos mesmos, de acordo com a legislação sobre direitos autorais.

A divulgação do trabalho, em outros meios não pertencentes ao Exército, somente pode ser feita com a autorização do autor ou da Direção de Ensino da Academia Militar das Agulhas Negras.

Resende, 18 de agosto de 2022.

Cad LUCAS FERNANDO PENA FARIAS

Dados internacionais de catalogação na fonte

F224a FARIAS, Lucas Fernando Peña

Análise da influência do uso de redes sociais por cadetes para a segurança da informação na AMAN em 2021. / Lucas Fernando Peña Farias – Resende; 2022. 40 p. : il. color. ; 30 cm.

Orientador: Nicolas Fiorito Ferreira Mouro Borba

TCC (Graduação em Ciências Militares) - Academia Militar das Agulhas Negras, Resende, 2022.

1.Golpes 2.Segurança da informação 3.Redes sociais 4.Phishing 5.Contato. I. Título.

CDD: 355

Ficha catalográfica elaborada por Jurandi de Souza CRB-5/001879

Lucas Fernando Peña Farias

ANÁLISE DA INFLUÊNCIA DO USO DE REDES SOCIAIS POR CADETES PARA A SEGURANÇA DA INFORMAÇÃO NA AMAN EM 2021

Monografia apresentada ao Curso de Graduação em Ciências Militares, da Academia Militar das Agulhas Negras (AMAN, RJ), como requisito parcial para obtenção do título de **Bacharel em Ciências Militares**.

Orientador: Ten Nicolas Fiorito Ferreira Mouro Borba

Resende
2022

Lucas Fernando Peña Farias

ANÁLISE DA INFLUÊNCIA DO USO DE REDES SOCIAIS POR CADETES PARA A SEGURANÇA DA INFORMAÇÃO NA AMAN EM 2021

Monografia apresentada ao Curso de Graduação em Ciências Militares, da Academia Militar das Agulhas Negras (AMAN, RJ), como requisito parcial para obtenção do título de **Bacharel em Ciências Militares.**

Aprovado em 01 de julho de 2022.

Banca examinadora:

Nicolas Fiorito Ferreira Mouro Borba – 1º Ten
(Orientador)

Eduardo Massayoshi Abe - Ten Cel

Lucas Espinato de Morais - 1º Ten

Resende
2022

Dedico primeiramente à Deus, que me acompanhou nesse longo caminho até a realização do meu sonho de me tornar oficial da linha de ensino militar bélico do Exército Brasileiro. Dedico, também, aos meus queridos pais, pilares fundamentais da minha educação e suportes para nunca me deixarem desistir desta caminhada.

AGRADECIMENTOS

Agradeço, antes de tudo à Deus, por ter orientado meu caminho durante toda a longa trajetória da formação da Academia Militar das Agulhas Negras atendendo sempre as minhas orações, mantendo-me sempre perseverante em relação aos inúmeros desafios e dificuldades impostas até o grande dia de tornar-se um oficial do Exército Brasileiro.

Agradeço também a minha família, principalmente meus pais, por estarem sempre ao meu lado quando eu mais precisei. Vocês são as grandes inspirações que me seguem em todas minhas conquistas.

Ao meu orientador, Tenente Fiorito, por dedicar seu tempo para me auxiliar e retirar dúvidas e me ajudar com tudo que eu precisei. Busco sempre me espelhar no senhor para crescer cada dia mais.

RESUMO

ANÁLISE DA INFLUÊNCIA DO USO DE REDES SOCIAIS POR CADETES PARA A SEGURANÇA DA INFORMAÇÃO NA AMAN

AUTOR: Lucas Fernando Peña Farias

ORIENTADOR: Nicolas Fiorito Ferreira Mouro Borba – 1º Ten

Golpes na internet tornaram-se mais recorrentes à medida em que a tecnologia passa pelo processo de desenvolvimento. Com isso, o impacto das ações cibernéticas passou a influenciar não só a vida de civis, mas também a de militares, principalmente dentro das organizações onde os mesmos atuam. A segurança da informação, nestas instituições, é comprometida devido ao descuido ou negligência dos usuários. Mediante isso, esse trabalho buscou abordar e analisar como o uso de redes sociais pode criar um potencial para o vazamento de informação da AMAN para o público externo, ilustrando desde a escolha da ferramenta utilizada, passando pela construção da engenharia social até a captura de informações sensíveis, de forma isolada e dentro de um ambiente controlado. O ponto de início parte da captura da credencial de uma vítima, em uma rede social, onde foi possível obter informações sobre como é o andamento de um dia de serviço nos parques da AMAN, fornecendo dados sensíveis que podem comprometer a segurança de militares e civis, tanto fora quanto no interior da organização militar. No primeiro momento, foi construído um contexto para convencer a vítima do golpe a acessar um link utilizado para realizar um golpe de "Phishing". Em seguida, obteve-se o usuário e a senha da vítima. Por último, após o acesso a conta, foi realizada a interação com um contato próximo da vítima para a extração dos dados, tomando o devido cuidado para não gerar dúvidas sobre a verdadeira identidade do agente malicioso. Como resultado, foram discutidos atitudes que o golpista poderia pôr em prática, agora que conhece as peculiaridades das atividades internas da AMAN.

Palavras-chave: Golpes. Segurança da informação. Redes sociais. Phishing. Contato.

ABSTRACT

ANALYSIS OF THE INFLUENCE OF THE USE OF SOCIAL NETWORKS BY CADETS FOR INFORMATION SECURITY AT AMAN EM 2021

AUTHOR: Lucas Fernando Pena Farias

ADVISOR: Lt. Nicolas Fiorito Ferreira Mouro Borba

Internet scams have become more frequent as the technology has gone through the development process. As a result, the impact of cybernetic actions began to influence not only the lives of civilians, but also the military, especially within the organizations where they operate. Information security, in these institutions, is compromised due to carelessness or users negligence, therefore, this work sought analyze how the use of social networks can create a potential information leakage in AMAN to the external public, illustrating from the choice of tool, through the construction of social engineering used to capture sensitive information, in isolation and within a controlled environment. The starting point is capturing the credential from a social network, where it was possible to obtain information about the progress of a service day in the AMAN parks, providing sensitive data that can compromise the security of military and civilians, both outside and inside the military organization. In the first moment, a context was built to convince the victim of the scam to access a link used to carry out a *"Phishing"* scam. Then, the victim's username and password were obtained. Finally, after accessing the account, an interaction was performed with a close contact of the victim to extract the data, taking care not to generate doubts about the true identity of the malicious agent. As a result, it was discussed behaviors that the scammer could put into practice, now that he knows the peculiarities of AMAN's internal activities.

Keywords: Scam. Information security. Social networks. Phishing. Contact.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

Com a criação da *Advanced Research Projects Agency Network (*ARPAnet), o universo da informática desenvolveu-se em proporções exponenciais, exigindo que sua administração evoluísse na mesma medida. É nesse contexto que os primeiros protocolos de comunicação entre computadores surgem, possibilitando, posteriormente, o embrião da internet como conhecemos nos dias atuais (FILIPPETTI, 2018). Acompanhada da nova rede de informação, os golpes em ambientes virtuais aprimoraram-se cada vez mais, apresentando diversas formas de invadir contas bancárias e, principalmente, redes sociais para obter, destruir ou modificar informações de pessoas desavisadas (MORENO, 2015).

Nesse sentido, a internet tornou-se algo tão presente e, talvez, um serviço quase obrigatório em qualquer estabelecimento, que acaba-se por ignorar os riscos que o uso descuidado da rede pode proporcionar. Seja em um aeroporto ou em uma cafeteria, ou até mesmo em uma simples praça de alimentação, as pessoas se tornam passíveis de golpes cibernéticos por não observar as boas práticas para o uso seguro da internet, especialmente nas redes sociais. (VIENAZINDYTE, 2020).

O crescimento de funcionalidades desses espaços virtuais proporciona um ambiente de interação interpessoal em qualquer parte do mundo. Qualquer pessoa pode, hoje, criar um perfil e compartilhar fotos, opiniões, notícias, rotina do dia a dia ou qualquer outra coisa sobre a vida. É nesse contexto que golpes em ambiente virtual acontecem e informações pessoais são furtadas e usadas para a prática de estelionato ou extorquir os usuários. (QUEIROZ, 2019).

Vale ressaltar que tais práticas podem ser feitas por qualquer pessoa que tenha acesso a um computador e internet, por mais leiga que seja. O acesso ao conhecimento é facilitado por tutoriais e blogs que ensinam a realização de uma armadilha de forma simples e direta. *Phishing* é uma das mais populares técnicas de fraudes on-line e que está em constante evolução. (JORGE, 2007).

Para realizá-lo, o agente malicioso utiliza-se de e-mails, sites falsos e aplicativos para se passar por outra pessoa ou instituição. Assim, envia mensagens falsas às vítimas e aguarda até que elas a acessem. Dependendo dos interesses do agente malicioso, basta o acesso à mensagem e, em outro caso, a vítima pode enviar e-mail e senha, credenciais de uma conta de usuário, podendo gerar efeitos irreversíveis. (KASPERSKY, 2022).

Para a Avast Academy, página de informações sobre segurança na internet da companhia de software de antivírus:

> Seja conduzido por e-mail, redes sociais, SMS ou outro vetor, todos os ataques de phishing seguem os mesmos princípios básicos. O golpista envia um texto direcionado, com o objetivo de convencer a vítima a clicar em um link, baixar um anexo, enviar as informações solicitadas ou até mesmo concluir um pagamento real. Quanto aos efeitos do phishing, eles dependem da imaginação e habilidade do phisher. O advento das redes sociais significa que os phishers têm acesso a mais informações pessoais sobre seus alvos do que nunca. Com todos esses dados à disposição, os phishers podem adaptar com precisão os ataques às necessidades, desejos e circunstâncias da vida de seus alvos, o que resulta em uma proposta muito mais atraente. Nesses casos, as redes sociais alimentam uma engenharia social mais poderosa. (AVAST, 2020)

Ainda nesse contexto, essa prática pode ser reproduzida dentro de organizações militares, em especial, a Academia Militar das Agulhas Negras (AMAN) o que pode constituir um problema. Com esses golpes, é possível espionar e expor a vida dos cadetes nas redes sociais, além de identificar atividades que são sensíveis para a segurança do cadete e da AMAN. Dentre elas estão a escala de serviço, exercícios escolares em campo e vida

Partindo desse problema, essa pesquisa abordará uma análise de golpes e técnicas de invasão ao universo dos cadetes do curso de intendência a fim de estudar qual o comportamento obtido acerca do impasse posto a eles e, por fim, ilustrar como a análise desses eventos podem ser utilizados para diminuir esses tipos de situações e conscientizar não só os cadetes, mas o usuário da rede propriamente dito.

No referencial teórico, são apresentados todos os conceitos necessários para o melhor entendimento e aproveitamento das sequência das ações, tomadas durante todo o processo da ação cibernética. Estruturas de uma rede, um sistema operacional e a captura de credencial são explicadas nesse capítulo.

A partir do referencial metodológico, demonstra-se, passo a passo, como são realizados os procedimentos para a captura de informação, utilizando a ferramenta de phishing *zphisher*.

Nos resultados, foram reunidos todos os dados coletados para ilustrar o envolvimento do golpista com a vítima, utilizando a identidade de alguém próximo, para aumentar a credibilidade.

Por fim, na discussão, busca-se chegar á conclusão do problema apresentado, discutindo os motivos que tornaram o golpe possível e que são sensíveis no que tange a segurança da AMAN.

1.1 OBJETIVOS

1.1.1 Objetivo geral

Analisar a influência de golpes cibernéticos em redes sociais de cadetes para observar quais as consequências para a segurança da informação na AMAN.

1.1.2 Objetivos específicos

Apresentar o método de criação de uma página falsa da internet;

Descrever como uma ação de engenharia social funciona;

Verificar como as informações capturadas podem ser obtidas;

Demonstrar como essas informações podem ser utilizadas e quais os riscos provocados;

Salientar a importância da postura proativa dos usuários no que tange ao uso seguro das redes sociais.

2 REFERENCIAL TEÓRICO

2.1 COMO FUNCIONA UMA REDE DE COMPUTADORES

Antes de entender um ataque, é preciso entender como computadores comunicam-se entre si. Essa comunicação é feita por um conjunto de protocolos que são responsáveis por receberem, interpretarem e responderem todas as informações compartilhadas. A fim de padronização entre diversos fabricantes, criou-se umas das mais importantes pilhas de protocolos de comunicação: o modelo teórico OSI (Open Systems Interconnection), atualmente aplicado no protocolo TCP/IP (Transmission Control Protocol / Internet Protocol). Esse novo modelo foi estruturado em quatro camadas conceituais e construído sobre uma quinta camada (COMER, 2000). Veja a comparação no quadro 1:

Quadro 1 - Comparação do modelo OSI com o modelo TCP/IP

OSI	TCP/IP
Aplicação	Aplicação
Apresentação	
Sessão	
Transporte	Transporte
Rede	Internet
Enlace	Enlace
Física	Física

Fonte: ELBORADO PELO AUTOR (2022)

Em seu livro, Tanenbaum explica que “basicamente, um **protocolo** é um acordo entre as partes que se comunicam, estabelecendo como se dará a comunicação” (TANENBAUM; WETHERALL, 2011 p. 18). De forma simplificada, quando duas máquinas tentam se comunicar, pacotes de dados são processados na camada de **aplicação**, onde temos aplicativos e programas voltados para a interação humana com a máquina. É nessa camada que conseguimos enviar links, documentos, e-mails e acessar páginas da internet. Em seguida, esses dados são enviados para a camada de **apresentação**, onde são traduzidos para os formatos da Web como HTML, XML JPEG OU GIF. Além disso, é nessa camada que esses dados são criptografados, caso seja necessário, para, em seguida, serem transportados de uma máquina a outra. Antes, porém, necessitam passar pela camada de **sessão** para garantir que os

hosts - dispositivo conectado à rede - estejam conectados para poderem configurar e coordenar a troca de dados de cada lado da conexão, mantendo a comunicação.

Os dados obtidos na camada anterior estão prontos para serem enviados e entram na camada de **transporte,** onde realmente serão enviados de uma ponta a outra da conexão. Isso é feito por dois protocolos: o TCP e o UDP.

O TCP (Transmission Control Protocol) recebe uma quantidade de dados e os dividem em partes menores. Esses pedaços, agora segmentos, são numerados e sequenciados, facilitando a reconstrução do dado inicial na camada de aplicação da máquina destinatária. Além disso, antes de iniciar a transmissão, os protocolos TCP das duas máquinas (remetente e destinatário) estabelecem um caminho pré-definido que será utilizado para o envio dos dados. Após uma quantidade de segmentos enviados, a máquina remetente aguarda um sinal ACK (*acknowledgement*) da máquina destinatária, uma confirmação de que os segmentos foram recebidos. Caso esse sinal não seja recebido, a máquina remetente irá retransmitir os segmentos que não foram confirmados. Esse protocolo ainda passa a determinar o volume de dados que serão transmitidos antes de o TCP de destino envie sua confirmação para transmissão, realizando-se assim um controle de fluxo de dados rigoroso e estabelecendo que o número de retransmissões seja o mínimo possível. (FILIPPETTI, 2018).

O UDP (User Datagram Protocol) vem como uma versão simplificada do TCP, tendo um cabeçalho com reduzido campo de controle, resultando em menos largura de banda durante a transmissão dos segmentos. Por isso, a confiabilidade da entrega não é o objetivo desse protocolo, mas sim a agilidade e eficiência. (FILIPPETTI, 2018).

Porém, faz-se necessário saber onde essas máquinas estão localizadas e, para isso, usa-se o endereço IP, o que identifica a máquina do usuário de origem e de destino na rede, na camada de **rede**. Quando a mensagem chega ao destinatário, os pacotes de dados são divididos e passados por um controle de fluxo, semelhante ao da camada de rede, mas dessa vez, em uma rede interna, verificando qual o endereço MAC do computador destinatário na camada de **enlace.** (FILIPPETTI, 2018).

Nessa camada, asseguram-se que os dados sejam transmitidos ao equipamento certo, além de fazer a conexão entre a camada de Rede e a mais baixa, a Física, o que torna possível a transmissão através de vários meios físicos. Em outras palavras, a "camada de enlace é responsável pela identificação física de cada máquina em uma rede local", usando para isso, o endereço de hardware - MAC *address* - sequencia de 48 bits sequenciados canonicamente. (FILIPPETTI, 2018).

Agora na última camada, todos os dados são convertidos em um fluxo de bits para serem interpretados na camada **física**, isto é, na forma de pulsos elétricos. O processo inverso é feito para fins de resposta ao computador remetente até a sua camada de aplicação, onde há a interação humana com a máquina. (FILIPPETTI, 2018).

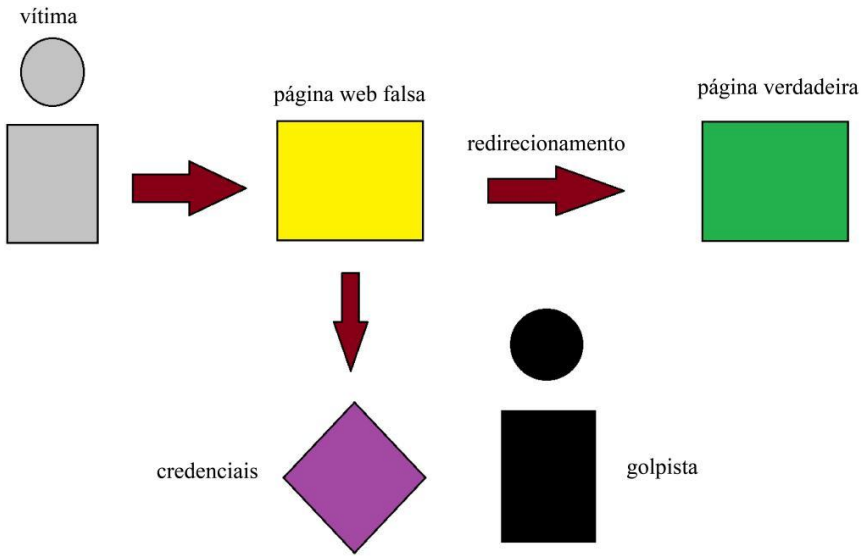
É exatamente nessa camada (aplicação), em que são realizados os ataques de phishing, que o usuário pode interagir com o ambiente virtual e acabar por enviar suas informações sem mesmo se dar conta disso. Para isso, o atacante pode utilizar uma série de ferramentas encontradas em uma das distribuições Linux: o Kali Linux, distribuição voltada para testes de penetração e análise de vulnerabilidades. Como explica Danel Moreno: O Kali Linux é um "sistema operacional, baseado no Debian, destinado a testes de penetração. Fornece diversas ferramentas para auditoria e realização de teste de segurança em redes de computadores, permitindo descobrir e explorar diversos tipos de vulnerabilidades." (MORENO, 2015, p.20).

Linux é um sistema operacional de computador. Um sistema operacional consiste no software que gerencia seu computador e permite que você execute aplicativos nele (NEGUS, 2014). O Linux nada mais do que o núcleo de um sistema operacional, o qual tem o papel de estabelecer a comunicação entre a parte física de uma máquina como o teclado, o monitor e as peças internas do computador (*hardware*) e a parte lógica como os aplicativos e programas (software). Sendo assim, esse núcleo, também chamado de *kernel*, em conjunto com os programas que interagem com ele são o que formam o sistema operacional utilizado pelo computador. Dessa maneira, o Kali Linux nada mais é do que um núcleo acompanhado de programas responsáveis para seu funcionamento acompanhado de uma série de ferramentas que são utilizadas para realizar ataques.

Agora que já se entende como a rede de computadores funciona e qual máquina utilizar, deve-se entender como é pensado o ataque e qual ferramenta utilizar.

Golpistas desenvolvem peças de e-mail ou SMS, aplicativos, fazem sites falsificados ou usam redes sociais para disparar milhões de mensagens por dia. Eles esperam até que os destinatários recebam e abram as mensagens (CERT.BR, 2012). Se estiver desatenta, a vítima fornecerá o usuário e senha, informações essas que estão prontas para serem capturadas pelo golpista. Feito o furto dos dados, a vítima é redirecionada para a versão da página verdadeira para que consiga realizar o *login* sem criar muitas suspeitas. Veja na figura 1.

Figura 1. Esquema de captura de credenciais



Fonte: AUTOR (2022)

Apesar de existirem inúmeras ferramentas para esse tipo de ataque, nenhum deles funcionaria sem antes garantir que a vítima se convença de que o que ela está compartilhando ou acessando é verdadeiro e seguro. Para isso usa-se a engenharia social, que é o uso de qualquer meio ou técnica para a manipulação ou persuasão a fim de obter-se informações confidenciais e acesso à áreas restritas. (MORENO, 2015).

Segundo Daniel Moreno (2015, p. 165), “Engenharia social consiste no ato de obter informações das pessoas”. Com e-mails, sites clonados ou SMS, todos seguem o mesmo princípio: busca-se induzir a vítima de que o que foi compartilhado é legitimo e que são de fontes confiáveis, como uma pessoa próxima da família, amigos ou alguma instituição de confiança. Altruísmo, raiva, culpa ou qualquer outro sentimento que faça alguém se identificar com o que foi compartilhado também são usados para convencer o usuário de que ele necessita acessar ou participar do que foi divulgado. (MORENO, 2015).

Entretanto, os métodos de engenharia social vão muito além de enviar e-mail e mensagens falsas. Frequentar algum estabelecimento e conseguir a confiança das pessoas é uma maneira lenta e gradual de obter capacidade de convencer outra pessoa somente pela credibilidade e intimidade confiada ao criminoso; monitorar as fotos e opiniões divulgadas por funcionários de uma empresa ou instituição com fins de espionagem e sabotagem também são meios de praticar a engenharia social. (AVAST, 2020)

2.2 DO GOLPE

Golpe na internet é qualquer ato em que sejam apresentadas informações falsas a alguém para obter qualquer vantagem. É usado para explorar potenciais fragilidades, buscando ludibriar as vítimas e fazê-las exporem informações pessoais ou sensíveis para que possam por em prática algum feito que possa comprometer a segurança da vítima ou de alguma organização. (Cert.br, 2020). Veja no quadro 2 os golpes mais comuns na internet.

Quadro 2. Golpes mais comuns na internet

Furto de identidade	Quando uma pessoa se passa por outra.
Fraude de antecipação de recursos	É a tentativa de induzir uma pessoa a fornecer informações confidenciais ou realizar pagamento adiantado.
Phishing	Tentativa de obter dados pessoais ou financeiros de um usuário pela utilização de meios técnicos e engenharia social.
Pharming	É um tipo específico de phishing que altera o funcionamento do serviço DNS do cliente, redirecionando-o para um site falso.
Boato (Hoax)	São mensagens com conteúdo falso e, em alguns casos, contém códigos maliciosos.

Fonte: CARTILHA DE SEGURANÇA PARA INTERNET (2020)

Nesse trabalho, será realizado um estudo utilizando o phishing. Entretanto, faz-se necessário o entendimento de que existem mais de um método de phishing. Vejamos alguns deles:

Vishing: é a versão do phishing por áudio na internet, onde o criminoso irá buscar fazer a vítima compartilhar informações pessoais, como a identidade ou a conta bancária, que pode ser usada para fazer compras sem que sem que a vítima saiba (AVAST, 2020).

Phishing por e-mail: método que utiliza um e-mail contendo links que redirecionam as vítimas para sites maliciosos ou que contenham algum malware, um programa de computador feito para infectar o computador ou prejudicar de alguma forma a vítima. (AVAST, 2020).

Smishing: método que utiliza SMS, isto é, mensagem de texto. Ela pedirá que a vítima acesse um link ou faça o download de um aplicativo de celular, entretanto isso fará com que o celular faça o download de um malware que passará a roubar informações pessoais da vítima e enviá-las ao atacante (AVAST, 2020).

Phishing nos sites: foco deste trabalho, este método cria falsificações de sites. É enviada à vitima uma cópia idêntica do site, apresentando-se como um ambiente aparentemente confiável, entretanto ao inserir os dados, estes serão furtados pelo atacante (AVAST, 2020).

3 REFERENCIAL METODOLÓGICO

3.1 TIPOS DE PESQUISA

Para cumprir os objetivos desse trabalho, foi feita uma pesquisa indutiva. Isto é, foi feita uma análise de eventos isolados, que são as bases das premissas construídas mais adiante. Para isso, foi utilizado o universo dos cadetes do curso de intendência como grupo de análise. Os cadetes foram expostos a métodos de furto de informação e foram questionados quanto ao ocorrido. A apresentação dos resultados obtidos foi realizada da forma qualitativa, com o objetivo de se conhecer o fenômeno estudado.

3.2 MÉTODOS

3.2.1 Levantamento

Foram feitos testes de êxitos na captura de dados dos cadetes do curso de intendência, tendo por auxílio a ferramenta zphisher no sistema operacional KaliLinux. Com isso, foi ilustrado como um golpe de phishing funciona passo a passo utilizando o quarto método anteriormente citado.

Para que se possa usar o zphisher, é necessária a ferramenta que irá clonar o programa e o endereço URL para o download, ambos pelo terminal do Linux:

Ferramenta de clonagem: esse comando irá instalar a ferramenta “git” que irá se encarregar de instalar o zphisher.

```
$ sudo apt install git
```

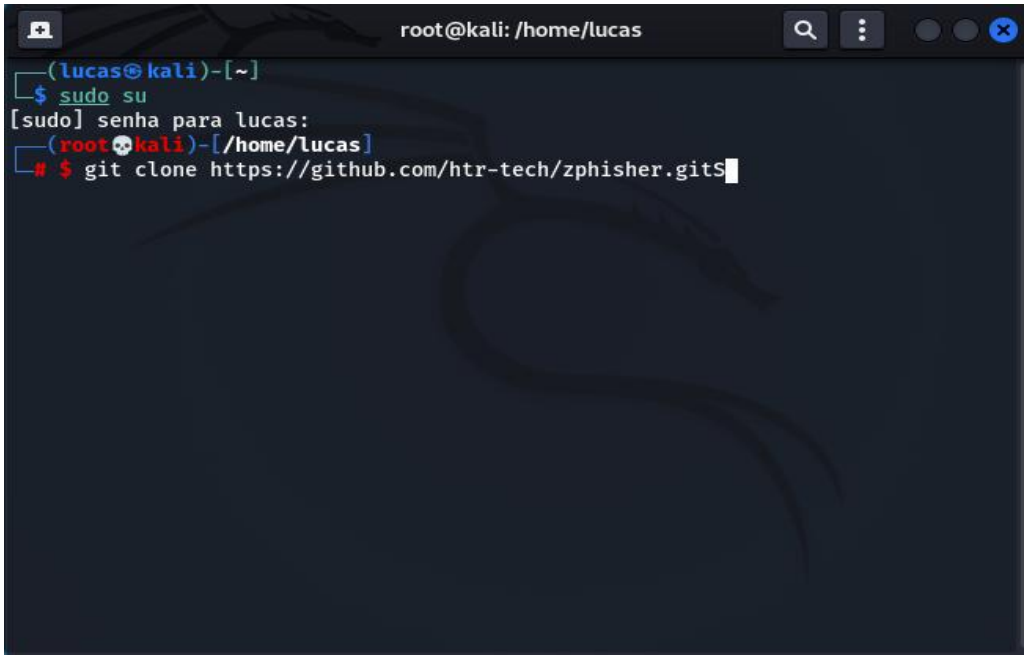
Figura 2 – Instalação do GIT

Fonte: AUTOR (2022)

O segundo passo é instruir o computador aonde está localizado o programa que se quer instalar por meio do endereço URL.

```
$ git clone git://github.com/htr-tech/zphisher.git
```

Figura 3 – Localização de download do zphisher

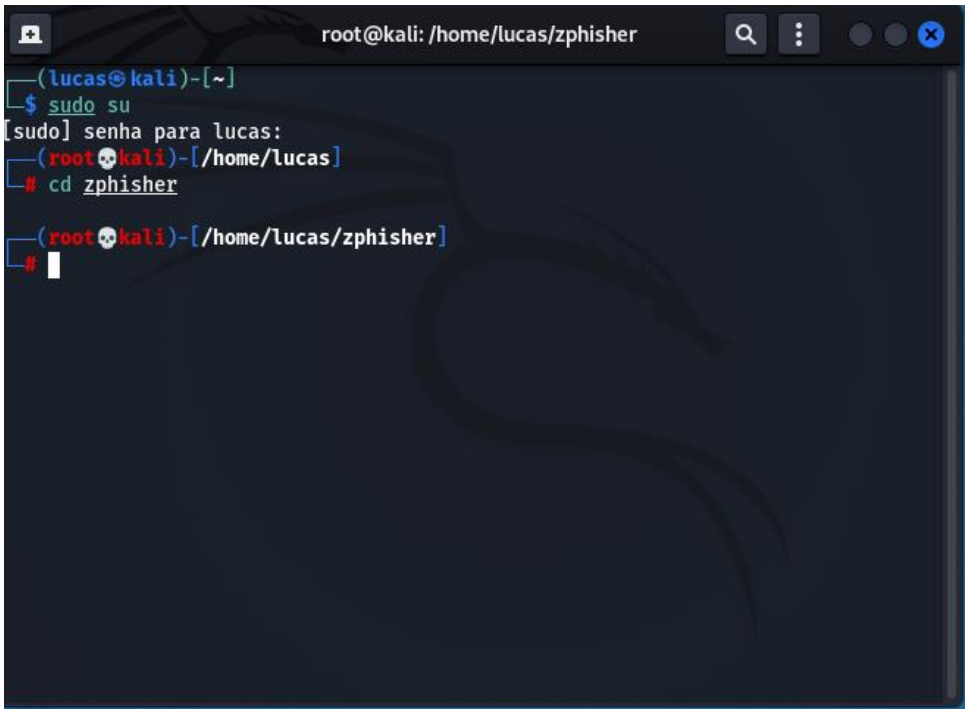


Fonte: AUTOR (2022)

Dados esses dois comandos, estamos prontos para iniciar o programa. Para isso devemos acessar o diretório do zphisher com o seguinte comando:

```
$ cd zphisher
```

Figura 4 – Acesso ao diretório do zphisher

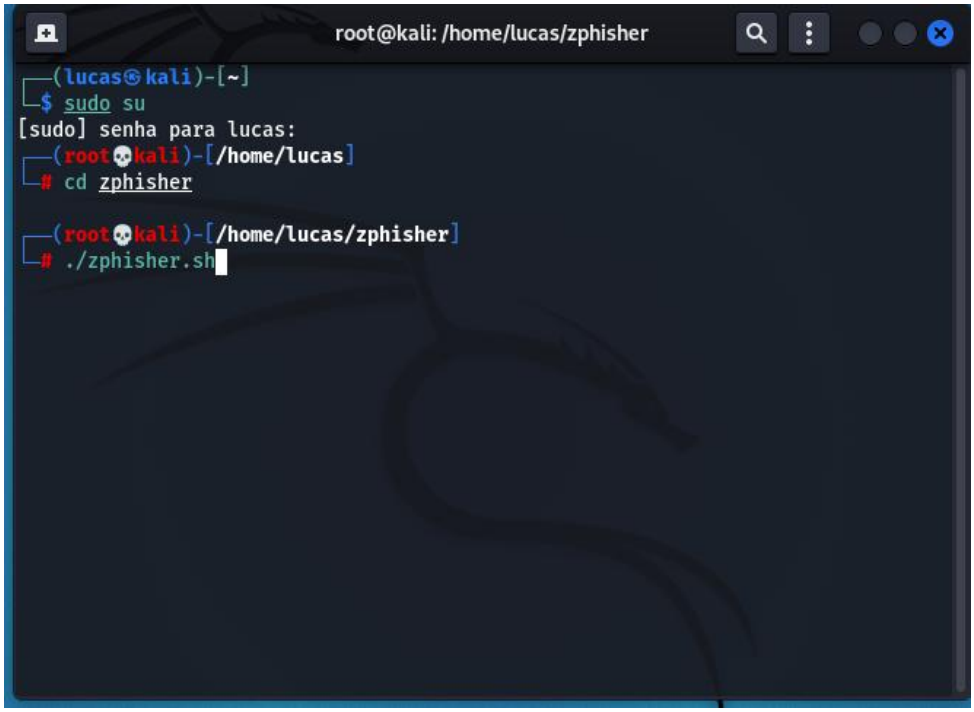


Fonte: AUTOR (2022)

Em seguida, vamos executar o programa com este com este comando:

```
$ ./zphisher.sh
```

Figura 5 – Execução do zphisher



Fonte: AUTOR (2022)

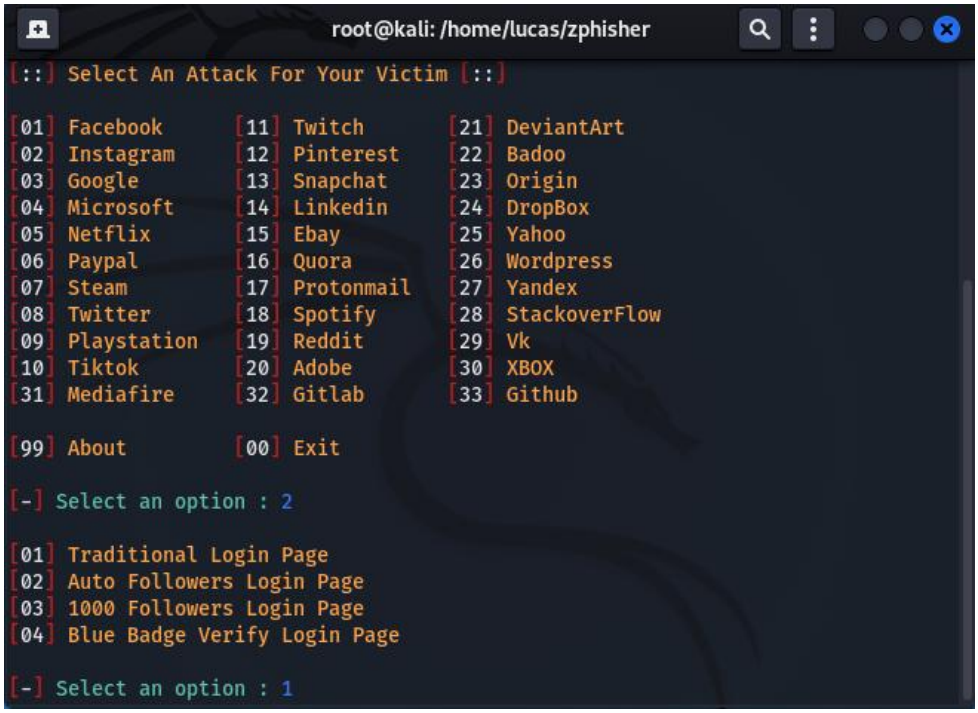
O zphisher, agora iniciado, mostrará uma série de páginas web para clonar.

Figura 6 – Lista de páginas web

Fonte: AUTOR (2022)

A página que será clonada para fins de demonstração será a do facebook, opção 1. Após a escolha, o programa perguntará o método de como se quer capturar as credenciais da vítima. Usaremos o método tradicional de uma página de login comum, isto é, a opção 1:

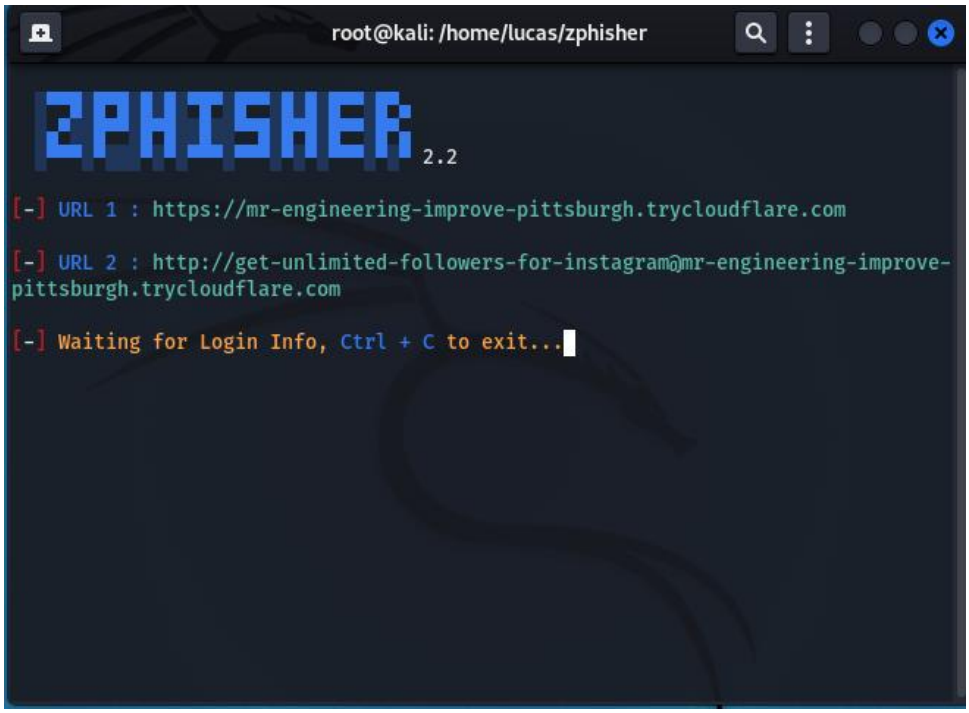
Figura 7 – Login



Fonte: AUTOR (2022)

Na terceira etapa, o zphisher dará três opções: Localhost, Ngrok.io e o Cloudflared. Essas opções nada mais são do que os métodos de como o golpista irá abrir uma conexão entre a sua máquina e a máquina da vítima. É uma maneira de dar acesso à aplicação do servidor local (golpista) através de um link externo. Utilizaremos a opção Cloudflared.

Figura 8 – Conexão com a vítima



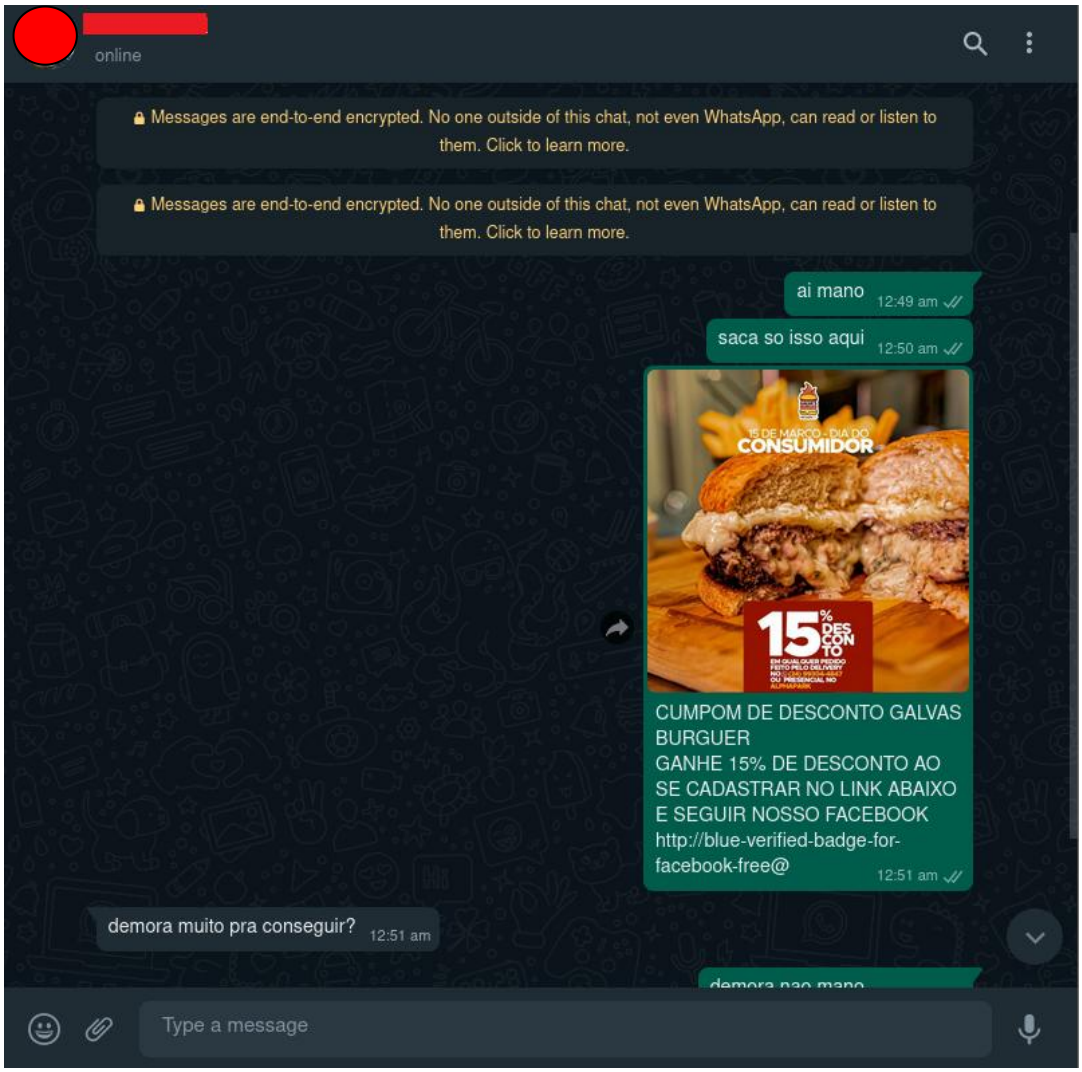
Fonte: AUTOR (2022)

Feitas todas as etapas, o zphisher está pronto e está aguardando a vítima acessar o link que é enviado por e-mail ou em um grupo de mensagem instantânea. É importante notar que assim que o link é acessado, o endereço IP da máquina visitante é registrado pelo programa. Assim que é realizado o login na página, senha e usuário também são capturados e salvos nos arquivos do zphisher. É certo que quando a vítima tentar acessar sua conta, não irá conseguir. Por isso, assim que ela solicita o acesso, o programa redireciona a pessoa para a página original do site, buscando não levantar muitas suspeitas. Uma vez que o atacante possui os dados de acesso à conta da vítima, pode começar a monitorar, roubar ou alterar o que bem entender.

4 RESULTADOS

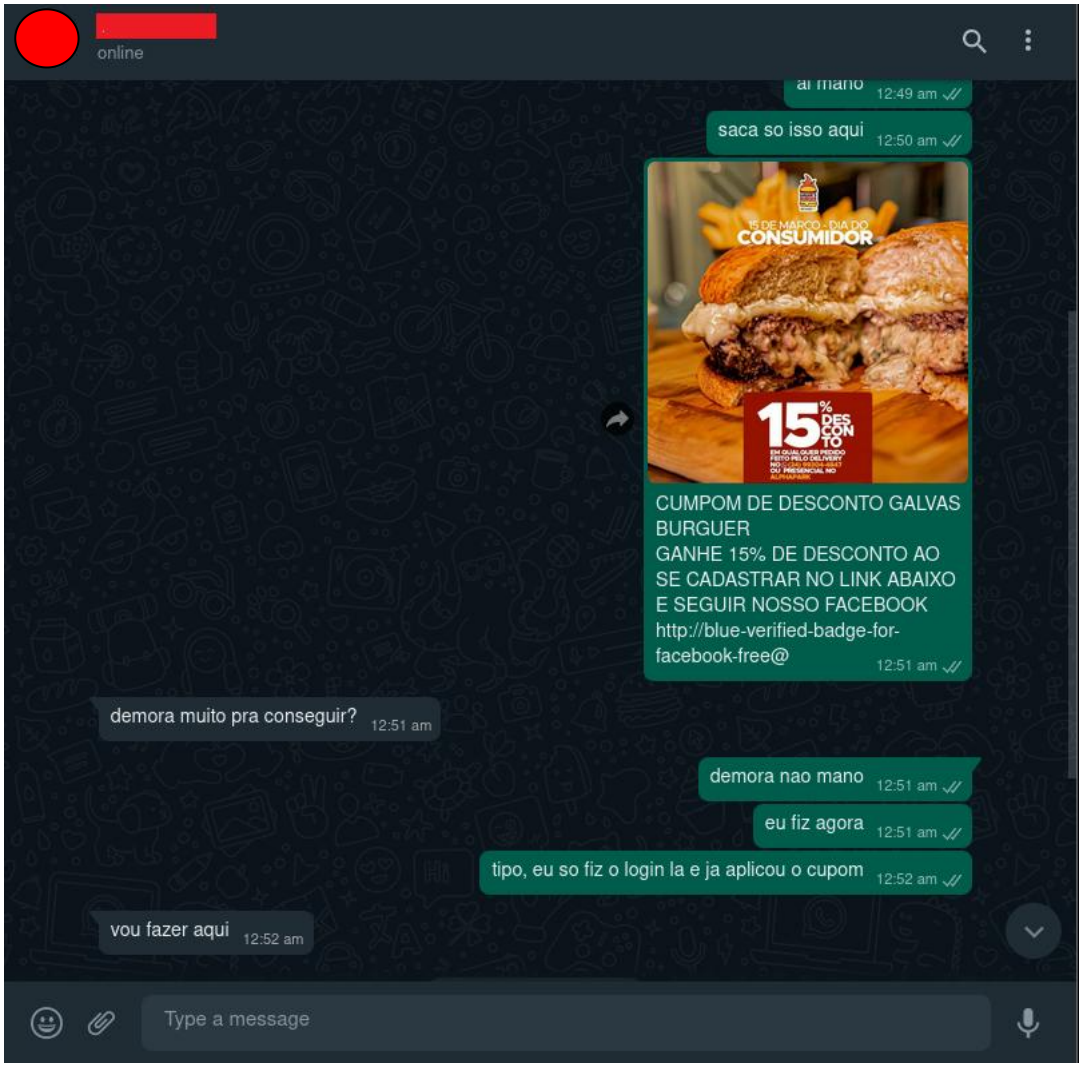
Para o primeiro momento, temos a aproximação do golpista com a vítima. Nesse momento, é construído um contexto amigável para induzir a vítima a acessar o link compartilhado.

Figura 9 – Contato amigável



Fonte: AUTOR (2022)

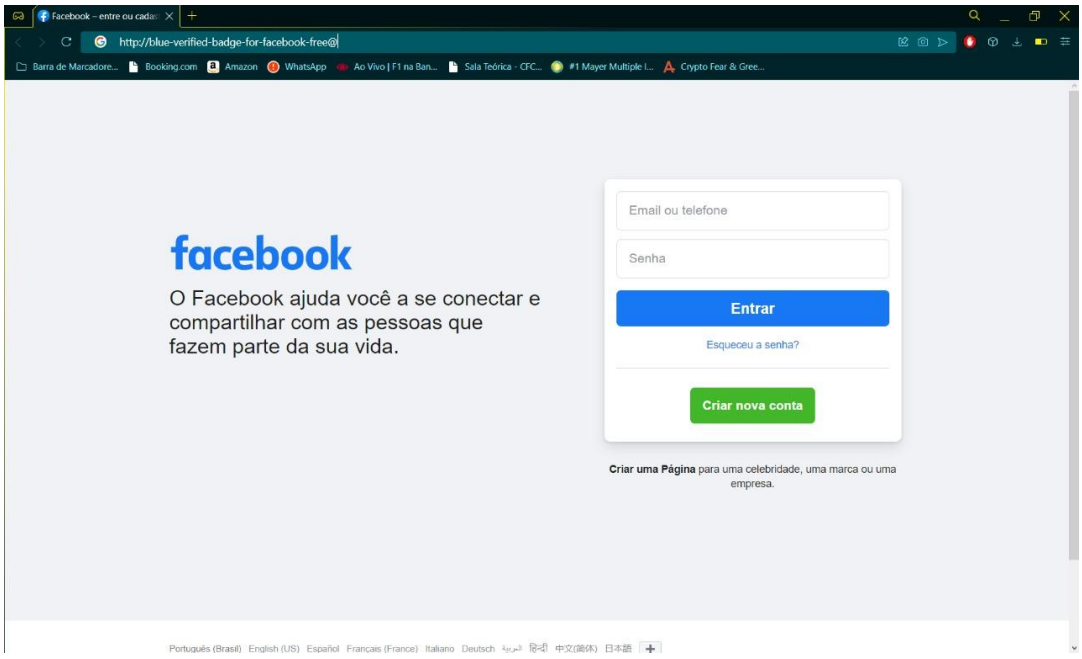
Figura 10 – Contato amigável 2



Fonte: AUTOR (2022)

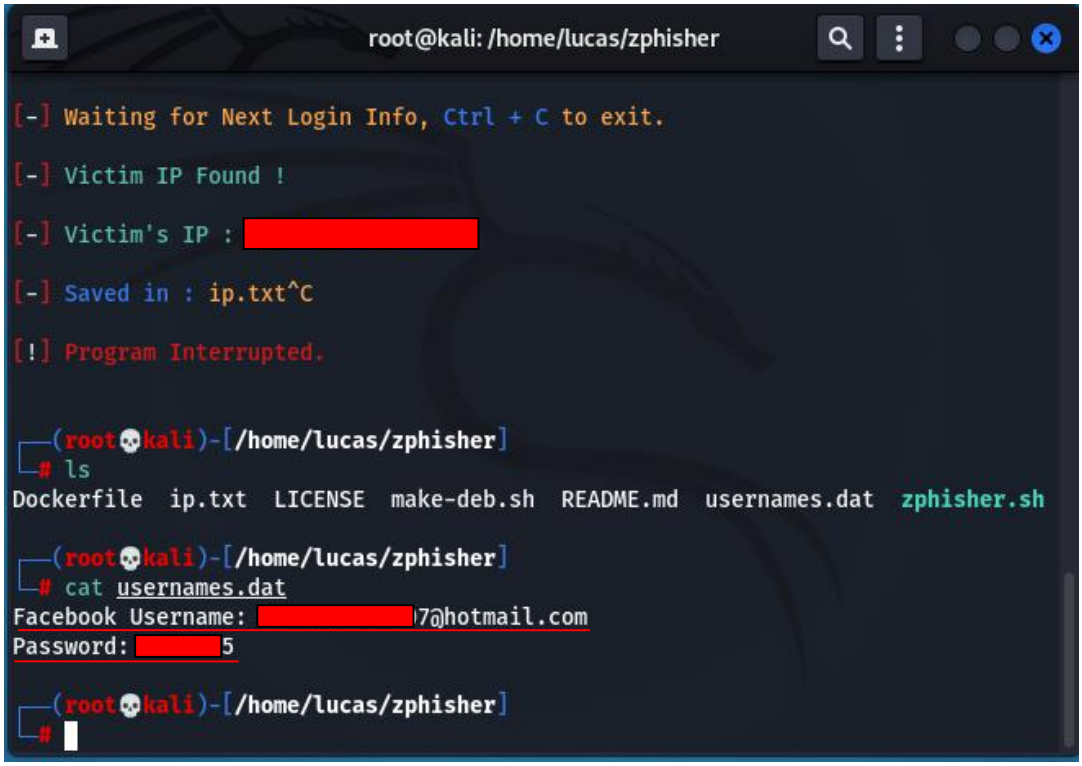
Com o link fornecido, a vítima terá acesso a uma página de login idêntica a original. É nessa fase que, desavisada e sem suspeitar da página, a vítima acaba fornecendo sua credencial á máquina do golpista.Veja na figura abaixo a página fornecida e as credenciais na máquina do golpista:

Figura 11 – Página idêntica á original



Fonte: AUTOR (2022)

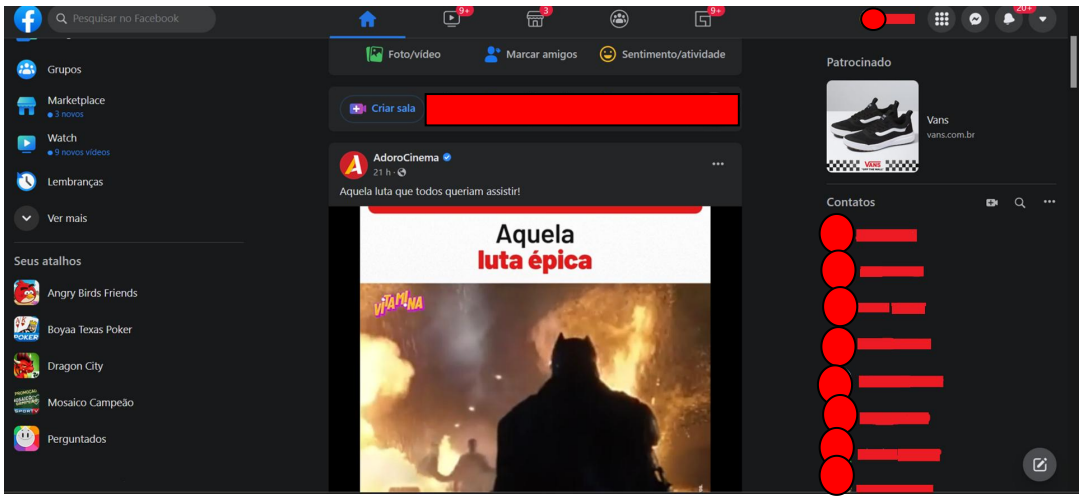
Figura 12 – Credenciais



Fonte: AUTOR (2022)

Após a apanha de dados, pode-se finalmente acessar a rede social da vítima. Observando a imagem abaixo, temos uma rede de contatos, além de fotos que mostram as caracteríscas da vítima que podem ser utilizadas para dar mais credibilidade a um futuro ataque de estelionato, por exemplo.

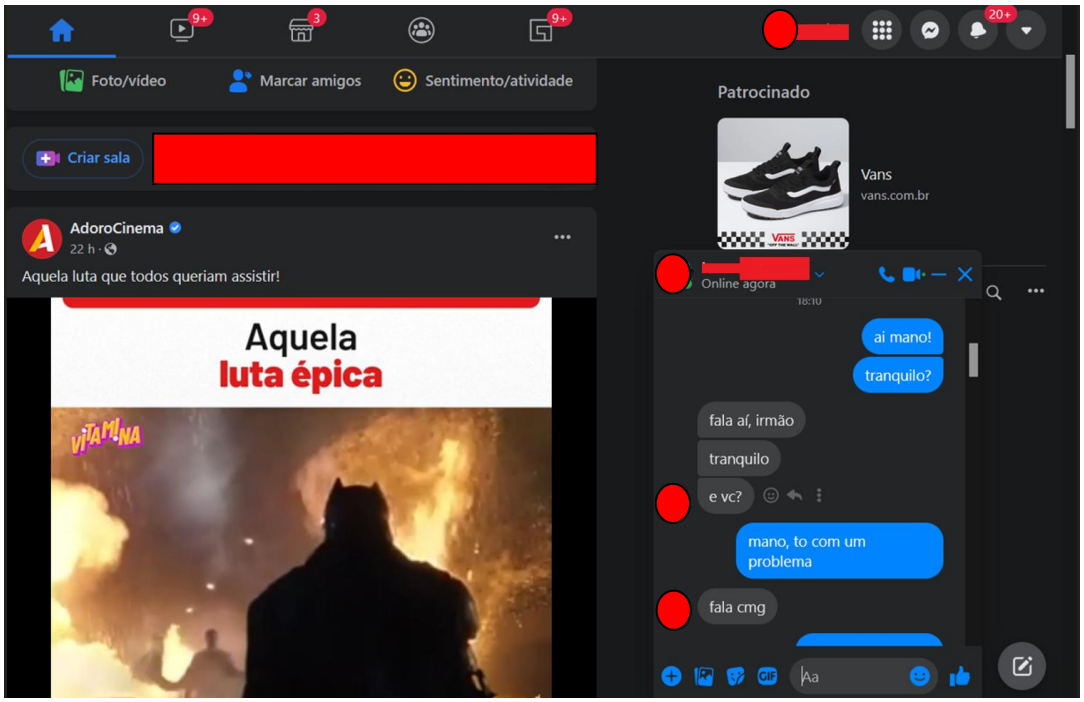
Figura 13 – Acesso a conta da vítima



Fonte: AUTOR (2022)

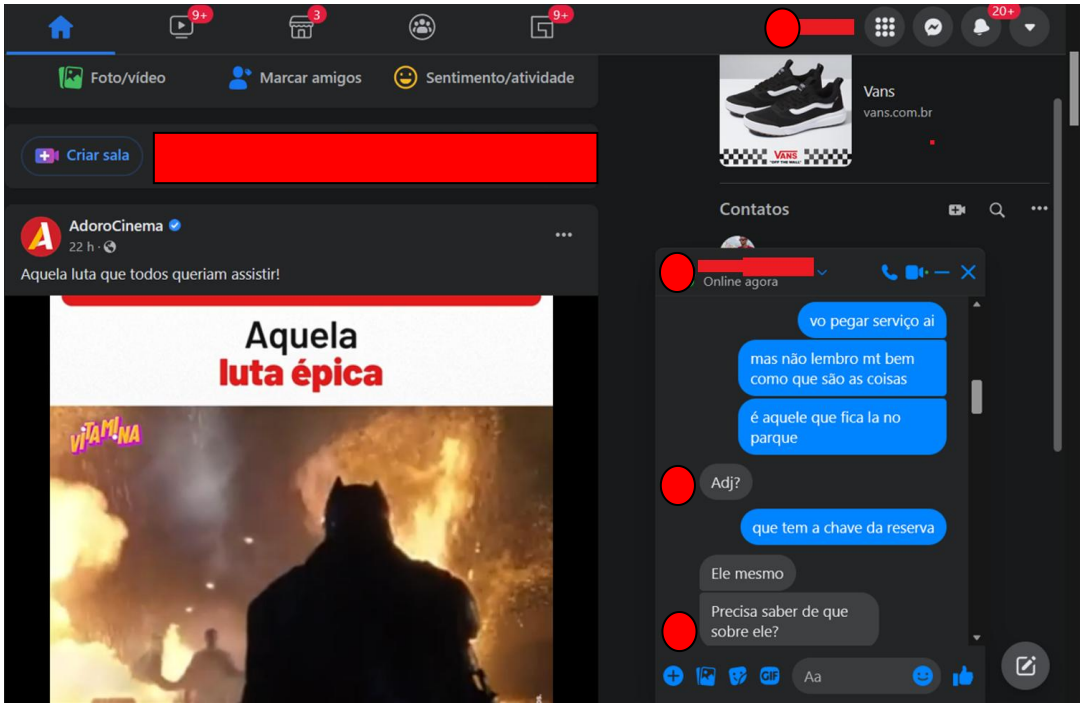
Passando-se pela vítima, é feito um diálogo com um contato qualquer, perguntando informações a respeito do serviço militar que será atendido. Veja:

Figura 14 – Interação com um contato da vítima



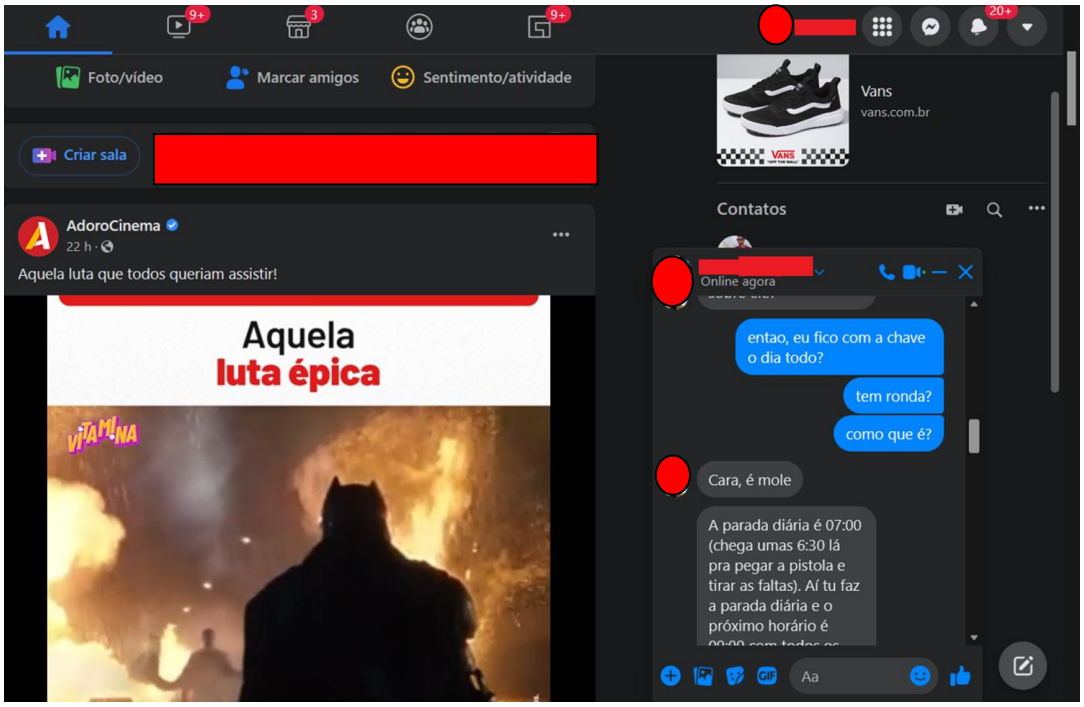
Fonte: AUTOR (2022)

Figura 15 – Captura de informações sensíveis (Fig 1)



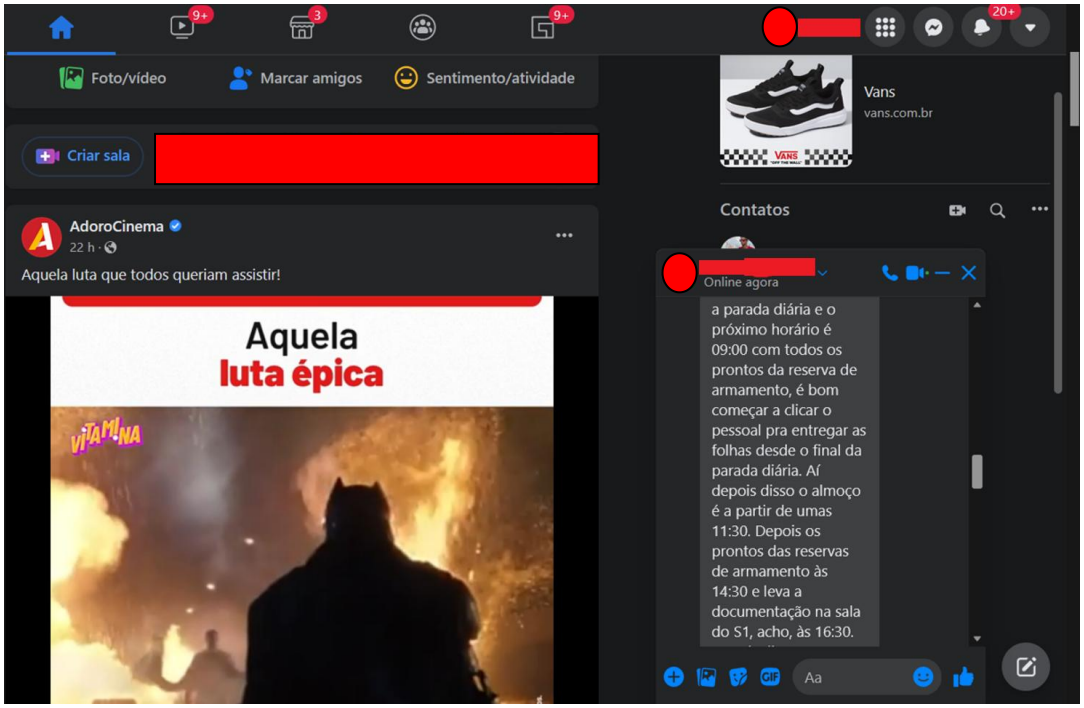
Fonte: AUTOR (2022)

Figura 16 – Captura de informações sensíveis (Fig 2)



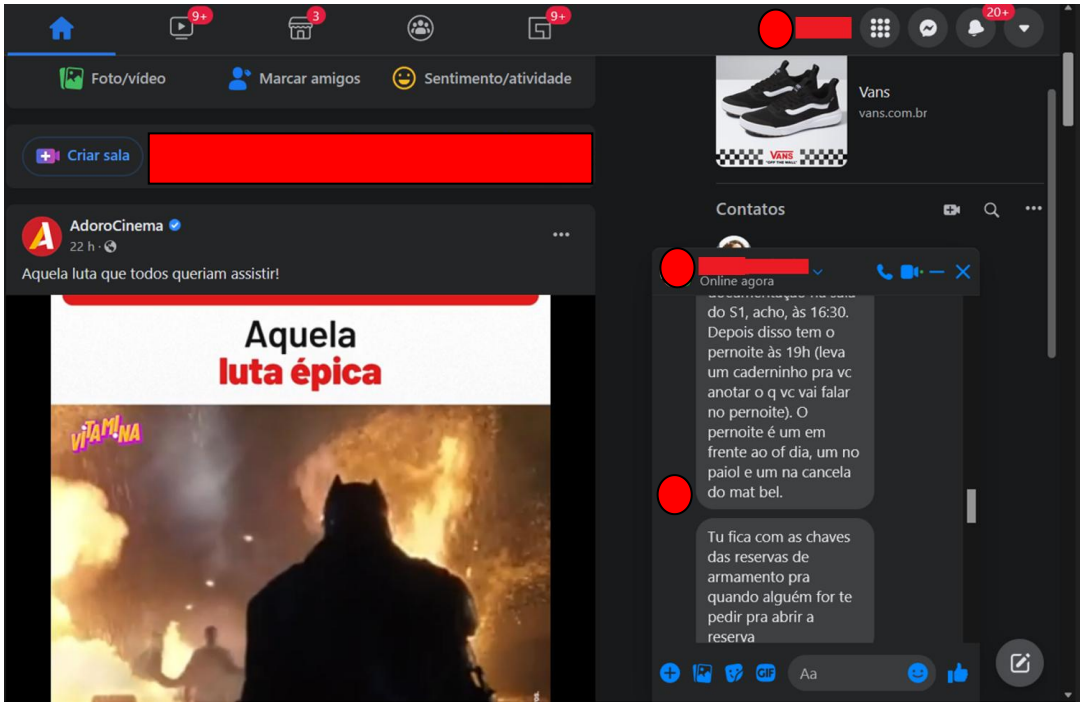
Fonte: AUTOR (2022)

Figura 17 – Captura de informações sensíveis (Fig 3)



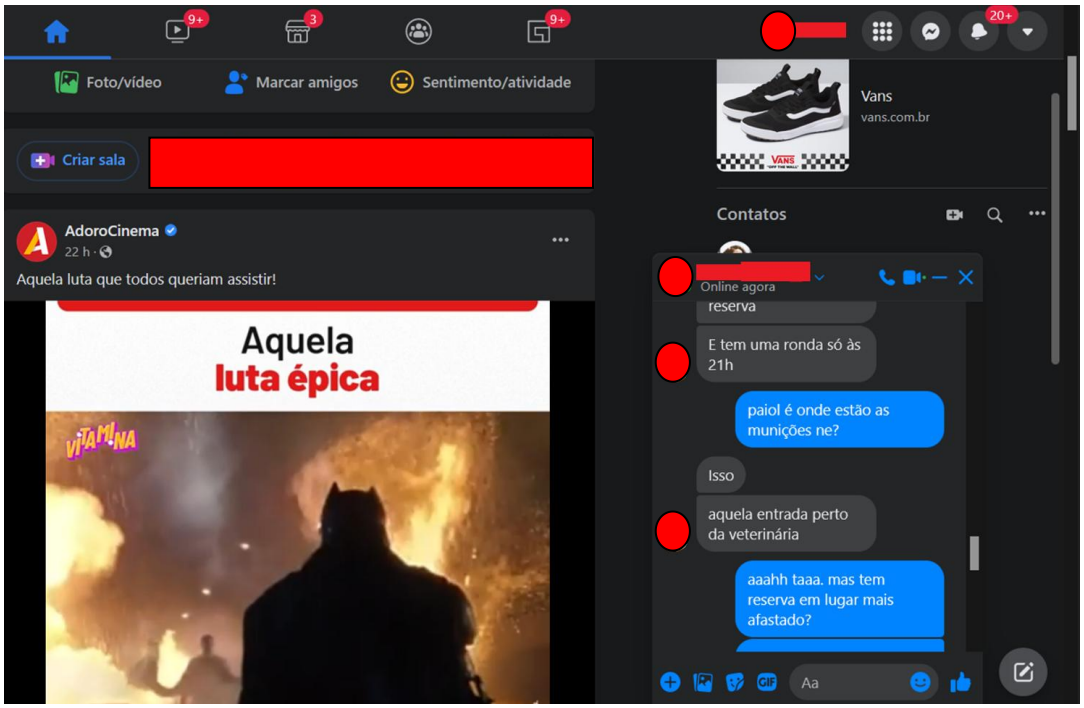
Fonte: AUTOR (2022)

Figura 18 – Captura de informações sensíveis (Fig 4)



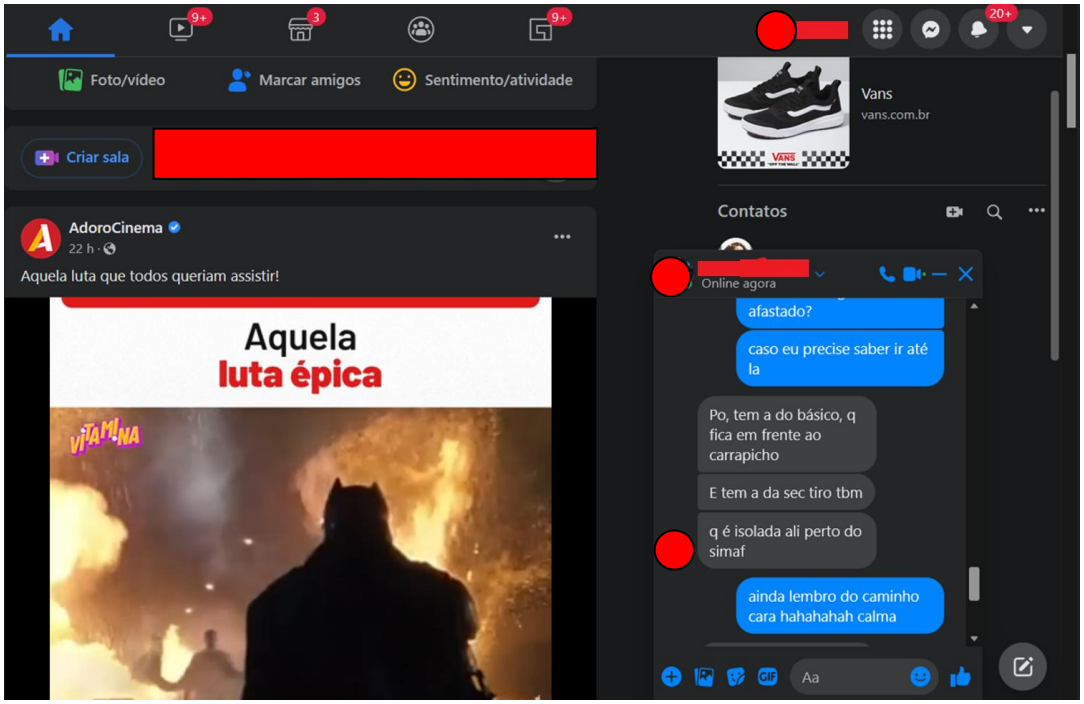
Fonte: AUTOR (2022)

Figura 19 – Captura de informações sensíveis (Fig 5)



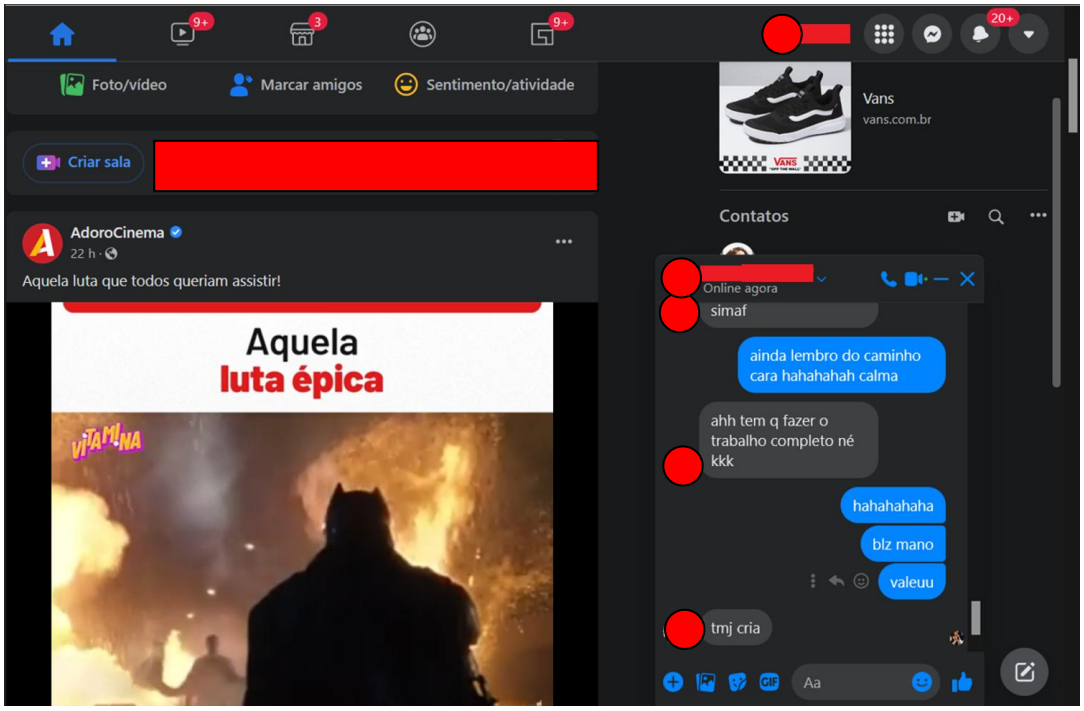
Fonte: AUTOR (2022)

Figura 20 – Captura de informações sensíveis (Fig 6)



Fonte: AUTOR (2022)

Figura 21 – Captura de informações sensíveis (Fig 7)



Fonte: AUTOR (2022)

5 DISCUSSÃO

Nota-se que, tomando o devido cuidado para não produzir suspeitas, não houve resistência ao fornecimento das informações solicitadas. A partir desse ponto, o agente malicioso tem livre escolha do que fazer com os dados coletados que englobam desde espionagem até obtenção de vantagem financeira.

Com facilidade e cuidado em todos os procedimentos feitos até agora, e observando minuciosamente cada etapa do processo, vê-se que qualquer pessoa com uma rápida leitura em sites e guias online, pode preparar, sem muita dificuldade, um golpe de phishing com objetivos que vão desde espionagem, roubo de credenciais e vantagens financeiras. As ferramentas são fáceis de utilizar, além de estar acessível a qualquer pessoa que possua um computador a sua disposição. As redes sociais são um ambiente com rica diversidade de dados, os quais ficam à disposição do agente malicioso para se adequar às suas necessidades.

O objetivo desta pesquisa, além de explicar como funcionamento de um golpe de phishing funciona, foi realizar uma breve análise de como essas informações que são fornecidas diariamente, estão passíveis de serem usadas e comprometer a segurança interna da AMAN e dos cadetes. Bastou um simples diálogo para que fossem fornecidos dados sensíveis da organização militar, os quais põem em situação de risco não só a vida dos cadetes, mas também a vida de funcionários e da família militar.

6 CONSIDERAÇÕES FINAIS

Este trabalho teve como objetivo analisar os riscos á segurança da informação que o uso de forma descuidada de redes sociais, pelos cadetes da AMAN, pode gerar, trazendo riscos não só a eles, mas também a todo o efetivo militar e civil que trabalha e vive dentro da organização militar. Para isso, foi utilizado um estudo de eventos isolados e pesquisa bibliográfica para atingir os objetivos propostos no trabalho.

Através de um golpe de phishing, em ambiente controlado, pôde-se demonstrar como é fácil realizar um roubo de credenciais, mesmo sem a necessidade de elevado conhecimento técnico. Basta que se siga alguns passos e, de imediato, é possível praticar um golpe. Somado a isso, o trabalho da engenharia social aumenta exponencialmente o êxito do golpe, vindo a ser peça chave para o sucesso da ação cibernética, pois é nessa fase que se convence a vítima a fornecer seus dados, sem suspeitas.

As redes sociais são, sem dúvida, um avanço no que tange as relações interpessoais, porém quando usadas de forma segura, isto é, considerando todas as boas práticas de segurança na internet. É necessário lembrar que o phishing é um método muito eficaz quando somado a uma boa engenharia social, buscando alcançar um único objetivo: explorar vulnerabilidades para obter vantagens.

Para oportunidade de pesquisa futura, é possível que se elabore uma cartilha de segurança do uso de redes social em ambiente militar, em complemento à cartilha de segurança da internet, trazendo boas práticas alinhadas com o contexto atual em que a população tanto civil quanto militar se encontram.

REFERÊNCIAS

ARPANET. **MDN Web Docs**, 2021. Dispinível em: <https://developer.mozilla.org/pt-BR/docs/Glossary/Arpanet>. Acesso em: 13 de jul. de 2021.

A TCP/IP Tutorial. **Datatracker ietf**, 1991. Disponível em: <https://datatracker.ietf.org/doc/html/rfc1180#page-2>. Acesso em: 13 de jul. de 2021.

BANCO PAN**. O que é phishing**: veja como ele pode te prejudicar e como se proteger. Disponível em: **<**https://www.bancopan.com.br/blog/publicacoes/o-que-e-phishing-e-como-se-proteger.htm**> .** Acesso em: 08 mar. 2022.

BELCIC, I. **O guia essencial sobre phishing:** Como funciona e como se proteger. Avast, 2020. Disponível em: <https://www.avast.com/pt-br/c-phishing>. Acesso em: 06 de mar. de 2022.

CERT.BR. **CARTILHA DE SEGURANÇA PARA INTERNET**, 2012. Dispinível em: <https://cartilha.cert.br/>. Acesso em: 13 de jul. de 2021.

COMER, D. E. **Internetworking with TCP/IP.** 4. ed. New Jersey: Prentice Hall, 2000. v. 1: principles, protocols, and architectures. 750 p. 31, 34, 38, 40

FILIPPETTI, M. A. **CCNA 6.0 guia completo de estudo**. 2. ed. Rio de Janeiro: Alta Books, 2018.

JORGE, P. **Fraudes na Internet:** Uma proposta de identificação e prevenção. Tese (Bacharel em Sistemas de Informação) - Curso de Sistemas de Informações, Faculdade Santa Maria. Recife, 2007.

MORENO, D. **Introdução ao Pentest**. São Paulo: Novatec Editora, 2015.

MOTA FILHO, J. E. **Análise de tráfego em redes TCP/IP:** utilize tcpdump na análise de tráfego em qualquer sistema operacional. São Paulo: Novatec Editora, 2013.

NEGUS, C. Começando com o Linux. In: ***Linux a bíblia****: o mais abrangente e definitivo guia sobre linux,* Alta books editora, 2014.

SENADO FEDERAL. **Lei nº 12.737/2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 13 de nov. de 2021.

TANENBAUM, A.; WETHERALL, D. **Redes de Computadores**. 5. ed. São Paulo: Pearson, 2011.

KASPERSKY. **Como evitar riscos à segurança em redes Wi-Fi públicas.** Disponível em: <https://www.kaspersky.com.br/resource-center/preemptive-safety/public-wifi-risks>. Acesso em: 06 de mar. de 2022.

VIENAZINDYTE, I. **Os perigos das redes sociais**. NordVPN, 2020. Disponível em: < https://nordvpn.com/pt-br/blog/os-perigos-das-redes-sociais/>. Acesso em: 08 de mar. de 2022.

QUEIROZ, Mariana Pessoa de.**Phishing e redes sociais:** um estudo de caso. Orientador: Profa. Dra. Maria Cristina Aranda Aranda. 2019. 87 f. TCC (Graduação) – Curso de Segurança em sistemas de informação, Faculdade de Tecnologia de Americana, Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2019. Disponível em: <http://ric.cps.sp.gov.br/bitstream/123456789/3780/1/20191S_QUEIROZMarianaPessoade_OD0669.pdf>. Acesso em: 14 abr. 2022.

Apêndice A - **AUTORIZAÇÃO DE AÇÃO CIBERNÉTICA**

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
ACADEMIA MILITAR DAS AGULHAS NEGRAS
(Academia Real Militar/1811)

AUTORIZAÇÃO DE AÇÃO CIBERNÉTICA

Eu, **FILIPE** ALVES DE **SOUSA**, Cadete do Serviço de Intendência, IDT 070036455-7, autorizo, para fins de pesquisa acadêmica, que o Cad LUCAS **FERNANDO** PEÑA FARIAS, do 4º ano do Serviço de Intendência da Academia Militar das Agulhas Negras, IDT 020764697-7, realize uma ação cibernética à minha pessoa.

RESENDE-RJ, 30 de novembro de 2021.

Cad **FILIPE** ALVES DE **SOUSA**
Idt 070036455-7

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
ACADEMIA MILITAR DAS AGULHAS NEGRAS
(Academia Real Militar/1811)

AUTORIZAÇÃO DE AÇÃO CIBERNÉTICA

Eu, DANIEL **COSTA ALVES**, Cadete do Serviço de Intendência, IDT 100061735-5, autorizo, para fins de pesquisa acadêmica, que o Cad LUCAS **FERNANDO** PEÑA FARIAS, do 4º ano do Serviço de Intendência da Academia Militar das Agulhas Negras, IDT 020764697-7, realize uma ação cibernética à minha pessoa.

RESENDE-RJ, 30 de novembro de 2021.

Cad DANIEL **COSTA ALVES**
Idt 100061735-5

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
ACADEMIA MILITAR DAS AGULHAS NEGRAS
(Academia Real Militar/1811)

AUTORIZAÇÃO DE AÇÃO CIBERNÉTICA

Eu, **LUCAS MACHADO** VAZ FEITOSA, Cadete do Serviço de Intendência, IDT 020765847-7, autorizo, para fins de pesquisa acadêmica, que o Cad LUCAS **FERNANDO** PEÑA FARIAS, do 4º ano do Serviço de Intendência da Academia Militar das Agulhas Negras, IDT 020764697-7, realize uma ação cibernética à minha pessoa.

RESENDE-RJ, 30 de novembro de 2021.

Cad **LUCAS MACHADO** VAZ FEITOSA
Idt 020765847-7