REVISTA ELETRÔNICA AMPLAMENTE
v.2, n.3 jul./ set. 2023 DOI: 10.47538/RA-2023.V2N3
ISSN: 2965-0003

O NAMORO DO "MATUTO" COM A PROFESSORA DULCE CÉLIA ALMEIDA RAMOS

Ricardo Santos David
USP - Universidade de São Paulo.
http://lattes.cnpq.br/8508122200950572
https://orcid.org/0000-0001-5850-0057
E-mail: ricardosdavid@hotmail.com.br

DOI-Geral: http://dx.doi.org/10.47538/RA-2023.V2N3
DOI-Individual: http://dx.doi.org/10.47538/RA-2023.V2N3-35

RESUMO: O presente artigo explora a complexidade dos crimes digitais e suas implicações através de uma abordagem metodológica que combina levantamentos bibliográficos e a demonstração prática da clonagem de um site. A análise é contextualizada com base no romance "o namoro do matuto com a professora", onde a acadêmica respeitada, Dulce, instrui o caipira, "Matuto", sobre crimes digitais, como clonagem de cartões de crédito, sites e rastreamento de IP. O estudo segue um método que envolve, primeiramente, um levantamento bibliográfico detalhado através de pesquisas em sites especializados, artigos e publicações relacionadas. Em seguida, a ferramenta SET - Social-Engineer Toolkit, é utilizada como recurso prático e simbólico para representar o conhecimento que Dulce transmite ao "Matuto", demonstrando de forma vívida a facilidade com que plataformas digitais podem ser manipuladas. Este artigo destaca a necessidade da abordagem multidisciplinar e da educação constante de usuários e potenciais criminosos frente aos desafios e responsabilidades do cenário digital contemporâneo.

PALAVRAS-CHAVE: Crimes digitais. Segurança Digital. Clonagem de Sites.

THE COURTSHIP OF "MATUTO" WITH PROFESSOR DULCE CELIA ALMEIDA RAMOS

ABSTRACT: The present article explores the complexity of digital crimes and their implications through a methodological approach that combines bibliographic surveys and the practical demonstration of website cloning. The analysis is contextualized based on the novel "o namoro do matuto com a professora", where the respected academic, Dulce, instructs the countryman, "Matuto", about digital crimes, such as credit card cloning, website cloning, and IP tracking. The study follows a path that involves, initially, a detailed bibliographical survey through research on specialized websites, articles, and related publications. Then, the SET - Social-Engineer Toolkit, is used as a practical and symbolic resource to represent the knowledge that Dulce transmits to "Matuto", vividly demonstrating how easily digital platforms can be manipulated. This article highlights the need for a multidisciplinary approach and the constant education of users and potential criminals facing the challenges and responsibilities of the contemporary digital scenario

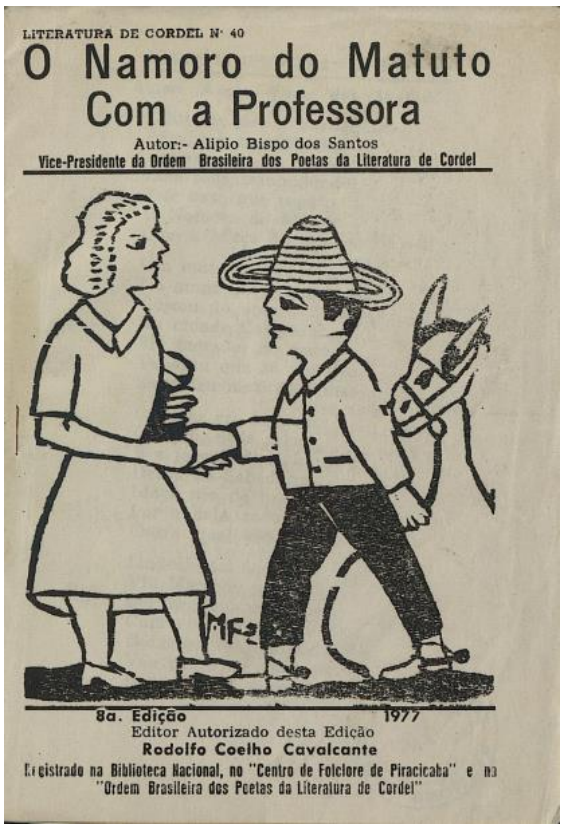
KEYWORDS: Digital Crimes. Digital Security. Website Cloning.

REVISTA ELETRÔNICA AMPLAMENTE
v.2, n.3 jul./ set. 2023 DOI: 10.47538/RA-2023.V2N3
ISSN: 2965-0003

INTRODUÇÃO

Baseado no cordel de Santos (1977), "o namoro do matuto com a professora", a hitória introdutória do presente artigo é da eminente Professora Dulce Célia Almeida Ramos, uma aclamada acadêmica com mestrado, doutorado e pós-doutorado em Literatura pela Universidade de São Paulo. Apesar sua respeitável posição social, a Professora Dulce se vê envolvida em um relacionamento incomum com um caipira peculiar conhecido como "Matuto", de acordo com Ribeiro (2019) o termo "Matuto" é usado principalmente na região nordeste do Brasil para descrever um indivíduo que vive no campo, conhecedor dos costumes e modos de vida campestres. Este termo também é usado para descrever alguém que é perspicaz, astuto e esperto, geralmente alguém que está imerso em seus próprios pensamentos.

Figura 1 - Capa do cordel "O namoro do matuto com a professor"



Fonte: Biblioteca Virtual Cordel

Como seus mundos são amplamente divergentes, ainda que interligados uma vez que Dulce ministra aulas de literatura na cidade do "Matuto", a professora se apaixona e

REVISTA ELETRÔNICA AMPLAMENTE
v.2, n.3 jul./ set. 2023 DOI: 10.47538/RA-2023.V2N3
ISSN: 2965-0003

rendendo-se a essa nova paixão, ela embarca na tarefa inédita de transmitir a "Matuto" um tipo peculiar de sabedoria - conhecimento sobre crimes digitais como clonagem de cartão de crédito, rastreamento de IP de computadores e celulares, escutas telefônicas e vários outros métodos de transmissão de conversas na televisão.

Por meio desta saga incomum da professora e o "Matuto" será lançada luz sobre a natureza multifacetada das fraudes de cartão de crédito e crimes digitais. A história caminha por uma linha tênue, equilibrando-se na cúspide da legalidade, moralidade e ambiguidade ética. Simultaneamente, oferece uma reflexão sobre as perspectivas de Dulce sobre o Espiritismo, alma, a reencarnação e o Karma, desvendando assim como essas crenças se infiltram em sua abordagem em relação aos crimes digitais e as interações com matuto.

O artigo avança, apoiando-se na análise da narrativa formada pela relação única de Dulce e Matuto e nas informações compartilhadas entre eles. Incorporada com uma avaliação profunda da literatura atual convergindo sobre crimes digitais, examinamos ainda mais suas implicações. Resumidamente, o objetivo deste artigo, é apresentar percepções valiosas sobre a natureza complexa dos crimes digitais suas implicações.

BREVE HISTÓRICO DOS CRIMES VIRTUAIS

A chegada dos computadores e das redes internacionais interligadas proporcionou maior conveniência em nossas vidas cotidianas. Atividades demoradas do passado agora são executadas em questão de instantes. Um computador é um aparelho que armazena e processa informações de acordo com instruções preestabelecidas (FRAGOMENI, 1987). Ao longo da história, os seres humanos têm buscado criar objetos e ferramentas que simplifiquem as tarefas do dia a dia e as tornem mais agradáveis. Uma das transformações significativas pelas quais a sociedade passou foi a Revolução Industrial, que modificou o cenário do mundo contemporâneo, alterou o estilo de vida da população e impulsionou a migração do campo para as áreas urbanas, iniciando-se no Reino Unido por volta do século XVIII. Provavelmente isso ocorreu devido à presença de abundantes jazidas de carvão no subsolo inglês, recurso energético fundamental para as máquinas da época (SCHWAB; DAVIS, 2019).

REVISTA ELETRÔNICA AMPLAMENTE
v.2, n.3 jul./ set. 2023 DOI: 10.47538/RA-2023.V2N3
ISSN: 2965-0003

A ascensão das máquinas, o desenvolvimento das cidades, a passagem do trabalho manual para o controle de equipamentos, o aumento da produção fabril e a criação de novas invenções, tais como navios e locomotivas movidos a vapor, aceleraram o transporte de mercadorias e matérias-primas. Com o tempo, inventores inovadores começaram a influenciar a maneira como percebemos o mundo. Entre as grandes invenções ao longo da história, destacam-se a fotografia (1839), o telefone (1876), a iluminação elétrica (1879) e a televisão (1924), entre muitas outras (BENTES, 2019).

O ENIAC, lançado em 1946, marcou o advento do primeiro computador digital eletrônico. A sigla representa "Eletronic Numerical Integrator and Calculator" e sua criação foi liderada pelo exército norte-americano. Com um peso colossal de aproximadamente 30 toneladas e ocupando cerca de 140 metros quadrados, o ENIAC simbolizou um marco na história da computação (CRESPO, 2011).

A evolução tecnológica continuou com a Xerox, que introduziu em 1981 o primeiro computador com interface gráfica e mouse. Logo em seguida, em 1982, a Intel lançou o primeiro computador pessoal 286. Desde os primórdios da computação até os tempos atuais, a sociedade tem experimentado transformações constantes, migrando dos registros em cavernas para o uso de papel, da escrita com penas e tinta para a codificação Morse, e da troca de e-mails para a realização de videoconferências (PECK, 2002).

No meio dessa revolução, a internet emergiu na década de 1960. Por volta de 1996, várias universidades se uniram para desenvolver a ARPANET (Advanced Research Projects Administration - Administração de Projetos e Pesquisas Avançados). Inicialmente concebida como resposta a necessidades militares, devido ao contexto da Guerra Fria, a internet rapidamente evoluiu (CRESPO, 2011).

Conforme a definição de Strasser; De Oliveira (2019), a internet é um meio que possibilita a troca de correspondências, arquivos e ideias, comunicação em tempo real, pesquisa documental, bem como a utilização de serviços e aquisição de produtos. Esse progresso contínuo ilustra a incrível jornada da sociedade em direção a uma interconectividade global sem precedentes.

A Internet constitui uma rede interligada de computadores, que por sua vez são agrupados em redes menores. Esses computadores se comunicam através de endereços

REVISTA ELETRÔNICA AMPLAMENTE
v.2, n.3 jul./ set. 2023 DOI: 10.47538/RA-2023.V2N3
ISSN: 2965-0003

lógicos conhecidos como endereços IP, viabilizando a troca de diversas informações. Entretanto, essa troca de informações também gera desafios, uma vez que uma vasta quantidade de dados pessoais fica acessível na rede, ficando exposta a inúmeros indivíduos que possuem acesso à internet. Além disso, essa disponibilidade de informações pessoais pode ser explorada por indivíduos mal-intencionados em busca de cometer crimes virtuais (INELLAS, 2004).

Lévy, em sua obra "Cyberdémocracie: Essai de Philosophie Politique", já havia observado o aumento progressivo do uso da internet pelas pessoas e antecipado um crescimento significativo desse uso devido ao contínuo desenvolvimento de novas tecnologias, interfaces de comunicação sem fio e a integração de dispositivos portáteis. A previsão de Lévy se confirmou, uma vez que a internet atualmente é acessível em diversas formas por meio de dispositivos portáteis. Muitas pessoas dedicam considerável tempo navegando na internet, muitas vezes mais do que interagindo com o mundo real. Isso abrange atividades como mídias sociais, leitura de livros, videoconferências, entre outras. A rede global de computadores é, essencialmente, uma rede global de indivíduos, e nesse ambiente virtual surgem relações jurídicas que demandam soluções do Direito (LEMOS; LEVY, 2010).

Para lidar com as complexidades e litígios que emergem nesse ambiente, o Direito desempenha um papel crucial. O Direito, como solução prática de planejamento e estratégia, necessita ser desenvolvido em colaboração com uma equipe que esteja em contato direto com as demandas em constante evolução da sociedade. A adaptação do Direito às demandas e aspirações da sociedade é uma tarefa desafiadora, especialmente em um cenário de transformações aceleradas (PINHEIRO, 2010).

Os primeiros delitos de informática surgiram nos anos 70, frequentemente perpetrados por especialistas em tecnologia. Eles visavam contornar sistemas de segurança de empresas, com foco principalmente nas instituições financeiras. Hoje, o perfil dos infratores mudou substancialmente desde aquela época.

Pessoas com conhecimento não tão especializado, mas que têm acesso à internet, têm a capacidade de cometer crimes de informática. O usuário comum tem agora um

REVISTA ELETRÔNICA AMPLAMENTE
v.2, n.3 jul./ set. 2023 DOI: 10.47538/RA-2023.V2N3
ISSN: 2965-0003

entendimento mais amplo sobre o uso de computadores e tecnologias voltadas para a internet (CASTRO, 2003).

CONCEITO DE CIBERCRIME SEU AUMENTO

Crimes digitais ou cibernéticos consistem em ações delituosas que ocorrem no contexto virtual, utilizando a informática de maneira geral. Segundo Rocha (2017, p. 13), crimes cibernéticos se referem a "comportamentos ilícitos executados por meio de dispositivos tecnológicos (...) dado que essas ações ocorrem em um ambiente virtual."

Rosa (2002) oferece uma definição abrangente do conceito de crimes de informática, descrevendo-o como:

> [...] É a conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. o Crime de Informática é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. Assim, o Crime de Informática pressupõe does elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão 5. Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc. (ROSA, 2002, p. 53-54).

Diante do aumento dos novos tipos de fraudes, torna-se essencial a implementação de medidas jurídicas no sistema legal do Brasil que possam efetivamente sancionar os crimes ocorridos no meio virtual. Além disso, é necessário reforçar os esforços em investigações e estabelecer penalidades mais rigorosas, de modo a coibir tais infratores e desencorajar suas práticas. A falta de punições efetivas e as lacunas nas investigações relacionadas a delitos virtuais persistem, como ressalta Alves em sua obra "Crimes Digitais" (2020). Muitas vezes, os crimes cometidos no meio virtual não deixam rastros

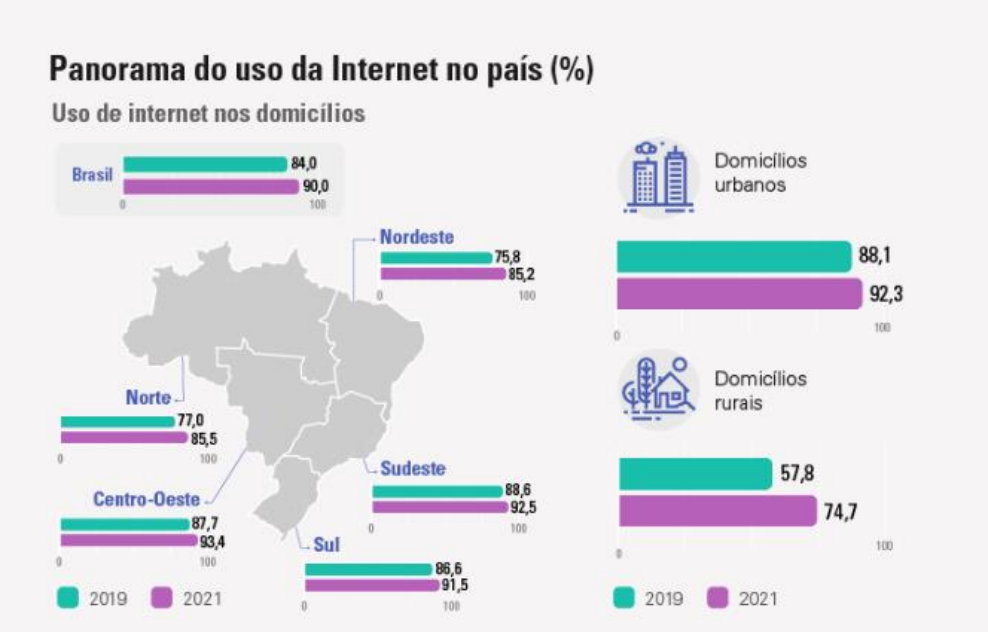
REVISTA ELETRÔNICA AMPLAMENTE
v.2, n.3 jul./ set. 2023 DOI: 10.47538/RA-2023.V2N3
ISSN: 2965-0003

suficientes para identificar os autores, destacando a fragilidade de nossa legislação nesse âmbito.

O aumento considerável no número de acessos e transações pela internet, bem como o aumento do tempo de interação em redes sociais e visitas a sites não seguros, têm propiciado um terreno fértil para uma série de golpes. Um exemplo é a clonagem do aplicativo de mensagens WhatsApp, que só em 2020 resultou em mais de 05 milhões de contas clonadas. No Brasil, somente em 2021, mais de 150 milhões de indivíduos foram afetados por golpes como phishing, que ilude as vítimas por meio de sites e aplicativos falsos. Essas estatísticas são apresentadas pelo DFNDR - LAB, um Laboratório Especializado em Cibersegurança da Psafe.

Com um número cada vez maior de usuários conectados à internet e uma enorme quantidade de informações circulando diariamente, os criminosos passaram a realizar ataques frequentes contra os internautas. Em 2021, o percentual de domicílios com acesso à internet já atingia 90,0%, de acordo com dados do Instituto Brasileiro de Geografia e Estatística (IBGE), conforme ilustrado no gráfico a seguir:

Gráfico 1: Quantidade de domincílios que usam Internet



Fonte: IBGE, 2021

Operando nas sombras, os cibercriminosos continuam sua busca incessante por roubo e apropriação indevida de dados pessoais, perpetrando seus delitos.

REVISTA ELETRÔNICA AMPLAMENTE
v.2, n.3 jul./ set. 2023 DOI: 10.47538/RA-2023.V2N3
ISSN: 2965-0003

De acordo com os registros da plataforma Consumidor.gov.br, o número de consumidores cujas informações pessoais ou financeiras foram consultadas, coletadas, divulgadas ou compartilhadas sem consentimento mais do que dobrou em comparação com o mesmo período do ano anterior.

Conforme Corrêa (2002, p. 42) enfatiza, a internet se apresenta como um campo vasto de informações inestimáveis, o que a torna altamente atrativa para ataques. O ambiente de fácil acesso, repleto de possibilidades e com uma extensa base de usuários que recorrem à internet diariamente, não apenas para entretenimento, mas também para trabalho e atividades acadêmicas, bem como transações financeiras, está mais ativo do que nunca. Isso se intensificou durante a pandemia de Covid-19, quando milhões de brasileiros se viram isolados e recorreram aos meios remotos de atendimento em todas as esferas, resultando no compartilhamento de informações pessoais e dados sensíveis. Esse cenário proporcionou uma oportunidade para os criminosos investirem mais esforços e elaborarem novas estratégias para aplicar golpes, dada à profusão de informações valiosas trafegando pela rede mundial de computadores.

Em 2021, essa busca por informações lucrativas culminou em dois imensos vazamentos de dados privados, expondo milhões de registros de indivíduos vivos e falecidos. Essas violações foram detectadas pela Psafe, uma empresa especializada em segurança cibernética. Os dados comprometidos estavam disponíveis para venda a outros grupos criminosos, ressaltando a vulnerabilidade do sistema em questão.

Em consonância com o pensamento do ministro Humberto Martins, que compartilhou sua opinião durante o seminário virtual “Criminalidade em tempos de Covid-19”, cabe ao Estado brasileiro aprimorar suas leis e regulamentos para prevenir a prática desses crimes, evitando assim prejuízos financeiros e patrimoniais a indivíduos, empresas e ao próprio governo. Ele enfatizou que os criminosos têm se voltado para fraudes eletrônicas ao perceberem o aumento substancial do uso da internet durante a pandemia.

REVISTA ELETRÔNICA AMPLAMENTE
v.2, n.3 jul./ set. 2023 DOI: 10.47538/RA-2023.V2N3
ISSN: 2965-0003

METODOLOGIA

A metodologia para a realização deste artigo pode ser classificada em duas etapas principais durante a primeira etapa, foi realizado um levantamento bibliográfico, com pesquisa direcionada em sites especializados, artigos e publicações literárias, focando especificamente no assunto de crimes digitais, incluindo fraudes de cartão de crédito e métodos de rastreamento de IP. Este levantamento foi fundamental para fundamentar os conceitos e ideias apresentados neste artigo.

Na segunda etapa, foi selecionada a ferramenta SET - *Social-Engineer Toolkit*, uma ferramenta popular para testes de intrusão, para uma demonstração prática de clonagem de um site. O alvo da clonagem não foi escolhido aleatoriamente, mas sim teve uma importância simbólica para o tema deste estudo. A ferramenta SET foi escolhida não apenas por suas capacidades técnicas, mas também como uma representação do conhecimento que a Professora Dulce escolhe transmitir ao "Matuto". Assim como Dulce ensina ao Matuto sobre os crimes digitais, o uso da ferramenta SET serve como uma metáfora para essa transferência de conhecimento, ilustrando o quão facilmente uma plataforma digital pode ser manipulada.

RESULTADOS

No presente exemplo, será apresentada uma simulação ilustrativa de como criar um site falso para enganar uma vítima, utilizando o sistema operacional Kali Linux. De acordo com o site TerminalRoot (2019), o Kali é amplamente empregado por hackers devido à abundância de ferramentas de ataque e testes de penetração incluídas nele.

O Kali Linux é um sistema operacional especializado utilizado para realizar testes de segurança, desenvolvido com base no Debian Linux. Para instalar o Kali Linux, é necessário possuir pelo menos 20 GB de espaço em disco. Com o CD do software em mãos, ao inseri-lo no computador e iniciar o processo de instalação, a opção "Graphical Install" deve ser escolhida. Em seguida, selecione o idioma, defina o idioma local, insira um nome para o sistema, especifique o fuso horário e opte por particionar o disco. A opção de particionamento manual é mais complexa e aconselhada para usuários experientes. Para a maioria dos usuários, é recomendável manter todos os arquivos em

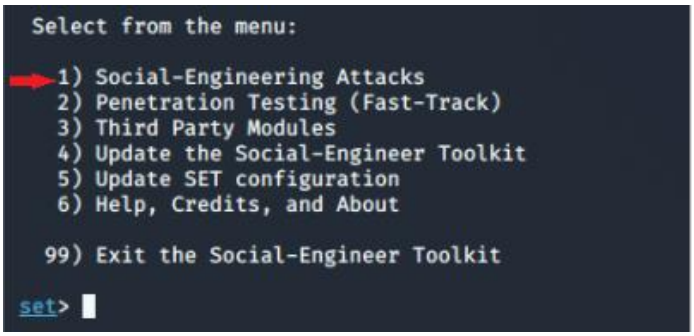
REVISTA ELETRÔNICA AMPLAMENTE
v.2, n.3 jul./ set. 2023 DOI: 10.47538/RA-2023.V2N3
ISSN: 2965-0003

uma única partição. Após a conclusão da instalação, o sistema operacional estará funcional (TRENTINO, F, 2019).

Ao utilizar a ferramenta Social-Engineer Toolkit (SET), é possível selecionar várias opções diferentes para testes e avaliações. No entanto, é importante salientar que para executar os comandos e utilizar eficazmente as ferramentas, é necessário ter familiaridade com o prompt de comando. A maioria dessas ferramentas não possui interfaces gráficas. Neste contexto, focaremos nos ataques de engenharia social, que são o ponto central deste tópico.

O procedimento se inicia ao escolher a opção 1 (*"Social-Engineering Attacks"*), o que conduzirá a um menu subsequente com diversos tipos de ataques de engenharia social (DE SOUZA TIESO, 2020) conforme figura 2 abaixo.

Figura 2: Seleção do Social-Engineering Attacks

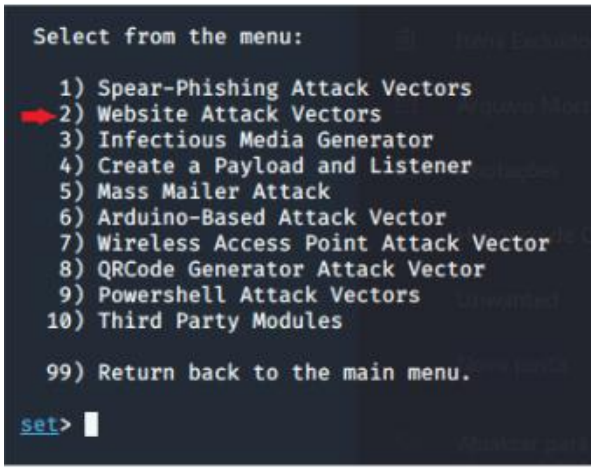


Fonte: DE SOUZA TIESO, 2020.

O próximo passo envolve escolher a opção número 2 ("*Website Attack Vetors*"), a qual oferecerá uma série de alternativas de ataque envolvendo websites.

REVISTA ELETRÔNICA AMPLAMENTE
v.2, n.3 jul./ set. 2023 DOI: 10.47538/RA-2023.V2N3
ISSN: 2965-0003

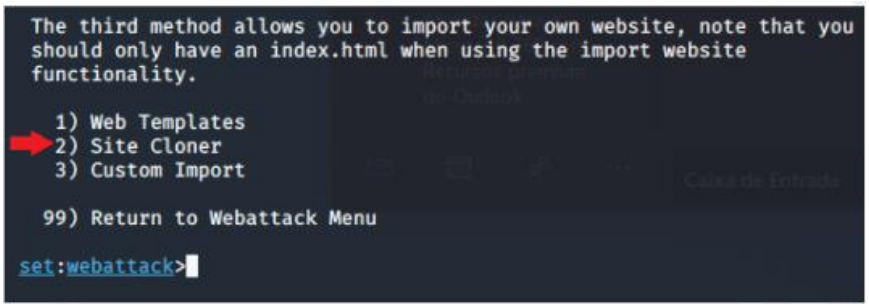
Figura 3: Seleção Website Attack Vetors



Fonte: DE SOUZA TIESO, 2020.

Após, será selecionada a segunda opção (*Site Cloner*)

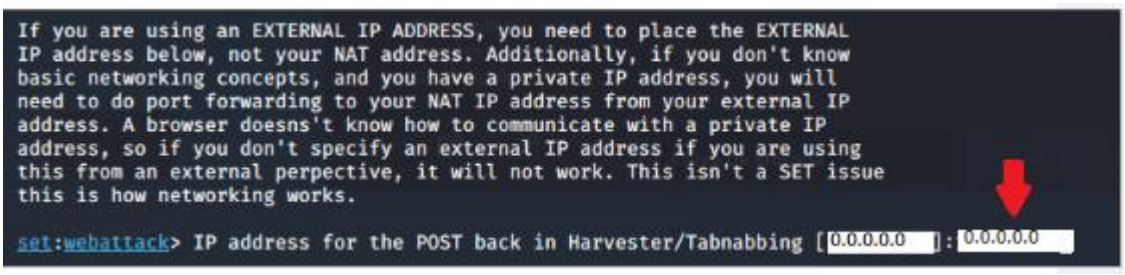
Figura 4: Selecionar Site Cloner



Fonte: DE SOUZA TIESO, 2020.

Após completar a etapa anterior, a ferramenta solicitará que seja inserido um endereço IP. As informações da vítima que acessar o nosso site clonado serão enviadas para esse endereço IP. Nesse cenário, é crucial usar o seu próprio endereço IP (Figura 05).

Figura 5: Inserindo do IP

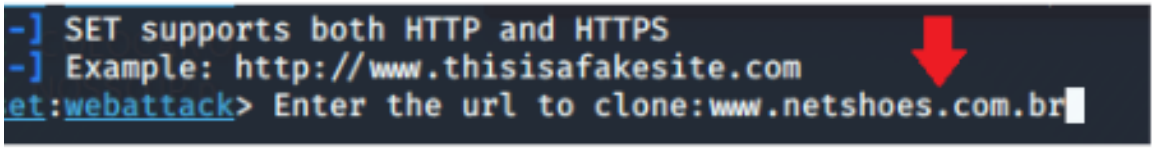


Fonte: DE SOUZA TIESO, 2020.

REVISTA ELETRÔNICA AMPLAMENTE
v.2, n.3 jul./ set. 2023 DOI: 10.47538/RA-2023.V2N3
ISSN: 2965-0003

Logo em seguida, a ferramenta requer a inserção da URL do site que será clonado. Embora a escolha do site seja flexível, é comum que hackers optem por sites populares frequentemente visitados. No exemplo, foi escolhido o site da Netshoes (Figura 06).

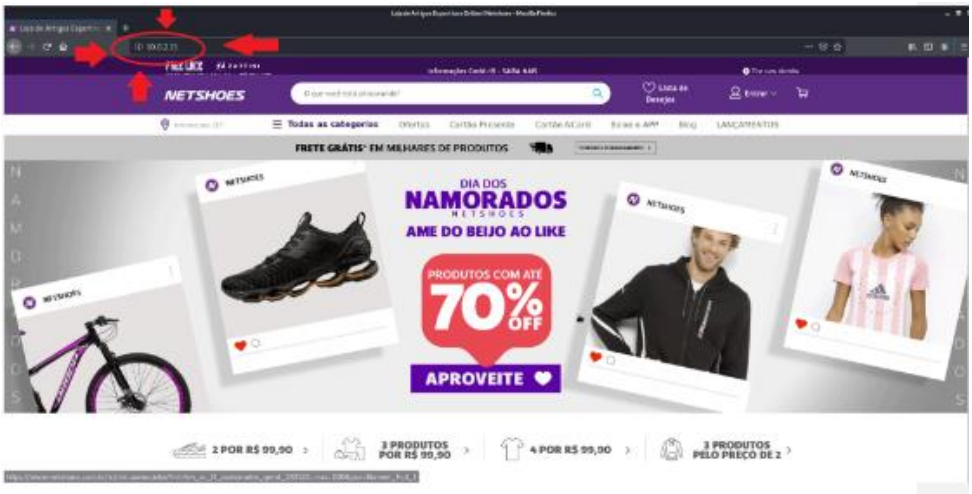
Figura 6: Inserindo o endereço do site clonado



Fonte: DE SOUZA TIESO, 2020.

Após essas etapas, basta digitar o mesmo endereço IP no seu navegador, tal como informado anteriormente. Isto resultará na abertura do site clonado (Figura 07).

Figura 7: O site clonado



Fonte: DE SOUZA TIESO, 2020.

É importante observar que, embora o site clonado seja visualmente idêntico ao site real, a URL (endereço do site) é exibida como um número de IP. Contudo, os hackers podem mascarar e alterar essa URL para evitar que os usuários percebam que estão interagindo com um site falso.

REVISTA ELETRÔNICA AMPLAMENTE
v.2, n.3 jul./ set. 2023 DOI: 10.47538/RA-2023.V2N3
ISSN: 2965-0003

Paulo Alves (2019) enfatiza algumas dicas fundamentais para verificar a autenticidade de um site e detectar se é falso. Verificar o domínio do site é sempre crucial, já que sites clones frequentemente utilizam nomes semelhantes. Por exemplo, "www.netfliix.com" inclui uma letra "i" adicional na palavra, que muitas vezes passa despercebida aos olhos dos usuários.

CONSIDERAÇÕES FINAIS

Em conclusão, o presente artigo alcançou seu objetivo central ao apresentar perspectivas valiosas sobre a complexa natureza dos crimes digitais e suas implicações, através de uma abordagem metodológica bem delineada.

A primeira etapa metodológica consistiu na realização de um minucioso levantamento bibliográfico, conduzido por meio de pesquisa direcionada a sites especializados, artigos e publicações literárias que se voltam especificamente para a temática dos crimes digitais.

A pesquisa teve um foco direcionado a conceituação dos crimes virtuais. Essa pesquisa desempenhou um papel fundamental ao fornecer os fundamentos necessários para sustentar os conceitos e ideias abordados ao longo do presente artigo.

Na segunda etapa, foi adotada uma abordagem prática, na qual foi selecionada a ferramenta SET - Social-Engineer Toolkit. A escolha dessa ferramenta não apenas levaram em consideração suas capacidades técnicas, mas também o simbolismo subjacente, representando o conhecimento que a Professora Dulce optou por transmitir ao "Matuto". A analogia entre a educação que Dulce ministrou sobre crimes digitais ao "Matuto" e o emprego da ferramenta SET para clonagem de sites e cartões ilustra de forma vívida a facilidade com que uma plataforma digital pode ser manipulada.

O resultado final deste artigo científico é uma análise abrangente que proporciona uma compreensão aprofundada das complexidades inerentes aos crimes digitais e suas implicações. As percepções obtidas por meio deste trabalho não somente enriquecem a compreensão desse campo em constante evolução, mas também destacam a importância de abordagens multidisciplinares e a necessidade de educar tanto os usuários quanto os

possíveis perpetradores sobre os desafios e responsabilidades no cenário digital contemporâneo. Em última análise, este artigo não apenas traz à tona uma narrativa singular, mas também contribui para a conscientização crescente sobre a crescente relevância dos crimes digitais na sociedade moderna e tecnologicamente avançada.

REFERÊNCIAS

ALVES, M. A. **Crimes Digitais:** Análise da criminalidade digital sob a perspectiva do direito processual penal e do instituto da prova – São Paulo - Editora Dialética, 2020.

ALVES, P. **Sete dicas para descobrir se um site é falso e evitar golpes online.** 25 mar.2019. Disponível em: <https://www.techtudo.com.br/listas/2019/03/sete-dicas-para-descobrir-se-um-site-e-falso-e-evitar-golpes-online.ghtml>. Acesso em: 17 agosto 2023

ALVES, R. F. L. **Crimes Virtuais:** Uma análise sobre os crimes Cibernéticos e a dificuldade na aplicação da legislação/ Rubens Fellipe Lima Alves. - João Pessoa, 2019. Disponível em: https://bdtcc.unipe.edu.br/wp-content/uploads/2019/09/CRIMES-DIGITAIS-1.pdf. Acesso em: 17 agosto 2023.

BENTES, T. K. et al. **Desenvolvimento de Interface para dispositivos móveis para interação entre demandantes e ofertantes de passagens no transporte aquaviário no Amazonas**. 2019.

CASTRO, C. R. A. C**rimes de Informática e seus Aspectos Processuais.** 2. ed. Rio de Janeiro: Lumen Juris, 2003.

CERT.BR - **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.** 2020

CORRÊA, G. T. **Aspectos Jurídicos da Internet**. São Paulo: Saraiva, 2002.

CRESPO, M. X. F. **Crimes digitais**. São Paulo: Saraiva, 2011.

HOLANDA FERREIRA, A. B. et al. **Míni Aurélio:** o dicionário da língua portuguesa. Positivo, 2010.

DE SOUZA TIESO, I. H.; DO ESPIRITO SANTO, F. ATAQUES DE ENGENHARIA SOCIAL**. Revista Interface Tecnológica**, v. 17, n. 02, p. 206-218, 2020.

HOLANDA FERREIRA, A. B. **Novo dicionário da língua portuguesa**. 02ª Ed. Rio de Janeiro: Nova Fronteira, 2000.

INELLAS, G. C. Z. **Crimes na Internet. São** Paulo: Editora Juarez de Oliveira, 2004.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA - IBGE. **Internet já é acessível em 90,0% dos domicílios do país em 2021.** Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34954-internet-ja-e-acessivel-em-90-0-dos-domicilios-do-pais-em-

2021#:~:text=Internet%20chega%20a%2090%2C0,%25%20para%2092%2C3%25.. Acesso em: 17 de agosto de 2023.

LEMOS, A.; /LÉVY, P. **O futuro da Internet:** em direção a uma ciberdemocracia. São Paulo: Paulus, 2010.

PECK, P. **Direito digital**. São Paulo: Saraiva, 2002.

PINHEIRO, P. P. **Direito Digital.** 04. Ed. São Paulo: Saraiva, 2010.

ROCHA, A. A. **Cibercriminalidade:** os crimes cibernéticos e os limites da liberdade de expressão na internet. Faculdade de Ensino Superior e Formação Integral, Curso de Direito, São Paulo, 2017 [Internet]. Disponível em: <https://www.faef.br/userfiles/files/23%20%20CIBERCRIMINALIDADE%20E%20OS 16 %20LIMITES%20DA%20LIBERDADE%20DE%20EXPRESSAO%20N%20INTERNE T.pdf. Acesso em: 17 agosto 2023.

ROSA, F. **Crimes de Informática**. Campinas: Bookseller, 2002.

SANTOS, A. B. **O namoro do matuto com a professora**. 1977. Disponível em: https://cordel.edel.univ-poitiers.fr/items/show/200. Acesso em: 17 de agosto de 2023..

SCHWAB, K.; DAVIS, N. **Aplicando a quarta revolução industrial**. Edipro, 2019.

STRASSER, F. A. C.; DE OLIVEIRA, M. G. **O advento da internet e seus desafios no campo jurídico brasileiro.** In: Colloquium Socialis. ISSN: 2526-7035. 2019. p. 06-19.

SUPERDICAS - **Invenções que mudaram o mundo e sobreviveram ao tempo**. Disponível em: <http://www.superdicas.com.br/almanaque/almanaque.asp?u_action=display&u_log=254>. Acessado em: [Mês]. [Ano].

TERMINALROOT. **As 22 Melhores Distros Linux para Hackers (Pentesting).** 18 dez.2019. Disponível em: <https://terminalroot.com.br/2019/12/as-22-melhores-distros-linux-para-hackers-218Interface Tecnológica -v. 17 n. 02 (2020)pentesting.html#:~:text=Kali%20Linux,digital%20e%20teste%20de%20invas%C3%A3o.>. Acesso em: 17 de agosto de 2023.

TRETINO, F. **Como instalar passo a passo o Kali Linux 2019**. 31 jan.2019. Disponível em: https://sempreupdate.com.br/como-instalar-passo-a-passo-o-kali-linux-2019/. Acesso em: 17 de agosto de 2023.

ZANELLATO, M. A. **Condutas Ilícitas na sociedade digital, Caderno Jurídico da Escola Superior do Ministério Público do Estado de São Paulo, Direito e Internet,** n. IV, Julho de 2002.

Data de submissão: 05/05/2023. Data de aceite: 08/06/2023. Data de publicação: 12/08/2023.