Uma proposta de ferramenta de análise de dados administrativos como estratégia defensiva ao estelionato digital

Carlos Eduardo Taranto Winter
Bacharelado em Sistemas de Informação
Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (Cefet-RJ)
Nova Friburgo, Brasil
carlos.winter@aluno.cefet-rj.br

Davi Heggdorne Klein
Bacharelado em Sistemas de Informação
Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (Cefet-RJ)
Nova Friburgo, Brasil
davi.klein@aluno.cefet-rj.br

Nilson Mori Lazarin
Bacharelado em Sistemas de Informação
Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (Cefet-RJ)
Nova Friburgo, Brasil
nilson.lazarin@cefet-rj.br

ABSTRACT

This paper addresses the growing concerns surrounding online security by introducing a WhatsApp bot designed to assist users in determining the trustworthiness of websites. With the surge in cyber threats, exemplified by 5.6 million recorded fraud attempts in Brazil in 2022, the imperative for robust information security measures is evident. The proposed solution involves the development of a bot to check the ".BR" top-level domain and correlate it with legal entity information found in domain registrations. Therefore, this implementation is expected to contribute to reducing user insecurity regarding e-commerce platforms.

KEYWORDS

Security, WhatsApp, E-commerce

1 INTRODUÇÃO

De acordo com a Associação Brasileira de Comércio Eletrônico, durante os anos de 2017 a 2022, o faturamento do comércio eletrônico no Brasil experimentou um impressionante crescimento de quase 182%. Paralelamente, o volume de pedidos online registrou um notável aumento de 163% durante esse mesmo intervalo de tempo, totalizando 368,7 milhões de transações em 2022 [1]. Esse incremento também acarretou um significativo aumento no número de golpes virtuais, invasões por hackers, vazamentos de dados pessoais, clonagem de cartões, vírus, entre outros [2]. Segundo a pesquisa realizada pela Unico IDtech, metade dos consumidores brasileiros já foi vítima de fraude no e-commerce [3]. Logo, no comércio eletrônico, o consumidor pode estar sujeito a várias formas de violação de seus direitos. Exemplos incluem produtos com defeitos, publicidade enganosa, recebimento de mercadorias diferentes das solicitadas, serviços de baixa qualidade e não cumprimento dos termos e cláusulas do contrato. Esses são alguns dos problemas enfrentados pelo consumidor [4].

Somado a isso, só em 2022, foram realizadas 5,6 milhões de tentativas de fraude, equivalentes a 5,8 bilhões de reais, segundo dados levantados pelo "Mapa da Fraude", pesquisa realizada pela ClearSale [5]. Esses números têm crescido rapidamente nos últimos anos, muitas vezes devido à falta de conhecimento dos usuários sobre como proteger sua integridade e seus dados na internet [6].

O estelionato emerge como um dos crimes mais beneficiados pela facilidade na criação de páginas e conteúdos fraudulentos. Adicionalmente, a replicação de sites de e-commerce reconhecidos é outra prática prejudicial nesse panorama. A criação de páginas falsas, muitas vezes imitando identidades visuais e estruturas de plataformas de compras online bem estabelecidas, visa enganar consumidores desavisados [7].

Este trabalho apresenta um protótipo ferramenta para auditoria de sites de e-commerce baseada em uma abordagem focada no lado do usuário. Através do simples compartilhamento de um link de oferta de e-commerce através do WhatsApp, a ferramenta é capaz de analisar os dados administrativos do registro do domínio e consultar as informações sobre a empresa responsável, junto à Receita Federal, apresentando um relatório ao usuário de forma simples. Dessa forma, espera-se auxiliar o usuário na tomada de decisões mais assertivas em relação à confiabilidade de e-commerce, promovendo uma experiência mais segura e consciente.

2 FUNDAMENTAÇÃO TEÓRICA

O registro de domínios na internet tornou-se fácil e acessível com a oferta de serviços de registro por meio de plataformas que possibilitam a pesquisa e registro de um nome desejado em poucos passos. Essa acessibilidade democratizou a criação de sites para indivíduos e empresas de todos os portes. Contudo, também facilitou práticas prejudiciais, como o *cybersquatting*, registro malicioso de domínios de marcas conhecidas, e o *phishing*, técnica de engenharia social usada para enganar o usuário de internet. Pois, a falta de confirmação de autenticidade em alguns serviços de registro de domínios contribuem para que indivíduos mal-intencionados explorarem esta característica para atos fraudulentos e danosos [8, 9].

O *Top-Level Domain* TLD ".br" refere-se ao domínio associado ao Brasil na internet. Ele é gerenciado pelo Registro.br, um departamento do NIC.br. Para registrar um domínio ".br", é necessário fornecer informações como Nome, CPF ou CNPJ, endereço, e contatos válidos. Esses dados são essenciais para a identificação do proprietário do domínio, contribuindo para a transparência e segurança no ambiente online [10].

Uma das formas de consultar os dados públicos de um domínio de internet é através do WHOIS, um sistema e protocolo que fornece informações, como o nome do proprietário, informações de contato, data de registro, data de expiração e outros detalhes relevantes. Essa funcionalidade é essencial para promover a transparência e a responsabilidade no ecossistema online [11].

3 PROPOSTA

Embora exista no Brasil uma importante iniciativa para a popularização da Segurança da Informação [12], usuários inexperientes e sem instrução digital muitas vezes são alvos de estelionato via internet. Mesmo que existam os selos de reputação em sites de e-commerce, estes podem ser forjados para enganar usuários leigos, além de já não trazer confiança, pois as métricas de avaliação não são tão claras e existem diversos exemplos de discrepância entre os selos e as notas dos usuários [13]. Neste contexto, foi proposta [14] uma estratégia defensiva ao estelionato digital focada no lado do usuário, baseada no uso de extensões de navegadores de internet para desktops.

Entretanto, o smartphone é o principal meio de acesso à internet, conforme o CGI.br, pois em 2023 99% de todos os usuários de internet no país utilizam smartphone para navegar e 62% desses acessam a rede exclusivamente pelo smartphone [15]. Além disso, 99% dos smartphones no país possuem o comunicador WhatsApp instalado, pois isso demonstra a crescente importância do celular e desse aplicativo na vida digital dos brasileiros, consolidando-se como uma plataforma essencial para comunicação e acesso à internet [16].

Dessa forma, este trabalho evoluí a estratégia defensiva, apresentando o Ricky(*inte**R**net Doma**I**n **C**hec**K** s**Y**stem*), um bot para WhatsApp que realiza a extração de dados administrativos de links de e-commerce, utilizando o protocolo WHOIS, e a verificação destes junto à Receita Federal. Para adicioná-lo, basta acessar o link https://bsi.cefet-rj.br/ricky/ ou escanear o QRCode presente na Figura 1, usando um smartphone. Além disso, o código fonte do bot está disponível para downlod no GitHub[1].

Figure 1: Contato WhatsApp do Ricky bot.

Uma prova de conceito é apresentada na Figura 2. O processo de verificação de um link de e-commerce é realizado nos passos descritos abaixo:

(1) *Extração do domínio*: O bot inicia o processo ao receber uma mensagem no WhatsApp. A primeira etapa consiste em extrair um domínio válido da mensagem recebida. Esse domínio será a chave para as consultas subsequentes.

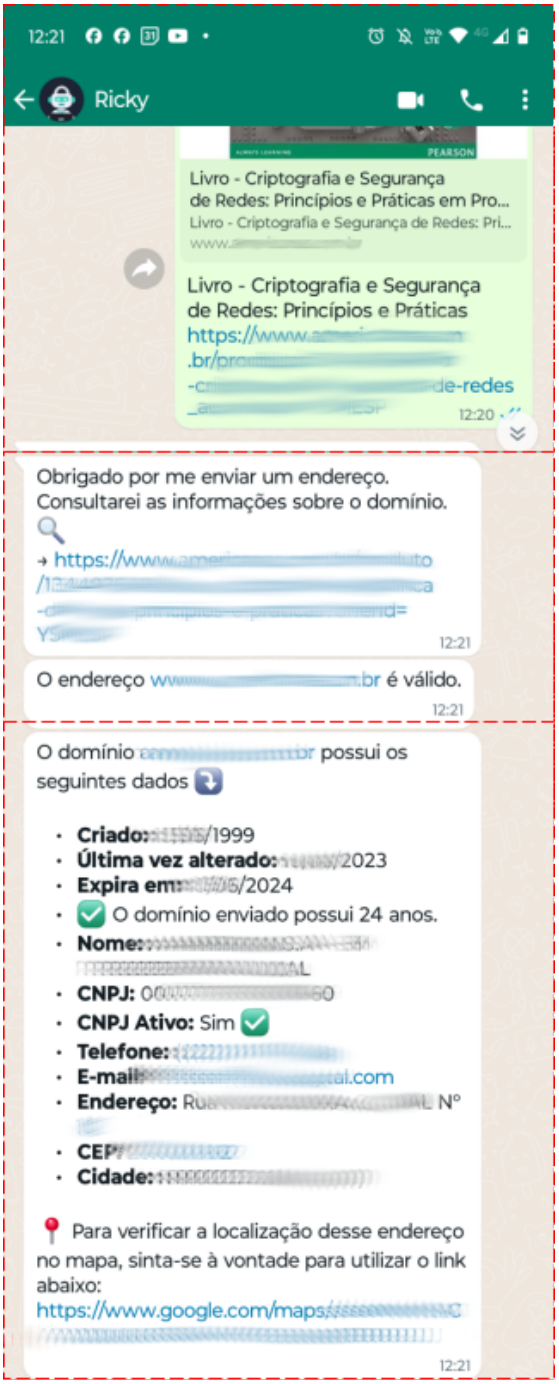

Figure 2: Interação de um usuário com o Ricky.

(2) *Identificação do TLD .br*: O sistema verifica se o domínio pertence ao TLD .br. Caso negativo, o bot realiza uma consulta para verificar se existe um domínio .br cujo IP seja equivalente. Essa etapa é crucial para garantir que sites que possuem domínios com e sem .br sejam identificados.

[1] https://github.com/LabRedesCefetNF/RickyBot

(3) *Consulta WHOIS*: Caso a comparação de IPs seja positiva, ou o domínio enviado já possua um TLD .br, o bot executa uma consulta WHOIS. Esse passo visa obter informações administrativas associadas ao domínio.
(4) *Relacionamento com a Receita Federal*: A partir dos dados administrativos extraídos do protocolo WHOIS, o bot realiza uma consulta na Receita Federal para correlacionar essas informações.
(5) *Resposta com os dados obtidos*: Ao concluir com êxito todas as fases do processo, o bot no WhatsApp entregará ao usuário uma mensagem abrangente, revelando informações cruciais sobre o domínio em questão.

A resposta, informada pelo bot, inclui dados essenciais, como a data de criação do domínio, a última vez que foi alterado, a data de expiração e a idade atual do domínio. Além disso, o usuário terá acesso aos dados registrados na Receita Federal, tais como o nome da empresa responsável, o número de CNPJ, a ativação do CNPJ, o número de telefone vinculado, o endereço de e-mail e a localização física. Dessa forma, visamos fornecer ao usuário uma compreensão completa e detalhada tanto dos aspectos técnicos do domínio quanto das informações administrativas, proporcionando uma experiência informativa e abrangente.

4 CONSIDERAÇÕES FINAIS

Atualmente, o projeto está em fase de implementação, e os próximos passos incluirão a realização de testes com usuários para avaliar a eficácia e usabilidade do bot. Essa etapa será fundamental para obter feedback valioso e identificar áreas de melhoria. Após os testes, planejamos implementar recursos adicionais para aprimorar sua capacidade de fornecer informações precisas e relevantes aos usuários.

REFERENCES

[1] Associação Brasileira de Comércio Eletrônico (ABComm). Crescimento do ecommerce brasileiro. https://dados.abcomm.org/crescimento-do-ecommerce-brasileiro, nov 2023.
[2] Matheus de Oliveira Mota. Estudo de caso sobre segurança em e-commerce, 2021. Pontifícia Universidade Católica de Goiás. https://repositorio.pucgoias.edu.br/jspui/handle/123456789/3206.
[3] Unico IDtech. Metade dos consumidores brasileiros já foi vítima de fraude no e-commerce, November 2022. URL https://mercadoeconsumo.com.br/01/11/2022/ecommerce/metade-dos-consumidores-brasileiros-ja-foi-vitima-de-fraude-no-e-commerce/.
[4] Michel Bernardo Fernandes da Silva. *Cibersegurança: Uma visão panorâmica sobre a segurança da informação na Internet*. Freitas Bastos Editora, Rio de Janeiro, RJ, January 2023. ISBN 9786556752440.
[5] ClearSale. Mapa da fraude 2022. https://br.clear.sale/mapa-da-fraude/, 2022. URL https://br.clear.sale/mapa-da-fraude/.
[6] Leonardo Guilherme, Matheus Ferreira, Gustavo da Fonseca, and Nilson Lazarin. Uma breve noção sobre o comportamento dos internautas em relação à segurança na rede. In *Anais da VII Escola Regional de Sistemas de Informação do Rio de Janeiro*, pages 1–7, Porto Alegre, 2021. SBC. URL https://doi.org/10.5753/ersirj.2021.16972.
[7] Danilo Moreira. E-commerce durante e a pandemia e o aumento do estelionato digital., 2022. Universidade São Judas. https://repositorio.animaeducacao.com.br/handle/ANIMA/29867.
[8] Radhika Vivek Bhusari, Karan Ramchandra Rampure, et al. Cybersquatting: A threat to the globalising world. *Indian Journal of Law and Legal Research*, 3(2): 2283–2304, 2022. URL https://doi.org/10.17613/9c3s-hb09.
[9] Pawankumar Sharma, Bibhu Dash, and Meraj Farheen Ansari. Anti-phishing techniques–a review of cyber defense mechanisms. *International Journal of Advanced Research in Computer and Communication Engineering ISO*, 3297:2007, 2022. URL https://ssrn.com/abstract=4335354.
[10] Carlos Ari Sundfeld and André Rosilho. A governança não estatal da internet e o direito brasileiro. *Revista de Direito Administrativo*, 270:41–79, set. 2015. URL https://doi.org/10.12660/rda.v270.2015.58737.
[11] Leslie Daigle. WHOIS Protocol Specification. RFC 3912, September 2004. URL https://www.rfc-editor.org/info/rfc3912.
[12] Helter Rocha, Erick Klein, Leonardo Rimes, and Nilson Lazarin. Iniciativas de popularização da segurança da informação: Um survey. In *Anais Estendidos do XVIII Simpósio Brasileiro de Sistemas de Informação*, pages 37–40, Porto Alegre, RS, Brasil, 2022. SBC. URL https://doi.org/10.5753/sbsi_estendido.2022.222787.
[13] Brayner Cristian Mello Carvalho, Gabrielly Ezequiel Corrêa, João Pedro Ribeiro De Moura Buzato Pinto, and Nilson Mori Lazarin. Sistemas de reputação e sua influência: Um comparativo. In *Anais do XIII Computer on the Beach - COTB'22*, pages 306–308, Itajaí - Santa Catarina - Brasil, July 2022. Universidade do Vale do Itajaí. URL https://doi.org/10.14210/cotb.v13.p306-308.
[14] Brayner Carvalho and Nilson Lazarin. Análise de dados administrativos de e-commerce: Uma abordagem focada no cliente. In *Anais Estendidos do XXIII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 243–248, Porto Alegre, RS, Brasil, 2023. SBC. URL https://doi.org/10.5753/sbseg_estendido.2023.233492.
[15] NIC.br. Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: pesquisa tic domicílios. 2022. URL https://cetic.br/pt/arquivos/domicilios/2022/individuos/.
[16] RD Station. Panorama de vendas 2023. 2023. URL https://materiais.resultadosdigitais.com.br/crm-panorama-de-vendas.