10º Encontro de Ensino Pesquisa e Extensão

Patrocínio, MG, outubro de 2023

UMA ANÁLISE DAS TECNOLOGIAS DE DETECÇÃO E MITIGAÇÃO NA IDENTIFICAÇÃO DE PÁGINAS DE PHISHING

Ronan de Paula Guedes, Júnio Moreira
<ronan.guedes@estudante.iftm.edu.br>,<juniomoreira@iftm.edu.br>
Instituto Federal do Triângulo Mineiro
Modalidade: Pesquisa
Formato: Artigo Completo

Resumo

O phishing é uma prática maliciosa que visa enganar os usuários, levando-os a divulgar informações pessoais ou financeiras, frequentemente por meio de páginas da web falsas. Apesar dos esforços incansáveis da comunidade científica em combater essa atividade, o phishing continua a se sofisticar e a atingir suas vítimas com sucesso. Este artigo apresenta uma análise das tecnologias de detecção e mitigação de páginas de phishing, uma ameaça persistente e crescente na segurança cibernética atual. A pesquisa examina as estratégias e tendências emergentes nessas tecnologias, abordando os desafios comuns encontrados na identificação de páginas de phishing. São fornecidas valiosas percepções sobre soluções eficazes, como a análise heurística, verificação de autenticidade de sites, detecção de anomalias de tráfego e análise de conteúdo, para proteger usuários e organizações contra esses ataques enganosos. Os resultados contribuem substancialmente para o aprimoramento da segurança cibernética, ao abordar a importância crítica do combate ao phishing na era digital.

Palavras-chaves: Phishing. Segurança Cibernética. Autenticidade de Sites. Anomalias de Tráfego. Análise de Tráfego de Dados.

Introdução

A proliferação da internet tem desempenhado um papel fundamental em nossa sociedade, moldando e afetando uma ampla variedade de setores e influenciando a vida cotidiana de um número cada vez maior de pessoas. No entanto, essa disseminação maciça da conectividade também tem gerado oportunidades para agentes maliciosos, destacando o crescimento do phishing como um dos crimes cibernéticos mais comuns e prejudiciais. Essa forma de ataque se baseia na engenharia social para enganar vítimas e obter informações pessoais ou sensíveis.

O phishing utiliza uma variedade de técnicas para enganar e manipular pessoas com o objetivo de adquirir informações confidenciais ou acesso a sistemas. Embora muitas vezes seja associado a ataques cibernéticos, vale ressaltar que o phishing não se limita ao ambiente digital e pode ocorrer em contextos não digitais, como telefonemas ou interações pessoais. Portanto, é fundamental reconhecer que a engenharia social abrange uma ampla gama de cenários, tornando-se uma ameaça digital que merece atenção (ALENCAR; LIMA; FIRMO, 2013).

Um exemplo clássico de phishing envolve o envio de mensagens de e-mail fraudulentas que se disfarçam de comunicações legítimas, como aquelas de instituições financeiras, com o objetivo de direcionar as vítimas para páginas da web falsas e extrair informações confidenciais (SAHINGOZ et al., 2019).

Apesar dos esforços de combate a esse tipo de crime, é notório que o phishing continua a ter sucesso. Uma das razões para isso é a constante evolução das estratégias e mecanismos empregados pelos phishers, tornando essencial a constante adaptação e aprimoramento das tecnologias de detecção e prevenção para proteger eficazmente os usuários e as organizações contra esses ataques enganosos.

Além das consequências financeiras e de privacidade, o phishing também tem um impacto significativo na confiança das pessoas no ambiente digital. A percepção de que qualquer link ou mensagem pode ser uma armadilha cria um clima de desconfiança que afeta a maneira como interagimos online. Isso não apenas prejudica a experiência do usuário, mas também prejudica a capacidade das empresas de conduzir negócios de maneira eficaz e segura na era digital. Portanto, entender e combater o phishing não é

apenas uma questão de segurança cibernética, mas também de proteger a integridade e a confiabilidade da infraestrutura digital que se tornou essencial em nossas vidas.

Desta forma, este artigo tem como objetivo aprofundar a análise das tecnologias que desempenham um papel fundamental na restauração da confiança dos usuários e na proteção das organizações contra os perigos do phishing. Em um contexto onde o phishing representa uma ameaça em constante crescimento para a segurança cibernética, nossa análise se concentra nas tecnologias de detecção e mitigação de páginas fraudulentas. Buscamos compreender e abordar essa ameaça, fornecendo percepções essenciais para a restauração da confiança digital e a proteção eficaz de usuários e organizações.

Fundamentação Teórica

Na segurança cibernética atual, o phishing é uma ameaça persistente e dominante. Para abordar efetivamente essa ameaça, é essencial entender tanto a proposta de pesquisa quanto a definição do próprio termo "phishing". A palavra "phishing"tem sua origem na língua inglesa e significa a atividade de pescar (PEREIRA, 2012).

Tomando por base esse contexto, a pesquisa se concentra em realizar uma análise aprofundada das tecnologias de detecção e mitigação na identificação de páginas de phishing, com o objetivo de identificar essas ameaças persistentes na segurança cibernética. A pesquisa visa contribuir para o desenvolvimento de soluções mais eficazes na identificação e combate ao phishing. As etapas da proposta incluem revisão da literatura, desenvolvimento de metodologia, análise de dados e a expectativa de apresentar resultados que abordem os desafios comuns encontrados na identificação de páginas de phishing, visando a segurança cibernética (DAMASCENO et al., 2021).

Além disso, é importante destacar que o phishing é uma forma de ataque cibernético em que os atacantes se passam por entidades confiáveis para enganar as vítimas e obter informações confidenciais, como senhas e números de cartões de crédito (SILVA, P. A. L. da, 2012). A premissa doo phishing é criar uma aparência atraente que eletronicamente para persuadir as vítimas, levando-as a crer que estão interagindo com uma fonte confiável (PIOVESAN et al., 2019).

O tráfego de spam é uma das ameaças mais antigas e persistentes na esfera digital, representando um problema significativo para indivíduos, empresas e organizações em todo o mundo. Apesar dos esforços para filtrar e excluir mensagens indesejadas em caixas de entrada de e-mail, o tráfego de spam continua a evoluir e encontrar novas formas de comprometer a segurança online (FONSECA et al., 2015). No contexto digital, a engenharia social é usada de maneira recorrente para enganar os usuários e obter informações pessoais ou instalar software malicioso (ARAÚJO; VENTURA, 2019).

Para mitigar os riscos do phishing, é crucial promover a conscientização, a educação e a implementação de medidas de proteção adequadas. Além disso, a discussão contínua sobre as implicações éticas da engenharia social é essencial, pois essa área continua a evoluir para melhorar a segurança e as técnicas de defesa contra o phishing (ESPADA, 2020).

Para realizar ataques de phishing na web, os agentes mal-intencionados frequentemente usam ferramentas da web chamadas de "kits de phishing". Esses kits são projetados para parecer páginas legítimas da web e podem ser facilmente encontrados na dark web. No entanto, alguns desses kits têm funcionalidades ocultas que enviam os dados coletados de volta para o desenvolvedor original do kit. Isso torna esses kits cada vez mais sofisticados e difíceis de serem identificados, representando uma ameaça significativa para a segurança online (LEITE et al., 2019).

É fundamental analisar o URL de um site para verificar se ele possui um certificado digital SSL (Secure Sockets Layer), que é uma parte crítica do protocolo de segurança da web. Essa verificação ajuda a garantir que o site seja seguro e protegido (RIBEIRO; BATISTA; PINA, 2020). A proteção pessoal e a conscientização são essenciais para uma experiência online segura.

Diversas pesquisas têm sido conduzidas com o objetivo de identificar e mitigar páginas de phishing. Os estudos em (MORGADO, 2023; COUTINHO, 2023; SOUZA; LEMOS et al., 2019; SOUZA; TANAKA, 2023), propõem a coleta e identificação de um grande volume de páginas maliciosas, visando caracterizá-las e desenvolver mecanismos de mitigação. No entanto, a coleta e identificação de páginas de phishing enfrentam desafios, levando à proposição de abordagens para reforçar a segurança contra essa ameaça, focando na melhoria da detecção e mitigação (MOREIRA FILHO,

2023). Além disso, ao analisar os modelos de segurança em (SOUZA; TANAKA, 2023) para proteger os dados pessoais e os direitos fundamentais, são identificados métodos que visam fortalecer a segurança, incluindo análise de conteúdo, URL, SSL, proteção anti-spam, firewall, antivírus e anti-spyware. Adicionalmente, os autores conseguiram melhorar significativamente o trabalho anterior (SILVA, F. R. C., 2023), contribuindo para avanços na segurança.

Proposta

O phishing é uma prática maliciosa que persiste como uma ameaça contínua e crescente na segurança cibernética contemporânea. Este estudo tem como objetivo abordar medidas iniciais de mitigação relacionadas à análise de phishing, considerando suas implicações prejudiciais para os usuários e organizações. O fenômeno do phishing envolve práticas enganosas que buscam persuadir indivíduos a divulgar informações pessoais ou financeiras por meio de páginas da web fraudulentas.

Nossa pesquisa se concentra em examinar e avaliar as estratégias, tendências e desafios encontrados na identificação de páginas de phishing, fazendo uso das tecnologias disponíveis. Isso inclui um estudo de técnicas de detecção existentes, tais como análise heurística, verificação de autenticidade de sites, detecção de anomalias de tráfego e análise de conteúdo. Além disso, investigaremos a aplicação de abordagens de aprendizado de máquina na detecção proativa de phishing, visando aprimorar a precisão e eficácia na identificação de ameaças. Essas tecnologias desempenham um papel crucial na redução de falsos positivos e na detecção de ataques de phishing cada vez mais sofisticados.

Este estudo também fornece orientações práticas para usuários e organizações na prevenção de ataques de phishing. Estas diretrizes incluirão estratégias para verificar a autenticidade de sites, identificar indicadores de phishing, preservando informações pessoais e implementar medidas de segurança cibernética eficazes.

Espera-se que os resultados desta pesquisa contribuam substancialmente para o fortalecimento da segurança cibernética, capacitando indivíduos e organizações a se defenderem de forma mais eficaz contra as persistentes ameaças de phishing.

Resultados

Os resultados enfatizam a constante complexidade do cenário de combate ao phishing. Embora a ameaça persista e se aprimore, as tecnologias de detecção e mitigação estão evoluindo de maneira dinâmica para enfrentar esse desafio em evolução constante. É crucial ressaltar que a conscientização dos usuários, a educação contínua e a colaboração ativa entre tecnologia, organizações e indivíduos permanecem como pilares essenciais na defesa contra o phishing em meio à sempre mutante na era digital.

Portanto, a luta contra o phishing continua a ser de importância crítica para aprimorar a segurança cibernética e garantir a proteção de nossos sistemas e informações online. Consequentemente, as próximas seções apresentam a análise dos resultados das técnicas estudadas.

Tendências e Estratégias de Ataque

Iniciamos nossa análise examinando as tendências e estratégias de ataque utilizadas pelos phishers. Observamos que, apesar dos esforços significativos da comunidade científica e da indústria de segurança cibernética, os ataques de phishing continuam a se sofisticar. Os phishers estão constantemente inovando, tornando seus ataques mais convincentes e difíceis de detectar. Isso inclui o uso de páginas da web falsas que se assemelham cada vez mais a sites legítimos, e-mails falsificados de instituições confiáveis e táticas de engenharia social altamente persuasivas.

Desafios na Identificação de Páginas de Phishing

Um dos principais desafios que encontramos está na identificação precisa de páginas de phishing. Os phishers estão usando técnicas para mascarar suas atividades, tornando-as menos óbvias para os sistemas de segurança. Além disso, eles frequentemente mudam rapidamente de hospedagem e domínios, tornando difícil rastreá-los. A falta de padrões claros em alguns casos também dificulta a detecção, já que os phishers adaptam suas táticas de acordo com as vulnerabilidades identificadas.

Soluções e Tecnologias de Mitigação

No entanto, nossa análise também destacou que existem soluções e tecnologias eficazes disponíveis para combater o phishing. A análise heurística, por exemplo, se mostrou uma abordagem valiosa para identificar páginas de phishing com base em padrões comportamentais suspeitos. A verificação da autenticidade de sites por meio de certificados SSL e protocolos HTTPS também se revelou uma medida eficaz na identificação de possíveis ameaças.

A detecção de anomalias de tráfego e análise de conteúdo desempenharam papéis cruciais na proteção dos usuários e organizações contra ataques enganosos. Além disso, a integração de técnicas de aprendizado de máquina está melhorando constantemente a precisão e a eficácia na identificação de ameaças de phishing.

Conscientização e Educação dos Usuários

Reforçamos a importância da conscientização e educação dos usuários na prevenção de ataques de phishing. Os usuários devem ser instruídos sobre como identificar sinais de phishing, como verificar a autenticidade de sites e como proteger suas informações pessoais. A conscientização contínua é essencial para capacitar os usuários a serem mais vigilantes durante suas interações online.

Considerações Finais

Em um cenário cada vez mais interconectado e dependente da tecnologia, a ameaça do phishing representa um desafio constante à segurança cibernética. Nossa análise das tecnologias de detecção e mitigação de páginas de phishing revelou a complexidade dessa batalha em curso. Apesar dos avanços na identificação e prevenção de ataques de phishing, os agentes maliciosos continuam a adaptar e aprimorar suas táticas. Portanto, é essencial reconhecer que a segurança cibernética é uma busca contínua, e as organizações devem investir em soluções inovadoras e manter-se atualizadas com as últimas tendências em segurança digital.

Além disso, a pesquisa proporcionou valiosos insights. As tecnologias de detec-

ção de phishing estão evoluindo e se tornando mais sofisticadas, incorporando aprendizado de máquina, análise de comportamento e outros métodos avançados para identificar ameaças. Além disso, a conscientização e a educação contínuas dos usuários desempenham um papel fundamental na defesa contra o phishing. À medida que os sistemas de segurança cibernética se tornam mais inteligentes, é crucial que os indivíduos também se tornem mais vigilantes e cientes dos riscos associados à engenharia social e ao phishing.

Em última análise, a luta contra o phishing é uma colaboração contínua entre a tecnologia, as organizações e os usuários. À medida que as tecnologias de detecção e mitigação de phishing avançam, e à medida que a conscientização e a educação cibernética aumentam, podemos esperar que o impacto do phishing seja reduzido. No entanto, a ameaça nunca desaparecerá completamente. Portanto, o compromisso com a inovação, a vigilância constante e a resposta eficaz a incidentes de phishing permanecem fundamentais para proteger nossos sistemas e informações na era digital em constante evolução.

REFERÊNCIAS BIBLIOGRÁFICAS

ALENCAR, G.; LIMA, M. de; FIRMO, A. O efeito da conscientização de usuários no meio corporativo no combate à engenharia social e phishing. In: SBC. ANAIS do IX Simpósio Brasileiro de Sistemas de Informação. [S.l.: s.n.], 2013. P. 254–259.

ARAÚJO, R. T. A. d.; VENTURA, T. B. Painel de apoio para uma central de detecção de padrões maliciosos, 2019.

COUTINHO, V. M. Detecção de páginas de phishing utilizando aprendizado de máquina. Universidade Estadual Paulista (Unesp), 2023.

DAMASCENO, H. et al. Monitoramento e Identificação de Páginas de Phishing. In: ANAIS do XXXIX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. Uberlândia: SBC, 2021. P. 378–391. DOI: 10.5753/sbrc.2021.16734. Disponível em: <https://sol.sbc.org.br/index.php/sbrc/article/view/16734>.

ESPADA, P. A. U. Métodos Orientados a Reducir Ataques de Ingeniería Social en Organizaciones. **INF-FCPN-PGI Revista PGI**, p. 76–79, 2020.

FONSECA, O. et al. Uma Análise do Custo do Tráfego de Spam para Operadores de Rede. **Anais do simpósio brasileiro de redes de computadores e sistemas distribuídos (SBRC). SBC**, 2015.

LEITE, C. et al. Waste Flooding: Ferramenta para Retaliaçao de Phishing. In: SBC. ANAIS Estendidos do XIX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. [S.l.: s.n.], 2019. P. 27–34.

MOREIRA FILHO, G. V. Mecanismos regulatórios em matéria de privacidade e proteção de dados pessoais: do modelo regulatório estatal aos modelos híbridos de regulação público-privada. Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, 2023.

MORGADO, E. M. CASO DE CYBER FRAUD POR TELEFONE NO BRASIL E A INTELIGÊNCIA ARTIFICIAL: VÍTIMAS IDOSAS, SPOOFING ATÉ A MANIPULAÇÃO POR ENGENHARIA SOCIAL. **Publicações**, 2023.

PEREIRA, C. G. **Phishing: conceitos e ações preventivas aplicadas à empresa**. 2012. TCC – Universidade de Brasília. Disponível em: <https://repositorio.uniceub.br/jspui/handle/235/8136>.

PIOVESAN, L. G. et al. ENGENHARIA SOCIAL: Uma abordagem sobre Phishing. **REVISTA CIENTÍFICA UNIBALSAS**, v. 10, n. 1, p. 45–59, 2019.

RIBEIRO, J. M.; BATISTA, D. M.; PINA, J. C. de. hashify: Uma Ferramenta para Visualizaçao de Hashes com Animaçoes. In: SBC. ANAIS Estendidos do XX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. [S.l.: s.n.], 2020. P. 109–116.

SAHINGOZ, O. K. et al. Machine learning based phishing detection from URLs. **Expert Systems with Applications**, v. 117, p. 345–357, 2019. ISSN 0957-4174. DOI: https://doi.org/10.1016/j.eswa.2018.09.029. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0957417418306067>.

SILVA, F. R. C. Análise prática e mitigação dos riscos da engenharia social na era digital. Instituto Federal de Educação, Ciência e Tecnologia do Piauí, 2023.

SILVA, P. A. L. da. Análise de Redes Sociais aplicada à Engenharia Social, 2012.

SOUZA, C.; LEMOS, M. et al. PhishKiller: Uma Ferramenta para Detecçao e Mitigaçao de Ataques de Phishing Através de Técnicas de Deep Learning. In: SBC. ANAIS Estendidos do XIX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. [S.l.: s.n.], 2019. P. 81–90.

SOUZA, L. C. de; TANAKA, S. S. Estudo sobre ataques de phishing e suas técnicas de defesa. **Revista Terra & Cultura: Cadernos de Ensino e Pesquisa**, v. 39, especial, p. 90–95, 2023.