ISSN 2596-2809

ESTUDO SOBRE ATAQUES DE PHISHING E SUAS TÉCNICAS DE DEFESA

STUDY ON PHISHING ATTACKS AND THEIR DEFENSE TECHNIQUES

Leonardo Correa de Souza[1]
Simone Sawasaki Tanaka[2]

RESUMO

Recentemente no Brasil e no mundo, ataques cibernéticos utilizando engenharias sociais chamados de phishing têm se tornado comuns e acumulado um enorme número de vítimas todos os anos. Durante o período da pandemia, houve uma alta no número de golpes pela internet em território nacional. Com o aumento crescente de pessoas acessando e utilizando a rede para transações com dados sensíveis, os atacantes têm causado enorme prejuízo a pessoas físicas e corporações. Com isso em mente, este trabalho propõe um estudo sobre as principais ferramentas e métodos utilizados na defesa deste tipo de ataque em específico. Para isso, o estudo cataloga os principais vetores de ataque, as características das vítimas mais comuns e os principais meios de defesa disponíveis no mercado. Por fim, foi feito uma avaliação de quais mecanismos de defesa são mais propícios a cada perfil de usuário. Foi concluído que grupos de usuários utilizadores de plataformas específicas como Android e Webmail são vítimas mais expostas a ataques de phishing.

Palavras-chave: engenharia social; ataque cibernético; phishing; proteção de dados

ABSTRACT

Recently in Brazil and in the world, cyber attacks using software engineering so-called phishing scams have become commonplace and amassed a huge number of victims every year. During the period of the pandemic, there was an increase in the number of number of scams on the internet in national territory. With the increasing increase of people accessing and using the network for transactions with sensitive data, the attackers have caused enormous damage to individuals and corporations. Therefore In mind, this work proposes a study on the main tools and methods used in the defense of this specific type of attack. For this, the study catalogs the main attack vectors, the characteristics of the most common victims and the main main means of defense available on the market. Finally, an evaluation of which defense mechanisms are most

[1] Graduando do curso de Ciência da Computação do Centro Universitário Filadélfia - UniFil
[2] Docente do Centro Universitário Filadélfia – UniFil. Departamento de Computação. Londrina – Paraná – Brasil. 86020-000 – simone.tanaka@unifil.br

ISSN 2596-2809

conducive to each user profile. It was con- included that user groups using specific platforms such as Android and Webmail are victims most exposed to phishing attacks.

Keywords: Social engineering; cyber attack; phishing; data protection

1 INTRODUÇÃO

Observando o mundo atual, percebe-se que as pessoas estão conectadas e fazem uso a todo momento da internet em proporções crescentes, utilizando diversos tipos de serviços e transmitindo informações e dados. O ambiente criado pela internet torna a vida das pessoas mais prática, porém traz consigo alguns riscos bem conhecidos como falsidade ideológica, roubo de dados e diversos tipos de fraudes virtuais. Um dos riscos mais comuns é chamado de " Ataque de phishing".

Ataques do tipo phishing são considerados uma engenharia social, sendo esse um determinante do sucesso desse tipo de fraude, pois o fator humano presente nas intervenções criadas por atacantes mal-intencionados podem considerar muitas particularidades. Características como o comportamento dos usuários online, seus tipos de postagens, suas informações pessoais expostas de maneira pública e muitas outras podem ser consideradas, tornando assim a maioria dos usuários suscetíveis a serem possíveis vítimas (DESOLDA et al., 2021).

Diversas empresas e entidades mundo afora tentam de diversas formas orientar usuários a tomar medidas de precaução para se protegerem de fraudes, os informando a não utilizar senhas fáceis, usar a autenticação de dois fatores e se prevenir contra comportamentos suspeitos. Porém, mesmo assim, os números e registros de diversas instituições de métricas informam que o número de ataques e vítimas continua sendo alarmante.

Considerando o constante número de ataques nos últimos anos e a onda de golpes digitais durante o período da pandemia que vem se estendendo até os dias atuais, se faz relevante uma pesquisa focada em formas de defesa contra o phishing. Este trabalho apresenta uma revisão bibliográfica sobre ataques e tipos de phishing, tipos de usuários, métodos de ataque e dados estatísticos. Como objetivo principal, é proposto um estudo sobre as principais técnicas de defesa e mitigação contra o phishing e também sobre os usuários mais afetados. Também é proposto uma análise

ISSN 2596-2809

sobre os tipos de usuários mais suscetíveis a serem alcançados por ataques de phishing.

2 DESENVOLVIMENTO

Para cumprir com os objetivos da pesquisa, é necessário o entendimento dos tipos de ataques existentes atualmente, onde os principais tipos de ataque serão listados a seguir:

Spear-phishing: quando um tipo de alvo específico é escolhido para receber um conteúdo malicioso, como e-mails com links suspeitos, se tratando do tipo mais comum de phishing atualmente Alkhalil et al. (2021). Um grupo de pessoas ou uma organização pode receber, por exemplo, um e-mail contendo um link malicioso, podendo ser direcionado a apenas um grupo pequeno de pessoas ou até mesmo individualmente.

Pharming: ocorre quando há uma tentativa de redirecionar o usuário a um endereço da web malicioso por meio do Domain Name System – Sistema de Nomes de Domínios (DNS). O DNS do dispositivo da vítima é alterado e irá direcioná-la parasites falsos que podem se assemelhar a endereços verdadeiros. A alteração é feita por meio de códigos maliciosos no computador da vítima que podem ter sido obtidos até mesmo por outros ataques de phishings, downloads contaminados na web, ataques direcionados pelo próprio atacante, entre outros (CHAUDHRY; CHAUDHRY; RITTENHOUSE, 2016).

Whaling: são marcados como alvos diretores de grandes empresas ou administradores de contas bancárias com grandes quantidades de dinheiro. Neste tipo de ataque são em pregadas diversas técnicas de engenharia social, normalmente em conjunto, visando fazer as vítimas divulgarem as informações desejadas.

Smishing: é uma modalidade de ataque onde é empregado o uso de mensagens SMS (conhecido como torpedo) ou ligações tendo como alvo aparelhos mobile mais comum hoje em dia sendo aparelhos Android ou IOS.

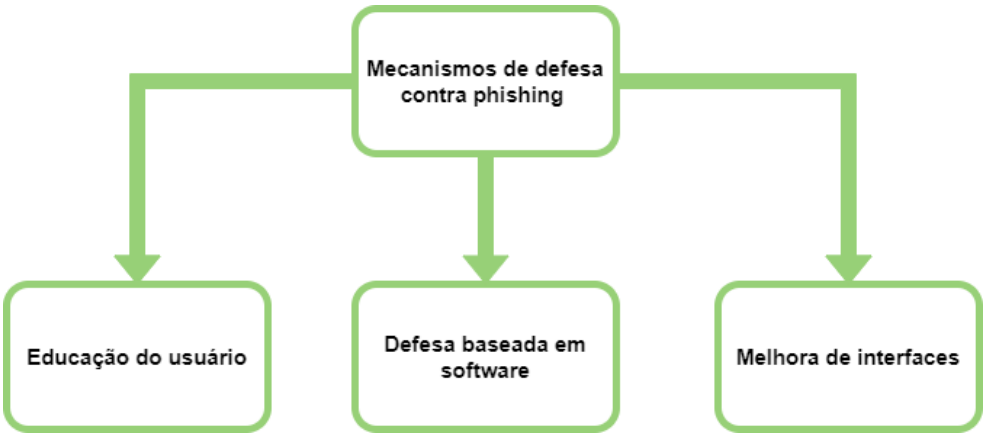
A seguir, será explicado sobre as principais formas de defesa contra o phishing. Na literatura é possível encontrar diversos trabalhos tratando de formas inovadoras de detecção de phishing, porém é difícil chegar a um consenso sobre qual a mais

ISSN 2596-2809

efetiva forma de mitigação. Para Hong (2012), uma combinação entre diversas técnicas é o ideal para se alcançar um alto nível de proteção e resiliência dos internautas e funcionários.

A Figura 1 apresenta um diagrama representando três categorias diferentes de formas de defesa contra o phishing que foram definidas baseados em diversos trabalhos consultados na literatura, sendo as categorias as seguintes: Educação do Usuário, Defesa baseada em software e Melhora de interfaces.

Figura 1 – Mecanismos de defesa



Fonte: Autoria própria

Tendo definido as principais formas de defesa, o outro objetivo principal da pesquisa é definir grupos de usuários mais suscetíveis contra ataques de phishing. A seguir serão listados e explicados os grupos escolhidos com base na revisão bilbiográfica:

Usuário com baixo conhecimento técnico: É importante ressaltar que a educação e o conhecimento de maneiras seguras de navegação na web são práticas que são recomendáveis a qualquer tipo de usuário em qualquer situação. Para esse grupo de usuários em específico, é importante que sejam conscientizados sobre os riscos e também sobre como podem se defender de ataques de phishing.

Usuários de SAAS e Webmail: Campanhas de spear phishing são atualmente um dos tipos de ataques mais perigosos e efetivos de phishing. Para este tipo de usuário é importante ressaltar a importância da aplicação de filtros e de e-mail, blacklists e modos de defesa que evitem ao máximo que o usuário final receba um e-

mail ou acesse uma página de phishing. Isso é evidenciado pois na atual circunstância, é difícil detectar visualmente, ou até mesmo pode passar despercebido o acesso a uma página, ou e-mail de phishing devido a semelhança dos mesmos com versões autênticas.

Usuário mobile: Considerando as particularidades de usuários mobile, é possível identificar que de certa forma a plataforma mesmo sendo um grande alvo, não possui a atenção que deveria para preparar seu usuário a lidar com ataques e golpes. O pouco conhecimento aliado à precariedade de algumas interfaces que são disponibilizadas tornam a ação de hackers ainda mais fácil. Percebe-se, quase que diariamente, que um celular de um usuário comum recebe ligações, SMS e mensagens via aplicativos mensageiros com origens suspeitas.

3 CONCLUSÃO

O estudo demonstrou que o phishing é considerado uma engenharia social, uma técnica utilizada para manipular seres humanos com o objetivo de conseguir informações sem o consentimento dos mesmos, por meio de influência, persuasão e sugestão. Foi relatado que o conceito e a categoria de crimes que são considerados phishing vem sendo alterado e atualizado conforme novas técnicas são desenvolvidas.

Foi possível definir três tipos de usuários mais suscetíveis a ataques de phishing: usuários com baixo nível de conhecimento técnico, utilizadores de SAAS e Webmail e utilizadores de plataformas mobile.

Como trabalhos futuros, propõe-se um estudo mais aprofundado sobre os datasets disponíveis para a criação e teste de novas ferramentas anti-phishing, algo que não foi possível para os autores do presente trabalho devido ao cronograma. Por fim, espera-se com este trabalho auxiliar no combate e prevenção contra o phishing.

REFERÊNCIAS

ALKHALIL, Z. et al. Phishing attacks: A recent comprehensive study and a new anatomy. **Frontiers in Computer Science**, Frontiers Media SA, v. 3, mar. 2021

DESOLDA, G. et al. Human factors in phishing attacks: A systematic literature review. **ACM Comput. Surv., Association for Computing Machinery**, New York, NY, USA, v. 54, n. 8, oct 2021. Disponível em: https://doi.org/10.1145/3469886.

HONG, J. The state of phishing attacks. **Commun. ACM, Association for Computing Machinery**, New York, NY, USA, v. 55, n. 1, p. 74–81, jan. 2012. Disponível em: https://doi.org/10.1145/2063176.2063197.

CHAUDHRY, J.; CHAUDHRY, S.; RITTENHOUSE, R. Phishing attacks and defenses. **International Journal of Security and Its Applications**, v. 10, p. 247–256, 01 2016.

DESOLDA, G. et al. Human factors in phishing attacks: A systematic literature review. **ACM Comput. Surv., Association for Computing Machinery**, New York, NY, USA, v. 54, n. 8, oct 2021. Disponível em: https://doi.org/10.1145/3469886.