FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

Sullivan Matheus Moreira Camargo

ANÁLISE TÉCNICA DE UM PHISHING DE E-MAIL SOB A LUZ DA FERRAMENTA PHISHTOOL

Americana-SP

2023

FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

Sullivan Matheus Moreira Camargo

Análise técnica de um phishing de e-mail sob a luz da ferramenta PhishTool

Projeto de Trabalho de Graduação desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Dr. José Luís Zem

Americana-SP

2023

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana Ministro Ralph Biasi-CEETEPS Dados Internacionais de Catalogação-na-fonte

CAMARGO, Sullivan Matheus Moreira

Análise técnica de um phishing de e-mail sob a luz da ferramenta PhishTool. / Sullivan Matheus Moreira Camargo – Americana, 2023.

33f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Dr. José Luís Zem

1. Correio eletrônico 2. Segurança em sistemas de informação. I. CAMARGO, Sullivan Matheus Moreira II. ZEM, José Luís III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681519
681.518.5

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

SULLIVAN MATHEUS MOREIRA CAMARGO

ANÁLISE TÉCNICA DE UM PHISHING DE E-MAIL SOB A LUZ DA FERRAMENTA PHISHTOOL

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação

Americana, 20 de junho de 2023

Banca Examinadora:

José Luiz Zem (Presidente)
Doutor
Fatec Americana

Henri Alves de Godoy
Doutor
Fatec Americana

Benedito Luciano Antunes de França
Mestre
Fatec Americana

RESUMO

Este trabalho aborda a análise técnica de um *phishing* de e-mail, com o objetivo de fornecer *insights* sobre as principais técnicas utilizadas pelos criminosos e como as empresas podem se proteger desses ataques, a importância de detectar e evitar os ataques de *phishing*, especialmente em um cenário em que as empresas armazenam cada vez mais dados sensíveis em suas redes e sistemas. A análise técnica permite identificar informações como o IP de origem e o verdadeiro e-mail de envio, possibilitando a configuração de medidas para evitar receber futuros e-mails do mesmo atacante e bloquear o domínio utilizado. A metodologia de pesquisa adotada é qualitativa e descritiva, utilizando métodos como pesquisa bibliográfica, pesquisa documental e análise de dados obtidos em publicações especializadas fornecidas pelo Security Blue Team. O objetivo principal é realizar uma análise técnica de um *phishing* de e-mail, coletando informações como endereço de e-mail de envio, endereço do destinatário, data e hora de envio e o IP de origem. A partir dessas informações, serão identificadas ações que as empresas podem adotar para se proteger contra-ataques de *phishing*, fortalecendo sua segurança. A disciplina de Fator Humano no curso de Segurança da Informação, que fornece conhecimentos sobre engenharia social e as técnicas utilizadas por engenheiros sociais para enganar suas vítimas. São abordados os temas de segurança da informação e engenharia social, incluindo a definição de segurança da informação, os três pilares da segurança (confidencialidade, integridade e disponibilidade) e as diversas técnicas utilizadas pelos engenheiros sociais para manipular o comportamento humano. Por fim, o *phishing* como uma das técnicas utilizadas pelos atacantes para obter informações confidenciais. O *phishing* consiste em simulações em que a vítima é atraída ou enganada para acessar links falsos, páginas falsas ou executar arquivos, resultando no furto de dados ou acesso indevido. O aumento dos ataques de *phishing* nos últimos anos destaca a importância de compreender os diferentes tipos de *phishing* e desenvolver estratégias de proteção eficazes. O trabalho também menciona a ferramenta PhishTool, que analisa os metadados relevantes de um e-mail de *phishing* e facilita a triagem de anexos e URLs suspeitos para uma análise mais eficiente e segura.

Palavras-Chave: *Phishing*; Análise técnica; *e-mail*; engenharia social.

ABSTRACT

This work addresses the technical analysis of an email phishing, aiming to provide insights into the main techniques used by criminals and how companies can protect themselves from such attacks. It emphasizes the importance of detecting and preventing phishing attacks, especially in a scenario where companies store increasingly sensitive data in their networks and systems. Technical analysis allows the identification of information such as the source IP and the true sending email, enabling the configuration of measures to prevent receiving future emails from the same attacker and blocking the used domain. The research methodology adopted is qualitative and descriptive, utilizing methods such as literature review, documentary research, and analysis of data obtained from specialized publications provided by the Security Blue Team. The main objective is to conduct a technical analysis of an email phishing, collecting information such as the sending email address, recipient address, date and time of sending, and the source IP. Based on this information, actions that companies can take to protect themselves against phishing attacks will be identified, strengthening their security. The Human Factor discipline in the Information Security course provides knowledge about social engineering and the techniques used by social engineers to deceive their victims. It covers topics such as information security and social engineering, including the definition of information security, the three pillars of security (confidentiality, integrity, and availability), and the various techniques used by social engineers to manipulate human behavior. Finally, phishing is presented as one of the techniques used by attackers to obtain confidential information. Phishing involves simulations where the victim is lured or deceived into accessing fake links, fake pages, or executing files, resulting in data theft or unauthorized access. The increase in phishing attacks in recent years highlights the importance of understanding the different types of phishing and developing effective protection strategies. The work also mentions the PhishTool tool, which analyzes relevant metadata from a phishing email and facilitates the screening of suspicious attachments and URLs for more efficient and secure analysis.

Keywords: *Phishing; Technical analysis; email; social engineering.*

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

INTRODUÇÃO

Nos últimos anos, temos visto um aumento significativo nos ataques de *phishing*, que consistem na tentativa de obtenção de informações confidenciais por meio de engenharia social e outros meios fraudulentos. Em um cenário em que as empresas armazenam cada vez mais dados sensíveis em suas redes e sistemas, é crucial que elas estejam preparadas para detectar e evitar esse tipo de ameaça.

Neste trabalho será abordado como realizar uma análise técnica de um *phishing* de e-mail, podendo responder algumas perguntas que possa ajudar em um cenário real.

Este trabalho tem como objetivo abordar a análise técnica de um *phishing* de e-mail, apresentando algumas das principais técnicas utilizadas pelos criminosos e fornecendo *insights* sobre como empresas podem se proteger desses ataques. Antes de entrar em detalhes sobre a análise em si, será apresentado brevemente o conceito de segurança da informação e seus três pilares, a engenharia social e as principais formas que os criminosos utilizam para conseguir informações confidenciais, bem como os diferentes tipos de *phishing*.

Quais são os possíveis benefícios para uma empresa realizar análises detalhadas de e-mails de *phishing* reportados por usuários, considerando que muitas vezes esses e-mails não são analisados minuciosamente pela equipe de operações de segurança (SOC)?

Com a análise técnica é possível identificar o IP de origem e o verdadeiro e-mail de envio, só com essas informações é possível realizar uma configuração para evitar receber futuros e-mails novamente desse atacante, no caso de bloquear o domínio que o atacante usou pode evitar ataques de outros criminosos utilizando o mesmo domínio.

A metodologia de pesquisa será de abordagem qualitativa e descritiva; os principais métodos serão pesquisa bibliográfica, pesquisa documental e análise de dados, a serem obtidos em publicações especializadas.

O objetivo deste trabalho é realizar uma análise técnica de um phishing de e-mail, coletando informações como o endereço de e-mail de envio, o endereço do destinatário, a data e hora de envio e o IP de origem. Essa análise fornecerá *insights* valiosos sobre esse tipo de ataque.

Além do objetivo geral, realizaremos uma pesquisa bibliográfica para embasar teoricamente o estudo e compreender as melhores práticas de segurança da informação, *phishing* e engenharia social. Também faremos uma pesquisa documental em relatórios técnicos de *phishing* de e-mail, obtendo dados concretos sobre casos reais de ataques e identificando as técnicas utilizadas pelos criminosos.

Com base nas informações coletadas, identificaremos ações que as empresas podem adotar para se proteger contra-ataques de *phishing*. Essa análise permitirá identificar padrões, vulnerabilidades e medidas de mitigação, fortalecendo a segurança das organizações.

Durante este trabalho, a disciplina Fator Humano do curso de Segurança da Informação foi de grande importância, pois permitiu a aquisição de conhecimento sobre engenharia social e as técnicas utilizadas por engenheiros sociais para enganar suas vítimas.

1. REVISÃO BIBLIOGRÁFICA

Neste tópico vamos abordar os temas de segurança da informação e engenharia social. Na seção sobre segurança da informação, é abordada a definição de segurança, a importância da proteção dos sistemas contra ameaças e os três pilares da segurança da informação: confidencialidade, integridade e disponibilidade. Na seção sobre engenharia social, é explorado o conceito e a história dessa tática, bem como seu crescente uso com o avanço da tecnologia. Na seção sobre *Phishing*, é discutido como o *phishing* pode ser realizado de várias maneiras, como e-mails de *phishing*, sites falsos e mensagens de texto. Também é mencionado como os cibercriminosos utilizam técnicas de persuasão, como urgência e medo, para induzir os usuários a fornecerem suas informações pessoais.

1.1 Segurança da Informação

A segurança da informação é um tema cada vez mais relevante no mundo atual, uma vez que as empresas e organizações dependem cada vez mais de sistemas de informação para armazenar e gerenciar informações importantes e confidenciais.

De acordo com o dicionário de Oxford Languages (2022), segurança significa “estado, qualidade ou condição de quem ou do que está livre de perigos, incertezas, assegurado de danos e riscos eventuais; situação em que nada há a temer.” Por sua vez, informação é o “conjunto de conhecimentos reunidos sobre determinado assunto ou pessoa”.

Segundo a norma ISO/IEC 17799:2000

> segurança da informação pode ser definida como a proteção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de possibilidades e investimentos.

Para garantir a segurança da informação, é preciso preservar os princípios básicos da informação, que são os três pilares da segurança da informação: confidencialidade, integridade e disponibilidade (CID) (ISO/IEC 17799:2000).

A confidencialidade é o primeiro pilar da segurança da informação e garante que apenas as pessoas autorizadas tenham acesso à informação. Isso significa que é necessário adotar medidas para evitar que pessoas não autorizadas tenham acesso a informações sensíveis ou confidenciais da empresa.

O segundo pilar é a integridade, que garante a completa e correta representação da informação. Isso significa que a informação não pode ser alterada por pessoas não autorizadas ou de forma acidental, e que deve estar disponível exatamente como foi enviada. É importante adotar medidas de controle e monitoramento para garantir que a integridade da informação seja preservada.

O terceiro pilar da segurança da informação é a disponibilidade, que garante que a informação esteja acessível quando necessário. Isso significa que é preciso adotar medidas para evitar interrupções nos serviços de informação e garantir que a informação esteja disponível para as pessoas autorizadas sempre que elas precisarem. A disponibilidade é afetada pela confidencialidade e integridade, uma vez que qualquer alteração nos mecanismos de controle desses pilares pode afetar a disponibilidade da informação. Portanto, é importante garantir que esses pilares trabalhem juntos de forma integrada para garantir a segurança da informação da empresa.

Galvão (apud ZANELLA, 2017, p.18) afirma que “a segurança da informação tem como objetivo a proteção dos sistemas contra a alteração e invasão dos dados por pessoas não autorizadas”. A segurança da informação é crucial, especialmente em tempos de guerra. Há muitos anos, reis infiltravam seus soldados em outros reinos para obter informações que os ajudassem em alguma estratégia. A informação poderia ser transmitida por pessoas ou por pombo-correio, e a chance de interceptação dessas mensagens poderia ser grande. No entanto, naquela época, eles já utilizavam métodos para que, caso alguém interceptasse a informação, não a entendesse, como a cifra de César. Podemos dizer que as mensagens eram criptografadas. Portanto, fica claro a importância da Confidencialidade, Integridade e da Disponibilidade na segurança da informação, pois eles já o utilizavam de forma indireta para garantir a segurança da informação.

1.2 Engenharia Social

Apesar do termo “engenharia social” estar se popularizando recentemente essa tática já é utilizada há muito tempo. Podemos utilizar como exemplo a famosa história de Adão e Eva, que Eva foi manipulada pela serpente para desfrutar do fruto proibido, no livro de Gênesis. Esse ato de manipular alguém para realizar algo é o termo, engenharia social, que que será abordado e explicado com maiores detalhes.

Segundo Mitnick (2003, p. 4) “A engenharia é a arte de manipular pessoas, a fim de obter informações sigilosas sem que percebam que estão sendo vítimas de um engenheiro social”.

Com o crescente avanço da tecnologia, os profissionais de segurança da informação, desenvolvem mais tecnologias relacionado a segurança, fazendo com que a engenharia social seja mais estudada e visada por pessoas mal-intencionadas, pois as formas de conseguir algumas informações sigilosas ocorre sendo menos trabalhosa, do que tentar aprender muitas ferramentas e habilidades técnicas para localizar algumas vulnerabilidades. Com isso, percebe que é mais fácil de enganar um humano, em vez de uma máquina.

A engenharia social é um campo de estudo que explora a maneira como o comportamento humano pode ser manipulado para levar uma pessoa a agir de acordo com a vontade do manipulador. Portanto, existe inúmeras técnicas que os engenheiros podem utilizar, para realizar essas técnicas há um método para se desenvolver e aplicar. De acordo com Mitnick (2003, p.264), “a engenharia social tem um ciclo baseado em quatro ações: pesquisa, desenvolvimento da credibilidade e da confiança, exploração da confiança e utilização das informações”.

A ação pesquisa, a primeira do ciclo, é quando o engenheiro social faz busca do alvo e coleta suas informações, podendo ser com terceiros sem contato direto com a vítimas ou mesmo pelas próprias redes sociais. Tendo as informações será possível manter contato com a vítimas sem levantar suspeita.

O desenvolvimento da credibilidade e da confiança, esse é o momento que o engenheiro aplica todas as informações que obteve com a primeira ação. Fingindo ser outra pessoa, buscando ajuda e explorando afinidades cita as informações obtidas com as redes sociais, assim conseguindo a confiança das vítimas.

As explorações da confiança, já com a confiança da vítima a pessoa mal-intencionada começa a pedir informações, ações que a vítima poderá fazer para ele e

podendo até manipulá-la a pedir ajudar, assim a vítima ficará “devendo uma” para o engenheiro.

A utilização das informações, agora o engenheiro irá utilizar as informações obtidas como desejar, como credenciais para acesso em algum lugar, acesso em sites, dados de cartão, entre outros. Caso as informações são apenas uma etapa para um objetivo final, o engenheiro irá refazer as etapas anteriores até que consiga o objetivo final (MITNICK, 2003).

A *Information System Audit and Control Association* 4 (ISACA), em sua publicação ‘O estado de segurança cibernética: implicações para 2016’, realizada com profissionais certificados na área de segurança da informação, apresenta os tipos de ataques mais frequentes nas organizações, que são combatidos rotineiramente por esses profissionais: a saber: roubo *on-line* de identidade, *hacking*, códigos maliciosos, roubo de propriedade intelectual, danos intencionais aos sistemas de informática, perdas físicas, *phishing* e negação de serviços

1.3 Phishing

Phishing é umas das técnicas que o atacante pode utilizar para obter suas informações. De acordo com Pinheiro (2020),

> O *Phishing*: consiste em uma simulação, na qual a vítima é atraída ou enganada para que, pensando se tratar de um conteúdo legítimo, clique em um link falso, acesse uma página falsa ou execute algum arquivo para que haja furto de dados ou acesso a elevação de privilégios. É uma técnica de engenharia social.

Nos últimos anos, temos observado um aumento significativo nos ataques de *phishing*, que consistem em tentativas de obtenção de informações confidenciais por meio de engenharia social e outros métodos fraudulentos. O *phishing* se manifesta de várias formas, sendo importante compreender cada uma delas para uma melhor proteção contratais ameaças. A Tabela 1 apresenta alguns exemplos de tipos de *phishing*, suas características e os métodos utilizados pelos criminosos. Essas informações são fundamentais para entender a complexidade desses ataques e desenvolver estratégias eficazes de proteção.

Quadro 1 - Tipos de *Phishing*

Tipo de phishing	**Onde ocorre**	**Principais focos**
Scam	Links e arquivos maliciosos	Usuário final
Blind Phishing	Links e arquivos maliciosos com disparos feitos aleatoriamente	Usuário final
Spear Phishing	Links e arquivos maliciosos	Usuário final (funcionários públicos, clientes de empresas) Empresas e bancos
Clone Phishing	Sites clonados	Usuário final
Whaling	Links e arquivos maliciosos	Usuário de alto poder executivo
Vishing	Ligações telefônicas e SMS	Usuário final
Pharming	Link redirecionando para um site falso	Usuário final Empresas
Smishing	SMS	Usuário final
Engenharia Social	Ataques interpessoais	Usuário final

Fonte: SALVIANO et al (2021).

Uma forma comum de *phishing* é o *scam*, que tem como objetivo enganar as pessoas e conseguir obter informações pessoais, financeiras ou confidenciais. Geralmente, os golpes de "*scam*" são realizados por meio de e-mails, mensagens de texto, telefonemas ou até mesmo através de redes sociais.

Os criminosos geralmente se passam por empresas ou organizações confiáveis, como bancos, lojas online ou sites de leilão, e tentam enganar as vítimas para que elas forneçam informações confidenciais, como senhas, números de cartão de crédito ou informações bancárias. Eles podem também criar falsos anúncios de emprego, concursos ou sorteios para atrair as vítimas.

Os golpistas também podem oferecer produtos ou serviços falsos ou de má qualidade, com preços muito baixos para atrair pessoas que buscam por uma oferta tentadora. Eles geralmente pedem para as vítimas fazerem o pagamento adiantado ou fornecerem informações financeiras para processar o pagamento (SOUZA, 2023).

Seguindo a tabela, outra forma de *phising* é o *Blind phishing*, que consiste no envio massivo de e-mails falsos para destinatários aleatórios, sem que os criminosos tenham informações específicas sobre as vítimas. Geralmente, esses e-mails são genéricos e não apresentam informações personalizadas, mas são projetados para

parecerem legítimos o suficiente para que a vítima clique em links maliciosos ou forneça informações pessoais.

Um exemplo de *Blind Phishing* pode ser o envio de um e-mail em massa que se passa por um banco conhecido, pedindo para a vítima clicar em um link para atualizar suas informações de conta. Esse link pode direcionar a vítima para uma página falsa que imita o site legítimo do banco, onde a vítima é solicitada a fornecer suas informações pessoais, como nome de usuário, senha e informações de cartão de crédito.

Esse tipo de ataque é particularmente perigoso, porque pode atingir uma ampla gama de pessoas sem que os criminosos tenham que se esforçar para reunir informações específicas sobre cada vítima. Além disso, como os e-mails são enviados aleatoriamente, é mais difícil para as equipes de segurança identificarem e bloquearem esses ataques com eficácia (SILVAA, 2022).

O *Spear Phishing* é um tipo de ataque direcionado a um grupo específico de usuários, como uma empresa, instituição ou até mesmo um indivíduo. Geralmente, o atacante pesquisa informações sobre o alvo para personalizar o e-mail de phishing de forma a torná-lo mais convincente. Essas informações podem ser encontradas em redes sociais, fóruns ou até mesmo em vazamentos de dados. O objetivo do ataque é obter informações confidenciais, como senhas, dados bancários ou informações corporativas.

O *Spear Phishing* pode ser considerado ainda mais perigoso do que outros tipos de *phishing*, pois é mais difícil de detectar. A personalização dos e-mails torna-os menos suspeitos e mais propensos a serem abertos e lidos pelo alvo. Além disso, muitas vezes o atacante usa técnicas de engenharia social para obter informações adicionais do alvo (GHAZAL, 2015).

O *Clone* P*hishing* envolve a criação de uma réplica de um site legítimo para enganar os usuários a inserir suas informações pessoais e de login. O ataque começa com o hacker criando uma cópia idêntica de um site legítimo, como um banco ou uma rede social, com o objetivo de fazer com que o usuário pense que está acessando o site real.

Uma vez que o site clone é criado, o hacker envia e-mails ou mensagens de texto que parecem ser legítimas, mas contêm um link para o site clone. Quando o usuário clica no link, ele é direcionado para o site clone, onde é solicitado a inserir

suas informações pessoais e de login. Essas informações são então roubadas pelo hacker para serem usadas em atividades maliciosas.

Para se proteger do Clone *Phishing*, é importante verificar sempre se o URL do site é o correto e se a conexão é segura antes de inserir suas informações pessoais e de login. Além disso, é importante estar atento a e-mails ou mensagens de texto suspeitos e nunca clicar em links ou baixar anexos de remetentes desconhecidos (SILVA, 2023).

O *Whaling* é um tipo de ataque direcionado a indivíduos de alto escalão em uma organização, como executivos, diretores e gerentes, em vez de se concentrar em indivíduos aleatórios. Nesse tipo de ataque, o criminoso cibernético se passa por um colega de trabalho, cliente ou parceiro de negócios confiável do destinatário, usando informações obtidas por meio de engenharia social para criar uma mensagem de *phishing* personalizada e convincente. A mensagem pode solicitar informações confidenciais, como senhas, informações bancárias ou informações de cartão de crédito, ou pode conter um link malicioso que, quando clicado, instala malware no computador da vítima.

Para evitar *Whaling*, é importante que as empresas implementem uma forte cultura de segurança cibernética e treinem seus funcionários para reconhecer os sinais de *phishing*. Os funcionários devem ser incentivados a verificar cuidadosamente as mensagens suspeitas, verificando o remetente e a URL do link antes de clicar em qualquer coisa ou fornecer informações confidenciais (SOUZA, 2023).

Além desses tipos de *phishing*, existem outras técnicas utilizadas pelos criminosos. O V*ishing*, por exemplo, utiliza chamadas telefônicas para obter informações pessoais e financeiras das vítimas.

Os criminosos que aplicam o *Vishing* geralmente se passam por representantes de empresas ou instituições financeiras, e usam informações falsas ou roubadas para convencer as vítimas a fornecer informações pessoais, como senhas, números de cartão de crédito e dados bancários.

Para se proteger do *Vishing*, é importante estar atento aos cuidados básicos de segurança, como não fornecer informações pessoais ou financeiras por telefone e desconfiar de ligações inesperadas, principalmente aquelas que pedem informações sensíveis. É importante lembrar que empresas sérias e instituições financeiras nunca solicitam informações pessoais ou financeiras por telefone (SILVA, 2023).

Já o *Pharming* envolve o redirecionamento do tráfego da internet de um site legítimo para um site fraudulento. Esse tipo de ataque pode ser realizado de várias maneiras, como a exploração de vulnerabilidades em servidores de DNS, o uso de malware para modificar as configurações de DNS em computadores infectados, ou a criação de sites fraudulentos que se parecem com sites legítimos, mas têm um endereço de IP diferente.

Um exemplo comum de *pharming* é o redirecionamento de usuários de um site bancário para um site fraudulento que se parece com o site legítimo, mas que é projetado para roubar informações de login e senhas (SOUZA, 2023).

Por fim, o S*mishing* utiliza mensagens de texto para enganar as vítimas, levando-as a inserir informações pessoais em páginas falsas (SOUZA, 2023).

É essencial estar ciente dessas técnicas de *phishing* e adotar medidas de segurança adequadas para proteger-se contra esses ataques. Manter-se atualizado sobre as ameaças e educar os usuários sobre as práticas seguras na internet são ações fundamentais para mitigar os riscos de *phishing* (SILVA, 2023).

2. DESENVOLVIMENTO

Neste tópico será abordado a ferramenta *PhishTool* para análise de ameaças cibernéticas. Na seção 3.1, é feita uma apresentação do *PhishTool*, sua funcionalidade e como pode ajudar a identificar possíveis ameaças cibernéticas. Na seção 3.2, é abordada a análise de *phishing* de e-mail utilizando o *PhishTool*, e são apresentadas etapas para analisar a autenticidade de um e-mail, incluindo a verificação do endereço de e-mail do remetente, a análise de cabeçalhos e a verificação do IP do remetente e destinatário.

2.1 PhishTool

PhishTool é uma ferramenta que analisa os metadados relevantes de um e-mail de *phishing*, fornecendo uma visão técnica abrangente e detalhada que ajuda a identificar possíveis ameaças cibernéticas. Além disso, a ferramenta possui um navegador seguro que facilita a triagem dos anexos e URLs suspeitos em uma única tela, tornando a análise de *phishing* mais eficiente e segura.

Durante a pesquisa, identificamos a ferramenta PhishTool, foi verificada que aborda todos os pontos necessários do *phishing* de forma simples e visível. Por esse motivo, optamos por selecionar essa ferramenta para auxiliar na análise.

Segundo o Phishtool (2023):

> Criado por analistas de segurança frustrados com a abordagem falsa de *phishing* de produtos de segurança de e-mail legados. O PhishTool existe para enfrentar o problema do *phishing* desde os primeiros princípios, porque as soluções fornecidas pelo setor de segurança até agora eram lamentavelmente insuficientes, até agora.

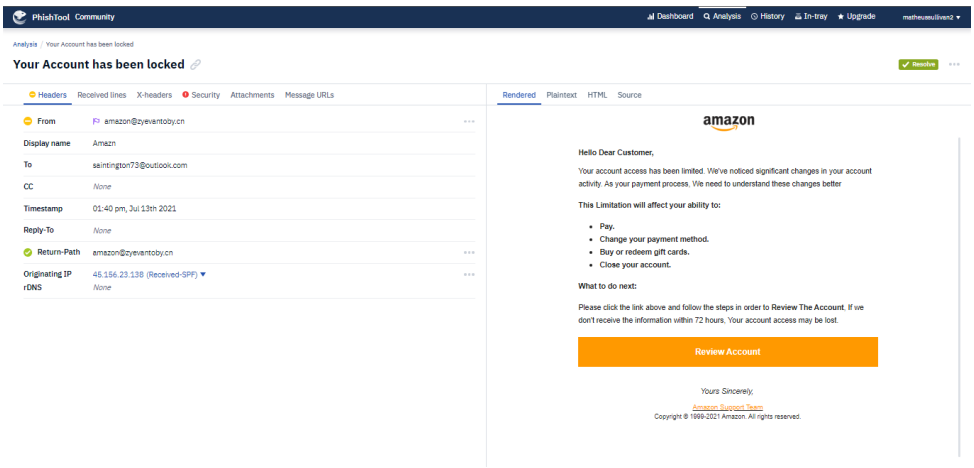
2.2 Análise do Phishing de e-mail

Após a apresentação do PhishTool, ferramenta selecionada para a realização da análise de *phishing* em questão, podemos prosseguir com o processo de análise. Para utilizar a ferramenta, é necessário salvar o e-mail suspeito em formato de arquivo. No Outlook, para realizar o download do e-mail suspeito, é necessário seguir alguns passos. Primeiramente, abra o e-mail na caixa de entrada. Em seguida, localize os "três pontinhos" ou o ícone de "mais opções" dentro do e-mail. Ao clicar nessa opção, será exibida uma lista de ações adicionais. Nessa lista, procure pela opção "Transferir" ou "Baixar" e selecione-a. Dessa forma, o Outlook iniciará o

download do arquivo associado ao e-mail, que geralmente é um arquivo com extensão .eml. Já no Gmail, é o mesmo processo, porém na lista de ações adicionais há uma opção “Fazer o *download* da mensagem” também é um arquivo com extensão .eml.

Após realizar o *download* do e-mail suspeito é necessário criar uma conta no site do PhishTool. Em seguida, basta fazer o upload do arquivo na plataforma, que redirecionará o usuário para a tela de análise, conforme ilustrado abaixo:

Figura 1 - PishTool



Fonte: PhishTool (2023)

Como mencionado anteriormente, os cibercriminosos usam táticas de *phishing* apelando para assuntos urgentes que chamam a atenção do usuário. Neste exemplo de e-mail, na Figura 1, o assunto é "Sua conta foi bloqueada", o que pode gerar preocupação. Além disso, o corpo do e-mail apresenta uma boa estrutura em HTML, o que pode aumentar a credibilidade percebida pelo destinatário.

No entanto, para evitar cair em um golpe, é importante fazer algumas perguntas iniciais:

- Quem é o remetente do e-mail?
- O endereço de e-mail é oficial da Amazon ou outra empresa mencionada no e-mail?

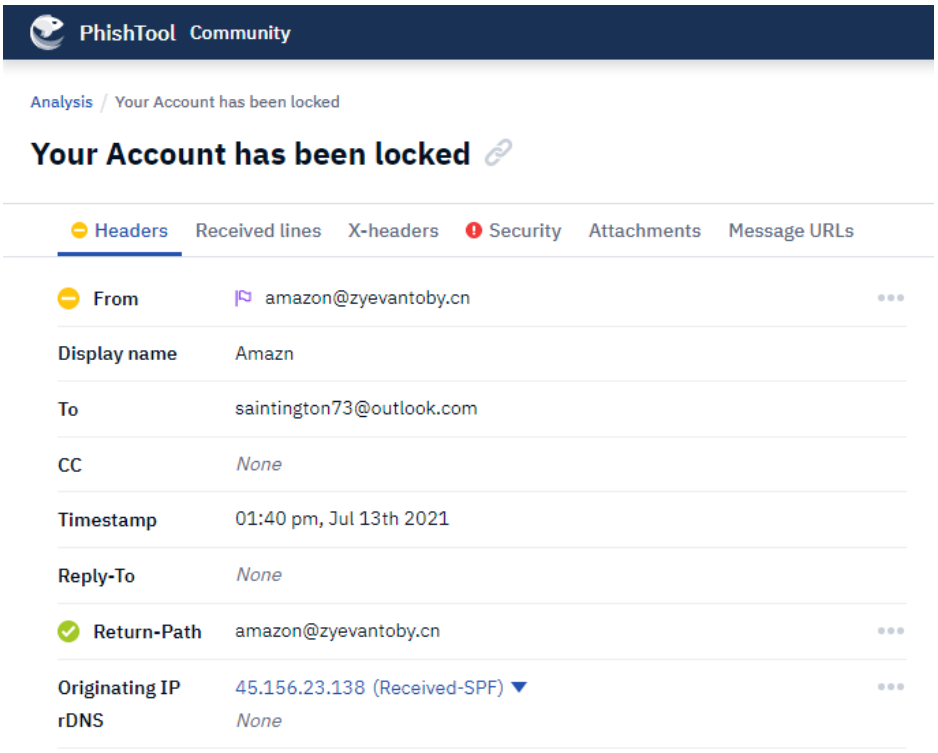
Sempre verifique o corpo do e-mail para identificar por qual empresa os golpistas estão tentando se passar.

No estudo realizado, foi utilizado um arquivo de phishing de e-mail disponibilizado pelo Blue Team Labs (Security Team Training Ltd) como um exemplo

representativo. Esse arquivo, intitulado 'Phishing Email, foi analisado minuciosamente para identificar as principais técnicas utilizadas pelos atacantes.

Para verificar as informações mencionadas anteriormente, vamos utilizar o PhishTool.

Figura 2 - Headers PhishToll



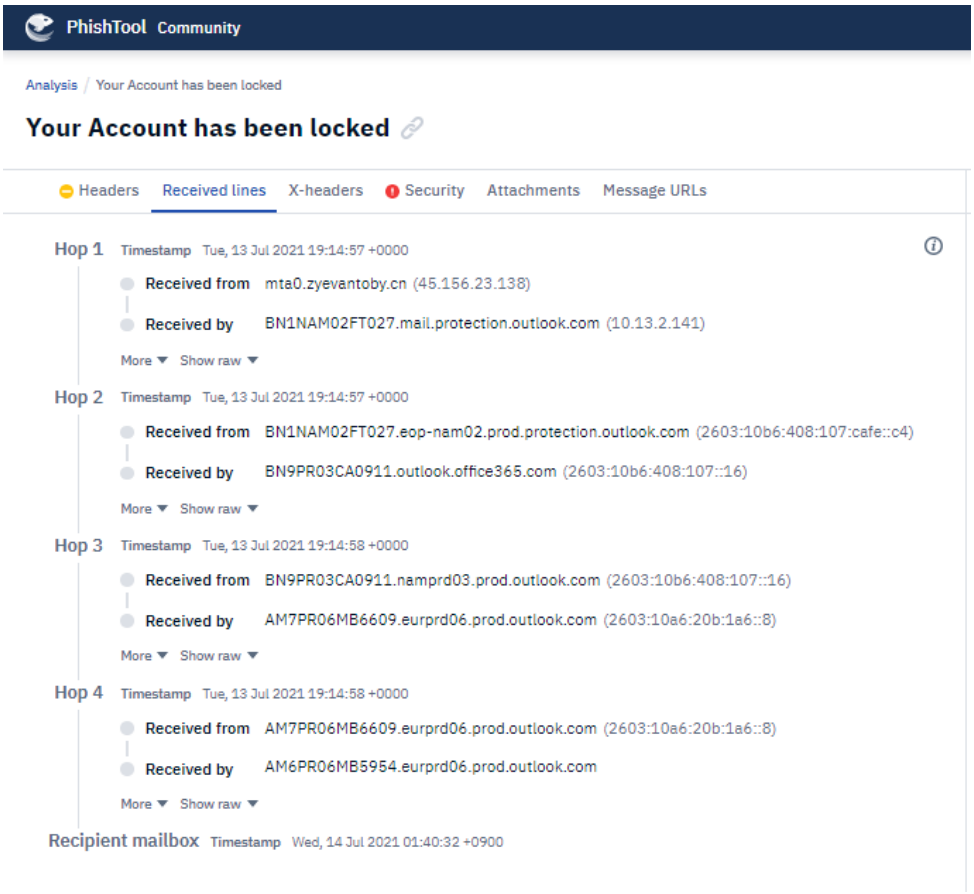
Fonte: PhishTool (2023)

De acordo com a Figura 2, ao verificar o campo "*From*" do e-mail de *phishing* em questão, foi identificado o endereço de e-mail "amazon@zyevantoby.cn". É importante observar que a presença da palavra "amazon" no endereço de e-mail não é suficiente para torná-lo válido. O que realmente importa é o domínio após o símbolo "@". O domínio oficial da Amazon é "@amazon.com" e não pode ser copiado e utilizado por qualquer pessoa, somente por funcionários autorizados pela empresa.

Embora a identificação do domínio já permita marcar o e-mail como "*SPAM*", é fundamental analisar outros detalhes relevantes para uma análise mais técnica.

Na figura 3, trata-se apenas das rotas pelas quais o e-mail percorreu até chegar ao destinatário.

Figura 3 - Rotas PhishTool



Fonte: PhishTool (2023)

Seguindo a definição da RFC 1154, que é uma publicação de documentos que descreve propostas ou padrões técnicos para a Internet, as RFCs são produzidas e divulgadas pelo Internet Engineering Task Force (IETF) e outras entidades interessadas em estabelecer padrões abertos para a Internet. Conforme a RFC, as palavras-chave que começam com "X-" são permanentemente reservadas para uso específico de implementações.

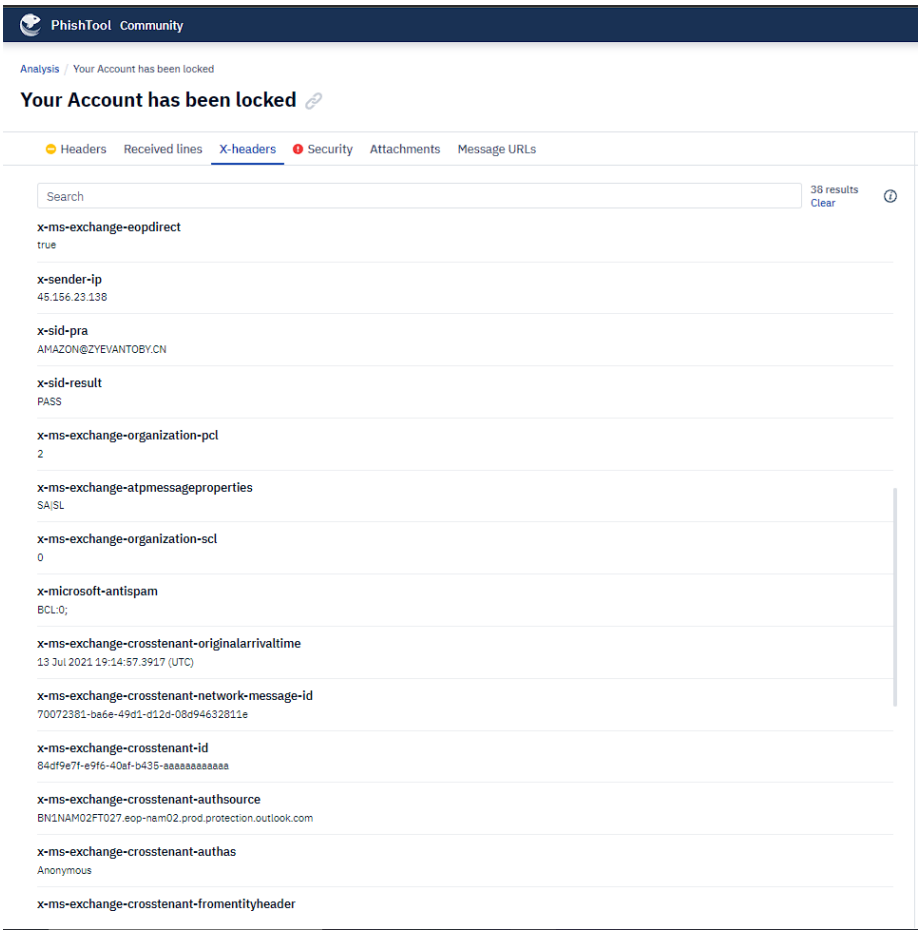
No contexto de e-mails, os cabeçalhos que iniciam com o prefixo "X-" têm sido amplamente empregados por servidores SMTP e aplicativos de e-mail para ler e registrar informações diversas de um e-mail. Esses cabeçalhos adicionais são utilizados para fornecer dados relevantes e auxiliar em várias funcionalidades. Por exemplo, é comum que gateways de segurança de e-mail e outros serviços intermediários adicionem cabeçalhos "X-" para registrar os resultados da verificação de segurança, como pontuações de spam e outras informações pertinentes.

A inclusão desses cabeçalhos "X-" é uma prática comum para complementar as informações básicas de um e-mail e registrar dados adicionais que podem ser

relevantes para a análise e o gerenciamento de mensagens. Essas informações podem ser utilizadas para identificar a origem do e-mail, rastrear possíveis ameaças de segurança ou fornecer métricas para avaliar a eficácia de políticas de segurança.

Na Figura 4, apresentada abaixo, podemos visualizar um exemplo ilustrativo dos cabeçalhos "X-" em um e-mail:

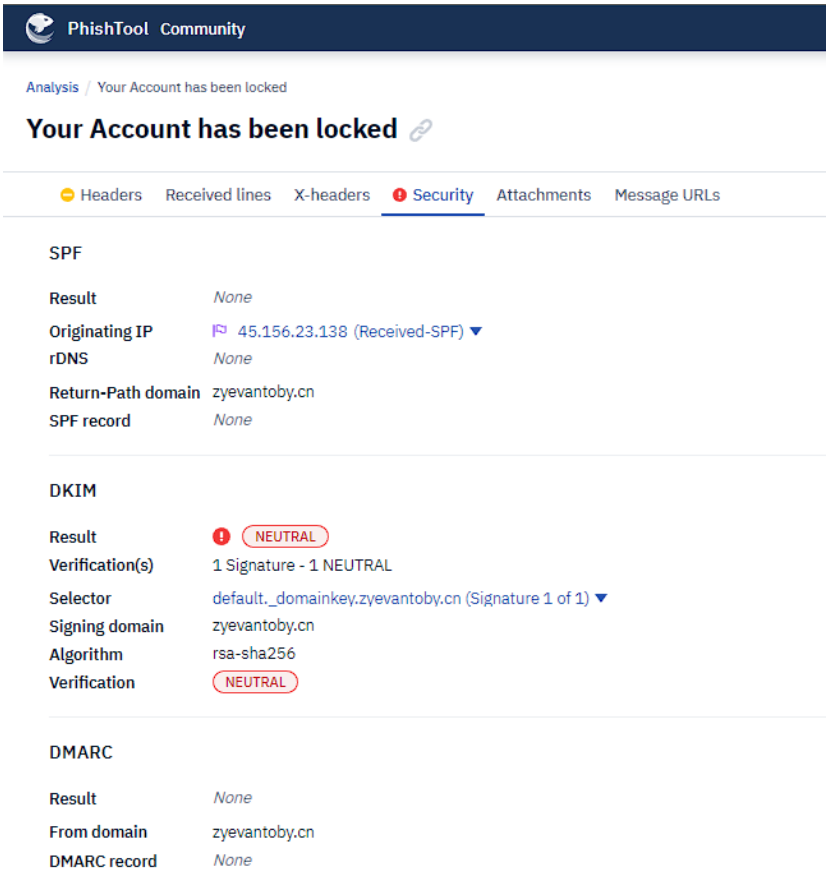
Figura 4 - X-Headers



Fonte: PhishToll (2023)

É importante ressaltar que a utilização desses cabeçalhos adicionais não é padronizada e pode variar entre diferentes servidores de e-mail e aplicativos. Portanto, é essencial ter em mente que a interpretação e o uso desses cabeçalhos "X-" podem variar de acordo com a implementação específica de cada sistema.

Figura 5 - Security



Fonte: PhishTool (2023)

Nesta seção, na Figura 5, é possível verificar alguns critérios importantes para garantir a segurança de e-mails. Na primeira parte, é verificado o IP do remetente e do destinatário para garantir que ambos sejam válidos e correspondam ao domínio da empresa que o e-mail se passa.

De acordo com a PhishTool (2023), a falsificação do endereço de e-mail "Return-Path" é possível para fins maliciosos. Um adversário pode falsificar o "Return-Path" com um endereço de e-mail localizado em um domínio controlado por eles e publicar um registro SPF legítimo nos registros de recursos DNS TXT desse domínio. Isso passaria por uma verificação SPF, enquanto o endereço de e-mail "De" (RFC5322.From) foi falsificado e desmarcado.

Quanto à segunda seção, que aborda o DKIM, é importante observar que existem dois sinais de alerta como "NEUTRAL" no PhishTool, o que significa que o hash do corpo da mensagem não foi verificado.

DKIM (*DomainKeys Identified Mail*) é um mecanismo de autenticação de e-mail que utiliza criptografia de chave pública para verificar a integridade de um e-mail e garantir que ele realmente tenha sido enviado pelo domínio alegado como remetente.

Quando um servidor de e-mail envia uma mensagem, ele adiciona uma assinatura digital criptografada com a chave privada do domínio de assinatura ao cabeçalho do e-mail. Ao receber a mensagem, o servidor de destino pode verificar a assinatura digital recuperando a chave pública do domínio de assinatura a partir de seus registros DNS e usando-a para descriptografar a assinatura digital.

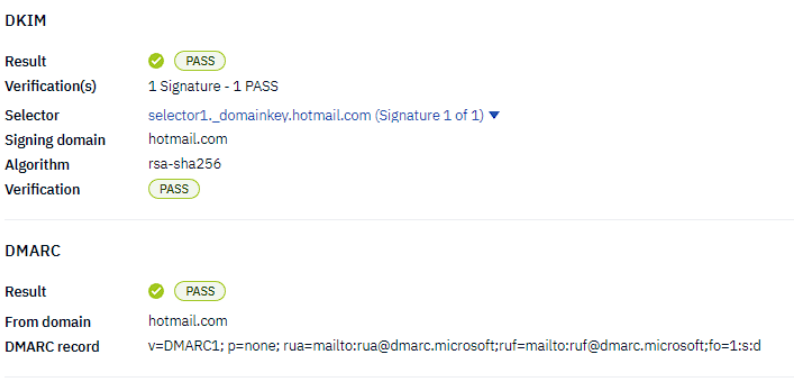
Se a assinatura for válida e a mensagem não tiver sido modificada em trânsito, a mensagem é considerada autenticada e pode ser confiável. Em outras palavras, o DKIM ajuda a evitar que mensagens falsas ou fraudulentas sejam enviadas em nome de um domínio de remetente legítimo.

A implementação do DKIM é relativamente simples e pode ser feita pelos administradores de domínio em seus servidores de e-mail. O DKIM é amplamente adotado por grandes provedores de e-mail, como Google, Yahoo e Microsoft, e é uma das principais medidas de segurança de e-mail usadas hoje. A especificação DKIM é definida em RFC6376 (Croker, et al 2011).

É importante ressaltar que a implementação do DKIM é simples. Além disso, a verificação do DKIM é fundamental, pois, se o remetente estiver com o domínio válido da empresa que o e-mail se passa e o mecanismo DKIM não estiver validado, o e-mail pode ter sido modificado em trânsito.

Quando os módulos SPF e DKIM explicados anteriormente retornarem com aprovação, e as verificações de alinhamento forem aprovadas, o DMARC será aprovado. Conforme a figura 6 abaixo:

Figura 6 - DMARC Validado



Fonte: PhishTool (2023)

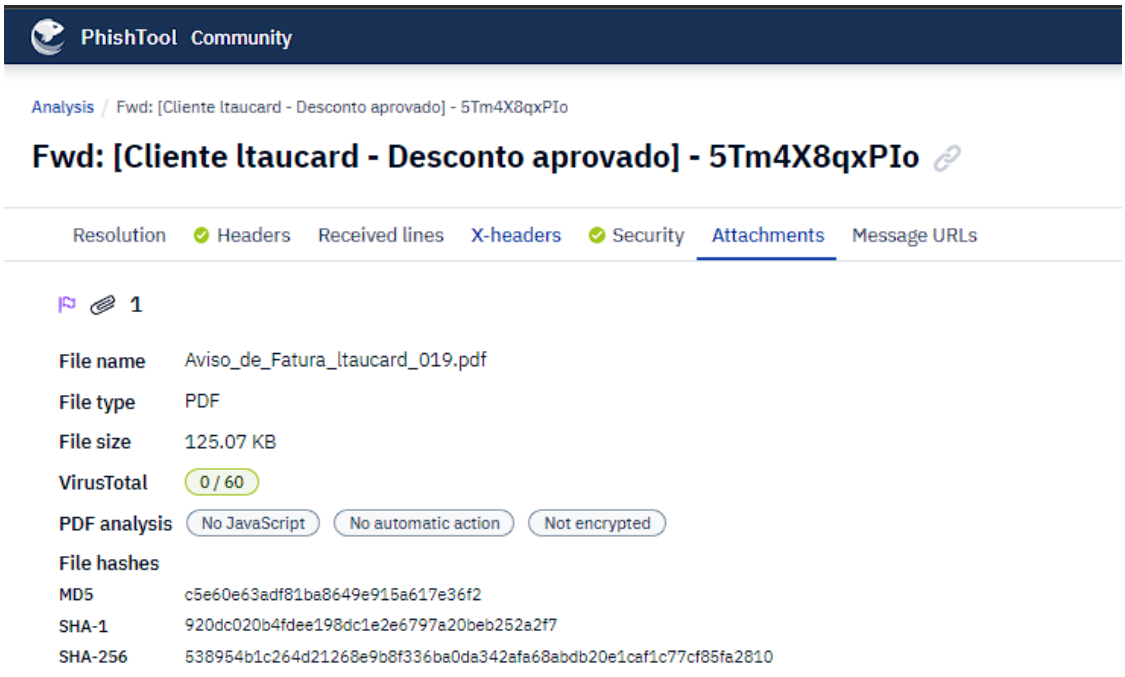
O DMARC atua como um mecanismo de política que permite aos remetentes especificar como seus e-mails devem ser autenticados e como os servidores de e-mail devem lidar com mensagens que não atendem aos critérios de autenticidade estabelecidos. Ele combina as informações do SPF e do DKIM para determinar se um e-mail é autêntico ou não.

Quando um e-mail passa pelas etapas de autenticação do SPF e DKIM com sucesso e as verificações de alinhamento são aprovadas, o DMARC considera o e-mail autenticado e alinhado. Isso significa que o remetente e o domínio do e-mail são confirmados como legítimos e que as mensagens não foram adulteradas ou modificadas durante o trânsito.

Essa validação do DMARC é fundamental para fortalecer a segurança e a confiança nas comunicações por e-mail. Ao implementar corretamente as políticas do DMARC, os remetentes podem garantir que suas mensagens sejam autenticadas e que qualquer tentativa de falsificação seja identificada e tratada de acordo com a política estabelecida.

Comprovando que o e-mail foi enviado pelo domínio. Abaixo, é possível verificar um exemplo de validação do DMARC, comprovando que o e-mail foi enviado de um domínio da Hotmail.

Figura 7 - Anexos



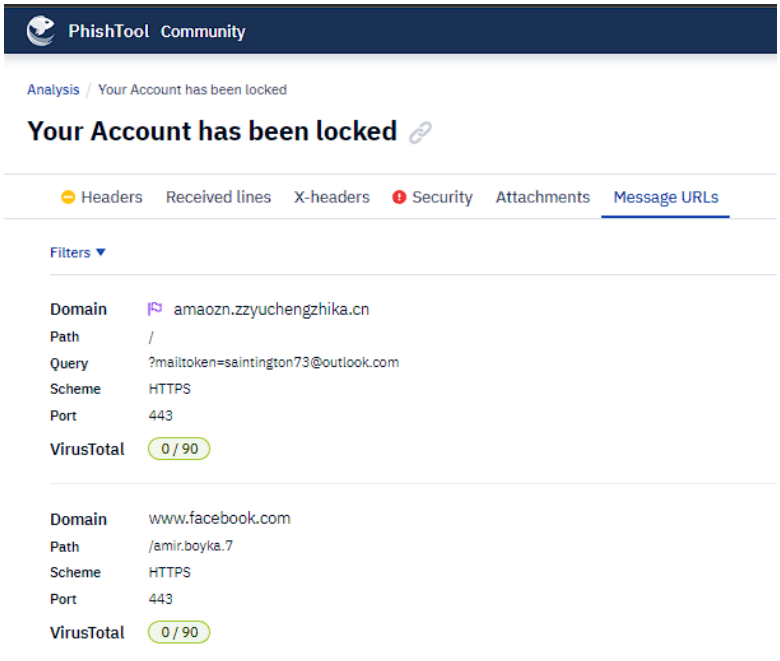
Fonte: PhishTool (2023)

Nesta Figura 7, foi realizado o uso de outro e-mail que continha um arquivo anexado para análise. A ferramenta PhishTool verifica se há algum código malicioso em JavaScript, ações automatizadas ou encriptação.

A atenção deve ser redobrada em relação ao pagamento de faturas por meio de e-mails, pois mesmo que não haja a presença de códigos maliciosos, existe o risco de o pagamento não ser direcionado para a empresa que o e-mail supostamente representa. É importante estar ciente de que os criminosos cibernéticos podem tentar induzir a vítima a realizar o pagamento em uma conta fraudulenta, que está sob o controle dos atacantes. Portanto, é fundamental verificar cuidadosamente as informações de pagamento, tais como dados bancários e informações de contato, antes de realizar qualquer transação financeira em resposta a um e-mail. Além disso, é recomendável que sejam adotados mecanismos de segurança, como a autenticação de dois fatores, para minimizar o risco de fraude.

Para realizar a verificação do arquivo através do VirusTotal, é necessário criar uma conta no VirusTotal, copiar a "*API KEY*" e, em seguida, acessar as configurações do PhishTool, integrando a conta do VirusTotal através da opção "VirusTotal *API*". Dessa forma, é possível obter uma análise mais completa e confiável do arquivo anexado ao e-mail.

Figura *8* - URLs



Fonte: PhishTool (2023)

Para finalizar, a Figura 8, é importante destacar que o PhishTool também realiza a análise de URLs contidas nos e-mails, verificando se elas são maliciosas ou não. Essa análise é realizada por meio do VirusTotal, que verifica se a URL contém códigos maliciosos ou se ela é conhecida por ser utilizada em golpes virtuais.

É fundamental salientar que as URLs presentes nos e-mails devem ser analisadas com cuidado, pois muitas vezes elas podem direcionar o usuário a sites falsos, que visam roubar informações pessoais e financeiras. Portanto, a análise realizada pelo PhishTool é de extrema importância para garantir a segurança das informações dos usuários.

Para realizar a verificação pelo VirusTotal é necessário criar uma conta no VirusTotal, copiar sua “API KEY” e depois ir em Configurações, integrações e VirusTotal API no PhishTool. É importante destacar que essa verificação deve ser feita sempre que houver suspeita de fraude ou *phishing*, a fim de evitar possíveis ataques virtuais.

3. RESULTADOS E DISCUSSÃO

A análise de e-mails suspeitos é uma prática importante na prevenção de ameaças cibernéticas. O PhishTool é uma ferramenta que oferece uma visão técnica abrangente e detalhada, permitindo uma análise mais eficiente e segura.

No exemplo analisado, o PhishTool mostrou-se útil para identificar possíveis ameaças. A partir do upload do arquivo, a plataforma redirecionou o usuário para a tela de análise, permitindo verificar o remetente do e-mail, o endereço de e-mail oficial da empresa mencionada no e-mail, as rotas pelas quais o e-mail percorreu até chegar ao destinatário, entre outros detalhes.

A análise do campo "*From*" do e-mail em questão mostrou que o endereço de e-mail não era oficial da Amazon, o que já seria suficiente para marcar o e-mail como "SPAM". Além disso, a verificação dos X-Headers permitiu verificar as rotas percorridas pelo e-mail, fornecendo informações relevantes para uma análise mais técnica.

Com base nos critérios de segurança analisados pelo PhishTool, pode-se garantir que a implementação do SPF e do DKIM em servidores de e-mail é uma das principais medidas de segurança utilizadas para evitar o envio de mensagens falsas ou fraudulentas em nome de um domínio de remetente legítimo. A verificação do DMARC também é importante para comprovar que o e-mail foi enviado pelo domínio alegado. Além disso, deve-se ter cuidado ao realizar pagamentos por meio de e-mails, pois há o risco de que esses e-mails sejam fraudulentos e direcionem o pagamento para contas controladas por atacantes. Em geral, é fundamental estar sempre atento e tomar medidas de segurança adequadas ao lidar com e-mails suspeitos ou desconhecidos.

Outro ponto importante na análise de e-mails suspeitos é verificar a segurança deles. Nesse sentido, a PhishTool mostrou-se eficiente ao verificar o IP do remetente e do destinatário, garantindo que ambos sejam válidos e correspondam ao domínio da empresa mencionada no e-mail.

Em resumo, o uso de ferramentas como o PhishTool é fundamental na prevenção de ameaças cibernéticas, permitindo uma análise mais técnica e eficiente de e-mails suspeitos. Através de uma abordagem abrangente e detalhada, é possível identificar possíveis ameaças e garantir a segurança da informação.

CONSIDERAÇÕES FINAIS

Com o crescente número de ataques cibernéticos, a segurança digital é uma preocupação constante para usuários e empresas. Nesse contexto, a análise de e-mails de *phishing* é uma importante ferramenta para identificar possíveis ameaças cibernéticas e evitar prejuízos.

A ferramenta PhishTool apresentada neste trabalho é uma opção eficiente para a análise de e-mails de *phishing*. Ela fornece uma visão técnica abrangente e detalhada, além de possuir um navegador seguro que facilita a triagem dos anexos e URLs suspeitos em uma única tela, tornando a análise mais eficiente e segura.

No exemplo de análise apresentado, o PhishTool foi capaz de identificar o endereço de e-mail falso utilizado pelo remetente do e-mail de *phishing* e demonstrou a importância de verificar outros detalhes relevantes para uma análise mais técnica.

Neste trabalho, foram abordados os objetivos propostos de realizar uma análise técnica de um *phishing* de e-mail e apresentar as principais técnicas utilizadas pelos criminosos, bem como fornecer *insights* sobre como empresas podem se proteger desses ataques. O estudo explorou conceitos fundamentais de segurança da informação, engenharia social e *phishing*, oferecendo uma visão abrangente sobre o tema. Além disso, a metodologia adotada, com pesquisa bibliográfica e documental, permitiu embasar teoricamente o estudo e identificar casos reais de ataques, fortalecendo a argumentação e as recomendações apresentadas.

Embora este trabalho tenha abordado de forma ampla a análise técnica de um *phishing* de e-mail e fornecido orientações para proteção contra esses ataques, existem várias possibilidades de desenvolver futuros trabalhos para aprofundar o tema. Algumas sugestões incluem:

Estudo de casos reais: Realizar uma análise detalhada de casos reais de ataques de *phishing*, coletando informações específicas sobre os métodos utilizados, as técnicas de engenharia social empregadas e os danos causados. Isso permitiria um maior entendimento das táticas mais recentes usadas pelos criminosos e forneceria *insights* valiosos para aprimorar as estratégias de defesa.

Desenvolvimento de técnicas de detecção avançadas: Investir na pesquisa e desenvolvimento de técnicas avançadas de detecção de e-mails de *phishing*, utilizando algoritmos de aprendizado de máquina e análise comportamental para identificar padrões suspeitos. Isso poderia ajudar a aprimorar os sistemas de segurança das empresas e reduzir a eficácia dos ataques de *phishing*.

Treinamento de conscientização em segurança: Realizar estudos sobre a eficácia de programas de treinamento de conscientização em segurança para funcionários, visando avaliar o impacto dessas iniciativas na redução dos casos de *phishing* bem-sucedidos. Esses estudos poderiam fornecer informações valiosas sobre a melhor forma de educar os usuários e fortalecer a segurança no ambiente corporativo.
Análise de técnicas de evasão: Investigar as técnicas utilizadas pelos criminosos para evadir sistemas de detecção de *phishing* e desenvolver contramedidas eficazes. Isso poderia envolver o estudo de técnicas de criptografia, uso de servidores intermediários e outros métodos usados para mascarar as atividades maliciosas.

Em suma, a análise cuidadosa de e-mails de *phishing* com o auxílio de ferramentas como o PhishTool pode ajudar a proteger usuários e empresas de possíveis ataques cibernéticos, contribuindo para a segurança digital.

REFERÊNCIAS

DAVE CROCKER, TONY HANSEN, MURRAY S. KUCHERAWY. RFC 6376: DKIM Signatures. [s.l: s.n.]. Disponível em: https://www.rfc-editor.org/rfc/pdfrfc/rfc6376.txt.pdf. Acesso em: 07 de maio de 2023

ISACA. Information systems audit and control association. O estado de segurança cibernética: implicações para 2016. Disponível em: http://www.isaca.org. Acesso em: 22 de setembro 2022.

Gênesis três. Disponível em: https://www.bibliaonline.com.br. Acesso em: 20 de setembro de 2022.

GHAZAL, Franciane. Vulnerabilidade das informações empresariais através do uso de dispositivos móveis. Trabalho de Conclusão de Curso (Especialização em Gestão Empresarial) – Universidade Tecnológica Federal do Paraná, Curitiba, 2015. Disponível em: http://repositorio.utfpr.edu.br/jspui/handle/1/19544. Acesso em: 27 abr. 2023.

MITNICK, Kevin D.; SIMON, Willian L. The art of deception: controlling the human element of security. São Paulo: Pearson Education, 2003. 284p.
Gênesis três. Disponível em: https://www.bibliaonline.com.br Acesso em: 20 de setembro de 2022.

PhishTool. Disponível em: https://www.phishtool.com. Acesso em: 27 de abril de 2023.

PINHEIRO, PATRICIA PECK. Ataques e crimes cibernéticos: conheça os principais tipos. Genjurídico. Disponível em: https://www.genjuridico.com.br. Acesso em: 20 de setembro de 2022

ROBINSON & ULLMANN. RFC 1154 Encoding Header Field for Internet Messages. [s.l: s.n.]. Disponível em: https://www.rfc-editor.org/rfc/pdfrfc/rfc1154.txt.pdf. Acesso em: 27 de abril de 2023.

Security Team Training Ltd. Phishing Email. Disponível em: https://blueteamlabs.online/home/challenge/phishing-analysis-2-a1091574b8 Acesso em: 10 de maio de 2023.

SALVIANO, EDGARD MESQUITA; SANTOS, JOÃO PEDRO RIBEIRO; SILVA, MATHEUS ALMEIDA. Principais tipos de ataques *Phishing* e mecanismos de segurança. Curso de Sistemas de Informação. 24 p. Gama. Centro Universitário do Planalto Central Apparecido dos Santos. 2021. Disponivel em: https://dspace.uniceplac.edu.br/handle/123456789/1611. Acesso em: 27 de abril de 2023.

SILVA, G. CRIMES DIGITAIS EVOLUCAO DOS CRIMES E APLICACAO DO DIREITO. https://repositorio.animaeducacao.com.br/handle/ANIMA/22552. Acesso em: 17 de junho de 2022.

SOUZA, Leonardo Correa de; TANAKA, Simone Sawasaki. Estudo sobre ataques de phishing e suas técnicas de defesa. Revista Terra & Cultura: Cadernos de Ensino e Pesquisa, [S.l.], v. 39, n. especial, p. 90-95, fev. 2023. ISSN 2596-2809. Disponível em: http://periodicos.unifil.br/index.php/Revistateste/article/view/2804. Acesso em: 07 de maio de 2023.

ZANELLA, TATIELI. ESTUDO SOBRE A QUEBRA DE CONFIDENCIALIDADE DA INFORMAÇÃO E MECANISMOS DE SEGURANÇA. Bacharel em Sistemas de Informação. 79 p. UNIVERSIDADE DE CAXIAS DO SUL. 2017. Disponivel em: https://repositorio.ucs.br/xmlui/bitstream/handle/11338/3807/TCC%20Tatiele%20Zanella.pdf?sequence=1&isAllowed=y Acesso em: 07 de maio de 2023