**UNIVERSIDADE ESTADUAL PAULISTA “JÚLIO DE MESQUITA FILHO” – CAMPUS DE PRESIDENTE PRUDENTE.**

**DEPARTAMENTO DE MATEMÁTICA E COMPUTAÇÃO.**

IGOR MENDES DOMINGUES MIRAS

ALEXANDRE TEVES ALCANTARA SANTOS

**ENGENHARIA SOCIAL NO MUNDO EMPRESARIAL: O uso do *phishing***

**PRESIDENTE PRUDENTE**

**2022**

IGOR MENDES DOMINGUES MIRAS

ALEXANDRE TEVES ALCANTARA SANTOS

**ENGENHARIA SOCIAL NO MUNDO EMPRESARIAL: O uso do *phishing***

Trabalho de Metodologia Científica apresentado como requisito para obtenção de aprovação na matéria, referente ao Curso de Graduação em Ciência da Computação, da Faculdade de Ciências e Tecnologia Universidade Estadual Paulista “Júlio de Mesquita Filho”, Campus de Presidente Prudente

Orientador: Prof. Dr. Ronaldo Toshiaki Oikawa

**PRESIDENTE PRUDENTE**

**2022**

**RESUMO**

A presente pesquisa aborda o tema da engenharia social e sua aplicação no setor empresarial, com um foco especial nos ataques por phishing a empresas de médio e grande porte. O objetivo deste trabalho é fornecer uma compreensão clara do que é a engenharia social e o phishing, apresentar os diferentes tipos de phishing, identificar as ferramentas comumente utilizadas pelos engenheiros sociais e apresentar métodos eficazes de defesa contra esses ataques. A pesquisa é exploratória em natureza e se baseia principalmente em revisão bibliográfica, incluindo uma rápida análise de dois estudos de caso. É importante destacar que a falta de conhecimento sobre a engenharia social e o aumento nos casos de ataques são aspectos preocupantes que precisam ser considerados. Portanto, é fundamental que as empresas estejam cientes da ameaça e tomem medidas para se proteger contra os ataques de engenharia social.

**Palavras-chave:** Engenharia Social; Phishing; mundo empresarial; Informação.

**ABSTRACT**

This research addresses the topic of social engineering and its application in the business sector, with a special focus on phishing attacks on medium and large companies. The aim of this work is to provide a clear understanding of what social engineering and phishing are, present the different types of phishing, identify the tools commonly used by social engineers, and present effective defense methods against these attacks. The research is exploratory in nature and is based primarily on a literature review, including a quick analysis of two case studies. It is important to note that the lack of knowledge about social engineering and the increase in attack cases are concerning aspects that need to be considered. Therefore, it is essential that companies be aware of the threat and take measures to protect themselves against social engineering attacks.

**Keywords:** Social Engineering; Phishing; business world; information.

**LISTA DE FIGURAS**

[Figura 1 - Caso de SILVA apud CIOUOL (2012). 12](#_Toc125946320)

[Figura 2 - Caso de SANTOS (2019). 13](https://reitoriaunespbr-my.sharepoint.com/personal/im_miras_unesp_br/Documents/ENGENHARIA_SOCIAL_NO_MUNDO_EMPRESARIAL%20(Recuperação%20Automática)1232.docx#_Toc125946321)

[Figura 3 - Interface inicial do SET. 14](https://reitoriaunespbr-my.sharepoint.com/personal/im_miras_unesp_br/Documents/ENGENHARIA_SOCIAL_NO_MUNDO_EMPRESARIAL%20(Recuperação%20Automática)1232.docx#_Toc125946322)

[Figura 4 - Interface de Website Attack Vectors 15](https://reitoriaunespbr-my.sharepoint.com/personal/im_miras_unesp_br/Documents/ENGENHARIA_SOCIAL_NO_MUNDO_EMPRESARIAL%20(Recuperação%20Automática)1232.docx#_Toc125946323)

[Figura 5 - Interface de Credential Harvester Attack Method 16](https://reitoriaunespbr-my.sharepoint.com/personal/im_miras_unesp_br/Documents/ENGENHARIA_SOCIAL_NO_MUNDO_EMPRESARIAL%20(Recuperação%20Automática)1232.docx#_Toc125946324)

[Figura 6 - Interface de Web Templates 16](https://reitoriaunespbr-my.sharepoint.com/personal/im_miras_unesp_br/Documents/ENGENHARIA_SOCIAL_NO_MUNDO_EMPRESARIAL%20(Recuperação%20Automática)1232.docx#_Toc125946325)

[Figura 7 - Interface do ngrok. 17](https://reitoriaunespbr-my.sharepoint.com/personal/im_miras_unesp_br/Documents/ENGENHARIA_SOCIAL_NO_MUNDO_EMPRESARIAL%20(Recuperação%20Automática)1232.docx#_Toc125946326)

[Figura 8 - Interface do SET para recuperação dos métodos POST. 17](https://reitoriaunespbr-my.sharepoint.com/personal/im_miras_unesp_br/Documents/ENGENHARIA_SOCIAL_NO_MUNDO_EMPRESARIAL%20(Recuperação%20Automática)1232.docx#_Toc125946327)

[Figura 9 - Site clonado do Gmail. 17](https://reitoriaunespbr-my.sharepoint.com/personal/im_miras_unesp_br/Documents/ENGENHARIA_SOCIAL_NO_MUNDO_EMPRESARIAL%20(Recuperação%20Automática)1232.docx#_Toc125946328)

[Figura 10 - Email phishing em HTML. 18](https://reitoriaunespbr-my.sharepoint.com/personal/im_miras_unesp_br/Documents/ENGENHARIA_SOCIAL_NO_MUNDO_EMPRESARIAL%20(Recuperação%20Automática)1232.docx#_Toc125946329)

[Figura 11 - Email recebido pela vítima. 18](https://reitoriaunespbr-my.sharepoint.com/personal/im_miras_unesp_br/Documents/ENGENHARIA_SOCIAL_NO_MUNDO_EMPRESARIAL%20(Recuperação%20Automática)1232.docx#_Toc125946330)

[Figura 12 - Informações da vítima exibidas ao atacante. 19](https://reitoriaunespbr-my.sharepoint.com/personal/im_miras_unesp_br/Documents/ENGENHARIA_SOCIAL_NO_MUNDO_EMPRESARIAL%20(Recuperação%20Automática)1232.docx#_Toc125946331)

**SUMÁRIO**

[**1 INTRODUÇÃO** 6](#_Toc126088298)

[**1.1** **Problemas da pesquisa** 7](#_Toc126088299)

[**1.2** **Hipótese** 7](#_Toc126088300)

[**1.3** **Objetivos Gerais** 7](#_Toc126088301)

[**1.4** **Objetivos Específicos** 8](#_Toc126088302)

[**1.5** **Justificativa** 8](#_Toc126088303)

[**1.6** **Metodologia** 8](#_Toc126088304)

[**2** **ENGENHARIA SOCIAL** 9](#_Toc126088305)

[**2.1** **Phishing** 10](#_Toc126088306)

[**2.2** **Estudos de caso** 12](#_Toc126088307)

[**2.2.1 Caso de SILVA *apud* CIOUOL (2012)** 12](#_Toc126088308)

[**2.2.2 Caso de SANTOS (2018)** 12](#_Toc126088309)

[**2.3** **Exemplo de ataque de phishing** 13](#_Toc126088310)

[**REFERÊNCIAS** 6](#_Toc126088311)

# INTRODUÇÃO

Qual o recurso mais valioso no mundo atual? O que um dia já foi o ouro, o petróleo, ou até mesmo o diamante, hoje, na sociedade da informação, pode ter se tornado os dados, que representam informações valiosas.

Na sociedade da informação, segundo Werthein (2000), “as tecnologias se desenvolvem para permitir o homem atuar sobre a informação propriamente dita (...)”, onde até mesmo países com menos industrialização estão seguindo essa tendência.

De acordo com Setzer (2001), dado é “uma sequência de símbolos quantificados ou quantificáveis. (...) Um dado é necessariamente uma entidade matemática e, desta forma, é puramente sintático.”. Mas, se dados são apenas símbolos puros, por que são tão valiosos?

Ainda com Setzer (2001), tem-se que “Informação é uma abstração informal (isto é, não pode ser formalizada através de uma teoria lógica ou matemática), que está na mente de alguém, representando algo significativo para essa pessoa.”. Portanto, o que realmente é de grande valia é a informação, que representa conhecimentos reunidos sobre algo ou alguém, podendo ser representada e mensurada por meio de dados.

O grande valor dos dados está na possibilidade de manipulação deles por meio de computadores, que possuem uma capacidade de trabalhar com dados de maneira mais eficiente que os seres humanos. Após o processamento dos dados de entrada por meio de programas, que são basicamente funções matemáticas, são retornados dados de saída. Os dados de saída são interpretados por seres humanos, já que máquinas não tem capacidade de atribuir significados abstratos a algo puramente sintático.

Visando o mundo empresarial, os dados têm um papel fundamental, impactando diretamente nas decisões de negócio que serão tomadas. O processamento computacional é de suma importância, já que, na maioria dos casos, os dados devem ser manipulados e retornados em tempo real (SHARDA; DELEN; TURBAN, 2019).

Apesar de todas as vantagens disponibilizadas pela utilização de dispositivos tecnológicos para manipulação e armazenamento de dados, existem também algumas desvantagens, como a possibilidade de comprometimento da integridade e segurança dos dados.

Por estarem armazenados em dispositivos tecnológicos, como HD’s (*Hard Disk*) ou SSD’s (*Solid State Drive*), os dados empresariais estão suscetíveis a ataques externos de hackers, sendo principalmente feitos por *Black Hats* e Hackers de corporações.

Black Hats são hackers que, para NordVPN (2022), “usam malwares (programas, códigos maliciosos) para invadir sistemas, roubar informações ou executar ações independentemente da vontade das vítimas;”. Já Hackers de corporações, segundo NordVPN (2022), “servem empresas e grupos privados. O principal objetivo deles é o de invadir, roubar e prejudicar sistemas, dispositivos, redes e servidores de empresas concorrentes.”.

Dentre o vasto leque de ferramentas e ataques sofisticados feitos por diferentes tipos de hackers, a Engenharia Social é um dos ataques mais utilizados e mais eficientes, tendo em vista que ela não depende puramente de conhecimentos técnicos sobre informática e tecnologia, sendo necessário também conhecimentos de comunicação interpessoal e persuasão.

## Problemas da pesquisa

Tendo em vista o contexto apresentado acima, a respeito dos impactos que um ataque de engenharia social pode trazer a uma corporação, graças a falta de conhecimento de funcionários a respeito do tema, temos que o problema a ser analisado pela presente pesquisa é: O que é a engenharia social e por que está ocorrendo um crescimento dos ataques de engenharia social em empresas?

## Hipótese

Para este estudo se desenvolveu as seguintes hipóteses: Os funcionários não têm conhecimento sobre o tema engenharia social; não existe uma política de segurança contra ataques de engenheiros sociais; A pandemia do COVID-19 aumentou as empresas conectadas remotamente, aumentando também o número de ataques de engenharia social e *phishing*.

## Objetivos Gerais

Temos como objetivos gerais para essa pesquisa:

* Compreender de maneira geral o que é a Engenharia Social e como ela pode ser aplicada em empresas principalmente de médio e grande porte.
* Compreender de maneira geral o que é *phishing*e suas técnicas, bem como se proteger.
* Estudar maneiras que o *phishing* pode ser realizado pelos engenheiros sociais.

## Objetivos Específicos

Temos como objetivos específicos para essa pesquisa:

* Mostrar as principais técnicas e métodos utilizados pelos engenheiros sociais e como se prevenir
* Analisar as ferramentas mais utilizadas para a Engenharia Social, como é o caso do software SET (Social-Engineer Toolkit).
* Entender como as empresas, principalmente de médio e grande porte, devem se defender de ataques de Engenharia Social.

## Justificativa

O desenvolvimento dessa pesquisa auxiliará empresas a garantir a integridade das informações armazenadas em seus sistemas contra ataques de Engenharia Social, e evitará prejuízos de milhões (ou até bilhões) de reais.

Segundo Equipe Propague (2022, grifo do autor): "a pesquisa mais recente da Federação Brasileira dos Bancos (Febraban) sobre segurança digital revela que o número de fraudes financeiras envolvendo métodos de engenharia social **avançou 165% no Brasil** entre o primeiro semestre e o segundo semestre de 2021".

## Metodologia

A presente pesquisa é de natureza exploratória. Segundo Gil (2002, p. 41) “Estas pesquisas têm como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a constituir hipóteses.”.

O trabalho embasou-se em revisão bibliográfica. De acordo com Gil (2002, p. 44) “A pesquisa bibliográfica é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos.”. A revisão bibliográfica foi feita com base em fontes secundárias, como artigos científicos, sites e livros sobre o tema Engenharia Social, analisando principalmente o phishing e suas diferentes aplicações. As palavras-chave utilizadas para a busca por informações foram: Engenharia Social, Phishing, mundo empresarial. Trata-se também ao decorrer da pesquisa sobre dois estudos de caso, que trazem dados quantitativos. O primeiro estudo de caso, de CIOUOL *apud* SILVA *et al.* (2012), traz dados sobre a porcentagem de funcionários de TI da empresa Check Point que foram vítimas de ataques de engenharia social e quanto de dinheiro elas perderam. O segundo estudo de caso, de SANTOS (2018), expõe a porcentagem de funcionários de uma empresa multinacional (não revelada) que tem conhecimento sobre o que é a engenharia social.

Mostram-se no trabalho métodos que empresas devem adotar para evitar que dados sejam vazados, além de ferramentas muito utilizadas em ataques, como o SET e o ngrok.

Por fim, o artigo tem como foco o mundo empresarial, que é onde as informações mais valiosas estão armazenadas.

# ENGENHARIA SOCIAL

O termo engenharia social pode parecer estranho, e até de difícil entendimento para quem desconhece do assunto. É um curso de alguma faculdade? Uma engenharia como todas as outras?

Tendo como referência Ferreira (1993), define-se **Engenharia** como:

“Arte de aplicar conhecimentos científicos e empíricos e certas habilitações específicas à criação de estruturas, dispositivos e processos que se utilizam para converter recursos naturais em formas adequadas ao atendimento das necessidades humanas.

Ainda baseado nas definições de Ferreira (1993), **social** define-se como “Da sociedade, ou relativo a ela.”.

Tendo em vista as duas definições apresentadas, pode-se concluir que a engenharia social não é puramente uma engenharia, como por exemplo a civil, mecânica, elétrica ou química, pois ela não utiliza da conversão de recursos naturais para atender as necessidades humanas.

Desconsiderando a utilização de recursos naturais no processo desejado, a engenharia social se encaixa perfeitamente no escopo de engenharia. Define-se então engenharia social como sendo a arte de aplicar conhecimentos científicos e empíricos sobre sociedade, comunicação interpessoal, linguagem corporal e persuasão para fins de extração de informações.

De acordo com Mitnick e Simon (2003, p. 5):

A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não e, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia.

Determinada empresa pode desfrutar dos melhores e mais seguros equipamentos tecnológicos, com investimento de milhões de dólares em *firewall’s*, criptografias, *proxy’s* e VPN’s, e ainda assim continuará exposta para ataques de engenharia social, devido ao elo mais frágil na segurança das informações de uma organização, que é o fator humano.

A segurança de uma empresa sempre estará em perigo enquanto existirem pessoas envolvidas nos processos tecnológicos. O tema em questão traz à tona uma famosa declaração do grande físico do século XX, Albert Einstein: “Duas coisas são infinitas: o universo e a estupidez humana. Mas, em relação ao universo, ainda não tenho certeza absoluta”.

Mitnick e Simon (2003, p. 4) comparam e descrevem um engenheiro social como sendo “(...) um mágico inescrupuloso que faz você olhar a sua mão esquerda enquanto com a mão direita rouba seus segredos. Esse personagem quase sempre é tão amistoso, desembaraçado e prestativo que você se sente feliz por tê-lo encontrado.”.

A engenharia social é dividida em duas categorias principais, a engenharia social com tecnologia e a engenharia social sem tecnologia. A engenharia social com tecnologia se refere ao uso de técnicas que necessitam ferramentas tecnológicas, como *phishing, vishing, smishing*, entre outros, para obtenção de informações confidenciais. Por outro lado, a engenharia social sem tecnologia se refere ao uso de técnicas de persuasão e manipulação para obtenção de informações, sem o uso de ferramentas tecnológicas.

Dentre as técnicas de engenharia social citadas acima, uma em especial merece uma atenção maior, já que é a mais utilizada hoje em dia. Por ser barato de se implementar e eficiente, o *Phishing* é a técnica mais utilizada dentro da engenharia social atualmente.

## Phishing

A definição exata de *phishing* varia muito entre fontes renomadas, como especialistas e corporações de segurança, não sendo possível determinar com precisão o que é phishing.

Na visão de Malwarebytes (c2022, grifo nosso), “Phishing é o **crime** de enganar as pessoas para que compartilhem informações confidenciais como senhas e número de cartões de crédito.”.

Já para Merwe et al. (2005, tradução nossa, grifo nosso), “*Phishing* é uma **atividade fraudulenta** definida como a criação de uma réplica de uma página da Web existente para enganar um usuário a submeter dados pessoais, financeiros ou senha.”.

Por último, de acordo com Microsoft (c2023), “Os ataques de phishing visam **roubar ou danificar** dados confidenciais enganando as pessoas para que revelem informações pessoais, como senhas e números de cartão de crédito.”.

Porém, todas as fontes citadas acima concordam em um ponto: *phishing* é uma prática criminosa que tem como finalidade conseguir informações, sejam elas confidenciais ou não.

Existem diferentes tipos de *phishing*, utilizando diferentes meios de comunicação, como por exemplo o *smishing*, *vishing*, e o tradicional *phishing* por email. Tendo em vista a definição dada por AVG (2022), *vishing* é “um esquema de phishing baseado em voz executado por telefone, aproveita a tecnologia e sua confiança para tentar roubar informações pessoais.”. Baseado em Kaspersky (c2023), “O termo smishing é uma combinação de ‘SMS’ (short message services, ou mensagens de texto) e ‘phishing’.”, sendo basicamente um phishing enviado por SMS.

A razão de existirem tantos ataques diferentes de *phishing* é simples, o phishing é uma excelente técnica de engenharia social, sendo talvez a mais barata e eficiente. De acordo com Keepnet LABS (2018, tradução nossa):

Mais de 90% dos vazamentos de dados bem-sucedidos são iniciados por um ataque baseado em e-mail, custando às empresas US$ 3 trilhões por ano e motivando investimentos tecnológicos consideráveis, como firewalls e anti-spam, para fornecer proteção.

Dentre os ataques de *phishing* tradicionais, temos algumas variações, como por exemplo o *spear phishing*, *clone phishing* e *whaling.*

“Pescar com uma vara pode levar a você vários itens abaixo da linha da água – um linguado, um alimentador de fundo ou um pedaço de lixo. Pescar com uma lança permite que você selecione um peixe específico. Daí o nome.” (TRENDMICRO, c2023). A metáfora acima remete a uma característica do *spear phishing* que faz ele se diferenciar do *phishing* tradicional. No *spear phishing*, o atacante tem informações específicas a respeito de uma pessoa ou grupo, como por exemplo o email institucional de alguma empresa, tornando o ataque mais letal.

*Clone phishing*, para Kaspersky (c2023), é um ataque no qual:

os criminosos copiam (ou clonam) um e-mail legítimo recebido anteriormente que contenha um link ou um anexo. Em seguida, o phisher substitui os links ou arquivos anexos por conteúdo malicioso para que passe pelo item verdadeiro.

*Whaling* (caça as baleias), é um tipo de *phishing* destinado aos “peixes grandes” de uma corporação, normalmente tendo como alvos CEO (Chief Executive Officer, ou diretor-executivo), CFO (Chief Financial Officer, ou diretor-financeiro) ou CTO (Chief Technology Officer, ou diretor de técnologia) de empresas. (TRENDMICRO, c2023).

## Estudos de caso

### 2.2.1 Caso de SILVA *apud* CIOUOL (2012)

O primeiro estudo de caso a ser analisado será o de SILVA apud CIOUOL (2012), no qual a empresa de segurança Check Point foi submetida a entrevistas com todos os funcionários de TI. Durante a pesquisa, foram entrevistados 850 profissionais. A pesquisa obteve os seguintes resultados: 48% foram vítimas de engenharia social e tiveram 25 ou mais ataques e custaram às vítimas de 25.000 a 100.000 dólares por incidente. O gráfico 1 ilustra os resultados do estudo.

Figura - Caso de SILVA apud CIOUOL (2012).

Fonte: Elaborado pelo Autor (2023).

### 2.2.2 Caso de SANTOS (2018)

O segundo estudo de caso a ser analisado será o de SANTOS (2018). O estudo foi desenvolvido com auxílio da ferramenta Survey Monkey. Segundo Waclawski (2012, tradução nossa), “Survey Monkey é um programa na internet e site de hospedagem que permite que uma pessoa crie uma pesquisa para uso na internet.”.

A pesquisa de SANTOS (2018) foi feita em uma empresa multinacional, na qual o nome não foi revelado por questões de segurança, em que os funcionários eram entrevistados a fim de saber se eles tinham conhecimento sobre o que era engenharia social. Os resultados foram: 78% dos entrevistados na pesquisa indicaram não ter conhecimento sobre o tema aludido, enquanto apenas 22% dos colaboradores conhecem sobre Engenharia Social. O gráfico 2 ilustra o caso.

Figura - Caso de SANTOS (2018).

Gráfico, Gráfico de barras

Descrição gerada automaticamente

Fonte: Santos (2018, p.45): Dados da pesquisa.

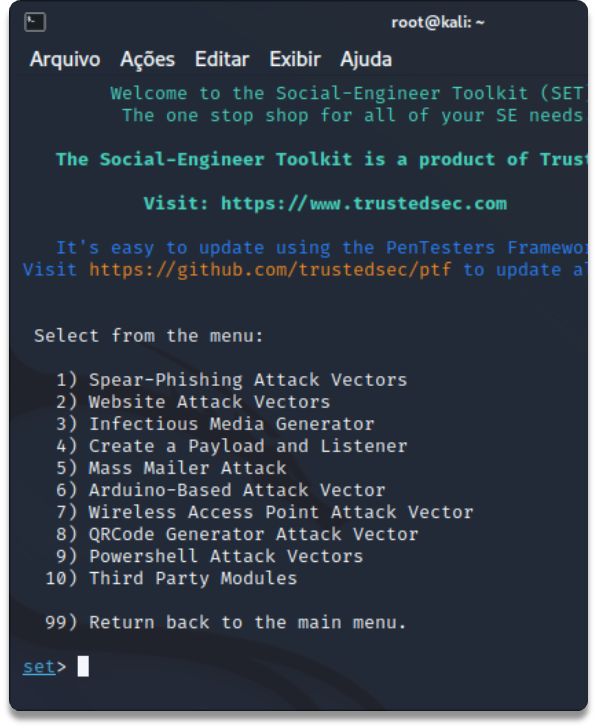
## Exemplo de ataque de phishing

Para demonstrar e exemplificar um dos mais simples e mais efetivos ataques de engenharia social por meio de phishing, serão utilizados dois softwares: SET e ngrok.

SET (Social-Engineer Toolkit) é um software Open-Source (de Código aberto) desenvolvido para auxiliar em diversos tipos de ataques de engenharia social. Dentre todas suas funções, o software consegue montar ataques de spear phishing, clonar websites, gerar uma mídia maliciosa (como por exemplo um pendrive infectado), criar um payload (código malicioso) e um listener (capturador de informações, como por exemplo um Keylogger), infectar um Arduino, criar um ponto de Wi-Fi falso, gerar um QRCode malicioso, ou até mesmo atacar o Powershell do Windows.

Ngrok é um software que, segundo Awari (2023), “cria uma conexão segura e encriptada (através de um túnel) entre um endpoint na internet e sua máquina local, permitindo que outras pessoas acessem sua aplicação rodando localmente através de um endereço de internet público.”. Basicamente, o ngrok será utilizado nesse exemplo de ataque para conectar o computador do atacante com a internet.

Figura - Interface inicial do SET.



Para esse exemplo de ataque, será utilizada a segunda opção do SET, Website Attack Vectors, que disponibiliza 7 métodos de ataques de Engenharia Social com base em criação de websites falsos.

Ao selecionar a segunda opção, o atacante dispõe de 7 opções de ataque baseados em criação de websites falsos.

Texto

Descrição gerada automaticamente

Figura - Interface de Website Attack Vectors

Dentre as opções disponibilizadas, a mais utilizada é a de número 3, *Credential Harvester Attack Method,* que, ao traduzida para o português, significa “Método de ataque coletor de credenciais”. Esse método clonará um website que possui campos de usuário e senha e colherá as informações digitadas pelo usuário.

Ao selecionar a opção de número 3, o atacante será servido de três opções para realizar seu ataque de colheita de credenciais: Web Templates, que disponibilizará uma lista de sites pré-definidos para serem clonados, como Gmail, Facebook ou Twitter. (Esta será a opção utilizada no exemplo de ataque atual); Site Cloner, que permite inserir o link do site desejado para ser clonado; Custom Import, que permite ao atacante inserir seu próprio site com um arquivo HTML (HyperText Markup Language, ou Linguagem de Marcação de Hipertexto, em português).

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

Figura 5 - Interface de Credential Harvester Attack Method

Após selecionada a primeira opção, Web Templates, o atacante recebe opções de sites famosos para clonar, como por exemplo o Gmail ou Twitter. Neste exemplo, será utilizado o template do site do Gmail.

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

Figura - Interface de Web Templates

Logo após, o software pede para o atacante digitar o endereço de IP para onde as informações recuperadas serão destinadas. Para que o site malicioso fique disponível à outras pessoas, é utilizada outra ferramenta, chamada *ngrok*, que cria um túnel entre a máquina do atacante e a internet.

Tela de computador com fundo preto

Descrição gerada automaticamenteO ataque funciona da seguinte maneira: em vez de o atacante colocar o próprio IP, que representará de onde os métodos POST enviados em formulários pela vítima serão recuperados, ele coloca o endereço gerado pelo ngrok.

Figura - Interface do ngrok.

Texto

Descrição gerada automaticamente

Figura - Interface do SET para recuperação dos métodos POST.

Interface gráfica do usuário, Site

Descrição gerada automaticamenteAo entrar no link criado pelo ngrok, a vítima irá se deparar com um site idêntico ao do Gmail.

Figura - Site clonado do Gmail.

Texto

Descrição gerada automaticamente Esse ataque ainda pode ser combinado com um phishing simples enviado por e-mail, onde o atacante se passará por alguém do time de segurança do Gmail. O e-mail será escrito em HTML, para fins de camuflar o real link do site no qual a vítima será destinada.

Figura - Email phishing em HTML.

Interface gráfica do usuário, Texto

Descrição gerada automaticamenteDentro do HTML existe um elemento <a> (âncora), que cria um link com outro documento, como por exemplo outro site. O elemento de âncora possui um atributo chamado “href”, que é para onde o usuário será redirecionado ao clickar no link. Porém, o segredo desse ataque está em escrever o link falso “https://www.google.com” entre a abertura e o fechamento do elemento <a>, pois assim a vítima pensará que o site é legítimo. A imagem abaixo retrata isso.

Figura - Email recebido pela vítima.

É importante notar que o atacante deve ter conhecimento sobre quem será a suas vítimas, e adequar o e-mail para cada uma delas.

Após a vítima inserir seus dados no formulário por método POST, as informações de e-mail e senha estarão dispostas para o atacante, como mostra a imagem abaixo.

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente



Figura - Informações da vítima exibidas ao atacante.

# REFERÊNCIAS

AUGUSTÉNÉ, A. **Diferentes tipos de hackers e os tipos mais comuns de ataques hacker.** NordVPN. Disponível em: <<https://nordvpn.com/pt-br/blog/tipos-de-ataque-hacker/>>. Acesso em: 20 jan. 2023.

BODNAR, D. **O que é um ataque de vishing?** AVG. Disponível em: < <https://www.avg.com/pt/signal/what-is-a-vishing-attack>>. Acesso em: 21 jan. 2023.

EQUIPE PROPAGUE. **Engenharia social: o que é e como ela impacta a segurança digital.** Instituto Propague. Disponível em: <<https://institutopropague.org/tecnologia-e-dados/engenharia-social-o-que-e-e-como-ela-impacta-a-seguranca-digital/>>. Acesso em: 20 jan. 2023.

FERREIRA, A. B. H. **Minidicionário da língua portuguesa**. 3 ed. Rio de Janeiro: Nova Fronteira, 1993.

GIL, A. C. **Como elaborar projetos de pesquisa.** 4. ed. São Paulo: Atlas, 2002. Disponível em: <<https://files.cercomp.ufg.br/weby/up/150/o/Anexo_C1_como_elaborar_projeto_de_pesquisa_-_antonio_carlos_gil.pdf>>. Acesso em: 21 jan. 2023.

KASPERSKY. **O que é smishing e como se proteger?** Kaspersky. Disponível em: < <https://www.kaspersky.com.br/resource-center/threats/what-is-smishing-and-how-to-defend-against-it>>. Acesso em: 22 jan. 2023.

KEEPNETLABS. **Phishing Simulator.** KeepnetLABS. Disponível em: < <https://keepnetlabs.com/wp-content/uploads/2022/02/Phishing-Simulator-v1.3.pdf>>. Acesso em: 22 jan. 2023.

MALWAREBYTES. **Phishing.** Malwarebytes. Disponível em: < <https://br.malwarebytes.com/phishing/>>. Acesso em: 21 jan. 2023.

MERWE, A. v. d.; MARIANNE, L.; MAREEK, D. Characteristics and responsibilities involved in a Phishing attack. **Winter International Synposium on Information and Communication Technologies: proceedings of the 4th international symposium on information and communication technologies**, Dublin, v. 5, p. 249-254, 2005. Disponível em: <https://dl.acm.org/doi/abs/10.5555/1071752.1071800>. Acesso em: 21 jan. 2023.

MICROSOFT. **O que é o phishing?** Microsoft. Disponível em: < <https://www.microsoft.com/pt-pt/security/business/security-101/what-is-phishing>>. Acesso em: 21 jan. 2023.

MITNICK, K. D.; SIMON, W. L. **A Arte de Enganar:** Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação**.** São Paulo: Pearson Education do Brasil Ltda, c2003. Disponível em: <[https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzdGFmZnR1dG9zfGd4OjQ0Njg2ZTgyYWJjODg1MWQ>](https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxzdGFmZnR1dG9zfGd4OjQ0Njg2ZTgyYWJjODg1MWQ) . Acesso em 13 dez. 2022.

SANTOS, S. O. **Engenharia social e políticas de segurança da informação no ambiente corporativo.** 2018. TCC (Tecnólogo em Segurança da Informação) - Faculdade de Tecnologia de Americana, Americana, 2018.

SETZER, V. W. Dado, informação, conhecimento e competência. **DataGramaZero - Revista de Ciência da Informação**, Rio de Janeiro, n.0, dez. 1999.

SHARDA, R.; DELEN, D.; TURBAN, E. **Business Intelligence e Análise de Dados para Gestão do Negócio.** 4. ed. São Paulo: Bookman, c2019.

SILVA, C. S. *et al*. Engenharia Social: o elo mais frágil da segurança nas empresas. **Revisa Eletrônica do Alto Vale do Itajaí – REAVI**. Ibirama, v. 1, n. 2, dez. 2012. Disponível em: <<http://www.revistas.udesc.br/index.php/reavi/article/view/2840>> Acesso em: 21 jan. 2023.

TRENDMICRO. **Quais são os diferentes tipos de phishing?** Trend Micro. Disponível em: <<https://www.trendmicro.com/pt_br/what-is/phishing/types-of-phishing.html#:~:text=Pescar%20com%20uma%20vara%20pode,voc%C3%AA%20selecione%20um%20peixe%20espec%C3%ADfico.>>. Acesso em: 22 jan. 2023.

WERTHEIN, J. A sociedade da informação e seus desafios. **Ciência da Informação**, Brasília, v. 29, n.2, p.71-77, maio/ago. 2000. Disponível em: <http://www.scielo.br/pdf/ci/v29n2/a09v29n2.pdf>. Acesso em: 09 fev. 2018.