UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS I - CAMPINA GRANDE
CENTRO DE CIÊNCIAS E TECNOLOGIA
DEPARTAMENTO DE COMPUTAÇÃO
CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

FRANKLIN DA SILVA BASILIO

O PAPEL DA ENGENHARIA SOCIAL NOS ATAQUES DE MALWARE

CAMPINA GRANDE
2022

FRANKLIN DA SILVA BASILIO

O PAPEL DA ENGENHARIA SOCIAL NOS ATAQUES DE MALWARE

Trabalho de Conclusão de Curso apresentado ao Curso de Bacharelado em Ciência da Computação da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de bacharel em Ciência da Computação.

Área de concentração: Cibersegurança

Orientadora: Profa. Me. Cheyenne Ribeiro Guedes Isidro

CAMPINA GRANDE
2022

B312p Basilio, Franklin da Silva.
O papel da engenharia social nos ataques de malware [manuscrito] / Franklin da Silva Basilio. - 2022.
50 p. : il. colorido.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Computação) - Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia , 2023.
"Orientação : Profa. Ma. Cheyenne Ribeiro Guedes Isidro , Coordenação do Curso de Computação - CCT."

1. Software malicioso. 2. Engenharia social. 3. Crime cibernético. I. Título

21. ed. CDD 005.1

Elaborada por Camile de A. Gomes - CRB - 15/559 BC/UEPB

FRANKLIN DA SILVA BASILIO

O Papel da Engenharia Social nos Ataques de Malware

Trabalho de Conclusão de Curso de Graduação em Ciência da Computação da Universidade Estadual da Paraíba, como requisito à obtenção do título de Bacharel em Ciência da Computação.

Aprovada em 11 de Abril de 2022.

Profa. MSc. Cheyenne Ribeiro Guedes Isidro (DC - UEPB)
Orientador(a)

Prof. Dr. Fábio Luiz Leite Júnior (DC/UEPB)
Examinador(a)

Profa. Dra. Kézia de Vasconcelos Oliveira Dantas (DC/UEPB)
Examinador(a)

RESUMO

O desenvolvimento de sistemas computacionais e o uso cada vez mais disseminado e abrangente da Internet tem beneficiado a sociedade de diversas formas. Em contrapartida tem permitido também que oportunistas utilizem esse meio para realizar o que chamamos de ataques cibernéticos, com a intenção de obter vantagem financeira em cima da vítima ou prejudicá-la. Além dos sistemas em si, a peça-chave nesses ataques é o fator humano, cujas características de personalidades têm sido exploradas mais e mais frequentemente. O usuário acaba permitindo que o ataque ocorra desavisadamente seja instalando um software, clicando em um link malicioso, repassando códigos de segurança, ou fornecendo informações sigilosas. Neste trabalho, portanto, buscamos alertar para a importância da Engenharia Social nesse contexto, uma vez que esta tem se mostrado a base para a concretização de ataques utilizando malwares, atuando com pré-requisito para o sucesso das invasões. Para tanto, abordamos ligação entre Engenharia Social e os fatores da personalidade humana, como encontrar a vítima que possua as características adequadas para ser manipulada em um ataque e também como defender-se. Em adição, apresentamos a classificação dos malwares e a evolução histórica dos ataques mais conhecidos e populares.

Palavras-Chave: Softwares maliciosos. Engenharia social. Crimes cibernéticos.

ABSTRACT

The development of computer systems and the increasingly widespread and comprehensive use of the Internet has been benefiting our society in many ways. On the other hand, it has also allowed opportunists to use it to carry out what we call cyber attacks, with the intention of harming or obtaining financial advantage over the victims. In addition to the computational systems themselves, the key to these attacks has been the human factor, whose personality traits have been explored more and more often. The user ends up allowing the attack to occur unknowingly by installing software, clicking on a malicious link, passing on security codes, or providing sensitive information. Therefore, in this work, we seek to alert to the importance of Social Engineering in this context, since it has proved to be the basis for carrying out attacks using malware, acting as a prerequisite for the success of invasions. To do so, we discuss the link between Social Engineering and human personality factors, how to find the victim who has the right characteristics to be manipulated in an attack and also how to defend ourselves. In addition, we present the classification of malware and the historical evolution of the most known and popular attacks.

Keywords: Malware. Social engineering. Cyber attacks.

LISTA DE ILUSTRAÇÕES

[1] Tradução nossa para: Social Engineering Attack Framework.

LISTA DE ABREVIATURAS E SIGLAS

AIDS	Aids Info Disk
APK	Android Package Kit
AOL	America OnLine
DDoS	Distributed Denial of Service
DNS	Domain Name System
DRM	Digital Restriction Management
DVRs	Digital Video Recorder
ENIAC	Electronic Numerical Integrator And Computer
IIS	Internet Information Services
IoT	Internet of Things
ISAPI	Internet Server Application Programming Interface
MBR	Master Boot Record
SELM	Social Engineering Land Mines
SCADA	Supervisory Control and Data Acquisition
SMB	Server Message Block

SUMÁRIO

1 INTRODUÇÃO

A história do desenvolvimento dos computadores nos permitiu partir de computadores unicamente utilizados para cálculos balísticos, tal como o ENIAC, até computadores de uso geral para os usuários domésticos, a exemplo do Apple I.

Com o passar dos anos, tais equipamentos foram evoluindo e agregando mais funcionalidades, e junto a essas criações, surgiram também os oportunistas que viram nesse meio um local de obter vantagem explorando falhas nesses sistemas computacionais. Inicialmente o propósito era a mera brincadeira, como forma de testar suas qualidades profissionais, e evoluíram para a obtenção de vantagens financeiras e/ou reconhecimento social em meio ao grupo pertencente, seja criando ou utilizando softwares maliciosos já existentes. Tais oportunistas conhecemos hoje como hackers e crackers, ambas categorias de indivíduos com alto grau de conhecimento técnico e que buscam falhas em sistemas computacionais, sendo que o segundo realiza isso com a intenção de obter vantagem financeira em cima da vítima ou prejudicá-la.

Os registros de softwares maliciosos - os **malwares** - existem desde 1971, (RAJESH, REDDY e REDDY, 2015) foram se diversificando em funções de acordo com o modus operandi no sistema invadido.

Com o passar do tempo, as brechas nos sistemas que permitiam tais ataques foram sendo reduzidas drasticamente, e após descoberta foram sendo corrigidas, através da liberação de atualizações para todos os usuários quase que de imediato. Com o aumento de segurança nos sistemas computacionais, os oportunistas foram profissionalizando-se em invasões de sistemas e trabalhando mais no fator humano, já que o ser humano foi a “peça” que continuou sendo a mesma durante todo esse período de evolução tecnológica.

Neste trabalho, portanto, buscamos alertar para a importância da Engenharia Social nesse contexto, uma vez que esta tem se mostrado a base para a concretização de ataques utilizando malwares.

1.1 Objetivo geral

Verificar se analisando o ser humano podemos evitar a infecção por malware nos sistemas computacionais.

1.2 Objetivo específico

- Qual o nível da contribuição da engenharia social para prática de crimes cibernético.
- Como a engenharia social influencia na escolha da vítima.
- Como é realizado o ataque e como se defender de investidas utilizando a engenharia social.

1.3 Justificativa

Devido o meu dia a dia no trabalho lidando com o público, de diversas classes sociais, surgiu o interesse em saber porque elas se tornavam vítimas de golpes cibernéticos após acreditarem em histórias contadas pelo atacante, vindo a seguir a seguir realizar comandos solicitados por ele.

Com este trabalho tenho como intuito através de pesquisa bibliográfica apresentar como o atacante utiliza a engenharia social para realizar o seu ataque afim de que a vítima ative o malware recebido.

Para tanto, abordamos nos capítulos seguintes a definição e classificação dos malwares atuais (Capítulo 2), o histórico de evolução dos ataques mais importantes até os dias atuais (Capítulo 3). No Capítulo 4, apresentamos os conceitos por trás da Engenharia Social e a sua ligação ao fator humano, e por fim, no Capítulo 5, discutimos a ligação entre a Engenharia Social e os malwares existentes.

2 FUNDAMENTAÇÃO TEÓRICA

Nesta seção apresentarei sobre os malwares, suas diferenças entre os mais conhecidos, sua evolução no decorrer dos anos, o que é a engenharia social, como ela é utilizada para conseguir informações uteis na realização de um ataque cibernético, como os autores citados neste trabalho determinam as características essenciais para obter a melhor vítima que venha a colaborar. As formas como se defender de investidas da engenharia social, conhecendo as formas de ataque e a sua relação com os malwares, utilizados contra a vítima, afim de que ela execute em seu sistema para que o atacante obtenha as vantagens que procura.

2.1 Os malwares e sua classificação

No início da era da informação entendíamos por vírus, todo tipo de programa malicioso que procurava tirar vantagem de um sistema após infectá-lo. Com o passar dos anos, os tipos de ameaças foram se diversificando de acordo com o propósito e a forma de ataque. Dessa forma o conjunto dessas pragas digitais ficou conhecido como **malware**, abreviação de *malicious software*, termo que se tornou comum na indústria de antivírus, e passou a abranger tipos diversos, tais como vírus, trojan, worms, ransomware, spyware, adware, DDoS, Banking Trojans, Phishing, CC sniffers, dentre outras modalidades de malwares. Cada uma dessas classes de malware tem uma forma específica de contaminar o sistema, e suas peculiaridades serão abordadas mais à frente neste trabalho.

Inicialmente os criadores tinham apenas a curiosidade de testar as habilidades e pregar peças em colegas de estudo ou trabalho, mas atualmente é utilizado para obter ganhos financeiros ou desestabilizar governos e empresas, gerando prejuízo financeiro e/ou estrutural para a vítima. Outra característica comum entre eles é que necessitam da participação do ser humano, mais precisamente uma ação da própria vítima para que o malware entre em funcionamento no sistema invadido. Essa é uma característica presente desde a primeira versão de “vírus” tal como o BRAIN, de 1986 (KORSAKOV, 2014).

Daquele tempo para os dias atuais mudou-se o meio utilizado dessa ação. Antes se dava por meio de disquete com um rótulo de um programa que a vítima desejava ter, (KORSAKOV, 2014, pg.39). Atualmente são pendrives perdidos na calçada, cuja vítima anseia em ter um espaço de armazenamento gratuito ou apenas pela curiosidade de saber o que tinha dentro daquele dispositivo “perdido”, como é citado por (MOUTON, LEENEN e VENTER, 2016). Ou pode acontecer através de um e-mail chamativo com proposta de dinheiro fácil, promoções relâmpagos, recall de algum produto que muitas das vezes a vítima não comprou, mas clica no link para saber do que se trata a informação.

Os golpes podem ser generalizados ou específicos para determinadas vítimas ou setores, em que a mesma mensagem é enviada para milhares de pessoas ao mesmo tempo. Segundo Lippi (2020), cerca de 3,4 bilhões de e-mails com phishing são enviados diariamente, sendo responsável por 80% de incidentes de segurança cibernética. Apesar de existir outras formas de comunicação atualmente via internet, o e-mail ainda é o maior vetor de transmissibilidade de malware, sendo responsável por 94% deles (LIPPI, 2020). Um dos motivos dessa enxurrada de ataques via e-mail são os grandes vazamentos de dados que ocorrem em servidores, que permitem que hackers ou qualquer pessoa com más intenções tenham dados de e-mail, nome de usuários, senhas já usadas, e outras informações pessoais. Segundo o relatório da Digital Shadows (2020) mais de 15 bilhões de credenciais roubadas encontram-se disponíveis para venda a preços variados dependendo do potencial das informações a serem utilizadas em outros golpes.

2.1.1 Classificação dos malwares

No decorrer dos anos os malwares foram se modificando em funcionalidades, algumas específicas e outras abrangentes de acordo com o objetivo de seus criadores. Devido ao vasto número de softwares maliciosos e suas variantes, apresentamos a seguir as principais famílias de malwares e suas definições.

2.1.1.1 Vírus

O termo “vírus de computador" surgiu devido ao artigo de COHEN (1987). Em 03 de novembro de 1983, o seu professor, Leonard Adleman batizou o software recém-criado de vírus de computador. A principal característica é a auto replicação, além de realizar funções pré-determinadas pelo autor do vírus. O primeiro vírus de computador com essas características encontrado fora de ambientes de estudos, foi o BRAIN (1986) dos irmãos Basit e Amjad Farooq Alvi, que infecta o setor de boot da máquina.

2.1.1.2 Worm

Worm (verme) é o malware que possui características semelhantes ao vírus, podendo se auto replicar pelos dispositivos, tendo também funções pré-determinadas pelo programador do worm. A diferença com o vírus é que o worm após infectar o sistema, já executa a sua programação interna deixando neste sistema apenas uma cópia de si e partindo para outros sistemas ligados pela rede, não necessitando ser ativado pela intervenção de um usuário. O primeiro worm registrado, foi o Creeper (1971) de Bob Thomas que exibia uma mensagem em tela e procurava outros computadores na rede para infectar e mostrar a mensagem novamente. Inicialmente Creeper era considerado um vírus, baseado na definição de (NEUMANN, 1966) que se prendia apenas na auto replicação do malware, mas com a evolução dos softwares maliciosos, novas definições mais específicas apareceram.

2.1.1.3 Trojan ou cavalo de troia

Trojan ou cavalo de troia tem seu nome na mitologia grega, e define um software aparentemente com funções legítimas de acordo com o esperado pelo o usuário, mas que também realiza outras operações ocultas do usuário e em benefício do criador do software, como captura de informações pessoais, logins, senhas. Segundo Aycock (2006) desde 1972 o termo é utilizado. Ele é definido como parasita, sem poder de crescimento ou autorreplicação.

2.1.1.4 Spyware

Spyware é um software instalado sem o consentimento do usuário que monitora e coleta informações do mesmo e repassa para terceiros sem a sua autorização. Também é utilizado para roubar informações pessoais, tais como senhas e credenciais do usuário. O spyware mais conhecido atualmente, é o Pegasus criado pela empresa israelense NSO Group. No artigo de Marczak (2020) é abordado o uso do Pegasus para espionar a jornalistas, membros da Anistia Internacional, dentre outros no ano de 2018. No ano de 2021, veio à tona o uso do Pegasus por governos para espionar mais de 50 mil smartphones, onde foi notícia nos principais jornais, Figura 1.

Figura 1 - Criador de spyware israelense está em destaque em meio a relatos de amplos abusos (tradução nossa)[2]


The New York Times

Israeli Spyware Maker Is in Spotlight Amid Reports of Wide Abuses

Data leaked to a consortium of news organizations suggests that several countries use Pegasus, a powerful cyberespionage tool, to spy on rights activists, dissidents and journalists.

Give this article 115

An NSO Group display at the European Police Congress in Berlin last February.
Hannibal Hanschke/Reuters

By Ronen Bergman and Patrick Kingsley

Published July 18, 2021 Updated Nov. 8, 2021

Fonte: The New York Times.[3]

[2] No original: Israeli Spyware Maker Is in Spotlight Amid Reports of Wide Abuses

[3] Disponível em: <https://www.nytimes.com/2021/07/18/world/middleeast/israel-nso-pegasus-spyware.html >. Acesso em 18 ago. 2021.

2.1.1.5 Phishing

Phishing é um método de enganar o usuário, levando a fornecer informações pessoais ou financeiras, por meio de uma página falsa que imita uma página de internet real, onde muitas das vezes o atacante envia um link para as vítimas para serem direcionadas a página falsa. Segundo (CHAUDHRY; CHAUDHRY e RITTENHOUSE, 2016) “É um ataque híbrido que combina engenharia social e aspectos tecnológicos”. O termo foi usado pela primeira vez em 1996, em ataques para subtrair informações de cartões de crédito dos usuários da AOL (America OnLine).

2.1.1.6 Adware

Advertisement Software ou software de propaganda, os Adwares são anexados preferencialmente em softwares distribuídos gratuitamente e em páginas de internet, onde exibirão propagandas de patrocinadores, enquanto coletam dados do usuário, na maioria ele não é visível, apenas as propagandas baseadas nos dados que ele está coletando. Esses dados são utilizados pelos criadores do Adware para diversos fins, na maioria para estatísticas e marketing digital.

2.1.1.7 Bot e Botnets

O Bot é um dispositivo conectado à internet que sofreu contaminação por malware, e partir desse momento ele realizará ações determinada pelo responsável pelo malware que o contaminou, podendo fazer parte de uma rede de bots, botnet que ficam ao aguardo de instruções para realização de ataques por negação de serviço distribuído, DDOS (Distributed Denial of Service), ou realizando atividades no dispositivo infectado de acordo com as instruções do malware.

Já Botnets é uma rede de bots ou rede de dispositivos conectados à internet infectado por malware que executa comandos encaminhados por uma central responsável por controlar os bots, chamado de mestre (VORMAYR, ZSEBY e FABINI, 2017).

2.1.1.8 Keylogger

Keylogger é o software responsável por registrar as teclas pressionadas, tanto em computadores quanto celulares smartphones.

2.1.1.9 Backdoor

Backdoor, ou porta dos fundos, é um malware que geralmente vem atrelado a um software legítimo, que permite ao atacante realizar os comandos do ataque de dentro da máquina infectada, agindo como se fosse o próprio usuário. Também é uma estratégia realizada pelos criadores de softwares, tais como, sistemas operacionais, usado para dar suporte e atualizações no sistema, quando hackers descobrem, as utilizam para as invasões que passam despercebidas.

2.1.1.10 Ransomware

Ransomware (Ransom Ware - software de resgate) é um malware utilizado para criptografar arquivos no computador da vítima e que deixa uma mensagem solicitando um valor em resgate para repassar a chave para retirar a criptografia dos arquivos, normalmente solicita o pagamento em moedas digitais, devido não serem rastreáveis a sua negociação entre contas, evitando assim descobrir quem realizou a contaminação.

2.1.1.11 Fileless

Fileless é um malware que não possui arquivo próprio, sua invasão ocorre por meio de outro arquivo qualquer que leva as instruções para programas que estejam na memória do dispositivo da vítima. Essas instruções fazem com que o software que está em execução na memória realize as instruções do ataque.

2.1.1.12 Cryptojacking

Cryptojacking ou cryptojacker é o uso de malware para mineração de moedas digitais, que vem inserido em softwares piratas, navegadores ou por meio de uma invasão. Esse malware utiliza o poder de processamento da máquina infectada para realização da mineração de moedas digitais sem o consentimento da vítima para terceiros.

2.1.1.13 CC Sniffers

Credit Card Sniffers ou farejadores de cartão de crédito são malwares utilizados para coleta de informações de cartões de crédito em sites de comércio eletrônico.

2.1.1.14 Banking trojans

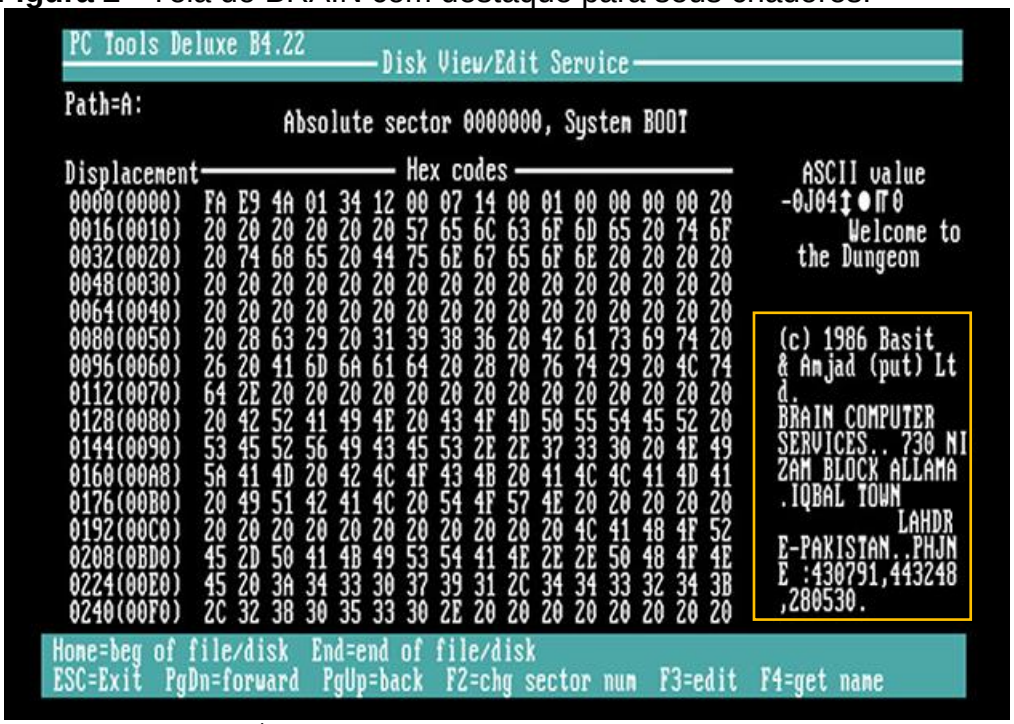
Banking trojans são malwares com funcionalidades de capturar informações bancárias em sites de bancos, comércio eletrônico e em redes sociais.

2.2 A evolução dos malwares

A teoria de NEUMANN (1966), na qual autômatos poderiam se auto-reproduzir, tornou-se uma explicação teórica do que mais tarde veio a ser apresentado como o primeiro vírus de computador, o *creeper.* (RAJESH, REDDY e REDDY, 2015) Desenvolvido por Bob Thomas e aprimorado por Ray Tomlinson em 1971, o creeper ao ser injetado em um computador deixava uma cópia de si, e procurava outro computador na rede para invadir.

Em 1986, foi descoberto o vírus Brain, dos irmãos Basit e Amjad Farooq Alvi, que o desenvolveram como forma de proteger um software que eles utilizavam. Segundo Korsakov (2014), em 1987 houve a primeira epidemia causada por um vírus de computador, mais precisamente pelo Brain. Quem utilizasse uma cópia do software sem autorização dos irmãos Farooq Alvi ativaria o Brain, que deixava uma mensagem após o ataque. Na Figura 2 é apresentada a tela do BRAIN.

Figura 2 - Tela do BRAIN com destaque para seus criadores.

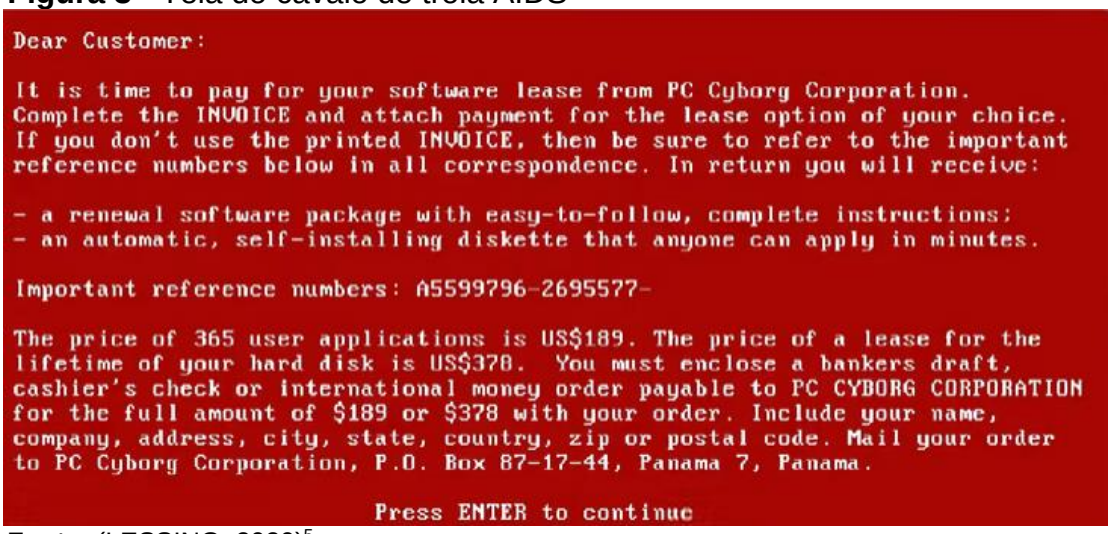


Fonte: (PAIVA, 2019)[4]

[4] PAIVA, Vitor. Primeiro vírus de computador veio antes mesmo da internet; entenda. Hypeness. 2019. Disponível em: <https://www.hypeness.com.br/2019/11/primeiro-virus-de-computador-veio-antes-mesmo-da-internet-entenda/>. Acesso em: 10 mar. 2022

Outro destaque na evolução dos *malicious software* foi o cavalo de troia AIDS (Aids Info Disk), do professor Dr. Joseph Popp de 1989, mencionado em KORSAKOV (2014, pág.38). Após infectar o dispositivo, este malware iniciava uma contagem de reinicialização da máquina e ao chegar na 90ª vez, criptografava os arquivos do sistema e deixava visível uma mensagem na tela exigindo uma quantia para desbloquear o sistema, valor que variava de 189 a 378 dólares. Iniciava neste momento o precursor do que hoje chamamos de *ransomware,* software que cobra resgate para liberar o acesso ao sistema infectado e criptografado. A Figura 3 apresenta a tela do cavalo de troia AIDS.

Figura 3 - Tela do cavalo de troia AIDS



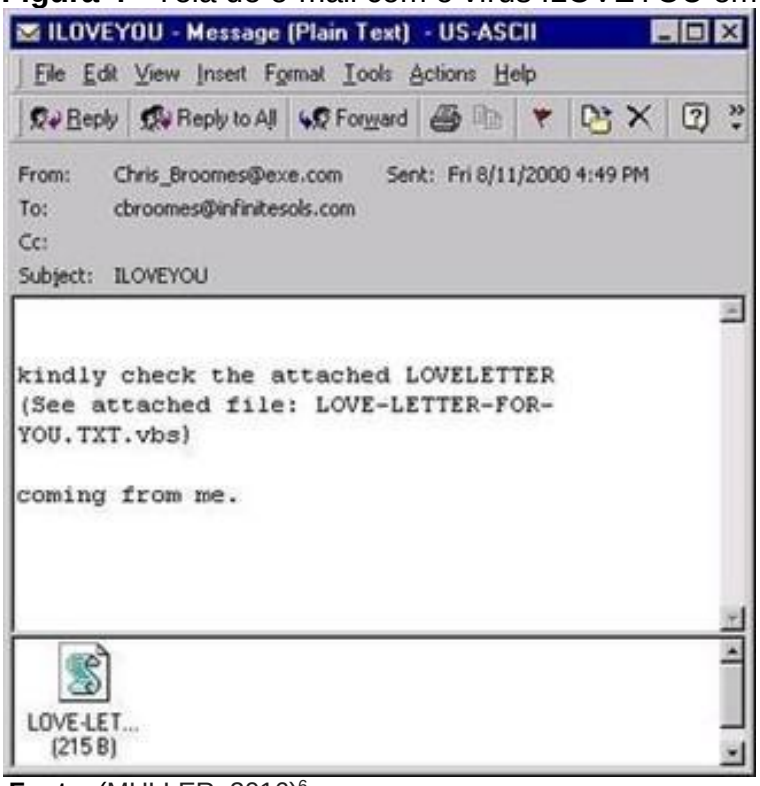
Fonte: (LESSING, 2020)[5]

O outro ponto marcante da evolução dos malwares ocorreu em 1999, com o vírus MELISSA e em 2000, com o vírus ILOVEYOU, também conhecido por LOVE-LETTER-FOR-YOU.txt.vbs, Figura 4. Esses dois vírus, sendo o segundo uma melhoria do primeiro, eram enviados por e-mail com uma mensagem chamativa que fazia com que suas vítimas baixassem o arquivo em anexo. Após aberto, o anexo tomava o controle do gerenciador de e-mail e replicava o vírus para os contatos da vítima, além de roubar os dados do computador. Na época foi estimado um prejuízo de 8,7 bilhões de dólares, e uma infecção de aproximadamente 10% dos

[5] LESSING, Marlene. Case Study: AIDS Trojan Ransomware. SDX central. 03 jun. 2020.Disponível em: <https://www.sdxcentral.com/security/definitions/case-study-aids-trojan-ransomware/>. Acesso em 24 fev. 2022.

computadores mundiais, além de congestionar a rede mundial, tendo alguns dos servidores de órgãos públicos e privados sido derrubados pelo congestionamento de envios de e-mails em massa pelas máquinas infectadas (GRIFFITHS, 2020).

Figura 4 - Tela de e-mail com o vírus ILOVEYOU em anexo



Fonte: (MULLER, 2016)[6]

2.2.1 Os malwares após a virada do milênio

Nos últimos 20 anos, tivemos uma evolução dos malwares, principalmente devido à participação de órgãos governamentais que desenvolveram seus próprios softwares capazes de realizar espionagem em dispositivos e redes sem o consentimento de seus usuários. Tal informação veio a público principalmente em 2013 com a apresentação de documentos vazados por Edward Snowden sobre a agência americana que realizava espionagem em toda rede de computadores (WOOD e WRIGHT, 2015). Outros responsáveis pela criação de malwares são os hackers em geral, que desenvolvem suas próprias soluções, quanto roubam malwares já prontos de governos ou outras entidades. Por exemplo, malwares do governo americano

[6] MULLER, Léo. 6 dos vírus de computador mais icônicos da História. Tecmundo. 05 set. 2016. Disponível em: <https://www.tecmundo.com.br/antivirus/108142-6-virus-computador-iconicos-historia.htm>. Acesso em: 02 mar. 2022.

foram furtados por hackers russos e em seguida anunciados em leilões virtuais. Tal informação foi confirmada por Snowden como sendo ferramentas realmente pertencentes às agências americanas. (OLHAR DIGITAL, EL PAÍS, 2016)

Diante da quantidade gigantesca de softwares maliciosos criados todo ano, e muito deles variantes de outros já existentes no decorrer da história, apresentamos a seguir os malwares mais conhecidos e que de uma forma ou de outra alteraram a estrutura financeira-estrutural da rede de computadores após a virada do milênio.

Devido à grande quantidade de malwares desenvolvidos e suas variantes, apresentamos a seguir alguns malwares que se destacaram cronologicamente nos últimos 20 anos, e que foram destaques nos telejornais da época.

Em 2003 se destacou o SQL Slammer, que realizava uma infiltração na máquina da vítima por meio de e-mail ou fragilidade do sistema já conhecido, ou deixado por outros malwares e em seguida se replicava pela rede contaminando outras máquinas. Com isso, ocorria um congestionamento das redes de computadores, vindo a deixar diversos serviços inoperantes em vários países, a exemplo do sistema bancário indisponível, sistema dos aeroportos fora do ar devido o fluxo intenso de troca de informações entre as máquinas contaminadas, além dos ataques DDoS (Distributed Denial of Service – Negação de Distribuição de Serviço). O SQL Slammer foi detectado novamente em 2016, na Ucrânia, China, México e Vietnã. Especialistas detectaram que máquinas com IPs nestes países lançaram ataques DDoS contra 172 países (CHINDIPHA e IRWIN, 2017).

Em 2005 veio a público por meio da empresa F-Secure e RUSSINOVICH[7], o malware utilizado pela Sony BMG, um rootkit de proteção utilizado pela mesma em seus CDs a fim de que o usuário final não realizasse pirataria do conteúdo dos CDs. Segundo Hussain (2006), os rootkit instalado sem o consentimento dos usuários tornavam os sistemas mais vulneráveis para ataques, além de que os rootkits enviavam informações de uso do usuário para o criador do rootkit, que neste caso era a própria SONY e suas parceiras, colocando, portanto, o rootkit utilizado na classificação de spyware. Continuando, Hussain(2006) aponta que mesmo a SONY disponibilizando ferramentas para retirada dos rootkit, essas deixaram falhas de segurança nos sistemas dos usuários ao retirar os rootkit. De acordo com Russinovich

[7] Mark Eugene Russinovich, (1966-). PHD em Engenharia da Computação, Diretor de Tecnologia da Azure.

(2005), o rootkit era tão complexo quanto problemático e estava escondido no sistema de DRM (Digital Restriction Management), gerenciamento de restrição digital, que impedia cópias piratas. Devido ao efeito negativo da divulgação pública a empresa realizou o recall de seus CDs, além de sofrer diversos processos na justiça. Na Figura 5, consta a chamada da matéria jornalística da Folha de São Paulo, sobre o caso da Sony utilizando técnicas hackers em seus produtos.

Figura 5 - A Sony é acusada de usar técnicas de hackers.

FOLHA DE S.PAULO

UM JORNAL A SERVIÇO DO BRASIL

SEGUNDA-FEIRA, 2 DE AGOSTO DE 2021 17H58

Opinião | Política | Mundo | Economia | Cotidiano | Esporte | Cultura | F5 | Tec | Classificados | Blogs | +SEÇÕES

ÚLTIMAS NOTÍCIAS

BBC BRASIL

03/11/2005 - 15h58

Sony é acusada de usar técnicas de hackers

MARK WARD
da BBC Brasil

A divisão musical da Sony foi acusada de usar táticas de hackers para evitar que seus CDs sejam pirateados.

Um dos sistemas de proteção analisados pelo técnico de computador Mark Russinovich usa arquivos disfarçados que se escondem no sistema Windows.

A operação para a retirada do programa da Sony é extremamente difícil, e o processo levou Russinovich a afirmar que os esforços da Sony para evitar a pirataria "tinham ido longe demais".

Em resposta à crítica, a Sony BMG disse que iria providenciar ferramentas para usuários e empresas de segurança que iriam revelar os arquivos escondidos.

Parecidos com vírus

Russinovich, um famoso especialista em programação do sistema Windows, encontrou o "sistema antipirataria" da Sony-BMG quando realizou o mapeamento de seu computador com um programa utilitário, que ele ajudou a criar e que encontra os chamados *rootkits*.

Os *rootkits* começaram a ser usados por alguns criadores de vírus de computador porque eles permitem que códigos malignos sejam inseridos no sistema Windows, significando que eles não serão encontrados pela maioria dos programas antivírus.

Depois de muita análise, Russinovich percebeu que o programa "disfarçado" tinha sido instalado quando ele ouviu pela primeira vez o álbum *Get Right With the Man*, da banda Van Zant.

+lidas

1. Alvo de piadas, Barron Trump se adapta à vida de filho do presidente
2. Facções terroristas recrutam jovens em campos de refugiados
3. Trabalhadores impulsionam oposição do setor de tecnologia a Donald Trump
4. Atentado contra Suprema Corte do Afeganistão mata 19 e fere 41
5. Regime sírio enforcou até 13 mil

Fonte: (WARD, 2005)[8]

Ainda em 2008, o malware, mais precisamente um trojan, Torpig, foi detectado sendo responsável por realizar diversos ataques em aplicações diferentes na máquina infectada, segundo Stone-Gross et al. (2009) além de roubar os dados confidenciais de suas vítimas e encaminhar para o atacante, o torpig criava uma rede de bots com suas vítimas, se destacando até aquele momento pela sua complexidade e danos

[8] WARD, Mark. Sony é acusada de usar técnicas de hackers. Folha de S.Paulo. 03 nov. 2005. Disponível em: <https://www1.folha.uol.com.br/folha/bbc/ult272u47773.shtml>. Acesso em: 24 fev. 2022.

causados. A infecção ocorria por meio do rootkit Mebroot, uma ferramenta que ao infectar a vítima atacava o MBR - Master Boot Record, Registro Mestre de Inicialização dos dispositivos, ele criava um backdoor em suas vítimas e ainda hoje versões atualizadas deste rootkit continuam a ser utilizados devido a sua complexidade de ser localizado pelos sistemas antivírus.

Em 2010 tivemos o aparecimento do worm stuxnet, que realiza ataques em sistemas SCADA (Supervisory Control and Data Acquisition). Sistema utilizado para controlar processos críticos em indústrias de diversos setores. (ZHU; JOSEPH e SASTRY, 2011) apresentam em seu trabalho as fragilidades desses sistemas para sofrerem ataques externos e os possíveis ataques cibernéticos que possam ocorrer. Nesse mesmo ano ele teve notoriedade nas mídias devido ter infectado sistemas de usinas nucleares, como pode ser visto na Figura 6.

Figura 6 - Saiba como age o vírus que invadiu usinas nucleares no Irã e na Índia.

Fonte: (ROHR, 2010)[9]

A partir de 2013, tivemos o início de ataques realizados por software maliciosos que entraram na categoria de softwares de resgate, ou simplesmente Ransomware. Esses softwares eram responsáveis por criptografar determinados arquivos ou o sistema operacional como um todo, deixando para a vítima uma mensagem em tela com dados para realizar o depósito do valor de resgate, uns com temporizador de tempo. Apesar de serem facilmente retirados utilizando um antivírus, os efeitos da criptografia não eram possíveis desfazer sem a chave que apenas os atacantes possuíam. Tivemos vários ransomware, a exemplo do Cryptolocker, 2013, Petya, 2016 e o WannaCry ou WannaCrypt, 2017, Figura 7, que por sinal utilizava uma brecha existente no Windows desde 1980, no sistema SMB v1 (Server Message Block)[10], (KAO, HSIAO 2018).

Esta falha de segurança só veio a ser sanada pela Microsoft em 2017 (MS17-010)[11] , apesar de existir em funcionamento as versões v2 e v3 que são mais seguras, ainda era possível utilizar a SMBv1.

Figura 7 - Tela do WannaCry exigindo pagamento do equivalente a US$ 300 em Bitcoins

[9] ROHR, Altieres. Saiba como age o vírus que invadiu usinas nucleares no Irã e na Índia. G1. 02 out. 2010. Tecnologia e Games. Disponível em: <https://g1.globo.com/tecnologia/noticia/2010/10/saiba-como-age-o-virus-que-invadiu-usinas-nucleares-no-ira-e-na-india.html>. Acesso em: 24 de fev. 2022.

[10] Protocolo de compartilhamento de arquivos em rede - Tradução nossa

[11] Disponível em:< https://support.microsoft.com/pt-br/topic/ms17-010-atualização-de-segurança-para-o-servidor-windows-smb-terça-feira-14-de-março-de-2017-435c22fb-5f9b-f0b3-3c4b-b605f4e6a655>. Acesso em: 09 ago. 2021

Fonte: (COSSETTI, 2017 com imagem divulgação da Symantec)[12]

Em agosto de 2016 tornou-se público o conhecimento do worm Mirai, um software malicioso que ataca os IoT (Internet of Things), que contamina roteadores, modens, câmeras de segurança, DVRs (Digital Video Recorder), dentre outros, seu objetivo é realizar a contaminação do maior número de aparelhos para em determinado momento ser utilizado pelo atacante para realização de ataques DDoS. Em outubro de 2016, o mirai foi utilizado para um ataque de negação de serviços nos servidores DNS (Domain Name System) da Dyn Inc, com isso a Twitter, Netflix, Reddit e GitHub, ficaram fora do ar por algumas horas. (KOLIAS, 2017)

A infecção pelo worm Mirai continua até os dias de hoje, com suas variantes abordando fragilidades de determinadas marcas de equipamentos e das falhas do “zero day”, quando uma falha torna público e os hackers aproveitam para infiltrar o malware antes das empresas fecharem a brecha no sistema. Também é utilizado um dicionário de senhas e logins para tomar o controle do equipamento que ainda esteja utilizando senhas e logins padrão de fábrica ou clássicas por meio de força bruta.

[12] COSSETTI, Melissa Cruz. WannaCry: tudo que você precisa saber sobre o ransomware. Techtudo. 17 maio 2017. Disponível em: <https://www.techtudo.com.br/listas/2017/05/o-que-voce-precisa-saber-sobre-o-ransomware-wannacrypt.ghtml >. Acesso em: 22 mar. 2022.

2.2.2 Ataque na pandemia da COVID-19

Em 2020 veio a público o ransomware, CovidLock, este último ransomware que aproveitou o momento de pandemia para se espalhar entre os usuários de Android, disfarçado de um APK (Android Package Kit), aplicativo com informações sobre a COVID-19, causada pelo vírus SARS-coV-2, e a localização de outras pessoas contaminadas próximas. Após a vítima baixar o aplicativo era infectado pelo ransomware que criptografava os dados e cobrava o valor de U$100,00 dólares em criptomoedas. Se a vítima não pagasse o valor em 48 horas, os dados do celular seriam apagados e algumas das informações seriam vazadas em redes sociais, Figura 8, (KHAN; BROHI e ZAMAN, 2020).

Apesar do susto causado pelo CovidLock, Desai (2020) nos traz informações obtidas pela equipe da Zscaler[13] que examinou o código fonte do ransomware e chegou às conclusões de que ele não tinha contato com a internet e era possível desfazer a criptografia sem precisar pagar por resgate, informação essa também trazida por Anderson (2020) juntamente com a equipe da DomainTools[14]

Figura 8 - Tela do aplicativo CovidLock informando do golpe e cobrando o resgate.

Fonte: (ANDERSON, 2020)

[13] Disponível em: < https://www.zscaler.com/blogs/security-research/covidlock-android-ransomware-walkthrough-and-unlocking-routine >. Acesso em: 24 mar. 2022

[14] Disponível em: <https://www.domaintools.com/resources/blog/covidlock-update-coronavirus-ransomware >. Acesso em: 24 mar. 2022

2.3 A engenharia social e o fator humano

Com os avanços contínuos na infraestrutura computacional, que englobam os computadores e os demais dispositivos que interligam a rede mundial de computadores, vem diminuindo drasticamente os chamados bugs nos sistemas. Empresas têm inclusive oferecido prêmios em dinheiro para profissionais colaborarem a localizar as falhas nos sistemas. Com isso, os pacotes de correção são liberados quase todos os dias. Dessa forma os hackers podem atacar se descobrirem as falhas no sistema antes das empresas em questão, ou se conseguirem atacar antes que os usuários realizem a correção do sistema liberada pelas empresas, ao utilizarem a informação oficial da falha, no chamado ataque “zero day”. Outro ponto sensível para realização de um ataque, e que independe do tempo de encontro da falha, é utilizar o próprio usuário do sistema, que ao ser manipulado pelo atacante pode realizar qualquer pedido do mesmo a qualquer tempo. As técnicas de manipulação do usuário são abordadas na Engenharia Social, onde se estuda a personalidade humana para com isso usar as fragilidades da pessoa a fim de que ela realize os pedidos do atacante.

Segundo Mitnick e Simon (2003), o ataque com engenharia social explora as qualidades do ser humano de querer ajudar, ser educado, participante de uma equipe e o desejo de realizar um trabalho.

Nesta mesma obra, Mitnick e Simon (2003) apresentam o pensamento humano em dois modos: sistêmico e heurístico. O modo sistêmico ocorre quando analisamos as nossas decisões e as suas consequências antes de falarmos ou agir. Já o modo heurístico, é quando tomamos uma decisão baseada em decisões anteriores em situações parecidas, mas sem avaliar as peculiaridades dessa decisão nesse fato novo. De forma automática, como se tudo fosse a mesma coisa.

Diante disso, os autores ressaltam que devem levar a vítima a realizar as suas decisões de forma heurística, para que o atacante tenha sucesso na obtenção das informações e acessos.

2.3.1 O que é Engenharia Social

Hadnagy (2010) abordou o tema em seu livro, onde até aquele momento não havia uma definição abrangente sobre Engenharia Social, vindo a apresentar as

diversas formas como as pessoas definiam de forma equivocada ou incompleta, com isto, ele definiu:

> "Engenharia Social é o ato de manipular uma pessoa para realizar uma ação que pode ou não ser do melhor interesse do "alvo"[14]. Isso pode incluir obter informações, obter acesso ou fazer com que o alvo execute determinada ação"[15] (tradução nossa).

Mouton et al. (2014) afirma que Engenharia Social é:

> "A ciência de usar a interação social como meio de persuadir um indivíduo ou uma organização a cumprir uma solicitação específica de um invasor em que a interação social, a persuasão ou a solicitação envolvem uma entidade relacionada ao computador"[16] (tradução nossa).

O ex-hacker Mitnick e Simon (2003) disse que:

> "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 é, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem uso da tecnologia"

2.3.2 Características para escolha de alvos

Mitnick e Simon (2003) ressaltam 06 (seis) características observadas na escolha de alvos para ataques com engenharia social, que são elas: momento de condescendência, o desejo de ajudar, atribuição, gostar, medo e reatância psicológica.

Momento de condescendência

O momento de condescendência pode ser entendido como um momento flexível, momento que a pessoa foi cedida, ou vencida no cansaço. Por exemplo, no meio de uma entrevista com o alvo o atacante realiza perguntas importantes para si,

[15]No original: "social engineering is the act of manipulating a person to take an action that may or may not be in the "target's" best interest. This may include obtaining information, gaining access, or getting the target to take certain action" (HADNAGY, C. 2010, pag. 32)

[16]No original: "The science of using social interaction as a means to persuade an individual or an organization to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity." (MOUTON et al., 2014, pág. 5)

mas que devido à enxurrada de perguntas realizadas o alvo não prestou atenção e respondeu no impulso, repassando informações valiosas para o atacante. Dessa forma, o alvo continua na inocência de que não repassou nenhuma informação valiosa ou até percebe, mas acredita que o atacante não estava atrás dessa informação.

Desejo de Ajudar

As pessoas se sentem bem consigo mesmas quando realizam algo por outras pessoas. Há pessoas que não sabem dizer um “não” para qualquer pedido. Tem medo de serem julgadas por não ajudarem os colegas. (MITNICK e SIMON, 2003). Dessa forma, o atacante escolherá o seu alvo que tiver mais ímpeto de ajudar os outros.

Atribuição

Nessa característica o atacante faz com que o alvo crie em sua mente as melhores qualidades para esse atacante baseado em experiências passadas ou impostas pela sociedade em que vive. O atacante ser visto próximo de pessoas influentes na empresa, que esteja usando boas vestimentas, tenha uma linguagem ou que demonstre ser mais experiente na área, mostre sinais de boa educação. Isso fará com que o alvo abaixe a guarda para esse atacante, querendo até mesmo estreitar o relacionamento ou chamar atenção com seu próprio conhecimento na área.

Gostar

Dificilmente uma pessoa diz um não ou nega algo a uma pessoa que gosta, baseado nisso, um atacante ao abordar um alvo informando que conhece pessoas que o alvo admira ou que tenha sentimentos agradáveis por essas pessoas, fará com que o atacante tenha mais chances de obter as informações que procura ou que o alvo execute procedimentos que o atacante deseje. Isto na intenção de que o atacante depois fale bem do alvo para as pessoas citadas.

Também é válido se o atacante realizar elogios ao alvo, a sua forma de trabalhar e o seu desempenho. Fazendo com que ela queira retribuir esses elogios com as informações de que o atacante precisa.

Medo

Essa característica é abordada já informando ao alvo de que algo ruim está para acontecer, ao se dar conta que não terá condições de resolver sozinho já sai de sua zona de conforto. Em seguida o atacante informa que possui a solução para o caso, oferecendo ajuda para resolver o problema, e o alvo colabora com o atacante acreditando que está resolvendo o seu problema, mas que na realidade o alvo está repassando as informações que o atacante precisava.

Reatância psicológica

“A ameaça ou a perda de uma liberdade motiva o indivíduo a restaurar essa liberdade” (tradução nossa)[17].

Se o atacante convencer o alvo de que o mesmo terá que realizar trabalho em horário extra, o alvo fará de tudo para reverter essa situação, já que se sentirá que perdeu algo de importante que é a sua folga, mesmo que temporário, e com isso fará o que o atacante pedir na tentativa de restaurá-la.

Essas seis características citadas por Mitnick e Simon (2003) colaboram na escolha do alvo ideal que contribuirá com o atacante repassando detalhes da vítima, facilitando aberturas em sistemas. A escolha errada de um alvo pode levar o atacante a perda de tempo ou insucesso na realização do ataque.

Enquanto Gragg (2003) apresenta 07 (sete) características como sendo gatilhos psicológicos por trás da engenharia social:

Afeto forte – Quando o atacante provoca no alvo reações que intensificam suas emoções a fim de prejudicar o seu senso de julgamento durante o ataque. Entre o afeto forte podemos citar, raiva, medo, emoção de saber que vai receber um grande prêmio.

Sobrecarregando – Quando o atacante envolve o alvo em meio de várias informações as quais o mesmo não consegue pensar logicamente em tudo, e no meio das informações há solicitações que o alvo não deveria responder, mas acaba fazendo por não saber naquele momento se é ou não algo restrito.

Reciprocidade – retribuir um favor que já havia recebido em algum momento, ou que o atacante faz o alvo pensar que está em dívida com o mesmo.

Relacionamentos enganosos – Criar vínculos de amizade com o alvo, até repassando informações ou ajudando o alvo, falando mal ou admirando terceiros que o alvo e o atacante tenham em comum, ou que o atacante finja conhecer.

Difusão de responsabilidade e dever moral – Quando o alvo repassa informações valiosas para o atacante acreditando que o mesmo não conseguirá realizar nada com aquela informação por achar que outros funcionários o impedirão, além de que o alvo acredita que poderá reverter a situação logo em seguida.

[17]No original: “the theory holds that a threat to or loss of a freedom motivates the individual to restore that freedom.” (BREHM, S.S e BREHM, J.W. 1981. Pág. 04)

Autoridade – pessoas tendem a obedecer a ordens de superiores hierárquicos, mesmo que essas ordens sejam totalmente prejudiciais, e mesmo que nunca tenham conhecido pessoalmente esse chefe, sejam essas ordens dadas pessoalmente ou por telefonema.

Integridade e Consistência – as pessoas tendem a cumprir com os compromissos assumidos no local de trabalho e a realizá-los mesmo achando que possam estar errados. Isso ocorre porque elas avaliam a outra pessoa que realizou o pedido como incapaz de realizar um pedido prejudicial.

Podemos chegar à conclusão ao analisar Mitnick e Simon (2003) e Gragg (2003) que ambos definiram termos diferentes, mas com sentidos parecidos na escolha e tratamento com o alvo para realizar o ataque.

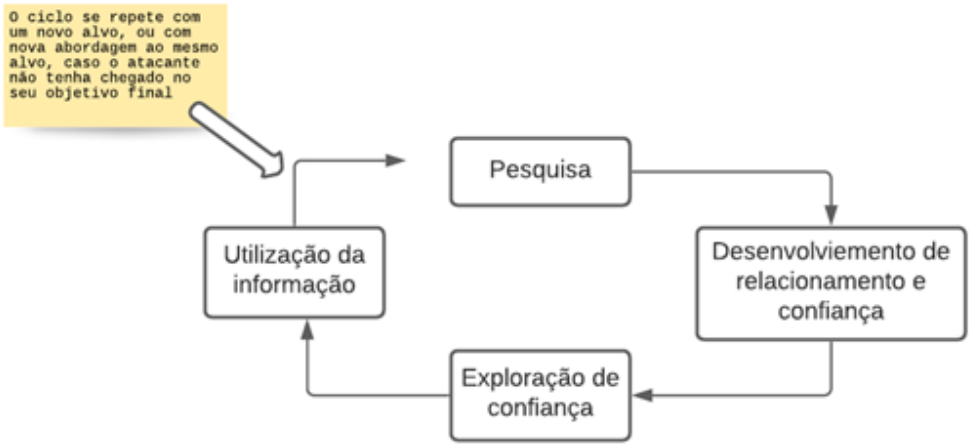
Analisando a obra de Gragg (2003) e a de Mitnick e Simon (2003) apresentam características que nos levam aos 06 princípios de persuasão de Cialdini (1984). Esses princípios foram apresentados em 1984 após uma pesquisa de campo que durou três anos, onde ele trabalhou e observou outros vendedores na prática, na tentativa de descobrir como os vendedores, independente do que estivesse vendendo, conseguiam obter êxito nas vendas, e descobriu essas características: afinidade, autoridade, coerência e compromisso, escassez, prova social, reciprocidade, como necessárias para persuadir uma pessoa. Sua obra é referência mundial em marketing e em outros setores do convívio social, onde se procura obter vantagem das relações interpessoal. Da mesma forma, vemos esses princípios citados, pelos nossos autores acima estudados utilizando dentro da Engenharia social, onde o atacante utiliza-se desses princípios para obter informações sobre o seu alvo, “a vantagem”.

2.3.3 Formas de ataque

Uma das primeiras formas de ataque mais popular utilizando engenharia social, e a mais difundida, foi o ciclo de Mitnick apresentado na obra de Mitnick e Simon (2003), que também foi citado por Mouton, Leenen e Venter (2016) o qual ainda definiu as etapas desse ciclo em trabalho anterior (MOUTON et al., 2014), já que na obra de Mitnick e Simon (2003), a explicação para cada etapa ficou muito ampla, segundo Mouton et al. (2014).

Vale salientar que o ciclo de Mitnick, conforme mostrado na Figura 9, era a forma como ele utilizava para realizar os seus ataques até 1995, quando foi preso pelos seus crimes.

Figura 9 - Ciclo de ataque de Mitnick utilizando Engenharia Social.



Fonte: MITNICK e SIMON (2003) com adaptações.

Em contexto geral, Mouton et al. (2014) quis dizer que:

Pesquisa é a fase onde o atacante buscará o maior número de informações sobre o alvo, em diversas fontes, tais como: vasculhando redes sociais, suas preferências na internet, observando o alvo pessoalmente, o que ela faz no dia a dia, buscando informações com amigos e colegas de trabalho.

Desenvolvimento de relacionamento e confiança, onde o atacante utilizando das informações obtidas na etapa anterior iniciará contato com o alvo a fim de obter um relacionamento mais próximo de confiança com a mesma, como uma cumplicidade, admiração, podendo se utilizar de elogios sobre a forma como o alvo desempenha o seu trabalho, massageando o ego dela elogiando suas vestimentas, penteado, etc. Vale até citar nomes de pessoas conhecidas do alvo (MITNICK e SIMON, 2003), ou até demonstrando ser alguém que possua um cargo acima do alvo para que ela se sinta no dever de colaborar com as informações que o atacante solicita.

Exploração de confiança, nesta etapa logo após criado um vínculo com o alvo, o atacante pode realizar um pedido, um favor, para o alvo o qual sem perceber pode

está repassando informações privilegiadas ou executando uma ação que coloque o atacante mais próximo de obter sucesso no ataque a vítima.

Utilização da informação, nesta etapa o atacante utilizará as informações repassadas pelo alvo, ou a brecha criada para finalmente seguir com seu ataque contra a vítima ou então chegar em outro ponto que necessite, de mais detalhes, vindo a repetir o ciclo de Mitnick, podendo utilizar o mesmo alvo, ou partindo para outro que possua informações privilegiadas mais restritas.

Mouton, Leenen e Venter (2016) apresentou um modelo de ataque de engenharia social diante das comparações de diversos ataques por meio de engenharia social e que os pesquisadores viram que existia semelhanças tanto pela forma de **comunicação, meio, objetivos, princípios ou técnicas de conformidade**.

Vale salientar que Mouton et al. (2014) determinou um modelo ontológico[18], onde um ataque baseado em engenharia social deveria ter:

- **Um tipo de comunicação**:
    - direta (subdivide em bidirecional e unidirecional);
    - indireta (quando o atacante realiza uma operação que faz com que o alvo realize algo que já era esperado ele fazer sem ninguém pedir);
- **Um engenheiro social:** pode ser um indivíduo ou organização;
- **Um alvo:** pode ser um indivíduo ou organização;
- **Um meio:** a forma como a comunicação será realizada, podendo ser por e-mail, face a face ou telefone;
- **Um objetivo:** o que o atacante deseja ganhar com a realização do ataque, podendo ser ganho financeiro (resgate, transferência de valores), acesso não autorizado a um sistema, como banco de dados, informações sigilosas, interrupção de serviços, como de saúde, energia, gás, dentre outros;
- **Um ou mais princípios de conformidade**: características marcantes no alvo que atendem as necessidades do atacante, ou seja, que demonstram que o alvo será mais fácil de repassar as informações que o atacante deseja;

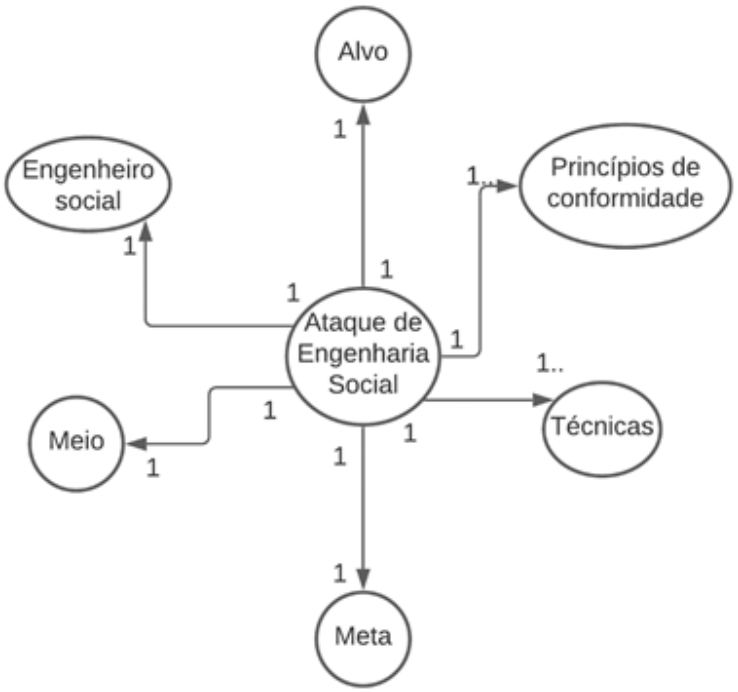
[18] É um modelo de dados que reúne vários conceitos dentro de um domínio e os relacionamentos entre os conceitos.

- Mouton et al.(2014) dá como exemplo em seu trabalho, os seguintes princípios: Amizade ou gosto (um alvo tende a repassar informações para pessoas conhecidas); Compromisso ou consistência (O alvo tende a ser mais solícito com pedidos ligados a sua posição ”massagem no ego”); escassez (O alvo tende a atender solicitações que ocorrem raramente); reciprocidade (O alvo atende solicitações de pessoas que já tenham feito algum favor anteriormente), validação social (Se o alvo acreditar que o pedido feito a ele é algo socialmente correto, ele fará), autoridade (pedidos feitos por superiores hierárquicos ou autoridades são mais fáceis de serem realizados);

- Uma ou mais técnicas: (técnicas diferenciadas tais como phishing, troca de informações de valores semelhantes - também conhecido por “quid pro quo”)

Na Figura 10 podem ser vistos os elementos de um ataque de Engenharia Social.

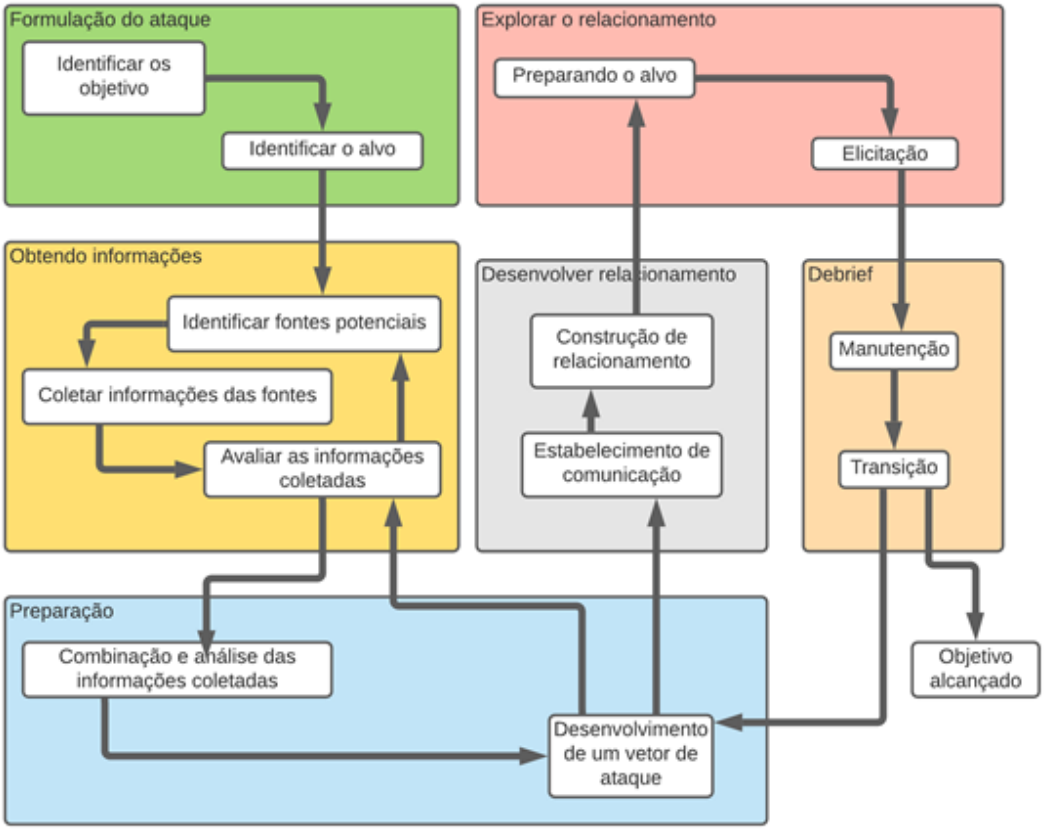
Figura 10 - Modelo ontológico do ataque de Engenharia Social proposto por Mouton.



Fonte: MOUTON et al. (2014), com adaptações.

Mouton et al. (2014) apresentou o ciclo de Mitnick de uma forma expandida e mais detalhada para abranger os diversos tipos de ataques baseado em engenharia social, conforme pode ser visto na Figura 11 a seguir.

Figura 11 - Modelo de ataque utilizando Engenharia Social[19]



Fonte: MOUTON et al. (2014), com adaptações.

2.3.4 Defendendo-se

Apresentamos a seguir comparativos de alguns estudos mostrando as melhores práticas para combater a Engenharia Social. É válido destacar que mesmo com as alternativas apresentadas, ainda persiste o fator humano como a brecha para o ataque bem sucedido.

[19] Tradução nossa para: Social Engineering Attack Framework.

2.3.4.1 Método humano versus método computacional

SALAHDINE e KAABOUCH (2019) apresenta em seu trabalho medidas que empresas e pessoas podem utilizar para minimizar os ataques de engenharia social, abordando o aspecto humano ou computacional.

No aspecto humano a medida principal seria o treinamento, fazendo com que o usuário tenha consciência do que é um ataque baseado em engenharia social. Ao mesmo tempo em que o treinamento é de fácil implementação e baixo custo para ser realizada, sua efetividade ainda esbarra em fatores humanos, dado que as pessoas são facilmente influenciadas emocionalmente, realizam decisões subjetivas, baseado em sentimentos pessoais, neste caso se a vítima acreditar que o atacante é uma boa pessoa, ou confiável ele atenderá ao pedido do atacante, pois tendem a confiar em seu julgamento pessoal do caráter das pessoas, vindo assim, a realizar o pedido da pessoa ao qual criou um vínculo com a vítima como colega de trabalho, ou uma pessoa para a qual deve um favor, mesmo que por educação, e baixam a guarda com relação aos protocolos de segurança da empresa / sistema.

Por outro lado, a medida de proteção baseada no computador utiliza softwares e ferramentas e é eficiente e precisa para evitar o ataque de engenharia social. No entanto, ela se torna cara, além de ser específica para determinadas ações, não abrangendo outras variantes do ataque.

A tabela 1, apresentada por SALAHDINE e KAABOUCH (2019), traz as ferramentas e softwares analisados com seus prós e contras na defesa de ataques baseados em engenharia social.

Tabela 1 - Comparação de contramedidas e técnicas de mitigação baseadas em computador.

Técnica	**Descrição**	**Vantagens**	**Limitações**
Ferramentas de filtragem	Ferramentas anti-phishing	Pode bloquear e-mails de phishing e sites	Ineficiente; os invasores podem enviar internamente e-mails; limitada por humanos; ferramentas caras

Alerta e software de digitalização	Antivírus, anti-spam, anti-scams	Eficiente em alertar; eficiente na digitalização; produtos com segurança forte;	Produtos caros; alertas ignorados por humanos
Soluções biométricas	Com base em características biológicas;	Distinguir perfis reais de falsos através de seus traços biológicos; eficiente;	Pode ser imitado
Inteligência artificial	Com base em sistemas de aprendizagem adaptativa	Eficiente, adaptativo	Complexo
Baseado em aprendizado de Máquina	Baseado na aprendizagem	Resultados bons; eficaz; aprendizagem online;	Complexo
Estrutura de Anti Engenharia social	Centrado em engenharia social de avaliação de risco	Eficiente; alta probabilidade de ataques	Muito caro
Threshold-based Baseado em limite	Usa limites para detectar ataques	Fácil	Não eficiente; limitado pelo valor do limite (threshold)
Baseado em telefone	Usa telefone	Fácil	Companhias telefônicas não são capazes de parar os robôs de ligação (robocalls)
Lista de permissão de fluxo	Identifica tráfico legítimo e malicioso que chega à rede da empresa	Eficiente; baseado em aprendizagem; capaz de distinguir tráfego legítimo e malicioso	Limitado pela consciência humana; Ignora os alarmes
Baseado em IDS	Sistema de detecção de intrusão	Capaz de detectar atividades suspeitas	Alta taxa de alarmes falsos

Fonte: SALAHDINE e KAABOUCH. 2019, p.13.

2.3.4.2 Defesa em níveis

Gragg (2003) abordou uma defesa contra ataques de engenharia social baseado em níveis de acordo com os 07 gatilhos psicológicos mencionados anteriormente, na seção 2.3.2, Características para escolha de alvos. Ele dividiu a defesa em 06 níveis sendo eles: **Fundamental, Parâmetro, Fortaleza, Persistência, Gotcha, Ofensivo**. O intuito de dividir em camadas é para que se o hacker conseguir penetrar em uma das camadas, ele possa ser parado na próxima camada, ou que a vítima seja capaz de identificar que está sendo atacada e possa contra-atacar.

No **Nível Fundamental** são apresentadas as políticas de segurança com foco em engenharia social. Gragg (2003) diz que “os usuários finais não devem estar em uma posição onde tem de considerar se certas informações podem ou não ser fornecidas”[20]. Essa situação deve ser planejada previamente para que cada usuário saiba qual o seu papel na empresa e até que ponto pode fornecer determinada informação.

Nas políticas de segurança são abordados o controle de acesso às informações, as configurações de contas, a aprovação de acesso e alterações de senhas, as fechaduras das portas, as identidades, as escoltas de visitantes e a trituração de papéis da empresa antes de irem para o lixo.

Neste nível o funcionário estará apto a se defender de ataques que utilize os gatilhos de Autoridade e Difusão de responsabilidade ou Dever moral, com isso o funcionário ao atender um atacante se passando por uma pessoa com poder de chefia, se sentirá à vontade para se recusar a realizar o pedido que foge do seu escopo de trabalho, podendo orientar a procurar a pessoa responsável pela informação.

O **Nível de Parâmetro** consiste no treinamento de conscientização de segurança para todos os usuários. Neste nível os funcionários são treinados para identificar sinais de um possível ataque baseado em engenharia social, como um engenheiro social trabalha, os tipos de perguntas mais comuns utilizadas por eles, as formas utilizadas para abordar as vítimas e que tipos de informações eles procuram.

O **Nível de Fortaleza** é responsável por realizar o treinamento da equipe que estará em contato direto com os demais funcionários da empresa ou usuários do

---

[20] “End users should not be in a position where they have to consider whether or not certain information can be given out” pag 11, (GRAGG, 2003) tradução nossa

sistema, dando suporte para trocas de senhas, problemas no sistema, tirando dúvidas, dentre outros. Como esse pessoal concentra a maior parte das informações sensíveis que um hacker ou engenheiro social necessite para realizar um ataque, logo serão os primeiros alvos deles, já que o contato é realizado por telefone ou sistema. O pessoal que passará por este treinamento também vai lidar com pessoas de diversas patentes, desde o estagiário até o presidente da empresa, e com isso deve estar preparado para negar uma informação que é solicitada sem a devida autorização. Dentre as formas de treinamento, o autor cita: Inoculação, Advertência e verificação de realidade.

No treinamento por inoculação, temos um paralelo com o ato da vacinação, onde a pessoa recebe um vírus enfraquecido para criar anticorpos contra a doença. No treinamento ocorre fato semelhante, onde os funcionários conhecerão argumentos utilizados por engenheiros sociais durante um ataque. Para o sucesso desse tipo de treinamento, o instrutor tem que ser capaz de apresentar os argumentos reais e os mais variados possíveis que um atacante possa utilizar, dessa forma os funcionários reconhecerão quando estiverem sendo atacados.

No treinamento de advertência é repassado para os funcionários as implicações que ocorrem se um ataque hacker for bem sucedido, quais são os prejuízos causados por ele e que mesmo conhecendo os argumentos utilizados no ataque, eles podem sofrer mudanças para beneficiar o atacante.

O Nível de persistência consiste em criar hábitos de verificar constantemente as regras de segurança contra os ataques de engenharia social por meios de lembretes, avisos, qualquer que seja a forma adotada pela empresa ou sistema, pode ser um checklist diário ou semanal. Todo conhecimento adquirido durante um treinamento pode ser perdido, caso não venha ser usado na prática, ou venha sofrer um ataque muito tempo depois de um treinamento. Com os avisos diários, os usuários sempre terão em mente o treinamento que receberam. Esses avisos tem que ser de uma forma que o usuário seja obrigado a ver ou interagir. Podemos citar como exemplo, janelas flutuantes com uma série de avisos que o usuário terá que interagir ao entrar no sistema.

O nível Gotcha[21], também chamado por Gragg (2003), de SELM (Social Engineering Land Mines), Minas Terrestres de Engenharia Social, consiste em criar armadilhas, tanto no sistema como na própria empresa, a fim de expor o intruso que

[21] “Gotcha” em tradução nossa: “Peguei vocês”

adentrou na empresa se passando por funcionário ou outra pessoa qualquer que esteja coletando informações para realizar um ataque posteriormente ou o ataque via sistema que esteja em andamento. Segundo o autor, as ideias para essas iscas são infinitas e vai de acordo com o responsável pelo setor de segurança, quanto mais qualificado e experiente, ele for, mais criativo será às SELM.

Podemos citar como exemplo, os avisos de log em e-mail, quando um determinado sistema é aberto em um computador pela primeira vez ou em computador não habitual para ser aberto, avisando assim, o responsável pelo setor de segurança que uma atividade fora do comum está acontecendo, para ser avaliado e tomado providência.

Um responsável por cada setor que verifique os transeuntes naquele setor e se apresentasse para auxiliar e ao mesmo tempo indagar o que estão fazendo e para onde estão indo, já encaminhando-os para seu destino sem permitir que interaja com o ambiente, mesas, armários, computadores do setor para obterem informações úteis para um ataque ou até mesmo iniciar um ataque daquele local.

O **Nível ofensivo**, o autor afirma que todos da empresa devam saber como agir quando um ataque ao sistema for iniciado, repassando para os demais o alerta de que o sistema está sob ataque e que a equipe responsável pelo contra-ataque comece os procedimentos, (GRAGG, 2003) salienta que esta equipe deva ser a mesma que monitora os logs do sistema, ou que tenha acesso aos logs do sistema que comunicou a invasão.

2.3.4.3 Personalidade versus Engenharia Social

UEBELACKER e QUIEL (2014) apresentaram uma correlação entre os ataques e os cinco fatores da personalidade descritos por MCCRAE e COSTA (2008), sendo estes fatores aceitos para traçar a personalidade de um indivíduo em processo de recrutamento realizado pelos recursos humanos de empresas. Estes fatores são: Abertura a novas experiências, Conscienciosidade, Extroversão, Neuroticismo e Simpatia.

No estudo apresentado por UEBELACKER e QUIEL (2014), eles apresentam que a personalidade do indivíduo impacta nos resultados obtidos através de um ataque utilizando engenharia social. Dos cinco fatores de personalidade de MCCRAE

e COSTA (2008), eles mostram que indivíduos que possuem Abertura a novas experiências, Conscienciosidade e Extroversão, tendem a serem alvos mais propensos a ataque baseado em engenharia social.

Eles apontam que para a conscienciosidade o indivíduo estaria disposto a trocar dados sigilosos por uma vantagem onde levaria em conta o custo-benefício da ação. Segundo PARRISH JR, BAILEY e COURTNEY (2009) em um estudo sobre ataques phishing essa quebra de segurança ocorreria com indivíduos treinados e que conhecem os padrões e procedimentos contra os ataques, se contrapondo ao esperado, já que um indivíduo treinado deveria ser resistente a ataques.

No estudo de DARWISH, EL ZARKA e ALOUL (2012) eles apresentam que indivíduos quanto mais extrovertidos e simpáticos, mais aumenta o risco de sofrerem ataques cibernéticos, destes, os jovens são os mais propensos a apresentarem altos índices de extroversão e simpatia, e separando por sexo, as mulheres seriam mais simpáticas do que os homens, sendo assim primeira escolha numa investida em realizar um ataque.

WEIRICH e SASSE (2001) apresentam em seu trabalho o porquê as pessoas extrovertidas tendem a quebrar regras de segurança, é porque querem evitar uma imagem negativa de si mesmas, já que indivíduos que seguem as regras de segurança são vistos como paranoicos, pessoas antissociais, nerds e até mesmo indivíduos que não fazem parte do coletivo. Logo, indivíduos introvertidos seriam alvos difíceis para ataques baseados em engenharia social, por não ligarem para julgamentos sociais de outros indivíduos.

JUNGLAS e SPITZMULLER (2006) diz que indivíduos com alta abertura para experiência são por natureza curiosos e estão mais aptos a tentar novas experiências e têm bom desempenho em programas de treinamento, mas, devido a isso são mais propensos a sofrerem ataques relacionados a privacidade, devido acreditarem mais nas vantagens do que nas desvantagens das novas experiências que se submetem.

Em contrapartida indivíduos com traços de personalidade neurótica, segundo JUNGLAS e SPITZMULLER (2006) tendem a ser inseguros e muito preocupados com falhas ou riscos potenciais. Esses indivíduos tendem a pensar em eventos negativos e possíveis perdas se sobrepondo a possíveis benefícios que poderiam receber. Sendo assim, seriam alvos difíceis de repassar informações através da engenharia social.

3 METODOLOGIA

Segundo Lakatos e Marconi (2003, pg.183, 9.1.2):

> “A pesquisa bibliográfica não é a mera repetição do que já foi dito ou escrito sobre certo assunto, mas propicia o exame de um tema sob novo enfoque ou abordagem, chegando a conclusões inovadoras.”

Diante disso foi realizado um levantamento bibliográfico com o intuito de mostrar a ligação entre os ataques de malware e a engenharia social, sendo realizado um levantamento bibliográfico em cima de livros e trabalhos científicos disponibilizados no formato eletrônico colhidos após uma pesquisa no Google Acadêmico, utilizando-se pesquisa pelos tópicos (“social engineering attacks” and “malware”) no espaço temporal entre os anos de 2005-2021 ordenados por relevância sugerido pelo Google Acadêmico. Em seguida realizou a verificação dos trabalhos apresentados se atendiam aos requisitos da pesquisa, descartando os trabalhos que fugiam do escopo dessa pesquisa. Optou-se por usar termos na língua inglesa devido as publicações mesmo em português, possuírem resumo em inglês e assim abranger uma quantidade maior de trabalhos acadêmicos para avaliar. Também foram descartados trabalhos em outras línguas.

4 RESULTADOS E DISCUSSÕES

No decorrer deste trabalho apresentamos os diversos tipos de ataques cibernéticos, abrangendo desde o vírus Brain (1986) - considerado o primeiro a realizar infecção em vários computadores a nível mundial (vide seção 2.1.1.1) -, aos mais variados tipos de malware apresentados na seção 2.1.1.

Dentre os malwares apresentados, vimos que cada um tem sua forma própria de contaminação e *modus operandi* diferenciados. Tais malwares podem se espalhar entre os computadores, replicando-se, travando sistemas, espionando a vítima e coletando dados para repassar a terceiros (seção 2.1.1.4), criptografando arquivos (seção 2.1.1.10) ou utilizando o poder computacional da máquina invadida em favor do invasor (seção 2.1.12).

Todas essas formas de ataque tiveram em algum momento a utilização da engenharia social para ser concretizada. Desde convencer a vítima a inserir um disquete, CD ou pen drive na máquina até o envio de e-mails chamativos com propagandas de ofertas imperdíveis, ganho de premiação, alertas de cobranças, por meio de técnicas de phishing (seção 2.1.1.5).

Também foi possível acontecer o ataque por meio de trocas de benefício, em que o atacante oferece softwares ou serviços gratuitos na internet, desde que a vítima dê consentimento ou não para a instalação de um software de monitoramento que vai oculto. Através dele o atacante coletará informações de navegação da vítima, muitas vezes sem a vítima saber realmente que está havendo a coleta de seus dados pessoais, por meio dos Adware (seção 2.1.1.6).

Destacamos outra forma de infecção via Engenharia social, realizada quando permissões foram dadas pelos próprios usuários ao utilizar mídias com direitos autorais, a exemplo dos produtos da Sony BMG, que ao serem utilizados nos sistemas operacionais Windows, instalavam também um rootkit sem o consentimento do usuário, que passava a vigiá-lo a fim de evitar a pirataria dos produtos Sony (seção 2.2.1).

Como podemos ver no decorrer da evolução dos malwares, os ataques que ocorriam inicialmente por brechas no sistema começaram a se tornar mais difíceis de serem concretizadas devido à própria evolução das tecnologias implantadas que buscavam mitigar as falhas existentes, tal como a invasão por meio do WannaCry,

2017, que aproveitava uma falha no sistema windows existente desde 1980, (seção 2.2.1).

Com esse avanço em segurança de dispositivos e correções contínuas de falhas existentes nos sistemas, os ataques passaram a ter uma participação maior do usuário, tornando-se o principal alvo dos atacantes para concretizar a invasão. Vemos, portanto, a importância da engenharia social por trás desses ataques, uma vez que ela é usada a fim de ludibriar a vítima a realizar exatamente o que o atacante deseja, sem levantar desconfiança de que o usuário esteja caindo em um golpe e, portanto, colaborando com a invasão. Tais técnicas permitem que o ataque ocorra desavisadamente pelo usuário seja instalando um software, clicando em um link malicioso, repassando códigos de segurança, fornecendo informações sigilosas, tal como os tipos de equipamentos utilizados numa empresa ou credenciais de usuários.

5 CONCLUSÃO

Neste trabalho apresentamos os diversos tipos de ataques cibernéticos, comumente chamados de malware, detalhando os respectivos *modus operandi* através de sua história e evolução.

Demos destaque também à Engenharia Social, uma técnica de captura de informações diversas, que pode ocorrer fora do ambiente computacional inclusive, e que permite que ataques aconteçam muitas vezes sem o menor conhecimento do usuário.

Por fim, pudemos observar que, apesar de cada tipo de malware ter as suas peculiaridades no momento da ativação do ataque cibernético, eles tiveram uma colaboração da Engenharia Social em algum momento. Com o decorrer dos anos essa contribuição vem aumentando, devido às falhas nos sistemas estarem sendo sanadas mais rapidamente pelas empresas. Dessa forma os atacantes recorrem muito mais ao fator comportamental dos usuários para que seus ataques sejam bem sucedidos, uma vez que o elemento humano ainda é um ponto crítico de fragilidade do sistema, devido principalmente às características da personalidade humana, como mencionamos no capítulo anterior. Com isso mostramos que os ataques por malware estão intimamente relacionados com a Engenharia Social, sendo até um passo primordial para o sucesso de uma ação delituosa ou apenas para testes de sistemas.

Neste trabalho percebemos que mesmo equipes bem treinadas ainda tendem a cair nas técnicas de engenharia social colocando em risco a segurança do sistema, (seção *2.3.4.3)*. Diante disso ressaltamos a importância de sempre está relembrando à equipe sobre os tipos de investida baseado em engenharia social, para tanto, sugerimos o uso de cards, posts em redes sociais da empresa ou no grupo de trabalho, mensagens em tela na estação de trabalho ao realizar login no sistema, aplicação de investidas utilizando engenharia social contra os funcionários de forma lúdica para identificar os funcionários mais displicentes e adverti-los dos perigos que colocaram a empresa ao cair nas técnicas de engenharia social, além de encaminhar para uma reciclagem de conhecimento.

Para **trabalhos futuros** sugerimos avaliar o impacto do treinamento de Engenharia Social em um determinado grupo de pessoas, traçando o perfil da personalidade das mesmas. Após determinado período de tempo realizar uma

investida com base em engenharia social contra este mesmo grupo, a fim de traçar e analisar o quanto foi absorvido do conhecimento e se o perfil de personalidade das pessoas influenciou nos resultados.

Outra sugestão para trabalhos futuros, seria uma pesquisa de campo entre alunos do ensino médio e/ ou universitários a fim de saber qual foi o tipo de investida por meio de engenharia social que mais foram vítimas e qual o nível de prejuízo que sofreram ao cair nessa investida, com isso traçar um plano de orientação específica para os demais alunos, buscando educá-los quanto à necessidade de manter-se “ciberseguro”.

REFERÊNCIAS

ANDERSON, Chad. CovidLock: Mobile Coronavirus Tracking App Coughs Up Ransomware. **Domaintools**. 2020. Disponível em: <https://www.domaintools.com/resources/blog/covidlock-mobile-coronavirus-tracking-app-coughs-up-ransomware#>. Acesso em: 24 fev. 2022.

ANDERSON, Chad. CovidLock Update: Deeper Analysis of Coronavirus Android Ransomware. **Domaintools**. 2020. Disponível em: <https://www.domaintools.com/resources/blog/covidlock-update-coronavirus-ransomware>. Acesso em: 24 fev. 2022.

AYCOCK, J. **Computer viruses and malware**. Springer Science & Business Media, 2006.

BREHM, S. S.; BREHM, J. W. **Psychological reactance**: A theory of freedom and control. Academic Press, 2013.

CHAUDHRY, J.A.; CHAUDHRY, S.A.; RITTENHOUSE, R.G. Phishing attacks and defenses. **International Journal of Security and Its Applications**, v. 10, n. 1, p. 247-256, 2016.

CHINDIPHA, S. D.; IRWIN, B. V.W. An analysis on the re-emergence of SQL Slammer worm using network telescope data. SATNAC. 2017

CIALDINI, R.B. **Influence**. The Psychology of Persuasion. New York, 1984.

COHEN, F. **Computer viruses**: theory and experiments. Computers & security, v. 6, n. 1, p. 22-35, 1987.

CONFIRMADO: hackers roubaram armas virtuais do governo dos EUA. **OLHAR DIGITAL**. 2016. Disponível em: https://olhardigital.com.br/2016/08/19/seguranca/confirmado-hackers-roubaram-armas-virtuais-do-governo-dos-eua/. Acesso em: 24 fev. 2022

DARWISH, A.; EL ZARKA, A.; ALOUL, F. Towards understanding phishing victims' profile. In: **2012 International Conference on Computer Systems and Industrial Informatics**. IEEE, 2012. p. 1-5.

DESAI, Shivang. CovidLock: Android Ransomware Walkthrough and Unlocking Routine. **Zscaler**. 2020. Disponível em: <https://www.zscaler.com/blogs/security-research/covidlock-android-ransomware-walkthrough-and-unlocking-routine>. Acesso em: 22 mar. 2022

FROM Exposure to Takeover: The 15 billion stolen credentials allowing account takeover. **Digital Shadows**, 2020. Disponível em: <https://resources.digitalshadows.com/whitepapers-and-reports/from-exposure-to-takeover>. Acesso em: 28 jul. 2021.

GORDON, Sarah. Virus and vulnerability classification schemes: Standards and integration. **Symantec Security Response**. Retrieved October, 2003. v. 3, p. 2005. Disponível em: https://vxug.fakedoma.in/archive/Symantec/virus-vulnerability-classifications-schemes-03-en.pdf Acesso em: 24 fev 2022

GRAGG, D. A multi-level defense against social engineering. **SANS Reading Room**, v. 13, p. 1-21, 2003.

GRIFFITHS, James. 'I love you': How a badly-coded computer virus caused billions in damage and exposed vulnerabilities which remain 20 years on. In: **CNN**, 04 mai. 2020. Disponível em: https://edition.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html. Acesso em: 24 fev. 2022.

GRUPO de hackers vaza programas de espionagem roubados da NSA. **EL PAIS**. 2016. Disponível em: https://brasil.elpais.com/brasil/2016/08/17/internacional/1471436554_088389.html. Acesso em: 24 fev. 2022

HADNAGY, C. **Social engineering:** The art of human hacking. John Wiley & Sons, 2010.

HUSSAIN, M. A. **CD-DRM & Sony BMG**: A Case Study. 2006.

JUNGLAS, I.; SPITZMULLER, C. Personality traits and privacy perceptions: an empirical study in the context of location-based services.In: **2006 International Conference on Mobile Business**. IEEE, 2006.

KAO, D.; HSIAO, S. The dynamic analysis of WannaCry ransomware. In: **2018 20th International conference on advanced communication technology** (ICACT). IEEE, 2018. p. 159-166.

KHAN, N. A.; BROHI, S. N.; ZAMAN, N. **Ten deadly cyber security threats amid COVID-19 pandemic**. 2020. Disponível em: https://www.techrxiv.org/articles/preprint/Ten_Deadly_Cyber_Security_Threats_Amid_Covid-19_Pandemic/12278792. Acesso em 24 fev. 2022.

KOLIAS, C. et al. DDoS in the IoT: Mirai and other botnets. **Computer**, v. 50, n. 7, p. 80-84, 2017.

KORSAKOV, A. **Cryptovirology and malicious software**. 2014. Dissertação de Mestrado. Itä-Suomen yliopisto.Pg.38-39

LAKATOS, E.M.; MARCONI, M. A. **Fundamentos de metodologia científica**. São Paulo. Atlas, 5º ed, 2003.

LIPPI, Dirceu. A maior parte dos malwares ainda chega por e-mail. **ISH**. 2020. Disponível em: <https://ish.com.br/blog/a-maior-parte-dos-malwares-ainda-chegam-por-e-mail/ >. Acesso em: 22 mar. 2022.

MARCZAK, B. et al. **Stopping the press: New York Times journalist targeted by Saudi-linked Pegasus spyware operator**, 2020.

MCCRAE, R. R.; COSTA JR, P. T. The five-factor theory of personality . In: **Handbook of personality**: Theory and research.The Guilford Press, 2008. p. 159–181.

MITNICK, K.D.; SIMON, W. L. **A arte de enganar:** Ataques de Hackers: Controlando o fator humano na segurança da informação. São Paulo. Pearson Universidades, 2003.

MOUTON, F.; et al. Towards an ontological model defining the social engineering domain. In: **IFIP International Conference on Human Choice and Computers**. Springer, Berlin, Heidelberg, 2014. p. 266-279.

MOUTON, F.; LEENEN, L.; VENTER, H. S. Social engineering attack examples, templates and scenarios. **Computers & Security**, 2016. v. 59, p. 186-209.

NEUMANN, J. V. **Theory of self-reproducing automata**. Edited by Arthur W. Burks, 1966.

PARRISH JR, J. L.; BAILEY, J. L.; COURTNEY, J. F. A personality based model for determining susceptibility to phishing attacks.In: **Little Rock: University of Arkansas**, 2009. p. 285-296.

RAJESH, B.; REDDY, Y. R. J.; REDDY, B. D. K. A survey paper on malicious computer worms. In: **International Journal of Advanced Research in Computer Science and Technology**, 2015. v. 3, n. 2, p. 161-167.

SALAHDINE, F.; KAABOUCH, N. Social engineering attacks: A survey. **Future Internet**, 2019. v. 11, n. 4, p. 89.

STONE-GROSS, B. et al. Your botnet is my botnet: analysis of a botnet takeover. In: **Proceedings of the 16th ACM conference on Computer and communications security**, 2009. p. 635-647.

UEBELACKER, S.; QUIEL, S. The social engineering personality framework. In: **2014 Workshop on Socio-Technical Aspects in Security and Trust**. IEEE, 2014. p. 24-30.

VORMAYR, G.; ZSEBY, T.; FABINI, J. Botnet communication patterns. **IEEE Communications Surveys & Tutorials**, v. 19, n. 4, p. 2768-2796, 2017.

WEIRICH, D.; SASSE, M. A. Pretty good persuasion: a first step towards effective password security in the real world. In: **Proceedings of the 2001 workshop on New security paradigms**, 2001. p. 137-143.

WOOD, D. M.; WRIGHT, S. Before and after Snowden. In: **Surveillance & Society**, 2015. v. 13, n. 2, p. 132-138.

ZHU, B.; JOSEPH, A.; SASTRY, S. A taxonomy of cyber attacks on SCADA systems. In: **2011 International conference on internet of things and 4th international conference on cyber, physical and social computing**. IEEE, 2011. p. 380-388.