FUNDAÇÃO EDUCACIONAL DE FERNANDÓPOLIS
FACULDADES INTEGRADAS DE FERNANDÓPOLIS
CURSO DE SISTEMAS DE INFORMAÇÃO

MÉTODOS DE INVASÃO EM REDE DE COMPUTADORES

FERNANDÓPOLIS – SP
2022

LUCAS SANTOS SILVA
WESLEY PEREIRA DA SILVA

MÉTODOS DE INVASÃO EM REDE DE COMPUTADORES

Trabalho de conclusão apresentado como requisito parcial para obtenção do título de bacharel em Sistemas de informação das Faculdades Integradas de Fernandópolis - FIFE.

Orientador (a): Guilherme de Morais

FACULDADES INTEGRADAS FERNANDÓPOLIS
FERNANDÓPOLIS – SP
2022

MÉTODOS DE INVASÃO EM REDE DE COMPUTADORES

Lucas Santos Silva[1]
Wesley Pereira da Silva[2]
Guilherme de Morais[3]

SILVA, L. S.; SILVA, W. P.; MORAIS, G. Métodos de invasão em rede de computadores. Fernandópolis, 2022.

RESUMO: Com o avanço da tecnologia surgiram diversos métodos de invasão que comprometem dados sigilosos, com isso é necessário que redobre a segurança dos dados. É notável que os ataques vêm se tornando mais frequentes e assim exigindo um conhecimento maior dos métodos existentes de invasão e formas de proteção. O objetivo do artigo é demonstrar os mais importantes e frequentes meios de ataques e contramedidas de segurança para evitar de ser acometido. Para poder conhecer os tipos de perigos cibernéticos é preciso saber a importância da segurança da informação e saber os três princípios básicos que são a confidencialidade, integridade e disponibilidade. A diferença do termo hacker e cracker e métodos de invasão citados no trabalho, como phishing e Pharming e malwares. Realizou-se um desenvolvimento de um projeto que tem como objetivo transparecer a funcionalidade do malware keylogger, mostrando como um cibercriminosos executa suas ações maliciosas. Com isso a proposta do artigo é mostrar a importância da segurança da informação, mostrando que com o avanço da tecnologia, passam a existir novos métodos de crimes cibernéticos.
PALAVRAS-CHAVE: Métodos de invasão. Rede de computadores. Vulnerabilidade de sistemas. Segurança de dados. Malware.

COMPUTER NETWORK INTRUSION METHODS

ABSTRACT: With the advance of technology, several methods of invasion that compromise sensitive data have arisen, making it necessary to redouble data security. It is notable that attacks are becoming more frequent and thus requiring a greater knowledge of the existing methods of invasion and forms of protection. The goal of this article is to demonstrate the most important and frequent means of attacks and security countermeasures to avoid being attacked. To be able to know the types of cyber-dangers it is necessary to know the importance of information security and to know the three basic principles that are confidentiality, integrity and availability. The difference of the term hacker and cracker and methods of invasion cited in the work, such as phishing and Pharming and malware. We developed a project that aims to show the functionality of the keylogger malware, showing how a cybercriminal performs his malicious actions. The purpose of this article is to show the importance of information security, showing that with the advancement of technology, new methods of cybercrime are emerging.
KEYWORDS: Intrusion Methods. Computer Networks. System Vulnerabilities. Data Security. Malware.

[1] Estudante de graduação em Sistemas de Informação das Faculdades Integradas de Fernandópolis – FIFE – E-mail: lucas_silvashow11@hotmail.com
[2] Estudante de graduação em Sistemas de Informação das Faculdades Integradas de Fernandópolis – FIFE – E-mail: westiry10@outlook.com
[3] Coordenador do curso Sistemas de Informação. Professor das Faculdades Integradas de Fernandópolis – FIFE *Endereço para correspondência: Rua Teotônio Vilela, 1.685 – Campus Universitário, Fernandópolis – SP, 15.608-380 Tel.: (17)3465 0000 E-mail: guilherme@fef.edu.br

INTRODUÇÃO

A tecnologia é um dos meios mais importantes atualmente, ela contribui em várias formas facilitando o acesso à informação, poupando tempo, automatizando vários tipos de serviços e causando uma eficiência maior (LOPES, 2021). Após a pandemia foi notável o grande crescimento no setor da tecnologia, deste modo comprovando o porquê propende a ser tão importante e pretende evoluir cada vez mais (MACEDO, 2022).

Com o crescimento da tecnologia é necessária uma maior segurança da informação, e muitas das vezes as empresas estão correndo risco por não ter essa visão de investir na segurança e orientar usuários das formas existentes de invasão que pode acabar capturando seus dados. Existem inúmeras formas de invasão, nelas as mais comuns como um *e-mail*, clonagem de cartão, golpes em redes sociais até meios de ataques avançados como vírus, pelo meio de *malware* (LIBERATO, 2022).

Ataques em redes de computadores ou aplicações *web* vêm crescendo cada vez mais no mundo e, geralmente, são realizados na maioria das vezes, para roubar ativos sigilosos, achar vulnerabilidades em sistemas, acessar contas bancarias, ou até mesmo prejudicar um *software* ou *hardware* ou qualquer outro tipo de equipamento tecnológico que tem uma conexão com internet como um celular, *notebook*, câmera de segurança, alarmes, roteadores, entre outros (OLIVEIRA, 2022).

Dessa forma, programas ou equipamentos que são afetados por esses ataques maliciosos, são infectadas por um programa que pode tanto deixar o *software* lento, ou algum *script* que pode coletar informações que são sigilosas para o usuário ou a empresa que ele trabalha através da abertura de um *e-mail*, ou um *click* em um anúncio (ROHR, 2014). Esses *scripts* implacáveis danificam a estrutura computacional que esteja utilizando. Geralmente, esses ataques são feitos por pessoas que querem coletar alguma informação muito sigilosa, testar a eficiência de um *script* malicioso ou até mesmo por diversão.

Esse trabalho tem como objetivo de transparecer métodos de invasões existentes que pode ocasionar a exposição de dados por pessoas não autorizadas e deixar claro a importância da segurança em rede de computadores, analisando principalmente diferentes tipos de ataques e buscando soluções para obter um ambiente de rede mais seguro. A segurança da informação visa a manutenção do acesso às informações que estão sendo disponibilizados para o usuário.

Tratando-se disso, significa que toda a informação disponibilizada deve chegar ao usuário de forma segura e íntegra.

MATERIAL E MÉTODO

O método de trabalho será por meio de um artigo de pesquisa que visa a demonstração das formas possíveis de invasões cibernéticas que podem promover exposição de dados sigilosos e mostrar viáveis táticas que consigam resguardar seus dados e, desenvolver um projeto prático que demonstra a funcionalidade de um *malware keylogger*.

Para o desenvolvimento do projeto prático de um *keylogger* foi utilizado de ambiente de desenvolvimento integrado *Spyder*, manipulada na linguagem de programação *python*.

Segurança da Informação

A segurança de informação, basicamente, em termos mais simples é um conjunto de práticas projetadas para proteger as informações e dados de terceiros mal-intencionados. Visando assim em sempre manter seus dados protegidos livre de ações maliciosas que possa manter a integridade e a importância das informações (TOTVS, 2021). A segurança da informação tem seus princípios básicos e primordiais que são a Confidencialidade, Integridade e Disponibilidade.

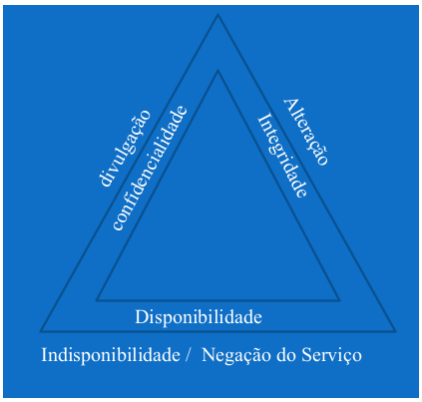

Figura 1 Princípios básicos da segurança

Confidencialidade tem como foco a privação de suas informações, que ela esteja protegida de forma que não se apresenta disponível para indivíduos ou entidades terceiras não autorizadas ao acesso e alteração dos dados, isto é só tem acesso pessoas autorizadas.

Integridade tem como foco a necessidade manter suas informações de formas exatas sem nenhuma alteração se quer acidentalmente ou maliciosamente, em outras palavras, a informação não pode ser remodelada de forma indevida.

Disponibilidade tem como foco manter os dados sempre ativos e assim acessível quando necessários para ser utilizados quando for autorizado, e para quem ele deve estar disponível. Também podem ser incluídas a preservação da autenticidade, responsabilidade, não repúdio e confiabilidade nos princípios básicos da segurança (HINTZBERGEN, 2018).

A segurança da informação, por ser diretamente envolvida com a proteção dos ativos pessoais ou empresariais, existe a possibilidade de serem invadidas por *hackers* ou *crackers*, com objetivo benéfico ou malicioso.

Hacker e Cracker

O termo *hacking* para visão de muitos é algo relacionado com a criminalidade, ou melhor, usado para fazer o mal, sendo eles exposição de dados de alguém, ou roubo de dinheiro em contas bancárias etc. Porém, esse tipo de criminalidade tem um nome, denominando-o *cracker*, que nesse caso é a pessoa que usa a habilidade para fins maliciosos.

Com o avanço da tecnologia, essa visão vem mudando a cada dia que passa, grandes empresas e governos começou enxergar essas pessoas com habilidades com a segurança de informação como um benefício, oferecendo-o a oportunidade de trabalhar com a segurança dessas empresas, governos e órgãos criando assim o *Ethical Hacking* que é a pessoa que usa suas habilidades para fins benéficos, ou seja, fazendo a proteção dos dados internos dessas empresas, e dados pessoais dos funcionários.

Uma das coisas que um *hacker* ou um *cracker* faz é um teste chamado *Pentest*, que por sua vez consiste em usar comandos em uma máquina para descobrir vulnerabilidades na rede de uma empresa ou uma *Web Application*, e com essas falhas em mãos fazer a modificação

em endereços IP's, mudança no tráfego de dados, ou alterações em *sites* modificando *layout*, menus, logotipos.

No mundo da segurança de informação, existe dois termos técnicos para definir a pessoa que usa essas habilidades tanto para fins maliciosos e para fins benéficos.

O *White-Hat* que por sua vez é destinado a fazer um tipo de teste de penetração sob a autorização da empresa para identificar vulnerabilidades que existem nelas, e fazer o *report* dessas falhas de segurança ao órgão que estiver prestando o serviço. O *Black-Hat* que por sua vez, é ao contrário do *White-Hat*, ele realiza invasões em redes e Aplicações *web* sem o consentimento da empresa ou órgão, ou seja, realiza ataques para fins maliciosos, a favor de coletar dados para benefício de si próprios.

Exemplificando o caso de um *black-hat*, existe diversas formas de invasões direcionado a espoliação de dados, um grande responsável por golpes cibernéticos que captura informações pessoais sem a autorização, até mesmo sem que o utente saiba, é o *Phishing* e *Pharming.*

Phishing e Pharming

O *Phishing* tem como seu objetivo maior ter acesso às informações pessoais, *login* e senha, números de cartão de crédito, contas bancárias, entre outros, através de um golpe cibercriminoso aonde o foco é direcionar o usuário para um *site* falso idêntico ao o original, na onde o usuário acaba não percebendo e atribui suas informações pessoais, deste modo o criminoso obterá todos os seus acessos em mãos (WAGNER, 2022).

O *Phishing* funciona geralmente em duas formas e uma delas é por um código malicioso e outra por envenenamento de DNS que é chamado de *Pharming*. Por meio do código malicioso o cibercriminoso envia um *malware* para o *e-mail* da vítima e assim automaticamente esse código nesse *e-mail* vai alterar o arquivo de *hosts* do computador, alterando a passagem natural e redirecionando o usuário para o *site* falso, igual ao original. Desta forma, mesmo que digite o endereço do *site* corretamente, sua máquina irá abrir a página falsificada.

Já o envenenamento de DNS é um meio muito difícil de acontecer, mas ela pode alcançar um grande número de vítimas quando utilizada, basicamente o *cracker* consegue

alterar a tabela de DNS de um servidor, fazendo com que vários usuários, naquele momento, que acessar o site original sejam direcionados para o site falso.

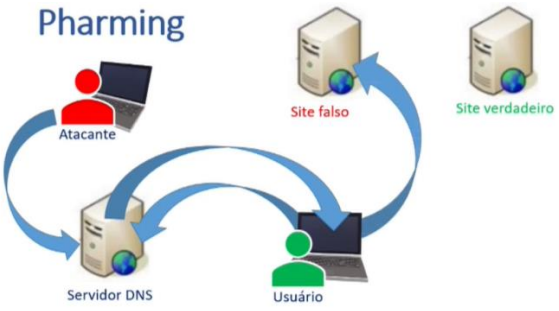

Figura 2 Exemplo de Pharming.

Infelizmente, não existe uma forma de detectar os ataques de *Phishing* e *Pharming*, mas existe algumas dicas para notar que podem indicar o método de ataque que são, cobranças estranhas de contas bancárias com frequência, programas que aparecem em sua máquina sem que você tenha instalado, entre outros.

Diferente do *Pharming*, que o *cracker* ataca o servidor DNS para manipular e capturar dados do usuário, existe os *bots* e *botsnets* que o atacante tem como objetivo portar inúmeros aparelhos em *lot* para impossibilitar a performance e operação de *websites*, servidores e computadores.

Bots e Botnet

A definição de *Bot* e *Botnet*, nada mais é de que um robô programado para realizar determinadas ações por comando de um *hacker* ou *cracker*. Criminosos virtuais usam diferentes tipos de *Malwares* especiais para violar a segurança de máquinas pessoais ou corporativas de vários usuários do mundo para implantar esse robô e ter o controle dessas máquinas e fazer a organização delas tornando uma verdadeira estrutura de computadores zumbi que pode ser gerenciada por uma só pessoa remotamente, formando assim uma rede *botnet*.

Depois de uma rede *botnet* criada, o coordenador dessa estrutura consegue enviar instruções para que ações maliciosas sejam executadas como: ataques DoS ou DDoS, roubo de dados, envio de *spam*, *phishing*, entre outros. Existe casos onde, *crackers* que fazem a criação dessa rede *botnet* com milhares de computadores zumbis, sem que o usuário saiba que está

infectado, e vendem essa rede ou até mesmo alugam para outras pessoas mal intencionadas, para realizar diferentes tipos de ataques em seu alvo.

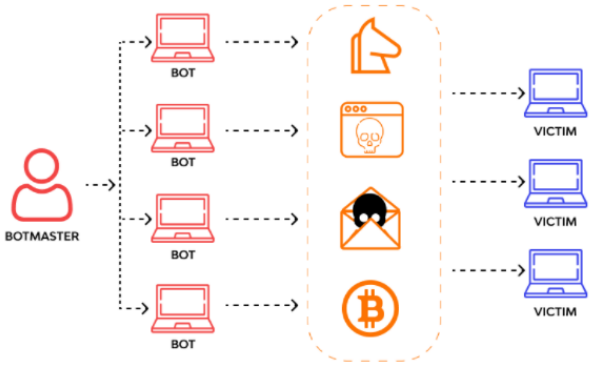

Figura 3 Estrutura de uma Botnet.

Ataque DoS/DDoS

Um ataque DoS (Ataque de negação de serviço), tem por sua vez fazer o uso de uma máquina para tirar de operação um serviço, ou seja, tem como objetivo deixar um serviço fora do ar, sendo eles uma rede ou um servidor fazendo com que *Websites* e sistemas lotados naquele servidor fique inativo. Dentre os ataques DoS, existe também o ataque chamado de DDoS (Ataque distribuído de negação de serviço), que em específico é um ataque coordenado por um *hacker* ou *cracker* que usa várias máquinas em diferentes locais atacando um só servidor, enviando várias requisições de todas as máquinas fazendo com que ele negue seu serviço e fique fora do ar, ficando disponível para o responsável explorar mais vulnerabilidades da rede, dispositivos em loT sendo eles computadores pessoais, *smartphones*, *tablets* e assim por diante.

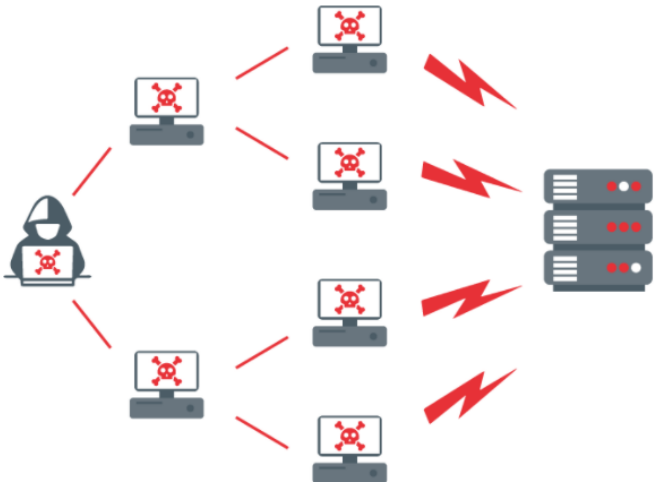

Figura 4 Estrutura de ataque DDoS.

Esse tipo de ataque também existe formas e mecanismos de se proteger, como a diminuição da área de exposição do servidor deixando apenas rotas específicas e desativando determinada quantidades de rotas onde esse servidor atinge, antivírus e até mesmo empresas especializadas para manter a segurança do serviço e do servidor (BELCIC, 2022).

As máquinas no comando de um *cracker*, como dito, que pode derrubar sites por meio de várias requisições das *botnets*, como podem ser utilizadas para a propagação de *malwares*.

Malwares

Malware em geral é qualquer tipo de *software* mal-intencionado, criado por *crackers* para danificar componentes e sistemas de uma máquina, servidor, ou até mesmo uma rede. Atualmente, existem diferentes tipos de *malwares* para todos os tipos de funcionalidade, dentre elas, são sequestro de dados para resgate, interceptação de informações, explosão de anúncios falsos, ou até mesmo para irritar uma pessoa.

Os *malwares* tem categorias para diferenciar cada um dos existentes na atualidade, como os que se espalham como um verme danificando componentes de computadores e provocando lentidão no sistema operacional, até os que roubam dados pessoais, abrem portas para um criminoso ter acesso a todos dados de pessoas (GARRETT, 2021).

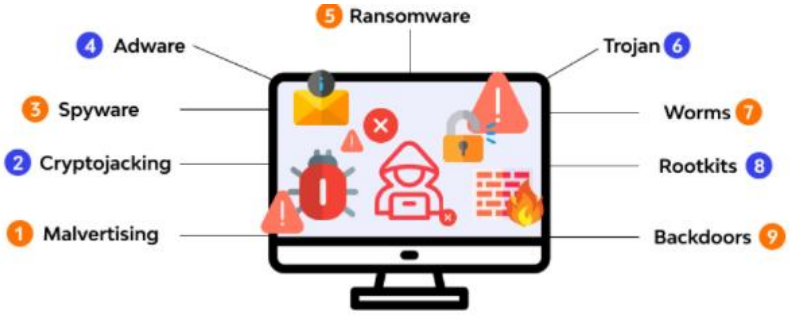

Figura 5 Exemplo ilustrativo de malwares.

Vírus é um *malware* muito comum e conhecido por diversas pessoas, seu propósito é infectar a máquina de um usuário e, assim, se propagar para outros computadores através de *pen-drives*, *sites* infectados, *e-mails* maliciosos, roteadores de internet entre outros. Desta forma, como um exemplo o vírus biológico que infecta seu hospedeiro e assim vai infectando uma grande quantidade de pessoas através de células contaminadas. O vírus é capaz de danificar seu disco rígido ou excluir arquivos armazenados em sua máquina e se for um vírus mais complexo e avançado pode se esconder e espalhar *spam* indesejados (PATRIZIO, 2021).

Spyware é um *malware* silencioso que infecta a máquina sem deixar rastros e começa a coletar dados monitorando suas atividades e copiando tudo que faz no computador como registrar tudo que você digita em seu teclado, incluindo *logins* e senhas, gravações de áudio e captura de tela, e muitos mais. Em alguns casos, o *spyware* não é considerado um *software* malicioso, pois muitas empresas implantam em suas máquinas para manter uma política de segurança assim controlando e limitando seus funcionários, pais que controlam seus filhos limitando e bloqueando sites inadequados é uma forma de *spyware*.

Uma das categorias de *spyware* bem conhecida é o *Keylogger* que sua função é determinada ao teclado de um computador, aonde ele grava todas as teclas digitalizadas, capturando senhas, dados bancários, informações pessoais. Ele pode ser malicioso quanto benigno, vai de quem implanta e qual são suas intenções. Para detectá-lo é bem difícil, como dito é um *malware* silencioso e difícil de ser notado, mas caso veja seu dispositivo esteja muito lento, congelando a tela e voltando, muitos *pop-ups* aparecendo, provavelmente, o dispositivo possa estar infectado (SEGUIN, 2022).

Ransomware é um tipo de código feito por meio de criptografia, servindo para roubar ou sequestrar dados de uma pessoa ou de uma empresa, no que geralmente esse tipo de *malware*, *crackers* criminosos usam a fim de receber algo em troca da liberação desses dados de volta

para a pessoa. A infecção ocorre por meio de algumas formas sejam elas através de *phishing* com o código malicioso em anexo, ou algo que induza o usuário a clicar em algum *link*, preencher algum formulário. Também pode ser infectado, caso o próprio sistema operacional não tenha recebido as atualizações necessárias.

Worm é um *malware* independente com objetivo de danificar sistemas, redes, servidores, componentes de um computador que se propaga sozinho como se fosse uma praga, ao contrário do vírus, pois ele é mais rápido e autônomo aonde não precisa de interação com o usuário para se propagar, *worms* não anexa a um arquivo ou programa, eles deslizam e entram em equipamentos por meio de vulnerabilidades de rede ou pelo sistema de segurança da máquina ou servidor (STIVANI, 2018). Para evitar e se proteger do *malware worms* é recomendado que seu antivírus esteja atualizado, sempre que for abrir pendrive escaneie o próprio com o antivírus para analisar se não existe algo malicioso, e nunca abrir nada suspeito, tanto em *sites* e *e-mails.*

Backdoor é um programa conhecido por criar portas vulneráveis no sistema de um computador e assim deixando sua máquina aberta para quando o *cracker* deseje voltar sem nenhuma dificuldade a um computador comprometido, pois sempre existirá uma porta do fundo aberto sem que usuários saiba e, assim, deixando sua máquina vulnerável, onde os criminosos invasores realize a invasão e consiga os dados pessoais sem deixar rastros (KOVACS, 2021).

Trojan-horse ou mais conhecido como cavalo de troia é um programa malicioso que chega de forma sorrateira, através de um presente por exemplo ou algo que parece ser bem intencionado só que na verdade é um *malware* projetado para espionar e roubar dados. Esse *malware* disfarça em arquivos legítimos enganando a vítima fazendo com que abra ou instale o arquivo e sendo atacado pelo cavalo de troia sem que ao menos saiba que o *malware* invadiu a máquina e instalou-se (BELCIC, 2022).

Rootkit é um conjunto de *software* maligno que quando instalado em um computador permite que o invasor acesse e se mantenha na máquina, livre para fazer as tarefas com controle total por acesso remoto, sem que seja detectado pelo o antivírus. Ele concede acesso de administrador ao sistema operacional, evitando de ser detectado, pois, o antivírus entenderá que o administrador esteja utilizando (BURDOVA, 2022). Sabendo da existência de tamanhos programas maléficos, existe a necessidade de contramedidas de segurança para que seus dados não sejam roubados, e evitando problemas futuros.

Contramedidas de Segurança

Torna-se necessário sempre estar atento a todos os tipos de ataque maliciosos a redes de computadores, pois desta maneira, será possível adotar modos de prevenção para garantir a segurança da informação, confira algumas contramedidas existentes para uma melhor segurança contra ataques cibercriminosos.

A primeira defesa necessária para o combate contra ataques maliciosos é o *software* antivírus, em que sua função é analisar e detectar anormalidades em seu *hardware*, além de proteger e evitar que os *malwares* infectem seu equipamento. Um dos pontos positivos é que o antivírus sempre estar atento a sites falsificados e arquivos maliciosos que são baixados em sua máquina, desta forma, sempre notificará o usuário que perigo.

Outro essencial é o *Firewall*, sua funcionalidade pode ser vista como uma barreira que restringe o tráfego da internet, monitorando a entrada e saída evitando atividades mal intencionadas de acordo com um conjunto de normas de segurança. *Firewall* pode ser um *software*, *hardware* ou os dois ao mesmo tempo.

RESULTADOS E DISCUSSÃO

Com o decorrer do desenvolvimento do artigo, foi elaborado um projeto responsável a transparecer a funcionalidade do malware *keylogger* que se enquadra na categoria *spyware* (Programa espião), desenvolvido na IDE *Spyder* na linguagem *python*. Como explícito o *malware* é voltado ao teclado do computador aonde visa detectar e gravar o que está sendo digitado e armazenar, assim, conseguindo obter dados particulares, como senhas, dados pessoais, entre outros.

```python
from pynput.keyboard import Listener
import subprocess
import smtplib
import re

arquivoLog = "C:/Log/Keylloger.txt"

def capturar(tecla):
    tecla = str(tecla)
    tecla = re.sub(r'\'','',tecla)
    tecla = re.sub(r'Key.space', ' ', tecla )
    tecla = re.sub(r'Key.enter', '\n', tecla )
    tecla = re.sub(r'Key.backspace', ' apagou ', tecla )
    tecla = re.sub(r'Key.alt_l', ' alt ', tecla )
    tecla = re.sub(r'Key.shift', ' Shift ', tecla )
    tecla = re.sub(r'Key.caps_lock', ' CapsLock ', tecla )
    tecla = re.sub(r'Key.right', ' seta direita ', tecla )
    tecla = re.sub(r'Key.left', ' seta esquerda ', tecla )
    tecla = re.sub(r'Key.up', ' seta acima ', tecla )
    tecla = re.sub(r'Key.down', ' seta abaixo ', tecla )
    tecla = re.sub(r'<96>', ' 0 ', tecla )
    tecla = re.sub(r'<97>', ' 1 ', tecla )
    tecla = re.sub(r'<98>', ' 2 ', tecla )
    tecla = re.sub(r'<99>', ' 3 ', tecla )
    tecla = re.sub(r'<100>', ' 4 ', tecla )
    tecla = re.sub(r'<101>', ' 5 ', tecla )
    tecla = re.sub(r'<102>', ' 6 ', tecla )
    tecla = re.sub(r'<103>', ' 7 ', tecla )
    tecla = re.sub(r'<104>', ' 8 ', tecla )
    tecla = re.sub(r'<105>', ' 9 ', tecla )
    print(tecla)

    with open (arquivoLog, "a") as log:
        log.write(tecla)

with Listener(on_press = capturar) as l:
    l.join()
```

Figura 6 Código do projeto *keylogger*

Todo texto digitado no computador é capturado e enviado para um documento de texto, salvando as palavras digitadas, através de um diretório programado no *script*.

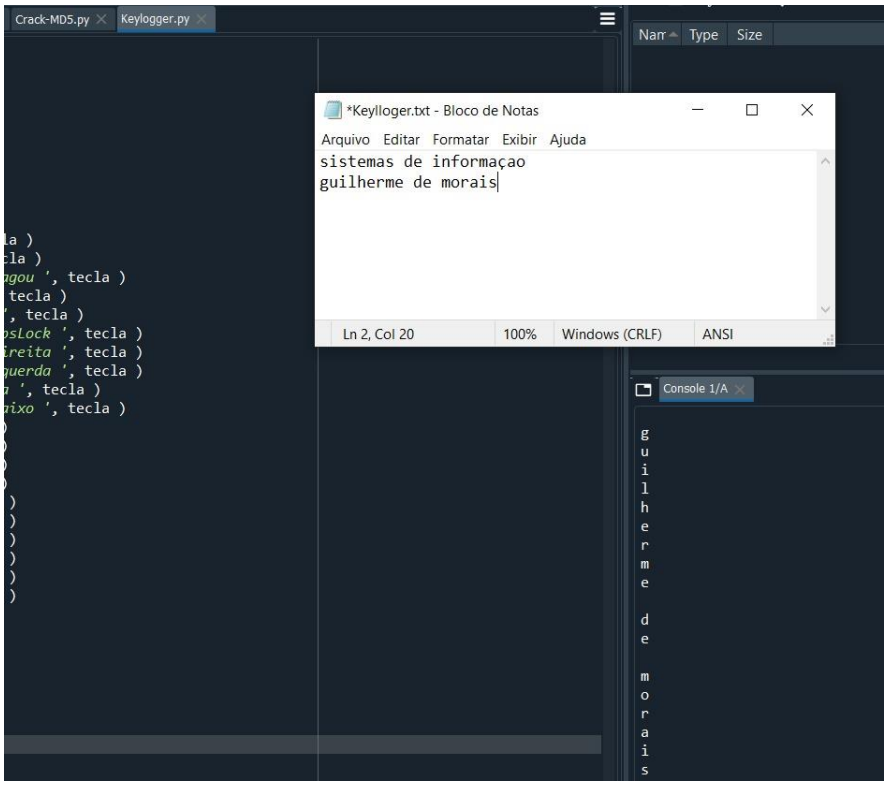

Figura 7 Palavras digitadas armazenadas no documento de texto

O intuito do desenvolvimento do *malware* mostrado no artigo, é mostrar como de fato um *hacker* ou *cracker* executa suas ações maliciosas e espiãs em máquinas de usuários convencionais ou empresariais no domínio de alguma empresa. O funcionamento do *malware* é um exemplo de como cibercriminosos conseguem obter informações de pessoas ou empresas através de um programa executável que opera silenciosamente tanto em um computador ou até mesmo dentro de um servidor. O serviço do *malware* roda sem que o usuário saiba que tudo que está sendo digitado, está sendo gravado, e todas essas informações são disponibilizadas para o criador do *malware*.

Há várias maneiras de implementação de um programa malicioso, tais como próprio dito a detecção e gravação de teclas digitadas no ativo da máquina, e isso pode ser enviado por *e-mail* para o criador do *script*, ou até mesmo conter uma rotina onde é programado para que o *malware* detecte apenas quando usuários e senhas forem digitados.

CONCLUSÃO

A proposta do artigo é mostrar como a importância da segurança da informação é essencial para qualquer pessoa ou empresa, assegurar os dados para que eles não sejam vazados, e fazer a proteção deles com várias camadas de proteção é o papel do profissional da segurança da informação. Existem vários métodos de invasão em redes de computadores, e com isso uma forma básica de evitar grande parte dessas invasões, sejam elas espiãs ou até mesmo um ataque em massa onde servidores ficam indisponíveis é usar antivírus como por exemplo *Symantec Endpoint Protection*, *Norton antivírus*, *Kaspersky Endpoint Security*, entre vários outros.

Assim como antivírus protegem aplicações de máquinas ou VM's *(Virtual Machine)* lotadas em servidores, existem também amadas de proteção feitas por esse profissional, seja por forma de um *script* na aplicação, ou validação de requisições feitas de máquinas externas como autenticação de fatores.

Conclui-se que com o avanço de novas tecnologias, há também um crescimento de crimes cibernéticos realizados por pessoas mal-intencionadas, e é de grande importância que as pessoas tenham a preocupação com a segurança dos seus dados, para que nada que vem do externo malicioso as afetem, ou até mesmo criar o hábito de sempre conferir a origem dos dados e sempre optar por ativar autenticação de vários fatores em qualquer aplicação que usar.

REFERÊNCIAS

BELCIC, Ivan. **AVAST**. Disponível em: <https://www.avast.com/pt-br/>. Acesso em: 01 de nov. de 2022.

BURDOVA, Carly. **AVAST**. Disponível em: <https://www.avast.com/pt-br/c-rootkit>. Acesso em: 01 de nov. de 2022.

GARRETT, Filipe. **TECHTUDO**. Disponível em: <https://www.techtudo.com.br/listas/2021/03/o-que-e-malware-veja-significado-tipos-e-saiba-remover.ghtml>. Acesso em: 11 de dez. de 2022.

HINTZBERGEN, Jule. Et al. **Fundamentos de Segurança da Informação:** Com base na ISO 270001 e na ISO 27002. Rio de Janeiro: Brasport Livros e Multimídia Ltda, 2018.

KOVACS, Leandro. **TECNOBLOG**. Disponível em: <https://tecnoblog.net/responde/o-que-e-backdoor-em-computacao/>. Acesso em: 01 de nov. de 2022.

LIBERATO, Rafael. **O Município BLUMENAU**. Disponível em: <https://omunicipioblumenau.com.br/tec-inova-seguranca-da-informacao-um-dos-maiores-riscos-para-pessoas-e-empresas/>. Acesso em: 19 de set. de 2022.

LOPES, Leonardo. **MIGALHAS**. Disponível em: <https://www.migalhas.com.br/depeso/342894/principais-vantagens-da-tecnologia-para-a-vida-moderna>. Acesso em: 28 de set. de 2022.

MACEDO, Bruna. **CNN BRASIL**. Disponível em: <https://www.cnnbrasil.com.br/business/setor-de-tecnologia-cresce-mais-de-60-durante-a-pandemia-aponta-estudo/>. Acesso em: 26 de set. de 2022.

OLIVEIRA, Ingrid. **CNN BRASIL**. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/levantamento-mostra-que-ataques-ciberneticos-no-brasil-cresceram-94/>. Acesso em: 09 de set. de 2022

PATRIZIO, Andy. **AVAST.** Disponível em: <https://www.avast.com/pt-br/c-malware-vs-virus>. Acesso em: 27 de out. de 2022.

ROHR, Altieres. **G1 Globo**. Disponível em: <https://g1.globo.com/tecnologia/blog/seguranca-digital/post/pacotao-virus-ao-abrir-mensagem-de-e-mail-e-compartilhamento-de-wi-fi.html>. Acesso em: 26 de set. de 2022.

SEGUIN, Patrick. **AVAST**. Disponível em: <https://www.avast.com/pt-br/c-spyware>. Acesso em: 27 de out. de 2022.

STIVANI, Mirella. **TECHTUDO**. Disponível em: <https://www.techtudo.com.br/noticias/2018/11/o-que-e-um-worm-entenda-o-malware-que-se-multiplica-sozinho.ghtml>. Acesso em: 01 de nov. de 2022.

TOTVS, Equipe. **TOTVS**. Disponível em: <https://www.totvs.com/blog/negocios/seguranca-da-informacao>. Acesso em: 10 de out. de 2022.

WAGNER, Pedro. **TECNOBLOG**. Disponível em: https://tecnoblog.net/responde/o-que-e-pharming/. Acesso em: 21 de out. de 2022.