INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA FARROUPILHA
CAMPUS AVANÇADO URUGUAIANA
CURSO TÉCNICO EM INFORMÁTICA INTEGRADO

DULY THAYNA ALVES

SEGURANÇA EM REDES DE COMPUTADORES: TIPOS DE AMEAÇAS, PREVENÇÕES E SOLUÇÕES

Uruguaiana/RS
2021

DULY THAYNA ALVES

SEGURANÇA EM REDES DE COMPUTADORES: TIPOS DE AMEAÇAS, PREVENÇÕES E SOLUÇÕES

Relatório referente ao Trabalho de Conclusão de Curso, apresentado como requisito para obtenção do título de Técnico em Informática, do Instituto Federal de Educação, Ciência e Tecnologia Farroupilha Campus Avançado Uruguaiana.

Orientador: Jhonathan Alberto dos Santos Silveira

Uruguaiana/RS

2021

DULY THAYNA ALVES

SEGURANÇA EM REDES DE COMPUTADORES: TIPOS DE AMEAÇAS, PREVENÇÕES E SOLUÇÕES

Relatório referente ao Trabalho de Conclusão de Curso, apresentado como requisito para obtenção do título de Técnico em Informática, do Instituto Federal de Educação, Ciência e Tecnologia Farroupilha Campus Avançado Uruguaiana.

Aprovado em 09 de dezembro de 2021.

BANCA EXAMINADORA

_____

Prof. Me. Jhonathan Alberto dos Santos Silveira - Orientador

_____

Prof. Me. Thiago Cassio Krug - Avaliador 1

_____

Prof. Me. Gustavo Griebler - Avaliador 2

DEDICATÓRIA

Dedico este trabalho primeiramente a Deus, por ser o meu guia nesta caminhada, a minha família e a minha mãe pelo total apoio e compreensão, também dedico a todos os meus colegas e professores do curso Técnico em informática, em especial, o prof. Jhonathan Silveira que foi o meu orientador neste trabalho.

AGRADECIMENTOS

Sou grata a Deus por ter me mantido com força neste trabalho.

Agradeço à minha família que sempre me incentivou e me incentiva nos meus sonhos e objetivos.

Agradeço ao meu orientador Jhonathan por aceitar e conduzir esse trabalho com entusiasmo e aos professores Thiago Krug e Gustavo Griebler por contribuírem para a conclusão desse.

Por fim, agradeço a todos os servidores do Instituto Federal Farroupilha do *Campus* Avançado Uruguaiana e aos meus colegas de curso, pela oportunidade de convívio e amizade.

Nenhum saber é saber completo. (Galileu Galilei)

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE ABREVIATURAS/SIGLAS

AC - Autoridade Certificadora
ASR - Redução de Superfície de Ataque
DNS - Domain Name System (Sistema de Nomes de Domínio)
FTP - File Transfer Protocol (Protocolo de Transferência de Arquivos)
HTTP - Hypertext Transfer Protocol (Protocolo de Transferência de Hipertexto)
HTTPS - Hypertext Transfer Protocol Secure (Protocolo de Transferência de Hipertexto Seguro)
IMAP - Internet Message Access Protocol (Protocolo de Acesso a Mensagens na Internet)
IP - Internet Protocol (Protocolo de Internet)
LCR - Lista de Certificados Revogados
POP3 - Post Office Protocol 3 (Protocolo dos Correios 3)
RG - Registro Geral
SMTP - Simple Mail Transfer Protocol (Protocolo Simples de Transferência de Correio)
TCP - Transmission Control Protocol (Protocolo de Controle de Transmissão)
TELNET - Virtual Network Terminal Protocol (Protocolo de Terminal Virtual de Rede)

SUMÁRIO

1 INTRODUÇÃO

Segurança de redes, um tabu enraizado para muitas organizações. Entretanto, muito essencial para as corporações, que tem como finalidade a garantia da confiabilidade, integridade e disponibilidade. Logo, esse fator se dá pela falta de informação do assunto, no qual deixa entreaberto uma porta para as vulnerabilidades a ataques.

Buscando sanar essa problemática, faz se necessário apresentar elementos de segurança como, criptografia, assinatura digital, certificado digital, autenticação e protocolos, com o objetivo de criar ou fortalecer barreiras de proteção contra software mal-intencionados que tentam roubar e espalhar o caos pelos usuários.

Visando essa proteção da máquina e da rede, o presente trabalho exibirá também cinco malwares, como suas funções, meios de propagação, proteção e remoção, para que sejam analisados e comparados perante seus atos, sendo esses malwares descritos: vírus, backdoor, rootkit, spywares e sniffing.

Em seguida, será analisado e descrito dois vírus que foram testados em uma máquina virtual, sendo um do Ransomware e o outro Trojan. Esses vírus passaram por três etapas cada de instalação, sendo cada uma das etapas diferenciadas. Portanto, cabe a este trabalho informar a importância da segurança e os reais perigos que uma máquina está sujeita a contrair.

Para que se fizesse concretizar essa programação, se fez o uso de uma prolongada procura de conteúdos, através de pesquisas bibliográficas, pesquisas na web, artigos e sistemas similares.

Este trabalho está organizado desta maneira: no capítulo 2 será apresentado os objetivos do presente trabalho. A revisão bibliográfica será tratada no capítulo 3. O capítulo 4 apresentará a metodologia utilizada para realização deste. O desenvolvimento do sistema de segurança será descrito no capítulo 5. As ameaças serão analisadas no capítulo 6, assim como sua prevenção no capítulo 7 e suas possíveis soluções no capítulo 8. As considerações finais serão apresentadas no capítulo 9. O capítulo 10 portará as referências utilizadas neste trabalho.

1.1 JUSTIFICATIVA

Muitos problemas ocasionados atualmente em redes, são ocasionados por ameaças de intrusos operacionais. Segundo o boletim de segurança (2020) da Kaspersky, “cerca de 131,4 milhões de ameaças surgiram ocasionadas pela criação de novos vírus”. Entretanto, muitas organizações não se sentem intimidados por esses novos vírus, porque não os têm conhecimento ou porque pensam que não os vale o investimento necessário.

Pensando neste aspecto, foi necessário apresentar a importância da segurança de redes, levando o conhecimento sobre os diferentes tipos de ameaças, os problemas ocasionados por elas quando instalados no sistema, as causas e as possíveis soluções.

2 OBJETIVOS

2.1 OBJETIVO GERAL

Verificar e propor possíveis soluções para as principais ameaças de computadores em segurança de redes, como também fazer o estudo de caso.

2.2 OBJETIVOS ESPECÍFICOS

1. Analisar os vírus, backdoor, rootkit, spyware e sniffing.
2. Analisar e comparar o comportamento dessas ameaças
3. Citar as formas de propagação dessas ameaças
4. Citar as formas de prevenção contra ataques maliciosos
5. Propor possíveis soluções para essas ameaças, para quando já estiverem instaladas.
6. Fazer um estudo de caso com dois vírus diferentes.

3 REVISÃO BIBLIOGRÁFICA

Neste capítulo serão apresentados os temas que norteiam este trabalho e alguns trabalhos acadêmicos dos anos anteriores relacionados a ele.

No trabalho do Mitshashi (2011), foi realizado um estudo sobre segurança de redes, no qual foram discutidas falhas na segurança, vulnerabilidades, ataques, etc. Este trabalho teve como intuito mostrar as técnicas para conseguir o máximo possível de segurança dentro de uma rede de computadores para minimizar os possíveis ataques.

Gouvêa (2016) elaborou um estudo sobre técnicas ultraleves de malware baseada em assinaturas para redes de computadores, onde ele falou sobre: programas maliciosos, prevenção de danos causados por ataques, vulnerabilidades nas redes corporativas e públicas e entre outros. A metodologia utilizada neste trabalho foi através de um levantamento bibliográfico, análise e desenvolvimento das técnicas de detecção baseadas em assinatura, etc.

Já no trabalho de Salvino (2017), foi abordado o estudo sobre segurança de redes no ambiente corporativo, onde Salvino tem como objetivo, mostrar os métodos mais confiáveis para uma organização estar protegida contra quaisquer ataques e falhas ocasionados por programas maliciosos. Neste trabalho foi realizada uma pesquisa realizada na internet em arquivos científicos, livros, etc.

4 METODOLOGIA

O quadro a seguir (Quadro 1) apresenta os procedimentos metodológicos deste trabalho de conclusão de curso.

Quadro 1 - Metodologia

Objetivo Específico	Ação
1. Analisar os diferentes tipos de ameaças	Explicar os diferentes tipos de ameaças de computadores
2. Analisar e comparar o comportamento dessas ameaças	Comparar o comportamento entre uma ameaça e outra
3. Citar as formas de propagação dessas ameaças	Explicar as diferentes formas de propagação dessas ameaças
4. Citar as formas de prevenção contra ataques maliciosos	Explicar as formas de prevenção contra determinados ataques
5. Propor possíveis soluções, para quando essas ameaças já estiverem instaladas	Trazer as melhores soluções possíveis, para possíveis ataques
6. Fazer um estudo de caso com dois vírus diferentes.	Fazer a análise de dois vírus em uma máquina virtual.

Fonte: Autoria própria

5 SEGURANÇA EM REDES DE COMPUTADORES

Este capítulo do trabalho apresenta itens importantes para a segurança em redes de computadores, proposto por esse trabalho de conclusão de curso, que está dividido em 5 partes: criptografia, assinatura digital, certificado digital, autenticação e protocolo de segurança.

5.1 CRIPTOGRAFIA

Criptografia palavra vinda do grego “kryptós” e “gráphein”, que significa respectivamente “escondido” e “escrita”, portanto, escrita oculta (MACHADO, 2014)

A criptografia ou o ato da escrita oculta, é o termo utilizado para a codificação de uma mensagem. Segundo Nakamura e Geus (2007), a codificação é a ciência de manter as mensagens seguras. Logo, esse método pode embaralhar caracteres e também substituí-lo por outros, tanto por letras quanto por números aleatórios, para que a mensagem se torne não entendível, caso haja um acesso não esperado.

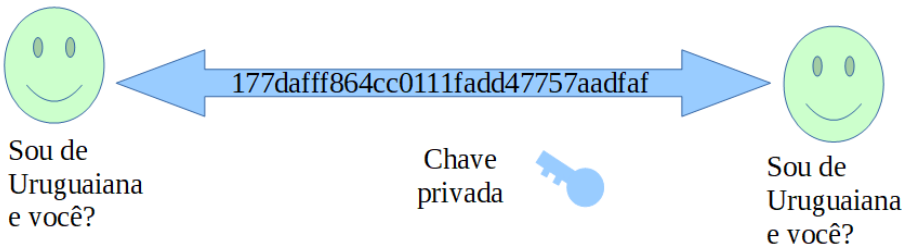
5.1.1 Chaves criptográficas

Em criptografia, “chaves” é um termo similar a senha, que é utilizado como forma de prevenção contra ataques mal-intencionados a arquivos e mensagens salvos no sistema (DOCUSIGN, 2019). A criptografia faz o uso de dois tipos de chaves, no qual são elas: simétricas e assimétricas.

Chave simétrica

A criptografia de chave simétrica, também chamada de criptografia de chave privada, é um método responsável pelo sigilo das informações, que faz o uso de uma única chave secreta, para codificar e decodificar dados fornecidos (NAKAMURA; GEUS, 2007).

Figura 1 - Chave simétrica



Fonte: Autoria própria

Segundo, o CERT (2017), “a criptografia de chave simétrica, quando comparado com a de chaves assimétricas, é a mais indicada para garantir a confidencialidade de grandes volumes de dados, pois seu processamento de dados é mais rápido”.

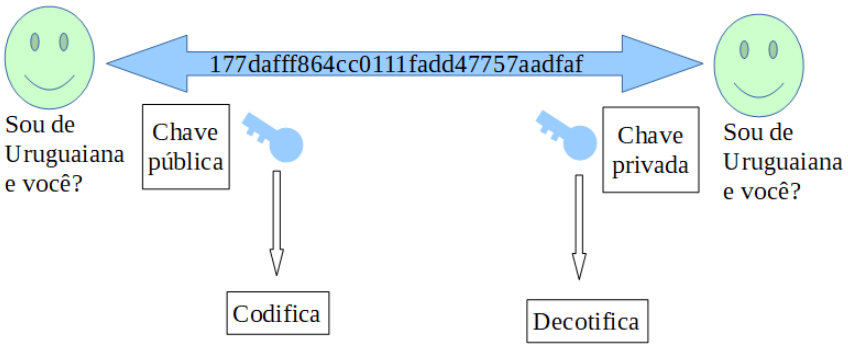
Contudo, com o uso dessa chave deve-se manter cuidado, pois, a chave precisa ser previamente compartilhada entre a origem e o destino antes de estabelecer o meio de criptografia. Logo, é importante saber que durante o processo de compartilhamento esta senha pode ser interceptada pelo atacante (MACHADO, 2014). Outro problema relacionado a esta chave é a não permissão do uso da assinatura digital e do certificado digital, podendo colocar o usuário em situação de perda de integridade, autenticidade e repúdio.

Chave assimétrica

A criptografia de chave assimétrica, também conhecida como criptografia de chave pública, é diferenciada da chave simétrica pelo uso de um par de chaves, sendo uma dessas chaves pública e a outra privada.

Logo, outro diferencial dessa chave em relação a chave simétrica, é a possibilidade do uso da assinatura digital e do certificado digital, fazendo com que a garantia da integridade, autenticidade e o não repúdio sejam maiores.

Figura 2 - Chave assimétrica



Fonte: Autoria própria

A chave pública e a chave privada servem para codificar uma mensagem e decodificar a mesma. Todavia, a mensagem só será decifrada com a chave correspondente, ou seja, se a mensagem for criptografada com a chave privada ela só será descriptografada com a chave pública e se a chave pública criptografar a mensagem só será revelada com através da chave privada (MACHADO, 2014).

5.2 ASSINATURA DIGITAL

A assinatura digital é um método “novo” de assinatura, no qual o usuário não dependerá mais do papel e da caneta para assinar um documento. Este método tem como finalidade garantir a segurança e integridade dos documentos, por ele assinados, pois permitirá a comprovação de autenticidade e integridade de uma informação gerada pelo remetente (CERT, 2017).

Este sistema de comprovação de assinatura digital, é baseado em chaves criptográficas, onde o remetente produz uma assinatura, gerando consigo uma chave pública, no qual, o destinatário conseguirá decodificar esta assinatura, com o uso de uma chave privada, completando assim o ciclo da chave assimétrica, e isso ocorre por conta da função hash. A função de hash utilizada neste método, é a parte criptografada da assinatura ou mensagem (NETO, 2013).

5.2.1 Função hash

Segundo, MACHADO (2014) a função hash trata-se de um método de resumo criptográfico, que pode ser aplicado em qualquer informação independente de seu tamanho. Todavia, essa função pode garantir através do valor gerado que a mensagem não foi alterada ao longo do percurso, se comparado com o valor do remetente com o do destinatário.

Logo, se o valor gerado for igual ao do remetente então a informação não foi modificada, se for diferente do remetente então essa informação tem forte indício de que foi alterada ou corrompida.

Quadro 2 - Hash

Entrada	**Função Hash**	**Valor gerado**
Instituto Federal Farroupilha	Hash	AA36GR45 1598PLO3 14PL6G3D MK239OI5 136QBAFF
Uruguaiana	Hash	AF35GR45 05K8P8O3 F4PL6G3E 1B239OFF 106FBAGF
Segurança de redes	Hash	1B06GR35 F590PLO3 P4P16G3D MF239OI5 176QB02F
Assinatura digital	Hash	1B0FGR38 F5902L43 10P10G3F 0F239OFE 186EB02F

Fonte: Autoria própria

5.3 CERTIFICADO DIGITAL

Certificado digital, também conhecido como RG virtual, por guardar o nome e assinatura digital, no qual é um arquivo eletrônico com validade jurídica, capaz de identificar pessoas e empresas do mundo virtual através da autoridade certificadora (AC).

A autoridade certificadora, além de emitir os certificados solicitados tem como função também, divulgar os certificados que não são mais confiáveis, ou seja, a autoridade inclui esses certificados em uma Lista de Certificados Revogados (LCR), para que as organizações sejam informadas dessas invalidades (MACHADO, 2014).

Contudo, esse arquivo digital pode-se dizer que é um meio seguro, pois faz o uso de criptografia de chave pública, gerando confiabilidade e integridade para o usuário. Logo, esse certificado pode ser dividido em dois modelos: o A1 e o modelo A3.

O modelo A1 é um arquivo eletrônico instalado diretamente no computador e não depende de cartões ou token, já o modelo A3 ao contrário do A1 faz o uso de cartão ou token, e também faz o uso de senha.

5.4 AUTENTICAÇÃO

A autenticação, bastante usada em ambientes corporativos, tem o papel de validar a identificação do usuário, ou seja, a autenticação poderá permitir ou negar o acesso do usuário no sistema da organização. Segundo Nakamura e Geus (2007) "a autenticação pode ser realizada com base em alguma coisa que o usuário sabe, em algo que o usuário possui ou em determinada característica do usuário".

- **Com base no que o usuário sabe:** esse método baseia-se em algum conhecimento do usuário, como por exemplo senhas, chaves criptográficas e dados pessoais, sendo esses elementos comuns para maioria das pessoas pela sua simplicidade.
- **Com base no que o usuário possui:** esse método de autenticação é utilizado em dispositivos que pertencem ao usuário através do uso de token, cartão ou smart card, em conjunto de senhas que o usuário sabe.
- **Com base nas características do usuário:** esse tipo de método, é o mais seguro em comparação com os métodos de cima, pois, diferentemente dos outros ele não possibilita o esquecimento e nem a perda de algo, visto que ele trabalha no reconhecimento de voz, impressão digital, reconhecimento de retina e entre outros, para a minimização de problemas.

5.4.1 Autorização

A autorização é a função vinda logo depois da autenticação. Esta função irá dizer para o usuário se ele pode ou não entrar no sistema e o que ele pode fazer como herdeiro de determinada característica válida.

5.4.2 Accounting

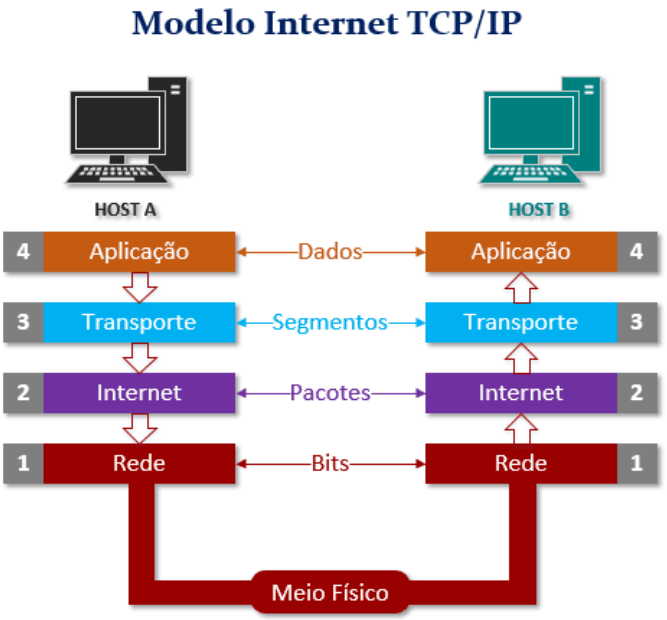
Esta função de accounting está diretamente ligada com a autenticação, pois, quando o usuário fornece seus dados à autenticação, esses dados começam a ser registrados nessa função.

5.5 PROTOCOLOS DE SEGURANÇA

Protocolo é um meio de linguagem de computador como se fosse dois ou mais computadores se comunicando através de uma mesma "língua". Este método de comunicação utiliza um protocolo padrão o TCP/IP, que significa respectivamente "Protocolo de Controle de Transmissão/Protocolo Internet", que são responsáveis por enviar e receber informações solicitadas pelo usuário (PROTOCOLOS, 2015).

A imagem a seguir representa a "comunicação" entre dois computadores através do uso de protocolo.

Figura 3 - Protocolo



Fonte: DataRain (2020)

Existem diversos protocolos dentro deste mesmo protocolo padrão TCP/IP, no mundo da internet, e alguns deles são FTP, HTTP, HTTPS, IMAP, POP3, SMTP e DNS (PROTOCOLOS, 2015).

Transferência de pastas e arquivos

- **FTP:** File Transfer Protocol - como se fosse o processo upload e download.

Transferência de páginas

- **HTTP:** Hypertext Transfer Protocol - protocolo que não emite segurança.
- **HTTPS:** Hypertext Transfer Protocol Secure - seguro pois faz o uso de criptografia.

Obs.: O URL da página que nos indicará o tipo de serviço que será prestado.

Protocolos de correio eletrônico

- **IMAP:** Internet Message Access Protocol - serve unicamente para acessar as mensagens do servidor e não baixá-las no aparelho;
- **POP3:** Post Office Protocol 3- tem a função de receber e-mails no aparelho. Quando recebido estes e-mails, por padrão eles são automaticamente apagados do servidor se não solicitado uma cópia;
- **SMTP:** Simple Mail Transfer Protocol - protocolo padrão para o envio de mensagens.

Conversão do nome

- **DNS:** Domain Name System - protocolo que tem como função converter o domínio, ou seja, o nome digitado pelo IP solicitado.

6 TIPOS DE AMEAÇAS

Esta seção tem como objetivo apresentar as ameaças que estão sujeitas a atacar os usuários do mundo virtual. Aqui serão abordados 5 tipos possíveis de ameaças, como suas características, modos de ataques e comportamentos quando instalados no sistema computacional.

6.1 VÍRUS

Vírus ou código malicioso é um tipo de malware que necessita de um hospedeiro para colocar em prática o seu dever, que é, alterar a forma de como o computador opera normalmente, sem que haja necessariamente o conhecimento do usuário (MACHADO, 2014). Logo, um vírus somente se propaga no sistema computacional quando executado pelo usuário, caso contrário ele não irá se replicar e causar danos.

6.1.1 Partes que compõem um vírus

Segundo, (VÍRUS, 2020), os vírus de computadores são constituídos por três partes, sendo essas partes: vetor de infecção, mecanismo de ativação e carga útil.

- **Vetor de infecção:** são os meios pelo qual o vírus consegue se propagar no computador.
- **Mecanismo de ativação:** condição que determina quando a carga útil será ativada.
- **Carga útil:** nome dado a função que o vírus irá exercer no computador, além de se propagar.

6.1.2 Tipos de vírus

No mundo virtual existem diversos tipos de vírus com diversas funções e alguns deles são: vírus de macro e vírus polimórficos.

- **Vírus de macro (ou macro-vírus):** é uma espécie de vírus que faz o uso da linguagem macro. Esse vírus, geralmente, é transmitido através de

e-mails e assim que executado é rapidamente proliferado. Ele tem como objetivo infiltrar-se em programas como o Microsoft Word, por exemplo, para executar uma série de atividades mal-intencionadas. Como exemplo deste grupo de vírus, temos o vírus Melissa, que surgiu em meados de 1999, que ficou famoso, por se propagar através de e-mails, infectando milhares de computadores em questão de muito pouco tempo.

- **Vírus polimórficos:** este vírus também conhecido como malware inteligente, é um tipo de vírus com a habilidade de se transformar a cada infecção pela assinatura, ou seja, antes do vírus criar cópias de si mesmo, ele muda seu código original, sendo essa transformação baseada na criptografia, dificultando sua detecção pelo antivírus. Como exemplo, temos o vírus VirLock, que é um worm polimórfico com recursos de infecção de arquivos que visam o Sistema Operacional Windows, que tem a capacidade de bloquear a tela do computador infectado e criptografar arquivos. Arquivos criptografados VirLock ganham uma extensão .exe. (NJCCIC, 2016).

6.2 BACKDOOR

Backdoor, também conhecido como portas dos fundos, é uma técnica bastante utilizada pelo ambiente corporativo, pois dá liberdade para os fabricantes o criarem em seus programas, com a alegação de que o software precisará de operações administrativas futuramente (MACHADO, 2014). Entretanto, os backdoors se tornam uma grande ameaça para quem o faz o uso, pois, muitos hackers conseguem ter acesso a essas portas, por meios de serviços criados, modificados e entre outros, com o objetivo de assegurar o acesso futuro ao computador que passa a estar comprometido (CARTILHA, 2012).

Quando instalado esse método no computador, o hacker passa a ter autonomia para praticar qualquer ação dentro da máquina de forma remota ou simplesmente espionar tudo que o usuário faz nele, sem que haja a necessidade de recorrer à técnica utilizada novamente na invasão (CARTILHA, 2012).

6.3 ROOTKIT

RootKit ou conjunto de programas e técnicas, é um software utilizado para exercer funções que na maioria das vezes é maliciosa. Contudo é um software muito inteligente, pois é capaz de se camuflar a processos de detecção de ameaças, dando ao invasor total acesso ao computador invadido e as informações que nele contém (CANALTECH, 2021?).

Segundo, Blunden(2020) os rootKits tendem a se concentrar em derrotar a resposta forense, utilizando uma variedade de estratégias de ocultação como por exemplo: ganchos, canais secretos, etc.

- **Ganchos:** também chamados de hooks são recursos que têm como finalidade manipular processos sem alterar o arquivo no núcleo.
- **Canais secretos:** é a passagem de uma informação de um dispositivo para o outro, onde somente o intruso tem acesso.

6.3.1 Detecção do antivírus

Segundo Malware (2020), quando um antivírus detecta um rootKit, o malware pode pode tentar desativar a proteção e deletar alguns componentes do antivírus para não ser deletado.

Podem também criar arquivos “irrelevantes” para serem detectados pelo antivírus, como uma espécie de armadilha. Quando o antivírus for acessar o arquivo, o rootKit tenta derrubá-lo e impedir futuras execuções e limpezas (MALWARE, 2020).

6.4 SPYWARE

Spyware, também conhecido como espião, é um programa que quando instalado no computador o proprietário pode visualizar atividades decorrentes do usuário. Sua função como espião é coletar e enviar informações, e isso pode ser usado tanto de forma legítima, quanto de forma maliciosa.

- **Legítimo**: quando instalado em um computador pessoal, pelo próprio dono ou com consentimento deste, com o objetivo de verificar se outras pessoas o estão de modo abusivo ou não autorizado(CARTILHA, 2012).

- **Malicioso:** quando executa ações que podem comprometer a privacidade do usuário e a segurança do computador, como monitorar e capturar informações referentes à navegação do usuário ou inseridas em outros programas (por exemplo, conta de usuário e senha) Cartilha (2012).

6.4.1 Tipos de spywares

Como se sabe esse malware é extremamente perigoso para os usuários, pois ele dá acesso a informações sigilosas deste e a rotina do mesmo. Sabe-se que existem vários tipos de spywares e riscos que eles trazem e alguns deles são: keylogger, screenlogger (CARTILHA, 2012) e browser hijacker.

- **Browser hijacker:** é um tipo de spyware responsável por realizar mudanças no browser da máquina, sem a autorização do usuário. Logo, essa invasão é responsável por muitas mudanças, dentre elas: páginas do navegador do equipamento alteradas e abertura de links aleatórios sem que haja a solicitação do usuário (MACEDO, 2015).
- **Keylogger:** spyware capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como acesso a um site específico de comércio eletrônico ou de Internet Banking (CARTILHA, 2012).
- **Screenlogger:** esse tipo de spyware muito inteligente é capaz de capturar tudo que o usuário faz com o cursor apresentado no monitor. Logo, ele é bastante utilizado pelos atacantes para capturar as teclas digitadas em teclados virtuais (CARTILHA, 2012).

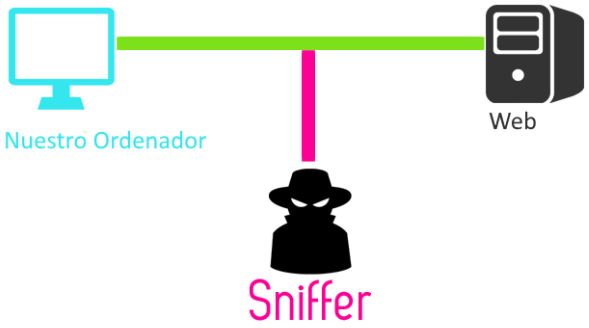
6.5 SNIFFING

Sniffing é uma técnica utilizada para controlar dados que trafegam na rede de computadores, por meio do uso do programa Sniffer, utilizado para capturar dados e levar para o atacante.

Segundo a Cartilha (2012) essa técnica Sniffing pode ser utilizada de duas maneiras, ou seja, de forma legítima e de forma maliciosa.

- **Legítima:** por administradores de redes, para detectar problemas, analisar desempenho e monitorar atividades maliciosas relativas aos computadores ou redes por eles administrados (CARTILHA, 2012).
- **Maliciosa:** por atacantes, para capturar informações sensíveis, como senhas, números de cartão de crédito e o conteúdo de arquivos confidenciais que estejam trafegando por meio de conexões inseguras, ou seja, sem criptografia (CARTILHA, 2012).

Figura 4 - Sniffing



Fonte: PC-Solución(2013)

6.6 COMPARAÇÃO ENTRE AS AMEAÇAS

A tabela a seguir (Quadro 3) apresenta os comparativos entre as ameaças: vírus, backdoor, rootkit, spywares, sniffing.

Quadro 3 - Comparação entre as ameaças

	Vírus	**Backdoor**	**Rootkit**	**Spywares**	**Sniffing**
Como é obtido:					
Recebido por e-mail	x			x	
Baixados em sites na internet	x			x	
Compartilhamento de arquivos	x			x	
Mensagens instantâneas	x			x	
Inserido por um invasor		x	x	x	x
Ação de outro malware		x	x	x	x

Instalação:					
Execução de um arquivo infectado	x				
Execução explícita do código malicioso				x	
Via execução de outro malware		x	x		x
Exploração de vulnerabilidades		x	x		
Como se propaga:					
Insere cópias de si próprio	x				
Não se propaga		x	x	x	x
Ações maliciosas mais comuns:					
Altera e/ou remove arquivos	x		x		
Furta informações sensíveis				x	x
Instala outros códigos maliciosos			x		
Possibilita o retorno do invasor		x	x		x
Procura se manter escondido	x	x	x	x	x

Fonte: Autoria própria baseado em Machado (2014, p.80).

7 COMO PREVENIR O COMPUTADOR

O que é prevenção? Bom, muitas pessoas já devem ter se feito essa pergunta e outras talvez nunca tenham se perguntado, mas o que realmente isso significa? A prevenção é o ato de se preparar, para serem evitados futuros problemas. Contudo, a prevenção na área da informática preza pela mesma ideia, pois, o ato do usuário por exemplo, cuidar dos dados fornecidos, senhas, etc. é evitar que problemas futuros alterem sua segurança e confiabilidade.

7.1 PREVENÇÃO DOS VÍRUS

Indubitavelmente, todas as pessoas querem se ver longe das ameaças causadas por vírus, porém, nunca conseguem ficar 100% livres de ataques feitos por esse malware tão temido. Deseja-se por muitos indivíduos métodos eficazes para proteção dos equipamentos, para que eles consigam chegar perto de um sistema parcialmente confiável.

Portanto, urge-se a procura de prevenções para o bloqueio desses vírus, já que tanto causam prejuízos. Algumas dessas possíveis prevenções são:

- **Instalação de antivírus:** antivírus é um software utilizado em computadores e em outros aparelhos tecnológicos, capaz de detectar uma ameaça por conta de informações que possui no banco de dados próprios, ou até mesmo pela análise heurística, sendo esse programa indispensável para a proteção da máquina (MACHADO, 2014).
- **Antivírus atualizado:** um antivírus instalado na máquina mas não atualizado, não oferece muita serventia, pois, ele irá abrir uma “brecha” para a entrada de novos vírus, pois seu catálogo interno não funcionará corretamente (BITDEFENDER, 2012).
- **Não fazer uso de dois antivírus:** segundo, Uol segurança digital (2013), fazer o uso de dois ou mais antivírus, pode ocasionar um grande problema para o usuário, pois, nesse caso o excesso de segurança, causará conflitos entre os antivírus, deixando a máquina vulnerável à entrada de ameaças.
- **Firewall:** segundo Machado (2014), o firewall é um mecanismo de segurança, que se enquadra como uma espécie de barreira, com o objetivo de bloquear

qualquer tráfego de dados não autorizados, impedindo assim, que ações maliciosas sejam realizadas na máquina do usuário.

- **Não instalação de aplicativos pirata:** deve-se manter longe de instalações de softwares pirateados, pois, esse pode ocasionar a infecção de uma máquina, pois, diversos vírus podem vir camuflados dentro do aplicativo (TECHTUDO, 2018).

- **Não abrir anexos contidos em e-mails desconhecidos:** e-mails de origem desconhecida e com anexos de extensões, por exemplo, .exe, js e .scr, devem ser evitados, pois, esses geralmente contém algum tipo de vírus embutido (CANALTECH, 2021).

7.2 PREVENÇÃO DO BACKDOOR

Embora, muitos backdoors estejam instalados em maquinas de forma legal, existem muitos acoplados de forma ilegal, como visto no capítulo 6.2, causando diversos problemas para os usuários. Portanto, em virtude disso, foi selecionado diversas formas de prevenção contra esta porta indesejável, que são elas:

- **Acesso a e-mails conhecidos:** acesso a e-mails somente de conhecidos ou solicitados, pois, assim evita que um backdoor se instale, por este meio, que por muitas vezes aparenta ser inofensivo.
- **Negligência de programas e sites com fontes duvidosas:** o não contato com programas e sites com fontes duvidosas é muito importante para o usuário, pois, a máquina fica mais distante do malware e de futuros problemas que ele poderia ocasionar.

- **Firewall:** segundo Nakamura e Geus (2007), o firewall é um mecanismo utilizado para a proteção de uma rede confiável contra uma não confiável. Logo, esse software pode contribuir contra a ação dos backdoor, negando-o o acesso indevido à máquina.

7.3 PREVENÇÃO DO ROOTKIT

Semelhante ao backdoor, o rootkit se mantém escondido do usuário evitando sua detecção, deixando o acesso ao computador aberto para o atacante ir e vir sem ser percebido (CANALTECH, 2021?). Contudo, esse malware pode ser evitado, fazendo o uso de prevenções como:

- **Possuir um antivírus:** é necessário que o usuário procure um antivírus avançado, pois, atualmente nem todos os antivírus são capazes de detectar e proteger a máquina contra esse tipo de malware (TECMUNDO, 2009).
- **Firewall:** A utilização de um firewall na máquina é indispensável, pois ele trabalhará para o tráfego de informações, no qual, impedirá a passagem de qualquer dado não informado ou indesejável (MACHADO, 2014).
- **Anti-spam:** o rootkit pode infectar uma máquina através da execução de uma mensagem indesejada e para que isso não ocorra, é necessário a instalação de um antispam, para que essas mensagens sejam bloqueadas (TECMUNDO, 2009).
- **Manter os softwares atualizados:** segundo a empresa tecnológica Kaspersky (2021), a atualização de software é muito importante para a proteção da máquina, pois essa contribui para um sistema mais seguro, evitando que o rootkit tire algum proveito das vulnerabilidades.

7.4 PREVENÇÃO DO SPYWARE

Incontestavelmente, a aplicação de forma maliciosa de spywares em máquinas é muito ruim e prejudicial para os usuários, pois, estes possuem informações sigilosas em suas máquinas, e um espião colocaria em risco, por exemplo, a sua privacidade (MACHADO, 2014). Todavia, não é necessário temer ele, seguindo alguns passos, que serão expostos logo abaixo.

- **Tenha um anti-spam:** spams ou mensagens indesejadas, são um dos responsáveis pela propagação de spywares, segundo Kawakani (2014). Portanto, deve-se manter longe dessas mensagens, logo urge, a instalação de um antispam, para o bloqueio dessas mensagens.
- **Não baixar programas com fontes desconhecidas:** negligenciar programas com fontes não confiáveis ou desconhecidas, é necessário, pois, apenas um

clique, pode colocar toda uma máquina em risco, pois, podem manter spywares escondidos (NEVES, 2021).

- **Instale um anti-spyware:** necessita-se a instalação desse software específico, pois em alguns casos ele pode garantir uma maior segurança da máquina ou da rede, pois, esse garante a detecção do spyware (GUISSO, 2017).

7.5 PREVENÇÃO DO SNIFFING

Esta técnica sniffing utilizada por muitos de forma legítima, pode causar diversos danos para os usuários, por aqueles que ainda hoje fazem o uso dessa técnica de forma ilegal, para interceptar e roubar dados sigilosos que trafegam pela rede (CARTILHA, 2012). Portanto, fez-se necessário a procura de prevenções para que esta ameaça não traga futuros problemas, e algumas dessas prevenções serão apresentadas logo abaixo.

- **Antivírus:** o antivírus é um elemento eficaz para a proteção de um sistema contra malwares, de acordo com Williams (2014) citado por Guisso (2017, p. 38). Logo, esse programa ao detectar alguma ameaça serve como proteção contra sniffing que por consequência pode vir junto com uma praga virtual.
- **Criptografia:** utilizar a criptografia de dados é um método de proteção muito importante, pois, ele evita que os dados sejam expostos para o atacante de forma legível (MACHADO, 2014).
- **Evitar programas com protocolos inseguros:** como visto no capítulo 5.5 através do protocolos, (2015), negligenciar protocolos inseguros, como o HTTP é muito importante, pois ele não garante a confiabilidade desejada. Logo, o site visitado com esse protocolo pode ter um sniffing à espera de sua execução.

8 COMO SOLUCIONAR PROBLEMAS OCASIONADOS POR AMEAÇAS

Quem nunca tentou solucionar um problema e acabou por convencido que não tinha solução? Bom, grande parcela da sociedade, mas para a área da segurança, os problemas não podem ser deixados de lado, como se não existisse. Nesta área, urge-se solucionar problemas o mais rápido possível, para que eles não se tornem ainda mais prejudiciais e de difícil eliminação. Portanto, solucionar estas adversidades não é uma opção e sim uma obrigatoriedade para quem trabalha em uma organização, pois, muitas informações confidenciais ficam a risco de criminosos. Contudo, é como o almirante William F. Halsey disse: "Todos os problemas se tornam menores quando você os confronta ao invés de evitá-los" Jornal do Empreendedor (2017).

8.1 SOLUÇÃO DOS VÍRUS

Sabe-se que essas pragas virtuais causam uma série de problemas, como o roubo de dados e a lentidão dos equipamentos, contudo sabe-se também a prevenção contra essas pragas. Porém, hipoteticamente, essas ameaças ultrapassam o sistema de prevenção imposto contra elas, terão que ser expulsas, para que não causem danos graves e nem leves, e algumas das formas de expulsá-las, são expostas abaixo.

- **Antivírus:** segundo Machado (2014), o antivírus é capaz de remover essa praga virtual, através de seu banco de dados próprio onde estão armazenados informações de determinados vírus ou através da remoção com base na heurística, que detecta e remove com base no comportamento do software malicioso.
- **Senhas alteradas:** após a detecção de um vírus e a sua exclusão, é necessário que haja a alteração de todas as senhas contidas no aparelho, caso haja dúvida delas terem sido capturadas pelo malware expulsado, pois, o atacante pode redefinir a senha e passar a ter acesso a alguma conta do usuário, aumentando assim, a gravidade ocasionada pelo vírus (BEGIN-IT, 2012?).
- **Formatação:** sendo a última opção, a formatação é um meio de solucionar problemas causados por vírus, pois, esse apagará totalmente o conteúdo da contido na máquina, sendo necessário reinstalar o sistema operacional nesta (NETSUPPORT, 2017).

8.2 SOLUÇÃO DO BACKDOOR

Indubitavelmente, os backdoors maliciosos são um grande problema para as organizações, pois, eles permitem o retorno de cibercriminosos (CARTILHA, 2012). Logo, ninguém e nenhuma organização deseja ter esta ameaça instalada e causando prejuízos, portanto, a seguir será apresentado uma possível solução para retirada deste malware.

- **Formatação:** a formatação nesse caso é essencial e eficaz, pois, ele eliminará todos os elementos contidos no equipamento (NETSUPPORT, 2017). Logo, esse fato contribui para a remoção do malware, pois esse irá retroceder a um estado de "novo", ou seja, ele exigirá a instalação do sistema operacional novamente.

8.3 SOLUÇÃO DO ROOTKIT

Inegavelmente, ter esse software malicioso instalado na máquina não é nada bom, como visto nos capítulos anteriores 6.3 e 7.3. Porém, a barreira feita para a não entrada dele, nem sempre está feita corretamente, logo, urge-se a exclusão dele, assim quando instalado na máquina. Para isso, deve-se seguir estes passos abaixo.

- **Anti-Rootkit:** o rootkit, como outras ameaças, faz o uso de uma programação muito avançada para prejudicar os usuários. Contudo, esses podem ser detectados e removidos, a partir do uso de um anti-rootkit, segundo o Techtudo (2010).
- **Restauração do sistema:** segundo Rohr (2005), a formatação nesse caso de difícil detecção, é eficaz, pois ela remove o malware. Logo, isso é possível, pois o conteúdo da máquina é totalmente apagado.

8.4 SOLUÇÃO DO SPYWARE

Como sabemos, ter este software malicioso instalado em um equipamento sem nenhum consentimento, não é nada bom, pois, os dados confidenciais como senhas dos usuários, passam a ser espionados. Logo, o usuário que tenha o instalado, urge retirar o mais rápido possível. Sendo assim, espera-se que o usuário siga estes passos abaixo.

- **Anti-Spywares:** diferentemente de um antivírus o anti-spyware, é um software capaz de eliminar programas de área “cinza” , ou seja, ele é capaz de eliminar o spyware e outros programas classificados como de difícil remoção (LINHA DEFENSIVA, 2018?).

- **Remoção manual no windows 10:** sabe-se que esse tipo de remoção é mais demorada, mas que pode ser uma boa alternativa. Para remover o spyware dessa forma, primeiro desliga-se a internet para que ele não envie dados confidenciais, depois reinicie o computador no modo seguro, logo exclua todos os arquivos temporários na máquina, em seguida desinstale todos os aplicativos de origem estranha e por fim reinicie o computador para entrar no modo normal (AVAST ACADEMY, 2020).

8.5 SOLUÇÃO DO SNIFFING

Como sabemos o programa sniffer em conjunto com a técnica sniffing representa uma série de ameaças a uma rede, pois, dessa forma podem revelar informações relevantes no tráfego para o intruso (HORA, 1999). Sendo assim, ter essa técnica instalada pode trazer sérios prejuízos ao usuário, para que isso não ocorra, necessita-se então que a organização siga o passo que será exposto logo abaixo.

- **Manualmente:** é necessário que o usuário ao saber que foi infectado procure analisar todos os seus aplicativos instalados no computador e é necessário também que a vítima organize suas pastas de downloads por data, para que fique mais fácil a remoção de programas não solicitados, pois, esses podem estar com a técnica embutida (LATTO, 2020).

Logo, se o sniffing permanecer no computador impossibilitando sua desinstalação é necessário que haja a instalação de um anti-malware capaz de remover esse tipo de software malicioso (LATTO, 2020).

9 ESTUDO DE CASO

Este capítulo do presente trabalho visa apresentar o estudo de caso baseado na instalação de um Ransomware Fantom e de um Trojan Memz, escolhido na plataforma do Github (2018). Para esse estudo foi primeiramente instalado a máquina do VirtualBox, onde foi escolhido o windows 7 para a atividade de instalação e remoção das ameaças. Logo, a esse passo foi selecionado o antivírus Avast para análise de sua funcionalidade em conjunto com o Windows Defender.

Enfim, cada ameaça passará por três situações de instalações, onde a primeira situação abordará a tentativa de instalação com o antivírus e a proteção do windows ativados, a segunda situação com a proteção do windows ativa e do antivírus desativada e a terceira situação com nenhuma proteção ativa.

9.1 FANTOM

A ameaça Fantom selecionada tem como objetivo passar por procedimento de atualização do sistema operacional, para começar sua atividade maliciosa de criptografar as pastas e deixar um bilhete pedindo um resgate para descriptografá-las (MESKAUSKAS, 2020).

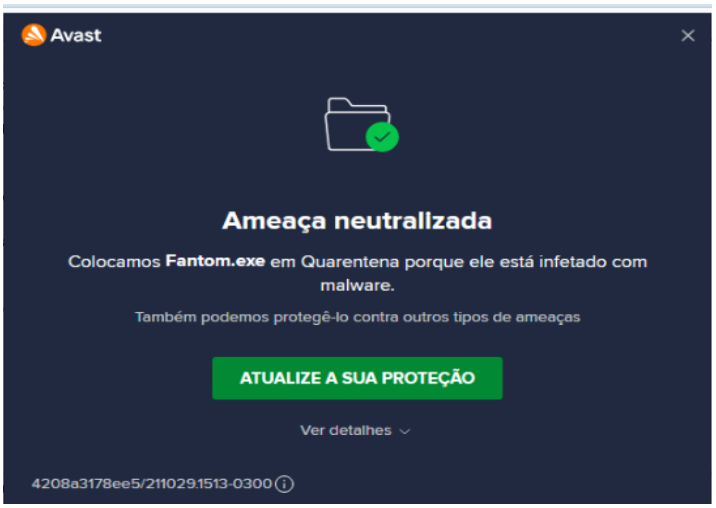
9.1.1 Situação 1 - Windows Defender e antivírus ativados

Ao instalar o windows 7 na máquina virtual, a primeira atividade feita foi a instalação do antivírus, no qual, já vinha todas as suas funcionalidades ativas, depois foi verificado a segurança no centro de ação do sistema operacional, onde a proteção estava inativa, mas que foi ligada rapidamente.

Logo, tudo funcionando, foi realizado o download do Ransomware, no qual, foi solicitado a execução, mas que não foi possível pelo barramento do antivírus, que o mandou para quarentena por apresentar algum risco ao computador.

A imagem a seguir, irá ilustrar como o antivírus funcionou no momento da solicitação de instalação do vírus.

Figura 5 - Fantom em quarentena



Fonte: Autoria própria

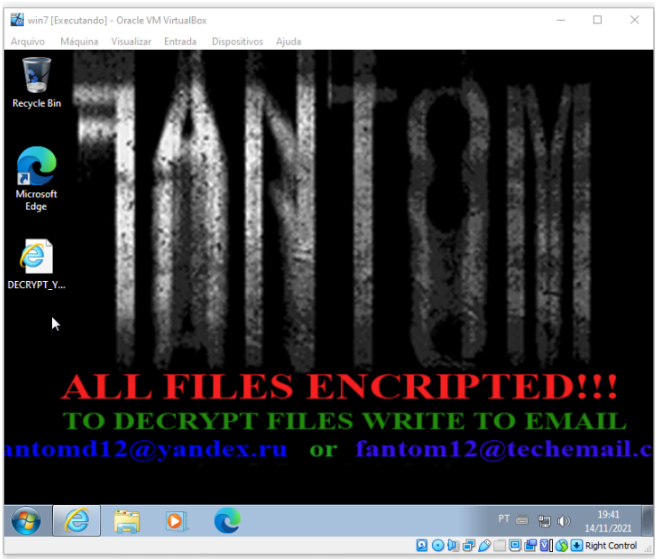
9.1.2 Situação 2 -Windows Defender ativado e antivírus desativado

A segunda etapa permanecendo somente com a proteção do windows, no qual foi ativada, foi bastante útil, pois, ao tentar a instalação do ransomware, foi emitido uma mensagem que perguntavam se era de desejo que o programa fizesse alterações no sistema e de que era de certeza a permissão para o software a ser executado.

Dessa forma, o usuário recebendo a mensagem tem a possibilidade de instalar ou não o software, nesse caso foi solicitado que sim. Logo, ao instalar, a tela do monitor virtual passou a ficar toda azul, dando a entender que estava ocorrendo uma atualização no sistema do windows, mas passado algum tempo reiniciei a máquina, e ao voltar o plano de fundo do windows estava alterado, com uma imagem informando um e-mail para o resgate e as pastas contidas no explorador de arquivos, estavam todas criptografadas com uma carta pedindo resgate.

A imagem a seguir, foi retirada no momento em que o plano de fundo foi alterado pelo vírus, causando uma espécie de “terror no usuario”.

Figura 6 - Fantom executado



Fonte: Autoria própria

Logo, com essa transformação, foi excluído o download do vírus e feito uma varredura no Windows Defender, no qual, não detectou nenhum software indesejado.

Ademais, com as pastas ainda criptografadas foi feita a restauração do sistema, com o objetivo de voltar a máquina ao seu estado normal, contudo, nesse processo não houve êxito, pois, tudo permaneceu da mesma maneira.

Portanto, com as pastas criptografadas, foi realizado como última medida a formatação, no qual trouxe o resultado esperado de remover o vírus, deixando a máquina no seu estado de novo, como quando saí da loja.

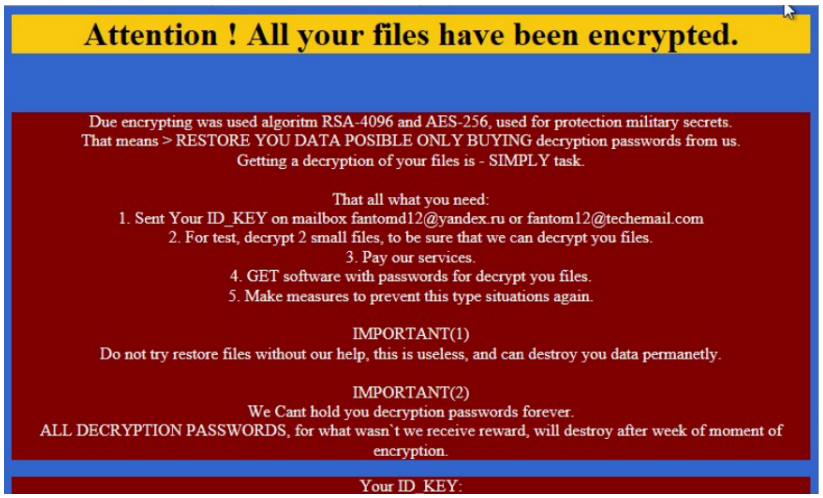
9.1.3 Situação 3 - Nenhuma proteção ativa

Nessa situação, foi desativado o Windows Defender, o Windows Firewall e o antivírus, para que a máquina ficasse bastante vulnerável. Contudo, com a proteção bastante fragilizada, foi solicitado a execução do ransomware, no qual, apareceu apenas um aviso de segurança perguntando se era de certeza a execução do software.

Enfim, com o vírus na máquina executado, a máquina passou por uma falsa atualização de sistema operacional, emitindo em todas as pastas uma espécie de carta, pedindo um pagamento para descriptografá-las. Logo, não atendendo essa solicitação, foi realizada a formatação desta, para removê-lo, no qual, esse objetivo foi atingido e a máquina voltou ao seu estado inicial, sem o vírus.

A imagem abaixo, foi retirada de uma das pastas criptografadas.

Figura 7 - Função do Fantom



Fonte: Autoria própria

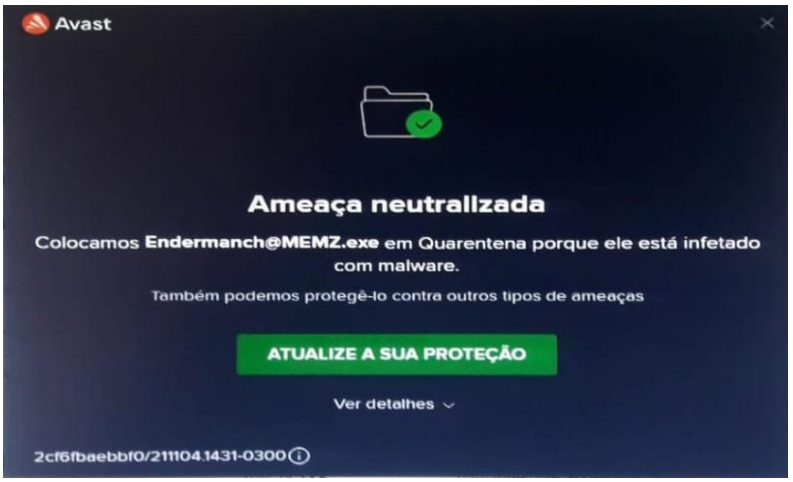
9.2 MEMZ

O Memz diferentemente de Fantom não pede nenhum resgate e não se passa por atualização, porém, tem como objetivo, deixar o sistema operacional da máquina incapaz, através da geração de links aleatórios, como também consultas de pesquisas na web sem a solicitação (DEVFESTPR, 2021?). Contudo, este trojan é bastante temido, também, pela função de reescrever o sistema operacional (GOV-CIVIL-SETUBAL, 2021).

9.2.1 Situação 1 - Windows Defender e antivírus ativados

Após a instalação do windows 7 e do antivírus (Avast) no VirtualBox, foi ativado o Windows Defender para maior proteção da máquina, já que esse software vem inicialmente inativo no sistema operacional. Logo, foi feito o download do trojan é tentado a execução desse, porém, não houve a instalação, decorrência de que o software malicioso foi para quarentena em questão da funcionalidade do antivírus em detectar ameaças.

Figura 8 - Memz em quarentena



Fonte: Autoria própria

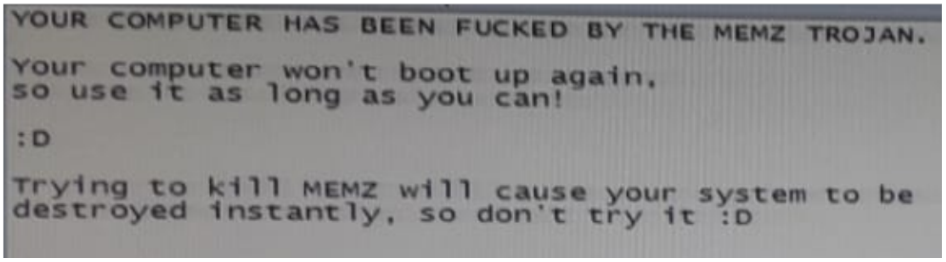
9.2.2 Situação 2 - Windows Defender ativado e antivírus desativado

Nesse segundo caso, houve a execução do vírus com sucesso na máquina, porém, diferentemente do caso 1, esse não contou com a participação do antivírus, pois ele foi desabilitado antes do processo, permanecendo a máquina somente com a proteção do computador.

Entretanto, assim que solicitado a execução desse, houve alguns alertas, dizendo que o software era um malware e que esse iria danificar o computador e deixá-lo inutilizável, como também, houve um aviso dizendo que o criador não teria responsabilidade qualquer por algum dano ocorrido por esse. Portanto, sabendo de todos os riscos possíveis sobre o software, foi permitida a execução.

Logo, a autorização mediante ao vírus, apareceu uma mensagem no bloco de notas do Memz dizendo que o computador não passaria por uma inicialização novamente. Contudo, para retratar essa mensagem foi tirada uma foto do ocorrido.

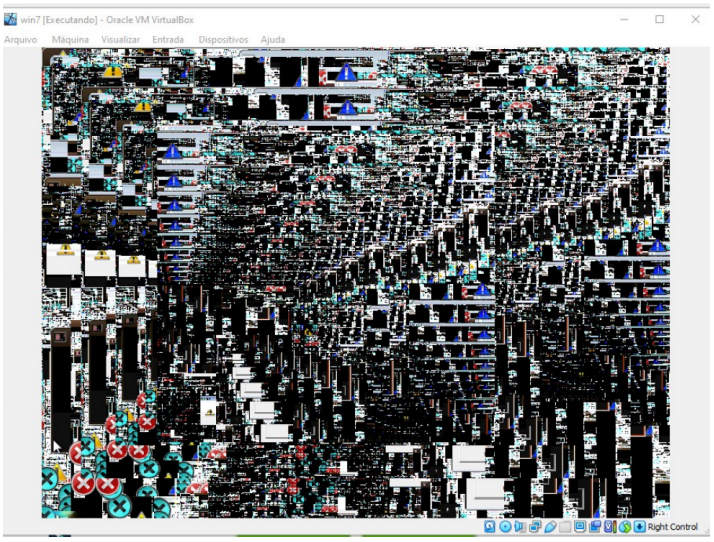
Figura 9 - Mensagem emitida pelo Memz



Fonte: Autoria própria

Ademais, a tela da máquina passou a oscilar muito de cores, a travar muito e a abrir várias páginas aleatórias, ou seja, a ameaça passou a comandar as execuções, impossibilitando que comandos próprios fossem realizados.

Figura 10 - Memz em ação



Fonte: Autoria própria

Enfim, para se ver livre desse trojan, foi realizada uma formatação na máquina, no qual, apresentou um resultado positivo, pois, ao terminar a formatação o vírus passou a não estar mais embutido no sistema.

9.2.3 Situação 3 - Nenhuma proteção ativa

Nesse terceiro caso e último, foi feita a instalação do Windows 7 como os demais casos acima. Porém, não houve a instalação de um antivírus, e o Windows Defender

como o Windows Firewall foram desativados, sendo assim, a máquina passou a ficar bastante vulnerável a ataques. Logo, ao fazer isso, foi gerado uma mensagem alertando sobre a importância de tais funções para a máquina.

Posteriormente a esses feitos, foi realizado o download do vírus e solicitado a sua execução, entretanto, ainda foi enviado uma mensagem perguntando se era de certeza a execução do malware, dito que sim, em poucos segundos a tela da máquina ficou cheia de mensagens até que tapou por completo, sendo direcionada para a formatação dessa.

Contudo, como a máquina foi formatada, essa passou a não ter mais o malware instalado. Enfim, para maior entendimento o processo foi realizado duas vezes, permanecendo esses com o mesmo resultado.

A imagem a seguir apresenta o momento em que o vírus começou a exercer sua função.

Figura 11 - Função do Memz

Fonte: Autoria própria

9.3 COMPARAÇÃO ENTRE AS AMEAÇAS

O quadro a seguir (Quadro 4) apresenta os comparativos entre as ameaças: Fantom e Memz.

Quadro 4 - Comparação entre o Fantom e o Memz

Fanton		
Situação	**Problema**	**Solução**
1.Windows Defender e antivírus ativados	Não apresentou nenhum problema.	O antivírus lançou a ameaça para quarentena.
2.Windows Defender ativado e o antivírus desativado	As pastas ficaram criptografadas com uma carta pedindo resgate para ter acesso novamente.	Realização da formatação da máquina.
3.Nenhuma proteção ativada	O vírus foi executado passando por uma falsa atualização e criptografando todas as pastas contidas na máquina	Máquina formatada.
Memz		
Situação	**Problema**	**Solução**
1.Windows Defender e antivírus ativados	Não apresentou nenhum problema.	O antivírus mandou a ameaça para quarentena.
2.Windows Defender ativado e o antívirus desativado	A máquina passou a ficar incontrolável, mostrando aleatoriamente mensagens de erro e alterando a cor de fundo do windows.	Formatação da máquina.
3.Nenhuma proteção ativada	Em poucos segundos depois da execução a máquina encheu de mensagens até completar toda a tela da máquina.	A máquina passou pelo processo de formatação.

Fonte: Autoria própria

10 CONSIDERAÇÕES FINAIS

Esse relatório apresentou o Trabalho de Conclusão do Curso Técnico Integrado de Informática. O objetivo do trabalho foi apresentar a suma importância da segurança em redes de computadores, como também, propor a proteção e as possíveis soluções a serem usadas contra software mal intencionados.

Além disso, este trabalho apresentou o estudo de caso, no qual, foram selecionadas duas ameaças, para análise, prevenção e remoção dessas. Ademais, esse estudo demonstrou a extrema importância de manter o windows defender/Windows firewall ativos, além de um antivírus atualizado.

Como trabalho futuro poderá ser adicionado pesquisas de outros malwares não citados anteriormente, para que o conhecimento seja amplo. Logo, poderá ser implementado também, estudos de casos, com vírus diferentes e com outras técnicas de remoção.

11 REFERÊNCIAS

AVAST ACADEMY. **Como remover spyware de um PC:** Como remover spyware de um computador. Site, 25 jun. 2020. Disponível em: https://www.avast.com/pt-br/c-remove-spyware-pc#:~:text=A%20maneira%20mais%20r%C3%A1pis%20e%20eficiente%20de%20remover,os%20malwares%20e%20removed%C3%AA-los%20do%20sistema%20para%20sempre. Acesso em: 5 set. 2021.

BEGIN-IT. Como se recuperar de uma infecção por vírus: 3 coisas que você precisa fazer. [*S.l.*], [2012?]. Disponível em: https://pt.begin-it.com/6432-how-to-recover-from-a-virus-infection-3-things-you-need-to-do. Acesso em: 24 ago. 2021.

BITDEFENDER. Antivírus Atualizado: 4 motivos para manter a sua segurança online. **Antivírus Atualizado: 4 motivos para manter a sua segurança online.,** blog Infotec Blog, 31 jan. 2012. Disponível em: https://www.infotecblog.com.br/motivos-manter-antivirus-atualizado/. Acesso em: 10 ago. 2021.

BLUNDEN, Bill. Anti-Forense a Conexão RootKit: Sobre este arquivo. In: BLUNDEN, Bill. **Anti-Forense a Conexão RootKit:** Sobre este arquivo. Site, 13 fev. 2020. Disponível em: https://forum.tuts4you.com/files/file/1235-anti-forensics-the-rootkit-connection/. Acesso em: 2 ago. 2021.

CANALTECH. **Aprenda a evitar malwares e vírus anexados a e-mails.** [*S. l.*], 2021. Disponível em: https://canaltech.com.br/seguranca/falha-em-roteadores-ameaca-seguranca-de-6-milhoes-de-usuarios-no-reino-unido-202279/. Acesso em: 10 set. 2021.

CANALTECH. **Em 2020, pelo menos 360 mil vírus para computador foram criados por dia.** [*S. l.*]: Ramon De Souza, 25 dez. 2020. Disponível em: https://canaltech.com.br/seguranca/em-2020-pelo-menos-360-mil-virus-para-computador-foram-criados-por-dia-176642/. Acesso em: 10 jun. 2021.

CANALTECH. **O que é rootkit?.** [*S. l.*], [2021?]. Disponível em: https://canaltech.com.br/seguranca/O-que-e-rootkit/. Acesso em: 20 ago. 2021.

CARTILHA de Segurança para Internet: Ataques na Internet. 2ª.ed. Website: Comitê Gestor da Internet no Brasil, 2012. 142 p. ISBN 978-85-600-54-6. Disponível em: Cartilha de Segurança para Internet – Versão 4.0. Acesso em: 4 ago. 2021.

CERT. Criptografia de chave simétrico e de chaves assimétricas. In: CERT. **Criptografia**. CERT.br, 16 mar. 2017. Disponível em: https://cartilha.cert.br/criptografia/. Acesso em: 4 jul. 2021.

DEVFESTPR. **Vírus MEMZ: o que é e como removê-lo para sempre.** [S. l.], [2021?]. Disponível em: https://devfestpr.org/591-memz-virus-what-it-is-and-how-to-remove-it-for-good#. Acesso em: 9 nov. 2021.

DATARAIN. **O que é o protocolo TCP/IP.** 2020. Disponível em: https://www.datarain.com.br/blog/tecnologia-e-inovacao/o-que-e-o-protocolo-tcpip/. Acesso em: 13 out. 2021.

DOCUSIGN. **Quando a criptografia deve ser usada?**. [S. l], 11 fev.2019. Disponível em: https://www.docusign.com.br/blog/criptografia-o-que-e-e-quando-ela-deve-ser-usada#:~:text=Esse%20recurso%20%C3%A9%20amplamente%20utilizado,computacionais%20com%20acesso%20%C3%A0%20Internet. Acesso em: 3 jul. 2021.

GITHUB. **MalwareDatabase**. [*S. l.*], 2018. Disponível em: https://github.com/Endermanch/MalwareDatabase. Acesso em: 30 out. 2021.

GOUVÊA, L. T. A. **Técnicas ultraleves para detecção de malware baseada para em assinaturas para redes de computadores.** Orientador: Kelton Augusto Pontara da Costa. 2016. 41p. TCC (Bacharelado em ciência da computação) - Universidade Estadual Paulista "Júlio de Mesquita Filho", Bauru, 2016. Disponível em em: https://mostra-de-tccs-bcc.github.io/TCC-BCC-Bauru-2016/gouvea/thesis-gouvea.pdf. Acesso em: 12 jun. 2021.

GOV-CIVIL-SETUBAL. O que é o vírus MEMZ? Como remover o vírus Trojan? Veja um guia!. [S. l.], 1 jan. 2021. Disponível em: https://gov-civil-setubal.pt/. Acesso em: 8 nov. 2021.

GUISSO, LEONARDO. **Segurança digital: avaliação do nível de conhecimento da população sobre os riscos de segurança atrelados ao uso da internet na região de Bento Gonçalves.** Orientador: Christian Zambenedetti. 2017. 84 p. Trabalho de Conclusão apresentado ao curso (Bacharel em Sistemas de Informação) - Campus Universitário da Região dos Vinhedos, da Universidade de Caxias do Sul., Bento Gonçalves, 2017. Disponível em: https://repositorio.ucs.br/xmlui/bitstream/handle/11338/3081/TCC%20Leonardo%20Guisso.pdf?sequence= 1 & isAllowed=y. Acesso em: 23 ago. 2021.

JORNAL DO EMPREENDEDOR. **27 citações para mudar como se pensa sobre problemas.** [*S. l.*], 4 maio 2017. Disponível em: https://jornaldoempreendedor.com.br/destaques/27-citacoes-para-mudar-como-se-pensa-sobre-problemas/. Acesso em: 19 ago. 2021.

HORA, Evandro Curvelo. "Sobre a detecção remota de sniffers para detectores de intrusão em redes TCP/IP": Os sniffers e sua detecção. Orientador: Fabiano Queda Bueno da Silva. 1999. 104 p. Dissertação de Mestrado (Pós-graduação em Ciência da computação) - Universidade Federal de Pernambuco, Recife, 1999. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/2550/1/arquivo4949_1.pdf. Acesso em: 5 set. 2021.

KAWAKANI, CLÁUDIO TOSHIO. **Segurança de computadores e aprendizado de máquina.** Orientador: Bruno Bogaz Zarpelão. 2014. 66 p. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) - Universidade Estadual de Londrina, LONDRINA-PR, 2014. Disponível em: http://www.uel.br/cce/dc/wp-content/uploads/TCC-ClaudioKawakani-BCC-UEL-2014.pdf. Acesso em: 6 ago. 2021.

LATTO, Nica. **O que é um sniffer e como não ser espionado?.** [*S. l.*], 26 mar. 2020. Disponível em: https://www.avg.com/pt/signal/what-is-sniffer#topic-5. Acesso em: 31 out. 2021.

LINHA DEFENSIVA. **Dúvidas sobre antivírus e anti-spyware.** [*S. l.*], [2018?]. Disponível em: https://linhadefensiva.org/faq/antivirus-antispyware/#antispy-01. Acesso em: 15 nov. 2021.

MACEDO , Joyce. **Browser Hijacker: veja como reparar um navegador sequestrado.** Canaltech, 9 abr. 2015. Disponível em: https://canaltech.com.br/seguranca/Browser-Hijacker-veja-como-reparar-um-navegador-sequestrado/. Acesso em: 28 jul. 2021.

MACHADO, Felipe Nery Rodrigues. **Segurança da informação:** Princípios e Controle de Ameaças. 1. ed. SP-Brasil: Beatriz M. Carneiro, 2014. 176 p. ISBN 978-85-365-0784-2.

MALWARE - RootKit + resumo sobre malwares. Direção: Rodrigo Campos. Produção: Rodrigo Campos. Gravação de Rodrigo Campos. YouTube: YouTube, 2020. Disponível em: https://youtu.be/6muMcV_haAc. Acesso em: 2 ago. 2021.

MESKAUSKAS, Tomas. Ransomware Fantom. PCrisk, 10 ago. 2020. Disponível em: https://www.pcrisk.pt/guias-de-remocao/8398-fantom-ransomware#:~:textO%20que%20%C3%A9%20Fantom%3F%20Fantom%20%C3%A9%20um%20v%C3%ADris,das%20v%C3%ADticas%20 em%20 sil%C3%AAncio%2C%20 sem%20mostrar%20qualquer%20 atividade. Acesso em: 18 nov. 2021.

MICROSOFT. **Malware de macro:** Como proteger malware de macro. Docs, 2021. Disponível em: Malware de macro - Windows security | Microsoft Docs . Acesso em: 13 ago. 2021.

MITSHASHI, Roberto Akio. **Segurança de Redes.** Orientador: Paulo Roberto Bernice. 2011. 62 p. TCC (Grau de Tecnólogo em Processamento de Dados) - Faculdade de tecnologia de São Paulo, SP-Brasil, 2011. Disponível em: http://www.fatecsp.br/dti/tcc/tcc0017.pdf. Acesso em: 10 jun.2021.

NAKAMURA; GEUS, Emilio Tissato e Paulo Lício. Segurança de Redes em ambientes cooperativos. 2. ed. SP-Brasil: Futura, 2007. 483 p. ISBN 978-85-7522-136-5.

NETO, Antonio Njaim Atalla. **Segurança em Redes de Computadores.** Orientador. Prof. Klaus Wehmuth. 2013. 51p. Monografia (Especialização em Redes de Computadores) - Universidade Federal de Juiz de Fora, Juiz de Fora, 2013.

NEVES, Cayan. **O que é e como evitar um spyware?.** [*S. l.*], 4 ago. 2021. Disponível em: https://auditsafe.com.br/o-que-e-e-como-evitar-um-spyware/. Acesso em: 20 ago. 2021.

NJCCIC(Nova Jersey). VirLock. In: **VirLock.** NJCCIC, 5 jul.2016. Disponível em: https://www.cyber.nj.gov/threat-center/threat-profiles/ransomware-variants/virlock. Acesso em: 1 ago. 2021.

PC-SOLUCIÓN. **Sniffer.** 2013. Disponível em: https://pc-solucion.es/2018/05/21/sniffer/. Acesso em: 14 out. 2021.

PROTOCOLOS. Direção: Márcio Lima. Produção: Cantinho da informática. YouTube:[s.n], 2015. Disponível em: https://youtu.be/031c04syZLs. Acesso em: 4 ago. 2021.

ROHR, Altieres. Rootkits: A prevenção é a solução: Análise: Mais do que nunca, rootkits estão mostrando a importância da prevenção de malwares aos usuários.. Linha Defensiva, 8 dez. 2005. Disponível em: https://linhadefensiva.org/2005/12/08/rootkit-prevencao-solucao/. Acesso em: 8 ago. 2021.

SALVINO, Douglas Silva. **Segurança de Redes:** Segurança de redes no ambiente corporativo. Orientadora: Mariana Nunes. 2017. TCC(Superior) - Universidade Anhanguera, SP-Brasil,2017.p.39.Disponível em:

https://repositorio.pgsskroton.com/bitstream/123456789/27177/1/TCC%2BSEGURAN%C3%87A%2BDE%2BREDES.pdf. Acesso em: 11 jun.2021.

TECHTUDO. **AVG Anti-Rootkit:** Proteção contra RootKits em poucos cliques. [*S. l.*], 25 jan. 2010. Disponível em: https://www.techtudo.com.br/tudo-sobre/avg-anti-rootkit.html#. Acesso em: 19 ago. 2021.

TECHTUDO. **Seis riscos de usar programas crackeados.** [*S. l.*], 16 dez. 2018. Disponível em: https://www.techtudo.com.br/listas/2018/12/seis-riscos-de-usar-programas-crackeados.ghtml. Acesso em: 23 ago. 2021.

TECMUNDO. **O que é rootkit?.** [*S. l.*], 1 jun. 2009. Disponível em: https://www.tecmundo.com.br/antivirus/2174-o-que-e-rootkit-.htm. Acesso em: 20 ago. 2021.

UOL SEGURANÇA DIGITAL. **Nunca use dois antivírus no mesmo computador.** Canatelch, 26 jun. 2013. Disponível em: https://seguranca.uol.com.br/antivirus/dicas/curiosidades/nunca-use-dois-antivirus-no-mesmo-computador.html#rmcl. Acesso em: 4 ago. 2021.

VÍRUS de computadores. Direção: Dicionário de Informática. Gravação de Dicionário de Informática. Produção: Dicionário de Informática. Gravação de Dicionário de Informática. YouTube: YouTube, 2020. Disponível em: https://www.youtube.com/watch?v=LSUwfF9lvgw. Acesso em: 31 jul. 2021.