UNIVERSIDADE FEDERAL DOS VALES DO JEQUITINHONHA E MUCURI

FACULDADE DE CIÊNCIAS EXATAS

DEPARTAMENTODE COMPUTAÇÃO

CURSO DE SISTEMAS DE INFORMAÇÃO

SEGURANÇA DA INFORMAÇÃO COM FOCO NO CONTEXTO HISTÓRICO E ABORDAGEM DAS PREVENÇÕES AO RANSOMWARE.

Jéssica Moreira Andrade

Diamantina/MG

2018

Jéssica Moreira Andrade

SEGURANÇA DA INFORMAÇÃO COM FOCO NO CONTEXTO HISTÓRICO E ABORDAGEM DAS PREVENÇÕES AO RANSOMWARE.

Trabalho de Conclusão de curso apresentado ao curso de Sistemas de Informação da Universidade Federal dos Vales do Jequitinhonha e Mucuri – UFVJM, como pré-requisito para obtenção do grau de bacharel. Orientador: Prof. MSc. Eduardo Pelli.

Diamantina/MG

2018

Monografia de projeto final de graduação sob o título "Segurança da Informação com foco no contexto histórico e abordagem das prevenções ao ransomware", defendida por Jéssica Moreira Andrade e aprovada em 08 de março de 2018, em Diamantina, Minas Gerais.

Banca Examinadora:

Prof. MSc. Eduardo Pelli
Orientador

Prof. MSc. Rafael Santin

Prof. MSc Luis Henrique Silva Rodrigues

AGRADECIMENTOS

Aos meus pais, pelo carinho, dedicação, apoio e suporte ao longo dessa caminhada.

À toda minha família, em especial a Tia Saula e Natalia, que sempre se mostraram dispostas a me apoiar e ajudar.

A todos os meus amigos que Diamantina me proporcionou, em especial as Lulus,e a Marli, que me acolheram como uma família em Diamantina, a Camila que foi o maior presente que o curso de Sistemas pode me dar.

Aos meus amigos de Ipatinga que sempre estiveram ao meu lado.

Ao meu orientador Eduardo Pelli, pela oportunidade, confiança, amizade, paciência, dedicação e conhecimentos compartilhados.

Agradeço aos colegas de curso pelos anos de caminhada e companheirismo. Agradeço também aos professores do Departamento de Computação da UFVJM, que foram extremamente importantes e me guiaram durante essa minha jornada.

"Entrego,confio,aceito e agradeço."
(Hermógenes)

RESUMO

O uso de tecnologias tem grande impacto na vida das pessoas e empresas. Os software estão cada vez mais inteligentes (Inteligência Artificial), os computadores mais avançados, redes mais velozes, aparelhos eletrônicos mais modernos, Internet usada em larga escala, trazendo benefícios para a sociedade. Porém, existem pessoas que preferem fazer o uso desse avanço tecnológico para prejudicar, utilizam de má fé, causando danos a outrem. Com todo o avanço, a informação é considerada o principal patrimônio de uma organização, sendo seu maior bem ativo. Daí surgiu a necessidade de proteger esse patrimônio,e para tanto urge buscar novas soluções para proteger essas informações, tanto no meio computacional quanto em relação a gestão de pessoas. A segurança da informação é uma área do conhecimento dedicada a proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. O presente trabalho teve por objetivo realizar um estudo sobre segurança da informação com enfoque no *ransomware*, e gerar um documento para conscientizar e alertar a importância da preservação da informação. O *ransomware* é um *malware* que limita o usuário de acessar suas informações, exigindo um resgate para obter novamente os seus dados. No decorrer do trabalho foi feito simulações do ataque *ransomware*(Hidden Tear), mostrando seu funcionamento e como alguns antivírus respondem a este ataque. Constatou-se no decorrer do trabalho que a população está muito aquém quanto a segurança de informação e os criminosos aproveitam dessa situação.

Palavras-chave: Ataques. Hidden Tear. Antivírus. Mecanismos de segurança. Trojan.

ABSTRACT

The use of technologies has greatly impacted the lives of people and companies. Softwares are increasingly intelligent (Artificial Intelligence), the most advanced computers, faster networks, more modern electronic devices, Internet used in large scale, bringing benefits to society. However, there are people who prefer to make use of this technological advance to harm, use in bad faith, causing harm to others. A With all the advancement, information is considered the main asset of an organization, its greatest asset being. Hence the need to protect this patrimony, and for that reason it is urgent to seek new solutions to protect this information, both in the computing environment and in relation to people management. Information security is an area of knowledge dedicated to the protection of information assets from unauthorized access, improper changes or unavailability. The present work aimed to carry out a study on information security with a focus on ransomware, and generate a document to raise awareness and alert the importance of information preservation. Ransomware is a malware that limits the user from accessing your information, requiring a redemption to get your data back. In the course of the work, it was made simulations of the ransomware attack, showing its operation and how some antivirus respond to this attack. It was found in the course of the work that the population is very short on information security and criminals take advantage of this situation.

Key-words: Attacks. Hidden Tear. Antivirus. Security mechanisms. Trojan

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

UFVJM	Univerisidade Federal dos Vales do Jequitinhonha e Mucuri
WI-FI	Wireless Fidelity
XML	Extensible Markup Language
TI	Tecnologia da Informação
WEB	World Wide Web
AES	Advanced Encryption Standard
RSA	Ronald Rivest, Adi Shamir e Leonard Adleman
DES	Data Encryption Standard
SSL	Secure Socket Layer
DoS	Disk Operating System
DDoS	Distributed Denial of Service
NAT	Network Address Translation
GB	Gigabyte
VM	Máquina Virtual
SO	Sistema Operacional

SUMÁRIO

1 INTRODUÇÃO

O acesso à Internet e a evolução da tecnologia vem crescendo em ritmo acelerado. Segundo KEMP (2017), o número de usuários globais que utilizam a Internet chega a um total de 3.77 bilhões, mais da metade da população total. Houve um aumento de 10% em relação a 2015. Consequentemente mais dispositivos conectados compartilhando informações.

De acordo com Campos (2007) "a informação é um dos recursos mais essenciais para uma organização, sendo um ativo de grande valor". É muito importante zelar pela informação, já que informações alteradas, não disponíveis ou sob o controle de pessoas com má indole e acessos indevidos, podem gerar problemas, tais como prejuízos financeiros, comprometendo a imagem das instituições, podendo até mesmo levar ao fechamento.

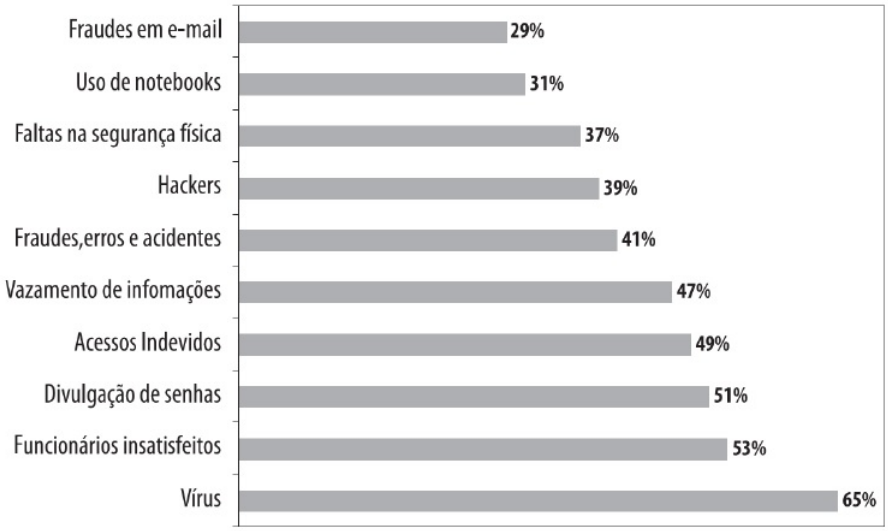
Todos os dados dispobilizando informações pessoais na Web , poderão ser acessados por qualquer pessoa que detenha certo conhecimento, e essas informações podem ser utilizadas de forma a causar danos. De acordo com a Corporation (2016), no Brasil cerca de 42.4 milhões de usuários foram afetados pelo cibercrime[1] em 2016 e 684.4 milhões de pessoas no mundo foram afetas por cibercrimes.

A *Módulo Security Solutions* (SOLUTIONS, 2003) fez uma pesquisa com o objetivo de apresentar as principais ameaças que a informação pode estar sujeita, sendo 65% vírus, 53% funcionários insatisfeitos, 51% divulgação de senha, 49% acessos indevidos. A Figura 1 apresenta todos os dados dessa pesquisa. Com o resultado da pesquisa podemos concluir o quanto é importante zelar pela segurança da informação.

No decorrer deste trabalho foram abordadas questões relacionadas à Segurança da Informação e vamos ver o quão a segurança da informação vai muito além de investimentos em novas tecnologias e boa política de segurança, também é preciso estar sempre capacitando funcionários, elaborar gerenciamento de risco, possuir boas ferramentas de defesa instaladas no computador.

[1] Delitos que vão de atividades criminosas contra dados até infração de conteúdo copyright.

Figura 1 – Principais ameaças as informações.



Fonte: (SOLUTIONS, 2003)

Atualmente percebemos que o rápido avanço tecnológico nos traz grandes impactos, novos ataques vão surgindo. Segundo o Relatório anual de Cibersegurança da Cisco (CISCO, 2017 apud REPORT, 2017), 49% dos negócios sofreram algum ciberataque de resgate em 2016, sendo que 39% eram ataques tipos *ransomware*, e que provavelmente o ano de 2017 poderia esperar novos ataques. No dia 12 de Maio de 2017 aconteceu o maior ciberataque até o presente trabalho, conhecido como *WannaCry*, ele aproveita de uma vulnerabilidade do Windows, e é executado remotamente. Rapidamente a Microsoft liberou uma atualização no *Microsoft Security Advisory 4022344* para resolver o problema, mas foi preciso que os usuários fizessem a atualização imediata do SO. O ataque foi registrado em aproximadamente 150 países (ALMEIDA, 2017). *WannaCry* é um tipo de *Ransomware*, ele deixa os dados do equipamento inacessíveis, e após o ataque é feito um pedido de resgate, caso o pagamento seja efetuado o usuário pode ter novamente acesso aos dados.

De acordo com a Kaspersky Lab (KASPERSKYLAB, 2016) os ataques a corporações em Janeiro cresceram de um ataque a cada 2 minutos, para um ataque a cada 40 segundos, e os ataques individuais cresceram de um a cada 20 segundos para um a cada 10 segundos. Essas pesquisas nos mostram que a população não está preparada para o ataque *ransomware*, e o quão as organizações e pessoas físicas precisam se informar melhor sobre o que é o ataque e como se prevenir.

Florenzano (2017), especialista em Segurança da Informação, acredita que a negligência com a TI e Segurança da Informação alavancaram o ciberataque mundial. Ele cita uma lista com os fatores para o ataque massivo com o *WannaCrypt* e outros ataques:

1 Uso de sistemas ultrapassados;

2 Carência de funcionários habilitados para conduzir sistemas;

3 O não uso de software livres, como por exemplo o Linux, que é considerado mais seguro que alguns software pagos;

4 A grande desvalorização do setor de TI, especialmente o de segurança da informação;

5 Falta de conhecimento sobre a segurança em ambientes de trabalho, como por exemplo, clicam em links maliciosos;

6 A maioria das empresas modernas tem o conhecimento do *Ransomware*, mas preferem esperar o ataque acontecer para resolverem agir.

Neste trabalho, são abordadas questões relacionadas à segurança da informação, com foco em *Ransomware*. Também foram realizadas simulações mostrando um exemplo de *Ransomware*, e como alguns software de proteção responderam a esse ataque. Por fim, foram efetuadas sugestões de melhorias de segurança para evitar futuros ataques.

1.1 Objetivo Geral

O objetivo geral deste trabalho foi realizar um estudo sobre Segurança da Informação, com enfoque no ataque *Ransomware* e gerar um documento para conscientizar e alertar a importância da preservação da informação.

1.1.1 Objetivos Específicos

a) Descrever sobre os conceitos de Segurança da Informação;

b) Apresentar alguns tipos de ataques e ameaças existentes;

c) Salientar a importância da proteção da informação;

d) Alertar uma parte população sobre o ataque *Ransomware*;

e) Fazer uma simulação do ataque *Ransomware* para mostrar seu funcionamento e como alguns tipos de mecanismos de segurança irão responder a esse ataque;

f) Propor sugestões para minimizar os riscos de ataques e ameaças;

2 CONCEITOS DE SEGURANÇA DA INFORMAÇÃO

2.1 Segurança da Informação

De Acordo com Araujo (2008):

> A Segurança da Informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplicam-se tanto as informações corporativas quanto as pessoais. Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para o uso restrito ou exposta ao público para consulta ou aquisição.(p.01)

Em sua introdução, a ABNT NBR ISO/IEC 17799, define segurança da informação como "a proteção da informação de vários tipos de ameaças, para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio". Manter a Segurança de informação pode ser uma das atividades fundamentais para atingir a lucratividade e assegurar a competitividade. Já de acordo com Sêmola (2003), "podemos definir Segurança da Informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade".

Os princípios básicos para garantir a Segurança da informação é manter a confidencialidade, disponibilidade, integridade e autenticidade (STALLINGS, 2014).

- Confidencialidade: Capacidade de assegurar que um sistema possa impedir usuários não autorizados de visualizar informações privadas e confidenciais, ao mesmo tempo em que usuários autorizados podem acessá-la (ALBURQUEQUE, 2002).

- Integridade: Capacidade de assegurar que um sistema possa impedir uma alteração ou destruição da informação no sistema sem autorização, ou detectar caso ocorra (ALBURQUEQUE, 2002).

- Disponibilidade: Assegurar que os sistemas não fiquem indisponíveis no momento que usuários autorizados queiram utilizá-los e que operem prontamente (STALLINGS, 2014).

- Autenticidade: Assegurar a fonte da informação.

Após definirmos o que é Segurança da Informação, cumpre-nos definir o que é um problema de segurança:é a perda de qualquer aspecto de segurança importante para o sistema (ALBURQUEQUE, 2002), exemplo: a disponibilidade ou integridade do sistema.

Na segurança temos a definição de alguns termos muito importantes:

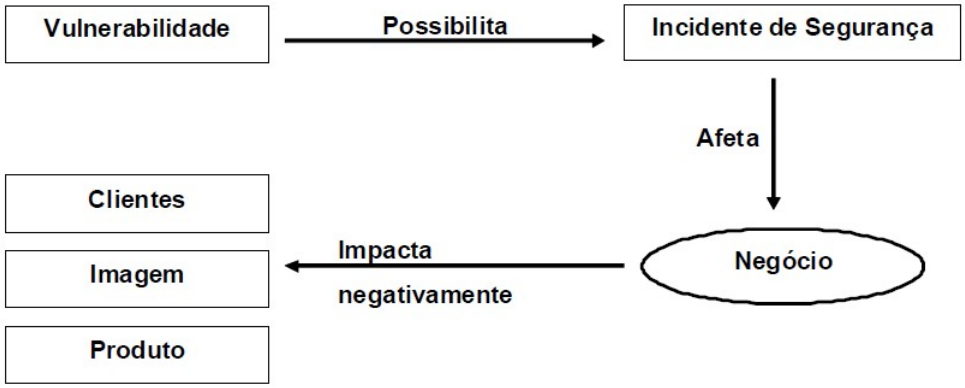
- Ameaça: Qualquer evento externo que possa afetar ou atingir o funcionamento, operação, disponibilidade e integridade da rede ou sistema é considerado uma ameaça. Existem as **ameaças involuntárias**, que são aquelas que não é possivel prevê-las, pois ocorrem devido a operações incorretas, ou seja, de um erro do usuário ou do administrador (ALBURQUEQUE, 2002), como por exemplo falta de energia. Existem também as **ameaças naturais**, ligadas ao meio ambiente, clima ou geografia local,como por exemplos: enchentes, terremotos, descargas atmosfericas, tsunamis, etc. A **ameaças intencionais** são aquelas feitas propositalmente, conscientemente, com o intuito de furtar, roubar, denegrir, destruir as informações, como o monitoramento não autorizado do sistema. Já as ameaças não intencionais, feitas inconscientemente, como por exemplo: a falta de preparo para manusear um equipamento ou o apagamento de um arquivo sem verificar sua importância para a organização ou para o sistema, e falha no *software/hardware*.

  Esses problemas precisam ser considerados quando da elaboração do planejamento da segurança do sistema, já que poderão destruir o ambiente físico do sistema.

- Ataques: São ameaças intencionais, feitos por agentes que buscam obter algum retorno, seja uma senha, dados, informações ou por exemplo derrubar um site importante, seja atingindo um ativo de valor. O ataque explora vulnerabilidades do sistema (ALBURQUEQUE, 2002). Ao contrário do outros problemas citados acima, o ataque é planejado pelo agente e difícil de ser previsto pelo usuário.

- Vulnerabilidade: São fatores internos capazes de expor informações, é o ponto fraco no sistema, onde este é suscetível a ataques ou falhas. A vulnerabilidade permiti a ocorrência de determinados incidentes de segurança, como por exemplo, acessos não autorizados ao sistema, vírus e outros códigos maliciosos, uso indevido de informações, etc, que afetam diretamente o negócio, impactando negativamente a imagem do produto e do cliente. De acordo com Laureano (2005) as vulnerabilidades do sistema são as principais causas das ocorrências de incidentes de segurança , conforme apresenta a Figura 2 .

Figura 2 – Como a vulnerabilidade possibilita incidente na segurança



Fonte: (LAUREANO, 2005)

- Risco: Embora existem vários significados para risco, /citeonlineadriana2005 afirma que na Área de TI, Risco é a probabilidade de um evento vir a acontecer, causando um impacto e podendo produzir perdas.

Beal (2005) alega que para asseverar a segurança da informação deve ser feita uma Análise de Risco. Nessa Análise serão identificados todos os riscos que ameaçam as informações, apresentando soluções que minimizem e eliminem os riscos. De acordo com ISO 27002, nessa análise os riscos serão classificados de acordo com sua importância, podendo ser grave ou não.

2.2 A importância da informação

Pereira (), enfatiza em seu artigo a importância da segurança da informação em caso de ataque, pois caso esteja a descoberto a empresa pode vir a perder informações valiosas suas e de seus clientes, gerando prejuízo de grande monta, podendo causar a paralização ou até mesmo o fechamento definitivo da empresa.

2.3 Ataques na Internet e a segurança.

Qualquer computador ou serviço que esteja conectado via Internet, podem ser alvos de ataques, ou participar deles, destacando que podem ser causados por autores com diferentes objetivos. Para cada objetivo os atacantes utilizam alguma técnica ou ferramenta. As subseções a seguir relatam os principais grupos de ameaça e ataques.

2.3.1 Engenharia Social

Engenharia social é uma técnica utilizada para obter informações confidenciais. Geralmente o atacante tem a habilidade de ludibriar as pessoas, então, aproveitando-se da ingenuidade das pessoas, persuadindo-as a fornecer as informações que precisam. Os ataques podem ser feitos por telefone, e-mails, salas de bate papo ou até mesmo pessoalmente.

Um exemplo citado pelos autores Carvalho e Torres (2003)

- “Bom dia. Sou o engenheiro do <fornecedor de serviços de telecomunicação da empresa alvo> estou a fazer testes na central da vossa zona. Preciso que me indique se existem modems ligados às vossas linhas e quais os respectivos números.”

O sucesso do ataque depende exclusivamente da inocência do usuário, se ele irá fornecer as informações ou clicar em algum programa. No caso citado acima, se a pessoa que atendeu o telefone passar as informações que o atacante solicitou provavelmente o ataque será bem sucedido.

Para evitar que os ataques aconteçam a empresa deve orientar seus funcionário, acerca da engenharia social, alertando-os e orientando-os a não passar informações para estranhos.

2.3.2 Exploração de vulnerabilidades

Um ataque de exploração de vulnerabilidades acontece quando existe alguma falha, seja na segurança seja em algum ponto fraco, e neste caso o "atacante"se aproveita dessa fissura para invadir o sistema, utilizando alguma técnica maliciosa para conseguir acessar informações confidenciais.

2.3.3 Varreduras em redes(*Scan*)

É uma técnica que permite fazer buscas minuciosas em redes, com o objetivo de encontrar computadores ativos e coletar informações. De posses dessas informações podem se saber os programas instalados, os serviços disponibilizados e descobrir as vulnerabilidades dos serviços e programas.

2.3.4 *Phishing*

É uma técnica, como o nome sugere ("phishing"em inglês é "pescaria"), tem por objetivo pescar informações importantes. É um tipo de fraude, na qual o atacante envia uma mensagem não solicitada pelo usuário. Geralmente são mensagens de instituições conhecidas, como por exemplo bancos e sites populares. Quando o usuário acessa as essas páginas falsas ele acaba sendo induzidos a preencher campos em branco com suas informações pessoais, e bancarias.

Exemplos de casos de *phishing*:

- E-mail com formulários contendo informações confidenciais;
- Páginas de Internet banking falsificadas;
- Mensagens com links maliciosos.

2.3.5 Interceptação de tráfego (*Sniffing*)

É uma técnica conscistente na inspeção dos dados sigilosos que trafegam pela rede, como por exemplo senhas. Pode ser usado beneficamente por administradores de rede para solucionar problemas, como também pode ser usado maliciosamente por atacantes com o intuito de captar dados sigilosos.

2.3.6 Força Bruta

Como diz o nome "Força Bruta" o atacante vai tentando todas as combinações possíveis até que senha seja encontrada. Atualmente os atacantes estão demorando para descobrir as senhas pela Força Bruta, haja vista, que as senhas estão com números e caracteres maiores, demandando uma gama de combinações e tempo prolongado para decifrar a senha/chave.

2.3.7 Desfiguração de página (*Defacement*)

É uma técnica que baseia-se na modificação do conteúdo e estética da página Web de um site.

As formas mais utilizadas por um atacante para realizar um *defacement* são:

- Furtar senhas de acessos a interface Web utilizada para administrar remotamente;
- Explorar erros da aplicação web;
- Explorar vulnerabilidades do servidor de aplicação web, onde o site está hospedado;
- Invadir o servidor onde encontra-se o site hospedado e realizar alterações no conteúdo e na estética que compõem o site;

2.3.8 Negação de serviço (DoS e DDoS)

Diferente do que já vimos até agora, o objetivo da negação de serviços não é o roubo de dado das vítimas, mas sim como tirar do ar os servidores, ele impede que usuários legítimos façam uso de recursos computacionais (DUMONT, 2006).

Na negação DoS, somente um invasor envia pacotes para um servidor, para deixar a rede inacessível (ATS, 2012).

Já na negação DDos, os ataques são distribuídos em várias maquinas para enviar os pacotes ao mesmo tempo para um servidor, com o intuito de sobrecarregá-lo. Na nageção DDos, além do atacante, existe também: os mestres que são os computadores que gerenciam os zumbis; os zumbis, que são as máquinas que fazem o ataque, elas inundam os computadores enviando pacotes, fazendo com que haja um congestionamento na rede (ATS, 2012).

Para a prevenção dos ataques é fundamental a verificação da configuração dos roteadores e firewalls para impossibilitar IPs inválidos, bem como bloquear filtros de protocolos que sejam desnecessários, e ainda habilitar a opção de logging(logs) para a realização de um controle das conexões existentes com os roteadores.

2.3.9 *SPAM*

SPAM é a atividade de enviar mensagens eletrônicas, sendo elas e-mails, fóruns de discussão, janelas *pop-up* em páginas da internet, para usuários que não solicitaram o envio. Essas mensagens geralmente possuem propagandas (CERT.BR; CGI.BR, 2012).

2.4 Códigos maliciosos (*Malware*)

Códigos Maliciosos(*malwares*) são programas de computadores que foram estritamente desenvolvidas com o intuito de destruir, corromper, ou usar de forma indevida informações (PROCOPIO, 2010). Segue alguns exemplos:

2.4.1 Vírus

Um vírus de computador é um programa malicioso, que é carregado ao seu computador sem a sua permissão ou conhecimento. Ele se propaga fazendo cópias de si mesmo em programas ou arquivos, podendo se alastrar para outros programas, arquivos e até outros computadores (CERT.BR; CGI.BR, 2012).

2.4.2 *Worm*

O *Worm* (em inglês, que significa "verme") é um programa auto replicável pelas redes, diferente do vírus que precisa da intervenção do usuário para se propagar ou do programa hospedeiro para se alastrar e não contamina programas. Ele envia cópia de si mesmo de computador para computador, explorando a vulnerabilidade do sistema.

2.4.3 *Spywares*

Os *spywares* são programas cuja função é monitorar/espionar as atividades executadas no computador e enviá-las para terceiros. Vírus também podem transportar Spywares, para fazer o monitoramento de dados sigilosos (CERT.BR; CGI.BR, 2012).

Um exemplo são empresas comerciais que espionam as atividades dos usuários da rede de computadores, avaliando seus costumes e preferências, na intenção de vender produtos de interesses do usuário.

2.4.4 Cavalos de Tróia

O cavalo de Tróia[1] é um programa que normalmente é recebido como um "presente", como álbuns de fotos, cartões virtuais animados, jogos e protetores de tela (CERT.BR; CGI.BR, 2012). É um programa que executa funções para o qual foi programado, geralmente maliciosas e sem o conhecimento do usuário. O arquivo contaminado necessita ser executado para que o cavalo de Tróia seja instalado no computador.

Diferentemente dos *malwares* que foram apresentados até o momento na seção Malware, o cavalo de tróia difere desses por não se propagar automaticamente e não infectar outros arquivos.

Eles podem alterar o seu sistema de segurança. Espionar o computador, como um *spyware*, até o usuário digitar uma senha, ou algo do seu interesse. Pode também transportar o *ransomware*.

2.4.5 *Ransowmare*

2.4.5.1 História

Em 1989 (JUNIOR, 2017) um novo ataque foi visto pela primeira vez: o *RANSOMWARE*[2]. Nessa época poucas pessoas possuíam e usavam computadores pessoais, a Web não existia e muito menos e-mails. A Internet era utilizada basicamente por especialistas, a criptografia quase não existia e a forma de pagamento internacional era burocrática. O vírus era enviado por meio dos correios, dentro de disquetes, que criptografavam o disco rígido exigindo um pagamento no valor de US$189 dólares (ALECRIM, 2016), para descriptografar. Mas como já foi dito, na época poucas pessoas utilizavam computadores e a forma de pagamento internacional era burocrática, redundando num fracasso.

[1] Os troianos aceitaram o "presente" dos gregos, um cavalo de madeira, e levaram o cavalo para o interior das muralhas de Tróia. Todos os soldados beberam e comemoraram a rendição do inimigo e, quando todos estavam dormindo, centenas de soldados gregos saíram de dentro do cavalo e atacaram a cidade

[2] A palavra "Ransom" é usada em referência a resgate, exigir resgate, pagar resgate (ALECRIM, 2016)

Com o avanço da tecnologia e da internet, novas ameaças foram surgindo. Após a primeira tentativa em 1989, o próximo ataque aconteceu no período de 2005-2006, na Rússia. De acordo com a Micro (2016a), que é uma empresa focada em segurança de informação, o incidente ocorreu em 2006, detectado como TROJ_CRYZIP.A. Esse vírus fechava certos tipos de arquivos e os substituia, deixando-os com exetensão .zip ,protegidos com senhas. Também foi criado um bloco de notas, que tinha como conteúdo um bilhete de resgate para informar aos usuários que eles poderiam recuperar seus arquivos em troca de US 300 dólares.

Em 2011 foi detectado o TROJ_ RANSOM.QOWA, que exibia uma página repetidamente para os usuários, até que finalmente fosse pago o resgate através de um certo número premium. Também em 2011 uma nova forma de *Ransomware* foi descoberta, O *Police Ransomware*, que bloqueava o acesso ao teclado e ao mouse, exibindo uma mensagem, apresentada na Figura 3, usando imagens de aplicação da lei. A imagem declarava que um crime havia sido cometido e que a vítima deveria pagar uma quantia para conseguir recuperar o acesso ao seu computador (SATZIACK, 2017).

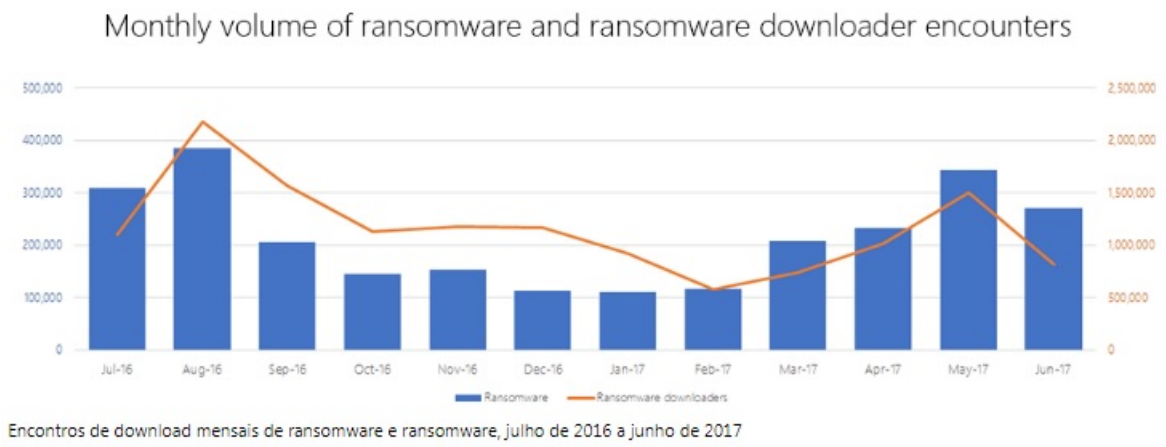
Figura 3 – O *Police* Ransomware.

Fonte: (SATZIACK, 2017)

No final de 2013, surgiu um novo tipo de *ransomware*, denominado *"Cryptolocker"* (MICRO, 2016a), que além de bloquear o sistema ele também criptografava os arquivos.

De acordo com Microsoft (2018) ao longo dos últimos anos, o Ransomware só tem evoluído, tornando-se um problema global.

Figura 4 – Número mensais de ataque Ransomware.



Encontros de download mensais de ransomware e ransomware, julho de 2016 a junho de 2017

Fonte: (MICROSOFT, 2018)

2.4.5.2 O que é?

O *Ransomware* (MICRO, 2016a) é um *malware* que limita o acessa do usuário ao sistema, bloqueando sua tela de computador ou criptografando (*Cryptolocker*) arquivos armazenados em um equipamento com uma senha, tornando-os inacessíveis. Para ter os dados de volta é exigido que o usuário pague um resgate, dentro de um tempo estipulado, assustando-os ou intimidando-os, fazendo com que na maioria das vezes o usuário pague para que possa obter novamente o acesso ao sistema ou seus dados.

O pagamento do resgate na maioria das vezes é feito em *Bitcoins*, a moeda virtual é descentralizada, ou seja não é controlada pelo Banco Central,consequentemente, impossível de ser rastreada (MCGOOGAN,). O seu valor é determinado pela lei da oferta e procura, a Trend Micro (MICRO, 2016a) também lista pagamentos feitos em cartões de presente iTunes e Amazon. Os preços variam de acordo com as taxas de câmbio das moedas digitais, muitas vezes é exigido um valor entre 0.3 e 1 Bitcoins (MCGOOGAN,).

Figura 5 – Página de Pagamento.

Fonte: (ALECRIM, 2016)

2.4.5.3 Como se propaga?

O *Ransomware* pode se propagar de diversas formas. O usuário pode abrir inconscientemente, baixar e instalar um arquivo infectado de um e-mail, ou visitar sites mal-intencionados (MICRO, 2016a). Além disso pode também vir na forma de um instalador falso, como exemplo, de um instalador de antivírus, levando o usuário a clicar em links comprometidos. Na maioria das vezes os atacantes se aproveitam da ingenuidade das usuários, utilizam-se da engenharia social, exibindo mensagens que tentam convencer a vítima de algo, como por exemplo, uma dívida não paga, uma pendência na justiça, uma atualização de segurança de banco, instigando o usuário a clicar no link. Em alguns casos o vírus consegue se propagar sozinho, como no caso do *Wannacry*, ele consegue passar de máquina para máquina dentro de uma rede (JUNIOR, 2017).

De acordo com Alecrim (2016), uma das técnicas de ataque mais eficaz utilizada pelos atacantes, é a engenharia social. Um exemplo citado pelo autor: o usuário recebe um e-mail de uma loja de comércio eletrônico informando que o pedido de determinado produto já saiu para a entrega, mas o usuário não fez nenhum pedido, intrigado o usuário acaba clicando no link para ver o conteúdo, e baixando o *malware*.

Figura 6 – Como o Ransomware se propaga?.

Fonte: (MICRO, 2015)

2.4.5.4 Como evitar?

De acordo com a Micro (2016a) , essas são algumas dicas para o usuário se defender de um possível ataque:

- A proteção mais indicada contra os ataques *ransomware* é fazer *backup* (cópia de segurança) de todos os arquivos em um sistema separado, seja por exemplo em um HD externo, ou em nuvem. Se você sofre um ataque não perderá nenhuma informação;
- Devemos sempre desconfiar de e-mail não solicitados, de remetentes desconhecidos;
- Não clicar em links desconhecidos;
- Outra proteção importante é ter um antivírus instalado no computador e sempre atualizado;
- Ativar os recursos de segurança e privacidade do seu navegador;
- Nunca baixe arquivos de sites que você não conheça.

2.4.5.5 Pagar ou Não Pagar?

De acordo com Alecrim (2016) pagar não é o mais recomendável, eis que incentiva os atacantes a continuarem, e não há garantia de que os dados serão devolvidos, todavia os invasores prefem fazer a devolução das informações, pois caso se propague a notícia de que

as informações não foram devolvivas, no caso de novos ataques as pessoas podem desistir de efetuar o pagamento.

Especialistas da Micro (2016a) não aconselham as vítimas a efetuar o pagamento antes de tentarem descriptografar os dados ou desbloquear o sistema. Embora não seja garantido que usuários terão acessos aos dados novamente, atualmente já existem ferramentas para tentar descriptografar os arquivos contaminados, mas infelizmente os hackers estão sempre lançando novas versões de *malware* e utilizam algoritmos criptografados mais resistentes. Um exemplo de ferramenta é a *Decryptor Trend Micro Ransomware File*, disponível para baixar no link : <https://success.trendmicro.com/solution/1114221>.

O primeiro passo que o usuário terá que fazer ao instalar *Decryptor Trend* Micro *ransomware*, é selecionar o nome do *ransowmare* (Figura 7). A maioria dos *ransomwares* inclui um arquivo texto para informar o usuário que seu sistema foi infectado por um determinado tipo. No site do *Decryptor Trend Micro Ransomware File*, o usuário consegue ter acessos a todos os passos que devem ser seguidos.

Figura 7 – Seleção do Ransomware.

Fonte: (MICRO, 2015)

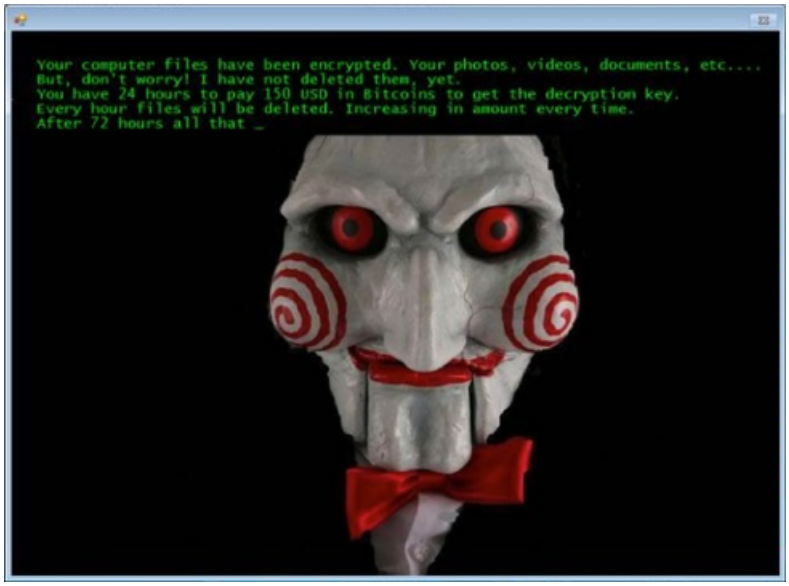
2.4.6 Exemplos de *Ransomware*

De acordo com o blog TrendMicro (2017)algumas das ameaças mais assustadoras do *ransomware* são:

- JIGSAW:

  Inspirado na série de filmes "Jogos mortais", Billy saúda os usuários que estão sofrendo o ataque com uma mensagem, mandando o usuário pagar o resgate ou lidar com as consequências. Os atacantes apagam os arquivos pouco a pouco até que o resgate seja pago.

Figura 8 – Ataque Jigsaw



Fonte: (TRENDMICRO, 2017)

- *CERBER*

  Existem várias versões do *Cerber*, mas a original é a mais assustadora. O Cerber conversa com as vítimas para alertá-los da infecção. -"ATENÇÃO, ATENÇÃO, seus arquivos foram criptografados". Eles dão o prazo de 7 dias para o usuário pagar o resgate, caso não seja efetuado eles dobram a quantia exigida no início.

- *MICROP*

  O *ransomware Microp* insulta as vítimas com mensagens culpando-as pelo ataque, como se estas estivessem atacando-o para furta-lo. E para ter os arquivos de volta, os criminosos pedem que a vítima devolva o que foi furtado.

  A pessoa mascarada que aparece na foto e os valores de resgate do Microp, de quase US$ 29 mil dólares, assustam as vítimas.

Figura 9 – Ataque MICROP

Fonte: (TRENDMICRO, 2017)

- *Crysis*

  O *ransomware Crysis* consegue criptografar até 185 tipos de arquivos e deletar os backups. Como os outros *ransomware* para ter novamente acesso aos dados, a vítima deve pagar um resgate.

- Stampado

  A característica principal do Stampado é que ele não disponibiliza muito tempo para as vítimas efetuarem o resgate, a cada seis horas um arquivo aleatório é excluído permanentemente, e após 96 horas a chave de descriptografar desaparece para sempre. O objetivo dos criminosos é fazer com que as vitímas paguem o resgate o mais rádido possível.

2.5 Técnicas de prevenção

De acordo com Vacca (2013), para uma empresa manter o foco na segurança da informação são necessário 10 (dez) passos:

1. Avaliar os riscos e ameaça

   Avaliar os riscos do negócio de uma organização, é um dos pontos mais importantes na segurança da informação. É fundamental saber os riscos do negócio, como preveni-lo e, caso aconteça como recuperar.

2. Ter cuidado com equívocos comum

Segundo Vacca (2013) um dos equívocos mais comum das organizações é achar que seu negócio nunca será alvo de ataques. Todos nós usuários precisamos entender que só de estarmos conectados a uma rede, temos grandes chances de ataques maliciosos.

3. Treinamento contínuo da equipe de Segurança da Informação

   É de extrema importância que a equipe esteja sempre atualizada e preparada para novas ameaças e vulnerabilidades.

4. Pensar fora da caixa

   É sempre importante atentar para todos os riscos que podem vir a acontecer, como por exemplo, caso um funcionário seja demitido da empresa, é necessario que se recolha os equipamentos e dispositivos USB por ele utilizados,evitando assim que ele os leve consigo.

5. Desenvolver nos funcionários uma cultura por segurança.

   É importante treinar todos os funcionários, incutindo-lhes que a segurança da informação é fundamental para um bom funcionamento da organização.

6. Identificar e utilizar aspectos de segurança do S.O.

   Saber como é o funcionamento das ferramentas de segurança do sistema operacional é fundamental.

7. Monitorar os sistemas

   É fundamental efetuar constatemente o monitorando das ferramentas de segurança, como por exemplo gerar relatórios, analisar os logs gerados pelo sistemas,etc.

8. Contratar terceirizados para auditar a segurança da empresa

   A contratação de empresas especializadas em auditorias para realizar um mapeamento nos processos de segurança da empresa é ferramenta fundamental eis que os tecnicos externos não possuem vinculação com a empresa, portanto não serão tendenciosos, e estão aptos a encontrar falhas na segurança e sugerir mecanismos para melhorias e proteção do sistema empresarial.

9. Não esquecer do básico

   Definir políticas de senhas fortes, não abrir arquivos de fontes desconhecidas,etc.

10. Manter os sistemas atualizados

    É extremamente importante que software de segurança estejam sempre atualizados.

2.6 Mecanismo de defesa

Nesta serão apresentados alguns mecanismos de Defesa que podem ser utilizados para a prevenção de ameaças e ataques a sistemas (MULATINHO, 2015).

2.6.1 Política de Segurança da Informação

A Política de Segurança da Informação é um documento que determina normas, métodos e procedimentos relacionadas ao uso seguro de dados, e que orienta e estabelece as diretrizes aos funcionários para a proteção dos ativos de informação (OLIVEIRA, 2013). A política deve ser comunicada a todos os funcionários, de todos os setores e deve ser revisada em intervalos de tempos regulares ou quando mudanças se fizerem necessárias.

2.6.2 Gerenciamento de Riscos

O gerenciamento de risco é um processo no qual é feito o controle dos riscos. Os riscos são identificados, analisados, reduzidos e/ou eliminados da organização. Os processos podem ser divididos em vários passos. De acordo com Vaughan e Vaughan (2008 apud MULATINHO, 2015), os passos a serem seguidos a fim de garantir um bom gerenciamento são os seguintes:

- Determinar os principais objetivos;
- Identificar os riscos ao qual a organização esta exposta;
- Avaliar os riscos;
- Considerar as alternativas e selecionar dispositivos para o tratamento dos riscos;
- Implementar as decisões tomadas;
- Avaliar e revisar o processo continuamente.

2.7 Mecanismo de segurança

Abaixo serão apresentados algumas funcionalidades e ferramentas que auxiliam na prevenção de ameaças e ataques.

2.7.1 Criptografia

A palavra Criptografia tem origem grega, a palavra *kryptós* significa "escondido", e *gráphein* "escrita". Como no significado de origem grega, a criptografia é a ciências e a arte de escrever e transformar informações e mensagens, em formas aparentemente ilegíveis, cifradas ou em códigos. Esse processo é chamado cifragem. Apenas o destinatário com a chave consegue decodificar e ler a mensagem, esse processo é chamado de decifragem (LAUREANO, 2005).

De acordo com Laureano (2005), a criptografia é um conjunto de técnicas, que tem como finalidade manter os dados seguros. Essas técnicas consistem na utilização de chaves e

algoritmos criptográficos. Mas como aqui veremos, a criptografia também pode ser utilizadas por pessoas mal intencionadas.

Os métodos criptográficos podem ser divididos em duas categorias de algoritmos criptográficos: simétricos (chave-secreta) e assimétrico (chave pública).

Na criptografia simétrica é utilizado a mesma chave para cifrar e decifrar os dados, quando uma pessoa vai comunicar com a outra ela gera a chave e a transmite no canal de comunicação para o destinatário.

A criptografia simétrica possui alguns problemas de segurança, durante transmissão da chave no canal alguém pode interceptar a chave no caminho e ter acesso aos dados.

Figura 10 – Criptografia Simétrica.

Fonte: (MICRO, 2015)

Os algoritmos de chaves simétricos podem utilizar dois tipos de cifras, a de bloco e cifras de fluxo.

Uma cifra de bloco cifram os dados a partir de um bloco, ou seja, um bloco de texto claro é tratado como um todo e usados para gerar um bloco de texto cifrado com o mesmo tamanho (STALLING, 2008). Se o dado é um texto, esse texto será dividido em blocos, e esses blocos serão criptografados.

Uma cifra de fluxo codifica um fluxo de dados, um bit ou um *byte* de cada vez, diferentemente da cifra de bloco.

Alguns dos algoritmos mais utilizados em chaves simétricas são:

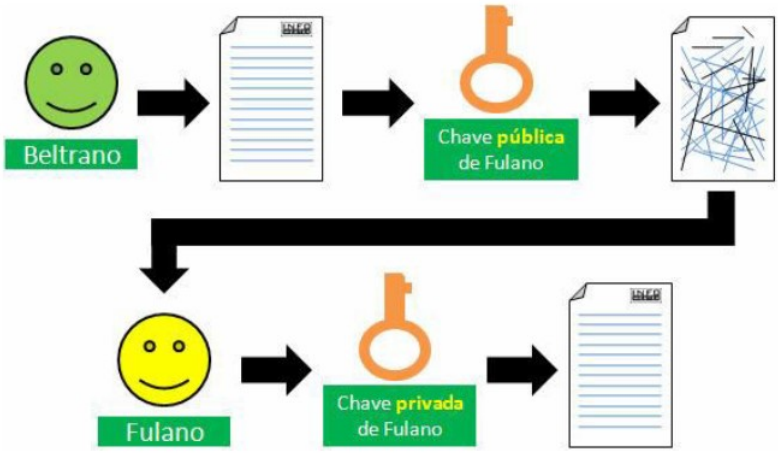
- DES (*Data Ecryption Standard*) : É um dos esquemas de criptografias mais utilizados (STALLING, 2008). Ele utiliza a cifra de blocos. O DES criptografa os textos claros em blocos de 64 bits, usando uma chave de 56 bits, produzindo um texto cifrado de 64 bits. O tamanho da chave é muito pequena, podendo se quebrar facilmente. Não é confiável, deve ser usado somente em modo de operação.

- AES (*Advanced Encryption Standart*) : É um esquema de criptografia que veio para substituir o DES, ele utiliza um tamanho de bloco de 128 bits e um tamanho de chave de 128, 192 ou 256 bits. O tamanho da chave de 128 bits é 16 bytes, da chave de 192 bits é de 24 byts e o tamanho criptografia de 256 bits é de 32 bytes. O AES é mais forte se comparado com o DES, por seu comprimento ser maior, levando mais tempo para quebrar um algoritmo de criptografia.

Já os algoritmos de chaves assimétricas, diferentemente das simétricas, utilizam chaves distintas, uma para cifrar e outra para decifrar, sendo uma pública, que pode ser divulgada, e uma privada, que deve ser mantida em segredo e pertence a apenas um participante, o destinatário. Uma desvantagem da criptografia assimétrica em relação a simétrica é que ela é mais lenta, requer mais capacidade de processamento para criptografar e descriptografar.

E como escolher a chave? Depende da proteção que o usuário deseja.

Figura 11 – Criptografia Assimétrica.



Fonte: (MICRO, 2015)

Alguns dos algoritmos mais utilizados em chaves assimétricas são:

- RSA (Ron Rivest, Adi Shamir e Len Adleman) : RSA é um Sistema de chave Assimétrica produzido por Ron Rivest, Adi Shamir e Len Adleman, por isso o nome RSA, e é o mais utilizado no mundo. O RSA utiliza a cifra de blocos, e utiliza números primos. É baseado na fatoração de número primos extensos.

- DSA(*Digital Signature Algorithm*) : É um procedimento muito mais eficiente se comparado com o RSA, porém a verificação é muito pesada. Sua chave privada opera sobre o hash da mensagem SHA-1. Para averiguar a assinatura um pedaço do código calcula o hash e outro pedaço usa a chave pública para descriptografar a assinatura (BARBOSA, 2013).

Também existe a criptografia hibrida, que é a junção das duas criptografias citadas acima. Utiliza a boa performance computacional da chave simétrica com a troca segura de chaves da assimétricas. Exemplo que utiliza: protocolo SSL(Secure Socket Layer).

2.7.2 AntiVírus

O antivírus é um *software* de defesa, o mais comumente utilizado, responsável por assegurar o computador bloqueando e impedindo a entrada de invasores e ameaças virtuais, como por exemplo, anexos de e-mails contaminados, arquivos corrompidos, sites infectados, links maliciosos. O *software* antivírus podem detectar *malwares* incluindo os tipos, vírus, *worms*, cavalos de Tróia, códigos maliciosos, ferramentas de atacantes.

Nem sempre os antivírus acertam, eles podem dar muitos falsos positivos, que são arquivos que os antivírus detectam como ameaças, mas não são. Esses arquivos ficarão bloqueados em quarentena, até o usuário remove-los.

Todo antivírus possui seu próprio banco de dados, onde são armazenadas as características dos *malwares* e das ameaças conhecidos em ambientes virtuais. Essas informações são atualizadas pelos fabricantes à medida que novas ameaças são detectadas, mas depende do usuário atualizá-lo para que o banco de dados do antivírus baixado seja atualizado.

Os antivírus operam verificando todos os arquivos abertos na máquina, sempre que abrimos um arquivo executável ele faz uma verificação para compará-lo com o *malware* conhecido. De acordo com Comodo (2018) as formas de detectar vírus são feitas através da detecção baseada em assinatura, baseada em heurística, e comportamento, segue a explicação:

- Baseada em Assinatura: A detecção de vírus /*malware* baseada por assinatura, verifica todos os arquivos executáveis e o válida com as listas conhecidas de vírus e malwares existentes. Esses vírus contêm assinaturas, ou seja, uma sequência continua de *bytes*. Quando é encontrado uma sequência equivalente no banco de dados do antivírus, é muito provável que se trate de um vírus conhecido.

  A detecção por assinatura é uma das mais utilizadas por todos os fabricantes de antivírus. Porém ela tem um grande problema, diariamente são criados dez tipos de vírus (PROCOPIO, 2010), e, até que os fabricantes consigam efetuar a atualização do *software* muitos usuários podem ser contaminados pelo vírus ainda não cadastrado. Por isso é fundamental outras técnicas de detecção.

- Baseado em Heurística: O software utiliza a detecção baseado em heurística quando são executados programas e/ou aplicativos com códigos suspeitos que não foram detectados no banco de dados, ou seja, não possuem assinaturas equivalentes.

  Diferentemente da técnica baseada em assinatura, a busca baseada em heurística não procura por assinaturas correspondentes, ela utiliza regras e algoritmos para detectar

malwares. Ela compara as características de *malwares* conhecidas, com as dos que ainda não foram cadastrados no banco de dados. A partir dessa comparação o antivírus consegue determinar se o arquivo ou programa tem alguma característica em comum com outros vírus e se pode ser um tipo vírus.

- Baseado em Comportamento: A detecção baseada em comportamentoo analisa e monitora os comportamentos do programa/arquivo, caso perceba algo fora do comum, ele interrompe a execução do programa. O modelo baseado em comportamento pode dar muitos falsos positivos .

Um exemplo citado pelo Tutoriaisti (2018):

> "Imagine que você esteja desconfiado de que uma pessoa é um ladrão de carros. Se essa pessoa tiver ficha na polícia por furto/roubo de carros, certamente é um ladrão de carros. Isso é detecção por assinatura, pois, graças a um furto anterior, você deduziu e determinou que ele rouba carros; Se ela não tem ficha na polícia, mas existe um conhecido ladrão com o nome muito parecido e com o mesmo endereço e tipo físico, provavelmente eles são a mesma pessoa: detecção heurística. Suas características são tão parecidas que permitem determinar que ele seja a mesma pessoa de quem você está desconfiado.Se não tem ficha na polícia nem nenhum indício que comprove que ele é um ladrão de carros, mas a pessoa comporta-se como tal, andando com chaves variadas, olhando seu carro com jeito estranho, sabe tudo de alarmes de carros e de como desativá-los: detecção por comportamento, por não termos assinatura (ficha) nem heurística (dados semelhantes), mas, devido seu comportamento, determinamos que ele é mesmo um ladrão de carros."(p.01).

Quando o antivírus escaneia seu computador e detecta algum arquivo malicioso, ou suspeito, ele para a execução do arquivo, colocando-o em quarentena. A quarentena é uma pasta gerenciada pelo antivírus que não permite que o vírus se espalhe pelo SO, ela criptografa os arquivos maliciosos de forma que outros antivírus não os identifique como vírus (ROHR, 2009).

O antivírus quando encontra um arquivo malicioso ou suspeito apresenta duas opções ao usuário: deletar ou colocar em quarentena. O antivirus não apaga imediatamente o arquivo/-programa, porque nem sempre eles são confiáveis, podendo detectar vírus em arquivos inócuos, com isso o usuário pode recuperar o arquivo. O antivírus não deleta o arquivo/programa imediatamente,repito, ele é colocado em quarentena, pois caso seja apagado definitamente do sistema, pode atrapalhar o bom funcionamento do computador fazendo com que ele não opere da forma correta.

Como vimos, um antivírus é capaz de atuar antes que os códigos maliciosos invadam e furtem dados do computador, assim ter um antivírus instalado e atualizado é fundamental, eis que a cada dia novas ameaças são detectadas, podendo comprometer a segurança de organizações e pessoas físicas.

2.7.3 *Backup*

O *backup* é um dos mecanismo de segurança mais seguros que existem. *Backup* é a cópia de determinado arquivo em local separado e seguro, o usuário pode acessar de qualquer computador, aparelho celular, ou HD externo. Um exemplo é salvar os dados em nuvem. É importante fazer *backups* sempre novas informações forem adicionadas. Pessoa física ou juridica que tiverem essa precaução de fazer *backups* todos os dias terão chances remotas de perder dados importantes (CERT.BR; CGI.BR, 2012).

2.7.4 Senhas

Segue algumas dicas para proteger senhas:

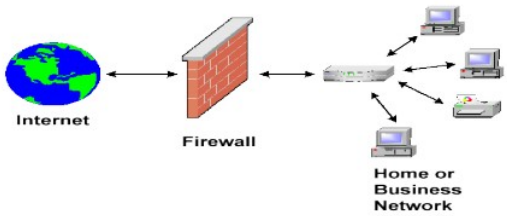
- Não utilizar como senha datas de aniversário ou que possam relacionar com você, seu nome, sobrenome, número de telefone, número de documento, placas de carro;
- Utilizar uma senha que tenha no mínimo oito caracteres, sendo números, letra maiúscula e minúscula, símbolos;
- Alterar a senha com frequência;
- Não utilizar a mesma senha para diversos serviços;

2.7.5 *Firewall*

A palavra *firewall* significa “Muralha de fogo” (SARAIVA, 2012). O firewall é um *software* ou *hardware* que protege o tráfego de dados entre computadores e redes, ele verifica as informações vindas da Internet podendo bloqueá-las ou não (MICROSOFT,).

De acordo com Mariano e Pereira *firewall* é um sistema que controla o acesso às redes de computadores, bloqueando acessos não autorizados em redes pessoais ou de empresa, ou seja uma política de *firewall* decide quem tem autorização para passar em cada direção, sendo de dentro pra fora ou vice-versa.

Figura 12 – Firewall



Fonte: (MICRO, 2015)

De acordo com (MICROSOFT,) existem 4 técnicas que os firewall utilizam para controlar o acesso e impor a política de segurança do site:

- Controle de serviço: Determina os tipos de serviços de Internet que podem ser acessados, de entrada ou saída.
- Controle de direção: Determina a direção que cada solicitação de serviço pode ser iniciada e permitida.
- Controle de usuário: Determina qual serviço especifico o usuário está tentando acessar.
- Controle de comportamento: Controla como um serviço especifico é usado.

Existem três tipos de *Firewall*:

1 . Filtro de pacote: É onde ocorre o bloqueio ou a liberação da passagem de pacotes.

2 .*Firewall* NAT *(Network Address Translation)*: Faz a tradução do endereço IP e porta TCP de uma rede para a internet.

3 . TextitFirewall Proxy: Um *proxy* é um servidor que faz a intermediação dos pedidos de um usuário com os outros servidores.

3 MATERIAL E METODOLOGIA

O trabalho foi executado em 5 etapas, ilustradas na Figura 13.

Inicialmente, foi realizado uma pesquisa bibliográfica, com o objetivo de aprimorar os conhecimentos sobre Sistemas de Informação e entender o ataque *ransomware*.

Porteriormente foi efetuada a escolha dos mecanismos de seguranças que seriam utilizados, os Antivírus . Após a escolha dos antivírus, o vírus *Hidden-Tear* foi compilado no software Visual Studio, gerando um arquivo executável.exe. Esse arquivo foi executado primeiramente sem antivírus e foi mostrado como é seu funcionamento. Após feita a simulação sem antivírus, foram feitas as simulações com os antivírus. A medida que os testes foram acontecendo,os antivírus eram instalados por vez, e ao terminar eles iam sendo desinstalados.

Após todas as simulações foram feitas análises.

Figura 13 – Metodologia Proposta

Fonte: Elaborado pela autora.

1 Aprofundamento nos estudos sobre Segurança da Informação, e *ransomware*;

2 Execução do Vírus *Hidden-Tear*;

3 Estudo sobre o comportamento dos antivirus após o ataque;

4 Alerta à população quanto a Segurança da Informação e ao *ransomware*;

5 Sugestão de melhorias;

3.1 Ferramentas utilizadas

3.1.1 Ambiente de Teste

Para o desenvolvimento do trabalho foi utilizado um ambiente de rede local, construído através de software de virtualização VirtualBox. A máquina hospedeira possui as seguintes configurações: Intel® Core™ i5-4210u CPU @1.70GHz 2.0GHz, com memória instalada(RAM) de 4,00 GB e o Sistema Operacional Windows 8.1 Professional 64 bits.

Na máquina virtual foi utilizado Intel® Core™ i5-4210u CPU @1.70GHz 2.39GHz e memória Ram de 2.00 GB e o Sistema Operacional Windows 10.

O Sistema Operacional utilizado na VM foi o Windows 10. De acordo com Stats (2017) o Windows é o software mais utilizado no mundo, porém, não é software mais seguro. Comparando com o sistema operacional Windows, o Linux é o mais seguro (DELFINO, 2018), pois, roda seus programas em modo de usuário, e, para acessar e modificar qualquer configuração, o usuário deve colocar a senha do administrador, diferentemente do Windows, onde o usuário tem acesso ao sistema.

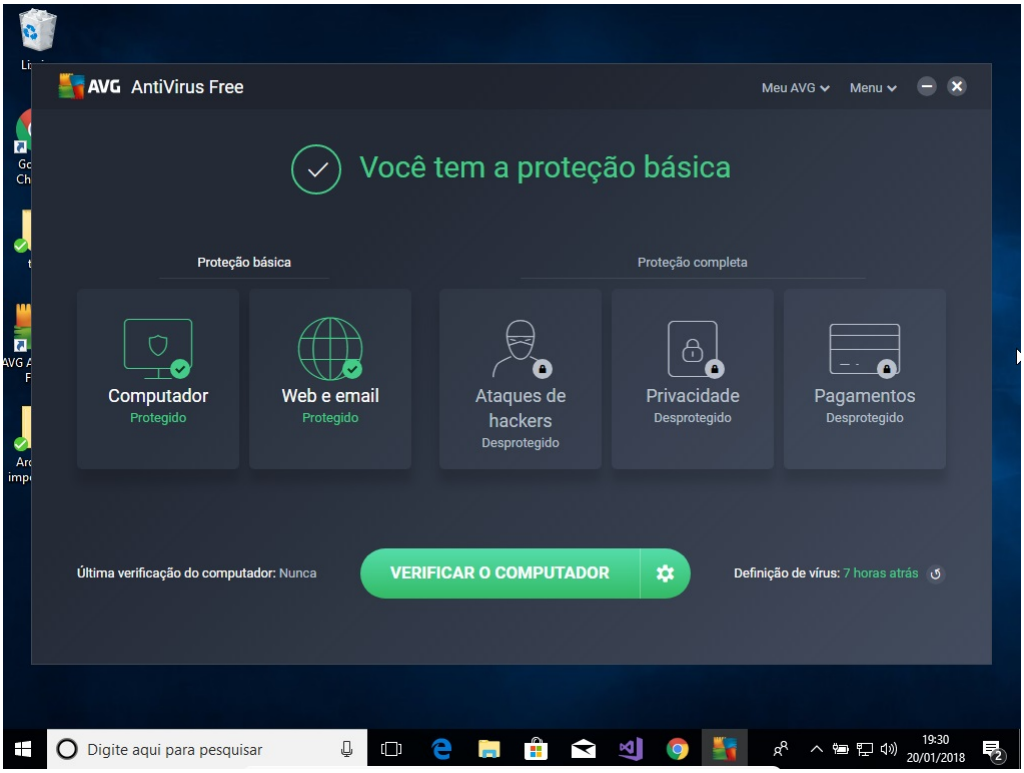
3.1.2 AntiVírus Utilizado

Para a simulação do ataque, optou-se pelos antivírus recomendados por Ciriaco (2017), a saber, AVG free, Avast Free, Avira e o Windows Defender. Anote-se que também foi utilizado <http://nodistribute.com/>

3.1.2.1 AVG free

O AVG AntiVirus Free está disponível para ser instalado no site: <https://www.avg.com/pt-br/free-antivirus-download>. O AVG garante ao usuário o bloqueio de vírus, *spywares, ransomware* e outros textitmalwares,o bloqueio de links, downloads e anexos de e-mails suspeitos. Verifica se há problemas de desempenho no PC, e obtém atualizações de segurança em tempo real. Ele utiliza a busca baseada em assinatura e baseado em heurística para a detecção de vírus.

Figura 14 – Tela inicial do AntiVirus AVG

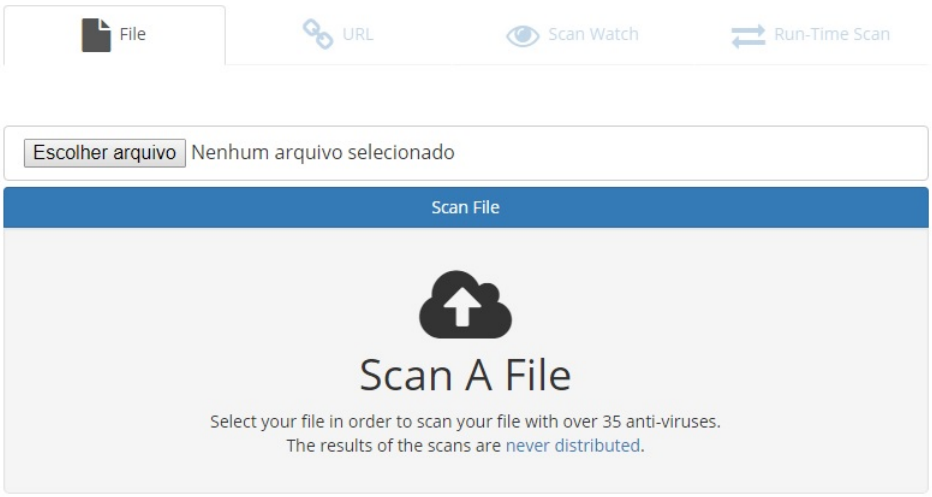


Fonte: Print screen do antivírus avg no sistema operacional Windows 10.

3.1.2.2 *NoDistribute*

O Site foi escolhido pela praticidade, o usuário não precisar ter o software instalado na máquina. Através do site <http://nodistribute.com/> o usuário consegue anexar o arquivo que pretende verificar e digitalizar. A verificação é feita on-line, com 35 Antivírus disponíveis.

Figura 15 – Tela inicial do Site *NoDistribute*

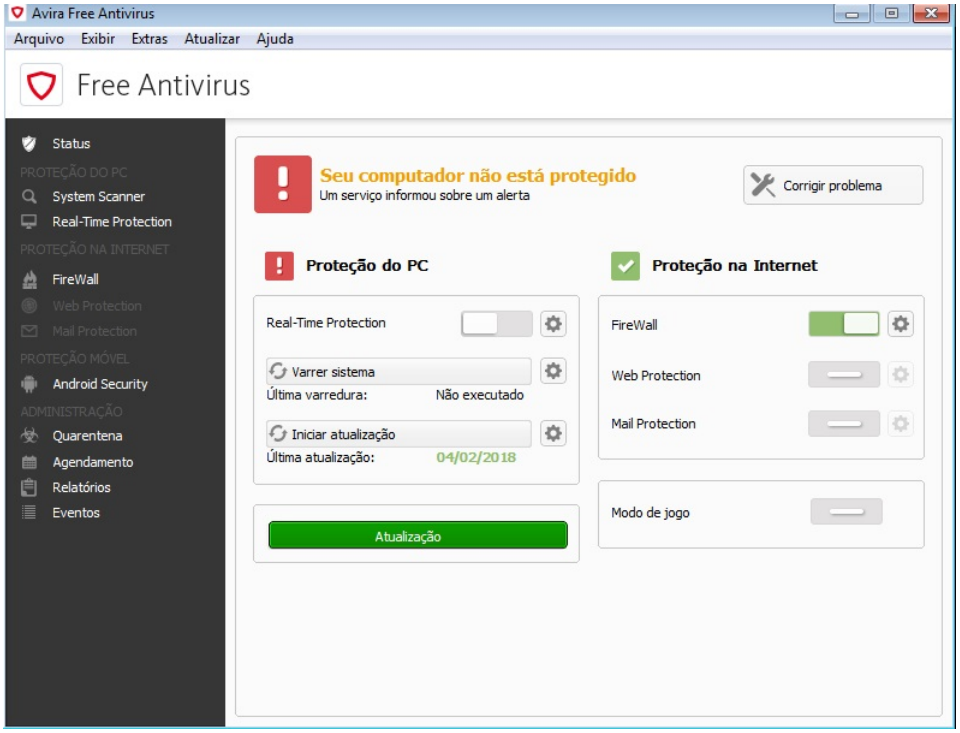


Fonte: Print screen do site Nodistribute no sistema operacional windows 10

3.1.2.3 Avira

O AntiVírus Avira pode ser instalado pelo site: <https://www.avira.com/pt-br/download/product/avira-free-antivirus>. O Avira garante ao usuário proteção de última geração, proteção para *ransomware*, garante a privacidade e oferece suporte coletivo.

Figura 16 – Avira Inicial

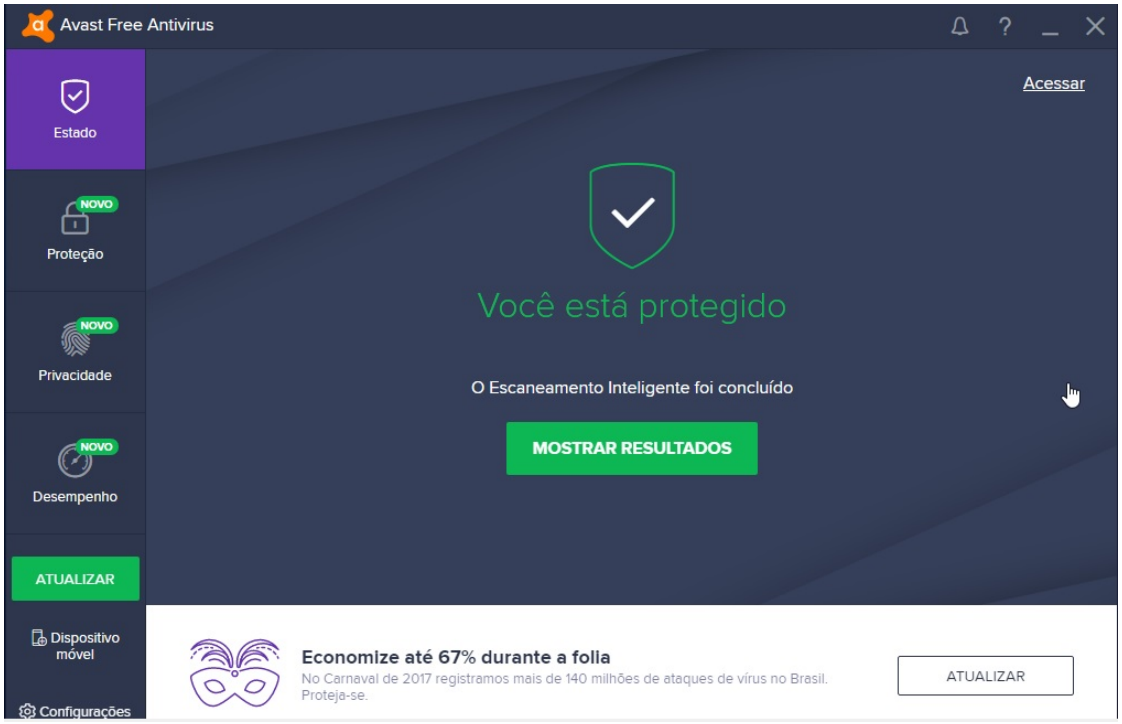


Fonte: Print screen do antivírus avira no sistema operacional Windows 10

3.1.2.4 Avast

O antivírus Avast está disponível para ser instalado no site, <https://www.avast.com>. O Avast promete ao usuário um Antivírus inteligente, que detecta e bloqueia vírus, *malware, spyware, ransomware e phishing*, usa análise inteligente para impedir que seja afetado. Envia automaticamente arquivos suspeitos para análise na nuvem e cria uma cura para todos os usuários do Avast, se houver uma ameaça. Ele também verifica Wi-Fi, detecta automaticamente pontos fracos em seu Wi-Fi doméstico e estranhos na rede. E por fim, garante o escaneamento inteligente, encontra pequenas falhas que permitem a entrada de *malwares*, de configurações e senhas inseguras e suspeitos e *software* desatualizados.

Figura 17 – Tela Inicial Avast



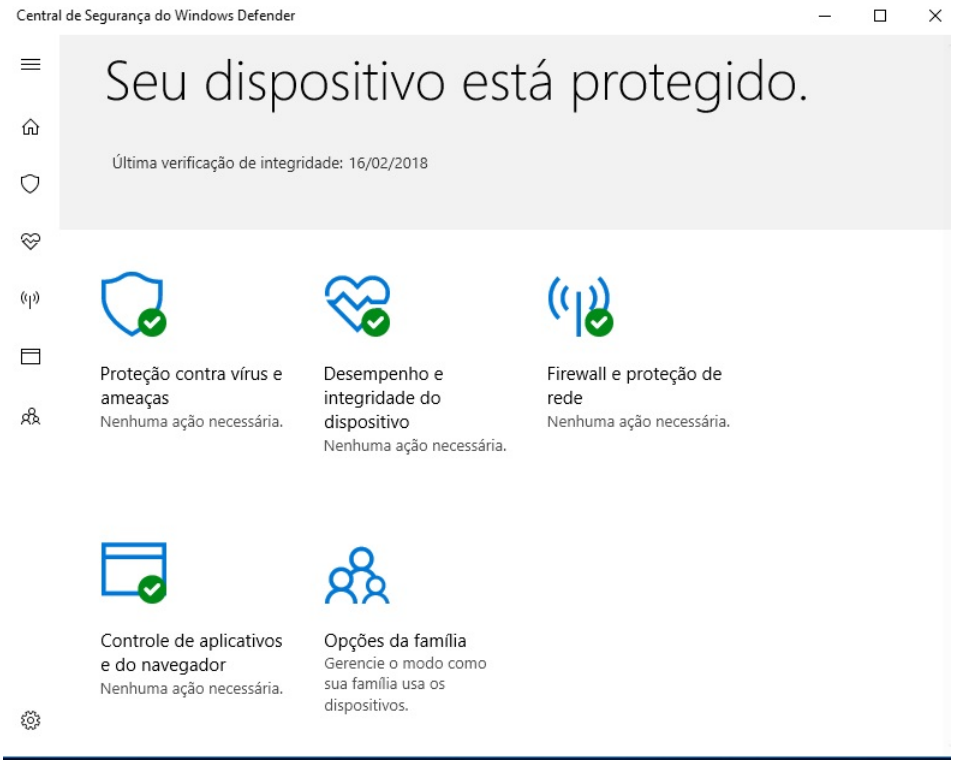
Fonte: Print screen do antivírus avast no sistema operacional Windows 10

3.1.2.5 *Windows Defender*

O Windows Defender é um software exclusivo do Windows. Disponível para as versões mais recentes do Windows, que são, Windows 8, Windows RT, Windows 8.1, Windows RT 8.1, Windows 10. Ele ajuda a proteger o computador em tempo real contra *spyware*, vírus, *rootkits* e outros tipos de *software* mal-intencionado. Quando encontra algo suspeito ele dá opção ao usuário de:

- Ignorar o alerta , e continuar a instalação/abrir um software;
- Enviar para a quarentena;
- Remover o arquivo;
- Permitir que o software altere configurações relacionadas à segurança do computador;

Figura 18 – Tela Inicial Windows Defender



Fonte: Print screen do windows defender no sistema operacional Windows 10

3.1.3 Código *Hidden-Tear*

O programa *Hidden-Tear* foi criado por um grupo de segurança turco, Otku Sen e está disponível no *GitHub* para fins educacionais. É possível ter acesso pelo link: <https: //github.com/goliate/hidden-tear/>.

Hidden-Tear é um trojan *Ransomware*, que criptografa os arquivos dos usuários do Windows. Ele utiliza algoritmo AES simétrico para criptografar arquivos, e envia uma chave de criptografia simétrica para um servidor. O servidor web que foi utilizado nesse trabalho foi o: 000 Web Host . Foi utilizado uma chave de tamanho 256 bits , e o tamanho do bloco de 128 bits.

Após os arquivos serem criptografados ele gera um arquivo texto, "LEIA.txt", na área de trabalho, que instrui o usuário como proceder. E a extensão dos arquivos passa a ser .LOCKED. Os arquivos criptografados podem ser descriptografados através de uma ferramenta, que contém um campo em branco onde deve ser inserido a chave de descriptografar. A ferramenta será enviada para o usuário por e-mail junto com a senha, após efetuado o pagamento.

4 RESULTADOS

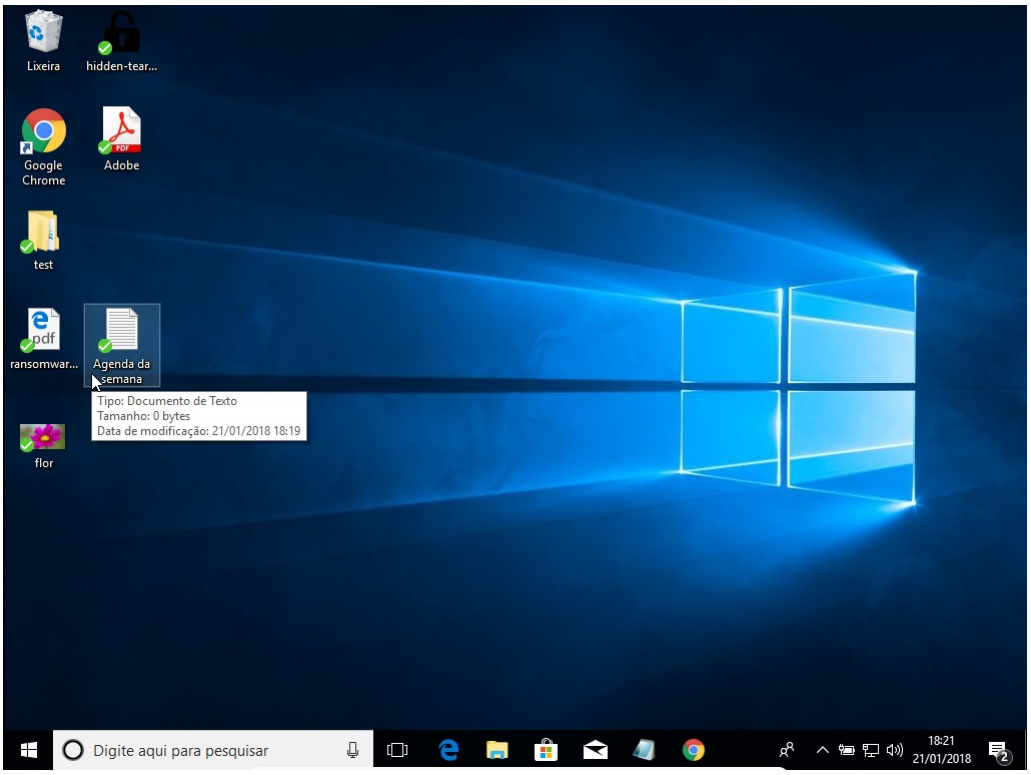
Para a execução das simulações de ataque foi utilizado o vírus *Hidden-Tear* e analisado como os antivírus e o Site NoDistribute responderam a estes ataques, ressaltando como já previamente relatado que antes de executar as simulações com o antivírus foram efetuadas simulações sem antivírus.

As simulações foram feitas com arquivos executáveis, gerados pelo visual Studio, e com arquivos infectados anexados, e enviados por e-mail, e logo após foram baixados do e-mail (Esses arquivo estavam com o *Hidden-Tear*).

4.1 Ataque sem antivírus

Primeiramente foi feita uma simulação do Vírus *Hidden-Tear* sem nenhum antivírus instalado no computador.

Figura 19 – Tela Inicial Windows

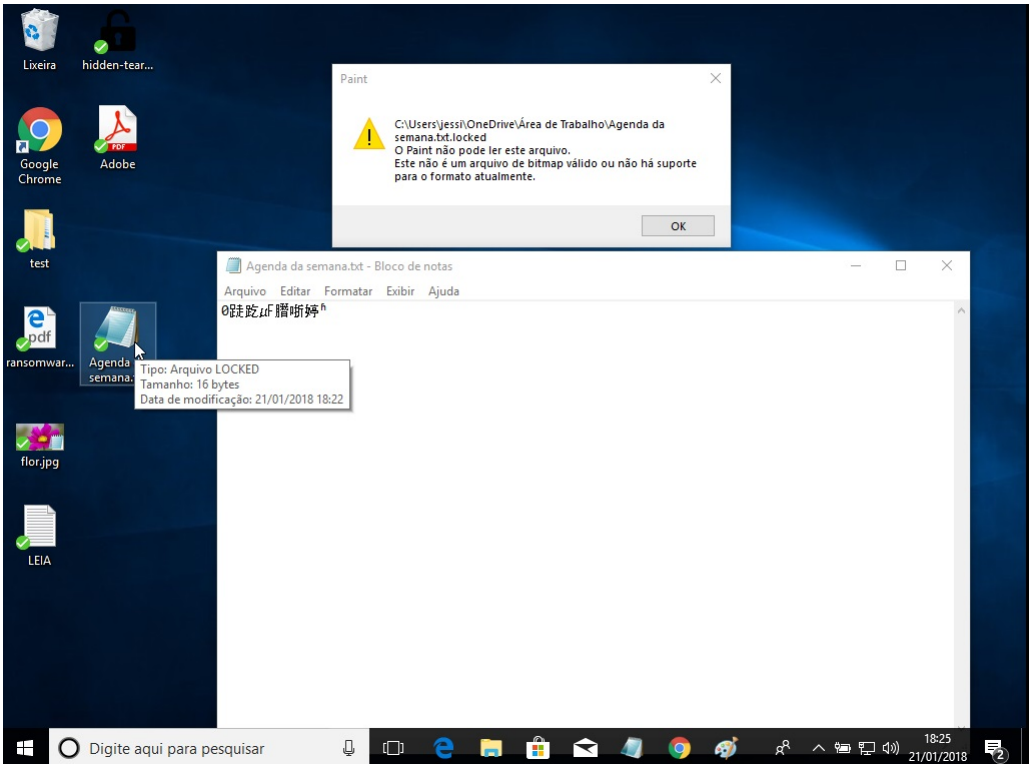


Fonte: Print screen no sistema operacional Windows 10

Conforme se verifica na Figura 19, os arquivos constantes na área de trabalho não estavam criptografados. Um exemplo é o arquivo "Agenda da semana.txt". O arquivo “ADOBE” é o

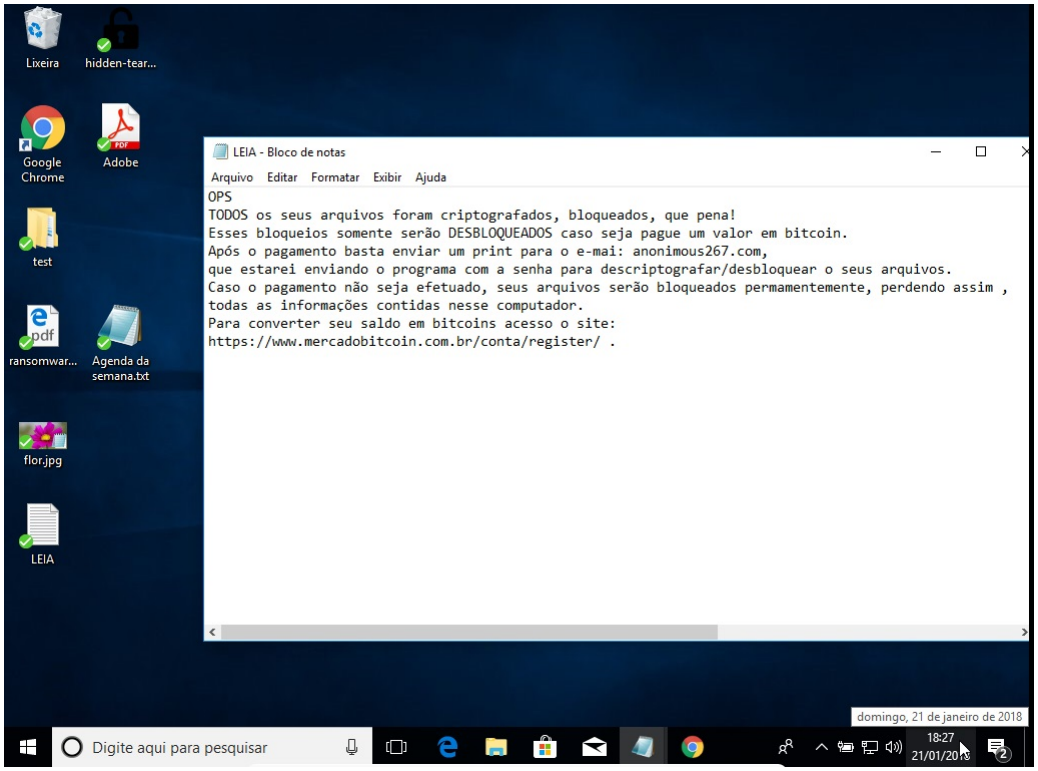
vírus *Hidden-Tear*. Ao clicar no arquivo infectado, os arquivos da área de trabalho foram todos criptografados (Figura 20). O arquivo "Agenda da semana" já passa a ter a extensão *LOCKED* e as informações nela contidas foram criptografadas. Também foi criada uma pasta "LEIA.txt", informando ao usuário o que está acontecendo e como deve agir (21)

Figura 20 – Tela após Criptografar os arquivos



Fonte: Print screen no Windows 10

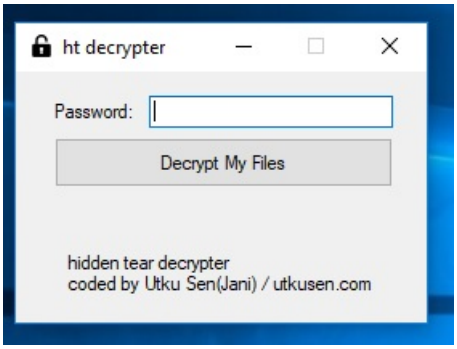
Figura 21 – Arquivo Leia



Fonte: Print screen no Windows 10

Para descriptografar os arquivos foi utilizado uma ferramenta de descriptografar (Figura 22). O usuário irá colocar a senha no campo em branco, e clicar em "(*Decrypt My Files*)".

Figura 22 – Ferramenta para descriptografar



Fonte: Print screen no Windows 10

Após digitar a senha e clicar para descriptografar, os arquivos criptografados foram todos recuperados.

4.2 Análise no site *nodistribute*

A segunda simulação realizada foi a verificação do arquivo "Arquivo Importante", no site <http://nodistribute.com/>.

Após inserir o arquivo, os antivírus detectaram a ameaça, bem como o vírus, de acordo com a base de dados de cada antivírus, e, no caso dos antivírus que não detectaram ameaças, foi mostrado na tela do computador a palavra "Clean"na frente do antivírus. De 36 antivírus, 21 reconheceram o Vírus, de acordo com o NoDistribute.

Como podemos ver na Figura 23, de acordo com o site, o antivírus AVG free e o AVAST não detectaram o vírus no banco de dados, ou seja, os respectivos antivírus não possuem os vírus na suas base de dados e o AVIRA detectou com o nome TR / ATRAPS.ttgrl.

4.3 AVG FREE

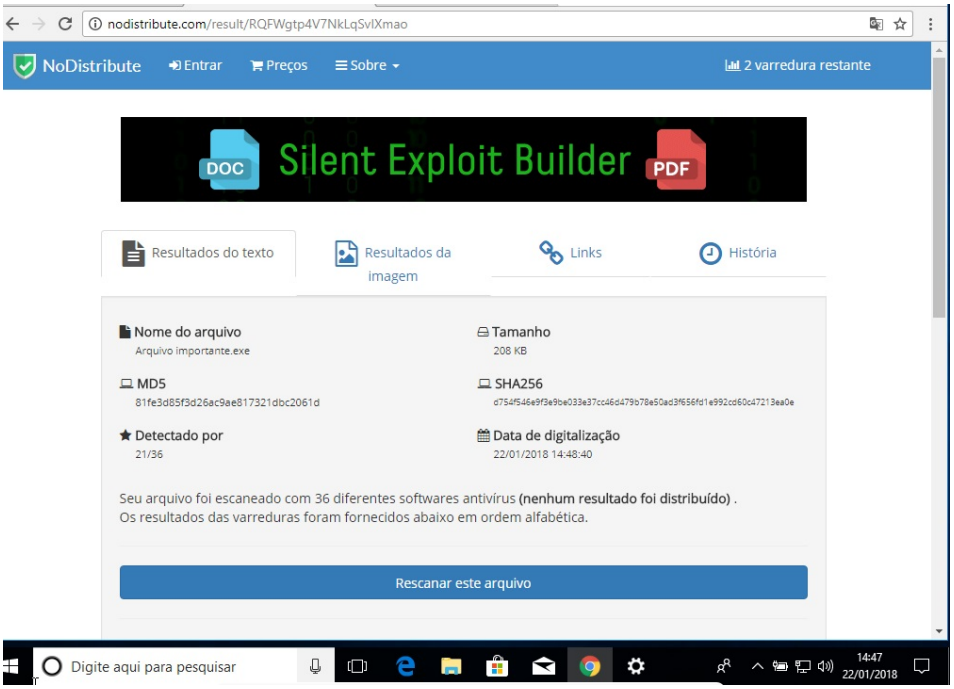
O primeiro *Software* antivírus que foi analisado foi o AVG free.

O software foi instalado no computador e logo em seguida foi feito a varredura no sistema, não detectando nada. Após a varredura, foi feita a simulação do ataque. O nome do arquivo executável que estava infectado era o "Arquivo Importante.exe", ao tentar abrir o arquivo apareceu uma mensagem do antivírus informando que a ameaça foi neutralizada e movida para a quarentena, ou seja, o antivírus detectou um vírus na sua base de dados, e moveu para quarentena, permitindo ao usuário optar se quer ou não deletar.

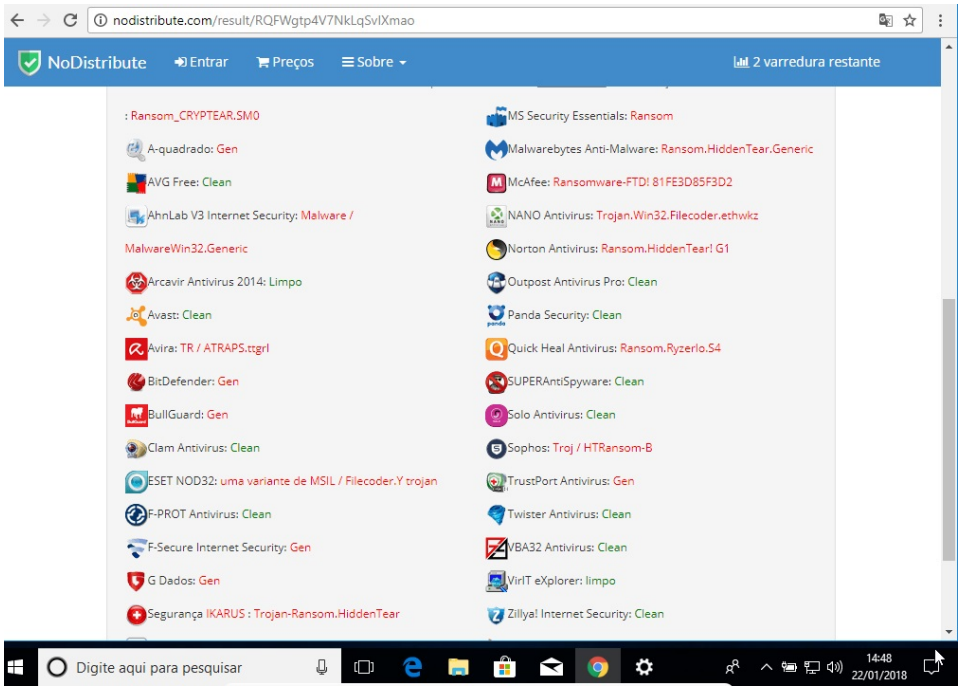
O vírus foi detectado pelo AVG com nome Win32 malware.gen. De acordo com <https://www.enigmasoftware.com/pt/win32malwaregen-remocao/> o Win32 malware.gen é uma infecção por um Trojan da plataforma do Windows. O Win32 malware.gen é capaz de se espalhar através de e-mails não solicitados, de sites maliciosos e redes de compartilhamento de arquivos. Depois que o Win32 malware.gen estiver dentro de um sistema, ele vai fazer alterações nas configurações do sistema e do registro, o que faz com que o desempenho do sistema se deteriore. O cavalo de tróia pode vir com outros malwares, como o *Ransomware*, que foi o que aconteceu.

Figura 23 – Verificação no NoDistribute

(a) Dados do Arquivo

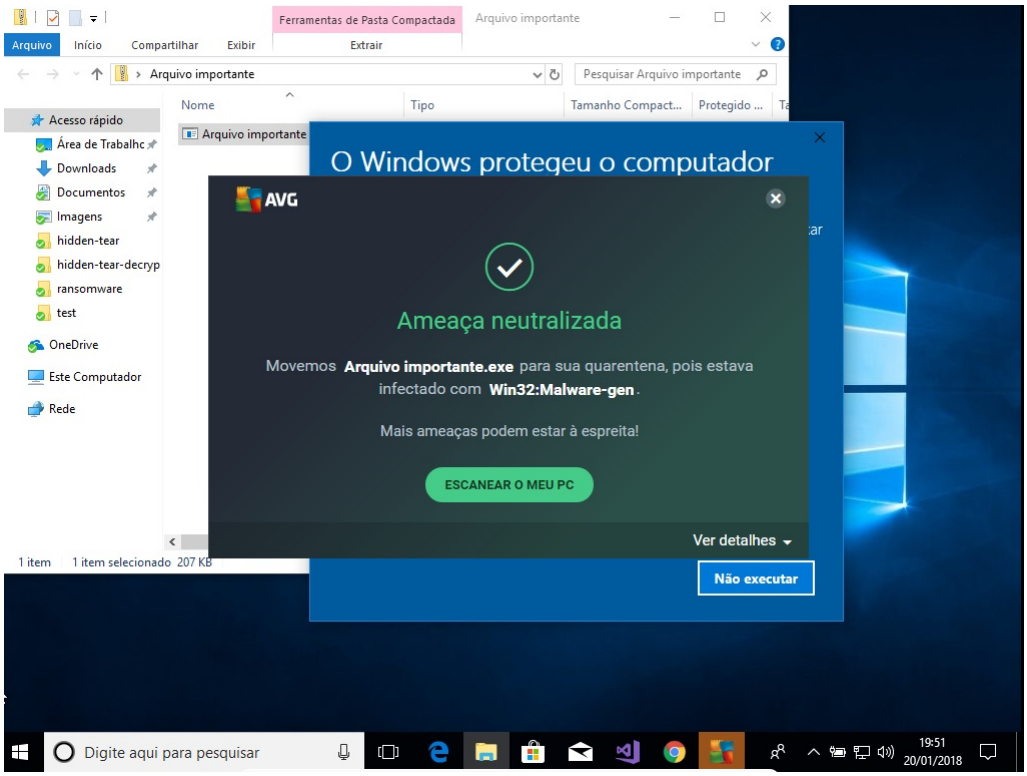


(b) 35 Tipos de AntiVirus



Fonte: Print screen do site Nodistribute no Windows 10

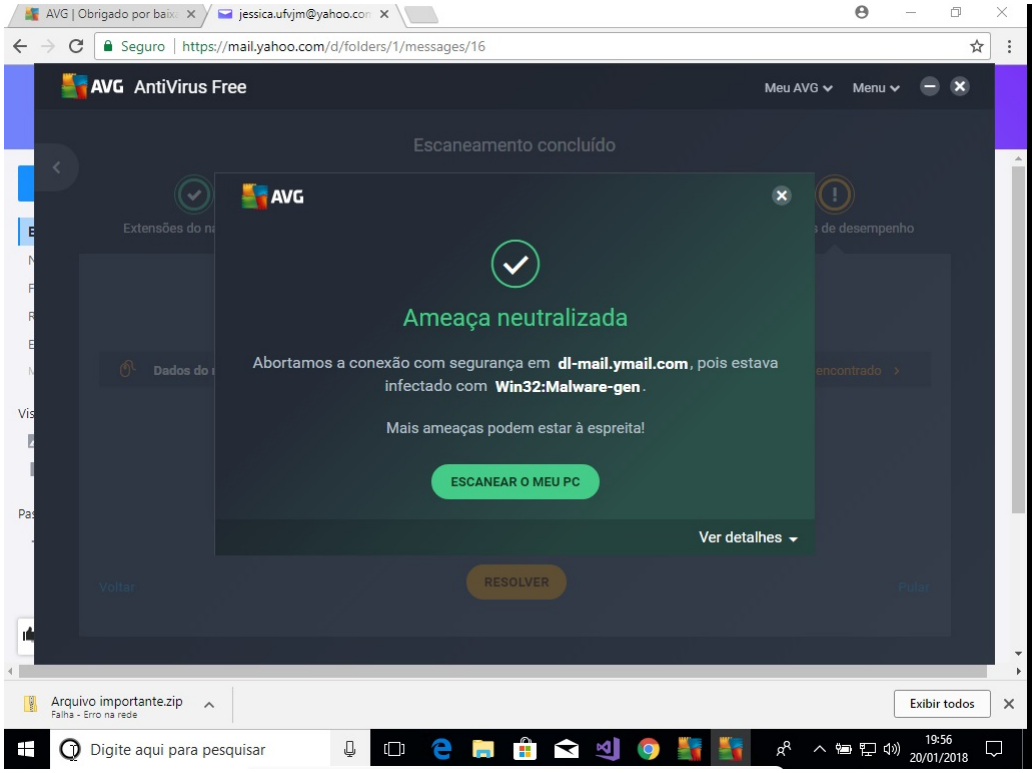
Figura 24 – Mensagem AVG ao tentar abrir o arquivo.



Fonte: Print screen do antivírus AVG no Windows 10

A próxima simulação foi tentar baixar uma pasta zipada, do e-mail. Ao tentar baixar a pasta o AVG detectou uma ameaça e ocorreu um erro, sendo a ameaça neutralizada (Figura25).

Figura 25 – Mensagem AVG ao tentar abrir o arquivo.



Fonte: Print screen do antivírus AVG no Windows 10

Na Figura 23, na simulação realizada no site Nodistrisbute, é possível visualizar que o antivírus AVG (do site Nodistribute) não reconheceu o vírus, contudo na simulação realizada com o antivírus AVG instalado no computador, o software detectou uma ameaça.

4.4 AVIRA

O segundo software que foi testado foi o AVIRA.O primeiro procedimento feito foi a varredura, e nada foi detectado. Ao tentar abrir o arquivo denominado "Arquivo Importante.exe"o Avira exibiu um alerta de segurança avisando que o arquivo foi bloqueado e movido para a quarentena (Figura 26),eis que foi detectado um vírus na sua base de dados, com o nome TR / ATRAPS.ttgrl (Figura 23). O termo ’TR’ refere-se a um Cavalo de Tróia que pode espionar dados, violar sua privacidade ou realizar modificações indesejadas no sistema.

Realizada outra simulação, ao tentar baixar o arquivo infectado do e-mail, o Avira reconheceu o vírus em sua base de dados e bloqueou o *download* do arquivo.

Figura 26 – Mensagem alerta AVIRA

Fonte: Print screen do antivírus Avira no Windows 10

4.5 AVAST

O terceiro software testado foi o Avast, e, a princípio, foi realizado uma varredura em todos os arquivos e nada foi detectado. Proseguindo foi efetuada tentativa de executar o arquivo denominado "Arquivo importante.exe", que, registre-se, estava infectado com o vírus *Hidden-tear*, contudo, o Avast não reconheceu nenhuma ameaça, haja vista que o vírus ainda não estava cadastrado em seu banco de dados.

Após abrir o "Arquivo importante.exe", os dados da área de trabalho foram todos criptografados, como é apresentado na Figura 20 e exibindo o arquivo "Leia.txt".

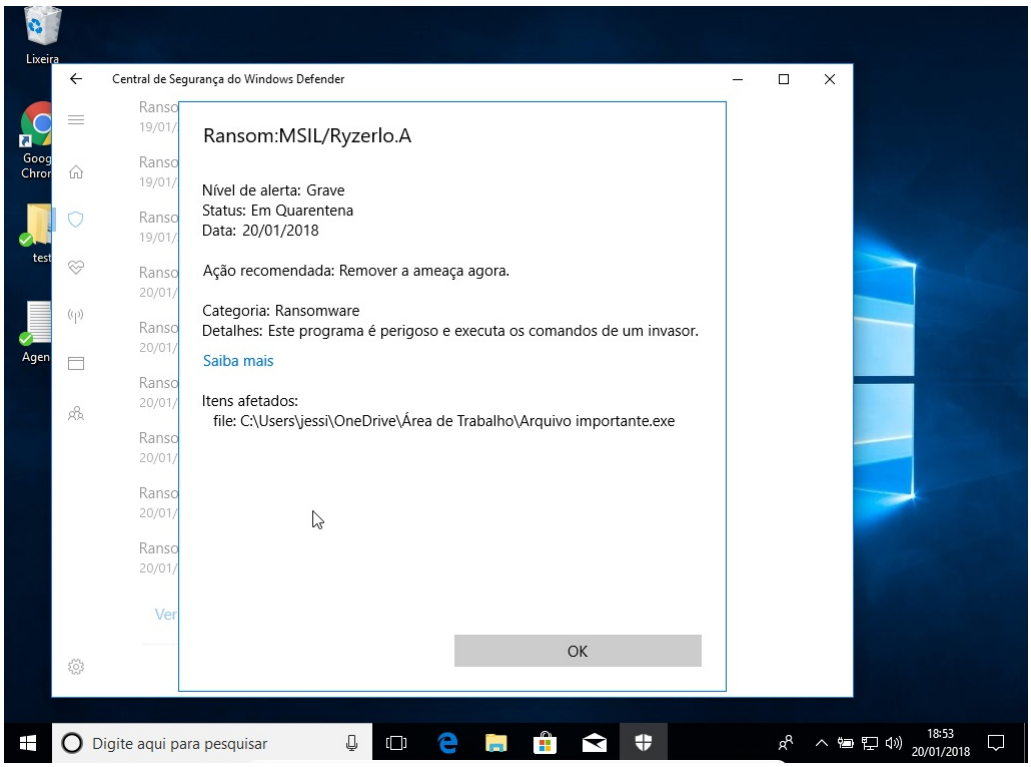
Também foi possível baixar a pasta zipada do e-mail, e mais uma vez executar o arquivo, e criptografar todos os arquivos da área de trabalho.

4.6 *Windows Defender*

O quarto e ultimo programa a ser testado, foi o *Windows Defender*.

Ao tentar abrir o arquivo denominado "Arquivo importante.exe"e fazer o download pelo e-mail, foi exibida uma mensagem informando que o Windows Defender encontrou ameaças em sua base de dados, com o nome Ransom:MSIL/Ryzerlo.A, que é um *ransomware*, de alerta grave, sendo o arquivo movido para a quarentena.

Figura 27 – Mensagem alerta*Windows Defender*



Fonte: Print screen do Windows Defender no Windows 10

5 CONSIDERAÇÕES FINAIS E CONCLUSÃO

Com a pesquisa bibliográfica foi possível compreender que Segurança da Informação vai muito além de investimentos em tecnologias e políticas de segurança. Para que uma organização empresarial mantenha-se segura, seus funcionários/usuários precisam ter acesso a treinados rotineiros, com os software de segurança sempre atualizados, equipes capacitadas para as respectivas áreas de trabalho e instruidas sobre a segurança da informação, utilizando boas soluções de backup, ter staffs de especialistas da área de segurança, possuir um gerenciamento de risco, definir sua política de segurança. Todos os usuários devem ser treinados nos conceitos básicos de segurança.

De acordo com Ferreira (2017), um dos vetores de ataque do *ransomware* mais utilizados é o e-mail, que foi objeto de simulaçoes no presente trabalho.

Segundo informações do Micro (2017a), no ano de 2016 houve um aumento surpreendente de 752%(setecentos e cinquenta e dois por cento) no número de famílias de *ransomware*, o que acaba por deixar os antivírus temporariamente inoperantes, eis que com a rapidez que estão surgindo novas famílias de *ransomware* os antivírus não conseguem atualizar sua base de dados com a mesma rapidez. Por isso é sempre bom o usuário atualizar a base de dados do software.

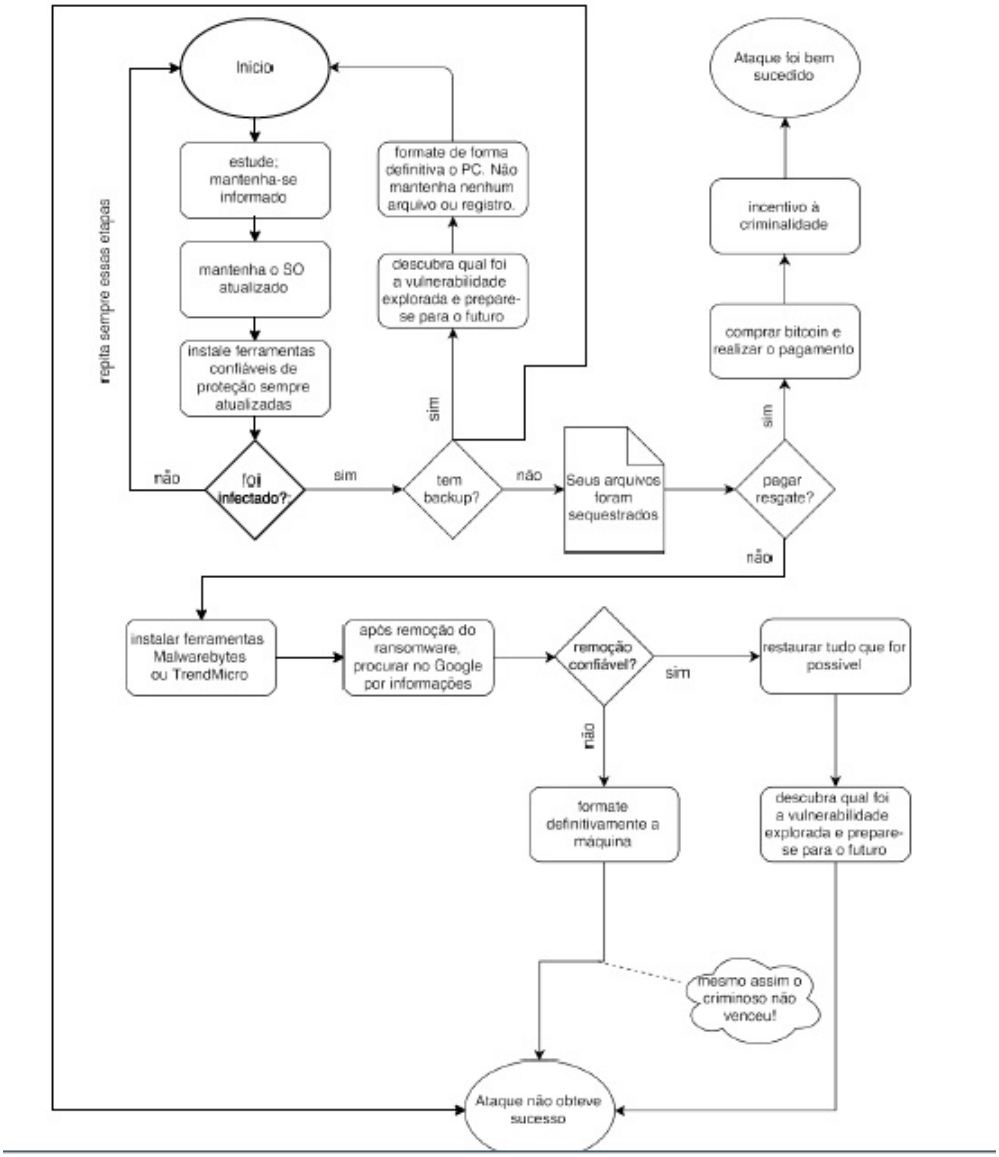
Ao avaliar as simulações foi possível verificar que as ferramentas testadas, com exceção do AVAST, estão capacitadas para proteger os usuários do vírus testado, e possuem base de dados para detectar alguns ataques de Ransomware, mas isso não quer dizer que o AVAST seja pior que os outros. Assim, é sempre recomendavél que o usuário atualize constantemente a base de dados do software antivírus, e da mesma forma que utilize de outras alternativas além do antivírus para se precaver. Segue algumas sugestões e dicas para minimizar o risco de ataques e perda dos dados:

- Fazer Backups regularmente;
- Atualizar regularmente o antivírus;
- Manter o sistema operacional sempre atualizado;
- Em hipótese alguma desativar o antivírus para abrir algum documento, se ele informou algum alerta de segurança é porque o arquivo está com alguma ameaça;
- Ter bastante cuidado ao clicar em links;
- Não abrir e-mail desconhecidos;

Dentre os arquivos que auxiliaram e deram norte ao presente trabalho, destacamos os de: Cauê Zaghetto, Luiz Henrique Morais Aguiar, Bruno Souza Lobo Almeida Gabriel Freitas

dos Santos, com tema "RANSOMWARE: ESTE PROBLEMA TAMBÉM PODE SER SEU", suas principais contribuições foi a explicação de como o *ransomware* age e o estudo de um fluxograma,(Figura 28) de ações preventivas e/ou reativas a serem adotadas, servindo para enfatizar a urgente necessidade do usuário em estar mais instruído sobre a necessidade da segurança e as ações que devem ser tomadas caso sejam infectados pelo *ransomware*.

Figura 28 – Fluxograma de ações preventivas e/ou reativas a serem adotadas.



Fonte: (ZAGHETTO et al., 2017)

Um dos maiores avanços tecnológicos de todos os tempos foi a Internet, que trouxe grandes benefícios a sociedade, que tem passado a maior parte do tempo na Web, seja para trabalho seja para lazer. Através dela é possível enviar e receber informação de todo o mundo, podendo também o usuário dela se utilizar para relização de pesquisas sem precisar se locomover. A Internet tem promovido oportunidade para a educação, haja vista a possibilidade de cursos a

distância (on-line), beneficiando a população de baixa renda, alunos que não tem condição de se locomover ate as unidades educacionais, facilitando também a comunicação entre o corpo discente e docente.

Estamos cada vez mais dependentes da Internet, contudo a sociedade ainda está desinformada acerca dos riscos da inerentes ao seu uso, oportunizando que hackers e pessoas mal intencionadas furtem ou façam uso negativo das informações alheias. É preciso que os usuários saibam utiliza-la e que também conheçam seus malefícios.

Podemos pois concluir que os antivírus, com exceção do AVAST, já possuem base de dados para o vírus *hidden tear*. Mesmo ele sendo um vírus antigo, criado em 2015, ainda existem antivírus que não o reconhecem.

Por todo o exposto percebe-se que, mesmo com todo o avanço tecnológico e as ferramentas disponibilizadas, há por parte de usuários(pessoas fisicas, empresas públicas e privadas) certa negligência com relação a segurança da informação, e, em face dessa desidia que deixa a rede em condição de vulnerabilidade é que sofrem os ataques.

Por fim, há que se dizer que este trabalho não teve a pretenção de esgotar o estudo sobre o referido tema e sim, lançar luzes, alimentar a discussão para que outros interessados e a categoria profissional possam continuar o debate sobre a discussão pretendida. Mas de forma relevante, mesmo com o pouco material encontrado sobre Segurança da Informação, funcionamento do antivírus, e o *ransomware*, houve base de orientação para uma reflexão crítica, enquanto trabalho de conclusão de curso.

REFERÊNCIAS

ALBURQUEQUE, R. *Segurança no Desenvolvimento de Software*. [S.l.]: Campos, 2002. Citado 2 vezes nas páginas 17 e 18.

ALECRIM, E. *O que é Ransomware?* 2016. Disponível em : <https://www.infowester.com/ransomware.php>. Acesso em 08 Dez.2017. Citado 3 vezes nas páginas 23, 26 e 27.

ALMEIDA, S. *Ataque de Ransomware: não chore pelo WannaCry*. 2017. Disponível em :<https://gblogs.cisco.com/pt/2017/06/14/ataque-de-ransomware-nao-chore-pelo-wannacry/>. Acesso em 30 Jan.2018. Citado na página 14.

ARAUJO, N. S. *Segurança da Informação*. 2008. Disponível em: <http://www.administradores.com.br/artigos/tecnologia/seguranca-da-informacao-ti/23933/>. Acesso em 07 de Set.2017. Citado na página 17.

ATS, G. *Entenda o que são os ataques dos e ddos.* 2012. Disponível em : <http://www.techtudo.com.br/artigos/noticia/2012/01/entenda-o-que-sao-os-ataques-dos-e-ddos.html>. Acesso em 07 set.2017. Citado na página 22.

BARBOSA, L. A. de M. *RSA, Criptografia Assimétrica e Assinatura Digital*. 2013. Disponível em :<http://www.braghetto.eti.br/files/Trabalho%20Oficial%20Final%20RSA.pdf>.Acesso em 03.Fev.2018. Citado na página 34.

BEAL, A. *Segurança Da Informação: Principios e Melhores Praticas Para a Proteção Dos Ativos de Informação Nas Organizações*. [S.l.]: Atlas, 2005. Citado na página 19.

CAMPOS, A. *SISTEMAS DE SEGURANÇA DA INFORMAÇÃO*. 2. ed. [S.l.]: Visual Books, 2007. Citado na página 13.

CARVALHO, P. T. S. H.; TORRES, C. B. *Segurança dos sistemas de informação: Gestão estratégica da segurança empresarial*. [S.l.]: Centro Atlantico, 2003. Citado na página 20.

CERT.BR; CGI.BR. *Cartilha de Segurança para Internet*. 2012. Disponível em <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf> Acesso em 08 Dez.2017. Citado 3 vezes nas páginas 22, 23 e 37.

CIRIACO, D. *Os melhores antivírus gratuítos e pagos*. 2017. Disponível em : <https://canaltech.com.br/antivirus/os-melhores-antivirus/>. Acesso em 20 Dez.2017. Citado na página 40.

CISCO. *Cisco 2017, Midyear Cybersecurity Report*. 2017. Disponível em :<https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/1456403/Cisco$_2$017$_M$idyear$_C$ybersecurity$_R$eport.pdf?$elqTrackId = f6ccd8439e9945639096a9846044695aelqaid = 5897elqat = 2 > .Acessoem06Jan.2018.Citadonapgina14.$

COMODO. *How AntiVirus Works?* 2018. Disponível em : <https://antivirus.comodo.com/how-antivirus-software-works.php>Acesso em 30 Jan.2018. Citado na página 35.

CORPORATION, S. *Norton Cyber Security Insights Report 2016*. 2016. Disponível em :<https://www.symantec.com/content/dam/symantec/br/docs/reports/2016-norton-cyber-security-insights-comparisons-brazil-pt.pdf>. Acesso em 30 Jan.2018. Citado na página 13.

DELFINO, P. *DUELO DE TITÃS: QUAL É O MELHOR SISTEMA OPERACIONAL? LINUX OU WINDOWS*. 2018. Disponível em : <http://e-tinet.com/linux/qual-e-melhor-sistema-operacional/>. Acesso em 30 Jan.2018. Citado na página 40.

DUMONT, C. *Segurança Computacional: Segurança em Servidores Linux em Camadas.* 2006. Citado na página 21.

FERREIRA, L. de M. *OS RISCOS DO SEQUESTRO DE INFORMAÇÕES PELOS RANSOMWARES*. 2017. Citado na página 57.

FLORENZANO, C. *Negligência com a TI e Segurança da Informação alavancaram ciberataque mundial.* 2017. Disponível em : <http://www.cbsi.net.br/2017/05/negligencia-com-ti-e-seguranca-alavancaram-ciberataque-mundial.html>. Acesso em 07 Fev.2018. Citado na página 14.

JUNIOR, A. *O que é o ransomware e como se proteger dele*. 2017. Disponível em : <http://gizmodo.uol.com.br/giz-explica-ransomware/>. Acesso em 08 Dez.2017. Citado 2 vezes nas páginas 23 e 26.

KASPERSKYLAB. *Ransomware:2016 em números*. 2016. Citado na página 14.

KEMP, S. *Digital in 2017: Global Overview.* 2017. Disponível em :<https://wearesocial.com/uk/special-reports/digital-in-2017-global-overview>Acesso em : 30 jan.2018. Citado na página 13.

LAUREANO, M. A. P. *Gestão de Segurança da Informação*. 2005. Citado 3 vezes nas páginas 18, 19 e 32.

MCGOOGAN, C. *O que é WannaCry e como o ransomware funciona?* Disponível em: <http://www.telegraph.co.uk/technology/0/ransomware-does-work/>. Acesso em 12 Dez.2017. Citado na página 25.

MICRO, T. *Ransomware: O que é e como você pode se proteger?* 2015. Disponível em <http://blog.trendmicro.com.br/ransomware-o-que-e-e-como-voce-pode-se-proteger/>. Citado 5 vezes nas páginas 27, 28, 33, 34 e 38.

MICRO, T. *Ransomware*. 2016a. Disponível em : https://www.trendmicro.com/vinfo/us/security/definition/ransomware>. Acesso em 9 Dez.2017. Citado 5 vezes nas páginas 24, 25, 26, 27 e 28.

MICRO, T. *Somente em 2016, vítimas perderam US$1 bilhão para ataques ransomware*. 2017a. Disponível em :<http://blog.trendmicro.com.br/vitimas-perderam-us1-bilhao-para-ataques-ransomware/>. Acesso em 07 Fev.2018. Citado na página 57.

MICROSOFT. *O Que é um firewall?* Citado 2 vezes nas páginas 37 e 38.

MICROSOFT. *FAQ Ransomware*. 2018. Disponível em : <https://www.microsoft.com/en-us/wdsi/threats/ransomware>. Acesso em 06. Fev.2018. Citado 2 vezes nas páginas 24 e 25.

MULATINHO, C. A. *Análise das principais ameaças e ataques em segurança de computadores e como o linux e seus módulos de segurança do kernel podem ajudar a mitigá-las*. 2015. Citado 2 vezes nas páginas 31 e 32.

OLIVEIRA, L. L. R. d. *Controle de Trajetória Baseado em Visão Computacional Utilizando o Framework ROS*. Dissertação (Mestrado) — Universidade Federal de Juiz de Fora, 2013. Citado na página 32.

PEREIRA, A. S. M. *IMPACTO QUE UM RANSOMWARE PODE GERAR PARA O NEGÓCIO DE UMA EMPRESA*. Disponível em :<https://riuni.unisul.br/bitstream/handle/12345/2959/Artigo$_A maro.pdf?sequence = 1 isAllowed = y > .Acessoem 03.Fev.2018. Citadonapgina 19.$

PROCOPIO, J. *Softwares de Segurança da Informação*. 2010. Disponivel em : <http://ead.ifap.edu.br/netsys/public/livros/LIVROAcesso em 07 Set.2017. Citado 2 vezes nas páginas 22 e 35.

REPORT, S. *Ransomware como serviço dispara casos de ataques ao redor do mundo*. 2017. Disponível em:<http://www.securityreport.com.br/destaques/ransomware-como-servico-dispara-casos-de-ataques-ao-redor-do-mundo/.Wnk3YyXwbIU>. Acesso em 06 Fev.2018. Citado na página 14.

ROHR, A. *Saiba como funcionam os programas antivírus*. 2009. Disponível em :<http://g1.globo.com/Noticias/Tecnologia/0,,MUL1345991-6174,00-SAIBA+COMO+FUNCIONAM+OS+PROGRAMAS+ANTIVIRUS.html>. Acesso em 26.Fev.2018. Citado na página 36.

SARAIVA, F. *Um estudo pratico sobre segurança da informação*. 2012. Citado na página 37.

SATZIACK, A. *UMA BREVE HISTÓRIA DO RANSOMWARE*. 2017. Disponível em: <https://www.domosolucoes.com.br/uma-breve-historia-ransomware/>. Acesso em 9 Dez.2017. Citado na página 24.

SÊMOLA, M. *Gestão da Segurança da Informação: Uma visão Executiva*. [S.l.]: Elsevier, 2003. Citado na página 17.

SOLUTIONS, M. S. 2003. Disponível em <http://www.modulo.com.br/media/9a$_p esquisa_n acional.pdf$ > $.Acessoem 06 Fev.2018. Citado 2 vezes na spginas 13 e$ 14.

STALLING, W. *Criptografia e segurança de redes*. 4. ed. [S.l.]: Pearson, 2008. Citado na página 33.

STALLINGS, W. *Criptografia e segurança de redes*. 6. ed. [S.l.]: Pearson, 2014. Citado na página 17.

STATS, G. *Operating System Market Share Worldwide*. 2017. Disponível em :<http://gs.statcounter.com/>. Acesso em 30 Jan.2018. Citado na página 40.

TRENDMICRO. *Os 6 tipos mais assustadores de ransomware*. 2017. Disponível em :<https://www.arcon.com.br/blog/os-6-tipos-mais-assustadores-de-ransomware>. Acesso em 03.Fev.2018. Citado 3 vezes nas páginas 28, 29 e 30.

TUTORIAISTI. *Antivírus – Como eles atuam?* 2018. Disponível em :< http://www.tutoriaisti.com.br/antivirus-como-eles-atuam/>. Acesso em 08. Fev.2018. Citado na página 36.

VACCA, J. *Network and System Security*. 2. ed. [S.l.]: Syngress, 2013. Citado 2 vezes nas páginas 30 e 31.

VAUGHAN, E. J.; VAUGHAN, T. *Fundamentals of Risk and Insurance*. 10. ed. [S.l.: s.n.], 2008. Citado na página 32.

ZAGHETTO, C. et al. Ransomware: Este problema tambÉm pode ser seu. *Revista Tenologias em projeção*, v. 8, n. 2, p. 14, 2017. Citado na página 58.