AVALIAÇÃO DE FERRAMENTAS PARA DETECÇÃO DE *MALWARES* BUSCANDO A SEGURANÇA DE COMPUTADORES

EVALUATION OF MALWARE DECTION TOOLS FOR COMPUTER SAFETY

Jeferson de Sousa Ataides[1]

Aparecido Alves da Silva Júnior[2]

Resumo:
É de grande valia pensar na segurança de computadores. Existem ferramentas que fazem a proteção de computadores contra arquivos maliciosos, são os antivírus se tornaram ferramentas que conseguem combater outros tipos de *malwares*, mas o usuário não tem certeza se o antivírus que está utilizando ou vai adquirir realmente consegue proteger o computador contra outros tipos de *malwares*. A proposta da pesquisa foi verificar se os antivírus realmente conseguem combater outros tipos de malwares além do vírus. O objetivo do trabalho é consciencializar o leitor a utilizar ferramenta para a proteção contra *malwares*, apresentando a eficiência das ferramentas antivírus testadas contra diferentes tipos de *malwares*. Foram feitos dois testes nas ferramentas antivírus para testar a hipótese se essas ferramentas protegem o computador contra vários tipos de malwares. Os resultados mais expressivos foi o teste de vulnerabilidade, onde a ferramenta *Bitdefender* detectou 97% dos malwares e removeu o colocou para quarentena 72% dos malwares detectado, já há ferramenta *Kaspersky* detectou 100% dos malwares e 83% dos malwares detectados foram removidos ou mandados para quarentenas. O ponto positivo foi que a maioria das ferramentas testadas apresentou um bom ou razoável resultado, o ponto negativo foi a ferramenta *Norton* por não apresentar uma boa eficiência nos testes.

Palavras-chave: Arquivos Maliciosos. Anti-Malwares. Segurança de Computadores.

Abstract:
It is very useful to think about computer security, there are tools that protect computers against malicious files, antivirus has become a tool that can combat other types of malware, but the user is not sure if the antivirus they are using or will use. Purchasing can really protect your computer from other types of malware. The problem researched was, if antivirus can really combat malware other than viruses. The objective of this work is to make the reader aware of the use of malware protection tools, presenting the efficiency of antivirus tools tested against different types of malware. Two anti-virus tools were tested to test whether these tools protect your computer against various types of malware. The most significant results were vulnerability testing, Bitdefender tool detected 97% of malware and removed it quarantined 72% of detected malware, Kaspersky tool already detected 100% of malware and 83% of detected malware was removed or sent to quarantines. The plus point was that most of the tools tested had a good or reasonable result, the downside was that the Norton tool did not perform well in the tests.

Keywords: Malicious Archives. Anti-malware. Computer Security.

[1] Acadêmico de Sistemas de Informação, Universidade Estadual de Goiás Campus Posse, jeferson.ataides50@gmail.com.
[2] Graduado em Sistema de Informação, Centro Universitário Toledo e Especialista em Docência do Ensino Superior, Universidade Cândido Mendes, prof.cido.posse@hotmail.com.

1 INTRODUÇÃO

Com o avanço e o aumento da utilização da tecnologia, veio a necessidade em pensar na segurança da informação. Segundo a empresa de segurança de computadores Kaspersky, todos os anos vem aumentando os ataques de malwares em computadores, em 2018 foram infectados 30% dos computadores mundiais, no Brasil os ataques mais recorrentes são os *malwares* específicos para fraudes financeiras (KASPERSKY, 2018).

Segundo Caldas (2016, p. 6), "*malwares* são programas desenvolvidos com o intuito de se infiltrar em um sistema de computador alheio de forma ilícita, para causar danos, alterações ou roubo de informações". Eles podem aparecer de diversos formatos como *script*, programas executáveis hostis e entre outras formas.

Buscando a segurança de computadores, é fundamental a utilização de ferramentas que façam a proteção. Existem ferramentas fundamentais para proteção dos computadores, que são os *anti-malwares* e os próprios antivírus que atualmente combatem vírus e também outros tipos de arquivos maliciosos, como *spyware, ransomware, phishing, trojan* e entre outros.

Existe diferença entre antivírus e *anti-malwares*, as ferramentas antivírus tem o propósito de proteger computadores contra vírus, mas algumas conseguem proteger contra outros tipos de *malwares* segundo a suas descrições e são mais conhecidas, já os *anti-malwares* são ferramentas com o propósito de proteger o computador contra vários tipos de *malwares* mas são menos conhecidas, um exemplo de ferramenta *anti-malware* é a *Malwarebytes* é uma ferramenta gratuita, segundo o seu fabricante consegue detectar e remover vários tipos de *malwares*.

No mercado existem várias ferramentas para detectar e remover *malwares* de diversos fabricantes, porém é complicado escolher qual delas devemos utilizar, pois não se sabe de fato qual ferramenta consegue proteger o computador de ameaças de *malwares*, não se pode confiar apenas nas descrições do fabricante, mas sim na sua eficiência. Geralmente o usuário

instala um *software* pago ou gratuito que promete fazer a proteção do computador, mas como saber se essa ferramenta escolhida, está realmente fazendo a proteção contra os *malwares*?

O problema que foi pesquisado, é se as ferramentas antivírus conseguem proteger o computador de outros tipos de malwares, o *spyware,* o *ransomware,* o *phishing* e o *trojan*, além do vírus, como afirmam os seus fabricantes. Porque se as ferramentas testadas de fato conseguem proteger o computador contra outros tipos malwares, o resultado da pesquisa poderá auxiliar o leitor a escolher uma boa ferramenta, que possa de fato proteger o seu computador de vários tipos de ameaças de arquivos maliciosos.

O objetivo do artigo é apresentar para o grau de eficiência das ferramentas antivírus que foram testadas contra diferentes tipos de *malwares*, para auxiliar o leitor a escolher uma ferramenta mais adequada. Para alcançar aos resultados foram testadas quatro ferramentas de antivírus, duas pagas e duas gratuitas de diferentes fabricantes, e que segundo os seus fabricantes, conseguem proteger dispositivos contra os mesmos tipos de *malwares*.

2 MALWARES

2.1 Definição de *Malware*

Segundo o Centro de Estudo, Resposta e Treinamento de Incidentes de Segurança no Brasil, códigos maliciosos ou também conhecidos como *malwares* são programas desenvolvidos especificamente para efetuar ações maliciosas que possam danificar o computador (CERTBR, 2016). Caso o computador seja infectado com algum tipo de malware, o dispositivo poderá sofrer ações ilícitas (CERON; GRANVILLE; TAROUCO, 2009).

2.2 Classificação dos *Malwares*

Existem vários tipos *malwares*, nesse artigo foram apresentados apenas os tipos de *malwares* que foram utilizados para realização do trabalho, os tais são:

- vírus de computador pode ser um trecho de código ou um pequeno programa com a intenção de prejudicar o computador e pode de replicar (Vinod; Jaipur; Laxmi; Gaur, 2009);
- trojan ou conhecido como cavalo de troia é um programa aparentemente seguro, executa as funções normalmente dele, mas por trás são executadas também ações maliciosas servindo como porta de entrada para outros tipos de malwares (LOVISON, 2012);
- spyware é um malware considerado espião, capaz de espionar o usuário infectado para reunir informações pessoais como dados do cartão de credito e outros tipos de ataques do gênero (Vinod; Jaipur; Laxmi; Gaur, 2009);
- ransomware é um malware capaz de sequestrar arquivos valiosos e sigilosos do usuário infectado, a vítima geralmente é extorquida para conseguir os seus arquivos novamente (GAZET, 2010);
- um malware para atividades fraudulentas utilizado a internet e especifico para roubo de identidade pessoal e conta financeira dos usuários infectados (OBEROI; SARJE, 2009).

Esses são apenas alguns tipos de *malwares*, existem vários outros tipos, que de diversas formas tentam infectar computadores e redes. Foram apresentados apenas esses, por serem dos mesmos tipos que todas as ferramentas testadas prometem fazer a proteção.

3 ANTIVÍRUS

3.1 Definição de Antivírus

Antivírus são sistemas capazes de detectar, bloquear e remover arquivos maliciosos de computadores. Atualmente existem antivírus que são considerados *anti-malwares*, pois além de fazer a proteção contra vírus são capazes de detectar outros tipos de arquivos maliciosos como *spyware*, *ransomware*, *phishing*, *trojan*. Na (tabela 1) abaixo são ferramentas antivírus que foram utilizadas para passar por testes. Foram escolhidas ferramentas

pagas e gratuitas de diversos fabricantes e suas versões mais recentes, todas foram baixadas em setembro de 2019. Essas ferramentas antivírus podem ser baixadas nos sites dos seus fabricantes que estão na nota de rodapé logo abaixo, nos sites encontra-se as descrições das ferramentas, os preços das licenças caso a ferramenta seja paga.

Tabela 1 – Ferramentas antivírus.

Ferramenta	Versão
Avast Free Antivirus [3]	19.7.4674.0
Bitdefender Total Security 2020[4]	24.0.1.143
Kaspersky Total Security[5]	20.0.14.1085
Norton Security Premium[6]	22.5.2.15

Avast Free Antivirus é uma ferramenta muita conhecida por ser um sistema de antivírus gratuito, mas segundo o fabricante a ferramenta também consegue fazer a proteção contra outros tipos de *malwares*, como spyware*, ransomware, phishing, trojan* e outras ameaças em tempo real, e são mais de 400 milhões de usuários instalados em vários dispositivos *Windows*, *Mac*, *Android*. Para usuário do *Windows* os requisitos mínimos são, *Windows* 7 versão 32 e 64 *bits*, memória *RAM* 1 *GB* e 2 *GB* de memória no disco livres. Para usuário do sistema *MAC* os requisitos mínimos são, *macOS* 10.10 ou posterior com no mínimo 500 MB de memória livre de espaço em disco. Para sistema *Android* é preciso que o *smartphone* ou *tablet* possua o sistema *Google Android* 5.0 ou superior.

Bitdefender Total Security 2020 é uma ferramenta gratuita que promete segundo o seu fabricante, fazer a proteção contra vários tipos de malwares principalmente os específicos que tem o propósito de cometer fraudes na internet como *phishing*. A ferramenta pode ser instalada nas plataformas *Windows*, *Mac*, *Android* e *iOS*. Para usuários do Windows os requisitos mínimos são sistema operacional *Windows* 7, processador *Intel CORE* 2 *Duo*

[3] https://www.avast.com/pt-br.
[4] www.bitdefender.com.br/.
[5] https://www.kaspersky.com.br/total-security.
[6] https://br.norton.com/norton-antivirus.

(2 *GHz*) ou equivalente, memória *RAM* 2 *GB* e espaço no disco de 2.5 *GB* livres. Para o sistema *MAC* os requisitos são, *macOS X* 10.10 ou superior e 1 *GB* de espaço livre no disco. Para sistema Android é necessário que o sistema operacional seja na versão 4.1 ou superior. Para sistema IOS é necessário que seja na versão iOS 11.2 ou superior.

Kaspersky Total Security é uma ferramenta paga, em outubro de 2019 o valor da ferramenta é de R$129, 90 por um ano, apenas uma conta por usuário. Promete além de proteger o computador contra vírus, também fazer proteção contra outros tipos de *malwares* como *ransomware* e várias outras ameaças. A ferramenta necessita da conexão com a internet para acessar alguns recursos, para usuário do *Windows* os requisitos mínimos são, sistema operacional *Windows* 7, processador 1 *GHz*, memória *RAM* 1 *GB* se o sistema operacional for na versão 32 *bits* e 2 GB se for 64 *bits* e espaço livre no disco 1.500 *MB*. Para usuário de *tablet* é necessário que possua o sistema operacional *Microsoft Windows* 8 ou superior, processador *Intel Celeron* 1,66 *GHz* ou superior e 1 *GB* de memória *RAM*. Para o sistema *MAC* os requisitos mínimos são, o sistema operacional dever ser *macOS* 10.12 ou superior, memória *RAM* 1 GB e espaço livre de 1300 *MB*.

Norton Security Premium é uma ferramenta paga, o preço de outubro de 2019 é de R$ 150, 00 por um ano de assinatura, dez conta por usuário. Segundo a fabricante a ferramenta faz a proteção do computador contra vírus e outros tipos de *malwares*. A ferramenta pode ser instalada nas plataformas *Windows*, *Mac*, *Android* e *iOS*, com em única assinatura protege *PCs*, *MCs*, *smartphones* e *tablets*. Para o usuário do *Windows* os requisitos mínimos do sistema são, memória *RAM* 2 *GB*, o processador *Pentium* ou compatível, sistema operacional *Windows XP* todas as versões de 32 bits. Para o sistema *MAC* os requisitos mínimos são, sistema operacional *macOS* 10.10 ou posterior, com 2 *GB* de memória *RAM* e com espaço livre no disco de 300 *MB*. Para o sistema *Android* os requisitos são, sistema operacional 4.1 ou superior com espaço de armazenamento 15 *MB*. Para sistema *IOS* é necessário que a versão do sistema operacional seja *iOS* 10.14.4 ou superior.

4 TRABALHOS RELACIONADOS

Essa seção tem o propósito de apresentar artigos relacionados ao problema de pesquisa deste trabalho, com o objetivo destacar os que já foram pesquisados e resultados mais importantes obtidos. Serão citados trabalhos com relação ao problema de pesquisa deste, explicando o objetivo do mesmo e apresentado os resultados obtidos com que possam ser comparados com o deste artigo.

O trabalho dos Togni, Tomazela e Pontes (2017) desenvolveu um trabalho, com o tema, Análise de ferramentas *anti-malwares* em ambiente de simulação para testes de proteção e detecção de botnets, o objetivo do trabalho foi realizar uma avaliação de ferramentas *antimawares* gratuitas e pagas para que o usuário final consiga escolher uma boa ferramenta. As ferramentas testadas foram *Avira Antivirus Free, AVG Antivirus Free, Avast Antivirus Free, Symantec Norton Security, McAfee LiveSafe* e *Kaspersky Total Security*. O propósito do trabalho foi provar ou não se as ferramentas fazem a proteção de computadores contra *malwares* focando principalmente no *botnets* que é um tipo de arquivo malicioso. Em relação aos resultados dos testes, nota-se que duas ferramentas tiveram melhores desempenho, foram as ferramentas *Avast Antivirus Free* e a *Kaspersky Total Security*.

O trabalho dos autores Antônio, Ramos, Fonseca, Luiza, Ferreira e Rodrigues (2014), com o tema Orientações ao usuário final: Principais Malwares e como evitar a contaminação, o objetivo do trabalho foi apresentar para usuário final conceitos sobre os *malwares* e demostrar formas de combatê-los. Foram realizados testes em apenas duas ferramentas, *Kaspersky* e na *Anvira*. Os testes tiveram como propósito de saber se realmente as ferramentas eram eficientes em proteger computadores contra arquivos maliciosos. O ponto negativo do trabalho foi que os testes foram feitos em apenas duas ferramentas, diferente deste artigo os testes foram realizados em mais ferramentas de diferentes fabricantes. Os resultados da pesquisa, demostram que entre as ferramentas testadas a ferramenta *Kaspersky Total Security* teve um melhor desempenho.

O trabalho dos autores Zarpelon e Santos (2018), com o tema Implementação de Ferramentas de Segurança da Informação em Pequenas Empresas. O objetivo do trabalho foi demostrar como as pequenas empresas podem solucionar problemas de segurança da informação com o menor investimento possível. Foi realizado um estudo de caso para pesquisar ferramentas e mecanismo de segurança da informação para que possam ser sugeridas para pequenas empresas. Este presente trabalho por realizar teste em ferramentas de *anti-malwares*, buscar sugerir ferramentas que tem um bom desempenho para que possam serem usadas em pequenas empresas. Os resultados do estudo de caso, indicam ferramentas para que possam ser implementadas em pequenas empresas com baixo custo, pensando na segurança da informação, as ferramentas foram *pfSense* utilizada para configurar o *firewall* da rede de internet, *Kaspersky Total Security, Zabbix* para monitorar o servidor da empresa.

Este artigo é diferente, pois, foi criado um ambiente de teste, que foi infectado com cinco diferentes tipos de *malwares trojan*, *spyware*, vírus, *ransomware* e *phishing*, com o objetivo de mostrar o grau de eficiência das ferramentas em detectar, bloquear e remover *malwares*, para que os leitores consigam escolher uma boa ferramenta para proteger o seu computador contra diferentes tipos de arquivos maliciosos.

5 METODOLOGIA DA PESQUISA

A finalidade do trabalho foi realizar uma pesquisa básica, esse tipo de pesquisa científica tem o objetivo de aprofundar o conhecimento científico sobre o tema sem a necessidade de ser aplicado na prática. O tipo de pesquisa científica quanto aos objetivos foi adotado a pesquisa exploratória, esse tipo de pesquisa tem o objetivo de explorar o tema para que o pesquisador tenha o domínio dos fatos e fenômenos ocorridos relacionado com o problema da pesquisa encontrado (FONTELLES; FONTELLES; SIMÕES; FARIAS, 2009).

Foi pesquisados e citados trabalhos científicos referentes ao tema, com o propósito o que já tem na literatura com o intuito de aprofundar o conhecimento

sobe o tema. A partir do problema da pesquisa estudado foi explorado alguns fatos, as ferramentas antivírus conseguem detectar estes malwares *spyware, ransomware, phishing, trojan*? Caso consigam, as ferramentas conseguem remove-los? Com base nos fatos estudados foi feito uma avaliação das ferramentas para saber o grau de eficiência das mesmas.

O tipo de abordagem, para analisar os dados coletados com a pesquisa, foi o quali-quantitativa, esse tipo de abordagem, uni as abordagens qualitativa e quantitativa, ou seja, além de fazer uma análise crítica dos dados levantados, passando para o leitor uma visão crítica dos resultados obtidos com a pesquisa, também foram coletados dados numéricos, que foram analisados com instrumentos estatísticos, foram construídos gráficos e tabelas para apresentar os resultados de maneira organizada para facilitar a leitura e a compreensão.

Os procedimentos utilizados foram, o bibliográfico, onde foram citados trabalhos relacionados com o tema e com o problema pesquisado. E o estudo de caso, a onde foram testadas algumas ferramentas antivírus, se as mesmas conseguem detectar, bloquear e remover *malwares* de vários tipos. Os resultados obtidos são referentes apenas as ferramentas testadas, mas abre espaço para que outros autores possam testar outras ferramentas.

5.1 Testes nas Ferramentas Antivírus

O ambiente dos testes foi um *desktop* com o sistema operacional *Windows* 10 versão 64 *bits*, com 4 *GB* de memória *RAM*, o processador *Intel Core* i3 8100, com o *HD* de 500 *GB*. Foram criados pontos de restauração, caso o sistema operacional sobre algum tipo de dano consiga restaurá-lo para iniciar outro teste, garantindo que os testes serão feitos no mesmo ambiente.

As ferramentas foram submetidas a dois testes, o teste da EICAR e teste de vulnerabilidade. Estes testes tem o objetivo de provar ou não se as ferramentas submetidas aos testes são capazes de detectar, bloquear e remover arquivos maliciosos de formar eficaz. Os resultados foram mostrados

em forma de gráfico, que demostram a eficiência das ferramentas e uma análise crítica dos dados coletados de cada ferramenta.

O *European Institute for Computer Antivirus Reseach* (EICAR), é o Instituto Europeu de Antivírus de Computador, empresa que tem parceria com diversos fabricantes de antivírus, um dos seus objetivos, é trazer soluções para combater os arquivos maliciosos. O EICAR indica trechos de códigos e vários arquivos para download que simula arquivos maliciosos, para submeter ferramentas antivírus a testes. As amostrar dos arquivos maliciosos são atualizados regulamente, a versão utilizada neste trabalho foi a de 10 de abril de 2019.

O teste de vulnerabilidade, o ambiente de teste foi exposto a vários tipos de *malwares*, logo mais as ferramentas foram observadas, se vão fazer a proteção do computador. Os tipos de *malwares* utilizados são spyware*, ransomware, phishing, trojan*. Para os testes com *ransomware* será utilizado a ferramenta *KnowBe4 Ransomware Simulator*, é uma ferramenta que simula vários arquivos maliciosos do tipo *ransomware*.

6 RESULTADOS DOS TESTES

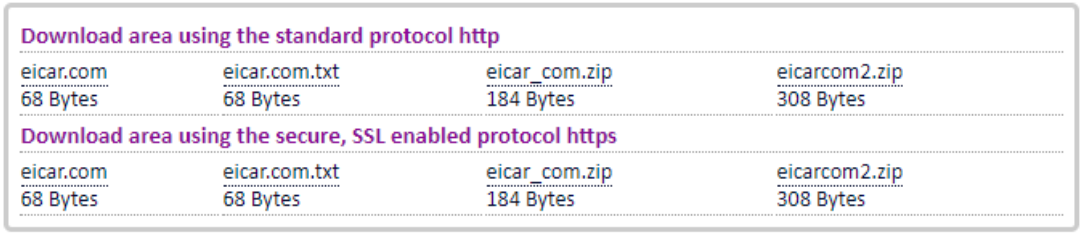
6.1 Teste EICAR

O primeiro teste foi o EICAR, as ferramentas foram submetidas à um trecho de código que simula um vírus. Esse trecho de código foi escrito em um bloco de notas e salvo com um nome qualquer e com a extensão *.exe*, também foram feitos *downloads* de arquivos com esse mesmo trecho de código, mas com outros tipos de extensões. A hipótese é se a ferramenta conseguir bloquear imediatamente estes arquivos ou remove-los está aprovada, caso contrário a ferramenta não passa no teste. O (quadro 1) logo abaixo mostra as ferramentas testadas, o tipo de teste, o código do vírus. E a (figura 1) são os arquivos de download de todas os tipos de extensão que foram utilizados nos testes. Todos os arquivos de downloads e o trecho de código foram disponibilizados no site do EICAR no mês de abril do ano de 2019.

Quadro 1 – Teste EICAR nas ferramentas antivírus.

Ferramentas	**Teste**	**Código do Vírus**
Avast Free Antivirus; *Bitdefender Total Security 2020;* *Kaspersky Total Security;* *Norton Security Premium.*	EICAR	X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Figura 1 – Teste EICAR arquivos de download.



A ferramenta *Avast Free Antivirus*, conseguiu bloquear os arquivos imediatamente, e não deixou o arquivo de teste ser salvo no computador. O tempo gasto para bloquear os arquivos foi de menos de 2 segundos, foi um tempo considerado bom, a ferramenta fez uma avaliação da gravidade da ameaça de nível 1 até o nível 3, o teste foi avaliado pela a ferramenta como nível 1. Nesse primeiro teste a ferramenta demostrou eficiente, e foi considerada aprovada no teste.

A ferramenta *Bitdefender Total Security* 2020, impediu o arquivo de teste do vírus ser salvo no computador e excluiu imediatamente o arquivo que foi considerado malicioso. A outra metade do teste a dos downloads, eles foram bloqueados, a ferramenta não deixou o navegador baixar. Neste teste a ferramenta demostrou eficiência, protegeu o computador de ameaça de vírus e foi considerada aprovada no teste.

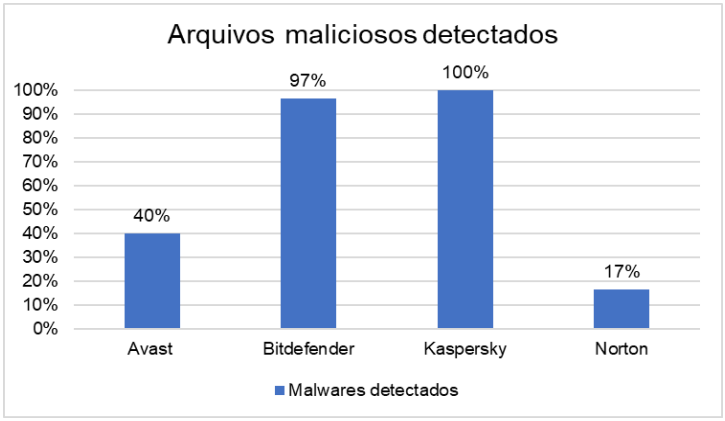
A ferramenta *Kaspersky Total Security*, não impediu o arquivo de teste do vírus ser salvo no computador, mas todos os *downloads* dos arquivos dos vírus feitos foram bloqueados imediatamente, não deixou o navegador prosseguir com os *downloads*. Neste teste, a ferramenta não impediu que a simulação do vírus de ser salvo no computador, então não teve uma boa eficiência mesmo bloqueando todos os downloads de arquivos de simulação de vírus.

A ferramenta *Norton Security Premium* conseguiu impedir que o arquivo de teste de vírus fosse salvo no computador, a ferramenta detectou, bloqueou e removeu o arquivo considerado malicioso imediatamente. Mas a outra metade do teste, que são as tentativas de downloads de arquivos maliciosos, a ferramenta falhou, não impediu que os arquivos de fossem baixados. Neste teste a ferramenta não teve um bom desempenho e foi considera reprovada no teste.

6.2 Teste Vulnerabilidade

O teste de vulnerabilidade, o ambiente de teste foi infectado com um total de 30 malwares de diversos tipos, spyware*, ransomware, phishing* e *trojan*. O *ransomware* teve o maior número de arquivos de teste foram 18, foi utilizando uma ferramenta chamada *KnowBe4 Ransomware Simulator* para simular os arquivos maliciosos, o *spyware* teve 2 arquivos de teste, o *phishing* foram testadas 4 páginas da web que portam esse tipo de malware e *trojan* foram 6 arquivos de teste.

Figura 2 – Gráfico de *malwares* detectados pelas ferramentas.



A (figura 2) é o gráfico que demonstra a quantidade de *malwares* detectados pelas ferramentas. A ferramenta *Avast* detectou 12 de 30 *malwares* na (figura 3) mostra o resultado, é o equivale 40% dos *malwares* foram detectados pela ferramenta. A ferramenta *Bitdefender* detectou 29 *malwares*, a (figura 4) mostra o resultado, ou seja, a ferramenta detectou 97% dos *malwares* de teste. A ferramenta *Kaspersky* detectou 30 *malwares* a (figura 5) mostra o

resultado, 100% dos *malwares* foram detectados. A ferramenta *Norton* detectou 5 *malwares* a (figura 6) mostra o resultado, o que equivale apena 17% dos *malwares* foram detectados.

Figura 2 – Resultado do escaneamento completo da ferramenta *Avast*.

Figura 3 – Resultado do escaneamento completo da ferramenta *Bitdefender*.

Figura 4 – Resultado do escaneamento completo da ferramenta *Kaspersky*.

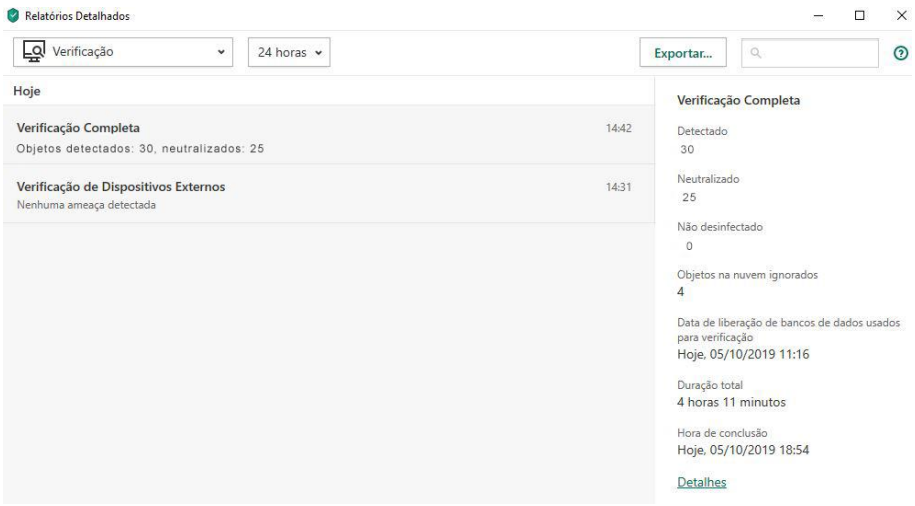


Figura 5 – Resultado do escaneamento completo da ferramenta *Norton*.

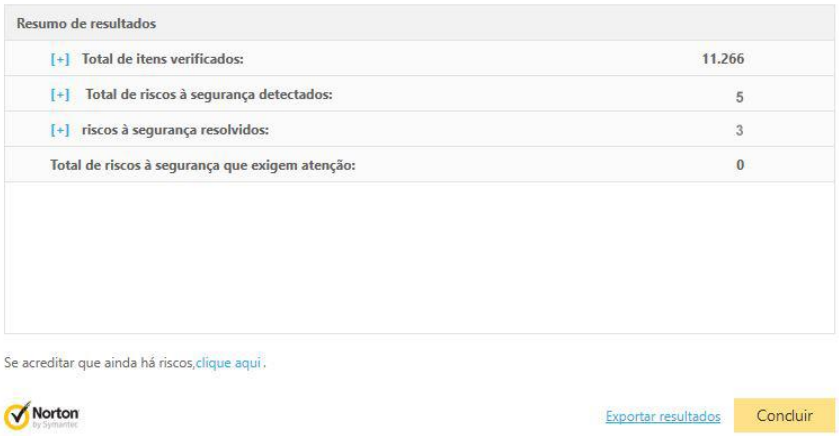
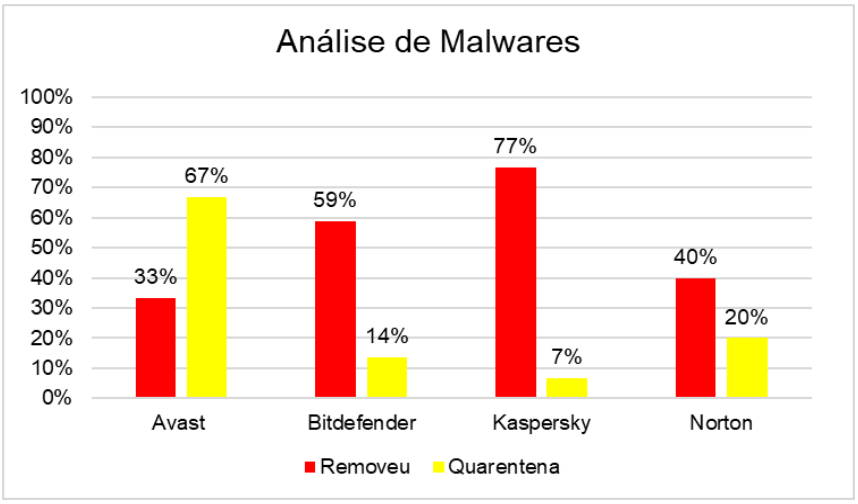


Figura 6 – Gráfico de *malwares* detectados que foram removidos ou enviados para quarentena.



A (figura 6) é um gráfico que demonstra dos *malwares* detectados quantos foram removidos e quantos foram para quarentena. A ferramenta *Avast* detectou 12 *malwares*, 4 foram removidos e 8 levados para quarentena, ou seja, 33% foram removidos e 67% levados para quarentena. A ferramenta *Bitdefender* detectou 29 *malwares*, 17 foram removidos e 4 levados para quarentena, ou seja, 59% foram removidos e 14% levados para quarentena. *Kaspersky* detectou 30 *malwares*, 23 foram removidos e 2 levados para quarentena, ou seja, 77% foram removidos e 7% enviados para quarentena. A ferramenta *Norton* detectou 5 *malwares*, 2 foram removidos e 1 levado para quarentena, ou seja, 40% foram removidos e 20% enviados para quarentena.

Quadro 2 – *Malwares* não detectados pelas ferramentas.

Ferramenta	***Trojan***	***Ransomware***	***Spyware***	***Phishing***
Avast	3	15	-	-
Bitdefender	1	-	-	-
Kaspersky	-	-	-	-
Norton	3	18	2	2

No (quadro 2) mostra a quantidade e quais malwares que não foram detectados por cada ferramenta. A ferramenta *Avast* não detectou 18 *malwares*, 3 *trojans* e 15 *ransomwares*. A ferramenta *Bitdefender* não detectou 1 *malware*, 1 *trojan*. A ferramenta *Kaspersky* detectou todos os *malwares*. A ferramenta *Norton* não detectou 25 *malwares*, 3 *trojans*, 18 *ransomwares*, 2 *spywares* e 2 *phishing*.

7 CONSIDERAÇÕES FINAIS

O objetivo deste artigo foi apresentar para o leitor a eficiência de alguns antivírus contra *malwares*, e assim auxiliar a escolher uma ferramenta que possa realmente proteger o computador contra arquivos maliciosos de vários tipos. Para alcançar esse objetivo foram feitos teste em quatro ferramentas antivírus de distintas fabricantes, pelas descrições das ferramentas prometem proteger dispositivos contra os mesmos tipos *malwares*.

Os resultados foram que uma ferramenta teve um melhor desempenho comparado com as demais, a ferramenta *Kaspersky Total Security*, ela é uma ferramenta paga e se mostrou eficiente nos testes que foram aplicados nela. Logo em seguida com um desempenho razoável a ferramenta *Bitdefender Total Security 2020* que é uma ferramenta paga, teve uma eficiência aceitável. A ferramenta *Avast Free Antivirus*, por ser uma ferramenta gratuita apresentou uma eficiência aceitável principalmente no teste do EICAR.

Para trabalhos futuros, podem passar pelos mesmos teste outras ferramentas, para que possam ser comprovadas ou não a eficiência em combater *malwares* buscando a segurança de computadores. Antes de adquirir um produto é sempre importante saber da sua procedência, escolher uma bom

antivírus não foge disso, é importante saber se ele realmente estar protegendo o computador.

REFERÊNCIAS

ANTÔNIO, Luciano; RAMOS, Jonathan; FONSECA, Bernardo; LUIZA, Ana; FERREIRA, Wagner; RODRIGUES, Igor. Orientações ao usuário final: Principais Malwares e como evitar a contaminação. Centro Universitário de Belo Horizonte (UNI-BH), Belo Horizonte, MG, p. 1-12, 10 outubro de 2014.

CALDAS, D. M. Análise e Extração de Características Estruturais e Comportamentais para Perfis de Malware. Dissertação de Mestrado, Publicação PPGENE.DM - 622 A/16, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 2016. 82p.

CENTRO DE ESTUDO, RESPOSTA E TREINAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (Brasil). Cartilha de Segurança para Internet. 4. ed. [S. l.]: CERT.br, 16 março 2017. Disponível em: https://cartilha.cert.br/malware/. Acesso em: 15 agosto de 2019.

CERON, Joao M.; GRANVILLE, Lisandro; TAROUCO, Liane. Taxonomia de Malwares: Uma Avaliação dos Malwares Automaticamente Propagados na Rede. 2009.

FONTELLES, Mauro José; SIMÕES, Marilda Garcia; FARIAS, Samantha Hasegawa; FONTELLES, Renata Garcia Simões. Metodologia da pesquisa científica: diretrizes para a elaboração de um protocolo de pesquisa. **Revista Paraense de Medicina**, v. 23, n. 3, p. 1-8, 2009.

GAZET, Alexandre. Análise comparativa de vários ransomware virii. **Revista em virologia de computadores**, v. 6, n. 1, p. 77-90, 2010

KASPERSKY (Brasil). **Kaspersky daily**: Kaspersky detecta 350 mil novos vírus por dia em 2018. Brasil: Renato Rodriguês, 6 dezembro 2018. Disponível em: https://www.kaspersky.com.br/blog/kaspersky-detecta-novos-virus-dia-2018/11143/. Acesso em: 5 agosto de 2019.

LOVISON, Henrique Dalla Costa. Uma metodologia de análise de programas daninhos. Instituto de informática, Universidade Federal do Rio Grande do Sul, Porto Alegre, RS, 2012. p. 13.

OBEROI, Kapil; SARJE, Anil K. An Anti-Phishing Application for the End User. **Hack. in 2009**, p. 17, 2009.

TOGNI, Jimi; MARIA DAS GRAÇAS, J. M.; PONTES, Aldo. Análise de ferramentas antimalware em ambiente de simulação para testes de proteção e detecção de botnets. **Reverte-Revista de Estudos e Reflexões Tecnológicas da Faculdade de Indaiatuba**, n. 15, 2017.

VINOD, P., JAIPUR, R., LAXMI, V., & GAUR, M. Survey on malware detection methods. In: **Proceedings of the 3rd Hackers' Workshop on computer and internet security (IITKHACK'09)**. 2009. p. 74-79.

ZARPELON, Felipe Schloser; SANTOS, Matheus Incocencio dos. **Implementação de ferramentas de segurança da informação em pequenas empresas**. 2018. Trabalho de Conclusão de Curso. Universidade Tecnológica Federal do Paraná.