Estudo Sobre Utilização e Eficiência de Antivirus

Tiago Alves[1], **Eduardo Maroñas Monks**[1], **Carlos Vinicius Alves**[1]

[1]Redes de Computadores – Faculdade de Tecnologia Senac Pelotas (FATEC)
Caixa Postal – 96015560 – Pelotas – RS – Brasil

tiago.a001@hotmail.com,emmonks@gmail.com,cvalves@senacrs.edu.br

Resumo. *Este artigo tem como objetivo analisar a utilização de antivírus corporativos e de uso doméstico, comparando a eficiência das ferramentas por meio de métodos de infecção de hosts e arquivos contaminados com malware.*

Abstract. *This article aims to analyze the use of corporate antivirus and household, comparing the efficiency of the tools by hosts infection methods and files infected with malware.*

1. Introdução

Toda vez em que há troca de dados em uma empresa como, por exemplo, transações bancárias e-mail é necessário proteger esses dados como também os computadores que são utilizados. Hoje há diversos tipos de malwares com capacidade de roubar os dados dos usuários. Como existem diversos malwares para combates também existem ferramentas para combater esses malwares, uma dessas ferramentas é o Antivírus que em muitas vezes são pagos em ambientes corporativos, sendo utilizados em casa, mas não tendo no final um bom resultado. Estes antivírus estão disponíveis por um período pequeno para teste e após este período acaba desabilitando alguns recursos, como a atualização da base de dados. Este trabalho tem como objetivo demonstrar a capacidade de alguns antivírus e comparar as diferenças ente eles e suas distribuições gratuitas, analisando por meio de testes a eficiência de dois antivírus bastante utilizados, o AVG e o AVAST, nas versões corporativas e gratuitas.

2. Antivírus

As ferramentas de antivírus têm como objetivo evitar que os vírus sejam executados nos sistemas operacionais dos hosts, a princípio o vírus é um programa como qualquer outro, sendo de código nativo aos sistemas operacionais e respectivos aplicativos. Os vírus são arquivos executáveis, ou seja, assim que são executados em um computador ficam ativos e se replicam no sistema, dessa forma infectam a máquina em questão. O vírus tem como objetivo alterar, corromper ou até mesmo destruir informações que estão armazenadas em um disco rígido de um computador.

2.1. O que e Antivírus

São softwares desenvolvidos para identificar e eliminar os malwares, atualmente existe no mercado diferentes produtos com grandes marcas, devido a diversas formas de infecção, assim, os antivírus se diferenciam na forma de detecção¸ funcionalidades e preço final.

2.2. Origem

Conforme [Inforquali 2012], o vírus teve origem na década de 80 devido a vários fatores um deles era o disquete. Na época os programas eram pequenos, muitos computadores não possuíam disco rígido sendo através desse sistema, quando o computador carregava o sistema operacional através dos disquetes. Assim sendo o vírus se apropriava dessa vulnerabilidade e se multiplicava

2.3. Formas de Infecção

Conforme [Serrano 2014], para que um computador seja infectado, é necessário uma forma de transmissão, alguns exemplos para infecção, são:

2.3.1. Diquete

Uma forma de infecção muito comum no inicio da década de 80, o vírus era gravado em um disquete e assim sendo executado em máquinas que posteriormente seriam utilizadas por pessoas, assim, se infectara com o vírus que já está na máquina fazendo com que se espalhe novamente para outras máquinas.

2.3.2. E-mail

Uma das formas mais utilizadas hoje em dia, ao abrir uma mensagem que contenha anexos isso claro tendo que muitas vezes baixar esse arquivo para o computador e executá-los para visualizar como fotos ou descompactar os mesmo, ao executar esses arquivos se inicia o processo de execução do vírus.

As instruções desses vírus e de auto copiar pra o disco rígido, buscando listas de endereço eletrônicos ou se auto enviar para os contatos do usuário.

2.3.3. Páginas web

Acessando uma página na internet, o usuário que não tem um domínio da parte de segurança ou muitas vezes uma pessoa idosa acaba clicando em um banner ou links que o próprio site disponibiliza, fazendo com que este usuário seja direcionado para uma página instalando *spyware* em seu computador. Alguns tipos de *spyware* registram as teclas pressionadas e as informações digitadas em sites ou programas e assim utilizam estas informações para anúncios dirigidos ou roubo de senhas, este programa pode ser instalado em computadores de diversas formas, mas, geralmente estão ocultos em outros softwares, jogos e protetores de tela baixados da internet.

3. Funcionamento dos Antivírus

Os antivírus tiveram que se adequarem conforme os vírus foram evoluindo, para isso, foram criadas diversas funcionalidades para detecção e proteção de hosts. As funcionalidades mais comuns encontradas nos antivírus atuais são o escaneamento de arquivos e checagem de integridade.

3.1. Escaneamento

E o método de varredura de todo disco rígido do computador em busca de qualquer tipo de vírus. O escaneamento e o método mais utilizado por qualquer tipo de antivírus sendo ele pago ou gratuito.

3.2. Checagem de Integridade

Conforme [webgroove 2014], é utilizado para detectar se há algum arquivo do computador contaminado, criando um banco de dados do próprio antivírus, assim quando o usuário solicitar uma verificação de segurança esse banco é verificado com base no histórico presente, e se encontrar algum desses arquivos com alteração o antivírus irá sinalizar o problema para o usuário.

4. Estudo de caso sobre antivírus

Para fundamentar o estudo de antivírus, foram testados neste projeto as versões corporativas e versões freeware de dois antivírus muito utilizados no mercado.

4.1. Ambiente

Para esse estudo sobre antivírus, foram criados ambientes virtuais, para isso foi utilizado o software VMware Workstation 10.0.1 e utilizados os sistemas operacionais Windows XP Professional e Windows Server 2003 Enterprise Edition SP2, onde foram montados os servidores de vírus escolhidos.

4.2. Antivírus usados

Para este estudo foram utilizados dois antivírus corporativos e suas versões freeware, estes antivírus foram selecionados por serem mais usados no mercado e de fácil uso mediante seus usuários, são eles: AVG Internet Security 2015, AVG Antivírus 2015, Avast Free antivírus e Avast Internet Security 2015.

4.3. História sobre Avast

Conforme [Avast 2014], ”em 1988 A primeira ferramenta contra o Vienna Vírus, Pavel Baudis um pesquisador no Instituto de Pesquisas de Máquinas Matemáticas de Praga, encontrou uma amostra do Vienna Virus e, intrigado por isto, escreveu um programa capaz de remove-lo. Ele então o mostra ao seu colega Eduard Kucera e, juntos, começam a cooperativa ALWIL Software, que lança o seu primeiro Avast antivírus. Por causa do regime opressivo, não lhes foi possível formar uma empresa naquele momento.

Em 1991 os fundadores Pavel Baudis e Eduard Kucera, livres das restrições sócio-econômicas do antigo regime, transformam finalmente a ALWIL Software de uma ’cooperativa’ em uma empresa de parceria conjunta.

Em 1995 um jovem universitário, Ondrej Vlcek (atualmente o CTO da Avast) se junta a ALWIL. Ele cria o primeiro programa antivírus para a Windows 95.

Em 1997 a ALWIL Software fornece o programa (+ o motor de escaneamento) do Avast antivírus para a McAfee, que o licencia para o uso na sua própria linha de produtos, McAfee antivírus, - provando a eficácia das tecnologias do Avast anti-vírus colocando

nas caixas do seu McAfee VirusScan a logomarca ”Capacitados pela tecnologia Avast”. E também, ALWIL contrata o seu primeiro especialista em suporte técnico, Pavel Mourek.

Em 2001 é lançado o Avast Free Antivirus o Co-fundador Eduard Kucera implementa uma estratégia inovativa de comunidade de usuários baseada no princípio de que todos usuários de computador tem direito a uma proteção contra ameaças prejudiciais, e que a segurança dos computadores não deveria ser um luxo que alguns não podem pagar. Então, em primeiro de Junho, a ALWIL Software lança uma solução não comercial para usuários domésticos, o 'free antivirus'. Seis meses depois (Janeiro de 2002), um novo sistema de registro presencia o primeiríssimo usuário a se registrar no Avast free antivirus, Home Edition.

Em 2005 o Avast se alia-se a SanDisk, como uma grande maneira para a Avast alcançar novos usuários nos tempos em que a internet não tinha tanta penetração, a ALWIL começou a sua cooperação com a SanDisk. Graças a essa parceria, a Avast precisa de localização (tradução) para todos os mercados da SanDisk. Portanto, ALWIL contrata o seu primeiro time interno para localização (tradução) e suporte - este é o primeiro passo para a Avast tornar-se um sucesso internacional em termos de idiomas com suporte. Lançamento de novos produtos: Avast U3 Edition e Avast 4.6.

Em 2010 o Avast Uniu-se a Summit Partners, a Summit Partners investiu US100 milhões (100 milhões de dólares) para uma participação minoritária na companhia, confirmando a posição única da Avast no mercado global.”A ALWIL Software muda seu nome para AVAST Software, para alinhar mais de perto a companhia com a marca, e Avast alcança 130 milhões de usuários registrados. Lançamento de novos produtos: Avast serie 5.0, com um novo programa antivírus e uma Silent Firewall (silenciosa) opcional e virtualização Sandbox”.

4.4. História sobre AVG

Conforme [AVG 2009] ”em 1991, quando Jan Gritzbach e Tomas Hofer, fundaram a empresa Girosft, na cidade de Brno na República Checa. O primeiro produto da nova empresa foi o antivírus AVG (abreviação de Anti-Virus Guard), lançado em 1992 no mercado local. Em 1997, as primeiras licenças do AVG foram vendidas na Alemanha e no Reino Unido e, em 1998, o AVG foi lançado nos Estados Unidos. Logo em seguida a GRISOFT iniciou a construção de uma rede internacional de distribuidores e revendedores, para fornecer seus serviços mundialmente.

Em 1999, a empresa resolveu adotar uma estratégia ousada que mudaria seu furuto: fornecer de graça o antivírus para tornar-se popular mundialmente. Com este lema, um dos fundadores da AVG, Jan Gritzbach, decidiu que preferiria dar o software a ficar para sempre desconhecido e, por conseqüência, não vender nada. O que alguns gurus poderiam taxar como loucura, de fato, funcionou. A empresa viu seu número de usuários aumentar extraordinariamente ano a ano. A marca ganhou visibilidade e, de quebra, o tão sonhado faturamento. Em 2001, Jan Gritzbach decidiu vender a empresa para o fundo de investimento Benson Oak Capital Acquisitions (com sede na República Theca). Quatro anos depois, o Benson Oak valorizou seu investimento, vendendo 65% da empresa para a Intel Capital e Enterprise Investors (fundo de private equity com sede na Polônia) por US$ 52 milhões.

Desde 2003, a linha de produtos AVG está presente no mercado brasileiro, abran-

gendo as linhas de varejo e corporativas. Seguindo o crescimento de spywares e outros e programas potencialmente indesejáveis, a empresa incluiu um produto anti-spyware no seu portfólio, depois de adquirir, em maio de 2006, a empresa alemã Ewido Networks e integrar o Ewido anti-spyware ao seu portfólio como AVG Anti-Malware. No final de 2007, a AVG incorporou a tecnologia LinkScanner para proteger mais de 60 milhões de usuários da sua suíte antivírus contra sites web com código malicioso e downloads que possam explorar falhas nos computadores dos usuários.

Em fevereiro de 2008, AVG Technologies tornou-se o novo nome da Grisoft, seguindo a estratégia de marca global definida pela empresa. Pouco depois, no dia 27 desse mês, a empresa anunciou o lançamento da versão 8.0 do antivírus, um a nova versão single-user da sua principal solução e plataforma de segurança para Internet para usuários finais, pequenas e médias empresas e usuários corporativos. O novo AVG 8.0 trazia mais de uma dezena de novos recursos e ferramentas de segurança aperfeiçoadas que permitiam uma capacidade excepcional de detecção de ameaças, melhor usabilidade e maior eficácia no exame do sistema operacional e arquivos seja em computadores isolados ou em redes. O último lançamento da AVG, anunciado em 2 de março de 2009, foi versão 8.5 de sua família de produtos de segurança. Desenvolvido com tecnologia da empresa recém-adquirida Sana Security, o ponto alto é evitar o roubo de informações (como senhas, dados bancários e números de cartão de crédito de proteção de identidade). Uma década depois de o fundador da AVG optar por oferecer o antivírus de graça empresa alcançou faturamento de US 85 milhões. Atualmente, empregando alguns dos melhores experts (vários deles com título de PhD) do mundo em desenvolvimento de software, detecção e prevenção de ameaças e análise de riscos, a AVG posiciona-se de forma única como líder em inovação no mercado. Esta empresa, com sede na pequena cidade de Brno, localizada cerca de duas horas e meia da capital Praga, e que ocupa apenas alguns andares de dois prédios comerciais, continua a investir em P&D, fazendo parceria com as principais universidades para manter a técnologia de ponta".

5. Testes Realizados

5.1. Avast corporativo / AVG corporativo

Foi montado primeiramente os servidores onde seriam hospedados os antivírus Avast Internet Security 2015 e AVG Internet Security 2015, ambos corporativos com as configurações iguais, ambas com 10 GiGA de HD, 1 GIGA de RAM. Foram feitas redes internas para cada servidor para manter um mesmo padrão simulando uma empresa corporativa, conforme Figura 1. Logo após foram criados dois hosts clientes em computadores XP Professional conforme Figura 1, com HD 10 GIGA e memória RAM de 1 GIGA, ambos iguais para não ter diferença nas análises.

5.2. Instalação dos Antivírus

No Avast Corporativo foi feita a instalação a partir de uma prática de laboratório, disponível no [Mussum 2014], onde foi criado um servidor para múltiplos clientes. No servidor Avast corporativo tem uma diferença comparada com o AVG corporativo, o Avast corporativo tem duas formas de ser instalado nos host cliente, uma delas é através de um link disponibilizado pelo servidor para ser instalado por um técnico de forma manual e outra é por descoberta por host no próprio servidor conforme a Figura 2, Já o AVG corporativo não foi encontrado um modo de ser instalado por meio automático apenas manual.

Figura 1. Rede configurada

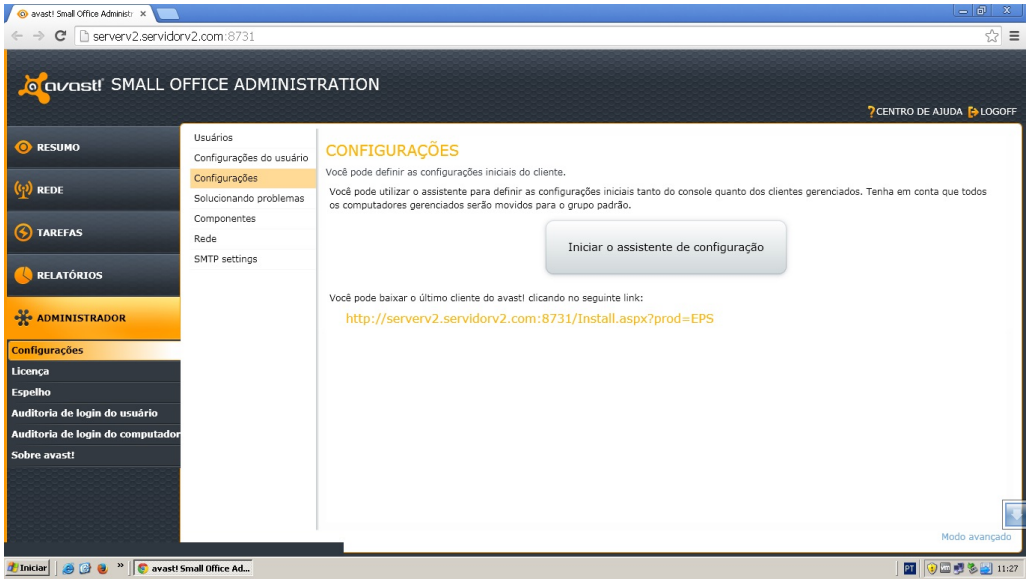

Figura 2. Ativacão do Avast para os clientes

No host, após ser configurada a rede interna do servidor, foi feita a instalação pelo modo manual por ser mais rápida. No AVG corporativo foi feita a instalação a partir do link disponível no [AvgBrasil 2014] , deverá ser feito um cadastro pessoal, para que possa ser baixado o antivírus, assim que for feito o cadastro seria enviado para o e-mail cadastrado uma chave, que seria solicitada mediante a instalação do produto, para isso antes deveria ser selecionado a quantidade de máquinas que serão utilizadas.

5.3. Testes feitos com os Hosts

Para os testes, foi realizado dois tipos de teste, onde o primeiro foi feito com arquivos infectados e o segundo por páginas web infectadas, para o teste com arquivos foi utilizado uma ISO disponível no [ISOVirus 2014]. Essa ISO contém diversos arquivos infectados onde estão compactados assim não podendo infectar a máquina hospedeira das máquinas virtuais onde seria feito os testes, não é aconselhável abrir esses arquivos em um com-

putador físico mediante o risco de danificar o sistema operacional e possível perda de arquivos. Para os testes foram selecionados dois tipos de arquivos infectados, os Arquivos PDF e Arquivos Jar, foram selecionados esses dois arquivos devido a quantidade, já que ambos eram o de maior quantidade e seria apropriado para as análises, nos hosts foram colocados os arquivos em pastas e foi feito um escaneamento de todos arquivos dentro desta pasta, assim sendo para obter os resultados no final dos escaneamentos, para as páginas Web foi feita a seleção dos sites disponíveis em listagem de sites infectados, onde esses links são atualizados diariamente assim disponível no [support.clean 2014], Foi utilizado o navegador Firefox versão 3.6, não foi feita a atualização do navegador para verificar o desempenho e o comportamento do mesmo para ingressar nos sites, para o teste foram selecionados 100 sites e foram abertos os navegadores dos hosts onde foram instalados os antivírus corporativos e Freeware. Simultaneamente, foram feitos quatro análises, pois para os sites não estava sendo analisado o processamento e sim a capacidade de reconhecer e bloquear os sites infectados, dessa forma os sites foram verificados um por um.

Para os testes de arquivos, foram selecionadas as pastas com maior quantidade de arquivos infectados, os arquivos em PDF com 191 arquivos e arquivos em Jar com 3708 arquivos e para o teste de web foi utilizado site que disponibiliza links de sites infectados, para o teste foi verificado 100 sites.

6. Resultados

Para o teste dos antivírus foi feita análise comparativa entre as versões corporativas e as versões freeware, para estes testes levou-se em conta a quantidade de arquivos que foram identificados com vírus, tempo que levou para análise dos arquivos escaneados, consumo de memória usado no processamento dos antivírus e sites identificados com vírus.

6.1. Testes com Arquivos PDF

PPara os testes realizados com arquivos PDF foi feito um escaneamento com as versões Avast corporativo, Avast Freeware, AVG Corporativo e AVG Freeware. Foi utilizado os Hosts com Windows XP básico, após ser instalado os antivírus nos hosts foram selecionado os arquivos PDF e escaneados, dos 191 arquivos PDF que continha dentro da pasta onde foram descompactados, foi verificado que nenhum dos antivírus detectou todos arquivos como infectados, mas conforme a Figura 3 demonstra que de 191 arquivos PDF escaneados, o Avast corporativo conseguiu detectar 149 arquivos, AVAST Freeware 126 arquivos, AVG Corporativo 124 arquivos e AVG Freeware detectou 116 arquivos, assim demonstrando que o Avast Corporativo e o Freeware conseguiram detectar mais arquivos infectados do que o AVG Corporativo e AVG Freeware

6.2. Testes com Arquivos Jar

Testes com Arquivos Jar Da mesma forma que o arquivo PDF, o Arquivo Jar foi selecionado e escaneados com os antivírus AVAST e AVG corporativos e Freewares, foram selecionados os arquivos Jar e escaneados, dos 3708 arquivos Jar que continha dentro da pasta onde foi descompactadas, foram verificados que também não obteve 100% de detecção dos antivírus, dos 3708 arquivos que foram escaneados pelos antivírus o AVAST corporativo conseguiu detectar 1367 arquivos Jar, o AVAST Freeware 1260 arquivos Jar,

Figura 3. Arquivos PDF

AVG Corporativo 1367 e AVG freeware obteve 1115 arquivos Jar detectados, assim demonstrando que suas versões corporativa de ambos antivírus obtiveram o mesmo número de arquivos detectados já as versões Freeware o AVAST detectou mais arquivos do que o AVG freeware conforme a Figura 4.

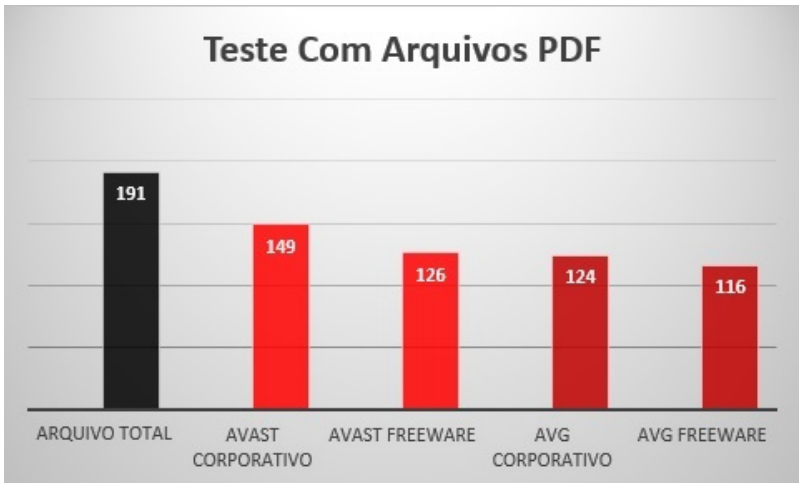

Figura 4. Arquivos PDF

6.3. Teste de Tempo de Escaneamento PDF

Para o teste de escaneamento dos arquivos PDF foi feita de acordo como tempo que os antivírus AVAST e AVG corporativos e suas versões Freeware levaram para escanear todos os arquivos PDF, foram analisados 191 arquivos PDF os mesmos arquivos para que não ocorrer alterações no resultado final. O AVAST Corporativo teve o maior tempo seguido da sua versão Freeware, para escanear 191 arquivos, o AVAST Corporativo levou 7 segundos, o AVAST Freeware levou 4 segundos, já o Antivírus AVG Corporativo e Freeware obtiveram 1 segundo cada, mesmo o AVAST corporativo tendo o maior tempo o mesmo foi o que mais detectou arquivos PDF infectados conforme a Figura 5, dos arquivos pdf detectados.

Figura 5. Arquivos PDF

6.4. Teste de Tempo de Escaneamento Jar

Para obter o tempo de escaneamento dos arquivos Jar, foi feito da mesma forma que os arquivos pdf. Foi feito um escaneamento de todos arquivos Jar, onde foram analisados 3708 arquivos Jar, estes 3708 arquivos o AVAST Corporativo levou 11 segundos, AVAST Freeware levou 10 segundos e AVG corporativo e freeware obtiveram o mesmo tempo 18 segundos cada um conforme a Figura 6.

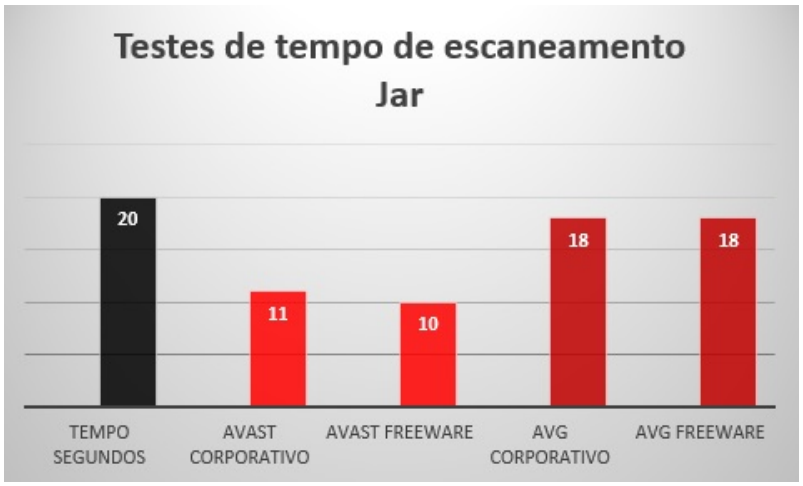

Figura 6. Arquivos PDF

6.5. Teste de Processamento PDF

Para os teste de consumo de memória utilizada, foi levado em conta o quando cada antivírus consumia de memória ao escanear arquivos PDF, para o teste foi verificado 191 arquivos PDF, como resultado o AVAST corporativo teve o maior consumo de memória chegando em média 36% e os demais antivírus se mantiveram 30% conforme a Figura 7.

6.6. Teste de processamento Jar

Para o teste de consumo de memória utilizada, foi levado em conta o quanto cada antivírus consumia de memória ao escanear arquivos Jar. Para o teste foram verificados 3708 arqui-

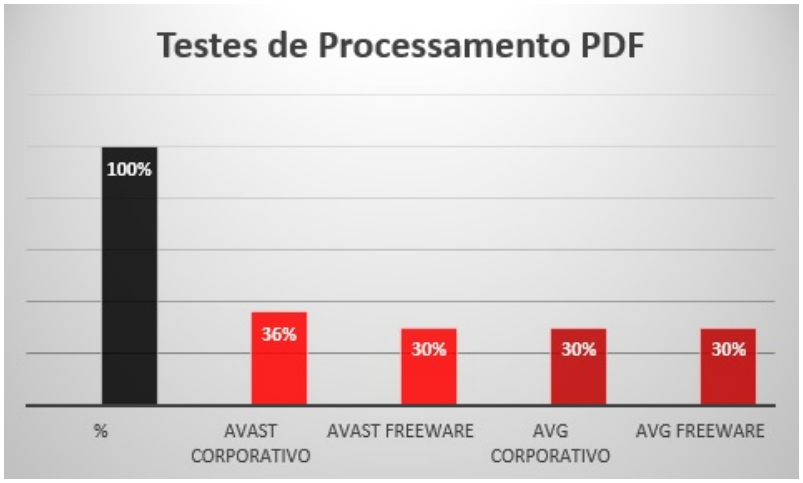

Figura 7. Arquivos PDF

vos Jar, como resultado o AVAST Corporativo e AVAST Freeware obtiveram maior processamento do que AVG corporativo e Freeware, AVAST Corporativo teve 80%, AVAST Freeware obteve 85%, AVG Corporativo e Freeware se mantiveram nos 60%, conforme Figura 8.

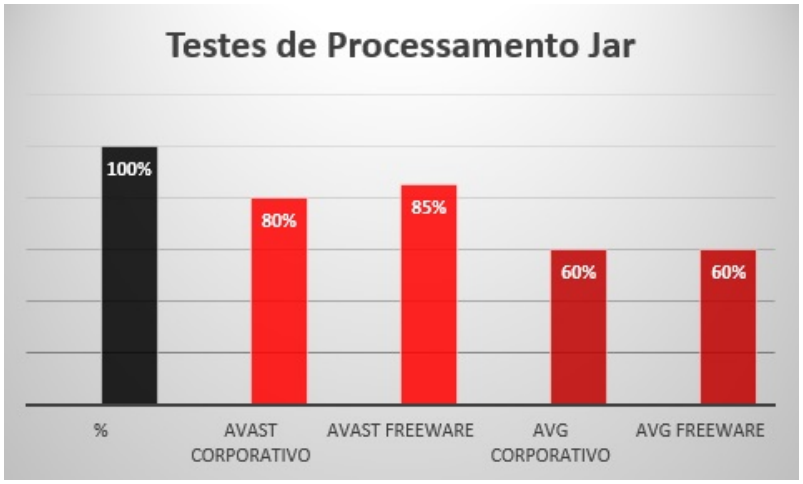

Figura 8. Arquivos PDF

6.7. Sites infectados

conforme e mostrado na Figura 9, o comportamento dos antivírus em sites infectados, foi verificado no total 100 sites para todos os antivírus. Os testes foram feitos ao mesmo tempo para que não houvesse problemas de sites fora do ar, após isso os resultados foram AVAST corporativo 95 detectados de 100, AVAST Freeware 94 detectados de 100 , AVG Corporativo 90 detectados de 100 e AVG Freeware 90 detectado de 100.

7. Conclusões

Baseando-se nos testes realizados, chegou-se a conclusão que o antivírus AVAST corporativo é superior em todos os aspectos em relação ao AVG, embora o AVG tenha seus

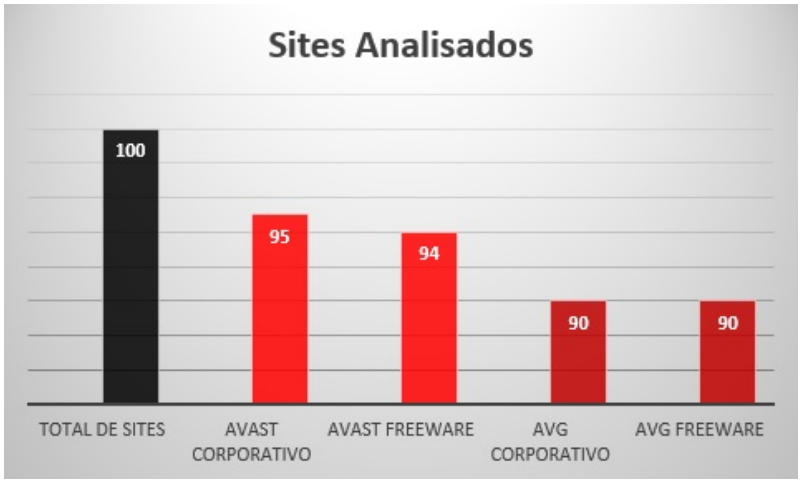

Figura 9. Sites infectados

escaneamentos rápidos deixa a desejar em termo de varredura em arquivos como constatado no resultado final apresentado, levando em conta que são dois dos maiores antivírus que hoje estão no mercado ainda sim o AVAST e superior.

Nos resultados de todos os testes, o AVAST se manteve sempre acima do AVG até mesmo a sua versão Freeware se manteve superior a versão pagado AVG, como demonstrados nos relatórios obtidos. Outro aspecto relevante é o valor, se for para ser utilizado numa empresa o AVAST oferece proteção para 10 computadores por 1 ano no valor de R$ 99,00 Reais já o AVG oferece para os mesmo 10 computadores por 1 ano o valor de R$ 415 Reais

Referências

Avast (2014). Historia sobre avast. Disponível em: <http://www.avast.com/pt-br/about//>. Acesso em: set 2014.

AVG (2009). Historia sobre avg. Disponível em: <http://mundodasmarcas.blogspot.com.br/2009/04/avg.html//>. Acesso em: set 2014.

AvgBrasil (2014). Avgbrasil. Disponível em: <http://www.avgbrasil.com.br/download-avg-internet-security-business//>. Acesso em: set 2014.

Inforquali (2012). Historia do antivirus. Disponível em: <http://www.inforquali.com/iq/pt/tutoriais/informativos/origem-e-historia-dos-virus-informaticos.php//>. Acesso em: nov 2014.

ISOVirus (2014). Dropbox iso vÃrus. Disponível em: <https://www.dropbox.com/sh/thurpg7l4p3eeew/AAC4rPduDj8N-yj1beNsoi71a?dl=0//>. Acesso em: set 2014.

Mussum (2014). SeguranÃ§a em redes. Disponível em: <http://187.7.106.14/emmonks/seguranca3/Pratica1/AVAST//>. Acesso em: set 2014.

Serrano, P. (2014). VÃrus cuidados com pc. Disponível em: <http://www.ebah.com.br/content/ABAAAAEscAJ/virus-cuidados-com-pc-paulo-serrano//>. Acesso em: set 2014.

support.clean (2014). support.clean-mx.de. Disponível em: <http://support.clean-mx.de/clean-mx/viruses//>. Acesso em: set 2014.

webgroove (2014). antivirus-gratuito. Disponível em: <http://www.webgroove.com.br/antivirus-gratuito-ou-pago-qual-a-melhor-opcao//>. Acesso em: set 2014.