ISSN:1983 7402 ITA, 23 a 25 de setembro de 2014

Aplicação do método Brasil de avaliação de *anti-malware* e as repercussões para a defesa cibernética

Antonio Montes Filho[1], Rogério Winter [2], Rodrigo de Souza Ruiz [1], Fernando Pompeo Amatte [3], José Geremonte Garcia [1], Bruna Stefani de Oliveira Martins [1]
1 Centro de Tecnologia da Informação Renato Archer - 2 Exército Brasileiro – 3 Pesquisador independente

***Resumo* — Semelhante ao risco financeiro e a reputação, o risco à segurança cibernética afeta profundamente uma empresa, órgão de governo e instituições militares. No contexto das ameaças cibernéticas, os malware apresentam uma tendência em expansão nos diversos setores produtivos. Escolher uma solução de software anti-malware eficiente é crucial para a organização.**

O método Brasil de avaliação de anti-malware se propõe a ser uma solução nacional para avaliar anti-malware com a base realidade de ameaças cibernéticas brasileiras. O trabalho visa responder aos seguintes questionamentos: deve-se continuar a adquirir anti-malware com base em recomendações de avaliadores independentes internacionais e o método Brasil é uma solução concreta para avaliação de anti-malware. Após experimentar o método Brasil com malwares coletados na internet brasileira o trabalho aponta para a necessidade de se aperfeiçoar o método em questão. Todavia, o método permitiu visualizar um panorama bem diferente daquele propagado por testadores independentes, pois apenas 50% da população dos malware coletados na internet brasileira foram detectados pelos anti-malware comercialmente disponíveis no Brasil.

***Palavras-Chave* — *anti-malware*, método, avaliação de produto de software.**

I. INTRODUÇÃO

Segurança é um sentimento de proteção, necessário e indispensável a uma sociedade e a cada um de seus integrantes, contra ameaças de qualquer natureza. Defesa é a ação capaz de garantir esse sentimento [1]. Baseado no conceito pode-se derivar questões para tratar de tecnologia da informação e de software tão necessários aos ambientes e sistemas que necessitam qualidade e confiabilidade para resguardar informações críticas.

A segurança da informação depende do funcionamento confiável de uma infraestrutura que por sua natureza é crítica. Ameaças cibernéticas exploram a crescente complexidade e conectividade de sistemas de infraestruturas críticas, colocando a segurança em risco. Semelhante ao risco financeiro e a reputação, o risco à segurança cibernética afeta profundamente uma empresa, órgão de governo e instituições militares. Ela pode elevar os custos e impactos na receita e prejudicar a capacidade da organização em inovar, ganhar e manter seus clientes. Com relação às instituições públicas, o maior prejudicado é o cidadão.

No contexto das ameaças cibernéticas, os *malware* apresentam uma tendência em expansão nos diversos setores produtivos. Segundo o relatório da empresa Check Point [2], quase 84% das organizações pesquisadas foram infectadas com *malware*. Segundo estimativas dos especialistas da Check Point, 2,2 *malware* desconhecidos batem nas empresas uma vez a cada hora.

Neste contexto, um sistema *anti-malware* ganha especial importância, pois ele representa o último elemento de defesa antes de um ataque se consumar. A natureza da tecnologia muda rapidamente, igualmente, a natureza dos *malware*. Os diversos fabricantes de software *anti-malware* anunciam novas e eficientes tecnologias que pretendem fornecer um melhor desempenho e respostas mais baratas nos incidentes de segurança com *malware*, dentro das organizações.

No entanto, existe atualmente pouca orientação sobre a melhor maneira de avaliar a eficácia de tais alegações. Claramente, só pode haver uma tecnologia que é mais rápida, melhor e mais eficiente do que todas as outras, mas essas reivindicações carecem de comprovação dentro dos limites de um rigoroso processo de análise operacional de um software *anti-malware*.

O objetivo do teste de software é mostrar a presença de defeitos caso eles existam [3]. Da mesma forma, o objetivo do teste de software *anti-malware* é identificar possíveis fragilidades nos sistemas e atribuir valores com indicadores chave de desempenho que permitam classificar os sistemas adequadamente através destes atributos.

Assim, este artigo tem por objetivo o de responder aos seguintes questionamentos: A avaliação realizada por instituições internacionais ou testadores independentes se aplica a realidade de ameaças cibernéticas brasileiras? O método Brasil é uma solução concreta para avaliação de *anti-malware*?

Desta forma, este trabalho apresenta uma perspectiva de teste de *anti-malware* alinhado com a validação dos atributos que buscam o equilíbrio entre desempenho da máquina com e sem o *anti-malware*, taxa de detecção de *malware* e taxa de falso positivo do mesmo.

O artigo apresenta as seguintes contribuições: inserção de teste de *anti-malware* no Brasil, validação dos *anti-malware* baseados nas características específicas da internet brasileira e apresenta um novo panorama dos softwares *anti-malware* comercializados no Brasil. O artigo está dividido em 6 (seis) partes: introdução, métodos relacionados, método Brasil, aplicação do método, resultados da avaliação, discussões e conclusão.

II. MÉTODOS RELACIONADOS

Existem no mercado internacional diversas instituições ou testadores independentes que realizam sistematicamente testes e divulgam os resultados dos diversos softwares *anti-malware* existentes. No momento em que este método estava sendo escrito, foi possível identificar os seguintes avaliadores: VB100 [4], AV-Comparatives [5], Anti-malware Test [6], AV-TEST [7], ICSALab [8], NSS Labs [9], West Coast Labs [10] e EICAR [11].

Os métodos e técnicas utilizadas nos testes em tela não são totalmente divulgados. Os laboratórios apresentam os resultados genericamente dos melhores produtos, contudo dependendo do método e da forma que os testes são executados os resultados também sofrem alterações.

Tradicionalmente, os resultados dos testes de *anti-malware* dos laboratórios em tela são utilizados como base na tomada de decisão do processo de aquisição em órgãos públicos e usuários corporativos.

III. MÉTODO BRASIL

De fato, o método Brasil insere uma nova perspectiva de validação de *anti-malware* realizada no Brasil em instituição pública de pesquisa isenta e comprometida com a segurança da informação nacional.

Para avaliar diversos *anti-malwares*, existe a necessidade da definição de características de qualidade que reflitam medidas de segurança adequadas. O desenvolvimento de um método de avaliação adota atributos que buscam o equilíbrio entre desempenho da máquina com e sem o sistema *anti-malware* instalado, taxa de detecção de *malware*, usabilidade do software em questão e taxa de falso positivo do mesmo. O desempenho, a taxa de detecção e usabilidade de um determinado produto deve ser máxima, buscando equilíbrio entre os mesmos, sem, portanto nenhum desses indicadores substituir o outro.

Esse tópico apresenta-se de forma resumida, o método para avaliação de *anti-malware*, baseada nas melhores praticas da AMTSO [12], NBR ISO/IEC 9126 [13] de qualidade de produto e base de casos de teste de segurança da Instituição.

O método visa analisar características de qualidade necessárias para incluir um software na categoria de *anti-*malware. O método é composto dos seguintes elementos de teste:

- ✓ Análise de varredura (Scan) - identificar e verificar as técnicas de varredura, considerando inclusive tipos de arquivos e extensões.
- ✓ Taxa de detecção - analisar as técnicas de detecção do produto e a comparação com outros *anti-malware* conhecidos no mercado brasileiro.
- ✓ Taxa de limpeza/remoção/quarentena é um processo que tem por objetivo a separar a parte maliciosa da parte não maliciosa de um arquivo, já o processo de remoção tem por objetivo apagar o arquivo, enquanto que a quarentena objetiva tonar um arquivo inacessível ao usuário ou a outros programas.
- ✓ Indicadores de desempenho - verificar como o produto impacta o consumo de CPU, memória e acesso a disco durante o uso do normal e diário do equipamento.
- ✓ Indicadores de instalação/atualização - identificar como o produto gerencia suas atualizações, incluindo detalhes de tamanho de base e frequência de atualizações.
- ✓ Usabilidade do software - identificar a facilidade de uso do sistema e a geração de relatórios do sistema em análise.
- ✓ Indicadores de estabilidade - identificar possíveis problemas relacionados à estabilidade do produto durante uso.
- ✓ Indicadores de segurança – identificar possíveis falhas de segurança que comprometam a eficácia e eficiência do software

Todavia, para os testes relatados no presente artigo foram utilizados os resultados dos seguintes itens da Fig 1: análise, taxa de detecção e indicadores de desempenho.

IV. APLICAÇÃO DO MÉTODO

A bancada de testes está em conformidade às orientações da AMTSO [12], a qual recomenda que os testes sejam efetuados em ambientes mais próximos da realidade. Os produtos testados foram instalados em suas últimas versões e suas configurações foram mantidas como o padrão sugerido pelo fabricante.

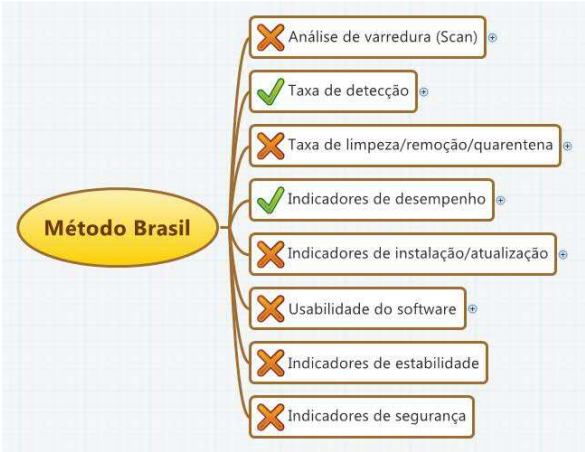

Fig 1 - Arquitetura geral do método

Todos os testes foram executados em máquinas com o Windows XP, *service* Pack 3. Em 08 de abril de 2014 a Microsoft terminou com o suporte para o Windows XP. Todavia, a escolha desse sistema baseou-se no fato de que os mercados corporativos e domésticos ainda usam essa plataforma.

De acordo com Newman [14] 95% dos 2,2 milhões de caixas automáticos do mundo utilizam o Windows XP. Da mesma forma, Paganini [15] afirma que SO XP ainda é amplamente utilizado em grande quantidade de sistemas que vão desde *Cashpoint* (ATM), *Point-of-sale* (POS) [16], máquinas para sistemas HMI/SCADA. Esta afirmação do autor é baseada na análise dos dados publicados em maio no STATCOUNTER [17], onde o uso de XP em escala mundial passou de 19,79% para 16,17% no último 6 (seis) meses. Além disso, Windows XP é amplamente adotado em ambientes críticos, computador dos sistemas de supervisão,

controladores lógicos programáveis e aplicações de interface homem-máquina.

Para a avaliação comparativa dos *anti-malware*, foi preparada uma bancada de testes baseada em critérios e características definidas no método. Para efeito de comparação (benchmark) 07 (sete) produtos *anti-malware* foram testados.

Critérios para escolha do anti-malware

Para a escolha dos produtos *anti-malware* foram adotados os seguintes critérios: facilidade de aquisição no mercado brasileiro, tempo e aceitação no mercado tanto doméstico quanto corporativo. Dos produtos *anti-malware* selecionados os fabricantes estão estabelecidos a pelo menos 20 anos no mercado exceto um dos produtos que existe a menos de 5 anos. Os *anti-malwares* utilizados são versões comerciais não gratuitas.

Critérios para escolha de malware e arquivos benignos

Os *malwares* utilizados foram selecionados a partir da base de dados de artefatos maliciosos da internet brasileira, armazenados em Instituição Pública, onde 80% da população são *malwares* nacionais, a fim de que resultado seja mais próximo possível da realidade brasileira. Para o teste do método, a população de *malware* foi dividida em três grupos de acordo com a data de coleta, da seguinte forma:

✓ 100 (cem) *malwares* coletados no dia do inicio dos testes;

✓ 100 (cem) *malwares* coletados no máximo 6 (seis) meses antes do inicio dos testes;

✓ 100 (cem) *malwares* coletados a mais de 6 (seis) meses antes do inicio dos testes.

Dentro de cada amostra a seleção dos exemplares foi realizada de forma aleatória.

Para medir a taxa de falso positivo, foram selecionados 300 arquivos benignos (não maliciosos), provenientes de fabricantes conhecidos como Microsoft, Adobe, Sun e Corel.

		Arquivos de teste					
Quant	Descrição	Arquivos binários	Sem extensão	Extensão .DOC	Extensão .EXE	Extensão aleatória	Compactado UPX
100	*malwares* coletados no dia do inicio dos testes;	100	100	100	100	100	100
100	*malwares* coletados no máximo 6 (seis) meses antes do inicio dos testes;	100	100	100	100	100	100
100	*malwares* coletados a mais de 6 (seis) meses antes do inicio dos testes.	100	100	100	100	100	100
300	Arquivos benignos (extensão .txt, .bmp, e etc)	300					
Total		600	600	600	600	600	600

Fig 2 - Resumo dos arquivos utilizados no teste

Realização dos Testes

Foram realizados 06 (seis) testes de detecção com a população de *malware*. Para os testes de detecção, os *malwares* e arquivos benignos foram organizados conforme demonstrado na Fig 2.:

✓ Arquivos binários de malware iguais aos capturados na internet brasileira;

✓ Arquivos sem extensão, a fim de medir a capacidade do *anti-malware* em analisar arquivos de tipos desconhecidos. O arquivo malicioso foi renomeado com o *hash* MD5 do arquivo malicioso;

✓ Arquivos com a extensão .EXE, com a finalidade de medir a capacidade do *anti-malware* em analisar arquivos executáveis;

✓ Arquivos com a extensão .DOC, visando medir a capacidade do *anti-malware* em analisar arquivos de tipos diferentes;

✓ Arquivos com as extensões aleatórias incluindo extensões inexistentes e extensões de arquivos relativos a arquivos que não deveriam ser infectados por *malware*, tais como.TXT, .Log e .BMP, visando medir a capacidade do anti-malware em analisar arquivos pelo tipo real do arquivo;

✓ Arquivos submetidos ao compactador UPX, com a finalidade de medir como o *anti-malware* se comporta com esse tipo de situação. O UPX [18] é um programa que compacta o executável e ainda mantém a funcionalidade do mesmo. A justificativa para o uso do UPX é que de acordo com o relatório da Trustwave [19], mais de 50% dos *malwares* usam o compactador em tela como técnica de ofuscação para burlar as proteções dos sistemas *anti-malware*.

✓ Os arquivos benignos foram renomeados da mesma maneira que os arquivos maliciosos e colocados juntamente com os arquivos maliciosos na bancada de testes.

V. RESULTADOS DA AVALIAÇÃO

Taxa de detecção

Os sistemas *anti-malware* avaliados apresentaram taxas de detecção em torno dos 45% (Fig. 3), quando analisaram os arquivos binários dos *malware*, ou seja, um pouco mais da metade dos *malwares* testados não foi detectada.

No teste de detecção no grupo de arquivos: sem extensão, extensão .DOC, extensão .EXE, extensão aleatória e compactado com UPXs a taxa média de detecção foi de 48.0%, 48.1%, 48.2%, 48.2% e 12.5%, respectivamente (Fig 4).

A observação que se faz é que não houve compactação recursiva.

Com relação à taxa de falso positivo, apenas dois *anti-malware* classificaram como *malware* os arquivos benignos. O *anti-malware* C e D classificaram 5 (cinco) e o 4 (quatro) arquivos, respectivamente como malware.

Por fim, a Fig. 5 demonstra uma distribuição da taxa de detecção dos *malwares* de acordo com a data de detecção. Com *malwares* coletados no dia do teste a taxa de detecção varia em torno dos 20%. Para *malwares* coletados com até 6 meses da data do teste o resultado varia entre 20% e 40%. Finalmente, *malwares* coletados a mais de 6 (seis) meses da data do teste a taxa de detecção está acima dos 70%.

Indicadores de desempenho

Os testes de desempenho foram realizados logo após a instalação do sistema anti-malware. A máquina de teste teve o seu desempenho avaliado com o software Boot timer [20], PassMark AppTimer [21] e Performance Test [22]

Os testes foram avaliados em 4 quesitos, sendo eles:

ISSN:1983 7402 ITA, 23 a 25 de setembro de 2014

1. Tempo na inicialização do sistema operacional (Boot);
2. Desempenho de hardware (CPU, Vídeo, Memória e Disco);
3. Desempenho na abertura de aplicativos;
4. Desempenho na realização de cópias, compactação e descompactação de arquivos.

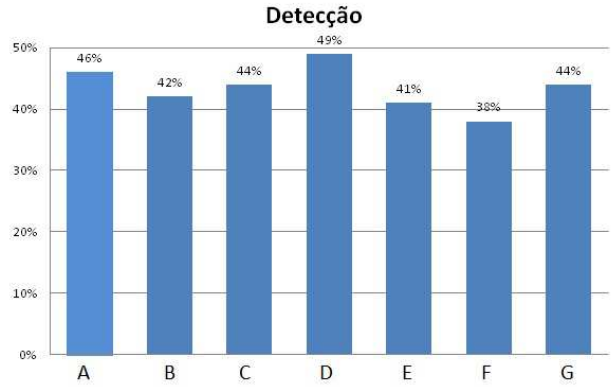

Fig 3 - Comparação de detecção do arquivo binário

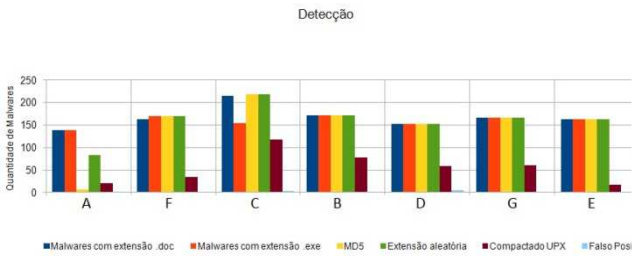

Fig 4 - Comparação das detecções com mudança de extensão

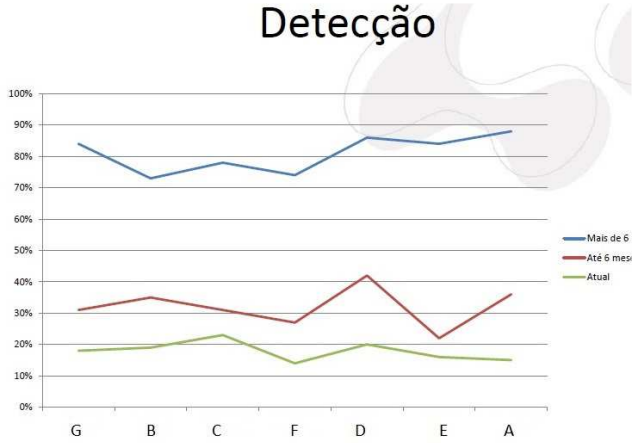

Fig 5 - Taxa de detecção para amostras ao longo do tempo

Para a avaliação de cada quesito foram realizados cinco testes consecutivos, sendo que os resultados são representados pelas medias das medições. As Fig 6 a 9 apresentam graficamente os resultados dos testes. A Fig. 6 apresenta um gráfico de comparação referente ao quesito 1, o qual trata do tempo na inicialização do sistema operacional. Neste quesito, as medições foram bem variadas em relação aos sistemas *anti-malware*, sendo o menor tempo de inicialização do sistema *anti-malware* de 40 s.

Desempenho do Hardware

A Fig. 7 representa o quesito 2, com informações sobre desempenho de hardware. Nos testes do quesito que trata do desempenho de hardware, os softwares *anti-malware* apresentaram resultados semelhantes, exceto o *anti-malware* E que apresentou o menor consumo de CPU.

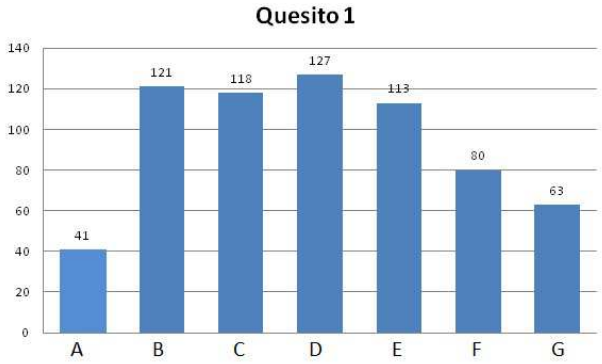

Fig 6 – Tempo em segundos na inicialização do sistema operacional

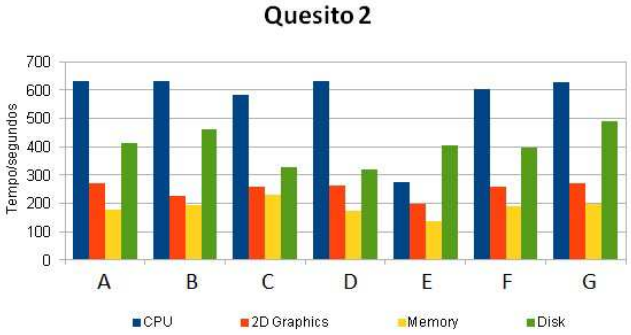

Fig 7 - Desempenho de hardware

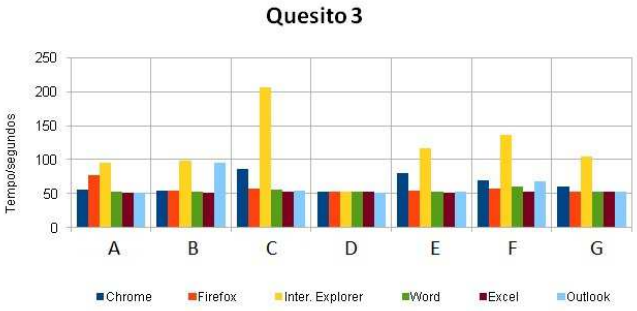

Fig 8 - Testes de desempenho de aplicativos

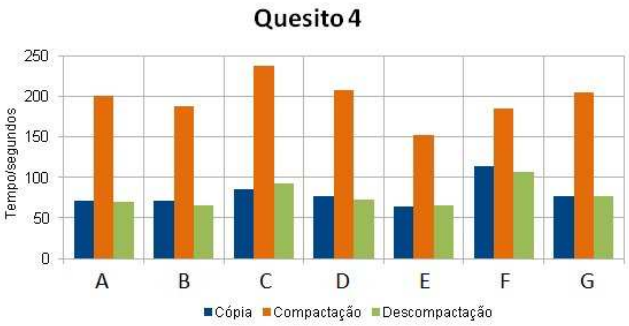

Fig 9 - Testes de cópia, compactação e descompactação

Desempenho na abertura de aplicativos.

A Fig. 8 apresenta um gráfico comparativo do quesito 3 desempenho na abertura de aplicativos. Foram utilizados os aplicativos considerados comuns para as máquinas de usuários brasileiros: Internet Explorer, Apache OpenOffice 3.4, Adobe Acrobat Reader, Adobe Flash Player, Java 7, directx 9, Microsoft Office Home and Busines 2010, Firefox e o Chrome. Além disso, o firewall e a atualização automática do Windows foram desativados.

Desempenho na realização de cópias, compactação e descompactação.

A Fig 9 demonstra o desempenho na realização de cópias, compactação e descompactação de arquivos. Na observação pode-se verificar que os produtos *anti-malware* não introduziram significativa carga aos computadores utilizados em teste.

VI. DISCUSSÃO E CONCLUSÃO

Na avaliação dos sistemas *anti-malware* os métodos ou metodologias existentes (II. MÉTODOS RELACIONADOS) apresentam resultados diferentes e bem variados daqueles encontrados nas medidas aqui apresentadas.

Com relação às taxa de detecção, os resultados são discrepantes. Os outros métodos e metodologias divulgam taxas de detecção próximos da perfeição. Todavia, em um teste real tomando como base à internet brasileira a imagem que se obtém é totalmente diferente. No teste de detecção de *malware* a taxa de detecção fica próxima de 50%, ou seja, apenas metade da população é detectada e classificada como *malware*, valor bem diferente quando comparado àquelas taxas divulgadas por outros métodos. Com toda a certeza, qualquer *malware* que ultrapasse a barreira de proteção do *anti-malware* podem causar consequências maléficas colocando em risco a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

Ao se alterar os arquivos maliciosos através da mudança de extensão para que se possam testar as diferentes abordagens de detecção dos *anti-malware* a média de detecção para a população de teste fica em torno dos 50%. Novamente, apenas metade dos *malware* foi detectada. De forma alarmante, quando foi utilizada uma compactação bem conhecida nos malwares, o UPX, o resultado é catastrófico, pois a média de detecção e classificação fica em torno dos 20%. A observação que se faz é que a compactação UPX é uma técnica de ofuscação utilizada para ludibriar os *anti-malware* e muito utilizada entre os fabricantes de *malware* conforme relatado pela *Trutwave* [19] e por Rubira Branco [23].

Analisando os resultados do teste de detecção, podemos inferir questões que são atraídas para o problema da defesa cibernética brasileira. As tecnologias presentes em soluções de software *anti-malware* e ofertadas no mercado nacional, são adquiridos de empresas internacionais. Essas soluções de software são disponibilizadas em aplicativos com código fonte proprietários e estabelecidas sob a égide de patentes. Os softwares *anti-malware* são soluções críticas, invasivas e possuem acesso integral às informações que trafegam nos equipamentos de TI nacional. Em virtude das características operacionais e funcionais, modelo de rastreio, captura e atualização dos softwares não é domínio do o usuário como as informações são tratadas ou utilizadas por parte dos fabricantes de software *anti-malware*. Além disso, a crença inquestionável em testadores independentes contribui na fragilização da defesa cibernética. Em estudo recente promovido pelo Instituto Ponemon [25], revelou que os profissionais de segurança têm sistemas deficientes em termos de proteção contra ataques digitais e vazamentos de dados. Assim, existe a necessidade de que os profissionais de segurança tenham acesso as melhores defesas e inteligência contra as ameaças.

No tocante a análise de desempenho, Denning [24] enunciou a seguinte característica desejável para um sistema responsável por detectar invasões: o seu funcionamento do sistema de detecção deve impor uma carga mínima no computador no qual está instalado. Desta forma, este é o objetivo de se avaliar o desempenho do sistema *anti-malware* para identificar possível sobrecarga que interfere no funcionamento da máquina. Ao analisar os gráficos explicitados pelas Fig. 6 a 9, podemos concluir que os diversos *anti-malware*, na média, não inseriram carga debilitante ao sistema de teste. Fato curioso é o demonstrado na tabela 1, pois, ao contrário do esperado, os sistemas sofreram uma otimização após a instalação do software *anti-malware*. Todavia, cabe um maior aprofundamento no assunto a fim de pacificar possíveis variáveis não tratadas pelo método.

Teste (segundos)	Sem *anti-malware*	Com *anti-malware*
PassMark Rating	317,4	305,1
CPU Mark	628	583
2D Graphics Mark	264,7	257,6
Memory Mark	209,3	229,9
Disk Mark	392,7	328,1

Tabela 1 - Comparativo do sistema com e sem *anti-malware*

Após as considerações realizadas nesta Seção, a validação e teste de sistemas *anti-malware* ganham importância e respaldam a inserção na agenda de trabalho de instituição de pesquisa nacional isenta e comprometida com a segurança da informação brasileira.

Do exposto, a resposta ao questionamento inicial é que os resultados divulgados por instituições internacionais e testadores independentes não consideram o teatro de ameaças cibernéticas brasileiras e não devem ser considerados isoladamente para respaldar processos decisórios de

ISSN:1983 7402

aquisição e escolha das soluções de software *anti-malware* para proteção.

As tecnologias que confiamos para fornecer proteção contra as ameaças cibernéticas devem se adaptar ao contexto no qual são utilizadas, da mesma forma que os processos e métodos de teste.

Na sequência de trabalhos futuros, novos relatórios de teste serão disponibilizados para consultas na página da internet: http://www.cti.gov.br/seguranca-de-sistemas-de-informacao-dssi.

REFERÊNCIAS

[1]. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Engenharia de software: Qualidade de produto. **NBR ISO/IEC 9126-1: modelo de qualidade**, Rio de Janeiro, 2003. 21. Disponivel em: <https://pt.wikipedia.org/wiki/Segurança_e_defesa>. Acesso em: 01 maio 2014.

[2]. CHECK POINT. 2014 Security Report. **Check Point**, 2014. Disponivel em: <http://www.checkpoint.com/documents/ebooks/security-report-2014/files/assets/common/downloads/Check Point Security Report 2014.pdf>. Acesso em: 13 maio 2014.

[3]. DELAMARO, M. E.; MALDONADO, J. C.; JINO, M. **Introdução ao Teste de Software**. 1. ed. Rio de Janeiro: Elsevier, v. 1, 2007.

[4]. VIRUS BULLETIN. testing methodology. **Virus Bulletin**, 2014. Disponivel em: <https://www.virusbtn.com/vbspam/methodology/index>. Acesso em: 10 fevereiro 2014.

[5]. AV COMPARATIVES. File Detection Tests. **AV Comparatives**, 2014. Disponivel em: <http://www.av-comparatives.org/detection-test/>. Acesso em: 10 fevereiro 2014.

[6.] ANTI-MALWARE TEST. Tests Methodologies. **Anti-malware Test**, 2014. Disponivel em: <http://www.anti-malware-test.com/testing-methodologies>. Acesso em: 10 fevereiro 2014.

[7]. AV TEST. AV Test - Test Procedures. **The Independent IT-Security Institute**, 2014. Disponivel em: <http://www.av-test.org/en/test-procedures/test-modules/>. Acesso em: 10 fevereiro 2014.

[8]. ISCA LABS. ICSA Labs Anti-Virus Certification Test Matrix. **ISCA Labs**, 2014. Disponivel em: <https://www.icsalabs.com/sites/default/files/AV%20Cert%20Test%20Suites%20Matrix%20v4%205.pdf>. Acesso em: 10 fevereiro 2014.

[9]. NSS LABS. Endpoint Protection – Evasion and Exploit: Test Methodology v4.0. **NSS Labs**, 2014. Disponivel em: <https://www.nsslabs.com/reports/endpoint-protection-%E2%80%93-evasion-and-exploit-test-methodology-v40>. Acesso em: 10 fevereiro 2014.

[10]. WEST COAST LABS. Technology Reports. **West Coast Labs**, 2014. Disponivel em: <http://www.westcoastlabs.org/>. Acesso em: 10 fevereiro 2014.

[11]. EICAR. EUROPEAN EXPERT GROUP FOR IT-SECURITY. **EICAR**, 2014. Disponivel em: <http://www.eicar.org>. Acesso em: 10 fevereiro 2014.

[12]. ANTI-MALWARE TESTING STANDARDS ORGANIZATION. Documents and Principles. **AMTSO**, 2009. Disponivel em: <http://www.amtso.org/documents.html>. Acesso em: 05 maio 2012.

[13]. ISO/IEC 9126. Qualidade de software. **Wikipedia**, 2014. Disponivel em: <https://pt.wikipedia.org/wiki/ISO/IEC_9126>. Acesso em: 10 maio 2014.

[14]. NEWMAN, L. H. Report: 95 Percent of the ATMs in the World Still Run Windows XP. **Future Tense**, 2014. Disponivel em: <http://www.slate.com/blogs/future_tense/2014/03/14/windows_xp_still_runs_on_95_percent_of_the_atms_in_the_world_says_reuters.html>. Acesso em: 15 março 2014.

[15]. PAGANINI, P. Impact of Windows XP End of life on Critical Infrastructure. **Security Affairs**, 2014. Disponivel em: <http://securityaffairs.co/wordpress/25984/security/xp-critical-infrastructure.html>. Acesso em: 29 junho 2014.

[16]. PAGANINI, P. Soraya PoS Malware, a new start in criminal ecosystem. **Security Affairs**, 2014. Disponivel em: <http://securityaffairs.co/wordpress/25479/cyber-crime/soraya-pos-malware.html>. Acesso em: 05 junho 2014.

[17]. STATCOUNTER. StatCounter Global Stats. **Stat Counter**, 2014. Disponivel em: <http://gs.statcounter.com/>. Acesso em: 10 junho 2014.

[18]. OBERHUMER, M. F. X. J.; MOLNÁ, L.; REISER, J. F. Ultimate Packer for Executables. **Sourceforge**, 1996. Disponivel em: <http://upx.sourceforge.net/>. Acesso em: 12 dezembro 2012.

[19]. TRUSTWAVE. 2012 Global Security Report - United States Secret Service. **Service Secret**, 2014. Disponivel em: <www.secretservice.gov/Trustwave_WP_Global_Security_Report_2012.pdf>. Acesso em: 10 abril 2014.

[20]. PLANETSOFT. Planet Soft. **Planet Soft**, 2012. Disponivel em: <http://www.planetsoft.org/>. Acesso em: 10 março 2012.

[21]. PASSMARK SOFTWARE. App Timer application's startup time. **PassMark Software**, 2010. Disponivel em: <http://www.passmark.com/products/apptimer.htm>. Acesso em: 10 março 2012.

[22]. PASSMARK SOFTWARE. PerformanceTest Software. **PassMark Software**, 2014. Disponivel em: <http://www.passmark.com/download/pt_download.htm>. Acesso em: 10 março 2014.

[23]. BRANCO, R. R.; BARBOSA, G. N.; NETO, P. D. Scientific but Not Academical Overview of Malware Anti-Debugging, Anti-Disassembly and Anti-VM Technologies. **Black Hat**, 2012. Disponivel em: <https://media.blackhat.com/bh-us-12/Briefings/Branco/BH_US_12_Branco_Scientific_Academic_Slides.pdf>. Acesso em: 10 dezembro 2012.

[24]. DENNING, D. E. An Intrusion-Detection Model. **IEEE TRANSACTIONS ON SOFTWARE ENGINEERING**, 1987, v. SE-13, NO. 2, p. 222-232, february 1987.

[25]. PONEMON INSTITUTE. Expondo as Lacunas da Cibersegurança: Brasil. **Websense, Inc**, 2014. Disponivel em: <http://www.websense.com/assets/reports/report-ponemon-2014-part1-summary-brazil-pt.pdf>. Acesso em: 24 junho 2014.

Antonio Montes Filho, antonio.montes@cti.gov.br, Rogerio Winter, winter@cdciber.eb.mil.br, Fernando Pompeo Amatte, famate@gmail.com, Rodrigo de S. Ruiz, rodrigo.ruiz@cti.gov.br, José Geremonte, zeca.ti@gmail.com, Bruna Martins bruna.martins@cti.gov.br Tel. +55-19-3746-6234