Preprint submitted sep/2020 to Journal of Applied Security Research WASR-2020-0066R1 acepted 16/07/2022
Article DOI: 10.1080/19361610.2022.2104104
To publish in the Journal: Journal of Applied Security Research - Journal ISSN: 1936-1629

Brazil Method of Anti-malware Evaluation and Cyber Defence Impacts

Rodrigo Ruiz[1], Rogério Winter[2], Dr Ferrucio de Franco Rosa[3],

Dr Pancham Shukla[4], Prof. Hassan Kazemian[4,5]

[1,3] DIMEC/CTI-Renato Archer -Brazilian Ministry of Science, Technology, Innovation and Communications
[2]FEEC/UNICAMP
[3] UNIFACCAMP
[1,4,5] School of Computing and Digital Media (SCDM) London Metropolitan University
[1]rodrigosruiz@outlook.com, [2]rogwinter@gmail.com, [3]ferrucio.franco@cti.gov.br, [4]p.shukla@londonmet.ac.uk, [5]h.kazemian@londonmet.ac.uk

Abstract: Cyber risk profoundly affects all. In the context of cyber threats, malware is trending in various productive sectors. Nowadays, anti-malware is essential to combat cyber threats; however, their efficiency is often questioned, because malware is different for different regions in the world. Choosing an efficient anti-malware software solution is crucial to protect information from different institutions. The method confirmed the reality of evaluating the different known methodologies, showing another scenario of efficiency of the different testers. The method allowed visualizing an interesting panorama because 50% of malware collected on the Brazilian Internet were detected by anti-malware commercially available in Brazil.

Keywords: **anti-malware efficiency, evaluate method software test, product evaluation.**

I. INTRODUCTION

Security is a feeling of protection, necessary and indispensable to society and each of its members, against threats of any nature. The defence is the action capable of ensuring that feeling (Escola Superior de Guerra, 2014). Based on the concept, questions may be derived to address information technology and software so necessary to environments and systems that need quality and efficiency to safeguard critical information.

Information security depends on the reliable functioning of an infrastructure that by its nature is critical. Cyber threats exploit the increasing complexity and connectivity of critical infrastructure systems, putting security at risk. Similar to financial risk, cybersecurity risk profoundly affects a company, government agency, and armed forces. It may drive up costs and revenue impacts and undermine the organization's ability to innovate and retain its customers. Concerning public institutions, citizens are the most affected.

In the context of cyber threats, malware is trending in various productive sectors. According to the company's Check Point report (Check Point Sofware Technologies Ltd, 2014), almost 84% of the organizations surveyed were infected with malware. According to estimates by CheckPoint experts, 2.2 unknown malware hits companies once every hour. The cyber virus in comparison with the similarity with biological systems is part of (Filiol, 2005) (Ludwig, 1993) (Ludwig, 1995)

An anti-malware system gains special importance because it represents the last element of defence before an attack is consummated. In the article (Nissim, et al., 2014), the author provides a method to improve detection while the nature of technology changes quickly, equally, the nature of malware. The various anti-malware software manufacturers announce new and efficient technologies that aim to provide better performance and cheaper responses in malware security incidents within organizations. However, there is currently little guidance on how best to assess the effectiveness of such claims. There may be only one technology that is faster, better and more efficient than all the others. However, these claims lack proof within the limits of a rigorous anti-malware software operational review process.

The purpose of software testing is to show the presence of defects if they exist (DELAMARO, et al., 2007). Similarly, the purpose of anti-malware software testing is to identify possible weaknesses in systems and assign values with key performance indicators that allow classifying systems appropriately through these attributes.

Thus, this article aims to answer the following questions: Does the evaluation carried out by international institutions or independent testers apply to the reality of Brazilian cyber threats? Is the Brazil method a concrete solution for anti-malware evaluation? This paper presents an anti-malware test perspective aligned with the validation of attributes seeking the balance between machine performance, malware detection rate, and false-positive rate.

The version of the Brazil Method was presented at the Symposium on Operational Applications in Defence Areas

Preprint submitted sep/2020 to Journal of Applied Security Research WASR-2020-0066R1 acepted 16/07/2022
Article DOI: 10.1080/19361610.2022.2104104
To publish in the Journal: Journal of Applied Security Research - Journal ISSN: 1936-1629

(Montes, et al., 2014) (SIGE)[1]. The Brazil Method was particularly important to the Brazilian Army because it was possible to list requirements for the corporate system. The Army's anti-malware project received an honourable mention from the Brazilian Federal Court of Accounts for software purchase processes by the Brazilian State.

The remainder of this paper is organized as follows: introduction, related methods, Brazil method, and application of the Method, evaluation results, discussions and conclusion.

II. RELATED METHODS

Several independent institutions or testers in the international market systematically test and disseminate the results of various existing anti-malware software. At the time this method was being written, it was possible to identify the following evaluators: VB100 (Virus Bulletin, 2014), AV-Comparatives (AV COMPARATIVES, 2014), Anti-malware Test (Anti-Malware-Test.com, 2012), AV-TEST (AV Test, 2014), ICSA Lab (ICSA Labs, 2014), NSS Labs (NSS Labs, 2018), West Coast Labs (West Coast Labs, 2014) and EICAR (EUROPEAN EXPERT GROUP FOR IT-SECURITY, 2020).

The methods and techniques used in screen testing are not fully disclosed. Laboratories present the results generically of the best products, however depending on the method results also change. Traditionally, results of anti-malware testing are used as the basis for decision-making of the procurement process in public agencies and corporate users.

Existing methods fail to clarify the details of the test methodology, preventing their reproducibility. On the other hand, the credibility of the tests may be affected, since the test companies' source of revenue is the advertisements of the antivirus companies themselves. Another characteristic made the creation of a method for the Brazilian Government important was the specificity of the national software. It is well known Brazil has developed over the last decades the most secure and efficient banking systems interconnect all banks offering services in the country. This makes attackers also evolve in their methods, intensifying competition between good and evil.

It is common to find published works analysing efficiency and individual performance of an anti-malware, especially when launching new versions in general published in paid magazines side by side with the merchandise of the same anti-malware. (FLEISHMAN, 2018) Normally magazines just link the anti-malware test companies' results with some flashy headline. (Consumer Watch, 2015) (Hachman, s.d.)

In the article (Nurhayati, et al., 2018) is presented a theoretical model, however, the authors did not show a real application of the method. Besides, this method was proposed in 2018, but the Brazilian government's need was for the project in 2014. Our literature review found other test methods (Bai, et al., 2019), (Valdi, et al., 2015), and (Shevchenko, et al., 2019). The Brazil Method is innovative in the Government area for anti-malware test and was a seed for author other method and works (Ruiz, et al., 2015) (Winter & Ruiz, 2017)

III. THE BRAZIL METHOD

The Brazil Method inserts a new perspective for anti-malware validation, as it is carried out in a Brazilian public institution exempt and committed to the security of national information. To evaluate various anti-malware, it is necessary to define quality characteristics that reflect the most appropriate security requirements. The development of an evaluation method adopts requirements seek to evaluate the performance of the computer, the rate of malware detection, the usability of the software and the rate of false positives. Computer performance may not be impaired when anti-malware is installed. The detection rate may be a maximum of the set of malware used to test the efficiency of the anti-malware. The usability of anti-malware is important, as difficulty in operating anti-malware may lead to risky situations. Finally, the false-positive rate assesses the anti-malware's ability to discern a benign file from malware without error. Our method was based on AMTSO's best practices and anti-malware assessment recommendations (NTI-MALWARE TESTING STANDARDS ORGANIZATIONS, 2009) and NBR ISO / IEC 9126 (Wikipedia, 2020) standards. The AMTSO Testing Protocol Standard provides testing protocol and behaviour expectations for testers and vendors relating to the testing of anti-malware solutions. The standard is maintained and run by the Standards Working Group (SWG), a team of volunteers from within the AMTSO membership including representatives of security product vendors and expert testing labs. NBR ISO / IEC 9126 is a model quality standard for software products. It defines a set of parameters to standardize the evaluation of software quality.

The Brazil Method was designed to assess anti-malware security requirements and anti-malware quality characteristics. In addition to the best practices anti-malware assessment, mandatory aspects of Brazilian law have been incorporated into the Method. To obtain a reliable assessment, our testbed performed the tests in the environment closer to reality. The main features of the Brazil Method (figure 1) are:

[1] https://www.sige.ita.br/?lang=en

Preprint submitted sep/2020 to Journal of Applied Security Research WASR-2020-0066R1 acepted 16/07/2022
Article DOI: 10.1080/19361610.2022.2104104
To publish in the Journal: Journal of Applied Security Research - Journal ISSN: 1936-1629

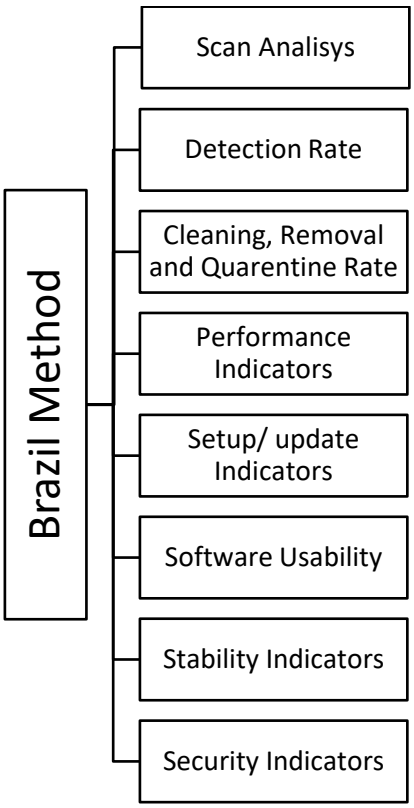

Figure 1 – Brazil Method

Definition

- ✓ Scan Analysis - the process of deep scanning the computer to identify malware infection. This process involves multiple tools and techniques to identify malware.
- ✓ Detection rate - analyse product detection techniques and comparison with other known anti-malware in the Brazilian market.
- ✓ Cleaning/removal/quarantine fee is a process that aims to separate the malicious part of the non-malicious part of a file, while the removal process aims to delete the file, while the quarantine aims to make a file inaccessible to the user or other programs.
- ✓ Performance indicators - check how the product affects CPU consumption, memory, and disk access during normal and daily use of equipment.
- ✓ Installation/update indicators - identify how the product manages its updates, including details of base size and frequency of updates.
- ✓ Software usability - identify the ease of use of the system and the generation of system reports under analysis.
- ✓ Stability indicators - identify possible problems related to product stability during use.
- ✓ Security indicators - identify potential security flaws that compromise software effectiveness and efficiency.

However, for the tests reported in this article, the results of the following items in Figure *1* were used: analysis, detection rate and performance indicators.

IV. APPLICATION OF THE METHOD

The tested products were installed in their latest versions and their settings were maintained as the standard suggested by the manufacturer.

OS selection criteria

All tests were run on machines running Windows XP, Service Pack 3. On April 8, 2014, Microsoft ended support for Windows XP. However, the choice of this system was based on the fact that the corporate and domestic markets still use this platform.

Windows XP was widely adopted in critical environments, computer supervision systems, programmable logic controllers and human-machine interface applications According to (Paganini, 2014), Windows XP SO is still widely used in many systems from Cashpoint (ATM), Point-of-sale (POS), and systems machines HMI/SCADA. This statement by the author is confirmed in the analysis of data from the first half of 2014 and published in the Statcounter Global Stats (Stat Counter, 2014), where the use of Windows XP represented a share close to 20% on a global scale.

Anti-malware selection criteria

Preprint submitted sep/2020 to Journal of Applied Security Research WASR-2020-0066R1 acepted 16/07/2022
Article DOI: 10.1080/19361610.2022.2104104
To publish in the Journal: Journal of Applied Security Research - Journal ISSN: 1936-1629

For the comparative evaluation of anti-malware, the testbed was based on criteria and characteristics defined in the Method. For benchmark 07 (seven) anti-malware products were tested. Any anti-malware can be submitted into this test Method.

For the selection of anti-malware products, the following criteria were adopted:

- Purchase availability in the Brazilian market;
- Compliance with legal requirements for public purchase in Brazil;
- Time de acceptance in both domestic and corporate markets Brazilian.

Of the selected anti-malware products manufacturers are established for at least 20 years on the market except one of the products. This anti-malware had existed for less than 5 years and was being put to use in the public administration. All versions of the evaluated anti-malware are commercial versions.

Malware selection criteria

The malware used was selected from the database of malicious artefacts on the Brazilian Internet, which were stored in a Public Institution. This database consisted of 80% of malware found on the Brazilian internet and thus the results are close to the Brazilian reality. The set of malware was divided into three groups according to the collection date, as follows::

- ✓ 100 (one hundred) malware collected on the day of the start of testing;
- ✓ 100 (one hundred) malware collected no more than 6 (six) months before the start of testing;
- ✓ 100 (one hundred) malware collected more than 6 (six) months before testing started.

Within each sample, the selection of the specimens was randomly performed.

Benign files selection criteria

To measure the rate of false positives, files from well-known manufacturers in the Brazilian market were chosen. In this way, 300 benign (non-malicious) files from the manufacturers Microsoft, Adobe, Sun and Corel were selected.

Testbed features

The files were analysed without extension to measure the anti-malware's ability to discern files of unknown types. The malicious file has been renamed with the malicious file's MD5 hash. Files with the extension.EXE files were used to measure the anti-malware's ability to analyse executable files. Files with the extension ".DOC" was aimed at measuring the anti-malware's ability to analyse files of different types. Files with random extensions were used, including non-existent extensions and file extensions related to files that should not be infected by malware, such as ".TXT", ".Log" and ".BMP". The goal is to measure the anti-malware's ability to discern files by the real file type. A part of the test suite was of files compressed with the UPX compactor, to measure how anti-malware behaves in this type of situation. UPX (OBERHUMER, et al., 1996) is a program that compresses the executable and still maintains its functionality. According to the Trustwave report (Trustwave, 2012), more than 50% of malware uses this compactor as an obfuscation technique to circumvent anti-malware system protections. The observation is there was no recursive compression. Finally, the benign files were renamed in the same way as the malicious files and were placed together with the malicious files on the testbed. Binary files of malware equal to those captured on the Brazilian Internet;

Performance indicators

Performance tests were performed shortly after the anti-malware system was installed. The test machine had its performance evaluated with boot-time software (Planet Soft, 2012), PassMark AppTimer (PassMark Software, 2010) and Performance Test (PassMark Software, 2014).

The tests were evaluated in 4 questions, which were:

1. Time at the start of the operating system (Boot);
2. Hardware performance (CPU, Video, Memory and Disk);
3. Performance in opening applications;
4. Performance in copying, compressing and unpacking files.

Table 1- Resume of files tested.

		Test files					
Quantity	Description	Binary file	No extension	.doc	.exe	Random extension	UPX compacted
100	Malware collected at beginning of test;	100	100	100	100	100	100
100	Malware collected at maximum six months before tests	100	100	100	100	100	100
100	Malware collected more than six months at the beginning of tests	100	100	100	100	100	100
300	Non malicious files .txt, .bmp and similar	300					

Preprint submitted sep/2020 to Journal of Applied Security Research WASR-2020-0066R1 acepted 16/07/2022
Article DOI: 10.1080/19361610.2022.2104104
To publish in the Journal: Journal of Applied Security Research - Journal ISSN: 1936-1629

Total		600	600	600	600	600	600

V. EVALUATION RESULTS

Detection rate

The result tested anti-malware systems showed detection rates around 45% Figure 2 when they analysed the binary files of the malware, i.e., a little more than half of the malware tested was not detected.

In the detection test in the filegroup: no extension, extension ". DOC", extension ".EXE", random and compressed extension with UPXs the average detection rate was 48.0%, 48.1%, 48.2%, 48.2% and 12.5%, respectively (Figure 3).

Testing

Six (6) detection tests were performed with the malware population. For detection tests, malware and benign files were organized as shown in Table 1**Erro! Fonte de referência não encontrada.**:

Concerning the false positive rate, only two anti-malware classified as malware the benign files. Anti-malware C and D classified 5 (five) and 4 (four) files, respectively as malware.

Finally, Figure 4 demonstrates a distribution of the detection rate of malware according to the date of detection. With malware collected on the day of the test, the detection rate varies around 20%. For malware collected up to 6 months from the date of testing the result varies between 20% and 40%. Finally, malware collected more than 6 (six) months from the date of testing the detection rate is above 70%.

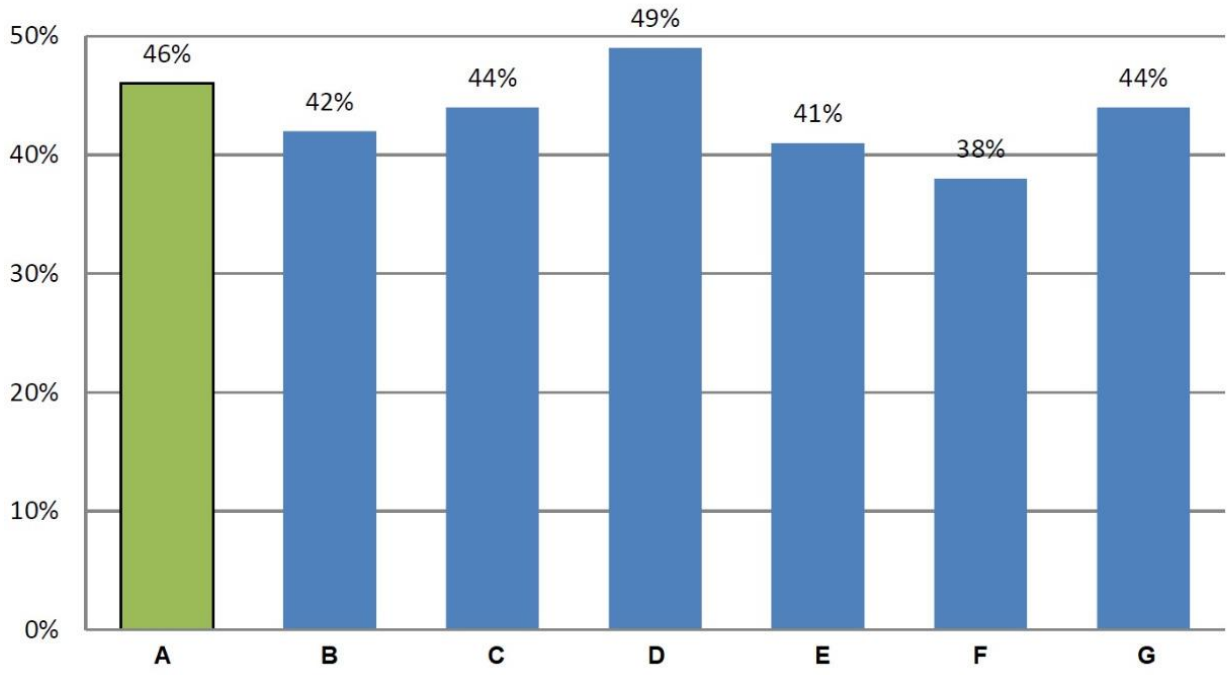

Figure 2 Comparison of binary file detection (The letters (A-G) identify the anti-malware manufacturers tested).

Preprint submitted sep/2020 to Journal of Applied Security Research WASR-2020-0066R1 acepted 16/07/2022
Article DOI: 10.1080/19361610.2022.2104104
To publish in the Journal: Journal of Applied Security Research - Journal ISSN: 1936-1629

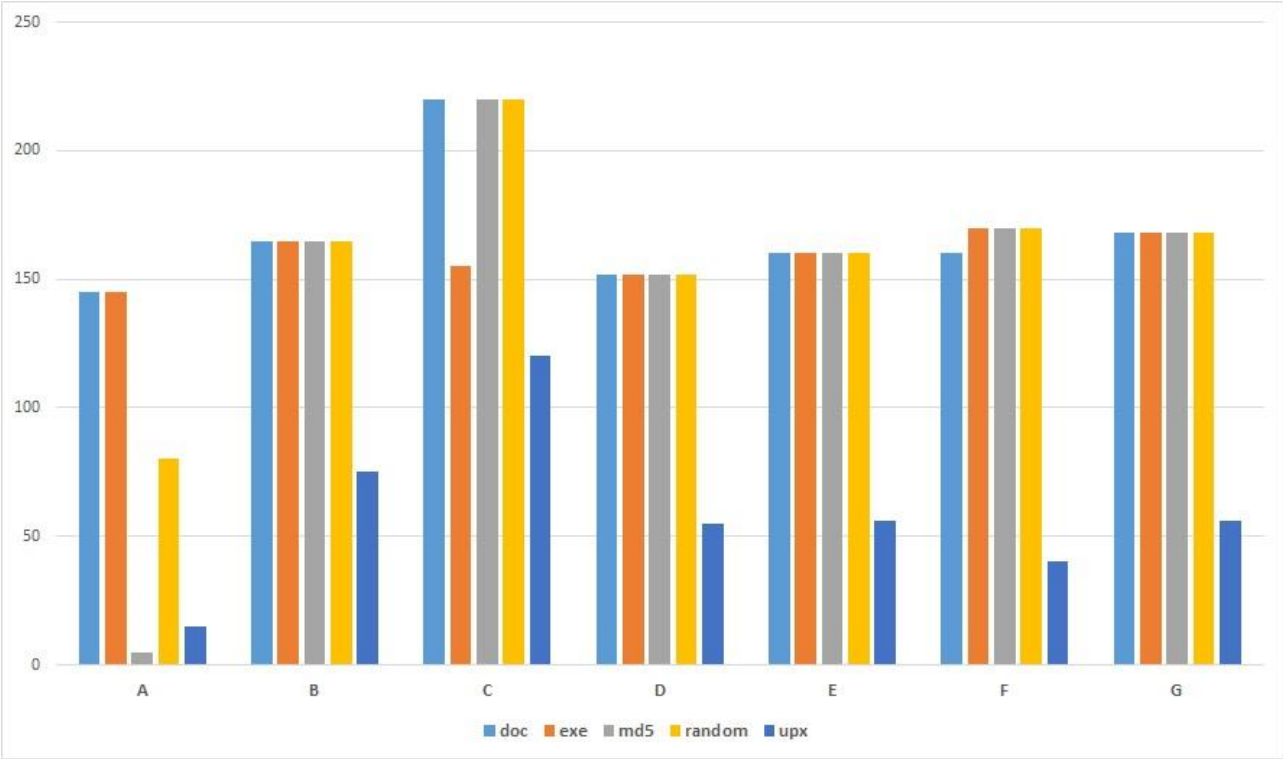

Figure 3 - Comparison of detection by extension changes.

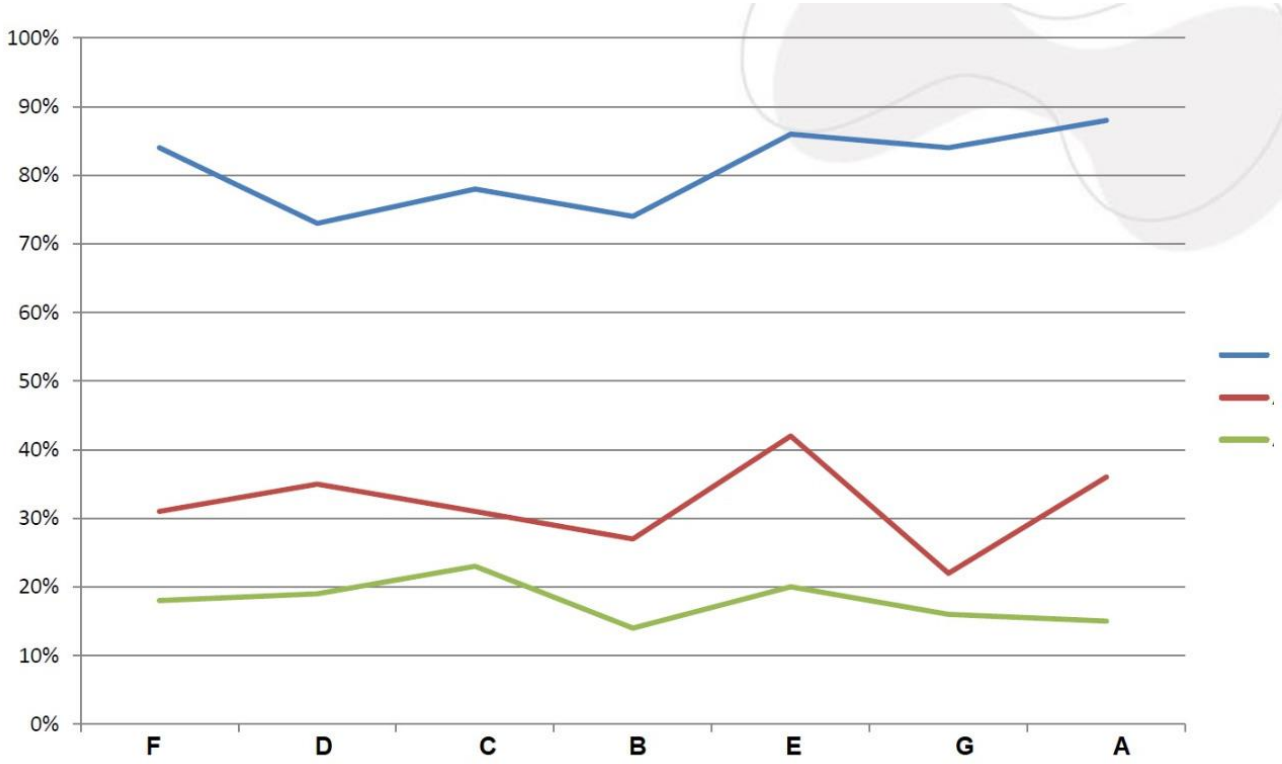

Figure 4 - Detection rate by long time samples (In the axis Y are expressed detection rate. The blue colour is malware collected for more than six months, red colour up to six months and green colour test date.

For the evaluation of each item, five consecutive tests were performed, and the results are represented by the measurements. Figs 5 to 8 graphically shows the test results. Figure *5* presents a comparison chart for initialization time, which deals with the time at the start of the operating system. In this regard, the measurements were quite varied with anti-malware systems, being the shortest initial time of the anti-malware system of 40 seconds.

Preprint submitted sep/2020 to Journal of Applied Security Research WASR-2020-0066R1 acepted 16/07/2022
Article DOI: 10.1080/19361610.2022.2104104
To publish in the Journal: Journal of Applied Security Research - Journal ISSN: 1936-1629

Hardware Performance

Figure *6* represents item 2, with information on hardware performance. In the hardware performance tests, anti-malware software showed similar results, except for anti-malware E, which had the lowest CPU consumption.

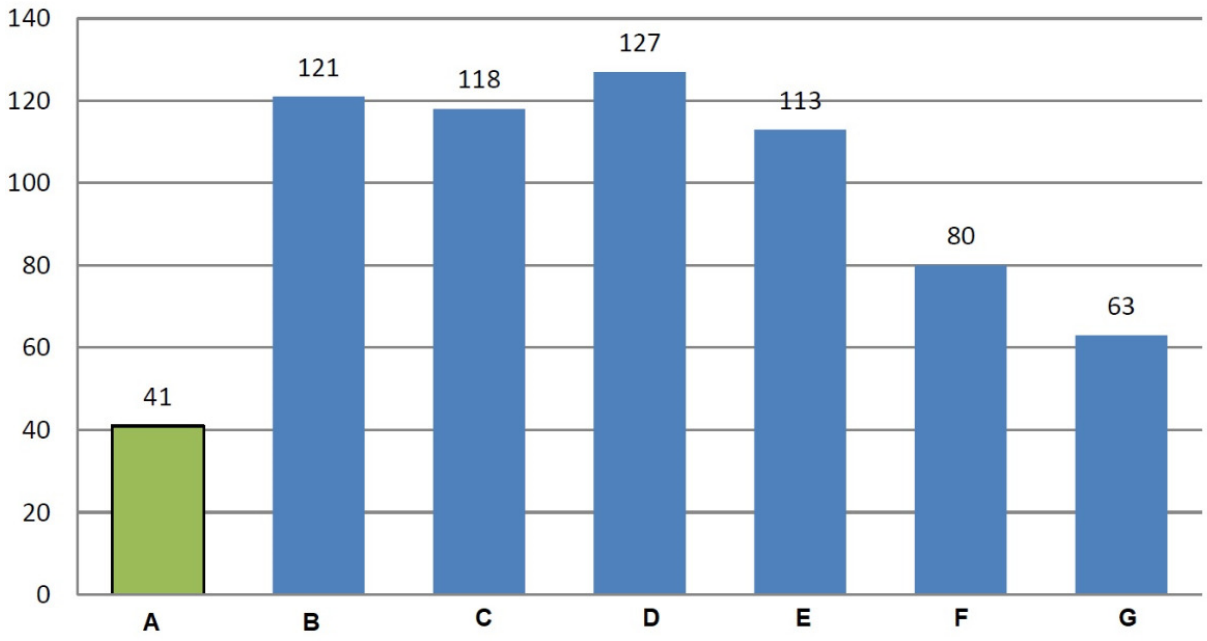

Figure 5 SO seconds to initialization

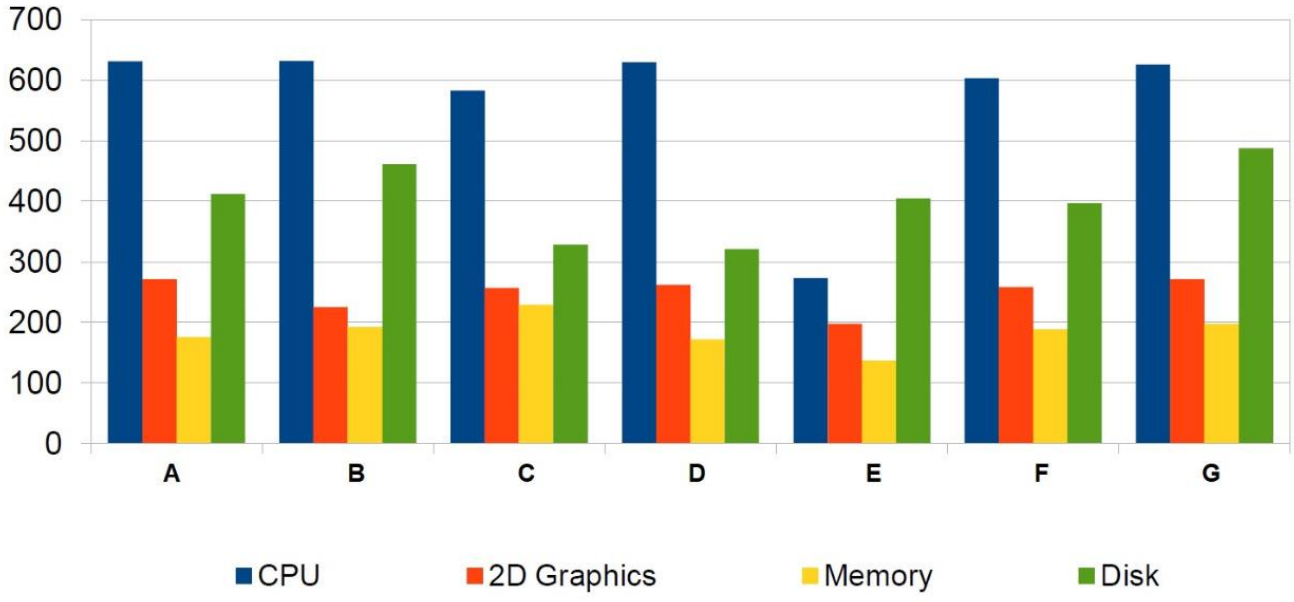

Figure 6 Hardware performance (In the Y-axis are expressed time in seconds).

Preprint submitted sep/2020 to Journal of Applied Security Research WASR-2020-0066R1 acepted 16/07/2022
Article DOI: 10.1080/19361610.2022.2104104
To publish in the Journal: Journal of Applied Security Research - Journal ISSN: 1936-1629

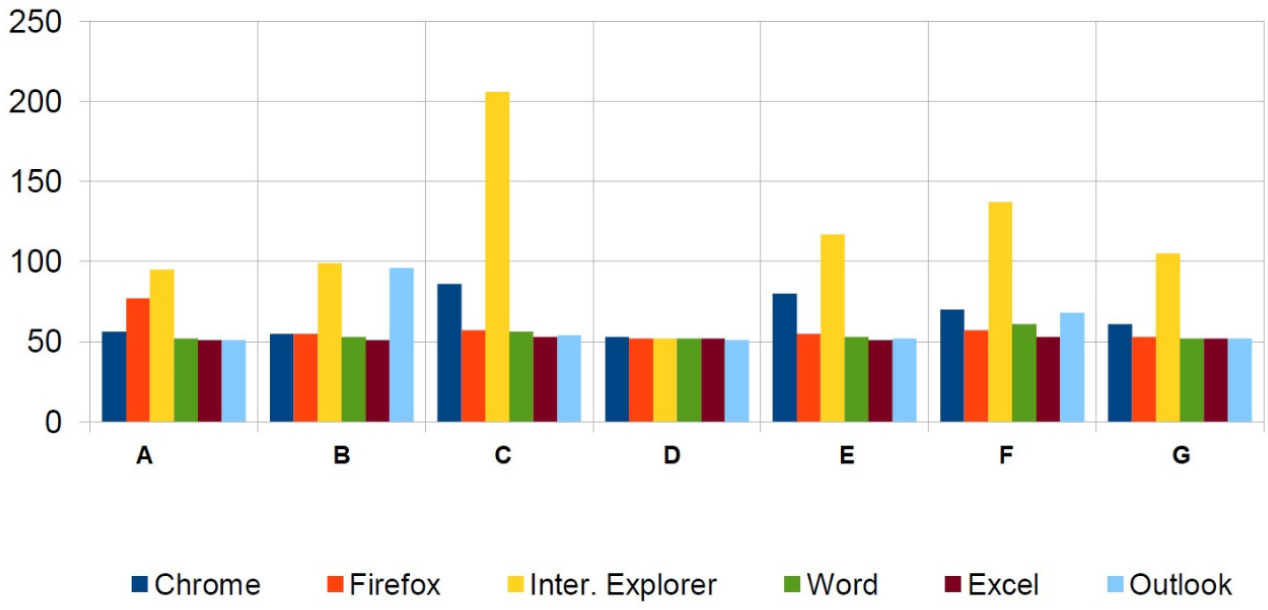

Figure 7 Applicative performance test (In the Y-axis are expressed time in seconds).

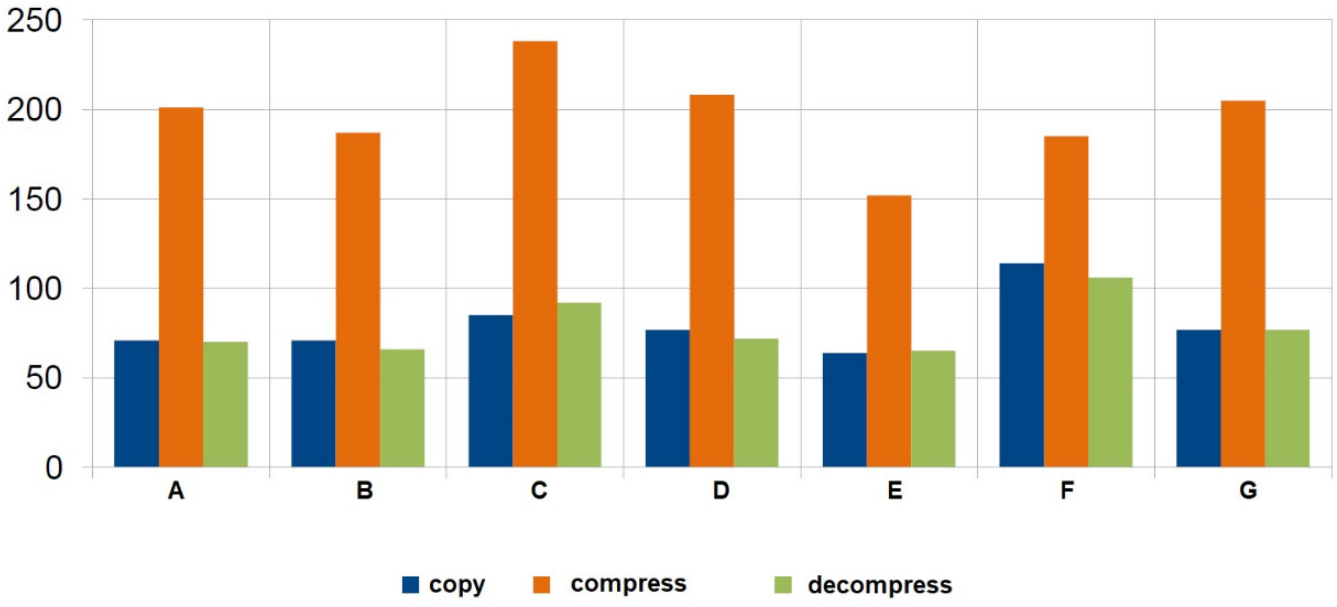

Figure 8 Compress and decompress test (In the Y-axis the time is expressed in second. Blue colour copy operation, orange colour compression and green colour unpacking)

Figure *7* Applicative performance test (In the Y-axis are expressed time in seconds).presents a comparative graph of the 3-performance item in the opening of applications. The applications considered common for the machines of Brazilian users were

Preprint submitted sep/2020 to Journal of Applied Security Research WASR-2020-0066R1 acepted 16/07/2022
Article DOI: 10.1080/19361610.2022.2104104
To publish in the Journal: Journal of Applied Security Research - Journal ISSN: 1936-1629

used: Internet Explorer, Apache OpenOffice 3.4, Adobe Acrobat Reader, Adobe Flash Player, Java 7, DirectX 9, Microsoft Office Home and Busines 2010, Firefox and Chrome. Also, windows firewall and automatic updating have been disabled.

Performance in copying, compression, and unpacking.

Figure *8* **Erro! Fonte de referência não encontrada.**demonstrates performance in copying, compressing and unpacking files. In the observation, it may be verified that the anti-malware products did not introduce significant load to the computers used in testing.

VI. DISCUSSION

In the evaluation of anti-malware systems, the existing methods or methodologies (II. RELATED METHODS) present different and very varied results from those found in the measurements presented here.

About detection rates, the results are discrepant. Other methods and methodologies disclose detection rates close to perfection. However, in a real test based on the Brazilian Internet, the image obtained is different. In malware detection testing the detection rate is close to 50%, that is, only half of the population is detected and classified as malware, a very different value when compared to those rates disclosed by other methods. Surely, any malware that crosses the anti-malware protection barrier may cause harmful consequences by endangering the availability, integrity, confidentiality and authenticity of the information.

A curious fact is the one demonstrated in Table 2, because, contrary to what was expected, the systems underwent an optimization after the installation of anti-malware software. However, further understanding of the subject is necessary to pacify possible variables not addressed by the.

Table 2 – Comparison of the system with anti-malware and system without anti-malware

Test (seconds)	Without anti-malware	Anti-malware present
Pass Mark 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

By changing the malicious files by changing the extension so that the different approaches of detection of anti-malware can be tested, the average detection for the test population is around 50%. Again, only half of the malware was detected. Alarmingly, when a well-known compression was used in malware, UPX, the result is catastrophic, because the average detection and classification is around 20%. The observation is that UPX compression is *an obfuscation technique used to evade anti-malware and widely used among malware manufacturers as reported by Trutwave* (Trustwave, 2012) and by Rubira Branco (BRANCO, et al., 2012).

By analysing the results of the detection test, we can infer questions that are attracted to the problem of Brazilian cyber defence. The technologies present in anti-malware software solutions and offered in the domestic market, are acquired from international companies. These software solutions are available in proprietary source code applications and established under the aegis of patents. Anti-malware software is critical, invasive solutions and has full access to information that travels on national IT equipment. Due to the operational and functional characteristics, the model of tracking, capturing and updating the software is not the user's domain as the information is treated or used by manufacturers of anti-malware software. Besides, the unquestionable belief in independent testers contributes to the weakening of cyber defence. In a recent study promoted by the Ponemon Institute (Ponemon Institut, 2014), revealed that security professionals have poor systems in terms of protection against digital attacks and data leaks. Thus, there is a need for security professionals to have access to the best defences and intelligence against threats.

Concerning performance analysis, Denning (DENNING, 1987) stated the following desirable feature for a system responsible for detecting intrusions: its operation of the detection system must impose a minimum load on the computer on which it is installed. This is the objective of evaluating the performance of the anti-malware system to identify possible overload that interferes with the operation of the machine. By analysing the graphs explained by Fig. 6 to 9, we can conclude that the various anti-malware, on average, did not insert debilitating load into the test system. After the considerations made in this Section, the

Preprint submitted sep/2020 to Journal of Applied Security Research WASR-2020-0066R1 acepted 16/07/2022
Article DOI: 10.1080/19361610.2022.2104104
To publish in the Journal: Journal of Applied Security Research - Journal ISSN: 1936-1629

validation and testing of anti-malware systems gain importance and support the insertion in the work agenda of a national research institution exempt and committed to the security of Brazilian information.

VII. CONCLUSION

Cyber threats are a big nightmare for companies around the world and may have evolved to make hacking more sophisticated. When we refer to viruses, Trojans and ransomware, we are dealing with types of malware. The consequences of the damage also vary according to the type of malware and the type of device infected, in addition to the nature of the data stored or accessed by the device. Choosing an efficient anti-malware software solution is crucial to protecting information from different institutions. A malware attack may profoundly affect business, government and armed forces, besides may be affected to its credibility. Anti-malware is considered an essential tool for preserving today's world businesses.

However, the efficiency of anti-malware is often questioned mainly by the inability to detect malware in different regions of the world. The main hypothesis is that the systems have particular configurations to accommodate different businesses and hackers have different objectives. Cyber protection depends intrinsically on four factors: technology, people, processes and the environments of use, so the article is justified with the insertion of an autochthonous Brazilian method.

The Brazil method confirmed the reality of evaluating the different known methodologies, showing a scenario focused on Brazil with a figure of efficiency different from that presented by the various traditional testers. Traditionally, Brazilians are known to have great creativity in solving complex problems and thus Brazilian malware may go through different stages and processes in their design, which goes beyond simple activities of recycling and adjusting old international artefacts. Brazilian malware is specific and is often not catalogued by international laboratories. Financial institutions in Brazil are made up of five large banks that force criminals to adjust to the specifics of local systems.

The Brazil method made it possible to visualize an interesting panorama, as only 50% of the population of malware collected on the Brazilian Internet were detected by anti-malware commercially available in Brazil. In this context, the Brazil method of anti-malware assessment confirmed to be an anti-malware assessment solution based on the reality of Brazilian cyber threats. This statement proved, therefore, that the national anti-malware solution was more efficient than the other anti-malware.

This article shows that the use of a local malware database, methodology oriented to the reality of local threats, testing of software by public entities and validating contracts based on technical efficiency is the best way to make public governance effective. The Brazil method received an honourable mention from the Federal Court of Accounts[2] for software purchase processes by the Brazilian State in 2012.

VIII. REFERENCES

Anti-Malware-Test.com, 2012. *ANTI-MALWARE TEST Tests Methodologies.* [Online]
Available at: http://www.anti-malware-test.com/node/198
[Accessed 19 07 2020].

AV COMPARATIVES, 2014. *AV COMPARATIVES File Detection Tests.* [Online]
Available at: https://www.av-comparatives.org/tests/file-detection-test-september-2014/
[Accessed 19 07 2020].

AV Test, 2014. *AV Test - Test Procedures. The Independent IT- Security Institute.* [Online]
Available at: https://www.av-test.org/en/about-the-institute/test-procedures/
[Accessed 19 07 2020].

Bai, L. et al., 2019. The Software Gene-Based Test Set Automatic Generation Framework for Antivirus Software. *JSW*, 4(10), pp. 449-456.

BRANCO, R. R., BARBOSA, G. N. & NETO, P. D., 2012. *Scientific but Not Academical Overview of Malware Anti-Debugging, Anti-Disassembly and Anti-VM Technologies.* Las Vegas, Black Hat Conference.

Check Point Sofware Technologies Ltd, 2014. *Check Point Security Report 2014.* [Online]
Available at: https://www.checkpoint.com/documents/ebooks/security-report-2014/files/assets/common/downloads/Check%20Point%20Security%20Report%202014.pdf
[Accessed 19 07 2020].

Consumer Watch, 2015. *Testing firm picks Kaspersky and Bitdefender as the best antivirus suites of 2015.* [Online]
Available at: http://web-a-ebscohost.ez106.periodicos.capes.gov.br/ehost/pdfviewer/pdfviewer?vid=0&sid=921b44a4-4174-45ae-8223-4562b8458cf5%40sdc-v-sessmgr02

[2] https://tcu.jusbrasil.com.br/jurisprudencia/316046265/3733820110/inteiro-teor-316046287 search for keyword Caso 7. CCOMGEX

Preprint submitted sep/2020 to Journal of Applied Security Research WASR-2020-0066R1 acepted 16/07/2022
Article DOI: 10.1080/19361610.2022.2104104
To publish in the Journal: Journal of Applied Security Research - Journal ISSN: 1936-1629

[Accessed 20 07 2020].
DELAMARO, M. E., MALDONADO, J. C. & JINO, M., 2007. *Introdução ao Teste de Software (in Portuguese).* 1 ed. Rio de Janeiro: Elsevier.
DENNING, D. E., 1987. An Intrusion-Detection Model. *IEEE TRANSACTIONS ON SOFTWARE ENGINEERING*, 13(2), pp. 222-232.
Escola Superior de Guerra, 2014. *BRASIL : ESCOLA SUPERIOR DE GUERRA. Manual Básico, vol I, Elementos Fundamentais. (in Portuguese)*, Rio de Janeiro: s.n.
EUROPEAN EXPERT GROUP FOR IT-SECURITY, 2020. *EICAR.* [Online]
Available at: www.eicar.org
[Accessed 19 07 2020].
Filiol, E., 2005. *Computer viruses: from theory to applications.* France: Springer Verlag .
FLEISHMAN, G., 2018. BITDEFENDER ANTIVIRUS FOR MAC: A PERFORMANCE JUMP MAKES IT FAR MORE RELIABLE. *MacWorld,* Volume August, pp. 93-97.
Hachman, M., n.d. *The Best Windows 8.1 Antivirus Software.* [Online]
Available at: http://web-a-ebscohost.ez106.periodicos.capes.gov.br/ehost/pdfviewer/pdfviewer?vid=1&sid=71fc32f5-c75d-48b3-aff1-8bc45bf482be%40sdc-v-sessmgr01
[Accessed 20 07 2020].
ICSA Labs, 2014. *ISCA LABS. ICSA Labs Anti-Virus Certification Test Matrix.* [Online]
Available at: https://www.icsalabs.com/technology-program/anti-virus/av-monthly-testing-reports
[Accessed 19 07 2020].
Ludwig, M., 1995. *The Giant Black Book of Computer Viruses.* Show Low, Arizona: American Eagle Publications, Inc..
Ludwig, M. A., 1993. *Computer Viruses, Artificial Life and Evolution.* Tucson, Arizona: American Eagle Publications, Inc..
Montes, A. et al., 2014. *Aplicação do método Brasil de avaliação de anti-malware e as repercuções para a defesa cibernética (in Portuguese).* São José Dos Campos, s.n., pp. 177-182.
Nissim, N., Moskovitch, R., Rokach, L. & Elovici, Y., 2014. Novel active learning methods for enhanced PC malware detection. *Expert Systems with Applications*, pp. 5843-5857.
NSS Labs, 2018. *NSS LABS. Endpoint Protection – Evasion and Exploit: Test Methodology.* [Online]
Available at: https://www.nsslabs.com/reports/evasions-test-methodology-v1-1/
[Accessed 19 07 2020].
Nurhayati, A., Gautama, A. & Naseer, M., 2018. *Decision making model design for antivirus software selection using Factor Analysis and Analytical Hierarchy Process.* s.l., s.n., pp. 1-6.
Paganini, P., 2014. *PAGANINI, P. Impact of Windows XP End of life on Critical Infrastructure.*. [Online]
Available at: http://securityaffairs.co/wordpress/25984/security/xp- critical-infrastructure.html
[Accessed 19 07 2020].
PassMark Software, 2010. *App Timer application's startup time.* [Online]
Available at: http://www.passmark.com/products/apptimer.htm
[Accessed 03 03 2014].
PassMark Software, 2014. *PerformanceTest Software.* [Online]
Available at: http://www.passmark.com/download/pt_download.htm
[Accessed 03 03 2014].
Planet Soft, 2012. *Planet Soft.* [Online]
Available at: http://www.planetsoft.org
[Accessed 03 03 2014].
Ponemon Institut, 2014. *Expondo as Lacunas da Cibersegurança: Brasil.* [Online]
Available at: http://www.websense.com/assets/reports/report-ponemon-2014-part1-summary-brazil-pt.pdf
[Accessed 07 07 2014].
Ruiz, R., Winter, R., Park, K. & Amatte, F., 2015. *Apoc@lypse: The end of antivirus.* North Charleston: North Charleston: CreateSpace Independent Publishing Plataform.
Shevchenko, S. M., Skladannyi, P. M. & Martseniuk, M., 2019. ANALYSIS AND RESEARCH OF THE CHARACTERISTICS OF STANDARDIZED IN UKRAINE ANTIVIRUS SOFTWARE. *Cybersecurty: Education, Science, Technique*, 4(4).
Trustwave, 2012. *Global Security Report - United States Secret Service.*. [Online]
Available at: www.secretservice.gov/Trustwave_WP_Global_Security_R eport_2012.pdf

Preprint submitted sep/2020 to Journal of Applied Security Research WASR-2020-0066R1 acepted 16/07/2022
Article DOI: 10.1080/19361610.2022.2104104
To publish in the Journal: Journal of Applied Security Research - Journal ISSN: 1936-1629

[Accessed 20 07 2014].
Valdi, A. et al., 2015. Scalable Testing of Mobile Antivirus Applications. *Computer*, 48(11), pp. 60-68.
Virus Bulletin, 2014. *Virus Bulletin Testing Methodology.* [Online]
Available at: https://www.virusbtn.com/vbspam/methodology/index
[Accessed 10 04 2014].
West Coast Labs, 2014. *WEST COAST LABS. Technology Reports.* [Online]
Available at: http://www.westcoastlabs.org
[Accessed 10 02 2014].
Winter, R. & Ruiz, R., 2017. Cyber Autoimmune Disease When the Virtual Life Imitates the Real Life. *International Journal of Cyber-Security and Digital Forensics*, Volume 7(1), pp. 21-30.