Serviços de Antivírus e *Antimalwares* – Análise Comparativa de Sistemas, Identificação de Vulnerabilidades e das Correspondentes Medidas de Mitigação

Jéssica Pedrosa
2180067@my.ipleiria.pt
Mestrado em Cibersegurança e Informática Forense, Escola Superior de Tecnologia e Gestão

Patrícia Silva
2180068@my.ipleiria.pt
Mestrado em Cibersegurança e Informática Forense, Escola Superior de Tecnologia e Gestão

Resumo

Os antivírus e *antimalwares* são aplicações que permitem detetar, prevenir e eliminar *malwares*. Existe uma enormidade de *malwares*, pudendo estes serem classificados em vários tipos, variando no tipo de danos que causam, propósito que têm e como funcionam. Daí estes tipos de programas serem de extrema importância, ainda mais nos dias de hoje. Assim, com o presente artigo, pretende-se explicar alguns conceitos relacionados com este vasto tema, algumas das formas de funcionamento destes *software*, e ainda a realização de testes de modo a exemplificar os conceitos apresentados.

Palavras-chave—Antivírus, *Antimalware*, *Malware*

1 Introdução

Os *malwares* já existem desde os finais dos anos XX, sendo que as primeiras teorias de autorreplicação automática apareceram em meados do ano 1970. Um dos primeiros tipos de *malwares* a aparecer foram os que viriam mais tarde a ser conhecidos como vírus. Um exemplo clássico é o caso do *Elk Cloner*, que surgiu em 1982, criado por Rich Skrenta. Este vírus, apresentava, nos computadores infetados, um "poema", a cada 50 vezes que o computador era executado com uma disquete infetada. No entanto, só em 1984 é que Frederick B. Cohem utilizou o termo vírus informático, pela primeira vez, num estudo. Mas já antes existiram outros códigos maliciosos, como o *Rabbit*, mais considerado um *fork bomb*, em 1974. [1]

Como se pode ver, estes tipos de ameaças não são novas, mas cada vez mais são uma preocupação por diversos motivos. Afinal, estas foram-se multiplicando a um ritmo assustador. Com o surgimento e globalização da internet, novas formas de ameaças e meios de propagação surgiram. Com o aparecimento destas ameaças, surgiu também *software* que permitisse proteger os sistemas das empresas e dos utilizadores "normais" da Internet. Os primeiros *software* a aparecer foram os antivírus, vocacionados para a proteção e eliminação de vírus, pois eram os mais comuns de se encontrar. Mas, nos dias de hoje, a realidade é outra e os vírus são uma das minorias do tipo de *malware* agora usado. Com o aparecimento de novos tipos de *malwares*, acabaram por ser criado os *antimalwares*, para dar resposta às novas ameaças.

Assim, com este artigo, ir-se-á explorar alguns conceitos deste vasto tema e exemplificar, através de testes, os conceitos abordados.

Na secção 2 são explicados alguns conceitos fundamentais para este artigo. Na secção 3 são apresentadas as ferramentas utilizadas para os testes, na secção 4 o *setup* dos mesmos e na secção 5 os testes efetuados. Na secção 6 são apresentados e discutidos os resultados obtidos. Na secção 7 são apresentadas as conclusões e por último, a secção 8 corresponde à bibliografia.

2 Conceitos Fundamentais

Malware não é nada mais que um código ou *software* malicioso que tem o objetivo de criar e/ou explorar vulnerabilidades num sistema. Este tipo de *software* pode criar *backdoors*, permitir acesso remoto a utilizadores não autorizados, eliminar dados entre muitas outras coisas. O *malware* é um nome genérico e inclui vários tipos de ameaças, como os vírus, os *ransomwares*, os *trojans*, os *worms* e muitos outros.

Os vírus são programados para se ocultar no sistema de modo a tornar mais difícil a deteção e posterior remoção. Comportam-se de forma semelhante aos vírus biológicos, ou seja, precisam de um hospedeiro, replicam-se e esperam o momento certo para atacar. Podem infetar um executável e ativarem-se quando esse ficheiro é executado. Os *worms* são programas maliciosos, independentes, que se espalham pelos sistemas através, por exemplo, da rede. Ao contrário dos vírus, este tipo de *malware*, é um programa completo, não sendo necessário, por exemplo, hospedar-se em ficheiros legítimos. Os *trojans* passam-se por *software* legítimo, e, enquanto fazem o que é esperado deles, também executam outras funções maliciosas, sem o conhecimento do utilizador. Os *ransomwares* limitam as funcionalidades de um sistema, pedindo, posteriormente, algum tipo de resgate para que o sistema volte ao seu normal funcionamento. [2]

Os primeiros antivírus que surgiram tinham como principal objetivo proteger contra vírus informáticos. Contudo, o aumento considerável da diversidade de ameaças possíveis levou ao surgimento de outros tipos de *malware*, para além dos vírus. Assim, de modo a combater algumas destas novas ameaças, os antivírus passaram a apresentar algumas funcionalidades que permitissem não só a deteção de vírus como também a deteção de alguns *malwares*. Deste modo, para uma proteção mais extensiva foram criados os *antimalwares*. Estes são *software* que protegem contra uma maior gama de tipos *malwares*, detetando-os e, por sua vez, removendo-os. [3]

Aquando o surgimento dos antivírus e *antimalwares*, ambos se referiam a dois conceitos divergentes. Contudo, nos dias de hoje, pode-se considerar que antivírus e *antimalware* são semelhantes apesar de existirem ligeiras diferenças entre estes conceitos, como por exemplo, a gama mais alargada de deteção de *malwares* dos *antimalwares* comparativamente aos antivírus. [3]

Independentemente de ser usado um antivírus ou um *antimalware*, para a deteção de *malware*, existem várias técnicas diferentes. Exemplos dessas mesmas técnicas são a baseada em assinaturas, a baseada em comportamento e a baseada em heurísticas.

No que diz respeito à técnica baseada em assinaturas, esta é excelente para a deteção de *malware* já conhecido. A esta mesma técnica está associada a existência de uma base de dados com assinaturas, sendo que cada assinatura corresponde a um *malware*. Sempre que for detetado um novo *malware*, a sua assinatura terá de ser adicionada à base de dados; deste modo, para que o *software* de prevenção tenha conhecimento deste novo *malware*, é necessário que a sua base de dados de assinaturas seja atualizada. Um *software* cujo funcionamento seja baseado nesta técnica, sempre que encontre algo suspeito, compara com o conteúdo presente na base de dados. Só se existir correspondência é que o *software* "irá ativar o alarme". [4] Uma das vantagens conhecidas desta técnica passa por apresentar um número reduzido de falsos positivos, uma vez que, dado que a comparação é efetuada com a assinatura de *malwares* já conhecidos e confirmados, na maioria das vezes em que deteta algo como ameaça é de facto uma ameaça. Já uma das desvantagens é a eventualidade de a base de dados não se encontrar atualizada. [5]

Já no caso dos *software* de deteção de *malware* baseados em comportamento, estes têm como objetivo detetar *malware* desconhecido. Assim, estes *software* de deteção irão monitorizar o comportamento do *software* de modo a verificar se o mesmo apresenta alguma atividade suspeita. A esta técnica encontram-se associados os conceitos de normal e anormal no sentido de que, caso a ação executada pelo *software* seja considerada anormal, então há alguma probabilidade de a mesma corresponder a uma ação não autorizada. [5] Uma das principais vantagens associadas a esta técnica de deteção é a possibilidade de detetar a presença de *malwares* desconhecidos. Contudo, um *software* baseado nesta técnica irá gerar um número elevado de falsos positivos, uma vez que pode ocorrer o caso de detetar algo como uma ameaça e despoletar o alarme, mas, na verdade, não o ser. [6]

Por fim, no que se refere à técnica baseada em heurísticas, esta consiste na utilização de regras e/ou algoritmos com o objetivo de procurar características que apresentem alguma intenção maliciosa. É importante mencionar o facto de alguns métodos inerentes a esta técnica serem capazes de detetar *malware* sem o auxílio da técnica baseada em assinaturas. Assim, para uma deteção com mais alguma garantia, muitas

vezes, os *software* de deteção de *malware* acabam mesmo por usar tanto a técnica baseada em assinaturas com a baseada em heurísticas. [7]

3 Ferramentas Utilizadas

De modo a se implementar os vários cenários de teste criados, foi necessário escolher ferramentas de deteção de *malware*. Para tal foi necessário realizar uma pesquisa acerca dessas ferramentas e, por sua vez, analisar as suas características e o seu funcionamento. De seguida, irão ser apresentadas as ferramentas selecionadas para o efeito tendo em consideração as informações mais recentes que se encontram disponíveis.

Os antivírus tradicionais efetuam uma comparação com a sua base de dados local de assinaturas, de modo a detetar a existência de algum tipo de ameaça. Contudo, estas comparações podem apresentar algumas consequências, como prejudicar a *performance* do computador. Deste modo, surgiram os antivírus *cloud-based*. Estes têm as suas bases de dados remotamente o que faz com que não só estejam constantemente atualizadas como também as comparações não serão efetuadas no próprio dispositivo. [8]

3.1 Microsoft Security Essentials (MSE)

O *Microsoft Security Essentials* é um antivírus gratuito da *Microsoft* para os sistemas operativos *Windows Vista* e *Windows 7*. O funcionamento deste antivírus é baseado principalmente em assinaturas. Contudo, também utiliza a técnica baseada em heurísticas que, por sua vez, se encontra relacionada com a opção *Real-time protection.* [9]

3.2 AVG AntiVirus Free

O *AVG AntiVirus Free* é um *software* de deteção produzido pela *AVG Technologies*. De acordo com a informação encontrada num *White Paper da AVG* (https://aa-download.avg.com/filedir/other/pf_wp-90_A4_us_z3162_20091112.pdf), e após a análise do mesmo, concluiu-se que o método de funcionamento deste antivírus assenta em assinaturas, em heurísticas e ainda em comportamento.

3.3 Bitdefender

Através da análise de um *White Paper* do *Bitdefender* (https://www.bitdefender.com/files/Main/file/BitDefender_Antivirus_Technology.pdf) e de alguma da informação presente no site oficial, o antivírus *Bitdefender* é um *software* de deteção que também têm como base de funcionamento três técnicas – assinaturas, heurísticas e ainda comportamento.

4 Setup

Antes de se iniciar a execução dos cenários de teste, foi necessário definir o *setup*. Assim, em primeiro lugar, foi selecionada uma máquina virtual. A informação do sistema operativo da máquina virtual encontra-se na Figura 1, e, como se pode ver, é um *Windows 7*.

Item	Value
OS Name	Microsoft Windows 7 Enterprise
Version	6.1.7601 Service Pack 1 Build 7601
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	IE8WIN7
System Manufacturer	innotek GmbH
System Model	VirtualBox
System Type	X86-based PC
Processor	Intel(R) Core(TM) i7-6500U CPU @ 2.50GHz, 2592 Mhz, 1 Core(s), 1 Logical Processor(s)
BIOS Version/Date	innotek GmbH VirtualBox, 12/1/2006
SMBIOS Version	2.5
Windows Directory	C:\Windows
System Directory	C:\Windows\system32
Boot Device	\Device\HarddiskVolume1
Locale	United States
Hardware Abstraction Layer	Version = "6.1.7601.17514"
User Name	IE8WIN7\IEUser
Time Zone	Pacific Standard Time
Installed Physical Memory (RAM)	Not Available
Total Physical Memory	2.50 GB
Available Physical Memory	988 MB
Total Virtual Memory	5.00 GB
Available Virtual Memory	3.96 GB

Figura 1 - Dados do sistema operativo

Serão usados 3 antivírus, com várias versões. De seguida, encontram-se especificados os mesmos e as suas versões.

4.1 AVG

Antes de se fazer *update*. Para efeitos deste artigo, dar-se-á pelo nome *AVG-1*:
- AVG Version e Program Version: 8.5.420
- Virus database version: 270.13.111/2391
- Release date: 23 de setembro de 2009

Após se fazer *update*. Para efeitos deste artigo, dar-se-á pelo nome *AVG-2*:
- AVG Version e Program Version: 8.5.445
- Virus database version: 271.1.1/5970
- Release date: 6 de julho de 2013

4.2 AVG de 2019

Para efeitos deste artigo, dar-se-á pelo nome *AVG-3*:
- Software Version: 18.8.3071 (build 18.8.4084.0)
- Virus definitions version: 181214-4
- UI version: 1.0.134
- Number of definitions: 5473576

4.3 Bitdefender

- Antivirus Free Edition: 1.0.14.74
- Engine Version: 7.78352

4.4 MSE

- Antimalware Client Version: 4.10.209.0
- Engine Version: 1.1.15500.2
- Antivirus definition e Antispyware definition: 1.283.577.0

Os *malwares* foram tirados de um repositório de amostras de *malwares*, produzida pelo projeto *theZoo*, que se encontra em http://thezoo.morirt.com/. De seguida, encontram-se os nomes dos *malwares* selecionados e a sua *hash*.

- *Worm – FannyWorm*
SHA256:
ce03f484268cd4fe9907f9b4474734590a6ed8eded5e87c07a340c75a40f3138
- *Trojan - Artemis*
SHA256:
834d1dbfab8330ea5f1844f6e905ed0ac19d1033ee9a9f1122ad2051c56783dc
- *Trojan - Dino*
SHA256:
427ece485005f1bd517b8f0c6c38a8f73bf32350795b83fb8cf937c86f99dfc8
- *Ransomware - Cerber*
SHA256:
e67834d1e8b38ec5864cfa101b140aeaba8f1900a6e269e6a94c90fcbfe56678
- *Ransomware – WannaCry*
SHA256:
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
- *Trojan - ZeusBanking* (26 de novembro de 2013)
SHA256:
69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169

5 Cenários de Testes

Como já foi referido, para os testes foram usados os 6 *malwares* e os 5 antivírus selecionados. Os antivírus foram instalados e o *scanning* efetuado à vez, na máquina virtual. Todo o processo de manipulação dos *malwares* foi realizado sem conexão à rede, sempre que possível, de forma a que os *malwares* não se espalhassem pela rede. Todos os

scannings foram efetuados na localização onde se encontravam os *malwares*.

Os *scannings* de todas as versões do *AVG* foram efetuados 2 vezes, uma com a opção heurísticas e a 2ª vez sem a opção heurísticas. O *scanning* do *MSE* também foi efetuado duas vezes, a 1ª vez com a opção *on-real time* selecionada e a última sem estar selecionada. Para comprovar a viabilidade dos *malwares* obtidos, os mesmos foram testados no *VirusTotal* (https://www.virustotal.com/), um *website* que permite obter *feedback* rápido em relação aos ficheiros que o utilizador considere suspeitos, uma vez que o *site* usa vários antivírus e *antimalwares* para dar uma resposta.

6 Apresentação e Discussão dos Resultados

Tal como já seria esperado, antes de se dar início aos testes propriamente ditos em cada *software* de deteção, foi instalado na máquina virtual, o antivírus necessário para cada cenário de teste. Após a instalação procedeu-se a uma breve exploração da *interface* do *software*. O processo de instalação em si também foi alvo de análise. Para tal, foram criadas duas métricas, correspondentemente, a usabilidade e a facilidade de instalação.

Tabela 1 - Métricas de usabilidade, facilidade de instalação e completude

	Usabilidade	Facilidade de Instalação	Completude
MSE	4	5	5/6
AVG-1	5	5	0/6
AVG-2	5	5	1/6
AVG-3	4	4	6/6
Bitdefender	4	3	6/6

Foi utilizada na Tabela 1, a escala de 1 a 5, sendo 1 nada fácil e 5 muito fácil, para a usabilidade e facilidade de instalação. Em relação à completude, esta refere-se ao número de ameaças que o *scanning* do antivírus encontrou, em relação ao número de ameaças existentes. Mais à frente voltar-se-á a esta métrica.

Em relação à facilidade de instalação, atribuiu-se 4 ao *AVG-3*, uma vez que se verificou que a instalação do mesmo foi demorada. No que diz respeito à instalação do *Bitdefender*, atribuiu-se 3 dado que, para que se possa usufruir do antivírus, o mesmo obriga à existência de uma versão recente do *browser Internet Explorer* (para este caso, a versão 11) e ainda exige ao utilizador criar/possuir uma conta no *Bitdefender*.

Em relação à usabilidade, deu-se 4 ao *MSE*, pois este não deixa efetuar o *scanning* sem estar atualizado. O *AVG-3* tem um 4 nesta métrica, pois não é possível através da *interface*, nesta versão, obter um histórico dos *scannings* efetuados. Apesar disso, na sua *interface*, existe uma opção que permite gerar relatórios, com formato *txt*, por exemplo, do *scanning* efetuado, o que permite, de certa forma, obter o histórico. Relativamente ao *Bitdefender*, a sua avaliação foi 4 pois a sua *interface* acaba por ser tão simplificada na zona onde se efetua os *scannings*, que é provável que um utilizador que nunca usou este antivírus, acabe por ter mais dificuldades, visto que em grande parte dos outros antivírus *free* no mercado, essa zona é diferente e com mais opções. No entanto, após se perceber o funcionamento, é um antivírus fácil e prático de se usar.

Após se proceder à instalação e exploração inicial dos antivírus, foram efetuados os *scannings* na localização dos *malwares*. Cada *scanning*, após a sua conclusão, mostra ao utilizador um relatório com os resultados obtidos. De seguida são apresentadas as imagens dos relatórios obtidos através do *MSE* (Figura 2) e através do *Bitdefender* (Figura 3). Através das imagens apresentadas, também se pode ter uma breve apreciação da *interface* dos antivírus, já discutida acima.

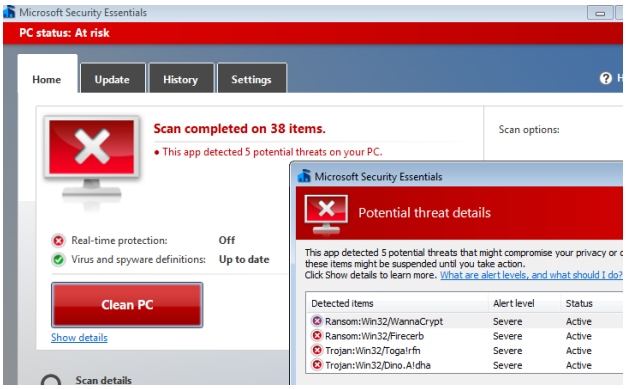

Figura 2 - Relatório do *MSE*

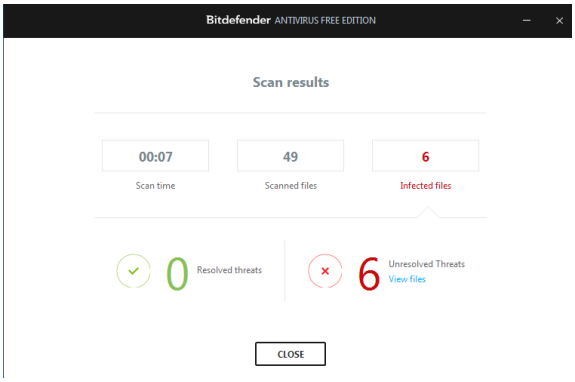

Figura 3 - Relatório do *Bitdefender*

De modo a facilitar a análise e a compreensão dos resultados obtidos nos testes efetuados foram definidas um conjunto de métricas, tendo em consideração o contexto em que se insere este trabalho. Assim, para além da usabilidade e da facilidade de instalação, foram definidas mais duas métricas, nomeadamente, a completude e a consistência.
Na Tabela 1, através da coluna referente à completude, pode-se concluir que os mais eficazes para as amostras selecionadas, foram o *AVG-3* e o *Bitdefender*. Em relação aos *scannings* efetuados pelas versões do *AVG* com a opção das heurísticas, o resultado foi exatamente o mesmo que sem a opção das heurísticas selecionada. Em relação à opção *on real-time* do *MSE*, o resultado foi igual nos 2 *scannings*.

Tabela 2 - Métrica consistência e resultados do *VirusTotal*

	Consistência	*VirusTotal*
Artemis	2/5	26/70
ZeusBanking	4/5	58/68
Cerber	3/5	56/69
WannaCry	3/5	61/68
FannyWorm	3/5	61/68
Dino	3/5	27/57

Entende-se neste trabalho, por consistência, como o número de antivírus que detetam a ameaça, em relação com a quantidade total de antivírus utilizados. Em relação à coluna designada por *VirusTotal*, falar-se-á dela mais tarde.

É importante referir, como se pode ver na Tabela 2, na coluna referente à consistência, que o *Artemis* só foi detetado no *Bitdefender* e no *AVG-3*. O *Cerber*, o *WannaCry*, o *FannyWorm* e o *Dino* não foram detetados no *AVG-2* e no *AVG-1* que, por sua vez, também não detetou o *ZeusBanking*.

Pode-se então concluir, que o *ZeusBanking* foi o único *malware* detetado pelo *AVG-2*. Isto pode ser explicado, através da atualização da base de dados de assinaturas que esta versão do *AVG* faz uso, pois uma versão mais antiga, como o caso do *AVG-1*, já não deteta esse *malware*, o que pode eventualmente significar que a sua assinatura não se encontra na base de dados. As Figura 4 e Figura 5 apresentam o relatório obtido no *AVG-1* e o obtido no *AVG-2*, respetivamente.

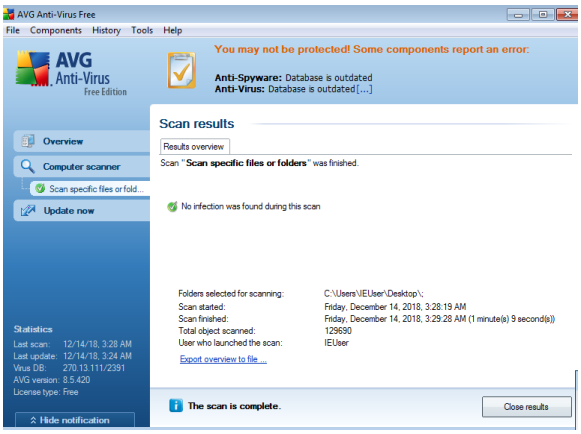

Figura 4 - Relatório do *AVG-1*

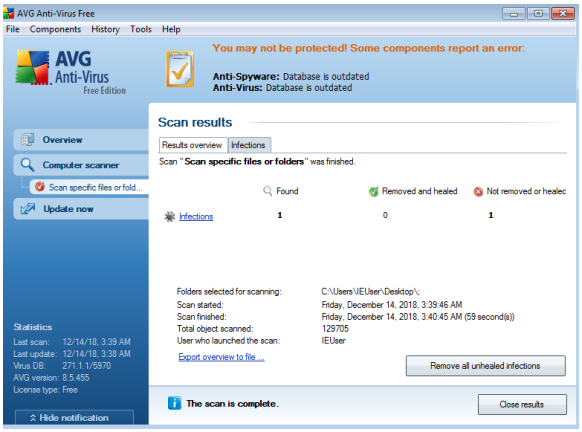

Figura 5 - Relatório do *AVG-2*

Para além disso, constata-se que o *malware Artemis* foi o menos detetado e o *ZeusBanking* o mais detetado pelos antivírus.

Estes *malwares* também foram testados no *VirusTotal* e os resultados encontram-se na Tabela 2, na referida coluna. Pode-se observar que o *Artemis* e o *Dino* são os que são menos detetados pelos vários antivírus e *antimalwares* que o *VirusTotal* usa. Perante este resultado não é surpreendente que o *Artemis* seja o *malware* menos detetado nos testes.

7 Conclusão

Atualmente, com o aumento das ameaças, os antivírus tentam, ao máximo, defender os dispositivos das mesmas. Para tal, estes acabam por apresentar mais do que uma forma de funcionamento. Pelos testes realizados, foi possível verificar que os antivírus mais recentes – *AVG-3* e *Bitdefender* – detetaram todos os *malwares* utilizados, ao contrário dos restantes, dado que esses correspondem a versões mais antigas, que surgiram numa altura em que alguns destes *malwares* ainda nem sequer existiam. Isto prova a ineficácia do *scanning* destas versões mais antigas perante ameaças desconhecidas à versão do antivírus.

Uma prova desta ineficácia e consequente diferença entre as versões do mesmo antivírus, foi a diferença do resultado fornecido pelo *AVG-1* e o *AVG-2*. O *AVG-2*, ao contrário do *AVG-1*, detetou um *malware*. Tal divergência possivelmente encontra-se relacionada com o facto de a assinatura digital desse *malware* não se encontrar na base de dados do *AVG-1* mas já estar na do *AVG-2*.

Uma das formas de mitigar os falsos positivos resultantes dos antivírus baseados em comportamento, consistiu em complementar os mesmos com as bases de dados de assinaturas. Contudo nos testes realizados neste trabalho, não foi possível verificar os efeitos desta medida de mitigação, dado que todas as amostras alvo de *scanning* eram já conhecidas.

Futuramente seria interessante perceber melhor o funcionamento das heurísticas nestes *software*, dado que nos resultados dos testes com e sem as mesmas, não se verificou qualquer diferença. Também seria interessante explorar o polimorfismo e outras técnicas utilizadas pelos *malwares* atuais para se "esconderem" e ainda o funcionamento e consequentes vulnerabilidades dos antivírus atuais.

8 Bibliografia

[1] Wikipédia, "Timeline of computer viruses and worms," [Online]. Available: https://en.wikipedia.org/wiki/Timeline_of_computer_viruses_and_worms. [Acedido em 19 dezembro 2018].

[2] Wikipédia, "Malware," [Online]. Available: https://pt.wikipedia.org/wiki/Malware#Diferen%C3%A7a_entre_v%C3%ADrus_e_worms. [Acedido em 19 dezembro 2018].

[3] C. Hopping, "What's the difference between antimalware and antivirus?," ITPRO, 6 junho 2018. [Online]. Available: https://www.itpro.co.uk/malware/28153/whats-the-difference-between-antimalware-and-antivirus-1. [Acedido em 19 dezembro 2018].

[4] Computer Hope, "How does an antivirus work?," 13 novembro 2018. [Online]. Available: https://www.computerhope.com/issues/ch001738.htm. [Acedido em 19 dezembro 2018].

[5] J. Martindale, "What is antivirus software and how does it work?," Digital Trends, 22 outubro 2018. [Online]. Available: What is antivirus software and how does it work?. [Acedido em 19 dezembro 2018].

[6] A. S. Y. H. K. S. Yoshiro Fukushima, "A behavior based malware detection scheme for avoiding false positive," IEEEXplore Digital Library, [Online]. Available: https://ieeexplore.ieee.org/document/5634444. [Acedido em 19 dezembro 2018].

[7] C. Cade, "Understanding Heuristic-based Scanning vs. Sandboxing," OPSWAT, 13 julho 2015. [Online]. Available: https://www.opswat.com/blog/understanding-heuristic-based-scanning-vs-sandboxing. [Acedido em 19 dezembro 2018].

[8] "Traditional Antivirus Software Versus Cloud-Based Solutions," ALURIA, janeiro 2018. [Online]. Available: https://www.aluriasoftware.com/traditional-anti-virus-vs-cloud-based/). [Acedido em 19 dezembro 2018].

[9] M. Brinkmann, "Update Microsoft Security Essentials On Computers Without Internet," GHACKS, 6 maio 2014. [Online]. Available: https://www.ghacks.net/2010/06/08/update-microsoft-security-essentials-on-computers-without-internet/. [Acedido em 19 dezembro 2018].