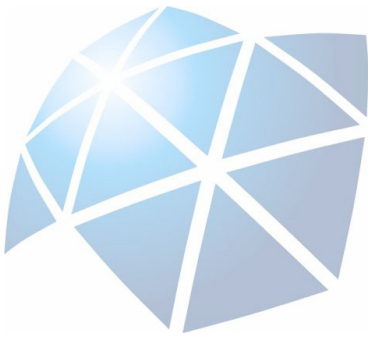
Universidade Estadual Paulista
FEIS - Faculdade de Engenharia de Ilha Solteira
DEE - Departamento de Engenharia Elétrica

Estudo Especial II

Avaliação das técnicas de detecção de código malicioso

Davidson Rodrigo Boccardo



São José do Rio Preto-SP, Setembro/2006

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução Geral

Nos tempos atuais, segurança em computadores é um assunto extremamente importante para as pessoas, negócios e governo. Programadores hostis escrevem programas com intenção maliciosa de coletar dados privados, distribuir *spam*, quebrar medidas de segurança, etc; e quando bem sucedidos na propagação de seus códigos maliciosos representam um efeito desastroso no mundo dos negócios e nas redes de computadores [8].

O primeiro passo em conter ataques maliciosos é a identificação dos programas maliciosos, diante disto, companhias de antivírus (AV) utilizam de várias técnicas de análise dinâmica e estática para identificar um código malicioso [22]. A maioria das ferramentas dos (AV) dependem do conhecimento das assinaturas dos códigos maliciosos, que são basicamente padrões de chamadas de sistema.

Contudo, o aumento da complexidade, quantidade e heterogeneidade dos sistemas de software dificultam o reconhecimento dos códigos maliciosos baseado em assinaturas. Para agravar ainda mais, atualmente os programadores hostis contam com ferramentas (comerciais ou disponíveis na comunidade *blackhat*) avançadas de evasão, que utilizam-se de estratégias como EPO *Entry Point Obscuring*[9], polismorfismo[15] e metamorfismo[19] que dificultam a suas detecções. Devido a isso, é de extrema importância a avaliação das ferramentas de detecção existentes (comerciais ou não) diante destas evoluções de código.

1.1 Organização do estudo

O capítulo 2 define a metodologia de avaliação das técnicas de detecção de código malicioso e mostra quais ferramentas de evasão e detecção foram utilizadas. No capítulo 3 são apresentados os testes e os resultados. No capítulo 4 estão as conclusões e no capítulo 5 as referências bibliográficas.

Capítulo 2

Metodologia de avaliação

Para o processo de avaliação das técnicas de detecção de código malicioso definiu-se um modelo experimental, que mostra a necessidade de um ambiente seguro neste tipo de avaliação e como foram realizadas as evoluções de código seguidas das deteçções destas. Este modelo é detalhado na seção 2.1. Na seção 2.2 são mostradas as métricas utilizadas na avaliação para uma posterior análise qualitativa das ferramentas de detecção de código malicioso. E por fim, na seção 2.3 são relatadas as ferramentas utilizadas tanto de detecção como de evasão.

2.1 Modelo experimental

Uma das exigências mais importantes em um modelo de análise de código malicioso é a instalação de um sistema dedicado, nas quais podem ser usadas as estratégias evasivas para subversão de detecção sem nenhum dano, como contra exemplo, a aplicação de técnicas evolutivas para um código malicioso, e sua execução inapropriada em um ambiente conectado a rede mundial poderia causar um prejuízo enorme, devido a disseminação desta nova variante maliciosa.

Na literatura são propostos dois métodos para sistemas dedicados: uso de sistemas reais ou uso de sistemas virtuais. Apesar de determinados códigos maliciosos falharem em sistemas virtuais como o W95/CIH[18], a avaliação de técnicas de detecção foi realizada em um sistema virtual desconectado da rede, pois o interesse está na detecção do código malicioso e não em sua execução e atuação.

Assim também não há a necessidade de se ter um ambiente próprio para cada tipo de código malicioso, para casos em que o código é dependente de alguma característica do ambiente, como arquietura ou do sistemas de arquivos. E em relação ao ambiente virtual ser desprovido de rede é para não existir nenhuma possibilidade de disseminação por uma execução indevida.

Dado um ambiente seguro, a etapa seguinte do modelo, consiste na aplicação de ferramentas evasivas em conjuntos de softwares maliciosos e não maliciosos para a geração dos testes de caso. Após esta geração, verificou-se a eficácia de cada detector através da varredura dos testes, confirmando se o detector acusava positivamente ou não o programa

alterado ou a variante criada. Para a análise desta eficácia foram utilizadas métricas que serão detalhadas na seção seguinte. Este modelo experimental é exibido na figura 2.1.

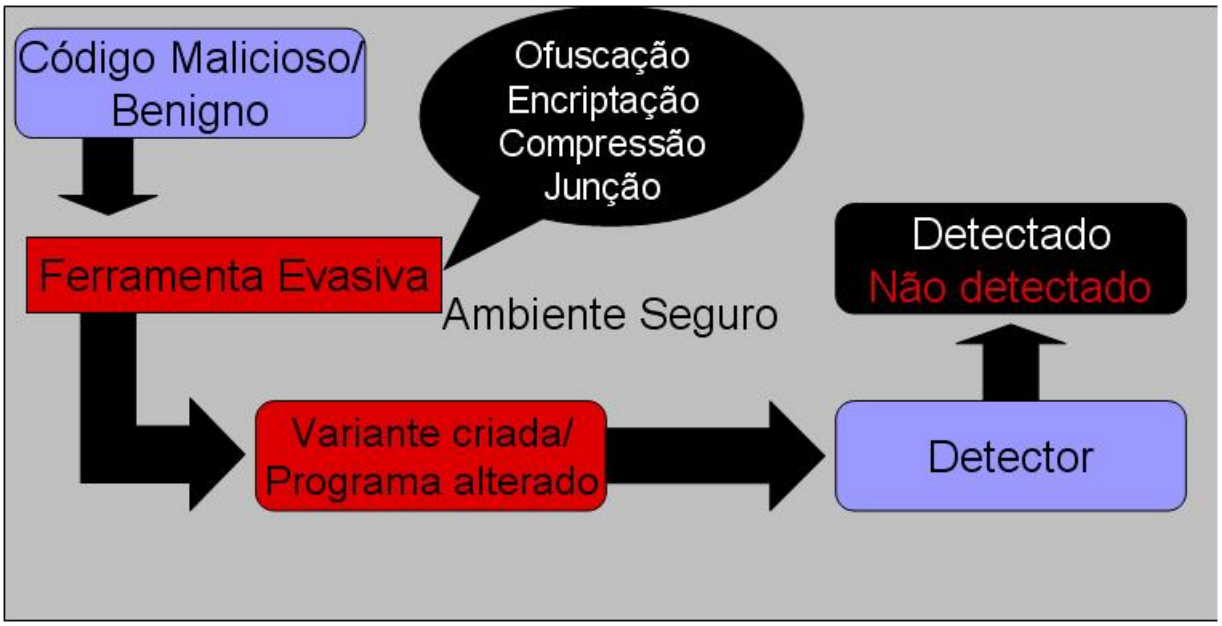


Figura 2.1: Modelo para avaliação dos detectores de código malicioso

2.2 Métricas para avaliação

Um detector de código malicioso trabalha analisando um objeto de dados (um arquivo, uma mensagem de email ou um pacote de rede) e, determina se os dados contêm um executável e se é malicioso. Este primeiro teste realizado pelo detector é geralmente baseado em um método do sistema operacional para descobrir o tipo do dado, que pode ser determinado por cabeçalhos MIME, extensões de arquivo, ou um "número mágico" que é único para um formato de arquivo. Dada estas técnicas existentes para determinar se um objeto de dados contêm um executável, restringimos a definição do detector de código malicioso para somente admitir como entrada programas executáveis.

Pode-se definir um detector de código malicioso D como uma função cujo domínio e intervalo são o conjunto dos programas executáveis P e o conjunto $(malicioso, benigno)$, respectivamente. Em outras palavras, um detector D é uma função $D : P \,!\, (malicioso, benigno)$ definida como:

$$D(p) = \begin{cases} \text{malicioso} & \text{se } p \text{ contêm código malicioso} \\ \text{benigno} & \text{caso contrário} \end{cases}$$

Avaliar um detector D significa interagir todos programas de entrada $p \in P$ e checar a corretude da resposta. Neste contexto, falsos positivos são programas benignos que o detector marca como infectado; e falsos negativos são códigos maliciosos que o detector falha em reconhecer. Também, o hit rate (taxa de acerto) mede a taxa de códigos

maliciosos detectados em relação ao número de códigos maliciosos usados na avaliação.

Em uma avaliação de um detector, o objetivo é verificar se a ferramenta detecta todos códigos maliciosos, dada a perigosa ameaça que podem ocasionar. Assim, é crucial reduzir o número de falsos negativos para próximo de zero. Por outro lado, o número de falsos positivos é importante para determinar a usabilidade do detector, pois se muitos programas benignos são reconhecidos como infectados, o usuário pode vir a perder a confiança no detector e parar de usá-lo.

Como o conjunto P de todos possíveis programas é infinito, simplesmente enumerar todas entradas para o detector de código malicioso não é viável. Todo conjunto de teste é então finito, e os falsos positivos, e os falsos negativos são definidos para um dado conjunto de teste. Um conjunto de teste P_T é classificado em dois conjuntos disjuntos, um de programas benignos B e outro de programas maliciosos M. A taxa de falsos positivos FP_{P_T}, falsos negativos FN_{P_T}, e a taxa de acerto HR_{P_T} (todos relacionados com o conjunto de testes P_T) são definidos como:

$$FP_{P_T} = \frac{|\ \{\ p\ \in\ B\ :\ D(p)\ =\ malicioso\ \}\ |}{|B|}$$

$$FN_{P_T} = \frac{|\ \{\ p\ \in\ M\ :\ D(p)\ =\ benigno\ \}\ |}{|M|}$$

$$HR_{P_T} = \frac{|\ \{\ p\ \in\ M\ :\ D(p)\ =\ malicioso\ \}\ |}{|M|}$$

O objetivo do processo de avaliação é medir a taxa de acerto e de falsos negativos para um conjunto P_T e prover a medida de eficácia da detecção, porém testes de falsos positivos também foram realizados. Como em todo outro procedimento de testes, a avaliação final da eficácia de um detector de código malicioso depende da qualidade dos casos de teste e das métricas que ditam o comportamento do detector de acordo com as entradas.

Nesta avaliação, os testes foram gerados a partir de variantes criadas por ferramentas de evasão, tanto de proteção de propriedade intelectual como de ferramentas da comunidade *blackhat*, criadas para que seus códigos maliciosos não sejam detectados. A seguir estão detalhadas as ferramentas de evasão utilizadas e os detectores avaliados.

2.3 Ferramentas utilizadas

A identificação do conjunto representativo de códigos maliciosos para submissão a avaliação, foram motivadas por ferramentas de proteção de propriedade intelectual, em que pesquisadores estudam evasão de código para tornar o processo de engenharia reversa

mais dispendioso; como também a aplicação de ferramentas disponíveis na comunidade *blackhat* para evasão de código para subversão de detecção. Estas ferramentas são relatadas na subseção 2.3.1.

Para a avaliação de técnicas de deteção foram utilizadas ferramentas comerciais de detecção (antivírus), devido a impossilidade de testar cada técnica de detecção em separado, visto que não existe uma ferramenta para cada técnica, e sim detectores baseados em técnicas combinadas. Os detectores são detalhados na subseção 2.3.2.

2.3.1 Ferramentas de evasão

As ferramentas de evasão envolvendo ofuscação, compressão, junção e encriptação utilizadas na avaliação foram:

- EXECryptor[17], software comercial usado para proteção de código, baseado na tecnologia de transformação metamórfica de código, dificultando a engenharia reversa, análise e modificação do código.A ferramenta possui recursos de antidepuração, antitrace e de proteção de importação. Ela também permite trabalhar com pequenas chaves de 12/16 caracteres de comprimento para comprimir código e recursos de uma aplicação;
- ASPACK [1], é um avançado compressor comercial de executáveis Win32, capaz de reduzir o tamanho de programas na margem dos 70%. Outra utilidade é a proteção contra engenharia reversa de hackers não profissionais. Os programas comprimidos com ASPack são auto contidos, e executam exatamente como anteriormente, sem nenhuma penalidade no tempo de execução;
- ASPROTECT[1], sistema comercial de proteção de aplicativos de software, com uma execução rápida dos mecanismos de proteção, especialmente designada para projetistas de software. É uma ferramenta projetada para tarefas específicas como trabalhar com chaves de registro e criação de versões de software de teste;
- PECompact2[5], é um compressor comercial de executáveis/módulos Win32 (i.e. *.EXE, *.DLL, *.OCX, *.SCR), e em tempo de execução os módulos comprimidos são rapidamente descomprimidos na memória. A ferramenta provê mecanismos de antivírus e proteção de software;
- PEncrypt (PE File Encryptor), é uma ferramenta da comunidade *blackhat* de encriptação multinível de arquivos PE, ela possui recursos contra engenharia reversa como Anti-Dump, Anti-Dasm, Anti-Trace, Anti-SoftICE, Anti-ICEDump, Anti-TRACEX, Anti-Debuggers, Ring0. A ferramenta também pode gerar decriptador polimórfico;
- Fast Small Good (FSG), é um compressor *blackhat* para executáveis pequenos;
- PE-PaCK (PE Packer), utilitário *blackhat* que comprime arquivos, criptografando-os no processo. Ele adiciona um cabeçalho que expande, de forma automática, o arquivo na memória ao ser executado e, em seguida, transfere o controle para este arquivo;

- fEvicol (Binder EXE+JPEG), utilitário *blackhat* que faz a junção de um executável (EXE) com uma imagem (JPEG). O ícone do executável gerado pode ser configurado, por padrão o ícone é de uma imagem;
- PEtite[14], é um compressor comercial de executáveis (EXE/DLL/etc...) Win32. A ferramenta também adiciona detecção de vírus para os executáveis comprimidos checando-os toda vez que são executados.
- UPX[20], é um utilitário gratuito, portável, estensível e de alto desempenho na compressão de executáveis de diferentes formatos. Este possui uma excelente taxa de compressão e oferece uma rápida descompressão, e os executáveis não sofrem nenhum *overhead* de memória. É um utilitário distribuído pela GNU e usa biblioteca de compressão NRV.

2.3.2 Ferramentas de detecção

Para a avaliação de detecção de códigos maliciosos foram utilizadas oito ferramentas de detecção conhecidas (antivírus), sete em versão de teste (*trial*) e uma gratuita. A avaliação foi realizada na mesma data com todos os detectores atualizados e avaliados separadamente (somente um detector instalado no sistema por vez, para não causar interferência). Os detectores avaliados foram:

- ClamAV 0.88.4[6], versão gratuita;
- Mcafee Antivírus 11.0.209[12], versão trial;
- Norton Antivírus 2006[13], versão trial;
- AVG 7.1 Build 405[3], versão trial;
- Sophos 6.0.2[16], versão trial;
- EZ Antivirus 7.2[7], versão trial;
- BitDefender 9.5 standard[4], versão trial;
- Kaspersky 6.0.0.303[11], versão trial.

Para uma melhor avaliação foram enviados emails para os detectores para informações sobre o processo de detecção, alguns emails não foram respondidos, outros não deram informações por causa da segurança. Já outros responderam, como o detector AVG dizendo que fazem uso de desempacotadores específicos nas várias ferramentas de ofuscação, fazem uso de emulador e alguns tipos de heurísticas; e também usam outras técnicas para detecção genérica de códigos maliciosos ofuscados através de pesquisa complexa de strings e algoritmos. Já o detector ClamAV respondeu para procurar as respostas no próprio código-fonte do antivírus, porém esta análise do fonte a procura destas respostas não foi realizada por restrições de tempo, pois o mesmo possui 576 arquivos com um tamanho total de 6,25 MB.

Capítulo 3

Testes e resultados

No capítulo anterior mostrou-se a necessidade de um ambiente seguro para avaliação de códigos maliciosos, para a construção deste ambiente foi utilizado o software VMWare 5.5[21]. Após a instalação do ambiente, foram coletados os códigos maliciosos e benignos, as ferramentas de evasão e detecção e posteriormente copiados para a máquina virtual. Após esta fase a máquina virtual foi desconectada totalmente da rede e passou-se para a fase de geração dos testes de caso.

3.1 Geração dos casos de teste

Os códigos maliciosos usados para geração dos casos estão entre os vinte mais encontrados em computadores no mês de julho de 2006, segundo a pesquisa realizada pelo laboratório Kaspersky [10]. Estes códigos incluem todas classes de programas maliciosos: vírus, *worms*, *Trojans*, *backdoors* e *adwares*. Esta variedade confirma que atualmente, um computador é vulnerável para ser atacado por qualquer classe de código malicioso.

Para o processo de avaliação da taxa de acerto e de falsos negativos, foram utilizadas somente 22 amostras de códigos maliciosos bem conhecidos (*backdoor* Rbot, *worms* NetSky e Mydoom, *trojans* Microjoin, Agent, Banker e Netbus, vírus Parite), visto que os novos códigos maliciosos são produzidos na maioria dos casos através de técnicas de evasão. Assim, com estas amostras e ferramentas de evasão foram criadas 147 variantes para serem submetidas a avaliação.

Para avaliação de possíveis falsos positivos, foram utilizados 8 aplicativos não maliciosos do sistema operacional Windows (calculadora, prompt de comando, terminal, discador, bloco de notas, wordpad, paint, tetris), e gerados 73 casos de teste através das ferramentas de evasão.

Na geração dos casos de teste dos códigos maliciosos notou-se que algumas das amostras já usavam algumas das ferramentas evasivas, como por exemplo, algumas variantes do *worm* Mydoom que estavam comprimidas pelo UPX, e algumas variantes do cavalo-de-tróia Banker comprimidas pelo FSG.

3.2 Avaliação dos detectores

Após a geração dos casos, foi feito o processo de avaliação para cada detector, e constatou que algumas das amostras ITW(In the wild)[1] não foram detectadas. Foram os casos do antívirus AVG que falhou na detecção do cavalo-de-tróia Banker.cv, do Sophos que não detectou os cavalos-de-tróia Agent.v, Banker.df e Banker.cv, e do Etrust EZ que falhou em detectar os *trojans* Microjoin.b e Banker.cv. Contudo no processo de avaliação das taxas de acerto e falsos negativos foram considerados apenas os casos de teste gerados.

Na detecção de algumas variantes os detectores obtiveram sucesso na detecção da ferramenta de evasão e não do código malicioso, ou seja, dado um código malicioso X que utiliza uma ferramenta de evasão Y, o detector detectava como sendo um código malicioso devido a detecção da ferramenta Y e não do código X. Como exemplo desta detecção, podemos citar a ferramenta fEvicol.

A seguir, serão detalhados os resultados da taxa de acerto, dos falsos negativos e dos falsos positivos para cada ferramenta de detecção. Uma observação é na coluna denominada número de variantes nas tabelas abaixo, o formato está xm/yb que significa que foram criadas x variantes maliciosas e y variantes não maliciosas (benignas).

Na tabela 3.1 pode-se notar que o detector ClamAV não conseguiu nenhum êxito diante de evasões realizadas pelas ferramenta fEvicol (comunidade *blackhat*) e PECompact2 (comercial), como também baixa taxa de acerto diante das outras ferramentas. A melhor taxa de detecção (100%) foi sobre a ferramenta UPX (amplamente usada por programadores hostis), que mostra que o detector possivelmente tem desempacotador específico para este tipo de ferramenta.

3.2.1 ClamAV

Ferramenta	N^o variantes	% taxa de acerto	% falsos negativos	% falsos positivos
ASPACK	19m/8b	5,26	94,74	0
ASPROTECT	19m/8b	36,84	63,16	0
EXECryptor	17m/8b	52,94	47,06	0
fEvicol	22m/8b	0	100	0
FSG	4m/8b	75	25	0
PECompact2	21m/8b	0	100	12,50
PEncrypt	19m/7b	10,52	89,48	0
PE-PaCK	17m/8b	82,35	17,65	0
PEtite	6m/3b	33,33	66,67	0
UPX	3m/7b	100	0	0

Tabela 3.1: Tabela de avaliação do detector ClamAV

Já nos resultados da tabela 3.2 do detector Mcafee, pode-se notar que a menor taxa de acerto foi diante a ferramenta comercial EXECryptor, porém no geral o detector obteve um porcentual relativamente maior do que as outras ferramentas de detecção, e

[1] códigos maliciosos que estão atualmente se disseminando e infectando novos alvos, diferenciando de amostras Zoo que são códigos criados em laboratório

ainda mais, obteve um percentual de detecção diante de todas as ferramentas de evasão. Uma outra observação é sobre as variantes obtidas através do UPX que foram totalmente identificadas, comprovando que os detectores já incluem desempacotadores específicos para ferramentas utilizadas maliciosamente pelos programadores hostis.

3.2.2 Mcafee VirusScan

Ferramenta	N^o variantes	% taxa de acerto	% falsos negativos	% falsos positivos
ASPACK	19m/8b	89,47	10,53	0
ASPROTECT	19m/8b	47,36	52,64	0
EXECryptor	17m/8b	17,64	82,36	0
fEvicol	22m/8b	77,27	22,73	87,50
FSG	4m/8b	75	25	0
PECompact2	21m/8b	61,90	38,1	0
PEncrypt	19m/7b	42,10	57,9	14,28
PE-PaCK	17m/8b	94,11	5,89	0
PEtite	6m/3b	83,33	16,67	0
UPX	3m/7b	100	0	0

Tabela 3.2: Tabela de avaliação do detector Mcafee VirusScan

A tabela 3.3 do detector da Norton mostra que nenhuma variante criada pela ferramenta fEvicol foi identificada e que uma variante criada pelo UPX não foi identificada. Este resultado é alarmante porque uma destas ferramentas é da comunidade *blackhat* e a outra é amplamente usada por *hackers* maliciosos. Contudo, a ferramenta não apresentou nenhum falso positivo.

3.2.3 Norton Antivirus

Ferramenta	N^o variantes	% taxa de acerto	% falsos negativos	% falsos positivos
ASPACK	19m/8b	84,21	15,79	0
ASPROTECT	19m/8b	26,31	76,69	0
EXECryptor	17m/8b	11,76	88,24	0
fEvicol	22m/8b	0	100	0
FSG	4m/8b	75	25	0
PECompact2	21m/8b	52,38	47,62	0
PEncrypt	19m/7b	21,05	78,95	0
PE-PaCK	17m/8b	88,23	11,77	0
PEtite	6m/3b	33,33	66,67	0
UPX	3m/7b	66,66	33,34	0

Tabela 3.3: Tabela de avaliação do detector Norton Antivirus

Os resultados da tabela 3.4 do detector da AVG mostram que não foram identificadas nenhuma variante criada pelo EXECryptor (comercial), contudo obteve 100% de detecção diante a ferramenta fEvicol (*blackhat*. Porém, em relação aos falsos positivos a ferramenta obteve 100% de falsos positivos diante desta mesma ferramenta (fEvicol), concluindo que

o detector possui padrões de assinatura para a ferramenta fEvicol e não para os códigos maliciosos.

3.2.4 AVG Antivirus

Ferramenta	N^o variantes	% taxa de acerto	% falsos negativos	% falsos positivos
ASPACK	19m/8b	52,63	47,37	0
ASPROTECT	19m/8b	26,31	73,69	0
EXECryptor	17m/8b	0	100	0
fEvicol	22m/8b	100	0	100
FSG	4m/8b	50	50	0
PECompact2	21m/8b	28,57	71,43	0
PEncrypt	19m/7b	5,26	94,74	0
PE-PaCK	17m/8b	76,47	23,53	0
PEtite	6m/3b	50	50	0
UPX	3m/7b	66,66	33,34	0

Tabela 3.4: Tabela de avaliação do detector AVG Antivirus

Conforme mostra a tabela 3.5 do detector Sophos, o detector não obteve nenhum êxito diante de variantes criadas por três ferramentas de evasão EXECryptor, PEncrypt(*blackhat*) e PEtite(comercial). Para variantes criadas pelo fEvicol a ferramenta detectou todos códigos (maliciosos ou não).

3.2.5 Sophos Antivirus

Ferramenta	N^o variantes	% taxa de acerto	% falsos negativos	% falsos positivos
ASPACK	19m/8b	73,68	26,32	0
ASPROTECT	19m/8b	15,78	84,22	0
EXECryptor	17m/8b	0	100	0
fEvicol	22m/8b	100	0	100
FSG	4m/8b	25	75	0
PECompact2	21m/8b	14,28	85,72	0
PEncrypt	19m/7b	0	100	0
PE-PaCK	17m/8b	64,70	35,3	0
PEtite	6m/3b	0	100	0
UPX	3m/7b	33,33	66,67	0

Tabela 3.5: Tabela de avaliação do detector Sophos Antivirus

Para o detector EZ, os resultados da tabela 3.6 são problemáticos, pois das dez ferramentas de evasão utilizadas para a geração dos casos de teste, o detector não detectou nenhuma variante de seis destas ferramentas. Contudo, a ferramenta não apresentou falsos positivos.

3.2.6 eTrust EZ Antivirus

Ferramenta	N^o variantes	% taxa de acerto	% falsos negativos	% falsos positivos
ASPACK	19m/8b	52,63	47,37	0
ASPROTECT	19m/8b	26,31	73,69	0
EXECryptor	17m/8b	0	100	0
fEvicol	22m/8b	0	100	0
FSG	4m/8b	25	75	0
PECompact2	21m/8b	0	100	0
PEncrypt	19m/7b	0	100	0
PE-PaCK	17m/8b	0	100	0
PEtite	6m/3b	0	100	0
UPX	3m/7b	33,33	66,67	0

Tabela 3.6: Tabela de avaliação do detector eTrust EZ Antivirus

Conforme a tabela 3.7 do detector BitDefender, o detector apresentou sempre um percentual de detecção diante das variantes criadas, tendo seu menor percentual de 11,76% para variantes criadas pela ferramenta EXECryptor. E também, não apresentou nenhum falso positivo.

3.2.7 BitDefender Antivirus

Ferramenta	N^o variantes	% taxa de acerto	% falsos negativos	% falsos positivos
ASPACK	19m/8b	52,63	47,37	0
ASPROTECT	19m/8b	94,73	5,27	0
EXECryptor	17m/8b	11,76	88,24	0
fEvicol	22m/8b	50	50	0
FSG	4m/8b	75	25	0
PECompact2	21m/8b	85,71	14,29	0
PEncrypt	19m/7b	36,84	63,16	0
PE-PaCK	17m/8b	88,23	11,77	0
PEtite	6m/3b	50	50	0
UPX	3m/7b	66,66	33,34	0

Tabela 3.7: Tabela de avaliação do detector BitDefender Antivirus

Já nos resultados da tabela 3.8 do detector Kaspersky, pode-se notar que o detector não detectou nenhuma variante da ferramenta comercial EXECryptor, porém no geral o detector obteve um porcentual relativamente maior do que as outras ferramentas de detecção, e ainda mais, 100% de êxito na detecção diante variantes criadas pelo fEvicol e pelo UPX. Contudo, apresentou também 100% de falsos positivos em programas modificados pela ferramenta fEvicol.

3.2.8 Kaspersky Antivirus

Ferramenta	N^o variantes	% taxa de acerto	% falsos negativos	% falsos positivos
ASPACK	19m/8b	94,73	5,17	0
ASPROTECT	19m/8b	21,05	78,95	0
EXECryptor	17m/8b	0	100	0
fEvicol	22m/8b	100	0	100
FSG	4m/8b	75	25	0
PECompact2	21m/8b	85,71	14,29	0
PEncrypt	19m/7b	31,57	68,43	0
PE-PaCK	17m/8b	94,11	5,89	0
PEtite	6m/3b	66,66	33,34	0
UPX	3m/7b	100	0	0

Tabela 3.8: Tabela de avaliação do detector Kaspersky Antivirus

3.2.9 Resultado geral

A seguir será exibido a tabela comparativa 3.9 das ferramentas de detecção em relação a suas taxas de acerto, falsos negativos e falsos positivos e posteriormente, a tabela 3.10 mostra as taxas de acerto de cada detector para cada ferramenta de evasão.

Ferramenta	% taxa de acerto	% falsos negativos	% falsos positivos
ClamAV	27,90	72,10	1,36
Mcafee VirusScan	63,95	36,05	10,95
Norton Antivirus	40,82	59,18	0
AVG Antivirus	43,54	56,46	10,95
Sophos Antivirus	37,42	62,58	10,95
eTrust EZ Antivirus	11,57	88,43	0
BitDefender Antivirus	61,23	38,77	0
Kaspersky Antivirus	63,95	36,05	10,95

Tabela 3.9: Tabela de avaliação geral das ferramentas de detecção

Diante do resultado da tabela 3.9 acima, é notável que as melhores taxas de detecção foram dos detectores Mcafee e Kaspersky, e a pior taxa de detecção foi do detector eTrust EZ.

Detector/Evasor	ASPACK	ASPROTECT	EXECryptor	fEvicll	FSG	PECompact2	PEncrypt	PEPaCK	PEtite	UPX
ClamAV	5,26	36,84	52,94	0	75	0	10,52	82,35	33,33	100
Mcafee	89,47	47,36	17,64	77,27	75	61,90	42,10	94,11	83,33	100
Norton	84,21	26,31	11,76	0	75	52,38	21,05	88,23	33,33	66,66
AVG	52,63	26,31	0	100	50	28,57	5,26	76,47	50	66,66
Sophos	73,68	15,78	0	100	25	14,28	0	64,70	0	33,33
eTrust EZ	52,63	26,31	0	0	25	0	0	0	0	33,33
BitDefender	94,73	57,89	11,76	50	75	85,71	36,84	88,23	50	66,66
Kaspersky	94,73	21,05	0	100	75	85,71	31,57	94,11	66,66	100

Tabela 3.10: Tabela de avaliação da taxa de acerto dos detectores em relação as ferramentas de evasão

A tabela 3.11 a seguir, mostra o percentual de detecção das variantes, independente de qual detector foi utilizado. Observa-se que algumas variantes geradas pelas ferramentas ASPROTECT, EXECryptor, PECompact2 e PEncrypt não foram detectadas por nenhum detector.

Ferramenta	% Número de variantes	% variantes detectadas
ASPACK	19	100
ASPROTECT	19	78,94
EXECryptor	17	70,58
fEvicol	22	100
FSG	4	100
PECompact2	21	90,47
PEncrypt	19	52,63
PE-PaCK	17	100
PEtite	6	100
UPX	3	100

Tabela 3.11: Tabela das taxas de acerto em relação as variantes criadas

Capítulo 4

Conclusão e trabalhos futuros

Devido aos resultados da avaliação, pode-se dizer que técnicas de teste baseadas em evasão são utéis para comparar detectores de códigos maliciosos, pois através destes resultados mostrou-se que podem ser geradas variantes que não seriam detectadas (pensando nos detectores testados), o que representa uma grande ameaça.

Em relação a eficácia de detecção, o detector da Kaspersky e da Mcafee se sobressaíram em relação aos demais, pois obtiveram uma taxa de acerto maior, apesar de acusarem falsos positivos para ferramentas de propósito malicioso (fEvicol). Já em relação a eficácia de evasão, as ferramentas em ordem crescente de evasão foram PECompact2, ASPROTECT, EXECryptor e PEncrypt.

Diante disso, ficou comprovado que os detectores atuais são falhos diante das estratégias evasivas usadas por programadores hostis, havendo a necessidade de uma nova abordagem baseada na semântica do código e não em sua sintaxe.

Referências Bibliográficas

[1] ASPACK Software *ASPACK: File Compressor.* http://www.aspack.com/, Último acesso, Agosto 2006.

[2] ASPACK Software *ASPROTECT: Protection of applications.* http://www.aspack.com/, Último acesso, Agosto 2006.

[3] Grisoft *AVG 7.1 for Windows.* http://www.grisoft.com, Último acesso, Agosto 2006.

[4] Bitdefender *BitDefender 9 Standard.* http://www.bitdefender.com.br/, Último acesso, Agosto 2006.

[5] Bitsum Technologies *PECompact2: File Compressor.* http://www.bitsum.com/pec2.asp, Último acesso, Agosto 2006.

[6] Clam Antivirus *Clam Antivirus.* http://www.clamav.net/, Último acesso, Agosto 2006.

[7] Ca *eTrust EZ Antivirus.* http://store.digitalriver.com/servlet/ControllerServlet?Action=Displ Último acesso, Agosto 2006.

[8] Gordon L. A., Loeb M. P., Lucyshyn W., and Richardson R.*2004 CSI/FBI computer crime and security survey.* Technical report, Computer Security Institute, 2004.

[9] GriYo *EPO: Entry-Point Obscuring.* Publicado online em VX Heavens http://vx.netlux.org/lib/vgy01.html . Último acesso, Agosto 2006.

[10] Kaspersky Lab *Online Scanner Top Twenty for July 2006.* Publicado online em http://www.viruslist.com/en/analysis?pubid=193366238. Último acesso, Agosto 2006.

[11] Kaspersky Lab *Kaspersky Anti-Virus.* http://www.kaspersky.com/, Último acesso, Agosto 2006.

[12] Mcafee *VirusScan.* http://www.mcafee.com/br/default.asp, Último acesso, Agosto 2006.

[13] Norton *Norton AntiVirus.* http://www.symantec.com/pt/br/index.jsp, Último acesso, Agosto 2006.

[14] PEtite *PEtite: Win32 Executable Compressor.* http://www.un4seen.com/petite, Último acesso, Agosto 2006.

[15] Skulason F. *Latest Trends in Polymorphism The Evolution of Polymorphic Computer Viruses.* Virus Bulletin Conference, 1995, pp. I-VII.

[16] Pugh *Sophos AntiVirus.* http://www.pugh.co.uk/Products/sophos/antivirus.htm, Último acesso, Agosto 2006.

[17] StrongBit technology *EXECryptor: Stop Crackers and software pirates.* http://www.strongbit.com/, Último acesso, Agosto 2006.

[18] Szor P. *The Art of Computer Virus Research and Defense.* Capítulo 15 - Malicious Code Analysis Techniques. Addison-Wesley Professional, Fevereiro 2005.

[19] Szor P. e Ferrie P. *Hunting for Metamorphic.* Virus Bulletin Conference, September 2001, pp. 123-144.

[20] UPX *UPX: Ultimate Packer for eXecutables.* http://upx.sourceforge.net/, Último acesso, Agosto 2006.

[21] VMware *VMware - Virtualization Software.* http://www.vmware.com/, Último acesso, Agosto 2006.

[22] Zeltser L. *Reverse Engineering Malware.* http://www.zeltser.com/sans/gcih-practical/revmalw.html, Último acesso, Abril 2006.