Análise de Antivírus Comerciais e Proposta de Solução na Detecção de *Ransomwares* em Programas

Trabalho de Conclusão de Curso

Engenharia da Computação

Jolu'son Almeida Queiroz
Orientador: Prof. Edison de Queiroz Albuquerque
Coorientador: Prof. Sidney Marlon Lopes de Lima

Universidade de Pernambuco
Escola Politécnica de Pernambuco
Graduação em Engenharia de Computação

Jolu’son Almeida Queiroz

Análise de Antivírus Comerciais e Proposta de Solução na Detecção de *Ransomwares* em Programas

Monografia apresentada como requisito parcial para obtenção do diploma de Bacharel em Engenharia de Computação pela Escola Politécnica de Pernambuco – Universidade de Pernambuco.

Recife, dezembro/2021.

Queiroz, Jolu'son Almeida
Análise de Antivírus Comerciais e Proposta de Solução na Detecção de Ransomwares em Programas / Jolu'son Almeida Queiroz. – Recife - PE, 2021.
vii, 36 f. : il. ; 29 cm.

Trabalho de Conclusão de Curso (Graduação em Engenharia de Computação) Universidade de Pernambuco, Escola Politécnica de Pernambuco, Recife, 2021.

Orientador: Prof. Dr. Edison de Queiroz Albuquerque.

Inclui referências.

1. Antivirus. 2. Ransomwares. 3. Redes Neurais. I. Título. II. Albuquerque, Edison de Queiroz. III. Universidade de Pernambuco.

Escola Politécnica de Pernambuco
Graduação em Engenharia de Computação
Projeto de Final de Curso

ESCOLA POLITÉCNICA
DE PERNAMBUCO

MONOGRAFIA DE FINAL DE CURSO

Avaliação Final (para o presidente da banca)*

No dia 27/12/2021, às 14h00min, reuniu-se para deliberar sobre a defesa da monografia de conclusão de curso do(a) discente **JOLU'SON ALMEIDA QUEIROZ**, orientado(a) pelo(a) professor(a) **EDISON DE QUEIROZ ALBUQUERQUE**, sob título Análise de Antivírus Comerciais e Proposta de Solução na Detecção de Ransonwares em Programas, a banca composta pelos professores:

LUIS CARLOS DE SOUSA MENEZES (PRESIDENTE)
EDISON DE QUEIROZ ALBUQUERQUE (ORIENTADOR)
SIDNEY MARLON LOPES DE LIMA (COORIENTADOR)

Após a apresentação da monografia e discussão entre os membros da Banca, a mesma foi considerada:

☒ Aprovada ☐ Aprovada com Restrições* ☐ Reprovada

e foi-lhe atribuída nota: 7,0 (sete)

*(Obrigatório o preenchimento do campo abaixo com comentários para o autor)

O(A) discente terá 7 dias para entrega da versão final da monografia a contar da data deste documento.

Luis Carlos de Sousa Menezes
AVALIADOR 1: Prof (a) **LUIS CARLOS DE SOUSA MENEZES**

Edison de Queiroz Albuquerque
AVALIADOR 2: Prof (a) **EDISON DE QUEIROZ ALBUQUERQUE**

Sidney Marlon Lopes de Lima
Prof. Pós Doutor Sidney Marlon Lopes de Lima
Departamento de Eletrônica e Sistemas
UFPE SIAPE: 1891425
AVALIADOR 3: Prof (a) **SIDNEY MARLON LOPES DE LIMA**

* Este documento deverá ser encadernado juntamente com a monografia em versão final.

Autorização de publicação de PFC

Eu, **Jolu'Son Almeida Queiroz** autor(a) do projeto de final de curso intitulado: **Análise de Antivírus Comerciais e Proposta de Solução na Detecção de Ransonwares em Programas;** autorizo a publicação de seu conteúdo na internet nos portais da Escola Politécnica de Pernambuco e Universidade de Pernambuco.

O conteúdo do projeto de final de curso é de responsabilidade do autor.

Jolu'Son Almeida Queiroz

Orientador(a): **Edison de Queiroz Albuquerque**

Prof. Pós Doutor Sidney Marlon Lopes de Lima
Departamento de Eletrônica e Sistemas
UFPE
SIAPE: 1891425

Coorientador(a): **Sidney Marlon Lopes de Lima**

Prof, de TCC: **Daniel Augusto Ribeiro Chaves** Data: 27/12/2021

Resumo

Este trabalho irá apresentar os resultados da análise de uma base de dados formadas por arquivos maliciosos de *ransomware* submetidos a avaliação, utilizando a API do VirusTotal, de antivírus utilizados comercialmente para avaliar a capacidade de detecção da base de dados de cada antivírus, e mostrando as limitações dos antivírus utilizados atualmente. Também, pretende apresentar uma alternativa preventiva e inteligente de detecção de *ransomwares* e sua comparação com soluções tradicionais equivalentes. A solução alcançou, em média, 99% de acurácia na classificação entre amostras malignas e benignas.

Abstract

This work will present the results of the analysis of a database formed by malicious ransomware files submitted to evaluation using the VirusTotal API of commercially used antivirus to evaluate the detection capacity of the database of each antivirus and showing limitations of the currently used antivirus. It also intends to present a preventive and intelligent alternative for detecting ransomware and its comparison with equivalent traditional solutions. The solution achieved, on average, 99% accuracy in classifying malignant and benign sample.

Lista de Tabelas

Sumário

Capítulo 1

Introdução

Na rede mundial de computadores, estamos expostos a uma grande quantidade de conhecimento, aplicações, redes sociais e seus respectivos usuários. A sociedade troca dados continuamente, sendo muitos deles sensíveis ou relevantes para realização de ações com consequências danosas no mundo fora do ambiente virtual. Por exemplo: a realização de fraudes financeiras, causar prejuízos a uma empresa ou chantagens financeiras através do sequestro de dados (pessoais ou empresariais).

Em geral, o mecanismo usado para efetuar a captura das informações necessárias para essas ações danosas é a atração de usuários desavisados a realizarem o download de aplicativos com a função de captura silenciosa, bloqueio da estação de trabalho ou danificar ativamente o sistema operacional. Esses são os *Malwares* ("*Malware*" é a junção das palavras "*malicious*" e "*software*").

Uma classe popular dessas ameaças são os *Ransomwares* (Trojan-Ransom). Um *ransomware* impede que o usuário possa acessar o seu computador ou a maioria dos dados de alto valor encontrados, criptografando os arquivos e solicitando um "resgate", pago com alguma moeda virtual (por não ser rastreável), para liberar os dados, porém não existe nenhuma garantia que após o pagamento da quantia se recupere o acesso ao conteúdo sequestrado.

Somente no período entre abril de 2014 e junho de 2015, as vítimas relataram mais de U$ 18 milhões em perdas devido às atuações dos *ransomwares*. Um exemplo famoso desse tipo de ataque virtual foi o *Wannacry*, que em maio de 2017 sequestrou sistemas em diversos países, afetando mais de 700 mil pessoas, entre consumidores, empresas, hospitais e até departamentos governamentais. A prevenção é a melhor estratégia contra *Ransomwares*, ou seja, detectar proativamente uma aplicação ou arquivo baixado pelo usuário, papel dos antivírus.

Geralmente, nos antivírus comerciais, a detecção dessa classe de ameaça ocorre através de uma "Lista Negra" composta por casos reportados por usuários

infectados (Vitimas) que foram analisados e criada uma vacina. Caso um arquivo suspeito seja apresentado ao antivírus, haverá a comparação deste com os casos da lista. Se o arquivo possui a mesma *hash* de algum deles, há a indicação de infecção e o arquivo é isolado ou vacinado. Caso contrário, o arquivo é liberado para uso pelo usuário.

Nessa lógica reativa, os prejuízos, por vezes irreversíveis, ocorreram para que fossem criadas defesas, representando risco alto em sistemas estratégicos como a base de dados de um banco, financeira e governos em que o registro de transações ou dados dos clientes podem ser alterados ou expostos.

O questionamento a esse modelo de proteção está ao apresentarmos um novo *ransomware* criado. Este será tratado como um arquivo livre de infecção, ou seja, um falso negativo porque não consta na lista negra existente.

O objeto deste trabalho é analisar a resposta dos antivírus comerciais a uma série de *ransomwares* conhecidos catalogados em VirusShare.com (VirusShare, 2021), que é um repositório de amostras de *malwares* para pesquisa composta de executáveis Windows 32bits. A resposta de detecção coletada através da plataforma VirusTotal, ambiente gratuito de avaliação de desempenho dos antivírus comerciais mais conhecidos acerca de uma dada ameaça, ao apresentarmos cada amostra selecionada.

Por fim, há a comparação dos resultados obtidos, salientando semelhanças e divergências entre as soluções comerciais e a proposição de uma solução proativa na detecção de *ransomwares* baseada no reconhecimento de padrões de entre aplicativos que são ameaças e programas conhecidos não infectados.

Capítulo 2

Limitação dos Antivírus Comerciais

Tecnicamente, a forma de ação para a identificação de arquivos e servidores maliciosos refere-se à consulta em bancos de dados de lista negra nomeados. Partindo deste princípio, um bom antivírus comercial possui uma extensa lista negra e frequentemente atualizada.

A plataforma VirusTotal emite diagnósticos sobre características malignas relacionadas a arquivos e servidores web. Quando se trata de arquivos suspeitos, o VirusTotal emite os diagnósticos fornecidos pelos principais produtos antivírus comerciais do mundo (VirusTotal, 2021). Em relação aos servidores da web suspeitos, o VirusTotal usa o banco de dados responsável por detectar endereços virtuais com práticas maliciosas.

O VirusTotal possui APIs (*Application Programming Interface*) que permitem aos programadores consultar a plataforma de forma automatizada. duas das APIs disponibilizadas pela VirusTotal são usadas. O primeiro é responsável por enviar os arquivos investigados ao servidor da plataforma. A segunda API, por sua vez, disponibiliza diagnósticos de antivírus comerciais para arquivos submetidos à plataforma pela primeira API.

Inicialmente, os *ransomwares* executáveis são enviados ao servidor pertencente à plataforma VirusTotal. Depois disso, os executáveis são analisados pelos 86 antivírus comerciais vinculados ao VirusTotal. Portanto, o antivírus fornece seus diagnósticos para os executáveis enviados à plataforma. O VirusTotal permite emitir três tipos diferentes de diagnósticos: *malware*, benigno e omissão.

Em seguida, por meio da plataforma VirusTotal, investiga 86 antivírus comerciais com seus respectivos resultados apresentados na Tabela 1. Usamos 1.174 executáveis maliciosos para arquitetura de 32 bits. O objetivo é verificar a quantidade de pragas virtuais catalogadas por antivírus. A motivação é que a aquisição de novas pragas virtuais desempenha um papel importante no combate a

aplicativos maliciosos. Portanto, quanto maior o banco de dados de *ransomwares* na lista negra, melhor tende a ser a defesa fornecida pelo antivírus.

Quanto à primeira possibilidade do VirusTotal, o antivírus detecta a ameaça do arquivo suspeito. No ambiente experimental proposto, todos os executáveis enviados são *ransomwares* de domínio público. Portanto, o antivírus acerta ao detectar a ameaça do executável investigado. A detecção de *ransomware* indica que o antivírus fornece um serviço robusto contra intrusões cibernéticas. Quanto maior o banco de dados da lista negra, melhor tende a ser a defesa fornecida pelo antivírus.

Na segunda possibilidade, o antivírus atesta a benignidade do arquivo investigado. Portanto, quando o antivírus atesta a benignidade do arquivo, trata-se de um falso negativo - já que todas as amostras são maliciosas. Ou seja, o executável investigado é um *ransomware*; no entanto, o antivírus atesta a benignidade da maneira errada.

Na terceira possibilidade, o antivírus não emite opinião sobre o executável suspeito. A omissão indica que o arquivo investigado nunca foi avaliado pelo antivírus nem tem capacidade para avaliá-lo em tempo real. A omissão do diagnóstico pelo antivírus aponta para sua limitação em serviços de grande escala.

Da Tabela 1 à Tabela 3, há a exibição dos resultados dos 86 produtos antivírus avaliados. Dois desses antivírus pontuaram acima de 97%. Esses antivírus foram: McAfee e McAfee-GW-Edition (mesmo fornecedor). Nível de detecção indicativo que esses programas antivírus fornecem um serviço confiável contra intrusões cibernéticas.

Tabela 1. Parte 1: resultado dos Antivírus Comerciais

Antivírus	Detecção (%)	Falso Negativo (%)	Omissão (%)
McAfee	97.63%	2.29%	0.07%
McAfee-GW-Edition	97.26%	2.43%	0.29%
Kaspersky	95.04%	4.50%	0.44%
BitDefender	94.53%	5.09%	0.36%
GData	94.38%	5.02%	0.59%
Avast	94.16%	5.46%	0.36%
AVG	94.16%	5.61%	0.22%
Symantec	93.05%	6.43%	0.51%
Sophos	92.90%	6.06%	1.03%
Panda	92.75%	6.87%	0.36%
Microsoft	91.94%	7.31%	0.73%

Tabela 2. Parte 2: resultado dos Antivírus Comerciais

Antivírus	Detecção (%)	Falso Negativo (%)	Omissão (%)
Ikarus	91.86%	2.95%	5.17%
Fortinet	91.72%	8.13%	0.14%
Emsisoft	91.57%	7.76%	0.66%
ESET-NOD32	91.57%	6.79%	1.62%
DrWeb	90.90%	7.98%	1.10%
NANO-Antivirus	90.83%	6.06%	3.10%
MicroWorld-eScan	89.43%	8.42%	2.14%
F-Secure	89.35%	7.90%	2.73%
VIPRE	88.76%	5.76%	5.46%
TrendMicro-HouseCall	85.80%	11.97%	2.21%
K7AntiVirus	85.58%	14.11%	0.29%
AhnLab-V3	85.36%	12.93%	1.69%
VBA32	84.92%	14.92%	0.14%
TrendMicro	80.78%	15.74%	3.47%
Antiy-AVL	80.78%	18.62%	0.59%
Ad-Aware	80.41%	7.83%	11.75%
K7GW	80.41%	12.41%	7.16%
Qihoo-360	78.71%	6.79%	14.48%
Jiangmin	76.94%	22.69%	0.36%
CAT-QuickHeal	76.79%	23.13%	0.07%
F-Prot	73.83%	26.16%	0.0%
Arcabit	70.95%	5.91%	23.13%
Tencent	70.95%	8.35%	20.69%
Cyren	70.36%	7.31%	22.32%
Avira	69.40%	7.83%	22.76%
Rising	69.32%	27.86%	2.80%
MAX	67.55%	1.25%	31.18%
ZoneAlarm	67.77%	2.36%	29.85%
Endgame	66.14%	1.03%	32.81%
AVware	66.14%	2.43%	31.41%
Webroot	66.00%	2.51%	31.48%
Zillya	64.59%	15.74%	19.66%
Comodo	64.22%	31.04%	4.73%
Yandex	63.41%	9.60%	26.97%
AegisLab	63.19%	22.32%	14.48%
Invincea	62.89%	7.53%	29.56%
TheHacker	61.19%	38.65%	0.14%
Cylance	61.12%	2.36%	36.51%
CrowdStrike	60.01%	3.69%	3.69%
SentinelOne	58.53%	8.57%	32.88%
ALYac	58.31%	16.70%	24.98%

Tabela 3. Parte 3: resultado dos Antivírus Comerciais

Antivírus	Detecção (%)	Falso Negativo (%)	Omissão (%)
Malwarebytes	58.31%	37.17%	4.50%
Baidu	57.28%	15.81%	26.90%
SUPERAntiSpyware	56.46%	43.31%	0.22%
ClamAV	50.33%	49.15%	0.51%
ViRobot	46.85%	53.06%	0.07%
Paloalto	44.05%	22.76%	33.18%
Bkav	41.09%	45.45%	13.45%
Kingsoft	39.09%	57.28%	3.62%
TotalDefense	37.69%	59.34%	2.95%
CMC	25.94%	59.12%	14.92%
nProtect	25.27%	25.86%	48.85%
Norman	19.43%	3.69%	76.86%
AntiVir	17.81%	4.43%	77.75%
Agnitum	15.96%	8.79%	75.24%
Commtouch	11.89%	10.05%	78.04%
PCTools	7.83%	3.47%	88.69%
Zoner	5.02%	73.31%	21.65%
ByteHero	1.55%	23.72%	74.72%
NOD32	1.40%	0.14%	98.44%
WhiteArmor	1.18%	5.17%	93.64%
VirusBuster	1.03%	0.88%	98.07%
eTrust-Vet	0.73%	0.81%	98.44%
eSafe	0.66%	7.61%	91.72%
Sunbelt	0.22%	0.07%	99.70%
Prevx	0.14%	1.10%	98.74%
Authentium	0.14%	0.14%	99.70%
a-squared	0.14%	0.0%	99.85%
Alibaba	0.07%	22.46%	77.45%
ahnlab	0.0%	0.0%	100.00%
Command	0.0%	0.0%	100.00%
SAVMail	0.0%	0.0%	100.00%
FileAdvisor	0.0%	0.0%	100.00%
Ewido	0.0%	0.0%	100.00%
Webwasher-Gateway	0.0%	0.0%	100.00%

Uma grande dificuldade no combate a aplicativos maliciosos é o fato de que os fabricantes de antivírus não compartilham suas listas negras de *malwares* devido a disputas comerciais. Por meio da análise da Tabela 1 à Tabela 3, nota-se outro agravante dessa adversidade: o mesmo fornecedor de antivírus nem mesmo compartilha seus bancos de dados entre seus diferentes programas antivírus. Observe, por exemplo, que os antivírus McAfee e McAfee-GW-Edition pertencem à

mesma empresa. Suas listas negras, embora efetivas, não são compartilhadas entre si. Portanto, as estratégias comerciais de uma mesma empresa dificultam o enfrentamento de *ransomwares*. Complementa o fato de os fornecedores de antivírus não estarem necessariamente preocupados em evitar invasões cibernéticas, mas em otimizar a receita de seus negócios.

A detecção de *ransomware* variou de 0% a 97,63%, dependendo do antivírus investigado. Em média, os 86 antivírus foram capazes de detectar 55,22% das pragas virtuais avaliadas, com desvio padrão de 30,05%. O alto desvio padrão indica que a detecção de executáveis maliciosos pode sofrer variações abruptas dependendo do antivírus escolhido. Está determinado que a proteção, contra invasões cibernéticas, se deve à escolha de um antivírus robusto com uma lista negra ampla e atualizada.

Quanto aos falsos negativos, em média, os antivírus atestaram falsos negativos em 13,15% dos casos, com desvio padrão de 11,49%. Não identificar o *ransomware* pode levar a danos irrecuperáveis. Uma pessoa ou instituição, por exemplo, utilizaria um determinado aplicativo, supostamente útil, quando, na verdade, é nocivo.

Em média, os antivírus estavam ausentes em 31,71% dos casos, com desvio padrão de 31,88%. A omissão do diagnóstico aponta para a limitação desses antivírus que possuem listas negras limitadas para detecção de *ransomwares* em tempo real.

Outro problema encontrado no combate a aplicativos maliciosos é o fato dos antivírus comerciais não possuírem um padrão na classificação dos *ransomwares* como visto na Tabela 4 à Tabela 7. Escolhemos 3 das 1.174 amostras de *ransomwares* a fim de exemplificar as classificações diversas de antivírus comerciais. Dessa forma, o momento em que os fabricantes reagem a uma nova praga virtual é afetado dramaticamente. Como não há um padrão, os antivírus fornecem os nomes que desejam, por exemplo, uma empresa pode identificar um *ransomware* como "HEUR:Trojan.Win32.Generic" e uma segunda empresa como "Win32:OnLineGames-FVR [Trj]". Portanto, a falta de um padrão, além do não compartilhamento de informações entre os fabricantes, dificulta a detecção rápida e eficaz de um aplicativo malicioso.

Tabela 4. Parte 1: classificação dos antivírus comerciais

Antivírus	VirusShare_00f6921f2a1ef6abcf691fb7e15bd997	VirusShare_0e0439c9f79b2c89d7967137832271f0	VirusShare_1ab4b5f294349e5c625f0b7b8b16965d
Ad-Aware	Trojan.PWS.OnlineGames.ZRK	OMISSÃO	OMISSÃO
AegisLab	Troj.GameThief.W32.OnLineGames.ssbs!c	OMISSÃO	OMISSÃO
Agnitum	OMISSÃO	Trojan.ShipUp!cwkcZDeN6vc	OMISSÃO
ahnlab	OMISSÃO	OMISSÃO	OMISSÃO
AhnLab-V3	Trojan/Win32.OnlineGameHack.R1320	Backdoor/Win32.ZAccess	BENIGNO
Alibaba	OMISSÃO	OMISSÃO	OMISSÃO
ALYac	Trojan.PWS.OnlineGames.ZRK	OMISSÃO	OMISSÃO
AntiVir	OMISSÃO	BENIGNO	BDS/Starter.I.1
Antiy-AVL	Trojan[GameThief]/Win32.OnLineGames	Trojan/Win32.ShipUp	BENIGNO
Arcabit	Trojan.PWS.OnlineGames.ZRK	OMISSÃO	OMISSÃO
a-squared	OMISSÃO	OMISSÃO	OMISSÃO
Authentium	OMISSÃO	OMISSÃO	OMISSÃO
Avast	Win32:OnLineGames-FVR [Trj]	Win32:Kryptik-MSQ [Trj]	OMISSÃO
AVG	Win32:OnLineGames-FVR [Trj]	Generic34.BDXE	PSW.Banker_c.KS
Avira	TR/Spy.Gen	OMISSÃO	OMISSÃO
AVware	Trojan.Win32.OnLineGames.CTB (v)	OMISSÃO	OMISSÃO
Baidu	Win32.Trojan-GameThief.OnlineGames.t	OMISSÃO	OMISSÃO
BitDefender	Trojan.PWS.OnlineGames.ZRK	Gen:Variant.Graftor.109841	OMISSÃO
Bkav	W32.OngameDP3.Worm	OMISSÃO	OMISSÃO
ByteHero	OMISSÃO	BENIGNO	BENIGNO
CAT-QuickHeal	Trojanpws.Onlinegam.5097	BENIGNO	BENIGNO
ClamAV	Win.Spyware.51146-2	BENIGNO	BENIGNO

Tabela 5. Parte 2: classificação dos antivírus comerciais.

Antivírus	VirusShare_00f6921f2a1ef6abcf691fb7e15bd997	VirusShare_0e0439c9f79b2c89d7967137832271f0	VirusShare_1ab4b5f294349e5c625f0b7b8b16965d
CMC	Trojan-GameThief.Win32.OnLineGames!O	OMISSÃO	OMISSÃO
Command	OMISSÃO	OMISSÃO	OMISSÃO
Commtouch	OMISSÃO	BENIGNO	BENIGNO
Comodo	TrojWare.Win32.GameThief.Onlinegames.~d046	TrojWare.Win32.Kryptik.BIWI	OMISSÃO
CrowdStrike	malicious_confidence_100% (D)	OMISSÃO	OMISSÃO
Cylance	Unsafe	OMISSÃO	OMISSÃO
Cyren	W32/Onlinegames.3!Generic	OMISSÃO	OMISSÃO
DrWeb	Trojan.PWS.Wsgame.6334	Trojan.Mods.1	BENIGNO
Emsisoft	Trojan.PWS.OnlineGames.ZRK (B)	Gen:Variant.Graftor.109841 (B)	OMISSÃO
Endgame	malicious (high confidence)	OMISSÃO	OMISSÃO
eSafe	OMISSÃO	OMISSÃO	BENIGNO
ESET-NOD32	Win32/PSW.OnLineGames.NQW	a variant of Win32/Kryptik.BIKE	BENIGNO
eTrust-Vet	OMISSÃO	OMISSÃO	OMISSÃO
Ewido	OMISSÃO	OMISSÃO	OMISSÃO
FileAdvisor	OMISSÃO	OMISSÃO	OMISSÃO
Fortinet	W32/OnlineGames.A!tr.pws	W32/ShipUp.EBPA!tr	PossibleThreat
F-Prot	W32/Onlinegames.3!Generic	BENIGNO	BENIGNO
F-Secure	Trojan.PWS.OnlineGames.ZRK	Gen:Variant.Graftor.109841	Trojan.Bat.Starter.I
GData	Trojan.PWS.OnlineGames.ZRK	Gen:Variant.Graftor.109841	OMISSÃO
Ikarus	Trojan-GameThief.Win32.OnLineGames	Trojan.Win32.ShipUp	Trojan.BAT.Starter
Invincea	heuristic	OMISSÃO	OMISSÃO
Jiangmin	TrojanDownloader.Agent.agfv	Trojan/ShipUp.job	TrojanDownloader.FlyStudio.ctb
K7AntiVirus	Password-Stealer (00006e851)	Riskware	BENIGNO
K7GW	Password-Stealer (00006e851)	Riskware	OMISSÃO

Tabela 6. Parte 3: classificação dos antivírus comerciais.

Antivírus	VirusShare_00f6921f2a1ef6abcf691fb7e15bd997	VirusShare_0e0439c9f79b2c89d7967137832271f0	VirusShare_1ab4b5f294349e5c625f0b7b8b16965d
Kaspersky	HEUR:Trojan.Win32.Generic	Trojan.Win32.ShipUp.ebpa	BENIGNO
Kingsoft	Win32.Troj.OnlineGamesT.ui.35328	Win32.Troj.Generic.a.(kcloud)	OMISSÃO
Malwarebytes	Spyware.OnlineGames	Trojan.FakeMS	OMISSÃO
MAX	*malware* (ai score=100)	OMISSÃO	OMISSÃO
McAfee	PWS-OnlineGames.f	Trojan-FCWH!0E0439C9F79B	Artemis!1AB4B5F29434
McAfee-GW-Edition	BehavesLike.Win32.PWSOnlineGames.ht	Trojan-FCWH!0E0439C9F79B	Artemis!1AB4B5F29434
Microsoft	PWS:Win32/OnLineGames	TrojanDropper:Win32/Gepys.A	OMISSÃO
MicroWorld-eScan	Trojan.PWS.OnlineGames.ZRK	Gen:Variant.Graftor.109841	OMISSÃO
NANO-Antivirus	Trojan.Win32.OnLineGames.dxkuol	Trojan.Win32.ShipUp.cdwwnr	OMISSÃO
NOD32	OMISSÃO	OMISSÃO	OMISSÃO
Norman	OMISSÃO	Kryptik.CCKH	W32/Multidrp.IN
nProtect	OMISSÃO	BENIGNO	OMISSÃO
Paloalto	BENIGNO	OMISSÃO	OMISSÃO
Panda	Trj/Lineage.JVK	Generic *Malware*	BENIGNO
PCTools	OMISSÃO	Trojan.Zeroaccess	Trojan-PSW.Banpaes
Prevx	OMISSÃO	OMISSÃO	OMISSÃO
Qihoo-360	*Malware*.Radar01.Gen	OMISSÃO	OMISSÃO
Rising	Trojan.PSW.Win32.GameOL.phv (CLOUD)	BENIGNO	BENIGNO
SAVMail	OMISSÃO	OMISSÃO	OMISSÃO
SentinelOne	static engine - malicious	OMISSÃO	OMISSÃO
Sophos	Mal/Behav-010	Mal/Generic-S	Mal/Generic-L
Sunbelt	OMISSÃO	OMISSÃO	OMISSÃO
SUPERAntiSpyware	Trojan.Dropper/Gen-CN	Trojan.Agent/Gen-Reveton	BENIGNO
Symantec	ML.Attribute.HighConfidence	Trojan.Zeroaccess!g46	OMISSÃO
Tencent	Trojan.TenThief.DNFTrojans.ple	OMISSÃO	OMISSÃO
TheHacker	Trojan/OnLineGames.srcn	Trojan/Kryptik.bike	Posible_Worm32
TotalDefense	Win32/QQPass.XI	BENIGNO	Win32/Rbot.EZH

Tabela 7. Parte 4: classificação dos antivírus comerciais.

Antivírus	VirusShare_00f6921f2a1ef6abcf691fb7e15bd997	VirusShare_0e0439c9f79b2c89d7967137832271f0	VirusShare_1ab4b5f294349e5c625f0b7b8b16965d
TrendMicro	TSPY_GAMETHI.A	TROJ_GEN.R0CBOC0HU13	TROJ_BANLOAD.CYC
TrendMicro-HouseCall	TSPY_GAMETHI.A	TROJ_GEN.R0CBOH0HU13	TROJ_BANLOAD.CYC
VBA32	BScope.Trojan-PSW.Gomex.21	Trojan.ShipUp	BENIGNO
VIPRE	Trojan.Win32.OnLineGames.CTB (v)	Trojan.Win32.Reveton.a (v)	Trojan.Win32.Generic!BT
ViRobot	Trojan.Win32.PSWIGames.535552.B	BENIGNO	OMISSÃO
VirusBuster	OMISSÃO	OMISSÃO	OMISSÃO
Webroot	W32.InfoStealer.OnlineGames.Gen	OMISSÃO	OMISSÃO
Webwasher-Gateway	OMISSÃO	OMISSÃO	OMISSÃO
WhiteArmor	OMISSÃO	OMISSÃO	OMISSÃO
Yandex	Trojan.OnlineGames.Gen.102	OMISSÃO	OMISSÃO
Zillya	Trojan.OnLineGames.Win32.13	OMISSÃO	OMISSÃO
ZoneAlarm	HEUR:Trojan.Win32.Generic	OMISSÃO	OMISSÃO
Zoner	BENIGNO	OMISSÃO	OMISSÃO

Capítulo 3

Metodologia Proposta

Dada as limitações demonstradas, pretende-se propor um antivírus, dotado de inteligência artificial, capaz de classificar aplicativos *ransomwares* e benignos de forma preventiva.

1.1. Materiais e Métodos

Este artigo propõe um banco de dados para a classificação de executáveis benignos e de *ransomwares* de 32 bits. Existem 1.174 *ransomwares* e 1.174 outros executáveis benignos (Ransomware, 2021), conjunto de dados para o aprendizado com inteligência artificial. Uma vez que ambas as classes de executáveis possuem a mesma quantidade, tem-se as condições adequadas para treinamento.

As Ameaças virtuais foram extraídas de bancos de dados fornecidos por grupos de estudo como a VirusShare (VirusShare_CryptoRansom_20160715), que é um repositório de amostras de *malwares* para fornecer a pesquisadores de segurança, analistas de incidentes, analistas forenses e curiosos da área de segurança amostras de código malicioso ativo (VirusShare, 2021). Quanto aos executáveis benignos, a aquisição veio de repositórios de aplicativos benignos, como sourceforge, github e sysinternals. Todos os executáveis benignos foram submetidos ao VirusTotal e todos eram benignos atestados pelos principais antivírus comerciais do mundo (VirusTotal, 2021).

O objetivo da criação do banco de dados é dar plena possibilidade de a metodologia proposta ser replicada por terceiros em trabalhos futuros. Portanto, espera-se que a metodologia sirva de base para a criação de novos trabalhos científicos.

1.2. Extração de Características dos Executáveis

A extração de características dos executáveis passa pelo processo de *disassembling* visando conhecer seu conteúdo a partir do código binários em mãos. Logo, o algoritmo, referente ao executável, pode ser estudado e posteriormente classificado pelas redes neurais descritas na próxima seção.

Também, Scripts próprios e a ferramenta pescanner, extrator das características descritas a seguir, são utilizadas na extração de informações dos executáveis. Especificamente, usa-se um ambiente controlado para manuseio de ameaças Linux, o REMnux (REMnux, 2021). Um kit de ferramentas Linux para engenharia reversa e análise de *software* malicioso. REMnux fornece uma coleção de ferramentas gratuitas criadas pela comunidade. Uma delas, pescanner.py, é um script incluso nessa distribuição Linux que permitiu fazer as análises nas amostras de *ransomwares* sem riscos de infecção já que foram analisados arquivos Windows em Linux.

No total, são extraídas 489 características, de cada executável da base criada. A seguir, são detalhadas os grupos de características extraídas referentes ao algoritmo dos executáveis investigados:

- ✓ Histograma das instruções responsáveis pela aquisição de dados (*imports*).
- ✓ Quantidade de sub-rotinas que invocam o TLS (*Transport Layer Security*).
- ✓ Quantidade de sub-rotinas responsáveis pela exportação de dados (*exports*).
- ✓ Histograma das importações das API (*Application Programming Interface* - Interface de Programação de Aplicações) empregadas pelo executável.
- ✓ Características relacionadas a indícios que o computador tenha sofrido fragmentação no seu disco rígido, além de tentativas de inicialização inválidas acumuladas.
- ✓ Modo de execução do aplicativo. Há duas opções:
    - *softwares* dotados de interface gráfica (GUI);
    - *softwares* executados no console.
- ✓ Características relacionadas ao Sistema Operacional - averigua se o arquivo testado tenta:

- identificar o nome do usuário atual do sistema operacional;
- acessar funções de *interface* de programação de aplicativo (API) para criar e gerenciar perfis de usuário atual do SO;
- detectar o número de milissegundos decorridos desde que o sistema foi inicializado;
- executar uma operação em um arquivo especifico;
- identificar a versão do Sistema Operacional Windows em uso;
- monitorar o tráfego de mensagens internas entre os processos do sistema;
- alterar as configurações e conteúdo da inicialização (STARTUPINFO) do SO Windows;
- permitir que aplicativos acessem a funcionalidade fornecida pelo *shell* do sistema operacional, além de alterá-lo;
- alterar as mensagens de logon na inicialização do SO Windows;
- alterar aplicativos nativos atrelados a caixas de diálogo padrão para abrir e salvar arquivos, escolhendo cor e fonte, dentre outras customizações;
- configurar o licenciamento do Servidor Windows;
- configurar o Windows Server 2003;
- alterar as configurações de energia do Sistema;
- abrir um processo, serviço ou biblioteca nativa do Sistema Operacional;
- excluir o contexto de certificados vinculados ao Sistema Operacional;
- copiar um arquivo existente para um novo arquivo;
- criar, abrir, excluir ou alterar um arquivo;
- criar e executar novo(s) processo(s).
- criar novo(s) diretório(s);
- procurar por arquivo(s) específico(s);
- criar um objeto de serviço e o adicionar ao banco de dados do gerenciador de controle de um determinado serviço;
- criptografar dados - estratégia é típica de *ransomwares* os quais sequestram os dados da vítima através da criptografia. Para recuperar os dados, o invasor pede ao usuário um montante monetário para ter

de volta todos os seus dados;

- acessar sistemas de arquivos, dispositivos, processos, *threads* e tratamento de erros;
- alterar as propriedades de som e dispositivo de áudio do sistema;
- acessar informações de conteúdo gráfico para monitores, impressoras e outros dispositivos de saída do SO Windows;
- usar e/ou monitorar a porta USB.
- controlar um *driver* de um determinado dispositivo;
- investigar se uma unidade de disco é uma unidade removível, fixa, de CD/DVD-ROM, de RAM ou de rede;

✓ Características relacionadas ao Registro (Regedit) do SO Windows. Cabe ressaltar que a vítima pode não estar livre da infecção de um *malware* mesmo após a sua detecção e eliminação. A persistência das malfeitorias, mesmo após a exclusão do *malware*, ocorre devido à inserção de entradas (chaves) maliciosas no Regedit. Logo, quando o sistema operacional é inicializado, o *cyber*-ataque recomeça devido à chave mal-intencionada invocar a vulnerabilidade explorada pelo *malware* (e.g.: redirecionar a página inicial do Internet Explorer). Logo, o antivírus criado audita se o aplicativo suspeito tenta:

- detectar o nome NetBIOS do computador local. Esse nome é estabelecido na inicialização do sistema, quando o sistema o lê no registro (Regedit);
- encerrar uma chave de um registro especifico;
- criar uma chave de um registro específico. Caso a chave já exista no Regedit, então, ela será lida;
- excluir uma chave e seus valores no Regedit;
- enumerar e abrir as subchaves da chave de um registro aberto específico.

✓ Características relacionadas a *spywares* como *keyloggers* (captura de informações do teclado visando o furto de senhas e *logins*) e *screenloggers* (filmagem da tela da vítima). Audita se o arquivo analisado tenta:

- detectar, em qual parte da tela da vítima, houver uma atualização;
- identificar a região de atualização da tela copiando-a para uma

determinada região;

- capturar filmes e vídeos AVI de câmeras da Web e outros hardwares de vídeo;
- capturar informações quanto à votação eletrônica, especificamente, da empresa *Optical Vote-Trakker*;
- copiar uma matriz de estados das teclas do teclado. Tal estratégia é típica dos *keyloggers*;
- monitorar a atividade da Internet do usuário e informações particulares;
- coletar senhas bancárias on-line e outras informações confidenciais e enviar os dados para seu criador;
- acessar um computador a partir de locais remotos, roubando senhas, transações bancárias pela Internet e dados pessoais;
- criar um BHO (Objeto de Auxílio ao Navegador) o qual é executado automaticamente toda vez que o navegador web for iniciado. Cabe ressaltar que os BHOs não são impedidos por firewalls pessoais porque são identificados como parte do próprio navegador. De maneira desvirtuada, os BHOs são frequentemente usados por adware e spyware visando gravar entradas de teclado e do mouse;
- localizar senhas armazenadas em um computador.

✓ Características relacionadas à anti-perícia Digital as quais são técnicas de remoção, ocultação e subversão de evidências com o objetivo de reduzir as consequências dos resultados de análises forense. Caso o arquivo periciado tente:

- suspender a sua própria execução até que um determinado intervalo de tempo limite tenha decorrido. Estratégia típica dos *malwares* que ficam inativos até o término da quarentena dos antivírus comerciais;
- desabilitar os mecanismos de defesa da vítima, inclui-se Firewall e Antivírus;
- desabilitar as atualizações automáticas do Windows;
- detectar se o próprio arquivo está sendo analisado por um depurador do Sistema Operacional;
- recuperar informações sobre o primeiro e o próximo processo encontrado em um snapshot do Sistema Operacional. Estratégia é

típica de *malwares* que visam corromper backups e pontos de restauração do Sistema Operacional;

- ocultar um arquivo em outro. Estratégia é denominada, tecnicamente, de esteganografia o qual visa esconder o *malware* em um programa benigno no Gerenciador de Tarefas;
- disfarçar o seu próprio nome no Gerenciador de Tarefas;
- fazer uso de bibliotecas associadas ao Hackers Encyclopedia 2002;
- criar um cyber-ataque do tipo ZeroAcess através de atualizações dos firmwares dos dispositivos de hardware (e.g.: controlada do disco rígido).

✓ Características relacionadas à criação de GUI (*Graphical User Interface* – Interface Gráfica do Usuário) do programa suspeito. Audita se o arquivo suspeito tenta:

- criar uma GUI em tempo de execução;
- usar o DirectX o qual permite que aplicativos multimídia desenhem gráficos 2D;
- criar módulo que contém rotinas de compactação e descompactação de bitmap usadas para o Microsoft Vídeo para Windows;
- criar gráficos 3D relacionadas a funções utilitárias usadas pelo OpenGL;
- detectar formas através de visão computacional e processamento digital de imagem;
- acessar funcionalidades visando criar e gerenciar janelas de tela e controles mais básicos, como botões e barras de rolagem, receber entrada de mouse e teclado e outras funcionalidades associadas à parte de GUI do Windows. Isso inclui coisas como barras de status, barras de progresso, barras de ferramentas e guias;

✓ Características relacionada à perícia ilícita da memória principal (RAM) do sistema local. Investiga se o aplicativo suspeito tenta:

- acessar informações em regiões específicas da memória principal;
- ler dados de uma área de memória ocupada por um processo específico;
- Gravar dados em uma área de memória em um processo específico;

- Reservar, confirmar ou alterar o estado de uma região de páginas no espaço de endereço virtual de um processo.

✓ Características relacionadas ao tráfego de rede. Averígua-se se o arquivo testado tenta:

- consultar servidores DNS;
- enviar solicitação para um o servidor HTTP;
- monitorar informações dos cabeçalhos dos pacotes de dados do computador associadas a uma solicitação HTTP;
- enviar uma solicitação de eco IPv4 ICMP;
- enviar uma solicitação SNMP utilizada para monitorizar equipamentos de rede local;
- encerrar a conexão com a Internet;
- criar uma sessão FTP ou HTTP em tempo de execução;
- fragmentar uma URL em tempo de execução;
- consultar um servidor para determinar a quantidade de dados disponíveis de tráfego;
- identificar o estado de conexão do sistema local em relação à Internet;
- inicializar o uso de um aplicativo das funções do WinINet (API do Windows visando a criação e utilização de aplicação utilizando a Internet);
- ler dados dos pacotes de rede feita a partir de requisições prévias do sistema local (comportamento típico de *sniffers*);
- sobrescrever dados em um pacote de rede do sistema local;
- gerenciar sistemas de rede locais e remotos;
- criar um *socket* de rede no sistema local. Em uma aplicação convencional, o servidor envia dados para o(s) cliente(s) de forma inversa, nos *malwares*, a vítima envia os dados (imagens, dígitos) para o servidor. Logo, os *malwares* podem criar sockets, no sistema local, aguardando (*listen*) que um computador mal intencionado remoto requisite uma conexão e, portanto, possa receber as informações íntimas da vítima;
- Receber dados de um socket. Estratégia típica de *backdoors* quando a vítima passa a receber comandos (ordens) remotos;

- Enviar dados em um socket. Estratégia típicas de *spywares* os quais, após a captura de informações íntimas, as enviam para um computador remoto mal-intencionado.

✓ Características relacionadas a programas aplicativos utilitários. O antivírus criado verifica se o arquivo suspeito tenta:

- reproduzir vídeos/áudios pelo *Windows Media Player*;
- alterar ícone atalho e configurações padrões de Internet exibidos na barra de endereços da barra de ferramentas do Explorer;
- alterar as configurações do *Wordpad*;
- alterar as configurações dos sockets, especificamente, gerenciados pela internet Explorer;
- alterar as configurações do Outlook Express e acessar a lista de contatos de e-mail da vítima;
- acessar informações atreladas ao *Microsof Office*;
- alterar as configurações do suíte da *Adobe Systems*;
- alterar as configurações da limpeza de disco do Sistema;
- alterar as configurações de jogos eletrônicos digitais nativos além dos vinculados às empresas *Tycoon*e *Electronic Arts*;
- alterar as configurações de atualizações do *Google Inc*;
- usar o *software* Visual Basic. Tal estratégia é típica dos vírus de macro os quais são visam infectar os aplicativos que suportam linguagem de macro como os navegadores web, o *Microsoft Office* e o *Adobe Systems*.
- alterar as configurações de acesso ao Wikipédia;

Caraterísticas descritas usando as informações contidas do relatório resultante da execução *pescanner* em cada arquivo investigado. A cada característica encontrada foi feita uma pesquisa no site de desenvolvedores da Microsoft para validar a funcionalidade de uma dada biblioteca ou função chamada pelo executável cujo relatório foi avaliado. Por exemplo, a descrição da biblioteca “winsock2.h” foi obtida em https://docs.microsoft.com/en-us/windows/win32/api/winsock2/nf-winsock2-socket.

Por meio da descrição das características auditadas pelo antivírus proposto, é possível estabelecer que os *ransomwares*, em grande parte dos casos, empregam serviços lícitos nativos do sistema operacional, no entanto, de forma desvirtuada (CONRAD, MISENAR, & and FELDMAN, 2017). Os *ransomwares*, por exemplo, usam o navegador de internet da vítima sem o seu consentimento. Conclui-se que é equivocado condenar um aplicativo por ele fazer uso de um determinado processo (e.g. webcam). Em síntese, é incorreto condenar uma aplicação por conta de uma única característica, pois tal característica também pode ser usada por aplicações benignas. Então, o reconhecimento de *ransomwares* deve ocorrer através do cruzamento de informações e, consequentemente, a ponderação de todos os comportamentos auditados.

1.3. Classificadores

Quanto ao reconhecimento de padrão de *ransomwares*, uma tarefa essencial diz respeito à atribuição de uma classe (rótulo) a cada arquivo investigado a partir de suas características. Então, com base em um conjunto de arquivos, chamado de conjunto de treinamento, é possível formular uma hipótese sobre as distintas classes atreladas ao antivírus inteligente proposto. Logo, cabe ao classificador estimar a classe de um arquivo inédito através da comparação entre as características do seu comportamento auditado e àquelas captadas durante a sua etapa de treinamento.

O objetivo do classificador é obter uma função de separação entre as classes do antivírus criado (*ransomware*, benigno). Dessa forma, ao ser apresentado a um aplicativo inédito, a função é aplicada e, então, atribui-se uma classe na qual esse aplicativo suspostamente pertence. Matematicamente, $c = f(x)$, onde $x = x_1, x_2, \dots, x_t$ é um vetor características extraídas do arquivo investigado, t corresponde às 429 características auditadas,c é a classe (rótulo), por fim, f é a função de mapeamento do classificador.

Especificamente, são empregadas as redes neurais do tipo MLP (*Multilayer Perceptron* - *Perceptron* com Múltiplas Camadas) dotadas de retropropagação como classificadores. Uma rede MLP é uma generalização da rede *Perceptron* simples pela adição de, ao menos, uma camada intermediária (HAGAN, H.B., & M.H., 1996). Convencionalmente, as redes MLP apresentam 3 (três) camadas: uma camada de

entrada, ao menos uma camada intermediária e uma camada de saída. Na camada de entrada, cada neurônio de entrada representa uma variável considerada como entrada para o problema. No antivírus inteligente criado, há 429 neurónios e dizem respeito a comportamentos maliciosos descritos na seção 1.1. Na camada escondida, há o encargo pela não linearidade da rede neural. Por fim, na camada de saída, há o reconhecimento do padrão quanto à resposta da rede e representa a variável desejada. No antivírus inteligente criado, a camada de saída possui dois neurônios correspondentes aos aplicativos benignos e *ransomwares*.

As redes MLP, baseadas em retropropagação, utilizam basicamente dois passos. No primeiro passo, há a propagação de dados (impulso sináptico) da camada de entrada para a camada de saída. Nesse passo, há o cálculo do sinal de saída e o erro (HAGAN, H.B., & M.H., 1996). O erro é a diferença entre o sinal de saída obtida e a saída desejada. Após isso, no segundo passo, há a propagação de dados partindo da camada de saída em direção à camada de entrada. Esse passo é conhecido como retropropagação e visa ajustar os pesos referentes às ligações sinápticas entre os neurônios. Cabe ressaltar que os pesos são determinados, inicialmente, de forma aleatória.

Com o objetivo de otimizar a precisão do antivírus criado, são averiguadas onze diferentes funções de aprendizado f baseadas em classificadores MLP dotados de retropropagação. A seguir, são detalhadas todas as onze diferentes formas de implementações das redes MLPs empregadas:

- ✓ Lotes de peso e limite bias: emprega um atualizações em lotes, que são atualizados ao final de cada época (HAGAN, H.B., & M.H., 1996).
- ✓ Gradiente Powell-Beale: emprega o método de retropropagação do gradiente conjugado baseado na técnica Powell-Beale (Powell, 1977).
- ✓ Retropropagação Fletcher-Powell: utiliza o método de retropropagação do gradiente conjugado baseado na técnica Fletcher-Reeves (NOTAY, 2000).
- ✓ Retropropagação Polak-Ribiere: aplica o método de retropropagação do gradiente conjugado inspirado na técnica Polak-Ribiere (SCALES, 1985).
- ✓ Retropropagação decrescente: emprega o método de retropropagação baseado em um gradiente descendente (HAGAN, H.B., & M.H., 1996).
- ✓ Retropropagação com momentos: emprego o método de retropropagação

baseado em um gradiente descendente com momentos. Esse classificador permite que a rede neural não apenas se baseie em informações locais, mas também tenha a capacidade de ignorar ruídos do gradiente. O objetivo é que a rede neural não se atenha a um mínimo local (HAGAN, H.B., & M.H., 1996).

- ✓ Retropropagação com taxa adaptativa: implementa uma taxa de aprendizagem adaptativa a qual se guia baseada nas informações do gradiente. Uma taxa de aprendizagem fixa pode apresentar problemas durante o treinamento. Uma taxa de aprendizagem fixa muito alta, o classificador pode oscilar e se tornar instável. Por outro lado, caso a taxa de aprendizagem fixa for muito baixa, o tempo de treinamento pode se tornar bastante elevado (HAGAN, H.B., & M.H., 1996).
- ✓ Retropropagação combinada: é a junção da retropropagação com taxa adaptativa com a retropropagação baseada em momentos. Isso quer dizer, essa rede neural não se baseia apenas em informações locais como também possui uma taxa de aprendizagem adaptativa (HAGAN, H.B., & M.H., 1996).

- ✓ Retropropagação secante em um passo: implementa a retropropagação do gradiente conjugado baseado na técnica da secante em um único passo (BATTITI, 1992).
- ✓ Retropropagação resiliente (Rprop): emprega o método de retropropagação do gradiente conjugado baseado no algoritmo Rprop (Riedmiller & Braun, 1993).
- ✓ Retropropagação gradiente escalonado: emprego o método de retropropagação do gradiente conjugado escalonado (Moller, 1993).

Nas redes neurais MLP, condições iniciais convenientes podem fazer com que a rede convirja em poucas épocas. Por outro lado, condições iniciais inadequadas podem demandar uma grande quantidade de épocas até a rede adquirir capacidade de generalização e, portanto o treinamento ser encerrado. Então, um cuidado metodológico adotado é averiguar a influência das condições iniciais nos resultados alcançados dos classificadores. Logo, são utilizados 30 (trinta) diferentes pesos iniciais aleatórios referentes às ligações sinápticas entre os neurônios. As variações são aleatórias com a semente do gerador aleatório entre 1 e 30 de maneira incremental.

A quantidade de pesos iniciais foi estabelecida como 30 (trinta) sementes de gerador aleatório. A motivação é que 30 (trinta) iterações constituem uma quantidade estatisticamente significativa de modo a se determinar o grau de dispersão das amostras. Então, para cada rede neural (função de aprendizado), são avaliadas 30 (trinta) amostras assim como ocorrem em diversas áreas como, por exemplo, em Engenharia Biomédica (LIMA, SILVA-FILHO, & SANTOS, 2016). Na Tabela 8 dos resultados, no capítulo seguinte, a dispersão é representada através do desvio padrão das 30 (trinta) iterações de cada função de aprendizado avaliada. Então, quanto menor o desvio padrão implica que a rede neural avaliada não sofre mudanças abruptas em função dos pesos iniciais aleatórios referentes às ligações sinápticas entre os neurônios. De modo oposto, quanto maior for o desvio padrão significa que a rede neural sobre brusca alteração, em sua precisão, em função dos pesos iniciais das ligações sinápticas.

Há o uso de três arquiteturas para cada MLP. A primeira arquitetura utiliza uma única camada escondida, com 100 neurônios. A segunda arquitetura utiliza duas camadas escondidas, com 100 neurônios cada. Os resultados da segunda abordagem são simbolizados com um asterisco. Por fim, a terceira arquitetura emprega uma camada escondida, no entanto, são utilizados 500 neurônios. A terceira abordagem é simbolizada através de dois asteriscos na Tabela 8 que exibirá os resultados alcançados. A hipótese é verificar se o aumento da quantidade de neurônios e, consequentemente, o aumento de cálculos numéricos da rede neural é capaz de prover melhores resultados. Para cada função de aprendizado, há 90 (3 arquiteturas * 30 pesos iniciais) iterações. São exploradas 3 (três) tipos de arquiteturas e 30 (trinta) diferentes pesos iniciais, referentes às ligações sinápticas entre os neurônios, para cada arquitetura

Quanto aos dados de entrada, 70% dos dados são destinados ao treinamento, 15% é reservado à validação cruzada, por fim 15% é utilizado à fase de testes. O número máximo de épocas, para treinamento, é 1000 (um mil). A validação cruzada ocorre após cada época com o objetivo da rede neural não perder a sua capacidade de generalização. Há uma tolerância de 5 (cinco) falhas para a validação cruzada. O tempo de treinamento das MLPs engloba, obviamente, o tempo gasto no treinamento juntamente com o tempo destinado à validação cruzada.

Capítulo 4

Resultados

Da Tabela 8 à Tabela 10, há a exibição da classificação dos resultados usando as redes MLP baseadas em retropropagação. Os melhores casos são destacados em negrito. O primeiro e segundo critérios são a média aritmética e o desvio padrão, respectivamente. São utilizadas onze diferentes funções de aprendizado. Para cada função, são estudados três tipos distintos de arquitetura, descritas na seção 1.3 do capítulo 3. Quanto ao tempo de treinamento, os classificadores apresentam tempos elevados assim como os desvios padrões. Esse fato indica que as MLPs sofrem variações abruptas, em relação ao tempo de treinamento, a depender dos pesos iniciais referentes às ligações sinápticas entre os neurônios. Conforme estabelecido, “”, “*”, “**” correspondem às arquiteturas com 1 (uma) camada escondida com 100 neurônios, 2 (duas) camadas escondidas cada qual com 100 neurônios e 1 (uma) camada escondida com 500 neurônios, respectivamente.

No tocante à precisão, a mínima taxa de acerto foi de 48,45% para a rede que emprega o Rprop (Retroprogação Resiliente). Essa abordagem possui uma arquitetura com uma camada escondida com 500 neurônios. Enquanto, a máxima precisão foi de 99,99% para a rede inspirada em Retropropagação Fletcher-Powell*. A arquitetura, dessa rede, contém duas camadas escondidas com 100 neurônios. Note também que o desvio padrão é de 0%. Demonstra o excelente desempenho da função de aprendizado do gradiente conjugado baseado na técnica Fletcher-Reeves, independente das condições iniciais.

Quanto ao tempo de treinamento, os classificadores baseados em retropropagação apresentam desvios padrões altos. Isso indica que as redes MLPs sofrem variações abruptas, em relação a tempo de aprendizado, a depender do conjunto de pesos iniciais. Observa-se que, em regra geral, ao expandir a quantidade de neurônios na camada escondida, também cresce o tempo de treinamento devido a um maior volume de cálculos da rede neural.

Quanto às arquiteturas das redes, aumentar a quantidade de camadas escondidas ou aumentar a sua quantidade de neurônios, não implica em um melhor desempenho de maneira sistemática. Em várias situações, aumentar a quantidade de neurônios na camada escondida provocou uma degradação no desempenho acompanhada de um maior tempo destinado ao treinamento devido ao grande volume de cálculos. Logo, a exploração de diferentes tipos de arquiteturas de redes neurais foi uma decisão salutar visto que não houve uma arquitetura ótima independente da variação da função de aprendizado.

Então, a inteligência artificial se torna uma boa alternativa para as fabricantes dos antivírus comerciais. Durante sua etapa de aprendizado, é capaz de analisar milhares de *ransomwares* e extrair características deles. Especificamente, são extraídas 429 características referentes ao algoritmo do arquivo suspeito. Então, após o aprendizado, caso um novo arquivo, ainda não catalogado, fosse investigado, haveria a possibilidade de ser corretamente classificado, como *ransomware*. O correto reconhecimento de padrão se dá através da comparação entre as características do seu código fonte e as aquelas captadas durante o processo de aprendizado da inteligência artificial.

Tabela 8. Parte 1: resultados das redes baseadas em retropropagação para classificação em duas classes de executáveis: benignos e *ransomwares*.

Função de aprendizado	Acerto treino (%)	Acerto teste (%)	Tempo treino (seg.)	Tempo teste (seg.)
Lotes de peso e limite bias	52,39 ± 16,93	52,61 ± 17,14	10,81 ± 29,9	0,03 ± 0,02
Lotes de peso e limite bias*	60,36 ± 20,62	60,42 ± 20,74	29,33 ± 57,32	0,03 ± 0,03
Lotes de peso e limite bias**	49,9 ± 10,9	49,52 ± 11,57	1,32 ± 1	0,04 ± 0,03
Gradiente Powell-Beale	98,92 ± 2,97	99,35 ± 2,01	16,23 ± 9,6	0,03 ± 0,02
Gradiente Powell-Beale*	99,55 ± 2,18	99,73 ± 1,45	25,65 ± 14,6	0,03 ± 0,02
Gradiente Powell-Beale**	98,88 ± 2,57	99,25 ± 2,1	36,98 ± 30,51	0,04 ± 0,04
Retropropagação Fletcher-Powell	99,09 ± 3,46	99,35 ± 2,49	55,7 ± 34,55	0,03 ± 0,02
Retropropagação Fletcher-Powell*	**99,99 ± 0,02**	**99,99 ± 0**	82,54 ± 58,28	0,03 ± 0,02
Retropropagação Fletcher-Powell**	99,07 ± 2,34	99,38 ± 1,67	85,98 ± 114,69	0,05 ± 0,03

Tabela 9. Parte 2: Resultados das redes baseadas em retropropagação para classificação em duas classes de executáveis: benignos e *ransomwares*.

Função de aprendizado	Acerto treino (%)	Acerto teste (%)	Tempo treino (seg.)	Tempo teste (seg.)
Retropropagação Polak-Ribiere	98,97 ± 2,93	99,31 ± 2,16	16,9 ± 10,28	0,02 ± 0,02
Retropropagação Polak-Ribiere*	99,53 ± 2,05	99,73 ± 1,4	24,39 ± 13,22	0,03 ± 0,02
Retropropagação Polak-Ribiere**	98,91 ± 2,48	99,24 ± 2,09	39,35 ± 30,48	0,06 ± 0,03
Retropropagação decrescente	87,96 ± 11,36	89,66 ± 11,57	8,92 ± 17,72	0,02 ± 0,02
Retropropagação decrescente*	87,2 ± 15,81	87,7 ± 15,47	37,23 ± 38,99	0,02 ± 0,02
Retropropagação decrescente **	49,31 ± 9,21	49,04 ± 10,14	1,68 ± 0,74	0,05 ± 0,04
Retropropagação com momentos	52,39 ± 16,93	52,61 ± 17,14	5,96 ± 16,47	0,02 ± 0,02
Retropropagação com momentos*	60,36 ± 20,62	60,42 ± 20,74	16,25 ± 31,47	0,02 ± 0,02
Retropropagação com momentos**	49,9 ± 10,9	49,52 ± 11,57	1,17 ± 0,92	0,06 ± 0,04
Retropropagação com taxa adaptativa	91,2 ± 3,35	93,18 ± 2,87	5,12 ± 1,73	**0,02 ± 0,02**
Retropropagação com taxa adaptativa*	90,82 ± 4,98	92,52 ± 5,03	6,46 ± 2,03	0,03 ± 0,03
Retropropagação com taxa adaptativa**	92,32 ± 8,44	93,23 ± 8,3	44,39 ± 33,63	0,05 ± 0,03
Retropropagação combinado	95,12 ± 8,34	96,27 ± 7,79	6,15 ± 2,21	0,02 ± 0,02
Retropropagação combinado*	97,15 ± 4,77	98 ± 4,73	8,24 ± 2,36	0,03 ± 0,02
Retropropagação combinado**	96,04 ± 9,75	96 ± 10,06	32,24 ± 10,85	0,04 ± 0,03
Retropropagação secante em um passo	99,92 ± 0,08	99,99 ± 0,05	18,38 ± 6,67	0,03 ± 0,02
Retropropagação secante em um passo*	99,87 ± 0,15	99,97 ± 0,09	21,52 ± 9,22	0,03 ± 0,02
Retropropagação secante em um passo**	99,9 ± 0,09	99,98 ± 0,07	51,95 ± 29,29	0,04 ± 0,03

Tabela 10. Parte 3: Resultados das redes baseadas em retropropagação para classificação em duas classes de executáveis: benignos e *ransomwares*.

Função de aprendizado	Acerto treino (%)	Acerto teste (%)	Tempo treino (seg.)	Tempo teste (seg.)
Retropropagação resiliente (Rprop)	55,19 ± 18,12	55,45 ± 18,36	1,05 ± 2,18	0,03 ± 0,02
Retropropagação resiliente (Rprop)*	49,79 ± 7,94	49,94 ± 7,5	**0,38 ± 0,08**	0,03 ± 0,02
Retropropagação resiliente (Rprop)**	48,85 ± 7,62	48,45 ± 8,23	0,66 ± 0,09	0,04 ± 0,03
Retropropagação gradiente escalonado	99,88 ± 0,07	99,99 ± 0,05	8,61 ± 3,36	0,03 ± 0,02
Retropropagação gradiente escalonado*	99,91 ± 0,09	99,98 ± 0,07	12,6 ± 4,94	0,03 ± 0,02
Retropropagação gradiente escalonado**	99,99 ± 0,04	99,99 ± 0	38,25 ± 16,28	0,05 ± 0,03

Um antivírus, ao empregar inteligência artificial, consegue automatizar a análise de centenas de características de arquivos suspeitos em larga escala e em tempo real. Logo, não seria mais necessário aguardar que algum cliente fosse infectado e, em sequência denunciasse um comportamento anômalo de seu dispositivo, para, então, tomar-se providências quanto à detecção de um novo *ransomware*. Cabe salientar que as malfeitorias dos *ransomwares* podem ser irreversíveis e irrecuperáveis. Logo, um antivírus deve detectar as pragas virtuais de forma preventiva ao invés de reativa. A inteligência artificial possibilita a detecção preventiva da praga virtual antes mesmo dela ser executada pela cliente. O antivírus inteligente criado alcança um desempenho médio de 99,99% na distinção entre executáveis benignos e *malwares*, acompanhado de um tempo de resposta médio de apenas 0,03 segundos.

Da Tabela 11 à Tabela 15, há exibição das matrizes de confusão das técnicas apresentadas da Tabela 8 à Tabela 10 em termos percentuais. A matriz de confusão é importante para a verificação da qualidade de um aprendizado supervisionado. Da Tabela 11 à Tabela 15, verdadeiros negativos significam os aplicativos sérios classificados corretamente como benignos, De maneira análoga, verdadeiros positivos dizem respeito aos ransomwares detectados pelos classificadores avaliados. Falsos positivos são os aplicativos benignos classificados erroneamente como maliciosos. Por fim, falsos negativos são os *ransomwares*

absolvidos de maneira equivocada pelos classificadores. Então, um bom classificador deve ter valores de verdadeiros negativos e verdadeiros positivos elevados enquanto as demais posições devem possuir valores baixos.

Na perícia forense digital, um falso positivo implicaria em um aplicativo benigno impedido de ser executado pelo sistema. Um falso negativo, no entanto, pode implicar em um ransomware que não foi detectado. Vale salientar que os *ransomwares* podem gerar malefícios irreversíveis e irrecuperáveis para toda a rede mundial de computadores. Isso posto, um falso negativo pode implicar na perda da dignidade, das finanças e da saúde mental da vítima.

Ainda quanto da Tabela 11 à Tabela 15, sensibilidade e especificidade dizem respeito à capacidade do antivírus identificar os aplicativos *ransomwares* e benignos, respectivamente. O trabalho proposto apresenta a matriz de confusão em termos percentuais de modo a facilitar a interpretação da sensibilidade e especificidade. Em síntese, a sensibilidade e a especificidade estão apresentadas na própria matriz de confusão, descrita da Tabela 11 à Tabela 15. Por exemplo, verdadeiros positivos estão relacionados à sensibilidade. Seguindo o mesmo raciocínio, os verdadeiros negativos estão associados à especificidade.

Tabela 11. Parte 1: Matrizes de confusão das redes neurais apresentadas da Tabela 8 à Tabela 10.

Função de Aprendizado	Respostas Possíveis	Treino	teste
Lotes de peso e limite bias	Verdadeiro Negativo	48,49% ± 49,09%	48,54% ± 49,08%
	Falso Positivo	43,71% ± 42,67%	43,31% ± 42,26%
	Falso Negativo	51,51% ± 49,09%	51,46% ± 49,08%
	Verdadeiro Positivo	56,29% ± 42,67%	56,69% ± 42,26%
Lotes de peso e limite bias*	Verdadeiro Negativo	66,75% ± 47,57%	66,74% ± 47,60%
	Falso Positivo	46,03% ± 45,32%	45,91% ± 44,97%
	Falso Negativo	33,25% ± 47,57%	33,26% ± 47,60%
	Verdadeiro Positivo	53,97% ± 45,32%	54,09% ± 44,97%
Lotes de peso e limite bias**	Verdadeiro Negativo	66,75% ± 47,57%	66,74% ± 47,60%
	Falso Positivo	46,03% ± 45,32%	45,91% ± 44,97%
	Falso Negativo	33,25% ± 47,57%	33,26% ± 47,60%
	Verdadeiro Positivo	53,97% ± 45,32%	54,09% ± 44,97%

Tabela 12. Parte 2: Matrizes de confusão das redes neurais apresentadas da Tabela 8 à Tabela 10.

Função de Aprendizado	Respostas Possíveis	Treino	teste
Gradiente Powell-Beale	Verdadeiro Negativo	99,99% ± 0,05%	99,98% ± 0,10%
	Falso Positivo	2,15% ± 5,91%	1,29% ± 4,01%
	Falso Negativo	0,01% ± 0,05%	0,02% ± 0,10%
	Verdadeiro Positivo	97,85% ± 5,91%	98,71% ± 4,01%
Gradiente Powell-Beale*	Verdadeiro Negativo	99,99% ± 0,05%	99,98% ± 0,10%
	Falso Positivo	0,88% ± 4,32%	0,51% ± 2,80%
	Falso Negativo	0,01% ± 0,05%	0,02% ± 0,10%
	Verdadeiro Positivo	99,12% ± 4,32%	99,49% ± 2,80%
Gradiente Powell-Beale**	Verdadeiro Negativo	99,63% ± 1,10%	99,62% ± 1,30%
	Falso Positivo	1,86% ± 4,07%	1,12% ± 2,93%
	Falso Negativo	0,37% ± 1,10%	0,38% ± 1,30%
	Verdadeiro Positivo	98,14% ± 4,07%	98,88% ± 2,93%
Retropropagação Fletcher-Powell	Verdadeiro Negativo	99,98% ± 0,11%	100,00% ± 0,00%
	Falso Positivo	1,79% ± 6,83%	1,31% ± 4,99%
	Falso Negativo	0,02% ± 0,11%	0,00% ± 0,00%
	Verdadeiro Positivo	98,21% ± 6,83%	98,69% ± 4,99%
Retropropagação Fletcher-Powell*	Verdadeiro Negativo	100,00% ± 0,00%	100,00% ± 0,00%
	Falso Positivo	0,01% ± 0,05%	0,00% ± 0,00%
	Falso Negativo	0,00% ± 0,00%	0,00% ± 0,00%
	Verdadeiro Positivo	99,99% ± 0,05%	100,00% ± 0,00%
Retropropagação Fletcher-Powell**	Verdadeiro Negativo	99,55% ± 1,78%	99,53% ± 1,69%
	Falso Positivo	1,40% ± 3,47%	0,76% ± 2,06%
	Falso Negativo	0,45% ± 1,78%	0,47% ± 1,69%
	Verdadeiro Positivo	98,60% ± 3,47%	99,24% ± 2,06%
Retropropagação Polak-Ribiere	Verdadeiro Negativo	100,00% ± 0,02%	99,98% ± 0,10%
	Falso Positivo	2,06% ± 5,84%	1,36% ± 4,24%
	Falso Negativo	0,00% ± 0,02%	0,02% ± 0,10%
	Verdadeiro Positivo	97,94% ± 5,84%	98,64% ± 4,24%
Retropropagação Polak-Ribiere*	Verdadeiro Negativo	99,98% ± 0,09%	100,00% ± 0,00%
	Falso Positivo	0,92% ± 4,01%	0,55% ± 2,80%
	Falso Negativo	0,02% ± 0,09%	0,00% ± 0,00%
	Verdadeiro Positivo	99,08% ± 4,01%	99,45% ± 2,80%
Retropropagação Polak-Ribiere**	Verdadeiro Negativo	99,74% ± 0,78%	99,68% ± 0,90%
	Falso Positivo	1,93% ± 4,21%	1,19% ± 3,38%
	Falso Negativo	0,26% ± 0,78%	0,32% ± 0,90%
	Verdadeiro Positivo	98,07% ± 4,21%	98,81% ± 3,38%

Tabela 13. Parte 3: Matrizes de confusão das redes neurais apresentadas da Tabela 8 à Tabela 10.

Função de Aprendizado	Respostas Possíveis	Treino	teste
Retropropagação decrescente	Verdadeiro Negativo	92,30% ± 17,75%	92,10% ± 17,36%
	Falso Positivo	16,38% ± 12,50%	12,78% ± 11,51%
	Falso Negativo	7,70% ± 17,75%	7,90% ± 17,36%
	Verdadeiro Positivo	83,62% ± 12,50%	87,22% ± 11,51%
Retropropagação decrescente*	Verdadeiro Negativo	94,75% ± 14,05%	94,64% ± 13,22%
	Falso Positivo	20,35% ± 27,33%	19,24% ± 27,10%
	Falso Negativo	5,25% ± 14,05%	5,36% ± 13,22%
	Verdadeiro Positivo	79,65% ± 27,33%	80,76% ± 27,10%
Retropropagação decrescente **	Verdadeiro Negativo	37,33% ± 45,69%	36,99% ± 45,77%
	Falso Positivo	38,71% ± 39,93%	38,90% ± 39,75%
	Falso Negativo	62,67% ± 45,69%	63,01% ± 45,77%
	Verdadeiro Positivo	61,29% ± 39,93%	61,10% ± 39,75%
Retropropagação com momentos	Verdadeiro Negativo	48,49% ± 49,09%	48,54% ± 49,08%
	Falso Positivo	43,71% ± 42,67%	43,31% ± 42,26%
	Falso Negativo	51,51% ± 49,09%	51,46% ± 49,08%
	Verdadeiro Positivo	56,29% ± 42,67%	56,69% ± 42,26%
Retropropagação com momentos*	Verdadeiro Negativo	66,75% ± 47,57%	66,74% ± 47,60%
	Falso Positivo	46,03% ± 45,32%	45,91% ± 44,97%
	Falso Negativo	33,25% ± 47,57%	33,26% ± 47,60%
	Verdadeiro Positivo	53,97% ± 45,32%	54,09% ± 44,97%
Retropropagação com momentos**	Verdadeiro Negativo	37,90% ± 46,36%	37,57% ± 46,44%
	Falso Positivo	38,10% ± 40,12%	38,54% ± 40,11%
	Falso Negativo	62,10% ± 46,36%	62,43% ± 46,44%
	Verdadeiro Positivo	61,90% ± 40,12%	61,46% ± 40,11%
Retropropagação com taxa adaptativa	Verdadeiro Negativo	98,43% ± 1,27%	98,43% ± 1,57%
	Falso Positivo	16,03% ± 6,68%	12,06% ± 5,47%
	Falso Negativo	1,57% ± 1,27%	1,57% ± 1,57%
	Verdadeiro Positivo	83,97% ± 6,68%	87,94% ± 5,47%
Retropropagação com taxa adaptativa*	Verdadeiro Negativo	97,52% ± 4,93%	97,18% ± 5,18%
	Falso Positivo	15,88% ± 6,46%	12,14% ± 5,71%
	Falso Negativo	2,48% ± 4,93%	2,82% ± 5,18%
	Verdadeiro Positivo	84,12% ± 6,46%	87,86% ± 5,71%
Retropropagação com taxa adaptativa**	Verdadeiro Negativo	97,01% ± 2,98%	96,29% ± 3,45%
	Falso Positivo	12,37% ± 15,09%	9,83% ± 14,81%
	Falso Negativo	2,99% ± 2,98%	3,71% ± 3,45%
	Verdadeiro Positivo	87,63% ± 15,09%	90,17% ± 14,81%

Tabela 14. Parte 4: Matrizes de confusão das redes neurais apresentadas da Tabela 8 à Tabela 10.

Função de Aprendizado	Respostas Possíveis	Treino	teste
Retropropagação combinado	Verdadeiro Negativo	99,05% ± 2,84%	98,88% ± 3,06%
	Falso Positivo	8,82% ± 14,37%	6,35% ± 12,78%
	Falso Negativo	0,95% ± 2,84%	1,12% ± 3,06%
	Verdadeiro Positivo	91,18% ± 14,37%	93,65% ± 12,78%
Retropropagação combinado*	Verdadeiro Negativo	99,46% ± 2,33%	99,28% ± 3,21%
	Falso Positivo	5,15% ± 7,67%	3,28% ± 6,69%
	Falso Negativo	0,54% ± 2,33%	0,72% ± 3,21%
	Verdadeiro Positivo	94,85% ± 7,67%	96,72% ± 6,69%
Retropropagação combinado**	Verdadeiro Negativo	97,47% ± 6,99%	97,26% ± 7,16%
	Falso Positivo	5,39% ± 12,56%	5,24% ± 13,06%
	Falso Negativo	2,53% ± 6,99%	2,74% ± 7,16%
	Verdadeiro Positivo	94,61% ± 12,56%	94,76% ± 13,06%
Retropropagação secante em um passo	Verdadeiro Negativo	100,00% ± 0,00%	100,00% ± 0,00%
	Falso Positivo	0,17% ± 0,17%	0,02% ± 0,10%
	Falso Negativo	0,00% ± 0,00%	0,00% ± 0,00%
	Verdadeiro Positivo	99,83% ± 0,17%	99,98% ± 0,10%
Retropropagação secante em um passo*	Verdadeiro Negativo	100,00% ± 0,00%	100,00% ± 0,00%
	Falso Positivo	0,26% ± 0,30%	0,06% ± 0,18%
	Falso Negativo	0,00% ± 0,00%	0,00% ± 0,00%
	Verdadeiro Positivo	99,74% ± 0,30%	99,94% ± 0,18%
Retropropagação secante em um passo**	Verdadeiro Negativo	100,00% ± 0,00%	100,00% ± 0,00%
	Falso Positivo	0,20% ± 0,17%	0,04% ± 0,14%
	Falso Negativo	0,00% ± 0,00%	0,00% ± 0,00%
	Verdadeiro Positivo	99,80% ± 0,17%	99,96% ± 0,14%
Retropropagação resiliente (Rprop)	Verdadeiro Negativo	57,92% ± 48,98%	58,09% ± 48,85%
	Falso Positivo	47,53% ± 44,90%	47,20% ± 44,49%
	Falso Negativo	42,08% ± 48,98%	41,91% ± 48,85%
	Verdadeiro Positivo	52,47% ± 44,90%	52,80% ± 44,49%
Retropropagação resiliente (Rprop)*	Verdadeiro Negativo	55,91% ± 46,95%	56,12% ± 46,79%
	Falso Positivo	56,33% ± 41,65%	56,23% ± 41,23%
	Falso Negativo	44,09% ± 46,95%	43,88% ± 46,79%
	Verdadeiro Positivo	43,67% ± 41,65%	43,77% ± 41,23%
Retropropagação resiliente (Rprop)**	Verdadeiro Negativo	37,27% ± 45,61%	36,93% ± 45,69%
	Falso Positivo	39,56% ± 39,99%	40,04% ± 39,81%
	Falso Negativo	62,73% ± 45,61%	63,07% ± 45,69%
	Verdadeiro Positivo	60,44% ± 39,99%	59,96% ± 39,81%

Tabela 15. Parte 5: Matrizes de confusão das redes neurais apresentadas da Tabela 8 à Tabela 10.

Função de Aprendizado	Respostas Possíveis	Treino	teste
Retropropagação gradiente escalonado	Verdadeiro Negativo	100,00% ± 0,00%	100,00% ± 0,00%
	Falso Positivo	0,24% ± 0,14%	0,02% ± 0,10%
	Falso Negativo	0,00% ± 0,00%	0,00% ± 0,00%
	Verdadeiro Positivo	99,76% ± 0,14%	99,98% ± 0,10%
Retropropagação gradiente escalonado*	Verdadeiro Negativo	100,00% ± 0,02%	100,00% ± 0,00%
	Falso Positivo	0,17% ± 0,17%	0,04% ± 0,14%
	Falso Negativo	0,00% ± 0,02%	0,00% ± 0,00%
	Verdadeiro Positivo	99,83% ± 0,17%	99,96% ± 0,14%
Retropropagação gradiente escalonado**	Verdadeiro Negativo	100,00% ± 0,00%	100,00% ± 0,00%
	Falso Positivo	0,03% ± 0,09%	0,00% ± 0,00%
	Falso Negativo	0,00% ± 0,00%	0,00% ± 0,00%
	Verdadeiro Positivo	99,97% ± 0,09%	99,99% ± 0,00%

Capítulo 5
Conclusão

Sistematicamente, ao longo da década, a produção de *malwares* é crescente (Cert.br, 2016). Então, é importante que os antivírus provenham serviços confiáveis, em larga escala e em tempo real, com o objetivo de coletar amostras maliciosas recém-criadas visando proteger seus clientes. Conclui-se que a escolha de um antivírus adequado exerce papel significante na proteção contra invasões cibernéticas, visto que a detecção de *ransomwares* variou entre 0% a 97,63%, a depender do antivírus comercial investigado, conforme detalhado no capítulo 2. Foram investigados 86 antivírus comerciais. Em média, eles foram capazes de detectar 55,22% das pragas virtuais avaliadas. Com aspecto desfavorável, os antivírus, em média, atestaram falsos negativos e foram omissos em 13,15% e 31,71% dos casos, respectivamente.

Foi empregado o VirusTotal como plataforma para submissão automatizada dos *ransomwares* aos antivírus comerciais. No VirusTotal, não há a possibilidade de escolha da versão gratuita dos antivírus. Logo, como limitação do estudo proposto, não foi possível averiguar a diferença dos serviços providos pelas versões pagas e as gratuitas de um mesmo antivírus. A suposição é que as versões gratuitas disponibilizam serviços significativamente inferiores às versões pagas.

Cerca de 7% dos antivírus avaliados não foram capazes de diagnosticar qualquer uma das amostras maliciosas. Nota-se, a limitação dos antivírus comerciais quanto à robustez de serviços em larga escala mesmo em suas versões completas (pagas). Cabe salientar que os *ransomwares*, pertencentes à base criada (Ransomware, 2021), são de domínio público, largamente empregados em atividades maliciosas e com as suas atuações amplamente divulgadas em fóruns, blogs e outros conteúdos online. Mesmo assim, 7% dos antivírus comerciais avaliados não tinham qualquer conhecimento sobre as suas existências.

Desenvolveu-se um antivírus, dotado de inteligência artificial, visando a classificação quanto a executáveis de arquiteturas de 32 bits entre benignos e *ransomwares*. A extração de características passa pelo processo de *disassembling*

visando conhecer seu conteúdo a partir do código binários em mãos. A classificação é baseada em redes neurais baseadas em retropropagação. As condições iniciais e arquiteturas são alternadas com o objetivo de maximizar a precisão dos classificadores.

Quanto à classificação, a função de aprendizado dotada de retropropagação de Retropropagação Fletcher-Powell* apresenta a maior precisão dentre todos os classificadores averiguados, com uma precisão média de 99,99%. Essa abordagem possui uma arquitetura com duas camadas escondidas de 100 neurônios. O classificador de mais baixa precisão foi de 48,45%, referente à função de aprendizado Retropropagação resiliente (Rprop)**. Esse pior cenário ocorre quando o Rprop** é formado por uma arquitetura com uma camada escondida com 500 neurônios. Conclui-se que a melhor abordagem é quase 100,00% superior ao pior cenário obtido. Logo, a escolha de uma adequada função de aprendizado, composta por uma correta arquitetura, é essencial para maximizar a precisão quanto à identificação de *ransomwares*.

A contribuição deste trabalho, em relação ao estado-da-arte, é suprir as limitações e imprecisões dos modelos empíricos e heurísticos comumente empregados na detecção de pragas virtuais (Prado, Penteado, & Grégio, 2016). Então, ao invés das listas negras, o peso ponderado referente a um comportamento suspeito é determinado através de redes neurais artificiais. Constata-se que a inteligência artificial pode contribuir bastante para o avanço da segurança da informação em dispositivos digitais. Espera-se que o antivírus inteligente proposto atue de forma preventiva e impeça que os *ransomwares* burlem os mecanismos de defesa da vítima, como firewall e plugins de segurança.

Como limitação, o antivírus inteligente criado somente é capaz de detectar *ransomwares*, especificamente, para arquitetura de 32 bits do Sistema Operacional Windows. A explicação é que cada Sistema Operacional tem seu próprio repertório de instruções, bibliotecas e APIs. Então, por exemplo, os repertórios de instruções do Windows e do Linux são diferentes. Logo, a extração de características para aplicativos Windows, conforme detalhada na seção 1.2 do capítulo 3, não serve para Linux ou para Android. Conclui-se que o antivírus inteligente proposto não teria validade mediante *ransomwares* dos sistemas Linux e Android.

Então, a meta futura diz respeito a criação de novos antivírus, baseados em inteligência artificial, no sentido de suas aplicações a outros tipos de sistemas operacionais além do Windows. A intenção é estender a metodologia proposta a arquivos executáveis do sistema Android visto que smartphones e tablets móveis estão gradativamente se tornando indispensáveis na vida diária. O Android, por ser um sistema operacional relativamente recente, possibilita que incontáveis *malwares* se escondam em uma grande quantidade de aplicações legítimas, o que ameaça de forma grave a segurança do sistema e afeta diretamente o usuário e seus dados, cada vez mais atrelados aos *smartphones*.

Referências

BATTITI, R. (1992). First and second order methods for learning: Between steepest descent and Newton's method.

Cert.br. (2016). Incidentes Reportados ao CERT.br.

CONRAD, E., MISENAR, S., & and FELDMAN, J. (2017). Eleventh Hour CISSP (Certified Information Systems Security Professional).

HAGAN, M., H.B., D., & M.H., B. (1996). Neural Network Design.

LIMA, S., SILVA-FILHO, A. G., & SANTOS, W. P. (2016). Detection and classification of masses in mammographic images in a multi-kernel approach.

Moller, F. M. (1993). A scaled conjugate gradient algorithm for fast supervised learning.

NOTAY, Y. (2000). Flexible Conjugate Gradients. .

Powell, M. (1977). Restart procedures for the conjugate gradient method.

Prado, N., Penteado, U., & Grégio, A. (2016). Metodologia de Detecção de Malware por Heurísticas Comportamentais.

Ransomware. (2021). Retrieval for Ransomware Malware Analysis - Repositório para análise de malwares do tipo Ransomware.

REMnux. (2021). Kit de ferramentas para lidar com applicaçoes maliciosas. Disponível em https://remnux.org/.

Riedmiller, M., & Braun, H. (1993). A direct adaptive method for faster backpropagation learning: the RPROP algorithm.

SCALES, L. (1985). Introduction to Non-Linear Optimization. .

VirusShare. (2021). Repositório de amostras maliciosas. Disponível em: https://virusshare.com/.

VirusTotal. (2021). Serviço online de consulta aos antivírus comerciais. Disponível em: https://www.virustotal.com/.