

# Estudo e Análise de Técnicas de Inteligência Artificial para Detecção de Infecção por Ransomware

Fernando M. da S. Machado<sup>1</sup>, Ivan Carlos Alcântara de Oliveira<sup>1</sup>

<sup>1</sup>Universidade Presbiteriana Mackenzie- São Paulo, SP – Brasil

[Fernando.mauadiemachado@gmail.com](mailto:Fernando.mauadiemachado@gmail.com), [ivan.oliveira@mackenzie.br](mailto:ivan.oliveira@mackenzie.br)

**Abstract.** *The growing cases of Ransomware attacks reveal the need to detect an infection as soon as possible, so the damages can be mitigated. One option to solve this problem is to use AI. For this purpose, this TCC makes an analysis based on the Elderan database, to find out which machine learning methods generate the best result.*

**Resumo.** *Os casos crescentes de ataques de Ransomware revelam a necessidade de detectar uma infecção o mais rápido possível, para que os danos possam ser mitigados. Uma opção para resolver esse problema é usar IA. Para tal, este TCC faz uma análise a partir da base de dados do Elderan para descobrir quais os métodos de aprendizado de máquina geram o melhor resultado.*

## 1. Introdução

### 1.1. Contextualização e Relevância do Tema

Segundo a Online Trust Alliance, 2017 foi o pior ano em vazamentos de dados e incidentes cibernéticos ao redor do mundo. Em 2017 o número de ataques dobrou, sendo Ransomware o tipo de ataque mais comum (Larry Leob, 2018). O ataque mais notório destes se chama WannaCry, em que vários computadores ficaram com seus arquivos encarapitados e exigiam um pagamento de 300 dólares em bitcoin. Mais recentemente a empresa televisiva Record sofreu com este tipo de ataque levando ao sequestro de reportagens (Gabriel Dias, 2022). A preocupação com esse tipo de ataques levou a um aumento de estudos envolvendo cyber segurança e inteligência artificial. Para isso foram desenvolvidos vários métodos diferentes para a detecção de um Ransomwares antes que ele possa causar danos substanciais.

### 1.2. Objeto de Pesquisa

#### 1.2.1. Contextualização do Problema de Pesquisa

O ataque do tipo Ransomware tem como objetivo privar o usuário de acessar os seus arquivos, e assim exigir um resgate. Portanto a detecção desse tipo de infecção tem que ser a mais rápida possível para que se possa minimizar os danos.

#### 1.2.2. Definição e delimitação do problema da pesquisa

Diante dos crescentes casos de Ransomware, se torna cada vez mais necessário o desenvolvimento de novas maneiras de detectar quando a infecção ocorre em um sistema para que não ocorram danos ou que no mínimo eles sejam mitigados. Uma das maneiras propostas é a utilização de inteligência artificial.

### 1.3. Objetivos do Estudo

### **1.3.1. Objetivo Geral**

O presente trabalho tem por objetivo geral: Realizar o estudo e a análise de técnicas de Inteligência Artificial para detectar a infecção por Ransomware, identificando aquela mais assertiva, pelo uso de uma base de dados pública.

### **1.3.2. Objetivos Específicos**

Para atingir os objetivos gerais tem-se os seguintes objetivos específicos: 1- Seleção dos métodos de aprendizado de máquina que serão utilizados. 2- Seleção e normalização dos dados da base de dados. 3- Redução da dimensionalidade. 4- Aplicação dos métodos de aprendizado de máquina. 5- Comparação dos resultados gerados por diferentes métodos de aprendizado de máquina.

### **1.4. Justificativa**

Com os crescentes ataques do tipo Ransomware, torna-se cada vez mais necessário a defesa contra esses tipos de ataque, portanto saber qual modelo gera a melhor previsão ajudará em pesquisas futuras sobre o assunto.

### **1.5. Organização do Estudo**

Este projeto de Trabalho de Conclusão de Curso (TCC) está organizado conforme os capítulos descritos a seguir: Além deste capítulo 1, de Introdução, têm-se ainda os capítulos descritos na sequência. No Capítulo 2, encontra-se a fundamentação teórica onde está estabelecida a base teórica e o “estado da arte” em que se encontra o tema deste TCC. No Capítulo 3, encontra-se a metodologia da pesquisa, neste capítulo está descrita a natureza, abordagem, fins e meios que a pesquisa seguiu. No capítulo 4, encontram-se os resultados onde estão detalhados os resultados obtidos. No Capítulo 5, encontra-se a conclusão da pesquisa, neste capítulo está demonstrada a conclusão do estudo.

## **2. Referencial teórico**

### **2.1. Ransomware**

O primeiro Ransomware surgiu em 1989 por Joseph Popp e ficou popularmente conhecido como "AIDS Trojan", Ele foi distribuído através de disquetes como um disquete educacional sobre AIDS. Entretanto as pessoas foram surpreendidas com uma mensagem de que o usuário deve pagar 189 dólares para a empresa PC Cyborg Corporation no Panamá. Os arquivos do computador presentes no drive C: forma criptografados, porém como a criptografia usava chave simétrica (a chave de criptografia era também a chave de decriptografia) e a chave de criptografia tinha que vir junto com o Ransomware foi possível analisar a chave e remover a criptografia. (O'Kane et. al., 2018). Os ataques mais atuais de Ransomware não são mais distribuídos por disquetes, mas sim pela internet. (O'Kane et. al., 2018). Assim como a forma de distribuição evoluiu também evoluíram as técnicas de extorsão. Em 2006 foi empregado técnicas de criptografia assimétrica (Uma chave de criptografia pública e uma chave de criptografia privada) o que significa que a chave de criptografia é diferente da chave de decriptografia o que permite a instalação do Ransomware em máquinas sem que a chave de criptografia entregue as informações de criptografia. Esse ataque teve o nome de Archiveus e tinha como alvo os arquivos arquivados na pasta “meus documentos” e demandava que comprasse um item específico de um site para obter a chave de decriptografia. (O'Kane et. al., 2018). Em 2013 surgiram os Scareware que são Ransoms que usam de alguma forma de assustar o usuário para que ele se sinta coagido a pagar o resgate do computador

que teve o acesso do usuário bloqueado, podem por exemplo fingir serem autoridades. O primeiro deles foi Reveton que bloqueava o computador, prevenia o acesso (técnica conhecida como locker) e alegava que o usuário tinha quebrado a lei e que precisava pagar uma multa para acessar o computador, esse pagamento era feito através de vouchers anônimos. (O'Kane et. al., 2018). Em 2013 surgiu também o CryptoLocker. A criptografia usada foi AES-256 para criptografar os arquivos e se distribuiu por arquivos em e-mail, sites comprometidos. (O'Kane et. al., 2018). 2014 foi importante pois nesse ano surgiu o pagamento via TOR-base Bitcoin. (O'Kane et. al., 2018). Em 2015 surgiu TeslaCrypt que encriptava os arquivos com AES-256 e a chave AES-256 era criptografada com RSA-4096. (O'Kane et. al., 2018). Em suma, os Ransomwares estão sempre evoluindo e cada vez mais perigosos.

## **2.2. Inteligência artificial e segurança de informação**

Segundo Ben Coppin, em inteligência artificial (2010), é possível criar sistemas especialistas que imitam o comportamento de um especialista. Para atingir esse objetivo, é utilizado uma base de dados e uma base de fatos para que se possa tomar as decisões.

No livro *Inteligência Artificial* 3. ed. de Stuart Russell e Peter Norvig (2013, p. 872) é afirmado que:

“[...]os algoritmos também funcionam em níveis humanos em tarefas que aparentemente envolvem julgamento humano ou, como Turing observou, “aprender a partir da experiência” e a capacidade de “distinguir o certo do errado”. Desde 1955, Paul Meehl (veja também Grove e Meehl, 1996) estudou os processos de tomada de decisão de especialistas treinados em tarefas subjetivas como prever o sucesso de um aluno em um programa de treinamento ou a reincidência de um criminoso. Em 19 dos 20 estudos que examinou, Meehl descobriu que algoritmos simples de aprendizado estatístico (como regressão linear ou Bayes ingênuo) fizeram previsões melhores que os especialistas.”

Estas constatações comprovam que uma IA pode agir tão bem quanto ou até melhor do que um especialista.

No livro *Cryptography and Network Security Principles and Practice* 7th ed. global edition, William Stallings (2018, p.38) estabelece que há duas superfícies ataques. A primeira é a superfície de ataque de software em que é explorada uma vulnerabilidade do código do software. Superfície de ataque humano em que nele são usadas técnicas de engenharia social, erros humanos, e internos confiáveis.

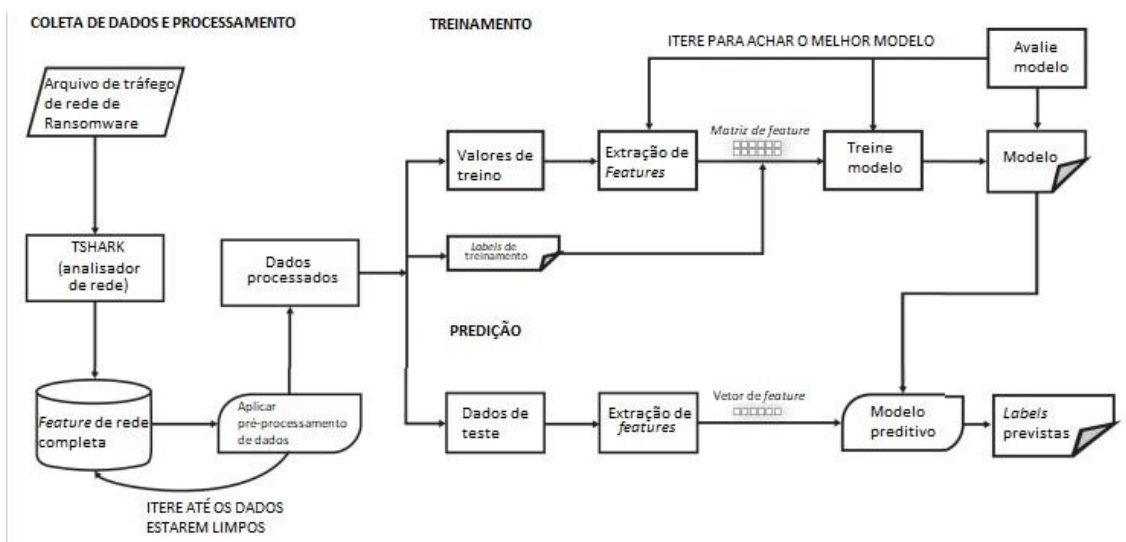
Pensando nesses dois problemas, surgiram modelos de IA que protegem os sistemas, e para isso essas inteligências artificiais são implementadas como sistemas especialistas. Isto pode ser comprovado na pesquisa *Artificial intelligence in cyber security: research advances, challenges, and opportunities* (ZHANG et al., 2022) em que nela são detalhados 4 métodos em que uma inteligência artificial pode ser usada para ajudar na proteção de rede. O primeiro deles é a autenticação de usuário em que a IA detecta comportamentos diferentes do usuário na hora da autenticação do usuário. O segundo desses métodos é a conscientização da situação de rede, em que a IA analisa a segurança da rede para detectar falhas. O terceiro método é o monitoramento de comportamento perigoso, no qual a IA detecta requisições estranhas dentro da rede. Por fim há a identificação de tráfego anormal, a inteligência artificial identifica locais em que o tráfego é anormal. Entretanto há limitações em que a inteligência artificial consegue trabalhar. Essas limitações podem ser causadas por: interferência de dados confusos, modelos maliciosamente modificados, falta de transparência no processo de decisão da IA e alto requerimento de dados. Deve então se considerar o humano no loop em que o

papel da IA é auxiliar o ser humano na tomada de decisões. A decisão final sobre algo é dada pelo ser humano se o nível de confiança da IA sobre algo for baixo. Isso resolve o fato de que a inteligência artificial necessita de grande quantidade de dados para funcionar. Uma maneira de implementar esses métodos é uma inteligência artificial que utiliza deep learning, pois como demonstra a pesquisa Cyber security meets artificial intelligence: a survey (LI, 2018), um dos usos do deep learning é a Análise de texto e processamento de linguagem natural. Esse sistema ajuda a prevenir uma 0-day vulnerability uma vez que, segundo a pesquisa k-Zero Day Safety: Measuring the Security Risk of Networks against Unknown Attacks (WANG et al., 2010) toda 0-day vulnerability, tem as seguintes características:

- “1. Não pode ser explorada a menos que
  - (a) existe uma conexão de rede entre a fonte e os hosts de destino,
  - (b) existe um serviço remoto com a vulnerabilidade no host de destino,
  - (c) e o invasor já tem privilégio no host de origem.
2. Sua exploração pode potencialmente render qualquer privilégio no host de destino

As suposições descrevem essencialmente um cenário de pior caso sobre as pré e pós-condições, respectivamente, de explorar uma vulnerabilidade de dia zero” (tradução nossa)

Portanto, sistemas que detectam comportamentos suspeitos ajudam em parte a prevenir uma 0-day vulnerability, uma vez que eles atuam no monitoramento da rede. Esse tipo de análise é possível também ser feita para Ransomwares em que é possível detectar a família do Ransomwares (Almousa et al., 2021a).



**Figura 1. Fluxo de trabalho experimental (Almousa et al., 2021a) (tradução nossa)**

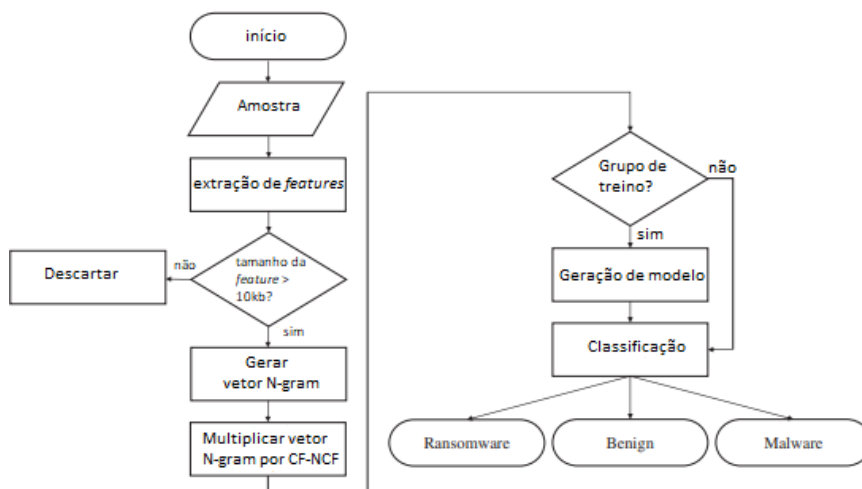
Porém os Ransomwares mais modernos trabalham para driblar as detecções como é o caso do Black Basta (inforchannel, 2022) por isso é necessário entender como um Ransomware age para que se possa fazer a detecção dele independente da família. A detecção estatística funciona bem para as famílias conhecidas de Ransomware, mas não para famílias desconhecidas, além do fato de que estão surgindo maneiras novas de burlar a detecção de Ransomwares conhecidos, os melhores resultados surgiram com o aprendizado de máquina e análises dinâmicas. (Nieuwenhuizen, 2017). É possível

também fazer análises em multiníveis incluído assambly (Poudyal; Dasgupta, 2020) o que ajuda na detecção de Ransomwares que utilizam outros softwares para se instalar, um exemplo disso é que hackers estão usando o anti-cheat do jogo genshi impact para instalar Ransomwares nos computadores, pois o anti-cheat roda no nível do kernel. (Soliven; Kimura, 2022). Outros estudos também indicam que machine learning e deep learning são os melhores para a detecção de Ransomware. (Fernando et al., 2020).

Nesse sentido podem se empregar diversas técnicas de detecção utilizando aprendizado de máquina, entre as técnicas estão, SVM, Naive Bayes, regressão logística (Sgandurra et al., 2016), KNN, SGD. (Bae et al., 2019). Outra maneira de detectar um Ransomware é através de uma rede neural convolucional. (Alvee et al., 2021). Para fazer as análises e conseguir determinar as variáveis mais relevantes é necessário ter uma base de dados, a base de dados mais recente e atualizada é a Ransap. (Hirano et al. 2021). Outra base pública é o EldeRan e segundo a pesquisa que originou essa base um dos dados mais relevantes são as chamadas de API (Sgandurra et al., 2016). Porém como as bases de dados tem muitos dados é necessário fazer uma redução das variáveis, é possível através de modelos matemáticos fazer uma redução das variáveis sem que haja perda dos dados. (Almoussa et al., 2021b). Nas pesquisas Malware Detection and Prevention using Artificial Intelligence Techniques (Faruk et.al, 2021), API-Based Ransomware Detection Using Machine Learning-Based Threat Detection Models (Almoussa et al., 2021b), foram utilizadas o PCA. Há também outros modelos que podem ser empregados para fazer a redução de dimensionalidade. Segundo as pesquisas Variable selection using random forests (Genuer et al. 2010), A new variable selection approach using Random Forests (Hapfelmeier; Ulm, 2012), Variable Selection Using Random Forests (Sandri; Zuccolotto, 2006) é possível utilizar o Random Forest como seletor de features.

### 2.3. Trabalhos similares

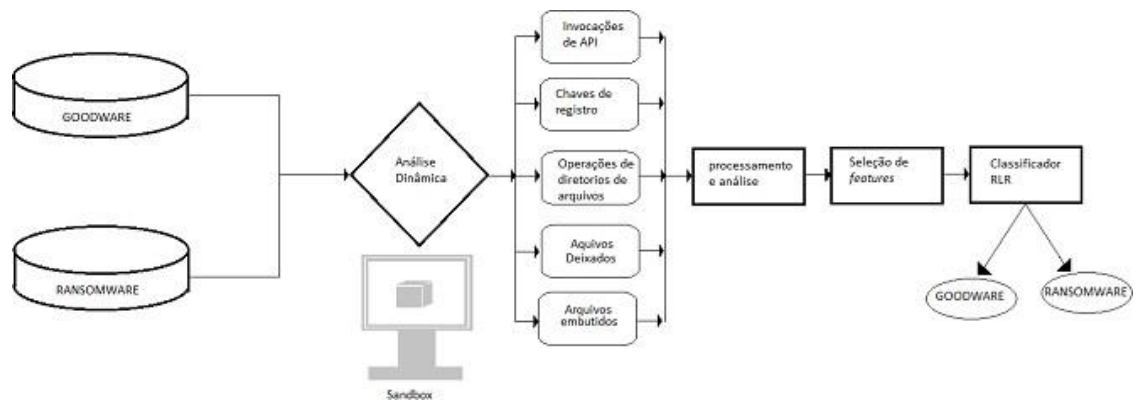
Foram propostos alguns modelos de detecção, entre eles estão: F-NCF, ilustrado na Figura 2; e EldeRan, apresentado na Figura 3.



**Figura 2. Fluxograma proposto (Bae et al. 2019) (tradução nossa)**

O modelo proposto na Figura 2 funciona da seguinte forma: primeiro é feita a extração de features de um arquivo executável, através do módulo de extração. Para fazer isso é necessário extrair as APIs nativas do Windows. Então é feita a extração dos elementos n-gram através das sequências de invocação de APIs nativas do Windows. O vetor de elementos n-gram gerados é multiplicado pelo valor CF-NCF, o valor CF-NCF age como peso que é utilizado para indicar a qual classe pertence o problema que pode

ser classificado entre Benign, Ransomware, Malware. O valor CF-NCF é usado como peso para indicar qual classe pertence ao problema, classificando-o em três classes.



**Figura 3. Elderan Treinamento e Análises em Sandbox (Sgandurra et al. 2016) (tradução nossa)**

Conforme Figura 3, EldeRan funciona da seguinte forma. Primeiro foi treinado em um ambiente Sandbox com Goodware e Ransomware onde foram feitas as capturas das informações que eram solicitadas no programa depois foi feita uma seleção de variáveis através de Mutual Information criterion após isso foi feita através de aprendizado de máquina a classificação.

### 3. Metodologia da Pesquisa

Em relação a metodologia que foi empregada neste TCC, o trabalho teve seu começo com uma revisão da base teórica sobre o tema da pesquisa. O foco dessa revisão é determinar onde se encontra o “estado da arte” em relação à pesquisa que foi desenvolvida. As bases teóricas foram obtidas através de artigos como: Artificial intelligence in cyber security: research advances, challenges, and opportunities, Cyber security meets artificial intelligence: a survey, Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection, bem como livros conceituados como: Inteligência artificial de Stuart Russell e Peter Norvig, entre outros. A lógica de raciocínio que fundamenta este estudo é a dedução, partindo do seguinte pensamento: As inteligências artificiais podem agir como tão bem quanto ou até melhor do que especialistas. Isto permite que a inteligência artificial através de métodos de aprendizado de máquina possa determinar quando um software se trata de um Goodware ou um Ransomware. Portanto, a hipótese que foi testada neste TCC é: O método de aprendizado de máquina que apresenta melhor resultado é a regressão logística. Para que seja possível validar a hipótese é necessária uma base de dados. Apesar da maior base de dados ser a Ransap ela acaba se tornando muito grande para esse projeto, portanto a base a ser utilizada será a base do EldeRan.

Pelo fato de a base selecionada ter 30970 variáveis e 1524 linhas é necessário fazer a redução de dimensionalidade. Para essa pesquisa foram escolhidas duas maneiras de fazer a redução. A primeira maneira é através do PCA. A segunda utilizando o Random Forest para escolher quais variáveis são as mais relevantes. Essas técnicas foram escolhidas, pois foram as técnicas utilizadas em outras pesquisas conforme o referencial teórico.

Quanto às técnicas de aprendizado de máquina foram feitas comparações entre Regressão logística, KNN, SVM, Naive Bayes, Redes Neurais, SGD. Essas técnicas foram selecionadas, pelo fato de serem técnicas que foram utilizadas em outras pesquisas

conforme o referencial teórico.

Para analisar os resultados foi utilizado a precisão da predição, entretanto por se tratar de um caso crítico se faz necessário do uso da matriz de confusão, uma vez que é ineficiente ter um modelo preciso, mas que há uma quantidade excessiva de falsos negativos. Além disso é necessário levar em consideração o tempo de execução, já que devemos eliminar o mais rápido possível a ameaça. Portanto a melhor técnica de aprendizado de máquina foi decidida pela técnica que melhor preencheu esses 3 fatores.

No que tange a classificação da pesquisa, ela é de natureza aplicada. Quanto à abordagem do problema, ela é uma pesquisa de abordagem qualitativa. Em relação aos fins, essa pesquisa tem um fim exploratório. Quanto aos meios, a pesquisa é uma pesquisa bibliográfica e um estudo de caso.

Sobre o cronograma, nos 3 primeiros meses foram feitos levantamentos de dados da pesquisa, onde foram levantados dados sobre Ransomware e IA bem como quais técnicas serão utilizadas. No mês seguinte foi selecionada a base de dados a ser utilizada. No 5º e no 6º mês foram feitas as conclusões parciais e a produção do banner. Nos 4 meses seguintes foram feitas as manipulações e explorações das bases de dados e os testes de predição utilizando diversas técnicas de aprendizado de máquina. Os últimos dois meses foram reservados para a produção do documento final.

## **4. Resultados**

### **4.1. Preparação dos dados**

A base de dados selecionada foi EldeRan. Ela contém 10 famílias de Ransomware, 30970 variáveis, 1524 linhas, além disso em relação ao Ransomware há dois tipos de classificação. A primeira é entre Ransomware e não Ransomware (Goodware). A segunda é a classificação de qual família de Ransomware ela pertence (no caso de não Ransomware é classificado como 0). Os dados foram obtidos através do monitoramento dos Ransomwares em ambientes Sandbox, porém devido a grande quantidade de variáveis é necessário fazer a redução da dimensionalidade, para isso foram feitos dois testes após a preparação dos dados. O primeiro teste utiliza PCA como redutor e o segundo utiliza Random Forest como redutor.

Primeiramente foi feita uma análise da base de dados e percebeu-se que a mesma não continha cabeçalho, portanto como é sabido que a base tem 30970 colunas foi feito um programa em Python para gerar um csv contendo apenas os números de 1 até 30970, em seguida foi acrescentado manualmente ao arquivo csv da base. Após este procedimento, a base de dados foi carregada em um dataframe no Pandas com o objetivo de preservar os dados originais foi feita uma cópia deste para um segundo dataframe (que será referenciado como df2). Foi percebido que as colunas 1 e 3 não poderiam estar na base de treinamento, pois conforme os documentos da base do EldeRan a coluna 1 representa o ID e a coluna 3 representa a família do Ransomware. Posteriormente foi verificado se havia dados nulos, porém nenhum foi encontrado. Para fazer a análise do PCA foi feita uma cópia do df2 para uma variável chamada de df3 a partir deste novo dataframe foram criadas duas variáveis X e y em que y recebe apenas a coluna 2 do dataframe e X recebe o dataframe inteiro menos a coluna 2, isso acontece porque a coluna 2 conforme a documentação do EldeRan representa a classificação entre Goodware e Ransomware, essa classificação é o nosso objetivo do modelo preditivo, em seguida foi aplicado o PCA para fazer a redução de dimensionalidade. Foi feito um procedimento similar para o Random Forest, a diferença é apenas que após aplicar o Random Forest é

feito um novo dataframe somente com as variáveis selecionadas pelo Random Forest, a partir deste novo dataframe foram feitas as análises de aprendizado de máquina para este caso.

## 4.2. Analisando os resultados

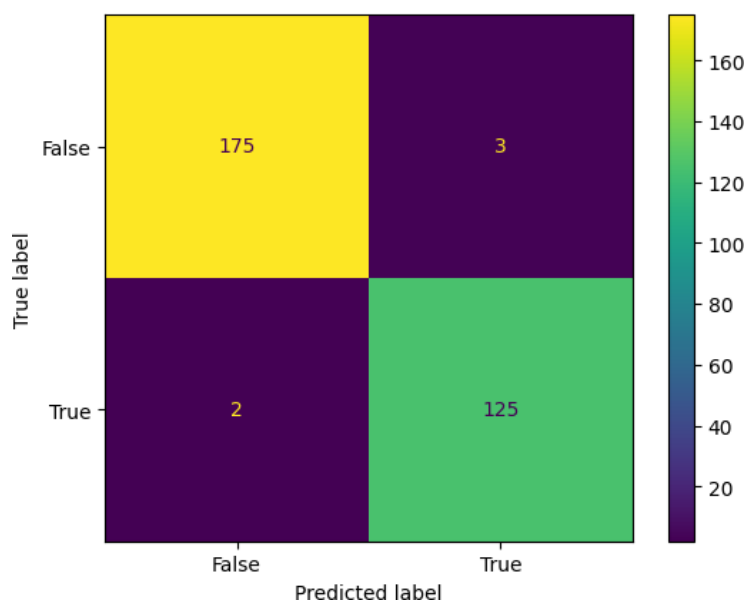
Para aplicar os métodos de aprendizagem de máquina foi usado o sklearn. O critério utilizado para comparar os métodos de aprendizado de máquina, foi a precisão da predição, os resultados das matrizes de confusão para verificar a quantidade de falsos negativos.

### 4.2.1. PCA

Os resultados obtidos através do PCA podem ser visualizados na tabela 1. O melhor resultado obtido foi de 0.9836065573770492 utilizando o modelo de Regressão Logística e tem a matriz de confusão conforme a figura 4.

**Tabela 1. Modelos e suas precisões utilizando PCA como redutor de dimensionalidade. (Tabela nossa)**

Modelo	Precisão
Regressão Logística	0.9836065573770492
KNN	0.9180327868852459
Gaussian Naive Bayes	0.5442622950819672
SVM	0.940983606557377
SGD	0.980327868852459
Redes Neurais	0.980327868852459



**Figura 4. Matriz de confusão da regressão logística utilizado o PCA para reduzir a dimensionalidade. (Figura nossa)**

Como pode ser observado na matriz, foram obtidos 2 casos de falso negativo, 3 casos de falso positivo e 300 casos de classificação correta.

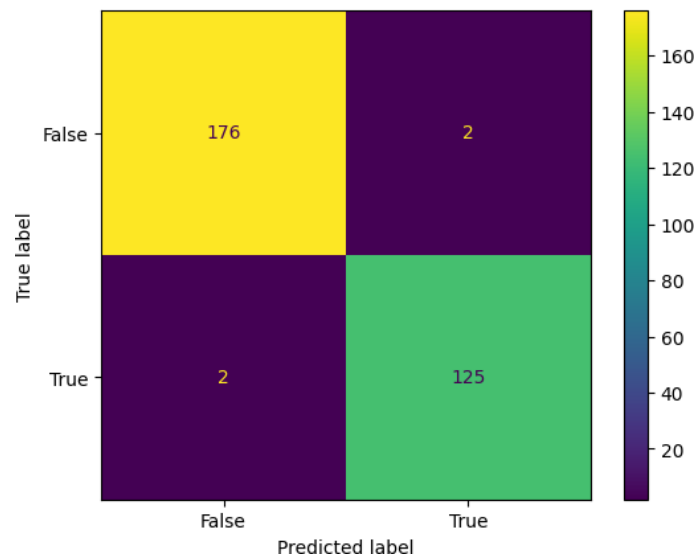


#### 4.2.2. Random Forest

Os resultados obtidos através do Random Forest podem ser visualizados na tabela 2. O melhor resultado obtido foi de 0.9868852459016394 utilizando o modelo SGD com o hiperparâmetro `random_state = 0` e tem a matriz de confusão conforme a figura 5.

**Tabela 2. Modelos e suas precisões utilizando Random Forest como redutor de dimensionalidade. [Tabela nossa]**

Modelo	Precisão
Regressão Logística	0.9770491803278688
KNN	0.8622950819672132
Gaussian Naive Bayes	0.6786885245901639
SVM	0.9606557377049181
SGD	0.9868852459016394
Redes Neurais	0.9704918032786886



**Figura 5. Matriz de confusão do SGD utilizado o Random Forest para reduzir a dimensionalidade. (Figura nossa)**

Como pode ser observado na matriz, foram obtidos 2 casos de falso negativo, 2 casos de falso positivo e 301 casos de classificação correta.

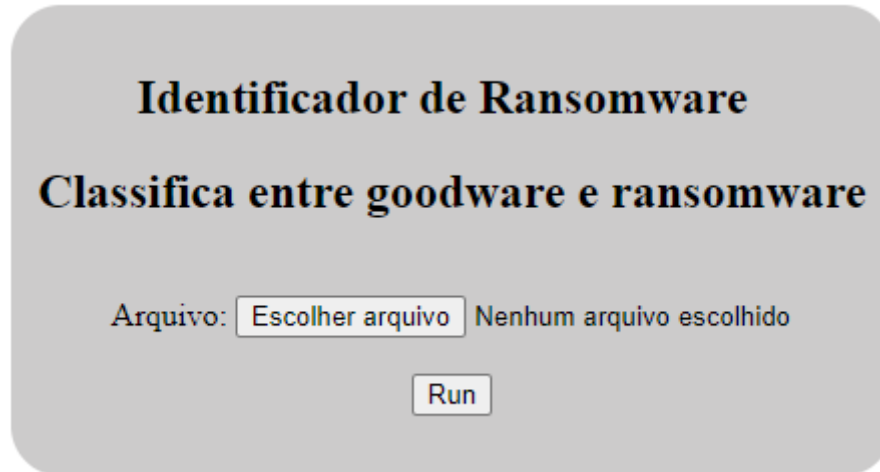
#### 4.3. Discussão dos experimentos.

Baseado nesses resultados, foi feito um `gridsearchcv` com o melhor método de aprendizagem de máquina de cada método de redução de dimensionalidade, com o objetivo de achar os melhores hiperparâmetros, para descobrir se é possível mais alguma otimização. Após verificar os melhores parâmetros foi constatado que não houve aumento da precisão em nenhum dos dois casos.

#### 4.4. Aplicação analítica.

Afim de determinar qual dos dois métodos tem uma aplicação prática mais veloz foi desenvolvido em Flask duas aplicações analíticas. A primeira aplicação utiliza Random Forest para fazer a redução da dimensionalidade e SGD como modelo preditivo. A

segunda aplicação utiliza PCA para fazer a redução da dimensionalidade e Regressão Logística como modelo preditivo. Para alcançar estes resultados foi retirada da base de dados 5 linhas aleatórias para servirem de entrada. Nos dois casos quando testados conseguiram fazer a classificação correta, mas a aplicação utilizando PCA e Regressão logística gerou o *output* dos resultados em uma velocidade consideravelmente mais rápidos.



**Identificador de Ransomware**

**Classifica entre goodware e ransomware**

Arquivo:  Nenhum arquivo escolhido

Figura 6. Tela inicial da aplicação em Flask (Figura nossa)



**Identificador de Ransomware**

**Classifica entre goodware e ransomware**

Arquivo:  linha2.csv

Figura 7. Tela com arquivo carregado (Figura nossa)



**Figura 8. Tela com o resultado de Ransomware (Figura nossa)**



**Figura 9. Tela com o resultado de Goodware (Figura nossa)**

As figuras foram extraídas da versão que utiliza PCA e regressão logística, porém o funcionamento é idêntico no modelo com Random Forest e SGD.

#### **4.5. Sobre este trabalho**

Este trabalho foi desenvolvido em um período de um ano na Universidade Presbiteriana Mackenzie. A documentação e o código fonte construído com o Jupyter notebook e o Flask pode ser encontrado no GitHub, endereço: <https://github.com/FernandoMauadieMachado/TCC-Fernando-Machado>.

Destaca-se que esta pesquisa foi selecionada para ser apresentado de forma parcial durante a semana do Workshop de Tendencias Tecnológicas (WTT) no Mackenzie realizada no primeiro semestre de 2023, mais especificamente no mês de abril.

#### **5. Conclusão e trabalhos futuros**

Dado às observações feitas nos resultados este estudo comprova a sua hipótese de que a regressão logística apresenta os melhores resultados, pois apesar de correr o risco de gerar

mais falsos positivos que o SGD essa diferença é irrisória e levando em consideração que a velocidade da obtenção da classificação da regressão logística utilizando o PCA como redutor de dimensionalidade é notoriamente mais veloz ela se torna superior uma vez que para esse tipo de problema é necessário que a classificação seja a mais rápida possível. Trabalhos futuros podem explorar mais formas de desenvolver uma aplicação analítica em que a própria aplicação atua para remover o vírus, proteger os arquivos, entre outras medidas de segurança, podem também explorar outras técnicas de redução de dimensionalidade, outras formas de aprendizado de máquina. Além disso pode-se pensar em pontos de otimização do código.

## Referências

- ALMOUSA, May; BASAVARAJU, Sai; ANWAR, Mohd. API-Based Ransomware Detection Using Machine Learning-Based Threat Detection Models. In: 2021 18th International Conference on Privacy, Security and Trust (PST). IEEE, 2021. p. 1-7.
- ALMOUSA, May; OSAWERE, Janet; ANWAR, Mohd. Identification of Ransomware families by Analyzing Network Traffic Using Machine Learning Techniques. In: 2021 Third International Conference on Transdisciplinary AI (TransAI). IEEE, 2021. p. 19-24.
- ALVEE, Syed RB et al. Ransomware Attack Modeling and Artificial Intelligence-Based Ransomware Detection for Digital Substations. In: 2021 6th IEEE Workshop on the Electronic Grid (eGRID). IEEE, 2021. p. 01-05.
- BAE, Seong Il; LEE, Gyu Bin; IM, Eul Gyu. Ransomware detection using machine learning algorithms. *Concurrency and Computation: Practice and Experience*, v. 32, n. 18, p. e5422, 2020.
- COPPIN, Ben. *Inteligência Artificial*. Rio de Janeiro: Grupo GEN, 2010.
- Dias, Gabriel. Record hackeada: entenda gravidade e como proteger os dados da sua empresa. TiltOUL. 17 de out. de 2022. Disponível em: <<https://www.uol.com.br/tilt/noticias/redacao/2022/10/17/ataque-hacker-record-roubo-de-dados-pode-ter-sido-um-dos-maiores-do-mundo.htm>>. Acessado em: 28 de nov. de 2022.
- FARUK, Md Jobair Hossain et al. Malware detection and prevention using artificial intelligence techniques. In: 2021 IEEE International Conference on Big Data (Big Data). IEEE, 2021. p. 5369-5377.
- FERNANDO, Damien Warren; KOMNINOS, Nikos; CHEN, Thomas. A study on the evolution of ransomware detection using machine learning and deep learning techniques. *IoT*, v. 1, n. 2, p. 551-604, 2020.
- FERNANDOMAUADIEMACHADO/TCC-FERNANDO-MACHADO. [S. l.], 25 maio 2023. Disponível em: <<https://github.com/FernandoMauadieMachado/TCC-Fernando-Machado>>. Acesso em: 26 maio 2023.
- GENUER, Robin; POGGI, Jean-Michel; TULEAU-MALOT, Christine. Variable selection using random forests. *Pattern recognition letters*, v. 31, n. 14, p. 2225-2236, 2010.
- HAPFELMEIER, Alexander; ULM, Kurt. A new variable selection approach using random forests. *Computational Statistics & Data Analysis*, v. 60, p. 50-69, 2013.

- HIRANO, Manabu; HODOTA, Ryo; KOBAYASHI, Ryotaro. RanSAP: An open dataset of ransomware storage access patterns for training machine learning models. *Forensic Science International: Digital Investigation*, v. 40, p. 301314, 2022.
- Loeb, Larry. Cybersecurity Incidents Doubled in 2017, Study Finds. *SecurityIntelligence*. 30 de jan. de 2022. Disponível em: <<https://securityintelligence.com/news/cybersecurity-incidents-doubled-in-2017-study-finds/>>. Acessado em 28 de nov. de 2022.
- LI, Jian-hua. Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, v. 19, n. 12, p. 1462-1474, 2018.
- NIEUWENHUIZEN, Daniel. A behavioural-based approach to ransomware detection. *Whitepaper. MWR Labs Whitepaper*, 2017.
- Novo ransomware desabilita sistemas de segurança. *Inforchannel*. 4 de nov. de 2022. Disponível em: <<https://inforchannel.com.br/2022/11/04/novo-ransomware-desabilita-sistemas-de-seguranca/>>. Acessado em 28 de nov. de 2022.
- POUDYAL, Subash; DASGUPTA, Dipankar. AI-powered ransomware detection framework. In: *2020 IEEE Symposium Series on Computational Intelligence (SSCI)*. IEEE, 2020. p. 1154-1161.
- RUSSELL, Stuart; NORVIG, Peter. *Inteligência Artificial*. 3. ed. Rio de Janeiro: Grupo GEN, 2013.
- SANDRI, M.; ZUCCOLOTTO, P. Data analysis, classification and the forward search. In: *Proceedings of the meeting of the classification and data analysis group (CLADAG) of the Italian Statistical Society, University of Parma*. 2006. p. 263-270.
- SGANDURRA, Daniele et al. Automated dynamic analysis of ransomware: Benefits, limitations and use for detection. *arXiv preprint arXiv:1609.03020*, 2016.
- Scikit-learn: Machine Learning in Python, Pedregosa et al., *JMLR* 12, pp. 2825-2830, 2011.
- STALLINGS, William. *Cryptography and Network Security Principles and Practice*. 7th ed. Harlow: Pearson Education Limited 2017.
- WANG, Lingyu et al. k-zero day safety: Measuring the security risk of networks against unknown attacks. In: *European Symposium on Research in Computer Security*. Springer, Berlin, Heidelberg, 2010. p. 573-587.
- WORKSHOP DE TENDENCIAS TECNOLOGICAS, 15., 2023, São Paulo, SP. Universidade Presbiteriana Mackenzie, 2023.
- ZHANG, Zhimin et al. Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, v. 55, n. 2, p. 1029-1053, 2022.