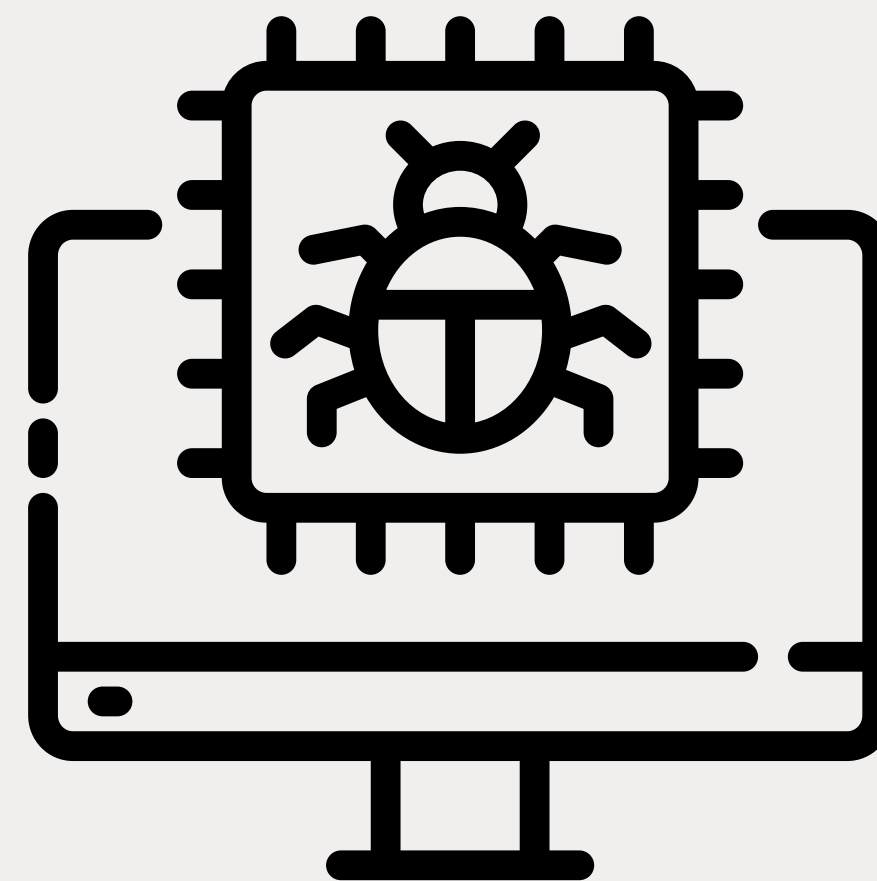




Ian Marques Breda

ML PARA DETECÇÃO DE RANSOMWARES



Tópicos

INTRODUÇÃO

Breve descrição do problema a ser resolvido e os objetivos desse trabalho

CONCEITOS IMPORTANTES

Conceitos de criptografia, floresta aleatória e pontos sobre o modelo

PROTÓTIPO

Apresentação do vírus criado

MODELO

Apresentação do modelo criado

RESULTADOS

Resultados do vírus, métricas de avaliação do modelo e arquivos gerados neste projeto.

Introdução



- Baixo risco e grande recompensa
- Grande aumento durante e pós pandemia
- Atingem todo tipo de usuário



- Segundo Darktrace: 53 grupos e +3.700 vítimas
- Segundo a FinCEN: Média mensal de 66M\$ (Jan-Jun, 2021)
- REvil ataca Kaseya e lucra 70M\$ em troca de ferramenta (Jul, 2021)



- WannaCry solto em 2017, 230k computadores, 150 países
- Compromete hospitais, Universidades, montadoras e linhas aéreas
- TJS, INSS, VIVO, NET e Ministério Público
- Prejuízo estimado de 4B\$

Objetivos

- Conhecer a área de segurança
- Estudar a floresta aleatória
- Estudar malwares e criptografia
- Explorar o uso da I.A. (promissor)
- Produzir material sobre o assunto



Conceitos Importantes

AES-128 bits:

- **Chave simétrica (única) para criptografar e reverter os dados**
- **AES gera no conteúdo um bloco e aplica transformações chamadas "rodadas". Durante essas rodadas, o conteúdo do bloco é embaralhado várias vezes, tornando-o irreconhecível**
- **A abordagem simétrica é muito rápida e eficiente para grandes volumes de dados**

Conceitos Importantes

RSA-2048 bits:

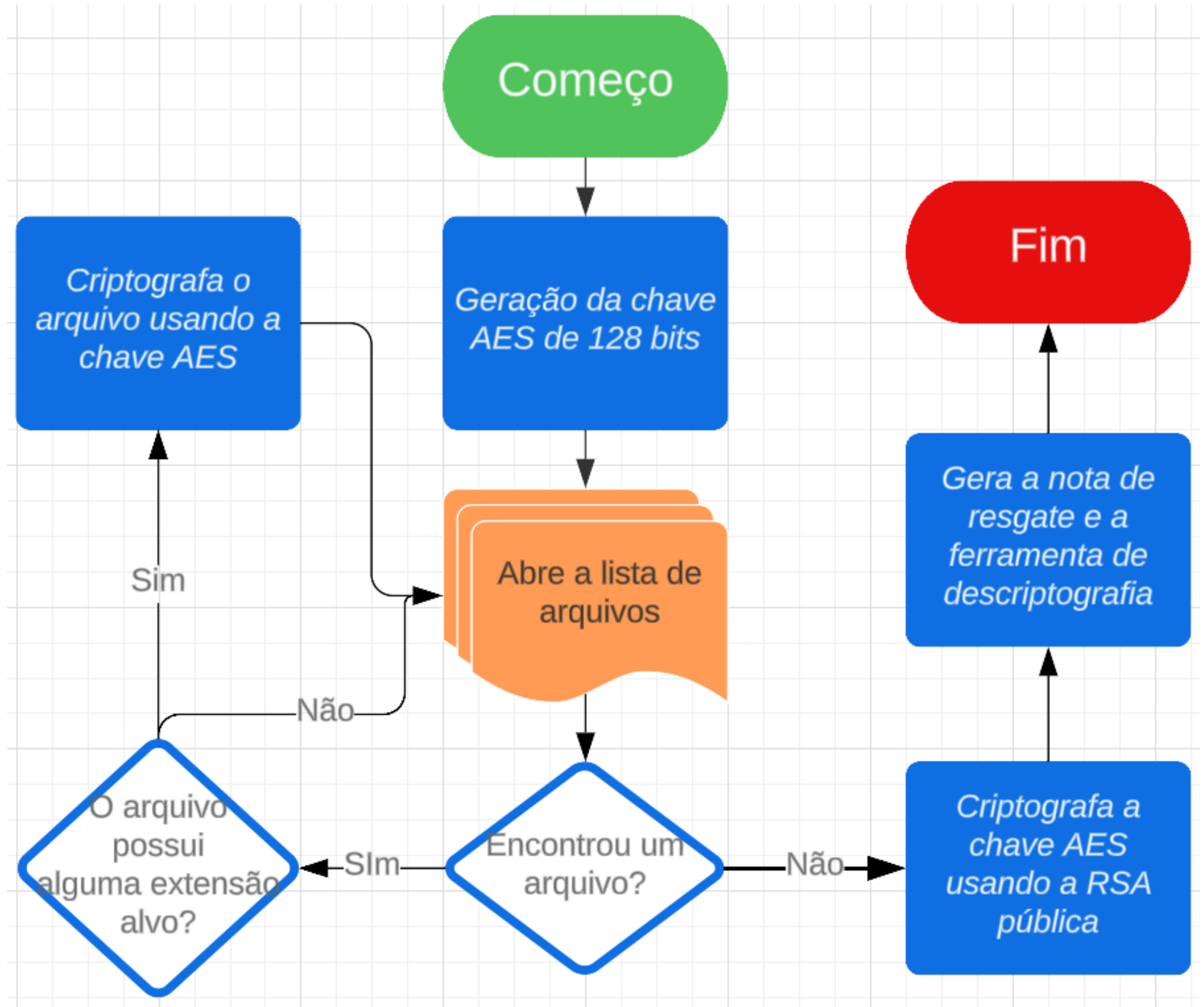
- **Chave assimétrica (pública e privada) para criptografar e reverter os dados**
- **O conteúdo deve ser menor que o tamanho da chave, senão o separa em vários blocos**
- **A abordagem assimétrica é lenta, pois pode precisar de várias operações de números primos e possíveis passos adicionais.**

Conceitos Importantes

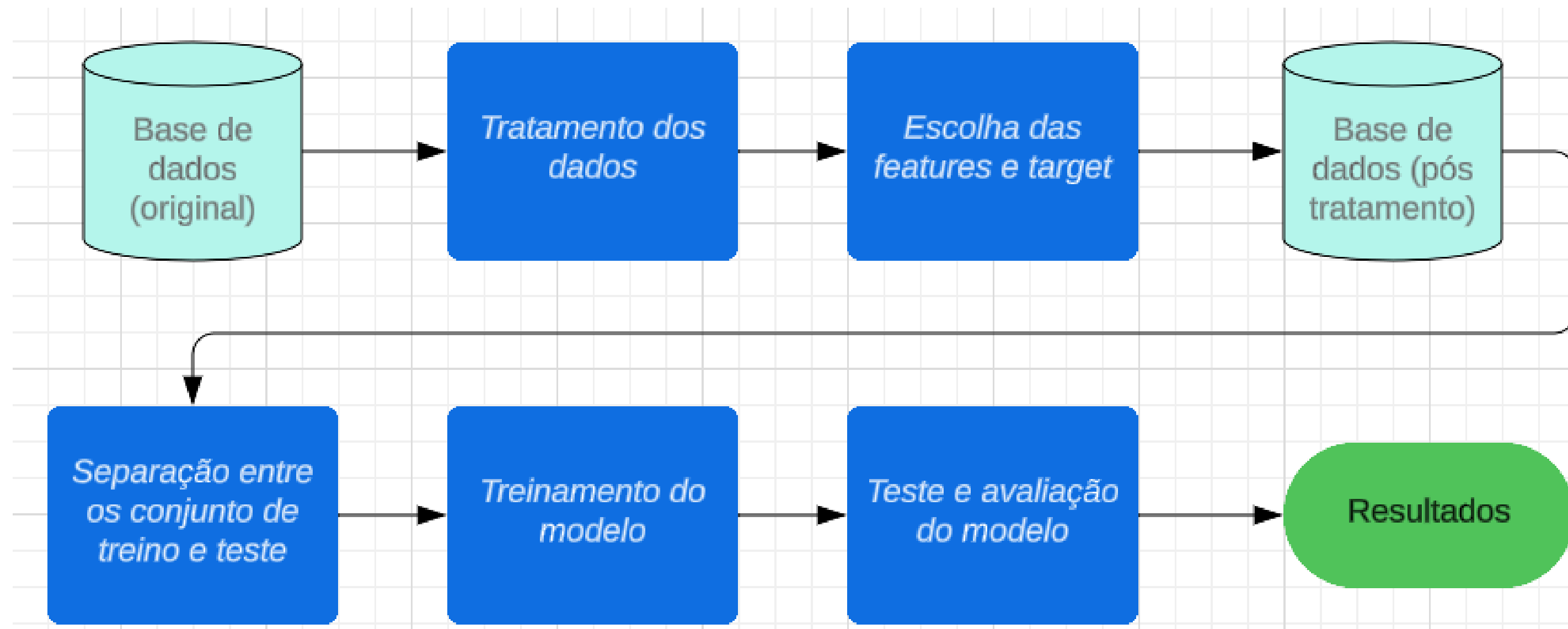
Modelo:

- **Floresta aleatória é um algoritmo de aprendizado de máquina que gera aleatoriamente várias árvores de decisão e vota pelo resultado**
- **Foram usadas as bibliotecas sklearn, pandas, pefile, matplotlib e shap**
- **Dataset foi retirado do kaggle**
- **XAI = Processos e métodos para explicar uma IA. Uma forma de explicar o output gerado por um modelo**

Protótipo



Modelo



Resultados do protótipo

Ian Marques Breda

✉ ian@email

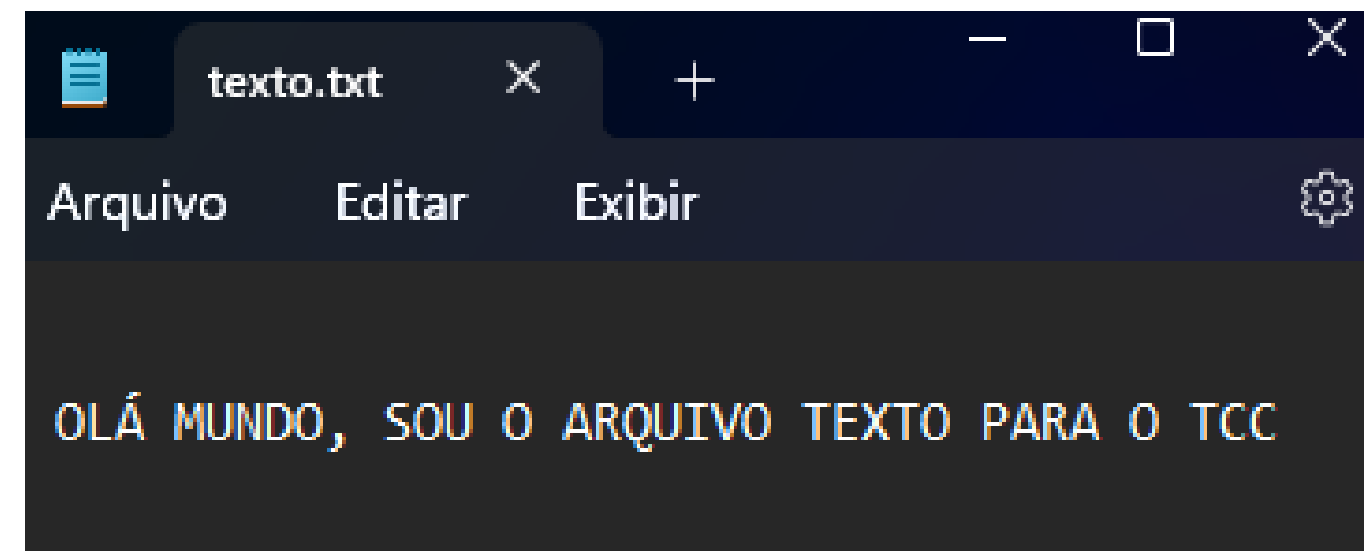
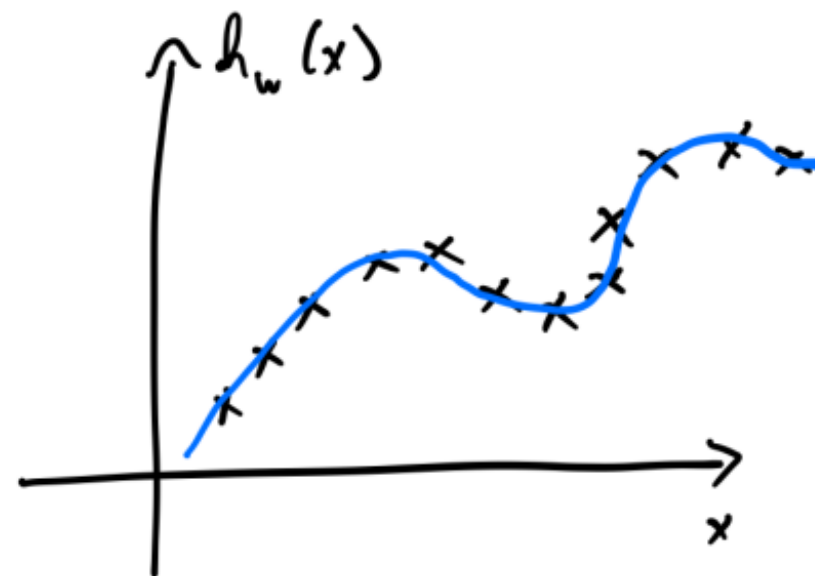
📞 +55 9 99 99999

🌐 www.linkedin.com/in/ianmbreda |

🔗 <https://github.com/ianBreda>

HABILIDADES

- Python | Data Science | SQL | Power BI | Machine Learning | C



Resultados do protótipo

Não é possível abrir este arquivo

Algo deu errado.

Atualizar



Captura de tela 2024-08-23 144514.png
Não há suporte para este formato de arquivo.



texto.txt



Arquivo

Editar

Exibir



```
78!b\5Y,8nfy&SOA01  
;: f00
```

Ln 1, Col 43

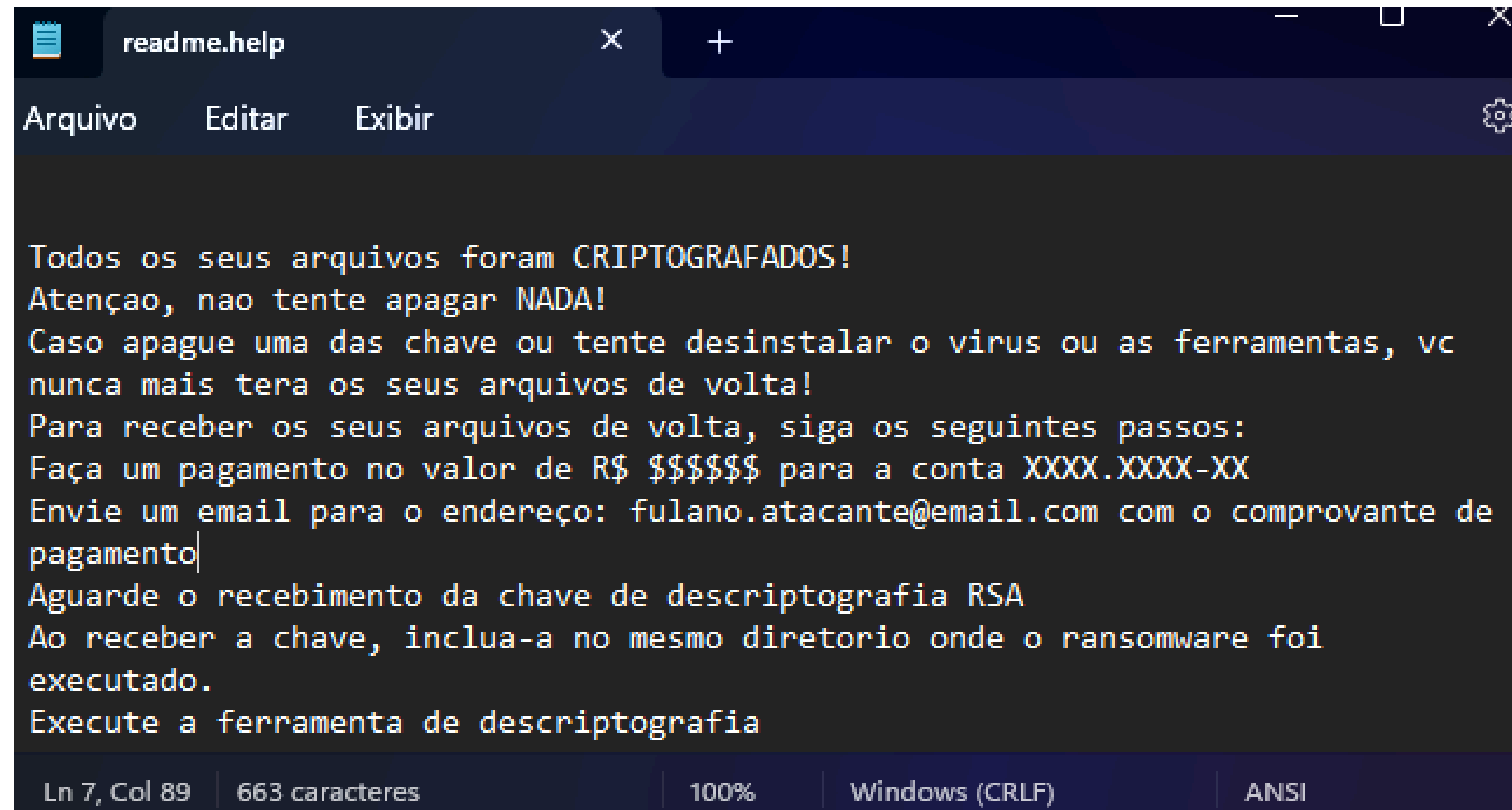
57 caracteres

100%

Windows (C

UTF-8

Resultados do protótipo



The image shows a screenshot of a ransomware message displayed in a text editor window. The window has a dark theme and a menu bar with 'Arquivo', 'Editar', and 'Exibir'. The message is written in a monospaced font and contains instructions for the victim to pay a ransom to retrieve their encrypted files. The status bar at the bottom shows 'Ln 7, Col 89', '663 caracteres', '100%', 'Windows (CRLF)', and 'ANSI'.

```
readme.help
Arquivo  Editar  Exibir

Todos os seus arquivos foram CRIPTOGRAFADOS!
Atencao, nao tente apagar NADA!
Caso apague uma das chave ou tente desinstalar o virus ou as ferramentas, vc
nunca mais tera os seus arquivos de volta!
Para receber os seus arquivos de volta, siga os seguintes passos:
Faça um pagamento no valor de R$ $$$$$$ para a conta XXXX.XXXX-XX
Envie um email para o endereço: fulano.atacante@email.com com o comprovante de
pagamento
Aguarde o recebimento da chave de descriptografia RSA
Ao receber a chave, inclua-a no mesmo diretorio onde o ransomware foi
executado.
Execute a ferramenta de descriptografia

Ln 7, Col 89 | 663 caracteres | 100% | Windows (CRLF) | ANSI
```

Resultados do protótipo

```
dados_chave_publica = b'''-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAYTQDpyp5mT46Lv4CfIqt
C9DI t7hWblvLNsNAr5Ad7keqKcivhIRSq0bgkfFvTZy7n9fhAQLqezlGmFIXtw4U
GrI0xvUvZN0nJdB09xmAjW6n37cHGd1hIqKOK971p3cHga/V9WWP0LkPXBxy1ryU
ywcg6Eve7zSFTXsjFRFxaaIE9cvumfZ1sHm8+u/Gy0Mz78SsjNnvgd/dZRpHpXxi
g8eZ8uNP7nyug/TdWoYE6Lca+ve2AaUeI2um2Q/QF0kT0yejt7d2mKM6qpOMMNYa
Jps7BoG3gz1vB3+TwVTfQ4iUGPgAtOAVRUm1tV0EOz7lW2p8luR1y6Ttzgp2DecI
LQIDAQAB
-----END PUBLIC KEY-----'''
```



chave_AE X

Arquivo

Editar

E

Êÿ- .1F00øE±-;Z6è

Ln 1, Col 17 | 16 caracteres

Resultados do protótipo

```
-----BEGIN RSA PRIVATE KEY-----
MIIEoAIBAAKCAQEAyTQDpyp5mT46Lv4CfIqtC9DI7hWb1vLN5NAr5Ad7keqKciv
hIRSq0bgkfFvTZy7n9fhAQLqez1GmFIXtw4UGrI0xvUvZN0nJdB09xmAjW6n37cH
Gd1hIqKOK971p3cHga/V9WWP0LkPXBxylryUywcg6Eve7zSFTXsjFRFxaaIE9cvu
mfZ1sHm8+u/Gy0Mz78SsjNnvgd/dZRpHpXxig8eZ8uNP7nyug/TdWoYE6Lca+ve2
AaUeI2um2Q/QF0kT0yejt7d2mKM6qpOMMNYaJps7BoG3gz1vB3+TwVTfQ4iUGPgA
tOAVRUmltV0EOz71W2p81uR1y6Ttzgp2DecILQIDAQABAoIBA Aj3hzkmQLSWbB/n
hKNZx9QIukVL0xhIgYI/iey5Gshhi8Egd0gL4KZ0+peuf6QhGdCKHbY+k8Ypm46S
zAlFuJom+oiqaTIQ1BuQkNBc49iJx7QF82xQ7DEptw/X+DE+Mgiy1jGBVPs7oCZe
AzJaFbSFrQ8FQJp/B/jXxcy80gXf1QRaLivrct4cUacgqk1jcFy0YMgJpahkEvpU
iHw38f5KyLzKL64xEVpLu4S2sMYKfr12hJOag3nu4oiaWyYIsQ1nePNXrX4ISh78
5d4rhwYehCm+gig+echjYmX1TMe+otUhQ0Gfc59MxfrVPmfqpyUtEC+iDaYn7guk
B8Ut+WkCgYE Ayf31mOL10bZ1SsNx1tcMzaF3s6uVvg1yzzTNDXp10Jw6qBtpVNrZ
13dBGd1EeSsQMaB10HXjMff1n8KSouRRkm9AVp92u4riu4jSR/3I87vf70yXvUWM
4TXN8peqlniVbfj6kzVrFD70x6Rq3pdYaXU7k3ygreKbNNVXpWgf79kCgYEA/wAP
Okt070ZiNhgsqNxUkpmGqw4mFzNezVZGRnuZf6F+sv24TTa/YCToXoQyJIK8hsvm
fwIY6CodWh05xkcnsXZD3vVbf/tjAXwptmZVxZ4zKXD0vrou2nrXW+8e0HgV1EJ4
q/0KGpMktMY6SGw3YNpEQ94YSEweMVn0f3dpenUCgYBItSIBdk+CJmnVYTDu/2QY
UKGIQX9JgpTqQ0k7fuamTNI10D/+4YhrcLF1ikD13V9qgPGALzu5PWzgh1rVEzHx
10Af1ImXGEW4UyI/X/uFb/f7dZqpOYWgwIRF2mvYYFDVjugUa/RJzm+KDATVhawE
z08yIaL711M2PFM6V2nT8QJ/GeXnpgQD3E1JsDTEVGIMNNdi1fyZ4cFV34TjnkTv
UgcU1xjtnunwhdM5x1+muA84Fn1e8EdGQE4GrSBKvdh8JPnd6scAg/8EDyKNGf1K
vMdUauEN+1DucUIInU2r04BetzAJEW6hmBFZqQJ460IUvcFtLXdg//a7GkgEs01v
yQKBgFZ87G8s9s+42TSvsgRr-fNRpzPc7rmBJvhGaNjw7cHP3L09bXohDfcVHDSrb
DIIq6YWXvgGWfn90XoQ6o1q+y4DGPVkbT2+r38Dn1msW8Vq0QsFjj05xuGwbKERn
av036y1m5kZ/+vpvrwICb1UNORc+o1FWC8h6ITuQtMNRq9Yn
-----END RSA PRIVATE KEY-----
```

Resultados do protótipo

```
def descriptografa_chave(caminho_diretorio):
    caminho_chave = os.path.join(caminho_diretorio, 'chave_AES.key')
    caminho_privada = os.path.join(caminho_diretorio, 'private.key')

    if os.path.exists(caminho_privada):
        with open(caminho_privada, 'rb') as file:
            chave_privada = RSA.import_key(file.read())

        cifra_rsa = PKCS1_OAEP.new(chave_privada)

        with open(caminho_chave, 'rb') as file:
            conteudo_chave_aes = file.read()

        descriptografado = cifra_rsa.decrypt(conteudo_chave_aes)

        with open(caminho_chave, 'wb') as file:
            file.write(descriptografado)
    else:
        print('Voce ainda nao recebeu a chave RSA, pague o resgate!')
        exit()
```

Resultados do protótipo

```
def descriptografa(chave_AES, caminho_diretorio):
    extensoes = ('.pdf', '.txt', '.png')

    for diretorio, pastas, arquivos in os.walk(caminho_diretorio):
        for arquivo in arquivos:
            if arquivo.endswith(extensoes):

                caminho_arquivo_criptografado = os.path.join(diretorio, arquivo)

                with open(caminho_arquivo_criptografado, 'rb') as file_cript:
                    iv = file_cript.read(16)
                    conteudo = file_cript.read()

                cifra = AES.new(chave_AES, AES.MODE_CBC, iv)
                conteudo_descri = cifra.decrypt(conteudo)
                conteudo_desp = unpad(conteudo_descri, AES.block_size)

                with open(caminho_arquivo_criptografado, 'wb') as file_decrypt:
                    file_decrypt.write(conteudo_desp)
                print(f'Conteudo de {caminho_arquivo_criptografado} foi descriptografado')
```


Métricas do modelo

- Acurácia: Mede a proporção de previsões corretas em relação ao total
- Recall: Proporção de previsões positivas corretas em relação ao total de verdadeiros positivos
- Validação Cruzada
- Precisão: Proporção de previsões positivas corretas em relação ao total de previsões positivas feitas
- F1-Score: Média harmônica entre a precisão e o recall
- Matriz de Confusão
- Importância das features

Resultados do modelo

```
ExportSize: 0.004392028442761652
NumberOfSections: 0.050632218496519776
SizeOfStackReserve: 0.069675172528663
DebugSize: 0.0908637348272874
DebugRVA: 0.07560296852052804
MajorImageVersion: 0.017841858789589927
MajorOSVersion: 0.14689162405412776
IatVRA: 0.017475082539628532
MajorLinkerVersion: 0.11760677001377616
MinorLinkerVersion: 0.017579809349436756
ExportRVA: 0.020942743702161985
Machine: 0.10003304354249651
DllCharacteristics: 0.19118717762812862
BitcoinAddresses: 0.0001858245417776691
ResourceSize: 0.07908994302311632
```

Valores únicos para o campo Machine: [332 34404 452 43620 0 870]

Valores únicos para o campo Benign: [1 0]

Ocorrências do valor 0 em Machine: 1

Ocorrências do valor 332 em Machine: 50624

Ocorrências do valor 34404 em Machine: 11685

Ocorrências do valor 452 em Machine: 98

Ocorrências do valor 43620 em Machine: 76

Ocorrências do valor 870 em Machine: 1

Machine = 332 e Benign = 1: 15263

Machine = 332 e Benign = 0: 35361

Machine = 34404 e Benign = 1: 11681

Machine = 34404 e Benign = 0: 4

Importância das Features:

NumberOfSections: 0.03803961604566686

SizeOfStackReserve: 0.07779992711544548

DebugSize: 0.20312268513790158

DebugRVA: 0.10857346353226245

MajorOSVersion: 0.09557941823823797

MajorLinkerVersion: 0.08988067773132569

DllCharacteristics: 0.28998706402273033

ResourceSize: 0.09701714817642973

Precisão do Modelo: 0.9793022511469114

Validação Cruzada: [0.99183804 0.9937585 0.99383852 0.99567896 0.99495879]

Média da validação cruzada: 0.9940145634952389

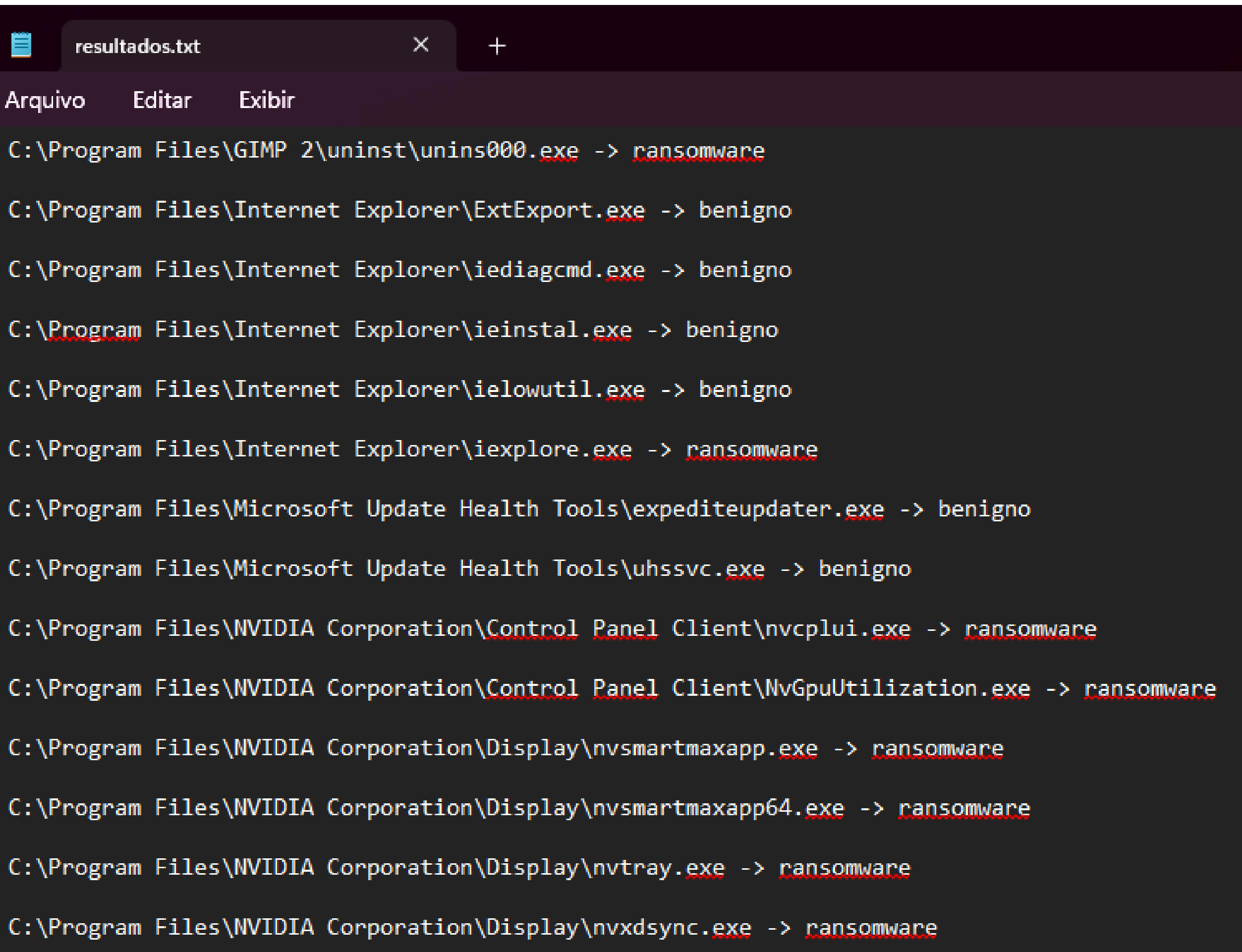
Report das Classificações:

	precision	recall	f1-score	support
0	0.97	0.99	0.98	10661
1	0.99	0.96	0.98	8085
accuracy			0.98	18746
macro avg	0.98	0.98	0.98	18746
weighted avg	0.98	0.98	0.98	18746

Matriz de Confusão:

[[10567 94]

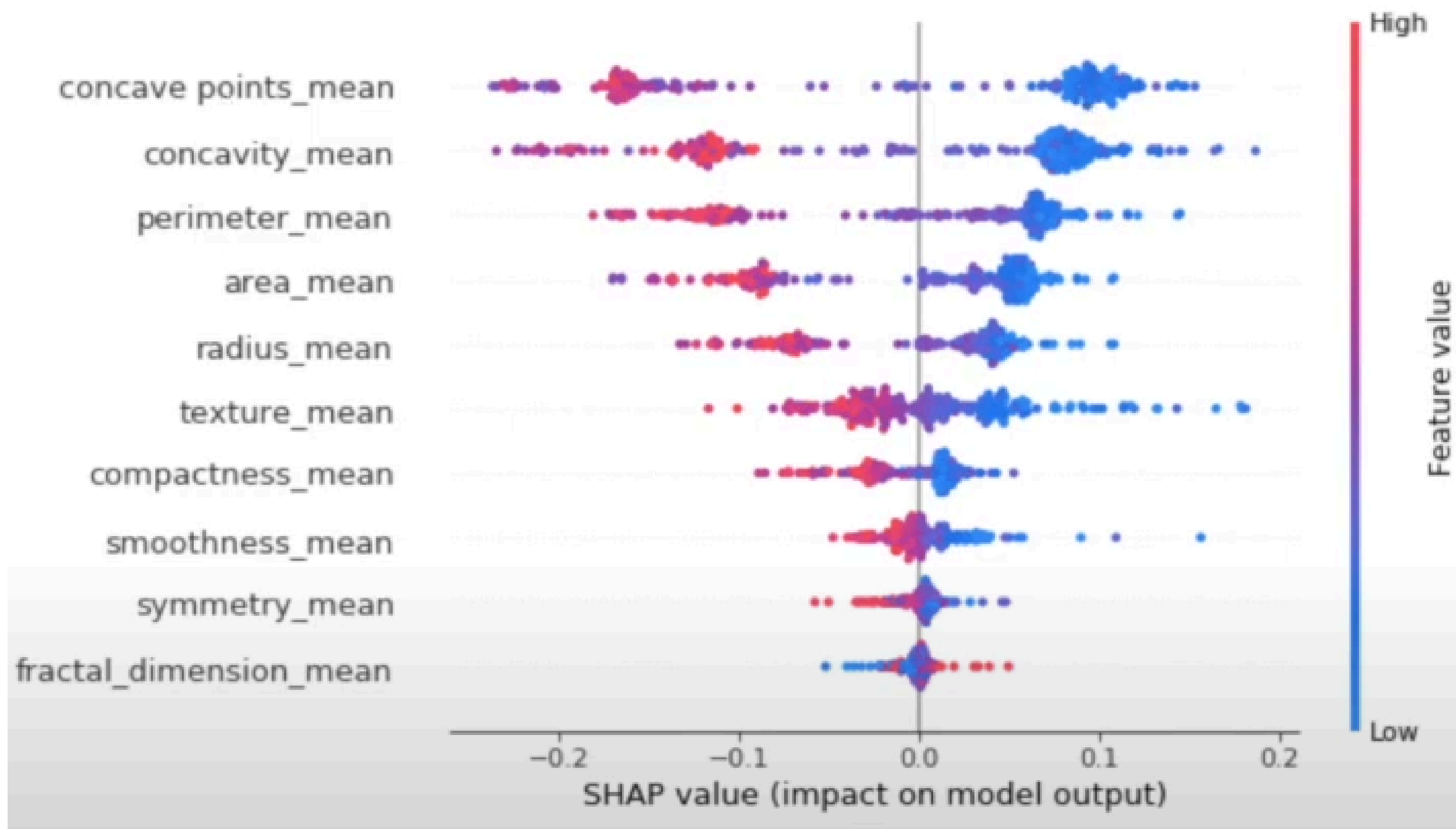
[294 7791]]

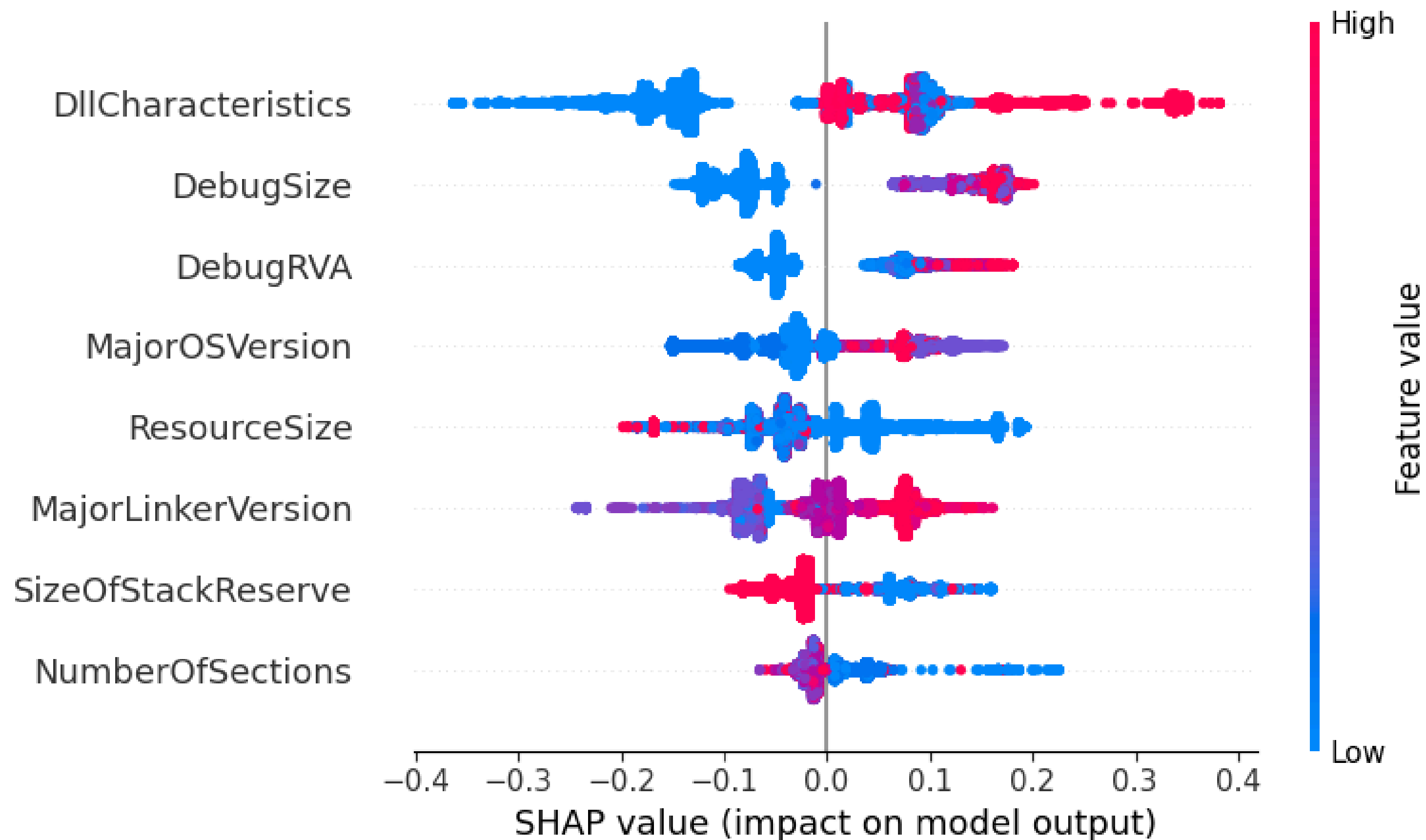


resultados.txt

Arquivo Editar Exibir

```
C:\Program Files\GIMP 2\uninst\unins000.exe -> ransomware
C:\Program Files\Internet Explorer\ExtExport.exe -> benigno
C:\Program Files\Internet Explorer\iediagcmd.exe -> benigno
C:\Program Files\Internet Explorer\ieinstal.exe -> benigno
C:\Program Files\Internet Explorer\ielowutil.exe -> benigno
C:\Program Files\Internet Explorer\iexplore.exe -> ransomware
C:\Program Files\Microsoft Update Health Tools\expediteupdater.exe -> benigno
C:\Program Files\Microsoft Update Health Tools\uhssvc.exe -> benigno
C:\Program Files\NVIDIA Corporation\Control Panel Client\nvcplui.exe -> ransomware
C:\Program Files\NVIDIA Corporation\Control Panel Client\NvGpuUtilization.exe -> ransomware
C:\Program Files\NVIDIA Corporation\Display\nvsmartmaxapp.exe -> ransomware
C:\Program Files\NVIDIA Corporation\Display\nvsmartmaxapp64.exe -> ransomware
C:\Program Files\NVIDIA Corporation\Display\nvtray.exe -> ransomware
C:\Program Files\NVIDIA Corporation\Display\nvxdsync.exe -> ransomware
```





**Obrigado pela
atenção!
Dúvidas!?**

