Universidade de Pernambuco
Programa de Pós-Graduação em Engenharia da Computação (PPGEC)

Proposta de Dissertação de Mestrado

Área: Computação Inteligente

Título: Antivírus Inteligente: Detecção Preventiva de Malware Empregando Redes Neurais Artificiais

Orientador – Sidney Marlon Lopes de Lima (sidney.lima@ufpe.br)

Descrição:

Os antivírus tradicionais, embora populares, demonstram falhas no combate às ameaças cibernéticas (LIMA, *et. al* 2023) (PINHEIRO, *et. al* 2022). O presente projeto propõe uma solução baseada em redes neurais artificiais visando detecção preventiva dos *malware* (malicioso + software). O sistema visa identificar proativamente ameaças recém lançadas, superando as limitações dos antivírus tradicionais. Modelos de aprendizado inteligente serão treinados com um vasto conjunto de dados de arquivos, permitindo a identificação de padrões e comportamentos maliciosos. Antes mesmo da execução, o modelo treinado determinará se o arquivo suspeito é benigno ou malicioso. Essa abordagem oferecerá várias vantagens, como a identificação eficaz de *malwares* novos e desconhecidos, a minimização de falsos positivos e maior acurácia na classificação, a atualização dos modelos de aprendizado de modo a acompanhar a evolução das ameaças, e a minimização de transtornos causados por falsos positivos. O impacto e os benefícios esperados incluem maior segurança para usuários e empresas, redução do risco de ataques cibernéticos e seus impactos negativos, maior capacidade de resposta a novas ameaças e vulnerabilidades e desenvolvimento de ferramentas mais robustas e confiáveis contra o *malware*.

Materiais e Habilidades necessárias

- Familiaridade com técnicas de redes neurais artificiais visando reconhecimento de padrão.
- Conhecimentos sólidos nas linguagens Python e Matlab.
- Ao menos um HD externo particular com capacidade mínima de 1 TB.

Referências Bibliográficas

Pinheiro, R.P., Lima, S.M.L., Souza, D.M. *et al.* Antivirus applied to JAR malware detection based on runtime behaviors. Scientific Reports - Nature Research 12, 1945 (2022). https://doi.org/10.1038/s41598-022-05921-5

Lima, S.M.L., Silva, S.H.M.T., Pinheiro, R.P. *et al.* Next-generation antivirus endowed with web-server Sandbox applied to audit fileless attack. Soft Computing 27, 1471–1491 (2023). https://doi.org/10.1007/s00500-022-07447-4