XLabPlatform

This innovative project aims to create a Windows/Mac application that utilizes language model (LLM) technology to continuously rewrite its own code and orchestrate the execution of multiple instances in a peer-to-peer (P2P) fashion. The primary objective of the XLabPlatform is to serve as a robust test target for modern antivirus applications, enabling researchers and developers to evaluate and enhance their effectiveness in detecting and mitigating evolving cyber threats.

Set of Questions or Problems to Address:

The XLabPlatform project aims to answer or address the following questions and problems:

- How can we develop an application that leverages LLM technology to continuously rewrite its own code, thereby creating a dynamic environment for testing antivirus software?
- Can we effectively orchestrate the execution of multiple instances of the application in a P2P manner, ensuring scalability and distribution of computational resources?
- How can we gather relevant datasets, such as crypto wallet withdrawal and captcha screenshots, and utilize AI technologies for screenshot understanding, as well as keyboard and mouse automation?
- How can we develop plugins, such as HumanLog, AVLog, RoboLocker, ScreenSpoofer, ClipboardSpoofer, CaptchaSolver, to simulate and evaluate various attack scenarios and system vulnerabilities?
- How can we enable distributed LLM inference, optimizing resource utilization by conducting CPU inference only when the computer is inactive?

Methodologies and Approaches:

The XLabPlatform project will employ the following methodologies and approaches:

- LLM Technology: Utilize state-of-the-art LLM technology to continuously rewrite the code of the XLabPlatform application, introducing variations and generating new instances for comprehensive testing.
- P2P Orchestration: Develop a robust P2P framework within the application to manage the execution and communication among multiple instances, ensuring scalability and efficient resource utilization.
- XCloudPlatform Integration: Integrate the XLabPlatform with the XCloudPlatformX to gather relevant datasets, leverage AI technologies for screenshot understanding, keyboard and mouse automation, and facilitate the seamless functioning of various plugins.
- Plugin Development: Implement a set of plugins, including HumanLog, AVLog, RoboLocker, ScreenSpoofer, ClipboardSpoofer, and CaptchaSolver, to simulate different attack

scenarios, monitor antivirus activities, automate user interactions, and test system vulnerabilities.

- Distributed LLM Inference: Develop a mechanism to perform lazy CPU inference of the LLM model upon remote request, optimizing computational resources by leveraging idle periods of the computer.

Expected Results:

The XLabPlatform project anticipates achieving the following results:

- A functional Windows/Mac application, XLabPlatform, capable of rewriting its own code using LLM technology and orchestrating the execution of multiple instances in a P2P manner.
- Successful integration with XCloudPlatformX, enabling the collection of relevant datasets, AI-driven screenshot understanding, keyboard and mouse automation, and seamless plugin operation.
- Implementation of essential plugins, such as HumanLog, AVLog, RoboLocker, ScreenSpoofer, ClipboardSpoofer, and CaptchaSolver, providing diverse attack simulation capabilities, antivirus monitoring, and system vulnerability testing.
- Demonstration of distributed LLM inference, effectively utilizing idle periods of the computer to conduct CPU inference upon remote request.
- A comprehensive test target for modern antivirus applications, enabling researchers and developers to evaluate and enhance the efficiency