PHÁT HIỆN MÃ ĐỘC LẨN TRÁNH DỰA TRÊN OPCODE SỬ DỤNG MẠNG NƠ-RON HỌC SÂU HỒI QUY KẾT HỢP XỬ LÝ NGÔN NGỮ TỰ NHIÊN

Trần Nguyễn Đức Huy

Trường ĐH Công nghệ Thông tin - Đại học Quốc gia TP. HCM

What ?

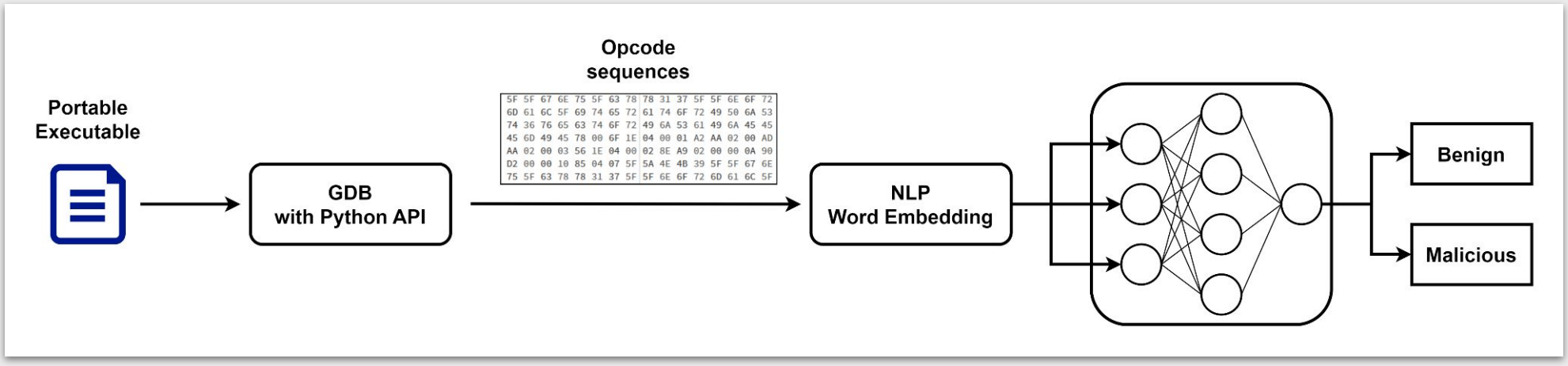
Chúng tôi xây dựng một giải pháp phát hiện mã độc lẩn tránh, trong đó:

- Opcode được trích xuất tại thời điểm thực thi thông qua GDB
- Kỹ thuật xử lý ngôn ngữ tự nhiên được áp dụng để tăng khả năng đúc kết hành vi của mã độc
- Mạng nơ-ron học sâu hồi quy được sử dụng để phát hiện mã độc dựa trên opcode

Why ?

- Các giải pháp phát hiện mã độc hiện tại còn giới hạn ở phương pháp phát hiện dựa trên đặc trưng tĩnh, không thể nhận diện các mã độc phức tạp được áp dụng các kĩ thuật lẩn tránh.
- Việc sử dụng kỹ thuật xử lý ngôn ngữ tự nhiên trong bài toán phân loại / phát hiện mã độc mang tiềm năng lớn

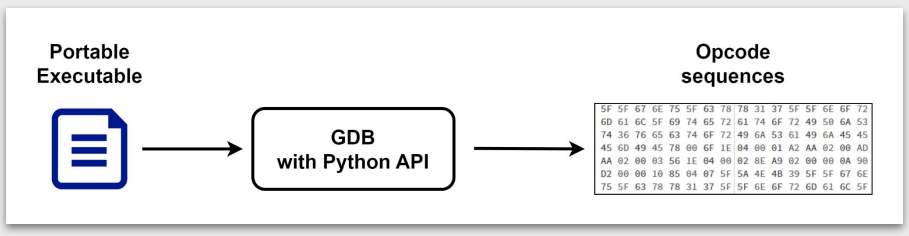
Overview



Description

1. Trích xuất opcode trong thời gian thực thi

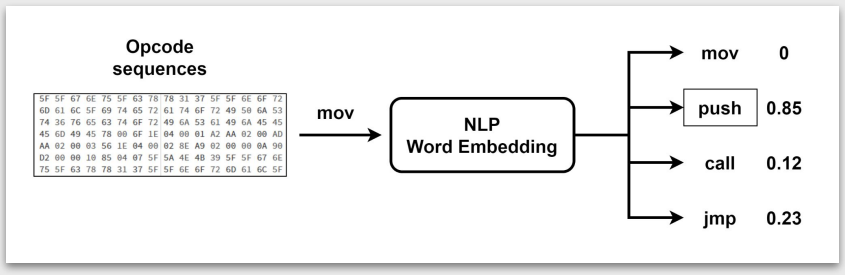
- Opcode từ các tệp thực thi được trích xuất thông qua trình dịch ngược GDB. Các tệp PE được thực thi bởi GDB và opcode được thu thập trong quá trình thực thi, giúp ta quan sát được hành vi thật sự của mã độc được áp dụng các kỹ thuật lẩn tránh.
- Python API của GDB sẽ được sử dụng để tự động hóa quá trình trích xuất opcode từ tệp thực thi.



Hình 1. Trích xuất opcode tại thời gian thực thi sử dụng GDB.

2. Phân tích opcode sử dụng kỹ thuật xử lý ngôn ngữ tự nhiên

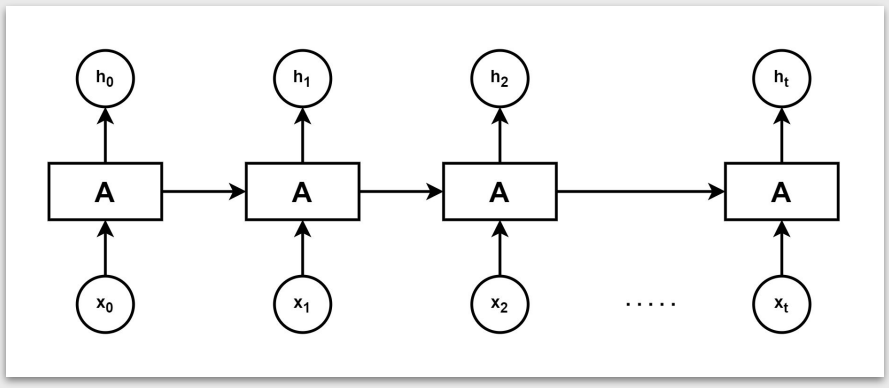
- Opcode cũng tương tự như ngôn ngữ nói, có thể được phân tích thông qua các kỹ thuật xử lý ngôn ngữ tự nhiên, giúp mô hình máy học dự đoán được hành vi của mã độc.



Hình 2. Dự đoán lệnh tiếp theo sử dụng NLP.

3. Phát hiện mã độc dựa trên mạng nơ-ron học sâu hồi quy

- Mạng nơ-ron học sâu hồi quy thích hợp với các bài toán với dữ liệu có tính tuần tự. Các thuật toán học sâu hồi quy có khả năng kết hợp dữ liệu từ các lớp trước với dữ liệu của lớp hiện tại, do đó mô hình máy học sâu hồi quy có khả năng học được các pattern phức tạp của dữ liệu.



Hình 3. Mạng nơ-ron học sâu hồi quy.

NII

Trần Nguyễn Đức Huy – Trường Đại học Công nghệ Thông tin - ĐHQG HCM

TEL : ********* Email : huytnd.18@grad.uit.edu.vn