Phương pháp phát hiện DGA Botnet dựa trên Học máy

1 VẤN ĐỀ BÀI BÁO

Trong nghiên cứu này, chúng tôi nhắm đến việc giải quyết hai vấn đề quan trọng nhất trong việc phát hiện botnet, bao gồm:

- Vấn đề phân loại nhị phân: Với dữ liệu đầu vào của các truy vấn tên miền, vấn đề này sẽ phân loại các tên miền thành hai lớp, bao gồm tên miền vô hại và tên miền độc hại.
- Vấn đề phân loại đa lớp: Với dữ liệu đầu vào của các truy vấn tên miền đã được đánh dấu độc hại, vấn đề này sẽ xác định xem tên miền thuộc về gia đình botnet DGA nào.

Kết quả nhận diện đó có thể hỗ trợ quét và loại bỏ botnet từ các máy tính bị nhiễm bệnh một cách tốt hơn.

Bài báo này [1] đề cập đến mối đe dọa đáng kể từ botnet đối với an ninh internet bằng cách đề xuất các giải pháp phát hiện và phân loại mới lạ nhằm mục tiêu cụ thể là botnet sử dụng thuật toán tạo tên miền (DGA). Bằng cách tận dụng mạng LSTM và các lớp Attention, các tác giả giới thiệu hai mô hình học sâu, LA_Bin07 và LA_Mul07, hiệu quả đối phó với thách thức phân loại nhị phân và đa lớp. Đánh giá trên tập dữ liệu UMUDGA, bao gồm 50 gia đình botnet DGA, thể hiện độ chính xác cao của các mô hình trong việc xác định các miền độc hại và phân loại các gia đình botnet.

2 PHƯƠNG PHÁP THỰC HIỆN

2.1 Chuẩn bị dataset

Thu thập tập dữ liệu UMUDGA, đóng vai trò là dữ liệu huấn luyện cho các mô hình. Tập dữ liệu này nên bao gồm các ví dụ đã được gán nhãn của tên miền cùng với phân loại tương ứng (benign hoặc thuộc về một gia đình botnet cụ thể).

2.2 Tiền xử lý dữ liệu

Thực hiện bất kỳ bước tiền xử lý nào cần thiết trên tập dữ liệu, chẳng hạn như tokenization, normalization hoặc feature extraction. Bước này đảm bảo dữ liệu có định dạng phù hợp để huấn luyện mô hình.

2.3 Thiết kế kiến trúc mô hình

Xác định kiến trúc của các mô hình LA_Bin07 và LA_Mul07. Các mô hình này nên kết hợp các lớp LSTM và lớp Attention. Các lớp LSTM giúp mô hình nắm bắt tính tuần tự của dữ liệu, trong khi lớp Attention giúp mô hình tập trung vào các phần quan trọng của đầu vào.

2.4 Huấn luyện mô hình

Huấn luyện các mô hình LA_Bin07 và LA_Mul07 bằng cách sử dụng tập dữ liệu đã được chuẩn bị và tiền xử lý. Trong quá trình huấn luyện, các mô hình học cách nhận ra các mẫu và đưa ra dự đoán chính xác dựa trên các tên miền đầu vào và phân loại tương ứng.

2.5 Đánh giá hiệu suất mô hình

Đánh giá hiệu suất của các mô hình đã được huấn luyện bằng cách sử dụng các độ đo đánh giá phù hợp, chẳng hạn như độ chính xác, độ precision, độ recall hoặc điểm F1. Bước này giúp xác định mức độ mô hình tổng quát hóa với dữ liệu chưa được nhìn thấy trước, kết quả mô hình phát hiện và phân loại botnet DGA một cách hiệu quả.

3 TẬP DATASET VÀ KẾT QUẢ

3.1 Dataset

- Andrey Abakumov's DGA Repository (Abakumov, 2016)
- OSINT DGA feed (OSINT 2021)
- UMUDGA dataset (Zago et al., 2020)
- 360NetLab dataset (360NetLab 2016)

Sử dụng 04 bộ dữ liệu trên để đánh giá vì chúng đáp ứng đầy đủ các tính chất sau:

- Tính nguyên bản: Các bộ dữ liệu này bao gồm các miền lành tính và độc hại ở dạng ban đầu và dữ liệu cũng đã được dán nhãn, phù hợp làm đầu vào cho các vấn đề nghiên cứu.
- Dễ so sánh: Bốn bộ dữ liệu đã được các nhà nghiên cứu khác sử dụng để đánh giá trong các nghiên cứu trước đây của họ. Thật thuận tiện cho việc so sánh giữa kết quả của chúng tôi và kết quả trước đó.
- Tính công khai: Các bộ dữ liệu này được cung cấp công khai trên Internet, dễ dàng truy cập và thuận tiện cho các nhà nghiên cứu.

3.2 Kết quả

3.2.1 Binary classification.

Mô hình được đánh giá thông qua các chỉ số như độ chính xác, precision, recall, F1-Score, ROC curve và AUC plots trên các tập dữ liệu thực tế. Kết quả thử nghiệm cho thấy mô hình đạt hiệu suất tốt trong việc phân loại botnets DGA, với các chỉ số đánh giá đáng chú ý như ROC Curve và AUC.

3.2.2 Multiclass classification.

Mô hình được đánh giá trên Google Colab Pro, môi trường Linux, sử dụng GPU NVIDIA Tesla T4 và thư viện Keras. Kết quả thử nghiệm cho thấy mô hình đạt hiệu suất tốt trong giải quyết vấn đề phân loại nhị phân, với các chỉ số như độ chính xác, precision, recall được đánh giá chi tiết. Đánh giá mô hình thông qua các tham số này giúp xác định kết quả phân loại và hiệu suất tổng thể của mô hình.

4 KẾT LUẬN

Mô hình đề xuất có sự tin cậy trong phát hiện và phân loại botnets DGA. Hiệu suất cao và thời gian thử nghiệm nhanh của mô hình đề xuất đáp ứng tốt yêu cầu xử lý thời gian thực trong thực tế.

5 PHƯƠNG HƯỚNG PHÁT TRIỂN TRONG TƯƠNG LAI

Trong tương lai, dự án sẽ tiếp tục nghiên cứu và phát triển các phương pháp mới để cải thiện hiệu suất phát hiện botnets DGA. Đồng thời, tập trung vào việc mở rộng dữ liệu và cải thiện mô hình để xử lý các trường hợp phức tạp hơn, đồng thời tối ưu hóa thời gian xử lý và nâng cao hiệu quả phân loại.

TÀI LIỆU

[1] Tuan, T. A., Long, H. V., & Taniar, D. (2022). On detecting and classifying DGA botnets and their families. Computers & Security, 113, 102549.