ỨNG DỤNG NATURAL LANGUAGE PROCESSING(NLP) ĐỂ THU THẬP TRI THỨC AN NINH MẠNG TRÊN TRÌNH DUYỆT WEB

Tác giả: Sử Chấn Hoài Bảo

Trường Đại học Công Nghệ Thông Tin - Đại Học Quốc Gia

What ?

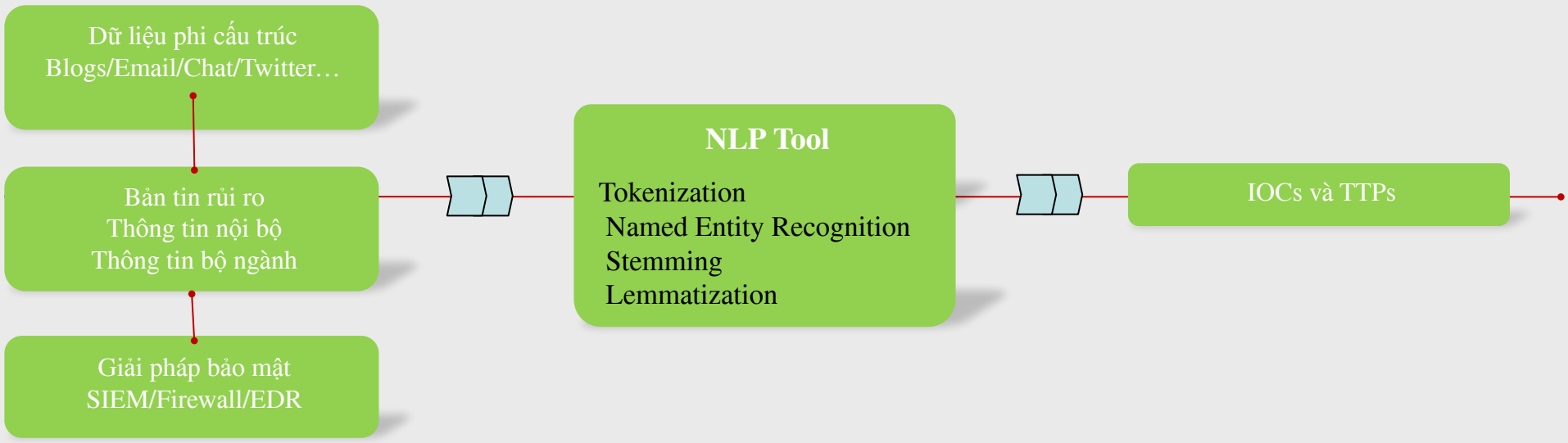
Nghiên cứu này đề xuất một giải pháp sử dụng NLP để phát hiện và thu thập tri thức an ninh mạng từ các nguồn nội dung phi cấu trúc:

- Phát triển một tiện ích mở rộng trên trình duyệt Chrome, Firefox, Edge
- Công cụ quét và thu thập thông tin tri thức an ninh mạng như IP, Domain, URL, Fire hash, Email v…

Why ?

- Những kẻ tấn công đang hợp tác và chia sẻ cách thức khai thác lỗ hổng cho nhau, các cuộc tấn công thường có quy mô hàng loạt. Việc chủ động thu thập tri thức an ninh mạng sẽ giúp tổ chức chủ động hơn trong việc phòng thủ
- Công cụ sử dụng NLP sẽ giúp tiết kiệm thời gian, tăng cường kiến thức. Giúp các chuyên gia an ninh mạng đưa ra các quyết định xử lý nhanh và chính xác.

Tổng Quan



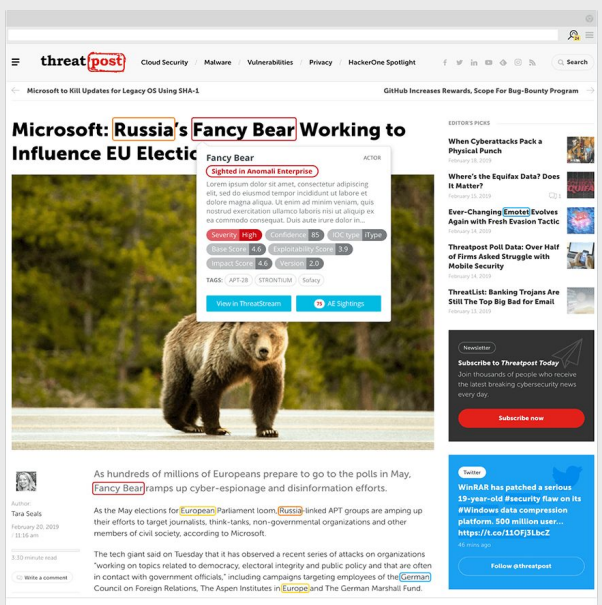
Mô tả

Nội dung

Công cụ này khai thác sức mạnh của Xử lý ngôn ngữ tự nhiên (NLP) để cho phép các tổ chức đưa ra quyết định nhanh hơn và chính xác hơn. Công cụ ngay lập tức xác định thông tin an ninh mạng chiến lược và chiến thuật từ bất kỳ trang trình duyệt.

Công cụ được thiết kế để phù hợp với các vai trò bảo mật bằng cách nâng cao trình độ của mọi nhà phân tích bảo mật lên trình độ của một chuyên gia có kinh nghiệm và chuẩn hóa toàn bộ quá trình nghiên cứu và báo cáo các mối đe dọa mạng.

Kết quả



Xác định các thực thể liên quan tới tri thức an ninh mạng trên trình duyệt web từ những nguồn nội dung phi cấu trúc, chuyển các dữ liệu này thành ngôn ngữ mà máy có thể hiểu được như CSV, Snort, OpenIOC, bao gồm nhưng không giới hạn tại các cấp độ tri thức an ninh mạng:

Cấp độ 1: Thông tin về các chỉ số thỏa hiệp như IP, Domain, URL, File hash, Email v.v…

Các thông tin này thường sẽ có giá trị trong vài tuần hoặc vài tháng, dùng để đánh chặn trực tiếp trên các thiết bị bảo mật.

Cấp độ 2: Thông tin liên quan tới kỹ thuật tấn công, các loại mã độc, họ phần mềm độc hại v.v.v

Các thông tin này có giá trị sử dụng vài tháng đến một năm, hỗ trợ các độ ngũ bảo mật điều tra, phân tích các hành vi đáng ngờ, chủ động ngăn chặn sớm các cuộc tấn công

Cấp độ 3: Thông tin liên quan đến các nhóm tấn công, các chiến dịch mà chúng thực hiện, các mục tiêu mà chúng đang nhắm đến.

Các thông tin này có giá trị sử dụng lên đến chục năm, cung cấp một bức tranh tổng quát, đưa ra cái nhìn sâu sắc về chiến lược phòng thủ an ninh mạng.

NII

Sử Chấn Hoài Bảo– Trường Đại học Công Nghệ Thông Tin - DHGQ HCM

TEL : 0903135775 Email : baosch.18@grad.uit.edu.vn