XÂY DỰNG ĐỒ THỊ TRI THỨC DỰA TRÊN HỌC MÁY TỪ THÔNG TIN ĐE DỌA MẠNG ĐỂ XÁC ĐỊNH NGUỒN GỐC APT

Tô Thị Mỹ Âu - 230202002

Tóm tắt

- Lớp: CS2205.CH181
- Link Github: *https://github.com/Tothimyau/CS2205.CH181*
- Link YouTube video: https://www.youtube.com/watch?v=6WQfGMJtOuE

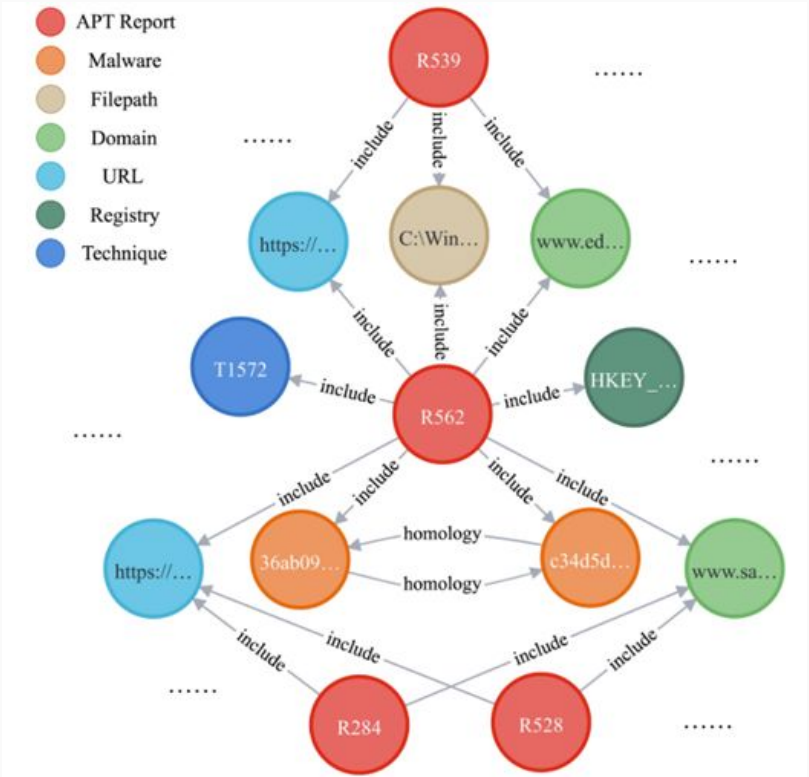
Tô Thị Mỹ Âu

Giới thiệu

- Các cuộc tấn công mạng ngày càng phức tạp và tiên tiến hơn, đặc biệt là các cuộc tấn công từ APT.
- Thế nên việc xác định nguồn gốc mối đe dọa là một chiến lược phòng thủ quan trọng để chống lại các mối dọa APT.
- Để xác định nguồn gốc APT, cần phải tìm hiểu và phân tích CTI từ các nguồn khác nhau.
- CTI giúp ngăn chặn sớm tấn công mạng, giảm thiểu tác động của chúng.
- Tuy nhiên, việc phân tích và xử lý lượng lớn thông tin này trở nên phức tạp và tốn thời gian nếu chỉ dựa vào phương pháp truyền thống.

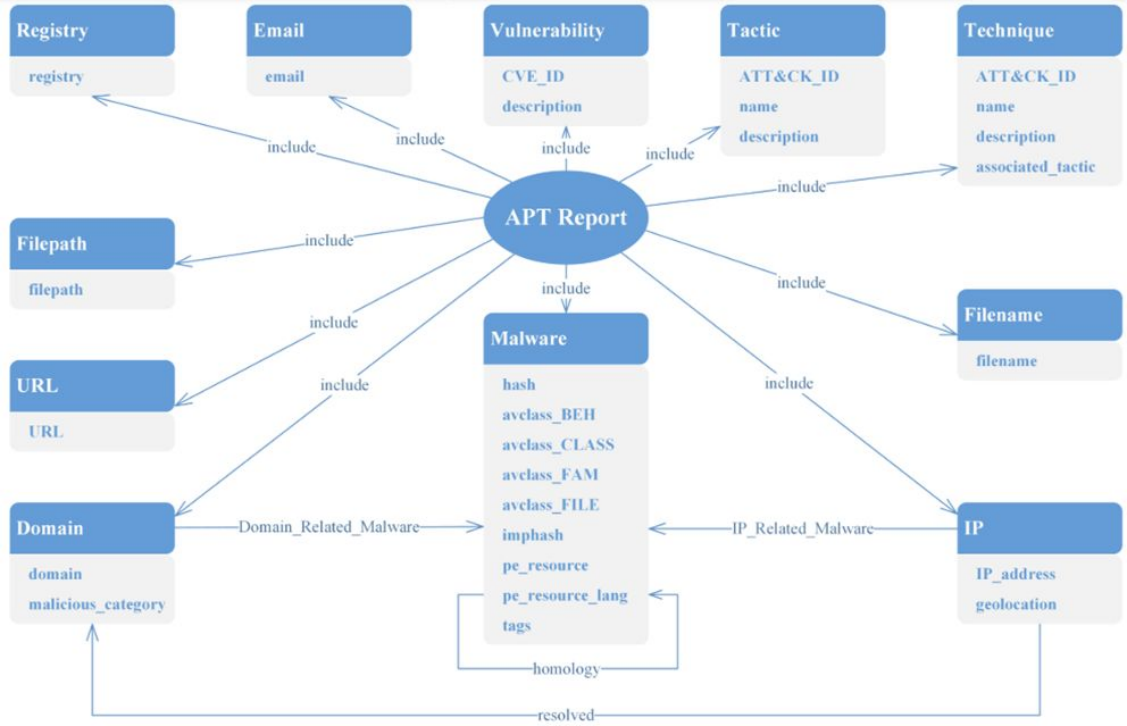
Giới thiệu

- KG được xem là một heterogeneous graph (đồ thị không đồng nhất).
- CSKG nhằm thay đổi cách biểu đạt tri thức về các mối đe dọa, giúp thu thập chính xác và hiệu quả các loại thông tin đe dọa khác nhau, giúp ra quyết định phòng chống hiệu quả nhanh chóng.



Giới thiệu

- Input: Các nguồn thông tin CTI.
- Output: Đồ thị tri thức từ CTI có biểu diễn nguồn gốc tấn công.



Mục tiêu

- Nghiên cứu, hiểu về phương pháp để xây dựng đồ thị tri thức trong an ninh mạng.
- Nghiên cứu về thuật toán để thực hiện thu thập, phân tích và trích xuất thông tin về mối đe dọa.
- Dựa trên đồ thị tri thức và thông tin thu thập được thực hiện xác định nguồn gốc của APT.

Nội dung và Phương pháp

- Tìm hiểu và đánh giá các hạn chế của phương pháp xác định nguồn gốc APT truyền thống.
- Tìm hiểu các phương pháp tự động hóa trích xuất và phân loại thực thể.
- Thu thập các nguồn dữ liệu mối đe dọa APT để thực nghiệm.
- Tiến hành đề xuất thiết kế kiến trúc cụ thể cho việc xây dựng đồ thị tri thức để xác định nguồn gốc APT.
- Thực nghiệm một hệ thống hoàn chỉnh, dựa trên các phương pháp đã đề xuất.
- Đánh giá kết quả của hệ thống vừa đề xuất với các hệ thống khác.

Nội dung và Phương pháp

Kế hoạch thực hiện được thể hiện dưới dạng biểu đồ Gantt

Công việc	Tháng 1	Tháng 2	Tháng 3	Tháng 4	Tháng 5	Tháng 6	Tháng 7
Nghiên cứu về CTI							
Nghiên cứu về đồ thị tri thức trong an ninh mạng							
Nghiên cứu phương pháp xác định nguồn gốc mối de dọa							
Thực hiện thu thập so sánh các bộ dữ liệu							
Đề xuất kiến trúc							
Xây dựng môi trường thực nghiệm							
Đánh giá hệ thống							

Kết quả dự kiến

- Hiểu về các phương pháp xây dựng và ứng dụng đồ thị tri thức trong lĩnh vực an ninh mạng.
- Tài liệu nghiên cứu khảo sát và thiết kế hệ thống đồ thị tri thức biểu diễn các mối đe dọa, xác định nguồn gốc tấn công APT.
- Báo cáo về xây dựng và thực nghiệm đồ thị tri thức dựa trên học máy từ thông tin mối đe dọa để xác định nguồn gốc APT.

Tài liệu tham khảo

[1]. Xiao, N., Lang, B., Wang, T., & Chen, Y. (2024). APT-MMF: An advanced persistent threat actor attribution method based on multimodal and multilevel feature fusion. *arXiv preprint arXiv:2402.12743*.

[2]. Sarhan, I., & Spruit, M. (2021). Open-cykg: An open cyber threat intelligence knowledge graph. *Knowledge-based systems*, *233*, 107524.

[3]. Ren, Y., Xiao, Y., Zhou, Y., Zhang, Z., & Tian, Z. (2022). CSKG4APT: A cybersecurity knowledge graph for advanced persistent threat organization attribution. *IEEE Transactions on Knowledge and Data Engineering*.

[4]. Yue, L., Liu, P., & Wang, H. (2020). Overview of network security threat intelligence sharing and exchange. *Computer research and development*, *57*(10), 2052.

[5]. Tian, Z. (2020). Detection and traceability of high covert unknown threats in cyberspace. *Information and communication technology*, *14*(06), 4-7.