ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

BÁO CÁO GIỮA KỲ

MÁY HỌC TRONG BẢO MẬT MẠNG VÀ HỆ THỐNG

TÊN ĐỀ TÀI: MAGIC: DETECTING ADVANCED PERSISTENT THREATS VIA MASKED GRAPH REPRESENTATION LEARNING

GIẢNG VIÊN HƯỚNG DẪN
TS. LÊ KIM HÙNG

HỌC VIÊN THỰC HIỆN

230202002 - TÔ THỊ MỸ ÂU
220202022 - NGUYỄN HỒNG SƠN
230202006 - NGÔ THÁI HƯNG

TP. HỒ CHÍ MINH, NĂM 2024

Mục lục

1 Tóm tắt bài báo

MAGIC là một phương pháp học có giám sát để phát hiện các cuộc tấn công APTs bằng cách sử dụng phương pháp học masked graph representation. Nó cải thiện một số phương pháp trước đó bằng cách trích xuất efficient deep feature và structure abstraction on provenance graphs.

MAGIC có khả năng phát hiện multi-granularity, handle concept drift with a model adaption mechanism và có khả năng mở rộng. Nó sử dụng phương pháp phát hiện ngoại lệ để xác định hành vi bất thường.

MAGIC được đánh giá dựa trên 3 dataset, cho kết quả phát hiện với chỉ số precision và recall cao, chi phí thấp và nhanh hơn nhiều so với các phương pháp hiện tại

Các kết quả của bài báo là một công trình được phát hành dưới dạng open-source, với tiềm năng phát triển nhiều trong lương lai.