Détection d'attaques par analyse de métriques dans les graphes complexes dynamiques

Organisation

Laboratoire de Recherche de l'EPITA

Contact : Mark Angoustures mark.angoustures@epita.fr

Introduction

Les menaces persistantes avancées sont difficiles à détecter en raison de leurs schémas d'attaque en plusieurs étapes s'accompagnant de phases lentes et rapides.

Ces types d'attaques impliquent généralement des moyens de persistances d'accès et des mouvements latéraux vers d'autres environnements.

Détecter une campagne d'APT revient à identifier des patterns d'attaques dans des données de natures très hétérogènes, sur différentes échelles temporelles.

Diverses techniques ont été récemment mises au point pour représenter ces patterns, notamment la représentation des interconnexions entre les nœuds du système d'information sous forme de graphes.

Différentes métriques et centralités de graphes sont sujettes à une corrélation des différentes phases des APT.

Objectif

L'objectif de la thèse est de proposer une méthode de détection des menaces persistances avancées basées sur des réseaux complexes statiques et dynamiques. La thèse mesurera l'impact et la corrélation entre différentes métriques de réseaux complexes (centralités, dynamique temporelle, etc.) et les phases d'attaques des APT. Le deuxième objectif de la thèse sera d'établir une méthode pour prédire une phase d'attaque par des calcul de métriques et de centralités. La piste des Graph Neural Networks (GNN) pour apprendre et prédire ces métriques et centralités dans les réseaux complexes sera étudiée.

Axes :

Axe 1 :

La première approche de la thèse consistera à évaluer les méthodes de détection d'APT. Cette première étape permettra d'identifier les problématiques liées à ces méthodes.

Ensuite la thèse visera à construire une représentation des données sous forme de graphes statiques et dynamiques. Cette représentation devra prendre en compte les propriétés liées aux phases d'APT. L'état de l'art de la thèse incorpora des différentes représentations existantes en graphes liées à la sécurité.

Axe 2 :

La thèse abordera la mesure entre différentes centralités dynamique et statiques (closeness, betweenness, eigenvector...) sur les réseaux complexes des données contenant les attaques.

Au début, Il s'agira de se concentrer sur une ou deux métriques et attaques pour pouvoir produire une publication et du code associé dans la première année de thèse.

Axe 3 :

Enfin, la thèse visera à proposer une méthode pour approximer ces centralités pertinentes selon les différentes attaques. Au vu de la forte volumétrie et haute intensité des données, les modèles basées sur les réseaux de neurones sur les graphes peuvent être une piste à envisager pour approximer les différentes valeurs de centralités. Cette approche sera comparée à d'autres pistes d'approximation algorithmique de métriques de graphes. L'objectif est d'optimiser la qualité de la détection et le compromis temps vs précision.

Profil :

Le candidat est un jeune diplômé d'une formation initiale (ingénieur ou master universitaire) en informatique avec une spécialisation dans le domaine de la cybersécurité.

Idéalement, le candidat à des connaissances en l'apprentissage automatique et idéalement de bonnes notions de graphes.

La maîtrise d'un langage de programmation est indispensable.

Références :

M. Ussath, D. Jaeger, Feng Cheng and C. Meinel, "Advanced persistent threats: Behind the scenes," *2016 Annual Conference on Information Science and Systems (CISS)*, 2016, pp. 181-186, doi: 10.1109/CISS.2016.7460498.

Kipf TN, Welling M (2017a) Semi-supervised classification with graph convolutional networks. In: International Conference on Learning Representations

W. W. Lo, S. Layeghy, M. Sarhan, M. Gallagher and M. Portmann, "E-GraphSAGE: A Graph Neural Network based Intrusion Detection System for IoT," *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, 2022, pp. 1-9, doi: 10.1109/NOMS54207.2022.9789878.

Jaiswal, Ashish, Ashwin Ramesh Babu, Mohammad Zaki Zadeh, Debapriya Banerjee, and Fillia Makedon. 2021. "A Survey on Contrastive Self-Supervised Learning" *Technologies* 9, no. 1: 2. https://doi.org/10.3390/technologies9010002

PERNET, Cédric. *Sécurité et espionnage informatique: Connaissance de la menace APT (Advanced Persistent Threat) et du cyberespionnage*. Editions Eyrolles, 2015.

M. Ghanem, C. Magnien and F. Tarissan, "Centrality Metrics in Dynamic Networks: A Comparison Study," in *IEEE Transactions on Network Science and Engineering*, vol. 6, no. 4, pp. 940-951, 1 Oct.-Dec. 2019, doi: 10.1109/TNSE.2018.2880344.