Proposition de post-doctorat
Réponse symptomatique aux attaques réseau

Alexis Olivereau, CEA, alexis.olivereau@cea.fr

Contexte

Plus de 60% des attaques impactantes sont aujourd'hui des attaques zero-day, c'est-à-dire des attaques jamais observées par le passé et donc contre lesquelles des signatures n'ont pas encore été publiées. La protection contre ces attaques passe non seulement par des techniques de détection comportementale, mais aussi par la mise en œuvre en temps réel de mécanismes de réponse visant à les empêcher de causer des dommages et de se propager. Or les solutions qui sont aujourd'hui proposées pour réagir en temps réel aux attaques requièrent le plus souvent une modélisation complexe des motivations de l'attaquant. Quand elles visent à rendre possible des contre-mesures plus génériques, ces solutions restent très limitées dans le nombre des actions possibles.

Objectif

L'objectif de cette action est de proposer un mécanisme s'appuyant sur des analogies, déterminées par IA, entre des manifestations d'attaques en cours et des manifestations équivalentes d'attaques connues, afin de mettre en œuvre des contre-mesures visant à reconfigurer le réseau pour atténuer automatiquement l'attaque. Les attaques en cours de propagation seront particulièrement ciblées, avec une identification dynamique de schéma de propagation permettant non seulement de remonter à la source d'une attaque, mais aussi de stopper les mécanismes qu'elle emploie pour se propager.

Approche envisagée

Nous construirons des modèles représentant la variation d'états d'interactions du réseau à travers le temps. Ces modèles pourront être statiques (typiquement, matrices) ou dynamiques (typiquement, graphes). Ils permettront ensuite à une analyse par IA – déclenchée sur anomalie réseau – d'identifier des variations représentatives de types d'attaques connues, et par corrélation temporelle de reconnaître les différentes phases de propagation d'une même attaque. Une attaque subtile multi-phases du type de celles que nous nous proposons de cibler ne se trouvant pas dans les datasets classiques, nous expérimenterons sur un réseau virtualisé nous permettant de jouer des scénarios d'attaques sur des topologies diverses et d'en faire varier les paramètres afin de valider le bon fonctionnement de notre approche.

Résultats attendus

Il est attendu de ce travail qu'il permette de concevoir une preuve de concept multi-topologies et multi-attaques, en mesure de contrer dynamiquement une attaque en cours de propagation dans un réseau.