BEEZH: une plateforme de détonation réaliste pour l'analyse des modes opératoires d'attaquants

Frédéric GUIHERY, Alban SIFFER, Joseph PAILLARD,

AMOSSYS
frederic.guihery@amossys.fr; alban.siffer@amossys.fr; joseph.paillard@amossys.fr;

Résumé.

Dans le cadre de la lutte informatique défensive, la connaissance du mode opératoire des groupes d'attaquants est essentielle pour pouvoir se défendre et adapter sa posture face aux nouvelles menaces cyber. Cette connaissance provient généralement de différentes capacités complémentaires, telles que la veille, l'analyse des vulnérabilités et codes d'exploitation, ou encore le suivi des groupes d'attaquants et leurs cibles d'intérêts. L'une de ces capacités, la détonation, consiste à attirer un attaquant en activant des vecteurs d'infection (par exemple, une pièce jointe suspecte) dans un environnement simulé et maitrisé, à des fins d'observation et d'apprentissage des techniques d'attaque employées. Cette détonation est typiquement réalisée dans un environnement de type honeypot faisant croire à l'attaquant qu'il est présent sur un système d'information opérationnel.

Les techniques d'attaques à observer proviennent ainsi soit directement du malware, soit de l'attaquant ayant le contrôle de ce dernier. Sur ces deux cas de figure, le besoin de réalisme de l'environnement honeypot généré est crucial puisque le malware (ou l'attaquant ayant pris le contrôle de la cible) peut exécuter des routines vérifiant la crédibilité de l'environnement attaqué.

D'autre part, une plateforme de détonation doit permettre de produire des renseignements précis et complets sur la menace, en couvrant à la fois les techniques d'attaques connues et, idéalement, celles encore inconnues ou non publiques. De tels renseignements peuvent prendre la forme d'indicateurs de compromission (hashs d'outils d'attaques, IP et DNS de l'infrastructure d'attaque, etc.), ou peuvent caractériser le mode opératoire des groupes d'attaquants (tactiques, techniques et procédures d'attaques usuellement employées, également appelées TTP). Les renseignements produits sont alors généralement partagés à d'autres entités menant des opérations de détection (équipes SOC) ou d'analyse de la menace (équipes CERT / CTI).

Les innovations présentées dans ce papier visent à répondre aux deux besoins exprimés, à savoir :

- le besoin de réalisme du honeypot ;
- la capacité à extraire les traces d'intérêts pour la production de renseignements sur la menace.

Concernant le besoin de réalisme du honeypot, plusieurs aspects doivent généralement être traités : l'environnement système et applicatif, l'environnement réseau, et également la pertinence de la vie qu'il peut y avoir sur le système d'information simulé (les ressources et les actions de vie manipulant ces ressources). Dans ce papier, le réalisme est ici principalement abordé sous l'angle de la simulation de comportements utilisateur permettant de produire de la vie sur le honeypot.

A des fins d'expérimentation et de validation des travaux, la plateforme de honeypot BEEZH, développée par AMOSSYS, est ici exploitée. Cette plateforme a reçu en 2020 le premier prix du défi Deceptive Security organisé par la Direction Générale de l'Armement, le Commandement de la Cyberdéfense et l'Innovation Défense Lab. Cette plateforme apporte notamment les capacités de base suivantes :

- une capacité de construction dynamique de systèmes d'information (inventaire SI et topologie) ;
- une capacité de personnalisation avancée de l'environnement simulé (paramétrage des OS, de l'Active Directory, des arborescences de fichiers, des comptes et groupes utilisateurs, etc.).

Mots clés :
Lutte Informatique Défensive; Investigation Numérique; Honeypot; Détonation; Threat Intelligence