HoneyWISE :
stratégie d'exploitation d'honeytokens en environnement Active Directory

Nathan FAEDDA, Augustin TOURNYOL DU CLOS

WAVESTONE
nathan.faedda@wavestone.com;
augustin.tournyol-du-clos@wavestone.com;

Résumé

Les stratégies de Deceptive Cyber restent peu adoptées dans le monde de l'entreprise, vingt ans après les premiers projets de recherche d'envergure sur le sujet (Honeynet project, Project HoneyPot). Pourtant, les avantages de ces systèmes de détection font figure d'exception pour les SOC saturés d'alertes : taux de faux positifs quasi inexistants, faible coût de déploiement et de maintenance…L'étude suivante, baptisée HoneyWISE, propose une stratégie concrète de Deception visant à déceler plusieurs attaques de l'Active Directory emblématiques au moyen de leurres (honeytoken). Le but : permettre à toute organisation de tester simplement l'apport de la Deceptive Cyber, du déploiement à la remédiation, au service d'une ressource essentielle de tout système d'information.

Mots clés :
Active Directory, honeytoken, leurres, deceptive cyber, détection