

Innovation en Cybersécurité : Détection Avancée des Kits d'Hameçonnage

Contexte et solution existante

Dans le cadre de son service Advanced DNS Security, Belnet déploie la solution Secure DNS développée par Secutec. Cette technologie sophistiquée surveille et analyse en permanence les domaines Internet, créant une barrière protectrice contre les sites malveillants susceptibles de compromettre l'intégrité des réseaux et la confidentialité des données des utilisateurs.

Vision et objectifs de l'extension

L'évolution du service s'articule autour d'une collaboration stratégique avec le Centre pour la cybersécurité Belgique (CCB), visant à renforcer significativement la protection des services publics. Cette nouvelle fonctionnalité permet notamment une détection ultrarapide des liens malveillants dans les communications électroniques entrantes, répondant ainsi à un enjeu crucial de sécurité.

Face aux 25 000 courriels quotidiens reçus par le CCB, le système déploie une analyse automatisée sophistiquée, capable d'identifier instantanément la présence de kits d'hameçonnage dans les liens et sites web signalés. Cette détection précoce s'avère particulièrement critique face aux cybercriminels qui exploitent ces kits pour orchestrer des campagnes massives de phishing, diffusant simultanément des milliers de messages frauduleux.

Architecture de l'extension

L'extension repose sur une synergie tripartite entre Secutec, le CCB et la police judiciaire, établissant un écosystème collaboratif d'échange d'informations et d'expertise. Cette collaboration se matérialise à travers quatre axes principaux :

1. Partage proactif par Secutec de son expertise sur l'évolution des schémas d'attaque et des kits d'hameçonnage identifiés.
2. Maintenance continue du système de détection, enrichi par l'intelligence collective des trois partenaires, avec mise à disposition du code source aux autorités.
3. Déploiement d'une infrastructure dédiée via un service web, permettant au CCB et à la Police Judiciaire d'accéder aux ressources de détection de Secutec.
4. Intégration dynamique des menaces détectées dans la solution Advanced DNS Security de Belnet, renforçant ainsi la protection de l'ensemble des utilisateurs du réseau.

Cette approche intégrée permet une réponse plus efficace et coordonnée face aux cyber-menaces émergentes.