AYI NEDJIMI Consultants

DNSTunnelDetector : détection temps réel des DNS et C2

10 mai 2026 • Mis à jour le 17 mai 2026 • 12 min de lecture • 2038 mots •

DNSTunnelDetector identifie en temps réel les tunnels DNS Iodine, dnscat2 beacons C2 type Cobalt Strike via analyse passive.

DNSTunnelDetector est un détecteur Python open source publié sur le portfolio Nedjimi. Il analyse passivement les flux DNS, qu'ils proviennent d'un capteur Zeek pcap, d'un journal Suricata ou d'un export Cloudflare Resolver, afin d'identifier en tunnels DNS et les beacons command and control qui réutilisent ce protocole. L'ou plusieurs heuristiques statistiques : entropie de Shannon sur les labels, longueur d subdomain, fréquence d'interrogation, ratio de requêtes TXT et NULL, dispersion sait reconnaître les patrons de Iodine, dnscat2, DNSCat-Powershell, Cobalt Strike DNS, NimDNScat et plusieurs implants APT documentés par MITRE. Les alertes pr normalisées en ECS et ingérables dans n'importe quel SIEM. L'objectif est de fourn analystes SOC un compagnon spécialisé pour une m et coûteus

À RETENIR

Points clés

DNSTunnelDetector détecte Iodine, dnscat2, Cobalt Strike DNS beacon et t
APT par analyse passive multi-features.

Entrées supportées : pcap, Zeek dns.log, Suricata EVE, Resolver query log
Cloudflare, Pi-hole et Unbound.

Heuristiques basées sur entropie de Shannon, longueur de subdomain, dis
des types de requêtes et beaconing temporel.

Sortie ECS prête pour Elastic Security, Wazuh, Splunk et Microsoft Sentinel

Pourquoi un détecteur dédié au tunneling DNS

Le DNS est le protocole le plus difficile à inspecter du SI moderne. Il est ouvert sur
tous les périmètres, son débit est généralement non limité et son contenu reste op
pare-feu classiques. Les attaquants l'utilisent depuis vingt ans pour exfiltrer des d
maintenir un canal de commande furtif. Les outils Iodine et dnscat2, devenus stan
offensifs, sont désormais accompagnés de modules natifs dans Cobalt Strike, dan
dans plusieurs implants d'APT documentés par les agences nationales.

Les solutions DNS Security commerciales fournissent une partie de la réponse ma
s'appuient majoritairement sur des listes de domaines connus malveillants, ce qui
aveugles aux campagnes neuves. DNSTunnelDetector adopte au contraire une ap
comportementale : il n'a pas besoin de connaître le d prendre qu'

Réponse sous 24h

Devis gratuit →