République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Centre De Recherche Sur L'information
Scientifique Et Technique

Mémoire de Projet de Fin D'études

Pour l'Obtention du Diplôme de Post Graduation

Spécialisé en Informatique

Option : Sécurité Informatique

Thème :

ANALYSE DES DONNÉES DARKNET POUR LE MONITORING DES CYBER ATTAQUES

Réalisé par :

Mr. DAHOU Mohamed
Mr. BOUKHATEM Abdelatif

Soutenu devant le jury composé de :

Président :	- Mr Boucenna Fateh	CERIST
Examinateurs :	- Mme Guemaraoui Lila	CERIST
	- Melle Zemmache Amina	CERIST
Encadreur :	- Melle Zeghache Linda	CERIST

Promotion 2018/2019

TABLE DES MATIERES

Résumé

Les Darknets, appelés aussi télescopes réseaux, sont un bloque contigu d'adresses IP publiques routables et non allouées. Ce terme est utilisé aussi pour décrire les systèmes de surveillance qui capturent le trafic réseau destiné à ces adresses en mode passif sans interaction avec la source de trafic.

Comme ces adresses IP ne sont pas utilisées, elles ne sont pas censées recevoir du trafic. Par conséquent, tout trafic observé à destination de ces hôtes soulève des soupçons et nécessite une investigation.

Plusieurs études confirment que les cybermenaces peuvent être observées à travers le monitoring du darknet. Il permet de collecter des informations et d'extraire des renseignements sur les cybermenaces sans interaction avec les attaquants.

Dans le cadre de ce travail, nous avons analysé des données collectées par un darknet déployé au niveau du CERIST sur 33 adresses IP non utilisées.
Pour le traitement des données Darknet nous avons utilisé un logiciel open source appelé la pile ELK (pile logicielle composée de **E**lastisearch, **L**ogstash et **K**ibana, nommée aussi **The Elastic Stack**). Cette suite open source permet de collecter des données à partir de différentes **sources serveur** (et cela dans n'importe quel format). Nous avons préparé les données et les avons ingéré et indexé dans elasticsearch à l'aide de Logstash. Ensuite nous avons utilisé Kibana pour créer différents types de visualisations (histogrammes, graphiques, diagrammes circulaires, etc.) pour chaque donnée. Dans le tableau de bord, les différentes visualisations interactives peuvent être combinées pour former une image globale dynamique du trafic réseau.
Cette étude nous a permis de comprendre la nature du trafic darknet pour pouvoir l'exploiter dans des analyser plus approfondies basées sur des techniques statistiques ou d'apprentissage automatique afin de prédire les futures attaques.