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

Présenté en vue de l'obtention du diplôme de poste graduation spécialisé
Informatique

Option : Big Data et calcule intensif

Thème :

Le Monitoring Des Cyber-Attaques Basé Sur Le Darknet En Utilisant Les Technologies Big Data

Réalisé par :

NAFAA Mohammed Sabri

RHASKALI Abdennacer

Soutenu devant le jury composé de :

Président : - Mr Belazzougui Djamel	CERIST
Examinatrice : - Mme Guemraoui Lila	CERIST
Encadreur : - Mme NOUALI-TABOUDJEMAT Nadia	CERIST
- Melle ZEGHACHE Linda	CERIST

2018-2019

BIBLIOTHEQUE DU CERIST

Remerciements

Tout d'abord nous remercions le bon Dieu de nous avoir donné la force et la volonté de débuter et de terminer ce modeste travail, tout en espérant qu'il soit bon et acceptable.

Mes remerciements les plus distingués vont, en premier lieu, à mon encadreur Dr.NOUALI-TABOUDJEMAT Nadia et Co-encadreur Dr.ZEGHACHE Linda pour sleur disponibilité et leur encouragement tout au long de la réalisation de ce mémoire.

Mes remerciements s'adressent également aux membres du jury qui m'ont fait l'honneur d'accepter d'évaluer ce travail.

Je remercie également toute personne ayant contribué de près ou de loin à l'élaboration de ce travail de recherche. Je tiens à remercier le personnel pédagogique et administratif du CERIST, pour leur aide précieuse et leur large disponibilité.

BIBLIOTHEQUE DU CERIST

Dédicace

Tous ceux et toutes celles qui nous ont soutenue tout au long de la préparation de ce travail et qui nous ont encouragé à le poursuivre et à l'achever, méritent dédicace de ce mémoire.

Je le dédié à :

Mes très chers parents : pour leur amour, soutien et énormes sacrifices.

A mon épouse pour son soutien et encouragement

A mes adorables fils Mohamed Nassim et Abd Errahmen

A mes chers frères et sœurs

A toute la famille et les amies qui m'ont moralement soutenu le long de ce travail de recherche.

BIBLIOTHEQUE DU CERIST

Résumé

Traditionnellement, les technologies et les outils utilisés pour le contrecarrer les cyber-menaces ont été plus réactifs que proactifs. Les cyber-menaces sont devenues de plus en plus complexes et difficiles à contrer. Cela a conduit les entreprises à revoir et à renouveler les moyens et les pratiques de la cyber-sécurité classique en adaptant de nouvelles technologies pour passer d'un système réactif à un système de proactif afin d'améliorer la sécurité.

Dans cette optique, nous nous sommes intéressés aux télescopes réseaux communément appelé Darknets, qui sont des systèmes de monitoring à base de piège permettant d'extraire des renseignements sur les cyber-menaces. Une analyse complexe sur Les données Darknet permet de révéler des prémisses d'attaques et d'assurer en plus de la détection la prévention contre les cyber-menaces.

Afin d'analyser les données Darknet plus rapidement et en temps quasi réel nous avons intégré les outils Big Data. Les outils analytiques du Big Data offrent la capacité d'analyser différents types de données en provenance de sources diverses et de réagir en temps réel. Ces outils ne permettent pas seulement de rassembler des informations, mais aussi de connecter ces données, et d'établir des corrélations et des connexions. Il est ainsi possible d'augmenter l'efficience et de contrecarrer plus facilement les cyber-attaques.

Dans notre travail nous avons analysé des données collectées par le Darknet du CERIST sous forme de fichiers Pcap, et les avons intégrés sur dans une plateforme Big Data. Nous avons défini un pipeline composé de plusieurs étapes de traitements utilisant chacune un outil Big Data adéquat afin de préparer les données à l'analyse et la visualisation.

Enfin, nous avons effectués des analyses et généré des aperçus en utilisation Elasticsearch pour l'indexation et Kibana comme tableau de bord pour la visualisation.

Mots clés : Big Data, Spark, Darknet, ELK, cyber-Attaques.

BIBLIOTHEQUE DU CERIST

ملخص

كانت التقنيات والأدوات التقليدية المستخدمة لإحباط التهديدات الإلكترونية أكثر تفاعلية من كونها استباقية، لكن التهديدات السيبرانية أضحت معقدة بشكل متزايد ويصعب مواجهتها مما دفع بالشركات لمراجعة وتجديد وسائل وممارسات الأمن السيبراني القديمة من خلال تكييف تقنيات جديدة للانتقال إلى نظام استباقي.

و للغرض السالف الذكر، وضعنا كل الاهتمام على تلسكوبات الشبكة المعروفة باسم Darknets ، وهي أنظمة مراقبة تعتمد أساسا على فخ لتمكيننا من استخراج معلومات حول التهديدات السيبرانية. إن التحليل المعقد لبيانات Darknet يمكننا من معرفة مصدر الهجمات، بالإضافة إلى التأكد و الكشف وتفادي التهديدات الإلكترونية.

قصد تحليل بيانات Darknet بشكل أسرع وفي الوقت الفعلي تقريبًا، قمنا بدمج أدوات البيانات الضخمة من أجل توفير القدرة على تحليل أنواع مختلفة من البيانات من مصادر مختلفة، والتفاعل في الوقت الفعلي. كما أنها لا تقوم بجمع المعلومات معًا فحسب، بل تعمل أيضًا على توصيل تلك البيانات وإنشاء الارتباطات والوصلات، مما يمكن زيادة الكفاءة ومنع الهجمات الإلكترونية بسهولة أكبر.

في عملنا هذا، قمنا بتحليل البيانات التي تم جمعها بواسطة Darknet الخاص ب CERIST في شكل ملفات Pcap ، ودمجناها في أرضية البيانات الضخمة، أين حددنا مخطط يتكون من عدة خطوات معالجة، كل منها يستخدم أداة مناسبة لإعداد البيانات لمرحلتي التحليل والتصور.

أخيرًا ، أجرينا التحليل وتوصلنا إلى رؤى باستخدام Elasticsearch للفهرسة و Kibana كلوحة تحكم للتصور.

الكلمات المفتاحية : Big Data، Spark، Darknet، ELK، cyber-Attacks.

BIBLIOTHEQUE DU CERIST

Summary

The traditional technologies and tools used to thwart electronic threats have been more reactive than proactive, but cyber threats are becoming increasingly complex and difficult to confront, prompting companies to review and renew old cybersecurity tools and practices by adapting new technologies to transition to a proactive system.

For the aforementioned purpose, we have put all our attention on network telescopes known as Darknets, which are surveillance systems that rely mainly on a trap to enable us to extract information about cyber threats. Darknet's intricate analysis of the data enables us to know the source of the attacks, as well as to confirm, detect and avoid cyber threats.

Intended to analyze Darknet data faster and in near real time, we have integrated big data tools in order to provide the ability to analyze different types of data from different sources, and interact in real time. Not only does it bring information together, but it also delivers that data and creates connections and connections, which can increase efficiency and prevent cyber attacks more easily.

In our work, we analyzed the data collected by CERIST's Darknet in the form of Pcap files, and integrated them into the Big Data floor, where we identified a chart consisting of several processing steps, each of which uses a suitable tool to prepare the data for the analysis and visualization stages.

Finally, we ran the analysis and came up with insights using Elasticsearch for indexing and Kibana as a dashboard for visualization.

Keywords : Big Data, Spark, Darknet, ELK, cyber-Attacks.

BIBLIOTHEQUE DU CERIST

Sommaire:

BIBLIOTHEQUE DU CERIST

Chapitre 2 : Big Data ; outils et qualités

BIBLIOTHEQUE DU CERIST

Chapitre 3 : Conception

BIBLIOTHEQUE DU CERIST

Chapitre 4 : Implémentation

BIBLIOTHEQUE DU CERIST

BIBLIOTHEQUE DU CERIST

Liste des figures

BIBLIOTHEQUE DU CERIST

Liste des tableaux

BIBLIOTHEQUE DU CERIST