IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Détection de malware par approche statistique

Groupe

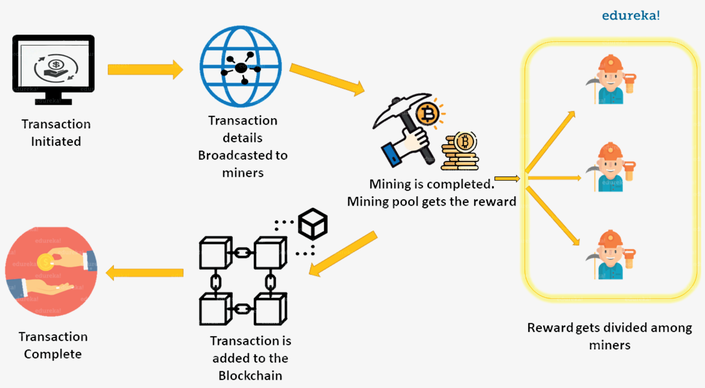
Albert Dulout
Elias Bey Boumezrag
Marc Serre
Tianrun Zhang

Tuteur

Françoise Sailhan

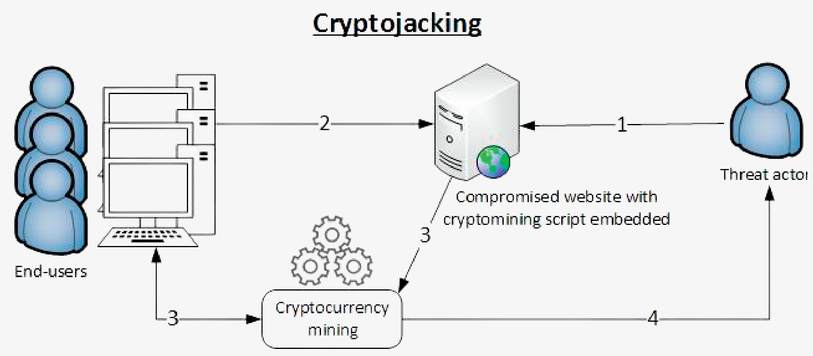
Contexte de l'étude et objectifs

Le cryptojacking est le minage de cryptomonnaies
grâce à l'installation de logiciels malveillants
sur l'ordinateur de la personne cible.
Le profit du minage va alors au pirate.



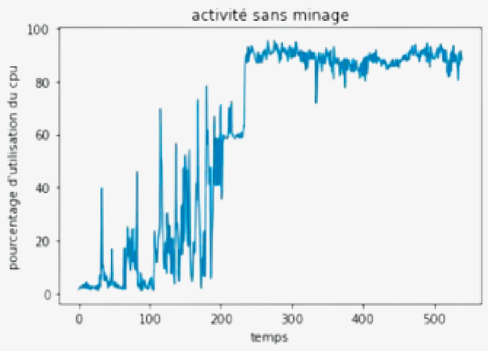
Le but est de pouvoir détecter une activité anormale sur un appareil victime de cryptojaking par :

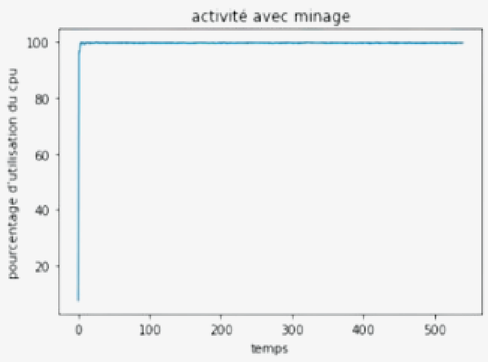
- l'analyse de la variation de l'activité du CPU,
- l'étude des paquets réseau.



Méthodes de reconnaissance de cryptojacking

1 Analyse de l'activité CPU





Si dépasse un seuil

2 Sniff de l'activité réseau (Scapy)

Adresses IP de la source et du destinataire
Direction du trafic
Longueur des paquets

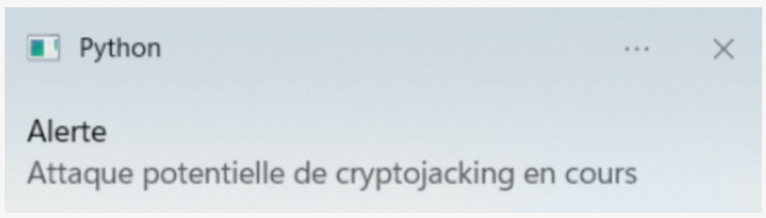
3 Feature Engineering (pandas)

Ecart temporel entre les paquets
Moyenne et Écart-type mobile de cet écart et de la longueur des paquets

4 Classification (XGBoost)

Si dépasse un seuil

5 Alerte de l'utilisateur



Sur les données test, on a un recall de 0.96

Conclusion

Nous avons proposé un outil permettant à un utilisateur de détecter la présence d'un malware de cryptojacking grâce à une approche de Machine Learning

Perspectives

- Améliorer les données d'entrainement du modèle en minant d'autres cryptomonnaies.
- Essayer des méthodes de détection d'anomalies non supervisées.