Cryptojacking

mateo fernandez-bede

July 2024

1 Introduction et problématique

Le cryptojacking est une menace de cybersécurité de plus en plus répandue. Elle consiste à utiliser les ressources informatiques d'une machine informatique à son insu pour miner des cryptomonnaies. Le minage peut être effectué sur tout types de machines qui ont une puissance de calcul. Cette pratique malveillante peut entraîner des ralentissements significatifs des systèmes affectés, une augmentation de la consommation d'énergie et une usure prématurée du matériel informatique. Les organisations et les particuliers doivent donc être conscients des méthodes de détection et de prévention du cryptojacking pour protéger leurs ressources numériques et maintenir la performance optimale de leurs systèmes.

Quels sont les indicateurs clés de performance (KPI) à surveiller pour détecter efficacement les attaques de cryptojacking dans un système informatique ?

2 Revue de littérature

1. Détection des menaces cryptojacking sur le Web : une approche avec des autooencodeurs et des réseaux neuronaux denses profonds

Cet article explore les défis de la détection du cryptojacking et propose une approche basée sur les auto encodeurs et les réseaux neuronaux denses profonds. L'approche proposée est évaluée sur un ensemble de données de trafic Web réel et montre des résultats prometteurs, avec une précision de détection élevée et un faible taux de faux positifs.

Lien: https://www.mdpi.com/2076-3417/12/7/3234

2. Le cryptojacking : une menace émergente pour la cybersécurité

Cet article offre un aperçu complet du cryptojacking, y compris ses définitions,

ses types, ses méthodes d'attaque et ses impacts. Il discute également des contre-mesures contre le cryptojacking, telles que la sensibilisation des utilisateurs, les logiciels de sécurité et les réglementations.

Lien: https://www.mdpi.com/2076-3417/12/7/3234

3. Cryptojacking : analyse des techniques, des attaques et des contre mesures

Cet article fournit une analyse approfondie des techniques de cryptojacking, des attaques courantes et des contre-mesures efficaces. Il discute également des implications juridiques et éthiques du cryptojacking.

Lien: https://ieeexplore.ieee.org/document/9581251

4. Impact du cryptojacking sur les performances des systèmes et les contre mesures potentielles

Cet article évalue l'impact du cryptojacking sur les performances des systèmes, y compris les ralentissements, les surchauffes et les augmentations de la consommation d'énergie. Il explore également des contremesures potentielles pour atténuer l'impact du cryptojacking sur les systèmes.

Lien: https://ieeexplore.ieee.org/document/9306696

5. Un système de détection de cryptojacking basé sur l'apprentissage automatique pour les réseaux mobiles

Cet article propose un système de détection de cryptojacking basé sur l'apprentissage automatique pour les réseaux mobiles. Le système proposé est évalué sur un ensemble de données de trafic réseau mobile réel et montre des résultats prometteurs, avec une précision de détection élevée.

Lien: https://ieeexplore.ieee.org/document/9800057

6. Cryptojacking : une menace évolutive pour la cybersécurité des appareils mobiles

Cet article examine la menace croissante du cryptojacking sur les appareils mobiles. Il discute des techniques de cryptojacking mobiles, des contre mesures et des défis futurs.

Lien: https://ieeexplore.ieee.org/document/9581251

7. Le cryptojacking sur le Web : tendances, défis et contremesures

Cet article offre un aperçu du cryptojacking Web, y compris ses tendances, ses défis et ses contre-mesures. Il discute des méthodes de monétisation du cryptojacking Web et des implications pour la sécurité des utilisateurs.

Lien: https://www.mdpi.com/2076-3417/12/7/3234

8. Vers un système de détection de cryptojacking en temps réel basé sur le réseau

Cet article propose un système de détection de cryptojacking en temps réel basé sur le réseau. Le système proposé utilise l'analyse du trafic réseau pour identifier les activités de cryptojacking.

Lien: https://ieeexplore.ieee.org/document/9117732

9. Un système de détection de cryptojacking basé sur l'analyse comportementale pour les navigateurs Web

Cet article développe un système de détection de cryptojacking basé sur l'analyse comportementale pour les navigateurs Web. Le système proposé identifie les activités de cryptojacking en analysant le comportement des scripts JavaScript.

Lien: https://ieeexplore.ieee.org/document/9117732

10. Analyse des techniques de cryptojacking et de leurs impacts sur les performances des systèmes cloud

Cet article explore les techniques de cryptojacking et leurs impacts sur les performances des systèmes cloud. Les auteurs analysent différentes techniques de cryptojacking et évaluent leur impact sur les performances des ressources cloud telles que le CPU, la mémoire et la bande passante réseau. L'étude montre que le cryptojacking peut avoir un impact significatif sur les performances des systèmes cloud, entraînant des ralentissements, des surchauffes et des augmentations de la consommation d'énergie.

Lien: https://ieeexplore.ieee.org/document/9306696

3 Expériences

Au cours de ces derniers mois, j'ai pu réaliser des expériences qui m'ont permis de mieux comprendre l'attaque cryptojacking. Grâce aux travaux précédents de mon collègue, il m'a été facile de mettre en place le minage sur ma machine. L'ordinateur utilisé pour ces expériences est un PC portable avec 8 GB de RAM et un Intel core I5 10210U 4 coeurs 8 threads 4,20 GHz de fréquence turbo. Le système d'exploitation utilisé est Ubuntu 22.04. Le nombre de threads peut faire changer les résultats dans certains cas. Dans le cas du Monéro qui utilise l'algorithme RandomX, il optimise le minage et utilise le multi-threading pour augmenter les capacités de minage ce qui fait augmenter le taux de H/s (hash rate per second). On appelle ça la parallélisation du calcul. C'est une utilisation intelligente des threads pour se concentrer sur le plus de processus à la fois. J'ai testé le minage de cinq cryptomonnaies pour obtenir des résultats variés : Monero, Versus Coin, Raven Coin, NIMIQ et Dogecoin. Il faut savoir que les algorithmes de minage sont différents. Plus l'algorithme est difficile, plus le hashrate sera bas. Plus l'algorithme est facile, plus le hashrate sera élevé. La complexité d'un algorithme a un impact sur le prix d'une cryptomonnaie. En général, plus l'algorithme est facile, plus le prix est faible. En revanche, plus l'algorithme est difficile, plus le prix sera élevé. Durant les expériences, j'ai récupéré plusieurs données :

- La fréquence au repos du processeur en GHz (quand celui ci n'effectue quasiment aucune tâche)
- La fréquence en utilisation du processeur en GHz (quand celui ci mine)
- L'utilisation de la mémoire RAM lors du minage en GB
- La consommation en Watts du PC durant le minage
- Le Hashrate en kh/s (kilohash per second)
- Le coût de chaque coin

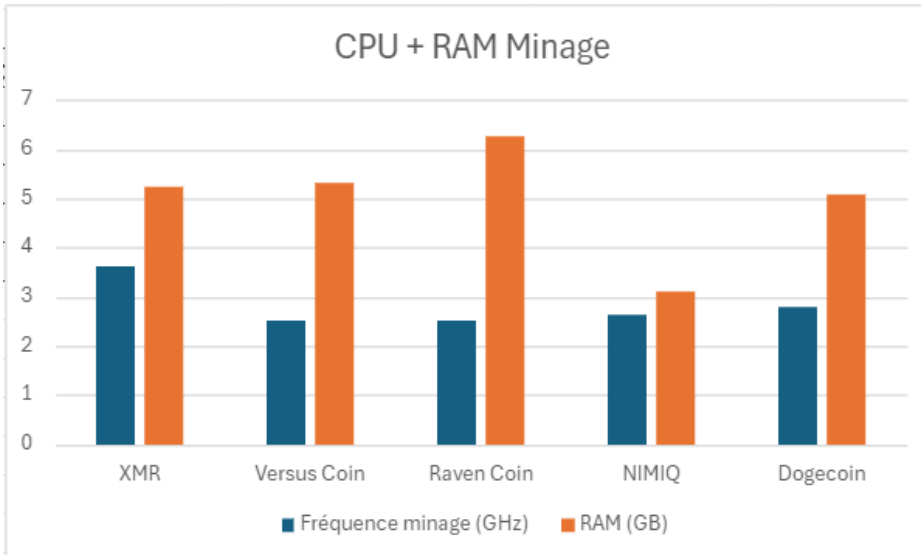
4 Résultats et Discussion des résultats

	Fréquence repos (GHz)	Fréquence minage (GHz)	RAM (GB)	Consomation (W)	Hash rate (Kh/s)	Cout ($CAD) 17/06:2024
XMR	1,1	3,63	5,26	33,9	1,1	240,51
Versus Coin	1,1	2,5	5,33	12,9	4600	1,73
Raven Coin	1,1	2,5	6,26	23	1	0.03003
NIMIQ	1,1	2,65	3,1	18	2	0.002202
Dogecoin	1,1	2,8	5,1	23,5	1,5	0.1834

Ci-dessus, le tableau démontrant mes récoltes de données sur le minage. On y retrouve La fréquence du CPU durant le minage et la fréquence en fonctionnement normal (1 fenêtre mozilla firefox et une fenêtre CMD ouverte), La RAM lors du minage (8GB au total), la consommation en Watts lors du minage (il faut prendre en compte que c'est un PC portable et que la consommation n'est pas en Watt/heure), le hashrate de chaque minage.

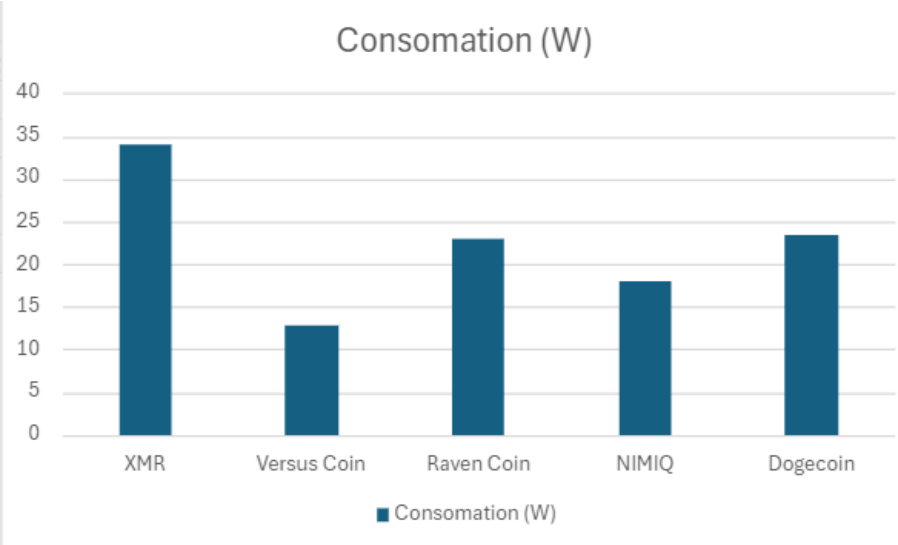
En suivant nous verrons plusieurs graphiques qui vont aider à comprendre les différentes données.

Ci-dessous le graphique de comparaison du CPU en fréquence de minage et la RAM.



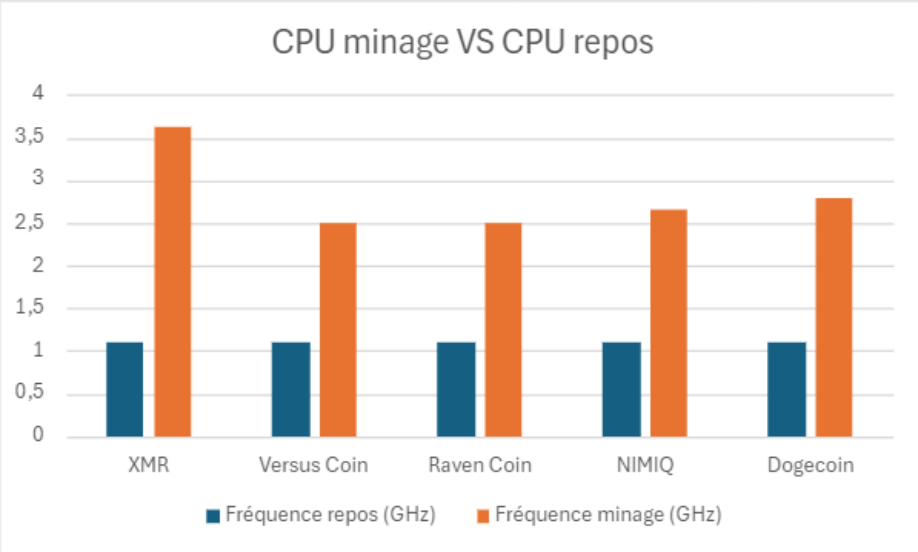
On remarque que l'utilisation de la RAM est différente selon les monnaies et que la fréquence du CPU varie mais de façon moins significative en fonction des coins. Le versus coin qui a le hashrate le plus élevé, a la fréquence CPU la moins élevée et la consommation électrique la moins élevée (voir le graphique ci-dessous). Cela démontre que le hashrate ne dépend pas que des performances de la machine, je pense que dans ce cas, l'algorithme utilisé est le moins complexe de tous.

Ci-dessous le graphique de comparaison de consommation entre les différents coins.

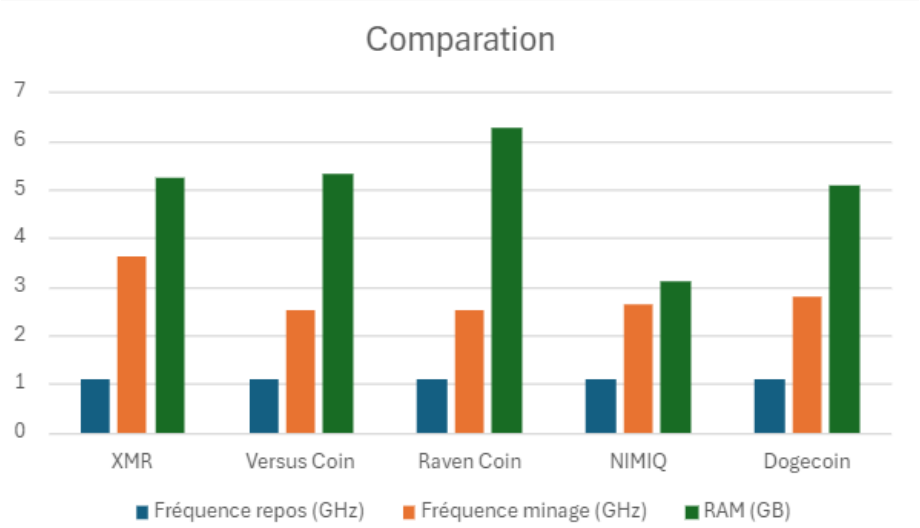


Comme je l'explique avec le graphique suivant, il est important de prendre les métriques quand le système d'information est en usage normal ou intensif pour pouvoir mesurer et déduire les menaces. Ici on voit que certaines monnaies peuvent être plus "furtives" que d'autres.

Ci dessous, le graphique qui compare la fréquence de minage au repos en en cours de minage.



Ce graphique nous montre la différence d'état du processeur quand il est en fonctionnement normal et quand il mine.



Ce dernier graphique montre la situation globale de la machine sur toutes les monnaies. On observe les données du hardware et on voit l'utilisation des ressources en minage et au repos sur toutes les monnaies. L'attaquant peut miner de façon plus furtive en utilisant le NIMIQ mais il y aura toujours une différence importante entre l'état minage et l'état repos du Système d'information

Quand le Système d'Information est en cours de fonctionnement et non infecté, il faut prendre les métriques de "base". RAM, CPU, consommation électrique, bande passante. On voit une augmentation globale importante de tout les composants de calculs. Cela pourrait nous alarmer sur l'état du SI et engager des procédures de détection et de réponse d'incident.

5 Analyse réseau

Durant le minage, j'ai pus observer plusieurs types de protocoles : TCP et TLSV1.2

TLSV1.2 :

- Handshake: TLSv1.2 commence par un processus de Handshake, où le client, le logiciel de minage (xmrig) et le serveur (le serveur du pool de minage)

négocient les paramètres de chiffrement et établissent une connexion sécurisée.

- Key Exchange: Pendant le handshake, le client et le serveur échangent des clés cryptographiques qui seront utilisées pour chiffrer et déchiffrer les données échangées entre eux.

- Data Transfer: Une fois la connexion sécurisée établie, le logiciel de minage commencera à transférer les données de l'application vers le serveur du pool de minage. Ces données comprennent des informations sur le travail effectué par votre plateforme de minage, telles que les hachages calculés pour miner un bloc.

- Encryption: Toutes les données transférées entre votre logiciel de minage et le serveur sont chiffrées à l'aide des clés établies pendant Handshake. Cela garantit que les données restent confidentielles et ne peuvent pas être interceptées ou altérées par des acteurs malveillants.

TCP :

- Connexion établie : Avant que le client de minage puisse envoyer des données au serveur du pool de minage, une connexion TCP $\longleftrightarrow$ deux parties. Cela se fait via un processus appelé Handshake TCP, où le client et le serveur échangent des informations pour établir et synchroniser la connexion.

-Transfert de données fiable : Une fois la connexion établie, TCP assure un transfert fiable des données entre le client et le serveur. Données envoyées par le client sont garanties d'arriver à destination dans l'ordre correct, sans perte ni altération, et que le serveur peut confirmer la réception des données.

Reprise sur incident : En cas de perte de connexion ou d'erreur de transmission, le TCP prend en charge la reprise sur incident en rétablissant la connexion et en reprenant la transmission là où elle s'était arrêtée. Cela garantit une communication fiable même dans des conditions réseau moins que parfaites.

6 Tableau wireshark

Tout d'abord, voici certains mots clé pour comprendre les abréviations :
UDP : User Datagram Protocol
ICMP : Internet Control Message Protocol
NTP : Network Time Protocol
DHCP : Dynamic Host Configuration Protocol
DNS : Domain Name System
TCP : Transmission Control Protocol
TLS : Transport Layer Security
HTTP : Hypertxt Transfert Protocol
OCSSP : Online Certificate Status Protocol
IGMP : Internet Group Management Protocol
ARP : Address Resolution Protocol

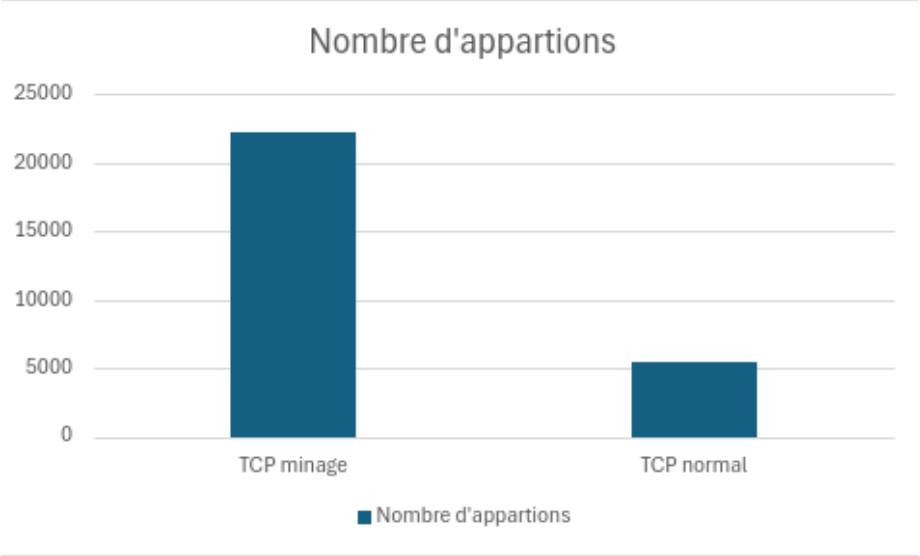
j'ai pu approfondir l'analyse réseau durant le minage grâce à Wireshark. Comprendre le trafic réseau du Système d'information est vital pour comprendre et pour découvrir une attaque. Comme je l'ai expliqué plus tôt, les protocoles de TCP et de TLS peuvent se démarquer au cours de l'attaque. Ci-dessous, un tableau comparatif des paquets capturés lors du minage et lors d'un usage sans le minage :

	Durant le minage			Sans le minage	
IPV6	Protocole	Nombre d'appartions		Protocole	Nombre d'appartions
	UDP	349		UDP	284
	ICMPv6	2		ICMPv6	12
	Multicast DNS	349		Multicast DNS	284
	TOTAL IPv6	700		**TOTAL IPv6**	580
IPV4	UDP	22953		UDP	3523
	NTP	14		NTP	6
	NetBIOS NS	74		NetBIOS NS	23
	Multicast DNS	369		Multicast DNS	378
	DHCP	11		DHCP	13
	DNS	772		DNS	778
	Data	1410		Data	2325
	TCP	22231		TCP	5405
	TLS	7205		TLS	2162
	Malformed Packet	8		Malformed Pack	1
	HTTP	43		HTTP	43
	OCSSP	18		OCSSP	2
	Data	215		Text Data	6
	IGMP	115		IGMP	161
	ICMP	7		ICMP	9
	ARP	673		ARP	328
	TOTAL IPV4	56118		802.1X Authenti	13
				TOTAL IPV4	15176

En général, je remarque que les données sont similaires. Le nombre d'apparition n'est pas mathématique, il dépend du trafic en temps réel du réseau. C'est pour ça que pour relever les facteurs importants, il faut observer les variation implorantes dans le trafic du réseau. A noter que les deux captures réalisées sur Wireshark ont été effectuées durant 1h à la même heure de la journée sur 2 journées différentes. Les conditions du test sont les mêmes pour les 2 tests.

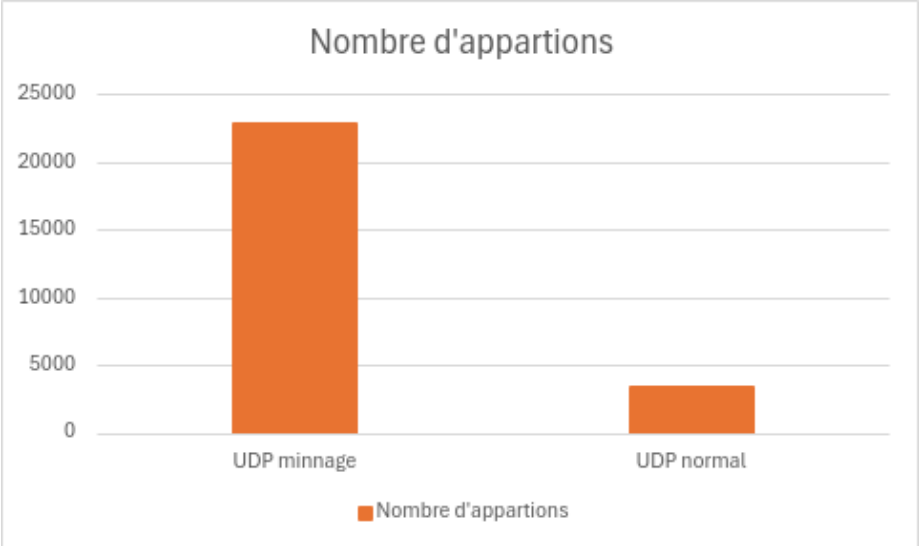
Les graphiques suivants sont des comparaisons entre le trafic normal et durant le minage. Tous les protocoles ne seront pas affichés. Seuls ceux qui présentent un écart très imporant entre les deux états.

Ci-dessous un graphique qui montre l'écart sur le protocole TCP :



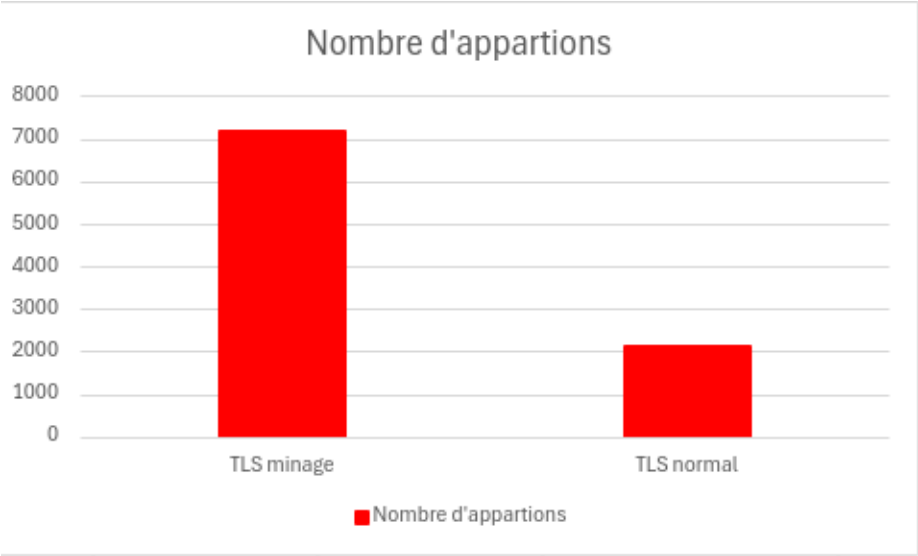
Dans ce graphique, je compare le nombre de paquets TCP capturés durant le minage et durant une utilisation normale. Durant le minage, j'ai capturé 22231 paquets contre 5405 paquets sur une utilisation normale. C'est 4,11 fois inférieur que durant le minage. On peut donc supposer que c'est un bon indicateur à surveiller.

Ci-dessous un graphique qui montre l'écart sur le protocole UDP :



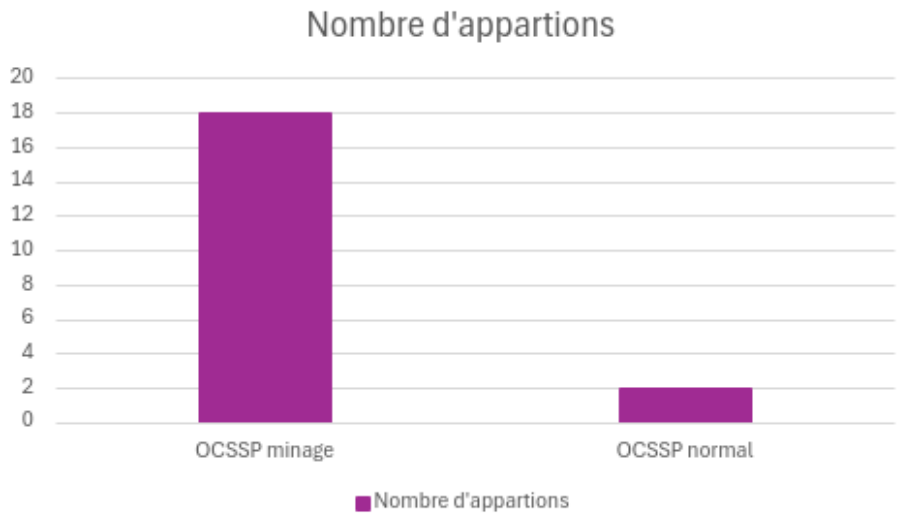
Dans ce graphique, je compare le nombre de paquets UDP capturés durant le minage et durant une utilisation normale. Durant le minage, j'ai capturé 22953 paquets contre 3523 paquets sur une utilisation normale. C'est 6,51 fois inférieur que durant le minage. On peut donc supposer que c'est un bon indicateur à surveiller.

Ci-dessous un graphique qui montre l'écart sur le protocole TLS :



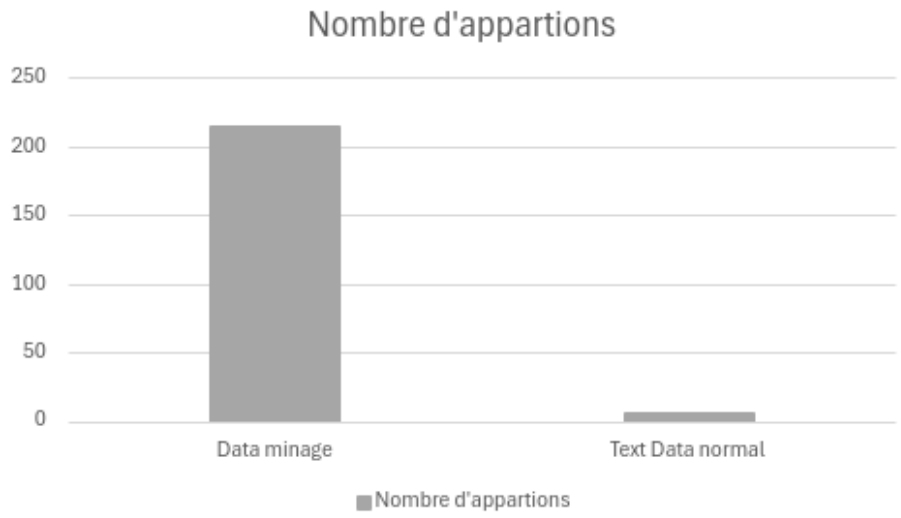
Dans ce graphique, je compare le nombre de paquets TLS capturés durant le minage et durant une utilisation normale. Durant le minage, j'ai capturé 7205 paquets contre 2162 paquets sur une utilisation normale. C'est 3,332 fois inférieur que durant le minage. On peut donc supposer que c'est un bon indicateur à surveiller.

Ci-dessous un graphique qui montre l'écart sur le protocole OCSSP :



Dans ce graphique, je compare le nombre de paquets OCSSP capturés durant le minage et durant une utilisation normale. Durant le minage, j'ai capturé 18 paquets contre 2 paquets sur une utilisation normale. C'est 9 fois inférieur que durant le minage. On peut donc supposer que c'est un bon indicateur à surveiller. Il faut noter que ce protocole n'est pas directement lié au minage. Celui-ci sert à sécuriser la communication entre les membres du pool et le serveur du pool. il vérifie la validité des certificats pour s'assurer que la communication soit sécurisé entre le pool et les membres du pool.

Ci-dessous un graphique qui montre l'écart sur les trames data:



Dans ce graphique, je compare le nombre de paquets des trames data capturés durant le minage et durant une utilisation normale. Durant le minage, j'ai capturé 215 trames contre 6 trames sur une utilisation normale. C'est 35,83 fois inférieur que durant le minage. On peut donc supposer que c'est un bon indicateur à surveiller. Certaines données doivent transiter via le réseau. Elles sont envoyé dans des trames data via TCP. Elles seront sécurisé grâce à TLS.

Pour finir cette partie, je pourrai citer le protocole ARP car il y a environ une différence de facteur 2 entre les 2 états mais dans notre cas, ce protocole n'a rien à voir avec le minage. Le protocole ARP est utilisé sur la couche réseau et il est en place dans les réseaux locaux. Dans notre cas le pool de minage n'est pas dans le réseau local. Cette augmentation d'ARP n'a donc rien à voir avec le minage. Grâce à cet exemple j'ai pus me rendre compte qu'il ne fallait pas seulement se fier aux chiffres mais analyser en réfléchissant et en utilisant des connaissances techniques, comparer et faire des recherches.

7 Detection

Pour renforcer la sécurité de notre infrastructure réseau, nous envisageons d'ajouter des règles de sécurité et des alertes au niveau du DNS, des routeurs, des switchs et des pare-feux. Nous devons toutefois veiller à ne pas bloquer toutes les communications, afin de préserver une bonne expérience utilisateur et garantir la disponibilité des services essentiels.

Afin d'optimiser cette approche, nous proposons l'utilisation de l'intelligence artificielle pour surveiller et analyser divers paramètres du réseau :

Détection des protocoles : Identifier et analyser les protocoles utilisés pour détecter toute activité suspecte ou non autorisée.

Détection des adresses IP et des ports : Surveiller les adresses IP et les ports pour repérer des connexions inhabituelles ou potentiellement dangereuses.

Réduction de la bande passante : Observer et gérer l'utilisation de la bande passante pour éviter les surcharges et garantir une distribution équitable des ressources.

Augmentation anormale de l'utilisation de la RAM ou du CPU : Détecter toute augmentation inhabituelle de l'utilisation de la mémoire RAM ou du processeur, pouvant indiquer une attaque ou une utilisation abusive des ressources.

Augmentation de la consommation d'énergie : Suivre la consommation d'énergie pour identifier des comportements anormaux qui pourraient signaler une attaque ou un dysfonctionnement matériel.

En mettant en place ces mesures, nous pourrons renforcer la sécurité de notre réseau tout en minimisant l'impact sur l'expérience utilisateur et la disponibilité des services essentiels.

8 Conclusion

Le cryptojacking représente une menace sérieuse et croissante pour les systèmes informatiques, affectant à la fois les performances et la durée de vie du matériel. À travers cette étude, nous avons démontré l'importance de surveiller certains indicateurs clés de performance (KPI) pour détecter efficacement cette forme d'attaque.

Les expériences menées ont révélé que le cryptojacking entraîne des augmentations significatives de la fréquence du processeur et de l'utilisation de la mémoire RAM, ainsi qu'une hausse notable de la consommation d'énergie. Ces changements peuvent être utilisés comme signes avant-coureurs pour identifier la présence de cryptojacking. En particulier, les variations de la fréquence du CPU et de la consommation de RAM sont des indicateurs cruciaux.

Les graphiques comparatifs ont illustré l'importance de recueillir des métriques de base en état de repos et en pleine activité pour établir des seuils d'alerte précis. Cette approche permet de distinguer les variations normales des indicateurs de performance des anomalies provoquées par des attaques de cryptojacking.

Pour conclure, la détection proactive du cryptojacking repose sur une surveillance continue et détaillée des performances du système informatique. Les organisations doivent mettre en place des mesures de surveillance robustes et adopter des procédures de réponse rapides pour atténuer les impacts de ces attaques. La combinaison de la surveillance des fréquences CPU, de la consommation de RAM et de la consommation électrique constitue une stratégie efficace pour protéger les ressources informatiques et maintenir une performance optimale.

9 Sources

Pour mesurer les fréquences du CPU et consomation de la machine, j'ai utilisé PowerTop sur Linux Ubuntu. Pour mesurer la RAM j'ai utilisé le logiciel Glances sur Linux Ubuntu

Pour observer les trames réseaux, j'ai utilisé le logiciel wireshark sur Linux Ubuntu.

Les données collectées ont été rassemblé sous forme de tableau sur Excel (voir 4 Résultats et Discussion des résultats). Les tableaux ont été généré sur Excel à partir des données collectées par moi même.