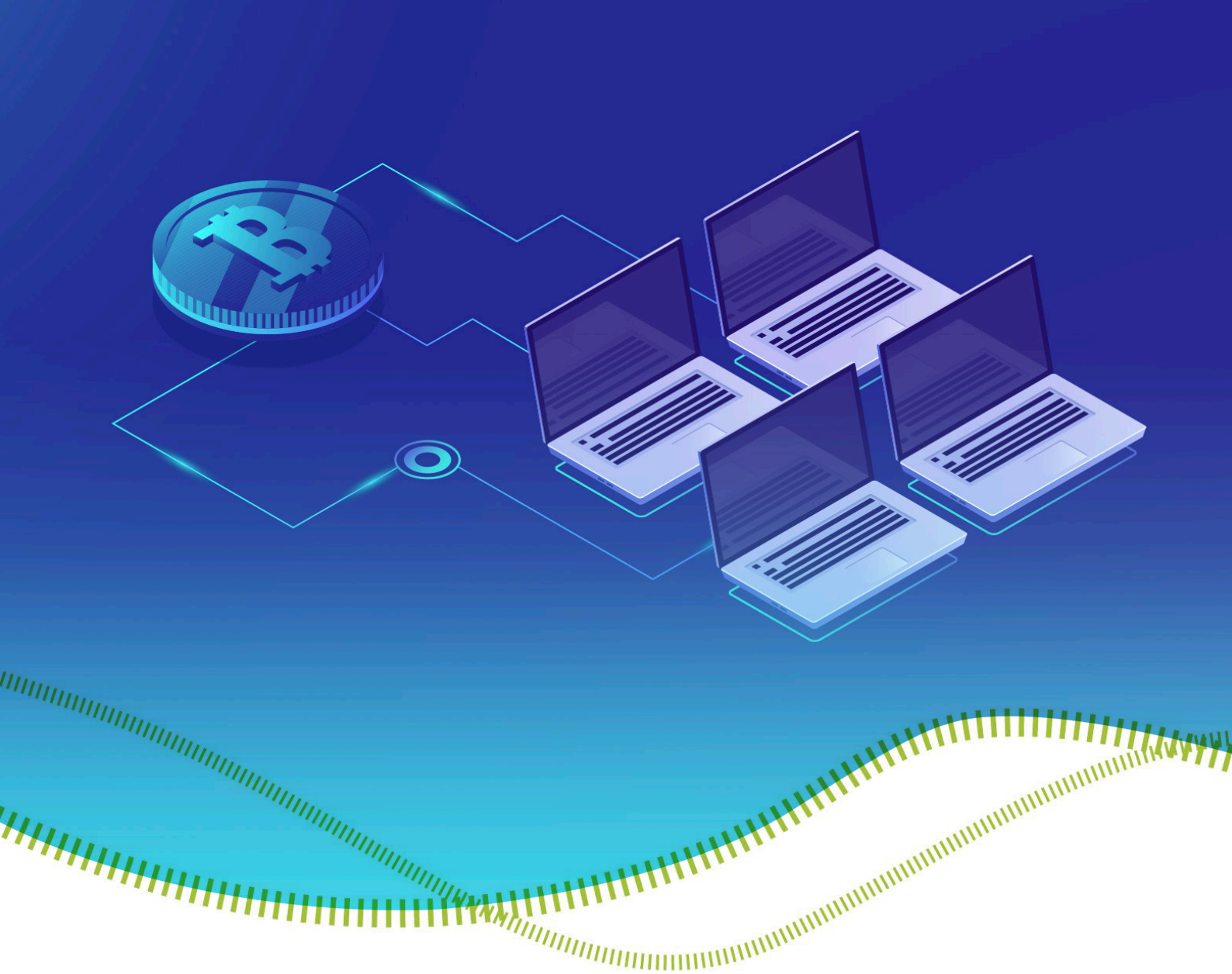


Cryptojacking

Qu'est-ce que c'est ? Pourquoi s'en prémunir ?

CERT.be
The Federal Cyber Emergency Team

The
Federal Cyber
Emergency Team

Table des matières

1 INTRODUCTION

Il y a quelque temps, un nouveau phénomène appelé *cryptojacking* est apparu. CERT.be note une augmentation du nombre d'infections ainsi que de leur complexité. En 2017, le nombre de détections de mineurs de crypto monnaies sur les ordinateurs terminaux a augmenté de 8 500 %. Vu ce taux, CERT.be s'attend à ce que le *cryptojacking* représente une menace plus sérieuse encore que les logiciels de rançon.

L'objectif de ce document est d'aborder le minage de navigateur et le phénomène du *cryptojacking*.

1.1 Que sont les crypto monnaies ?

Les crypto monnaies sont des monnaies virtuelles qui dépendent fortement de la cryptologie pour fonctionner. La crypto monnaie la plus populaire était le Bitcoin et offrait un système de caisse numérique décentralisé, comme alternative au système de caisse classique. Aujourd'hui, il existe quelques centaines de crypto monnaies différentes, mais on utilise le Bitcoin dans ce document comme exemple.

Comme le prix de certaines de ces monnaies cryptographiques augmente rapidement, le minage de crypto monnaies gagne en popularité.

1.2 Qu'est-ce que le minage ?

Pour générer un Bitcoin et donc gagner de l'argent, un ordinateur doit effectuer de nombreux calculs qui nécessitent une quantité importante de ressources (CPU). Pour ces calculs, l'ordinateur ou le smartphone est récompensé en Bitcoins. Ce processus s'appelle le minage.

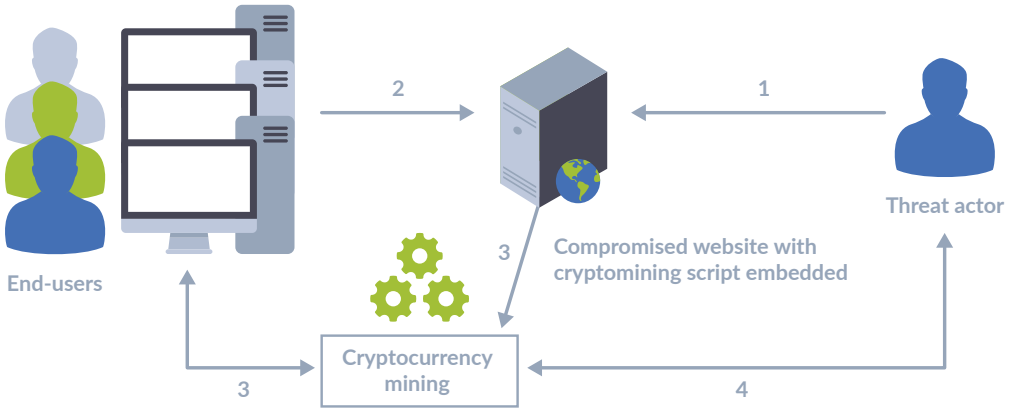
Comme la quantité de calculs nécessaires est vraiment élevée (et augmente périodiquement), la meilleure façon de maximiser les profits est de disposer d'un grand nombre d'appareils capables d'effectuer ces calculs (ce qu'on appelle un pool d'appareils).

Parce qu'un plus grand pool engendre de plus grands bénéfices, certains acteurs sur Internet ont commencé à inclure des programmes de minage (appelés scripts) dans leurs sites Web. Cela signifie que les visiteurs du site vont extraire les crypto monnaies pour le compte du propriétaire du site Web. Le processus est masqué, de sorte que l'utilisateur peut ne pas en être conscient.

Si l'utilisateur donne l'autorisation au site de procéder au minage depuis son appareil, c'est considéré comme une compensation pour l'utilisation du site Web et ces services.

Toutefois, le problème se pose lorsque l'utilisateur n'est pas conscient que son navigateur est utilisé pour générer de la crypto monnaie.

Comment fonctionne le cryptojacking



Steps

1. The threat actor compromises a wesbite
2. Users connect to the compromised website ad the cryptomining script executes
3. Users start unknowinlgy mining cryptocurrency on behalf of the threat actor
4. Uppon successfully adding a new block to the blockchain, the threat actor receives a reward in cryptocurrency coins

Source: Enisa

2 QU'EST-CE QUE LE CRYPTOJACKING ?

2.1 Qu'est-ce que le phénomène cryptojacking ?

Si le navigateur de l'utilisateur est utilisé pour miner des crypto monnaies sans le consentement de ce dernier, l'utilisateur est victime de *cryptojacking*.

Pendant que le cryptomineur fonctionne, l'utilisateur remarquera un très haut niveau d'utilisation de la carte graphique et/ou du CPU. Le navigateur utilise 40% ou plus de la puissance de votre ordinateur. Cela signifie que l'ordinateur ou le smartphone fonctionne plus lentement, que la batterie se décharge plus rapidement et que la température de l'appareil augmente tant que le script est en cours d'exécution.

De plus, l'augmentation de la charge de travail de l'appareil entraîne une augmentation de la facture d'électricité.

2.2 Comment le détecter ?

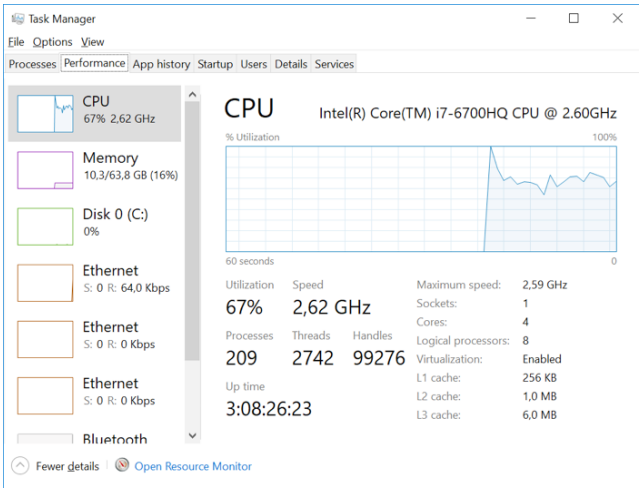
Pour savoir si le navigateur est en train de miner des crypto monnaies, vous pouvez utiliser le gestionnaire de tâches (Windows) ou le moniteur d'activité (Apple) :

2.2.1 Gestionnaire de tâches Windows

1. Ouvrez le gestionnaire de tâches par un clic droit sur la barre de tâches et en sélectionnant « Task manager »
2. Cliquez sur « More details »
3. Dirigez-vous vers la barre des performances pour connaître votre utilisation CPU

2.2.2 Moniteur d'activité Macintosh

1. Appuyez sur « Command+Spacebar » pour afficher le champ de recherche Spotlight.
2. Tapez « Activity Monitor ».
3. Appuyez sur la touche Retour lorsque le moniteur d'activité s'affiche dans les résultats.
4. Vous êtes maintenant dans le moniteur d'activité où vous pouvez gérer et manipuler les tâches.



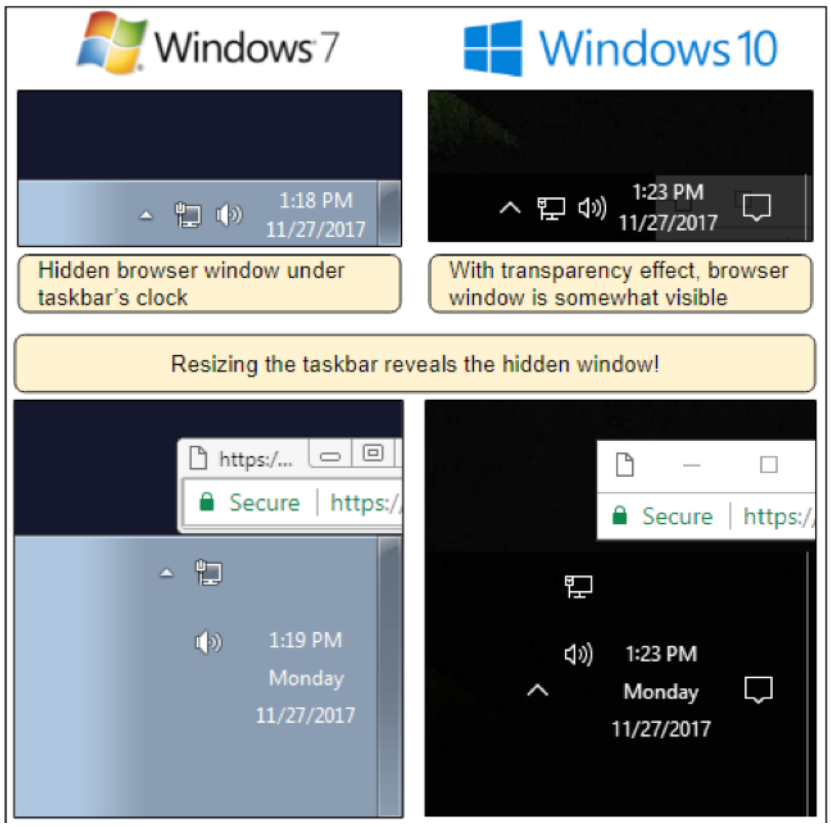
Gestionnaire de tâches avec aperçu de l'utilisation CPU

2.3 Comment fonctionne le cryptojacking ?

Le *cryptojacking* peut prendre diverses formes :

- Le script est directement inclus dans le site web.
- Le script est inclus dans la publicité d'une tierce partie chargée par le site web.
- L'utilisateur a installé un plugin/une extension de navigateur qui injecte le script dans les sites web.
- L'appareil de l'utilisateur a été infecté par des logiciels malveillants qui exécutent des opérations de *cryptomining* en arrière-plan.

Une nouvelle version de cryptomining a récemment été détectée : un site web ouvre une fenêtre pop-up qui est cachée sous la barre des tâches (voir image). Cela signifie que même après avoir quitté la page d'origine, le script de minage continuera à utiliser les ressources. Le script peut ainsi être exécuté plus longtemps, maximisant ainsi les profits du fournisseur de script.



Hidden Window - Copie d'écran de blog.malwaresbytes.com

3 COMMENT SE PRÉMUNIR ?

Heureusement, le risque de *cryptojacking* peut être facilement atténué.

3.1 L'internaute

- Envisagez d'utiliser un bloqueur d'annonces ou un anti-virus car beaucoup d'entre eux empêchent ces scripts de s'exécuter.
- N'installez que des extensions/plugins de navigateur en lesquels vous avez confiance et qui sont distribués par un magasin d'applications fiable (Google Play, Microsoft store, etc.).
- Vérifiez régulièrement les extensions installées et retirez celles qui ne sont plus nécessaires. Plus le nombre d'extensions est élevé, plus le risque est grand que surviennent des comportements malveillants ou des vulnérabilités, alors limitez-les au minimum.
- Désactivez les extensions de navigateur inutiles.
- Si l'ordinateur ou le smartphone est plus lent ou plus chaud, ou si le navigateur Web ne répond pas, redémarrez le navigateur Web.
- Les utilisateurs avancés peuvent désactiver JavaScript par défaut et n'autoriser que les sites Web de confiance à exécuter JavaScript.
- Vérifiez régulièrement si votre navigateur est toujours propre avec des outils comme : https://cryptojackingtest.com
- Informez CERT.be en envoyant un email à cert@cert.be. Vous nous aiderez ainsi à surveiller la cybersécurité en Belgique.
- Puisque vous êtes victime, vous pouvez déposer une plainte à la police local.

3.2 Propriétaire de site

Si vous remarquez des plaintes d'utilisateurs concernant le *cryptomining* ou une plateforme plus lente que d'habitude, assurez-vous de ne pas distribuer des scripts de minage sans le vouloir. De plus ces scripts sont **illégaux en Belgique** sans le consentement de l'utilisateur et la peine maximale est de 5 ans de prison (pour la première infraction).

3.3 Administrateur système

- Bloquez le trafic d'entrée et de sortie vers les ports TCP et UDP 3333, 5555, 7777, 8000 et 14444 à votre point de démarcation, en l'absence d'un objectif commercial avéré.
- Désactivez ou supprimez les logiciels, ports, protocoles et services qui ne sont pas utilisés.
- Une liste noire des noms de domaine est publiée sur : http://iplists.firehol.org/

4 UTILISATION LÉGALE ET ILLÉGALE DU CRYPTOMINING

Il est important de faire la distinction entre l'utilisation légale d'un mineur de cryptomonnaies et l'utilisation illégale du processus de cryptomining, notamment le *cryptojacking*. La différence subtile réside dans le consentement et la transparence dont fait l'objet le processus de minage pour l'utilisateur qui extrait la cryptomonnaie.

Cryptomining : le cryptomining est par exemple une nouvelle activité légitime dans l'exercice de laquelle les entreprises et les individus lui consacrent une quantité considérable de puissance CPU, un processus intensif de calcul et de résolution de problèmes mathématiques complexes afin de remporter une Proof of Work, qui vérifie le bloc suivant dans la chaîne.

Cryptojacking : Le cryptojacking est une forme de cyberattaque dans laquelle un pirate détourne la puissance de traitement d'une cible afin de miner des cryptomonnaies pour le compte du pirate. L'utilisateur n'est pas au courant et n'a pas donné son consentement à l'assaillant.

La base de la sanction liée à ces infractions est définie dans le Code pénal belge :

- **Article 504quater Code pénal – Fraude informatique**

  §1er. Celui qui cherche à se procurer, pour lui-même ou pour autrui, avec une intention frauduleuse, un avantage économique illégal en introduisant dans un système informatique, en modifiant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique (l'utilisation normale) des données dans un système informatique.

- **Article 550ter Code pénal – Piratage informatique**

  §1er. Celui qui, sachant qu'il n'y est pas autorisé, directement ou indirectement, introduit dans un système informatique, modifie ou efface des données, ou qui modifie par tout moyen technologique l'utilisation normale de données dans un système informatique.

  §3. Celui qui, suite à la commission d'une infraction visée au § 1er, empêche, totalement ou partiellement, le fonctionnement correct du système informatique concerné ou de tout autre système informatique, est puni d'un emprisonnement de un an à cinq ans et d'une amende de vingt-six [euros] à cent mille [euros] ou d'une de ces peines seulement.

https://www.symantec.com/about/newsroom/press-releases/2018/symantec_0321_01
https://bittrex.com/home/markets
https://blog.malwarebytes.com/cybercrime/2017/11/persistent-drive-by-cryptomining-coming-to-a-browser-near-you/
https://bitcoin.org/bitcoin.pdf

5 CONTACT

The Federal Cyber Emergency Team
Rue de la Loi 16
1000 Bruxelles
info@cert.be

The Federal Cyber Emergency Team
Rue de la Loi 18
1000 Bruxelles
info@cert.be

À propos de CERT.be

La cyber emergency team (l'équipe d'intervention d'urgence en sécurité informatique) fédérale (CERT.be) est le service opérationnel du Centre pour la Cybersécurité Belgique (CCB) qui soutient les autorités publiques, les services vitaux et les entreprises dans la prévention, la coordination et l'assistance sur le plan des cyberincidents.
www.cert.be

À propos du Centre pour la Cybersécurité Belgique

Le Centre pour la Cybersécurité Belgique (CCB) est le centre national pour la cybersécurité en Belgique. Le CCB a pour objectif de superviser, de coordonner et de veiller à l'application de la stratégie belge en matière de cybersécurité. L'optimalisation de l'échange d'informations permettra d'offrir une protection adéquate à la population, aux entreprises, aux autorités et aux secteurs vitaux.
www.ccb.belgium.be

Éditeur responsable

Centre pour la Cybersécurité Belgique, Miguel De Bruycker, 18 rue de la Loi, 1000 Bruxelles