STEVEN MEYER
FONDATEUR DE ZENDATA

Possédant un master de l'EPFL spécialisé en cyber-sécurité & cryptographie, Steven Meyer est aussi certifié Certified Information Systems Security Professional (CISSP). Après avoir travaillé chez Microsoft, il a été crackeur de mots de passe et consultant expert en sécurité informatique. Steven a finalement, en 2012, fondé ZENData (https://zendata.ch) une compagnie spécialisée en cyber-protection.

28 Septembre 2017

Êtes-vous en train de miner des crypto-monnaies à votre insu?

Grâce aux crypto-monnaies, les ordinateurs sont devenus des machines qui génèrent de l'argent. Et certains criminels en tirent déjà profit. En mai de cette année, des chercheurs ont découvert que plus de 15'000 machines étaient utilisées par un seul hackeur pour miner des Monero lui apportant 25'000$ par mois (https://www.cyberscoop.com/monero-mining-botnet-earns-suspected-chinese-hacker-25000-per-month/). Et le cas et loin d'être isolé.

Le «mining» consiste à mobiliser la ressource informatique (puissance de calcul, microprocesseur) d'un ordinateur pour valider les transactions effectuées dans une crypto-monnaie donnée. De nos jours les ressources demandées pour miner des crypto-monnaie sont devenues tellement grandes qu'un ordinateur seul n'a que très peu de chance de pouvoir en récupérer. Cette difficulté a poussé les mineurs à se regrouper en coopérative pour combiner leurs ressources de calcul

de hacking, qui consiste à «voler» de la puissance de calcul informatique.

Depuis le mois de mai, beaucoup de groupes de hackers exploitent ainsi les ressources de leur victime pour miner de l'argent. En Russie, par exemple, il est estimé que 30% des ordinateurs sont infectés par des «mining-virus» (https://cointelegraph.com/news/bitcoin-virus-has-infected-30-of-russian-devices-putin-advisor); mais les ordinateurs ne sont pas les seules objets détournés; des routeurs, caméras de surveillance et même des smartphones sont exploités dans ce sens.

Plus récemment, ThePirateBay a décidé de miner sur les navigateurs des visiteurs (https://torrentfreak.com/the-pirate-bay-website-runs-a-cryptocurrency-miner-170916/) de leur site web afin de générer du revenu plutôt que d'afficher des publicités qui sont souvent bloquées par leurs visiteurs. Le week-end dernier, Showtime.com a aussi forcé leur visiteur à miner (https://www.theregister.co.uk/2017/09/25/showtime_hit_with_coinmining_script/) des Monero pendant qu'il regardait leur série TV en ligne (ce n'est pas encore clair si c'est dû à un partage).

Est-ce que c'est grave?

Non et oui. C'est n'est pas terriblement grave que votre ordinateur soit utilisé pour faire du calcul pendant son temps libre. On se souvient de SETI@home (https://setiathome.berkeley.edu/) en 1999 qui utilisait les CPU des ordinateurs en veille pour rechercher de l'intelligence extraterrestre de façon tout à fait légitime. Le risque d'utiliser les ressources libres d'un ordinateur ne fait qu'augmenter de façon infime la facture électrique à la fin du mois.

Par contre il y a quand même plusieurs problèmes dans les exemples de «minage» décrits ci-dessus.

Dans le cas des hackeurs, le malware installé sur l'ordinateur qui «mine» les crypto-monnaie ouvre quand même une porte dérobée (backdoor) qui peut, dans le futur, être utilisée pour des attaques beaucoup plus destructrice. Aussi les ressources consommées sur les machines sont tellement grandes qu'elles peuvent rendre les ordinateurs quasi inutilisables ; et dans le cadre d'un smartphone, ce dernier aura sa batterie vidée en mois d'une heure.

Comment se protéger?

Comme toujours, il faut avoir une bonne hygiène informatique: garder son système à jour, faire attention aux liens sur lesquels on clique, bien vérifier un email avant d'ouvrir une pièce jointe, mettre un antivirus et ne pas réutiliser des mots de passe.

Concernant les «minages» dans les navigateurs, il existe des outils tels que NoScrpit, scriptSafe et uBlock Origine qui peuvent empêcher leur exécution.

Si vous voyez votre ordinateur devenir lent et votre CPU consommer beaucoup de ressource (https://www.youtube.com/watch?v=z4I3034FmG0)s, sans raison évidente (attention les mises à jour de Windows consomment beaucoup de ressources), vous pouvez essayer de déconnecter votre ordinateur d'internet. Le minage de crypto-monnaie demande une connexion permanente; en coupant votre connexion internet, votre ordinateur ne reçoit plus de «problèmes» mathématiques à résoudre et vos ressources se libèrent. Cette démarche peut vous donner une indication si vous avez été infecté.

Pour conclure, l'approche de pirater un ordinateur pour «miner» des crypto-monnaie est clairement illégale et dangereuse. Par contre, l'approche de remplacer de la publicité sur les sites web par du minage est intéressant et pourrait offrir une alternative à la publicité qui est souvent trop envahissante sur notre écran et dans notre vie privée.

THÈMES

CRYPTO-MONNAIE (/TAG/CRYPTO-MONNAIE) / **PIRATAGE INFORMATIQUE** (/TAG/PIRATAGE-INFORMATIQUE)

PLUS D'OPINIONS

STEVEN MEYER (/STEVEN-MEYER)

Les dangers de l'internet des objets (IoT) (/steven-meyer/dangers-de-linternet-choses-iot)

L'internet des objets (Internet of Things - IoT) et les appareils connectés ou «Smart devices» sont...