La Cyber Threat Alliance (CTA), l'une des principales associations au monde de professionnels de la cybersécurité a publié, le 19 septembre 2018, un rapport intitulé « La menace du minage illicite de cryptomonnaie », faisant état d'une explosion sans précédent de ces pratiques criminelles depuis 2017.

Le minage de cryptomonnaie est une opération, fortement consommatrice en énergie, qui consiste à effectuer un calcul cryptographique appelé « validation par la preuve de travail » (*proof of work,* voir *La rem* n°44, p.97), permettant au protocole de sécuriser les transactions sur le réseau et de générer de nouvelles unités de cryptomonnaies en récompense de ce calcul (voir *La rem* n°45, p.17).

Également appelé « *cryptojacking* »*,* le minage illicite de cryptomonnaie consiste, pour des *hacker*s, à pirater des ordinateurs, des navigateurs web, des périphériques de l'internet des objets, des appareils mobiles et des infrastructures de réseau, afin de s'accaparer de leur puissance de traitement, et miner ainsi des cryptomonnaies pour recevoir les récompenses prévues pour la validation des transactions.

Les valeurs de certaines cryptomonnaies augmentant et leur utilisation devenant de plus en plus répandue, cette nouvelle menace informatique est en pleine expansion et touche tout autant les entreprises que les particuliers.

Le rapport de la CTA fait état d'une augmentation de 459 % de détections illicites de logiciels malveillants depuis 2017 et cette forte croissance ne montre aucun signe de ralentissement. Quant au rapport sur la sécurité informatique publié, en juin 2018, par l'éditeur de logiciel anti-virus McAfee, il note une augmentation de 629 % de logiciels malveillants de minage pour le seul premier trimestre 2018.

Pour miner des cryptomonnaies à l'insu des propriétaires des appareils utilisés, les pirates recourent à une variété de techniques qui peuvent être menées de deux façons : soit en installant un programme exécutable ou une application directement sur un périphérique, appelé « minage basé sur du binaire » (*binary-based mining*)*,* soit directement à travers le moteur Javascript du navigateur web utilisé, appelé « minage basé sur le navigateur » (*browser-based mining*)*.*

Le programme de « minage basé sur du binaire », qui nécessite une installation sur un ordinateur, peut être envoyé par courriel et *spam,* afin que le propriétaire de l'appareil l'ouvre et l'exécute, mais il peut aussi être installé à distance, lorsque les machines sont déjà infectées par un autre virus.

Les programmes binaires diffusés par courriel s'appuient sur des failles de sécurité du système d'exploitation Windows de Microsoft, déjà exploitées lors des attaques de rançongiciels (*ransomwares*) Wannacry et NotPetya, menées en mai 2017 et qui avaient atteint 200 000 systèmes informatiques dans 150 pays (voir *La rem* n°41, p.54).

Ces failles de sécurité et ces outils de piratage ont été divulgués en 2016 par des pirates, les « Shadows Brokers », qui les attribuent à un groupe connu sous le nom d'Equation Group, lié à l'unité « Opération d'accès sur mesure » (*Tailored Access Operations*) de la National Security Agency (NSA). Après la diffusion de ces outils, plusieurs « exploits » (programmes exploitant une faille de sécurité), dont EternalBlue et EternalRomance, avaient été lancés à l'assaut de diverses versions du système d'exploitation Windows de Microsoft.

Ces mêmes outils sont utilisés pour miner de manière illicite des cryptomonnaies. Le rapport de la CTA cite en particulier le logiciel malveillant PyRoMine, créé à partir d'EternalRomance. Le logiciel est envoyé par courriel sous la forme d'un fichier exécutable compressé puis, explique la CTA : *« si une personne utilisant un réseau d'entreprise ouvre le programme PyRoMine, le logiciel malveillant commence immédiatement à rechercher les machines vulnérables à l'exploit d'EternalRomance. Une fois infectées, les machines récupèrent et utilisent le programme binaire XMRig pour miner la cryptomonnaie Monero. XMRig est un programme utilisé par les mineurs pour effectuer des opérations minières légitimes et ne devrait pas en soi être considéré comme un logiciel malveillant. »*

Lancée en avril 2014, Monero est une cryptomonnaie assurant l'anonymat et fonctionnant sur un système décentralisé. Le 1er janvier 2017, elle s'échangeait contre environ 15 dollars, après avoir approché les 500 dollars en janvier 2018 ; elle est aujourd'hui cotée 120 dollars. Cette cryptomonnaie est particulièrement appréciée des pirates puisque, contrairement à Bitcoin, elle n'est pas aisément traçable. En juillet 2018, selon les données recueillies par Palo Alto Networks, l'un des leaders mondiaux de la cybersécurité, également membre de la CTA, *« la majorité des logiciels malveillants de cryptomonnaie illicites minent Monero (85 %), suivi de Bitcoin (8 %). Toutes les autres cryptomonnaies représentent les 7 % restants »*.

Le rapport de la CTA indique également que des réseaux de *botnets* sont utilisés pour miner de manière illicite des cryptomonnaies. Un réseau de *botnets* (contraction des mots « robot » et « Net ») permet d'exécuter des tâches à partir de programmes installés sur de nombreux appareils électroniques connectés à l'internet communiquant entre eux simultanément. Utilisé par des pirates, ce réseau de machines infectées est ensuite activé pour mener des attaques, rançongiciel ou déni de service, comme celle subie par OVH au cours de l'automne 2016 (voir *La rem* n°40, p.27).

Ces réseaux de *botnets* sont aujourd'hui utilisés par les pirates pour installer des logiciels de minage sur des machines déjà infectées. Selon la CTA, plusieurs *botnets* à grande échelle comme Smominru, Jenkins Miner ou encore Adylkuzz ont déjà généré des millions de dollars en cryptomonnaie.

La seconde façon de miner des cryptomonnaies à l'insu des propriétaires des appareils utilisés consiste à s'appuyer sur le navigateur web utilisé par les internautes. Le plus connu pour le minage de cryptomonnaies s'appelle CoinHive. C'est un navigateur parfaitement légitime, dont l'objet est de proposer

une alternative aux navigateurs basés sur l'exploitation des données personnelles, comme Chrome de Google, en permettant à l'utilisateur d'échanger les ressources de son navigateur contre une expérience de navigation sans publicité.

La méthode selon laquelle CoinHive est installé sur un site web détermine si son usage est licite ou non. L'usage est licite lorsqu'un site web ajoute le code informatique de CoinHive en informant ses utilisateurs. Il est illicite lorsqu'un site web y recourt à l'insu de ses utilisateurs, qui minent alors des cryptomonnaies sans le savoir. À la date du 2 juillet 2018, selon le rapport de la CTA, une recherche sur PublicWWW, moteur de recherche de code source, indiquait que 23 000 sites web avaient intégré le code source de CoinHive. En septembre 2017, *via* ses sites web, Showtime, chaîne de télévision payante américaine appartenant à CBS Corporation, qui diffuse principalement des films et des séries, s'est fait prendre la main « dans le sac ». Les sites web showtime.com et showtimeanytime.com exécutaient le script de CoinHive pour miner la cryptomonnaie Monero, et cela sans en avertir les internautes, ce que certains, l'ayant découvert, se sont empressés de dénoncer sur Twitter.

Le minage illicite de cryptomonnaies concerne aussi les entreprises, pour lesquelles les répercussions peuvent être particulièrement lourdes de conséquences. En effet, le minage par la preuve de travail requérant une utilisation à pleine puissance des processeurs, le matériel informatique de l'entreprise peut rapidement être en surchauffe. En outre, la consommation d'électricité d'une entreprise infectée augmentera significativement. Toujours selon la CTA, ce type d'attaques peut être annonciateur de menaces potentiellement beaucoup plus importantes : dès lors que les pirates ont accès aux systèmes informatiques de l'entreprise, ils peuvent procéder au vol de données, à la modification de données, à la location de l'infrastructure à d'autres attaquants potentiels ou encore bloquer des ressources tout en exigeant une rançon. Toutes les entreprises sont de ce fait concernées. Entre septembre 2017 et mars 2018, des chercheurs en sécurité informatique ont révélé que les infrastructures Cloud Amazon Web Services et Microsoft Azure des entreprises Tesla, Aviva et Gemalto avaient été infiltrées par des programmes de minage illicite.

Loin d'être un phénomène passager, le minage illicite de cryptomonnaies aurait même vocation à croître dans les prochaines années puisqu'il est avéré que le nombre d'attaques augmente en même temps que la valorisation des cryptomonnaies.

Sources :

- « Smominru Monero mining botnet making millions for operators », Kafeine, proofpoint.com, January 31, 2018.
- « Lessons from the Cryptojacking Attack at Tesla », CSI Team, redlock.io, 20 février 2018.
- « Python-Based Malware Uses NSA Exploit to Propagate Monero (XMR) Miner », Jasper Manuel, fortinet.com, April 24, 2018.
- « Explosion du minage illicite de cryptomonnaies liée à une fuite de la NSA (rapport) », AFP *in* tv5monde.com, 19 septembre 2018.
- « The illicit cryptocurrency mining threat », Neil Jenkins, Scott Scher, Cyber Threat Alliance, cyberthreatalliance.org, September 19, 2018.