Un millier de PC piratés pour générer de la crypto-monnaie Zcash

Pour obtenir des crypto-monnaies comme le Bitcoin (BTC), la plus populaire, il faut soit l'acheter, soit la «miner». C'est-à-dire fournir de la capacité de calcul pour exécuter les algorithmes liés au système de «preuves de travail» (proof-of-work) qui va protéger la monnaie électronique des risques de contrefaçon et valider les transactions effectuées (à travers la Blockchain). Zcash (ZEC) est l'une de ces nombreuses crypto-monnaies. Apparue sur le marché le 28 octobre dernier, elle est réputée plus anonyme que le bitcoin. Ses créateurs la définissent ainsi: *« Si le bitcoin est le HTTP de la monnaie, Zcash en est le HTTPS. »* Un niveau d'anonymisation supplémentaire qui attire l'intérêt des universitaires, des investisseurs et des… cybercriminels.

Alexandre Gostev, chercheur en sécurité pour Kaspersky Lab, révèle que le Zcash a poussé des pirates à créer des botnets chargés de miner la crypto-monnaie pour leur compte. *« En novembre, nous avons enregistré plusieurs incidents où le logiciel minier Zcash a été installé sur les ordinateurs des utilisateurs sans autorisation »*, déclare le chercheur sur le blog de Securelist. Ces logiciels n'étant pas en soi des malwares, ils ne sont généralement pas détectés comme indésirables par les antivirus. Un avantage dont profitent les criminels pour infecter les PC de leurs victimes.

Pas encore d'exploitation massive

L'installation de ce que Kaspersky Lab détecte comme «not-a-virus:RiskTool.Win64.BitCoinMiner» s'effectue par l'intermédiaire d'autres logiciels que l'utilisateur installe sciemment. Généralement des applications piratées et téléchargées en P2P (torrents). Le logiciel de minage peut également avoir été installé «manuellement» à distance sur des PC précédemment infectés. *« Jusqu'à présent, nous n'avons pas vu de cas d'envoi massif ou de vulnérabilités dans des sites Web exploitées pour distribuer des logiciels d'exploitation »*, rassure Alexandre Gostev. Avant de prévenir : *« mais si l'exploitation minière reste aussi rentable qu'aujourd'hui, ce n'est qu'une question de temps »* avant que les pirates n'étoffent leurs moyens de distribution des logiciels de minage.

Le plus populaire d'entre eux est nheqminer de l'équipe Micemas. Il mine aussi bien des Zcashs que des bitcoins. Selon Kaspersky, les cybercriminels doivent juste référencer le programme lié à la crypto-monnaie dans leur «wallet» (leur porte-monnaie électronique) pour tirer leurs marrons du feu. Pour l'heure, seul un millier de PC seraient infectés par une application de minage de Zcash. La capacité de calcul ainsi fournie permet de générer autour de 6200 dollars par mois, soit 75000 dollars par an.

A condition que le logiciel de minage soit lancé à chaque démarrage de la machine. Pour y parvenir, en plus de maquiller les applications derrière des noms communs de processus Windows (comme system.exe ou svchost.exe), les cybercriminels les ajoutent au Planificateur de tâches de Windows ou dans les clés d'auto-exécution du Registre.

Un phénomène ancien

L'exploitation de botnet pour miner des crypto-monnaies n'est pas un phénomène nouveau. Le bitcoin et d'autres crypto-monnaies avaient également connu des tentatives similaires à leurs débuts, rappelle le chercheur. Mais l'activité n'était visiblement pas assez rentable et les botnets avaient été abandonnés. Car l'action de miner est tout sauf discrète, malgré les précautions prises par les cybercriminels pour dissimuler leurs logiciels illégitimes dans le système.

Un calcul d'exploitation minière dévore quasiment 90% de la mémoire vive, ce qui ralentit le système et le reste des applications. De même, l'exploitation permanente du processeur amène à consommer plus d'électricité que d'habitude. Ce qui finit par se voir sur la facture et risque d'attirer l'attention de l'utilisateur sur l'usage réel qui est fait de son ordinateur. S'il parvient à découvrir l'origine de cette surconsommation, il s'attachera à éradiquer sa cause en désinstallant les logiciels de minage. Le succès de la nouvelle génération de botnets dédiés au minage de Zcash reste donc à vérifier dans le temps.

Lire également
Le Bitcoin victime de hackers sponsorisés par un État ?
Bientôt un Bitcoin pour rémunérer les attaques DDoS ?
Tracfin : le renseignement financier cible les dérives du numérique