Attention aux voleurs de crypto-monnaies

Grâce à des logiciels malveillants, des pirates informatiques parviennent à « braquer » les plateformes d'échange de monnaies virtuelles. Explications.

PAR **BAUDOUIN ESCHAPASSE**

Modifié le 18/12/2017 à 10:51 - Publié le 16/12/2017 à 14:45 | Le Point.fr

i

C'est la monnaie préférée des pirates informatiques. Celle qu'exigent les hackers lorsqu'ils formulent une demande de rançon. Mais pas seulement ! Depuis que le bitcoin flambe (il a dépassé le 15 décembre les 17 000 dollars), de plus en plus de fonds d'investissement, alléchés par les perspectives haussières de son cours, s'y intéressent. Et de nombreux sites de commerce en ligne se mettent à facturer produits et services dans cette crypto-monnaie.

Le bitcoin reste, aujourd'hui encore, très convoité par les hackers. En témoignent les nombreuses arnaques informatiques recensées, ces derniers mois, sur les sites proposant d'acquérir ou de vendre cette crypto-monnaie. Les vols se multiplient... Les braquages de détenteurs de bitcoins s'opèrent en général au moment où ils convertissent leur fortune virtuelle en argent sonnant et trébuchant.

Les affaires médiatisées sont encore rares. « Les possesseurs de bitcoin aiment en général la discrétion et sont peu disposés à se faire connaître même lorsqu'ils ont été escroqués », témoigne Caroline Laverdet, avocate spécialisée en droit des nouvelles technologies. Il n'empêche. « La multiplication des affaires devrait inciter les usagers à la plus grande prudence », poursuit-elle.

« Parce que la crypto-monnaie (...) se répand activement à travers le monde, devient plus accessible pour les utilisateurs et constitue une cible de plus en plus tentante pour les criminels, nous nous attendons à voir cette tendance se poursuivre », complète Sergey Yunakovsky, analyste en malware chez Kaspersky.

Attention aux arnaques

La plus célèbre affaire remonte à février 2014, quand le site Mt.Gox (prononcer Mount Gox), le deuxième plus gros « broker » de crypto-monnaie après BTC China (qui a suspendu ses activités, sur ordre de Pékin, en septembre 2017), fait faillite après que des pirates informatiques ont détourné plus de 650 000 bitcoins. L'escroquerie ébranle pendant quelques jours la confiance des opérateurs et entraîne une chute de 20 % du cours de la monnaie virtuelle. Mais le bitcoin ne tarde pas à repartir à la hausse. Depuis lors, les « casses numériques » se sont multipliés.

En août et octobre 2016, ce sont près de 120 000 bitcoins qui sont volés à plusieurs particuliers par des hackers, parvenus à se connecter sur la plateforme Bifinex, via une faille de sécurité. En avril 2017, Yapizon, un site sud-coréen d'échange de crypto-monnaie porte plainte pour le vol de 3 800 bitcoins (estimés à 5 millions de dollars au moment du « casse »).

Des montants de plus en plus élevés

Au mois de septembre suivant, le groupe américain de cybersécurité FireEye révèle que des pirates informatiques originaires de Corée du Nord sévissent sur plusieurs plateformes proposant d'acheter et de vendre des crypto-monnaies. Ciblés ? Outre le bitcoin... l'éthereum (une crypto-monnaie soutenue notamment par Microsoft, JP Morgan Chase et Intel) et le bithumb, une monnaie virtuelle sud-coréenne. Le montant du butin se chiffre en millions de dollars.

En novembre 2017, le groupe Tether, à l'origine de la crypto-monnaie USDT, porte plainte pour un cambriolage « online » de plus de 31 millions de dollars dans ses portefeuilles virtuels. Dernier en date : le piratage de NiceHash, une plateforme d'échange et de « minage » de bitcoins reconnaît le 6 décembre dernier s'être fait braquer 4 700 bitcoins pour un montant estimé à plus de 68 millions de dollars.

Comment ça marche

Si la technologie blockchain sécurise les transactions réalisées en bitcoins, comment cette monnaie peut-elle aujourd'hui être l'objet d'attaques informatiques ? Le groupe de cybersécurité Kaspersky l'explique simplement. Ses chercheurs ont identifié sur la Toile plusieurs logiciels malveillants spécialement dédiés au détournement de crypto-monnaie.

Surnommés « crypto-stealers » (ou « voleurs de crypto-monnaie »), ces programmes malveillants ciblent les systèmes de transfert de monnaie virtuelle. Si un utilisateur souhaite effectuer un versement d'un bitcoin d'un compte à un autre, il doit connaître l'identifiant du porte-monnaie du destinataire (un numéro distinct composé de plusieurs chiffres). Les utilisateurs préférant souvent copier-coller ce numéro plutôt que de le recopier dans le champ « adresse de destination » du logiciel employé pour la transaction, il suffit de surveiller le presse-papiers de la machine infectée pour obtenir cette précieuse information.

Or, un « cheval de Troie » remplace l'adresse du porte-monnaie de l'utilisateur par celle du créateur (ou du bénéficiaire) du malware. La victime transfère ainsi directement, et à son insu, son argent à ses voleurs. Seuls les utilisateurs les plus attentifs s'aperçoivent de ce tour de passe-passe. Quelques millisecondes suffisent à substituer le code du compte destinataire. « La plupart du temps, l'usager n'y voit donc que du feu. La majorité des crypto-monnaies utilisent en effet des adresses commençant de la même façon et comportant le même nombre de caractères. Des hackers peuvent ainsi créer sans difficulté des codes de remplacement valables », explique-t-on chez Kaspersky.

Tour de passe-passe

Le plus connu de ces programmes malveillants se nomme « CryptoShuffler ». Actif depuis plus d'un an, il cible un large éventail de crypto-monnaies, parmi les plus répandues : bitcoin, éthereum, Zcash, dash. Une liste qui pourrait s'allonger quand l'on sait qu'il existe plus de 1 300 monnaies virtuelles en circulation.

« CryptoShuffler » n'est malheureusement pas le seul à cibler les utilisateurs de cryptomonnaies. Dans une récente étude sur les botnets effectuant des missions de « bitcoinmining », les ingénieurs du même groupe russe de sécurité informatique ont ainsi découvert un malware encore plus redoutable. Baptisé « DiscordiaMiner », il frappe les usagers d' une autre monnaie virtuelle : le Monero.

« DiscordiaMiner » peut télécharger et exécuter des fichiers depuis un serveur à distance et présente des similitudes avec le virus « NukeBot ». Un programme informatique, découvert en janvier dernier, et particulièrement redouté des responsables informatiques des groupes bancaires, car il se propage sur les réseaux en toute discrétion, et infecte prioritairement les serveurs des établissements financiers.