

Plus d'1 consommateur sur 10 règle désormais ses achats en cryptomonnaie

12 février 2019

La cryptomonnaie, souvent associée aux spécialistes de l'informatique ou à des personnes en quête de profits rapides, est aujourd'hui devenue un moyen de paiement répandu selon une récente [étude de Kaspersky Lab](#), révélant que plus d'un consommateur sur dix (13 %) s'en sert pour régler des achats. Cependant, des cybercriminels exploitent eux aussi cette tendance en ciblant les bourses de cryptomonnaie et en [modifiant des menaces existantes](#) afin d'attaquer les investisseurs. Avec des pirates qui développent des méthodes complexes pour accéder à leurs fonds, ces derniers risquent de perdre leurs économies conservées au moyen de cette technologie non protégée.

Des entreprises en nombre croissant acceptent désormais les paiements en cryptomonnaie, notamment des sites [e-commerce](#), et en particulier dans le secteur de l'[alimentation](#). Or, alors que les consommateurs manifestent un intérêt pour la cryptomonnaie tant pour y investir que pour dépenser leur argent, leurs capitaux sont vulnérables au vol de portefeuilles numériques, ainsi qu'au manque de sécurité des bourses et des ICO (levées de fonds en cryptomonnaie). Des incidents de grande ampleur se sont en effet déjà produits, aboutissant au [vol de sommes pouvant atteindre l'équivalent de 530 millions de dollars en jetons numériques](#).

Vitaly Mzokov, responsable de la vérification au sein du Growth Center de Kaspersky Lab, commente : « *En dépit de la baisse des cours des cryptomonnaies, il demeure un vif appétit de transactions numériques parmi les consommateurs. Notre enquête auprès d'eux révèle que 13 % se servent d'une cryptomonnaie comme moyen de paiement, ce qui a été pour nous une constatation surprenante. Cependant, il existe de réels dangers liés aux bourses en ligne car celles-ci n'en sont qu'à leurs balbutiements. Un défaut de sécurisation des fonds pourrait avoir des conséquences financières catastrophiques pour les utilisateurs.* »

« *Alors que les acteurs malveillants gagnent en sophistication dans leurs attaques, les bourses de cryptomonnaies et les ICO en sont les premières cibles, offrant aux cybercriminels un moyen simple de dérober des sommes considérables, faute de la mise en place de mesures de cybersécurité. En outre, rien ne saurait remplacer la vigilance : si quelque chose vous paraît tant soit peu suspect, n'investissez pas !* »

Les acteurs malveillants peuvent recourir à un large éventail de pratiques pour dérober des fonds dans les crypto-wallets ainsi que lors des transactions en cryptomonnaies et des ICO. Des épisodes très médiatisés, par exemple le [vol de 120 000 bitcoins dans des portefeuilles clients séparés sur Bitfinex](#) il y a déjà quatre ans et demi ou le [piratage de Coincheck pour un montant de 530 millions de dollars en 2018](#), illustrent l'insécurité de ces places boursières et la facilité avec laquelle des cybercriminels peuvent accéder à des réseaux en direct et y causer des dommages vastes et irréparables. En cas de vol de la totalité des capitaux d'une bourse de cryptomonnaie, celle-ci n'a plus qu'à fermer boutique et les investisseurs en seront pour leurs frais.

Les ICO sont particulièrement menacées car les personnes qui les organisent sont souvent dépourvues de formation ou d'expérience dans la cybersécurité. Elles sont par conséquent dans l'incapacité de protéger les fonds et de réagir efficacement en cas d'incident. En définitive, le marché des cryptomonnaies n'est toujours pas réglementé et aucun mécanisme d'évaluation des risques n'y a encore été mis en place.

Les investisseurs doivent avoir conscience des inconvénients potentiels concernant les bourses de cryptomonnaies :

- Ces plates-formes prélèvent généralement des commissions sur les retraits de fonds.
- Les utilisateurs ne peuvent pas réagir promptement aux variations de cours s'ils décident de retirer leur argent.
- De nombreuses opérations portant sur de la monnaie fiduciaire provenant de sources anonymes peuvent soulever des questions de la part des autorités.

Kaspersky Lab adresse ses recommandations aux consommateurs souhaitant continuer à investir dans les cryptomonnaies et à s'en servir comme moyen de paiement :

- Vérifier systématiquement l'adresse d'un portefeuille web et ne jamais suivre des liens pointant vers une banque en ligne ou un portefeuille web.
- Utiliser des crypto-wallets matériels.
- Vérifier et revérifier l'adresse du destinataire, le montant transféré ainsi que celui de la commission prélevée avant de valider une transaction.
- Noter une phrase mnémotechnique qui permettra de récupérer l'accès à un crypto-wallet en cas d'oubli ou de perte de mot de passe.
- Installer une solution de sécurité de haute qualité, telle que [Kaspersky Internet Security](#), afin de protéger les appareils utilisés pour accéder à des crypto-wallets et effectuer des transactions sur des bourses de cryptomonnaies.

Kaspersky Lab travaille activement à la sécurité future des cryptomonnaies et des ICO. La société a ainsi réalisé un [audit de cybersécurité pour Merkleon](#), l'éditeur autrichien d'un logiciel de cryptomonnaie, afin de s'assurer que cette solution est protégée contre les menaces potentielles.

Pour en savoir plus sur la perception des paiements numériques par les consommateurs, rendez-vous sur <https://www.kaspersky.com/blog/money-report-2018/>

Méthodologie : Etude réalisée par Kaspersky Lab auprès de 12 448 consommateurs dans 22 pays en 2018.

À propos de Kaspersky Lab

Kaspersky Lab est une société de cybersécurité mondiale qui est active sur le marché depuis plus de 20 ans. L'expertise de Kaspersky Lab en matière de « Threat Intelligence » et sécurité informatique vient perpétuellement enrichir la création de solutions et de services de sécurité pour protéger les entreprises, les infrastructures critiques, les gouvernements et les consommateurs à travers le monde. Le large portefeuille de solutions de sécurité de Kaspersky Lab comprend la protection avancée et complète des terminaux et un certain nombre de solutions et de services de sécurité dédiés afin de lutter contre les menaces digitales sophistiquées et en constante évolution. Les technologies de Kaspersky Lab aident plus de 400 millions d'utilisateurs et 270 000 clients à protéger ce qui compte le plus pour eux.

Pour en savoir plus : www.kaspersky.com/fr/

Pour plus d'informations sur l'actualité virale : <http://www.securelist.com>

Salle de presse virtuelle Kaspersky Lab : <http://newsroom.kaspersky.eu/fr/>

Blog français de Kaspersky Lab : <http://blog.kaspersky.fr/>



Hotwire pour Kaspersky Lab

Marion Delmas / Séverine Randjelovic / Noémie Minster / Aliénor Gamerdinger

01 43 12 55 62 / 57 / 73 / 47

KasperskyFrance@hotwireglobal.com