Bitcoins : ce qu'il vous faut savoir pour protÃ©ger cette monnaie Ã©lectronique
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 17/3/2014 13:30:00

De plus en plus de gens commencent Ã utiliser de la crypto-monnaie telle que le bitcoin, et certaines entreprises commencent Ã l'accepter. La consÃ©quence de cette popularitÃ© croissante est que des voleurs s'y intÃ©ressent de plus en plus. **Thierry Karsenti**, Directeur Technique Europe - **Check Point Software Technologies**, nous en parle un peu plus.

La crypto-monnaie est une monnaie Ã©lectronique. Elle n'est pas physique ; il n'existe pas de piÃ¨ces ni de billets, et est gÃ©nÃ©rÃ©e (Â« extraite Â») par des ordinateurs effectuant des calculs mathÃ©matiques complexes.

Le bitcoin est probablement la monnaie Ã©lectronique la plus connue actuellement, mÃªme s'il en existe beaucoup d'autres, notamment dogecoin, mazacoin, megacoin ou encore solarcoin.

La valeur de ces diffÃ©rentes crypto-monnaies fluctue, mais ces quelques derniers mois, la valeur du bitcoin n'a cessÃ© d'augmenter. De nombreuses personnes pensent maintenant qu'il peut Ãªtre une alternative viable au dollar tout-puissant, Ã l'euro et Ã d'autres monnaies. C'est une progression naturelle.

La popularitÃ© croissante des bitcoins conduit de plus en plus de gens Ã en acheter, de plus en plus d'entreprises Ã les accepter comme moyen de paiement, et de plus en plus de voleurs Ã considÃ©rer que cette monnaie a suffisamment de valeur pour Ãªtre dÃ©robÃ©e.

Il est important de protÃ©ger vos bitcoins, car comme tout argent liquide, une fois volÃ©, il est impossible de le rÃ©cupÃ©rer ni de dÃ©couvrir qui l'a pris.

ProblÃ¨me de sÃ©curitÃ© des bitcoins

Il existe dÃ©jÃ plus d'une centaine de familles de logiciels malveillants uniques capables de dÃ©tourner de la crypto-monnaie, selon une Ã©tude rÃ©cente de Dell SecureWorks.

Cette liste comprend des logiciels malveillants spÃ©cifiquement conÃ§us pour cibler de la monnaie Ã©lectronique, ainsi que des logiciels malveillants existants qui ont Ã©tÃ© modifiÃ©s pour intÃ©grer de nouvelles fonctionnalitÃ©s spÃ©cifiques.

Â

Ce qui est assez alarmant Ã propos de ce rapport, est le fait que la plupart des logiciels malveillants de vol de crypto-monnaie ne sont pas vraiment sophistiquÃ©s et peuvent Ãªtre dÃ©veloppÃ©s par quiconque ayant des compÃ©tences rudimentaires en programmation.

Par exemple, si un cheval de Troie est dÃ©jÃ conÃ§u pour dÃ©rober des identifiants de sites bancaires en ligne, il n'est pas trÃ¨s difficile de modifier ses fonctions pour intercepter des identifiants de portefeuilles ou de bourses d'Ã©change de bitcoins.

Le logiciel malveillant surveille les activitÃ©s des utilisateurs et commence Ã enregistrer les frappes au clavier lorsqu'un utilisateur accÃ¨de Ã son portefeuille dans le Cloud ou se connecte au site web d'une bourse d'Ã©change pour envoyer et retirer des bitcoins.

Les identifiants sont interceptÃ©s et envoyÃ©s aux agresseurs qui peuvent ensuite les utiliser pour vider son compte.
Les criminels peuvent Ã©galement trÃ¨s facilement acheter des kits de logiciels malveillants sur des forums clandestins et les utiliser pour dÃ©rober des bitcoins.

Gardez vos bitcoins Ã l'abri

Le type le plus courant de logiciel malveillant de vol de crypto-monnaie cible les portefeuilles des utilisateurs stockÃ©s sur leur ordinateur. Les logiciels malveillants recherchent le fichier Â« wallet.dat Â» ou d'autres fichiers et rÃ©pertoires couramment utilisÃ©s sur l'ordinateur.

Ils tÃ©lÃ©chargent ensuite le portefeuille sur un serveur distant pour que les agresseurs puissent extraire la clÃ© et transfÃ©rer les fonds du portefeuille vers un autre compte.

Une fois que l'argent a disparu, il ne peut Ãªtre pistÃ©. C'est pourquoi il est trÃ¨s important de s'assurer que votre antivirus est mis rÃ©guliÃ¨rement Ã jour pour dÃ©tecter les infections de logiciels malveillants, et d'Ãªtre Ã©galement trÃ¨s attentif Ã ce que vous tÃ©lÃ©chargez depuis le web.

L'augmentation de l'utilisation de bitcoins et autres types de monnaie Ã©lectronique attirera inÃ©vitablement les voleurs. L'un des plus gros problÃ¨mes de la fraude en ligne est l'encaissement des fonds volÃ©s aprÃ¨s qu'ils aient Ã©tÃ© extraits des comptes des utilisateurs.

Ce n'est pas le cas des bitcoins, qui sont uniquement liÃ©s Ã une adresse email spÃ©cifique.

Aucun nom, aucune information d'identification, et aucun moyen de dÃ©terminer leur destination. En consÃ©quence, les utilisateurs doivent faire trÃ¨s attention aux infections de logiciels malveillants.

Si vous dÃ©cidez d'investir dans des bitcoins ou d'autres types de crypto-monnaie, assurez-vous d'avoir de bonnes habitudes de sÃ©curitÃ©. Faites attention Ã ce que vous tÃ©lÃ©chargez, gardez votre antivirus Ã jour et faites Ã©galement attention aux messages de phishing qui tentent de dÃ©rober les identifiants de votre portefeuille.

i vous avez un pare-feu ou un produit de sÃ©curitÃ© similaire, vous pouvez empÃªcher les logiciels malveillants de se connecter Ã leur serveur distant pour transfÃ©rer les fichiers de votre portefeuille. ProtÃ©gez vos comptes de messagerie et sÃ©lectionnez des mots de passe renforcÃ©s pour votre compte sur une bourse d'Ã©change et votre portefeuille, afin que les agresseurs ne puissent pas utiliser de mÃ©thodes de force brute pour les dÃ©couvrir facilement.

Au final, les vols de bitcoins et de crypto-monnaie pourraient Ãªtre plus lucratifs que les vols classiques de cartes bancaires et les dÃ©tournements de fonds. Mais vous pouvez prendre des mesures pour vous protÃ©ger.