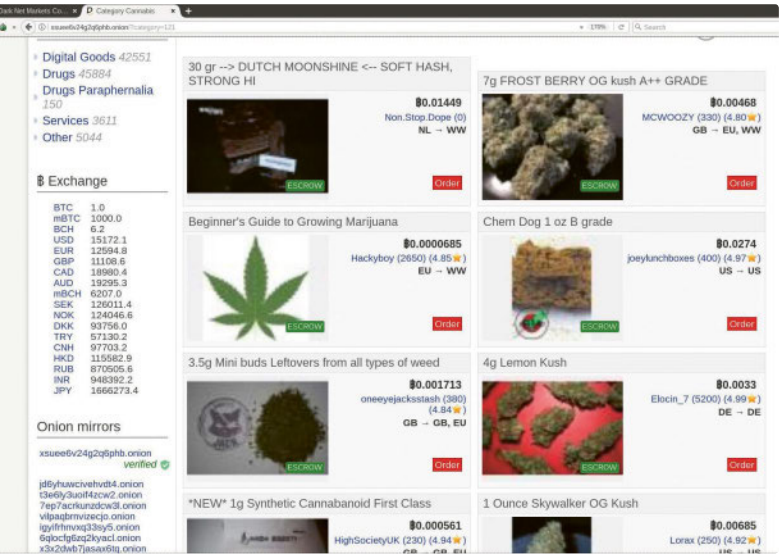
Avez-vous confiance
dans votre dealer de drogue sur le Net?

Dr Emmanuel Benoist
Professeur à la Division d'informatique, BFH

Le Darknet permet d'échanger tout type de biens illégaux. Comme tout commerce, il repose sur une certaine «confiance», confiance pour le client d'être livré, ou pour le vendeur d'être payé. Cette confiance est basée à la fois sur un mécanisme de réputation et sur un contrôle par les utilisateurs des transactions financières.

Cocaïne, héroïne, médicaments, hachisch, numéros de cartes de crédits, comptes Paypal. Vous pouvez tout acheter sur le Darknet. Le Darknet est une partie de l'Internet qui n'est pas accessible avec un navigateur normal, mais nécessite l'usage d'outils adaptés. On y accède en utilisant le réseau Tor (The Onion Routing) et particulièrement le navigateur Tor-Browser. Ce réseau est normalement utilisé pour anonymiser l'accès à Internet. Ici, il sert à héberger des sites dont le nom se termine en .onion et qui ne sont pas accessibles depuis un navigateur standard.

Les sites les plus visités du Darknet sont les sites de «marchés» sur lesquels on peut trouver toutes sortes de produits. Les premiers gros marchés ont été Silk Road, Black Market Reloaded et Alpha Bay. Tous ces sites ont été fermés par les forces de police. Actuellement, le site contenant le plus de produits est Dream Market. Il contient actuellement environ 100 000 annonces. On y trouve toutes sortes de drogues (cannabis, extasy, médicaments), mais aussi des produits digitaux (numéros de cartes de crédit, scans de documents d'identité) ou des services (faux documents d'identité, faux permis de conduire).



Quelques annonces de cannabis du site Dream Market

Sur le Darknet, il n'y a pas de tribunal

Sur ces sites, l'anonymat est de rigueur. Ni les vendeurs, ni les acheteurs ne souhaitent être connus. Les sites ont dû mettre en place des techniques permettant de compenser cette opacité. Si on achète sur ce site, on souhaite être livré, et on souhaite obtenir la qualité promise; et si on vend on souhaite être payé. C'est pourquoi des mécanismes augmentant la confiance ont été mis en place.

Dans le monde réel, si un client a un problème avec un produit de la Migros, il le rapporte. La Migros le rembourse. Si elle ne le fait pas, il peut même porter plainte ou refuser le paiement par carte de crédit. Cela apporte de la confiance dans l'achat. L'acheteur est certain d'obtenir son produit et si ce n'est pas le cas, il peut récupérer son argent. Il existe un système pour régler les différends, c'est le tribunal.

Sur le Darknet, il n'y a pas de tribunal, pas de personne que l'on peut poursuivre, impossible d'annuler une transaction en Bitcoins. Les sites ont donc mis en place des procédures pour donner aux acheteurs le maximum de confiance tout en protégeant l'anonymat des vendeurs.

Le premier mécanisme est similaire à tous les sites de vente, c'est la réputation. Pour chaque vendeur, le site publie la quantité de transactions effectuées ainsi que les avis des consommateurs. Chaque consommateur est appelé à donner son avis (c'est parfois obligatoire). Un acheteur potentiel peut donc voir si le vendeur a été sérieux et si la marchandise est de qualité.

Pour communiquer son adresse à un vendeur, les utilisateurs doivent encrypter celle-ci à l'aide de la clé publique du vendeur. Seul celui-ci possède la clé privée permettant de lire cette adresse. De cette manière, per-

sonne sur le site ne peut connaître l'adresse des clients. La clé publique du vendeur est comme sa carte d'identité. Il va utiliser la même sur tous les sites sur lesquels il est actif. Comme les sites sont régulièrement désactivés et saisis par les forces de police, la clé publique est utilisée pour transférer la réputation d'un site à un autre. On peut donc par exemple savoir sur Dream Market quelle était la réputation d'un vendeur sur Alpha Bay.

«Escrow» ou «multisig»?

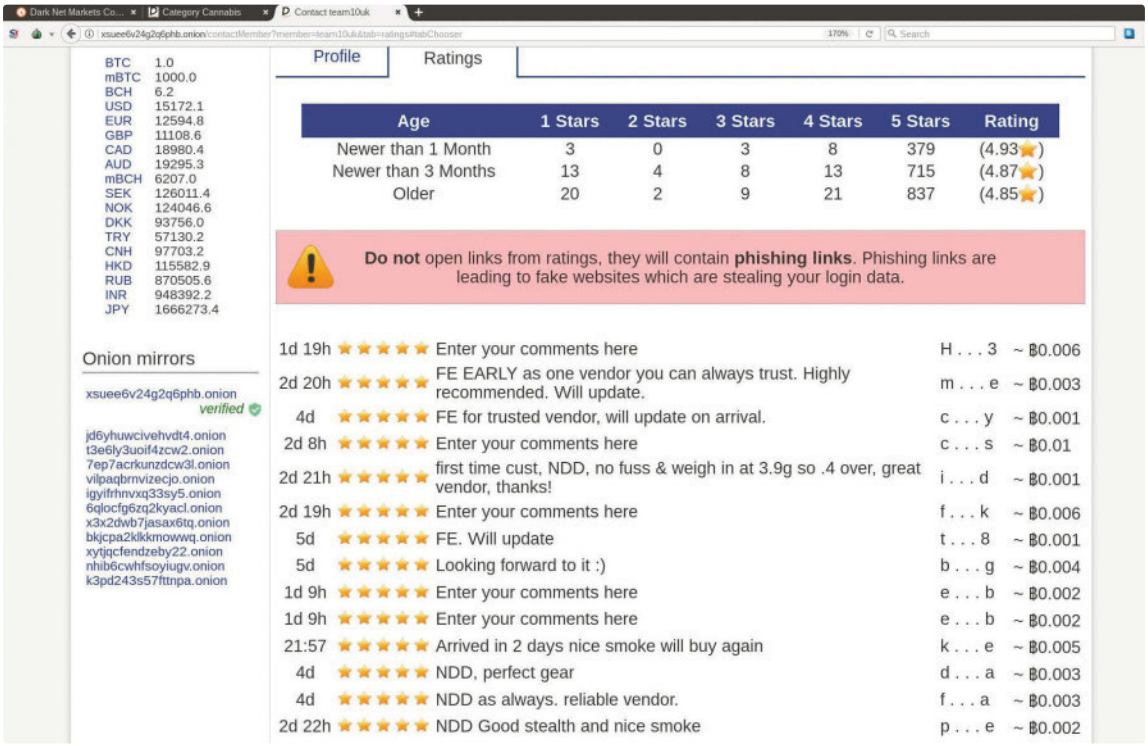
Une transaction en Bitcoins est irrévocable. Un acheteur ne peut donc pas refuser de payer un produit qui n'a pas été livré s'il a déjà payé en Bitcoins, mais si le vendeur envoie la marchandise avant son paiement, il ne peut pas non plus poursuivre l'acheteur s'il refuse de payer. Il existe deux méthodes assurant la sécurité de la transaction. Dans la première, on utilise le site comme un intermédiaire fiduciaire («escrow» en anglais). L'acheteur dépose l'argent sur un compte contrôlé par le site. Lorsque l'acheteur confirme avoir reçu le bien, l'argent est envoyé au vendeur. Le gros problème avec ce mécanisme est que les acteurs n'ont pas tous confiance dans le site. Certains administrateurs de sites sont partis en emportant la caisse, d'autres sites ont été saisis par les forces de l'ordre. Un autre système est utilisé pour sécuriser les paiements, il s'agit du système multisig de bitcoin. Dans ce système, trois acteurs (l'acheteurs, le vendeur et le site) créent un compte bitcoin. Ensuite, il faut l'accord de deux des trois pour utiliser l'argent déposé sur ce compte. Normalement, l'utilisateur confirme au site que la transaction s'est bien passée. Le site signe donc la transaction et l'envoie au vendeur qui n'a plus qu'à signer lui-même. En cas de désaccord entre acheteur et vendeur, le site est l'arbitre et peut décider qui reçoit quoi. Si le site fait défaut, l'acheteur et le vendeur peuvent disposer de l'argent.

Sans confiance, pas de commerce. Sur le Darknet, la confiance est une denrée rare. Chacun essaie de commercer avec un minimum de risques en vérifiant la réputation du vendeur, du site, en contrôlant le transfert d'argent. Cela ne suffit pas à rendre le Darknet sécurisé. De très nombreux acteurs ont intérêt à ce que des transactions se passent mal: des escrocs qui souhaitent gagner vite de l'argent, des concurrents qui veulent vendre leurs produits, des sites concurrents qui souhaitent empêcher les sites de fonctionner pour récupérer le marché et aussi les services de police qui souhaitent infiltrer et désactiver ces sites. Des intérêts très grands sont en jeu pour des acteurs très puissants. Les risques d'être la victime d'une attaque malveillante sur ces sites sont très élevés. Les précautions à prendre pour rester relativement en sécurité sur le Darknet dépassent largement les compétences d'un utilisateur lambda.

Anonymat, sécurité des transactions, réputations, ces techniques utilisées sur le Darknet peuvent aussi être très utiles dans la vraie vie. Adapter certaines de ces méthodes aux domaines de la banque, du e-commerce ou de la e-health est un challenge très stimulant.

Contact:
– emmanuel.benoist@bfh.ch

Infos:
– risis.bfh.ch
– ti.bfh.ch/informatique



Evaluations pour l'utilisateur team10uk sur le site Dream Market