Accueil – INFO-DU-CONTINENT.COM

Accueil – INFO-DU-CONTINENT.COM

Actualités Nigéria – Interdiction formelle de l'usage des monnaies (…) Gambie – Amnistie totale pour Yahya Jammeh Afrique – Une nouvelle chenille menace l'agriculture sur le (…) Ethiopie – Hailemariam Dessalegn, invité du AFRICA CEO FORUM (……[Lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement..
(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur sur cette page.

Réagissez à cet article

Bitcoin est-il suffisamment anonyme ?

Bitcoin est-il suffisamment anonyme ?

L’anonymat de Bitcoin lui a valu nombre d’adhérents parmi les anarchistes et les trafiquants de drogue à travers le monde. Mais il semble maintenant que cette monnaie numérique n’est plus assez anonyme……[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l’étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages…) pour mieux s’en protéger** (Autorisation de la Direction du travail de l’Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d’informations sur sur cette page.

Réagissez à cet article

Bitcoin est-il suffisamment

anonyme ?

Bitcoin est-il suffisamment anonyme ?

L’anonymat de Bitcoin lui a valu nombre d’adhérents parmi les anarchistes et les trafiquants de drogue à travers le monde. Mais il semble maintenant que cette monnaie numérique n’est plus assez anonyme……[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l’étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages…) pour mieux s’en protéger** (Autorisation de la Direction du travail de l’Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d’informations sur sur cette page.

Réagissez à cet article

Le bitcoin victime d’une faille dans le système ?

Le bitcoin victime d’une faille dans le système ?

Bitfinex, plus grande place d'échange de bitcoins en dollars, suspend son activité après le vol de près de 120 000 bitcoins dans son système. La cryptomonnaie a perdu 5,5 % de sa valeur dans la journée.

La plateforme de change hongkongaise Bitfinex a annoncé mardi dans un communiqué avoir « *découvert une faille de sécurité qui l'oblige à geler toute transaction* […] *ainsi que tout dépôt et retrait de fonds* ». « *Je peux confirmer que la perte à la suite du hack est de 119 756 BTC* », a déclaré Zane Tackett, CTO du groupe, sur Reddit. Au cours actuel de 540 dollars pour un bitcoin, la valeur des bitcoins qui se sont volatilisés s'élève à environ 65 millions de dollars.

En noir, la valeur d'échange du bitcoin au dollar (échelle de droite). En vert et en rouge, les volumes des transactions (échelle de gauche en milliers de bitcoins).

Le cours du bitcoin a perdu 5,5 % contre le dollar dans la journée de mardi, soit une chute de 13 % en deux jours. La valeur de la cryptomonnaie avait cela dit perdu 6,2 % lundi, sans que le lien avec le hack soit avéré. C'est au total l'équivalent de 1,5 milliard de dollars qui s'est évaporé de la capitalisation marchande du bitcoin cette semaine.

Avant l'incident, Bitfinex était la plus grosse plateforme de change avec le dollar, totalisant 8,5 % de tous les échanges de bitcoins. Elle était néanmoins derrière le chinois OKCoin, dont 90 % du trading s'effectue en yuans.

LES ATTAQUANTS DOIVENT COMPROMETTRE LES DEUX ORGANISATIONS AVANT D'OBTENIR LES FONDS

La plateforme hongkongaise assure sa sécurité avec BitGo, une firme basée à Palo Alto (Californie), via un système de multi-signature. Lors du partenariat, Bitfinex avait déclaré que grâce à un tel procédé, « les attaquants doivent compromettre les deux organisations avant d'obtenir les fonds ». Aujourd'hui, BitGo affirme ne pas avoir découvert de brèches de son côté.

En février 2014 s'était déjà produit un événement similaire d'une ampleur bien plus grave. La plateforme tokyoïte Mt.Gox, où s'échangeaient à l'époque 70 % des bitcoins du monde, avait également affirmé avoir été victime de pirates : 744 408 bitcoins, soit 450 millions de dollars selon la valeur du cours au moment de l'incident, avaient été dérobés au système.

Depuis, MtGox a mis la clé sous la porte après de forts soupçons sur son honnêteté, et qui perdurent encore aujourd'hui. En l'espace d'un mois, la cryptomonnaie avait plongé 30 % mais, habituée à une volatilité extrême, elle s'en était vite remise.

Article original de Victoria Castro

Réagissez à cet article

Original de l'article mis en page : Le bitcoin dévisse après un piratage à 65 millions de dollars — Business — Numerama

Satana, un ransomware pire que Petya

	Satana, un ransomware pire que Petya

Le nouveau rançomware Satana cumule chiffrement des fichiers et remplacement du secteur d'amorçage du disque.

Une nouvelle génération de ransomware est en train d'émerger. Satana, nom du nouveau malware, combine chiffrement des fichiers et écriture de code sur le secteur d'amorçage du disque, le MBR. Deux techniques inspirées de Petya et Mischa, note Malewarebytes qui constate la croissance du nouvel agent satanique ces dernières semaines.

« Satana fonctionne en deux modes, note la société de sécurité sur son blog. *Le premier se comporte comme Petya, un fichier exécutable (sous Windows, NDLR) [et] écrit au début du disque infecté un module de bas niveau, un bootloader avec un noyau personnalisé. Le deuxième mode se comporte comme un ransomware typique et chiffre les fichiers un par un (tout comme Mischa). »* Mais à la différence que les deux modes ne sont pas exploités alternativement mais bien appliqués ensemble, l'un après l'autre, pour s'attaquer à leurs victimes.

Payer ne garantit rien chez Satana

Malwarebytes ne le précise pas mais le mode de propagation de Satana reste probablement classique. A savoir par e-mail (et éventuellement d'un expéditeur en recherche de travail avec des liens vers les fichiers infectieux comme dans le cas de la première version de Petya). Une fois le MBR remplacé, le malware s'attaque au chiffrement des fichiers du disque (et des éventuels volumes reliés à l'ordinateur) et attend patiemment que le système soit redémarré. Quand c'est le cas, un message s'affiche sur l'écran expliquant la démarche à suivre pour récupérer l'accès à son PC, à savoir le paiement d'une rançon de 0,5 bitcoin (plus de 300 euros au cours du jour).

Si l'utilisateur parvient néanmoins à remplacer le MBR par un fichier d'amorçage sain (une manipulation manuelle qui est loin d'être à la portée de tout le monde), il se heurtera aux fichiers chiffrés sur le disque. Lesquels ont été renommés avec, en en-tête du nom, un e-mail aléatoirement choisi parmi ceux de l'équipe des développeurs de Satana, selon l'expert en sécurité (Gricakova@techmail.com, dans l'exemple présenté). Et les méthodes de chiffrement semblent suffisamment avancées pour rendre les fichiers piégés définitivement irrécupérables. D'autant que Malewarebytes pointe un bug pour le moins problématique pour la victime. De par le mécanisme de chiffrement/déchiffrement des fichiers, en cas de déconnexion au serveur de commandes et contrôle (C&C), la clé de décryptage (qui est la même que pour le cryptage) est perdue. Brisant tout espoir de la victime à pouvoir récupérer ses données (sauf à avoir fait préalablement des sauvegardes). *« Même les victimes qui paient peuvent ne pas récupérer leurs fichiers si elles (ou le C&C) sont hors ligne lorsque le chiffrement arrive »*, prévient la société de sécurité.

Du code en cours de perfectionnement

Ce n'est pas la seule bizarrerie que remarque le chercheur Hasherezade, auteur du billet. Il constate également que, le ransomware affiche toute la procédure de son déploiement, y compris la progression du chiffrement des fichiers. *« Habituellement les auteurs de logiciels malveillants ne veulent pas laisser le code de débogage dans leur produit final »*, écrit le chercheur. Lequel conclut que Satana est probablement encore en cours de développement et contient des failles. *« Le code d'attaque de bas niveau semble inachevée – mais les auteurs montrent un intérêt dans le développement du produit dans ce sens et nous pouvons nous attendre que la prochaine version sera améliorée. »* Une nouvelle génération de rançongiciel est bien en marche.

Article original de Christophe Lagane

Réagissez à cet article

Original de l’article mis en page : Satana, un ransomware pire que Petya

---

24.000 bitcoins saisis par la police vendus aux enchères

24.000 bitcoins saisis par la police vendus aux enchères

La police Australienne va mettre aux enchères, le 20 juin 2016, 24.000 bitcoins saisis dans des affaires criminelles. Montant du lot, plus de 15.000 euros.

15 882 euros de bitcoins saisis par la justice (24,500 BTC) vont être mis aux enchères, le 20 juin, par la police australienne. De l'argent « dématérialisé » qui sera mis en vente le 20 juin 2016. Pour les autorités, cet argent « virtuel » doit être converti en monnaie sonnante et trébuchante afin de le reverser à l'autorité fiscale locale. Ces bitcoins ont été saisis dans des affaires criminelles et la police a décidé de passer par le mode enchères publique pour s'en débarrasser. C'est la société Ernst & Young qui va se charger de la vente. Ca sera la deuxième vente mondiale de ce type de « produit ».

24.000 Bitcoins saisis

Je vous révélais, en 2014, comment la police fédérale américaine des US Marshall avait revendu pour treize millions de dollars de Bitcoins (144.000 BTC), soit l'équivalent de 8.431.689 euros, dans une vente aux enchères qui commercialisait les BTC du propriétaire de Silk Road, Ross Ulbricht, une boutique du blackmarket spécialisée dans la commercialisation de drogue.
Les bitcoins australiens, ils sont au nombre de 24.518, ont été confisqués en décembre 2013 dans une affaire de drogue, à Melbourne. Son propriétaire, Richard Pollard, 32 ans, a été condamné en octobre 2015, à 11 ans de prison pour trafic de drogue… sur le site Silk Road. Les bitcoins seront vendus par lots d'environ 2.000 BTC… [Lire la suite]
Article original de Damien Bancal

Réagissez à cet article

Source : *ZATAZ Vente aux enchères de 24.000 bitcoins saisis par la police – ZATAZ*

Faut-il adapter la blockchain à la cybersécurité ?

Faut-il adapter la blockchain à la cybersécurité ?

En suivant l'actualité des nouvelles technologies, il est difficile de passer à côté d'un nouveau « buzz world » qui enflamme les débats : Blockchain ou chaîne de blocs en français. Initialement inventée pour les crypto-monnaies (comme Bitcoin par exemple), la technologie blockchain connait un développement rapide (même la banque de France lance une étude sur l'architecture blockchain) et certains prédisent même une révolution comparable à l'invention du protocole TCP-IP. Il nous a semblé utile de creuser un peu cette technologie afin d'imaginer son impact potentiel dans le domaine de la cybersécurité.

La blockchain Késako ?

Le concept de la chaine de blocs repose sur la décentralisation par opposition à un système pyramidal et hiérarchisé. La chaine permet de regrouper l'ensemble des transactions effectuées par ses membres depuis sa création. Il s'agit en quelque sorte d'un grand livre de compte, anonyme et infalsifiable (certaines chaines sont publiques et d'autres privées).

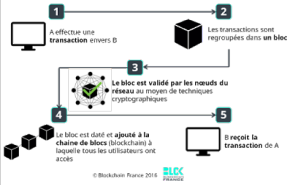
(Image issue du site: blockchainfrance.net)

Le site présente alors le système comme suit:

Toute blockchain publique fonctionne nécessairement avec une monnaie ou un token (jeton) programmable. Bitcoin est un exemple de monnaie programmable.

Les transactions effectuées entre les utilisateurs du réseau sont regroupées par blocs. Chaque bloc est validé par les noeuds du réseau appelés les "mineurs", selon des techniques qui dépendent du type de blockchain. Dans la blockchain du bitcoin cette technique est appelée le "Proof-of-Work", preuve de travail, et constitue en la résolution de problèmes algorithmiques..

Une fois le bloc validé, il est horodaté et ajouté à la chaîne de blocs. La transaction est alors visible pour le récepteur ainsi que l'ensemble du réseau.



*Plusieurs techniques existent pour « valider » un bloc. Bitcoin utilise la « **proof of work** » – PoW- (preuve de travail) où chaque noeud (mineur) doit effectuer un calcul cryptographique, mais d'autres utilisent la « proof of stake« (PoS) où l'utilisateur doit faire la preuve qu'il détient une certaine quantité de monnaie partagée. Le projet **Ethereum** tente de faire basculer le PoW vers une forme de PoS. **La question de la validation par la communauté est essentielle dans le concept de blockchain, il en est l'essence mais également la fragilité**. En effet, cette étape engendre un temps de latence (jusqu'à 15 min pour Bitcoin) qui rend difficile l'implémentation généralisée de ces techniques. En outre, les « mineurs » consomment de l'énergie à effectuer des calculs cryptographiques inutiles, en clair le PoW ne produit rien (à part de la chaleur et une bonne facture d'électricité).*

Pourquoi faut-il adapter la blockchain à la cybersécurité ?

Que peut-on retenir de cette présentation rapide? En premier lieu la technologie Blockchain permet de supprimer les intermédiaires et les autorités centrales en favorisant un système totalement distribué. En matière de sécurité des systèmes d'information de nombreuses applications reposent sur une « autorité de certification » (signature électronique, certificats etc…). Cette dernière est garante de la confiance entre tiers lors des échanges (messagerie, commerce, déclarations en ligne, vote…), dans ce contexte, blockchain pourrait largement modifier notre environnement. Au sein d'une structure (entreprise ou administration) la sécurité des échanges pourrait ainsi être garantie par la mise en place d'une chaine locale (qui a en outre l'excellente idée d'être auditable).

*Un des développement récent de la blockchain réside dans la notion de « **smart contracts**« :*

les smart contracts sont des programmes, accessibles et auditables par toutes les parties autorisées, dont l'exécution est donc contrôlée et vérifiable ; conçus pour exécuter les termes d'un contrat de façon automatique lorsque certaines conditions sont réunies. Les règles qui régissent le programme peuvent notamment recouvrir tout événement vérifiable de façon informatique

*On peut donc imaginer un développement permettant d'améliorer la détection d'intrusion en implémentant la technologie blockchain au sein même d'un réseau d'entreprise. La confiance entre machines reposerait alors sur des « **smart contracts** » qui, lorsqu'ils sont rompus (machine compromise) déclencheraient des mécanismes d'alerte.*

*Outre la détection d'intrusion au sein d'un réseau de confiance « monitoré » par une blockchain, les applications les plus triviales devraient voir le jour dans les échanges entre systèmes connectés. Là encore, le double intérêt de la technologie repose sur la notion de **confiance décentralisée** et de**traçabilité** deux aspects essentiels pour la cybersécurité.*

La route est encore longue…

En dépit de nombreux avantages et de promesses alléchantes, la technologie blockchain est encore en phase d'expérimentation dans bien des domaines et ne semble pas (à ce jour) en mesure de « passer à l'échelle » pour des applications immédiates en matière de cybersécurité (détection d'intrusion, prévention des attaques etc.). Les limites juridiques ne manqueront pas d'émerger, les tentatives de détournements et de contrôle pour revenir à un état ante en « étoile » et contrôlé sont autant d'obstacles sur le chemin.

Enfin, les expérimentations devront chercher à valoriser l'étape de validation afin de limiter l'empreinte énergétique de cette technologie. Si sous bien des aspects la comparaison avec l'arrivée de TCP-IP est valable, le « modèle blockchain » semble toutefois porteur de changements plus profonds. Le monde de la cybersécurité devrait sans nul doute se lancer rapidement dans la course et expérimenter de nouvelles techniques de défense… [Lire la suite]

Pour aller plus loin:

https://blockchainfrance.net/

https://www.ethereum.org/

https://fr.wikipedia.org/wiki/Cha%C3%AEne_de_blocs

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, arnaques Internet…) et judiciaires (contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Suivez-nous sur

Réagissez à cet article

Source : *Cybertactique: BlockChain et cybersécurité, en route vers une révolution ?*

La face cachée du Web caché, le « dark Web »

	La face cachée du Web caché, le « dark Web »

Le «dark Web», dont les utilisateurs sont anonymes et intraçables, est utilisé, pour le pire et pour le meilleur, par des trafiquants d'armes autant que par des dissidents opprimés par les États totalitaire.

«Sur Internet, on peut acheter une kalachnikov en deux clics.» Pour qui n'y connaît rien, ce genre de phrases, entendues à la radio ou à la télévision, interroge.

Depuis les attentats de janvier notamment, Internet (1) est au cœur des préoccupations. «Dans quelle mesure, Internet et le Web profond sont-ils utilisés pour recruter, communiquer et préparer des actions criminelles?», interrogeait Nathalie Goulet, présidente de la commission d'enquête sénatoriale sur les réseaux djihadistes, lors d'une table ronde fin janvier.

Web profond, Web sombre ou dark Web… Tous ces termes renvoient à une même idée: il existerait un espace sombre, caché et donc suspect, dans lequel chacun pourrait, en quelques minutes, se procurer une arme ou de la drogue. De fait, à première vue, la chose n'est pas bien compliquée.

Pour commencer, il faut télécharger sur son ordinateur un navigateur personnalisé, libre et gratuit, comme TOR par exemple (pour The Onion Router). Ses paramètres permettent la connexion au réseau TOR. L'intérêt? Alors qu'habituellement, un utilisateur surfant sur Internet dispose d'une adresse IP, sorte de plaque d'immatriculation de son ordinateur, TOR brouille l'adresse IP de l'utilisateur.

«Les criminels ont recours à ce type de technologie pour anonymiser leurs échanges d'informations, ne pas être identifiés ni localisés, et de ce fait, ne pas être inquiétés par les forces de l'ordre, explique Solange Ghernaouti, directrice du Swiss Cybersecurity Advisory & Research Group, à l'Université de Lausanne. En rendant impossible la surveillance ou les filatures numériques, TOR permet l'anonymat et d'avancer masqué dans l'Internet.»

Une fois sur TOR, pas de moteur de recherche. Sur TOR, on ne trouve que ce que l'on sait chercher: il faut directement taper l'adresse du site souhaité dans la barre d'adresse. Pourquoi? Pour comprendre ce point, il faut s'imaginer Internet comme un iceberg. La partie immergée, la plus connue, est celle où nous avons l'habitude d'aller et dont les pages sont agrégées par des moteurs de recherche, comme Google. On y lit nos mails, on y achète des produits, on y fait des recherches… C'est l'Internet «surfacique», une petite partie d'Internet.

Sous la surface, on trouve le Web profond, qui contient les pages non indexées par les moteurs de recherche parce qu'elles sont mal conçues, non reliées, protégées par leur créateur… C'est le même Internet, mais en moins balisé.

Enfin vient le dark Web, ou plutôt les dark Nets, c'est-à-dire un ensemble de réseaux virtuels privés et décentralisés, constitués par des internautes qui se connectent entre eux.

Comment donc trouver une arme quand on n'y connaît rien? En récupérant des adresses de sites sur des forums, entre initiés. Ou grâce à des annuaires collaboratifs, référençant des adresses sous forme thématique, comme The Hidden Wiki (le «wiki» caché). Voulez-vous acheter un passeport? Rendez-vous à telle adresse. Des armes, de la drogue? Ce sera par là. Ainsi, on peut rapidement trouver un passeport français pour 600 € ou un pistolet SIG Sauer de calibre 9 mm pour 790 €.

Concrètement, pour acheter sur le dark Net, il a fallu à peine plus de deux clics: rechercher des adresses sur un annuaire, télécharger TOR, le lancer puis rentrer l'adresse dans la barre de navigation.

De là à acheter le produit, il reste encore quelques pas… Sur le dark Net en effet, les prix sont donnés en euros, mais les achats se font en bitcoins, une monnaie virtuelle et chiffrée, échangée entre deux ordinateurs. Datant de 2009, ce système fonctionne sans les États et sans les banques. Il est possible d'acheter ou de vendre des bitcoins contre des devises ayant cours légal, sur des plates-formes en ligne. Payer en bitcoin permet donc d'effectuer des transactions de personne à personne dans le monde entier, sans intermédiaire et à moindres frais. Ces échanges sont publics mais anonymes. Une fois son porte-monnaie approvisionné, il reste à se créer un compte client, comme sur eBay ou Amazon.

Mais attention, comme sur le Web surfacique, les escroqueries prolifèrent: sans régulation, ni contrôle, difficile de savoir si l'on peut faire «confiance» à un vendeur. De plus, les adresses changent sans arrêt, pour des raisons pratiques, techniques ou de sécurité, les rendant rapidement obsolètes.

Au final, le dark Web reste donc le domaine des initiés et des mafieux. D'ailleurs, alors qu'Internet compte cinq milliards d'utilisateurs, TOR en compterait deux millions quotidiens. Parmi eux, plusieurs profils. Il y a, bien sûr, les délinquants, trafiquants, hors-la-loi, parfois les mêmes que l'on retrouve dans le monde réel. Pour eux, Internet est un «facilitateur de la performance criminelle», selon Solange Ghernaouti: «Internet reflète notre réalité sociale, économique, politique et criminelle, poursuit-elle. Il n'est ni pire ni meilleur, mais contribue à faciliter certaines actions, y compris le passage à l'acte criminel du fait de la dématérialisation – on agit caché derrière un écran – à distance.»

Mais on trouve aussi sur le dark Net tous ceux qui veulent communiquer à l'abri des regards, les «internautes soucieux de préserver leur vie privée et leur intimité numérique ou les cyberdissidents à des régimes non démocratiques», poursuit le professeur. Tout un volet positif du dark Net, mais dont on parle beaucoup moins.

———

LES MOTS POUR COMPRENDRE

Internet représente un réseau de télécommunication international reliant des ordinateurs à l'aide du protocole TCP/IP. Il sert de support à la transmission de données: pages Web, courriels, fichiers informatiques.

Une adresse IP (Internet Protocol) est un numéro d'identification attribué à chaque appareil connecté à un réseau informatique utilisant l'Internet Protocol. Une adresse IP est un numéro unique permettant à un ordinateur de communiquer dans un réseau.

Un moteur de recherche est un site Internet régi par une application sur lequel, en entrant des mots-clés, on obtient une liste de sites correspondant à la demande. Exemple: Google.

Un réseau virtuel privé est un passage ou un lien qui permet d'ouvrir un réseau local vers l'extérieur et de le connecter à un autre réseau local, grâce à une connexion Internet et avec une sécurité optimisée.

Le wiki est une application Web participative dont les internautes peuvent modifier les contenus.

Le terme bitcoin (de l'anglais « bit », unité d'information binaire, et « coin », pièce de monnaie) désigne à la fois un système de paiement virtuel et l'unité de compte utilisée par ce système.

Le chiffrement est une technique d'écriture en langage crypté ou codé. C'est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant de clés.

Réagissez à cet article

Source : http://www.la-croix.com/Ethique/Sciences-Ethique/Sciences/La-face-cachee-du-dark-Web-2015-12-08-1390141

Le créateur du bitcoin enfin démasqué ?

	Le créateur du bitcoin enfin démasqué ?

Une partie de la presse croit avoir mis la main sur le créateur du bitcoin. Connu sous le pseudonyme Satoshi Nakamoto, le père de la monnaie virtuelle, s'appellerait en réalité Craig Steven Wright.

L'identité du créateur du bitcoin passionne une partie de la presse américaine. Deux nouveaux sites affirment avoir découvert la personne qui se cache derrière la monnaie virtuelle. Il ne s'agirait pas d'un japonais mais d'un homme d'affaires australien, basé à Sydney.

On doit l'invention du bitcoin à un développeur connu sous le nom de Satoshi Nakamoto. Un pseudonyme qui lui a permis de demeurer loin de l'agitation et de toute caméra. Toutefois, sa véritable identité n'a jamais été exposée au grand jour. C'est pourquoi Gizmodo.com et Wired ont mené l'enquête afin de découvrir le nom du père du bitcoin.

Si les deux sites estiment savoir qui est le créateur de la monnaie, ils demeurent cependant prudents quant à leurs affirmations. Selon leurs informations, Craig Steven Wright aurait mis au point le bitcoin. Il aurait été épaulé d'un second collaborateur, en la personne de Dave Kleiman, un développeur américain dont le décès remonte à 2013.

La police australienne perquisitionne

Ces nouveaux éléments sont rapidement remontés aux oreilles des autorités australiennes. Suite à la publication de ces informations, la police du pays a procédé à la perquisition du domicile de Craig Steven Wright. Une célérité étonnante mais à laquelle la police a tenu à apporter un démenti. Cette visite impromptue ne serait pas due à ces révélations mais à une enquête liant l'homme d'affaires au fisc australien.

De leur côté, Gizmodo.com et Wired indiquent que leurs informations proviennent d'une série de courriers électroniques échangés entre Wright et son collaborateur mais également du cache de son blog personnel. Des publications, effacées depuis, font directement référence à la monnaie virtuelle.

Ainsi en janvier 2009, soit peu de temps après la sortie des premiers bitcoins, l'homme publiait un billet précisant que « la bêta de Bitcoin est en ligne aujourd'hui. C'est décentralisé… on essaye jusqu'à ce que ça marche ».

Plus tard, en 2011 Craig Wright évoquait le pseudonyme « Nakamoto » nommément dans un e-mail. « Je ne peux plus faire le Satoshi. Ils n'écoutent plus. Je suis mieux en tant que mythe. Retour à mes cours, mes gueulantes et au fait que tout le monde m'ignore. J'ai horreur de ça Dave, mon pseudonyme est plus populaire que je n'aurais jamais pu espérer », précisait-il.

Une chasse à l'homme et de grosses incertitudes

La recherche de Satoshi Nakamoto a déjà connu des ratés. En mars 2014, le magazine Newsweek avait cru tenir l'identité du père du bitcoin en la personne de Dorian Satoshi Nakamoto. Le japonais de 64 ans résidant aux Etats-Unis avait démenti être le créateur de la crypto-monnaie. L'homme était même allé plus loin en affirmant qu'il comptait attaquer le magazine américain devant les tribunaux suite à la publication de propos qu'il juge mensongers. L'ingénieur avait entrepris de lever des fonds pour soutenir sa cause. Pour éviter de telles nouvelles incertitudes, la presse américaine précise uniquement avoir obtenu des informations émanant d'une source anonyme.

Un hoax de haute volée ?

Face à la publication de ces nouvelles informations, les journalistes prennent des précautions nécessaires. Les documents mis en ligne par les auteurs de cette révélation ne peuvent, pour le moment, pas être clairement authentifiés et plusieurs incertitudes planent encore sur les implications réelles des deux individus dans la création de la monnaie virtuelle.

Les données présentées par Gizmodo.com et Wired doivent donc restées sujettes à caution. Une partie de la vérité pourrait être trouvée par les autorités britanniques. Craig Steven Wright aurait quitté l'Australie pour déménager à Londres. Si la police décide de poursuivre l'affaire, elle pourrait interroger l'homme d'affaires pour démêler une partie des informations.

Réagissez à cet article

Source :

http://pro.clubic.com/it-business/securite-et-donnees/monnaies-virtuelles/actualite-789108-bitcoin-vrai-createur-australie-nakamoto.html

Le Bitcoin financerait le terrorisme

	Le Bitcoin financerait le terrorisme

Les pays européens prévoient d'attaquer le Bitcoin et d'autres modes de paiement anonymes telles que les cartes de crédit prépayées parce qu'ils permettent aux terroristes de financer leurs attaques.

Reuters prétend que les pays européens préparent un projet pour contrer le Bitcoin et d'autres modes de paiement anonymes.

On a le Bitcoin, mais également les cartes de crédit prépayées.

Les ministres de la justice et de l'intérieur de nombreux pays européens vont se réunir la semaine prochaine à Bruxelles afin de voter de nouvelles mesures pour contrer le terrorisme en Europe.

Il y a de nombreuses mesures pénales, mais il y a également un projet pour attaquer les paiements anonymes. Selon les informations obtenues par Reuters, une réunion préliminaire a déjà eu lieu et elle a proposé de meilleurs contrôles sur le Bitcoin, les cartes de crédit prépayées, l'or et les métaux précieux. Notons que l'or ne sera pas directement attaqué (ce serait trop évident), mais il sera interdit d'utiliser des paiements anonymes pour transférer de l'or ou d'autres métaux précieux (Les investisseurs sur les métaux précieux comprendront rapidement ce qui se trame).

Les ministres européens estiment également que le contrôle du Bitcoin et des paiements anonymes permettra de réduire le commerce des biens illicites.

Les attaques sur Paris ont eu le vendredi dernier. Samedi, on a déjà une déclaration de guerre de la part de la France, lundi, on a un projet de loi en France sur l'Etat d'urgence qui transforme ce pays en l'une des pires dictatures avec des pouvoirs de surveillance illimités. Mardi, les républicains aux Etats-Unis profitent de l'attaque sur Paris pour rejeter les réfugiés syriens à la mer, mercredi, les partis d'extrême-droite redoublent d'effort pour alimenter l'islamophobie et jeudi, on attaque le Bitcoin, les paiements anonymes, l'or et les métaux précieux, soit les principales épines dans le pied du système financier.

Est-ce qu'on sait que les terroristes ont utilisé le Bitcoin ? Est-ce que Daesh paie ses armes avec de l'or ? Est-ce que le Bitcoin est principalement utilisé par des criminels ? On a un triple non. En 5 jours, les politiciens américains et européens votent tout ce qu'ils peuvent pour faire chier leurs populations respectives pour les prochaines décennies. Il reste encore 2 jours… On craint le pire.

Réagissez à cet article

Source : http://actualite.houss
eniawriting.com/tech
nologie/2015/11/19/leurope-va-attaquer-le-bitcoin-
parce-quil-finance-le-terrorisme/10675/