CTRF CELLULE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER خلية معالجة الإستعلام المالي CTRF

LETTRE D'INFORMATION DES ACTUALITES INTERNATIONALES
DANS LE DOMAINE DE LA LUTTE CONTRE LE BLANCHIMENT D'ARGENT
ET LE FINANCEMENT DU TERRORISME

Lettre n°105

Monnaies virtuelles : Entre révolution technologique et spéculation financière

La monnaie virtuelle raisonne dans l'esprit de nombreux individus comme un moyen facile de gagner de l'argent, et attire de ce fait de plus en plus d'investisseurs. Créée en 2009, le Bitcoin est la crypto-monnaie de référence et continue de susciter aujourd'hui un intérêt croissant aux quatre coins du globe. Les monnaies virtuelles échappant aux banquiers centraux offrent une multitude d'avantages aux investisseurs mais ce marché, très volatil, est toutefois bien difficile à comprendre et peut s'avérer très risqué.Le Bitcoin et l'Ether, qui sont les deux crypto-monnaies les plus populaires, atteignent des plus hauts historiques depuis ce début d'année et la capitalisation de l'ensemble des crypto-monnaies a franchi au mois de juin, le cap significatif des 100 milliards de dollars. Le Bitcoin a également dépassé les 3.000 USD durant cette même période et l'Ether, les 400 USD, avant de retomber respectivement sous la barre des 2.600 et 260 USD.

Comment expliquer cette soudaine montée des cours et cet intérêt particulier pour les monnaies virtuelles depuis ce début d'année ?

ØUn effet de mode : la grande tendance ces derniers mois dans le milieu de la blockchain c'est : l'ICO (Initial Coin Offering). C'est un moyen pour les entreprises de lever des fonds rapidement tel que le crowdfunding (financement participatif). Selon la Blockchain France, « plus de 300 ICO sont attendues au cours de l'année 2017, contre 64 réalisées l'an passé ».

ØLe Japon et la Russie s'intéressent à la monnaie virtuelle : les deux pays ont légalisé le Bitcoin. Le Japon, en avance dans le secteur de la technologie, était prêt à adopter les monnaies numériques. De plus, la BoJ ne cesse d'imprimer des billets pour relancer son économie (politique monétaire accommodante), ce qui effraie les épargnants japonais. Ainsi, au lieu de placer leur argent dans une monnaie sous-évaluée, cela leur rapporte plus de le placer en cryptomonnaie. De nombreux magasins et distributeurs acceptent désormais les crypto-monnaies, comme par exemple la compagnie aérienne japonaise Peach Aviation qui accepte le paiement en Bitcoin.

ØLes cartes graphiques s'adaptent au monde de la cryptomonnaie : Afin de pouvoir miner* de nouveaux Bitcoins (ou autres monnaies virtuelles), les investisseurs utilisent des processeurs graphiques GPU (Graphics Processing Unit) ou des ASICS (Application Specific Integrated Circuits). Cela correspond à l' « ensemble de l'équipement matériel, mécanique, magnétique, électrique et électronique, qui entre dans la constitution d'un ordinateur » (cnrtl.fr) et permet de réaliser tous les calculs et d'ajouter une intelligence artificielle plus fiable. Les ASICS n'ont pas d'autre utilité que celle du minage, ces processeurs sont nettement plus puissants et consomment peu, néanmoins ils coûtent beaucoup plus chers. Puisque cette monnaie devient populaire, il y en a davantage en circulation et donc les calculs deviennent encore plus complexes. Les mineurs ont alors besoin d'augmenter, pour continuer à exploiter la blockchain, la puissance de calculs de leurs ordinateurs en s'appropriant de nouveaux GPU, toujours plus puissants. Nvidia et AMD, deux acteurs américains, se sont alors positionnés sur

ce marché grandissant, en proposant des nouveaux GPU spécialement dédiés au minage des cryptomonnaies.

ØUne valeur refuge : Entre la dépréciation du yuan (devise chinoise) face au dollar, la suppression des grosses coupures en Inde, l'élection de D. TRUMP, etc. la monnaie cryptée s'est imposée dans l'esprit de ces nouvelles générations comme une valeur refuge, ne nécessitant aucune intervention de banques centrales et résultant simplement de la confrontation de l'offre et de la demande. A noter que les générations Y et Z ont grandi avec les objets connectés, Internet, etc. et font davantage confiance en cette monnaie, qu'ils considèrent comme « stable » en période de crise (malgré la forte volatilité), plutôt que l'or par exemple.

Alors que la monnaie virtuelle prend de plus en plus d'ampleur et que le cadre géopolitique mondial est particulièrement instable (élections présidentielles, terrorisme, cybercriminalité et rançons), les autorités observent ce phénomène d'un œil attentif et le fossé se creuse entre les partisans et les anti monnaies virtuelles.

Les plus frileux parlent de… :

- … Flash krach, les investisseurs craignent une bulle spéculative sur les cryptomonnaies. En effet, le cours du bitcoin (ci-dessous en dollars, sur la célèbre plateforme Coinbase), a progressé de près de 200% depuis ce début d'année et a atteint un niveau record en juin dernier, avant de perdre plus de 18%. De nombreux investisseurs restent alors sur leur garde pensant que les prix sont déconnectés de la valeur réelle de la cryptomonnaie, du fait de l'emballement général et que celle-ci va chuter brutalement au moment de l'éclatement de la bulle (ce qu'elle aurait alors commencé à faire depuis le mois de juin ?).

Concernant l'Ether, elle a gagné plus de 6000% en quelques mois, avant de perdre 50% depuis son plus haut historique atteint mi-juin.

- … D'individus mal intentionnés : les transactions virtuelles sont en grande partie non traçables et anonymes, ce qui peut les inciter à utiliser cette monnaie dans le blanchiment d'argent, sur le darknet, ou dans le financement du terrorisme (selon Symantec, les ransomwares ont plus que triplé en 2016 et continuent de progresser cette année).
- … Consommation massive d'électricité, de batterie et de réseau (d'ailleurs, selon le site digiconomist.net, le Bitcoin et l'Ether consommeraient à eux deux l'équivalent d'une centrale nucléaire française).

Les pro-monnaies virtuelles … :

- … Pensent que les cours vont continuer de monter après la correction qu'elles subissent actuellement.
- … Mettent en avant le fait que certains pays ont une monnaie fortement indexée sur les matières premières (par exemple sur le pétrole), ainsi quand le cours de la matière première s'effondre, la monnaie du pays aussi, et la monnaie virtuelle peut alors paraître plus stable. Le système à base de blocs peut alors être utilisé pour comptabiliser de manière transparente et enregistrer à peu près n'importe quelle transaction.
- … Diront que son utilisation peut s'adapter à différents secteurs (notarial, assuranciel, etc.)
- … Trouvent l'utilisation de la cryptomonnaie rapide, discrète et mondiale.
- … Voient en la monnaie cryptée, une monnaie d'avenir. C'est une idée que partage notamment la Banque Privée Suisse Falcon, qui sera dès mercredi 19 juillet ravie de fournir à ses clients une gestion d'actifs de la blockchain (selon Reuters).
- … Sont optimistes à l'idée que la SEC réexamine le projet d'ETF basé sur le Bitcoin. Selon des informations de Reuters, elle se pencherait à nouveau sur la demande des frères Winklevoss.

Tous les arguments sont bons à prendre en compte car ce marché est complexe, il est donc nécessaire de disposer du maximum d'informations afin de bien connaître ce nouvel environnement. Avant de se lancer, il faut tout d'abord savoir pourquoi investir dans une

monnaie virtuelle ? A quelles fins ? Pour savoir combien et comment investir. Il est également nécessaire de prendre en compte le fait qu'elles soient fortement volatiles et qu'il vaut donc mieux éviter les effets de levier, qui pourraient faire perdre beaucoup d'argent. La plateforme d'échange est alors à choisir avec attention, car la cotation peut différer en passant de l'une à l'autre et pour éviter les plateformes CFD.
Concernant la sécurité de ses transactions, elle est assurée par la Blockchain (comprendre son fonctionnement dans cet article : l'Ether est-il le nouveau Bitcoin?), néanmoins les fraudes et les manipulations sont possibles et se font le plus souvent via des emails (contenant la plupart du temps des pièces jointes) propageant des virus.
*Le mining, c'est le fait qu'un individu mette à disposition du réseau son ordinateur, et que celui-ci, ajouté aux ordinateurs des autres membres, contribue à la maintenance du réseau. Grâce à leur puissance de calcul commune, avant qu'une transaction soit effectuée, des vérifications concernant l'historique des transactions passées, la véracité des informations, etc. sont effectuées, et si tout est bon, l'opération se réalise et la monnaie virtuelle est échangée. Ainsi, les individus sont considérés comme des « mineurs », et sont rémunérés en cette monnaie.
https://www.zonebourse.com/actualite-bourse/Monnaies-virtuelles-Entre-revolution-technologique-et-speculation-financiere--24747128/

Escroqueries financières : les précautions à prendre pour se protéger

Les escroqueries financières revêtent différentes formes. Comment s'en protéger ? La Financial Services Commission (FSC) et Hemraj Bootun, Senior Manager d'Agileum, nous en disent plus.
Pyramides de Ponzi, 'pump and dump' ou encore 'boiler rooms'. Ce sont les différentes formes d'escroquerie qui existent. Dans le cas d'une pyramide de Ponzi, indique-t-on à la FSC, les escrocs proposent des retours sur investissements importants.
Ils paient les intérêts des premiers clients avec les placements des suivants jusqu'à ce que les nouveaux entrants ne suffisent plus à payer les intérêts des anciens. Dans le cas des 'pump and dump', les escrocs achètent à la Bourse les actions d'une entreprise dont le cours est bas. Puis, ils en vantent le potentiel pour inciter des investisseurs à en faire de même. Le prix de l'action grimpe et ils revendent leurs actions en dégageant des plus-values. Pour les escrocs, les 'boiler rooms' consistent à vendre des actions d'entreprises fictives ou surévaluées.
« Lorsqu'un individu reçoit des informations sur des investissements, il doit rester prudent et ne doit pas répondre sans s'être fait conseiller. Nous recommandons de n'investir qu'auprès d'opérateurs licenciés dont les listes sont disponibles sur les sites internet de la FSC et de la Banque de Maurice (BoM) », prévient la FSC.
Certains signes doivent alerter les investisseurs, comme des promesses de retours importants sur investissements, des profits garantis, des investissements sans risque et des pressions pour investir rapidement. Lors de retraits aux guichets automatiaues (ATM) ou de paiements par carte bancaires, il est recommandé de cacher le clavier lors des saisies des codes.

Les cyber-attaques

Avec le développement d'Internet, les escroqueries ont lieu plus couramment en ligne. Il s'agit de cyber-attaques sous différentes formes. Selon Hemraj Bootun, Senior Manager d'Agileum, on trouve par exemple le phishing' et les rançongiciels. Le phishing se réfère aux cas où des escrocs se font passer pour des institutions connues comme des banques pour soudoyer des informations confidentielles comme les mots de passe. Ils s'en servent ensuite pour débiter des comptes bancaires. Les rançongiciels sont des virus qui cryptent les données

d'ordinateurs. Afin de récupérer les informations, les fichiers et les données, les victimes sont invitées à verser des rançons.
Hemraj Bootun dira qu'avec des règles élémentaires, les risques sont minimisés. « Sauvegardez vos données sur CD-ROM, clé USB, disque dur externe ou en ligne. Faites régulièrement plusieurs copies des données les plus sensibles. Ayez un antivirus de dernière génération à jour et utilisez-le aussi pour scanner les pièces jointes des emails.
Installez un pare-feu. Procédez régulièrement aux mises à jour des logiciels. Ne communiquez jamais vos données personnelles. Vos mots de passe doivent être longs et composés de chiffres, lettres et caractères spéciaux. Votre mot de passe privé doit être différent de celui de votre travail », conseille l'expert.
http://defimedia.info/escroqueries-financieres-les-precautions-prendre-pour-se-proteger

Le rançongiciel existe depuis presque 30 ans, alors pourquoi on ne panique que maintenant ?

Mardi 27 juin, un rançongiciel répondant au petit nom de NotPetya a infecté des milliers d'ordinateurs partout dans le monde. Particulièrement virulent, le rançongiciel ne date pourtant pas d'hier.
Le rançongiciel n'est pas nouveau. Le *malware*, ou logiciel malveillant, qui chiffre des données et demande des paiements en échange des clés de déchiffrement, existe depuis presque 30 ans.
En un clin d'œil, le rançongiciel est passé d'une obscure menace pesant sur un petit groupe à un fléau mondial s'attaquant aux hôpitaux, aux banques, aux systèmes de transports et même aux jeux vidéo. Cette soudaine augmentation d'attaques au rançongiciel ne semble pas s'atténuer, laissant de plus en plus de victimes désarmées. Pourquoi ? Vraisemblablement à cause de la cryptomonnaie et de l'Agence de sécurité nationale américaine (NSA).

Un peu d'histoire

La première attaque au rançongiciel enregistrée a ciblé le secteur de la santé et remonte à 1989. D'après le blog dédié à la cybersécurité Practically Unhackable, un biologiste du nom de Joseph Popp a envoyé près de 200 000 disquettes à d'autres chercheurs, arguant qu'elles contenaient un sondage qui aiderait les scientifiques à déterminer les risques qu'avait un patient d'attraper le virus du SIDA.
Ce qu'il oublie de dire, c'est que chaque disquette chiffre aussi les noms de fichiers sur les ordinateurs infectés – les rendant inutilisables. Plutôt qu'un écran de démarrage, les victimes voient apparaître un message exigeant 189 dollars pour débloquer le système.
Joseph Popp, docteur à Harvard, est un biologiste évolutionniste mais pas un hacker à proprement parler. D'après The Atlantic, le scientifique a expliqué qu'il avait l'intention de donner tout l'argent récolté à la recherche pour le SIDA, après avoir été arrêté et accusé de chantage.
Au-delà du débat autour de ses véritables intentions, le succès de son attaque est alors limité par deux facteurs : les disquettes ont besoin de la poste pour être envoyées, et le chiffrement utilisé, connu désormais sous le nom de PC Cyborg, est réversible sans avoir recours au chercheur. 28 ans plus tard, les hackers ont trouvé un moyen de contourner ces limites. C'est là que les choses ont empiré.

La cryptomonnaie et la NSA

Quand on pense à l'envergure des dernières attaques au rançongiciel qui ont touché le monde, il faut garder en tête deux éléments : la fréquence et la portée. Un rapport de 2016 du département américain de la justice relève 7 694 plaintes liées à des rançongiciels depuis 2005, un chiffre probablement bien en-deçà de la réalité. L'attaque WannaCry de mai 2017,

pour sa part, a touché 150 pays. Deux facteurs ont joué un rôle-clé dans l'ascension du rançongiciel : le développement des monnaies virtuelles et la disponibilité de failles informatiques détenues par la NSA.
En effet, les monnaies virtuelles comme le Bitcoin offrent aux pirates une chance réelle de récupérer de l'argent de la rançon. C'est une amélioration considérable par rapport à l'époque de Joseph Popp, où une boîte postale était nécessaire pour espérer voir un jour les billets verts réclamés. Il suffit maintenant d'envoyer aux victimes un lien où ils pourront effectuer le paiement en Bitcoin.
D'après l'entreprise de cybersécurité Palo Alto Networks, le premier rançongiciel à avoir demandé le paiement en Bitcoin était le Cryptowall de 2013. Le premier, et loin d'être le dernier. Le confort apporté par le paiement en cryptomonnaie combiné à la popularité croissante du Bitcoin auraient contribué à l'augmentation de 300 % des incidents liés à un rançongiciel, pointée du doigt par un rapport d'IBM en 2016.
Alors pourquoi l'envergure de ces attaques est-elle si large ? Si beaucoup de facteurs peuvent jouer, l'un d'entre eux est primordial : le dévoilement par le groupe de hackers Shadow Brokers d'une série de failles informatiques que possédait la NSA. Dans la liste se trouvait la fameuse faille EternalBlue, qui couplée avec un rançongiciel, a permis la propagation incroyable du virus WannaCry. La même faille a apparemment joué un rôle clé (mais pas exclusif) dans la diffusion de NotPetya, qui a touché 65 pays.
Et tandis que Microsoft a déjà dévoilé un patch pour parer la faille EternalBlue au moment où le virus se propageait dans le monde, le feu de forêt qu'ont été WannaCry et NotPetya sert de rappel violent que tout le monde n'est pas à jour en terme de sécurité.
Et maintenant, qu'est-ce qu'on fait ?
L'échelle sans précédent de ces deux attaques, propulsées par les failles volées à la NSA et facilitées par la cryptomonnaie, suggère que nous nous sommes entrés dans un nouvel âge de rançongiciels particulièrement virulents. Les attaques comme WannaCry risquent de devenir monnaie courante, comme l'indique le rapport 2017 de l'entreprise de cybersécurité Symantec qui note "une augmentation de 36 % des attaques au rançongiciel dans le monde".
Il est intéressant cependant de remarquer que le rançongiciel pourrait finir par être victime de son succès. Le petit nombre d'ordinateurs infectés combiné aux mécanismes de paiement défaillants de NotPetya et WannaCry signifient que même si les gens choisissent de payer la rançon, ils ne reçoivent pas leur clé de déchiffrement. Pourquoi payer si vous savez que vous ne reverrez de toute façon pas vos fichiers ? La rumeur s'est vite propagée, et à l'heure où nous écrivons ces lignes, l'adresse Bitcoin associée à NotPetya n'a reçu que 46 paiements, soit environ 10 317 dollars.
Tout cela montre que si la forme d'extorsion numérique développée par Joseph Popp ne montre aucun signe de ralentissement, le revenu n'y est pas. C'est peut-être là le seul espoir que nous avons de mettre fin au fléau grandissant du rançongiciel.
http://mashable.france24.com/tech-business/20170630-rancongiciel-ransomware-wannacry-notpetya-nsa

NotPetya, Petyr, GoldenEye : pourquoi ce rançongiciel est plus inquiétant que WannaCry

Le rançongiciel aux multiples noms qui sévit actuellement dans le monde entier dispose de caractéristiques particulières, qui le rendent plus dangereux que ses prédécesseurs pour les entreprises.
Comme un air de déjà-vu… Le logiciel malveillant qui se propage dans le monde depuis mardi 27 juin ressemble à un enfant terrible de Wannacry, le rançongiciel qui avait créé une

panique générale début mai en infectant des dizaines, voire des centaines de milliers d'ordinateurs.

Ces deux menaces cyber prennent des ordinateurs en otage en bloquant l'accès à des fichiers cruciaux et imposent de payer une rançon pour en récupérer le contrôle. Ils exploitent aussi, tous les deux, au moins une faille de sécurité de Windows qui a, prétendument, été dérobé à la NSA (l'Agence national de sécurité américaine) en 2016.

Une attaque plus ciblée

Mais le nouveau logiciel malveillant – baptisé NotPetya, Petyr ou encore GoldenEye (selon l'enteprise de cybersécurité qui s'exprime) – présente de telles différences avec les précédents rançongiciels qu'on "peut se demander s'il ne s'agit pas d'un virus dont le but réel est de détruire des fichiers tout en se faisant passer pour un rançongiciel classique", s'interroge Bogdan Botezatu, expert en cybersécurité pour la société roumaine Bitdefender.

"On peut se demander s'il ne s'agit pas d'un virus dont le but réel est de détruire des fichiers"

Ainsi ce virus ne se propage pas aussi vite que ses prédécesseurs. Il y quelques milliers d'ordinateurs tout au plus qui ont été infectés alors que lors de l'épidémie Wannacry, les victimes se comptaient par dizaines de milliers dès le premier jour. "La cyberattaque en cours est beaucoup plus ciblée", précise le spécialiste roumain. Ce nouveau rançongiciel a tout d'abord frappé des banques et entreprises ukrainiennes, puis des grands groupes comme le français Saint-Gobain ou le géant danois de la logistique Maersk. Le fonctionnement d'infrastructures, comme le port indien de Nhava Sheva ou la centrale nucléaire de Tchernobyl, a aussi été perturbé. Wannacry cherchait à faire un maximum de victimes, alors que cette fois-ci, les cybercriminels semblent avoir une idée plus précise en tête.

8 000 dollars seulement

"L'attaque est moins vaste, mais beaucoup plus dangereuse pour les entreprises", affirme Bogdan Botezatu. Alors que le commun des rançongiciels bloque seulement l'accès à un certain nombre de fichiers sensibles ou critiques, NotPetya fait bien plus encore puisqu'il verrouille l'ensemble du disque dur. Pour les internautes, le résultat est le même : ils n'ont plus accès à leurs données.

Pour payer, il faut envoyer toutes les informations à une adresse email... désormais désactivée par la société qui la gère

Mais en milieu industriel ou commercial, ce n'est pas la même histoire. Le nouveau rançongiciel rend l'ordinateur infecté inutile, tandis que Wannacry n'empêchait pas le poste informatique touché de faire tourner des programmes en tâche de fond s'ils ne font pas appel aux fichiers bloqués. La différence est de taille pour un ordinateur qui contrôle, par exemple, une fonction critique dans une centrale nucléaire. "C'est pourquoi une centrale électrique et un opérateur télécom en Ukraine ont dû interrompre leur fonctionnement", souligne l'expert de Bitdefender.

Les auteurs de la cyberattaque en cours semblent s'intéresser davantage à la perturbation du fonctionnement des entreprises qu'au gain financier. Pour l'instant, leur butin s'élève à 8 000 dollars en bitcoins, ce qui est encore plus modeste que les 20 000 dollars récupérés par les criminels à l'origine de Wannacry. Surtout, ils ont fait une erreur de débutants dans leur demande de rançon : pour payer, il faut envoyer toutes les informations nécessaires à une adresse email. Posteo, la société allemande qui gère l'adresse utilisée, a rapidement désactivé le compte des cybercriminels. Il n'y a, donc, à l'heure actuelle plus aucun moyen de payer la rançon… Pour Bogdan Botezatu, "faire une telle erreur lorsqu'on a mis au point une cyberattaque comme celle-ci peut sembler étrange". Même à l'ONU, le directeur du programme de lutte contre la cybercriminalité Neil Walsh trouve que tous ces indices remettent en cause "le motif financier des auteurs".

http://mashable.france24.com/tech-business/20170628-notpetya-petyr-goldeneye-rancongiciel-destruction-massive

La blockchain dans le viseur d'Interpol

Plusieurs institutions de lutte contre la criminalité, sociétés privées et universités ont noué un partenariat pour étudier sur trois ans comment la blockchain est utilisée pour des pratiques frauduleuses.

C'est à l'origine une infrastructure dédiée à des transactions en bitcoins. Mais depuis quelques temps, beaucoup de monde, et pas seulement dans la finance, s'intéresse à la blockchain, ce système décentralisé permettant de se passer d'intermédiaire. Des banques internationales travaillent sur le sujet bien sûr, mais aussi le monde de l'énergie, de la gestion de droits d'auteurs ou de la santé. Et Interpol.

Fin mai, l'organisation de police internationale a annoncé la création d'un consortium de quinze membres destiné à la lutte contre les usages criminels de la blockchain : transactions douteuses, financement du terrorisme, blanchiment d'argent, etc. Le projet, appelé Titanium et financé à hauteur de 5 millions d'euros par l'Union européenne, réunit, entre autre, autour d'Interpol les spécialistes néerlandais de la cybersécurité de Coblue Cybersecurity, l'université autrichienne d'Innsbruck, le University College de Londres, l'Institut de Technologie de Karlsruhe, la société CounterCraft espagnole, l'Office fédéral de police criminelle allemand, les ministères de l'Intérieur autrichien et espagnol)… Les travaux sont prévus pour durer trois ans.

Des outils d'informatique légale

L'idée consiste à concevoir des outils d'informatique légale basés sur des caractéristiques typiques d'agissements frauduleux sur la blockchain. Pour cela, des données issues de plusieurs sources (réseaux peer-to-peer, forums, place de marchés du darknet, etc) seront étudiées, croisées, confrontées.

Ce n'est pas la première fois qu'Interpol a la blockchain dans le viseur. Au début de l'année, l'organisation participait à une conférence sur les monnaies numériques dans le financement du terrorisme. En septembre 2016, elle annonçait des travaux sur le sujet avec Europol. Et il y a deux ans, suite à une étude menée avec les experts sécurité de Kasperky Labs, Interpol avait alerté sur les possibilités de diffusion de virus permises par la blockchain. Vu comment fonctionne le système pour valider des opérations, des logiciels malveillants peuvent y être stockés et, une fois là, s'avéreraient extrêmement difficiles à déloger. Or, la blockchain étant un programme et une base de données décentralisés, tous ses utilisateurs en ont la même version téléchargée sur leurs ordinateurs.

https://www.sciencesetavenir.fr/high-tech/la-blockchain-dans-le-viseur-d-interpol_114301

Facebook, YouTube, Twitter et Microsoft créent un Forum mondial contre le terrorisme

Facebook, YouTube (Google), Twitter et Microsoft ont annoncé le lancement d'un Forum mondial de l'Internet contre le terrorisme. L'objectif de ce collectif est de lutter plus efficacement contre la propagande en ligne, grâce à une collaboration accrue entre les géants de la tech.

Pour lutter contre le terrorisme, les géants de la tech que sont Facebook, Twitter, YouTube (Google) et Microsoft ont décidé de renforcer leur collaboration en créant un Forum mondial de l'Internet contre le terrorisme.

« *Nous sommes convaincus qu'en travaillant ensemble, en partageant les meilleurs éléments technologiques et opérationnels de nos efforts individuels, nous aurons un plus grand impact sur la menace causée par le contenu terroriste en ligne* » explique ainsi Twitter dans son annonce du lundi 26 juin 2017.

Si le Forum promet de créer de nouvelles initiatives, il s'appuie déjà en grande partie sur des partenariats existants, comme la base commune « d'empreintes numériques » créée en décembre 2016 par ces mêmes entreprises. Elles y répertorient les contenus de propagande terroriste identifiés pour pouvoir les effacer plus rapidement sur d'autres plateformes. Ainsi, si Facebook supprime une vidéo, son empreinte digitale, une fois intégrée à la base, permettra aux autres géants de l'effacer à leur tour si elle est présente sur leur service.

Un moyen de répondre aux critiques des gouvernements

L'objectif de la plateforme, selon ses créateurs, est d'améliorer la « *détection de contenu et les techniques de classification à l'aide de machine learning* » mais aussi de faire preuve de plus de transparence en matière de suppression de contenu de propagande terroriste, celle-ci étant souvent opérée dans le secret.

Le Forum mondial contre le terrorisme affirme aussi s'appuyer sur des discussions qui ont eu lieu à l'occasion du dernier G7 ou encore avec le gouvernement britannique, particulièrement critique du rôle joué par ces plateformes au lendemain des récentes attaques terroristes subies sur son territoire.

Le Forum prévoit de collaborer avec des gouvernements mais aussi avec des groupes de la société civile

Les géants de la tech promettent par ailleurs plus de collaboration avec des spécialistes de la lutte anti-terroriste, dont des « *gouvernements, des groupes issus de la société civile* ». Le Forum entend aider les petites entreprises à se doter des technologies nécessaires pour lutter contre la prolifération de ce type de contenu, comme multiplier les ateliers pour lutter contre le recrutement terroriste, sur le modèle du programme Creators for Change de YouTube. Celles-ci se feront notamment avec l'aide du UN CTED/ICT4Peace, un comité de l'ONU contre le terrorisme.

Il s'agit d'un moyen pour les grands groupes de répondre aux critiques, qui leur reprochent de ne pas être assez efficaces dans la modération de propagande terroriste, alors que l'Union européenne envisage de renforcer la modération des réseaux sociaux sous l'impulsion de l'Allemagne, qui prévoit une loi forte en la matière, dont l'amende record de 50 millions d'euros inquiète Facebook.

Une modération compliquée

Récemment, Facebook a choisi la carte de la transparence en dévoilant ses mesures de lutte contre le terrorisme. Mais le réseau social qui compte près de 2 milliards d'utilisateurs s'est surtout trouvé empêtré dans un scandale en la matière : *The Guardian* a révélé que certains modérateurs en charge de supprimer ces contenus ont vu leur identité exposée à de potentiels terroristes. Ces équipes, qui doivent apprendre les noms et visages de 600 leaders terroristes et passent leurs heures de travail à parcourir du contenu violent (dont des vidéos ou images de décapitation), s'estiment sous-payées.

Facebook, YouTube et Twitter doivent aussi trouver le délicat équilibre entre défense de la liberté d'expression et censure. Ces plateformes doivent notamment apprendre à faire la distinction entre une image — comme des sympathisants armés de Daech qui brandissent un drapeau de l'organisation — utilisée à des fins de propagande ou simplement pour illustrer un article d'actualité.

Facebook a récemment fait polémique en supprimant un groupe pour l'indépendance de la Tchétchénie au motif qu'il s'agissait d'un groupe terroriste. Une erreur depuis corrigée par le réseau social. Si le Forum mondial de lutte contre le terrorisme promet d'en dire plus sur son action « *en temps voulu* », ses contours restent pour l'instant assez flous.

http://www.numerama.com/tech/270668-facebook-youtube-twitter-et-microsoft-creent-un-forum-mondial-contre-le-terrorisme.html

Mise en garde de la Banque de Chine contre les monnaies virtuelles

Les monnaies virtuelles ont récemment connu des déboires, deux de ces crypto-monnaies les plus populaires, le Bitcoin et l'Ethereum, étant tombées à leur nouveau niveau le plus bas en un mois et demi.

La quasi-totalité des autres monnaies virtuelles à base de chaînes de 100 blocs ont subi un sort similaire, certaines ayant même diminué de près de 35%.

Selon les experts de chaînes de blocs, les hauts et les bas aussi prononcés que ceux-ci sont courants pour les devises virtuelles.

« Certaines institutions privées ont versé de l'argent dans le Bitcoin pour le faire monter et de nombreux investisseurs ont suivi », a déclaré Zhou Yu, directeur de recherche sur les chaînes de blocs chez China Unionpay, une association de l'industrie chinoise des cartes bancaires. « Il y a beaucoup de spéculations sur le marché ».

D'autres disent qu'il ne faut pas s'empresser de conclure que la technologie de la chaîne de blocs entraîne nécessairement de la volatilité.

« Des choses comme le Bitcoin utilisent non seulement la technologie des chaînes de blocs, mais elles utilisent aussi un réseau peer-to-peer pour qu'il n'y ait pas de contrôle central », a précisé Cai Weide, directeur du laboratoire des chaînes de blocs de l'Université d'aéronautique et d'astronautique de Beijing. « Leurs créateurs les ont conçus de cette façon précisément pour empêcher les supervisions des autorités. C'est pour cette raison que le Bitcoin deviendra un outil de blanchiment d'argent ».

Les experts estiment quant à eux qu'une devise numérique émise et gérée par une banque centrale est en fait favorable du point de vue des décideurs politiques.

« Contrairement aux impressions des gens, une monnaie officielle de chaîne de blocs peut être très utile aux régulateurs, car la technologie de la chaîne de blocs garantit la traçabilité de toutes les transactions », a souligné M. Cai.

Cela pourrait avoir des implications positives pour la gestion fiscale d'un gouvernement, ses efforts de lutte contre la corruption et un large éventail d'autres efforts.

C'est la banque centrale britannique qui a annoncé la première en 2015 qu'elle faisait des recherches sur une possible monnaie virtuelle officielle.

« Beaucoup de banques centrales font des recherches, et l'important est que, contrairement au Bitcoin, les monnaies virtuelles officielles aient un contrôle politique central », a dit M. Zhou.

La banque centrale chinoise a créé un institut de recherche plus tôt ce mois-ci à Beijing pour étudier les devises virtuelles.

Mais, selon les experts, nous sommes toutefois encore assez éloignés du lancement d'une monnaie virtuelle officielle dans un proche avenir.

http://french.peopledaily.com.cn/Economie/n3/2017/0714/c31355-9241853.html

Japon: début du procès du patron français de la plateforme de bitcoins MtGox

Au Japon s'ouvre ce 11 juillet le procès de l'ex-baron autoproclamé des bitcoins, un Français, Mark Karpeles.

Sa plateforme d'échange de monnaie virtuelle avait fait faillite au début de 2014 après une perte d'environ 355 millions d'euros. Il comparaît notamment pour détournement de fonds.

Mark Karpeles est accusé d'avoir accédé au système informatique de la plateforme d'échange de monnaie virtuelle, MtGox, qu'il avait créée à Tokyo, d'avoir falsifié les données de ses comptes et détourné une somme de 2,4 millions d'euros.

L'accusé dit avoir été victime d'une attaque informatique massive et plaide non coupable, attaque qui aurait fait perdre à la plateforme MtGox l'équivalent de 350 millions d'euros et causé sa faillite.

Agé aujourd'hui de 32 ans, Mark Karpeles avait déjà été condamné en 2010 en France à un an de prison pour intrusion frauduleuse dans un système informatique.

La faillite de la plateforme MtGox avait fait grand bruit. Au plus haut de son activité, elle revendiquait la gestion de 80 % des transactions mondiales de bitcoins. Ce marché des monnaies virtuelles est aujourd'hui pris en main par Wall Street et certains magasins de Tokyo acceptent des paiements en bitcoins.

Les investisseurs lésés, des étrangers expatriés au Japon pour la plupart, espèrent récupérer une partie des sommes investies, au choix, en devises traditionnelles... ou en bitcoins.

http://www.rfi.fr/asie-pacifique/20170711-japon-debut-proces-patron-francais-plateforme-bitcoins-mtgox