La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ?

	La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ?

Aux États-Unis, une affaire judiciaire pose la question du droit que peuvent avoir les autorités judiciaires à contraindre un suspect à débloquer son iPhone avec le capteur Touch ID qui permet d'accéder au contenu du téléphone avec les empreintes digitales.

La question s'est certainement déjà posée dans les commissariats et dans les bureaux des juges d'instruction, et elle devrait devenir plus pressant encore dans les années à venir : alors qu'un suspect peut toujours prétendre avoir oublié son mot de passe, ou refuser de répondre, les enquêteurs peuvent-ils contraindre un individu à débloquer son téléphone lorsque celui-ci est déblocable avec une simple empreinte digitale ?
Le débat sera tranché aux États-Unis par un tribunal de Los Angeles. Le Los Angeles Times rapporte en effet qu'un juge a délivré un mandat de perquisition à des policiers, qui leur donne le pouvoir de contraindre physiquement la petite amie d'un membre d'un gang arménien à mettre son doigt sur le capteur Touch ID de son iPhone, pour en débloquer le contenu.

Le mandat signé 45 minutes après son placement en détention provisoire a été mis en œuvre dans les heures qui ont suivi. Le temps était très court, peut-être en raison de l'urgence du dossier lui-même, mais aussi car l'iPhone dispose d'une sécurité qui fait qu'au bout de 48 heures sans être débloqué, il n'est plus possible d'utiliser l'empreinte digitale pour accéder aux données. Mais l'admissibilité des preuves ainsi collectées reste sujette à caution et fait l'objet d'un débat entre juristes.

EN MONTRANT QUE VOUS AVEZ OUVERT LE TÉLÉPHONE, VOUS DÉMONTREZ QUE VOUS AVEZ CONTRÔLE SUR LUI
Certains considèrent qu'obliger un individu à placer son doigt sur le capteur d'empreintes digitales de son iPhone pour y gagner l'accès revient à forcer cette personne à fournir elle-même les éléments de sa propre incrimination, ce qui est contraire à la Constitution américaine et aux traités internationaux de protection des droits de l'homme. « En montrant que vous avez ouvert le téléphone, vous montrez que vous avez contrôle sur lui », estime ainsi Susan Brenner, une professeur de droit de l'Université de Dayton. Le capteur Touch ID ne sert pas uniquement à débloquer le téléphone, mais aussi à le déchiffrer, en fournissant une clé qui joue le rôle d'authentifiant du contenu.
D'autres estiment qu'il s'agit ni plus ou moins que la même chose qu'une perquisition à domicile réalisée en utilisant la clé portée sur lui par le suspect, ce qui est chose courante et ne fait pas l'objet de protestations. Ils n'y voient pas non plus de violation du droit de garder le silence, puisque le suspect ne parle pas en ne faisant que poser son doigt sur un capteur.

ET EN FRANCE ?
Pour le moment, le sujet n'est pas venu sur la scène législative en France. Mais il pourrait y venir par analogie avec d'autres techniques d'identification biométrique.
En matière de recherche d'empreintes digitales ou de prélèvement de cheveux pour comparaison, l'article 55-1 du code de procédure pénale punit d'un an de prison et 15 000 euros d'amende « le refus, par une personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis ou tenté de commettre une infraction, de se soumettre aux opérations de prélèvement ». De même en matière de prélèvements ADN, le code de procédure pénale autorise les policiers à exiger qu'un prélèvement biologique soit effectué sur un suspect, et « le fait de refuser de se soumettre au prélèvement biologique est puni d'un an d'emprisonnement et 30 000 euros d'amende ».
Sans loi spécifique, les policiers peuvent aussi tenter de se reposer sur les dispositions anti-chiffrement du code pénal, puisque l'empreinte digitale sert de clé. L'article 434-15-2 du code pénal punit de 3 ans de prison et 45 000 euros d'amende le fait, « pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre, sur les réquisitions de ces autorités ». Mais à notre connaissance, elle n'a jamais été appliquée pour forcer un suspect à fournir lui-même ses clés de chiffrement, ce qui serait potentiellement contraire aux conventions de protection des droits de l'homme… [Lire la suite]

Réagissez à cet article

Source : *La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ? – Politique – Numerama*

Forum économie mondial à Kigali : l'Afrique sur le chemin de la transformation numérique

Forum économie mondial à Kigali : l'Afrique sur le chemin de la transformation numérique

---

Identifier les opportunités de coopération public-privé pour les dirigeants africains qui veulent bâtir des économies compétitives et prospères en relevant le défi du numérique. C'est l'objectif du 26ème Forum économique mondial sur l'Afrique qui va se tenir du 11 au 13 mai à Kigali sur le thème « Connecter les ressources de l'Afrique à travers la transformation numérique »

Dans un communiqué publié vendredi, Elsie Kanza, le directeur du Forum économique mondial pour l'Afrique, a indiqué que la rencontre va mobiliser plus de 1.200 participants. Des chefs d'Etat et de gouvernement africains sont attendus. Sont annoncées à Kigali d'importantes délégations des pays tels que la Guinée, le Sénégal, la Côte d'Ivoire, le Gabon, l'Ethiopie, le Togo et le Kenya.
Selon le document, ce rendez-vous de haut niveau verra également la participation des ministres et officiels hollandais, suédois, américains et russes.
Les échanges inter-Etats étant considérés comme un moyen de connecter les ressources en Afrique, la rencontre enregistrera la coopération du Centre commercial international (ITC), le Fonds international pour le développement agricole (IFAD) et le Fonds des Nations Unies pour la population (FANUAP), ainsi que d'autres organisations internationales.
Comme l'a expliqué M. Kanza, la présence de tant de dirigeants et de décideurs ouvre « un vaste champ pour la coopération public-privé », pour aider les pays africains à se développer dans les marchés de plus en plus numériques… [Lire la suite]

Réagissez à cet article

Source : *Forum économie mondial à Kigali : l'Afrique sur le chemin de la transformation numérique | CIO-MAG*

La Rédaction CIO Mag

Airbus déjoue douze attaques informatiques majeures par an

	**Airbus déjoue douze attaques informatiques majeures par an**

Source : *Piratage informatique : Airbus déjoue douze attaques majeures par an – 06/05/2016 – ladepeche.fr*

article de Gil Bousquet

Comment s’introduire dans le web invisible ?

Comment s’introduire dans le web invisible ?

La façon la plus répandue et la plus simple de s'introduire dans cette partie immergée du web est le serveur Tor, acronyme pour The Onion Router. Pourquoi oignon ? Parce que le logiciel assure plusieurs couches de protection, qui permettent entre autres de conserver l'anonymat de l'internaute.

Tous les sites qui ont cours sur ce moteur de recherche se terminent par .onion. L'étudiant en informatique qui a accepté de faire une démonstration à L'Express affirme qu'à toutes les fois qu'une personne brassant des affaires sur le «*deep web*» fait une requête, elle ne passe jamais par le même chemin afin de brouiller les pistes.
«Tout le monde se connecte sur un même serveur et une fois que tu es connecté sur ce serveur, tu passes par un réseau de connections international, explique-t-il. Tu as un serveur d'entrée et un serveur de sortie. Ce qui se passe entre, on ne le sait pas. Ton adresse IP se perd. »

Un enseignant en informatique au Cégep de Drummondville, Louis Marchand, abonde également en ce sens : «Si la personne est excessivement prudente dans ses démarches, la seule chose qui pourrait être retracée serait sa connexion au réseau Tor. Toutes les actions, légales ou pas, que cette personne a pu effectuer à l'intérieur du serveur sont pratiquement introuvables.» Pratique lorsqu'on veut publier des anecdotes sur un blogue en évitant la censure… ou pour publier une offre d'achat de cocaïne.
Ce moteur de recherche, développé par la marine américaine, se télécharge aussi facilement que Google Chrome et est associé avec le moteur Firefox. Comme quoi Tor n'est pas illégal du tout : «c'est l'utilisation qu'on en fait qui peut être négative», complète l'étudiant.

Les bitcoins, la monnaie virtuelle anonyme
La monnaie ayant cours sur le web invisible est le *bitcoin*, une forme d'argent virtuelle cryptée. Elle n'est soumise à aucun taux de change ni à aucune banque, donc aucun intermédiaire n'existe entre l'acheteur et la marchandise. Cependant, son atout majeur pour les consommateurs de produits illicites est qu'elle peut être utilisée de façon anonyme.
Louis Marchand décrit le bitcoin comme n'étant rien d'autre qu'un fichier. «Il faut faire attention à ça : toutes les transactions sont enregistrées, même si le bitcoin en tant que tel n'est pas identifié. C'est beaucoup plus difficile de retracer de l'argent liquide, puisque absolument rien ne lie un 20 $ à son propriétaire», spécifie-t-il.

Selon l'enseignant, le bitcoin fonctionne exactement comme l'or ou le diamant. «Ce qui diffère, c'est que quelque chose de virtuel change beaucoup plus rapidement que n'importe quelle ressource physique. Demain, un bitcoin peut valoir 2 $ et le lendemain, plus de 2000 $. C'est un coup de dé.»
Cette monnaie est cependant extrêmement difficile à générer et est très coûteuse en électricité, d'après Louis Marchand : elle nécessite beaucoup de ressources et de temps, puisqu'elle doit correspondre à des critères mathématiques très précis. C'est notamment ce qui expliquerait la valeur toujours montante des bitcoins. Au moment de la vérification de L'Express, un de ces fichiers valait 550 $.
Selon les dires de l'étudiant en informatique qui a préféré conserver l'anonymat, lorsqu'il s'est lui-même procuré huit bitcoins il y a quelques années, ça ne lui avait pas coûté plus d'une centaine de dollars. «Si je me souviens bien, ça a déjà monté à 1400 $. C'est hallucinant», s'étonne-t-il.
Il faut dire que le marché du web invisible, dans lequel évoluent les bitcoins, est aussi extrêmement lucratif. La Sureté du Québec, les deux compères ayant testé les drogues du «*deep web*» et l'informaticien s'accordent tous sur un point : la rémunération est la motivation principale de n'importe quel trafiquant de marchandises illégales sur Internet, selon eux.
«Moins c'est légal, plus c'est payant. Personne n'ira vendre un foie sur Internet, à part pour l'argent que ça rapporte. Il faut oublier le côté humain et ne penser qu'au montant final», croit Louis Marchand… [Lire la suite]

Source : *Le logiciel Tor, la porte d'entrée du web invisible – Actualités – L'Express – Drummondville*

Dénoncez les hôtes Airbnb, Paris vous le rendra…

Dénoncez les hôtes Airbnb, Paris vous le rendra…

La mairie de Paris appelle les voisins à dénoncer les hôtes Airbnb non déclarés aux services municipaux.

Dans le dernier chapitre d'une bataille en cours sur l'économie de partage en France, la ville de Paris demande aux résidents de dénoncer leurs voisins qui ne sont pas correctement enregistrés comme meublé ou hôte du site Airbnb.
Selon le site Europe1.fr, les services municipaux ont créée une nouvelle section sur le portail open data de la ville qui répertorie les résidents qui se sont inscrits comme un hôte Airbnb. 126 résidences sont aujourd'hui listées comme locations saisonnières sur la plate-forme Airbnb alors que le site revendique plus de 41 000 logements (35 185 appartements et 5 827 chambres). Paris serait une des destinations les plus populaires sur sa plate-forme selon Airbnb. Et avec la carte publiée par la ville de Paris, il est facile de repérer les hôtes en règle, c'est à dire qui auront déclarés ces revenus et encaissés la taxe de séjour reversée ensuite à la mairie. C'est une des batailles engagées depuis plusieurs mois par les hôteliers qui crient à la concurrence déloyale. La ville de Berlin a également engagé un bras de fer avec Airbnb pour limiter les locations de meublés sur la plate-forme.

Dans une interview avec Europe1, Mathias Vicherat, chef de cabinet pour le maire de la ville, indique espérer que les résidents utiliseront les informations sur le portail de données ouvertes pour faire pression sur leurs voisins qui ne respectent pas les règles. Les hôtes Airbnb en violation avec les règlements de la ville pourraient faire face à une amende de 25 000€ s'ils louent plus de quatre mois par an leurs logements à des touristes. « On souhaite que cela provoque un espèce de choc de conscience de civisme, et que les gens se mettent en règle d'eux-mêmes, sans attendre d'être éventuellement signalé par un de leurs voisins », dit-il. La mairie explique qu'il n'est pas question d'appeler à la dénonciation comme durant la Seconde Guerre Mondiale où cinq millions de lettres anonymes avaient été envoyées à la police ou la Gestapo… [Lire la suite]

Réagissez à cet article
Article de Serge Leblal

Source : *Paris incite ses habitants à dénoncer les hôtes Airbnb – Le Monde Informatique*

Des centaines de milliers de dossiers de santé désormais en libre accès pour Google

Des centaines de milliers de dossiers de santé désormais en libre accès pour Google

Un accord signé entre Google et le National Health Service (NHS) britannique va permettre à Google d'accéder à plus de 1,6 millions de dossiers médicaux.

Le National Health Service (NHS) est le système de la santé publique du Royaume-Uni. Sa mission, permettre aux britanniques de se soigner dans les meilleures conditions. Quatre NHS régissent le système de santé publique des Écossais, Britanniques, Irlandais et Gallois. Les sujets de sa gracieuse majesté vont adorer apprendre que le NHS a signé un accord avec une filiale de Google, DeepMind. Finalité de ce partenariat, comprendre la santé humaine. Sauf qu'il semble que ce contrat passé en 2014 vient de prendre une nouvelle tournure plus intrusive.
DeepMind a dorénavant un accès complet à 1,6 millions de dossiers de patients britanniques. Des dossiers de patients passés par les trois principaux hôpitaux de Londres : Barnet, Chase Farm, et le Royal Free. En février, la filiale de Google dédiée à l'intelligence artificielle a indiqué avoir mis en place une application appelée Streams. Elle est destinée à aider les hôpitaux à surveiller les patients atteints de maladie rénale. Cependant, il vient d'être révélé que l'étendue des données partagées va beaucoup plus loin et inclut des journaux d'activité, au jour le jour, de l'hôpital (qui rend visite au malade, quand…) et de l'état des patients.
Les résultats des tests de pathologie et de radiologie sont également partagés. En outre, DeepMind a accès aux registres centralisés de tous les traitements hospitaliers du NHS au Royaume-Uni, et cela depuis 5 ans. Dans le même temps, DeepMind développe une plate-forme appelée Rescue Patient. Le logiciel utilise les flux de données de l'hôpital. Des informations qui doivent permettre de mener à bien un diagnostic. New Scientist explique que l'application compare les informations d'un nouveau patient avec des millions d'autres cas Patient Rescue pourrait être en mesure de prédire les premiers stades d'une maladie. Les médecins pourraient alors effectuer des tests pour voir si la prédiction est correcte… [Lire la suite]

Réagissez à cet article

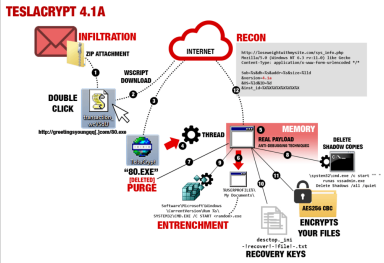
Source : *Google s'ouvre les portes de centaines de milliers de dossiers de santé – Data Security Breach*

Le CryptoVirus TeslaCrypt s’attaque à de nouveaux fichiers et améliore sa protection

	Le CryptoVirus TeslaCrypt s’attaque à de nouveaux fichiers et améliore sa protection

Ces nouveaux exemplaires de TeslaCrypt sont diffusés massivement en tant que pièce jointe dans des spams qui imitent les avis de réception de colis des courriers express. D'après Endgame, la version 4.1A est apparue il y a environ une semaine ; outre les extensions déjà ciblées, elle attaque également les fichiers suivants .7z, .apk, .asset, .avi, .bak, .bik, .bsa, .csv, .d3dbsp, .das, .forge, .iwi, .lbf, .litemod, .litesql, .ltx, .m4a, .mp4, .rar, .re4, .sav, .slm, .sql,

La diffusion de TeslaCryp via le spam constitue également un changement : lors des campagnes récentes de TeslaCrypt, le ransomware avait été propagé via des kits d'exploitation et des redirections depuis des sites WordPress et Joomla. Dans ce cas, la victime doit ouvrir le fichier ZIP en pièce jointe afin d'activer un downloader JavaScript qui utilise Wscript (un composant de Windows) pour télécharger le fichier binaire de TeslaCrypt depuis le domaine greetingsyounggqq[.]com.
D'après notre interlocutrice, l'analyse de la version actualisée du ransomware fut complexe car elle lance de nombreux flux d'application et d'opérations de débogage afin de compliquer la tâche des outils de protection. Comme l'explique Amanda Rousseau, « il semblerait qu'il essaie de dissimuler les lignes dans la mémoire. Il est plus difficile pour l'Antivirus de les détecter s'il n'analyse pas la mémoire. »



Le recours à Wscript rend également la détection plus compliquée car le trafic ressemble à des communications légitimes de Windows. Selon Amanda Rousseau, il aura fallu quatre jours aux outils de détection pour identifier la technique et l'ajouter aux signatures. La durée de service des serveurs de commande sur lesquels se trouve TeslaCrypt a été limitée. A l'issue de celle-ci, les individus malintentionnés changent d'hébergement.
La version actualisée du ransomware utilise également un objet COM pour dissimuler les lignes de code extraites et élimine les identifiants de zone afin qu'ils ne soient pas découverts. De plus, pour éviter la surveillance, le malware arrête plusieurs processus Windows : Task Manager, Registry Editor, SysInternals Process Explorer, System Configuration et Command Shell. Pour garantir sa présence permanente, il se copie sur le disque et crée le paramètre correspondant dans la base de registres.
Vous trouverez une description technique détaillée de TeslaCrypt, y compris de ses méthodes de chiffrement et de ses techniques de lutte contre le débogage sur le blog d'Endgame.
Amanda Rousseau a indiqué dans ses commentaires que lors des essais, les nouveaux échantillons ont atteint les disques réseau connectés et ont tenté de chiffrer les fichiers qui s'y trouvaient. Ils tentent également de supprimer le cliché instantané du volume afin de priver la victime de toute chance de récupération.
Mais il y a malgré tout une bonne nouvelle : la version actualisée de TeslaCrypt chiffre les fichiers à l'aide d'une clé AES 256 et non pas à l'aide d'une clé RSA de 4 096 bits comme indiqué dans la demande de rançon et qui plus est, les informations indispensables au déchiffrement restent sur la machine infectée. « Nous avons trouvé l'algorithme de chiffrement : il fonctionne correctement, mais laisse le fichier de restauration dans le système » a confirmé Amanda Rousseau. « Si l'on part du programme de déchiffrement antérieur de TeslaCrypt et que son code est actualisé conformément aux [découvertes], il sera possible de réaliser le déchiffrement. » Il y a un an environ, Cisco a diffusé un utilitaire de ligne de commande capable de déchiffrer les fichiers touchés par TeslaCrypt.
Amanda Rousseau a également signalé que les auteurs de la version actualisée du ransomware avait emprunté beaucoup de code aux versions antérieures, notamment l'utilisation des objets COM et certaines techniques de débogage. « On dirait que les individus malintentionnés suivent les chercheurs à la trace en surveillant le code [de déchiffrement] publié sur Github en open source » explique le président d'Endgame en montrant les modifications introduites au cours du dernier mois depuis la version 4.0 jusqu'à la version 4 1A. – De petites modifications sont introduites dans chaque version et à la sortie de chaque nouveau décrypteur. Il prenne le meilleur de ce qui était utilisé il y a deux mois et l'appliquent aujourd'hui. »… [Lire la suite]

Source : *TeslaCrypt s'attaque à de nouveaux fichiers et améliore sa protection – Securelist*

Les informations bancaires de la famille royale du Quatar et d'espions mis en ligne – France 24

Les informations bancaires de la famille royale du Quatat . et d'espions mis en ligne

La Banque nationale du Qatar semble avoir été piratée et les données bancaires de clients prestigieux comme des membres de la famille royale al-Thani ou des ministres sont accessibles en ligne.

La QNB a d'ailleurs refusé, mercredi, de confirmer la réalité de ce vol informatique évoquant officiellement des "spéculations sur les réseaux sociaux". Mais plusieurs médias, dont France 24, ont pu consulter ces documents et des clients de l'établissement ont confirmé la véracité des informations les concernant.

Prédicateur controversé

Une partie de l'élite politique et médiatique du pays, dont des membres de la famille dirigeante al-Thani, voient ainsi certaines informations (numéro de compte, téléphone, adresse email) rendues publiques. Il en va de même pour plusieurs ministres, des personnalités du monde des affaires ou encore de hauts gradés de l'armée. La vie bancaire d'une dizaine de journalistes de la chaîne Al Jazeera est aussi mise à nu.

Mais ce ne sont pas seulement les hommes de pouvoir qataris qui ont intéressé les pirates informatiques. Ils pensent aussi avoir identifié plusieurs espions, aussi bien qataris que d'autres pays, parmi les clients de la QNB. Des comptes et informations personnelles concerneraient deux Français soupçonnés d'être des agents secrets. Un membre désigné du contre-espionnage britannique ou encore un autre des services polonais du renseignement font également partie de ce groupe. Dans la plupart des cas, les pirates informatiques ont tenté de trouver des documents connexes, comme des CV ou des liens vers les réseaux sociaux, qui attesteraient que ces personnes appartiennent bien à la communauté du renseignement.

Un homme a droit à un traitement spécial : Youssef al-Qardaoui. Les pirates ont consacré un dossier entier aux différents comptes à la QNB de ce controversé prédicateur, porte voix des Frères musulmans. Cette figure théologique influente a dû fuir l'Égypte dans les années 1960 pour trouver réfuge au Qatar, où il a été un proche de l'ancien émir. En 2014, l'Égypte a demandé et obtenu d'Interpol un mandat d'arrêt international pour incitation au meurtre, vandalisme, violence et vol.

Appât du gain ?

Ce tri des données et les recherches faites pour tenter de ranger les clients par catégories – "famille al-Thani", "Al Jazeera", "banques", "espions" – semblent indiquer que les pirates informatiques n'ont pas agi par pur appât du gain. Ils auraient pu, sinon, simplement mettre en vente la base de données brute.

Reste que contrairement à des lanceurs d'alerte, ces pirates informatiques n'ont rien dit sur les motivations de leur assaut contre la forteresse QNB. Pour Simon Edwards, expert en sécurité informatique pour l'entreprise japonaise d'antivirus Trend Micro, les pirates cherchaient à "mettre en avant certaines transactions" et identifier les comptes les plus sensibles.

Il explique au site International Business Times qu'outre les noms et données bancaires des clients, les détails sur l'historique de leurs transactions (mode de paiement, montant, compte débiteur et créditeur, date de l'opération) ont été mis en ligne. Ce genre d'information peut servir à des cybercriminels financièrement intéressés à faire des profils précis de cibles potentielles.

Un responsable anonyme d'une banque dont les informations ont été publiées en ligne a ainsi assuré à l'agence Reuters que cela "va me pousser à sortir mes avoirs hors du Qatar et si d'autres font comme moi, cela pourrait finir par faire du mal à la banque"… [Lire la suite]

Réagissez à cet article

Source : *Qatar : les informations bancaires de la famille royale et d'espions mis en ligne – France 24*

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).

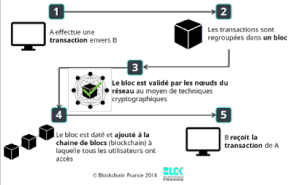
(Image issue du site: blockchainfrance.net)

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 ?*

Une Afrique de plus en plus connectée mais qui doit faire face aux cybermenaces mondiales

Une Afrique de plus en plus connectée mais qui doit faire face aux cybermenaces mondiales

---

Avec un taux de croissance au niveau des TIC de l'ordre de 30% sur un marché de plus d'un milliard de personnes, l'Afrique représente le nouvel Eldorado du monde numérique.

Or, la surface d'attaque augmentant, les cybercriminels élargissent leur champ d'action. La cybercriminalité en Afrique est organisée et bien enracinée, en particulier au Nigéria, au Ghana et en Côte d'Ivoire. Désormais, l'Afrique n'est plus le théâtre des seuls cybercriminels mais aussi de cyberhacktivistes voire de hackers. Le Sénégal a été la victime de cyberattaques en janvier dernier revendiquées par le collectif anonymous du Sénégal. Par rebond des attaques massives menées en janvier en France suite aux attentats de Charlie Hebdo, les serveurs de l'agence de l'informatique de l'Etat du Sénégal sont tombés.
Devant ce désert cybernétique, les Etats d'Afrique tentent de réagir en relevant le défi de sécuriser leurs infrastructures réseau, leurs données et en formant leurs personnels. La France participe activement à la formation cyber des officiers et des techniciens par le biais de la coopération opérationnelle (ministère de la défense). Depuis 2013, une centaine d'officiers et sous-officiers ont été formés au Sénégal, au Niger et au Burkina Faso par les Eléments français au Sénégal.

SecurityDay 2016

Avec la présence des plus grands décideurs du monde de la confiance numérique, l'évènement SecurityDay 2016 vous ont proposé pendant deux jours des conférences sur le thème « cybersécurité et confiance numérique ».
Les SecurityDays ont pour objectif de réunir l'ensemble de l'écosystème numérique africain et d'accélérer le développement d'un espace de confiance afin d'accompagner l'essor du numérique en Afrique, vecteur durable de croissance économique et de développement.
Avec le soutien de l'ANSSI française et de l'ADIE sénégalaise, cet évènement unique en Afrique de l'Ouest est un cadre d'échanges entre experts militaires, civils, décideurs IT, chefs d'entreprise, industriels et utilisateurs finaux pour réfléchir conjointement aux problématiques liées à la cybersécurité en Afrique. … [Lire la suite]

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

Denis JACOPINI est expert informatique assermenté spécialisé en cybercriminalité en Afrique de l'Ouest

Suivez-nous sur

Réagissez à cet article

Source : *SecDay 2016*