Mais à quoi sert Spaces, le nouveau service de Google ?

Mais à quoi sert Spaces, le nouveau service de Google ?

Google a sorti aujourd'hui son nouveau service nommé Spaces. Disponible sur le web, sur iOS et sur Android, cet outil est difficile à cerner : voici quelques pistes d'utilisation après un premier test à la rédaction.

Le monde découvre en ce moment un nouveau service Google : Spaces. Non, il ne s'agit pas du petit nom du programme spatial de Mountain View, mais d'une application qui vous permet de créer des groupes avec des amis / collègues / inconnus pour partager… des choses. Des liens, des images, des commentaires et des vidéos YouTube pour l'instant.
Mais à quoi cela sert ? Eh bien c'est assez difficile à dire pour l'instant. Nous nous sommes empressé de créer un groupe pour Humanoid et d'inviter nos collègues préférés à tester l'application qui se paie le luxe d'être multiplateformes, disponible sur le web, iOS et Android. Nous avons partagé quelques liens, modifié ce qui était modifiable. Nous sommes aussi passés à côté des premiers bugs : une phrase qui sort de l'écran (dommage, c'est celle qui présente le service) ou l'impossibilité d'utiliser un compte Gmail d'entreprise… alors qu'il est proposé au lancement de l'application… [Lire la suite]

Réagissez à cet article

Source : *Mais à quoi sert Spaces, le nouveau service de Google ? – Tech – Numerama*

Pourquoi 95% des distributeurs de billets sont encore vulnérables au piratage

Pourquoi 95% des distributeurs de billets sont encore vulnérables au piratage

---

Lorsque Microsoft a abandonné Windows XP en 2014, on pouvait alors découvrir que 95% des distributeurs de billets de banque tournaient encore sous cette version obsolète de l'OS, devenant ainsi vulnérables au piratage. En 2016, rien n'a changé et les banque comme les constructeurs ne semblent pas décidés à faire le nécessaire.

Lorsque Microsoft a abandonné Windows XP en 2014, la menace de piratage est devenue de plus en plus grande pour les distributeurs de billets. Pourtant, fin 2015, **95% d'entre eux** tournaient encore sous cette version obsolète du système d'exploitation. On dénombre d'ailleurs pas moins de 9000 risques de sécurité sur ces machines. Pourtant les banques semblent s'en laver les mains, pourquoi ?
Comme l'explique Alexey Osipov, ingénieur chez Kaspersky, les constructeurs de distributeurs automatiques ont très peu de concurrents et les banques sont sous contrat avec eux, ils ne font donc pas l'effort de prendre les mesures suffisantes pour sécuriser leurs machines.
Pour Olga Kochetova, également ingénieur chez Kaspersky après avoir travaillé plusieurs années sur le marché des distributeurs bancaires, la réponse est encore plus simple. Ces machines étant désormais trop vieilles pour faire tourner des versions plus récentes et sécurisées de Windows, elles nécessitent donc d'être remplacées, or « **l'investissement serait trop coûteux** ». En outre, ça impliquerait aussi d'embaucher un nouveau personnel mieux formé vis à vis des nouveaux risques de piratage.

Il faut dire que pour un hacker, pirater un distributeur de billet est d'une simplicité enfantine puisqu'il suffit d'acheter une clé sur internet pour se connecter physiquement aux machines. Ils prennent ainsi tout simplement le contrôle du DAB pour lui réclamer la somme qu'ils souhaitent. L'an dernier, une attaque massive baptisée « Carbanak » avait fait perdre plus de **10 millions de dollars** à différentes banques situées un peu partout dans le monde… [Lire la suite]

Réagissez à cet article

Source : *Pourquoi 95% des distributeurs de billets sont encore vulnérables au piratage*

Windows 10 Mobile acceptera l’empreinte digitale comme moyen d’authentification cet été

Windows 10 Mobile acceptera l’empreinte digitale comme moyen d’authentification cet été

La version mobile de Windows 10 gagnera bientôt la compatibilité avec les lecteurs d'empreinte digitale déjà exploités par Android et iOS.

Selon *Engadget*, Microsoft en a fait l'annonce aujourd'hui dans le cadre de la conférence WinHEC. Alors qu'il était déjà possible de déverrouiller son téléphone Windows grâce à la reconnaissance faciale du système, la lecture d'empreinte digitale pourra également être employée.

Pour en bénéficier, il faudra attendre que les fabricants de téléphones Windows ajoutent le lecteur en question.

Ainsi, Windows Hello gagnera cette fonctionnalité dans la mise à jour anniversaire de Windows 10 Mobile dont le déploiement est prévu pour juillet prochain.

Bien entendu, pour en bénéficier, il faudra attendre que les fabricants de téléphones Windows ajoutent le lecteur en question. Pour le moment, seul l'Elite X3 de HP – un téléphone Windows toujours en développement destiné pour le marché des affaires et promettant d'agir comme un ordinateur portable – intègre un lecteur d'empreinte digitale… [Lire la suite]

Réagissez à cet article

Source : *Windows 10 Mobile acceptera l'empreinte digitale comme moyen d'authentification cet été | Branchez-vous*

Laurent LASALLE

Retrouvrer les traces d’une attaque informatique peut s’avérer complexe et coûteuse

Retrouvrer les traces d’une attaque informatique peut s’avérer complexe et coûteuse

Selon l'un des principes fondamentaux de la police scientifique, sur une scène de crime, tout contact laisse une trace. Dans l'univers de la cybercriminalité, chercher les traces pour remonter le fil des événements jusqu'à l'auteur de l'attaque, se révèle souvent compliqué.

Lorsqu'un incident survient, il est généralement difficile pour l'entreprise de définir qui a accédé à son système d'information et ce que cette personne – ou groupe de personnes – a fait. La tâche se complique encore un peu plus lorsque cet incident provient d'utilisateurs internes bénéficiant d'un haut niveau de privilèges sur le système – voire même de la personne en charge de prévenir les attaques sur le réseau.
Que l'incident soit le résultat d'une action malveillante d'un utilisateur interne, d'une erreur humaine ou d'une faille, dès lors que l'entreprise n'est pas capable de remonter les informations, elle passe à côté de preuves cruciales, et rend l'enquête beaucoup plus longue et onéreuse.

Le facteur temps : la clé de la réussite
Dans toutes investigations post-incident de sécurité, le temps est un facteur crucial. Pour mener à bien une enquête, il est plus facile, plus précis et généralement moins couteux de conduire une analyse criminalistique, dite forensics, poussée immédiatement, plutôt que plusieurs semaines voire plusieurs mois après l'incident.
L'examen approfondi des logs : remonter les étapes d'une attaque
Lorsqu'une faille est avérée, l'entreprise dépend des logs générés par les terminaux et les applications sur le réseau, pour déterminer la cause initiale et remonter les étapes de l'attaque. En pratique, trier les informations peut prendre des jours – en d'autres termes, cela revient à chercher une aiguille dans une botte de foin.
L'intégrité des logs : le respect du standard des preuves
Si les logs ont été modifiés et qu'ils ne peuvent pas être présentés dans leur format original, l'intégrité des données de logs peut être remise en question lors d'une procédure légale. Les logs doivent respecter le standard légal des preuves, en étant collectés de manière inviolable. A contrario, les logs qui ont été modifiés ou qui n'ont pas été stockés de manière sécurisée, ne seront pas acceptés comme preuve légale dans une cour de justice.
Cependant, même pour les organisations qui ont implémenté des solutions fiables de collecte et de gestion des logs, l'information cruciale peut manquer et ce chainon manquant peut empêcher l'entreprise de reconstituer tout le cheminement de l'incident et ainsi de retrouver la source initiale du problème.

Les comptes à privilèges : une cible fructueuse pour les cybercriminels
En ciblant les administrateurs du réseau et autres comptes à privilèges qui disposent de droits d'accès étendus, voire sans aucune restriction au système d'information, aux bases de données, et aux couches applicatives, les cybercriminels s'octroient le pouvoir de détruire, de manipuler ou de voler les données les plus sensibles de l'entreprise (financières, clients, personnelles, etc.).

L'analyse comportementale : un rempart nouveau pour les entreprises
Les nouvelles approches de sécurité basées sur la surveillance des utilisateurs et l'analyse comportementale permettent aux entreprises d'analyser l'activité de chacun des utilisateurs, et notamment les événements malveillants, dans l'intégralité du réseau étendu.
Ces nouvelles technologies permettent aux entreprises de tracer et de visualiser l'activité des utilisateurs en temps réel pour comprendre ce qu'il se passe sur leur réseau. Si l'entreprise est victime d'une coupure informatique imprévue, d'une fuite de données ou encore d'une manipulation malveillante de base de données, les circonstances de l'événement sont immédiatement disponibles dans le journal d'audit, et la cause de l'incident peut être identifiée rapidement.
Ces journaux d'audit, lorsqu'ils sont horodatés, chiffrés et signés, fournissent non seulement des preuves recevables légalement dans le cadre d'une procédure judiciaire, mais ils assurent à l'entreprise la possibilité d'identifier la cause d'un incident grâce à l'analyse des données de logs.
Lorsque ces journaux sont complétés par de l'analyse comportementale, cela offre à l'entreprise une capacité à mener des investigations forensics beaucoup plus rapidement et à moindre coût, tout en répondant pro activement aux dernières menaces en temps réel… [Lire la suite]

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Liberté) ;
- 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

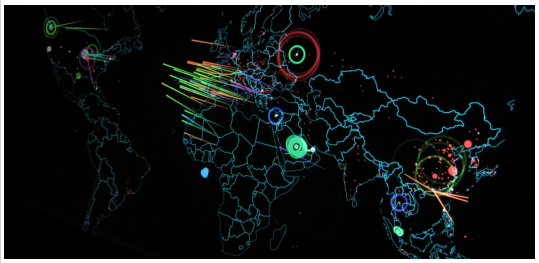
Réagissez à cet article

Source : *Recouvrer les traces d'une attaque informatique : l'investigation peut s'avérer complexe et coûteuse – JDN*

A quoi doit-on s'attendre en matière de cybersécurité à l'horizon 2020 ?

A quoi doit-on s'attendre en matière de cybersécurité à l'horizon 2020 ?

A l'heure où les objets connectés continuent de se déployer et où les piratages de données personnelles ou professionnelles se multiplient, quel avenir peut-on envisager en termes de cybersécurité ? Un groupe de chercheurs a élaboré plusieurs scénarios.



Le Centre pour la cybersécurité à long terme, un groupe de chercheurs pluridisciplinaires de l'Université de Berkeley en Californie, s'est questionné sur ce possible avenir en fonction de divers paramètres (déploiement de l'IoT, avancées technologiques, initiatives politiques, etc.). Et selon eux, plusieurs scénarios émergent :

• The New Normal décrit un monde où les cyberattaques à grande ou petite échelle seront, en 2020, autant légion que personnelles, dépassant les pouvoirs publics par leur nombre et leur ampleur, et encombrant les cours de justice de dossiers liés à la criminalité digitale – une sorte de « Far West 2.0 » dans lequel les utilisateurs n'hésiteraient pas à se rendre justice par eux-mêmes ;

• Omega conte, quant à lui, le futur de l'analyse prédictive : bien au-delà des études démographiques, la nouvelle génération d'algorithmes pourrait cibler plus étroitement les caractéristiques et préférences d'un individu donné, ce qui pourrait introduire un débat des plus clivants, à la frontière du philosophique et du politique, sur la manipulation comportementale ;

• Sensorium, enfin, dépeint l'évolution du *quantified self* jusqu'à faire d'Internet un vaste système de « lecteurs d'émotions », comme le souligne The Conversation, touchant du doigt les aspects les plus intimes de la psychologie humaine. Au risque que les données des applications de *quantified self* émotionnelles puissent être « retournées » contre leurs utilisateurs.

Plus d'informations et plus de scénarios ici.

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, 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

Réagissez à cet article

Source : *Quel avenir pour la cybersécurité à l'horizon 2020 ?* |

Paypal ne protégera plus les transactions crowdfunding

Paypal ne protégera plus les transactions crowdfunding

Trop d'arnaques au financement participatif ? Trop de remboursements pour des produits jamais livrés ? Paypal ne protégera plus les transactions crowdfunding à partir de la fin juin 2016.

Paypal semble ne plus apprécier les transactions bancaires entre ses utilisateurs et les projets lancés sur les portails de crowdfunding. Trop d'arnaques au Crowdfunding ? Á partir du 26 juin 2016, le géant de la finance, ne protégera plus les transactions effectuées sur les sites de financement participatif.
Trop d'arnaques au transactions crowdfunding ? Trop d'argent envolé sans le moindre produit/projet finalisé ? Bref, des problèmes se posent des deux côtés – vendeurs et acheteurs. Paypal ne veut tout simplement plus faire partie d'une équation qui le place au milieu des conflits. Par conséquent, vous pourrez toujours payer via Paypal, mais la structure financière n'assurera plus cette transaction. Elle sera à vos risques et périls.

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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, 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

Réagissez à cet article

Source : *ZATAZ Paypal ne protégera plus les transactions crowdfunding – ZATAZ*

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*

Des drivers USB dans le Cloud pour piloter à distance les périphériques

Piloter à distance des périphériques USB grace au Cloud, ca vous dit ?

Des ingénieurs de Google proposent une norme pour piloter à distance des périphériques USB, à travers un driver situé dans le Cloud, appelé uniquement lorsqu'il est nécessaire. Objectif : toujours mieux intégrer le Web et le hardware.

Deux ingénieurs de Google, Reilly Grant et Ken Rockot, proposent au World Wide Web Consortium (W3C) de travailler sur une nouvelle norme appelée WebUSB, qui permettrait de piloter à distance des périphériques USB sans avoir à installer de drivers sur son ordinateur. Le pilotage des appareils branchés au PC ou au Mac se ferait directement depuis le cloud.
L'idée est de faciliter l'utilisation des appareils USB qui sortent de l'ordinaire (par exemple un calibreur d'écran, une imprimante 3D, un circuit Arduino, un chauffe-tasse USB,…), et d'offrir aux services en ligne une API sécurisée qui permettrait de les configurer et de les exploiter quelle que soit la machine de l'utilisateur.

USB-plug

Puisqu'il n'y a plus de drivers à installer et que tout le pilotage se fait à distance par internet, les périphériques seraient fonctionnels aussi bien sous Windows que sous Mac OS, Linux… ou même Chrome OS ou Android. On voit donc bien l'intérêt pour Google d'une telle norme, qui accélérerait la « terminalisation » des ordinateurs, de plus en plus réduits à assurer l'affichage, alors que le stockage et la puissance de calcul sont déportés sur le cloud.
En pratique, la norme proposée prévoit que les constructeurs d'appareils USB puissent définir dans le firmware un ou plusieurs domaines (par exemple chauffe-tasse.numerama.com) qui sont autorisés à piloter ou à mettre à jour l'appareil. Seules les connexions sécurisées vers ces domaines seraient permises. Les autres sites internet qui veulent exploiter les possibilités d'un périphérique devraient alors intégrer le support du driver à travers une iframe, qui appelle le pilotage à travers une interface autorisée.

EN CONTREPARTIE, LES UTILISATEURS PERDENT ENCORE UN PEU PLUS LE CONTRÔLE DE LEURS APPAREILS

Grant et Rockot assurent que leur technique est même plus sûre que les drivers USB traditionnels, qui peuvent être piratés pour obtenir, par exemple, le contrôle à distance d'une webcam.
Pour défendre leur idée, les ingénieurs prennent l'exemple d'une imprimante 3D et d'un service de modèles 3D à télécharger, comme Thingiverse. Actuellement les utilisateurs sont obligés de télécharger un driver pour leur imprimante, ainsi qu'un logiciel d'impression. Ils doivent télécharger les fichiers STL des modèles 3D, et les ouvrir avec le logiciel d'impression. Mais avec leur idée, Thingiverse pourrait appeler l'API de l'imprimante de l'utilisateur (qui pourrait être déclarée au site par le navigateur), et offrir lui-même une application de calibrage et d'impression des modèles.
L'idée est loin d'être idiote, et c'est certainement une voie d'avenir. Mais elle signifie aussi, en contrepartie, que les utilisateurs perdent encore un peu plus le contrôle de leurs appareils. Ils n'auraient plus vraiment le choix des drivers à installer, ni la possibilité de les modifier pour installer d'autres drivers officieux.
.. [Lire la suite]

Réagissez à cet article

Source : *Des drivers USB dans le Cloud pour piloter à distance les périphériques – Tech – Numerama*

Morpho, le français qui fiche un milliard d'Indiens – Challenges.fr

Morpho, le français qui fiche un milliard d'Indiens

La filiale de Safran est en train de fournir une identité numérique à 1,2 milliard d'Indiens. Une base de données biométrique unique au monde, qui effraie certains.

Une base de données biométrique rassemblant 1,3 milliard d'individus, soit 18% de la population mondiale… C'est le défi incroyable que le français Morpho, filiale de Safran, est en train de relever en Inde.
Concrètement, le programme, baptisé Aadhaar (socle, en hindi), consiste à offrir un numéro d'identification unique à 12 chiffres à chaque citoyen. Cette identité numérique est sécurisée par la prise des données biométriques de son propriétaire: les 10 empreintes digitales, les 2 iris, et une photo du visage. Quatre ans après le début de l'opération, la base de données vient d'atteindre la barre symbolique du milliard d'individus fichés. « Chaque jour, jusqu'à 1 million de personnes peuvent être « enrôlées » dans le système », souligne Jessica Westerouen van Meeteren, directrice de la division Government Identity chez Morpho.
Pourquoi cette base de données géante? L'idée de départ du programme, lancé en 2009 par New Delhi, était d'offrir une existence officielle à des centaines de millions d'Indiens qui, faute de carte d'identité, restaient invisibles à l'administration, et donc exclus des programmes d'aide sociale. Dans un pays à l'administration pléthorique où la corruption reste importante, l'argent atterrissait souvent dans les mauvaises poches. Le numéro d'identification doit permettre de corriger le problème des fraudes à l'identité, mais aussi d'ouvrir un compte en banque simplifié ou d'obtenir un passeport plus facilement.

La complexité d'un programme spatial

Pour mener à bien ce projet colossal, le gouvernement indien a créé une agence d'Etat, la Unique Identification Authority of India (UIDAI).
Morpho est l'un des fournisseurs retenus par l'agence, avec le japonais NEC et l'américain L1 (autre filiale de Safran). Le groupe français fournit les scanners biométriques destinés à l'enregistrement des données, mais aussi la technologie de « dédoublonnement » qui permet de vérifier qu'un individu n'est pas déjà enregistré sous un autre numéro. Le système est capable de répondre à un million de requêtes par jour. « C'est un programme d'une complexité inédite dans le secteur, qu'on peut comparer à celle d'un programme spatial », assure Jean-Pierre Pellestor, directeur de programme chez Morpho.
Si le projet est en train d'arriver à bon port, c'est en grande partie grâce à l'action d'un homme: Nandan Nikelani, le cofondateur du géant de l'informatique indien Infosys. Le puissant homme d'affaires, qui fut le premier président de l'UIDAI, a pesé de tout son poids pour passer outre les légendaires pesanteurs de l'administration indienne. Au point que la loi avalisant le programme n'a été votée à la Lok Sabha, la chambre basse du parlement indien, que le 16 mars dernier… soit six ans après le début des opérations d'enregistrement. Nikelani avait même réussi à convaincre le premier ministre Narendra Modi, très critique contre Aadhaar durant la campagne électorale de 2014, de poursuivre le projet. « Modi l'a finalement accéléré », se félicite-t-on chez Morpho.

Risque de Big Brother?

Le programme ne fait pourtant toujours pas l'unanimité en Inde. Si plus d'un milliard de personnes ont accepté de s'enregistrer dans la base de données, d'aucuns y voient un Big Brother potentiel, qui pourrait être détourné au détriment de la vie privée des citoyens. « Le gouvernement peut-il nous assurer que Aadhaar et les données collectées ne vont pas être détournées comme ce qui a été fait par la NSA aux Etats-Unis? »,s'interrogeait auprès de Reuters Tathagata Satpathy, une avocate basé dans l'Odisha (est de l'Inde). L'accès au fichier pour un usage lié à la « sécurité nationale » fait notamment débat. « Le projet apporte une protection de la vie privée d'une grande robustesse, au-delà de tout ce qu'ont apporté les autres lois en Inde« , répondait mi-mars Nandan Nikelani à l'Indian Express.
En tout cas, Morpho espère bien surfer sur le contrat indien pour vendre d'autres systèmes similaires. « Nous avons des campagnes commerciales en cours dans d'autres pays sur des programmes comparables, mais la taille du projet indien restera probablement unique », détaille Jessica Westerouen van Meeteren. Mais la bonne santé de Morpho (1,9 milliard d'euros de chiffre d'affaires en 2015, en croissance organique de 11%) n'empêche pas le directeur général de Safran Philippe Petitcolin de réfléchir à son avenir, la division n'ayant pas vraiment de synergie avec le reste du groupe, ni le poids suffisant pour équilibrer les activités aéronautiques. Après avoir mis en vente l'activité de détection d'explosifs (Morpho Detection), le groupe pourrait annoncer la cession de toute la division dans le courant de l'année 2016… [Lire la suite]

Réagissez à cet article

Source : *Morpho, le français qui fiche un milliard d'Indiens – Challenges.fr*

Utilisateurs de Tor identifiés – Le FBI reste muet

Utilisateurs de Tor identifiés – Le FBI reste muet

Le FBI soppose à une demande de la justice qui exige de la police américaine quelle présente sa méthode lui ayant permis didentifier des utilisateurs d'un site pédopornographique, en les piratant.

Le FBI n'a absolument aucune envie de dévoiler la méthode secrète qu'il a employé pour pirater plus d'un millier de membres d'un site pédopornographique. Et cela, même si c'est la justice américaine qui lui demande.
C'est en effet ce qu'est en train de révéler le procès visant une personne accusée d'avoir fréquenté cet espace, dont l'accès ne pouvait se faire qu'à travers le réseau d'anonymisation TOR.
Dans cette affaire, les avocats du prévenu souhaitent connaître la technique utilisée par la police fédérale pour infecter les ordinateurs de ceux qui visitaient Playpen – le nom de ce site pédopornographique – lorsqu'il était encore en ligne.
Pour la défense, il s'agit de tenter de démontrer que le FBI a outrepassé ses prérogatives au cours de l'enquête, en débordant du cadre de son mandat.

Sceau FBI

L'approche du FBI dans l'affaire PlayPen fait polémique outre-Atlantique.
En février, le magistrat a donné suite à cette demande et exigé du FBI qu'il communique à la partie adverse tous les détails de sa méthode de piratage. Mais comme le pointe la BBC, le service de police est particulièrement hostile à cette demande. Un courrier a été adressé cette semaine au juge afin de l'inviter à reconsidérer sa position, estimant que la défense dispose déjà de suffisamment de pièces pour travailler.
En réalité, l'opposition du FBI vise avant tout à préserver l'intérêt de sa technique. En effet, il se pourrait qu'une communication des détails à la partie adverse affaiblisse l'efficacité de cette méthode. Si celle-ci devient publiquement connue, les failles qu'elle exploite seraient tôt ou tard colmatées par TOR, les navigateurs et les serveurs hébergeant des sites web. De même, les utilisateurs se montreraient aussi plus prudents.

LE FBI VEUT PRÉSERVER L'EFFICACITÉ DE SA MÉTHODE EN LA GARDANT SECRÈTE

C'est sans doute ce scénario que le FBI veut éviter, afin de pouvoir l'appliquer de nouveau à l'avenir si le besoin s'en fait sentir. Et si la position de la police fédérale se défend, celle de la défense, qui agit dans l'intérêt de son client, est tout aussi audible : le FBI a-t-il enfreint son mandat au nom de la loi ? Et la méthode employée est-elle vraiment fiable ? Une erreur au niveau de l'identification de l'internaute est toujours possible.
L'affaire Playpen remonte au tout début de l'année 2015, lorsque le FBI réussit à prendre le contrôle des serveurs du site pédopornographique. Plutôt que de le fermer immédiatement, ce qui a aussi provoqué son lot de critiques lorsque l'information a été révélée publiquement, la police opte pour une autre approche, celle du honeypot : le site est demeuré actif pendant près de deux semaines, en utilisant ses propres serveurs, de façon à voir qui se connecte sur Playpen.

Le principe du réseau TOR rappelle celui des couches de l'oignon qui masquent le cœur de la plante.
C'est à ce moment-là que le FBI a utilisé sa fameuse technique pour contaminer le poste informatique des visiteurs, afin, notamment, de récupérer leur véritable adresse IP, qui est habituellement cachée avec le réseau d'anonymisation TOR, puisque la connexion passe par une succession de relais afin de camoufler la géolocalisation du PC d'origine.
Une fois l'adresse IP en main, il a suffit de contacter les fournisseurs d'accès à Internet – en tout cas ceux aux USA – pour avoir l'identité des internautes. Au total, la technique du FBI a permis de collecter pas moins de 1 300 adresses IP… [Lire la suite]

Réagissez à cet article

Source : *Le FBI refuse de dire comment il identifie des utilisateurs de Tor – Politique – Numerama*