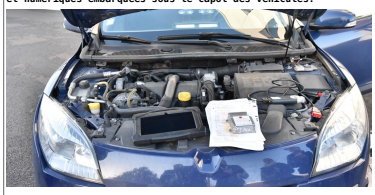
Policiers et gendarmes auront accès aux données embarquées des véhicules – Next INpact

	Policiers et gendarmes auront accès aux données embarquées des véhicules

L'Ordinateur de bord de votre voiture n'aura bientôt plus de secret pour les autorités. Une disposition adoptée dans le projet de loi sur la justice du XXIe siècle va autoriser gendarmes et policiers à fouiller les données physiques et numériques embarquées sous le capot des véhicules.



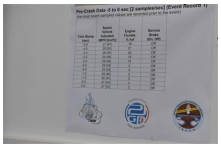
C'est un champ d'investigation suivi de près par les autorités, comme cela a pu nous être expliqué en janvier dernier, lors d'une visite au Pôle judiciaire de la Gendarmerie nationale de Cergy-Pontoise. Dans les véhicules les plus récents, les agents peuvent techniquement scruter tous les relevés techniques glanés quelques secondes avant un accident de la route. Vitesse, direction, freinage, etc. sont une mine d'informations pour confirmer ou fragiliser les affirmations du type : « *je roulais à 50 km/h, j'ai immédiatement freiné lorsque j'ai vu la future victime traverser la route* ».

Dans le projet de loi sur la justice du XXIe siècle, un amendement du gouvernement pousse davantage encore l'usage de ces investigations. Ce texte, numéroté CL180, avait été adopté en commission des lois début mai. Il a été conservé en l'état lors de la séance publique, la semaine dernière :
« *Art. L. 311-2. – Les agents compétents pour rechercher et constater les infractions au présent code, dont la liste est fixée par décret en Conseil d'État, ont accès aux informations et données physiques et numériques embarquées du véhicule afin de vérifier le respect des prescriptions fixées par le présent code* ».

L'article intègrera le titre Ier du Code de la route relatif aux dispositions techniques. Il autorisera les agents, désignés par décret, à avoir un plein accès aux données physiques et informatiques de votre véhicule. Pour cela, ils n'auront qu'à justifier de la recherche ou de la constatation d'une infraction au Code de la route. Si la pêche est bonne, alors on passera du contrôle à la possible sanction.

La cible, le diagnostic embarqué… mais pas seulement

Dans son exposé des motifs, le gouvernement souligne qu'il s'agit d'ouvrir « *notamment* » un accès « *aux systèmes de diagnostic embarqués* ». Concrètement, via un ordinateur portable connecté sur la prise de l'ordinateur de bord, policiers et gendarmes pourront prendre connaissance des données issues « *notamment* » des capteurs.



Analyses menées à Cergy-Pontoise Crédits : Marc Rees (CC BY SA 3.0)

Selon l'exécutif, la proposition a été soufflée par le comité interministériel de sécurité routière. Seulement, s'il l'envisage « *dans le cadre du contrôle du respect des dispositions techniques liées aux véhicules* », son texte est bien plus large. Le gouvernement a d'ailleurs ajouté cette phrase, à la fin de l'article : « *le fait que ces opérations révèlent des infractions autres que celles visées au premier alinéa ne constitue pas une cause de nullité des procédures incidentes* ». En clair, en recherchant des infractions au Code de la route, les agents pourront en toute quiétude découvrir d'autres éléments illicites, par exemple planqués dans un disque dur connecté au véhicule.

La latitude est d'autant plus large que n'est pas spécifié l'art et la manière dont aura lieu l'accès. Celui-ci pourra donc se faire par liaison physique (connexion par câble sur la prise du système embarquée), ou pourquoi pas à distance, avec le développement des véhicules connectés.

Le Syndicat de la magistrature réclame un encadrement de l'accès

De son côté, le Syndicat de la magistrature se dit « *hostile à l'introduction d'un [tel] article donnant accès aux informations et données physiques et numériques embarquées du véhicule sans autre condition que « pour rechercher et constater les infractions au présent code » et en permettant que les infractions révélées incidemment puissent être utilisées alors même qu'elles ne correspondent pas à celles recherchées* ». Selon le SM, une telle extension en effet, « *ne saurait être ainsi avalisée, sans aucun contrôle de nécessité ou de proportionnalité, ni procédure encadrant ces accès* ».

Adopté par les députés, mais non encore par les sénateurs, cet article va faire l'objet d'un arbitrage en Commission mixte paritaire dans les prochains jours.

Fichier des assurances, contrôles par lecture automatisé des plaques

Toujours dans le secteur de l'automobile, le même projet organise également la création d'un fichier des assurés, qui sera exploité par les dispositifs de contrôle automatisés et de vidéoverbalisation.

Un autre projet de loi, celui sur la réforme pénale a, lui, augmenté les hypothèses où les services de police, de gendarmerie nationale et des douanes pourront mettre en place une LAPI (ou Lecture automatique de plaques minéralogiques) ainsi qu'une prise photographique des occupants d'un véhicule. Ces hypothèses sont celles inscrites à l'article 706-73-1 du Code de procédure pénale, à savoir l'escroquerie en bande organisée, le travail dissimulé, le blanchiment, et même la non-justification des ressources… [Lire la suite]

Merci à Marc Rees, l'auteur de cet article

Réagissez à cet article

Source : *Policiers et gendarmes auront accès aux données embarquées des véhicules – Next INpact*

L'Écosse veut désactiver les téléphones utilisés en prison

L'Écosse veut désactiver les téléphones utilisés en prison

L'Écosse a trouvé possiblement une solution radicale pour lutter contre la présence des téléphones portables dans les prisons : elle veut tout simplement pouvoir faire désactiver la carte SIM en cause dans les mains des opérateurs.

Les tribunaux de shérif d'Écosse (ou «Sheriff courts») auront bientôt la compétence de contraindre les opérateurs télécoms à déconnecter les téléphones portables non autorisés dont on détecterait une utilisation en prison. Concrètement, le tribunal ordonnera à l'opérateur de réseaux de désactiver ou déconnecter un téléphone mobile et/ou une carte SIM. C'est le sens d'un texte qui vient d'être notifié à Bruxelles, cette disposition imposant une restriction normative dans un État membre.

Accéder aux réseaux sociaux, intimider les témoins

« *Des détenus ont utilisé des téléphones portables non autorisés pour accéder aux réseaux sociaux, intimider des témoins et poursuivre et contrôler leurs activités criminelles depuis les institutions pénitentiaires,* expliquent les autorités écossaises en appui de leur texte. *Ils représentent par conséquent une menace notable pour la sécurité et le bon fonctionnement des établissements pénitentiaires.* »

Le hic est qu'actuellement, « *il est extrêmement difficile de trouver à l'intérieur d'institutions pénitentiaires des cartes SIM en raison de leur taille. Si c'est moins le cas pour les téléphones portables, ces détenus qui ont pris possession de téléphones portables seront prêts à faire l'impossible pour empêcher la détection desdits téléphones, notamment par des menaces et l'intimidation d'autres personnes.* »

En France, le projet de loi sur la réforme pénale

Le texte pourra entrer en vigueur dans trois mois, une fois achevé le round de la notification bruxelloise. En France, si les pouvoirs du juge profitent théoriquement d'une large latitude pour ordonner ce type de mesure, dans le projet de loi sur la réforme pénale, la réaction du législateur gagne plusieurs crans au-dessus par rapport aux textes antérieurs.

D'un, le pénitentiaire va devenir un service du renseignement. De deux, les autorités, qu'elles soient judiciaires ou administratives et sans qu'on sache très bien où se placera la frontière de leurs compétences, pourront installer une ribambelle de dispositifs techniques pour détecter des communications, et notamment des IMSI catchers. De là, elles seront en capacité d'effectuer des interceptions de sécurité pour prendre connaissance des correspondances échangées avec l'extérieur, etc… [Lire la suite]

Marc Rees auteur de cet article

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 : *L'Écosse veut désactiver les téléphones utilisés en prison – Next INpact*

Deux applications accusées

d’espionner les coureurs

Deux applications accusées d’espionner les coureurs

Les applications Runkeeper et Tinder viennent d'être dénoncées par le conseil des consommateurs norvégien. En effet, elles exploiteraient illégalement les données des utilisateurs.

Si vous ne le savez pas encore, Runkeeper est une application qui permet de mesurer ses performances sportives. Si on parle d'elle aujourd'hui, ce n'est pas vraiment pour les fonctionnalités qu'elles proposent, mais plutôt pour un sujet plus serré. En effet, cette application qui est la possession de la société FitnessKeeper violerait les règles de confidentialité des données personnelles. D'après le NCC (conseil des consommateurs norvégien), afin de pouvoir évaluer l'état de l'utilisateur, elle doit d'abord accéder à des fonctionnalités stratégiques telles que la géolocalisation.
Et le comble dans tout cela, c'est le fait que les données de l'utilisateur ayant été collectées seraient ensuite utilisées pour des finalités commerciales. En effet, elles seraient revendues à des entreprises de publicité et seraient même sauvegardées même après la suppression du compte. En tout cas, c'est ce qu'avance un rapport qui date du 10 mai. Interrogé sur cette question, le fondateur de Runkeeper a indiqué que le problème vient d'un bug. « Nous sommes en train de sortir une nouvelle version de notre application qui élimine ce bug… Nous prenons au sérieux la confidentialité des données des utilisateurs… », a-t-il indiqué. Par ailleurs, outre l'application Runkeeper, le NCC pointe aussi du doigt l'application Tinder, laquelle est une application pour les fans de rencontre amoureuse. Elle, aussi, conserverait les données des utilisateurs, notamment, les photos et les conversations… [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 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

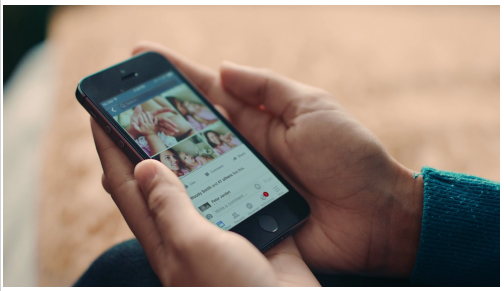
Source : *Runkeeper et Tinder : les deux applications accusées d’espionner les coureurs – MeilleurActu*

Facebook vous traque sur le Web même si vous n’êtes pas membre

Facebook vous traque sur le Web même si vous n’êtes pas membre

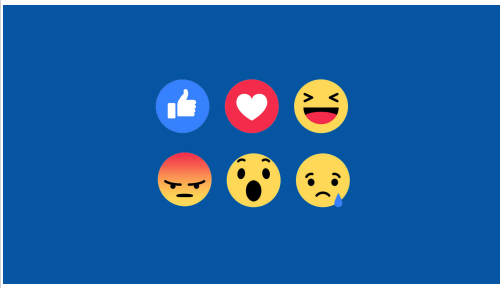
---

Facebook devient une régie publicitaire ouverte aux sites tiers, et affichera des publicités ciblées y compris pour les internautes qui ne sont pas inscrits sur le réseau social. Il utilisera ses scripts présents sur de nombreux sites pour suivre l'internaute dans ses déplacements sur le Web, et comprendre ce qui l'intéresse.

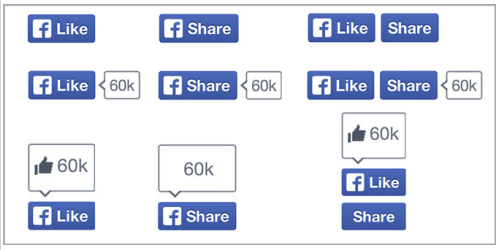


On connaît tous une ou deux personnes qui se refusent à utiliser Facebook et échappent encore et toujours aux griffes du réseau social. Mais l'empire de Mark Zuckerberg ne cesse de s'étendre et touchera bientôt même ces irréductibles qui n'ont jamais ouvert de compte sur la plateforme.

L'entreprise a annoncé qu'elle allait diffuser des annonces à tous les visiteurs de sites utilisant sa régie publicitaire Facebook Audience Network, concurrente de Google Adsense. Autrement dit, même les personnes qui ne sont pas inscrites sur Facebook et celles qui n'y sont pas connectées seront ciblées par des publicités qui, jusqu'ici, n'étaient visibles que par les personnes connectées au réseau social.
Ce n'est un secret pour personne, la force de Facebook réside dans sa capacité à récolter des données sur ses utilisateurs. Grâce à cela, il peut facilement montrer des publicités ciblées et adaptées sur mesure en fonction des préférences identifiées. Une aubaine pour les annonceurs qui ne perdent ainsi pas de temps et d'effort à diffuser tous azimuthes leurs contenus.



TRAQUER LES HABITUDES DE TOUS LES INTERNAUTES
Mais comment Facebook peut-il en faire de même avec les personnes qui ne se trouvent pas dans son réseau ? Il va utiliser plusieurs outils à sa disposition pour traquer efficacement un maximum d'internautes, comme le fait Google. Facebook va ainsi se servir de cookies, de ses propres boutons et plugins de partage affichés sur les sites, ainsi que d'autres informations collectées sur les sites tiers.
« Nos boutons et nos plugins envoient des informations de base sur les sessions de navigation des utilisateurs. Pour les non-membres de Facebook, auparavant nous ne les utilisions pas. Maintenant nous allons les utiliser pour mieux comprendre comment cibler ces personnes », assume très clairement Andrew Bosworth, vice-président de Facebook en charge des publicités et de la plateforme commerciale.



Ce dispositif permettra à Facebook de repérer les habitudes des internautes en insérant des bouts de codes dans les cookies et dans les boutons ou autres contenus « embeddés », qui permettront d'identifier l'internaute, soit directement en tant que membre de Facebook, soit par un numéro unique qui lui sera attribué. Si vous visitez régulièrement un site de cuisine, Facebook affichera des publicités pour une cocotte-minute ou une friteuse sur les autres sites que vous fréquentez, en rémunérant le site qui les affiche.

QUELLE LÉGALITÉ EN EUROPE ?
Ce changement de politique de Facebook va certainement mécontenter une partie de la communauté des internautes, y compris chez les membres qui pourront continuer à être suivis même lorsqu'ils sont déconnectés du réseau social. Elle pourrait surtout déclencher les foudres des autorités si le système est déployé en Europe.
Lorsque la justice belge avait condamné Facebook à ne plus tracer les Belges non-membres de Facebook, le réseau social s'était fait fort de crier à l'injustice, en prétendant que son cookie (le DATR) avait pour seul intérêt de lutter contre le spam. « Nous utilisons le cookie datr depuis plus de 5 ans pour sécuriser Facebook pour 1,5 milliard de personnes à travers le monde », s'était agacé le réseau social. Or six mois plus tard, Facebook prouve que les autorités avaient raison de s'inquiéter.
En France aussi, la Cnil a demandé à Facebook de ne plus tracer les internautes qui ne sont pas inscrits et connectés sur le réseau social. Avec d'autres homologues, elle avait estimé que Facebook devait « se conformer à ce jugement (belge) sur tout le territoire de l'Union européenne ».
Selon la législation européenne, il est illégal de réaliser un traitement de données personnelles à des fins commerciales, sans le consentement explicite de la personne. Or si ce consentement peut être donné à l'inscription par Facebook, il ne peut certainement pas l'être par les non-membres… [Lire la suite]

Article de Omar Belkaab

Réagissez à cet article

Source : *Facebook vous traquera sur le Web même si vous n'êtes pas membre – Business – Numerama*

Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue

Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue

---

Les chercheurs d'ESET découvrent un malware qui a échappé à la surveillance des chercheurs d'antivirus depuis au moins 2008. Ce malware, nommé Win32/Prikormka et détecté par ESET comme malware utilisé pour mener des activités de cyber-espionnage, cible principalement les séparatistes anti-gouvernementaux des républiques autoproclamées de Donetsk et Luhansk.

« Avec la crise ukrainienne de l'EST du pays, ce dernier a connu de nombreuses cyber-attaques ciblées ou de menaces persistantes avancées (APTs). Nous avons découvert par le passé plusieurs attaques utilisant des logiciels malveillants tels que BlackEnergy qui avait entraîné une panne d'électricité. Mais dans l'opération **Groundbait**, l'attaque utilise des logiciels malveillants qui n'avaient encore jamais été utilisés. », explique Robert Lipovský, ESET Senior Malware Researcher.
Le vecteur d'infection principalement utilisé pour diffuser les logiciels malveillants dans l'opération Groundbait est le spear-phishing. «Au cours de nos recherches, nous avons observé un grand nombre d'échantillons ayant chacun son numéro de campagne ID désigné, avec un nom de fichier attrayant pour susciter l'intérêt de la cible. », explique Anton Cherepanov, Malware Researcher chez ESET.
L'opération a été nommée **Groundbait** (appât) par les chercheurs d'ESET suite à l'une des campagnes des cybercriminels. Alors que la majorité des autres campagnes utilisent les thèmes liés à la situation géopolitique actuelle de l'Ukraine et la guerre de Donbass pour attirer les victimes dans l'ouverture de la pièce jointe, la campagne en question, elle, affiche une liste de prix d'appâts de pêche à la place.
« Pour l'heure, nous ne sommes pas en mesure d'expliquer le choix de ce document comme leurre », ajoute Lipovský.
Comme c'est souvent le cas dans le monde de la cybercriminalité et des APTs, il est difficile de trouver la source de cette attaque. Nos recherches à ce sujet ont montré que les cybercriminels viennent très probablement de l'intérieur de l'Ukraine. Quoi qu'il en soit et au vu des cibles choisies, il est probable que cette opération de cyber-surveillance soit nourrie par une motivation politique. « En dehors de cela, toute nouvelle tentative d'attribution serait à ce point spéculatif. **Il est important de noter que, outre les séparatistes, les cibles de cette campagne sont les responsables gouvernementaux ukrainiens, les politiciens et les journalistes.** La possibilité de l'existence de fausses bannières doit également être prise en compte. », conclut Robert Lipovský.

Vous trouverez davantage de détails au sujet de l'opération Groundbait ici.

Article de Benoit Grunemwald
Directeur Commercial & Marketing ESET France

Réagissez à cet article

Source : *Découverte ESET sur le Cyber-espionnage des séparatistes ukrainiens : surveillance continue*

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

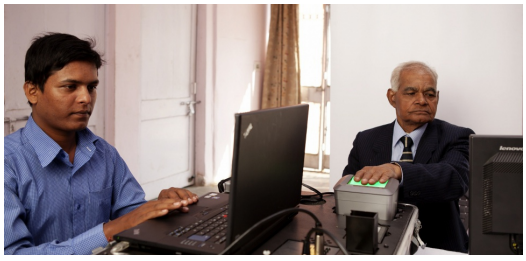
Airbus déjoue douze attaques informatiques majeures par an

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

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*

Les sites pour enfants se transformeraient-ils en pièges pour voler les données personnelles de leurs parents ?

Les sites pour enfants se transformeraient-ils en pièges pour voler les données personnelles de leurs parents ?

Les hackers ne sont jamais à court d'idées lorsqu'il s'agit de pirater vos données personnelles. En témoigne le recours aux sites pour jeunes publics dont les contenus sont truffés de malwares. Un phénomène déjà observable sur les sites pornographiques.

Atlantico: Les sites pour enfants sont-ils les plus pollués par les virus ?

Fabrice Epelboin: Les malwares qui infectent les sites le font le plus souvent de façon opportuniste : ils profitent d'une faille de sécurité sur un site pour l'infecter et en faire un vecteur d'attaque enver ses visiteurs. A ce jeu, ce sont plutôt les amateurs de pornographie, qu'on devine adultes et plutôt masculins, qui sont les premier visés, non pas pour ce penchant particulier, mais plus pour la multitude de failles de sécurité que l'on trouve sur ces sites, ainsi que la facilité qu'il y a d'en monter de nouveaux dans le seul but d'infecter ses visiteurs.
Les contenus sont faciles à trouver et à réagencer, et les réseaux publicitaires dédiés à ce type de contenus peu regardant sur les publicités qu'ils véhiculent – potentiellement infectées ou menant vers des sites infectés. L'utilisation d'un adblocker est d'ailleurs en passe de devenir une bonne pratique en matière de sécurité informatique si vous surfez sur ce genre de site.
L'idée que les enfants soient plus particulièrement visés relève plus à mon avis du fantasme. Certes leurs compétences en sécurité informatique n'est pas bien élevée, mais de nos jours, on peut en dire de même pour la plupart des parents, qui sont tout aussi faciles à piéger, parfois avec des moyens d'une simplicité désarmante.
Quand je vois la fréquence avec laquelle des personnes du troisième âge se transmettent des documents Powerpoint remplis de chatons sous forme de slideshows remplis de macro infectés, je me dis que les afficionados de LOLcats sont probablement les plus à risque, au même titre que les amateurs compulsifs de pornographie.

Comment procèdent les cyber-criminels pour tenter les jeunes consommateurs ?

Comme avec les adultes : en leur proposant des contenus gratuits qui les séduisent, voir en poussant à installer sur leur machine des logiciels dont ils ignorent tout. Il est courant, sur les sites de téléchargement de contenus piratés, de télécharger, en guise de contenu, un éxécutable portant le nom du contenu désiré. Les chances d'infecter sa machine en lançant un tel éxécutable sont proches de 100%. Les enfants, comme la plupart des adultes, peuvent se faire avoir.
Dans le cas relevé récemment par la BCC, on attire non pas les enfants, mais les joueurs de Minecraft avec un "mod", un programme qui va ajouter une fonctionnalité au jeu et qui, au passage, va infecter la machine sur laquelle il est installé. Cette attaque aurait tout aussi bien pu viser un adulte – ils sont nombreux à jouer à Minecraft – et n'a été évitée, dans ce cas, que du fait de la compétence en sécurité informatique du père, ce qui n'est pas si courant que cela.
Le cas de figure le plus courant est plutôt le suivant : des parents parfaitement ignorants de la chose informatique et des enfants débrouillards, pas forcément en sécurité informatique, mais dans le contournement de tous les obstacles que leurs parents auraient pu mettre en place en matière de sécurité. C'est un domaine où la valeur n'attend pas le nombre des années, à l'image de ce garçon de 12 ans qui a mis en place un stratagème pour mettre à jour le code secret du coffre fort de ses parents.

Quel risque pour nos données numériques ?

De se les faire dérober, la plupart du temps. Selon les données, cela peut représenter un risque plus ou moins grand. Vous pouvez être victime, une fois vos coordonnées dérobées, de multiples campagnes de phishing, d'usurpation d'identité, ou pire, de ransomware – particulièrement à la mode ces temps ci – un malware qui va chiffrer les données de votre disque dur et vous réclamer une rançon pour les déchiffrer.
Dans le cas où c'est une agence de renseignements qui dérobe vos données, les risques sont différents. Si vous êtes un opposant politique, vous risquez d'être surveillé de près de façon à perturber vos activités et mettre à jour vos réseaux politiques ; si vous êtes un journaliste d'investigation, on s'interessera plutôt à vos sources ; et si vous travaillez dans une entreprise sensible ou présente dans des marchés internationaux, on peut se servir de vos données pour attaquer votre employeur.

Les sécurités parentales servent-elles à quelque chose ?

Si votre enfant n'est pas très éveillé, oui, cela peut être utile. S'il est malin, non, il se fera un plaisir de contourner tout cela. Les "sécurités parentales" servent, la plupart du temps, à interdire l'accès aux contenus pornographiques aux enfants. C'est à mon sens une illusion – surtout dès qu'on parle d'adolescents – et cela ne fait que rendre ces contenus plus désirables.
Ces filtres parentaux ont systématiquement été contournés, et le mode d'emploi pour le faire se retrouve tôt ou tard sur Internet. Cela ne peut que pousser les enfants à comprendre comment ils marchent pour les désactiver, et cela aurait presque des vertus pédagogiques en matière d'éveil des enfants aux technologies, mais les conséquences sont fâcheuses, c'est le moins que l'on puisse dire, d'autant que cela ne fera que creuser l'écart de compétences entre les enfants et leurs parents, au détriment de ces derniers.
En pratique, rien ne remplace l'éducation, mais encore faut-il maîtriser un domaine pour éduquer ses enfants à celui-ci, ce qui ramène encore une fois vers la transmission au plus grand nombre d'un ensemble de règles de base en matière de sécurité informatique, à la façon d'un permis de conduire qui permet à chaque automobiliste de se sécuriser et de sécuriser les autres par la même occasion, en appliquant à la lettre un ensemble de règles simples.
Le problème c'est que personne n'est véritablement responsable de cette transmission d'information. Ni l'école – le primaire, le secondaire comme le supérieur – ni l'entreprise ne se sont saisis de cette mission. Or, chacun de ces acteurs pourrait tout à fait mettre en œuvre des programmes pédagogiques simples qui permettrait à tout un chacun d'échapper à une large partie des pièges tendus par les cybercriminels. On pourrait enseigner cela dès l'école primaire. On pourrait intégrer cela dans la formation permanente des employés – ce serait du reste très rentable pour les entreprises qui perdent des fortunes du fait d'attaques informatiques qui tirent parti de l'ignorance de leurs employés… [Lire la suite]

Réagissez à cet article

Fabrice Epelboin est enseignant à Sciences Po et cofondateur de Yogosha, une startup à la croisée de la sécurité informatique et de l'économie collaborative.

Source : *Quand les sites pour enfants se transforment en pièges pour voler les données personnelles de leurs parents | Atlantico.fr*