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.

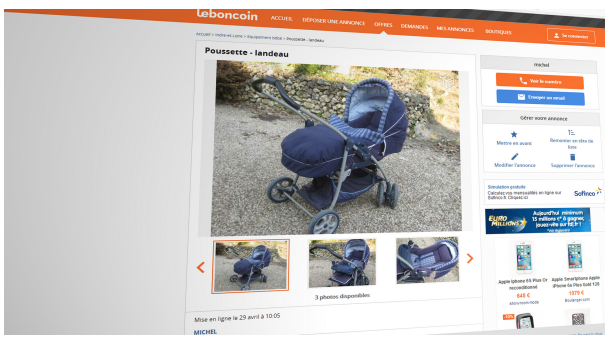
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

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

Et si le Sénat obligeait Le Bon Coin à déclarer au fisc les produits vendus



Et si le Sénat obligeait Le Bon Coin à déclarer au fisc les produits vendus

---

Le Sénat a imposé vendredi au gouvernement un nouvel article du projet de loi numérique, qui ferait obligation à toute plateforme en ligne de déclarer à l'administration fiscale tout revenu obtenu grâce à elle par chacun de ses utilisateurs.

Les vives protestations d'Axelle Lemaire n'y auront rien changé. Vendredi matin, les sénateurs ont refusé de supprimer l'article 23 quater du projet de loi numérique qui avait été ajouté en commission des finances du Sénat, qui obligera toutes les plateformes web à déclarer au fisc l'ensemble des « revenus bruts » perçus par un utilisateur à travers les servives qui y sont offerts.
Cela vise par exemple les petites annonces intégrées à Facebook, les chambres louées sur AirBnb, ou les vélos revendus sur Le Bon Coin.

leboncoin
Le texte, qui devra être confirmé en commission mixte paritaire (CMP), impose que tout « opérateur de plateforme en ligne », qu'il serve ou non d'intermédiaire pour le paiement, devra transmettre annuellement à l'administration fiscale toute une série d'informations sur les activités de chacun de ses utilisateurs « présumés redevables de l'impôt en France » :
1° Pour une personne physique, le nom, le prénom et la date de naissance de l'utilisateur ;
2° Pour une personne morale, la dénomination, l'adresse et le numéro Siren de l'utilisateur ;
3° L'adresse électronique de l'utilisateur ;
4° Le statut de particulier ou de professionnel caractérisant l'utilisateur sur la plateforme ;
5° Le montant total des revenus bruts perçus par l'utilisateur au cours de l'année civile au titre de ses activités sur la plateforme en ligne, ou versés par l'intermédiaire de celle-ci ;
6° La catégorie à laquelle se rattachent les revenus bruts perçus ;
7° Toute autre information définie par décret, à titre facultatif ou obligatoire.
L'obligation est sans exceptions et commence donc dès le premier euro reçu, voire même dès l'inscription sur n'importe quelle plateforme. Il ne précise pas non plus que ces données ne doivent être transmises que si la plateforme en a connaissance, ce qui laisse un flou sur l'éventuelle obligation des plateformes web de collecter toutes les données qu'elles n'ont pas actuellement. Faudra-t-il qu'elles s'assurent de l'identité des utilisateurs pour transmettre les bonnes informations ou fisc, ou que Le Bon Coin, par exemple, se mette à vérifier si un objet mis en vente a bien été vendu au prix annoncé ?

L'amendement vise tout « opérateur de plateforme en ligne », défini comme :
Toute personne physique ou morale proposant, à titre professionnel, de manière rémunérée ou non, un service de communication en ligne reposant sur :
1° Le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par des tiers ;
2° Ou la mise en relation de plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un contenu, d'un bien ou d'un service.

C'EST PAS PARCE QU'ON VEND UNE POUSSETTE QU'IL FAUT LE DÉCLARER
La secrétaire d'État au numérique Axelle Lemaire a tenté de faire entendre raison au Sénat, qui est aux mains de l'opposition, mais en vain. Les sénateurs sont apparus obsédés par l'idée de tout savoir sur les revenus obtenus par les internautes à travers le Web (peu importe qu'il y ait bénéfice ou non), pour s'assurer qu'ils soient bien déclarés en bonne et due forme à la fin de l'année.

senat-lemaire-2
« L'objectif est louable », a admis Axelle Lemaire, en pointant toutefois du doigt une série de problèmes, en particulier pour la vie privée. « C'est irréaliste et dangereux », a-t-elle lancé, en s'insurgeant contre l'idée que tout ce qui est fait en ligne devrait être connu de l'État. « Ce n'est pas parce que c'est du numérique qu'il faut tout déclarer ! C'est pas parce qu'on vend une poussette qu'il faut la déclarer ».
« Ce que vous proposez est trop complexe, ça ne pourra pas être mis en œuvre », a-t-elle de toute façon prévenu. Les modalités d'application étant laissées à un décret, il est fort probable que même s'il était confirmé en CMP, un tel décret ne verra jamais le jour.
« À l'heure actuelle, il n'y a que deux catégories d'organisations ou d'entités qui ont une obligation de transmission à l'administration : les banques, et les employeurs. Étendre une telle obligation à des plateformes pour tous les secteurs, dans tous les cas de figure, risque de mettre un véritable coup de frein à l'économie collaborative »… [Lire la suite]

Source : *Vous revendez votre poussette ? Le Sénat oblige Le Bon Coin à le déclarer au fisc – Politique – Numerama*

Fuite, perte, piratage de données ? Entreprise, il va falloir communiquer ! – Data Security BreachData Security

Breach

	**Fuite, perte, piratage de données ? Entreprise, il va falloir communiquer !**

La directive européenne de protection des données personnelles est morte ! Vive le règlement général sur la protection des données (GDPR). Fuite, perte, piratage de données ? Entreprise, il va falloir communiquer !

En 1995, l'Europe s'équipait de la directive européenne de protection des données personnelles. Mission, protéger les informations des utilisateurs d'informatique. 21 ans plus tard, voici venir le règlement général sur la protection des données (GDPR). La Commission européenne avait proposé en 2012 un nouveau règlement portant sur un ensemble de règles unique pour toutes les données collectées en ligne afin de garantir qu'elles soient conservées de manière sûre et de fournir aux entreprises un cadre clair sur la façon dont les traiter.

Mercredi 13 avril 2016, le paquet législatif a été formellement approuvé par le Parlement dans son ensemble. Le GDPR impose aux entreprises (petites ou grandes) détenant des données à caractère personnel d'alerter les personnes touchées par une fuite, une perte, un piratage de la dire informations privée.

Grand groupe, PME, TPE doivent informer les autorités de contrôle nationales (CNIL) en cas de violation importante de ces données.
Comme je pouvais déjà vous en parler en 2014, il faut alerter les autorités dans les 72 heures après avoir découvert le problème. Les entreprises risquent une grosse amende en cas de non respect : jusqu'à 4% de son chiffre d'affaire. Les informations que nous fournissons doivent être protégées par défaut (Art. 19). A noter que cette régle est déjà applicable en France, il suffit de lire le règlement de la CNIL à ce sujet. Faut-il maintenant que tout cela soit véritablement appliqué.

Fuite, perte, piratage de données
Parmi les autres articles, le « 7 » indique que les entreprises ont l'obligation de demander l'accord « *clair et explicite* » avant tout traitement de données personnelles. Adieu la case par défaut imposée, en bas de page. De l'opt-in (consentement préalable clair et précis) uniquement. Plus compliqué à mettre en place, l'article 8. Je le vois dans les ateliers que je mets en place pour les écoles primaires et collèges. Les parents devront donner leur autorisation pour toutes inscriptions et collectes de données. Comme indiqué plus haut, les informations que nous allons fournir devront être protégées par défaut (Art. 19). Intéressant à suivre aussi, l'article 20. Comme pour sa ligne téléphonique, le numéro peut dorénavant vous suivre si vous changez d'opérateur, cet article annonce un droit à la portabilité des données. Bilan, si vous changez de Fournisseur d'Accès à Internet par exemple, mails et contacts doivent pouvoir vous suivre. L'histoire ne dit pas si on va pouvoir, du coup, garder son adresse mail. 92829@orange.fr fonctionnera-t-il si je passe chez Free ?
La limitation du profilage par algorithmes n'a pas été oublié. En gros, votre box TV Canal +, Orange ou Netflix (pour ne citer que le plus simple) utilisent des algorithmes pour vous fournir ce qu'ils considèrent comme les films, séries, émissions qui vous conviennent le mieux. L'article 21 annonce que l'algorithme seul ne sera plus toléré, surtout si l'utilisateur n'a pas donné son accord.
Enfin, notre vie numérique est prise en compte. Les articles 33 et 34 s'annoncent comme les défenseurs de notre identité numérique, mais aussi notre réputation numérique. L'affaire Ashley Madisson est un des exemples. Votre identité numérique est volée. L'entreprise ne le dit pas. Votre identité numérique est diffusée sur Internet. Vous ne la maîtrisez plus.
Bref, 33 et 34 annonce clairement que les internautes ont le droit d'être informé en cas de piratage des données. La CNIL sera le récipiendaire des alertes communiquées par les entreprises piratées. Bref, fuite, perte, piratage de données ? Entreprise, il va falloir communiquer !
Les entreprises ont jusqu'au 1er janvier 2018 pour se mettre en conformité. Les 28 pays membres doivent maintenant harmoniser leurs lois sur le sujet. Je me tiens à la disposition des entreprises, associations, particuliers qui souhaiteraient réfléchir à leur hygiène informatique.

Police : nouvelles règles sur les transferts de données
Le paquet sur la protection des données inclut par ailleurs une directive relative aux transferts de données à des fins policières et judiciaires. La directive s'appliquera aux transferts de données à travers les frontières de l'UE et fixera, pour la première fois, des normes minimales pour le traitement des données à des fins policières au sein de chaque État membre.
Les nouvelles règles ont pour but de protéger les individus, qu'il s'agisse de la victime, du criminel ou du témoin, en prévoyant des droits et limites clairs en matière de transferts de données à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales – incluant des garanties et des mesures de prévention contre les menaces à la sécurité publique, tout en facilitant une coopération plus aisée et plus efficace entre les autorités répressives.

« ***Le principal problème concernant les attentats terroristes et d'autres crimes transnationaux est que les autorités répressives des États membres sont réticentes à échanger des informations précieuses*** », a affirmé Marju Lauristin (S&D, ET), députée responsable du dossier au Parlement.
« ***En fixant des normes européennes sur l'échange d'informations entre les autorités répressives, la directive sur la protection des données deviendra un instrument puissant et utile pour aider les autorités à transférer facilement et efficacement des données à caractère personnel tout en respectant le droit fondamental à la vie privée***« , a-t-elle conclu… [Lire la suite]

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

- Expertise techniques et judiciaire en litige commercial, piratages, arnaques Internet;
- Expertise de systèmes de vote électronique;
- Formation en cybercriminalité;
- Formation de C.I.L. (Correspondants Informatique et Libertés);
- Accompagnement à la mise en conformité CNIL de votre établissement.

Contactez-nous

Suivez nous sur

Réagissez à cet article

Source : *Fuite, perte, piratage de données ? Entreprise, il va falloir communiquer ! – Data Security BreachData Security Breach*

Mieux connaître le consommateur avec ses données

Mieux connaître le consommateur avec l'analyse prédictive et le Big Data

Grâce aux nouvelles technologies et particulièrement aux réseaux sociaux, il est désormais possible d'étudier tout ce que font vos clients.

Grâce aux nouvelles technologies et particulièrement aux réseaux sociaux, il est désormais possible d'étudier tout ce que font vos clients. Habitudes d'achat, fréquence et lieux des visites, horaires… Toutes ces informations forment une base de données gigantesque et sans cesse en mouvement. C'est ce que l'on nomme « Big Data » et il s'agit d'une véritable mine d'or pour les professionnels du marketing. Fini les suppositions logiques et autres préjugés, l'analyse prédictive permet maintenant de dégager des statistiques et schémas de consommation concrets.

D'où viennent les informations qui composent le Big Data ?

Chaque fois que vous activez votre géolocalisation en consultant un site internet ou une application, cela laisse une trace. Les données du Big Data sont également composées par vos habitudes de navigation sur le net, les endroits où vous vous rendez, combien de temps vous restez, d'où vous venez, ce que vous regardez… Bien sûr toutes ces informations sont rendues anonymes, mais vos terminaux, dont votre smartphone, sont de véritables espions dans votre poche. Un data scientist, tels que sont nommés les experts du Big Data, s'intéressera aux patterns et croisera vos données avec celles de milliers d'autres personnes. Il s'agira par exemple de créer des algorithmes adaptés aux habitudes de navigation des utilisateurs d'un moteur de recherche. L'idée est d'aller chercher dans les données des tendances, et d'identifier des comportements. Analyser, comprendre… puis prédire les actions futures. Cela est désormais possible et relativement simple avec les outils dont disposent les analystes.

Le Big Data, un outil d'analyse prédictive qu'il faut savoir exploiter

Si le Big Data peut servir à améliorer l'expérience des utilisateurs d'un produit, il révèle surtout son potentiel dans le secteur du marketing. Grâce à l'analyse du flot des données, il est possible d'établir des segments toujours plus pertinents. Finie la publicité « à destination de la ménagère de 40 ans ». Vous êtes désormais en mesure de savoir qui est réellement susceptible d'utiliser vos produits, et avec quel argument mettre en avant votre offre. Bien sûr, cela demande un réel travail d'analyse et ce n'est pas un hasard si vous voyez fleurir les offres d'emploi de data scientist ou de data mining. Le marketing et l'analyse prédictive deviennent des travaux de statisticien. Cela demande également de disposer des bons outils. Il s'agit d'un investissement en plusieurs étapes :

1. Vous collectez les données transmises par toutes les sources pertinentes ;
2. Vous analysez les données et isolez les schémas de consommation qui vous intéressent. L'étude de leurs occurrences sera la base de vos analyses prédictives ;
3. Enfin, vous établissez une stratégie de marketing ciblée en fonction des résultats obtenus.

Pour une efficacité maximale, la majeure partie de ce processus sera automatisée. Pour gagner en efficacité mais aussi en efficience grâce à des outils de traitement des données en temps réel, il est possible de créer des processus semi-automatisés. L'intervention humaine n'est plus utile ? C'est le contraire. Elle est essentielle. L'œil humain est là pour aller chercher dans les données, fouiner et faire émerger des signaux faibles. La technologie libère le potentiel des données, mais il faut une intervention humaine pour bien utiliser ces outils, et en tirer des décisions actionnables.

Comment se servir de l'analyse prédictive pour optimiser son ROI ?

S'il peut être intéressant d'analyser le Big Data pour de multiples raisons, en matière de marketing l'objectif est avant tout d'améliorer votre ROI (Return On Investment). Pour cela, votre démarche analytique doit s'inscrire dans un plan d'action concret.
Que vous soyez spécialisé dans le e-commerce ou que vous réalisiez toutes vos ventes dans des magasins physiques, utilisez les données pour améliorer votre marketing digital.

Lancez des campagnes de marketing ciblées ;

Démarquez-vous du flot de publicité, et adaptez votre proposition aux envies réellement exprimées de vos clients.
Mais l'analyse prédictive ne sert pas qu'à générer des ventes. Elle trouve aussi son utilité dans le maintien de la relation client. Il est par exemple possible de déterminer quand un client est sur le point de résilier un abonnement, quand celui-ci est sur le point de basculer chez un concurrent… pour pouvoir le retenir ! A l'aide de ces informations contenues dans votre Big Data, vous pouvez améliorer votre taux de fidélité en adaptant vos offres au bon moment. Un exemple ? La chaîne d'hôtel Hyatt utilise désormais l'analyse prédictive pour donner à son personnel d'accueil des informations supplémentaires sur les clients. En analysant la recherche menée par ces derniers sur le site et les applications du groupe, Hyatt précise si un client peut être intéressé par une chambre avec vue (car il a regardé plusieurs fois la page) ou s'il désire peut-être une chambre avec des oreillers anallergiques, car il a tapé ce mot clé dans le moteur de recherche interne… Un bel exemple de personnalisation de la relation client, grâce aux données.M… [Lire la suite]

Suivez nous sur

Réagissez à cet article

Source : *Analyse prédictive et Big Data : mieux connaître le consommateur avec ses données*

Un piratage sur Tor par le FBI prive les victimes d'une justice

Un piratage sur Tor par le FBI prive les victimes d'une justice

---

La lutte contre la pédocriminalité est une absolue nécessité, qui exige une absolue rigueur. Un juge américain a dû invalider un mandat utilisé par le FBI pour pirater les ordinateurs de membres d'un site pédopornographique hébergé derrière le réseau Tor, privant les victimes et leurs proches de la possibilité d'un procès.

C'est un coup très dur pour le FBI, mais surtout pour les familles des victimes. Dans un jugement prononcé mercredi, un tribunal américain situé au Massachusetts a invalidé le mandat que la police fédérale avait utilisé pour maintenir un site pédopornographique en ligne et procéder au piratage des ordinateurs de plus d'un millier de ses membres. Le site en question, Playpen, n'était accessible qu'à travers le célèbre réseau d'anonymisation Tor, qui masquait l'adresse IP véritable des visiteurs, rendant très difficile leur identification et leur poursuite.
C'est sur un argument purement juridictionnel que s'est appuyé le magistrat pour dénoncer l'illégalité du mandat employé par le FBI. Selon le code de procédure pénal américain, les magistrats n'ont pas l'autorité suffisante pour émettre des mandats situés en dehors de leur compétence géographique. C'est pourtant ce qu'il s'est produit dans au moins l'un des cas de l'affaire Playpen.
Le site The Intercept, qui se fait l'écho des conclusions de la décision, explique en effet que le mandat a été émis au départ par un juge se trouvant en Virginie. Or, l'un des suspects qui a été attrapé par le FBI dans le cadre de l'enquête vit dans le Massachusetts. Les éléments contre lui – qui est à l'origine de la plainte visant à obtenir l'invalidation du mandat – ne peuvent donc pas être retenus comme preuves, car ils ont été obtenus sans mandat valable.
Le verdict rendu cette semaine risque fort de réduire à néant toute la stratégie du FBI pour faire fermer Playpen et mettre la main sur ses visiteurs américains. La décision est tout à fait susceptible de faire tache d'huile. D'autres accusés pourraient très bien se mettre à attaquer la légalité du mandat sur le même argument juridictionnel, ce qui ferait tomber des preuves à charge contre eux.
Christopher Soghoian, membre de l'American Civil Liberties Union, une association de protection des droits et libertés aux États-Unis, indique que le piratage du site pédopornographique a permis de constituer 1 300 dossiers en attente. À supposer que tous vivent aux USA, combien se trouvent dans des États qui sont en dehors de la compétence géographique de la Virginie ? Sans doute une grande majorité.

UNE FAILLE LÉGISLATIVE BIENTÔT CORRIGÉE ?
Cette règle de la procédure pénale pourrait toutefois disparaître. Le département de la justice américain souhaite lever cette barrière afin que les juges puissent délivrer des mandats pour des recherches à distance sur des ordinateurs qui sont situés en dehors de leur juridiction ou lorsque leur emplacement géographique est inconnu.
Selon The Intercept, le changement législatif a de bonnes chances de passer et le feu vert de la Cour Suprême est très probable – il devrait survenir très bientôt – malgré les protestations des organisations de défense des libertés individuelles et de quelques sociétés, comme Google. Le Congrès aura ensuite six mois pour l'approuver ou la rejeter, sinon la modification entrera en vigueur.

L'AFFAIRE PLAYPEN ET LE PIRATAGE DU FBI
L'affaire Playpen remonte début 2015, quand le FBI parvient à prendre le contrôle des serveurs du site. Au lieu de le fermer tout de suite, la police choisit une autre approche, celle du honeypot : le site reste actif pendant environ deux semaines, sur les serveurs du FBI, afin de savoir qui se connecte sur Playpen. Tactique qui provoquera au passage un déluge de critiques sur le FBI.
C'est au cours de cette période que le FBI a procédé à la contamination des ordinateurs des visiteurs, afin de collecter des informations sur eux, comme leur véritable adresse IP, qui est habituellement masquée avec le réseau d'anonymisation. En effet, la connexion transite par une succession de relais afin de camoufler la géolocalisation du PC. C'est avec ces données que le FBI s'est ensuite adressé aux opérateurs pour obtenir l'identité des internautes – en tout cas ceux aux USA… [Lire la suite]

Réagissez à cet article

Source : *Pédopornographie : quand un piratage par le FBI sur Tor prive les victimes d'une justice*

Microsoft poursuit le gouvernement américain

	Microsoft poursuit le gouvernement américain

Aux États-Unis, Microsoft a initié une procédure à l'encontre du Department of Justice afin de faire invalider certaines dispositions de l'Electronic Communications Privacy Act. En substance, le géant veut pouvoir prévenir ses clients quand les autorités réclament des données les concernant.

Au fil des 18 derniers mois, Microsoft a reçu 5 624 demandes d'information émanant des autorités. Sur ce total, la firme a compté la bagatelle de 2 576 requêtes associées à une obligation de garder le silence. Elle a en outre relevé 1 752 cas dans lesquels cette contrainte était valable jusqu'à nouvel ordre – autant dire ad vitam æternam. Pour Microsoft, cette situation n'est pas acceptable. Sous couvert de l'Electronic Communications Privacy Act, établi en 1986, les autorités ignorent complètement la Constitution. Une procédure légale vient donc d'être engagée.
Concrètement, Microsoft s'attaque au Department of Justice (équivalent de notre ministère de la Justice), à qui il reproche d'ignorer sciemment deux amendements de la Constitution. En empêchant la firme de prévenir un client lorsque ses données sont consultées par une agence du gouvernement, celui-ci ferait à la fois fi de la liberté d'expression de Microsoft (1er amendement de la Constitution) et du droit du client à savoir ce que les autorités font avec sa propriété (4e amendement). En conséquence, plusieurs dispositions de l'Electronic Communications Privacy Act devraient tout simplement être invalidées. Reste à voir si le tribunal de Washington partagera ce point de vue.

Rappelons que ce n'est pas la première initiative de Microsoft pour mettre un terme aux indiscrétions silencieuses de la NSA (entre autres). Cela fait deux ans, maintenant, que la firme réclame ouvertement une très sérieuse remise en question des pratiques du gouvernement et des différents corps policiers qui en dépendent. L'appel, cependant, n'a toujours pas porté le moindre fruit. Il est donc temps, à l'évidence, d'actionner d'autres leviers pour espérer aboutir à un résultat… [Lire la suite]

Réagissez à cet article

Source : *Données personnelles : Microsoft poursuit le gouvernement américain*

CNIL, un nombre record de plaintes en 2015

CNIL, un nombre record de plaintes en 2015

L'année 2015 est marquée par une forte augmentation de l'activité de la CNIL, avec 13 790 demandes provenant de particuliers : 7908 plaintes dont 36% concernent l'e-réputation et 5 890 demandes de droit d'accès indirect. Cette évolution témoigne de la volonté des citoyens de reprendre leurs droits en main au bénéfice de plus de transparence et de sécurité, notamment dans la gestion de leur e-réputation.

Protéger sa vie privée en ligne : de la préoccupation à la responsabilisation

En 2015, la CNIL a enregistré 7 908 plaintes, soit 2000 de plus qu'en 2014 (36 % de hausse).

Cette augmentation importante s'explique par la prise de conscience croissante des citoyens, notamment pour la gestion de leur réputation en ligne. Cela se traduit par la pratique régulière de l'ego-surfing, qui est souvent à l'origine de demandes de retraits de contenus ou de déréférencement. En cas de refus de l'éditeur du site ou du moteur de recherche, la CNIL peut être saisie d'une plainte. A titre indicatif, la CNIL a ainsi reçu près de 700 plaintes depuis l'été 2014 et la consécration par la Cour de justice de l'Union européenne d'un droit au déréférencement. Enfin, la médiatisation d'affaires touchant à la sécurité des données tend aussi à sensibiliser les citoyens à cette problématique croissante.

L'opposition à figurer dans un fichier, tous secteurs confondus, constitue le principal motif de plaintes, ainsi que l'exercice du droit d'accès.

Afin de faciliter les démarches des personnes qui la saisissent et de fiabiliser leurs demandes, la CNIL a amélioré en avril 2015 son service de plaintes en ligne en déployant une cinquantaine de scénarios correspondant aux plaintes les plus fréquentes.

C'est nouveau ! A suivre …

Les plaintes reçues permettent à la CNIL d'identifier de nouvelles tendances telles que : la géolocalisation des salariés non plus via leur véhicule mais via des bracelets connectés ou leur smartphone, de nouvelles techniques de vidéosurveillance des salariés via une application sur smartphones ou une webcam.

Des municipalités invitent leurs administrés à leur envoyer des photos ou du son pour signaler des incivilités (déjections canines, stationnement abusif, tapage nocturne, dépôt d'ordure, affichage sauvage, etc).

Des demandes de droit d'accès indirect toujours en hausse

En 2015, la CNIL a reçu 5890 demandes de droit d'accès indirect, soit une augmentation de 12% par rapport à 2014. Ces demandes reçues représentent un total de 8377 vérifications à mener concernant par ordre d'importance : le fichier FICOBA de l'administration fiscale, le fichier TAJ des antécédents judiciaires de la police et de la gendarmerie et les fichiers de renseignement.

Les effets des attentats et de l'état d'urgence sur les demandes de droit d'accès indirect

La CNIL a reçu ces derniers mois près de 155 demandes de droit d'accès indirect liées au contexte de l'état d'urgence (perquisitions administratives, assignations à résidence, retrait de badges aéroportuaires ou de cartes professionnelles). Ces demandes portent notamment sur le Traitement d'Antécédents Judiciaires (TAJ) et les fichiers des services de renseignement du ministère de l'intérieur.

Le renforcement des effectifs au sein des forces de sécurité depuis les attentats du 13 novembre 2015 (création annoncée de 8500 postes dans la police, la gendarmerie, la douane et l'administration pénitentiaire) et l'accroissement du nombre de candidats à ces fonctions contribuent également à accroître le nombre demandes de droit d'accès indirect au fichier TAJ, consulté dans le cadre des enquêtes administratives menées pour l'accès à ce type d'emplois.

Au premier trimestre 2016, la CNIL a déjà constaté une augmentation de 18 % des demandes d'accès au fichier TAJ par rapport au premier trimestre 2015.

Une action répressive en hausse, notamment grâce aux contrôles en ligne

La logique de la loi et son application par la CNIL visent avant tout la mise en conformité des organismes mis en cause. A chaque phase d'instruction d'une plainte et/ou d'un contrôle, ceux-ci ont la possibilité de suivre les mesures recommandées par la CNIL pour se mettre en conformité. **Dans l'immense majorité des cas, la simple intervention de la CNIL se traduit par une mise en conformité de l'organisme**. Le prononcé de sanctions par la CNIL permet de sanctionner des organismes qui persistent dans des comportements répréhensibles, et constitue donc un instrument de dissuasion important.

L'année 2015 se caractérise par une forte augmentation du nombre de mises en demeure adoptées par la Présidente de la CNIL. **En effet, 93 mises en demeure** ont été adoptées contre 62 en 2014.

Cette hausse s'explique par la possibilité de réaliser des contrôles en ligne et par le fait que des contrôles s'inscrivaient dans des thématiques ayant révélé de nombreux manquements :

- cookies (40 mise en demeure),
- sites de rencontre (8 mise en demeure),
- services dématérialisés d'actes d'état civil (20 mise en demeure).

10 sanctions ont été prononcées par la formation restreinte, dont 3 sanctions pécuniaires.

La CNIL a réalisé **501 contrôles** en 2015, dont **87 contrôles portant sur des dispositifs vidéo**.

155 contrôles en ligne ont été réalisés sur de nombreuses thématiques telles que :

- les sites de tirage de photos ou de créations d'albums photo,
- de conseil de santé en ligne,
- de crédit en ligne,
- d'adhésion à des partis politiques,
- de demande d'actes d'état civil,

28 contrôles en ligne réalisés en 2015 ont conduit à une mise en demeure en 2015, 2 procédures de sanction ont été engagées et toujours en cours.

Les données personnelles, au cœur de l'actualité législative en France et en Europe

En 2015, l'actualité législative s'est fortement structurée autour de la protection des données personnelles et des libertés numériques, comme en témoignent les 122 avis que la CNIL a rendus.

Le renseignement et la lutte contre le terrorisme

La CNIL s'est prononcée sur **14 projets de dispositions législatives ou réglementaires directement relatives au traitement de données à des fins de renseignement ou de lutte contre le terrorisme**. Des dispositifs d'une nouvelle ampleur, en termes de volume de données traitées comme de modalités de collecte, ont été légalisés. De nouveaux fichiers ont été créés, certains fichiers existants ont été modifiés, de nouvelles techniques d'enquête et de recueil de données ont été utilisées pour surveiller et contrôler des communications.

Une personnalité qualifiée au sein de la CNIL est chargée depuis février 2015 de contrôler le blocage administratif des sites provoquant des actes de terrorisme ou en faisant l'apologie ainsi que les sites à caractère pédopornographique. Ce contrôle vise à s'assurer que le blocage n'est pas disproportionné afin d'éviter tout « sur blocage ». Alexandre Linden, la personnalité qualifiée désignée par les membres de la CNIL, présentera un rapport dédié à cette activité.

Dans le cadre du projet de loi relatif au renseignement, la CNIL a rendu un avis le 5 mars 2015, dans lequel elle a été très attentive aux modalités de contrôle des fichiers de renseignement. Ces fichiers bénéficient actuellement d'un cadre législatif spécifique interdisant le contrôle de leur régularité du point de vue de la loi Informatique et Libertés. Or, un tel contrôle général constitue une exigence fondamentale afin d'asseoir la légitimité démocratique de ces fichiers dans le respect des droits et libertés des citoyens.

La CNIL a proposé que le projet de loi lui permette d'exercer un tel contrôle, selon des modalités particulières, adaptées aux activités des services de renseignement, et en coopération avec la CNCTR (Commission Nationale de Contrôle des Techniques de Renseignement). Cette proposition n'a pas été suivie d'effet.

Le projet de loi pour une République numérique conforte et renforce l'action de la CNIL

La CNIL s'est prononcée, lors de la séance plénière du 19 novembre 2015, sur l'avant projet de loi pour une « République numérique », dans sa version alors envisagée par le Gouvernement. Le projet de texte adopté en première lecture à l'Assemblée nationale comporte de nombreuses modifications, qui tiennent notamment compte de l'avis de la CNIL. La CNIL a insisté dans son avis sur la nécessaire cohérence avec les autres textes en préparation et particulièrement le règlement européen qui sera d'application directe en 2018.

Le projet de loi tend également à renforcer les pouvoirs de la CNIL et à conforter ainsi son engagement dans la régulation du numérique et son activité d'accompagnement des particuliers, des entreprises et des administrations.

La loi du 26 janvier 2016 sur la modernisation de notre système de santé

La CNIL a été sollicitée sur le projet de loi et a participé à de nombreuses auditions.

En Europe

Au plan international, la finalisation du projet de règlement européen sur les données personnelles qui a fait l'objet d'un accord à l'issue du trilogue en décembre 2015 et l'arrêt de la CJUE d'octobre 2015 invalidant le Safe Harbor ont très fortement mobilisé la CNIL. La Présidente de la CNIL a été réélue à la présidence du G29 (groupe des CNIL européennes) en février 2016, pour un mandat de deux ans.

Réagissez à cet article

Source : *Download the Latest Version – FreeFileSync*

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*

L’évolution De La Carte SIM

	L’évolution De La Carte SIM

Une carte SIM, ou Suscriber Identity Module en anglais (module d'identification de l'abonné), est un élément familier d'un téléphone portable. Elle peut facilement être échangée ou remplacée, mais elle n'est néanmoins pas née en même temps que le téléphone portable. Les premiers téléphones portables ne permettaient que des normes de communication « intégrées » : les paramètres de souscription étaient codés en dur dans la mémoire du terminal mobile.

Les normes analogues les plus anciennes comme NMT-450 n'utilisaient aucune sécurité : les données d'abonnement pouvaient être copiées sur un autre appareil et clonées, ce qui permettait d'appeler et d'accepter des appels au nom du propriétaire légitime sans payer.

Le premier dispositif de sécurité, inventé un peu plus tard, fut le code SIS, Suscriber Identity Security en anglais (sécurité de l'identité de l'abonné) : il s'agissait d'un nombre à 18 chiffres unique à chaque appareil et codé en dur dans un processeur d'application. Les codes SIS étaient répartis entre les fournisseurs de manière à ce que deux appareils ne puissent pas partager le même code SIS. Le processeur comportait également un code RID de 7 chiffres qui était transmis à une station de base lorsqu'un abonné s'inscrivait dans un réseau mobile.

La station de base générait un nombre aléatoire que le processeur SIS utilisait couplé avec une réponse SIS unique pour produire la clé d'autorisation.

Les clés et les nombres étaient relativement courts, mais appropriés pour l'année 1994 ; de façon assez prévisible, le système a été décrypté plus tard, tout juste trois ans avant l'apparition de la norme GSM, Global System for Mobile en anglais (Communications – Système global pour les communications mobiles). Il était conçu de manière plus sûre étant donné qu'il utilisait un système d'autorisation similaire, mais au chiffrement plus résistant. Ainsi, la norme est devenue « détachée » .

Cela signifie que l'autorisation dans sa totalité avait lieu sur un processeur externe intégré dans une carte intelligente. La solution a été appelée SIM. Avec l'introduction des cartes SIM, l'abonnement ne dépendait plus l'appareil et l'utilisateur pouvait changer d'appareil aussi fréquemment qu'il le désirait tout en gardant son identité mobile.

Fondamentalement, une carte SIM est une carte intelligente selon la norme ISO 7816, qui ne présente pas de différence significative par rapport à d'autres cartes intelligentes de contact comme les cartes de crédit ou les cartes téléphoniques. Les premières cartes SIM faisaient même la taille d'une carte de crédit, mais la tendance globale de réduction des dimensions a mené à une nouvelle forme plus compacte.

Les cartes SIM traditionnelles 1FF (1st Form Factor) de taille complète ne rentraient plus dans les téléphones, et l'industrie a donc trouvé une solution de compatibilité simple : une carte SIM plus petite (mini-SIM, 2FF ou 2nd Form Factor) qui est commune pour les utilisateurs modernes, a été placée dans un support en plastique de taille 1FF afin que la nouvelle forme de carte comporte la puce et les contacts, mais avec une empreinte plus petite, et puisse facilement être sortie.

Bien que cette tendance à la réduction continue avec la micro-SIM (3FF) puis la nano-SIM (4FF) , la forme et les contacts ainsi que les fonctionnalités de ces puces intégrées n'ont pas changé depuis presque 25 ans. De nos jours, de grands supports en plastique sont produits pour répondre aux besoins des utilisateurs qui préfèrent encore des combinés à l'ancienne.

Ceci dit, de nombreux appareils obsolètes ne supporteraient pas les cartes SIM actuelles, même dans leur version complète. Cela vient du fait que la tension de fonctionnement était de 5 V dans les anciennes cartes SIM alors que les actuelles exigent 3 V. De nombreux fabricants de SIM préfèrent sacrifier la compatibilité pour réduire les coûts, et la majorité des cartes SIM modernes ne supporteraient donc pas deux tensions. C'est pour cela que dans un ancien téléphone uniquement compatible avec 5 V, les cartes SIM de seulement 3V ne fonctionneraient même pas à cause de la protection de la tension de leur processeur.

Lors de la production, certaines informations sont écrites dans la mémoire d'une carte SIM : l'IMSI (International Mobile Suscriber Identity, Identité de l'abonné mobile international), en accord avec le porteur ayant commandé la carté, ainsi qu'une clé de 128 bits nommée Ki (Key Identification, identification de clé). Pour résumer simplement, on peut dire que l'IMSI et le Ki sont le l'identifiant et le mot de passe respectifs de l'abonné codés en dur dans la puce de la carte SIM.

La correspondance entre l'IMSI d'un abonné et son numéro de téléphone est stockée dans une base de données spéciale appelée HLR (Home Location Register). Ces données sont copiées sur une autre base de données, VLR (Visitor Location Register) dans chaque segment du réseau, sur la base de l'enregistrement temporaire de l'abonné en tant qu' « invité » sur une autre station de base.

Le processus d'autorisation est relativement simple. Lorsqu'un abonné est inscrit dans la base de données temporaire, VLR envoie un numéro de 128 bits aléatoire (RAND) au numéro de téléphone. Le processeur de la carte SIM utilise l'algorithme A3 pour créer une réponse de 32 bits (SRES) au VLR basé sur le numéro RAND et le Ki. Si VLR obtient une réponse qui correspond, l'abonné est inscrit dans le réseau.

La SIM crée également une autre clé temporaire appelée Kc. Sa valeur est calculée sur la base du RAND et du Ki mentionnés ci-dessus, à l'aide de l'algorithme A8. Cette clé est ensuite utilisée à son tour pour chiffrer des données transmises par l'algorithme A5.

Les noms de tous ces acronymes peuvent paraître un peu compliqués, mais l'idée de base est très simple : vous avez tout d'abord un identifiant et un mot de passe codés en dur dans la SIM, puis vous créez des clés de vérification et de chiffrement avec quelques trucs mathématiques et ça y est : vous êtes connecté !

Ce chiffrement est toujours activé par défaut, mais dans certaines circonstances (par exemple si un mandat est fourni), il peut être désactivé, ce qui permet qu'une agence de renseignement puisse intercepter les conversations par téléphone. Dans ce cas, les anciens dispositifs affichaient un cadenas ouvert, alors que les téléphones modernes (à part Blackberry) n'affichent aucune indication de ce type.

Il existe une attaque spécifiquement conçue pour intercepter les conversations téléphoniques ; pour la réaliser, l'adversaire a seulement besoin d'un appareil appelé IMSI Catcher qui imite une station de base et enregistre les téléphones qui se connectent avant d'envoyer tous les signaux vers une station de base réelle.

Dans ce cas, tout le processus d'autorisation se déroule de façon normale (il n'est pas nécessaire de décrypter les clés de chiffrement), mais la fausse station de base ordonne au dispositif de les transmettre sous forme de texte brut afin qu'un adversaire puisse intercepter les signaux sans que la compagnie ou l'abonné ne le sachent.

Cela peut paraître étrange, mais cette vulnérabilité n'en est pas vraiment une : en fait, cette fonctionnalité a été conçue pour faire partie du système depuis le début, afin que les services de renseignements puissent réaliser des attaques intermédiaires dans les cas appropriés… [Lire la suite]

Réagissez à cet article

Source : *L'évolution De La Carte SIM – Kaspersky Daily – | Nous Utilisons Les Mots Pour Sauver Le Monde | Le Blog Officiel De Kaspersky Lab En Français.*