

Déchiffrement des communication numériques (Telegram et autres). Où en est-on ?



Déchiffrement
des
communication
numériques
(Telegram et
autres). Où
en est-on ?

Ce mardi 23 Août, Bernard Cazeneuve se réunissait avec son homologue allemand pour discuter d'une initiative européenne contre le chiffrement des données, afin de lutter contre le terrorisme. Une initiative qui ne fait pas l'unanimité.

Une initiative européenne contre les chiffrements trop forts ?

Face au terrorisme international et sachant que les messageries instantanées visées par le projet de loi sont majoritairement américaines, Bernard Cazeneuve s'en remet à une initiative européenne. L'idée serait d'étendre aux services de messageries et d'appels sur internet, les mêmes règles de sécurité et de confidentialité destinées jusque-là, aux opérateurs télécom. Le ministre a ainsi fermement déclaré vouloir obliger les services en ligne «*non coopératifs*» à «*retirer des contenus illicites ou déchiffrer des messages dans le cadre d'enquêtes judiciaires, que leur siège soit en Europe ou non*».

Conscient de la polémique qui entoure ce projet de loi, le ministre a précisé que l'utilisation des données déchiffrées ne servirait que dans le cadre «*judiciaire*». Ce qui voudrait dire qu'elles ne seraient pas utilisées par les services secrets, comme le redoutent beaucoup de personnes. Se voulant rassurant, il a insisté «*Il n'a bien sûr, jamais été question de remettre en cause le principe du chiffrement des échanges*». Le 16 septembre prochain, le projet de loi contre le chiffrement des données sera discuté lors du sommet des chefs d'états européens.

...[lire la suite]

Denis Jacopini anime des **conférences et des formations** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur : <https://www.lenetexpert.fr/formations-en-cybercriminalite-et-en-protection-des-donnees-personnelles>



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.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Une initiative franco-allemande contre le chiffrement numérique

Révélation sur de petits piratages informatiques entre alliés...



Révélation
sur de petits
piratages
informatiques
entre alliés...

C'est une révélation assez rare pour être soulignée, mais elle était passée inaperçue. Bernard Barbier, l'ancien directeur technique de la DGSE, le service de renseignement extérieur français, s'est livré en juin dernier à une longue confession devant les élèves de l'école d'ingénieurs Centrale-Supélec (voir vidéo ci-dessous), comme l'explique Le Monde.

Cet ex-cadre de l'espionnage a notamment confirmé que les Etats-Unis étaient bien responsables de l'attaque informatique de l'Elysée en 2012.

Entre les deux tours de la présidentielle de 2012, des ordinateurs de collaborateurs de Nicolas Sarkozy avaient été infectés à l'Elysée. Jusqu'à présent, les soupçons se portaient bien vers la NSA mais ils n'avaient jamais été confirmés. « Le responsable de la sécurité informatique de l'Elysée était un ancien de ma direction à la DGSE. Il nous a demandé de l'aide. On a vu qu'il y avait un malware », a expliqué Bernard Barbier en juin dernier. « En 2012, nous avions davantage de moyens et de puissance techniques pour travailler sur les métadonnées. J'en suis venu à la conclusion que cela ne pouvait être que les Etats-Unis. »

La France aussi impliquée dans un pirate informatique

Ce cadre de la DGSE a ensuite été envoyé par François Hollande pour s'entretenir avec ses homologues américains. « Ce fut vraiment un grand moment de ma carrière professionnelle », explique-t-il. « On était sûrs que c'était eux. A la fin de la réunion, Keith Alexander (l'ex-directeur de la NSA), n'était pas content. Alors que nous étions dans le bus, il me dit qu'il est déçu, car il pensait que jamais on ne les détecterait. Et il ajoute : 'Vous êtes quand même bons.' Les grands alliés, on ne les espionnait pas. Le fait que les Américains cassent cette règle, ça a été un choc. » Pourtant, au cours de cette conférence, Bernard Barbier a aussi révélé l'implication de la France dans une vaste opération d'espionnage informatique commencée en 2009 qui avait touché notamment l'Espagne, la Grèce ou l'Algérie. Le Canada, lui aussi visé, avait à l'époque soupçonné Paris, mais rien n'avait été confirmé en France. « Les Canadiens ont fait du reverse sur un malware qu'ils avaient détecté. Ils ont retrouvé le programmeur qui avait surnommé son malware Babar et avait signé Titi. Ils en ont conclu qu'il était français. Et effectivement, c'était un Français. »

Article original de Thomas Liabot



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.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Les Etats-Unis étaient bien à l'origine du piratage informatique de l'Elysée en 2012 – leJDD.fr

Le malware Pegasus exploite 3 failles 0 day sur iPhone



Les trois failles corrigées par Apple dans iOS 9.3.5 (ainsi que dans la dernière bêta d'iOS 10 livrée, contre toute attente, vendredi dernier) sont redoutables. Elles ont été exploitées par NSO Group, une société israélienne dont le fonds de commerce n'est autre que l'espionnage de journalistes et de militants. Le site Motherboard raconte la découverte de l'affaire qui relève du thriller.

Ce 10 août, Ahmed Mansoor, un militant des droits de l'homme dans les Émirats Arabes Unis, reçoit sur son iPhone un message lui proposant d'en savoir plus sur de «nouveaux secrets sur la torture dans les prisons d'État ». Un lien accompagnait ce message, qu'il s'est bien gardé de lancer.



Les deux messages reçus par Mansoor – Cliquer pour agrandir

À la place, il a contacté un chercheur du Citizen Lab, un organisme de défense des droits numériques rattaché à l'université de Toronto. Aidé par Lookout, un spécialiste de la sécurité mobile, ils ont pu mettre au jour un mécanisme très élaboré de surveillance par iPhone interposé.

Si Mansoor avait touché le lien, il aurait provoqué le jailbreak de son iPhone et donné à NSO Group le plein contrôle de son smartphone. « Un des logiciels de cyberspionnage parmi les plus sophistiqués que nous ayons jamais vus », expliquent les chercheurs.

NSO Group vient d'apparaître sur les radars, mais cette entreprise très discrète (aucune présence sur internet) opère depuis 2010. Le malware qu'elle a mis au point, baptisé Pegasus, permet d'infecter un iPhone, d'intercepter et de voler les données et les communications. Une arme redoutable, qualifiée de « fantôme » par NSO pendant une de ses rares interventions publiques en 2013. Cette société vend Pegasus au plus offrant, notamment des gouvernements peu regardants sur les droits de l'homme.



Les données volées par Pegasus – Cliquer pour agrandir

NSO a visiblement pu pénétrer par effraction dans des iPhone depuis le modèle 5. Son malware est programmé avec des réglages qui remontent jusqu'à iOS 7.

Ces trois failles zero day, baptisées Trident par les chercheurs, ont été communiquées à Apple il y a dix jours. « Nous avons été mis au courant de cette vulnérabilité et nous l'avons immédiatement corrigée avec iOS 9.3.5 », explique un porte-parole du constructeur. « iOS reste toutefois le système d'exploitation mobile grand public le plus sécurisé disponible », rassure Dan Guido, patron de la société de sécurité informatique Trail Of Bits, qui travaille souvent avec la Pomme. Il indique toutefois qu'il reste à améliorer le système de détection des vulnérabilités. Apple a annoncé début août un programme de chasse (rémunérée) aux failles.

Article original de Michaël Bazoge



Denis JACQUET est Expert Informatique spécialisé en cybersécurité et en protection des données personnelles.

- Expertises techniques (virus, logiciels, piratages, réseaux, systèmes d'information, etc.) et juridiques (cybersécurité, logiciels, droits de l'homme, contrefaçon, diffamation de données, etc.)

- Expertises de systèmes de vote électronique

- Formations et conférences en cybersécurité

- Formations de C.S.I. (Compétences Informatiques et Logicielles)

- Accompagnement à la mise en conformité OGD de votre établissement



Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Cyberspionnage : derrière les failles Trident d'iOS, le redoutable malware Pegasus | iGeneration

Pourquoi le Conseil d'État autorise une exploitation de données saisies via l'état d'urgence ?



Pourquoi le
Conseil
d'Etat
autorise une
exploitation
de données
saisies via
l'état
d'urgence ?

Alors que le tribunal en première instance avait jugé que les éléments n'étaient pas réunis pour justifier une telle procédure extra-judiciaire, le Conseil d'État a autorisé la police à exploiter des données informatiques saisies à Roubaix chez un suspect ayant fait l'objet d'une perquisition administrative.

À la suite de l'attentat de Nice, le gouvernement a réintégré en juillet dernier dans le dispositif de l'état d'urgence la possibilité pour la police de procéder à la saisie de matériels ou données informatiques présentes ou accessibles sur les lieux d'une perquisition administrative. Mais conformément aux préconisations du Conseil constitutionnel, il l'a fait en assortissant cette entorse à la vie privée et au droit de propriété d'un certain nombre de garanties minimales.

En particulier, il est désormais précisé que de tels matériels et données ne peuvent être saisis que « si la perquisition révèle l'existence d'éléments, notamment informatiques, relatifs à la menace » que représenterait la personne visée. Par ailleurs, les policiers ne peuvent rien faire des données saisies sans l'autorisation d'un juge des référés d'un tribunal administratif, qui a 48 heures pour donner son aval.



Or Nextinpact rapporte que le ministère de l'intérieur a dû faire appel d'une décision défavorable du tribunal administratif de Roubaix, pour avoir le droit d'exploiter les données saisies chez un suspect. Sur place, la perquisition et la fouille des données informatiques accessibles n'avaient apporté strictement aucun élément matériel permettant d'étayer une éventuelle infraction pénale du justiciable. Le juge de première instance en avait donc déduit qu'il ne pouvait pas autoriser l'exploitation des données injustement saisies.

Ce faisant, le juge restait dans l'esprit de l'avis du Conseil constitutionnel, qui s'opposait aux saisies et exploitations de données « alors même qu'aucune infraction n'est constatée ».

L'INTÉRESSÉ A INDIQUÉ COMMUNIQUER AVEC EUX AU MOYEN DE SON TÉLÉPHONE PORTABLE, EN USANT NOTAMMENT DE MESSAGERIES INSTANTANÉES OU CRYPTÉES

Mais le Conseil d'État, lui, en reste à une lecture plus littérale de ce que le gouvernement a écrit dans la nouvelle loi, qui n'a pas été soumise au Conseil constitutionnel. Celle-ci ne demande pas qu'une infraction soit constatée, mais uniquement que la perquisition « révèle l'existence d'éléments », matériels ou non, relatifs à la menace. C'est beaucoup plus vague.

Or la haute juridiction administrative note dans **son ordonnance (.pdf)** que « l'intéressé a déclaré au cours de la perquisition être resté en contact avec quatre amis de Roubaix, qu'il a nommé désignés, partis en Syrie et en Irak pour y mener le djihad », et qu'il « a indiqué communiquer avec eux au moyen de son téléphone portable, en usant notamment de messageries instantanées ou cryptées ». Ces déclarations sont donc en elles-mêmes des éléments relatifs à la menace que pourrait représenter l'individu, qui justifient d'autoriser l'exploitation des données saisies.

UNE OBLIGATION DE RESTITUTION SOUS 15 JOURS

Cette affaire fera certainement redire aux avocats qu'il est toujours primordial de garder le silence, mais il faut noter que le suspect semble pleinement coopératif, et qu'il a accepté que ses données soient inspectées. Il a peut-être préféré que son innocence soit ainsi vérifiée, plutôt que sa présomption d'innocence reste, dans l'esprit des services de renseignement, une présomption de culpabilité.

Selon le PV de perquisition, la police avait procédé à la saisie d' « un ordinateur de marque ACER et de son chargeur, d'un téléphone portable de marque Apple et de son chargeur, d'une clef USB rouge de marque Emtec d'une capacité de 16 Gb, d'une clé USB noire de marque Verbatim d'une capacité de 16 Gb, d'une carte SD de marque Viking d'une capacité de 512 Mb et d'une carte SD de marque Sandisk d'une capacité de 8 Gb ».

Selon les termes de la loi, l'ensemble de ces matériels doivent être retournés à leur propriétaire dans les 15 jours suivant l'autorisation (délivrée ici par ordonnance du 23 août), sans prorogation motivée ou découverte d'éléments probants. Les données non pertinentes devront être détruites sous un délai de 3 mois.

Article original de Guillaume Champeau



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.

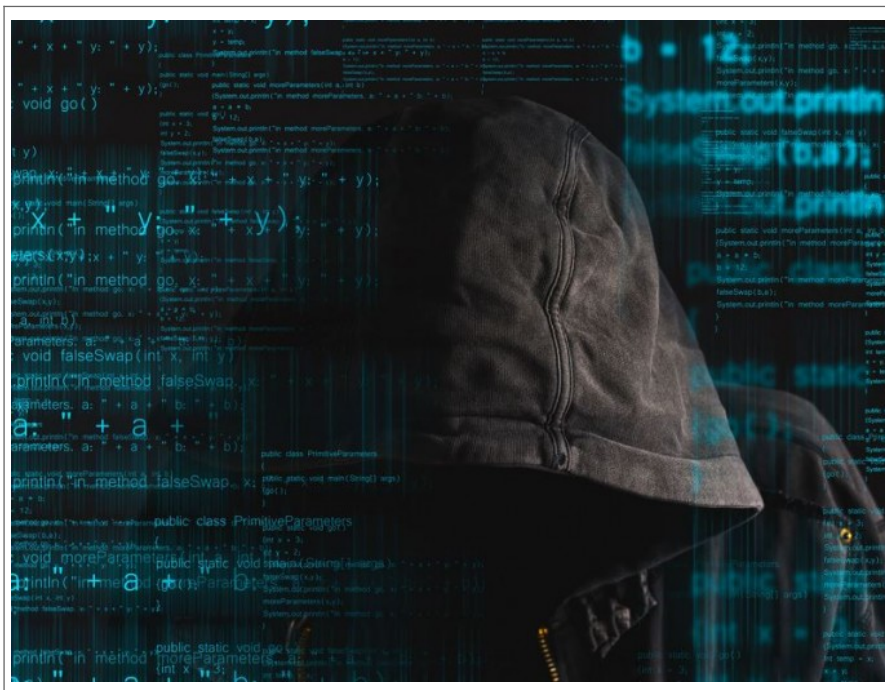


[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Pourquoi le Conseil d'État autorise une exploitation de données saisies via l'état d'urgence – Politique – Numerama

Shadow Brokers, une affaire de Cyberespionnage



Shadow Brokers,
une affaire de
Cyberespionnage

1) Pourquoi un tel intérêt pour les Shadow Brokers ?

2) Le hacking de la NSA est-il établi ?

3) Que dit cette affaire du groupe Equation ?

4) Que renferme l'archive des Shadow Brokers ?

Al-Bassam ou la synthèse réalisée par Softpedia). On y trouve des exploits, autrement dit des codes d'exploitation permettant de prendre le contrôle ou d'espionner des pare-feu ou passerelles VPN fournis par de grands constructeurs comme Cisco, Juniper ou Fortinet. Des constructeurs qui ont déjà reconnu que les outils mis en ligne menaçaient bien certains de leurs matériels. Mais, dans tous les cas, il s'agit de générations anciennes de machines. Les appliances Cisco Pix, ciblées par plusieurs outils, ne sont par exemple plus supportées par le constructeur depuis 2009. [lire la suite]

Et il y a aussi les outils dont la vocation ne s'arrête pas à cibler une gamme de machines en particulier. *The Intercept* explique ainsi que des éléments d'une architecture exploitée par la NSA pour mettre en place des attaques de type Man-in-the-Middle, autorisent l'interception de requêtes Web, figurent dans l'archive des Shadow Brokers. Sans risque de se tromper, la réponse est non. « Comme il y a 300 Mo de code, de documentations, de binaires, personne n'a publié d'analyse complète », remarquent Hervé Schauer et Christophe Renard. [lire la suite]

« Voir de tels outils mis à la disposition de cybercriminels est évidemment inquiétant. « On est ici face à des outils d'attaque de haut niveau, mis librement à disposition sur le Web, explique Jérôme Billots. Les entreprises doivent donc être très attentives, effectuer l'inventaire des matériels exposés sur leur parc et apporter les modifications nécessaires pour protéger leurs infrastructures. Heureusement, les exploits mis au jour sont assez anciens et ciblent donc du matériel âgé. Mais certaines machines peuvent toujours être en exploitation. » Au fur et à mesure que les codes de l'archive des Shadow Brokers seront décryptés, des correctifs et des indicateurs de compromission vont être publiés. Ce qui permettra aux RSSI de contrer la menace. C'est donc plutôt une course de fond qui s'engage. [lire la suite]

La liste des suspects s'est très vite limitée quelques noms. Très rapidement, Nicolas Weaver, de l'université de Berkeley, pointe la Chine, soupçonnée de nombreux actes de cyber-espionnage contre les intérêts américains, et la Russie. Une seconde hypothèse que défend lui aussi Edward Snowden, précisément réfugié en Russie après avoir été à l'origine de la plus importante fuite de données de la NSA. [lire la suite]

9) Quelles sont les conséquences possibles ?

10) Qu'en pense Bernard Cazeneuve ?



Article original de Reynald Fléchaux



- 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.



Contactez-nous

Réagissez à cet article

Votre vie privée numérique en danger sur Leakedsource

<p>Pour [redacted] @damienbancal.fr>★</p> <p>Yeah - I can definitely confirm my Paypal was hacked a while back. I felt it was weird that they didn't bother to try to steal money or change my password - but I guess they were just harvesting as much information as they could get.</p> <p>This is all good to know though - I didn't know my amazon was hacked.</p> <p>Thank you very much for the alert - it's very much appreciated</p>	<p>Votre vie privée numérique en danger sur Leakedsource</p>
--	--

Depuis quelques semaines, le site leakedsource engrange des centaines de millions de données volées par des pirates informatiques. Un business juteux qui met en danger des millions d'internautes.

LeakedSource, nouvelle source d'informations pour pirates informatiques ? Souvenez-vous, on vous parlait en juillet, de données volées appartenant à un ancien garde du corps de Vladimir Poutine, le Président Russe, ou encore de Nicolas Sarkozy, ancien Président de la République Française. Son identité, ses données privées, des courriels... Un piratage qui semblait être particulièrement compliqué à orchestrer tant les sources d'informations concernant ce body guard étaient variés. Après enquête, j'ai découvert que si le résultat pouvait être particulièrement préjudiciable pour la cible, la mise en place et l'exécution de cette attaque était aussi simple que « 1 + 1 font 2 ».

Leakedsource, source quasi inépuisable de malveillances

Pour ce garde du corps, mais aussi pour de nombreuses personnalités, le risque est énorme. Tout débute par le piratage de centaines de bases de données de part le monde. Myspace, Adobe, LinkedIn, Twitch, Xat, Badoo... ne sont que des exemples parmi d'autres. Je gère, avec le protocole d'alerte ZATAZ, des dizaines de fuites de données par mois concernant des PME et entreprises Françaises. Imaginez donc ce que brassent des sites comme leaked source.

Leakedsource.com, un espace web tenu par des Russes, a pour mission de regrouper les informations volées par des pirates et de permettre de consulter les informations en question. Les administrateurs du portail expliquent que leur service est fait pour s'assurer que les données volées ne vous concernent pas. Sauf que, des données, il y en a des centaines de millions, et vous pourriez bien vous y retrouver, comme Mark Zuckerberg, cofondateur et directeur général de Facebook, piraté en juin 2016 parce que son mot de passe « DaDaDa » était accessible dans une base de données piratées et stockées chez Leakedsource.

Vous ne risquez rien ? Vraiment ?

Cela n'arrive qu'aux autres ? Allez donc regarder du côté de vos données. C'est d'ailleurs ce qu'aurait dû faire l'auteur des jeux vidéo Garrysmod et de Rust, Garry Newman. J'ai pu avoir une longue conversation avec l'auteur de divertissements vidéo ludique qui ne s'attendaient pas à découvrir sa vie numérique mise en pâture de la sorte. Il faut dire aussi que plusieurs pirates ont contacté la rédaction de ZATAZ.COM pour se vanter d'avoir mis la main sur ses données Paypal, Amazon, Gmail de ce créateur de jeux vidéo britannique. Bref, pour 4 dollars (le prix journalier d'un abonnement Leaked source pour accéder aux données) n'importe quel internaute peut se transformer en vulgaire violeur de vie 2.0. Il suffit de rentrer un mail, un pseudonyme ou encore une adresse IP et Leakedsource cherche dans ses bases de données la moindre concordance. Cerise sur le gâteau, quand le mot de passe est hashé, donc illisible à la première lecture, Leaked source propose la version du précieux sésame déchiffré. « **Si les personnes [les pirates, NDR] sont malines, elles peuvent faire beaucoup de dégâts avec ce genre d'outil accessible à Monsieur tout le monde** » me confirme un utilisateur.

Que faire pour éviter ce type de fuite de données ?

Je vais très rapidement être honnête avec vous, si vous mettez vos données en ligne, dites vous qu'elles ne sont plus en sécurité. Et ce n'est pas notre vénérable CNIL qui pourra vous aider. Avec plusieurs centaines de cas de fuite de données que je traite avec le protocole d'alerte de zataz par an, j'ai déjà pu croiser mes propres informations. Je vous parlais plus haut de Leakedsource, j'ai pu y retrouver mon compte Adobe. Pourtant, le géant du logiciel l'avait juré, il était « secure » [sécurisé, ndr].

Tellement « secure » qu'un de mes mails, et le mot de passe attendant, sont disponibles dans ce big data du malveillant. Autant dire que l'adresse mail et le mot de passe en question ont été détruits et ne seront plus utilisés.

Que faire donc ? D'abord, un compte mail par service. Je sais, c'est long est fastidieux. Mais je pense qu'il va être beaucoup plus long et fastidieux pour Garry Newman de revalider l'ensemble de ses comptes « infiltrés », car il utilisait la même adresse électronique pour ses accès Paypal, Amazon...

Ensuite, ne mettez pas le même mot de passe pour l'ensemble de vos services en ligne. On a beau le répéter, cesser de vous croire plus malin que les 010101 qui nous régissent. Mark Zuckerberg et son « DaDaDa » lui ont coûté son Twitter et son Pinterest. Pour Garry, plus grave encore, son compte Amazon et Paypal, avec des données sensibles [adresses postales, données bancaires...] qui ne devraient pas être disponibles à la planète web. Donc, oui, c'est fastidieux, mais un mot de passe par compte est une obligation.

Pour finir, en ce qui concerne l'IP, n'hésitez plus à utiliser un VPN. L'outil permet de cacher votre véritable adresse de connexion, en plus de chiffrer vos informations transitant sur la toile. Je vous invite à regarder du côté de nos partenaires et amis de chez **NoLimitVPN** ou encore HMA! pour blinder vos connexions PC, Mac et mobiles.

Article original de Damien Bancal



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.

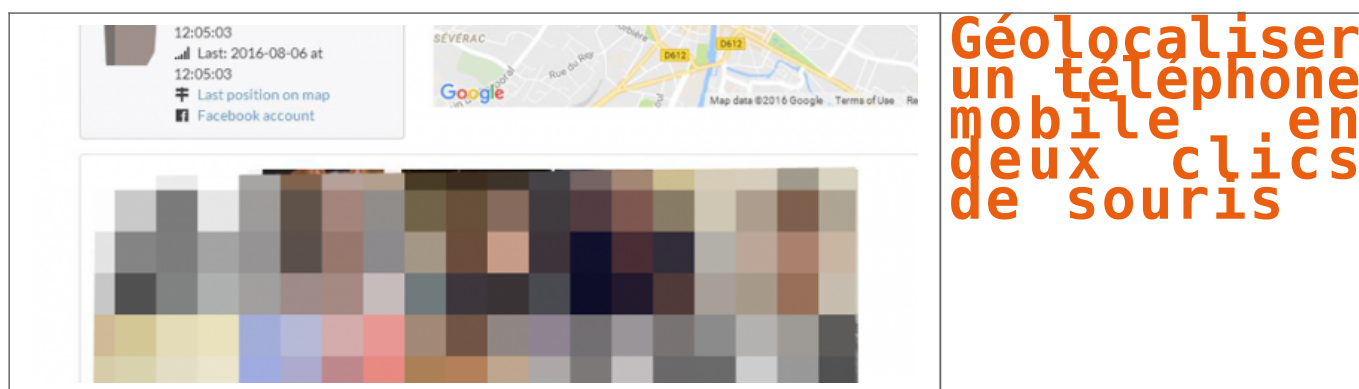


[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : ZATAZ Leakedsource, le site qui met en danger votre vie privée – ZATAZ

Géolocaliser un téléphone mobile en deux clics de souris



Cyber géolocaliser un porteur de téléphone est de plus en plus simple. Un chercheur en informatique montre à ZATAZ.COM comment créer un tracker maison devient simple comme bonjour.

Les téléphones portables, de nos jours, sont de véritables ordinateurs aux capacités de traçage, surveillance et cyber surveillance qui fait froid dans le dos. Regardez, prenons les exemples tels que Facebook et son option « amis à proximité » ou encore PokemonGo et sa capacité de géolocalisation. Du traçage au centimètre. Des technologies de « ciblage » qui deviennent simple à créer et à utiliser. Tristan, informaticien Parisien, vient de contacter ZATAZ pour présenter son cas d'étude : un outil de traçage en temps réel capable de tracer l'itinéraire de ses cibles.

Géolocaliser un téléphone : Souriez, vous êtes pistés

Depuis quelques temps Tristan s'intéresse aux applications proposées dans les mobiles, et plus précisément aux logiciels qui font transiter des informations telles que des positions de latitude et de longitude. Avec un associé, il a lancé Lynx Framework, une entité spécialisée dans la création d'outils de sécurité pour les applications web.

A parti de ses recherches, Tristan a créé un outil de « traque », de quoi géolocaliser un téléphone qui met à jour les dangers de nos mobiles et de leurs capacités à indiquer notre emplacement, mais aussi, nos itinéraires. « **En analysant les requêtes envoyées par certaines applications je me suis rendu compte qu'il serait possible de récupérer le positionnement de plusieurs personnes en même temps et de les positionner sur une carte de type google map.** » m'explique le chercheur.

A l'image des sauvegardes de Google Map que je vous indiquais en 2015, l'outil « privé » de Tristan fait pareil, mais en plus discret encore. Via un outil légal et disponible sur Internet, Burp Suite, notre chercheur a analysé les requêtes envoyées par plusieurs logiciels de rencontres disponible dans le Google Play.

Comment cela fonctionne-t-il ?

« *Le tracker prend le contrôle de plusieurs comptes d'application de rencontre et récupère la position des personnes à proximité, indique-t-il à ZATAZ.COM. Il ajoute ces informations dans sa base de données et vérifie l'existence des positions pour cette identité.* » *Si l'application de Tristan retrouve la même personne, mais pas à la même position, il va créer un itinéraire de l'individu via son ancienne position* ». Nous voilà avec la position et le déplacement exacts d'un téléphone, et donc de son propriétaire, à une heure et date données.

Géolocaliser un téléphone : Chérie, tu faisais quoi le 21 juillet, à 12h39, à 1 cm de ta secrétaire ?

Après quelques jours de recherche, Tristan a mis en place une base de données de déplacement dans une ville. Une commune choisie au hasard. Son outil est en place, plusieurs systèmes sont lancés : Une carte avec le positionnement des personnes croisées ; une page plus explicite pour chaque personne avec la date de croisement, son âge... ; une page ou notre chercheur gère ses comptes dans l'application. Bonus de son idée, un système d'itinéraire complet a été créé. Il permet de tracer un « chemin » de déplacement si la personne croisée a déjà été croisée dans le passé, dans un autre lieu. « J'ai positionné un compte au centre de la ville, un autre à l'entrée et le suivant à la sortie, ce qui a données en quelques heures une 50ème de données » confie-t-il « Il est inquiétant de voir autant de données personnelles transitées en clair via ces applications ».

Géolocaliser un téléphone : détournement possible d'un tel « tracker » ?

Vous l'aurez compris, « tracer » son prochain est facilité par ses applications qui ne protègent pas les informations de positionnement des utilisateurs. Il devient possible d'imaginer une plateforme, en local, avec plusieurs comptes positionnés à des endroits différents dans une ville. Bilan, suivre plusieurs individus devient un jeu d'enfant. Si on ajoute à cela les applications de déplacement de type UB, qui communique les données de ses chauffeurs par exemple, ainsi que celles d'autres réseaux sociaux, il devient réellement inquiétant de se dire que positionner une personne et la tracer se fait en quelques secondes. Deux solutions face à ce genre de traçage : jeter votre portable ou, le mieux je pense, forcer les éditeurs d'applications à vérifier la sécurisation des données envoyées, et les chiffrer pour éviter qu'elles finissent en clair et utilisable par tout le monde.

Article original de Damien Bancal



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.

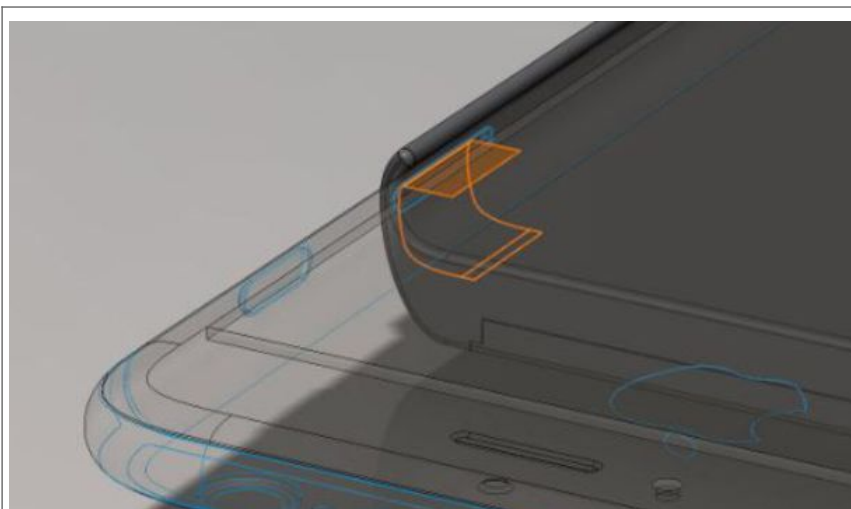


[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : ZATAZ Géolocaliser un téléphone mobile en deux clics de souris – ZATAZ

Snowden conçoit une coque d'iPhone anti-espionnage – L'Express L'Expansion



Snowden conçoit
une coque
d'iPhone anti-
espionnage

Cette coque a pour objectif de protéger les données de nos smartphones. Un premier prototype sera rendu public d'ici un an.

Edward Snowden continue son combat contre la surveillance. L'ancien analyste de la NSA et lanceur d'alerte, qui a levé le voile sur les pratiques d'écoute massive à travers le monde, travaille à la réalisation d'une nouvelle coque d'iPhone. Son atout: elle est capable de protéger les données du téléphone qu'elle abrite.

Pour ce projet, Edward Snowden s'est associé au hacker Andrew «Bunnie» Huang. Dans un rapport, les deux hommes précisent que le mode avion est loin d'être efficace contre le piratage. «Croire au mode avion d'un téléphone hacké équivaut à laisser une personne ivre juger de sa capacité à conduire», indiquent-ils.

Contrôler les signaux envoyés à l'iPhone

Le système, encore au stade d'étude, a été présenté à l'occasion d'une conférence le 21 juillet. L'objet est un périphérique sous logiciel libre qui se pose à l'emplacement de la carte SIM. Il permet ensuite de contrôler les signaux électriques envoyés aux antennes internes du téléphone et donc de savoir si le téléphone partage des informations avec des tiers, sans que vous en soyez conscients.



Une alerte est envoyée dès lors qu'une transmission anormale est détectée.

Mashable explique que «lorsque le mode avion est activé et que les connexions réseaux sont supposées être désactivées, une alerte est envoyée dès lors qu'une transmission anormale est détectée». L'anomalie repérée, le périphérique peut même éteindre le téléphone immédiatement.

Journaliste, activiste et lanceur d'alerte

L'outil, dont le premier prototype devrait être rendu public d'ici un an, a été pensé pour venir en aide aux journalistes, activistes et lanceurs d'alerte «pour détecter quand leurs smartphones sont surveillés et trahissent leurs localisations».

Le programme d'espionnage américain de la NSA, révélé par Edward Snowden a, permis la collecte de données personnelles de millions de citoyens, ainsi que des institutions et chefs d'Etats étrangers. Ces révélations ont montré que ces collectes dépassaient le cadre de la lutte nécessaire contre le terrorisme ou contre les autres risques géopolitiques.

Article original de l'express



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.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Snowden conçoit une coque d'iPhone anti-espionnage – L'Express L'Expansion

Détecter les futurs terroristes sur Internet ? L'Europe veut s'inspirer d'Israël



Détecter
les futurs
terroristes
sur
Internet ?
L'Europe
veut
s'inspirer
d'Israël

Le coordinateur de l'anti-terrorisme pour l'Union européenne, Gilles de Kerchove, s'est rendu en Israël pour trouver des solutions technologiques qui permettraient de détecter automatiquement des profils suspects sur les réseaux sociaux, grâce à des algorithmes de plus en plus intrusifs.

Plus les attentats en Europe se multiplient, plus on découvre que les profils psychologiques et sociaux des kamikazes et de leurs associés sont très divers, jusqu'à paraître indétectables. Le cas de Mohamed Lahouaiej-Bouhlel, dont on ne sait pas toujours très bien s'il s'agit d'un déséquilibré qui se cherchait un modèle ultra-violent à imiter, ou d'un véritable djihadiste islamiste radicalisé à une vitesse inédite, laisse songeur. Bisexuel, amant d'un homme de 73 ans, mangeur de porc, aucune connexion connue avec des réseaux islamistes... l'auteur de l'attentat de Nice était connu des services de police pour des faits de violence de droit commun, mais n'avait rien de l'homme que l'on pourrait soupçonner d'organiser une tuerie motivée par des considérations idéologiques.

Or c'est un problème pour les services de renseignement à qui l'on demande désormais l'impossible, à la Minority Report, c'est-à-dire de connaître à l'avance le passage à l'acte d'un individu, pour être capable de l'appréhender avant son méfait, même lorsqu'objectivement rien ne permettait de présager l'horreur.

C'EST POUR ÇA QUE JE SUIS ICI. NOUS SAVONS QU'ISRAËL A DÉVELOPPÉ BEAUCOUP DE MOYENS DANS LE CYBER

Néanmoins, l'Union européenne ne veut pas se résoudre à la fatalité, et va chercher en Israël les méthodes à appliquer pour détecter sur Internet les terroristes susceptibles un jour de passer à l'acte. « C'est un défi », explique ainsi à l'agence Reuters Gilles de Kerchove, le coordinateur de l'UE pour l'anti-terrorisme, en marge d'une conférence sur le renseignement à Tel Aviv. « Nous allons trouver bientôt des moyens d'être beaucoup plus automatisé » dans la détection des profils suspects sur les réseaux sociaux, explique-t-il. « C'est pour ça que je suis ici ».

« Nous savons qu'Israël a développé beaucoup de moyens dans le cyber », pour faire face aux attaques d'Israéliens par des Palestiniens, ajoute le haut fonctionnaire européen, et l'UE veut s'en inspirer.

ÉTABLIR DES PROFILS SOCIOLOGIQUES ET SURVEILLER LES COMMUNICATIONS

Selon un officiel israélien interrogé par l'agence de presse, il s'agit d'établir constamment des profils types de personnes à suspecter, en s'intéressant non plus seulement aux métadonnées qui renseignent sur le contexte des communications et les habitudes d'un individu, mais bien sur le contenu-même des communications sur les réseaux sociaux.

Mis à jour quotidiennement au gré des nouveaux profils qui émergent, des paramètres comme l'âge de l'internaute, sa religion, son origine socio-économique et ses liens avec d'autres suspects, seraient aussi pris en compte par les algorithmes israéliens – ce qui semble difficilement compatible en Europe avec les textes internationaux protégeant les droits de l'homme, que l'Union européenne s'est engagée à respecter.

DES BOÎTES NOIRES TOUJOURS PLUS INTRUSIVES ?

En somme, c'est exactement ce que nous redoutions avec les fameuses boîtes noires permises par la loi Renseignement en France, dont le Conseil constitutionnel n'a su que dire, et qui se limitent officiellement aux métadonnées. Là aussi, il s'agit d'utiliser des algorithmes, dont on ne sait pas du tout sur quoi ils se basent, pour détecter des profils suspects.

Eagle Security & Defense, une société israélienne proposant des solutions de surveillance sur Internet, a reçu la visite de Christian Estrosi en début d'année.

Il n'est toutefois pas dit que la technologie israélienne soit importée telle quelle, d'autant que M. De Kerchove a lui-même rappelé que le droit européen n'autoriserait pas un tel degré d'intrusion dans la vie privée. Mais le mécanisme décrit par l'officiel d'Israël est très proche.

Il vise tout d'abord à réaliser une première détection sommaire des profils suspects, puis à déterminer parmi eux ceux qui doivent faire l'objet d'une surveillance individualisée. C'est exactement ce que prévoit la loi Renseignement, qui autorise l'installation de boîtes noires chez les FAI ou les hébergeurs et éditeurs pour détecter des comportements suspects d'anonymes, avant de permettre une identification des personnes dont il est confirmé qu'elles méritent une attention particulière.

En Israël, le ratio serait d'environ 20 000 personnes considérées suspectes pour 1 million d'internautes, sur lesquelles ressortiraient entre 10 et 15 profils nécessitant une surveillance étroite.

CHRISTIAN ESTROSI DÉJÀ INTÉRESSÉ

L'information de Reuters confirme ce qu'indiquaient Les Échos le week-end dernier dans un reportage bien informé. « L'Etat hébreu, dont la population a connu sept guerres et deux Intifada depuis sa création, est bel est bien devenu un cas d'école, dans sa façon de gérer une situation d'insécurité permanente. Une expertise dans la mire des décideurs européens », écrivait le quotidien,

Il précisait qu'en février dernier, l'ancien maire de Nice et actuel président de la région Provence-Alpes-Côte d'Azur, Christian Estrosi, s'était déjà rendu en Israël, où il aurait rencontré le PDG de la société Eagle Security and Defense, Giora Eiland, qui est aussi ex-directeur du Conseil de sécurité nationale israélien.

Lors de cette visite, Christian Estrosi aurait insisté sur la nécessité « d'être à la pointe de la lutte par le renseignement contre la cybercriminalité lorsqu'on sait que la radicalisation se fait par le biais des réseaux sociaux ». On imagine que cette conversation lui est revenue en mémoire lorsque sa ville a été meurtrie.

Article original de Guillaume Champeau



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.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Détecter les futurs terroristes sur Internet ? L'Europe veut s'inspirer d'Israël – Politique – Numerama

Quel cadre pour l'État d'urgence et la copie des données informatiques ?



Quel cadre pour
l'État
d'urgence et la
copie des
données
informatiques ?

