

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

Denis JACOPINI  vous informe	Policiers et gendarmes auront accès aux données embarquées des véhicules
---	---

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



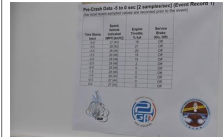
C'est un champ d'investigation suivi de près par les autorités, comme cela a pu nous être expliqué en janvier dernier, lors d'une visite au Pôle judiciaire de la Gendarmerie nationale de Cergy-Pontoise. Dans les véhicules les plus récents, les agents peuvent techniquement scruter tous les relevés techniques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

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

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

La cible, le diagnostic embarqué... mais pas seulement

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



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

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

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

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

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

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

Fichier des assurances, contrôles par lecture automatisée des plaques

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

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

Merci à Marc Rees, l'auteur de cet article



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 téléphoniques, disques durs, e-mails, contenus, débrouchements 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

Régissez à cet article

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

L'Écosse veut désactiver les téléphones utilisés en prison



L'Écosse veut désactiver les téléphones utilisés en prison

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



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

Accéder aux réseaux sociaux, intimider les témoins

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

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

En France, le projet de loi sur la réforme pénale

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

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

Marc Rees auteur de cet article



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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Consultant en Cybercriminalité et en Protection des Données Personnelles

[Contactez-nous](#)

Réagissez à cet article

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

La Cnil accorde un sursis à

Facebook pour faire preuve de loyauté (ou pas)



La Cnil accorde
un sursis à
Facebook pour
faire preuve de
loyauté (ou pas)

Alors qu'il s'apprête à lancer de la publicité ciblée hors de ses services, y compris auprès des non-utilisateurs de sa plateforme, Facebook a obtenu un sursis de 3 mois de la Cnil. L'autorité lui reproche une collecte déloyale de données personnelles.

Le réseau social a été mis en demeure le 9 février par l'autorité française de protection des données personnelles. La Cnil reproche à Facebook une collecte déloyale de données de navigation d'internautes non membres et l'absence de recueil d'un consentement pour le croisement de données à des fins publicitaires.

La firme de Mark Zuckerberg disposait d'un délai de trois mois pour se mettre en conformité. Mais d'après le JDN, Facebook a sollicité auprès de la Cnil un délai supplémentaire de trois mois. Celui-ci lui a été accordé.

Sécurité et publicité grâce au même cookie finalement

« Nous avons repoussé au 9 août le délai obligatoire pour se mettre en conformité » répond la Cnil. Sur le plan commercial, Facebook se montre plus dynamique. La société a annoncé tout récemment un changement de cap.

Elle entend en effet proposer de la publicité ciblée à tous les internautes et non uniquement à ceux inscrits sur son réseau. Pour suivre ces internautes, Facebook met à profit son cookie Datr. La firme assurait pourtant jusqu'à présent que ce cookie avait pour seule finalité la sécurité.

Plus d'ambiguïté à présent. Le réseau social précise que sa régie publicitaire, Audience Network, suivra dorénavant l'ensemble des internautes via ses cookies « même ceux qui ne disposent pas de compte Facebook ou ne s'y connectent pas. »... [Lire la suite]

Merci à ZdNet



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

Source : La Cnil accorde un sursis à Facebook pour faire preuve de loyauté (ou pas) – ZDNet

24.000 bitcoins saisis par la police vendus aux enchères

 Denis JACOPINI DENIS JACOPINI EXPERT INFORMATIQUE ASSERMENTÉ SPÉCIALISÉ EN CYBERCRIMINALITÉ vous informe	24.000 bitcoins saisis par la police vendus aux enchères
---	---

La police Australienne va mettre aux enchères, le 20 juin 2016, 24.000 bitcoins saisis dans des affaires criminelles. Montant du lot, plus de 15.000 euros.



15 882 euros de bitcoins saisis par la justice (24,500 BTC) vont être mis aux enchères, le 20 juin, par la police australienne. De l'argent « dématérialisé » qui sera mis en vente le 20 juin 2016. Pour les autorités, cet argent « virtuel » doit être converti en monnaie sonnante et trébuchante afin de le reverser à l'autorité fiscale locale. Ces bitcoins ont été saisis dans des affaires criminelles et la police a décidé de passer par le mode enchères publique pour s'en débarrasser. C'est la société Ernst & Young qui va se charger de la vente. Ca sera la deuxième vente mondiale de ce type de « produit ».

24.000 Bitcoins saisis

Je vous révélais, en 2014, comment la police fédérale américaine des US Marshall avait revendu pour treize millions de dollars de Bitcoins (144.000 BTC), soit l'équivalent de 8.431.689 euros, dans une vente aux enchères qui commercialisait les BTC du propriétaire de Silk Road, Ross Ulbricht, une boutique du blackmarket spécialisée dans la commercialisation de drogue.

Les bitcoins australiens, ils sont au nombre de 24.518, ont été confisqués en décembre 2013 dans une affaire de drogue, à Melbourne. Son propriétaire, Richard Pollard, 32 ans, a été condamné en octobre 2015, à 11 ans de prison pour trafic de drogue... sur le site Silk Road. Les bitcoins seront vendus par lots d'environ 2.000 BTC... [Lire la suite]

Article original de Damien Banca



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

Source : ZATAZ Vente aux enchères de 24.000 bitcoins saisis par la police – ZATAZ

Alerte Arnaques ! Des pirates informatiques se font passer pour des stars

 Denis JACOPINI FR ? vous informe	Alerte Arnaques ! Des pirates informatiques se font passer pour des stars
--	--

Des pirates informatiques se font passer pour les animateurs vedettes de NRJ, Virgin Radio et autres stars de la FM pour soutirer des informations bancaires.



Des pirates informatiques se font passer pour les animateurs vedettes de NRJ, Virgin Radio et autres stars de la FM pour soutirer des informations bancaires.

Nous connaissons la Fraude au Président, l'arnaque aux faux virements via des informations bancaires soutirées à des entreprises par ruse. Un piège qui fonctionne, malheureusement aussi, sur les locataires de logements sociaux. Les escrocs se font passer pour le bailleur afin de faire modifier les données concernant les virements des loyers.

Aujourd'hui, je viens d'apprendre une nouvelle ruse. Des escrocs se font passer pour les stars de la radio (Manu de NRJ, Camille Combal de Virgin Radio...) en téléphonant et en promettant de l'argent à leurs interlocuteurs. « Un homme dans un soi-disant bureau d'antenne de radio vous dit que vous venez de gagner 2000€ et de doubler votre salaire, souligne l'un des témoins de ZATAZ.COM. Il y a beaucoup de bruit derrière. Comme dans un studio de radio ».

Ils visent vos informations bancaires

Une fois l'interlocuteur appâté, l'appel est transféré à une standardiste « On vous demande un numéro de compte bancaire, souligne un autre lecteur de ZATAZ. Ce qui m'a mis la puce à l'oreille est que le soi-disant animateur fusionne plusieurs jeux du 6/9 de NJR et de Virgin Radio. Pour mettre la personne en confiance, on vous ovationne et félicite pour votre prix. »

La question est de savoir maintenant comment les escrocs peuvent avoir le numéro de téléphone portable et l'identité complète (Nom, prénom) des personnes appelées.

Bref, prudence ! Si vous ne vous inscrivez pas à un jeu officiel, il n'y a pas de raison que ce dernier vous téléphone !... [Lire la suite]

Merci à Damien Bancal auteur de cet article



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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

M

Réagissez à cet article

Source : ZATAZ Informations bancaires : des pirates se font passer pour Manu, Camille Combal – ZATAZ

Denis JACOPINI présent à Abidjan pour le IT Forum 2016 les 7 et 8 juin 2016



La Cybersecurité des banques européennes bientôt soumises à un stress-test ?

Denis JACOPINI  vous informe	La Cybersecurité des banques européennes bientôt soumises à un stress-test ?
--	---

Les attaques visant les systèmes bancaires connectés au réseau Swift soulèvent de vastes inquiétudes au point que les autorités européennes pourraient être appelées à conduire un stress-test visant à éprouver leur cybersécurité.



Recommander les autorités locales des pays membres de l'Union européenne à soumettre les systèmes de sécurité informatique des institutions financières à des stress-tests. C'est l'idée qu'a avancé Andrea Enria, président de l'Autorité Bancaire Européenne, l'autorité indépendante chargée de garantir un niveau de surveillance prudentiel efficace et cohérent à l'échelle de l'Union, à l'occasion d'un échange avec nos confrères de Reuters.

Dans ce cadre, il estime que les banques pourraient avoir à provisionner des réserves supplémentaires afin de se protéger, financièrement, du risque associé à des attaques informatiques. Le risque informatique doit d'ailleurs être explicitement pris en compte dans le cadre des règles Pilier 2. Celles-ci font partie des accords Bâle II et portent justement sur la surveillance prudentielle ainsi que la gestion des risques.

Et la prise en compte des risques associés aux attaques informatiques apparaît particulièrement importante qu'ils sont appelés à être de plus en plus considérés dans les analyses de solvabilité des agences de notation. Moody's et Standard & Poor l'ont ainsi ouvertement indiqué à l'automne dernier.

Fin 2013, les banques britanniques ont été soumises à un stress-test IT, après un premier en 2011. Mais l'opération n'avait pas manqué de soulever plusieurs critiques, certains experts estimant notamment qu'elle devrait survenir plus régulièrement. D'autres s'interrogeaient sur la manière dont étaient définies les attaques imaginées pour l'exercice.

Très récemment, la patronne du gendarme des marchés boursiers américains a de son côté estimé que le risque d'attaque informatique constitue la principale menace pour le système financier mondial, notamment après les opérations qui ont visé dernièrement les systèmes plusieurs banques connectés au réseau Swift... [Lire la suite]

Merci à Valery Marchive pour son article



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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Source : *Vers un stress-test de la cybersécurité des banques*

européennes ?

ZATAZ Santé et fuite de données : et s'il était déjà trop tard – ZATAZ



Santé et fuite de données – Plus de 200 millions de dossiers médicaux de ressortissants américains ont disparu depuis 2015. Et si la lutte contre la protection de nos données de santé était déjà perdue d'avance ?



Le Parlement européen a adopté le jeudi 14 avril 2016 le règlement européen sur la protection des données. Le règlement qui sera applicable à partir du 25 mai 2018 dans l'ensemble des pays membres de l'Union européenne. Avec cette jolie annonce que l'on attend depuis des années, je me suis penché sur un cas concret de fuites de données : les dossiers médicaux. A la fin de ma compilation et analyses des datas collectées, ma question est la suivante : Et si la lutte contre la protection de nos données de santé était déjà perdue d'avance ?

Santé et fuite de données : Plus de 200 millions de dossiers médicaux perdus en 1 an

*J'ai analysé les établissements de santé américains. Il faut dire que cela est plus simple. La France n'a aucun moyen de contrôle au sujet des fuites d'informations dans le secteur Français de la santé. Et ce n'est pas faute d'avoir des personnes très compétentes au Ministère de la Santé et des Affaires Sociales. Mais en France, pour le moment, aucune obligation n'est faite pour que les patients soient alertés en cas de fuite, de piratage, de perte de leurs données (clé usb, portable...). Sur le sol de l'Oncle Sam, il en est tout autre. La loi **Hitech Act** (section 13402) impose l'affichage public de toutes fuites d'informations concernant plus de 500 patients dans le même établissement.*

*En 1 an, la plus grosse fuite de données médicales aux USA aura visé l'Anthem, Inc. Affiliated Covered Entity. Nous sommes alors en mars 2015. 78,8 millions de dossiers suite à un « **Hacking/IT Incident Network Server** » comme le référence le Ministère américain de la Santé (HHS). Depuis le 1er janvier 2016, 103 établissements de santé (Hôpitaux, centres de soin...) ont été touchés par une perte, un vol, un piratage. Dernier cas en date, 2.213.597 de données de patients piratés au 21st Century Oncology de Floride. Ici aussi, le HHS (U.S. Department of Health and Human Services) parle de « **Hacking/IT Incident Network Server** ». L'attaque date du 4 avril 2016.*

Depuis le 1er janvier 2016, 3.605.511 dossiers de patients américains ont volés, piratés ou perdus. Et en France ?

Article 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

Source : ZATAZ Santé et fuite de données : et s'il était déjà trop tard – ZATAZ

Après 3 semaines d'insistance de ZATAZ, la CNIL fait corriger une fuite de données sur le site du PS en quelque heures



Pendant trois semaines, j'ai tenté de faire corriger une fuite de données découverte sur le site du Parti Socialiste. J'ai dû faire appel à la CNIL pour qu'un sympathique communicant de ce parti politique français daigne écouter !

Pendant trois semaines, j'ai tenté de faire corriger une fuite de données découverte sur le site du Parti Socialiste. J'ai dû faire appel à la CNIL pour qu'un sympathique communicant de ce parti politique français daigne écouter !

Des fuites de données, j'en croise des dizaines par mois, des centaines par années. Depuis la création de mon blog, voilà plus de trente ans (sur disquette, puis papier) et bientôt 20 ans sur le web, ZATAZ a pu aider plus de 60.000 entreprises, associations, particuliers à se protéger des malveillants du web. Bref, permettre de corriger une fuite de données, une faille, un problème de piratage via le protocole d'alerte ZATAZ.

Dans 99,9% des cas, cela se passe bien, voire très très bien. Pour les cas étatiques, par exemple, l'ANSSI me répond dans la minute, même un dimanche, à 3h du matin. La CNIL ne met pas plus de temps. Seulement, il y a ce 0,1 % de ... J'ai un mot en tête, mais n'étant pas grossier de nature, je vous laisse l'imaginer.

Allô ! le Parti Socialiste ? vous avez une fuite de données !

Il y a trois semaines, je constatais une étonnante fuite de données visant un sous domaine du site Internet du Parti Socialiste. Je passerai le côté technique de la chose. Il suffisait de cliquer sur un lien particulièrement formulé vers le sous dossier « Archive » pour que s'ouvre un espace d'administration du portail politique du PS. Le « oueb » de ce groupe politique fait parti du 0,1 % de cette froideur intellectuelle et de « je-m'en-foutisme » qui pourraient coûter très chers si un interlocuteur moins impliqué que moi avait eu en main l'accès à cette fuite de données. Car fuite de données il y avait. Il était possible d'accéder aux noms, prénoms, adresses physiques, mails des adhérents, montant des cotisations, code dossier, département ... de l'espace adhésion (en attente de traitement, transmise, non finalisée et effective).

De Moi <urgent@damienbancal.fr>
Sujet **Alerte ZATAZ - faille sur parti-socialiste.fr**
Pour communication@parti-socialiste.fr
Copie à ProtocoleAlerte@zataz.com

Répondre Répondre à tous Transférer Archiver Indésirable Supprimer Autres

22/05/2016 13:51

Bonjour,

Je suis Damien Bancal, journaliste, chercheur dans la lutte contre les malveillances informatiques.

Je tente, désespérément, de joindre un responsable informatique en charge de votre site Internet.

Une faille informatique a été découverte dans parti-socialiste.fr qui donne accès aux informations des adhérents du PS (et il y a de forte chance qu'un malveillant passe par ce biais pour en créer des fictifs.)

Exemples :

J'ai tenté d'avoir une écoute sérieuse de plusieurs personnes proche de votre communication/système informatique, via Twitter/Facebook, afin de transmettre l'information pour une correction rapide. :

https://twitter.com/Damien_Bancal/status/734338571071557634
https://twitter.com/Damien_Bancal/status/734339540188160006

Pour information, j'ai alerté (Nord - 59), élu PS du sud de Lille, , afin qu'il soit alerté de ma démarche.

Bref, après deux mails au service presse (sans réponse) ; deux mails aux DSI BS et JW (sans réponse) ; plusieurs Tweets dont une discussion hallucinante avec l'un des DSI que je tentais de contacter, autant dire qu'au bout de trois semaines, j'ai beau faire cela bénévolement, la moutarde commençait à me monter au nez, surtout après la lecture de plusieurs articles indiquant que d'étonnantes adhésions au PS étaient apparues dans plusieurs circonscriptions (Metz, ...). Je me suis résolu à contacter des élus du PS officiant dans ma région, ainsi que la CNIL. Autant dire qu'avec la prestigieuse dame, cela n'aura pas pris trois semaines. Deux heures après mon alerte à la Commission Informatique et des Libertés, l'étonnant accès disparaissait du web... [Lire la suite]

Article 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

Source : ZATAZ La CNIL fait corriger une fuite de données sur le site du PS – ZATAZ

Plusieurs millions de comptes MySpace en vente en ligne sur le marché noir



Un fichier comportant des informations sur plusieurs centaines de millions de comptes MySpace, dont 427 millions de mots de passe, a été mis en vente sur un site spécialisé, a révélé le site LeakedSource. Selon des tests effectués par Motherboard, les mots de passe figurant dans les documents correspondent bien à des comptes existant ou ayant existé.



Selon LeakedSource, les mots de passe de la base de données étaient chiffrés, mais protégés par une technologie aisément contournable avec du temps et de la puissance de calcul. L'intégralité de la base de donnée a été mise en vente pour environ 2 500 euros sur un site spécialisé dans le recel de données volées.

Un milliard d'inscrits

MySpace, considéré il y a dix ans comme le site le plus populaire pour les adolescents et les étudiants, n'est aujourd'hui plus que l'ombre de ce qu'il était. Le service, qui permet de créer sa page personnelle, avait notamment construit sa popularité en attirant de nombreux groupes de musique populaires. Le service existe toujours, et annonçait à la fin de 2015 avoir dépassé le seuil symbolique du milliard d'inscrits au cours de son existence. Les données contenues dans les fichiers volés restent cependant sensibles – de nombreux internautes réutilisent le même mot de passe pour plusieurs applications ou services. Il est conseillé aux utilisateurs ayant détenu ou détenant un compte MySpace de changer leur mot de passe s'ils l'ont réutilisé sur d'autres services... [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.



[Contactez-nous](#)

Réagissez à cet article

Source : *Les informations de millions de comptes MySpace en vente en ligne*