Votre historique de recherche reste toujours accessible… même effacé

	Votre historique de recherche reste toujours accessible… même effacé

Des sites pornographiques qu'on a visités aux simples liens un peu honteux en passant par les plus classiques marketplaces et réseaux sociaux, on n'aime pas forcément qu'un tiers fouille dans notre historique Internet. C'est pour ça qu'on le supprime assez régulièrement. Mais selon un chercheur en sécurité informatique, ça serait loin de suffire : on peut désanonymiser votre navigation.

Ce n'est pas la première fois qu'une telle thèse est prouvée : cette fois, Svea Deckert et Andreas Dewes en ont fait la démonstration lors de la conférence **Def Con 2017** de Las Vegas.

Les données anonymes collectées par les sites ne sont pas si anonymes que ça

Encore une fois, ce sont les sites Internet qui sont en cause et plus particulièrement les données de navigation qu'ils collectent. Ces données sont stockées pour être revendues à des tiers qui les utilisent, entre autres, pour faire de la publicité ciblée. Il n'y a rien d'illégal là-dedans, pour peu que ces données soient totalement anonymes, c'est-à-dire qu'elles ne doivent pas être reliées à l'adresse IP, unique, de l'utilisateur. Théoriquement, l'anonymisation de ces données devrait suffire à garantir qu'il soit impossible de remonter à vous et de dire que vous avez visité telle ou telle page. Sauf que Svea Eckert et Andreas Dewes ont prouvé le contraire, en se basant sur les données collectées par 10 extensions pour navigateur Internet parmi les plus populaires du marché…[lire la suite]

Réagissez à cet article

Source : *Votre historique de recherche reste toujours accessible… même effacé*

Que sait de nous Google grâce à nos comportements sur Internet ?

	Que sait de nous Google grâce à nos comportements sur Internet ?

Mondialement connue, la firme américaine Google est utilisée par de nombreux internautes, pour son moteur de recherche, mais aussi pour ses nombreux services gratuits (Gmail, Drive, Youtube, Google Maps…). Seul petit hic ? Le revers de la médaille. Puisque Google exploite vos données sans que vous n'en ayez toujours conscience.

Tout le monde connaît Google pour son moteur de recherche ultra-performant. C'est d'ailleurs le moteur préféré des Français. Fin 2016, selon Netbooster, plus de 94 % d'entre eux l'ont utilisé pour effectuer leurs recherches en ligne. Pour apprécier la démesure de ce chiffre, il suffit de voir la part restante à ses principaux concurrents : moins de 4 % pour Bing (Microsoft) et à peine plus de 2 % pour Yahoo.

Plus de 200 services gratuits…

À travers sa maison mère « **Alphabet** », Google est l'une des premières capitalisations mondiales avec une valeur de 588 milliards de dollars, juste derrière Apple. La firme de Moutain View n'est pas la seule à analyser les données qui lui parviennent. Tous les géants du secteur (Apple, Amazon, Facebook…) le font en s'appuyant sur les traces que nous laissons chaque jour sur Internet. Ils engrangent des milliards de dollars grâce à ces informations personnelles.

Inutile donc d'être un financier avisé pour comprendre que la seule activité de moteur de recherche ne suffit pas à générer de telles entrées d'argent. Google est une pieuvre géante, dont les tentacules s'étendent dans des domaines aussi nombreux que variés. Le système d'exploitation Android, le navigateur Internet Chrome, les vidéos YouTube, la plateforme de téléchargement Google Play, la cartographie Google Maps, la suite bureautique Google Documents, le site de partage de photos Picasa…

Ce sont plus de 200 services proposés gratuitement par l'entreprise. Pour la plupart d'entre eux, la seule contrepartie demandée est l'ouverture d'un compte Gmail, le service de messagerie en ligne maison. L'adresse email et le mot de passe associé deviennent alors vos sésames pour vous identifier et entrer dans la sphère Google, depuis n'importe quel terminal à travers le monde.

… en échange de vos données personnelles

Toute cette gratuité a cependant une face cachée : l'exploitation commerciale de nos données personnelles. En effet, elles représentent une manne financière des plus importante. En acceptant les « **conditions générales d'utilisation** », que nous ne lisons quasiment jamais, nous donnons le droit à Google de tracer et d'utiliser tout ce que nous faisons sur Internet : les sites visités, les achats effectués, les lieux dans lesquels nous nous rendons, les films regardés, les livres lus, la musique écoutée…

L'ensemble de ces données est alors analysé par les puissants ordinateurs de la firme, dans le but créer une sorte de carte d'identité très précise de chaque utilisateur. Ces profils, compilant de très nombreuses données, se revendent à prix d'or aux marques désireuses de cibler au mieux leur publicité. C'est ce que l'on appelle le « **Big Data** ».

Pour profiter gratuitement des services de Google, comme ceux de nombreux autres acteurs des nouvelles technologies, nous devons donc rogner sur notre vie privée, en abandonnant la confidentialité de nos données personnelles. Il existe une formule qui résume parfaitement cette pratique : « **si c'est gratuit, c'est que le produit c'est vous !** »…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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

---

Réagissez à cet article

Source : *Données personnelles. Voici ce que Google sait de vous*

Big data. Comment les entreprises recueillent et utilisent nos données ?

Big data. Comment les entreprises recueillent et utilisent nos données ?

En 2015, 11 % des entreprises françaises ont traité des big data, selon l'Insee. Les sources de données les plus utilisées sont la géolocalisation, les médias sociaux et les objets connectés ou capteurs. Les grosses entreprises sont les plus à l'aise pour traiter ces données nombreuses et complexes.

Par Julie DURAND

1 % des entreprises françaises ont traité des big data en 2015. Selon l'Insee, qui a réalisé cette enquête, la big data est constituée de » **données complexes, dont le volume important et l'actualisation constante rendent difficile l'exploitation par les outils classiques** « .

7 % des entreprises traitent des données de géolocalisation

Sans surprise, les grosses entreprises sont plus nombreuses à en utiliser que les petites (24 % contre 9 %). Les barrières à l'utilisation de la data sont plus difficiles à franchir pour elles : mauvaise compréhension du sujet et de son intérêt, manque de compétences, coût trop élevé et législation contraignante.

La donnée la plus recueillie et la plus utilisée est la géolocalisation (pour 62 % des entreprises qui utilisent des data, soit 7 % de l'ensemble des entreprises françaises). Cette donnée intéresse surtout les entreprises de transports (92 %) et la construction (89 %).
Deuxième source : les médias sociaux (pour 32 % des entreprises qui utilisent des data, soit 4 % de l'ensemble). Ces données intéressent surtout l'hébergement-restauration (76 %) et l'information-communication (64 %).
Enfin, les objets connectés et capteurs sont la troisième source de data (29 % des entreprises qui en utilisent, soit 3 % de l'ensemble), utilisés principalement par l'industrie (46 %).

Traitement en interne ou externalisée des données ?

74 % des entreprises qui traitent des données le font en interne et 42 % par des prestataires extérieurs, 16 % utilisent donc ces deux méthodes. Le choix entre traitement interne ou externe dépend du secteur et de la taille de l'entreprise. 90 % des entreprises de l'infomation-communication et 84 % des activités scientifiques et techniques le font en interne, » **car les employés sont probablement mieux formés pour cela que dans d'autres secteurs** ». Tous secteurs confondus, 83 % des entreprises de plus de 250 personnes traitent les data en interne, contre 73 % pour les moins de 250 salariés.
Selon l'Insee, les entreprises utilisent toutes ces données pour optimiser leurs processus internes, améliorer leurs produits ou services et/ou rendre plus efficace leur marketing ou leur gestion des ventes.

Réagissez à cet article

Source : *Big data. Comment les entreprises recueillent et utilisent nos données ?*

Jusqu’où les Objets connectés sont les maillons faibles de la cybersécurité ?

Jusqu’où les Objets connectés sont les maillons faibles de la cybersécurité ?

La Chine s'impose parmi les principaux pays créateurs d'objets quotidiens connectés à l'internet, mais elle génère ainsi de gigantesques failles sécuritaires exploitables par des pirates informatiques, a prévenu mardi John McAfee, créateur américain du logiciel antivirus portant son nom.

S'exprimant devant une conférence spécialisée à Pékin, M. McAfee a cité des précédents, dans lesquels des pirates sont parvenus à distance à prendre le contrôle de coffre-forts, de systèmes de chauffage, mais aussi d'ordinateurs de bord d'automobiles ou d'aéroplanes.

« La Chine prend la tête des progrès sur les objets intelligents, depuis les réfrigérateurs jusqu'aux thermostats, et c'est le maillon faible de la cybersécurité », a-t-il martelé, disant vouloir « lever un drapeau rouge » d'avertissement.
« Il y a tellement plus de ces objets, et plus vous en connectez ensemble, plus les risques de piratage augmentent », a encore souligné John McAfee.
L'excentrique septuagénaire avait fait fortune aux débuts d'internet dans les années 1990, après avoir mis au point un logiciel antivirus qui porte son nom et est maintenant la propriété d'Intel.
Plombé par la crise financière de 2008, il avait défrayé la chronique en 2012 après la mort de son voisin au Belize, pays où il vivait à l'époque et qu'il avait fui après l'ouverture d'une enquête de la police locale.
M. McAfee a livré à Pékin un discours au ton sombre et inquiétant, à l'heure où sa nouvelle société MGT Capital se prépare à lancer de nouveaux produits de cybersécurité d'ici la fin de l'année.
« Notre espèce n'a jamais été confrontée jusqu'ici à une menace de cette ampleur. Et pour l'essentiel, nous n'en prenons pas conscience », a-t-il averti.
« Vous pouvez penser que j'exagère, que je tombe dans l'alarmisme. Mais je compte parmi mes amis beaucoup de +hackers+ (pirates) qui ont les capacités de faire d'énormes dégâts si l'envie leur en prend », a-t-il ajouté.
A l'instar de Xiaomi, fabricant de smartphones ayant élargi son offre dans l'électroménager « intelligent », nombre d'entreprises chinoises intègrent désormais une connexion wi-fi à des produits variés, des autocuiseurs pour riz aux purificateurs d'air, permettant aux usagers de les allumer à distance depuis leur téléphone.
De telles connexions créent de graves failles qui accentuent les vulnérabilités de leurs réseaux, selon John McAfee.
Dans un entretien avec des journalistes à Pékin, l'Américain a cependant noté « n'avoir entendu parler d'aucune » attaque informatique de grande ampleur en Chine sur l'année passée, tandis que les Etats-Unis en enregistraient « des centaines ».

Réagissez à cet article

Original de l’article mis en page : Objets connectés : le créateur de l’antivirus McAfee met en garde la Chine contre les failles de sécurité | La Provence

---

Collectes massives et illégales par le Renseignement allemand

Collectes massives et illégales par le Renseignement allemand

---

Après avoir réalisé un contrôle sur place des services de renseignement, la Cnil allemande a dressé un bilan extrêmement critique des activités du Bundesnachrichtendienst (BND) en matière de collecte d'informations sur Internet.

Le site Netzpolitik a dévoilé le contenu d'un rapport jusque là confidentiel produit en juillet 2015 par Andrea Voßhoff, le commissaire à la protection des données en Allemagne, qui accable les services de renseignement allemands. Le rapport a été réalisé après la visite de l'homologue de la Cnil dans la station d'écoutes Bad Aibling, opérée conjointement en Bavière par l'agence allemande du renseignement, la Bundesnachrichtendienst (BND), et par la National Security Agency (NSA) américaine.
Malgré les difficultés à enquêter qu'il dénonce, Voßhoff dénombre dans son rapport 18 violations graves de la législation, et formule 12 réclamations formelles, qui obligent l'administration à répondre. Dans un pays encore meurtri par les souvenirs de la Stasi, le constat est violent.
L'institution reproche au BND d'avoir créé sept bases de données rassemblant des informations personnelles sur des suspects ou simples citoyens lambda, sans aucun mandat législatif pour ce faire, et de les avoir utilisées depuis plusieurs années au mépris total des principes de légalité. Le commissaire a exigé que ces bases de données soient détruites et rendues inutilisables.

Parmi elles figure une base assise sur le programme XKeyScore de la NSA, qui permet de réunir et fouiller l'ensemble des informations collectées sur le Web (visibles ou obtenues par interception du trafic), pour les rendre accessibles aux analystes qui veulent tout savoir d'un individu et de ses activités en ligne. Alors que XKeyScore est censé cibler des suspects, Voßhoff note que le programme collecte « un grand nombre de données personnelles de personnes irréprochables », et cite en exemple un cas qu'il a pu consulter, où « pour une personne ciblée, les données personnelles de quinze personnes irréprochables étaient collectées et stockées », sans aucun besoin pour l'enquête…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Le Renseignement allemand pris en flagrant délit de collectes massives illégales – Politique – Numerama

Ce que Facebook sait (espionne) sur vous

	Ce que Facebook sait (espionne) sur vous

Si vous vous êtes déjà demandé pourquoi Facebook semble connaître une quantité alarmante de chose sur vous; comme tous les sites Web que vous visitez, pour qui vous votez, et quelle quantité vous buvez, voici pourquoi.

Où que vous alliez, quoi que vous fassiez (si c'est en ligne) les chances sont que Mark Zuckerberg vous observe, et apprend.
Facebook recueille des données lorsque vous êtes sur d'autres sites, dans les applications, et dans Facebook lui-même; développant un profil de 98 *« points de données »* sur vous.
Facebook a récemment déployé une mise à jour de son outil Ad Préférences qui révèle un peu plus les données recueillies par Facebook (tout est fait pour vous servir des publicités *« personnalisées »*).
Certaines d'entre elles sont assez alarmantes (comme si vous êtes enceinte, votre race, et votre titre d'emploi) toutes ces données sont récoltées tranquillement, sans avoir un formulaire à remplir.
Voici les 98 *« points de données »* que Facebook sait probablement de vous, où s'il ne les connait pas encore, il essaye de les apprendre, selon le Washington Post.

Qu'est-ce que Facebook sait sur vous

1. L'emplacement
2. L'âge
3. La génération
4. Le sexe
5. La langue
6. Le niveau d'éducation
7. Le domaine d'études
8. L'école
9. L'affinité ethnique
10. Le revenu et la valeur nette
11. La valeur de la propriété et le type
12. La valeur domestique
13. La surface du terrain
14. La superficie de la maison
15. L'année de construction de la maison
16. La composition du ménage
17. Les utilisateurs qui ont un anniversaire dans les 30 jours
18. Les utilisateurs qui sont loin de leur famille ou de leur ville natale
19. Les utilisateurs qui sont amis avec quelqu'un qui a un anniversaire, nouvellement marié ou engagé, récemment déménagé, ou a un anniversaire à venir
20. Les utilisateurs dans les relations à longue distance
21. Les utilisateurs qui ont de nouvelles relations
22. Les utilisateurs qui ont de nouveaux emplois
23. Les utilisateurs qui sont nouvellement engagés
24. Les utilisateurs qui sont nouvellement mariés
25. Les utilisateurs qui ont récemment déménagé
26. Les utilisateurs qui ont des anniversaires bientôt
27. Les parents
28. Les futurs parents
29. Les occupations, rangées par « type » (football, mode, etc.)
30. Les utilisateurs qui sont susceptibles de participer à la politique
31. Les conservateurs et les libéraux
32. La situation amoureuse
33. L'employeur
34. Le travail
35. Les fonctions du travail
36. Les statuts au travail
37. Les loisirs
38. Les utilisateurs qui possèdent des motos
39. Les utilisateurs qui ont l'intention d'acheter une voiture (et quel type / marque de voiture, et dans combien de temps)
40. Les utilisateurs qui ont acheté des pièces ou accessoires automobiles récemment
41. Les utilisateurs qui sont susceptibles d'avoir besoin de pièces ou de services automobiles
42. Le style et la marque de voiture que vous conduisez
43. L'année d'achat de votre voiture
44. L'âge de votre voiture
45. Combien d'argent l'utilisateur est susceptible de dépenser pour la voiture suivante
46. Lorsque l'utilisateur est susceptible d'acheter la voiture suivante
47. Combien d'employés possède votre entreprise
48. Les utilisateurs qui possèdent des petites entreprises
49. Les utilisateurs qui travaillent dans la gestion ou qui sont cadres
50. Les utilisateurs qui ont fait don à la charité (divisés par type)
51. Le système d'exploitation
52. Les utilisateurs qui jouent à des jeux de navigateur
53. Les utilisateurs qui possèdent une console de jeu
54. Les utilisateurs qui ont créé un événement sur Facebook
55. Les utilisateurs qui ont utilisé les paiements Facebook
56. Les utilisateurs qui ont passé plus que la moyenne sur les paiements Facebook
57. Les utilisateurs qui administrent une page Facebook
58. Les utilisateurs qui ont récemment téléchargé des photos sur Facebook
59. Le navigateur Internet
60. Le service de messagerie e-mail
61. Le passage précoce / tardif à la technologie
62. Les expatriés (divisés par le pays d'origine)
63. Les utilisateurs qui appartiennent à une coopérative de crédit, la banque nationale ou banque régionale
64. Les utilisateurs qui sont investisseurs (divisés par type d'investissement)
65. Le nombre de crédits
66. Les utilisateurs qui utilisent des cartes de crédit
67. Le type de carte
68. Les utilisateurs qui ont une carte de débit
69. Les utilisateurs qui effectuent un solde sur leur carte de crédit
70. Les utilisateurs qui écoutent la radio
71. La préférence dans les émissions télévisées
72. Les utilisateurs qui utilisent un appareil mobile (divisé par quelle marque ils utilisent)
73. Le type de connexion Internet
74. Les utilisateurs qui ont récemment fait l'acquisition d'un smartphone ou d'une tablette
75. Les utilisateurs qui accèdent à Internet via un smartphone ou une tablette
76. Les utilisateurs qui utilisent des coupons
77. Les types de vêtements achetés
78. Le temps passé dans les magasins
79. Les utilisateurs qui sont des « gros » acheteurs de bière, de vin ou de spiritueux
80. Les utilisateurs qui achètent dans les épiceries (et quelles types)
81. Les utilisateurs qui achètent des produits de beauté
82. Les utilisateurs qui achètent des médicaments contre les allergies, la toux / médicaments contre le rhume, les produits de soulagement de la douleur
83. Les utilisateurs qui dépensent de l'argent sur les produits ménagers
84. Les utilisateurs qui dépensent de l'argent sur les produits pour les enfants ou les animaux domestiques, et quels types d'animaux de compagnie
85. Les utilisateurs dont les ménages font des achats plus que ce qui est en moyenne
86. Les utilisateurs qui ont tendance à faire des achats en ligne
87. Les types de restaurants
88. Les types de boutiques et magasins
89. Les utilisateurs qui sont « réceptifs » aux offres des compagnies offrant des assurances auto en ligne, l'éducation ou des prêts hypothécaires plus élevés, les cartes prépayées / la TV par satellite
90. La durée du temps passé dans une maison
91. Les utilisateurs qui sont susceptibles de se déplacer rapidement
92. Les utilisateurs qui sont intéressés par les Jeux Olympiques, le football, le cricket ou le Ramadan
93. Les utilisateurs qui voyagent fréquemment, pour le travail ou pour le plaisir
94. Les utilisateurs qui font la navette jusqu'au travail
95. Les types de vacances d'un utilisateur
96. Les utilisateurs qui sont récemment revenus d'un voyage
97. Les utilisateurs qui ont récemment utilisé une application de voyage
98. Les utilisateurs qui participent à une multipropriété

Source : **Metro.co.uk**

Réagissez à cet article

Original de l'article mis en page : Voici 98 choses que Facebook sait sur vous

---

Position du CERT-FR (Computer Emergency Response Team de

l’ANSSI) vis à vis de Pokemon Go

	Position du CERT-FR (Computer Emergency Response Team de l’ANSSI) vis à vis de Pokemon Go

Cyber-risques liés à l'installation et l'usage de l'application Pokémon GoLancé courant juillet par la société Niantic, le jeu Pokémon Go est depuis devenu un phénomène de société, au point d'être installé sur plus de 75 millions de terminaux mobiles dans le monde. Certains acteurs malveillants ont rapidement tenté d'exploiter la popularité du jeu à des fins criminelles. Certaines précautions s'imposent donc avant de pouvoir tenter de capturer un Dracaufeu ou un Lippoutou sans porter atteinte à la sécurité de son ordiphone.

Cyber-risques liés à l'installation et l'usage de l'application Pokémon Go

Lancé courant juillet par la société Niantic, le jeu Pokémon Go est depuis devenu un phénomène de société, au point d'être installé sur plus de 75 millions de terminaux mobiles dans le monde. Certains acteurs malveillants ont rapidement tenté d'exploiter la popularité du jeu à des fins criminelles. Certaines précautions s'imposent donc avant de pouvoir tenter de capturer un Dracaufeu ou un Lippoutou sans porter atteinte à la sécurité de son ordiphone.

Applications malveillantes

Des sociétés spécialisées en sécurité informatique ont mis en évidence la présence de nombreuses fausses applications se faisant passer pour une version officielle du jeu. Ces applications sont susceptibles de naviguer sur des sites pornographiques pour simuler des clics sur des bannières publicitaires, de bloquer l'accès au terminal et de ne le libérer qu'en contrepartie d'une rançon, ou bien même d'installer d'autres codes malveillants. Au vu du nombre d'applications concernées (plus de 215 au 15 juillet 2016), cette technique semble très populaire, en particulier dans les pays où le jeu n'est pas encore disponible via les sites officiels.

Niveau de permissions demandées par l'application

La version initiale du jeu sur iOS présentait un problème au niveau de la gestion des permissions. En effet, le processus d'enregistrement d'un compte Pokemon Go à l'aide d'un compte Google exigeait un accès complet au profil Google de l'utilisateur.
Suite à la prise de conscience de ce problème, la société Niantic a rapidement réagi en précisant qu'il s'agissait d'une erreur lors du développement. Elle propose désormais une mise à jour pour limiter le niveau d'accès requis au profil Google de l'utilisateur. A noter que la version Android du jeu ne semble pas avoir été affectée par ce problème.
Dans le doute, il est toujours possible de révoquer cet accès en se rendant sur la page de gestion des applications autorisées à accéder à son compte Google.

Collecte de données personnelles

De par son fonctionnement, l'application collecte en permanence de nombreuses données personnelles qui sont ensuite transmises au développeur du jeu, par exemple les informations d'identité liées au compte Google ou la position du joueur obtenue par GPS. Certaines indications visuelles (nom de rue, panneaux, etc) présentes sur les photos prises avec l'application peuvent aussi fournir des indications sur la position actuelle du joueur. La désactivation du mode « réalité augmentée » lors de la phase de capture permet de se prémunir de ce type de risques (et accessoirement, de réduire l'utilisation de la batterie de l'ordiphone).

Pokemons et BYOD

Il peut être tentant d'utiliser un ordiphone professionnel pour augmenter les chances de capture d'un Ronflex. Même s'il est souvent délicat de répondre par la négative à une requête émanant d'un VIP, il semble peu opportun de déployer ce type d'application dans un environnement professionnel, en raison des différents risques évoqués précédemment.

Recommandations

Le CERT-FR recommande de n'installer que la version originale du jeu présente sur les boutiques d'Apple et de Google. En complément, il convient de désactiver la possibilité d'installer une application téléchargée depuis un site tiers (sous Android, paramètre « Sources inconnues » du menu « Sécurité »).
Il est également conseillé de vérifier les permissions demandées par l'application. La version originale du jeu nécessite uniquement :
• d'accéder à l'appareil photo pour les fonctionnalités de réalité augmentée ;
• de rechercher des comptes déjà présents sur l'appareil ;
• de localiser l'utilisateur grâce au GPS ou aux points d'accès Wi-Fi ;
• d'enregistrer localement des fichiers sur le téléphone.
Toute autre permission peut sembler suspecte et mettre en évidence la présence sur l'ordiphone d'une version altérée de l'application.
Le CERT-FR suggère de mettre en place un cloisonnement entre l'identité réelle du joueur et celle de dresseur Pokémon. Pour cela, il est possible d'ouvrir un compte directement auprès du Club des dresseurs Pokémon [8] ou bien de créer une adresse Gmail dédiée à cet usage.
Enfin, le CERT-FR déconseille de pratiquer cette activité dans des lieux où le geo-tagging du joueur pourrait avoir des conséquences (lieu de travail, sites sensibles, etc) [9]…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Bulletin d'actualité CERTFR-2016-ACT-031

Pokémon Go inquiète l’armée française !

	Pokémon Go inquiète l’armée française !

Une note de la Direction de la protection des installations militaires explique en quoi le jeu Pokémon Go représente une menace pour les sites protégés du ministère de la Défense, et délivre des consignes pour interdire le jeu à proximité des zones concernées.

L'accès aux sites militaires est interdit – ou très restreint – au grand public. Et cela vaut également pour les Pokémon. Du moins c'est l'intention affichée par le ministère de la Défense dans une note dévoilée par Le Canard Enchaîné dans son numéro du 31 août (page 4).

Le document révélé date du 25 juillet et est en effet signé par le contre-amiral Frédéric Renaudeau, patron de la Direction de la protection des installations, moyens et activités de la Défense (DPID). On y apprend que plusieurs zones sensibles du ministère de la défense « *abriteraient ces objets et créatures virtuelles. Les risques d'intrusion ou d'attroupement à proximité immédiate sont réels* ».

TOUTE PRÉSENCE DE CRÉATURES ET D'OBJETS VIRTUELS À L'INTÉRIEUR DES ENCEINTES DEVRA ÊTRE SIGNALÉE

Le ton est grave et les risques de Pokémon Go sont fortement soulignés par le contre-amiral. Celui mentionne en effet plusieurs points qu'il juge très dangereux :

• « sous couvert du jeu, il ne peut être exclu que des individus mal intentionnés cherchent à s'introduire subrepticement ou à recueillir des informations sur nos installations […] ;

• les données de géolocalisation des joueurs, non protégées, pourraient donner lieu à exploitation ;

• ce jeu peut générer des phénomènes addictifs préjudiciables à la sécurité individuelle et collective du personnel de la défense. »

Pour contrer la menace, le contre-amiral a délivré des consignes strictes. Le Canard Enchaîné affirme ainsi que dans une annexe de la note, ce dernier interdit l'utilisation de l'application à l'intérieur et à proximité des sites militaires et demande à ce que les forces de sécurité intérieure soient alertées en cas d'attroupement sur la voie publique.

La conclusion de la note est sûrement l'élément le plus incongru. Il y est en effet précisé que « toute présence de créatures et d'objets virtuels à l'intérieur des enceintes » devra être signalée à la DPID. Grâce à cela, le document officiel estime que « cette cartographie permettra de consolider notre évaluation de la menace ».

Il est intéressant de voir à quel point le jeu Pokémon Go peut susciter les pires craintes des hautes sphères décisionnelles. Ici, on ne peut s'empêcher d'esquisser un sourire en lisant les termes un tantinet exagérés pour parler des dangers de l'application. On peut également dénoncer quelques paradoxes. En effet, comment signaler la présence d'une créature sur les sites concernés si l'utilisation de Pokémon Go est formellement interdite ?

On peut tout de même nuancer en estimant que le ton un brin catastrophique de la note est de rigueur pour tout ce qui touche à la sécurité intérieure, surtout dans le contexte actuel. À noter que, récemment, la ministre Najat Vallaud-Belkacem, a demandé rendez-vous avec Niantic pour retirer tous les Pokémon rares dans les établissements scolaires.

Article original de Omar Belkaab

Réagissez à cet article

Original de l'article mis en page : Quand Pokémon Go inquiète l'armée française – Pop culture – Numerama

---

Géolocaliser un téléphone mobile en deux clics de

souris

	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 50ène 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

Réagissez à cet article

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

Ma vie disséquée à travers mes données personnelles

Ma vie disséquée à travers mes données personnelles

Plusieurs centaines de fois par jour, nous générons des données qui disent où nous allons, ce que nous faisons, avec qui nous mangeons et ce que nous avons pris comme dessert.

La NSA. Google. Les opérateurs téléphoniques. Nos banques. La DGSE. Les cartes de fidélité. Le Pass Navigo. La vidéosurveillance. Du lever au coucher, on sait depuis quelques années que nos vies se copient en temps presque réel dans des bases de données, parfois sans notre véritable consentement. L'anonyme dans la foule est de moins en moins flou.
A quoi ressemble une vie contemporaine, et donc numérisée ? Dessine-t-elle un portrait fidèle de ce que je suis ? Est-ce même encore possible, en 2014, de le savoir ?

Vendredi matin, mon réveil sonne. Mon premier réflexe : allumer mon iPhone. Son réflexe ? Se géolocaliser. Il répète l'opération plusieurs fois dans la journée, si l'option n'a pas été désactivée, afin d'*« améliorer ses performances et proposer des informations utiles en fonction des lieux où vous êtes »*.

Apple n'assure que les données sont stockées sur mon iPhone, accessible uniquement par moi, et non dans un « datacenter ». La vague certitude que le détail de mes allers et venues n'est pas mémorisé dans un lieu que j'imagine froid, vaste et à l'autre bout du monde est une maigre consolation.

Pour accéder à ce menu : Réglages > Confidentialité > Services de localisation > Services système > Lieux fréquents.

Je constate la réception, pendant la nuit, de iMessages dont je préférerais qu'ils ne soient pas lus par d'autres. Apple m'assure qu'ils sont chiffrés et être incapable elle-même de les lire. Mais en même temps, la NSA a ajouté l'entreprise à son programme Prism, qui permet d'accéder de manière privilégiée aux données de plusieurs géants du Web, en octobre 2012.
Ce n'est pas tout : Apple a récemment détaillé la manière dont l'entreprise répond aux demandes de données des autorités. On y apprend que même les passages au « Genius Bar », le service après-vente d'Apple, sont mémorisés.
Sur la table du petit déjeuner, l'iPhone a remplacé le dos de la boîte de céréales. Les corn-flakes ne pouvaient pas savoir où j'habitais. L'iPhone, si : chacune de mes localisations, implacablement consignées dans sa mémoire, lui permet de situer mon « domicile » sur une carte. Les corn-flakes n'étaient pas l'allié objectif de mon patron. L'iPhone, lui n'indique le temps nécessaire pour rejoindre un autre lieu qu'il a identifié : *« Si vous partiez maintenant, il vous faudrait 28 minutes pour arriver sur votre lieu de travail. »*
La pluie me pousse vers la station de métro. Le portique s'ouvre après le passage du badge. Le Pass Navigo, gratuit, est recommandé à tous les utilisateurs réguliers de la RATP ; il est associé à toute son identité. Il ne sauvegarde que mes trois dernières validations aux portiques de la RATP.
La raison ? Un combat de dix ans avec la Commission nationale de l'informatique et des libertés (CNIL) qui s'est efforcée de limiter l'appétit en données de la RATP. Un Navigo « découverte », anonyme mais coûtant 5 euros existe, mais il est difficile de se le procurer.
Mes trajets de métro, mes séances ciné… Tout est stocké quelque part.
Arrivée 26 minutes plus tard sur mon lieu de travail. Le badge à l'accueil fait biper la porte. Un son qui devrait me rappeler que toutes mes allers et venues sont consignées également dans une base de données.
Renseignements pris, on m'assure que mon chef ne peut y avoir accès, même si certains ont tenté, mais les données servent, en cas de problème, à savoir qui est entré dans le bâtiment. J'ai essayé, en vain, d'avoir le détail des données associées à mon badge, mais je n'ai reçu aucune réponse.
A peine arrivé au bureau, je prévois déjà d'aller au cinéma le lendemain. En cherchant les horaires, je me fais la réflexion que ma carte UGC Illimité doit enregistrer l'ensemble des informations et des films que je suis allé voir.
Cette recherche personnelle devient donc professionnelle : hélas, impossible de savoir quelles données sont conservées. Les conditions générales d'abonnement, qui sont rarement lues, n'en font pas mention. Et impossible de savoir où réclamer l'accès à mes données. UGC n'est d'ailleurs pas d'une très grande aide : *« Tout le monde est à Cannes »*, me répond-on quand j'essaie d'en savoir plus.
Ces exemples d'organismes pas très enthousiastes à l'idée de répondre à mes demandes ne sont pas isolés. Je me rends vite compte du nombre effarant de bases de données dans lesquelles figurent des bribes de mon existence, ainsi que de la réticence (ou l'incompréhension) de certains organismes.
La loi informatique et libertés de 1978 prévoit pourtant explicitement un droit quasiment inconditionnel d'accès aux données personnelles. En cas de refus ou au bout de deux mois sans réponse, je peux même saisir laCNIL, qui peut *« faire usage de ses pouvoirs de contrôle et de sanction »*. Et même, en dernier recours, le procureur de la République.
La composition de mon déjeuner est stockée pendant treize mois
A l'heure du déjeuner, nouveau big caractéristique : celui de ma carte de cantine. Là aussi, l'historique de mes consommations est gardé pendant treize mois. Que peut donc faire le chef avec mes pâtes fraîches achetées en juin 2013 ? *« Oh, nous n'en faisons rien, mais je peux vous sortir tous vos tickets. »*
Passage ensuite à la pharmacie. La carte Vitale, obligatoire pour obtenir le remboursement des médicaments, enregistre la transaction. En jaugeant ce qu'est capable de faire la Sécu avec les données de ses assurés, j'imagine que mon achat d'aujourd'hui va rejoindre ceux que j'ai faits tout au long de ma vie dans les serveurs de l'assurance-maladie.
Analyse épidémiologique avec le Sniiram (Système national d'information inter-régimes de l'Assurance maladie) ou surveillance de la fraude chez les consommateurs avec Erasme, la Sécu mouline mes données, sûrement pour mon bien. Et certains espèrent même pouvoir y accéder pour leur bien à eux dans le cadre d'une ouverture des données publiques…
La loi permet aux organismes détenteurs de nos données de facturer leur envoi, à un coût qui ne doit pas dépasser leur coût de reproduction. La plupart des gens autour de moi n'ont qu'à se connecter à leur espace client, sur Internet, pour accéder à leurs factures détaillées. Mon opérateur (BbYou) me propose également ces documents… Mais les numéros de téléphone de mes correspondants y sont expurgés de leurs deux derniers chiffres. Pour les ajouter , il m'en coûtera 7 euros… par facture.

Mon activité sur Google, jour par jour, heure par heure. Google

Cette quête de mes données est sans fin. J'utilise Google des centaines de fois par jour. Normalement, j'ai désactivé la sauvegarde automatique de chacune de mes recherches. Je vérifie… Manqué : les 11 999 recherches effectuées dans Google depuis le 1er septembre 2012 sont là, à portée de clic depuis mon compte Google.
Requêtes personnelles et professionnelles se mélangent allégrement, et « cat eating quinoa » ou « scary manchot » côtoient « rapport de la Cour des comptes sur l'assiette des impôts locaux » ou « imprimé de changement de situation ameli ».
Prises individuellement, ces recherches font sourire ou consternent, paraissent étranges ou anodines, déplacées ou cryptiques. Mais en parcourant plusieurs pages, c'est tout simplement mes intérêts professionnels, mes lubies, mes passe-temps qui sont soigneusement classés par ordre chronologique. Me revient alors en mémoire le livre de l'artiste Albertine Meunier, qui compile trois ans de recherches Google. Et je désactive aussi sec la mémorisation de mes recherches.
La journée avance et les données continuent de s'égrener derrière moi. La carte de fidélité du supermarché qui garde l'historique de mes achats pour me profiler, mes écoutes sur Spotify, mon achat de billet de train à la SNCF, les centaines de caméras de vidéosurveillance devant lesquelles je passe chaque jour, mes données bancaires, celles de mon compte Apple…

L'ensemble des données liées à un abonnement Vélib LeMonde.fr

La soirée s'éternise, le dernier métro est passé. Je prends un vélo à la station la plus proche. La carte Vélib longue durée libère un vélo. Dans le même temps, les informations sur la prise du vélo sont envoyées au serveur de JCDecaux, en délégation de service public. Selon le publicitaire, les données relatives à la base de départ et à la base d'arrivée seront effacées dès que mon vélo sera rattaché sur la station d'arrivée. Ils gardent tout de même deux ans d'historique de mes contacts avec l'assistance Vélib.
Sur le chemin, je repense alors à mes données de géolocalisation sur mon iPhone. Il n'y a aucune raison pour que Google ne fasse pas la même chose. Chez moi, une recherche (sur Google) m'apprend que le géant de la recherche stocke bien ma géolocalisation en temps réel. Je me précipite sur mon historique de localisation. Rien, la carte qui s'affiche est vide. Par acquit de conscience, je demande le lendemain à une collègue qui possède un téléphone fonctionnant sous Android, donc Google, d'aller sur la même page que moi.

Des déplacements récents effectués dans Paris. Le Monde
Mon week-end dans L'Ain, mes sorties de course à pied, mes promenades, tout y est.
Elle ne peut pas retenir un cri : sur la carte de Paris, des centaines de petits points rouges, traces bien voyantes de tous ses déplacements. Pour illustrer cet article, j'active, heureusement non sans mal, la même fonctionnalité sur mon iPhone. Au bout d'un mois, tous mes déplacements sont minutieusement consignés chez le géant californien. Ma position quasiment minute par minute, à toute heure du jour et de la nuit. Mon week-end dans L'Ain, mes sorties de course à pied, mes promenades, tout y est.
Au terme de cette plongée ardue dans les traces ma propre existence, difficile de parvenir à une conclusion. Certes, avoir la liste de toutes les applications iPhone téléchargées depuis la création de mon compte n'est pas très intéressant, y compris pour moi. Oui, le détail de mes menus de cantine ne fera peur qu'à un nutritionniste. D'accord, je ne donne pas ces données gratuitement, et trouve formidablement pratique de pouvoir me repérer dans une capitale ou pouvoir écouter de la musique librement.

Des déplacement récents effectués en France. | Le Monde

Mais mises bout à bout, ces bases de données réunissent mes goûts, mes habitudes, mes obsessions, mes loisirs, mes centres d'intérêt. Dispersées sur des ordinateurs aux quatre coins du monde, ces données, souvent analysées, résistent encore aux croisements et recoupements divers. Mais pour combien de temps ?
Autre évidence : de plus en plus, les entreprises, les outils et les services que nous utilisons vont collecter nos données. Souvent activés par défaut, ces dispositifs ne nous laissent pas souvent le choix. Que faire, puisque personne ne peut vivre parfaitement déconnecté, ni ne peut passer maître dans la dissimulation de toutes ses traces ?
Article original de Alexandre Léchenet et Martin Untersinger

Réagissez à cet article

Original de l'article mis en page : Ma vie disséquée à travers mes données personnelles