Une série de clics suffisent à vous identifier

Une série de clics suffisent à vous identifier

Corréler l'historique des pages Web visitées aux profils Twitter permet d'identifier les internautes, expliquent des chercheurs de Princeton et de Standford. Ou quand le Big Data vient lever ce qui restait d'anonymat sur le Web.

L'anonymat sur Internet, un vœu pieux ? C'est en somme la démonstration d'une équipe de chercheurs des universités de Princeton et Standford. Ces derniers ont imaginé une extension pour le navigateur Chrome qui permet aux utilisateurs de prendre conscience de l'intérêt des traces qu'ils laissent sur le Net pour des publicitaires ou des espions. L'utilitaire, appelée Footprints, collecte les liens cliqués par l'utilisateur au cours des 30 derniers jours et, à partir de ces seules informations, renvoie une liste de 15 profils Twitter susceptibles de coller à cet usage. Ensuite, l'extension s'efface d'elle-même, assurent les chercheurs.
Professeur assistant à l'université de Standford, Sharad Goel explique que l'objectif de cet outil est avant tout éducatif : « *nous n'envisageons pas de rendre cet outil accessible à d'autres, il s'agit avant tout de réveiller les consciences.* » Un outil de ce type permettrait par exemple à une entreprise traçant déjà ses utilisateurs – soit la totalité des sites marchands notamment – de deviner l'identité des internautes, par corrélation avec leur usage d'un réseau social. En effet, si les publicitaires ou les spécialistes du marketing analysent déjà les traces laissées par les utilisateurs pour personnaliser l'expérience des clients online, ils ne sont en général pas en mesure de remonter jusqu'à l'identité réelle de l'internaute. Les chercheurs montrent que cette anonymat déjà tout relatif pourrait en pratique être levé, grâce à des analyses statistiques et au Big Data.

Dis-moi ce que tu cliques, j'en déduirai qui tu es

Dans un billet de blog, une étudiante de Standford ayant participé à la conception de Footprints, Jessica Su, explique le principe de la méthode : « *Partant de la combinaison unique de pages Web qu'un individu a visitées, nous déterminons les fils de réseau social similaires à cet historique, calculant une liste d'utilisateurs qui ont toutes les chances d'avoir produit cette série de clics. De cette façon, nous pouvons relier l'identité réelle d'une personne à un jeu de liens visités, y compris les liens qui n'ont jamais été postés publiquement sur aucun réseau social.* »…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Une série de clics et Twitter suffisent à vous identifier

---

Comment Facebook manipule le contenu qu’il nous affiche ?

Comment Facebook manipule le contenu qu’il nous affiche ?

Censure d'une photo historique, choix d'articles qui renforcent les partis pris: les centaines de millions d'internautes qui s'informent via leurs «amis» sur Facebook, plutôt que par les médias classiques, courent le risque d'une information biaisée, selon des experts.

Dernier exemple en date, la censure par Facebook la semaine dernière de la célèbre photo d'une petite Vietnamienne nue brûlée au napalm, au nom de sa politique contre la nudité des enfants. Critiqué dans le monde entier, le groupe américain a rétabli la photo et promis de tenir compte à l'avenir du «statut d'icône» des clichés historiques.
Cette polémique a révélé l'importance prise par Facebook comme source d'information pour une majorité d'internautes dans le monde.
Un sondage international du Reuters Institute montre que 51% des personnes interrogées dans 26 pays s'informent par les réseaux sociaux, dont 44% par Facebook, et que 12% en ont fait leur première source d'information. En France, un Français sur deux consulte Facebook, surtout sur mobile, et peut y passer plusieurs heures par semaine.
Aucun des 1,7 milliard d'utilisateurs ne voit les mêmes informations dans son «newsfeed» (fil d'actualités), qui compile les messages de ses «amis»: un mélange de commentaires personnels et d'articles partagés, provenant aussi bien de grands médias que de blogues inconnus.
Entre les milliers de messages produits par ses amis, impossible de tout lire: c'est l'algorithme de Facebook qui, pour chacun, classe ceux placés en haut de page. Et donc ceux qui seront vus, car en moyenne l'utilisateur ne lit que 200 des 2000 messages de son fil.
Les utilisateurs ignorent le plus souvent l'existence et les critères de ce tri, qui ont changé sans cesse en 10 ans d'existence. En juin, Facebook a brusquement décidé de privilégier les messages personnels au détriment des partages d'articles, diminuant la place des médias classiques…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** 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-cybercriminalite-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.

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

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Comment Facebook filtre notre connaissance du monde | Laurence BENHAMOU | Internet

---

Même le FBI vous recommande très fortement de faire cela sur votre ordinateur !! Suivez leurs conseils !

Même le FBI vous recommande très fortement de faire cela sur votre ordinateur !! Suivez leurs conseils !

C’est lors d’une conférence organisée à Washington que le directeur du Bureau fédéral d’enquête (FBI), James Comey, a évoqué la question de la cybersécurité.

C’était le 14 Septembre dernier. Et il a donné un conseil très précieux que nous devrions tous appliquer : « *Si vous allez dans n’importe quel bureau du gouvernement, vous verrez ces petites caméras au-dessus des écrans. Toutes ont un petit cache placé dessus. On fait ça pour éviter que des gens qui n’y sont pas autorisés ne nous regardent.* […] *Je pense que c’est une bonne chose.* »

Effectivement, même si vous êtes un simple particulier, vous n’êtes pas à l’abri qu’un hacker prenne la main sur votre ordinateur et accède à votre webcam et votre micro. Etre écouté et observé dans son intimité ? Non merci sans façon ! Alors on vous conseille d’aller vite mettre un petit bout d’adhésif sur votre ordi…Question de précaution !

Beaucoup de gens le font déjà, rappelez vous au mois de Juin, nous vous avions parlé de **cette photo de Mark Zuckerberg où l’on peut voir son ordinateur avec la cam et le micro protégés …**

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l’étranger** 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-cybercriminalite-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.

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

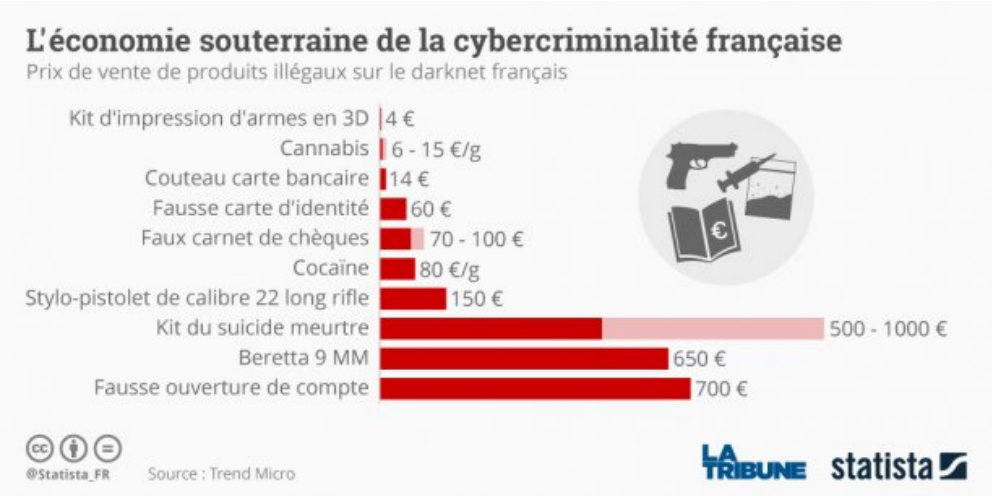
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Le FBI vous recommande très fortement de faire cela sur votre ordinateur !! Suivez

leurs conseils !

Qui sont les escrocs du darknet français ?



Qui sont les escrocs du darknet français ?

Pour la première fois, une étude, réalisée par la société de cybersécurité Trend Micro, s'est penchée sur l'organisation de la sphère cybercriminelle française. D'après ses estimations, 40.000 escrocs réalisent un chiffre d'affaires compris entre 5 et 10 millions d'euros par mois.

À quoi ressemble l'économie souterraine de la cybercriminalité française ? Combien de hackers malveillants y prospèrent ? Comment s'organisent-ils, que vendent-ils et combien gagnent-ils ? Pour la première fois en France, une étude, réalisée par l'entreprise de cybersécurité Trend Micro et publiée ce mercredi, donne des réponses. Pendant un an, ses équipes de R et D ont scruté les marchés souterrains nationaux et compris ses spécificités.
Le panorama dressé, plutôt inquiétant, révèle les dessous du « web underground » français. Un écosystème criminel qui prospère dans le *darknet* (l'internet caché), mais qui apparaît très bien organisé, en pleine professionnalisation et… en pleine croissance.

40.000 cybercriminels dans une centaine de places de marché

Selon les estimations de l'auteur de l'étude, qui souhaite rester anonyme, le cybercrime français se compose de 40.000 individus. Un chiffre « relativement faible » par rapport aux marchés plus importants comme la Russie ou les États unis, mais comparable à celui de l'Allemagne. Ce chiffre a été obtenu en compilant et en pondérant le nombre de membres de la centaine de « marketplaces » du *darknet*, c'est-à-dire les forums de discussions qui sont indispensables aux hackers pour organiser leurs fraudes.
Quel est le profil de ces cybercriminels ? Bien évidemment, tout le monde utilise un ou plusieurs pseudo, des plus loufoques aux plus lyriques. Mais les connaisseurs de ce milieu estiment qu'il s'agit surtout d'hommes jeunes, entre 20 et 30 ans. Au regard de leurs compétences techniques, certains sont « *certainement des développeurs professionnels*« . On assiste aussi au retour en force des anciens « spammers nigérians », les escrocs qui envoyaient des courriels pour demander de l'aide dans les années 1990 et 2000, et qui se reconvertissent désormais dans les virus informatiques.
Relatif soulagement : la plupart des 40.000 cybercriminels français ne vivent pas exclusivement de cette activité. Seule une petite centaine d'entre eux seraient « de vrais pros ». Les autres sont plutôt à la recherche d'un complément de revenus. Mais cela n'empêche pas cet écosystème de prospérer. D'après les données de la Gendarmerie nationale et de la Police nationale, la cybercriminalité française générerait entre 5 et 10 millions d'euros de chiffre d'affaires tous les mois.

Armes, drogues, données bancaires

Les places de marché, qui attirent au moins plusieurs milliers, voire une dizaine de milliers d'utilisateurs chacune (la plupart du temps, les hackers sont membres de plusieurs forums) sont très bien structurées, avec des sous-sections clairement identifiées en fonction des « besoins » : armes, logiciels malveillants, drogues…
Comment s'organise ce commerce ? « *Généralement, il existe trois canaux de vente de biens et de services illégaux au sein de l'underground français* », décrypte l'étude. Certains fraudeurs font la promotion de leurs produits directement sur les places de marchés. D'autres, plus paranoïaques, guettent les messages et contactent eux-mêmes leurs clients. Enfin, il existe aussi des « autoshops », c'est-à-dire de véritables boutiques gérées par les vendeurs eux-mêmes, dont beaucoup sont accessibles depuis les forums. C'est même la grande spécialité française.
Les vendeurs proposent un catalogue impressionnant de produits illégaux, à des prix très compétitifs. On y trouve des armes discrètes (poings américains, couteaux de petits formats, stylo-pistolets de calibre 22 long rifle), vendues entre 10 et 150 euros. Mais aussi des armes lourdes, vendues entre 650 et 1.800 euros, ainsi que des kits d'impression d'armes en 3D, que l'on peut acquérir pour une poignée d'euros.
Au rayon des stupéfiants, le cannabis se vend entre 6 et 15 euros le gramme, mais on trouve aussi de la cocaïne, de l'héroïne, de la MDMA, du LSD et autres champignons. »*Les dealers ne vendent qu'en France pour ne pas se faire détecter lors des transactions transfrontalières* », note l'étude. Les autoshops proposent également des fichiers comportant des bases de données personnelles (comme des numéros de carte bancaire) pour environ 400 euros…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** 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-cybercriminalite-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.

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

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Cybercriminalité : qui sont les escrocs du darknet français ?

Trend Micro ausculte la cybercriminalité underground en France

	A quoi ressemble de DarkNet ?

L'éditeur de sécurité a dressé un état des lieux de l'underground de la cybercriminalité en France. Méfiance, bitcoins et forte orientation vers les falsifications des documents sont les maîtres mots.
Un chercheur de Trend Micro s'est livré à un exercice délicat : plonger dans l'univers de la cybercriminalité souterraine en France. Connu sous le vocable « underground », cette partie du web accueille des places de marchés, des forums où s'achètent contre monnaie virtuelle des armes, de la drogue, des faux documents, mais aussi des malwares.
Dans son étude, l'éditeur japonais précise que le tréfonds du web français reste relativement modeste par rapport à d'autres pays comme la Chine ou la Russie. Néanmoins, il recense 40 000 cybercriminels sur l'underground hexagonal ayant des compétences hétérogènes (expert à novice). Ce foyer génère entre 5 à 10 millions d'euros par mois.

Une prudence de sioux
Un des leitmotiv des cybercriminels français est la prudence. Pour approcher ce monde souterrain, il faut montrer patte blanche. L'objectif est d'éviter de se faire coincer par les forces de l'ordre. Le climat de méfiance règne donc allant jusqu'à la délation (signalement des actes malhonnêtes et frauduleux) et jusqu'à l'affrontement (les places de marché se piratent mutuellement pour se piquer des clients).
L'acceptation sur les forums fait par cooptation, par évaluation de la réputation. Mais ce qui distingue le Dark Net Français, c'est le recours à des tiers de confiance (escrow en anglais). Ils jouent un rôle d'intermédiaire dans la transaction entre les deux parties pour s'assurer que chacun récupère son dû. Ces intermédiaires prennent une commission (entre 5 et 7%) sur la transaction. Certaines places de marché ont même créé leurs propres plateformes de tiers de confiance (mais faut-il encore avoir confiance ?).
La disparition des forums est aussi un grand classique, comme le précise le chercheur de Trend Micro. « Un des forums les plus en vue du French Dark Net qui recensait 40 000 utilisateurs avec la possibilité de gérer leurs transactions a fermé du jour au lendemain et les administrateurs se sont enfuis avec la caisse. Le préjudice est estimé à 180 000 euros. » Et d'ajouter que les mêmes administrateurs ont créé une nouvelle structure dans les jours suivant. Rien ne se perd, tout se crée.

Chiffrement et bitcoin de rigueur
Parmi les autres enseignements, l'underground français n'échappe pas à la vague du chiffrement des communications. Logique, avec un degré de méfiance qui frise la paranoïa, les conversations sont chiffrées et plutôt fortement, assure Trend Micro. « On est principalement sur du PGP. » De même, l'usage de Tor s'est banalisé. Pour trouver les forums ou les places de marché, il est quasiment impossible de les repérer sur le web normal. Les sites se terminent par .onion indiquant son appartenance au réseau anonymisé Tor.
Le Bitcoin et les cartes prépayées sont les moyens de paiement préférés sur l'underground français. La crypto-monnaie est traditionnellement utilisée dans ce genre de secteur. Mais la carte prépayée PCS est une spécificité française. « Elles sont devenues si populaires que certains cybercriminels vendent ce type de cartes avec de faux papiers d'identité et des fausses informations personnelles comme adresse physique, e-mail et carte SIM. L'objectif est de déverrouiller le plafond de paiement pour atteindre jusqu'à 3000 euros. L'opération coûte à peu près 60 euros », souligne Trend Micro.

Le royaume des faux documents officiels et Pass PTT
Héritage du système jacobin et du régime napoléonien, la France est la partie des papiers administratifs. On ne s'étonnera donc pas que les propositions commerciales sur le Dark Net hexagonal concernent la fraude aux documents administratifs. Fausse carte d'identité, carte grise (500 euros), carte PMR (mobilité réduite pour 40 euros), justificatif de domicile (utile pour certaines démarches), vente de points pour le permis de conduire, ouverture d'un compte bancaire (700 euros).
Autre élément typiquement français, le pass PTT. Il s'agit d'une clé dont dispose les livreurs pour ouvrir l'ensemble des boîtes aux lettres d'un immeuble. Les personnes peuvent ainsi chercher des plis contenant de l'argent, des chéquiers ou des clés de maison. Ces pass PTT sont disponibles sur les forums underground à des tarifs abordables. Un vendeur proposait 25 clés pour 220 euros, un autre vendait à l'unité au tarif de 15 euros et un troisième livrait un fichier d'impression 3D de la dite clé, rapporte l'éditeur de sécurité…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Trend Micro ausculte la cybercriminalité underground en France

---

Extension de règles de sécurité des opérateurs aux acteurs du Net en Europe

Extension de règles de sécurité des opérateurs aux acteurs du Net en Europe

---

En proposant de nouvelles règles télécom cette semaine, la Commission européenne introduirait des obligations de sécurité aux services de messagerie. Des obligations déjà en vigueur pour les opérateurs, qui réclament une parité réglementaire avec les acteurs en ligne.

Équilibrer les obligations entre opérateurs et messageries en ligne ressemble souvent à un travail de funambule, dans lequel se lancerait la Commission européenne. Dans quelques jours, l'institution doit dévoiler une révision des règles télécoms en Europe. Selon un brouillon obtenu par Reuters, elle y introduirait des obligations de sécurité pour les services de messagerie en ligne, déjà appliquées par les opérateurs.

Des obligations de signalement des brèches

À la mi-août, plusieurs médias affirmaient que la Commission européenne comptait proposer cette parité entre acteurs. Le brouillon obtenu par Reuters viendrait donc confirmer cette piste. Dans celui-ci, les services « over the top » devront ainsi signaler les brèches « *qui ont un impact important sur leur activité* » aux autorités et disposer d'un plan de continuité de l'activité. Les services qui proposent des numéros de téléphone ou d'en appeler, comme Skype, devront aussi permettre les appels d'urgence.

Pourtant, ces règles pourront être plus légères pour ces services que pour les opérateurs classiques, dans la mesure où les services ne maîtrisent pas complètement la transmission des contenus via les tuyaux. Dans l'absolu, ces règles doivent réduire l'écart d'obligations entre les acteurs télécoms et ceux d'Internet, avec en toile de fond le combat entre des acteurs européens et des sociétés principalement américaines.

Rappelons que le règlement sur les données personnelles, voté en avril par le Parlement européen, doit lui aussi obliger les services à divulguer aux autorités les fuites de données, dans un délai court. En France, cette obligation ne concerne que les opérateurs.

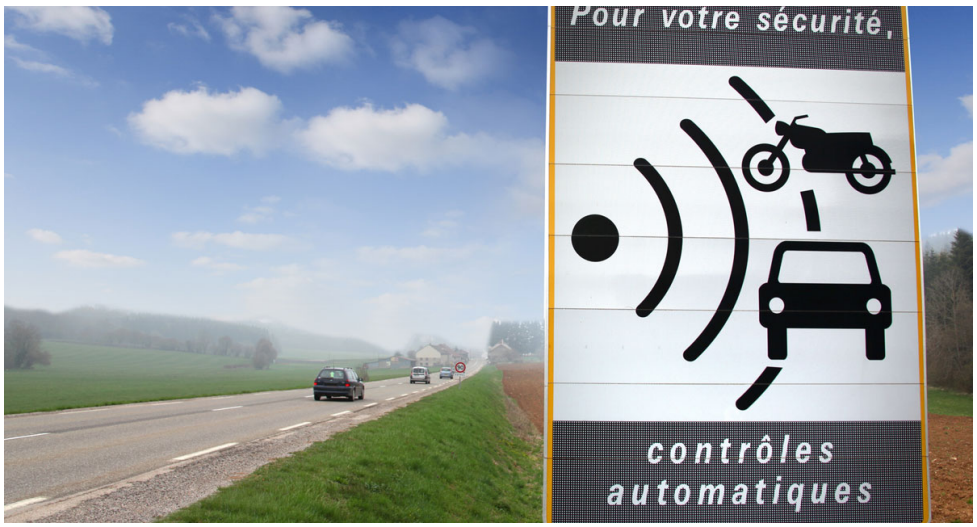
Le moment est d'ailleurs pour celle-ci, le secteur télécom étant notamment le théâtre de lobbyings intenses. Elle a d'ailleursretiré une proposition de « fair use » pour la fin des frais d'itinérance il y a quelques jours, suite à des levées de bouclier du côté des associations de consommateurs, des opérateurs et des eurodéputés. Comme le rappelle Reuters, ce texte passera entre les mains du Parlement et du Conseil de l'Europe, avec des changements possibles à la clé…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : L’UE préparerait l’extension de règles de sécurité des opérateurs aux acteurs du Net

---

Est-ce que la cour de cassation a finalement jugé illégal le signalement des radars par Facebook ?



Est-ce que la cour de cassation a finalement jugé illégal le signalement des radars par Facebook ?

La cour de cassation a jugé que les pages Facebook sur lesquels les internautes s'informent de la localisation de contrôles de police sur les routes ne sont pas illégales au regard de l'état actuel du code pénal, qui interdit les avertisseurs radars.

Le fait d'utiliser un réseau social comme Facebook pour prévenir ses amis ou d'autres internautes de la géolocalisation de contrôles routiers et de radars automatiques n'est pas une violation de la loi pénale, a tranché cette semaine la cour de cassation, dont l'arrêt est cité par Le Figaro.

La haute juridiction s'était penchée sur la question à la demande du parquet de Montpellier, qui s'était pourvu en cassation après la décision de la cour d'appel de Montpellier de relaxer des individus qui avaient créé une page Facebook intitulée « *le groupe qui te dit où est la police en Aveyron* ».

Alors que la douzaine d'internautes avait été condamnée en première instance en décembre 2014, au motif que l'utilisation d'un tel groupe Facebook violerait le code de la route qui interdit les avertisseurs de radars depuis 2012, la cour de Montpellier avait adopté une lecture plus littérale de l'article R413-15 du code de la route, pour estimer que ça n'était pas la même chose.

UN RÉSEAU SOCIAL N'EST PAS UN DISPOSITIF D'AVERTISSEUR RADAR

Cet article interdit les « *dispositifs ou produits visant à avertir ou informer de la localisation d'appareils, instruments ou systèmes servant à la constatation des infractions à la législation ou à la réglementation de la circulation routière* ». Toute la question était de savoir si un groupe Facebook, ou équivalent, pouvait être assimilé à un « *dispositif visant à avertir ou informer de la localisation* » de contrôles de sécurité routière.

.La cour de cassation apporte une réponse claire puisqu'elle indique que « *l'utilisation d'un réseau social, tel Facebook, sur lequel les internautes inscrits échangent des informations, depuis un ordinateur ou un téléphone mobile, ne peut être considérée comme l'usage d'un dispositif de nature à se soustraire à la constatation des infractions relatives à la circulation routière incriminée par l'article R.413-15 du code de la route* ».

Peu importe, au final, que les internautes en question aient utilisé des messages cryptiques pour se faire comprendre (du genre « les poulets cuisent au soleil à 500 mètres du rond point »). Même s'ils avaient communiqué de façon très explicite, la loi ne l'interdit pas, au grand dam de la gendarmerie qui doit de temps en temps rappeler que signaler des contrôles routiers, c'est aussi aider des personnes recherchées qui peuvent être appréhendées par ce biais.

Nul doute, dès lors, que des propositions visant à compléter la loi devraient parvenir sur nos écrans dans les prochaines semaines ou les prochains mois.

Article de Guillaume Champeau

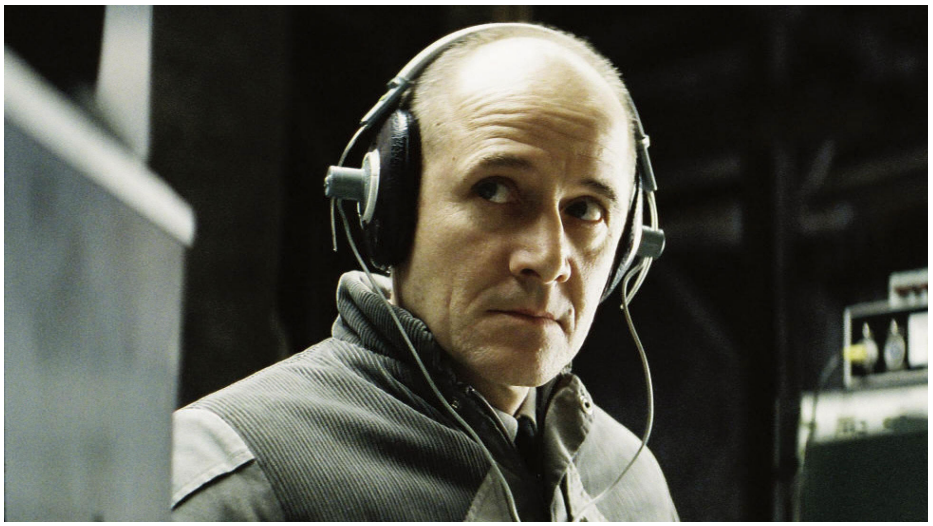
Réagissez à cet article

Original de l'article mis en page : Signaler des radars avec

Facebook ? La cour de cassation juge que c’est légal – Politique – Numerama

---

Collectes massives et illégales par le Renseignement allemand

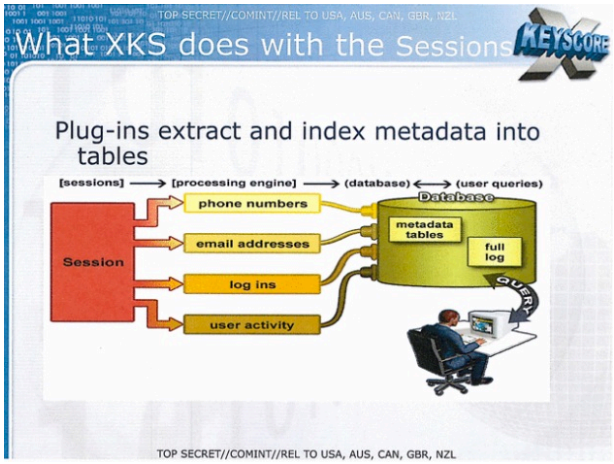


Collectes massives et illégales par le Renseignement allemand

---

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]

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