

# Au Royaume-Uni, une loi de surveillance aussi extrême qu'effrayante vient d'être votée

 **Au Royaume-Uni, une loi de surveillance aussi extrême qu'effrayante vient d'être votée**

Le Royaume-Uni pourrait bien voir appliquer l'une des lois les plus extrêmes en matière de surveillance de ses concitoyens. Celle-ci, déjà baptisée la Charte des fouineurs, autoriserait l'État à fouiller quand il le souhaite, dans chaque élément de votre vie numérique....[Lire la suite ]

---

Denis JACOPINI Expert en cybercriminalité et en protection des données personnelles réalise des audits sécurité, vous explique comment vous protéger des pirates informatiques et vous aide à vous mettre en conformité avec le règlement Européen sur la protection des données personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84). Plus d'informations sur sur cette page.

---



Réagissez à cet article

---

# Au Royaume-Uni, une loi de surveillance aussi extrême qu'effrayante vient d'être votée

 **Au Royaume-Uni, une loi de surveillance aussi extrême qu'effrayante vient d'être votée**

Le Royaume-Uni pourrait bien voir appliquer l'une des lois les plus extrêmes en matière de surveillance de ses concitoyens. Celle-ci, déjà baptisée la Charte des fouineurs, autoriserait l'État à fouiller quand il le souhaite, dans chaque élément de votre vie numérique....[Lire la suite ]

---

Denis JACOPINI Expert en cybercriminalité et en protection des données personnelles réalise des audits sécurité, vous explique comment vous protéger des pirates informatiques et vous aide à vous mettre en conformité avec le règlement Européen sur la protection des données personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).  
Plus d'informations sur sur cette page.



Réagissez à cet article

---

# Au Royaume-Uni, une loi de surveillance aussi extrême qu'effrayante vient d'être votée

 **Au Royaume-Uni, une loi de surveillance aussi extrême qu'effrayante vient d'être votée**

Le Royaume-Uni pourrait bien voir appliquer l'une des lois les plus extrêmes en matière de surveillance de ses concitoyens. Celle-ci, déjà baptisée la Charte des fouineurs, autoriserait l'État à fouiller quand il le souhaite, dans chaque élément de votre vie numérique....[Lire la suite ]

---

Denis JACOPINI Expert en cybercriminalité et en protection des données personnelles réalise des audits sécurité, vous explique comment vous protéger des pirates informatiques et vous aide à vous mettre en conformité avec le règlement Européen sur la protection des données personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).  
Plus d'informations sur sur cette page.



Réagissez à cet article

---

# Au Royaume-Uni, une loi de surveillance aussi extrême qu'effrayante vient d'être votée

 Au Royaume-Uni, une loi de surveillance aussi extrême qu'effrayante vient d'être votée

Le Royaume-Uni pourrait bien voir appliquer l'une des lois les plus extrêmes en matière de surveillance de ses concitoyens. Celle-ci, déjà baptisée la Charte des fouineurs, autoriserait l'État à fouiller quand il le souhaite, dans chaque élément de votre vie numérique....[Lire la suite ]

---

Denis JACOPINI Expert en cybercriminalité et en protection des données personnelles réalise des audits sécurité, vous explique comment vous protéger des pirates informatiques et vous aide à vous mettre en conformité avec le règlement Européen sur la protection des données personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).  
Plus d'informations sur sur cette page.



Réagissez à cet article

---

# Sednit : dissection d'un groupe de cyber-espions

✖	<b>Sednit : dissection d'un groupe de cyber-espions</b>
---	---

---

**Les chercheurs ESET annoncent la publication d'un vaste document de recherche en 3 parties « En route with Sednit ». L'observation de l'utilisation simultanée d'un bootkit et d'un rootkit par les cybercriminels a permis d'analyser leurs cibles et méthodes.**

Ce groupe aussi connu sous le nom d'APT28, Fancy Bear ou Sofacy, agit depuis 2004. Son principal objectif **est le vol d'informations confidentielles de cibles spécifiques :**

- **Partie 1 :** « En route with Sednit : Approaching the Target » se concentre sur la cible des campagnes de phishing, les méthodes d'attaque utilisées ainsi que la première phase de l'attaque utilisant le malware SEDUPLOADER, composé d'un compte à rebours et d'une charge utile associée.

- **Partie 2 :** « En route with Sednit : Observing the comings and goings » couvre les activités de Sednit depuis 2014 et détaille la boîte à outils d'espionnage utilisée pour la surveillance à long terme des ordinateurs compromis. Cela est rendu possible grâce à deux backdoor SEDRECO et XAGENT, ainsi qu'à l'outil réseau XTUNNEL.

- **Partie 3 :** « En route with Sednit : a mysterious downloader » décrit le logiciel permettant la première phase de l'attaque DOWNDHELPH qui selon nos données de télémétrie n'aurait servi que 7 fois. A noter que certains de ces déploiements ont requis des méthodes de « persistance avancées » : Windows bootkit et Windows rootkit.

« L'intérêt d'ESET pour ces activités malveillantes est née de la détection d'un nombre impressionnant de logiciels personnalisés déployés par le groupe Sednit au cours des deux dernières années », déclare Alexis Dorais-Joncas, Security Intelligence team lead chez ESET et dédié à l'exploration des activités du groupe Sednit. « L'arsenal de Sednit est en constante évolution. Le groupe déploie régulièrement des logiciels et techniques de pointe, tandis que leur malware phare a également évolué de manière significative au cours des dernières années ».

Selon les chercheurs ESET, les données collectées à partir des campagnes de phishing menées par Sednit montrent que plus de **1.000 profils d'individus hauts-placés impliqués dans la politique d'Europe de l'EST ont été attaqués.** « Contrairement aux autres groupes d'espionnage, le groupe Sednit a développé son propre « exploit kit » et utilisé un nombre étonnamment important d'exploits 0-day», conclut Alexis Dorais-Joncas.

Les activités du groupe cybercriminel de ces dernières années envers les personnalités hauts-placées, ont suscité l'intérêt de nombreux chercheurs. **Le document réalisé par les experts ESET fournit une description technique accessible et contenant les indicateurs de compromission (IOCs), à destination des chercheurs et des entreprises afin de vérifier qu'ils n'ont pas été compromis par le groupe Sednit.**

La première partie de cette recherche est disponible sur WeLiveSecurity, l'intégralité l'étant sur le Github ESET.

---

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

Plus [d'informations](https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles) sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Original de l'article mis en page : Boîte de réception (2) –

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

	<b>Même le FBI vous recommande très fortement de faire cela sur votre ordinateur !! Suivez leurs conseils !</b>
---	---

---

**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 avons 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>



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 !

---



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

<input type="checkbox"/>	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'ailleurs retiré 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]

---

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>



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

---

# Piratage de l'électricité, de l'eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie

✕	Piratage de l'électricité, de l'eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie
---	---

---

On ne cesse de vous le répéter, il est très important de rester au courant des dernières actualités concernant la cybersécurité et ses menaces. Mieux vaut prévenir que guérir.

Cependant, même ceux qui connaissent tout en matière de cybersécurité, qui utilisent des mots de passe fiables et qui les changent régulièrement, qui reconnaissent des messages d'hameçonnage au premier coup d'œil et qui protègent leurs dispositifs avec une excellente solution de sécurité, même ceux qui font *tout*, ne sont pas totalement à l'abri. Tout simplement parce que nous vivons en société.

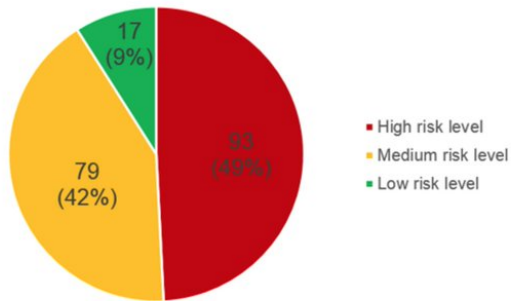


Le problème est que nous avons le contrôle sur nos objets personnels, mais pas sur celui des équipements industriels, qui est loin de notre portée.

#### Vous avez dit cybersécurité ?

Nos experts en cybersécurité ont mené une étude afin de découvrir où nous en sommes concernant la sécurité des systèmes de contrôle industriel.

Shodan, le moteur de recherche pour les dispositifs connectés, nous a montré que 188 019 systèmes industriels dans 170 pays sont accessibles sur Internet. La majorité d'entre eux sont localisés aux Etats-Unis (30,5%) et en Europe, essentiellement en Allemagne (13,9%), Espagne (5,9%) et en France (5,6%).



ICS vulnerabilities in 2015 by risk level (CVSS v.2 and CVSS v.3)

92% (172 982) des systèmes de contrôle industriel (SCI) détectés sont vulnérables. Lamentablement, 87% ont un niveau de risque moyen de bugs et 7% connaissent des problèmes critiques.

Ces cinq dernières années, les experts ont méticuleusement examiné de tels systèmes et y ont découvert de nombreuses failles de sécurité. Durant ce laps de temps, le nombre de vulnérabilités dans les composants SCI a multiplié par dix.

Parmi les systèmes que nos experts ont analysés, 91,6% ont utilisé des protocoles non sécurisés, en donnant l'opportunité aux cybercriminels d'intercepter ou de modifier les données utilisant des attaques de l'homme du milieu.

Egalement, 7,2% (environ 13 700) des systèmes appartiennent à de grandes compagnies aéronautiques, des transports et de l'énergie, pétrolières et gazières, métallurgiques, de l'industrie alimentaire, de la construction et autres secteurs primordiaux.



En d'autres termes, des hackers qualifiés peuvent influencer n'importe quel secteur économique. Leurs victimes (les entreprises piratées) porteraient préjudice à des milliers ou millions de personnes en leur fournissant de l'eau contaminée ou de la nourriture immangeable, ou en leur coupant le chauffage en plein hiver.

#### Qu'est-ce que cela implique pour nous tous ?

...[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>



Réagissez à cet article

Original de l'article mis en page : Piratage de l'électricité, de l'eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie. | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.

---

# Collectes massives et illégalles par le Renseignement allemand

 Collectes massives et illégalles 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]

---

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

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

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



Réagissez à cet article

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

---

# 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 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.

## 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]

---

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

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

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



Réagissez à cet article

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