

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. Connue 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 chèquiers 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]

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.



[Contactez-nous](#)

Réagissez à cet article

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

Est-ce qu'un lien vers un contenu illégal est lui aussi illégal ?



Est-ce
qu'un
lien
vers un
contenu
illégal
est lui
aussi
illégal
?

Le fait de publier un lien renvoyant vers un contenu illicite est lui-même constitutif de contrefaçon ? À cette éminente question, la Cour de justice de l'Union européenne vient de répondre que non, sous deux importantes réserves : que le lien litigieux ait été diffusé sans but lucratif et que son auteur n'ait pas eu connaissance de son illicéité.

C'est suite à une saisine de la Cour de cassation des Pays-Bas que la justice européenne a rendu son arrêt de ce jour. Au cœur de ce dossier, un vrai jeu du chat et de la souris. Une dizaine de photos d'une présentatrice hollandaise furent hébergées sur FileFactory, puis « linkées » sur Geenstijl.nl, important site néerlandais. Le renvoi vers ces images, destinées à être publiées dans l'édition nationale de Playboy, avait rapidement provoqué la colère de la revue de charme. Sauf que même après avoir réussi à obtenir leur retrait de FileFactory, de nouveaux liens furent établis par Geenstijl.nl, cette fois via ImageShack.us notamment...

D'où la question : publier des liens vers ces images signalées comme manifestement illicites constituait-il un nouvel « acte de communication » d'une œuvre au public au sens de la directive européenne relative au droit d'auteur – dès lors soumis à l'autorisation obligatoire (et préalable) des ayants droit ? Pour la CJUE, la réponse est oui...[lire la suite]

L'arrêt de la CJUE (PDF)

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.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : La CJUE juge qu'un lien

vers un contenu illégal peut être illégal

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

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.



[Contactez-nous](#)

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

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 connaît 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](https://www.metro.co.uk)

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>



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

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



Le Net Expert
INFORMATIQUE
Conseil et accompagnement en
Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

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

Alerte : Un canular sur Facebook qui diffuse de fausses informations terroristes



Les chercheurs ESET ont découvert une arnaque qui cible les utilisateurs de Facebook. D'abord répandu en République Tchèque et en Slovaquie, elle pourrait se propager dans d'autres pays

Les utilisateurs de Facebook en République Tchèque et en Slovaquie font face à une vague de fausses informations sur une attaque meurtrière à Prague. Quand l'utilisateur clique sur le canular, il est redirigé vers une page Internet de phishing qui essaye de le tromper en l'incitant à partager ses identifiants Facebook.

« D'après ce que nous savons à propos de cette campagne, l'attaque pourrait se propager dans plusieurs autres pays » met en garde Lukáš Štefanko, Malware Researcher chez ESET.

Cette prétendue attaque terroriste est facile à discréditer car la photo publiée ne ressemble pas à Prague, ni à aucune autre ville d'Europe. Malgré cela, l'arnaque se diffuse rapidement. « Les utilisateurs de Facebook partagent fréquemment des histoires sans les avoir lues. Les campagnes d'arnaques, si elles font appel à l'émotion, réussissent étonnamment bien à cause de notre empathie naturelle » commente Lukáš Štefanko.

Peu après le lancement de la campagne, Facebook a commencé à stopper les pages de phishing utilisées dans cette campagne. Les solutions de sécurité ESET sont conçues pour bloquer les pages Internet de phishing liées à ce type d'escroquerie ainsi que d'autres domaines enregistrés par cette même personne.



« Au cours des dernières semaines, il y a eu 84 domaines enregistrés par la même personne. La plupart d'entre eux possède une fonction de phishing, tandis que d'autres pourraient être utilisées à l'avenir lors d'une attaque à plus grande échelle » ajoute Lukáš Štefanko.

Voici les recommandations des experts ESET pour ceux qui pensent avoir été escroqué en partageant leurs identifiants Facebook :

- Changez votre mot de passe Facebook et utilisez les deux facteurs d'authentification fournis par Facebook
- Si vous avez utilisé le même mot de passe pour plusieurs services, changez-le partout – et mettez un terme à cette pratique très dangereuse.

Denis JACOPINI vous recommande les outils de protection suivants :



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

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



Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Boîte de réception –
denis.jacopini@gmail.com – Gmail

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



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, contenus, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

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

Comment se prémunir de la

**cybercriminalité, ce risque
sur Internet pour les
particuliers et les
professionnels ?**

	Comment se prémunir de la cybercriminalité, ce risque sur Internet pour les particuliers et les professionnels ?
---	--

La police recommande, de nombreuses attaques ciblent les particuliers mais aussi les entreprises et les administrations. Elles visent à obtenir des informations personnelles afin de les exploiter ou de les revendre (données bancaires, identifiants de connexion à des sites marchands, etc.). **hameçonnage (phishing)** et **«rançongiciel» (ransomware)** sont des exemples connus d'actes malveillants portant préjudice aux internautes.

Pour s'en prémunir, des réflexes sages s'imposent.

QUELS SONT LES DIFFÉRENTS TYPES D'ATTAQUES ?

Attaque par hameçonnage (phishing)

Le hameçonnage, phishing en l'anglais, est une technique malveillante très courante sur Internet. L'objectif : opérer une usurpation d'identité afin d'obtenir des renseignements personnels et des identifiants bancaires pour en faire un usage criminel.

1. Le cybercriminel se « déguise » en un tiers de confiance (banque, administration, fournisseur d'accès à Internet...) et diffuse un mail frauduleux, ou contamine une pièce jointe piégée, à une large liste de contacts. Le mail invite les destinataires à mettre à jour leurs informations personnelles (et souvent bancaires) sur un site internet falsifié vers lequel ils sont redirigés.

2. Le site comprend un nombre et important de contacts et augmente les chances que l'un des destinataires se sente concerné par le message diffusé.

3. De ce site, il est redirigé vers le site falsifié qui va recueillir l'ensemble des informations qu'il recueille.

4. Les informations sont alors mises à disposition du cybercriminel qui n'a plus qu'à faire usage des identifiants, mots de passe ou données bancaires récupérées.

Voici la vidéo de la Blockchain sur le phishing (CCDF – partenaire ANSSI)

Pour s'en prémunir :

- N'avez pas une confiance aveugle dans le nom de l'expéditeur de l'e-mail. Au moindre doute, n'hésitez pas à contacter l'expéditeur par un autre biais.
- Méfiez-vous des pièces jointes, elles pourraient être contaminées. Au moindre doute, n'hésitez pas à contacter l'expéditeur pour en connaître la teneur.
- Ne répondez jamais à une demande d'informations confidentielles par mail.
- Pensez votre accès au-dessus des liens, faites attention aux caractères accablés dans la liste ainsi qu'à la qualité du français ou de la langue pratiquée par votre interlocuteur (ex : orthographe).

Pour aller plus loin, n'hésitez pas à consulter la page sur les conseils aux usagers qui reprend les bonnes pratiques à mettre en place pour sécuriser ses équipements et ses données.

Attaque par «rançongiciel» (ransomware)

Les rançongiciels sont des programmes informatiques malveillants de plus en plus répandus (ex : Locky, TeslaCrypt, Cryptolocker, etc.). L'objectif : chiffrer des données puis demander à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.

1. Le cybercriminel diffuse un mail qui contient des pièces jointes et / ou des liens piégés. Le corps du message contient un message correctement rédigé, parfois en français, qui demande de payer rapidement une facture par exemple.

2. De ce site, le logiciel est téléchargé sur l'ordinateur et commence à chiffrer les données personnelles : les documents bureautiques (doc, xls, pdf, etc.), les photos, les vidéos, les vidéos, etc.

3. Les fichiers données indisponibles, un message s'affiche pour exhorter le versement d'une rançon, payable en bitcoins ou via une carte prépayée, en échange de la clé de déchiffrement. Attention, rien n'indique que le déchiffreur en question soit efficace !

Pour s'en prémunir :

- N'avez pas une confiance aveugle dans le nom de l'expéditeur de l'e-mail. Au moindre doute, n'hésitez pas à contacter l'expéditeur par un autre biais.
- Méfiez-vous des pièces jointes et des liens dans les messages dont la provenance est douteuse. Au moindre doute, n'hésitez pas à contacter l'expéditeur pour en connaître la teneur.
- Effectuez des sauvegardes régulièrement sur des périphériques externes.
- Mettez à jour régulièrement tous vos principaux logiciels en privilégiant leur mise à jour automatique.

Pour aller plus loin, n'hésitez pas à consulter la page sur les conseils aux usagers qui reprend les bonnes pratiques à mettre en place pour sécuriser ses équipements et ses données.

VOUS ÊTES VICTIME D'UN RANSOMWARE OU DE FISHING ?

Suite à une intrusion de site cyberattaque, déposez plainte auprès d'un service de **Police nationale** ou de **Gendarmerie nationale** ou bien adressez un courrier au Procureur de la République auprès du Tribunal de Grande Instance compétent.

Maintenez-vous de tous les renseignements suivants :

- Références de la loi des transferts d'argent effectués
- Références de la loi des personnes contactées : adresse de messagerie ou adresse postale, pseudos utilisés, numéros de téléphone, fax, copie des courriels ou courriers échangés.
- Numéro compte de votre carte bancaire après avoir eu paiement : référence de votre banque et de votre compte, et copie du relevé de compte bancaire ou appareil le débit frauduleux
- Tout autre renseignement pouvant aider à l'identification de l'auteur

Une plainte déposé auprès de la police ou de la gendarmerie nationale vous sera adressée la plateforme de signalement « Paris » ou le numéro dédié : 02 47 82 17.

Des services spécialisés se chargent ensuite de l'enquête :

- **Police nationale** : l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) qui dépend de la Sous-direction de lutte contre la cybercriminalité (SDCL) : 02 47 84 97 33
- **Gendarmerie nationale** : le centre de lutte contre les criminalités numériques (CLCN) du Service Central de Renseignement Criminel (SCRC) cybergendarmerie.interieur.gouv.fr
- **Préfecture de police** : la Préfecture de police de Paris, de la Direction centrale du renseignement intérieur (DCRI) et des Equipes de la Brigade d'enquête sur les Fraudes aux technologies de l'information (BEFTI) compétente uniquement pour Paris et petite couronne (75, 92, 93 et 94) : 01 40 70 07 50

Article original de gouvernement.fr

Original de l'article mis en page : Cybercriminalité | Gouvernement.fr

Alerte : Twitter pour Android infecté par un Cheval de Troie



Alerte :
Twitter pour Android
infecté par
un Cheval de
Troie

ESET découvre le premier botnet sous Android qui contrôle Twitter

Les chercheurs ESET ont découvert une porte dérobée sous Android qui contient un Cheval de Troie et qui est contrôlée par des tweets. Détecté par ESET comme étant Android/Twittoor, **il s'agit de la première application malveillante utilisant Twitter** au lieu d'une commande et d'un contrôle traditionnel de serveur (C&C).

Après son lancement, le Cheval de Troie cache sa présence sur le système et vérifie le compte Twitter défini par intervalle régulier pour les commandes. Sur la base des commandes reçues, il peut soit télécharger des applications malveillantes, soit basculer le serveur C&C d'un compte Twitter à un autre.

« L'utilisation de Twitter pour contrôler un botnet est une étape innovante pour une plateforme Android », explique Lukáš Štefanko, malware researcher chez ESET et qui a découvert cette application malicieuse.

Selon Lukáš Štefanko, les canaux de communication basés sur des réseaux sociaux sont difficiles à découvrir et impossible à bloquer entièrement – alors qu'il est extrêmement facile pour les escrocs de rediriger les communications vers un autre compte de façon simultanée.

Twitter a d'abord été utilisé pour contrôler les botnets de Windows en 2009. « En ce qui concerne l'espace Android, ce moyen de dissimulation est resté inexploité jusqu'à présent. Cependant, nous pouvons nous attendre à l'avenir à ce que les cybercriminels essayent de faire usage des statuts de Facebook ou de déployer leurs attaques sur LinkedIn et autres réseaux sociaux », prévoit Lukáš Štefanko.

Android/Twittoor est actif depuis juillet 2016. Il ne peut pas être trouvé sur l'un des app store officiels d'Android (selon Lukáš Štefanko) mais il est probable qu'il se propage par SMS ou via des URL malveillantes. Il prend l'apparence d'une application mobile pour adulte ou d'une application MMS mais sans fonctionnalité. Plusieurs versions de services bancaires mobiles infectés par un malware ont été téléchargées. Cependant, les opérateurs de botnet peuvent commencer à distribuer d'autres logiciels malveillants à tout moment, y compris des ransomwares selon Lukáš Štefanko.

Twittoor est le parfait exemple de l'innovation des cybercriminels pour leur business. Les utilisateurs d'Internet devraient continuer à protéger leurs activités avec de bonnes solutions de sécurité valables pour les ordinateurs et les appareils mobiles », conclut Lukáš Štefanko.

Source : ESET

Pour protéger vos équipements, nous recommandons l'application suivante :



Anti-Phishing
Filtrage des appels et SMS
Antivol
Localisation GPS

PROTEGEZ LES MOBILES

Cliquez ici



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

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

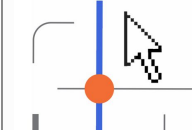


[Contactez-nous](#)

Réagissez à cet article

15 millions de comptes

Telegram d'Iraniens piratés

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 LE NET EXPERT AUDITS & EXPERTISES	 LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES	 LE NET EXPERT RGPD CYBER MISES EN CONFORMITE	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
		15 millions de comptes Telegram d'Iraniens piratés			

Une ancienne faille non corrigée dans Telegram aurait permis de mettre la main sur des millions d'informations d'utilisateurs Iraniens.

Des chercheurs en sécurité informatique ont annoncé à l'agence de presse Reuters que l'application Telegram avait subi une attaque informatique qui a donné l'occasion aux malveillants de mettre la main sur 15 millions de données d'utilisateurs Iraniens.

Pour rappel, Telegram a été fondé en 2013 par le Russe Pavel Durov. Cet outil de messagerie permet de rendre « illisible » des communications entre personnes autorisées (sauf si groupe publique). Pour cela, les communications sont chiffrées. Dans les options de l'application : chiffrer les messages, auto destruction des textes...

Collin Anderson et Claudio Guarnieri, les deux chercheurs travaillent entre autres pour Amnesty International, ont expliqué que la vulnérabilité est exploitable via son utilisation des SMS. Une faille qui avait pourtant été révélée en 2013 par Karsten Nohl. Selon les deux chercheurs, les utilisateurs Iraniens ont été touchés par une infiltration qui a peut-être permis à des « espions » de mettre la main sur les informations de 15 millions d'utilisateurs de ce pays.

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

[Les 10 conseils pour ne pas se faire « hacker » pendant l'été](#)

[Les meilleurs conseils pour choisir vos mots de passe](#)

[Victime d'un piratage informatique, quelles sont les bonnes pratiques ?](#)

[Victime d'usurpation d'identité sur facebook, tweeter ?](#)

[Portez plainte mais d'après quel article de loi ?](#)

[Attaques informatiques : comment les repérer ?](#)

[block id="24760" title="Pied de page BAS"]

Original de l'article mis en page : Piratage de comptes

L'ANSSI alerte sur les risques liés à Pokémon Go

	L'ANSSI alerte sur les risques liés à Pokémon Go
---	--

Face au phénomène Pokémon Go, l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'information) a publié un bulletin de sécurité sur l'installation et l'usage de cette application.

Devant l'ampleur du phénomène (près de 100 millions de téléchargements), l'application Pokémon Go pose quelques problèmes de sécurité. L'ANSSI (en quelque sorte le Gardien de la sécurité des Systèmes d'Information des Organisme d'Importance Vitale, des Organes et Entreprise de l'état Français selon Denis JACOPINI expert Informatique assermenté spécialisé en cybercriminalité) ne pouvait pas rester sourde à cette question et vient de publier via le CERT-FR un bulletin de sécurité dédié aux « *cyber-risques liés à l'installation et l'usage de l'application Pokémon Go* ».

Applications malveillantes et collectes de données

Dans ce bulletin, il est rappelé qu'avec le succès, de nombreuses fausses applications se sont créées. Le CERT-FR en a recensé 215 au 15 juillet 2016. Elles sont surtout présentes dans les pays où le jeu n'est pas présent. Il recommande donc de ne pas télécharger cette application sur des sites tiers, et de n'installer que les versions originales disponibles sur Google Play ou l'Apple Store. Nous nous étions fait l'écho de la disponibilité d'APK Pokémon Go pour Android qui contenait des malwares. Le bulletin constate aussi que Niantic a résolu le problème de permission qui exigeait un accès complet au profil Google de l'utilisateur.

Sur les données personnelles, l'ANSSI observe comme beaucoup d'autres organisations que Pokémon Go collecte en permanence de nombreuses données personnelles. Informations d'identité liées à un compte Google, position du joueur par GPS, etc. L'UFC-Que Choisir avait récemment alerté sur cette question de la collecte des données. La semaine dernière la CNIL a publié un document concernant « jeux sur votre smartphone, quand c'est gratuit... » où elle constatait que ce type d'application était très gourmande en données. L'ANSSI préconise la désactivation du mode « réalité augmentée » lors de la phase de capture d'un Pokémon.

BYOD et Pokémon Go, le pouvoir de dire non

L'ANSSI répond sur le lien qu'il peut y avoir entre le BYOD (Bring Your Own Device), c'est-à-dire l'utilisation de son terminal personnel dans un cadre professionnel et Pokémon Go. Le CERT-FR constate qu'il est « *tendant d'utiliser un ordiphone professionnel pour augmenter les chances de capturer un Ronflex (un Pokémon rare à trouver)* ». Surtout quand la demande émane d'un VIP et qu'il est souvent difficile de refuser. Eh bien comme Patrick Pailloux (prédécesseur de Guillaume Poupard à la tête de l'ANSSI) l'avait dit en son temps, il faut avoir le pouvoir de dire non à l'installation de ce type d'application dans un environnement professionnel.

Toujours dans le cadre du travail, l'agence déconseille l'usage de l'application dans des lieux où le geo-tagging du joueur pourrait avoir des conséquences (lieu de travail, sites sensibles).

Article original de Jacques Cheminat



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

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



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : L'ANSSI alerte sur les
risques liés à Pokémon Go