#PokemonGo hacké en moins de 2h…

	#PokemonGo hacké en moins de 2h…

Suricate Concept, un GIE (Groupement d'Intérêt Economique) spécialisé dans la cyber-sécurité, a publié un rapport de 10 pages sur des failles de sécurité majeures identifiées dans le nouveau phénomène de société « Pokemon Go », après avoir réussi à pirater le jeu en un temps record.

L'étude intitulée « Comment on a hacké Pokemon Go en moins de 2h… » explique en détails comment l'équipe d'experts en cyber-sécurité s'est penché par hasard sur l'application et a rapidement identifié des failles qui permettaient aux joueurs de gagner des niveaux sans efforts en manipulant le programme.

Monir Morouche, à la tête du département cyber-sécurité et Président du GIE Suricate Concept a déclaré : « Chez Suricate Concept, tous les jours nous nous battons pour rendre le web un endroit plus sur et pour protéger les données et la vie privée des utilisateurs ainsi que les ressources en ligne de nos clients. Lorsque l'on a découvert Pokemon Go, complètement par hasard, on voulait savoir si le programme avait été suffisamment sécurisé par ses développeurs et si nous serions capable de trouver des failles dans l'application « .

Ce qui débuta comme un challenge interne au détour d'une pause de travail devint rapidement la base pour une étude plus poussée lorsque l'équipe réalise comment ils parvenaient facilement à manipuler le programme, générant ainsi des gains de niveaux et de ressources rapides pour un joueur à qui il faudrait normalement plusieurs semaines d'efforts pour y parvenir.

« Au sein de l'équipe, nous sommes toujours en train de nous challenger les uns les autres lorsque que quelque chose de nouveau dans l'univers du web ou des nouvelles technologies apparait. Pokemon Go était un sujet d'étude rêvé, du fait qu'il était présent partout dans l'actualité. Nous ne pouvions pas passer à côté. Dans toutes les démonstrations de hacking que nous conduisons, l'objectif premier est de sensibiliser les utilisateurs aux risques encourus et les éduquer sur comment être un utilisateur du web responsable », poursuit Monir Morouche.

L'étude publiée par Suricate Concept inclut une analyse technique de la façon dont l'équipe a procédé au hack en contournant les systèmes de sécurité existant du jeu, sans pour autant dévoiler tous les détails, qui « seront mis à disposition des développeurs de Pokemon Go sur demande » a indiqué Monir Morouche. Cela afin de que ces derniers ne soient pas utilisés à mauvais escient par des joueurs ou hackers mal intentionnés. Il ne s'agit pas du premier coup d'essai de la team Suricate Concept qui régulièrement au travers de démonstrations choc met en avant des failles de sécurité dans des services en ligne, ou objets connectés utilisés quotidiennement par le public. On peut par exemple citer parmi leurs récents travaux le hacking du moteur de recherche Google ou celui des cartes de paiement sans contact.

Suricate Concept a également annoncé il y a quelques mois lors du dernier Forum International de la Cyber-sécurité avoir réussi à hacker un objet médical connecté , un pace-maker, afin d'en prendre le contrôle complet. La démonstration a été dévoilée dans une vidéo avec un scénario d'inspiration hollywoodienne intitulée « The hacking dead » , en rapport avec la série à succès The Walking Dead.

Article original de

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 : Lille, 28 Juillet 2016 – Communiqué de presse: « Comment on a hacké PokemonGo en moins de 2h… » | Farouk JEBALI | LinkedIn

---

L'arnaqueur Chinaper Chinapa roi de l'escroquerie sur Internet enfin arrêté

L'escroc présentaient ses chaussures magiques d'où sortaient des billets de banque !

L'arnaqueur Chinaper Chinapa roi de l'escroquerie sur Internet enfin arrêté

Il se nomme Chinaper Chinapa, un arnaqueur de Côte d'Ivoire qui vient d'être arrêté. Il arnaquait des hommes et des femmes sur Internet.

Les scammeurs, les brouteurs, bref les escrocs qui s'attaquent aux internautes sont légions sur la toile. Ils usent de multiples arnaques pour soutirer de l'argent à leurs victimes. Ils jouent ensuite les « rois » dans leur quartier. Parmi les pièges usités : l'arnaque à l'amour, le wash-wash, la création de billets, le faux mail d'inquiétude d'un proche perdu, la fausse location ou loterie… Pour Chinaper Chinapa, chaussures et portes feuilles magiques en bonus ! Je possède une liste d'une quarantaine d'arnaques possibles mises en place par les brouteurs.

Chinaper Chinapa le chenapant !

L'un des « rois » des brouteurs se nommait Chinape Chinapa. L'amateur de casquettes et baskets « bling-bling » se faisait passer pour un « magicien ». Il affirmait être capable de faire sortir des billets de chaussures, de boite magique. Il avait aussi mis en place des arnaques amoureuses, se faisant passer pour des hommes et des femmes à la recherche de l'âme sœur. Il volait les photos sur Facebook et « chassait », ensuite, sur des sites de rencontres.

J'ai pu croiser cet escroc de Chinaper Chinapa, il y a quelques mois, dans son pays (il se baladait aussi beaucoup au Bénin). Ce « roi » des boites de nuit qui sortait les billets de banque plus vite que 007 son Walther PPK.

Mi juin 2016, l'homme avait été tabassé par des personnes qu'il avait escroquées. Quinze jours plus tard, la police lui mettait la main dessus pour une série d'escroqueries. Arrêté par la police début juillet, détail confirmé par le journal Koaci. Le flambeur s'est retrouvé les menottes aux poignets dans son appartement de Cocody. Il est accusé d'activités cybercriminelles et de multiples escroqueries. Pas évident que sa « magie » fonctionne dans la prison d'Abidjan.

Un ami a besoin de vous

15h, un courrier signé d'un de vos amis arrive dans votre boîte mail. Pas de doute, il s'agit bien de lui. C'est son adresse électronique. Sauf que derrière ce message, il y a de forte chance qu'un brouteur a pris la main sur son webmail. Les courriels « piégés » arrivent toujours avec ce type de contenu « ***Je ne veux pas t'importuner. Tu vas bien j'espère, puis-je te demander un service ?***« . Le brouteur, par ce message, accroche sa cible. En cas de réponse de votre part, l'interlocuteur vous sortira plusieurs possibilités liées à sa missive « ***J'ai perdu ma carte bancaire. Je suis coincé en Afrique, peux-tu m'envoyer de l'argent que je te rembourserai à mon retour*** » ; « ***Je voudrais urgemment recharger ma carte afin de pouvoir régler mes frais de déplacement et assurer mon retour. J'aimerais s'il te plaît, que tu me viennes en aide en m'achetant juste 4 coupons de rechargement PCS MASTER CARD de 250 € puis transmets moi les codes RECH de chaque coupon de rechargement, je te rembourserais dès mon retour***« . Je possède plus d'une centaine de variantes d'excuses.

Bien entendu, ne répondez pas, ne versez encore moins d'argent. Attention, selon les brouteurs, des recherches poussées sur leurs victimes peuvent être mises en place. J'ai dernièrement traité le cas d'un brouteur qui connaissait le lieu de résidence du propriétaire du compte webmail que le voyou utilisait. De quoi faire baisser les craintes des amis contactés.

A noter que le scammeur indiquera toujours un besoin de confidentialité dans sa demande : « ***Je souhaite également que tu gardes ce mail pour toi uniquement. Je ne veux pas inquiéter mon entourage. Y'a t'il un buraliste ou un supermarché non loin de toi ?***« .

Remboursement de l'argent volé

Une autre arnaque de brouteurs est intéressante à expliquer. Elle est baptisée « *remboursement*« . Le voleur écrit aux internautes se plaignant, dans les forums par exemple, d'avoir été escroqués. L'idée de l'arnaque est simple : le voleur indique qu'il a été remboursé grâce à un policier spécialisé dans les brouteurs. Le voyou fournit alors une adresse électronique.

Suivre

ZATAZ.COM Officiel @zataz

Prudence à l'adresse « interpol.police.antiarnaque@gmail(.)com » qui n'est pas celle d' #interpol *! L'escroc cherche des personnes escroquées.*

23:12 – 14 Mai 2015

•

•

1111 Retweets

•

55 j'aime

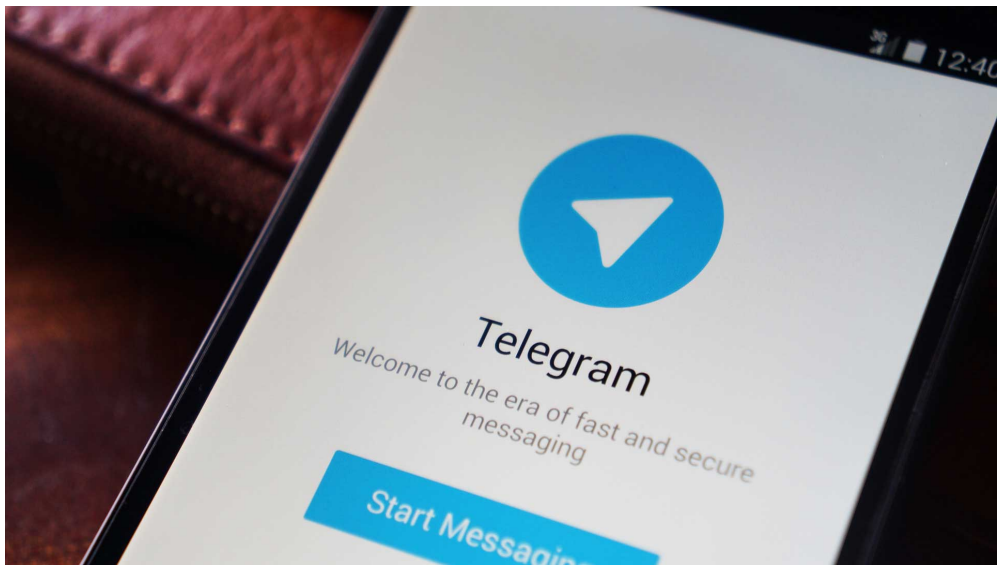
Derrière cette fausse adresse de policier, un autre brouteur. Il va tenter d'escroquer le pigeon déjà pigeonné. Sa mission, se faire envoyer de l'argent via Western Union, MoneyGram. Certains brouteurs sont à la solde de petits commandants locaux qui imposent un quota d'argent à collecter. En 2013, la cyber police de Côté d'Ivoire estimait que les brouteurs avaient pu voler pas moins de ***21 millions d'euros****. N'hésitez pas à me contacter si vous avez croisé la route d'arnaques.*

Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : ZATAZ Brouteur : Chinaper Chinapa roi de l’escroquerie 2.0 – ZATAZ

Attentat dans une église : la messagerie chiffrée Telegram utilisée par un terroriste ? – Politique – Numerama



Attentat dans une église : la messagerie chiffrée Telegram utilisée par un terroriste ?

Selon La Voix du Nord, au moins l'un des deux auteurs de l'attentat de l'église de Saint-Étienne-du-Rouvray utilisait régulièrement la messagerie chiffrée Telegram pour communiquer avec des islamistes, et aurait posté un message une heure avant l'attentat.

Il faut s'attendre à voir très vite renaître le débat sur le chiffrement et l'obligation qui pourrait être faite aux fournisseurs de messageries électroniques de laisser les services de Renseignement accéder aux communications. La Voix du Nord affirme qu'Adel Kermiche, l'un des deux coauteurs de la tuerie de l'église de Saint-Étienne-du-Rouvray, près de Rouen, utilisait la messagerie chiffrée Telegram, à des fins djihadistes. Il aurait envoyé un message sur un canal de discussion une heure avant l'attaque.
« Selon nos informations, Adel Kermiche avait ouvert sur Telegram une « private channel » (haqq-wad-dalil), une chaîne lui permettant de s'adresser à une audience ultra-sélectionnée. Il avait choisi pour nom de code Abu Jayyed al-Hanafi et la photo de Abou Bakr al-Baghdadi, chef suprême de l'État islamique, comme représentation », écrit le quotidien régional.

TÉLÉCHARGER (SIC) CE QUI VA VENIR ET PARTAGER LE EN MASSE ! ! ! !
Selon les membres arabophones de la rédaction de Numerama, haqq-wad-dalil signifierait quelque chose comme « preuve de la vérité » ou « guide de la vérité ».
La Voix du Nord ajoute que « le terroriste correspondait depuis des mois via ce canal avec près de 200 personnes, dont une dizaine de Nordistes », qui étaient d'abord approchés par Facebook. Le matin de l'attentat, le 26 juillet 2016 à 8h30, il aurait envoyé sur ce salon un message qui disait : « Télécharger (sic) ce qui va venir et partager le en masse ! ! ! ! ».
Le quotidien ne dit rien d'un éventuel document qui aurait pu être mis en partage par la suite, ce qui ne laisse la voie qu'à des spéculations. Peut-être Kermiche avait-il prévu de filmer son acte odieux, ou des revendications, et espérait trouver des relais à sa diffusion à travers ses contacts sur Telegram.
Si cette information se confirme ce serait, à notre connaissance, la première fois qu'un lien direct est effectué entre un attentat terroriste en France et l'utilisation de messageries chiffrées.

COMMENT SURVEILLER TELEGRAM ?
La Voix du Nord ne dit pas par quel biais le message aurait été découvert. Il est possible que les enquêteurs aient trouvé ce message en accédant à l'historique Telegram du terroriste, depuis son téléphone mobile qui n'aurait pas été bloqué. Le plus probable est toutefois que l'information provienne d'un autre utilisateur du salon haqq-wad-dalil, puisque le quotidien cite le témoignage de l'un d'entre eux, qui explique que les échanges pouvaient y être « écrits ou oraux mais toujours détruits rapidement ».
Il est connu depuis de très nombreux mois que Telegram, qui dispose de plus de 100 millions d'utilisateurs à travers le monde, est aussi utilisé par des djihadistes qui recherchent la sécurité d'une messagerie chiffrée.
Après avoir refusé d'opérer la moindre censure, en tout en continuant à livrer la moindre information personnelle sur ses utilisateurs, Pavel Durov a fini par décider en novembre 2015 de fermer des salons de discussion liés à l'État islamique, pour mettre fin aux accusations de complicité passive. Il avait appelé les internautes à les signaler pour permettre leur fermeture.
Théoriquement, les canaux de discussion peuvent être infiltrés par les agents des services de renseignement. Reste qu'en l'absence de communication d'informations sur les utilisateurs, il peut être difficile de remonter jusqu'à l'auteur d'un message présentant une menace particulièrement élevée.
Article original de Guillaume Champeau

Original de l'article mis en page : Attentat dans une église : la messagerie chiffrée Telegram utilisée par un terroriste ? — Politique — Numerama

---

Connaissez-vous le réseau plus anonyme et rapide que Tor ?

Connaissez-vous le réseau plus anonyme et rapide que Tor ?

Le Massachusetts Institute of technology (MIT), aux États-Unis, et l'École polytechnique fédérale de Lausanne (EPFL), en Suisse, annoncent la création d'un nouveau réseau anonyme sur Internet, baptisé Riffle, encore plus rapide et sécurisé que Tor, la référence en la matière.

A l'image de Tor, le plus célèbre des réseaux de ce type, Riffle permet de surfer et de communiquer en théorie en parfait anonymat en s'appuyant sur le protocole de chiffrement "en oignon". Cela signifie qu'il est composé d'une multitude de couches de routeurs, autant de "noeuds" par lesquels transitent les flux d'informations sur le réseau, garantissant ainsi l'anonymat de ses utilisateurs. Les données personnelles de l'internaute (adresse IP, pays) ne peuvent ainsi plus être localisées par les sites visités. Cette alternative serait toutefois selon ses créateurs bien plus sécurisée et fiable que Tor et consorts.
Selon le MIT, l'avantage de Riffle repose sur ses serveurs, capables de permuter l'ordre de réception des messages rendant l'analyse du trafic encore plus complexe et favorisant donc l'anonymat des utilisateurs. Si, par exemple, les messages provenant d'expéditeurs Alice, Bob et Carol atteignent le premier serveur dans l'ordre A, B, C, ils peuvent être renvoyés dans un ordre complètement différent au serveur suivant, et ainsi de suite. Les utilisateurs du réseau deviennent alors en théorie parfaitement impossibles à identifier.
Dernier point non négligeable, Riffle proposerait une meilleure bande passante, garantissant une navigation plus fluide et des échanges de fichiers accélérés.
Cette annonce intervient alors que la sécurité de Tor a récemment été mise à mal par des chercheurs de la Northeastern University de Boston (États-Unis) qui a découvert plus d'une centaine de "nœuds-espions", en réalité des serveurs, capables d'identifier des services cachés et éventuellement de les pirater.
Davantage de détails sur Riffle, toujours en phase de développement, seront communiqués lors de sa présentation officielle à la conférence Privacy Enhancing Technologies Symposium (PETS), qui se déroulera du 19 au 22 Juillet à Darmstadt (Allemagne).
Article original de Etienne Froment

Réagissez à cet article

Original de l'article mis en page : Riffle, le nouveau réseau garanti plus anonyme et rapide que Tor | geeko

Jeux Olympiques de Rio : OP Hashtag infiltre des terroristes

	Jeux Olympiques de Rio : OP Hashtag infiltre des terroristes

Op hashtag – La police fédérale Brésilienne aurait infiltré le WhatsApp et Telegram utilisaient par des terroristes locaux. Plusieurs groupes échangeaient des informations sur des tactiques de guerre. Des attentats prévus lors des Jeux Olympiques de Rio ?

Un nouveau cheval de bataille pour la justice brésilienne qui tente de contrôler les réseaux sociaux au Brésil. J'apprends dans le journal brésilien blasting news que La police fédérale brésilienne aurait infiltré le WhatsApp et Telegram de terroristes locaux lors d'une opération baptisée Op Hashtag. Plusieurs personnes s'échangeaient des informations sur des tactiques de guerre. Dans ce nouveau cas, la police fédérale parle clairement de « djihadiste » qui fomentaient des attaques à l'occasion des Jeux Olympique de Rio.

Opération HashTag

L'opération « Hashtag » a été lancée dans la matinée du jeudi 21 juillet. Cette action policière démontre comment la police fédérale aurait réussi à avoir accès aux messages de plusieurs groupes de « terroristes ». Des commanditaires d'attaques en Europe, qui souhaiteraient agir au Brésil.
Alexandre Moraes, le ministre de la Justice, a expliqué que la police tentait de surveiller les conversations WhatsApp. Action difficile puisque tous les messages sont chiffrés « ce qui rend impossible pour quiconque d'avoir accès, y compris à la justice« . Cependant, l'infiltration avec la création de faux comptes d'internautes aurait porté ses fruits. Le ministre a refusé de donner des détails sur la façon dont l'enquête a été menée, mais comme il est impossible de surveiller les messages échangés dans l'application, il est certain que les agents de police se sont présentés comme des candidats brésiliens aux actes assassins réclamaient par Daesh, Al Qaeda …
La Cour fédérale du Paraná a lancé 12 mandats d'arrêt grâce aux enregistrements téléphoniques d'internautes qui se seraient déclarés prêts à orchestrer des attaques lors des JO de Rio. Des internautes qui s'échangeaient aussi des modes d'emploi de tactiques militaires. Le ministre de la Justice a également révélé que certains des brésiliens arrêtés lors de l'Opération Hashtag avaient prêtés serment d'allégeance à l'État islamique.

Contrôler les réseaux sociaux

Le Brésil est précurseur sur de nombreux points concernant le contrôle des réseaux sociaux. Ce pays, qui est un immense vivier de pirates informatiques, tente aussi de cyber surveiller les propos et les internautes passant par ses Internet. Souvenez-vous, en juin 2014, lors de la coupe du monde football, les cyber manifestations lancées par Anonymous. Plus proche de nous, décembre 2015, avec le blocage de WhatsApp durant 48 heures. Un troisième blocage interviendra en mai 2016. Sans oublier l'arrestation d'un dirigeant de Facebook.
Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : ZATAZ Jeux Olympiques de Rio : OP Hashtag infiltre des terroristes – ZATAZ

Détecter les futurs

terroristes sur Internet ? L’Europe veut s’inspirer d’Israël

Détecter les futurs terroristes sur Internet ? L’Europe veut s’inspirer d’Israël

Le coordinateur de l'anti-terrorisme pour lUnion européenne, Gilles de Kerchove, s'est rendu en Israël pour trouver des solutions technologiques qui permettraient de détecter automatiquement des profils suspects sur les réseaux sociaux, grâce à des algorithmes de plus en plus intrusifs.

Plus les attentats en Europe se multiplient, plus on découvre que les profils psychologiques et sociaux des kamikazes et de leurs associés sont très divers, jusqu'à paraître indétectables. Le cas de Mohamed Lahouaiej-Bouhlel, dont on ne sait pas toujours très bien s'il s'agit d'un déséquilibré qui se cherchait un modèle ultra-violent à imiter, ou d'un véritable djihadiste islamiste radicalisé à une vitesse inédite, laisse songeur. Bisexuel, amant d'un homme de 73 ans, mangeur de porc, aucune connexion connue avec des réseaux islamistes… l'auteur de l'attentat de Nice était connu des services de police pour des faits de violence de droit commun, mais n'avait rien de l'homme que l'on pourrait soupçonner d'organiser une tuerie motivée par des considérations idéologiques.
Or c'est un problème pour les services de renseignement à qui l'on demande désormais l'impossible, à la Minority Report, c'est-à-dire de connaître à l'avance le passage à l'acte d'un individu, pour être capable de l'appréhender avant son méfait, même lorsqu'objectivement rien ne permettait de présager l'horreur.

C'EST POUR ÇA QUE JE SUIS ICI. NOUS SAVONS QU'ISRAËL A DÉVELOPPÉ BEAUCOUP DE MOYENS DANS LE CYBER

Néanmoins, l'Union européenne ne veut pas se résoudre à la fatalité, et va chercher en Israël les méthodes à appliquer pour détecter sur Internet les terroristes susceptibles un jour de passer à l'acte. « C'est un défi », explique ainsi à l'agence Reuters Gilles de Kerchove, le coordinateur de l'UE pour l'anti-terrorisme, en marge d'une conférence sur le renseignement à Tel Aviv. « Nous allons trouver bientôt des moyens d'être beaucoup plus automatisé » dans la détection des profils suspects sur les réseaux sociaux, explique-t-il. « C'est pour ça que je suis ici ».
« Nous savons qu'Israël a développé beaucoup de moyens dans le cyber », pour faire face aux attaques d'Israéliens par des Palestiniens, ajoute le haut fonctionnaire européen, et l'UE veut s'en inspirer.

ÉTABLIR DES PROFILS SOCIOLOGIQUES ET SURVEILLER LES COMMUNICATIONS

Selon un officiel israélien interrogé par l'agence de presse, il s'agit d'établir constamment des profils types de personnes à suspecter, en s'intéressant non plus seulement aux métadonnées qui renseignent sur le contexte des communications et les habitudes d'un individu, mais bien sur le contenu-même des communications sur les réseaux sociaux.
Mis à jour quotidiennement au gré des nouveaux profils qui émergent, des paramètres comme l'âge de l'internaute, sa religion, son origine socio-économique et ses liens avec d'autres suspects, seraient aussi pris en compte par les algorithmes israéliens – ce qui semble difficilement compatible en Europe avec les textes internationaux protégeant les droits de l'homme, que l'Union européenne s'est engagée à respecter.

DES BOÎTES NOIRES TOUJOURS PLUS INTRUSIVES ?

En somme, c'est exactement ce que nous redoutions avec les fameuses boîtes noires permises par la loi Renseignement en France, dont le Conseil constitutionnel n'a su que dire, et qui se limitent officiellement aux métadonnées. Là aussi, il s'agit d'utiliser des algorithmes, dont on ne sait pas du tout sur quoi ils se basent, pour détecter des profils suspects.

Eagle Security & Defense, une société israélienne proposant des solutions de surveillance sur Internet, a reçu la visite de Christian Estrosi en début d'année.
Il n'est toutefois pas dit que la technologie israélienne soit importée telle quelle, d'autant que M. De Kerchove a lui-même rappelé que le droit européen n'autoriserait pas un tel degré d'intrusion dans la vie privée. Mais le mécanisme décrit par l'officiel d'Israël est très proche.
Il vise tout d'abord à réaliser une première détection sommaire des profils suspects, puis à déterminer parmi eux ceux qui doivent faire l'objet d'une surveillance individualisée. C'est exactement ce que prévoit la loi Renseignement, qui autorise l'installation de boîtes noires chez les FAI ou les hébergeurs et éditeurs pour détecter des comportements suspects d'anonymes, avant de permettre une identification des personnes dont il est confirmé qu'elles méritent une attention particulière.
En Israël, le ratio serait d'environ 20 000 personnes considérées suspectes pour 1 million d'internautes, sur lesquelles ressortiraient entre 10 et 15 profils nécessitant une surveillance étroite.

CHRISTIAN ESTROSI DÉJÀ INTÉRESSÉ

L'information de Reuters confirme ce qu'indiquaient Les Échos le week-end dernier dans un reportage bien informé. « L'Etat hébreu, dont la population a connu sept guerres et deux Intifada depuis sa création, est bel est bien devenu un cas d'école, dans sa façon de gérer une situation d'insécurité permanente. Une expertise dans la mire des décideurs européens », écrivait le quotidien,
Il précisait qu'en février dernier, l'ancien maire de Nice et actuel président de la région Provence-Alpes-Côte d'Azur, Christian Estrosi, s'était déjà rendu en Israël, où il aurait rencontré le PDG de la société Eagle Security and Defense, Giora Eiland, qui est aussi ex-directeur du Conseil de sécurité nationale israélien.
Lors de cette visite, Christian Estrosi aurait insisté sur la nécessité « d'être à la pointe de la lutte par le renseignement contre la cybercriminalité lorsqu'on sait que la radicalisation se fait par le biais des réseaux sociaux ». On imagine que cette conversation lui est revenue en mémoire lorsque sa ville a été meurtrie.
Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : Détecter les futurs terroristes sur Internet ? LEurope veut sinspirer dIsraël – Politique – Numerama

---

Trois histoires vrais de vies inquiétées par du piratage informatique ciblé

Trois histoires vrais de vies inquiétées par du piratage informatique ciblé

L'expérience le prouve : même les vieux habitués d'Internet n'arrivent pas toujours à se protéger des piratages ciblés. Étant donné que notre vie quotidienne devient de plus en plus connectée à Internet et à d'autres réseaux, la sécurité en ligne s'est convertie comme un besoin impératif.

La plupart d'entre nous ont un email, un compte sur les réseaux sociaux et une banque en ligne. On commande sur le web, et utilisons notre mobile pour nous connecter à Internet (par exemple, dans les solutions de l'authentification à deux facteurs) et pour d'autres choses tout aussi importantes. Malheureusement, aucun de ces systèmes n'est 100% sûr.
Plus nous interagissons en ligne et plus nous devenons les cibles de hackers sournois. Les spécialistes en sécurité appellent ce phénomène » la surface d'attaque « . Plus la surface est grande et plus l'attaque est facile à réaliser. Si vous jetez un coup d'œil à ces trois histoires qui ont eu lieu ces trois dernières années, vous comprendrez parfaitement le fonctionnement de cette attaque.

1. Comment détourner un compte : faut-il le pirater ou simplement passer un coup de fil ?

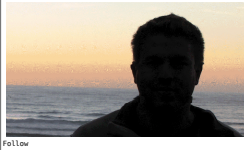
Un des outils les plus puissants utilisés par les hackers est le » piratage humain » ou l'ingénierie sociale. Le 26 février dernier, le rédacteur en chef de Fusion Kevin Roose, a voulu vérifier s'il était aussi puissant qu'il n'y paraissait. Jessica Clark, ingénieure sociale spécialisée en piratage informatique et l'expert en sécurité Dan Tentler ont tout deux accepté ce défi.
Jessica avait parié qu'elle pouvait pirater la boîte mail de Kévin rien qu'avec un email, et sans grande difficulté elle y est arrivé. Tout d'abord, l'équipe de Jessica a dressé un profil de 13 pages qui définissait quel genre d'homme il était, ses goûts, etc, provenant de données collectées de diverses sources publiques.
Après avoir préparé le terrain, Jessica a piraté le numéro mobile de Kévin et appelé sa compagnie de téléphone. Pour rendre la situation encore plus réelle, elle ajouta un fond sonore d'un bébé en train de pleurer.
Jessica se présenta comme étant la femme de Roose. L'excuse inventée par cette dernière fut qu'elle et son » mari » devaient faire un prêt, mais qu'elle avait oublié l'email qu'ils utilisaient en commun, en se faisant passer pour une mère de famille désespérée et fragile. Accompagnée des cris du bébé, Jessica ne mit pas longtemps à convaincre le service technique de réinitialiser le mot de passe du mail et ainsi d'y avoir pleinement accès.
Dan Tentler a accompli cette tâche avec l'aide de l'hameçonnage. Tout d'abord, il avait remarqué que Kevin possédait un blog sur Squarespace et lui envoya un faux email officiel depuis la plateforme, dans lequel les administrateurs de Squarespace demandaient aux utilisateurs de mettre à jour le certificat SSL (Secure Sockets Layer) pour des questions de » sécurité « , permettant ainsi à Tentler d'accéder à l'ordinateur de Kévin. Dan créa de nombreux faux pop-up demandant à Roose des informations bien spécifiques et le tour était joué.
Tentler réussit à obtenir l'accès à ses données bancaires, son email, ses identifiants sur les sites web, ainsi que ses données de cartes de crédit, son numéro de sécurité sociale. De l'écran de son ordinateur, il capturait des photos toutes les deux minutes et ce pendant 48h.
View image on Twitter

Follow

Kaspersky Lab
@kaspersky
What is phishing and why should you care? Find outhttps://kas.pr/6bpe #iteducation #itsec
8:05 PM – 11 Dec 2015
•
•
1717 Retweets
•
77 likes

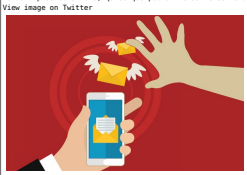
2. Comment détourner de l'argent à un ingénieur informatique en moins d'une nuit

Au printemps 2015, le développeur de logiciels Partap Davis a perdu 3000$. Durant une nuit, en seulement quelques heures, un hacker inconnu a obtenu l'accès de ses comptes mail, son numéro de téléphone et son Twitter. Le coupable a contourné habilement le système de l'authentification à deux facteurs et littéralement vidé le portefeuille des bitcoins de Partap. Comme vous devez sans doute l'imaginer, Davis a passé une mauvaise journée le lendemain.
Il est important de noter que Partap est une pointure concernant l'usage d'Internet : il choisit toujours des mots de passe fiables et ne clique jamais sur des liens malveillants. Son email est protégé avec le système d'authentification à deux facteurs de Google, ce qui veut dire que lorsqu'il se connecte depuis un nouvel ordinateur, il doit taper les six numéros envoyés sur son mobile.



Follow

The Verge
@verge
Anatomy of a hack: a step-by-step account of an overnight digital heist http://www.theverge.com/a/anatomy-of-a-hack …
4:02 PM – 4 Mar 2015
•
•
6969 Retweets
•
7171 likes
Davis gardait ses économies sur trois portefeuilles Bitcoin, protégés par un autre service d'authentification à deux facteurs, conçu par l'application mobile Authy. Même si Davis utilisait toutes ces mesures de sécurité prévoyantes, ça ne l'a pas empêché de se faire pirater.
Suite à cet incident, Davis était très en colère et a passé plusieurs semaines à la recherche du coupable. Il a également contacté et mobilisé des journalistes de The Verge pour l'enquête. Tous ensemble, ils sont parvenus à trouver comment le piratage avait été exécuté. Davis utilisait comme mail principal l'adresse suivante : Patrap@mail. Tous les mails furent envoyés à une adresse Gmail plus difficile à mémoriser (étant donné que Patrap@gmail était déjà utilisé).
Pendant plusieurs mois, quiconque pouvait ensuite se rendre sur la page Hackforum et acheter un script spécial afin d'obtenir les mots de passe qui se trouvaient dans la boite mail. Apparemment, le script était utilisé pour contourner l'authentification à deux facteurs et changer le mot de passe de Davis.
View image on Twitter



Follow

Kaspersky Lab
@kaspersky
Unfortunately two-factor authentication can't save you from#banking Trojans https://kas.pr/S4jV #mobile
4:40 PM – 11 Mar 2016
•
•
2828 Retweets
•
1515 likes
Ensuite, l'hacker a fait une demande de nouveau mot de passe depuis le compte de Davis et demandé au service client de transférer les appels entrants à un numéro de Long Beach (ville en Californie). Une fois le mail de confirmation reçu, le service technique a donné le contrôle des appels à l'hacker. Avec une telle technique, il n'était pas bien difficile de contourner l'authentification à deux facteurs de Google et avoir accès au compte Gmail de Davis.
Pour surmonter cet obstacle, l'hacker a tout simplement réinitialisé l'application sur son téléphone en utilisant une adresse mail.com et une nouvelle confirmation de code, envoyée de nouveau via un appel vocal. Une fois que l'hacker mit la main sur toutes les mesures de sécurité, il changea les mots de passe des portefeuilles Bitcoin de Davis, en utilisant Authy et l'adresse email .com afin de lui détourner de l'argent.
L'argent des deux autres comptes est resté intact, l'un des services interdisant le retrait des fonds 48h après le changement du mot de passe, et l'autre demandant une copie du permis de conduire de Davis, que l'hacker n'avait pas en sa possession.

3. La menace rôde sur nos vies

Comme l'a écrit le journal Fusion en octobre 2015, la vie de la famille Straters s'est retrouvée anéantie à cause d'une pizza. Il y a plusieurs années, des cafés et restaurants locaux se sont installés sur leur arrière-cour, les envahissant de pizzas, tartes et toute sorte de nourriture.
Peu de temps après, des camions de remorquage ont déboulé munis de grandes quantités de sable et de gravier, tout un chantier s'était installé sans aucune autorisation au préalable. Malheureusement, il ne s'agissait que de la partie visible de l'iceberg comparé au cauchemar des trois années suivantes.
Follow

Techmeme @Techmeme
How the Strater family endured 3 years of online harassment, hacked accounts, and swatting http://fusion.net/story/212802/haunted-by-hackers-a-suburban-familys-digital-ghost-story/ …http://www.techmeme.com/151025/p4##a151025p4 …
6:36 PM – 25 Oct 2015

Haunted by hackers: A suburban family's digital ghost story

A suburban Illinois family has had their lives ruined by hackers.
fusion.net
•
•
88 Retweets
•
66 likes
Paul Strater, ingénieur du son pour une chaine de télé locale et sa femme, Amy Strater, ancienne directrice générale d'un hôpital, ont été tout deux victimes d'un hacker inconnu ou de tout un groupe. Il s'avérait que leur fils Blair était en contact avec un groupe de cybercriminels. Les autorités ont reçu des menaces de bombe signées du nom du couple. Les hackers ont utilisé le compte d'Amy pour publier une attaque planifiée dans une école primaire, dans lequel figurait ce commentaire » Je tirerai sur votre école « . La police faisait des visites régulières à leur domicile, n'améliorant en rien les relations du couple avec leur voisinage, qui à force se demandait ce qu'il se passait.
Les hackers ont même réussi à pirater le compte officiel de Tesla Motors et posté un message qui encourageait les fans de la page à appeler les Strater, en échange de gagner une voiture Tesla. Les Strater » croulaient sous les appels téléphoniques « , environ cinq par minute, provenant des » admirateurs » de Tesla, désireux de gagner la voiture. Un jour, un homme s'est même présenté au domicile des Strater en demandant aux propriétaires d'ouvrir leur garage, prétendant qu'ils cachaient la Tesla à l'intérieur.
Follow

r00t @rootworx
Again, There is no free car, I did not hack Elon Musk or Tesla's Twitter account. A Finnish child is having fun at your (and my) expense.
12:51 AM – 26 Apr 2015
•
•
1414 Retweets
•
1818 likes
Paul tenta de démanteler le groupe d'hackers en changeant tous les mots de passe de ses comptes et en donnant l'ordre aux patrons des restaurants locaux de ne rien dévoiler sur leur adresse. Il contacta également le Département de Police d'Oswego en leur demandant de vérifier à l'avance si une urgence était bien réelle, avant d'envoyer des renforts. En conséquence de tous ces problèmes, Paul et Amy finirent par divorcer.
Les attaques ont continué par la suite. Les réseaux sociaux d'Amy ont été piratés et utilisés pour publier toute une série de revendications racistes, ce qui a causé la perte de son emploi. Elle fut licenciée malgré avoir dit à ses supérieurs qu'elle et sa famille étaient les victimes de hackers et que leur vie s'était transformée en un véritable cauchemar.
Amy réussit à temps à reprendre le contrôle de son LinkedIn et à supprimer son compte Twitter. Malheureusement, elle était incapable de retrouver un travail dans sa branche à cause de ce qui s'était passé. Elle fut contrainte de travailler chez Uber pour arrondir ses fins de mois, mais disposait de ressources insuffisantes pour payer son loyer.
» Avant, lorsqu'on tapait son nom sur Google, on pouvait voir ses nombreux articles scientifiques et son travail admirable » a déclaré son fils Blair au journal Fusion. » Désormais, on ne voit plus que des hackers, hackers, hackers « .
De nombreuses personnes ont critiqué Blair Strater pour avoir été impliqué lui-même dans de nombreux réseaux de cybercriminels, où il n'arrivait pas à se faire d'amis. Dans le cas précis de la famille Strater, les parents de Blair ont payé pour les » crimes » de leur fils, alors qu'eux n'avaient absolument rien à voir avec les hackers.
Article original de Kate Kochetkova

Denis JACOPINI ne peut que vous recommander d'être prudent.
Si vous désirez être sensibilisé aux risques d'arnaques et de piratages afin d'en être protégés, n'hésitez pas à nous contacter, nous pouvons animer conférences, formations auprès des équipes dirigeantes et opérationnelles.
La sécurité informatique et la sécurité de vos données est plus devenu une affaire de Qualité (QSE) plutôt qu'un problème traité par des informaticiens.
Vous souhaitez être aidé ? Contactez-nous

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 pirater, détourner de l’argent et rendre la vie de quelqu’un impossible sur Internet : trois histoires inquiétantes de piratages ciblés. | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.

Que faire quand son compte Facebook est piraté ?

	**Que faire quand son compte Facebook est piraté ?**

Pour certains, se faire hacker son compte Facebook revient à vivre un cauchemar. Imaginez qu'un inconnu invisible puisse accéder à tous vos messages privés, contacter vos amis, usurper votre identité et effacer (ou remplacer) toutes vos données personnelles. Effrayant, n'est-ce pas ? Pour éviter cela, changez régulièrement votre mot de passe, et verrouillez bien les réglages de sécurité.

Si malgré tout votre compte Facebook était piraté, il faut agir vite. Et rassurez-vous, vous pouvez tout à fait retrouver votre espace Facebook comme il était auparavant (ou presque) !

Comment savoir si mon compte Facebook a été piraté ?

Il n'est pas évident de **deviner que son compte Facebook a été hacké**, surtout si rien ne semble avoir changé (mur, photos, etc.). Il existe pourtant un **moyen très simple** d'en avoir le cœur net : si une tierce personne a accédé à votre compte, vous pouvez retrouver une**trace de sa session**. Pour ce faire, cliquez sur *Accueil* < *Paramètres du compte* < *Sécurité* < *Sessions actives*.

Si vous pensez que votre compte a été détourné, **supprimez les sessions douteuses**, et **procédez aux étapes suivantes**.

1. Changez ou réinitialisez votre mot de passe

Si le pirate n'a pas modifié votre mot de passe, vous êtes plutôt chanceux ! **Changez-le immédiatement** pour que le hacker ne puisse plus se connecter à votre place : cliquez sur*Accueil* < *Paramètres du compte* < *Général* < *Mot de passe*. Renseignez votre mot de passe actuel, puis saisissez deux fois le nouveau mot de passe, avant d'enregistrer les modifications.

Si vous n'avez plus accès à votre compte parce que le mot de passe à été changé par le pirate, cliquez sur < *Mot de passe oublié ?* > depuis la page d'identification.

Vous avez alors le choix entre **3 méthodes d'authentification** :

Si le pirate a réellement modifié vos informations personnelles, le choix le plus efficace sera le troisième (identification via un ami). Facebook vous propose alors un compte, probablement le vôtre. Si tel est le cas, et que les moyens de vous contacter affichés sont toujours d'actualité, cliquez sur « **Réinitialiser le mot de passe**» . Dans le cas contraire, cliquez sur « **Ceci n'est pas mon compte** » et/ou compléter les champs permettant à Facebook de vous contacter.

2. Rapporter la compromission du compte Facebook

Si votre compte n'a pas été seulement piraté, mais qu'il fait également l'objet d'**envois publicitaires et de spams** à vos amis, signalez-le via cette adresse :http://www.facebook.com/hacked/

3. Limiter les dégâts

Prévenez vos amis Facebook de votre mésaventure, pour éviter qu'ils ne tombent dans le même piège : des messages leur sont peut-être envoyés depuis votre compte, à votre insu.

Si vous n'avez plus accès à votre compte, contactez-les par mail, téléphone, etc.

4. Supprimez les applications suspectes

La plupart du temps, ce n'est pas une personne mal intentionnée qui pirate les comptes Facebook, mais des **applications frauduleuses**, auxquelles vous avez donné les autorisations nécessaires par manque de vigilance. Supprimez les applications malveillantes en cliquant sur *Accueil* < *Paramètres du compte* < *Applications* :

Cliquez sur une des applications pour obtenir le **détail de ses droits** automatiques, et**supprimez celles dont vous n'avez plus besoin ou qui vous semblent louches**. Certaines applications autorisent aussi la **suppression de certains accès**.

Voila, ca va mieux ?

Article original de panoptinet.com

Le Net Expert INFORMATIQUE

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Que faire quand son compte Facebook est piraté ? | Panoptinet

---

Attention aux versions piégées de Pokémon GO

Attention aux versions piégées de Pokémon GO

L'application Pokémon Go fait un carton dans les smartphones. Prudence, non encore officiel en Europe, installer le jeu via des boutiques hors de contrôle des auteurs met en danger votre vie privée.

Pas de doute, le phénomène Pokémon GO débarque en force en cet été 2016. L'application tirée du jeu éponyme de Nintendo permet de s'éclater à trouver des Pokemons un peu partout dans le monde. De la réalité virtuelle bien venue pour l'été.

Édité par Niantic, le créateur de Pokémon GO ne propose son appli qu'aux États-Unis, en Australie et en Nouvelle-Zélande. Un pré lancement pour tester les serveurs, très sollicités, et la stabilité du jeu. Bref, normalement, il n'est pas possible d'y jouer en Europe, et donc en France. Sauf qu'il y a toujours des possibilités, comme celle d'installer Pokémon GO vient l'APK (le programme) proposé par de nombreux sites Internet non officiels.

Attention ! des sites qui ne sont pas maîtrisés et contrôlés par les auteurs. Des espaces de téléchargements qui sont des limites du Play Store de Google et de l'App Store d'Apple. Bref, à vos risques et périls.

J'ai déjà pu repérer des APK piégés (ransomwares, cheval de Troie, …) proposés, je l'avoue, dans des lieux peu recommandables. Prenez l'avertissement très au sérieux. Pokemon GO ne vous demandera JAMAIS d'accéder à vos messages [SMS, MMS], à vos appels téléphoniques. Si l'APK que vous avez téléchargez vous propose ces « autorisations », ne l'installez surtout pas. Attendez la version officielle.

Je ne me voile pas la face, le phénomène attire beaucoup d'internautes, jeunes et moins jeunes. Et avec les vacances, une bonne occasion de sauter sur le jeu pour smartphone de l'été. Des milliers de Français l'ont fait. J'en croise beaucoup, dans la rue, comme le montre ma photographie, prise ce 13 juillet dans les rues de Paris. Je rentre de New York, l'engouement est… pire !

A noter que plusieurs éditeurs d'antivirus ont mis la main sur une version « malveillante » de Pokémon GO. Bitdefender, par exemple, parle de DroidJack. Ce cheval de Troie ouvre une backdoor et donne l'accès aux données des appareils mobiles infectés, permettant ainsi leur prise de contrôle à distance par les pirates. Ce malware disponible pour seulement 200 dollars sur certains sites Web, offre au pirate une interface de contrôle facile à utiliser lui permettant par exemple de surveiller l'activité des appareils corrompus, de passer des appels, d'envoyer des SMS, de localiser l'appareil, d'utiliser l'appareil photo ou le microphone ou même d'accéder aux dossiers.

La version iPhone malmenée par la version officielle

Autre mise en garde pour les joueurs de Pokémon GO : sur iOS, l'application semble demander plus d'autorisations que nécessaire. L'accès à l'application via un compte Google semble conférer au développeur Niantic (ex Start-up de Google), un accès complet aux comptes des utilisateurs. Ce problème est en cours de résolution et n'est pas présent dans les versions Android.

Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : ZATAZ Pokémon GO, prudence aux fichiers vérolés – ZATAZ

Secret des conversations, Facebook Messenger bientôt chiffré

	**Secret des conversations, Facebook Messenger bientôt chiffré**

Non, tous les échanges sur Messenger ne sont pas chiffrés de bout en bout. Pas encore du moins. Facebook teste le procédé à travers une nouvelle fonctionnalité, #Secret Conversations. En y ajoutant un petit côté messages éphémères à la Snapchat.

Facebook chantre du chiffrement de bout en bout ? L'entreprise vient de lancer une nouvelle option pour Messenger permettant de démarrer une conversation sécurisée. Baptisée Secret Conversations, celle-ci permet de créer, via la fiche d'un contact, une conversation chiffrée entre deux utilisateurs. Derrière, on retrouve le protocole Signal, également utilisé par WhatsApp.
Mais, contrairement à #WhatsApp, Secret Conversations se veut optionnel, pour ne pas dire ponctuel. Car il s'agit là de préférer la sécurité au confort, un choix auquel Facebook n'entend pas contraindre ses utilisateurs. Ainsi, via cette fonctionnalité, on ne peut envoyer que du texte et des photos à un unique destinataire. Pas de vidéo, de GIF, de paiement ou de discussion de groupe.

Ce message s'autodétruira automatiquement dans 4…3…

Cette sobriété se conjugue avec l'absence de synchronisation entre les appareils d'un même utilisateur. Impossible donc de commencer une conversation chiffrée avec son iPhone et de passer ensuite à sa tablette : la discussion est uniquement rattachée au terminal avec lequel elle a été initiée. En outre, preuve que Mark Zuckerberg n'a toujours pas digéré le refus de son offre de rachat sur Snapchat, il est possible de définir à l'aide d'un minuteur la durée de vie d'un message. Qui s'autodétruira une fois le délai écoulé.
L'option est intégrée à l'application Messenger pour Android et iOS. Déjà disponible pour certains, elle sera déployée plus largement au cours de l'été. Pour l'heure, il semble que rien ne soit prévu pour les versions navigateur du service.

Article original de Guillaume Périssat

Réagissez à cet article

Original de l'article mis en page : Secret Conversations : Facebook Messenger en mode chiffré