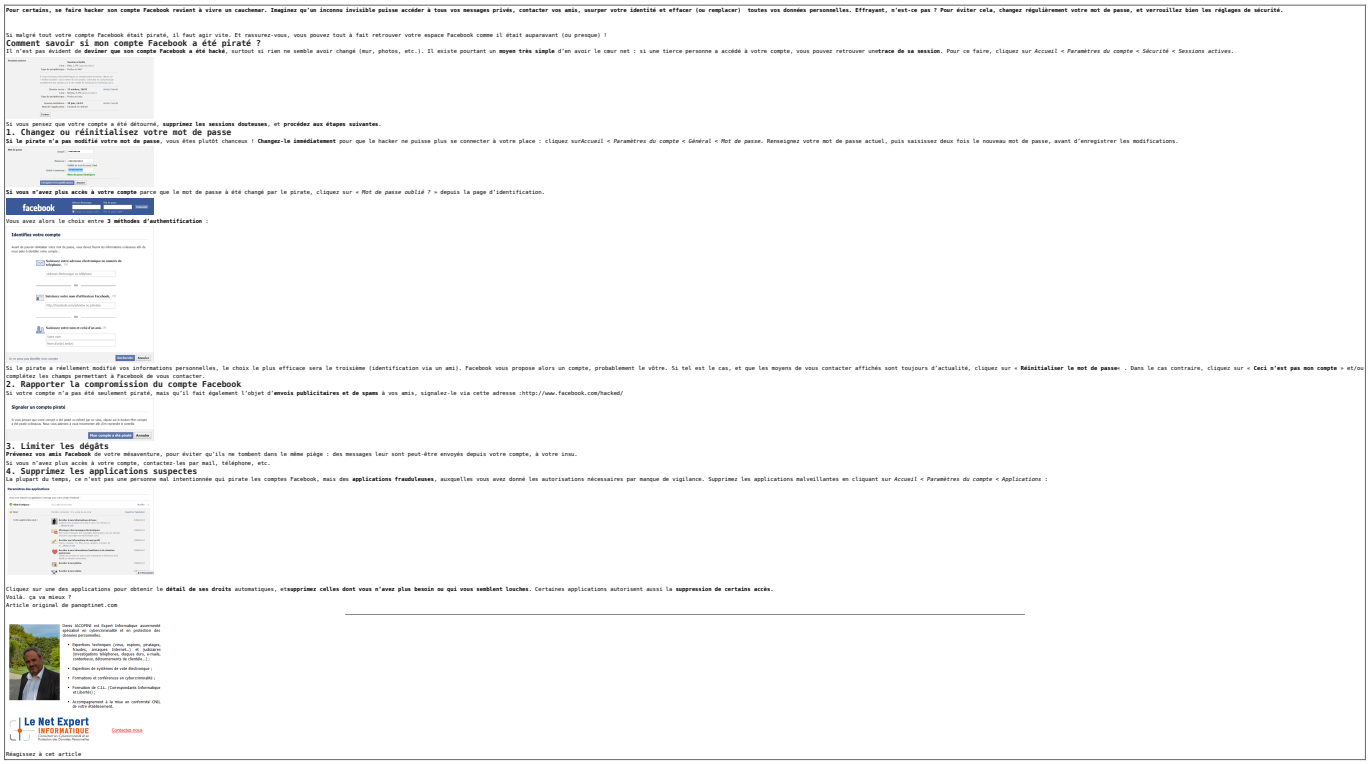
Que faire quand son compte Facebook est piraté ?

	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

Réagissez à cet article

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

---

Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s'en prend à vos données »

Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s'en prend à vos données »

Locky, TeslaCrypt, Cryptolocker, Cryptowall… Depuis plusieurs mois, les rançongiciels (« ransomware »), ces virus informatiques qui rendent illisibles les données d'un utilisateur puis lui réclament une somme d'argent afin de les déverrouiller, sont une préoccupation croissante des autorités. Le commissaire François-Xavier Masson, chef de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, une unité de la police spécialisée dans la criminalité informatique, explique au Monde les dangers de cette menace.

Combien y a-t-il d'attaques par rançongiciel en France ?
On ne le sait pas avec précision, nous n'avons pas fait d'étude précise à ce sujet. Statistiquement, le rançongiciel ne correspond pas à une infraction pénale précise et il recoupe parfois l'intrusion dans un système automatisé de traitement de données. Il faudrait affiner le cadre car nous avons besoin de connaître l'état de la menace.
Avez-vous quand même une idée de l'évolution du phénomène ?
L'extorsion numérique est clairement à la hausse, c'est la grande tendance en termes de cybercriminalité depuis 2013. Tout le monde est ciblé : les particuliers, les entreprises, même l'Etat. Les attaques gagnent en sophistication et en intensité. Il y a aussi une industrialisation et une professionnalisation. La criminalité informatique est une criminalité de masse : d'un simple clic on peut atteindre des millions de machines. Désormais, il n'y a plus besoin de vous mettre un couteau sous la gorge ou de kidnapper vos enfants, on s'en prend à vos données.
Les victimes ont-elles le réflexe de porter plainte ?
Certaines victimes paient sans porter plainte. Ce calcul est fait par les entreprises qui estiment que c'est plus pratique de payer la rançon – dont le montant n'est pas toujours très élevé, de l'ordre de quelques bitcoins ou dizaines de bitcoins – et qu'en portant plainte, elles terniront leur image et ne récupéreront pas nécessairement leurs données. Elles pensent aussi que payer la rançon coûtera moins cher que de payer une entreprise pour nettoyer leurs réseaux informatiques et installer des protections plus solides. C'est une vision de court terme. Nous recommandons de ne pas payer la rançon afin de ne pas alimenter le système. Si l'on arrête de payer les rançons, les criminels y réfléchiront à deux fois. C'est la même doctrine qu'en matière de criminalité organisée.
Qu'est-ce qui pousse à porter plainte ?
Chaque cas est unique mais généralement, c'est parce que c'est la politique de l'entreprise ou parce que le montant de la rançon est trop élevé.
Qui sont les victimes ?
Il s'agit beaucoup de petites et moyennes entreprises, par exemple des cabinets de notaires, d'avocats, d'architectes, qui ont des failles dans leur système informatique, qui n'ont pas fait les investissements nécessaires ou ne connaissent pas forcément le sujet. Les cybercriminels vont toujours profiter des systèmes informatiques vulnérables.
Quel est votre rôle dans la lutte contre les rançongiciels ?
La première mission, c'est bien sûr l'enquête. Mais nous avons aussi un rôle de prévention : on dit que la sécurité a un coût mais celui-ci est toujours inférieur à celui d'une réparation après un piratage. Enfin, de plus en plus, nous offrons des solutions de remédiation : nous proposons des synergies avec des entreprises privées, des éditeurs antivirus. On développe des partenariats avec ceux qui sont capables de développer des solutions. Si on peut désinfecter les machines nous-mêmes, on le propose, mais une fois que c'est chiffré, cela devient très compliqué : je n'ai pas d'exemple de rançongiciel qu'on ait réussi à déverrouiller.
Quel rapport entretenez-vous avec les entreprises ?
On ne peut pas faire l'économie de partenariats avec le secteur privé. Nous pourrions développer nos propres logiciels mais ce serait trop long et coûteux. Il y a des entreprises qui ont des compétences et la volonté d'aider les services de police.
Parvenez-vous, dans vos enquêtes, à identifier les responsables ?
On se heurte très rapidement à la difficulté de remonter vers l'origine de l'attaque. Les rançongiciels sont développés par des gens dont c'est le métier, et leur activité dépasse les frontières. On a des idées pour les attaques les plus abouties, ça vient plutôt des pays de l'Est. Mais pas tous.
Parvenez-vous à collaborer avec vos homologues à l'étranger ?
Oui, c'est tout l'intérêt d'être un office central, nous sommes le point de contact avec nos confrères internationaux. Il y a beaucoup de réunions thématiques, sous l'égide de l'Office européen de police (Europol), des pays qui mettent en commun leurs éléments et décrivent l'état d'avancement de leurs enquêtes. C'est indispensable de mettre en commun, de combiner, d'échanger des informations. Il peut y avoir des équipes d'enquête communes, même si ça ne nous est pas encore arrivé sur le rançongiciel.
De plus en plus d'enquêteurs se penchent sur le bitcoin – dont l'historique des transactions est public – comme outil d'enquête. Est-ce aussi le cas chez vous ?
C'est une chose sur laquelle on travaille et qui nous intéresse beaucoup. S'il y a paiement en bitcoin, il peut y avoir la possibilité de remonter jusqu'aux auteurs. C'est aussi pour cela que l'on demande aux gens de porter plainte même lorsqu'ils ont payé.
Article original de Martin Untersinger

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 : Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s’en prend à vos données »

Deux hommes ont volé 1,7 million d’euros en piratant des distributeurs de billet

Deux hommes ont volé 1,7 million d’euros en piratant des distributeurs de billet

---

Sans utiliser la moindre carte de crédit, deux hommes ont volé 1,7 millions d'euros à la First Commercial Bank de Taïwan.

Les « casses du siècles » deviennent de plus en plus cocasses et subtiles à l'ère du tout numérique. Chaque mois ou presque, on peut trouver un exemple de vol de banque, qui mêle développement logiciel et matériel. Cette fois le crime n'implique pas le vol ou la copie de cartes de crédit : à Taïwan, deux pirates ont réussi à retirer l'argent de 30 distributeurs sans se faire prendre. La somme volée s'élève à 70 millions de dollars taïwanais.
Leur méthode était particulièrement rodée. En moins de 10 minutes, les voleurs ont exécuté un programme dans le système du distributeur de billet qui, bien gentiment, a offert ses devises sans demander de compte. Le logiciel a ensuite pris soin d'effacer toute trace du larcin. Et les voleurs sont repartis, à 30 reprises, avec le gros lot. Les enquêteurs ne savent toujours pas comment les pirates ont fait pour déployer leur code aussi rapidement sur les distributeurs, ni quel moyen a été utilisé pour se connecter aux machines – un smartphone est évoqué.

LES VOLEURS SONT REPARTIS, À 30 REPRISES, AVEC LE GROS LOT
Les deux hommes seraient des étrangers : l'un d'eux a été identifié comme étant un citoyen russe qui s'est enfui de l'île dimanche et est recherché par Interpol. L'identité et la nationalité de l'autre homme ne sont pas connues. En attendant les experts de la compagnie allemande qui fournit les distributeurs à la banque taïwanaise qui a été prise pour cible, la décision de bloquer tous les distributeurs du même fournisseur a été prise par les autorités. 400 distributeurs de billet ont donc été rendus inactifs.
Article original de Julien Cadot

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

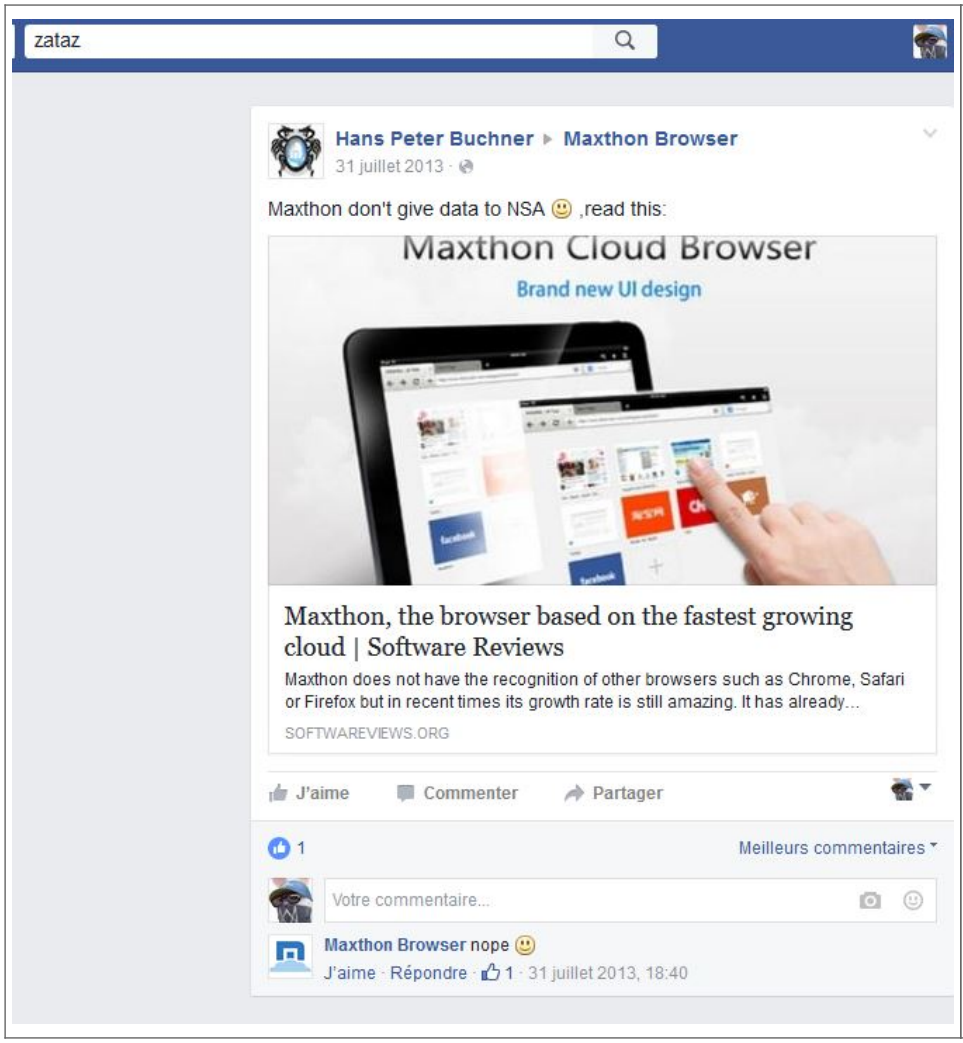
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Deux hommes ont volé 1,7 million d’euros en piratant des distributeurs de billet – Tech – Numerama

---

Attention, le navigateur Maxhton espionne ses utilisateurs !



Attention, le navigateur Maxhton espionne ses utilisateurs !

Le navigateur Maxhton ne serait rien d'autre qu'un outil d'espionnage à la solde de la Chine ?

Des experts en sécurité informatiques de l'entreprise polonaise Exatel viennent de révéler la découverte de faits troublant visant le navigateur *Maxhton*. Ce butineur web recueille des informations sensibles appartenant à ses utilisateurs. Des informations qui sont ensuite envoyées à un serveur basé en Chine. Les chercheurs avertissent que les données récoltées pourraient être très précieuses pour des malveillants.

Les données des utilisateurs de Maxhton envoyées en Chine !
Et pour cause ! Les ingénieurs de *Fidelis Cybersecurity* et *Exatel* ont découvert que Maxthon communiquait régulièrement un fichier nommé ueipdata.zip. Le dossier compressé est envoyé en Chine, sur un serveur basé à Beijing, via HTTP. Une analyse plus poussée a révélé que ueipdata.zip contient un fichier crypté nommé dat.txt. Dat.txt stocke des données sur le système d'exploitation, le CPU, le statut ad blocker, l'URL utilisé dans la page d'accueil, les sites web visités par l'utilisateur (y compris les recherches en ligne), et les applications installées et leur numéro de version.
En 2013, après la révélation du cyber espionnage de masse de la NSA, Maxhton se vantait de mettre l'accent sur la vie privée, la sécurité, et l'utilisation d'un cryptage fort pour protéger ses utilisateurs. (Merci à I.Poireau)
Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : ZATAZ Le navigateur Maxhton espionne ses utilisateurs – ZATAZ

Un concessionnaire Lamborghini de Mulhouse piraté

Un concessionnaire Lamborghini de Mulhouse piraté

Le vol de données peut souvent cacher des arnaques et attaques informatiques plus vicieuses encore. Exemple avec le piratage d'un concessionnaire de Lamborghini de l'Est de la France.

Derrière un piratage informatique, 99 fois sur 100, se cache le vol des données que le malveillant à pu rencontrer dans son infiltration. Des données qui se retrouvent, dans l'heure, quand ce n'est pas dans les minutes qui suivent la pénétration du site dans des forums et autres boutiques dédiés à l'achat et revente d'informations subtilisées.Un concessionnaire de Lamborghini, à Mulhouse, vient d'en faire les frais.

Une fois les contenus dérobés exploités (phishing, escroqueries…) le pirate s'en débarrasse en les diffusant sur la toile. C'est ce qui vient d'arriver à un concessionnaire automobile de l'Est de la France. Ici, nous ne parlons pas de la voiture de monsieur et madame tout le monde, mais de Lamborghini.

Prend son site web par dessus la jambe et finir piraté !

Le concessionnaire se retrouve avec l'ensemble des pousses bouton de la planète aux fesses. De petits pirates en mal de reconnaissance qui profitent d'une idiote injection SQL aussi grosse que l'ego surdimensionné de ces « piratins ». Bilan, le premier pirate a vidé le site, revendu/exploité les données. Il a ensuite tout balancé sur la toile. Les « suiveurs » se sont jetés sur la faille et les données. J'ai pu constater des identifiants de connexion (logins, mots de passe) ou encore des adresses électroniques lâchées en pâture. Des courriels internes (webmaster, responsables du site…).

Article original de Damien Bancal

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 : ZATAZ Un concessionnaire Lamborghini de Mulhouse piraté – ZATAZ

Google met en avant ses succès contre le piratage

Google met en avant ses succès contre le piratage

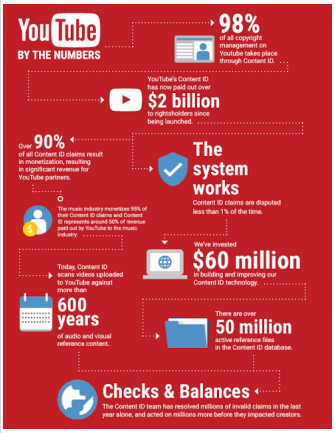
Google combat le piratage, et cherche de plus en plus à le faire savoir. En plus de son filtrage qui limite l'utilisation de Google pour trouver des contenus piratés, Google a reversé 2 milliards de dollars aux ayants droits dont les contenus ont été mis en ligne sur YouTube. Difficile, toutefois, de savoir si c'est beaucoup… ou très peu.
Depuis plusieurs années, Google aime à s'afficher comme défenseur des droits d'auteur, alors que le moteur de recherche a souvent été vilipendé par des ayants droit qui lui reprochaient de donner trop facilement accès à des sites pirates. La firme de Mountain View, qui doit soigner des partenaires commerciaux pour YouTube et pour ses services de distributions de contenus sur Google Play, publie même désormais un document de 62 pages pour expliquer « Comment Google combat le piratage ».

Sur son blog dédié aux politiques publiques, Google précise certains points qui ont été mis à jour dans ce document, lequel était inimaginable quand les recherches avec des mots clés comme « torrents », « mp4 » ou « streaming » renvoyaient encore le plus souvent vers des pages de sites pirates.
NOS ALGORITHMES DE CLASSEMENT DES RECHERCHES RÉTROGRADENT CE SITE DANS LES FUTURS RÉSULTATS DE RECHERCHE

Aujourd'hui, « la grande majorité des requêtes liées à des médias que les utilisateurs soumettent chaque jour retournent des résultats qui incluent seulement des liens vers des sites légitimes », se félicite le géant de la recherche. Et lorsque l'utilisateur cherche à forcer la recherche avant des mots clés spécifiques au streaming gratuit ou au téléchargement sur BitTorrent, « nos systèmes de traitement des demandes de suppressions pour violation du droit d'auteur gèrent des millions d'URL chaque jour », qui font qu'en cas d'infractions répétées sur un site, « nos algorithmes de classement des recherches rétrogradent ce site dans les futurs résultats de recherche ».

2 MILLIARDS DE DOLLARS REVERSÉS PAR YOUTUBE AUX AYANTS DROITS

*Sur YouTube, la chasse au piratage et aux utilisations non autorisées d'extraits de vidéos ou de musique est fortement automatisée, avec **Content ID** qui détecte les empreintes des contenus et permet aux ayants droit de choisir, soit la suppression des exploitations illégales, soit de recevoir les revenus publicitaires attachés à cette exploitation – ce qui n'est pas sans poser régulièrement quelques problèmes de retraits abusifs ou de détournement de revenus par des ayants droits qui s'accaparent toute œuvre dérivée.*
*Ainsi selon Google, 98 % des problèmes de droits d'auteur sur YouTube sont désormais gérés directement avec Content ID, ce qui ne laisse que 2 % de demandes de suppression envoyées par formulaire. **Dans 90 % des cas les ayants droit choisissent de percevoir une rémunération** plutôt que demander le retrait des vidéos mises en cause.*
*Google dit ainsi avoir versé 2 milliards de dollars de droits grâce à Content ID depuis son lancement, ce qui est beaucoup et peu à la fois. Il ne dit pas à combien de visionnages cela correspond, ce qui ne permet pas de calculer le gain par vidéo vue. La **page officielle des statistiques de YouTube**, dont la mise à jour ne semble pas récente, indique que « depuis juillet 2015, plus de 8 000 partenaires (parmi lesquels de nombreux grands groupes audiovisuels, studios de cinéma et maisons de disques) ont revendiqué plus de 400 millions de vidéos via Content ID ».*
Le système est aujourd'hui capable de détecter 50 millions d'œuvres, réattribuées à leurs propriétaires respectifs en cas de réclamation.



Article original de Guillaume Champeau

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 : Google met en avant ses succès contre le piratage – Politique – Numerama

---

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

L’accord sur la transmission des données validé par la Commission Européenne

	L’accord sur la transmission des données validé par la Commission Européenne – Filière 3e

---

Le 8 juillet, la Commission européenne a validé le projet des représentants des Etats-membres de l'UE et des Etats Unis sur le transfert des données en ligne. Une législation qui pourrait favoriser l'Open Data, les objets connectés ainsi que la mise en place de projets de transition énergétique.

A l'origine l'accord sur la transmission des données était appelé « Safe Harbour ». La Cour de Justice de l'Union européenne (CJUE) avait invalidé le texte en octobre 2015 en raison de sa faible sécurité pour les données personnelles. Après des mois de débats, l'accord sur la « protection de la vie privée » (Privacy Shield) a été approuvé par les Etats membres et est entré en vigueur le 11 juillet 2016. Il a pour but de faciliter le transfert des données entre les Etats-Unis et l'Union européenne dans le cadre de la signature du Traité Transatlantique (TAFTA ou TIPP). Ce texte a pour but de faciliter les échanges économiques entre l'UE et les Etats-Unis, en harmonisant les normes européennes à celles américaines. Ces échanges serviraient à encadrer le progrès dans la croissance économique, en favorisant les flux correspondant au secteur du numérique. Dans un communiqué de presse, Andrus Ansip, membre désigné de la Commission Juncker comme vice-président chargé du marché numérique, et la commissaire à la Justice, Vera Jourva, ont déclaré communément : « le texte est fondamentalement différent de l'ancien Safe Harbour: il impose des obligations claires et fortes aux entreprises traitant les données et s'assure que ces règles sont suivies et mises en pratique ».

L'Open Data utile à la transition énergétique ?

Largement décriée, la récupération des données servira pourtant à construire le monde de demain en s'inscrivant dans une logique de transition énergétique. Ainsi les villes, les maisons et les énergies fonctionneront dans un même système connecté et durable. Nombreuses sont les start-up a créer des applications facilitant la mobilité, la sécurité et l'habitat dans le cadre de projets « verts ». Les données deviennent un facteur important du marché économique et énergétique. Pour Christian Buchel, Directeur général adjoint, Chef digital et international pour le groupe ENEDIS : « l'Open Data est utilisé dans le monde entier. Humaniser la DATA c'est mieux comprendre la consommation générale d'énergie ». Des informations qui pourraient être utilisées à grande échelle afin d'accroître la capacité de gestion des énergies. L'anonymat des données serait préservé puisque seul le consommateur aurait accès à ses informations. Pour Sampo Hietanen, de MAAS Finlande, une entreprise spécialisée dans l'Open DATA, il faut « générer de l'information pour construire la ville de demain afin que les services proposés communiquent ensemble ».
Les Etats Unis ont déjà commencé à déployer ce système numérique avec la mise en place de compteurs intelligents, récupérant les données des citoyens pour adapter la consommation énergétique à la demande. La France et ERDF commencent à commercialiser Linky, le compteur intelligent français. En ce sens, la signature du Traité Transatlantique devrait favorisait les partenariats énergétiques et numériques entre l'Union Européenne et les Etats-Unis.
Article original de Mailys Kerhoas

Réagissez à cet article

Original de l'article mis en page : L'accord sur la transmission des données validé par la Commission Européenne — Filière 3e

---

Le malware Nymaim s'attaque

désormais aux institutions financières du Brésil

Le malware Nymaim s'attaque désormais aux institutions financières du Brésil

Après avoir contaminé l'Europe et l'Amérique du Nord en 2013, le malware Nymaim refait surface 3 ans plus tard et se propage désormais via une campagne de spearphising intensive, en utilisant un document Microsoft Word comme pièce jointe infectée

Lors de la découverte de la souche originale de Nymaim en 2013, notamment avec ses techniques de code modulaire (chaîne d'abattage et d'évasion), nous avions pu remarquer que plus de 2,8 millions d'infections s'étaient propagées. Sur le premier semestre 2016, ESET a de nouveau observé une augmentation significative de détections du malware Nymaim.

Infectant principalement la Pologne (54%), l'Allemagne (16%) et les Etats-Unis (12%), cette mutation du malware Nymaim a été détectée comme appartenant à la catégorie *Win32/TrojanDownloader.Nymaim.BA.* Elle utilise le spearphishing et une pièce jointe (type Word.doc) contenant une macro malveillante. Utilisée pour contourner les paramètres de sécurité par défaut de Microsoft Word via les techniques d'ingénierie sociale, l'approche est très dangereuse dans les versions anglaises de MS Word.

« Grâce à ses techniques d'évasion sophistiquées, l'anti-VM, l'anti-débogage et les flux de contrôle, cette fusée à deux étages sert à livrer le ransomware comme charge utile finale. Ce code que l'on peut nommer « Trojan modulaire » est impressionnant par sa faculté à voler les informations d'authentification de sites de banque électroniques dans les formulaires typiques en contournant la protection SSL. Ce code malveillant a évolué de façon à fournir des logiciels espions », explique Cassius de Oliveira Puodzius, Security Researcher chez ESET en Amérique Latine.

En avril 2016, la version précitée a été rejointe par une variante hybride de Nymaim (Gozi) qui avait pour cible les institutions financières d'Amérique du Nord, mais également en Amérique latine et principalement au Brésil. Cette variante fournit aux cybercriminels le contrôle à distance des ordinateurs compromis plutôt que de chiffrer les fichiers ou bloquer la machine – comme cela se fait habituellement.

En raison des similitudes entre les cibles visées dans chaque pays et les taux de détection, nous pouvons affirmer que les institutions financières restent au centre de cette campagne.

« L'étude complète de cette menace est toujours en cours. Toutefois, si vous pensez que votre ordinateur ou votre réseau a été compromis, nous vous recommandons de vérifier que les adresses IP et les URL que nous avons partagées dans l'article complet de WeLiveSecurity ne se trouvent pas dans votre pare-feu et dans le journal de votre proxy. Nous vous conseillons de mettre en place une stratégie de prévention en ajoutant une liste noire des des adresses IP contactées par ce malware au pare-feu et les URL à un proxy, aussi longtemps que votre réseau prendra en charge ce type de filtrage », conclut Cassius de Oliveira Puodzius.

Pour lire l'intégralité du rapport et ainsi obtenir des informations complémentaires sur le malware Nymaim, cliquez ici.

Réagissez à cet article

Pokémon Go peut-il vraiment prendre le contrôle de votre compte Gmail ?

Pokémon Go peut-il vraiment prendre le contrôle de votre compte Gmail ?

Malgré son succès indéniable, il semblerait que l'application Pokémon Go rencontre des premiers couacs, notamment en matière de protection de la vie privée. Selon certaines informations, depuis démenties, elle pourrait accéder et composer des emails sur le compte Gmail des utilisateurs.

Après avoir soulevé certains problèmes récemment avec le cas des voleurs armés aux États-Unis qui utilisaient le jeu pour cibler leurs victimes ou celui d'une jeune adolescente qui aurait retrouvé un cadavre pendant sa « chasse » aux Pokémon. La polémique n'en finit plus autour de Pokémon Go. C'est aujourd'hui un problème d'éthique et de sécurité qui est désormais pointé du doigt.

Pokémon Go : comment le jeu a rendu fou le monde entier

En effet lorsque vous installez et que vous jouez à Pokémon Go pour la première fois, le jeu sur smartphone développé par la firme Niantic, demande deux types de connexion. La première consiste à créer un compte via l'application tandis que la deuxième exige de se connecter directement depuis son compte Google. C'est la deuxième connexion qui soulève plusieurs problèmes.

Sur son blog, l'analyste en sécurité Adam Reeve expliquait ainsi ce week-end que cette identification par Google pouvait poser plusieurs problèmes puisque l'application accédait à plusieurs paramètres de votre compte Google : « Pokémon Go et Niantic peuvent désormais lire tous vos emails, envoyer des emails de votre part, accéder à vos documents Google Drive, rechercher dans votre historique de recherche et de navigation, accéder à toutes les photos privées hébergées sur Google Photos et bien davantage ». Des accès qui ne sont, bien évidemment, pas nécessaires pour profiter de l'expérience de jeu de l'application développée par Niantic.

Des informations démenties par Google et Niantic

Cependant, interrogé par le site Gizmodo, Adam Reeve a finalement fait marche arrière sur ses affirmations, expliquant ne pas être « certain à cent pour cent » que son billet de blog est exact. Il a par ailleurs expliqué au site Internet qu'il n'avait jamais développé lui-même d'application utilisant l'identification Google et n'a pas expérimenté ce qu'il indiquait sur son blog.

Du côté de Google également, l'information a été démentie auprès de Dan Guido, expert en sécurité informatique. La firme de Mountain View explique que les autorisations de Pokémon Go ne concernent que la partie « Mon Compte » de Google et n'autorise pas d'accès spécifique à différents services.

Enfin, le studio Niantic, qui développe l'application avec The Pokémon Company, a publié ce mardi un communiqué de presse afin de rassurer les utilisateurs : « Pokémon Go n'accède qu'aux informations basiques des profils Google (votre identification et votre adresse email). Aucune autre information de votre compte Google n'est ou ne sera collectée. […] Google réduira prochainement les autorisations de Pokémon Go uniquement aux données de profil dont Pokémon Go a besoin, les utilisateurs n'auront pas besoin d'effectuer le moindre changement ».

Article original de GEOFFROY HUSSON

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 : Pokémon Go peut-elle vraiment prendre contrôle de votre compte Gmail ?