Pokémon Go inquiète l’armée française !

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

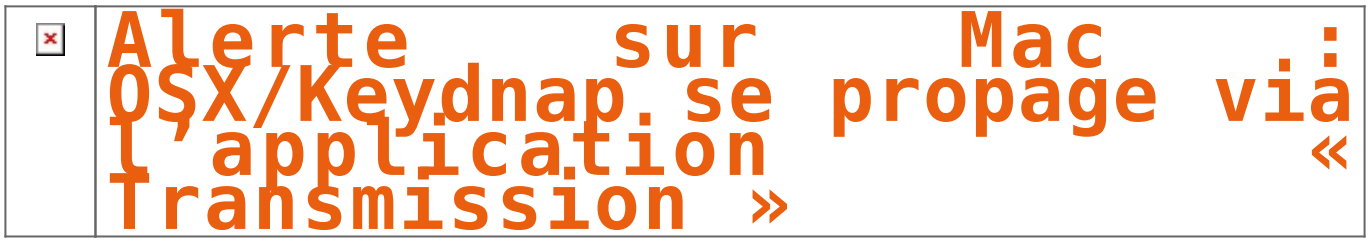
Réagissez à cet article

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

---

Alerte sur Mac : OSX/Keydnap

se propage via l’application « Transmission »



Le mois dernier, les chercheurs d’ESET ont découvert un malware sur Mac OS X nommé OSX/Keydnap, qui exfiltre les mots de passe et clés stockés dans le gestionnaire de mots de passe « KeyChain » ; et qui crée une porte dérobée permanente.
Au moment de la découverte, notre Malware Researcher Marc-Etienne Léveillé expliquait que « tous les utilisateurs d’OS X doivent rester vigilants car nous ne savons toujours pas comment Keydnap est distribué, ni combien de victimes ont été touchées ».

Les équipes ESET viennent de découvrir que le malware OSX/Keydnap se distribue via une version compilée de l’application BitTorrent.

Une réponse instantanée de l’équipe de transmission

Suite à l’alerte donnée par ESET, l’équipe de transmission a supprimé le fichier malveillant de leur serveur Web et a lancé une enquête pour identifier le problème. Au moment de la diffusion de la première alerte, il était impossible de préciser depuis combien de temps le fichier malveillant a été mis à disposition en téléchargement.

Selon les informations de la signature, l’application a été

signée le 28 août 2016, mais ne se serait répandue que le lendemain. Ainsi, les équipes ESET conseillent aux personnes qui ont téléchargé la transmission V2.92 entre le 28 et le 29 août 2016 de vérifier si leur système est compromis en testant la présence de l'un des fichiers ou répertoires suivant :

- /Applications/Transmission.app/Contents/Resources/-License.rtf
- /Volumes/Transmission/Transmission.app/Contents/-Resources/License.rtf
- $HOME/Library/Application Support/com.apple.iCloud.sync.-daemon/icloudsyncd
- $HOME/Library/Application Support/com.apple.iCloud.sync.-daemon/process.id
- $HOME/Library/LaunchAgents/com.apple.iCloud.sync.daemon.-plist
- /Library/Application Support/com.apple.iCloud.sync.-daemon/
- $HOME/Library/LaunchAgents/com.geticloud.icloud.photo.-plist

Si l'un d'eux est présent, cela signifie que l'application malveillante de « transmission » a été exécutée et que le malware Keydnap est probablement en cours d'exécution. Notez également que l'image malicieuse du disque se nomme Transmission 2.92.dmg tandis que l'original se nomme Transmission–2.92.dmg (trait d'union).

Article original de ESET

Pour protéger votre Mac, Denis JACOPINI recommande l'application suivante :

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

Des systèmes biométriques piratés à partir de vos photos Facebook

Des systèmes biométriques piratés à partir de vos photos Facebook

Des chercheurs découvrent comment pirater des systèmes biométriques grâce à Facebook. Les photographies sauvegardées dans les pages de Facebook peuvent permettre de vous espionner.

De nombreuses entreprises de haute technologie considèrent le système de reconnaissance faciale comme l'une des méthodes fiables pour être reconnu par votre ordinateur. J'utilise moi-même la reconnaissance biométrique digitale, rétinienne et du visage pour certaines de mes machines. C'est clairement un des moyens simples et fiables de vérification d'une identité. Cependant, des chercheurs prouvent que la biométrie peut se contourner, dans certains cas, avec une photo, de la colle…

Une nouvelle découverte vient de mettre à mal, cette fois, la reconnaissance faciale mise en place par Facebook. Comme je pouvais vous en parler en 2014, Facebook met en place une reconnaissance faciale que des commerçants Américains ont pu tester avec succès. Des chercheurs ont découvert que cette prouesse technologique n'est pas encore parfaite et sujette au piratage. Des pirates peuvent utiliser votre profil Facebook, et les photos sauvegarder.

Systèmes biométriques

Des étudiants de l'Université de Caroline du Nord ont expliqué lors de la conférence d'Usenix, à Austin, avoir découvert une nouvelle technique particulièrement exaspérante pour intercepter l'intégralité d'un visage, via Facebook. Le rendu 3D et certaines « lumières » peuvent permettre de cartographier votre visage en deux clics de souris. Les chercheurs ont présenté un système qui créé des modèles 3D du visage via les photos trouvées sur Facebook. Leur modèle 3D va réussir ensuite à tromper quatre systèmes de reconnaissance faciale… sur 5 testés : KeyLemon, Mobius, TrueKey, BioID, et 1D.

Pour leur étude, 20 cobayes volontaires ont participé à l'expérience. Leurs photos sont tirées d'espaces publiques comme Facebook, mais aussi LinkedIn et Google+. La modélisation des visages à partir de 27 images différentes va permettre de créer des modèles en 3D, avec des animations faciales : bouches, yeux… Les chercheurs ont reconstruit les visages via les bouts trouvés sur les différentes photographies.

Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : Pirater des systèmes biométriques à partir de vos photos Facebook — Data Security BreachData Security Breach

Filtre anti espion sur les prochains ordinateurs portables Hewlett-Packard

Filtre anti espion sur les prochains ordinateurs portables Hewlett-Packard

Le géant de l'informatique Hewlett-Packard s'associe avec 3M pour préinstaller sur ses prochains ordinateurs portables professionnels un filtre anti espion.

Quoi de plus courant que de croiser à la terrasse d'un café, dans le train ou dans un aéroport ces fiers commerciaux pressés de travailler, même dans un lieu non sécurisé. Autant dire que collecter des données privées, sensibles, en regardant juste l'écran de ces professionnels du « c'est quoi la sécurité informatique ? » est un jeu d'enfant.

Hewlett-Packard (HP), en partenariat avec 3M, se prépare à commercialiser des ordinateurs portables (Elitebook 1040 et Elitebook 840) dont les écrans seront équipés d'un filtre anti voyeur. Un filtre intégré directement dans la machine. Plus besoin d'utiliser une protection extérieure.

Une sécurité supplémentaire pour les utilisateurs, et un argument de vente loin d'être négligeable pour le constructeur. Selon Mike Nash, ancien chef de la division de sécurité de Microsoft et actuellement vice-président de Hewlett-Packard, il est possible de croiser, partout, des utilisateurs d'ordinateurs portables sans aucune protection écran. Bilan, les informations affichés à l'écran peuvent être lues, filmées, photographiées.

Le filtre pourra être activé et désactivé à loisir.

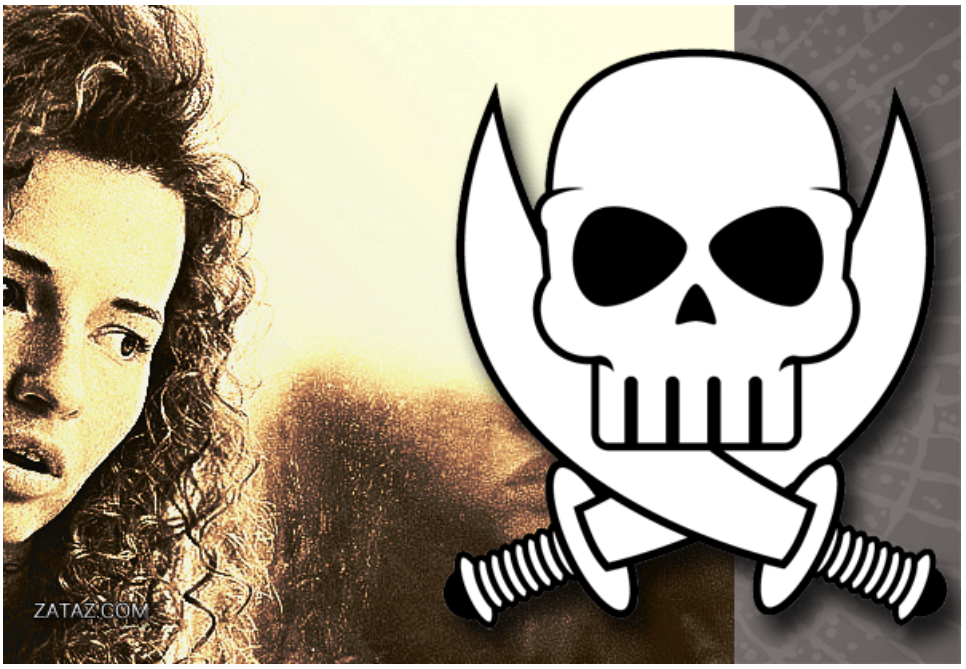
Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : Filtre anti espion sur les prochains Hewlett-Packard – Data Security BreachData Security Breach

---

Des sites de rencontres touchés par des attaques dites de leurre venant du réseau TOR



Des sites de rencontres touchés par des attaques dites de leurre venant du réseau TOR

Les chercheurs mettent en garde contre une augmentation d'attaques par leurre visant les sites de rencontres venant du réseau TOR.
Les attaques par leurre sont montées via un site de rencontres concurrent pour détourner les utilisateurs d'un site victime vers celui de l'attaquant. La plupart de ces attaques ciblent de multiples services de rencontres et diffusent des spams à un grand nombre d'utilisateurs, en les invitant à rejoindre d'autres sites, probablement tous contrôlés par le même pirate. La motivation de l'instigateur de ces attaques semble donc claire, écarter les utilisateurs d'un site victime et les attirer vers le sien.
Les chercheurs d'Imperva ont récemment assisté à une augmentation des pirates utilisant le réseau TOR pour dissimuler leur identité et mener à bien ce type d'attaques.
Les attaques par leurre venant du réseau Tor se caractérisent par des messages en provenance de clients Tor à un taux relativement faible (mais régulier), de 1 à 3 demandes chaque jour, probablement pour passer sous le radar des mécanismes de limite de vitesse et éviter les contrôles de détection automatique des navigateurs. Malgré le taux très faible des demandes qu'Imperva a pu observer, il est probable que le nombre total de celles-ci soit beaucoup plus élevé, avec seulement quelques demandes exposées dans l'aperçu du trafic utilisateurs Tor.
Il faut également prendre en compte le déficit d'image que représente ces attaques menées par les centaines de faux profils très attractifs qui harcèlent les utilisateurs du site victime et qui abaissent la crédibilité de celui-ci.
Selon Itsik Mantin, directeur de la recherche de sécurité à Imperva : « ***Ces attaques ont le potentiel de perturber considérablement le business des opérateurs de site de rencontres. En utilisant le réseau TOR les attaquants sont capables de cacher leur emplacement réel et leurs identités, ce qui les rends encore plus difficiles à détecter et à bloquer*** ».
Afin de se protéger contre les attaques par leurre, il est recommandé aux sites de rencontre de surveiller de près les faux comptes et de fermer tout ce qui pourrait être considéré comme illégitime. Il est également conseillé de monitorer l'ensemble du trafic TOR et de bloquer toute activité suspecte.
Article original de Damien Bancal

Les conseils de Denis JACOPINI
Quelque soit l'e-mail reçu, ceci nous prouve une fois de plus qu'il est nécessaire de décupler notre vigilance. Sachez que le protocole d'envoi des e-mails, le fameux SMTP, se base sur la norme RFC 821 qui date de 1982. Ceci dit, vous comprendrez mieux si je vous dis que ce protocole ne prévoyait pas les dérives d'usages que nous connaissons aujourd'hui.
De nos jours, cette faille, exploitée à outrance par les pirates informatiques, autorise sans aucune difficulté l'usurpation d'identité. Avec les technologies d'aujourd'hui, n'importe qui peut se faire passer pour n'importe qui, et rien ne vous empêche de vous faire passer pour Larry Page ou Serguei Brin (les fondateurs de Google en 1998) en créant une adresse e-mail de type larry.page@gmail.com ou serguei.brin@gmail.com pour peu que ces adresses e-mail ne soient pas prises. Pire, vous pouvez recevoir un e-mail indiquant le vrai nom et la vraie adresse e-mail de votre meilleur ami alors que vous répondre à une adresse e-mail légèrement différente, celle du pirate usurpant l'identité de votre ami…
De qui peut-on encore se fier ?
Besoin de conseils ? de formation ?, contactez Denis JACOPINI

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 Des sites de rencontres touchés par des attaques dites de leurre venant du réseau TOR – ZATAZ

Devez-vous changer votre mot de passe DropBox ?

Devez-vous changer votre mot de passe DropBox ?

On vous demande de créer un nouveau mot de passe sur dropbox.com. Pourquoi et que devez-vous faire ?
L'entité propose de faire des sauvegardes de ses fichiers dans le Cloud, le fameux nuage. Bref, des disques durs hors de chez vous, hors de votre entreprise, sur lesquels vous déposez vos données afin d'y accéder partout dans le monde, et peu importe le support : Ordinateur, smartphone…
Depuis quelques heures, une vague de courriels aux couleurs de DropBox vous indique « ***On me demande de créer un nouveau mot de passe sur dropbox.com. Pourquoi et que dois-je faire ?***« , si les plus paranoïaques ont jeté la missive de peur d'être nez-à-nez avec un phishing, je me suis penché sur le sujet, histoire de m'assurer que l'alerte valait la peine d'être lancée. Je vais être rapide avec le sujet, oui, il s'agit bien d'un courriel officiel de la firme US.

Lors de votre prochaine visite sur dropbox.com, vous serez peut-être invité à créer un nouveau mot de passe. Une modification « ***à titre préventif à certains utilisateurs*** » souligne Dropbox. Les utilisateurs concernés répondent aux critères suivants : ils ont créé un compte Dropbox avant mi-2012 et ils n'ont pas modifié leur mot de passe depuis mi-2012. Vous commencez à comprendre le problème ? Comme je vous le révélais la semaine dernière, des espaces web comme Leakedsource, le site qui met en danger votre vie privée, sont capable de fournir aux pirates une aide précieuse. Comment ? En diffusant les informations collectées dans des bases de données piratées.

Que dois-je faire ?
Si, quand vous accédez à dropbox.com, vous êtes invité à créer un nouveau mot de passe, suivez les instructions sur la page qui s'affiche. Une procédure de modification des mots de passe qui n'a rien d'un hasard. Les équipes en charge de la sécurité de DropBox effectuent une veille permanente des nouvelles menaces pour leurs utilisateurs. Et comme vous l'a révélé ZATAZ, Leaked Source et compagnie fournissent à qui va payer les logins et mots de passe d'utilisateurs qui utilisent toujours le même sésame d'accès, peu importe les sites utilisés. Bref, des clients Adobe, Linkedin … ont peut-être exploité le même mot de passe pour DropBox.
Bilan, les pirates peuvent se servir comme ce fût le cas, par exemple, pour ma révélation concernant le créateur des jeux Vidéo Rush et GarryMod ou encore de ce garde du corps de Poutine et Nicolas Sarkozy. Les informaticiens de Dropbox ont identifié « ***d'anciennes informations d'identification Dropbox (combinaisons d'adresses e-mail et de mots de passe chiffrés) qui auraient été dérobées en 2012. Nos recherches donnent à penser que ces informations d'identification sont liées à un incident de sécurité que nous avions signalé à cette époque***. » termine DropBox.
A titre de précaution, Dropbox demande à l'ensemble de ses utilisateurs qui n'ont pas modifié leur mot de passe depuis mi-2012 de le faire lors de leur prochaine connexion.
Article original de Damien Bancal

Les conseils de Denis JACOPINI
Comme tout e-mail reçu, la prudence est de rigueur. Avant de valider l'authenticité d'un e-mail envoyé par une firme telle que Dropbox, nous avons dû analyser l'entête de l'e-mail reçu et comparer les données techniques de celles répertoriées dans les bases de données connues.
J'imagine que vous n'aurez pas le courage d'apprendre à le faire vous même ni que vous trouverez l'intérêt de consacrer du temps pour ça.
Comme chaque mise à jour demandée par un éditeur ou un constructeur, comme tout changement de mot de passe recommandé par une firme, nous vous conseillons de le faire en allant directement sur le site concerné.
Dans le cas de « Dropbox », nous vous recommandons de rechercher « dropbox.com » dans google ou de taper « dropbox.com » dans votre barre d'adresse et de vous identifier. Vous serez ainsi sur le site officiel et en sécurité pour réaliser la procédure demandée.

Attention
Vous ne serez en sécurité que si votre ordinateur n'est pas déjà infecté. En effet, taper un nouveau mot de passe si votre ordinateur est déjà infecté par un programme espion revient à communiquer au voleur une copie de vos nouvelles clés. Taper l'ancien mot de passe revient aussi à donner au voleur la clé permettant peut-être d'ouvrir d'autres portes !!!

Besoin de conseils ? de formation ?, contactez Denis JACOPINI

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 Changez votre mot de passe DropBox – ZATAZ

La cybercriminalité a de belles années devant elle

La cybercriminalité a de belles années devant elle

Les prochaines années laissent entrevoir de beaux moments pour les cybercriminels de tout acabit. Les raisons expliquant cela sont nombreuses. Quelles sont-elles?

Suivre la scène de la sécurité informatique a ceci de particulier : c'est à la fois fascinant et grandement décourageant. C'est d'autant plus décourageant que les tendances présentes au cours des derniers mois laissent entrevoir de beaux jours pour les cybercriminels. Essentiellement, quatre raisons expliquent cela.

La multiplication des cibles potentielles

La première raison est assez évidente : il y a de plus en plus de cibles disponibles pour les criminels. La surmultiplication du nombre de plateformes exploitant Internet a pour effet de toutes les transformer en des opportunités potentielles pour des gens malintentionnés. La manifestation la plus flagrante de cette surmultiplication se transpose dans la fulgurante montée de l'Internet des objets.
Ce nouvel eldorado porte toutefois les gènes de sa propre insécurité. En effet, le marché est meublé par une multitude de joueurs, et leur intérêt porté à la chose sécuritaire est tout aussi variable. Ainsi, alors que l'objectif est d'occuper le marché le plus rapidement possible, bon nombre de joueurs impliqués dans la course à l'Internet des objets arrivent sur le marché avec des produits qui sont, volontairement ou involontairement, plus ou moins sécurisés.
Bref, nous sommes placés devant un cercle vicieux duquel nous ne pouvons pas nous sortir : plus de technologies signifient nécessairement plus de vulnérabilités et, conséquemment, plus d'opportunités criminelles. De plus, croire que l'on puisse mettre un frein à l'évolution technologique est illusoire.

Le difficile marché de la sécurité

Le contexte actuel rend les ressources extrêmement difficiles à conserver ou à acquérir pour les petites et moyennes entreprises qui n'ont pas les moyens d'offrir des salaires élevés.
Alors que le domaine apparaît comme extrêmement complexe, le manque criant de main-d'œuvre est de plus en plus problématique dans les entreprises. Forbes affirme pourtant que ce secteur vaudra sous peu 75 milliards de dollars US et que le marché créera plus d'un million d'emplois.
Non seulement manque-t-il de spécialistes en sécurité, mais il manque aussi de plus en plus de pirates black hat sur le marché, faisant en sorte que les cybercriminels eux-mêmes se tournent de plus en plus vers des modèles de sous-traitance pour effectuer leurs opérations.
Ce manque d'expertise a pour effet de rendre l'économie globalement plus ou moins axée sur la sécurité. Certes, certains secteurs ont les moyens de leurs ambitions, mais le contexte actuel rend ces ressources extrêmement difficiles à conserver ou à acquérir pour les petites et moyennes entreprises qui n'ont pas les moyens d'offrir des salaires élevés. Les effets sont bien sûr conséquents : la situation engendre une sécurité bien inégale, avec le lot de vulnérabilités qu'elle impose.

La rentabilité évidente

Autre point extrêmement important pour expliquer pourquoi la cybercriminalité aura le vent dans les voiles? C'est lucratif. La logique criminelle est relativement simple : il s'agit de faire le plus d'argent possible, le plus facilement possible. En somme, c'est le capitalisme en action.
Dans le domaine de la cybercriminalité, cela fonctionne décidément. On estime à 445 milliards de dollars US le marché de la cybercriminalité. Bon, je vous entends déjà geindre et dire que c'est fort de café. Soit. Admettons que ce soit la moitié moins, c'est tout de même 222 milliards, batinse!
Pour rappel, le budget du Canada est d'environ 290 milliards de dollars CA. C'est donc payant, et c'est bien dommage, mais les conséquences de la cybercriminalité sont minimes. Les chances d'arrêter les criminels sont plutôt basses (voir point suivant) et les peines encourues ne sont pas adaptées.

L'incapacité d'action des agences d'application de la loi

Les cybercriminels ont donc le beau jeu, puisque le risque de se faire prendre est extrêmement bas. En effet, les forces policières sont mal équipées pour confronter la cybercriminalité, faisant en sorte que trop souvent, elles doivent capituler devant les actions commises par les criminels. Dans les cas les plus extrêmes, les agences tenteront de déployer les efforts nécessaires pour faire culminer une enquête, mais cela se fera à grands coups de contrats avec le secteur privé afin de se procurer l'expertise nécessaire pour résoudre le crime en question. Le fait que le FBI ait versé un montant de 1,3 million à un groupe de «chercheurs en sécurité», considérés par plusieurs comme ayant des mœurs on ne peut plus douteuses, pour accéder aux données présentes dans l'iPhone du terroriste de San Bernardino en est, en soi, la manifestation la plus éloquente.
Lutter contre la cybercriminalité demande essentiellement quatre choses. Une culture particulière, une collaboration internationale, des moyens et des techniques disponibles, et des compétences de pointe dans le domaine des technologies. Le dur constat qu'il faut faire, c'est qu'outre la collaboration internationale, les autorités compétentes n'ont pas les moyens pour atteindre les trois autres prérequis. Par conséquent, la vaste majorité des corps policiers ne s'attaqueront aux cybercrimes que lorsque les infractions sont trop exagérées.

La somme de toutes les peurs

Au final, ce qui est le plus inquiétant dans cette situation, c'est que plus le temps avance, plus les réseaux de cybercriminels deviennent solides, sophistiqués et ont de plus en plus de moyens. Les laisser agir en toute impunité a pour effet de les rendre toujours plus coriaces, ce qui rendra la tâche de lutter contre eux d'autant plus difficile à long terme. Il faudra que l'on prenne le problème à bras le corps une fois pour toute, sinon, nous risquons d'avoir de mauvaises surprises dans les prochaines années.
Article original de branchez-vous.com

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 : La cybercriminalité a de belles années devant elle | Branchez-vous

---

Les services de renseignement devraient-ils avoir accès aux clés de déchiffrement ?

Les services de renseignement devraient-ils avoir accès aux clés de déchiffrement ?

Une initiative franco-allemande va tenter de convaincre les acteurs internationaux d'Internet et de l'informatique de la nécessité d'ouvrir leurs codes et leurs chiffrements pour lutter contre le terrorisme. Des voix s'élèvent au nom de la sécurité et des libertés.

Après le conseil restreint de Défense à l'Élysée le 4 août 2016, le ministre de l'Intérieur, Bernard Cazeneuve, a parlé chiffre. Avec son homologue allemand, Thomas de Maizière, il a proposé le 23 août une initiative européenne à vocation internationale pour « faire face au défi du chiffrement, une question centrale dans la lutte antiterroriste ». Le sujet est brûlant. Pas seulement depuis l'assassinat du père Hamel par des usagers de Telegram , d'ailleurs pas considéré comme la solution la plus hermétique d'un marché en plein essor.
Outre Telegram, les terroristes, des criminels et des gens très soucieux de l'intégrité de leurs communications utilisent pléthore de dispositifs de chiffrement comme ChatSecure, Conversations, Kontalk, Signal, Threema ou WhatsApp (même s'il appartient à Facebook depuis 2014), sans parler des anonymes Tor (réseau décentralisé) ou ToX (pair à pair). Là n'est d'ailleurs pas la question centrale. L'ennemi pourrait émigrer vers d'autres cieux numériques voire créer son propre outil chiffré…

Incapable de casser le code

Depuis l'audition à l'Assemblée le 10 mai de Patrick Calvar, le directeur général de la sécurité intérieure, la pression monte. Pour les attentats de Bruxelles, le DGSI avoue que « même une interception n'aurait pas permis de mettre au jour les projets envisagés puisque les communications étaient chiffrées sans que personne soit capable de casser le chiffrement ». Face au chiffrement aléatoire et autres complications futures, le DGSI a une réponse martiale : « Je crois que la seule façon de résoudre ce problème est de contraindre les opérateurs. » Nous y voilà. En février, le FBI s'est heurté au refus d'Apple de livrer les données de l'iPhone d'un des meurtriers de Daech qui a tué 14 personnes à San Bernardino le 2 décembre 2015. Avant que le FBI n'annonce avoir réussi à casser le chiffre de la pomme…
Bernard Cazeneuve ne dit pas autre chose. Il prend pour exemple sa négociation avec les majors d'Internet en février 2015 qui a permis d'élaborer une charte sur le retrait des contenus et le blocage des sites haineux. « Sur le chiffrement, il faut que nous ayons la même méthode, la même volonté, le sujet est crucial. »
Sauf qu'un courrier, publié par Libération, du directeur de l'Agence nationale de sécurité des systèmes d'information (ANSSI) et lui-même cryptologue, Guillaume Poupard, affirme le contraire aux autorités : « Un affaiblissement généralisé serait attentatoire à la sécurité numérique et aux libertés de l'immense majorité des utilisateurs. » Permettre une intrusion des services de renseignement (par des « portes dérobées ») pourrait profiter à des gens ou des États (pas seulement islamiques) mal intentionnés. Quelle tendance va l'emporter ? En cette époque sécuritaire, de l'état d'urgence éternel et du désarroi politique…
Article original de Olivier Berger

Réagissez à cet article

Original de l’article mis en page : Lutte contre le terrorisme : Faut-il ouvrir la porte du chiffrement aux services de renseignement ? – La Voix du Nord

---

Peur d’être surveillés ? mettez à jour votre iPhone

Peur d’être surveillés ? mettez à jour votre iPhone

Original de l’article mis en page : Trois failles zero day d’iOS servaient à espionner des dissidents

---

Ransomware : Locky se fait passer pour un fichier système Windows

Alerte : le Ransomware Locky se fait passer pour un fichier système Windows

Une variante du ransomware Locky se fait passer pour un fichier DLL dans l'espoir de tromper les filtres de sécurité.

Toujours plus vicieux. Le ou les groupes de cybercriminels qui se cachent derrière le Locky ne cessent de faire évoluer l'un des plus populaires ransomware de la Toile. Objectif : déjouer les dernières mises à jour des solutions de protection et attraper toujours plus de victimes dans les filets. Victimes qui, rappelons-le, n'auront d'autre choix que de payer une rançon (généralement en bitcoin) pour récupérer leurs données si elles n'ont pas pris soin de faire des sauvegardes.
Aux dernières nouvelles, la dernière variante de Locky se distingue en se cachant derrière un fichier .DLL et non plus derrière un .EXE comme précédemment. Les DLL (Dynamic Link Library) sont des bibliothèques logicielles exploitées par Windows pour exécuter une application. « Ce que nous trouvons le plus intéressant dans cette dernière vague Locky est qu'au lieu de télécharger un binaire EXE, ce composant ransomware arrive maintenant en tant que binaire DLL, soulignent les chercheurs en sécurité de Cyren. Qui plus est, le fichier DLL ainsi téléchargé est personnalisé pour empêcher les scanners de virus de le détecter facilement. »

Attention au zip
Si le DLL parvient à passer les filtres de sécurité, son exécution reste identique à celle constatée jusqu'à présent, à savoir que le rançongiciel part à la recherche de fichiers à chiffrer avant de rediriger ses victimes vers une page affichant la facture (et la méthodologie du mode de paiement). Petite variante, le mécanisme d'attaque attribue l'extension .zepto aux fichiers devenus illisibles. « Comparé aux précédentes, cette nouvelle variante ajoute un autre niveau d'obscurcissement qui déchiffre et exécute le réel script chargé du téléchargement de Locky », constatent toutefois les chercheurs.
Le mode de distribution et d'infection de JS/Locky.AT!Eldorado, nom de cette nouvelle variante de Locky, n'a, lui, pas changé : il tente toujours de se propager par l'envoi d'un e-mail trompeur invitant à cliquer sur une pièce jointe au format ZIP renfermant le code Javascript qui va déclencher la décompression des fichiers et l'exécution des commandes de téléchargement de l'agent infectieux proprement dit. Etre doublement attentif lors de la réception de ce genre d'e-mail (et éviter de cliquer sur des fichiers ZIP sans être absolument certain de leur origine) reste le meilleur moyen d'éviter de l'infection.

Article original de Christophe Lagane

Réagissez à cet article

Original de l’article mis en page : Ransomware : Locky se fait passer pour un fichier système Windows