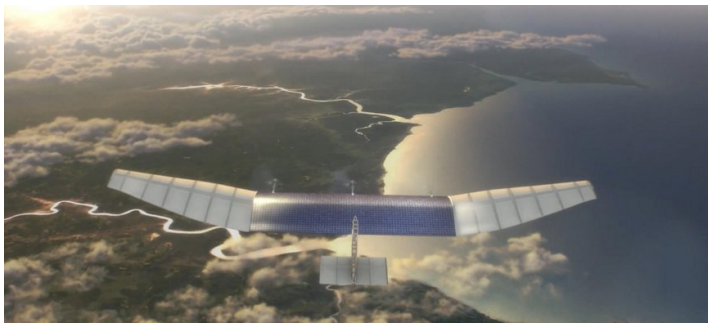
Boeing planche sur des drones capables de déployer des logiciels espions | Le Net Expert Informatique



Boeing planche sur des drones capables de déployer des logiciels espions

Le spécialiste de l'aéronautique Boeing travaille sur la production de drones capables d'infecter les ordinateurs et smartphones aux alentours.

En début de mois, nous apprenions que la société milanaise Hacking Team, qui propose des outils d'interception des communications entre internautes aux gouvernements ou aux pouvoirs publics, avait elle-même été hackée. Quelque 400 gigaoctets de données confidentielles ont été récupérés révélant la nature des relations entre Hacking Team et ses partenaires. Ces documents sont mis à disposition sur le site Wikileaks.
Parmi les informations révélées, la filiale Insitu de Boeing, spécialisée dans la production de drones, avait signé un partenariat avec Hacking Team afin de procéder à des hacks à distance. L'appareil serait ainsi en mesure de cibler un smartphone ou un ordinateur portable en particulier puis de l'infiltrer via un réseau Wi-Fi.
Selon le magazine The Intercept, qui rapporte l'information, le drone en question est prévu pour pouvoir accéder aux fichiers à distance, récupérer le journal des appels, l'historique des messageries instantanées ou encore les emails.
Au sein des emails aspirés sur les serveurs de Hacking team, nous trouvons notamment une feuille de route datant du mois de juin. Celle-ci fait mention d'un petit appareil pouvant être transporté par un drone et capable de récupérer les données transitant via les réseaux.
Le document explique que l'attaque devra prendre en charge Windows 10 ainsi que le navigateur Microsoft Edge et Skype Web. Sur OS X, Hacking Team a finalisé un dispositif scannant les sauvegardes locales d'iTunes et planchait sur la capture des certificats d'iCloud et des images de l'application Photos.
Retrouvez tous les détails de ce projet en italien sur cette page.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/spyware-logiciel-espion/actualite-774222-boeing-planche-drones-capables-deployer-spyware.html

---

Attention aux arnaqueurs qui sévissent sur le site Immoweb

! | Le Net Expert Informatique

Attention aux arnaqueurs qui sévissent sur le site Immoweb !

Avec l'été, les fausses petites annonces pour des lieux de villégiature fleurissent sur les sites internet. Et dans quelques semaines, ce sera au tour des faux kots pour étudiants.

Le modus operandi des arnaqueurs est simple : on vous appâte avec un bien à louer à prix cassé. Puis, on vous demande une caution, à verser via un mandat postal ou Western Union. Et vous êtes quitte de votre argent… Immoweb tire la sonnette d'alarme. L'arnaque en question n'est pas nouvelle, mais elle a repris de plus belle avec l'arrivée des vacances scolaires. Pour l'instant, ce sont principalement des annonces pour des lieux de villégiature qui se révèlent fausses. « On peut ainsi voir une maison dans le sud de la France ou dans un lieu exotique, à un prix dérisoire », explique Olivier Bogaert, commissaire à la Computer Crime Unit, l'unité spécialisée dans la cybercriminalité de la police fédérale.
Le candidat locataire tombe sous le charme des photos alléchantes, et du prix cassé. Et il contacte via le site internet le propriétaire. Les discussions quittent alors l'espace du site internet où était placée l'annonce.
« Le propriétaire peut expliquer qu'il avait un locataire qui s'est désisté au dernier moment et qu'il baisse donc le prix, ou qu'il recherche surtout à ce que sa maison ou son appartement ne reste pas vide. Il est souvent à l'étranger, de sorte qu'il demande à ce que vous versiez un acompte ou le loyer via Western Union, ou via une banque étrangère. Il peut aussi demander à ce que vous lui envoyiez une carte de crédit prépayée, que vous aurez crédité d'un certain montant ».

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.sudinfo.be/1334805/article/2015-07-17/immoweb-previent-ses-utilisateurs-attention-aux-arnaqueurs-qui-sevissent-sur-le

---

Les salariés doivent aussi prendre conscience des conséquences des failles de sécurité | Le Net Expert

Informatique

	**Les salariés doivent aussi prendre conscience des conséquences des failles de sécurité**

Lors des Assises de la Sécurité MobileIron présentera sa plateforme conçue pour sécuriser et gérer les systèmes d'exploitation tout en préservant la confidentialité des données personnelles. Pour Sid-Ahmed Lazizi, Directeur Général France, MobileIron Il est essentiel de faire prendre conscience aux salariés des conséquences potentielles des failles de sécurité, tout comme définir le type de données auquel on peut ou ne peut pas accéder depuis un appareil portable.

Global Security Mag : Qu'allez-vous présenter à l'occasion des Assises de la Sécurité ?
Sid-Ahmed Lazizi : Lors des Assises de la Sécurité, MobileIron présentera sa plateforme conçue pour sécuriser et gérer les systèmes d'exploitation modernes dans le cadre d'une utilisation de terminaux divers et variés. Elle prend en compte l'identité, le contexte et les règles de confidentialité établies pour définir le niveau approprié d'accès aux données et services des entreprises. MobileIron sécurise les données statiques sur les terminaux, dans les applications et dans le cloud. Son action de sécurisation porte également sur les data-in-motion (données dynamiques) lorsqu'elles circulent entre le réseau d'une entreprise, les terminaux et les référentiels de stockage. Grâce à MobileIron, les services informatiques peuvent assurer la sécurité des données des entreprises où qu'elles soient, tout en préservant la confidentialité des données personnelles des employés. Cette plateforme se compose de trois produits :
MobileIron Core : serveur qui permet aux services informatiques de définir des règles de sécurité et de gestion sur les systèmes d'exploitation mobiles les plus répandus
MobileIron Client : logiciel qui réside sur les appareils afin d'y appliquer les règles définies par le service informatique
MobileIron Sentry : passerelle intelligente qui sécurise le trafic des données entre les appareils mobiles et les systèmes back-end de l'entreprise

GS Mag : Quelle va être le thème de votre conférence cette année ?
Sid-Ahmed Lazizi : Le thème de notre conférence qui aura lieu le 2 octobre à 11h est « Le nouveau modèle de sécurité en entreprise ». Les employés choisissent de plus en plus de travailler sur des terminaux mobiles dotés de systèmes d'exploitation modernes tels que Android, iOS ou Windows 10, et ce en lieu et place des ordinateurs de bureau traditionnels et des outils conçus pour Windows. Le défi engendré en termes de sécurité par ces nouveaux systèmes d'exploitation est bien différent de ceux de l'ancienne ère du PC, ce qui nécessite d'aborder la situation sous un autre angle et d'utiliser une technologie nouvelle.

GS Mag : Quel est votre message aux RSSI ?
Sid-Ahmed Lazizi : À mesure que les terminaux mobiles et objets connectés se multiplient, s'adaptent et intègrent le monde de l'entreprise, les services informatiques découvrent de nouvelles menaces qui pèsent sur les données et doivent relever de nouveaux défis pour les protéger. Ils doivent repenser leurs stratégies et infrastructures informatiques pour permettre une utilisation sûre et efficace de ces terminaux et objets, qui représentent une véritable opportunité d'augmenter la productivité des collaborateurs de l'entreprise.
Les technologies portables étant relativement récentes, elles se développent et s'améliorent constamment. Elles présentent le même défi que celui des smartphones quand ces derniers sont apparus. En effet, lorsque les technologies mobiles ont commencé à s'imposer, la réponse initiale des directions informatiques fut de réguler ou restreindre les accès mobiles. Cette approche s'est révélée majoritairement inefficace, les employés trouvant de plus en plus de solutions pour contourner les recommandations de leur département IT.
Liés aux smartphones, les technologies portables vont très rapidement débarquer en entreprise Etant donné que la restriction n'est pas toujours une option viable, reste le problème de la sécurité des données. Pour commencer, les départements informatiques devraient se concentrer sur les plateformes qui permettent de gérer et de sécuriser au niveau fichier, ce que certaines sociétés avancées font déjà sur mobile. Ces types de services garantissent la protection des données de l'entreprise même si le dépôt central de stockage des données est corrompu.
Les départements informatiques devront également travailler main dans la main avec les équipes RH et juridique pour définir un cadre d'utilisation clair de ces appareils mobiles au sein de l'entreprise, tout comme rappeler les risques de sécurité induits par l'accès aux données de l'entreprise sur des appareils portables ou similaires. Idéalement, ces règlements devraient être communiqués aux employés de façon positive pour valider le potentiel d'exploitation des appareils mobiles à la fois sur le plan professionnel et personnel.

Il est essentiel de faire prendre conscience aux salariés des conséquences potentielles des failles de sécurité, tout comme définir le type de données auquel on peut ou ne peut pas accéder depuis un appareil portable. Cela permettra de favoriser la relation de confiance entre les directions informatiques et les employés.

Source : https://www.globalsecuritymag.fr/Sid-Ahmed-Lazizi-MobileIron-Les,20150716,54434.html

---

Augmentation de la taille moyenne d'attaques DDoS | iTPro.fr | Le Net Expert

Informatique

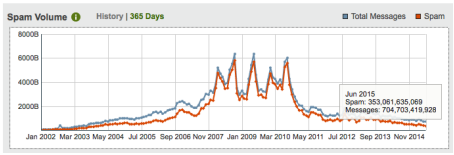
Augmentation de la taille moyenne d'attaques DDoS

Arbor Networks, spécialiste de la protection contre les attaques DDoS, publie ses statistiques relatives aux attaques DDoS pour ce second trimestre.

Tant en bits par seconde qu'en paquets par seconde, il semblerait que les attaques de type DDoS soient de plus en plus imposantes. L'attaque la plus forte de ce second trimestre de type « UDP Flood » a atteint 196 bits/s. Le problème réside surtout dans le fait que cette amplitude n'est plus aussi rare qu'auparavant.Au deuxième trimestre, 21 % d'entre elles ont dépassé 1 Gbit/s, la progression la plus forte enregistrée étant celle dans la fourchette des 2 à 10 Gbit/s. Le mois de juin a aussi été marqué par l'augmentation des attaques entre 50 et 100 Gbit/s principalement de type « SYN Flood » ciblant le Canada et les Etats-Unis.
Darren Anstee, directeur des technologies de sécurité pour Arbor Networks explique que« si les attaques d'une ampleur extrême monopolisent les gros titres, c'est la progression de la taille moyenne des attaques DDoS qui inquiète les entreprises à travers le monde. Les entreprises doivent définir clairement leur risque en matière de DDoS. Face à des attaques moyennes capables de saturer l'accès Internet de bon nombre d'entreprises, il est essentiel de saisir les risques et les coûts d'une attaque et de mettre en place les plans, services et solutions appropriés. »
Du côté des attaques par amplification et réflexion, il semblerait que celles exploitant SSDP soient en baisse puisque 84 000 ont été détectées au second trimestre contre 126 000 au deuxième. Cependant, la taille moyenne des attaques d'amplification par réflexion DNS, NTP, SSDP et Chargen a augmenté au deuxième trimestre 2015 et 50 % de ce type d'attaques ciblaient le port UDP 80 (HTTP/U) pour une durée de 20 minutes (contre 19 pour le premier). A noter que ce type d'attaque permet d'amplifier la volumétrie du trafic par un nombre de réponses envoyé plus important tout en masquant les sources. Cette technique exploite notamment le manque de mesures mises en place par les opérateurs pour filtrer le trafic et la mauvaise configuration d'équipement fournissant des services UDP.

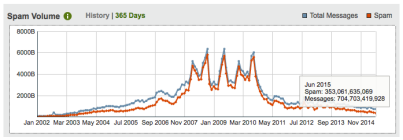
Source : http://www.itpro.fr/n/augmentation-taille-moyenne-dattaques-ddos-21404/

Le spam est à son niveau le plus bas | Le Net Expert Informatique



Le spam est à son niveau le plus bas

Aurons-nous finalement raison du spam ? Il semblerait en tout cas que les efforts menés sur ce secteur commencent à porter leurs fruits selon un rapport du cabinet Symantec.
Les analystes de Symantec ont publié leur rapport de sécurité portant sur le mois de juin. Selon les chiffres internes, le taux de spam sur l'ensemble des emails envoyés le mois dernier n'était que de 49,7%. « C'est la première fois depuis plus de dix ans que ce taux passe sous la barre des 50% », expliquent ainsi les experts. Plus précisément, la proportion de courriers indésirables est donc à son plus bas depuis le mois de septembre 2003.
Symantec affirme que les actions en justice menées contre les réseaux criminels contrôlant les réseaux de botnets portent véritablement leurs fruits. Il est possible que le spam ne soit plus une source de revenus stables pour les cybercriminels.



Symantec ajoute que le taux d'attaques par phishing ou le déploiement de malware par email est également en baisse. En revanche, sur le mois de juin, 57,6 millions de nouvelles variantes de malware ont été identifiées, contre 44,5 millions au mois de mai et 29,2 millions en avril. Cela signifie donc que si les activités criminelles ne ralentissent pas, elles sont désormais effectuées de manière différente (par exemple via les réseaux communautaires, la messagerie instantanée, les applications mobiles ou les pages Web malveillantes).
Récemment, l'équipe de Gmail annonçait avoir optimisé l'intelligence artificielle appliquée aux filtres anti-spam avec un réseau de neurones artificiels. Les algorithmes s'en trouvent alors plus performants et devraient être capables de mieux discerner les courriers indésirables. En octobre dernier, Microsoft expliquait pour sa part bloquer 10 millions de spams chaque minute. La firme de Redmond a notamment participé à la fermeture de plusieurs botnets.
Consulter le rapport dans son intégralité sur cette page (PDF)

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/spam-pourriel/actualite-773950-spam-niveau-bas-12-ans.html?estat_svc=s%3D223023201608%26crmID%3D639453874_1070073452#pid=22889469

Inquiétude sur les données de connexion | Le Net Expert

Informatique

Inquiétude sur les données de connexion

C’est, pour le Conseil constitutionnel, un petit tour de chauffe avant sa décision, vendredi 24 juillet, sur la loi renseignement, un mois après avoir été saisi par le président de la République et 106 parlementaires. Le Conseil examinait en effet, mardi 21 juillet, une question prioritaire de constitutionnalité (QPC), transmise par le Conseil d’Etat, sur la délicate surveillance des données Internet.

Trois associations (French Data Network, la Quadrature du Net et la Fédération des fournisseurs d’accès à Internet associatifs) attaquaient un article décisif, repris par la loi renseignement, de la loi de programmation militaire de décembre 2013 sur « l’accès administratif [policier] aux données de connexion » qu’elles jugent contraire « aux droits au respect de la vie privée, à un procès équitable et à la liberté de communication ».
Les associations s’inquiètent d’une mesure, introduite dans le code de la sécurité intérieure, qui autorise « le recueil, auprès des opérateurs de communications électroniques, (…) des informations et documents traités ou conservés par leurs réseaux ».

Que sont exactement ces « informations et documents » ? Les données de connexion ? Le contenu des correspondances ?
La loi ne le dit pas et a donc, pour les associations, délégué au pouvoir réglementaire – à l’administration – le soin de faire pour le mieux. Ça ne se fait pas. Le Conseil constitutionnel supporte mal de voir « reporter sur des autorités administratives ou juridictionnelles le soin de fixer des règles dont la détermination…
Lire la suite….

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.lemonde.fr/societe/article/2015/07/22/inquietude-sur-les-donnees-de-connexion_4693599_3224.html
Par Franck Johannès

Déjà des backdoors et keyloggers pour Windows 10 chez Hacking Team | Le Net Expert Informatique

Déjà des backdoors et keyloggers pour Windows 10 chez Hacking Team

Anticipant sur les besoins de ses clients, Hacking Team s'est assuré d'être prêt au lancement de Windows 10. La société italienne a adapté ses outils pour être capable d'installer un backdoor sous Windows 10, et ainsi de pouvoir collecter à distance toutes les frappes de touches au clavier.

Windows 10 n'est pas encore officiellement sorti, mais les firmes qui fournissent aux autorités les outils permettant d'accéder à distance aux données sont déjà à pied d'oeuvre pour s'adapter au niveau système d'exploitation de Microsoft. Ainsi l'entreprise italienne Hacking Team, dont les e-mails ont fuité ce mois-ci, s'est assurée dès l'an dernier de pouvoir fournir à ses clients de quoi espionner des utilisateurs de Windows 10.

« Nous avons testé Windows 10 Preview et ça fonctionne », a ainsi expliqué Marco Valleri, le directeur de Hacking Team, dans un e-mail du 4 novembre 2014. Il répondait à l'ancien responsable des opérations à Singapour, Serge Woon, qui se demandait si « RCS 9.4 supporte Windows 8.2 » (en fait Windows 10). RCS est l'acronyme de « Remote Control System », le malware qui permet à Hacking Team de prendre à distance le contrôle d'un ordinateur pour accéder à ses données.

Un autre e-mail du 29 juin 2015 montre que deux employés de Hacking Team, Marco Fontana et Andrea Di Pasquale, ont testé avec succès l'installation hors ligne de plusieurs outils sur Windows 10 Enterprise Insider Preview. Ils disent avoir vérifié notamment « l'installation d'un backdoor », « l'exportation de preuves depuis le backdoor », et la « désinstallation du backdoor ».

« Super ! », s'enthousiasme le directeur technique Marco Valleri, qui propose aussitôt une réunion pour déployer la mise à jour dans un git, probablement celui de RCS.

La société Hacking Team dispose également d'un outil invisible pour Windows 10 permettant de collecter toutes les frappes de touches au clavier (un « keylogger »), comme le montre un courriel du 5 juin. Marco Fontana, qui semble être une petite star dans l'entreprise, y rend compte d'une réunion du mercredi 3 juin 2015, où « l'un des thèmes de la réunion était le test du mécanisme d'injection dans l'application Metro ».

Il explique que « le POC du keylogger pour Windows 10 est prêt et peut être testé pour vérifier sa « compatibilité » avec les antivirus ». Le POC (Proof-of-concept) est une démonstration de faisabilité.

Dans un e-mail du 15 juin, Marco Fontana précise à son équipe qu'il a testé une « technique d'injection dans l'application Metro de Windows 10 », et que « l'exécutable 'ExeLoader' injecte la DLL ApiHookDll dans un processeur notepad.exe et capture les touches ». Il s'agit d'un POC visant à collecter les touches tapées sous sur l'application « Bloc Notes » de Windows 10.

« Si tout fonctionne correctement, dans le dossier temporaire de Windows (%temp%) vous verrez un fichier texte créé qui contient les touches enfoncées dans notepad. Le fichier a un préfixe KBD_ et une valeur aléatoire (ex: KBD_000407E600C553CE.txt) ».

Tout l'objet du logiciel RCS de Hacking Team est justement d'installer à distance les backdoors qui permettent d'installer des outils tels que ce keylogger, lequel permet ensuite de récupérer, par exemple, les mots de passe saisis pour accéder à des comptes e-mail, ou des mots de passe de clés de chiffrement.

« On ne peut pas croire à la sécurité d'un OS pour le grand public », s'était amusé en novembre dernier David Vincenzetti, le président de Hacking Team, en lisant une actualité selon laquelle Windows 10 pourrait signer la fin des malwares.

Source : http://www.numerama.com/magazine/33727-deja-des-backdoors-et-keyloggers-pour-windows-10-chez-hacking-team.html
par Guillaume Champeau

Hacking Team a travaillé sur un drone capable d'infecter des ordinateurs à distance | Le Net Expert Informatique

Hacking Team a travaillé sur un drone capable d'infecter des ordinateurs à distance

De nouvelles informations émergent des centaines de milliers d'e-mails piratés au fabricant de logiciels espions Hacking Team. Des échanges ont montré que l'entreprise italienne a été contactée par Insitu, un fabricant de drones appartenant à Boeing, pour travailler sur un système qui permettrait aux engins de pirater des réseaux Wi-Fi à distance, a relevé le site The Intercept.

Un rapport daté du 1er juillet montre d'ailleurs qu'Hacking Team travaillait sur un système d'injection réseau utilisable par drone, c'est-à-dire « un équipement conçu pour insérer du code malicieux dans les communications d'un réseau Wi-Fi », explique le site spécialisé Ars Technica.

« Nous ne pouvons vendre nos produits qu'à des entités gouvernementales »

Selon un premier e-mail envoyé en avril, Insitu s'est montré intéressé par une présentation de Hacking Team à l'IDEX 2015, un salon de la défense qui s'est tenu aux Emirats arabes unis en février. « Nous aimerions potentiellement intégrer votre système de piratage de Wi-Fi à un système aérien et nous souhaiterions prendre contact avec un de vos ingénieurs qui pourrait nous expliquer, plus en détail, les capacités de l'outil, notamment la taille, le poids et les spécifications de votre système Galileo [un logiciel espion] », écrit alors Giuseppe Venneri, ingénieur mécanique en formation chez Insitu.

« Gardez à l'esprit que nous ne pouvons vendre nos produits qu'à des entités gouvernementales », répond un responsable de Hacking Team, sans fermer la porte à une collaboration. Selon un e-mail interne, le même responsable de Hacking Team indique qu'Insitu travaille avec des agences gouvernementales et demande quels produits seraient les plus adaptés à la demande du fabricant.

Aucun accord trouvé

La correspondance entre Insitu et Hacking Team s'est arrêtée en mai et a été fortement retardée par des discussions d'ordre légal, chaque entreprise souhaitant utiliser son propre accord de non-divulgation avant de démarrer les discussions commerciales. Les courriels les plus récents suggèrent que les négociations n'ont jamais commencé.

Le vendeur de logiciels espions italien Hacking Team est sous pression depuis un piratage qui a conduit à la publication de plus de 400 gigabits de données confidentielles début juillet. Certains documents indiquent notamment que l'entreprise pourrait avoir vendu des solutions de surveillance à des pays sous embargo comme le Soudan et la Russie.

Source : http://www.lemonde.fr/pixels/article/2015/07/20/hacking-team-a-travaille-sur-un-drone-capable-d-infecter-des-ordinateurs-a-distance_4691260_4408996.html
Par Florian Reynaud

Ashley Madison tente de rassurer ses clients infidèles | Le Net Expert Informatique

12	Ashley Madison tente de rassurer ses clients infidèles

Alors qu'un maître-chanteur menace de diffuser un fichier de près de 40 millions d'hommes et de femmes inscrits sur Ashley Madison pour tromper leur conjoint, l'éditeur affirme qu'il a trouvé la parade : la loi américaine de protection du droit d'auteur.

Ce matin, nous rapportions que l'éditeur canadien du site de rencontres adultères Ashley Madison s'était fait pirater une base de données avec les noms de quelques 37 millions d'utilisateurs du service qui promet discrétion et anonymat. Alors qu'ils n'en ont publié que des extraits, les hackers promettent de publier l'intégralité de la base de données sur internet si la société Avid Life Media basée à Toronto ne ferme pas Ashley Madison et deux autres sites internet qu'elle édite.
Mais l'entreprise n'entend visiblement pas céder aux pressions et essaye de rassurer tant bien que faire se peut ses clients. Dans un communiqué envoyé à Numerama, Avid Life Media explique les contre-mesures mises en place, qui pourraient toutefois s'avérer vaines si les hackers décidaient de mettre leurs menaces à exécution et de passer par un réseau P2P incontrôlable comme BitTorrent pour publier la base de données intégrale. La société mise sur la loi américaine sur le droit d'auteur sur internet (le DMCA) qui impose aux plateformes de supprimer les contenus publiés sans l'autorisation des ayants droit lorsqu'elles sont notifiés. Elle estime que sa base de données est couverte par le DMCA.
Jusqu'à présent, les extraits des bases communiqués à titre de preuve du piratage ont effectivement été mis en ligne sur des sites de téléchargement direct qui acceptent de retirer les liens illicites qui leur sont notifiés, et qui l'ont fait. Mais ce ne sera pas le cas si les hackers (ou « le » hacker si l'on en croit les soupçons que porte l'entreprise sur un ancien collaborateur) décident, par exemple, de publier un simple fichier .torrent, comme l'ont fait récemment les pirates de Hacking Team. Il n'y a alors personne à qui envoyer une demande de DMCA, et/ou beaucoup de sites de liens BitTorrent qui ne les respectent pas.

Voici le communiqué reçu :
Suite à une intrusion injustifiée et criminelle dans notre système samedi 18 juillet 2015, Avid Life Media a immédiatement engagé l'une des équipes de sécurité informatique les plus pointues au monde afin de prendre toutes les mesures possibles pour résoudre cette crise.
En utilisant la Digital Millennium Copyright Act (DMCA), notre équipe a supprimé avec succès tous les messages liés à cet incident ainsi que toutes les Informations Personnelles Identifiables (PII) publiées en ligne à propos de nos utilisateurs.
La confidentialité des informations concernant nos utilisateurs a toujours été notre plus grande priorité, et nous sommes rassurés que les dispositions contenues dans le DMCA aient permis de résoudre ce problème efficacement. Notre équipe de spécialistes et de professionnels sécurité informatique, en plus de faire appliquer la loi, continuent d'enquêter sur cet incident, et nous publierons de futurs bulletins dès que de nouveaux éléments verront le jour.

Source : http://www.numerama.com/magazine/33730-quand-ashley-madison-tente-de-rassurer-ses-clients-infideles.html
Par Guillaume Champeau

A Guédiawaye (Sénégal), la police démantèle un réseau de ressortissants nigérians | Le Net Expert Informatique

	A Guédiawaye (Sénégal), la police démantèle un réseau de ressortissants nigérians

6 ressortissants nigérians ont été interpellés par les éléments de la Brigade de recherches du Commissariat de police de Golf Sud (Guédiawaye). Le matériel qui a été découvert chez eux a permis de conclure que ces derniers s'activaient dans la cybercriminalité, selon le journal Grand Place.

La police de Guédiawaye (Sénégal) vient de démanteler un vaste réseau de cybercriminalité entretenu par des ressortissants nigérians. C'est suite à une information anonyme relative aux agissements répréhensibles de ces derniers que l'agent de police en chef de la commune de Golf Sud a mis sur pied un plan de neutralisation. Ainsi, ses hommes en civil se sont rendus sur les lieux dans la nuit du vendredis 10 juillet, aux environs de 23h, et ont pu arrêter 6 ressortissants nigérians.
Une perquisition de l'immeuble où ils ont été trouvés a permis de mettre la main sur 6 ordinateurs portables de marques différentes. L'exploitation des différents logiciels et autres systèmes des machines a permis la découverte d'installations et de fichiers de comptes bancaires de tiers ainsi que de faux documents étatiques et de réfugiés politiques.
Il y avait aussi plusieurs systèmes sur les ordinateurs portables avec des noms de code permettant à leurs propriétaires d'exercer, en toute discrétion, une activité criminelle.
– L'un permet d'effacer toutes les données après chaque redémarrage de l'outil informatique,
– alors que le deuxième est un système de navigation qui consiste à utiliser Internet sans pour autant être tracé ou repéré par les opérateurs de téléphonie.
– Et le troisième logiciel installé sur la machine ouvre la possibilité aux présumés cybercriminels de pirater les comptes bancaires d'autrui sans laisser des traces.

Source : http://www.leral.net/Cybercriminalite-a-Guediawaye-La-police-demantele-un-reseau-de-ressortissants-nigerians_a149877.html