La panoplie du hacker pour voler une voiture connectée | Le Net Expert Informatique

La panoplie du hacker pour voler une voiture connectée

Interception de paquets wifi, brouillage de signal, détection de mots de passe… L'utilisation grandissante des technologies sans fil dans les automobiles multiplie les vecteurs d'attaque. Démonstration.

Depuis qu'elles deviennent connectées, les voitures aiguisent de plus en plus l'appétit des hackers. A l'occasion de la conférence DEF CON 23, le chercheur Samy Kamkar – connu pour ses bricolages hors du commun – a montré différentes techniques permettant de voler une voiture en toute discrétion.
Pour ses besoins d'étude, il s'est penché sur la Chevrolet Volt d'un ami. Comme beaucoup d'automobiles aujourd'hui, elle dispose d'une application mobile compagnon, fournie par le constructeur General Motors (GM) et baptisée OnStar RemoteLink MobileApp. Elle permet de localiser le véhicule, de vérifier certains paramètres techniques, de le déverrouiller, d'allumer ses phares, de klaxonner et même de le démarrer. Pour réussir cela, l'application mobile se connecte aux serveurs de GM qui eux feront le lien avec le véhicule, grâce à une connexion cellulaire.

L'application mobile utilise des connexions SSL, mais ne vérifie pas les certificats. Elle est donc vulnérable à des attaques de type « Man in the middle ». Samy Kamkar a fabriqué un boîtier tout-en-un basé sur Raspberry Pi capable de créer un hotspot wifi, d'usurper l'identité des serveurs de GM quand un utilisateur s'y connecte, d'extraire ses données d'accès (login et mot de passe) et de les renvoyer au pirate par une connexion cellulaire. L'appareil, baptisé « OwnStar », est totalement autonome. On peut donc la placer à proximité de la cible et attendre que la connexion se fasse.

Mais comment inciter la future victime à se connecter sur ce faux réseau wifi? « On peut utiliser un nom de réseau usuel tel que 'attwifi' (le réseau de hotspots de l'opérateur américain ATT, ndlr) qui sont utilisés par beaucoup de personnes. Si on l'on est à proximité de la cible, on peut également intercepter les requêtes de connexion que son smartphone envoie automatiquement. C'est un bon moyen pour connaître les hotspots sur lesquels il se connecte habituellement », explique le hacker. Contacté par M. Kamkar, GM a depuis mis à jour son application mobile.

Si la cible n'utilise pas d'applications mobiles, le hacker propose un autre vecteur d'attaque: la clé de contact. Souvent, celles-ci permettent désormais de déverrouiller une voiture à distance, au moyen d'un code envoyé par un bref signal électromagnétique. Ce code n'est pas chiffré, mais il est à usage unique: à chaque fois que l'utilisateur appuie sur le bouton, un nouveau code est envoyé, et celui-ci n'est accepté qu'une seule fois. L'intercepter n'apporte donc rien à priori… à moins de faire en sorte que le code n'arrive pas à destination. Samy Kamkar a créé un autre boîtier qui va brouiller le signal pour que la voiture ne puisse pas capter les messages de la clé de contact, tout en étant capable d'extraire le code que l'attaquant pourra utiliser ultérieurement pour déverrouiller la voiture.

Reste enfin un dernier petit obstacle: ouvrir le garage dans lequel la voiture est éventuellement garée. Là encore, il n'est pas rare qu'une porte de garage puisse s'ouvrir à distance, au moyen d'un d'un badge. En décortiquant ces badges, Samy Kamkar découvre qu'ils utilisent généralement un code de 8 à 12 bits. Ce qui fait au total 88.576 possibilités. C'est suffisamment bas pour tenter une attaque par force brute. Originalité de la manoeuvre: pour créer ses signaux, il utilise un jouet Barbie, le Mattel IM-ME, un joli petit boîtier rose pour envoyer des messages texte. « C'est un appareil très pratique. Il dispose d'un bon chipset, d'un écran, d'un clavier et en plus il a une jolie couleur », souligne Samy Kamkar.

Une fois l'appareil reprogrammé, le hacker n'a besoin que de 8 secondes pour essayer toutes les possibilités et ouvrir la porte de garage. Une belle performance qui s'appuie notamment sur l'algorithme de De Bruijn, une méthode qui permet de scanner plus rapidement un espace de valeurs.

HotSpot Shield, le VPN Gratuit

Source : http://www.01net.com/actualites/def-con-23-la-panoplie-de-hacker-pour-voler-une-voiture-connectee-661671.html
Par Gilbert Kallenborn

Le paiement par selfie en cours de test aux Pays-Bas | Le Net Expert Informatique

Le paiement par selfie en cours de test aux Pays-Bas

Mastercard a récemment présenté la technologie aux Etats-Unis, c'est maintenant au tour de 750 Néerlandais de tester le service de paiement par selfie jusqu'au 30 novembre prochain.

Lors d'un achat en ligne via leur smartphone ou leur tablette, les clients pourront donc confirmer leur paiement au moyen d'une empreinte digitale ou d'un autoportrait. Mastercard collabore pour ce test avec CA technologies. En fonction des résultats, l'entreprise décidera si elle déploie la technologie sur l'ensemble du Vieux Continent.

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

Source : http://www.informaticien.be/index.ks?page=news_item&id=20948

Les drones de Parrot peuvent facilement se faire hacker | Le Net Expert Informatique

Les drones de Parrot peuvent facilement se faire hacker

Il y a quelques semaines, nous vous faisons part des piratages de voitures et encore plus tôt dans l'année, d'avions… Aujourd'hui, c'est au tour des drones Parrot de succomber aux hackers !

Ou plutôt à un hacker. Ryan Satterfield, connu pour sa chaîne Planet Zuda, qui a profité de la Def Con pour faire une démonstration. À l'aide de son smartphone et d'une simple clef, il a réussi à faire atterrir un AR.Drone 2.0.
Les drones de la société française n'ont malheureusement que trop peu de protections. Ces derniers tournent sous Linux avec des ports WiFi et Telnet ouverts, sans nécessiter un quelconque mot de passe pour s'y relier…. Il suffit de s'y connecter en utilisant le port 23 et de rentrer la commande « kill 1″. De suite, le drone redescend sur terre. Parrot a précisé qu'elle était consciente de ces failles de sécurité, mais n'a pourtant pas annoncé de correctif. Notez que le dernier drone, le Parrot Bebop, serait lui aussi touché, a annoncé le chercheur Michael Robinson.

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.journaldugeek.com/2015/08/17/les-drones-de-parrot-peuvent-facilement-se-faire-hacker
Par 4ugeek

La foudre frappe des serveurs Google rendant des données momentatnément inaccessibles | Le Net Expert Informatique

La foudre frappe des serveurs Google rendant des données momentatnément inaccessibles

A la suite d'un orage en Belgique, des serveurs appartenant à Google ont été privés de courant avec pour conséquence l'inaccessibilité de certaines données personnelles.

La foudre peut frapper deux fois au même endroit, la preuve un bâtiment situé en Belgique a reçu jeudi dernier quatre éclairs en l'espace d'un orage. Celui-ci, un data-center abrite des centaines de serveurs appartenant à Google. A l'intérieur de ceux-ci étaient stockées les données personnelles de nombreux utilisateurs et lorsque la foudre a frappé, le courant a sauté.
La BBC relate que cet aléa météorologique a eu quelques conséquences pour certains utilisateurs du service de stockage en ligne Google Drive. Leurs données ont en effet été momentanément inaccessibles.
Contacté par MyTf1news, le géant de l'Internet a réagi. « C'est une quantité infinitésimal qui a été affectée » a expliqué un responsable avant de poursuivre : « Aucune donnée n'a été perdue grâce à un système de sauvegarde décentralisé ». Dans les faits, il existait une copie des données affectées par la coupure de courant dans un autre data-center ailleurs sur la planète. Les documents des utilisateurs ont donc étaient inaccessibles juste le temps que ce système prenne le relai.
Les bâtiments de ce type sont généralement très bien protégés contre la foudre mais la répétition de ce phénomène n'avait apparemment pas été anticipée. Interrogé par la BBC, Justin Gale, un responsable d'Orion, une entreprise britannique spécialisée dans la protection des infrastructures contre la foudre revient sur le phénomène. L'éclair n'a pas besoin de frapper la structure en elle-même explique-t-il avant de préciser : « Un câble à un kilomètre peut être touché et le choc peut remonter jusqu'au data-center et tout faire disjoncter » détaille-t-il.
Dans un communiqué publié en ligne, Google relativise l'incident. Selon l'entreprise « moins de 0,000001% » de la surface des disques durs alloués à la zone géographique est concernée. La compagnie a néanmoins fait savoir qu'elle avait l'intention de renforcer ses protections contre les coupures de courant pour assurer la sécurité des données stockées sous sa responsabilité.

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

Source : http://lci.tf1.fr/high-tech/des-serveurs-de-google-frappes-par-la-foudre-des-donnees-personnelles-8646545.html
Illustration. Un éclair / Crédits : Comstock/Thinkstock

Un hack permet de pirater le bouton de commande physique

d’Amazon | Le Net Expert Informatique

Un hack permet de pirater le bouton de commande physique d’Amazon

Le développement des objets connectés va constamment soulever davantage des questions de sécurité à mesure qu’ils se propageront. Un utilisateur américain en fait l’expérience en piratant une balise permettant de commander sur Amazon.

L’Amazon Dash se présente comme une balise adhésive. Disposée à l’endroit de son choix et reliée en WiFi, elle permet à une personne de passer une commande en appuyant sur un unique bouton physique. Aux Etats-Unis, le principe est simple puisqu’il autorise par exemple un foyer à se réapprovisionner en couche ou en lessive, lorsque ces produits viennent à manquer.
Le client n’a en effet que ce bouton à appuyer pour générer une nouvelle commande. Le procédé lui évite de se rendre en magasin ou même de commander en ligne par le biais des traditionnels sites de vente. Depuis plusieurs mois, ces boutons connectés sont donc déployés sur le territoire.
Surfer sur la vague des objets connectés n’est toutefois pas sans risques. Aux Etats-Unis, un spécialiste en sécurité est parvenu à intercepter le signal émis par ces boutons de commandes afin de commander autre chose que les objets normalement prévus. Dans une note, Ted Benson détaille sa démarche.
Il a ainsi rédigé un code en Python capable de sniffer les connexions WiFi et en particulier détecter ces boutons, lorsqu’ils émettent un signal. En les reprogrammant, il est en mesure de leur attribuer une autre tâche que la simple commande de produits. S’il ne s’agit que d’une expérience, le spécialiste demande à présent à l’ensemble des internautes de reproduire la démarche afin de trouver de nouveaux usages à ces boutons.

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://pro.clubic.com/it-business/securite-et-donnees/actualite-776644-dash-amazon-hack.html?estat_svc=s%3D223023201608%26crmID%3D639453874_1114740199#pid=22889469

La société numérique d’aujourd’hui et de demain ? | Le Net Expert Informatique

La société numérique d'aujourd'hui et de demain ?

La diffusion au grand public du numérique s'est accélérée ces dernières années. Les enquêtes de l'Observatoire du numérique traduisent parfaitement ce succès. Il ressort notamment que les français ont un équipement adéquat et un usage élevé de l'internet. La France se place dans la moyenne des pays européens, mais on observe un décollage.

Équipements numériques :
82% des français ont un accès à internet depuis leur domicile. En 2002, c'était seulement 22% des foyers. La progression est fulgurante. L'Usage régulier d'internet (au moins une fois par semaine) concerne 78% des Français, contre 91% pour les Pays-Bas. L'Usage quotidien d'internet touche 66% des Français. Chiffres clés 2014

L'internet mobile confirme sa percée : 30% des particuliers de 16 ans et plus en France utilisent une connexion via un réseau de téléphonie mobile pour connecter leur appareil mobile à Internet, contre 23% dans l'UE et contre 56% en Suède. Enquête communautaire 2013
Pour les infrastructures du numérique, la France occupe une très bonne position sur les connexions à haut débit : elle se situe au 5e rang européen pour le ratio abonnements à haut débit par 100 habitants, soit 37% contre 28% dans l'UE. Enquête communautaire 2013

Usages du numérique :
59% des particuliers ont acheté des biens ou services en lignes sur la période étudiée, contre 47% des particuliers dans l'Union Européenne. Enquête communautaire 2013
L'administration numérique progresse bien en France, puisque 60% des particuliers et 96% des entreprises utilisent internet dans leurs relations avec l'administration, contre 41% et 88% dans l'UE. Enquête communautaire 2013
Les usages en entreprises sont plus contrastés et une marge de progression existe encore pour la possession d'un site web. Enquête communautaire 2013
L'ère du numérique est arrivée avec des équipements moins coûteux, un marché à forte concurrence et le développement des usages. La possession d'un ordinateur n'est plus un enjeu. Internet se massifie. Le nouvel enjeu, c'est l'internet mobile.
Le numérique, entendu comme l'ensemble des équipements permettant le passage à Internet et l'ensemble des services associés, est entré dans la vie des français. La France est devenue une société numérique. Quels sont les facteurs de cette transformation?

Un numérique séducteur : le marketing au renfort de la technologie.
Le succès du numérique peut d'abord s'expliquer par un procédé de miniaturisation des objets numériques qui sont devenus conviviaux. Steeve jobs a été visionnaire : il a pensé l'informatique comme un objet convivial. C'est penser les objets par les usages. Apple a changé la vision de l'informatique avec la conception assistée par l'usage.
Les avancées technologiques de l'informatique, conjuguées avec une meilleure prise en compte de l'utilisateur dans le développement d'interfaces numériques toujours plus simples, interactionnelles et esthétiques, ont permis d'ouvrir des pratiques numériques jusqu'alors restreintes à un public d'informaticiens.
Cette démocratisation des outils et des pratiques s'est faite à grand renfort de marketing. Internet arrive en France en 1994 mais ne prend son essor que plus tard. Apple ne devient pas spontanément une méga-marque. La culture numérique a lentement gagné la guerre du marketing.
La diffusion grand public des médias numériques ne peut dès lors se réduire à un déterminisme technique. Quelque chose dans la société a favorisé la réception de ces outils. En 20 ans, 1993-2013, nous avons basculé dans le monde numérique. On peut comparer la situation à la diffusion de l'imprimerie en Europe entre 1450 et 1500.
Ces délais montrent bien que la seule innovation technique n'est rien avant d'être pleinement reconnue dans les usages comme une innovation sociale.

Entrée dans une société de l'information : les facteurs extrinsèques.
Le rapport Nora-Minc sur l'informatisation de la société en 1978 est une photographie prospective de la société actuelle fondée sur l'informatique et les télécommunications. Cette informatisation a conduit à une société de l'information, de l'outil d'information et des données. Une société de la connaissance où la valeur est tombée sur l'information.

La première des raisons, c'est la mondialisation qui conduit à une nouvelle phase du capitalisme, le néo-libéralisme, et au passage à une économie de services. En tant que média vierge, sans frontières et sans règles, Internet a incarné plus que n'importe quel autre espace le néo-libéralisme et symbolise bien cette époque.

La privatisation et la fin des monopoles dans le secteur des télécoms aux États-Unis et les politiques de dérégulation conduites en parallèle par la CE et les pays du sud ont préparé les économies à cet avènement. Enfin, la Financiarisation de l'économie a achevé de déconnecter les flux financiers des réalités matérielles.

Au niveau politique, la disparition des idéologies a permis d'imposer un système unifié pour internet et d'ouvrir le réseau en remettant un peu plus en cause le rôle des états. Contrairement aux états, La démocratie profite de ces outils pour développer des modèles participatifs qui pourraient la sortir d'une situation de crise déjà éprouvée.

Enfin, les sociétés occidentales ont connu d'importants changements dans les systèmes éducatifs avec une population plus éduquée, confrontée à la formation continue. Le développement des MOOCs est une réponse à cette évolution. L'élévation du niveau de vie a également développé une société des loisirs qui met l'individu au cœur de l'économie.

Homo numericus : Un nouvel individu accueille le numérique dans sa vie.
D'un point de vue sociologique, les années 80 ont conduit à un changement de valeurs sociales avec le triomphe de l'individualisme et de nouveaux modèles familiaux éclatés. Cette décennie est le ferment de toute la société actuelle avec une critique du modèle classique et du patriarcat, l'émancipation des femmes et l'autonomie des individus.

Ces outils numériques favorisent l'individualisme. Au départ très chers et donc mis en commun, ils sont pourtant conçus comme des outils individuels. Aujourd'hui, le lien affectif à un mobile ou à un portable est avéré et il va aller en s'accentuant avec les objets connectés portatifs devenant une excroissance de leur propriétaire.
Conçus comme le prolongement de l'individu, ces outils lui ont donné l'opportunité de se créer une nouvelle identité numérique, parfois en opposition à une identité réelle. Elle va constituer une échappatoire pour l'individu dans une société en manque de repères. Cette situation fait émerger une nouvelle culture psychologique : la quête de soi.

Les communautés numériques, la blogosphère, puis le web 2.0 apportent un élément de réponse en ce qu'ils vont donner à l'individualisme la possibilité de se connecter. L'individu devient le noyau central de la société de services et de cette société de l'information. Sa croisade pour la quête du lien social sera désormais numérique.

En si peu de temps, le numérique est devenu un mode de vie, un idéal de transformation vers des sociétés dématérialisées, un puissant instrument de socialisation et presque une extension de nous même. Les discours idéologiques sont nombreux et contribuent puissamment à l'idée que nous allons rater quelque chose en nous déconnectant.

Le virtuel est désormais aussi important que le réel. Cet espace virtuel modifie l'individu, contracte sa perception du temps, de l'espace et des liens sociaux. Il donne des modèles de société. C'est un véritable séisme au niveau cognitif qui reconfigure l'être humain et la culture humaine, nous parlerons de plus en plus des « digital humanities ».

Une vision européenne du phénomène sur le site de la Commission.

Source : http://siecledigital.fr/2015/08/societe-numerique-realites-perspectives/

Votre iPhone est débridé ? Alors vous l'avez rendu vulnérable | Le Net Expert

Informatique

Votre iPhone est débridé ? Alors vous l'avez rendu vulnérable

Quand la firme d'espionnage Hacking Team s'est faite détroussée de 400 gigaoctets de documents internes compromettants sur ses activités, ces derniers ont révélé des failles importantes dans les téléphones iPhone qui ont subi un débridage par leur propriétaire.

Débrider son iPhone le rendrait vulnérable aux intrusions.

La firme d'espionnage Hacking Team en Italie s'est fait prendre, le moins qu'on puisse dire, les «culottes baissées».

Imaginez une société privée, qui vend ses services aux plus offrants – généralement des gouvernements -, développe des procédés informatiques pour infiltrer et dérober à l'aide de logiciels espions et autres chevaux de Troie les ordinateurs de sociétés ou de gouvernements amis comme ennemis.

Et bien Hacking Team s'est fait littéralement détrousser de 400 Go de documents par un petit groupe de pirates qui les a mis en ligne. On y a appris beaucoup de choses, dont que les iPhone débridés par leur propriétaire les rendaient vulnérables aux intrusions.

Hacking Team dispose de moyens pour percer tout type de systèmes d'exploitation; Windows, Mac OS, Linux et les systèmes mobiles comme iOS, Android, Symbian et même BlackBerry.

Si l'espionnage de haute voltige ne concerne véritablement que les services de renseignements des gouvernements, il est intéressant de constater que les utilisateurs d'iPhone – c'est-à-dire vous et moi – deviennent potentiellement des cibles quand les appareils tournant sous iOS sont débridés (jailbreakés) par leurs utilisateurs.

À QUOI SERT DE DÉBRIDER SON IPHONE?

Le débridage permet de passer outre les verrouillages imposés par Apple pour ses téléphones iPhone. Ainsi, il devient possible d'installer des extensions non approuvées et accéder à toutes les fonctions du système.

À chaque mise à jour du système iOS (iOS 8.1, 8.2, 8.3), Apple colmate les brèches découvertes, mais les spécialistes du débridage trouvent toujours un moyen de contourner les parades.

En soi, débrider son appareil mobile n'est pas illégal, mais la manœuvre lui fait perdre sa garantie, auquel cas le propriétaire doit auparavant remettre en état son iPhone pour le faire réparer.

OUPS, DÉBRIDER OUVRE DES «PORTES» DU IPHONE

Dans le grand déballage de documents de Hacking Team, on apprend que les iPhone et iPad modifiés par débridage (tous deux roulent le même système iOS) devenaient vulnérables aux intrusions par ceux qui employaient les outils d'Hacking Team.

Pour environ 72 000 $, Hacking Team vendait au client un module de surveillance (snooping module) capable d'infiltrer les iPhone. Seul préalable, les appareils iOS devaient être débridés.

Note aux petits malins du bidouillage, votre iPhone «maison» a peut-être les portes grandes ouvertes, quel bel accueil pour les intrus!

Apple a depuis peu un argument de poids pour décourager la pratique du débridage. La société fait d'ailleurs tout en son possible pour empêcher les développeurs d'applications de sortir des limites permises d'iOS afin de protéger l'intégrité de son système mobile.

Plus encore, un iPhone débridé et infecté permet non seulement d'accéder à son contenu, mais de pénétrer les informations contenues dans l'ordinateur qui sert à sa synchronisation.

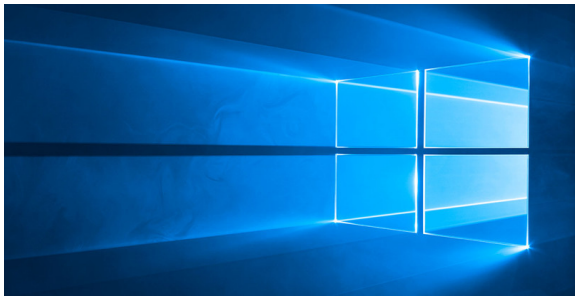
Avec tous les fichiers et applications «illégitimes» qui circulent librement sur les réseaux louches, l'idée de les croire tous «sains» et sans danger n'est que pur délire.

Pour terminer, les activités d'Hacking Team ciblent essentiellement les appareils de quelques individus en raison de leurs activités politiques, par exemple, les chances que vous soyez visé sont pratiquement nulles. Mais la leçon à retenir ici demeure que les protections qu'impose Apple à ses produits sont justifiées.

Quant à la pratique du débridage, elle vient de perdre des points.

Source : http://fr.canoe.ca/techno/materiel/mobiles/apple/archives/2015/08/20150806-120618.html

Malgré vos paramètres de confidentialité, Windows 10 communique toujours avec Microsoft | Le Net Expert Informatique



Malgré vos paramètres de confidentialité, Windows 10 communique toujours avec Microsoft

Même en désactivant le partage de données, Windows 10 continue de transmettre des renseignements attribuables à votre PC à Bing, Cortana, OneDrive et d'autres services de Microsoft.

Windows 10 est certes le système d'exploitation de Microsoft qui exploite le plus Internet dans le but d'offrir aux utilisateurs une panoplie de bénéfices. Il existe des paramètres de confidentialité permettant de désactiver cette forme de surveillance exercée par Microsoft, et bien qu'ils permettent de retrouver un minimum de confidentialité, des données identifiant votre PC sont tout de même transmises à l'entreprise.
C'est en effet ce que démontre aujourd'hui Ars Technica, qui a analysé le comportement de Windows 10 lorsque le partage de telles informations est désactivé. Tel que nous le soupçonnions en juillet dernier, il semble impossible pour l'instant de rendre Windows 10 complètement étanche à cet égard.

Comment se comporte Windows 10
Si une portion de la transmission semble totalement inoffensive, d'autres requêtes soulèvent plus d'inquiétudes.
D'abord, même lorsque Cortana et la recherche web du menu Démarrer sont désactivées, Windows 10 communique avec les serveurs de Bing en transmettant ce qui semble être un numéro d'identification propre à l'ordinateur employé afin d'obtenir un fichier nommé threshold.appcache. Le fichier ainsi obtenu semble contenir certaines informations liées à Cortana.
À noter que le numéro d'identification transmis est persistant, et demeure le même après un redémarrage.
Si une portion de la transmission semble totalement inoffensive, son existence apparaît injustifiée. Sans compter que d'autres requêtes soulèvent plus d'inquiétudes. Par exemple, Windows 10 achemine périodiquement des données à un serveur qui semble être employé par OneDrive et d'autres services de Microsoft, et ce, même lorsque OneDrive est désactivé et que l'utilisateur emploie un compte local. Ars Technica n'a pas été en mesure d'identifier le contenu de ces données, mais soupçonne qu'il pourrait s'agir d'informations télémétriques – des données statistiques permettant à Microsoft d'évaluer le comportement de son OS dans le but de produire de nouvelles mises à jour.
Enfin, même lorsqu'un PC est configuré pour employer un proxy pour toutes les transmissions utilisant les protocoles HTTP et HTTPS (à la fois au niveau de l'utilisateur et au niveau du système), Windows 10 semble effectuer des requêtes à un réseau de distribution de contenu en ignorant ces paramètres. Par conséquent, Ars Technica n'a pas été en mesure d'évaluer le contenu de ces mystérieuses communications.

La réponse de Microsoft
«Aucune donnée liée à l'historique des requêtes de recherche n'est transmise à Microsoft, conformément aux paramètres de confidentialité choisi par l'utilisateur.»
«Dans le cadre de l'offre de Windows 10 en tant que service, des mises à jour peuvent être déployées afin d'ajouter progressivement de nouvelles fonctionnalités à la recherche Bing, telles que des changements à l'interface visuelle, aux styles et au code du moteur de recherche», a déclaré un porte-parole de Microsoft à Ars Technica.
«Aucune donnée liée à l'historique des requêtes de recherche n'est transmise à Microsoft, conformément aux paramètres de confidentialité choisi par l'utilisateur. Cela vaut également pour la recherche hors-ligne d'éléments tels que les applications, les fichiers et les paramètres de l'appareil.»
S'il est vrai qu'aucune donnée liée à l'historique de recherche n'est transmise à Microsoft, le comportement de Windows 10 est susceptible d'aller à l'encontre des attentes de la majorité de ses utilisateurs. Par exemple, dans le cas où Cortana et la recherche web sont désactivées, l'utilisateur est en droit de s'attendre à ce que le système d'exploitation ne communique aucunement avec Internet lors d'une recherche locale à partir de menu Démarrer. Ce n'est manifestement pas le cas, et la présence d'un numéro d'identification propre au PC dans ces communications demeure suspecte, même si le contenu des transmissions pourrait être anodin.
Il va de soi qu'Internet et PC sont aujourd'hui indissociables. Les nouveaux systèmes d'exploitation vont inévitablement continuer d'imposer des compromis à la vie privée de leurs utilisateurs. Pour la majorité des consommateurs, ces compromis sont acceptables, et permettent de bénéficier de services tels que Cortana, Siri ou Google Now, de la synchronisation infonuagique de fichiers, mots de passes et paramètres.
N'empêche, le fait qu'il soit impossible de totalement désactiver ce type de transmission de données outre que de complètement déconnecter son PC d'Internet est désolant.

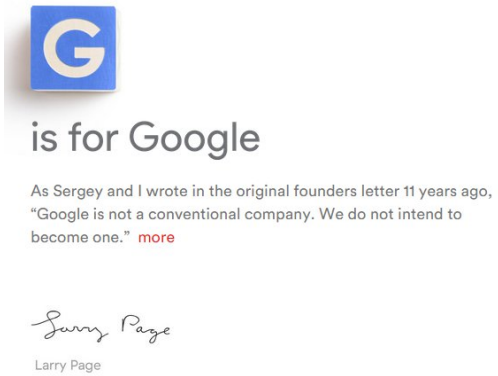
Source : http://branchez-vous.com/2015/08/13/malgre-vos-parametres-de-confidentialite-windows-10-communique-toujours-avec-microsoft/
Par Laurent LaSalle

Google devient Alphabet | Le Net Expert Informatique

	**Google devient Alphabet**

Les deux fondateurs de Google annoncent une importante restructuration donnant naissance à une nouvelle société, Alphabet, laquelle englobera le moteur de recherche, les activités satellite historiques et tous les projets initiés par le duo.

Larry Page et Sergey Brin ont annoncé lundi 10 août la plus profonde restructuration financière jamais entreprise par Google depuis son introduction en bourse en 2004. Dans une lettre commune, ils indiquent que le groupe qu'ils ont fondé sera désormais englobé au sein d'une nouvelle société, baptisée Alphabet.



Un nom à dimension holistique, qui recouvrira les activités historiques du moteur de recherche ainsi que les nouveaux projets lancés au sein de ses laboratoires qui deviendront autant de nouvelles entités, de Life Sciences et ses lentilles connectées pour diabétiques à Calico, dont l'objectif consiste à prolonger la vie de l'homme en passant par la livraison par drone promise par Wing. Google ne sera donc plus désormais que le « G » de l'Alphabet selon Page et Brin.
« Qu'est donc Alphabet ? Alphabet consiste principalement en une collection de sociétés. Dont la plus importante est bien sûr Google. Ce nouveau Google est un peu allégé, dans la mesure où les sociétés qui sont éloignées de nos principaux produits liés à Internet sont maintenant contenus dans Alphabet », expliquent les deux hommes.
L'explication appelle à la logique, partant du principe qu'il n'est pas forcément aisé de mener un moteur de recherche, la première régie publicitaire en ligne au monde et le développement de voitures autonomes ou la recherche en biotechnologies à l'aide de rênes uniques.
« Fondamentalement, nous pensons que (cette nouvelle structure) nous permettra de mieux adapter notre gestion dans la mesure où nous conduisons de façon indépendante des choses qui ne sont pas liées ». Chaque entité au sein d'Alphabet sera menée par son propre chef d'orchestre, Page et Brin assurant le pilotage général, le premier en tant que CEO et le second au poste de président.
La direction du nouveau Google reviendra quant à elle à Sundar Pichai. Il englobe la recherche, la publicité en ligne, YouTube, la cartographie, Android et l'ensemble des infrastructures techniques associées, qui constituent aujourd'hui le bras armé de Google sur le plan financier.
Nest (thermostat connecté), Fiber (fournisseur d'accès) et les différentes entités dédiées à l'investissement (Google Ventures, Google Capital), activités moins « stables » dans le sens où elles induisent des investissements importants associés à une certaine part de risque, appartiendront en revanche à l'ensemble Alphabet.
Au Nasdaq, Alphabet Inc. remplacera Google Inc. en tant qu'entité publique, et l'ensemble des actions sera automatiquement convertis, à valeur et droits équivalents.
En attendant de mesurer l'accueil des marchés boursiers face à ce changement inédit, Page et Brin renouvellent leur profession de foi : cette nouvelle organisation devrait selon eux permettre d'accomplir des tâches toujours plus importantes, inscrites dans une vision à long terme, tout en favorisant le développement de l'ensemble de l'écosystème, de façon toujours plus transparente… pour in fine « améliorer la vie d'autant de personnes que possible ».
Derrière la portée symbolique et les accents humanistes de la déclaration, difficile de ne pas supposer en arrière plan des manœuvres plus terre à terre, visant à redonner de l'agilité sur le plan financier à celle qui fut un jour une start-up et pèse aujourd'hui parmi les plus importantes capitalisations boursières de la planète.

Source : http://pro.clubic.com/entreprises/google/actualite-776160-google-restructure-sein-maison-mere-alphabet.html
Par Alexandre Laurent

On peut voler des identifiants Active Directory depuis Internet via SMB | Le Net Expert Informatique

On peut voler des identifiants Active Directory depuis Internet via SMB

Deux chercheurs ont montré sur la conférence Black Hat 2015 qu'une attaque via le protocole de partage de fichiers SMB connue pour s'effectuer au sein d'un réseau local peut en fait servir à attaquer des serveurs Windows hébergés dans le cloud.

Lors de la conférence Black Hat 2015 (Las Vegas, du 1er au 6 août), deux chercheurs ont montré qu'une technique d'attaque via le protocole de partage de fichiers SMB que l'on croyait ne fonctionner que sur les réseaux locaux peut en fait être exécutée sur Internet. Avec cette attaque, dite de relais SMB, un ordinateur Windows appartenant à un domaine Active Directory laisse apparaître les informations d'identification de l'utilisateur quand celui-ci consulte une page web, un courriel dans Outlook ou regarde une vidéo dans Windows Media Player. L'attaquant peut ensuite détourner ces identifiants pour s'authentifier au nom de l'utilisateur sur des serveurs Windows où il dispose d'un compte, y compris ceux hébergés dans le cloud.
Dans un réseau Active Directory, les ordinateurs Windows retournent automatiquement leurs informations d'identification pour accéder aux différents services de partage de fichiers à distance, aux serveurs de messagerie Microsoft Exchange ou aux outils de collaboration SharePoint. Ces informations d'authentification – en l'occurrence le nom de l'ordinateur, le nom de l'utilisateur, tous deux en texte clair, et un hash cryptographique dérivé du mot de passe de l'utilisateur – sont envoyées à l'aide du protocole d'authentification NTLMv2. En 2001, des chercheurs en sécurité avaient déjà mis au point une attaque dite par relais SMB : en se positionnant entre un ordinateur Windows et un serveur, les attaquants pouvaient intercepter les informations d'identification, puis les relayer vers le serveur et s'authentifier à la place de l'utilisateur légitime. Mais à l'époque, tout le monde pensait que l'attaque ne fonctionnait qu'en local.

Authentification configurée par défaut dans IE
Sauf que, dans Internet Explorer, l'authentification de l'utilisateur est configurée par défaut avec l'option « ouverture de session automatique réservée à la zone intranet ». Or, les chercheurs en sécurité Jonathan Brossard et Hormazd Billimoria, ont constaté que cette option était ignorée et qu'il était possible de duper le navigateur pour que celui-ci laisse fuiter vers Internet les informations Active Directory de l'utilisateur – c'est à dire son nom et la séquence de code cryptographique basée sur son mot de passe – pour les transmettre à un serveur SMB distant contrôlé par les pirates. Les chercheurs ont pu suivre le trajet d'un fichier DLL propre à Windows, utilisé aussi bien par Internet Explorer que par de nombreuses applications pouvant accéder aux URL, comme Microsoft Outlook, Windows Media Player ou d'autres programmes tiers. « Quand l'application veut accéder à une URL, le fichier DLL vérifie les informations d'authentification dans le registre, mais tout en les ignorant », ont expliqué les chercheurs pendant leur présentation.

Toutes les versions actuelles de Windows et d'Internet Explorer (ou encore supportées) sont concernées par le problème. « C'est la première attaque à distance capable de compromettre potentiellement Windows 10 et le nouveau navigateur Microsoft Edge », a alerté Jonathan Brossard. « Nous sommes au courant de ce problème et nous enquêtons à ce sujet », a déclaré jeudi un représentant de Microsoft par courriel.

Plusieurs scénarios possibles
« Une fois que les attaquants ont mis la main sur les informations d'identification de l'utilisateur, ils peuvent les utiliser de différentes façons », a précisé Jonathan Brossard. Un premier scénario consisterait à monter une attaque par relais SMB pour s'authentifier à la place de la victime sur des serveurs hébergés hors du réseau local en utilisant une fonctionnalité appelée « NTLM over http », ajoutée pour étendre le périmètre des réseaux dans les environnements cloud. Les pirates pourraient notamment accéder à un shell distant sur le serveur qu'ils utiliseraient ensuite pour installer des logiciels malveillants ou exécuter des programmes exploitant des failles. Si le serveur distant est un serveur Exchange, les attaquants pourraient télécharger toute la boîte aux lettres de l'utilisateur.

Un autre scénario impliquerait de casser la séquence de code cryptographique et de l'utiliser pour accéder à un serveur Remote Desktop Protocol. Des pirates peuvent y arriver en utilisant des plates-formes spécialisées ou des services donnant accès à une grosse puissance de calcul. Un mot de passe de huit caractères ou moins peut être craqué en deux jours environ. « Et, déchiffrer toute une liste de hashs volés ne serait pas plus long, puisque le processus teste toutes les combinaisons à la fois », a ajouté le chercheur. Des identifiants Windows volés via Internet seraient également utiles à des attaquants qui ont déjà réussi à se faufiler dans un réseau local, mais ne disposent pas des privilèges d'administration. En envoyant un simple message électronique à l'administrateur légitime, ils pourraient récupérer ses identifiants dans Outlook et utiliser le hash volé pour mener une attaque par relais SMB contre les serveurs connectés au réseau local.

Source : http://www.lemondeinformatique.fr/actualites/lire-black-hat-2015-on-peut-voler-des-identifiants-active-directory-depuis-internet-via-smb-62000.html
Par Jean Elyan et IDG News Service