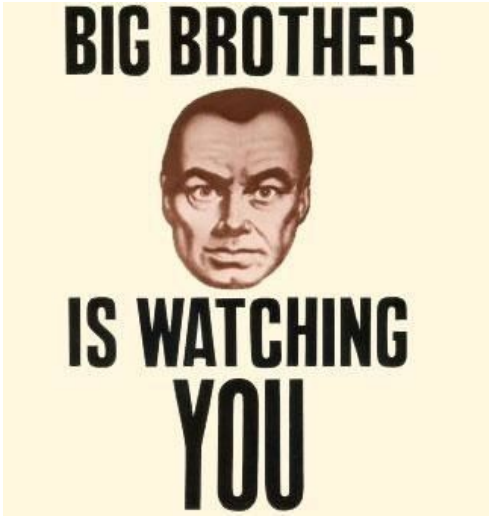
Alerte Faille Android ! Big Brother pourrait bien vous surveiller | Le Net Expert Informatique

	Alerte Faille Android ! Big Brother pourrait bien vous surveiller

Des chercheurs en sécurité ont récemment découvert une faille de sécurité considérée comme la pire jamais découverte dans le système Android. Détecté dans la bibliothèque multimédia de l'OS, ce bug nommé « Stagefright » expose près d'1 milliard de terminaux Android aux malwares.

En exploitant la faille « Stagefright », les hackers peuvent accéder aux contacts et aux autres données stockées dans un appareil mobile telles que les photos et les vidéos. Ils peuvent également accéder au microphone et à la caméra de cet appareil, ce qui leur permet d'espionner l'utilisateur via l'enregistrement de son et la prise d'images.

Tous les appareils exécutant des versions Android 2.2 Froyo jusqu'aux versions 5.1.1 Lollipop sont concernés. Cela représente environ 95% de l'ensemble des terminaux Android.

Le plus effrayant, c'est que les pirates ont uniquement besoin du numéro de téléphone de l'utilisateur pour infecter son appareil. Le malware est transmis lors de l'envoi d'un message multimédia à n'importe quelle application de messagerie pouvant traiter les formats vidéo MPEG4, telle que l'application de messagerie par défaut de l'appareil Android, Google Hangouts ou Whatsapp. Comme ces applications de messagerie Android récupèrent automatiquement des vidéos ou du contenu audio, le code malveillant est exécuté sans que l'utilisateur n'ait besoin de faire quoi que ce soit. En effet, la faille n'exige pas que la victime ouvre le message ou clique sur un lien. Il s'agit d'un malware unique en son genre car ce type de menace nécessite généralement une action de la part de l'utilisateur pour que l'appareil soit infecté. Il pourrait par exemple être relayé via un lien envoyé par courrier électronique ou partagé sur les réseaux sociaux. Toutefois, cela nécessiterait encore et toujours une action de la part de l'utilisateur, puisque le chargement d'une vidéo se fait uniquement via l'ouverture d'un lien. Cela est extrêmement dangereux, car si les utilisateurs sont infectés via MMS, aucune action ne leur sera demandée et les effets indésirables seront imperceptibles. Avant même que les victimes s'en aperçoivent, le hacker est en mesure d'exécuter le code et de retirer toute trace attestant que l'appareil a été infecté.

Le rêve du cybercriminel et du dictateur

Les cybercriminels profitent de cette faille de sécurité pour espionner des millions de personnes et exécuter d'autres codes malveillants. Les gouvernements répressifs pourraient abuser de ce bug en vue d'espionner leurs citoyens ou leurs ennemis. Toutefois, ce bug pourrait également être utilisé à des fins d'espionnage apolitique. Les pirates peuvent facilement surveiller les personnes de leur entourage comme leur conjoint ou leurs voisins. Ils n'ont besoin pour ce faire que du numéro de téléphone de la personne visée. Les hackers ont aussi la possibilité de dérober des informations personnelles qu'ils utiliseront pour faire chanter des millions de personnes ou usurper leur identité. Les conséquences possibles de ce type de faille sont donc à prendre au sérieux.

Une nécessité urgente de patchs

Des patchs complets doivent désormais être fournis par les fabricants de téléphones à l'aide d'une mise à jour à distance ou « over-the-air » (OTA) d'un firmware pour les versions Android 2.2 et plus. Malheureusement, les mises à jour pour appareils Android ont toujours mis beaucoup de temps pour arriver jusqu'à l'utilisateur final. Espérons que les constructeurs réagiront plus rapidement dans ce cas précis.

Google y a pour sa part déjà répondu d'après un témoignage d'HTC publié dans le magazine d'information hebdomadaire américain Time : « Google a informé HTC de cette problématique et fourni les patchs nécessaires qu'HTC a commencé à prendre en compte dans les projets mis en œuvre au début du mois de juillet. Tous les projets en cours contiennent le patch requis. » Pour le moment et par mesure de précaution, il est recommandé aux utilisateurs de désactiver la fonction récupération automatique des MMS dans les paramètres par défaut de l'application de messagerie.

Source : http://www.journaldun
et.com/solutions/expert/61932/big-brother-po
urrait-bien-vous-surveiller-grace-a-la-faille-stagefright.shtml
Par Filip Chytrý

Les cyber-attaques provenant

du Dark Web empruntent de plus en plus le réseau Tor | Le Net Expert Informatique

	Les cyber-attaques provenant du Dark Web empruntent de plus en plus le réseau Tor

I**BM Sécurité vient de dévoiler les résultats de son rapport Q3 2015 IBM X-Force Threat Intelligence. Celui-ci pointe les dangers grandissants provoqués par les cyber-attaques provenant du Dark Web à travers l'utilisation du réseau Tor (The Onion Router), ainsi que les nouvelles techniques mises en place par les criminels pour les attaques avec rançon. Rien que depuis le début de l'année, plus de 150 000 événements malveillants provenant de Tor ont eu lieu aux Etats-Unis.**

Même si on entend davantage parler des fuites de données que des demandes de rançon, les « ransomware » représentent une menace grandissante. Comme la sophistication des menaces et des attaquants croît, leur cible fait de même, et ainsi certains attaquants se sont par exemple spécialisés dans la demande de rançon concernant les fichiers de joueurs de jeux en lignes populaires. Le rapport dévoile que les agresseurs peuvent maintenant également bénéficier de « Ransomware as a Service » en achetant des outils conçus pour déployer de telles attaques.
Comme les hauts fonds des océans, le Dark Web demeure largement inconnu et inexploré, et il héberge des prédateurs. L'expérience récente de l'équipe IBM Managed Security Services (IBM MSS) montre que les criminels et d'autres organisations spécialisées dans les menaces utilisent Tor, qui permet d'anonymiser les communications aussi bien en tant que vecteur d'attaques que d'infrastructure, pour commander et contrôler les botnets. La façon dont Tor masque le cheminement offre des protections supplémentaires aux attaquants en les rendant anonymes. Ils peuvent aussi masquer la location physique de l'origine de l'attaque, et même la remplacer par une autre de leur choix.
Le rapport étudie également Tor lui-même, et fournit des détails techniques permettant de protéger les réseaux contre les menaces, intentionnelles ou non, véhiculées par Tor.
Le rapport est accessible ici.

Source : http://www.infodsi.com/art
icles/157784/cyber-attaques-provenant-dark-web-emprunt
ent-plus-plus-reseau-tor.html

Écoutes : la mise en place de la PNIJ avance doucement | Le Net Expert Informatique

Écoutes : la mise en place de la PNIJ avance doucement

Interpelé par un député qui se plaignait de la lenteur des procédures de réquisition effectuées auprès des opérateurs de téléphonie mobile, le ministre de l'Intérieur vient de donner quelques nouvelles de la Plateforme nationale des interceptions judiciaires (PNIJ), qui n'en finit pas d'accumuler du retard.

Initialement prévue pour fin 2013, la PNIJ n'est toujours pas opérationnelle. Cet énorme centre, placé dans les locaux du géant Thales, était pourtant censé faciliter le travail des enquêteurs – même si ce n'est pas l'avis de ses détracteurs. Autorisée par un décret publié en octobre au Journal officiel, cette plateforme doit en effet permettre de centraliser les nombreuses interceptions de correspondances ordonnées par la justice, de même que les réquisitions de données de connexion (quel abonné derrière telle adresse IP ou numéro de téléphone, etc).
Aujourd'hui, pour identifier un client d'Orange ou SFR, les réquisitions « sont transmises par les moyens de communication classiques – principalement le fax – et traitées par les employés des services des obligations légales des différentes sociétés », reconnaît ainsi le ministre de l'Intérieur au travers d'une réponse à une question écrite du député Jean-Luc Bleunven. Si le Code de procédure pénale permet théoriquement aux opérateurs de répondre à ces réquisitions par voie électronique, le locataire de la Place Beauvau explique qu'en pratique, ce n'est pas encore totalement le cas, en raison des retards de la PNIJ.

Une expérimentation menée depuis février en vue des identifications d'abonnés
Bernard Cazeneuve indique toutefois que des « protocoles » permettant de « mettre en place un système de réponse automatisé aux demandes de l'autorité judiciaire » a été signé « récemment » avec les quatre principaux opérateurs de téléphonie : Orange, SFR, Bouygues et Free. « L'expérimentation de la PNIJ sur ce point est en cours depuis le 9 février 2015 dans certains services d'enquête » poursuit le ministre de l'Intérieur. Selon lui, « les résultats sont extrêmement probants : les réponses aux réquisitions dont les opérateurs ont automatisé le traitement sont obtenues par les services d'enquête en quelques minutes contre plusieurs jours ou semaines auparavant ».
Restera maintenant à voir quand cette expérimentation limitée à quelques « services d'enquête » sera généralisée… Point sur lequel ne s'avance pas le premier flic de France.

Source : http://www.nextinpact.com/news/96181-ecoutes-mise-en-place-pnij-avance-doucement.htm
Par Xavier Berne

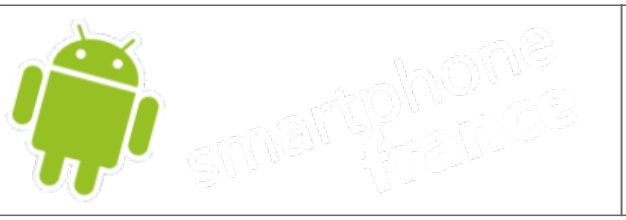
Quatre jours de coupure informatique à la suite d’une Cyberattaque | Le Net Expert Informatique

Le Bundestag allemand plongera jeudi son système informatique dans un sommeil de quatre jours pour des opérations de maintenance, à la suite d'une vaste attaque informatique dont avait été victime fin mai la chambre basse du Parlement, a annoncé mercredi son président.

Passé ce délai, le système sera « à nouveau pleinement utilisable », soit à partir de lundi, a annoncé Norbert Lammert, le président du Bundestag.
Cette opération, initialement prévue quelques jours plus tôt, a dû être repoussée en raison du rappel des députés allemands pour voter mercredi sur le troisième plan d'aide à la Grèce.
La chambre basse du Parlement allemand avait été visée fin mai par une attaque informatique, qui s'était avérée beaucoup plus importante et vaste que prévue, les services du Bundestag peinant à la contrôler. Un ordinateur de la chancelière Angela Merkel avait également été touché.
Les hackers auraient pendant plusieurs semaines profondément infiltré le réseau informatique, parvenant à pirater des données, avait rapporté la presse allemande.
Les sites officiels de Mme Merkel, de la chancellerie et du Bundestag avaient déjà fait l'objet en janvier d'une cyberattaque, revendiquée par des hackers russes.
Selon des médias allemands, la dernière attaque contre le Bundestag viendrait aussi de Russie et pourrait avoir été lancée par des services de renseignements de ce pays.

Source : http://www.notretemps.com/internet/le-parlement-allemand-va-eteindre-son,i92309

Nos empreintes digitales en danger à cause d’Android ? | Le Net Expert Informatique

	Nos empreintes digitales en danger à cause d’Android ?

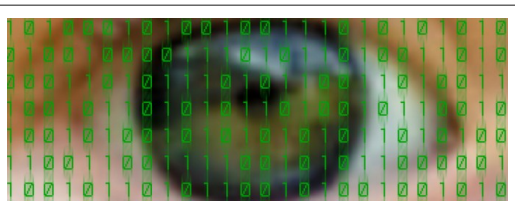
Alors que les failles de sécurités concernant Android n'ont jamais été aussi nombreuses à être révélées, une nouvelle attaque permettrait de voler les empreintes digitales à cause d'une nouvelle lacune du système Android ! Une affaire qui mérite certainement d'être prise au sérieux non ?

S'il est vrai qu'Android n'est pas le meilleur exemple en termes de sécurité, succès oblige comme Windows il y a quelques années, on ne peut cependant pas l'accuser de tout et n'importe quoi. Cette soi-disant faille permettrait à un pirate de récupérer les empreintes d'un utilisateur qui utilise ce type de fonctionnalité sur son smartphone afin d'en assurer la sécurité d'accès. Quelle horreur nous sommes donc tous en danger !
Plus sérieusement le risque évoqué est assez limité et avec n'importe quel objet qu'on touche nous laissons tous des empreintes digitales un peu partout. Ne pas être totalement parano est certainement la meilleure chose à faire et être prudent dans la manière de protéger ses données personnelles est la seconde chose à penser. Avec l'informatique nous sommes tous vulnérable et des victimes potentielles de piratage et c'est en faisant attention à ce qu'on fait qu'on se protégera le mieux. Pour rappel une empreinte digitale même si elle est unique est sans aucun doute un des moyens les moins sûrs pour protéger un système informatique. Utiliser une empreinte c'est comme laisser un Post-It avec son mot de passe sur chaque objet qu'on touche !

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

Source : http://android.smartphonefrance.info/actu.asp?ID=3966

NSA Playset : un kit de surveillance électronique en open source | Le Net Expert Informatique



NSA Playset : un kit de surveillance électronique en open source

Une équipe de chercheurs tente d'imiter les techniques de la NSA à travers une série d'outils open source destinés à mettre en place des écoutes sophistiquées.

Via de petits outils ou gadgets bon marché dont le design est placé en open source, une communauté de chercheurs en sécurité informatique travaille à rendre accessibles au plus grand nombre les techniques les plus pointues de la NSA.
Les fruits d'une année de travaux ont été présentés la semaine passée dans le cadre de la conférence Black Hat USA 2015, organisée à Las Vegas.
Pour mettre au point leurs solutions d'espionnage électronique, les chercheurs se sont inspirés du catalogue ANT, du nom de cette entité qui fournit, au sein de la NSA, des services de piratage « sur étagère » aux différentes divisions de l'agence de renseignement.
Le catalogue en question avait été révélé fin 2013 par le quotidien allemand Der Spiegel, sur la base de documents exfiltrés par Edward Snowden. D'une cinquantaine de pages, il regroupe des exploits basés sur certaines techniques bien connues… et d'autres plus inédites, reposant notamment sur l'interception de signaux au coeur même des appareils ciblés.
Les outils – finalisés ou en cours de développement – doivent surtout permettre de préparer des systèmes qui peuvent y résister. Ils sont classés en cinq catégories.

Première sur la liste, l'interception radio passive. On y trouve, entre autres, Levitivus (analyseur de spectre GSM qui prend la forme d'un téléphone Motorola dont le firmware a été modifié) et KeySweeper (enregistreur de frappe basé sur un matériel Arduino et déguisé en chargeur USB ; voir, à ce propos, notre article « Sécurité IT : les adaptateurs secteur ont des oreilles »).
Deuxième catégorie, la « domination physique » avec, entre autres, le dispositif Slotscreamer, qui s'insère dans un port PCIe sur la machine, offrant un accès direct à la mémoire et aux entrées-sorties. Le tout en contournant les mesures de sécurité physiques et logiques.
Troisième rubrique : les implants hardware, symbolisés par Chuckwagon, qui tire parti du port I2C – présent sur nombre d'ordinateurs – pour l'installation de malware.
En quatrième sur la liste, les techniques d'injection radio active, par exemple à travers Tiny Alamo, qui cible souris et clavier Bluetooth pour insérer des informations dans le système ciblé.
Ultime rubrique : les rétroréflecteurs, illustrés par Congaflock, destiné à être implanté sur tout type d'appareil transmettant des signaux par câble. Son rôle : récupérer de nombreuses données, de la frappe clavier aux images affichées sur l'écran.

Source : http://www.itespresso.fr/nsa-playset-kit-surveillance-electronique-open-source-104776.html

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.

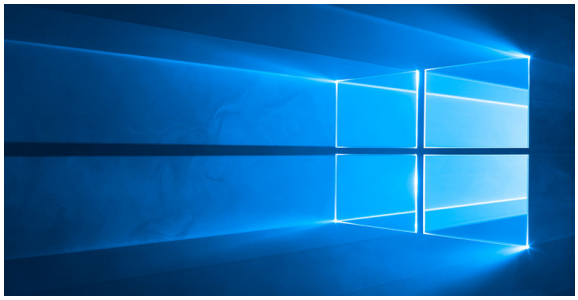
Avec tous les fichiers et applications «illégitimes» qui circulent librement sur les réseaux louches, l'idée de les croire tous «sains» et sans danger n'est que pur délire.

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

Une faille de sécurité de Hacking Team a été utilisée par un important groupe de pirates | Le Net Expert Informatique

Une faille de sécurité de Hacking Team a été utilisée par un important groupe de pirates

Des groupes de pirates informatiques ont utilisé, peu après leur publication, le contenu des fichiers volés à l'entreprise Hacking Team pour se livrer à des tentatives de piratage, révèle l'entreprise de sécurité Kaspersky. Selon Kaspersky, le groupe « Darkhotel », notamment, a utilisé des vulnérabilités qui avaient été employées par Hacking Team, une entreprise spécialisée dans la vente de logiciels de surveillance.

« Darkhotel » s'est notamment signalé par le passé pour avoir utilisé des méthodes élaborées pour placer des logiciels espions – par exemple en prenant le contrôle des réseaux wifi utilisés dans de grands hôtels. Parmi ses cibles figurent des dirigeants de très grandes entreprises, dans la chimie, les cosmétiques ou la pharmacie, des militaires et des responsables d'ONG, dans plusieurs pays d'Europe, d'Asie et d'Afrique, toujours selon Kaspersky. Des cibles et un niveau de sophistication qui laissent supposer à Kaspersky qu'il s'agit d'un groupe étatique ou soutenu par un Etat.
Hacking Team, société italienne à la réputation sulfureuse, est spécialisée dans la vente de logiciels espions et de dispositifs de surveillance électronique. L'intégralité des données de l'entreprise a été publiée en ligne après un piratage, y compris le contenu des messageries de la société. Des associations et des élus européens ont demandé l'ouverture d'une enquête sur les pratiques commerciales de la société, soupçonnée d'avoir notamment vendu des logiciels au Soudan, et une réforme de la législation sur l'exportation de ces technologies.

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.lemonde.fr/pixels/article/2015/08/10/une-faille-de-securite-de-hacking-team-a-ete-utilisee-par-un-important-groupe-de-pirates_4719735_4408996.html

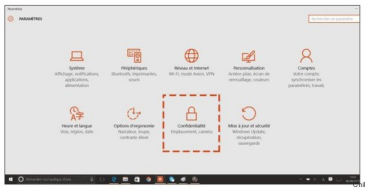
Vie privée et données personnelles sous Windows 10 : les astuces de la Cnil pour vous protéger | Le Net Expert Informatique

Vie privée et données personnelles sous Windows 10 : les astuces de la Cnil pour vous protéger

La Commission nationale de l'informatique et des libertés (Cnil) a diffusé lundi 10 août un communiqué pour aider les utilisateurs du flambant neuf Windows 10 à protéger leurs données personnelles.

Au cœur d'une polémique depuis l'adoption d'une nouvelle politique sur la collecte des données privées, le dernier système d'exploitation de Microsoft s'est vu attaqué ces derniers jours par des utilisateurs mais aussi par Marine Le Pen qui dénonçait « l'espionnage généralisé des ordinateurs des Français ».
La présidente du FN avait d'ailleurs interpellé la Cnil « pour analyser les conséquences de Windows 10 sur la vie privée des Français » et demandé des mesures « afin que Microsoft se conforme à la loi française sur la protection de la vie privée. »
Rien de tel pour l'heure mais l'organisme propose à défaut la série de réglages ci-dessous pour « limiter la communication de vos informations à l'éditeur et à ses partenaires. »

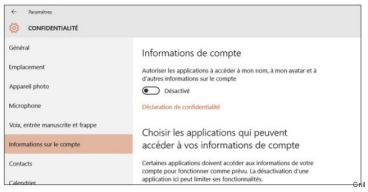
• Cliquez sur le logo Windows en bas à gauche puis sur » Paramètres « . Sélectionnez alors le menu » confidentialité » où vous pourrez modifier les principales fonctionnalités qui collectent des données :



Cnil

• Pour limiter le plus l'envoi de vos données, vous pouvez systématiquement tout désactiver.

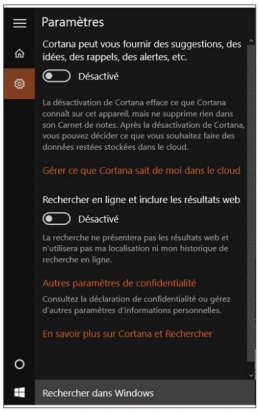
• Par défaut la géo-localisation de votre poste est activée. Il est recommandé de la désactiver depuis l'onglet » Emplacement « .



Cnil

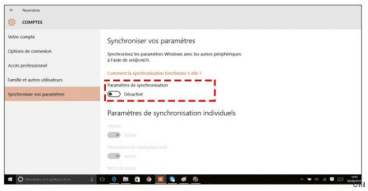
• Vous pouvez désactiver complètement la collecte de données ou empêcher certaines applications d'y accéder. Notamment pour l'Appareil photo, le Microphone, les Informations de Compte, les Contacts, lu Calendrier, la Messagerie, les communications Radio et la synchronisation avec les Autres appareils.

• Cortana, l'assistante embarquée dans Windows 10, a besoin d'accéder à plusieurs types d'informations pour fonctionnet. Vous pouvez désactiver Cortana soit en cliquant sur l'icone de Cortana (le cercle) soit directement depuis la barre des taches, soit depuis le menu démarrer. En cliquant sur le livre puis sur » Paramètres » de Cortana.



Cnil

• Si vous disposez d'un compte connecté qui synchronise vos paramètres entre les différents terminaux équipés de Windows 10, vous pouvez désactiver cette synchronisation (et la collecte des données associées), en allant dans la fenêtre de » Paramètres » et en cliquant sur » Comptes « .



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

Source : http://www.huffingtonpost.fr/2015/08/10/vie-privee-donnees-personnelles-windows-10-astuces-cnil_n_7965788.html