Alerte à partager : Urgent – Mise à jour URGENTE votre Windows | Le Net Expert Informatique

Alerte à partager : Mise à jour URGENTE votre Windows

La découverte d'une faille critique ou Zero-Day dans Internet Explorer a contraint Microsoft à anticiper le prochain Patch Tuesday pour délivrer un correctif de sécurité. Le navigateur Edge de Windows 10 n'est pas affecté.

Selon le bulletin d'alerte de l'éditeur, une vulnérabilité expose les internautes, lors d'une visite sur un site piégé, à une exécution distante de code sur les postes Windows affectés. La faille zero-day (CVE-2015-2502) repose sur la façon dont Internet Explorer gère les objets dans la mémoire.
Une exploitation réussie de la vulnérabilité permet à l'attaquant d'obtenir les mêmes droits que l'utilisateur actif sur la session Windows, précise le bulletin de sécurité. Par conséquent, les utilisateurs dont le compte est paramétré avec les droits administrateurs sont les plus exposés.

Windows 10 et Edge : « la meilleure protection »
Selon Microsoft, aucun signe ne laisse penser que cette faille logicielle soit déjà exploitée pour des attaques. Un correctif est donc disponible, à télécharger sur le site de l'éditeur ou via Windows Update.
A noter que le navigateur Edge, le logiciel par défaut sur Windows 10, n'est pas affecté par la faille de sécurité. « Nous recommandons à nos clients d'utiliser Windows 10 et le navigateur Microsoft Edge pour la meilleure protection » ne manque d'ailleurs pas d'ajouter l'éditeur.
La découverte de cette vulnérabilité critique d'Internet Explorer est attribuée à un ingénieur de Google, Clement Lecigne. C'est le deuxième mois consécutif que Microsoft doit diffuser un correctif en-dehors de son cycle habituel.

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

Source : http://www.zdnet.fr/actualites/microsoft-corrige-en-urgence-toutes-les-versions-windows-39823686.htm

---

Cyber-attaque de pompe à morphine : mise en garde de

la FDA | Le Net Expert Informatique

Cyber-attaque de pompe à morphine : mise en garde de la FDA

La FDA met en garde contre les risques de prise de contrôle à distance des pompes à morphine ou PCA (de type PCA analgésie autocontrôlée par le patient) de type Symbiq Infusion System (produites par la marque Hospira). Ces pompes sont généralement prescrites dans le cadre de soins de suite ou d'hospitalisations à domicile.

Elles sont reliées sans fil aux systèmes de communication de l'hôpital pour transmettre des données sur les doses utilisées quotidiennement. Ces informations sont utilisées par les médecins pour adapter les protocoles de soins.

Un cyber-spécialiste démontre la possibilité d'attaques

C'est la deuxième fois en 4 mois que les pompes de ce fabricant font l'objet de cyber attaques, les premiers modèles impliqués étaient les LifeCare PCA3 et PCA 5 qui permettent de délivrer différents types de médicaments ou de traitements intraveineux.

Hospira a annoncé avoir cessé de produire les pompes en question ainsi que les Symbiq Infusion Systemet la FDA met en garde les établissements et les professionnels en les incitant à ne plus utiliser ces dispositifs.

Le département de la sécurité américain s'est saisi du dossier en raison des risques associé à ces cyber attaques (surdoses, ou sous dosage).

C'est un cyber spécialiste – Billy Rios [2] – qui a le premier soulevé cette question sur son blog et expliquant qu'il avait pu modifier les paramètres des pompes à distance sans disposer des codes spécifiques à chaque machines qui sont théoriquement indispensables pour modifier les doses.

Aucun cas de cyber attaque n'a été rapporté en utilisation thérapeutique aux Etats-Unis jusqu'à présent.

Une utilisation contrôlée en France – en théorie

En France, les pompes de type PCA sont utilisées dans les hôpitaux, en hospitalisation à domicile (dans un contexte de lien ville-hôpital), dans les services de soins palliatifs et dans certains centres de soins de suites/maisons de retraite médicalisés.

Elles servent à la prise en charges des douleurs chroniques de l'adulte, essentiellement d'origine cancéreuses et en soins palliatifs. Les principales marques de pompes à morphine de type PCA sont marque Vygon, Baxter, Gelstar, CADD Legacy et Rytmic Plus.

Les pompes à PCA électroniques ne doivent – en théorie – être manipulées que par le personnel médical (médecin ou IDE). Chaque marque diffuse avec le matériel un manuel d'utilisation pour les soignants et des codes permettant de modifier les paramètres ou changer les piles. Mais depuis quelques années, on peut trouver sur Internet des copies de ces manuels, ce qui pourrait permettre aux utilisateurs qui auraient récupéré les codes de façon illicite de modifier les paramètres dans un but de mésusage.

Source : http://www.medscape.fr/voirarticle/3601689
Par Dr Isabelle Catala avec Robert Lowes

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/

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

Les entreprises européennes bientôt obligées de signaler toute cyber-attaque ? | Le Net Expert Informatique

Les entreprises européennes bientôt obligées de signaler toute cyber-attaque ?

Les entreprises du domaine des nouvelles technologies opérant en Europe pourraient devoir systématiquement reporter toute intrusion sur leurs installations informatiques. Une directive devrait étendre cette obligation au secteur du numérique. Depuis 2013, l'Europe mène des discussions autour d'un texte visant à obliger les entreprises des secteurs de l'énergie, des transports, de la santé ou des services financiers à implémenter des mesures de sécurité minimales pour leurs installations informatiques. Baptisée NIS (pour Network and Information Security), cette directive implique surtout à ces mêmes professionnels de rapporter aux autorités compétentes tout incident informatique (cyber-attaque, intrusion, perte de données…).
Selon Reuters, cette directive pourrait être étendue à de nouveaux secteurs, à savoir à l'ensemble du domaine des nouvelles technologies. A terme, **ces sociétés qu'elles soient majeures ou non pourraient être soumises à ce devoir de divulgation en cas d'attaque informatique**.
A ce jour, certaines obligations incombent déjà aux opérateurs de réseaux d'importance vitale (eau, électricité…) mais également aux opérateurs de télécommunications. Ces derniers doivent par exemple signaler à la Cnil d'éventuelles pertes ou fuites concernant les informations personnelles de leurs clients.
Ce type d'obligation pourrait donc être étendu à davantage de sociétés. Ce volet doit toutefois être discuté devant les institutions communautaires ainsi que les Etats membres. Ces derniers devraient faire part de leurs critiques au sujet d'une extension trop large de ce texte à l'ensemble du secteur du numérique.

Un débat encore vif et des critiques toujours présentes
La question de la communication en cas de faille de sécurité reste majeure. Les exemples de fuites de données massives, comme celui de Sony, ont montré l'importance de tenir informer les personnes concernées mais aussi les autorités, pour qu'elles puissent éventuellement agir.
En Europe, et notamment en France, la question reste également pertinente. Comme nous le rapportions suite à une conférence sur le sujet, certaines entreprises préfèrent rester discrètes quant à leurs dispositifs et les relations entre « hackers blancs » peuvent rapidement tourner à l'incompréhension.
C'est pourquoi de nombreux professionnels, ou leurs représentants, critiquent une extension trop large des obligations de notification des failles de sécurité. Ces derniers craignent que ce type de contrainte nuise à la compétitivité des entreprises, ou n'entraîne un jeu du chat et de la souris peu profitable aux professionnels.

Source : http://pro.clubic.com/it-business/securite-et-donnees/actualite-776250-directive-nis.html
Par Olivier Robillart

Darkhotel récupère une faille chez Hacking Team | Le Net Expert Informatique

Le groupe de hackers Darkhotel, spécialisés dans le vol de données ciblant des dirigeants, récupère une faille zero day issue du piratage de Hacking Team pour peaufiner son arsenal.

Selon Kaspersky Lab, laboratoire de recherches en sécurité de l'éditeur, le groupe de hackers Darkhotel, connu pour avoir piraté les réseaux Wifi de luxueux hôtels afin de compromettre les machines de dirigeants d'entreprise, utilise un exploit récupéré lors de l'attaque contre Hacking Team. Rappelons que cette entreprise italienne, spécialisée dans la vente de failles zero day à des gouvernements, a été piratée en juillet. Une opération au cours de laquelle 400 Go de données avaient été dérobés, dont des informations sur des failles jusqu'alors inconnues. Certaines de ces vulnérabilités ont été corrigées en urgence dans le courant de l'été (par Adobe et Microsoft notamment).
Selon Kaspersky, Darkhotel utilise depuis début juillet une vulnérabilité zero day issue de la collection Hacking Team et ciblant Flash Player. L'exploit est hébergé sur un site web compromis (tisone360.com). « N'étant pas connu comme un client de Hacking Team, le groupe Darkhotel semble s'être emparé des fichiers lors de leur divulgation publique », explique l'éditeur russe.

27 antivirus contournés
Les chercheurs de la société estiment que, au cours de ces dernières années, le groupe de hackers a employé une demi-douzaine, voire plus, de ces vulnérabilités visant Adobe Flash Player et a investi largement pour bâtir cet arsenal. Le groupe de hackers a par ailleurs sophistiqué son kit d'infection, en améliorant notamment ses capacités à échapper aux antivirus. L'outil de téléchargement que déploient les hackers afin d'infecter les systèmes de leurs victimes identifie désormais 27 technologies d'antivirus, afin de les contourner.
« De précédentes attaques nous ont appris que Darkhotel espionne les Pdg, senior vice-présidents, directeurs marketing ou commerciaux et de hauts responsables en R&D », rappelle Kurt Baumgartner, chercheur en sécurité au sein des Kaspersky Lab.

Source : http://www.silicon.fr/darkhotel-recupere-faille-hacking-team-123796.html
Par Reynald Fléchaux

Les attaques DRDOS peuvent se propager via les clients BitTorrent | Le Net Expert Informatique

Les attaques DRDOS peuvent se propager via les clients BitTorrent

L'attaque DRDOS (Distributed Reflective Denial of Service) est une variante du DDoS, mais elle est plus puissante et elle peut se propager sur de nombreux protocoles incluant ceux du BitTorrent. Florian Adamsky de la City University London propose un article sur le potentiel nuisible du DRDOS concernant les protocoles BitTorrent.

La plupart connaissent les attaques DDoS, mais le DRDOS est un peu différent. Dans une attaque DDoS, le pirate contrôle un ensemble de machines zombies pour attaquer la cible. Dans une DRDOS, le pirate envoie le trafic à un réseau légitime (appelé le réflecteur) qui transmet ensuite le trafic à la victime. Le trafic qui est envoyé au réflecteur est modifié pour que pour l'adresse IP de la victime soit utilisé plutôt que le paquet d'origine. Et quand le réflecteur respecte les normes habituelles des protocoles internet pour établir la connexion, alors tout le trafic est balancé vers la victime. Et étant donné que cela implique d'envoyer une énorme quantité de trafic vers un réflecteur, les pirates ont trouvé le moyen de l'utiliser pour amplifier le trafic. Les attaques DRDOS peuvent être utilisées vers les protocoles TCP, DNS et NTP. Mais l'article d'Adamsky démontre aussi que le DRDOS peut être exploité avec de nombreux protocoles du BitTorrent.

Les protocoles uTP, MSE, DHT et BTSync sont vulnérables aux attaques DRDOS

Selon Adamsky, les protocoles BitTorrent affectés sont l'uTP (Micro Transport Protocol), le DHT (Distributed Hash Table) et le MSE (Message Stream Encryption). Ces protocoles sont intégrés en natif sur les clients de Torrent BitTorrent, uTorrent et Vuze. De plus, le protocole de synchronisation BTSync, qui est utilisé avec BitTorrent Sync, est également vulnérable. Florian Adamsky a démontré que les tests permettaient d'amplifier le trafic de 50 à 120 fois sur la norme BTSync.

Les attaques DRDOS sur les protocoles BitTorrent sont indétectables par les pare-feu

Mais la mauvaise nouvelle ne s'arrête pas là. En plus d'amplifier considérablement l'attaque, le DRDOS sur BitTorrent ne peut pas être détecté avec des pare-feu standard à cause de l'utilisation de ports dynamiques et du chiffrement pendant les échanges de données sur ces protocoles. Pour contrer ce type d'attaque, il faudrait utiliser une solution telle que DPI (Deep Packet Inspection) qui est trop coûteuse pour la majorité des infrastructures. BitTorrent a corrigé certains de ces problèmes avec sa version en bêta, mais Vuze et BitTorrent travaillent encore pour colmater les brèches qui permettent d'exploiter le DRDOS.

Source : http://actualite.housseniawriting.com/technologie/2015/08/16/les-attaques-drdos-peuvent-se-propager-via-les-clients-bittorrent/7227/
Par Houssen Moshinaly

CNIL Besoin d’aide ? – Séances du conseil municipal : faut-il déclarer à la CNIL leur enregistrement vidéo ? | Le Net Expert Informatique

Faut-il déclarer à la CNIL les enregistrement vidéo des séances du conseil municipal ?

L’enregistrement et la diffusion sur internet des images d’une séance d’un conseil municipal constituent un traitement automatisé de données à caractère personnel. En effet, les membres du conseil peuvent être identifiés sur ces images.

Dès lors, celui qui filme et diffuse les images, qu’il s’agisse de la mairie, d’un conseiller municipal ou d’un membre du public, doit effectuer une déclaration normale auprès de la CNIL.
En outre, les personnes filmées doivent en être informées.

Nous réalisons régulièrement des actions de **mises en conformité de collectivités auprès de la CNIL**. pour vous permettre de respecter la loi informatique et libertés, la réglementation de référence relative à la protection des données personnelles.
Besoin d’informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

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 : https://cnil.epticahosting.com/selfcnil/site/template.do;jsessionid=1984913614D7AAF7D9FD169D254E833A?id=174&back=true

---

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.

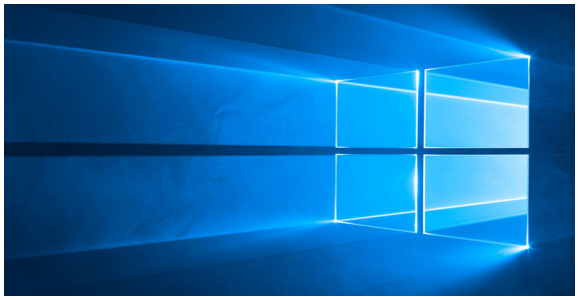
Avec tous les fichiers et applications «illégitimes» qui circulent librement sur les réseaux louches, l'idée de les croire tous «sains» et sans danger n'est que pur délire.

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