L’anonymat du WHOIS remis en question à l’ICANN | Le Net Expert Informatique

	L’anonymat du WHOIS remis en question à l’ICANN

Une proposition de l'ICANN s'est attiré les foudres des commentateurs et de l'EFF. La suggestion propose de rendre impossible l'anonymisation des données personnelles sur le service WHOIS pour les sites à vocation commerciale.

Le service WHOIS est un outil particulièrement utile pour savoir qui se cache derrière un nom de domaine et comment contacter les responsables d'un site. Fourni par les registres de noms de domaines, il permet d'interroger les bases de données des bureaux d'enregistrement afin de connaître le nom et l'identité de la personne ou de la société détenant le nom de domaine, ainsi que certaines informations de contacts.
Ces informations ne sont pas forcement accessibles à tout le monde : dans de nombreux cas et pour éviter de voir ces informations personnelles à l'air libre, les bureaux d'enregistrement proposent un service d'enregistrement via proxy permettant de dissimuler au public les données et de les réserver aux seules personnes munies d'autorisations légales fournies par un service judiciaire national. Le service agit donc comme un écran afin d'offrir un moyen de contacter le propriétaire du nom de domaine tout en protégeant ses données personnelles.
Mais une proposition de l'ICANN, ouverte depuis mardi aux commentaires publics, envisage de revenir sur le fonctionnement de ce système en ouvrant à tous les données WHOIS des sites à but commercial. Selon l'EFF, cette règle s'appliquant « à tous les sites commerciaux » pourrait toucher de nombreux petits administrateurs de sites et de communautés en ligne qui ont choisi de mettre en place de la publicité ou un système de dons pour subvenir au coût de leur site.
L'EFF cite ainsi l'exemple de TG Storytime, un paisible site de fanfiction à destination des communautés LGBT, qui pourrait ainsi se voir obligé de révéler certaines informations personnelles liées à l'administrateur du site si la nouvelle proposition était approuvée par l'ICANN.

L'EFF dans la boucle
L'EFF explique que ce changement est notamment soutenu par le secteur du divertissement, qui entend ainsi simplifier les procédures judiciaires à l'égard des sites diffusant des contenus constituant des infractions relatives à la propriété intellectuelle. Outre le risque que cette proposition peut faire peser sur les données personnelles des utilisateurs, on peut également évoquer les dangers relatifs à la cybersécurité.
Cedric Pernet, dans son ouvrage sur les Advanced Persistent Threat, citait ainsi les informations de service WHOIS parmi la liste des sources utiles aux attaquants pour préparer leurs attaques, en leur permettant d'identifier précisément le bureau d'enregistrement d'un site, un numéro de téléphone ou encore le nom de l'employé chargé d'administrer le nom de domaine.Autant d'informations utiles pour une attaque de type spear phishing.
La proposition est ouverte aux commentaires jusqu'au 7 juillet, et suscite déjà un certain engouement de la part des opposants à ce changement de politique, qui ont déjà posté des milliers de commentaires invitant l'ICANN à refuser cette proposition.

Source : http://www.zdnet.fr/actualites/l-anonymat-du-whois-remis-en-question-a-l-icann-39821566.htm
Par Louis Adam

Un centre de compétence Kaspersky doit être mis en place très prochainement au Gabon | Le Net Expert Informatique

Un centre de compétence Kaspersky doit être mis en place très prochainement au Gabon

Un centre de compétence Kaspersky doit être mis en place très prochainement au Gabon, selon les termes d'un accord de partenariat signé mardi à Libreville entre l'Agence nationale des infrastructures numériques et des fréquences (Aninf) et l'éditeur Kaspersky.

En vertu de cet accord, signé par le directeur général de l'Aninf, Alex Bernard Bongo Ondimba et le vice-président de Kaspersky, Veniamin Levtsov, le futur centre, qui aura, par ailleurs, une vocation sous régionale, doit permettre au Gabon d'assurer la veille, la détection, l'analyse et la prévention des cyber-attaque.

« Ce partenariat est très salutaire pour le Gabon du fait qu'il nous permettra de nous doter d'un véritable système de défense en matière de virus et en ce qui concerne la cybercriminalité », a déclaré M. Alex Bernard Bongo Ondimba.

Outre la mise en place d'un centre de compétence au Gabon, l'accord signé porte également sur le transfert des compétences dans les domaines de la sécurité industrielle et de la cybercriminalité.

'Nous entendons contribuer à sauver le monde en mettant en place des systèmes de lutte contre des attaques axées sur la cybercriminalité. Nous voulons également apporter nos compétences aux structures locales », a affirmé, pour sa part, M. Levtsov.

Implantée dans plusieurs pays d'Afrique et dans d'autres continents, Kasperky est une entreprise russe leader mondiale en matière de sécurité informatique.

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

Source :
https://mail.google.com/mail/u/0/?hl=fr&shva=1#inbox/14e3b659f932c0fd?compose=14e2eb99aeedd11a

Surveillance informatique par la NSA, C’est bien réel | Le Net Expert Informatique

Surveillance informatique par la NSA, C’est bien réel

Sur son blog, le cybercriminologue Jean-Paul Pinte a relayé un article du « Monde » racontant comment la NSA avait pu surveiller les organes de pouvoir de la France. « C'est bien réel, ce n'est pas de la science-fiction » assure-t-il.

Maître de conférences à l'université de Lille, spécialiste de la veille et de l'intelligence compétitive, il estime que la France devait savoir qu'elle était surveillée. Notamment « après l'expérience vécue par Angela Merkel en 2012 et 2013. Il ne peut donc y avoir de surprise, surtout vis-à-vis des États-Unis. Ceci dit, pour les pays qui subissent ce genre de surveillance, la principale chose qui les dérange c'est qu'ils ne peuvent pas faire la même chose. »
> Les moyens des États-Unis. Pour Jean-Paul Pinte la puissance acquise par les États-Unis dans le domaine du renseignement n'a pas d'égal. « Ils ont des logiciels comme Upstream qui vont capter les informations et analyser les contenus. Même involontairement, on peut être à la base d'une surveillance. Imaginez deux personnes qui communiquent par mail. L'une fait partie d'Alcatel ou EDF et si elle raconte qu'il y a du mouvement dans son entreprise, ce sera capté. » On a beaucoup parlé du programme Prisme, « cela prouve que les États-Unis pratiquent ce genre de surveillance depuis très longtemps ». Et les écoutes téléphoniques à la sauce américaine ont « plus de 50 ans ».
> L'espionnage dépasse les États. C'est pour cela que Jean-Paul Pinte ne croit absolument pas à la possibilité d'instaurer un code de bonne conduite. « Il faut être naïf pour penser s'en sortir comme ça. C'est une méconnaissance des entrailles du Web qui vont au-delà des États. Les États-Unis ont par ailleurs une certaine emprise sur Internet, ils peuvent fermer ou ouvrir des robinets et bloquer des pays, ils ont accès aux infrastructures, aux câbles et Prisme, Upstream… sont tellement puissants qu'ils sont presque devenus indolores. »
> Avoir toujours un coup d'avance. L'espionnage a toujours existé. « Aujourd'hui encore, des passagers montent dans l'Eurostar en première classe uniquement pour écouter les conversations de cadres ou de patrons du Cac40 et en faire des rapports. » Et le citoyen lambda n'est pas en reste. « Nous laissons énormément d'informations en chemin. C'est ce qu'on appelle aussi des métadonnées qui permettent de suivre nos pérégrinations, nos interactions sur les réseaux sociaux… » Pour l'espion, le tout est de ne pas se faire prendre. « Ce qui importe c'est que celui qu'on surveille ne soit pas conscient des écoutes. En cybercriminalité, c'est la même chose. C'est ce qui permet de se garantir d'avoir toujours un coup d'avance. »
Lire la suite….

Source : http://www.centre-presse.fr/article-397900-jean-paul-pinte-il-ne-peut-y-avoir-de-surprise-surtout-venant-des-etats-unis.html

---

Un hacker cloue plusieurs

avions au sol | Le Net Expert Informatique

Un hacker cloue plusieurs avions au sol

Une attaque informatique subie par la compagnie polonaise LOT a causé l'annulation de 20 vols dimanche.

Des hackers qui clouent des avions au sol. Ce n'est pas le scénario d'un film catastrophe, mais la mésaventure subie dimanche par la compagnie polonaise LOT et racontée par CNN.
Les ordinateurs au sol piratés. Tout a commencé à l'aéroport Chopin de Varsovie, où la compagnie dit avoir été victime d'une attaque. Ses ordinateurs au sol, utilisés pour créer les plans de vols, ont subi une attaque. Résultat : impossible de créer des plans de vols pour les avions au départ de la capitale polonaise.
Au total, la compagnie polonaise a dû annuler pas moins de 20 vols et plusieurs autres ont subi des retards. Quelque 1.400 passagers ont ont été affectés. Une enquête a été ouverte, mais les autorités ignorent l'identité des hackers.
Un hacker arrêté en mai. Ce n'est pas la première fois que des hackers illustrent la vulnérabilité des compagnies aériennes : fin mai, un pirate américain a été arrêté par le FBI après s'être vanté sur Twitter d'avoir réussi à hacker un avion en plein vol. Il assure s'être connecté au système informatique de l'avion et avoir légèrement modifié la trajectoire de l'avion, afin de démontrer les faiblesses du système de sécurité aérien.

Source : http://www.europe1.fr/international/un-hacker-cloue-plusieurs-avions-au-sol-1359726

Une convention internationale pour lutter contre le cybercrime | Le Net Expert Informatique

	Une convention internationale pour lutter contre le cybercrime

En avril 2015, la société Symantec spécialisée dans la sécurité informatique présentait son rapport annuel. Selon ses dires, en 2014, 317 millions de nouveaux programmes malveillants auraient été crées au niveau mondial. Enfin, faut-il rappeler ce qui est arrivé à nos amis de TV5 Monde, il y a de cela quelques semaines ? Ecran noir pour la chaîne les 8 et 9 avril 2015. Sans que pour le moment on sache d'où vient l'attaque.

C'est une évidence, la cybercriminalité est en pleine croissance. Multiforme, mondialisée, l'œuvre d'un petit génie malfaisant, ou d'organisations criminelles quand il ne s'agit pas d'une nouvelle arme d'Etat. Une pieuvre, Octopus…

La Convention de Budapest

Pour le moment, le seul grand texte international existant dans le cadre de la lutte contre ce type de criminalité est l'œuvre du Conseil de l'Europe. Signée à Budapest en novembre 2001, la convention traite des infractions possibles à l'égard des droits d'auteur, de la sécurité des réseaux informatique, des fraudes en général et aussi à la lutte contre la pornographie enfantine. Un texte unique en son genre, qui dépasse le seul cadre du Conseil de l'Europe. Puisque déjà 66 pays du monde entier ont adhéré. Dernier en date, il y a de cela quelques jours le Sri Lanka.

Que ce soit le Conseil de l'Europe qui est en pointe dans ce combat ne paraît pas illogique. Comme le rappelle le spécialiste de cette lutte au sein du Conseil de l'Europe, Alexander Seger, ce sont les droits de l'Homme et la démocratie qui sont en danger.

Ce texte permet avant tout de mener la bataille du droit. Il n'a pas de rapport avec les lois en cours sur le renseignement et qui font beaucoup la Une dans de nombreux pays dont la France. En revanche, devant la croissance de ce type de criminalité et le développement toujours plus rapide de la technique, ce texte doit constamment évoluer de même que les pratiques des autorités. Ainsi le Conseil de l'Europe vient-il de créer à Bucarest un bureau destiné à encadrer et à proposer une aide technique aux juristes ou aux politiques lancés dans ce combat.

De même, tous les 18 mois, une grande réunion internationale se tient avec tous les acteurs concernés. C'est cette réunion qui répond au doux nom d'Octopus. La dernière se tient à Strasbourg ces jours-ci. Ces conférences permettent de faire le point sur de nouvelles pratiques problématiques qui apparaissent. Ainsi sur le droit des victimes passablement oubliées pour le moment ou bien encore, et ce sera le thème principal des travaux, sur la difficulté pour la justice de trouver des preuves informatiques. Dans quel disque dur les trouver, quel nuage explorer ? En rappelant à nouveau qu'il ne s'agit là que d'un texte portant sur le judiciaire.

Il y a quelques semaines, à La Haye, s'est tenu également une Conférence mondiale sur le Cyber espace 2015. Cette rencontre qui prend en compte les extraordinaires possibilités qu'offre internet avait pris en compte également la question de la sécurité qui doit régner dans le cyberespace. La prise de conscience est donc bien là, il faut espérer que les techniques des criminels quels qu'ils soient n'aillent pas en se développant plus vite que les solutions. Or, et l'on revient à l'étude annuelle de Symantec, il faut désormais aux éditeurs de logiciels beaucoup plus de temps pour créer et déployer des correctifs en cas de faille sécuritaire.

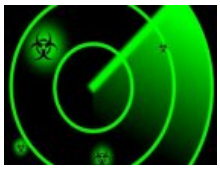
Et s'il fallait vous convaincre du problème, un dernier exemple, celui des « rançongiciels ». Ils prennent le contrôle de vos PC et vous piquent littéralement vos données rendues plus tard contre rançon. Une entreprise française s'est vu réclamer ainsi 90.000 euros.

Et vous, si vous êtes amateurs de pizzas, vous risquez gros…

Lire la suite….

Source : http://geopolis.francetvinfo.fr/une-convention-internationale-pour-lutter-contre-le-cybercrime-65027

Une faille de Flash exploitée pour des attaques de phishing contre des entreprises | Le Net Expert Informatique



Une faille de Flash exploitée pour des attaques de phishing contre des entreprises

Alerté début juin par FireEye de l'exploitation d'une faille inconnue de Flash pour des attaques ciblées de phishing, Adobe met à jour son plugin Flash sur Windows et Mac OS X.

Une nouvelle faille critique de Flash a été identifiée. C'est banal, presque. Adobe, l'éditeur de Flash, est régulièrement confronté à des problèmes de sécurité. Toutefois, si la vulnérabilité a été découverte c'est car celle-ci faisait d'ores et déjà l'objet d'exploitations malveillantes.
C'est la société de sécurité FireEye qui a détecté ces attaques. Plus tôt ce mois-ci, ses chercheurs ont repéré des campagnes de phishing dirigées contre des entreprises et exploitant une faille inconnue de Flash.

Des attaques « limitées »
Selon FireEye, ces attaques de phsihing ont ainsi ciblé des entreprises des secteurs de l'aéronautique, de la défense, de la construction, des transports mais aussi de l'informatique et des télécoms. L'acteur de la sécurité a alerté Adobe début juin.
L'éditeur a donc été contraint de diffuser un correctif de sécurité, en dehors de son cycle habituel de mise à jour. Adobe assure que le nombre d'attaques ciblées exploitant la faille est resté limité.
La firme ajoute qu'Internet Explorer sur Windows 7 (et les versions suivantes) est affecté par ce problème de sécurité, tout comme Firefox sur Windows XP. La version 18.0.0.194 du plugin Flash remédie à la vulnérabilité sur Windows et Mac OS. Les utilisateurs de Chrome recevront automatiquement la mise à jour.

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

Source : http://www.zdnet.fr/actualites/une-faille-de-flash-exploitee-pour-des-attaques-de-phishing-contre-des-entreprises-39821388.htm

Les gouvernements occidentaux sous le feu des cyberattaques | Le Net Expert Informatique

24

Mercredi 17 juin, Tony Clement, le président du Conseil du Trésor (l'équivalent du ministre du Budget), a confirmé une cyberattaque en cours contre des sites gouvernementaux. À savoir, celui du Sénat, du ministère des Travaux Publics, du ministère de l'Industrie ou encore du service aux citoyens.

Cette attaque a entraîné le blocage de ces sites pendant plusieurs heures. Contrairement à l'attaque du Bundestag, cette cyberattaque a été revendiquée par le mouvement des Anonymous, qualifié de « groupe terroriste » par plusieurs médias canadiens.
Les Anonymous souhaitent « protester contre une nouvelle loi antiterroriste qui accroît significativement les pouvoirs des services secrets canadiens, mais sans aucun garde-fou autonome », nous précise Le Monde.
La loi antiterroriste C-51, adoptée le 6 mai dernier, porterait atteinte aux droits et libertés des Canadiens en ne visant que « les groupes minoritaires et les dissidents ». Elle donnerait en outre beaucoup plus de pouvoir au Service canadien du renseignement de sécurité (SCRS).
« Troque-t-on notre vie privée au nom de la sécurité ? », se demande la vidéo YouTube diffusée sur les réseaux sociaux. Une question très actuelle et surtout applicable à moult pays en guerre contre le terrorisme.
Néanmoins, le compte Anon_GovernmentWatch a assuré sur Twitter que « ce n'était pas nous cette fois-ci ».
La multitude de comptes se revendiquant des Anonymous rend difficile toute prise de position officielle. Mais au vu des messages qui suivent, le doute est de mise.
En revanche, il s'amuse du terme de « cyberattaque » employé pour une attaque en DDoS et encore plus du qualificatif de « terroriste ».

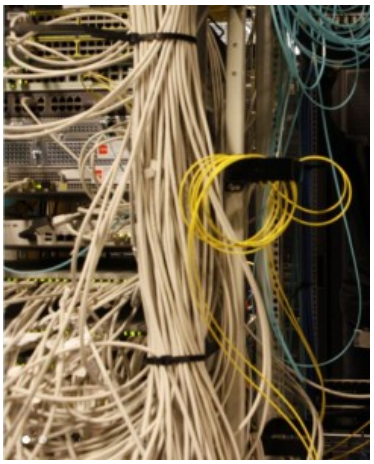
Encore une fois, ces attaques, contrastées dans leurs moyens et leur finalité, montrent à quel point les gouvernements sont exposés et vulnérables face aux cyberattaques, révélant des failles béantes en matière de cyberdéfense alors même que ces administrations prônent une surveillance toujours plus accrue et rendue possible par un déploiement de moyens ultra sophistiqués. Tragiquement ironique.

« On est un peu les cancres en ce qui a trait à la cybersécurité. On est les derniers élèves dans le fond de la classe », se désole Rosane Dorée Lefebre, porte-parole adjointe en matière de sécurité publique du NPD dans les colonnes de Radio Canada.

Quoi qu'il en soit, la classe de remplie de plus en plus de cancres… et les pirates ou « services étrangers » en profitent allègrement. Russes ? Chinois ? Accusations avérées ou non, le pacte de non-agression 2.0 signé récemment entre la Chine et la Russie apparaît donc très opportun…

Source : http://www.journaldugeek.com/2015/06/18/gouvernements-occidentaux-sous-le-feu-des-cyberattaques/

Le business des écoutes et des données personnelles | POLICEtcetera | Le Net Expert Informatique



Le business des écoutes et des données personnelles

Au moment où les États-Unis sont en train – timidement – de faire machine arrière sur le Patriot Act, la France se dote d'une véritable armada de machines électroniques pour surveiller ses propres ressortissants – et à l'occasion, les étrangers de passage dans notre beau pays. Dans cette guerre secrète contre le crime et le terrorisme, qui s'est amplifiée ces dernières années, pas de chars, pas d'avions, pas d'armes, mais un chiffre d'affaires en pleine érection. On peut se demander à qui profite le crime et combien cela va nous coûter… Dans quelle poche va-t-on prendre les sous ? Au détriment de quels services publics ?…

Nous sommes tellement habitués à ces projets qui capotent, comme Ecomouv ; ou d'autres qui aboutissent, mais dont la facture a été multipliée par 2, 3, 4…
Tiens, par exemple, parlons de la plateforme nationale d'interceptions judiciaires (PNIJ). En 2007, il était question d'une enveloppe de 17 millions d'euros. En 2010, elle était de 42 millions, et en 2014, de 47. En cette année 2015, alors que les premiers essais ont commencé dans certains services de police et de gendarmerie sur le ressort des cours d'appel de Paris, Versailles et Rouen, on se rapprocherait des 55 millions. C'est du moins ce que dit Le Canard enchaîné daté du 20 mai 2015, ajoutant malicieusement, que, pour l'instant, seuls les clients d'Orange peuvent être mis sous écoute.
En fait, l'addition sera beaucoup plus lourde, car, parallèlement, les fournisseurs d'accès à Internet ont dû effectuer des travaux et notamment déployer des fibres optiques jusqu'à Élancourt, dans les Yvelines, sur le site de Thales qui accueille la PNIJ. Il faut également revoir les réseaux des services de police, de gendarmerie, des douanes… Lors du jeu de questions à l'Assemblée Nationale, le député Alain Tourret a avancé un surplus de 50 millions. Il n'a obtenu ni confirmation ni infirmation de ce chiffre, la garde des Sceaux se contentant de dire qu'il était prévu que le ministère de l'Intérieur participe au pot commun.
Et l'addition n'est pas close, car il pourrait se révéler nécessaire de renforcer la sécurité de la PNIJ. On se souvient des propos tenus lors du débat sur la loi sur le renseignement : la centralisation des données dans un même lieu géographique « pourrait constituer une source de vulnérabilité importante ». La centralisation nationale des réquisitions judiciaires constitue donc une faiblesse dans la sécurité, ce que policiers et magistrats n'ont cessé de clamer depuis que l'idée est dans l'air. D'autant que cette plateforme, contrairement à ce que son nom peut laisser penser, n'est pas seulement destinée à intercepter les communications téléphoniques : c'est un système complet de traitement automatisé de données à caractère personnel. Une machine qui va brasser et enregistrer les données personnelles de toutes les personnes impliquées ou suspectées dans une affaire judiciaire.
Une caverne d'Ali Baba sur laquelle les services de renseignement, français ou étrangers, vont forcément loucher. À ce sujet, on peut d'ailleurs s'interroger sur la portée exacte de l'amendement de dernière minute (un de plus) présenté par le gouvernement à la loi sur le renseignement : les services habilités pourront avoir accès aux traitements automatisés de données à caractère personnel, y compris celles des procédures judiciaires en cours. Il s'agit pour ces services, nous dit-on, de pouvoir consulter le TAJ, c'est-à-dire le fichier d'antécédents judiciaires (qui a remplacé le STIC de la police et le JUDEX de la gendarmerie). Mais alors, pourquoi ce pluriel dans l'article L.234 : « pourront avoir accès aux traitements automatisés… » Cela vise-t-il également le fichier Cassiopée du ministère de la Justice et la PNIJ ?
Je vais finir parano !
Lire la suite….

Source : http://moreas.blog.lemonde.fr/2015/06/21/le-business-des-ecoutes-et-des-donnees-personnelles
par G.Moréas

Des hackers paralysent l’aéroport de Varsovie pendant cinq heures | Le Net Expert Informatique

Des hackers paralysent l’aéroport de Varsovie pendant cinq heures

Une attaque contre les systèmes informatiques de la compagnie aérienne polonaise LOT a cloué au sol dimanche 1400 passagers pendant plus de cinq heures à l’aéroport Chopin de Varsovie. Une dizaine de vols intérieurs et internationaux ont été annulés.

L’attaque a eu lieu vers 17 heures (en Suisse). Le système informatique visé régit le plan des vols de la compagnie, sans lequel aucun décollage ne peut se faire. Le problème a été maîtrisé vers 22 heures, a annoncé LOT.
Le trafic aérien a repris en fin de soirée. « Il s’agit d’une première attaque de ce genre (contre LOT, ndlr). Il y a eu dans le passé des attaques contre d’autres compagnies aériennes », a déclaré un porte-parole de la compagnie.
« Ces attaques ont des effets pénibles et très spectaculaires », a-t-il ajouté, en déplorant les inconvénients causés aux passagers. Il a assuré qu’ils avaient reçu l’aide nécessaire, y compris la possibilité de passer la nuit dans des hôtels à Varsovie.
Les services de sécurité polonais, notamment l’agence de sécurité intérieure ABW et le centre gouvernemental de sécurité, ont été mobilisés.

Source : http://www.lacote.ch/fr/monde/cybercriminalite-des-hackers-paralysent-l-aeroport-de-varsovie-pendant-cinq-heures-481-1476594
Source : ATS

Les Samsung Galaxy vulnérables aux cyber-attaques | Le Net Expert Informatique

Twin Design / Shutterstock.com	**Les Samsung Galaxy vulnérables aux cyber-attaques**

Les claviers virtuels SwiftKey, pré-installés sur les Samsung, pourraient être une porte ouverte pour les hackers. Une société de cybersécurité américaine a découvert une faille dans plus de 600 millions de portables.

Vous avez peut-être déjà été hacké

Le coupable : le clavier virtuel SwiftKey. Il appartient à la suite d'applis et de fonctionnalités que les Samsung rajoute à Android,. Comme toute application, SwiftKey subit des mises à jour fréquentes. La société de cybersécurité NowSecure a découvert que lorsque le téléphone recherche des mises à jour à effectuer, il communique ouvertement, sans chiffrer sa requête.

Pour étayer leur dires, les chercheurs de NowSecure ont réussi à se faire passer pour le serveur qui envoie les mises à jour aux téléphones Samsung et à y injecter des programmes permettant d'exploiter les appareils à l'insu des utilisateurs. Peut-être que, sans le savoir, vous avez déjà été hacké.

Impossible à désinstaller

Cette vulnérabilité concerne les modèles Galaxy S4, S4 Mini, S5 et S6. Le problème étant que l'application SwiftKey fait partie des programmes de base livrés avec le téléphone, au même titre que les applis de Google. Il est donc impossible de la désinstaller.

En attendant que le problème soit réglé, NowSecure conseille aux utilisateurs d'« éviter les réseaux Wi-Fi non sécurisés », ou plus radicalement d'« utiliser un autre appareil mobile ». Samsung a lui annoncé une future mise à jour de sa solution de sécurité Knox, pour combler cette faille.

Actuellement, un hackeur s'attaquant à votre téléphone pourrait avoir accès aux capteurs et aux ressources comme le GPS, l'appareil photo et le micro, installer secrètement des applications malveillantes, espionner les messages entrants et sortants ou les appels ou encore tenter d'accéder à des données personnelles sensibles comme les photos ou les textos.

Qu'en est-il en France ?

Contactée par Le Figaro, la société NowSecure confirme que le phénomène est «mondial», et donc que la France est concernée. Elle a notifié cette faille à Samsung en décembre 2014, ainsi qu'à l'équipe de sécurité d'Android.

Si Samsung a publié un correctif début 2015, « on ne sait pas si les opérateurs téléphoniques ont implémenté ce correctif dans les appareils de leurs réseaux », explique NowSecure. L'entreprise n'a diffusé qu'une liste des opérateurs touchés aux États-Unis.

En France, seul Bouygues Télécom a pour l'instant été en mesure de fournir une réponse des plus inquiétantes, assurant que « Samsung n'a jamais fait remonter le problème à nos équipes techniques » et qu'il est désormais « très sérieusement à l'étude ».

Source : http://news.radins.com/actualites/les-samsung-galaxy-vulnerables-aux-cyber-attaques,13394.html