Les 5 dangers pour vos ordinateurs, smartphones et données en 2016

Les 5 dangers pour vos ordinateurs, smartphones et données en 2016

Les 5 tendances qui motiveront leurs actions envers votre ordinateur, votre smartphone, vos données…

Ecartelée entre la démocratisation de l'Internet des objets (thermostat intelligent, balance connectée…), la prise de pouvoir du stockage dans le « cloud » et l'émergence des nouveaux smartphones vedettes, la sphère des nouvelles technologies subira en 2016 les assauts des virus virulents, des arnaques en ligne, des cybercriminels.
Comme un caméléon virtuel, la cybercriminalité s'adaptera plus que jamais à l'air du temps pour exploiter les nouveaux territoires en friche.
Entre prudence et clairvoyance, voici les 5 tendances cybercriminelles qui se développeront ces 12 prochains mois, selon les experts de l'éditeur de solution de sécurité BullGuard.

1. La montée en puissance du « ransomware »
Impitoyable méthode d'extorsion, le « ransomware » bloque votre ordinateur, crypte vos fichiers personnels et vous réclame un paiement en ligne pour les libérer.
La menace brandie en cas de refus de payer la rançon : l'extermination de vos données (photos, vidéos, documents…).
Alors que les virus à l'ancienne et les chevaux de Troie accusent une certaine perte de vitesse, le « ransomware » est appelé à les dribbler.
Ces logiciels malveillants s'attrapent en visitant un site préalablement « hacké » (piraté) ou un obscur site volontairement malveillant, en téléchargeant des fichiers vérolés, notamment sur les plateformes d'échange de fichiers illégaux…

2. Le smartphone, cette cible indiscrète
Connecté à Internet 7 jours sur 7, 24 heures sur 24 dans le scénario le plus extrême, le smartphone concentre une myriade de données personnelles, des adresses email de vos contacts au numéro de votre carte de crédit.
Le téléphone est par conséquent une cible de choix pour les cybercriminels, qui rivalisent d'ingéniosité pour contourner les nouvelles barrières de sécurité régulièrement déployées par Apple pour ses iPhone et Google pour son système d'exploitation mobile Google Play.
Après avoir concentré leurs efforts sur la Chine et l'Extrême-Orient, les cybercriminels devraient viser tout particulièrement l'Europe en 2016.
Certes, nos smartphones étaient déjà menacés par le virus et les logiciels malveillants. Hélas, le niveau d'alerte devrait grimper de quelques degrés.

3. L'Eldorado inquiétant de l'Internet des objets
Nouvelle marotte des constructeurs, l'Internet des objets entend envahir notre quotidien pour évaluer et prédire nos besoins, mesurer notre activité, adapter l'éclairage et le chauffage de notre habitation en fonction de nos usages…
Qu'il s'agisse d'un pèse-personne connecté ou d'un thermostat intelligent, ces appareils vulnérables de par leur connexion constante à Internet récoltent au kilo les données personnelles.
Imaginons le cas d'une caméra de sécurité connectée. Elle pourrait simplement être détournée par un cybercriminel pour détecter les moments où vous quittez votre maison.
Toujours en quête d'un standard, notamment pour la sécurité, la galaxie de l'Internet des objets, tout juste née de son Big Bang historique, ne manquera pas de révéler en 2016 ses failles et ses vulnérabilités.

4. Des nuages dans le ciel du « cloud »
Inexorable lame de fond qui modifiera à jamais le monde du stockage, le « cloud » éparpille données et fichiers dans un nuage de serveurs (ordinateurs) répartis dans d'immenses « data center » aux quatre coins du monde.
Ces « fermes » informatiques dédiées au stockage et au traitement des données présentent un double intérêt pour les cybercriminels.
Leur puissance peut être détournée à d'autres fins, tandis que les données stockées constituent un sérieux trésor de guerre au cœur duquel il est tentant de piocher.
Objet de toutes les attentions des esprits mal intentionnés, la vulnérabilité du « cloud » risque d'être régulièrement soulignée ces prochains mois.

5. Les gangs sous les projecteurs
Les cybercriminels se structurent en gangs d'une efficacité redoutable, souligne BullGuard.
« Ils passent des semaines, voire des mois, à effectuer des missions de reconnaissance avant d'attaquer des organisations », témoignent les experts de l'éditeur. « Ces entreprises ont été conçues dès le départ pour se spécialiser dans les crimes informatiques et ont des hiérarchies cloisonnées qui incorporent des programmeurs spécialisés dans le piratage, de vendeurs de données et des gestionnaires, tous supervisés par un cadre supérieur. Ces équipes de cybercriminels occuperont le devant de la scène en 2016. »

Réagissez à cet article

Source : *Virus, arnaques en ligne, cybercriminalité : les 5 dangers de l'année 2016 – L'Avenir Mobile*

Une célèbre PME de Montmorillon victime de piratage et de chantage

Une célèbre PME de Montmorillon victime de piratage et de chantage

Des pirates informatiques ont volé les données de clients sur le site de l'entreprise montmorillonnaise et tenté de faire chanter ses dirigeants.

Ils ne venaient pas pour les macarons et le chocolat : en début de semaine, des pirates informatiques ont attaqué le site internet de Rannou-Métivier, célèbre PME de Montmorillon. Ils visaient particulièrement la base de données de la clientèle.
« Notre service informatique a immédiatement réagi pour renforcer la sécurité du site. Cependant, des données ont déjà été volées », a fait savoir l'entreprise, mardi après-midi, dans un courrier adressé à tous ses clients disposant d'un compte sur son site.
« Une personne malintentionnée nous a demandé de l'argent en échange de la non-divulgation des données »
Les intrus ont en effet enregistré des adresses de messagerie électronique et postales, ainsi que des mots de passe d'une partie des clients. Une tentative de chantage a suivi : *« Une personne malintentionnée nous a demandé de l'argent en échange de la non-divulgation des données »* nous a précisé l'entreprise hier.

Les dirigeants ont en fait déposé plainte et révélé l'affaire eux-mêmes, informant les clients concernés afin qu'ils prennent leurs précautions.
« Nous vous conseillons de changer le mot de passe de votre messagerie personnelle s'il est identique à celui utilisé pour votre compte Rannou-Métivier, explique l'entreprise*. Si d'autres de vos comptes (Facebook, Ebay, Dropbox…) utilisent à la fois cette même adresse de messagerie et ce même mot de passe, nous vous conseillons d'en changer le mot de passe dans les plus brefs délais. Nous vous présentons toutes nos excuses pour la gêne occasionnée. »*

Pas de données bancaires piratées
Rannou-Métivier assure qu'aucune donnée bancaire n'est tombée entre les mauvaises mains : *« Elles n'ont jamais été stockées sur nos serveurs, elles sont utilisées uniquement le temps du paiement sur le site de la banque. Il n'y a aucun risque de perte d'argent pour nos clients. ».* La faille du site exploitée par le pirate a été identifiée mardi et la sécurité renforcée, tandis que le cryptage des données est en cours.

Rannou-Métivier emploie une soixantaine de personnes, la moitié dans ses laboratoires de production récemment agrandis à Montmorillon, le reste de l'effectif se partageant entre les boutiques de Montmorillon, Poitiers, Châtellerault et Tours.

Réagissez à cet article

Source : *Rannou-Métivier victime de piratage et de chantage – 31/12/2015 – La Nouvelle République Vienne*

Vos données personnelles en otage, puis chantage

Vos données personnelles en otage, puis chantage

Chantage aux données personnelles et « rançongiciels » : de nouvelles formes de cybercriminalité

Quel mode opératoire ?

Le mode opératoire est toujours sensiblement le même :
Un individu parvient à s'introduire dans le système informatique d'une entreprise ou d'un particulier. en extrayant les données y étant stockées.
Dans un second temps, l'internaute ou l'entreprise victime se voit réclamer le versement d'une rançon.
A défaut de paiement, ces informations personnelles seront diffusées sur la toile.
L'exemple le plus significatif en la matière est le cas du site de rencontres extraconjugales canadien ASHLEY-MADISON.COM, victime d'une cyberattaque le 15 juillet 2015.
Un groupe de « hackers » se faisant appel « The Impact Team » a réussi à pénétrer sur les serveurs du site et à en récupérer les données relatives à ses 37 millions d'abonnés de par le monde.
La fermeture du site a alors été exigée, son éditeur se voyant menacé d'une publication en ligne de l'intégralité de ses données. Précisons que cette menace a été mise à exécution au cours du mois d'août 2015.
Une fois ces informations rendues publiques, certains (anciens) clients du site se sont vus demander la remise de fonds, à défaut de quoi leurs informations personnelles seraient adressées directement à leurs proches ou à leurs relations professionnelles.
Autant dire que l'image de l'entreprise victime est ternie, la sécurité de son système informatique étant clairement remise en cause.
Les abonnés voient également des informations (très) personnelles dévoilées publiquement, telles que leur lieu de résidence, leurs coordonnées bancaires, leurs loisirs et habitudes de consommation, leurs fantasmes et désirs sexuels.

Dans une moindre mesure, les particuliers peuvent être individuellement les cibles de phénomènes de ce type.

Pour ces derniers, il prendra la forme d'un programme informatique malveillant appelé « rançongiciel », dérivé de l'anglicisme «ransomware » et, précisons-le, contraction des termes « rançon » et « logiciel ».
Ce programme chiffre ou crypte les données de l'internaute, présentes sur le disque dur de son ordinateur.
Si il souhaite les récupérer ou éviter leur divulgation, il devra là encore payer la rançon exigée.
Une variante consiste à arborer le logo d'une unité de police de type INTERPOL, en accusant l'internaute de détenir illicitement des œuvres protégées par le droit d'auteur ou bien des vidéos ou photographies pédopornographiques.

Quelles Infractions pénales ?

Le chantage et l'extorsion

« Le chantage est le fait d'obtenir, en menaçant de révéler ou d'imputer des faits de nature à porter atteinte à l'honneur ou à la considération, soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque. » (article 312-10 du Code pénal)
Ce délit est puni de 5 ans d'emprisonnement et de 75.000,00 Euros d'amende.
« Lorsque l'auteur du chantage a mis sa menace à exécution, la peine est portée à sept ans d'emprisonnement et à 100.000 euros d'amende. » (article 312-11 du Code pénal)
La menace sera mise à exécution, à partir du moment où les données sensibles seront publiées en ligne ou communiquées à des tierces personnes.
« L'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque. »
« L'extorsion est punie de sept ans d'emprisonnement et de 100 000 euros d'amende. » (article 312-1 du Code pénal)
En la matière, la contrainte ne reposera pas sur la force physique, mais sera purement morale ou psychologique.

L'intrusion dans un système informatique

L'accès et le maintien frauduleux dans un système

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende.
Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende. » (article 323-1 du Code pénal)

L'entrave au fonctionnement d'un système

« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende. » (article 323-2 du Code pénal)
Le chiffrement ou le cryptage de données entrave nécessairement le bon fonctionnement d'un sytème informatique.

La suppression ou la modification frauduleuse de données

« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende. » (article 323-3 du Code pénal)

Les atteintes à la vie privée

« Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :
1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;
2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.» (article 226-1 du Code pénal)
« Est puni des mêmes peines le fait de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes prévus par l' article 226-1.» (article 226-2 du Code pénal)
L'atteinte à l'intimité de la vie privée sera ainsi caractérisée, lorsque l'objet du chantage consistera en des photographies ou des vidéos représentant des personnes dans un lieu privé.

La violation du secret des correspondances (électroniques)

« Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende.
Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions. » (article 226-15 du Code pénal)
Le délit de violation du secret des correspondances est pleinement constitué, dès lors que la menace porte sur la teneur de courriers électroniques, d'emails ou de messages privés échangés entre abonnés ou utilisateurs d'un site.

Les infractions à la législation sur les données personnelles

Le traitement illicite de données personnelles
« Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. »(article 226-16 du Code pénal)
La collecte frauduleuse de données personnelles
« Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 € d'amende. » (article 226–18 du Code pénal)
Le défaut de sécurité des données
La particularité de cette dernière infraction est qu'elle vise, non pas l'auteur de l'attaque, mais bel et bien sa victime directe, le responsable du traitement des données.

En effet, les personnes, entreprises, organismes et collectivités, en charge du traitement des données de leurs utilisateurs ou de leurs usagers, sont tenus de mettre en œuvre toutes les mesures nécessaires, afin d'assurer la sécurité et la confidentialité desdites données.
A défaut, ils engageront leur responsabilité civile et pénale sur le fondement des articles 34 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et 226–15 du Code pénal:
« Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. » (article 34 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)
« Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 € d'amende. » (article 226-15 du Code pénal)

Au cas par cas, d'autres infractions peuvent également être constituées, telles que les délits d'escroquerie, d'usurpation d'identité (numérique), voire même d'usurpation de fonctions, dans la situation où le cyber-délinquant se fait passer pour une unité de police, afin de se faire remettre des fonds.

Quelles solutions ?

La plainte pénale

Que l'on soit une entreprise, une collectivité ou un particulier victime de ce type d'agissements, le premier réflexe est de déposer plainte auprès des services de police ou de gendarmerie ou bien directement auprès du Procureur de la République.
Ce dernier se réservera le droit d'engager des poursuites ou bien de procéder à un classement sans suite de la plainte, faute notamment de disposer d'éléments suffisants afin d'identifier et de localiser précisément le ou les auteur(s) des faits.
En cas de classement sans suite, la victime disposera alors de la faculté de se constituer partie civile auprès du doyen des juges d'instruction, ce qui déclenchera automatiquement des poursuites pénales.

Le retrait de contenus illicites

Si les informations personnelles sont publiées sur un site internet en particulier, leur retrait peut être demandé directement auprès de son éditeur.
A défaut de réponse de sa part ou si il n'existe aucun moyen de le contacter, la suppression des contenus illégaux devra être alors demandée à l'hébergeur du site, en application de l'article 6-I-5 de la loi n°2004-575 pour la confiance dans l'économie numérique.

Le déréférencement et la désindexation des moteurs de recherche

Lorsque le nom et le prénom d'une personne sont tapés sur un moteur de recherche, la liste des résultats de recherche peut faire apparaître des liens renvoyant vers les informations frauduleusement obtenues et divulguées.
Dans ce cas, il est envisageable de demander la désindexation de ces liens directement auprès du moteur de recherche et, le cas échéant, par voie judiciaire.

Réagissez à cet article

Source : *Chantage aux données personnelles et « rançongiciels » : de nouvelles formes de cybercriminalité – Maître thibault prin*
Thibault PRIN AVOCAT
Avocat inscrit au Barreau de PARIS

---

50 attaques informatiques qui ont marqué le web Français en 2015

50 attaques informatiques qui ont marqué le web Français en 2015

Pendant qu'il est possible de lire un peu partout sur le web le « top 5 », le « top 7 » des attaques informatiques dans le monde, ZATAZ préfère regarder du côté de VOS ordinateurs avec le top 50 des attaques informatiques qui ont touché la France et les internautes francophones. Des cas traités par ZATAZ.

Madison, Hacking Team, Hôtels Trump, Madisson, Vtech… les cas de piratage et de fuites de par le monde ont été pléthoriques, encore une fois, cette année. Revenir sur ces cas, pourquoi pas, mais il suffit d'en parler aux internautes francophones croisés sur la toile pour se rendre compte qu'ils ne se sentent pas concernés, et considères ces actes comme « drôles », ou « insignifiants » pour leur vie 2.0. Bilan, sur 1 475 personnes interrogées par ZATAZ (Âgés de 18 à 55 ans – entre le 22 décembre et le 30 décembre – 71% d'hommes – 43% évoluant dans le monde de l'informatique) seules 96 personnes interrogées avaient pris soins de modifier leurs mots de passe, car utilisés plusieurs fois dans des comptes différents (webmails, forums, …). 27 des interviewés confirmaient qu'ils regardaient plus souvent leur compte en banque. 339 avaient décidé, cette année, de faire un backup mensuel de leurs données (Je vous conseille fortement de pratiquer une sauvegarde, chaque jour, ndr).

Opération Anti Charlie

Janvier 2015, les attentats contre la rédaction de Charlie Hebdo et une supérette parisienne met en émoi le monde et le web. Les Anonymous décident de s'attaquer aux sites de djihadistes. Les participants s'attaquent à tout et n'importe quoi, dont des commerces de produits Hallal. En réponse, de jeunes internautes musulmans et plus d'une centaine de pirates du Maghreb et d'Asie lancent l'Opération Anti Charlie. Plus de 20 000 sites en .fr sont modifiés et/ou infiltrés. A noter que certains sites piratés, mais aussi infiltrés sans que la moindre trace du piratage n'apparaisse publiquement, ne sont toujours corrigés 11 mois plus tard. Une attaque informatique qui, sous l'excuse d'une cyber manifestation, était surtout menée et manipulée par des commerçants officiant dans le blackmarket. Dans la liste des espaces touchés : plusieurs centaines de sites du CNRS et des Restaurants du cœur, ainsi que 167 établissements scolaires d'Aquitaine ou encore de vieux espaces du Ministère de l'Intérieur et de la Défense.

TV5 Monde

Avril, le piratage de TV5 Monde fait grand bruit dans un contexte politique tendu. Au début du mois d'avril, la chaîne fait face à une cyberattaque d'ampleur. Ses différents comptes de réseaux sociaux sont piratés et diffusent de la propagande de la secte de Daesh. La diffusion des émissions de la chaîne sont coupées de l'antenne par la direction. Trend Micro évoque l'implication possible d'un groupe d'APT d'origine russe, Pawn Storm. Les autorités restent discrètes sur les différents éléments de l'affaire, si bien qu'encore aujourd'hui, on peine à se faire une idée de ce qu'il s'est vraiment passé dans le SI de France TV5 Monde. C'est surtout l'impact médiatique de cette attaque que l'on retiendra. Cinq mois après l'attaque, ZATAZ alertera l'ANSSI et TV5 Monde pour corriger d'autres failles informatiques découvertes sur les serveurs de la chaîne. A noter qu'un internaute est arrêté au mois d'août en Bulgarie. Des documents retrouvés dans son ordinateur son signé CyberCaliphate, le pseudonyme utilisé lors de l'attaque de TV5 Monde.
Un piratage qui fait ressortir que les media Français sont totalement dépassés par les potentialités malveillantes qui planent au-dessus de leurs claviers. Pour preuves, les différentes fuites de données et autres failles remontées par ZATAZ auprès de France Télévision [Fuite de données de téléspectateurs] ; du journal telecablesat.fr et 13 833 comptes clients volés.

Infiltrations

Les banques, les grands groupes Français sont visés, chaque jour, par des tentatives de piratage. Des attaques réussies ou non. Les clients ne sont jamais informés. Pendant ce temps, des millions d'informations appartenant aux Français sont pillés, copiés, revendues sur la toile. Par exemples, avec trois espaces de filiales de la BNP Paribas. Des sites retrouvés dans un espace pirate. Les malveillants s'échangeant les failles donnant accès à des bases de données. ; le pétrolier Total, et sa boutique, attaquée et pillée en janvier 2015. 29.657 clients d'un espace commercial grand public du pétrolier. Les pirates m'avouaient avoir vendu pour 500€ des informations de Français collectés dans cette BDD. Des fuites de données accessibles directement, ou via des tiers commerciaux, comme ce fût le cas pour TF1 et 1,9 millions de clients Français, abonnés à des journaux papiers ; Le site Internet La Boutique Officielle, spécialisé dans la vente de vêtements « Urban », visité par des pirates informatiques. Données des clients volées. L'entreprise ferme son espace numérique plusieurs jours ; de son côté, la CNIL contrôle 13 sites de rencontres français, 8 sont mis en demeure de mieux contrôler les informations de leurs « clients » ; En Mars, une faille informatique permettait à un pirate informatique de mettre la main sur les données d'un espace Orange Business.
Juin 2015, le portail Associations Sportives, qui répertorie plus de 240.000 clubs et associations françaises est infiltré. Le pirate diffuse un extrait de la base de données. Même sanction pour l'enseigne King jouet qui corrigera une fuite de données visant ses clients. Quinze ans de factures disponibles sur le web d'un simple clic de souris ; Un pirate informatique annonçait, en septembre, le vol des données appartenant au laboratoire Santé Beauté. Le groupe Santé Beauté regroupe des marques telles que « Barbara Gould », « Linéance », « Email diamant », « Batiste », « Nair », « Poupina » et « Femfresh ».
En octobre, le piratage de plusieurs espaces de la marque de lingerie ETAM était annoncé. Le jeune pirate diffusait plusieurs captures écrans qui ne laissent rien présager de bon pour la marque de textile.

Ransomwares

La grande mode des logiciels dédiés au chantage 2.0 (blocage de disque dur, chiffrement de données, NDR) aura frappé très fort en cette année 2015. ZATAZ a reçu pas moins de 3.022 mails de personnes et de PME piégés par ce genre d'attaque informatique. J'ai pu référencer plusieurs dizaines de mairies ou entités publiques malmenées par un ransomware, comme GDF Suez.

Arnaques et autres fraudes

Des arnaques au ransomware qui oblige les « pirates » à payer pour récupérer leurs informations prises en otage. Des arnaques qui existent aussi sous d'autres formes, comme la fraude au président. KPMG, Michelin, le Printemps, LVMH, Vinci, Total, Brevini, Areva, le cabinet d'avocats Baker & McKenzie, Finder France, SAM, Abuba, Vallourec, Sonia Ryckiel, Dargaud, Seretram… quelques exemples d'entreprises qui ont versé de l'argent à des professionnels du social engineering. Des pirates qui avaient collecté un grand nombre d'informations sur l'entreprise. Des données qui vont permettre de convaincre les services comptables de verser des millions d'euros aux pirates. Ces derniers se faisant passer pour le patron, un client, un fournisseur. Les premières arrestations ont eu lieu en février 2015. Elles concernaient les pirates ayant jeté leurs dévolus sur le club de football de l'Olympique de Marseille (OM). Deux hommes (50 et 34 ans) seront été arrêtés à Tel-Aviv.
Autre chantage, autre arnaque, celle mise en place par Rex Mundi. Plus de 15 000 identités de patients d'un laboratoire de santé français diffusées par le pirate. Le maître chanteur réclamait 20.000€ contre son silence. Le laboratoire n'a pas payé. Les informations sensibles et privées des patients seront diffusées.
Des pirates informatiques qui se spécialisent, même dans les prénoms à l'image de cet arnaqueur qui ne visait que les « Jacquelines« . Un prénom que l'escroc considère comme étant celui de personnes âgées.
Le chômage et la « crise » économique profitent aux pirates. Comme avec le site Internet Crédit Financement Fiable qui cachait une escroquerie numérique ; ou encore avec plusieurs cas d'arnaques téléphoniques. Le pirate se faisant passer pour la FNAC, Conforama ou encore Darty ; Les hôteliers, les chambres d'hôtes ne sont malheureusement pas oubliés avec une vague massive de fausses réservations de séjours.

Universités et écoles

Piratage, spams massifs, infiltration par des pirates présumés Chinois et maintenant, la diffusion d'une base de données d'élèves. L'informatique de l'université de Lyon 3 était-elle devenue complétement folle en février 2015 ? Quelques mois plus tard, rebelote, avec de nouvelles fuites de données. D'autres grandes écoles seront visées par des fuites, comme l'extranet du groupe éducatif ESG fermé à la suite d'un piratage informatique ; ou encore le cas de milliers de documents privés, et pour certains sensibles, d'étudiants de l'EPITECH. Plus de 47 000 dossiers pour quatre ans de fuite.

Fuite de données d'adresses postales

En Mars 2015, via le site Internet Degrouptest, il était possible de trouver l'adresse postale collée à un numéro de téléphone. Même une ligne téléphonique sur liste rouge pouvait être démasquée ; Neuf mois plus tard, le même type de fuite touchait un site Bouygues Telecom. Ici aussi, il suffisait de rentrer un numéro de téléphone pour accéder aux adresses postales. Liste rouge comprise.
Des fuites de données que connaitra aussi la société Somfy (spécialiste de la domotique). Zataz.com a pu constater que l'un de ses espaces web, il était dédié au personnel de l'entreprise, avait été infiltré par de nombreux pirates informatiques. Des pirates qui s'étaient empressés d'installer des backdoors, des portes cachées, leur permettant de jouer, à loisir, avec le serveur et son contenu.
Fuite de données sous forme de CV aussi, comme ce fût le cas pour un site d'Ametix. Des milliers de CV sauvegardés directement dans un dossier du WordPress d'un site dédié à une opération marketing.

Viagra et baskets dans votre site web

Le Black Seo, l'utilisation malveillante du référencement de liens et pages pirates via un site légitime, aura permis à des escrocs d'installer de fausses pharmacies et autres boutiques de contrefaçons dans des centaines de sites Français. Des Mairies, des boutiques, des sites étatiques ; Sans parler des sites propres sur eux, capable d'attirer dans leurs filets des milliers de Français, comme la fausse boutique officielle Nike RBFIRM.
En juin, le site Internet officiel de la chambre des Huissiers de Justice de Paris est (le site diffuse toujours des liens malveillants, ndr) piraté et exploité par des vendeurs de viagra ; des attaques que zataz révélera aussi en août 2015 à l'encontre du site de la Haute Autorité de la Santé ; ou encore en septembre pour la Fédération nationale des associations d'accueil et de réinsertion sociale, pour le portail dédié à une étude médicale en France et l'Établissement de Préparation et de Réponse aux Urgences Sanitaires (APRUS).

DDoS

Bloquer un site Internet, un serveur, un streamer (joueur en ligne) … la grande mode des petits pirates, en 2015. Des attaques qui ont eu pour mission de bloquer un site, d'empêcher son bon fonctionnement. Cette année, le groupe de presse belge Rossel (Le soir, La Voix du Nord, …), mais aussi NRJ, BFM, l'Académie de Grenoble ou encore l'UMP ont été attaqués de la sorte.
Des attaques faciles à mettre en place pour le premier idiot qui passe. Les boutiques vendant du DDoS poussent comme les champignons à l'automne. A noter que durant ce mois de décembre 2015, de très nombreux amateurs de jeux en ligne, des streamers, se sont retrouvés menacer par un maître chanteur demandant de l'argent pour stopper ses blocages.

Cartes Bancaires

La fraude à la carte bancaire se porte bien ! La police de Toulouse, et plus précisément la SRPJ, a mis la main sur trois cinéphiles pas comme les autres au mois d'avril 2015. Les individus avaient piégé un distributeur de billets installé dans le cinéma Gaumont Wilson ; En Juin, la banque postale déposé plainte après que des distributeurs de billets soient piégés par des skimmeur, du matériel pirate capable d'intercepter les données inscrites sur une carte bancaires ; Des cartes bancaires qui sont devenues causantes, en mode sans fil. Bilan, même le CNRS a tiré la sonnette d'alerte en indiquant que les cartes de paiement sans contact comportent de graves lacunes de sécurité ; du sans fil qui attire, en novembre, les Frotteurs 2.0 dans le bus, le métro et autres lieux publiques ; du matériel pirate que l'on a retrouvé, entre autre, au mois d'août 2015, dans un parking proche de la gare Montparnasse (Paris). Et les arrestations se succèdent, comme à Tours, et de la prison ferme (7 mois) pour l'un de ces pirates.

Objets connectés

En Mai, je vous expliquais que pour moins de 40 euros, des voleurs de voiture s'invitaient dans les véhicules que les propriétaires pensaient avoir fermé. Même le Ministère de l'Intérieur Français s'en inquiètera quelques jours plus tard ; des panneaux d'affichage seront attaqués, modifiés (Lille, Paris…). De la geek security attitude qui démontre aussi et surtout la faiblesse des villes connectées. La partie immergée d'un problème qui pourrait être bien plus dramatique.

Swatting

Le swatting, une mode venue des Etats-Unis. L'idée du pirate, envoyer les forces de l'ordre au domicile d'un joueur en ligne. En juillet, un second cas de swatting touchait la France. Domingo est un jeune Youtuber/Streamer. Un de ces jeunes professionnels du jeu en ligne qui diffuse ses parties, en direct. Il s'est retrouvé nez-à-nez avec la police après ce genre de mauvaise blague ; Le premier cas, en février 2015, BibixHD. L'action de la police, à son domicile, sera diffusé en directe alors qu'il était en train de jouer au jeu DayZ. Un inquiétant jeu qui amuse des adolescents en mal de repères. Certains vendant des possibilités de swatting pour quelques euros comme je le révélais au moins d'août !

Phreaking

Le piratage téléphonique, le phreaking, un acte numérique qui ne connait pas la crise. Mission du pirate, mettre la main sur une ligne téléphonique qu'il pourra commercialiser, surtout les minutes disponibles d'appels. Par exemples, en juillet, 5.288€ de détournement téléphonique pour la Maison de la Jeunesse de Nancy. En novembre, 43 000€ d'appels téléphoniques détournés pour le département des Deux-Sèvres.

Heartbleed

En juillet, la faille Heartbleed refaisait surface dans mes recherches. Une vulnérabilité datant d'avril 2014. Plusieurs centaines d'importants serveurs Français étaient toujours faillibles, 16 mois plus tard.

Scientologie

Des Anonymous se sont attaqués à plusieurs sites Français de la secte de la scientologie. Les manifestants 2.0 ont voulu rappeler l'affaire de Gloria Lopez, une ancienne scientologue retrouvée morte en 2006.

Box

Cette année, nous aurons connu chez ZATAZ cinq cas, dont deux considérés comme sérieux. Numéricâble, et Bouygues. Ce dernier avait son option Playin'TV particulièrement sensible. Plusieurs problèmes qui auraient pu servir à des actions malveillantes.

Réagissez à cet article

Source : *ZATAZ Magazine » Les 50 attaques informatiques qui ont marqué le web Français en 2015*

Les plus gros piratages de 2015 | Techniques de l'ingénieur

Les plus gros piratages de 2015 | Techniques de l'ingénieur

Année après année, c'est la même constat : quels que soient leur taille et leur secteur d'activité, les entreprises ne protègent pas assez efficacement leurs réseaux et les données personnelles ou sensibles qu'elles hébergent. Dans la majorité des cas, les attaques informatiques ont été facilitées par le non-respect de règles essentielles : mises à jour des logiciels, mots de passe faible, données sensibles pas chiffrées…

Janvier : 20 000 sites français piratés
Des mairies, des universités, des conseils généraux, des églises ou des PME… Après l'attentat contre Charlie Hebdo, de nombreux sites ont été victimes de pirates se réclamant du groupe État islamique. Dans la majorité des cas, ce piratage s'est limité à du « défacement » (modification de la page d'accueil notamment en remplaçant du texte par des revendications et/ou des images). Ce nombre élevé peut surprendre. En réalité, très peu de sites appliquent des règles élémentaires de sécurité.

Février, le « casse » du siècle
Selon l'éditeur russe d'antivirus Kaspersky, une centaine d'établissements bancaires d'une trentaine de pays auraient perdu entre 260 à 800 millions d'euros. Cette attaque massive aurait été organisée par des équipes russes et ukrainiennes.

Avril : mauvais vol chez Ryanair
Environ 4,5 millions d'euros ont été dérobés d'un des comptes de la compagnie aérienne à bas coûts Ryanair. Selon la société irlandaise, des pirates informatiques se seraient emparés de la somme par « un transfert

Juillet : des états civils plus privés
Des informations confidentielles sur la vie et l'état civil de près de 7% des américains ont été volées dans les serveurs de l'Office of Personnel Management, une agence du gouvernement fédéral des États-Unis qui gère notamment les demandes d'emploi dans la fonction publique. 22, 5 millions de personnes sont concernées par ce vol de données personnelles. Ce n'est pas la première fois que des administrations américaines sont victimes d'intrusion.

Juillet : des hackers au volant
Ne plus se plus se véhicules seront connectés d'ici quelques années. Les constructeurs devront renforcer la sécurité de leurs modèles sous peine de sortie de route ! Dans le Missouri, deux hackers ont en effet démontré qu'il était possible de prendre le contrôle à distance d'une Jeep Cherokee commercialisée par le groupe Fiat Chrysler. Situés à une quinzaine de kilomètres du véhicule, Charlie Miller et Chris Valasek (deux experts en sécurité, le premier étant connu notamment pour avoir révélé plusieurs failles dans l'iOS d'Apple) ont coupé le moteur pendant que la voiture roulait sur une autoroute. Ils ont également pris le contrôle des freins et du volant.

Août : des rencontres adultères… publiques
37 millions de comptes utilisateurs (dont des Français avec des adresses du ministère de l'Intérieur, de la Culture ou de plusieurs mairies) d'Ashley Madison ont été récupérés par un pirate. La base de données de cet important site de rencontres adultères comprend des informations très sensibles, comme les préférences sexuelles ou le numéro de téléphone. Pire, aux États-Unis, plus de 15 000 adresses email utilisées pour la création du compte provenaient de l'administration américaine ou de l'armée. De quoi lancer des opérations d'usurpation d'identité ou du chantage. Des sanctions disciplinaires et des peines de prison sont annoncées. Les conséquences sont parfois dramatiques. La police canadienne enquête sur deux suicides potentiellement liés au piratage de ce site géré par Avid Life Media, une société canadienne de Toronto.

Novembre : jouets en panne
Le fabricant de jouets VTech a été victime du piratage d'une de ses bases de données. Des clients français, canadiens, ainsi que des ressortissants d'autres pays étaient enregistrés dans ce fichier d'environ 6 millions de données. Un internaute britannique de 21 ans a été arrêté le 17 décembre. Il ne serait pas le seul pirate à avoir pénétré ce serveur…

0
Réagissez à cet article

Source : *Les plus gros piratages de 2015 | Techniques de l'ingénieur*

Et si les fuites de données sur Réseaux sociaux venaient de vos voisins ?

Et si les fuites de données sur Réseaux sociaux venaient de vos voisins ?

Selon une étude de l'université de Penn State aux Etats-Unis, les utilisateurs de réseaux sociaux se soucieraient bien moins de livrer des informations privées sur leur liste d'amis que de divulguer les leurs.

Quel internaute n'a jamais utilisé une application externe à Facebook qui demande d'accéder à sa date de naissance, à ses photographies et même aux informations personnelles de ses amis ? Les développeurs qui créent des applications tierces à lancer à partir des plateformes de réseaux sociaux demandent régulièrement l'accès à des données privées pas toujours nécessaires. En revanche, elles peuvent être revendues et cela constitue une source financière non négligeable pour ces développeurs.
Mais qu'en est-il des internautes ? A combien jugent-ils la valeur de leurs informations personnelles, et considèrent-ils la vie privée de leurs amis aussi précieuse que la leur ?

Révélée le 14 décembre dernier lors de l'International Conference on Information Systems au Texas, une étude montre que les internautes sont plus soucieux de leurs données privées que de celles de leurs amis. En effet, lorsqu'on leur demandait d'évaluer en dollars la valeur de leurs propres informations quand une application tierce en avait besoin pour pouvoir fonctionner, la moyenne était de $2.31, alors que celles de leurs amis étaient évaluées à $1.56.
Les réseaux sociaux fonctionnent le plus souvent sur le modèle de l'interconnexion des données pour créer de la valeur. La vie que l'utilisateur affiche et qu'il veut voir rester privée est donc intrinsèquement liée à la confidentialité des informations des autres. A noter qu'en avril 2015, la société Facebook, régulièrement attaquée pour sa politique d'utilisation des données d'utilisateurs, a annoncé de sérieuses restrictions quant aux informations demandées par des applications tierces.

Réagissez à cet article

Source : *Réseaux sociaux : les données du voisin valent moins | L'Atelier : Accelerating Business*

AVG dévoile ses prévisions d'attaques informatiques et technologiques pour 2016

AVG dévoile ses prévisions d'attaques informatiques et technologiques pour 2016

L'apparition de voitures autonomes n'est pas le seul élément prouvant que les systèmes logiciels « intelligents » vont améliorer notre sécurité. D'autres indicateurs sont également visibles sur Internet.
Chez AVG, il nous a fallu des années pour concevoir nos récents algorithmes de détection des brèches et de réputation des fichiers. Pour notre tout dernier moteur antivirus, nous avons utilisé des techniques sophistiquées d'apprentissage neuronal et de collecte de données dans le cloud, qui ont été conçues pour intercepter les logiciels malveillants plus en amont, et de manière plus systématique.

En 2016, de nouvelles solutions de sécurité fondées sur l'intelligence artificielle vont faire leur apparition.
On peut donc espérer que la bataille engagée contre les mauvais génies d'Internet va connaître un regain d'énergie très attendu, et que les menaces seront encore plus vite contrées et éliminées. Les progrès de l'intelligence artificielle et des systèmes d'apprentissage profond (ou « deep learning ») sont devenus bien plus accessibles. C'est ce que l'on a pu voir récemment, par exemple, lorsque Google a ouvert le code source de l'outil Tensorflow mis au point au sein de la division chargée de l'intelligence artificielle chez Google.

Autorités de certification : une disparition annoncée
La nécessité de sécuriser tout le trafic HTTPS des sites Web via un mode de chiffrement prend de l'ampleur. En 2016, avec l'apparition de nouvelles normes ouvertes et le fait que les propriétaires de sites pourront plus facilement faire des choix, il se pourrait que cette réalité devienne globale. Certaines autorités de certification, qui par comparaison commencent à paraître un peu dépassées, risquent de connaître des moments difficiles.
Ces dernières années, certains cas d'erreurs de gestion des certificats, des incidents de sécurité et des brèches de données les ont mis sur la sellette et ont fragilisé la puissance de ces géants. La confiance dans les certificats SSL a également été ébranlée, notamment par le fait que des organismes d'état pourraient infiltrer, dans certains cas, nos communications Web prétendument sûres.
Traditionnellement, le rôle d'une autorité de certification est de confirmer l'identité du propriétaire légitime d'un site Web avant d'émettre un certificat SSL signé. Cela reste une bonne idée pour les entreprises qui peuvent se le permettre, et certaines protections et indemnités d'assurance sont également prévues. En revanche, pour un blogueur ou un propriétaire de site professionnel lambda, il est à la fois laborieux et inutile de payer une autorité de certification et se soumettre à ce qui peut sembler un processus laborieux de vérification et de confirmation. Dans ce contexte, les alternatives techniques telles que Let's Encrypt (actuellement en phase bêta) devraient prospérer.
En outre, l'identification des faux certificats SSL va se poursuivre dans le cadre du programme de transparence des certificats de Google, grâce à des systèmes de détection intégrés dans les navigateurs Web modernes. Google continue à demander aux autorités de certification d'assumer leurs responsabilités, afin que nous soyons tous mieux protégés.
Enfin, avec l'annonce d'autres solutions telles que le protocole DANE proposé par Internet Society, qui offre la possibilité à n'importe quel propriétaire de site Web de valider son propre certificat SSL et donc de se passer totalement d'une autorité de certification, l'année 2016 va nous réserver des nouveautés intéressantes !

Malvertising et réseaux publicitaires : réagir ou disparaître
La publicité malveillante ou « malvertising » désigne ce qui se produit lorsque des visiteurs innocents sont la cible d'éléments malveillants, causés par des échanges avec des tiers douteux et une sécurité déficiente sur plusieurs réseaux publicitaires en ligne. En 2016, les réseaux publicitaires vont devoir réagir ou disparaître, avant qu'ils ne détruisent l'économie numérique qu'ils ont contribué à bâtir, et ne ruinent les résultats des sites Web dont la survie dépend des recettes publicitaires.
Ce problème a une cause principale : la « surface d'attaque » des scripts de publicité et de suivi toujours plus nombreux et complexes fournis par les réseaux publicitaires et intégrés par les éditeurs (souvent de façon transparente) sur leurs sites Web.
Sur mobile, plus de la moitié de la bande passante est utilisée pour la diffusion d'annonces publicitaires, beaucoup plus que pour le contenu même de la page !
S'il est associé avec des attaques réseau plus classiques, ce nouveau vecteur peut servir à infecter des milliers de victimes qui visitent des sites pourtant légitimes. Il faut aussi savoir que, même si beaucoup de grands réseaux publicitaires réagissent rapidement et arrêtent le flux de trafic lorsqu'un cas de malvertising se produit, quelques minutes suffisent pour toucher des centaines, voire des milliers de victimes. Toute personne ayant récemment installé un système de blocage publicitaire vous certifiera que ses sites Web préférés se chargent incroyablement plus vite, ce qui paradoxalement n'arrange rien.
Il faut malheureusement reconnaître qu'une grande partie des sites Web riches en contenu, pour qui les recettes publicitaires sont essentielles, se chargent lentement. En fait, une étude menée par le New York Times a montré que, pour la version mobile de nombreux sites d'actualité, plus de la moitié de la bande passante utilisée sert à la diffusion d'annonces publicitaires. Cela représente un volume de données (chargement des annonces, scripts et codes de suivi) supérieur au contenu effectivement affiché sur la page que vous lisez !
Toutefois, les systèmes de blocage de la publicité ne sont pas une solution à long terme à ce qui, finalement, est un problème de mise en œuvre. C'est encore plus vrai si vous convenez que la disparition du principe de monétisation actuellement en vigueur sur Internet pourrait avoir des conséquences économiques désastreuses. De plus, une récente déclaration de l'IAB (Interactive Advertising Bureau) confirme que les annonceurs « tiennent beaucoup moins compte de l'expérience utilisateur » dans leur manière d'élaborer des contenus.
Pour empêcher les systèmes de blocage d'annonces de se répandre, l'IAB a imaginé L.E.A.N. (de l'anglais Light, Encrypted, Ad Choice Supported and Non-Invasive), un programme basé sur des principes intervenant dans la prochaine phase des normes techniques publicitaires destinées à la chaîne d'approvisionnement publicitaire numérique globale. Quelle que soit la solution choisie, une chose est certaine : les réseaux publicitaires doivent réagir et régler les problèmes de sécurité, faute de quoi l'année 2016 pourrait bien être celle où la « vague scélérate » du malvertising aura emporté des millions d'entre nous.

Les mots de passe résistent
Les mots de passe sont un concept, pas une technologie, et la grande majorité d'entre nous va continuer à se servir de cet outil pour de nombreuses ressources, dans la vie privée comme dans la vie professionnelle. Alors certes, les mots de passe seront toujours utilisés en 2016, mais ils ne sont pas la panacée universelle, et vous avez donc intérêt à connaître certaines alternatives.
Cette année, Yahoo a annoncé le lancement d'une solution de sécurité qui utilise des périphériques mobiles plutôt qu'un mot de passe pour contrôler les accès, et nous avons même vu Google intégrer des fonctionnalités de verrouillage intelligent Smart Lock capables de déverrouiller votre smartphone en se servant des appareils présents à proximité.
Il existe des alternatives intéressantes aux mots de passe, même si ces derniers ont encore de beaux jours devant eux grâce à leur gratuité.
En matière de contrôle d'accès, la validation en deux étapes est un système efficace qui a tendance à se répandre et reste très utilisé chez de nombreux fournisseurs basés dans le cloud. Lorsqu'elle est proposée, vous avez tout intérêt à l'utiliser, surtout si vous n'êtes pas un spécialiste des mots de passe. Même s'il est interminable, le code de votre smartphone n'est pas inviolable, et le dispositif de lecture d'empreintes n'est peut-être pas si inutile.
Les mots de passe sont gratuits, et toutes les autres solutions ont généralement un coût, que ce soit sur le plan de la technologie ou de la complexité, ce qui explique que les mots de passe aient de beaux jours devant eux. Il est certain qu'en 2016, les problèmes liés aux mots de passe (réutilisation, stockage mal sécurisé, par exemple) ne risquent pas de disparaître. Espérons toutefois que nous saurons maintenir la vigilance des consommateurs et des entreprises !
L'Internet des objets : le principe de sécurité intégrée atteint le point d'ébullition Cela peut certes être amusant de posséder une de ces toutes nouvelles bouilloires WiFi, que vous pouvez allumer depuis votre smartphone, sans vous lever de votre fauteuil, mais ces objets normalement inoffensifs peuvent aussi révéler votre clé WiFi. Ceci n'est qu'un exemple de plus du problème existant au niveau de l'intégration de la sécurité.
S'ils ne sont pas protégés, chaque appareil périphérique, chaque téléviseur ou système stéréo intelligent, chaque système d'éclairage ou de sécurité domotique, et même ces nouveaux réfrigérateurs à la mode et ces voitures autonomes, bref tout ce qui est connecté à un réseau peut être la cible d'un hacker.
Les cybercriminels testent le matériel, analysent les ondes et recueillent mots de passe et autres données personnelles, quel que soit l'emplacement où ces informations sont conservées. Dans ce nouveau monde d'objets connectés, le danger augmente à mesure que la technologie vieillit.
Nous sommes nombreux à avoir paramétré nos ordinateurs et nos appareils mobiles de manière à ce qu'ils se mettent à jour automatiquement. En même temps, aucun d'entre nous ne pense à gérer la sécurité de ses appareils domestiques et à installer la dernière version logicielle.
Les objets connectés du quotidien peuvent réveler votre clé Wifi, et être la cible d'un hacker…Nous devons revoir notre façon de considérer ces appareils.
Dans certains cas, il est impossible de les mettre à jour. Nous devons considérer ces appareils et ces gadgets comme des ordinateurs déguisés, et les protéger aussi bien que nous le ferions pour notre PC et notre téléphone. Nous allons continuer à voir de nombreuses choses surprenantes connectées à Internet, et si aucun effort n'est fait pour y intégrer la sécurité, le problème risque d'empirer, car certains fabricants ne prennent pas le temps de mesurer les risques que courent les objets connectés au réseau.
Pour revenir un instant à l'analogie avec la bouilloire, rappelons que, dans une entreprise, si un employé achète une bouilloire intelligente, personne ne va s'en inquiéter et personne ne s'attendra à ce que le département informatique ait son mot à dire sur ce genre d'achat. Nous devons donc revoir entièrement notre façon de considérer ces appareils.

Mettre à jour : un élément vital !
Aujourd'hui plus que jamais, il est absolument essentiel que chaque logiciel, appareil, gadget ou équipement soit mis à jour.
Les constructeurs de voitures autonomes tels que Google annoncent déjà qu'ils assumeront la responsabilité des infractions au code de la route, et éventuellement des accidents ou des blessures corporelles dont leurs véhicules seraient responsables. Maigre consolation, avouons-le, si vous êtes victime d'un accident parce que vous avez oublié d'installer la dernière version du logiciel sur votre voiture … À mesure que les systèmes logiciels intelligents s'installent dans nos vies de multiples manières, ces mêmes logiciels pourraient décider de mettre votre vie en danger, il faut en être conscient.
Il va réellement devenir impératif que vous mettiez systématiquement vos logiciels à jour, en même temps que vos autres appareils. Un jour, cela vous sauvera peut-être la vie…

Réagissez à cet article

Source : *Cyber-Sécurité : AVG dévoile ses prévisions pour 2016 – Global Security Mag Online*

URGENT : Phishing Free Mobile, ne vous faites pas avoir !

URGENT : #Phishing Free Mobile, ne vous faites pas avoir !

Réagissez à cet article

Source : *URGENT : Phishing Free Mobile, ne vous faites pas avoir ! – Le Blog du Hacker*

Apple contre le projet de loi

britannique sur le renseignement !

Apple contre le projet de loi britannique sur le renseignement !

Le monde semble actuellement « en guerre » contre les projets de loi sur le renseignement qui fleurissent un peu partout dans les pays développés. Et nombreux sont ceux qui prennent part à ces actions. Apple, par exemple, a clairement affiché ses objections face au projet de loi britannique.

Le monde semble actuellement « en guerre » contre les projets de loi sur le renseignement qui fleurissent un peu partout dans les pays développés. Et nombreux sont ceux qui prennent part à ces actions. Apple, par exemple, a clairement affiché ses objections face au projet de loi britannique.

Pour la firme de Cupertino, affaiblir les techniques de chiffrement, comme le souhaite le gouvernement britannique, reviendrait à diminuer la sécurité des « données personnelles de millions de citoyens respectueux des lois« . La création d'une porte dérobée présente, elle, un risque majeur : « une clef laissée sous le paillasson ne serait pas là uniquement pour les gentils. Les méchants sauraient la trouver également. » Voici en substance les points qu'Apple a voulu souligner à la commission en charge de ce projet de loi.

Autre point sensible : la modification du fonctionnement de iMessage pour pouvoir être écouté « placerait une entreprise comme Apple, dont la relation avec les clients est en partie construite sur un esprit de confiance quant à la confidentialité des données, dans une position très difficile« .

La commission saura-t-elle prendre en compte ce genre de considérations ? À suivre !

Réagissez à cet article

Source : *Apple contre le projet de loi britannique sur le renseignement !*

L’histoire interdite du piratage informatique (Documentaire)

L’histoire interdite du piratage informatique (Documentaire)

Hacker
C’est au cours des années 80 que ce mot a été utilisé pour catégoriser les personnes impliquées dans le piratage de jeux vidéos, en désamorçant les protections de ces derniers, puis en en revendant des copies.
Aujourd’hui ce mot est souvent utilisé à tort pour désigner les personnes s’introduisant dans les systèmes informatiques.

Réagissez à cet article

Source : *[Documentaire] L’histoire interdite du piratage informatique – TrLoad.net | Download Info | Video | Global Music Video | Top Videos, Artist, Songs, Free Mobile Music Download*