Apple contre le FBI : Un cadeau aux pirates informatiques ?

	Apple contre le FBI : Un cadeau aux pirates informatiques ?

Le Haut-Commissariat aux droits de l'homme de l'ONU a décidé de soutenir officiellement Apple dans l'affaire qui l'oppose au FBI. Le chiffrement doit rester un droit fondamental, même dans les affaires de terrorisme.

C'est excessivement rare, si ce n'est pas une première, que des représentants des Nations Unies s'invitent très directement dans une affaire judiciaire. Pourtant, c'est bien aux côtés de très nombreux industriels et organisations de la société civile (dont Apple dresse la liste) que le Haut-Commissariat aux droits de l'homme de l'ONU a décidé de venir apporter à la firme de Cupertino son soutien très officiel, contre le FBI.

Totalement indépendant des états membres de l'ONU, le Rapporteur Spécial des Nations Unies pour la protection et la promotion de la liberté d'expression et d'expression, David Kaye, a ainsi écrit (.pdf) à la juge californienne Sheri Pym, avec le soutien du Haut-Commissariat chargé de veiller au respect des traités en matière de droits de l'homme. Il demande à la magistrate de ne pas ordonner à Apple de supprimer la protection qui permettrait au FBI de découvrir le code de déblocage de l'iPhone 5C de l'auteur de la tuerie de San Bernardino, pour accéder en clair aux données chiffrées qui y sont stockées.
Pour David Kaye, la législation américaine ne permet pas à un tribunal de prendre une telle décision qui obligerait Apple, non pas à fournir des données qui sont en sa possession, mais à fournir son aide technique pour accéder à des données qui, normalement, ne doivent être accédées par personne d'autre que le propriétaire du téléphone.

LA VIE PRIVÉE GARANTIT LA LIBERTÉ DE PENSER ET DE S'EXPRIMER

Il rappelle que l'article 19 du pacte international relatif aux droits civils et politiques(PIDCP) n'autorise des restrictions à la liberté d'opinion – qui comprend celle de les dissimuler – et d'expression que si elles sont « *expressément fixées par la loi* ». C'est le même raisonnement, appuyé sur la Constitution américaine, qu'a eu le juge de New York qui a donné tort au FBI dans une affaire similaire.
Il peut paraître surprenant que l'auteur du courrier soit l'expert de l'ONU chargé de la liberté d'expression, et non celui en charge de la vie privée, Joe Cannataci, qui ait pris la plume pour soutenir Apple. Mais c'est parce que les droits de l'homme sont liés et interdépendants.

Atteindre à la vie privée des individus pour aller sonder ce qu'ils pensent ou ce qu'ils se disent en privé, c'est inciter les individus à ne plus penser librement, ou à ne plus se parler librement.
LES DÉBATS SUR LE CHIFFREMENT ET L'ANONYMAT SE SONT BIEN TROP SOUVENT CONCENTRÉS UNIQUEMENT SUR LEUR UTILISATION POTENTIELLE POUR DES DESSEINS CRIMINELS

David Kaye, Rapporteur spécial des Nations unies sur la promotion et la protection de la liberté d'opinion et d'expression.

C'est pourquoi David Kayes avait déjà à plusieurs reprises exigé le respect du droit au chiffrement. L'expert, qui a été mandaté en 2014, est aussi un opposant farouche aux backdoors, auxquels peut s'assimiler la méthode demandée à Apple au FBI (non pas fournir la clé, mais faire en sorte que la serrure ne fonctionne plus). « Les gouvernements qui proposent des accès par backdoor n'ont pas démontré que l'utilisation criminelle ou terroriste du chiffrement serve de barrière insurmontable pour les objectifs d'application de la loi », avait-il critiqué dans un rapport contre les backdoors.
« Les débats sur le chiffrement et l'anonymat se sont bien trop souvent concentrés uniquement sur leur utilisation potentielle pour des desseins criminels dans des périodes de terrorisme. Mais des situations urgentes ne dispensent pas les États de leur obligation de s'assurer du respect du droit international des droits de l'homme »,
UN CADEAU FAIT AUX RÉGIMES AUTORITAIRES ET AUX PIRATES INFORMATIQUES

L'initiative de David Kayes en faveur d'Apple est publiquement soutenue par la Haut-Commissaire de l'ONU aux droits de l'Homme, Zeid Ra'ad Al Hussein, qui ***explique*** *que « dans le but de régler un problème de sécurité relatif au chiffrement des données dans un cas bien précis, les autorités risquent d'ouvrir la boîte de Pandore, avec des implications qui pourraient être extrêmement dommageables pour les droits de l'Homme de millions de personnes, y compris pour leur sécurité physique et financière ».*
« Un succès dans l'affaire contre Apple aux États-Unis établirait un précédent qui pourrait rendre impossible pour Apple ou toute autre société informatique internationale majeure de protéger la vie privée de ses clients partout dans le monde. Cela pourrait être un cadeau fait aux régimes autoritaires et aux pirates informatiques ». ***[Lire la suite]***

Réagissez à cet article

Source : *Apple contre le FBI : l'ONU intervient au nom des droits de l'homme – Politique – Numerama*

Mise à disposition d'un accès Internet au public – Quelles précautions

Mise à disposition d'un accès Internet au public – Quelles précautions ?

Source : *Mise en place de points d’accès public à internet – informations et conseils juridiques*

Sans GPS Google sait d’où vient une photo

Sans GPS, Google sait d’où vient une photo

Ce logiciel PlaNet de Google devine le lieu d'une prise de vue, sans recourir aux coordonnées GPS de la photo.

Les équipes de Google spécialisées en intelligence artificielle mettent actuellement au point un logiciel capable d'identifier le lieu où a été prise une photo, sans avoir besoin d'utiliser les données GPS de la prise de vue.

Baptisé « PlaNet », ce projet de Google n'a pas encore atteint des résultats vraiment fiables, mais le logiciel est déjà meilleur que les humains pour reconnaître la géolocalisation d'une photo.

En se fondant sur une base de données de plus de 2 millions d'images géolocalisées de FlickR, les ingénieurs de Google sont désormais capables de deviner à 48% l'endroit où a été prise une photo. Ce niveau de performance permet à PlaNet de battre des humains 3 fois sur 5 en moyenne.

Sur le site GeoGuessR, les internautes sont invités à se confronter à PlaNet. En 20 secondes, les visiteurs doivent essayer de deviner l'endroit où une photo a été prise, ce qui est un véritable défi quand il s'agit d'un paysage désertique.

A ce petit jeu de géolocalisation, le logiciel PlaNet atteint une précision de 1 130 kilomètres, là où les humains n'en sont qu'à 2 320…

Un résultat surprenant pour un logiciel léger, qui pourrait tenir sans problème sur un smartphone, et devenir à terme, un logiciel de reconnaissance d'images que Google pourrait utiliser … [Lire la suite]

Réagissez à cet article

Source : *Sans GPS Google sait d'où vient une photo*

Failles de sécurité dans les antivirus

Failles de sécurité dans les antivirus

Des experts révèlent que les antivirus présentent des failles de sécurité exploitables par les pirates.

Imaginez votre antivirus ou votre pare-feu reconverti en cheval de Troie permettant à un pirate de pénétrer au sein de votre ordinateur pour mieux l'attaquer.
C'est exactement ce que viennent de découvrir des experts en sécurité informatique qui ont mis la main sur plusieurs failles de sécurité au sein de logiciels de sécurité. Tomer Bitton, vice-président recherche au sein de la société de sécurité EnSilo, a analysé avec son collègue Udi Yavo une douzaine d'antivirus et de pare-feux.
Résultat : les solutions censées protéger nos ordinateurs peuvent en fait représenter la porte d'entrée des attaques.
« Au total, nous avons découvert six failles différentes, dont quatre très critiques, permettant d'exécuter du code arbitraire. De plus, le pirate n'a même pas besoin d'un accès administrateur, les privilèges de l'utilisateur sont suffisants » rapporte Tomer Bitton.
Ces failles de sécurité peuvent être utilisées assez facilement par les pirates sans trop de difficultés sur tous les systèmes Windows. Une des techniques à laquelle ont recours les pirates est le « hooking », qui consiste à introduire du code arbitraire dans un processus.
Les deux experts ont immédiatement alerté les éditeurs. Bon nombre d'entre eux ont mis en place des correctifs pour colmater les brèches. Néanmoins, certains n'ont pris aucune mesure en dépit de l'avertissement des experts, lesquels ont constaté avec étonnement qu'il n'existait pas d'étroite collaboration entre les éditeurs et les analystes de logiciels malveillants.
Les experts ne se sont pas cantonnés à la simple observation. Ils ont aussi conçu un outil permettant de détecter les failles baptisé « AVulnerabilityChecker »… [Lire la suite]

Réagissez à cet article

Source : *Failles de sécurité dans les antivirus*

Stop aux photos d’enfants sur Facebook ?

	Stop aux photos d’enfants sur Facebook ?

La gendarmerie nationale met en garde les utilisateurs de Facebook contre les chaînes de photos d'enfants.

Plusieurs chaînes de publication de photos d'enfants comme le « Motherhood Challenge » inquiètent les gendarmes français, qui viennent de poster sur leur page officielle Facebook des consignes de prudence. Les autorités rappellent que la publication de photos sur Facebook n'est pas un geste anodin, notamment lorsqu'il s'agit de mineurs.

De nombreux messages circulent actuellement avec un grand succès sur le réseau social, incitant les papas et mamans à poster des photos de leurs enfants, et à encourager leurs amis à en faire autant. Devant l'ampleur du phénomène, la Gendarmerie Nationale renvoie les membres de Facebook aux recommandations de la CNIL concernant les chaînes de publication.

Il est essentiel de régler ses paramètres de confidentialité de manière stricte, pour que les photos et contenus postés ne soient pas diffusés sans limite sur les réseaux sociaux. Il est également indispensable de supprimer à intervalles réguliers les données obsolètes encore en ligne. Les autorités rappellent qu'au-delà des dangers immédiats, la publication de photos de mineurs sur Facebook peut avoir des conséquences à long terme.

Que penseront les enfants en question si ces photos sont utilisées dans 5 ou 10 ans ?

Le droit à l'oubli et la protection de la vie privée des mineurs doivent s'envisager sur la durée.

… [Lire la suite]

Réagissez à cet article

Source : *Stop aux photos d'enfants sur Facebook ?*

L’ADN remplacerait-il bientôt nos disques durs pour stocker nos données ?

L’ADN remplacerait-il bientôt nos disques durs pour stocker nos données ?

De récentes avancées de l'université de Zurich laissent entrevoir un avenir radieux – et une longévité d'un million d'années – pour les données stockées sur l'ADN.

Qu'est-ce que l'ADN ? Un immense support pour stocker l'information. L'information génétique dans les organismes vivants, évidemment. Mais aussi bien d'autres choses. Il suffit d'élaborer un code à partir des quatre bases (les lettres qui constituent le code ADN) pour y stocker n'importe quelle donnée, et notamment les données numériques.
Les chercheurs de l'université Harvard, du laboratoire européen de biologie moléculaire de Heidelberg et de l'école polytechnique fédérale de Zurich testent les possibilités des brins d'ADN depuis plusieurs années, rappelle *Digital Trends.* Et ce sont les Suisses qui viennent d'obtenir la dernière grande avancée, celle qui résout le problème de la conservation des informations sur une longue durée.

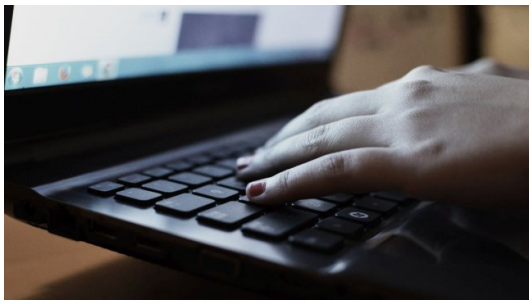
Informations préservées pendant des centaines de milliers d'années
Dans un fragment d'ADN, ils ont encodé la Charte fédérale suisse de 1921 et la méthode des théorèmes mécaniques d'Archimède. Ils ont ensuite inséré ce fragment d'ADN dans une minuscule sphère de verre mesurant 150 nanomètres de diamètre, des fossiles synthétiques en quelque sorte. Ils ont ensuite soumis cette "bille" à des conditions extrêmes pour simuler un vieillissement accéléré. A la fin de l'expérience, ils pouvaient toujours lire les données, explique *ExtremeTech.*
Stockées de cette façon, à basse température (–18 °C), les informations pourraient être préservées pendant des centaines de milliers d'années, estiment les chercheurs.

Le monde dans quatre grammes
Mais pourquoi se donner tout ce mal ? Parce que l'avantage de la molécule d'ADN, c'est son immense capacité de stockage. En théorie, toutes les données numériques existant pourraient "tenir" dans quatre grammes d'ADN, rappelle*Digital Trends.*
Reste à lever deux obstacles principaux. Le coût de cette technologie, toujours très élevé. Et le fait qu'une fois écrite et "vitrifiée", l'information ne peut plus être corrigée.
Mais selon le Dr Nick Goldman, du laboratoire européen de biologie moléculaire (EMBL), le coût pourrait baisser suffisamment pour que la technologie soit accessible d'ici dix ans.
Microsoft, quant à lui, a déjà développé un langage spécifique baptisé DNA Strand Displacement Tool, qui peut être utilisé pour concevoir des séquences génétiques capables de faire fonctionner des circuits électroniques, rappelle la *MIT Technology Review.*
Virginie Lepetit… [Lire la suite]

Réagissez à cet article

Source : *Technologie. L’ADN, plus fort que le disque dur pour stocker des données | Courrier international*

Arnaque à la SexTape – Ne vous découvrez pas d’un clic



Arnaque à la SexTape – Ne vous découvrez pas d’un clic

Mélange de Sexe et d'Extorsion, la Sextorsion, autrement dit l'utilisation du sexe pour faire chanter des internautes, est un phénomène qui prend de l'ampleur sur internet. Le 24 février dernier, un garçon de 13 ans qui habite en Haute-Vienne près de Limoges a ainsi été contacté sur Internet.

Le 24 février dernier, un garçon de 13 ans qui habite en Haute-Vienne près de Limoges a ainsi été contacté sur Internet. Une « prétendue » jeune fille l'a abordé sur les réseaux sociaux et l'a encouragé à se déshabiller devant sa webcam puis lui a demandé 150 € en mandat-cash sous peine de diffuser la vidéo. Une grosse frayeur pour l'adolescent qui a eu le bon réflexe de prévenir ses parents.
D'abord abordé puis dragué, le mode opératoire est bien rodé pour ces cyberdélinquants et peut toucher la plupart d'entres vous.

Adultes ou adolescents, ils sont de plus en plus nombreux à tomber dans le piège

LA TECHNIQUE
1- Repérage
La technique consiste à repérer ses victimes sur des sites renfermant des nids de cibles faciles. Les forums, les réseaux, sociaux, les sites de rencontre, les sites de loisirs et de manière générale tous les sites internet favorisant le dialogue, les rencontres amicales et surtout amoureuses sont les plus couramment utilisés.
Ca ne fait pas peur au prédateur d'aborder dans la même journée plusieurs dizaines de cibles. L'essentiel est d'avoir un minimum quotidien de victimes pour s'assurer un revenu minimum et régulier.
Trouver des victimes sur Internet pourrait bien finit un jour, comme les envois en masse de mailings ou des opérations en masse de phoning, par avoir ses propres statistiques de retour (Un pourcentage assuré de victimes par rapport au nombre de cibles).

2- Le contact
Une fois la cible repérée, il faut la vérouiller.
Si la cible est un homme, l'usurpateur prendra la peau (les photos et les vidéos) d'un modèle de beauté féminin; et si la cible est une femme, c'est à un bel étalon ou quelqu'un excessivement attentionné que le pirate ressemblera. Il n'y a que l'embarra du choix sur Internet. Un simple clic droit sur une photo permet de l'enregistrer sur son ordinateur et ensuite de l'utiliser impunément.
Le dialogue est alors très dirigé, cherchant à faire parler la victime d'elle, la complimentant, lui trouvant un nombre important de points communs (ça fait partie des techniques de manipulation comportementale que ces voyous savent très bien uiliser) cherchant à instaurer un climat de confiance, développer de la complicité et surtout faire baitre, **DES SENTIMENTS** !
Ne vous en faites pas pour le malfrat, quoi qu'il vous dise, il n'a de son coté aucun sentiment, il atend juste que des sentiments commenent à naitre chez sa proie et on peut alors consédérer qu'elle est malheureusement vérouillée.

3- Le piège
Il existe une technique similaire consistant à vous dérober de l'argent et parfois même, des montants faramineux. Mais c'est la tournure d'une arnaque à la SexTape que prendra la relation à distance si vous avez une Webcam.
Rapidement, au bout de quelques heures ou quelques jours, une fois les sentiments vous faisant quitter le monde rationnel mais plutôt voyager dans le monde des émotions, votre interlocuteur, le plus beau ou la plus belle du monde vous invite à vous dévoiler physiquement pour son plus grand bonheur… Une démarche plus ou moins naturelle vous me direz, dans le cadre d'une relation amoureuse qui commence à s'installer…
Cependant, à l'autre bout de la souris, l'interlocuteur malintentionné est prêt à appuyer sur sa gachette pour …. vous enregistrer en train de vous dénuder, en train de jouer.
Une fois cette étape franchie, le piège s'est refermé et votre interlocuteur ou votre fausse interlocutrice détient précieusement des images compromettantes.

4- Le chantage
Une fois le piège refermé sur vous, et cette étape franchie, le cybercriminel s'empresse de mettre fin au jeu sexuel pour le remplacer par un jeu de force, consistant à vous menacer de dévoiler sur Internet d'envoyer à votre famille, à votre employeur ou à d'autres de vos contacts la vidéo ou les photos compromettantes capturées si vous ne payez pas une somme d'argent. C'est du chantage (action d'extorquer de l'argent ou tout autre avantage par la menace, notamment de révélations compromettantes ou diffamatoires).
Les pirates vous demanderont à tous les coups, pour conserver l'anonymat grace à des complices, de régler par mandat cash, westernu union ou par monnaie électronique, naturellement anonyme.

5- Que faire pour s'en protéger ?
L'action la plus citoyenne que vous pourriez faire consisterait à nous aider à faire de la prévention en partageant cet article, en parlant à votre entourrage ou à vos proches de l'existence de ce fléau pour éviter qu'ils se fassent attraper, car une fois le piège refermé sur vous, vu que les communicatins peuvent être surveillées, enregistrées, sauvegardées et partagées dans le cloud, il est souvent trop tard pour supprimer toutes traces de photos ou vidéos compromettantes et ceci, même si vous payez la rançon…
Quelques conseils
• Sois méfiant à l'égard de ceux qui veulent en savoir trop.
• Ne donne aucune information sur toi ou sur ta famille (comme ton nom, ton numéro de téléphone, ton adresse ou celle de ton école…) sans en parler avec tes parents.
• Si tu reçois ou si tu vois quelque chose qui te met mal à l'aise, ne cherche pas à en savoir plus par toi-même, déconnecte toi et parles-en à tes parents.
• Si tu envisages de rencontrer quelqu'un que tu as connu en ligne n'y va jamais sans en parler à tes parents.
• Supprime, sans les ouvrir, les mails que tu n'as pas demandés ou qui te sont envoyés par des personnes en qui tu n'as pas confiance.
• N'achète jamais rien sur Internet, sauf si tes parents sont avec toi pour te conseiller.
• Ne donne jamais un mot de passe.

6- Et si c'est trop tard
Si c'est malheureusement trop tard pour vous et que vous êtes bel et bien victime d'arnaque à la Sex Tape, il faut surmonter sa honte et en parlet à des amis ou des confidents. Si vous êtes mineur, parlez-en immédiatement à vos parents. Il faut relativiser, se dire que ce n'est pas catastrophique. Vous êtes juste victime d'une escroquerie.
Ensuite, il est important que pouvoir récolter le maximum d'éléments techniques qui permettront de remonter jusqu'à l'auteur de cette machinerie. Pseudos, courriers électroniques avec leurs entêtes, récupérer les adresses IP, garder les SMS, etc…. seont un point de départ solide pour une enquête.

Il est également important de porter plainte.
Si vous n'avez pas encore payé, malgré les menaces ou la diffusion de vidéos, ne le faites surtout pas. Payer n'engagera pas la personne à supprimer les informations compromettantes.
Si vous pensez avoir été victime d'une escroquerie sur Internet, mais n'êtes pas sûr, si vous voulez des conseils suite à une tentative d'escroquerie dont vous auriez été victime, vous pouvez contacter la plateforme téléphonique Info Escroqueries, où des policiers et des gendarmes vous répondent au 0811 02 02 17 (coût d'un appel local) », porter plainte en brigade de Gendarmerie ou au Commissariat de Police ou bien signaler l'acte malveillant dont vous êtes victime sur la plateforme PHAROS (Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements) sur www.internet-signalement.gouv.fr.

Ces escroqueries sentimentales sont souvent organisées, par des réseaux structurés, depuis des pays d'Afrique, où la justice peine à se faire entendre même si le cyber harcèlement est puni en France par l'article 222-33-2-2 du code pénal (2014) de 2 ans à 3 d'emprisonnement et de 30 000 à 45 000 € d'amende.

Réagissez à cet article

Auteur : Denis JACOPINI

Sources :

http://lci.tf1.fr/france/faits-divers/escroquerie-a-la-sextape-sur-le-net-comment-reagir-6280167.html

http://france3-regions.francetvinfo.fr/limousin/haute-vienne/cybercriminalite-un-jeune-limousin-victime-de-sextorsion-937350.html

https://www.internet-signalement.gouv.fr

Est-ce légal d'utiliser un

VPN pour contourner le filtrage géographique ?

Est-ce légal d'utiliser un VPN pour contourner le filtrage géographique ?

Vous songez à utiliser un VPN pour accéder aux catalogues de Netflix diffusés dans d'autres pays, mais ne savez pas si c'est légal ? La réponse.

Alors que NordVPN part en guerre contre le blocage de ses serveurs par Netflix, vous vous posez peut-être la question : est-ce légal pour un internaute de passer par les services d'un VPN pour contourner le filtrage géographique et accéder à des œuvres qui, normalement, ne sont pas diffusées en France ou le sont par d'autres services ?
La réponse est loin d'être aussi évidente qu'on pourrait le penser. Elle n'est en tout cas, comme souvent en droit, pas binaire. Il est impossible de répondre « oui » ou « non ». Mais tentons une réponse argumentée.
Il fait peu de doute que les blocages géographiques imposés par les ayants droit peuvent être considérés comme des mesures techniques de protection, qui sont celles destinées à « empêcher ou à limiter les utilisations non autorisées par les titulaires d'un droit d'auteur ». Quand un studio accorde des droits à Netflix US, il le fait pour autoriser l'accès depuis les États-Unis, pas depuis les autres pays, et le blocage géographique vise à s'en assurer.
Or l'article L335-3-1 du code de la propriété intellectuelle punit bien de 3 750 euros d'amende « le fait de porter atteinte sciemment, à des fins autres que la recherche, à une mesure technique efficace (…) afin d'altérer la protection d'une oeuvre par un décodage, un décryptage ou toute autre intervention personnelle destinée à contourner, neutraliser ou supprimer un mécanisme de protection ou de contrôle ».
Fin de l'histoire ? Non. Car il y a deux obstacles.

LE FILTRAGE GÉOGRAPHIQUE, UNE MESURE TECHNIQUE DE PROTECTION « EFFICACE » ?

Le contournement du filtrage géographique par contrôle d'adresse IP n'est interdit que s'il s'agit d'une mesure technique « efficace », ce qu'il ne faut pas prendre au sens commun. Il suffit pas de pouvoir contourner pour dire que ça n'est pas efficace.
La loi précise que les « mesures techniques sont réputées efficaces lorsqu'une utilisation […] est contrôlée par les titulaires de droits grâce à l'application d'un code d'accès, d'un procédé de protection tel que le cryptage, le brouillage ou toute autre transformation de l'objet de la protection ou d'un mécanisme de contrôle de la copie qui atteint cet objectif de protection ».
Il paraît clair que le contrôle de l'adresse IP n'est pas un contrôle de code d'accès, ni un procédé de transformation de l'œuvre tel que le brouillage ou le cryptage. Mais s'agit-il d'un « mécanisme de contrôle de la copie » ? Il y aurait débat, puisque techniquement, l'utilisateur de Netflix ne réalise pas de copie. Mais admettons.

L'UTILISATEUR D'UN VPN EST-IL RESPONSABLE ?

Un deuxième problème se pose. L'amende de 3 750 euros prévue par l'article L335-3-1 ne peut s'appliquer que si le contournement est réalisé par « d'autres moyens que l'utilisation d'une application technologique, d'un dispositif ou d'un composant » qui existe déjà, fourni par un tiers.
Dans ce dernier cas, c'est le fait de « procurer ou proposer sciemment à autrui, directement ou indirectement, des moyens conçus ou spécialement adaptés pour porter atteinte à une mesure technique efficace » qui devient punissable, de six mois de prison et 30 000 euros d'amende. L'idée est que c'est d'abord celui qui fournit l'outil en toute connaissance de cause qui doit être tenu responsable pénalement, et pas celui qui s'en sert.

Dès lors, il faut distinguer deux cas, assez paradoxaux :
Si l'internaute utilise un service de VPN qui est clairement promu comme un outil de contournement du filtrage (typiquement NordVPN), il n'est pas responsable ;
Si l'internaute utilise un service de VPN totalement neutre, qui ne fait que fournir une adresse IP géolocalisée dans d'autres pays, sans dire à quoi ça peut servir, c'est lui qui le transforme en outil de contournement de la mesure technique de protection, et il devient donc responsable.
Dans tous les cas, l'internaute est potentiellement coupable de recel de contrefaçon, mais c'est une réflexion qui nous amènerait trop loin. Et songez surtout qu'en pratique, il reste extrêmement peu probable qu'existe un jour une plainte pour utilisation d'un VPN, qui demanderait d'obtenir l'adresse IP des internautes en cause. Mais si vous vous posiez la question, vous avez une réponse.

Source : Guillaume CHAMPEAU

Réagissez à cet article

Source : *Est-ce légal d'utiliser un VPN pour contourner le filtrage géographique ? – Politique – Numerama*

Gare aux « tarifs délirants » des numéros en 118

Gare aux « tarifs délirants » des numéros en 118

Les numéros de renseignements téléphoniques comme le « 118 218 » existent encore, et ils sévissent auprès d'usagers fragiles, mal informés ou pressés… qui en paient le prix fort.

Des numéros de renseignements téléphoniques, la plupart d'entre vous n'en connaissent que le duo moustachu qui amusait la galerie dans les spots TV voilà quelques années. À force de le répéter sur un air de générique des années 80, le numéro « 118 218 » s'est peut-être inscrit durablement chez certains. Ce que l'on sait moins, c'est que cette société – leader du marché – ainsi que ses pairs, génèrent une « vague de plaintes » des utilisateurs.

L'association 60 Millions de consommateurs dit avoir reçu un certain nombre de réclamations de personnes ayant vu leur facture téléphonique exploser suite à un appel en « 118 ». Après la libéralisation complète du « 12 » en 2007, ces services se sont mis à pulluler. Depuis, la plupart a disparu et le nombre d'appels a fondu, mais une dizaine survit. Le 118 218, de la société Le Numéro (filiale de l'américain KGB), a même lancé son application.

Une arnaque en 3 leçons

« Pour à peine 2 minutes et 40 secondes au bout du fil, un de nos lecteurs s'étonne d'avoir payé 10,80 euros au 118 218 », rapporte l'association. Elle voit trois explications. La première : « Face à la baisse des appels, les services de renseignements téléphoniques ont augmenté leurs tarifs jusqu'à des sommets inédits. La plupart facturent désormais 5 à 6 euros la première minute d'appel, puis 2,50 à 3 euros les minutes suivantes. »

En effet, les services de renseignements téléphoniques « sont les seuls numéros surtaxés pour lesquels la réglementation ne fixe aucun plafond tarifaire », rappelle 60 Millions de consommateurs, alors que les autres numéros à tarification majorée (08) ont plafonnés à 0,80 euro la minute depuis la réforme d'octobre 2015.

Réagissez à cet article

Source : *Gare aux « tarifs délirants » des numéros en 118*

Alerte vigilance – Ransomware Lockyx

Alerte vigilance – #Ransomware Lockyx

Bonjour, Une vague d'attaques du ransomware Locky touche actuellement de nombreuses entreprises dans le monde et depuis peu en France.Voici nos conseils pour se protéger contre cette nouvelle menace :

CONSEIL N°1 : VIGILANCE UTILISATEUR

Informez vos collaborateurs de l'importance de ne pas ouvrir la pièce jointe d'un email envoyé par un expéditeur inconnu. Soyez très vigilant notamment avec les pièces jointes .zip, .doc, .xls : sources de propagation de Locky.

Les sensibiliser à l'utilisation des macros et/ou les désactiver, source de propagation de Locky.

CONSEIL N°2 : SOLUTION DE PRA

Assurez-vous que vos machines sont correctement sauvegardées, et les images externalisées pour une restauration rapide en cas d'attaque.

Les équipes ESET sont mobilisées à l'heure actuelle pour vous apporter une solution rapide et continue contre ce ransomware et ses multiples variantes quotidiennes.

Note : si vos machines sont déjà infectées, isolez-les des autres, initiez leur restauration et lancez une analyse complète de vos systèmes.

Cordialement,

L'équipe ESET

… [Lire la suite]

Réagissez à cet article

Source : *Alerte vigilance – Ransomware Lockyx*