

Vers l'adhésion de la Tunisie à la convention de Budapest sur la cybercriminalité | Le Net Expert Informatique



Vers l'adhésion de la Tunisie à la convention de Budapest sur la cybercriminalité

Le chef du gouvernement Habib Essid a présidé ce mercredi 23 septembre 2015, la deuxième réunion du Conseil stratégique de l'économie numérique, à la Kasbah.

Une batterie de mesures ont été décidées à cette occasion, dont :

- L'élargissement de la composition du conseil en y intégrant les ministres de la Défense et de la Santé. Faire participer les composantes de la société civile qui sont actives dans le domaine du numérique.
- L'approbation de l'objectif stratégique : « Un accès haut débit pour toutes les familles tunisiennes ».
- L'intensification des concertations entre les secteurs public et privé dans le but d'œuvrer à la « numérisation totale des écoles ».
- La mise en place d'une base de données topographique au service de la géo-localisation et signature, à cet effet, d'un contrat de partenariat public-privé sur une période de six mois.
- L'appui des efforts pour que la Tunisie abrite le sommet africain sur l'open enseignement « African MOOCs Summit ».
- La formation d'une équipe conjointe entre le public et le privé pour développer le cadre juridique et procédural des appels d'offre publique dans le domaine du numérique.
- L'approbation d'une série de mesures à caractère technique et structurel ayant relation avec l'e-administration tel que l'identifiant unique.
 - Le lancement du projet de numérisation du patrimoine culturel.
- Le dépôt de la candidature de la Tunisie pour adhérer à la convention de Budapest sur la cybercriminalité.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

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

Source :

<http://www.jawharafm.net/fr/article/vers-l-adhesion-de-la-tunisie-a-la-convention-de-budapest-sur-la-cybercriminalite/90/27865>

Par Zeyneb Dridi

Un nouveau virus découvert sur des distributeurs de billets | Le Net Expert Informatique

✖	Un nouveau virus découvert sur des distributeurs de billets
Un nouveau malware a été en mesure d'attaquer des distributeurs automatiques de billets. Baptisé GreenDispenser, il entre dans la longue liste des outils informatiques permettant de vider le contenu d'une machine.	
<p>Après Suceful, Plotus ou encore Padpin, des experts en sécurité annoncent avoir découvert un nouveau malware informatique capable de s'attaquer aux distributeurs de billets. GreenDispenser agit comme un virus classique et permet de faire sauter les barrières de sécurité mises en place sur ce type d'appareil. Le procédé d'attaque est classique. Les pirates doivent être en mesure d'accéder physiquement au distributeur. Le système peut alors être infecté par le biais du virus en se focalisant sur un middleware utilisé sur de nombreuses machines de ce type (utilisant la norme XFS). Ce logiciel, censé faire le lien entre la partie les périphériques (le clavier par exemple) fait fonctionner le distributeur ainsi que le reste de l'équipement va être le point faible.</p> <p>Toujours est-il que le malware est capable d'agir sur le processus d'authentification à double facteurs des appareils. GreenDispenser permet également de mettre hors service un distributeur et dispose même d'un mécanisme d'autodestruction, le rendant particulièrement difficile à détecter par les éditeurs en sécurité ou d'éventuels enquêteurs.</p> <p>A l'heure actuelle, GreenDispenser a principalement sévi au Mexique. Selon l'éditeur de sécurité Proofpoint, le malware pourrait toutefois facilement s'étendre à d'autres régions géographiques en dehors de l'Amérique latine. La société conseille aux professionnels détenant des distributeurs de vérifier la sécurité de leur dispositif et d'appliquer d'éventuelles mises à jour.</p>	
<p>Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours. Nos domaines de compétence :</p> <ul style="list-style-type: none">• Expertises et avis techniques en concurrence déloyale, litige commercial, piratages, arnaques Internet.. ;• Consultant en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;• Formateur et chargé de cours en sécurité informatique, cybercriminalité et déclarations à la CNIL. <p>Contactez-nous</p>	
<p>Cet article vous plait ? Partagez ! Un avis ? Laissez-nous un commentaire !</p>	
<p>Source : http://pro.clubic.com/it-business/securite-et-donnees/actualite-780740-virus-decouvert-distributeurs-billets.html?estat_svc=s%3D223023201608%26crmID%3D639453874_1167429992#pid=22889469</p>	

L'essor du chiffrement inquiète le renseignement anglais | Le Net Expert Informatique

Informatique



L'essor du chiffrement inquiète le renseignement anglais

Dans une interview à la BBC, le patron du renseignement intérieur britannique (MI5) a exprimé ses inquiétudes à l'égard de l'évolution des technologies de chiffrement. Selon lui, les entreprises technos ont le devoir éthique d'informer les autorités de menaces potentielles.

Le gouvernement britannique n'en démord pas et veut ses backdoors : dans une interview donnée à la BBC, le dirigeant du MI5, les services de sécurité de la Grande-Bretagne, évoque à nouveau le débat autour des technologies de chiffrement qui se développent à destination du grand public.

Pour Andrew Parker, directeur du MI5, les services de police ont de plus en plus de mal à obtenir des informations en ligne et les entreprises du secteur technologique devraient selon lui informer les agences de renseignement des potentielles menaces détectées via leurs outils. Il explique au micro de la BBC que les services de police sont confrontés à la difficulté croissante d'obtenir « les relevés de communications des utilisateurs suspectés d'activités terroristes, et ce même en disposant d'un mandat de justice. »

Haro sur le chiffrement

Une critique déjà entendue fréquemment et qui fait écho au développement d'outils de chiffrement de bout-en-bout, mouvement qui gagne en intensité dans l'industrie des nouvelles technologies et des services en ligne suite aux révélations d'Edward Snowden.

Et la problématique n'est cantonnée Outre-Manche, où David Cameron a annoncé son intention de légiférer sur le sujet. Aux États Unis, on a ainsi pu voir les dirigeants du FBI exprimer une demande similaire, évoquant la possibilité de mettre en place des backdoors connues des seuls services de renseignement afin de pouvoir accéder aux données échangées sur les plateformes de messagerie en ligne. En France, c'est le procureur de la République de Paris qui s'y colle : celui-ci avait signé en août une tribune dans le New York Times déplorant l'essor du chiffrement et l'obstacle que celui-ci constituait dans les enquêtes judiciaires.

Face à cette offensive, les défenseurs de la cryptographie s'inquiètent tout particulièrement des conséquences que pourrait apporter la mise en œuvre d'une telle volonté politique : pour Bruce Schneier, expert américain de la cryptographie, s'appuyer sur ce type de procédé viendrait immanquablement contredire le principe même de la cryptographie, supposé garantir la sécurité des échanges entre les destinataires. De plus, et l'affaire récente des clefs d'accès aux cadenas TSA le rappelle bien : les backdoors ne sauraient garantir que la personne qui les utilise est bien un représentant des forces de l'ordre, laissant la possibilité à des cybercriminels ou à des pays étrangers de les exploiter.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

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

Source :

<http://www.zdnet.fr/actualites/le-renseignement-anglais-s-inquiete-lui-aussi-de-l-essor-du-chiffrement-39825120.htm>

Cybercriminalité : Les gendarmes en pleine enquête | Le Net Expert Informatique



Le capitaine Abdoulaye Mbodj Ndiaye et ses hommes mènent de nombreuses enquêtes concernant des arnaques par Internet.

Cybercriminalité :
Les gendarmes en
pleine enquête

La Section de recherches de Dakar nous a ouvert ses portes. Coup de chance, elle investiguait justement sur une arnaque par Internet. La victime, une religieuse, y a laissé un joli montant.

«Pour être plus efficaces, il nous manque encore du matériel»

«Ici, c'est le laboratoire des N-Tech», explique Sekou Diatta en nous faisant entrer dans la pièce. Les fameux «N-Tech», ce sont les enquêteurs en cybercriminalité de la gendarmerie sénégalaise.

Le long du mur, une immense étagère remplie de matériel pour perquisitions et scènes de crime. Comme dans les films: sachets plastiques, rubans de signalisation et gants en latex. Mais les enquêtes menées par Sekou Diatta et ses cinq collègues sont plutôt numériques.

«Nous sommes chargés de récolter toutes les informations relatives au délit. Par exemple sur des disques durs ou des clés USB», détaille le spécialiste. Et il espère que son équipe s'agrandira rapidement. «A six, cela fait un peu juste pour couvrir tout le territoire», reconnaît-il.

Ce qui n'empêche pas les enquêteurs de traiter déjà les nombreux cas de cybercriminalité qui touchent le Sénégal actuellement, selon lui. «Mais c'est vrai que pour être plus efficaces, il nous manque encore du matériel.»

Le capitaine Abdoulaye Mbodj Ndiaye est un homme pressé. C'est dans sa voiture de service, en route pour la caserne de gendarmerie, que le numéro 2 de la Section de recherches nous accorde quelques minutes. «Il y a de plus en plus de plaintes liées à des escroqueries sur Internet. Ce sont des affaires très courantes ces derniers temps au Sénégal», explique-t-il tout en conduisant. L'après-midi est déjà bien avancée et il lui reste encore beaucoup de travail. Le matin même, ses hommes sont intervenus dans un bureau de transfert d'argent pour arrêter un arnaqueur.

Mais pas le temps de se féliciter, l'affaire qui le préoccupe actuellement est une fraude à plus de 260 millions de francs CFA (environ 400 000 francs suisses). Sur ce dossier, Abdoulaye Mbodj Ndiaye n'en dira pas plus. En revanche, il accepte de nous laisser assister à l'enquête sur l'escroquerie par Internet dont une religieuse sénégalaise a été victime.

Marie* vient justement de déposer une plainte. «En juillet, j'ai reçu un courriel d'une Canadienne qui voulait correspondre avec quelqu'un au bout du monde», raconte-t-elle. Une proposition que la religieuse accepte avec plaisir. La dénommée Cassandra lui envoie alors plusieurs photos et lui donne de nombreux détails sur sa famille. Quelques échanges de courriels plus tard, la fausse

Canadienne fait une proposition étonnante à Marie. «Elle m'a dit qu'elle avait envoyé un colis avec des ordinateurs et des appareils photo à sa sœur au Bénin.» Sauf que celle-ci a dû rentrer au pays en urgence. Cassandra demande donc à la religieuse si elle peut récupérer les paquets à sa place.

Marie a des doutes, mais la Canadienne sait comment la convaincre. «Elle m'a pris par les sentiments en me disant qu'il y avait aussi un album de photos de famille. Cela m'a émue», précise la sœur. Elle entame donc les démarches pour récupérer le colis et apprend qu'elle doit payer des taxes. «Tout a été très vite, j'ai versé la somme demandée pour rendre service», explique-t-elle. Le colis n'arrivera bien sûr jamais. Intriguée, la religieuse se renseigne sur Internet et découvre qu'elle a été victime d'une arnaque. «Ils m'ont encore appelée pour me réclamer plus d'argent, donc je me suis décidée à porter plainte», précise-t-elle.

Marie souhaite surtout que son escroc soit mis hors d'état de nuire. «Cela m'a choquée, ils prennent vraiment l'argent de n'importe qui. Que tu sois pauvre ou riche», regrette-t-elle.

Investigations numériques

De son côté, le capitaine Abdoulaye Mbodj Ndiaye et ses hommes ont déjà commencé leur enquête. Ils inspectent l'ordinateur portable que la victime a amené avec elle. «Cela nous permet de recueillir un maximum d'éléments numériques pour mener nos investigations», explique-t-il. Ils commencent par analyser le contenu des échanges, en l'occurrence des e-mails Yahoo. «Là, par exemple, on a un numéro du Bénin alors que l'escroc prétend être au Canada», explique un spécialiste en plein travail. Les gendarmes vont ensuite s'attaquer à l'enquête numérique à proprement parler. Cela va notamment leur permettre de récupérer l'adresse IP du suspect. Quelques secondes plus tard, ils la géolocalisent dans un quartier de Cotonou, la capitale du Bénin.

Le capitaine doit donc procéder à une réquisition de coopération internationale pour obtenir plus d'informations sur ce dossier. Ce qui peut parfois prendre du temps. Mais il assure qu'il ne donne pas la priorité à certains dossiers en fonction de l'origine des victimes ou des suspects. «Ce qui compte pour nous, c'est la gravité des cas. Notamment la valeur du délit et le risque d'atteintes physiques», précise-t-il.

Il reconnaît toutefois que devant le nombre croissant d'affaires d'escroquerie, la cinquantaine de gendarmes qu'il dirige est parfois obligée de déléguer à d'autres unités. «Mais nous ne jetons jamais un cas aux oubliettes, nous faisons toujours de notre mieux.» Surtout que la cybercriminalité n'est pas leur seule préoccupation. «C'est pour cela que l'unité spécialisée qui sera créée en novembre prochain est très importante», conclut-il.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

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

Source : <http://www.lematin.ch/monde/gendarmes-pleine-enquete/story/22226136>
Par Fabien Feissli (textes) et Maxime Schmid (photo)

Liste des applications iPhone et iPad infectées par le logiciel malveillant XcodeGhost | Le Net Expert Informatique

x	Liste des applications iPhone et iPad infectées par le #logiciel malveillant XcodeGhost
---	---

Des experts en sécurité ont récemment découvert sur un certain nombre d'applications dans l'App Store d'Apple un maliciel iOS appelé XcodeGhost. Les créateurs de XcodeGhost ont été en mesure d'intégrer un code malveillant dans ces applications à l'insu de leurs développeurs. Parmi les applications touchées, on retrouve les populaires WeChat et CamCard. Nous pouvons donc estimer que le nombre de victimes potentielles du logiciel malveillant XcodeGhost s'élèverait à de centaines de millions d'utilisateurs.

Voici une liste non exhaustive des applications détectées en tant que malveillantes :

CamCard Business
Action: Update to latest version
Current Status: Patched
Last version checked: 1.8.2

CamScanner Free| PDF Document Scanner and OCR
Action: Update to latest version
Current Status: Patched
Last version checked: 3.8.2

CamScanner +| PDF Document Scanner and OCR
Action: Update to latest version
Current Status: Patched
Last version checked: 3.8.2

Cam Scanner Pro
Action: Update to latest version
Current Status: Patched
Last version checked: 3.8.2

WeChat
Action: Update to latest version
Current Status: Patched
Last version checked: 6.2.6

WinZip - The leading zip unzip and cloud file management tool
Action: Update to the latest version
Current Status: Patched
Last version checked: 4.3

MP3 - MP3 Converter
Action: Update to latest version
Current Status: Patched
Last version checked: 2.9.0

OPlayerHD Lite
Action: Update to latest version
Current status: Patched
Last version checked: 2.1.03

MP3 - MP3 Converter
Action: Update to latest version
Current Status: Patched
Last version checked: 4.2.9

LifeSmart
Action: Uninstall immediately
Current status: Still malicious
Last version checked: 1.0.45

10000+ Wallpapers for iOS 8, iOS 7, iPhone, iPod and iPad
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 3.0

MP3Podcasts - MP3Podcasts
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 4.3.8

MP3 - MP3 Converter
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 1.8.0

MP32 - MP32
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 2.1.1

MP3
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 1.1.5

MP3
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 3.6.5

MP3 - MP3 Converter
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 1.1.0

MP3
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 3.2

MP3
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 2.40.01

Plus d'infos sur : <https://blog.lookout.com/blog/2015/09/21/xcodeghost-apps>

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet...
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

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

Source : <https://blog.lookout.com/fr/2015/09/23/xcodeghost-apps/>

5,6M d'empreintes digitales de fonctionnaires américains dérobées | Le Net Expert Informatique



5,6M
d'empreintes
digitales de
fonctionnaires
américains
dérobées

Alors qu'il était estimé à 1,1 million, le nombre d'empreintes digitales volées à l'occasion du gigantesque piratage du service du personnel des fonctionnaires américains révélé cet été se monte désormais à 5,6 millions. Un coup dur pour cette administration qui poursuit ses investigations.

Le bilan s'alourdit concernant le piratage massif dont a été victime l'Office of Personnel Management (OPM) aux Etats-Unis. Révélé en plein coeur de l'été, ce piratage a débouché sur le vol de données personnelles en tous genres dont essentiellement des numéros de sécurité sociale, mais pas seulement (historiques de consommation de drogue, problèmes juridiques et financiers, dossiers scolaires, historiques de carrières...), appartenant à plus de 20 millions de fonctionnaires américains.

Parmi les données volées se trouvaient également des empreintes digitales. Mais alors que le nombre d'empreintes dérobées était auparavant estimé à 1,1 million, l'OPM a revu ce nombre à la hausse.

« Sur les 21,5 millions de personnes dont les numéros de sécurité sociale et d'autres informations sensibles ont été impactées par la faille, le nombre d'empreintes digitales qui ont été volées a été revu à la hausse pour passer de 1,1 à 5,6 millions », a indiqué l'administration. « Cela ne fait pas grimper le nombre de 21,5 millions de personnes touchées par cet incident ».

Les victimes notifiées seulement maintenant

Par ailleurs, le service du personnel des fonctionnaires américains indique qu'une équipe inter-agence est toujours mobilisée pour analyser et affiner les données précisément volées et se prépare à envoyer des lettres de notification à toutes les personnes touchées. A l'heure du big data et des solutions de traitement en masse de données, on ne peut que s'interroger sur le temps de latence – plus de deux mois – dont a eu besoin cette administration pour faire un point complet sur l'ensemble des personnes et données touchées. Un temps dont ont certainement pu profiter les pirates pour exploiter et mettre à l'abri ces données en vue de les réutiliser à des fins frauduleuses ou bien de les revendre.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

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

Source :

<http://www.lemondeinformatique.fr/actualites/lire-5-6m-d-empreintes-digitales-de-fonctionnaires-americains-derobees-62451.html>

Des hackers dupent Apple et infectent des millions d'iPhone | Le Net Expert Informatique



Des hackers dupent
Apple et infectent des
millions d'iPhone

Pour la première fois, des pirates ont réussi à diffuser des applications malveillantes sur le magasin AppStore, en trafiquant le langage de codage utilisé par les développeurs.

Après ses ordinateurs Mac, c'est au tour des iPhone et iPad d'Apple de se frotter aux virus. Le groupe à la pomme croquée a confirmé à Reuters que son magasin d'applications AppStore a été victime de sa toute première faille de sécurité majeure. Jusqu'à présent, l'AppStore était réputé comme ultra-sûr puisqu'Apple inspecte minutieusement chaque appli avant de la proposer aux téléchargements (à l'inverse du Play Store de Google), afin d'éviter les logiciels malveillants mais aussi imposer sa chape de plomb sur le sexe.

Sauf que des pirates malins ont trouvé une parade pour échapper à la vigilance de la pomme. Les hackers sont remontés jusqu'à la source de toutes les applis, le langage de codage Xcode, pour diffuser auprès des développeurs naïfs une version compromise (intitulée XcodeGhost).

Toutes les applis créées avec cet outil pouvant dès lors de se transformer en logiciel malveillant. Un porte-parole d'Apple souligne auprès de Reuters :

Nous travaillons avec les développeurs afin de garantir qu'ils utilisent la version authentique de Xcode pour redévelopper leurs apps ». La version compromise de Xcode a été identifiée comme hébergée sur un serveur chinois. Les développeurs ont préféré celle-ci puisqu'elle s'avérait beaucoup plus rapide à télécharger que le logiciel officiel hébergé sur le serveur d'Apple.

Des centaines de millions d'iPhone exposés

Selon la firme de sécurité Palo Alto Networks Inc, 39 applications malicieuses ont été découvertes et certaines sont particulièrement populaires, dont :

- l'incontournable appli de discussion instantanée WeChat,
- le très utilisé enregistreur de cartes de visites CamCard,
- Didi Chuxing, le concurrent chinois d'Uber,
- l'unique appli pour acheter des billets de train en Chine Railway 12306.

Au total, plusieurs centaines de millions d'utilisateurs pourraient avoir été victimes d'un vol de données tels que des mots de passe, estime l'entreprise, même si aucun cas n'a pour l'heure été constaté.

La firme de sécurité chinoise Qihoo360 affirme elle avoir détecté pas moins de 344 applis compromises. Plusieurs ont été retirées de l'AppStore par Apple, mais le groupe refuse de donner le nombre exact d'applications concernées. Un porte-parole affirme à « l'Obs » : *Nous prenons la sécurité très au sérieux et iOS [le système de l'iPhone et l'iPad, NDLR] est conçu pour être fiable et sécurisé. Pour protéger nos clients, nous avons supprimés les applications de l'AppStore que nous savons créées avec cet outil contrefait.* »

Sur son blog, WeChat affirme que seule la version de son appli antérieure au 10 septembre était affectée par la faille de sécurité. Une nouvelle version a depuis été diffusée pour remédier au problème.

Les iPhone, « des cibles de choix »

Selon Ryan Olson de Palo Alto Networks Inc, « l'information n'est toutefois pas à prendre à la légère », puisque cela montre que l'AppStore peut être compromis par des hackers qui ciblent les développeurs. Pis, cela pourrait donner des idées à d'autres et il sera difficile de s'en prémunir, estime-t-il.

L'iPhone ne serait-il plus aussi sûr qu'à ses débuts ? « Avec l'augmentation des parts de marché d'Apple, le nombre de cibles augmente et l'intérêt des cybercriminels augmente », pointe Laurent Heslault, responsable des stratégies de sécurité chez Symantec. Jérôme Billois, administrateur du Club de la sécurité de l'information français (Clusif), renchérit :

Surtout que les utilisateurs d'Apple sont connus pour avoir des revenus plus élevés, faisant d'eux des cibles de choix ».

Surtout que les utilisateurs d'iPhone – et plus largement de smartphones – n'ont pas encore pris pleinement conscience des risques de piratage sur ces mini-ordinateurs. Rien que l'an dernier, l'entreprise de sécurité Symantec a découvert 6,3 millions d'appli malicieuses capables d'infecter les terminaux.

Apple n'est donc pas beaucoup plus sûr que ses concurrents. Le rapport annuel de Symantec pointe que 84% des vulnérabilités découvertes le sont sur iPhone (contre 11% pour Android). Le plus souvent, elles sont exploitées pour infecter l'appareil, dérober des informations personnelles (mots de passe, comptes bancaires...), afficher des publicités, ou encore envoyer des SMS surtaxés. Laurent Heslault interroge :

Il y a des centaines de milliers d'applications gratuites disponibles, croyez-vous qu'il y ait autant de philanthropes ? »

La vigilance est donc de rigueur avant de cliquer sur un lien, entrer ses identifiants sur un site, etc. Même prudence lorsqu'une fenêtre pop-up s'ouvre sur l'iPhone, réclamant l'identifiant et le mot de passe iCloud. Si elle n'a pas de raison de s'ouvrir (par exemple lors de la consultation de ses e-mails), alors il n'y a pas de raison de lui donner les informations.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

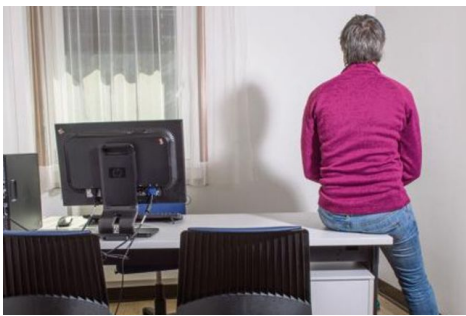
- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

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

Source : <http://tempsreel.nouvelobs.com/tech/20150921.0BS6188/des-hackers-dupent-apple-et-infectent-des-millions-d-iphone.html>
Par Boris Manenti

Une famille valaisanne a volé en éclats après que le père a été victime d'un arnaqueur | Le Net Expert Informatique



Une famille valaisanne a volé en éclats après que le père a été victime d'un arnaqueur.

«C'est quarante ans de mariage et de vie de famille mis à la poubelle.» La voix de Suzanne est emplie de larmes. En six mois, sa famille a volé en éclats. La faute à une arnaque sur le Web.

«Début 2015, j'ai entendu mon père passer un coup de fil pour faire verser une grosse somme d'argent au Mali via Western Union», raconte la Valaisanne. Intriguée, Suzanne prévient son frère, puis sa mère.

Ensemble, ils vont découvrir que le père de famille est en réalité victime d'une escroquerie via Internet. «Il croit discuter avec une Française partie vivre au Mali. Il l'a rencontrée sur un jeu en ligne», explique la Valaisanne. La prétendue expatriée, mère de famille et veuve, jure avoir hérité de près d'un million de francs. Seul problème, pour débloquer la somme, elle a besoin d'un petit investissement de départ. «Papa a déjà versé plusieurs dizaines de milliers de francs. Heureusement, on a réussi à faire bloquer les comptes pendant un temps», détaille la Valaisanne. Elle a bien essayé de discuter avec son père, mais le résultat a été catastrophique. «Il s'est énervé et il a quitté la maison. Il est persuadé que tout est vrai», soupire-t-elle. Le père n'a donc plus aucun contact avec le reste de la famille, surtout que les parents de Suzanne se sont officiellement séparés en juin dernier.

La juge, tout comme la police avant elle, a bien essayé de raisonner le sexagénaire, mais rien n'y fait. «Pourtant, il est loin d'être bête, mais là c'est gros comme un camion et il ne voit rien», assure Suzanne. Au point qu'elle se demande s'il se rendra compte un jour qu'il s'agit d'une arnaque. «Il a tellement peur qu'elle l'abandonne qu'il continue de verser encore et encore», précise la Valaisanne. Mais le plus dur pour elle, c'est le côté humain. «On est désemparés et on ne comprend pas. Il a toujours été plutôt radin, et là, il dépense des fortunes pour une femme qu'il ne connaît pas. Il rêve même de faire baisser la pension alimentaire de ma mère parce qu'il n'a plus un rond à lui envoyer», souligne-t-elle.

Aujourd'hui, Suzanne ne sait plus quoi faire. Elle regrette le manque de structures de soutien en Suisse. «Il n'y a rien ni personne pour nous aider. Je suis fatiguée par cette histoire. Cela me rend malade.»

Une détresse que comprend André Frachebourg, responsable sécurité d'un établissement bancaire et connaissance de la famille. «Les enfants ont un sentiment d'impuissance. Leur père ne croit plus ce que ses proches disent, il n'écoute plus personne», témoigne-t-il. Lui-même a essayé de raisonner le sexagénaire. En vain. «Il est dans ce qu'on appelle un effet «tunnel», analyse-t-il.

En tant que responsable sécurité, il a régulièrement affaire à ce genre de cas: «Il y a des victimes de tout âge. Nous, on essaie de faire des mises en garde quand on voit qu'il y a des sommes inhabituelles qui sortent», explique-t-il.

André Frachebourg regrette que le phénomène soit encore aussi tabou en Suisse: «Souvent, les victimes n'osent pas en parler. Elles ont honte d'avoir été grugées. Il devrait y avoir un soutien plus fort pour elles», conclut-il.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

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

Source : <http://www.lematin.ch/suisse/On-est-desempares-on-ne-comprend-pas/story/12808386>

Un phishing a permis de voler 1,8 millions de \$ en Bitcoins | Le Net Expert Informatique



Un phishing a permis de voler 1,8
millions de \$ en Bitcoins

BitPay, un spécialiste du Bitcoin basé à Atlanta (USA) a été frappé, en décembre 2014, par un filoutage de masse à l'encontre de ses utilisateurs. Un phishing qui aurait permis au pirate de détourner 5.000 bitcoins. L'Atlanta Business Chronicle indique que le pirate s'est fait passer pour le patron de BitPay, Bryan Krohn. Via de faux courriels, l'escroc a réussi à piéger plusieurs personnes, dont David Bailey, fondateur du journal yBitcoin. Le voleur a réussi trois transferts via SecondMarket et Bitstamp pour une valeur de 1.000 (deux fois) et 3.000 bitcoins.

C'est la troisième fois que BitPay se fait pirater en 10 mois. Une affaire qui ne serait jamais sortie de l'ombre si l'assureur de BitPay, la Massachusetts Bay Insurance Compagny avait remboursé les 950.000\$ de perte occasionnée par cette attaque. Bilan, BitPay a mis son assureur devant les tribunaux en juin 2015. Le tribunal (2) a mis en ligne les informations.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

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

Source : <http://www.zataz.com/bitcoins-piratage-bitpay/>

Un électeur peut-il utiliser la liste électorale ? | Le Net Expert Informatique

 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité</p> <p>vous informe...</p>	<h2>Un électeur peut-il utiliser la liste électorale ?</h2>
<p>Tout électeur peut obtenir de sa mairie une copie de la liste électorale à condition de s'engager à ne pas en faire un usage commercial. A noter : la Commission d'accès aux documents administratifs (CADA) considère que l'accès aux listes électorales peut s'exercer par consultation gratuite sur place ou par envoi de copies, sur support papier ou informatique.</p>	
<p>Nous organisons régulièrement des actions de sensibilisation ou de formation au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.</p> <p>Besoin d'informations complémentaires ? Contactez-nous Denis JACOPINI Tel : 06 19 71 79 12 formateur n°93 84 03041 84</p>	
<p>Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.</p> <p>Nos domaines de compétence :</p> <ul style="list-style-type: none">• Expertises et avis techniques en concurrence déloyale, litige commercial, piratages, arnaques Internet.. ;• Consultant en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;• Formateur et chargé de cours en sécurité informatique, cybercriminalité et déclarations à la CNIL. <p>Contactez-nous</p>	
<p>Cet article vous plaît ? Partagez ! Un avis ? Laissez-nous un commentaire !</p>	
<p>Source : http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=16F67A95B36120F226D2F8E337B98601?name=Liste+%C3%A9lectorale+%3A+un+%C3%A9lecteur+peut-il+l%27utiliser+%3F6id=175</p>	