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.

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.

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.

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.

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://pro.clubic.com/it-business/securite-et-donnees/actualite-780740-virus-decouvert-distributeurs-billets.html?estat_svc=s%3D223023201608%26crmID%3D639453874_1167429992#pid=22889469

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

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.

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

	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

网易云音乐-好口碑,电台FM歌曲下载必备
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

网易公开课 — 教育视频平台，名校名师名课，TED演讲、优质纪录片
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: 3.6

喜马拉雅FM (Podcasts) 儿童故事评书段子财经相声radio
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 4.3.8

开眼 — 精选视频推介，每天大开眼界
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 1.8.0

愤怒的小鸟2-李易峰至尊手游
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 2.1.1

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

电话号码归属地助手
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 3.6.5

自由之战-真·5V5(第一MOBA手游)
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 1.1.0

中国联通手机营业厅(官方版)
Action: Uninstall immediately
Current Status: Still malicious
Last version checked: 3.2

股市热点
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/xc
odeghost-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.

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 compromises (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. Gérome 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

Source : http://tempsreel.nouvelobs.com/tech/20150921.OBS6188/des-hackers-dupent-apple-et-infectent-des-millions-d-iphone.html
Par Boris Manenti

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 Massachusettes 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.

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

Cyberespace : les USA et la Chine font la paix | Le Net Expert Informatique

L**e New York Times informe qu'un accord de non-agression contre les sites d'infrastructure critique en temps de paix devrait être signé au cours de la visite du président chinois Xi Jinping aux États-Unis la semaine prochaine.**

Plus tôt, le président américain Barack Obama avait parlé du risque d'aggravation des relations bilatérales en cas d'impossibilité de trouver un terrain d'entente. Au printemps, un tel accord avait déjà été signé entre la Russie et la Chine. Un nouveau régime international de conduite des pays dans le cyberespace pourrait ainsi voir le jour progressivement.

Les représentants de la Chine et des USA mènent des négociations sur un accord les engageant mutuellement à ne pas porter d'attaques cybernétiques contre des sites d'infrastructure critique en temps de paix. Cet accord visera à prévenir les attaques contre les centrales électriques, les systèmes bancaires, les réseaux téléphoniques et les hôpitaux. Les sources du NYT auprès de l'administration du président américain soulignent que ce document devrait contenir peu d'aspects concrets. Il impliquera très probablement des engagements sur le respect des principes et des règles de conduite dans le cyberespace adoptés par un groupe d'experts gouvernementaux de l'Onu en juin dernier.

L'accord en question ne devrait pas concerner l'espionnage industriel des sites commerciaux qui, selon les USA, constituent la grande partie des intrusions chinoises. Ces derniers temps, ce problème est devenu central dans les relations bilatérales. « A un certain moment nous commencerons à considérer les cyberattaques comme une menace à la sécurité nationale et nous y réagirons en conséquence », a déclaré le 11 septembre Barack Obama à Fort Meade devant les militaires américains. Le 16 septembre, il déclarait aussi aux représentants de la communauté d'affaires: « Nous avons préparé plusieurs mesures appelées à montrer que si cette question n'était pas réglée, elle compliquerait considérablement les relations bilatérales ».
Les opinions exprimées dans ce contenu n'engagent que la responsabilité de l'auteur.

Source : http://fr.sputniknews.com/presse/20150921/1018285357/cyberespace-usa-chine.html
Par Kommersant

Emission Infrarouge sur France 2 ce mardi à 22h50 : On nous écoute : Cyberguerre, l'arme fatale ? – 1ère partie | Le Net Expert Informatique

Emission Infrarouge sur France 2 ce mardi à 22h50 : On nous écoute : Cyberguerre, l'arme fatale ? – 1ère partie

« Plus rien ne peut rester secret, même nos vies. Parano de grande ampleur ? Complot d'état ? Quelle est la réalité de la plus grande campagne de surveillance jamais élaborée ? »
Edward Snowden, est interviewé en exclusivité à Moscou pour le documentaire.A l'heure où la France vient de voter la très contestée Loi sur le Renseignement, où le hacking, le tracking et la cyber-surveillance font partie des grands débats de nos sociétés, où les révélations d'Edward Snowden ont enflammé la planète, les questions que posent ces 2 films deviennent incontournables.

Sommes-nous tous des coupables potentiels à surveiller ? Faudra-t-il abandonner notre présomption d'innocence pour une sécurité dont tout le monde sait qu'elle ne peut pas être totale ? Comment contrôler les services de renseignements sans les empêcher de travailler efficacement ? Et sommes-nous prêts à protéger nos propres lanceurs d'alerte face aux pressions récurrentes d'un Etat-surveillance de plus en plus puissant ?

Une guerre d'un nouveau genre a vu le jour, qui bouleverse les règles et les enjeux des conflits traditionnels. Internet est en train de modifier totalement les champs de bataille, de brouiller les frontières entre alliés et ennemis, entre espionnage et sabotage, entre guerre et paix. Pas avec des armes lourdes mais avec des codes et des virus de plus en plus sophistiqués pour déstabiliser, prendre le contrôle ou détruire des centrales électriques ou nucléaires, un réseau ferroviaire, un ministère, des ordinateurs de guidage …

Nos armées se dotent de moyens toujours plus sophistiqués pour lutter contre un ennemi inconnu, invisible et imprévisible. Comment se défendre ? Comment attaquer ?

De nos choix dépendra la société dans laquelle nous vivrons à l'avenir.

Une série documentaire inédite (2X52′) écrite et réalisée par Pierre-Olivier François
Une coproduction Artline Films, WGBH Frontline et NOVA
Produit par Olivier Mille
Avec la participation de France Télévisions
Avec le soutien du Centre National du Cinéma et de l'Image Animée
Unité de programmes documentaires de France 2 : Fabrice Puchault et Barbara Hurel
La case Infrarouge invite les téléspectateurs à réagir et commenter les documentaires en direct sur twitter via le hashtag #infrarouge

---

Source : http://www.france2.fr/emissions/infrarouge/diffusions/22-09-2015_341460

Des applications malveillantes dans l’App Store | Le Net Expert Informatique

Des pirates ont trouvé le moyen de faire entrer des applications malveillantes dans la boutiques d'Apple. Ils ont pour cela convaincu des développeurs d'utiliser une version modifiée de Xcode, introduisant ainsi des malwares sur l'App Store.

Pour minimiser les risques d'infection des terminaux mobiles, les éditeurs de plateformes recommandent (ou imposent) l'utilisation de leurs boutiques d'applications officielles. Il est malgré tout possible d'éviter les mécanismes de contrôle mis en place par exemple par Google et Apple.

Et Apple vient d'ailleurs d'en faire les frais. La firme a confirmé officiellement à Reuters avoir dû retirer plusieurs apps de l'App Store suite à la découverte d'une faille de sécurité. Des pirates ont trouvé une solution pour échapper à la vigilance de l'éditeur.

Xcode corrompu pour pénétrer l'App Store

Pour concevoir des applications pour iOS et OS X, les développeurs ont recours aux outils de développement d'Apple regroupés au sein du logiciel Xcode. Les pirates ont ainsi mis au point une version modifiée de Xcode, diffusée ensuite auprès de développeurs d'apps. Les applis réutilisant cet outil se transformaient dès lors en malwares.

Présenté sous la dénomination XcodeGhost, ce malware a pu faire son entrée sur l'App Store. Plusieurs applications populaires ont été compromises par cette méthode dont la messagerie WeChat, CamCard ou le concurrent chinois d'Uber, Didi Chuxing.

WeChat a précisé dans un billet de blog 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.

« Nous travaillons avec les développeurs afin de garantir qu'ils utilisent la version authentique de Xcode pour redévelopper leurs apps » déclare un porte-parole d'Apple auprès de Reuters. Le malware XcodeGhost est présenté par la société de sécurité Palo Alto Networks comme particulièrement nuisible et dangereux.

L'éditeur de sécurité précise également que la version compromise de Xcode a été identifiée sur un serveur en Chine. Et si elle a été utilisée par les développeurs, c'est probablement car elle s'avérait plus rapide à télécharger que le logiciel officiel hébergé chez Apple.

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

Source : http://www.zdnet.fr/actualites/apple-contraint-de-supprimer-des-apps-malveillantes-de-l-app-store-39825174.htm