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

	Cyberespace : les USA et la Chine font la paix

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.**

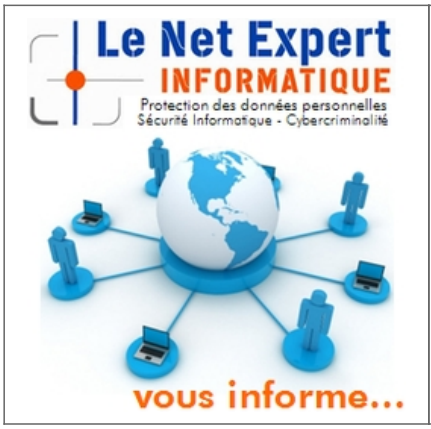
Plus tôt, le président américain Barack Obama avait parlé du risque d'aggravation des relations bilatérales en cas d'impossibilité de trouver un terrain d'entente. Au printemps, un tel accord avait déjà été signé entre la Russie et la Chine. Un nouveau régime international de conduite des pays dans le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

Le Cameroun se couvre contre la cybercriminalité | Le Net Expert Informatique

	Le Cameroun se couvre contre la cybercriminalité

Un atelier initié par l'Ecole nationale supérieure polytechnique et financé par le Fonds spécial des activités de sécurité du ministère des Postes et télécommunications, veut mettre fin à la vulnérabilité des systèmes d'information des administrations publiques.

La rencontre de Yaoundé intervient en réponse aux intrusions malveillantes, dans le réseau d'interconnexion électronique, des systèmes d'information de l'administration mis en place par le ministère des Postes et télécommunications (Minpostel). Ce phénomène, explique le patron dudit département, Jean Pierre Biyiti bi Essam, cause de nombreuses pertes à l'Etat.

Les chiffres donnent en effet des sueurs froides, interpellant les pouvoirs publics pour une mise sur pied immédiate de nouvelles mesures de lutte contre un fléau planétaire. En 2014, les administrations camerounaises ont accusé plus de 14 milliards de FCfa de manque à gagner du fait de la cybercriminalité. En 2012, la compagnie aérienne nationale Camair-Co a perdu 2 millions FCfa en vente de billets ; Ecobank s'est fait hacker 43 comptes en 24 heures avec 3 milliards de FCfa, l'opérateur Mobile Telecommunications Networks (Mtn) a perdu un 1,8 milliard d'envoi de crédits. Plusieurs personnalités et représentations diplomatiques n'ont pas échappé aux attaques en ligne.

Le phénomène de la cybercriminalité a pris une envergure mondiale et sa propension, au Cameroun, a contraint le Jean Pierre Biyiti bi Essam à se rendre au front le 8 septembre à Yaoundé, pour le lancement d'un atelier de formation des personnels des administrations publiques. Il est question de sensibiliser les personnes en charge desdits systèmes sur les risques qui planent sur les réseaux des administrations, d'améliorer le niveau de sécurité des outils utilisés.

Un premier forum sous-régional sur la cybersécurité et la cybercriminalité s'était tenu du 24 au 27 février 2015 au Palais des congrès de Yaoundé. Organisée en partenariat avec l'Union internationale des télécommunications et le Commonwealth Telecommunication Office (CTO) en collaboration avec Interpol, la Communauté économique et monétaire des Etats de l'Afrique centrale (Cemac) et la Communauté économique des États de l'Afrique centrale (Ceeac), cette rencontre avait permis de mener des réflexions en vue de l'harmonisation des stratégies de lutte contre le phénomène, des régulations et réglementations en matière de cybersécurité et cybercriminalité, des moyens et outils de lutte, l'adoption de bonnes pratiques visant à créer une culture de cybersécurité en Afrique centrale, le renforcement des capacités et le partage des connaissances ainsi que la protection de l'enfant en ligne.

TIC

Les technologies de l'information et de la communication (TIC) se développent de manière exponentielle et irréversible, induisant une nouvelle civilisation ayant pour socle l'économie dite numérique. Force est cependant de souligner que les TIC s'accompagnent d'une poussée vertigineuse d'infractions et crimes de toute nature. Les atteintes aux biens renvoient à la fraude des cartes bancaires, à la vente, par petites annonces ou aux enchères, d'objets volés ou contrefaits, à l'encaissement d'un paiement sans livraison de la marchandise et autres arnaques de la même veine, au piratage d'ordinateurs, à la gravure pour soi ou pour autrui de musiques, films ou logiciels, etc. Les atteintes aux personnes se réfèrent quant à elles à la propagation d'images pédophiles, à la diffusion, auprès des enfants, de photographies à caractère pornographique ou violentes, de méthodes de suicide, de recettes d'explosifs ou d'injures à caractère racial, d'atteinte à la vie privée, etc.

Selon un rapport publié en 2011, McAfee, une société de sécurité informatique basée aux Etats-Unis, indique le «.cm» du Cameroun fait partie des cinq noms de domaine les plus risqués de la planète (.cm, .com, .cn, .ws, .info), avec un taux de risque de 36,7% sur environ 27 millions de noms de domaines analysés. Ce fléau a connu une flambée sans précédent entre juin 2009 et juin 2010. Les cybercriminels sont allés jusqu'à pirater le site officiel des services du Premier ministre en créant un site web frauduleux («http://www.govcamonline.com/») dont la page d'accueil portait les mêmes informations, jusqu'aux appels d'offres lancés sur le vrai site.

C'est ainsi que de nombreuses personnes, tant du Cameroun qu'ailleurs, se sont vues extorquer d'importantes ressources. Bien d'autres sites web camerounais ont également fait l'objet de cyberattaques à l'instar la douane, en 2008, du ministère des Domaines et des Affaires foncières au cours de la même année, de l'université de Yaoundé I en 2009, des quotidiens La Nouvelle Expression et Cameroon Tribune en 2011, etc.

Mesures de sécurité à parfaire

Le Cameroun a développé un certain nombre d'applications visant à automatiser les procédures, dans le cadre de la politique de mise en place de la gouvernance électronique. Il s'agit notamment de Sigipes, Sydonia, Depmi, e-Guce, etc. De même, les activités de transfert électronique d'argent, de consultation des comptes bancaires en ligne et bien d'autres services encore, se développent de manière étonnante. Le monde étant devenu un village planétaire, ces applications n'échappent pas aux menaces cybernétiques. D'où l'implémentation de systèmes visant à lutter contre les cyberattaques.

Une loi (n°2010/012) relative à la cybersécurité et à la cybercriminalité a été promulguée en fin 2010. Elle vise à instaurer la confiance dans l'utilisation des réseaux de communications électroniques et des systèmes d'information, à fixer le régime juridique de la preuve numérique. Elle protège également les droits fondamentaux des personnes physiques, notamment le droit à la dignité humaine, à l'honneur et au respect de la vie privée, entre autres.

Au plan institutionnel, trois structures sont en charge de la gestion de la question de cybersécurité et de la cybercriminalité au Cameroun. D'une part, le Minpostel est chargé de l'élaboration et de la mise en œuvre de la politique de sécurité des communications électroniques et des systèmes d'information, en fonction de l'évolution technologique et des priorités du gouvernement dans le domaine. L'Agence nationale des technologies de l'information et de la communication (Antic), en collaboration avec l'Agence de régulation des télécommunications (ART), assure, pour le compte de l'Etat, la régulation, le contrôle et le suivi des activités liées à la sécurité des systèmes d'information et des réseaux de communications électroniques ainsi que la certification électronique.

Le Cameroun a également entrepris, depuis 2009, de mettre en place, avec le concours de la République de Corée, une plateforme de sécurité appelée PKI (Public Key Infrastructure, ou infrastructure à clé publique), en vue de sécuriser les transactions gouvernementales en ligne. Ce dispositif donne les moyens suffisants au pays d'ouvrir le marché de la certification, dans lequel l'Antic représente à la fois les autorités de certification racine et de certification gouvernementale. Cette architecture s'inscrit dans le cadre des mesures techniques à prendre en vue de garantir la sécurité des transactions gouvernementales dans le cyberespace national. La plateforme de sécurité permet aussi, grâce aux services d'authentification, de non répudiation, d'intégrité et de confidentialité, de prémunir les données et les échanges électroniques gouvernementales d'attaques provenant de cybercriminels.

L’Europe prend un mauvais virage en matière numérique | Le Net Expert Informatique

	L’Europe prend un mauvais virage en matière numérique

Dans l'exercice consistant à élaborer de bonnes politiques en matière numérique, l'Europe a raté son premier test majeur. Au mois de mai, la Commission européenne annonçait la création d'un marché unique du numérique réunissant 500 millions de consommateurs, censé apporter 415 milliards € au PIB de l'Union européenne et créer quelque 3,8 millions d'emplois. Seulement voilà, une récente décision autour d'une problématique numérique majeure – la confidentialité des données – menace de faire dérailler la locomotive.

Au mois de juin, les ministres de l'Intérieur et de la Justice de l'UE ont voté en faveur de la conservation de pouvoirs nationaux significatifs en matière de protection de la confidentialité numérique, plutôt que d'élaborer un ensemble de règles s'appliquant aux 28 Etats de l'UE. Si le Parlement européen venait à approuver cette proposition, la divergence des règles nationales serait alors de retour. Plus inquiétant encore, ceci ouvrirait la voie à la mise en place de dispositions rendant illégales les activités bénignes et peu risquées d'exploration des données, qui sous-tendent la publicité en ligne.

La publicité sur Internet permet aux citoyens de l'UE d'accéder à de l'information, à des contenus éducatifs, à des canaux de commerce et autres sites de divertissement, sans avoir à en payer directement l'accès. En Europe, les montants dépensés dans ce domaine sont en pleine augmentation. Les revenus du secteur ont plus que quadruplé depuis 2006, malgré la stagnation de l'économie européenne dans son ensemble. Le nouveau combat de la confidentialité en UE vient menacer toute cette évolution. Non seulement faut-il s'attendre à une importante charge administrative liée aux coûts supplémentaires et aux difficultés bureaucratiques, mais un risque réel existe également de voir ces nouvelles règles mettre à mal le modèle d'entreprise d'un grand nombre des principales sociétés européennes en ligne.

Il s'agirait d'un véritable gâchis – qui plus est facilement préventible. En 2012, la Commission européenne a formulé une proposition de remplacement de la législation de l'UE existante en matière de protection des données, dont la plus récente version avait été élaborée en 1995, époque à laquelle Internet ne jouait qu'un rôle minime dans l'économie. Le texte initial était prometteur. Il entendait harmoniser les cadres juridiques fragmentés de l'Europe, fournir aux entreprises un guichet unique fort utile, et rassurer les consommateurs en leur garantissant une utilisation appropriée de leurs données.

Malheureusement, beaucoup des propositions les plus judicieuses ont été depuis abandonnées. Lors du rassemblement ministériel du mois de juin, le principe majeur de guichet unique a été véritablement éviscéré. Plutôt que de permettre aux entreprises d'avoir affaire à l'autorité de protection des données compétente au sein du pays dans lequel ces entreprises possèdent leur siège ou leur principale implantation européenne, les Etats membres insistent aujourd'hui pour que les régulateurs nationaux conservent le contrôle. Conformément aux nouvelles règles proposées, toute autorité « concernée » pourrait s'opposer à une décision prise par un autre régulateur national, donnant lieu à une procédure d'arbitrage complexe faisant intervenir l'ensemble des 28 agences.

Les ministres ont également adopté une large définition de ce que l'on entend par données personnelles. Y figureraient ainsi à la fois les cookies (petits ensembles de données stockés sur l'ordinateur d'un internaute) et les adresses IP (code utilisé pour identifier un ordinateur lorsqu'il se connecte à Internet) – bien que ces éléments ne fournissent aucun lien en direction d'un individu donné. Au mieux, cette définition étendue et peu pointue des données personnelles menace de créer des obstacles inutiles pour les annonceurs numériques basés dans l'UE. Au pire, elle risque de plonger leur modèle d'entreprise dans l'illégalité.

Ces règles inutilement strictes en matière de données sont vouées à affecter les entreprises européennes dans une mesure disproportionnée. On peut comprendre qu'il soit demandé à Google, Facebook et autres géants américains d'Internet de solliciter le consentement explicite de leurs utilisateurs. Pour autant, le secteur européen de l'Internet est dominé par des entreprises de B to B, dont les marques peu connues traitent effectivement les données des consommateurs, mais manquent d'un contact direct avec les utilisateurs. Ainsi, la seule véritable alternative consistera pour ces sociétés Internet européennes à travailler auprès des grandes plateformes américaines, et à devenir encore plus dépendantes de celles-ci.

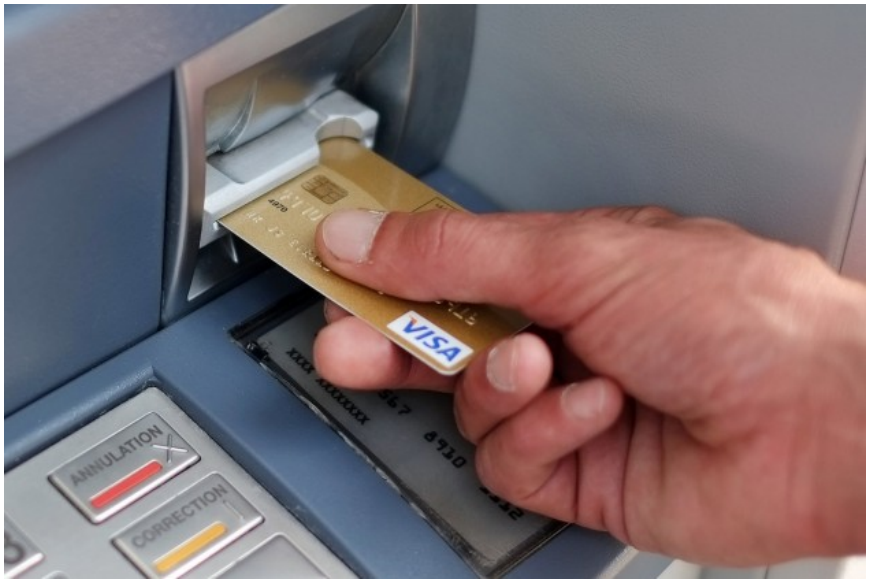
Bien que le Royaume-Uni, la Suède, la Norvège et les Pays-Bas comptent parmi les pays leaders de l'Internet à travers le monde, de nombreux autres Etats européens évoluent considérablement à la traîne. Ainsi, l'économie numérique contribue au PIB de l'UE à hauteur d'environ 4 %, contre 5 % aux États-Unis et 7,3 % en Corée du Sud. Les nouvelles réglementations proposées ne feront qu'accentuer cet important retard des entreprises européennes par rapport à leurs concurrentes internationales.

L'Europe est confrontée à un choix important. Bien entendu, l'UE doit pouvoir rassurer ses citoyens quant à l'utilisation appropriée de leurs données ; les mesures en ce sens peuvent contribuer à la croissance de l'économie numérique. En revanche, les dirigeants du continent ne doivent pas oublier qu'un marché unique du numérique ne pourra exister aussi longtemps que les règles accentueront la divergence des approches nationales autour de la confidentialité, et qu'elles feront obstacle à l'utilisation par Internet des données anonymes à des fins de publicité numérique. Le sort d'une génération toute entière d'entrepreneurs numériques européens est aujourd'hui en jeu.

Source : http://www.libe.ma/L-Europe-prend-un-mauvais-virage-en-matiere-numerique_a66663.html

Par Christopher Engman PDG de la société suédoise de commercialisation en ligne, «Vendemore» (Traduit de l'anglais par Martin Morel)

Ce malware avale des cartes bancaires pour les restituer… aux pirates | Le Net Expert Informatique



Ce malware avale des cartes bancaires pour les restituer… aux pirates

Un nouveau code malveillant a été découvert par des chercheurs en sécurité, ciblant les distributeurs de marque NCR et Diebold.

Un nouveau type de malware pourrait bientôt frapper les distributeurs de banque dans le monde. Les chercheurs en sécurité de FireEye viennent de mettre la main sur un code particulièrement vicieux et, semble-t-il, unique en son genre. Baptisé « Backdoor.ATM.Suceful », il est capable d'infecter des distributeurs de marque NCR ou Diebold -sous Windows- qui sont également présents en France. Son originalité est qu'il s'attaque directement à la carte bancaire de l'utilisateur. Il l'avale tout cru en faisant croire qu'il s'agit d'une erreur de manipulation ou de logiciel.

Le pirate pourra ensuite la récupérer auprès du distributeur. Il lui suffira, pour cela, de tapoter un code particulier sur le clavier de la machine. Le malware peut également lire la bande magnétique ou la puce de la carte. Il peut aussi désactiver certaines fonctionnalités de l'appareil, comme l'alarme, la lumière ou le capteur audio. « Suceful est le premier malware ciblant des distributeurs dans le but de voler les données des cartes ainsi que les cartes elles-mêmes. Le degré de sophistication atteint donc un nouveau record », estime FireEye, dans une note de blog.

Toutefois, il n'existe pas encore de preuve que ce malware soit réellement utilisé à l'heure actuelle. Le code a été trouvé dans la base partagée de VirusTotal, avec une date de création du 25 août 2015. Il pourrait s'agir d'une version de développement, estiment les experts. Par ailleurs, le code n'indique pas comment les pirates pourraient l'installer sur un distributeur.

Quoi qu'il en soit, si votre carte est avalée, il est recommandé d'aller immédiatement prendre contact avec l'agence. Tout en gardant un œil sur le distributeur… sait-on jamais !

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.01net.com/actualites/ce-malware-avale-des-cartes-bancaires-pour-les-restituer-aux-pirates-915042.html
et FireEye

La Police se dote d'un laboratoire cybercriminalistique

informatique | Le Net Expert Informatique

La Police se dote d’un laboratoire cybercriminalistique informatique

La Police nationale s’est dotée d’un laboratoire cybercriminalistique informatique qui est un dispositif qui consiste à mettre des méthodes et protocoles d’investigation permettant de récolter une preuve numérique en vue de mieux lutter contre la cybercriminalité et la cybersécurité, selon Papa Gueye, élève-commissaire à l’Ecole nationale de police.

’’Il s’agit d’un laboratoire cybercriminalistique informatique logé au sein de la Division des investigations criminelles (DIC). Il est équipé avec des matériels de dernière génération et sert à analyser les données et supports informatiques’’, a expliqué M. Gueye.

Il intervenait à une table ronde à l’initiative de la Direction générale de la police nationale sur le thème : ’’La cybercriminalité et la cybersécurité : enjeux et défis pour les forces de sécurité’’.
Cette rencontre qui entre dans le cadre des cycles de conférences intitulées ’’Les mercredi de la police’’, a réuni des experts informatiques, des juristes, des spécialistes en cybercriminalité, plusieurs policiers entre autres participants.

’’De plus en plus les forces de la police sont appelées à faire face à des crimes nouveaux avec une cybercriminalité pointue et trés bien structurée, d’où la nécessité de se doter de ce genre de laboratoire’’, a poursuivi Papa Gueye qui a introduit un exposé intitulé ’’Cybercriminalité au Sénégal : manifestations et réponses des forces de sécurité’’.

Dans sa communication, M. Gueye, ancien officier à la Police, est revenu sur les différents types de cybercriminalité au Sénégal, les réponses apportées par les forces de la police et les obstacles liés à la répression du phénomène. Pour lui, il est ’’obligatoire pour les forces de défense de s’adapter face à des infractions de type nouveau’’.

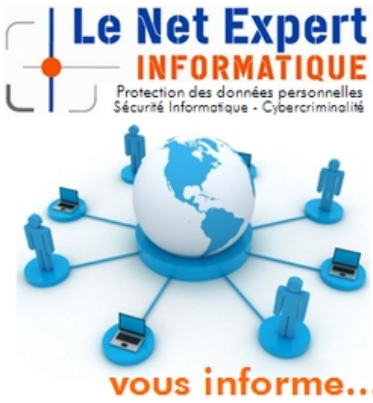
Il a invité les populations à se rendre auprès de la DIC qui héberge ce laboratoire pour exposer leurs mésaventures si elles sont victimes d’infractions liées à la cybercriminalité. Papa Gueye a aussi insisté sur la nécessité de capaciter les acteurs de la police et de sensibiliser les populations sur ces ’’crimes nouveaux’’.

Source :
http://www.aps.sn/actualites/societe/article/la-police-se-dote-d-un-laboratoire-cybercriminalistique-informatique-commissaire

---

Savoir profiter des erreurs

des Cybercriminels | Le Net Expert Informatique



Savoir profiter des erreurs des Cybercriminels

L'affaire Ashley Madison semble le prouver une fois de plus, les cybercriminels commettent des erreurs qui peuvent leur nuire. Détecter ces fautes et savoir les utiliser sont des éléments essentiels dans la gestion des crises cyber.

DES ATTAQUES DONT LES OBJECTIFS SONT SOUVENT DIFFICILES À CERNER

L'actualité le montre trop régulièrement, les actes cybercriminels se multiplient et visent tous types d'organisation. Certains sont revendiqués et leurs objectifs sont rapidement connus. C'est le cas pas exemple de l'attaque visant le site Ashley Madison où les motivations sont explicites.

Mais dans la plupart des cas, les objectifs de l'attaquant sont beaucoup plus difficiles à identifier ! Il est pourtant crucial de le faire pour pouvoir réagir au mieux et protéger rapidement ce qui n'a pas encore été touché par l'attaque.

Une des clés pour mieux comprendre une attaque consiste à exploiter les erreurs des attaquants. En effet, malgré leur niveau de compétences potentiellement élevé, les pirates restent des humains et commettent souvent des erreurs. Des fautes qu'il est possible d'exploiter pour mieux comprendre l'attaque et la contrer, mais aussi pour identifier ceux à son origine.

UTILISER LES ERREURS DES ATTAQUANTS POUR MIEUX LES COMPRENDRE

Le cas récent d'Ashley Madison semble être un bon exemple, même s'il faudra attendre les investigations complètes pour confirmer tous les éléments. Les attaquants auraient diffusé les données volées via BitTorrent en utilisant un serveur loué chez un hébergeur aux Pays Bas. Ils auraient cependant oublié de sécuriser ce serveur, en particulier ils n'ont pas mis de mot de passe sur les interfaces d'administration web. Même si cela ne permet pas de les identifier directement, il s'agit d'une piste de premier choix pour les forces de l'ordre en charge des investigations. Il faut cependant rester prudent car cela peut aussi être une forme de diversion réalisée par les attaquants. Affaire à suivre !

Autre exemple, le cas « Red October ». C'est l'affaire d'une vaste opération de cyber espionnage qui a commencé en mai 2007 et qui a été découverte par le cabinet Kaspersky quelques années plus tard. Le cabinet a réussi à identifier, bloquer et neutraliser le logiciel malveillant en utilisant une faille de l'attaque. En effet, les noms de domaines pour les serveurs d'exfiltration qui étaient utilisés dans le code malveillant n'avaient pas été réservés par les attaquants. Cela a permis à Kaspersky de simuler un de ces serveurs et de voir qui était infecté et quelles données étaient capturées.

Parfois, ces erreurs permettent même d'identifier les auteurs de l'attaque, comme ce fut le cas avec la traque de la personne derrière le malware PlugX.

Nos consultants ont d'ailleurs eux aussi rencontré ce genre de situation dans le cadre d'une attaque ciblée chez un de nos clients. Les pirates avaient en effet « oublié » la présence d'un keylogger sur les serveurs internes utilisés pour l'exfiltration des données, ce qui a permis à nos experts d'identifier quelles données étaient ciblées et où elles étaient envoyées. Nous avons même pu récupérer le login et le mot de passe utilisés par les attaquants. Le concept de « l'arroseur arrosé » remis au goût du jour.

SAVOIR TIRER PARTI DE CES INFORMATIONS POUR MIEUX GÉRER LA CRISE

Les informations obtenues grâce à ces erreurs sont très précieuses, elles permettent ensuite d'adapter la réponse à l'incident. D'autant plus que les attaquants utilisent parfois des mécanismes de diversion « bruyants » (redémarrage de machines, effacement de fichiers, forte activité CPU, voir déni de service…) afin de détourner l'attention des vrais données qu'ils visent. Une compréhension « métier » des objectifs de l'attaque permet d'éviter de se focaliser sur ces pièges.

Il est même souvent intéressant de laisser l'attaque se dérouler pour mieux la comprendre.

Les réflexes face aux incidents de sécurité « classiques » (déployer des signatures antivirales, réinstaller des serveurs…) sont donc aujourd'hui largement révolus. Il faut adopter une approche dynamique de la crise, s'intéresser à son objectif métier et utiliser les erreurs des attaquants pour être plus pertinent, en pouvant même envisager des réponses « actives » à l'attaque. Un challenge pour les équipes de réponses à incidents, qui doivent adapter leurs méthodologies et leurs réflexes, mais un objectif crucial pour lutter contre ces attaques

---

Source :

http://www.solucominsight.fr/2015/08/attaques-ciblees-profiter-des-erreurs-des-attaquants-pour-mieux-les-comprendre-et-les-contrer/

Le secteur public ciblé par la cybercriminalité | Le Net Expert Informatique

Le secteur public ciblé par la cybercriminalité

« Au cours du second trimestre, nous avons assisté à une mutation dans l'univers des menaces. Les pirates informatiques font désormais preuve de davantage de sophistication et de créativité afin de renforcer et de réinventer leurs méthodes d'attaques existantes », observe Raimund Genes, CTO de Trend Micro. « La vision éthérée de la cybercriminalité n'est plus d'actualité. Ce trimestre a démontré que les dommages potentiels des cyberattaques vont bien au-delà de simples bugs logiciels. Le piratage d'avions, de voitures intelligentes et des chaines de TV est en effet devenu une réalité. »

Les hackers identifient et affinent leurs approches de façon plus stratégique, ciblant ainsi leurs victimes de manière plus sélective afin d'améliorer le taux d'infection de leurs attaques. Une tendance qui reflète une réelle progression de plusieurs méthodes d'attaques traditionnelles, avec notamment un bond de 50% de l'utilisation du kit d'exploitation Angler et de +67% pour les menaces utilisant des kits d'exploitation en général. Les attaques ciblant les banques en ligne sont par ailleurs en forte augmentation dans l'hexagone, avec plus de 60% du nombre de PC infectés entre le premier et le second trimestre 2015. D'autre part, l'adware Opencandy et le malware Upatre ont été particulièrement actifs en France ce trimestre, avec respectivement 12 773 et 3 854 PC infectés. Le malware Dyre arrive quant à lui en 4ème position avec 1 469 infections.

De même, les administrations ont été les cibles privilégiées de cyberattaques au cours du second trimestre, avec les piratages massifs des données de l'Internal Revenue Service (le fisc américain) en mai et du système de l'U.S. Office of Personnel Management (une agence gouvernementale américaine responsable de la fonction publique) en juin. Le piratage des données de l'OPM constitue un modèle du genre avec, à la clé, la divulgation de données personnelles identifiables portant sur près de 21 millions d'individus. D'autres agences gouvernementales ont été impactées par des campagnes ciblées utilisant des macros malveillantes, de nouveaux serveurs C&C (Command & Control), de nouvelles vulnérabilités, ainsi que la faille zero-day Pawn Storm.

En se penchant sur le panorama global des menaces au cours du second trimestre, on remarque que les États-Unis jouent un rôle majeur, que ce soit en tant que pays d'origine mais également en tant que cible de nombreuses attaques. Les liens malveillants, le spam, les serveurs C&C et les ransomware y sont tous très présents.

Parmi les points essentiels du rapport :

Des attaques perturbant les services publics : réseaux de diffusion, avions, véhicules automatisés et routeurs résidentiels présentent non seulement un risque d'infection élevé par malware, mais sont également susceptibles d'avoir des répercussions sur l'intégrité physique de leurs utilisateurs.

Le succès d'attaques ransomware ou ciblant les terminaux de points de vente (PoS), aubaine pour les cybercriminels solitaires en quête de notoriété : en déployant les attaques FighterPoS et MalumPoS, ainsi que keylogger Hawkeye, les hackers solos "Lordfenix" et "Frapstar" ont démontré que la force de frappe d'individus isolés est aujourd'hui indéniable.

La lutte des gouvernements contre la cybercriminalité : Interpol, Europol, le département américain de la sécurité nationale et le FBI ont contribué à démanteler des réseaux botnets majeurs et déjà bien établis. D'autre part, l'inculpation de Ross Ulbricht, fondateur de Silk Road, a mis en lumière la nature obscure et redoutable du Dark Web.

Les impacts nationaux et politiques d'attaques ciblant des organisations gouvernementales : la redoutable attaque sur l'OPM a prouvé que la confidentialité de nos données personnelles n'est pas avérée. Les macros malveillantes, les tactiques d'island-hopping (piratage d'une entité tierce avant de remonter vers la cible finale) et les serveurs C&C comptent parmi les tactiques les plus utilisées pour cibler les informations gouvernementales lors d'attaques.

De nouvelles formes de menaces visant les sites web publics et les dispositifs mobiles : alors que les menaces ciblant les logiciels sont toujours d'actualité, les vulnérabilités des applications web se montrent tout aussi dangereuses. Les assaillants savent tirer parti de toute vulnérabilité existante, tandis que les applications personnalisées nécessitent une prise en charge toute aussi personnalisée afin de neutraliser ces passerelles potentielles d'intrusion.

Le rapport

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.globalsecuritymag.fr/Trend-Micro-identifie-de-nouvelles,20150917,55924.html

---

L'écran de verrouillage

d'Android cède une nouvelle fois | Le Net Expert Informatique

L'écran de verrouillage d'Android cède une nouvelle fois

La méthode, assez simple, ne nécessite pas l'injection d'un malware. Elle concerne tous les terminaux sous Android 5.x et supérieurs.

Contourner l'écran de verrouillage des smartphones Android n'est décidément pas très compliqué. Un spécialiste en fait une nouvelle fois la démonstration, utilisant une méthode assez simple qui n'exige pas de connaissances particulières ni l'injection d'un malware. Elle concerne tous les terminaux sous Android 5.x et supérieurs dont l'accès est protégé par un code (et pas un schéma).
La marche à suivre consiste d'abord à accéder aux appels d'urgence puis d'entrer une chaîne de caractères, les surligner (double-clic) et les copier. Il s'agit ensuite de copier et de coller autant de fois que c'est possible cette chaîne dans le champ mot de passe. Puis de se rendre dans l'appli photo, de faire apparaître la zone de notifications et de copier la chaîne de caractère lorsque l'appli demande à nouveau le mot de passe.
A ce moment, (après un moulinage plus ou moins long), l'appli Photo plante et le terminal se débloque comme par magie, permettant d'accéder à tout son contenu.
Prévenu de cette faille, Google n'a pas encore communiqué sur la question.

Source :
http://www.zdnet.fr/actualites/android-l-ecran-de-verrouillage-cede-une-nouvelle-fois-39824986.htm