Cyberattaques : la protection de la France passe désormais par les ordinateurs | Le Net Expert Informatique

	Cyberattaques : la protection de la France passe désormais par les ordinateurs

Après la multiplication des cyberattaques en France, le gouvernement a mis le paquet sur la cyberdéfense : un budget de près d'un milliard d'euros et un premier colloque international organisé à Paris.

C'est un champ de bataille très particulier. Pas de chars, de canons ou d'avions. Pourtant, les victimes peuvent être très nombreuses. Nous voilà dans le monde de la cyberdéfense. Jeudi 24 septembre à Paris se tenait à l'École militaire le premier colloque international consacré au sujet. La France n'est évidemment pas à l'abri. Il faut donc trouver la parade. Le combat numérique, c'est la guerre du XXIème siècle à gagner.

Rappelez-vous du chaos provoqué par l'attaque informatique contre TV5 : des hackers (russes certainement) ont contraint la chaîne de télévision à interrompre ses programmes pendant plusieurs heures après avoir propager par e-mail un virus. En 2010, les services spécialisés américains et israéliens ont créé Stuxnet. Le « ver », le « tenia » informatique, sournois, a été capable d'embrouiller les meilleurs cerveaux iraniens en charge du programme nucléaire, en multipliant les bugs sur les centrifugeuses du site de Natanz. À la clé, Téhéran a perdu deux ans de recherche.

400 anomalies depuis le début de l'année

Aujourd'hui, si Daesh occupe l'espace numérique plutôt comme vecteur de propagande, dans un futur proche avec les moyens dont disposent les djihadistes pourquoi ne pas se lancer dans de telles attaques ? D'autant qu'il a du monde prêt à se vendre au diable, souligne le vice-amiral Arnaud Coustillière, patron de la cyberdéfense française.

« Cet espace numérique a été complètement investi par des pirates informatiques. Je vous parle de mercenaires informatiques. Les mafias se structurent, elles ont des capacités importantes. Il faut donc que les militaires trouvent leur juste place pour être capable d'identifier nos ennemis », dit-il.

On a trouvé plus de 45 virus sur le PC portable d'un sous-traitant

Arnaud Coustillière, patron de la cyberdéfense française

L'an dernier, notre ministère de la Défense a été le théâtre de 780 incidents. On ne parle pas d'attaques. Depuis le début de l'année, on tourne déjà autour de 400 anomalies identifiées, principalement sur les sites de communication (comme celui de la Dicod ou de l'état-major). Pour le reste, le ministère est plus discret. Mais il ne faut pas oublier les industriels de la défense : les grands groupes, comme les plus petites société. Là le bât blesse : la vulnérabilité est de tous les jours.

« Ce qui nous préoccupe également c'est, comme dans toutes les sociétés, les interventions dans l'environnement des plateformes de nos sous-traitants. On a trouvé plus de 45 virus sur le PC portable d'un sous-traitant qui venait faire une maintenance sur un système d'arme qui devait tirer en exercice quelques jours après. C'est inadmissible », relate Arnaud Coustillière.

Un drone Harfang avait connu des problèmes avant son décollage d'Afghanistan, justement parce qu'un serveur en France était contamine. La mission avait été retardée. Ce qui fait désordre, mais surtout peut coûter la vie à des militaires non protégés.

Maîtres en logiciels

Il ne faut pas se priver d'attaquer. Mais il faut d'abord se défendre. Au moins la menace a été prise en compte en 2009. Il y a eu la création de l'Agence nationale de la sécurite des systèmes d'information (Anssi), avec son groupe d'intervention. Il y a aussi un centre opérationnel 7 jours sur 7, 24 heures sur 24 qui apporte son expertise : il veille, détecte et alerte.

La nouvelle loi de programmation militaire vient apporter un milliard d'euros supplémentaires dans l'escarcelle et 1.000 spécialistes de plus, à recruter dans les écoles d'ingénieurs notamment. Il y a également ces compagnies cyber, maîtres en logiciels, qui sont formées. Il y en a une déployée à Abou Dhabi dans le cadre de l'operation « Chamal », et bientôt une autre sur le Charles-de-Gaulle qui doit appareiller en novembre. Avec, c'est certain, une double priorite pif-paf attaque-défense.

Source :
http://www.rtl.fr/actu/societe-faits-divers/cyberattaques-la-protection-de-la-france-passe-desormais-par-les-ordinateurs-7779843074

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.

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.

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

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

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 :

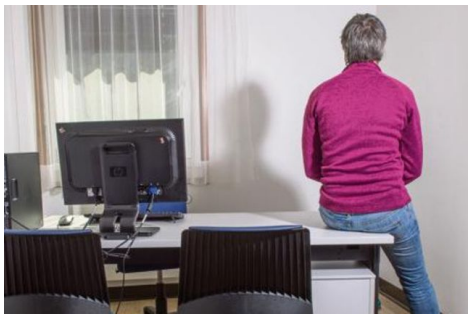
Il y a des centaines de milliers d'applications gratuites disponibles, croyez-vous qu'il y ait autant de philanthropes ? »

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

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.

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 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/

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.

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