Attention aux arnaqueurs qui sévissent sur le site Immoweb ! | Le Net Expert Informatique

Attention aux arnaqueurs qui sévissent sur le site Immoweb !

Avec l'été, les fausses petites annonces pour des lieux de villégiature fleurissent sur les sites internet. Et dans quelques semaines, ce sera au tour des faux kots pour étudiants.

Le modus operandi des arnaqueurs est simple : on vous appâte avec un bien à louer à prix cassé. Puis, on vous demande une caution, à verser via un mandat postal ou Western Union. Et vous êtes quitte de votre argent… Immoweb tire la sonnette d'alarme. L'arnaque en question n'est pas nouvelle, mais elle a repris de plus belle avec l'arrivée des vacances scolaires. Pour l'instant, ce sont principalement des annonces pour des lieux de villégiature qui se révèlent fausses. « On peut ainsi voir une maison dans le sud de la France ou dans un lieu exotique, à un prix dérisoire », explique Olivier Bogaert, commissaire à la Computer Crime Unit, l'unité spécialisée dans la cybercriminalité de la police fédérale.
Le candidat locataire tombe sous le charme des photos alléchantes, et du prix cassé. Et il contacte via le site internet le propriétaire. Les discussions quittent alors l'espace du site internet où était placée l'annonce.
« Le propriétaire peut expliquer qu'il avait un locataire qui s'est désisté au dernier moment et qu'il baisse donc le prix, ou qu'il recherche surtout à ce que sa maison ou son appartement ne reste pas vide. Il est souvent à l'étranger, de sorte qu'il demande à ce que vous versiez un acompte ou le loyer via Western Union, ou via une banque étrangère. Il peut aussi demander à ce que vous lui envoyiez une carte de crédit prépayée, que vous aurez crédité d'un certain montant ».

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

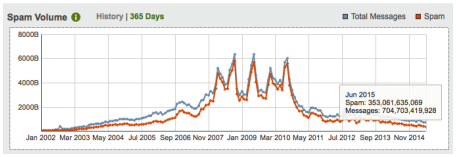
Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.sudinfo.be/1334805/article/2015-07-17/immoweb-previent-ses-utilisateurs-attention-aux-arnaqueurs-qui-sevissent-sur-le

---

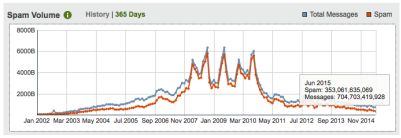
Le spam est à son niveau le plus bas | Le Net Expert

Informatique



Le spam est à son niveau le plus bas

Aurons-nous finalement raison du spam ? Il semblerait en tout cas que les efforts menés sur ce secteur commencent à porter leurs fruits selon un rapport du cabinet Symantec.
Les analystes de Symantec ont publié leur rapport de sécurité portant sur le mois de juin. Selon les chiffres internes, le taux de spam sur l'ensemble des emails envoyés le mois dernier n'était que de 49,7%. « C'est la première fois depuis plus de dix ans que ce taux passe sous la barre des 50% », expliquent ainsi les experts. Plus précisément, la proportion de courriers indésirables est donc à son plus bas depuis le mois de septembre 2003.
Symantec affirme que les actions en justice menées contre les réseaux criminels contrôlant les réseaux de botnets portent véritablement leurs fruits. Il est possible que le spam ne soit plus une source de revenus stables pour les cybercriminels.



Symantec ajoute que le taux d'attaques par phishing ou le déploiement de malware par email est également en baisse. En revanche, sur le mois de juin, 57,6 millions de nouvelles variantes de malware ont été identifiées, contre 44,5 millions au mois de mai et 29,2 millions en avril. Cela signifie donc que si les activités criminelles ne ralentissent pas, elles sont désormais effectuées de manière différente (par exemple via les réseaux communautaires, la messagerie instantanée, les applications mobiles ou les pages Web malveillantes).
Récemment, l'équipe de Gmail annonçait avoir optimisé l'intelligence artificielle appliquée aux filtres anti-spam avec un réseau de neurones artificiels. Les algorithmes s'en trouvent alors plus performants et devraient être capables de mieux discerner les courriers indésirables. En octobre dernier, Microsoft expliquait pour sa part bloquer 10 millions de spams chaque minute. La firme de Redmond a notamment participé à la fermeture de plusieurs botnets.
Consulter le rapport dans son intégralité sur cette page (PDF)

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

Source :
http://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/spam-pourriel/actualite-773950-spam-niveau-bas-12-ans.html?estat_svc=s%3D223023201608%26crmID%3D639453874_1070073452#pid=22889469

A Guédiawaye (Sénégal), la police démantèle un réseau de ressortissants nigérians | Le Net Expert Informatique

A Guédiawaye (Sénégal), la police démantèle un réseau de ressortissants nigérians

6 ressortissants nigérians ont été interpellés par les éléments de la Brigade de recherches du Commissariat de police de Golf Sud (Guédiawaye). Le matériel qui a été découvert chez eux a permis de conclure que ces derniers s'activaient dans la cybercriminalité, selon le journal Grand Place.

La police de Guédiawaye (Sénégal) vient de démanteler un vaste réseau de cybercriminalité entretenu par des ressortissants nigérians. C'est suite à une information anonyme relative aux agissements répréhensibles de ces derniers que l'agent de police en chef de la commune de Golf Sud a mis sur pied un plan de neutralisation. Ainsi, ses hommes en civil se sont rendus sur les lieux dans la nuit du vendredis 10 juillet, aux environs de 23h, et ont pu arrêter 6 ressortissants nigérians.
Une perquisition de l'immeuble où ils ont été trouvés a permis de mettre la main sur 6 ordinateurs portables de marques différentes. L'exploitation des différents logiciels et autres systèmes des machines a permis la découverte d'installations et de fichiers de comptes bancaires de tiers ainsi que de faux documents étatiques et de réfugiés politiques.
Il y avait aussi plusieurs systèmes sur les ordinateurs portables avec des noms de code permettant à leurs propriétaires d'exercer, en toute discrétion, une activité criminelle.
– L'un permet d'effacer toutes les données après chaque redémarrage de l'outil informatique,
– alors que le deuxième est un système de navigation qui consiste à utiliser Internet sans pour autant être tracé ou repéré par les opérateurs de téléphonie.
– Et le troisième logiciel installé sur la machine ouvre la possibilité aux présumés cybercriminels de pirater les comptes bancaires d'autrui sans laisser des traces.

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

Source : http://www.leral.net/Cybercriminalite-a-Guediawaye-La-police-demantele-un-reseau-de-ressortissants-nigerians_a149877.html

---

Avis trimestriel N° 02-2015

de la Commission de protection des données personnelles du Sénégal (CDP) | Le Net Expert Informatique

Avis trimestriel N° 02-2015 de la Commission de protection des données personnelles du Sénégal (CDP)

Le présent avis trimestriel de la CDP concerne la période allant du 1er avril au 30 juin 2015. Il décrit les activités au sein de la Commission et les constats sur le traitement des données personnelles par les acteurs des secteurs public et privé au Sénégal.

La Commission publie ainsi ledit avis trimestriel conformément à l'article 43 de son Règlement intérieur et après en avoir délibéré en sa séance plénière du 10 juillet 2015.

1 – Compte rendu des activités :
Au cours de ce deuxième trimestre 2015, la CDP a constaté une meilleure prise de conscience des responsables de traitement. En effet, 38 structures se sont rapprochées de l'Autorité de protection afin de mieux s'imprégner de la législation et de connaitre leurs obligations déclaratives.
La Commission a traité 134 dossiers dont 89 déclarations et 45 demandes d'autorisation. A l'issue des 06 sessions plénières, les commissaires ont délivré 54 récépissés de déclaration et 28 autorisations.
Au titre des signalements et des plaintes, la CDP a enregistré l'usage illégitime de numéros courts, une arnaque sur le réseau d'un opérateur de télécommunications, la collecte non autorisée d'empreintes digitales dans un système financier décentralisé, la diffusion de fausses nouvelles, l'arnaque et le chantage sur le net, l'utilisation abusive et sans autorisation de photos et la publication dans la presse de données personnelles d'employés sans leur consentement. Ces cas d'atteinte à la vie privée ont donné lieu à des demandes d'explication qui ont abouti à des déclarations et régularisations devant la CDP. Par ailleurs, la CDP a prononcé un (01) avertissement à l'endroit d'une structure pour envoi répété de courriels et de SMS non sollicités sans mise à disposition d'une possibilité de désabonnement fonctionnel.
Dans le cadre de sa mission de sensibilisation, la Commission a initié des visites de courtoisie auprès d'acteurs institutionnels. C'est ainsi qu'elle a été reçue par la Cellule Nationale de Traitement des Informations Financières(CENTIF), l'Agence nationale de la Banque Centrale des Etats de l'Afrique de l'Ouest(BCEAO), l'Office national de Lutte contre la Fraude et la Corruption(OFNAC) et en fin le Conseil Economique Social et Environnemental(CESE). De même, la phase pilote de la campagne de sensibilisation ''Internet, c'est moi qui décide'' a été lancée en partenariat avec la société Computech Groupe au sein d'établissements secondaires de Dakar.
Enfin, la CDP a organisé un Forum africain sur la protection des données personnelles (FAPDP 2015) à Dakar les 19 et 20 mai 2015. Cet évènement a enregistré la participation de plus de 350 personnes dont des autorités de protection de 13 pays africains (33 délégués), le Conseil de l'Europe et l'Association francophone des autorités de protection des données personnelles (AFAPDP).

2 – Observations /constats :
A l'examen des dossiers reçus à la CDP, des manquements ont été relevés dans le traitement des données personnelles de quelques structures.

Du point de vue juridique, on note :
• l'installation dans un lieu de travail d'un nombre disproportionné de caméras de surveillance;
• le non-respect des conditions de la prospection directe notamment, les droits des personnes concernées (consentement, opposition, etc.) ;
• le non accomplissement des formalités déclaratives devant la CDP préalables au traitement des données ;
• la durée illimitée de conservation des données traitées ;
• l'absence d'engagement de confidentialité entre le responsable de traitement et son sous-traitant.

Sur le plan technique, la pratique de l'externalisation reste une préoccupation pour la Commission. Cette situation constitue un défi supplémentaire pour la protection des données en ce sens que le responsable de traitement n'a plus le total contrôle de son système d'information.

Concernant le traitement des données sensibles comme les données de santé et la biométrie, les responsables de traitement devraient mettre une authentification forte au lieu de recourir simplement à un login et un mot de passe.

Enfin, il a été relevé dans certaines structures, l'absence de politique formalisée d'accès aux données et de mécanismes de sensibilisation des usagers sur les mesures de sécurité mises en place. Il est important que de telles dispositions soient prises par le responsable de traitement conformément à l'article 71 de la loi n° 2008-12 du 25 janvier 2008 portant sur les données à caractère personnel et la délibération n°2014–014/CDP du 3 avril 2014 portant sur les mesures de sécurité applicables aux traitements des données à caractère personnel.

3 – Recommandations :
Au regard des constats à l'examen des dossiers instruits, la CDP formule au profit de toutes les parties prenantes, les responsables de traitement du secteur public, du secteur privé, des organismes de la société civile et autres acteurs, les recommandations suivantes :

• Préciser le lieu exact (ville ou pays) de stockage du serveur contenant les données selon qu'il appartient à la structure ou à l'hébergeur (serveur mutualisé, serveur dédié);
• Signer obligatoirement un engagement de confidentialité en cas d'intervention d'un tiers dans le système mis en place afin d'augmenter le niveau de sécurité des données;
• Utiliser un langage codé et accessible uniquement au corps médical pour les dossiers de santé et mettre en place une authentification forte dans le cadre de la collecte de données de santé;
• Informer les personnes concernées de la présence de caméras de vidéosurveillance (affiches avec indication du numéro du récépissé de la CDP, panneau de signalement) et veiller à positionner les caméras uniquement sur les parties communes et s'assurer que les parties privées ne soient pas filmées;
• Désinscrire gratuitement et systématiquement, dans le cadre de la prospection commerciale, les personnes qui en font la demande avec effet immédiat;
• Veiller à assurer une protection des données transférées dans des serveurs à l'étranger en mettant en place des mécanismes de sauvegarde et de réplication/duplication;
• Recueillir le consentement, libre et éclairé des personnes qui font l'objet de prospection, tout comme le consentement des personnes concernées avant toute publication ou communication à des tiers de leurs données personnelles (photos, vidéos, etc.);
• Ne pas publier dans la presse des décisions individuelles mettant en cause les employés/salariés sans leur consentement;
• Saisir la CDP pour la suppression de tout contenu pouvant nuire à la réputation des personnes;
• Etre prudent sur les informations à communiquer sur les réseaux sociaux;
• Se rapprocher de la CDP pour une meilleure connaissance de la législation sénégalaise sur la protection des données personnelles.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

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

Source : http://www.actusen.com/avis-trimestriel-n-02-2015-de-la-commission-de-protection-des-donnees-personnelles-du-senegal-cdp/#

Cybercriminalité : 80 interpellations enregistrées au premier trimestre 2015 en Côte d'Ivoire – Abidjan.net | Le Net Expert Informatique

Cybercriminalité : 80 interpellations enregistrées au premier trimestre 2015 en Côte d'Ivoire

Quatre-vingts personnes soupçonnées de cybercriminalité ont été interpellés au premier trimestre 2015 en Côte d'Ivoire, avec 480 affaires traitées contre 450 affaires traitées et 70 interpellations 2014 dans le pays, a appris l'AIP auprès du directeur de la direction de l'informatique et des traces technologiques (DITT), le commandant Ouattara Guelpetchin.

Le directeur de la DITT, qui a fait cette annonce vendredi à Yamoussoukro, lors d'un colloque international sur la cybercriminalité, a indiqué par ailleurs que 90 % des infractions recensées au monde sont des infractions classiques avec usage des technologies de l'information et de la communication (TIC).

» En 2013, 85% de ces infractions sont commis depuis l'Afrique « , a précisé le commandant Ouattara Guelpetchin.
Initié par l'institut de lutte contre la criminalité économique (ILCE) de la haute école de gestion Arc (HEG Arc) et l'Ecole supérieure de commerce et d'administration des entreprises (ESCAE) de l'institut national polytechnique Houphouët-Boigny de Yamoussoukro, le colloque international a pour thème » l'impact de la cybercriminalité sur la société Ouest-africaine : exemple de la Côte d'Ivoire « .
Les infractions qualifiées « délinquance astucieuse » sur internet ont un impact au plan culturel, social et sur les investissements étrangers. « On évalue le préjudice subi à 1,5 milliards F CFA », a confié lors de sa communication l'étudiant Koné Aboubacar Sidiki de l'INP-HB dans le cadre de ses travaux de recherche .
Le colloque international sur la cybercriminalité, deuxième du genre, rassemble des experts du domaine en provenance de Suisse et de la Côte d'Ivoire, ainsi que les représentants des institutions publiques, des entreprises privées et des établissements d'enseignement supérieur, la presse et société civile.

Source : http://news.abidjan.net/h/559340.html

Menacé de chantage sur Skype, un lycéen se suicide| Le Net Expert Informatique

Menacé de chantage sur Skype, un lycéen se suicide

Après avoir été menacé par son interlocutrice virtuelle de voir une « vidéo intime » diffusée sur Internet s'il refusait de la payer, un jeune homme s'est donné la mort dans sa chambre.

Mercredi 4 juin, un peu avant 20 heures, à Castelsarrasin (Tarn-et-Garonne), un lycéen de 18 ans – qui s'appellerait Quentin – est attendu à la table familiale pour dîner. En l'absence de réponse à leurs appels, ses parents se rendent dans sa chambre. Et le découvrent dans une mare de sang, un couteau planté en plein coeur.
Quentin est déclaré mort peu après l'arrivée des secours. Les policiers qui leur font suite se concentrent sur son ordinateur portable, resté allumé. Ils y découvrent les causes probables de son suicide grâce à la fenêtre de conversation restée ouverte sur sa messagerie vidéo Skype : un chantage à la webcam.

Une jeune femme le menace de diffuser une vidéo intime
Les enquêteurs remontent le fil de la discussion et constatent que Quentin s'était filmé nu pour son interlocutrice. Celle-ci l'avait ensuite menacé de diffuser cet enregistrement sur internet s'il refusait de payer une certaine somme d'argent sur le champ. Pris de panique, Quentin se serait donné la mort pour éviter un scandale.
Le parquet de Montauban a ouvert une enquête préliminaire.
« La Dépêche du midi », qui avait d'abord évoqué l'hypothèse d'un chagrin d'amour avant de retenir celle du chantage, précise que la mère du lycéen l'aurait découvert avec une « corde au cou ». Mais évoque également, comme RTL, une « mare de sang ».
Le jeune homme, décrit comme un « très bon élève » de terminale au lycée professionnel de Beaumont-de-Lomagne, n'avait jamais parlé de suicide à ses proches. Les centres d'intérêt de son probable profil Facebook tournaient essentiellement autour des mangas.

Un scénario similaire à Brest, en 2012
Ce suicide rappelle un drame similaire survenu à Brest en octobre 2012. Un jeune homme de 18 ans s'était dénudé par webcam, sur Facebook, à la demande d'une jeune femme rencontrée en ligne qui faisait de même. Avant d'interrompre le « jeu » au bout de 10 minutes en le menaçant : « J'ai une vidéo porno de toi, si tu ne me donnes pas 200 euros, je vais détruire ta vie. »
Paniqué à l'idée de voir la vidéo diffusée à ses amis Facebook, le lycéen s'était pendu après avoir laissé un SMS d'adieu à ses parents. L'adresse IP de la femme provenait de Côte d'Ivoire, où des maîtres chanteurs connus sous le nom de « brouteurs » sont devenus des professionnels de ce genre de pratique.

Source : http://tempsreel.nouvelobs.com/faits-divers/20150605.OBS0251/menace-de-chantage-sur-skype-un-lyceen-se-suicide.html
Par Alexis Orsini

Exclusif : 47 grandes entreprises françaises ciblées par une tentative d’escroquerie à grande échelle | Le Net Expert Informatique

	47 grandes entreprises françaises ciblées par une tentative d’escroquerie à grande échelle

Selon nos informations, une cinquantaine de grandes entreprises sont actuellement – ou ont été au cours des derniers jours – la cible d'un réseau criminel spécialisé dans l'escroquerie aux faux ordres de virement (FOVI), encore appelée « Arnaque au président ». La technique n'est pas nouvelle. Ce qui interpelle, dans le cas présent, c'est l'ampleur de l'offensive mise à jour.

« L'arnaque au président » n'est pas vraiment d'un genre nouveau. D'ailleurs son pionnier, Gilbert Chikli, poursuivi par 33 banques et aujourd'hui réfugié en Israël, vient d'être condamné par contumace à 7 ans de prison et à 1 millions d'euros d'amende.

En cause : des escroqueries jugées « hors-norme », dont l'essaimage est devenu en quelques mois la bête noire des grandes directions financières, à commencer par celles que l'on pensait être les plus aguerries. Ainsi en 2012, c'est KPMG qui en a fait les frais : le géant mondial de l'audit et du conseil en fiscalité a laissé s'envoler à son insu pas moins de 7,6 millions d'euros.

Ces tentatives d'escroquerie n'épargnent personne : pas plus Michelin ou le Palais de l'Elysée, que nos PME régionales. Si Gilbert Chikli promet aujourd'hui avoir tiré sa révérence, il n'est en revanche pas improbable qu'il ait, directement ou non, inspiré quelques disciples.

47 entreprises sous la menace imminente de la criminalité financière

C'est une longue liste de cibles que s'est procuré la rédaction du JDE, par l'intermédiaire d'un cabinet privé spécialisé dans l'investigation et la lutte anti-fraude. Pour des raisons évidentes de sécurité, les consultants qui nous ont transmis cette information préfèrent rester anonymes.

Ils témoignent : « la spécificité de cette affaire réside dans l'ampleur de l'attaque. A ce jour, nous ne pouvons confirmer son état de progression ou son éventuel aboutissement. Nous avons contacté chacune des entreprises ciblées pour tenter d'être mis en relation avec les directions générales ou financières afin de de les en avertir. Malheureusement, le personnel n'étant pas toujours sensibilisé à ce type de risque, certains de nos appels sont restés sans suite. »

Une situation qui n'étonne guère ces analystes rompus à la gestion des affaires réservées des dirigeants : «Malheureusement, ces escroqueries aboutissent la plupart du temps à cause de défaillances dans la sûreté et les procédures internes de l'entreprise. La formation des collaborateurs, la circulation intelligente de l'information et l'instauration de procédures de vérification restent les meilleurs remparts contre ces attaques. »

Parmi les entreprises ciblées ou déjà attaquées, recensées par les enquêteurs, on retrouve de grands noms de l'économie française, des groupes familiaux plus discrets, et des enseignes bien connues des Français. « Des attaques qui sont en préparation depuis fin avril », précisent nos interlocuteurs, qui nous livrent ci-après le nom des entreprises ou organismes concernés :

Direction Finance, Ludendo, Système U, Abbott, 3 Suisses, GE Capital, Sonepar, Joué Club, Monoprix, BHR Béton, La Redoute, Eurofactor, Sephora, Picard, Imerys, Groupe Flo, GSF, DB Apparel, Optic 2000, Marionnaud, Groupe Pigeon, Invacare, Franck Provost, Auchan, Continental Corporation, Pronatura, Finifac, Provalliance, Carrefour, Vivendi, Korian, Accor, Servair, Bricorama, SKF, SNEF, SNCF, Rexel, Ecolab, Soprasteria, Chausson Matériaux, Faurecia, Immochan, Eiffage, Clemessy.

Comment réagir en cas d'attaque ?

« Nous avons pris des mesures directes pour tenter d'endiguer la marge de manœuvre des 'assaillants' et prévenir le risque d'escroquerie, et travaillons en étroite relation avec nos partenaires depuis plus d'un mois, expliquent les analystes. Surtout, nous accompagnons nos clients dans la mise en place d'une procédure judiciaire à l'encontre des auteurs de la tentative d'escroquerie, en sachant pertinemment qu'elle sera longue et complexe. »

D'après le cabinet, en effet, les quelques traces électroniques analysées laissent apparaître un mode opératoire assez classique, probablement piloté depuis Israël ou un territoire voisin comme l'indiquent les paquets de données qui ont été analysés.

« Dans certains pays, les moyens de paiement prépayés sont très répandus et peu régulés, donc difficilement traçables. Ils peuvent être ensuite utilisés en France, pour acquérir de l'information légale sur les sociétés ou à l'étranger, pour recourir anonymement aux services d'une plateforme téléphonique ». Ce sont également ces cartes prépayées qui, en toute vraisemblance, auront permis aux escrocs de réserver des noms de domaine pour peaufiner leur déguisement électronique.

Un déguisement qui va, selon les experts, jusqu'à l'usurpation d'identité de personnes vivantes ou décédées : « Pour brouiller les pistes, ces brigands 2.0 utilisent vos adresses, numéros de téléphone, dates de naissance pour réserver des noms de domaine et procéder à certaines formalités en ligne. C'est probablement supposé divertir les enquêteurs », ironise l'un de nos experts.

Piqûre de rappel : le mode opératoire

Une opération couronnée de succès est une opération bien préparée. Les escrocs commencent par une phase de renseignement en « zone grise », en collectant un maximum d'informations sur leur cible. C'est ce qu'on appelle le « social engineering », dont le but est de recueillir suffisamment de données quant à l'environnement humain (personnes clés, numéros de téléphone, adresse email) et économique (contrats, fournisseurs, bilans, etc.) de l'entreprise.

C'est bien moins compliqué qu'il n'y paraît : munis d'une carte prépayée, il leur suffit de se rendre sur une base de données de type Infogreffe et de télécharger les documents les plus riches en information : derniers statuts et actes déposés, PV d'assemblées générales, ou comptes annuels par exemple. L'identification, sur les réseaux sociaux, des « personnes clés » dans l'organigramme de la cible permet parfois de se familiariser avec leurs futurs interlocuteurs.

Depuis une plateforme téléphonique située à l'étranger, mais avec un numéro français d'apparence, l'escroc appelle un directeur financier, un service comptable, ou tout individu ayant compétence à agir sur les comptes de l'entreprise.

Se faisant généralement passer pour le dirigeant de l'entreprise, il déploie alors des trésors de créativité et/ou de séduction. Tantôt flatteur, tantôt menaçant, il prétexte une situation d'urgence (opération boursière sensible, ou imminence d'un contrôle fiscal par exemple) et exige le virement immédiat d'une importante somme sur un compte habituellement hébergé en Chine.

Nos interlocuteurs invitent donc les entreprises à la plus grande vigilance : « ces offensives sont généralement fulgurantes et, le temps de réagir, nos escrocs sont déjà loin »…

Source : http://www.journaldeleconomie.fr/Exclusif-47-grandes-entreprises-francaises-ciblees-par-une-tentative-d-escroquerie-a-grande-echelle_a2456.html

Un réseau de fraude de clés de connexion Internet démantelé | Le Net Expert Informatique

Un réseau de fraude de clés de connexion Internet démantelé

La brigade ville de la gendarmerie de Bogodogo vient de mettre hors d'état de nuire un réseau qui disposerait de clés de connexion internet de l'ONATEL SA à navigation illimitée.

La cybercriminalité est en pleine expansion au Burkina Faso. Face à ce fléau, le commandement de la Gendarmerie a décidé de lancer une opération d'envergure.
C'est ainsi que la Brigade ville de Bogodogo découvre par une source digne de foi, un réseau de vendeurs de clés de connexion de l'ONATEL SA sur le marché noir, selon le Colonel Sam Djiguiba Ouédraogo, Commandant du groupement départemental de la Gendarmerie de Ouagadougou.
Une enquête ouverte à cet effet a permis de mettre la main sur un auteur principal et trois complices.

La gendarmerie invite la population à la vigilance
Technicien d'exploitation et de maintenance à l'ONATEL SA, l'auteur de la fraude profite de son accès à la base technique pour activer des clés de connexions internet déjà résiliées ou suspendues pour en faire des clés de connexion à navigation illimitée.
Il les met ensuite sur le marché noir par l'intermédiaire de ses complices à des prix variant de 50 000 F CFA à 250 000 F CFA, soutient le commandant de la gendarmerie.
Une fois de plus, la gendarmerie invite la population à la vigilance et à signaler aux forces de sécurité toutes activités suspectes.

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

Source : http://burkina24.com/2015/06/24/cybercriminalite-un-reseau-de-fraude-de-cles-de-connexion-internet-demantele/
Par Serge Balma (stagiaire)

Alerte: Nouveaux courriels de phishing au nom d'Apple (iTunes) | Le Net Expert

Informatique

	Alerte: Nouveaux courriels de phishing au nom d'Apple (iTunes)

Des fraudeurs envoient des courriels au nom d'Apple (iTunes) afin de s'emparer des données d'accès à votre compte.
Par ces courriels, les destinataires sont informés que leur compte n'a pas pu être validé et que celui-ci a été bloqué. Les escrocs demandent de suivre un lien et de fournir des données personnelles (nom d'utilisateur et mot de passe) sous prétexte de pouvoir réactiver leur compte.

Le SCOCI conseille :
1. Effacez le courriel !
2. Si vous soupçonnez quelqu'un d'être en possession de vos données d'accès à votre compte, veuillez immédiatement prendre contact avec le support d'Apple.
3. Soyez prudents avec tous les courriels qui vous demandent de cliquer sur un lien Internet pour contrôler vos données personnelles. En règle générale, ceci est l'œuvre de fraudeurs.
4. Contrôlez toujours l'adresse Internet (URL) sur laquelle vous êtes redirigés (cf. rectangle rouge sur l'image). De manière générale, si vous devez vous connecter à un compte en ligne, inscrivez l'URL vous même dans votre navigateur plutôt que de cliquer sur un lien qui vous est transmis par courriel.
5. Signalez ces cas au SCOCI par le biais de son formulaire d'annonce en ligne afin que nous puissions analyser ces courriels et faire fermer au plus vite les sites frauduleux.

En cas de doute sur une usurpation d'identité ou de doute sur une arnaque, n'hésitez pas à contacter Denis JACOPINI expert informatique assermenté.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

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

Source : https://www.cybercrime.admin.ch/kobik/fr/home/warnmeldungen/2015/2015-05-15.html

---

Les «usines à clics» tournent

à plein régime aux Philippines | Le Net Expert Informatique

Les «usines à clics» tournent à plein régime aux Philippines

Les « usines à clics » aux Philippines produisent en masse de faux comptes pour les réseaux sociaux. De nombreuses célébrités, des personnalités politiques, de grandes entreprises et même de simples internautes en manque de fans, usent et abusent de cette contrefaçon numérique afin accroître leur popularité sur la Toile.

Un journaliste du magazine en ligne New Republic a enquêté aux Philippines sur les « usines à clics », ces fabriques singulières qui créent à la chaîne de faux comptes « clef en main » et inondent les réseaux sociaux de recommandations bidons, de « j'aime » chimériques, de fans fictifs et de suiveurs imaginaires.

Le prix d'un faux profil n'excède pas 1€50, et n'importe quel internaute ou de grandes entreprises peuvent ainsi, en

quelques clics, gonfler artificiellement leur visibilité sur la Toile. Une activité frauduleuse en plein essor qui s'appuie sur un réseau d'intermédiaires peu scrupuleux, comme le démontrait récemment le magazine Envoyé Spécial sur France Télévisions, qui a surpris une start-up française spécialisée dans la revente d'abonnés virtuels, en pleine transaction.

Selon les conditions d'utilisation des réseaux sociaux, le commerce de faux profils en ligne est formellement interdit. Mais les autorités des Philippines considèrent que ces règlements n'ont aucune valeur juridique sur leur territoire. Pour elles, c'est donc un négoce illicite mais pas illégal.

Un fléau pour les géants d'Internet

Ce marché noir de la « web réputation » menace maintenant l'économie numérique mondiale, il serait nuisible aux activités des entreprises qui ont depuis longtemps investi dans les réseaux sociaux.

C'est un fléau, selon les géants du web, qui ne parviennent pas à endiguer le phénomène, particulièrement pour Facebook, Twitter et Google, dont les modèles économiques reposent exclusivement sur des offres publicitaires ciblées pour le commerce en ligne.

Les usines à clics fonctionnent comme de vraies entreprises, avec un personnel qualifié qui est composé principalement de jeunes informaticiens diplômés gagnant cinq fois le salaire d'une femme de ménage.

Les patrons, eux, profitent pleinement des infrastructures technologiques implantées dans le pays par de grandes compagnies américaines comme Microsoft. Un miracle économique

inattendu de la délocalisation, conclut ironiquement le journaliste de New Republic. Les « usines à clics » sont devenues en quelques années les principaux moteurs de la croissance aux Philippines.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous

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

Source : http://www.rfi.fr/asie-pacifique/20150506-philippines-usine-clics-commerce-fans-internet-reseaux-sociaux/?aef_campaign_date=2015-05-06&aef_campaign_ref=partage_user&ns_campaign=reseaux_sociaux&ns_linkname=editorial&ns_mchannel=social&ns_source=twitter