Enquête sur le piratage à La Poste du Sénégal: le DG auditionné par la Gendarmerie

Enquête sur le piratage à La Poste du Sénégal: le DG auditionné par la Gendarmerie

L'enquête sur le piratage de la plate-forme de transfert d'argent de la Poste se poursuit. Après avoir entendu plusieurs responsables de la boite, la section de recherches de Colobane (Dakar) a reçu hier dans ses locaux le directeur général, Ciré Dia. D'après le quotidien sénégalais L'Observateur qui donne l'information dans sa livraison du jour, un important arsenal technique a été mis à contribution pour remonter la filiale.

En s'introduisant dans le système de transfert international du réseau, les cybercriminels avaient emporté près de 400 millions de francs CFA. Un coup dur pour la société qui traverse actuellement des moments difficiles selon L'Enquête qui fait état de problèmes de recouvrement des montants dus par les sociétés de transfert d'argent au groupe, des montants estimés entre 4 et 5 milliards CFA.

Réagissez à cet article

Original de l'article mis en page : Enquête sur le piratage à La Poste du Sénégal: le DG auditionné par la Gendarmerie hier | CIO MAG

Cybersécurité et Cyberdéfense : leviers de l’intelligence économique

	La transition numérique en Afrique étroitement liée à l’intelligence économique

La numérisation de la société africaine s'accélère : la part du numérique dans les services, les produits, les métiers ne cesse de croître. Réussir la transition numérique est devenu un enjeu continental. Vecteur d'innovation et de croissance, la numérisation présente aussi des risques pour l'Etat, les acteurs économiques et les citoyens. La cybercriminalité, l'espionnage, la propagande, le sabotage ou l'exploitation excessive de données personnelles menacent la confiance et la sécurité dans le numérique et appellent une réponse collective.

Le second pilier de l'intelligence économique est par définition la sécurité du patrimoine immatériel. Composante indispensable au développement. Le problème est que ce patrimoine est de plus en plus numérisé en Afrique comme partout dans le monde. A cela il faut rajouter le fait que la technologie est injectée à forte dose dans les entreprises pour améliorer la croissance et la compétitivité. Il y va de même pour les Etats.
Dans ce contexte, l'utilisation, l'accès et l'exploitation de la technologie est en forte croissance. Ce qui a pour implication d'exposer les données stratégiques. Il faut alors disposer de mécanismes efficaces pour protéger ce patrimoine. « La cybersécurité est la prévention des risques de sécurité et de sûreté liés à l'emploi des technologies de l'information. Elle est à ce titre un volet de « l'intelligence des risques » elle-même composante de l'intelligence économique. » Bernard Besson.
De nouveaux crimes, risques, infractions et menaces sont apparus dans le cyberespace africain : utilisations criminelles d'internet (cybercriminalité), espionnage politique, économique et industrielle, attaques contre les infrastructures critiques de la finance, des transports, de l'énergie et des communications à des fins de spéculation, de sabotage et de terrorisme.
Émanant de groupes étatiques ou non-étatiques, les cyberattaques n'ont aucune contrainte de distances, de frontières et même d'espaces ; peuvent être complètement anonymes ; ne nécessitent plus de coûts et de moyens importants et peuvent présenter de très faibles risques pour l'attaquant…[lire la suite]

Denis Jacopini anime des **conférences et des formations** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Cybersécurité et Cyberdéfense : leviers de l'intelligence économique. »

Le FBI remonte une Cyberattaque jusqu’à Abidjan

Le FBI remonte une Cyberattaque jusqu’à Abidjan

La Banque centrale des Etats-Unis d'Amérique reçoit sur son système d'information (SI) un flux important de données provenant d'un réseau de machines inconnues. Lorsque les cyberdétectives du Bureau fédéral d'investigation (FBI) essaient de remonter jusqu'à l'origine de l'offensive, ils sont dirigés vers plusieurs continents, via des serveurs informatiques qui interagissent entre eux. Autant de rebonds sur des machines, rendant la piste des attaquants difficile à suivre.

Toutefois, des empreintes laissées sur internet permettent aux agents du FBI de localiser des serveurs situés en Côte d'Ivoire. Signe de la gravité de la cyberattaque, les fins limiers du web américain débarquent à Abidjan.

Sur place, après une séance de travail avec l'équipe d'experts en sécurité informatique du**CI-CERT (Côte d'Ivoire – Computer emergency response team)**, le FBI parvient à identifier à partir d'une liste d'adresses IP, des entreprises ivoiriennes, dont les machines infectées, sont utilisées à leur insu par des hackers basés en Thaïlande, pour lancer des offensives contre le SI de la Banque centrale des Etats-Unis d'Amérique.

Ce n'est pas le scénario d'un film américain, mais une réelle attaque informatique qui s'est déroulée dans le premier trimestre de l'année 2013, et qui a été décrite à CIO Mag par Jean-Marie Nicaise Yapoga, chef de service du CI-CERT, alors responsable technique adjoint. Pointant la vulnérabilité des entreprises qui s'exposent à des risques dus au non-respect des bonnes pratiques en matière de cybersécurité (Cf. CIO Mag N°29 – décembre 2013/janvier 2014).

L'expertise du CERT ivoirien dans cette affaire a permis aux entreprises infiltrées de limiter les dégâts et de réduire le coût du retour à un fonctionnement normal. Mais elle rappelle surtout l'essentiel de sa mission : assurer, au niveau local, la fonction de point focal pour toutes les questions de cybersécurité.

Des couches de sécurité sans protection suffisante

Vu l'ampleur des menaces sur les fleurons de l'économie ivoirienne, un pan de la mission de sensibilisation du CI-CERT est toujours orientée vers les chefs d'entreprise. Moins réceptives à l'idée d'investir dans le recrutement d'un responsable de la sécurité des systèmes d'information (RSSI), nombre d'entreprises empilent en effet des couches de sécurité (pare-feu, anti-virus, etc.), qui n'offrent souvent pas de protection suffisante.

Une situation que le chef de service déplore dans la parution de CIO Mag susmentionnée : « C'est lorsqu'elles (ces entreprises) doivent faire face à des incidents informatiques qu'elles se rendent compte de l'importance de la cybersécurité. Malheureusement, entre l'alerte et le temps mis pour rétablir le réseau, l'entreprise peut avoir déjà perdu plusieurs millions de FCFA. »

Partenariat public/privé

Côte d'Ivoire – Computer emergency response team.

Aujourd'hui, le CI-CERT peut se vanter d'avoir favorisé le recrutement de RSSI dans des entreprises de télécommunications. « On en retrouve également au sein des banques et de plusieurs groupes d'entreprises », révélait l'analyste-administrateur de sécurité des SI.

Pour limiter les incidents informatiques, le CERT ivoirien organise des ateliers et séminaires de formation, notamment avec les directeurs de système d'information (DSI) et les RSSI. Objectif ? Créer un partenariat public/privé destiné à poser des actions de prévention. C'est-à-dire, diffuser des bulletins d'information et des avertissements, et établir un réseau d'information et d'alerte gouvernementale sur les attaques et les menaces.

Au cours de ces rencontres, les responsables informatiques et de cybersécurité sont briffés sur les menaces répertoriées sur le cyber espace national mais également sur les types d'attaques rapportées au CI-CERT par ses partenaires internationaux : IMPACT (Organisation internationale de lutte contre les cyber-menaces) et la communauté des CERT étrangers.

La nécessité de se doter d'un CERT

En Côte d'Ivoire, la nécessité de se doter d'un CERT (Computer incident response team) a été perçue dès 2009. Dans un contexte où l'image du pays était fortement écorchée sur le plan international du fait des nombreux cas de défacement de sites web gouvernementaux et de cyberescroquerie.

Hormis les pertes financières provoquées par ces actes de piratage avérés, d'autres conséquences majeures ont été enregistrées : « Adresse IP ivoiriennes mises sur des listes noires ; achats en ligne interdits avec IP des FAI ivoiriens sur les plateformes telles que PayPal et Yahoo », peut-on lire dans un document dont CIO Mag a reçu copie.

C'est donc pour faire face à la récurrence de ces incidents qui constituent une menace, à la fois sur l'économie et la notoriété du pays que le CI-CERT a vu le jour, en 2009. Depuis leurs bureaux situés à l'époque dans la commune du Plateau, en plein centre des affaires, cinq ingénieurs informaticiens se sont activés à écrire les premières pages du CI-CERT.

Sous tutelle de **l'Autorité de régulation des télécommunications/TIC de Côte d'Ivoire (ARTCI)**, leurs actions consistaient à lutter contre la cyberescroquerie et à émettre des alertes et annonces de sécurité.

Plus de 40 000 incidents traités au 1er semestre 2015

Aujourd'hui, cette structure joue pleinement son rôle de cyber pompier de l'Etat avec une quinzaine d'ingénieurs menant une série d'activités regroupées en deux axes:

• Protection du cyber espace national avec un portefeuille de services réactifs (alertes et avertissements, traitement d'incidents, coordination de traitement de vulnérabilité, etc.) et proactifs (annonces, veille technologique, détection d'intrusion, partage d'informations), ainsi qu'un service de management de la qualité de la sécurité orienté sur la sensibilisation, la formation et la consultance.

• Lutte contre la cybercriminalité dans le cadre de la Plateforme de lutte contre la cybercriminalité (PLCC) grâce à une convention de partenariat entre l'ARTCI et la Police nationale.

Au cours du premier semestre de 2015, le CI-CERT a collecté et traité 40 264 incidents de sécurité informatique, envoyé 145 bulletins et avis de sécurité et participé aux cyberdrill UIT- IMPACT et OIC-CERT, traduisant son leadership sur le cyber espace national.

Article original de CIO-Mag

Réagissez à cet article

Original de l’article mis en page : Cyberattaque : quand le FBI débarque à Abidjan | CIO MAG

« AITEX – AFRICA IT EXPO » : le Sénégal et la Côte d’Ivoire à l’honneur au Maroc, du 21 au 24 septembre 2016

« AITEX – AFRICA IT EXPO » : le Sénégal et la Côte d’Ivoire à l’honneur au Maroc, du 21 au 24 septembre 2016

Le Sénégal et la Côte d'Ivoire, qui compte parmi les pays d'Afrique subsaharienne à avoir engagé des projets de gouvernance électronique, seront à l'honneur au Maroc lors de la première édition du Salon de l'innovation et de la transformation digitale en Afrique, « AITEX – AFRICA IT EXPO », qui aura lieu du 21 au 24 septembre 2016 à Casablanca.

Dans un communiqué transmis à notre Rédaction, la **Fédération marocaine des technologies de l'information, des télécommunications et de l'Offshoring (APEBI),** chef d'orchestre de l'AFRICA IT EXPO, explique le choix du Sénégal et de la Côte d'Ivoire par le souci d'établir une connexion sud-sud des ressources du continent. Un défi majeur que le Royaume chérifien veut relever en commençant par ces deux pays qui sont la locomotive économique de la sous-région ouest-africaine. La Côte d'Ivoire connaît une forte croissance économique qui se situe entre 7 et 8 % par an. Une performance portée en partie par un secteur privé qui fait de la transformation numérique, un vecteur de compétitivité. Le Sénégal, deuxième économie de l'Afrique de l'Ouest francophone derrière la Côte d'Ivoire, est plébiscitée pour les efforts fournis dans le domaine du digital. Là où l'Afrique a atteint un taux de pénétration moyen autour de 100%, le Sénégal lui signe un taux de 113,66% en mars 2016. En choisissant ces deux pays, le Maroc veut leur apporter son « soutien pour conforter leur leadership régional et aussi pour accélérer leur transformation numérique ».

Le communiqué :
« Salon des Technologies de l'Information « AITEX – AFRICA IT EXPO » – 21 – 24 septembre 2016 à Casablanca
Le 1er salon de l'innovation et de la transformation digitale du continent met à l'honneur le Sénégal et la Côte d'Ivoire

La Fédération marocaine des technologies, de l'information, des télécommunications et de l'Offshoring (APEBI) organise la 1ère édition du Salon des Technologies de l'Information « AITEX – AFRICA IT EXPO », qui aura lieu du 21 au 24 septembre 2016 à la foire internationale de Casablanca. « AITEX – AFRICA IT EXPO » est la première plateforme de l'innovation et de la transformation digitale en Afrique, qui va réunir 150 exposants – tous issus des entreprises référencées dans le domaine -, 200 donneurs d'ordre, mais aussi des experts et des utilisateurs venus d'Afrique, du Moyen Orient et d'Europe. Pour cette édition, l'APEBI met à l'honneur le Sénégal et la Côte d'Ivoire, deux pays amis avec lesquels le Royaume entretient des relations de longue date, qui constituent un modèle de coopération exemplaire, et qui jouent par ailleurs un rôle de locomotive en Afrique de l'Ouest dans le domaine des TIC.

Aujourd'hui, la transformation digitale est devenue un enjeu majeur pour les sociétés, une mutation indispensable pour les entreprises et l'économie. A l'ère du numérique, cette transformation constitue un avantage fort pour nos sociétés, qui crée de la valeur… L'évolution très rapide des TIC -Technologies de l'Information et de la Communication- a profondément façonné le changement de nos modes de vie. Face à la généralisation des TIC dans les pays industrialisés, l'intégration de ces compétences (mais surtout leur maîtrise et leur exploitation) est un enjeu stratégique, sociétal, culturel et technologique en Afrique.
Le continent, qui poursuit son processus de mondialisation et sa dynamique d'émergence doit se « mettre à niveau » pour améliorer l'efficience de son économie et « booster » sa compétitivité locale et internationale. Grâce à une approche bien encadrée, qui va intégrer tous les paramètres, les enjeux et aussi les risques induits, la transformation digitale est sans conteste un levier de croissance économique et de compétitivité, créateur de valeur ajoutée.
La Fédération marocaine des technologies, de l'information, des télécommunications et de l'Offshoring (APEBI), est un acteur régional stratégique en Afrique car elle regroupe des entreprises qui jouent un rôle clé dans l'économie et qui sont des références dans leur domaine.
Pendant trois jours, l'APEBI va être le catalyseur d'une dynamique nouvelle, qui va accélérer le développement du numérique dans le continent.

AITEX – AFRICA IT EXPO : Première plateforme de l'innovation et de la transformation digitale d'Afrique
Cette édition sera marquée par une forte présence d'experts de haut niveau, des opérateurs nationaux et internationaux reconnus, tous réunis autour d'un programme ambitieux qui a pour vocation d'être la première plateforme de l'innovation et de la transformation digitale en Afrique.
Organisé avec le soutien institutionnel de Maroc Export, le salon « AITEX – AFRICA IT EXPO » va accueillir principalement des distributeurs, des fournisseurs de technologie, des intégrateurs de solutions, éditeurs, opérateurs télécoms, ISP, ASP, délocalisation de fonctions de gestion, TMA, help desk conseil, offshoring, mobility, big data, Cloud, réseaux, e-Commerce… Vitrine de l'offre numérique et des dernières évolutions digitales, « AITEX – AFRICA IT EXPO » est une *plateforme* unique de rencontres, d'échanges et d'opportunités d'affaires.
Véritable révélateur des nouvelles tendances, le Salon «AITEX – AFRICA IT EXPO » est une occasion unique de rencontrer et d'échanger sur les problématiques quotidiennes des entrepreneurs, collectivités et de trouver les réponses appropriées grâce au concours de spécialistes, eux-mêmes engagés dans les processus de développement des économies émergentes et de la coopération sud-sud.
Placé sous le thème, «Transformation Digitale : Levier de développement en Afrique», le salon offre une nouvelle occasion de conscientiser et sensibiliser nos sociétés sur la formidable opportunité offerte par les technologies numériques pour accélérer le développement du continent. Des rencontres sont organisées au cours de ces trois journées pour débattre des problématiques actuelles et des enjeux sociétaux de ces mutations afin d'adopter les meilleures pratiques et ainsi anticiper les défis auxquels les entreprises et économies africaines sont confrontées. «AITEX – AFRICA IT EXPO » va promouvoir les relations d'affaires et la mise en réseau des différents acteurs économiques du continent, à travers des coopérations sud-sud, nord-sud et public-privé.

Le Sénégal et la Côte d'Ivoire à l'honneur
Le défi numérique en Afrique passe inéluctablement par la connexion des ressources du continent. Un aspect *que l'APEBI a compris et intégré dans l'organisation de ce salon, c'est pourquoi la fédération a décidé de mettre à l'honneur, pour sa première édition, le Sénégal et la Côte d'Ivoire.* Ces deux pays, représentant deux premières puissances économiques de l'Afrique de l'ouest francophone engagés dans une dynamique de croissance depuis plusieurs années, ont à cœur de poursuivent respectivement leurs ambitions numériques.
La Côte d'Ivoire connaît une forte croissance économique qui se situe entre 7 et 8 % par an et le développement du numérique est devenu un enjeu majeur, créateur de richesses. Le numérique constitue un potentiel énorme, présent dans tous les esprits, aussi bien du côté du gouvernement que des dirigeants d'entreprise. Selon une étude publiée par le cabinet Deloitte en mai 2016, seulement 36 % des entreprises estiment avoir atteint la maturité numérique.
Le Sénégal, quatrième économie de la sous-région ouest africaine après le Nigéria, la Côte d'Ivoire et le Ghana, et deuxième économie en Afrique de l'Ouest francophone derrière la Côte d'Ivoire s'est largement distingué dans l'évolution de l'économie numérique, premier levier de la transformation digitale. Là où l'Afrique a atteint un taux de pénétration moyen autour de 100%, le Sénégal lui signe un taux de 113,66% en mars 2016.
Le *Sénégal et la Côte d'Ivoire font partie des premiers pays africains à initier des* projets de gouvernance électronique (e-Gouv). Ils ont réalisé au fil des années des progrès importants dans les domaines tels l'économie numérique, la monétique, le courrier hybride, ou encore le taux de connectivité internet, etc.) Néanmoins, les disparités qui existent entre les différents pays du continent peuvent être réduites si un effort de coopération est accompli.
En mettant en avant ces deux pays amis, qui constituent un modèle important d'exemplarité sur le continent africain (et en particulier de ses voisins ouest-africains), le Maroc apporte son soutien pour conforter leur leadership régional et aussi pour accélérer leur transformation numérique. »
Article original de Cio-Mag

Réagissez à cet article

Original de l'article mis en page : « AITEX – AFRICA IT EXPO » : le Sénégal et la Côte d'Ivoire à l'honneur au Maroc, du 21 au 24 septembre 2016 | CIO MAG

L'arnaqueur Chinaper Chinapa roi de l'escroquerie sur Internet enfin arrêté

L'arnaqueur Chinaper Chinapa roi de l'escroquerie sur Internet enfin arrêté

Il se nomme Chinaper Chinapa, un arnaqueur de Côte d'Ivoire qui vient d'être arrêté. Il arnaquait des hommes et des femmes sur Internet.

Les scammeurs, les brouteurs, bref les escrocs qui s'attaquent aux internautes sont légions sur la toile. Ils usent de multiples arnaques pour soutirer de l'argent à leurs victimes. Ils jouent ensuite les « rois » dans leur quartier. Parmi les pièges usités : l'arnaque à l'amour, le wash-wash, la création de billets, le faux mail d'inquiétude d'un proche perdu, la fausse location ou loterie… Pour Chinaper Chinapa, chaussures et portes feuilles magiques en bonus ! Je possède une liste d'une quarantaine d'arnaques possibles mises en place par les brouteurs.

Chinaper Chinapa le chenapant !

L'un des « rois » des brouteurs se nommait Chinape Chinapa. L'amateur de casquettes et baskets « bling-bling » se faisait passer pour un « magicien ». Il affirmait être capable de faire sortir des billets de chaussures, de boite magique. Il avait aussi mis en place des arnaques amoureuses, se faisant passer pour des hommes et des femmes à la recherche de l'âme sœur. Il volait les photos sur Facebook et « chassait », ensuite, sur des sites de rencontres.

J'ai pu croiser cet escroc de Chinaper Chinapa, il y a quelques mois, dans son pays (il se baladait aussi beaucoup au Bénin). Ce « roi » des boites de nuit qui sortait les billets de banque plus vite que 007 son Walther PPK.

Mi juin 2016, l'homme avait été tabassé par des personnes qu'il avait escroquées. Quinze jours plus tard, la police lui mettait la main dessus pour une série d'escroqueries. Arrêté par la police début juillet, détail confirmé par le journal Koaci. Le flambeur s'est retrouvé les menottes aux poignets dans son appartement de Cocody. Il est accusé d'activités cybercriminelles et de multiples escroqueries. Pas évident que sa « magie » fonctionne dans la prison d'Abidjan.

Un ami a besoin de vous

15h, un courrier signé d'un de vos amis arrive dans votre boîte mail. Pas de doute, il s'agit bien de lui. C'est son adresse électronique. Sauf que derrière ce message, il y a de forte chance qu'un brouteur a pris la main sur son webmail. Les courriels « piégés » arrivent toujours avec ce type de contenu « ***Je ne veux pas t'importuner. Tu vas bien j'espère, puis-je te demander un service ?***« . Le brouteur, par ce message, accroche sa cible. En cas de réponse de votre part, l'interlocuteur vous sortira plusieurs possibilités liées à sa missive « ***J'ai perdu ma carte bancaire. Je suis coincé en Afrique, peux-tu m'envoyer de l'argent que je te rembourserai à mon retour*** » ; « ***Je voudrais urgemment recharger ma carte afin de pouvoir régler mes frais de déplacement et assurer mon retour. J'aimerais s'il te plaît, que tu me viennes en aide en m'achetant juste 4 coupons de rechargement PCS MASTER CARD de 250 € puis transmets moi les codes RECH de chaque coupon de rechargement, je te rembourserais dès mon retour***« . Je possède plus d'une centaine de variantes d'excuses.

Bien entendu, ne répondez pas, ne versez encore moins d'argent. Attention, selon les brouteurs, des recherches poussées sur leurs victimes peuvent être mises en place. J'ai dernièrement traité le cas d'un brouteur qui connaissait le lieu de résidence du propriétaire du compte webmail que le voyou utilisait. De quoi faire baisser les craintes des amis contactés.

A noter que le scammeur indiquera toujours un besoin de confidentialité dans sa demande : « ***Je souhaite également que tu gardes ce mail pour toi uniquement. Je ne veux pas inquiéter mon entourage. Y'a t'il un buraliste ou un supermarché non loin de toi ?***« .

Remboursement de l'argent volé

Une autre arnaque de brouteurs est intéressante à expliquer. Elle est baptisée « *remboursement*« . Le voleur écrit aux internautes se plaignant, dans les forums par exemple, d'avoir été escroqués. L'idée de l'arnaque est simple : le voleur indique qu'il a été remboursé grâce à un policier spécialisé dans les brouteurs. Le voyou fournit alors une adresse électronique.

Suivre

ZATAZ.COM Officiel @zataz

Prudence à l'adresse « interpol.police.antiarnaque@gmail(.)com » qui n'est pas celle d' #interpol ! L'escroc cherche des personnes escroquées.

23:12 – 14 Mai 2015

•

•

1111 Retweets

•

55 j'aime

Derrière cette fausse adresse de policier, un autre brouteur. Il va tenter d'escroquer le pigeon déjà pigeonné. Sa mission, se faire envoyer de l'argent via Western Union, MoneyGram. Certains brouteurs sont à la solde de petits commandants locaux qui imposent un quota d'argent à collecter. En 2013, la cyber police de Côté d'Ivoire estimait que les brouteurs avaient pu voler pas moins de 21 millions d'euros. N'hésitez pas à me contacter si vous avez croisé la route d'arnaques.

Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : ZATAZ Brouteur : Chinaper Chinapa roi de l’escroquerie 2.0 – ZATAZ

Le Bénin, capitale de la cyber-arnaque en Afrique de l’Ouest

Au Bénin, les cybercriminels sont habituellement connus sous le nom de « Gaymans. » Les premières méthodes d'escroquerie concernaient les réseaux de jeunes se faisant passer pour des homosexuels, pour appâter des personnes de la même orientation sexuelle dans les pays occidentaux, d'où le nom de « Gayman » donné à la plupart des cybercriminels opérant à partir du Bénin.

Le phénomène fait son apparition dans les années 2000 et se caractérise essentiellement par des arnaques en ligne par des individus sans connaissance particulière en informatique, mais avec de solides atouts en psychologie.

Pour Nicaise Dangnibo, le directeur de l''Office central de répression de la cybercriminalité (OCRC), une unité spéciale de la police béninoise, « le phénomène a pris ses racines à partir du Nigeria, l'un des tout premiers pays d'Afrique de l'Ouest confrontés au phénomène de la cybercriminalité. »

Avec les premières mesures de rétorsion mises en place par les autorités nigérianes, les cybercriminels se sont massivement délocalisés au Bénin et en Côte d'Ivoire.

Ces derniers copiaient sur Internet des photos de jeunes hommes « beaux et musclés » à la recherche de l'âme soeur.

Les méthodes d'escroquerie se sont ensuite diversifiées, pour s'étendre au love chat, au porno-chantage, puis à des montages complexes de fausses affaires.

"Internet a certes révolutionné le monde au point qu'il serait difficile d'imaginer un autre monde sans internet ; mais, autant les coupeurs de routes existent et pourtant nous circulons sur nos routes, autant les flibustiers existent et pourtant nous naviguons sur les eaux ; autant les cybercriminels existeront toujours et nous allons toujours surfer sur le net."
Pierre Dovonou Lokossou
Gestionnaire de projets technologiques

Selon Pierre Dovonou Lokossou, gestionnaire de projets technologiques, « la première arnaque via l'Internet au Bénin a eu lieu deux ans après l'arrivée du web dans le pays. Il s'agissait d'un Nigérian se prénommant Christopher qui avait escroqué un pasteur américain (Jim), en se faisant livrer 40 ordinateurs, 10 imprimantes et un millier de bibles, en échange d'un chèque délivré par une banque fictive ».

Pierre Dovonou Lokossou raconte qu'à cette époque, « la plupart des mails indésirables (spams) provenant du Bénin étaient en anglais. La répression des actes de cybercriminalité au Nigéria avait vite fait de déverser au Bénin et dans la sous-région de jeunes Nigérians qui pouvaient désormais poursuivre en toute impunité leurs sales besognes… »

« Par la suite, ajoute-t-il, de l'anglais, les spams ont commencé à être rédigés dans un français approximatif, signe qu'avec le séjour de ces cybercriminels anglophones au Bénin, l'apprentissage de la langue française a été mis à contribution. »

Mais actuellement, à en croire le gestionnaire de projets, « le phénomène a pris de l'ampleur dans toute la sous-région ouest-africaine ». « Aussi bien des Béninois que des Togolais et des Burkinabè, des Nigériens et des Ivoiriens s'adonnent à cœur joie à ce cyber-banditisme », précise-t-il.

Offres de vente

Il s'agit le plus souvent de propositions de prêts, voire de dons ou d'offres de vente assez diversifiées diffusées sur des sites internet, ou parfois envoyées sous forme de spams aux internautes.

Les offres de vente vont des appareils électroménagers aux métaux précieux en passant par les téléphones portables, les ordinateurs, les véhicules, voire les animaux ou les domaines fonciers.

Une étudiante en Relations internationales, Adidjath Kitoyi, raconte avoir été contactée en 2012 sur le réseau social Facebook par « une Suissesse âgée de 83 ans atteinte d'un cancer au stade très avancé » qui souhaitait lui céder « une fortune héritée de ses parents et qui se trouve dans les coffres d'une banque à Genève ».

Appâtée, Adidjath s'était empressée d'envoyer à une adresse indiquée (qui se révèlera inexistante) tous les documents administratifs réclamés par son interlocuteur avant d'effectuer à l'attention d'un « intermédiaire » basé en Côte d'Ivoire un transfert de 150 000 FCFA représentant « les frais de dossiers ».

Par la suite, il ne lui était plus possible de communiquer avec la Suissesse donatrice, ni avec l'intermédiaire en Côte d'Ivoire.

La mésaventure d'Adidjath Kitoyi n'est qu'un cas parmi des centaines, voire des milliers d'autres victimes des cybercriminels.

Pierre Dovonou Lokossou distingue trois catégories de cybercriminels.

« La première est celle de ces jeunes qui n'ont pas un emploi légal connu et qui ne fréquentent que les cybercentres ou qui sont toujours avec leur ordinateur portatif et qui ont un train de vie largement au-dessus de la moyenne. Ils changent souvent de motos ou de voitures. Ils peuvent disparaître du quartier pendant des mois et réapparaître pour faire croire aux gens qu'ils étaient en France ou à Abidjan, alors qu'ils étaient en prison ou en cavale; la deuxième catégorie est celle des jeunes qui vont, soit au collège, soit à l'université, ou qui ont un emploi, mais s'adonnent à la cybercriminalité et à divers autres actes d'escroquerie; la troisième catégorie comporte les jeunes qui sont embauchés souvent par les cyber-bandits de la première ou deuxième catégorie et qui jouent le rôle d'assistants. Ce sont eux qui vont récupérer l'argent à la banque, qui jouent le rôle de secrétaire, d'avocat, de notaire pour confirmer au téléphone que le patron ou "son client" est quelqu'un de "bonne foi"…

Dispositif législatif

De 1997 à ce jour, ce qui n'était alors qu'un cas isolé à l'époque s'est mué en un cas d'école. De 2005 à 2010 notamment, le nombre de jeunes quittant les bancs au profit des cybercafés a considérablement augmenté.

Aujourd'hui encore, le phénomène est palpable et les nombreuses descentes de la police ne découragent pas les malfaiteurs.

A la sous-direction des crimes économiques et financiers de la police béninoise (ex-Brigade économique et financière-BEF), la cellule de lutte contre la cybercriminalité a déjà eu à effectuer plusieurs arrestations.

De source proche de ce service de police, quelques-uns des auteurs de ces forfaits via le web croupissent en prison.

La loi portant lutte contre la corruption, adoptée en 2011, qui y consacre tout son chapitre XV (« Des infractions cybernétiques, informatiques et de leur répression »), condamne fermement la cybercriminalité.

L'article 124 dispose notamment : « Quiconque a procédé à la falsification de documents informatisés, quelle que soit leur forme, de nature à causer un préjudice à autrui, est puni d'un emprisonnement d'un an à cinq ans et d'une amende de deux millions de francs CFA à vingt millions. »

Mais du dispositif législatif à la réalité sur le terrain, semble exister un grand fossé.

La note d'alerte de l'ambassade de France au Bénin citée plus haut est sans ambages :

Toutefois, des réflexions existent sur le plan local en faveur de la lutte contre la cybercriminalité.

En 2010, le professeur agrégé de droit, Joseph Djogbénou, concluait ainsi une étude intitulée « la cybercriminalité : enjeux et défis pour le Bénin » :

« Le cybermonde appelle la cybercriminalité. A la lumière de l'ensemble de ces considérations, la réponse nationale devra répondre à une double exigence de cohérence. En premier lieu, elle doit, et il ne saurait en être autrement, tenir compte de la convention de Budapest avec laquelle elle doit nécessairement être compatible. En second lieu, elle doit forcément s'inscrire dans un environnement régional propice. La situation est donc mûre (à notre sens) pour un instrument régional en la matière. Toutefois, il faut sur ce sujet un changement d'approche. En effet, l'examen des travaux réalisés jusqu'ici montre que la cybercriminalité n'est pas traitée de façon spécifique, mais comme un aspect particulier de la criminalité organisée. Ici encore c'est aux experts béninois et africains de mettre en exergue la nécessité et l'exigence d'une approche spécifique de la question. C'est à ce prix que l'Afrique parviendra à s'arrimer à la révolution post-industrielle en cours. »

Pour sa part, le gestionnaire de projets technologiques, Pierre Dovonou Lokossou appelle à éviter le piège de la résignation : « Internet a certes révolutionné le monde au point qu'il serait difficile d'imaginer un autre monde sans internet ; mais, autant les coupeurs de routes existent et pourtant nous circulons sur nos routes, autant les flibustiers existent et pourtant nous naviguons sur les eaux ; autant les cybercriminels existeront toujours et nous allons toujours surfer sur le net. »

Le plus urgent, selon lui, « c'est que nos autorités prennent le taureau par les cornes pour freiner de façon drastique ce fléau qui n'honore pas le Bénin et la sous-région ouest-africaine. »

Article original de Virgile Ahissou

Réagissez à cet article

Original de l’article mis en page : Le Bénin, capitale de la cyber-arnaque en Afrique de l’Ouest – SciDev.Net Afrique Sub-Saharienne

---

Le Maroc peut-il créer une Silicon Valley au Maghreb ?

Le Maroc peut-il créer une Silicon Valley au Maghreb ?

Le Maroc a-t-il les capacités de se transformer en « Silicon Valley » du Maghreb? Hamza Hraoui, conseiller en communication d'influence pour les entreprises et les dirigeants, estime que »oui ». Dans un entretien paru jeudi 7 juillet au HuffpostMaroc, cet expert estime que le Maroc a toutes les potentialités pour cet objectif, à condition de revoir le fonctionnement de l'Agence nationale de réglementation des télécommunications (ANRT). »Nous sommes en tout cas crédibles et légitimes pour être le spot technologique de la région », souligne t-il. »Le taux de pénétration d'internet dépasse 56% chez nous alors qu'en Tunisie c'est 44%, en Algérie c'est moins de 20%. En plus d'avoir la population la plus connectée du Maghreb, le Maroc connaît également le plus fort dynamisme de ses médias en ligne. » En outre, le Maroc a pris de l'avance sur le plan des infrastructures de TIC, selon lui: » quand l'Algérie a introduit la 3G qu'en 2013, nous avons aujourd'hui la couverture 4G la plus large du Maghreb. » Mais, tempère l'expert, le pays accuse déjà un retard dans ce domaine.

Le »Hic »

»Au Maroc on est au point mort », affirme t-il, avant d'expliquer que »si la stratégie industrielle (du Ministre de l'Industrie et de l'Economie numérique) a esquissé les grandes lignes de l'économie numérique du pays, la structuration des écosystèmes numériques tarde à venir », même si »le potentiel est là. » Pour Hamza Hraoui, »il faut enclencher maintenant notre transformation et prendre le train de la nouvelle économie en misant sur notre tissu entrepreneurial. » Car »les Marocains attendent un vrai plan du numérique, conquérant et volontariste qui permettra d'accompagner les projets structurants des entreprises sur les marchés, où le Maroc peut acquérir d'ici 3 à 5 ans, un leadership continental: fabrication additive comme les imprimantes 3D, les objets connectés, la réalité augmentée, les villes intelligentes, les écoles du numérique… » Pour cela, il faut que bien des barrières tombent, et que les opérateurs du secteur rattrapent le retard accusé par le Maroc dans le digital et l'économie numérique.

Faire sauter les barrières

Et, surtout, libérer le secteur des »interdits » et des blocages. Il estime ainsi que la Maroc, en interdiction de la VoiP, »donne un mauvais signal aux acteurs de la nouvelle économie suite à cette interdiction. » »Et ses répercussions se feront sentir à moyen et à long terme », ajoute cet expert en communication, qui appelle l'ANRT à faire »son update ». Plus direct, il accuse l'ANRT de cloisonner le secteur des TIC et empêcher l'économie numérique de se développer. »A l'heure du décloisonnement de l'information, de l'explosion de la data et de l'émergence de l'économie collaborative, l'ANRT poussée et pressée par les opérateurs télécom, nous a montré qu'elle vit encore à l'âge de pierre en enlevant aux jeunes étudiants, aux chercheurs, aux start-upers qui créent de la richesse dans ce pays l'essence même du progrès: le droit à la mobilité. » Pour lui, »cela nous montre à quel point nos institutions ont du mal à admettre que la relation public-autorité et l'ordre établi sont profondément bouleversés par le digital, obligeant les hommes politiques à revoir en profondeur leurs messages, décisions et façons de faire. » A fin décembre 2015, le Maroc comptait 13,89 millions d'abonnés à l'Internet fixe, soit un taux de pénétration de 41,1 %, alors que le parc de l'internet mobile compte 12,81 millions d'abonnés avec une progression de 69,58% par an.

Article original de Amin Fassi-Fihri

Réagissez à cet article

Original de l'article mis en page : TIC: Le Maroc peut créer une Silicon Valley au Maghreb, mais…(Expert) – Maghreb Emergent

Les magistrats du palais de justice de Ouagadougou outillés pour combattre la cybercriminalité

	Les magistrats du palais de justice de Ouagadougou outillés pour combattre la cybercriminalité

La Commission de l'Informatique et des Libertés (CIL) en partenariat avec les tribunaux du palais de justice de Ouagadougou, organise un séminaire de sensibilisation des magistrats et greffiers du palais de justice de Ouagadougou aux « enjeux de la protection des données personnelles et de la vie privée des citoyens à l'ère du numérique ». Ce séminaire se déroule à Ouagadougou ce mardi 28 juin 2016.

« Aucune personne n'est, de nos jours, à l'abri des actes cybercriminels, quel que soit son statut, son rang ou l'état de ses connaissances », a lancé Marguerite Ouédraogo/Bonané, présidente de la CIL. Si de nos jours la cybercriminalité avance à grand pas dans le monde entier, force est de constater que les initiatives pour l'affronter ne manquent pas. La lutte contre cette nouvelle forme de criminalité impose donc que de « nouvelles approches soient développées et que toutes ses dimensions soient maitrisées », a-t-elle reconnu. Dans l'optique de protéger les données des justiciables en justice, la CIL entend informer et sensibiliser les magistrats aux droits des personnes dont les données sont utilisées. « Notre mission aujourd'hui c'est de les informer et de les sensibiliser aux droits des personnes dont les données sont utilisées », a confié marguerite Ouédraogo/Bonané. A l'en croire, la protection des données couvre tout le territoire. Par conséquent, tous les Burkinabé sont concernés par cette protection. Elle révèle que ce séminaire ouvert aux magistrats permettra à ces derniers de protéger les données des justiciables comme le stipule « notre loi ».

Des communications qui seront faites dans ce séminaire

Plusieurs communications seront faites durant ce séminaire. En substance, une communication sera faite à l'intention des magistrats pour leur faire connaitre le cadre juridique et institutionnel des données personnelles au Burkina Faso. Une autre sera de leur faire connaitre la communication sur l'enquête judiciaire et la protection des données personnelles face à l'enquête judiciaire. Aussi, la formation sur l'utilisation de l'internet et des réseaux sociaux leur sera-t-elle donnée.

Vu l'importance de ce séminaire qui est focalisé sur les acteurs de la justice, Dieudonné Manly, Conseiller Technique du ministère de la justice, accorde un peu plus de crédit à l'ordre du jour quand il affirme qu' « aujourd'hui la cybercriminalité a pris de l'ampleur et il va falloir outiller les magistrats afin qu'ils puissent faire face à ce phénomène ». Aussi, pense-t-il que les thèmes choisis sont bien réfléchis et que ces thèmes vont, à son avis, « permettre aux magistrats de faire face à la cybercriminalité ».

Article original de Armand Kinda

Réagissez à cet article

Original de l'article mis en page : Lutte contre la cybercriminalité : les magistrats du palais de justice de Ouagadougou outillés pour en faire face

---

Découvrez le TOP 5 des arnaques informatiques les plus récurrentes au premier trimestre 2016 selon la PLCC

Découvrez le TOP 5 des arnaques informatiques les plus récurrentes au premier trimestre 2016 selon la PLCC

En Côte d'Ivoire, les préjudices financiers causés par les cybercriminels se chiffrent en milliards. Dans sa stratégie de sensibilisation, la Plateforme de Lutte Contre la Cybercriminalité (PLCC) entreprend d'informer les populations sur les arnaques les plus récurrentes afin de leur permettre de ne pas tomber dans le piège.

Selon les chiffres communiqués par la PLCC, au cours de l'année 2015, le préjudice financier causé par la cybercriminalité a atteint 3 980 833 802 FCFA, contre **5 280 000 FCFA** en 2015. Ce sont **1 409** plaintes qui ont été enregistrées. Elles ont abouti à l'arrestation de **205** individus, dont **159** ont été déférés au parquet. Afin d'informer davantage les populations, la PLCC a sorti les 5 types arnaques qui ont été les plus récurrentes au cours du premier trimestre 2016.

1- La Sextorsion (Enregistrement illégal de communication privée, chantage à la vidéo)

Ce type d'arnaque a occasionné un préjudice de **119 millions de Franc CFA**. Cette technique consiste pour un cybercriminel à se procurer une vidéo intime de sa victime et d'exercer sur elle un harcèlement dont la condition de dénouement est le paiement d'une somme d'argent. Pour y arriver, le cybercriminel s'arrange à établir une relation amicale voire amoureuse avec sa future victime, de manière à gagner son entière confiance. Par la suite, il lui demandera de lui fournir ladite vidéo (en lui demandant d'activer sa caméra au cours d'un échange par exemple), qui deviendra finalement le moyen de pression du cybercriminel.

2 – L'accès frauduleux à un système informatique

Ce type d'arnaque est généralement orienté vers les entreprises. Au premier trimestre 2016, il a causé un préjudice financier de **42.271.426 F CFA**. Elle consiste pour le cybercriminel, à forcer l'accès d'un système informatique pour éventuellement voler des donner, ou causer des dégâts pour porter préjudice.

3 – L'usurpation d'identité (Utilisation frauduleuse d'élément d'identification de personne physique ou morale)

L'usurpation d'identité consiste pour un individu à se faire passer pour une autre. Avec des moyens détournés, le cybercriminel réussi à soutirer des informations sensibles qu'il utilise plus tard pour effectuer des paiements, effectuer des paiements etc. Il peut même aller plus loin en engageant la personne de sa victime, par une signature d'accord par exemple, sans son consentement préalable. Ce sont 37.851.973 Franc CFA de dommages qui ont été causés par ce type d'arnaque sur la même période.

Lire aussi : INTERNET : La sécurité des usagers, dernier soucis des fournisseurs d'accès en Côte d'Ivoire ?

4 – L'arnaque au faux sentiment

Ce type d'arnaque est en net recul, après avoir fait de nombreuses victimes à travers le monde. De plus en plus, les internautes sont plus prudents quoique des victimes continuent de se faire duper. 28.754.746 F CFA, c'est le préjudice causé par ce type d'arnaque au premier trimestre 2016.

5 – La fraude sur le porte-monnaie électronique

Avec l'expansion des services de porte-monnaie électronique via le mobile, ce type d'arnaque a pris de l'ampleur.

Bien ficelée, cette technique pousse la victime donner le contrôle absolu à un cybercriminel sur son compte, sans même le réaliser. Par un simple appel ou SMS, le cybercriminel invite son sa victime à saisir un code USSD, pour bénéficier d'un prétendu bonus. Une fois que la procédure est engagée, la carte SIM de la victime est désactivée, son compte transférée sur une nouvelle carte SIM. Le cybercriminel a alors le contrôle absolu.

Article original de Stéphane Agnini

CREDIT : DR

Réagissez à cet article

Original de l’article mis en page : Regionale.info
CYBERCRIMINALITE : TOP 5 des arnaques les plus récurrentes au premier trimestre 2016 selon la PLCC > Regionale.info

---

Des cybercriminels s’attaquent à la ministre Raymonde Goudou

Des cybercriminels s’attaquent à la ministre Raymonde Goudou

La cybercriminalité prend de plus en plus de l’ampleur en Côte d’Ivoire. Malgré les moyens mis en place par le ministère de l’Intérieur à travers la plateforme de lutte contre la cybercriminalité (PLCC), certaines personnes s’évertuent à poursuivre cette infraction sans être inquiétés. La dernière en date est celle d’une personne qui se fait passer pour la Ministre de la Santé, Raymonde Goudou Coffie, pour arnaquer.

Nous ne savons pas si des individus ont piraté le compte Facebook de la ministre ivoirienne de la santé ou s’il s’agit d’une usurpation d’identité. Quoiqu’il en soit, des individus utilisent l’identité de la ministre Raymonde Goudou Coffie pour faire de l’aumône auprès des utilisateurs des réseaux sociaux.
A titre illustratif, nous vous publions la conversation que ces prémusés arnaqueurs (brouteurs dans le jargon ivoirien) ont eu avec l’une de leurs victimes.

K.O.
Article original de imatin

Réagissez à cet article

Original de l’article mis en page : Cybercriminalité: Des « brouteurs » s’attaquent à la ministre Raymonde Goudou