AUTORITE DE REGULATION DES TELECOMMUNICATIONS/TIC DE CÔTE D'IVOIRE

POLE RESSOURCES ET TECHNOLOGIES

CENTRE SPECIALISE CI-CERT

RAPPORT ANNUEL 2016

SOMMAIRE

I. FAITS MARQUANTS EN 2016

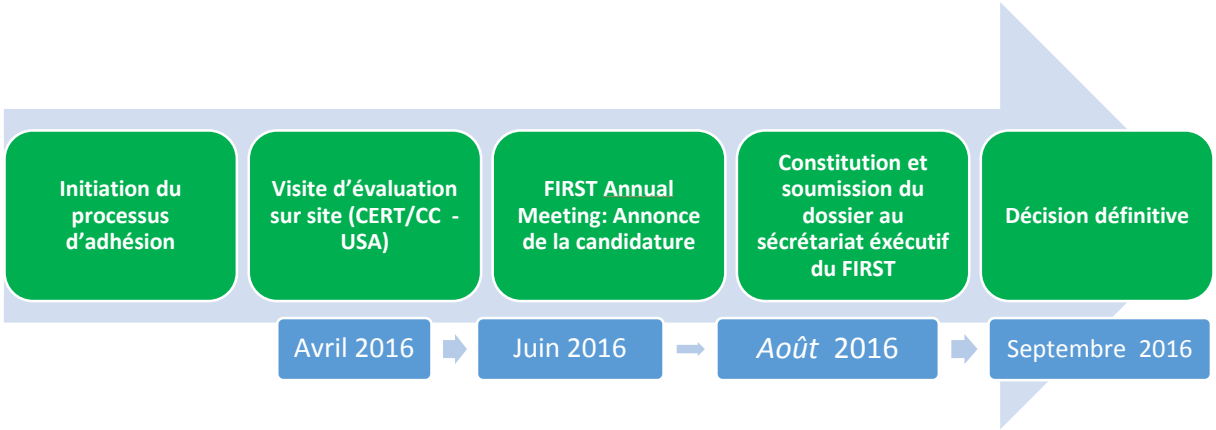
I.1. Résumé des principales activités

I.1.A. Activités Stratégiques

a. Processus d'adhésion au FIRST : Chronogramme de réalisation

Le **FIRST** (Forum for Incident Response and Security Team) est la première organisation et la plus grande **communauté** internationale réunissant 360 centres de réponse aux incidents de sécurité informatique (CERTs) du monde entier représenté par plus de 200 pays. Il a été créé depuis 1990 et il réunit la crème mondiale des spécialistes de la cybersécurité. En effet, c'est un forum très sélectif qui offre l'opportunité d'accéder aux ressources d'un réseau d'experts chevronnés dans le domaine de la cybersécurité. L'adhésion du CI-CERT au FIRST est l'aboutissement d'un long processus démarré en 2015, dont l'une des étapes importantes a été la mission d'audit sur site du CERT AMERICAIN (CERT/CC), notre sponsor primaire. L'objectif de ladite mission était de faire un audit organisationnel du CI-CERT, une revue documentaire et un audit de conformité du CI-CERT par rapport aux exigences du FIRST.

A PROPOS DU PROCESSUS D'ADHESION



Réalisé

Ainsi, après la revue de notre candidature par l'ensemble des membres, le secrétariat exécutif du FIRST a annoncé, le **07 Septembre 2016, l'adhésion officielle de la Côte d'ivoire à travers le CI-CERT au FIRST.**

b. Première participation à la réunion annuelle de l'OIC-CERT suite à notre adhésion

Membre depuis 2015 de l'Organisation of The Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT), le CI-CERT a enregistré sa première participation à la réunion annuelle de ladite organisation du 11 au 14 décembre 2016 au siège des pays membres de l'Organisation de la coopération islamique (OIC).

La 8éme conférence annuelle des CERT des Etats membre de l'OIC, l'OIC-CERT sur le thème « Towars Cyber Resilient Ummah ». Cette rencontre était combinée avec l'Assemblée Générale annuelle (AGM 2016). La conférence annuelle e l'OIC-CERT est l'occasion pour les pays membres de débattre sur les questions prioritaires de l'organisation et d'établir les orientations stratégiques pour le développement de la cybersécurité.

Au cours de cette rencontre, les nouvelles demandes d'adhésion ont été présentées et les nouveaux membres pays invités à prendre part aux échanges afin de se familiariser avec les organisations et ses membres. La Côte d'Ivoire à travers le CI-CERT est membre de l'OIC-CERT depuis juin 2015, c'est dans ce cadre que le Directeur Générale de l'ARTCI a instruit Monsieur YAPOGA Jean-Marie Nicaise, Responsable Technique du CI-CERT à prendre part aux différentes sessions prévues.

Rappelons que l'Organisation de la Conférence islamique-CERT (OIC-CERT) a été créée en vertu de la Résolution INF 35/3 adoptée par la 35e session du CFM à Kampala. L'OIC-CERT vise à renforcer et à promouvoir la coopération entre les équipes similaires établies dans les États membres de l'Organisation de la Conférence Islamique. Les objectifs peuvent être résumés comme suit :

- Renforcement des relations entre les CERT (Computer Emergency Response Teams) dans les États membres ;
- Promouvoir l'échange d'informations ;
- Prévenir ou réduire au minimum le cyberterrorisme et les délits informatiques ;
- Améliorer les programmes d'éducation et de sensibilisation ;
- Accroître le niveau de coopération dans les domaines de la recherche et du développement technologiques.

c. Atelier de validation de la stratégie nationale de cybersécurité

L'atelier de validation de la stratégie nationale de cybersécurité s'est tenu du 05 au 06 Février 2016 à NSA Hôtel de Grand-Bassam. L'objectif de cet atelier était de présenter les résultats des réflexions sur les travaux d'établissement de la stratégie et valider avec les acteurs impliqués les conclusions du projet de stratégie. L'atelier au cours duquel le CI-CERT a pris une part active, a enregistré la participation d'une centaine d'acteurs du secteur public et du secteur privé.

d. Atelier international sur la cybersécurité et la cyberdéfense organisé par l'OIF

La conférence Internationale des pays francophones sur la Cybersécurité et la Cyberdéfense s'est tenue du 08 au 10 Février 2016 à NSA Hôtel à Grand-Bassam, République de Côte d'Ivoire. Cette conférence a enregistré la participation du CI-CERT et d'une centaine d'experts venus d'une vingtaine de pays francophones.

A l'issu des échanges fructueux entre les participants et les experts, les propositions suivantes ont été faites à l'endroit des parties prenantes, notamment les Gouvernements, les structures publiques et privées, la société civile :

- Un guide pratique sur la cybersécurité permettant de contribuer à assainir l'espace numérique pour une meilleure expression des forces nationales dans le développement des pays ;
- Un plan d'actions de la Francophonie pour le renforcement de la cybersécurité et de la cyberdéfense ;
- Un projet de déclaration de principes en matière de cybersécurité et de cyberdéfense à soumettre aux Gouvernements des Etats francophones.

e. Mission d'évaluation du CI-CERT par le CERT_CC (USA)

La mission d'évaluation conduite par les représentants du CERT Américain (CERT/CC) au CI-CERT (Côte d'Ivoire Computer Emergency Response Team) dans le cadre du processus de son

adhésion, en tant que CERT National Ivoirien, au forum international des équipes de réponses aux incidents informatique dénommé FIRST s'est effectuée du 18 au 20 avril 2016.

Photo 1 : Délégation américaine et Représentants de

Le but de cette mission d'évaluation était de s'assurer que le CI-CERT répond aux exigences minimales en termes d'organisation et de niveau de maturité, dans l'optique de l'adhésion à ce forum mondial des CERTs. En effet, l'adhésion au FIRST est soumise à une étude d'éligibilité préalable basée sur des critères strictement alignés sur les standards internationaux en matière d'organisation, de services fournis, etc. par les CERTs.

f. Participation à l'Atelier Cyberdrill pour la région Afrique à l'Île Maurice organisé par l'Union International des Télécommunications (UIT)

La troisième Edition de l'atelier CyberDrill – ALERT (Exercice pratique pour les équipes de réponses aux incidents informatiques – CERTs) pour la région Afrique, organisé par l'Union International des Télécommunications, s'est tenue du 4 au 8 avril 2016, à l'Île Maurice, à l'invitation de Mauritius National Computer Board (NCB).

L'objectif de cet évènement régional était d'améliorer les capacités de communication avec les parties prenantes et celles de réponses aux incidents des CERTs participants, la coopération entre les CERTs africains pour assurer des efforts collectifs continus et apporter des réponses appropriées contre les cybermenaces, le renforcement de capacités des CERTs africain et l'initiative d'une plate-forme de communication dans le cadre du traitement des incidents cybernétiques.

Cette troisième édition du CyberDrill a connu un très fort engouement avec la participation de dix-neuf (19) pays répartis en douze (12) équipes.

Lors des conférences et du panel, la délégation ivoirienne a fait des interventions sur :

- Expérience de la Cote d'Ivoire en matière de Partage d'information notamment avec le modèle de convention adoptée avec les Fournisseurs d'Accès à Internet (FAI) et la police nationale dans le cadre de la PLCC ; Partage d'information sur le mode fonctionnement du CI-CERT dans le traitement des incidents et dans la veille proactive ;
- Proposer d'abriter un atelier Cyberdrill en Côte d'Ivoire. A cet effet, l'accord de principe a été donné par M. Mohamed TRAORE, Directeur TIC, Système d'Information, Sécurité en attendant le cahier des charges pour l'organisation éventuel dudit évènement.


Photo 2 et 3 : Discussion entre la délégation ivoirienne (Mohamed Traoré et Claude C. DOFFOU) et l'IUT (Marco OBISO et Serges

A l'occasion de cette réunion AFRINIC 25, AfricaCERT a organisé en collaboration avec JPCERT (02) deux formations techniques (03) trois jours durant (25, 26,27 Novembre 2016). Ces formations étaient intitulées :

- **Network Forensic:** avec pour objective de connaitre les fondamentaux et la maitrise des outils de network forensic

- **Malware Analysis Basics :** dont l'objectif est de Maitriser les bases et les outils de l'analyse de Malware

Les participants étaient de diverses organisations notamment, des établissements universitaires, de la société civile, des fournisseurs de services, des équipementiers, des ingénieurs, etc.

I.1.B. Activités opérationnelles

En cette année 2016, le CI-CERT a :

- Traité cinquante-quatre mille cinq (54005) incidents informatiques majoritairement constitués d'attaques de type : Scan, Spam et BOTNET.
- Diffusé deux mille sept cent soixante-cinq (2765) vulnérabilités en 2016 contre en 2015, deux mille cent trente-quatre (2134) failles de sécurité majoritairement constitués de vulnérabilités liées à des mauvaises configurations des protocoles de sécurité utilisés sur des serveurs publics.
- Publié sur son site Internet au cours de l'année 2016, trois cent vingt-deux (326) bulletins de sécurité contre deux cent quatre-vingt-quatorze (294) en 2015.

Pour le compte de la cybercriminalité, comparé à 2015, le nombre d'affaires a augmenté. Il passe de 1409 à 2067 soit 31 %. Quand, le préjudice 2016 estimé à 2 978 999 322 FCFA contre 2 652 763 885 FCFA en 2015 soit une légère hausse d'environ 10%.

II. A PROPOS DU CI-CERT

II.1. Aperçu général

Le CI-CERT, premier organe du genre en Côte d'Ivoire, a été créé en Juin 2009 par l'ARTCI. Il constitue l'une des mesures organisationnelles et l'outil par excellence en matière de politique nationale de cybersécurité et de protection des infrastructures critiques des systèmes d'information de l'Etat Ivoirien. Le CI-CERT est un centre spécialisé rattaché à la Direction Générale qui joue le rôle de CERT national.

II.2. Missions

Les missions du CI-CERT sont :

- Assurer la fonction de point focal national en matière de cybersécurité ;
- Assurer la coordination du traitement des incidents de sécurité informatique au niveau national pour les acteurs des secteurs privé et public ;
- Contribuer à la lutte contre la cybercriminalité ;
- Contribuer à assurer la sécurité des infrastructures critiques de l'Etat ;
- Assurer la veille technologique en matière de sécurité de l'information ;
- Sensibiliser la population sur les dangers liés à l'utilisation des TIC ;
- Développer la culture de la cybersécurité au plan national.

II.3. Parties prenantes

En tant que CSIRT national du gouvernement de Côte d'Ivoire, le CI-CERT coordonne et facilite la gestion des incidents sur le cyberespace national. Cela se fait soit directement, comme c'est le cas avec les structures du gouvernement, soit indirectement par l'intermédiaires des fournisseurs de services Internet.

La communauté des parties prenantes du CI-CERT est constituée de :

- Organismes gouvernementaux ;
- Opérateurs des Télécommunications et Fournisseurs d'accès Internet ;
- Les organismes d'application de la loi ;
- Utilisateurs d'Internet ;
- Organisations du secteur privé (secteur financier, sociétés commerciales opérant en Côte d'Ivoire).

II.4. Contacts

Le CI-CERT est accessible via les canaux suivants :

- **Tel**: (+225) 20 34 44 48 / poste 51 00. GMT (+00)
- **Fax** : (+225) 20 22 43 73

- **Email** : info@cicert.ci / equipe@ci-cert.ci
- **Déclaration d'incident** : incidents@cicert.ci
- **Site web**: http://www.cicert.ci/
- Adresse Géographique : Abidjan - Marcory Anoumabo
- Adresse Postale : 18 BP 2203 Abidjan 18 - Côte d'Ivoire

II.5. Organisation et Services offerts

L'équipe CI-CERT est composée d'un chef de centre et de trois (03) équipes opérationnelles chargées de :

- **Communication & Sensibilisation**
- **Veille et Monitoring**
- **Traitement d'Incidents**

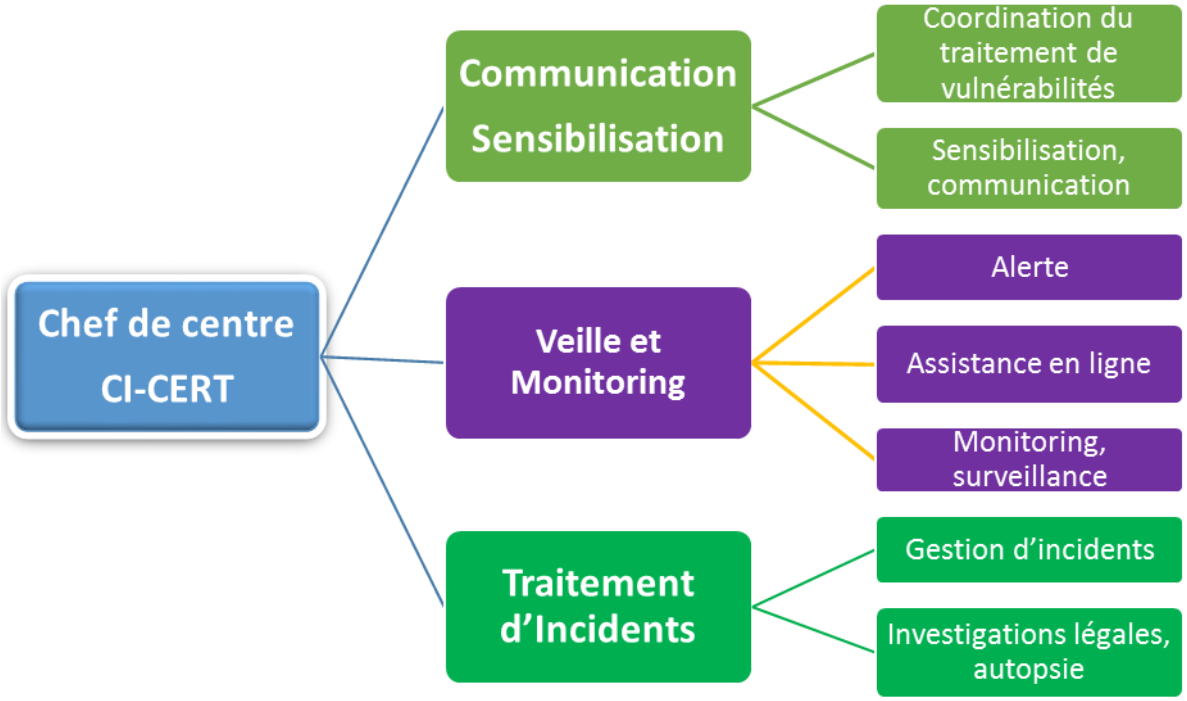


Figure 1 : Organisation du CI-CERT

III. ACTIVITES REALISEES ET RESULTATS OBTENUS

III.1. Traitements d'incidents de sécurité informatique

Le CI-CERT propose des services réactifs en matière de sécurité informatique. Il collecte et traite les incidents informatiques qui surviennent sur le cyberespace national notamment les systèmes d'informations de ses parties prenantes. Les incidents collectés et traités par le CI-CERT au cours de cette année sont de divers ordres, à savoir : Réseau de BOTNET, Infection par des virus ou chevaux de Troie informatique (Ransomware), attaques sur les infrastructures, Scans actifs, défacement de site web, etc.

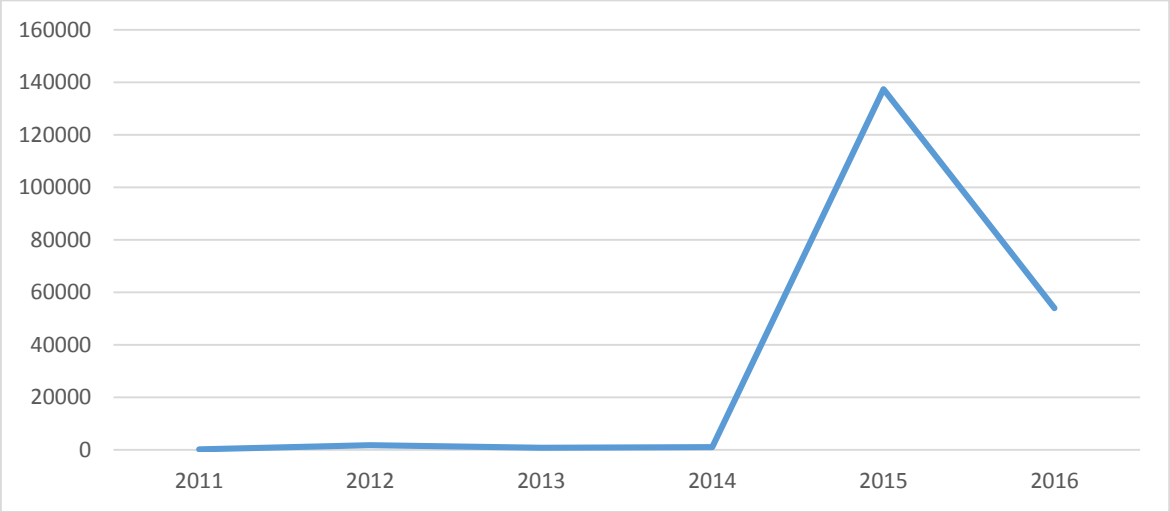
Au total, le CI-CERT a traité au cours de cette année cinquante-quatre mille cinq (54005) incidents informatiques majoritairement constitués d'attaques de type : Scan, Spam et BOTNET.

Les détails des activités sont consignés dans le tableau suivant :

Période	TYPES D'INCIDENTS INFORMATIQUE						BOTNET
	Spam	Scan	Phishing	Ransomware (CTB-Locker ; TeslaCrypt ; Locky)	Attaques (XSS, SQL Injection,DDoS)	Défacement de site web	
Janvier	146	-	-	12	-	-	1128
Février	160	-	1	08	-	-	-
Mars	-	-	-	-	4	-	2456
Avril	60	-	10	-	02	3	-
Mai	-	517	-	19	22	-	9269
Juin	215	268	-	01	12	-	6238
Juillet	-	125		-	15	5	
Août		110	2	-	-	-	513
Septembre	115	-	2	-	-	-	8124
Octobre	-	615	-	-	45	-	4253
Novembre	-	-	38	491	19	1	2136
Décembre	123	-	92	576	79	-	11481
Total	**819**	**1635**	**145**	**1107**	**192**	**4509**	**45598**

Tableau incidents traités par catégorie en 2016

L'année 2016 a été marquée par une forte baisse des incidents collectés comparativement à l'année 2015 comme l'indique la courbe évolutive ci-dessous. Elle s'explique par la prise en compte des recommandations du CI-CERT dans le cadre de la résolution d'incidents proposées en fin d'année 2015 aux les parties prenantes.



Graphique 1 : Courbe évolutive d'incidents collectés depuis 2011 à 2016

En somme, le CI-CERT a contribué à traiter au cours de ces six (06) dernières années un total d'environ cent quatre-vingt-quinze mille quatre cent vingt-neuf (195429) incidents informatiques. Cela marque indiscutablement le gain en maturité et en expérience de l'équipe dans le traitement des incidents et ce taux devrait connaître une évolution plus conséquente dans les années à venir en incitant les parties prenantes à déclarer les incidents informatiques.

III.2. Coordination des vulnérabilités

Aussi, en cette année 2016, le CERT national ivoirien a assuré la coordination du traitement des vulnérabilités qui a pour objectif de notifier l'existence des vulnérabilités, failles de sécurité sur les réseaux nationaux et fournir des informations sur les moyens d'y remédier ou d'en atténuer les effets. Le CI-CERT s'assure que les recommandations ont été appliquées avec succès.

Deux mille sept cent soixante-cinq (2765) en 2016 contre en 2015, deux mille cent trente-quatre (2134) failles de sécurité majoritairement constitués de vulnérabilités liées à des mauvaises configurations des protocoles de sécurité utilisés sur des serveurs publics.

III.3. Veille technologique et Sensibilisation

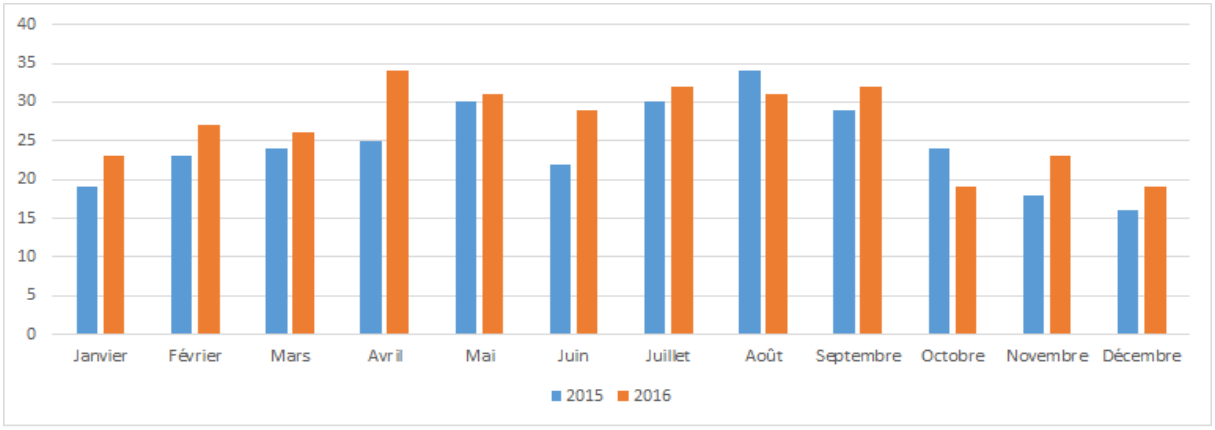
A travers sa cellule de Veille et Monitoring, le CI-CERT assure la surveillance de l'environnement technologique afin de présenter de l'information utile aux parties prenantes en matière de sécurité informatique. Pour ce faire, le CI-CERT réalise les activités suivantes :

III.3.a. Publications d'informations de sécurité : alertes, bulletins et avis de sécurité

Ce service de type proactif consiste à publier des informations utiles relatives aux risques de sécurité, innovations en matière technologique, sur des produits informatiques divers (CMS, Systèmes d'exploitation, navigateur web, logiciels, etc.).

Notons que le chiffre des publications a connu une légère augmentation comparativement à l'année précédente. En effet, le CI-CERT a publié sur son site Internet au cours de l'année 2016, trois cent vingt-deux (326) bulletins de sécurité contre deux cent quatre-vingt-quatorze (294) en 2015.

Les résultats présentés ci-dessus sont illustrés à travers le graphe suivant :



Graphique 2 : Répartition des publications par mois (Janvier 2015 à Décembre 2016)

III.3.b. Diffusion de la Mailing-List

Le CI-CERT s'est engagé à la diffusion d'informations de sécurité, en tenant compte des besoins spécifiques de chaque partie prenante. Ainsi, les informations sont transmises de façon hebdomadaire via une mailing-list.

Au cours de l'année 2016, le CI-CERT a diffusé trois cent vingt-six (**326**) *bulletins de sécurité* et quatorze (**14**) *alertes de sécurités* via mailing-list.

De plus, la stratégie de communication et l'augmentation du volume d'activités de l'équipe ont eu un impact fort considérable sur le niveau d'interaction entre le grand public et le CI-CERT. Cette tendance est justifiée par l'augmentation exponentielle du nombre de souscripteurs à ce service (mailing-list), passant de trois cent cinquante-quatre (**354**) souscriptions en 2015 à trois cent soixante-onze (**371**) souscriptions en 2016.

Ce nombre de récipiendaires est en constante croissance, montrant l'intérêt accordé par les parties prenantes aux bulletins de sécurité du CI-CERT.

QUELQUES RECOMMANDATIONS DU CI-CERT

- **Mettre à jour** *régulièrement votre* **solution antivirale**.
- *Activer* **la mise à jour automatique** *de votre* **système Android et toutes les applications (p.ex. navigateur, PDF Reader) installées sur votre Smartphone, de manière automatique lorsque cela est possible**.
- **Vérifier l'authenticité des expéditeurs** *avant la lecture de chaque message reçu par* **e-mail** *ou affiché sur votre mûr de* **Facebook / Twitter** *et en cas de doute* **ne suivez pas les recommandations figurant dans le texte, ne suivez pas les liens indiqués et n'ouvrez pas les documents attachés**, *ne répondez pas et supprimer le immédiatement*.
- **Se connecter** *à Internet en utilisant un* **compte avec des privilèges limités**.
- *Installer et tenir à jour un pare-feu (firewall) personnel.*

III.3.c. Sensibilisation (interne et externe) et communication sur le site et réseaux sociaux

Au cours de l'année 2016, l'accent a été mis sur la sensibilisation du personnel de l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire et du grand public via les réseaux sociaux.

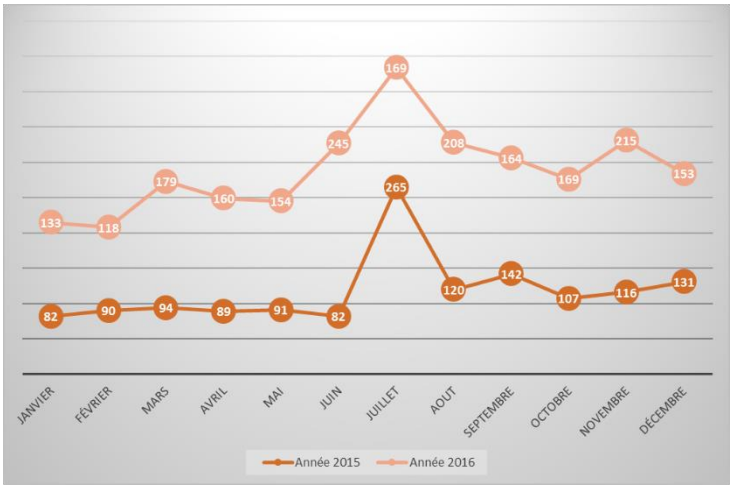
Cette sensibilisation a porté sur des thématiques variées en rapport avec l'actualité de la sécurité informatique au cours de l'année 2016.

Figure 2 et 3 : Exemple de maquette de sensibilisation

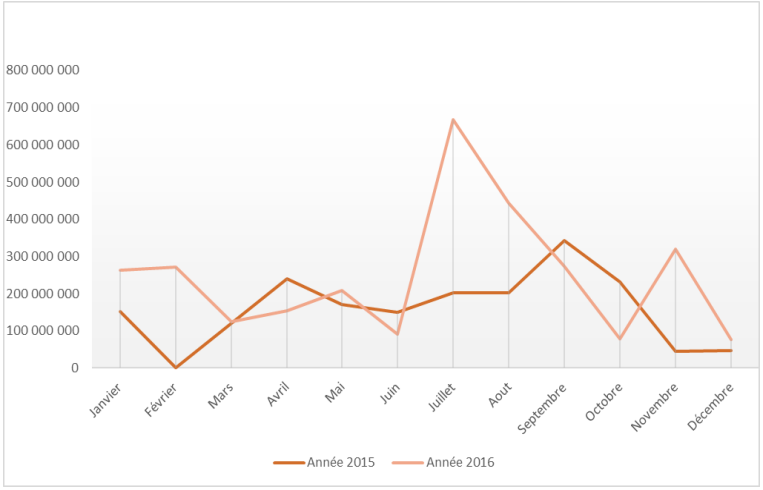
III.4. Lutte contre la cybercriminalité

Au titre de la lutte contre la Cybercriminalité, cette activité est menée par la Plateforme de Lutte Contre la Cybercriminalité (PLCC) qui est le fruit de l'accord de partenariat signé en 2011 et actualisé le 27 janvier 2014, entre la Direction Générale de la Police Nationale (DGPN) et l'ARTCI.

Les réalisations de la PLCC pour l'année 2016 :



Graphique 3 - Nombre d'affaires cumulées par mois



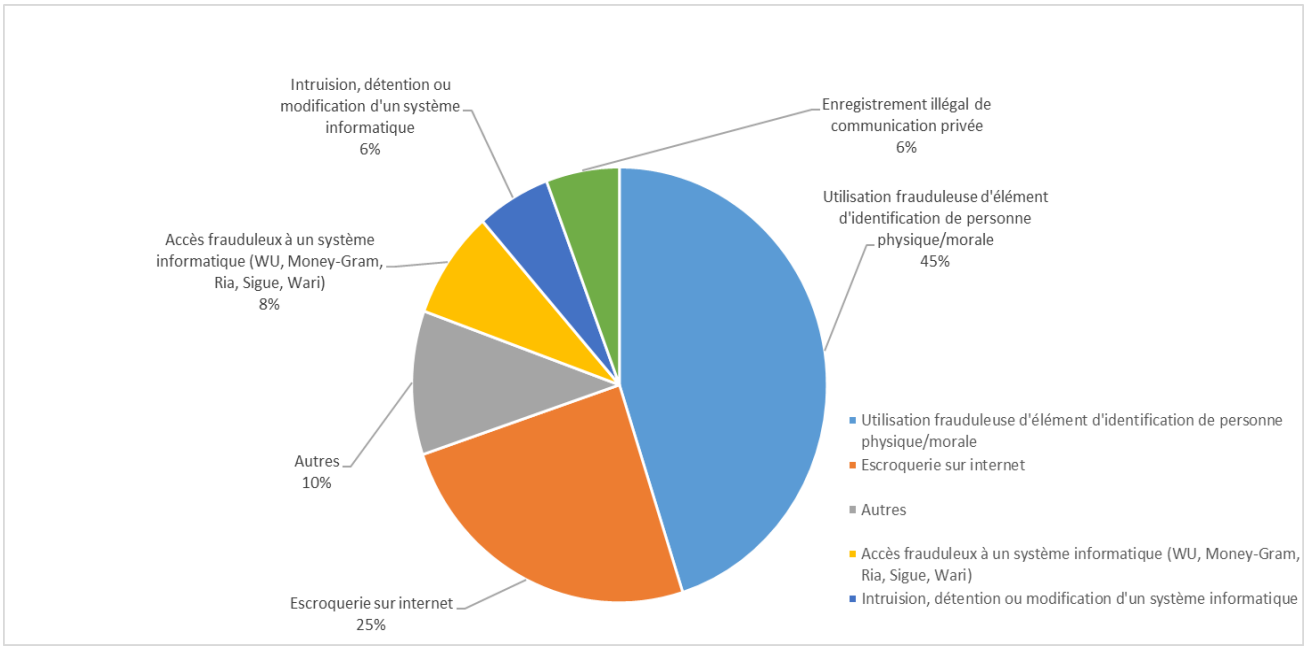
Graphique 4 - Nombre de préjudices financiers cumulés par mois

Comparé à 2015, le nombre d'affaires a augmenté. Il passe de 1409 à 2067 soit 31 %. Quand, le préjudice 2016 estimé à 2 978 999 322 FCFA a connu une légère augmentation de 10 %. Plusieurs raisons expliquent cette baisse :

- La baisse du préjudice est due à l'intensification de la sensibilisation faite par la PLCC via les réseaux sociaux et les actions sur le terrain (entreprises et grand public) ;
- L'augmentation du nombre de cas est due d'une part à la présence accrue de la PLCC sur le terrain (cybercafés, perquisitions, renseignement, etc.) entrainant des interpellations massives et d'autre part à la confiance de plus en plus grande que la population a en la PLCC, pour lui dénoncer les cas.

Par ailleurs, nous constatons une hausse du nombre d'affaires pendant les vacances scolaires (Juin -Aout) et en fin d'année (Octobre-Décembre). Cela s'explique par le nombre important des cyberdélinquants encore élèves ou étudiants.

Par ailleurs, nous constatons une hausse du nombre d'affaires pendant les vacances scolaires (Juillet –Septembre). Cela s'explique par le nombre important des cybers-délinquants encore élèves ou étudiants.



Graphique 5 - Préjudice financier par type

Il ressort entre autres du graphique ci-dessus que 45% des préjudices financiers concerne les utilisations frauduleuses d'éléments d'identification de personnes physique ou morale : 393 cas

ont été enregistrés au cours de l'année 2016. Les victimes sont essentiellement des personnes vivant en Côte d'Ivoire. Cette infraction consiste pour le cybercriminel à usurper l'identité d'une personne physique ou morale pour se faire passer pour celle-ci afin de soit demander de l'aide financière à ses correspondants, soit pour proposer des produits ou des services. Pour l'année 2016, un préjudice total de 1 342 690 062 F CFA a été constaté par la PLCC contre 49 858 257 FCFA en 2015, soit une hausse 96 %.

IV. PERSPECTIVES 2017

- Renouvellement de l'accord de partenariat entre l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) et la Direction Générale de la Police Nationale (DGPN) pour le renforcement de la Plateforme de Lutte Contre la Cybercriminalité (PLCC) dans le cadre de la lutte contre la cybercriminalité
- Collaboration avec le CERT_CC pour le renforcement des capacités du CI-CERT : plan de formation 2017
- Organisation de la réunion annuelle de l'OIC-CERT 2017
- Isolement du réseau informatique du CI-CERT de celui de l'ARTCI (établir donc les conditions et les moyens de mise en œuvre de ce LAN)