CI-CERT

CÔTE D'IVOIRE - COMPUTER EMERGENCY RESPONSE TEAM

# RAPPORT D'ACTIVITES

## ANNEE 2012

# SOMMAIRE

# RESUME

La sécurité informatique de nos jours est de plus en plus primordiale avec la recrudescence des arnaques dans notre pays. Depuis quelques années, la notion de sécurité informatique s'est de mieux en mieux définie. Les entreprises et particuliers prennent de plus en plus conscience de l'importance de se doter de mesures visant à assurer une meilleure protection des données.

Conscient de cela depuis quatre (4) ans, le CERT ivoirien dénommé CI-CERT travaille sans relâche pour assurer une confiance dans l'utilisation de l'Internet et contribue à la sécurité des systèmes d'information sur le cyberespace national.

Au cours de l'année 2012, le CI-CERT a traité mille huit cent soixante-deux (1862) incidents informatiques majoritairement constitués d'attaques de type **:** Scan, Spam et BOTNET. A-t-il aussi mené des audits de vulnérabilités sur les infrastructures en ligne de nos parties prenantes dans différents secteurs d'activités

Aussi, la prévention à travers la diffusion d'avis, d'alertes et publications de sécurité a connu une hausse passant de quatre cent cinquante (450) bulletins de sécurité contre cent soixante-treize (173) en 2011 ; soit plus du double. De plus l'outil de surveillance de sites web (SYSWEB) mise en place par nos ingénieurs a permis d'assurer le monitoring permanent de cent quarante et un (141) sites web.

Concernant l'activité de lutte contre la cybercriminalité, la Plate-forme de Lutte Contre la Cybercriminalité (PLCC) composée essentiellement de la Direction de l'Informatique et des Traces Technologiques de la Police Scientifique (DITT) et Côte d'Ivoire – Computer Emergency Response Team (CI-CERT) représentant de l'ATCI s'est dotée de moyens techniques et opérationnels en vue d'accentuer la répression. Pour l'année 2012, la PLCC a procédé à l'interpellation de soixante et onze (**71**) suspects dont cinquante et un (**51**) ont été condamnés à des peines de prison par la Justice Ivoirienne.

L'un des faits marquant de l'année 2012 est l'adhésion au programme UIT/ IMPACT marquée par la signature d'une convention lors de l'ITU Telecom World 2012 à Dubaï entre le Directeur Général de l'ATCI et le Secrétaire général de l'UIT. Cette adhésion nous permettra de respecter toutes les normes internationales en matière de sécurité informatique.

En outre, le CI-CERT dans sa fonction de centre de coordination, a administré des séances de formations et de sensibilisation aux étudiants et aux entreprises.

Malgré l'absence de cadre juridique en matière de cybersécurité, l'année 2012 a montré des avancées à tous les niveaux.

# AVANT PROPOS

Le CI-CERT (Côte d'Ivoire - Computer Emergency Response Team) est l'équipe d'urgence et de réponses aux incidents informatiques de la Côte d'Ivoire. Il est le premier CERT au plan national et constitue l'un des piliers dans le domaine de la sécurité informatique au niveau sous-régional. Composé d'experts de haut niveau en sécurité informatique, il s'appuie également sur un vaste réseau professionnel international, en vue de proposer des services proactifs et réactifs à l'ensemble de ses parties prenantes établies sur le territoire Ivoirien.

En sa qualité de CERT national, le CI-CERT est financé par un organe d'Etat notamment l'**ATCI** (Agence des Télécommunications de Côte d'Ivoire) dans le but d'assurer une disponibilité des ressources matérielles, humaines, techniques et financières nécessaires. Ces ressources sont utiles à la réalisation de sa mission qui est de contribuer à la sécurisation du cyberespace, des infrastructures critiques nationales et d'assurer la fonction de point focal en matière de cybersécurité.

# I. A PROPOS DU CI-CERT

## 1) CREATION

Le CI-CERT, premier organe du genre en Côte d'Ivoire, a été créé en Juin 2009 par l'Agence des Télécommunications de Côte d'Ivoire (ATCI). 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 rattaché administrativement à l'ATCI, et fonctionne sous la tutelle du Ministère des Postes et Télécommunications de Côte d'Ivoire (MPTIC).

## 2) MISSIONS

Les principales missions du CI-CERT sont de:

- Assurer la fonction de point focal de la Côte d'Ivoire pour les cas de cybersécurité ;
  - Œuvrer à la réduction de la cyberescroquerie en provenance de la Côte d'Ivoire ;
  - Contribuer à assurer la sécurité des infrastructures critiques d'information ;
  - Collecter et traiter les incidents survenant sur les réseaux et systèmes d'information ;
  - Assurer la veille technologique en matière de sécurité ;
- Sensibiliser la population sur les dangers liés à l'utilisation des TICs ;
- Proposer des programmes de formation de haut niveau en matière de sécurité des SI.

Pour mener à bien ses missions, le CI-CERT réalise les activités suivantes :

- Collecte, analyse et diffusion d'informations sur les incidents cybernétiques ;
- Prévisions et alertes d'incidents de sécurité informatique ;
- Prescription de mesures d'urgence pour gérer les incidents de sécurité informatique ;
- Coordination des activités de réponses aux incidents cybernétiques ;
- Diffusion de directives, avis, notes de vulnérabilité et de livres blancs relatifs aux pratiques de sécurité ;
- Réalisation d'audits de sécurité sur les infrastructures critiques de l'Etat et des parties prenantes ;
- Toutes autres fonctions liées à la cybersécurité qui peuvent être prescrites.

## 3) CONSTITUTION DE L'EQUIPE

Le CI-CERT est composé d'un personnel technique, administratif et juridique.

## 4) CIRCONSCRIPTION

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

- Administration publique ;
- Communauté Internet nationale ;
- Gouvernement ;
- Fournisseurs d'accès à internet.

## 5) COMMENT CONTACTER LE CI-CERT ?

Le CI-CERT est accessible via les canaux suivants :

- **Tel**: (+225) 20 22 91 97 / (+225) 20 22 91 99. GMT (+00)
- **Fax** : (+225) 20 22 92 27
- **Email** : info@cicert.ci
- **Déclaration d'incident** : incidents@cicert.ci
- **Site web**: http://www.cicert.ci/
- **Adresse géographique** : 17 BP 885 Abidjan 17, Abidjan Plateau, Tour Postel 2001, Mezzanine

# II. ACTIVITES ET OPERATIONS

## 1) COLLECTE ET TRAITEMENT D'INCIDENTS INFORMATIQUES

Le CI-CERT propose des services réactifs en matière de sécurité informatique. Il collecte et traite les incidents informatiques qui surviennent sur 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[1], Infection par des virus ou chevaux de Troie informatique (DNS Changer), attaques sur les infrastructures, Scans actifs, défacement de site web, etc.

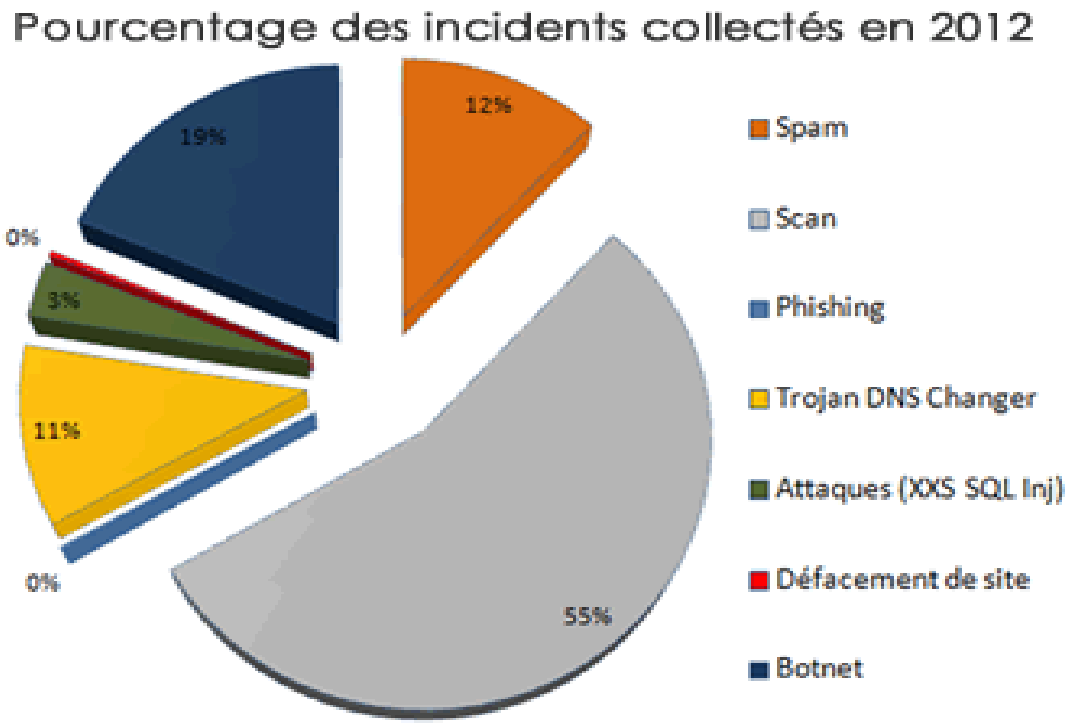
Au total, le CI-CERT a traité au cours de cette année mille huit cent soixante-deux (**1862**) **incidents informatiques** majoritairement constitués d'attaques de type **:** Scan, Spam et BOTNET.

Les détails des activités sont consignés dans le tableau suivant :

[1] Réseaux de machines compromises ou zombies

| Période | TYPES D'INCIDENTS INFORMATIQUE | | | | | | BOTNET |
|---|---|---|---|---|---|---|---|
| | Spam | Scan | Phishing | Trojan DNS Changer | Attaques (XSS, SQL injection) | Défacement de site web | |
| Janvier | - | - | - | - | 5 | - | - |
| Février | 160 | - | 1 | 70 | - | - | - |
| Mars | - | - | - | 112 | 4 | - | - |
| Avril | 60 | - | - | - | 02 | - | 03 |
| Mai | - | 517 | - | 19 | 22 | - | 126 |
| Juin | - | 268 | - | 01 | 12 | - | 08 |
| Juillet | - | 125 | | - | 15 | 5 | 65 |
| Août | - | 110 | 2 | - | - | - | 65 |
| Septembre | - | - | 2 | - | - | - | 19 |
| Octobre | - | - | - | - | - | - | 10 |
| Novembre | - | - | - | 1 | 2 | 1 | 14 |
| Décembre | - | - | - | - | - | - | 37 |
| Total | **220** | **1020** | **4** | **203** | **62** | **6** | **347** |

Tableau 1: Incidents informatiques reçus au cours de l'année




2012

**Figure 1: Répartition des incidents par types d'incidents**

Le premier semestre de l'année a connu une très forte activité avec mille trois cent trente-six (**1336**) incidents informatiques collectés ; soit un pourcentage de **71.75%** des incidents traités au cours de toute l'année.

En somme, le CI-CERT a contribué à traiter au cours de ces trois (03) dernières années environ deux mille trois cent dix-neuf (**2319**) incidents informatiques. Cependant, l'année 2012 est marquée par un fort taux d'accroissement de l'activité du CI-CERT. Cela marque indiscutablement le gain en maturité et en expérience de l'équipe dans le traitement des incidents. Ce taux devrait connaître une évolution plus conséquente dans les années à venir en incitant les parties prenantes à déclarer les incidents informatiques.

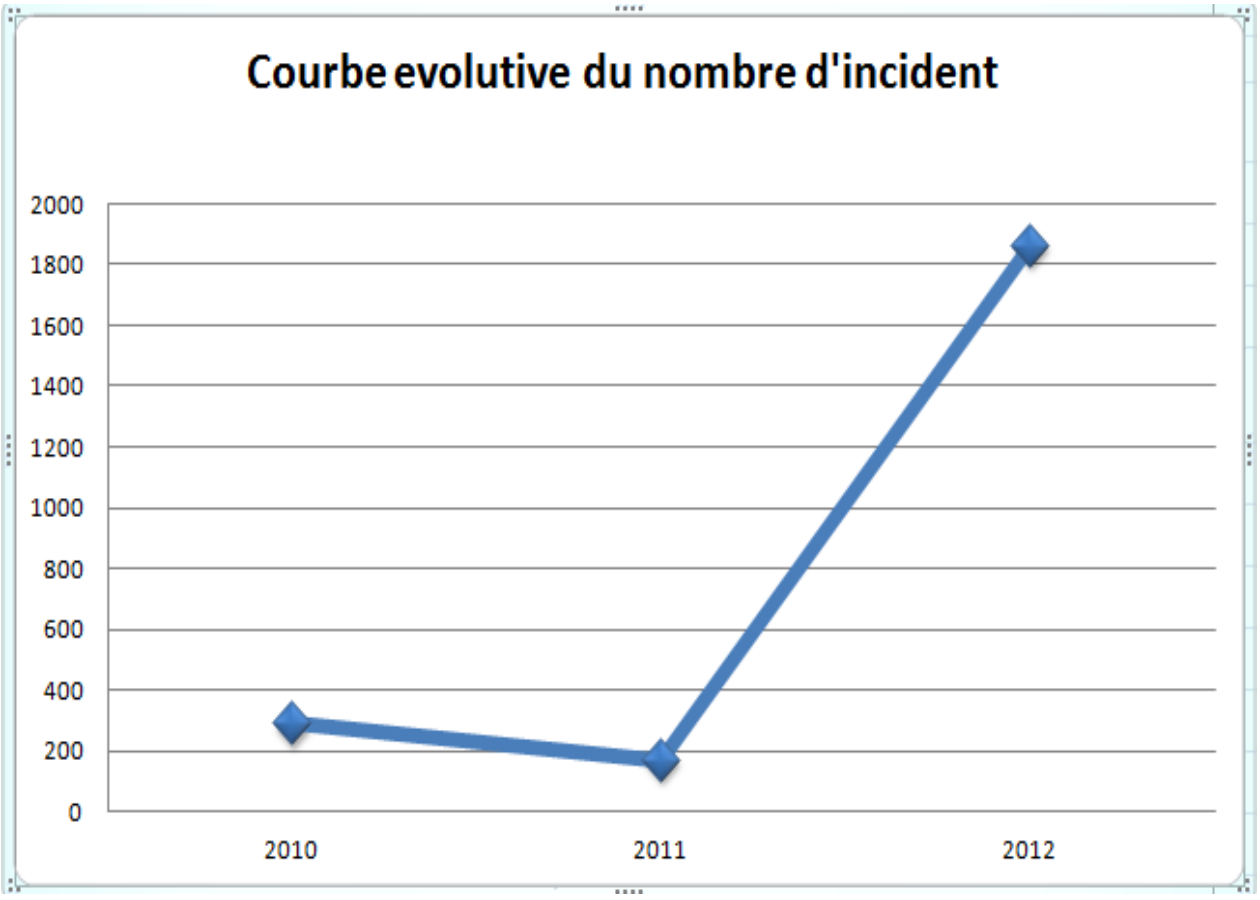



**Figure 2: Courbe évolutive du nombre d'incidents reçus**

## 2) AUDIT DE SECURITE DES INFRASTRUCTURES

Conformément à son plan d'action 2012, le CI-CERT a mené des audits de vulnérabilités sur les infrastructures en ligne de ses parties prenantes. Pour l'année écoulée, les audits concernaient trois (03) secteurs d'activités :

- Les sites web du domaine « gouv.ci » ;
- Les sites web d'entreprises du secteur des télécommunications ;

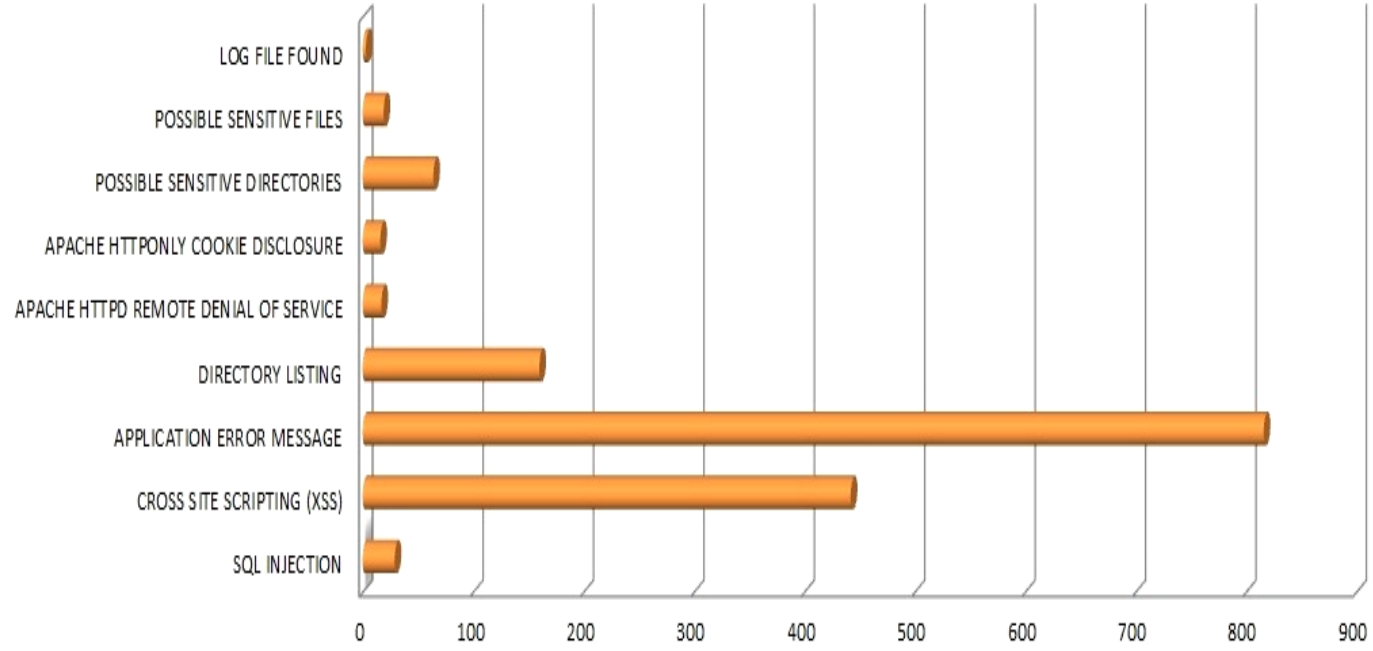
### a) Sites web du domaine « gouv.ci »

Au total, vingt (20) sites du domaine « gouv.ci » ont été audités, conduisant à la découverte de mille cinq-cents soixante six (1566) failles de sécurité. Les failles les plus récurrentes sont essentiellement de type Application Error message, Cross Site Scripting (XSS) et Directory Listing, avec respectivement 52.1% ; 28.22% et 10.21%. Ces vulnérabilités font parties du top dix (10) des risques de sécurité applicatifs Web les plus critiques.

| Type de vulnérabilité | Nombre | Pourcentage (%) |
|---|---|---|
| **Application error message** | **816** | **52,1** |
| **Cross Site Scripting (XSS)** | **442** | **28,22** |
| **Directory listing** | **160** | **10,21** |
| **Possible sensitive directories** | **64** | **4,08** |
| **SQL Injection** | **29** | **1,85** |
| **Possible sensitive files** | **19** | **1,21** |
| **Apache http remote denial of service** | **17** | **1,08** |
| **Apache http only cookie disclosure** | **16** | **1,02** |
| **Log files found** | **3** | **0,19** |
| **Total** | **1566** | **100** |

**Tableau 2: Récapitulatif des failles découvertes sur les sites du domaine "gouv.ci"**

Vous trouverez ci-joint la liste des sites Internet du domaine « gouv.ci » audités : *Cf annexe 1*




| | SQL INJECTION | CROSS SITE SCRIPTING (XSS) | APPLICATION ERROR MESSAGE | DIRECTORY LISTING | APACHE HTTPD REMOTE DENIAL OF SERVICE | APACHE HTTPONLY COOKIE DISCLOSURE | POSSIBLE SENSITIVE DIRECTORIES | POSSIBLE SENSITIVE FILES | LOG FILE FOUND |
|---|---|---|---|---|---|---|---|---|---|
| Series1 | 29 | 442 | 816 | 160 | 17 | 16 | 64 | 19 | 3 |

**Figure 3: Graphe de répartition des vulnérabilités découvertes sur les sites du domaine "gouv.ci"**

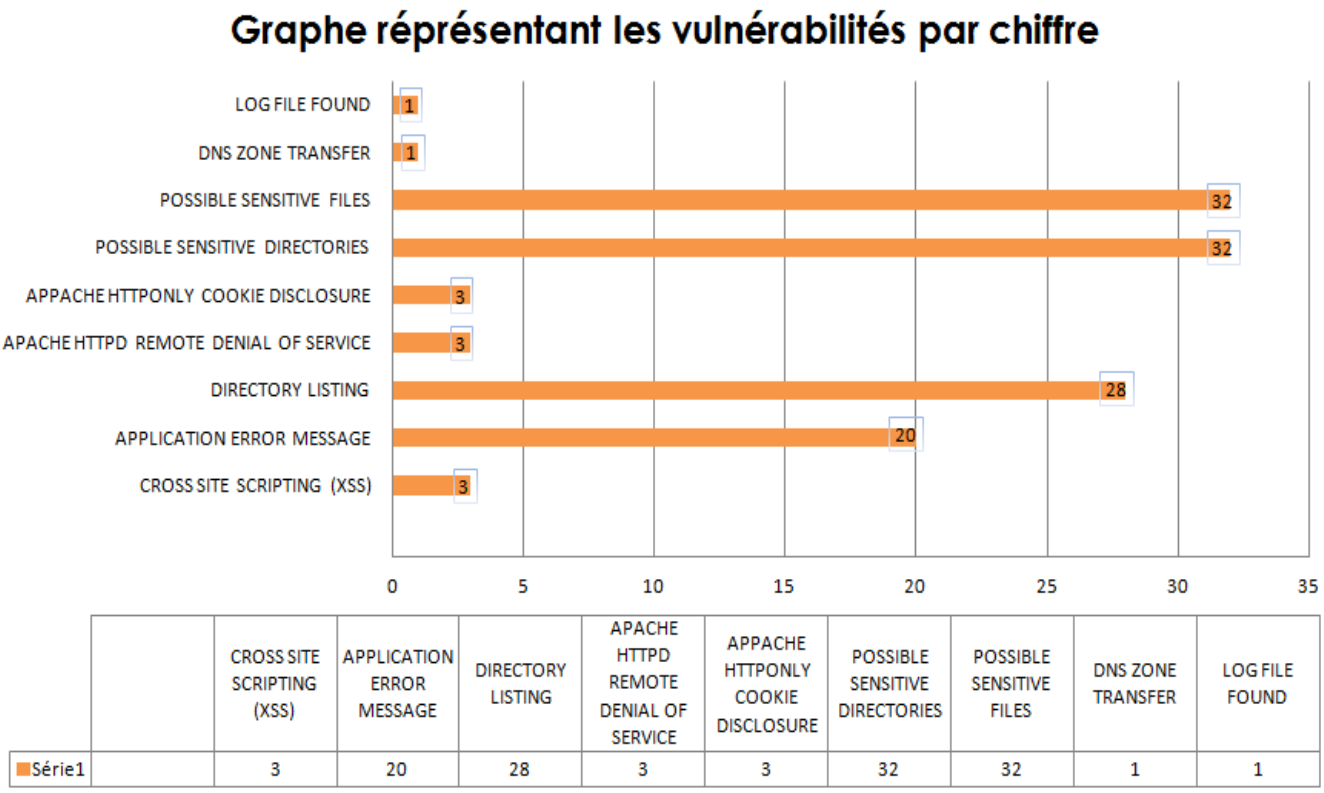
b) les sites web d'entreprises du secteur des télécommunications

Au total, le CI-CERT a audité six (06) sites_web d'opérateurs du secteur des télécommunications et découvert cent vingt-trois (123) failles de sécurité.

Les failles les plus nombreuses sont de type Possible Sensitive files, possible sensitive directories et Directory Listing, avec respectivement 26,01 % et 22,76 %. Voir la liste des entreprises : *cf.* annexe 2)

| Type de vulnérabilités | Nombre | Pourcentage |
|---|---|---|
| **Possible sensitive directories** | 32 | 26.01 |
| **Possible sensitive files** | 32 | 26.01 |
| **Directory Listing** | 28 | 22.76 |
| **Application Error message** | 20 | 16.26 |
| **Cross site Scripting (XSS)** | 03 | 2.43 |
| **Apache httpd remote denial of service** | 03 | 2.43 |
| **Apache http only cookie disclosure** | 03 | 2.43 |
| **DNS Zone transfer** | 01 | 0.81 |
| **Log file found** | 01 | 0.81 |
| **Total** | **123** | **100** |

**Tableau 3: Récapitulatif des vulnérabilités découvertes sur les sites internet du secteur des Télécommunications**




| | | CROSS SITE SCRIPTING (XSS) | APPLICATION ERROR MESSAGE | DIRECTORY LISTING | APACHE HTTPD REMOTE DENIAL OF SERVICE | APPACHE HTTPONLY COOKIE DISCLOSURE | POSSIBLE SENSITIVE DIRECTORIES | POSSIBLE SENSITIVE FILES | DNS ZONE TRANSFER | LOG FILE FOUND |
|---|---|---|---|---|---|---|---|---|---|---|
| Série1 | | 3 | 20 | 28 | 3 | 3 | 32 | 32 | 1 | 1 |

**Figure 4: Répartition des vulnérabilités par type**

## 3) VEILLE TECHNOLOGIQUE

A travers sa cellule de veille technologique, le CI-CERT assure la surveillance de l'environnement technologique afin de présenter les informations utiles aux parties prenantes en matière de sécurité informatique.

Pour ce faire, le CI-CERT réalise les activités suivantes :

### a) Publications d'informations de sécurité sur le site internet: 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 augmentation considérable comparativement à l'année précédente. En effet, le CI-CERT a publié sur son site Internet au cours de l'année

2012, quatre cent cinquante (450) bulletins de sécurité contre cent soixante-treize (173) en 2011 ; soit plus du double.

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

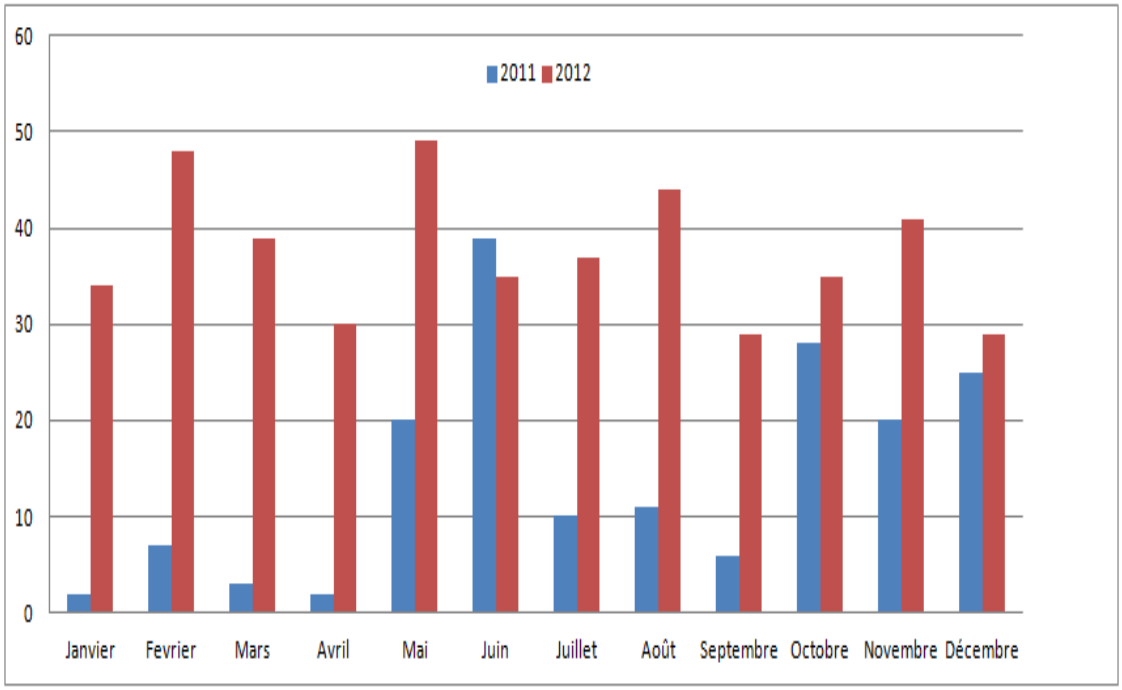



**Figure 5: Répartition des publications par mois (Janvier 2011 à Décembre 2012)**

### b) Diffusion de la Mailing-List

Au cours de l'année 2012, le CI-CERT a diffusé quatre cent cinquante (450) bulletins de sécurité et douze (12) 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 treize (13) souscriptions en 2011 à deux cent soixante-deux (262) souscriptions en 2012.

En outre l'audience du site internet du CI-CERT (www.cicert.ci) a également connu un accroissement significatif ; à raison de sept mille trois cent vingt et un (7321) visites au cours de l'année 2012, contre trois mille trois cent quarante-trois (3343) l'année précédente.

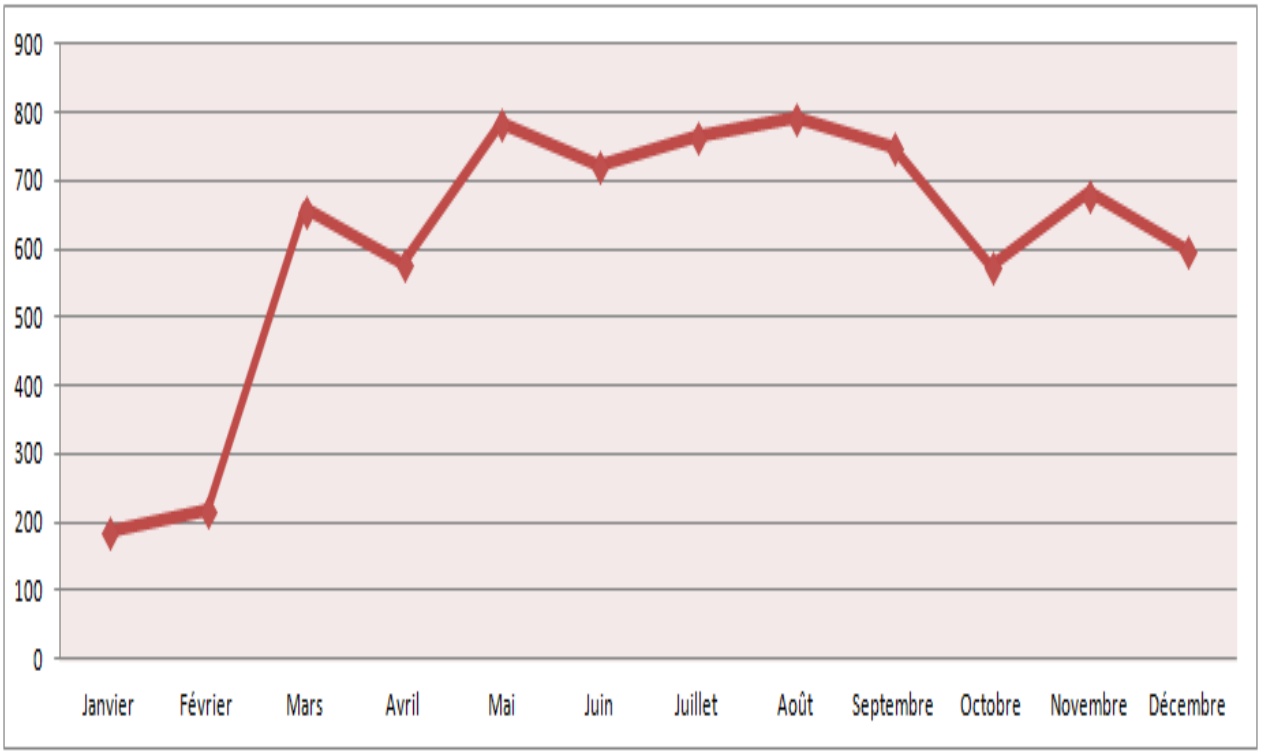



**Figure 6: Nombre d'internautes ayant visité le site web**

### c) Surveillance des Sites web

L'outil de surveillance de sites web du CI-CERT (SYSWEB) a permis d'assurer le monitoring permanent de cent quarante et un (141) sites web au cours de cette année 2012. Ce sont en l'occurrence les ressources critiques d'Institutions gouvernementales, administratives (ministère, établissements publics) et d'établissements du secteur privé (banques, entreprises de télécommunications, etc.) qui ont été « monitorées ».

## 4) DEVELOPPEMENT D'OUTILS DE SECURITE

Initié en 2009, l'outil de surveillance des sites web (SYSWEB) a connu au cours de cette année des améliorations majeures en tenant compte des exigences et besoins actuels des parties prenantes. En effet, SYSWEB s'est mué en une véritable plateforme automatisée de supervision et de surveillance de sites web dédiée à la veille technologique et à la gestion des incidents informatiques. De nouveaux modules y ont été intégrés, à savoir :

- Enregistrement et inscription automatisés à l'application via le site web (www.cicert.ci) ;
- Intégration d'un service d'alertes par e-mail ;
- Développement d'une interface cliente intégrant les processus métiers du CI-CERT en termes de traitement d'incidents informatiques (Gestion des contacts, notification des alertes par e-mail suivi des incidents, tableau de bord de gestions des incidents, rapport, statistiques, etc).

## 5) LUTTE CONTRE LA CYBERCRIMINALITE

Le CI-CERT, précurseur de la lutte contre la cybercriminalité en Côte d'Ivoire, constitue l'un des maillons essentiels de la Plateforme de Lutte Contre la Cybercriminalité (PLCC). Cette plateforme, regroupant les agents de la Police Nationale représentés par la DITT (Direction de l'Informatique et des Traces Technologiques) et des agents de l'ATCI représentés par le CI-CERT, a été créée dans le but d'apporter une réponse viable aux problèmes que pose cette activité criminelle dans notre pays.

### a) Les plaintes et dénonciations

Au total, mille huit cent quarante-six (1846) e-mails de signalement émanant des populations tant locales qu'internationales ont été enregistrés par la PLCC. Cette tendance à la hausse affirme le rôle central qu'acquiert cet organe en termes de coordination des actions de lutte contre la cybercriminalité.

Les mois de Juillet et Août ont été marqués par un grand nombre de plaintes déposées pour des affaires de cybercriminalité ; soit deux cent quatre-vingt-dix-huit (298) plaintes (43.06%) au

cours de ces deux mois, sur un total de six cent quatre-vingt-douze (692) plaintes au cours de l'année 2012.

| | Janvier | Février | Mars | Avril | Mai | Juin | Juillet | Août | Septembre | Octobre | Novembre | Décembre |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Nombre de plaintes | 57 | 36 | 23 | 37 | 50 | 24 | 126 | 172 | 56 | 41 | 48 | 22 |

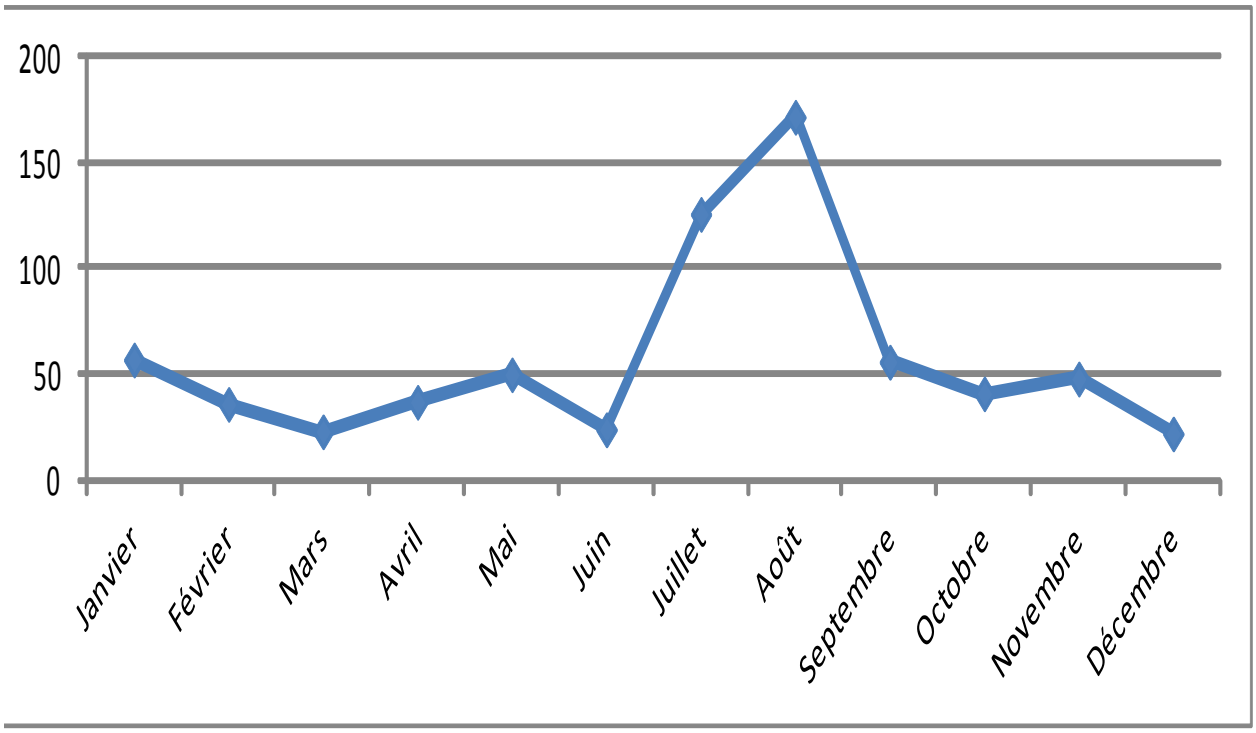
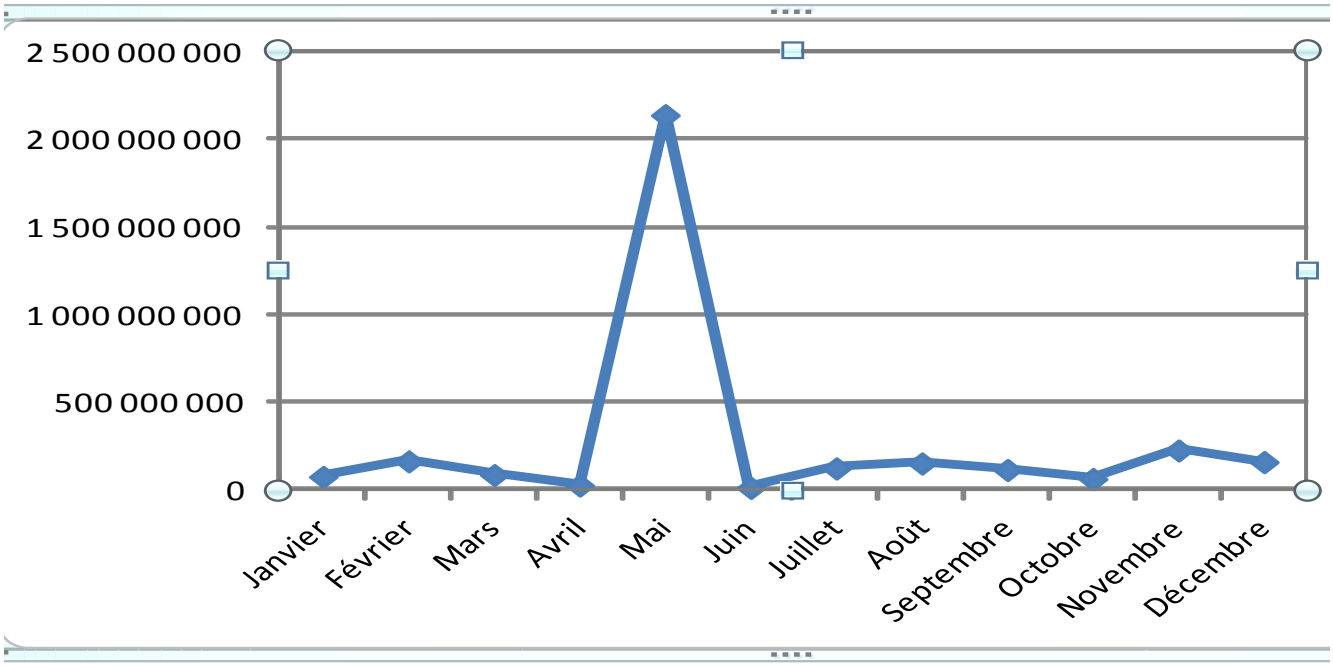



**Figure 7: Illustration des plaintes reçues**

b) Le préjudice financier

Le préjudice financier total de la cybercriminalité, enregistré par les services de la PLCC, s'élève à un montant total de trois milliards trois cent quatre-vingt-quatre millions neuf cent soixante-douze mille quatre-vingt-treize (3.384.972.093) FCFA.

| TYPE D'ARNAQUE | PERTE FINANCIERE | POURCENTAGE |
|---|---|---|
| Janvier | 79 117 885 | 2,34 |
| Février | 167 678 352 | 4,95 |
| Mars | 89 315 950 | 2,64 |
| Avril | 29 886 447 | 0,88 |
| Mai | 2 142 203 981 | 63,29 |
| Juin | 16 198 150 | 0,48 |
| Juillet | 127 435 833 | 3,76 |
| Août | 155 376 084 | 4,59 |
| Septembre | 118 170 830 | 3,49 |
| Octobre | 66 968 443 | 1,98 |
| Novembre | 229 600 549 | 6,78 |
| Décembre | 163 019 589 | 4,82 |
| **TOTAL** | **3 384 972 093** | **100** |




c) La répression

La PLCC s'est doté de moyens techniques et opérationnels, en vue d'accentuer la répression de cette activité criminelle. Au total, elle a procédé à l'interpellation de soixante et onze (**71**) suspects, dont cinquante et un (**51**) ont été condamnés à des peines de prison par la Justice Ivoirienne ; soit un pourcentage de 71,83% de suspects incarcérés.

Les détails des interpellations et incarcération sont consignés dans le tableau suivant :

| Mois | Nombre d'interpellés | Nombre de déférés | Nombre d'interpellés Cumul Année 2012 | Nombre de déférés Cumul Année 2012 | Peine minimale infligée |
|---|---|---|---|---|---|
| **Janvier** | 05 | 05 | 05 | 05 | - |
| **Février** | 04 | 03 | 09 | 08 | 6 mois |
| **Mars** | 04 | 03 | 13 | 11 | - |
| **Avril** | 07 | 07 | 20 | 18 | 2 mois |
| **Mai** | 15 | 10 | 35 | 28 | - |
| **Juin** | 07 | 04 | 42 | 32 | 1 mois |
| **Juillet** | 09 | 05 | 51 | 37 | 1 mois |
| **Août** | 09 | 06 | 60 | 43 | 2 semaines |
| **Septembre** | 03 | 02 | 63 | 45 | - |
| **Octobre** | 04 | 02 | 67 | 47 | - |
| **Novembre** | 04 | 04 | 71 | 51 | - |
| **Décembre** | 00 | 00 | 71 | 51 | - |

**Tableau 4: Récapitulatif des interpellations et incarcérations**

# III. COORDINATION ET COLLABORATION

## 1) AU PLAN INTERNATIONAL

### a) Mission d'audit UIT-IMPACT

Dans le cadre du Programme 3 du Plan Opérationnel Doha adopté à la Conférence Mondiale de Développement des Télécommunications (CMDT) 2006, le BDT assiste les pays africains dans l'évaluation de leur préparation à l'établissement de Centres de Veille sur la Cybersécurité (CERT). Ces activités sont menées dans le cadre de la collaboration entre l'Union Internationale des Télécommunications (UIT) et IMPACT (International Multilateral Partership Against Cyber Threats), et suivant le Programme mondial cyber sécurité (GCA). En effet, le CI-CERT a fait une demande d'adhésion au programme IMPACT. Ainsi dans le cadre de son partenariat avec UIT-IMPACT, deux (02) experts de ladite organisation ont effectués une mission d'audit du 17 au 22 Juin 2012 à Abidjan. L'objectif de cette mission était entre autres la réalisation d'un audit des ressources du CI-CERT, en vue de l'optimisation des procédures et méthodes de travail, en vue de la finalisation de son adhésion au programme UIT IMPACT.
Cette mission s'est soldée par l'adhésion officielle de la Côte d'Ivoire au programme à travers la signature de documents officiels entre le Directeur Général de l'ATCI et le Secrétaire général de l'UIT à ITU Telecom World 2012 à Dubaï, aux Emirats Arabe Unis.

### b) Adhésion à la plateforme RIPE ATLAS

L'adhésion à cette plateforme permet au CI-CERT de disposer d'une sonde de mesures des flux de connectivités Internet et le volume de données transitant sur les cyberespaces des différents membres et du monde en général.

c) Collaboration avec le CERT Espagnol concernant les activités malveillantes sur les réseaux des opérateurs de téléphonie et des fournisseurs d'accès internet

Le CI-CERT a établi des liens de coopération étroits avec le CERT espagnol dans le cadre de la résolution de nombreuses attaques de type BOTNET. Provenant essentiellement du cyberespace Ivoirien, ces attaques massives avaient pour cible des ressources situées dans le cyberespace Espagnol. La collaboration entre les deux organes a débouché sur la mise en route de solutions viables, conduisant à la gestion des incidents informatiques (BOTNET).

d) Participation aux échanges dans le cadre des activités du réseau des CERT Africains (AfricaCERT)

Le CI-CERT est membre de la communauté des Certs africains dénommée (AfricaCERT), organisation qui a pour but de promouvoir une culture de cybersécurité en Afrique, de soutenir les efforts ou initiatives en sécurité de l'information sur le continent et à créer un réseau des CERTs africains.

e) Participation à la session de formation sur la technologie IPV6 et le projet de déploiement national de IPV6, organisée par AFRINIC

Dans le cadre du renforcement des capacités de ses agents, le CI-CERT a participé du 21 au 24 Août 2012, à une session de formation sur les enjeux de la migration d'IPv4 vers IPv6. Cette session de formation a été l'occasion pour les agents de parfaire leurs connaissances sur cette technologie, en vue de participer activement à la sécurisation des ressources informatiques critiques utilisant IPv4 qui reposeront sur ce nouveau protocole Internet et de participer aux bancs d'essai ou laboratoire IPv6 sur le plan national.

## 2) AU PLAN NATIONAL

### a) Déjeuner-débat organisé en partenariat avec IVOPREST

En partenariat avec le CI-CERT, le cabinet de formation en sécurité informatique IVOPREST a organisé un déjeuner-débat à l'attention des DSI (Directeur des Systèmes d'Information) des entreprises installées en Côte d'Ivoire le 22 Juin 2012. Cet évènement a enregistré la présence d'un grand nombre de visiteurs, notamment de plusieurs chefs d'entreprises et experts travaillant dans le domaine des TICs. L'objectif était de présenter les activités du CI-CERT et d'établir des liens étroits de collaboration sur le plan national.

### b) Atelier d'échange entre le CI-CERT, les DSI et les webmasters des sites internet du domaine « gouv.ci »

Cet atelier d'échange s'est tenu le Jeudi 02 Août 2012 et a été un réel cadre d'échange et de partage de connaissances. Il a permis entre autre de mieux faire connaître les activités et services offerts par le CI-CERT, ouvrir le débat sur la sécurité des infrastructures critiques des organismes gouvernementaux et renforcer la coopération entre les différents acteurs sus cités.

### c) Participation aux JNTIC

Le CI-CERT a participé du 15 au 18 Mai 2012 aux Journées Nationales des Technologies de l'Information et de la Communication (JNTIC), qui se sont déroulées au palais de la Culture d'Abidjan-Treichville. Cette lucarne a été l'occasion pour l'équipe de faire connaître son champ d'action, ses domaines de compétences et les services offerts au grand public. Cette campagne a été une vraie réussite dans l'ensemble, comme en témoigne les résultats obtenus (audience des conférences, nombres de visiteurs par jour au stand, souscriptions aux services du CI-CERT).

d) Participation à la campagne de sensibilisation sur la cybersécurité initiée par GOOGLE

Le CI-CERT a participé en collaboration avec GOOGLE et IGICI à l'organisation et au lancement d'une campagne nationale de sensibilisation sur la cybersécurité. Cette campagne prévue pour démarrer effectivement en 2013 se situe dans la ligne droite du plan d'action du CI-CERT en termes de formation et de sensibilisation.

e) Signature de conventions de partenariat avec les opérateurs de téléphonie mobile (ORANGE, MTN et MOOV)

En vue d'établir un mécanisme de traitement accéléré des réquisitions de la Police dans le cadre de la lutte contre la cybercriminalité, des conventions de partenariat ont été signées avec les principaux opérateurs de téléphonie mobile du pays. Ces conventions permettront d'accélérer les procédures de traitement des réquisitions et intensifier ainsi la lutte contre la cybercriminalité.

# IV. DIFFICULTES RENCONTREES

### 1) Absence de cadre juridique

L'absence de règles juridiques précises en matière de cybersécurité (loi sur la cybercriminalité, organes institutionnels, etc.) pose un véritable frein à l'action du CI-CERT. Bien que disposant de compétences techniques et matérielles de haut niveau, le CI-CERT reste dans bien des cas impuissant face à certains problèmes touchant à la cybersécurité nationale.

### 2) Collaboration avec les parties prenantes

Dans l'accomplissement de ses missions, le CI-CERT s'est trouvé confronté à de nombreuses difficultés, tenant principalement aux questions de collaboration avec les parties prenantes.

En effet, grand nombre de parties prenantes gestionnaires de ressources Internet critiques de l'Etat Ivoirien, restent encore très peu coopératifs quant aux recommandations et avis de sécurité émis par le CI-CERT.

Cet état de fait pose inévitablement la question du pouvoir coercitif dont devrait disposer le CI-CERT, en vue d'assurer un niveau de sécurité suffisant des infrastructures critiques nationales.

# V. PERSPECTIVES ET PROJETS

Le CI-CERT entend renforcer à moyen terme son image et sa notoriété, tant au plan national qu'international. Pour ce faire une stratégie sera mise en place, avec pour objectifs de :

- Accroître la notoriété du CI-CERT sur le plan national et international ;
- Avoir la reconnaissance internationale par l'adhésion à la grande communauté des CERTS (Forum for Incident Response and Security Teams : FIRST) ;
- Organiser une série de séminaires de formation à l'endroit des Directeurs des Systèmes d'Informations et responsables des infrastructures informatiques nationales sur la sécurité des sites web en ligne ;
- Accroître les services offerts aux parties prenantes ;
- Etre le point de coordination de tous les incidents sur le plan national ;
- Renforcer les capacités des agents de l'équipe à travers un plan de certification de haut niveau. ;
- Renforcer la collaboration entre les différents partenaires.

CI-CERT

Côte d'Ivoire - Computer Emergency and Response Team

## NOUS CONTACTER :

(225) 20 22 91 97

(225) 20 22 91 99

info@cicert.ci

www.cicert.ci

## SIGNALER UN INCIDENT INFORMATIQUE

incidents@cicert.ci