Cote d'Ivoire Computer Emergency Response Team

RAPPORT D'ACTIVITES

19 juin – 31 Décembre 2009

SOMMAIRE

AVANT PROPOS

La cybercriminalité désigne l'ensemble des infractions pénales susceptibles d'être commises sur les réseaux de télécommunications en général et plus particulièrement sur Internet. Ces dernières années, ce phénomène a fortement affecté l'image de la Côte d'Ivoire au point d'être classé pays à risque dans les transactions en ligne internationales. Une étude realisée par le CIRES[1] a montré que 71% des internautes jugent le niveau de criminalité sur le réseau Internet ivoirien important.

Vu l'ampleur du phénomène, l'Agence des Télécommunications Côte d'Ivoire (ATCI) a entrepris diverses actions dans le cadre de la lutte contre la cybercriminalité notamment des ateliers, des interviews, des émissions télé et radio et des conférences. La dernière en date est la conférence régionale africaine sur la Cybersécurité[2] sous le thème: "Bâtir un espace numérique de confiance en Afrique". C'est à l'issue de ces réflexions que l'ATCI a décidé de mettre en place un centre de veille, de surveillance et traitement des menaces et incidents sur les réseaux d'information au niveau national. Ce centre est dénommé Cote d'Ivoire Computer Emergency Response Team (CICERT).

Le CICERT a débuté ses activités le 19 juin 2009 avec comme objectif principal de lutter contre la cyberescroquerie. Depuis cette date, de nombreuses actions ont été menées visant à freiner l'expansion de ce phénomène. Le présent document est le rapport annuel ; il relate les principales activités et les résultats obtenus.

[1] : Centre Ivoirien de Recherches Economiques et Sociales

[2] : voir le site de la conférence africaine pour plus amples informations. www.afcybersec.org

1 - PRESENTATION DU CICERT

1.1 Création

Le centre de surveillance et des traitements des menaces et incidents la Côte d'Ivoire s'appelle **CICERT** (*Cote d'Ivoire Computer Emergency Response Team*) a été crée par l'ATCI et a débuté ses activités le 19 juin 2009.

Le site web du CICERT est : www.cicert.ci et son adresse Email de contact est info@cicert.ci.

1.2 Missions

Le CICERT a pour ambition de contribuer à assurer la confiance dans l'utilisation de l'Internet par la communauté des Internautes ivoiriens (le secteur public, le secteur privé et les particuliers).

A cet effet, l'équipe CICERT s'est assignée les missions suivantes :

- Mettre fin aux escroqueries via Internet venant de la Côte d'Ivoire ;
- Sensibiliser la population des dangers à l'utilisation des Tics ;
- Promouvoir l'utilisation appropriée des technologies de l'information et de la communication ;
- Proposer des programmes de formation de haut niveau dans les différentes branches de la sécurité des systèmes d'information ;
- Faciliter la communication entre les professionnels et les experts travaillant dans le domaine de la sécurité informatique ;

1.3 Organisations

Le CICERT est constitué d'une équipe technique comprenant 6 Ingénieurs informaticiens spécialisés en sécurité informatique.

Cette équipe exécute les tâches suivantes :

- Traiter les plaintes portant sur l'escroquerie sur Internet reçues en ligne à l'adresse info@cicert.ci,
- Détecter et résoudre les incidents informatiques ;
- Publier des bulletins de vulnérabilités
- Sensibiliser sur les nouvelles méthodes d'arnaques

1.4 Ressources matérielles

L'équipe technique dispose des ressources matérielles ci-dessous :

Tableau 1. Ressources du CICERT

DESIGNATION		**QUANTITE**
Ordinateurs de bureau	Workstations	06
	Firewall monté sous linux (IP table)	01
	MS Forefront threat manager	01
Ordinateur portable		03
Disques durs externes de 512 Gbo		02
Routeur		02
Switch		02
Imprimantes		02
Liaison internet dédiée de 512 kb/s		01
Onduleur		01
Scanneur		01
Lignes téléphoniques		03
Fax		01

2 – ACTIVITES

2.1 Les statistiques de la lutte contre la cyber-escroquerie

Dans le cadre de la lutte contre la cybercriminalité, le CICERT et la Sous Direction des Traces Technologiques (SDTT) de la Police scientifique collaborent dans le cadre d'une plateforme. Les réalisations de la plate forme sont présentées à travers les statistiques suivantes.

2.1.1 Classification des arnaques

6 types d'arnaques ont été recensés depuis le début des activités du CICERT ; ce sont :

- L'arnaque à Héritage ;
- Love Tchat ;
- Loterie ;
- Usurpation de comptes mails ;

- Arnaque aux Grains ;
- Commande avec promesse d'achat ;
- Usurpation d'identité ;
- Arnaque par Téléphone Portable.

Pour la description de chaque type d'arnaque se reporter en annexe.

2.1.2 Les dénonciations

Le CICERT a enregistré 950 dénonciations en 2009. Ces dénonciations représentent l'ensemble des mails des victimes de cyber-escroquerie et des Spams reçus sur info@cicert.ci.

Les dénonciations parviennent au CICERT par :

- E-mails (info@cicert.ci);
- appels téléphoniques (20 22 91 99 / 20 22 91 97)
- la police (les plaintes déposées auprès de la police ou du Parquet).

Les plaignants sont en général :

- des personnes physiques ou particulières
- des ONGs et les associations
- des entreprises (les banques ; sociétés Immobilières, etc)

✓ **Les dénonciations par types d'arnaques**

La répartition des dénonciations par types d'arnaques est présentée ci-dessous sous formes de tableau et de graphique :

Tableau

Types d'arnaques	**Chiffres**	**Pourcentages**
Héritage	285	30,0%
Love Tchat	177	18,6%
Loterie	163	17,2%
Usurpation de comptes mails	80	8,4%
Arnaque aux Grains	71	7,5%
Commande avec promesse d'achat	70	7,4%
Usurpation d'identité	64	6,7%
Arnaque par Téléphone Portable	40	4,2%
Total	**950**	**100%**

Tableau 2. Statistiques des dénonciations / types d'arnaques en 2009

Graphique

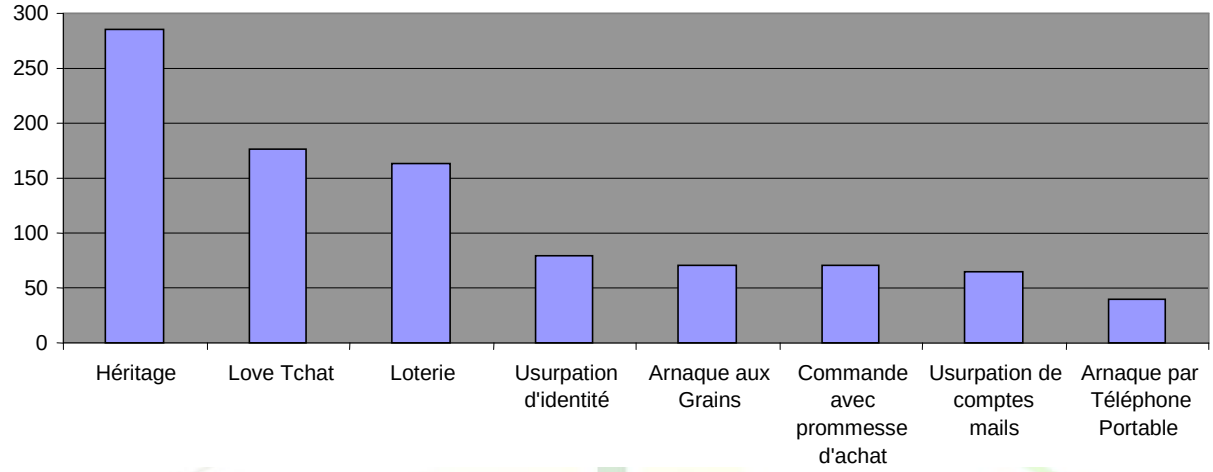

Figure 1. Répartition des dénonciations/types d'arnaques en 2009

La figure 1 montre la répartition des d'arnaques dénoncés sur le cyberespace Ivoirien au cours du deuxième semestre de l'année 2009.

Nous observons que l'arnaque à l'héritage, love tchat et à la loterie sont les plus dénoncés avec des taux respectifs de 30%, 18.6% et 17.2%. Ceci s'explique par le fait que ce sont les techniques les plus anciennes et les plus répandues.

A contrario, nous remarquons le faible taux des 5 derniers types dû au fait qu'elles sont récentes.

- ✓ **Classification des arnaques dénoncées par pays d'origine**

Les 950 dénonciations d'arnaques enregistrées par le CICERT ne proviennent pas toutes du territoire de la Côte d'Ivoire. En effet, nous avons découvert que des arnaques dénoncées par les internautes proviennent des certains pays (territoire) de la sous région.

La répartition des dénonciations par pays d'origine est présentée ci-dessous sous formes de tableau et de graphique :

Tableau

Pays	Chiffres	Pourcentages
Cote d'Ivoire	783	82,4%
Bénin	68	7,16%
Nigeria	63	6,6%
Burkina-Faso	20	2,1%
Togo	10	1%
Mali	3	0,3%
Ghana	2	0,2%
Afrique du sud	1	0,1%
TOTAL	950	100%

Tableau 3. Statistiques des dénonciations pays d'origine en 2009

Graphique

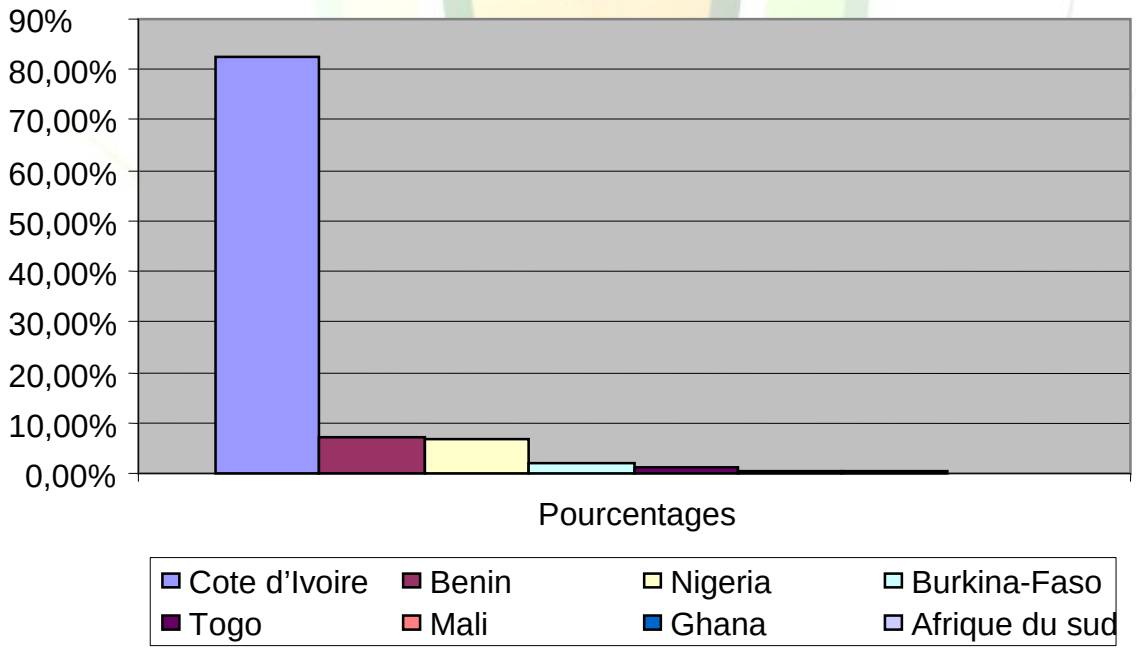

Figure 2. Dénonciation par pays d'origine en 2009

2.1.3 Les cyberescrocs interpellés

76 personnes suspectées de mener des activités de cyber escroquerie ont été interpellées.

- ✓ Les personnes interpellées par types d'arnaques

La répartition des personnes interpellées par types d'arnaques est présentée ci-dessous sous formes de tableau et de graphique :

Tableau

Types d'arnaques	interpellés	Pourcentage
Love Tchat	30	39,5%
Héritage	19	25,0%
Usurpation d'identité	16	21,1%
Arnaque par Téléphone Portable	4	5,3%
Loterie	4	5,3%
Arnaque aux Grains	2	2,6%
Commande avec promesse d'achat	1	1,3%
Usurpation de comptes mails	0	0,0%
Total	76	100,0%

Tableau 4. Les personnes interpellées par types d'arnaques

Graphique

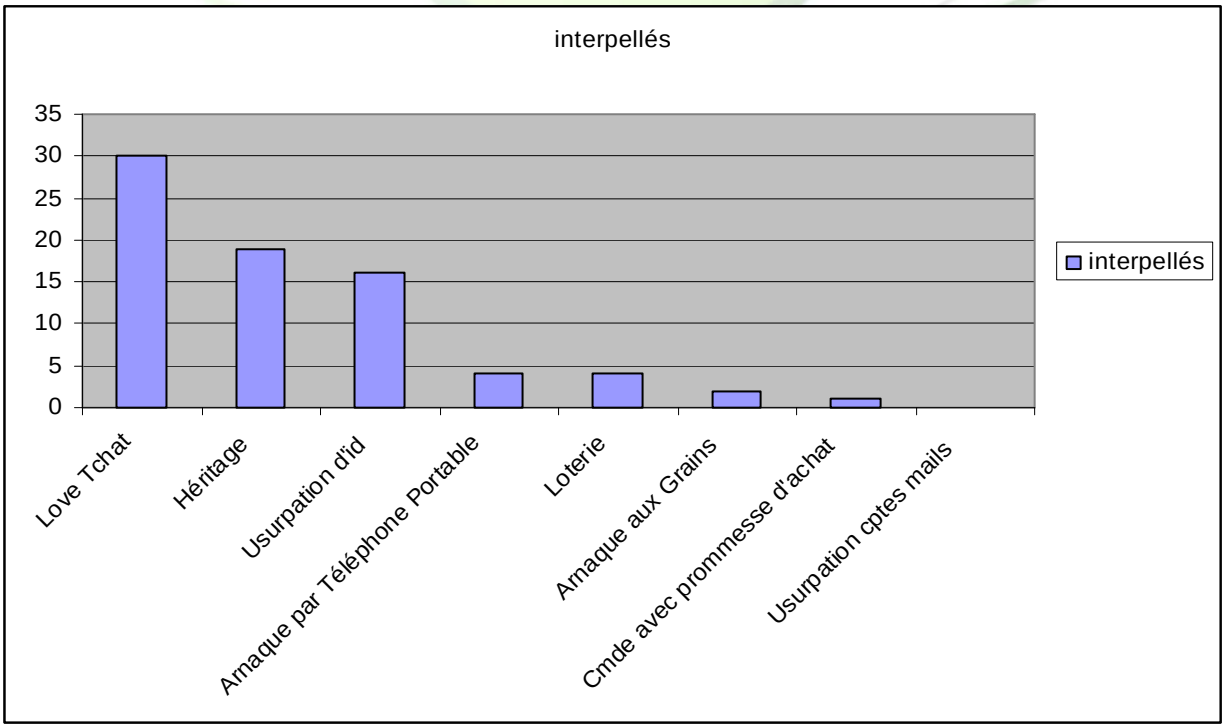

Figure 3. Les personnes interpellées par types d'arnaques

Nous observons que la plus part des suspects interpellés sont ceux qui pratiquent le love tchat. En effet, c'est l'une des techniques d'arnaques les plus courantes dans les cybercafés car très facile à réaliser.

- ✓ Les personnes interpellées par nationalité

La répartition des personnes interpellées par nationalité est présentée ci-dessous sous formes de tableau et de graphique :

Tableau

Nationalité	Effectif	Pourcentage
Ivoirienne	43	56,7%
Nigériane	20	26,3%
Togolaise	5	6,6%
Béninoise	2	2,6%
Burkinabé	2	2,6%
Camerounaise	2	2,6%
Malienne	2	2,6%
TOTAL	**76**	**100%**

Tableau 5. Les personnes interpellées par nationalité

Graphique

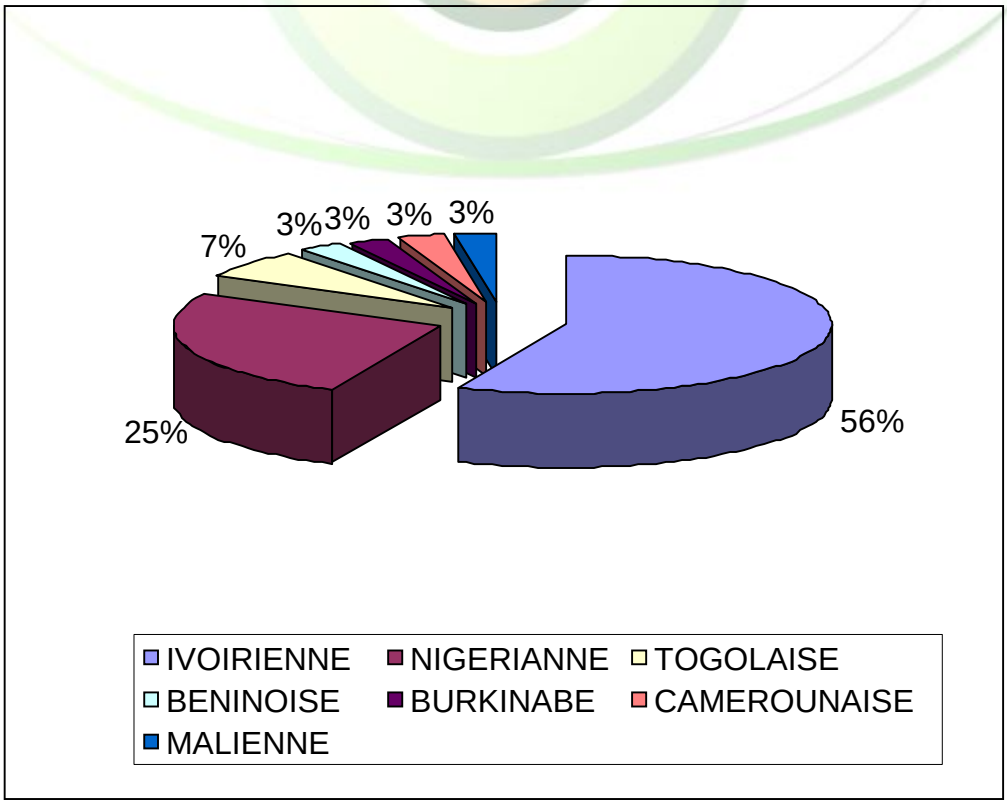

Figure 4. Les personnes interpellées par nationalité

Les citoyens ivoiriens sont de loin les personnes les plus impliquées dans l'activité de cyber escroquerie avec plus de la moitié des personnes interpellées (56%), suivis des ressortissants nigérians (25%). Ces chiffres montrent bien que les internautes ivoiriens sont entrain de devenir des cyberescrocs.

- ✓ Les personnes interpellées par Commune (Abidjan)

La répartition des personnes interpellées par commune d'Abidjan est présentée ci-dessous sous formes de tableau et de graphique :

Tableau

Commune	Effectif	Pourcentage
COCODY	35	46,1%
YOPOUGON	14	18,4%
KOUMASSI	11	14,5%
PORT BOUET	8	10,5%
MARCORY	5	6,6%
TREICHVILLE	3	3,9%
TOTAL	**76**	**100%**

Tableau 6. Les cyberescrocs interpellés par Commune

Graphique

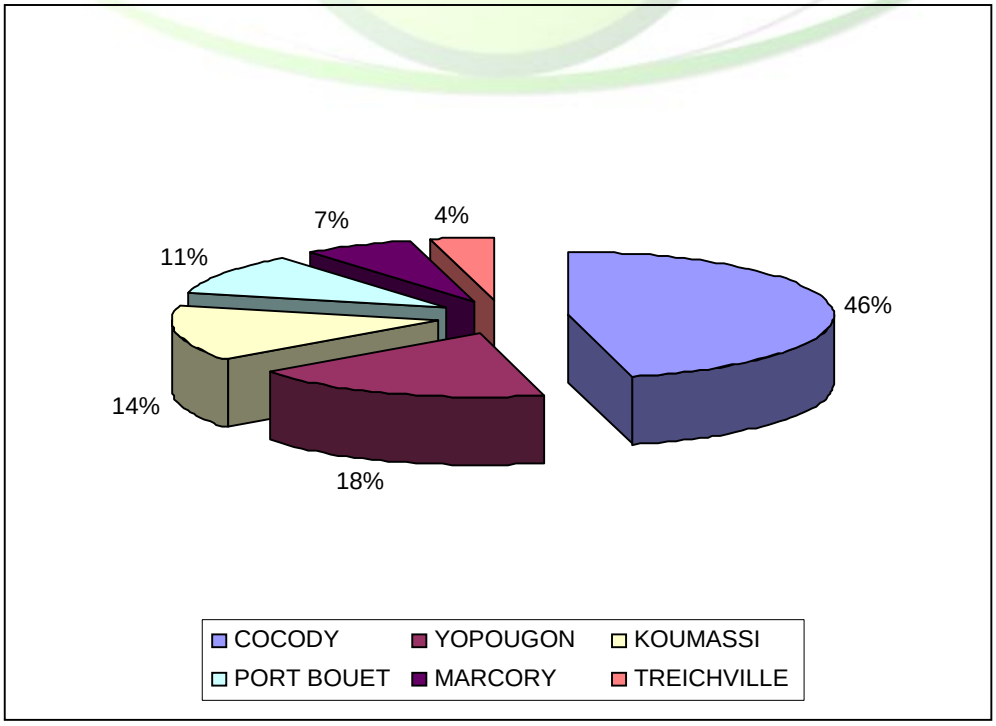

Figure 5.Les personnes interpellées par Commune d'Abidjan

La commune de Cocody est la commune de la ville d'Abidjan où résident la majorité des cyberescrocs interpellés (46%). Elle semble présenter les conditions les plus favorables pour la pratique des activités d'escroqueries via Internet.

2.1.4 Les cyberescrocs déférés

Parmi les personnes interpellées, 37 cyberescrocs ont été déférés devant le Parquet d'Abidjan Plateau.

- ✓ Cyberescrocs déférés par types d'arnaques

La répartition des cyberescrocs déférés par types d'arnaques est présentée ci-dessous sous formes de tableau et de graphique :

Tableau

Types d'arnaques	déférés	Pourcentage
Héritage	15	40,5%
Usurpation d'id	6	21,6%
Love Tchat	6	21,6%
Loterie	4	10,8%
Arnaque par Téléphone Portable	4	0,0%
Commande avec promesse d'achat	2	5,4%
Arnaque aux Grains	0	0,0%
Usurpation de comptes mails	0	0,0%
Total	37	100,00%

Tableau 7. Les cyberescrocs déférés types d'arnaques

Graphique

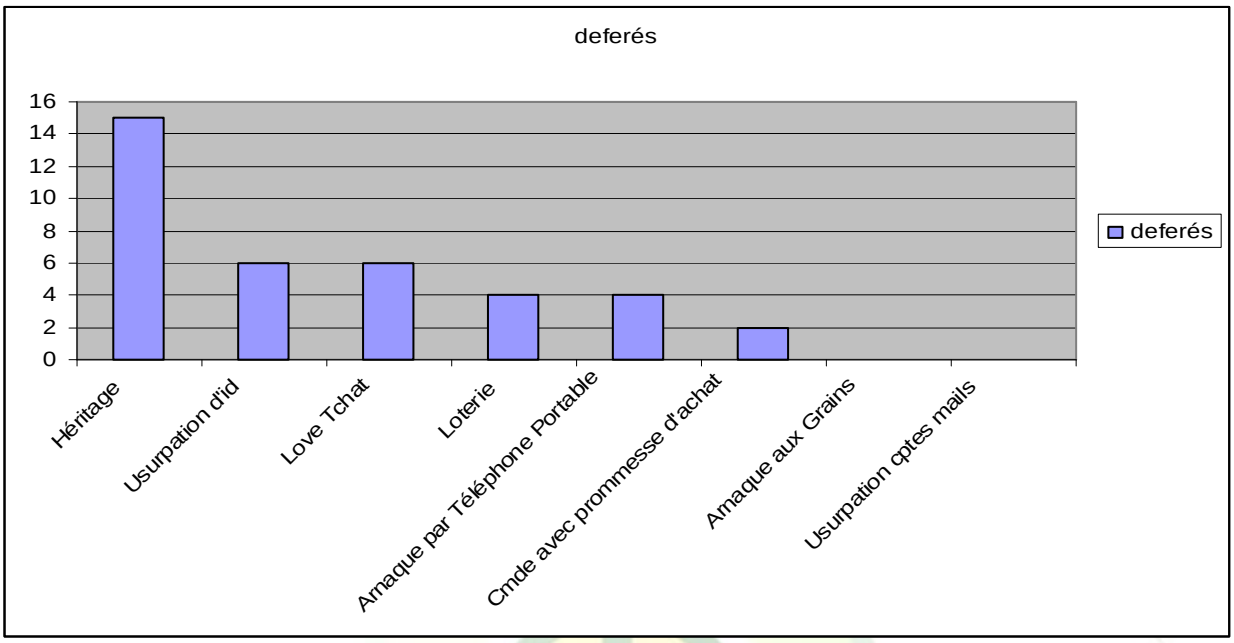

Figure 6. Les cyberescrocs déférés par types d'arnaques

- ✓ Les cyberescrocs déférés par nationalité

La répartition des cyberescrocs déférés par nationalité est présentée ci-dessous sous formes de tableau et de graphique :

Tableau

Nationalité	**Nombre**	**Pourcentage**
Ivoirienne	23	62,2%
Nigériane	11	29,7%
Béninoise	1	2,7%
Togolaise	1	2,7%
Camerounaise	1	2,7%
Total	37	100%

Tableau 8. Les cyberescrocs déférés par nationalités

Graphique

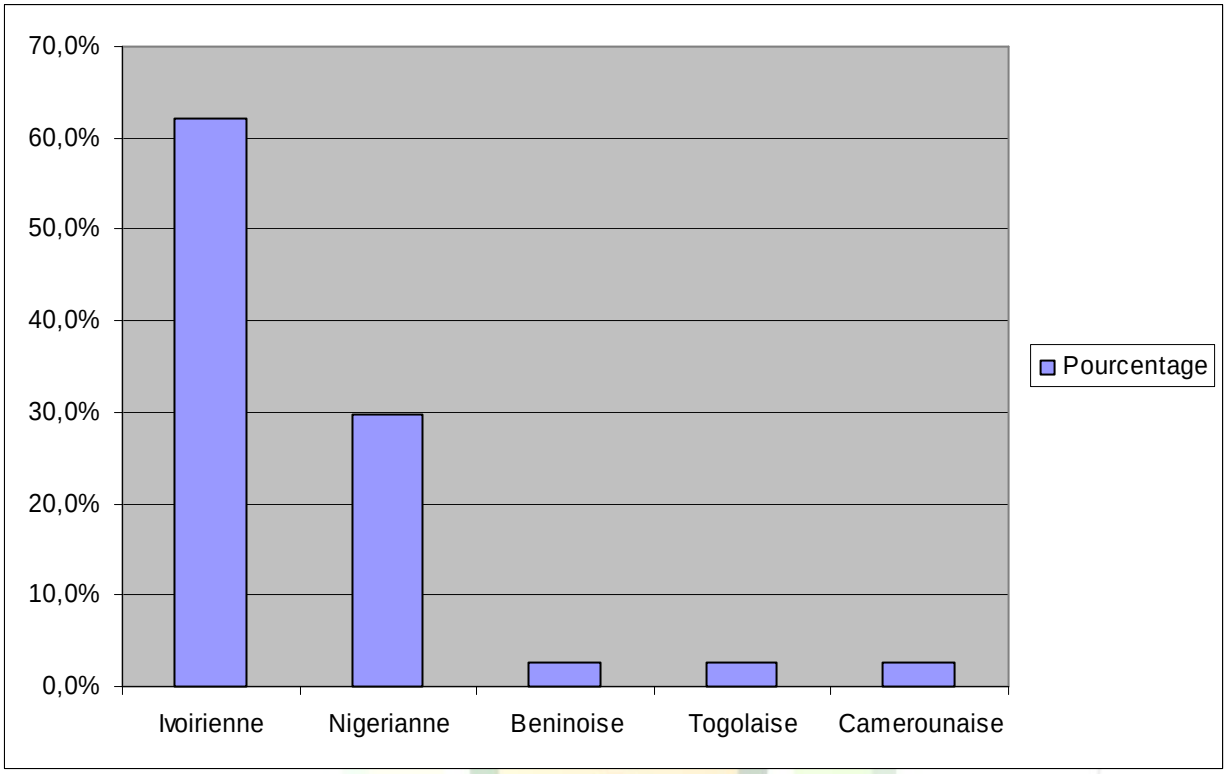

Figure 7. Les cyberescrocs déférés par nationalités

✓ Les cyberescrocs déférés par Commune (Abidjan)

La répartition des cyberescrocs déférés par Commune d'Abidjan est présentée ci-dessous sous formes de tableau et de graphique :

Tableau

Commune	Nombre	Pourcentages
Cocody	13	35,1%
Yopougoon	7	18,9%
Koumassi	5	13,5%
Treichville	4	10,8%
Port-bouet	4	10,8%
Marcory	4	10,8%
TOTAL	37	100%

Tableau 9. Les cyberescrocs déférés par Commune

Graphique

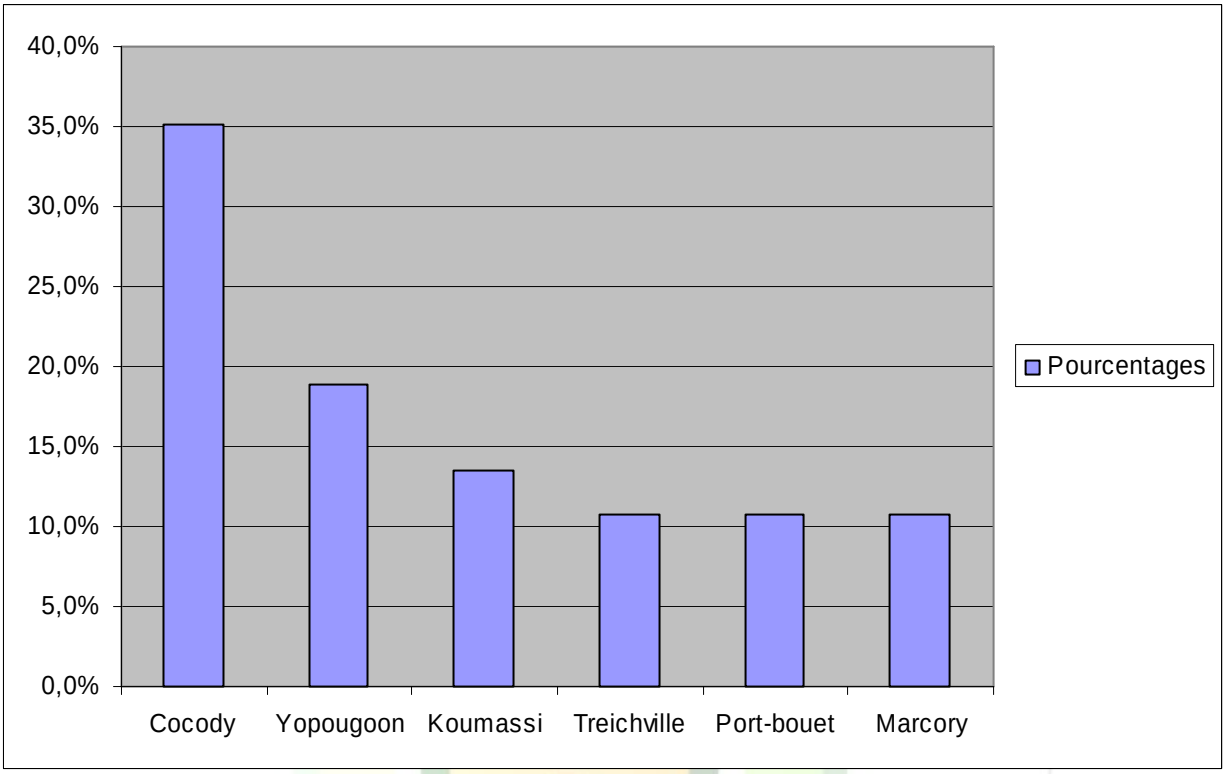

Figure 8. Les cyberescrocs déférés par Commune

2.2 Les audits informatiques et perquisitions de comptes mails

Lors de l'interpellation d'un cyberescrocs, il arrive que la police saisisse des ordinateurs. Le CICERT, à la demande de la police, perquisitionne les comptes mails et au besoin fait un audit sur le matériel informatique saisi à la recherche d'éléments en rapport avec l'escroquerie.

Audit et Perquisition	**Nombre**	**Pourcentage**
Audits techniques	50	18,2%
Perquisition E-mail	224	81,7%
Total	274	100%

Tableau 10. Audits et Perquisitions

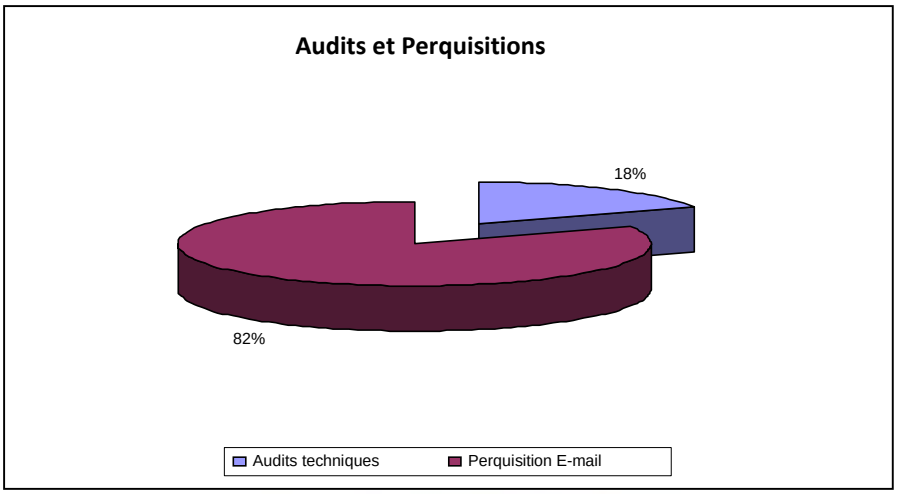

Figure 9.Audits et Perquisitions

2.3 L'assistance à tiers

Les usagers d'Internet résidant ou non sur le territoire ivoirien contactent le CICERT en vue d'être assistés. Cette assistance à tiers consiste à :

- aider les victimes pour récupérer les entêtes SMTP
- prodiguer des conseils à une victime d'arnaques et à lui indiquer la démarche à suivre pour porter plainte
- sensibiliser le public sur les arnaques via Internet
- donner des conseils afin d'éviter d'être arnaqué

2.4 Les bulletins de sécurité

Outre la lutte contre la cyber-escroquerie, une autre activité du CICERT est la veille sur les menaces, les vulnérabilités ainsi que les cyber-attaques. Dans le cadre de cette activité, le CICERT effectue des recherches sur Internet pour être informé des failles découvertes sur les systèmes d'exploitations et autres logiciels publiés en général par des sociétés d'édition de logiciels.

Le CICERT publie alors des bulletins de sécurité qui peuvent être répartis en deux catégories : Les alertes et les mises à jour.

Les mises à jour sont des informations complémentaires ou des correctifs à un bulletin de sécurité existant. Ils constituent un mécanisme permettant de libérer rapidement des informations importantes d'une façon moins structurée.

Les alertes sont des informations détaillées sur des menaces ou des vulnérabilités spécifiques.

Le CICERT a publié sur son site web en 2009, **84 bulletins de sécurité** repartis comme suit : **44 avis d'alertes** et **40 avis de mise à jour**. Le graphique ci-dessous illustre cette activité.

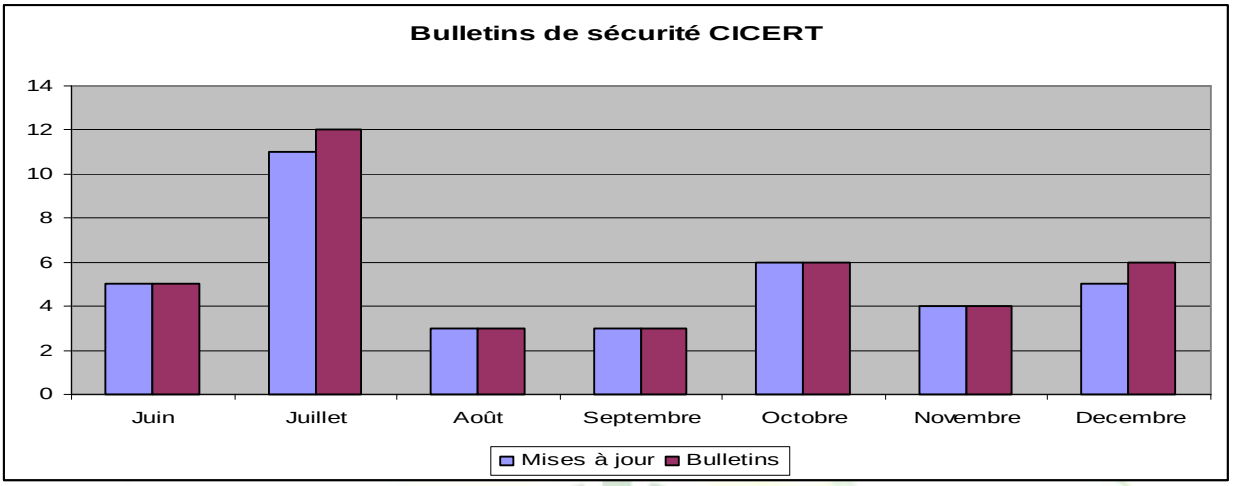

Figure10 .Editions des bulletins de sécurité

2.5 Développement d'outils propres au CICERT

Nous présentons succinctement les ressources logicielles développées par le CICERT.

2.5.1 Base de données des cybercafés : Logiciel INM

Face aux lenteurs et quelque fois aux refus de certains fournisseurs d'accès Internet (FAI) de donner des informations sur la localisation géographique (de la personne qui utilise une adresse IP), et en vue de surmonter cet obstacle, le CICERT a développé un logiciel baptisé INM (identification, Numérisation et Mappage). Après avoir déterminé une adresse IP d'un mail suspect, il est possible en utilisant le logiciel de voir en temps réels :

- Le nom du cybercafé ;
- La localisation géographique ;
- Et les coordonnées GPS

Le domaine de fonctionnement de l'application se limite aux cybercafés.

2.5.2 Logiciel de gestion des dénonciations : DOCKEUR

La conception de cette application contribue au bon fonctionnement du CICERT. Cette application permet d'enregistrer toutes les dénonciations reçues par le CICERT.

Pour chaque dénonciation reçue, l'application DOCKEUR effectue un enregistrement dans une base de données et génère automatiquement un rapport de traitement au format pdf.

Ce logiciel est actuellement fonctionnel et accessible à tous les postes authentifiés sur le réseau local du CICERT.

2.5.1 Le site web du CICERT

Depuis sa mise en place, le CICERT a développé et communiqué diverses informations à travers son site web (www.cicert.ci). Sur ce site l'on trouve les contacts et publications (bulletins, articles, et des statistiques, etc.) du CICERT.

3 – DIFFICULTES AVEC LES PARTIES PRENANTES

Dans l'exercice de ses activités, le CICERT rencontre des difficultés qui l'empêchent d'être plus efficace. En effet, malgré l'émission de réquisitions (DE PAR LA LOI) conjointement signées par la police et le parquet, donc respectant la procédure réglementaire en la matière, les exploitants des réseaux d'information (opérateurs de réseau et fournisseurs d'accès Internet) ne répondent pas aux sollicitations ou alors répondent avec des délais trop longs.

3.1 Fournisseurs d'accès a Internet (FAI)

Des adresses IP sont extraites des mails de dénonciations reçus des victimes.
L'adresse IP renvoie à la machine utilisée par le cyberescroc pour envoyer le message.
Les requêtes sont donc faites aux FAI pour donner la localisation de la machine et l'identité de l'abonné.
Le tableau ci-dessous donne la répartition par FAI des adresses IP envoyés au cours de l'année 2009.

Fournisseurs d'accès a Internet (FAI)	IP Suspectées d'escroquerie	Pourcentages
Aviso	721	79%
Afnet	105	11,5%
Alink Telecom	85	9,3%
VipNet	2	0,2%
Total	913	100%

Tableau 11.Repartition du nombre d'IP suspectes/ FAI

AVISO : Les vingt premières réquisitions émises à AVISO ont reçues un écho favorable. Par la suite, toutes les autres réquisitions sont restées sans réponses. Cela a entraîné une grande inefficacité et un ralentissement dans nos activités.

AFNET : La non conservation des fichiers journaux (logs) des clients ne permet pas de localiser l'utilisateur d'une adresse IP.

ALINK : La non conservation des fichiers journaux (logs) des clients et le fait qu'il soit possible que plusieurs personnes se connectent simultanément et à des endroits différents à partir d'un seul compte ne permettent pas de localiser l'utilisateur d'une adresse IP.

ViPNET : aucune difficulté

3.2 Opérateurs de réseaux (téléphonie fixe et mobile)

Difficultés pour avoir les informations sur l'identité et la situation géographique de l'escroc à partir des numéros téléphoniques que celui-ci utilise.

3.3 Etablissement bancaire

Difficultés pour avoir les informations sur l'identité d'une personne utilisant un compte bancaire servant au cyberescroc de recevoir de l'argent.

3.4 Western Union

La diversité du réseau Western Union constitue un frein à la bonne collaboration avec la plate forme pour avoir l'information sur l'agence et le payeur d'un transfert d'argent fait à un cyberescroc.

4 – PERSPECTIVES

Pour l'année 2010, nous avons recensés les projets qui permettront au CICERT d'accroître ses performances.

4.1 Collaboration avec les FAI

La collaboration entre le CICERT et les FAI apparaît fondamentale, car lorsque le CICERT détermine une adresse IP, seuls les FAI sont en mesure de fournir les éléments permettant de retrouver le cyberescroc. Une procédure de coopération devra donc être mis e en place.

4.2 Projet Western Union

Il s'agit de créer un cadre de collaboration technique entre le réseau Western Union, la police scientifique et le CICERT..

.

Objectif : Rendre les transactions sur réseau Western Union plus fiables.

4.3 Audit Technique des Systèmes d'Information (SI)

Relever les différentes vulnérabilités sur les systèmes d'informations de l'administration et du secteur privé et les porter à la connaissance de ceux-ci en vue de les corriger.

4.4 Application IMEI TRACKING (Recherche des Téléphones Volés)

Le projet de Tracking des IMEI a été initié, afin de répondre aux plaintes et réclamations à propos des terminaux mobiles volés.

Objectifs : L'objectif de ce projet est de mettre en place une application informatique qui permettra de connaître le numéro d'appel utilisant un terminal volé (identifié par son IMEI) et servira à identifier le numéro utilisant un appareil donné.

4.5 Formation du personnel CICERT

La formation du personnel du CICERT a pour objectif principal de renforcer la crédibilité du CICERT. Les actions de formation auront pour objectif de :

- accroître les compétences techniques des ingénieurs;
- mettre en place des procédures de travail pour accroître la fiabilité des résultats et des décisions ;
- acquérir ou développer des outils logiciels permettant d'élargir et de développer les services fournis par le CICERT
- parrainage du CICERT par un CERT membre de la communauté FIRST[3].

---

[3] Communauté des CERT : www.first.org

Annexe

Description des différents types d'arnaques

Fausses donations ou lègues (Héritage)

Pour ce qui est des fausses donations, elles proviennent le plus souvent, de personne malades condamnés à court terme, atteints soit d'un cancer ou de toute autre maladie mortelle.

Ils prétendent être sans famille, sans descendance et sont à la recherche d'un parfait inconnu à qui léguer leur fortune. Ils se disent très pieux et souhaitent de préférence que leur donation soit faite au bénéfice d'une œuvre caritative.

Demandes d'aides

Pour les demandes d'aides, plusieurs cas de figure entrent en ligne de compte, mais les plus souvent utilisés. L'escroc se fait passer pour :

- ✓ une orpheline, veuve ou une personne influente poursuivie par les assassins de son père ou de son mari, réfugiée dans une ONG ou une église ;
- ✓ l'héritière d'une importante somme d'argent se trouvant dans une malle, confiée à une société de sécurité.

A la réception du Scam l'escroc vous demande de l'aider à sortir une somme d'argent de son pays et vous propose en contrepartie 15% à 20 % du montant.

Fausses loteries

La fausse loterie consiste à faire soit des promotions au nom de grandes firmes internationales, usurpant ainsi le nom, la marque, etc.., ensuite intervient une désignation des gagnants fictifs en envoyant des spams. C'est ainsi qu'on retrouve souvent des loteries COCA-COLA, MICROSOFT, BMW, PARAMOUNT, etc..

Ces fausses loteries sont également organisées à l'occasion d'évènements nationaux comme la CAN FOOT 2010 en Angola, le Mondial FOOT 2010 en Afrique du Sud, Olympique loterie etc..

Usurpation d'Identité

C'est une technique permettant d'obtenir des informations confidentielles d'une personne, en lui donnant des raisons valables de le faire.

Dans ce cas, le cyber-escroc envoie un spam dans lequel il se fait passer pour le support technique d'un fournisseur de mail quelconque (Yahoo ou Hotmail…) et demande aux potentielles victimes de communiquer leurs informations confidentielles (login, Mot de passe..).

Le cyber-escroc prend alors le contrôle total de la messagerie de la victime et envoie des messages malveillants aux contacts de cette victime.

Love tchat

Une romance Scam est une arnaque où un étranger prétend avoir une attirance, des sentiments amoureux et gagne ainsi l'affection de sa victime.

Elle repose sur la création de liens affectifs forts qui sortent de toute logique habituelle et font appel à des émotions intenses. Ces émotions sont suscitées en ayant recours à des photos attractives, des profils de rêves sur des sites de rencontre, des lettres flatteuses, des pratiques mystiques etc.

La stratégie consiste principalement à obtenir de la victime qu'elle tombe amoureuse et ait envie d'être avec l'arnaqueur. La promesse d'un mariage est courante.

La manipulation psychologique est telle que la victime perd tout discernement et libre arbitre.

Commande de marchandises avec promesse de paiement par carte de Crédit ou virement bancaire

Les escrocs passent des commandes de matériels à des exportateurs français ou à des hôtels en France au nom de fausses entreprises ivoiriennes et proposent de payer, soit par cartes de crédit (il s'agit alors de cartes volées ou fausses), soit par virements bancaires (de faux ordres de virement vous sont adressés en pièces jointes : la qualité de ces faux ordres de virement peut être excellente).
