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

POLE RESSOURCES ET TECHNOLOGIES

CENTRE SPECIALISE CI-CERT

RAPPORT ANNUEL 2017

SOMMAIRE

INTRODUCTION

Le présent document est le rapport annuel d'activités du centre spécialisé CI-CERT ; il relate les principales activités et les résultats obtenus au cours de l'année 2017.

Ce rapport, structuré en six chapitres, consigne l'essentiel des activités de cybersécurité, les actions réalisées et les résultats obtenus par l'équipe CI-CERT. Egalement, les activités au titre de la lutte contre la cybercriminalité.

RESUME

Dans le cadre de l'adhésion du CI-CERT au FIRST, le CERT Américain (CERT/CC) a effectué une mission de travail en Côte d'Ivoire en vue de sponsoriser l'ARTCI.

Lors de cette mission, il s'est engagé à accompagner le CERT ivoirien pour le renforcement de capacités afin de répondre aux exigences du FIRST et aux besoins du CI-CERT. Ainsi une première formation avait été organisée du 13 au 17 février 2017 dans la salle de conférence de l'ARTCI. Parallèlement à cette formation destinée aux techniciens, des discussions entre le Département d'Etat Américain, l'Ambassade des USA à Abidjan et la Direction Générale de l'ARTCI ont porté sur un cadre de collaboration en vue d'une stratégie pour la montée en puissance du CI-CERT tant au niveau national que régional.

A l'issue des trois (3) jours d'échanges fructueux, cinq (5) axes ont été identifiés dans le cadre de la collaboration. Ces axes sont les suivants :

- **Formation :** Proposition de formations pour les gestionnaires des systèmes d'informations de l'Administration et prise en compte des besoins en formation du CI-CERT.
- **Projet de charte de collaboration entre le CI-CERT et ses parties prenantes :** Accompagnement d'un expert désigné par le CERT/CC et organisation d'un atelier de validation de la charte de collaboration entre le CI-CERT et ses parties prenantes.
- **Cyberdrill national :** Organisation d'un exercice de simulation avec l'appui d'un partenaire du CERT/CC pour le renforcement des équipes opérationnelles des parties prenantes.
- **Développement des services actuels du CI-CERT** : Assistance à l'implémentation des nouveaux services proposés par le CERT/CC conformément aux exigences du FIRST.

- **Coopération avec d'autres CERT :** Proposition par le CERT/CC d'un plan de coopération pour le CI-CERT avec d'autres CERT internationaux.

Concernant la lutte contre la cybercriminalité, le CI-CERT a contribué à la révision de **l'accord de partenariat** signé depuis 2011 entre l'ARTCI et la Direction Générale de la Police Nationale (DGPN) pour la mise en place de la Plateforme de Lutte Contre la Cybercriminalité **(PLCC)**. Cet accord de partenariat a été actualisé le **10 juillet 2017**.

I. APERÇU GENERAL

1. Création et Missions

Le CERT National dénommé Côte d'Ivoire Computer Emergency Response Team (CI-CERT) a été créé en Juin 2009.

Les missions du CI-CERT sont :

- 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.

2. Organisation du CI-CERT

L'équipe du CI-CERT est composée de six (06) ingénieurs dont trois (03) sont détachés à la PLCC. Le CERT National est constitué d'un (01) chef de centre et de deux (02) équipes :

- **Le chef de Centre** assure :
  - La gestion des activités opérationnelles et les relations avec les parties prenantes du CI CERT ;
  - La fonction de point de contact dans le traitement des incidents de sécurité informatique survenant sur le cyberespace national et les systèmes d'information nationaux.

- **L'équipe Gestion des Incidents** est chargée de :
  - La coordination des incidents de sécurité informatique ;
  - La réponse aux incidents de sécurité informatique ;
  - L'Investigation légale et contribuer à la lutte contre la cybercriminalité ;
  - La gestion du Système d'information du CI-CERT.

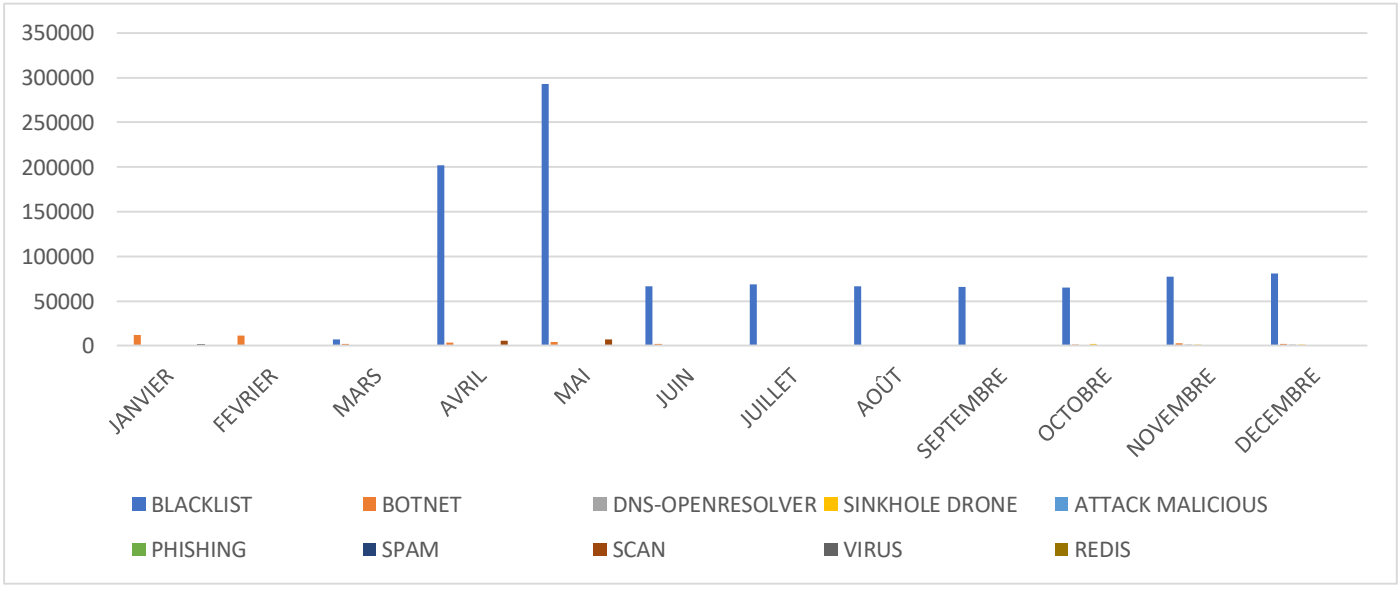
- **L'équipe Veille et Sensibilisation** en charge :
  - De la veille technologique ;
  - Du monitoring des infrastructures critiques ;
  - De la sensibilisation et la communication sur la cybercriminalité ;
  - Du développement d'applications métier.

II. REALISATIONS

1. Traitement d'incidents de sécurité informatique

Les incidents collectés et traités par le CI-CERT au cours de cette année sont : Réseau de BOTNET, DNS OPEN RESOLVER, PHYSHING, SPAM, etc.

Au total, le CI-CERT a traité au cours de l'année 2017 **1 066 366 incidents** de sécurité informatique majoritairement constitués de BOTNET et BLACKLIST. Les détails des activités sont consignés dans le graphique ci-après :



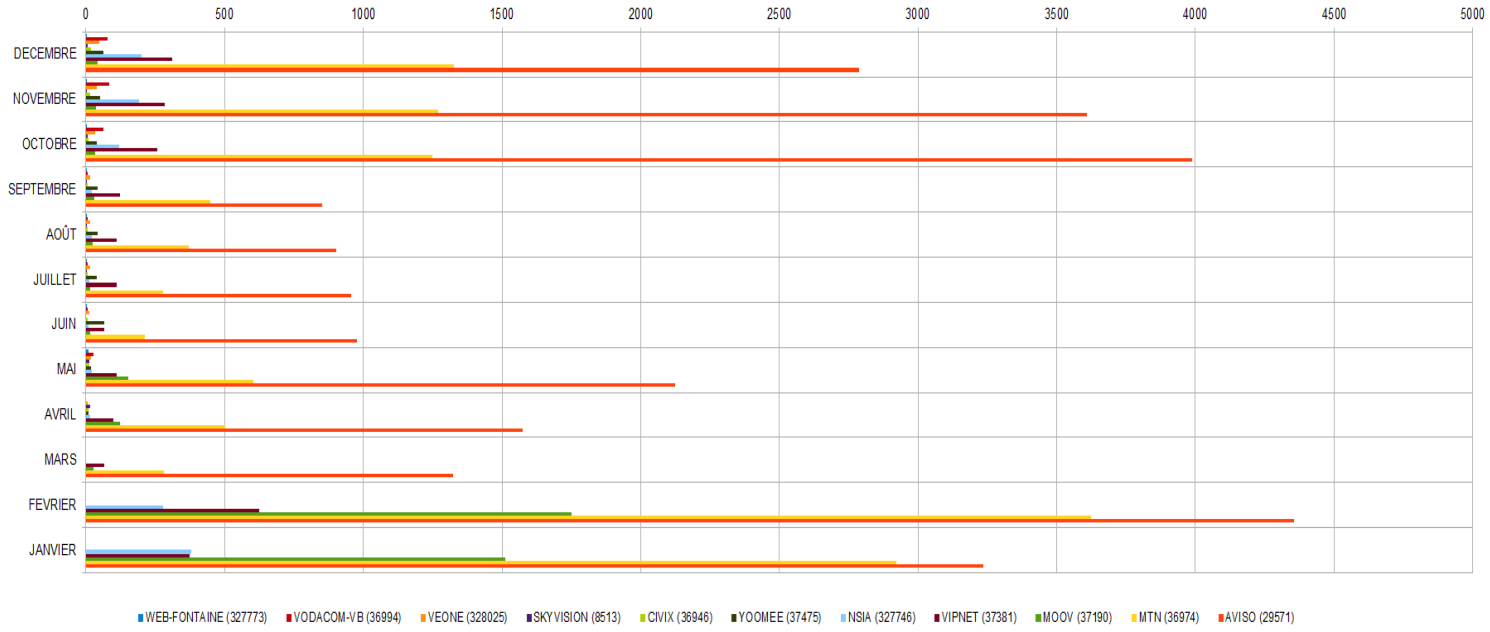
Graphique 1 - Nombre d'incidents par type

Le graphique 1 montre la répartition annuelle des incidents de sécurité, nous observons que les incidents de type BLACKLIST ont été les plus traités au cours des mois d'Avril et de Mai 2017. Ceci s'explique par un nombre important d'adresses IP, de listes de serveurs, services en ligne ou de réseaux IP mis sur liste noire et connus pour contribuer ou être source de plusieurs attaques et incidents de sécurité en particulier les SPAM.

Suite à de nouvelles mesures pour une meilleure prise en charge des incidents de type BLACKLIST, nous constatons une réduction significative (environ 80 %) au cours du dernier trimestre 2017.

2. Coordination des vulnérabilités

Le CI-CERT a notifié **48350 vulnérabilités** ont été notifiées aux parties prenantes impactées en 2017 contre 2765 en 2016.



Graphique 2 – Nombre de vulnérabilités par mois et par opérateurs

Du graphique 2, il ressort que les opérateurs ayant reçu plus de notifications sur les vulnérabilités sont VODACOM, VEONE et MOOV-CI.

Par ailleurs, au cours de l'année 2017, nous avons constaté un nombre important de vulnérabilités sur les réseaux des opérateurs. Ces vulnérabilités sont la conséquence des faiblesses dans la conception, la mise en œuvre ou l'utilisation des composants matériel ou logiciels des systèmes d'information et surtout le non–respect des bonnes pratiques de sécurité et des mesures d'hygiène informatique.

3. Veille technologique et Sensibilisation

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

Le CI-CERT a publié sur son site Internet au cours de l'année 2017, deux cent quatre-vingt-trois (283) bulletins de sécurité contre trois cent vingt-deux (326) en 2016.

b. Diffusion de la Mailing-List

En 2017, le CI-CERT a diffusé deux cent quatre-vingt-trois (**283**) *bulletins de sécurité* et quatorze (**14**) *alertes de sécurités* via la mailing-list.

Le nombre de souscripteurs à la mailing-list est passé de trois cent cinquante-quatre (**371**) souscriptions en 2016 à cinq cent trente (**530**) souscriptions en 2017.

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

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

Le CI-CERT publie des articles de sensibilisation sur les réseaux sociaux. On peut citer :

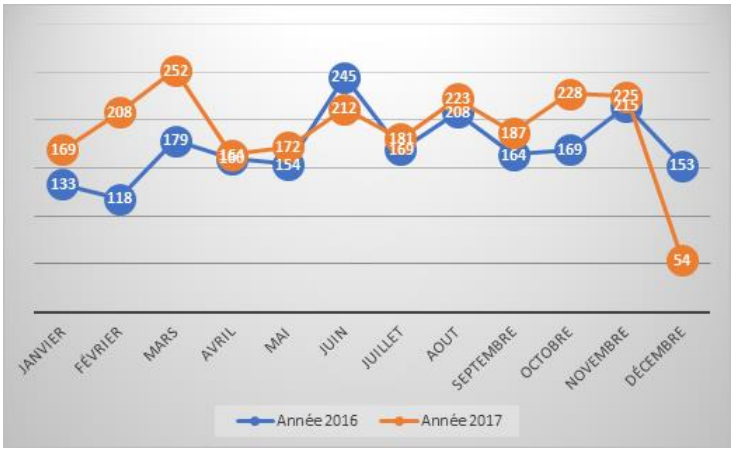
- Escroquerie en ligne : Ayons les bons réflexes ;
- Faîtes attention aux doublons de compte/profil Facebook afin d'éviter tout désagrément et préservez ainsi votre e-réputation ;
- Comment créer le mot de passe parfait ? Banque, e-commerce, messagerie électronique, documents, administration : de nombreuses démarches passent désormais par Internet et par la création de comptes sur les différents sites ;
- Une campagne de Phishing* vise actuellement les clients détenteurs de la carte bancaire VISA résidents en Côte d'Ivoire par la diffusion de sms les invitant à cliquer sur un lien illicite.

Le compte Facebook du CI-CERT compte en 2017 : **919 membres**.

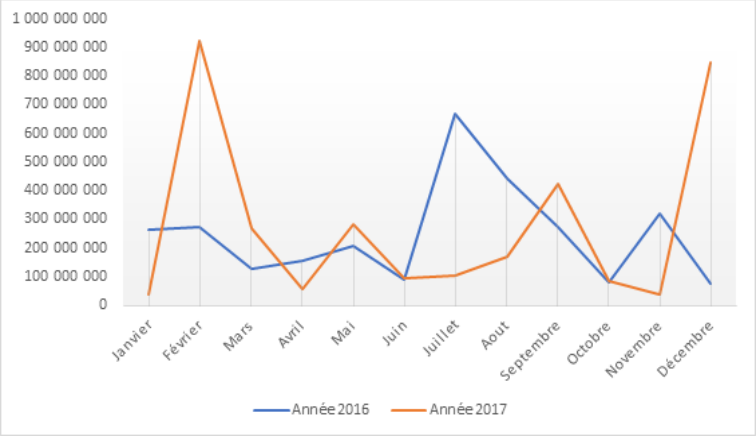
4. Lutte contre la cybercriminalité

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. Cet accord de partenariat a été actualisé le **10 juillet 2017**.

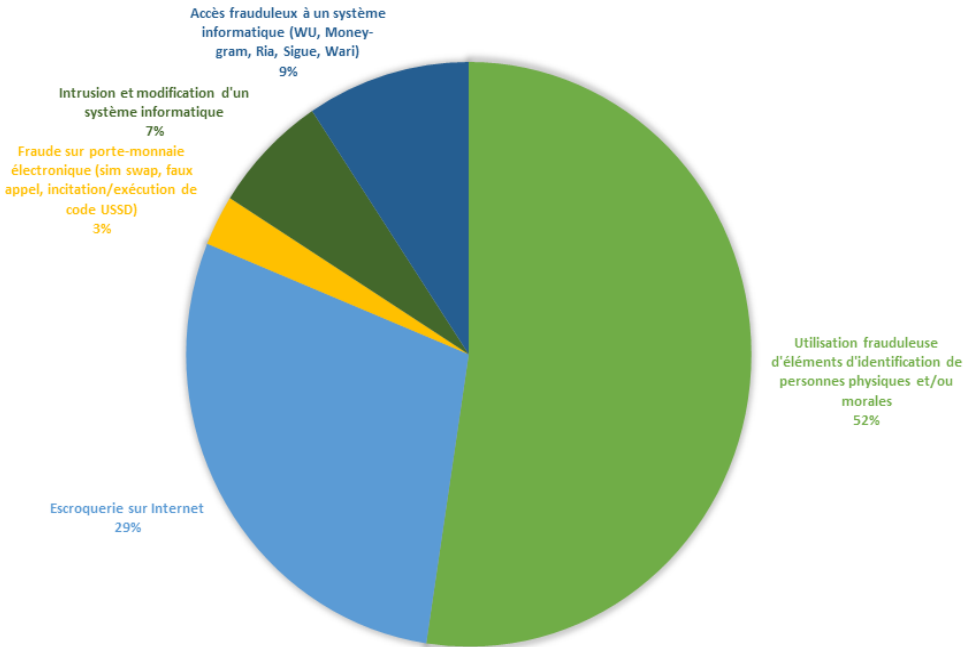
Les réalisations de la PLCC pour l'année 2017 :



Graphique 3 - Nombre d'affaires cumulées par mois



Graphique 4 - Nombre de préjudices financiers cumulés par mois



Graphique 5 - Préjudices financiers par type d'infraction

Comparé à 2017, le nombre d'affaires a légèrement augmenté. Il passe de 2067 à 2275 soit 10 %, quand le préjudice 2017 estimé à 5 106 121 649 FCFA a connu une augmentation de 24 %. Plusieurs raisons expliquent cette hausse :

- Elle 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 d'affaires est due 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 forte activité cybercriminelle pendant les vacances scolaires (Juin-Août) et en fin d'année (Octobre-Décembre). Cela s'explique par le nombre important des cyberdélinquants encore élèves ou étudiants.

Les infractions en 2017 sont constituées essentiellement entre autres de :

- **Fraude sur porte-monnaie électronique (sim swap, faux appel, incitation/exécution de code USSD)** (18,64%)
- **Utilisation frauduleuse d'élément d'identification de personne physique ou morale** (18,51%)
- **Atteinte à l'image (menace, injures, harcèlement, diffamation, dénonciation calomnieuse sur réseaux sociaux)** (13,10%)
- **Vol** (Transfert frauduleux, vol de téléphones, données informatiques, etc.) (11,74%)

En cette 2017, **2 275** victimes de cybercriminalité contre 2 067 en 2016 sont majoritairement constituées à **89%** d'ivoiriens. Ensuite, 3% d'entre elles sont françaises. Et **166 interpellations et 138 déférés,** la PLCC défère plus de 83 % des personnes qu'elle interpelle.

III. DIFFICULTES RENCONTREES

En 2017, les difficultés constatées sont :

- Insuffisance du personnel : la moitié du personnel a été recruté dans les autres directions.
- Dépendance du réseau informatique de l'ARTCI : ce qui entraine des difficultés dans l'exploitation de nos ressources.

IV. FORMATIONS

1. GESTION AVANCEE DES INCIDENTS DE SECURITE

Du 13 au 17 février 2017 s'est tenue à la salle de conférence de l'ARTCI une formation organisée par le CERT Coordination Center (CERT/CC) sur le thème « **Advanced Incident Handling** ».

Cette formation s'inscrit dans le cadre de la collaboration entre le CI-CERT et le CERT/CC à la suite de notre adhésion au FIRST. L'objectif étant de permettre aux participants de :

- Acquérir les outils de management d'un CERT ;
- Rédiger les procédures de travail et les politiques de sécurité ;
- Maîtriser les méthodologies de gestion avancée d'incident informatique ;
- Instaurer un espace d'échanges d'idées et d'expériences entre le CI-CERT et ses parties prenantes afin d'aboutir à des stratégies pertinentes pour contribuer au renforcement de la confiance numérique et à la protection du cyberespace.

2. COMMUNICATIONS PAR SATELLITE

A l'initiative de l'International Télécommunications Satellite Organization (ITSO) et en partenariat avec l'Union Internationale des Télécommunications (UIT), le CI-CERT a participé à un Atelier de Formation sur les communications par satellite du 10 au 14 juillet 2017 à l'École Supérieure Africaine des Technologies de l'Information et de la Communication (ESATIC).

Cet atelier a couvert une gamme étendue de questions concernant les communications par satellites, le rôle des organisations régionales et internationales et les aspects réglementaires de l'utilisation des satellites.

V. REPRESENTATIONS A L'EXTERIEUR ET BENCHMARK

1. FORUM INTERNATIONAL DE LA CYBERSECURITE (FIC 2017)

Du 24 au 25 janvier 2017 s'est tenu au « Grand Palais » de Lille en France, le 9ième Forum International de la Cybersécurité, le FIC 2017 sur le thème « **Smarter security for future technologies** ». Il s'inscrit dans une démarche de réflexions et d'échanges visant à promouvoir une vision commune de la cybersécurité.

2. PARTICIPATION A LA 2ème EDITION DU SALON INTERNATIONAL DES TIC (SITIC)

Le SITIC AFRICA est un événement international consacré exclusivement au Business. Dans sa 2ème édition, il s'est érigé en salon professionnel international pour mieux faire connaître l'offre TIC tunisienne aux autres secteurs de l'Economie Tunisienne (Agriculture, Industrie et Services) tout en étant une plateforme internationale de partenariat et d'échanges. Sa dimension africaine est atteinte par l'invitation de plus d'une centaine de décideurs publics et privés africains pour leur présenter l'offre tunisienne et les inviter à un partenariat gagnant-gagnant Tunisie-Afrique-Pays Occidentaux.

La Côte d'Ivoire était représentée par une forte délégation dont l'ARTCI.

En marge de ce salon, l'ARTCI a été reçue à la **Direction Générale de la Poste de Tunisie,** à **l'Instance Nationale des Télécommunications de Tunisie (INTT),** à **l'Agence Tunisienne d'Internet (ATI)** et au **Centre d'Etude et de Recherche en Télécommunication (CERT)** pour des échanges. Les discussions lors de cette visite de travail ont porté sur :

- L'observatoire des marchés et des offres afin de profiter de l'expérience de l'INTT dans ce domaine ;
- La stratégie mise en place par l'ATI pour la migration de l'IPv6 ;
- Le développement des points d'échanges internet (IXP) ;
- La supervision de la sécurité au Centre d'Opération de Sécurité : SOC (Security Operation Center).

3. PARTICIPATION A LA 29ème CONFERENCE ANNUELLE DU FIRST

Du 11 au 17 juin 2017 s'est tenue à San Juan (Porto Rico) la 29ème conférence annuelle du FIRST. Cette rencontre était couplée avec la 12ème réunion annuelle technique pour les CERT à responsabilité nationale qui s'est tenue du 16 au 17 juin 2017. Ces conférences annuelles sont l'occasion pour les équipes CERT des pays membres de partager leurs expériences et connaissances sur la sécurité des systèmes d'information en générale et plus particulièrement de la prévention et de la gestion des incidents de sécurité informatique. Aussi de débattre des questions d'organisation et d'orientations stratégiques liées à la cybersécurité.

4. PARTICIPATION A FIRST-ITU REGIONAL SYMPOSIUM & CYBER DRILL FOR AFRICA AND ARAB REGIONS

Le CI-CERT a participé au Symposium Régional et Cyber Drill - ALERT (Exercice pratique pour les équipes de réponses aux incidents informatiques – CERT) pour la région Afrique et Arabe, organisé par l'Union International des Télécommunications qui s'est tenu du 13 au 17 novembre 2017 en Tanzanie, à l'invitation de Tanzania Communications Regulatory Authority (TCRA).

L'objectif de cet évènement régional était :

- De réfléchir aux initiatives de sécurité pour atténuer les menaces informatiques et réduire les risques de cybermenaces ;
- De créer un cadre de coopération entre les CERTs participants afin de mutualiser les expériences et les compétences dans la réponse aux incidents de sécurité informatique ;
- D'améliorer les capacités de communication avec les parties prenantes ;
- Assurer des efforts collectifs continus et apporter des réponses appropriées contre les cybermenaces ;
- De renforcer les capacités des CERTs africain ;
- Initier une plate-forme de communication dans le cadre du traitement des incidents cybernétiques.

VI. PERSPECTIVES

Pour l'année 2018, les centres spécialisés se sont fixés de nombreux défis à relever pour contribuer au développement d'une économie numérique dans un environnement favorable inspirant la confiance des utilisateurs des technologies de l'information et de la communication. Ce sont :

- Organisation d'un séminaire de formation en cybersécurité pour les gestionnaires des systèmes d'information de l'administration ;
- Poursuivre la collaboration avec le CERT/CC et le département d'ETAT des Etats-Unis pour le renforcement des capacités opérationnelles du CI-CERT ;
- Organisation de FIRST-ITU Cyberdrill & Symposium pour la région Afrique et Arabe ;
- Formalisation de la collaboration avec les acteurs de la sécurité de l'écosystème numérique en Côte d'Ivoire ;
- Renforcement de la collaboration avec les acteurs de la communauté internet nationale (Gouvernement, Registrars, Entreprises, Utilisateurs finaux).

Lexique

- **Botnet** : Un botnet (de l'anglais, contraction de « robot » et « réseau ») est un réseau de bots informatiques, des programmes connectés à Internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches. Historiquement, botnet désignait des réseaux de robots IRC.

- **Blacklist** : sont des répertoires d'adresses IP qui ont été identifiées par les différents FAIs et webmails comme générant beaucoup de spam. En d'autres termes, si une adresse IP est inscrite sur la liste noire d'un service d'emailing, cela signifie que son utilisateur a de fortes chances d'être un spammeur.

- **CcTLD** : Un domaine de premier niveau national (en anglais country code top-level domain ou **ccTLD**) est un type de domaines de premier niveau (TLD) maintenus par l'Internet Assigned Numbers Authority (IANA) pour une utilisation dans le système de nom de domaine d'Internet.

- **Whois** est un service de recherche fourni par les registres Internet, par exemple les Registres Internet régionaux ou bien les registres de noms de domaine permettant d'obtenir des informations sur une adresse IP ou un nom de domaine.

- **Phishing :** L'hameçonnage, phishing ou filoutage est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité.

- **DNS-Openresolver :** DNS fournissant la résolution récursive de nom pour les clients à l'extérieur de son domaine administratif.

- **Sinkhole Drone** : C'est une machine cible utilisée par les chercheurs pour recueillir des informations sur un botnet particulier.

- **Attack Malicious :** Attaque malicieuse

- **Spam :** Le « spam » ou « pollupostage », désigne les communications électroniques massives, notamment de courrier électronique, non sollicitées par les destinataires, à des fins publicitaires ou malhonnêtes : le pourriel contient généralement de la publicité.

- **Scan : (Port Scan)** En informatique, le balayage de ports (port scanning en anglais) est une technique servant à rechercher les ports ouverts sur un serveur de réseau. ... Les balayages de ports se font habituellement sur le protocole TCP ; néanmoins, certains logiciels permettent aussi d'effectuer des balayages UDP.

- **Virus :** C'est un programme écrit dans le but de se propager sournoisement et rapidement à d'autres ordinateurs. Il perturbe plus ou moins gravement le fonctionnement de l'ordinateur infecté.

- **Redis :** (de l'anglais REmote DIctionary Server qui peut être traduit par « serveur de dictionnaire distant » et jeu de mot avec Redistribute1) est un système de gestion de base de données clef-valeur scalable, très hautes performances, écrit en C ANSI et distribué sous licence BSD.

- Le Domain Name System (ou **DNS**, système de noms de domaine) est un service permettant de traduire un nom de domaine en informations de plusieurs types qui y sont associées, notamment en adresses IP de la machine portant ce nom.

- **Mailing-List :** Liste des récipiendaires des informations de sécurité informatique.

- **Fraude sur le porte-monnaie électronique :** Un appel ou un SMS est émis à l'endroit de la victime lui demandant de saisir des codes (USSD) pour bénéficier d'un prétendu bonus ou pour valider la réception de son transfert. A l'insu de la victime, sa carte SIM est désactivée et réactivée sur une nouvelle puce. Le détenteur de la nouvelle puce a alors un contrôle total de ses comptes électroniques.
- **Code USSD :** Message constitué de suite de caractères, envoyés comme commande au réseau de téléphonie afin d'y exécuter des programmes.

- **Utilisation frauduleuse d'éléments d'identification de personnes physiques et/ou morale :** 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.

- **Atteinte à l'image (à la cyber réputation) :** Le droit pénal offre plusieurs textes permettant de protéger son e-réputation lorsqu'elle est atteinte aux moyens des réseaux sociaux notamment.

- **Injure :** Toute expression outrageante, termes de mépris ou invective qui ne renferme l'imputation d'aucun fait. (Ex : le PDG de l'entreprise X est un voleur etc.)

- **Diffamation :** Allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne.

- **La divulgation de la vie privée :** elle concerne spécifiquement la vie sentimentale d'une personne, la publication d'informations concernant la santé d'une personne, puis le droit à l'image.

- **Vol de données informatiques** : Le cyber délinquant s'approprie frauduleusement les informations numériques de sa victime à des fins délictueuses.