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

DIRECTION DE LA CONFIANCE NUMERIQUE ET SECURITE DES RESEAUX

CENTRE TECHNIQUE CI-CERT

RAPPORT ANNUEL 2019

SOMMAIRE

AVANT-PROPOS

Le présent document est le rapport annuel d'activités du Centre de veille et de réponse aux incidents de sécurité informatique dénommé Côte d'Ivoire Computer Emergency Response Team (CI-CERT). Comme les précédentes années, il relate les principales activités et les résultats obtenus au cours de l'année 2019 en matière de protection du cyberespace ivoirien et de la lutte contre la cybercriminalité.

Ce rapport rend compte des activités menées par le CI-CERT pour accompagner l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire (ARTCI) dans sa mission de sécurisation et de protection des réseaux et assurer une confiance dans l'utilisation des Technologies de l'Information et de la Communication.

I. PRESENTATION DU CI-CERT

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.

II. BILAN DES ACTIVITES REALISEES EN 2019

1. Au titre de la cybersécurité et de la lutte contre la cybercriminalité

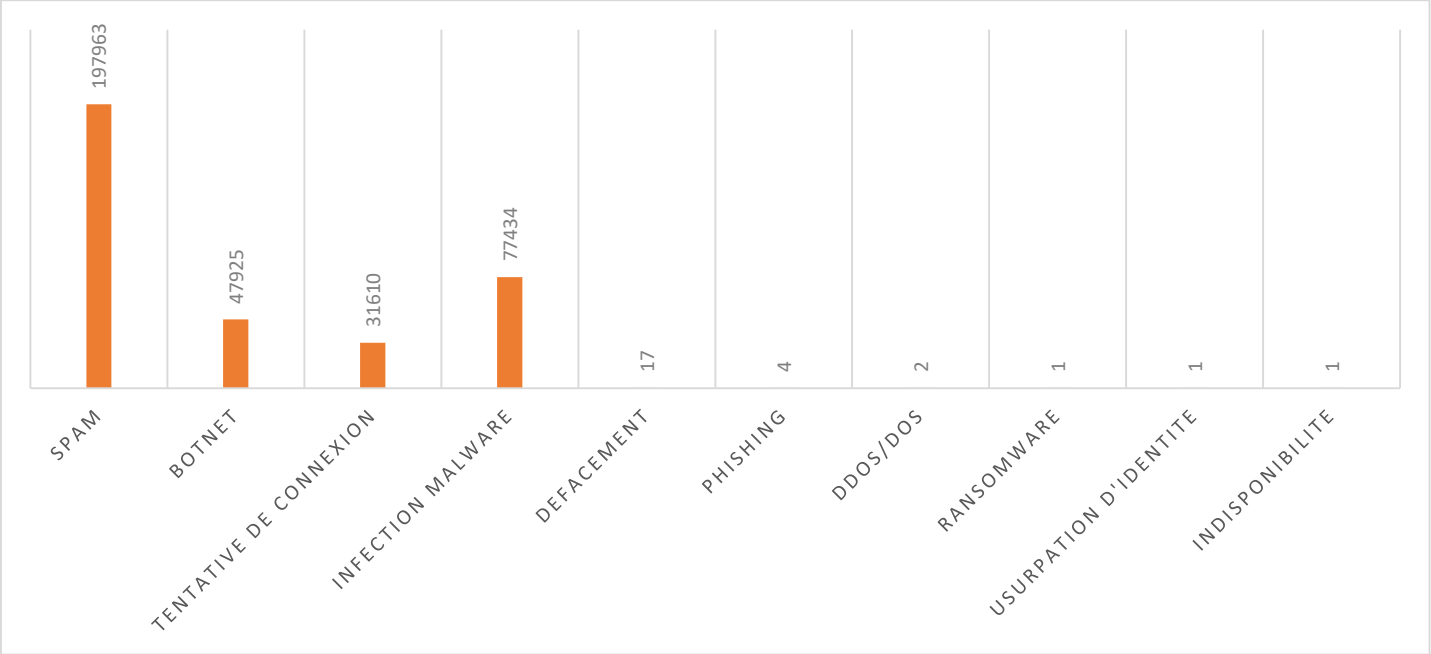
a. Traitement d'incidents de sécurité informatique

Le traitement des incidents est un service réactif qui consiste à recevoir, trier et répondre aux demandes et aux signalements, et à analyser les incidents et évènements. Les actions de réponse peuvent plus particulièrement consister à :

- Prendre des mesures pour protéger les systèmes et réseaux concernés ou menacés par une intrusion ;
- Proposer des solutions et des actions d'atténuation à partir des alertes et bulletins de sécurité pertinents ;
- Rechercher une activité éventuelle de l'intrus sur d'autres parties du réseau ;
- Filtrer le trafic sur le réseau ;
- Restaurer les systèmes ;
- Appliquer des correctifs aux systèmes ou les réparer ;
- Développer d'autres stratégies de réponse ou solutions temporaires.

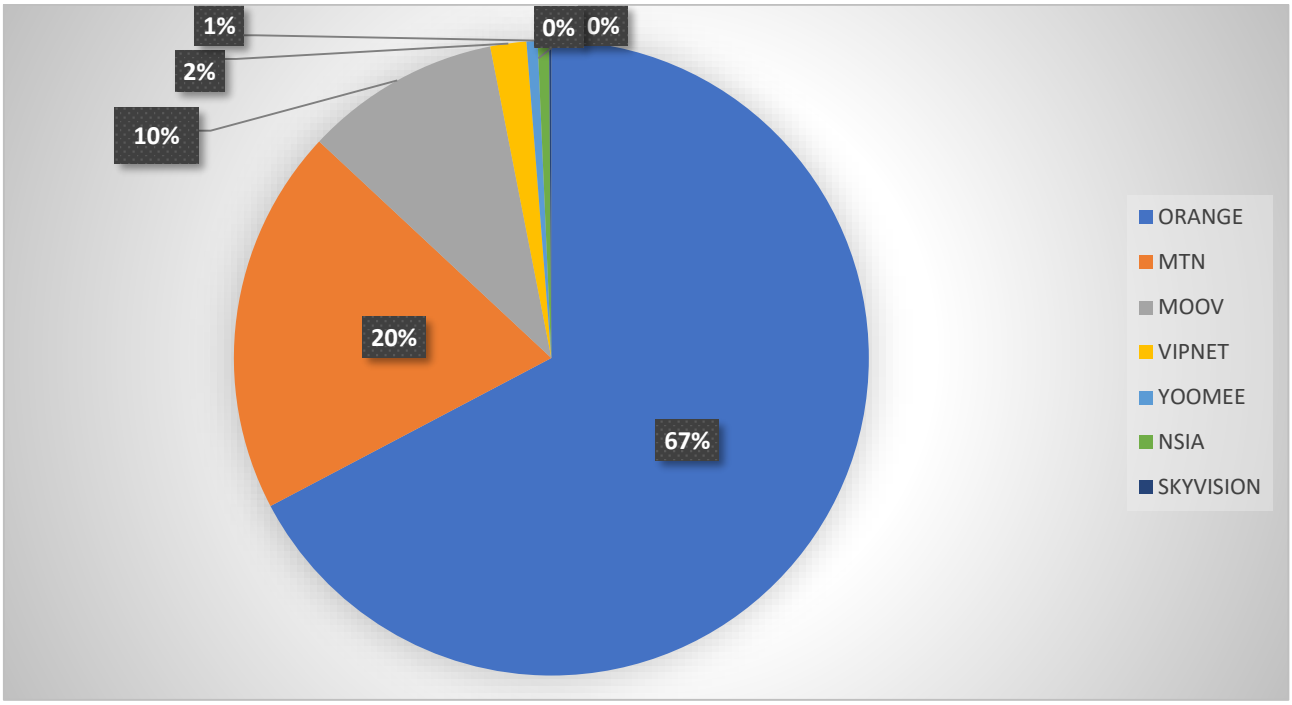
Ainsi le CI-CERT a traité au cours de cette année 2019, 354 960 incidents de sécurité informatique. Ce nombre a chuté de 65,43 % par rapport à 2018. Cette baisse s'explique en partie par la requalification des incidents de sécurité informatique collectés et traités conformément aux standards internationaux.

Les détails des incidents de sécurité informatique sont consignés dans le graphique ci-après :



Graphique 1 : Type d'incidents

Le graphique suivant indique la proportion des adresses IP des fournisseurs d'accès à internet (FAI) concernées par les incidents de sécurité informatique traités.



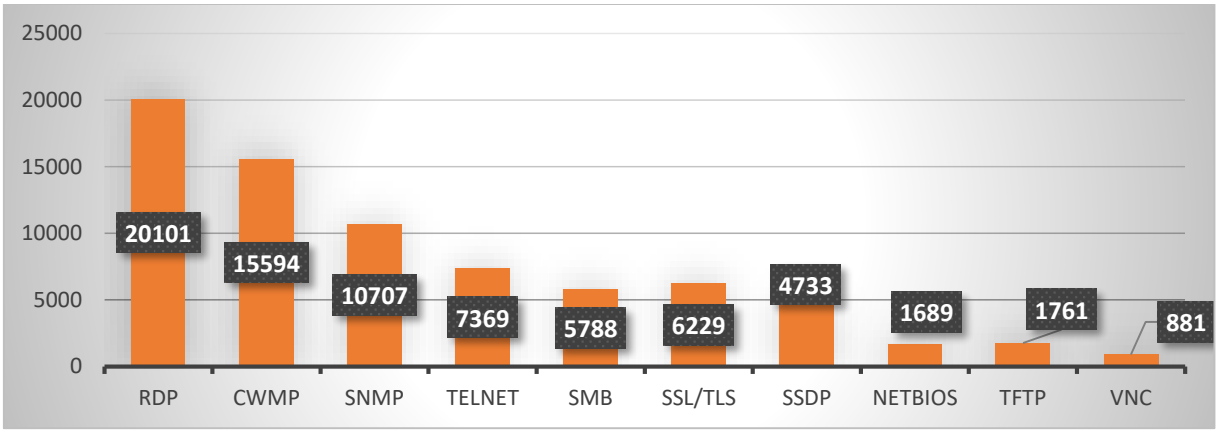
Graphique 2 : Proportion d'incidents par FAI

Les adresses IP du Fournisseur d'Accès à Internet de l'opérateur Orange CI ont connu le nombre d'incidents le plus élevé avec 67%, suivi des opérateurs MTN avec 20% et MOOV avec 10%.

b. Coordination des vulnérabilités

Le CI-CERT avertit les différentes parties prenantes de l'existence de vulnérabilités, correctifs ou solutions temporaires y afférents et fournit des informations sur les moyens d'y remédier ou d'en atténuer les effets.

Pour cette année, **74851 vulnérabilités** ont été notifiées aux parties prenantes impactées contre **68 655 vulnérabilités** contre en 2018 soit une hausse de 9,02% par rapport à 2018.



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.

c. Veille et Sensibilisation

Dans le cadre du suivi de l'actualité et du développement de la culture de cybersécurité, le CI-CERT a publié sur ses différents canaux de communications des avis et alertes de sécurité, des plaquettes de sensibilisation, des guides et des bonnes pratiques en matière de sécurité des système d'information pour informer et expliquer les bonnes pratiques et recommander certaines précautions en matière de sécurité informatique.

- **Site web www.cicert.ci**

	Année 2018	2019
Nombre d'alertes	14	18
Nombre d'avis	302	347
Nombre de guides	-	5

Ci-après quelques guides publiés et téléchargeables sur le site du CI-CERT :

- 10 conseils pour se protéger en ligne | Télécharger
- Gestion de mot de passe : Comment créer un « mot de passe fort » ? | Télécharger
- Cartes bancaires : 7 astuces de sécurité | Télécharger
- Sécurité sur les réseaux sociaux | Télécharger
- Ransomware : comment se prémunir de cette attaque ? | Télécharger

- **Twitter et Facebook**

	Année 2019
Publications page Facebook	34
Nombre d'abonnés sur Facebook	1079
Publications Twitter	91
Nombre d'abonnés sur Twitter	51

- **Plaquettes de sensibilisation**

N°	Thèmes
1	Gestion de Mots de passe : Comment créer le mot de passe parfait?
2	Six (06) astuces pour un bon mot de passe
3	Tout savoir sur les Malwares : Quelques définitions
4	Tout savoir sur les Malwares : Les méthodes d'infection
5	Tout savoir sur les Malwares : Comment se protéger contre les malwares ?
6	Attention !!! Des millions de smartphones sous Android infectés en Côte d'Ivoire par le malware ARRKII.
7	Mobile Money : Conseils de sécurité pour ne pas se faire arnaquer
8	[Alerte]: 85 Applications potentiellement nuisibles pour votre smartphone !
9	Mobile Banking : Conseils de sécurité.
10	[Conseils de sécurité]: Cartes bancaires
11	[Conseils de sécurité]: 5 comportements à avoir sur les réseaux sociaux
12	[Conseils de sécurité]: Méfiez-vous de l'infection au ransomware (rançongiciel)
13	[Conseils de sécurité]: 9 règles pour SÉCURISER son appareil mobile
14	[OctobreCyberSecu]: Mois de Sensibilisation à la Cybersécurité
15	[OctobreCyberSecu]: Comprendre la cybermenace
16	[OctobreCyberSecu] : Comprendre se protéger en ligne ?
17	[OctobreCyberSecu]: : Hameçonnage (phishing)
18	[OctobreCyberSecu]: Ma sécurité sur les réseaux sociaux
19	[OctobreCyberSecu]: Cybersécurité lors des déplacements
20	[OctobreCyberSecu]: Sécurité en ligne, protégez vos enfants
21	[OctobreCyberSecu]: Authentification multifacteur
22	[OctobreCyberSecu]: Mobile Banking
23	[OctobreCyberSecu]: 5 conseils pour protéger son entreprise
24	Risques et menaces associés aux clés USB
25	Sauvegarde de données informatiques.

26	La mise à jour informatique
27	Le rançongiciel
28	La sécurité des usages pro-perso
29	Fêtes de fin d'année : Attention aux cyber arnaques !
30	Fêtes de fin d'année: Evitez les usurpations d'identité
31	Fêtes de fin d'année: 6 commandements pour éviter le piratage.
32	[Compte à rebours 2020]
33	[Compte à rebours 2020/j-04] : Eduquez vos enfants à la prudence sur internet.

d. Coopération nationale

Des rencontres avec les responsables de sécurité des systèmes d'information ont été initiées et dénommées « Matinales du CI-CERT ». Celles-ci ont été l'occasion pour le CI-CERT de renforcer les liens de collaboration et de partage d'informations en matière de sécurité des systèmes d'information.

Ces rencontres ont enregistré la participation de plusieurs administrations publiques et privées.

Administration invitée	FAI, SIR-SIFCA-DGI-SOLIBRA	Banques	Assurances	Gouvernement	Hôpitaux et Cliniques
Nombre de participants	10	9	10	8	5

e. Participations aux séminaires, colloques et congrès.

- **Atelier de sensibilisation des magistrats sur la cybercriminalité et la preuve numérique, Abidjan (Côte d'Ivoire)**

Il s'est déroulé à l'hôtel Palm Club des 2-Plateaux, un atelier de sensibilisation des magistrats sur la cybercriminalité et la preuve numérique. Étaient présents pour le CICERT, Mlle LEPREGNON Carole, M. AMAN Vladimir et Mme AKISSI Flavie.

- **Atelier de formation « Sécurité des applications d'internet et de mobile Banking ».**

- **Clinique des TIC, Abengourou (Côte d'Ivoire)**

Le CI-CERT a participé à la première édition de la CLINIQUE DES TIC 2019 organisée dans la ville d'Abengourou du 28 au 29 novembre 2019. Il s'agit d'une audience foraine organisée par l'ARTCI pour sensibiliser les usagers des TIC sur leur droit, les métiers de l'ARTCI notamment la lutte contre la cybercriminalité, la portabilité, l'identification des cybercafés, la protection des données personnelles.

III. PERSPECTIVES 2020

Pour le CI-CERT, les perspectives pour l'année à venir sont les suivantes :

- Le Projet « Sah Analytics » pour la montée en charge du CI-CERT ;
- L'organisation d'un séminaire de formation en cybersécurité pour les gestionnaires des systèmes d'information de l'administration.