REPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie

AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

REPUBLIC OF CAMEROON
Peace – Work – Fatherland

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

RAPPORT SUR LA CYBERCRIMINALITE ET LA CYBERSECURITE AU CAMEROUN DE 2015 A 2017

I. Statistiques sur la cybercriminalité

Au cours de ces dernières années, le Cameroun a enregistré plusieurs actes cybercriminels qui ont eu un impact négatif sur le plan économique et sur l'image de certaines de ses Institutions. Les principales manifestations du phénomène de cybercriminalité ont pris la forme suivante au Cameroun, dans la période de 2015 à 2017 :

- attaques contre les sites web gouvernementaux ;
- usurpations d'identité sur les réseaux sociaux ;
- fraudes à la carte bancaire ;
- scamming ;
- fraude à la SIMBOX.

I.1 Attaques contre des sites web gouvernementaux

Entre 2015 et 2017, les sites web gouvernementaux ont été régulièrement ciblés par des hackers. Les attaques menées étaient essentiellement :

- de type web defacement ;
- les infections par des programmes malveillants ;
- de type force brute ;
- la saturation de serveur DNS.

I.1.1 Attaques de type web defacement

Les attaques de type web defacement visent principalement les sites web des Administrations publiques. Elles consistent en la modification d'une page du site web afin d'ajouter des messages de propagande à la solde de la cause défendue (homosexualité, islam radical, etc) par l'attaquant. Entre 2015 et 2017, **sept (07)** sites web d'Administrations publiques camerounaises ont subi une attaque de type web defacement ainsi que consigné dans le tableau ci-dessous.

Année	2015	2016	2017	TOTAL
Nombre d'attaques perpétrées	02	04	01	07

I.1.2 Infection par des programmes malveillants

Des sites web gouvernementaux ont également été infectés par des programmes malveillants entre 2015 et 2017. Par conséquent, plusieurs de ces sites web ont figuré dans des listes noires sur Internet.

Sur **cent quarante-quatre (144)** sites web gouvernementaux analysés en 2017, des programmes malveillants ont été détectés sur **trente-quatre (34)** d'entre eux, soit un pourcentage de **23, 61 %** de sites infectés.

I.1.3 Autres types d'attaques

Comme autres types d'attaques survenues, l'on note : les attaques de type force brute et les saturations de serveur DNS. La force brute est une technique utilisée par les hackers pour découvrir le mot de passe d'accès à un compte d'utilisateur d'un système en essayant plusieurs tentatives d'authentification à l'aide de combinaisons de caractères. Quant à la saturation du serveur DNS, elle vise à réaliser un déni de service du service DNS par l'envoi d'un grand nombre de requêtes au serveur. La situation de ces attaques notifiées à l'ANTIC se présente ainsi qu'il suit :

Type	2015	2016	2017
Saturation de serveur DNS	-	-	01
Tentative d'attaque de type force brute	01	01	01

I.2 Usurpations d'identité sur les réseaux sociaux

A cause de l'authentification approximative des utilisateurs, plusieurs cas d'usurpations d'identité et de cyberchantage ont été enregistrés sur les réseaux sociaux. Les victimes camerounaises se comptent parmi les hautes personnalités et les citoyens ordinaires. **Plusieurs centaines** de cas d'usurpation d'identité sur les réseaux sociaux ont été enregistrés ces dernières années au Cameroun, dont **cent quatre-vingt-deux (182)** concernaient des membres du Gouvernement.

I.3 Scamming

Le scamming est une fraude perpétrée à travers Internet par des individus malhonnêtes dans le but d'escroquer de l'argent ou un bien de valeur à leurs victimes. Les scammers opèrent de plusieurs manières, parmi lesquelles :

- la création de sites web représentant des entreprises fictives (n'ayant ni existence légale, ni implantation au Cameroun), afin de nouer des contacts et arnaquer des investisseurs étrangers ;
- l'envoi d'e-mails ou de SMS en masse annonçant aux destinataires qu'ils sont bénéficiaires d'une énorme somme d'argent (soit par gain de la loterie, héritage, etc) afin de l'escroquer ;
- la création de faux comptes sur les réseaux sociaux afin d'arnaquer les proches ou les contacts de la victime ;
- le cybercriminel usurpe l'identité d'une personne et simule une situation de détresse dans le but de solliciter l'assistance des proches de cette personne.

Les dommages du scamming au Cameroun sont essentiellement la détérioration de l'image de marque du Cameroun à l'étranger et les pertes économiques. Les pertes économiques liées au scamming sont estimées à environ **quatre (04) milliards de Francs CFA**.

Les principaux foyers d'actes de scamming au Cameroun sont les zones universitaires des villes de Bamenda, Buéa, Yaoundé et Douala.

I.4 Fraude à la carte bancaire

La fraude à la carte bancaire est un acte cybernétique par lequel le cybercriminel obtient de façon illégitime les données de la carte bancaire de la victime afin de les utiliser pour retirer de l'argent dans un distributeur automatique ou faire des achats aux frais de la victime en ligne.

Néanmoins, sur la base d'informations qui nous sont parvenues, l'on peut estimer les pertes dues à la fraude à la carte bancaire à environ **3,7 milliards de Francs CFA**.

I.5 Fraude à la SIMBOX

La fraude à la SIMBOX consiste en l'utilisation d'un boitier électronique (SIMBOX) et du réseau Internet afin de contourner la passerelle des échanges internationaux dans l'acheminement des communications téléphoniques internationales.

L'objectif des auteurs de cette fraude est de faire passer le trafic téléphonique international pour du trafic national et bénéficier ainsi d'une tarification souple. Au cours de ces dernières années, les Opérateurs de télécommunications ont perdu **plusieurs milliards de FCFA** à cause de ce fléau.

II. Statistiques sur la cybersécurité

Dans le cadre du renforcement de la cybersécurité au Cameroun, l'ANTIC a mené plusieurs activités dans les domaines suivants :

- les audits de sécurité ;
- la sensibilisation et les formations sur la cybersécurité ;
- les scans de vulnérabilité ;
- l'émission des bulletins de sécurité ;
- la veille informationnelle ;
- l'assistance des Forces de Sécurité et des usagers dans le traitement des réquisitions et des plaintes liées à la cybercriminalité.

II.2 Sensibilisation et formation sur la cybersécurité

L'ANTIC a organisé, de 2015 à 2017, **cinq (05)** campagnes de sensibilisation sur la cybersécurité dans les chefs-lieux des régions et **soixante-sept (67)** émissions de sensibilisation au Poste National de la CRTV et à FM 105.

II.2.1 Campagnes de sensibilisation sur la cybersécurité

Les campagnes de sensibilisation réalisées par l'ANTIC sont présentées dans le tableau ci-dessous.

Année	2015	2016	2017	TOTAL
Nombre de campagnes organisées	**02**	**02**	**01**	**05**

Année	Villes
2017	**Garoua**
2016	**Ebolowa**

	Bertoua
2015	**Buéa**
	Maroua

II.2.2 Séminaire de formation sur la cybersécurité

Les séminaires de formation organisés par l'ANTIC sont présentés dans le tableau ci-dessous.

Année	Séminaire	Participants
2016	Séminaire de formation des Magistrats de la Région du Centre Yaoundé, du 21 au 22 avril 2016	300
	Séminaire de formation des personnels TIC des Administrations publiques et des Forces de l'ordre sur la cybersécurité Buéa, du 19 au 23 septembre 2016	77
2017	Séminaire de formation des Magistrats de la Région du Littoral Douala, du 04 au 05 mai 2017	180
	Séminaire de formation sur la cybersécurité, la Protection des Infrastructures Critiques d'Information et le Cloud Computing Yaoundé, du 12 au 23 juin 2017	56

II.2.3 Emissions de sensibilisation à la Radio

Les émissions Radio animées par l'ANTIC sont présentées dans le tableau ci-dessous.

Année	2015	2016	2017	TOTAL
Nombre d'émissions au Poste National de la Crtv	**22**	**22**	**13**	**57**
Nombre d'émissions à FM 105	**-**	**-**	**10**	**10**

II.3 Scans de vulnérabilité

Au cours de la période de janvier 2015 à octobre 2017, **quatre-vingt-trois (83)** scans de vulnérabilités de sites web d'Administrations publiques ont été réalisées. Ces scans ont permis de détecter **dix mille neuf cent quatre-vingt-deux (10 982)** vulnérabilités, soit une moyenne de **cent trente-deux (132)** vulnérabilités par site web.

Le tableau suivant présente des vulnérabilités les plus présentes au sein des sites/applications web Départements ministériels et des Etablissements privés durant les scans de vulnérabilité réalisés au cours de la période de 2015 à 2017.

	VULNERABILITE	NOMBRE D'OCCURRENCE
1	**Session Cookie without Secure flag set**	**129**
2	**Session Cookie without HttpOnly flag set**	**126**
3	**Open Ports**	**126**
4	**Clickjacking: X-Frame-Options header missing**	**102**
5	**HTML form without CSRF protection**	**95**
6	**User credentials are sent in clear text**	**85**
7	**POP3 Cleartext Logins Permitted**	**52**
8	**Cross site Scripting**	**50**
9	**SSH server CBC mode ciphers enabled**	**48**
10	**SSL certificate Cannot be Trusted**	**47**
11	**SSL RC4 Cipher Suites Supported**	**43**
12	**Login page password-guessing attack**	**43**
13	**Slow HTTP Denial of Service Attack**	**42**
14	**SSL 64-bit Block Size Cipher Suites Supported**	**40**
15	**SSL Medium Strength Cipher Suites Supported**	**40**
16	**Application error message**	**37**
17	**SMTP Cleartext Logins Permitted**	**36**
18	**SSL Version 2 and 3 Protocol Detection**	**36**
19	**Directory Listing**	**33**
20	**Documentation file**	**28**

II.4 Emission des bulletins de sécurité

L'ANTIC a émis de 2015 à 2017 **trente-six (36)** bulletins de sécurité, contenant un récapitulatif des dernières vulnérabilités des systèmes informatiques utilisés par les Administrations publiques, ainsi que les correctifs associés.