

DPDP et Sécurité

Par : **Miguel SOSSOUHOUNTO**, Manager bjCSIRT
Roland AÏKPE, Analyste Senior bjCSIRT



ANSSI

AGENCE NATIONALE DE LA
SÉCURITÉ DES SYSTÈMES
D'INFORMATION

PRÉSIDENTE DE LA RÉPUBLIQUE DU BÉNIN

SOMMAIRE

- **Panorama des cybermenaces,**
- **Sécurité informatique : points fondamentaux pour un DPDP,**
- **Les règles d'hygiène informatique**



PANORAMA DES CYBERMENACES



ANSSI AGENCE NATIONALE DE LA
SÉCURITÉ DES SYSTÈMES
D'INFORMATION
PRÉSIDENTE DE LA RÉPUBLIQUE DU BÉNIN

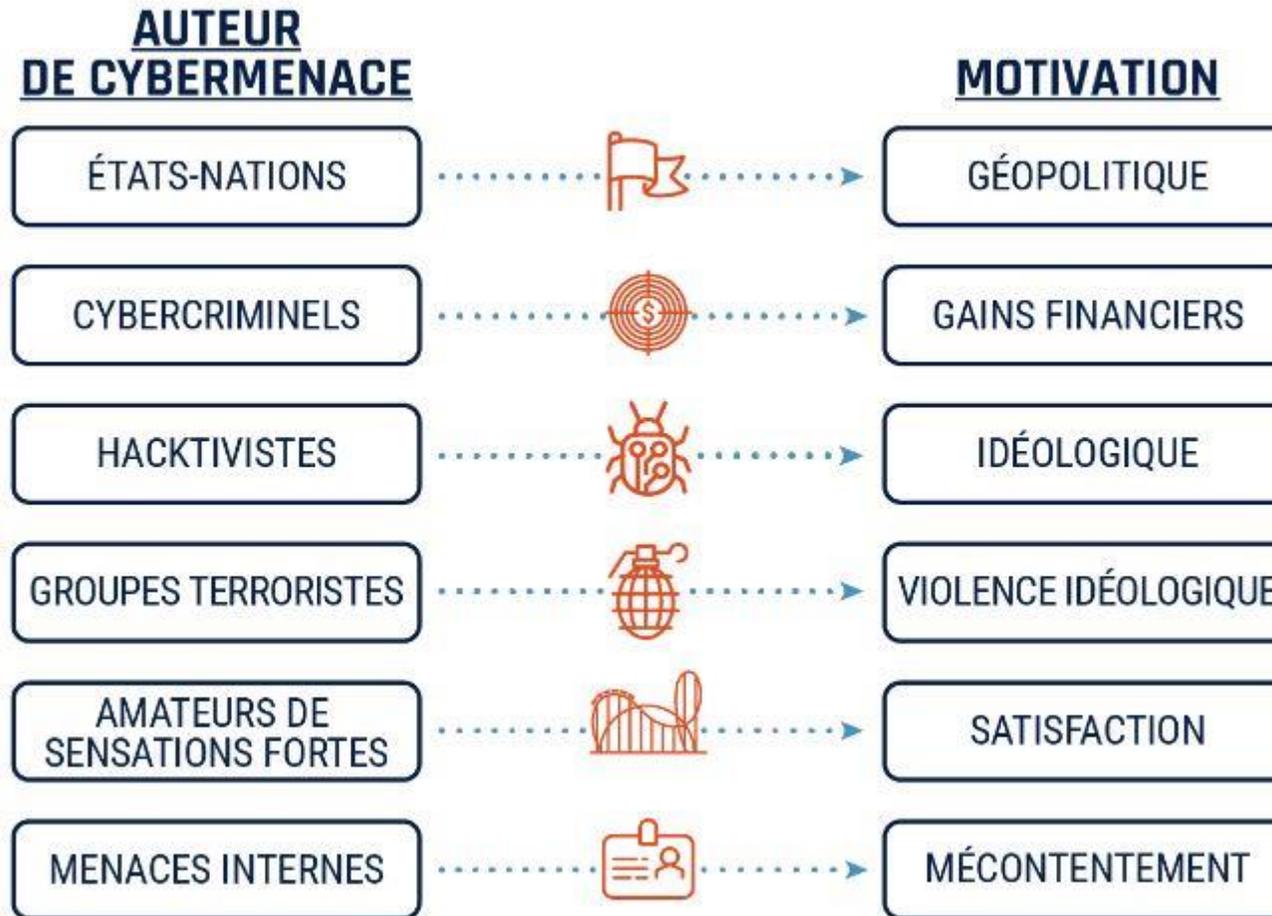
I- PANORAMA DES CYBERMENACES

Une **cybermenace** est une activité qui vise à **compromettre la sécurité** d'un système d'information ou d'une infrastructure d'information en altérant la **disponibilité, l'intégrité ou la confidentialité** du système ou de l'information qu'il contient.

Le cyberspace (environnement des cybermenaces) : est l'espace virtuel où les auteurs de cybermenaces mènent des activités de cybersécurité malveillantes.



I- PANORAMA DES CYBERMENACES



Source : Centre canadien pour la cybersécurité –
introduction à l'environnement de cybermenaces, Page 2



ANSSI AGENCE NATIONALE DE LA
SÉCURITÉ DES SYSTÈMES
D'INFORMATION
PRÉSIDENTE DE LA RÉPUBLIQUE DU BÉNIN

I- PANORAMA DES CYBERMENACES

Les **cybermenaces** peuvent être classifiées en de plusieurs catégories :

Niveau Etat

- Déstabilisation
- Espionnage
- Sabotage
- Cybercriminalité
- Cyber arnaques

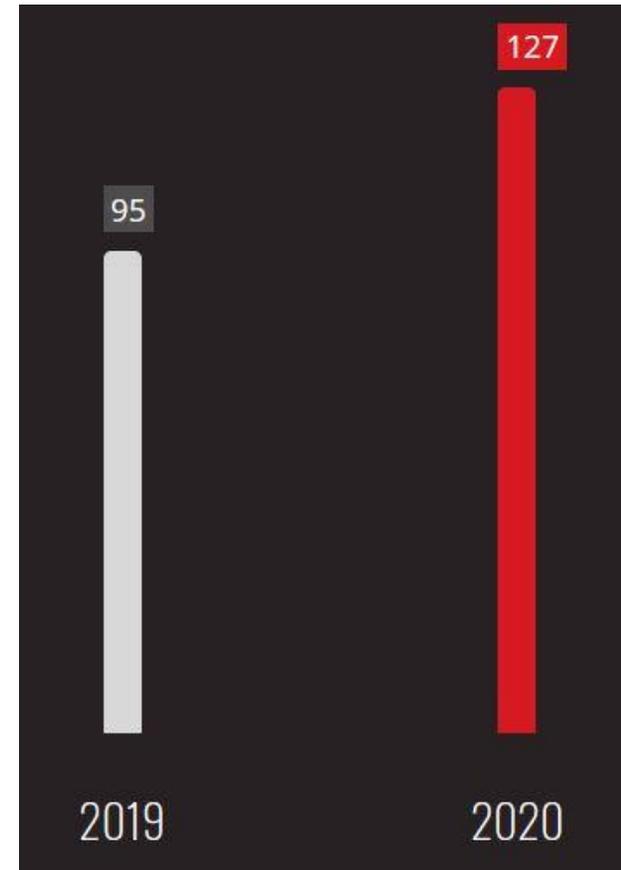
Niveau entreprise ou individu

- logiciels malveillants ;
- Vulnérabilités liées au Supply chain ;
- Business Email Compromise ;
- cyber anarques ;
- risques liés au cloud et IoT;
- menaces persistantes avancées (APT) ;
- failles Zero-Day ;
- etc.

I- PANORAMA DES CYBERMENACES

Logiciels malveillants : Ransomwares

Selon TREND MICRO :



Comparaison du nombre de nouvelles familles de ransomwares en 2019 et 2020

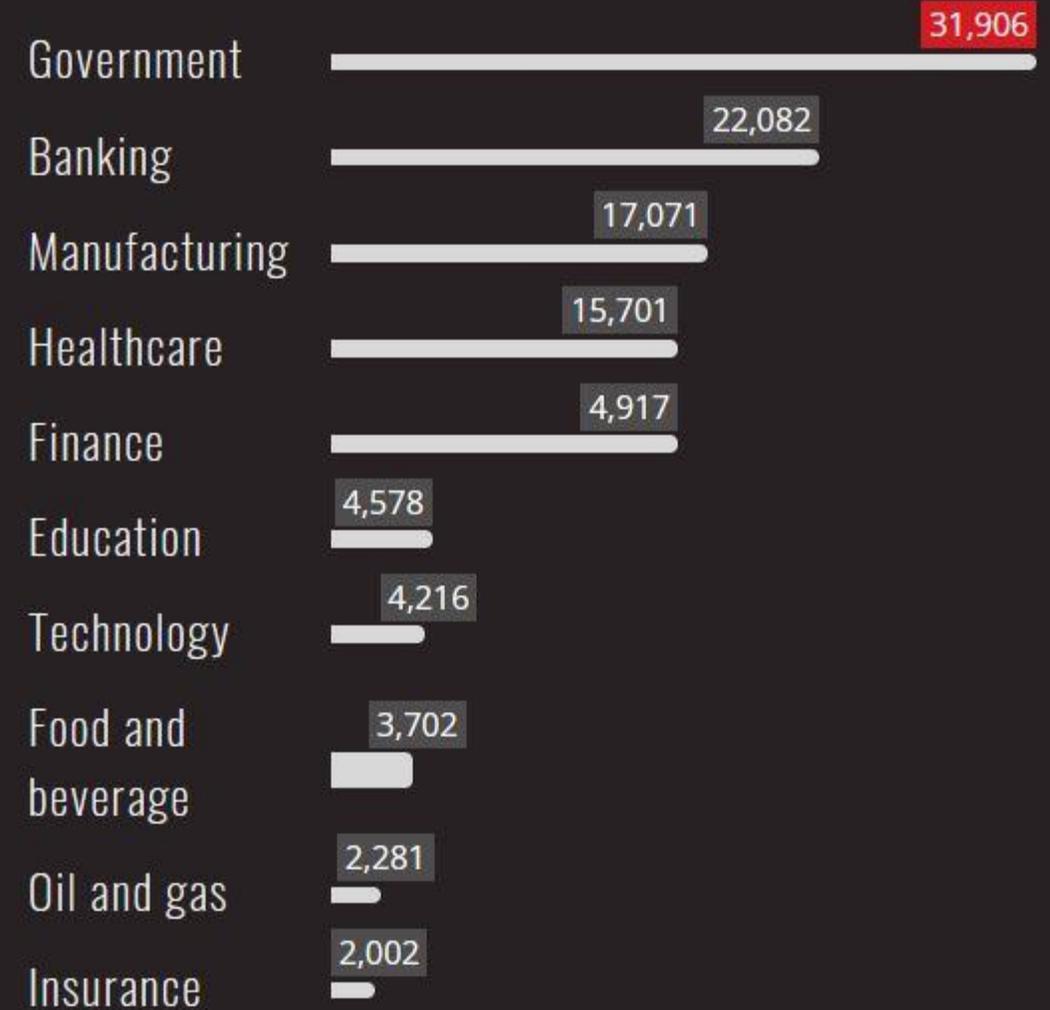


ANSSI AGENCE NATIONALE DE LA
SÉCURITÉ DES SYSTÈMES
D'INFORMATION
PRÉSIDENTE DE LA RÉPUBLIQUE DU BÉNIN

PANORAMA DES CYBERMENACES

Logiciels malveillants : Ransomwares

Les 10 secteurs les plus ciblés par les attaques de ransomware en 2020



ANSSI AGENCE
SÉCURITÉ
D'INFORMATION

PRÉSIDENTE DE LA RÉPUBLIQUE DU BÉNIN

PANORAMA DES CYBERMENACES

Vulnérabilités liées au Supply chain

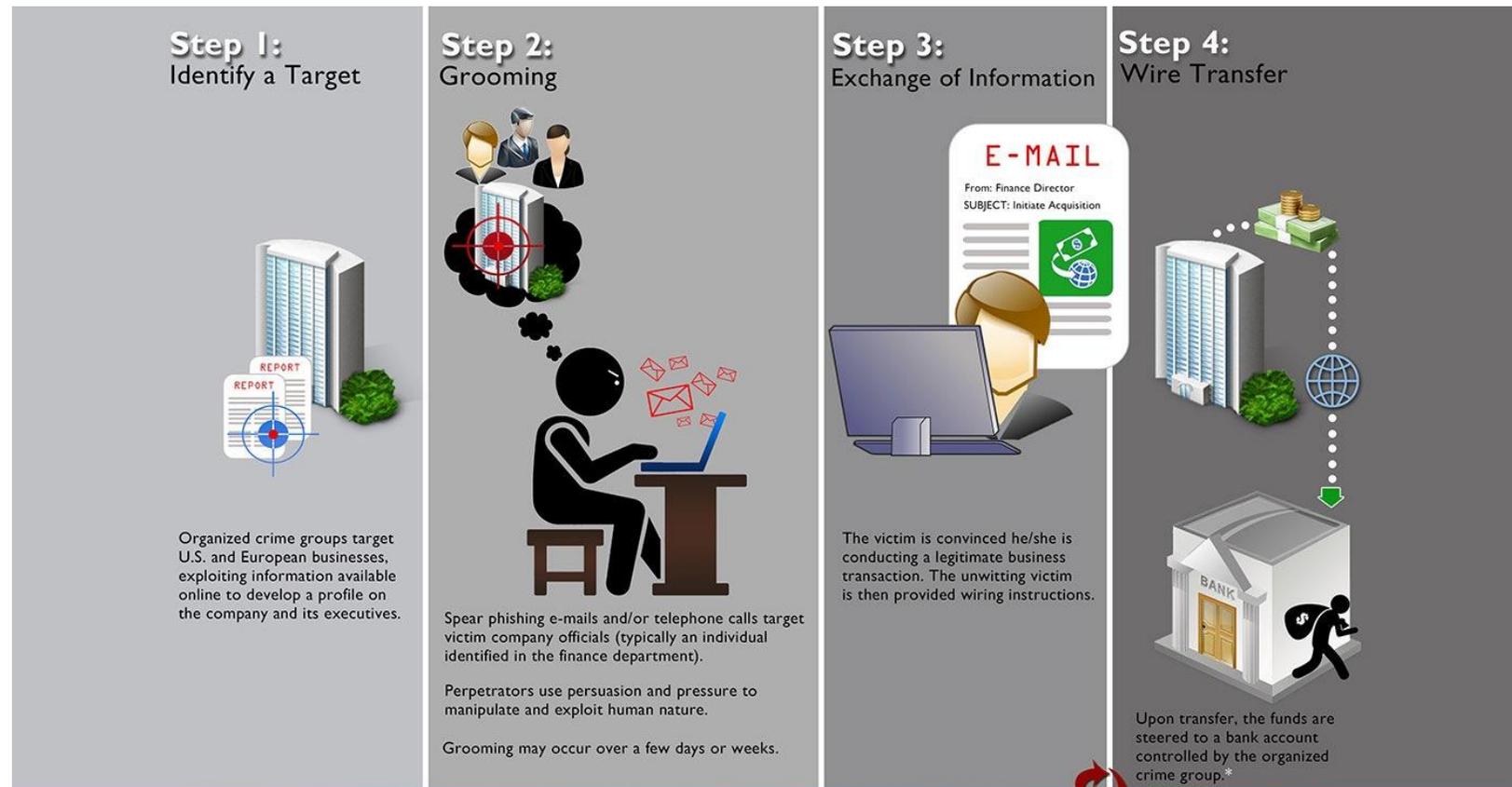


- **Backdoor intégré dans le** logiciel Orion de **SolarWinds** ;
- Attaquant nommé **Sunburst** ;
- **Cible** : Département du Commerce, Département du Trésor, **Département de l'Intérieur, Département de l'Énergie, Département de la Défense**, le département de la Santé et des Services sociaux, ...
- **18 000** institutions ou entreprises, dont Microsoft.



PANORAMA DES CYBERMENACES

Business Email Compromise



Source : <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise>

Business E-Mail Compromise Timeline

An outline of how the business e-mail compromise is executed by some organized crime groups

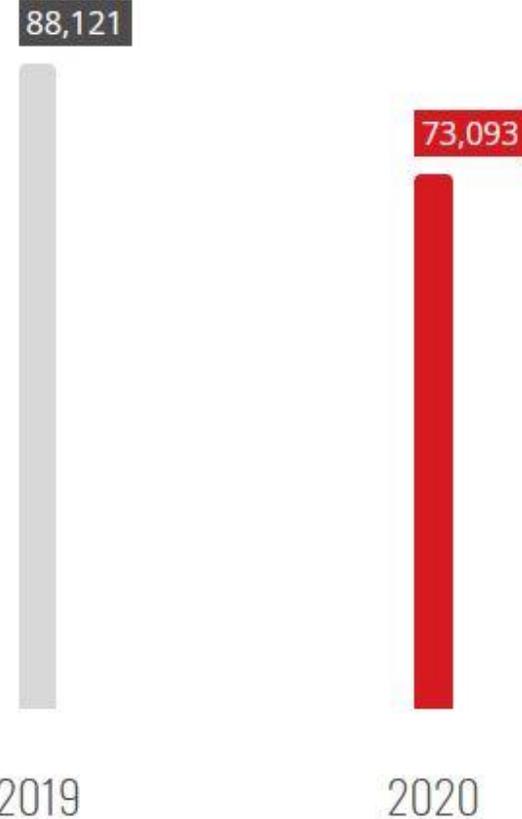


*Note: Perpetrators may continue to groom the victim into transferring more funds.

I- PANORAMA DES CYBERMENACES

Business Email Compromise

Selon TREND MICRO :



Comparaison du nombre de tentatives de BEC détectées en 2019 et 2020



ANSSI AGENCE NATIONALE DE LA
SÉCURITÉ DES SYSTÈMES
D'INFORMATION
PRÉSIDENTE DE LA RÉPUBLIQUE DU BÉNIN

I- PANORAMA DES CYBERMENACES

Business Email Compromise

Au Bénin entre **2020 et 2021**

- au moins **07** attaques, visant de grandes entreprises
- Préjudices : **600 et 700 millions de francs CFA.**



I- PANORAMA DES CYBERMENACES

Cyber anarques

- Toutes formes d'arnaques commises au moyen d'un système informatique ou de la technologie.

Exemples :

- **Faux sites d'e-commerce, de prêts, de bourses, ... ;**
- **Anarques liées aux faux transferts de mobile money ;**
- **Anarques liées aux faux colis ;**
- **Sextorsions, portefeuilles magiques, etc...**



I- PANORAMA DES CYBERMENACES

Cyber anarques

A votre attention:
Les frais de dossier 200\$CAD sont requis avant l'étude de votre demande à envoyer au nom du chargé de la M.R.C.C au BÉNIN

Adresse: 75 Edmonton Street
Gatineau (Québec) J8Y 6W9

Tél
+1 (438) 809-6569

Email
direction@bcbee.org

Working Hour
8h-19h

Bureau Canadien des Bourses d'Études Emplois
Une bourse pour de meilleures études universitaires

[DEMANDE DE BOURSE](#)

ACCUEIL A PROPOS BOURSE D'ÉTUDE ÉTUDIER AU CANADA HÉBERGEMENT PARTENAIRES TÉMOIGNAGES CONTACT

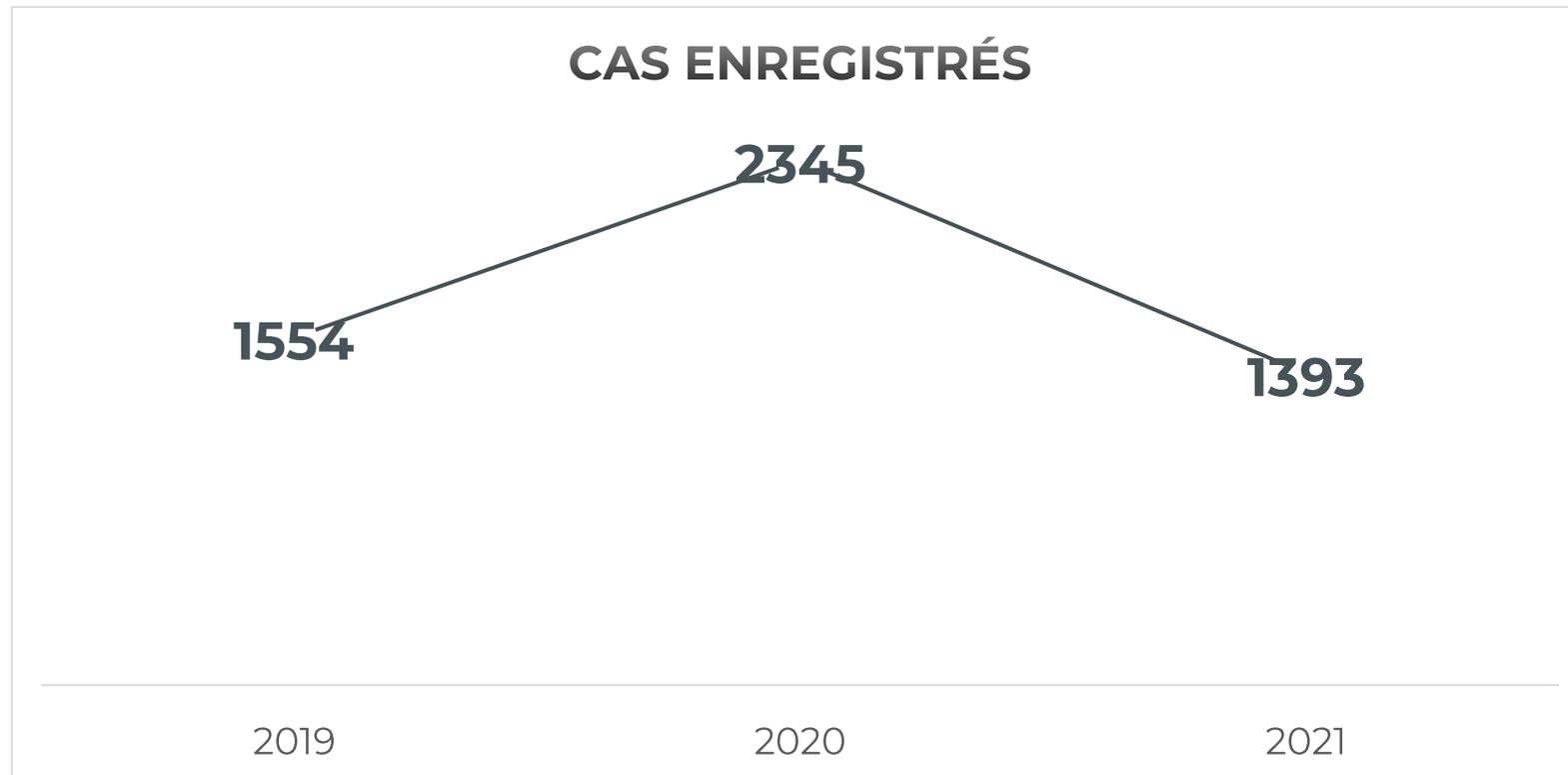
existe beaucoup...

HÉBERGEMENT
LOGEMENTS Trouver un logement dans les grandes villes du Canada

PANORAMA DES CYBERMENACES

Cyber anarques

Au BENIN

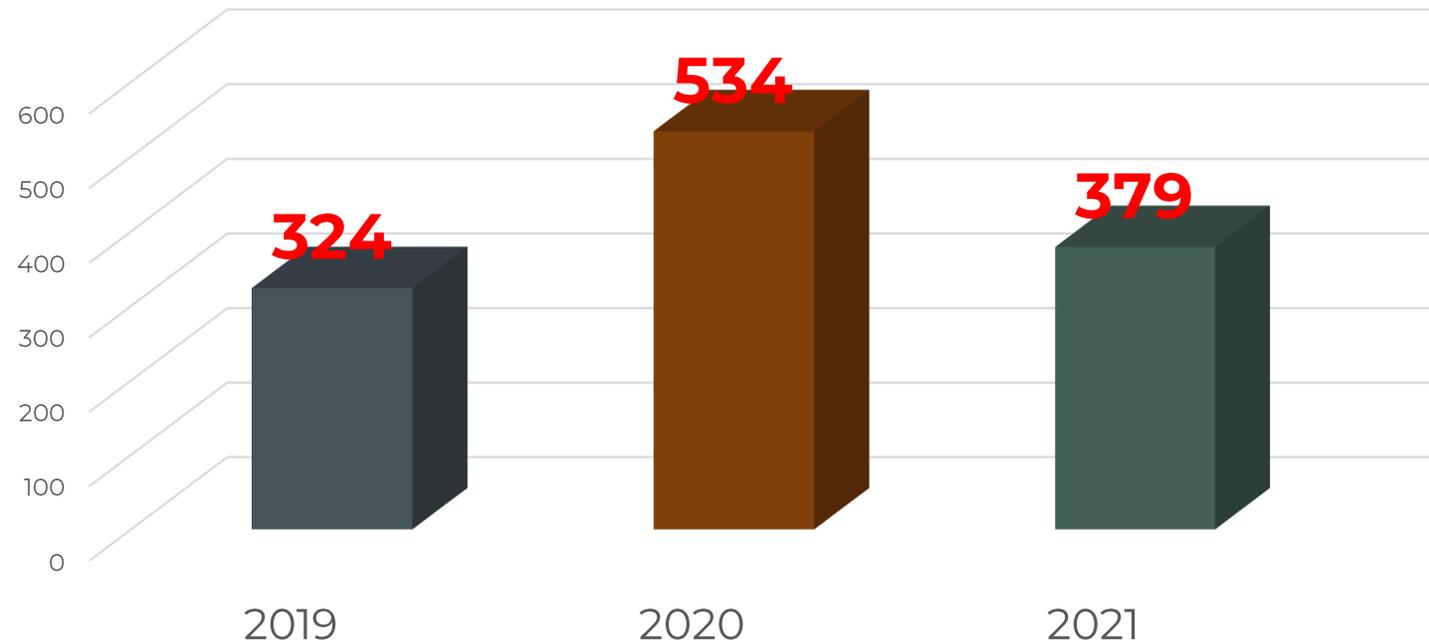


PANORAMA DES CYBERMENACES

Cyber anarques

Nombre de personnes déférées

Au BENIN

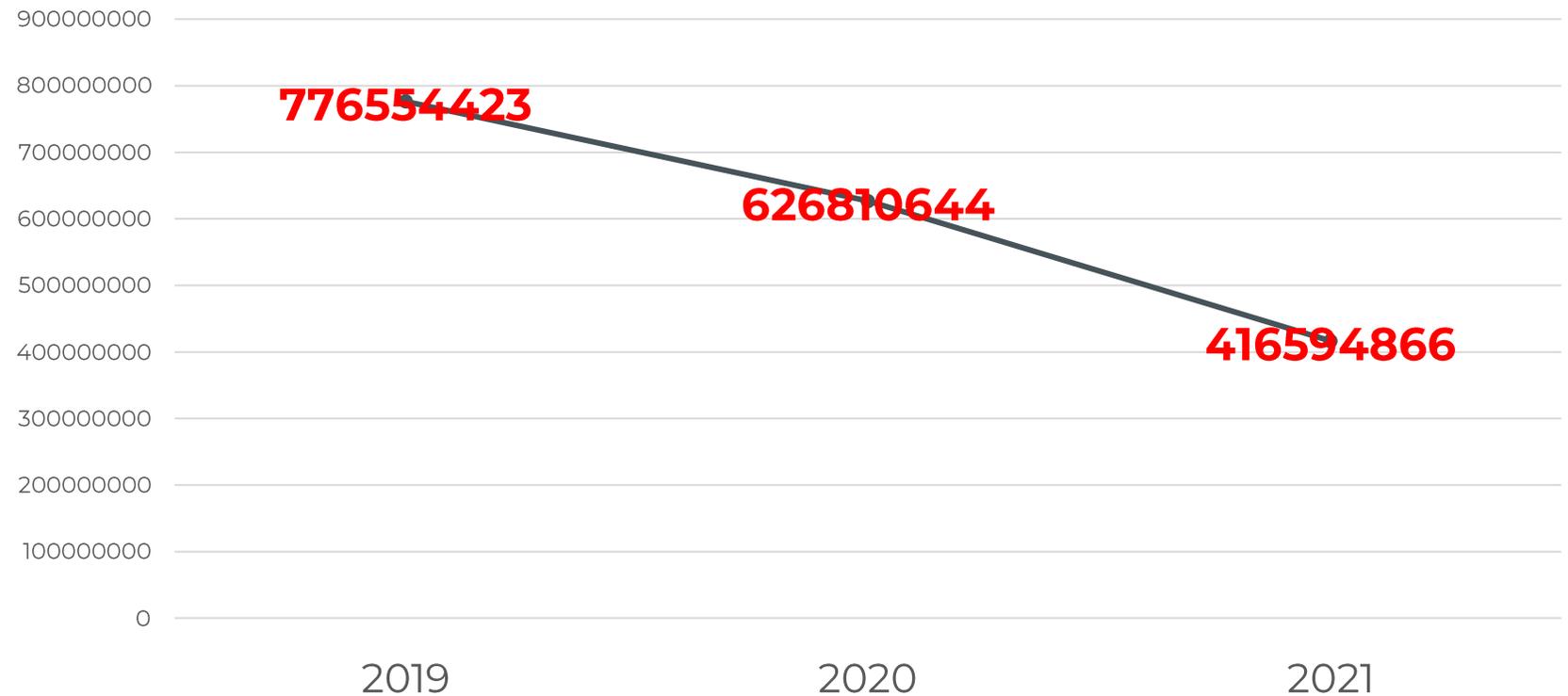


PANORAMA DES CYBERMENACES

Cyber anarques

Au BENIN

Préjudices causés FCFA



ANSSI AGENCE NATIONALE DE LA
SÉCURITÉ DES SYSTÈMES
D'INFORMATION
PRÉSIDENTE DE LA RÉPUBLIQUE DU BÉNIN

I – PANORAMA DES CYBERMENACES

Autres cybermenaces :

- **Menaces persistantes avancées** : se dissimulent et se fondent dans l'activité de la cible pour éviter toute détection.
- **Attaques basées dans le cloud et IoT**: Face à l'adoption massive du télétravail et des plateformes de collaboration dans le cloud, les cybercriminels s'attaquent davantage aux identités qu'aux machines, que ce soit au moyen d'attaques par hameçonnage ciblé ou par la prise de contrôle de comptes.



I – PANORAMA DES CYBERMENACES

- **Failles « zero-day »** : les cybercriminels cherchent les vulnérabilités dénommées « Zero-day » existantes sur les logiciels de messagerie, antivirus, systèmes d'exploitation et les solutions de protection des endpoints.
- **Cryptojacking** : Le domaine des cryptomonnaies est assez récent, mais il n'a pas fallu longtemps pour qu'il attire des personnes mal intentionnées. Le but de ce procédé est d'utiliser, sans votre consentement, la puissance inutilisée de votre ordinateur pour extraire de la cryptomonnaie plus rapidement.



II – SÉCURITÉ INFORMATIQUE : POINTS FONDAMENTAUX POUR UN DPDP



ANSSI AGENCE NATIONALE DE LA
SÉCURITÉ DES SYSTÈMES
D'INFORMATION
PRÉSIDENTE DE LA RÉPUBLIQUE DU BÉNIN

II- SÉCURITÉ INFORMATIQUE : POINTS FONDAMENTAUX POUR UN DPDP

La **sécurité de l'information** fait référence à la protection de l'information et des systèmes d'information qui traite, stocke et transmet l'information contre les accès non autorisés, les divulgations, l'altération et la destruction.

La protection de l'information fait référence aux données :

- **en transit;**
- **au repos.**



ANSSI AGENCE NATIONALE DE LA
SÉCURITÉ DES SYSTÈMES
D'INFORMATION
PRÉSIDENTE DE LA RÉPUBLIQUE DU BÉNIN



II- SÉCURITÉ INFORMATIQUE : POINTS FONDAMENTAUX POUR UN DPDP

Éléments de la sécurité de l'information :

- **Confidentialité** : L'assurance que seules les personnes autorisées ont accès à l'information.
- **Intégrité** : L'assurance que seules les modifications autorisées ont été effectuées.
- **Disponibilité** : L'assurance que les systèmes traitant l'information sont accessibles en cas de besoin par les utilisateurs.



ANSSI AGENCE NATIONALE DE LA
SÉCURITÉ DES SYSTÈMES
D'INFORMATION
PRÉSIDENTE DE LA RÉPUBLIQUE DU BÉNIN



II – SÉCURITÉ INFORMATIQUE : POINTS FONDAMENTAUX POUR UN DPDP

Pour aller plus loin

- La **non répudiation** : La garantie que toutes les actions effectuées dans le système d'information ne peuvent être réfutées par les personnes concernées.
- L'**authentification** : L'assurance que chaque personne faisant parti de l'échange est bien celui qu'il prétend être.



ANSSI AGENCE NATIONALE DE LA
SÉCURITÉ DES SYSTÈMES
D'INFORMATION
PRÉSIDENTE DE LA RÉPUBLIQUE DU BÉNIN



III – REGLES D’HYGIENE INFORMATIQUE



ANSSI AGENCE NATIONALE DE LA
SÉCURITÉ DES SYSTÈMES
D'INFORMATION
PRÉSIDENTE DE LA RÉPUBLIQUE DU BÉNIN

III – REGLES D’HYGIENE INFORMATIQUE

1 - Recommandations sur les mots de passe

- **utiliser la double authentification** sur tous vos comptes supportant ce mécanisme.
- **Choisir des mots de passe d’au moins douze (12) caractères.**
- **Choisir des mots de passe complexes** et qui n’évoquent rien par rapport à votre profil.



ANSSI AGENCE NATIONALE DE LA
SÉCURITÉ DES SYSTÈMES
D'INFORMATION
PRÉSIDENTE DE LA RÉPUBLIQUE DU BÉNIN



III – REGLES D’HYGIENE INFORMATIQUE

1 - Recommandations sur les mots de passe

- **Changer vos mots de passe au moins une fois tous les six(06) mois** ou dès que vous soupçonnez un vol de données.
- Ne pas utiliser pas le même mot de passe partout.
- Ne pas mettre vos mots de passe sur papier.
- Ne pas saisir vos mots de passe sur des sites non sécurisés



ANSSI AGENCE NATIONALE DE LA
SÉCURITÉ DES SYSTÈMES
D'INFORMATION
PRÉSIDENTE DE LA RÉPUBLIQUE DU BÉNIN



III – REGLES D’HYGIENE INFORMATIQUE

2 - Sept astuces pour protéger votre vie privée en ligne

- Installer HTTPS Everywhere sur les navigateurs.
- Installer Privacy badger pour interdire le tracking de vos habitudes de navigation.
- Essayer le Navigateur TOR pour l’anonymat sur internet.



ANSSI AGENCE NATIONALE DE LA
SÉCURITÉ DES SYSTÈMES
D'INFORMATION
PRÉSIDENTE DE LA RÉPUBLIQUE DU BÉNIN



III – REGLES D’HYGIENE INFORMATIQUE

2 - Sept astuces pour protéger votre vie privée en ligne

- Installer AdBlock Plus pour bloquer les publicités.
- Installer Netcraft pour prévenir le phishing.
- Installer Password Checker pour vérifier la force de vos mots de passe.



ANSSI AGENCE NATIONALE DE LA
SÉCURITÉ DES SYSTÈMES
D'INFORMATION
PRÉSIDENTE DE LA RÉPUBLIQUE DU BÉNIN



III – REGLES D’HYGIENE INFORMATIQUE

3 - Recommandations sur la messagerie électronique.

❑ Lorsque que vous recevez un mail :

- Vérifier correctement l’adresse électronique de l’expéditeur.
- Vérifier les informations d’entêtes.
- Scanner toutes les pièces jointes.
- Éviter au maximum de cliquer sur des liens douteux.
- Ne remplir aucun formulaire suspect.



ANSSI AGENCE NATIONALE DE LA
SÉCURITÉ DES SYSTÈMES
D'INFORMATION
PRÉSIDENTE DE LA RÉPUBLIQUE DU BÉNIN

III – REGLES D’HYGIENE INFORMATIQUE

3 - Recommandations sur la messagerie électronique

□ Lorsque vous envoyez un mail :

- Ne mettre pas d’informations sensibles tant que le mail n’est pas chiffré.
- Vérifier que vous avez entré **le bon destinataire**.
- N’utiliser pas vos adresses électroniques professionnelles pour vous enregistrer dans des foras, des sites de marketings, etc.
- Contacter votre service informatique pour l’utilisation de PGP.



ANSSI AGENCE NATIONALE DE LA
SÉCURITÉ DES SYSTÈMES
D'INFORMATION
PRÉSIDENTE DE LA RÉPUBLIQUE DU BÉNIN



III – REGLES D’HYGIENE INFORMATIQUE

4 - Recommandations sur l’usage de téléphones mobiles

- Activer **une protection antivirus** pour mobiles.
- Verrouiller les écrans de vos mobiles.
- **Verrouiller l’accès aux applications** contenant des données sensibles.



ANSSI AGENCE NATIONALE DE LA
SÉCURITÉ DES SYSTÈMES
D'INFORMATION
PRÉSIDENTE DE LA RÉPUBLIQUE DU BÉNIN



III – REGLES D’HYGIENE INFORMATIQUE

4 - Recommandations sur l’usage de téléphones mobiles.

- **Chiffrer vos mobiles.** Sur votre téléphone Android, allez dans Paramètres-->Sécurité-->Chiffrer le téléphone.
- Télécharger vos applications seulement sur les **Store Officiels.**
- **Suivre** votre téléphone à la trace.



ANSSI AGENCE NATIONALE DE LA
SÉCURITÉ DES SYSTÈMES
D'INFORMATION
PRÉSIDENTE DE LA RÉPUBLIQUE DU BÉNIN



III – REGLES D’HYGIENE INFORMATIQUE

5 - Recommandations sur l’usage d’ordinateurs

- **Mettre à jour régulièrement** votre ordinateur et tous les logiciels qui y sont installés.
- Eviter les logiciels **crackés**.
- Chiffrer vos données confidentielles avec **VeraCrypt**.
- Scanner régulièrement votre ordinateur.
- Scanner automatiquement toute clé amovible avec un antivirus professionnel.



ANSSI AGENCE NATIONALE DE LA
SÉCURITÉ DES SYSTÈMES
D'INFORMATION
PRÉSIDENTE DE LA RÉPUBLIQUE DU BÉNIN



QUESTIONS ?



ANSSI AGENCE NATIONALE DE LA
SÉCURITÉ DES SYSTÈMES
D'INFORMATION
PRÉSIDENTE DE LA RÉPUBLIQUE DU BÉNIN

ENJEUX DE SECURITE RELATIFS A L'IDENTITE NUMERIQUE

Par,

l'Agence Nationale de la Sécurité des Systèmes d'Information

Site web: <https://www.anssi.bj>, email: contact@anssi.bj

Twitter: [@anssi_benin](https://twitter.com/anssi_benin)



ANSSI AGENCE NATIONALE DE LA
SÉCURITÉ DES SYSTÈMES
D'INFORMATION

PRÉSIDENCE DE LA RÉPUBLIQUE DU BÉNIN