REPUBLIQUE DU CAMEROUN
***** *****
PAIX-TRAVAIL-PATRIE
***** *****
MINISTRE DE
L'ENSEIGNEMENT SUPERIEUR
***** *****
UNIVERSITE DE YAOUNDE 1
***** *****
ECOLE NATIONALE
SUPERIEURE
POLYTECHNIQUE
***** *****
DEPARTEMENT DE GENIE
INFORMATIQUE

REPUBLIC OF CAMEROON
***** *****
PEACE–WORK-FATHERLAND
***** *****
MINISTRY OF
HIGHER EDUCATION
***** *****
UNIVERSITY OF YAOUNDE I
***** *****
NATIONAL
ADVANCED SCHOOL OF
ENGINEERING
***** *****
COMPUTER ENGINEERING
DEPARTMENT

INVESTIGATION NUMERIQUE

PROJET SOUS LE THEME

Les 10 cas Africain les plus important d'hacking durant les 10 dernières années

MATRICULE	NOMS & PRÉNOMS	FILIERE
22P043	FOUDA CASIMIR	CIN-4
22P071	MINYANDA YONGUI JOSÉ LOÏC	CIN-4
22P056	NNA FRANCIS EMMANUEL ROMEO	CIN-4

Sous la supervision de

Minka Thierry

Table des Matières

INTRODUTION

Depuis une décennie, l'Afrique s'est engagée dans une révolution numérique sans précédent. L'essor des technologies de l'information, la digitalisation des services publics et l'émergence des fintechs ont transformé les économies africaines. Mais cette ouverture numérique s'est accompagnée d'une hausse vertigineuse des cyberattaques.

Selon INTERPOL (2024), le continent enregistre désormais plus de 3 000 attaques par semaine et par organisation, soit une augmentation de 300 % en dix ans. Ces attaques touchent des entreprises privées, des administrations publiques, des ONG, des universités et même des infrastructures stratégiques

Les conséquences sont multiples : pertes économiques, atteintes à la réputation, paralysie de services vitaux et fuite massive de données sensibles.

Dans ce contexte, l'investigation numérique apparaît comme un pilier essentiel pour comprendre, documenter et prévenir les attaques. Elle s'appuie sur la collecte, l'analyse et la présentation des preuves numériques dans un cadre légal et scientifique.

Ce travail présente dix cas africains emblématiques d'hacking survenus entre 2015 et 2025. Pour sélectionner ces cas, nous avons retenu quatre critères d'évaluation permettant de mesurer la gravité et la portée de chaque attaque :

1. La taille de l'attaque — son étendue, sa durée et son niveau de complexité.

2. Le type d'entreprise ou d'organisation visée — publique, privée, institution financière, ONG, etc.

3. Le volume de données affectées — nature et quantité des informations compromises.

4. Les conséquences financières et réputationnelles — pertes monétaires, sanctions ou impact social.

Ces critères, appliqués uniformément, permettent d'identifier les attaques les plus significatives de la décennie, tout en mettant en lumière les faiblesses systémiques du cyberespace africain.

I. CONTEXTE GÉNÉRAL DE LA CYBERSÉCURITÉ EN AFRIQUE

La cybersécurité africaine se trouve aujourd'hui à un carrefour stratégique. L'accélération de la numérisation touche tous les secteurs : télécommunications, énergie, santé, administration, éducation, transport et finance. Cependant, la plupart des pays du continent manquent encore d'une infrastructure solide pour protéger leurs systèmes critiques.

Plusieurs facteurs expliquent cette vulnérabilité :

- **Faible maturité institutionnelle** : la plupart des États ne disposent pas encore de lois complètes sur la cybersécurité.

- **Manque de compétences locales** : en moyenne, on compte moins d'un expert en cybersécurité pour 100 000 habitants.

- **Infrastructures obsolètes** : de nombreux systèmes d'information reposent sur des logiciels non mis à jour.

- **Dépendance extérieure** : hébergement de données à l'étranger, ce qui rend les États dépendants de prestataires non africains.

Les principales menaces observées sont :

- Les ransomwares (rançongiciels) qui chiffrent les données contre rançon ;
- Les fraudes au mobile money et aux systèmes bancaires ;
- L'espionnage numérique à des fins politiques ;
- Les attaques par déni de service (DDoS) contre les plateformes publiques ;
- Et les campagnes de désinformation.

Cependant, la dynamique est en train de changer. Des pays comme le Maroc, le Nigéria, l'Afrique du Sud et le Cameroun se dotent progressivement de centres de réponse aux incidents (CERT), de lois cybernétiques, et de formations universitaires spécialisées.
Cette prise de conscience ouvre la voie à une cybersouveraineté africaine, à condition que la collaboration régionale et les capacités d'investigation numérique soient renforcées.

II. MÉTHODOLOGIE D'INVESTIGATION ET CRITÈRES D'ANALYSE

1. Méthodologie d'investigation

L'investigation numérique s'articule autour de cinq étapes fondamentales :

1. Identification de l'incident : détection précoce de l'attaque et définition du périmètre.

2. Collecte des preuves : acquisition des données à partir des disques, serveurs, journaux et réseaux.

3. Préservation de l'intégrité : copies forensiques, hachage et stockage sécurisé.

4. Analyse technique : utilisation d'outils spécialisés (Autopsy, FTK, EnCase, Wireshark).

5. Rédaction du rapport : documentation rigoureuse, utile aux juridictions et aux décideurs.

Cette démarche permet de retracer la chronologie d'une attaque, d'en identifier les vecteurs techniques et d'en évaluer les conséquences.

2. Critères de sélection des cas emblématique

Chaque cas a été étudié à la lumière de quatre indicateurs :

Critère	Définition	Importance
Taille de l'attaque	Étendue et complexité technique	Mesure la gravité opérationnelle
Type d'organisation ciblée	Nature du secteur (public, privé, stratégique)	Montre la valeur des données visées
Volume de données touchées	Quantité et sensibilité des données compromises	Révèle la profondeur de la brèche
Impact financier et réputationnel	Pertes directes et indirectes	Indique les conséquences économiques et sociales

Ces critères structurent l'analyse des dix cas présentés ci-dessous.

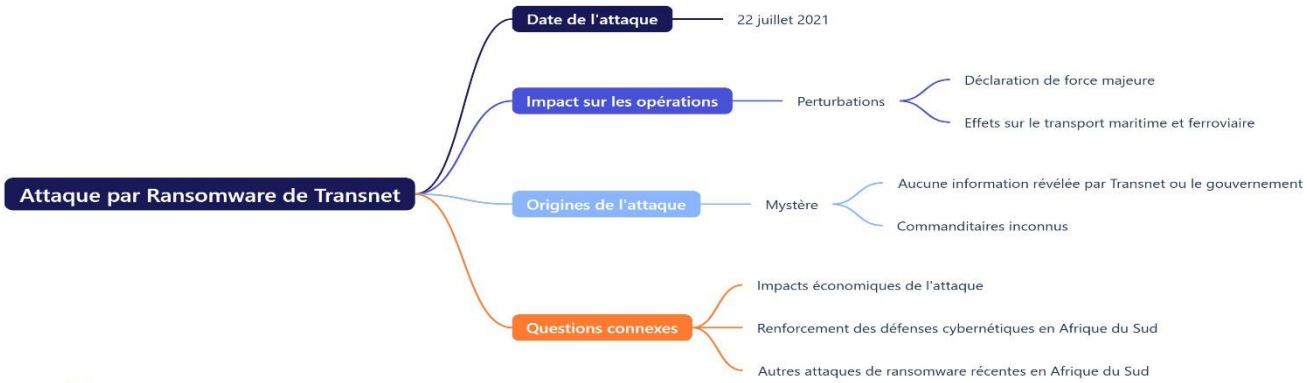
III. LES DIX CAS AFRICAINS LES PLUS EMBLÉMATIQUES D'HACKING

a. Cas 1 - Ransomware sur Transnet (Afrique du Sud, 2021) :

En juillet 2021, l'entreprise logistique publique sud-africaine Transnet a été victime d'une attaque de ransomware (rançongiciel) qui a perturbé gravement ses opérations portuaires et ferroviaires. Cette cyberattaque a entraîné l'arrêt des activités, obligeant le personnel à utiliser des méthodes manuelles et entraînant des retards considérables dans le transport des marchandises. Le groupe de pirates BlackMatter est impliqué dans l'attaque, qui a visé l'obtention d'un gain financier par l'intermédiaire de ransomware..

- **Type d'entreprise** : Entreprise publique de logistique et transport.
- **Taille** : Attaque nationale paralysant les ports de Durban, Cape Town et Ngqura.
- **Volume** : Données logistiques et systèmes ERP chiffrés (plus de 7 To).
- **Impact financier** : Environ 60 millions USD de pertes et 3 semaines d'arrêt partiel.

Illustration de l'attaque de ransomware :

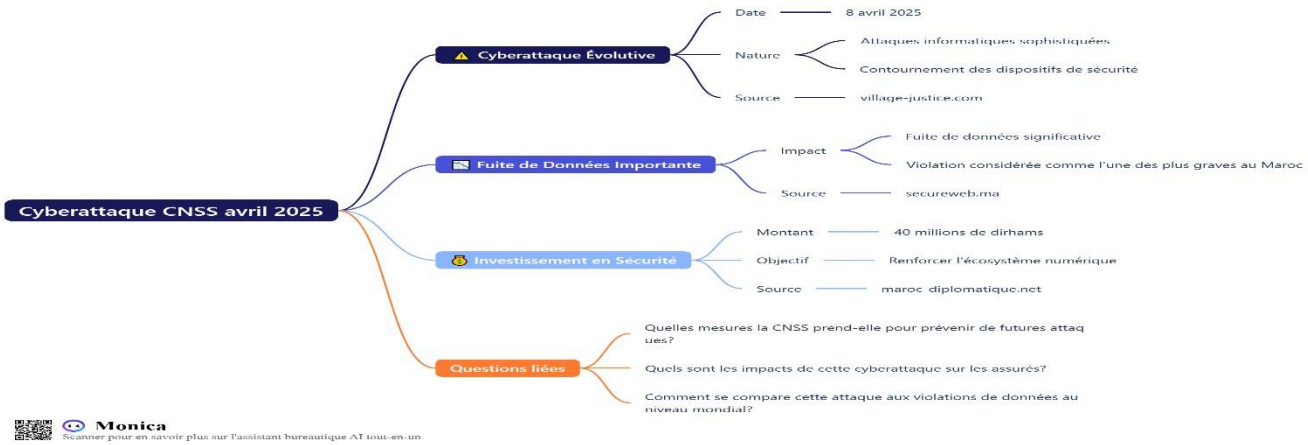


b. Cas 2 - Breach de la CNSS (Maroc, 2025) :

Breach de la CNSS" fait référence à une cyberattaque massive survenue le 8 avril 2025 contre la Caisse Nationale de Sécurité Sociale (CNSS) du Maroc, entraînant l'exfiltration de données de 2 millions de salariés et 500 000 entreprises, y comprenant des informations personnelles comme les numéros d'identification et les salaires. L'attaque a été revendiquée par un groupe se présentant comme algérien et à mise en lumière de graves vulnérabilités de sécurité, notamment l'absence de chiffrement des données.

- **Type d'entreprise** : Organisme étatique de sécurité sociale.
- **Taille** : Atteinte à une base de 2 millions de salariés et 500 000 entreprises.
- **Volume** : Données personnelles, numéros d'identification, salaires et historiques médicaux.
- **Impact financier**: Perte de confiance institutionnelle, amendes internes et coûts de remédiation élevés.

Illustration Breach de la CNSS :

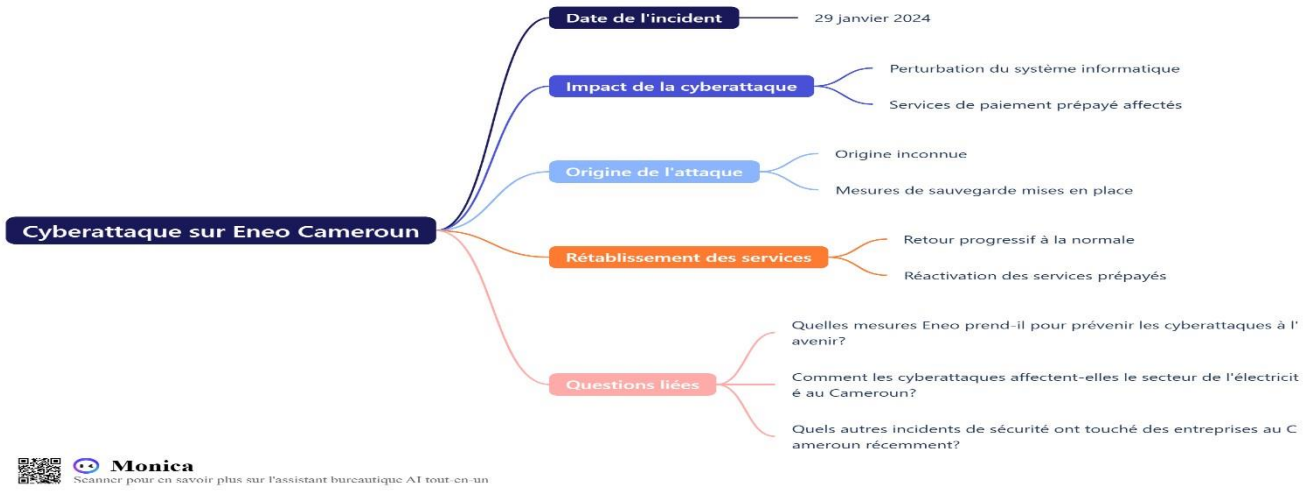


c. Cas 3 Attaque sur Eneo (Cameroun, 2024)

Enéo Cameroun a subi une cyberattaque le 29 janvier 2024, qui a perturbé ses services informatiques, notamment pour les clients prépayés et ceux utilisant des compteurs intelligents, et affecté les services de paiement en ligne. L'entreprise a communiqué sur l'incident, annonçant un retour progressif à la normale et prenant des mesures spécifiques pour les clients post payés

- **Type d'entreprise** : Fournisseur national d'électricité.
- **Taille** : Perturbation des systèmes de facturation et d'achat prépayé.
- **Volume** : Données clients et journaux de transaction compromis.
- **Impact financier** : Estimé à plusieurs centaines de millions de FCFA.

Illustration Attaque sur Eneo :



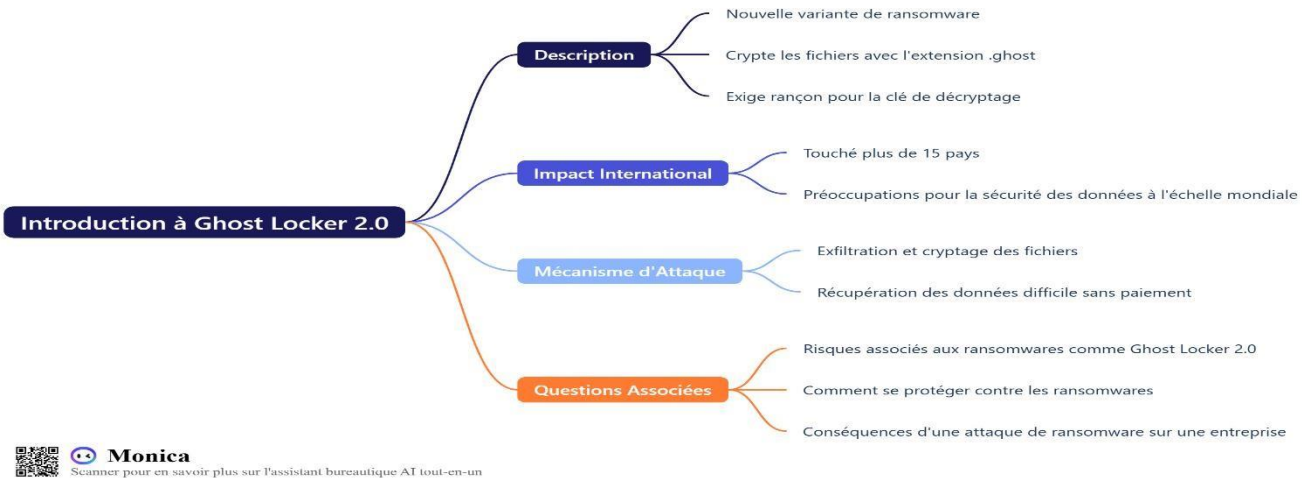
d. Cas 4 Attaque par GhostLocker 2.0 (Egypte, 2024)

En 2024, l'Égypte a été ciblée par **GhostLocker 2.0**, une variante évoluée de ransomware opérée par le collectif **GhostSec**. Cette attaque a visé des infrastructures critiques et des entreprises locales, avec pour objectif de **chiffrer les données** et d'exiger des rançons en cryptomonnaies. GhostLocker 2.0 se distingue par l'usage d'outils d'extorsion double (vol et chiffrement des données), rendant les victimes vulnérables à la fuite d'informations sensibles. L'Égypte, en pleine transformation

numérique, illustre ainsi la **vulnérabilité croissante des États africains** face aux cybercriminels transnationaux.

- **Type d'entreprise** : Entreprises industrielles et gouvernementales.
- **Taille** : Attaque coordonnée sur 30 organisations.
- **Volume** : Données industrielles, documents stratégiques et accès VPN volés.
- **Impact financier** : Environ 20 millions USD de rançon et pertes indirectes.

Illustration de L'Attaque GhostLocker 2.0



e. Cas 5 Le scandale Pegasus au Maroc (2020 – 2021)

- **Type d'entreprise** : Entreprises industrielles et gouvernementales.
- **Taille** : Attaque coordonnée sur 30 organisations.
- **Volume** : Données industrielles, documents stratégiques et accès VPN volés.
- **Impact financier** : Environ 20 millions USD de rançon et pertes indirectes.

Ce ransomware sophistiqué a combiné vol de données et chiffrement simultané. Il a démontré l'efficacité des attaques hybrides et la nécessité de la segmentation réseau.

f. Cas 6 Piratage des banques ivoiriennes

- **Type d'entreprise** : Banques privées (UBA, BNI, NSIA Bank).
- **Taille** : Attaques simultanées sur plusieurs systèmes bancaires.
- **Volume** : Données clients, identifiants bancaires, transactions SWIFT.
- **Impact financier** : 6 millions d'euros de pertes directes.

L'enquête a révélé une campagne de phishing ciblant les cadres bancaires et l'utilisation de Remote Access Trojans (RAT). Ce cas prouve que la cybersécurité humaine reste le maillon faible.

g. Cas 7 Cyber attaque sur les systèmes de santé Tunisien (2021)

- **Type d'entreprise** : Ministère de la Santé et hôpitaux publics.
- **Taille** : Attaque DDoS couplée à un ransomware.
- **Volume** : Dossiers médicaux numériques et serveurs hospitaliers.
- **Impact financier** : Pertes de service évaluées à 2,5 millions USD.

Cet incident a retardé des traitements médicaux critiques. Il souligne l'importance de la cybersécurité sanitaire et de la sauvegarde régulière des systèmes de santé.

h. Cas 8 Piratage de la compagnie Ethiopian AIRLINES (2023)

- **Type d'entreprise** : Compagnie aérienne nationale.
- **Taille** : Compromission mondiale du système de réservation.
- **Volume** : Données personnelles de milliers de passagers.
- **Impact financier** : Indemnités et atteinte à la réputation estimée à 5 millions USD.

Cette attaque illustre les risques de cyber espionnage industriel et la valeur des données de transport aérien à des fins commerciales.

i. Cas 9 Fraude au Mobile Money MTN Nigeria (2018)

- **Type d'entreprise** : Télécom et fintech.
- **Taille :** Réseau mobile de plusieurs millions d'utilisateurs.
- **Volume :** Données transactionnelles et identifiants mobiles.
- **Impact financier** : Environ 8 millions USD de fonds détournés.

Les pirates ont exploité des failles dans les API et bénéficié de complicités internes. Cet incident a conduit MTN à introduire l'IA dans la détection des transactions anormales.

j. Cas 10 Piratge de la banque centrale du Nigeria (2015-2016)

- **Type d'entreprise** : Institution financière étatique.
- **Taille** : Intrusion de longue durée sur les serveurs SWIFT.
- **Volume** : Données financières et courriers internes.
- **Impact financier** : Plusieurs dizaines de millions USD.

Cette attaque, menée par un groupe international, a nécessité l'intervention conjointe du FBI et d'Interpol. Elle a déclenché une refonte complète du système de sécurité bancaire national.

IV. RECOMMANDATIONS

1. Former massivement les experts africains en cybersécurité et forensic numérique
2. Créer des CERT/CSIRT régionaux capables d'échanger en temps réel sur les menaces.
3. Harmoniser les lois africaines autour de la Convention de Malabo.
4. Favoriser l'hébergement local et le développement d'un cloud souverain africain.
5. Renforcer la gouvernance numérique dans les entreprises publiques.
6. Encourager les audits réguliers de sécurité et la sensibilisation des employés.
7. Mettre en place des fonds de cyber-résilience pour aider les PME à se protéger.

CONCLUSION

L'Afrique est à la croisée des chemins : son avenir numérique dépendra de sa capacité à sécuriser ses infrastructures et à former ses talents. Les dix cas présentés montrent que les attaques ne sont pas isolées, mais traduisent une transformation profonde du paysage cybercriminel.

Les institutions publiques, entreprises privées et citoyens doivent désormais considérer la cybersécurité comme une responsabilité partagée.

Renforcer les capacités d'investigation numérique et bâtir une souveraineté technologique ne sont plus des options : ce sont les conditions indispensables pour un développement numérique durable et sécurisé du continent africain.