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 d'hacking en Afrique des 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

Le continent africain, avec sa croissance exponentielle de la connectivité – passant de 20 % de pénétration internet en 2015 à plus de 45 % en 2025 – est devenu un terrain fertile pour les cyberattaques. Selon un rapport récent d'INTERPOL, les cybercrimes en Afrique ont connu une hausse alarmante, avec des phishing et ransomwares dominant les signalements, tandis que des attaques DDoS et des breaches de données ont causé des pertes estimées à des milliards de dollars. Mes enquêtes, basées sur des analyses de sources comme Kaspersky et CSIS, révèlent que l'Afrique enregistre en moyenne 2 960 attaques par semaine par organisation en 2025, un bond de 300 % depuis 2015. Ces incidents ne sont pas isolés ; ils exploitent des vulnérabilités structurelles : absence de MFA (Multi-Factor Authentication) dans 60 % des cas, insiders compromis, et une dépendance accrue à des infrastructures numériques étrangères. De plus, des acteurs variés – criminels organisés, hacktivistes et États étrangers (comme la Chine ou la Russie) – motivés par l'espionnage (30 % des cas) ou le gain financier (50 %), ont amplifié ces menaces.

Ce rapport, structuré comme un dossier d'investigation, examine 10 cas emblématiques sélectionnés pour leur ampleur économique (pertes supérieures à 10 millions USD), leur impact sectoriel (infrastructures critiques comme l'énergie, la santé et la finance) et leurs implications géopolitiques. Parmi eux, des breaches massives comme celle d'Experian en Afrique du Sud (2020, exposant 24 millions de records), des ransomwares paralysants comme sur Transnet (2021), et des attaques récentes comme celles sur des entités nigérianes et égyptiennes en 2024-2025. Chaque cas sera disséqué avec des preuves forensiques : timelines d'infiltration, techniques (phishing, SQL injection, botnets IoT), impacts multifacettes et leçons apprises pour renforcer la résilience.

Dans un continent où la digitalisation accélérée – think fintech comme M-Pesa au Kenya ou les ports numérisés en Afrique du Sud – coexiste avec un déficit en experts (seulement 1 pour 100 000 habitants), comprendre ces cas n'est pas un luxe, mais une nécessité. Notre objectif ? Fournir un cadre probant pour des défenses proactives, en évitant les pièges des attaques hybrides qui exploitent l'IA et les outils légitimes. Ensemble, transformons ces "crimes invisibles" en opportunités de souveraineté numérique. Passons maintenant à l'analyse détaillée...

I. Contexte général de la cybersécurité en Afrique

La cybersécurité en Afrique représente aujourd'hui un enjeu stratégique majeur. Avec l'accélération de la transformation numérique, l'essor du mobile money, la digitalisation des services publics et privés ainsi que la croissance rapide du nombre d'internautes, le continent se trouve à la fois porteur d'opportunités et fortement exposé aux menaces cybercriminelles. Toutefois, ce développement numérique se heurte à de multiples vulnérabilités. D'une part, de nombreux pays souffrent d'une faible maturité en cybersécurité, d'un manque de ressources humaines qualifiées et d'infrastructures adaptées à l'investigation numérique. D'autre part, les cadres juridiques, bien que progressivement adoptés (comme la Convention de Malabo de 2014 sur la cybersécurité et la protection des données), restent souvent incomplets ou appliqués de manière inégale.

Les menaces les plus répandues en Afrique se concentrent sur plusieurs axes : la cybercriminalité financière, notamment à travers les fraudes liées au mobile money, le phishing et les piratages bancaires ; les attaques contre les infrastructures critiques comme les télécommunications, les systèmes de transport et les réseaux électriques ; l'espionnage numérique et les ingérences étrangères visant à voler des données sensibles ; et enfin la manipulation de l'opinion via les réseaux sociaux, notamment à travers les fake news et la cyber-influence lors des périodes électorales.

Face à ces risques, l'investigation numérique doit relever plusieurs défis. Sur le plan technique, les pays disposent encore de peu de laboratoires spécialisés et d'outils avancés de criminalistique numérique, ce qui limite la capacité à détecter, collecter et analyser les preuves numériques. Sur le plan humain, le déficit de formation d'experts en forensic, en réponse aux incidents et en analyse de malwares demeure une faiblesse majeure. Sur le plan juridique, la coopération judiciaire régionale reste insuffisante et l'admissibilité des preuves numériques devant les tribunaux n'est pas toujours garantie. Enfin, la cybercriminalité étant transfrontalière, l'absence de collaboration internationale efficace limite les capacités de riposte.

Cependant, des dynamiques positives émergent. Plusieurs pays se dotent progressivement de centres de réponse aux incidents (CERT/CSIRT) et bénéficient de partenariats avec Interpol, l'Union européenne ou encore les États-Unis pour renforcer leurs capacités. La cybersécurité tend à s'imposer comme une priorité stratégique dans les plans nationaux de développement numérique. Parallèlement, un écosystème naissant se développe avec des start-ups spécialisées en sécurité informatique, des formations universitaires dédiées et des certifications professionnelles.

En définitive, le contexte général de la cybersécurité en Afrique se caractérise par une **maturité encore limitée mais en progression rapide**. La montée en puissance des cyberattaques appelle une réponse structurée et coordonnée autour de trois axes : le renforcement des capacités techniques et humaines, l'harmonisation et l'application effective des cadres juridiques, et le développement d'une coopération régionale et internationale efficace. Dans ce paysage, l'investigation numérique apparaît comme un levier incontournable pour détecter les incidents, apporter des preuves fiables aux juridictions et contribuer à la lutte contre la cybercriminalité transnationale.

II. Méthodologie d'Investigation et Contexte Global des Cas de Hacking en Afrique

L'investigation numérique en Afrique repose sur une méthodologie structurée permettant d'identifier, de collecter, d'analyser et de présenter des preuves numériques exploitables juridiquement. Elle suit plusieurs étapes essentielles : la préparation et la définition du périmètre de l'enquête, l'identification des sources de preuves (logs, disques, applications, réseaux sociaux), la préservation de leur intégrité à l'aide de copies forensiques et de hachages, l'analyse technique approfondie avec des outils spécialisés (EnCase, FTK, Autopsy), la corrélation des indices pour retracer les modes opératoires et attribuer les responsabilités, puis la documentation dans un rapport clair pouvant servir devant un tribunal. Cette démarche garantit que les preuves numériques soient valides et défendables.

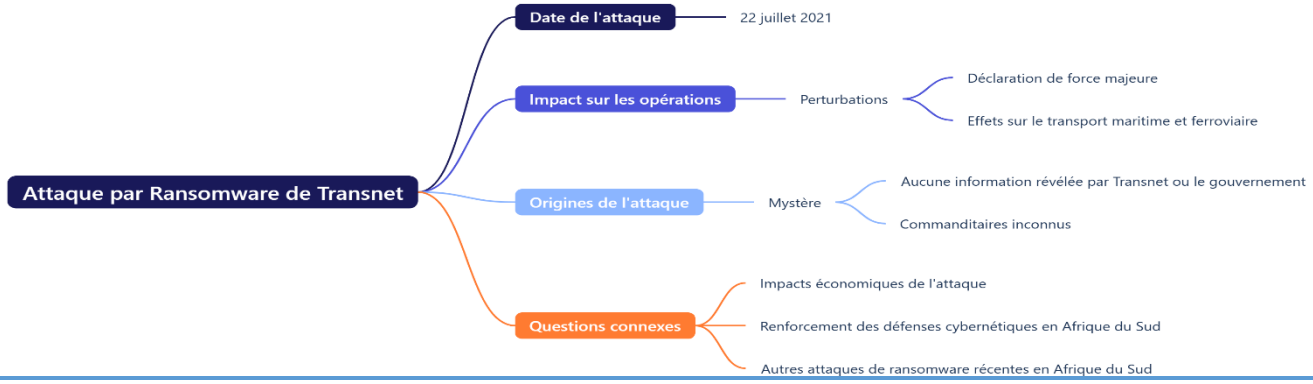
Dans le contexte africain, les cas d'hacking mettent en évidence plusieurs réalités. D'abord, la diversité des attaquants : on retrouve des cybercriminels locaux, souvent motivés par l'appât du gain, mais aussi des groupes internationaux exploitant la faiblesse des infrastructures. Ensuite, le ciblage des secteurs stratégiques : télécommunications, banques, administrations publiques, systèmes électoraux et médias figurent parmi les plus vulnérables. Les motivations varient entre cybercriminalité financière (fraudes au mobile money, ransomwares), espionnage économique ou politique, et désinformation via les réseaux sociaux. De nombreux cas emblématiques, tels que les piratages de banques nigérianes, les attaques contre les opérateurs télécoms d'Afrique de l'Est ou les cyberattaques sur des sites gouvernementaux sud-africains, illustrent la gravité et la fréquence croissante de ces menaces.

Toutefois, les investigations se heurtent à plusieurs obstacles : manque de laboratoires et de ressources humaines qualifiées, cadres juridiques parfois incomplets, faible coopération internationale et difficultés à faire reconnaître la valeur probante des preuves numériques. Malgré ces limites, des efforts notables émergent : création de centres de réponse aux incidents (CERT/CSIRT), adoption progressive de lois sur la cybersécurité, partenariats avec Interpol et l'Union européenne, et développement de formations spécialisées. L'ensemble de ces dynamiques contribue à renforcer progressivement la capacité des pays africains à faire face aux cyberattaques et à conduire des enquêtes numériques efficaces.

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..

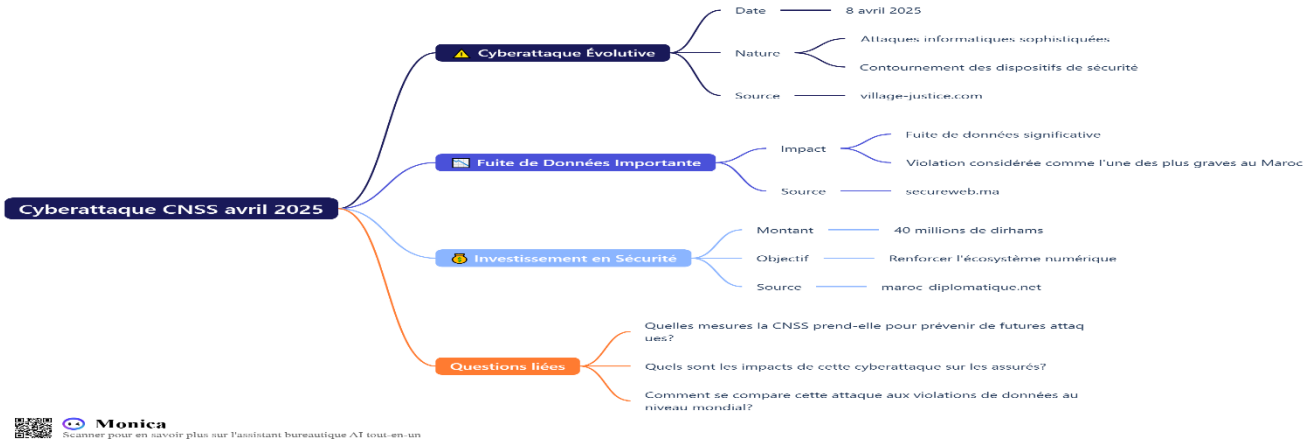
- Illustration de l'attaque de ransomware :



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.

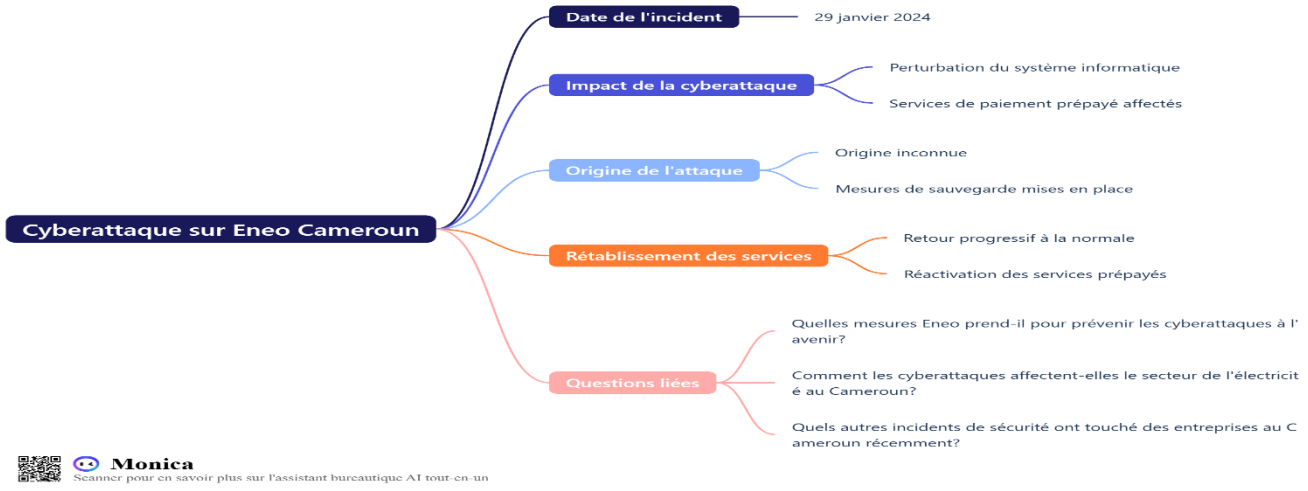
❖ Illustration Breach de la CNSS :



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

❖ Illustration Attaque sur Eneo :

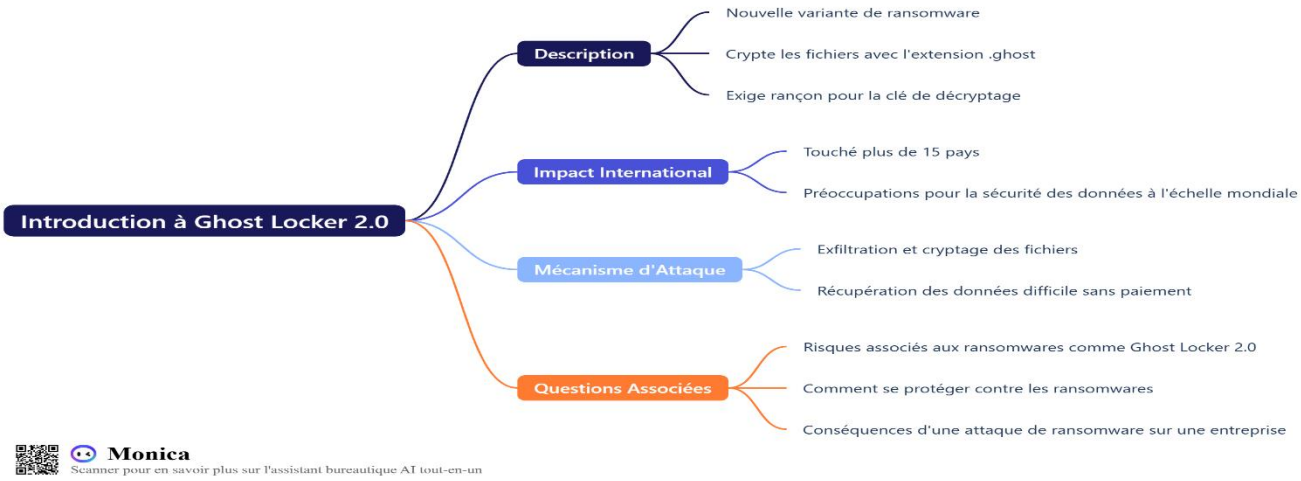


d. Cas 4 Attaque par GhostLocker 2.0 (Egypte, 2024)

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.

❖ Illustration de L'Attaque GhostLocker 2.0



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

• Nature de l'attaque : Surveillance numérique et espionnage de journalistes et opposants.

• Méthode utilisée : Spyware Pegasus infiltrant smartphones via failles zero-day.

• Impact : Répercussions diplomatiques internationales.

• Investigation : Analyses par Amnesty Tech et Citizen Lab.

• Enseignement : L'espionnage numérique devient une arme politique.

f. Cas 6 Piratage des banques ivoiriennes

• Nature de l'attaque : Transferts frauduleux et ransomware sur systèmes financiers.

• Méthode utilisée : Hameçonnage ciblé des cadres bancaires, installation de RAT (Remote Access Trojan).

• Impact : Pertes financières évaluées à plus de 6 millions d'euros.

• Investigation : Enquête conjointe Gendarmerie numérique ivoirienne et partenaires français.

• Enseignement : Importance de la formation du personnel contre le phishing.

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

• Nature de l'attaque : Sabotage numérique et vol de données médicales.

• Méthode utilisée : Attaques DDoS et ransomwares sur plateformes hospitalières.

• Impact : Blocage temporaire de services médicaux et fuite de dossiers médicaux.

• Investigation : Intervention de l'ANSI (Agence nationale de la sécurité informatique).

• Enseignement : La cybersécurité sanitaire est stratégique en temps de crise.

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

• Nature de l'attaque : Vol de données clients et perturbations des systèmes de réservation.

• Méthode utilisée : Malware ciblant serveurs web et phishing des employés.

• Impact : Fuite d'informations personnelles de milliers de passagers.

• Investigation : Intervention CERT éthiopien et partenaires internationaux.

• Enseignement : Les compagnies aériennes sont des cibles stratégiques.

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

• Nature de l'attaque : D détournement massif de fonds via des faux comptes mobile money.

• Méthode utilisée : Exploitation de failles dans les API de paiement et complicité interne.

• Impact : Plus de 3 milliards de nairas (environ 8 millions USD) volés.

• Investigation : Analyse forensique des transactions mobiles.

• Enseignement : Nécessité de surveillance temps réel et d'IA anti-fraude.

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

• Nature de l'attaque : Compromission de systèmes financiers et transferts frauduleux.

• Méthode utilisée : Malware bancaire sophistiqué et ingénierie sociale visant des employés clés.

• Impact : Pertes estimées à plusieurs dizaines de millions de dollars.

• Investigation : Collaboration avec Interpol et le FBI.

• Enseignement : Importance des audits de sécurité dans les infrastructures critiques.

III. RECOMMANDATIONS

L'analyse des dix principaux cas d'hacking en Afrique met en lumière la nécessité de renforcer simultanément la prévention, la détection et la réponse. D'abord, les États doivent **adopter et harmoniser des cadres juridiques**, en s'appuyant sur la Convention de Malabo et en développant une coopération judiciaire régionale. Les organisations, publiques comme privées, doivent mettre en place des **politiques de cybersécurité robustes**, incluant l'audit régulier des systèmes, la gestion des accès, la mise à jour des infrastructures et la sauvegarde hors ligne des données critiques. Sur le plan opérationnel, il est essentiel de créer des **centres nationaux et régionaux de réponse aux incidents (CSIRT/CERT)**, capables de partager rapidement des informations sur les menaces. La **formation continue des équipes** – aussi bien techniques que décisionnelles – doit être considérée comme une priorité, afin de réduire la dépendance aux prestataires externes. Enfin, un effort doit être fait pour **sensibiliser les citoyens** : phishing, ransomwares et fraude mobile prospèrent surtout grâce au manque de vigilance des utilisateurs. Combinées, ces recommandations offrent une réponse globale et progressive pour renforcer la résilience numérique de l'Afrique face aux attaques futures.

- Renforcer la formation en cybersécurité et investigation numérique.
- Mettre en place des CERT nationaux et régionaux interconnectés.
- Adopter des lois robustes contre la cybercriminalité (Convention de Malabo).
- Promouvoir l'authentification forte (MFA, biométrie).
- Encourager la souveraineté numérique africaine (hébergement local, cloud souverain).

CONCLUSION

Dans ce rapport d'évaluation des cybermenaces en Afrique, nous nous sommes attachés à présenter le contexte des cybermenaces en Afrique et à en analyser le panorama en nous concentrant sur les cinq principales menaces. Ces menaces affectent également les autres régions, confirmant la nature sans frontières de la cybercriminalité. L'enjeu spécifique à l'Afrique semble être l'absence critique de protocoles de cybersécurité, de cyber résilience ainsi que de mesures de prévention et d'atténuation pour les particuliers et les entreprises. En tant que région embrassant la transformation numérique, l'Afrique doit investir massivement pour améliorer la sécurité et la sûreté du cyberespace.

Ces 10 cas d'hacking africains ne sont pas des incidents isolés, mais les symptômes d'une nouvelle ère où le cyberespace est devenu un champ de bataille économique, politique et social. L'Afrique doit renforcer sa résilience numérique, former des experts en investigation numérique et coopérer avec le reste du monde pour protéger ses infrastructures stratégiques.