INTERPOL

RAPPORT INTERPOL DE 2024 SUR L'ÉVALUATION DES CYBERMENACES EN AFRIQUE

PERSPECTIVES DU BUREAU POUR LES OPÉRATIONS DE LUTTE CONTRE LA CYBERCRIMINALITÉ EN AFRIQUE

3ème édition

AVRIL 2024

TABLE DES MATIÈRES

AVANT-PROPOS D'INTERPOL

Dans notre monde actuel, les technologies ne sont pas seulement synonymes de confort : elles sont essentielles à notre vie quotidienne. Internet, qui constitue la pierre angulaire de cette ère technologique, est crucial pour gérer les infrastructures critiques, sécuriser les opérations financières, maintenir le lien avec ses proches, faire des achats en ligne et accéder à une mine d'informations et de divertissements. Sa capacité à effacer la distance et à permettre un accès immédiat à des données et des expériences virtuelles en fait un outil indispensable pour tous.

Toutefois, l'ère numérique apporte son lot de défis, à commencer par la menace grandissante de la cybercriminalité. Les méthodes utilisées par les cybercriminels s'adaptent au gré des évolutions technologiques et sont toujours plus élaborées pour exploiter les failles ; la cybercriminalité représente ainsi un risque majeur pour les personnes et les organisations. Les victimes se retrouvent souvent démunies financièrement, psychologiquement et sur le plan affectif. Dans le même temps, le contexte des menaces est exacerbé par les vastes évolutions sociales, économiques et politiques, en particulier l'inégalité croissante entre les pays, organisations et personnes cyber-résilient(e)s et ceux/celles qui ne le sont pas. Tous ces aspects sont exploités par les cybercriminels à l'échelle nationale, régionale et mondiale, laissant derrière eux d'innombrables victimes.

Tandis que nous abordons l'année 2024, nous ne saurions trop insister sur l'importance d'adopter des stratégies globales en matière de cybersécurité. Les entités, quelle que soit leur taille, doivent se protéger contre un vaste éventail de cybermenaces, des attaques traditionnelles aux nouveaux procédés plus complexes.

Cela fait désormais neuf ans qu'INTERPOL pilote un programme international harmonisé et cohérent en matière de cybercriminalité, étayé par sa Stratégie mondiale de lutte contre la cybercriminalité, dont l'objectif est de limiter l'impact mondial de cette forme de criminalité et de protéger les populations pour un monde plus sûr. INTERPOL coordonne et assiste ses 196 pays membres dans le cadre d'activités visant à prévenir et détecter la cybercriminalité, ainsi qu'à enquêter à son sujet et y faire obstacle, en ciblant, d'une part, les infractions les plus préjudiciables et dont les conséquences sont dévastatrices, et, d'autre part, les infractions très fréquentes ou d'intérêt majeur pour les populations que nous souhaitons protéger. Ce programme s'articule autour de trois axes de mise en œuvre, qui fournissent un appui aux pays membres dans les domaines de l'échange d'informations, de la coordination opérationnelle, et de l'élaboration de stratégies / du renforcement des capacités.

Pour ce faire, INTERPOL adopte une approche régionale en vue d'apporter un soutien sur-mesure par l'intermédiaire des Bureaux régionaux pour les opérations de lutte contre la cybercriminalité. Le Bureau pour les opérations conjointes de lutte contre la cybercriminalité en Afrique (AFJOC), financé par le Bureau britannique des Affaires étrangères, du Commonwealth et du Développement, en est un parfait exemple. Ce Bureau est spécialisé dans le recueil et l'analyse d'informations sur les activités cybercriminelles, la coordination d'actions répressives fondées sur le renseignement, ainsi que la promotion de la coopération et des bonnes pratiques dans les pays membres africains, sans oublier la formation de partenariats avec des acteurs publics et privés.

J'ai ainsi le plaisir de vous présenter la dernière édition du Rapport sur l'évaluation des cybermenaces en Afrique. Cette évaluation comprend une analyse globale du contexte des cybermenaces sur le continent africain, en se concentrant plus précisément sur les rançongiciels, les escroqueries aux faux ordres de virement et les autres formes d'escroqueries en ligne. Elle ne se contente pas de dresser l'état des lieux des cybermenaces ; elle s'intéresse également aux initiatives nationales visant à accroître sans cesse la cyber-résilience. Le rapport conclut avec des recommandations stratégiques afin de définir la marche à suivre.

Tout au long de l'analyse, la nécessité absolue de la coopération internationale et régionale entre les services chargés de l'application de la loi pour lutter contre la cybercriminalité s'est révélée incontestable. L'adoption d'une approche harmonisée accroît la capacité à intervenir efficacement contre les menaces via le partage de renseignements et de méthodes d'enquête, et l'exploitation des technologies de pointe.

L'action policière est toujours menée à l'échelle locale et fait partie intégrante de nos sociétés. Néanmoins, les infractions relevant de la cybercriminalité ont une portée mondiale et leur volume, leur ampleur ainsi que leur complexité représentent un défi pour nous tous. Notre responsabilité collective consiste à prévenir, détecter, enquêter sur et neutraliser les individus et groupes qui en sont à l'origine. Nous devons être mieux protégés, aussi bien en tant que particuliers qu'en tant qu'entreprises connecté(e)s à Internet.

Dans cet environnement complexe, un acteur ne peut, à lui seul, assurer notre sécurité collective. Conscient de cela, INTERPOL fait office d'interlocuteur neutre et de confiance qui encourage la collaboration entre les services chargés de l'application de la loi et les secteurs public et privé. En unissant les forces et en mettant en commun l'expertise, INTERPOL vise à renforcer nos défenses collectives contre les cybermenaces, tout en soulignant la responsabilité de tous pour rendre le monde numérique plus sûr.

En conclusion, je souhaiterais remercier nos pays membres de la région africaine et nos partenaires pour leur soutien et leur engagement indéfectibles en faveur de cette cause, ainsi que pour leur participation à cette évaluation. Leur travail acharné et leur détermination sans faille sont essentiels à la réalisation de notre objectif commun : rendre le monde numérique plus sûr pour tous.

Craig Jones
Directeur de la Cybercriminalité
INTERPOL

AVANT-PROPOS D'AFRIPOL

Tandis que nous dressons le bilan de l'année écoulée et que nous nous tournons vers l'avenir, le paysage des cybermenaces en Afrique, de même que dans le monde, évolue et se complexifie sans cesse. La comparaison entre la situation à la fin des années 1990, lorsque l'accès à Internet en Afrique était un luxe réservé à une élite, et celle d'aujourd'hui, où l'on observe un bond de connectivité, illustre la trajectoire remarquable des évolutions technologiques. Cette progression apporte toutefois son lot de défis. La prolifération des cybermenaces s'accélère, touchant les moindres recoins de notre continent et n'épargnant ni les personnes, ni les gouvernements, ni les entreprises.

L'année 2023 a été charnière pour déterminer notre réaction face à ces nouvelles menaces. En s'appuyant sur les bases jetées au cours des années précédentes, la lutte contre la cybercriminalité a considérablement gagné du terrain. Notre collaboration avec INTERPOL n'a jamais été aussi forte, donnant lieu à des initiatives innovantes et au déploiement de technologies de pointe visant à consolider nos cyberdéfenses. La création du centre de données et des bases de données de police scientifique d'AFRIPOL, ainsi que l'inauguration de l'unité d'analyse criminelle, marquent un tournant majeur dans notre démarche de sécurisation de l'environnement virtuel en Afrique.

Le lancement de la Formation intensive aux enquêtes sur la cybercriminalité témoigne, là encore, de la volonté d'AFRIPOL de renforcer les capacités sur le continent. L'élargissement de ces programmes via l'intégration de modules approfondis sur les cybermenaces et les stratégies d'intervention vient compléter notre arsenal de lutte contre les cybercriminels. La participation massive des États membres et l'amélioration notable des compétences du personnel spécialisé dans la cybersécurité sont des signaux très positifs.

En 2023, nous avons développé nos partenariats au-delà de nos alliés traditionnels, en nous associant à de grandes entreprises de technologie et des établissements d'enseignement supérieur. Ces collaborations nous ont permis de bénéficier de recherches et de technologies de pointe, grâce auxquelles nous avons accru notre capacité d'adaptation à cet environnement virtuel en constante évolution. Nous nous sommes également penchés sur les conséquences socioéconomiques des cybermenaces, car nous sommes conscients que la cybersécurité n'est pas qu'un simple défi technique : c'est l'une des pierres angulaires de notre stabilité et de notre croissance économiques. L'économie numérique est en plein essor sur le continent africain, et il est impératif de protéger ce secteur crucial si nous voulons nous assurer un développement durable.

À l'aube de 2024, AFRIPOL est déterminée à multiplier les initiatives dans quatre domaines stratégiques :
1. Conscients du caractère transnational des cybermenaces, nous entendons consolider notre réseau de coopération à travers le continent et avec nos partenaires mondiaux, notamment via l'échange de renseignements, la conduite d'opérations conjointes et l'harmonisation des cadres juridiques afin de faire front commun contre la cybercriminalité. Nous renforçons également la collaboration avec le secteur privé dans le but d'harmoniser et de normaliser les procédures et technologies, ainsi qu'aux fins du recueil de renseignements à travers le continent.

Début 2024, AFRIPOL a signé un protocole d'accord avec Group-IB, un chef de file mondial de la cybersécurité. Ce partenariat accroîtra l'échange de renseignements et dotera les États membres de l'Union africaine de technologies de pointe et de connaissances spécifiques dans des domaines clés comme les enquêtes sur la cybercriminalité, l'ingénierie inverse et la gestion des incidents. En exploitant ces outils et cette expertise avancés, AFRIPOL renforcera ses capacités de protection contre les cybermenaces sur le continent. AFRIPOL prévoit par ailleurs de signer un accord avec Kaspersky, un partenaire privé stratégique.

2. L'une des composantes majeures de notre stratégie consiste en la création d'une cellule spéciale dédiée au partage d'informations sur les incidents cybercriminels et à l'apport du soutien nécessaire aux enquêtes. Nous nous engageons à fournir à nos États membres le matériel et les logiciels essentiels à la conduite d'enquêtes sur la cybercriminalité, ainsi qu'à leur dispenser des formations spécialisées sur ces outils. Parmi les initiatives que nous menons, nous pouvons citer la troisième opération conjointe INTERPOL-AFRIPOL de lutte contre la cybercriminalité, baptisée Cyber Surge Afrique 3, notre formation spécialisée sur les actifs virtuels et la fourniture d'outils d'enquête cruciaux en collaboration avec INTERPOL, chacune d'elles illustrant notre détermination sans faille à renforcer nos capacités de cyberdéfense à travers le continent.

3. Nous continuerons à explorer et intégrer les technologies émergentes, telles que l'intelligence artificielle et les chaînes de blocs, toujours dans l'optique de renforcer nos capacités de cyberdéfense. Ces technologies proposent des solutions prometteuses en termes d'analyse prédictive des menaces, de gestion sécurisée des données et d'affectation efficace des ressources. De plus, nous adoptons les technologies en sources ouvertes dans le cadre de nos programmes de formation, démontrant ainsi notre volonté de surmonter les difficultés financières liées au coût élevé des licences.

4. Nous mettons de plus en plus l'accent sur la mobilisation communautaire et prévoyons de mener des campagnes de cyber-sensibilisation auprès des populations vulnérables, dont les jeunes et les PME. L'éducation de ce public clé aux bonnes pratiques d'hygiène informatique est primordiale pour tuer dans l'œuf le risque représenté par les cybermenaces.

Le chemin qui nous attend est semé d'embûches, mais nous sommes plus déterminés que jamais. Tandis que nous progressons dans l'année 2024, notre vision est claire : bâtir une Afrique numérique sûre et résiliente, dans laquelle les technologies sont une source de progrès, et non un vecteur de vulnérabilité. Ensemble, grâce au soutien indéfectible de nos partenaires et aux efforts collectifs de nos États membres, nous sommes en passe de concrétiser cette vision. Empruntons ce chemin avec détermination et optimisme, car la sécurité du cyberespace est la pierre angulaire de notre prospérité commune.

M. Jalel CHELBA, Ambassadeur
Directeur exécutif par intérim,
AFRIPOL

ABRÉVIATIONS ET ACRONYMES

AFJOC	Opération conjointe de lutte contre la cybercriminalité en Afrique
AMF	Authentification multifacteur
CaaS	Criminalité en tant que service
CERT	Équipe d'intervention informatique d'urgence
CSIRT	Cellule d'intervention en cas d'atteinte à la cybersécurité
DCP	Donnée à caractère personnel
DDoS	Déni de service distribué
ECC	Échange de connaissances sur la cybercriminalité
FOVI	Faux ordres de virement
GLACY+	Action globale sur la cybercriminalité élargie (actuellement GLACY-e)
HC	Hébergement complaisant
IA	Intelligence artificielle
IP	Protocole Internet
ISPA	Programme INTERPOL d'appui à l'Union africaine
LLM	Grand modèle de langage
PCC - Opérations	Plateforme collaborative sur la cybercriminalité - Opérations
PME	Petites et moyennes entreprises
RAT	Cheval de Troie contenant un outil de prise de contrôle à distance
RDP	Protocole de bureau à distance

REMERCIEMENTS

Le présent rapport d'évaluation a été préparé par le Bureau pour les opérations de lutte contre la cybercriminalité en Afrique sous l'égide de l'Opération conjointe de lutte contre la cybercriminalité en Afrique (AFJOC) et avec le financement du Bureau britannique des Affaires étrangères, du Commonwealth et du Développement. Le programme INTERPOL d'appui à l'Union africaine (ISPA) y a également contribué ; ce programme et le présent rapport bénéficient tous deux du soutien du ministère fédéral allemand des Affaires étrangères.

Le présent rapport s'appuie sur l'évaluation des informations fournies à INTERPOL par les pays membres concernés et les partenaires privés de l'Organisation, dont Bi.Zone, Fortinet, Group-IB, Kaspersky Lab et Trend Micro.

RÉSUMÉ

Le présent rapport expose l'analyse des principales cybermenaces touchant le continent africain réalisée par INTERPOL en s'appuyant sur des renseignements internes, des observations opérationnelles, des résultats d'étude et des contributions de partenaires du secteur privé.

Les principales conclusions du rapport mettent en évidence l'intensification de la cybercriminalité à travers le continent, les rançongiciels, les escroqueries aux faux ordres de virement et les autres formes d'escroqueries en ligne ressortant comme les menaces dont l'essor a été le plus rapide en 2023. Les rançongiciels, en particulier, ont été identifiés comme une menace émergente critique qui cible régulièrement des infrastructures essentielles, tandis que les escroqueries en ligne demeurent la cyberinfraction la plus courante contre les particuliers et les entreprises, dont le volume et les conséquences financières sont considérables. Le rapport souligne également l'évolution rapide des cybercriminels et de leur mode opératoire, notamment l'exploitation croissante des médias sociaux, le recours à l'intelligence artificielle et le perfectionnement des techniques d'ingénierie sociale.

Ce document présente en outre les initiatives nationales de lutte contre la cybercriminalité en Afrique, notamment en matière d'évolution législative, de renforcement des capacités des services chargés de l'application de la loi, de partenariats et de mobilisation publique. Bien que les pays membres aient pris des mesures importantes pour renforcer leurs cyberdéfenses et améliorer la riposte des services chargés de l'application de la loi, plusieurs obstacles doivent encore être surmontés afin de parvenir à une approche globale, coordonnée et durable en matière de lutte contre la cybercriminalité à travers le continent.

L'engagement d'INTERPOL envers l'Afrique dans le cadre de la lutte contre la cybercriminalité et l'assistance qu'il fournit dans ce domaine sont manifestes tout au long du rapport. Cela se traduit principalement par une approche régionale spécifique pilotée par le Bureau pour les opérations de lutte contre la cybercriminalité en Afrique d'INTERPOL et mise en œuvre via le projet « Opération conjointe de lutte contre la cybercriminalité en Afrique », financé par le Bureau britannique des Affaires étrangères, du Commonwealth et du Développement. D'autres activités majeures viennent compléter cette initiative, telles que celles menées dans le cadre du Programme INTERPOL d'appui à l'Union africaine et de l'Action globale sur la cybercriminalité élargie.

Le rapport conclut avec des recommandations stratégiques formulées par INTERPOL afin d'évoluer au mieux dans l'environnement des cybermenaces en Afrique et de renforcer la cybersécurité sur le continent. Ces recommandations portent notamment sur l'adoption ou la consolidation de mesures globales et harmonisées en matière de cybersécurité, l'investissement dans les cybercapacités des services chargés de l'application de la loi (personnes, processus et technologies), la création de synergies au sein de l'écosystème de la cybersécurité, la sensibilisation du grand public, ainsi que le renforcement de la coopération internationale et régionale.

INTRODUCTION

Les pays africains vivent une incroyable transformation numérique. En dépit des difficultés persistantes liées à la couverture, l'accès et la qualité des infrastructures, le nombre d'internautes ne cesse de croître à travers le continent : en effet, plus de 160 millions de personnes ont eu régulièrement accès au cyberespace entre 2019 et 2022[1]. L'impact de la migration vers le numérique est manifeste dans bon nombre de secteurs, qu'il s'agisse des infrastructures critiques, du secteur bancaire, ou encore du commerce électronique. Cette transformation touche également de nombreux aspects de la vie quotidienne des citoyens africains, de l'augmentation rapide du nombre de paiements numériques au temps croissant passé en ligne, en particulier sur les plateformes de médias sociaux. À l'échelle individuelle, l'accès à Internet est grandement facilité par la généralisation des téléphones mobiles : pour plus de 650 millions d'Africains, ils représentent le principal moyen d'accès à Internet.

Cette révolution numérique concerne particulièrement la jeunesse africaine, qui représente plus de 60 % de la population du continent[2]. De plus en plus de jeunes utilisent Internet, généralement via leur téléphone mobile, pour communiquer, travailler, transférer de l'argent, faire des achats et laisser libre cours à leur créativité. Les jeunes Africains adoptent rapidement les technologies numériques et contribuent ainsi au développement d'une société dynamique et ancrée dans le cyberespace. Cela crée d'incroyables opportunités pour les pays en termes de maintien de la croissance et d'innovation, mais aussi de nouveaux défis et de nouvelles failles en matière de cybersécurité.

Le nombre croissant d'Africains utilisant Internet, mais aussi d'économies et de sociétés dépendant des technologies, ainsi que l'avènement des « natifs du numérique » élargissent inévitablement le champ des cyberattaques pour les criminels. De fait, la cybercriminalité explose en Afrique, et constitue l'une des menaces qui se propagent le plus rapidement à travers le continent. Le premier Rapport sur l'évaluation des cybermenaces en Afrique, rédigé par INTERPOL en 2021, estimait l'incidence financière de la cybercriminalité dans la région à plus de 4 milliards d'USD, soit environ 10 % du produit intérieur brut total de l'Afrique[3]. Depuis, les défis auxquels sont confrontés les 54 pays membres africains d'INTERPOL n'ont cessé de croître en termes de volume, d'impact et de complexité.

Il est donc plus qu'urgent de remédier au manque de maîtrise numérique, à la préparation inadéquate aux cybermenaces et à l'absence généralisée de bonnes pratiques d'hygiène informatique. Heureusement, les pays africains ont pris des mesures importantes en 2023 en vue de sécuriser davantage les économies numériques et de protéger leur population en ligne. INTERPOL est résolu à accompagner ses pays membres dans la réalisation de ces objectifs. En tenant compte de l'incroyable diversité du continent africain, notamment en termes de cultures, de langues et de situations économiques, des projets et programmes majeurs, à l'instar de l'Opération conjointe de lutte contre la cybercriminalité en Afrique (AFJOC) et du Programme INTERPOL d'appui à l'Union africaine (ISPA), mènent des initiatives essentielles, adaptées aux besoins des différents services nationaux chargés de l'application de la loi.

1 Banque mondiale (2024) : https://www.worldbank.org/en/results/2024/01/18/digital-transformation-drives-development-in-afe-afw-africa

2 Forum économique mondial (2023) : https://www.weforum.org/agenda/2022/09/why-africa-youth-key-development-potential

3 Étude réalisée par l'entreprise de cybersécurité kényane Serianu. Consultable sur : [https://phys.org/news/2021-05-rights-group-tool-stem-cybercrime.html]

PRÉSENTATION DES TENDANCES DANS L'ENVIRONNEMENT DES CYBERMENACES EN AFRIQUE : 2023

En 2023, l'environnement des cybermenaces en Afrique est resté très dynamique, les attaques évoluant rapidement en termes de sophistication et d'ampleur. D'après les renseignements et données opérationnelles issus des activités régionales d'INTERPOL, complétés par les résultats d'un questionnaire transmis aux pays membres africains et les informations fournies par des partenaires du secteur privé, INTERPOL a identifié les principales menaces et tendances ci-après :

Le volume et l'impact de la cybercriminalité ne cessent de croître en Afrique

- Le nombre d'attaques cybercriminelles continue d'augmenter à travers le continent africain, comme indiqué par les pays membres d'INTERPOL[4].
- Plus de deux tiers des pays interrogés ont évalué les infractions dépendant d'Internet et commises à l'aide d'Internet comme représentant un risque moyen à élevé dans leur juridiction. Plus précisément, les pays ont signalé une hausse des répercussions financières et sociales de ce type d'infraction.
- Autre exemple de l'essor rapide de la cybercriminalité en Afrique, l'on estime qu'en 2023, le nombre moyen de cyberattaques hebdomadaires par organisation a augmenté de 23 % en glissement annuel. C'est la moyenne la plus élevée au monde[5].

Les rançongiciels, les escroqueries aux faux ordres de virement et autres escroqueries en ligne sont les cybermenaces ayant connu l'expansion la plus rapide en 2023

- Les précédentes éditions du Rapport d'évaluation des cybermenaces en Afrique d'INTERPOL ont mis en évidence les principales cybermenaces suivantes : les attaques par logiciel malveillant (rançongiciels, chevaux de Troie bancaires et voleurs d'informations), le hameçonnage et les escroqueries en ligne (ex. escroqueries aux faux ordres de virement (FOVI)), et les logiciels criminels en tant que service (logiciels espions et kits de hameçonnage). Ces menaces continuent de peser sur l'environnement virtuel africain et causent des préjudices importants aux populations du continent.
- En 2023, les principales cybermenaces identifiées par les pays membres africains étaient les rançongiciels, les escroqueries aux FOVI et les autres escroqueries en ligne.
- Les rançongiciels ont été cités parmi les plus graves menaces émergentes sur le continent car ils ciblent régulièrement des infrastructures critiques, tandis que les escroqueries en ligne demeurent la principale cyberinfraction contre les personnes et les organisations en termes de volume et d'incidence financière.

Les cybercriminels et leur mode opératoire évoluent rapidement : techniques d'ingénierie sociale plus élaborées et recours accru aux médias sociaux et à l'intelligence artificielle

- Les cybercriminels opérant à la fois en et depuis l'Afrique continuent à exploiter en priorité les failles humaines pour mener leurs attaques. Ils déploient des techniques d'ingénierie sociale toujours plus élaborées pour cibler les personnes et les organisations.
- Le hameçonnage par courriel demeure l'un des premiers vecteurs d'attaque initiaux dans le cadre de nombreuses cyberinfractions, dont les attaques par rançongiciel et diverses formes d'escroqueries en ligne. De plus, les criminels exploitent progressivement différents canaux de communication, tels que les médias sociaux et les applications de messagerie instantanée, suivant ainsi les tendances technologiques et sociales dans la région.
- Les criminels intègrent les évolutions technologiques à leur mode opératoire. Parmi les exemples les plus parlants, citons le recours croissant au vol de données aux fins d'extorsion, ou encore le détournement de l'intelligence artificielle.

4 Cette information s'appuie sur les autodéclarations des pays membres africains. Il convient de noter que la définition de « cybercriminalité » peut varier d'une juridiction à l'autre.

5 Check Point (2023) : https://blog.checkpoint.com/security/average-weekly-global-cyberattacks-peak-with-the-highest-number-in-2-years-marking-an-8-growth-year-over-year-according-to-check-point-research/

Face à la menace grandissante représentée par la cybercriminalité, les pays membres africains ont pris des mesures importantes pour accroître la cyber-résilience et renforcer les capacités des services chargés de l'application de la loi

- Le nombre d'arrestations, d'interventions et d'enquêtes s'est inscrit en hausse grâce au développement des ressources en matière de lutte contre la cybercriminalité. À titre d'exemple, 19 pays membres ont recensé un total cumulé de 10 490 arrestations en lien avec la cybercriminalité entre janvier et décembre 2023. Étant donné que ces pays ne représentent que 35 % du continent, le nombre total d'arrestations en lien avec la cybercriminalité est probablement beaucoup plus élevé.
- Au cours des deux dernières années, une dizaine de pays africains ont adopté, ou ont entamé un processus visant à adopter, une nouvelle législation en matière de cybercriminalité. Cela témoigne d'une démarche proactive de consolidation des cadres juridiques pour lutter contre la cybercriminalité.
- Une augmentation significative des investissements dans la lutte contre la cybercriminalité a également été observée sur le continent, que ces investissements proviennent des pays membres africains ou d'acteurs extérieurs à la région. En 2023, davantage de pays ont créé des unités spécialisées dans la cybercriminalité, près de la moitié ont étoffé le personnel de ces unités, et plus de 60 % ont déclaré participer à des initiatives de renforcement des capacités. Par ailleurs, plus de 130 formations et 40 campagnes de sensibilisation ont été organisées sur le continent.

Néanmoins, des difficultés majeures d'enquête persistent en matière de prévention, de détection, d'enquête et de répression efficaces de la cybercriminalité en Afrique

- La sous-évaluation persistante des cyberinfractions entrave la capacité des services chargés de l'application de la loi à intervenir. Dans certains pays, ce problème est exacerbé par l'absence de plateforme de signalement et d'enregistrement dédiée ou facile à utiliser.
- En dépit de quelques progrès, la collaboration entre les services chargés de l'application de la loi et d'autres acteurs clés (dont le secteur privé et les services chargés de la cybersécurité) demeure difficile dans certaines juridictions.
- L'hygiène informatique insuffisante continue de saper la cyber-résilience à travers le continent ; en effet, la plupart des organisations et des citoyens africains sont peu préparés à faire face aux cyberattaques.

Les sections suivantes présentent une analyse approfondie des tendances liées aux principales cybermenaces identifiées par les pays membres d'INTERPOL en Afrique : les rançongiciels, les escroqueries en ligne et les escroqueries aux faux ordres de virement.

RANÇONGICIELS ET EXTORSION EN LIGNE

Points clés :

- Les rançongiciels et l'extorsion en ligne ont le vent en poupe, plus de la moitié des pays membres africains d'INTERPOL ayant signalé des attaques contre leurs infrastructures critiques.
- Les courriels de hameçonnage demeurent les vecteurs d'attaque les plus courants dans le cadre des attaques par rançongiciel en Afrique, tandis que les méthodes d'extorsion et le modèle économique adoptés par les cybercriminels évoluent.
- Dans l'ensemble, les pays membres africains prennent des mesures en vue d'accroître leur résilience face aux attaques par rançongiciel, mais des difficultés persistent, en particulier s'agissant du signalement des attaques et du paiement des rançons.

Les rançongiciels et l'extorsion en ligne ont le vent en poupe en Afrique

Les rançongiciels et l'extorsion en ligne ont été identifiés par les pays membres d'INTERPOL comme l'une des plus graves cybermenaces sur le continent africain. Ces attaques sont particulièrement préoccupantes en raison de leur forte incidence financière, de leur capacité à perturber gravement les infrastructures critiques et les services essentiels, ainsi que des préjudices qu'elles peuvent causer aux organisations et aux personnes touchées. L'ampleur du problème est évidente : d'après l'entreprise de cybersécurité Chainalysis, les paiements de rançon dans le cadre de ces attaques s'élevaient à plus de 1 milliard d'USD dans le monde en 2023[6].

Le volume, la fréquence et l'impact des attaques par rançongiciel ne cessent de croître en Afrique. Une étude réalisée par l'entreprise de cybersécurité Check Point révèle qu'en moyenne, une organisation africaine sur 15 a été victime d'une tentative d'attaque par rançongiciel chaque semaine au cours du premier trimestre 2023. Ce chiffre est plus élevé que la moyenne hebdomadaire mondiale d'environ une organisation sur 31[7]. Au cours d'une seule semaine en février 2023, le partenaire privé d'INTERPOL Kaspersky a déclaré avoir détecté plus de 300 tentatives d'attaque par rançongiciel en Afrique du Sud, ce qui illustre la fréquence croissante des attaques[8]. Leurs répercussions financières semblent également s'inscrire en hausse : d'après IBM, le coût moyen d'une attaque par rançongiciel était de 5,13 millions d'USD en 2023, soit une hausse de 13 % par rapport à 2022[9].

Les infrastructures critiques africaines dans le viseur

Plus inquiétant encore, près de la moitié des pays africains interrogés ont signalé des attaques par rançongiciel ciblant leurs infrastructures critiques entre janvier et décembre 2023. Il s'agit notamment des attaques ciblant les infrastructures publiques, les hôpitaux, les établissements financiers et les fournisseurs d'accès à Internet. À titre d'exemple, ces dernières années, Electricity Company of Ghana (ECG) (le plus grand distributeur d'électricité du pays), les banques nationales de la Zambie et du Soudan du Sud, des organismes publics de l'Éthiopie, du Sénégal et du Zimbabwe, ou encore le fournisseur d'accès à Internet sud-africain RSAWEB ont tous été victimes d'attaques par rançongiciel. Même l'Union africaine a été la cible d'une attaque paralysante menée par le groupe BlackCat (également connu sous le nom d'ALPHV) contre son réseau interne en 2023, dont les conséquences ont pu être atténuées par INTERPOL et ses partenaires[10]. Le ciblage des infrastructures critiques est particulièrement alarmant, tandis que la transformation numérique poursuit son accélération sur le continent et que les systèmes essentiels sont de plus en plus interconnectés.

Outre les infrastructures critiques, les pays membres africains ont signalé des attaques par rançongiciel ciblant diverses entreprises dans des secteurs comme la finance, l'industrie et le commerce de détail. À titre d'exemple, d'après la société de sécurité informatique Sophos, 78 % des entreprises sud-africaines ont été victimes d'attaques par rançongiciel en 2023[11]. Parmi les attaques de grande envergure, nous pouvons citer celles contre le siège de Porsche à Johannesburg, en Afrique du Sud, et contre la division sud-africaine du bureau de crédit international TransUnion. Ces tendances sont en droite ligne avec les évolutions mondiales. D'après des données compilées fournies par des partenaires du secteur privé d'INTERPOL, si les secteurs bancaire, public, du commerce de détail, des technologies et de la santé sont les plus touchés à l'échelle mondiale, aucun(e) secteur, organisme ou organisation n'est à l'abri d'une attaque par rançongiciel.

6 Chainalysis (2024) : https://www.chainalysis.com/blog/ransomware-2024/

7 Check Point (2023) : https://blog.checkpoint.com/research/global-cyberattacks-continue-to-rise/

8 News24 (2023) : https://www.news24.com/fin24/companies/rsaweb-victim-of-cyberattack-as-wave-of-ransomware-attempts-hits-sa-in-past-week-20230206

9 IBM (2023) : https://www.ibm.com/reports/data-breach

10 Le Monde (2023) : https://www.lemonde.fr/afrique/article/2023/04/25/vent-de-panique-a-l-union-africaine-apres-une-nouvelle-cyberattaque_6170976_3212.html

11 Sophos (2023) : https://news.sophos.com/en-us/2023/05/10/the-state-of-ransomware-2023/

Exploitation persistante de l'élément humain

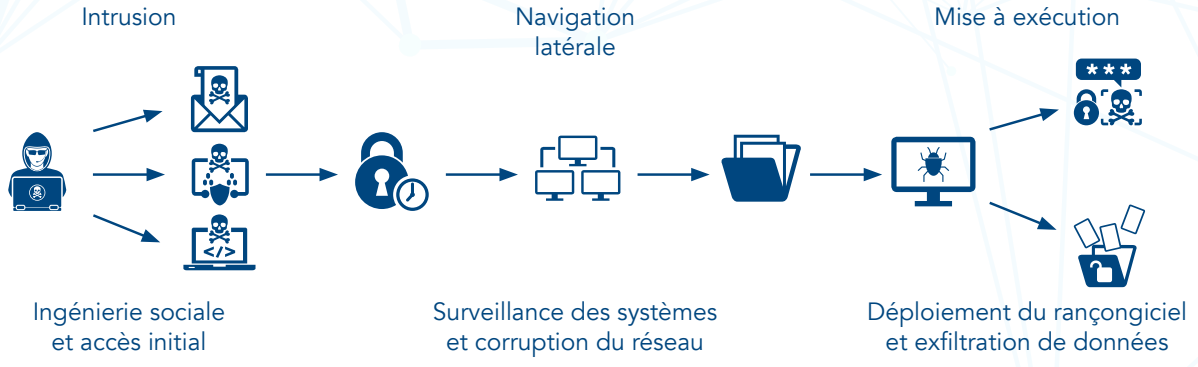
S'agissant du mode opératoire, **il semblerait que les courriels de hameçonnage constituent les vecteurs d'attaque les plus courants** dans le cadre des attaques par rançongiciel en Afrique ; **en effet, près de la moitié des pays membres africains d'INTERPOL ont signalé des cas de hameçonnage au cours de ces attaques.** Ces courriels contiennent généralement un fichier ou lien malveillant, conçu pour faciliter l'accès à un système par un cybercriminel ou pour déployer un logiciel malveillant à l'ouverture du fichier ou du lien. Les autres méthodes d'infection couramment utilisées par les groupes spécialisés dans les attaques par rançongiciel en Afrique comprennent l'exploitation de connexions par protocole de bureau à distance (RDP) non sécurisées et d'autres failles. Ces tendances régionales sont cohérentes avec les conclusions tirées à l'échelle mondiale par le partenaire privé d'INTERPOL Trend Micro[12]. D'après l'entreprise de cybersécurité, les vecteurs d'attaque initiaux les plus couramment utilisés par les groupes spécialisés dans les attaques par rançongiciel dans le monde sont les courriels, Internet et les applications en ligne, les logiciels malveillants comme les fausses applications mobiles, et l'exploitation des failles des systèmes, telles que les connexions par RDP non sécurisées.

Il est primordial de comprendre comment les cybercriminels parviennent à accéder aux systèmes en vue de déployer des rançongiciels afin d'améliorer la prévention, la détection et l'atténuation de ces attaques. Il convient de noter que la plupart des vecteurs d'attaque exploitent l'élément humain, qu'il s'agisse d'un utilisateur cliquant sur un lien malveillant ou d'un administrateur informatique oubliant de mettre à jour ou corriger régulièrement ses systèmes. Une étude réalisée par l'entreprise de cybersécurité Fortinet, partenaire du projet Gateway d'INTERPOL, révèle que bon nombre de groupes spécialisés dans les attaques par rançongiciel passent désormais plus de temps à choisir et se renseigner sur leurs cibles[13]. Ils exploitent les informations figurant sur les comptes personnels de médias sociaux, les sites Web d'entreprise et les pages consacrées à des conférences, ainsi que celles issues de précédentes fuites de données, pour mener des attaques par ingénierie sociale plus efficaces et accéder aux systèmes en vue de déployer des rançongiciels.

Évolution des tactiques d'extorsion en ligne

Une fois que les cybercriminels sont parvenus à accéder au système, ils visent généralement à cartographier l'infrastructure réseau de leur cible et à naviguer latéralement dans le système en exploitant les failles et en élargissant leurs droits. C'est alors qu'ils déploient un logiciel malveillant qui crypte les données, puis demandent une rançon à leurs victimes en échange de la restauration des fichiers. Afin d'augmenter la pression exercée sur leurs cibles, de nombreux groupes ont recours à des logiciels basés sur la peur ou à d'autres tactiques d'extorsion. Par exemple, les cybercriminels peuvent exfiltrer des données avant de les crypter, puis menacer de divulguer des informations sensibles (double extorsion), mener des attaques d'interruption de service pour paralyser les cibles refusant de payer la rançon (triple extorsion), voire menacer les partenaires tiers de leurs victimes principales en vue d'intensifier la pression (quadruple extorsion).

Ces dernières années, INTERPOL a observé une hausse de l'exfiltration de données aux fins d'extorsion en ligne. Après s'être introduits dans le système de leur cible, certains groupes spécialisés dans les attaques par rançongiciel préfèrent désormais passer l'étape du chiffrement et se contentent d'exfiltrer les données sensibles. Ils menacent ensuite de divulguer ces informations si la victime refuse de payer une rançon. En raison des risques de préjudice financier, psychologique et d'atteinte à la réputation que comporte une telle divulgation, la plupart des organisations sont plus enclines à payer la rançon. Ces paiements peuvent représenter plusieurs millions de dollars, alors même que l'effacement des données volées par les cybercriminels n'est en aucun cas garanti. Au vu de son potentiel lucratif, l'exfiltration de données s'impose rapidement comme un mode opératoire privilégié, tant à la place de qu'en association avec le chiffrement, la transformation des rançongiciels et l'extorsion en ligne.



Déploiement du rançongiciel et exfiltration de données

12 Trend Micro (2023) : https://newsroom.trendmicro.com/2022-08-31-Trend-Micro-Warns-of-75-Surge-in-Ransomware-Attacks-on-Linux-as-Systems-Adoptions-Soared

13 Fortinet (2023) : https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2023-ransomware-global-research.pdf

Les programmes d'affiliation et l'essor de l'écosystème des services cybercriminels

Outre l'évolution du mode opératoire, l'impact croissant des attaques par rançongiciel s'explique en partie par l'émergence de nouveaux modèles organisationnels adoptés par les cybercriminels. INTERPOL et ses partenaires ont observé que de nombreux groupes spécialisés dans les attaques par rançongiciel géraient désormais des programmes d'affiliation complexes, notamment via le développement de plateformes proposant des rançongiciels en tant que service à d'autres criminels, appelés « affiliés ». Les affiliés peuvent se servir des plateformes mises à disposition par ces groupes pour déployer des logiciels malveillants, publier des données exfiltrées et blanchir les bénéfices générés par leurs activités criminelles. En contrepartie de l'utilisation de la plateforme, les affiliés rémunèrent le groupe spécialisé dans les attaques par rançongiciel, soit sous forme d'abonnement mensuel, soit à hauteur d'un pourcentage des paiements de rançon perçus via la plateforme.

Au fur et à mesure qu'elles se professionnalisent, ces opérations de rançongiciels en tant que service permettent aux cybercriminels de rationaliser leurs processus et de développer leurs activités. Elles favorisent également l'émergence de nouvelles variantes, plus élaborées et plus agressives. Fortinet a recensé plus de 10 600 nouvelles variantes de rançongiciel au cours du premier semestre 2022, soit le double des variantes recensées au cours du semestre précédent[14]. Point essentiel, les programmes d'affiliation et autres opérations de rançongiciels en tant que service s'appuient sur le développement continu et la spécialisation de l'écosystème des services cybercriminels. Le noyau de membres des groupes spécialisés dans les attaques par rançongiciel recrute divers spécialistes pour gérer les programmes d'affiliation, tels que des développeurs, des testeurs de pénétration, des administrateurs système, des gestionnaires de données, des négociateurs, des recruteurs, des experts juridiques et des comptables[15]. Il recourt également à des prestataires de services externes, comme des courtiers d'accès initial, ainsi qu'à des services de blanchiment d'argent et d'hébergement complaisant. À titre d'exemple, Br0k3r, l'un des courtiers d'accès initial les plus actifs en Afrique et au Moyen-Orient, proposait plus de 60 solutions d'accès à des réseaux d'entreprise avec des droits d'administration de domaine sur sa propre boutique en ligne l'année dernière[16]. Étant donné que le noyau de membres, les affiliés et les prestataires de services peuvent appartenir à différents groupes, il convient de désorganiser l'écosystème des services cybercriminels dans son ensemble si l'on veut lutter efficacement contre la cybercriminalité.

COURTIER D'ACCÈS INITIAL	AFFILIÉ D'UN GROUPE SPÉCIALISÉ DANS LES ATTAQUES PAR RANÇONGICIEL	GESTIONNAIRE DE DONNÉES	OPÉRATEUR DU RANÇONGICIEL	NÉGOCIATEUR	OPPRESSEUR	COMPTABLE
Obtain initial access Obtention d'un accès initial aux organisations Monétisation des réseaux en les vendant à des cybercriminels	Persistance/ reconnaissance Navigation latérale Élargissement des droits Déploiement du rançongiciel	Mise à disposition d'une infrastructure et d'un logiciel d'exfiltration de données Exfiltration de données appartenant à l'organisation victime Publication des données exfiltrées (le cas échéant)	Mise à disposition d'un rançongiciel et de l'infrastructure associée	Négociation avec l'organisation victime	Pression sur l'organisation victime en la menaçant d'attaques répétées et de divulgation des données volées	Blanchiment des paiements de rançon
DANS	À TRAVERS		EN DEHORS			

Source: Northwave-Cybersecurity.com

Vue d'ensemble de l'écosystème des services cybercriminels à l'appui des attaques par rançongiciel

14 Fortinet (2023) : https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2023-ransomware-global-research.pdf

15 Europol (2023) : https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight%20Report%20-%20Cyber-attacks%20the%20apex%20of%20crime-as-a-service.pdf

16 Group-IB (2024) : https://www.group-ib.com/resources/research-hub/hi-tech-crime-trends-2023-mea/

OPÉRATION LANDSLIDE

Début 2023, INTERPOL a lancé une opération sous le nom de code « Landslide », qui cible les infrastructures favorisant les cyberinfractions, dont les attaques par rançongiciel. L'objectif précis de l'opération Landslide est d'éliminer un vecteur de criminalité depuis trop longtemps hors de portée des services chargés de l'application de la loi : l'hébergement complaisant (HC). En collaboration avec les autorités des Seychelles et son partenaire privé Trend Micro, INTERPOL a identifié plusieurs hébergeurs complaisants impliqués dans des activités illicites. En s'appuyant sur les résultats de précédentes opérations, INTERPOL est parvenu à nettoyer et démanteler l'infrastructure malveillante. L'opération est en cours.

Résilience face aux attaques par rançongiciel en Afrique : progrès notables et difficultés persistantes

Les pays membres africains d'INTERPOL prennent des mesures fortes pour lutter contre la menace persistante des attaques par rançongiciel. En effet, plus de 60 % d'entre eux ont instauré un mécanisme de signalement des cyberinfractions en vue de favoriser la détection, l'atténuation et l'enquête sur ces attaques. Les États collaborent également de plus en plus avec le secteur privé, près de deux tiers des pays membres africains interrogés ayant formé des partenariats avec des acteurs privés en vue de lutter contre les attaques par rançongiciel. Par ailleurs, les pays africains indiquent redoubler d'efforts pour sensibiliser les entreprises à la menace de cyberextorsion. À l'échelle régionale, une autre évolution positive est marquée par la création de cellules spéciales conjointes, auxquelles participent les services chargés de l'application de la loi du continent et dont la mission est d'améliorer la riposte aux attaques par rançongiciel et de sensibiliser à leur impact.

En dépit de ces progrès notables, les pays membres ont mis en évidence des difficultés persistantes. Le degré de signalement des attaques par rançongiciel par les victimes demeure problématique et entrave la capacité des services chargés de l'application de la loi à ouvrir des enquêtes. De plus, les pays membres ont déclaré que 16 % des victimes finissaient par payer la rançon en cas d'attaque par rançongiciel. Malheureusement, le fait de payer la rançon ne garantit en aucun cas l'arrêt de l'attaque ni le retrait du logiciel malveillant des systèmes. Dans certains cas, les victimes ne récupèrent finalement pas leurs données ou paient le double d'une restauration des systèmes[17]. Le fait de payer la rançon ne prémunit pas non plus contre la revictimisation. Pire encore, cela peut inciter les cybercriminels à poursuivre et développer leurs activités grâce à ces nouvelles ressources. Conscient de cette difficulté, INTERPOL, aux côtés de 50 pays membres de l'International Counter Ransomware Initiative, a publié une déclaration commune en novembre 2023 visant à dissuader fortement les organisations d'accéder aux demandes de rançon dans le cadre d'attaques par rançongiciel[18].

ESCROQUERIES EN LIGNE

Points clés :

- Les escroqueries en ligne et les modes opératoires associés évoluent en permanence ; les cybercriminels ciblent des victimes dans tous les groupes démographiques et les secteurs.
- Le hameçonnage par courriel et via les médias sociaux exploite l'élément humain et ouvre la voie à d'autres cyberinfractions.
- L'intelligence artificielle élargit les horizons des criminels se livrant à des arnaques de type « dépeçage de cochon » et à des escroqueries aux sentiments.
- Dans la lignée des tendances sociales, les smartphones sont de plus en plus ciblés par les escrocs, qui recourent à des chevaux de Troie bancaires.

17 Sophos (2023) : https://news.sophos.com/en-us/2023/05/10/the-state-of-ransomware-2023/

18 La déclaration est consultable sur le site Web officiel de l'International Counter Ransomware Initiative : https://counter-ransomware.org/briefingroom/8ed7d1de-1a74-4a36-a2df-d5950624ebd8

Escroqueries en ligne : une crise socio-économique majeure en Afrique

Outre les rançongiciels, l'une des principales cybermenaces identifiées par les pays membres africains en 2023 était les escroqueries en ligne, notamment en termes de volume et d'incidence financière globale. Une escroquerie en ligne est un acte ou une opération frauduleux(se) réalisé(e) par l'intermédiaire des technologies informatiques et d'Internet, dans le but de voler de l'argent et/ou des informations personnelles appartenant à des personnes ou organisations. Pour ce faire, les cybercriminels recourent généralement à une combinaison d'éléments techniques, tels que le hameçonnage et les logiciels malveillants, associée à des tactiques d'ingénierie sociale[19].

L'explosion des escroqueries en ligne est liée à la vague de transformation numérique qui déferle sur le continent africain[20]. Étant donné que les Africains passent plus de temps dans le cyberespace, par exemple, en communicant via les médias sociaux ou en utilisant les services bancaires mobiles, la surface d'attaque s'élargit pour les criminels cherchant à commettre des actes frauduleux à l'aide d'outils numériques. Il est difficile de quantifier les pertes découlant des escroqueries en ligne sur le continent africain, mais les pays membres d'INTERPOL indiquent que les particuliers qui en sont victimes appartiennent à toutes les tranches d'âge, tous les genres et tous les secteurs d'activité. Si des groupes sont particulièrement exposés à certaines formes de fraude en ligne, en définitive, tout citoyen peut en être victime. De même, les organisations ciblées par les escroqueries en ligne peuvent être des petites et moyennes entreprises (PME) comme de très grandes organisations, et appartiennent à tous les secteurs d'activité. En résumé, l'omniprésence des escroqueries en ligne en Afrique est à l'origine d'une crise socio-économique majeure, qui touche les pays de la région mais pas seulement.

Parmi la diversité d'escroqueries en ligne, les pays membres africains d'INTERPOL ont recensé cinq types de mécanismes frauduleux particulièrement utilisés en 2023. En respectant l'ordre dans lequel ils ont été cités, il s'agit **des escroqueries aux faux ordres de virement, des escroqueries par hameçonnage, des escroqueries aux sentiments, des arnaques de type « dépeçage de cochon » et des escroqueries par téléphone.** Ces différentes formes d'escroqueries en ligne sont analysées ci-dessous, à l'exception des escroqueries aux faux ordres de virement qui font l'objet d'une section distincte en raison de leur très forte présence en Afrique.

Le hameçonnage par courriel et via les médias sociaux ouvre la voie à d'autres cyberinfractions

Le hameçonnage a été identifié par les pays membres africains comme la principale menace en matière d'escroquerie en ligne, s'agissant à la fois du nombre de cas et des répercussions économiques et sociales à travers le continent. Les escroqueries par hameçonnage sont une forme de fraude en ligne consistant, pour les cybercriminels, à se faire passer pour des organisations ou entités légitimes par courriel, via des plateformes de messagerie ou sur de faux sites Web afin d'amener les victimes à renseigner des informations personnelles sensibles[21]. Ces informations comprennent généralement des identifiants de connexion, des informations financières (ex. numéros de carte bancaire), le numéro de sécurité sociale et d'autres données permettant d'obtenir un accès non autorisé à des comptes ou de procéder à une usurpation d'identité ou à un vol. Les tentatives de hameçonnage prennent souvent la forme de communications urgentes ou alarmantes en vue d'inciter le destinataire à agir immédiatement, par exemple, en cliquant sur un lien malveillant, en téléchargeant une pièce jointe infectée par un logiciel malveillant ou en renseignant directement des informations confidentielles. Si l'objectif premier du hameçonnage est d'exploiter la psychologie humaine pour accéder à des données ou actifs de valeur, **en réalité, les attaques par hameçonnage ouvrent bien souvent la voie à d'autres cyberinfractions, telles que les attaques par rançongiciel et diverses formes d'escroqueries en ligne.**

En Afrique, deux formes distinctes de hameçonnage ont été identifiées à partir des résultats de l'enquête et des données internes d'INTERPOL : le hameçonnage traditionnel et le hameçonnage social. Dans ce contexte, les pays membres africains ont cité le hameçonnage traditionnel comme étant la principale cybermenace dans la région. Majoritairement orchestrées par courriel, les campagnes de hameçonnage traditionnel prennent généralement la forme de courriels provenant d'adresses qui semblent légitimes, mais qui sont, en réalité, fausses. Le but est d'inciter les destinataires à se rendre sur des sites Web frauduleux ou à cliquer sur des liens malveillants, puis à renseigner des informations personnelles qui sont ensuite volées par les cybercriminels. Une forme très répandue de hameçonnage par courriel est l'escroquerie aux faux ordres de virement, qui est détaillée dans la section suivante.

19 Afin d'endiguer les escroqueries en ligne, la Direction de la Cybercriminalité d'INTERPOL collabore étroitement avec le Centre INTERPOL de lutte contre la criminalité financière et la corruption (IFCACC). Pour de plus amples informations sur l'IFCACC, rendez-vous sur https://www.interpol.int/fr/Infractions/Criminalite-financiere.

20 IJSSRR (2023) : https://www.ijssrr.com/journal/article/view/1360

21 CSCR (2023) : https://csrc.nist.gov/projects/human-centered-cybersecurity/research-areas/phishing

Bien que le hameçonnage traditionnel reste prédominant, les pays membres africains signalent le recours accru **aux médias sociaux et aux messageries instantanées pour commettre des attaques par hameçonnage.** Le mode opératoire est similaire à celui du hameçonnage traditionnel, mais les cybercriminels utilisent de faux comptes de médias sociaux et des publications trompeuses comme appâts en vue d'obtenir les données financières et les données à caractère personnel (DCP) de leurs victimes. D'après les données fournies par les pays membres d'INTERPOL, les plateformes les plus couramment détournées aux fins d'escroquerie par hameçonnage en Afrique sont Meta (anciennement Facebook), Messenger et WhatsApp. L'adaptation des techniques de hameçonnage aux médias sociaux et aux services de messagerie permet de cibler les principaux modes de communication dans la région et illustre la capacité des escrocs à exploiter les tendances technologiques et sociales à des fins malveillantes.

Ces deux formes de hameçonnage s'appuient sur l'ingénierie sociale. À cet égard, le fait que les pays membres d'INTERPOL indiquent que les cybercriminels recourent à des tactiques d'ingénierie sociale toujours plus élaborées dans le cadre des campagnes de hameçonnage modernes est préoccupant. À titre d'exemple, l'opération Echoes, dirigée par le Maroc avec l'appui d'INTERPOL et de ses partenaires privés, a révélé que le criminel connu sous le pseudonyme « Ex-Robotos » et qui a développé le kit de hameçonnage du même nom, ciblait méticuleusement ses victimes en effectuant des recherches sur Internet, et privilégiait les directeurs généraux et autres dirigeants. Dans d'autres cas, les escrocs utilisent des services légitimes et prennent le contrôle de domaines et de comptes de messagerie électronique en vue d'accroître le taux de réussite de leurs campagnes de hameçonnage. Enfin, les données issues des pays membres d'INTERPOL et des partenaires du projet Gateway suggèrent que l'intelligence artificielle est la toute dernière avancée technologique exploitée par les criminels, notamment pour minimiser les signaux d'alerte du hameçonnage traditionnel.

OPÉRATION ECHOES :

En mai 2023, les autorités marocaines, en étroite collaboration avec INTERPOL, Microsoft et Group-IB, sont parvenues à démanteler les activités de cybercriminels suspectés d'utiliser un kit de hameçonnage Microsoft 365 pour cibler des milliers de victimes. Ce kit leur avait permis de voler les données des victimes, qu'ils pouvaient ensuite monétiser ou vendre sur le réseau Internet clandestin. Cette action conjointe, baptisée « opération Echoes », s'est appuyée sur l'expérience de collaboration avec les autorités marocaines, notamment dans le cadre de l'opération Lyrebird, et illustre la détermination du pays en matière de lutte contre les cybermenaces.

L'épidémie des escroqueries aux sentiments alimentée par la cyberimposture et la sextorsion

Les données fournies par les pays membres africains d'INTERPOL ont également mis en évidence le volume, l'impact et la sophistication croissants des escroqueries aux sentiments sur et en provenance du continent africain en 2023. Les escroqueries aux sentiments peuvent prendre diverses formes, mais elles consistent toutes à feindre une relation romantique ou une amitié intime dans un but lucratif. En général, les escrocs prennent contact avec leurs victimes sous couvert d'une relation romantique, en utilisant une fausse identité en ligne. D'après les données fournies par les pays membres d'INTERPOL, les criminels du continent abordent le plus souvent leurs cibles via les médias sociaux, les services de messagerie et les applications de rencontre. Ils tentent ensuite de nouer une relation personnelle avec la victime, en exploitant sa vulnérabilité et ses faiblesses. Cette étape peut se dérouler très rapidement, ou durer plusieurs années. Une fois qu'ils sont parvenus à établir un semblant de relation de confiance, les cybercriminels manipulent et/ou volent leurs victimes.

En Afrique, les pays membres d'INTERPOL ont signalé deux tendances majeures en matière d'escroquerie aux sentiments : la **cyberimposture** et la **sextorsion**. Dans le cadre de l'escroquerie aux sentiments, la cyberimposture consiste, pour les escrocs, à créer un faux profil en ligne afin de tromper leurs victimes[22]. Pour ce faire, ils volent des informations et des photos appartenant à d'autres personnes pour se créer une fausse identité. La tromperie peut aller de l'utilisation d'une photo de profil volée pour paraître plus attirant à l'appropriation totale de l'identité d'une autre personne, y compris son nom, sa photo, son genre, sa date de naissance et sa localisation. **D'après les déclarations des pays membres africains d'INTERPOL, la cyberimposture vise généralement des cibles précises et se déroule sur une longue période.** Une fois leurs victimes choisies, les escrocs suivent un script soigneusement élaboré afin d'établir une relation de confiance, puis

22 La pratique de la cyberimposture existe depuis de nombreuses années, en particulier sur les sites et forums de rencontre en ligne. Les personnes s'adonnent à la cyberimposture pour diverses raisons : certaines sont empreintes d'un sentiment d'insécurité, quand d'autres sont mues par des intentions malveillantes (ex. cyberharcèlement ou escroquerie).

ils tentent de les manipuler sur le plan affectif pour qu'elles leur virent de l'argent. Par exemple, l'escroc peut prétendre que lui ou l'un de ses proches est malade, blessé ou emprisonné, ou il peut demander une aide financière pour organiser une rencontre en personne ou planifier un avenir commun[23]. Une fois les fonds transférés, l'escroc disparaît, laissant la victime non seulement démunie financièrement, mais également bouleversée sur le plan affectif et psychologique. Outre le recours à des tactiques d'ingénierie sociale toujours plus élaborées, **certains escrocs aux sentiments exploitent les avancées de l'intelligence artificielle (IA).** En plus de générer des photos par hypertrucage pour appâter leurs victimes, ils utilisent des agents conversationnels à intelligence artificielle comme « LoveGPT » pour créer de faux profils, obtenir une aide à la rédaction et escroquer leurs cibles sur des applications de rencontre[24].

La seconde tendance en matière d'escroquerie aux sentiments mise en évidence par les pays membres africains est l'essor de la sextorsion. La sextorsion présente des similitudes avec d'autres formes d'escroquerie aux sentiments. Les criminels prennent généralement contact avec leurs victimes (souvent jeunes) sous une fausse identité par l'intermédiaire d'applications de rencontre, de médias sociaux et d'autres plateformes en ligne. Une fois qu'ils ont gagné leur confiance, les escrocs convainquent leurs cibles de leur envoyer du contenu intime ou à caractère sexuel, puis les font chanter en menaçant de publier ce contenu en ligne ou de le diffuser à des parents et amis. Afin d'augmenter la pression exercée sur les victimes, les criminels peuvent commencer à publier ce contenu intime en ligne, puis demander un paiement en contrepartie du retrait du contenu. Bien que la sextorsion soit souvent associée à des messages, photos ou vidéos à caractère sexuel, il convient de noter que, selon les us et coutumes de la communauté concernée, la menace de publier des échanges romantiques peut suffire pour extorquer une victime.

Le mode opératoire de la sextorsion semble particulièrement dynamique. À titre d'exemple, certains pays membres ont signalé des cas de sextorsion dans lesquels des techniques de hameçonnage ont été utilisées pour accéder au contenu privé (non publié) des comptes Facebook et Instagram des victimes. Dans ce type de cas, le cybercriminel accède illégalement au profil des victimes sur les médias sociaux, puis recherche systématiquement du contenu intime en vue de l'extraire. La dimension criminelle de l'opération atteint son point d'orgue lorsque le cybercriminel extorque les victimes en les menaçant de publier leur contenu intime sur les plateformes de médias sociaux, ou de le diffuser de quelque manière que ce soit, si elles ne paient pas. Autre évolution récente, le recours à l'intelligence artificielle pour générer des images à caractère sexuel « aussi vraies que nature » en vue d'intimider et d'extorquer les victimes, y compris mineures[25]. Au vu des difficultés considérables auxquelles elles pourraient se heurter pour retirer ce contenu manipulé une fois publié en ligne, certaines victimes préfèrent payer les extorqueurs.

Les escroqueries aux sentiments se révèlent particulièrement rentables. Les déclarations des pays membres africains indiquent que les paiements effectués dans le cadre d'escroqueries aux sentiments, comprenant à la fois la cyberimposture et la sextorsion, ne sont pas simplement ponctuels. En réalité, la plupart des victimes se retrouvent à payer ce qui s'apparente à une redevance mensuelle, soit pour préserver leur semblant de relation romantique, soit pour éviter la diffusion de leur contenu personnel. D'après certaines estimations, les pertes mondiales liées à cette cybermenace s'élèveraient à plus de 1,3 milliard d'USD pour la période 2017 - 2022, une victime perdant en moyenne près de 4 400 USD par escroquerie[26]. Outre leur incidence financière, les escroqueries aux sentiments peuvent avoir des conséquences dévastatrices sur le plan affectif pour les victimes, certains cas les conduisant même au suicide. En raison du sentiment de honte, de culpabilité et/ou de déni qui envahit les victimes, ainsi que de la stigmatisation sociale, bon nombre de ces incidents ne sont pas signalés. À l'instar d'autres cyberinfractions, cela signifie que l'incidence réelle des escroqueries aux sentiments est probablement beaucoup plus forte que ce que les chiffres officiels ne le laissent à penser. Étant donné que le volume, l'ampleur et la complexité croissants des escroqueries aux sentiments va inévitablement compliquer les activités d'enquête des services africains chargés de l'application de la loi, la fourniture d'une formation et de capacités adéquates en matière de criminalistique est essentielle.

OPÉRATION CONTENDER : LA CONTRE-ATTAQUE FACE AUX ESCROQUERIES AUX SENTIMENTS

Dans le cadre de l'opération Contender, INTERPOL a collaboré avec les unités spécialisées dans la cybercriminalité du Bénin, de Côte d'Ivoire, du Nigéria, de Finlande et de Suisse, ainsi qu'avec plusieurs partenaires privés, en vue de démanteler les réseaux cybercriminels organisés impliqués dans les escroqueries aux sentiments. L'opération a donné lieu à l'arrestation de trois suspects en Côte d'Ivoire et au Bénin début 2023, ainsi qu'à la saisie d'appareils numériques et mobiles utilisés à des fins malveillantes.

23 FTC (États-Unis, 2023) : https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed

24 Avast (2023) : https://decoded.avast.io/threatintel/lovegpt-how-single-ladies-looking-for-your-data-upped-their-game-with-chatgpt/

25 Reuters (2023) : https://www.reuters.com/world/us/fbi-says-artificial-intelligence-being-used-sextortion-harassment-2023-06-07/

26 FTC (États-Unis, 2022) : https://www.ftc.gov/news-events/blogs/data-spotlight/2022/02/reports-romance-scams-hit-record-highs-2021

Les arnaques de type « dépeçage de cochon », une nouvelle menace hybride qui gagne rapidement du terrain

Comme dans d'autres régions du monde, en 2023, les pays membres africains d'INTERPOL ont identifié les arnaques de type « dépeçage de cochon » comme l'une des formes d'escroqueries en ligne à l'essor le plus rapide. Bien qu'il s'agisse d'un phénomène relativement nouveau, ce type d'incident a été signalé par plus d'un tiers des pays membres africains en 2023, en particulier en Afrique australe et de l'Ouest[27]. D'après des données internes, les arnaques de type « dépeçage de cochon » ont une incidence financière majeure à travers le continent, en droite ligne avec la situation observée à l'échelle mondiale. Des études révèlent que la somme médiane versée dans les portefeuilles de cybermonnaies des escrocs est comprise entre 10 000 et 100 000 USD, tandis que les pertes mondiales attribuées aux arnaques de type « dépeçage de cochon » et autres escroqueries aux cybermonnaies ont, selon les estimations, presque doublé depuis 2022, dépassant les 3,3 milliards d'USD en 2023[28].

Comme expliqué dans l'Évaluation de la fraude financière mondiale 2024 d'INTERPOL, les arnaques de type « dépeçage de cochon » constituent une forme d'escroquerie hybride, associant des aspects de l'escroquerie aux placements et de l'escroquerie aux sentiments. Ces arnaques se déroulent généralement en trois grandes étapes : tout d'abord, les criminels prennent contact avec des personnes via des plateformes numériques, telles que les médias sociaux (Facebook, Instagram), les services de messagerie (SMS, WhatsApp, Telegram, Signal) et les applications de rencontre. Ils prétendent avoir obtenu les coordonnées de la victime sur recommandation ou par un ami commun. Afin de mieux appâter leurs cibles, les criminels utilisent souvent de faux comptes et se font passer pour des personnes attirantes grâce à des photos volées ou générées par l'IA, selon un mode opératoire semblable à celui des escroqueries aux sentiments. L'étape suivante consiste à « engraisser » leurs victimes en gagnant leur confiance et en se présentant progressivement comme des experts en investissement. Les criminels incitent alors leurs victimes à investir dans des projets de cybermonnaie qui semblent licites et rentables. Néanmoins, dès que les victimes ont versé des sommes importantes ou commencent à comprendre qu'elles se font escroquer, les criminels empochent l'argent et disparaissent. En vue de rendre le traçage et le recouvrement des avoirs le plus difficile possible, les criminels tentent généralement de convertir les fonds de leurs victimes via des paiements numériques ou des plateformes de cybermonnaies. Au cours de cette ultime étape, connue sous le nom d'« abattage », les cybercriminels ne répondent plus aux messages et appels de leurs victimes, leur causant un préjudice financier et affectif.

Les phases du "Pig butchering" (Source: IGCR 2023)

27 Évaluation de la fraude financière mondiale 2024 d'INTERPOL : https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2024/INTERPOL-led-operation-targets-growing-cyber-threats

28 Trend Micro (2023) : https://www.trendmicro.com/vinfo/sg/security/news/cybercrime-and-digital-threats/unmasking-pig-butchering-scams-and-protecting-your-financial-future

Dans les cas d'arnaques de type « dépeçage de cochon » signalés par les pays membres africains, une distinction générale a été opérée s'agissant du moyen de contact initialement utilisé par les cybercriminels, à savoir les plateformes de médias sociaux (Facebook, Instagram) ou les services de messagerie mobile (WhatsApp, Telegram, Signal, SMS), y compris les conversations de groupe. Les personnes ciblées sur les plateformes de médias sociaux sont souvent victimes de techniques d'ingénierie sociale plus agressives par rapport à la démarche plus vaste et moins personnalisée observée via les services de messagerie. De plus, les pays membres ont mentionné la simplicité des arnaques de type « dépeçage de cochon » et la grande disponibilité des kits de hameçonnage comme les principaux facteurs expliquant l'augmentation constante de ces cas tout au long de l'année 2023.

Cette forte hausse a poussé les services chargés de l'application de la loi des pays membres africains à identifier les obstacles majeurs aux enquêtes, tels que la difficulté à obtenir des données auprès des fournisseurs de services et la quantité d'appareils nécessitant une analyse criminalistique. Sans compter que l'essor des arnaques de type « dépeçage de cochon », à l'instar d'autres cyberinfractions, complique les questions de compétence. Face à ces difficultés, les pays ont d'ores et déjà pris des mesures. Une cellule spéciale conjointe de lutte contre les arnaques de type « dépeçage de cochon » a été créée en Afrique australe, et elle a déjà fait ses preuves. Par ailleurs, INTERPOL dispense des sessions de formation et organise des réunions avec les fournisseurs de services du continent en vue de renforcer les activités régionales de lutte contre les arnaques de type « dépeçage de cochon ».

Les smartphones plus que jamais dans le viseur des escrocs en Afrique

Les pays membres africains ont recensé un nombre croissant d'escroqueries ciblant les utilisateurs de smartphones en 2023. Cette tendance reflète la hausse constante du taux de pénétration des technologies mobiles en Afrique, ainsi que l'augmentation rapide de l'utilisation des services bancaires mobiles à travers le continent[29]. Les escroqueries par smartphone les plus couramment détectées par les services africains chargés de l'application de la loi appartiennent à deux grandes catégories, souvent corrélées : l**es attaques par hameçonnage sur téléphone mobile et les chevaux de Troie bancaires.**

La première catégorie est dérivée des attaques par hameçonnage précédemment évoquées ; en effet, les criminels tentent de rediriger les victimes vers des sites frauduleux comme de faux sites bancaires via le navigateur de leur téléphone mobile. La seconde catégorie d'escroqueries par smartphone fréquemment observées par les services africains chargés de l'application de la loi comprend le recours à des chevaux de Troie bancaires. Il s'agit de programmes malveillants conçus pour voler des informations financières et sensibles, telles que des identifiants de banque en ligne, des numéros de compte et des données de carte bancaire, à partir de machines infectées. Les chevaux de Troie bancaires peuvent être déployés à l'aide de différents vecteurs d'attaque : courriels de hameçonnage, téléchargements furtifs, ou encore téléchargement d'un logiciel piraté comme une fausse application mobile. À l'instar des autres chevaux de Troie, ils se font généralement passer pour des logiciels légitimes afin d'accéder à la machine, ce qui rend leur détection difficile. De plus, ce sont des chevaux de Troie contenant un outil de prise de contrôle à distance, qui permettent aux cybercriminels de contrôler à distance le système infecté et de mener d'autres attaques, notamment par rançongiciel[30]. Une fois installé, le logiciel malveillant recueille et exfiltre des données sensibles via diverses méthodes : enregistrement de la frappe, prise de captures d'écran, dumping des identifiants mis en cache et recherche des mots de passe enregistrés dans le système. Les cybercriminels peuvent ensuite utiliser ces informations pour dérober de l'argent à leurs victimes, par exemple, en accédant à distance à leur application bancaire, ou pour commettre d'autres infractions, telles qu'une usurpation d'identité et d'autres formes d'escroqueries.

Les chevaux de Troie bancaires et les escroqueries en ligne associées représentent un défi majeur pour le continent africain au vu du nombre de cas signalés, en particulier en Afrique australe. Étant donné que les citoyens utilisent de plus en plus les smartphones et les services de paiement mobile, l'ensemble des pays membres africains se disent fortement préoccupés par les éventuelles répercussions économiques et sociales des escroqueries par smartphone. De plus, les chevaux de Troie bancaires augmentent la pression exercée sur les capacités et ressources de criminalistique numérique dans la région. En vue de relever ce défi, plusieurs pays investissent massivement dans des outils de criminalistique, ce qui leur a permis de procéder à l'analyse de centaines d'appareils au cours de la période étudiée. De nombreux pays africains prennent également des mesures fortes pour mieux prévenir, enquêter sur et éliminer les chevaux de Troie bancaires mobiles, notamment en formant des partenariats avec les banques afin de saisir et recouvrer les avoirs d'origine criminelle, et en menant des campagnes de sensibilisation aux risques liés à l'utilisation des services bancaires en ligne auprès des citoyens.

29 Cf. par exemple Statista (2023) : https://www.statista.com/statistics/1133777/sub-saharan-africa-smartphone-subscriptions/
30 Check Point (2023) : https://www.checkpoint.com/cyber-hub/cyber-security/what-is-trojan/what-is-a-banking-trojan/

ESCROQUERIES AUX FAUX ORDRES DE VIREMENT

Points clés :

- Les escroqueries aux faux ordres de virement, qui allient des éléments techniques et des tactiques d'ingénierie sociale élaborées, représentent une menace croissante pour les organisations et les personnes en Afrique, en particulier dans le secteur financier.
- L'essor de cette menace hybride est alimenté par les évolutions techniques, dont l'expansion de la cybercriminalité en tant que service et l'incidence nouvelle de l'intelligence artificielle.
- En dépit des accomplissements majeurs des services chargés de l'application de la loi, l'offensive permanente des auteurs d'escroqueries aux FOVI sur et en provenance du continent africain complique considérablement les activités d'enquête.

Escroqueries aux faux ordres de virement : une menace croissante en Afrique

Dans la grande catégorie des escroqueries en ligne, les pays membres africains d'INTERPOL ont identifié les escroqueries aux faux ordres de virement (FOVI) comme l'une des principales menaces. Les escroqueries aux FOVI sont des cyberinfractions ayant recours à des courriels frauduleux pour attaquer les organisations et les personnes. Elles consistent généralement, pour les cybercriminels, à pirater des comptes de messagerie électronique personnels ou professionnels légitimes via l'ingénierie sociale et/ou l'intrusion informatique, puis à tenter d'inciter les victimes à procéder à des transferts de fonds non autorisés ou à divulguer des informations confidentielles.

En Afrique, les activités cybercriminelles en lien avec les escroqueries aux faux ordres de virement se multiplient, en termes à la fois de volume et de répercussions des attaques. Cette évolution reflète les tendances mondiales : entre avril 2022 et avril 2023, Microsoft a détecté et enquêté sur 35 millions de tentatives d'escroquerie aux FOVI, soit environ 156 000 tentatives d'attaque par jour[31]. En parallèle, l'incidence financière mondiale des escroqueries aux FOVI a augmenté depuis 2013, et s'élève à plus de 50 milliards d'USD en 2023[32]. Outre les pertes financières directes, les escroqueries aux FOVI peuvent causer des préjudices à long terme, tels que la perte de données confidentielles en cas de divulgation d'échanges sensibles ou d'atteinte à la propriété intellectuelle, et avoir un impact psychologique sur les victimes.

En 2023, les entreprises ont été les principales cibles des escroqueries aux FOVI dans les pays membres africains d'INTERPOL. Les entreprises qui exercent des activités à l'étranger et réalisent donc des opérations financières régulières, ainsi que celles dont les contrôles de sécurité sont relativement faibles, semblent particulièrement exposées. En termes de taille, les petites et moyennes entreprises comme les grandes organisations peuvent être prises pour cible. **Le secteur de la finance a été le plus fréquemment touché dans les pays membres africains, mais aucun secteur n'est épargné par les escroqueries aux FOVI.** Outre les banques et les entreprises spécialisées dans la microfinance, des attaques contre des entreprises intervenant dans les secteurs de l'import-export, du pétrole et du gaz, des produits pharmaceutiques, du transport et du commerce électronique ont régulièrement été signalées. En parallèle, les attaques contre les organismes publics (en particulier parapublics), le secteur du bénévolat et les particuliers se sont multipliées sur le continent africain.

Mode opératoire privilégié pour les escroqueries aux FOVI dans les pays africains

S'agissant du mode opératoire, **les courriels de hameçonnage ont été identifiés comme le vecteur d'attaque le plus courant dans le cadre des escroqueries aux FOVI par près de 80 % des pays membres africains en 2023.** Par rapport à d'autres formes de hameçonnage, les courriels utilisés dans le cadre des escroqueries aux FOVI sont plus difficiles à détecter car ils ne contiennent pas de lien malveillant et ne sont pas envoyés en masse, c'est pourquoi ils sont moins susceptibles d'être signalés comme courriers indésirables. Les pays membres ont indiqué qu'en combinaison avec les courriels de hameçonnage, les cybercriminels exploitaient différents moyens de communication dans le cadre des escroqueries aux FOVI, tels que les messages texte, les appels téléphoniques et les réunions virtuelles. À

31 Microsoft (2023) : https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW15yVe
32 IC3 (États-Unis, 2023) : https://www.ic3.gov/Media/Y2023/PSA230609

titre d'exemple, certains cybercriminels rejoignent des réunions virtuelles par connexion commutée et volent des informations professionnelles confidentielles. Par ailleurs, les médias sociaux et les services de messagerie instantanée sont de plus en plus souvent détournés pour mener des activités de reconnaissance et/ou prendre contact avec des victimes[33].

La plupart des cas recensés par les pays membres d'INTERPOL peuvent être classés dans cinq catégories ou selon cinq procédés :

1. **Vol de données :** les cybercriminels piratent la messagerie électronique et les identifiants de salariés travaillant dans des domaines précis, tels que les ressources humaines et la comptabilité, afin d'obtenir les données à caractère personnel ou les déclarations fiscales d'autres salariés ou dirigeants. Les données ainsi obtenues sont utilisées dans le cadre d'autres escroqueries aux FOVI. Ce procédé est en plein essor, les criminels utilisant les données exfiltrées dans le cadre d'une double, voire d'une triple, extorsion à l'encontre des victimes.

2. **Piratage de compte / atteinte à la sécurité :** un autre procédé régulièrement signalé par les pays membres consiste, pour les cybercriminels, à pirater la messagerie électronique d'un salarié ou d'un dirigeant et de l'utiliser pour envoyer des demandes de règlement de factures à divers fournisseurs. En effet, plusieurs pays africains ont recensé des attaques dites « de l'homme au milieu », dans le cadre desquelles les cybercriminels interceptent et transmettent secrètement des messages entre deux parties.

3. **Usurpation d'identité du directeur général :** également appelé « escroquerie au chef d'entreprise », ce procédé consiste, pour les criminels, à se faire passer pour de hauts dirigeants en vue d'effectuer un paiement vers un compte dont ils ont le contrôle. Cette forme d'escroquerie aux FOVI nécessite d'effectuer des recherches et des activités de reconnaissance vis-à-vis de l'organisation ciblée.

4. **Usurpation d'identité d'un fonctionnaire, d'un agent chargé de l'application de la loi ou d'un avocat :** cette forme d'escroquerie aux FOVI consiste, pour les cybercriminels, à prendre contact avec leurs cibles en se faisant passer pour une figure d'autorité, telle qu'un fonctionnaire ou un avocat, qui gère des dossiers confidentiels et urgents. En 2023, plusieurs pays ont également signalé des cas d'usurpation d'identité d'agents chargés de l'application de la loi ou de membres d'organisations internationales, dont INTERPOL. Les criminels recourent ensuite à diverses méthodes pour inciter leurs victimes à transférer des fonds rapidement ou secrètement.

5. **Fausses factures :** les criminels tentent d'exploiter les relations durables entre leur cible et ses fournisseurs. Ils se font ainsi passer pour un fournisseur et envoient une facture falsifiée en demandant à leur victime de transférer des fonds vers un compte frauduleux.

OPÉRATION HARRIER : ARRESTATION DES MEMBRES DE GROUPES CRIMINELS ORGANISÉS IMPLIQUÉS DANS DES ESCROQUERIES AUX FOVI

Face aux risques considérables et persistants représentés par les escroqueries aux FOVI, et notamment les répercussions financières, affectives et psychologiques évoquées dans la présente évaluation des menaces, INTERPOL a formé un partenariat stratégique avec le groupe Atlas du Forum économique mondial (FEM). Cette collaboration avait un double objectif : approfondir la compréhension du contexte mondial des cybermenaces et favoriser l'échange de renseignements en vue d'atténuer l'impact mondial de la cybercriminalité.

INTERPOL, de concert avec des participants à l'initiative Cybercrime Atlas du Forum économique mondial (FEM), est parvenu à identifier l'auteur d'une escroquerie aux FOVI de plusieurs millions de dollars suivant le mode opératoire des fausses factures. Grâce à un vaste échange de renseignements, l'individu en question a été relié à un réseau criminel complexe associé au groupe criminel organisé Black Axe, opérant en Afrique de l'Ouest. Ces informations ont été transmises aux pays membres africains concernés, ce qui a permis de procéder à l'arrestation de l'individu.

Si les vecteurs d'attaque initiaux et les procédés généraux des escroqueries aux faux ordres de virement sont bien établis, l'évolution des techniques d'ingénierie sociale, la disponibilité croissante de logiciels criminels en tant que service et l'incidence nouvelle de l'intelligence artificielle alimentent l'essor des escroqueries aux FOVI.

33 Centre d'études stratégiques de l'Afrique (2023) : https://africacenter.org/fr/spotlight/lafrique-a-lepreuve-des-nouvelles-formes-de-cybercriminalite/

Évolution des techniques d'ingénierie sociale

Comme bon nombre d'escroqueries en ligne, les escroqueries aux FOVI tirent grandement parti des failles humaines. En gardant cela à l'esprit, le fait que la plupart des pays membres africains aient signalé une sophistication des techniques d'ingénierie sociale est alarmant. En effet, les auteurs d'escroqueries aux FOVI passent beaucoup de temps à surveiller et se renseigner sur leurs cibles potentielles afin de renforcer leur appât ou vecteur d'attaque initial. Ils exploitent les informations accessibles au public ou issues de précédentes fuites de données pour élaborer les messages les plus personnalisés et authentiques possible. Dans certains cas, les criminels vont jusqu'à reproduire le style d'écriture de leur cible ou mentionner des événements à venir auxquels les victimes sont invitées. **Comme témoignage de cette sophistication accrue, plus de la moitié des pays membres africains d'INTERPOL ont observé un taux de réussite élevé, voire très élevé, des courriels de hameçonnage utilisés dans le cadre d'escroqueries aux FOVI.**

De nombreux auteurs d'escroqueries aux FOVI semblent passer plus de temps à naviguer latéralement dans le système de leur cible une fois qu'ils y ont accès. Ils peuvent recourir à diverses méthodes de persistance, telles que l'ajout d'une application d'authentification secondaire sur le compte piraté pour contourner l'authentification multifacteur[34]. Les cybercriminels fouillent ensuite les échanges par courriel ou les applications de partage de fichiers en ligne de leurs victimes, puis se servent de ces informations pour élaborer des procédés plus convaincants. À titre d'exemple, via l'analyse d'une chaîne de courriels, des cybercriminels sont parvenus à utiliser de faux noms de domaine pour créer plusieurs adresses électroniques frauduleuses. Ces adresses permettent de créer plusieurs profils et de se faire passer pour une entreprise, en faisant croire aux victimes qu'elles communiquent avec les différents destinataires de la chaîne d'origine.

Dans le même esprit, INTERPOL a observé une tendance croissante à l'exfiltration de données dans le cadre des escroqueries aux FOVI. Une fois qu'ils ont accès au système, les cybercriminels exfiltrent des données non seulement pour élaborer des attaques plus efficaces, mais également pour extorquer ultérieurement leurs victimes. Ils menacent de divulguer des informations sensibles (double extorsion) ou des données de partenaires tiers (triple extorsion). Le recours croissant à l'exfiltration de données témoigne, là encore, de la sophistication accrue des escroqueries aux FOVI.

Principaux signaux d'alerte des escroqueries aux FOVI :

La cybercriminalité en tant que service s'inscrit en hausse

L'essor rapide de la cybercriminalité en tant que service (CaaS) illustre à nouveau la sophistication, l'organisation et la spécialisation accrues des escroqueries aux FOVI. En effet, la Microsoft Digital Crimes Unit a observé une hausse de 38 % des activités de CaaS ciblant les comptes de messagerie électronique professionnels entre 2019 et 2022[35]. Une multitude de kits de hameçonnage sont désormais disponibles, comprenant des modèles et scripts prêts à l'emploi qui permettent aux auteurs d'escroqueries aux FOVI de développer rapidement et facilement leurs activités. À titre d'exemple, en 2023, le partenaire du projet Gateway d'INTERPOL Group-IB a signalé les activités de W3LL, un criminel qui fournit des kits de hameçonnage sur-mesure à au moins 500 auteurs d'escroqueries aux FOVI[36]. Générant un chiffre d'affaires estimé à 500 000 USD,

34 Cf. par exemple : https://www.kroll.com/en/insights/publications/cyber/mfa-bypass-leads-to-account-compromise
35 Microsoft (2023) : https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW15yVe
36 Group-IB (2023) : https://www.group-ib.com/media-center/press-releases/w3ll-phishing-report/

les logiciels criminels en tant que service fournis par W3LL sont des outils hautement personnalisés qui permettent de commettre des escroqueries aux FOVI, notamment en contournant l'authentification multifacteur. Entre octobre 2022 et juillet 2023, les kits de hameçonnage fournis par W3LL auraient été utilisés pour cibler plus de 56 000 comptes professionnels Microsoft 365.

Par ailleurs, les chercheurs en cybersécurité ont identifié un nombre croissant de plateformes illicites proposant des services de bout en bout, dont des modèles, des services d'hébergement et d'autres services automatisés, en vue de mener des campagnes d'escroquerie aux FOVI à grande échelle. L'une de ces plateformes est BulletProftLink, qui permet aux criminels non seulement d'obtenir les identifiants et l'adresse de protocole Internet (IP) des victimes, mais également d'utiliser des **adresses IP résidentielles** afin que les campagnes semblent être générées localement. Ils peuvent ainsi contourner efficacement les alertes de type « Impossible Travel », une méthode de détection couramment utilisée pour identifier et bloquer les activités suspectes[37].

L'incidence nouvelle de l'intelligence artificielle

La sophistication accrue des tactiques d'ingénierie sociale et l'essor de la cybercriminalité en tant que service sont d'autant plus préoccupants que l'intelligence artificielle (IA) et les médias synthétiques se développent rapidement. L'année 2023 a été marquée par des avancées majeures dans le domaine de l'IA, les grands modèles de langage (LLM) comme ChatGPT attirant l'attention du monde entier. Malheureusement, s'il existe de nombreux cas d'utilisation positifs, l'IA peut être détournée par les criminels, notamment ceux impliqués dans les escroqueries aux faux ordres de virement. Conscient de cette nouvelle menace, INTERPOL a publié une notice mauve afin d'alerter les pays membres sur le risque d'utilisation de l'IA et de l'hypertrucage par les criminels pour donner de la crédibilité aux escroqueries, par exemple, en dissimulant leur identité et en se faisant passer pour des membres de la famille ou des amis des victimes, ou encore des personnes souhaitant nouer une relation sentimentale avec elles[38].

À un niveau élémentaire, l'IA générative peut permettre aux auteurs d'escroqueries aux FOVI de créer facilement des courriels frauduleux ou de faux messages de demande d'authentification (parfois à une échelle industrielle), tout en déjouant les paramètres de détection de base, tels que les fautes d'orthographe et de grammaire. Lorsqu'ils sont alimentés avec les bonnes données, les LLM permettent même d'imiter le style et le vocabulaire d'une organisation ou d'une personne, et aident ainsi les cybercriminels à rédiger des courriels plus personnalisés et plus convaincants pour tromper les victimes[39]. Par ailleurs, les cybercriminels tirent d'ores et déjà parti de l'évolution rapide de l'hypertrucage pour piéger leurs cibles, par exemple, en reproduisant les traits et la voix d'une personne lors d'appels téléphoniques ou vidéo[40]. Étant donné la vitesse à laquelle l'IA se développe et la possibilité considérable qu'elle offre de multiplier les escroqueries aux FOVI ainsi que d'accroître leur degré de sophistication et d'authenticité, les pays membres devront suivre attentivement ces évolutions.

Neutraliser les auteurs d'escroqueries aux FOVI sévissant depuis l'Afrique

En 2023, les pays membres africains d'INTERPOL ont poursuivi les opérations musclées visant à neutraliser les auteurs d'escroqueries aux FOVI opérant depuis la région. Dans le cadre de l'opération Nervone, INTERPOL, AFRIPOL, Group-IB et la Direction de l'Information et des Traces Technologiques (DITT) de la Côte d'Ivoire ont procédé à l'arrestation du chef du groupe connu sous le nom d'OPERA1ER. Également connue sous les pseudonymes NXM, DESKTOP Group et Common Raven, cette organisation criminelle extrêmement organisée aurait mené des campagnes d'escroquerie aux faux ordres de virement à grande échelle lui ayant permis de dérober jusqu'à 35 millions d'USD dans 15 pays d'Afrique, d'Asie et d'Amérique latine[41]. En parallèle, dans le cadre de l'opération Jackal, INTERPOL a coordonné et assisté des services de police, des unités spécialisées dans la criminalité financière et des services spécialisés dans la cybercriminalité lors d'un coup de filet mené contre des groupes criminels organisés d'Afrique de l'Ouest, dont Black Axe, une organisation mafieuse violente connue pour se livrer à des escroqueries aux FOVI et d'autres escroqueries en ligne[42]. Les opérations comme celles-ci illustrent la détermination des pays membres africains à protéger leur population de l'incidence des escroqueries aux FOVI.

37 Microsoft (2023) : https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW15yVe

38 INTERPOL (2023) : https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2023/300-millions-d-USD-saisis-et-3-500-suspects-arretes-dans-le-cadre-d-une-operation-internationale-contre-la-criminalite-financiere

39 CSA (Singapour, 2023) : https://www.csa.gov.sg/Tips-Resource/publications/cybersense/2023/chatgpt---learning-enough-to-be-dangerous

40 INTERPOL (2023) : https://www.interpol.int/content/download/20035/file/ChatGPT-Impacts%20on%20Law%20Enorcement-%20August%202023.pdf

41 INTERPOL (2023) : https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2023/Arrestation-lors-d-une-operation-conjointe-d-un-individu-suspecte-d-etre-un-membre-majeur-d-une-organisation-connue-pour-ses-activites-de-cybercrim

42 INTERPOL (2023) : https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2023/Mobilisation-contre-la-criminalite-organisee-en-Afrique-de-l-Ouest-plus-de-2-millions-d-EUR-saisis-dans-le-cadre-de-l-operation-Jackal

OPÉRATION NERVONE : ARRESTATION D'UN MEMBRE MAJEUR D'UN GROUPE CYBERCRIMINEL ORGANISÉ

Au cours des quatre dernières années, le groupe cybercriminel connu sous le nom d'OPERA1ER a orchestré des campagnes de hameçonnage et d'escroquerie aux FOVI ainsi que des attaques par logiciel malveillant à grande échelle contre des services financiers et bancaires mobiles du monde entier, empochant jusqu'à 35 millions d'USD. Début juin 2023, INTERPOL, aux côtés d'AFRIPOL, de la Côte d'Ivoire, des États-Unis et de partenaires privés dont Orange, Group-IB, Booz Allen Hamilton et DarkLabs, a identifié et arrêté des individus suspectés d'être des membres majeurs du groupe. La réussite de cette opération, baptisée « Nervone », tient exclusivement à un échange constant de renseignements et à une étroite coopération sur plusieurs années.

Outre ces opérations réussies, les pays membres africains ont redoublé d'efforts en matière de prévention et d'atténuation. **Plus de 60 % des pays membres interrogés ont mené, en 2023, des campagnes de sensibilisation des personnes et organisations au risque représenté par les escroqueries aux FOVI.** Ces campagnes de sensibilisation ont été diffusées via différentes plateformes médiatiques (radio, télévision, sites Web institutionnels et réseaux sociaux) dans le but d'améliorer l'hygiène informatique et de prévenir l'exploitation de l'élément humain par les cybercriminels.

En dépit de ces mesures, des obstacles majeurs entravent toujours l'atténuation de l'impact des escroqueries aux FOVI en Afrique. **Un nombre important d'auteurs d'escroqueries aux FOVI se situent en Afrique, en particulier en Afrique de l'Ouest, mais également de plus en plus au sud du continent** ; certaines études indiquent que 11 pays recensent la majorité des escroqueries aux FOVI commises sur le continent[43]. Certains des groupes criminels impliqués sont désormais des organisations multimillionnaires[44]. Ils s'appuient généralement sur des structures organisationnelles complexes, comprenant des fonctions spécialisées telles qu'administrateur d'infrastructure, opérateur de messagerie électronique et mule financière. De plus, notamment en réaction aux réussites enregistrées par les services chargés de l'application de la loi, les escrocs recourent de plus en plus à des méthodes d'obfuscation pour dissimuler leur infrastructure criminelle et ont tendance à se disperser géographiquement, ce qui complique les activités d'enquête des services chargés de l'application de la loi.

CYBER-RÉSILIENCE ET CAPACITÉS DES SERVICES CHARGÉS DE L'APPLICATION DE LA LOI SUR LE CONTINENT AFRICAIN

Afin d'obtenir une vision globale du contexte actuel des cybermenaces, il convient non seulement d'identifier les cybermenaces imminentes, mais également d'évaluer les capacités actuelles de lutte contre ces menaces. De fait, la présente section étudie quatre axes de la cyber-résilience africaine, d'après les données fournies par les pays membres : **les cadres législatifs, les capacités des services chargés de l'application de la loi, les partenariats et la participation du grand public.**

1. Les cadres législatifs africains contre l'essor de la cybercriminalité

L'efficacité des cadres législatifs est une composante fondamentale de la cyber-résilience et un paramètre crucial pour les activités de police. À cet égard, l'adoption de lois visant à lutter contre la cybercriminalité en Afrique est encourageante. En 2023, plusieurs pays africains ont adopté des lois, amendé certains textes ou mis en application des lois récemment adoptées en vue de lutter contre la cybercriminalité[45]. Nous pouvons notamment citer la loi relative à l'interception des communications en Ouganda, la loi portant charte de protection des enfants en ligne au Cameroun, la loi relative à la protection des données à caractère personnel au Gabon, les dispositions à l'attention des opérateurs de TIC en matière de préservation des données au Burkina Faso, ou encore la loi relative aux actifs virtuels au Botswana. Six autres pays ont indiqué que des lois étaient en cours de promulgation. Ces mesures importantes s'ajoutent à l'expansion des instruments régionaux et internationaux actuels, **dont la Convention de l'Union africaine (UA) sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo),** la Stratégie de transformation numérique pour l'Afrique (2020-2030) de l'UA, ainsi que la Convention de Budapest sur la cybercriminalité et ses Protocoles additionnels.

43 Agari (2023) : ag-acid-geography-of-bec-gd.pdf (fortra.com)
44 Agari (2023) : https://www.agari.com/resources/videos/scattered-canary-evolution-business-email-compromise-enterprise
45 Lexology (2023) : https://www.lexology.com/library/detail.aspx?g=baef72ee-10bd-4eb9-a614-a990c236bb45

INTERPOL soutient activement ses pays membres dans la transformation de la législation en vue de lutter contre la cybercriminalité via diverses initiatives. En 2023, INTERPOL a participé à la mise en œuvre du projet « Action globale sur la cybercriminalité élargie » (GLACY+, actuellement élargi sous le nom de GLACY-e). Cette initiative, fruit de la collaboration entre l'Union européenne et le Conseil de l'Europe, vise à renforcer les cybercapacités des pays d'Afrique, d'Asie-Pacifique, d'Amérique latine et des Caraïbes dans le cadre de la Convention de Budapest. L'ambition première du projet GLACY+ est la consolidation d'une législation, de politiques et de stratégies harmonisées en matière de cybercriminalité. INTERPOL joue un rôle essentiel dans cette initiative, puisqu'il contribue au renforcement des capacités et des compétences opérationnelles des services de police dans les pays participants. L'objectif est d'améliorer la maîtrise des enquêtes sur les cyberinfractions et de favoriser la coopération policière internationale via une série d'activités.

En parallèle, tout au long de l'année 2023, INTERPOL a activement échangé avec des processus politiques et législatifs majeurs en matière de cybercriminalité à l'échelle internationale, en particulier le Comité spécial chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles[46]. Ce Comité a pour but de rédiger un nouveau traité mondial sur la lutte contre les cybermenaces qui, une fois ratifié, mettra à disposition des pays d'Afrique et d'ailleurs des instruments législatifs renforcés. Dans le cadre de sa participation, INTERPOL veille à ce que les intérêts et besoins de ses 196 pays membres soient pleinement pris en compte dans la future convention.

Enfin, depuis le lancement du Programme INTERPOL sur la cybercriminalité, l'Organisation développe des instruments cruciaux à l'appui de la lutte contre la cybercriminalité dans les pays membres, à savoir des résolutions mondiales (dernièrement, la résolution de 2021 intitulée « Lutter contre les menaces mondiales liées à la cybercriminalité par le canal d'INTERPOL »[47]), la Stratégie mondiale INTERPOL de lutte contre la cybercriminalité 2022 - 2025 et, plus précisément pour l'Afrique, la recommandation régionale 2022[48], qui appelle les pays membres africains à exploiter pleinement les ressources d'INTERPOL pour accroître la collaboration opérationnelle, échanger des renseignements et renforcer leurs capacités.

2. Le renforcement des cybercapacités des services chargés de l'application de la loi

Les données reçues par INTERPOL indiquent que les ressources humaines affectées à la lutte contre la cybercriminalité demeurent insuffisantes, bien que les pays prennent des mesures proactives pour y remédier. À titre d'exemple, en 2023, près de la moitié des services chargés de l'application de la loi des pays membres d'INTERPOL ont déclaré une augmentation du nombre d'agents affectés à la lutte contre la cybercriminalité. De plus, au moins quatre pays ont précisé qu'ils avaient récemment créé une unité spécialisée dans la cybercriminalité ou que la création d'une telle unité était en cours. En parallèle, au cours de l'année 2023, plus de 70 % des services chargés de l'application de la loi des pays membres africains ont déclaré avoir organisé ou participé à des formations sur la cybercriminalité, représentant 32 pays et plus de 130 formations. Cela témoigne des efforts consentis pour investir dans le personnel et les compétences afin de lutter plus efficacement contre les cybermenaces, ainsi que de la volonté des pays membres africains d'accroître la cyber-résilience à travers le continent.

Conformément à l'Objectif 3 de la Stratégie mondiale INTERPOL de lutte contre la cybercriminalité 2022 - 2025, l'Organisation vise à accompagner ses pays membres dans l'élaboration de stratégies et le renforcement des capacités en la matière. Pour ce faire, INTERPOL participe à plusieurs initiatives de renforcement des capacités sur le continent africain, dont l'AFJOC, le projet GLACY-e et le Programme ISPA. En 2023, ces initiatives ont permis d'organiser huit sessions de formation et ateliers consacrés aux techniques d'enquête en matière de cybercriminalité, et plus particulièrement aux actifs virtuels. Par ailleurs, 72 outils et licences spécialisés jouant un rôle crucial dans ce type d'enquête ont été achetés et répartis entre 22 pays membres, dont l'utilisation a fait l'objet d'une formation sur-mesure. INTERPOL met également à disposition deux plateformes spécialisées garantissant une connexion fluide entre les services chargés de l'application de la loi des pays membres : il s'agit de la plateforme « Échange de connaissances sur la cybercriminalité » (ECC) pour l'échange d'informations non opérationnelles, et de la Plateforme collaborative sur la cybercriminalité – Opérations (PCC – Opérations) pour l'échange sécurisé et restreint de renseignements opérationnels. Ce sont deux outils efficaces de coordination de la lutte internationale contre la cybercriminalité, qui proposent un mécanisme élaboré de participation collaborative.

46 Pour obtenir plus d'informations sur le Comité spécial : https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

47 INTERPOL (2021) : https://www.interpol.int/fr/News-and-Events/Events/2021/89th-INTERPOL-General-Assembly

48 INTERPOL (2022) : https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2022/La-Conference-regionale-africaine-d-INTERPOL-se-conclut-par-un-appel-a-une-intensification-de-l-echange-de-donnees

3. Les défis de coordination dans l'écosystème de la cybersécurité

La formation et la consolidation de partenariats ouverts, inclusifs et pluriels sont essentielles à une coopération efficace en matière de lutte contre la cybercriminalité. Cependant, les pays membres africains ont déclaré éprouver des difficultés à instaurer une collaboration entre les services chargés de l'application de la loi et les acteurs de la cybersécurité. La collaboration difficile avec les fournisseurs de services, en particulier ceux situés à l'étranger, semble toujours être un obstacle majeur aux enquêtes sur la cybercriminalité. Par ailleurs, il a été indiqué que la coopération public-privé intervenait souvent de manière ponctuelle, et non dans un cadre structuré et normalisé.

Au vu des difficultés à former des partenariats public-privé officiels et à créer des plateformes aidant les entreprises à lutter contre la cybercriminalité, les initiatives stratégiques menées par INTERPOL peuvent jouer un rôle déterminant. Le projet **Gateway** d'INTERPOL constitue la pierre angulaire de l'analyse approfondie dans le domaine de la cybercriminalité, en s'appuyant sur de nombreuses sources d'information pour localiser les cybercriminels, identifier les victimes et signaler les infrastructures corrompues en vue des interventions nécessaires. Fondé sur le Statut d'INTERPOL et ses principes directeurs (souveraineté, respect des droits de l'homme, neutralité et coopération active), le projet Gateway définit le cadre juridique de l'échange d'informations avec des entités privées via la conclusion d'accords de partage de données. INTERPOL participe également à des initiatives majeures favorisant la coopération entre divers acteurs. C'est notamment le cas de l'initiative **Cybercrime Atlas du Forum économique mondial**[49], qui rassemble les services chargés de l'application de la loi et les secteurs public et privé en vue d'étudier l'écosystème cybercriminel sous un nouvel angle. La coopération entre INTERPOL et la communauté Cybercrime Atlas donne lieu à d'impressionnants résultats opérationnels issus d'analyses, tels que le profilage et l'arrestation de membres d'un groupe cybercriminel connu sous le nom de « SilverTerrier », sévissant principalement à partir de l'Afrique de l'Ouest.

4. La sensibilisation du grand public et une meilleure hygiène informatique

Face à la multiplication des techniques d'ingénierie sociale utilisées pour commettre des cyberinfractions, les pays ont pris des mesures importantes visant à sensibiliser davantage le grand public et à améliorer l'hygiène informatique. Il est encourageant de voir qu'environ 80 % des pays membres africains interrogés mènent des campagnes de sensibilisation afin de prévenir les cyberinfractions. Si elles sont principalement visibles en ligne, ces campagnes s'affichent occasionnellement dans des lieux physiques, en particulier dans les établissements d'enseignement, où elles s'adressent en priorité aux jeunes et à leur réseau de soutien (parents, famille et enseignants). Ces campagnes sont déployées sur diverses plateformes médiatiques, dont la télévision, la radio, les actualités en ligne et les médias sociaux, Facebook en tête. L'une des caractéristiques notables de ces initiatives est la collaboration entre les services chargés de l'application de la loi et des entités des secteurs public et privé. Les axes prioritaires de ces campagnes sont la promotion de bonnes pratiques en matière d'hygiène informatique et la sensibilisation générale aux escroqueries en ligne. Ces initiatives nationales s'inscrivent dans la droite ligne de la Stratégie d'éducation numérique de l'Union africaine[50], qui vise essentiellement à accélérer l'adoption des technologies numériques dans les domaines de l'enseignement, de l'apprentissage, de la recherche, de l'évaluation et de l'administration.

Dans le cadre d'une initiative mondiale complémentaire, INTERPOL a lancé plusieurs campagnes de sensibilisation (#ÇaNArrivePasQuAuxAutres, #UnSeulClic, #OnlineCrimeIsRealCrime) en vue d'accroître la vigilance du grand public pour lutter contre la multitude de cybercriminels déterminés à exploiter les failles, à voler des données, à commettre des escroqueries en ligne ou à perturber le monde virtuel. La campagne #ÇaNArrivePasQuAuxAutres a rencontré un franc succès à l'échelle mondiale : elle a été soutenue par 79 pays membres ainsi que des partenaires privés, des organisations internationales, des entités privées et des organisations non gouvernementales, ce qui lui a permis de toucher un large public. En 2024, INTERPOL prévoit de poursuivre sur cette lancée avec une nouvelle campagne axée sur la menace représentée par les logiciels malveillants.

49 Pour obtenir plus d'informations sur l'initiative Cybercrime Atlas du FEM : https://initiatives.weforum.org/cybercrime-atlas/home

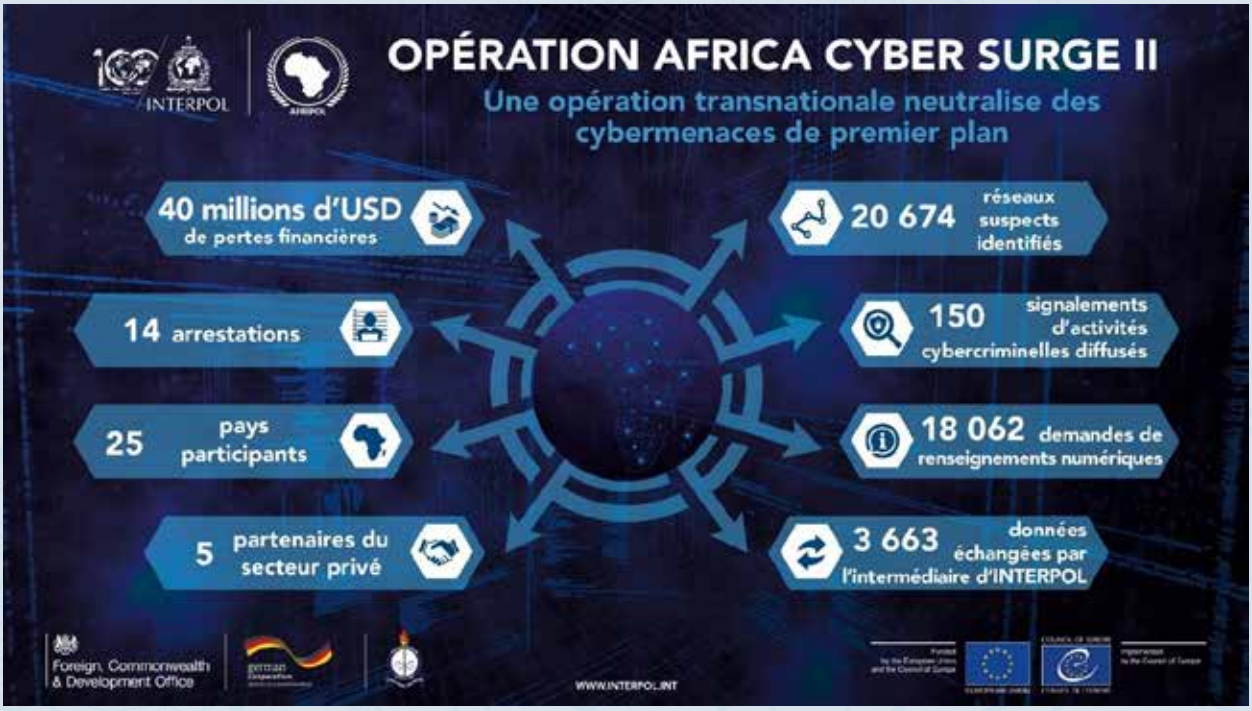
50 Stratégie d'éducation numérique de l'Union africaine (2022) : https://au.int/en/documents/20221125/digital-education-strategyand-implementation-plan

APPUI À LA CYBER-RÉSILIENCE AFRICAINE : OPÉRATION CYBER SURGE AFRIQUE II D'INTERPOL

INTERPOL œuvre en faveur de la cyber-résilience africaine via des partenariats, des plateformes et des activités de renforcement des capacités.

Un exemple parfait en est l'opération Cyber Surge Afrique II :

- Les partenaires du projet Gateway d'INTERPOL et de l'initiative Cybercrime Atlas du Forum économique mondial ont fourni des informations essentielles qui ont été déterminantes pour la réussite de l'opération
- Les pays participants ont utilisé la PCC – Opérations aux fins d'échange d'informations et de coordination opérationnelle
- Plusieurs formations préparatoires visant à perfectionner les compétences des enquêteurs ont été dispensées dans divers domaines en lien avec les enquêtes sur la cybercriminalité



MARCHE À SUIVRE

D'après les résultats de l'évaluation, notamment de l'analyse des cybermenaces connaissant l'expansion la plus rapide en Afrique et des contre-mesures prises, la présente section émet des recommandations dont l'objectif est de limiter l'impact et les préjudices causés par la cybercriminalité sur le continent et dans le monde.

1. Introduire des instruments de cybersécurité robustes et harmonisés, ou renforcer les instruments existants

INTERPOL recommande aux pays membres africains de continuer à créer des instruments nationaux de cybersécurité robustes et harmonisés, et/ou de renforcer les instruments existants, afin de se prémunir et de lutter contre la cybercriminalité. Ces instruments sont notamment les stratégies, politiques et cadres juridiques donnant les moyens aux pays de lutter efficacement contre les cybermenaces et d'atténuer les risques y afférents, par exemple, en éliminant les obstacles juridiques pour les enquêteurs.

2. Investir dans les cybercapacités des services chargés de l'application de la loi : personnes, processus et technologies

Conscient de l'importance de développer les ressources de cybersécurité sur le continent, **INTERPOL appelle les parties prenantes internes et externes à investir davantage dans les services africains chargés de l'application de la loi et à leur fournir un appui à long terme.** La sophistication accrue des cyberinfractions nécessite des unités, agents qualifiés, outils et plateformes plus spécialisés. De fait, les pays sont encouragés à participer activement aux activités de renforcement des capacités proposées par des entités régionales et internationales, telles que celles organisées par le Bureau pour les opérations de lutte contre la cybercriminalité en Afrique (AFJOC) d'INTERPOL.

3. Créer des synergies au sein de l'écosystème de la cybersécurité

Étant donné la dimension transnationale de la cybercriminalité, **INTERPOL recommande fortement aux pays membres africains d'intégrer les initiatives menées par les acteurs de la cybersécurité dans la lutte contre la cybercriminalité.** La coopération avec des parties prenantes comme le secteur privé et les services chargés de la cybersécurité est primordiale pour améliorer les interventions en cas d'atteinte à la cybersécurité, l'accès aux données, l'échange de renseignements sur les menaces, le démantèlement des infrastructures malveillantes et la sensibilisation à la cybersécurité. Par ailleurs, les pays sont encouragés à créer et recourir à des équipes d'intervention informatique d'urgence (CERT) et des cellules d'intervention en cas d'atteinte à la cybersécurité (CSIRT) au niveau national. En vue de favoriser une collaboration plus étroite entre les services chargés de l'application de la loi et les CERT/CSIRT actuelles, INTERPOL et le Forum of Incident Response and Security Teams (FIRST) ont constitué un Special Interest Group (SIG).

4. Mettre l'accent sur l'éducation numérique et la sensibilisation

Afin de lutter contre des techniques d'ingénierie sociale toujours plus élaborées, il convient de mettre l'accent sur le facteur humain, et donc, sur la prévention. **INTERPOL encourage les pays membres africains à poursuivre l'amélioration de l'hygiène informatique, avec l'aide des secteurs public et privé.** Cette stratégie consiste à sensibiliser massivement le grand public dans le cadre d'initiatives officielles et à encourager les personnes et les organisations à sécuriser davantage leurs comptes de messagerie électronique, à utiliser l'authentification multifacteur (AMF), à dispenser des formations approfondies aux salariés et à privilégier les technologies de paiement sécurisé.

De plus, les citoyens doivent être encouragés à signaler systématiquement les cyberinfractions dont ils sont victimes aux services nationaux chargés de l'application de la loi. **À cette fin, il est recommandé aux pays membres de simplifier, dans la mesure du possible, la procédure de signalement et d'enregistrement, par exemple, en mettant à disposition des pages et plateformes en ligne.** Ces mesures proactives permettront non seulement de sécuriser davantage le monde numérique, mais également de mieux comprendre l'environnement virtuel africain.

5. Élargir et approfondir la coopération internationale et régionale

Une collaboration régionale et mondiale efficace est essentielle pour endiguer l'expansion géographique des groupes criminels organisés et de leurs victimes. **INTERPOL exhorte les pays membres à poursuivre l'élargissement et l'approfondissement de leur coopération afin de faire front commun contre la menace mondiale représentée par la cybercriminalité.** Pour ce faire, il convient d'accroître l'échange d'informations et de mener des actions coordonnées et fondées sur le renseignement par l'intermédiaire du Bureau pour les opérations de lutte contre la cybercriminalité en Afrique d'INTERPOL.

INTERPOL continuera d'aider les pays membres africains à limiter l'impact mondial et les préjudices causés par la cybercriminalité, ainsi qu'à protéger les populations pour un monde plus sûr.

CADRE OPÉRATIONNEL CONJOINT POUR L'AFRIQUE

Le Bureau pour les opérations de lutte contre la cybercriminalité en Afrique d'INTERPOL a élaboré un cadre opérationnel conjoint visant à promouvoir une approche cohérente et méthodique en matière de perfectionnement des opérations proactives coordonnées contre la cybercriminalité sur le continent. Ce cadre comprend quatre étapes :

Étape I : Recueil et analyse
La première étape concerne l'analyse approfondie des informations relatives aux principales cybermenaces, aux infrastructures malveillantes et aux cybercriminels ciblant la population dans la région africaine. En s'appuyant sur les renseignements communiqués par les services chargés de l'application de la loi, les recherches menées par l'Unité du Renseignement en matière de cybercriminalité d'INTERPOL et les divers accords de partage de données conclus avec les partenaires du projet Gateway d'INTERPOL, le Bureau pour les opérations de lutte contre la cybercriminalité en Afrique publie le Rapport sur l'évaluation des cybermenaces en Afrique, qui permet aux services chargés de l'application de la loi du continent d'approfondir leur compréhension du contexte des cybermenaces.

Étape II : Priorités et stratégie
Le Rapport sur l'évaluation des cybermenaces en Afrique publié au cours de l'étape I servira de document de référence pour les pays membres africains dans le cadre de l'élaboration ou de l'actualisation de leurs stratégies et méthodes d'enquête, et orientera la priorisation régionale des opérations menées conjointement avec INTERPOL pour l'année à venir. Conscient de la diversité du continent africain et des difficultés spécifiques rencontrées par chaque pays, le Bureau pour les opérations de lutte contre la cybercriminalité en Afrique sollicitera le chef de l'unité Cybercriminalité de chaque pays (avec l'autorisation de son B.C.N.) lors de cette étape en vue d'étudier les possibilités de collaboration tant intrarégionale qu'interrégionale. À l'issue de cette étape, une feuille de route régionale, fondée sur une stratégie commune et définissant clairement les résultats opérationnels pour l'année, sera prête à être publiée.

Étape III : Opérations
Le Bureau pour les opérations de lutte contre la cybercriminalité en Afrique élaborera des plans tactiques standard (PTS) pour mettre en œuvre la stratégie convenue lors de l'étape II. Les PTS définissent clairement les objectifs, les fonctions et les responsabilités, ainsi qu'un concept opérationnel en matière de lutte contre certaines cybermenaces. Chaque PTS comprend généralement un plan détaillé concernant 1) la planification et l'analyse, 2) l'organisation, 3) la tactique et 4) l'évaluation. Les PTS sont ensuite soumis à l'approbation des pays participants.

Les unités spécialisées dans la cybercriminalité désignées par les B.C.N. s'engageront alors à mener les actions décrites dans les PTS et apporteront tout leur soutien à la réalisation des buts et objectifs opérationnels convenus. Une fois les PTS approuvés, les opérations seront coordonnées par le Bureau pour les opérations de lutte contre la cybercriminalité en Afrique et menées par les enquêteurs désignés selon le calendrier défini dans les PTS. Les données relatives aux opérations seront transmises à INTERPOL pour analyse via son système de communication sécurisé I-24/7 ou sa Plateforme collaborative sur la cybercriminalité - Opérations.

À réception des informations opérationnelles, les points de contact désignés de chaque pays membre se mettront en relation avec le Bureau pour les opérations de lutte contre la cybercriminalité en Afrique en vue d'échanger des informations selon les objectifs fixés et le calendrier de l'opération. Le pays membre à l'origine de l'opération en assurera la direction de bout en bout.

La coordination de la conservation et de la diffusion des relevés Internet (informations élémentaires sur les abonnés, données de transmission, contenu, etc.) se feront sur la base du volontariat et sera encouragée dans le cadre des opérations menées en matière de cybercriminalité, au vu de la volatilité des éléments de preuve électroniques. Dans la mesure autorisée par leurs lois et politiques, les pays membres seront fortement invités à communiquer les avancées des enquêtes et les renseignements spécifiques susceptibles d'aider d'autres pays membres pour leurs propres enquêtes. Dans la mesure du possible, les points de contact devront faciliter l'échange d'informations avec d'autres services nationaux tels que les équipes d'intervention informatique d'urgence (CERT) et les banques centrales, en fonction des besoins de chaque opération.

Étape IV : Évaluation
Au cours de l'étape IV, un rapport de retour d'expérience (RRE) sera dressé afin d'identifier les enseignements tirés des opérations. Le Bureau pour les opérations de lutte contre la cybercriminalité en Afrique recommandera des ajustements pour les futures opérations conjointes en s'appuyant sur ce rapport et les nouvelles informations issues des opérations. Les renseignements recueillis lors de l'étape III seront également évalués en vue d'approfondir la compréhension régionale des principales cybermenaces et d'alimenter le prochain Rapport sur l'évaluation des cybermenaces en Afrique.

NOTES méthodologiques relatives au Rapport INTERPOL de 2024 sur l'évaluation des cybermenaces en Afrique

Le présent rapport s'appuie sur les précédentes éditions pour fournir une analyse approfondie du contexte des cybermenaces tel qu'il est perçu par les pays membres africains. Cette édition contient une analyse minutieuse axée sur les principales menaces que sont les rançongiciels, les escroqueries aux faux ordres de virement et les autres formes d'escroqueries en ligne. Outre l'identification de ces problématiques majeures, le rapport étudie les initiatives nationales actuellement menées en vue d'accroître la cyber-résilience à travers le continent. Il conclut avec des recommandations concrètes visant à orienter les futures activités de cybersécurité en Afrique.

L'évaluation est principalement étayée par les renseignements et données opérationnelles issus des activités régionales d'INTERPOL. Des informations supplémentaires proviennent d'une enquête réalisée par INTERPOL, comprenant 40 questions quantitatives et qualitatives sur les thèmes de la prévention, de la détection, de la conduite d'enquêtes et de la répression. Au total, 46 pays membres ont répondu à cette enquête, soit un taux de réponse supérieur à 80 %.

- Afrique du Sud
- Algérie
- Angola
- Bénin
- Botswana
- Burkina Faso
- Burundi
- Cabo Verde
- Cameroun
- Comores
- Congo
- Côte d'Ivoire
- Djibouti
- Guinée équatoriale
- Érythrée
- Eswatini
- Éthiopie
- Gabon
- Gambie
- Ghana
- Guinée
- Guinée-Bissau
- Kenya
- Lesotho
- Libéria
- Madagascar
- Malawi
- Mali
- Maurice
- Mauritanie
- Mozambique
- Namibie
- Niger
- Ouganda
- République démocratique du Congo
- Rwanda
- Sao Tomé-et-Principe
- Sénégal
- Seychelles
- Sierra Leone
- Somalie
- Soudan du Sud
- Tanzanie
- Togo
- Zambie
- Zimbabwe

Enfin, cet ensemble de données a été complété par des concertations stratégiques avec les partenaires du projet Gateway d'INTERPOL, dont Bi.Zone, Fortinet, Group-IB, Kaspersky Lab et Trend Micro.

À PROPOS D'INTERPOL

INTERPOL est l'organisation internationale de police la plus importante au monde. Son rôle est d'assister les services chargés de l'application de la loi de nos 196 pays membres dans la lutte contre toute forme de criminalité transnationale. Il s'emploie à aider les polices du monde entier à relever les défis (de plus en plus nombreux) de la lutte contre la criminalité au 21ème siècle en leur apportant un appui technique et opérationnel grâce à une infrastructure de pointe. Les services de l'Organisation comprennent des formations ciblées, un soutien spécialisé aux enquêtes, des bases de données spécialisées et un système de communication policière sécurisé.

LA VISION D'INTERPOL : « RELIER LES POLICES POUR UN MONDE PLUS SÛR »

La vision d'INTERPOL est celle d'un monde dans lequel chaque professionnel des services chargés de l'application de la loi pourra, par la voie de l'Organisation, transmettre, échanger et consulter en toute sécurité des informations de police vitales, à tout moment et en tout lieu où il en aura besoin, afin d'assurer la sécurité des personnes sur toute la surface du globe. Face aux défis mondiaux rencontrés par la police et la sécurité, INTERPOL n'a de cesse de promouvoir et d'apporter des solutions innovantes et de pointe.

À PROPOS DU PROGRAMME INTERPOL SUR LA CYBERCRIMINALITÉ

Dans un monde numérique dynamique où plus de la moitié de la population mondiale est susceptible d'être exposée à la cybercriminalité, le Programme mondial d'INTERPOL sur la cybercriminalité fournit un appui à la communauté internationale des services chargés de l'application de la loi. Nous sommes déterminés à préparer et piloter une riposte mondiale visant à prévenir et détecter la cybercriminalité, ainsi qu'à enquêter à son sujet et y faire obstacle, avec l'objectif ultime de limiter son impact mondial et de protéger les populations pour un monde plus sûr.

La Stratégie mondiale INTERPOL de lutte contre la cybercriminalité a quatre objectifs principaux :

- Favoriser une démarche proactive et agile en matière de prévention et de répression de la cybercriminalité, en cernant en profondeur le paysage des cybermenaces grâce à l'échange d'informations et l'analyse de renseignements.
- Agir avec efficacité pour prévenir et détecter la cybercriminalité, qui cause des préjudices importants à l'échelle nationale, régionale et mondiale, ainsi qu'enquêter à son sujet et y faire obstacle, en jouant un rôle de direction, de coordination et d'appui auprès des pays membres dans le cadre d'activités opérationnelles transnationales.
- Appuyer l'élaboration des stratégies et le renforcement des capacités des pays membres en matière de lutte contre la cybercriminalité en nouant des partenariats ouverts, inclusifs et pluriels, et en instaurant la confiance dans l'écosystème mondial de la cybersécurité.
- Promouvoir le rôle et les capacités d'INTERPOL dans le processus visant à façonner la sécurité mondiale via la participation à des instances internationales dans le domaine de la cybercriminalité.

Notre Stratégie et ses objectifs sont mis en œuvre selon un modèle simple et constructif, reposant sur trois grands piliers :

- Réponse aux cybermenaces : apporter une réponse rapide et coordonnée aux cybermenaces immédiates et émergentes.
- Opérations de lutte contre la cybercriminalité : mettre en œuvre une stratégie opérationnelle régionale pour lutter efficacement contre la cybercriminalité.
- Renforcement des capacités en matière de cybercriminalité : renforcer les stratégies et les capacités via des plateformes et projets innovants.

Ces piliers s'appuient sur notre vaste réseau de partenaires publics et privés, qui encourage la collaboration et tire parti de l'expertise collective pour lutter contre la cybercriminalité.

Pour de plus amples informations, nous vous invitons à nous contacter à l'adresse suivante : EDPS-CD@interpol.int.

À PROPOS DE L'OPÉRATION CONJOINTE DE LUTTE CONTRE LA CYBERCRIMINALITÉ EN AFRIQUE D'INTERPOL

Le projet AFJOC est une initiative menée par INTERPOL qui vise à renforcer les capacités des services nationaux chargés de l'application de la loi en Afrique en matière de prévention, de détection, d'enquête et de lutte contre la cybercriminalité. Il convient, pour y parvenir, de :

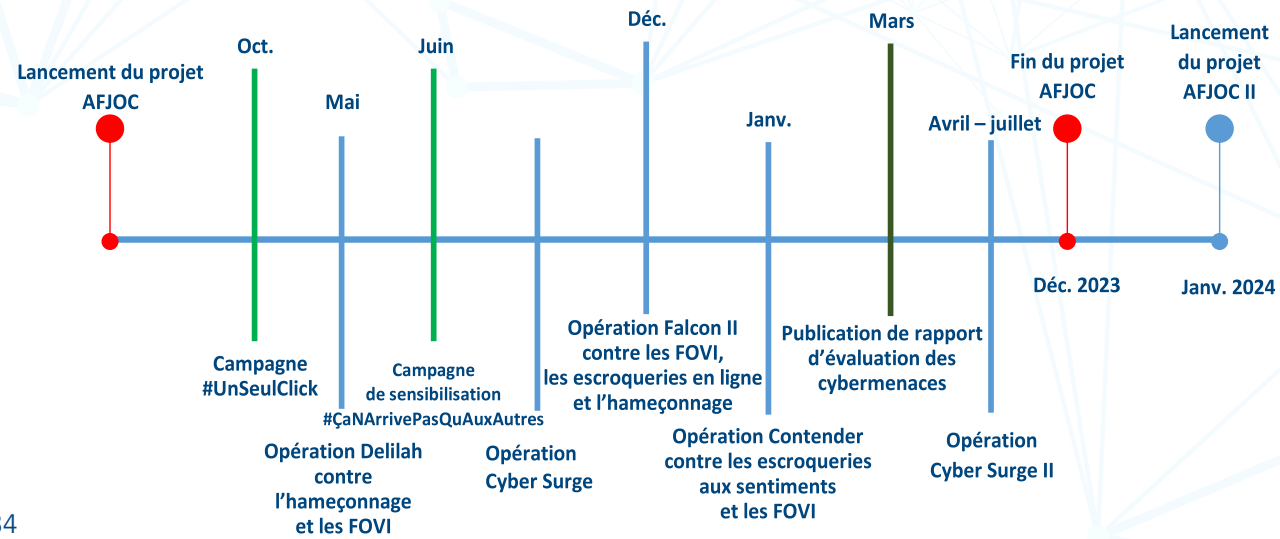
- recueillir et d'analyser les informations relatives aux activités cybercriminelles ;
- mener des actions coordonnées et fondées sur le renseignement ;
- promouvoir la coopération et les bonnes pratiques dans les pays africains.

La phase 1 de l'initiative, qui s'est déroulée de 2021 à 2023, a été financée par le Bureau britannique des Affaires étrangères, du Commonwealth et du Développement. La phase 2, qui bénéficie toujours du soutien du Bureau britannique des Affaires étrangères, du Commonwealth et du Développement, s'appuie sur les réalisations de la première phase et vise à renforcer encore davantage les capacités des services nationaux chargés de l'application de la loi en Afrique.

Activités menées dans le cadre du projet

- Soutien en matière d'analyse et renseignement : des renseignements exacts et obtenus en temps utile sont la clé de toute riposte efficace contre la cybercriminalité. Nos signalements d'activités cybercriminelles constituent d'importantes ressources, qui répertorient les cybermenaces ciblant certains pays ou régions.
- Renforcement des capacités et moyens régionaux de lutte contre la cybercriminalité : des plateformes collaboratives telles que la Plateforme collaborative sur la cybercriminalité et la Plateforme de fusionnement sur la cybercriminalité facilitent la communication et l'échange sécurisés de données sur les opérations.
- Cadre opérationnel conjoint : il cible les cybermenaces via la collaboration entre les services chargés de l'application de la loi, le secteur privé et d'autres organisations internationales ou intergouvernementales.
- Appui opérationnel et coordination : nos opérations contribuent au démantèlement des réseaux cybercriminels.
- Campagnes de sensibilisation : promotion de bonnes pratiques informatiques auprès des particuliers et des entreprises en Afrique.

Le Bureau pour les opérations de lutte contre la cybercriminalité en Afrique d'INTERPOL est responsable de l'exécution du projet AFJOC dans le cadre d'un partenariat étroit avec des acteurs régionaux de premier plan, en particulier l'Union africaine et AFRIPOL, la communauté des services chargés de l'application de la loi et le secteur privé.



INTERPOL

INTERPOL Global Complex for Innovation
18 Napier Road
Singapore 258510

Suivez-nous :

INTERPOL HQ | @INTERPOL_HQ | INTERPOL | INTERPOL HQ | INTERPOL_HQ