ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

cooperation germany – ecowas

EUROPEAN UNION

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Global Gateway

SHADOWSERVER

Région de la CEDEAO :

Informations et recommandations en matière de cybersécurité

Février 2026

SHADOWSERVER

Table des matières

Résumé Analytique

La Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) vise à promouvoir la coopération économique entre ses douze États membres pour rehausser les niveaux de vie et favoriser le développement économique. Dans la poursuite de cet objectif, la Commission et la région de la CEDEAO dans leur ensemble adoptent de plus en plus les technologies numériques en tant que moteur de croissance clé. On a ainsi observé ces dernières années une transformation numérique rapide qui a contribué à stimuler la croissance économique et le développement. Dans le même temps, cette transformation a également fait ressortir l'existence d'une multitude de déficiences ou de « lacunes » institutionnelles et opérationnelles en matière de cybersécurité dans la région, dont certaines sont importantes. Ensemble, ces facteurs (c'est-à-dire, la croissance économique, une empreinte numérique étendue et des déficiences connues en termes de cybersécurité) font de la région une cible de plus en plus attrayante et vulnérable pour les **acteurs malveillants***[1].

Le nombre, l'étendue et l'impact des cyberattaques dans la région de la CEDEAO augmentent à un rythme alarmant. Un rapport d'INTERPOL publié en juin 2025 a averti au sujet d'une forte hausse de la cybercriminalité en Afrique, la cybercriminalité représentant plus de 30 % de tous les crimes signalés en Afrique de l'Ouest[2]. Le rapport estime également à plus de 3 milliards de dollars les pertes financières dues à des cyber-incidents survenus sur l'ensemble du continent entre 2019 et 2025[3].

Récemment, la région a subi des attaques coûteuses par des **logiciels rançonneurs*** ciblant la Compagnie d'électricité du Ghana (Electricity Company of Ghana) [4] et la Banque centrale de la Gambie[5], des attaques par **déni de service distribué (DDOS)*** qui ont perturbé les sites Internet du gouvernement sénégalais [6] et l'opérateur de télécommunications MTN Nigeria[7], ainsi qu'une violation dévastatrice de la sécurité des systèmes de la société de technologie financière ivoirienne de traitement de paiements CinetPay, qui doit plus d'un million de dollars à ses clients[8]. Cela suscite des préoccupations croissantes quant aux capacités de la région en matière de cybersécurité et un sentiment d'urgence à agir.

Il est essentiel de combler les lacunes identifiées dans ce rapport pour garantir que les capacités en termes de cybersécurité ainsi que la cyber-résilience globale suivent le rythme de l'expansion numérique rapide dans la région et qu'elles sont adaptées au volume, à l'ampleur et à la sophistication des nouvelles menaces qui ciblent la région. S'ils ne sont pas résolus, ces problèmes pourraient creuser de plus en plus les lacunes en matière de cybersécurité dans la région, ce qui compromettrait le développement économique, éroderait la confiance du public et affecterait les services qui influent sur la qualité de vie.

Les cybermenaces actuelles auxquelles la région de la CEDEAO est exposée sont clairement documentées. Elles comprennent des **logiciels rançonneurs***, des

---

1 Les termes et les expressions en gras et suivies d'une astérisque (*) sont définis dans la section « Glossaire » à la fin du présent rapport.

2 « Un nouveau rapport d'INTERPOL met en garde contre la forte augmentation de la cybercriminalité en Afrique », *Communiqué de presse d'INTERPOL*, 23 juin 2025. https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2025/Un-nouveau-rapport-d-INTERPOL-met-en-garde-contre-la-forte-augmentation-de-la-cybercriminalite-en-Afrique

3 « Africa faces $3bn in cybercrime losses, Interpol flags top 4 threats », *Ecofin Agency*, 26 août 2025. https://www.ecofinagency.com/news/2608-48171-africa-faces-3bn-in-cybercrime-losses-interpol-flags-top-4-threats

4 « ECG Systems Hacked with Ransomware », *Ghana Business News*, 1er octobre 2022. https://www.ghanabusinessnews.com/2022/10/01/ecg-systems-hacked-with-ransomware-sources/

5 « Hackers Reportedly Demand US$2.5M from Central Bank After Major Data Breach », *The Alkamba Times*, 17 novembre 2022. https://alkambatimes.com/hackers-reportedly-demand-us2-5m-from-central-bank-after-major-data-breach/

6 « Senegalese government websites hit with cyber attack », *Reuters*, 27 mai 2023. https://www.reuters.com/world/africa/senegalese-government-websites-hit-with-cyberattack-2023-05-27/

7 « Au cœur de la cyberattaque de huit heures qui a tenté de paralyser MTN Nigeria », *Techcabal*, 9 juillet 2025. https://techcabal.com/fr/2025/07/09/cyberattack-that-tried-to-cripple-mtn-nigeria/

8 « Les clients de CinetPay se voyaient réclamer plus d'un million de dollars plusieurs mois après une cyberattaque présumée », *Techcabal*, 1er février 2026. https://techcabal.com/fr/2026/02/01/cinetpay-cyberattack/

attaques sur des **infrastructures critiques*, des attaques par déni de service distribué***, la **compromission de messagerie d'entreprise***, des arnaques à la fraude et la sextorsion en ligne, pour n'en citer que quelques-unes. Le présent rapport s'appuie sur des données et des analyses de la Shadowserver Foundation concernant les menaces ainsi que sur ses nombreuses années d'expertise dans le domaine pour informer les principales parties prenantes des lacunes actuelles en matière de cybersécurité institutionnelle et opérationnelle qui rendent la région de la CEDEAO particulièrement vulnérable à ces attaques et à d'autres types de cyberattaques. Ce rapport propose également des recommandations de mesures qui peuvent être prises aux niveaux national et régional pour combler ces lacunes.

Les lacunes *institutionnelles* les plus urgentes et les plus importantes portent sur la nécessité d'institutions de cybersécurité efficaces dans la région, en particulier des **Centres nationaux de réponse aux incidents de sécurité informatique (CSIRT nationaux)*,** un **Centre de partage et d'analyse de l'information (ISAC)* de la CEDEAO,** ainsi que des **CSIRT sectoriels*.** Pour s'acquitter efficacement de leurs obligations et responsabilités respectives, ces entités ont besoin d'un accès à des données, des outils, des services et des plateformes gratuits et/ou abordables ; d'experts techniques internes ; de formations et de services de renforcement des capacités ; d'évaluations de la maturité pour mesurer les progrès en matière de développement ; de partenariats mondiaux et régionaux ; et de la création de **services d'alerte précoce*** pour servir leurs membres.

Outre les lacunes *institutionnelles*, les lacunes techniques *opérationnelles* en matière de cybersécurité associées aux **surfaces d'attaque*** des États membres de la CEDEAO sont moins connues. À l'instar de nombreuses surfaces d'attaque aux attaques, celle de la région de la CEDEAO se caractérise par des **appareils*** et des **services*** qui sont exposés publiquement sur l'Internet (ce qui étend inutilement la surface d'attaque et offre des points d'entrée potentiels dans un réseau) ; des **vulnérabilités critiques*** dans les actifs exposés que des acteurs malveillants peuvent exploiter si elles ne sont pas corrigées ; des **actifs compromis*** qui peuvent *également* être exploités si la compromission n'est pas corrigée ; et des appareils infectés par des **logiciels malveillants***, auxquels les acteurs malveillants ont (ou ont eu) accès et sur lesquels ils exercent (ou ont exercé) un contrôle sans autorisation, souvent par le biais d'un **réseau zombie*** plus étendu.

Un facteur important est que la gestion de la surface d'attaque de la région de la CEDEAO impliquera la mise en œuvre de réglementations appropriées par chaque État membre, afin de veiller à ce que les principaux spécialistes de la défense réseau (en particulier ceux au sein des gouvernements et du secteur des infrastructures critiques) réalisent des **inventaires des actifs*,** garantissent que les actifs ne sont pas inutilement exposés à l'Internet et remédient en temps utile aux **vulnérabilités*** critiques/de sévérité élevée, **aux vulnérabilités exploitées connues *** et aux **actifs compromis*.**

Il est impératif que chacune des principales parties prenantes puisse évaluer sa surface d'attaque aux cyberattaques pour faciliter la formulation de politiques efficaces, élaborer une législation appropriée et mettre en œuvre des mesures de protection de la sécurité de ses réseaux. Il est essentiel que les dirigeants gouvernementaux, les décideurs politiques, les spécialistes de la défense réseau et les experts en cybersécurité travaillent de manière collaborative à la résolution des problèmes identifiés dans le présent rapport.

Un moyen permettant d'informer les principales parties prenantes de la surface d'attaque d'une nation et/ou d'une région consiste à utiliser le Tableau de bord public de Shadowserver. Ce Tableau de bord permet au public d'interroger les données de Shadowserver pour trouver des statistiques agrégées, par pays ou par région, portant sur les dernières cybermenaces survenues au cours des deux dernières années. Ces statistiques peuvent ensuite être utilisées pour établir la priorité des efforts de remédiation et en assurer un suivi, afin de minimiser ou d'éliminer les menaces critiques. Le Tableau de bord permet de rechercher des statistiques associées à un pays ou à une région donnée, notamment un nouvelle fonction de recherche spécifique à la région de la CEDEAO.

Recommandations

Les recommandations de mesures clés pour résoudre les déficiences ou les lacunes institutionnelles et opérationnelles en matière de cybersécurité qui sont identifiées dans le présent rapport sont les suivantes :

Recommandations au niveau des institutions :

CSIRT NATIONAUX

Établir un CSIRT national efficace dans chaque État membre de la CEDEAO.

ISAC DE LA CEDEAO

Établir un ISAC de la CEDEAO pour contribuer à garantir que tous les CSIRT nationaux dans la région travaillent de manière collaborative, partagent des informations, accomplissent des progrès dans leur développement et promeuvent des partenariats vitaux aux niveaux national, régional et international.

CSIRT SECTORIELS

Établir un CSIRT sectoriel pour un secteur comportant des infrastructures critiques identifié comme le plus vulnérable et le plus essentiel dans chaque pays. Dans les limites des fonds disponibles, des CSIRT sectoriels peuvent ensuite être établis dans différents secteurs pour veiller à ce que chaque secteur bénéficie d'une expertise, d'informations sur les menaces, d'une gestion des risques et de services d'intervention face aux incidents qui répondent aux besoins uniques du secteur concerné.

ACCÈS À DES DONNÉES, DES OUTILS ET DES SERVICES GRATUITS/ABORDABLES

Les CSIRT nationaux et les spécialistes de la défense réseau de tous types et dans tous les secteurs doivent tirer parti des données, des outils, des services et des plateformes gratuits et/ou abordables à disposition portant sur les cybermenaces. Cela inclut les rapports de remédiation de réseau quotidiens gratuits de Shadowserver, ainsi que des outils gratuits en open source (notamment IntelMQ, Elasticsearch, Kibana et d'autres) requis pour assimiler, stocker, analyser, interroger, visualiser, évaluer et utiliser efficacement les flux de données sur les menaces. Il convient également d'envisager des outils et services commerciaux potentiellement abordables, notamment Arctic Hub, une plateforme d'automatisation d'informations sur les cybermenaces qui est accessible gratuitement la première année, puis à des tarifs réduits les années suivantes, pour les CSIRT nationaux admissibles, dans le cadre du Programme de développement de CSIRT d'Arctic Security. Comme l'indique le site Internet d'Arctic Security, le CSIRT national de la Gambie (gmCSIRT) participe actuellement au programme.

EXPERTS TECHNIQUES INTERNES

Veiller à ce que les employés de chaque CSIRT national et des spécialistes de la défense réseau dans les systèmes gouvernementaux et d'infrastructures critiques possèdent des compétences techniques adéquates pour pouvoir sécuriser et défendre efficacement les réseaux de la nation. Les États membres de la CEDEAO doivent collaborer avec les universités pour élaborer des programmes de formation et de stage qui peuvent servir de réserve de talents possédant des compétences techniques. Les États membres doivent également collaborer avec le secteur privé pour développer des programmes dans lesquels des experts chevronnés du secteur privé peuvent accomplir un travail temporaire, mais étendu au sein du CSIRT national et des entités gouvernementales/des infrastructures critiques pour accompagner et former les employés moins expérimentés et moins techniques.

Recommandations au niveau des institutions :

FORMATIONS ET RENFORCEMENT DES CAPACITÉS

Rechercher les opportunités existantes en matière de projets de formation et de renforcement des capacités (en particulier des projets opérationnels axés sur l'établissement et l'utilisation efficace de données, d'outils, de services et de plateformes gratuits/en open source). De tels projets sont souvent financés par les ministères des Affaires étrangères (y compris le Bureau fédéral allemand des Affaires étrangères et l'Agence allemande de coopération internationale [GIZ], ainsi que le ministère britannique des Affaires étrangères, du Commonwealth et du Développement) et des entités privées (dont Microsoft et Google), ainsi que par la Banque mondiale, les Nations Unies et l'Union européenne, entre autres entités.

DÉVELOPPEMENT DE PARTENARIATS

Créer un cadre nécessitant que les CSIRT nationaux établissent et entretiennent des relations professionnelles solides avec leurs membres/parties prenantes dans leurs pays respectifs (notamment les fournisseurs d'accès à Internet, les opérateurs d'infrastructures critiques, les entités gouvernementales, les entreprises, les universités, les gouvernements étatiques et locaux, les prestataires de soins de santé, les institutions financières, etc.), ainsi qu'avec les autres CSIRT nationaux de la région de la CEDEAO et du reste du monde. Ces relations sont essentielles pour favoriser le partage d'informations, la collaboration et le renforcement des capacités. Les opportunités permettant aux CSIRT nationaux d'établir des partenariats mondiaux comprennent le recours à un ISAC de la CEDEAO, en devenant membre de FIRST.org et en rejoignant la plateforme de discussion gratuite Alliance Mattermost de Shadowserver, qui facilite un accès direct au personnel de Shadowserver, aux partenaires de l'Alliance issus de l'ensemble de l'industrie et aux CSIRT nationaux du monde entier.

ÉVALUATIONS DE LA MATURITÉ

Pour établir un niveau de maturité de référence, chaque CSIRT national est tenu de se soumettre à l'outil d'autoévaluation en ligne (SIM3) du modèle de maturité de la gestion des incidents de sécurité de l'Open CSIRT Foundation et de mettre en œuvre les mesures recommandées en matière d'amélioration.

SERVICES D'ALERTE PRÉCOCE

Les CSIRT nationaux, les CSIRT sectoriels, les ISAC et d'autres entités sont tenus de proposer des services d'alerte précoce gratuits par lesquels leurs membres reçoivent des avis d'alerte automatisés au sujet d'appareils et de services exposés, mal configurés, exploitables, vulnérables et compromis sur leurs réseaux pour en faciliter une remédiation rapide. Il est recommandé de consulter l'un des nombreux CSIRT nationaux qui fournissent de tels services d'alerte précoce, comme le Centre national britannique de la cybersécurité (UK NCSC) et le CSIRT-RD de la République dominicaine.

Recommandations au niveau opérationnel :

INVENTAIRES D'ACTIFS

Établir des politiques imposant la conduite régulière d'inventaires d'actifs*, particulièrement au sein du gouvernement et des secteurs comportant des infrastructures critiques. Cela aidera les propriétaires de réseau à appliquer rapidement des correctifs, ainsi que dans leurs efforts de remédiation à mesure que de nouvelles vulnérabilités critiques se présentent. *Voir* la « Directive opérationnelle contraignante 23-01 : améliorer la visibilité des actifs et la détection des vulnérabilités sur les réseaux fédéraux ».

VEILLER À CE QUE LES ACTIFS NE SOIENT PAS INUTILEMENT EXPOSÉS À L'INTERNET PUBLIC

S'assurer que les propriétaires de réseau (en particulier, les infrastructures critiques, les gouvernements et les fournisseurs d'accès à Internet de grande envergure) n'exposent pas inutilement certains types d'appareils et de services à l'Internet public, sauf si cela est nécessaire pour des raisons de fonctionnalité. Cette mesure permettra de réduire la surface d'attaque globale de la région. La conduite de formations et d'ateliers dédiés avec les CSIRT nationaux, les fournisseurs d'accès à Internet et d'autres propriétaires de réseau dans la région de la CEDEAO pourrait aboutir à des activités proactives renforcées visant à cibler et à réduire les cas d'exposition inutile d'appareils et de services.

RÉGLEMENTATIONS IMPOSANT UNE REMÉDIATION DES VULNÉRABILITÉS CRITIQUES ET À HAUT RISQUE

Mettre en œuvre des réglementations qui nécessitent que les agences gouvernementales et les infrastructures critiques corrigent les vulnérabilités identifiées comme présentant un « risque critique » dans un délai de 15 jours civils et celles présentant un « risque élevé » dans un délai de 30 jours civils à compter de la date à laquelle elles ont été décelées. *Voir* la « Directive opérationnelle contraignante 19-02 : exigences en matière de remédiation des vulnérabilités pour les systèmes accessibles par Internet ».

RÉGLEMENTATIONS IMPOSANT UNE REMÉDIATION DES VULNÉRABILITÉS EXPLOITÉES CONNUES

Mettre en œuvre des réglementations qui nécessitent que le gouvernement et les infrastructures critiques corrigent les « vulnérabilités exploitées connues » dans un délai de 14 jours. La DHS-CISA tient un catalogue des vulnérabilités exploitées connues identifiant les vulnérabilités considérées comme activement exploitées sur la toile que les agences du gouvernement fédéral américain doivent immédiatement corriger. L'AESRI tient à jour un catalogue similaire – la Base de données des vulnérabilités de l'Union européenne. Enfin, le Tableau de bord public de Shadowserver tient une liste Shadowserver des vulnérabilités exploitées connues identifiées au travers de son réseau de leurres de détection. *Voir* la « Directive opérationnelle contraignante 22-01 : réduire les risques importants en termes de vulnérabilités exploitées connues ».

RÉGLEMENTATIONS IMPOSANT UNE REMÉDIATION DES APPAREILS COMPROMIS IDENTIFIÉS ET INFECTÉS PAR DES LOGICIELS MALVEILLANTS

Mettre en œuvre des réglementations exigeant des CSIRT nationaux, des agences gouvernementales, des infrastructures critiques, des fournisseurs d'accès à Internet et des autres propriétaires de réseau dans la région qu'ils résolvent, dans un délai court, mais spécifique, les problèmes liés aux appareils identifiés comme étant compromis et infectés par des logiciels malveillants, notamment ceux identifiés dans les rapports de remédiation de réseau quotidiens gratuits de Shadowserver.

Recommandations au niveau opérationnel :

CAMPAGNES D'ATTÉNUATION/ D'ÉLIMINATION DES MENACES

Imposer aux CSIRT nationaux, en coordination avec les fournisseurs d'accès à Internet, de concevoir et de mettre en œuvre des campagnes d'atténuation et d'élimination des menaces à l'échelle nationale contre les vulnérabilités critiques et les appareils compromis sur les réseaux dans l'ensemble du pays, et d'assurer un suivi de l'avancement des efforts de remédiation. Un exemple en est la campagne nationale dirigée par l'Australian Signals Directorate (ASD) en vue d'éliminer les implants « Bad Candy » dans des appareils Cisco IOS XE compromis dans l'ensemble de l'Australie.

TABLEAU DE BORD PUBLIC GRATUIT DE SHADOWSERVER

Le Tableau de bord public de Shadowserver peut être un outil efficace pour informer les principales parties prenantes (par ex. les décideurs politiques, les dirigeants gouvernementaux, les spécialistes de la défense réseau, les chercheurs en cybersécurité, etc.) des dernières cybermenaces qui touchent leur pays et/ou la région. Ce Tableau de bord permet au public d'interroger les données de Shadowserver pour trouver des statistiques agrégées, par pays ou par région, portant sur les dernières cybermenaces survenues au cours des deux dernières années. Ces statistiques peuvent ensuite être utilisées pour établir la priorité des efforts de remédiation et en assurer un suivi, afin de minimiser ou d'éliminer les menaces critiques. Le Tableau de bord permet de rechercher des statistiques associées à un pays ou à une région donnée, notamment un nouvelle fonction de recherche spécifique à la région de la CEDEAO.

Introduction

L'une des priorités clés des efforts de la CEDEAO a porté sur les domaines de la cybersécurité et de la cybercriminalité. En 2021, par exemple, la CEDEAO a adopté sa *Stratégie régionale de cybersécurité et de lutte contre la cybercriminalité*, qui définit des mesures à prendre au niveau national pour « améliorer la cyber-résilience dans la région, aider les États membres à renforcer leurs capacités en termes de cybersécurité, protéger leur cyberespace et leurs infrastructures d'information critiques et instaurer la confiance et la sécurité dans l'utilisation des technologies de l'information et de la communication (TIC)[9] ». Parmi les mesures proposées figurent « l'adoption de stratégies nationales pour la cybersécurité, le renforcement des développements et des capacités en matière de cybersécurité et la priorisation des efforts en faveur de la cybersécurité pour les infrastructures critiques et les services essentiels[10] ».

La Stratégie de la CEDEAO indique que « la transformation numérique rapide en cours en Afrique de l'Ouest est d'une grande importance pour améliorer le fonctionnement et l'efficacité des administrations, des politiques publiques et des économies, ainsi que le bien-être des populations[11] ». Il est bien établi qu'une infrastructure numérique sécurisée et stable est requise pour assurer une croissance économique durable dans la région de la CEDEAO. Entre autres éléments, elle encouragera les investissements financiers, renforcera le développement des affaires, améliorera l'efficience opérationnelle et la productivité, protégera les infrastructures critiques, facilitera les services publics essentiels, fournira un accès aux marchés mondiaux et, peut-être le point le plus important, elle favorisera la confiance des consommateurs, des entreprises et des investisseurs dans la sécurité numérique de la région pour promouvoir la croissance économique.

À l'inverse, l'économie à croissance rapide de la région de la CEDEAO et son empreinte numérique en pleine expansion en font une cible de plus en plus attrayante pour les acteurs malveillants. Les lacunes en cybersécurité de la région, qui risquent de l'empêcher de suivre le rythme de l'intensification des menaces et donc d'accroître son exposition aux attaques, suscitent des préoccupations.

Le présent rapport a été rédigé par la Shadowserver Foundation (« Shadowserver ») conformément au projet de renforcement des cyber-capacités prévu dans le cadre du partenariat entre la CEDEAO et le G7 pour la cybersécurité, la « Plateforme conjointe pour l'avancement de la cybersécurité » (JPAC) en Afrique de l'Ouest. Ce projet a été lancé par la Commission de la CEDEAO en collaboration avec la présidence allemande du G7 en 2022 et il a été commandité par le Bureau fédéral allemand des Affaires étrangères et la Commission de l'Union européenne en 2023.

---

[9] « Information and Communication Technology: ECOWAS adopts a Regional Strategy for Cybersecurity and the fight against Cybercrime » (Technologies de l'information et de la communication : la CEDEAO adopte une Stratégie régionale de cybersécurité et de lutte contre la cybercriminalité), *site Internet officiel du Parlement de la CEDEAO*, https://www.parl.ecowas.int/information-and-communication-technology-ecowas-adopts-a-regional-strategy-for-cybersecurity-and-the-fight-against-cybercrime/

[10] « Digital transformation, development and resilience in West Africa », *chapitre du Business Continuity Institute (BCI) en Afrique de l'Ouest*, https://www.thebci.org/news/digital-transformation-development-and-resilience-in-west-africa.html

[11] « Introduction : Stratégie régionale de cybersécurité et de lutte contre la cybercriminalité de la CEDEAO », *cyberportail de la CEDEAO*, https://cyberportal.ecowas.int/wpfd_file/ecowas-regional-cybersecurity-cybercrime-strategy-en/

La focalisation géographique du présent rapport est la région de la CEDEAO et ses douze (12) États membres, à savoir, le Bénin, Cabo Verde, la Côte d'Ivoire, la Gambie, le Ghana, la Guinée, Guinée-Bissau, le Liberia, le Nigeria, le Sénégal, la Sierra Leone et le Togo. Les constatations et les recommandations reposent sur les plus de 20 années d'expérience de Shadowserver sur le terrain, ainsi que sur des analyses de données pertinentes pour la région de la CEDEAO au cours de la période du 1er octobre 2024 au 24 avril 2025.

Les objectifs du rapport sont de fournir aux dirigeants gouvernementaux, aux décideurs politiques et aux autres parties prenantes clés des informations sur les aspects suivants :

Le paysage **des cybermenaces*** et la **surface d'attaque*** dans la région de la CEDEAO, en utilisant des renseignements concrets sur les menaces, des analyses de données et les avis d'experts de Shadowserver au cours de la période concernée

Les lacunes **institutionnelles et opérationnelles en termes de cybersécurité** dans la région qui accroissent la vulnérabilité de cette dernière face aux cybermenaces

Les **mesures recommandées** qui peuvent être prises aux niveaux national et régional pour combler les lacunes de cybersécurité identifiées, afin d'améliorer la sécurité numérique et de renforcer la cyber-résilience dans la région de la CEDEAO

L'impact économique et sociétal potentiel si les lacunes institutionnelles et opérationnelles identifiées en termes de cybersécurité restent irrésolues.

1.0// Perspectives de Shadowserver sur les Cybermenaces dans la Région de la CEDEAO

Le **paysage actuel des cybermenaces*** dans la région de la CEDEAO se caractérise par des attaques par des logiciels rançonneurs, des attaques sur des infrastructures critiques, des attaques par déni de service distribué, la compromission de messagerie d'entreprise (BEC), des arnaques à la fraude en ligne et la sextorsion numérique, entre autres types d'attaques.

Un rapport d'INTERPOL publié en juin 2025 met en garde contre une forte hausse de la cybercriminalité en Afrique. Ce rapport présente une analyse étendue des menaces en matière de cybercriminalité qui touchent actuellement l'Afrique (y compris l'Afrique de l'Ouest en particulier), et il est recommandé à toutes les parties prenantes clés de la région de la CEDEAO de le lire. Étant donné que les cybermenaces qui ciblent actuellement la région de la CEDEAO sont clairement documentées dans le rapport d'INTERPOL et dans une multitude d'autres ressources (par ex. « Africa Cyberthreat Landscape Report 2025 » de Kaspersky Labs), le présent rapport se concentre moins sur l'éventail de cybermenaces elles-mêmes, et davantage sur les lacunes de cybersécurité qui exposent la région à ces menaces. Néanmoins, le présent rapport fournit au lecteur un aperçu de haut niveau sur certaines menaces au sujet desquelles Shadowserver peut fournir des informations utiles.

1.1// Logiciels rançonneurs et double extorsion

Les **logiciels rançonneurs*** et les attaques connexes par **double extorsion*** continuent de poser d'importants problèmes dans la plupart des régions du monde, et la région de la CEDEAO n'y fait pas exception. En novembre 2022, il a été signalé que des pirates ont violé la sécurité des systèmes numériques de la Banque centrale de la Gambie et exigé le paiement d'une rançon de 2,5 millions de dollars US en échange de deux téraoctets de données sensibles volées à la Banque[12]. Les données volées comprenaient vraisemblablement les finances personnelles des Gambiens ; des données sur l'économie nationale ; des bases de données de clients et de partenaires ; des données sur le chiffre d'affaires afférant à des transactions financières avec les États-Unis et d'autres pays ; des données liées à la distribution de titres ; et des données sur les liquidités des banques commerciales du pays. Ces attaques peuvent générer des préjudices dévastateurs sur le plan financier et en termes de réputation.

Shadowserver recueille des informations sur les activités de divers groupes de criminels utilisant des logiciels rançonneurs. Les informations sont recueillies dans le cadre d'observations systématiques de **sites de fuite de données*** de groupes utilisant des logiciels rançonneurs. Shadowserver alerte régulièrement les CSIRT nationaux et les agences de répression du monde entier au sujet des informations publiées sur les sites de fuite.

En 2024 et 2025, Shadowserver a observé que des groupes inconnus utilisant des logiciels rançonneurs revendiquaient de

Acteur	Pays de la victime	Date de publication sur le site	Secteur de la victime	Nbre d'employés	Chiffre d'affaires annuel (en dollars)
Blacksuit	Nigeria	Mai 2024	Services professionnels, scientifiques et techniques	766	1 090 000 000
	Ghana	Octobre 2024	Services utilitaires	405	29 700 000
Brain Cipher	Ghana	Août 2024	Finances et assurances	106	9 000 000
Hunters International	Côte d'Ivoire	Mai 2024	Administration publique	1 879	392 000 000
	Sénégal	Septembre 2024	Autres services	33	6 000 000
Kill Security	Nigeria	Novembre 2024	Services professionnels, scientifiques et techniques	S.O.	S.O.
	Ghana	Février 2025	Finances et assurances	S.O.	S.O.
	Nigeria	Mars 2025	Services administratifs, de soutien, de gestion des déchets et de remédiation	5 578	306 800 000
LockBit 3.0	Côte d'Ivoire	Février 2024	Services professionnels, scientifiques et techniques	211	26 900 000
	Sénégal	Mai 2024	Services professionnels, scientifiques et techniques	95	5 000 000
Lynx	Cabo Verde	Novembre 2024	Finances et assurances	S.O.	5 400 000
Pryx	Nigeria	Octobre 2024	Inconnu – 29 victimes potentielles	S.O.	S.O.
RansomHub	Nigeria	Janvier 2025	Services professionnels, scientifiques et techniques	1 628	293 800 000
Space Bears	Côte d'Ivoire	Août 2024	Services administratifs, de soutien, de gestion des déchets et de remédiation	105	S.O.
Funksec	Nigeria	Janvier 2025	Information	S.O.	S.O.
	Nigeria	Décembre 2024	Administration publique	19 627	157 500 000
GDLockerSec	Nigeria	Janvier 2025	Administration publique	S.O.	S.O.
DragonRansomware	Côte d'Ivoire	Décembre 2024	Services administratifs, de soutien, de gestion des déchets et de remédiation	S.O.	S.O.

Figure 01. **Auteurs d'attaques par logiciel rançonneur ayant revendiqué des attaques dans des États de la CEDEAO (entre janvier 2024 et mai 2025)**

[12] « Hackers Reportedly Demand US$2.5M from Central Bank After Major Data Breach », *The Alkamba Times*, 17 novembre 2022. https://alkambatimes.com/hackers-reportedly-demand-us2-5m-from-central-bank-after-major-data-breach/

nombreuses attaques contre des organisations de la région de la CEDEAO. Toutefois, du fait que les organisations qui payent une rançon ne sont généralement pas nommées sur le site de fuite, il n'est pas possible d'établir avec certitude le nombre total d'attaques par logiciel rançonneur qui sont survenues dans un pays ou une région spécifique. Néanmoins, on s'attend à une hausse probable des attaques par logiciel rançonneur et par double extorsion dans la région de la CEDEAO, car la croissance économique et l'expansion numérique continuent de dépasser les capacités en cybersécurité.

La Figure 01 ci-dessous contient un résumé des informations sur les victimes de logiciels rançonneurs dans la région de la CEDEAO, qui proviennent de sites de fuite de groupes utilisant des logiciels rançonneurs. Les noms réels des victimes et les adresses URL associées ont été supprimés pour protéger l'anonymat des victimes. Veuillez noter que Shadowserver n'observe pas nécessairement tous les sites de fuite existants, en particulier ceux associés à des acteurs malveillants dont le champ d'action est plus régional.

Comme l'indique la Figure 01, les revendications portent sur divers secteurs, tant publics que privés. La plupart des revendications se focalisent sur le Nigeria, la Côte d'Ivoire et le Ghana.

Les attaques par logiciel rançonneur peuvent entraîner des bouleversements coûteux dans les activités et la perte d'informations et de données critiques. Avec la poursuite du développement des entreprises et de la croissance des économies dans la région de la CEDEAO, il est probable que les attaques par logiciel rançonneur augmenteront. Si la sécurité numérique dans la région ne suit par le rythme de la croissance économique actuelle, les résultats pourraient être graves, avec une poursuite de la hausse de la cybercriminalité et une chute majeure du développement des entreprises et des investissements financiers dans la région.

1.2// Attaques sur les infrastructures critiques

Les cyberattaques contre les réseaux d'**infrastructures critiques*** se présentent sous de nombreuses formes, qui dépendent généralement de la nature et des motivations des attaquants. Par exemple, les acteurs malveillants d'États-nations peuvent chercher à violer la sécurité de réseaux d'infrastructures critiques à des fins d'espionnage, pour infliger des préjudices destructeurs ou pour faire des déclarations politiques, tandis que les groupes de cybercriminalité transnationale déploient des logiciels rançonneurs à des fins lucratives.

En 2022, la Compagnie d'électricité du Ghana (ECG), le plus grand fournisseur d'électricité dans le pays, a été la victime d'une attaque par logiciel rançonneur. Suite à cette attaque, les clients auraient été privés d'électricité et/ou n'auraient pas été en mesure d'acheter de l'électricité pendant plusieurs jours, du fait que les attaquants avaient crypté diverses sections du système d'ECG pour qu'elles soient inutilisables[13]. Par la suite, le directeur général d'ECG a confirmé que l'attaque par logiciel rançonneur avait entraîné la perte de près de 500 millions de cedis ghanéens (soit environ 40 millions d'euros ou 47 millions de dollars US)[14].

En décembre 2024, le Bureau national de la statistique (NBS) du Nigeria a subi une cyberattaque qui a temporairement paralysé ses systèmes et perturbé l'accès du public à des données nationales critiques pendant près d'un mois.[15] Cette violation a également suscité des préoccupations quant à « l'exposition potentielle de données critiques, notamment des rapports économiques, des statistiques démographiques et d'autres informations essentielles vitales pour la planification nationale et la formulation de politiques[16] ».

Ces exemples témoignent de la focalisation croissante des acteurs malveillants sur les institutions nationales et les infrastructures critiques, ainsi que de l'impact sociétal qui peut résulter de telles attaques.

[13] « ECG Systems Hacked with Ransomware », *Ghana Business News*, 1er octobre 2022. https://www.ghanabusinessnews.com/2022/10/01/ecg-systems-hacked-with-ransomware-sources/

[14] « ECG Lost Nearly GH¢500 Million Due to Ransomware Attack », Electricity Company of Ghana Limited, 29 août 2024 https://ecg.com.gh/index.php/en/media-centre/news-events/ecg-lost-nearly-gh-500-million-due-to-ransomware-attack-managing-director-confirms

[15] « NBS to resume services on January 15, three weeks after cyberattack », *Techpoint*, 9 janvier 2025. https://techpoint.africa/news/nbs-to-resume-services-on-january-15/

[16] « Cyberattack Hits Nigeria's Statistics Bureau », *TechInAfrica*, 25 décembre 2024. https://www.techinafrica.com/cyberattack-hits-nigerias-statistics-burea/

1.3// Déni de service distribué (DDoS)

Shadowserver recueille des données provenant d'environ 2 700 **leurres de détection*** qu'elle conserve dans des centres de données et d'autres lieux dispersés dans le monde. Ces capteurs sont des leurres configurés pour sembler être des actifs de réseau (notamment des applications logicielles, des serveurs et d'autres appareils) légitimes, mais vulnérables en vue d'inciter les acteurs malveillants à les attaquer. Les capteurs enregistrent alors les activités des attaquants et recueillent des informations sur leurs tactiques, leurs outils et leurs procédures/techniques. Les données recueillies contribuent à identifier les sources des attaques et les nouvelles méthodes d'attaque, à développer des défenses et à prévenir des attaques futures.

Grâce aux observations de nos leurres de détection, Shadowserver surveille diverses formes d'attaques par DDoS. En conséquence, nous sommes en mesure de retrouver les victimes d'attaques à un moment donné. Nous observons des attaques par DDoS régulières dans la région de la CEDEAO, principalement au Nigeria.

Comme le montrent les Figures 02 et 03 ci-dessous, le pays le plus attaqué (par adresse IP cible unique et en nombre de tentatives) était le Nigeria.

Les attaques par DDoS peuvent provoquer des perturbations considérables et coûter très cher aux entreprises et aux gouvernements.

En mai 2023, un groupe de pirates appelé Mysterious Team a désactivé la connexion Internet de plusieurs sites Internet du gouvernement sénégalais suite à une attaque par DDoS[17].

Figure 02. **Attaques par DDoS par adresse IP cible unique – région de la CEDEAO**

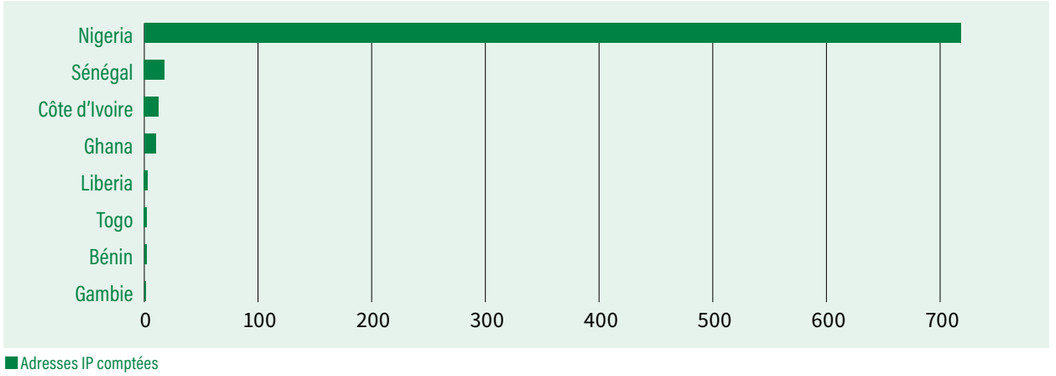
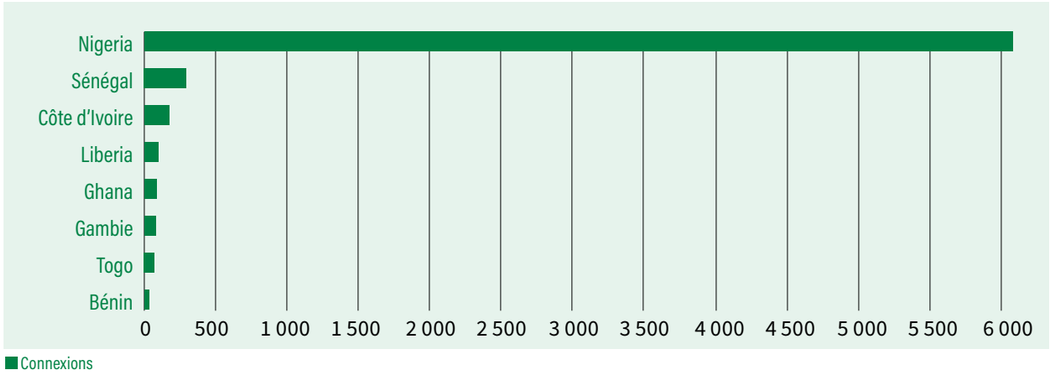


Figure 03. **Attaques par DDoS – par tentative unique – région de la CEDEAO**



[17] « Senegalese government websites hit with cyber attack », *Reuters*, 27 mai 2023. https://www.reuters.com/world/africa/senegalese-government-websites-hit-with-cyberattack-2023-05-27/

En août 2023, le plus grand opérateur de télécommunications au Nigeria, MTN Nigeria, a subi l'une des attaques par DDoS les plus étendues jamais observées contre une entreprise d'Afrique de l'Ouest. L'attaque, menée par un célèbre groupe de cybermilitants appelé Anonymous Sudan, a duré près de huit heures, submergeant le réseau de MTN de trafic malveillant provenant d'ordinateurs compromis du monde entier, en vue de perturber les services vocaux et de données de MTN[18].

Ces exemples montrent que les attaques par DDoS peuvent avoir des effets dévastateurs sur la société et qu'elles entraveront la croissance des affaires et le développement économique si elles ne sont pas résolues. Des stratégies d'atténuation et de protection contre les attaques par DDoS doivent être conçues et mises en œuvre aux niveaux national et régional.

1.4// Compromission de messagerie d'entreprise (BEC)

Selon certaines informations, les arnaques par compromission de messagerie d'entreprise (BEC) seraient en hausse dans la région de la CEDEAO. En juillet 2024, le Département national des Technologies de l'information (NITDA) du Nigeria a lancé une alerte nationale au sujet des taux alarmants d'arnaques par BEC contre des personnes et des organisations à travers le Nigeria[19].

En outre, bien que les détails soient limités et que l'événement n'ait pas été largement médiatisé, l'annonce récente par INTERPOL de l'Opération Sentinel comprenait une référence à une société pétrolière majeure au Sénégal qui avait « décelé l'existence d'un système de BEC sophistiqué dans lequel les fraudeurs infiltraient des systèmes de messagerie électronique et se faisaient passer pour des cadres afin d'autoriser des transferts frauduleux d'argent d'un montant de 7,9 millions de dollars US ». L'annonce indiquait que les autorités sénégalaises avaient gelé de toute urgence les comptes de destination et qu'elles étaient parvenues à stopper la transaction avant le retrait des fonds.

Dans le cadre de tactiques de BEC moins sophistiquées, par exemple, les arnaqueurs créent de fausses adresses électroniques et de faux domaines similaires à des adresses et domaines légitimes pour tromper les destinataires. Dans les tactiques de BEC plus sophistiquées, les arnaqueurs peuvent violer la sécurité d'un serveur de messagerie électronique ou accéder sans autorisation au compte de messagerie électronique d'un employé par le biais d'un hameçonnage et/ou de logiciels malveillants et en envoyant des demandes de paiements de factures à des fournisseurs qui figurent parmi les contacts de messagerie de l'employé. Bien que la protection d'un employé contre une arnaque par BEC repose principalement sur les formations et l'éducation qu'il a suivies, il est tout aussi important de sécuriser les serveurs et les comptes de messagerie électronique à mesure que les arnaques par BEC deviennent de plus en plus sophistiquées.

[18] « Au cœur de la cyberattaque de huit heures qui a tenté de paralyser MTN Nigeria », *Techcabal*, 9 juillet 2025. https://techcabal.com/fr/2025/07/09/cyberattack-that-tried-to-cripple-mtn-nigeria/

[19] « NITDA warns of rising business email compromise scams in Nigeria », *Technology Times*, 17 juillet 2024. https://technologytimes.ng/nitda-warns-of-business-email-compromise-scams/

2.0// Lacunes institutionnelles en termes de cybersécurité et recommandations

2.1// **Centres nationaux de réponse aux incidents de sécurité informatique (CSIRT nationaux)**

2.2// **ISAC de la CEDEAO**

2.3// **ISAC sectoriels**

2.4// **Accès à des données, outils et services gratuits/abordables**

2.5// **Experts techniques internes**

2.6// **Formations et renforcement des capacités**

2.7// **Développement de partenariats**

2.8// **Évaluations de la maturité**

2.9// **Services d'alerte précoce**

2.1// Centres nationaux de réponse aux incidents de sécurité informatique (CSIRT nationaux)

Deux États membres de la CEDEAO ne disposent actuellement pas de CSIRT national défini.

L'établissement d'un CSIRT national au sein de chaque nation de la CEDEAO est une première étape essentielle hautement prioritaire pour s'assurer de mieux protéger la cybersécurité d'une nation (et une région).

Le principal défi sera toutefois de s'assurer que tous les CSIRT nationaux dans la région assument leurs obligations et responsabilités de manière efficace. Les recommandations figurant dans la présente se focalisent sur les moyens permettant d'améliorer l'efficacité des CSIRT nationaux ainsi que celle d'entités similaires telles que les ISAC et les CSIRT sectoriels.

RECOMMANDATION :
Établir un CSIRT national efficace dans chaque État membre de la CEDEAO.

2.2// ISAC de la CEDEAO

Un Centre de partage et d'analyse de l'information (ISAC) est une organisation dirigée par ses membres qui regroupe, analyse et diffuse des informations concrètes sur les menaces pour aider ses membres à en atténuer les risques de manière proactive. Shadowserver est informée qu'un ISAC de la CEDEAO est actuellement prévu. L'initiative vise à renforcer la cybersécurité régionale en créant une plateforme de collaboration pour le partage de renseignements sur les menaces, des meilleures pratiques et de ressources parmi les nations de l'Afrique de l'Ouest. Contrairement à un CSIRT national, les coûts d'exploitation associés à un ISAC régional de la CEDEAO peuvent être partagés entre les États membres.

Shadowserver fournit chaque jour des renseignements gratuits sur les cybermenaces à 201 CSIRT nationaux responsables de 175 pays pour les aider à sécuriser les réseaux de leur nation. Un CSIRT national efficace est essentiel pour renforcer la cyber-résilience dans un pays.

Il fait office d'autorité centrale du pays pour répondre aux incidents de cybersécurité au niveau national et les gérer, protéger les infrastructures critiques nationales, fournir des orientations et des avis de sécurité aux secteurs public et privé et faciliter la coopération dans le cadre de cyber-événements transfrontières.

Les principales responsabilités d'un CSIRT national comprennent la détection et l'analyse des incidents, la conduite d'activités de réponse et de remédiation des incidents, le partage d'informations et la diffusion d'alertes/de renseignements concernant les menaces/d'avis de sécurité, la coordination avec les agences nationales et leurs homologues internationaux, et la mise en œuvre de mesures de prévention dans un pays.

RECOMMANDATION :
L'établissement d'un ISAC de la CEDEAO est fortement recommandé et sera essentiel pour aider à s'assurer que tous les CSIRT nationaux de la région travaillent de manière collaborative, partagent des informations et avancent dans leur développement. Un ISAC de la CEDEAO contribuera également à favoriser des partenariats régionaux avec des entités telles que les fournisseurs d'accès à Internet et les opérateurs d'infrastructures critiques, ainsi que des partenariats internationaux avec les CSIRT nationaux. Contrairement à un CSIRT national, les coûts de développement et d'exploitation associés à un ISAC régional de la CEDEAO peuvent être partagés entre les États membres.

2.3// CSIRT sectoriels

Un CSIRT sectoriel est une entité spécialisée qui traite les réponses à des incidents de cybersécurité, promeut le partage d'informations pour atténuer des menaces et offre des connaissances et une expertise spécialisées dans un secteur spécifique (par ex. eau, santé, énergie, finances, transports, etc.) d'un pays ou d'une économie. Il permet d'assurer des activités efficaces uniques à son secteur pour prévenir des menaces et y répondre. La priorité doit porter sur protection des infrastructures critiques et des services publics. Une manière d'y parvenir consiste à établir des CSIRT sectoriels pour chaque secteur comportant des infrastructures critiques. Suite à l'établissement d'un CSIRT national efficace, il faut créer des CSIRT sectoriels, dans les limitées des financements disponibles, en commençant par le secteur identifié comme étant le plus critique. Ensuite, il est possible d'étendre progressivement la création de CSIRT sectoriels supplémentaires aux différents secteurs.

RECOMMANDATION :
Après l'établissement d'un CSIRT national efficace dans chaque État membre, un CSIRT sectoriel doit être créé pour le secteur comportant des infrastructures critiques qui est considéré comme le plus vulnérable et le plus vital à protéger dans chaque pays. Selon les fonds disponibles, des CSIRT sectoriels supplémentaires pourront être établis dans d'autres secteurs. Cela contribuera à garantir que chaque secteur aux infrastructures critiques bénéficie d'une expertise, d'informations sur les menaces, d'une gestion des risques et de services d'intervention face aux incidents qui répondent aux besoins uniques du secteur concerné.

2.4// Accès à des données, outils et services gratuits/abordables

Il est impératif que les CSIRT nationaux, les équipes sectorielles d'intervention en cas d'urgence informatique (CERT sectorielles), les ISAC et les spécialistes de la défense réseau de tous types et dans l'ensemble des secteurs puissent accéder aux données, outils, services et plateformes de qualité consacrés aux cybermenaces qui sont requis pour que ces entités puissent assumer comme il se doit leurs obligations et fonctions respectives. Cela inclut les outils nécessaires pour assimiler, stocker, analyser, interroger, visualiser, évaluer et utiliser efficacement les données sur les cybermenaces. Des plateformes automatisées sont également requises pour diffuser des avis d'alerte aux propriétaires de réseaux de membres touchés concernant les vulnérabilités critiques et les actifs compromis, afin d'en assurer une résolution rapide.

Malheureusement, les restrictions de fonds et les coûts élevés liés à un grand nombre de ces éléments constituent un obstacle majeur. Toutefois, des données, outils, services et plateformes sont disponibles gratuitement ou à un prix abordable et tous les spécialistes de la défense réseau dans la région doivent mettre pleinement à profit ces précieuses ressources pour pouvoir sécuriser leurs réseaux de façon adéquate.

Lacunes institutionnelles en termes de cybersécurité et recommandations

Dans la région de la CEDEAO, par exemple, les CSIRT nationaux du Bénin, de la Côte d'Ivoire, de la Gambie, du Ghana, du Nigeria, de la Sierra Leone et du Togo sont tous abonnés aux rapports de remédiation de réseau quotidiens gratuits de Shadowserver pour pouvoir sécuriser les réseaux de leur nation. Ces rapports fournissent à chaque CSIRT national des données nationales avec toutes les adresses IP géolocalisées dans leurs pays respectifs. Les rapports identifient les appareils exposés, exploitables, mal configurés, vulnérables et compromis nécessitant des correctifs ou une remédiation avant que des acteurs malveillants parviennent à les exploiter (ou à les exploiter davantage). Il incombe à chaque CSIRT national d'utiliser ces rapports pour diffuser des avis d'alerte aux propriétaires des réseau affectés dans l'ensemble de leur pays.

Les propriétaires de réseau individuels de tous types et dans l'ensemble des secteurs (par ex., banques, hôpitaux, fournisseurs d'accès à Internet, universités, organisations à but non lucratif et ONG, petites et grandes entreprises, gouvernements locaux/étatiques, etc.) peuvent également s'abonner pour recevoir *directement* les rapports de remédiation de réseau de Shadowserver qui sont associés à leurs propres réseaux individuels. En conséquence, l'utilisation des rapports de remédiation de réseau quotidiens gratuits de Shadowserver doit être étendue à tous les spécialistes de la défense réseau dans la région, particulièrement ceux au sein de gouvernements, d'infrastructures critiques, de fournisseurs de télécommunications et de fournisseurs d'accès à Internet, entre autres acteurs.

Des outils gratuits en open source, notamment IntelMQ, Elasticsearch, Kibana et d'autres, sont disponibles pour aider à assimiler, analyser, interroger, visualiser et évaluer les flux de données de Shadowserver et d'autres portant sur des menaces. Nombre d'outils commerciaux abordables sont également disponibles. Par exemple, Arctic Hub, une plateforme d'automatisation de renseignements sur les cybermenaces qui recueille, harmonise et distribue des données sur les menaces provenant de nombreux flux de données, est accessible gratuitement la première année, puis à un tarif réduit les années suivantes pour les CSIRT nationaux admissibles, dans le cadre du Programme de développement de CSIRT d'Arctic Security. Comme l'indique le site Internet d'Arctic Security, le CSIRT national de la Gambie (gmCSIRT) participe actuellement au programme.

RECOMMANDATION :
Les CSIRT nationaux et les spécialistes de la défense réseau de tous types et dans tous les secteurs doivent tirer parti des données, des outils des services et des plateformes gratuits et/ou abordables à disposition portant sur les menaces. Cela inclut les rapports de remédiation de réseau quotidiens gratuits de Shadowserver, ainsi que des outils gratuits en open source (notamment IntelMQ, Elasticsearch, Kibana et d'autres) requis pour assimiler, stocker, analyser, interroger, visualiser, évaluer et utiliser efficacement les flux de données sur les menaces. Il convient également d'envisager des outils commerciaux potentiellement abordables. Par exemple, Arctic Hub, une plateforme d'automatisation de renseignements sur les cybermenaces qui recueille, harmonise et distribue des données sur les menaces provenant de nombreux flux de données, est accessible gratuitement la première année, puis à un tarif réduit les années suivantes pour les CSIRT nationaux éligibles, dans le cadre du Programme de développement de CSIRT d'Arctic Security. Le CSIRT national de la Gambie (gmCSIRT) participe actuellement à ce programme.

2.5// Experts techniques internes

La disponibilité de données, d'outils et de services gratuits ou abordables sur les menaces nécessite toutefois des experts techniques en interne capables de les utiliser efficacement. Shadowserver a rencontré des CSIRT nationaux et d'autres entités dont les employés manquent des connaissances techniques permettant d'utiliser efficacement les données, outils et services disponibles.

Il peut être difficile de recruter et de retenir des employés possédant l'expertise technique nécessaire, particulièrement pour les CSIRT nationaux, les CSIRT sectoriels et d'autres entités gouvernementales qui ne parviennent pas à rivaliser avec les niveaux de salaire du secteur privé. Pour résoudre ce problème, il est conseillé aux États membres de la CEDEAO de collaborer avec les universités en vue d'élaborer des programmes de formations et de stage qui peuvent servir de pipeline pour attirer au sein du gouvernement des talents sans expérience, mais qui possèdent des compétences techniques. Il est également recommandé que les États membres collaborent avec le secteur privé pour développer des programmes dans lesquels des experts chevronnés du secteur privé peuvent accomplir un travail temporaire au sein du CSIRT national et des entités gouvernementales/des infrastructures critiques pour accompagner et former les employés moins expérimentés et moins techniques.

RECOMMANDATION :
Veiller à ce que les employés de chaque CSIRT national et des spécialistes de la défense réseau dans les systèmes gouvernementaux et d'infrastructures critiques possèdent des compétences techniques adéquates pour pouvoir sécuriser et défendre efficacement les réseaux de la nation. Les États membres de la CEDEAO doivent collaborer avec les universités pour élaborer des programmes de formation et de stage qui peuvent servir de réserve de talents possédant des compétences techniques. Les États membres doivent également collaborer avec le secteur privé pour développer des programmes dans lesquels des experts chevronnés du secteur privé peuvent accomplir un travail temporaire, mais étendu au sein du CSIRT national et des entités gouvernementales/des infrastructures critiques pour accompagner et former les employés moins expérimentés et moins techniques.

2.6// Formations et renforcement des capacités

Il est également possible de combler le manque d'expertise technique interne par des services d'assistance, de formation et de renforcement des capacités qui sont souvent à disposition dans le cadre de projets formels financés par les ministères des Affaires étrangères (y compris le Bureau fédéral allemand des Affaires étrangères et l'Agence allemande de coopération internationale [GIZ], ainsi que le ministère britannique des Affaires étrangères, du Commonwealth et du Développement) et des entités privées (dont Microsoft et Google), ainsi que par la Banque mondiale, les Nations Unies et l'Union européenne, entre autres entités.

Par exemple, outre le projet actuel de la CEDEAO financé par le Bureau fédéral allemand des Affaires étrangères et mis en œuvre par la GIZ, le ministère britannique des Affaires étrangères, du Commonwealth et du Développement (FCDO britannique) dirige de nombreux projets de renforcement des cyber-capacités en Afrique, notamment des projets avec Shadowserver.

Un grand nombre de projets de renforcement des cyber-capacités comprennent des opportunités de formation en personne et à distance. Par exemple, en novembre 2024, Shadowserver s'est associée avec FIRST pour dispenser une formation d'une journée complète intitulée « Getting the Most Out of Free Shadowserver Daily Feeds and Other Community Services via Automation » (Mettre pleinement à profit les flux de données quotidiens de Shadowserver et d'autres services communautaires grâce à l'automatisation) lors du symposium de FIRST et AfricaCERT : régions Afrique et des États arabes à Livingston en Zambie.

RECOMMANDATION :
Rechercher les opportunités existantes en matière de projets de formation et de renforcement des capacités (en particulier des projets opérationnels axés sur l'établissement et l'utilisation efficace de données, d'outils, de services et de plateformes gratuits/en open source). De tels projets sont souvent financés par les ministères des Affaires étrangères (y compris le Bureau fédéral allemand des Affaires étrangères et l'Agence allemande de coopération internationale [GIZ], ainsi que le ministère britannique des Affaires étrangères, du Commonwealth et du Développement) et des entités privées (dont Microsoft et Google), ainsi que par la Banque mondiale, les Nations Unies et l'Union européenne, entre autres entités.

2.7// Développement de partenariats

Il est également impératif que les CSIRT nationaux dans la région de la CEDEAO nouent des relations avec leurs membres/parties prenantes au sein de leurs pays respectifs (par ex. les fournisseurs d'accès à Internet, les prestataires de services de télécommunications, les infrastructures critiques et d'autres propriétaires de réseau de grande envergure), ainsi qu'avec des CSIRT homologues nationaux de la région de la CEDEAO et dans le reste du monde. Ces relations sont essentielles pour établir un environnement qui favorise la collaboration et le partage d'informations. Par exemple, des relations de travail étroites avec les membres/parties prenantes dans son pays permettent à un CSIRT national de diffuser rapidement des alertes sur les menaces à la sécurité ciblant des actifs vulnérables et compromis aux propriétaires de réseau afin que ces derniers puissent procéder à des corrections et à une remédiation avant que les acteurs malveillants puissent exploiter ces actifs.

Des relations solides avec les CSIRT homologues nationaux sont également importantes, car elles promeuvent le partage d'informations, la collaboration et le renforcement des capacités. Les opportunités en matière d'établissement de telles relations professionnelles sont nombreuses. Par exemple, Shadowserver propose aux CSIRT nationaux un accès gratuit à sa plateforme de discussion en ligne Alliance Mattermost, où le personnel de Shadowserver, les partenaires de l'Alliance de l'ensemble du secteur et des CSIRT nationaux du monde entier partagent et reçoivent les dernières informations sur les renseignements liés aux menaces et travaillent de manière collaborative pour s'attaquer aux nouvelles menaces.

Les CSIRT nationaux doivent également s'efforcer d'adhérer à FIRST, le forum mondial des Centres de réponse aux incidents de sécurité informatique. FIRST est une éminente organisation de membres pour les CSIRT nationaux en matière de réponse aux incidents et de la sécurité. L'adhésion à FIRST permet aux Centres de réponse aux incidents de mieux intervenir dans le cadre d'incidents de sécurité. FIRST regroupe un éventail de Centres de réponse aux incidents de sécurité informatique provenant d'organisations gouvernementales, commerciales et éducatives. Il vise à favoriser la coopération et la coordination dans la prévention des incidents, à simuler une réaction rapide face aux incidents et à promouvoir le partage d'informations entre les membres et dans l'ensemble de la communauté. En dehors du réseau de confiance qu'il propose au sein de la communauté mondiale de réponse aux incidents, FIRST offre également un certain nombre de services aux CSIRT nationaux. Actuellement, FIRST comporte plus de 800 membres disséminés à travers l'Afrique, les Amériques, l'Asie, l'Europe et l'Océanie. Comme le montre la Figure 4 ci-dessous, parmi les pays de la CEDEAO, seuls le Bénin, le Ghana, la Côte d'Ivoire, le Nigeria et Togo disposent des CSIRT nationaux qui sont membres de FIRST.

RECOMMANDATION :

Créer un cadre nécessitant que les CSIRT nationaux établissent et entretiennent des relations professionnelles solides avec leurs membres/parties prenantes dans leurs pays respectifs (notamment les fournisseurs d'accès à Internet, les opérateurs d'infrastructures critiques, les entités gouvernementales, les entreprises, les universités, les gouvernements étatiques et locaux, les prestataires de soins de santé, les institutions financières, etc.), ainsi qu'avec les autres CSIRT nationaux de la région de la CEDEAO et du reste du monde. Ces relations sont essentielles pour favoriser le partage d'informations, la collaboration et le renforcement des capacités. Les opportunités permettant aux CSIRT nationaux d'établir des partenariats mondiaux

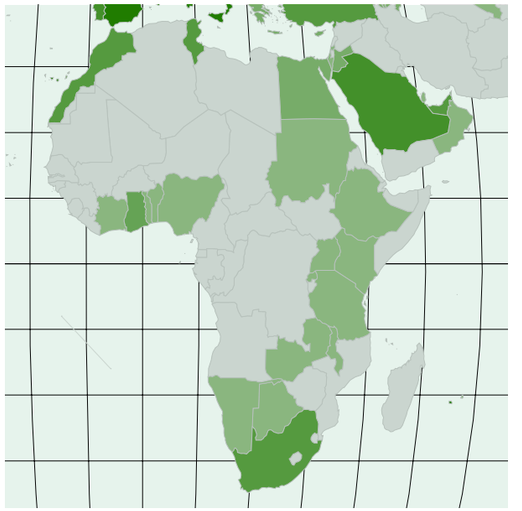


Figure 04. **Carte des nations africaines dont les CSIRT nationaux sont actuellement membres de FIRST**

comprennent le recours à un ISAC de la CEDEAO, en devenant membre de FIRST.org et en rejoignant la plateforme de discussion gratuite Alliance Mattermost de Shadowserver, qui facilite un accès direct au personnel de Shadowserver, aux partenaires de l'Alliance issus de l'ensemble de l'industrie et aux CSIRT nationaux du monde entier.

2.8// Évaluations de la maturité

Pour contribuer à son développement, chaque CSIRT national doit disposer d'une évaluation de référence de son niveau de maturité. L'Open CSIRT Foundation a créé le modèle de maturité dans la gestion des incidents de sécurité (SIM3) sous forme de cadre aidant les organisations à mesurer et à améliorer les fonctions de leur centre de réponse aux incidents de cybersécurité. Ce modèle évalue les centres sur un ensemble de 44 paramètres, dans quatre domaines clés : organisation, ressources humaines, outils et processus. Il détermine ensuite un niveau de maturité sur une échelle de 0 (non disponible : à savoir que la capacité est inexistante) à 4 (audit explicit : à savoir que les capacités sont formalisées, auditées régulièrement et continuellement améliorées dans le cadre d'une gouvernance formelle). L'Open CSIRT Foundation a développé un outil d'autoévaluation SIM3 en ligne pour tous les types de CSIRT.

RECOMMANDATION :
Pour établir un niveau de maturité de référence, chaque CSIRT national est tenu de se soumettre à l'outil d'autoévaluation en ligne (SIM3) du modèle de maturité de la gestion des incidents de sécurité de l'Open CSIRT Foundation et de mettre en œuvre les mesures recommandées en matière d'amélioration.

2.9// Services d'alerte précoce

Les entreprises et d'autres propriétaires de réseau à l'échelle d'un pays peuvent ne pas savoir que des données quotidiennes gratuites sur les cybermenaces sont à leur disposition directement auprès d'organisations de cybersécurité comme Shadowserver pour les aider à sécuriser leurs réseaux. Pour surmonter ce problème, les CSIRT nationaux, les CSIRT sectoriels, les ISAC et les autres entités comportant beaucoup de membres peuvent élaborer et faire connaître leurs propres services d'alerte précoce en utilisant les données gratuites de Shadowserver sur les cybermenaces (sous forme de rapports de remédiation de réseau) et les données sur les menaces disponibles auprès d'autres sources. Les organisations de membres fournissent leurs adresses IP publiques et leurs noms de domaine au CSIRT national (ou à une autre autorité compétente). En échange, elles reçoivent des avis d'alerte automatisés au sujet des appareils et des services qui sont exposés, vulnérables et compromis sur leur réseau pour faciliter une remédiation rapide, un peu comme si elles étaient abonnées aux rapports de Shadowserver. Les entités proposant des types de services sont nombreuses, par exemple les services d'alerte précoce (Early Warning Services) proposés par le Centre national de la cybersécurité du Royaume-Uni (UK NCSC) et ceux du CSIRT-RD de la Dominique républicaine.

RECOMMANDATION :
Les CSIRT nationaux, les CSIRT sectoriels, les ISAC et les autres entités comportant un grand nombre de membres doivent être chargés de proposer des services d'alerte précoce gratuits à leurs membres, sur la base des données gratuites de Shadowserver et d'autres sources disponibles sur les cybermenaces. Les organisations de membres fournissent leurs adresses IP publiques et leurs noms de domaine et, en échange, elles reçoivent des avis d'alerte automatisés au sujet des appareils et des services qui sont exposés, mal configurés, exploitables, vulnérables et compromis sur leurs réseaux pour faciliter une remédiation rapide. Il est recommandé de consulter l'un des nombreux CSIRT nationaux qui fournissent de tels services d'alerte précoce, comme le Centre national britannique de la cybersécurité (UK NCSC) et le CSIRT-RD de la République dominicaine.

3.0// Lacunes opérationnelles en termes de cybersécurité et recommandations : la Surface d'Attaque de la Région de la CEDEAO

Une « **surface d'attaque*** » désigne tous les points faibles, ou vecteurs d'attaque possibles qu'un acteur malveillant peut exploiter pour accéder sans autorisation à un système ou un réseau. Bien que certains vecteurs d'attaque dépendent d'erreurs humaines (par ex., **hameçonnage***, ingénierie sociale), un grand nombre reposent sur des déficiences techniques dans un réseau (par ex. actifs mal configurés et exposés ; **vulnérabilités* non corrigées** ; **vulnérabilités jour zéro*** ; **actifs compromis*** ; etc.)

Shadowserver recueille et analyse d'importants volumes de données sur les cybermenaces à l'échelle d'Internet en utilisant divers moyens techniques, qui sont expliqués ci-dessous. Shadowserver partage ensuite gratuitement des données au quotidien avec plus de 9 000 organisations et propriétaires de réseau du monde entier (c'est-à-dire, des hôpitaux, des universités et des circonscriptions scolaires, des organisations à but non lucratif et non gouvernementales, des gouvernements fédéraux/étatiques/locaux, des petites et moyennes entreprises, des entreprises du classement Fortune 500, des fournisseurs d'accès à Internet, des institutions financières, des fournisseurs d'infrastructures critiques, et beaucoup d'autres entités). De plus, Shadowserver fournit chaque jour des données gratuites et étendues sur les menaces à l'échelle nationale aux Centres nationaux de réponse aux incidents de sécurité informatique (CSIRT nationaux) assumant des responsabilités spécifiques en termes de prévention et de réponse aux incidents dans 175 pays, notamment en Afrique et, plus particulièrement dans le cadre du présent rapport, dans un grand nombre d'États membres de la SEDEAO.

Shadowserver partage les données sur les menaces sous forme de rapports de remédiation de réseau. Ces rapports servent à la fois de services d'alerte précoce, en identifiant les appareils exposés, mal configurés et vulnérables qu'il faut corriger sur un réseau avant que des acteurs malveillants puissent s'y infiltrer, et un service d'information aux victimes, en identifiant les appareils compromis sur un réseau qu'il faut corriger avant qu'ils soient exploités davantage, par exemple dans le cadre d'une attaque par logiciel rançonneur. Les données recueillies peuvent contribuer à clarifier l'étendue de la surface d'attaque de la région de la CEDEAO.

3.1// Données de balayage

Shadowserver effectue quotidiennement un balayage de ports plus de 150 fois pour identifier des **adresses de protocole Internet (IP)*** publiquement exposées/assignables, à savoir, environ 3,7 milliards d'adresses IPv4 et les listes d'occurrences d'approximativement deux milliards d'adresses IPv6 observées sur la toile. Les données de balayage sont utilisées pour informer les CSIRT nationaux et les propriétaires de réseau dans l'ensemble des secteurs au sujet d'appareils exposés, exploitables, mal configurés, vulnérables et parfois compromis qu'il faut corriger ou sinon réparer avant que des acteurs malveillants les exploitent (ou les exploitent davantage).

Les acteurs malveillants procèdent souvent à leur propre balayage ou achètent des données de balayage auprès de fournisseurs commerciaux pour identifier les réseaux à cibler en vue de les attaquer. En conséquence, les données de balayage gratuites de Shadowserver constituent un outil essentiel qui permet aux CSIRT nationaux et aux propriétaires de réseau de déterminer ce que les acteurs malveillants peuvent voir au sujet de leurs réseaux, notamment les moyens permettant d'y accéder sans autorisation et, potentiellement, de les exploiter.

Une analyse des **données de balayage** de Shadowserver est utile pour identifier les éléments suivants :

a les appareils et les services qui sont (parfois inutilement) publiquement exposés sur Internet, ce qui étend inutilement leur surface d'attaque

b les vulnérabilités critiques dans des actifs exposés

c les actifs exposés qui sont compromis

3.1a// APPAREILS ET SERVICES PUBLIQUEMENT EXPOSÉS SUR INTERNET

Les appareils* et **les services*** publiquement exposés sur Internet sont des vecteurs d'attaque courants pour les acteurs malveillants qui cherchent à infiltrer un réseau. Pourtant, de nombreux propriétaires de réseau ne connaissent pas pleinement tous les actifs sur leurs réseaux, car ils n'en tiennent pas un inventaire à jour.

La conduite d'un **inventaire des actifs*** est essentielle pour comprendre l'étendue d'une surface d'attaque et améliorer la cyber-résilience, en couvrant deux objectifs clés :

1. Un tel inventaire permet à un propriétaire de réseau de connaître le fournisseur, le type, le modèle et l'emplacement des appareils exposés sur un réseau, ce qui facilite ensuite une correction et une remédiation rapides en cas de découverte et d'annonce publique de nouvelles vulnérabilités dans ces appareils et dans les logiciels associés.
2. Il permet aux propriétaires de réseau de réduire leur surface d'attaque globale en apportant des correctifs sur les appareils et les services qui sont inutilement exposés sur Internet.

Des conseils utiles sur la mise en œuvre des réglementations qui imposent aux agences gouvernementales fédérales la conduite d'inventaires des actifs figurent dans la « Directive opérationnelle contraignante 23-01 : améliorer la visibilité des actifs et la détection des vulnérabilités sur les réseaux fédéraux » supervisée par l'Agence de cybersécurité et de sécurité des infrastructures du Département américain de la sécurité intérieure (DHS-CISA). Cette directive exige que les branches, les départements et les agences aux niveau fédéral et exécutif procèdent, entre autres mesures, à une découverte automatisée (un inventaire) des actifs tous les 7 jours. Elle exige également qu'ils lancent un processus de recensement des vulnérabilités dans tous les actifs découverts, notamment les appareils nomades/en itinérance (par ex. des ordinateurs portables) découverts, tous les 14 jours.

Lacunes opérationnelles en termes de cybersécurité et recommandations : la Surface d'Attaque de la Région de la CEDEAO

Shadowserver gère une fonction d'empreintes de détection pour les *appareils* exposés qui ont été identifiés dans la région de la CEDEAO, dans le cadre de notre balayage quotidien de l'Internet. Cela comprend l'identification du fournisseur, du type et du modèle d'appareil publiquement exposé.

Comme le montre la Figure 05, le Nigeria, la Côte d'Ivoire et le Ghana affichent le plus haut volume d'appareils exposés dans la région de la CEDEAO, ce qui corrèle avec la taille de leurs infrastructures IP respectives.

Le graphique à barres dans la Figure 06 présente les 20 principaux

Figure 05. **Volume d'identifications d'appareils par pays de la CEDEAO** (résultats moyens des balayages quotidiens entre le 1er octobre 2024 et le 24 avril 2025)

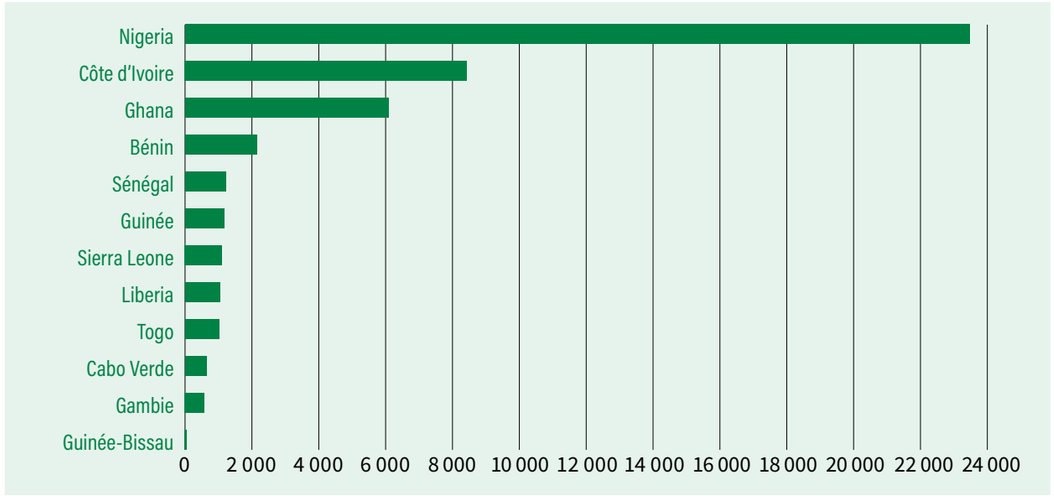
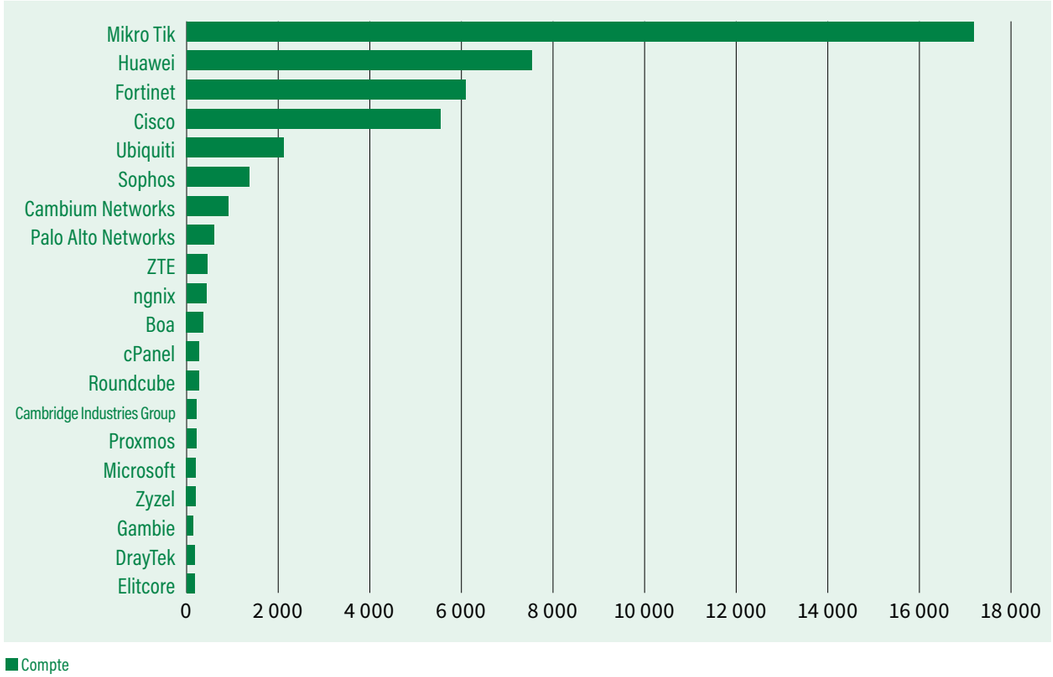


Figure 06. **20 principaux fournisseurs d'appareils dans la région de la CEDEAO** (résultats moyens des balayages quotidiens)



fournisseurs par volume qui ont été identifiés dans la région de la CEDEAO, notamment des fournisseurs bien connus tels que Huawei, Fortinet, MikroTik et Cisco.

S'agissant du premier fournisseur par volume, c'est de loin le routeur grand public de MikroTik que les consommateurs choisissent le plus dans la région de la CEDEAO. L'importance de ce résultat en termes de surface d'attaque est que plusieurs vulnérabilités critiques et de sévérité élevée ont été identifiées et exploitées dans des appareils MikroTik. La possibilité de déterminer si ces appareils sont sur un réseau et où, dans le cadre d'un

inventaire des actifs, est essentielle pour corriger rapidement de nouvelles vulnérabilités identifiées.

Les **routeurs*** font partie des appareils que les acteurs malveillants ciblent le plus, car ils sont généralement les gardiens des réseaux des utilisateurs, ils sont toujours connectés à Internet (et donc faciles à découvrir), leurs identifiants d'utilisateur sont souvent la valeur par défaut ou d'un niveau de sécurité faible, et leurs vulnérabilités sont rarement corrigées. Une fois exploités, ces appareils sont souvent intégrés dans de vastes réseaux zombie et utilisés pour diverses activités malveillantes telles que des attaques par DDoS, la distribution de logiciels malveillants, le vol de données et des campagnes de hameçonnage.

Shadowserver peut cartographier les appareils exposés et dont les empreintes ont été relevées, notamment les routeurs, dans la région de la CEDEAO, en les ventilant par type d'appareil. Bien que certains types d'appareils, comme des **pare-feux*** et des **services de VPN***, soient souvent exposés à l'Internet public dans le cadre de leurs fonctions centrales, il est généralement inutile que les routeurs et d'autres appareils spécifiques soient exposés.

Un bon exemple illustrant les dangers liés à l'exposition inutile d'actifs à Internet est le piratage des réseaux d'infrastructures critiques que CyberAv3ngers, un groupe de piratage affilié au Corps des Gardiens de la Révolution islamique (IRGC), a démarré en novembre 2023. Entre novembre 2023 et janvier 2024, CyberAv3ngers est parvenu à compromettre au moins 75 automates programmables Unitronics fabriqués en Israël et utilisés dans une multitude de secteurs aux infrastructures critiques, notamment les secteurs de l'eau et des eaux usées. Il s'agissait d'appareils à technologie opérationnelle qui étaient inutilement exposés au public sur Internet, soit avec un mot de passe par défaut, soit sans aucun mot de passe[20]. La plus impressionnante de ces attaques a été contre l'autorité de traitement des eaux municipales d'Aliquippa, une petite communauté de l'ouest de la Pennsylvanie[21]. Ces attaques ont fait ressortir le niveau de vulnérabilité des réseaux comportant des infrastructures critiques face à des cyberattaques et le préjudice potentiel pour le public en cas de violation de la sécurité de tels systèmes.

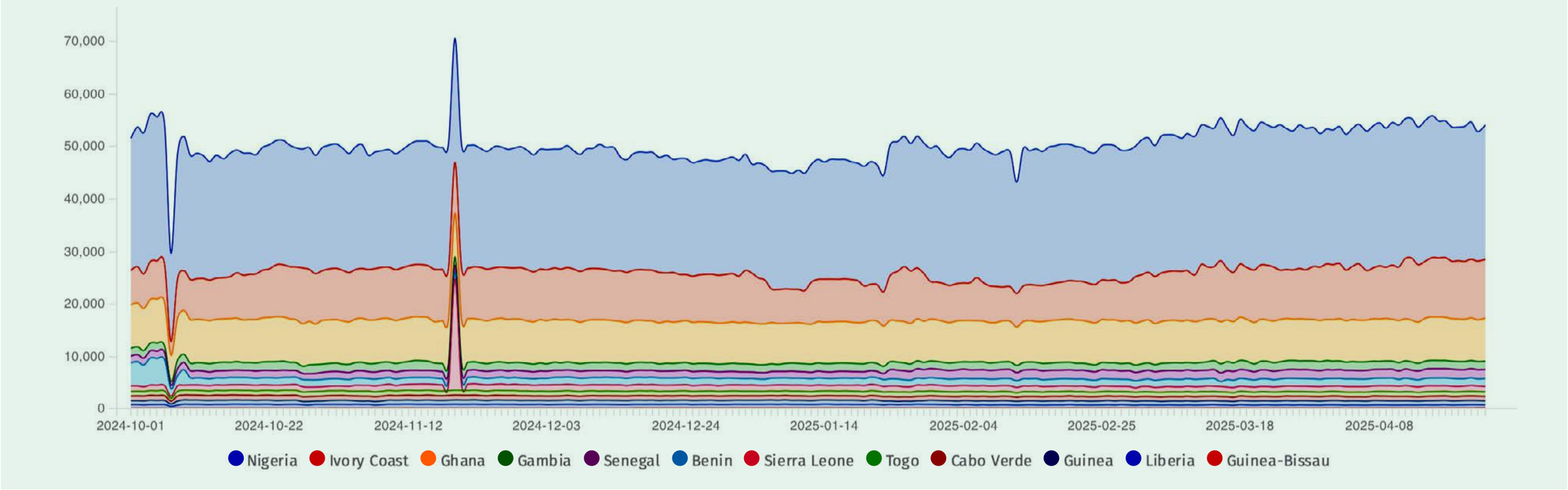
Les réseaux aux infrastructures critiques sont de plus en plus la cible de cyberattaques perpétrées par des acteurs malveillants. Ces attaques peuvent aboutir à des préjudices sociétaux majeurs si des éléments comme la distribution d'eau, l'alimentation en électricité et les services de santé sont perturbés, voire compromis. En conséquence, il est important de veiller à ce que les actifs ne soient pas inutilement exposés à l'Internet public pour sécuriser un réseau et réduire la surface d'attaque.

Shadowserver partage avec les CSIRT nationaux et les propriétaires de réseau des données qui sont exploitables, détaillées et spécifiques aux adresses IP d'appareils exposés sur un réseau/dans un groupe de membres, par le biais du rapport d'Identification des appareils.

[20] « IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, including US Water and Wastewater Systems Facilities », *Bulletin de cybersécurité, Agence pour la cybersécurité et la sécurité des infrastructures*, 18 décembre 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

[21] « Iran-linked Cyberattacks Threaten Equipment Used in U.S. Water Systems and Factories », *NPR*, 2 décembre 2023. https://www.npr.org/2023/12/02/1216735250/iran-linked-cyberattacks-israeli-equipment-water-plants

Figure 07. **Cas d'applications côté serveur exposées par pays de la région de la CEDEAO**

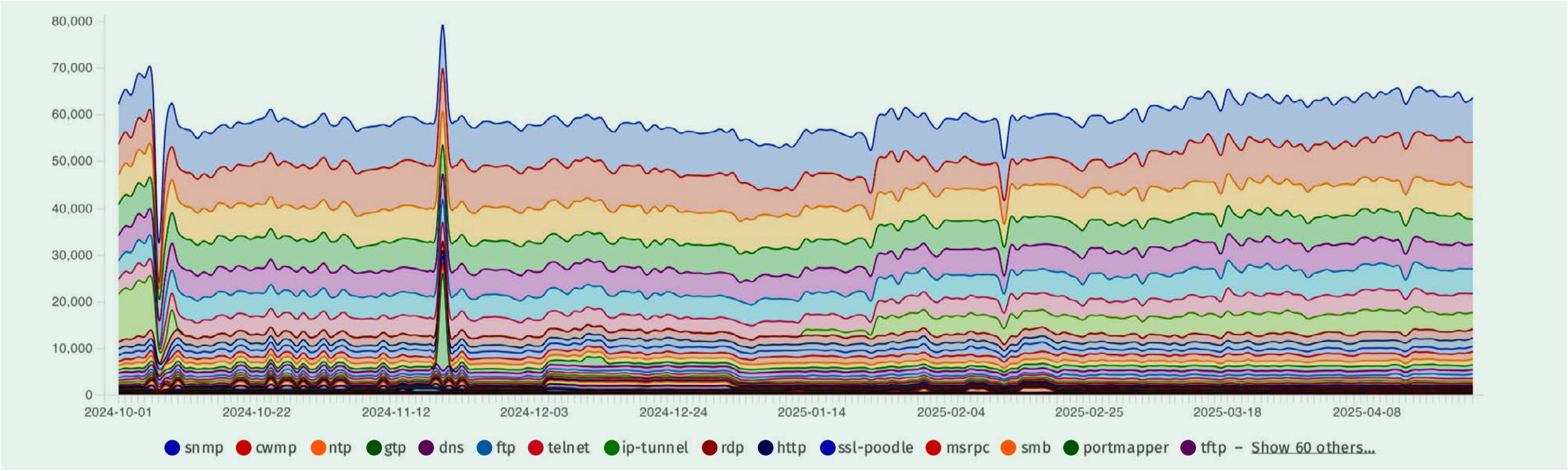


The items at the bottom of each graph are arranged left to right in descending order in which they appear on the graph.

Outre les appareils publiquement exposés, les **services*/applications côté serveur*** qui sont publiquement exposés sur Internet sont également une source de préoccupation et contribuent à une surface d'attaque globale. La Figure 07 présente des cas de services exposés par pays de la région de la CEDEAO, où le Nigeria, la Côte d'Ivoire et le Ghana occupent les trois premières places. Ces services exposés sont considérés comme problématiques, car ils sont mal configurés, exploitables ou inutilement accessibles depuis l'Internet public, faisant d'eux des cibles prioritaires pour les acteurs malveillants qui cherchent à s'infiltrer dans des réseaux.

Lacunes opérationnelles en termes de cybersécurité et recommandations : la Surface d'Attaque de la Région de la CEDEAO

Figure 08. **Cas d'applications côté serveur exposées par type de balayage dans la région de la CEDEAO**



The items at the bottom of each graph are arranged left to right in descending order in which they appear on the graph.

La Figure 08 indique que le **SNMP (protocole simple de gestion de réseau*)** est le service le plus exposé à Internet dans la région de la CEDEAO. Le protocole SNMP joue un rôle essentiel dans la surveillance, la gestion et la sécurisation des appareils en réseau. Il permet aux administrateurs de réseau de recueillir des informations, de configurer des appareils et de répondre à distance à des événements survenant sur le réseau, ce qui en fait un outil essentiel pour maintenir la performance et la sécurité d'un réseau.

Un grand nombre d'appareils exposés contiennent des vulnérabilités que des acteurs malveillants peuvent exploiter. Par exemple, des services de SNMP exposés dans certains routeurs Cisco contiennent une vulnérabilité appelée CVE-2017-6742. En avril 2023, un Bulletin de cybersécurité (CSA) délivré par les agences de sécurité américaine et britannique a révélé que des pirates de l'unité de renseignements militaires 26165 de la direction générale des renseignements de la Russie (appelée APT28, Fancy Bear et Sofacy, entre autres) ont exploité cette vulnérabilité pour explorer les routeurs et déployer des logiciels malveillants[22].

[22] « Advisory: APT28 Exploits Known Vulnerability to Carry Out Reconnaissance and Deploy Malware on Cisco Router », *Centre national de la cybersécurité, Royaume-Uni*, 18 avril 2023. https://www.cisa.gov/sites/default/files/2023-04/apt28-exploits-known-vulnerability-to-carry-out-reconnaissance-and-deploy-malware-on-cisco-routers.pdf

Ces exemples soulignent la menace potentielle que posent les appareils et les services exposés, que des acteurs malveillants, y compris des pirates d'États-nations, peuvent exploiter.

RECOMMANDATIONS :

Établir des politiques imposant la conduite régulière d'inventaires d'actifs*, particulièrement au sein du gouvernement et des secteurs comportant des infrastructures critiques. Cela aidera les propriétaires de réseau à appliquer rapidement des correctifs, ainsi que dans leurs efforts de remédiation à mesure que de nouvelles vulnérabilités critiques se présentent. Des conseils utiles sur la mise en œuvre des réglementations qui imposent aux agences gouvernementales fédérales la conduite d'inventaires des actifs figurent dans la « Directive opérationnelle contraignante 23-01 : améliorer la visibilité des actifs et la détection des vulnérabilités sur les réseaux fédéraux » supervisée par l'Agence de cybersécurité et de sécurité des infrastructures du Département américain de la sécurité intérieure (DHS-CISA).

S'assurer que les propriétaires de réseau (en particulier, les infrastructures critiques, les gouvernements et les fournisseurs d'accès à Internet de grande envergure) n'exposent pas inutilement certains types d'appareils (y compris des appareils à technologie opérationnelle et d'autres types précités) et de services (y compris SNMP) à l'Internet public, sauf si cela est nécessaire pour des raisons de fonctionnalité. Cette mesure permettra de réduire la surface d'attaque globale de la région. La conduite de formations et d'ateliers dédiés avec les CSIRT nationaux, les fournisseurs d'accès à Internet et d'autres propriétaires de réseau dans la région de la CEDEAO pourrait aboutir à des activités proactives renforcées visant à cibler et à réduire les cas d'exposition inutile d'appareils et de services.

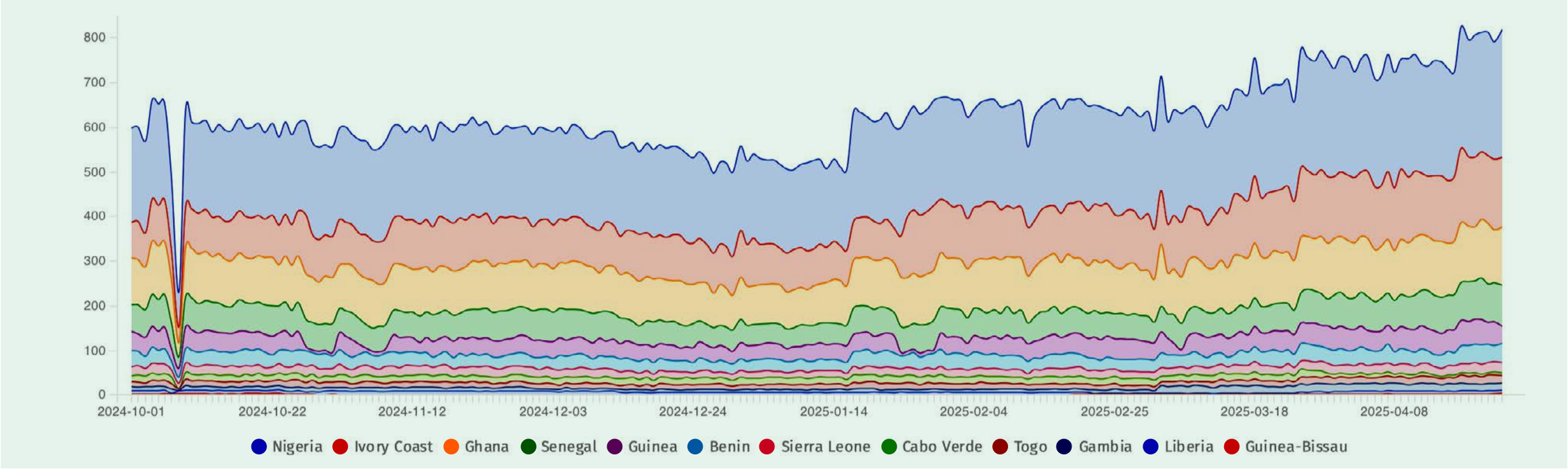
3.1b// VULNÉRABILITÉS CRITIQUES DANS DES ACTIFS EXPOSÉS

Les acteurs malveillants continuent principalement d'exploiter des vulnérabilités non corrigées pour s'introduire dans des réseaux et causer des préjudices, notamment au moyen d'attaques par logiciel rançonneur et par DDoS. Dans le cadre de ses activités principales, Shadowserver balayage l'Internet à la recherche de cas de **vulnérabilités et expositions courantes (CVEs)*** critiques et de sévérité élevée dans les appareils et les logiciels. Shadowserver alerte ensuite les propriétaires de réseau et les CSIRT nationaux au sujet des vulnérabilités dans leurs réseaux qui doivent être corrigées avant que des acteurs malveillants puissent les exploiter, s'y infiltrer et causer d'autres préjudices.

Dans un exemple récent, des vulnérabilités non corrigées dans un logiciel de partage d'informations et de collaboration SharePoint de Microsoft, appelé « ToolShell », ont été exploitées en juin 2025 par des acteurs malveillants qui ont ciblé au moins une demi-douzaine d'entités en Afrique du Sud, notamment le Trésor public, une organisation du secteur de la construction automobile, une université, plusieurs entités de gouvernements locaux et une entité du gouvernement fédéral[23].

[23] « African Orgs Fall to Mass Microsoft SharePoint Exploits » *DarkReading*, 30 juillet 2025. https://www.darkreading.com/cyber-risk/african-orgs-mass-microsoft-sharepoint-exploits

Figure 09. **CVE critiques détectées à distance dans des actifs exposés, par pays de la région de la CEDEAO**



The items at the bottom of each graph are arranged left to right in descending order in which they appear on the graph.

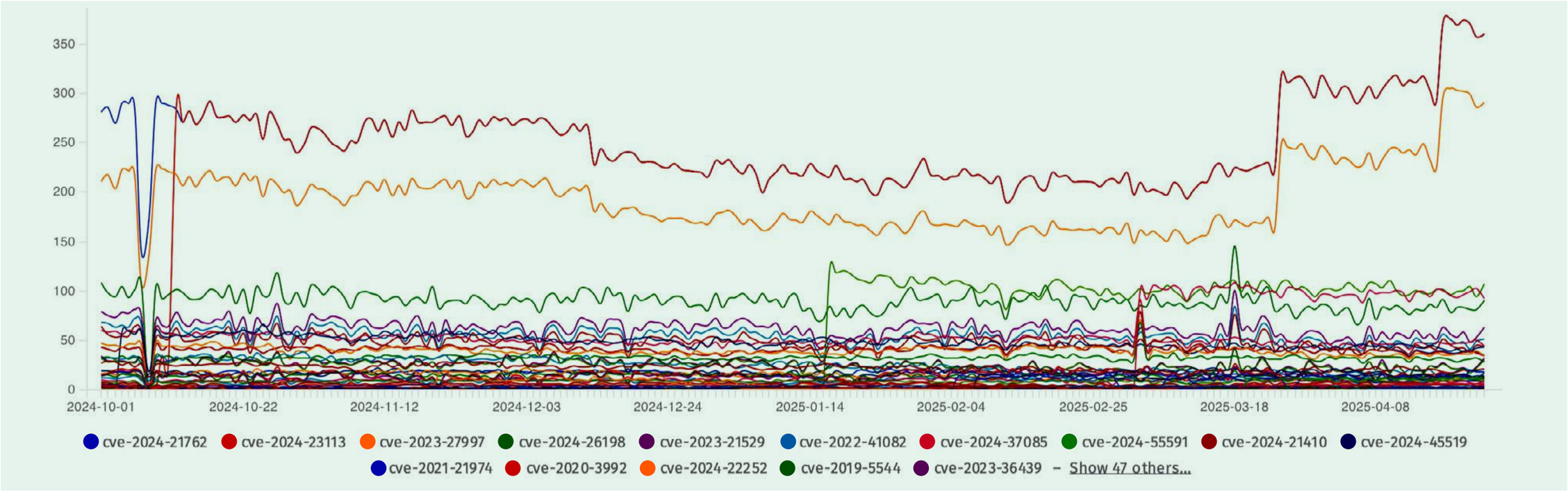
Comme le montre la Figure 09, les balayages quotidiens de Shadowserver font ressortir un nombre modeste de vulnérabilités critiques présentes dans des infrastructures exposées au sein de la région de la CEDEAO, les pays où les nombres sont les plus élevés étant le Nigeria, la Côte d'Ivoire et le Ghana. Malheureusement, ces vulnérabilités peuvent être exploitées à tout moment.

Comme le montre la Figure 10, il y a plusieurs vulnérabilités inquiétantes liées à des CVE critiques dans la région de la CEDEAO. Par exemple, la CVE-2024-23113 est une vulnérabilité critique dans Fortinet FortiOS qui, si elle est exploitée, pourrait permettre à un pirate non authentifié d'exécuter à distance un code ou des commandes arbitraire(s) sur un système[24]. Peu après l'annonce de la vulnérabilité en octobre 2024, Shadowserver a identifié plus de 87 000 adresses IP Fortinet probablement vulnérables à la

[24] « Critical CVE in 4 Fortinet Products Actively Exploited », *Cybersecurity Dive*, 14 octobre 2024. https://www.cybersecuritydive.com/news/critical-cve-fortinet-exploited/729736/

Lacunes opérationnelles en termes de cybersécurité et recommandations : la Surface d'Attaque de la Région de la CEDEAO

Figure 10. **CVE critiques détectées à distance dans des actifs exposés au sein de la région de la CEDEAO**



The items at the bottom of each graph are arranged left to right in descending order in which they appear on the graph.

CVE-2024-23113[25]. Par ailleurs, à la même époque, l'Agence de la cybersécurité et de la sécurité des infrastructures du Département américain de la sécurité intérieure (DHS-CISA ou « CISA ») a ajouté la CVE-2024-23113 à son catalogue de vulnérabilités connues, ce qui signifie que des acteurs malveillants exploitaient activement la CVE sur la toile et que les agences du gouvernement américain doivent la corriger en priorité[26].

Les vulnérabilités non corrigées fournissent aux acteurs malveillants des vecteurs d'attaque pour accéder sans autorisation à des réseaux. Les vulnérabilités pour lesquelles on a observé qu'elles étaient activement exploitées sur la toile (également appelées des « **vulnérabilités exploitées connues*** ») suscitent des préoccupations particulières et doivent faire l'objet d'une remédiation immédiate en priorité. La correction des vulnérabilités, particulièrement celles dont la sévérité est critique et élevée et celles qui sont activement exploitées sur la toile, est essentielle pour renforcer la sécurité des infrastructures numériques et les agences gouvernementales et les infrastructures critiques doivent être tenues de la mettre en œuvre au cours d'une période bien définie.

[25] https://x.com/Shadowserver/status/1845478432479846737

[26] « Alert: CISA Adds Three Known Exploited Vulnerabilities to Catalog », *Agence de la cybersécurité et de la sécurité des infrastructures*, 9 octobre 2024. https://www.cisa.gov/news-events/alerts/2024/10/09/cisa-adds-three-known-exploited-vulnerabilities-catalog

Lacunes opérationnelles en termes de cybersécurité et recommandations : la Surface d'Attaque de la Région de la CEDEAO

Des conseils utiles figurent dans les « directives opérationnelles contraignantes (BODs) » que supervise la DHS-CISA. Ces BOD nécessitent que les branches, les départements et les agences aux niveaux fédéral et exécutif prennent certaines mesures pour protéger les informations fédérales et les systèmes d'information.

Par exemple, la directive « BOD 19-02 : Exigences en matière de remédiation des vulnérabilités pour les systèmes accessibles par Internet » exige notamment qu'à compter de leur identification initiale, les vulnérabilités critiques soient corrigées dans un délai de 15 jours civils, et les vulnérabilités élevées dans un délai de 30 jours civils. Si des vulnérabilités ne sont pas corrigées dans les délais spécifiés, la CISA soumettra aux points de contact de l'agence un plan de remédiation partiellement rempli identifiant toutes les vulnérabilités concernées qui restent à corriger, afin que l'agence le valide et le remplisse. L'agence renverra ensuite le plan de remédiation rempli à la CISA dans un délai de trois jours ouvrés à compter de la date de réception du plan, accompagné d'informations expliquant : (i) les contraintes rencontrées dans la remédiation des vulnérabilités ; (ii) les mesures d'atténuation provisoires destinées à surmonter ces contraintes ; et (iii) une estimation de la date d'achèvement de la remédiation des vulnérabilités.

De même, la directive « BOD 22-01: réduire le risque majeur des vulnérabilités exploitées connues » a été créée pour améliorer la BOD 19-02, sans pour autant la remplacer. La BOD 22-01 a établi un catalogue administré par la CISA recensant les vulnérabilités exploitées connues qui peuvent poser un risque important pour les activités fédérales. La BOD a également établi des exigences afin que les agences corrigent toutes les vulnérabilités figurant dans le catalogue dans le délai spécifié, à savoir 6 mois pour les vulnérabilités auxquelles un identifiant de vulnérabilités et expositions courantes (CVE) a été attribué avant 2021 et deux semaines pour toutes les autres vulnérabilités.

Quant à la question de savoir s'il est plus important de corriger les vulnérabilités critiques/élevées ou les vulnérabilités exploitées connues en premier, la CISA a expliqué que « les vulnérabilités exploitées connues doivent être la plus haute priorité en termes de remédiation. (…) La directive BOD 22-01 met l'accent sur les vulnérabilités qui sont des menaces actives ».[27]

RECOMMANDATIONS :

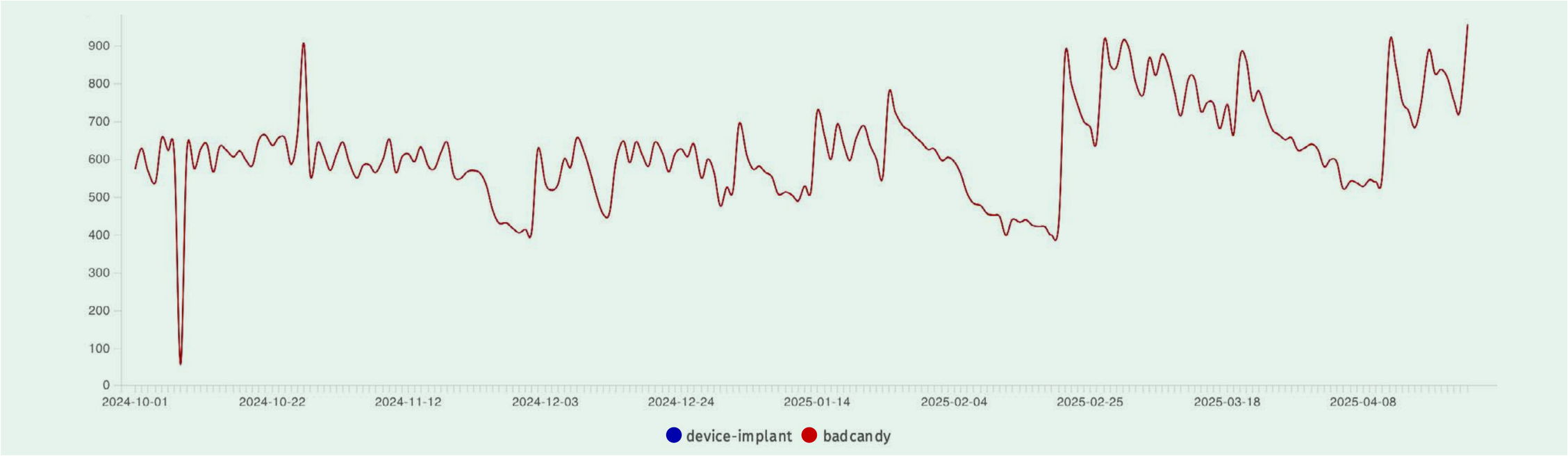
mettre en œuvre des réglementations qui nécessitent que les agences gouvernementales et les infrastructures critiques corrigent les vulnérabilités identifiées comme présentant un « risque critique » dans un délai de 15 jours civils et celles présentant un « risque élevé » dans un délai de 30 jours civils à compter de la date à laquelle elles ont été décelées. Des conseils utiles figurent, par exemple, dans la « Directive opérationnelle contraignante (BOD) 19-02 : exigences en termes de remédiation des vulnérabilités pour les systèmes accessibles par Internet » supervisée par l'Agence de cybersécurité et de sécurité des infrastructures du Département américain de la sécurité intérieure (DHS-CISA).

mettre en œuvre des réglementations qui nécessitent que le gouvernement et les infrastructures critiques corrigent les « vulnérabilités exploitées connues » dans un délai de 14 jours. La DHS-CISA tient un catalogue des vulnérabilités exploitées connues identifiant les vulnérabilités considérées comme activement exploitées sur la toile que les agences du gouvernement fédéral américain doivent immédiatement corriger. L'AESRI tient à jour un catalogue similaire – la Base de données des vulnérabilités de l'Union européenne. Enfin, le Tableau de bord public de Shadowserver tient une liste Shadowserver des vulnérabilités exploitées connues identifiées au travers de son réseau de leurres de détection. Des conseils utiles sur une telle réglementation figurent, par exemple, dans la « Directive opérationnelle contraignante (BOD) 22-01 : réduire le risque majeur des vulnérabilités exploitées connues » supervisée par la DHS-CISA.

[27] « BOD 22-01: réduire le risque majeur des vulnérabilités exploitées connues », *Agence de cybersécurité et de sécurité des infrastructures*, 3 novembre 2021. https://www.cisa.gov/news-events/directives/bod-22-01-reducing-significant-risk-known-exploited-vulnerabilities

Lacunes opérationnelles en termes de cybersécurité et recommandations : la Surface d'Attaque de la Région de la CEDEAO

Figure 11. **Appareils compromis dans l'ensemble de la région de la CEDEAO**



The items at the bottom of each graph are arranged left to right in descending order in which they appear on the graph.

3.1c// ACTIFS EXPOSÉS QUI SONT COMPROMIS

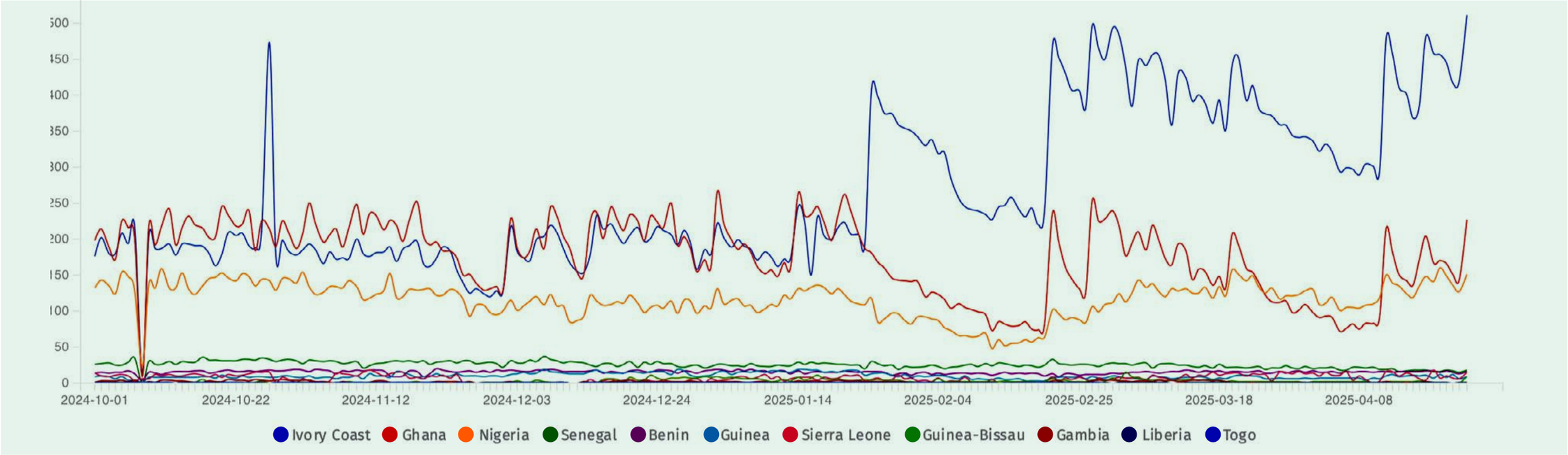
De plus, Shadowserver balaye continuellement les actifs de réseaux critiques qui ont été compromis par des acteurs malveillants lorsque des éléments factuels suffisants pour une détection sont disponibles. Cette procédure se fait principalement par un balayage non intrusif visant à rechercher certains éléments ou artefacts qui sont souvent installés sur un appareil une fois qu'il a été compromis (par ex. des **implants***, des **consoles Web malveillantes*** et des **injections de codes de vol d'authentifiants***).

Par exemple, fin 2023, le logiciel Cisco IOS XE a été compromis par ce que l'on appelle des implants « Bad Candy » – des **consoles Web malveillantes*** installées sur des milliers d'appareils du réseau Cisco connectés à Internet qui ont été exploitées par deux **vulnérabilités jour zéro***. [Une vulnérabilité jour zéro est une faille précédemment inconnue dans des logiciels, des équipements ou des micrologiciels que des attaquants peuvent exploiter avant que le fournisseur s'en rende compte et qu'il ait eu la possibilité de développer un correctif destiné à la corriger.] Ces attaques permettent aux acteurs malveillants d'exercer d'un contrôle administratif complet sur le système et, potentiellement, de surveiller le trafic sur le réseau, d'accéder à des réseaux protégés et de lancer divers types d'attaques[28].

[28] « Cisco's Critical IOS XE Software Zero Day is a 'Bad Situation' », *Cybersecurity Dive*, 17 octobre 2023. https://www.cybersecuritydive.com/news/ciscos-critical-ios-xe-zero-day/696791/

Lacunes opérationnelles en termes de cybersécurité et recommandations : la Surface d'Attaque de la Région de la CEDEAO

Figure 12. **Appareils compromis dans la région de la CEDEAO, par pays**



The items at the bottom of each graph are arranged left to right in descending order in which they appear on the graph.

Les résultats du balayage de Shadowserver indiquent qu'un grand nombre d'appareils Cisco IOS XE dans la région de la CEDEAO sont compromis avec des implants « Bad Candy ». La Figure 11 présente une moyenne de près 500 compromissions d'appareils Cisco IOS XE/liées à Bad Candy dans la région de la CEDEAO au cours de la période examinée. Cela constitue la majorité des appareils compromis détectés dans la région.

Il est intéressant de noter, comme le montre la Figure 12, que la plupart des compromissions liées à Bad Candy surviennent dans des réseaux en Côte d'Ivoire, avec des nombres bien plus élevés que dans les autres nations de la CEDEAO, notamment le Nigeria, qui possède le plus vaste espace d'adresses IPv4 dans la région.

Les appareils compromis, comme le Cisco IOS XE/Bad Candy, représentent des menaces majeures et peuvent faire l'objet d'une nouvelle exploitation à tout moment, avec des conséquences potentiellement graves, notamment des perturbations opérationnelles, des dommages sur le réseau, un vol de données, des attaques par logiciels rançonneurs et d'autres fondées sur des logiciels malveillants, un vol d'authentifiants, des dommages à la réputation et une mise en cause de la responsabilité juridique.

Shadowserver signale l'existence de divers types d'appareils compromis identifiés dans le cadre d'un balayage de détection d'implants installés par des attaquants. Les CSIRT nationaux et d'autres agences gouvernementales peuvent utiliser ces signalements, ainsi que les flux de données provenant

d'autres sources, pour élaborer des campagnes nationales visant à éliminer ces menaces et à sécuriser les appareils compromis.

Par exemple, l'Australian Signals Directorate (ASD) a mené une campagne nationale en vue d'éliminer les implants Bad Candy dans des appareils Cisco IOS XE compromis à travers l'Australie. Dans le cadre de cette campagne, les responsables de l'ASD ont envoyé des avis sur les victimes directement aux propriétaires de réseau concernés, ou à leur fournisseur de services s'il n'a pas été possible d'identifier le propriétaire de réseau. Les avis contenaient des instructions pour appliquer des correctifs, effectuer un redémarrage et répondre à des incidents survenus sur des appareils affectés, en vue de supprimer l'implant Bad Candy et d'atténuer le risque d'une nouvelle exploitation. L'ASD a ensuite surveillé la baisse générale du nombre d'appareils comportant un implant Bad Candy sur une période de plusieurs mois, à mesure que des ensembles d'avis en vrac étaient publiés.

RECOMMANDATIONS :

Mettre en œuvre des réglementations exigeant des CSIRT nationaux, des agences gouvernementales, des infrastructures critiques, des fournisseurs d'accès à Internet et des autres propriétaires de réseau dans la région qu'ils apportent des correctifs dans les appareils identifiés comme étant compromis dans un délai court, mais spécifique, notamment ceux identifiés dans les rapports de remédiation de réseau quotidiens gratuits de Shadowserver.

Imposer aux CSIRT nationaux, en coordination avec les fournisseurs d'accès à Internet, de concevoir et de mettre en œuvre des campagnes d'atténuation et d'élimination des menaces à l'échelle nationale contre les vulnérabilités critiques et les appareils compromis sur les réseaux dans l'ensemble du pays, et d'assurer un suivi de l'avancement des efforts de remédiation. Un exemple en est la campagne nationale dirigée par l'Australian Signals Directorate (ASD) en vue d'éliminer les implants « Bad Candy » dans des appareils Cisco IOS XE compromis dans l'ensemble de l'Australie.

3.2// Données « sinkhole »

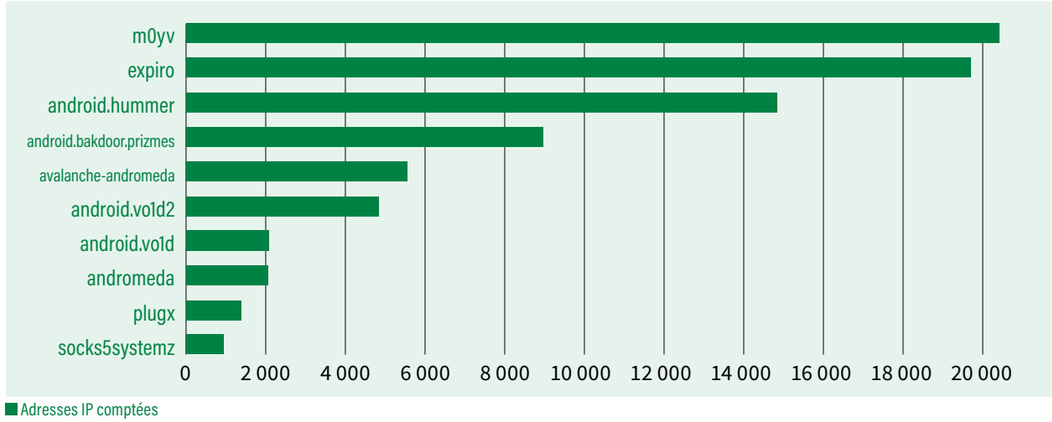
Shadowserver exploite une vaste infrastructure de « sinkholing » (engouffrement) de **systèmes de noms de domaine (DNS*)** lui permettant de recueillir des données sur les appareils de victimes infectés par les logiciels malveillants. « **Sinkholing*** » (engouffrement) est une technique consistant à perturber les communications entre les appareils de victimes infectés par des logiciels malveillants et des serveurs contrôlés de manière illicite avec lesquels les logiciels malveillants ordonnent aux appareils infectés de communiquer. Les communications, ou le trafic, sont ensuite redirigées vers des serveurs « sinkhole » (où les communications sont « engouffrées ») pour empêcher les criminels d'accéder aux appareils des victimes, de les contrôler et de communiquer avec. Shadowserver recueille l'adresse IP et d'autres informations d'identification associées aux appareils de victimes infectés par des logiciels malveillants qui communiquent avec les serveurs sinkhole. Les informations sont ensuite ajoutées dans les rapports de remédiation de réseau gratuits quotidiens de Shadowserver pour informer les CSIRT nationaux et les propriétaires de réseau abonnés au sujet des appareils infectés par un logiciel malveillant qui nécessitent une remédiation.

Cette perturbation se fait généralement en prenant le contrôle des domaines ou des adresses IP malveillant(e)s qui contrôlent les communications entre les appareils de victimes infectés par des logiciels malveillants et les infrastructures contrôlées par les criminels. Cela se fait souvent par le biais d'ordonnances de tribunaux pénaux ou civils signifiées à des **opérateurs de registre*** et des **registraires***, par une action volontaire d'opérateurs de registre et de registraires suite à la violation de conditions de services ou par l'achat des domaines malveillants qui ne sont pas encore enregistrés par les acteurs malveillants. Les domaines malveillants saisis sont souvent transférés au registraire en dernier recours (RoLR) de Shadowserver, un registraire de DNS à but non lucratif spécialement dédié qui a été créé pour assurer une mise en quarantaine à long terme des domaines malveillants, à titre gratuit (ou à un prix bas) en tant que service public.

Lacunes opérationnelles en termes de cybersécurité et recommandations : la Surface d'Attaque de la Région de la CEDEAO

Le « sinkholing » (engouffrement) est une technique importante pour garantir que les acteurs malveillants ne peuvent plus accéder aux appareils de victimes infectés par des logiciels malveillants et qu'ils ne peuvent plus les contrôler ni communiquer avec (à moins que d'autres types de logiciels malveillants non couverts par l'opération de sinkhole infectent également les appareils).

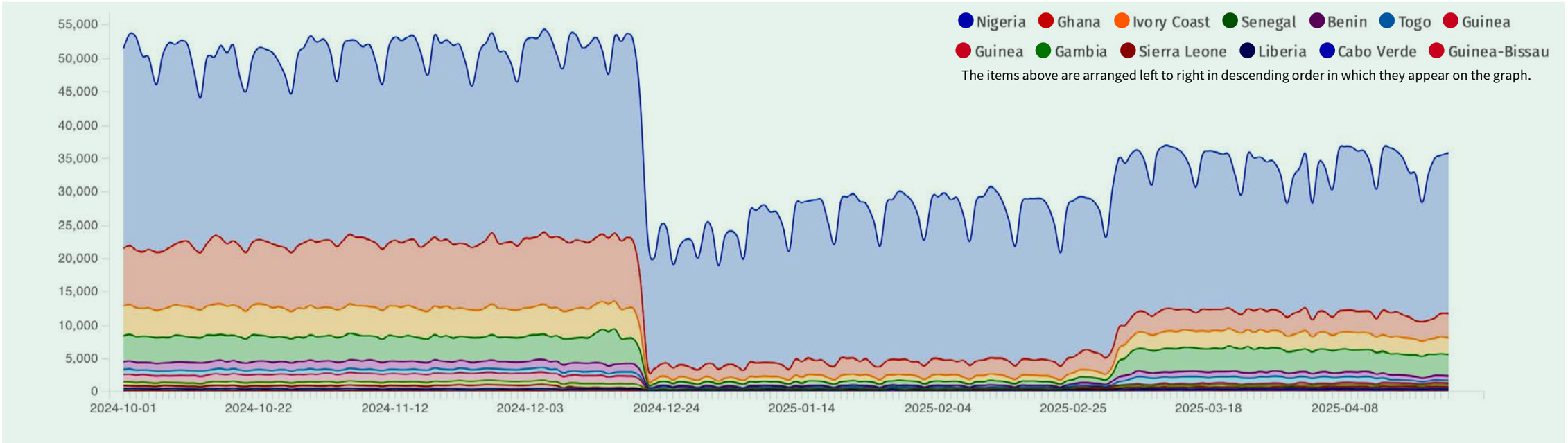
Figure 13. **10 principales infections sinkhole par type dans la région de la CEDEAO**



Selon les ensembles de données sur les infections sinkhole, le graphique à barres de la Figure 13 ci-dessous présente une moyenne de plus de 80 000 adresses IP complètes infectées chaque jour par un logiciel malveillant dans la région de la CEDEAO. En d'autres termes, plus de 80 000 appareils dont les adresses IP sont géolocalisées dans la région de la CEDEAO sont infectés par des logiciels malveillants et (à moins qu'ils soient infectés par d'autres types de logiciels malveillants n'ayant pas fait l'objet d'un sinkhole) étaient précédemment contrôlés par des acteurs malveillants avant d'être redirigés vers les serveurs sinkhole de Shadowserver.

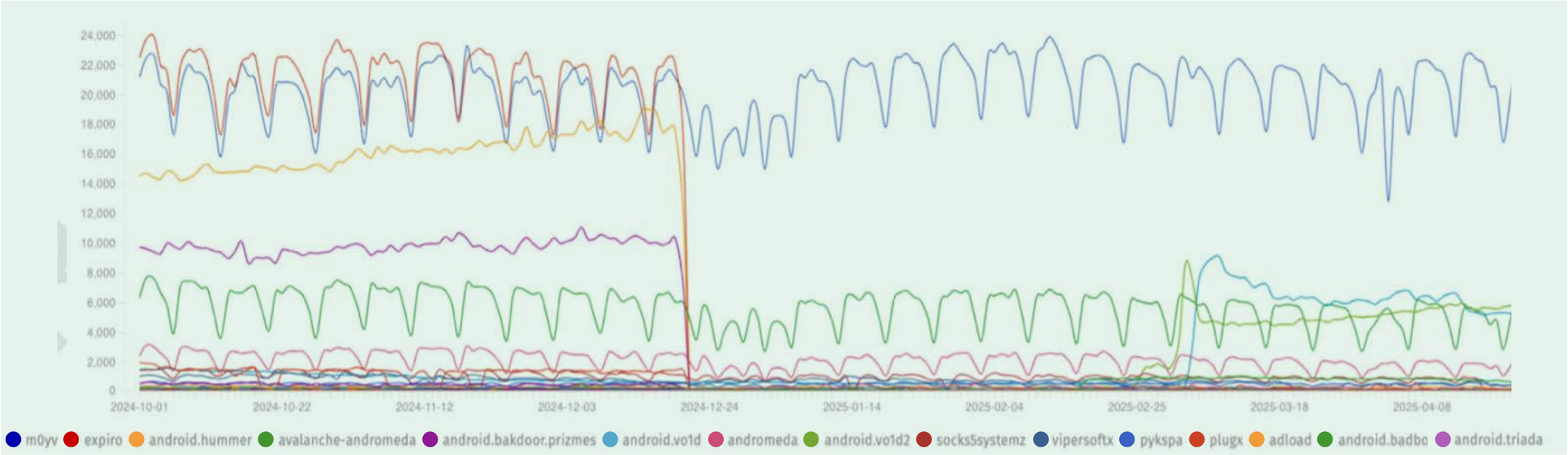
La Figure 14 ci-dessous montre que la plupart des infections d'appareils surviennent au Nigeria, suivi du Ghana ; cela découle probablement, en partie, du vaste espace d'adresses IP attribuables à ces nations.

Figure 14. **Pays les plus touchés par des logiciels malveillants dans la région de la CEDEAO – conformément aux données sinkhole**



Lacunes opérationnelles en termes de cybersécurité et recommandations : la Surface d'Attaque de la Région de la CEDEAO

Figure 15. **Principales infections contenues dans les sinkholes de Shadowserver dans la région de la CEDEAO – par type de logiciel malveillant**



The items at the bottom of each graph are arranged left to right in descending order in which they appear on the graph.

L'analyse des données sinkhole par type d'infection nous permet d'examiner de plus près les statistiques sur les infections pour observer les tendances dans le type de logiciels malveillants identifiés dans l'ensemble de la région.

La Figure 15 présente un éventail de variantes de logiciels malveillants infectant des appareils à l'échelle de la région de la CEDEAO. Par exemple, M0yv est un virus modulaire multifonctionnel utilisé par le groupe de logiciel rançonneur Maze en vue d'infecter des fichiers. Le groupe de logiciel rançonneur Maze était un gang de cybercriminels connu pour populariser la technique d'« extorsion double » qui lui permettait de voler les données de ses victimes et de les crypter. Si une rançon était payée, les données étaient décryptées et à nouveau accessibles à la victime. Si la rançon n'était pas payée, le groupe publiait les données volées sur des sites de fuite qu'il gérait.

RECOMMANDATIONS :

Mettre en œuvre des réglementations exigeant des CSIRT nationaux, des agences gouvernementales, des infrastructures critiques, des fournisseurs d'accès à Internet et des autres propriétaires de réseau dans la région qu'ils collaborent dans la remédiation des appareils identifiés comme étant infectés par des logiciels malveillants dans un délai court, mais spécifique, notamment ceux identifiés dans les rapports de remédiation de réseau quotidiens gratuits de Shadowserver.

3.3// Ensembles de données uniques provenant d'opérations des forces de l'ordre contre la cybercriminalité

Des ensembles de données uniques sont recueillis par Shadowserver ou partagés avec cette dernière dans le cadre de notre soutien aux **opérations de perturbation des forces de l'ordre contre la cybercriminalité***. Depuis plus de 15 ans, l'équipe spéciale de projets de Shadowserver (SSPT) apporte un soutien à un grand nombre des opérations internationales majeures de perturbation de la cybercriminalité. Ce soutien s'est présenté sous une multitude de formes, mais il implique généralement que Shadowserver mène des opérations sinkhole, mette en quarantaine les noms de domaines malveillants par le biais du registraire en dernier recours (RoLR), et contribue aux efforts de divulgation d'avis concernant les victimes par la distribution de données sur les victimes aux propriétaires de réseaux affectés et/ou à leur CSIRT national respectif dans ses rapports de remédiation de réseau quotidiens gratuits.

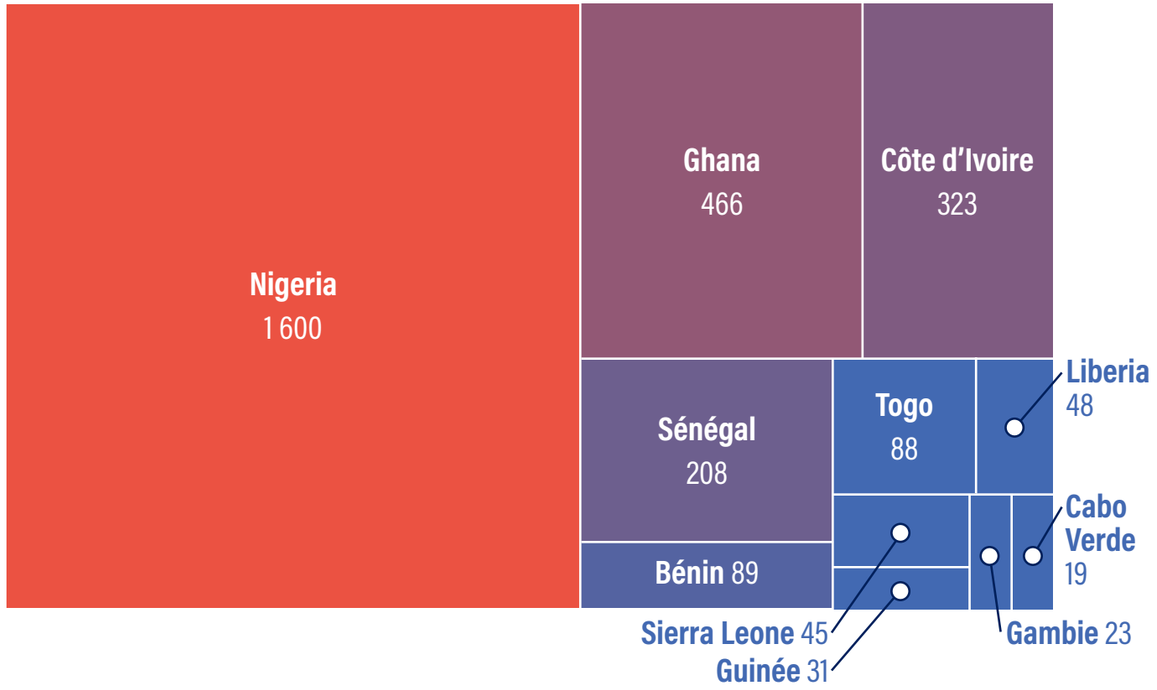
Les forces de l'ordre partagent souvent avec Shadowserver des ensembles de données uniques sur les infections passées d'appareils de victimes ainsi que sur les infections actives d'appareils de victimes qui communiquent avec les serveurs sinkhole de Shadowserver lorsque de vastes **réseaux zombie*** sont démantelés. Les infections passées sont partagées avec les CSIRT nationaux dans des rapports spéciaux ponctuels, et les infections actives sont communiquées dans le cadre des rapports de remédiation de réseau gratuits quotidiens de Shadowserver. Ces ensembles de données uniques acquis dans le cadre d'opérations de perturbation des forces de l'ordre révèlent l'existence d'appareils de victimes infectés par des logiciels malveillants dans la région de la CEDEAO qui faisaient partie de réseaux zombie contrôlés par des criminels.

Par exemple, le réseau zombie du logiciel malveillant Qakbot a été perturbé dans le cadre d'une opération de répression menée par le FBI et le ministère de la Justice américain aux côtés d'un grand nombre d'autres partenaires en août 2023. Qakbot (également appelé QBot, Pinkslipbot, Quakbot et Oakbot) a été activé vers l'année 2007, après avoir initialement été développé sous forme de logiciel de vol d'informations et de logiciel malveillant **cheval de Troie bancaire***, avant de devenir ensuite principalement un réseau de distribution d'autres logiciels malveillants/rançonneurs. Ces dernières années, Qakbot a été utilisé comme vecteur d'infection initial par de nombreux groupes de logiciel rançonneur, notamment Conti, ProLock, Egregor, REvil, MegaCortex et Black Basta. Il est probable que cela a donné lieu à d'importantes pertes financières au niveau mondial.

Comme le montre la Figure 16 ci-dessous, 2 941 infections passées par Qakbot ont été identifiées sur des appareils dans l'ensemble de la région de la CEDEAO.

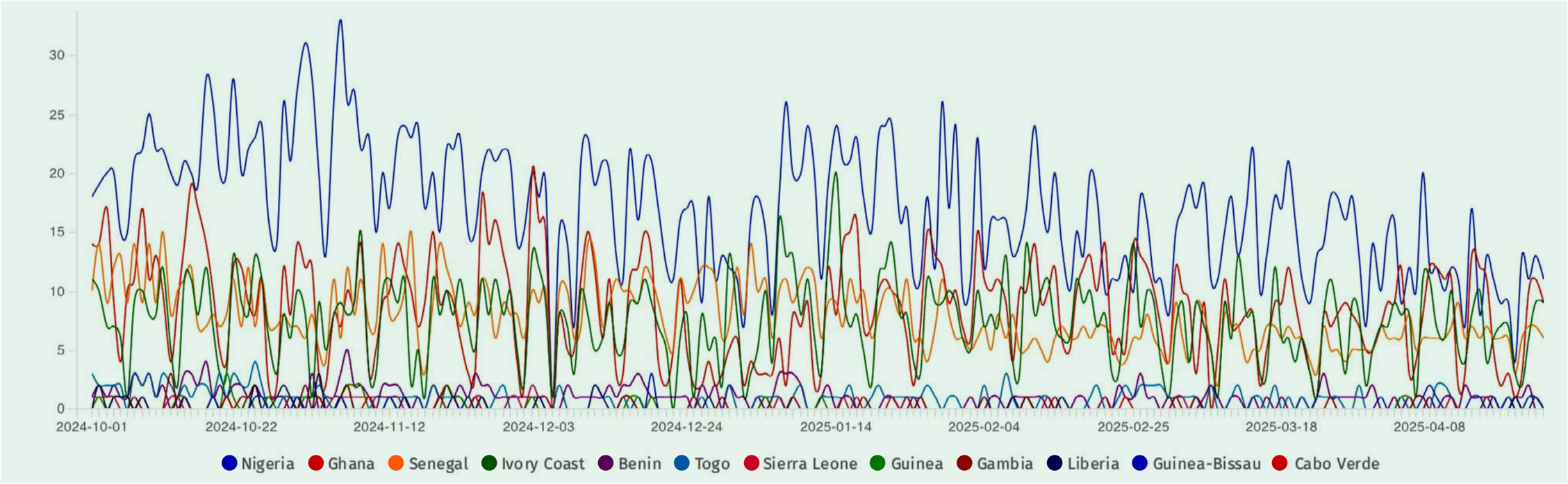
Un autre exemple : Operation Endgame était une opération internationale

Figure 16. **Infections passées par Qakbot dans l'ensemble de la région de la CEDEAO (24 août 2023)**



Lacunes opérationnelles en termes de cybersécurité et recommandations : la Surface d'Attaque de la Région de la CEDEAO

Figure 17. **Infections par Smokeloader dans l'ensemble de la région de la CEDEAO**



The items at the bottom of each graph are arranged left to right in descending order in which they appear on the graph.

de répression dirigée par Europol contre des injecteurs de logiciels malveillants, notamment IcedID, SystemBC, Pikabot, Smokeloader et Bumblebee, qui a abouti à quatre arrestations et au démantèlement de plus de 100 serveurs à l'échelle mondiale en mai 2024. Les injecteurs sont des programmes malveillants conçus pour introduire d'autres logiciels malveillants dans l'appareil d'une victime. Dans le chronogramme (Figure 17), on constate que toutes les nations de la CEDEAO ont été touchées par SmokeLoader, les nations comportant le plus d'adresses IPv4 étant les plus infectées.

Les ensembles de données sur les victimes acquis par Shadowserver au travers d'opérations de perturbation des forces de l'ordre contre la cybercriminalité sont uniques et ne sont directement disponibles nulle part ailleurs, et certainement pas auprès de fournisseurs commerciaux. Les CSIRT nationaux et les propriétaires de réseau dans l'ensemble de la région de la CEDEAO doivent mettre pleinement à profit l'accessibilité de ces précieuses données gratuites pour pouvoir appliquer des correctifs sur les appareils infectés par des logiciels malveillants et, ainsi, mieux sécuriser leurs réseaux. Bien que Shadowserver en ait assuré un sinkhole, ces appareils de victimes demeurent infectés, à moins et jusqu'à ce qu'ils fassent l'objet d'une remédiation, ce qui est possible dans le cadre d'efforts collaboratifs entre les CSIRT nationaux et les propriétaires de réseau affectés.

Tableau de bord public de Shadowserver

Le présent rapport comprend des statistiques de données sur les menaces et des visualisations provenant du Tableau de bord public gratuit de Shadowserver, financé par le ministère britannique des Affaires étrangères, du Commonwealth et du Développement (FCDO). Ce Tableau de bord permet au public d'interroger les ensembles de données de Shadowserver pour trouver des statistiques agrégées, par pays ou par région, sur un éventail d'aspects liés à des menaces. Dans le cadre du projet actuel, Shadowserver a créé un nouveau regroupement régional de pays dans le Tableau de bord pour couvrir spécifiquement les statistiques concernant la région de la CEDEAO. (Voir la Figure 18).

Le Tableau de bord peut être un outil utile pour informer les dirigeants gouvernementaux, les décideurs politiques, les chercheurs en cybersécurité, les spécialistes de la défense réseau, les organes de presse et d'autres acteurs sur les dernières cybermenaces qui touchent un pays et/ou une région. Le Tableau de bord fournit également des statistiques qui contribuent à surveiller l'avancement des efforts de correction et de remédiation au sein d'un pays ou d'une région relativement à une menace spécifique.

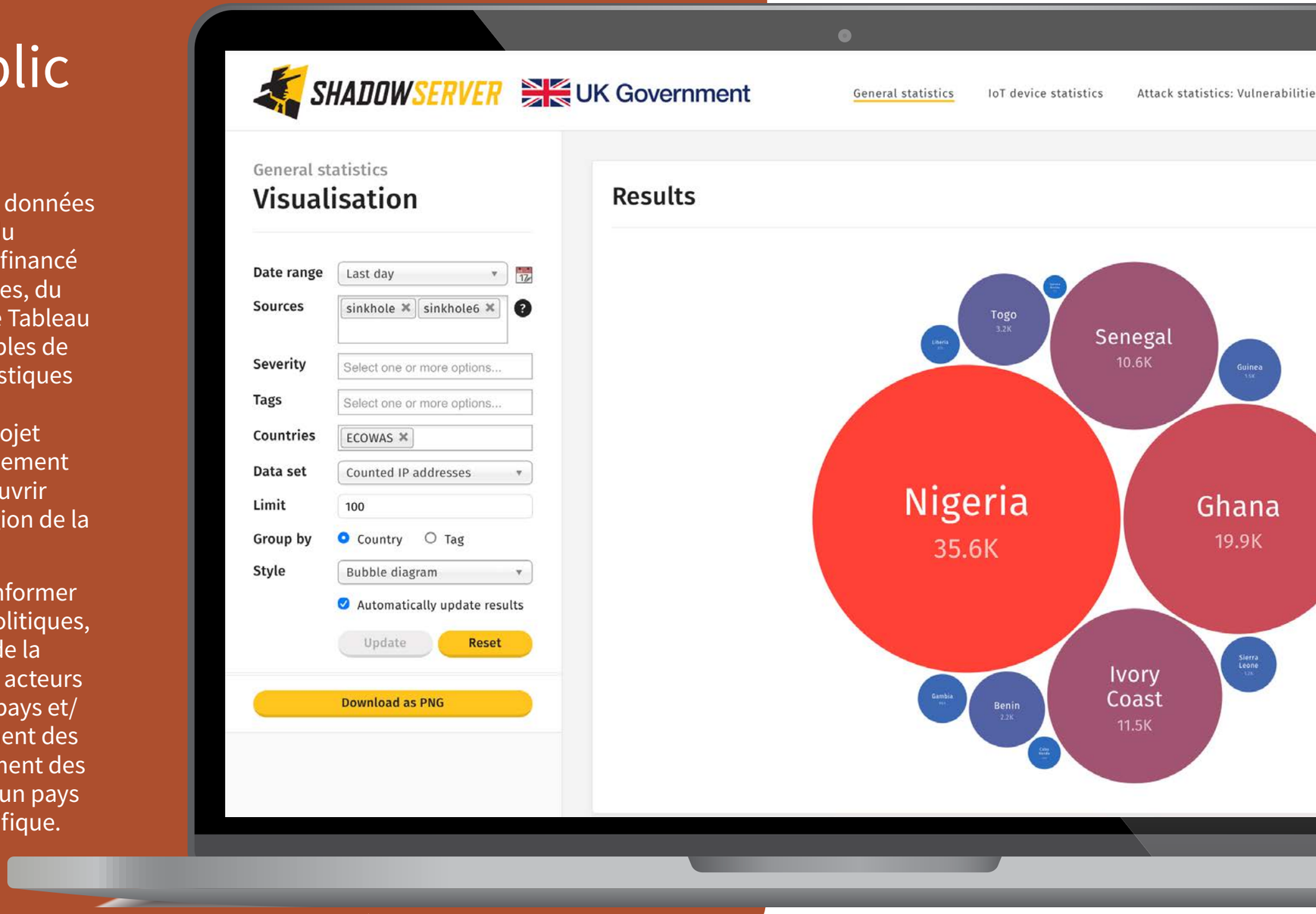


Figure 18. **Regroupement des pays de la région de la CEDEAO dans le Tableau de bord public de Shadowserver**

Tableau de bord public de Shadowserver

Par exemple, imaginez qu'un responsable de l'Équipe d'intervention en cas d'urgence informatique du Nigeria (ngCERT) prend connaissance du préjudice potentiel d'appareils domestiques connectés à l'internet facilitant des activités criminelles dans le cadre d'un vaste réseau zombie appelé Badbox 2.0. Des recherches complémentaires en ligne indiquent au responsable de la ngCERT que Google, HUMAN Security, Trend Micro et la Shadowserver Foundation se sont associées à une opération de perturbation contre le réseau zombie Badbox 2.0 dans laquelle Shadowserver a procédé à l'engouffrement (**sinkhole***) d'appareils infectés de manière à ce qu'ils communiquent désormais avec les serveurs sinkhole de Shadowserver et à ce que les acteurs malveillants ne puissent plus les contrôler. https://www.humansecurity.com/learn/blog/satori-disrupting-badbox-2/

Le responsable de la ngCERT souhaite obtenir des fonds du gouvernement pour une campagne de sensibilisation du public à Badbox 2.0 au Nigeria et pour une initiative de remédiation ciblée avec les CERT nationales homologues et les fournisseurs d'accès à Internet dans l'ensemble de la région de la CEDEAO. Pour contribuer à informer les représentants gouvernementaux du Nigeria et des États membres de la CEDEAO sur la menace de Badbox 2.0 dans la région, le responsable de la ngCERT peut interroger le Tableau de bord public de Shadowserver.

En cliquant sur l'onglet de données Sinkhole de Shadowserver, le responsable de la ngCERT peut ajouter des filtres à sa recherche sur la gauche de l'écran, notamment le jour (« Day »), les balises (« Tags ») (dans ce cas, « android.badbox2 »), et les pays (« Countries ») (dans ce cas, la CEDEAO, mais cela pourrait également être un pays unique, comme le Nigeria). Le résultat est une carte arborescente présentant les infections par Android Badbox 2.0 qui sont survenues la veille dans les divers États membres de la CEDEAO. (Voir la Figure 19).

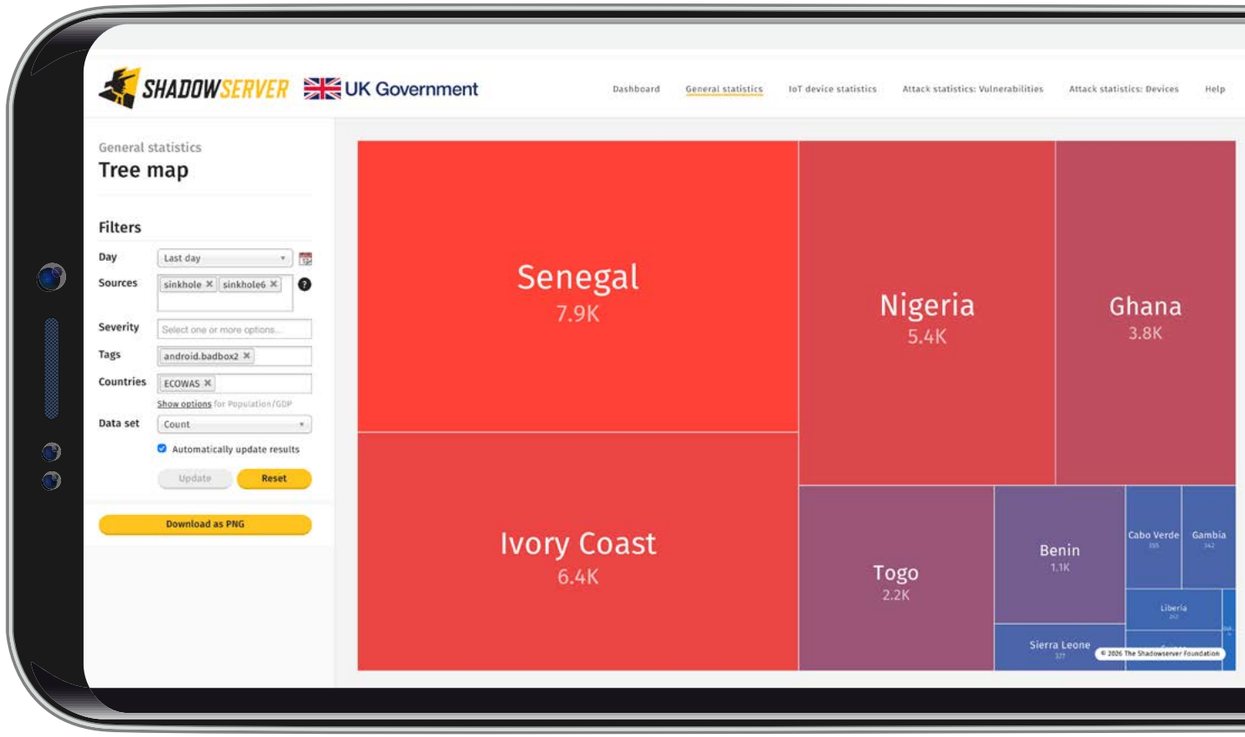


Figure 19. **Appareils infectés par Android Badbox 2.0 dans la région de la CEDEAO qui communiquent avec les serveurs sinkhole de Shadowserver**

Tableau de bord public de Shadowserver

Le responsable de la ngCERT peut également interroger les données dans un chronogramme (« Time Series ») (voir la Figure 20) pour surveiller les infections par Badbox 20 dans la région de la CEDEAO qui communiquent avec les serveurs sinkhole de Shadowserver au cours d'une période spécifique (dans ce cas, sur 3 mois). Le responsable de la ngCERT peut aussi survoler le graphique avec sa souris pour faire apparaître les statistiques correspondant à une date donnée.

RECOMMANDATION :
Le Tableau de bord public de Shadowserver peut être outil efficace pour informer les principales parties prenantes (par ex. les dirigeants gouvernementaux, les décideurs politiques, les chercheurs en cybersécurité, les spécialistes de la défense réseau, les organes de presse et d'autres acteurs) sur les dernières cybermenaces qui touchent leur pays et/ou la région. Ce Tableau de bord permet au public d'interroger les données de Shadowserver pour trouver des statistiques agrégées, par pays ou par région, portant sur les dernières cybermenaces survenues au cours des deux dernières années. Ces statistiques peuvent ensuite être utilisées pour établir la priorité des efforts de remédiation et en assurer un suivi, afin de minimiser ou d'éliminer les menaces critiques. Le Tableau de bord permet de rechercher des statistiques associées à un pays ou à une région donnée, notamment un nouvelle fonction de recherche spécifique à la région de la CEDEAO.

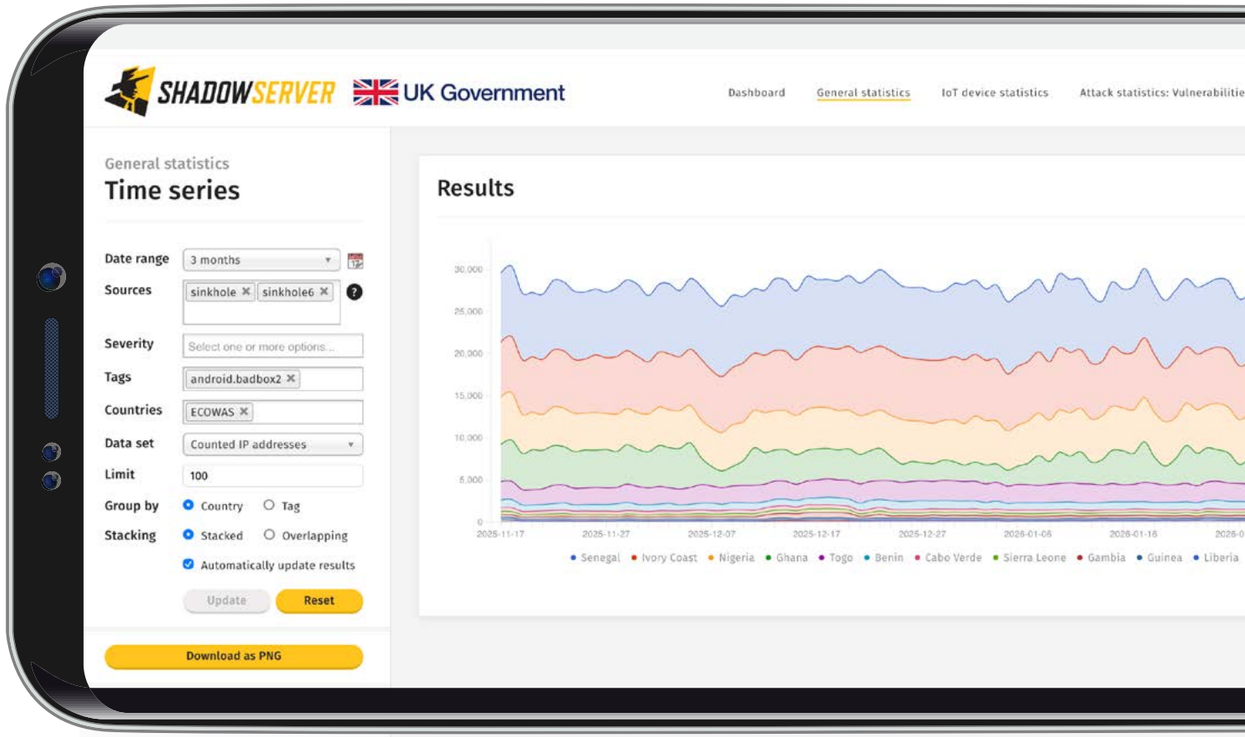


Figure 20. **Appareils infectés par Android Badbox 2.0 au cours des 3 derniers mois à compter de la date de la requête dans la région de la CEDEAO qui communiquent avec les serveurs sinkhole de Shadowserver**

Glossaire

Inventaire d'actifs : un catalogue complet continuellement mis à jour de tous les composants matériels, logiciels, de données et de réseau qu'une organisation possède ou utilise, qui sont essentiels pour identifier des vulnérabilités, gérer des risques, détecter des menaces et répondre à des incidents.

Surface d'attaque : tout point d'entrée ou vecteur d'attaque possible, notamment des vulnérabilités logicielles, que des attaquants peuvent exploiter pour s'infiltrer dans un système.

Cheval de Troie bancaire : un type de logiciel malveillant qui se fait passer pour un logiciel légitime en vue de tromper des utilisateurs pour les amener à l'installer, avec pour objectif principal de voler des informations financières sensibles (par ex. des authentifiants de compte bancaire en ligne, des détails de cartes de crédit, etc.) et d'effectuer des transactions financières non autorisées.

Réseau zombie : un réseau d'appareils interconnectés qui est infecté par un logiciel malveillant et contrôlé sous forme de groupe sans que le propriétaire le sache ou y ait consenti ; souvent utilisé par des acteurs malveillants pour échafauder des projets criminels, notamment l'envoi de pourriels et de courriels d'hameçonnage, le lancement d'attaques par déni de service distribué et le vol de données, entre autres activités.

Compromission de messagerie d'entreprise (BEC) : un type de système de fraude en ligne par lequel des cybercriminels se font passer pour des personnes de confiance (par ex. des PDG, des fournisseurs, etc.) associées à une entreprise, notamment en usurpant ou en piratant les comptes de messagerie électronique légitimes de ces personnes, afin de tromper des employés pour qu'ils transfèrent de l'argent, changent les détails de transactions de paiements ou envoient des données sensibles comme des informations fiscales ou des authentifiants de connexion.

Identifiant de vulnérabilités et d'expositions courantes (CVE) : failles de sécurité divulguées publiquement dans des logiciels, des équipements ou des micrologiciels auxquels un identifiant unique, ou identifiant CVE a été attribué, pour faciliter des communications cohérentes et une surveillance des vulnérabilités au sein de la communauté de la cybersécurité.

Actif compromis : toute ressource organisationnelle (y compris un serveur, un réseau, un compte ou des données) dont la sécurité a été violée, ce qui ouvre la porte à des accès, des divulgations, des modifications ou des destructions non autorisé(e)s, affectant ainsi la confidentialité, l'intégrité ou la disponibilité de cette ressource.

Injection de code de vol d'authentifiant : un type de cyberattaque où les acteurs malveillants exploitent des vulnérabilités dans une application pour injecter et exécuter un code dans un réseau ou un système ciblé et pour recueillir des informations d'authentification comme des noms d'utilisateur et des mots de passe.

Infrastructures critiques : les actifs, systèmes et réseaux fondamentaux – tant physiques que virtuels – qui sont essentiels au bon fonctionnement de l'économie, de la sécurité et de la santé d'une nation, y compris, sans toutefois s'y limiter, dans des secteurs tels que l'énergie, les systèmes hydriques, les ressources nucléaires, les transports, les télécommunications, la défense et les systèmes alimentaires et agricoles.

Acteur malveillant : toute personne ou tout groupe de personnes portant intentionnellement des préjudices dans la sphère numérique, notamment des cybercriminels, des pirates d'États-nations/de gouvernements, des terroristes, des cybermilitants (hacktivistes) et des initiés.

Paysage des cybermenaces : l'environnement global en évolution des risques, des menaces et des dangers potentiels et reconnus en cybersécurité, notamment les types d'attaquants et leurs motivations, qui affecte des groupes d'utilisateurs, des organisations ou des industries spécifiques, ou une période donnée.

Glossaire

Internet clandestin (Dark Net) : un réseau qui nécessite des logiciels spécifiques pour pouvoir y accéder, favorisant ainsi l'existence de portions cachées de l'Internet conçues pour préserver l'anonymat.

Double extorsion : une cyberattaque où les criminels volent des données sensibles, puis demandent une rançon pour empêcher la divulgation publique, la vente ou tout autre type d'utilisation détournée de données qui pourrait infliger à la victime de graves préjudices financiers, juridiques et réputationnels.

Site dédié aux fuites : un site Internet ou une plateforme Web, souvent hébergé(e) sur l'Internet clandestin, où des cybercriminels divulguent publiquement des noms et des données qui ont été volées à des organisations victimes dans le cadre d'attaques par logiciel rançonneur et/ou d'une double extorsion, afin d'exploiter les victimes en leur faisant payer une rançon pour éviter les préjudices financiers, juridiques et réputationnels qui pourraient découler de la divulgation de données sensibles.

Appareils : les entités matérielles (comme des ordinateurs et des serveurs) sur un réseau.

Déni de service distribué (DDoS) : un type de cyberattaque par lequel plusieurs systèmes compromis, souvent agencés sous forme de réseau zombie, submergent un réseau, un serveur ou un service en ligne ciblé avec un énorme volume de trafic susceptible de ralentir, voire de faire planter ses systèmes. Les attaques par DDoS génèrent de graves perturbations et sont capables de provoquer des temps d'arrêt, des pertes financières et des préjudices réputationnels considérables.

Système de noms de domaines (DNS) : un système qui traduit des noms de domaines facilement lisibles (comme www.exemple.com) en adresses IP lisibles par machine (comme 192.0.2.44) que les ordinateurs utilisent pour se connecter et trouver des ressources en ligne tout en s'assurant que les utilisateurs n'ont pas besoin de mémoriser une longue chaîne de chiffres dans une adresse IP pour accéder à des sites Internet ou à des services en ligne.

Service d'alerte précoce : un service gratuit offert par de nombreux CSIRT nationaux (ainsi que par un certain nombre de CERT sectorielles, d'ISAC et d'autres entités comptant beaucoup de membres) où les membres fournissent leurs adresses IP publiques et noms de domaines et, en échange, reçoivent des avis d'alerte automatisés concernant des appareils et services exposés, vulnérables et compromis sur leur réseau pour faciliter une remédiation rapide.

Pare-feu : un système de sécurité de réseau qui sert de barrière entre un réseau interne de confiance et un réseau externe non fiable, comme l'Internet.

Leurres de détection (Honeypot) : leurres configurés pour sembler être des actifs de réseau légitimes, mais vulnérables (notamment des applications logicielles, des serveurs et d'autres appareils) en vue d'inciter les acteurs malveillants à attaquer. Les capteurs enregistrent alors les activités des attaquants et recueillent des informations sur leurs tactiques, leurs outils et leurs procédures/techniques. Les données recueillies contribuent à identifier les sources des attaques et les nouvelles méthodes d'attaque, à développer des défenses et à prévenir des attaques futures.

Implant : un programme intégré dans un réseau ou un système pour créer des mécanismes d'accès à distance et exécuter diverses fonctions sans que l'utilisateur le sache, notamment un vol de données, des perturbations et le maintien d'un accès persistant.

Centre de partage et d'analyse de l'information (ISAC) : une organisation dirigée par ses membres qui regroupe, analyse et diffuse des informations concrètes sur des menaces pour aider ses membres à en atténuer les risques de manière proactive.

Adresse de protocole Internet (IP) : un identifiant numérique unique attribué à chaque appareil qui se connecte à l'Internet.

Vulnérabilité exploitée connue : une vulnérabilité dans un logiciel, une application ou

Glossaire

un système qui est activement exploitée par des acteurs malveillants, exposant ainsi cette vulnérabilité à un risque hautement prioritaire qui nécessite un correctif immédiat pour empêcher une violation.

Opération de perturbation des forces de l'ordre contre la cybercriminalité : une initiative proactive d'agences de répression destinée à perturber des activités cybercriminelles en démantelant des infrastructures (par ex. serveur, sites Internet, etc.) criminelles, en arrêtant des acteurs malveillants et en saisissant des actifs.

Logiciel malveillant : un logiciel conçu spécifiquement pour endommager ou perturber un système informatique, ou pour y accéder sans autorisation.

Centre national de réponse aux incidents de sécurité informatique (CSIRT national) : une entité désignée par un gouvernement qui coordonne les réponses nationales face à des cyber-incidents, protégeant ainsi les infrastructures critiques, les activités du gouvernement et la sécurité économique en gérant les menaces dans le cyberespace, en diffusant des informations, en sensibilisant aux cyber-stratégies existantes et en les mettant en œuvre. Ils servent souvent de point central pour signaler des cyber-événements de grande ampleur dans un pays et y répondre.

Hameçonnage : un type de cyberattaque reposant sur des courriels, des messages texto, des appels téléphoniques ou des sites Internet frauduleux destinés à tromper des victimes pour les inciter à partager des données sensibles (comme des noms d'utilisateur, des mots de passe, des informations de compte bancaire, des numéros de cartes de crédit ou d'autres informations importantes), à télécharger des logiciels malveillants ou, sinon, à s'exposer à des activités cybercriminelles.

Logiciel rançonneur : un type de logiciel malveillant qui crypte/verrouille les fichiers et les systèmes d'une victime pour les rendre inaccessibles, puis qui demande le paiement d'une rançon en échange d'une clé de décryptage permettant de rétablir l'accès.

Registraire : une société qui vend et gère des noms de domaines, agissant comme un intermédiaire pour les personnes et les entreprises (appelées « titulaires de noms de domaines ») et les organisations (appelées « opérateurs de registre ») qui contrôlent des domaines de haut niveau.

Registre : un registre de noms de domaines est une organisation qui gère des noms de domaines de haut niveau en créant des extensions de nom de domaine, en établissant les règles pour un nom de domaine spécifique et en travaillant avec les registraires pour vendre des noms de domaines au public. Par exemple, Verisign gère l'enregistrement des noms de domaines .com et de leur système de noms de domaines (DNS).

Routeur : un appareil qui transmet des paquets de données aux sections appropriées d'un réseau informatique.

Centre sectoriel de réponse aux incidents de sécurité informatique (CSIRT sectoriel) : une entité spécialisée qui traite les réponses à des incidents de cybersécurité, promeut le partage d'informations pour atténuer des menaces et offre des connaissances et une expertise spécialisées dans un secteur spécifique d'un pays ou d'une économie (par ex. eau, santé, énergie, finances, transports, etc.).

Application côté serveur : désigne les fonctions, les procédures, les calculs ou les méthodes de traitements effectué(e)s sur un serveur et géré(e)s en arrière-plan sur un système à distance plutôt que sur l'appareil d'un utilisateur.

Services : les applications ou fonctions logicielles que des appareils fournissent ou consomment (par ex. serveur Web, messagerie électronique ou stockage de fichiers) et qui facilitent les communications et le partage de ressources en réseau.

Protocole simple de gestion de réseau (SNMP) : un protocole qui assume un rôle vital dans le suivi, la gestion et la sécurisation d'appareils en réseau,

en permettant aux administrateurs de réseau de recueillir des informations, de configurer des appareils et de répondre à distance à des événements sur le réseau, ce qui en fait un outil essentiel pour maintenir la performance et la sécurité d'un réseau.

Sinkholing : une technique consistant à perturber les communications entre les appareils de victimes infectés par des logiciels malveillants et les serveurs contrôlés de manière illicite avec lesquels les logiciels malveillants ordonnent aux appareils infectés de communiquer. Le trafic est redirigé vers les serveurs sinkhole qui appartiennent à une entité responsable, de façon à ce que les criminels ne puissent plus accéder aux appareils de victimes ni les contrôler, bien que ces appareils restent infectés par des logiciels malveillants tant qu'ils n'ont pas fait l'objet d'une remédiation.

Services VPN : un service de réseau virtuel privé (VPN) est un outil en ligne qui crée un « tunnel » crypté sécurisé pour le trafic Internet, masquant l'adresse IP et l'emplacement réels d'un utilisateur pour améliorer sa confidentialité et sa sécurité.

Vulnérabilité/vulnérabilités : une faiblesse dans un système d'information, les procédures de sécurité d'un système, des contrôles internes ou une mise en œuvre qui pourrait être exploitée par un acteur malveillant pour accéder sans autorisation à un système, un réseau ou un appareil, ou pour l'endommager.

Console Web malveillante : un script ou un programme malveillant que des acteurs malveillants déploient sur un serveur Web compromis pour obtenir (et maintenir) un accès à distance à ce serveur et le contrôler. Les acteurs malveillants peuvent ainsi réaliser un éventail d'activités malveillantes, notamment le vol de données et la dissémination de logiciels malveillants.

Vulnérabilité jour zéro : une vulnérabilité de la sécurité d'un logiciel, équipement ou micrologiciel dont le fournisseur n'a pas connaissance et que des attaquants exploitent avant que le fournisseur s'en rende compte et qu'il ait eu la possibilité de développer un correctif pour y remédier.