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

Região da CEDEAO:

Informações e recomendações sobre cibersegurança

Fevereiro de 2026

SHADOWSERVER

Índice

Resumo executivo

A Comunidade Económica dos Estados da África Ocidental (CEDEAO) procura promover a cooperação económica entre os seus doze estados-membros, de modo a melhorar os níveis de vida e a promover o desenvolvimento económico. Em busca deste objetivo, a Comissão da CEDEAO e a região no seu conjunto têm vindo a contemplar cada vez mais as tecnologias digitais como um motor essencial de crescimento. O resultado tem sido uma rápida transformação digital nos últimos anos que ajudou a impulsionar o crescimento e desenvolvimento económico. No entanto, também evidenciou imensas falhas ou «lacunas» institucionais e operacionais em termos de cibersegurança na região, algumas das quais significativas. Estes fatores (isto é, crescimento económico, um rasto digital expandido e falhas conhecidas no âmbito da cibersegurança) combinados tornam a região um alvo cada vez mais atrativo e vulnerável de **agentes de ameaças cibernéticas*.**[1]

O número, dimensão e impacto dos ciberataques na região da CEDEAO estão a aumentar a um ritmo alarmante. Um relatório da INTERPOL publicado em junho de 2025 advertiu sobre um acentuado aumento do cibercrime em África, sendo o cibercrime responsável por mais de 30 por cento de todo o crime reportado na África Ocidental.[2] O relatório referiu ainda perdas financeiras estimadas num montante superior a 3 mil milhões de dólares resultantes de incidentes cibernéticos por todo o continente entre 2019 e 2025.[3]

Recentemente, a região suportou ataques de **ransomware*** onerosos na Electricity Company of Ghana (Empresa de Eletricidade do Gana)[4] e no Banco Central da Gâmbia,[5] ataques de **negação de serviço distribuído (DDoS)*** causadores de perturbações contra websites do governo senegalês[6] e a operadora de telecomunicações MTN Nigeria,[7] e a intrusão devastadora da empresa fintech de processamento de pagamentos com sede na Costa do Marfim CinetPay que deve mais de 1 milhão aos clientes.[8] O resultado tem sido uma crescente preocupação em relação às capacidades da região em termos de cibersegurança e um forte senso de urgência para agir.

Fazer face às lacunas identificadas neste relatório é crucial para garantir que as capacidades de cibersegurança e a resiliência cibernética global acompanham a rápida expansão digital da região, bem como o volume, magnitude e sofisticação de ameaças emergentes que visam a região. Se não forem abordadas, estas lacunas podem tornar a cibersegurança da região cada vez mais incompleta, comprometendo assim o desenvolvimento económico, minando a confiança pública e causando impacto nos serviços que afetam a qualidade de vida.

---

1 As palavras e frases em negrito e assinaladas com um asterisco (*) estão definidas no “Glossário” no final deste relatório.

2 “New INTERPOL Report Warns of Sharp Rise in Cybercrime in Africa,” *INTERPOL News Release*, 23 de junho de 2025. https://www.interpol.int/en/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa

3 “Africa faces $3bn in cybercrime losses, Interpol flags top 4 threats,” *Ecofin Agency*, 26 de agosto de 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*, 1 de outubro de 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 de nov. de 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 de maio de 2023. https://www.reuters.com/world/africa/senegalese-government-websites-hit-with-cyberattack-2023-05-27/

7 “Inside the Eight-Hour Long Cyberattack that Tried to Cripple MTN Nigeria,” *Techcabal*, 9 de julho de 2025. https://techcabal.com/2025/07/09/cyberattack-that-tried-to-cripple-mtn-nigeria/

8 “CinetPay customers owed over $1 million months after alleged cyberattack,” *Techcabal*, 1 de fevereiro de 2026. https://techcabal.com/2026/02/01/cinetpay-cyberattack/

As atuais ameaças cibernéticas que a região da CEDEAO enfrenta estão bem documentadas. Incluem **ransomware***, ataques a **infraestruturas críticas*, ataques DDOS***, **comprometimento de e-mail empresarial***, fraudes e burlas online e extorsão sexual digital para citar alguns. Este relatório utiliza os dados de ameaças cibernéticas, a análise e inúmeros anos de conhecimento especializado da The Shadowserver Foundation na área para informar os principais intervenientes sobre as atuais lacunas institucionais e operacionais em termos de cibersegurança que tornam a região da CEDEAO particularmente vulnerável a estas e a outras ameaças cibernéticas.
O relatório fornece ainda recomendações de ação que podem ser realizadas a nível nacional e regional para abordar tais lacunas.

As lacunas *institucionais* mais urgentes e significativas estão relacionadas com a necessidade de instituições de cibersegurança eficazes na região, particularmente as **Equipas Nacionais de Resposta a Incidentes de Segurança Informática (CSIRT nacionais)***, um **Centro de Partilha e Análise de Informações da CEDEAO** e as **CSIRT Sectoriais***. Para executarem eficazmente os respetivos deveres e responsabilidades, estas entidades necessitam de acesso a dados, ferramentas, serviços e plataformas gratuitos e/ou acessíveis; competência técnica interna; formação e serviços de desenvolvimento de capacidades; avaliações de maturidade para medir o progresso no desenvolvimento; parcerias globais e regionais; e a criação de **serviços de alerta precoce*** para servir as respetivas partes interessadas.

Além das lacunas *institucionais*, são menos divulgadas as lacunas de cibersegurança *operacionais* técnicas associadas às **superfícies de ataques cibernéticos*** dos Estados-membros da CEDEAO. À semelhança de muitas superfícies de ataque, a região da CEDEAO caracteriza-se por **dispositivos*** e **serviços*** publicamente expostos à Internet (que expandem desnecessariamente a superfície de ataque e proporcionam potenciais pontos de entrada numa rede); **vulnerabilidades*** críticas em ativos expostos que podem ser exploradas por agentes de ameaças caso não sejam solucionadas; **ativos comprometidos*** que podem *continuar* a ser explorados caso não sejam solucionados; e dispositivos infetados com **malware*** por meio dos quais os agentes de ameaças tiverem (ou têm) acesso e controlo não autorizados, muitas vezes como parte de uma **botnet*** mais alargada.

Um fator importante na gestão da superfície de ataque da região da CEDEAO envolverá a implementação de regulamentos apropriados por cada estado-membro que garantam que os especialistas em proteção de redes essenciais (particularmente os que atuam nos setores governamental e de infraestruturas críticas) realizem **inventários de ativos*,** garantam que os ativos não estejam desnecessariamente expostos à Internet e solucionem oportunamente **vulnerabilidades*** críticas/de elevada gravidade, **vulnerabilidades exploradas conhecidas*** e **ativos comprometidos*.**

É imperativo que os principais intervenientes compreendam as respetivas superfícies de ataque cibernético para permitir a definição eficaz de políticas, elaborar legislação apropriada e implementar medidas de segurança que protejam as redes. É essencial que os líderes governamentais, os decisores, os especialistas em proteção de redes e os especialistas em cibersegurança trabalhem colaborativamente para abordar as questões identificadas neste relatório.

Uma forma de ajudar a informar os principais intervenientes sobre a superfície de ataque de uma nação e/ou região é utilizar o Painel público da Shadowserver. O Painel permite que o público consulte os dados da Shadowserver para obter dados estatísticos agregados, ao nível nacional ou regional associados às mais recentes ameaças cibernéticas que ocorreram nos dois anos anteriores. Este pode então ser utilizado para priorizar e monitorizar os esforços de mitigação para minimizar ou erradicar ameaças críticas.
O Painel pode ser consultado para obtenção de dados estatísticos associados a um país individual bem como a uma região, incluindo uma consulta recém-criada especificamente para a região da CEDEAO.

Recomendações

As principais ações recomendadas decorrentes das falhas ou lacunas institucionais e operacionais em termos de cibersegurança identificadas neste relatório são as seguintes:

Recomendações institucionais:

CSIRT NACIONAIS

Estabelecer uma CSIRT Nacional operacionalmente eficaz em cada Estado-membro da CEDEAO.

ISAC (CENTRO DE PARTILHA E ANÁLISE DE INFORMAÇÃO) DA CEDEAO

Estabelecer um ISAC da CEDEAO para ajudar a garantir que todas as CSIRT Nacionais da região trabalham colaborativamente, partilham informações, progridem no respetivo desenvolvimento e promovem parcerias nacionais, regionais e internacionais vitais.

CSIRT SECTORIAIS

Estabelecer uma CSIRT Sectorial para um setor de infraestruturas crítico identificado como o mais vulnerável e o mais indispensável em cada país. Na medida que o financiamento o permita, CSIRT Sectoriais adicionais podem ser estabelecidas posteriormente entre setores para garantir que cada setor recebe competências técnicas, informações sobre ameaças, gestão de riscos e serviços de resposta a incidentes de acordo com as necessidades únicas do respetivo setor.

ACESSO A DADOS, FERRAMENTAS E SERVIÇOS GRATUITOS/ACESSÍVEIS

CSIRT Nacionais e especialistas em proteção de redes de todos os tipos e entre todos os setores devem beneficiar de dados, ferramentas, serviços e plataformas gratuitos e/ou acessíveis sobre ameaças cibernéticas que estejam disponíveis. Tal inclui relatórios de remediação de redes diários e gratuitos da Shadowserver, bem como ferramentas de código aberto gratuitas (incluindo IntelMQ, Elasticsearch, Kibana e outras) necessários para ingerir, armazenar, interpretar, pesquisar, visualizar, analisar e utilizar eficazmente fluxos de dados de ameaças. Deve igualmente considerar-se ferramentas e serviços comerciais potencialmente acessíveis, incluindo a Arctic Hub, uma plataforma de automação de informações sobre ameaças cibernéticas disponível gratuitamente no primeiro ano e nos anos subsequentes mediante taxas reduzidas para CSIRT Nacionais qualificadas através do Programa de Desenvolvimento de CSIRT da Arctic Security. Tal como apresentado no website da Arctic Security, a CSIRT Nacional da Gâmbia (gmCSIRT) é uma atual participante no programa.

COMPETÊNCIA TÉCNICA INTERNA

Assegurar que cada CSIRT Nacional e especialistas em proteção de redes do governo e sistemas de infraestruturas críticas têm funcionários que possuem competências técnicas adequadas para proteger e defender eficazmente as redes do país. Os Estados-Membros da CEDEAO devem colaborar com as universidades para desenvolver programas de formação e de estágios que possam atuar como um pipeline de talentos tecnicamente qualificados. Os Estados-Membros devem também colaborar com o setor privado para desenvolver programas nos quais especialistas experientes do setor privado possam desempenhar funções temporárias, embora de longa duração nas CSIRT Nacionais e em entidades governamentais/de infraestruturas críticas para prestar mentoria e formar funcionários menos experientes e menos técnicos.

Recomendações institucionais:

FORMAÇÃO E DESENVOLVIMENTO DE CAPACIDADES

Procurar oportunidades para projetos de formação e desenvolvimento de capacidades (em particular projetos operacionais focados em configurar e utilizar eficazmente dados, ferramentas, serviços e plataformas gratuitas/de código aberto que estejam disponíveis). Tais projetos são frequentemente financiados por ministérios de negócios estrangeiros (incluindo o Ministério Federal dos Negócios Estrangeiros da Alemanha e o GIZ e o Ministério dos Negócios Estrangeiros, da Commonwealth e do Desenvolvimento do Reino Unido), entidades do setor privado (incluindo a Microsoft e a Google), bem como o Banco Mundial, as Nações Unidas e a União Europeia, para citar alguns.

DESENVOLVIMENTO DE PARCERIAS

Criar um quadro de referência que exija que as CSIRT Nacionais estabeleçam e mantenham relações profissionais sólidas com partes interessadas/intervenientes nos respetivos países (incluindo prestadores de serviços de Internet, operadores de infraestruturas críticas, entidades governamentais, empresas, universidades, governos estaduais e locais, prestadores de cuidados de saúde, instituições financeiras, etc.), bem como com CSIRT Nacionais na região da CEDEAO e em todo o mundo. Estas relações são cruciais para promover a partilha de informações, a colaboração e o desenvolvimento de capacidades. As oportunidades para as CSIRT Nacionais desenvolverem parcerias globais incluem através de um ISAC da CEDEAO, tornando-se membro do FIRST.org, e aderindo à plataforma de conversação Alliance Mattermost online gratuita da Shadowserver que permite o acesso direto aos funcionários da Shadowserver, Parceiros da Alliance de todo o setor e CSIRT Nacionais de todo o mundo.

AVALIAÇÕES DE MATURIDADE

Para estabelecer um nível de maturidade inicial, cada CSIRT Nacional deve ser mandatada para passar pela avaliação da ferramenta online de autoavaliação do Modelo de Maturidade de Gestão de Incidentes de Segurança (SIM3) da Open CSIRT Foundation e implementar recomendações para melhoria.

SERVIÇOS DE ALERTA PRECOCE

CSIRT Nacionais, CSIRT Sectoriais, ISAC e outras entidades com grandes grupos de destinatários devem ser mandatados para oferecer Serviços de Alerta Precoce gratuitos nos quais os respetivos integrantes recebem notificações automáticas de alerta sobre dispositivos e serviços expostos, configurados incorretamente, passíveis de abuso, vulneráveis e comprometidos nas respetivas redes para facilitar a remediação oportuna. A consulta com uma das inúmeras CSIRT Nacionais que operam tais Serviços de Alerta Precoce é recomendada, como o Centro Nacional de Cibersegurança do Reino Unido (NCSC do Reino Unido) e o CSIRT-RD da República Dominicana.

Recomendações operacionais:

INVENTÁRIOS DE ATIVOS

Estabelecer políticas para mandatar a realização de inventários de ativos periódicos, em particular nos setores governamental e de infraestruturas críticas. Essa medida ajudará os proprietários de redes nos esforços de correção e remediação oportunos enquanto surgem novas vulnerabilidades críticas. *Ver* "Diretiva Operacional Vinculativa 23-01: Melhoria da Visibilidade de Ativos e da Deteção de Vulnerabilidades nas Redes Federais".

GARANTIR QUE OS ATIVOS NÃO SEJAM EXPOSTOS DESNECESSARIAMENTE NA INTERNET PÚBLICA

Garantir que os proprietários de redes (em particular, infraestruturas críticas, governo e grandes fornecedores de serviços de Internet) não expõem desnecessariamente determinados tipos de dispositivos e serviços na Internet pública, a menos que seja necessário para fins de funcionalidade. Esta medida reduzirá a superfície de ataque global da região. Formações e workshops focados com CSIRT Nacionais, fornecedores de serviços de Internet e outros proprietários de redes na região da CEDEAO poderão culminar em atividade de reforço proativo para visar e reduzir casos de dispositivos e serviços expostos desnecessariamente.

REGULAMENTOS QUE MANDATAM A REMEDIAÇÃO DE VULNERABILIDADES CRÍTICAS E DE ELEVADO RISCO

Implementar regulamentos que exijam que as agências governamentais e infraestruturas críticas remediem as vulnerabilidades designadas como "risco crítico" no prazo de 15 dias civis e as designadas como "elevado risco" no prazo de 30 dias civis a partir da data de deteção inicial. *Ver* "Diretiva Operacional Vinculativa (BOD) 19-02: Requisitos de Remediação de Vulnerabilidades para Sistemas Acessíveis pela Internet".

REGULAMENTOS QUE MANDATAM A REMEDIAÇÃO DE VULNERABILIDADES EXPLORADAS CONHECIDAS

Implementar regulamentos que exijam que o governo e as infraestruturas críticas remediem "vulnerabilidades exploradas conhecidas" no prazo de 14 dias. O DHS (Departamento de Segurança Interna) e a CISA (Agência de Segurança Cibernética e de Infraestruturas) dos EUA mantêm um catálogo de Vulnerabilidades Exploradas Conhecidas (KEV) que identifica vulnerabilidades observadas como estando a ser ativamente exploradas em ambiente real e que devem ser remediadas pelas agências federais governamentais dos Estados Unidos. A ENISA (Agência Europeia para a Segurança das Redes e da Informação) mantém um catálogo semelhante conhecido como a Base de Dados de Vulnerabilidades da União Europeia. Por último, o Painel público da Shadowserver mantém a lista de vulnerabilidades exploradas conhecidas da Shadowserver identificada através da respetiva rede de sensores de honeypots. *Ver* "Diretiva Operacional Vinculativa (BOD) 22-01: Redução do Risco Significativo de Vulnerabilidades Exploradas Conhecidas".

REGULAMENTOS QUE MANDATAM A REMEDIAÇÃO DE DISPOSITIVOS COMPROMETIDOS E INFETADOS COM MALWARE IDENTIFICADOS

Implementar regulamentos que exijam que as CSIRT Nacionais, agências governamentais, infraestruturas críticas, fornecedores de serviços de Internet e outros proprietários de redes na região remediem dispositivos comprometidos e infetados com malware identificados num período de tempo breve mas especificado, incluindo os identificados nos relatórios diários de remediação de redes gratuitos da Shadowserver.

Recomendações operacionais:

CAMPANHAS DE ATENUAÇÃO/ERRADICAÇÃO DE AMEAÇAS

Mandatar CSIRT Nacionais, em coordenação com os Fornecedores de Serviços de Internet (FSI), para conceber e implementar campanhas de atenuação e erradicação de ameaças a nível nacional contra vulnerabilidades críticas e dispositivos comprometidos em redes espalhadas pelo país e monitorizar o progresso dos esforços de remediação. Um exemplo disso é a campanha a nível nacional liderada pela Australian Signals Directorate (ASD) para erradicar implantes Bad Candy em dispositivos Cisco IOS XE comprometidos em toda a Austrália.

PAINEL PÚBLICO GRATUITO DA SHADOWSERVER

O Painel público da Shadowserver pode ser uma ferramenta eficaz para informar os principais intervenientes (por exemplo, decisores, líderes governamentais, especialistas em proteção de redes, investigadores no âmbito da cibersegurança, etc.) sobre as mais recentes ameaças cibernéticas que afetam o seu país e/ou a região. O Painel permite que o público consulte os dados da Shadowserver para obter dados estatísticos agregados, ao nível nacional ou regional associados às mais recentes ameaças cibernéticas que ocorreram nos dois anos anteriores. Este pode então ser utilizado para priorizar e monitorizar os esforços de mitigação para minimizar ou erradicar ameaças críticas. O Painel pode ser consultado para obtenção de dados estatísticos associados a um país individual bem como a uma região, incluindo uma consulta recém-criada especificamente para a região da CEDEAO.

Introdução

Um foco central dos esforços da CEDEAO tem sido nas áreas da cibersegurança e do cibercrime. Em 2021, por exemplo, a CEDEAO adotou a sua *Estratégia Regional para a Cibersegurança e o Cibercrime*, delineando ações a adotar ao nível nacional para "aumentar a resiliência cibernética na região, ajudar os Estados-Membros a fortalecer as suas capacidades no âmbito da cibersegurança, proteger o seu ciberespaço e infraestruturas de informação críticas, bem como desenvolver confiança e segurança na utilização de tecnologias de informação e comunicação (TIC).[9] Incluídas entre as ações sugeridas a tomar estão "a adoção de estratégias nacionais para a cibersegurança, desenvolver capacidades e avanços na área da cibersegurança e priorizar os esforços de cibersegurança para infraestruturas críticas e serviços essenciais."[10]

A Estratégia da CEDEAO assinala que "a rápida transformação digital em curso na África Ocidental reveste-se de grande importância para melhorar a funcionalidade e a eficiência das administrações, políticas e economias públicas, bem como o bem-estar das populações."[11] É facto estabelecido que uma infraestrutura digital segura e estável é necessária para o crescimento económico sustentável na região da CEDEAO. Entre outros aspetos, servirá de incentivo para o investimento financeiro, aumentará o desenvolvimento empresarial, melhorará a eficiência operacional e a produtividade, protegerá infraestruturas críticas, capacitará serviços governamentais essenciais, fornecerá acesso a mercados globais e, talvez o mais importante, promoverá a confiança na segurança digital da região junto dos consumidores, empresas e investidores para impulsionar o crescimento económico.

Em contrapartida, o rápido crescimento da economia da região da CEDEAO e a expansão do rasto digital tornam-na um alvo cada vez mais atrativo de agentes de ameaças cibernéticas. Constata-se o aumento das preocupações em relação às falhas de cibersegurança da região que podem impedir que as capacidades acompanhem o ritmo das ameaças crescentes, tornando a região progressivamente mais vulnerável a ataques.

Este relatório foi elaborado pela The Shadowserver Foundation ("Shadowserver") no âmbito do projeto de reforço de capacidades em cibersegurança ao abrigo da parceria CEDEAO-G7 para cibersegurança, a "Joint Platform for Advancing Cyber Security" (JPAC - Plataforma Conjunta para o Avanço da Cibersegurança) na África Ocidental. O projeto foi lançado pela Comissão da CEDEAO em colaboração com a presidência alemã do G7 em 2022 e nomeado pelo Ministério Federal dos Negócios Estrangeiros da Alemanha e pela Comissão da União Europeia em 2023.

[9] "Information and Communication Technology: ECOWAS adopts a Regional Strategy for Cybersecurity and the fight against Cybercrime,"*Official Website of the ECOWAS Parliament*, 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,"*The Business Continuity Institute (BCI) Western Africa Chapter*, https://www.thebci.org/news/digital-transformation-development-and-resilience-in-west-africa.html

[11] "Introduction: ECOWAS Regional Cybersecurity and Cybercrime Strategy," *ECOWAS Cyberportal*, https://cyberportal.ecowas.int/wpfd_file/ecowas-regional-cybersecurity-cybercrime-strategy-en/

O foco geográfico deste relatório é a região da CEDEAO e os respetivos doze (12) estados-membros, nomeadamente, Benim, Cabo Verde, Costa do Marfim, Gâmbia, Gana, Guiné, Guiné-Bissau, Libéria, Nigéria, Senegal, Serra Leoa e Togo. As conclusões e recomendações baseiam-se na experiência de mais de 20 anos da Shadowserver na área, bem como na análise de dados relevantes para a região da CEDEAO durante o período de 1 de outubro de 2024 até 24 de abril de 2025.

Os objetivos do relatório são informar os líderes governamentais, decisores e outros principais intervenientes quanto ao seguinte:

o **cenário de ameaças cibernéticas*** e a **superfície de ataque*** da região da CEDEAO mediante a utilização das informações sobre ameaças acionáveis, a análise de dados e os insights de especialistas da Shadowserver para o período de tempo relevante

as **lacunas institucionais e operacionais no âmbito da cibersegurança** da região que a tornam cada vez mais vulnerável a ameaças cibernéticas

ações recomendadas que podem ser tomadas a nível nacional e regional para abordar as lacunas de cibersegurança identificada para melhorar a segurança digital e melhorar a resiliência cibernética na região da CEDEAO

o **potencial impacto económico e social** caso as lacunas institucionais e operacionais identificadas em termos de cibersegurança não sejam abordadas.

1.0// Insights da Shadowserver sobre Ameaças Cibernéticas na Região da CEDEAO

O atual **cenário de ameaças cibernéticas*** da região da CEDEAO caracteriza-se por ransomware, ataques a infraestruturas críticas, ataques de negação de serviço distribuído (DDoS), comprometimento de e-mail empresarial (BEC), fraudes e burlas online e extorsão sexual digital para citar alguns.

Um relatório da INTERPOL publicado em junho de 2025 adverte para um aumento acentuado do cibercrime em África. O relatório fornece uma análise exaustiva das atuais ameaças de cibercrime que afetam a África (incluindo especificamente a África Ocidental) e a sua leitura é recomendada para todos os principais intervenientes na região da CEDEAO. Devido ao facto das atuais ameaças cibernéticas que visam a região da CEDEAO estarem bem documentadas no relatório da INTERPOL e inúmeras outras fontes (por exemplo, o "Africa Cyberthreat Landscape Report 2025" (Relatório do Cenário de Ameaças Cibernéticas em África de 2025) da Kaspersky Labs), este relatório concentra-se menos nas várias e próprias ameaças cibernéticas e mais nas lacunas de cibersegurança que tornam a região vulnerável a estas ameaças. Não obstante, este relatório fornece ao leitor uma visão geral de elevado nível de determinadas ameaças para as quais a Shadowserver pode fornecer insights úteis.

1.1// Ransomware e extorsão através da fuga de dados

Ransomware* e os ataques de **extorsão através da fuga de dados*** relacionados continuam a ser problemas significativos na maioria das regiões do mundo e a região da CEDEAO não é exceção. Em novembro de 2022, foi reportado que hackers invadiram os sistemas digitais no Banco Central da Gâmbia e exigiram um pagamento de resgate de 2,5 milhões de dólares em troca dos dois terabytes de dados confidenciais roubados do banco.[12] Os dados roubados incluíam alegadamente as finanças pessoais de gambianos; dados relativos à economia nacional; bases de dados de clientes e parceiros; dados relativos ao volume de transações financeiras com os EUA e outros países; dados relacionados com a distribuição de títulos; e dados relativos à liquidez dos bancos comerciais do país. Tais ataques podem causar danos financeiros e reputacionais devastadores.

A Shadowserver recolhe informações sobre a atividade de vários grupos criminosos de ransomware. As informações são recolhidas através da observação sistemática de **sites dedicados à divulgação de fugas de dados*** dos grupos de ransomware. A Shadowserver alerta regularmente as CSIRT Nacionais e as Autoridades Policiais em todo o mundo relativamente a informações publicadas nos sites dedicados à divulgação de fugas de dados.

Em 2024 e 2025, a Shadowserver observou inúmeras reivindicações de grupos de ransomware conhecidos de ataques contra organizações na região da CEDEAO.

Agente	Local do país da vítima	Data publicada no local	Setor da vítima	Funcionários	Volume de negócios anual ($)
Blacksuit	Nigéria	Maio de 2024	Serviços profissionais, científicos e técnicos	766	1.090.000.000
	Gana	Outubro de 2024	Setor dos serviços públicos	405	29.700.000
Brain Cipher	Gana	Agosto de 2024	Setor financeiro e dos seguros	106	9.000.000
Hunters International	Costa do Marfim	Maio de 2024	Administração pública	1879	392.000.000
	Senegal	Setembro de 2024	Outros serviços	33	6.000.000
Kill Security	Nigéria	Novembro de 2024	Serviços profissionais, científicos e técnicos	N/A	N/A
	Gana	Fevereiro de 2025	Setor financeiro e dos seguros	N/A	N/A
	Nigéria	Março de 2025	Serviços administrativos e de apoio e gestão de resíduos e serviços de remediação	5578	306.800.000
LockBit 3.0	Costa do Marfim	Fevereiro de 2024	Serviços profissionais, científicos e técnicos	211	26.900.000
	Senegal	Maio de 2024	Serviços profissionais, científicos e técnicos	95	5.000.000
Lynx	Cabo Verde	Novembro de 2024	Setor financeiro e dos seguros	N/A	5.400.000
Pryx	Nigéria	Outubro de 2024	Desconhecido - 29 potenciais vítimas	N/A	N/A
RansomHub	Nigéria	Janeiro de 2025	Serviços profissionais, científicos e técnicos	1628	293.800.000
Space Bears	Costa do Marfim	Agosto de 2024	Serviços administrativos e de apoio e gestão de resíduos e serviços de remediação	105	N/A
Funksec	Nigéria	Janeiro de 2025	Informação	N/A	N/A
	Nigéria	Dezembro de 2024	Administração pública	19627	157.500.000
GDLockerSec	Nigéria	Janeiro de 2025	Administração pública	N/A	N/A
DragonRansomware	Costa do Marfim	Dezembro de 2024	Serviços administrativos e de apoio e gestão de resíduos e serviços de remediação	N/A	N/A

Figura 01. **Agentes de ransomware com reivindicações de vítimas nos estados da CEDEAO (janeiro de 2024 - maio de 2025)**

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

Contudo, devido ao facto das organizações que pagam o resgate não serem normalmente identificadas no site dedicado à divulgação de fugas de dados, não existe forma de saber definitivamente o número total de ataques de ransomware num determinado país ou região. No entanto, prevê-se que ataques de ransomware e de extorsão através da fuga de dados na região da CEDEAO aumentem à medida que o crescimento económico e a expansão digital continuam a superar as capacidades de cibersegurança.

A Figura 01 abaixo contém um resumo de informações relativas a vítimas de ransomware na região da CEDEAO recolhidas a partir de sites dedicados à divulgação de fugas de dados de grupos de ransomware. Os nomes reais das vítimas e URL associados foram removidos para preservar o anonimato das vítimas. De notar que a Shadowserver pode não observar todos os sites dedicados à divulgação de fugas de dados existentes, especialmente os associados a agentes de ameaças com um foco mais a nível regional.

Conforme observado na Figura 01, as reivindicações dizem respeito a uma variedade de setores, tanto públicos como privados. A maioria das reivindicações estão relacionadas com a Nigéria, Costa do Marfim e Gana.

Os ataques de ransomware podem causar interrupções onerosas a operações e a perda de informações e dados críticos. À medida que as empresas continuam a se desenvolver e as economias continuam a crescer na região da CEDEAO, é provável que os ataques de ransomware aumentem. Se a segurança digital na região não conseguir acompanhar o ritmo do atual crescimento económico, os resultados podem ser graves com o constante aumento do cibercrime e o declínio significativo no desenvolvimento empresarial e investimento financeiro na região.

1.2// Ataques a infraestruturas críticas

Os ataques cibernéticos contra redes de **infraestruturas críticas*** assumem muitas formas, dependendo normalmente da natureza e das motivações do perpetrador do ataque. Por exemplo, os agentes de ameaças ao estado-nação podem tentar invadir redes de infraestruturas críticas para fins de espionagem, danos destrutivos ou a formulação de declarações políticas, enquanto os grupos de cibercrime transnacionais utilizam ransomware para fins de ganhos monetários.

Em 2022, a Electricity Company of Ghana (ECG - Empresa de Eletricidade do Gana), o maior fornecedor de eletricidade do país, foi vítima de um ataque de ransomware. Conforme reportado, o ataque deixou os clientes sem eletricidade e/ou impossibilitados de adquirir eletricidade por vários dias como resultado dos perpetradores do ataque encriptarem várias secções do sistema da ECG, tornando-a inoperacional.[13] O diretor-geral da ECG confirmou mais tarde que o ataque de ransomware resultou numa perda de quase 500 milhões de GH¢ (aproximadamente 40 milhões de EUR ou 47 milhões de USD).[14]

Em dezembro de 2024, o Instituto Nacional de Estatística (NBS) da Nigéria foi alvo de um ciberataque que paralisou temporariamente os seus sistemas e perturbou a acesso público a dados nacionais críticos por quase um mês.[15] A invasão também suscitou preocupações quanto “à potencial exposição de dados críticos, incluindo relatórios económicos, dados estatísticos sobre a população e outras informações essenciais indispensáveis para o planeamento e a elaboração de políticas nacionais.”[16]

Estes exemplos ilustram o crescente foco dos agentes de ameaças cibernéticas em instituições nacionais e infraestruturas críticas, bem como o impacto social que pode resultar de tais ataques.

[13] “ECG Systems Hacked with Ransomware,” *Ghana Business News*, 1 de outubro de 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 de ago. de 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 de janeiro de 2025. https://techpoint.africa/news/nbs-to-resume-services-on-january-15/

[16] “Cyberattack Hits Nigeria’s Statistics Bureau,” *TechInAfrica*, 25 de dezembro de 2024. https://www.techinafrica.com/cyberattack-hits-nigerias-statistics-burea/

1.3// Negação de serviço distribuído (DDOS)

A Shadowserver recolhe dados de aproximadamente 2700 **sensores de honeypots*** que mantém em centros de dados e outros locais ao redor do mundo. Estes sensores são alvos falsos configurados para parecerem legítimos, contudo, vulneráveis, ativos de redes (incluindo aplicações de software, servidores e outros dispositivos) com a finalidade pretendida de atrair os agentes de ameaças a perpetrarem ataques. Os sensores registam as atividades do perpetrador do ataque e recolhem informações sobre as táticas, ferramentas e procedimentos/técnicas do perpetrador do ataque. Os dados recolhidos ajudam a identificar as origens dos ataques, novos métodos de ataque, a desenvolver defesas e a prevenir ataques futuros.

Através das observações dos nossos sensores de honeypots, a Shadowserver monitoriza várias formas de ataques de DDOS. Como resultado, somos capazes de rastrear as vítimas de ataques num determinado momento. Observamos a ocorrência regular de ataques de DDOS na região da CEDEAO, principalmente na Nigéria.

Como ilustrado nas Figuras 02 e 03, o país mais atacado (através de endereço IP de destino único e na maioria das tentativas) foi a Nigéria.

Os ataques de DDOS podem ser altamente perturbadores e extremamente onerosos para as empresas e os governos suportarem.

Em maio de 2023, um grupo de hackers designado Mysterious Team fez com que múltiplos websites do governo senegalês ficassem offline como resultado de um ataque de DDOS.[17]

Figura 02. **Ataques de DDOS através de endereço IP de destino único - Região da CEDEAO**

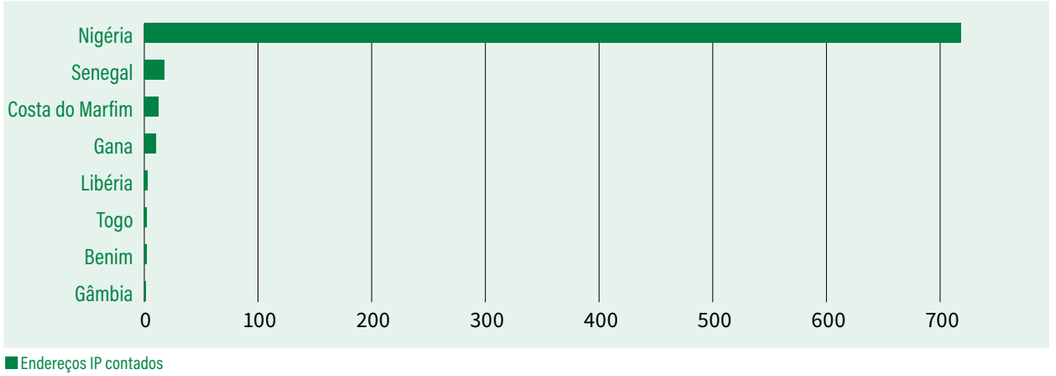
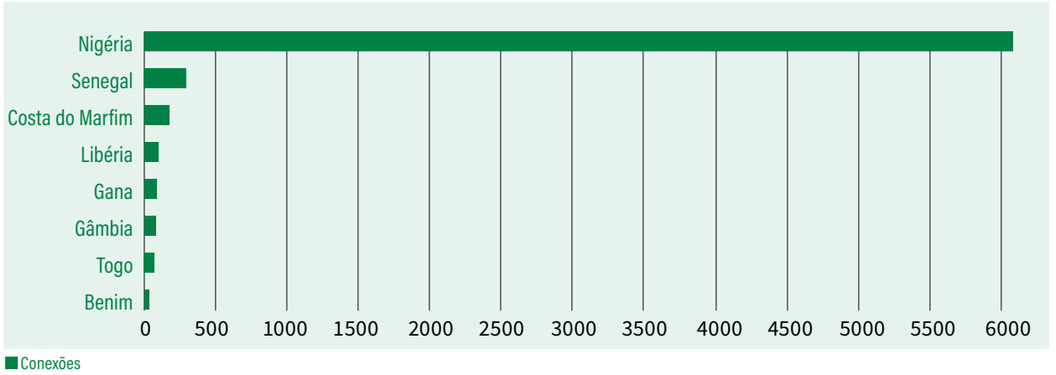


Figura 03. **Ataques de DDOS - através de tentativas únicas - Região da CEDEAO**



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

Em agosto de 2023, a maior operadora de telecomunicações da Nigéria, a MTN Nigeria, foi vítima de um dos maiores ataques de DDOS alguma vez registados contra uma empresa na África Ocidental. O ataque foi perpetrado por um famoso grupo de hacktivistas conhecido como Anonymous Sudan e durou quase oito horas dado que a rede da MTN foi inundada de tráfego malicioso proveniente de computadores comprometidos em todo o mundo num esforço de perturbar os serviços de voz e dados da MTN.[18]

Estes exemplos demonstram que os ataques de DDOS podem ter um impacto devastador na sociedade e impedem o crescimento empresarial e o desenvolvimento económico caso não sejam abordados. Deve-se delinear e implementar estratégias abrangentes de proteção e atenuação de DDOS a nível nacional e regional.

1.4// Comprometimento de e-mail empresarial (BEC)

As burlas por Comprometimento de E-mail Empresarial (BEC) estão a aumentar na região da CEDEAO, conforme reportado. Em julho de 2024, o Departamento Nacional de Tecnologias de Informação (NITDA) da Nigéria publicou um alerta nacional a advertir para as taxas alarmantes de burlas de BEC que afetam indivíduos e organizações em todo o território da Nigéria.[19]

Adicionalmente, embora os detalhes sejam limitados e o evento não tenha sido amplamente reportado, o recente anúncio da Operação Sentinel da INTERPOL incluiu a referência a uma importante empresa petrolífera no Senegal que "detetou uma sofisticada burla de BEC na qual os burlões se infiltraram nos sistemas de e-mail internos e fizeram-se passar por executivos para autorizar uma transferência bancária fraudulenta de 7,9 milhões de USD." O anúncio registou que as autoridades senegalesas congelaram imediatamente as contas de destino e impediram com sucesso a transação antes que os fundos pudessem ser levantados.

Táticas de BEC menos sofisticadas incluem burlões menos sofisticados que criam endereços de e-mail e domínios falsos semelhantes aos legítimos para enganar os destinatários. Táticas de BEC mais sofisticadas incluem burlões que invadem um servidor de e-mail ou obtêm acesso não autorizado à conta de e-mail de um funcionário através de phishing ou malware e enviam pedidos de pagamento de faturas para fornecedores listados nos contactos de e-mail do funcionário. Embora evitar que um funcionário se torne vítima de uma burla de BEC dependa principalmente de formação e educação, a proteção dos servidores e contas de e-mail é também extremamente importante à medida que as burlas de BEC se tornam mais sofisticadas.

[18] "Inside the Eight-Hour Long Cyberattack that Tried to Cripple MTN Nigeria," *Techcabal*, 9 de julho de 2025. https://techcabal.com/2025/07/09/cyberattack-that-tried-to-cripple-mtn-nigeria/

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

2.0// Lacunas institucionais de cibersegurança e recomendações

2.1// Equipas Nacionais de Resposta a Incidentes de Segurança Informática (CSIRT nacionais)

Dois Estados-Membros da CEDEAO não têm atualmente uma CSIRT Nacional definida.

O estabelecimento de uma CSIRT Nacional em cada nação da CEDEAO é um primeiro passo crítico para garantir uma nação (e região) mais cibersegura e deve ser uma prioridade máxima.

O principal desafio, contudo, será assegurar que todas as CSIRT Nacionais da região sejam eficazes a realizar os respetivos deveres e responsabilidades. As recomendações contidas no presente incidem sobre as formas de tornar as CSIRT Nacionais, e entidades semelhantes como os ISAC (Centros de Partilha e Análise de Informação) e as CSIRT Sectoriais, mais eficazes.

RECOMENDAÇÃO:
Estabelecer uma CSIRT Nacional operacionalmente eficaz em cada Estado-membro da CEDEAO.

2.2// ISAC (Centro de partilha e análise de informação) DA CEDEAO

Um Centro de Partilha e Análise de Informação (ISAC) é uma organização orientada pelos membros que recolhe, analisa e dissemina informações sobre ameaças acionáveis para ajudar os membros a atenuar os riscos de forma proativa. A Shadowserver tem conhecimento de que um ISAC (Centro de Partilha e Análise de Informação) da CEDEAO está a ser planeado no momento. A iniciativa visa fortalecer a cibersegurança regional ao criar uma plataforma colaborativa para partilhar informações sobre ameaças, as melhores práticas e recursos entre as nações da África Ocidental. Ao contrário de uma CSIRT Nacional, os custos operacionais associados a um ISAC (Centro de Partilha e Análise de Informação) regional da CEDEAO podem ser partilhados entre os estados-membros.

A Shadowserver fornece informações sobre ameaças cibernéticas diárias gratuitas a 201 CSIRT Nacionais responsáveis por 175 países para ajudá-las a proteger as respetivas redes nacionais. Uma CSIRT Nacional eficaz é essencial para alcançar maior resiliência cibernética num país.

Serve como autoridade central do país para dar resposta e gerir incidentes de cibersegurança a nível nacional, proteger a infraestrutura crítica nacional, prestar orientação e consultoria aos setores público e privado e facilitar a cooperação para eventos cibernéticos transfronteiriços.

As principais responsabilidades de uma CSIRT Nacional incluem a deteção e análise de incidentes, a resposta a incidentes e a respetiva remediação, a partilha de informação e disseminação de alertas/informações sobre ameaças/consultorias, coordenação com agências domésticas e contrapartes internacionais e implementação de medidas preventivas num país.

RECOMENDAÇÃO:
O estabelecimento de um ISAC (Centro de Partilha e Análise de Informação) da CEDEAO é altamente recomendável e será crucial para ajudar a garantir que todas as CSIRT Nacionais da região trabalham colaborativamente, partilham informações e progridem no respetivo desenvolvimento. Um ISAC (Centro de Partilha e Análise de Informação) da CEDEAO ajudará também a promover parcerias regionais com entidades como os fornecedores de serviços de Internet (FSI) e operadores de infraestruturas críticas, bem como parcerias internacionais com CSIRT Nacionais. Ao contrário de uma CSIRT Nacional, os custos operacionais e de desenvolvimento associados a um ISAC (Centro de Partilha e Análise de Informação) regional da CEDEAO podem ser partilhados entre os estados-membros.

2.3// CSIRT Sectoriais

Uma CSIRT Sectorial é uma entidade especializada que gere a resposta a incidentes de cibersegurança, promove a partilha de informações para atenuar ameaças e oferece conhecimento especializado e competências técnicas para um setor particular de um país ou economia (por exemplo, água, saúde, energia, financeiro, transportes, etc.). Serve para prevenir e responder eficazmente a ameaças únicas para o respetivo setor. A proteção de infraestruturas críticas e de serviços governamentais deve ser priorizada. Uma das formas de implementar esta medida é através do desenvolvimento de CSIRT Sectoriais para cada setor de infraestruturas críticas. Na sequência do estabelecimento de uma CSIRT Nacional, as CSIRT Sectoriais devem ser criadas à medida que o financiamento disponível o permita, começando pelo setor identificado como o mais crítico. Após o estabelecimento, a criação de CSIRT Sectoriais adicionais podem então ser implementadas em larga escala entre os vários setores com o passar do tempo.

RECOMENDAÇÃO:
Na sequência do estabelecimento de uma CSIRT Nacional eficaz em cada estado-membro, deve ser criada uma CSIRT Sectorial para o setor de infraestruturas críticas identificado como o mais vulnerável e mais crucial para proteger em cada país. À medida que o financiamento disponível o permita, podem ser estabelecidas CSIRT Sectoriais subsequentes noutros setores. Isto ajudará a garantir que cada setor de infraestruturas críticas recebe competências técnicas, informações sobre ameaças, gestão de riscos e serviços de resposta a incidentes de acordo com as necessidades únicas do respetivo setor.

2.4// Acesso a dados, ferramentas e serviços gratuitos/acessíveis

É imperativo que as CSIRT Nacionais, as CERT Sectoriais, os ISAC (Centros de Partilha e Análise de Informação) e os especialistas em proteção de redes de todos os tipos e entre todos os setores tenham acesso a dados, ferramentas, serviços e plataformas de qualidade sobre ameaças cibernéticas necessários para executar adequadamente os respetivos deveres e funções. Isso inclui as ferramentas necessárias para ingerir adequadamente, armazenar, interpretar, pesquisar, visualizar, analisar e utilizar eficazmente os dados sobre ameaças cibernéticas. As plataformas automáticas são também necessárias para disseminar notificações de alertas para proprietários de redes de partes interessadas afetadas sobre vulnerabilidades críticas e ativos comprometidos para garantir a correção oportuna.

Infelizmente, o financiamento disponível limitado e os elevados custos associados a muitos destes itens representam um desafio significativo. Contudo, estão disponíveis dados, ferramentas, serviços e plataformas gratuitos ou, de outra forma, acessíveis e todos os especialistas em proteção de redes devem beneficiar plenamente destes recursos valiosos para os ajudar a proteger as suas redes de forma adequada.

Lacunas institucionais de cibersegurança e recomendações

Na região da CEDEAO, por exemplo, as CSIRT Nacionais no Benim, Costa do Marfim, Gâmbia, Gana, Nigéria, Serra Leoa e Togo subscrevem todas os relatórios diários e gratuitos de remediação de redes da Shadowserver para as ajudar a proteger as redes dos respetivos países. Estes relatórios fornecem a cada CSIRT Nacional dados nacionais associados a todos os IP cuja geolocalização corresponde aos respetivos países. Os relatórios identificam dispositivos expostos, passíveis de abuso, configurados incorretamente, vulneráveis e comprometidos para serem corrigidos ou, de outra forma, remediados antes de poderem ser explorados (ou continuar a ser explorados) por agentes de ameaças cibernéticas. Cabe a cada CSIRT Nacional a responsabilidade de utilizar os relatórios para disseminar notificações de alerta para proprietários de redes afetadas por todo o país.

Os proprietários de redes individuais de todos os tipos e entre todos os setores (por exemplo, bancos, hospitais, fornecedores de serviços de Internet, universidades, organizações sem fins lucrativos e ONG, pequenas a grandes empresas, governos locais/estatais, etc.) também podem subscrever para receberem *diretamente* relatórios de remediação de redes da Shadowserver associados às respetivas redes individuais. Em conformidade, o uso de relatórios diários gratuitos de remediação de redes da Shadowserver deve ser expandido a todos os especialistas em proteção de redes da região, em particular aos do governo, infraestruturas críticas, fornecedores de telecomunicações e fornecedores de serviços de Internet, entre outros.

Estão disponíveis ferramentas de código aberto gratuitas, incluindo IntelMQ, Elasticsearch, Kibana e outras para ajudar a ingerir, armazenar, interpretar, pesquisar, visualizar e analisar fluxos de dados sobre ameaças do Shadowserver e outros. Estão também disponíveis muitas ferramentas comerciais acessíveis. Por exemplo, a Arctic Hub, uma plataforma de automação de informações sobre ameaças cibernéticas que recolhe, harmoniza e distribui dados sobre ameaças de inúmeros fluxos, está disponível gratuitamente no primeiro ano e nos anos subsequentes mediante taxas reduzidas para CSIRT Nacionais qualificadas através do Programa de Desenvolvimento de CSIRT da Arctic Security. Tal como apresentado no website da Arctic Security, a CSIRT Nacional da Gâmbia (gmCSIRT) é uma atual participante no programa.

RECOMENDAÇÃO:
CSIRT Nacionais e especialistas em proteção de redes de todos os tipos e entre todos os setores devem beneficiar de dados, ferramentas, serviços e plataformas gratuitos e/ou acessíveis que estejam disponíveis. Tal inclui relatórios de remediação de redes diários e gratuitos da Shadowserver, bem como ferramentas de código aberto gratuitas (incluindo IntelMQ, Elasticsearch, Kibana e outras) necessários para ingerir, armazenar, interpretar, pesquisar, visualizar, analisar e utilizar eficazmente a Shadowserver e outros fluxos de dados de ameaças. Deve igualmente considerar-se ferramentas comerciais potencialmente acessíveis. Por exemplo, a Arctic Hub, uma plataforma de automação de informações sobre ameaças cibernéticas que recolhe, harmoniza e distribui dados sobre ameaças de inúmeros fluxos, está disponível gratuitamente no primeiro ano e nos anos subsequentes mediante taxas com desconto para CSIRT Nacionais qualificadas através do Programa de Desenvolvimento de CSIRT da Arctic Security. A CSIRT Nacional da Gâmbia (gmCSIRT) é atualmente participante no programa.

2.5// Competência técnica interna

A disponibilidade de dados, ferramentas e serviços sobre ameaças gratuitos ou, de outra forma, acessíveis exigem, contudo, competência técnica interna capaz de utilizá-los eficazmente. A Shadowserver deparou-se com algumas CSIRT Nacionais e outras entidades cujos funcionários carecem de competências técnicas para utilizar eficazmente os dados, ferramentas e serviços.

A contratação e manutenção de funcionários com o conhecimento técnico necessário pode ser desafiador, particularmente para CSIRT Nacionais, CSIRT Sectoriais e outras entidades governamentais incapazes de competir com a maioria dos salários do setor privado. Para abordar esta questão, é recomendável que os Estados-Membros da CEDEAO colaborem com as universidades para desenvolver programas de formação e de estágios capazes de atuar como uma pipeline para trazer talentos inexperientes mas tecnicamente competentes para o governo. É também recomendável que os estados-membros colaborem com o setor privado para desenvolver programas nos quais especialistas técnicos experientes do setor privado possam desempenhar funções temporárias nas CSIRT Nacionais e em entidades governamentais/de infraestruturas críticas para prestar mentoria e formar funcionários menos experientes e menos técnicos.

RECOMENDAÇÃO:
Assegurar que cada CSIRT Nacional e especialistas em proteção de redes do governo e sistemas de infraestruturas críticas têm funcionários que possuem competências técnicas adequadas para proteger e defender eficazmente as redes do país. Os Estados-Membros da CEDEAO devem colaborar com as universidades para desenvolver programas de formação e de estágios que possam atuar como um pipeline de talentos tecnicamente qualificados. Os Estados-Membros devem também colaborar com o setor privado para desenvolver programas nos quais especialistas experientes do setor privado possam desempenhar funções temporárias, embora de longa duração nas CSIRT Nacionais e em entidades governamentais/de infraestruturas críticas para prestar mentoria e formar funcionários menos experientes e menos técnicos.

2.6// Formação e desenvolvimento de capacidades

A falta de competência técnica interna disponível também pode ser abordada através da assistência, formação e serviços de desenvolvimento de capacidades geralmente disponíveis através de projetos formais financiados por ministérios de negócios estrangeiros (incluindo o Ministério Federal dos Negócios Estrangeiros da Alemanha e o GIZ e o Ministério dos Negócios Estrangeiros, da Commonwealth e do Desenvolvimento do Reino Unido), entidades do setor privado (incluindo a Microsoft e a Google), bem como o Banco Mundial, as Nações Unidas e a União Europeia, para citar alguns.

Por exemplo, para além do atual projeto da CEDEAO financiado pelo Ministério Federal dos Negócios Estrangeiros da Alemanha e implementado pelo GIZ, o Ministério dos Negócios Estrangeiros, da Commonwealth e do Desenvolvimento do Reino Unido (FCDO do RU) financiou inúmeros projetos de desenvolvimento de capacidades cibernéticas em África, incluindo projetos com a Shadowserver.

Muitos projetos de desenvolvimento de capacidades cibernéticas incluem oportunidades de formação presencial e remota. Por exemplo, em novembro de 2024, a Shadowserver estabeleceu uma parceria com o FIRST e ministrou uma formação de um dia intitulada “Maximizar os Fluxos Diários Gratuitos da Shadowserver e Outros Serviços Comunitários através da Automação” no Simpósio FIRST e AfricaCERT: África e Regiões Árabes em Livingston, Zâmbia.

RECOMENDAÇÃO:
Procurar oportunidades para projetos de formação e desenvolvimento de capacidades (em particular projetos operacionais focados em configurar e utilizar eficazmente dados, ferramentas, serviços e plataformas gratuitas/de código aberto que estejam disponíveis). Tais projetos são frequentemente financiados por ministérios de negócios estrangeiros (incluindo o Ministério Federal dos Negócios Estrangeiros da Alemanha e o GIZ e o Ministério dos Negócios Estrangeiros, da Commonwealth e do Desenvolvimento do Reino Unido), entidades do setor privado (incluindo a Microsoft e a Google), bem como o Banco Mundial, as Nações Unidas e a União Europeia, para citar alguns.

2.7// Desenvolvimento de parcerias

É também imperativo que as CSIRT Nacionais na região da CEDEAO desenvolvam relações com as partes interessadas/intervenientes nos respetivos países (por exemplo, fornecedores de serviços de Internet, fornecedores de telecomunicações, infraestruturas críticas e outros grandes proprietários de redes), bem como com CSIRT Nacionais membros da região da CEDEAO e de todo o mundo. Estas relações são cruciais para criar um ambiente que promova a colaboração e a partilha de informações. Por exemplo, as relações de trabalho estreitas com as partes interessadas/intervenientes no respetivo país permitem que uma CSIRT Nacional dissemine rapidamente alertas de ameaças à segurança sobre ativos vulneráveis e comprometidos para proprietários de redes, permitindo-lhes corrigir e remediar antes que possa ocorrer a exploração por parte de agentes de ameaças.

Relações sólidas com CSIRT Nacionais membros são igualmente importantes, dado que promovem a partilha de informação, a colaboração e o desenvolvimento de capacidades. Existem muitas oportunidades para desenvolver estas relações profissionais. Por exemplo, a Shadowserver oferece às CSIRT Nacionais acesso gratuito à sua plataforma de conversação online Alliance Mattermost na qual os funcionários da Shadowserver, Parceiros da Alliance de todo o setor e CSIRT Nacionais de todo o mundo partilham e recebem as mais recentes informações sobre inteligência de ameaças e trabalham colaborativamente para abordar ameaças emergentes.

As CSIRT Nacionais devem também envidar esforços para se tornarem membros do FIRST, o Fórum Global de Equipas de Resposta a Incidentes e Segurança. O FIRST é uma organização de membros líder para CSIRT Nacionais na arena de resposta a incidentes e segurança. A adesão ao FIRST permite que as equipas de resposta a incidentes respondam com mais eficácia a incidentes de segurança. O FIRST reúne uma variedade de equipas de resposta a incidentes de segurança informática de organizações governamentais, comerciais e educacionais. Visa promover a cooperação e a coordenação na prevenção de incidentes, estimular a reação rápida a incidentes e promover a partilha de informações entre os membros e a comunidade em geral. Para além da rede de confiança que o FIRST disponibiliza na comunidade global de resposta a incidentes, o FIRST oferece também inúmeros serviços a CSIRT Nacionais. Atualmente, o FIRST conta com mais de 800 membros, distribuídos por África, as Américas, Ásia, Europa e Oceânia. Conforme ilustrado na Figura 4 abaixo, entre os países da CEDEAO, apenas o Benim, Gana, Costa do Marfim, Nigéria e Togo têm CSIRT Nacionais que são membros do FIRST.

RECOMENDAÇÃO:
Criar um quadro de referência que exija que as CSIRT Nacionais estabeleçam e mantenham relações profissionais sólidas com partes interessadas/intervenientes nos respetivos países (incluindo prestadores de serviços de Internet, operadores de infraestruturas críticas, entidades governamentais, empresas, universidades, governos estaduais e locais, prestadores de cuidados de saúde, instituições financeiras, etc.), bem como com CSIRT Nacionais na região da CEDEAO e em todo o mundo. Estas relações são cruciais para promover a partilha de informações, a colaboração e o desenvolvimento de capacidades. As oportunidades para as CSIRT Nacionais desenvolverem parcerias globais incluem através de um ISAC da CEDEAO, tornando-se membro do FIRST.org, e aderindo à plataforma de

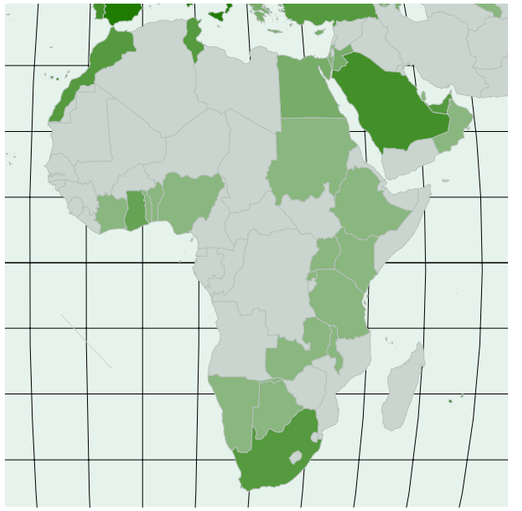


Figura 04. **Mapa das nações africanas cujas CSIRT Nacionais são atuais membros do FIRST**

conversação Alliance Mattermost online gratuita da Shadowserver que permite o acesso direto aos funcionários da Shadowserver, Parceiros da Alliance de todo o setor e CSIRT Nacionais de todo o mundo.

2.8// Avaliações de maturidade

Para ajudar no seu desenvolvimento, cada CSIRT Nacional deve ter uma avaliação de referência do respetivo nível de maturidade. A Open CSIRT Foundation criou o Modelo de Maturidade de Gestão de Incidentes de Segurança (SIM3) como quadro de referência que ajuda as organizações a medir e melhorar as suas funções na equipa de resposta a incidentes de cibersegurança. Avalia as equipas entre 44 parâmetros em quatro principais áreas: Organização, Recursos Humanos, Ferramentas e Processos. Em seguida, determina o nível de maturidade numa escala de 0 (Não Disponível: que se traduz pela inexistência de capacidades) a 4 (Auditado Explicitamente: que se traduz pela formalização de capacidades, auditado regularmente e alvo de melhoria contínua através de governança formal). A Open CSIRT Foundation desenvolveu uma ferramenta online de autoavaliação SIM3 para todos os tipos de CSIRT.

RECOMENDAÇÃO:
Para estabelecer um nível de maturidade inicial, cada CSIRT Nacional deve ser mandatada para passar pela avaliação da ferramenta online de autoavaliação do Modelo de Maturidade de Gestão de Incidentes de Segurança (SIM3) da Open CSIRT Foundation e implementar recomendações para melhoria.

2.9// Serviços de alerta precoce

As empresas e outros proprietários de redes distribuídos por um país podem desconhecer que dispõem de dados diários e gratuitos sobre ameaças diretamente de organizações de cibersegurança como a Shadowserver para os ajudar a proteger as suas redes. Uma forma de superar esta situação é as CSIRT Nacionais, CSIRT Sectoriais, ISAC (Centros de Partilha e Análise de Informação) e outras entidades com grandes grupos destinatários desenvolverem e divulgarem os seus próprios Serviços de Alerta Precoce através da utilização dos dados gratuitos sobre ameaças cibernéticas da Shadowserver (sob a forma de relatórios de remediação de redes) e dos dados sobre ameaças disponíveis de outras fontes. As organizações constituintes fornecem os respetivos endereços IP públicos e nomes de domínio às CSIRT Nacionais (ou outra autoridade). Por sua vez, recebem notificações automáticas de alerta sobre dispositivos e serviços expostos, vulneráveis e comprometidos na sua rede para facilitar a remediação oportuna, à semelhança do que receberiam caso subscrevessem os relatórios da Shadowserver. Embora existam muitos, dois desses exemplos são os Serviços de Alerta Precoce oferecidos pelo Centro Nacional de Cibersegurança do Reino Unido (NCSC do Reino Unido) e o CSIRT-RD da República Dominicana.

RECOMENDAÇÃO:
As CSIRT Nacionais, CSIRT Sectoriais, ISAC (Centros de Partilha e Análise de Informação) e outras entidades com grandes grupos de destinatários devem ser mandatados para oferecerem Serviços de Alerta Precoce gratuitos aos respetivos grupos de destinatários através da utilização de dados gratuitos sobre ameaças cibernéticas da Shadowserver e de outras fontes disponíveis. As organizações constituintes fornecem os respetivos endereços IP públicos da rede e nomes de domínio e, por sua vez, recebem notificações de alerta automáticas sobre dispositivos e serviços expostos, configurados incorretamente, passíveis de abuso, vulneráveis e comprometidos nas respetivas redes para facilitar a remediação oportuna. A consulta com uma das inúmeras CSIRT Nacionais que operam tais Serviços de Alerta Precoce é recomendada, como o Centro Nacional de Cibersegurança do Reino Unido (NCSC do Reino Unido) e o CSIRT-RD da República Dominicana.

3.0// Lacunas operacionais de cibersegurança e recomendações: Superfície de ataque da região da CEDEAO

Uma "**superfície de ataque***" refere-se a todos os pontos fracos possíveis, ou vetores de ataque, que podem ser explorados por um agente de ameaça para obter acesso não autorizado a um sistema ou rede. Embora alguns vetores de ataque se baseiem em erro humano (por exemplo, **phishing***; engenharia social), muitos baseiam-se em falhas técnicas numa rede (por exemplo, ativos configurados incorretamente e expostos; **vulnerabilidades sem correção***; **vulnerabilidades de dia zero***; **ativos comprometidos***; etc.)

A Shadowserver recolhe e analisa dados volumosos sobre ameaças cibernéticas à escala da Internet através da utilização de uma variedade de meios técnicos explicados abaixo. Depois partilha esses dados gratuitamente todos os dias com mais de 9000 organizações e proprietários de redes em todo o mundo (isto é, hospitais, universidades e distritos escolares, organizações sem fins lucrativos e não-governamentais, governos federais/estatais/locais, pequenas e médias empresas, empresas da Fortune 500, fornecedores de serviços de Internet, instituições financeiras, fornecedores de infraestruturas críticas e muitos outros).
A Shadowserver fornece também dados gratuitos, diários, de âmbito nacional sobre ameaças a Equipas Nacionais de Resposta a Incidentes de Segurança Informática (CSIRT Nacionais) designadas com responsabilidades específicas de prevenção e resposta a incidentes em 175 países, incluindo em África e, mais relevante para este relatório, muitos Estados-Membros da CEDEAO.

Os dados sobre ameaças partilhados pela Shadowserver encontram-se sob a forma de relatórios de remediação de redes. Estes relatórios atuam como um Serviço de Alerta Precoce, identificando dispositivos expostos, configurados incorretamente e vulneráveis numa rede a corrigir antes que os agentes de ameaça possam invadir a rede, *e* um Serviço de Notificação à Vítima, identificando dispositivos comprometidos numa rede a ser remediada antes que possa ocorrer mais exploração, tal como um ataque de ransomware. Os dados recolhidos podem ajudar a esclarecer a superfície de ataque da região da CEDEAO.

3.1// Dados de varrimento

A Shadowserver realiza o varrimento diário de portas mais de 150 vezes por dia para **endereços de Protocolo de Internet (IP)*** publicamente expostos/roteáveis; nomeadamente, aproximadamente 3,7 mil milhões de endereços IPv4 e listas de ocorrências de aproximadamente dois mil milhões de endereços IPv6 observados em ambiente real. Os dados de varrimento são utilizados para notificar as CSIRT Nacionais e os proprietários de redes em todos os setores sobre dispositivos expostos, passíveis de abuso, configurados incorretamente, vulneráveis e, por vezes, comprometidos para serem corrigidos ou, de outra forma, remediados antes de poderem ser explorados (ou continuar a ser explorados) por agentes de ameaças.

Os agentes de ameaças realizam, muitas vezes, o seu próprio varrimento ou adquirem dados de varrimento de fornecedores comerciais para identificar redes a visar para perpetrar o ataque. Em conformidade, os dados de varrimento gratuitos da Shadowserver são uma ferramenta essencial que permitem que as CSIRT Nacionais e os proprietários de redes vejam o que os agentes de ameaças veem sobre as suas redes, incluindo formas de obter acesso não autorizado e potencialmente explorar as redes.

Uma análise dos **dados de varrimento** da Shadowserver é importante para identificar o seguinte:

a dispositivos e serviços publicamente expostos (por vezes, desnecessariamente) à Internet que aumentam desnecessariamente uma superfície de ataque

b vulnerabilidades críticas em ativos expostos

c ativos expostos comprometidos

3.1a// DISPOSITIVOS E SERVIÇOS PUBLICAMENTE EXPOSTOS À INTERNET

Dispositivos* e **serviços*** publicamente expostos à Internet são vetores de ataque comuns para agentes de ameaças tentarem invadir uma rede. Contudo, muitos proprietários de redes não conhecem totalmente todos os ativos nas respetivas redes porque não mantêm um inventário atualizado dos seus ativos.

A execução de um **inventário de ativos*** é crucial para compreender uma superfície de ataque e melhorar a resiliência cibernética ao servir dois propósitos principais:

1. Permite que um proprietário de redes conheça o fornecedor, tipo, modelo e localização de dispositivos publicamente expostos numa rede que, por sua vez, permita a rápida correção e remediação quando novas vulnerabilidades nesses dispositivos e software relacionado são detetadas e publicamente anunciadas.
2. Permite que os proprietários de redes reduzam a sua superfície de ataque global ao remediar dispositivos e serviços expostos desnecessariamente à Internet.

Orientações úteis sobre como implementar os regulamentos que mandatam a realização de inventários de ativos por agências governamentais federais encontram-se disponíveis em "Diretiva Operacional Vinculativa 23-01: Melhorar a Visibilidade de Ativos e a Deteção de Vulnerabilidades nas Redes Federais" com a supervisão da Agência de Cibersegurança e Segurança de Infraestruturas do Departamento de Segurança Interna dos Estados Unidos (DHS-CISA). A diretiva exige que os departamentos e agências federais, poder executivo, entre outras coisas, executem uma descoberta automática de ativos (inventário) a cada 7 dias. Exige ainda que estes "iniciem a enumeração de vulnerabilidades entre todos os ativos descobertos, incluindo dispositivos nómadas/de roaming descobertos (por exemplo, computadores portáteis), a cada 14 dias.

A Shadowserver mantém assinaturas de deteção para *dispositivos*

expostos observados na região da CEDEAO como parte do nosso varrimento diário da Internet. Tal inclui a identificação do fornecedor, tipo e modelo de dispositivos publicamente expostos.

Como ilustrado na Figura 05, a Nigéria, Costa do Marfim e o Gana apresentam o volume mais elevado de dispositivos expostos na região da CEDEAO, consistente com a dimensão das respetivas infraestruturas IP.

O gráfico de barras na Figura 06 mostra os 20 Principais fornecedores por volume identificados em toda a região da CEDEAO, incluindo alguns fornecedores bem conhecidos como a Huawei, Fortinet, MikroTik e Cisco.

Figura 05. **Volume de identificação de dispositivos por país da CEDEAO** (resultados médios de varrimentos diários de 1 de outubro de 2024 até 24 de abril de 2025)

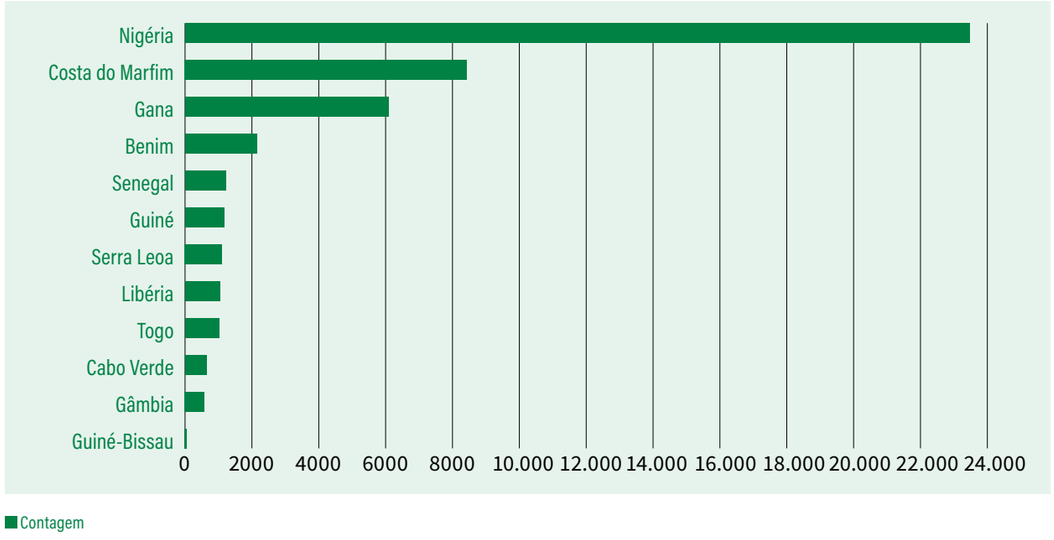
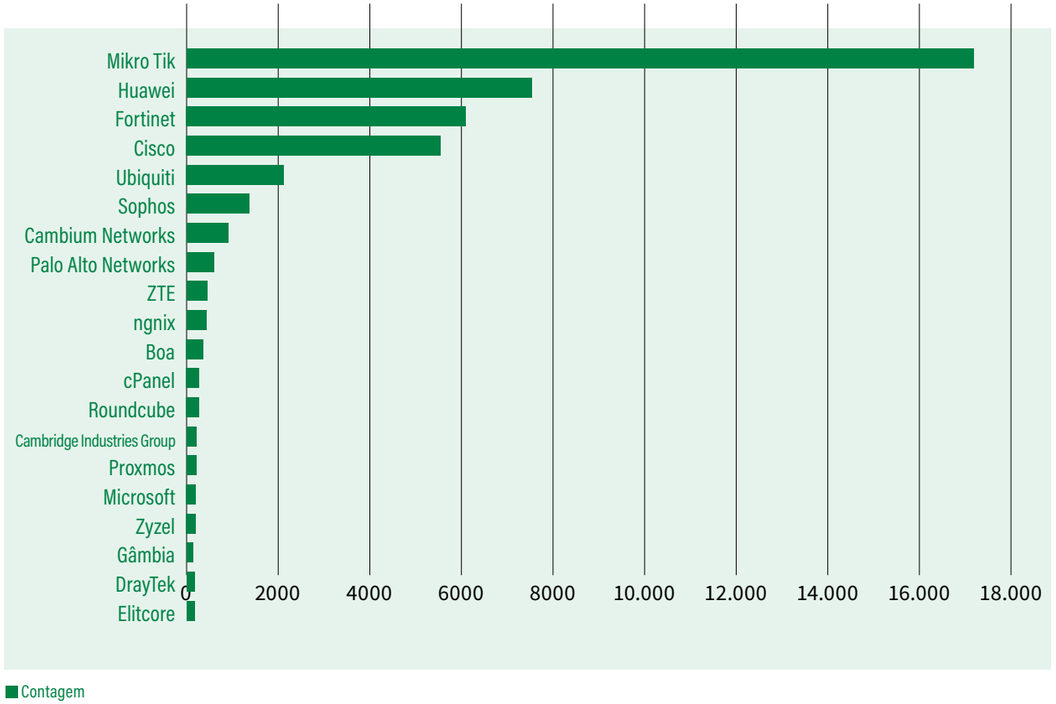


Figura 06. **20 Principais Fornecedores de Dispositivos encontrados em toda a Região da CEDEAO** (resultados médios de varrimentos diários)



Analisando o fornecedor com o maior volume, a MikroTik é de longe a escolha de router dos consumidores na região da CEDEAO. A relevância disto, partindo da perspetiva da superfície de ataque, é que foram identificadas e exploradas diversas vulnerabilidades críticas e de elevada gravidade em dispositivos MikroTik. Saber se e onde estes dispositivos se

encontram numa rede através de um inventário de ativos é crucial para uma rápida correção à medida que novas vulnerabilidades são identificadas.

Os **routers*** estão entre os dispositivos mais visados pelos agentes de ameaças porque geralmente controlam o acesso às redes dos utilizadores, estão sempre ligados à Internet (e, como tal, facilmente passíveis de serem descobertos), muitas vezes têm credenciais de utilizador predefinidas ou mais fracas e as suas vulnerabilidades permanecem muitas vezes por corrigir. Uma vez explorados, estes dispositivos são muitas vezes incorporados em grandes botnets e utilizados para uma variedade de atividades maliciosas como ataques de DDOS, distribuição de malware, roubo de dados e campanhas de phishing.

A Shadowserver pode mapear dispositivos expostos e identificados com impressão digital, incluindo routers, na região da CEDEAO por tipo de dispositivo. Embora determinados tipos de dispositivos, como **firewalls*** e **serviços VPN***, estejam frequentemente expostos à Internet pública como parte das respetivas funções centrais, os routers e determinados outros dispositivos não necessitam normalmente de estar expostos.

Uma história de alerta sobre os perigos de ativos expostos desnecessariamente à Internet pode ser encontrada na intrusão de redes de infraestruturas críticas que teve início em novembro de 2023 pelo CyberAv3ngers, um grupo de hackers afiliado ao Corpo da Guarda Revolucionária Islâmica do Governo do Irão (IRGC). Entre novembro de 2023 e janeiro de 2024, o CyberAv3ngers conseguiu comprometer com sucesso pelo menos 75 dispositivos PLC Unitronics de fabrico israelita utilizados em múltiplos setores de infraestruturas críticas, incluindo o setor da água e do saneamento. Os dispositivos eram dispositivos de tecnologia operacional (TO) expostos publicamente à Internet de forma desnecessária com uma palavra-passe predefinida ou sem palavra-passe implementada.[20] O mais proeminente destes ataques foi perpetrado contra a Autoridade Municipal da Água de Aliquippa, uma pequena comunidade na região oeste da Pensilvânia.[21] Estes ataques revelaram o quão vulneráveis são as redes de infraestruturas críticas a ciberataques e o quão prejudicam o público se tais sistemas forem alvo de intrusão.

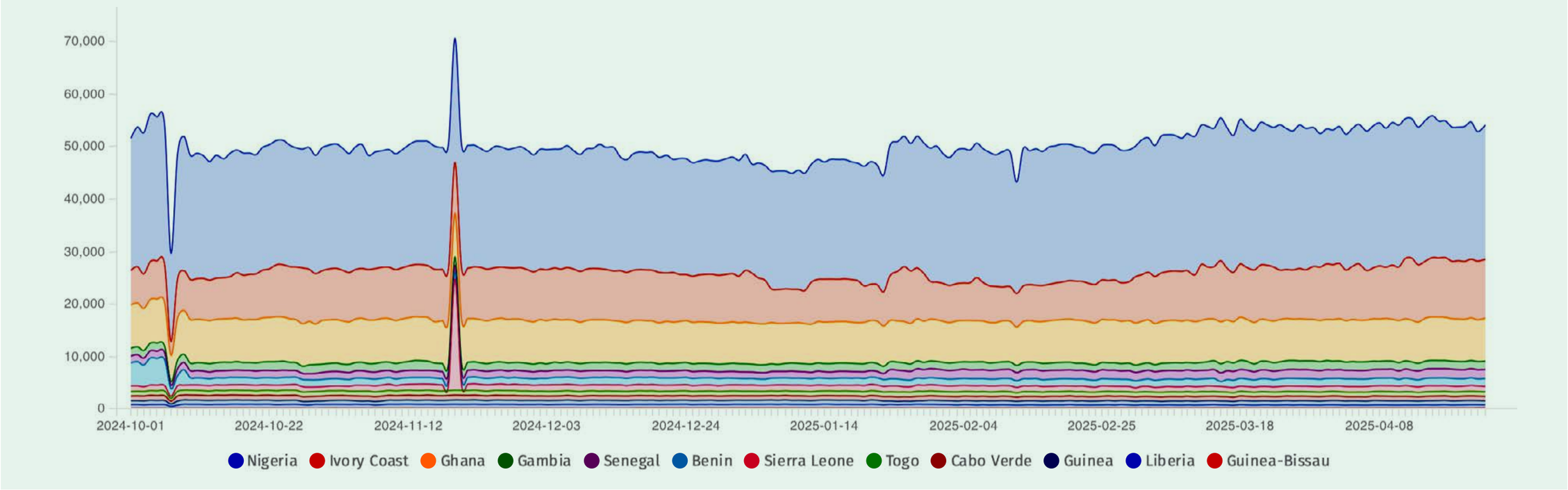
As redes de infraestruturas críticas são cada vez mais visadas por ciberataques por agentes de ameaças. Estes ataques podem causar prejuízos sociais significativos quando serviços como abastecimento de água, fornecimento de eletricidade e serviços de cuidados de saúde sofrem perturbações ou são, de outra forma, comprometidos. Em conformidade, assegurar que os ativos não são desnecessariamente expostos à Internet pública é um passo importante para proteger uma rede e reduzir a superfície de ataque.

A Shadowserver partilha com as CSIRT Nacionais e com os proprietários de redes dados acionáveis, detalhados e específicos do IP sobre dispositivos expostos numa rede/grupo de destinatários no relatório de «Identificação de Dispositivos».

[20] "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, including US Water and Wastewater Systems Facilities," *Cybersecurity Advisory, Cybersecurity and Infrastructure Security Agency*, 18 de dezembro de 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 de dezembro de 2023. https://www.npr.org/2023/12/02/1216735250/iran-linked-cyberattacks-israeli-equipment-water-plants

Figura 07. **Casos de aplicações do lado do servidor expostas por país na Região da CEDEAO**

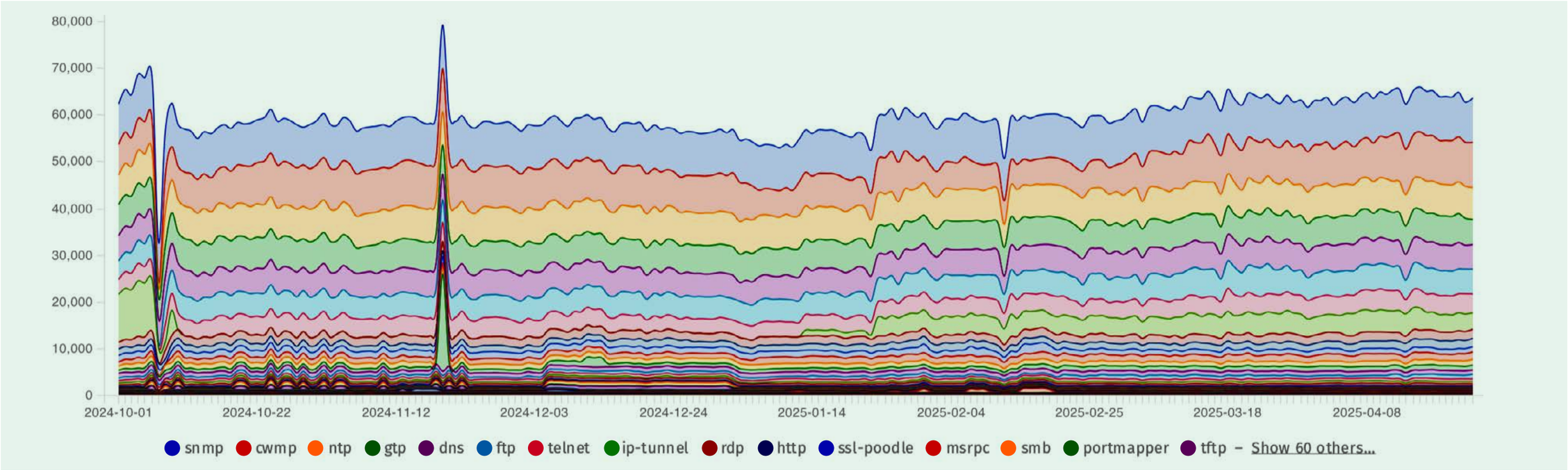


The items at the bottom of each graph are arranged left to right in descending order in which they appear on the graph.

Para além de dispositivos publicamente expostos, os **serviços*/aplicações do lado do servidor*** que são publicamente expostos à Internet são também um motivo de preocupação e contribuem para uma superfície de ataque global. A Figura 07 mostra casos de serviços expostos por país na região da CEDEAO com a Nigéria, Costa do Marfim e o Gana, os três principais. Estes serviços expostos são considerados problemáticos porque são configurados incorretamente, passíveis de abuso, vulneráveis ou, de outra forma, desnecessariamente acessíveis a partir da Internet pública, tornando-os alvos preferenciais de agentes de ameaças que procuram invadir redes.

Lacunas operacionais de cibersegurança e recomendações: Superfície de ataque da região da CEDEAO

Figura 08. **Casos de aplicações do lado do servidor expostas por tipo de varrimento na Região da CEDEAO**



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

A Figura 08 mostra que **o SNMP (Protocolo Simples de Gestão de Rede*)** é o serviço mais exposto à Internet na região da CEDEAO. O SNMP é um protocolo que desempenha um papel crucial na monitorização, gestão e proteção de dispositivos de rede. Permite que os administradores de redes recolham informações, configurem dispositivos e respondam a eventos da rede remotamente, tornando-o uma ferramenta essencial para manter o desempenho e a proteção da rede.

Muitos serviços expostos contêm vulnerabilidades que podem ser exploradas por agentes de ameaças. Por exemplo, os serviços de SNMP expostos em determinados routers Cisco contêm uma vulnerabilidade designada como CVE-2017-6742. Em abril de 2023, um Aviso de Cibersegurança (CSA) conjunto publicado pelas agências de segurança dos EUA e do RU revelou que hackers da Unidade 26165 da Inteligência Militar do GRU russo (conhecidos como APT28, Fancy Bear e Sofacy, entre outros) exploraram esta vulnerabilidade para realizar o reconhecimento de routers e implementar malware.[22]

[22] "Advisory: APT28 Exploits Known Vulnerability to Carry Out Reconnaissance and Deploy Malware on Cisco Router," *National Cyber Security Centre, United Kingdom*, 18 de abril de 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

Estes exemplos destacam a potencial ameaça representada por dispositivos e serviços expostos que pode ser explorada por agentes de ameaças, incluindo hackers de estados soberanos.

RECOMENDAÇÕES:
Estabelecer políticas para mandatar a realização de inventários de ativos periódicos*, em particular nos setores governamental e de infraestruturas críticas. Essa medida ajudará os proprietários de redes nos esforços de correção e remediação oportunos enquanto surgem novas vulnerabilidades críticas. Orientações úteis sobre como implementar os regulamentos que mandatam a realização de inventários de ativos por agências governamentais federais encontram-se disponíveis em "Diretiva Operacional Vinculativa 23-01: Melhorar a Visibilidade de Ativos e a Deteção de Vulnerabilidades nas Redes Federais" com a supervisão da Agência de Cibersegurança e Segurança de Infraestruturas do Departamento de Segurança Interna dos Estados Unidos (DHS-CISA).

Garantir que os proprietários de redes (em particular, infraestruturas críticas, governo e grandes fornecedores de serviços de Internet) não expõem desnecessariamente determinados tipos de dispositivos (incluindo dispositivos de TO e outros mencionados anteriormente) e serviços (incluindo SNMP) na Internet pública, a menos que seja necessário para fins de funcionalidade. Esta medida reduzirá a superfície de ataque global da região. Formações e workshops focados com CSIRT Nacionais, fornecedores de serviços de Internet e outros proprietários de redes na região da CEDEAO poderão culminar em atividade de reforço proativo para visar e reduzir casos de dispositivos e serviços expostos desnecessariamente.

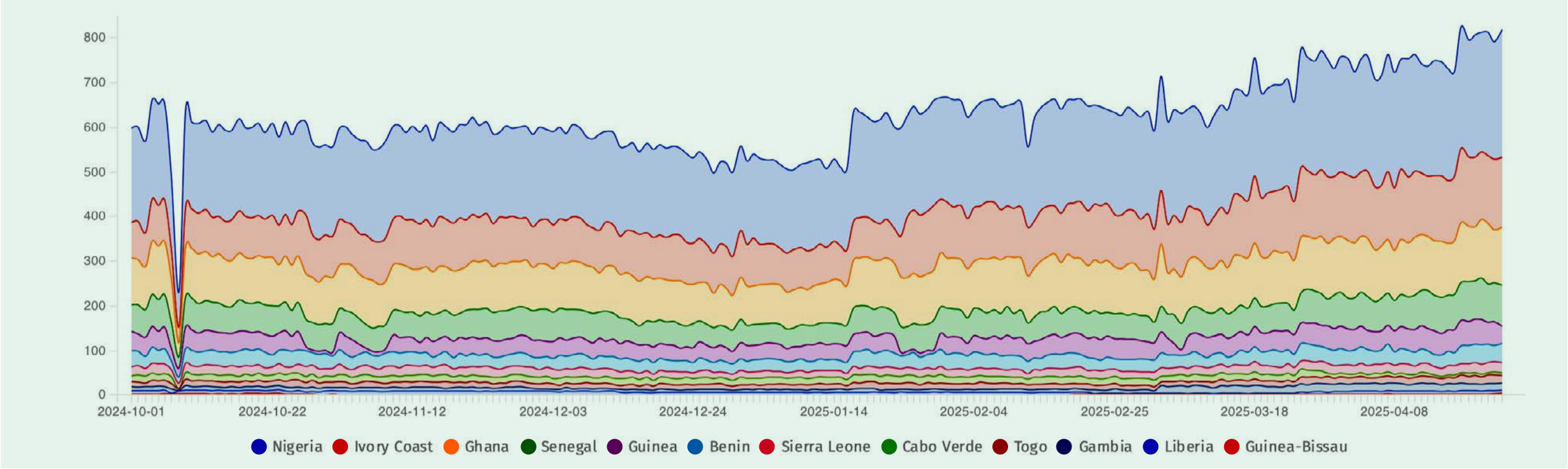
3.1b// VULNERABILIDADES CRÍTICAS EM ATIVOS EXPOSTOS

Os agentes de ameaças continuam a explorar vulnerabilidades não corrigidas como um meio principal de intrusão de redes e causa de prejuízos, incluindo ransomware e ataques de DDOS. Como parte das suas atividades centrais, a Shadowserver varre a Internet à procura de casos de determinadas **Vulnerabilidades e Exposições Comuns (CVE)*** críticas e de elevada gravidade em dispositivos e software. De seguida, alerta os proprietários de redes e as CSIRT Nacionais sobre estas vulnerabilidades nas respetivas redes a serem corrigidas antes que os agentes de ameaças possam explorar as vulnerabilidades, invadir a rede e causar mais prejuízos.

Como exemplo recente, foram exploradas vulnerabilidades não corrigidas no software de colaboração e partilha de informação SharePoint da Microsoft conhecido como "ToolShell" em junho de 2025 por agentes de ameaças que visaram pelo menos meia dúzia de entidades na África do Sul, incluindo o Tesouro Nacional, uma organização do setor de fabrico de automóveis, uma universidade, diversas entidades do governo local e uma entidade do governo federal.[23]

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

Figura 09. **CVE remotas críticas detetadas em ativos expostos por país em toda a região da CEDEAO**



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

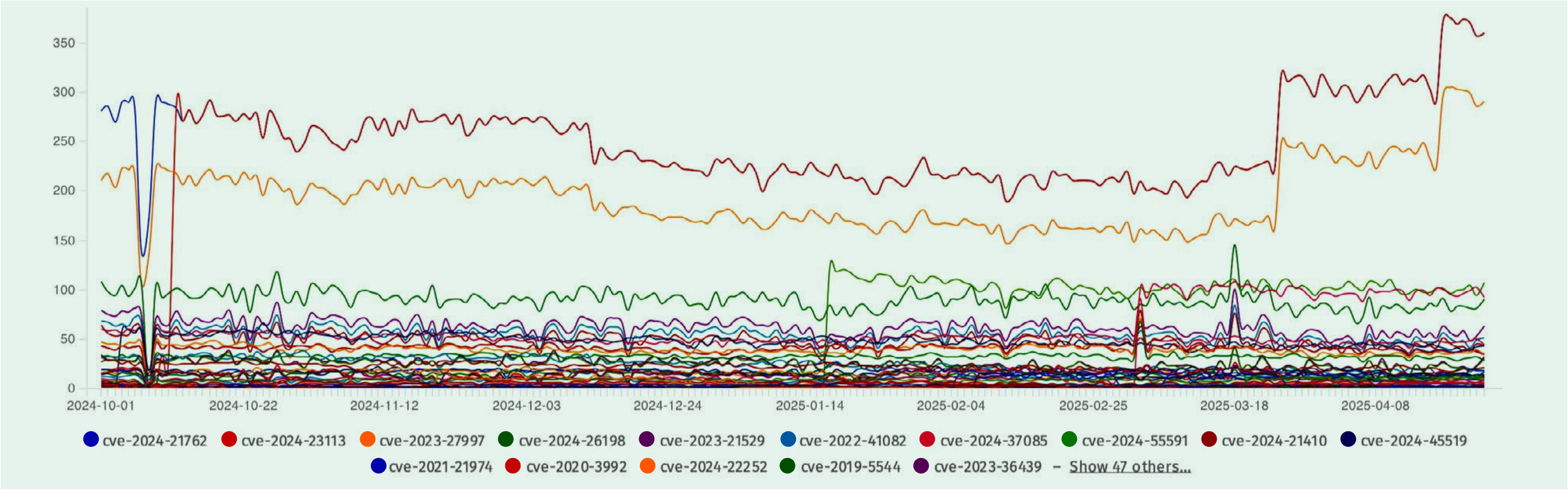
Como ilustrado na Figura 09, os varrimentos diários da Shadowserver revelam um número modesto de vulnerabilidades críticas em infraestruturas expostas na região da CEDEAO, com os exemplos mais vistos na Nigéria, Costa do Marfim e Gana. Estas vulnerabilidades podem infelizmente ser exploradas em qualquer altura.

Como ilustrado na Figura 10, existem diversas vulnerabilidades críticas relacionadas com CVE na região da CEDEAO que suscita preocupação. Por exemplo, a CVE-2024-23113 é uma vulnerabilidade crítica no FortiOS da Fortinet que, se explorada, poderá permitir que um hacker remoto, não autenticado execute código ou comandos arbitrários num sistema.[24] Pouco depois do anúncio da vulnerabilidade em outubro de 2024, a Shadowserver

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

Lacunas operacionais de cibersegurança e recomendações: Superfície de ataque da região da CEDEAO

Figura 10. **CVE remotas críticas detetadas em ativos expostos em toda a Região da CEDEAO**



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

identificou mais de 87.000 IP da Fortinet provavelmente vulneráveis à CVE-2024-23113.[25] Adicionalmente, por volta da mesma altura, a Agência de Cibersegurança e Segurança de Infraestruturas do Departamento de Segurança Interna dos Estados Unidos (DHS-CISA ou "CISA") adicionou a CVE-2024-23113 ao seu Catálogo de Vulnerabilidades Exploradas Conhecidas, o que significa que a CVE estava a ser ativamente explorada em ambiente real por agentes de ameaças e deve ser uma prioridade de correção principal para as agências governamentais dos EUA.[26]

As vulnerabilidades não corrigidas proporcionam aos agentes de ameaças vetores de ataque para obter acesso não autorizado a redes. As vulnerabilidades observadas ativamente exploradas em ambiente real (também referidas como "**vulnerabilidades exploradas conhecidas***") são motivo de particular preocupação e devem ser priorizadas para remediação imediata. A correção de vulnerabilidades, particularmente as de gravidade elevada e crítica e as que estão a ser ativamente exploradas em ambiente real, é crucial para alcançar uma infraestrutura digital mais segura e a sua execução deve ser obrigatória para as agências governamentais e infraestruturas críticas num período de tempo bem definido.

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

[26] "Alert: CISA Adds Three Known Exploited Vulnerabilities to Catalog," *Cybersecurity and Infrastructure Security Agency*, 9 de outubro de 2024. https://www.cisa.gov/news-events/alerts/2024/10/09/cisa-adds-three-known-exploited-vulnerabilities-catalog

Lacunas operacionais de cibersegurança e recomendações: Superfície de ataque da região da CEDEAO

Orientações úteis encontram-se disponíveis nas "diretivas operacionais vinculativas (BOD)" com a supervisão da DHS-CISA. Estas BOD exigem que os departamentos e agências federais, poder executivo, tomem determinadas medidas para salvaguardar informações e sistemas de informação federais.

Por exemplo, a "BOD 19-02: Requisitos de Remediação de Vulnerabilidades para Sistemas Acessíveis pela Internet" exige, entre ouras coisas, que as vulnerabilidades críticas sejam remediadas no prazo de 15 dias civis a partir da deteção inicial e que as elevadas vulnerabilidades sejam remediadas no prazo de 30 dias civis a partir da deteção inicial. Se as vulnerabilidades não forem remediadas nos prazos especificados, a CISA enviará um plano de remediação parcialmente preenchido a identificar todas as vulnerabilidades nesse âmbito em atraso para os pontos de contacto da agência para validação e preenchimento. As agências devem então devolver o plano de remediação preenchido à CISA no prazo de três dias úteis após a receção com a informação preenchida que explica: (i) as limitações de remediação de vulnerabilidades; (ii) as ações de atenuação temporárias para superar as limitações; e (iii) a data prevista de conclusão para remediar a vulnerabilidade.

De forma similar, a "BOD 22-01: Redução do Risco Significativo de Vulnerabilidades Exploradas Conhecidas" foi criada para melhorar, mas não substituir a BOD 19-02. A BOD 22-01 estabeleceu um catálogo gerido pela CISA de vulnerabilidades exploradas conhecidas que representam risco significativo para as entidades federais. A BOD estabeleceu ainda requisitos para as agências remediarem quaisquer vulnerabilidades desta natureza incluídas no catálogo no prazo especificado; nomeadamente, no prazo de 6 meses para vulnerabilidades com um ID de Vulnerabilidades e Exposições Comuns (CVE) atribuído antes de 2021 e no prazo de duas semanas para todas as outras vulnerabilidades.

Relativamente à questão de as vulnerabilidades elevadas/críticas ou as vulnerabilidades exploradas conhecidas serem ou não mais importantes para remediar primeiro, a CISA explicou: "As vulnerabilidades exploradas conhecidas devem ser a principal prioridade para remediação a BOD 22-01 muda o foco para as vulnerabilidades que são ameaças ativas." [27]

RECOMENDAÇÕES:

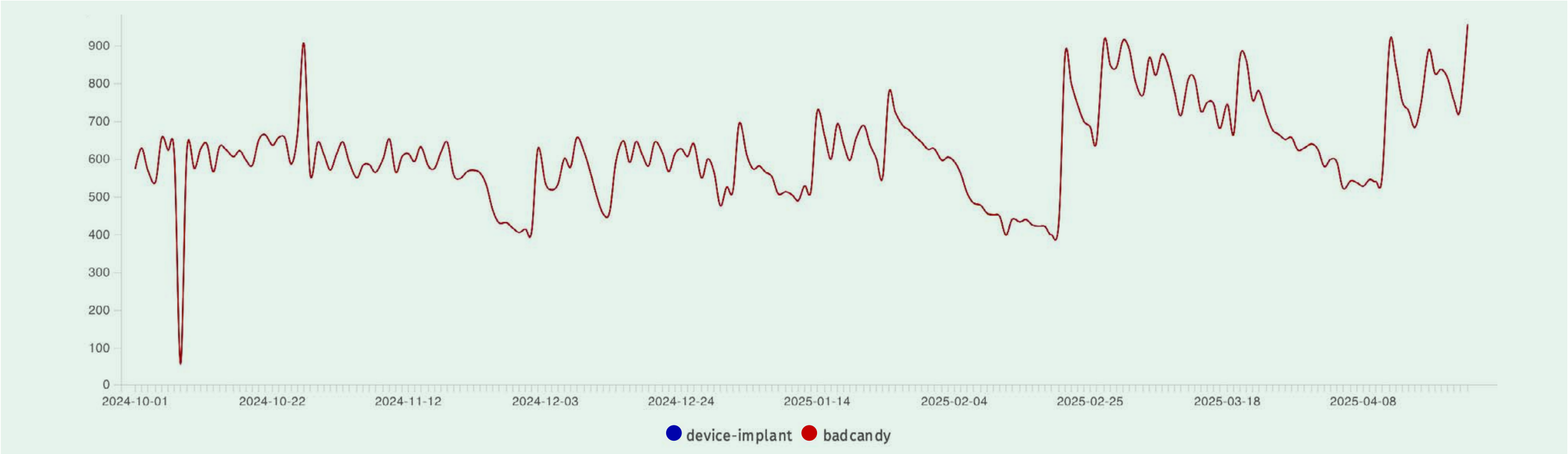
Implementar regulamentos que exijam que as agências governamentais e infraestruturas críticas remediem as vulnerabilidades designadas como "risco crítico" no prazo de 15 dias civis e as designadas como "elevado risco" no prazo de 30 dias civis a partir da data de deteção inicial. Orientações úteis encontram-se disponíveis, por exemplo, na "Diretiva Operacional Vinculativa (BOD) 19-02: Requisitos de Remediação de Vulnerabilidades para Sistemas Acessíveis pela Internet" com a supervisão da Agência de Cibersegurança e Segurança de Infraestruturas do Departamento de Segurança Interna dos Estados Unidos (DHS-CISA).

Implementar regulamentos que exijam que o governo e as infraestruturas críticas remediem "vulnerabilidades exploradas conhecidas" no prazo de 14 dias. O DHS (Departamento de Segurança Interna) e a CISA (Agência de Segurança Cibernética e de Infraestruturas) dos EUA mantêm um catálogo de Vulnerabilidades Exploradas Conhecidas (KEV) que identifica vulnerabilidades observadas como estando a ser ativamente exploradas em ambiente real e que devem ser remediadas pelas agências federais governamentais dos Estados Unidos. A ENISA (Agência Europeia para a Segurança das Redes e da Informação) mantém um catálogo semelhante conhecido como a Base de Dados de Vulnerabilidades da União Europeia. Por último, o Painel público da Shadowserver mantém a lista de vulnerabilidades exploradas conhecidas da Shadowserver identificada através da respetiva rede de sensores de honeypots. Orientações úteis sobre tal regulamento encontram-se disponíveis, por exemplo, na "Diretiva Operacional Vinculativa (BOD) 22-01: Redução do Risco Significativo de Vulnerabilidades Exploradas Conhecidas" com a supervisão do DHS-CISA.

[27] "BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities," *Cybersecurity and Infrastructure Security Agency*, 3 de novembro de 2021. https://www.cisa.gov/news-events/directives/bod-22-01-reducing-significant-risk-known-exploited-vulnerabilities

Lacunas operacionais de cibersegurança e recomendações: Superfície de ataque da região da CEDEAO

Figura 11. **Dispositivos comprometidos na Região da 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// ATIVOS EXPOSTOS COMPROMETIDOS

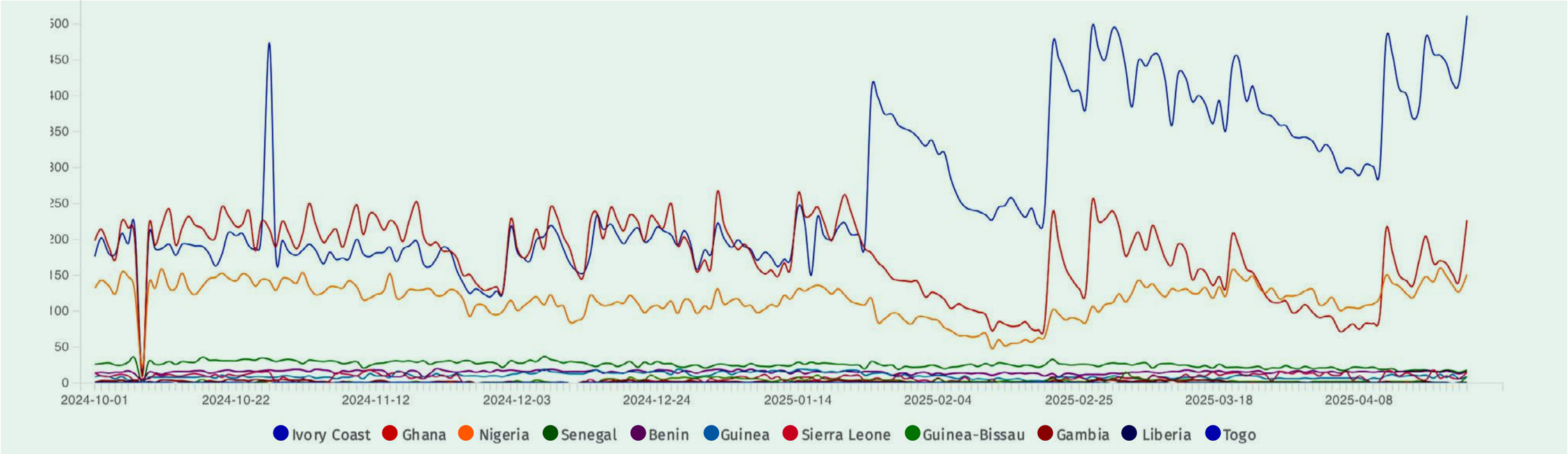
A Shadowserver efetua também continuamente varrimentos quanto a ativos de rede críticos que tenham sido comprometidos por agentes de ameaças quando estão disponíveis indícios suficientes para deteção. Esta medida é efetuada principalmente através de varrimento não-intrusivo para determinados itens ou artefactos frequentemente instalados num dispositivo após ter sido comprometido (por exemplo, **implantes***, **web shells*** e **injeções de código para roubo de credenciais***).

Por exemplo, no final de 2023, o software Cisco IOS XE foi comprometido pelo que se conhece como implantes "Bad Candy", que consistiam em **web shells*** maliciosos instalados em milhares de dispositivos de rede Cisco voltados para a Internet por agentes de ameaças que exploraram duas **vulnerabilidades de dia zero***. [Uma vulnerabilidade de dia zero é uma falha anteriormente conhecida no software, hardware ou firmware que os perpetradores do ataque podem explorar antes que o fornecedor fique ciente da sua existência e tenha a oportunidade de desenvolver uma correção para solucioná-la.] Estes ataques permitiram que os agentes de ameaças obtivessem controlo administrativo total do sistema e permitiram-lhes potencialmente monitorizar o tráfego da rede, aceder a redes protegidas e executar uma variedade de ataques.[28]

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

Lacunas operacionais de cibersegurança e recomendações: Superfície de ataque da região da CEDEAO

Figura 12. **Dispositivos comprometidos na Região da CEDEAO por país**



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

Os resultados de varrimento da Shadowserver mostram um número significativo de intrusões no Cisco IOS XE com implantes Bad Candy na região da CEDEAO. Na Figura 11, pode ver as intrusões no Cisco IOS XE/ relacionadas com Bad Candy na região da CEDEAO cuja média se situa abaixo de 500 dispositivos para o período reportado. Este número comporta o volume de dispositivos comprometidos detetados na região.

Curiosamente, a Figura 12 revela que a maioria dos compromissos relacionados com Bad Candy encontram-se em redes na Costa do Marfim com números muito mais elevados do que qualquer outra nação da CEDEAO, incluindo a Nigéria que possui o mais amplo espaço IPv4 da região.

Os dispositivos comprometidos, como Cisco IOS XE/Bad Candy, são ameaças significativas e podem continuar a ser explorados em qualquer altura com consequências potencialmente graves, incluindo interrupções operacionais, danos na rede, roubo de dados, ransomware e outros ataques baseados em malware, roubo de credenciais, danos reputacionais e responsabilidade legal.

A Shadowserver elabora relatórios sobre vários tipos de dispositivos comprometidos identificados através da deteção baseada em varrimentos do implante instalado pelo perpetrador do ataque. Estes relatórios, juntamente com fluxos de dados de outras fontes, podem ser utilizados pelas CSIRT Nacionais e por outras agências governamentais para conceber

campanhas de âmbito nacional para erradicar tais ameaças e proteger os dispositivos comprometidos.

Por exemplo, a Australian Signals Directorate (ASD) implementou uma campanha a nível nacional para erradicar implantes Bad Candy em dispositivos Cisco IOS XE comprometidos em toda a Austrália. Como parte da campanha, representantes oficiais da ASD enviaram notificações à vítima diretamente para os proprietários de redes afetadas ou para o respetivo fornecedor de serviços caso não fosse possível identificar o proprietário da rede. As notificações continham instruções para corrigir, reiniciar e realizar a resposta a incidentes em dispositivos afetados para remover o implante Bad Candy e atenuar o risco de nova exploração. A ASD rastreou em seguida o declínio global do número de dispositivos implantados com Bad Candy no decurso de vários meses à medida que iam sendo publicados lotes de notificações em massa.

RECOMENDAÇÕES:
Implementar regulamentos que exijam que as CSIRT Nacionais, agências governamentais, infraestruturas críticas, fornecedores de serviços de Internet e outros proprietários de redes na região remediem dispositivos comprometidos identificados num período de tempo breve mas especificado, incluindo os identificados nos relatórios diários da Shadowserver, tais como Cisco/implantes Bad Candy.

Mandatar CSIRT Nacionais, em coordenação com os Fornecedores de Serviços de Internet (FSI), para conceber e implementar campanhas de atenuação e erradicação de ameaças a nível nacional contra vulnerabilidades críticas e dispositivos comprometidos em redes espalhadas pelo país e monitorizar o progresso dos esforços de remediação. Um exemplo disso é a campanha a nível nacional liderada pela Australian Signals Directorate (ASD) para erradicar implantes Bad Candy em dispositivos Cisco IOS XE comprometidos em toda a Austrália.

3.2// Dados de sinkhole

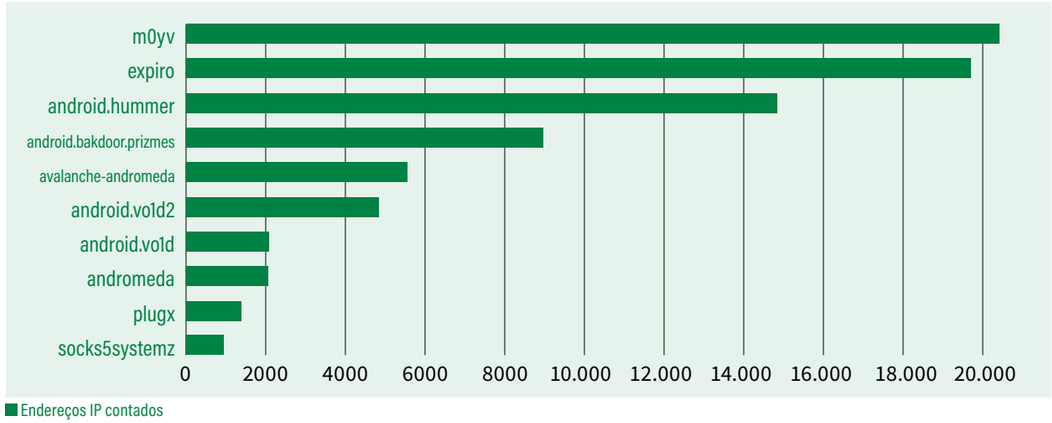
A Shadowserver opera uma grande infraestrutura de sinkholing do **sistema de nomes de domínio (DNS*)** através da qual recolhe dados sobre dispositivos infetados com malware das vítimas. “**Sinkholing***” é uma técnica que envolve a interrupção das comunicações entre os dispositivos infetados com malware das vítimas e os servidores controlados de forma criminosa para os quais o malware os direciona para comunicar. A comunicação, ou tráfego, é depois redirecionado para servidores de sinkhole de modo que os criminosos deixem de poder aceder, controlar ou comunicar com os dispositivos das vítimas. A Shadowserver recolhe o endereço IP e outras informações de identificação associadas aos dispositivos infetados por malware das vítimas que reportam aos servidores de sinkhole. As informações são então adicionadas aos relatórios diários e gratuitos de remediação de redes da Shadowserver para notificar as CSIRT Nacionais e os proprietários de redes subscritores de dispositivos infetados com malware a serem remediados.

Este desmantelamento é normalmente alcançado ao assumir o controlo dos domínios ou endereços de IP maliciosos que controlam as comunicações entre os dispositivos infetados com malware da vítima e a infraestrutura controlada pelos criminosos. Geralmente tal é feito através de ordens judiciais penais ou cíveis proferidas em **registos*** e **entidades de registo***, através da ação voluntária dos registos e das entidades de registo como resultado de violações dos termos de serviço ou através da aquisição desses domínios maliciosos que ainda não estão registados pelos agentes de ameaças. Os domínios maliciosos apreendidos pelas autoridades são muitas vezes transferidos para a Entidade de Registo de Último Recurso (RoLR) da Shadowserver, uma entidade de registo de DNS sem fins lucrativos de finalidade específica criada com o propósito de colocar domínios maliciosos em quarentena sem encargos (ou com encargos mínimos) a longo prazo como um serviço público.

Sinkholing é uma técnica importante para garantir que os agentes de ameaças deixem de poder aceder, controlar ou comunicar com dispositivos infetados

Lacunas operacionais de cibersegurança e recomendações: Superfície de ataque da região da CEDEAO

Figura 13. **10 principais infeções detetadas por sinkhole por tipo na Região da CEDEAO**



por malware das vítimas (salvo infetados com outros tipos de malware que não seja objeto da operação de sinkhole).

Com base nos conjuntos de dados de infeção obtidos por sinkhole, o gráfico de barras na Figura 13 mostra mais de 80.000 endereços IP infetados por malware no total por dia em média na região da CEDEAO. De forma mais simples, mais de 80.000 dispositivos cuja geolocalização dos IP se encontra na região da CEDEAO estão infetados com malware e (salvo infetados com outros tipos de malware que não estão a ser sujeitos a sinkholing) eram anteriormente controlados por agentes de ameaças antes de serem redirecionados para servidores de sinkhole da Shadowserver.

A Figura 14 abaixo revela que a maioria das infeções de dispositivos são constatadas na Nigéria, seguindo-se o Gana, provavelmente devido em parte ao grande espaço de IP atribuível a essas nações.

Figura 14. **Maioria dos países afetados por malware na Região da CEDEAO - conforme observado nos dados de sinkhole**

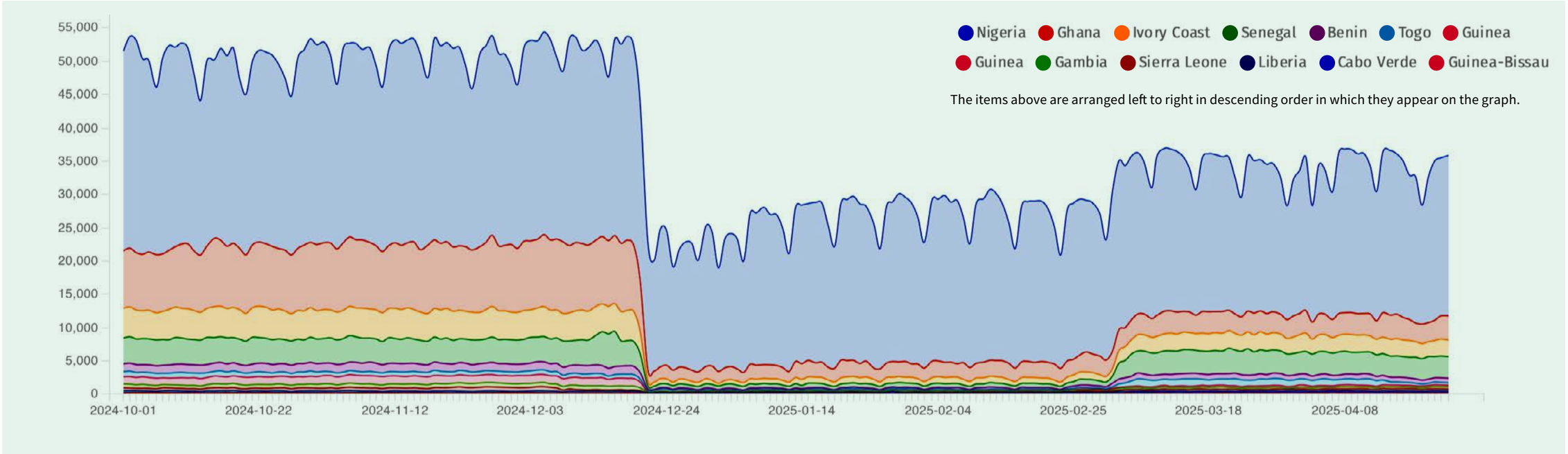
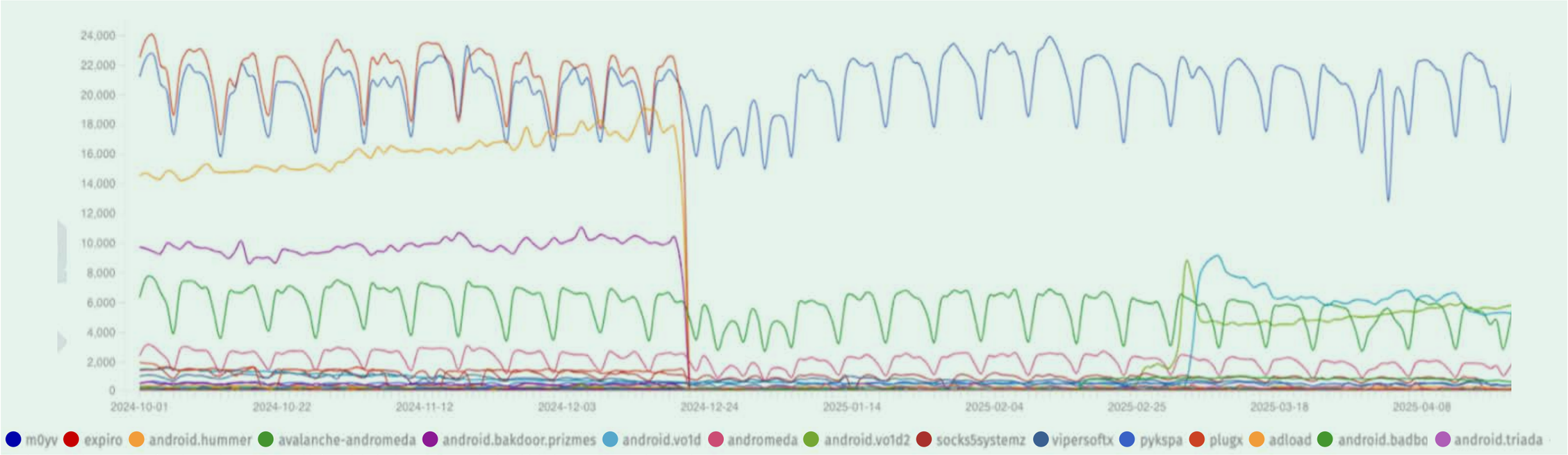


Figura 15. **Principais infeções observadas em sinkholes da Shadowserver na Região da CEDEAO - por tipo de malware**



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

A análise de dados de sinkhole por tipo de infeção permite-nos aprofundar ainda mais os dados estatísticos referentes a infeções para procurar tendências no tipo de malware observado na região.

Na Figura 15, observamos uma variedade de variantes de malware em dispositivos infetados por toda a região da CEDEAO. Por exemplo, M0yv é um vírus que infeta ficheiros modular, multifuncional desenvolvido e utilizado pelo grupo de ransomware Maze. O grupo de ransomware Maze era uma rede de criminosos cibernéticos conhecida por popularizar a técnica de “dupla extorsão” por meio da qual roubariam os dados da vítima e os encriptariam. Caso um resgate fosse pago, os dados seriam desencriptados e tornados acessíveis novamente para a vítima. Caso o resgate não fosse pago, o grupo divulgaria publicamente os dados roubados em sites de fugas de dados que mantinham.

RECOMENDAÇÕES:
Implementar regulamentos que exijam que as CSIRT Nacionais, agências governamentais, infraestruturas críticas, fornecedores de serviços de Internet e outros proprietários de redes na região colaborem para remediar dispositivos infetados com malware identificados num período de tempo breve mas especificado, incluindo os identificados nos relatórios diários de remediação de redes gratuitos da Shadowserver.

3.3// Conjuntos de dados únicos de operações de combate ao cibercrime das Autoridades Policiais

Conjuntos de dados únicos são recolhidos por, ou partilhados com, a Shadowserver como resultado do nosso apoio às **operações de combate ao cibercrime das Autoridades Policiais***. Durante mais de 15 anos, a Equipa de Projetos Especiais da Shadowserver (SSPT) prestou apoio gratuito a muitas das operações de desmantelamento de cibercrime internacionais mais significativas. Este apoio tem vindo a assumir muitas formas, mas normalmente inclui a realização por parte da Shadowserver de operações de sinkhole, a colocação de nomes de domínio maliciosos em quarentena através da Entidade de Registo de Último Recurso (RoLR) e a assistência em esforços de notificação da vítima através da distribuição dos dados da vítima a proprietários de redes afetadas e/ou respetiva CSIRT Nacional nos nossos relatórios diários e gratuitos de remediação de redes.

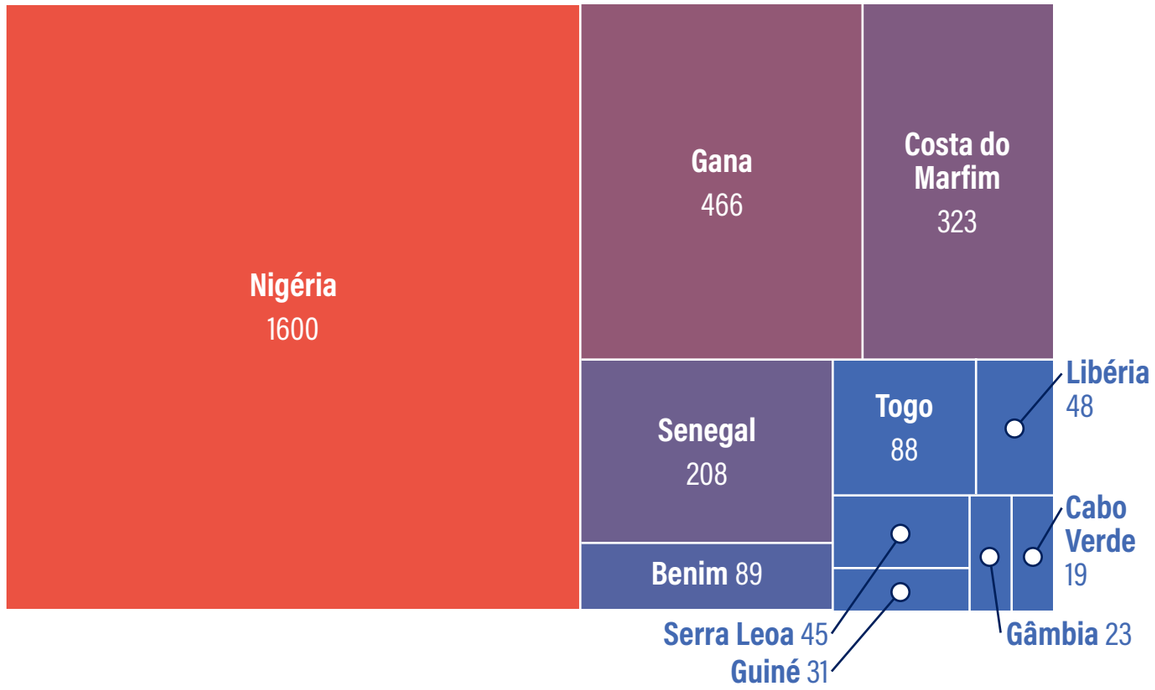
As autoridades policiais partilham frequentemente com a Shadowserver conjuntos de dados únicos de infeções históricas de dispositivos de vítimas bem como infeções ativas de dispositivos de vítimas que reportam a servidores de sinkhole da Shadowserver quando são desmanteladas grandes **botnets***. O histórico de infeções é partilhado com CSIRT Nacionais em Relatórios Especiais pontuais, enquanto as infeções ativas são partilhadas através de relatórios diários e gratuitos de remediação de redes da Shadowserver. Estes conjuntos de dados únicos adquiridos através de operações de desmantelamento das Autoridades Policiais revelam dispositivos de vítimas infetados com malware na região da CEDEAO que faziam parte de botnets controladas de forma criminosa.

A título de exemplo, a botnet de malware Qakbot foi desmantelada numa operação das autoridades policiais pelo FBI e pelo Departamento de Justiça dos EUA juntamente com vários outros parceiros em agosto de 2023. Qakbot (também conhecida como QBot, Pinkslipbot, Quakbot e Oakbot) tem estado ativa desde cerca de 2007, tendo sido inicialmente desenvolvida como um malware de roubo de informação e malware **trojan bancário***, antes de mais tarde se tornar principalmente uma rede de distribuição para outro malware/ransomware. Nos últimos anos, a Qakbot tem sido utilizada como um vetor de infeção inicial por muitos grupos de ransomware, incluindo Conti, ProLock, Egregor, REvil, MegaCortex e Black Basta. Isto possibilitou provavelmente significativas perdas financeiras a nível global.

Conforme ilustrado na Figura 16, foram detetadas 2941 infeções históricas pela Qakbot em dispositivos em toda a região da CEDEAO.

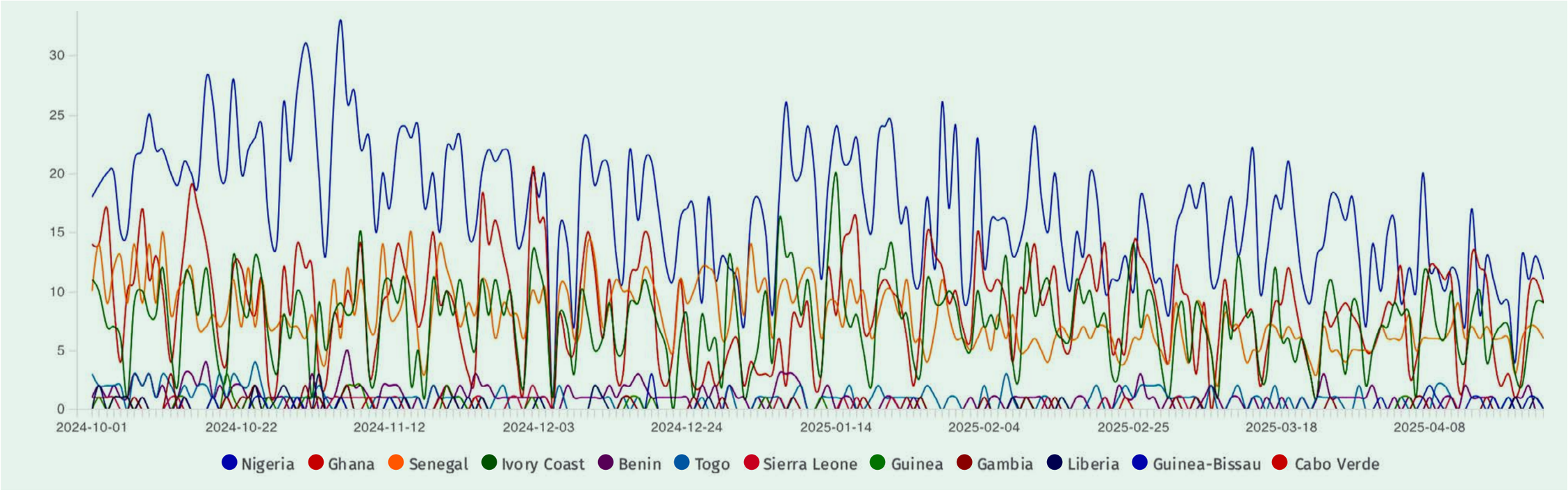
A título de segundo exemplo, a Operation Endgame foi uma operação

Figura 16. **Infeções históricas pela Qakbot em toda a Região da CEDEAO (2023-08-24)**



Lacunas operacionais de cibersegurança e recomendações: Superfície de ataque da região da CEDEAO

Figura 17. **Smokeloader em toda a Região da CEDEAO**



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

internacional das Autoridades Policiais liderada pela Europol contra droppers de malware, incluindo IcedID, SystemBC, Pikabot, Smokeloader e Bumblebee, que culminou em quatro detenções e no desmantelamento de mais de 100 servidores em todo o mundo em maio de 2024. Droppers são programas maliciosos concebidos para entregar outro malware no dispositivo de uma vítima. No gráfico temporal (Figura 17) podemos observar que todas as nações da CEDEAO foram impactadas pelo SmokeLoader, em que as nações IPv4 mais populosas exibiram a maioria das infeções.

Os conjuntos de dados de vítimas adquiridos pela Shadowserver através de operações de desmantelamento de cibercrime das Autoridades Policiais são únicos e não se encontram prontamente disponíveis noutro lugar, especialmente através de fornecedores comerciais. As CSIRT Nacionais e os proprietários de redes em toda a região da CEDEAO devem beneficiar plenamente para aceder a estes dados gratuitos valiosos no sentido de os ajudar a remediar dispositivos infetados com malware para melhor proteger as suas redes. Embora sujeitos a sinkholing pela Shadowserver, estes dispositivos de vítimas permanecem infetados, salvo e até que sejam remediados, o que pode ser alcançado através de esforços colaborativos entre CSIRT Nacionais e proprietários de redes afetadas.

Painel público da Shadowserver

Este relatório inclui dados estatísticos e visualizações de dados de ameaças do Painel público gratuito da Shadowserver financiado pelo Ministério dos Negócios Estrangeiros, da Commonwealth e do Desenvolvimento (FCDO) do Reino Unido. O Painel permite que o público consulte os conjuntos de dados da Shadowserver para obter dados estatísticos agregados, ao nível nacional ou regional relativos a uma variedade de questões relacionadas com ameaças. Como parte do atual projeto, a Shadowserver criou um novo agrupamento regional de países no Painel para abranger especificamente dados estatísticos relevantes para a região da CEDEAO. (Ver Figura 18).

O Painel pode ser uma ferramenta útil para informar os líderes governamentais, decisores, investigadores no âmbito da cibersegurança, especialistas em proteção de redes, órgãos de comunicação social e outros sobre as mais recentes ameaças cibernéticas que afetam um país e/ou região. O Painel também pode disponibilizar dados estatísticos que ajudam a rastrear o progresso de esforços de correção e remediação num país ou região relacionados com uma ameaça específica.

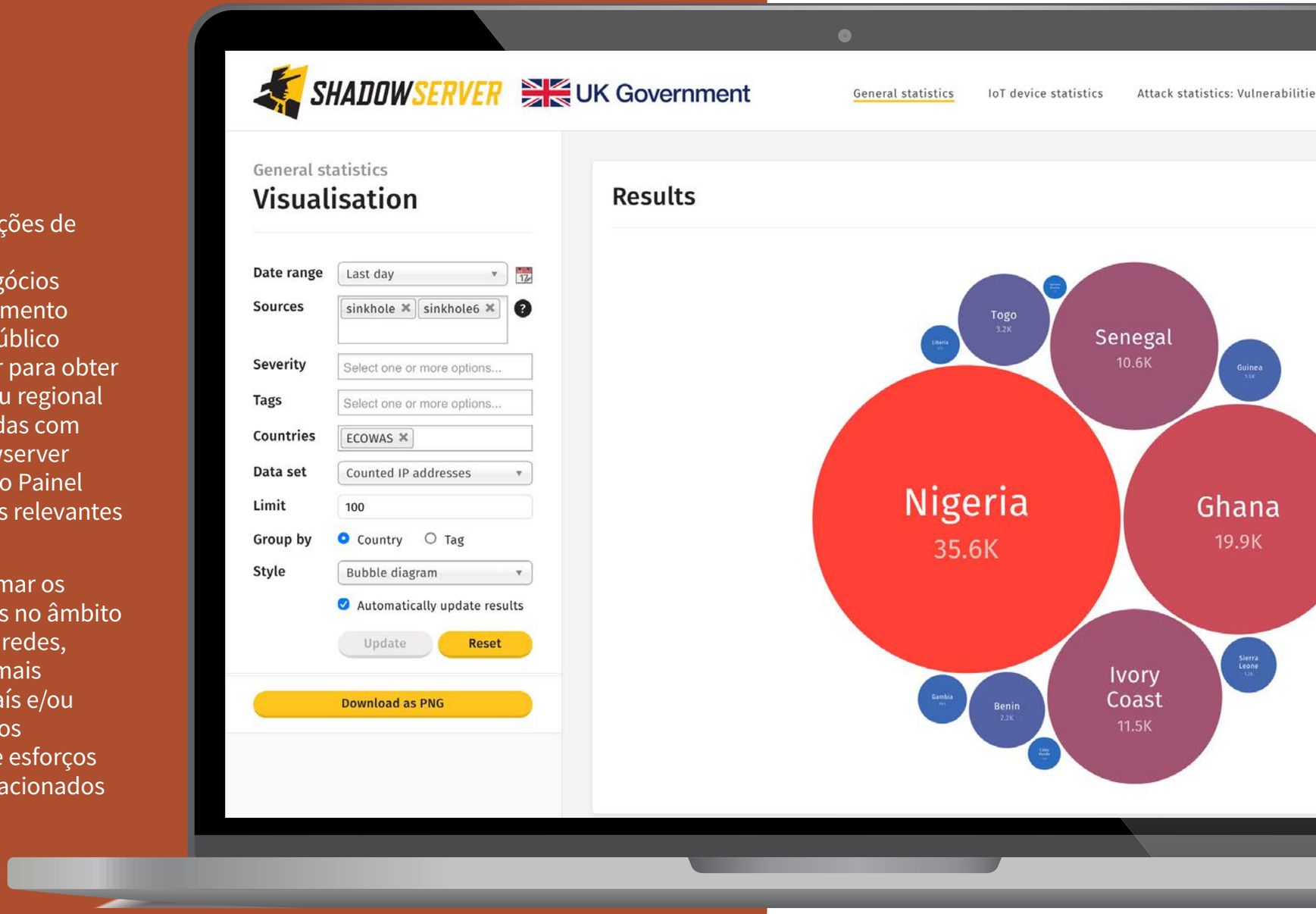


Figura 18. **Agrupamento regional de países da região da CEDEAO no Painel público da Shadowserver**

Por exemplo, suponha que um representante oficial da Equipa de Resposta a Emergências Informáticas da Nigéria (ngCERT) toma conhecimento dos potenciais danos causados por dispositivos domésticos ligados à Internet que facilitam atividade criminosa como parte de uma grande botnet conhecida como Badbox 2.0. Após investigação adicional online, o representante oficial da ngCERT toma conhecimento de que a Google, HUMAN Security, Trend Micro e a The Shadowserver Foundation estabeleceram uma parceria para levar a cabo uma operação de desmantelamento contra a botnet Badbox 2.0 na qual a Shadowserver sujeitou os dispositivos infetados a **sinkholing*** para que possam agora reportar aos servidores de sinkhole da Shadowserver e deixem de poder ser controlados por agentes de ameaças criminosos. https://www.humansecurity.com/learn/blog/satori-disrupting-badbox-2/

O representante oficial da ngCERT pretende obter financiamento do governo para uma campanha de sensibilização pública sobre a Badbox 2.0 na Nigéria e uma iniciativa de remediação direcionada com CERT Nacionais membros e Fornecedores de Serviços de Internet (FSI) em toda a região da CEDEAO. De modo a ajudar a informar os representantes oficiais do governo da Nigéria e dos Estados-Membros da CEDEAO sobre a ameaça da Badbox 2.0 na região, o representante oficial da ngCERT pode consultar o Painel público da Shadowserver.

Ao clicar no separador de dados de Sinkhole da Shadowserver, o representante oficial da ngCERT pode adicionar filtros à consulta no lado esquerdo do ecrã, incluindo o “Dia,” os “Tags” (neste caso, “android.badbox2”) e os “Países” (neste caso, a CEDEAO, mas também pode ser um país individual como a Nigéria). O resultado é um Treemap que mostra infeções no Android pela Badbox 2.0 para o dia anterior entre os diversos Estados-Membros da CEDEAO. (Ver Figura 19).

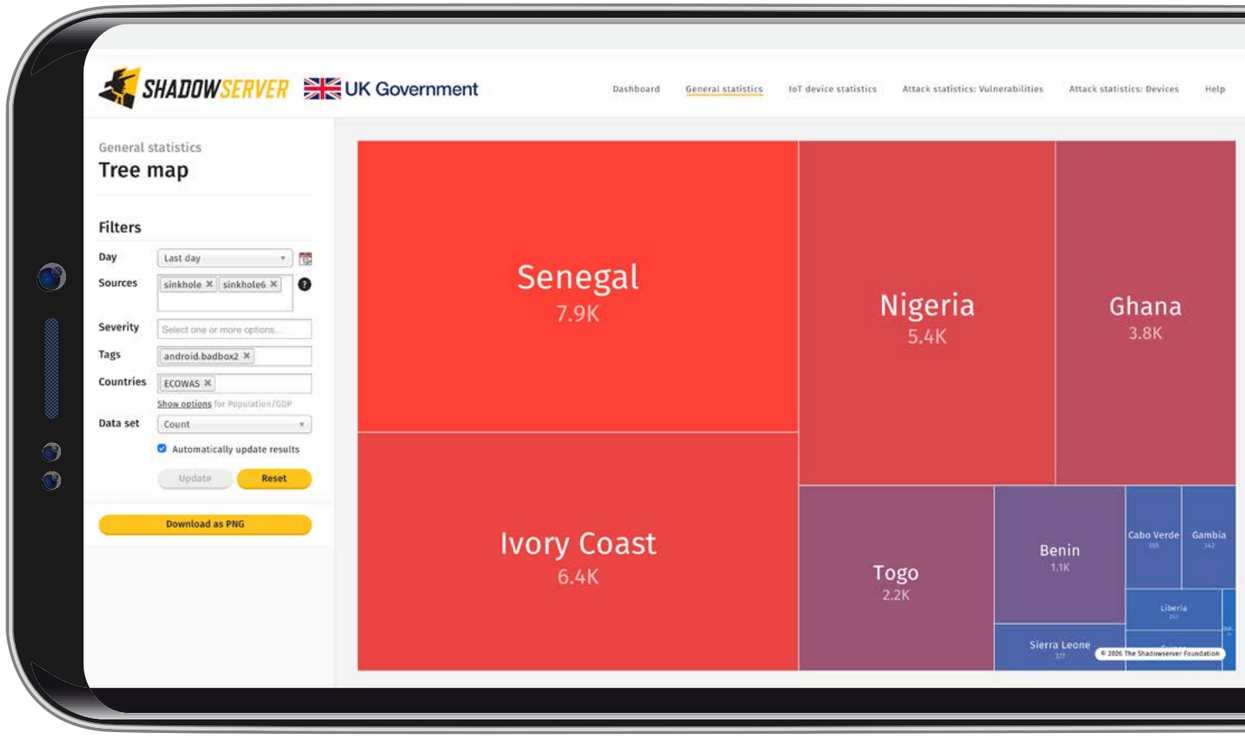


Figura 19. **Dispositivos Android infetados pela Badbox 2.0 na região da CEDEAO que reportam aos servidores de sinkhole da Shadowserver**

O representante oficial da ngCERT pode também consultar os dados num gráfico “Temporal” (ver a Figura 20) para rastrear as infeções pela Badbox 2.0 na região da CEDEAO que reportam aos servidores de sinkhole da Shadowserver ao longo de um determinado período de tempo (neste caso, um período de 3 meses). O representante oficial da ngCERT também pode deslizar sobre o gráfico para revelar dados estatísticos para um determinado dia.

RECOMENDAÇÃO:
O Painel público da Shadowserver pode ser uma ferramenta eficaz para informar os principais intervenientes (por exemplo, líderes governamentais, decisores, investigadores no âmbito da cibersegurança, especialistas em proteção de redes, órgãos de comunicação social e outros) sobre as mais recentes ameaças cibernéticas que afetam o seu país e/ou a região. O Painel permite que o público consulte os dados da Shadowserver para obter dados estatísticos agregados, ao nível nacional ou regional associados às mais recentes ameaças cibernéticas que ocorreram nos dois anos anteriores. Este pode então ser utilizado para priorizar e monitorizar os esforços de mitigação para minimizar ou erradicar ameaças críticas. O Painel pode ser consultado para obtenção de dados estatísticos associados a um país individual bem como a uma região, incluindo uma consulta recém-criada especificamente para a região da CEDEAO.

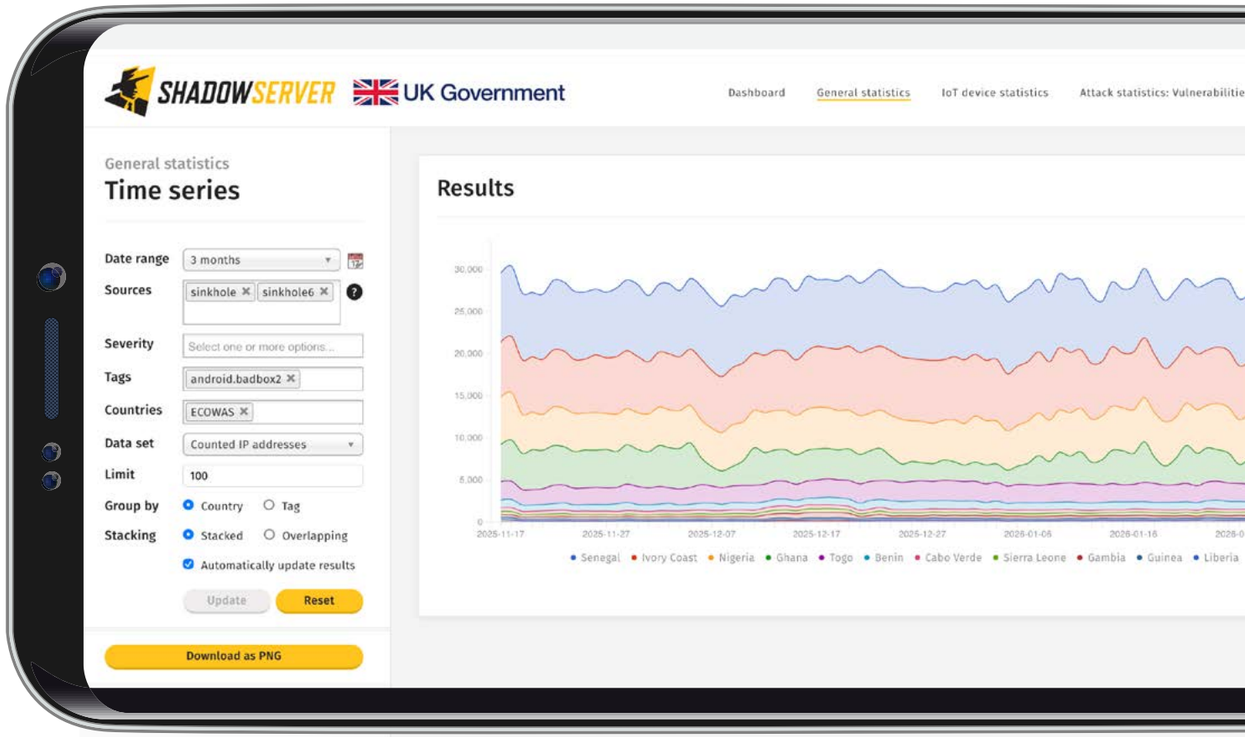


Figura 20. **Dispositivos Android infetados pela Badbox 2.0 na região da CEDEAO que reportam aos servidores de sinkhole da Shadowserver ao longo dos últimos 3 meses a partir da data de consulta**

Glossário

Inventário de ativos: um catálogo completo, continuamente atualizado de todo hardware, software, dados e componentes de rede que uma organização possui ou utiliza, crucial para identificar vulnerabilidades, gerir riscos, detetar ameaças e responder a incidentes.

Superfície de ataque: quaisquer possíveis pontos de entrada ou vetores de ataque, incluindo vulnerabilidades de software, que os perpetradores de ataques podem explorar para invadir um sistema

Trojan bancário: um tipo de software malicioso que se disfarça como software legítimo para enganar os utilizadores a instalá-lo, com o principal objetivo de roubar informações financeiras confidenciais (por exemplo, credenciais de contas bancárias, dados de cartões de crédito, etc.) para executar transações financeiras não autorizadas.

Botnet: uma rede de dispositivos interligados infetados com malware e controlados como um grupo sem o conhecimento ou consentimento dos proprietários; muitas vezes utilizada por agentes de ameaças para facilitar burlas criminosas, incluindo o envio de e-mails de spam e phishing, a perpetração de ataques de negação de serviço e roubo de dados, para citar alguns.

Comprometimento de e-mail empresarial (BEC): um tipo de burla fraudulenta online na qual criminosos cibernéticos se fazem passar por indivíduos de confiança (por exemplo, CEO, fornecedores, etc.) associados a uma empresa, incluindo através de spoofing ou intrusão em contas de e-mail legítimas desses indivíduos, para enganar funcionários a efetuar transferências de dinheiro, alterar dados de transação de pagamento ou enviar dados confidenciais como informações fiscais ou credenciais de início de sessão.

ID de vulnerabilidades e exposições comuns (CVE): falhas de segurança divulgadas publicamente em software, hardware ou firmware às quais foram atribuídas um identificador único, ou ID de CVE, para facilitar a comunicação consistente e o rastreio de vulnerabilidades na comunidade de cibersegurança.

Ativo comprometido: qualquer recurso organizacional (incluindo um servidor, rede, conta ou dados) cuja segurança foi violada, levando ao acesso não autorizado, divulgação, modificação ou destruição, impactando assim a respetiva confidencialidade, integridade ou disponibilidade.

Injeção de código para roubo de credenciais: um tipo de ciberataque no qual os agentes de ameaças exploram vulnerabilidades numa aplicação para injetar e executar código numa rede ou sistema visado para recolher credenciais como os nomes de utilizador e as palavras-passe.

Infraestrutura crítica: os ativos, sistemas e redes fundamentais – tanto físicos como virtuais – que são essenciais para o funcionamento adequado da economia de um país, segurança e saúde, incluindo, mas não se limitando, os setores como a energia, sistemas de água, recursos nucleares, transportes, telecomunicações, defesa e sistemas de alimentação e agricultura.

Agente de ameaça cibernética: qualquer pessoa ou grupo de pessoas que causam intencionalmente danos na esfera digital, incluindo criminosos cibernéticos, hackers de estados soberanos/governo, terroristas, ativistas hackers (hacktivistas) e agentes internos.

Cenário de ameaças cibernéticas: o ambiente amplo e em evolução de potenciais e reconhecidos riscos de cibersegurança, ameaças e perigos, incluindo os tipos de perpetradores de ataques e respetivas motivações, que afetam grupos de utilizadores, organizações, setores específicos ou um período particular.

Glossário

Darknet: uma rede que exige software específico para o seu acesso, resultando em partes ocultas da Internet concebidas para anonimato.

Extorsão através da fuga de dados: um ciberataque no qual os criminosos roubam dados confidenciais e depois exigem um resgate para impedir a divulgação pública dos dados, venda ou outra utilização indevida que possa resultar em diversos prejuízos financeiros, legais e reputacionais para a vítima.

Site dedicado à divulgação de fugas de dados: um website ou plataforma web, frequentemente alojado(a) na dark web, onde criminosos cibernéticos divulgam publicamente os nomes e dados roubados de organizações vítimas como parte de um ataque de ransomware e/ou extorsão através de fuga de dados, concebido para coagir as vítimas a pagar resgate para evitar prejuízos financeiros, legais e reputacionais que possam resultar da divulgação dos dados confidenciais.

Dispositivos: as entidades de hardware (como computadores e servidores) numa rede.

Negação de serviço distribuído (DDOS): um tipo de ciberataque no qual múltiplos sistemas comprometidos, frequentemente orquestrado como uma botnet, invadem uma rede visada, servidor ou serviço online com um considerável volume de tráfego capaz de provocar lentidão ou até causar o colapso dos sistemas visados. Os ataques DDOS são altamente perturbadores e capazes de causar períodos de imobilização, perdas financeiras e danos reputacionais significativos.

Sistema de nomes de domínio (DNS): um sistema que traduz nomes de domínio de fácil leitura (como www.exemplo.com) em endereço IP legíveis por máquina (como 192.0.2.44) que os computadores utilizam para estabelecer ligação e procurar recursos online ao mesmo tempo que assegura que os utilizadores não tenham de memorizar uma cadeia de números longa num endereço IP para obter acesso a websites ou serviços online.

Serviço de alerta precoce: um serviço gratuito oferecido por muitas CSIRT Nacionais (bem como algumas CERT Sectoriais, ISAC (Centros de Partilha e Análise de Informação) e outras entidades com grandes grupos destinatários) no qual grupos de destinatários fornecem os respetivos endereços IP públicos e nomes de domínio e, por sua vez, recebem notificações automáticas de alerta sobre dispositivos e serviços expostos, vulneráveis e comprometidos na sua rede para facilitar a remediação oportuna.

Firewall: um sistema de segurança da rede que atua como uma barreira entre uma rede interna fiável e uma rede externa não fiável, como a Internet.

Sensores honeypots: alvos falsos configurados para parecerem legítimos, contudo, vulneráveis, ativos de redes (incluindo aplicações de software, servidores e outros dispositivos) com a finalidade pretendida de atrair os agentes de ameaças a perpetrarem ataques. Os sensores registam as atividades do perpetrador do ataque e recolhem informações sobre as táticas, ferramentas e procedimentos/técnicas do perpetrador do ataque. Os dados recolhidos ajudam a identificar as origens dos ataques, novos métodos de ataque, a desenvolver defesas e a prevenir ataques futuros.

Implante: um programa incorporado numa rede ou sistema para criar mecanismos de acesso remoto e executar várias funções sem o conhecimento do utilizador, incluindo roubo de dados, perturbação e manutenção de acesso persistente.

Centro de Partilha e Análise de Informação (ISAC): uma organização orientada pelos membros que recolhe, analisa e dissemina informações sobre ameaças acionáveis para ajudar os membros a atenuar os riscos de forma proativa.

Endereço de protocolo de Internet (IP): um identificador numérico único atribuído a cada dispositivo que estabelece ligação à Internet.

Vulnerabilidade explorada conhecida: uma vulnerabilidade num software, hardware, aplicação ou sistema que está a ser ativamente explorada pelos agentes de ameaças, tornando a vulnerabilidade um risco de segurança de elevada prioridade que exige correção imediata para impedir uma intrusão.

Operação de desmantelamento de cibercrime das autoridades policiais: um esforço proativo efetuado pelas Autoridades Policiais para desmantelar atividades de cibercrime ao desmantelar infraestruturas criminosas (por exemplo, servidores, websites, etc.), capturar agentes de ameaças e apreender bens.

Glossário

Malware: designação abreviada de "software malicioso" que consiste em qualquer software especificamente concebido para danificar, interromper ou obter acesso não autorizado a um sistema informático.

Equipas Nacionais de Resposta a Incidentes de Segurança Informática (CSIRT nacionais): uma entidade designada pelo governo que coordena respostas a nível nacional a incidentes cibernéticos, protegendo infraestruturas críticas, operações governamentais e a segurança económica através da gestão de ameaças relacionadas com cibersegurança, disseminação de informações, desenvolvimento de conhecimento e implementação de estratégias cibernéticas; servindo muitas vezes como um ponto central para reportar e responder a eventos cibernéticos de grande escala num país.

Phishing: um tipo de ciberataque que utiliza e-mails fraudulentos, mensagens de texto, chamadas telefónicas ou websites para enganar vítimas no sentido de partilharem dados confidenciais (como nomes de utilizador, palavras-passe, informações sobre contas bancárias, números de cartões de crédito ou outros dados importantes), transferir malware ou, de outra forma, exporem-se a atividade cibercriminosa.

Ransomware: um tipo de software malicioso (isto é, malware) que encripta/bloqueia os ficheiros e sistemas de uma vítima, tornando-os inacessíveis e que, em seguida, exige um pagamento de resgate em troca da chave de desencriptação para restaurar o acesso.

Entidade de registo: uma empresa que vende e gere nomes de domínio, que atua como intermediária para indivíduos e empresas (conhecidos como «titulares de registo») e as organizações (conhecidas como «registos») que controlam domínios de nível superior.

Registo: um registo de nomes de domínio é uma organização que gere nomes de domínio de nível superior através da criação de extensões de nomes de domínio, definição das regras para um nome de domínio particular e colaboração com entidades de registo para vender nomes de domínio ao público. Por exemplo, a Verisign gere o registo de nomes de domínio .com e o respetivo sistema de nomes de domínio (DNS).

Router: um dispositivo que encaminha pacotes de dados para as partes apropriadas de uma rede informática.

Equipa Sectorial de Resposta a Incidentes de Segurança Informática (CSIRT Sectorial): uma entidade especializada que gere a resposta a incidentes de cibersegurança, promove a partilha de informações para atenuar ameaças e oferece conhecimento especializado e competências técnicas para um setor particular de um país ou economia (por exemplo, água, saúde, energia, financeiro, transportes, etc.)

Aplicação do lado do servidor: refere-se às funções, procedimentos, cálculos ou métodos de processamento executados num servidor e geridos nos bastidores num sistema remoto em vez de no dispositivo de um utilizador.

Serviços: as aplicações ou funções de software que os dispositivos fornecem ou consomem (como um servidor web, e-mail ou armazenamento de ficheiros) que permitem a comunicação na rede e a partilha de recursos.

Protocolo Simples de Gestão de Rede (SNMP): um protocolo que desempenha um papel crucial na monitorização, gestão e proteção de dispositivos de rede, ao permitir que os administradores de redes recolham informações, configurem dispositivos e respondam a eventos na rede por via remota, tornando-o assim uma ferramenta essencial para manter o desempenho e a proteção de redes.

Sinkholing: uma técnica que envolve interromper as comunicações entre os dispositivos infetados com malware das vítimas e os servidores controlados de forma criminosa para os quais o malware os direciona a comunicar. O tráfego é redirecionado para os

servidores de sinkhole pertencentes a uma entidade responsável, de modo que os criminosos deixem de obter acesso e controlo sobre os dispositivos das vítimas apesar do facto de os dispositivos permanecerem infetados com malware, salvo e até que sejam remediados.

Serviços VPN: um serviço VPN (rede privada virtual) é uma ferramenta online que cria um "túnel" encriptado seguro para tráfego na Internet, ocultando um endereço IP real do utilizador e a localização para melhorar a privacidade e a segurança.

Vulnerabilidade/vulnerabilidades: uma fraqueza num sistema de informação, procedimentos de segurança do sistema, controlos internos ou implementação que possa ser explorada por um agente de ameaça cibernética para obter acesso não autorizado ou causar danos a um sistema, rede ou dispositivo.

Web Shell: um script ou programa malicioso que os agentes de ameaças implementam num servidor web comprometido para obter (e manter) o acesso remoto e o controlo sobre este, permitindo assim que os agentes de ameaças executem uma variedade de atividades maliciosas, incluindo roubo de dados e distribuição de malware.

Vulnerabilidade de dia zero: uma vulnerabilidade de segurança no software, hardware ou firmware desconhecida para o fornecedor que os perpetradores de ataques podem explorar antes que o fornecedor tenha conhecimento desta e tenha a oportunidade de desenvolver uma correção para solucioná-la.