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

ECOWAS Region:

Cybersecurity Insights and Recommendations

February 2026

SHADOWSERVER

Contents

Executive Summary

The Economic Community of West African States (ECOWAS) seeks to promote economic cooperation among its twelve member states in order to raise living standards and promote economic development. In pursuit of this objective, the ECOWAS Commission and the region as a whole have increasingly embraced digital technologies as a key driver of growth. The result has been a rapid digital transformation in recent years that has helped spur economic growth and development. Yet, it has also brought to light a host of institutional and operational cybersecurity deficiencies or "gaps" within the region, some of which are significant. These factors (i.e., economic growth, an expanded digital footprint, and known cybersecurity deficiencies) combine to make the region an increasingly attractive and vulnerable target of **cyber threat actors*.**[1]

The number, scale and impact of cyberattacks in the ECOWAS region are increasing at an alarming rate. An INTERPOL report issued in June 2025 warned of a sharp rise in cybercrime in Africa, with cybercrime accounting for more than 30-percent of all reported crime in Western Africa.[2] The report further noted estimated financial losses of more than $3 billion from cyber incidents across the continent between 2019 and 2025.[3]

The region recently endured costly **ransomware*** attacks on the Electricity Company of Ghana[4] and the Central Bank of The Gambia,[5] disruptive **distributed denial of service (DDoS)*** attacks against Senegalese government websites[6] and telecom operator MTN Nigeria,[7] and the devastating breach of Ivorian-based fintech payment processor CinetPay that owes more than $1 million to customers.[8] The result has been a growing concern over the region's cybersecurity capabilities and a strong sense of urgency to act.

Addressing the gaps identified in this report is critical to ensuring cybersecurity capabilities and overall cyber resilience keep pace with the

[1] Words and phrases in bold print and denoted with an asterisk (*) are defined in the "Glossary" at the end of this report.

[2] "New INTERPOL Report Warns of Sharp Rise in Cybercrime in Africa," *INTERPOL News Release*, June 23, 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*, August 26, 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*, Oct. 1, 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*, Nov. 17, 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*, May 27, 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*, July 9, 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*, February 1, 2026. https://techcabal.com/2026/02/01/cinetpay-cyberattack/

region's rapid digital expansion as well as the volume, magnitude, and sophistication of emerging threats targeting the region. Left unaddressed, these gaps could make the region's cybersecurity increasingly deficient, thereby jeopardizing economic development, eroding public trust, and impacting services that affect quality of life.

The current cyber threats facing the ECOWAS region are well documented. They include **ransomware*,** attacks on **critical infrastructure*, DDoS*** attacks, **business email compromise*,** online fraud scams, and digital sextortion, to name a few. This report uses The Shadowserver Foundation's cyber threat data, analysis, and many years of expertise in the field to inform key stakeholders on the current institutional and operational cybersecurity gaps that make the ECOWAS region particularly vulnerable to these and other cyber threats. The report further provides recommended actions that can be undertaken on national and regional levels to address those gaps.

The most pressing and significant *institutional* gaps relate to the need for effective cybersecurity institutions within the region, particularly **National Computer Security Incident Response Teams (National CSIRTs)*,** an **ECOWAS Information Sharing and Analysis Center (ISAC)*,** and **Sectoral CSIRTs*.** To effectively carry out their respective duties and responsibilities, these entities require access to free and/or affordable data, tools, services and platforms; in-house technical experts; training and capacity building services; maturity assessments to measure developmental progress; global and regional partnerships; and the creation of **early warning services*** to serve their constituencies.

Aside from the *institutional* gaps, lesser known are the technical *operational* cybersecurity gaps associated with the cyber **attack surfaces*** of ECOWAS Member States. Like many attack surfaces, the ECOWAS region is characterized by **devices*** and **services*** publicly exposed to the Internet (which unnecessarily expand the attack surface and offer potential entry points to a network); critical **vulnerabilities*** in exposed assets that can be exploited by threat actors if not remediated; **compromised assets*** that can be *further* exploited if not remediated; and **malware***-infected devices over which threat actors had (or have) unauthorized access and control, often as part of a larger **botnet*.**

An important factor in managing the ECOWAS region's attack surface will involve the implementation of appropriate regulations by each member state that ensure key network defenders (particularly those in government and critical infrastructure sectors) conduct **asset inventories*,** ensure assets are not needlessly exposed to the Internet, and timely remediate critical / high severity **vulnerabilities*, known exploited vulnerabilities*,** and **compromised assets*.**

It is imperative that key stakeholders understand their respective cyber attack surfaces to enable effective policymaking, craft appropriate legislation, and implement protective network security measures. It is essential that government leaders, policymakers, network defenders, and cybersecurity experts work collaboratively to address the issues identified in this report.

One way to help inform key stakeholders on a nation's and/or region's attack surface is to utilize Shadowserver's public Dashboard. The Dashboard allows the public to query Shadowserver's data for aggregated, country-level or regional-level statistics associated with the latest cyber threats spanning the prior two years. It can then be used to prioritize and track remediation efforts to minimize or eradicate critical threats. The Dashboard can be queried for statistics associated with an individual country as well as a region, including a newly created query specifically for the ECOWAS region.

Recommendations

The key recommended actions stemming from the institutional and operational cybersecurity deficiencies or gaps identified in this report are as follows:

Institutional Recommendations:

NATIONAL CSIRTS

Establish an operationally effective National CSIRT within each ECOWAS Member State.

ECOWAS ISAC

Establish an ECOWAS ISAC to help ensure that all National CSIRTs in the region work collaboratively, share information, progress in their development, and foster vital national, regional and international partnerships.

SECTORAL CSIRTS

Establish a Sectoral CSIRT for a critical infrastructure sector identified as most vulnerable and most vital within each country. As funding permits, additional Sectoral CSIRTs can thereafter be established across sectors to ensure that each sector receives expertise, threat intelligence, risk management, and incident response services tailored to the unique needs of its sector.

ACCESS TO FREE / AFFORDABLE DATA, TOOLS, AND SERVICES

National CSIRTs and network defenders of all types and across all sectors should take advantage of available free and/or affordable cyber threat data, tools, services, and platforms. This includes Shadowserver's free, daily network remediation reports, as well as free open-source tools (including IntelMQ, Elasticsearch, Kibana, and others) needed to ingest, store, parse, search, visualize, analyze, and effectively utilize threat data feeds. Consideration should also be given to potentially affordable commercial tools and services, including Arctic Hub, a cyber threat intelligence automation platform available for free the first year and at reduced rates in subsequent years for qualifying National CSIRTs through Arctic Security's CSIRT Development Program. As shown on Arctic Security's website, The Gambia's National CSIRT (gmCSIRT) is a current participant in the program.

IN-HOUSE TECHNICAL EXPERTS

Ensure that each National CSIRT and network defenders of government and critical infrastructure systems have employees that possess adequate technical skills to effectively secure and defend the nation's networks. ECOWAS Member States should collaborate with universities to develop training and internship programs that can act as a pipeline for technically skilled talent. Member states should also collaborate with the private sector to develop programs in which seasoned private sector experts can do temporary but extended work details at the National CSIRT and government / critical infrastructure entities to mentor and train less experienced, less technical employees.

Institutional Recommendations:

TRAINING AND CAPACITY BUILDING

Seek opportunities for training and capacity building projects (particularly operational projects focused on setting up and effectively using available free / open source data, tools, services and platforms). Such projects are often funded by government foreign ministries (including the German Federal Foreign Office and GIZ, and the UK's Foreign, Commonwealth and Development Office) private sector entities (including Microsoft and Google), as well as the World Bank, the United Nations, and the European Union, to name a few.

PARTNERSHIP DEVELOPMENT

Create a framework that requires National CSIRTs to build and maintain strong professional relationships with constituents / stakeholders within their respective countries (including Internet service providers, critical infrastructure operators, government entities, businesses, universities, state and local governments, healthcare providers, financial institutions, etc.), as well as with National CSIRTs within the ECOWAS region and around the world. These relationships are key to fostering information-sharing, collaboration, and capacity building. Opportunities for National CSIRTs to develop global partnerships include through an ECOWAS ISAC, by becoming a member of FIRST.org, and by joining Shadowserver's free online Alliance Mattermost chat platform that enables direct access to Shadowserver staff, Alliance Partners from across the industry, and National CSIRTs from around the world.

MATURITY ASSESSMENTS

To establish a baseline maturity level, each National CSIRT should be mandated to undergo the Open CSIRT Foundation's Security Incident Management Maturity Model (SIM3) self-assessment online tool and implement recommendations for improvement.

EARLY WARNING SERVICES

National CSIRTs, Sectoral CSIRTs, ISACs, and other entities with large constituencies should be mandated to offer free Early Warning Services in which their constituents receive automated alert notifications about exposed, misconfigured, abusable, vulnerable, and compromised devices and services on their networks to facilitate timely remediation. Consultation with one of the many National CSIRTs that operate such Early Warning Services is recommended, such as the United Kingdom's National Cyber Security Centre (UK NCSC) and the Dominican Republic's CSIRT-RD.

Operational Recommendations:

ASSET INVENTORIES

Establish policies to mandate the conducting of periodic asset inventories, particularly in government and critical infrastructure sectors. Doing so will aid network owners in timely patching and remediation efforts as new critical vulnerabilities emerge. *See* "Binding Operational Directive 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks".

ENSURE ASSETS ARE NOT NEEDLESSLY EXPOSED TO THE PUBLIC INTERNET

Ensure that network owners (in particular, critical infrastructure, government, and large ISPs) do not needlessly expose certain device types and services to the public Internet unless necessary for functionality purposes. Doing so will reduce the region's overall attack surface. Focused trainings and workshops with National CSIRTs, ISPs, and other network owners in the ECOWAS region could culminate in proactive surge activity to target and reduce instances of unnecessarily exposed devices and services.

REGULATIONS MANDATING REMEDIATION OF CRITICAL AND HIGH RISK VULNERABILITIES

Implement regulations that require government agencies and critical infrastructure to remediate vulnerabilities designated as "critical risk" within 15 calendar days and those designated as "high risk" within 30 calendar days of initial detection. *See* "Binding Operational Directive (BOD) 19-02: Vulnerability Remediation Requirements for Internet-Accessible Systems".

REGULATIONS MANDATING REMEDIATION OF KNOWN EXPLOITED VULNERABILITIES

Implement regulations that require government and critical infrastructure to remediate "known exploited vulnerabilities" within 14 days. DHS-CISA maintains a catalog of Known Exploited Vulnerabilities (KEV) that identifies vulnerabilities seen actively exploited in the wild that must be remediated by U.S. federal government agencies. ENISA maintains a similar catalog known as the European Union Vulnerability Database. Finally, Shadowserver's public Dashboard maintains Shadowserver's list of known exploited vulnerabilities identified via its honeypot sensor network. *See* "Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities".

REGULATIONS MANDATING REMEDIATION OF IDENTIFIED COMPROMISED AND MALWARE-INFECTED DEVICES

Implement regulations requiring National CSIRTs, government agencies, critical infrastructure, ISPs, and other network owners in the region to remediate identified compromised and malware-infected devices within a brief but specified time period, including those identified in Shadowserver's free, daily network remediation reports.

Operational Recommendations:

THREAT MITIGATION / ERADICATION CAMPAIGNS

Mandate National CSIRTs, in coordination with Internet Service Providers (ISPs), to devise and implement nationwide threat mitigation and eradication campaigns against critical vulnerabilities and compromised devices on networks throughout the country, and track the progress of remediation efforts. One such example is the nationwide campaign led by the Australian Signals Directorate (ASD) to eradicate Bad Candy implants in compromised Cisco IOS XE devices throughout Australia.

SHADOWSERVER'S FREE PUBLIC DASHBOARD

Shadowserver's public Dashboard can be an effective tool to inform key stakeholders (e.g., policymakers, government leaders, network defenders, cybersecurity researchers, etc.) about the latest cyber threats affecting their country and/or the region. The Dashboard allows the public to query Shadowserver's data for aggregated, country-level or regional-level statistics associated with the latest cyber threats spanning the prior two years. It can then be used to prioritize and track remediation efforts to minimize or eradicate critical threats. The Dashboard can be queried for statistics associated with an individual country as well as a region, including a newly created query specifically for the ECOWAS region.

Introduction

A key focus of ECOWAS' efforts has been in the areas of cybersecurity and cybercrime. In 2021, for example, ECOWAS adopted its *Regional Cybersecurity and Cybercrime Strategy*, outlining actions to be taken at the national level to "increase cyber resilience in the region, help Member States strengthen their cybersecurity capacities, protect their cyberspace and critical information infrastructures, as well as build confidence and security in the use of information and communication technologies (ICT).[9] Included among the suggested actions to be taken are "the adoption of national cybersecurity strategies, building cybersecurity developments and capacity, and prioritising cybersecurity efforts for critical infrastructures and essential services."[10]

The ECOWAS Strategy notes that "the rapid digital transformation underway in West Africa is of great importance to improve the functioning and efficiency of administrations, public policies and economies, as well as the well-being of populations."[11] It is well established that a secure and stable digital infrastructure is necessary for sustained economic growth in the ECOWAS region. Among other things, it will encourage financial investment, increase business development, enhance operational efficiency and productivity, protect critical infrastructure, enable essential government services, provide access to global markets and, perhaps most importantly, foster trust in the region's digital security with consumers, businesses and investors to drive economic growth.

Conversely, the ECOWAS region's rapidly growing economy and expanding digital footprint make it an increasingly attractive target of cyber threat actors. Growing concerns surround the region's cybersecurity deficiencies that could prevent capabilities from keeping pace with the increased threats, leaving the region increasingly vulnerable to attack.

This report was written by The Shadowserver Foundation ("Shadowserver") pursuant to the cyber capacity building project under the ECOWAS-G7 partnership for cybersecurity, the "Joint Platform for Advancing Cyber Security" (JPAC) in West Africa. TheThe project was launched by the ECOWAS Commission in collaboration with Germany's G7 presidency in 2022 and commissioned by the German Federal Foreign Office and the European Union Commission in 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/

The geographic focus of this report is the ECOWAS region and its twelve (12) member states; namely, Benin, Cabo Verde, Côte d'Ivoire, The Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Nigeria, Senegal, Sierra Leone and Togo. Findings and recommendations are derived from Shadowserver's more than 20 years of experience in the field as well as analysis of data relevant to the ECOWAS region during the period 1 October 2024 to 24 April 2025.

The report's objectives are to inform government leaders, policymakers, and other key stakeholders on the following:

The ECOWAS region's cyber **threat landscape*** and **attack surface*** using Shadowserver's actionable threat intelligence, data analysis, and expert insights for the relevant time period

The region's **institutional and operational cybersecurity gaps** that make it increasingly vulnerable to cyber threats

Recommended actions that can be undertaken at the national and regional levels to address the identified cybersecurity gaps to improve digital security and enhance cyber resilience in the ECOWAS region

The potential economic and societal impact should the identified institutional and operational cybersecurity gaps remain unaddressed.

1.0// Shadowserver Insights on Cyber Threats in Ecowas Region

The current **cyber threat landscape*** of the ECOWAS region is characterized by ransomware, attacks on critical infrastructure, distributed denial of service (DDoS) attacks, business email compromise (BEC), online fraud scams, and digital sextortion, to name a few.

An INTERPOL report issued in June 2025 warns of a sharp rise in cybercrime in Africa. The report provides extensive analysis of the current cybercrime threats affecting Africa (including specifically West Africa), and is recommended reading for all key stakeholders in the ECOWAS region. Because the current cyber threats targeting the ECOWAS region are well documented in the INTERPOL report and numerous other sources (e.g., Kaspersky Labs' "Africa Cyberthreat Landscape Report 2025"), this report focuses less on the various and cyber threats themselves, and more on the cybersecurity gaps that make the region vulnerable to these threats. Nevertheless, this report provides the reader with a high-level overview of certain threats for which Shadowserver can provide helpful insights.

1.1// Ransomware and Data Leak Extortion

Ransomware* and related **data leak extortion*** attacks continue to be significant problems in most regions of the world, and the ECOWAS region is no exception. In November 2022, it was reported that hackers breached the digital systems at the Central Bank of The Gambia and demanded a USD $2.5 million ransom payment in return for two terabytes of sensitive data stolen from the bank.[12] The stolen data reportedly included the personal finances of Gambians; data on the national economy; customer and partner databases; data on the turnover of financial transactions with the US and other countries; data relating to the distribution of securities; and data on the liquidity of the nation's commercial banks. Such attacks can result in devastating financial and reputational harm.

Shadowserver collects information on the activity of various ransomware crime groups. The information is collected through systematic observation of ransomware groups' **dedicated leak sites*.** Shadowserver regularly alerts National CSIRTs and Law Enforcement Agencies across the world to information published on the leak sites.

In 2024 and 2025, Shadowserver observed numerous claims from known ransomware groups of attacks against

Actor	Victim Country Location	Date Published On Site	Victim Sector	Employees	Annual Business Revenue ($)
Blacksuit	Nigeria	May 2024	Professional, Scientific, and Technical Services	766	1,090,000,000
	Ghana	October 2024	Utilities Sector	405	29,700,000
Brain Cipher	Ghana	August 2024	Finance and Insurance Sector	106	9,000,000
Hunters International	Cote d'Ivoire	May 2024	Public Administration	1,879	392,000,000
	Senegal	September 2024	Other Services	33	6,000,000
Kill Security	Nigeria	November 2024	Professional, Scientific, and Technical Services	N/A	N/A
	Ghana	February 2025	Finance and Insurance Sector	N/A	N/A
	Nigeria	March 2025	Administrative and Support and Waste Management and Remediation Services	5578	306,800,000
LockBit 3.0	Cote d'Ivoire	February 2024	Professional, Scientific, and Technical Services	211	26,900,000
	Senegal	May 2024	Professional, Scientific, and Technical Services	95	5,000,000
Lynx	Cabo Verde	November 2024	Finance and Insurance Sector	N/A	5,400,000
Pryx	Nigeria	October 2024	Unknown - 29 potential victims	N/A	N/A
RansomHub	Nigeria	January 2025	Professional, Scientific, and Technical Services	1,628	293,800,000
Space Bears	Cote d'Ivoire	August 2024	Administrative and Support and Waste Management and Remediation Services	105	N/A
Funksec	Nigeria	January 2025	Information	N/A	N/A
	Nigeria	December 2024	Public Administration	19627	157,500,000
GDLockerSec	Nigeria	January 2025	Public Administration	N/A	N/A
DragonRansomware	Cote d'Ivoire	December 2024	Administrative and Support and Waste Management and Remediation Services	N/A	N/A

Figure 01. **Ransomware actors with claims of victims in ECOWAS states (Jan 2024 - May 2025)**

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

organizations in the ECOWAS region. However, because organizations that pay the ransom typically are not named on the leak site, there is no way to know definitively the total number of ransomware attacks in a given country or region. Nevertheless, it is anticipated that ransomware and data leak extortion attacks in the ECOWAS region will likely increase as economic growth and digital expansion continue to outpace cybersecurity capabilities.

Figure 01 contains a summary of ransomware victim information in the ECOWAS region collected from ransomware groups' leak sites. The actual victim names and associated URLs have been removed to preserve the victims' anonymity. Please note that Shadowserver may not observe all existing leak sites, especially those associated with more regionally focused threat actors.

As seen in Figure 01, the claims concern a variety of sectors, both public and private. Most claims relate to Nigeria, Cote d'Ivoire and Ghana.

Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data. As businesses continue to develop and economies continue to grow in the ECOWAS region, ransomware attacks will likely increase. If digital security in the region fails to keep pace with the current economic growth, the results could be severe with continued increases in cybercrime and significant decline in business development and financial investment in the region.

1.2// Attacks on Critical Infrastructure

Cyberattacks against **critical infrastructure*** networks take many forms, typically depending on the nature and motivations of the attacker. For example, nation state threat actors may seek to breach critical infrastructure networks for purposes of espionage, destructive harm, or the making of political statements, whereas transnational cybercrime groups deploy ransomware for purposes of monetary gain.

In 2022, the Electricity Company of Ghana (ECG), the largest electricity supplier in the country, was the victim of a ransomware attack. The attack reportedly left customers without power and/or unable to purchase power for several days as a result of the attackers encrypting various sections of ECG's system rendering them inoperable.[13] ECG's managing director later confirmed the ransomware attack resulted in a loss of nearly GH¢500 million (approximately EUR 40 million or USD 47 million).[14]

In December 2024, Nigeria's National Bureau of Statistics (NBS) suffered a cyberattack that temporarily paralyzed its systems and disrupted public access to critical national data for nearly a month.[15] The breach also sparked concerns over "the potential exposure of critical data, including economic reports, population statistics, and other essential information vital for national planning and policymaking."[16]

These examples illustrate the increasing focus of cyber threat actors on national institutions and critical infrastructure, as well as the societal impact that can result from such attacks.

[13] "ECG Systems Hacked with Ransomware," *Ghana Business News*, Oct. 1, 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, Aug. 29, 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*, January 9, 2025. https://techpoint.africa/news/nbs-to-resume-services-on-january-15/

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

1.3// Distributed Denial of Service (DDoS)

Shadowserver collects data from approximately 2,700 **honeypot sensors*** which it maintains at data centers and other locations around the world. These sensors are decoys configured to appear as legitimate, yet vulnerable, network assets (including software applications, servers and other devices) for the intended purpose of luring threat actors to attack. The sensors then log the attacker's activities and collect information on the attacker's tactics, tools, and procedures / techniques. The collected data helps identify sources of attacks, new attack methods, develop defenses, and prevent future attacks.

Using observations from our honeypot sensors, Shadowserver monitors various forms of DDoS attacks. As a result, we are able to track the victims of attacks at a given point in time. We observe DDoS attacks happening regularly in the ECOWAS region, primarily in Nigeria.

As shown in Figures 02 and 03, the most attacked (by unique target IP address and by most attempts) was Nigeria.

DDoS attacks can be highly disruptive and extremely costly for businesses and governments to withstand.

In May 2023, a group of hackers called Mysterious Team caused multiple Senegalese government websites to go offline as a result of a DDoS attack.[17]

Figure 02. **DDoS Attacks by unique target IP address - ECOWAS Region**

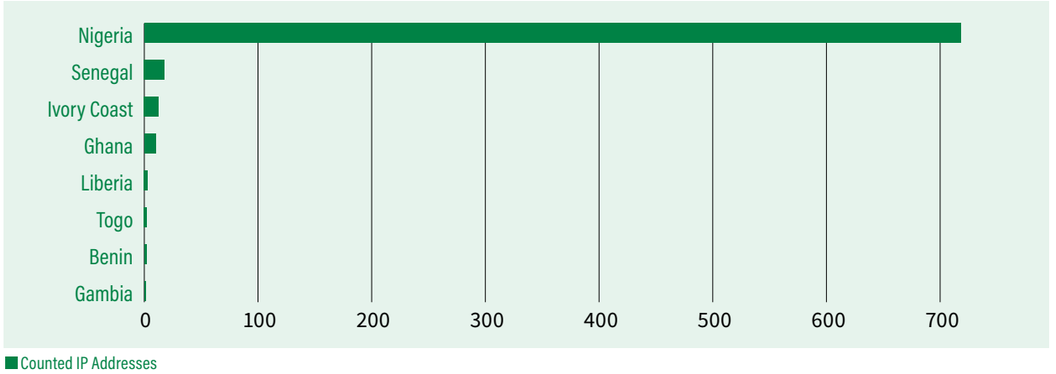
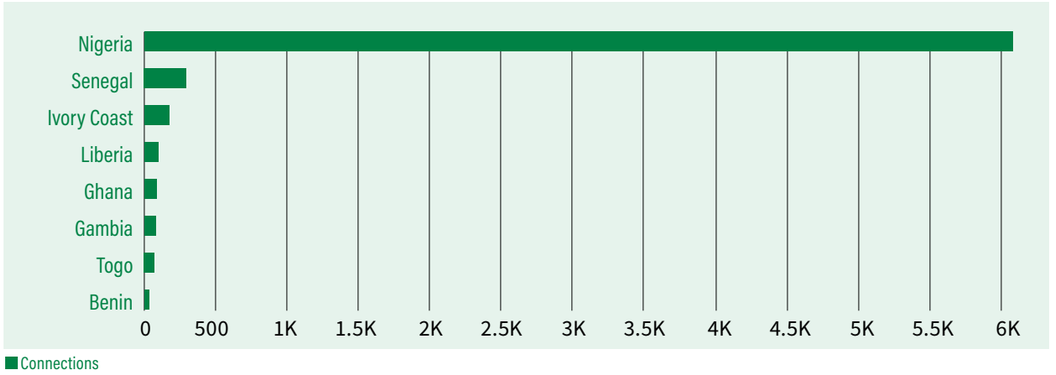


Figure 03. **DDoS Attacks - by unique attempts - ECOWAS Region**



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

In August 2023, Nigeria's largest telecom operator, MTN Nigeria, was the victim of one of the most extensive DDoS attacks ever recorded against a West African company. The attack was conducted by a notorious hacktivist group known as Anonymous Sudan and lasted for nearly eight hours as MTN's network was flooded with malicious traffic from compromised computers around the world in an effort to disrupt MTN's voice and data services.[18]

These examples demonstrate that DDoS attacks can have a devastating impact on society and will impede business growth and economic development if not addressed. Comprehensive DDoS protection and mitigation strategies must be designed and implemented at the national and regional levels.

1.4// Business Email Compromise (BEC)

Business Email Compromise (BEC) scams are reportedly on the rise in the ECOWAS region. In July 2024, Nigeria's National Information Technology Department (NITDA) issued a nationwide alert warning of alarming rates in BEC scams affecting individuals and organizations across Nigeria.[19]

Additionally, although details are limited and the event was not widely reported, INTERPOL's recent announcement of Operation Sentinel included reference to a major petroleum company in Senegal that "detected a sophisticated BEC scheme in which fraudsters infiltrated internal email systems and impersonated executives to authorize a fraudulent wire transfer of USD 7.9 million." The announcement noted that Senegalese authorities urgently froze destination accounts and successfully halted the transaction before funds could be withdrawn.

Less sophisticated BEC tactics include scammers creating fake email addresses and domains similar to legitimate ones to trick recipients. More sophisticated BEC tactics include scammers breaching an email server or gaining unauthorized access to an employee's email account through phishing or malware and sending requests for invoice payments to vendors listed in the employee's email contacts. While preventing an employee from falling victim to a BEC scam relies primarily on training and education, securing email servers and accounts is also critically important as BEC scams become more sophisticated.

[18] "Inside the Eight-Hour Long Cyberattack that Tried to Cripple MTN Nigeria," *Techcabal*, July 9, 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*, July 17, 2024. https://technologytimes.ng/nitda-warns-of-business-email-compromise-scams/

2.0// Institutional Cybersecurity Gaps and Recommendations

2.1// **National Computer Security Incident Response Teams (National CSIRTs)**

2.2// **ECOWAS ISAC**

2.3// **Sectoral ISACs**

2.4// **Access to Free / Affordable Data, Tools, and Services**

2.5// **In-House Technical Experts**

2.6// **Training and Capacity Building**

2.7// **Partnership Development**

2.8// **Maturity Assessments**

2.9// **Early Warning Services**

2.1// National Computer Security Incident Response Teams (National CSIRTs)

Two ECOWAS Member States do not currently have a defined National CSIRT.

Establishing a National CSIRT within each ECOWAS nation is a critical first-step to ensuring a more cybersecure nation (and region) and should be a top priority.

The key challenge, however, will be ensuring that all National CSIRTs in the region are effective in carrying out their duties and responsibilities. The recommendations contained herein focus on ways to make National CSIRTs, and similar entities such as ISACs and Sectoral CSIRTs, most effective.

RECOMMENDATION:
Establish an operationally effective National CSIRT within each ECOWAS Member State.

2.2// ECOWAS ISAC

An Information Sharing and Analysis Center (ISAC) is a member-driven organization that gathers, analyzes, and disseminates actionable threat information to help members proactively mitigate risk. Shadowserver is aware that an ECOWAS ISAC is currently being planned. The initiative aims to strengthen regional cybersecurity by creating a collaborative platform for sharing threat intelligence, best practices, and resources across West African nations. Unlike a National CSIRT, the operating costs associated with a regional ECOWAS ISAC can be shared among the member states.

Shadowserver provides free, daily cyber threat intelligence to 201 National CSIRTs responsible for 175 countries to help them secure their nation's networks. An effective National CSIRT is essential to achieving greater cyber resilience within a country.

It serves as a country's central authority for responding to and managing national-level cybersecurity incidents, protecting national critical infrastructure, providing guidance and advisories to public and private sectors, and facilitating cooperation for cross border cyber events.

A National CSIRT's key responsibilities include incident detection and analysis, incident response and remediation, information sharing and dissemination of alerts/threat intelligence/advisories, coordination with domestic agencies and international counterparts, and implementing preventative measures within a country.

RECOMMENDATION:
Establishing an ECOWAS ISAC is strongly recommended and will be vital in helping to ensure that all National CSIRTs in the region work collaboratively, share information, and progress in their development. An ECOWAS ISAC will also help foster regional partnerships with entities such as Internet service providers (ISPs) and critical infrastructure operators, as well as international partnerships with National CSIRTs. Unlike a National CSIRT, the development and operating costs associated with a regional ECOWAS ISAC can be shared among the member states.

2.3// Sectoral CSIRTs

A Sectoral CSIRT is a specialized entity that handles cybersecurity incident response, fosters information sharing to mitigate threats, and offers specialized knowledge and expertise for a particular sector of a country or economy (e.g., water, health, energy, financial, transportation, etc.). It serves to effectively prevent and respond to threats unique to its sector. Protecting critical infrastructure and government services should be prioritized. One way this can be done is by developing Sectoral CSIRTs for each critical infrastructure sector. Following the establishment of an effective National CSIRT, Sectoral CSIRTs should be created as available funding permits, starting with the sector identified as most critical. Once established, the creation of additional Sectoral CSIRTs can then be scaled across the various sectors over time.

RECOMMENDATION:
Following the establishment of an effective National CSIRT within each member state, a Sectoral CSIRT should be created for the critical infrastructure sector identified as most vulnerable and most vital to protect within each country. As available funding permits, subsequent Sectoral CSIRTs can be established within other sectors. This will help to ensure that each critical infrastructure sector receives expertise, threat intelligence, risk management, and incident response services tailored to the unique needs of its sector.

2.4// Access to Free/Affordable Data, Tools, and Services

It is imperative that National CSIRTs, Sectoral CERTs, ISACs, and network defenders of all types and across all sectors have access to quality cyber threat data, tools, services, and platforms needed to adequately perform their respective duties and functions. This includes the necessary tools to properly ingest, store, parse, search, visualize, analyze and effectively utilize the cyber threat data. Automated platforms are also needed for disseminating alert notifications to affected constituent network owners about critical vulnerabilities and compromised assets to ensure timely patching.

Unfortunately, limited available funding and the high costs associated with many of these items present a significant challenge. However, free or otherwise affordable threat data, tools, services, and platforms are available, and all network defenders in the region should take full advantage of these valuable resources to help them adequately secure their networks.

In the ECOWAS region, for example, National CSIRTs in Benin, Côte d'Ivoire, The Gambia, Ghana, Nigeria, Sierra Leone, and Togo all subscribe to Shadowserver's free, daily network remediation reports to help them secure their nation's networks. These reports provide each National CSIRT with nationwide data associated with all IPs that geolocate to their respective countries. The reports identify exposed, abusable, misconfigured, vulnerable and compromised devices to be patched or otherwise remediated before they can be exploited (or further exploited) by cyber threat actors. It is the responsibility of each National CSIRT to utilize the reports to disseminate alert notifications to affected network owners throughout the country.

Individual network owners of all types and across all sectors (e.g., banks, hospitals, internet service providers, universities, nonprofits and NGOs, small to large businesses, local / state governments, etc.) can also subscribe to *directly* receive Shadowserver's network remediation reports associated with their own individual networks. Accordingly, use of Shadowserver's free, daily network remediation reports should be expanded to all network defenders in the region, particularly those in government, critical infrastructure, telecommunications providers, and internet services providers, among others.

Free open-source tools, including IntelMQ, Elasticsearch, Kibana, and others, are available to help ingest, store, parse, search, visualize, and analyze Shadowserver and other threat data feeds. Many affordable commercial tools are also available. For example, Arctic Hub, a cyber threat intelligence automation platform that collects, harmonizes, and distributes threat data from numerous feeds, is available for free the first year and at reduced rates in subsequent years for qualifying National CSIRTs through Arctic Security's CSIRT Development Program. As shown on Arctic Security's website, The Gambia's National CSIRT (gmCSIRT) is a current participant in the program.

RECOMMENDATION:
National CSIRTs and network defenders of all types and across all sectors should take advantage of available free and/or affordable threat data, tools, services, and platforms. This includes Shadowserver's free, daily network remediation reports, as well as free open-source tools (including IntelMQ, Elasticsearch, Kibana, and others) needed to ingest, store, parse, search, visualize, analyze, and effectively utilize Shadowserver and other threat data feeds. Consideration should also be given to potentially affordable commercial tools. For example, Arctic Hub, a cyber threat intelligence automation platform that collects, harmonizes, and distributes threat data from numerous feeds, is available for free the first year and at discounted rates in subsequent years for qualifying National CSIRTs through Arctic Security's CSIRT Development Program. The Gambia's National CSIRT(gmCSIRT) is currently a participant in the program.

2.5// In-House Technical Experts

The availability of free or otherwise affordable threat data, tools, and services nevertheless require in-house technical experts capable of effectively utilizing them. Shadowserver has encountered some National CSIRTs and other entities whose employees lack the technical proficiency to effectively use available data, tools, and services.

Acquiring and maintaining employees with the necessary technical expertise can be challenging, particularly for National CSIRTs, Sectoral CSIRTs, and other governmental entities unable to compete with most private sector salaries. To address this issue, it is recommended that ECOWAS Member

States collaborate with universities to develop training and internship programs that can act as a pipeline to bring inexperienced but technically skilled talent to the government. It is also recommended that member states collaborate with the private sector to develop programs in which seasoned technical experts from the private sector can do temporary work details at the National CSIRT and government / critical infrastructure entities to mentor and train less experienced, less technical employees.

RECOMMENDATION:
Ensure that each National CSIRT and network defenders of government and critical infrastructure systems have employees that possess adequate technical skills to effectively secure and defend the nation's networks. ECOWAS Member States should collaborate with universities to develop training and internship programs that can act as a pipeline for technically skilled talent. Member states should also collaborate with the private sector to develop programs in which seasoned private sector experts can do temporary but extended work details at the National CSIRT and government / critical infrastructure entities to mentor and train less experienced, less technical employees.

2.6// Training and Capacity Building

The lack of available in-house technical expertise can also be addressed by assistance, training, and capacity building services often available through formal projects funded by government foreign ministries (including the German Federal Foreign Office and GIZ, and the UK's Foreign, Commonwealth and Development Office), private sector entities (including Microsoft and Google), as well as the World Bank, the United Nations, and the European Union, to name a few.

For example, in addition to the current ECOWAS project funded by the German Federal Foreign Office and implemented by GIZ, the United Kingdom's Foreign, Commonwealth and Development Office (UK FCDO) has funded numerous cyber capacity building projects in Africa, including projects with Shadowserver.

Many cyber capacity building projects include in person and remote training opportunities. For example, in November 2024 Shadowserver partnered with FIRST and provided a full-day training titled "Getting the Most Out of Free Shadowserver Daily Feeds and Other Community Services via Automation" at the FIRST & AfricaCERT Symposium: Africa and Arab Regions in Livingston, Zambia.

RECOMMENDATION:
Seek opportunities for training and capacity building projects (particularly operational projects focused on setting up and effectively using available free / open source data, tools, services and platforms). Such projects are often funded by government foreign ministries (including the German Federal Foreign Office and GIZ, and the UK's Foreign, Commonwealth and Development Office) private sector entities (including Microsoft and Google), as well as the World Bank, the United Nations, and the European Union, to name a few.

2.7// Partnership Development

It is also imperative that National CSIRTs in the ECOWAS region develop relationships with constituents / stakeholders within their respective countries (e.g., Internet service providers, telecommunications providers, critical infrastructure, and other large network owners), as well as with fellow National CSIRTs within the ECOWAS region and around the world. These relationships are key to building an environment that fosters collaboration and information sharing. For example, close working relationships with constituents / stakeholders within their country enables a National CSIRT to quickly disseminate security threat alerts about vulnerable and compromised assets to network owners, allowing them to patch and remediate before exploitation by threat actors can occur.

Strong relationships with fellow National CSIRTs are equally important, as they promote information sharing, collaboration, and capacity building. Many opportunities exist to develop these professional relationships. For example, Shadowserver offers National CSIRTs free access to its online Alliance Mattermost chat platform where Shadowserver staff, Alliance Partners from across the industry, and National CSIRTs from around the globe share and receive the latest threat intelligence information and work collaboratively to address emerging threats.

National CSIRTs should also strive to become members of FIRST, the global Forum of Incident Response and Security Teams. FIRST is a leading member organization for National CSIRTs in the incident response and security arena. Membership in FIRST enables incident response teams to more effectively respond to security incidents. FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organizations. It aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large. Apart from the trust network that FIRST provides in the global incident response community, FIRST also offers a number of services to National CSIRTs. Currently, FIRST has more than 800 members, spread over Africa, the Americas, Asia, Europe and Oceania. As shown in Figure 4 below, among ECOWAS countries, only Benin, Ghana, Côte d'Ivoire, Nigeria, and Togo have National CSIRTs that are members of FIRST.

RECOMMENDATION:
Create a framework that requires National CSIRTs to build and maintain strong professional relationships with constituents / stakeholders within their respective countries (including Internet service providers, critical infrastructure operators, government entities, businesses, universities, state and local governments, healthcare providers, financial institutions, etc.), as well as with National CSIRTs within the ECOWAS region and around the world. These relationships are key to fostering information-sharing, collaboration, and capacity building. Opportunities for National CSIRTs to develop global partnerships include through an ECOWAS ISAC, becoming a member of FIRST.org, and joining Shadowserver's free online Alliance

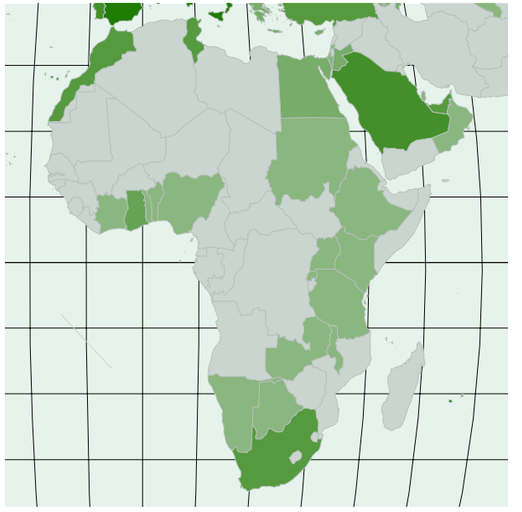


Figure 04. **Map of African nations whose National CSIRTs are current members of FIRST**

Mattermost chat platform that enables direct access to Shadowserver staff, Alliance Partners from across the industry, and National CSIRTs from around the world.

2.8// Maturity Assessments

To aid in their development, each National CSIRT should have a baseline assessment of their maturity level. The Open CSIRT Foundation created the Security Incident Management Maturity Model (SIM3) as a framework that helps organizations measure and improve their cybersecurity incident response team functions. It evaluates teams across 44 parameters in four key areas: Organization, Human Resources, Tools, and Processes. It then determines a maturity level on a scale from 0 (Not Available: meaning capability does not exist) to 4 (Explicit Audited: meaning capabilities are formalized, regularly audited, and continuously improved through formal governance). The Open CSIRT Foundation developed an online SIM3 self-assessment tool for all types of CSIRTs.

RECOMMENDATION:
To establish a baseline maturity level, each National CSIRT should be mandated to undergo the Open CSIRT Foundation's Security Incident Management Maturity Model (SIM3) self-assessment online tool and implement recommendations for improvement.

2.9// Early Warning Services

Businesses and other network owners throughout a country may be unaware that free, daily cyber threat data is available to them directly from cybersecurity organizations like Shadowserver to help them secure their networks. One way to overcome this is for National CSIRTs, Sectoral CSIRTs, ISACs, and other entities with large constituencies to develop and publicize their own Early Warning Services using Shadowserver's free cyber threat data (in the form of network remediation reports) and threat data available from other sources. The constituent organizations provide their public IP addresses and domain names to the National CSIRT (or other authority). In return they receive automated alert notifications about exposed, vulnerable, and compromised devices and services on their network to facilitate timely remediation, much like they would receive if subscribed to Shadowserver's reports. Although there are many, two such examples are the Early Warning Services offered by the United Kingdom's National Cyber Security Centre (UK NCSC) and the Dominican Republic's CSIRT-RD.

RECOMMENDATION:
National CSIRTs, Sectoral CSIRTs, ISACs, and other entities with large constituencies should be mandated to offer free Early Warning Services to their constituents using free cyber threat data from Shadowserver and other available sources. Constituent organizations provide their network's public IP addresses and domain names, and in return they receive automated alert notifications about exposed, misconfigured, abusable, vulnerable, and compromised devices and services on their networks to facilitate timely remediation. Consultation with one of the many National CSIRTs that operate such Early Warning Services is recommended, such as the United Kingdom's National Cyber Security Centre (UK NCSC) and the Dominican Republic's CSIRT-RD.

3.0// Operational Cybersecurity Gaps and Recommendations: ECOWAS Region's Attack Surface

An "**attack surface***" refers to all possible weak points, or attack vectors, that can be exploited by a threat actor to gain unauthorized access to a system or network. While some attack vectors rely on human error (e.g., **phishing***; social engineering), many rely on technical deficiencies in a network (e.g., misconfigured and exposed assets; **unpatched vulnerabilities***; **zero-day vulnerabilities***; **compromised assets***; etc.)

Shadowserver collects and analyzes voluminous cyber threat data at Internet-scale using a variety of technical means explained below. It then shares that data free-of-charge every day with more than 9,000 organizations and network owners around the world (i.e., hospitals, universities and school districts, nonprofit and non-governmental organizations, federal / state / local governments, small to medium sized businesses, Fortune 500 companies, internet service providers, financial institutions, critical infrastructure providers, and many others). Shadowserver also provides free, daily, expansive nationwide threat data to National Computer Security Incident Response Teams (National CSIRTs) designated with specific prevention and incident response responsibilities in 175 countries, including in Africa and, most relevant to this report, many ECOWAS Member States.

The threat data shared by Shadowserver is in the form of network remediation reports. These reports act as both an Early Warning Service, identifying exposed, misconfigured, and vulnerable devices on a network to be patched before threat actors can breach the network, and a Victim Notification Service, identifying compromised devices on a network to be remediated before further exploitation, such as a ransomware attack, can occur. The data collected can help shed light on the ECOWAS region's attack surface.

3.1// Scan Data

Shadowserver performs daily port scanning more than 150 times per day to publicly exposed / routable **Internet Protocol (IP) addresses***; namely, approximately 3.7 billion IPv4 addresses and hitlists of approximately two billion IPv6 addresses observed in the wild. Scan data is used to notify National CSIRTs and network owners across all sectors of exposed, abusable, misconfigured, vulnerable and sometimes compromised devices to be patched or otherwise remediated before they can be exploited (or further exploited) by threat actors.

Threat actors often conduct their own scanning, or purchase scan data from commercial vendors, to identify networks to target for attack. Accordingly, Shadowserver's free scan data is a critical tool that allows National CSIRTs and network owners to see what threat actors see about their networks, including ways to gain unauthorized access and potentially exploit the networks.

An analysis of Shadowserver's **scan data** is valuable in identifying the following:

a devices and services publicly exposed (sometimes unnecessarily) to the Internet that needlessly increase an attack surface

b critical vulnerabilities in exposed assets

c compromised exposed assets

3.1a// DEVICES AND SERVICES PUBLICLY EXPOSED TO THE INTERNET

Devices* and **services*** publicly exposed to the Internet are common attack vectors for threat actors seeking to breach a network. Yet many network owners are not fully aware of all assets on their networks because they fail to maintain an updated inventory of their assets.

Performing an **asset inventory*** is crucial to understanding an attack surface and improving cyber resilience by serving two key purposes:

1. It allows a network owner to know the vendor, type, model, and location of publicly exposed devices on a network which, in turn, enables quick patching and remediation when new vulnerabilities in those devices and related software are discovered and publicly announced.
2. It allows network owners to reduce their overall attack surface by remediating devices and services unnecessarily exposed to the Internet.

Helpful guidance on implementing regulations that mandate the conducting of asset inventories by federal government agencies can be found in "Binding Operational Directive 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks" overseen by the United States Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (DHS-CISA). The directive requires federal, executive branch, departments and agencies to, among other things, perform an automated asset discovery (inventory) every 7 days. It further requires them to "initiate vulnerability enumeration across all discovered assets, including discovered nomadic / roaming devices (e.g., laptops), every 14 days.

Shadowserver maintains detection fingerprints for exposed *devices* observed in the ECOWAS region as part of our daily Internet scanning. This includes identifying the vendor, type and model of publicly exposed devices.

As shown in Figure 05, Nigeria, Côte d'Ivoire, and Ghana have the highest volume of exposed devices in the ECOWAS region, consistent with the size of their respective IP infrastructures.

Figure 05. **Device identification volume by ECOWAS country** (average daily scan results from 1 October 2024 to 24 April 2025)

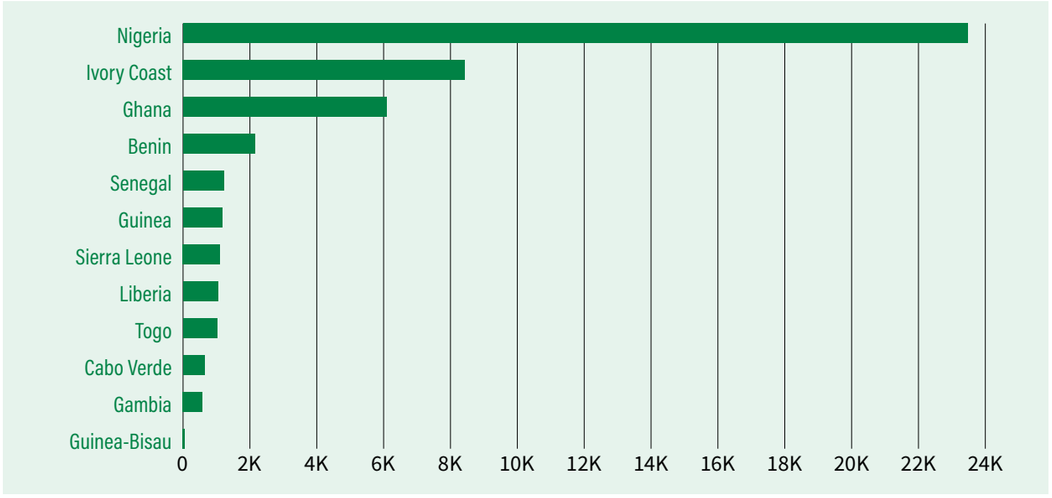
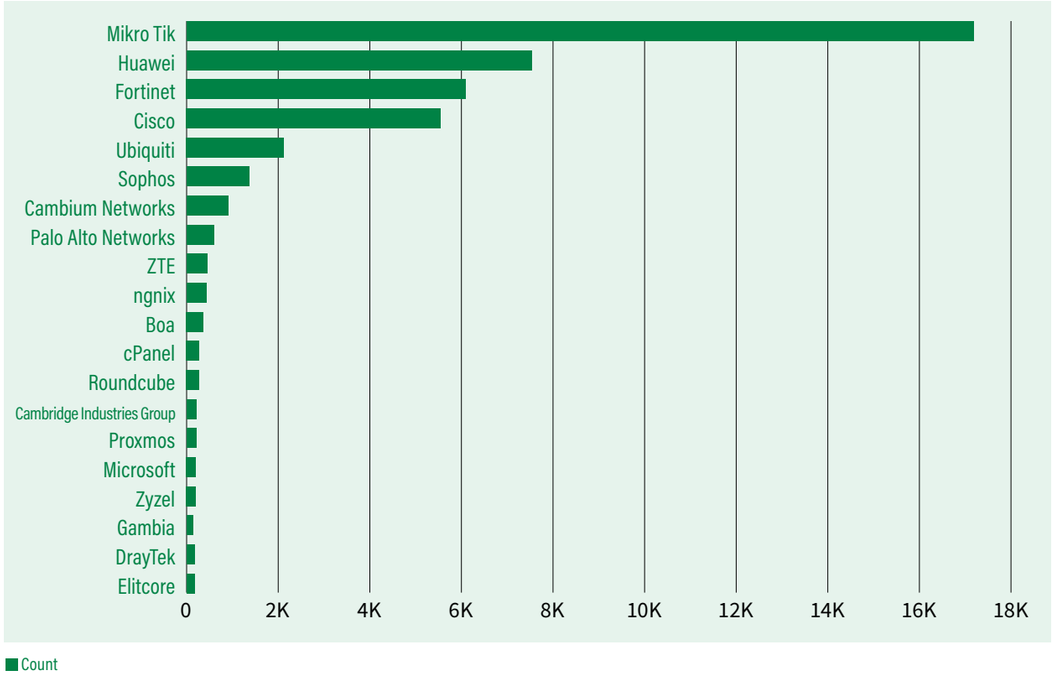


Figure 06. **Top 20 Device Vendors found across the ECOWAS Region** (average daily scan results)



The bar chart in Figure 06 shows the Top 20 vendors by volume identified across the ECOWAS region including some well-known vendors such as Huawei, Fortinet, MikroTik and Cisco.

Looking at the highest vendor by volume, MikroTik is by far the consumer router choice in the ECOWAS region. The significance of this from an attack

surface perspective is that several critical and high severity vulnerabilities have been identified and exploited in MikroTik devices. Knowing whether and where these devices are on a network through an asset inventory are keys to quick patching as new vulnerabilities are identified.

Routers* are among the most-targeted devices by threat actors because they are usually gatekeepers to users' networks, are always connected to the Internet (and thus easily discoverable), often have default or weak user credentials, and their vulnerabilities often remain unpatched. Once exploited, these devices are often incorporated into large botnets and used for a variety of malicious activities such as DDoS attacks, malware distribution, data theft, and phishing campaigns.

Shadowserver can map exposed and fingerprinted devices, including routers, in the ECOWAS region by device type. While certain device types, such as **firewalls*** and **VPN services***, are often exposed to the public Internet as part of their core functions, routers and certain other devices typically need not be exposed.

A cautionary tale about the dangers of assets unnecessarily exposed to the Internet can be found in the hack of critical infrastructure networks beginning in November 2023 by CyberAv3ngers, a hacking group affiliated with the Iranian Government's Islamic Revolutionary Guard Corps (IRGC).

Between November 2023 and January 2024, CyberAv3ngers successfully compromised at least 75 Israeli-manufactured Unitronics PLC devices used in multiple critical infrastructure industries, including the water and wastewater sector. The devices were operational technology (OT) devices unnecessarily publicly exposed to the Internet with either a default password or no password in place.[20] The most prominent of these attacks was against the Municipal Water Authority of Aliquippa, a small community in Western Pennsylvania.[21] These attacks revealed how vulnerable critical infrastructure networks are to cyberattacks and the potential harm to the public if such systems are breached.

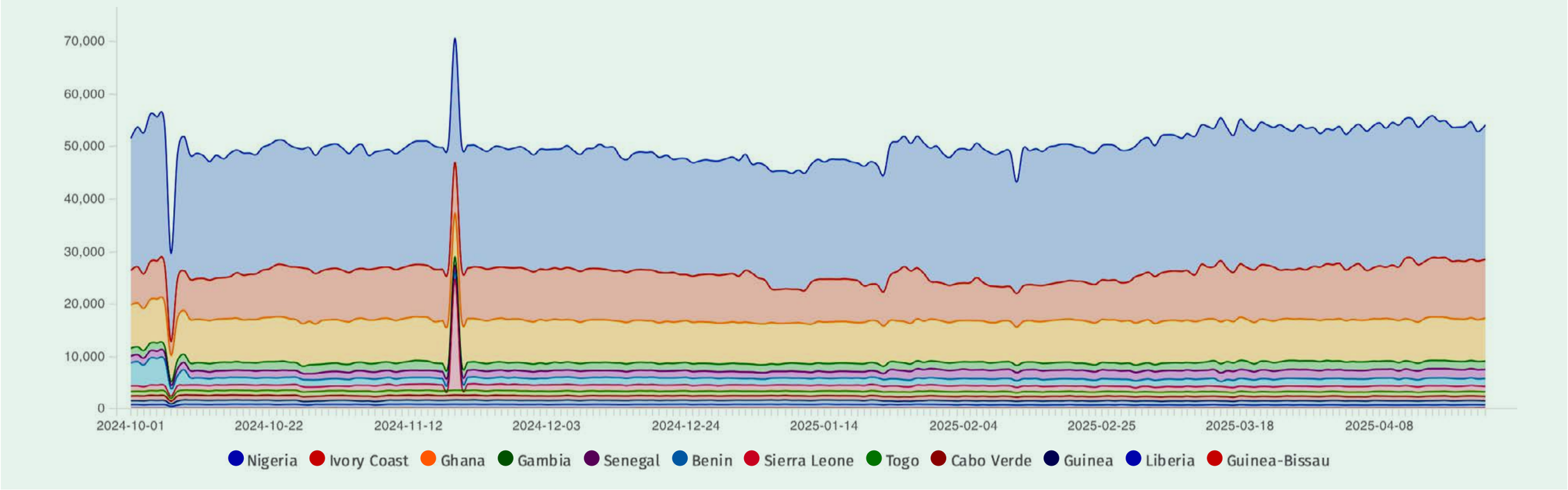
Critical infrastructure networks are increasingly targeted for cyberattacks by threat actors. These attacks can lead to significant societal harms when things like water supply, power supply, and healthcare services are disrupted or otherwise compromised. Accordingly, making sure that assets are not unnecessarily exposed to the public Internet is an important step in securing a network and reducing the attack surface.

Shadowserver shares with National CSIRTs and with network owners actionable, detailed and IP-specific data on exposed devices in a network/constituency in the 'Device Identification' report.

[20] "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, including US Water and Wastewater Systems Facilities," *Cybersecurity Advisory, Cybersecurity and Infrastructure Security Agency*, December 18, 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*, December 2, 2023. https://www.npr.org/2023/12/02/1216735250/iran-linked-cyberattacks-israeli-equipment-water-plants

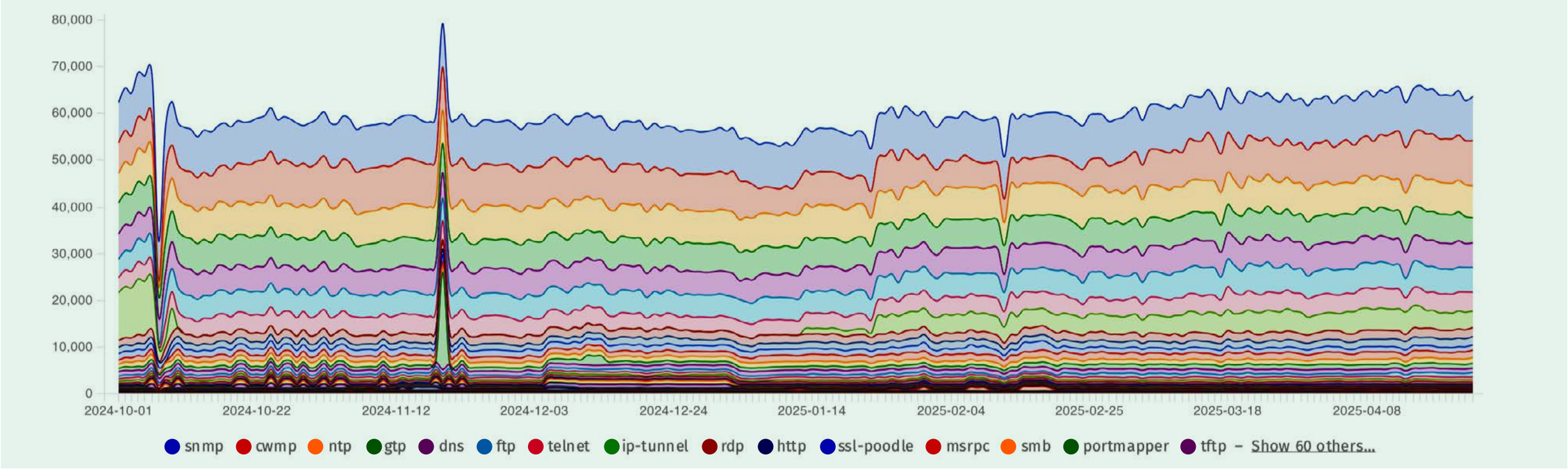
Figure 07. **Exposed server-side application instances by country in the ECOWAS Region**



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

In addition to publicly exposed devices, **services*** / **server-side applications*** that are publicly exposed to the Internet are also a reason of concern and contribute to an overall attack surface. Figure 07 shows instances of exposed services by country in the ECOWAS region with Nigeria, Côte d'Ivoire, and Ghana the top three. These exposed services are considered problematic because they are either misconfigured, abusable, vulnerable or otherwise unnecessarily accessible from the public Internet, making them prime targets of threat actors looking to breach networks.

Figure 08. **Exposed server-side application instances by scan type in the ECOWAS Region**



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

Figure 08 shows that **SNMP (Simple Network Management Protocol*)** is the most Internet-exposed service in the ECOWAS region. SNMP is a protocol that plays a crucial role in monitoring, managing, and securing network devices. It allows network administrators to collect information, configure devices, and respond to network events remotely, making it an essential tool for maintaining network performance and security.

Many exposed services contain vulnerabilities that can be exploited by threat actors. For example, exposed SNMP services in certain Cisco routers contain a vulnerability designated as CVE-2017-6742. In April 2023, a joint Cybersecurity Advisory (CSA) issued by US and UK security agencies revealed that Russian GRU Military Intelligence Unit 26165 hackers (known as APT28, Fancy Bear, and Sofacy, among others) exploited this vulnerability to carry out reconnaissance of routers and deploy malware.[22]

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

These examples underscore the potential threat posed by exposed devices and services that can be exploited by threat actors, including nation-state hackers.

RECOMMENDATIONS:
Establish policies to mandate the conducting of periodic asset inventories*, particularly in government and critical infrastructure sectors. Doing so will aid network owners in timely patching and remediation efforts as new critical vulnerabilities emerge. Helpful guidance on implementing regulations that mandate the conducting of asset inventories by federal government agencies can be found in "Binding Operational Directive 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks" overseen by the United States Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (DHS-CISA).

Ensure that network owners (in particular, critical infrastructure, government, and large ISPs) do not needlessly expose certain device types (including OT devices and others mentioned above) and services (including SNMP) to the public Internet unless necessary for functionality purposes. Doing so will reduce the region's overall attack surface. Focused trainings and workshops with National CSIRTs, ISPs, and other network owners in the ECOWAS region could culminate in proactive surge activity to target and reduce instances of unnecessarily exposed devices and services.

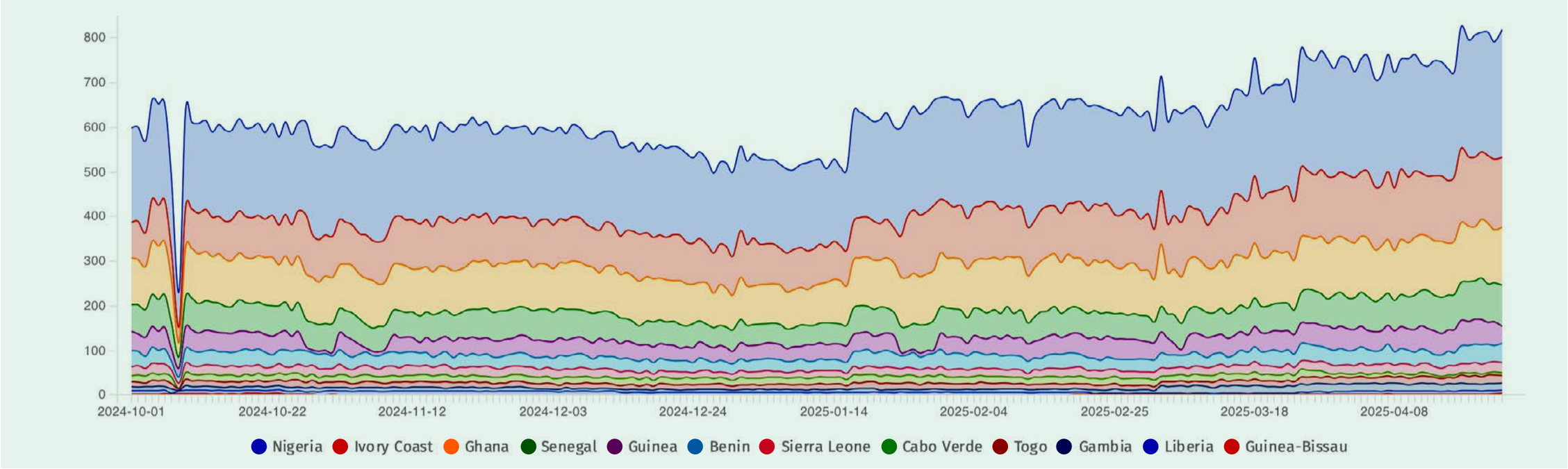
3.1b// CRITICAL VULNERABILITIES IN EXPOSED ASSETS

Threat actors continue to exploit unpatched vulnerabilities as a primary means of breaching networks and causing harm, including through ransomware and DDoS attacks. As part of its core activities, Shadowserver scans the Internet looking for instances of certain critical and high severity **Common Vulnerabilities and Exposures (CVEs)*** in devices and software. It then alerts network owners and National CSIRTs of these vulnerabilities on their networks to be patched before threat actors can exploit the vulnerabilities, breach the network, and cause further harm.

As a recent example, unpatched vulnerabilities in Microsoft's SharePoint information-sharing and collaboration software known as "ToolShell" were exploited in June 2025 by threat actors who targeted at least a half-dozen entities in South Africa, including the National Treasury, an organization in the car-manufacturing industry, a university, several local government entities and a federal government entity.[23]

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

Figure 09. **Critical remote CVEs detected in exposed assets by country across the ECOWAS region**



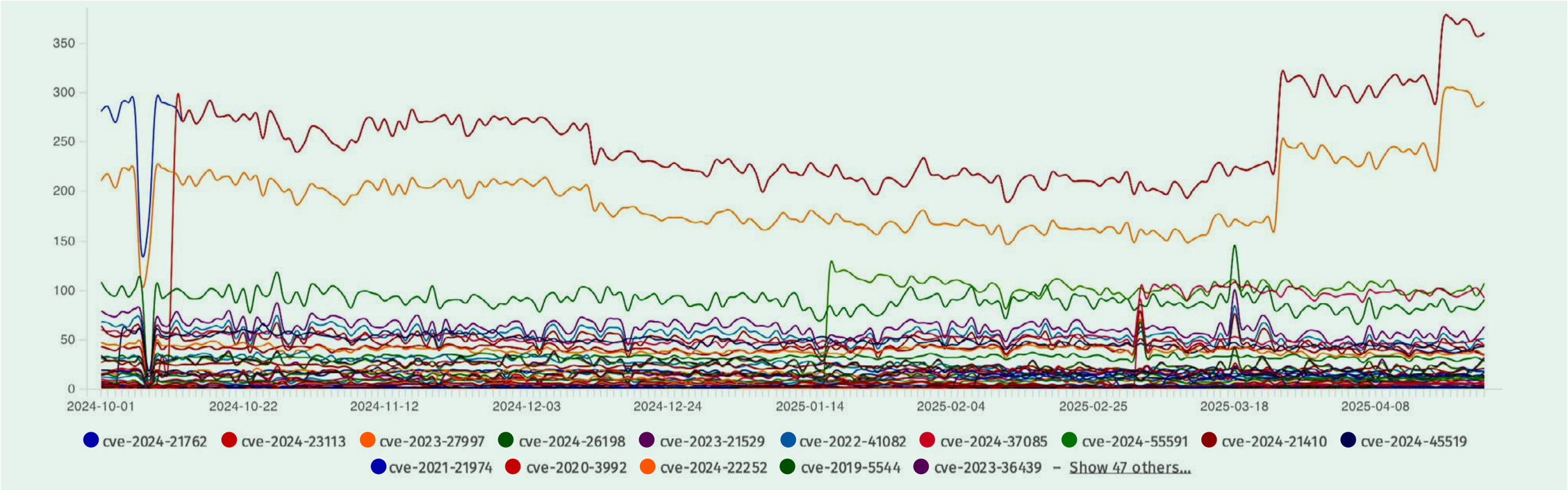
The items at the bottom of each graph are arranged left to right in descending order in which they appear on the graph.

As shown in Figure 09, Shadowserver's daily scans reveal a modest number of critical vulnerabilities in exposed infrastructure within the ECOWAS region, with the most seen in Nigeria, Côte d'Ivoire, and Ghana. These vulnerabilities can unfortunately be exploited at any time.

As shown in Figure 10, there are several critical CVE-related vulnerabilities in the ECOWAS region of concern. For example, CVE-2024-23113 is a critical vulnerability in Fortinet FortiOS which, if exploited, could allow a remote, unauthenticated hacker to execute arbitrary code or commands on a system.[24] Shortly after the vulnerability was announced in October 2024,

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

Figure 10. **Critical remote CVEs detected in exposed assets across the ECOWASRegion**



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

Shadowserver identified more than 87,000 Fortinet IPs likely vulnerable to CVE-2024-23113.[25] Additionally, around the same time, the United States Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (DHS-CISA or "CISA") added CVE-2024-23113 to its Known Exploited Vulnerability Catalog, meaning the CVE was being actively exploited in the wild by threat actors and must be a top patching priority for U.S. government agencies.[26]

Unpatched vulnerabilities provide threat actors with attack vectors to gain unauthorized access to networks. Vulnerabilities seen actively exploited in the wild (also referred to as "**known exploited vulnerabilities***") are of particular concern and should be prioritized for immediate remediation. Patching vulnerabilities, particularly those of critical and high severity and those being actively exploited in the wild, are vital to achieving a more secure digital infrastructure and should be mandatory for government agencies and critical infrastructure to complete within a well-defined time period.

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

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

Helpful guidance can be found in "binding operational directives (BODs)" overseen by DHS-CISA. These BODs require federal, executive branch, departments and agencies to take certain actions to safeguard federal information and information systems.

For example, "BOD 19-02: Vulnerability Remediation Requirements for Internet-Accessible Systems" requires, among other things, that critical vulnerabilities be remediated within 15 calendar days of initial detection, and high vulnerabilities be remediated within 30 calendar days of initial detection. If vulnerabilities are not remediated within the specified timeframes, CISA will send a partially populated remediation plan identifying all overdue, in-scope vulnerabilities to the agency's points of contact for validation and population. Agencies shall then return the completed remediation plan to CISA within three working days of receipt with completed information that explains: (i) the vulnerability remediation constraints; (ii) the interim mitigation actions to overcome constraints; and (iii) the estimated completion date to remediate the vulnerability.

Similarly, "BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities" was created to enhance, but not replace BOD 19-02. BOD 22-01 established a CISA-managed catalog of known exploited vulnerabilities that carry significant risk to the federal enterprise. The BOD further established requirements for agencies to remediate any such vulnerabilities included in the catalog within the specified timeframe; namely, within 6 months for vulnerabilities with a Common Vulnerabilities and Exposures (CVE) ID assigned prior to 2021 and within two weeks for all other vulnerabilities.

On the issue of whether critical / high vulnerabilities or known exploited vulnerabilities are more important to remediate first, CISA explained, "Known exploited vulnerabilities should be the top priority for remediation…BOD 22-01 shifts the focus to those vulnerabilities that are active threats." [27]

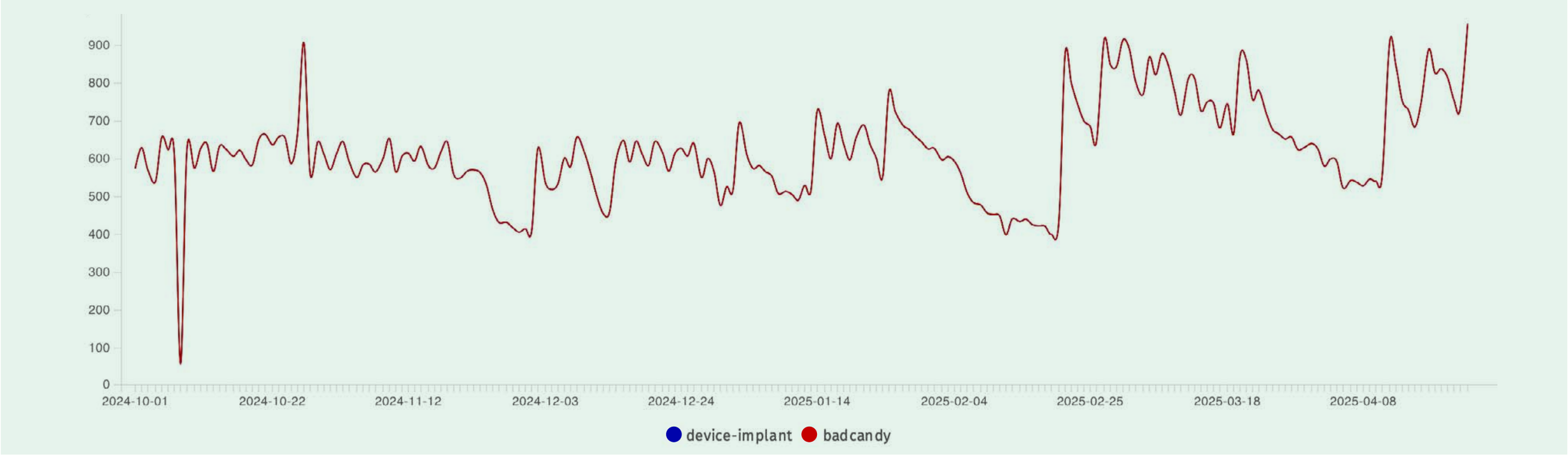
RECOMMENDATIONS:

Implement regulations that require government agencies and critical infrastructure to remediate vulnerabilities designated as "critical risk" within 15 calendar days and those designated as "high risk" within 30 calendar days of initial detection. Helpful guidance can be found, for example, in "Binding Operational Directive (BOD) 19-02: Vulnerability Remediation Requirements for Internet-Accessible Systems" overseen by the United States Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (DHS-CISA).

Implement regulations that require government and critical infrastructure to remediate "known exploited vulnerabilities" within 14 days. DHS-CISA maintains a catalog of Known Exploited Vulnerabilities (KEV) that identifies vulnerabilities seen actively exploited in the wild that must be remediated by U.S. federal government agencies. ENISA maintains a similar catalog known as the European Union Vulnerability Database. Finally, Shadowserver's public Dashboard maintains Shadowserver's list of known exploited vulnerabilities identified via its honeypot sensor network. Helpful guidance on such a regulation can be found, for example, in "Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities" overseen by DHS-CISA.

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

Figure 11. **Compromised devices across the ECOWAS Region**



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

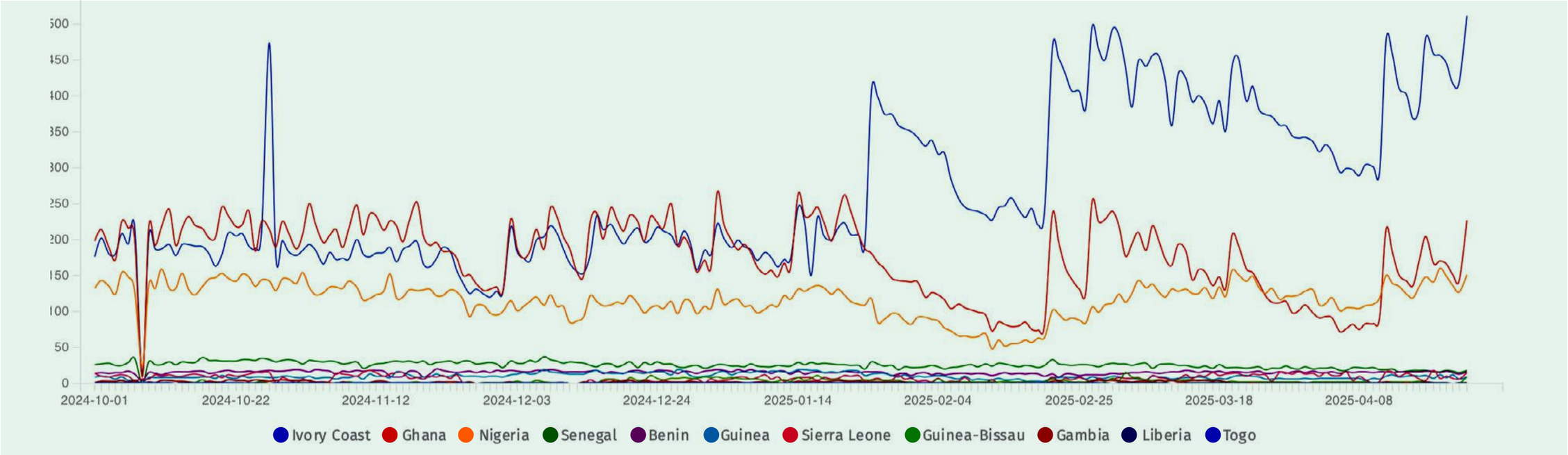
3.1c// COMPROMISED EXPOSED ASSETS

Shadowserver also continuously scans for critical network assets that have been compromised by threat actors when sufficient evidence for detection is available. This is done primarily by non-intrusively scanning for certain items or artifacts often installed on a device after it's been compromised (e.g., **implants***, **web shells***, and **credential stealer code injections***).

For example, in late 2023, Cisco IOS XE software was compromised by what's known as "Bad Candy" implants, which were malicious **web shells*** installed on thousands of internet-facing Cisco network devices by threat actors who exploited two **zero-day vulnerabilities***. [A zero-day vulnerability is a previously unknown flaw in software, hardware, or firmware that attackers can exploit before the vendor is aware of it and has a chance to develop a patch to fix it.] These attacks allowed the threat actors to gain full administrative control over the system and enabled them to potentially monitor network traffic, access protected networks, and perform a variety of attacks.[28]

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

Figure 12. **Compromised Devices in the ECOWAS Region by Country**



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

Shadowserver's scan results show a significant number of Cisco IOS XE compromises with Bad Candy implants in the ECOWAS region. In Figure 11, you can see Cisco IOS XE / Bad Candy-related compromises in the ECOWAS region averaging just under 500 devices for the reporting period. This makes up the bulk of the compromised devices detected in the region.

Interestingly, Figure 12 reveals that most of the Bad Candy-related compromises are found in networks across Côte d'Ivoire with far higher numbers than any other ECOWAS nation, including Nigeria who has the largest IPv4 space in the region.

Compromised devices, such as the Cisco IOS XE / Bad Candy, are significant threats and can be further exploited at any time with potentially serious consequences, including operational disruptions, damage to the network, data theft, ransomware and other malware-based attacks, credential theft, reputational damage, and legal liability.

Shadowserver reports various types of compromised devices identified via scan-based detection of the attacker's installed implant. These reports, along with data feeds from other sources, can be utilized by National

CSIRTs and other government agencies to devise nationwide campaigns to eradicate such threats and secure the compromised devices.

For example, the Australian Signals Directorate (ASD) implemented a nationwide campaign to eradicate Bad Candy implants in compromised Cisco IOS XE devices throughout Australia. As part of the campaign, ASD officials sent victim notifications directly to affected network owners, or to their service provider if the network owner could not be identified. The notifications contained instructions to patch, reboot, and conduct incident response on affected devices to remove the Bad Candy implant and mitigate the risk of re-exploitation. The ASD then tracked the overall decline in the number of Bad Candy implanted devices over the course of several months as batches of bulk notifications were issued.

RECOMMENDATIONS:

Implement regulations requiring National CSIRTs, government agencies, critical infrastructure, ISPs, and other network owners in the region to remediate identified compromised devices within a brief but specified time period, including those identified in Shadowserver's daily reports such as Cisco / Bad Candy implants.

Mandate National CSIRTs, in coordination with Internet Service Providers (ISPs), to devise and implement nationwide threat mitigation and eradication campaigns against critical vulnerabilities and compromised devices on networks throughout the country, and track the progress of remediation efforts. One such example is the nationwide campaign led by the Australian Signals Directorate (ASD) to eradicate Bad Candy implants in compromised Cisco IOS XE devices throughout Australia.

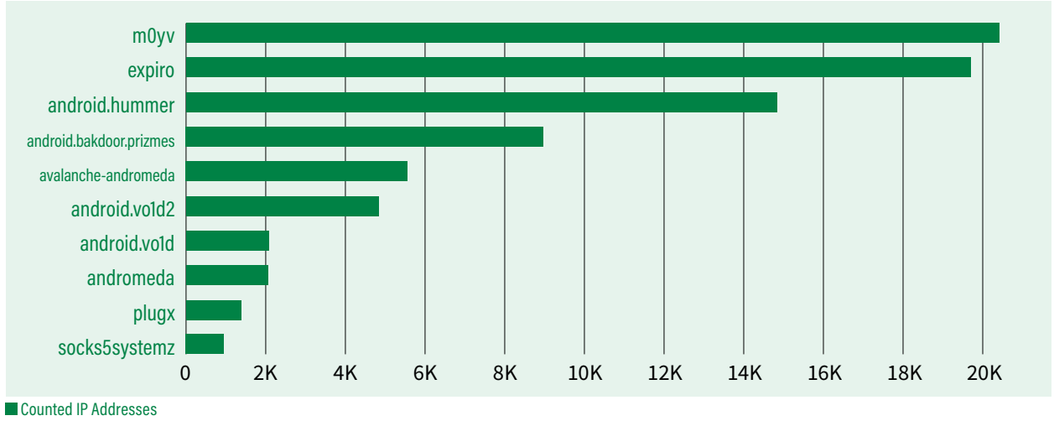
3.2// Sinkhole Data

Shadowserver operates a large **domain name system (DNS*)** sinkholing infrastructure through which it collects data on victims' malware-infected devices. "**Sinkholing***" is a technique that involves disrupting the communications between victims' malware-infected devices and the criminally-controlled servers to which the malware directs them to communicate. The communication, or traffic, is then redirected to sinkhole servers so the criminals can no longer access, control, or communicate with the victims' devices. Shadowserver collects the IP address and other identifying information associated with the victims' malware-infected devices reporting to the sinkhole servers. The information is then added to Shadowserver's free daily network remediation reports to notify National CSIRTs and subscribing network owners of malware-infected devices to be remediated.

This disruption is typically accomplished by taking control of the malicious domains or IP addresses that control the communications between the victim's malware-infected devices and the infrastructure controlled by the criminals. This is often done through criminal or civil court orders served on **registries*** and **registrars*,** by voluntary action of registries and registrars as a result of terms of service violations, or by purchasing those malicious domains that are not yet registered by the threat actors. Seized malicious domains are often transferred to Shadowserver's Registrar of Last Resort (RoLR), a nonprofit special purpose DNS registrar created for the purpose of quarantining malicious domains at no (or low) cost for the long term as a public service.

Sinkholing is an important technique to ensure that threat actors can no longer access, control, or communicate with victims' malware-infected devices (unless infected with other types of malware not the subject of the sinkhole operation).

Figure 13. **Top 10 sinkhole infections by type in the ECOWAS Region**



Based on sinkhole infection datasets, the bar chart in Figure 13 shows more than 80,000 total malware-infected IP addresses per day on average in the ECOWAS region. To state more simply, more than 80,000 devices whose IPs geo-locate to the ECOWAS region are infected with malware and (unless infected with other malware types not being sinkholed) were previously controlled by threat actors before being redirected to Shadowserver's sinkhole servers.

Figure 14 below reveals that most device infections are seen in Nigeria followed by Ghana, likely due in part to the large IP space attributable to those nations.

Figure 14. **Most affected countries by malware in the ECOWAS Region - as seen in sinkhole data**

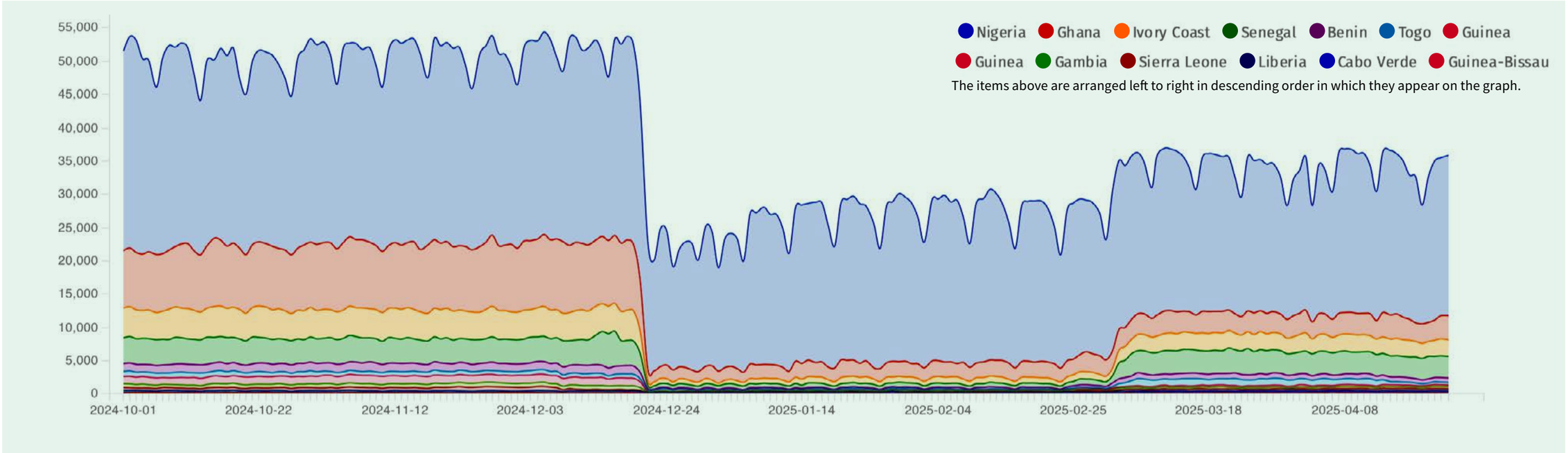
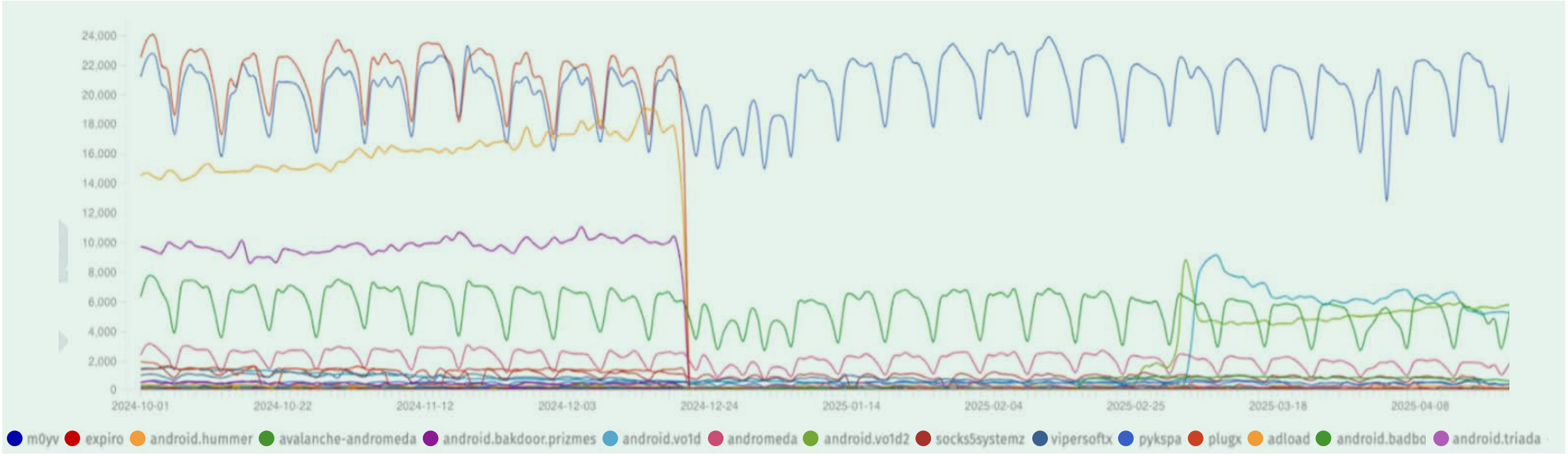


Figure 15. **Top infections seen in Shadowserver sinkholes in the ECOWAS Region - by malware type**



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

Analysis of sinkhole data by infection type allows us to drill deeper into infection statistics to look for trends in the type of malware seen across the region.

In Figure 15, we see a variety of malware variants in infected devices throughout the ECOWAS region. For example, M0yv is a modular, multi-functional file-infecting virus developed and used by the Maze ransomware group. The Maze ransomware group was a cybercriminal gang known for popularizing the "double extortion" technique whereby they would both steal a victim's data and encrypt it. If a ransom was paid, the data would be decrypted and made accessible to the victim once again. If the ransom was not paid, the group would publicly release the stolen data on leak sites they maintained.

RECOMMENDATIONS:
Implement regulations requiring National CSIRTs, government agencies, critical infrastructure, ISPs, and other network owners in the region to

collaborate on remediating identified malware-infected devices within a brief but specified time period, including those identified in Shadowserver's free, daily network remediation reports.

3.3// Unique Data Sets from Law Enforcement Cybercrime Disruption Operations

Unique data sets are collected by, or shared with, Shadowserver as a result of our support of **Law Enforcement cybercrime disruption operations***. For more than 15 years, Shadowserver's Special Projects Team (SSPT) has provided free support to many of the most significant international cybercrime disruption operations. This support has taken on many forms, but it typically includes Shadowserver conducting sinkhole operations, quarantining malicious domain names through the Registrar of Last Resort (RoLR), and assisting in victim notification efforts by distributing victim data to affected network owners and/or their respective National CSIRT in our free, daily network remediation reports.

LEAs often share with Shadowserver unique data sets of historical infections of victim devices as well as active infections of victim devices reporting to Shadowserver's sinkhole servers when large **botnets*** are dismantled. Historical infections are shared with National CSIRTs in one-off Special Reports, whereas active infections are shared via Shadowserver's free, daily network remediation reports. These unique data sets acquired through Law Enforcement disruption operations reveal malware-infected victim devices in the ECOWAS region that were part of criminally controlled botnets.

By way of one example, Qakbot malware botnet was disrupted in a law enforcement operation by the FBI and US Department of Justice along with multiple other partners in August 2023. Qakbot (also known as QBot, Pinkslipbot, Quakbot and Oakbot) has been active since around 2007, having initially been developed as an information stealer and **banking trojan*** malware, before later becoming primarily a distribution network for other malware / ransomware. In recent years, Qakbot has been used as an initial infection vector by many ransomware groups including Conti, ProLock, Egregor, REvil, MegaCortex, and Black Basta. This has likely enabled significant financial losses globally.

As shown in Figure 16, 2,941 historical Qakbot infections were found on devices across the ECOWAS region.

Figure 16. **Qakbot historical infections across the ECOWAS Region (2023-08-24)**

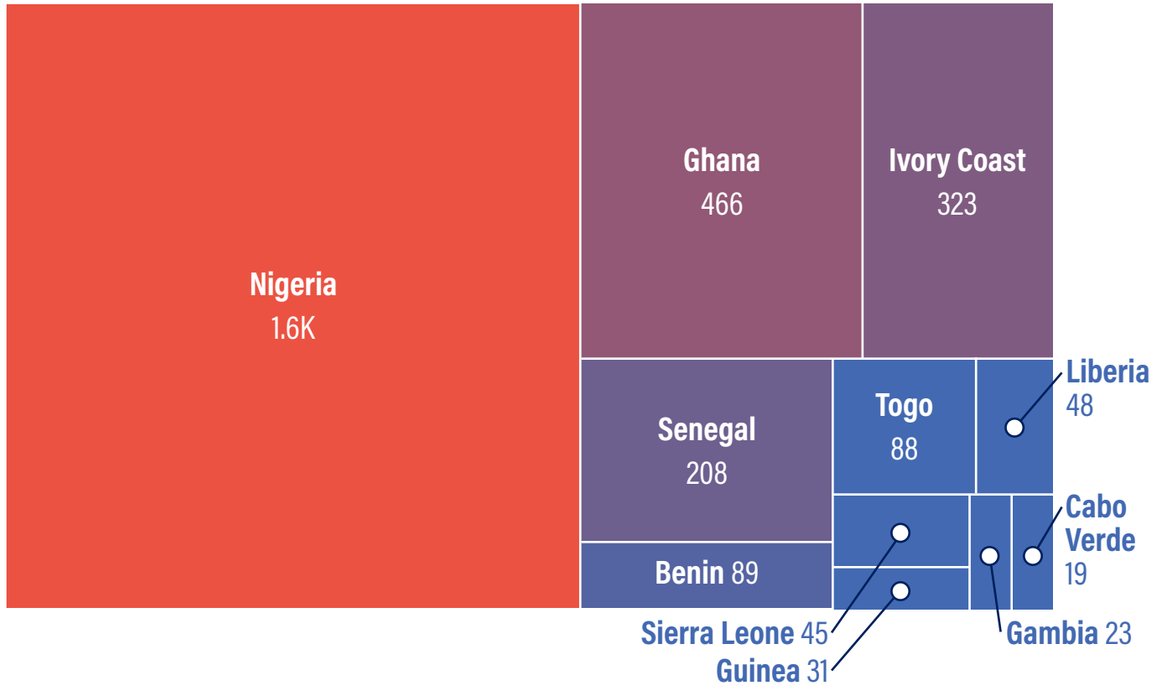
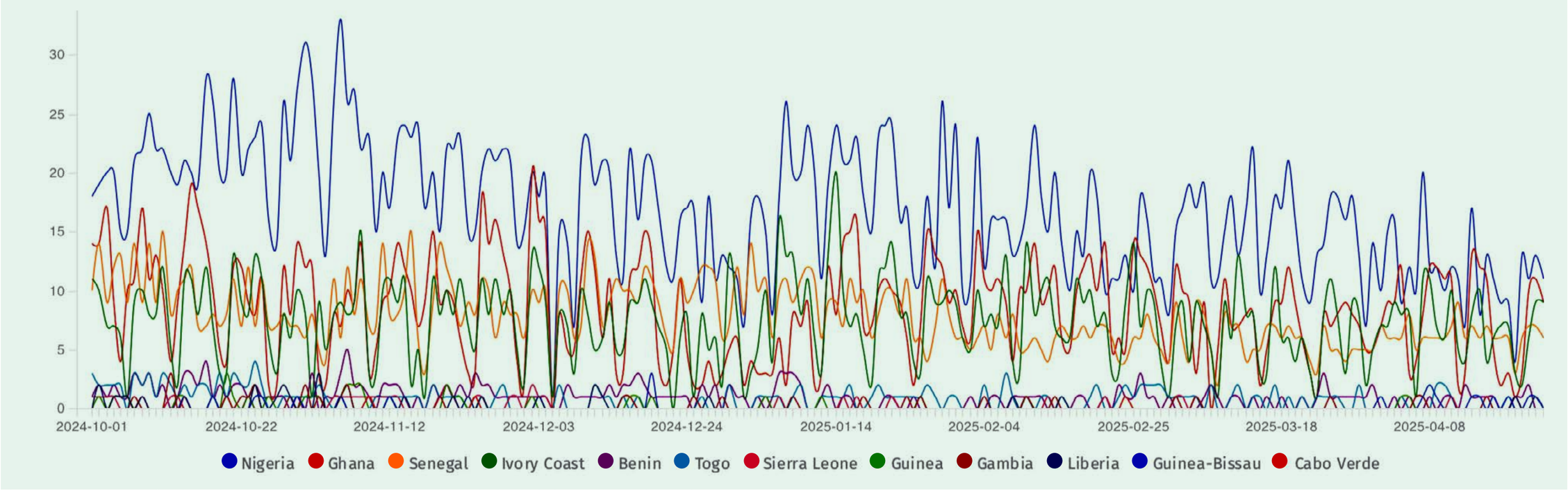


Figure 17. **Smokeloader across the ECOWAS Region**



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

By way of a second example, Operation Endgame was a Europol led international Law Enforcement operation again malware droppers, including IcedID, SystemBC, Pikabot, Smokeloader and Bumblebee, which led to four arrests and the takedown of over 100 servers worldwide in May 2024. Droppers are malicious programs designed to deliver other malware to a victim's device. In the time series chart (Figure 17) we can see that all ECOWAS nations were impacted by SmokeLoader with the more populous IPv4 nations exhibiting the most infections.

Victim data sets acquired by Shadowserver through Law Enforcement cybercrime disruption operations are unique and not readily available elsewhere, especially not through commercial vendors. National CSIRTs and network owners across the ECOWAS region should take full advantage to access this valuable, free data to help them remediate malware-infected devices to better secure their networks. Although sinkholed by Shadowserver, these victim devices remain infected unless and until they are remediated, which can be accomplished through collaborative efforts between National CSIRTs and affected network owners.

Shadowserver's Public Dashboard

This report includes threat data statistics and visualizations from Shadowserver's free, public Dashboard funded by the United Kingdom's Foreign, Commonwealth and Development Office (FCDO). The Dashboard allows the public to query Shadowserver's data sets for aggregated country-level or regional-level statistics on a variety of threat issues. As part of the current project, Shadowserver created a new regional country grouping in the Dashboard to specifically cover statistics relevant to the ECOWAS region. (See Figure 18).

The Dashboard can be a helpful tool in informing government leaders, policymakers, cybersecurity researchers, network defenders, media outlets, and others about the latest cyber threats affecting a country and/or a region. The Dashboard can also provide statistics that help track the progress of patching and remediation efforts in a country or region related to a specific threat.

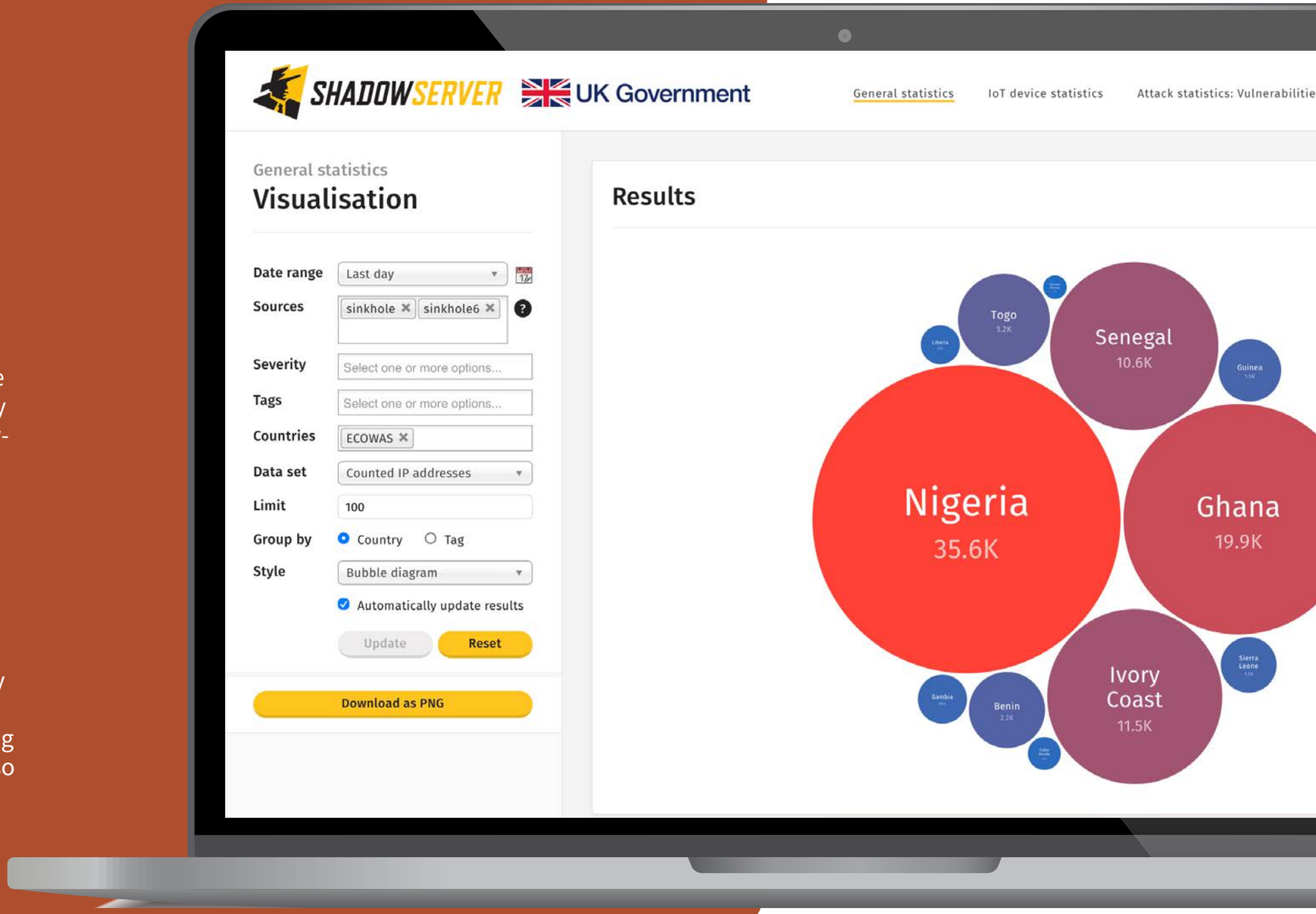


Figure 18. **ECOWAS region country grouping on Shadowserver's public Dashboard**

For example, imagine an official with Nigeria's Computer Emergency Response Team (ngCERT) learns of the potential harm caused by home internet connected devices that facilitate criminal activity as part of a large botnet known as Badbox 2.0. Upon further online research, the ngCERT official learns that Google, HUMAN Security, Trend Micro, and The Shadowserver Foundation partnered in a disruption operation against the Badbox 2.0 botnet in which Shadowserver **sinkholed*** infected devices so they now report to Shadowserver's sinkhole servers and can no longer be controlled by the criminal threat actors. https://www.humansecurity.com/learn/blog/satori-disrupting-badbox-2/

The ngCERT official wants to seek government funding for a Badbox 2.0 public awareness campaign in Nigeria and a targeted remediation initiative with fellow National CERTs and Internet Service Providers (ISPs) across the ECOWAS region. In order to help inform government officials from Nigeria and ECOWAS Member States on the Badbox 2.0 threat within the region, the ngCERT official can query Shadowserver's public Dashboard.

By clicking on Shadowserver's Sinkhole data tab, the ngCERT official can add filters to the query on the left hand side of the screen, including the "Day," the "Tags" (in this case "android.badbox2"), and "Countries" (in this case ECOWAS, but could also be an individual country such as Nigeria). The result is a Tree Map showing Android Badbox 2.0 infections for the previous day among the various ECOWAS Member States. (See Figure 19).

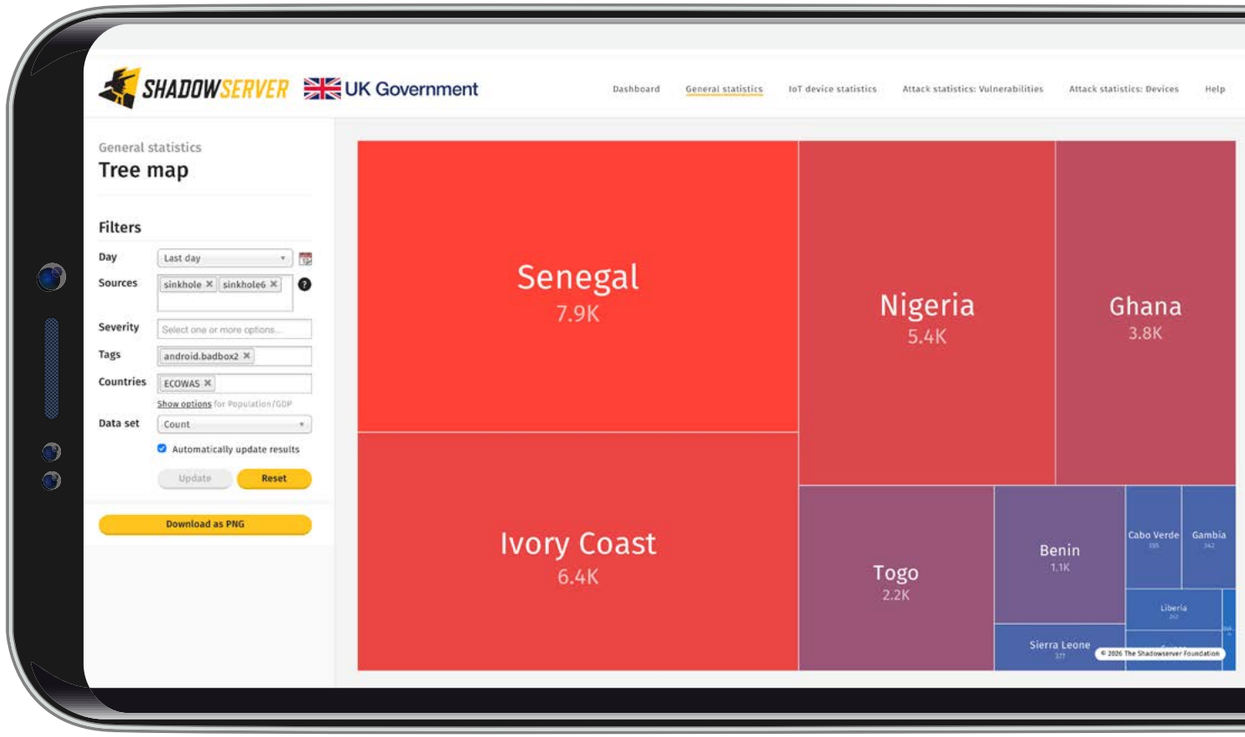


Figure 19. **Infected Android Badbox 2.0 devices in ECOWAS region reporting to Shadowserver's sinkhole servers**

The ngCERT official can also query the data in a "Time Series" graph (see Figure 20) to track Badbox 2.0 infections in the ECOWAS region reporting to Shadowserver's sinkhole servers over a designated period of time (in this case a 3-month period). The ngCERT official can also hover over the graph to reveal statistics for a given day.

RECOMMENDATION:
Shadowserver's public Dashboard can be an effective tool to inform key stakeholders (e.g., government leaders, policymakers, cybersecurity researchers, network defenders, media outlets and others) about the latest cyber threats affecting their country and/or the region. The Dashboard allows the public to query Shadowserver's data for aggregated, country-level or regional-level statistics associated with the latest cyber threats spanning the prior two years. It can then be used to prioritize and track remediation efforts to minimize or eradicate critical threats. The Dashboard can be queried for statistics associated with an individual country as well as a region, including a newly created query specifically for the ECOWAS region.

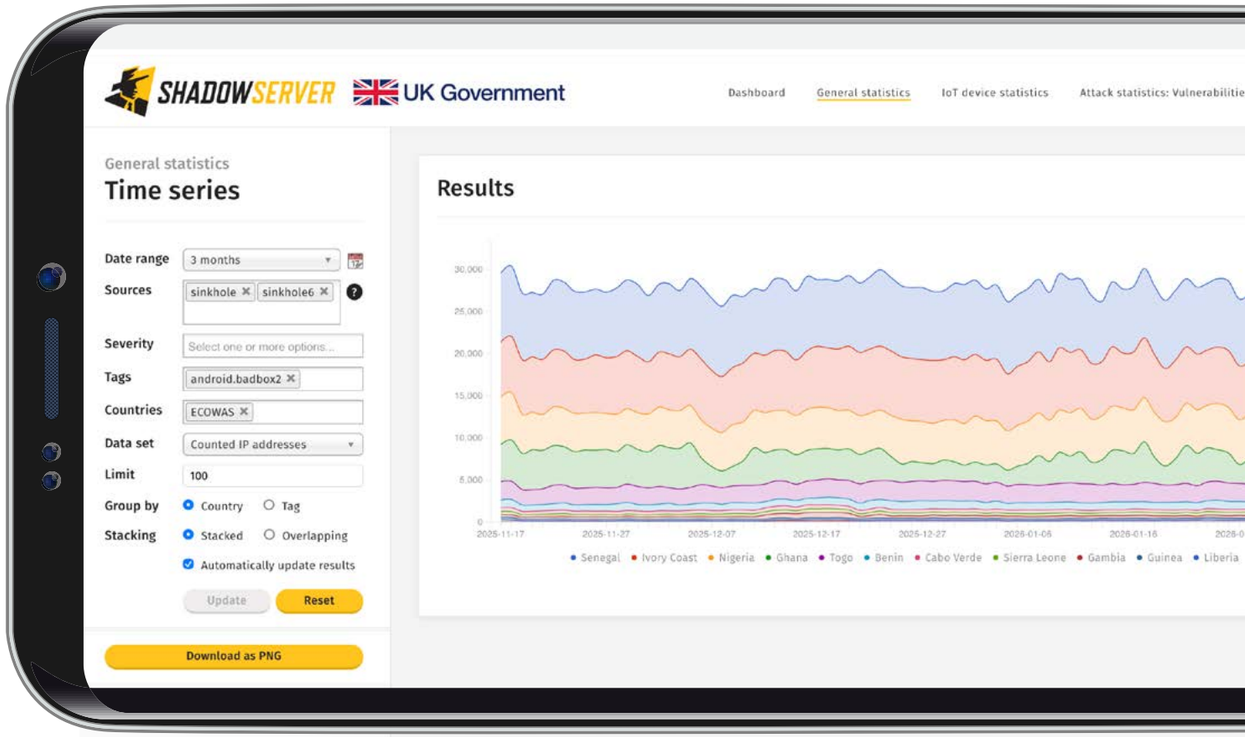


Figure 20. **Infected Android Badbox 2.0 devices in ECOWAS region reporting to Shadowserver's sinkhole servers over the past 3 month period from the date of query**

Glossary

Asset Inventory: a comprehensive, continuously updated catalog of all hardware, software, data, and network components an organization owns or uses, crucial for identifying vulnerabilities, managing risks, detecting threats, and responding to incidents.

Attack Surface: any possible entry points or attack vectors, including software vulnerabilities, that attackers can exploit to breach a system

Banking Trojan: a type of malicious software that disguises itself as legitimate software to trick users into installing it, with the primary goal of stealing sensitive financial information (e.g., online bank account credentials, credit card details, etc.) to perform unauthorized financial transactions.

Botnet: a network of inter-connected devices infected with malware and controlled as a group without the owners' knowledge or consent; often used by threat actors to facilitate criminal schemes, including the sending spam and phishing emails, launching denial of service attacks, and stealing data, to name a few.

Business Email Compromise (BEC): a type of online fraud scheme in which cybercriminals impersonate trusted individuals (e.g., CEOs, vendors, etc.) associated with a business, including by spoofing or hacking into legitimate email accounts of those individuals, to trick employees into wiring money, changing payment transaction details, or sending sensitive data such as tax information or login credentials.

Common Vulnerabilities and Exposures (CVE) ID: publicly disclosed security flaws in software, hardware, or firmware that have been assigned a unique identifier, or CVE ID, to facilitate consistent communication and tracking of vulnerabilities within the cybersecurity community.

Compromised Asset: any organizational resource (including a server, network, account, or data) whose security has been breached, leading to unauthorized access, disclosure, modification, or destruction, thereby impacting its confidentiality, integrity, or availability.

Credential Stealing Code Injection: a type of cyberattack in which threat actors exploit vulnerabilities in an application to inject and execute code in a targeted network or system to harvest credentials such as usernames and passwords.

Critical Infrastructure: the fundamental assets, systems, and networks – both physical and virtual – that are essential to the proper functioning of a nation's economy, security, and health, including but not limited to sectors such as energy, water systems, nuclear resources, transportation, telecommunications, defense, and food and agriculture systems.

Cyber Threat Actor: any person or group of persons that intentionally cause harm in the digital sphere, including cybercriminals, nation-state / government hackers, terrorists, hacker activists (hacktivists) and insiders.

Cyber Threat Landscape: the evolving and broad environment of potential and recognized cybersecurity risks, threats, and hazards, including the types of attackers and their motivations, affecting user groups, organizations, specific industries, or a particular time.

Glossary

Dark Net: a network that requires specific software to access, resulting in hidden portions of the internet designed for anonymity.

Data Leak Extortion: a cyberattack in which criminals steal sensitive data and then demand a ransom to prevent the data's public release, sale, or further misuse which could result in severe financial, legal, and reputational harm to the victim.

Dedicated Leak Site: a website or web platform, often hosted on the dark web, where cybercriminals publicly disclose the names and stolen data of victim organizations as part of a ransomware and/or data leak extortion attack, designed to leverage victims to pay a ransom in order to avoid financial, legal, and reputational harm that can result from disclosure of the sensitive data.

Devices: the hardware entities (such as computers and servers) on a network.

Distributed Denial of Service (DDoS): a type of cyberattack in which multiple compromised systems, often orchestrated as a botnet, flood a targeted network, server, or online service with an overwhelming volume of traffic that can slow down or even crash the target's systems. DDoS attacks are highly disruptive and capable of causing significant downtime, financial losses, and reputational harm.

Domain Name System (DNS): a system that translates human-friendly domain names (like www.example.com) into machine-readable IP addresses (like 192.0.2.44) that computers use to connect and find resources online while ensuring users do not need to memorize a long string of numbers in an IP address to access websites or online services.

Early Warning Service: a free service offered by many National CSIRTs (as well as some Sectoral CERTs, ISACs, and other entities with large constituencies) in which constituents provide their public IP addresses and domain names, and in return receive automated alert notifications about exposed, vulnerable, and compromised devices and services on their network to facilitate timely remediation.

Firewall: a network security system that acts as a barrier between a trusted internal network and an untrusted external one, such as the internet.

Honeypot Sensors: decoys configured to appear as legitimate, yet vulnerable, network assets (including software applications, servers and other devices) for the intended purpose of luring cyber threat actors to attack. The sensors then log the attacker's activities and collect information on the attacker's tactics, tools, and procedures / techniques. The collected data helps identify sources of attacks, new attack methods, develop defenses, and prevent future attacks.

Implant: a program embedded in a network or system in order to create remote access mechanisms and perform various functions without the user's knowledge, including data theft, disruption, and maintaining persistent access.

Information Sharing and Analysis Center (ISAC): a member-driven organization that gathers, analyzes, and disseminates actionable threat information to help members proactively mitigate risk.

Internet Protocol (IP) address: a unique numerical identifier assigned to each device that connects to the internet.

Known Exploited Vulnerability: a vulnerability in a software, hardware, application or system that is actively being exploited by threat actors, making the vulnerability a high-priority security risk that requires immediate patching to prevent a breach.

Law Enforcement Cybercrime Disruption Operation: a proactive effort by Law Enforcement Agencies to disrupt cybercrime activities by taking down criminal infrastructure (e.g,, servers, websites, etc.), arresting threat actors, and seizing assets.

Glossary

Malware: short for "malicious software" it is any software specifically designed to damage, disrupt, or gain unauthorized access to a computer system.

National Computer Security Incident Response Teams (National CSIRTs): a government-designated entity that coordinates national-level responses to cyber incidents, protecting critical infrastructure, government operations, and economic security by managing cyber-related threats, disseminating information, building awareness and implementing cyber strategies; often serving as a central point for reporting and responding to large-scale cyber events within a country.

Phishing: a type of cyberattack that uses fraudulent emails, text messages, phone calls or websites to trick victims into sharing sensitive data (such as usernames, passwords, bank account information, credit card numbers, or other important data), downloading malware, or otherwise exposing themselves to cybercriminal activity.

Ransomware: a type of malicious software (i.e., malware) that encrypts / locks a victim's files and systems making them inaccessible and then demands a ransom payment in exchange for the decryption key to restore access.

Registrar: a company that sells and manages domain names, acting as a go-between for individuals and businesses (known as "registrants") and the organizations (known as "registries") that control top-level domains.

Registry: a domain name registry is an organization that manages top-level domain names by creating domain name extensions, setting the rules for a particular domain name, and working with registrars to sell domain names to the public. For example, Verisign manages the registration of .com domain names and their domain name system (DNS).

Router: a device that forwards data packets to the appropriate parts of a computer network.

Sectoral Computer Security Incident Response Team (Sectoral CSIRT): a specialized entity that handles cybersecurity incident response, fosters information sharing to mitigate threats, and offers specialized knowledge and expertise, for a particular sector of a country or economy (e.g., water, health, energy, financial, transportation, etc.)

Server-side Application: refers to the functions, procedures, calculations, or processing methods performed on a server and managed behind the scenes on a remote system rather than on a user's device.

Services: the software applications or functions that devices provide or consume (such as a web server, email, or file storage) which enable network communication and resource sharing.

Simple Network Management Protocol (SNMP): a protocol that plays a crucial role in monitoring, managing, and securing network devices, by allowing network administrators to collect information, configure devices, and respond to network events remotely, thereby making it an essential tool for maintaining network performance and security.

Sinkholing: a technique that involves disrupting the communications between victims' malware-infected devices and the criminally controlled servers to which the malware directs them to communicate. The traffic is redirected to the sinkhole servers belonging to a responsible entity so the criminals can no longer access and control the victims' devices despite the fact the devices remain infected with malware unless and until remediated.

VPN Services: a VPN (virtual private network) service is an online tool that creates a secure, encrypted "tunnel" for internet traffic, hiding a user's real IP address and location to enhance privacy and security.

Glossary

Vulnerability / Vulnerabilities: a weakness in an information system, system security procedures, internal controls, or implementation, that could be exploited by a cyber threat actor to gain unauthorized access or cause harm to a system, network, or device.

Web Shell: a malicious script or program that threat actors deploy on a compromised web server to gain (and maintain) remote access and control over it, thereby allowing the threat actors to perform a range of malicious activities, including data theft and malware distribution.

Zero-Day Vulnerability: a security vulnerability in software, hardware, or firmware unknown to the vendor that attackers can exploit before the vendor is aware of it and has a chance to develop a patch to fix it.