INTERPOL

INTERPOL AFRICAN CYBERTHREAT ASSESSMENT REPORT 2024

OUTLOOK BY THE AFRICAN CYBERCRIME OPERATIONS DESK

3rd edition

APRIL 2024

CONTENTS

FOREWORD BY INTERPOL 2
FOREWORD BY AFRIPOL 3
ABBREVIATIONS AND ACRONYMS 5
ACKNOWLEDGEMENT 8
EXECUTIVE SUMMARY 9
1 Introduction 14
2 Overview of trends in the African Cyber threat landscape: 2023 16
3 Ransomware and digital extortion 18
4. Online scams 21
5. Business email compromise 22
6. Cyber resilience and law enforcement capabilities across the African continent 25
7. Way forward 25
ABOUT INTERPOL 2

FOREWORD BY INTERPOL

In today›s world, technology is not just a convenience; it is a foundation of our daily lives. The Internet, a cornerstone of this technological era, is vital for managing critical infrastructures, executing secure financial transactions, maintaining connections with loved ones, indulging in online shopping, and accessing a wealth of information and entertainment. Its ability to bridge vast distances and facilitate immediate access to data and virtual experiences has made it indispensable for all of us.

However, the digital age comes with its own set of challenges, mainly, the escalating threat of cybercrime. As technology advances, so do the tactics used by cybercriminals, who employ increasingly sophisticated methods to exploit vulnerabilities, posing a significant risk to individuals and organizations alike. Victims are often left financially, psychologically, and emotionally destitute. At the same time, the threat landscape is exacerbated by broader social, economic, and political developments, including the growing inequality between those countries, organizations, and individuals that are cyber resilient and those that are not. All these circumstances are exploited by cybercriminals at a national, regional, and global level, leaving behind an endless list of victims.

As we step into 2024, the importance of implementing comprehensive cybersecurity strategies cannot be overstated. Both large and small entities must safeguard themselves against a wide range of cyber threats, from conventional attacks to emerging, more sophisticated dangers.

For the last nine years, INTERPOL has been leading a cohesive and coherent international cybercrime programme, underpinned by its Global Cybercrime Strategy which aims to reduce the global impact of cybercrime and protect communities for a safer world. INTERPOL coordinates and supports its 196 member countries through activities which prevent, detect, investigate, and disrupt cybercrimes that cause high levels of harm and have a high impact, or that are very frequent or of high interest within the communities we help protect. This is implemented via a three-sided framework that provides support to member countries in the areas of information sharing, operational coordination, and strategic and capabilities development.

Within this context, INTERPOL has introduced a regional approach that offers tailored support through the Regional Cybercrime Operations Desks. The Africa Joint Cybercrime Operations Desk (AFJOC), funded by the United Kingdom Foreign, Commonwealth & Development Office, is an example of this initiative. It specializes in gathering and analysing information on cybercriminal activity, carrying out intelligence-led coordinated law enforcement action, and overall promoting cooperation and best practices amongst African member countries, as well as partnerships with both public and private stakeholders.

With this in mind, I am privileged to introduce the latest edition of the African Cyberthreat Assessment Report. This assessment provides a comprehensive analysis of the cyberthreat landscape in the African continent, specifically examining ransomware, business email compromise, and other forms of online scams. It goes beyond merely highlighting these cyber threats, but also examines continued national efforts to improve cyber resilience. The report concludes with strategic recommendations to pave the way forward.

Throughout the analysis, the critical need for international and regional cooperation among law enforcement agencies in the face of cybercriminal activities is shown to be incontestable. A unified approach enhances the ability to address threats effectively, allowing for intelligence exchange, sharing investigative practices, and making use of advanced technologies.

Policing will always need to be delivered locally and will always be an integral part of our communities. However, crimes such as cybercrime have a global footprint and involve a volume, scale and complexity that can be challenging for all. We have a collective responsibility to prevent, detect, investigate, and disrupt the criminals and groups behind these crimes. Whether individuals or business connecting to the Internet, we need to be safer.

In this complex landscape, no single actor alone can enable us to ensure our collective safety. Acknowledging this, INTERPOL serves as a neutral and trusted interlocutor, fostering collaboration between law enforcement and the public and private sectors. By combining efforts and sharing expertise, INTERPOL aims to strengthen our collective defences against cyber threats, emphasizing the responsibility we share to secure our digital world.

In conclusion, I would like to extend my gratitude to our member countries in the African region and to our partners, for their unwavering support and dedication to this cause and their contribution to producing this assessment. Their relentless effort and commitment are key to advancing our shared goal of a safer digital environment for all.

Craig Jones
Director, Cybercrime Directorate
INTERPOL

FOREWORD BY AFRIPOL

As we reflect on the past year and look towards the future, the landscape of cyber threats in Africa, and indeed globally, continues to evolve, becoming increasingly complex. The journey from the late 1990s, where Internet access in Africa was a luxury few could afford, to today, where we are witnessing a surge in connectivity, illustrates the remarkable trajectory of technological advancement. This journey, however, is not without its challenges. The proliferation of cyber threats has escalated, reaching every corner of our continent and affecting individuals, governments, and industry alike.

The year 2023 has been pivotal in shaping our response to these emerging threats. Building on the foundations laid in previous years, the battle against cybercrime has made significant progress. Our collaboration with INTERPOL has never been stronger, and is marked by innovative initiatives and the deployment of advanced technologies aimed at fortifying our cyber defences. The establishment of the AFRIPOL data centre and forensic databases, and the inauguration of the Criminal Intelligence Analysis Unit (CIA), are critical milestones in our journey towards a safer cyber environment in Africa.

The launch of the AFRIPOL Bootcamp on Cybercrime investigation is testament to our commitment to capacity building on the continent. The expansion of these programmes to include advanced modules on cybersecurity threats and response strategies has enriched the arsenal we can use against cybercriminals. The engagement from member states has been overwhelmingly positive, with participation numbers soaring and a marked improvement in the skillsets of our cybersecurity personnel.

In 2023, our partnerships have flourished, extending beyond our traditional allies to include tech giants and academic institutions. These collaborations have enabled us to tap into cutting-edge research and technology, thus enhancing our adaptability to the ever-changing cyber landscape. Our focus has also expanded to address the socioeconomic impact of cyber threats, in the knowledge that cybersecurity is not just a technical challenge but a cornerstone of our economic stability and growth. Africa has a burgeoning digital economy, and protecting this vital sector is paramount for our sustainable development.

Looking ahead to 2024, AFRIPOL is committed to multiplying our efforts on four strategic fronts:

1. Recognizing the borderless nature of cyber threats, we aim to strengthen our network of cooperation across the continent and with our global partners. This includes sharing intelligence, joint operations, and harmonizing legal frameworks to ensure a unified front against cybercrime. We are also strengthening collaboration with the private sector in order to harmonize and standardize procedures and technologies, and to enable intelligence-gathering across the continent.

At the start of 2024, AFRIPOL signed a Memorandum of Understanding with Group IB, a global leader in cybersecurity. This partnership will enhance intelligence sharing and equip the African union member states with cutting-edge technology and specialized knowledge in critical areas such as cyber investigations, reverse engineering, and incident management. By leveraging these advanced tools and expertise, AFRIPOL will bolster its capabilities in safeguarding against cyber threats on the continent. Moreover, AFRIPOL is due to sign an agreement with Kaspersky, a strategic private partner.

2. A key element of our strategy involves forming a task force for sharing information on cybercrime incidents and providing the necessary investigative support. We are dedicated to supplying essential hardware and software for cybercrime investigations to our member states, along with specialized training on these tools. Some examples of our initiatives are the INTERPOL-AFRIPOL 3rd Joint Cybercrime Operation, known as Africa Cyber Surge 3, our specialized training on virtual assets, and the provision of crucial investigation tools jointly with INTERPOL, all of which underscore our unwavering commitment to bolstering our cyber defence capabilities across the continent.

3. We will continue to explore and integrate emerging technology such as artificial intelligence and blockchain in order to enhance our cyber defence capabilities. These technologies offer promising avenues for predictive threat analysis, secure data management, and efficient resource allocation. Furthermore, we are embracing open-source technologies through our training programs, which shows our commitment to overcoming the financial challenges associated with costly licensing fees.

4. We have an increased focus on community engagement, and plan to launch comprehensive cyber-awareness campaigns targeting vulnerable populations, including young people and SMEs. Educating these key demographics on cyber hygiene practices is a critical element in mitigating the risk of cyber threats at a grassroots level.

The path ahead is fraught with challenges, but our resolve remains unshaken. As we forge ahead into 2024, we have a clear vision: to create a secure, resilient digital Africa where technology serves as a beacon of progress, not a vector of vulnerability. Together, with the unwavering support of our partners and the collective efforts of our member states, we are poised to make this vision a reality. Let us embrace this journey with determination and optimism, as the security of our cyberspace is the cornerstone of our shared prosperity.

Ambassador Jalel CHELBA
Ag. Executive Director,
AFRIPOL

ABBREVIATIONS AND ACRONYMS

AFJOC	African Joint Operation against Cybercrime
AI	Artificial Intelligence
BEC	Business Email Compromise
BPH	Bulletproof Hosting
CaaS	Crime-as-a-Service
CCP - Operation	Cybercrime Collaborative Platform - Operation
CERT	Computer Emergency Response Teams
CSIRT	Computer Security Incident Response Team
CKE	Cyber Knowledge Exchange
DDoS	Distributed Denial of Service
GLACY+	Global Action on Cybercrime Extended (currently GLACY-e)
IP	Internet Protocol
ISPA	INTERPOL's Support Programme for the African Union
LLM	Large Language Models
MFA	Multi-Factor Authentication
PII	Personally Identifiable Information
RAT	Remote Access Trojan
RDP	Remote Desktop Protocol
SMEs	Small and Medium-sized Enterprises

ACKNOWLEDGEMENT

This assessment report was written by the Africa Cybercrime Operations Desk under the aegis of the African Joint Operation against Cybercrime (AFJOC), and funded by the United Kingdom's Foreign, Commonwealth and Development Office (FCDO). INTERPOL's Support Programme for the African Union (ISPA), supported by the German Federal Foreign Office, also contributed to this report, with the support of the German Federal Foreign Office.

This report is based on the assessment of information provided to INTERPOL by the relevant member countries and INTERPOL's private partners, including Bi.Zone, Fortinet, Group-IB, Kaspersky Lab, and Trend Micro.

INTERPOL

Foreign & Commonwealth Office

Auswärtiges Amt

EXECUTIVE SUMMARY

This report presents INTERPOL's analysis of the main cyber threats affecting the African continent, drawing on internal intelligence, operational insights, survey results, and contributions from private sector partners.

The key findings of the report underscore the continent-wide escalation of cybercrime, with ransomware, business email compromise, and other forms of online scams emerging as the most rapidly expanding threats in 2023. Ransomware in particular was identified as a critical emerging threat which frequently targets essential infrastructure, while online scams remain the most common form of digital crime against individuals and companies, with significant volume and financial implications. The report also notes the rapid evolution of threat actors and their modus operandi, including the growing exploitation of social media, the use of artificial intelligence, and advanced social engineering techniques.

The document sheds light on African national efforts in addressing cybercrime, focusing on legislative development, the enhancement of law enforcement capabilities, fostering partnerships, and public engagement. While member countries have taken important steps to strengthen their cyber defences and improve law enforcement responses, there is still a range of hurdles to achieving a comprehensive, coordinated, and sustainable approach to countering cybercrime across the continent.

INTERPOL's commitment to Africa in terms of fighting cybercrime, as well as the assistance it provides in this area, can be seen throughout the report. This is primarily carried out through a specialized regional approach led by the INTERPOL Africa Cybercrime Operations Desk and implemented via the "Africa Joint Operation Against Cybercrime" project, which is funded by the United Kingdom's Foreign, Commonwealth and Development Office. This initiative is complemented by other significant activities, included those delivered by the INTERPOL Support Programme for the African Union and the Global Action on Cybercrime Extended.

The report concludes with strategic recommendations from INTERPOL on how to navigate the African cyber threat landscape and strengthen cybersecurity across the continent. Recommendations include adopting or improving comprehensive and unified cybersecurity measures, investing in law enforcement cyber capacities (people, processes, and technology), creating synergies within the cybersecurity ecosystem, raising public awareness, and strengthening international and regional cooperation.

INTRODUCTION

African countries are experiencing a remarkable digital transformation. Despite ongoing challenges in infrastructure coverage, access, and quality, the number of Internet users continues to increase across the continent, with over 160 million individuals regularly accessing cyberspace between 2019 and 2022.[1] The impact of digitalization is clear to see across numerous sectors, ranging from critical infrastructure to banking and e-commerce. It is also permeating many aspects of African citizens' daily lives, from the rapidly rising number of digital payments to the increasing amount of time spent online, especially on social media platforms. On an individual level, growing access to the Internet is facilitated in particular by the widespread adoption of mobile phones, with over 650 million Africans using these devices as their primary means of accessing the Internet.

This digital revolution is having a particular impact on Africa's young people, who represent over 60 per cent of the continent's population.[2] Many are increasingly turning to the Internet, often via mobile phones, to communicate, work, transfer money, shop, and express their creativity. As young Africans rapidly adopt digital technologies, they are contributing to the development of a youthful, cyber-driven society. This presents countries with incredible opportunities for continued growth and innovation, but also emerging cyber security challenges and vulnerabilities.

The rising number of Africans who are going online, economies' and societies' growing reliance on technology, and the advent of so-called "digital natives" are inevitably broadening the cyber-attack surface for criminals. As a result, cybercrime is surging across Africa, and is one of the fastest emerging threats across the continent. The first INTERPOL Africa Cyberthreat Assessment Report (2021) estimated the financial impact of cybercrime in the region to be more than USD 4 billion, which is about 10 per cent of Africa's total gross domestic product.[3] Since then, the challenge confronting INTERPOL's 54 African member countries has only grown in volume, impact, and complexity.

Addressing poor digital literacy, inadequate cyber preparedness, and a general lack of good cyber hygiene practices is becoming increasingly urgent. Fortunately, African countries have taken important steps in 2023 to build more secure digital economies and protect their communities online. INTERPOL is committed to supporting its member countries in fulfilling these objectives. Recognizing the incredible diversity of the African continent, including its vast array of cultures, languages, and economic conditions, key projects and programmes such as the African Joint Operation against Cybercrime (AFJOC) and the INTERPOL Support Programme for the African Union (ISPA) deliver critical activities tailored to the needs of the various African national law enforcement agencies.

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

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

3 Research from a Kenyan IT cybersecurity company, Serianu: Available at: [https://phys.org/news/2021- 05-rights-group-tool-stem-cybercrime.html]

OVERVIEW OF TRENDS IN THE AFRICAN CYBER THREAT LANDSCAPE: 2023

In 2023, the African cyber threat landscape remained highly dynamic, with attacks evolving rapidly in sophistication and scale. Based on intelligence and operational data from INTERPOL's regional activities, complemented with the results of a questionnaire distributed to African member countries and information from private sector partners, INTERPOL has identified the following key threats and trends:

The volume and impact of cybercrimes continue to surge across Africa

- The number of cybercrime attacks continues to rise across the African continent, as highlighted by INTERPOL member countries.[4]
- Over two thirds of respondents assessed cyber-dependent and cyber-enabled crimes as being medium to high risks in their jurisdiction. In particular, countries indicated an increase in the financial and social impact of these crimes.
- In a further illustration of the rapid growth of cybercrime, it is estimated that in 2023, there was a 23 per cent year-on-year increase in the average number of weekly cyberattacks per organization in Africa. This average was the highest in the world.[5]

Ransomware, business email compromise, and other online scams were the fastest growing cyber threats in 2023

- Previous editions of the INTERPOL African Cyberthreat Assessment Report identified the following most prominent cyberthreats: malware attacks, including ransomware, banking trojans and stealers; phishing and online scams, such as business email compromise (BEC); and crimeware-as-a-service, such as spyware and phishing kits. These threats continue to have an impact on the African cyber landscape, causing significant harm to communities across the continent.
- In 2023, the top cyber threats identified by African member countries were ransomware, BEC, and other online scams.
- Ransomware was highlighted as one of the most serious emerging threats on the continent, often targeting critical infrastructure, while online scams are still the main form of digital crime affecting individuals and organizations, in terms of volume and financial impact.

Threat actors and their modus operandi are evolving rapidly – from more sophisticated social engineering techniques to the increasing use of social media and artificial intelligence

- Cybercriminals operating both in and from Africa continue to exploit human vulnerabilities as a main method of attack. They are deploying increasingly sophisticated social engineering techniques to target organizations and individuals.
- Email phishing remains one of the primary initial attack vectors across a variety of cybercrimes, including ransomware and many forms of online scams. In addition, criminals are progressively exploiting different communication channels, including social media and instant messaging apps, in line with regional technological and societal trends.
- Perpetrators are integrating technological advances into their modus operandi. Prominent examples include the growing use of data theft as a form of extortion, as well as the rising misuse of artificial intelligence.

4 This information is based on self-reporting by African member countries. It should be noted that definitions of cybercrime may vary across jurisdictions.

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

In response to the escalating threat posed by cybercrimes, African member countries have taken important steps to enhance cyber resilience and law enforcement capabilities

- There was an increase in arrests, actions, and investigations, aided by the expansion of anti-cybercrime resources. For instance, 19 member countries highlighted a cumulative total of 10,490 arrests related to cybercrime from January to December 2023. Considering that these countries represent only 35 per cent of the continent, the total number of cybercrime arrests is likely to be much higher.
- Over the last two years, a dozen African countries have adopted or have engaged in the process of adopting new cybercrime-related legislation. This marks a proactive stride towards strengthening legal frameworks to combat cybercrime.
- There was also substantial growth in investment in countering cybercrime on the continent, including from African member countries and stakeholders outside the region. In 2023, more countries established dedicated cybercrime units, nearly half increased staffing levels, and over 60 per cent reported being involved in capacity-building initiatives. Furthermore, there were over 130 training initiatives, as well as more than 40 public awareness campaigns on the continent.

However, significant investigative challenges remain in terms of effectively preventing, detecting, investigating and disrupting cybercrime across Africa

- The continued underreporting of cybercrimes hinders law enforcement's ability to act. In some countries, this challenge is aggravated by the absence of specific or easy-to-use reporting and recording platforms.
- Despite some progress, collaboration between law enforcement and other key stakeholders – including the private sector and cybersecurity agencies – remains a challenge in some jurisdictions.
- Insufficient cyber hygiene continues to undermine cyber resilience across the continent, as many African organizations and individuals still show low levels of preparedness against cyberattacks.

The following sections provide an in-depth analysis of the trends in the top cyber threats identified by INTERPOL's member countries in Africa: ransomware, online scams and business email compromise.

RANSOMWARE AND DIGITAL EXTORTION

Key Points:

- Ransomware and digital extortion are on the rise, with over half of INTERPOL's African member countries reporting attacks against their critical infrastructure.
- Phishing emails remain the most common attack vector for ransomware attacks in Africa, while the extortion methods and business models used by cybercriminals are evolving.
- Overall, African member countries have taken positive steps to enhance their resilience to ransomware attacks, but persistent challenges remain, notably in terms of the reporting of attacks and the payment of ransoms.

Ransomware and digital extortion on the rise in Africa

Ransomware and digital extortion were identified by INTERPOL member countries as one of the most serious cyberthreats faced by the African continent. Such attacks are of particular concern due to their high financial impact, their ability to severely disrupt critical infrastructure and essential services, and the harm they can cause to the organizations and individuals affected. The scale of the challenge is clear: according to cyber security company Chainalysis, ransomware payments exceeded USD 1 billion globally in 2023.[6]

The volume, frequency, and impact of ransomware attacks continues to grow in Africa. Research from cyber security firm Check Point suggests that on average, 1 out of every 15 organizations in Africa experienced a ransomware attempt every week during the first quarter of 2023. This is even higher than the global weekly average, which stood at about 1 in every 31 organizations.[7] During a single week in February 2023, INTERPOL private partner Kaspersky reportedly detected over 300 cases of ransomware attempts in South Africa, which illustrates the increasing frequency of attacks.[8] The financial impact of attacks also appears to be on the rise: according to IBM, the average cost of a ransomware attack in 2023 was USD 5.13 million, which is a 13 per cent increase on 2022.[9]

African critical infrastructure under attack

Worryingly, nearly half of the African countries surveyed reported ransomware attacks against their critical infrastructure between January 2023 and December 2023. This includes attacks targeting government infrastructure, hospitals, financial institutions, and Internet service providers. To give a few examples, in recent years Ghana's largest electricity seller, the Electricity Company of Ghana (ECG), the national banks of Zambia and South Sudan, government institutions in Ethiopia, Senegal and Zimbabwe, and South African Internet service provider RSAWEB have all been subjected to ransomware attacks. Even the African Union faced a crippling attack from the BlackCat group (also known as ALPHV) against its internal network in 2023, which INTERPOL and its partners were able to mitigate.[10] The targeting of critical infrastructure is particularly alarming, as digital transformation continues to accelerate across the continent and essential systems become increasingly connected.

Besides critical infrastructure, African member countries also reported ransomware attacks across various sectors. This includes a significant number of attacks against businesses across sectors such as finance, manufacturing, and retail. For instance, according to IT security company Sophos, 78 per cent of companies in South Africa suffered ransomware attacks in 2023.[11] Some examples of high-profile attacks include those against Porsche South Africa's Johannesburg headquarters, and the South African division of international credit bureau TransUnion. These trends are in line with global developments. According to aggregated data provided by INTERPOL private sector partners, while banking, government, retail, and the technology and healthcare sectors were the most targeted globally, no sector, institution, or organization is immune to ransomware attacks.

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

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

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

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

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

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

Persistent exploitation of the human element

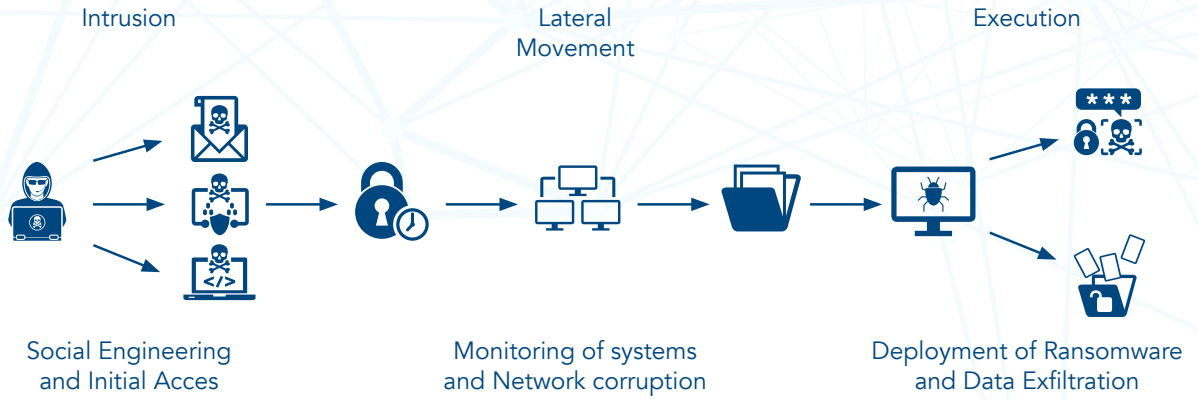
In terms of modus operandi, **phishing emails appear to be the most common delivery vector** for ransomware attacks in Africa, **with about half of INTERPOL's African member countries reporting instances of phishing during such attacks.** These emails typically contain a malicious file or URL, designed to facilitate access to a system by a threat actor or to immediately deploy malware when clicked on. Other common infection methods used by ransomware groups in the African region include the exploitation of unsecured remote desktop protocol (RDP) connections and other vulnerabilities. These regional trends are consistent with the global findings of INTERPOL private partner Trend Micro.[12] According to the cyber security firm, the most common initial attack vectors used by ransomware groups worldwide are email, web and web applications, malicious software such as fake mobile apps, and the exploitation of system vulnerabilities such as unsecured RDP connections.

Understanding how threat actors gain initial access in order to deploy ransomware is paramount to improving prevention, detection and mitigation efforts. Notably, most of the attack vectors exploit the human element, whether it is a user clicking on a malicious URL or an IT administrator failing to regularly update or patch their systems. In fact, research from cyber security firm Fortinet, an INTERPOL Gateway partner, indicates that many ransomware groups are spending more time selecting and researching their targets.[13] They leverage information from personal social media accounts, company websites, conference webpages, and previous data leaks in order to carry out more effective social engineering attacks and gain initial access to systems to deploy ransomware.

Evolving tactics for digital extortion

Once ransomware threat actors have gained initial access, they typically aim to map out the network infrastructure of their target and to move laterally across the system by exploiting vulnerabilities and increasing their privileges. They will then deploy malware that encrypts their target's data and demand a ransom from their victims, in exchange for restoring their files. To increase the pressure on their targets, many groups use scareware or additional extortion tactics. For instance, attackers may exfiltrate data before encrypting it and later threaten to leak sensitive information (double extortion), use service disruption attacks to cripple targets who are reluctant to pay (triple extortion), and even threaten their main victim's third-party associates in order to increase the pressure (quadruple extortion).

However, in recent years INTERPOL has detected the growing use of data exfiltration for digital extortion. Following the initial intrusion into their target's system, some ransomware groups now prefer to bypass the encryption stage and simply exfiltrate sensitive data. They then threaten to leak this information unless their victims pay a ransom. Because of the potential financial, reputational, and psychological damage from such leaks, many organizations appear more willing to pay. Ransom payments can reach several millions of dollars, even though there is no guarantee that the attackers will actually delete the stolen data. Due to its lucrative potential, data exfiltration is rapidly emerging as a key modus operandi, both instead of and in combination with encryption, transforming the ransomware, and digital extortion.



Overview of a typical ransomware and data exfiltration attack

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

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

Affiliate programs and the growth of the cybercriminal services ecosystem

Besides evolving modus operandi, the growing impact of ransomware may be partly attributed to the rise of new organizational models employed by cybercriminals. INTERPOL and its partners have detected that many ransomware groups now run elaborate affiliate programs, which involve the development of platforms offering ransomware as a service to third party criminals, known as "affiliates". Affiliates can use the platforms provided by the core ransomware group to deploy malware, post exfiltrated data, and launder the proceeds of their crimes. In exchange for using the platform, the affiliates pay a fee to the core ransomware group, which can be a monthly subscription or a percentage of the ransom payments received through the platform.

As they become more mature, such ransomware-as-a-service operations are enabling cybercriminals to streamline processes and upscale their activities. They are also contributing to the emergence of new, more sophisticated and aggressive variants. Fortinet detected over 10,600 new ransomware variants in the first half of 2022, which is double the number seen in the six months prior.[14] Crucially, affiliate programs and other ransomware-as-a-service operations draw on the continuous development and specialization of the cybercriminal services ecosystem. Core members of ransomware groups recruit various specialists to run the affiliate programs, including developers, pen-testers, system administrators, data managers, negotiators, recruiters, legal experts, and accountants.[15] They also draw on external service providers, such as initial access brokers, and money laundering and bulletproof hosting services. For instance, Br0k3r, one of the most active initial access brokers targeting Africa and the Middle East, had over 60 offers to access corporate networks with domain administrate privileges for sale on its own online store in the past year.[16] As core members, affiliates and service providers can be part of several groups, and it is important to disrupt the cybercriminal services ecosystem as a whole in order to effectively disrupt cybercrime.

INITIAL ACCESS BROKER	RANSOMWARE AFFILIATE	DATA MANAGER	RANSOMWARE OPERATOR	NEGOTIATOR	CHASER	ACCOUNTANT
Obtain initial access to organizations	Persistence/ Reconnaissance	Supply data exfiltration infrastructure and software	Supply ransomware infrastructure and software	Negotiate with victim organisation	Put pressure on victim organisations by threatening with continuous attacks and leaking of stolen data	Launder ransom payment
Monetize networks by selling them to any actor	Lateral movement	Exfiltrate data from victim organisation				
	Privilege escalation	Publish exfiltrated data if applicable				
	Ransomware deployment					
IN	THROUGH		OUT			

Source: Northwave-Cybersecurity.com

Overview of cybercriminal services ecosystem that enables ransomware

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

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

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

OPERATION LANDSLIDE

Beginning in early 2023, INTERPOL initiated an operation code-named Landslide which targets the infrastructure that enables cybercrimes such as ransomware. The specific aim of operation Landslide was to take down an enabler of crime that for too long has been beyond the reach of law enforcement: bulletproof hosting (BPH). Working with authorities in the Seychelles and private partner Trend Micro, INTERPOL identified a number of bulletproof hosting providers involved in enabling illicit activities. Using the results of previous operational activities, INTERPOL succeeded in cleaning and taking down malicious infrastructure. The operation is ongoing.

Resilience to ransomware in Africa: significant progress and ongoing challenges

INTERPOL's African member countries have taken significant steps to address the persistent threat of ransomware. For example, more than 60 per cent have introduced a cyber breach reporting mechanism to support the detection, mitigation, and investigation of attacks. States are also increasing collaboration with the private sector, with nearly two thirds of African member countries surveyed having established partnerships with private stakeholders in order to combat ransomware. In addition, African countries have reported increased efforts to raise companies' awareness of the threat of cyber extortion. At a regional level, another positive development is the establishment of joint task forces involving law enforcement agencies across Africa in order to better respond to ransomware attacks and raise awareness about their impact.

Despite these significant achievements, member countries also reported ongoing challenges. The level of reporting by victims of ransomware attacks remains an issue, and affects law enforcement's ability to launch investigations. Additionally, member countries reported that 16 per cent of victims ended up paying the ransom during ransomware attacks. Unfortunately, paying the ransom does not guarantee that the attack will stop, nor that the malicious software will be removed from systems. In some cases, the victim may not even get their data back, or will face double the recovery cost.[17] In addition, paying the ransom does not prevent re-victimization. Worse, it may provide incentives and resources for ransomware actors to continue and expand their activities. Recognizing this challenge, INTERPOL, alongside fifty countries who are members of the International Counter Ransomware Initiative, issued a joint statement in November 2023, strongly discouraging organizations from paying ransomware demands.[18]

ONLINE SCAMS

Key Points:

- Online scams and related modus operandi are constantly evolving, with perpetrators targeting victims from all demographic groups and sectors.
- Email and social media phishing exploit the human element and act as an important gateway for other cybercrimes.
- Artificial Intelligence is providing new avenues for criminals engaging in pig butchering and romance scams.
- In a reflection of social trends, smartphones are increasingly being targeted by scammers through banking trojans.

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

18 The statement is available on the official website of the Counter Ransomware Initiative: https://counter-ransomware.org/briefingroom/8ed7d1de-1a74-4a36-a2df-d5950624ebd8

Online scams, a major socio-economic crisis in Africa

In addition to ransomware, one of the top cyber threats identified by African member countries in 2023 was online scams, particularly in terms of their volume and overall financial impact. An online scam is a fraudulent act or operation conducted through the use of computer technology and via the Internet, with the intent of stealing money and/or personal information from individuals or organizations. To achieve their objectives, criminals typically use a combination of technical elements, such as phishing and malware, associated with social engineering techniques.[19]

The explosive growth of online scams is linked to the digital transformation sweeping across the African continent.[20] As Africans spend more time in the cyber realm, for instance communicating through social media or paying via mobile banking, the attack surface has expanded for criminals seeking to commit fraud through digital means. It is difficult to quantify the losses caused by online scams across the African continent, however INTERPOL's member countries have indicated that individual victims are spread across all age groups, genders, and professions. While some groups may be more vulnerable to specific forms of online fraud, ultimately, any citizen may become a victim. Likewise, the organizations targeted by online scams can range from small and medium-sized enterprises (SMEs) to very large organizations, and are distributed across all sectors and industries. In short, the prevalence of online scams in Africa is a major socio-economic crisis, affecting countries in the region and beyond.

Among the wide range of online scams, INTERPOL's African member countries reported five particularly prominent types of fraudulent schemes in 2023. Presented in the order of their discussion, these are: **business email compromise, phishing scams, romance scams, pig butchering, and mobile phone scams.** These different forms of online scams are analysed below, with the exception of business email compromise, which is examined in a separate section due to its particularly high prevalence in Africa.

Email and social media phishing act as a gateway into other cybercrimes

Phishing was identified by African member countries as the most predominant online scam threat, both in terms of the number of cases and their socio-economic impact across the continent. Phishing scams are a type of online fraud where attackers impersonate legitimate organizations or entities through email, messaging platforms, or fake websites, to deceive individuals into providing sensitive personal information.[21] This information often includes login credentials, financial details (such as credit card numbers), social security numbers, and other data that can be used to obtain unauthorized access to accounts or to carry out identity theft or financial theft. Phishing attempts typically involve urgent or alarming communications that aim to provoke the recipient into taking immediate action, such as clicking on a malicious link, downloading an attachment infected with malware, or directly providing confidential information. While the primary goal of phishing is to exploit human psychology to access to valuable data or assets, **in practice phishing attacks often act as a gateway for other cybercrimes, including ransomware and various types of online scams.**

Across Africa, two distinct forms of phishing have been identified, based on the results of the survey and in accordance with INTERPOL internal data: traditional phishing and social phishing. Within this context, African Member Countries have identified traditional phishing as the most significant cybercrime threat in the region. Primarily executed via email, traditional phishing campaigns often involve emails that come from addresses which appear to be legitimate, but which are in fact fake. The objective is to manipulate recipients into visiting fraudulent websites or clicking on malicious links, where any personal information entered is then stolen by the perpetrators. One prevalent form of email phishing attack is business email compromise, which is discussed further in the next section of this assessment.

19 To counter the growth of online scams, the INTERPOL Cybercrime Directorate works closely with the INTERPOL Financial Crime and Anti-Corruption Centre (IFCACC). Further information about IFCACC is available here: https://www.interpol.int/en/Crimes/Financial-crime

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

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

Despite the continued importance of traditional phishing, African member countries are reporting a growth in the use of **social media and instant messaging to commit phishing attacks.** The modus operandi is similar to traditional phishing but on different platforms, with perpetrators using fake social media accounts and deceptive posts as lures to obtain victims' financial data and personally identifiable information (PII). According to data provided by INTERPOL member countries, the platforms most commonly abused for phishing scams in Africa were Meta (formerly Facebook), Messenger, and WhatsApp. The adaptation of phishing techniques to include social media and messaging services is a way of targeting the prevalent modes of communication in the region and illustrates scammers' ability to exploit technological and social trends for malicious purposes.

Both forms of phishing are underpinned by social engineering. In this regard, it is concerning that INTERPOL member countries are reporting threat actors deploying increasingly sophisticated social engineering tactics as part of modern phishing campaigns. For instance, during Operation Echoes, led by Morocco with the support of INTERPOL and its private partners, it was revealed that the criminal known as 'Ex-Robotos', who is known for developing a phishing kit with the same name, meticulously targeted victims through online research, with a preference for CEOs and other executives. In other cases, scammers have made use of legitimate services and the takeover of domains and email accounts to improve the success rate of their phishing campaigns. Lastly, data from INTERPOL member countries and Gateway partners suggests that artificial intelligence is the latest technological development exploited by criminals, for example to minimize traditional phishing warning signs.

OPERATION ECHOES:

In May 2023, Moroccan authorities, working in close collaboration with INTERPOL, Microsoft, and Group-IB, successfully dismantled the activities of cybercriminals suspected of using a Microsoft 365 phishing kit to target thousands of victims. The kit had enabled criminals to steal victims' data, which could then be directly monetized or sold on the dark web. The joint action, dubbed Operation Echoes, built on past collaboration with Moroccan authorities, including Operation Lyrebird, and demonstrates the country's resolve in terms of addressing cyber threats.

Catfishing and sextortion fuel an epidemic of romance scams

Data provided by INTERPOL African member countries also highlighted the growing volume, impact and sophistication of romance scams occurring in and originating from the African continent in 2023. Romance scams can take a variety of forms, but they all revolve around criminals faking a romantic relationship or intimate friendship for financial gain. Generally, fraudsters will connect with their victims under the guise of a romantic connection, often using a fake online identity. According to the data provided by INTERPOL member countries, criminals across Africa most frequently approach their targets through social media, messaging services, and online dating applications. They then attempt to develop a personal relationship with the victim, preying on their vulnerabilities and weaknesses. This stage can be over very quickly, or can last several years. Once they have succeeded in establishing the illusion of a trusted relationship, perpetrators proceed to manipulate and/or steal from their victims.

In Africa, INTERPOL member countries highlighted two trends of particular importance for romance scams: **catfishing** and **sextortion**. In the context of romance scams, catfishing schemes occur when scammers create a fake online persona to deceive their victims.[22] They do this by stealing information and images from other people to create fake identities for themselves. The deception may range from using a stolen profile picture to appear more attractive, to fully appropriating another individual's identity, including their name, image, gender, date of birth, and geographical location. **As reported by INTERPOL African member countries, catfishing schemes tend to be aimed at selected targets and occur over a long period of time.** After choosing their victims, scammers use a carefully crafted script to build a trusted relationship, before attempting to emotionally manipulate them into transferring money. For instance, a scammer may claim that they or someone close to them is sick, hurt, or in jail, or ask for financial support to meet in person or plan for a joint future.[23] Once the funds have been transferred, they disappear, leaving the victim not only financially destitute but also emotionally and

22 The practice of catfishing has been around for many years, especially on online dating forums and websites. Individuals may engage in catfishing for different reasons. Some may be driven by insecurity, while others have malicious intent – e.g., for cyberbullying or to scam victims.

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

psychologically distraught. Besides using increasingly sophisticated social engineering tactics, **some romance scammers are also harnessing advances in artificial intelligence (AI) technology.** In addition to creating deepfake images to hook their victims, they are exploiting AI chatbots such as "LoveGPT" to create fake profiles, help with text-writing, and, ultimately, catfish their targets on dating apps.[24]

The second trend in romance scams reported by African member countries is a rise in instances of sextortion. Sextortion bears some similarity to other forms of romance scams. Criminals generally use a fake identity to contact their victims - often young people – through dating apps, social media, and other online platforms. However, after gaining their trust, scammers convince their target to send intimate or sexually explicit information, and then threaten to publish this content online or to share it with relatives and friends as a form of blackmail. To put more pressure on their victims, criminals sometimes begin by releasing their target's intimate information online and then demand a payment in exchange for taking the content down. While sextortion is often associated with explicit messages, photos, or videos, it is important to note that, depending on the particularities of the community in question, it may be enough for a scammer to threaten to publicize romantically charged chats to extort their victim.

The modus operandi of sextortion appear to be highly dynamic. For instance, some member countries reported sextortion cases in which phishing methods were used to target victims' private (unpublished) content on their Facebook and Instagram accounts. In these scenarios, the perpetrator unlawfully accesses victims' social media profiles and, upon gaining entry, systematically searches for and extracts intimate content. The criminal aspect of this operation culminates when the perpetrator then extorts the victims, threatening to publish their private content on social media platforms, or share it in any form, unless a payment is made. Another recent development involves the use of artificial intelligence to generate "true-to-life" sexually explicit images to intimidate and extort victims – including minors.[25] Given the significant challenges that they can face in removing such manipulated content once it is published online, some victims prefer to pay the extortionists.

Romance scams have proven to be highly profitable. Reports from African member countries reveal that payments made in response to romance scams, which encompass both catfishing and sextortion, are not merely isolated incidents. Instead, victims often find themselves paying what amounts to a recurring monthly fee, either to preserve their perceived romantic relationship or to prevent the release of their personal content. According to some estimates, global losses associated with this cyber threat exceeded USD 1.3 billion between 2017 and 2022, with the average victim losing around USD 4,400 per scam.[26] Besides their financial impact, romance scams can have a devastating emotional impact on victims, with some cases even resulting in suicide. In fact, because of feelings of shame, guilt and/or denial experienced by victims, as well as enduring social stigma, many incidents still go unreported. As with other cybercrimes, this means the actual impact of romance scams is likely to be even higher than the official figures suggest. As the increasing volume, scale, and complexity of romance scams is set to create a growing number of investigative challenges for law enforcement agencies across Africa, the provision of adequate training and forensics capabilities will be essential.

OPERATION CONTENDER: STRIKING BACK AGAINST ROMANCE SCAMS

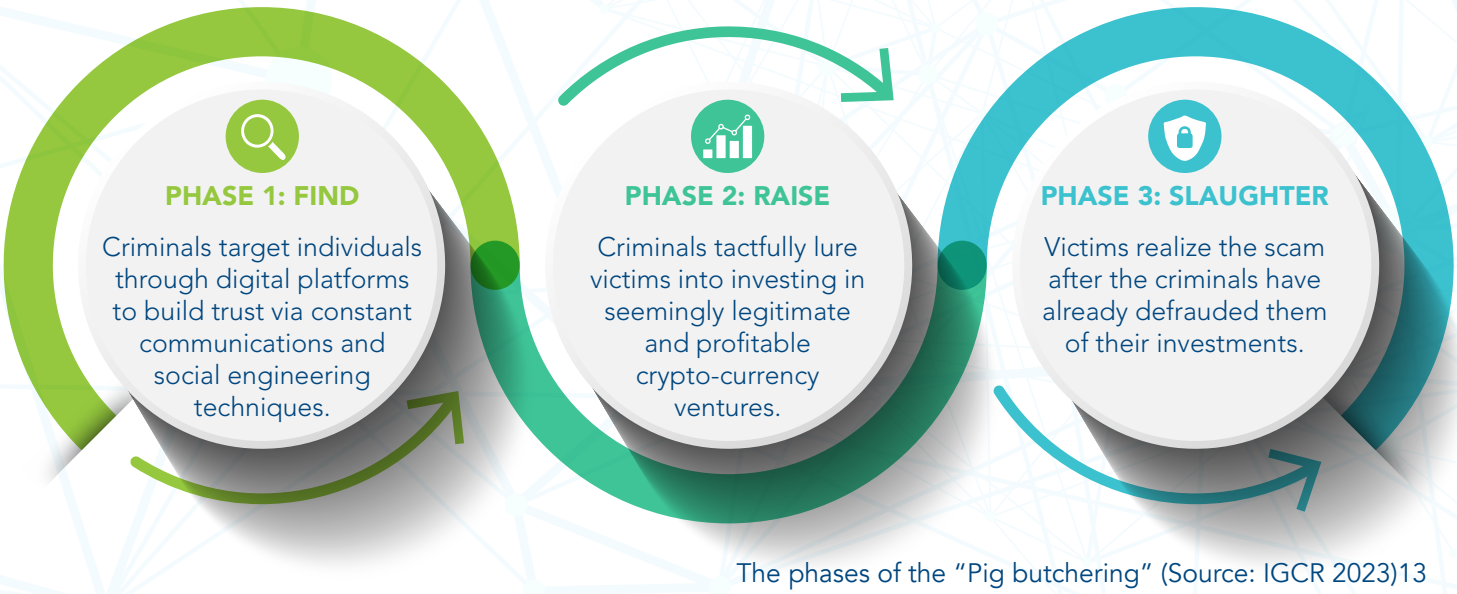
During Operation Contender, INTERPOL worked with cybercrime units in Benin, Côte d'Ivoire, Nigeria, Finland, and Switzerland, as well as with several private partners, to disrupt organized cybercriminal networks involved in romance scams. The operation resulted in the arrest of three suspects in Côte d'Ivoire and Benin in early 2023, as well as the seizure of digital and mobile devices used for malicious purposes.

24 Avast (2023): https://decoded.avast.io/threatintel/lovegpt-how-single-ladies-looking-for-your-data-upped-their-game-with-chatgpt/
25 Reuters (2023): https://www.reuters.com/world/us/fbi-says-artificial-intelligence-being-used-sextortion-harassment-2023-06-07/
26 US FTC (2022): https://www.ftc.gov/news-events/blogs/data-spotlight/2022/02/reports-romance-scams-hit-record-highs-2021

Pig butchering, a rapidly emerging hybrid threat

As in other parts of the world, in 2023 INTERPOL member countries identified so-called "pig butchering" as one of the fastest emerging forms of online scams. Despite being a relatively new phenomenon, incidents were reported by more than a third of African member countries in 2023 – especially in West and Southern Africa.[27] According to internal data, pig butchering is having a major financial impact across the continent, in line with global patterns. Research suggests that the median sum transferred into fraudsters' cryptocurrency wallets is somewhere between USD 10,000 and 100,000, while worldwide losses attributed to pig-butchering and related cryptocurrency scams are estimated to have nearly doubled since 2022, to exceed USD 3.3 billion in 2023.[28]

As explained in the INTERPOL Global Financial Fraud Assessment 2024, pig butchering is a hybrid scam, combining elements of cryptocurrency investment fraud and romance scams. These schemes typically follow three main steps. First, criminals contact individuals through digital platforms, including social media platforms such as Facebook and Instagram, messaging services such as SMS, WhatsApp, Telegram, and Signal, or dating apps. They may claim to have received the victim's contact details through a referral or a mutual friend. To better lure their targets in, criminals often use a fake account, impersonating an attractive person with photos stolen from other individuals or generated using AI, in a modus operandi similar to that of romance scams. In the next step, they "fatten up" the victim by gaining their trust and gradually portraying themselves as investment experts. The criminals' tactic is to bait victims into investing in seemingly legitimate and profitable cryptocurrency ventures. However, as soon as the victim has transferred substantial amounts, or they begin to realize they are being scammed, the criminals cash out and disappear. To make tracing and recovering assets as difficult as possible, criminals typically seek to convert their victims' funds using digital payments or cryptocurrency platforms. During this final step, sometimes known as "slaughtering", perpetrators stop responding to messages or calls from the victim, which leads to financial and emotional harm.



The phases of the "Pig butchering" (Source: IGCR 2023)13

27 INTERPOL Global Financial Fraud Assessment 2024: https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2024/INTERPOL-led-operation-targets-growing-cyber-threats

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

In the cases of pig-butchering scams reported by African member countries, there was a general distinction between the initial methods of contact used by cybercriminals, split between social media platforms (such as Facebook and Instagram) and mobile messaging services (such as WhatsApp, Telegram, Signal, and SMS), including the use of group chats. Individuals targeted via social media platforms often experienced more aggressive social engineering techniques compared to the broader, less personalized approach observed on messaging platforms. Moreover, member countries highlighted the simplicity of pig butchering schemes and the widespread availability of phishing kits as major factors in the steady rise of cases throughout 2023.

This surge has led law enforcement in African member countries to identify serious obstacles to their investigations. These include barriers to acquiring data from service providers, and the large numbers of devices requiring forensic analysis. Additionally, the growth of pig butchering scams, in line with other cybercrimes, exacerbates jurisdictional issues. In response to these challenges, countries have already taken positive steps. A joint task force to combat pig butchering was initiated in southern Africa, with some notable successes. Furthermore, INTERPOL has been running a series of training sessions and facilitating meetings with relevant service providers on the continent in order to strengthen regional action against pig butchering.

Smartphones, a growing target for scammers in Africa

African member countries experienced an increasing number of scams targeting smartphone users in 2023. This reflects both the steady growth of the mobile penetration rate across Africa, as well as the rapid rise in the use of mobile banking services across the continent.[29] The most common smartphone scams detected by African law enforcement agencies typically belong to two main, often interrelated, categories: **mobile phishing attacks and banking trojans.**

The first type is an expansion of the phishing attacks discussed previously, in which criminals attempt to redirect victims to fraudulent sites such as fake banking websites via their mobile phone web browsers. The second type of smartphone scam frequently observed by African law enforcement involves the use of malware-like banking trojans. These are malicious programs designed to steal financial and other sensitive information such as online banking credentials, account numbers, and credit card data from infected machines. Banking trojans may be deployed through various attack vectors, including phishing emails, drive-by download attacks, or the downloading of cracked software, including fake mobile apps. Like other trojan horse malware, they typically disguise themselves as legitimate software to gain access to a machine, making them difficult to detect. In addition, they act as remote access trojans (RATs), enabling the perpetrator to remotely control the infected system and carry out further attacks, including ransomware.[30] Once installed, the malware collects and exfiltrates sensitive data through a variety of methods, such as keystroke logging, screen capturing, dumping cached credentials, and searching the system for saved passwords. Threat actors can then use this information to steal money directly from their victims, for example by remotely accessing their banking apps, or to commit further crimes, such as identity theft and other types of scams.

Banking trojans and associated online scams pose a significant challenge for the African continent, with a high number of cases being reported, especially in southern Africa. Considering citizens' increasing reliance on smartphones and mobile payments, all African member countries have expressed growing concerns about the potential socio-economic impact of smartphone-related scams. In addition, banking trojans are placing greater pressure on digital forensics capabilities and capacity across the region. In order to address this challenge, several countries have been making significant investments in forensic tools which have enabled them to report the forensic analysis of hundreds of devices over the review period. Many African states are also taking important steps to better prevent, investigate, and disrupt mobile banking trojans. This includes initiating partnerships with banks to seize and recover the proceeds of crime, as well as launching awareness-raising campaigns to inform citizens about the risks associated with the use of online banking.

29 See for example Statista (2023): https://www.statista.com/statistics/1133777/sub-saharan-africa-smartphone-subscriptions/

30 Checkpoint (2023): https://www.checkpoint.com/cyber-hub/cyber-security/what-is-trojan/what-is-a-banking-trojan/

BUSINESS EMAIL COMPROMISE

Key Points:

- Business email compromise combines both technical components and sophisticated social engineering methods, and is a growing threat to organizations and individuals across Africa, especially those in the financial sector.
- The surge of this hybrid threat is fuelled by developments in the technical domain, including the growth of Cybercrime-as-a-Service and the emerging impact of artificial intelligence.
- Despite major law enforcement successes, the continued operation of BEC actors in and from the African continent poses important investigative challenges.

Business email compromise: a growing threat across Africa

Within the broad category of online scams, INTERPOL member countries in Africa identified business email compromise (BEC) as one of the most significant threats. BEC is a type of cybercrime that involves the use of email fraud to attack organizations and individuals. It generally involves cybercriminals compromising legitimate business or personal email accounts through social engineering and/or computer intrusion and attempting to trick organizations and individuals into making unauthorized transfers of funds or divulging confidential information.

Across Africa, cybercriminal activity around business email compromise is increasing, in terms of both the volume of the attacks and their impact. This development reflects global trends: between April 2022 and April 2023, Microsoft detected and investigated 35 million BEC attempts, which corresponds to about 156,000 attempted attacks every day.[31] Meanwhile, the global financial impact of BEC is reported to have grown since 2013 to exceed USD 50 billion in 2023.[32] Apart from the direct financial losses, BEC can result in long-term damage, including the loss of confidential data in cases where sensitive correspondence or intellectual property have been disclosed, and can also have a psychological impact on victims.

In 2023, businesses were the most common target for BEC attacks in INTERPOL's African member countries. Companies which conduct business abroad carry out frequent financial transactions, and which have less-well-developed security controls, appear to be particularly at risk. However, targets can range from small and medium-sized enterprises to large corporations. **Finance was the most commonly impacted sector across African member countries, but no sector or industry is impervious to BEC.** Aside from banks and microfinance companies, attacks were frequently recorded against companies involved in import and export, oil and gas, pharmaceuticals, transport, and e-commerce. Likewise, there were increasing number of attacks on government institutions, especially parastatals, as well as the voluntary sector and individuals across the African continent.

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

Common BEC modus operandi across African countries

In terms of modus operandi, **phishing emails were identified as the most common attack vector for business email compromise in nearly 80 per cent of African member countries in 2023.** Compared to other forms of phishing, emails used in BEC cases tend to be more difficult to detect because they do not contain malicious links and are not mass-emailed – and are therefore less likely to be flagged as spam. Member countries reported that, in combination with phishing emails, perpetrators are exploiting various media as part of BEC schemes, including text messages, phone calls, and virtual meetings. For instance, some threat actors have joined virtual meetings as dial-in users to steal confidential corporate information. Social media and instant messaging services are also increasingly being abused to carry out reconnaissance and/or contact victims.[33]

Most of the cases reported by INTERPOL member countries can be classified into five categories or schemes:

1. **Data theft:** threat actors compromise the email and credentials of role-specific employees, such as human resources and bookkeeping staff, to obtain the personally identifiable information or tax statements of other employees or executives. The data obtained is then used to launch further BEC attacks. This last scheme was reported to be on the rise, with criminals using the exfiltrated data to apply double and even triple extortion tactics against their victims.
2. **Account compromise / system breach:** another BEC scheme often reported by member countries features threat actors hacking the email of an employee or executive and then using the compromised account to send requests for invoice payments to multiple vendors. For instance, several African countries have reported so-called man-in-the-middle attacks, in which perpetrators secretly intercept and relay messages between two parties.
3. **CEO impersonation:** also known as the business executive scam or masquerading, this scheme involves criminals seeking to impersonate high-level executives to initiate a payment to an account they control. This version of BEC often involves some level of research and reconnaissance by threat actors against the targeted organization.
4. **Government, law enforcement or attorney impersonation:** in this version of BEC, attackers contact their targets claiming to be a figure of authority, such as a government official or lawyer, who is handling confidential and time-sensitive matters. In 2023, several countries also reported cases involving the impersonation of law enforcement officials or those from international organizations, including INTERPOL. Criminals then use various methods to pressure their victim into transferring funds quickly or secretly.
5. **Bogus invoice scheme:** criminals try to exploit established relationships between their target and its suppliers. Posing as a supplier, they send a forged invoice and ask their victim to transfer funds to a fraudulent account.

OPERATION HARRIER: APPREHENDING ORGANIZED CRIME MEMBERS INVOLVED IN BEC

In response to the significant and enduring risks posed by BEC, including the financial, emotional, and psychological ramifications outlined in this threat assessment, a strategic partnership was formed between INTERPOL and the World Economic Forum's (WEF) Atlas Group. This collaboration was established with the dual objectives of enhancing the comprehension of the global cyber threat landscape and facilitating the exchange of intelligence to mitigate the worldwide impact of cybercrime.

INTERPOL, working with contributors to the World Economic Forum's (WEF) Cybercrime Atlas initiative, was able to identify the perpetrator of a sophisticated multi-million-dollar BEC scheme using the bogus invoice modus operandi. Through extensive intelligence sharing, the individual in question was linked to a complex network of criminality associated with Black Axe organized crime group, based in West Africa. This information was passed on to the relevant African member countries, resulting in the criminal being apprehended.

While the initial attack vectors and general schemes of business email compromise are well established, evolving social engineering techniques, the growing availability of crimeware-as-a-service, and the emerging impact of artificial intelligence are driving a surge in BEC activity.

33 Africa Center (2023) https://africacenter.org/spotlight/africa-evolving-cyber-threats/

Evolving social engineering techniques

Like many online scams, BEC attacks rely heavily on exploiting human vulnerabilities. With this in mind, it is alarming that many African member countries have reported an uptick in sophisticated social engineering techniques. For example, BEC threat actors are spending considerable time researching and monitoring potential targets to strengthen their initial lure or attack vector. They harness information available publicly or obtained from previous data leaks to design messages that are as personal and as authentic as possible. In some cases, criminals have gone so far as to replicate their target's writing style or to reference upcoming events their victims have been invited to. **Reflecting these growing levels of sophistication, more than half of INTERPOL member countries in Africa observed a high or very high success rate for phishing emails used in BEC attacks.**

Many BEC threat actors also appear to be expending more time on moving laterally through their target's system after gaining initial access. They may use various methods to achieve persistence, such as adding a secondary authenticator app to the compromised account to bypass multi-factor authentication.[34] The attackers will then search through their victim's email correspondence or web-based file sharing applications. The information obtained is used to craft more convincing schemes. For instance, by analysing a specific email thread, some threat actors have managed to use fake domain names to create multiple fraudulent email addresses. These addresses are used to create multiple personas and simulate a company, tricking their victim into believing that they are communicating with the various recipients of the original thread.

In a related development, INTERPOL has detected a growing trend towards data exfiltration being used in BEC campaigns. After gaining initial access, threat actors exfiltrate data not only to design more effective attacks, but also to further extort their victims. They threaten to leak sensitive information (double extortion) or the data of associated third parties (triple extortion). The increasing use of data exfiltration strategies is another reminder of the increasing sophistication of the BEC landscape.

Common red flags of BEC:

01 Unexplained urgency

02 Last-minute changes to wire instructions or recipient account information

03 Last-minute changes to established communication platforms or email account addresses

04 Last-minute changes to established communication platforms or email account addresses

05 Communications only in email and refusal to communicate via telephone or online voice or video platforms

06 Requests for advanced payment of services when not previously required

34 See for example: https://www.kroll.com/en/insights/publications/cyber/mfa-bypass-leads-to-account-compromise

Cybercrime-as-a-service operations on the rise

Another indication of the growing sophistication, organization, and specialization of the BEC ecosystem is the rapid development of Cybercrime-as-a-Service (CaaS). Reflecting this development, Microsoft's Digital Crimes Unit detected a 38 per cent increase in CaaS targeting business email accounts between 2019 and 2022.[35] A plethora of phishing kits are now available, offering ready-made templates and scripts which enable BEC threat actors to scale up their activities quickly and easily. For instance, in 2023 INTERPOL Gateway partner Group-IB reported on the operations of W3LL, an offender who provided custom phishing kits to at least 500 BEC threat actors.[36] With an estimated turnover of USD 500,000, W3LL's crimeware-as-a-service provided users with highly customized tools for carrying out BEC attacks, which enabled them, amongst other things, to bypass multi-factor authentication. Between October 2022 and July 2023, W3LL's phishing kit is estimated to have been used to target over 56,000 corporate Microsoft 365 accounts.

Moreover, cybersecurity researchers have identified a growing number of illicit platforms offering end-to-end services, including templates, hosting and other automated services, for launching large-scale BEC campaigns. An example of such a platform is BulletProftLink, which enables criminals not only to obtain their victim's credentials and Internet protocol (IP) address, but also to leverage **residential IP addresses** to make their attack campaigns appear locally generated. In turn, this enables them to effectively circumvent "impossible travel" alerts, a detection method commonly used to identify and block suspicious activity.[37]

The emerging impact of artificial intelligence

The trends towards more sophisticated social engineering tactics and Cybercrime-as-a-Service are even more concerning given the rapid development of artificial intelligence (AI) and the rise of synthetic media. The year 2023 was marked by ground-breaking advances in AI technology, with large language models (LLM) such as ChatGPT capturing the world's attention. Unfortunately, despite many positive use cases, AI also has the potential to be misused by criminals, including those engaged in business email compromise schemes. In recognition of this emerging threat, INTERPOL has issued a purple notice to warn member countries about the risk of AI and deep fake technology being used by criminals to lend credibility to scams, for instance to hide their identities and to pretend to be family members, friends, or love interests.[38]

At a basic level, generative AI can enable BEC threat actors to easily create fraudulent emails or spoof authentication request messages – potentially on an industrial scale – while evading basic detection parameters such as spelling and grammar mistakes. When fed with the right data, LLMs can even enable threat actors to mimic the style and linguistic patterns of specific organizations and individuals, assisting them in crafting more personalized and convincing emails to lure and deceive victims.[39] Additionally, rapid advances in deepfake technology are already being exploited by cybercriminals to trick their targets, for example by replicating a person's likeness and voice during phone or video calls.[40] Given the speed with which AI technology is evolving, as well as its significant potential to scale up the volume of BEC attacks and to enhance their level of sophistication and authenticity, member countries will have to closely monitor future developments.

Disrupting BEC actors operating from Africa

In 2023, INTERPOL's African member countries continued to take tough operational action to disrupt BEC actors working from the region. During Operation Nervone, INTERPOL, AFRIPOL, Group-IB, and the Côte d'Ivoire Direction de l'Information et des Traces Technologiques (DITT) succeeded in arresting the senior member of the group known as OPERA1ER. Also known under the aliases NXM, DESKTOP Group, and Common Raven, this highly-organized criminal organization is believed to have used large-scale business email compromise campaigns to steal up to USD 35 million across 15 countries in Africa, Asia, and Latin America.[41] Meanwhile, as part of Operation Jackal, INTERPOL coordinated and supported police forces, financial crime units, and cybercrime agencies in a crackdown on West African organized crime groups, including Black Axe, a violent mafia-style gang renowned for committing BEC and other online scams.[42] Operations such as these showcase African member countries' commitment to protecting their communities from the impact of BEC.

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

36 Group-IB (2023): https://www.group-ib.com/media-center/press-releases/w3ll-phishing-report/

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

38 INTERPOL (2023): https://www.interpol.int/en/News-and-Events/News/2023/USD-300-million-seized-and-3-500-suspects-arrested-in-international-financial-crime-operation

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

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

41 INTERPOL (2023): https://www.interpol.int/en/News-and-Events/News/2023/Suspected-key-figure-of-notorious-cybercrime-group-arrested-in-joint-operation

42 INTERPOL (2023) https://www.interpol.int/en/News-and-Events/News/2023/Closing-ranks-on-West-African-organized-crime-more-than-EUR-2-million-seized-in-Operation-Jackal

OPERATION NERVONE: APPREHENDING A KEY FIGURE OF AN ORGANIZED CYBERCRIMINAL GROUP

Over the last four years, the cybercriminal group known as OPERA1ER orchestrated large-scale BEC schemes, phishing campaigns, and malware attacks against financial and mobile banking services worldwide, amassing up to USD 35 million. In early June 2023, INTERPOL, together with AFRIPOL, Côte d'Ivoire, the United States, and private partners including Orange, Group-IB, Booz Allen Hamilton, and DarkLabs, identified and arrested individuals suspected of being key senior members of the group. The success of this operation, dubbed "Operation Nervone", was only possible due to diligent intelligence sharing and close cooperation over the course of several years.

Alongside these operational successes, African member countries have also strengthened prevention and mitigation efforts. **Over 60 per cent of the member countries surveyed deployed campaigns in 2023 to warn individuals and organizations of the risk of BEC attacks.** These public awareness campaigns were launched via various media platforms, including radio, television, government websites, and social networking sites, with the aim of improving cyber hygiene and preventing further exploitation of the human element by cybercriminals.

Despite these positive steps, there are still major obstacles to further reducing the impact of BEC in Africa. **A substantial number of BEC actors are still located in Africa, especially Western Africa, but also increasingly the southern parts of the continent** - with some studies indicating that 11 countries account for the largest part of BEC activity on the continent.[43] Some of the criminal groups involved have turned into multi-million-dollar enterprises.[44] They may be underpinned by sophisticated organizational structures, featuring a number of specialized functional roles ranging from infrastructure administrators to email operators and money mules. In addition, partly in response to law enforcement successes, BEC operations are increasingly adopting obfuscation methods to hide their criminal infrastructure and are becoming more geographically dispersed, which exacerbates the investigative challenges facing law enforcement.

CYBER RESILIENCE AND LAW ENFORCEMENT CAPABILITIES ACROSS THE AFRICAN CONTINENT

To create a comprehensive picture of the current cyber threat landscape, it is important not only to consider the most pressing cybercrime threats, but also to assess existing capabilities for countering them. Accordingly, this section examines four areas of African cyber resilience, using data provided by member countries: **legislative frameworks, law enforcement capabilities, partnerships, and engagement with the public.**

1. African legislative frameworks against cybercrime expanding

Effective legislative frameworks are a fundamental component of cyber resilience and a key parameter for law enforcement activities. In this regard, it is encouraging to observe the development of laws aimed at combating cybercrime across Africa. In 2023, several African countries implemented new laws, amended existing statutes, or activated recently introduced legislation aimed at combating cybercrime.[45] Some noteworthy examples include Uganda's Regulation on the Interception of Communications Regulations; Cameroon's Law to institute the charter on child online protection; Gabon's Law on the protection of personal data; Burkina Faso's stipulations for ICT operators in data preservation; and Botswana's Act on virtual assets. An additional six countries indicated that they are in the process of enacting new legislation. These significant efforts are in addition to the expansion of existing regional and international instruments, **including the African Union (AU) Convention on Cyber Security and Personal Data Protection, also known as the Malabo Convention;** the AU Digital Transformation Strategy for Africa (2020-2030); and the Budapest Convention on Cybercrime and its additional Protocols.

43 Agari (2023) ag-acid-geography-of-bec-gd.pdf (fortra.com)

44 Agari (2023): https://www.agari.com/resources/videos/scattered-canary-evolution-business-email-compromise-enterprise

45 Lexology (2023): https://www.lexology.com/library/detail.aspx?g=baef72ee-10bd-4eb9-a614-a990c236bb45

INTERPOL actively supports member countries' efforts to transform legislation in order to combat cybercrime through various initiatives. In 2023, INTERPOL participated in the implementation of the Global Action on Cybercrime Extended (GLACY+, currently extended as GLACY-e) project. This initiative, a collaborative effort by the European Union and the Council of Europe, aims to strengthen the cyber capabilities of countries across Africa, Asia-Pacific, Latin America, and the Caribbean region within the scope of the Budapest Convention. A principal ambition of GLACY+ is the advancement of consistent cybercrime legislation, policies, and strategies. INTERPOL plays a critical role in this endeavour in terms of enhancing the capacities and operational skills of police forces in participating countries. This effort is directed towards improving their proficiency in investigating cybercrimes and bolstering international police cooperation through a series of activities.

At the same time, throughout 2023 INTERPOL has been proactively engaging with key international cyber policy and legislative processes, most notably the United Nations Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (AHC).[46] The AHC aims to establish a new global treaty to combat cyber threats, which, once ratified, will provide enhanced legislative tools for states in Africa and beyond. Through its contributions, INTERPOL has sought to ensure that the interests and needs of its extensive membership are accurately represented in the forthcoming Convention.

Finally, since the establishment of the INTERPOL Cybercrime Programme, the Organization has been developing essential instruments to support member countries in the fight against cybercrime. These include global resolutions (most recently, the 2021 Resolution on Tackling global cybercrime threats through INTERPOL channels[47]), the INTERPOL Global Cybercrime Strategy for 2022-2025, and, specific to Africa, the 2022 regional recommendation.[48] This calls on African member countries to fully leverage INTERPOL's resources to enhance operational collaboration, share intelligence, and strengthen capabilities.

2. Growing law enforcement cyber capabilities

The data received by INTERPOL indicates that the human resources allocated to combat cybercrime are still insufficient, although countries are taking proactive steps to improve the situation. For instance, in 2023, almost half of law enforcement agencies in INTERPOL member countries reported an increase in the numbers of personnel assigned to combat cybercrime. In addition, at least four countries highlighted the fact that they have recently established a cybercrime unit or are in the process of doing so. Meanwhile, over the course of 2023, more than 70 per cent of law enforcement agencies in African member countries reported having either conducted or participated in cyber-training activities: a total of 32 countries and over 130 training initiatives. This highlights the efforts being made to invest in staff and skills in order to better combat cyber threats, underscoring African member countries' commitment to bolstering cyber resilience across the continent.

In line with Objective 3 of the INTERPOL Global Cybercrime Strategy for 2022-2025, the Organization aims to support the development of its member countries' strategies and capabilities for combating cybercrime. Accordingly, INTERPOL contributes to several capacity-building initiatives on the African continent, including AFJOC, GLACY-e, and the ISPA Programme. In 2023, these efforts led to the delivery of eight training sessions and workshops focused on cyber investigation techniques, with a particular emphasis on virtual assets. Additionally, 72 specialized tools and licences which are crucial for cybercrime investigations were acquired and distributed across 22 member countries, accompanied by bespoke training on how to apply them. INTERPOL also provides two specialized platforms to ensure a seamless global connection between member countries' law enforcement agencies. These are the Cybercrime Knowledge Exchange (CKE) for non-operational information sharing, and the Cybercrime Collaborative Platform – Operation (CCP – Operation) for the secure and restricted exchange of operational intelligence. These are effective tools in coordinating an international response to cybercrime, and offer a sophisticated mechanism for collaborative engagement.

46 For more information about AHC: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

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

48 INTERPOL (2022): https://www.interpol.int/en/News-and-Events/News/2022/INTERPOL-African-conference-ends-with-call-for-greater-data-exchange

3. Coordination challenges across the cyber ecosystem

Establishing and strengthening open, inclusive, and diverse partnerships is key to fostering effective cooperation in the fight against cybercrime. However, African member countries reported challenges in fostering collaboration between law enforcement and the relevant stakeholders in the cyber ecosystem. Working with service providers, especially when located overseas, appears to remain a major difficulty for cybercrime investigations. Meanwhile, it was reported that public-private cooperation is often conducted on an ad hoc basis rather than through established, standardized frameworks.

With all of these challenges to establishing formal public-private partnerships and platforms to aid businesses in combating cybercrime, INTERPOL's strategic initiatives can play a crucial role. INTERPOL's dedicated initiative, "**Gateway**", serves as a cornerstone for conducting in-depth cybercrime analysis, using a broad spectrum of information sources to pinpoint threat actors, identify victims, and flag compromised infrastructures for necessary interventions. Grounded in the INTERPOL Constitution and its guiding principles of sovereignty, respect for human rights, neutrality, and active cooperation, the Gateway framework sets out a legal framework for information exchange with private entities through signed data-sharing agreements. Furthermore, INTERPOL is also involved in key initiatives to foster multi-stakeholder cooperation. Amongst them is the **World Economic Forum's Cybercrime Atlas,**[49] which brings together law enforcement and the public and private sector to gain new insight into the cybercriminal ecosystem. Cooperation between INTERPOL and the Cybercrime Atlas community has also led to impressive analytics-led operational outcomes, including the profiling and arrest of members of a prominent threat group known as 'Silver Terrier,' predominantly operating out of West Africa.

4. Raising public awareness and cyber hygiene

In response to the rise in social engineering techniques being used to commit cybercrimes, countries have taken important steps to enhance public awareness and cyber hygiene. It is encouraging that approximately 80% of the African member countries surveyed have initiated public awareness campaigns aimed at preventing cybercrime. Although predominantly conducted online, these campaigns occasionally occurred in physical settings, primarily within educational institutions, thereby focusing on young people and their support networks, including parents, families, and educators. These campaigns were rolled out via a variety of online platforms, including television, radio, web news, and social media channels, with Facebook being particularly prominent. A relevant feature of these efforts is the collaboration between law enforcement agencies and entities from both the public and private sectors. The primary areas of focus for these campaigns included the promotion of best practices for cyber hygiene and general awareness of online scams. These national efforts are in line with the African Union Digital Education Strategy[50] that focuses mainly on accelerating the adoption of digital technologies for teaching, learning, research, assessment, and administration.

In a complementary global effort, INTERPOL has launched several awareness-raising campaigns, such as #YouMayBeNext, #JustOneClick, and #OnlineCrimeIsRealCrime, to bolster community vigilance to combat the array of cybercriminals intent on exploiting vulnerabilities, stealing data, committing online fraud, or causing disruption in the digital realm. The #YouMayBeNext campaign in particular saw remarkable global participation: it was supported by 79 member countries, as well as private partners, various international organizations, private entities, and non-governmental organizations, achieving significant outreach. Looking ahead to 2024, INTERPOL plans to continue this momentum with a new campaign focused on the threat of malware.

49 For more information about WEF Cybercrime Atlas: https://initiatives.weforum.org/cybercrime-atlas/home

50 African Union Education Strategy (2022): https://au.int/en/documents/20221125/digital-education-strategyand-implementation-plan

SUPPORTING AFRICAN CYBER RESILIENCE: INTERPOL AFRICA CYBER SURGE OPERATION SURGE II

INTERPOL supports African cyber resilience through partnerships, platforms, and capability-development activities.

A prime illustration of this is Operation Africa Cyber Surge II:

- INTERPOL Gateway and the World Economic Forum's Cybercrime Atlas partners provided essential information that was crucial for the operation's success
- The use of CCP – Operations by participating countries for information exchange and operational coordination
- A series of pre-operation training sessions aimed at enhancing the skills of investigators in various domains of cybercrime investigation

WAY FORWARD

Based on the results of the assessment, including the analysis of the fastest growing cyber threats in Africa and the related efforts to counter them, this section presents recommendations that aim to reduce the impact and harm of cybercrime on the continent and worldwide.

1. Introducing or strengthening robust and harmonized cybersecurity instruments
INTERPOL recommends that African member countries should continue to establish and/or reinforce robust and harmonized national cybersecurity instruments aimed at defending against and responding to cybercrimes. These tools include strategies, policies, and legal frameworks whose objective is to empower countries to fight cyber threats effectively and to mitigate the related risks. This includes, but is not limited to, removing legal obstacles for investigators.

2. Investing in law enforcement cyber capabilities: people, processes, technology
In an acknowledgment of the importance of strengthening cybersecurity resources on the continent, **INTERPOL is encouraging greater investment in and long-term support for African law enforcement agencies from internal and external stakeholders.** Increasingly sophisticated cyber-criminality requires more specialized units, skilled officers, tools, and platforms. Accordingly, countries are encouraged to actively engage with existing capability-development activities offered by regional and international entities, such as those provided by the INTERPOL Africa Cybercrime Operations Desk (AFJOC).

3. Establishing synergies across the cybersecurity ecosystem
Given the transnational nature of cybercrime, **INTERPOL strongly recommends that African member countries should integrate relevant stakeholders' efforts in the fight against cybercrime.** Cooperation with relevant stakeholders such as the private sector and cybersecurity agencies plays a crucial role in enhancing incident response, access to data, threat intelligence sharing, the takedown of malicious infrastructure, and cybersecurity awareness. In addition, countries are encouraged to establish and make use of national Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs). To help to promote closer collaboration between law enforcement and existing CERTs / CSIRTs, INTERPOL and the Forum of Incident Response and Security Teams (FIRST) have established a Special Interest Group (SIG).

4. Strengthening digital education and awareness
To counter increasingly sophisticated social engineering techniques, renewed attention must be focused on the human factor, and therefore, on prevention. **INTERPOL encourages African member countries to continue to focus on improving cyber hygiene, with support from both the public and private sectors.** This strategy includes expanding public awareness through governmental initiatives and encouraging individuals and organizations to implement stronger email security, use multi-factor authentication (MFA), conduct thorough employee training, and adopt secure payment technology.
Similarly, citizens should be encouraged to report to national law enforcement authorities whenever they become victims of cybercrime. **To that end, it is recommended that member countries streamline the reporting and recording process where possible, for instance through the use of online webpages and platforms.** Such proactive measures will ensure not only a more secure digital environment but also a more comprehensive understanding of the African cyber landscape.

5. Broadening and deepening international and regional cooperation
Effective regional and global collaboration are essential to addressing the geographical spread of organized criminal groups and their victims. **INTERPOL urges member countries to continue to broaden and deepen their cooperation in order to offer a unified front against the global threat of cybercrime.** This includes strengthening information sharing and carrying out intelligence-led, coordinated action through the INTERPOL Africa Cybercrime Operation Desk.

INTERPOL will continue to support its African member countries in further reducing the global impact of and harm caused by cybercrime, and protecting communities for a safer world.

AFRICA JOINT OPERATIONAL FRAMEWORK

The INTERPOL Africa Cybercrime Operations Desk has developed a Joint Operational Framework to promote a coherent and methodological approach in order to improve proactive coordinated operations against cybercrime on the continent. This framework consists of four phases.

Phase I – Collection and Analysis
The first phase focuses on in-depth analysis of information pertaining to the prevalent cyberthreats, malicious infrastructures, and threat actors operating within/against the community in the African region. Using intelligence from law enforcement communities, research conducted by INTERPOL's Cybercrime Intelligence Unit, and the extensive data-sharing agreements with INTERPOL's Project Gateway partners, the Africa Cybercrime Operations Desk will publish the African Cyberthreat Assessment Report to help law enforcement communities in Africa gain a better understanding of the cyberthreat landscape on the continent.

Phase II – Priorities and Strategy
The African Cyberthreat Assessment Report, published during Phase I of the cycle, will serve as a reference document to help African member countries to develop or update their investigation strategies and investigative approach, and steer regional prioritization of operational efforts undertaken jointly with INTERPOL for the year ahead. In recognition of the diversity of the African region and the unique challenges facing each country, the African Cybercrime Operations Desk will involve each country's Head of Cybercrime during this phase (with the authorization of the relevant NCB) in order to explore opportunities for both intra-and inter-regional collaboration. By the end of this phase, a regional roadmap, based on an agreed joint strategy with clear operational outcomes for the year, will be ready for publication.

Phase III – Operations
The African Cybercrime Operations Desk will develop Standard Tactical Plans (STPs) to operationalize the strategy agreed upon in Phase II. STPs provide a clear set of objectives, roles, and responsibilities, and an operational concept for dealing with specific cyberthreats. Each STP typically includes detailed plans on the following: (1) planning and analysis; (2) organization; (3) tactics; and (4) evaluation. STPs are then shared with participating countries for endorsement.

The participating cybercrime units nominated by the NCBs will then commit to the action outlined in the STPs and will provide full support in order to achieve the agreed operational aims and objectives. Following endorsement, the operations will be coordinated by the Africa Cybercrime Operations Desk and carried out by designated investigators in accordance with the timeline specified in the STPs. Data relating to the operations are received by INTERPOL via its secure I-24/7 communications system, or via its Cybercrime Collaborative Platform - Operation, for analysis.

Once they have received the operational information, nominated Points of Contact (PoCs) from each member country will liaise with the Africa Cybercrime Operations Desk for information exchange as per the designated objectives and timeframe of the operation. The initiating member country will maintain the operational lead throughout the operation.

The facilitation of the preservation and disclosure of Internet records (basic subscriber information, transmission data, content, etc.) will be on a voluntary basis and will be encouraged for all cybercrime operations, given the volatility of electronic evidence. Member countries are strongly encouraged, within the limits of their respective laws and policies, to share updates on investigations and specific intelligence that may help other members in their own investigations. As far as possible, the PoCs shall facilitate the sharing of information with other national agencies such as Computer Emergency Response Teams (CERT) and central banks depending on the needs of each operation.

Phase IV – Evaluation
During Phase IV, an After-Action-Review (AAR) will be conducted to identify the lessons learnt from the operations. The Africa Cybercrime Operations Desk will recommend adjustments to future joint operations based on reviews and new information arising from the operations. The intelligence collected during Phase III will also be evaluated to enhance regional understanding of the prevalent cyberthreats and inform the following African Cyberthreat Assessment Report.

NOTES ON The methodology used for the 2024 INTERPOL Africa Cyberthreat Assessment Report

The 2024 INTERPOL Africa Cyberthreat Assessment Report builds on previous editions to offer an in-depth analysis of the cyber threat landscape as experienced by African member countries. This edition presents a thorough analysis, focusing on key threats such as ransomware, business email compromise, and other forms of online scams. More than just identifying these pressing issues, the report also investigates the ongoing national initiatives aimed at bolstering cyber resilience across the continent. It concludes with actionable recommendations aimed at guiding future cybersecurity efforts on the continent.

The assessment draws mainly on intelligence and operational data resulting from INTERPOL's various activities in Africa. Additional information comes from an INTERPOL-led survey, consisting of 40 quantitative and qualitative questions on the topic of prevention, detection, investigation, and disruption. A total of 46 member countries contributed information, representing a response rate of over eighty per cent.

- Algeria
- Angola
- Benin
- Botswana
- Burkina Faso
- Burundi
- Cameroon
- Cabo Verde
- Comoros
- Congo
- Côte d'Ivoire
- Democratic Republic of the Congo
- Djibouti
- Equatorial Guinea
- Eritrea
- Eswatini
- Ethiopia
- Gabon
- Gambia
- Ghana
- Guinea
- Guinea-Bissau
- Kenya
- Lesotho
- Liberia
- Madagascar
- Malawi
- Mali
- Mauritania
- Mauritius
- Mozambique
- Namibia
- Niger
- Rwanda
- São Tomé And Príncipe
- Senegal
- Seychelles
- Sierra Leone
- Somalia
- South Africa
- South Sudan
- Tanzania
- Togo
- Uganda
- Zambia
- Zimbabwe

Finally, this dataset was complemented by strategic consultations with INTERPOL Gateway partners, such as Bi.Zone, Fortinet, Group-IB, Kaspersky Lab, and Trend Micro.

ABOUT INTERPOL

INTERPOL is the world's largest international police organization. Its role is to assist law enforcement agencies in the Organization's 196 member countries to combat all forms of transnational crime. It works to help police across the world meet the growing challenges of crime in the 21st century by providing a high-tech infrastructure of technical and operational support. The Organization's services include targeted training, expert investigative support, specialized databases, and secure police communications channels.

INTERPOL'S VISION: "CONNECTING POLICE FOR A SAFER WORLD"

INTERPOL's vision is that of a world where each and every law enforcement professional will be able to use the Organization to securely communicate, share, and access vital police information whenever and wherever needed, to ensure the safety of the world's citizens. INTERPOL constantly provides and promotes innovative and cutting-edge solutions to global challenges in policing and security.

ABOUT THE INTERPOL CYBERCRIME PROGRAMME

In a dynamic digital age, where over half the global population is at potential risk from cybercrime, the INTERPOL Global Cybercrime Programme stands in support of the international law enforcement community. We are dedicated to developing and leading a global response in order to prevent, detect, investigate, and disrupt cybercrime – with the ultimate mandate of reducing its global impact and protecting communities for a safer world.

The INTERPOL Global Cybercrime Strategy focuses on four main objectives:

- Enabling a proactive and agile approach to the prevention and disruption of cybercrime by developing an in-depth understanding of the cybercrime threat landscape through information sharing and intelligence analysis.
- Effectively preventing, detecting, investigating, and disrupting cybercrime that causes significant harm on a national, regional, and global scale by leading, coordinating, and supporting member countries in transnational operational activities.
- Supporting the development of member countries' strategies and capabilities for combating cybercrime by cultivating open, inclusive, and diverse partnerships and building trust in the global cybersecurity ecosystem.
- Promoting INTERPOL's role and capabilities in shaping global security by participating in international forums in the field of cybercrime.

We implement our Strategy and objectives via a simple and constructive delivery model, which consists of three core pillars:

- Cybercrime Threat Response: Addressing immediate and emerging cyber threats with a rapid and coordinated response.
- Cybercrime Operations: Implementing a regionally focused operational strategy to combat cybercrime effectively.
- Cyber Capabilities Development: Enhancing strategies and capabilities through innovative projects and platforms.

Underpinning these pillars is our extensive network of public-private partnerships, which fosters collaboration and leverages collective expertise to fight cybercrime.

For any further information, please contact us at the following email address: EDPS-CD@interpol.int

ABOUT THE INTERPOL AFRICA JOINT OPERATION AGAINST CYBERCRIME

AFJOC is an INTERPOL initiative aimed at strengthening the capability of African national law enforcement agencies to prevent, detect, investigate, and disrupt cybercrime. This is achieved by:

- Gathering and analysing information on cybercriminal activity;
- Carrying out intelligence-led, coordinated action; and
- Promoting cooperation and best practice amongst African member countries.

Phase 1 of the initiative was funded by the United Kingdom Foreign, Commonwealth & Development Office, and ran from 2021 to 2023. The second phase, still supported by the UK FCDO, is building upon the achievements of the first, and aims to further enhance the capabilities of national law enforcement agencies in Africa.

Project Activities

- Analytical support and intelligence – timely and accurate intelligence is vital in any effective law enforcement response to cybercrime. Our Cyber Activity Reports are important resources, providing insight on cyber threats targeting specific countries or regions;
- Developing regional capacity and capabilities to combat cybercrime – collaborative platforms such as the Cybercrime Collaborative Platform and the Cyber Fusion Platform allow for secure communications and the exchange of data on operations;
- Joint Operational Framework – this addresses cybercrime threats through collaboration between law enforcement agencies, the private sector, and other international/ intergovernmental organizations;
- Operational support and coordination – our operations help dismantle the criminal networks behind cybercrime;
- Awareness-raising campaigns – promoting good cyber practices among individuals and businesses in Africa.

The INTERPOL African Cybercrime Operations Desk is responsible for implementing the AFJOC. It works in close partnership with key regional stakeholders, in particular the African Union and AFRIPOL, law enforcement communities, and the private sector.

INTERPOL

INTERPOL Global Complex for Innovation
18 Napier Road
Singapore 258510

Follow us:

INTERPOL HQ

@INTERPOL_HQ

INTERPOL

INTERPOL HQ

INTERPOL_HQ