INTERPOL

AFRICAN CYBERTHREAT ASSESSMENT REPORT CYBERTHREAT TRENDS

OUTLOOK BY THE AFRICAN CYBERCRIME OPERATIONS DESK

March 2023

CONTENTS

LEGAL DISCLAIMER

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of INTERPOL concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The designations of country groups are intended solely for statistical or analytical convenience and do not necessarily express a judgment about a particular country or area.

References to names of firms and commercial products and processes do not imply their endorsement by INTERPOL, and any failure to mention a particular firm, commercial product, or process is not a sign of disapproval.

All reasonable precautions have been taken by INTERPOL to verify the information contained in this publication. However, the published material is distributed without warranties of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader. In no event shall INTERPOL be liable for damages arising from its use.

INTERPOL takes no responsibility for the continued accuracy of the information or for the content of any external website.

INTERPOL has the right to alter, limit, or discontinue the content of this publication.

FOREWORD

Today, technology is an indispensable part of our lives, especially the Internet, which plays a critical role in both our professional and personal activities. We use it to control critical infrastructure systems, conduct financial transactions securely and efficiently, stay connected with friends and family, and shop conveniently and quickly online, as well as to entertain ourselves by watching videos or playing games. In addition to its many applications, the internet also provides us with unprecedented access to information that was previously out of reach. The Internet has enabled us to connect with people across the world and has simplified the process of gathering data and information for research purposes. It has even allowed us to explore virtual worlds that go beyond what is possible in the physical realm. With all these advantages, it›s no surprise that the Internet is now a ubiquitous part of our daily lives.

With the emergence of new technologies, cybercrime has also been a growing concern in recent years. Cybercriminals are constantly evolving their techniques to exploit new vulnerabilities, resulting in an increased risk to both individuals and organizations worldwide. Cybercrime today is a far cry from what it used to be; there are now more sophisticated attack vectors such as distributed denial-of-service (DDoS) attacks, phishing attempts, malware campaigns, ransomware attacks, and other malicious activities that can cause a great deal of harm and have a serious impact on organizations and communities.

Overall, it is clear that the threat landscape is constantly changing and evolving, with new hybrid forms of cybercrime emerging every day —it is therefore imperative for organizations around the globe to stay vigilant against these threats by continually updating their security protocols and practices accordingly. As we move forward into 2023 and beyond, it will be critical for large and small companies alike to implement comprehensive cybersecurity solutions that will help protect them from the high volume of traditional forms of cyberattacks as well as the new hybrid methods being created by malicious actors worldwide.

Under the mandate of reducing the global impact of cybercrime and protecting communities for a safer world, INTERPOL Cybercrime Directorate’s core activities are preventing, detecting, investigating, and disrupting cybercrime. In order to achieve this, and to provide better support for member countries in understanding cyberthreats at a national, regional, and global level, cybercrime data and information must be collected, processed, analysed, and evaluated.

As part of these efforts, I am proud to present the second edition of the African Cyberthreat Assessment produced by the African Cybercrime Operations Desk (”African Desk”).

This report provides in-depth analysis of and insight into the latest cyberthreat landscape faced by member countries in the African region. As technology advances, so do the methods used by criminals to exploit vulnerabilities within networks and systems. In recent years, African states have seen a rise in cyberattacks targeting critical infrastructure, financial institutions, and other organizations as they become increasingly reliant on digital services.

We must recognize the fact that international cooperation between law enforcement agencies is an essential part of any strategy to counter and combat cybercrime. As cybercriminals become increasingly sophisticated and organized, a global coordinated effort is required to ensure that threats are properly addressed.

Working together with our 195 member countries and using methodologies coordinated at a regional and national level can help improve investigative outcomes by making it easier to exchange intelligence on emerging threats, share best practices for investigation techniques, and make the best use of technology to strengthen capabilities.

Additionally, joint operations should be encouraged wherever possible, as they help build trust between participating member countries while providing opportunities for them to learn from each other's experiences in tackling similar threats.

It is also important for law enforcement agencies to work closely with private sector organizations, as they can often share valuable intelligence on emerging cyber threats, offer training programs for personnel, and share technical expertise which may not be available within government entities. Engaging with the private sector allows law enforcement agencies to utilize enforcement databases and legislative powers which enable them to respond quickly to threats before they cause significant harm or impact.

With the aim of protecting digital economies and communities in the African region, this report also highlights strategies and presents a way forward for the region.

While Advanced Persistent Cybercrimes (APC) such as ransomware, phishing, banking trojans, and stealer malware are highlighted in this report, it also contains analysis of various types of cyber scams and fraud. Indeed, as soon as these types of crime were detected, the African Desk was able to lead on-the-ground action against the cybercriminals involved by developing a plan for multi-jurisdictional actions and coordinating joint operations (codenamed Falcon II and Delilah).

The increased and improved operational support and the sharing of proactive intelligence will provide better support for member countries, in a way that reflects the unique challenges and needs within this region.

The aim of this report is to help improve understanding of the regional cyberthreat landscape in order to provide a prioritised and targeted response to cybercrime threats via INTERPOL channels.

We thank the member countries in African region and our partners for their strong commitment in this endeavour. We are immensely appreciative of their dedication, hard work, and perseverance in furthering this cause.

Craig Jones
Director, Cybercrime Directorate
INTERPOL

FOREWORD

In the late 1990s, the pioneers of Internet access in Africa were connected using geostationary satellites. Only a handful of privileged people were able to access the Internet. Twenty years later, all the countries of the continent are connected to the global network via submarine or terrestrial cables, satellites, and even using drones and balloons. 25 per cent of the African population in the South Sahara has permanent access to the Internet, compared to 60 per cent of the population in North Africa, while on average only 50.8 per cent of the world's population is connected to the Internet.

37 African countries have set up universal access funds to expand national Internet coverage, which has led to the African continent having one of the highest connectivity growth rates in the world. However, as with any new emerging technology, the development of the Internet has also led to an increase in cybercrime. Cyber-dependent and Cyber-enabled crimes now affect all sectors of activity, with new trends involving collaboration between traditional forms of crime and cybercrime. For example, terrorist groups may use the services of cybercriminals to raise funds using cryptocurrencies, and criminal human trafficking networks are exploring the dark web in order to gain expertise in designing fake travel documents. These new developments in organized crime make it impossible to dissociate the fight against cybercrime from the fight against all other forms of crime.

The second alarming fact is that two years after the COVID-19 pandemic, the after-effects are still being felt on the African continent, particularly with the loss of jobs that has destroyed certain sectors such as the hotel industry, tourism, and aviation. In addition, working methods have evolved since COVID-19 and some employees now prefer remote work, which leaves the way open to attacks such as fishing and BEC.

Overall awareness of the threat of cybercrime is very real on the African continent. Initiatives such as awareness campaigns and regional and continental conferences, as well as bootcamps and capacity building programs, have become more and more frequent in recent years. As part of this policy of responding to cybercrime, AFRIPOL organized the first session of its Bootcamp on Cybercrime investigation, including phishing, malware, OSINT, the darknet, and cryptocurrencies, from the 21st to the 23rd of September 2022. This first session recorded a total of 136 participants from 22 countries.

AFRIPOL is pleased with its collaboration with INTERPOL, and they are still our main partner, working together through the Interpol Support Program to the African Union in relation with AFRIPOL (ISPA). 2022 has been a particularly fruitful year for this collaboration, with the realization of numerous projects: Africa Cyber Surge, the purchase of digital triage SPEKTOR devices and training for 7 countries, the purchase of 12 CHAINALYSIS licenses and training for beneficiary countries, and the purchase of approximately twenty CYBERBELT Tools licenses and training for beneficiary countries.

Other successful partnerships, with the German Federal Police via GIZ and with the United Kingdom Foreign, Commonwealth & Development Office (UK FCDO), have also facilitated the realization of numerous projects, such as the Network of Excellence in Forensics and the first Bootcamp in Cybercrime. Many large-scale projects are planned for 2023, with the upcoming launch of the new AFRIPOL datacentre and forensic databases and the establishment of a Criminal Intelligence Analysis Unit (CIA).

The more we progress in the fight against cybercrime, the more we realize that this fight is expensive and requires the pooling of resources. There are huge disparities between African countries. Some have highly qualified experts and investigative laboratories equipped with modern tools, while others are just beginning to develop basic legislative and legal frameworks to fight cybercrime. The sacred principle of solidarity that prevails within the African Union means that a holistic approach to the problem is needed, and that all must benefit from developments.

Henceforth, AFRIPOL is therefore focusing the operational element of its fight against cybercrime on the following three axes:

1. Training with non-proprietary and license-free technologies when the cost of expensive licenses is preventing anti-cybercrime units from responding quickly.
2. Establishing a fund for the fight against cybercrime with contributions from all partners interested in this field, to finance joint purchases of licenses and equipment in order to reduce costs and logistics.
3. Strengthening collaboration with the private sector in order to harmonize and standardize procedures and technologies, and for intelligence-gathering purposes throughout the continent.

Africa is catching up fast in terms of connectivity; a double-edged sword that creates both development opportunities and threats to people's security and that of their property. It is also clear that the power of the Internet has erased borders across the world. A cyber-attack launched from Africa can reach a target anywhere in the world, which is why we must mount a joint response to the global scourge of cybercrime. An upgrade of defence and fighting capabilities must be conducted between African countries and the rest of the world. This can be achieved via a complete global harmonization of procedures, technologies, and training programs.

Finally, we hope that in 2023 we will achieve our goals and better coordinate the actions of Law Enforcement Agencies.

Ambassador Jalel CHELBA
Ag. Executive Director,
AFRIPOL

ABBREVIATIONS AND ACRONYMS

AFJOC	African Joint Operation against Cybercrime
BEC	Business E-mail Compromise
CERTs	Computer Emergency Response Teams
CII	Critical Information Infrastructure
CnC	Command and Control server
CARs	Cyber Activity Reports
DDoS	Distributed Denial-of-Service
DNS	Domain Name System
EU	European Union
FBI	Federal Bureau of Investigation
HTTPS	Hypertext Transfer Protocol Secure
IGCI	INTERPOL Global Complex for Innovation
IP	Internet Protocol
IRC	Internet Relay Chat
OSINT	Open-Source Intelligence
P2P	Peer-to-Peer
PoS	Point-of-Sale
PPP	Public Private Partnerships
RATs	Remote Access Tools
SMEs	Small and Medium-sized Enterprises
SSL	Secure Sockets Layer

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) also contributed to this report, with the support of the German Federal Foreign Office.

This report is based on assessments of information provided to INTERPOL by the relevant Member Countries and INTERPOL's private partners, including Group-IB, Kaspersky, Shadow Server, and Trend Micro.

EXECUTIVE SUMMARY

In a globalized world, where economies are increasingly interconnected and technology is advancing at an unprecedented rate, the threat of cybercrime is a serious challenge for governments, businesses, and citizens alike. The range and complexity of attacks has grown exponentially in recent years, with criminals exploiting new methods of infiltration in order to access confidential data and sensitive information.

As this trend continues, the security risks for all organizations are greatly increased, at an immeasurable cost to the global economy.

An article published by the World Economic Forum's Centre for Cybersecurity[1] stated that "nearly half of businesses are being hit by economic crime, with cybercrime the gravest threat".

Cybercrime has become a multi-billion-dollar industry, and it is tempting for the traditional crime syndicates to shift their activities into cyber space or even commit cybercrime with the use of sophisticated tools and evolving tactics, which means that organizations and individuals alike must keep their security measures up to date. Cybercriminals have been known to engage in activities including exploiting weak passwords, masking their identity through proxy servers, stealing confidential information from businesses and governments, identity theft, and ransomware attacks.

Governments around the world have recognized the threat posed by cybercrime and continue to invest significant resources in protecting their citizens online. Law enforcement agencies have developed effective tactics such as capability building, tracking malware origins, and developing cybersecurity best practices for organizations. In addition, many countries are working together via international mechanisms such as INTERPOL's Joint Operation Framework in order to better share cybercrime-related intelligence.

Despite this action being taken by law enforcement agencies and governments around the world, cybercriminals are still one step ahead. Cybercriminals are known for taking advantage of security vulnerabilities in order to gain access to sensitive information or financial assets, and this results in billions of dollars' worth of losses each year.

A good example is Business Email Compromise (BEC), an increasingly prevalent form of transnational cybercrime that does not require sophisticated technical skills yet has the capacity to cause massive monetary losses.

In the United States of America alone, the Internet Crime Complaint Center (IC3) reported receiving close to 20,000 BEC complaints in 2021, with estimated adjusted losses of roughly USD 2.4 billion.

The Federal Bureau of Investigation reported that BEC has caused staggering losses of more than USD 43 billion globally, with an increase of 65 per cent between 2019 and 2021, most likely due to the COVID-19 pandemic, which forced many individuals to shift to conducting business virtually.

Even without the effect of the COVID-19 pandemic, the volume and persistence of these cyber-attacks is expected to continue increasing.

Cybercriminals have no limits in terms of sharing resources and know-how, which is in part what allows them to thrive. By the same token, binding ourselves closer together via the exchange of information and professional advice may be our best weapon in the combat against the frustrating threat of cybercrime.

In order to reduce the global impact of Cybercrime and protect communities for a safer world, agencies must stay abreast of these new trends and develop innovative means of responding to them. Doing this in a timely fashion will discourage possible criminal activity and dissuade potential perpetrators in advance.

[1] World Economic Forum's Center for Cybersecurity (https://www.weforum.org/agenda/2022/07/fraud-cybercrime-financial-business/)

With data drawn from INTERPOL's member countries, private partners, and research conducted by the Africa Cybercrime Operations Desk, this 2022 report provides a comprehensive overview of cyberthreat trends in the African region. The following are some of the prominent cyberthreats identified in the report, and this trend continues in the African region:

- **Business Email Compromise** campaigns continue to be the most prevalent, with businesses suffering major losses: it has proven to be low-cost and low-risk, but most profitable for cybercriminals. The cybercriminals behind BEC are becoming more sophisticated and are using highly technical tools to carry out their fraudulent activities.
- **Phishing** is a growing concern in Africa due to the rapid adoption and use of digital technologies. As more people are turning to online services and applications, they are becoming increasingly vulnerable to phishing attacks.
- **Ransomware attacks** where cybercriminals target government, retail, and public institutions have been increasing rapidly in number. Critical infrastructure including the energy and transportation sectors have even been targeted.
- **Banking Trojans and Stealers** pose an emerging and imminent threat to online shoppers, as well as damaging confidence in online financial payments. It is easy to obtain different kinds of Trojans and Stealers on underground forums, which makes it easy for cyber-criminals to launch their malicious campaigns. Evolving functionalities make it even more challenging for law enforcement agencies to investigate these crimes.
- **Online Scams** are becoming increasingly prevalent as internet access is becoming widely available. This problem is compounded by victims' poor levels of digital literacy, which makes them easy targets for cyber criminals who lure them in with false promises that will ultimately cost them financially.
- **Cyber Extortion** will still need to be monitored: it goes hand in hand with the proliferation of the Internet and mobile technologies, as more people are susceptible to demands for financial payments and extortion.
- **Crimeware-as-a-Service** is becoming more popular in Africa due to its ease of use, affordability, and lack of consequences due to weak legal frameworks regarding cybercrime enforcement. It provides criminals with an easy way to conduct financially motivated attacks against vulnerable systems and businesses with minimal effort or technical knowledge.

It is also important to note that increased access to technology comes with an increased risk of falling victim to these types of crimes, which makes it essential for citizens and organizations alike to stay vigilant when dealing with digital matters. In addition, regional law enforcement agencies need to be better equipped with the tools and knowledge needed to detect, investigate, and prosecute the individuals behind these malicious acts, and must work together with international partners such as INTERPOL at a global level when necessary.

Under the mandate of reducing the global impact of cybercrime and protecting communities for a safer world, the INTERPOL Africa Cybercrime Operations Desk, as part of the AFJOC project, aims to use this threat assessment as a basis to drive intelligence-led, coordinated action against cybercrime and its perpetrators in African member countries.

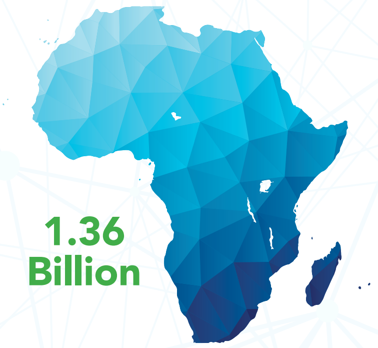
Collective efforts in sharing intelligence and formulating a joint operational framework will greatly bolster regional capabilities and capacity in the fight against cybercrime. Cooperation between governments, law enforcement, private companies, and academic institutions is key to harnessing the most comprehensive data sets and resources available, which can then be used to develop more effective strategies to combat cybercrime.

The effectiveness of such joint operations has already been seen in the recent African Cyber Surge Operation, coordinated by INTERPOL's Cybercrime Directorate and the INTERPOL Support Programme for the African Union (ISPA) in collaboration with AFRIPOL.

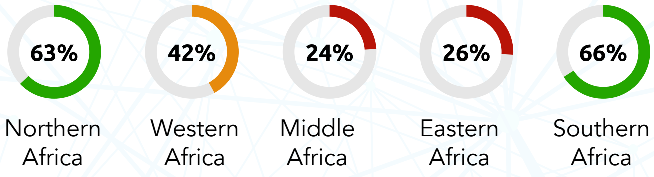
As well as improving intelligence sharing, INTERPOL is committed to developing the regional capabilities and capacities law enforcement agencies across the continent need if they are to successfully and efficiently investigate cases involving technology-based crime.

1. CURRENT DIGITAL DEVELOPMENT IN THE AFRICAN REGION

Africa is an incredibly diverse region, with countries ranging from desert landscapes to lush tropical islands. It is home to the world's second-largest population and is one of the most culturally-diverse regions on Earth. It is also rich in natural resources such as oil and gas, gold and diamonds, tin and copper ores, uranium, bauxite and many other minerals. These are some of the main drivers of economic growth in Africa, along with industries such as agribusiness, manufacturing, and tourism. Africa has an abundance of arable land that provides many of its countries with a significant agricultural base that contributes a quarter of their GDP.



Manufacturing has also played an increasingly important role in Africa's development in recent years. Its increasing focus on value-added production has seen a significant rise in foreign direct investment, creating jobs and boosting local economies in many parts of the region.

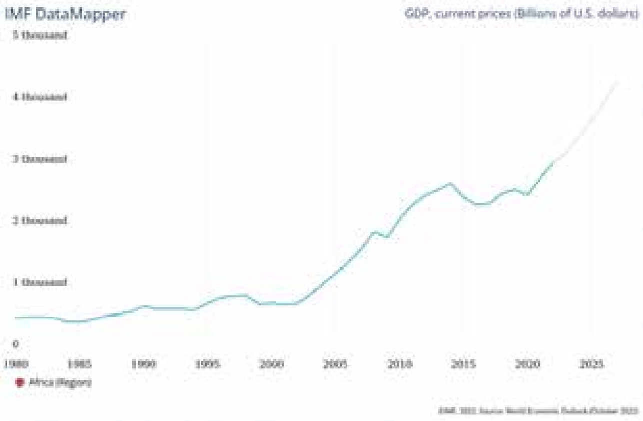


The region's combined GDP[2] has more than quintupled in just 20 years, from USD 695.88 billion in 2002 to USD 2.98 trillion in 2022. The African region is one of the largest markets in the world, and is predicted to exceed USD 4 trillion by 2027. The Internet penetration rate in Africa is relatively high compared to global rates.

According to the 2022 Global Digital Report[3], the average Internet penetration rate in Africa is about 44 per cent.

It has been increasing rapidly over the past few years and shows no signs of slowing down, with African countries making significant financial investments in infrastructure and digital access. In addition, many countries are rolling out 5G coverage throughout their respective nations, further amplifying this increase.

It is also worth noting that most of this growth can be attributed to mobile internet usage (as opposed to fixed line connections) due to its convenience and affordability. Mobile networks have become increasingly reliable across most African countries, making it easier for people to remain connected online and benefit from access to online services such as e-commerce and social media platforms.



Additionally, many governments in Africa are taking measures to ensure that everyone has fair access to digital tools and can benefit from the new opportunities offered by the ever-changing digital landscape. For example, the African Union launched the National Digital Transformation Strategy for Africa (2020-2030)[4], which aims to provide an internet connection for all citizens in Africa by 2030 as well to foster inclusive digital skills and human capacity in various digital fields such as coding, programming, analysis, security, blockchain, machine learning, artificial intelligence, robotics, engineering, innovation, entrepreneurship, and technology policy and regulation.

[2] GDP (Current) in USD. Source: International Monetary Fund

[3] 2022 Digital Global Report (www.wearesocial.com)

[4] The Digital Transformation Strategy For Africa 2020-2030 (https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf)

On a separate note, the average social media penetration in the African region is about 27 per cent, with a higher proportion of active social media users in the Northern African and Southern African regions (56 per cent and 45 per cent respectively).

The African region is seeing unprecedented growth and development in the digital technology sector, particularly in financial technology and e-commerce. This has increased demand for Internet and broadband services, making it one of the most competitive markets in the world. A plethora of investors from around the world are vying to capitalise on this opportunity, but the increased reliance on online infrastructure has also brought with it a variety of security threats that can cause serious problems.

The digital transformation of Africa is a growing phenomenon that has seen many countries on the continent take advantage of advancements in modern technology to boost their economic growth, as well as increase access to essential services. As digital technologies continue to expand across the continent, African nations are beginning to embrace them and integrate them into their economies. This process of digital transformation has been enabled by several factors, including the increased availability of data and information, better access to the Internet, the emergence of innovative start-ups and organizations, improved infrastructure for communication and commerce, and government initiatives aimed at promoting digital investment.

In recent years, many African countries have made remarkable progress in terms of embracing digital transformation. Ethiopia, for example, has implemented technology-enabled strategies[5] such as the National Rural Land Administration Information System (NRLAIS) that have helped increase efficiency in its agricultural sector. In Kenya, tech companies such as Microsoft are helping farmers utilize data to make their farming practices more efficient. Rwanda has also embraced digital transformation with initiatives set up as part of its Smart City Rwanda Masterplan[6].

[5] Digital Ethiopia 2025 (https://www.pmo.gov.et/media/other/b2329861-f9d7-4c4b-9f05-d5bc2c8b33b6.pdf)

[6] Smart City Rwanda Masterplan (https://www.minict.gov.rw/fileadmin/user_upload/minict_user_upload/Documents/Strategies/Smart_City_Rwanda_Masterplan.pdf)

2. INSIGHTS ON TRENDS IN AFRICAN CYBERTHREATS: 2022

Using data drawn from INTERPOL's member countries in the African region and private partners, and the research conducted by the African Cybercrime Operations Desk, this section will provide in-depth analysis of the threats and trends in cybercrime, as well as its underlying motivations. The African Cybercrime Operations Desk identified some of the most prominent cyberthreats in 2022, and these trends continue in terms of the threats faced by member countries in the African region.

Business Email Compromise (BEC)

Business Email Compromise is a form of cyberattack where malicious actors gain unauthorised access to an organization›s email account and then use it to send out fraudulent messages to its business associates for financial gain. These emails often contain malicious links or attachments that, when clicked on, can install malware on the recipient›s device or provide the attacker with access to confidential information. In addition to sending out emails, perpetrators may also manipulate existing email threads and delete important emails such as payment requests containing bank account details. Business Email Compromise can lead to significant financial losses and damage an organization's reputation.

Phishing

Phishing is a form of cyber-attack carried out by malicious actors in order to steal sensitive information such as usernames, passwords, and credit card details from unsuspecting victims. Phishers typically use deceptive emails or websites that appear to be legitimate in order to lure people into providing their personal information. They may also use social engineering tactics such as spoofing, impersonation, and malware attacks to gain access to confidential data. Phishing attacks can cause significant financial damage and even be used for identity theft.

Ransomware

Ransomware is a malicious form of software that locks users out of their own data, systems, and devices by encrypting their files. Once the encryption process is complete, the victims receive a message informing them that they must pay a certain amount of money (usually in Bitcoin or another cryptocurrency) to have their files decrypted and regain access. This type of attack has become increasingly popular with cybercriminals due to its ability to quickly generate large profits with minimal effort: in many cases an attacker can carry out a successful ransomware attack simply by sending out a single email. Ransomware can also be spread through malicious adverts on websites and social media, as well as via malicious downloads from websites.

Banking Trojans and Stealers

Banking Trojans and Stealers are malicious software programs designed to steal sensitive information such as usernames, passwords, and financial data from unsuspecting victims. These trojans can be installed through phishing emails, malicious websites, drive-by downloads, or other means. Once the Trojan is installed on a victim›s computer, it attempts to gain access to online banking accounts by capturing keystrokes or stealing login credentials. It can also modify webpages displayed in the browser to redirect any transfers of funds to the criminals' accounts instead of the intended recipient. Banking Trojans are often used together with other malware tools such as Spyware and Rootkits in order to spread more quickly throughout a network or system.

Banking Trojans have become increasingly sophisticated over the years, employing advanced techniques such as man-in-the-browser attacks that allow attackers to manipulate transactions without being detected.

Online Scams

Cyber fraud is the most common and threatening form of fraud, and it takes place at an international level. Cyber fraud can be defined as any fraudulent crime which is conducted via a computer or using computer data.

Cyber Extortion

Cyber Extortion is a type of cybercrime wherein the criminal uses digital methods to threaten or extort victims for money and/or other assets. It often involves the attacker threatening to reveal embarrassing personal information, delete important data, sabotage systems and networks, or launch distributed denial-of-service (DDoS) attacks.

Crimeware-as-a-Service

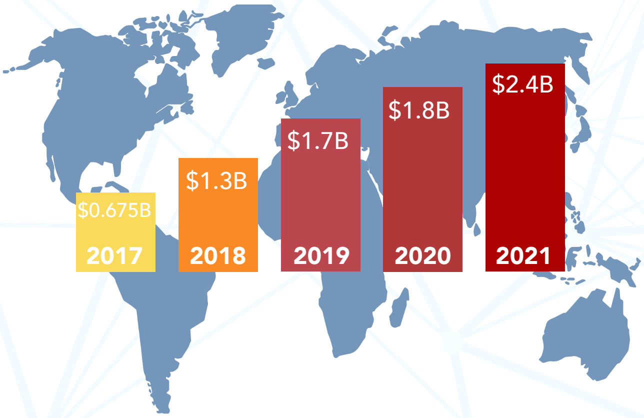
Crimeware-as-a-service, or CaaS, is any computer programme or set of programmes that are designed to facilitate illegal activity online. Spyware, phishing kits, browser hijackers, and key loggers, amongst others, are all available to attackers through CaaS.

2.1 Business Email Compromise

For the seventh consecutive year, Business Email Compromise (BEC) attacks have been the most financially devastating cyber threat worldwide. Last year alone, US companies lost a staggering USD 2.4 billion[7] due to these attacks, representing a 28 per cent jump from 2020 and a huge increase of over half a billion dollars. This number is an alarming reminder of just how powerful and damaging BEC attacks can be for businesses of all sizes.

Apart from causing significant financial losses, BEC scams can also damage an organization›s reputation if customers become aware that they have been affected by such malicious activities.

US COMPANIES' BEC LOSSES



Many of the actors carrying out BEC scams have been found to be based in West Africa, but unfortunately for their victims, their schemes are not confined by geographical borders. These criminals often have connections with larger criminal networks worldwide, which allows them to target large numbers of victims on a global scale. It is indeed a sobering fact that the same actors behind BEC scams are also responsible for many other types of cybercrime.

These cybercriminals have become increasingly more sophisticated in recent years and have developed ways to avoid detection by law enforcement: using multiple email accounts and routing funds through international bank accounts and shell companies. They may also use encrypted communication channels such as chat apps or dark web forums to further conceal their activities, which makes it even more difficult for law enforcement agencies to track them down, especially as they may be spread across multiple countries or jurisdictions. Moreover, some scammers even collaborate with money mules who help launder money through a variety of shell companies and offshore bank accounts. This enables them to remain anonymous and puts them beyond the reach of the authorities.

In response to the high concentration of BEC actors detected within the Nigerian region, INTERPOL's Africa Cybercrime Operations Desk, alongside its private partners Group-IB, Palo Alto Networks, and Trend Micro, and the Nigerian Police Force (NPF), launched a successful operation in May 2022: "Operation Delilah "[8]. The purpose of this operation was to severely disrupt a prolific BEC group known as "SilverTerrier" or "TMT" and this led to the arrest of the head of a transnational cybercrime group.

The team behind Operation Delilah also successfully identified key individuals who were directly involved in committing these malicious cybercrimes, which has significantly reduced their ability to continue their criminal activity. Additionally, vital evidence was obtained that led to the identification and confiscation of stolen funds, as well as incriminating documents and digital devices used by members of the criminal network.

This proactive law enforcement action was followed by another operation, codenamed "Killer Bee"[9],

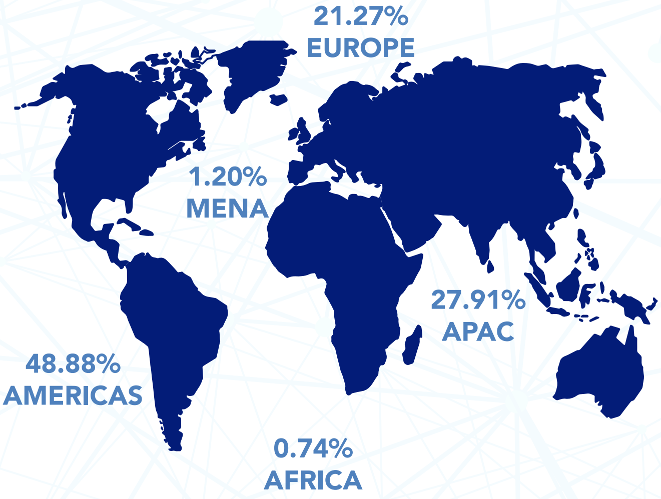
[7] Federal Bureau of Investigation Internet Crime Report 2021 (https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf)

[8] Suspected head of cybercrime gang arrested in Nigeria, May 2022 (https://www.interpol.int/News-and-Events/News/2022/Suspected-head-of-cybercrime-gang-arrested-in-Nigeria)

[9] Online scamming fraud: three Nigerians arrested in INTERPOL Operation Killer Bee, May 2022 (https://www.interpol.int/en/News-and-Events/News/2022/Online-scamming-fraud-three-Nigerians-arrested-in-INTERPOL-Operation-Killer-Bee)

based on intelligence received from a private-sector partner, Trend Micro. This INTERPOL-led operation resulted in the arrest of 3 Nigerian BEC actors after an extensive investigation by the Nigerian Economic and Financial Crimes Commission (EFCC). These men are thought to have used a Remote Access Trojan (RAT) to reroute financial transactions and steal confidential online connection details from corporate organizations including oil and gas companies in Southeast Asia, the Middle East, and North Africa.

The efficacity of Operation Delilah and Killer Bee in disrupting ongoing BEC activities within Nigeria highlights just how vital it is for international law enforcement organizations such as INTERPOL and local law enforcement agencies like the NPF and EFCC to work together if they are to successfully combat the organized crime networks operating throughout the country. These joint efforts provide extra support in tackling such sophisticated cybercrime networks, providing an additional layer of protection for citizens against various forms of fraud and malicious activities online.



BEC ATTEMPTS PER REGION (2021 - MAY 2022)
SOURCE: TREND MICRO

Trend Micro also reported that cybercriminals are increasingly targeting other regions, particularly those with higher concentrations of high-value targets where the economic impact is greater. The African region has also been the victim of BEC attacks in recent years, with financial losses and disruption to businesses caused by cyberattacks continuing to rise.

Despite African countries representing just 0.75 per cent of global BEC attempts between 2021 and May 2022, data from Trend Micro reveals that South Africa accounted for more than half of the BEC cases reported in the region during the same period.

The threat of BEC has become particularly acute in the African region due to the rapid transition to an increasingly digitalised economy. With more and more users relying on technology for day-to-day transactions, there are more opportunities for malicious actors to exploit vulnerable organisations. Additionally, many parts of Africa lack effective cyber security measures, which further increases the risk of BEC attacks.

Another factor that contributes to the rise in BEC attacks across Africa is the lack of basic cyber security practices within companies operating on the continent. Many organizations do not have adequate policies in place for managing access control protocols, authentication processes, or encryption standards, thus leaving themselves vulnerable to attack through unsecured systems and user accounts with weak passwords. This means that even if an employee were able to detect fraudulent emails sent by scammers, there would still be no way for them to protect themselves against the threat they pose – financially or operationally – as the proper defences are not in place from the outset.

One of the most common characteristics of BEC attacks in Africa is the use of social engineering techniques by scammers who exploit their understanding of regional culture and language. These malicious actors may impersonate someone their victims know and create a sense of urgency or panic, leading them to comply with the requests made in the emails without checking that they are legitimate.

Statistics from the 22 member countries in the African region show that 399 cases of BEC were reported to law enforcement agencies in 2021. An assessment of the data related to Business Email Compromise (BEC) cases in the African region specifically would help paint a more accurate picture of the situation. Unfortunately, it has become increasingly apparent that a significant amount of BEC cases go unreported in this area, which exacerbates the issue.

This lack of reporting also hinders law enforcement agencies› ability to properly prosecute the criminals involved and to allocate resources more effectively in order to tackle these forms of cybercrime.

As such, it is vital to create public awareness for businesses to report any instances of BEC threats they encounter so that valuable information related to BEC operations can be collected by law enforcement agencies across Africa and used to gain further insight into this crime trend and implement measures to combat it.

2.2 Phishing

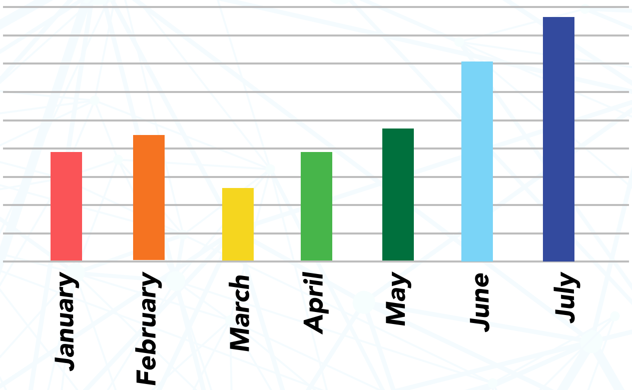
Phishing is one of the oldest and most pervasive cyberthreats in existence. It is estimated that up to 90 per cent of data breaches[10] are linked to successful phishing attacks, making it a major source of stolen credentials and information. Phishing techniques have grown increasingly sophisticated over the years as attackers learn how to target victims with greater accuracy. Attackers can craft messages that appear to be from trusted sources such as banks, governments, or even friends and family members. These messages typically contain malicious links or attachments which can lead victims to malicious websites or malicious files containing viruses or malware.

In addition to stealing credentials, the ultimate aim of phishing attacks is often to gain access to confidential data such as financial information, passwords, and detailed contact information, amongst others. Once obtained, this data can be used for financial gain and/or identity theft by selling it on dark web markets or using it for other malicious purposes such as extortion or furthering other types of cybercrime-related activities. This makes phishing a significant threat, not only due to the potential financial losses but also due to the damage caused by the other forms of cybercrime that may result from a successful attack.

As technology advances and attackers become more sophisticated in their techniques, phishing remains an ever-present threat for organizations and individuals alike. Attackers use social engineering tactics such as impersonation and scare tactics to increase their chances of success. Furthermore, automated tools such as spam bots have made it easier for attackers to send large numbers of emails or messages and therefore increase their chances of success. All these factors combined lead to a continuing and unprecedented level of risk associated with phishing attacks which makes them one of the most dangerous cyber threats that exist today.

Between January 2022 and July 2022, Kaspersky reported an alarming 15,769,298 phishing objects detected in Africa. The majority of these malicious activities were conducted through emails or web pages using a popular social engineering method known as phishing.

Detection of phishing objects by Kaspersky between Jan 2022 - Jul 2022



Group-IB identified an alarming 1,352,412 phishing URLs between January and August 2022 in the African region. This is a major security concern, as phishing attacks can have devastating results for the individuals and organizations that may be caught off guard by them.

One of the more popular phishing scams in Africa is the brand anniversary scam. It involves threat actors posing as a well-known brand, such as Ethiopian Airlines, in order to entice unsuspecting individuals with the promise of a free gift if they complete a brief survey or questionnaire. Once an individual has entered their details, they are then asked to spread the message to five WhatsApp groups or 20 friends before they can receive their reward. Unfortunately, these scammers will in fact use this as an opportunity to harvest personal details and even device information from those that unwittingly comply with their demands.

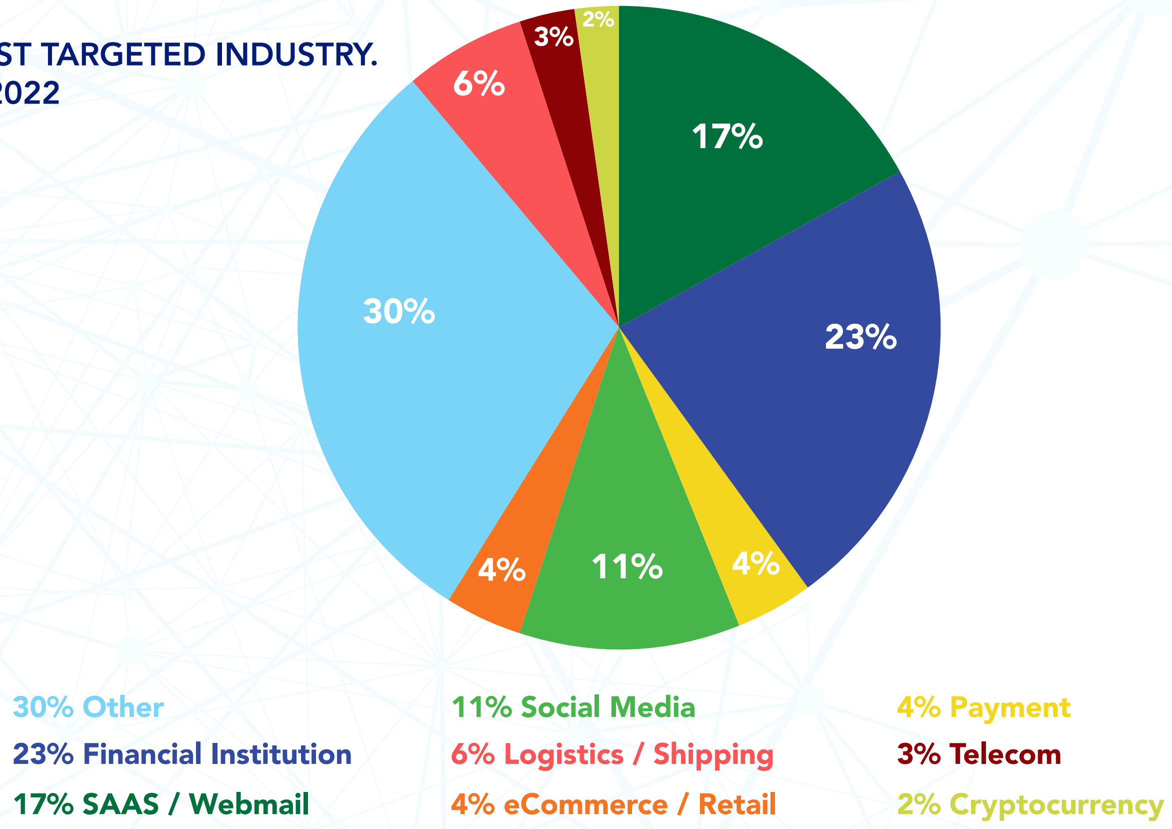
[10] CISCO's 2021 Cybersecurity Threat Trends Report (https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list)

The brand anniversary scam is just one example of how powerful and effective phishing attacks can be for criminals looking to make a quick profit through illicit activities at the expense of innocent victims. Phishing emails are becoming increasingly sophisticated in terms of both design and content, making them harder for the average person to spot. Furthermore, criminals have been known to use social engineering tactics in order to make them appear more authentic. For instance, many scammers will create fake email accounts using domain names which are similar to legitimate company names in order to increase their chances of success when targeting unsuspecting users. This can often lead victims to believe that they are interacting with a genuine representative of the company which is being impersonated.

To make matters worse, public awareness campaigns and education are lacking. As such, citizens are not adequately informed about these types of scams, nor are they provided with resources and guidance on how to protect themselves from these cyberthreats. The lack of knowledge surrounding cyber hygiene in Africa makes people even more vulnerable and makes it even easier for those committing these crimes to launch successful phishing campaigns without detection or reprisals from local authorities.

The latest report[11] published by the Anti-Phishing Working Group reveals that the financial sector, which includes banks, remained the biggest target of phishing, constituting more than 23 per cent of all attacks. The number of attacks against webmail and software-as-a-service (SAAS) providers remained the same, while attacks against retail/e-commerce sites fell to 4 per cent, down from 14.6 per cent.

MOST TARGETED INDUSTRY. 3Q2022



[11] APWG Phishing Activity Trends Report 3rd Quarter 2022 (https://apwg.org/trendsreports/)

The proliferation of phishing attacks can be attributed to the relative ease with which an individual can engage in this type of criminal activity. This is due, in part, to the availability of Phishing as a Service (PaaS) on the dark market. For as little as USD 20, an individual can purchase a phishing kit that comes with all the materials necessary for launching a successful attack. In addition, video tutorials are provided which demonstrate how to use and assemble the kit. There are also after-sales service packages with regular updates that help prevent the criminals' phishing emails from being detected by modern internet security solutions. Threat actors who may not have any technical knowledge can therefore launch their own phishing attacks with minimal effort.

Through their research, Group-IB also identified a post on the XSS forum in which a threat actor advertised the sale of phishing pages to target banks. Amongst the banks listed was Banco BIC, a Portuguese/Angolan bank with numerous branches worldwide. The post boasted that for a small fee anyone could purchase the phishing pages and gain access to users› accounts.

This low entry barrier has resulted in an increase in phishing activity in recent years. The kits themselves often contain snippets of code and scripts written by experienced developers which enable users to host their websites without the need for any knowledge on how website hosting works. Furthermore, they include pre-made anti-detection tools and templates for designing effective emails that can bypass spam filters to reach victims› inboxes undetected. This means that those engaging in this type of criminal activity do not even need to possess basic coding skills or any technical knowhow, and anyone with access to the black market and a few dollars can become a professional level cybercriminal almost instantaneously.

While numerous malicious phishing attacks have been detected in the African region, the number of reports to law enforcement agencies is much lower than expected. In 20 countries across Africa, only 2087 reports have been made; this discrepancy can be attributed to several factors, ranging from incorrect classification of cases to a lack of public awareness on how to report such crimes.

In Africa, out of 42 countries surveyed, 24 countries have shared that they have yet to establish any form of online platform or mechanism to enable the public to report cybercrime. These shortfalls hinder the ability of law enforcement agencies to not only detect but also properly respond to cases of cyberattacks. As a result, incidents are often under-reported or ignored altogether.

2.3 Ransomware

The number of ransomware attacks has been rising steeply over the last few years, and they are now considered to be one of the most serious threats faced by organizations of all sizes worldwide. Cybercriminals use this malicious software to take control of an organization's critical business systems, encrypt their data, and demand payments in exchange for restoring access. Such attacks can be extremely costly to businesses, as the financial losses incurred due to downtime and recovery efforts quickly add up.

The number of ransomware attacks is not showing any signs of slowing down and the costs associated with such attacks are expected to increase in 2023. One of the leading research and publishing firms, Cybersecurity Venture[12] , estimates that global ransomware costs will reach USD 265 billion by 2031.

Companies affected by ransomware attacks also risk significant reputational damage as customer data may be made public or stolen during such incidents, thus jeopardizing their trustworthiness in the eyes of customers and other stakeholders.

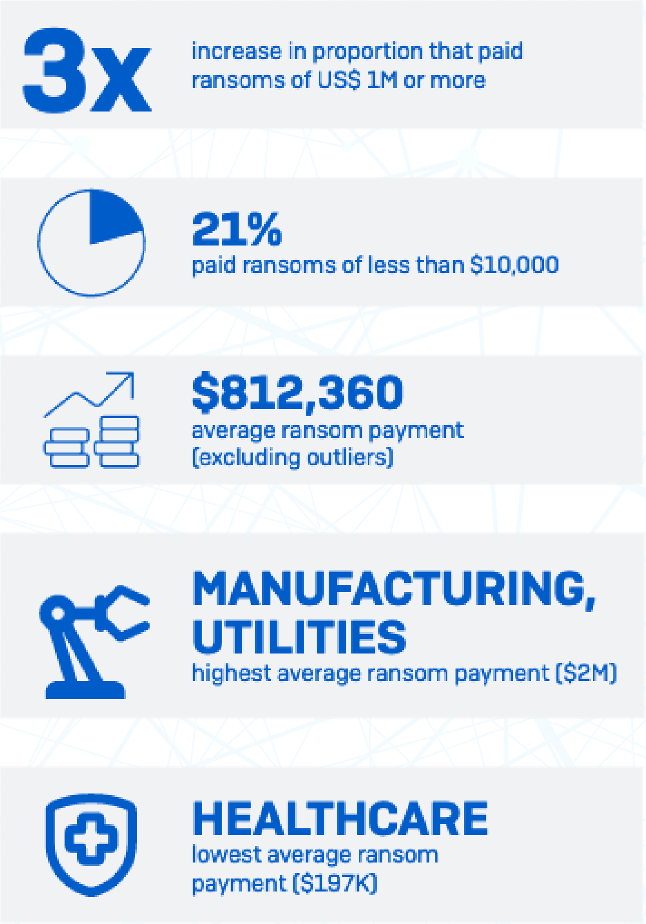
According to IBM's 2022 Cost of a Data Breach Report[13] , the total average cost of a ransomware attack was considerably higher than the average cost of a data breach, with ransomware attacks amounting to a staggering USD 4.54 million compared to the already costly USD 4.35 million for a data breach. The proportion of breaches caused

[12] Global Ransomware Damage Costs (https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/13

[13] Cost of a Data Breach Report 2022 (https://www.ibm.com/reports/data-breach)

by ransomware grew by 41 per cent last year and it took 49 days longer than average for them to be identified and contained.

This is further evidenced by Sophos State of Ransomware 2022[14] which found that mid-sized organizations paid even higher average ransoms: USD 812,360 per attack. These costs can be broken down into various components such as downtime and people time required for mitigation efforts, device costs (replacing or repairing affected hardware), network costs (restoring networks or services), lost opportunities due to delays in operations, and ransom payments made by organizations where applicable.



3x increase in proportion that paid ransoms of US$ 1M or more

21% paid ransoms of less than $10,000

$812,360 average ransom payment (excluding outliers)

MANUFACTURING, UTILITIES highest average ransom payment ($2M)

HEALTHCARE lowest average ransom payment ($197K)

SOURCE: SOPHOS STATE OF RANSOMWARE 2022

The US Treasury Department[15] has also reported that US banks processed roughly USD 1.2 billion in ransomware payments in 2021 – far more money than most hackers could ever have expected when they first developed ransomware decades ago.

With such high financial incentives, it is likely that this increase in the use of ransomware will continue unless significant steps are taken to combat it, as it requires little effort, is largely automated, the risk of getting caught is low, and the pay-outs are high.

According to Shadowserver, data collated from ransomware leak sites for the period Jan-Sep 2022 indicates that African victims are being targeted by a wide range of ransomware families. During this period, the most prevalent ransomware family was Lockbit2.0, which accounted for approximately 38.8 per cent of all detected infections across Africa. This was followed closely by Pysa at 14.3 per cent, then Lockbit3.0 which accounted for 8.2 per cent. Other notable ransomware families in this period included Conti, HiveLeaks, Midas, and BlackByte (4.1 per cent, respectively).

The impact of other malicious programs should not be underestimated. All these threats have the potential to significantly disrupt business operations by encrypting critical data or systems, resulting in hefty ransom payments or extensive downtime while organizations struggle to recover the affected files. Moreover, the proliferation of ransomware has resulted in an alarming rise in financially motivated cybercrime activities across Africa.
Shadowserver also reported that South Africa is the nation most targeted by ransomware attacks, accounting for 42 per cent of all detected attacks. Morocco is next with 8 per cent, while Botswana and Egypt come in at 6 per cent. Tanzania and Kenya each account for 4 per cent of detected ransomware attacks. Such a high level of malicious activity in South Africa is concerning, as it suggests that the number of undetected ransomware activities taking place in the country is even higher.

[14] The State of Ransomware 2022 (https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf)

[15] Remarks by Deputy Secretary of the Treasury (https://home.treasury.gov/news/press-releases/jy1067)

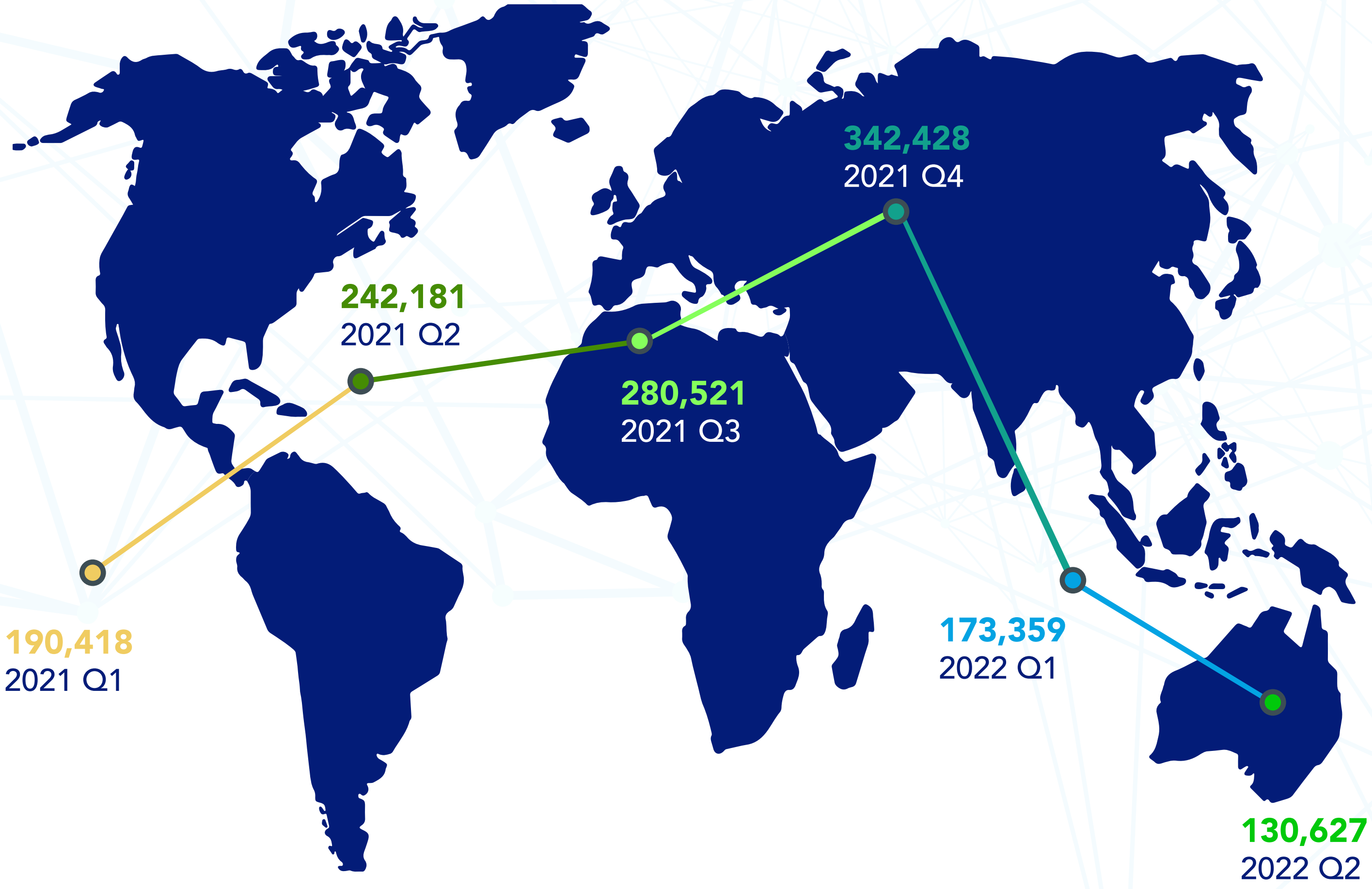
Most of these malicious activities may have been facilitated by outdated systems and ineffective security solutions that leave gaps for cybercriminals to exploit. A lack of cybercrime regulations and legislation may also be contributing to the rise in ransomware attacks across the country. With no clear-cut rules or guidelines on how to protect against such threats, many organizations are left open to exploitation by cybercriminals.

According to Trend Micro, ransomware only accounts for 1.4 per cent of all cybercrime detected across the world between January 2022 and July 2022. However, the threat of ransomware in the African region is still very real with significant numbers of these types of crime being detected. However, it should be noted that rates were lower in both the first and second quarters of 2022 compared to 2021. This decrease may be due to a variety of factors, however one possible contributing factor is the peak in the number of detections in March. This peak appears to have been primarily due to a high number of Conti ransomware detections in Tunisia, with Trend Micro noting that the shutdown of this ransomware family may be responsible for the significant drop in detections seen in April.

Another report from Trend Micro revealed that the top five most frequently attacked sectors include government agencies, education, energy, retail, and fast-moving consumer goods. Another report observed that critical infrastructure including healthcare and transportation is also targeted.

Data protection and backup tools have improved significantly over time, which has rendered traditional

RANSOMWARE DETECTION



SOURCE: TREND MICRO

ransomware tactics increasingly ineffective. When an organization has a backup of their locked data, they do not need to pay the recovery ransom demanded by the cybercriminals. As a result, these malicious actors have had to become more creative, developing double and triple extortion ransomware.

The latest evolution has been the development of Ransomware as a Service (RaaS), which allows cybercriminals to lease pre-developed versions of ransomware which can be used to carry out attacks. With the availability of RaaS, implementing successful ransomware attacks is easier than ever and attackers no longer need to have advanced technical skills and experience. In addition, this type of service also makes it much easier for attackers to target multiple victims at once due to its scalability and flexibility. Moreover, attackers can easily adjust their techniques depending on what works best in each case as they can quickly switch between different versions of malware. All these features make RaaS even more dangerous, as it is no longer necessary for attackers to have highly sophisticated skills and infrastructure to carry out successful attacks.

Data shared by 42 countries in the African region revealed that only 59 reports of ransomware cases have been filed with law enforcement agencies in 11 African countries. The actual situation is believed to be worse: as many individuals and businesses are unwilling to report these cases to the police, it is estimated that only a small percentage of ransomware incidents are made public.

The reasons for not reporting a ransomware attack may be the individual's fear that the data that has been encrypted will lose value, or companies not wanting their customers to know that their data has been compromised – a far more serious and worrying concern for businesses. Victims often remain silent about incidents and pay ransoms quietly, while attackers do not always publish data from compromised networks.

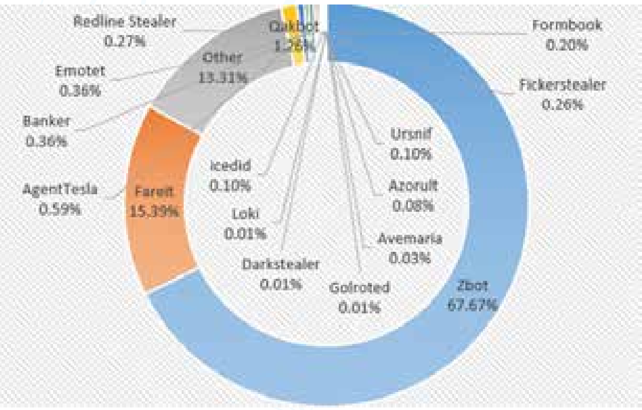
2.4 Banking Trojans and Stealers

The African region is seeing an immense surge in the digital technology sector, particularly in financial technology and e-commerce. This growth is due to increased internet access and improved mobile penetration, which allows people to access services that were previously unavailable. This has opened up new opportunities for businesses to grow and expand their operations across the continent.

However, this rapid growth also facilitates attacks in the form of malicious software such as banking trojans or stealers, which represent one of the greatest threats to both individuals' security as well as organizations' cyber infrastructures due to their potential to cause widespread damage if not detected quickly enough.

Banking Trojans and Stealers can be installed manually or remotely using social engineering techniques such as emails containing malicious links or attachments. Once installed, banking Trojans and Stealers collect personal information from an infected computer and communicate this stolen data via the internet to a remote server controlled by the attacker. Cybercriminals may use the information obtained to steal money directly from the victim, or sell the information on underground markets.

As revealed by the Trend Micro detections, Morocco is the most affected African country, with a staggering 18,827 detections. South Africa is close behind with 6560 detections of malicious software. 5366 instances of malicious software were detected in Nigeria, 1462 in Cameroon, and 691 in Algeria. Reports have also revealed that the most prevalent banking Trojan and stealer malwares are Zbot and Fareit. The former constitutes 67.67 per cent of all detections in the region while the latter accounts for 15.39 per cent. The use of both malicious software programs has increased in recent years, which affects African businesses and individuals.



Both Zbot and Fareit are difficult to detect, and therefore often manage to steal personal and financial information from their victims before they are even aware that an attack has taken place – resulting in significant losses.

Another stealer malware to be aware of in the African region is RedLine Stealer: Group-IB's research has revealed that between January 2022 and August 2022 alone, as many as 5,862,188 compromised accounts located within African IPs were acquired using the RedLine Stealer.

It has been shown that this stealer malware is usually distributed through cracked games, applications, and services, with the intent to steal sensitive information such as web browser data, cryptocurrency wallets, and application credentials for users of popular programs such as FileZilla, Discord, Steam, Telegram, and VPNs.

Banking trojans and stealers pose a real threat in Africa, one which needs to be taken seriously if citizens are to be protected from the financial losses that result from stolen funds or identity theft. Moroccan citizens are particularly vulnerable to banking trojans, as demonstrated by the high levels of malicious software detected in the country; however, citizens of other African countries should also remain vigilant and keep their online security measures up to date in order to deter potential attacks. It is important to note that these figures do not include any instances of fraud that have gone undetected or unreported; the actual amount of damage inflicted by banking trojans may therefore be much higher than these statistics indicate.

Banks and financial institutions need to put in place measures to protect customers from cybercrime such as phishing scams and malware infections, but individuals must also remain aware and be proactive when using the internet for financial transactions. Keeping devices up to date with the latest anti-virus/malware protection software can serve as a first line of defence against threats such as banking trojans; however, users should also use passwords that are unique and difficult for attackers to guess in order to ensure optimum security. Ultimately, a collective effort between banks, government agencies, and individual users is required in order to stem the tide of cybercrime caused by banking trojans in Africa.

2.5 Online Scams and Extortion

Online scams include a wide range of fraudulent activities in the digital sphere. Advance payment/non-delivery scams, shopping scams, romance scams, sextortion, tech support scams, and cryptocurrency scams are among the most common online scams and are becoming increasingly prevalent in the African region.

In advance payment scams, fraudsters ask for financial deposits before delivering goods or services. Criminals usually use this strategy to collect fees from unsuspecting individuals and then disappear without providing any goods or services. In order to make it appear legitimate, scammers may even send bogus documents or ask for personal information such as credit card details, bank account numbers, and email addresses.

Shopping scams involve criminals attempting to deceive online buyers into believing they are purchasing genuine products at discounted prices. Instead of these products, victims receive counterfeit items or nothing at all. Unsuspecting customers can easily be tricked into paying money upfront without knowing that they are dealing with a fake vendor.

Romance scams occur when fraudsters build an emotional connection with an unsuspecting person by creating a false identity on a social media platform or dating website. After establishing trust and gaining access to personal accounts, the criminal uses this relationship to solicit money from their victim under false pretences, or steal sensitive information such as passwords and bank account details.

Sextortion is another concerning type of online scam – a hybrid form of romance scam – where criminals blackmail victims by threatening to share intimate images or videos unless a ransom is paid.

Tech support scams are a type of fraud wherein criminals pose as legitimate representatives from technology companies offering technical assistance in order to gain access to users› computers and extract valuable data such as passwords and financial information. Criminals may employ several strategies such as cold calls, pop-up ads, bogus emails, or automated messages claiming that users' computers are infected with malware in order to convince their victims into allowing remote access to their systems.

Cryptocurrency scams take advantage of the increasing popularity of cryptocurrencies such as Bitcoin and Ethereum by enticing investors into buying fake currencies. Cryptocurrency scammers have also been found to use sophisticated tactics such as creating fake wallets and exchanges in order to steal funds from unsuspecting victims.

With billions of users and everyday usage skyrocketing, social media platforms have become a lucrative target for cybercriminals and scammers.

Although people's attitudes towards social media have changed in recent years, their behaviour has not kept up with that shift. Many users are still operating under the same flawed assumptions about the way their personal information is handled, which leaves them vulnerable to exploitation by malicious actors. Cybercriminals use deceptive tactics such as phishing emails or malicious links in order to gain access to users' accounts, steal sensitive data, or hijack accounts to carry out identity theft. Scams are also very common on social media platforms, from fake job offers to pyramid schemes and investment fraud. Unfortunately, these scams often target those who are already struggling financially, and are therefore even more vulnerable to financial loss and emotional distress. Scammers who are particularly savvy can even hack into user accounts or create fake accounts in order to send out malicious links or messages containing malware. Cybercriminals also take advantage of the massive global audiences accessible via these platforms by creating scams specifically tailored to different

locations. This tactic allows them to spread disinformation quickly and easily, leading people into believing false news stories or investing in fraudulent schemes. Additionally, some malicious actors exploit the interactive nature of social media by impersonating well-known personalities or companies in order to further enhance their credibility and gain access to more victims.

These types of online crimes are particularly prolific in the African region due to a lack of public awareness about their existence and the way they operate. With technology advancing so quickly, it can be difficult for individuals to keep up with the latest trends in cybercrime and identify the potential danger signs in order to avoid becoming a victim of such crimes. Furthermore, people facing financial difficulties are often more prone to accepting offers from scammers under the belief that they offer a way out of financial hardship, when this is not actually the case. It is therefore important for governments and law enforcement agencies to take proactive steps to educate citizens about the various forms of online scams and the way they operate, and the measures people can take to protect themselves against falling victim to these schemes.

The effects of this type of cybercrime can be devastating; not only do victims lose money but they may also have their identities stolen and lives ruined as a result. Moreover, this kind of fraud is often perpetrated on an international scale: hackers can easily set up phony accounts across multiple countries that allow them to operate under the radar while perpetrating their crimes against unsuspecting victims across the world. It is therefore important for users to remain vigilant when engaging in online activity in order to avoid becoming victims. It is also important for social media companies to take proactive steps to protect their users from these kinds of malicious activities by increasing their security measures in order to close loopholes in their systems that criminals may exploit.

While these cybercrimes seem to be orchestrated via social engineering, researchers at Trend Micro identified 7.7 million malicious web detections as part of their research, with most of these detections related to scam websites (40.31 per cent). It has also been reported that extortion spam schemes remain a popular method of cyber-attack around the world. Of the African countries tracked, 69.24 per cent (13,002) of the extortion schemes detected were in Morocco.

INTERPOL
WAIT!
Do you know the sender?
Is the sender's email address correct?
Is the attachment suspicious?
Were you expecting this?
NEVER OPEN A SUSPICIOUS ATTACHMENT!
#JustOneClick
DOWNLOAD
TORRENT

When looking at the global distribution of extortion spam detected by Trend Micro, 2.44 per cent of sender IP addresses were geolocated to South Africa, 2.13 per cent to Morocco, 0.94 per cent to Kenya, and 0.91 per cent to Tunisia – suggesting that these servers were either compromised or form part of a botnet used for malicious activities such as extortion spam campaigns. It is highly likely that attackers have taken advantage of vulnerabilities in these servers to gain control and perform malicious tasks such as spreading malware and carrying out phishing attacks.

In response to the rapidly changing cybercrime landscape, global law enforcement and cybersecurity communities have formed an alliance to protect the public.

Harnessing the expertise of this alliance, INTERPOL has launched several global awareness campaigns (#YouMayBeNext, #JustOneClick, #OnlineCrimeIsRealCrime) to maintain communities' awareness of the cybercriminals seeking to exploit, steal data, commit online scams, or simply cause disruption in the virtual world.

2.6 Crimeware-as-a-Service

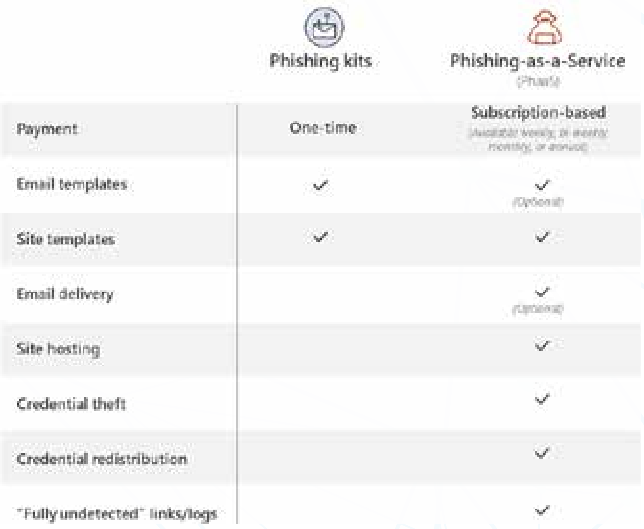
The CaaS model – crimeware being offered as a service – is something cybersecurity experts, law enforcement communities and other stakeholders involved in digital security have always been aware of. CaaS has made it possible for cybercriminals to offer their malicious code as a "service" to other criminals, who use it to infect computers, steal data, and ultimately monetize their illegal activities. This modus operandi of the criminal underground has revolutionized the way cybercriminals operate, allowing them to easily access hard-to-find tools and services such as botnets, ransomware-as-a-service, and DDoS attack resources. Furthermore, by shifting into an enterprise business model, these criminals have become better organized and are able to increase both their technical capabilities and their profit margins.

By offering crimeware via a CaaS model, cybercriminals can now provide access to a wide range of malware variants at an affordable cost. The ease with which they can purchase or subscribe to such services, or even use them on a 'pay-per-use' basis, allows them to quickly deploy malware on a global scale without the need for any specialized technical knowledge. These services also enable attackers to stay anonymous, as most providers guarantee complete anonymity throughout the transaction process.

While traditional cybercrime operations are often limited by geographical constraints or slow internet connections which can limit access or severely impact delivery times, newer CaaS models which use cloud computing technologies have drastically changed this dynamic, allowing for rapid deployment of crimeware packages in minutes from all around the world. This significantly reduces operational costs for criminals while simultaneously making it easier for them to target victims more quickly and efficiently than before.

This approach also eliminates much of the risk associated with traditional methods of acquiring malware. Since all transactions are conducted online using cryptocurrencies or similar payment methods, the chances of being caught are significantly reduced. This serves as an added incentive for criminals looking to benefit from the lucrative opportunities created by CaaS models without having to worry about getting caught.

Overall, CaaS has lowered the entry barrier for new, less technology-savvy cyber-criminals, and facilitates cyber-criminals' malicious activities by enabling them to carry out sophisticated attacks without the need for advanced technical skills. CaaS services on cybercrime dark web forums and marketplaces are broadly advertised as a cheap solution, and a range of services is readily available. It is also offered as an optimal choice for advanced attackers who want to conduct hit-and-run campaigns.



	Phishing kits	Phishing-as-a-Service (PhaaS)
Payment	One-time	Subscription-based (Available weekly, bi-weekly, monthly, or annual)
Email templates	✓	✓ (Optional)
Site templates	✓	✓
Email delivery		✓ (Optional)
Site hosting		✓
Credential theft		✓
Credential redistribution		✓
"Fully undetected" links/logs		✓

Feature comparison between phishing kits and phishing-as-a-service.

Source: Microsoft

Another element that attracts cyber-criminals to Crimeware-as-a-Service in order to venture into new areas or targets is the availability of stolen data that can be used to conduct further campaigns. The CaaS model makes it difficult to attribute a crime to a particular individual because the means and infrastructure are shared among multiple malicious actors or syndicate groups. What makes the CaaS model particularly dangerous is its role as an enabler for increasingly sophisticated attacks that are fuelling the rapid development of new advanced threats.

With combinations of various attack services, cyber-criminals can also effectively challenge law enforcement's capabilities and capacities to investigate and attribute the attacks to specific actor(s) and syndicate groups.

Phishing-as-a-service (PassS) offers automated and longer phishing campaigns, which can be deployed rapidly in a cost-effective manner. Simply by making a payment in Bitcoin for botnet services, countless malware infected machines around the world can launch powerful DDoS attacks on designated targets, with the desired network capacity and attack duration.

In recent years, there has been an unprecedented increase in ransomware attacks, largely due to the availability of ready-made ransomware-as-a-service (RaaS). This allows users to easily carry out multiple campaigns without having to write any code. Through its user-friendly online portals, RaaS platforms provide support services as well as offering low subscription costs. Typically, they take a cut ranging from 20 per cent – 40 per cent of any ransoms collected.

The increased use of these cybercrime tools has led to a surge in malicious activity on the web as well as an escalation of the losses associated with these crimes. Furthermore, it is not uncommon for criminals to collaborate with each other by sharing technical expertise and resources via dedicated forums in order to increase their chances of success by carrying out a range of cyberattacks. Additionally, some of these services provide threat intelligence that enables users to target specific organizations or customer segments to increase a phishing operation's chances of success. With the increasing ease of launching such attacks and their profitability, it is no wonder that hackers continue to use RaaS services despite the risks involved.

With the increasing amount of CaaS on offer on cybercrime and hacking forums, especially those hosted on the darknet, it is crucial to monitor such platforms in order to identify new threats early and rapidly share information in order to detect them and reduce the risks posed by cyberattacks.

3. BRIEF OVERVIEW OF CYBER CAPABILITIES IN THE AFRICAN REGION

In order to effectively combat cybercrime, law enforcement agencies in the African region need robust and well-structured cybercrime and cybersecurity mechanisms. Having policy, legislation, and agencies in place can provide an appropriate level of response to the broad range of cyber threats and incidents that are faced by countries worldwide and should be a key priority. The data shared by the 42 countries surveyed reveals that the majority of the countries in the African region have adequate cyber-related policy, legislation, and agencies in place to provide an appropriate level of response to the broad range of cyber threats that are faced by countries worldwide and significant priority.

However, 8 of the countries reported that they do not have a dedicated unit for handling cybercrime cases, and 7 of the countries stated that they do not have the necessary cybercrime legislation in place. With weak cybercrime legislation – non-existent in certain countries – criminals can operate with impunity, because even if they are discovered, they are not prosecuted or extradited to countries with stricter laws.

In order to keep pace with the evolving nature of cybercrime and criminal acts that target computer systems, it is highly recommended that the countries in the African region continue to review existing cybercrime legislation and keep it up-to-date with the latest technological progress.

It is also recognized that dedicated cybercrime units may arguably have the biggest impact on the prevention, detection, investigation, and prosecution of cybercrime for citizens and businesses. Indeed, in terms of providing a visible service to the public and meeting their expectations and needs, a dedicated cybercrime investigation unit is an integral part of any governmental response.

With the increased use of technology comes an increased risk of criminals misusing such technology. This fact is widely recognized by all the relevant institutions. While a majority of the law enforcement agencies in the African region have established or strengthened Cybercrime Unit(s) in order to tackle cybercrime, it is clear that there are still capability limitations within these units in terms of handling sophisticated acts of cybercrime. Furthermore, the African region covers a large geographical area, and there are limited outreach efforts in terms of improving the capabilities of Cybercrime Investigators at a provincial and district level.

In an environment where there is a thriving economy, there are several options that the relevant law-enforcement agencies in the African region and other government stakeholders could consider. An integrated and coordinated cybercrime strategy or action plan can help to create the vision, goals, and priorities needed to better combat cybercrime: directly, through the provision of a law-enforcement response, and indirectly via cross-Government working and by developing partnerships with the public and private sector, domestically and internationally, to create a resilient and reliable cyber environment.

The aim is to avoid duplicate work being undertaken and to tackle issues such as those relating to internet content and regulation, to provide a long-term strategic enabling framework through which to examine the challenges and opportunities we face, and ultimately to identify priority areas where nations should be focusing their efforts in terms of cyber security and combating cybercrime for the benefit of all stakeholders (such as cybercrime prevention and promoting good cyber hygiene and security practices among the general public). The rate of cybercrime and cyber-enabled crime is increasing globally, and law enforcement agencies across the world are aware of this, often making significant investments in large numbers of cases and expanding cybercrime investigation units.

At a management level, it has been acknowledged that a dedicated cybercrime unit may arguably have the utmost impact on the prevention, detection, investigation, and prosecution of cybercrime for the benefit of citizens and businesses. Indeed, in terms of providing a visible service to the public and meeting their expectations and needs, a dedicated cybercrime investigation unit is an integral part of any governmental response.

LEAs should also consider investing in strengthening their capacity to combat cybercrime and cyber-enabled crime and increase the efficacy of Cybercrime Investigation Divisions/Units and other Investigation Divisions, for example by:

- Reviewing cyber-related investigation unit and digital forensic unit capabilities
- Enabling tools such as Big Data Analytics and crypto-tracing
- Building external relationships with major industry entities for better information sharing and the exchange of expertise
- Developing SOPs for investigations and forensic examinations
- Centralizing digital forensics tools using a service centre model that serves all parts of the policing agency, with benefits in terms of knowledge transfer and individual specialization, and efficiency gains in terms of procurement
- For scalability, an e-learning platform comprising cybercrime and digital evidence content should be developed.

Prevention will always be the first and best line of defence against cyber criminals. Like any other criminal activity, those most vulnerable tend to be the first targeted. Education and awareness will go a long way in helping the vulnerable to protect themselves against many types of cybercrime.

While the majority of the countries in the African region have set up cybercrime awareness and prevention initiatives of some kind, 10 of the countries stated that they do not have any form of cybercrime prevention-related initiatives. More can be done in this area to obtain the best outcomes. Given that there a large proportion of the population uses social media platforms such as Facebook, WhatsApp, Instagram, Twitter etc., it may be also beneficial to have a dedicated page where law enforcement agencies can give crime prevention advice to the public and gather information on cybercrimes.

4. WAY FORWARD: PROACTIVE ACTION AGAINST EVOLVING CYBER THREATS IN THE AFRICAN REGION

We have discussed the various types of cyberthreats and trends that pose a risk to the African region, but we also need greater awareness and understanding of the threats the region will need to respond to in the future. Cyber strategies tend to focus on reactive measures to prevent cyberattacks such as ransomware, phishing, BEC, and malware attacks.

However, because cybercriminals primarily operate, sell, and share knowledge on the Dark Web, law-enforcement agencies and corporate cybersecurity teams need to be proactive in collecting and analysing external threat intelligence and seeking out cyberthreats before they manifest into attacks.

Intelligence gathering is a vital piece of the puzzle, and INTERPOL provides support to its member countries in this area to successfully curb the impact of evolving cyberthreats by establishing capabilities such as the African Cybercrime Operations Desk. The African Cybercrime Operations Desk, supported by INTERPOL's Cyber Intelligence Unit, shares intelligence on cyberthreats and coordinates joint operations involving private and public entities. Knowing how threat actors will attack and when they plan to do so is crucial to thwarting a cyberattack at the start of the cyber kill chain.

In today's increasingly digital world, the sooner countries are aware of a threat, the sooner they can take steps to mitigate the risks and neutralize any cyberthreats they face.

Additionally, law-enforcement agencies need to improve their collective efforts in terms of intelligence-sharing and implementing a joint operational framework in order to successfully combat cybercrime in the African region.

Whilst the law-enforcement agencies in the African region have established good relationships and bilateral cooperation arrangements for tackling traditional types of crime, an operational framework to deal with cybercrime is lacking.

To improve the effectiveness of intra- and interregional joint operations, the African Cybercrime Operations Desk has established an operational framework known as the Joint Operational Framework for Improving Coordinated Action against Cybercrime in African region.

This framework will guide INTERPOL-led operations with the law-enforcement community in the African region, setting out how to formulate, coordinate, and communicate joint operations in order to ensure the effective and timely exchange of information. The framework specifically calls for effective cooperation between law-enforcement communities, other international/intergovernmental organizations, and the private sector.

With the development of new policies and legislative frameworks in African countries, this framework will be a living document, and as such will adopt new developments in order to remain relevant and keep up with prevailing regional and international norms.

5. AFRICA CYBERCRIME OPERATIONS DESK ANNUAL PLANNING CYCLE

To achieve its intended purpose, the Africa Joint Operational Framework proposes a four-phase annual planning cycle for the Africa Cybercrime Operations Desk in order to promote a coherent and methodological approach to improve proactive coordinated operations against cybercrime in the region.

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 in/against the community in the African region. The Africa Cybercrime Operations Desk will use 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 to produce the African Cyberthreat Assessment Report, which will help law enforcement communities in Africa gain a better understanding of the cyberthreat landscape in the country.

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 develop and update their investigation strategies and investigation approach, and steer regional prioritization of operational efforts undertaken jointly with INTERPOL for the year ahead. Africa is a diverse region, and each country has its own unique challenges; the African Cybercrime Operations Desk will therefore involve each country's Head of Cybercrime during this phase (with authorization from the relevant NCB) in order to explore opportunities for both intra- and interregional collaboration. By the end of this phase, a regional roadmap based on an agreed joint strategy and 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 execute 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 for the following: (1) planning and analysis; (2) organization; (3) tactics; and (4) evaluation. The STP is then shared with participating countries for endorsement.

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

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

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 volatile nature 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 member countries with their own investigations. As far as possible, 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 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. Intelligence collected during Phase III will also be evaluated in order to improve regional understanding of the prevalent cyberthreats and inform the subsequent African Cyberthreat Assessment Report.

INTERPOL

INTERPOL Global Complex for Innovation
18 Napier Road
Singapore 258510

FOLLOW US:

INTERPOL

INTERPOLHQ

INTERPOL_HQ

@INTERPOL_HQ

INTERPOL HQ

www.interpol.int