INTERPOL

AFRICAN CYBERTHREAT ASSESSMENT REPORT

INTERPOL'S KEY INSIGHT INTO CYBERCRIME IN AFRICA

October 2021

TABLE OF CONTENTS

FOREWORD

The impact of cybercrime is far-reaching and extends beyond national boundaries. Coupled with increased reliance on online activities during the COVID-19 pandemic, it poses a formidable challenge to security worldwide. What exacerbates the situation is the 'gap' in law enforcement cyber capabilities within and across regions. This gap is a key enabler for criminal opportunities, networks and infrastructure.

In recognition of this challenge, INTERPOL is supporting its 194 member countries in enhancing their law enforcement capabilities and capacity to combat cybercrime. INTERPOL offers a number of tools, platforms and operational support, with a view to connecting police and creating a safer world. In particular, INTERPOL's Global Cybercrime Programme has been pivotal in leading the global law enforcement response against cybercrime.

Partnership has been at the heart of these efforts. Collaboration with the various actors in the global cybersecurity ecosystem is crucial. Their diverse views, expertise and datasets can help shape effective policies and operational responses to cybercrime. Partnership also allows us to pool our wisdom so we can be resilient and agile in times of uncertainty.

Leveraging this partnership framework, INTERPOL takes a regional approach to operational coordination in combating cybercrime. Although cybercrime is a global challenge, every region responds differently. By understanding how the threats are evolving and what kind of harm they are causing in each region, we can defeat them more effectively.

With this in mind, INTERPOL has drawn up this African Cyberthreat Assessment Report for member countries in Africa. The aim is to accurately assess the threat landscape so as to be able to provide tailored support. The report was produced under the aegis of the African Joint Operation against Cybercrime (AFJOC) with support from the United Kingdom's Foreign, Commonwealth and Development Office.

Looking ahead, the newly-created African Cybercrime Operations Desk under the AFJOC project will drive intelligence-led, coordinated actions against cybercrime and its perpetrators in African member countries based on this threat assessment. To effectively support the region, INTERPOL also works closely with key regional organizations such as the African Union and Afripol to maximize coordination and implementation efforts in order to boost regional capabilities and capacity in the fight against cybercrime.

I trust that this report will help close the gaps within Africa and beyond, and contribute to the effectiveness of the global law enforcement response. We thank the member countries in Africa and our partners for their strong commitment in this endeavour.

Stephen Kavanagh
Executive Director of Police Services
INTERPOL

FOREWORD

The African continent has huge potential in terms of information and communication technologies, especially because of the youth of its population. Indeed, about 60% of the African population in 2020 is under 25 years old. This factor is driving strong growth in the use of new technologies.

However, we are also witnessing an upsurge in activities related to Cybercrime, especially in this COVID-19 pandemic period. The loss of jobs related to this pandemic and the low economic growth recorded has opened up opportunities for criminal organizations. Hence the special attention that the African Union Commission is paying to the fight against all forms of organized crime: money laundering, transnational crime and cybercrime.

In terms of Internet coverage capacity and bandwidth speed, Africa remains under-served, especially in rural areas, yet it has the fastest-growing telephone and Internet networks in the world. On this young continent, every economic challenge generates an innovative solution that may sometimes, unfortunately, be at the limit of what the law allows. For example, the low rate of banking facilities for African populations has led to the creation of new financial services such as mobile banking, but also to the resurgence of new forms of scam linked to these new technologies.

Our strategy to fight cybercrime is based on three pillars:

- Raising awareness in the populations
- The reinforcement of policy, treaty and common legislation to fight cybercriminals
- The establishment of technologies on a national scale to reinforce cyber-defence

In collaboration with INTERPOL, AFRIPOL has initiated training for national police officers in protection against DNS (Domain Name Service) attacks. Also, a strategy of public-private rapprochement has been initiated in order to sign partnerships with Internet leaders and crypto-currency providers.

The Internet has abolished borders. A cyber-attack launched in Africa may have a direct or indirect impact on any citizen anywhere in the world. This fight is a long-term one and it is by being united that we will succeed in effectively defeating cybercrime in Africa and the world.

Tarek A. Sharif
Executive Director
AFRIPOL

ABBREVIATIONS AND ACRONYMS

AFJOC	African Joint Operations against Cybercrime
BEC	Business Email Compromise
CA	Communication Authority
CCP	Cybercrime Collaborative Platform
CD	Cybercrime Directorate
CNP	Card not present fraud
CKE	Cybercrime Knowledge Exchange
CSA	Cyber Security Authority
CTR	Cyber Threat Response Team
DDoS	Distributed Denial-of-Service
FCDO	Foreign, Commonwealth and Development Office
FCU	Financial Crime Unit
Gbps	Gigabytes-per-second
ISPA	INTERPOL Support Programme for the African Union
ISS	Institute for Security Studies
LEA	Law Enforcement Agencies
M.O.	Modus Operandi
NPF	Nigerian Police Force
OCG	Organized Crime Group
PII	Personal Identifiable Information
RAT	Remote Access Trojans
SABRIC	South African Banking Risk Information Centre
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
TTP	Tactics, Techniques and Procedures
VPS	Virtual Private Servers
VSA	Virtual System/Server Administrator

ACKNOWLEDGMENT

The African Cyberthreat Assessment Report 2021 was written by INTERPOL's Cybercrime Directorate 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. The report benefited from the data and expertise of INTERPOL's private partners, namely Group-IB, Kaspersky, Palo Alto Networks and Trend Micro.

EXECUTIVE SUMMARY

This report provides INTERPOL's insights into key cyberthreats that are affecting the African region. It also presents in-depth analysis on the impact of these threats as well as examples of INTERPOL's operational support in combating cybercrime and the regional cybercrime strategy for Africa. Based on input from the member countries in Africa and data drawn from INTERPOL's private partners, the most prominent threats were identified as below.

- **Online Scams** – For African member countries, the highest-reported and most pressing cyberthreat across the region was identified as online scamming. This threat seeks to target and take advantage of victims' fears, insecurities, and vulnerabilities through phishing, mass mailing and social engineering. Member countries have reported a sharp increase in the number of online banking scams, including instances of banking and credit card fraud.
- **Digital Extortion** – This threat is also identified as one of the most prominent cyberthreats within the region. Digital extortion seeks to target individuals with either allegations of sexually compromising images or through direct blackmail campaigns. While such threats are not new on the threat landscape, the move towards a digital society – particularly within the African region – has created new attack vectors for criminals to both obfuscate their identity and target new victims.
- **Business Email Compromise** – Alongside online scams, Business Email Compromise (BEC) was identified as a significant concern and threat to the region. Businesses and organizations that rely heavily on wire transfer transactions are vulnerable to this threat in Africa. The COVID-19 pandemic has contributed to the increase in this type of cybercrime.
- **Ransomware** – The threat of ransomware is expanding across the African continent. Allegedly, more than 61% of companies in this region were affected by ransomware in 2020 alone.[1] These attacks targeted some African countries' critical infrastructure, including healthcare and maritime sectors.[2]
- **Botnets** – Botnets are networks of compromised machines used as a tool to automate large-scale campaigns such as DDoS attacks, phishing, malware distribution, etc. The number of botnet victim detections in Africa was around 50,000, with a monthly average detection of 3,900. In Africa, there have been numerous high-profile instances of such DDoS attacks on critical infrastructure within the past five years.

Recognizing the need for a change in the approach to cybercrime within Africa as a region that is embracing digital transformation, the report concludes with INTERPOL's regional cybercrime strategy to support member countries in Africa. The strategy encompasses the four strategic objectives below:

- **Enhancing cybercrime intelligence for effective responses to cybercrime**;
- **Strengthening cooperation for joint operations against cybercrime;**
- **Developing regional capacity and capabilities to combat cybercrime;**
- **Promoting good cyber hygiene for a safer cyberspace.**

INTERPOL stands ready to support African member countries in fulfilling these objectives and further developing a joint operational framework to improve coordinated actions against cybercrime in Africa. Collective efforts in sharing intelligence and formulating a joint operational framework will boost regional capabilities and capacity in the fight against cybercrime.

---

1 Lumu, 2020 Ransomware Flashcard, Available at: [https://lumu.io/resources/2020-ransomware-flashcard/]

2 Institute for security Studies, Africa can't risk a major maritime cyber-attack. Reva, D., 28 October 2020. Available at: [https://issAfrica.org/iss-today/Africa-cant-risk-a-major-maritime-cyberattack]

1. INTRODUCTION

Africa has more than 500 million Internet users, placing the region ahead of other regions such as North America, South America, and the Middle East.[3] This volume of users relative to population equates to about 38%, which implies the number is expected to grow in the coming years, given the accelerated digitalization. The leading countries are Kenya with 83% of its population being online, Nigeria with 60% and South Africa with 56%.[3] Mobile banking in particular is noted to be used widely within these three countries, contributing to Africa's active role in digital financial services.[4] It poses a significant future threat, with the rise in malicious apps on mobile devices exploiting increasing vulnerabilities.

Despite the high demand for online mobile banking, the digital divide remains a challenge, especially as the member countries in Africa move forward to incorporate digital infrastructure into the foundations of their society, including government, banking, business and critical infrastructure. This transformation highlights the urgent need to ensure cybersecurity parameters and standards meet the demands and future needs of this community, including financial inclusion.[5]

However, the absence of these standards is pervasive in Africa. 90% of African businesses are operating without the necessary cybersecurity protocols in place.[6] Without these protocols, threat actors are able to exploit increasing vulnerabilities as they continue to invent new cyberattack vectors. This leads to significant financial loss. In 2016, cybercrime has cost the Kenyan economy about 36 million USD, the South African economy 573 million USD and the Nigerian economy 500 million USD.[7] A research study from Deloitte indicated the financial loss for financial institutions in Kenya, Rwanda, Uganda, Tanzania, and Zambia since 2011 to be more than 245 million USD.

> ***"More than 90% of African businesses are operating without the necessary cyber security protocols in place."***
>
> Source: CGTN

In the past year, the COVID-19 pandemic has accelerated the cybercrime ecosystem,[8] with a persisting digital divide and increasing cybersecurity vulnerabilities across the region. Similarly to other regions,

---

3 Council on Foreign Relations, Last Month, Over Half-a-Billion Africans Accessed the Internet, Campbell, July 2019. Available at: [https://www.cfr.org/blog/last-month-over-half-billion-Africans-accessed-internet]

4 Cision, Africa Leads World in Digital Financial Services Deployments with Prepaid Cards an Important Part of Mix, Says Axiom Prepaid Holdings Reps, June 2020. Available at: [https://www.prweb.com/releases/Africa_leads_world_in_digital_financial_services_deployments_with_prepaid_cards_an_important_part_of_mix_says_axiom_prepaid_holdings_reps/prweb17214821.htm]

5 International Finance Corporation, Digital Access: The Future of Financial Inclusion in Africa, 2018. Available at: [https://www.ifc.org/wps/wcm/connect/region__ext_content/ifc_external_corporate_site/sub-saharan+africa/resources/201805_report_digital-access-africa]

6 CGTN, Rights group launches tool to stem cybercrime in Africa, Odonkor, A, 27 October 2020. Available at: [https://news.cgtn.com/news/2020-10-27/Unveiling-the-cost-of-cybercrime-in-Africa-UVhmu1PJeM/index.html.]

7 Scidenet, Cybercrime in Africa: Facts and figures. Fassassi, Akoussan, July 2016. Available at: [https://www.scidev.net/sub-saharan-Africa/features/cybercrime-Africa-facts-figures/]

8 Symantec, Cybercrime and Cyber Security Trends in Africa. November 2016. Available at: [https://www.thehaguesecuritydelta.com/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf]

the African region experienced attacks against critical infrastructure and frontline services during the pandemic. This was most prominently seen in South Africa and Botswana. For instance, South Africa's Life Healthcare Group, responsible for managing 66 health facilities, was hit by a serious and sustained cyberattack.[9]

Indeed, the growing rate of digital transformation within the African region is facilitating the emergence of new attack vectors and opportunities for cybercriminals. In recognition of the magnitude of the problem caused by cyberthreats in Africa, the next section provides in-depth analysis on the cybercrime threat landscape in Africa.

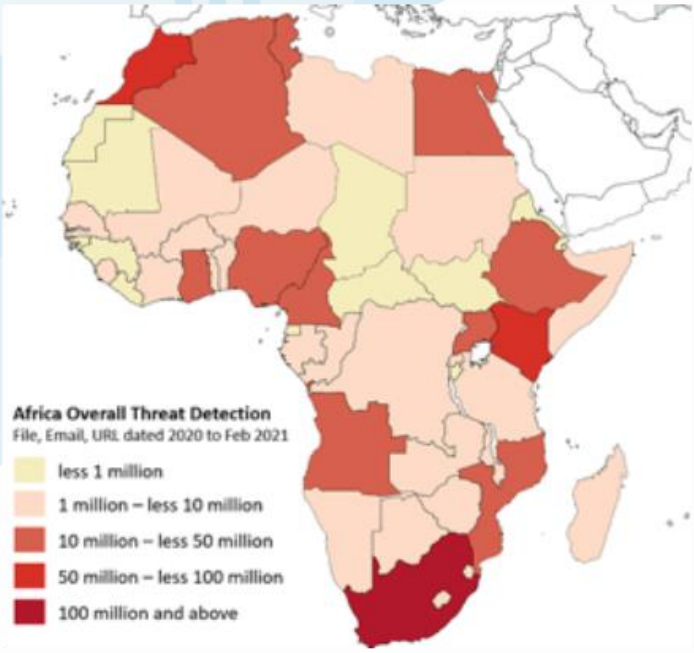


Figure 1. Overall detection of cyber threats in Africa using Trend Micro sensors (Source: Trend Micro)

Research from a Kenyan IT cybersecurity company, Serianu, highlighted that cybercrime reduced GDP within Africa by more than 10%, at a cost of an estimated 4.12 billion USD in 2021.[10] INTERPOL's partner, Trend Micro, recorded millions of threat detections in Africa from January 2020 to February 2021:

- Email: 679 million detections
- Files: 8.2 million detections
- Web: 14.3 million detections

More specifically, South Africa had 230 million threat detections in total, while Kenya had 72 million and Morocco 71 million. In South Africa, 219 million detections were related to email threats. South Africa also had the highest targeted ransomware and BEC attempts.

The exploitation of these vulnerabilities within South Africa was further highlighted by Accenture, who identified that South Africa has the third highest number of cybercrime victims worldwide, at a cost of R2.2 billion a year.[11] The scale of this cyber criminality is further evidenced when we consider that the country has seen a 100% increase in mobile banking application fraud and is estimated to suffer 577 malware attacks an hour.[12] Such malware attacks are one of the emerging threats.

With the diversified and evolving attack vectors and the targeted approach against frontline response organizations, global supply chains and critical infrastructure, there has never been a more crucial time to both chart a way forward and ensure that efforts are focused on improving security and safety in cyberspace for all African member countries.

---

[9] Cybercrime Magazine, Cybercrime To Cost The World $10.5 Trillion Annually By 2025, Morgan, S., 13 November 2020. Available at: [https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/]

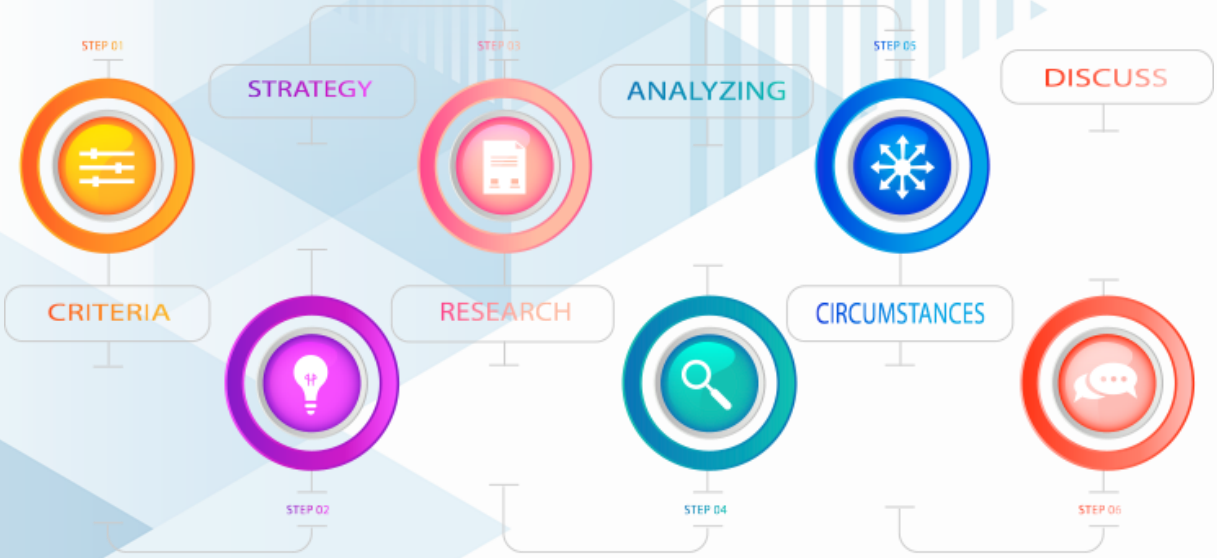
[10] Physorg, Rights group launches tool to stem cybercrime in Africa. Available at: [https://phys.org/news/2021-05-rights-group-tool-stem-cybercrime.html]

[11] Accenture, Insight into the cyber threat landscape in South Africa, 27 May 2020. Available at: [https://www.accenture.com/za-en/insights/security/cyberthreat-south-Africa]

[12] Business Insider South Africa, Hackers on the dark web love South Africa – here's why we suffer 577 attacks per hour, 23 June 2020. Available at: [https://www.businessinsider.co.za/sa-third-highest-number-of-cybercrime-victims-2020-6].

1.1 Methodology

To conduct this assessment, INTERPOL has sought input from its member countries in Africa and a total of 22 member countries out of 55 have responded to the survey providing their national views on cyberthreats. INTERPOL has also received relevant data from its private partners including Group-IB, Kaspersky, Palo Alto Networks and Trend Micro. The collected information has been combined with internal detections and analysis by INTERPOL Cybercrime Directorate, and an open-source review of information, data and assessments relevant to this region. This multi-stakeholder approach has formulated a comprehensive assessment of the cyberthreat landscape within the region.



The creation of the AFJOC project in March 2021 was a catalyst for developing this report in terms of outreach and coordination with INTERPOL's African member countries. Based on the assessment result, the AFJOC project will develop an operational framework within the region to provide a framework for consideration by member countries when developing governance policies, roles and responsibilities, procedures, communications and capacity development. In delivering this, collaboration with the key regional organizations is crucial, such as The African Union and Afripol. The ISPA project underpins these relationships, collaborations and potential synergies.

AFRICA

JOINT

OPERATIONS AGAINST

CYBERCRIME

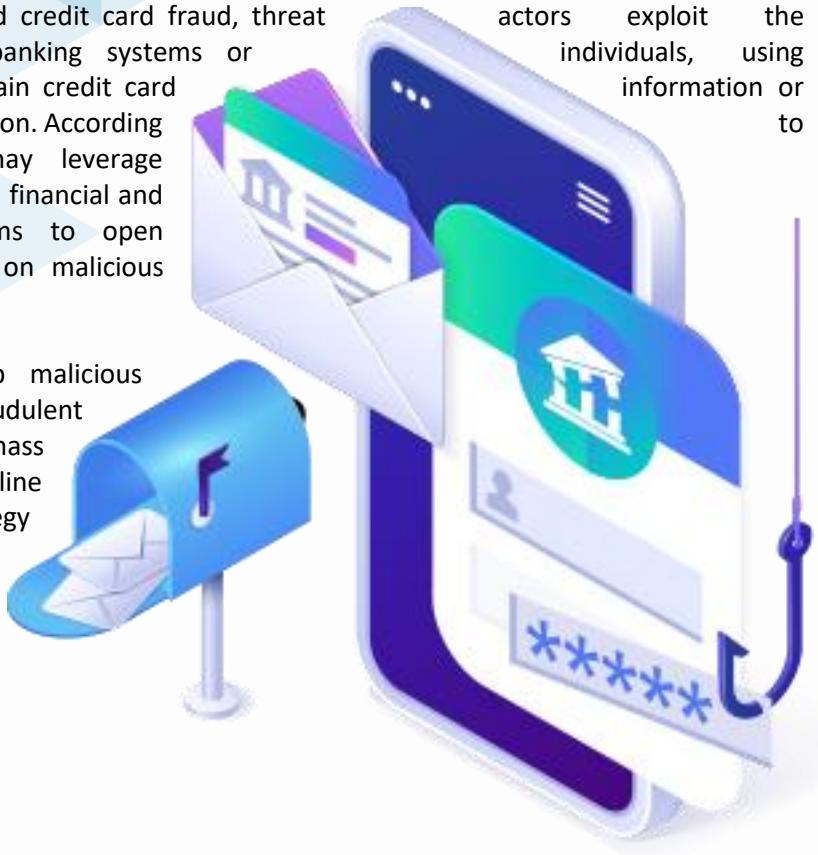
2. KEY CYBERTHREATS IN AFRICA

2.1 Online Scams

ONLINE SCAMS

Online scams encompass various types of fraud in cyberspace. They range from, inter alia, phishing, credit card theft, identity theft, advance payment fraud, card-not-present (CNP) fraud and cryptocurrency scams. They typically seek to exploit victims' fears, insecurities or vulnerabilities while using numerous tactics, techniques, and procedures (TTPs) online. Complex organized crime groups often run bespoke sophisticated malware tools to make illicit financial gains from unsuspecting victims.

The most common type of online scam is phishing. It can be facilitated by emails, SMS, phone calls or a phishing kit.[13] For banking and credit card fraud, threat actors exploit the vulnerabilities of unpatched banking systems or individuals, using social engineering tactics to obtain credit card information or access to online banking information. According to Kaspersky, phishing emails may leverage scenarios such as delivery, postal, financial and HR services, convincing victims to open malicious attachments or click on malicious links.[14]



Online scammers also set up malicious domains to facilitate fraudulent activities. They may make use of mass phishing tools or kits. Online scamming is a cost-effective strategy adopted by threat actors, as there are minimal technical requirements and low start-up costs.

[13] A phishing kit is a tool purchased by one threat actor from another to allow for mass facilitation of phishing campaigns.

[14] Kaspersky, The year of social distancing or social engineering? Phishing goes targeted and diversifies during COVID-19 outbreak, August 2020. Available at: [https://www.kaspersky.com/about/press-releases/2020_the-year-of-social-distancing-or-social-engineering]

Situation in Africa

According to African member countries, the most prevalent and pressing cyberthreat is online scams. In particular, banking and credit card fraud is recognized as a serious threat in Africa. It involves the theft of personal data and banking details which are then used by a threat actor to either purchase goods, siphon funds or sell on markets. Coupled with the COVID-19 pandemic and its impact on the cybercrime landscape, Africa saw a sustained increase in the volume of cyberattacks,[15] including the 238% rise in cyberattacks on online banking platforms in 2020.[16]

At the same time, threat actors in Africa are deploying Trojan information stealers such as Agent Tesla, Lokibot, Fareit and others to commit online scams. Many cybercriminals offer toolkits as a service and training available online has contributed to the continuous operations and development of cybercriminals.

Considering the broader online scam situation across the African region, data received from Trend Micro indicates that 27% of its web threat detection in Africa related to online scams in May 2021, as shown in Figure 2 below.

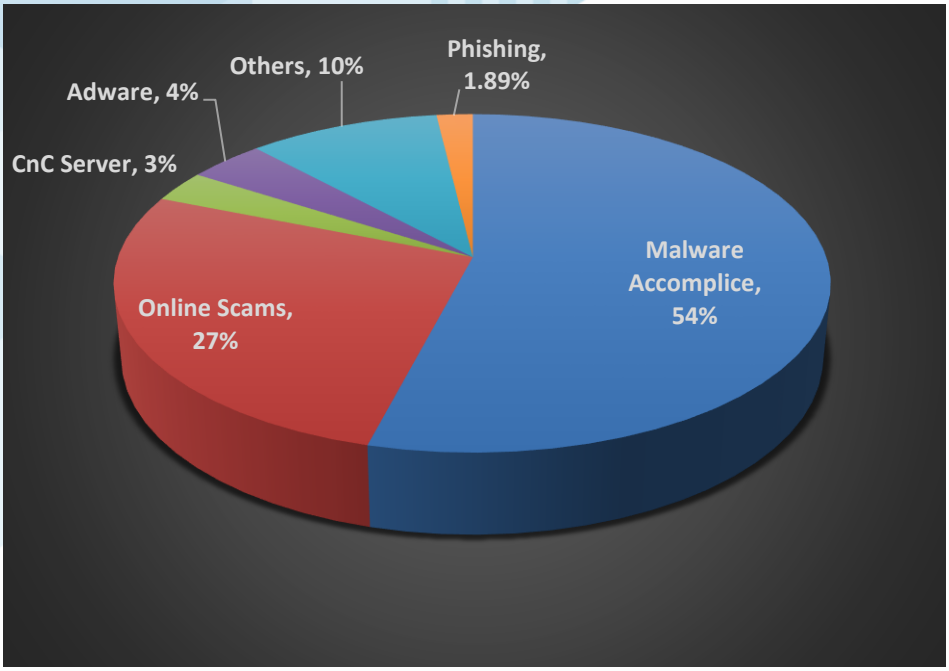


Figure 2. Top Web Threat Detection in Africa in May 2021 only (Source: Trend Micro)

The South African Banking Risk Information Centre (SABRIC) evidenced that "gross fraud losses on South African issued cards increased by 20.5% from 2018 to 2019" with CNP fraud and banking malware attacks, behind only Russia.[17] Yet this number fails to take into account the influx of COVID-19 related phishing attempts and the financial, emotional and mental impact they have on victims. Stolen data from carding scams is auctioned off to the highest bidder or sold within underground forums – meaning unsuspecting victims of credit card fraud in the African region may have their credit card information misused globally following the breach.

[15] INTERPOL, INTERPOL report shows alarming rate of cyberattacks during COVID-19, 4 August 2020. Available at: [https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19]

[16] Institute for security Studies, Africa can't risk a major maritime cyberattack, Reva, D., 28 October 2020. Available at: [https://issAfrica.org/iss-today/Africa-cant-risk-a-major-maritime-cyberattack]

[17] Accenture, Insight Into The Cyber Threat landscape in South Africa, 2020. Available at: [https://www.accenture.com/_acnmedia/PDF-125/Accenture-Insight-Into-The-Threat-Landscape-Of-South-Africa-V5.pdf]

According to the KnowBe4 African Report 2019[18] with over 800 respondents across South Africa, Kenya, Nigeria, Ghana, Egypt, Morocco, Mauritius and Botswana, phishing was one of the top cyber threats faced by the African region. 28.14% of respondents reported that they had previously clicked on a phishing email, 27.71% had previously fallen for a scam, and 19% had forwarded a spam or hoax email. INTERPOL's private partner Kaspersky detected that South Africa, Kenya, Egypt, Nigeria, Rwanda and Ethiopia had about 2 million phishing attempts in 2020 alone.[19]

Another growing concern for African member countries is cryptocurrency scams, in which threat actors seek to defraud victims of their cryptocurrency. An ISS report has highlighted two examples of cryptocurrency investment scams in South Africa.[20] These examples involved, firstly, a Ponzi scheme where thousands of investors were allegedly scammed out of 588 million USD in Bitcoin by the company Mirror Trading International in 2020. The second case was where the two founders of the trading company Africrypt allegedly absconded with 3.6 billion USD from investors in April 2021.

South Africa was therefore one of the top ten countries globally where threat actors received the highest volume of cryptocurrency from illicit addresses. In addition to investment scams, a growing threat in the cryptocurrency space is that of wallet phishing, where threat actors utilize false or misleading advertisements, imposter domains, fake wallet or decentralized finance platforms to obtain a victim's cryptocurrency wallet private keys, thus enabling them to steal funds from the victim's accounts.

[18] Knowbe4, African Cybersecurity Research Report, 2019. Available at: [https://www.knowbe4.com/hubfs/African%20Cybersecurity%20Research%20Report.pdf]

[19] Creamer Media's Engineering News, Phishing attacks in Africa diversify, target small companies, Burger, S., August 2020. Available at: [https://www.engineeringnews.co.za/article/phishing-attacks-in-Africa-diversify-target-small-companies-2020-08-21]

[20] Institute for Security Studies, Africa: new playground for crypto scams and money laundering, Chelin, R., August 2021. Available at: [https://issafrica.org/iss-today/africa-new-playground-for-crypto-scams-and-money-laundering]

2.2 Digital Extortion

DIGITAL EXTORTION

What is digital extortion?

One of the most prevalent cyberthreats in Africa was reported to be digital extortion involving blackmailing and sextortion. It involves threat actors coercing individuals with either false claims or proof of stolen personal data or files, for which the victim is then asked to pay in exchange for recovering the data or not leaking it online. More specifically, sextortion threat actors utilize phishing and blackmail across multiple platforms to get money from their victims, with claims that they have obtained compromising sexual images or the sexual browsing history of their victim.

INTERPOL's analysis identified the most common modus operandi for digital extortion as being where threat actors rent Virtual Private Servers (VPS) with a Simple Mail Transfer Protocol (SMTP) service to launch bulk extortion emails. Within these digital extortion emails, threat actors often claim to have compromised the security of the victims' computers, files or history.

Cyber blackmail can also be combined with social engineering techniques that seek to research their victims and take advantage of Personally Identifiable Information (PII) that victims leave online in social media posts, or from previous data breaches that have been released on either open or dark Web forums, as threat actors use increasingly sophisticated techniques to create personalized extortion messages for each victim.

Similarly, the modus operandi for sextortion can also involve false claims about access to individuals' webcams or browsing history, and then be followed up with demands for payment in crypto to prevent this information being leaked to close friends or publicly. While such claims are often mass-produced, sextortion activities have also been detected in apps, where threat actors will trick unsuspecting victims, who are usually male, to pre-record or send videos of themselves performing sex acts to what they believe are females, with the threat actors then threatening to release the footage unless the victim pays a financial sum.[21]

(Graphic Source: Financial Post)

[21] Trend Micro and INTERPOL, Cybercrime in West Africa; Poised for an Underground Market, 2017. Available at: [https://documents.trendmicro.com/assets/wp/wp-cybercrime-in-west-Africa.pdf]

Situation in Africa

Pivoting from the understanding of digital blackmail via extortion, data provided from INTERPOL's private partner Trend Micro identified some IP addresses in Africa that were used to send out digital extortion spam messages. From January 2021 to May 2021, the count of unique IP addresses is about 10.6% of the overall number. The top sender countries include South Africa, Morocco, Kenya and Tunisia. The IP addresses can be from botnet networks or dedicated VPSs rented by the cybercriminals.

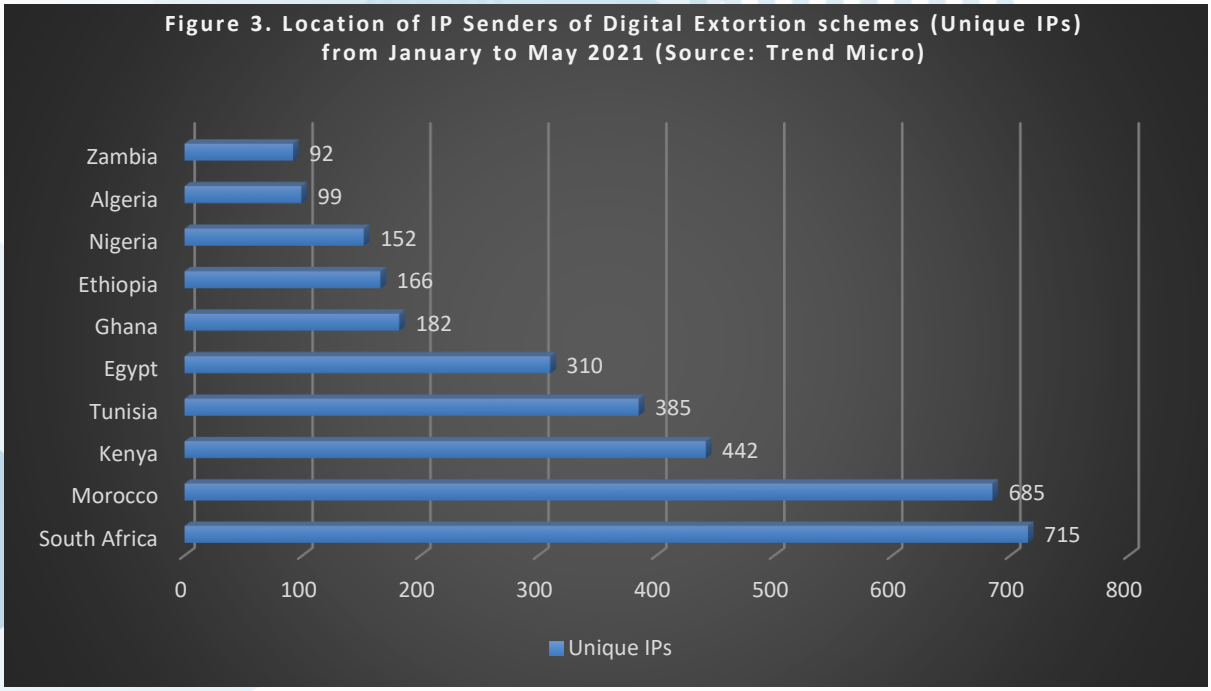
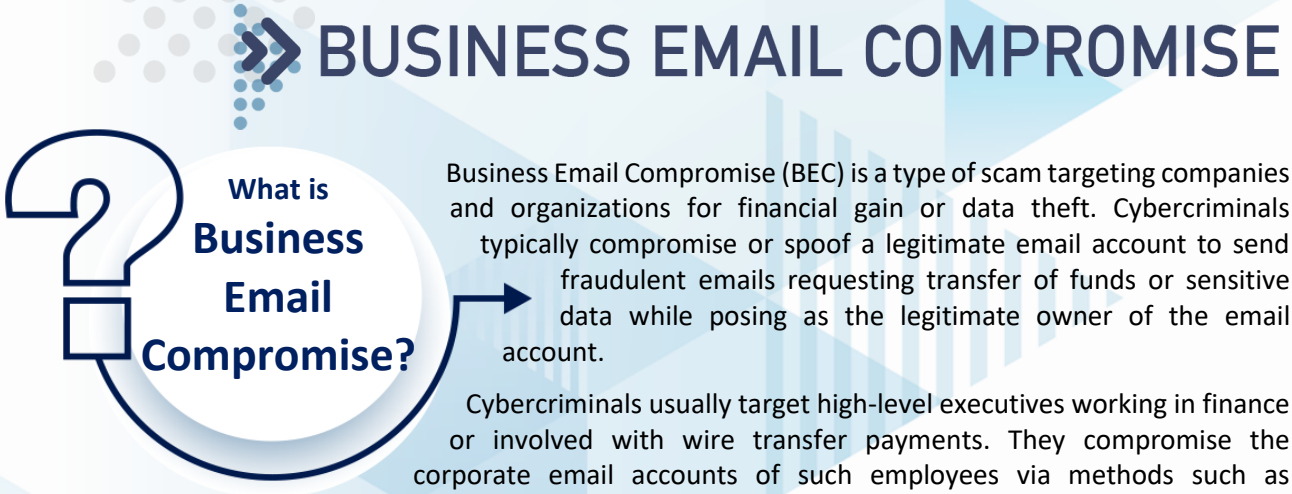


Figure 3. Location of IP Senders of Digital Extortion schemes (Unique IPs) from January to May 2021 (Source: Trend Micro)

This Trend Micro telemetry data is in line with the volume of digital extortion schemes reported by African member countries to INTERPOL, which made them one of the highest reported cybercrimes within the region.

2.3 Business Email Compromise

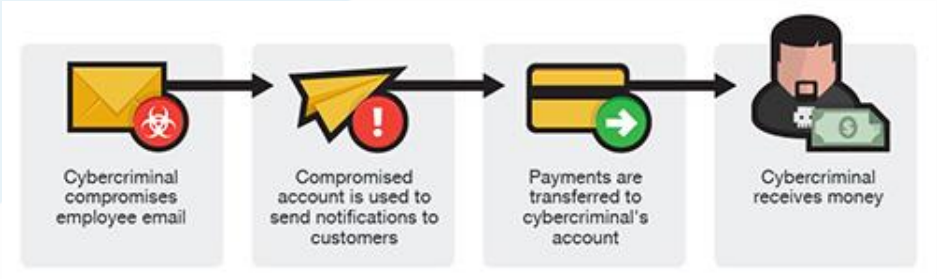


Business Email Compromise (BEC) is a type of scam targeting companies and organizations for financial gain or data theft. Cybercriminals typically compromise or spoof a legitimate email account to send fraudulent emails requesting transfer of funds or sensitive data while posing as the legitimate owner of the email account.

Cybercriminals usually target high-level executives working in finance or involved with wire transfer payments. They compromise the corporate email accounts of such employees via methods such as keylogging or phishing attacks, or simply spoof their emails to appear as though it is sent from the target's legitimate email account. Fraudulent emails are then sent from these email accounts with an established level of trust to other employees or related individuals, asking them to transfer funds or data to a specific bank account. The three types of BEC scam are illustrated in the diagrams below, developed by Trend Micro.

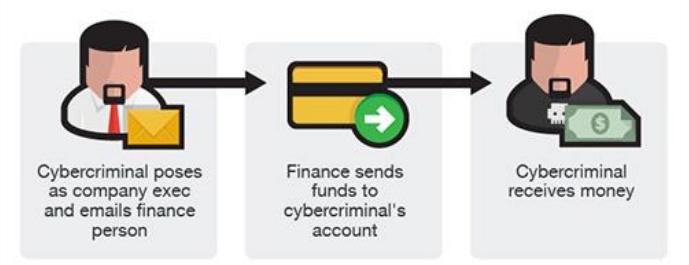
Bogus Invoice Scheme

The Bogus Invoice Scheme usually involves a business that has an established relationship with a supplier. The fraudster asks for invoice payment monies to be wired to an alternative, fraudulent account via a spoofed email, telephone, or fax message.



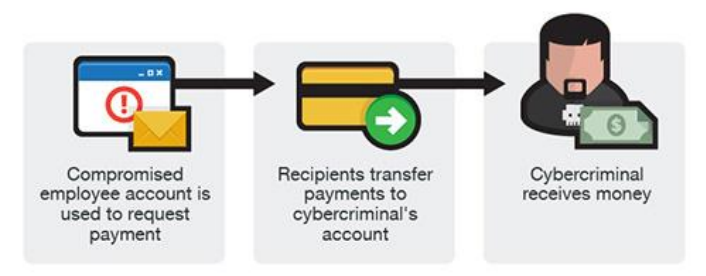
CEO Fraud

In CEO Fraud, the fraudsters identify themselves as high-level executives (CFO, CEO, CTO, etc.), lawyers, or other types of legal representative, and purport to be handling confidential or time-sensitive matters and initiate a wire transfer to an account they control. In some cases, the fraudulent request for wire transfer is sent directly to the financial institution with instructions to urgently send funds to a bank. This scam is also known as "CEO Fraud", "Business Executive Scam", "Masquerading", and "Financial Industry Wire Fraud".



Account Compromise

In Account Compromise cases, an employee's email account is hacked and then used to make requests for invoice payments to fraudster-controlled bank accounts. Messages are sent to multiple vendors identified from the employee's contact list. The business may not become aware of the scheme until their vendors follow up to check the status of the invoice payment.



To assist individuals and organizations further in avoiding BEC, the FBI has also published a list of red flags and tips for recognizing and preventing such BEC attempts (see Table 1).

Unexplained urgency	Be sceptical of last-minute changes to wiring instructions or recipient account information.
Last-minute changes to wire instructions or recipient account information	Verify any changes of information via the contact on file—do not contact the vendor through the number provided in the email.
Last-minute changes to established communication platforms or email account addresses	Ensure the URL in emails is associated with the business it claims to be from.
Last-minute changes to established communication platforms or email account addresses	Be alert to hyperlinks that may contain misspellings of the actual domain name.
Communications only in email and refusal to communicate via telephone or online voice or video platforms	Verify the email address used to send emails, especially when using a mobile or handheld device, by ensuring the sender's email address appears to match who it is coming from.
Requests for advanced payment of services when not previously required	Be wary of last-minute changes to wiring instructions or recipient account information.

Table 1: Red flags and best practice and tips for avoiding BEC scams (Source: FBI)

Situation in Africa

According to Trend Micro, the proportion of BEC attempts on victims in Africa from 2020 to April 2021 was less than 1% of global BEC attempts. The top BEC attempts are in English-speaking countries such as the United States, Australia and the UK. As BEC cybercriminals usually target larger corporations which will potentially lead to bigger pay-outs, the likely reason for the lower proportion of BEC attempts in Africa is the relatively smaller concentration of large businesses and corporations there.

However, there are several offshore companies based in Africa, and the COVID-19 pandemic situation contributed to the increase in this type of cybercrime. Their employees rely heavily on wire transfer transactions, opening up more opportunities for cybercriminals to exploit. Within Africa, it was mainly detected in countries like South Africa, Tunisia, Morocco, Mauritius, Nigeria and Kenya (see Figure 4).

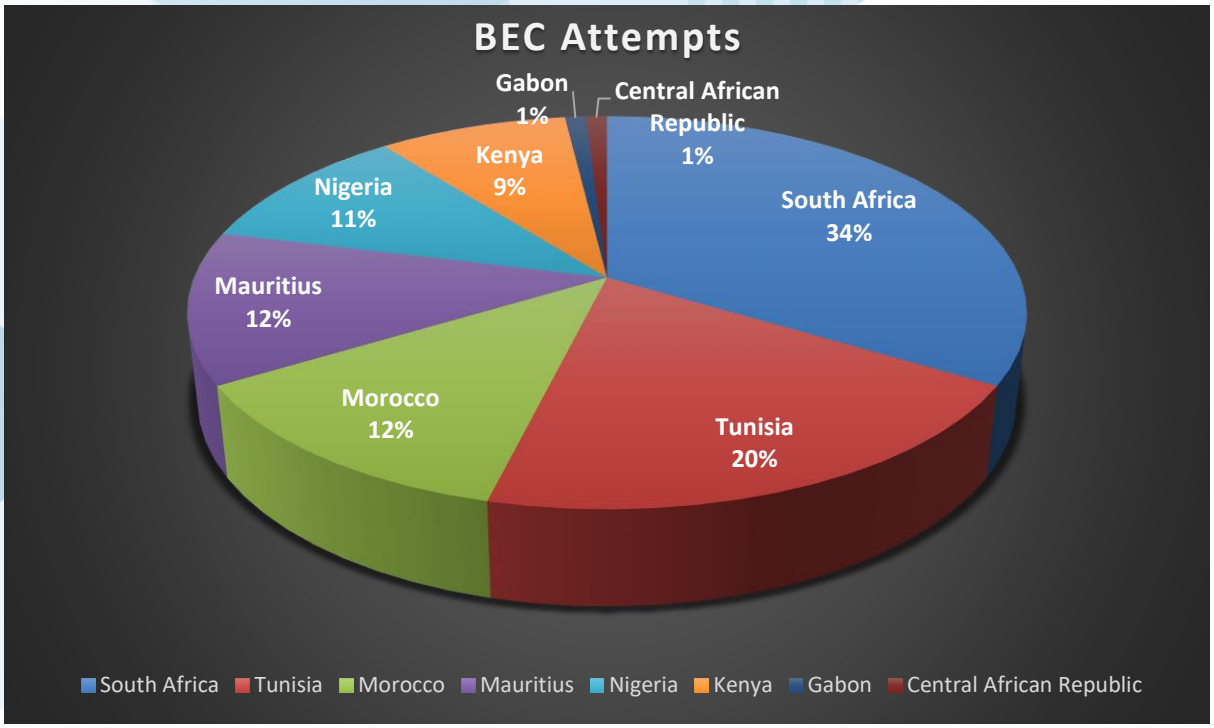


Figure 4. BEC Attempts in Africa (Source: Trend Micro)

This figure is likely to rise, given the strong potential and positive economic projections for the African region. In addition, 2020 statistics showed that African countries dominated the ranking of countries with the highest GDP growth worldwide.[22] Although COVID-19 slowed GDP growth significantly, the economic fundamentals are still in place and demonstrate the possibility that BEC actors might increasingly target the region in the hope of higher pay-outs in the future.

Meanwhile, a 2020 report from Agari's Cyber Intelligence Division (ACID) stressed that a majority (60%) of BEC actors globally were located in Africa, across 11 countries in the region. The report also found that "83% percent of African attackers, as well as 50% of global BEC actors, hailed from Nigeria".[23]

[22] Statista. African countries with the highest Gross Domestic Product (GDP) in 2020. Available at: [https://www.statista.com/statistics/1120999/gdp-of-African-countries-by-country/]

[23] Agari, The Geography of BEC. The Global Reach of the World's Top Cyber Threat, 2020. Available at: [https://www.agari.com/cyber-intelligence-research/whitepapers/acid-agari-geography-of-bec.pdf]

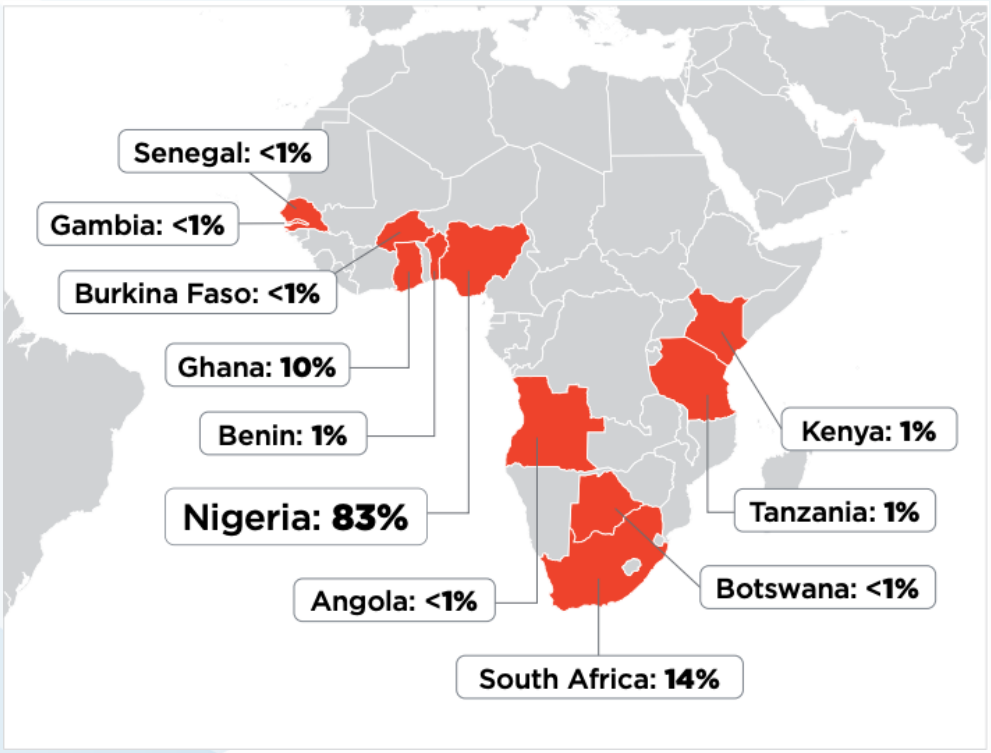
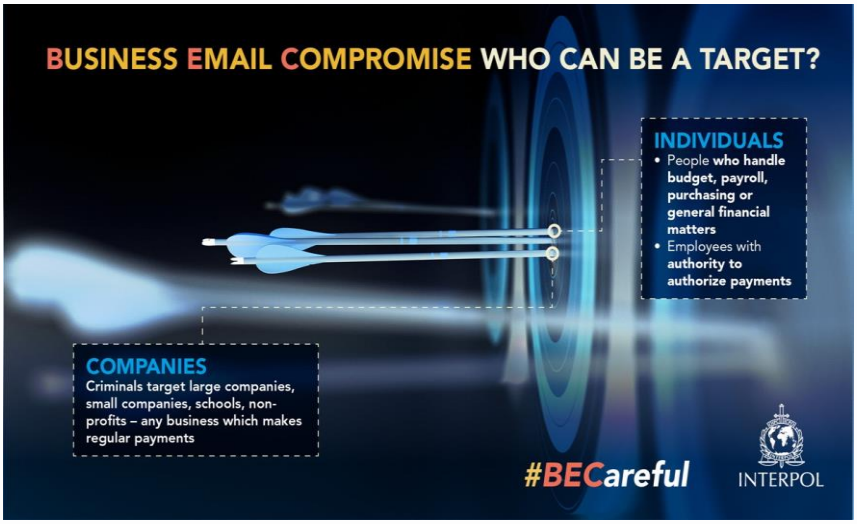


Figure 5. BEC Actor Distribution within Africa (Source: Agari)

In response to the detected high concentration of BEC actors within the Nigerian region, INTERPOL, alongside its private partner Group-IB and the Nigerian Police Force (NPF), launched the successful "Operation Falcon", which severely disrupted a prolific BEC group and led to three arrests. This proactive law enforcement action was also followed up with the arrest of another prominent group of Nigerian BEC actors in March 2021 after an investigation by the Nigerian Economic and Financial Crimes Commission.[24]

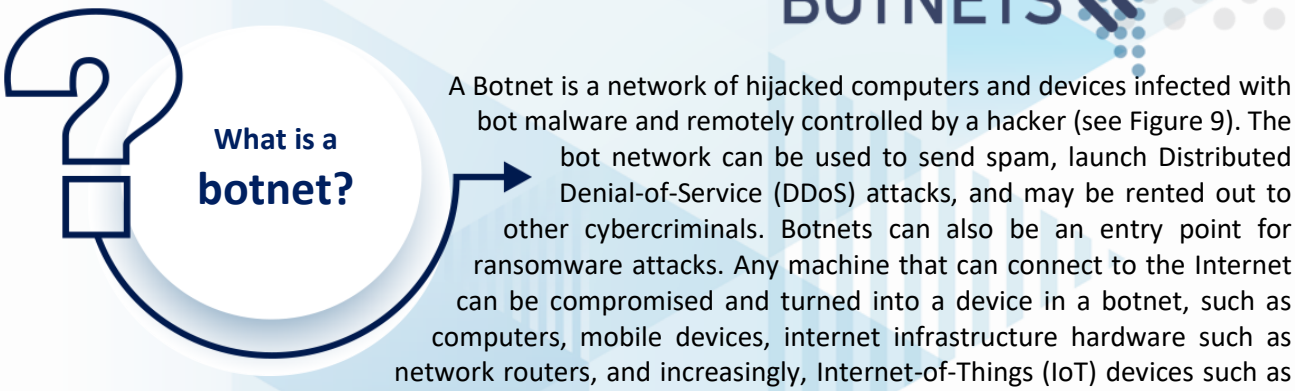
In September 2019, a month-long operation entitled "rewired", led by the FBI, disrupted and dismantled BEC schemes. It resulted in 281 arrests in Nigeria, Turkey, Ghana, France, Italy, Japan, Kenya, Malaysia, the United Kingdom and the United States. It also successfully seized nearly 3.7 million USD and recovered about 118 million USD in fraudulent wire transfers.[25] This operation was another example that demonstrated the importance of international police cooperation to effectively fight against transitional BEC schemes.



[24] Recorded Future, Suspected BEC gang arrested in Nigeria amid internet fraud crackdown efforts, 2021. Available at: [https://therecord.media/suspected-bec-gang-arrested-in-nigeria-amid-internet-fraud-crackdown-efforts/]

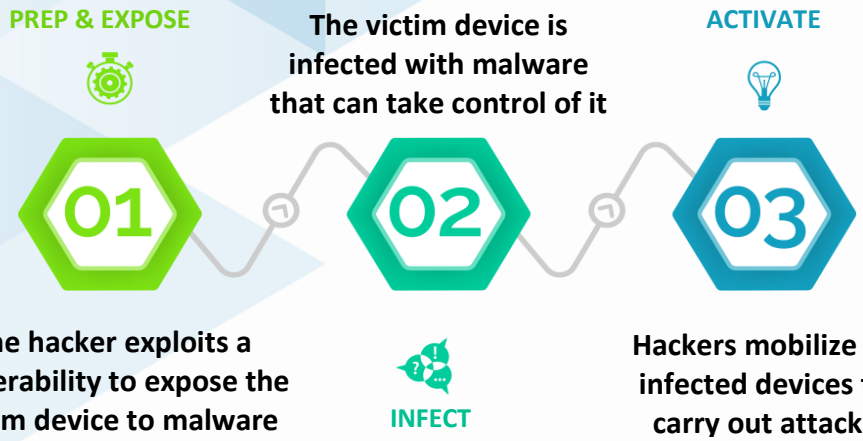
[25] FBI, Worldwide Sweep Targets Business Email Compromise, 10 September 2019. Available at: [https://www.fbi.gov/news/stories/operation-rewired-bec-takedown-091019]

2.4 Botnets



A Botnet is a network of hijacked computers and devices infected with bot malware and remotely controlled by a hacker (see Figure 9). The bot network can be used to send spam, launch Distributed Denial-of-Service (DDoS) attacks, and may be rented out to other cybercriminals. Botnets can also be an entry point for ransomware attacks. Any machine that can connect to the Internet can be compromised and turned into a device in a botnet, such as computers, mobile devices, internet infrastructure hardware such as network routers, and increasingly, Internet-of-Things (IoT) devices such as smart home devices.

According to Kaspersky, there are three stages to building a botnet:[26]



Upon activation, hackers send commands and control the botnet from a main server, known as the Command & Control (C&C) server. Older C&C models use a centralized C&C server where all commands are sent from. However, since this reduces the anonymity of the hackers, as their C&C servers can be traced, newer C&C models now use a decentralized peer-to-peer model where the hackers can send and spread commands to the entire botnet via any of the bots, thus concealing their identity.

[26] Kaspersky, What is a Botnet? Available at: [https://www.kaspersky.com/resource-center/threats/botnet-attacks]

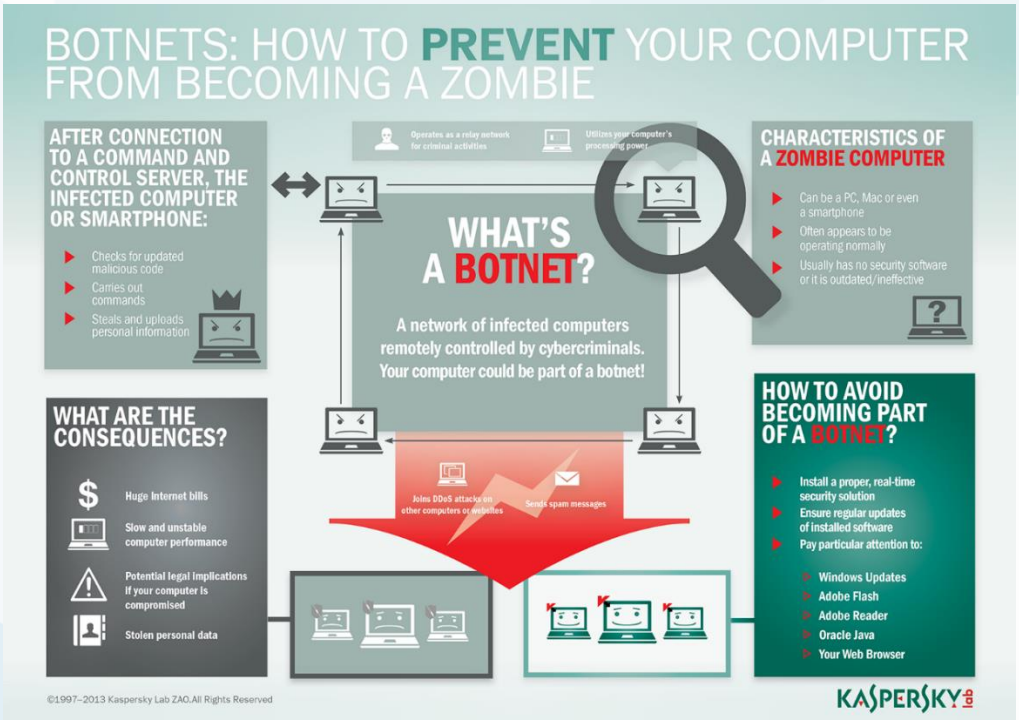


Figure 9. An overview of a botnet attack (Source: Kaspersky)

Situation in Africa

According to Trend Micro, the victims of botnets in Africa average 3,900 detections monthly, with roughly 50,000 detections in total. Several threat actors in Africa are deploying spam run campaigns with enclosed Trojan stealers such as Emotet, Lokibot, Agent Tesla, Fareit, etc. Surprisingly, Namibia had the highest detections of Emotet, although it subsided after global efforts to disrupt the Emotet botnet early this year. Other top malware detections are backdoor web shells and Dorkbot that is able to spread via removable drives, e-mail and social media.

Cybercriminals are recruiting new members by training and introducing several cybercrime toolkits. This has been one of the reasons for the expansion of DDoS operations of this type with cybercrime as a service available through the open and dark Web environments. The expansion of online communication platforms has provided a learning environment for cybercriminals to develop and enhance their skills, learn and exchange information on cybercrime toolkits, and even share their lessons learnt, stolen data and successful exploits with other individuals.

There have been many high-profile instances of such DDoS attacks on critical infrastructure in Africa in the past five years. For example, the 2016 Mirai botnet DDoS attack on Liberia crippled the internet infrastructure of the entire country, with attacks of over 500 gigabytes-per-second (Gbps), then among the largest DDoS attacks ever.[27] More recently, in September 2019, a large South African Internet Service Provider (ISP) was also the victim of a DDoS attack which brought it down for an entire day.[28]

Similarly, in October 2019 and 2020, South African banks also experienced a sustained wave of DDoS attacks, though no significant damage was reported. Although there have been no significant recent cyber incidents arising from DDoS attacks, DDoS attacks remain a concerning threat that organizations in Africa will need to guard against.

---

[27] ZDNET, 'Carpet-bombing' DDoS attack takes down South African ISP for an entire day. Cimpanu, C. 2019. Available at: [https://www.zdnet.com/article/carpet-bombing-DDoS-attack-takes-down-south-African-isp-for-an-entire-day/]

[28] CPO Magazine, Sustained DDoS Attack on South African Banks Accompanied by Ransom Notes. Ikeda, S. 2019. Available at: [https://www.cpomagazine.com/cyber-security/sustained-DDoS-attack-on-south-African-banks-accompanied-by-ransom-notes/]

2.5 Ransomware

Ransomware is a form of malware which encrypts victim data or locks down systems, disrupting the operations of victim organizations by rendering their data and systems inaccessible. Ransomware actors subsequently demand a ransom, usually in cryptocurrency for anonymity, in exchange for decrypting the data. It should be noted that the deployment of ransomware code onto an organization's network follows a legitimate (trusted insider) or illegitimate breach of that network, exploration of the network by cybercriminals, and the theft of organizational information and data. The deployment of ransomware is generally the final phase of a successful hack or penetration on that organization.

With TTPs becoming ever more sophisticated, the facilitation of ransomware attacks by organized crime groups has expanded to include double and triple extortions – where the initial ransomware attack is compounded by the theft of sensitive company data, ransom demands from victims with the threat of publicly shaming them through the release of stolen information and the re-exploitation of previously-exposed vulnerabilities within organizations to leave them facing a never-ending cycle of ransomware attacks.

Capable of bringing governments, business and supply chains to a grinding halt, the impact of ransomware attacks also has a reputational impact on victims alongside the economic impact, with the latter evidenced in research from INTERPOL's private partner, Palo Alto Networks, showing that the average ransomware payment has accelerated to more than 300,000 USD.[29]

This impact is further compounded when we consider the growing adoption of the TTP by organized crime groups which results in key files and backups being deleted, adding to the estimated average downtime of 21 days for each ransomware attack[30]. With research suggesting a ransomware attack occurs every 11 seconds, and given the previously-highlighted cyber vulnerabilities within the African region, the need for both a thorough understanding of the ransomware situation within Africa and implementation of the prevent and protect principles has never been more urgent.

[29] Palo Alto Networks, Extortion Payments Hit New Records as Ransomware Crisis Intensifies, Baylor, Brown and Martineau, August 2021. Available at: [https://www.paloaltonetworks.com/blog/2021/08/ransomware-crisis/]

[30] Forbes, Ransomware is everywhere, Durbin, S., 2021. Available at: [https://www.forbes.com/sites/forbesbusinesscouncil/2021/06/01/ransomware-is-everywhereheres-what-you-need-to-consider/?sh=1ded127c1f0f.]

Situation in Africa

Research from Kaspersky shows that there were more than 1.5 million ransomware detections in 2020. In the first quarter of 2021, Egypt, South Africa, and Tunisia suffered the most with the highest detection counts across Africa, and Egypt alone accounting for almost 35% of all ransomware detections in Africa (see Table 2).

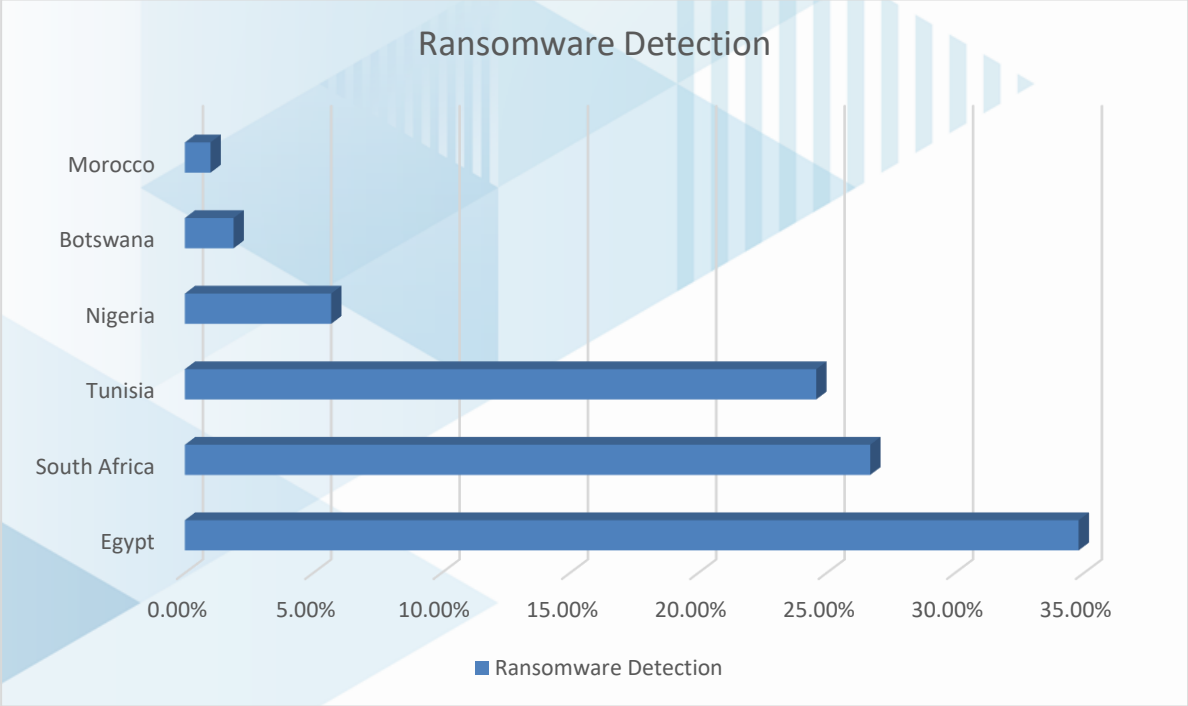


Table 2: Ransomware detection in Africa in March 2021 (Source: Trend Micro)

Although the ratio of overall ransomware detections within Africa ranked in the bottom 10% compared to all other regions, research from Check Point Software Technologies reported that African organizations have seen the "highest increase in attacks, at 34%", from January to April 2021.[31] According to the Africa Center for Strategic Studies in January 2021, "as Internet penetration rises and systems become more connected, critical infrastructure across Africa will likely become even more vulnerable to costly, disruptive cyberattacks".[32]

In Africa, Wannacry remains a top ransomware program and cybercriminals are also expanding their operations into double extortion. One example is the notorious ransomware Nefilim, where it affects banking and government sectors.

[31] Checkpoint, The New Ransomware Threat: Triple Extortion, 2020. Available at: [https://blog.checkpoint.com/2021/05/12/the-new-ransomware-threat-triple-extortion/]

[32] Africa Center for Strategic Studies, Africa's Evolving Cyber Threats. Allen, N. January 2021. Available at: [https://Africacenter.org/spotlight/Africa-evolving-cyber-threats/]

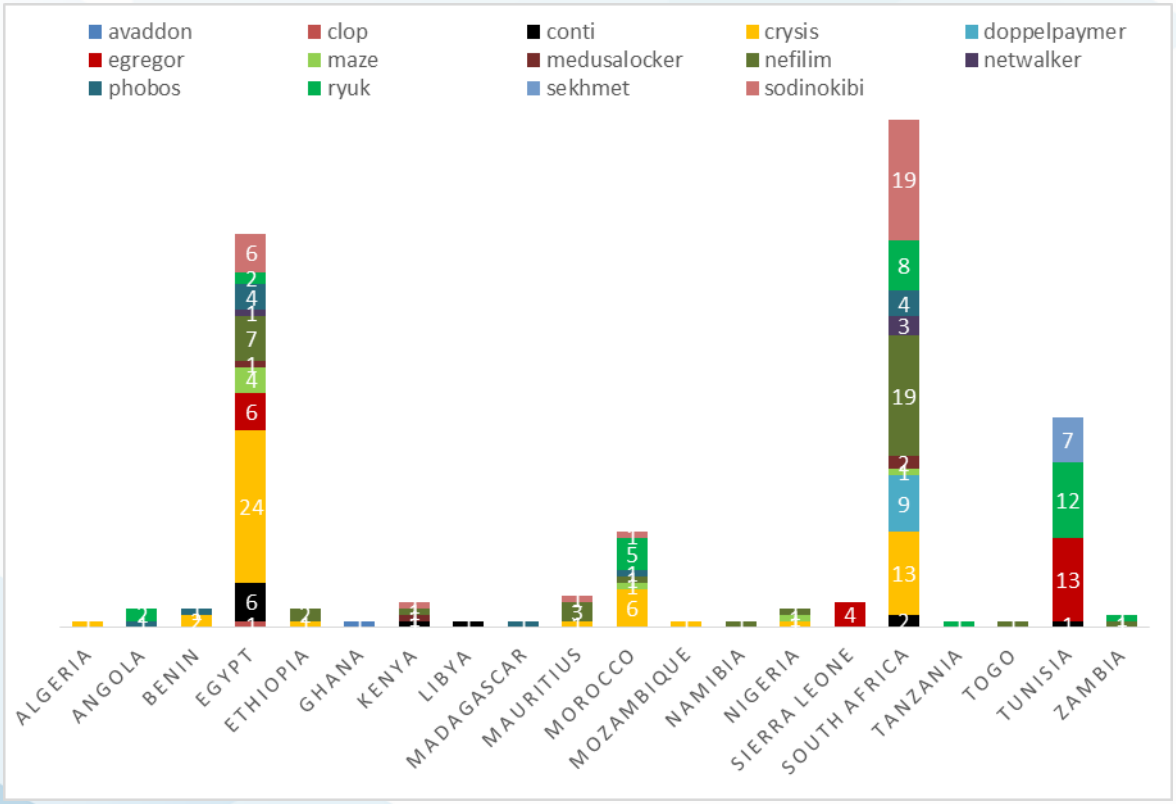


Figure 6. Targeted ransomware in Africa, unique detections and selected families (Source: Trend Micro)

According to Figure 6 above, South Africa was the country most heavily affected by targeted ransomware in the first quarter of 2021, with a variety of families such as Crysis, Nefilim, Ryuk, Clop, and Conti ransomware. Subsequently, Egypt was the next hardest-hit country with a similar profile of targeted ransomware detection. Tunisia was the third most affected country, targeted mainly with Egregor (before its shutdown in February 2021), Ryuk, and Sekhmet ransomware.

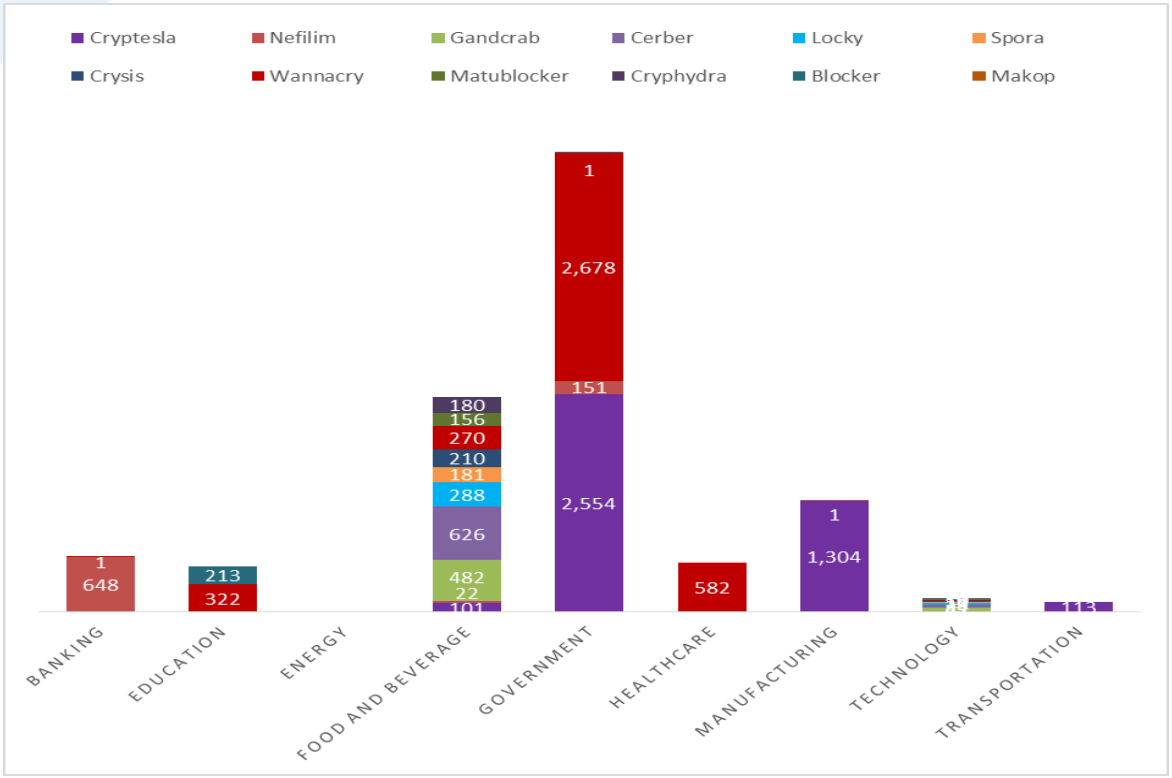


Figure 7. Industries affected by ransomware in Africa from January 1 to April 2021 (Source: Trend Micro)

The industries most affected in Africa are the government and food-and-beverage sectors, according to Trend Micro (see Figure 7). It has been observed that the reason the Wannacry ransomware is so prevalent in the government sector is that many machines have not been patched for the vulnerability in the Server Message Block (SMB) protocol, which is a known target of Wannacry ransomware.

Meanwhile, there is also a variety of old ransomware families like Cerber, Gandcrab, Locky, Cryptesla that target the government, food-and-beverage, and manufacturing sectors. However, one notable exception is the newer and notorious Nefilim ransomware, discovered in March 2020,[33] which is targeting the banking industry in the Africa Region.

Since ransomware actors are profit-driven, the problem will persist globally as long as victim organizations are willing or forced to pay ransoms. According to the Brookings Institution in March 2021, cyber threats in Africa are exacerbated by vulnerabilities in public cybersecurity strategies and the economic impact of the COVID-19 pandemic.[34]

"Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19."

Jürgen Stock, INTERPOL Secretary General

[33] Trend Micro, An Analysis of the Nefilim Ransomware. February 2021, Agcaoili, Gelera. Available at: [https://www.trendmicro.com/en_us/research/21/b/nefilim-ransomware.html]

[34] Brookings, How African states can improve their cybersecurity, Signe & Signe, 16 March 2021. Available at: [https://www.brookings.edu/techstream/how-African-states-can-improve-their-cybersecurity/]

EXAMPLES OF ATTACKS AGAINST CRITICAL INFRASTRUCTURE IN AFRICA

- In South Africa, the organization Life Healthcare, which is the second-largest private hospital operator responsible for administering digital services in hospitals across Southern Africa, was hit by a cyberattack in June 2020.[32] This attack, instigated during the COVID-19 pandemic, affected its admission systems, business processing systems and email servers, with some systems being forced offline. It is believed to have cost the organization more than a month in downtime in the midst of the pandemic.
- There were the twin attacks in October 2020, where firstly key social services in Johannesburg, including bill payments, social advice and the emergency services network were impacted and shut down following a data breach and then deployment of ransomware. Analysis of the attack identified not only the exploitation of a vulnerability, but also that after employing lateral movement techniques the threat actors deliberately deployed their ransomware to coincide with the "end of the month" payment cycle – in an effort to further coerce South African authorities to pay the cryptocurrency ransom.[33]
- In Kenya, an attack targeted the markets and interconnected cyber systems, with INTERPOL warning that the threat of supply chain attacks may well define the cyber threat landscape over the coming decade. High-profile attacks on supply chains, with the compromise of the Kaseya IT service by the ransomware group REVIL[34] are particularly affecting customers in Kenya.
- There was a DDoS attack on South African banks – again timed to hit and disable services at the "end of the month" payment cycle. This was launched against several major banks across South Africa – with a ransom again demanded in cryptocurrency. While the reported damage from this attack was minimal and caused only disruption to services, the conjunction of this attack with the simultaneous ransomware attack in Johannesburg emphasizes the scale, impact and seriousness of the threat to critical infrastructure across the African region.
- The State-owned Transnet organization in South Africa faced an unprecedented cyberattack in July 2021, which resulted in severe disruption to its services.[35] The Institute for Security Studies (ISS) highlighted that "first time the integrity of South Africa's critical maritime infrastructure has been severely disrupted" with an attack on the port able to delay or shut down a critical trade route and disrupt vital trade services in the middle of a global pandemic. The attack is believed to have suspended the automated and online container-handling facility in both Cape Town and Durban – with the Durban port being the busiest port in sub-Saharan Africa and a maritime hub for the movement of essential goods between other African countries, including Zambia and the Democratic Republic of Congo.

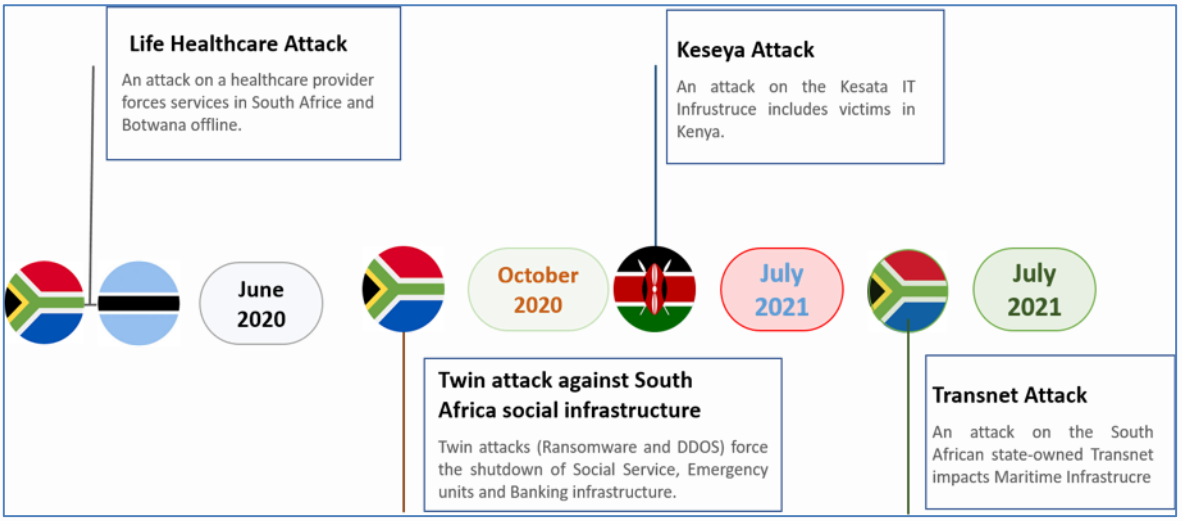


Figure 8. The major publicly documented critical Incidents in Africa 2020-2021

3. OPERATIONAL SUCCESS

Under its mandate of reducing the global impact of cybercrime and protecting communities for a safer world, the INTERPOL Cybercrime Directorate delivers policing capabilities to all member countries through the Global Cybercrime Programme. The Global Cybercrime Programme has three core pillars, namely: (i) Cybercrime Threat Response, (ii) Cyber Strategy and Capabilities Development, and (iii) Cybercrime Operations.

The Cybercrime Threat Response pillar identifies, triages and coordinates a global response to cyberthreats in a targeted and focused manner, leveraging private partners' expertise and cybercrime data. It focuses on intelligence development of identified threats to design disruption-and-prevention strategies that mitigate high-risk and high-impact cyberthreats. It also aims to provide quality advice and guidance on the current threat landscape, as well as operational support through the provision of actionable intelligence.

The Cyber Strategy and Capabilities Development pillar supports member countries by developing cyber skills, knowledge and technical capabilities that are customized to their needs, in line with INTERPOL standards. In collaboration with its stakeholders, the team plans, develops and delivers cyber capability and capacity-building projects and programmes, as well as tools and platforms, to enhance member countries' ability to tackle cybercrime globally.

The Cybercrime Operations pillar leads and coordinates transnational operational activities with member countries in tackling cyberthreats that cause significant harm on a national, regional and global scale. In close cooperation with member countries, the public-private sector and national Computer Emergency Response Team (CERT) communities, it conducts operational activities targeting high-impact cybercrime through the 'Regional Cybercrime Operations Desk' approach.

In May 2021, INTERPOL launched a new Regional Cybercrime Operations Desk to boost the capacity of 49 African countries to fight cybercrime under the framework of the AFJOC project. This African Cybercrime Operations Desk will help shape a regional strategy to drive intelligence-led coordinated actions against cybercriminals and support joint operations. The two operations highlighted below have provided timely and effective operational support to member countries in Africa.

3.2 Operation Lyrebird

In July 2021, an alleged prolific cybercriminal was apprehended in Morocco following a joint two-year investigation by INTERPOL, the Moroccan police and Group-IB. Acting under the pseudonym 'Dr Hex', the suspect is believed to have targeted thousands of unsuspecting victims over several years through global phishing, fraud and carding activities involving credit card fraud.

He is also accused of defacing numerous websites by modifying their appearance and content, and targeting French-speaking communications companies, multiple banks and multinational companies with malware campaigns. The suspect is also alleged to have helped develop carding and phishing kits, which were then sold to other individuals through online forums to allow them to facilitate similar malicious campaigns against victims.

These were then used to impersonate online banking facilities, allowing the suspect and others to steal sensitive information and defraud trusting individuals for financial gain, with the losses of individuals and companies published online in order to advertise these malicious services.

Under Operation Lyrebird, INTERPOL's Cybercrime Directorate worked closely with Group-IB and with the Moroccan Police via the INTERPOL National Central Bureau in Rabat to eventually locate and apprehend the individual, who remains under investigation.

3.3 Operation Falcon

Under 'Operation Falcon', three suspects were arrested in Lagos in November 2020 following a joint INTERPOL, Group-IB and Nigerian Police Force cybercrime investigation. The Nigerian nationals are believed to be members of a wider organized crime group responsible for distributing malware, carrying out phishing campaigns and extensive BEC scams.

The suspects are alleged to have developed phishing links, domains, and mass-mailing campaigns in which they impersonated representatives of organizations. They then used these campaigns to disseminate 26 malware programs, spyware and remote access tools, including Agent Tesla, Loki, Azorult, Spartan and the Nanocore and Remcos Remote Access Trojans. These programs were used to infiltrate and monitor the systems of victim organizations and individuals, before launching scams and syphoning funds.

According to Group-IB, the prolific gang is believed to have compromised government and private sector companies in more than 150 countries since 2017. The year-long investigation saw INTERPOL's Cybercrime Directorate and Financial Crime units work closely with Group-IB to identify and locate threats and, ultimately, assist the Nigerian Police Force via the INTERPOL National Central Bureau in Abuja, in taking swift action.

INTERPOL | THE NIGERIA POLICE | GROUP IB

4. INTERPOL'S REGIONAL CYBERCRIME STRATEGY FOR AFRICA

INTERPOL provides a regional cybercrime strategy for Africa which underpins the operational framework of the African Cybercrime Operations Desk. In support of the activities of this Desk, the strategy encompasses four strategic objectives, outlined below.

Strategic Objective 1:
Enhancing cybercrime intelligence for effective responses to cybercrime

Strategic Objective 2:
Strengthening cooperation for joint operations against cybercrime

Strategic Objective 3:
Developing regional capabilities and capacity to combat cybercrime effectively

Strategic Objective 4:
Promoting good cyber hygiene and resilience for a safer cyberspace

The African Cybercrime Operations Desk under the AFJOC project will address cybercrime in support of the African region through the following strategic pillars:

- **[Objective 1] Enhancing cybercrime intelligence for effective responses to cybercrime**

  Within the partnership framework of Gateway, INTERPOL will collaborate with private entities to request and receive up-to-date information related to cybercrime threats, trends and risks in the African region. By processing and analysing information using external tools and those developed in-house, INTERPOL will deepen its understanding of the cybercrime threat landscape, generating timely and accurate cyber intelligence and threat responses for African member countries.

- **[Objective 2] Strengthening cooperation for joint operations against cybercrime**

  In close cooperation with member countries, private partners and national Computer Emergency Response Team (CERT) communities, INTERPOL will strengthen cooperation and increase joint operations targeting high-impact cybercrime through the African Cybercrime Operations Desk.

- **[Objective 3] Developing regional capacity and capabilities to combat cybercrime**

  In collaboration with its stakeholders, INTERPOL will plan, develop and deliver cyber capability and capacity-building projects and programmes to enhance member countries' ability to tackle cybercrime in Africa. As part of this effort, it will maximize the use of tools and platforms including the Cybercrime Knowledge Exchange, Cybercrime Collaborative Platform – Operations, and Cyber Fusion Platform.

- **[Objective 4] Promoting good cyber hygiene for a safer cyberspace**

  INTERPOL will run a global awareness campaign with the aim of raising public awareness of the key cyberthreats and promoting good cyber hygiene for individuals and businesses in Africa. This campaign will also support regional law enforcement mitigation and prevention efforts targeting the top cyberthreats, for better operational outcomes.

The African Cybercrime Operations Desk acts as a conduit between law enforcement communities in Africa and the private sector to achieve these objectives and further develop the operational framework to improve coordinated actions against cybercrime in Africa.

CONCLUSION

This African Cyberthreat Assessment Report 2021 has detailed the context and analysis of the cybercrime threat landscape in Africa, focusing on the top five threats. These threats are affecting other regions equally, confirming the borderless nature of cybercrime. The unique challenge for Africa appears to be the critical absence of cybersecurity protocol, cyber resilience as well as mitigation and prevention measures for individuals and businesses. As a region that is embracing digital transformation, Africa needs to invest extensively in improving the safety and security of cyberspace.

The report also underlined how INTERPOL is supporting its member countries in addressing cyberthreats by coordinating cybercrime operations that have led to successful identification and apprehension of threat actors in collaboration with its private partners. The result of this assessment may encourage member countries to prioritize and allocate resources to address cybercrime, in order to increase such operational activities and achieve better outcomes.

Given the fast-evolving and transnational nature of cybercrime, it is evident that cybercrime can only be tackled effectively through a coordinated and rapid response. Intelligence gathering and sharing is a vital component in achieving an effective law enforcement response. INTERPOL is equipped with the intelligence capability hosted within its Cybercrime Threat Response team and through the establishment of the African Cybercrime Operations Desk.

In this context, member countries should leverage and maximize the use of police-level cooperation through INTERPOL's channels, platforms and capabilities for a timely and effective response. Collective efforts in sharing intelligence and formulating a joint operational framework will boost the regional capabilities and capacity in the fight against cybercrime. With this in mind, this report also suggested a regional cybercrime strategy for Africa which will serve as a basis for the joint operational framework to be developed for Africa.

Looking ahead, law enforcement must be a trusted partner, as data sharing is key – including between national police forces, and with the public and private sectors. At a time when the international community is under exceptional pressure, bolstering our common security requires us to move towards more collaboration. Together with our member countries and partners, INTERPOL will continue to reduce the impact of cybercrime and protect communities for a safer world.

INTERPOL Contributors

Wookyung Jung, Policy Analyst, Cybercrime Directorate

Richard Lim, Project Manager, African Joint Operation against Cybercrime

Emmanuel Kabera, Cybercrime Intelligence Officer, African Joint Operation against Cybercrime

Mohammed Isah, Cybercrime Operations Officer, African Joint Operation against Cybercrime

Shane Cross, Acting Head Cybercrime Intelligence Unit, Cybercrime Threat Response

Joyce Sin, Cybercrime Intelligence Officer, Cybercrime Threat Response

Peter Stanier, Cybercrime Intelligence Officer, Cybercrime Threat Response

Agnese Carlini, Cybercrime Intelligence Officer, Cybercrime Threat Response

Dean Watkinson, Cyber Specialized Officer, INTERPOL Support Programme for the African Union

ABOUT INTERPOL

INTERPOL is the world's largest international police organization. Its role is to assist law enforcement agencies in the Organization's 194 member countries to combat all forms of transnational crime. It works to help police across the world to 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.

INTERPOL

INTERPOL Global Complex for Innovation

18 Napier Road

Singapore 258510

WWW.INTERPOL.INT

INTERPOL_HQ

@INTERPOL_Cyber

INTERPOL HQ

INTERPOL