ANNUAL CYBERSECURITY REPORT

NIGERIA 2019

An internally generated report based on a cyber-intelligence platform built by CyberSOC Africa

CYBERSOC

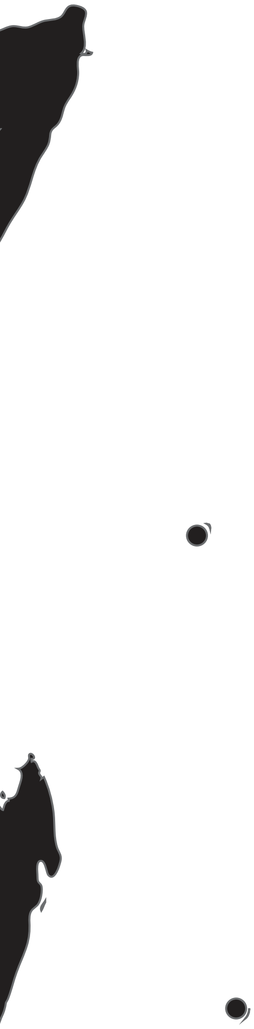
Incident Response and Security Services

“

Highlights three of the most
salient aspects of security
problems in Nigeria;

Cyber-Attack, Fraud & Law Enforcment

”



CONTENT

CYBERSOC
Incident Response and Security Services

About the Report

David Dan

CEO CyberSOC Africa

CyberSOC Africa is operating in-country state-of-the-art ISO certified Security Operations Center: Close to 300 sq meters of uncompromising quality, rigorous engineering, and best-in-breed technologies coupled with an elite team of cyber experts to deliver robust cyber enforcement and superior technological capability. Our analysts are exposed to a wide array of cyber incidents, customers, technologies, incidents, verticals and disciplines - which gives them the ability to provide our clients with unmatched value in terms of cyber expertise and as a result, unmatched cyber resilience.

We provide visibility and identify potential threats in all critical areas of an organization's IT infrastructure, along with actionable, intelligence-driven insights to assess the state of an organization's security posture, meet compliance regulations and design the future state of security.

CyberSOC Africa, the continent's cybersecurity leader, protects and defends Financial Institutes, Telcos, Oil & Gas, Governments and SMEs' IT assets and data against cyber crime. We are closing the ever-growing gap between cyber needs and the resources to address them by training hundreds of African cyber security specialist annually - and employing the very best of them. With strong local presence and an unmatched cyber intelligence network, the company possesses a true understanding of Africa's unique threat landscape, local cyber crime motivators, and attackers' method of operation.

CyberSOC Africa's 2019 Annual Report for Nigeria was birthed from in-depth research analyzed, compiled and published by the company's DART (Data Analytics and Research Team) and Cyber Threat Intelligence Team.

The data used to develop this report was obtained from our cyber-intelligence platform; an automated threat intelligence web crawler built by CyberSOC Africa to crawl Nigerian based internet sites and social media platforms primarily for information retrieval which through structured techniques is evaluated using automated machine processes and human analysis.

Introduction

Yaniv Ovitz

CTO CyberSOC Africa

We are proud and excited to present to the public the first edition of our annual report detailing security incidents, trends,alongside the impact and changes of Nigeria's cyberspace.
In 2019, we launched our DART(Data Analytics and Research Team) tasked with a mission to develop a report that analyzes our roboust intelligence web research platform, a dedicated crawling platform modeled to provide insight and information on activities within the Nigerian cyber ecosystem ranging from underground markets to crimes.

At CyberSOC Africa, our aim is not to only provide the best safety solutions to organizations with regards to information security and cyber threats,
but as a leader and pace-setter in Cyber Security, is facilitate and improve the overall security posture of the country at large.

Preface

Victor Funmipe

SOC Manager and Lead Researcher,
CyberSOC Africa

CyberSOC Africa's Report highlights three of the most salient aspects of security challenges in Nigeria; Law enforcement, Fraud & Cyber-Attacks. To aid the authenticity and quality of the Report, many references to thoroughly researched data with adequate statistics were made. This enabled appropriate analysis and provision of a detailed & valuable information on the three aspects of security being highlighted.

The aim is to shed more light on these aspects to raise the level of awareness & enlightenment of the general public.It is pertinent to mention that apart from the inputs from researches, resources, materials, methods, time and efforts of CyberSOC's professionals, consultations and collaborations with relevant Government Agencies like the NPF, EFCC and the ICPC also enhanced the quality and value of this Report.

On financial fraud, records from research revealed that approximately N80 Billion was the cumulative amount lost from fraud related activities alone in year 2019.

Hence, this report examines the intricacies of Fraud in relation to the overall posture of security in Nigeria.

A significant portion of this Report focuses on Cyber-Attack and its Effects on Nigeria's Financial Sector in year 2019. CyberSOC Africa x-ray's cyber attacks based on modes, methods and trends from observations and researches in the year 2019.

The ultimate aim of CyberSOC Africa as a leader and pace-setter in Cyber Security, is not to only provide the best safety solutions to organizations with regards to information security and cyber threats, but also the facilitation and improvement of the overall security posture of the country at large.

Authors & Contributors

Yaniv Ovitz
Chief Cyber Technology Officer

Victor Funmipe O
SOC Manager and Lead Researcher

Ofure Aigbefo
Team-lead, Data Analytics and Research

Yesufu Khalid
Team-lead, Professional Services

Abodunrin Oladayo
Team-lead, Operations

Obajuwana Kesiena
Team-lead, Cyber Threat Intelligence

Ooreofeoluwa Koyejo
Member, Data Analytics and Research

Adesola Braimah
Member, Operations

Daini Ademayokun
Member, Operations

Aturaka Oluwatosin
Member, Cyber Threat Intelligence

Ashraf Abbas
Member, Operations

Sangotayo Ifeoluwa
Member, Cyber Threat Intelligence

Onwukwe Sylvia
Developer, Cyber Threat Intelligence

Cyber-Attacks & Fraud

Cyber-Attack In Financial Industry

Cyber-Attack refers to the deliberate exploitation of computer systems, technology-dependent enterprises and computer networks. It involves the use of malicious codes and specially crafted techniques to alter legitimate computer data, codes or logic resulting in disruptive consequences to users, organizations or agencies.

The financial sector, for its tremendous value of information and data, is the primary target of most instituted forms of cyber-attacks worldwide. The computerization and automation processes employed in the financial sector has also exposed the sector to various modes of exploit attempts. Cyber-attacks can take on various forms and techniques tailored for specific kinds of exploits.

Nigeria has had her fair share of cyber-attacks in 2019, and the most common forms of cyber-attacks recorded in the financial sector are discussed below.

1. Data Leakage

Data leakage is the unauthorized transmission of data, physically (mobile data storage devices, USB, optical media) or electronically (e-mail, web sites) from within an organization to an external destination or recipient.

Data leakage poses huge problems in the financial sector; from confidential documents being exposed, to damage of reputations, lawsuits, decline in revenue and massive financial penalties.

Data leakage could occur in several ways sides those mentioned above;
Accidental breaches, where there is no malicious intent.
An example is accidentally sending confidential/sensitive information to a wrong recipient.

Data leakage accounts for at least 2.03% of the attacks experienced in the financial sector of NIgeria.

A disgruntled employee or an unhappy em ployee or exemployee could leak confidential information about an organization.

Data leakage can also occur through electronic communications with malicious destinations over the internet, instant messaging applications, websites, e-mails etc. These mediums are capable of file transfer and are often the targets of mal ware. A vast majority of data loss occurs via printers, cameras, photocopy machines, re movable USB drives.

2. Malware

A malware or malicious software is any program or file that is created with the intent of performing malicious functions on computer systems or devices and users or organizations. The programs can perform a variety of activities such as stealing, encrypting, deleting sensitive data, altering or hijacking core computing functions and monitoring a user's computer activity without permission. Malwares can be categorized as viruses, trojans, ransomware, worms, spyware etc.

Majority of malware are also capable of spying on the activities of a victim, remaining undetected until it gathers enough information an attacker needs, or to eventually turn the infected system to a zombie as part of a botnet under the control of a hacker. It is often hidden in the attachments of legitimate looking e-mails or in free downloads on websites.

*Malware exploits make up **18.2%** of cyber-attacks recorded in the Nigerian financial sector in 2019.*

It is important to never open or download emails and attachments from unknown sources. Deleting such messages will eliminate the malware threat.

3. Ransomware

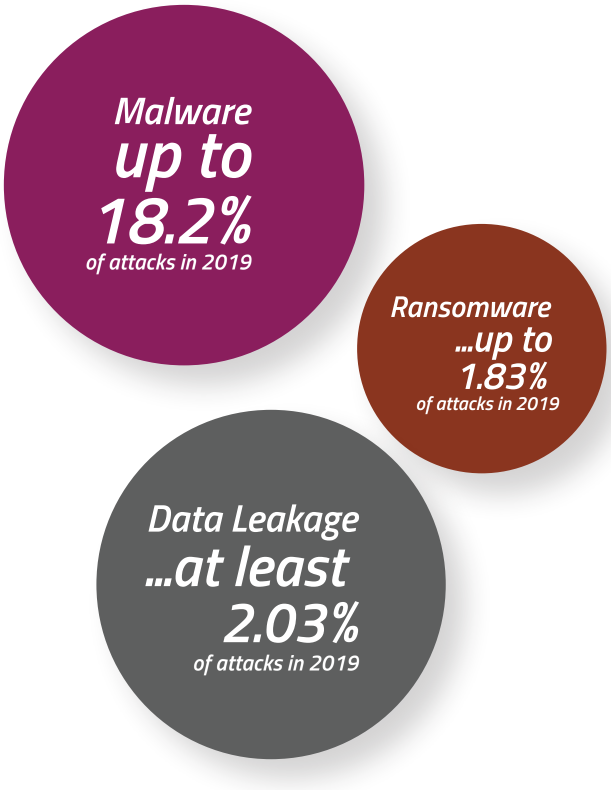
Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the user's files unless a ransom is paid.

More recent ransomware variants encrypt certain file types on infected systems and force users to pay a ransom, usually in cryptocurrency, to get a decryption key.
Ransomware attacks may be encountered via a variety of ways; from being downloaded onto systems when unsuspecting users visit compromised websites. It could also be delivered as payload from other malware or as attachments from spam e-mails, and malicious pages through malvertisements.
Once executed, the ransomware locks the screen of the infected computer, or in the case of crypto-ransomware, it encrypts specific files.

One of the more notable incidents involved a variant of highrisk ransomware called ETH.
The ransomware typically gets into a system via Trojans, software cracking tools, fake updates, third party download sources and through spam e-mail campaigns. Another notorious variant of ransomware witnessed is an executable namely "mssecsvc.exe". The "mssecsvc.exe" is an executable file associated with the WannaCry ransomware. The malware is persistent in nature and is programmed to be executed every time the infected host starts up. This is the reason why the infection keeps recurring even though the antivirus reports that the file has been deleted.

*Ransomware-related attacks constituted up to **1.83%** of the cyber-attacks recorded in the financial sector in the year 2019 in Nigeria.*

It is advised that victims never contact or pay the ransom requested by the attackers as research show that attackers take payment and disappear.
Also, invoking a system restore process or employing a professional anti-spyware removal tool can help restore the infected system to normal conditions.
Reputable anti-virus and anti-spyware programs can protect systems from such malware activities. Users are also advised to maintain up-to-date regular backups and only download, open or run attachments from trusted sources.



4. Phishing Attack

Phishing is the fraudulent use of electronic communication techniques to deceive unsuspecting users by sending emails purporting to be from reputable companies or sources, in order to induce individuals into divulging sensitive and confidential information such as usernames, passwords, credit card details etc.
Phishing relies on social engineering techniques applied to email or other electronic communication methods including SMS or direct messages sent over social networks like Facebook & LinkedIn, in a bid to gather background information about an impending victim.

Indicators of a phishing scam includes misspelled URLs (typosquatting), use of public email address rather than a corporate one, messages written to convey fear with a sense of urgency, requests to verify personal information, financial details, passwords, and so on.

Attackers would normally send out thousands of spam email messages to random users in order to have a high success rate of getting victims that will click on malicious links and divulge sensitive information. The attacks could also be targeted and closely monitored to gather as much information as possible that would be sufficient to craft a believable and seemingly authentic message, one that is good enough to launch an attack against the individual.

Phising exploits make up ***0.63%*** *of cyber-attacks recorded in the Nigerian financial sector in 2019*

Phishing
...up to 0.63%
of attacks in 2019

Network Attacks
...about
79.14%
of attacks in 2019

Although financial institutions in Nigeria have adopted efficient systems to mitigate the damage and impact of phishing scams against their organizations, the trend is not likely to slow down in the nearest future. Therefore, it is imperative that financial institutions schedule regular training programs for staff and gear up towards ensuring foolproof security systems in their environment.

5. Network Attacks

Operations aimed at disrupting, degrading or destroying information resident on computers and computer networks, or the computers and networks themselves, are classified as network attacks.
Computer network attacks refer to unauthorized actions against private, corporate or government IT assets in order
to destroy, modify or steal sensitive data. It involves methods or processes maliciously used to compromise network security.
In Nigeria's financial institutions for the year 2019, the most devastating forms of Cyber-attacks perpetrated has certainly been via different modes of Network Attacks.

CyberSOC's research data reveals that network-related attacks account for about ***79.14%*** *of Cyber-attacks recorded in the financial sector throughout 2019.*

The most common forms of network attacks experienced are highlighted in subsequent paragraphs.

Communications with Malicious IP Addresses:

Data collected from the beginning of 2019 indicates consistent and persistent connection attempts were made by malicious IP addresses to gain access into corporate networks of financial institutions. The IP addresses were investigated and confirmed to have bad reputations and high threat scores as analyzed by Cyber Threat Intelligence platforms such as IBM Xforce, Open Threat Exchange, RecordedFuture and CISCO's Talos Intelligence, etc.

A lot of the communications were initiated by IP addresses linked to known indicators of compromise and hacker groups like Lazarus (FastCash) cybercriminal group, Nivdort, Emotet, Danabot, Sodinokibi, to mention a few of the more popular ones. Making up nearly 60% of the common forms of network attacks against financial institutions in Nigeria in 2019, communications with malicious IP addresses have proven to be a major threat to the security of corporate networks.

Insecure Port Communications:

Computer ports are connection points or interfaces between a computer and an external, or internal device.
Ports have numerous functions & connectors of varying designs for specific uses. Based on protocols or services being used, ports can be secure or insecure.
Insecure ports communication refers to connections that are susceptible to interception or sniffing by attackers. Due to this, best practices and standards have been set with necessary security implementations and measures to protect against data leakage or penetration of networks via vulnerable ports.
Data from financial institutions is of great interest to people with malicious intents, and with just slightly above 18% communications involving insecure ports, the financial sector is prone to data leakage and network attacks through port communications.

Brute-Force Attacks:

A brute-force attack is a trial-and-error method used to obtain information such as a username, password/passphrase or personal identification number (PIN). Brute force attacks involve the use of automated tools to guess various combinations of usernames and passwords in continuous attempts to get the required information.
The motive behind brute-force attacks is to gain illegal access to a targeted system and utilize it in either executing another kind of attack like ex-filtration of data or to shut down the system/network all together.

Constituting at least 7.8% of the network related incidents recorded against Nigerian financial institutions in 2019, this mode of network attack is gaining popularity due to its relative ease, and readily available tools on the internet for propagation.
Multifactor authentication, strong password policies and geo-location logon restrictions are some of the methods used mitigate against brute-force attacks.

Communication with TOR IP Addresses:

The Onion Routing (TOR) is an anonymity software that hides a user's IP address in communications over the web. The intention is to conceal information about user activities and location. It is often used by hackers and cyber criminals to keep their communications and locations private and sometimes, for ex-filtration of data by employees.
TOR communications pose the threat of bypassing network security, connecting to criminal sites on the "dark web", and exposing the corporate network to malware infections and other forms of attacks. Use of the software is largely discouraged in corporate environments for these reasons. Preventive methods like monitoring communications and blocking TOR associated IP addresses on the corporate firewall, uninstalling identified TOR applications from hosts and pushing policies prohibiting TOR related activities should be implemented by organizations to strengthen their security posture.

Approximately 8% of attacks carried out against financial institutions in Nigeria in 2019 involved the use of TOR software.

Peer-to-Peer Communications:
Communications that involve direct connection between source and destination without any intermediary on a network is referred to as a peer-to-peer communication. Files can be shared directly between systems on the network without the need of a central server. In other words, each computer on a P2P network becomes a file server as well as a client.
This poses the risk of data ex-filtration and allows remote access to files on a victim's computer, leaving the corporate network open to security risks, malware infections and overall system and network compromise.

Our research show that about 6% of net work-related attacks against financial institutions in Nigeria in 2019 involved peer-to-peer communications.

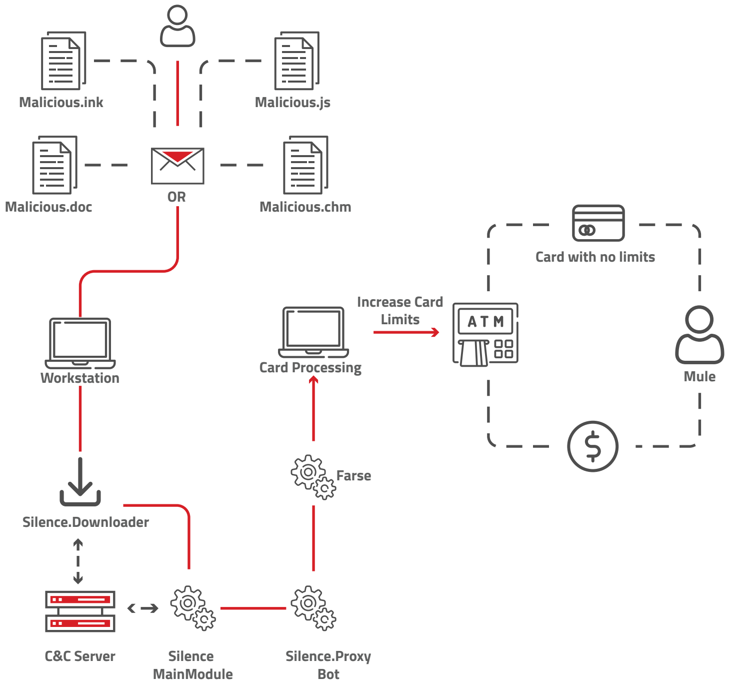
Advanced Persistent Threat (APT) -
Silence Silence is a Russian-speaking cyber-criminal group. Their first attack was recorded in June 2016, with a failed attempt to make a withdrawal from a Russian bank after gaining access to the Banks' network. Although the attack was unsuccessful, the group consistently made several attempts until its first successful theft recorded in October 2017 Using a different attack method, Silence, successfully stolen over $100,000 in one night via an ATM cyber-attack.
There have been several successful attacks carried out by the group between June 2016 and June 2019, with losses in millions of US dollars. Silence started with attacks focused on Russian banks; however, in 2019, their targets changed from Russia to other financial institutions in more than 30 countries in Asia, Africa, Europe, and some Commonwealth Independent States.

A recent analysis of Silence's attack shows that spearphishing is the attack vector frequently employed by the group. Phishing is an attack vector used by hackers to trick an employee into opening a malicious email, link, or downloading an infected file attachment. When an employee clicks or opens a malicious file with extensions such as .chm, .ink, .js, or .doc file, the malicious program embeded is downloaded and executes a binary dropper. The dropper is usually a win32 executable file that allows communication with the attacker's command and control (C&C) server.

Once a connection is established, the infected system could be monitored and controlled to capture screenshots, screen recording, track the user's activity and get information on the system or network's specifics and infrastructure.
According to Kaspersky Lab, the group, Silence, has penetrated the internal network of several African financial organizations, and majority of the attacks are "in the final stages."
The losses from attack is not restricted to large sums of money but as well as loss of other confidential data.

Silence Thefts

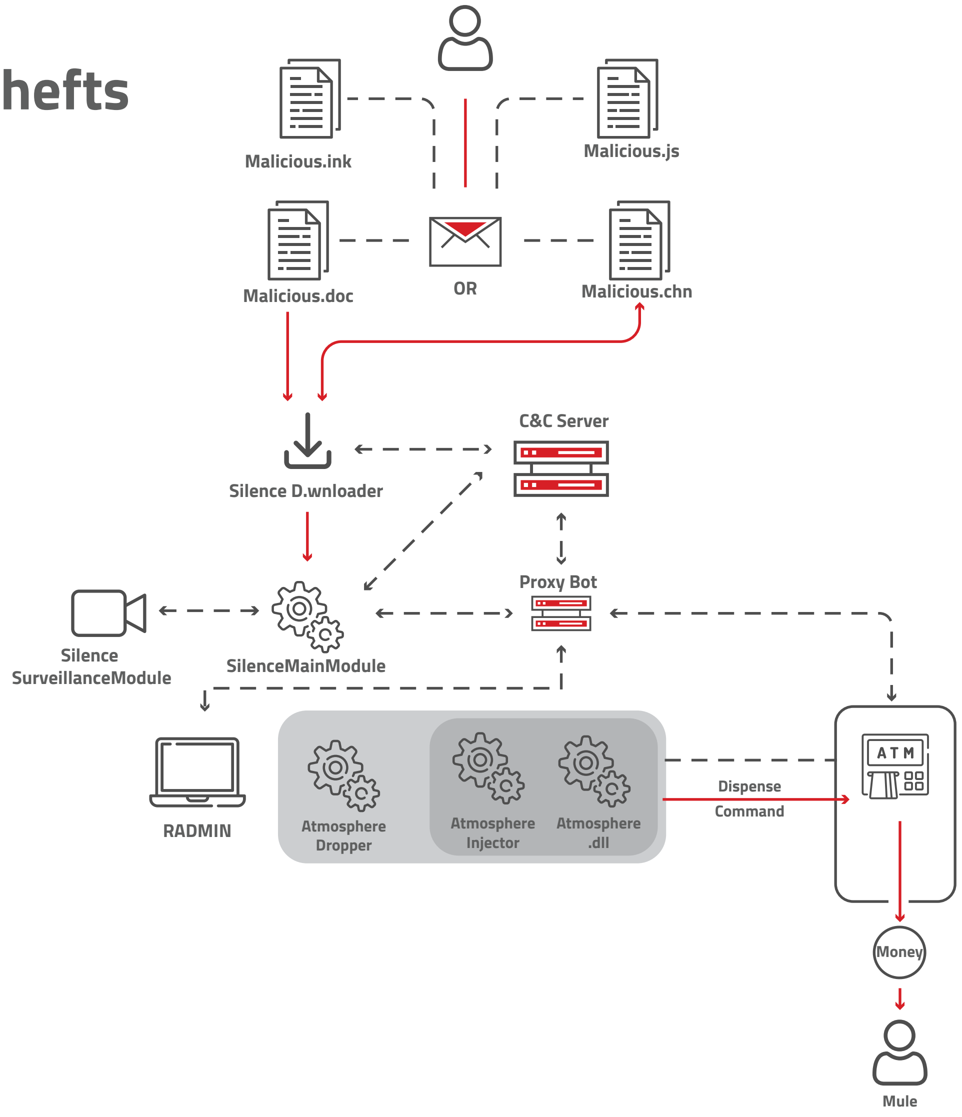
Targeting Card Processing Figure 1



Silence Thefts

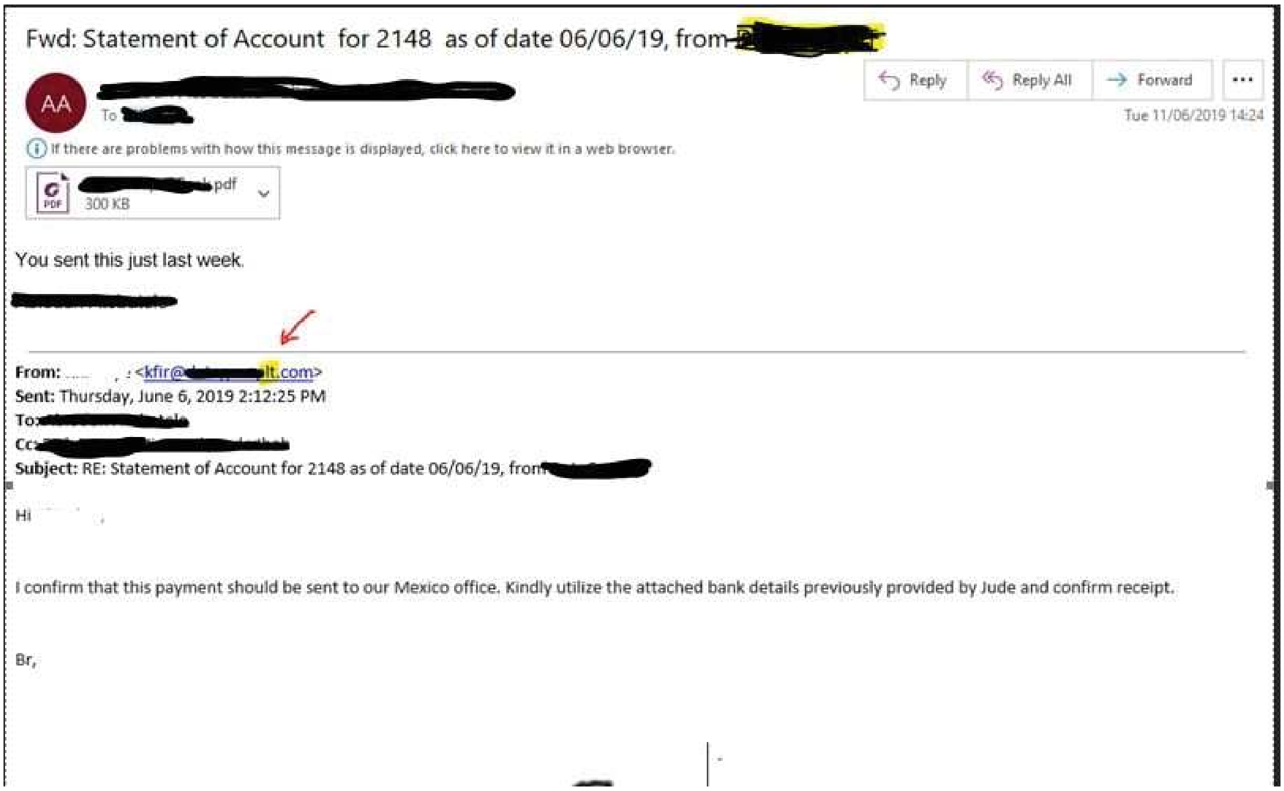
Targeting ATM's

Figure 2



BEC (Business Email Compromise):
BEC is a type of attack targeted at rganizations with international relations in suppliers/vendors or businesses with electronic forms of payments (e-commerce). BEC attacks are carried out by compromising corporate email accounts using social engineering or other forms of computer intrusion methods to conduct unauthorized transfer of funds (Internet crime report).
According to the FBI, Business Email Compromise has 5 major types of attack implementation; the bogus scheme, CEO fraud, account compromise, attorney impersonation and data theft. BEC attacks are not easy to detect because they do not require exploiting core technical security controls.
It was revealed that few private companies have suffered BEC attacks but this is handled and kept confidential which is mainly to avoid breaking the agreement of trust which can take an adverse effect on the business and prevent customers/investors from panicking. On the average, at estimate of $200,000 thousands dollars per month is lost to BEC.

SWIFT Attack
SWIFT being an acronym for Society for Worldwide Interbank Financial Telecommunication is a system, an important element in international banking; which has widely adopted codes known as Business Identifier Codes (BICs) previously known as Bank Identifier Codes and popularly called SWIFT codes. SWIFT allows sending and receiving of financial information worldwide in a secure, standardized and reliable environment.



Fwd: Statement of Account for 2148 as of date 06/06/19, from [redacted]

AA [redacted]

To [redacted]

Tue 11/06/2019 14:24

If there are problems with how this message is displayed, click here to view it in a web browser.

[redacted] pdf
300 KB

You sent this just last week.

[redacted]

From: <kfir@[redacted]lt.com>
Sent: Thursday, June 6, 2019 2:12:25 PM
To: [redacted]
Cc: [redacted]
Subject: RE: Statement of Account for 2148 as of date 06/06/19, from [redacted]

Hi

I confirm that this payment should be sent to our Mexico office. Kindly utilize the attached bank details previously provided by Jude and confirm receipt.

Br,

With its headquarters in Belgium, founded in 1973 and owned by 3,000 financial institutions. SWIFT means several things in the financial world, it functions as - a secure network for transmitting messages between financial institutions; - a set of syntax standards for financial messages (for transmission over SWIFTNet or any other network)

- a set of connection software and services allowing financial institutions to transmit messages over SWIFT network.

Similar activities/steps used in the SWIFT attacks;

- Attackers compromise the bank's environment.
- Attackers obtain valid operator credentials that have the authority to create, approve and submit SWIFT messages from customers' back-offices or from their local interfaces to the SWIFT network.
- Attackers submit fraudulent messages by impersonating the operators from whom they stole the credentials.
- Attackers hide evidence by removing some of the traces of the fraudulent messages.

Recent research revealed that three banks in Nigeria have suffered SWIFT attacks though the level of damage is currently undisclosed.

Common Automated Teller Machine Attack: Fastcash

On October 2, 2018, US-CERT published an alert revealing that Lazarus Group has been conducting "FASTCASH" attacks against banks in Asia and Africa to steal money from automated teller machines (ATMs) since at least 2016.

This attack enabled the group to remotely empty ATMs of cash which was done by first breaching the targeted banks' networks and then compromise the switch application servers handling ATM transactions. Upon successful compromise, the Trojan FASTCash is deployed.

Risk Exposure

Financial Loss is the major risk attached to this attack; it is estimated that the group have stolen tens of millions of dollars. In

2017, they enabled simultaneous cash withdrawal from ATMs in over 30 different countries, and in 2018 from ATMs in 23 different countries. Some other impacts of this attack are:

- Reputational damage to the organization involved.
- Financial costs to restore systems and Files.
- Temporary or permanent loss of sensitive data.

Fastcash Activities Involving Nigeria

A cyber-security company called Barac disclosed that Lazarus Group is targeting an unnamed African financial institution which puts Nigerian banks at risk of being targets.

At the time where said fastcash attack was noticed in Bulgaria the group had already started making small transactions which were detected immediately.

The international strategy of cyberspace published by The White House which reserves the right to use military force in response to a cyberattack automatically makes other regions without any form of international cyberattack policy with Africa being a major target, vulnerable to attacks from such threat actors

Table 1: Suspicious Traffic In and Out of Nigeria

INBOUND COMMUNICATION				OUTBOUND COMMUNICATION			
IPs	Recorded Future threat score	whois.com	Country	IPs	Recorded Future threat score	whois.com	Country
77.37.240.23	89	NKS broadband customers	Russia	139.59.59.137	95	DigitalOcean, LLC	Singapore
186.154.217.190	82	MANUFACTURAS GONZO Y CIA LTDA	Colombia	198.20.87.98	89	SingleHop LLC	US
112.85.42.181	81	China Unicom Jiangsu province network	China	120.150.246.241	93	TELSTRAINTERNET47-AU	Australia
62.219.3.48	87	Cloud Web Manage	Israel	181.31.213.158	74	Telecom Argentina S.A.	Argentina
218.92.0.212	81	CHINANET jiangsu province network	China	95.165.143.8	90	Moscow Local Telephone Network (OAO MGTS)	Russia
103.85.255.40	81	Advance Network Security Limited	HongKong	80.82.77.33	89	PV NETBLOCK	Netherlands
218.92.0.164	81	CHINANET jiangsu province network	China	193.142.219.104	88	ORG-PDMI1-RIPE	Ukraine
81.30.182.215	81	JSC "Ufanet"	Russia	92.63.197.60	89	ORG-FHVA2-RIPE	Ukraine
218.92.0.131	82	CHINANET jiangsu province network	China	80.82.77.139	89	IPV NETBLOCK	Netherlands
				94.246.128.46	90	ORG-ASzo12-RIPE	Poland

Table 2: Good to Have IOCs in Your SIEM

VIRUS	HASH	COUNT	TROJAN	HASH	COUNT
W32/Sality.gen.z	58372bf0475d6eb0e57e96c311ef8bfd	217225	NSIS/Coinminer.a	09931128f6c895d0b46b0cd0cdb4fd50	18707
Heur.AdvML.B	eb5be448b8453bea317dd589382607d3	6870	W32.Fix☒o.B!inf	a54f448022aec29e334a93b1cf27d618	4948
Generic.adm	7339a0efc768310a86b6d4f61d88b910	3381	Trojan-Coinminer	99d847fc458c04983fa3cb62ba37b093	3606
W32/Virut.n.gen	d9310cbf208c42c48bd43150bac0a322	2372	W32/Swisyn.ag	393aa522405df1635b298f4a8ee0fb65	2060
W32.Chir.B@mm	633d94f9d2f940b2358e46ed2f2b5c67	793	Trojan.Gen.MBT	950c09702da1a556ae30762322fa9ba7	192
Iframe.Exploit	a9e470648d6a7e7f73b0072051b8f452	769	Trojan.Gen	4d3ff9cba2e72c28a102a241d8b1dddc	180
Exploit-MIME.gen.c	eb3f9afb98194c26a5514e1b41508395	499	Trojan.Gen.8!cloud	b7e0f1d78b1fdd9a8eb0a600626cf957	117
NightMiner-FXM	94d8fa39c7535447dae06ad058a9c362	285	Trojan.Gen.NPE	79eb1f67f25d32a7a821b93a0eea9e62	101
			SMG.Heur!gen	56b55d01868f91cebb34ed11081e3a09	84
			CL.Downloader!gen	50 9e7c7c99b23bafdef9407aa88c8c0850	x76

Table 3: Indicators of Compromise (IOC) associated with Silence

Filename	printsrv.exe	inteldrv.exe	winss.ex_	Others
MD5	1136c47332daa275d2ecc179a0bf4c0c	043b383e895a26848bef90abb8da2216	3f5372c2776e5cc8aec8a7107f49cf8a	692c4e4db4aaec596dc570b1f12b8c2a
SHA1	f4277cc5c755d90405 a3b15201a1b4ed398deb61	3727cf8ca830f067 a65e446977292159baa2573d	5a7a2fcd906062f2c9e3bc5 edf2b82741fc0658b	043b383e895a26848bef90abb8da2216
SHA256	21176810b854c2253f522e71039c9344b81eff 697b7a36abd86ab6c220ea23dc	ae88e45b7e1c92b0e2a8e6c8f969b bdd0b260660a42468e5c61fa6ab834678ff	14696a979206432f9bbd74f3cdf27bc22d caf5889e33b612ca27065d1af5769e	c70b67a3db95d3a4063835cccbcd2c8b 3f5372c2776e5cc8aec8a7107f49cf8a
Note	Silence.ProxyBot Malware	Silence.ProxyBot Malware	Silence.ProxyBot Malware	9b38aa473fde5803c87f6f29a8241abe
Tcp Activity	91.92.136[.]193:443	45.84.0.201:443	79.141.168.114:443	050114e8ef758830cfe82004fdc7304b ac7985473c3d9b93f62707c3a8e64c64

"Losses from financial fraud in Nigeria for 2019 amounted to an estimate of

N79,986,840,807

$220,349,420

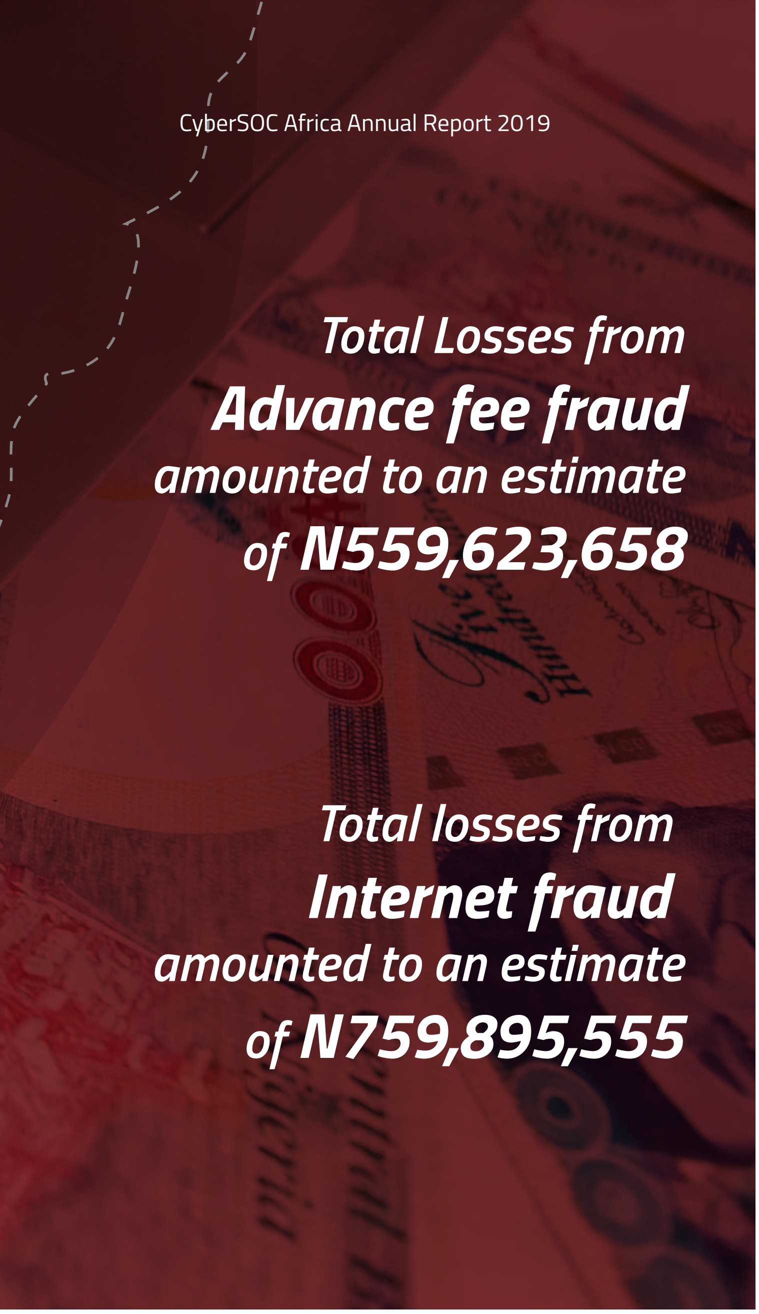
"Fraud costs the global economy over US$5 trillion

Financial Fraud

Financial fraud is defined as an intentional act of criminal deception through the use of false or misleading information aimed at illegally depriving a person or entity of money, property or legal rights.

Propagation of financial fraud may vary in form and technique.
The intent or motiveof the perpetrators is always the same-illegal financial benefit. Incidences of financial fraud are presently almost at the peak with daily introduction of new methods/schemes nationwide. The negative impacts and the devastating blow on the economic & financial status of the victims in particular and nation at large may impose additional burden for easy recovery. Perusal of relevant records for losses from financial fraud in the country from January 2019 till date showed the cumulative estimate amount as N79,986,840,807. Analysis of the data gathered by CyberSOC Africa's Intelligence Team are detailed below.

Advance Fee Fraud:
This scheme requires the payment of a substantial amount (upfront) in advance by individuals or businesses before taking delivery of the promised products, goods,



Total Losses from ***Advance fee fraud*** *amounted to an estimate of* ***N559,623,658***

Total losses from ***Internet fraud*** *amounted to an estimate of* ***N759,895,555***

tocks or services which in most cases are ultimately never delivered. The usual medium for perpetration of this fraud is the e-mail & an invitation to partake in a high profit-sharing investment. So far, the total amount involved in advanced fee fraud in 2019 estimated at N559,623,658.

The South Western region (Ekiti, Oyo, Osun, Ondo, Ogun, Lagos) had the largest cut of the total amount lost to advance fee fraud at an estimate of N405,567,000 with Lagos state claiming the 90% of the total amount lost in the region

Approximately 8% of attacks carried out against financial institutions in Nigeria in 2019 involved the use of TOR software.

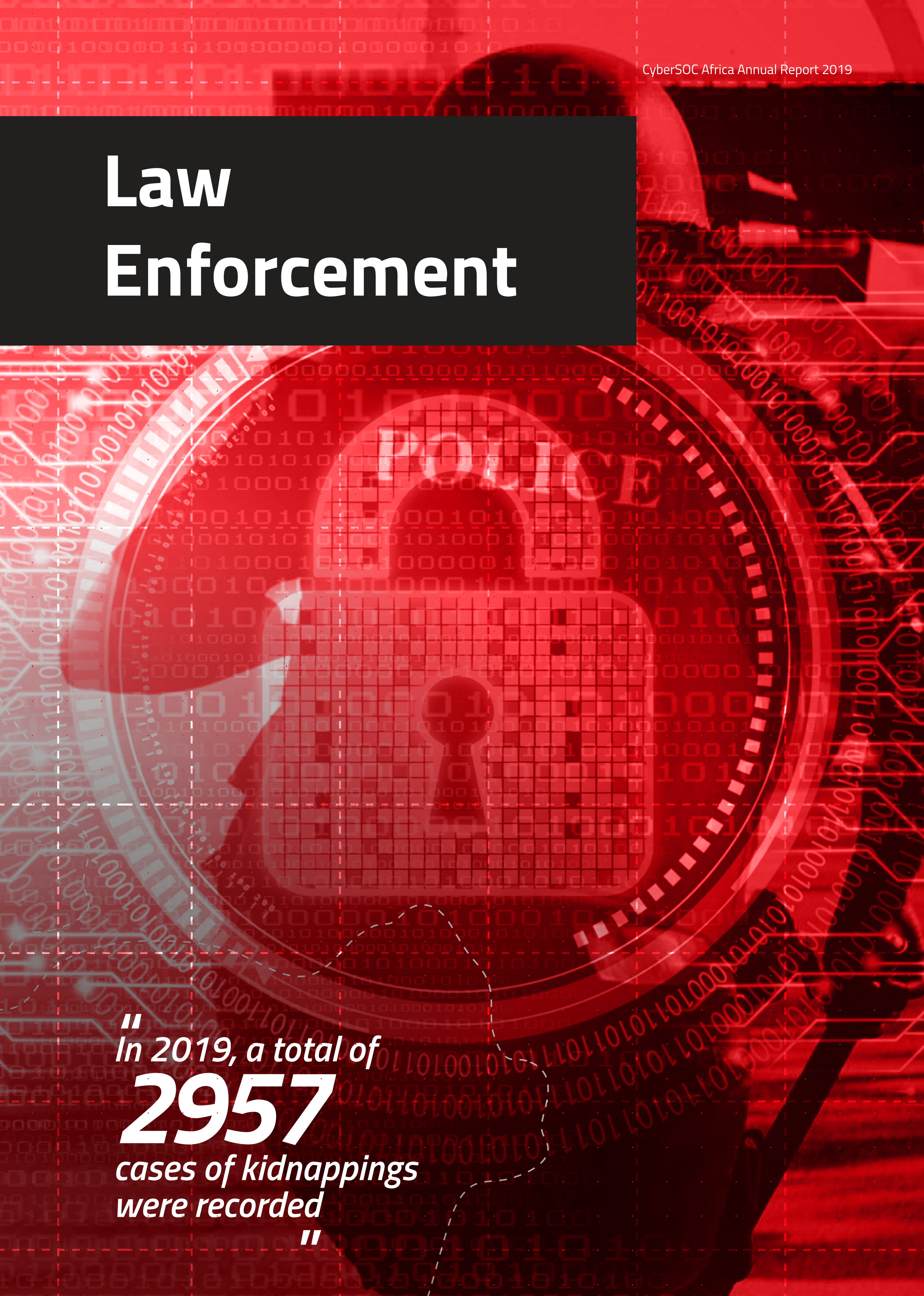
North Central region (Niger, Benue, Nassarawa, Plateau, Kogi, Kwara) accounts for an estimate of N69,003,193 with Kwara state contributing up to 90% (≈ N62,850,000) of the total amount lost in the region.
Kaduna Starred as the only state in the North Western region with an estimate of N36,138,480

Akwa-Ibom accounts for over 96% of the total amount lost in the region at an estimate of N28,234,735 of the total (≈ N28,684,735) from the South Southern States, Borno State accounts for the total estimated value of N11,059,000 from the North Eastern region, and Enugu also contributed 100% of the money lost in the South East, at an estimated value of N9,171,250.

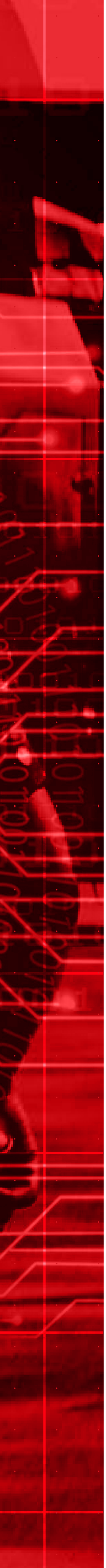
Internet Fraud:
This involves the use of internet services or software with internet access to defraud unsuspecting victims. Since it covers a wide range of illegal and illicit actions carried out in the cyberspace it is not a distinctive crime. Its mode of operation entails obstruction of information or provision of incorrect information to deceive potential victims and extort money or valuable properties from them. This type often utilizes malicious software (virus, ransomware), phishing/spoofing, denial of service, business email compromise, data breach, websites etc. for propagation of fraud.

Internet fraud related incidents recorded losses amounting to a total estimate of N759,895,555 for year 2019.
An estimated value of N525,172,580 was recorded in the South-South region with 100% from Akwa-Ibom State.
Approximately N234,500,000 in the South West with Lagos State accounting for all the money lost in the region due to internet fraud, and an estimated value of N222,975 lost in the North Central region, with Abuja and Benue sharing the total equally in the region.

Law Enforcement



> "In 2019, a total of **2957** cases of kidnappings were recorded"



Nigerian Security Landscape

Kidnapping

Kidnapping is a criminal offense consisting the unlawful taking and carrying away of a person by force or fraud, or the unlawful seizure and detention of a person against his will, oftentimes, for a ransom.

Nigeria has one of the world's highest rates of kidnap-forransom cases. Its menace has led to the loss of tens of thousands of lives, and huge sums of money.

The first notable case of kidnapping was recorded in 2006 in the Niger-Delta region of Nigeria, where expatriates in the Oil & Gas Sector were taken by militants who protested the inequality in oil profits shared and the poisoning of their lands and water bodies due to insistent and reckless oil spillage.

Since then, kidnapping has seen a quick rise, spreading wildly across other regions of the country, from the South to the terrorist sects in the North.

It has become a lucrative business for criminals especially since there has been no proper checks, mitigation and disciplinary procedures put in place by the Government, despite the creation of the Special Anti-Kidnapping Squad by the Police Force in early 2000s.

The United Nations' required standard for police protection per 500 people or 1,000 people within a space, is unattainable in Nigeria as the force is short on manpower and adequate intelligence. This has also been a serious deterrent to the fight against kidnapping in the country.

CyberSOC Africa's intelligence platform reveals that for the year 2019, a total of approximately 2957 cases were recorded.

In the first quarter of 2019, analysis showed that there were an estimate of 685 cases reported, approximately 57% of the cases occurring in Northern region (≈393). The Northwest region (Jigawa, Kano, Katsina, Kaduna, Kebbi, Zamfara, Sokoto) ranks the highest number of incidents (≈ 172) reported.

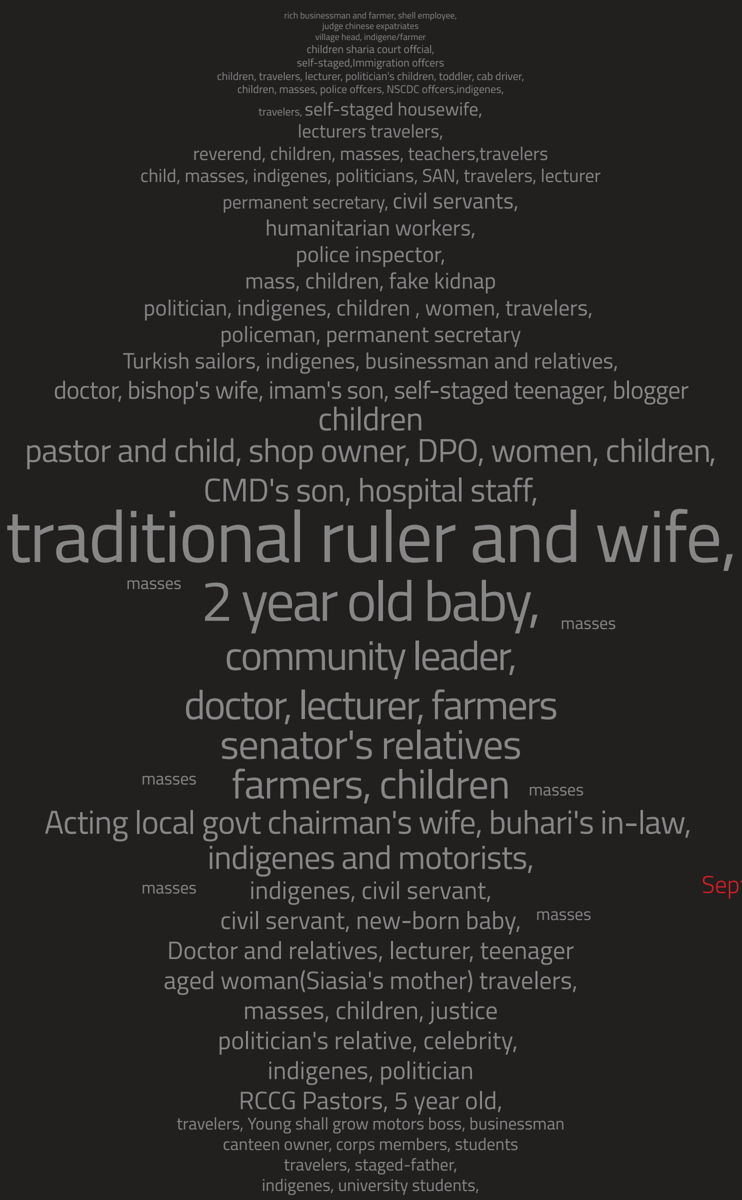
A total of approximately 292 cases, 42.6% were reported in the Southern region, with the South-South (Akwa-Ibom, Cross-River, Bayelsa, Rivers, Delta, Edo) recording the largest number of incidents at an estimated value of 120. In the second quarter of the year, approximately 537 cases were recorded with the Southern region having 55.5% (≈298) of the cases while the Northern region had 44.5% (≈239) of the cases. Surprisingly, the North-central region (Niger, Benue, Nassarawa, Plateau, Kogi, Kwara) recorded the highest number of incidents (≈108) from the North.

The third quarter recorded the HIGHEST number of kidnap incidents of the year, approximately 1049 cases. Close to half of the total cases for year 2019 were recorded in this quarter. The North contributed an estimated value of 652; Northwest - an estimate of 251 cases, North Central - approximately 244 and the North East at an estimated value of 157. The Southern

region recorded a total of approximately 397 incidents of kidnap; South-South with approximately 178, the highest.
South-East, an estimate of 128 and South-West, an estimate of 91.

October and November had a combined number of approximately 553 cases of kidnap reported. an estimated value of 303 from the North and an estimate of 250 from the South.
Kidnapping continues to rage and wreak havoc across the country with no realistic or effective approach that will see to the reduction or end of this menace any time soon.

Kidnap Summary



Profile of Victims

Figure 3 shows the profile of victims involved in the kidnap cases for the year 2019.

Resolved Vs Identified Vs Unidentified

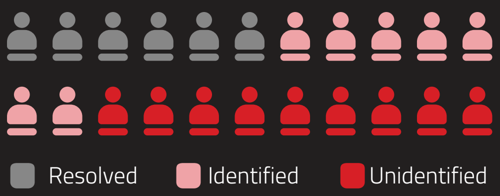
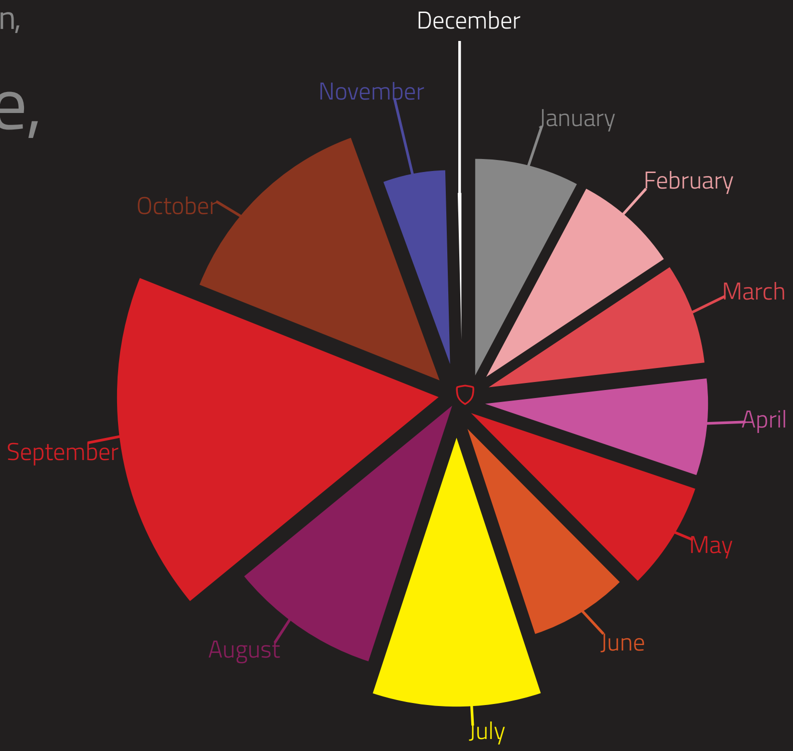
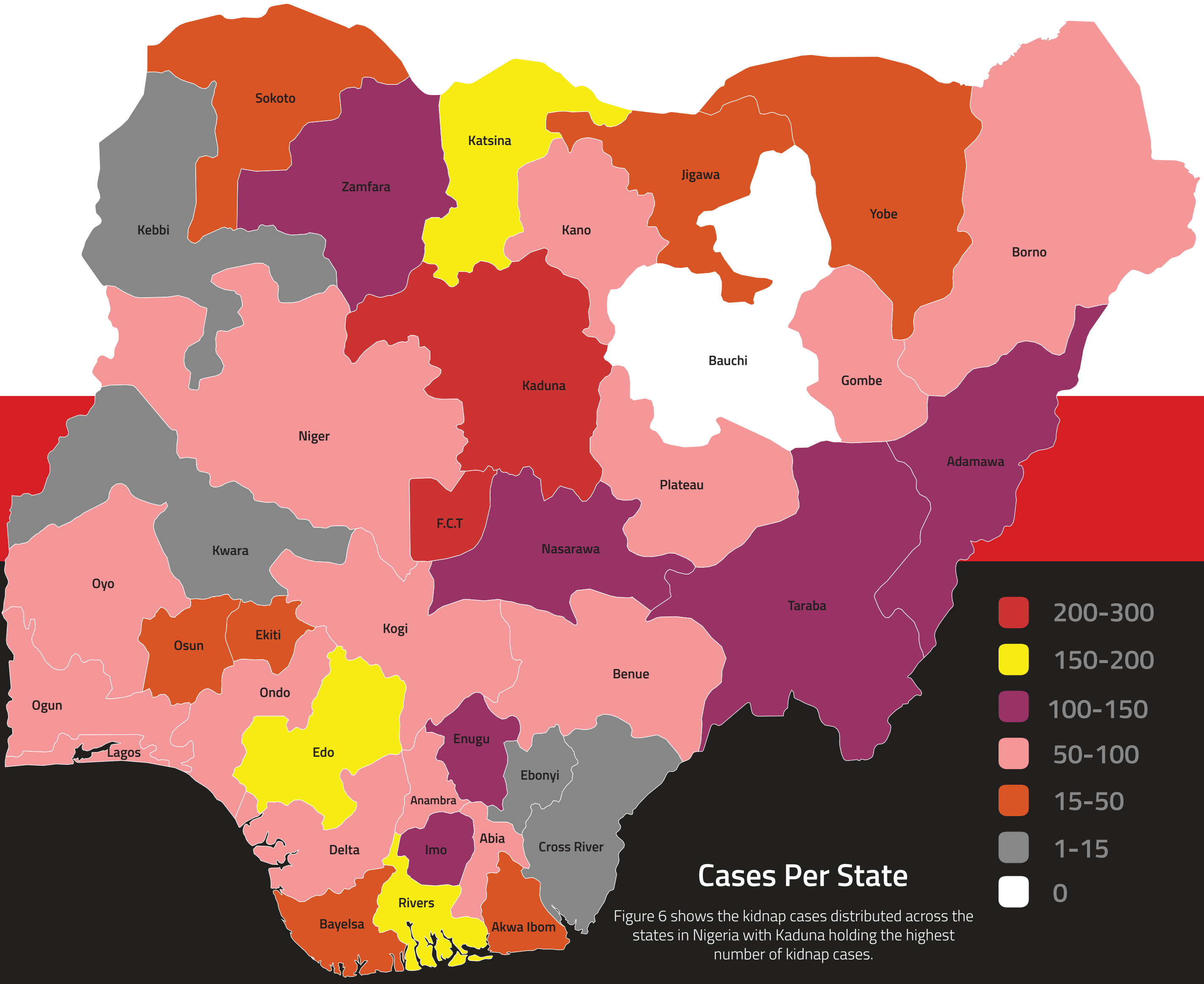


Figure 4 shows the distribution of kidnap cases in resolved, unresolved and unidentified. Majority of the cases are unidentified due to the inadequate follow up on kidnap cases after it has been reported.



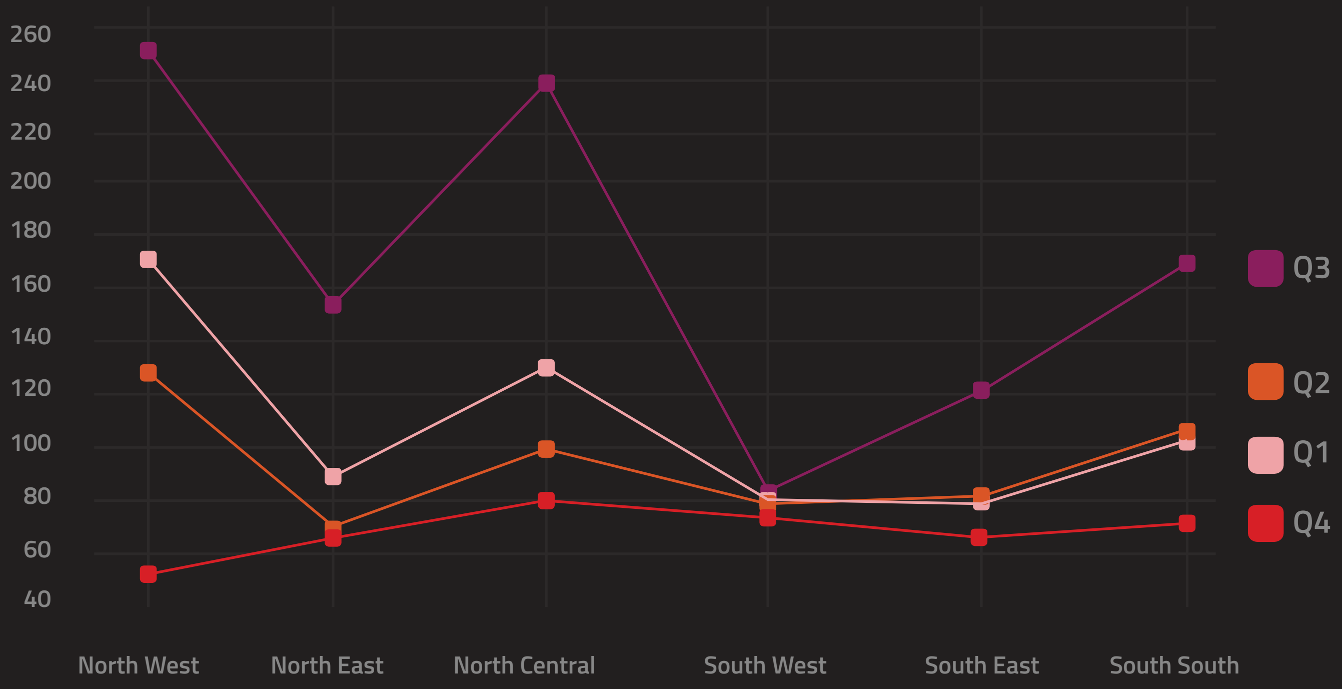
Total Number of cases per month

Figure 5 shows the number of kidnap cases recorded per month in the year 2019, with the month of September recording the highest number of kidnap cases in the year.



Cases Per State

Figure 6 shows the kidnap cases distributed across the states in Nigeria with Kaduna holding the highest number of kidnap cases.



Number of Cases Per Region and Quarter

Figure 7 shows the number of cases recorded per region in each quarter of the year. The third quarter recorded he highest number of cases,

Impersonation:
This is an act of (assuming) accessing a person's genuine personal data without authorization with the ultimate aim of defrauding him/her for illegal financial benefit. The victim's name, address, PIN, credit card details etc would be used to access his/her email, online accounts, social media accounts, bank or loan accounts.

To aid the propagation of this fraud, false or forged documents are usually used. Hence, Identity Theft, Forgery and Credit Card Fraud all fall under this category of financial fraud. Data collected for fraud involving impersonation reveals that an estimated total of N226,017,806 was lost. The breakdown of the activities per region are as follows;

Approximately N128,368,705 lost in the North Eastern region, with Borno State accounting for all the money lost in the region.
An estimated value of N 84,649,101 was lost in the South West, Lagos producing over 95% of the total money lost in the region, while approximately N13,000,000 was lost in the South East, all coming from Enugu State.

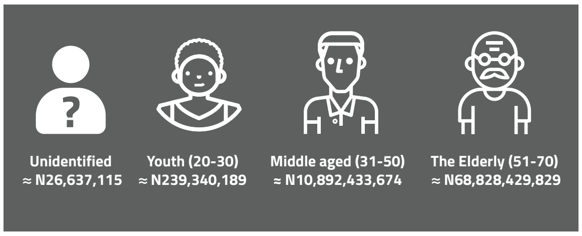
Money Laundering:
This scheme involves the realization of huge amounts of money earned through illegal and criminal means but made to appear as emanating from a legitimate source. The origin of such money is usually concealed because of its illegality as it passes through a long and complex sequence of bank transfers or commercial transactions. Recently, cryptocurrencies such as bitcoins, one coin etc. are being used for money laundering as it helps conceal details such as bank numbers, names and data of individuals involved in the fraudulent activities.

A staggering estimate of N78,441,303,788 was lost due to money laundering related activities this year. Approximately N60,347,905,530 lost in the North Central region, Abuja with over 50% of the total of loss made, and Kwara State, with about 40% the total in the region.

An estimated value of N47,800,000 in the North Western region, Kano State accounting for all the monetary losses in the region. An estimate of N46,000,000 was lost in the South-South, and Edo Sate was the sole contributor of the loss made in the region.

Approximately N44,218,049 was lost in the North East, 100% of the value coming from Borno State, and an estimate of N17,955,380,209 lost in the South West, Lagos with over 95% of the losses, and Oyo state accounting for the rest.

Fraud Age Distribution:
CyberSOC Africa's research also revealed the age range of people involved in the total amount of fraudulent schemes recorded across the country to be between 20-70



Unidentified: approximately N26,637115
The notoriety of financial fraud in Nigeria has seen both local and foreign agencies including the EFCC, ICPC, NPF and the FBI, pull resources and efforts in a bid to combat all forms of activities relating to financial fraud as they affect the local and international communities.

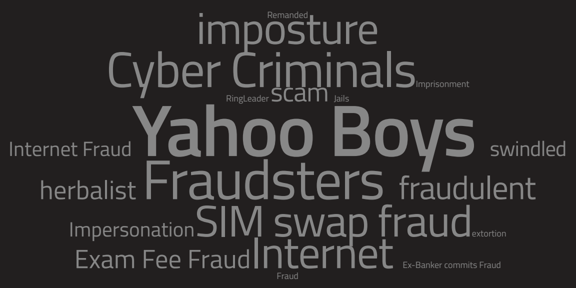
The federal government still has a lot to do in bringing an end to the menace of fraud in the society and reducing its deadly effects on lives, the economy and the overall posture/image of the country in the international community.

Fraud Summary

Money Laundering	Internet Fraud	Advanced Fee Fraud	Impersonation
N78,441,303,788	N759,895,555	N559,623,658	N226,017,806

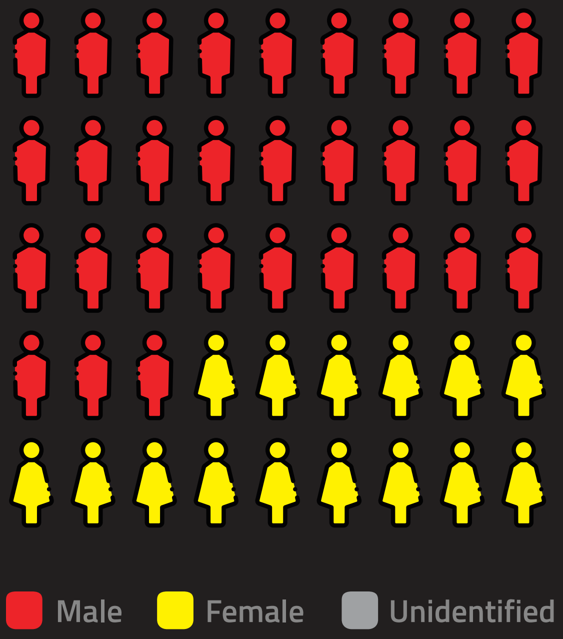
Total Amount Per Category

Figure 8 shows the category of fraud cases in the year 2019 with Money laundering accounting for the largest loss.



Trending Words

Figure 12 shows the trending terms associated with fraud in Nigeria.



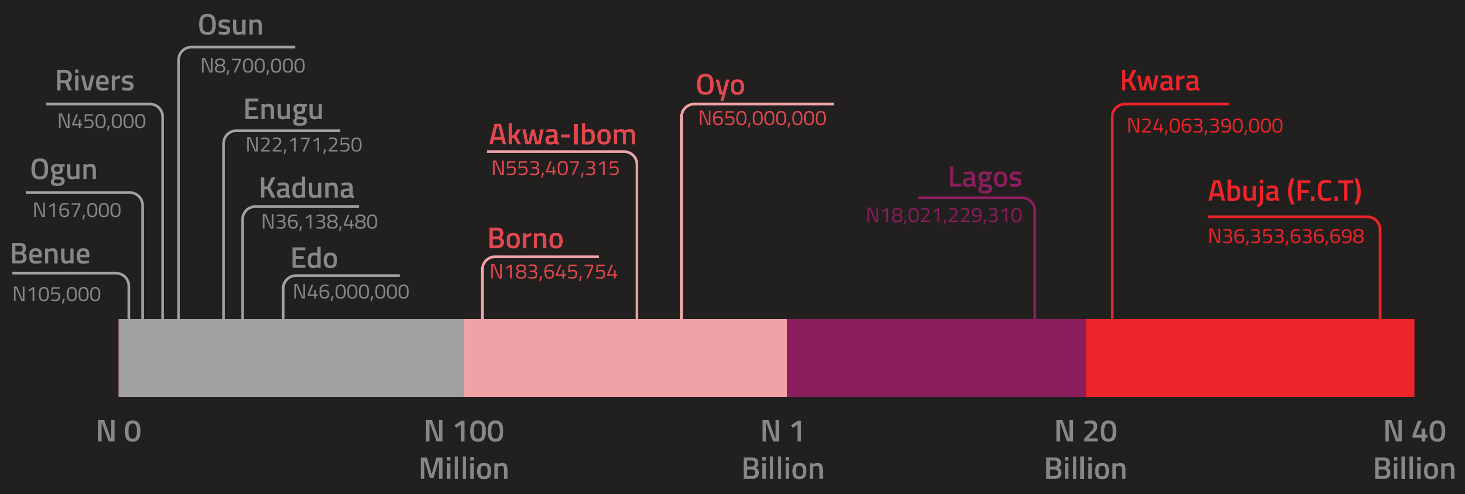
Total Amount Per Gender

Figure 9 shows the gender distribution of fraud cases with the male gender being the most involved in fraud cases

Unidentified	Youth (20-30)	Middle aged (31-50)	The Elderly (51-70)
≈ N26,637,115	≈ N239,340,189	≈ N10,892,433,674	≈ N68,828,429,829

Total Amount Per Gender

Figure 10 shows the age distribution of fraud cases with the elderly being the most involved in fraud cases.



Amount Per State

Figure 11 shows the fraud cases distributed across the states in Nigeria with Abuja holding the highest number of fraud cases.

Projections & Predictions

Projections
Cyber-criminals constantly seek avenues to exploit known vulnerabilities in security systems/infrastructures and implement newer approaches to discover new types of vulnerabilities.

An analysis of cyber-crime trends and patterns show that the modes of exploits have not really changed over the years, as some of the attack methods have been in use for a while. These attacks are still being perpetrated successfully mainly because a lot of organizations have not taken serious steps to mitigate against attacks and revamp their security postures. Majority of organizations fail to apply strategic upgrades to current network security postures, thereby exposing them to repeated attacks.

For this reason, the Central Bank of Nigeria developed a Risk-Based Cybersecurity Framework and Guidelines for organizations classified as Deposit Money Banks (DMB) and Payment Service Providers (PSP) to ensure they remain resilient with the increase in number and sophistication of cybersecurity threats. It is important to note that the framework be fully integrated into their business goals and objectives.

Based on the trends and patterns studied, and our analysis on data and statistics presented in the report, the following projections and predictions have been drawn:
An increase in network-based attacks on financial institutions is expected in year 2020, especially within the first two quarters of the year. This is because the modes

of attacks witnessed in 2019 saw a rise from 2018, albeit forms of security measures implemented by some institutions.

These forms of attacks, specifically those that involve communications with malicious IPs, insecure ports and brute force, have gained popularity and has seen a rapid rate of occurrence since 2017.
With little awareness and the security posture of most organizations still lax, defending and greatly mitigating against these forms of threats will prove very difficult.
The CBN framework has created awareness about cybersecurity and this will greatly influence the sector in which organizations and CISOs will focus their budget and investments.

Therefore, there will be an increase in the adoption of new technologies to build a more resilient infrastructure. Due to the sharp increase and consistent rate of occurrences recorded in 2019, we can also expect to witness an increase in malware and phishing related attacks in the year 2020.

Following trends from 2017, these forms of attacks have seen constant and sophisticated reinventions by cyber criminals at an alarming rate, in a bid to circumvent security measures being developed to combat the known malware
signatures and incidents.

For year 2019, organizations have done well in implementing measures (especially internally) to mitigate against data leakage and related incidences.

Hence, we project a reduction in Data Exfiltration incidents in the year 2020, provided measures put in place are strictly adhered to and revamped by organizations to keep up with current security practices.

According to trends and patterns regarding Financial Fraud schemes in Nigeria for 2019, it is expected that 2020 will see a reduction in figures and incidents.

We project, based on our report and analysis, that Money Laundering schemes should witness reduced figures and incidents, due to the awareness programs and clampdown on related activities by Law enforcement (both local and international), in conjunction with Financial institutions to fight against the menace.

There has also been a clampdown on impersonation and credit card schemes, especially with awareness campaigns by financial institutions and several forms of security technologies that have been implemented throughout 2019.
However, Advance fee fraud and Internet fraud schemes are expected to spike in 2020 due to its popularity, ease of perpetration and success rates recorded over the years.
Unfortunately, kidnapping in Nigeria is expected to rise and see more worrisome incidents and figures in year 2020. The trend has seen a consistent spike in kidnap incidents over the years with very little progress being made at curbing and solving the problem throughout the country. The economic situation, coupled with the overall deteriorating security posture of the entire country, leaves much to be hopeful for in the year 2020.

Business Email Compromise (BEC) scam is increasingly popular; however, rganizations often fail to provide appropriate security awareness to enlighten employees. Employees are the first line of organizational security defense. BEC scam rate will likely decline in 2020 due to the series of employees' security awareness provided in 2019.

Predictions

Technologies evolve at an impressive rate and alongside, new exploits and vulnerabilities that can be exploited by cyber criminals. In recent years, cyber-attack methodologies have become more sophisticated and has seen a steady success rate of exploitation.
Stronger and more sophisticated methods

and tools have been developed to detect, respond to and tackle cyberattacks and mitigate against security threats, however, these measures have seen cyber criminals become more creative in their approach to circumventing these measures. The following predictions highlight methods that could effectively obstruct the operations of cyber criminals in future:

1. The Evolution of AI as a System
One of the objectives of developing security-focused artificial intelligence (AI) has been to create an adaptive immune system for the network similar to the one in the human body, and biometric login is an example of AI's incredible contribution to cyber security.
AI's complex algorithms and pattern recognition software can also be used to effectively detect threats and malicious activities that conventional systems just cannot keep up with. AI systems can also help with mutli-factor authentication to provide access to users.

AI will also help prevent subscription services fraud: The big content streaming companies have formed an alliance designed to fight password sharing and criminal offerings of compromised passwords. Unfortunately, device-based and location-based controls are no longer holding as technologies to spoof devices and geo-location are readily available. New technologies such as behavioral bio-metrics and unsupervised anomaly detection AI will prove to fare much better against misuse of subscription services.
AI's capabilities are endless and with the right cyber security firms, the full potential of AI security systems can be attained and implemented.

2. Federated Machine Learning (Data analytics and research)
In the world of information technology today, it is impossible to deploy any effective cyber-security technology without relying on Machine Learning procedures.

Machine learning can make cybersecurity easier, more effective and proactive. However, this method is only as good as the data provided to support the machine learning process of the complete environment.

In addition to leveraging traditional forms of threat intelligence pulled from feeds or derived from internal traffic and data analysis, machine learning will eventually rely on a flood of relevant information coming from new edge devices to local learning nodes.

3. Combining AI and Playbooks to Predict Attacks (SOC playbooks and AI, Automation and orchestration)
Investing in AI not only allows organizations to automate tasks, but it can also enable an automated system that can look for and discover attacks, after the fact, and before they occur. Combining machine learning with statistical analysis will allow organizations to develop customized action planning tied to AI to enhance threat detection and response.

4. The Opportunity in Counterintelligence and Deception (Fraud, EFCC, cyber-intelligence)
One of the most critical resources in the world of espionage is counterintelligence, and the same is true when attacking or defending an environment where moves are being carefully monitored. Defenders have a distinct advantage with access to the sorts of threat intelligence that cybercriminals generally do not, which can be augmented with machine learning and AI.

5. Tighter Integration with Law Enforcement (Kidnaping and fraud, police ICPC, EFCC)
Whilst Cyber-security involves specific requirements in relation to things like privacy and access, Cyber-crime knows no boundaries. Hence, law enforcement organizations are developing global command centers and have started connecting them to the private sector, as this will enabled them to effectively respond to cyber-criminals in real-time.

References

Hervajec Group, 2019 Official Annual Cybercrime Report; Steve Morgan, Editor-in-Chief, Cybersecurity Ventures.

https://security.berkeley.edu/faq/ransomware/

http://www.nigeria-law.org/Criminal%20Code%20Act-Part%20VI%20%20to%20the%20end.htm

https://www.quora.com/What-is-the-difference-between-malware-virus-worm-and-trojans

https://tools.cisco.com/security/center/resources/virus_differences

Crime, Law and Society in Nigeria: Essays in Honor of Stephen Ellis

https://www.fbi.gov/scams-and-safety/common-fraud-schemes/advance-fee-schemes/

https://en.wikipedia.org/wiki/Spanish_Prisoner

Kidnapping Nigeria: An Emerging Social Crime and the Implications for the Labour Market by Ngwama, Justice Chidi, 2014

https://www.pulse.ng/news/local/igp-says-1071-people-killed-685-kidnapped-in-nigeria-in-2019/681pntp

The Evolution of kidnapping in Nigeria by Dennis Amachree for Bulwark Intelligence, 2017

https://www.forcepoint.com/cyber-edu/data-leakage

2018 Internet Crime Report by FBI

https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)

https://www.webopedia.com/TERM/B/business-email-compromise-bec.html

https://www.intego.com/mac-security-blog/whats-the-difference-between-malware-trojan-virus-and-worm/

https://www.us-cert.gov/ncas/tips/ST04-015

https://nigerianobservernews.com/2014/12/nature-and-types-of-fraud/

2019 Data Breach Investigation Report by Verizon

https://www.kaspersky.com/cyber-crime-lazarus-swift

https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/malicious.threats-peer-to-peer-networking-03-en.pdf

https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report-emea.pdf

www.cybersocafrica.com

CBC Towers, Olubunmi Owa
Street, Off Admiralty Road,
Lekki Phase 1, Lagos, Nigeria