



# Cybercrime in West Africa

Poised for an Underground Market

Trend Micro and INTERPOL

#### **TREND MICRO LEGAL DISCLAIMER**

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

#### **INTERPOL LEGAL DISCLAIMER**

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

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

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

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

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

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

#### **WRITTEN BY:**

Ryan Flores, Bakuei Matsukawa, Lord Alfred Remorin, and David Sancho of the Trend Micro Forward-Looking Threat Research (FTR) Team with Takayuki Yamazaki and Allan Wong of the INTERPOL Global Complex for Innovation (IGCI)

# Contents

4


The Current State of Cybercrime in West Africa

15

West African Cybercriminal Tools of the Trade

30

Are We Bound to See a West African Underground Market?



In some regions of the world, it is a fact that cybercriminal underground markets where criminals sell and/or buy products and services for committing cybercrime exist. But when the phrase “cybercriminal underground market” is uttered, Africa probably would not come to mind.

As early as 2012, Trend Micro predicted that we would see a cybercriminal underground market emerge from the region.<sup>1</sup> What are cybercriminals up to in this part of the world, especially in West Africa? The arrest of the mastermind behind Limitless following the joint efforts of INTERPOL and the Nigerian Economic and Financial Crime Commission, aided by security vendors including Trend Micro, showed that the threat of cybercrime from West Africa is growing. To more clearly map the landscape, INTERPOL conducted a survey among its member countries in West Africa.\* The survey results, combined with Trend Micro research findings, revealed that West African cybercriminals are experts in committing crimes against individuals and businesses, aided by very clever social engineering tactics.

Two major types of cybercriminals reign in West Africa—so-called “Yahoo boys”<sup>2</sup> and “next-level cybercriminals.” Yahoo boys excel in committing simple types of fraud (advance-fee, stranded-traveler and romance scams/fraud) under the supervision of ringleaders or masterminds. Next-level cybercriminals, meanwhile, are more experienced and prefer to pull off “long cons” (business email compromise [BEC] and tax scams/fraud) or crimes that require more time, resources, and effort. They use malware (keyloggers, remote access tools/Trojans [RATs], etc.) and other crime-enabling software (email-automation and phishing tools, crypters, etc.) that are easily obtainable from underground markets.<sup>3</sup>

Cybercriminals are bound to continue honing their know-how, skill sets, and arsenals to slowly but surely form their own community. There may not be a West African cybercriminal underground market now, but cybercrime is definitely an issue in the region. This can be seen from the constant increase in the volume of cybercrime-related complaints targeting both individuals and businesses that law enforcement agencies in the region receive, as shown by the INTERPOL survey.

This research paper is a product of a Trend Micro and INTERPOL partnership framework. It aims to build awareness about cybercrime across West Africa, provide an analysis of the issue, and identify effective ways to reduce the impact of cybercrime and better protect the public.

*\* The countries covered by the INTERPOL Regional Bureau for West Africa include Benin, Burkina Faso, Cape Verde, Côte d’Ivoire, Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Mali, Mauritania, Niger, Nigeria, Senegal, Sierra Leone and Togo. Those who responded to the survey include Benin, Cape Verde, Côte d’Ivoire, Gambia, Ghana, Liberia, Mauritania, Niger, Nigeria, Senegal, and Sierra Leone.*

# The Current State of Cybercrime in West Africa

## The West African Threat Landscape

One thing is clear—we are poised to see a West African underground market in the near future. This can be seen from the constant increase in the volume of cybercrime-related complaints received by law enforcement agencies in the region, according to the INTERPOL survey.

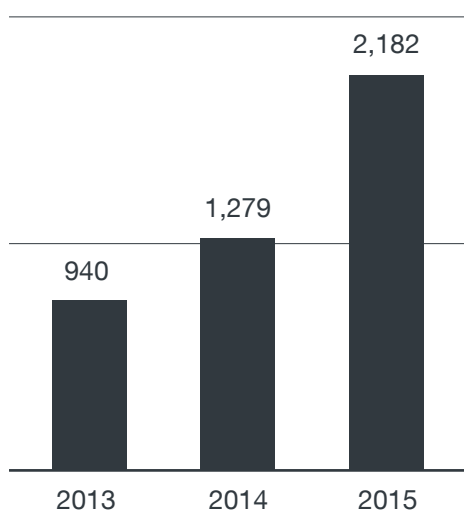


Figure 1: Volume of cybercrime-related complaints received in West Africa from 2013 to 2015

Law enforcement agents in the region did not remain idle though, as the INTERPOL survey revealed that an average of 30% of the cybercrimes reported to them each year led to arrests.

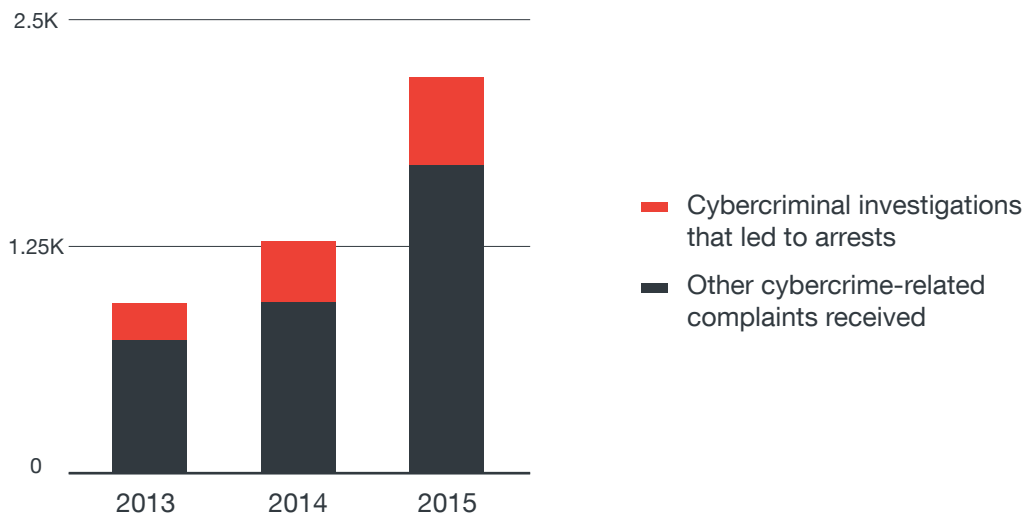


Figure 2: Volume of cybercrime-related complaints that led to arrests in West Africa from 2013 to 2015

## West African Cybercriminal Cultural Mindset

Within the West African criminal culture, there appears to be a forgiving mindset with fraud,<sup>4,5</sup> with some claims that this culture encourages cybercrime, equating it to outsmarting victims, especially foreigners.<sup>6</sup> This cultural mindset is reportedly most evident in Ghana<sup>7</sup> where sakawa—a ritualized practice of online fraud—is practiced. In sakawa, a supreme being is believed to bless criminals with protection and good fortune. This encourages West African cybercriminals to defraud foreign victims (typically Westerners) online as a means to escape poverty. It even serves as a means to justify ends, taking out the unethical element in victimizing the unwitting.

## West African Cybercriminal Profile

West African cybercriminals have one skill they are particularly good at—defrauding victims. But why resort to cybercrime? It is actually quite simple, almost half of the 10 million graduates from more than 668 African universities each year do not find employment.<sup>8</sup> According to the INTERPOL survey, West African law enforcement agencies recognize that about 50% of the cybercriminals that they identified in the region are unemployed.

The Internet aids cybercriminals to do two essential things in order to steal money from victims—create fake personas and attempt to defraud as many victims as possible. Creating personas usually involves obtaining several email addresses for various online profiles, even on social media, to support acts of fraud. Performing fraud against potential victims, meanwhile, involves sending them socially engineered emails and messages.

Note that West African cybercriminals are far more trusting than their French counterparts,<sup>9</sup> according to previously published Trend Micro research. They constantly communicate with one another. They do not hesitate to share know-how with fellow cybercriminals. This is actually how “newbie” cybercriminals learn to defraud potential victims and eventually differentiate themselves from others. They talk about which kind of people will most likely fall for particular types of fraud and what types of fraud actually work and pay off. This could be why some types of fraud that have proven effective become even more popular. In essence, the West African cybercriminal ecosystem can be considered as a self-learning portal and a self-sustaining system, improving through trial and error and the sharing of best practices.

Advance-fee fraud (also known as 419 fraud in the Nigerian Penal Code), romance fraud, and the newer BEC fraud (which will be discussed in more detail later) are not only committed by known groups. Novices start off committing 419 fraud then move on to more complicated schemes such as BEC fraud. Cybercriminal gangs, meanwhile, may prefer to pull off romance or BEC fraud. It all just depends on their preferences, needs, and available resources. The INTERPOL survey confirms that a West African cybercriminal group will generally commit multiple types of fraud.

The INTERPOL survey also revealed that West African cybercriminals are mostly between 19 and 39 years old. In addition, most reports<sup>10, 11</sup> on West African cybercriminals paint a prototypical profile—male with basic technical know-how and skills and a flair for showing off wealth in real life and on social media.

# A Comparison of West African Cybercriminal Types

West African cybercriminals can be categorized into two major types—Yahoo boys and next-level cybercriminals.

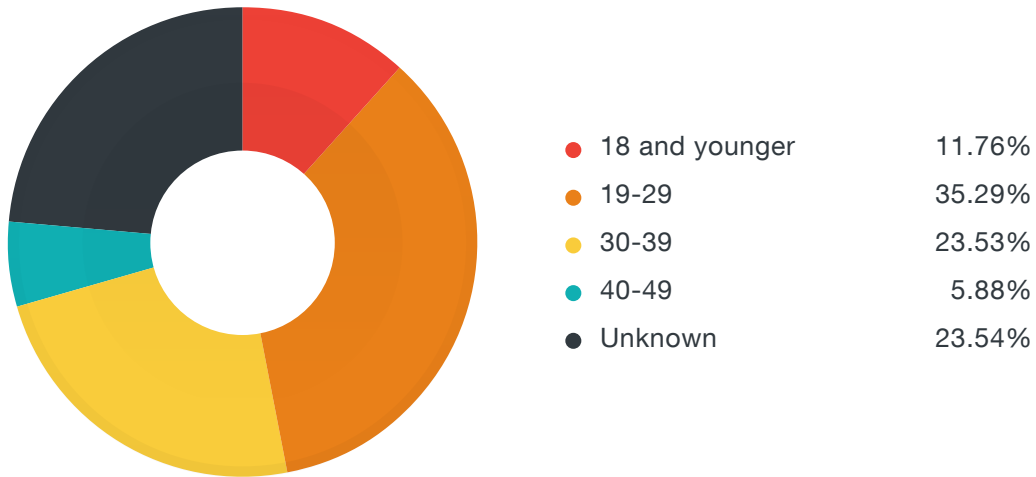


Figure 3: Cybercriminals' age ranges

## Yahoo Boys

Yahoo boys, dubbed such due to their heavy use of Yahoo!® apps for communication via email and instant messaging (IM) in the early 2000s, are often part of groups operating in the same physical location—normally cybercafés. They are supervised by more experienced cybercriminals—usually ringleaders or gang masterminds. Each cybercriminal takes care of an entire operation—from scouring the Internet for email addresses to send spam to, to communicating with each potential victim, and finally receiving the defrauded money. This operating model does not require work segmentation and specialization. Cybercriminals can use more than one fraud type at the same time. In fact, they usually run several different types of fraud at the same time. They can, for instance, run a romance fraud with one victim and an advance-fee fraud with another while sending a stranded-traveler fraud email to other potential victims.

Yahoo boys continue to use Yahoo! apps but probably not as much as in the past, when they first earned their nickname. They actively use social media, particularly Facebook®, to post pictures showing off their ill-gotten wealth—newly acquired vehicles or luxury items. Their social circles comprise contacts who generally reside in the same physical locations as they do, which tells us that they may be close friends and meet face-to-face.

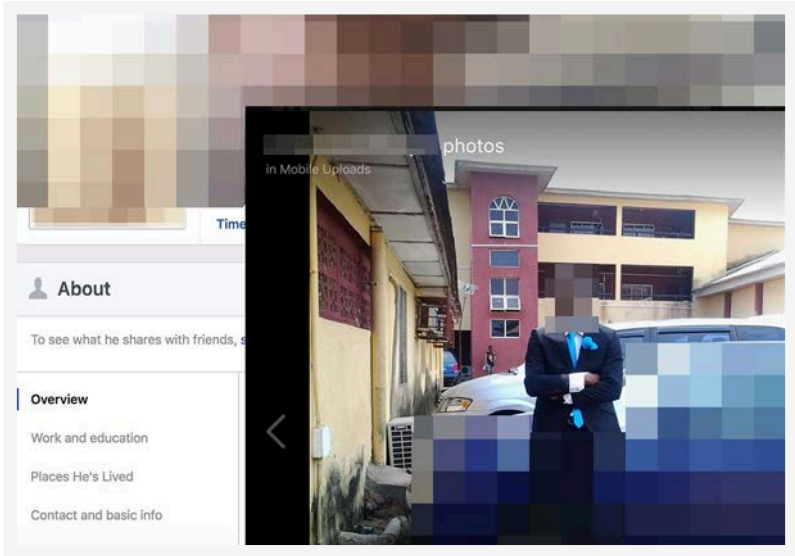


Figure 4: A Facebook page identified from research into a fraud campaign

### The Yahoo Boys Playbook

Some of the fraud types in the Yahoo boys' playbook have been repeatedly used and seen, as well as constantly improved and developed over the years.

#### *Advance-Fee Fraud*

The advance-fee fraud<sup>12</sup> is the oldest and simplest fraud type. It is also the most varied in terms of pretense and storyline, though the most popular type is the Nigerian prince fraud.

In the Nigerian prince fraud, the cybercriminal asks a target to help transfer large sums of money with the promise of compensation after providing assistance. However, prior to being compensated, the victim is asked to pay small amounts supposedly for various fees—deposits, notarization, parcel, and transfer fees—that in the end, add up to hundreds, even thousands of dollars.



Some storylines used in advance-fee fraud through the years include:

- A member of the royal family or a high-ranking government official requesting assistance in transferring wealth
- The target being an heir to a recently deceased member of the royal family
- The target being a lottery prize winner

### ***Stranded-Traveler Fraud***

Stranded-traveler fraud<sup>13</sup> first gained notoriety in the early 2010s. These used compromised Facebook and other social networking accounts to request money from the account holders' contacts. In this type of fraud, the cybercriminal first take control of an account then impersonates the account owner and asks contacts for help with an "emergency," usually while overseas. The supposed emergency can range from incarceration, kidnapping, a sudden health-related case, or being robbed at gunpoint—anything that would require immediate, no-questions-asked monetary assistance.

Recent versions of stranded-traveler fraud do not require account hacking and instead use accounts mimicking those of real people (even using their photos and personal details).

### ***Romance Fraud***

Romance fraud<sup>14</sup> typically involves creating fake but very appealing (to as many potential suitors as possible) accounts on several online-dating sites. Romance fraud can be likened to a "long con," a confidence trick that usually runs for weeks, even months. In it, the cybercriminal spends time building an online relationship with a target. Once trust is established, the cybercriminal starts asking the victim for money for various reasons, including:

- Paying for traveling fees to meet his/her "lover" in person
- A death in the family
- Disability due to an illness or an accident
- Loss of employment

While this particular type of fraud usually targets middle-aged to elderly single women, some also target men, especially recent retirees. This may be due to the preconception that they have disposable cash.

## Next-Level Cybercriminals

A new breed of West African cybercriminals has recently surfaced, who in some aspects are the opposite of Yahoo boys. They seem well-off and highly respected on social media but tend to shy away from showing off their wealth. Some are also family men and mature in terms of personal behavior.

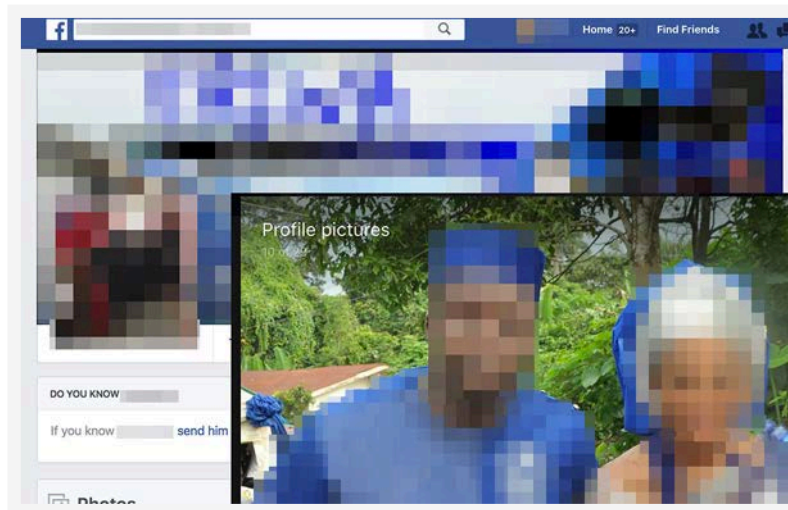


Figure 5: A Facebook page identified from research into a fraud campaign

Next-level cybercriminals engage in more complex types of fraud. As such, we can deduce that they are more technically proficient than Yahoo boys. They normally purchase keylogging software and hire encryption service providers from Russian<sup>15</sup> and other underground forums that use English.

Next-level cybercriminals also possess better money-laundering capabilities. They maintain financial accounts and connections overseas, as evidenced by the fact that they use bank accounts in the countries or regions their victims are from to pull off various types of fraud, typically BEC fraud. Maintaining overseas accounts and contacts not only makes their schemes more convincing, but hiring regional mules is often perceived to reduce the chances of law enforcement agencies identifying them. Establishing and maintaining money-laundering networks requires constant communication. Next-level cybercriminals' mules are mainly West Africans who may have migrated to target countries. In fact, the INTERPOL survey revealed that the majority of the West African cybercriminal groups expand their operations overseas. This setup—asking countrymen who reside overseas to help with illegal operations—is part of the general West African cybercriminal culture.

Trend Micro research on BEC fraud (that may involve next-level cybercriminals from West Africa) showed that the most-targeted country was the United States, closely followed by China.

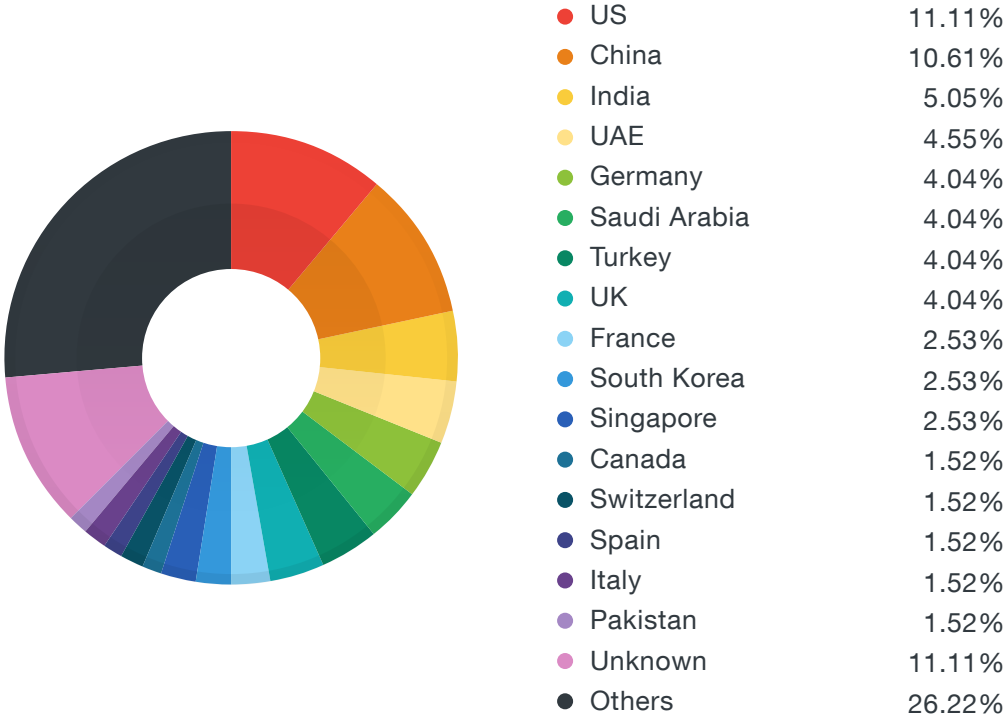


Figure 6: Locations of BEC fraud target companies in 2016

Given the same data set, we found that the manufacturing industry was the most targeted by BEC fraudsters, followed by a long list of other industries including food and beverage, transportation, and healthcare. This is possibly due to the fact that manufacturing companies typically supply resources to smaller companies and so engage in a lot of email conversations and transactions that may contain invoice details.

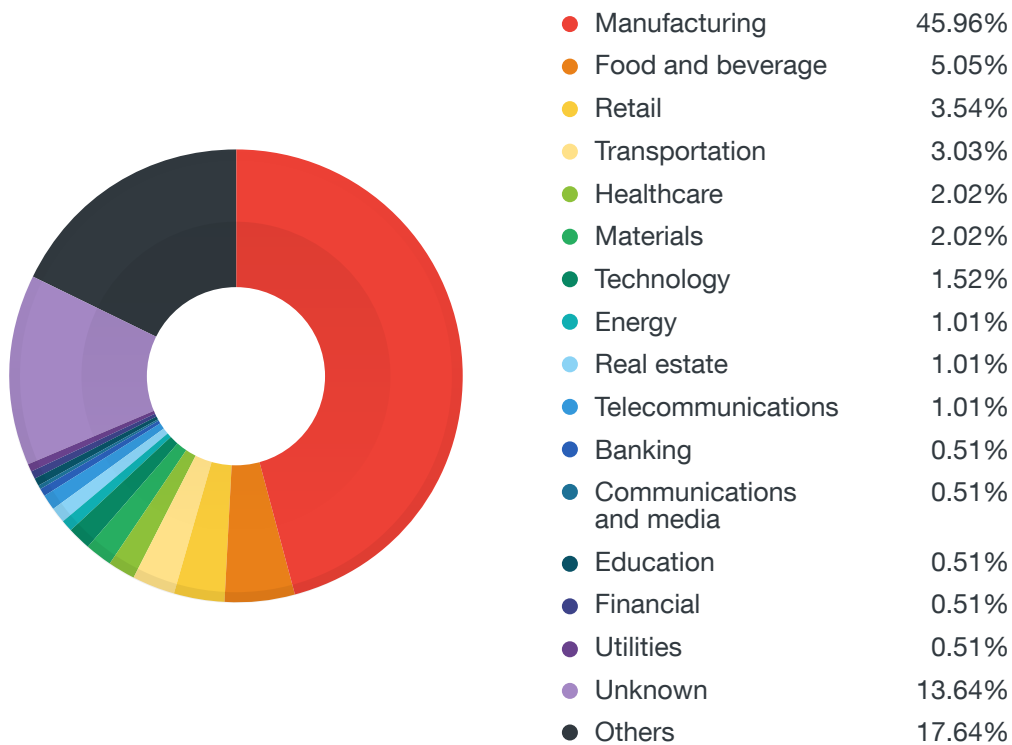


Figure 7: Industries targeted by BEC fraud campaigns in 2016

## The Next-Level Cybercriminal Playbook

### *BEC Fraud*

BEC fraud<sup>16</sup> typically involves the cybercriminal using a compromised business email address to intercept and spoof in-office communications and eventually trick top executives or company officers to wire money to a bank account under the criminal’s control.

BEC fraud can take various forms, five of which were listed in an official warning from the Federal Bureau of Investigation (FBI).<sup>17</sup> All five types have the same core idea—deceiving employees with access to corporate financial resources into paying out large sums of money. The only real differences being the people impersonated or spoofed and the reasons for requesting funds (legal settlement fees, funds for “secret” deals, emergency salary advances, etc.). In all of them, the modus operandi remains the same. FBI reports show that between October 2013 and May 2016 alone, more than US\$3 billion was stolen by BEC fraudsters.<sup>18</sup>

## ***Tax Fraud***

Tax fraud<sup>19</sup> is the most recent entry to the next-level cybercriminals' playbook. It only recently gained notoriety in the West African region and usually targeted U.S.-based companies toward the end of the tax season (from January to April).

Tax fraud follows the same pattern as BEC fraud—a cybercriminal impersonates an executive of the victim company then requests for payroll and W2 form information from the human resources (HR) or finance department, usually via email. Should the HR or finance department fall for the ruse and send the information over, the cybercriminal uses that data to steal tax refunds intended for the actual taxpayers.

Note that BEC and tax fraud requires much more time and effort on the cybercriminals' part than the types of fraud seen in the Yahoo boy's playbook. They require reconnaissance and in-depth research on the executives and companies the cybercriminals wish to target, as well as enough technical know-how to maintain access to the compromised business email accounts. Often, cybercriminals move laterally, not just within a target company, but also to external companies associated with it—partners, suppliers, and so on. All of this is proof of West African cybercriminals' continuing evolution, including purchasing and using products and services sold in established underground markets such as those of Russia and China.<sup>20</sup> These include malware, crypters, keyloggers and bulletproof-hosting services, among others.

## **Cybercriminal Operation Structure and Payoff**

The INTERPOL survey revealed that Internet fraud targeting businesses instead of individuals enabled West African cybercriminals to steal more money. An average of US\$2.7 million from businesses and US\$422,000 from individuals is stolen each year (data from 2013 to 2015 was used). This could be the reason why we are seeing an increase in the BEC fraud volume over time.

The INTERPOL survey also revealed that almost half of the West African cybercriminals profiled only knew their peers online. This characteristic is more applicable to next-level cybercriminals, however, than Yahoo boys.

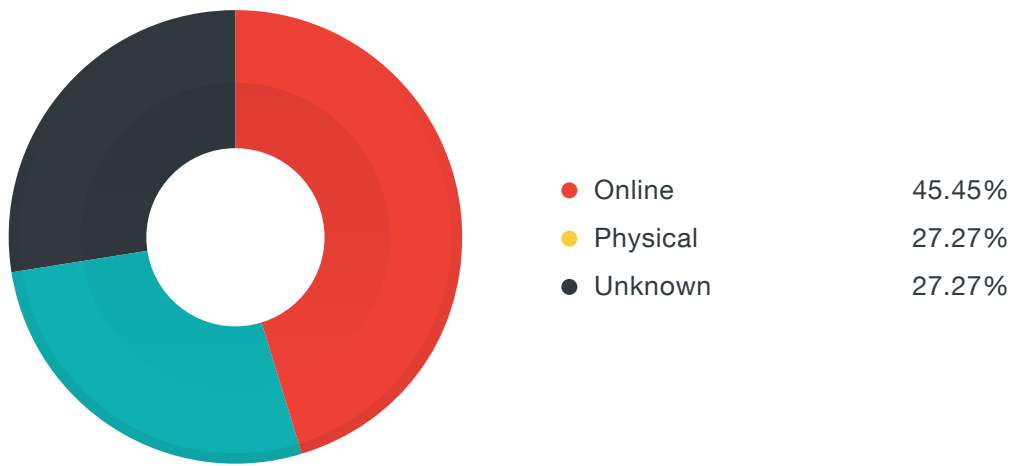


Figure 8: Cybercriminal relationship breakdown

INTERPOL surveyed respondents to identify the roles that cybercriminals played in a group. The respondents were asked to choose from among five categories—leader, fraud operator who actually engages in social engineering activities, financial operator who manages monetary transactions, IT technician who takes care of the operational infrastructure, and money mule. The small number of money mule arrests could be due to the fact that many of the mules reside outside West Africa (typically where they are required), which poses jurisdiction and proportionate resource considerations for law enforcement agencies. West African law enforcement agencies’ attention is directed at cybercriminals residing in the region and so more technicians and fraud operators are apprehended. In addition, these roles are also the most overt in terms of interacting externally and engage in activities that leave traces that law enforcement agencies and security researchers can jointly explore and take action on as investigation leads.

Role	Response Share
Leader	44%
Fraud operator	67%
Financial operator	22%
IT technician	78%
Money mule	33%

Table 1: Typical roles seen in a cybercriminal operation according to law enforcement responses

# West African Cybercriminal Tools of the Trade

\* Note that all of the images that appear in this section were obtained from publicly accessible sources.

## Email-Automation and Phishing Tools

The majority of the Internet fraud originating from West Africa is instigated via spam. West African cybercriminals start by gathering target email addresses using free and readily available tools, the most popular of which is Email Extractor Lite—an online tool hosted at evil-brain.org.

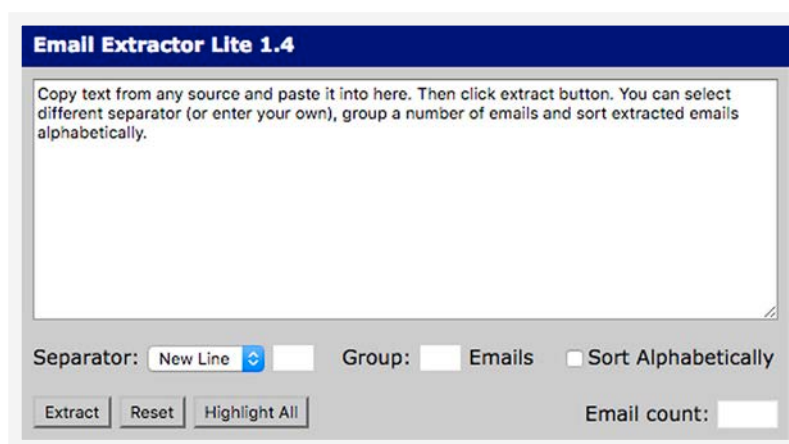


Figure 9: Email Extractor Lite 1.4's console

Other West African cybercriminals use a much more advanced tool dedicated to harvesting email addresses from websites. The two most popular of these tools are Bulk Email Extractor, which crawls through web pages to gather email addresses, and GSA Email Spider, which harvests email addresses aided by search engines. These tools allow West African cybercriminals to filter victims, depending on the types of fraud they are running.

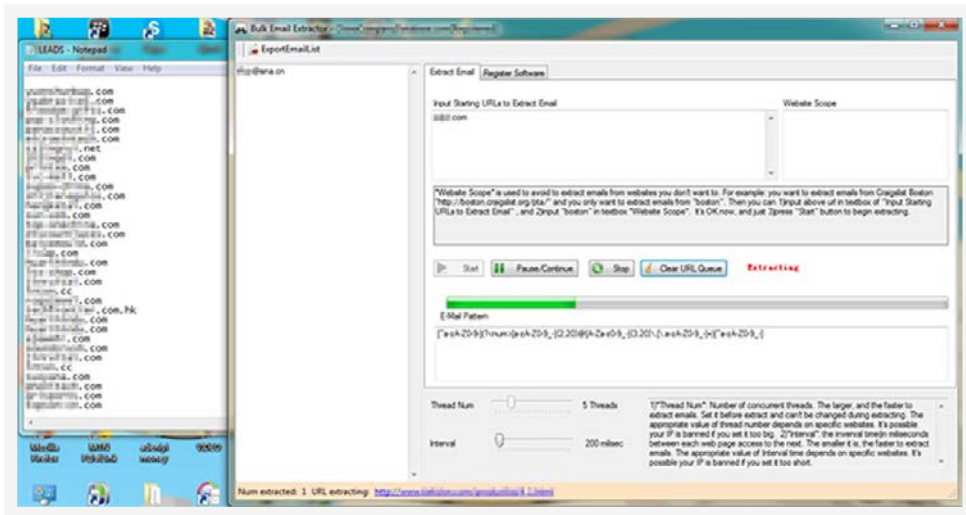


Figure 10: Bulk Email Extractor's console

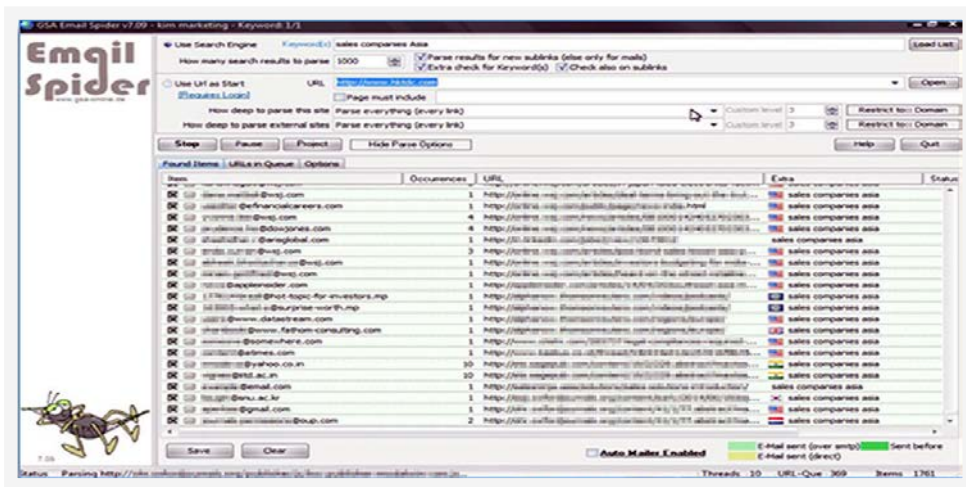


Figure 11: GSA Email Spider's console

To automate spam sending when carrying out attacks, West African cybercriminals usually hack legitimate servers then use tools such as PHPMailer—an open source, full-featured email-creation and transfer-class tool. Note that PHPMailer and most email-automation tools such as those discussed in this section are not necessarily malicious in nature.





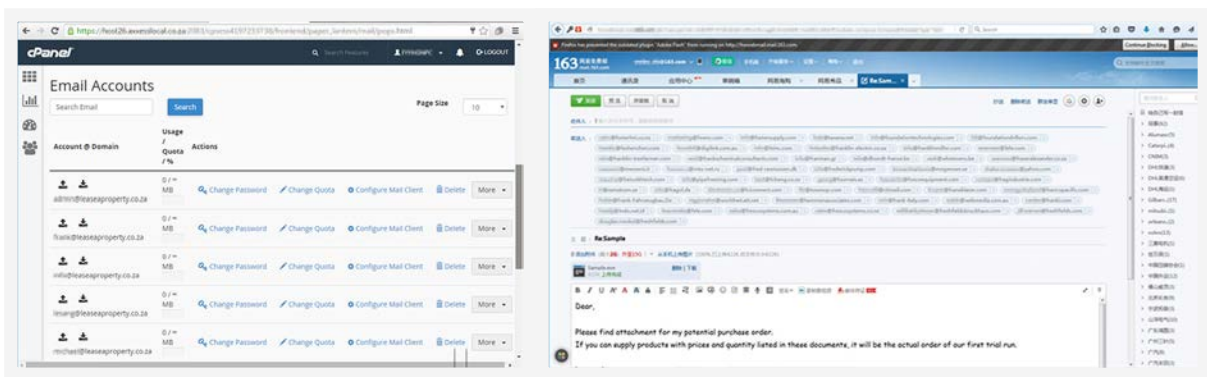


Figure 14: Tools used to send out spam from compromised and/or fake company email mailboxes

Not only do West African cybercriminals use fake domains to set up several mailboxes for spamming, they also use these to set up fake company web pages. These fake pages serve as phishing sites, luring users to sign up with their email addresses. The owners of the email addresses, in turn, become the next phishing or spear-phishing targets.

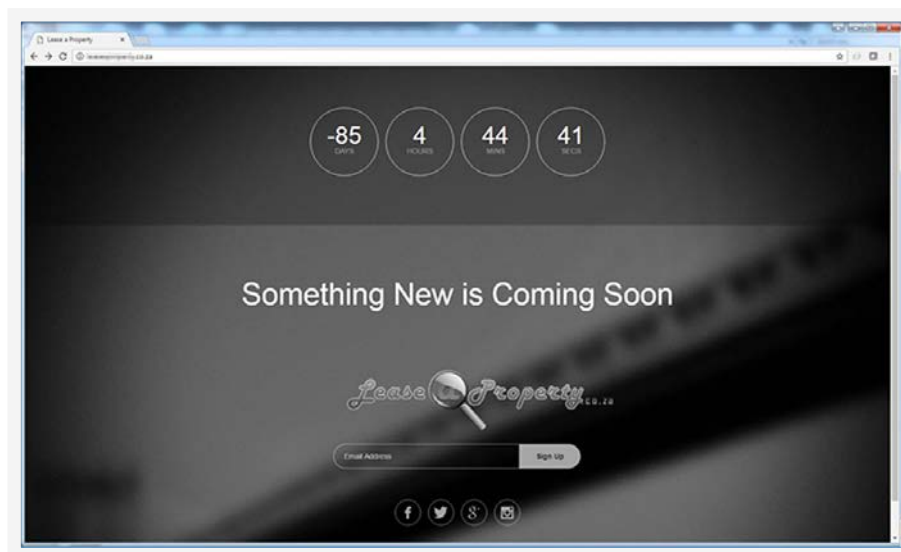


Figure 15: Fake company web page used to phish for email account credentials

West African cybercriminals who pull off romance fraud use online-dating sites to find targets. They engage targets in fake romantic relationships. Once a strong trust relationship has been built, the cybercriminal starts asking the victim for money by telling tragic stories that require financial assistance.

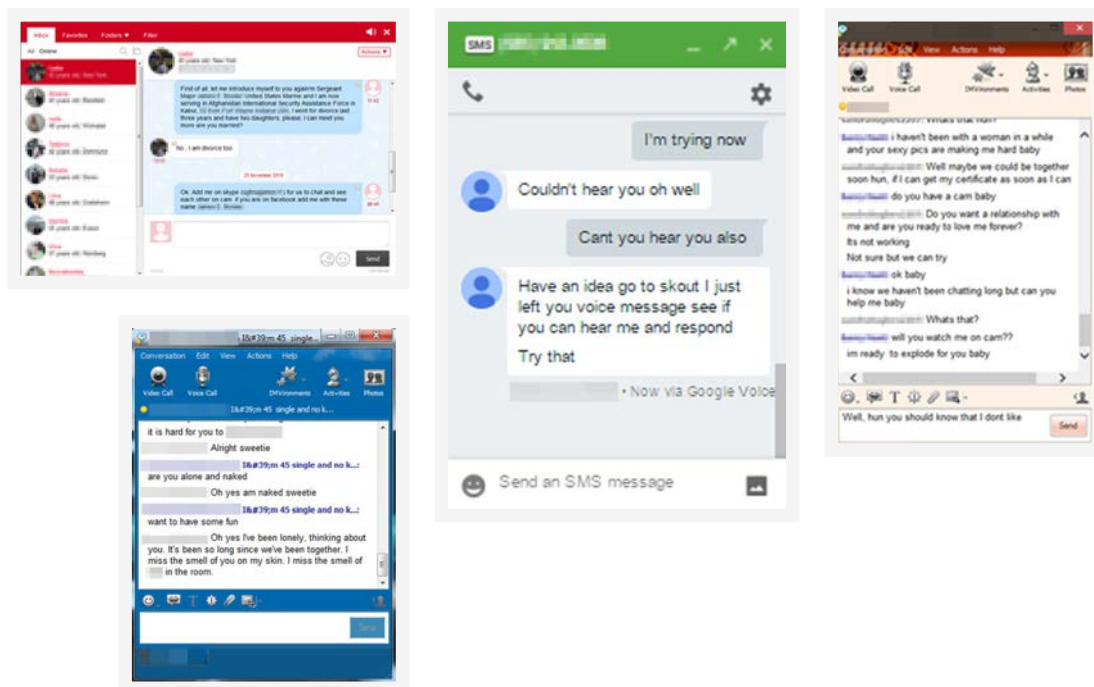


Figure 16: Sample romance fraud chats

Though sextortion<sup>21</sup> is somewhat similar to romance fraud, the two differ in terms of means to obtain money. While romance fraudsters cajole and seduce victims by inducing pity or sympathy, sextortion operators rely on blackmail to get money from their victims.

Cybercriminals behind sextortion use apps such as Virtual Cam Whore to trick victims (normally men) into thinking they are attractive women. The app simulates a webcam feed using prerecorded video footage of an attractive woman waving at the camera, winking, or performing sexual acts. These prerecorded actions are controlled by the criminal. A victim may then be fooled into thinking the woman he is watching is truly interacting with him. In response, the cybercriminal tricks the victim into performing sexual acts that will be recorded and later utilized for blackmail.

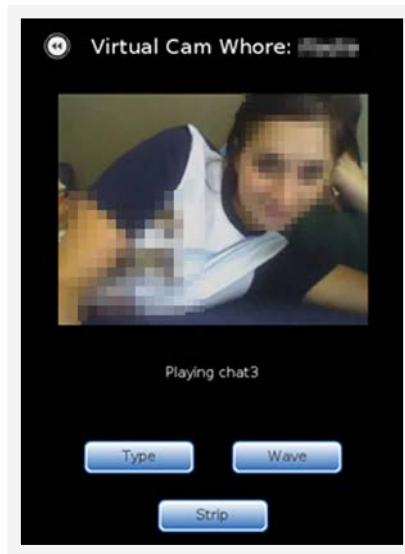


Figure 17: Sample footage seen via Virtual Cam Whore

## Malware and Crypters

As far back as 2013, we began seeing West African cybercriminals use banking Trojans, specifically Ice IX,<sup>22</sup> to gather victims' credentials. As BEC fraud gained popularity, RATs and keyloggers quickly took banking Trojans' place. For instance, Nigerian cybercriminals arrested as a result of a joint effort between INTERPOL and security vendors, including Trend Micro, in August 2016,<sup>23</sup> used keyloggers such as Predator Pain and Limitless.<sup>24</sup>

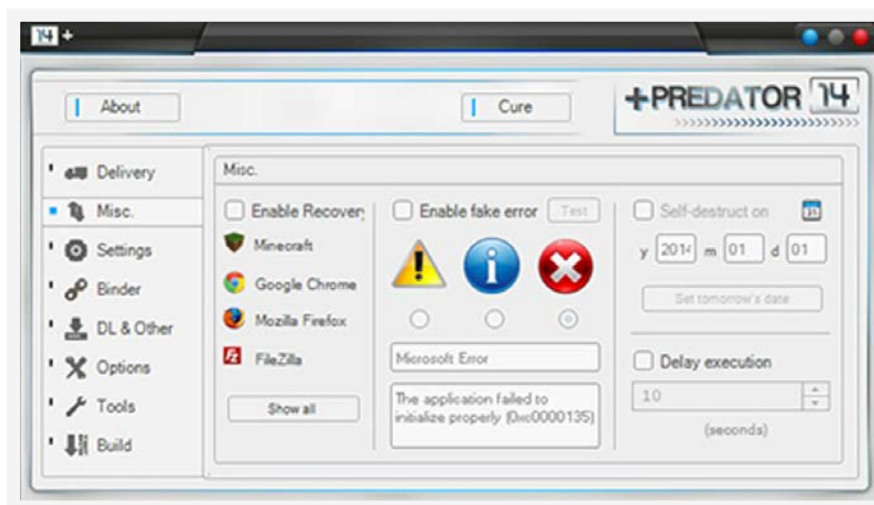


Figure 18: Predator Pain's console

Using ready-made malware is advantageous to nontechnically proficient cybercriminals—the kind typically seen in West Africa. These tools are readily available in any of the more advanced and established underground markets.<sup>25</sup> They are also sold at very affordable prices, ranging from US\$20 to US\$100, or can even be obtained free of charge.

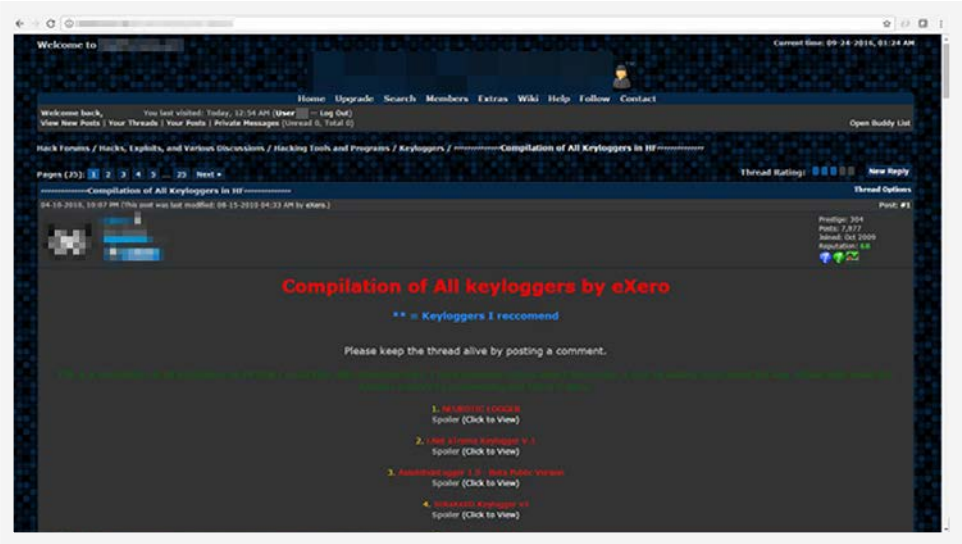


Figure 19: Sample keylogger offerings seen in a typical underground forum

Another advantage of using RATs and keyloggers is that they are regularly employed by a large number of cybercriminals worldwide. They are easy to set up and use, thanks to the various online communities that offer how-to guides and troubleshooting help.

Finally, keyloggers are very effective BEC fraud tools because they can dig up even cached or browser-stored account credentials. All the cybercriminals need to do is retrieve the corporate email account credentials stolen by keyloggers, intercept any ongoing business transactions, and use those accounts to get to their next victims.

Unencrypted malware can be easily detected and blocked by anti-malware solutions. That is why cybercriminals use crypters and counter-antivirus (AV) services to evade detection. Like malware kits, crypters can also be easily bought from hacking forums and other underground marketplaces. Their prices vary considerably, depending on their popularity and complexity. Some sellers even offer configuration advice and technical support.

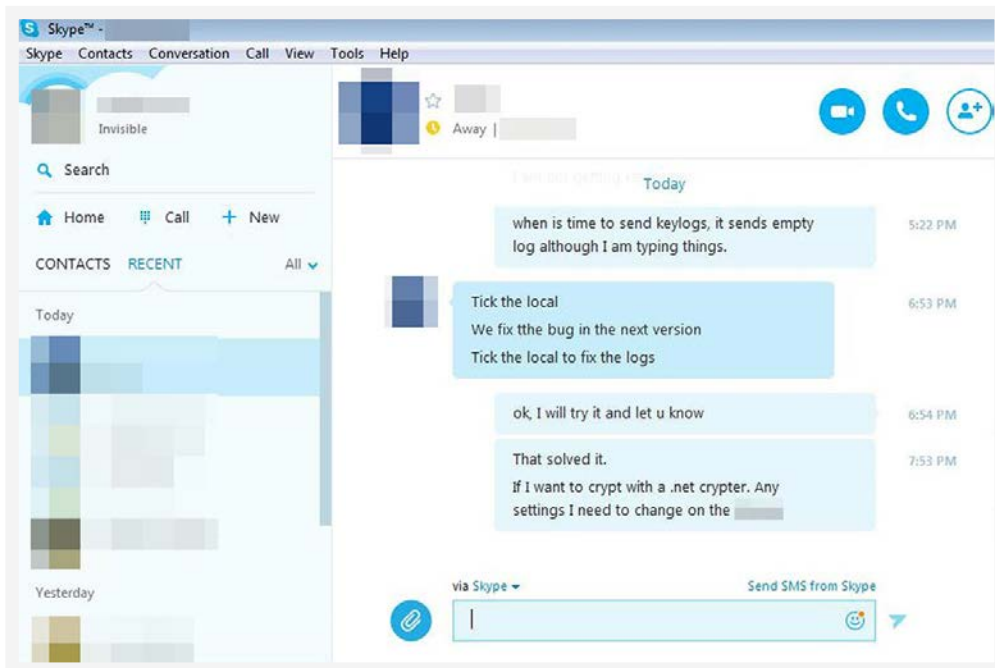


Figure 20: Cybercriminal asking a crypter seller how to use the product

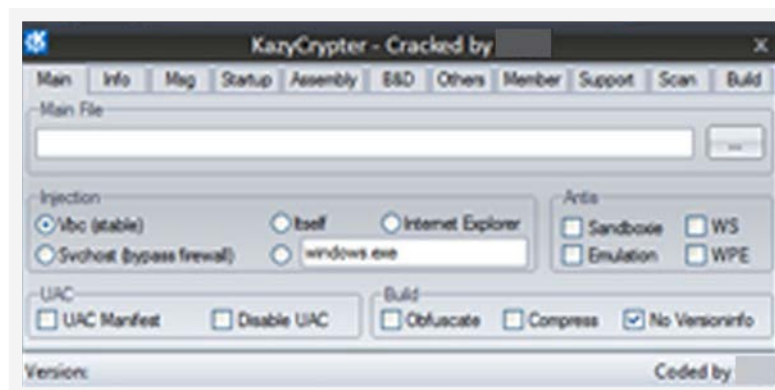


Figure 21: Sample crypter—KazyCrypter—sold underground

## Communication Tools

West African cybercriminals typically operate in tight-knit groups. Each group member constantly communicates with peers—sharing targets, compromised email accounts, tools, and best practices. Though cybercriminals use attack tools usually restricted to technical communities or only commonly seen in underground markets, the communication tools they use are less clandestine in nature. According to the INTERPOL survey, most West African cybercriminals use email and social media to communicate with one another although some still use IM applications such as Yahoo! Messenger.

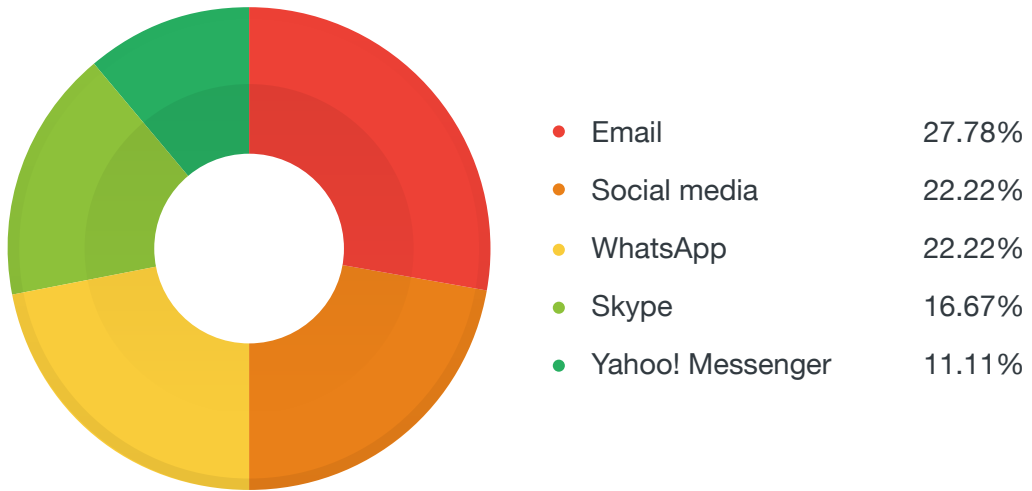


Figure 22: Cybercriminals' preferred communication tools

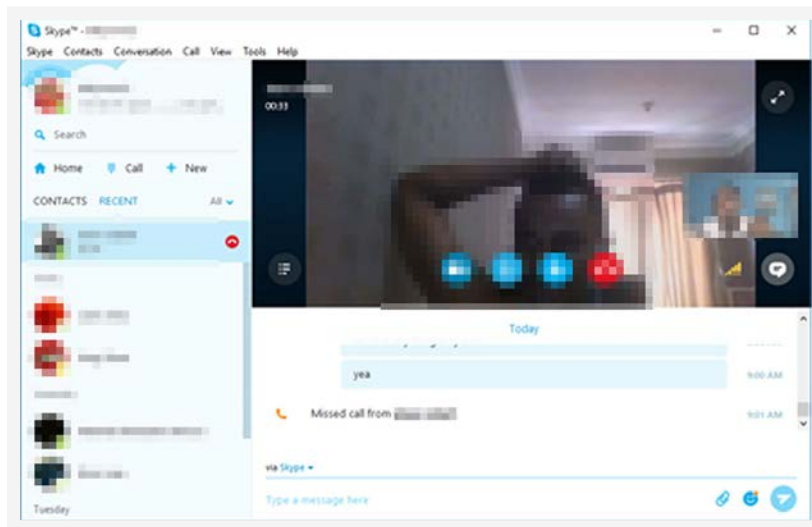


Figure 23: A Skype screenshot identified from research into a fraud campaign

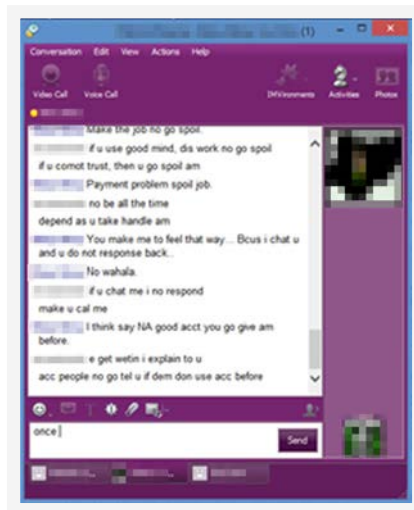


Figure 24: A Yahoo! Messenger screenshot identified from research into a fraud campaign

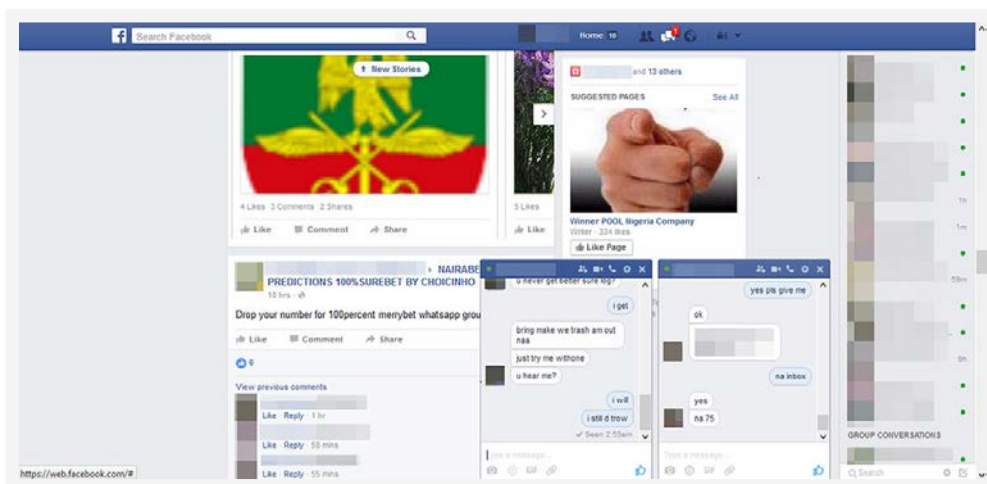


Figure 25: A Facebook Messenger screenshot identified from research into a fraud campaign

According to the INTERPOL survey, when targeting businesses, West African cybercriminals prefer to use email although online-dating websites, social media, and IM applications are also used when engaging a target. When targeting individuals, however, they prefer to use social networking and online-dating websites, which were primarily created for personal use.



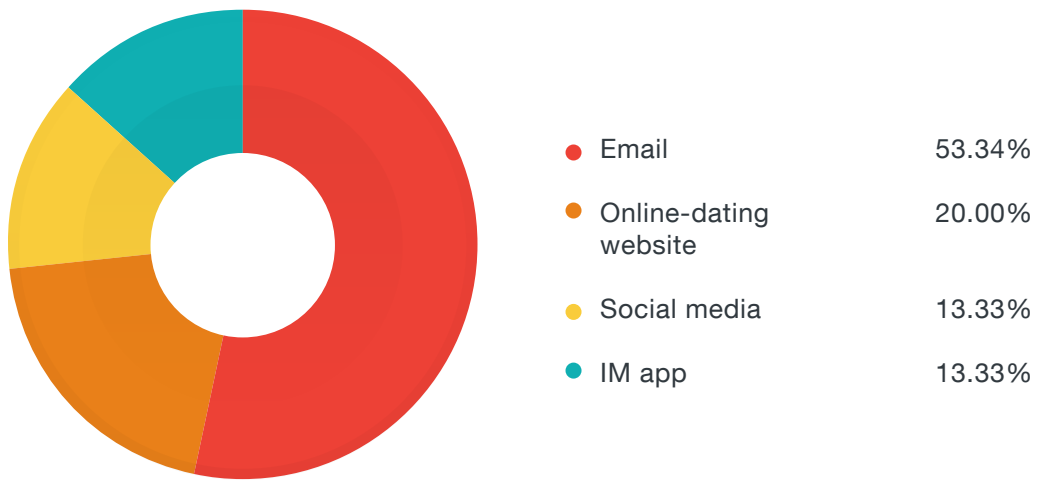


Figure 26: Portals used by cybercriminals to target businesses

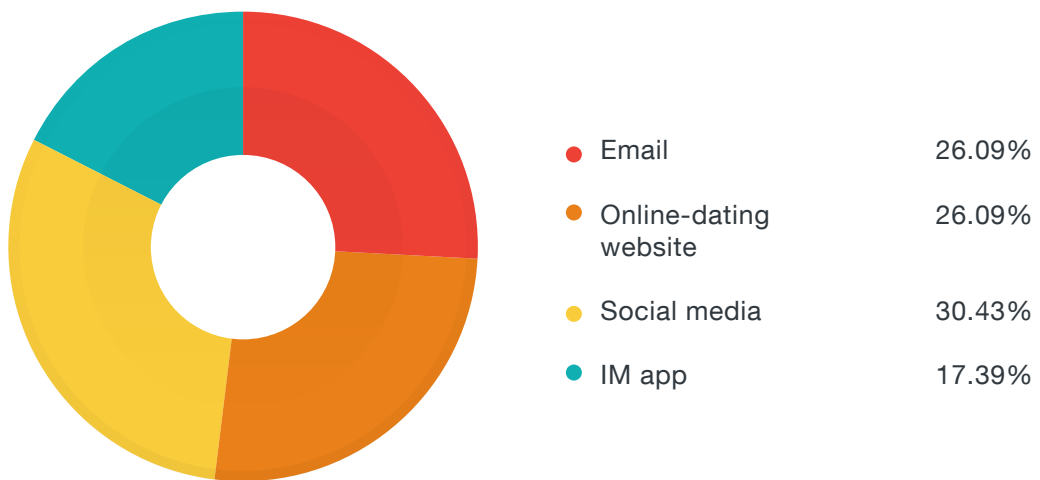


Figure 27: Portals used by cybercriminals to target individuals

# A Closer Look at a West African Cybercriminal Operation: Z\*N

In the course of conducting research on West African cybercriminals, we came across an actor who exemplifies our operational and behavioral observations. This actor installs keyloggers on victims' corporate computers then uses the email credentials he steals to hijack business transactions and direct funds to his own personal account. While perpetrating one of his schemes, he mistakenly installed the keylogger he was using on his own machine, allowing us to access his logs and find very interesting information about him, his background, and modus operandi. This error allowed us to obtain screenshots from a publicly accessible open directory.

We selected some screenshots that showed how his operation works. Bear in mind that the examples featured in this section do not pertain to a single operation or victim so they do not form a single story. All of them, however, came from a machine that we have dubbed “Z\*N” and illustrate the different stages of a range of crimes that the operator engages in on a daily basis.

## Steps in a Typical West African Fraud Operation

The first step in a typical fraud operation is composing and sending out spam. The email is generic in nature and should appear nonmalicious while convincing the intended victim to take the bait.

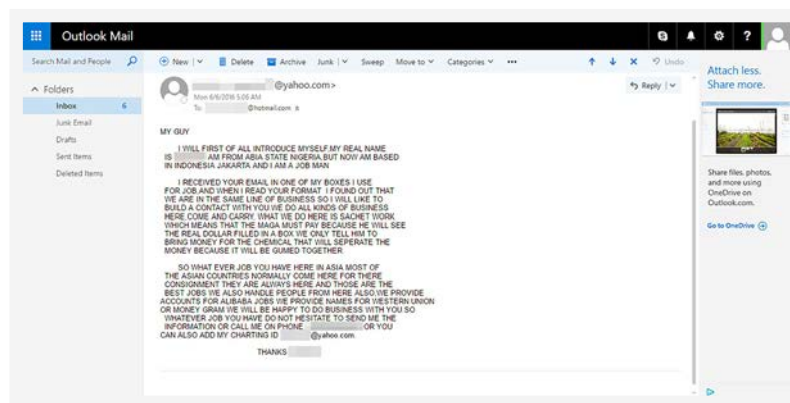


Figure 28: Typical socially engineered email

The cybercriminal then prepares the malicious file, encrypts it, checks it with a counter-AV tool, and renames it specifically to fit his conversation with a victim.

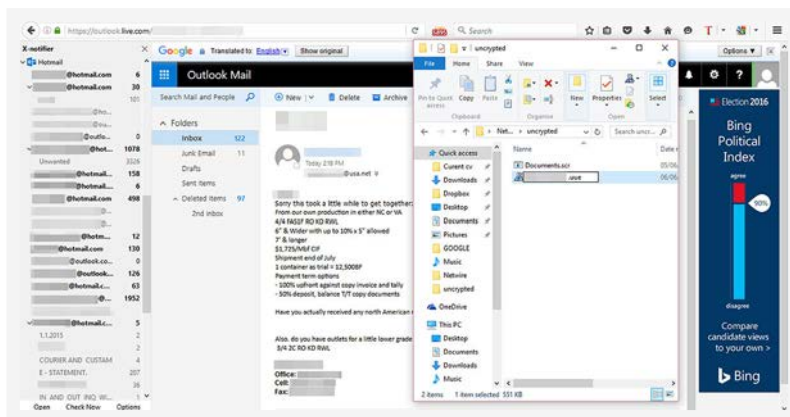


Figure 29: Cybercriminal renames the malicious file to fit the email's content

In more sophisticated attacks, the cybercriminal also configures the RAT so that only he can control the infected machine, which means only he can remotely access an infected machine because only he has the password.

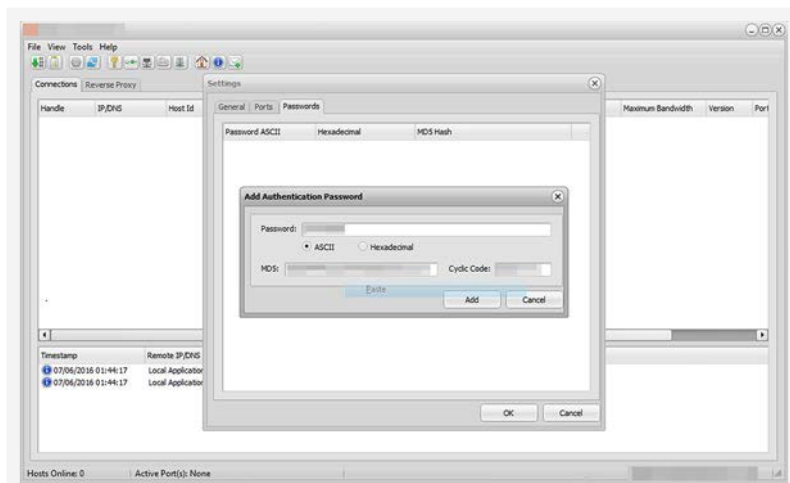


Figure 30: Cybercriminal password-protects the RAT so only he can control the machine it runs on

The cybercriminal replies to a victim who took the bait. In his reply, you can see that the victim already ran the Trojan and so infected her computer.

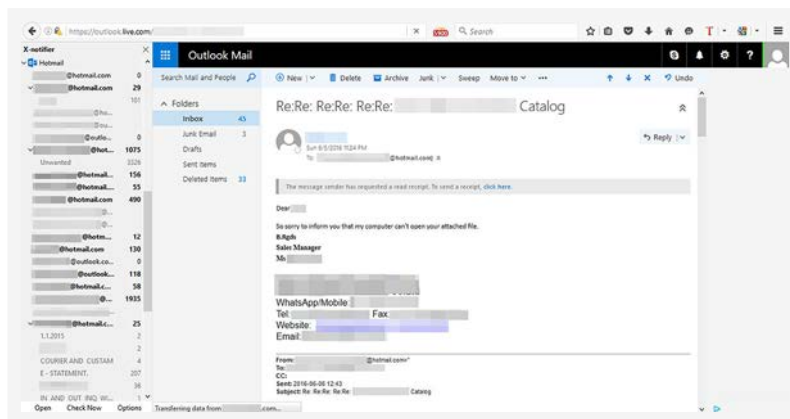


Figure 31: Opening the malicious file attachment led to the infection of the victim’s system

Once the cybercriminal gains control of the victim’s machine, he can log in and remotely manage it.

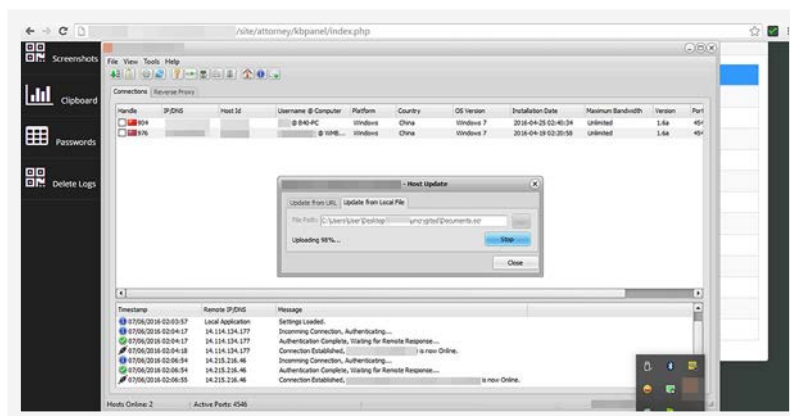


Figure 32: Cybercriminal remotely manages access to and controls infected PCs

After some time, the cybercriminal collects logs (where passwords stolen from infected PCs are saved) from the command-and-control (C&C) server via a web console.

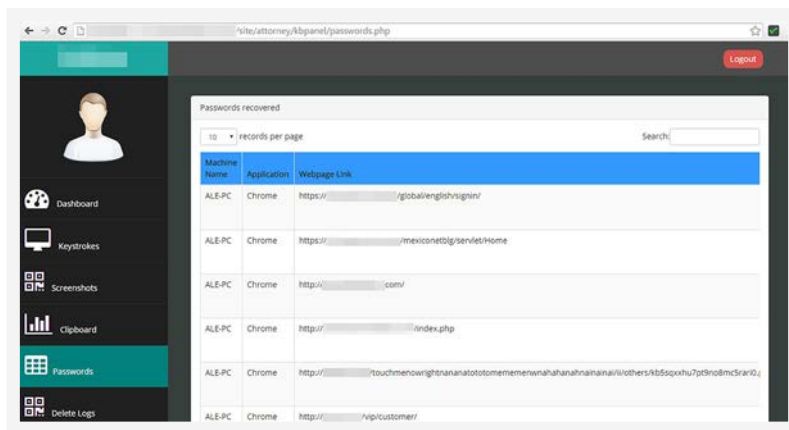


Figure 33: Logs containing passwords stolen from victims' PCs

The passwords stolen from the victim's PC allow a cybercriminal to hijack email conversations with persons of interest such as suppliers.

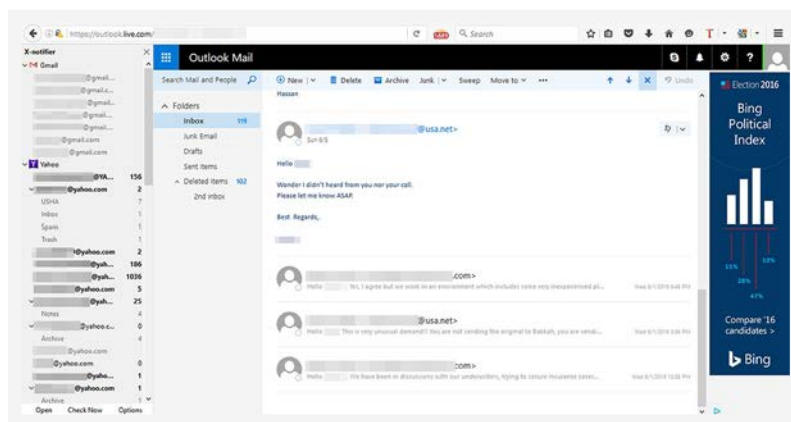


Figure 34: In a conversation, a supplier was somewhat surprised by some of the cybercriminal's responses but still bought the story

West African cybercriminals, as has been said, constantly communicate with peers using even their personal accounts. We saw evidence of this in Z\*N's logs. The cybercriminal logged in to Facebook using his own phone number. By searching for the cybercriminal's phone number on Facebook, his personal account became identifiable. Knowing all of the information about Z\*N and his operation helps law enforcement agencies possibly launch an investigation to help rid not just West Africa of another cybercriminal but keep the rest of the world safe from Internet fraudsters.

# Are We Bound to See a West African Underground Market?

Although best known for simple types of fraud at present, West African cybercriminals are clearly shifting to more elaborate crimes, complex operations, and business models—BEC and tax fraud, in particular. Armed with their social engineering expertise and ingenuity, and augmented by tools and services (keyloggers, RATs, crypters, counter-AV services, etc.), West African cybercriminals are stealing large amounts of money via crimes targeting individuals and companies worldwide. We believe they will continue down this track and soon become as sophisticated and innovative as cybercriminals in other countries or regions.

West African cybercriminals will eventually start creating online communities, not just small groups of close friends with whom they share technical skills and know-how. Some may start selling products and services that work for their crimes, leading to the formation of a West African underground market. Younger West African cybercriminals and those working toward becoming criminals will continue to be as bold as those from Brazil,<sup>26</sup> flaunting their ill-gotten gains for the world to see.

Cybercrime in West Africa is real. Just because today's attacks are less sophisticated than those we are accustomed to seeing from cybercriminals in other countries or regions, it does not mean they do not have adverse effects. In fact, the simplest attacks enabled by very clever social engineering tactics such as BEC fraud have crippled all types of companies, regardless of size.

A West African underground market is emerging and stronger law enforcement actions are needed to stop the evolution of a sophisticated market. Although an average of 30% of the total number of cybercrimes reported to West African law enforcement agencies each year resulted in arrests, some of the INTERPOL survey respondents cited recurring roadblocks when it came to investigating cybercrime. These include difficulties in obtaining information from overseas and identifying cybercriminals and their physical locations. Possible reasons for these challenges include lack of logistical resources and cybercrime training for local law enforcement agents as well as the lack of cybercrime laws in the country or region concerned.

Recurring Investigation Roadblock	Response Share
Difficulties obtaining information from overseas	100%
Difficulties identifying cybercriminals' physical locations	75%
Difficulties identifying cybercriminals	50%

Table 2: Recurring investigation roadblocks cited by the INTERPOL survey respondents

The INTERPOL Global Complex for Innovation (IGCI) provides a neutral collaborative platform where contextualized threat intelligence can be shared to support law enforcement investigations into cybercrime. Trend Micro has been a long-term supporter and has dedicated resources in building up and continuously improve the IGCI's capabilities. Together, these two organizations, along with other contributors, will continue to support law enforcement agencies in West Africa and other INTERPOL member-countries and exert effort to alleviate the further proliferation of cybercrime.

# References

1. Raimund Genes. (13 December 2012). *TrendLabs Security Intelligence Blog*. “Trend Micro Predictions for 2013 and Beyond: Threats to Business, the Digital Lifestyle, and the Cloud.” Last accessed on 3 November 2016, <http://blog.trendmicro.com/trendlabs-security-intelligence/predictions-for-2013/>.
2. The Conversation. (28 July 2016). *U.S. News*. “Meet the ‘Yahoo Boys’—Nigeria’s Undergraduate Conmen.” Last accessed on 7 November 2016, <http://www.usnews.com/news/best-countries/articles/2016-07-28/meet-the-yahoo-boys-nigerias-undergraduate-conmen>.
3. TrendLabs. (1 April 2016). *Trend Micro Security News*. “The Many Faces of Cybercrime.” Last accessed on 27 January 2017, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-many-faces-of-cybercrime>.
4. Joseph Oduro-Frimpong. (18 January–1 February 2011). *Media Anthropology Network e-Seminar European Association of Social Anthropologists (EASA)*. “Sakawa: On Occultic Rituals and Cyberfraud in Ghanaian Popular Cinema.” Last accessed on 27 January 2017, [http://www.media-anthropology.net/file/frimpong\\_rituals\\_cyberfraud.pdf](http://www.media-anthropology.net/file/frimpong_rituals_cyberfraud.pdf).
5. Ghanaian Times. (25 March 2015). *Modern Ghana*. “Sakawa Boys Threaten to Teach Minister ‘Bitter Lesson.’” Last accessed on 27 January 2017, <https://www.modernghana.com/sports/607031/1/sakawa-boys-threaten-to-teach-minister-bitter-less.html>.
6. Vice Staff. (6 April 2011). *Vice*. “The Sakawa Boys.” Last accessed on 27 January 2017, [https://www.vice.com/en\\_us/article/mbd-vbs-the-sakawa-boys](https://www.vice.com/en_us/article/mbd-vbs-the-sakawa-boys).
7. Sammy Darko. (10 May 2015). *BBC News*. “Inside the World of Ghana’s Internet Fraudsters.” Last accessed on 2 November 2016, <http://www.bbc.com/news/world-africa-32583161>.
8. African Center for Economic Transformation (ACET). (1 April 2016). *ACET*. “Unemployment in Africa: No Jobs for 50% of Graduates.” Last accessed on 2 November 2016, <http://acetforafrica.org/highlights/unemployment-in-africa-no-jobs-for-50-of-graduates/>.
9. Cedric Pernet. (14 September 2016). *Trend Micro Security News*. “The French Underground: Under a Shroud of Extreme Caution.” Last accessed on 27 January 2017, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-french-underground-under-a-shroud-of-extreme-caution>.
10. Sean Jacobs. (2 May 2011). *Africa Is a Country*. “The Representation of Ghana.” Last accessed on 27 January 2017, <http://africasacountry.com/2011/05/the-sakawa-boys/>.
11. Dominic Moses Awiah. (4 May 2015). *Graphic Online*. “The Confession of Three Sakawa Boys; We Want to Stop but...” Last accessed on 27 January 2017, <http://www.graphic.com.gh/features/opinion/the-confession-of-three-sakawa-boys-we-want-to-stop-but.html>.
12. Macky Cruz. (4 February 2008). *TrendLabs Security Intelligence Blog*. “419 Scammers Admit to Mail Fraud.” Last accessed on 2 November 2016, <http://blog.trendmicro.com/trendlabs-security-intelligence/419-scammers-admit-to-mail-fraud/>.
13. Liz Phillips. (13 November 2013). *The Guardian*. “How I Got Caught Up in a ‘Stranded Traveler’ Phishing Scam.” Last accessed on 2 November 2016, <https://www.theguardian.com/money/2013/nov/13/stranded-traveller-phishing-scam>.
14. TrendLabs. (12 February 2016). *Trend Micro Security News*. “Tainted Love: Online Scams Cashing in on Romance.” Last accessed on 2 November 2016, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/tainted-love-online-scams-cashing-in-on-romance>.
15. Max Goncharov. (28 July 2015). *Trend Micro Security News*. “The Russian Underground Today: Automated Infrastructure, Sophisticated Tools.” Last accessed on 27 January 2017, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/russian-underground-automized-infrastructure-services-sophisticated-tools>.



16. TrendLabs. (11 January 2016). *Trend Micro Security News*. "Security 101: Business Email Compromise (BEC) Schemes." Last accessed on 2 November 2016, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/business-email-compromise-bec-schemes>.
17. Vicki D. Anderson. (29 March 2016). *FBI Cleveland*. "FBI Warns of Rise in Schemes Targeting Businesses and Online Fraud of Financial Officers and Individuals." Last accessed on 2 November 2016, <https://www.fbi.gov/contact-us/field-offices/cleveland/news/press-releases/fbi-warns-of-rise-in-schemes-targeting-businesses-and-online-fraud-of-financial-officers-and-individuals>.
18. FBI. (14 June 2016). *FBI*. "Business Email Compromise: The 3.1 Billion Dollar Scam." Last accessed on 27 February 2017, <https://www.ic3.gov/media/2016/160614.aspx>.
19. Loucif Kharouni. (15 April 2015). *TrendLabs Security Intelligence Blog*. "Behind Tax Fraud: A Profile of 3 IRS Scammers." Last accessed on 2 November 2016, <http://blog.trendmicro.com/trendlabs-security-intelligence/behind-tax-fraud-a-profile-of-3-irs-scammers/>.
20. Lion Gu. (23 November 2015). *Trend Micro Security News*. "Prototype Nation: The Chinese Cybercriminal Underground in 2015." Last accessed on 2 November 2016, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/prototype-nation-the-chinese-cybercriminal-underground-in-2015>.
21. Ryan Flores, Akira Urano, Noriaki Hayashi, Lion Gu, Lord Alfred Remorin, Ju Zhu, Philippe Lin, and Joey Costoya. (2015). *Trend Micro Security News*. "Sextortion in the Far East." Last accessed on 2 November 2016, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/sextortion-in-the-far-east-blackmail-goes-mobile>.
22. Loucif Kharouni. (2013). *Trend Micro Security Intelligence*. "'Ice 419': Cybercriminals from Nigeria Use Ice IX and the 419 Scam." Last accessed on 10 October 2016, <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-ice-419.pdf>.
23. Trend Micro Senior Threat Researchers. (1 August 2016). *TrendLabs Security Intelligence Blog*. "INTERPOL Arrests Business Email Compromise Scam Mastermind." Last accessed on 2 November 2016, <http://blog.trendmicro.com/trendlabs-security-intelligence/interpol-arrests-business-email-compromise-scam-mastermind/>.
24. Bakuei Matsukawa, David Sancho, Lord Alfred Remorin, Robert McArdle, and Ryan Flores. (2014). *Trend Micro Security News*. "Predator Pain and Limitless: When Cybercrime Turns into Cyberspying." Last accessed on 2 November 2016, <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cybercrime-to-cyberspying-limitless-keylogger-and-predator-pain>.
25. TrendLabs. (2016). *Trend Micro Security News*. "Deep Web Threat Intelligence Center." Last accessed on 2 November 2016, <http://www.trendmicro.com/vinfo/us/security/threat-intelligence-center/deep-web/>.
26. Trend Micro Forward-Looking Threat Research (FTR) Team. (12 January 2016). *Trend Micro Security News*. "Ascending the Ranks: The Brazilian Cybercriminal Underground in 2015." Last accessed on 30 January 2017, <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/brazilian-cybercriminal-underground-2015>.

Created by:

**TrendLabs**

The Global Technical Support and R&D Center of TREND MICRO

**TREND MICRO™**

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit [www.trendmicro.com](http://www.trendmicro.com).



Securing Your Journey  
to the Cloud

[www.trendmicro.com](http://www.trendmicro.com)

**INTERPOL**

INTERPOL's role is to enable police in its 190 member countries to work together to make the world a safer place. INTERPOL provides a range of capabilities to help them meet the growing challenges of fighting today's crimes, including databases of police information on criminals and crime, operational support, forensics and analysis services, and training. These services are delivered worldwide and support three global programmes: Counter-terrorism, Cybercrime, and Organized and emerging crime.



**INTERPOL**

[www.interpol.int](http://www.interpol.int)