
# INTELLIGENCE REPORT:

## CSIR - 18004

## NIGERIAN CONFRATERNITIES EMERGE AS BUSINESS EMAIL COMPROMISE THREAT

PUBLISHED 20 MARCH 2018

**CROWDSTRIKE GLOBAL INTELLIGENCE TEAM**

web: WWW.CROWDSTRIKE.COM | twitter: @CROWDSTRIKE

email: INTELLIGENCE@CROWDSTRIKE.COM

# TABLE OF CONTENTS

# **Executive** Summary

CSIR-18004

# EXECUTIVE SUMMARY

Business email compromise (BEC) is a form of fraud by which a team of cybercriminals convince victims to wire large amounts of funds or send valuable data to criminally controlled accounts; it is facilitated by the victim's belief that they are actually being asked or instructed to do so by a trusted party. According to the Internet Crime Complaint Center (IC3), BEC occurs when "a criminal compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds".

In 2016, the IC3 received 12,005 BEC complaints amounting to losses of more than $360 million USD. There have been multiple open-source reports describing how money stolen through BEC fraud is directed to bank accounts in China, particularly Hong Kong. The IC3 has tracked fraudulent bank transfers to 72 countries and it has determined that the majority go to banks in China and Hong Kong.

As eCrime has evolved over the past decade and become a global issue costing companies and individuals billions of dollars, prolific Nigerian cybercriminals have evolved, too. They have moved to BEC scams, which are much more sophisticated than advanced-fee fraud (also called 419 fraud). Industry reporting shows that BEC has been perpetrated by Nigerian groups or individuals and that the tools are readily available.[1] Additional analysis by CrowdStrike Intelligence shows that larger and more sinister Nigerian criminal groups are involved in BEC, specifically Nigerian Confraternities.

The Neo Black Movement (NBM) was founded in 1977 at the University of Benin, Nigeria. NBM claims that it is an officially registered organization in Nigeria, however it is widely considered to be one and the same as the Black Axe confraternity, and both have been banned by law. Since its foundation, Black Axe has developed into a formidable criminal organization and has developed a hierarchical, inter-state organization while at the same time retaining cult-like tendencies.

Black Axe gangs are involved in a multitude of organized crime ventures such as running prostitution rings, human trafficking, narcotics trafficking, grand theft, money laundering, and email fraud/cybercrime. These activities primarily take place in Nigeria, and they also are conducted by Black Axe members (known as Axemen) in Europe and North America.

Black Axe maintains a hierarchical command structure at the national level, and it also operates Black Axe "Zones" (also pyramidal in structure) in foreign locations. Arrests of criminals in Canada in 2015 revealed that the Black Axe zone for Canada is heavily involved in wire fraud, money laundering, romance scams, and BEC.

U.S. law enforcement arrested several Nigerian criminals on BEC fraud over the past few years, and Canadian and Italian law enforcement agencies have had limited success confronting and dealing with the Black Axe zones in their respective countries. Yet the magnitude of this criminal threat has only recently begun to be understood. As such, the threat posed by Black Axe and similar groups will remain high for the foreseeable future, and BEC will remain an effective eCrime technique in the near to mid-term.

[1] Trend Micro, "Cybercrime in West Africa", 2017, https://documents.trendmicro[.]com/assets/wp/wp-cybercrime-in-west-africa.pdf

# KEY POINTS

- Business email compromise (BEC) is a form of fraud where criminals compromise legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.
- Over the past 12 months, CrowdStrike has observed three different types of BEC scams: wire transfer attempts, payroll fraud, and compromises that have led to follow-on spam campaigns. In many BEC cases, CrowdStrike has observed Office 365 (or Google suites) being compromised because two-factor authentication (2FA) was not enabled.
- CrowdStrike has also observed eCrime campaigns using the *Netwire* remote access tool (RAT) that are tied to Nigerian BEC fraud and that have affected companies in the energy, travel, financial, and hospitality sectors.
- In many cases, money stolen through BEC fraud is directed to bank accounts in China, particularly Hong Kong.
- Nigerian confraternities, most notably Black Axe, have developed into formidable criminal organizations that include cyber components.
- The Black Axe confraternity maintains a pyramidal command structure at the national level, and also operates Black Axe "Zones" that conduct wire fraud in foreign locations.
- In mid-2015, police in Toronto, Canada arrested three Nigerian criminals on fraud charges for stealing more than $600,000 USD from a Canadian widow through a romance scam. Police also charged one with the crime "money laundering for criminal organization" because they identified him as the bookkeeper for Black Axe's Canada zone.
- Although the perpetration of Nigerian 419 scams is not as advanced technically as the activity conducted by Russian actors who develop and manage sophistication banking Trojans, Nigerian BEC scams are just as advanced given their global scale, the amount of money involved, and the advanced money laundering techniques that include the use of banks in China.
- As such, the threat posed by Black Axe and similar groups will remain high for the foreseeable future, and BEC will remain an effective eCrime technique in the near to mid-term.

## Introduction

While fraud and identity theft have existed for a long time, BEC is pertinent to the field of eCrime because of its reliance on email and related factors, such as account hijacking via phishing, impersonation, and others. BEC incidents normally rely on social engineering techniques, such as knowledge of the targeted person or organization, exploitation of business hierarchies or dynamics, and multimedia interactions (such as following up on an email with a telephone call). In some BEC campaigns, malware may be used to gain initial access to a target environment and conduct research.

BEC is considered by U.S. law enforcement authorities—particularly the Federal Bureau of Investigation (FBI)—as one of the main eCrime vectors when measured by total amount of stolen funds. IC3 has determined there are five main scenarios for BEC scams:

| IC3 BUSINESS EMAIL COMPROMISE SCENARIOS[2] | |
|---|---|
| **Scenario 1** | Business working with a foreign supplier |
| **Scenario 2** | Business [executive] receiving or initiating a request for a wire transfer |
| **Scenario 3** | Business contacts receiving fraudulent correspondence through compromised email |
| **Scenario 4** | Business executive and attorney impersonation |
| **Scenario 5** | Data theft |

Table 1. BEC Scenarios

### BEC Orchestration

Although there are many different scenarios and variations to BEC operations, the basic structure of the scam is relatively consistent. Criminal actors typically follow these steps when conducting BEC fraud:

## Operational Kill Chain

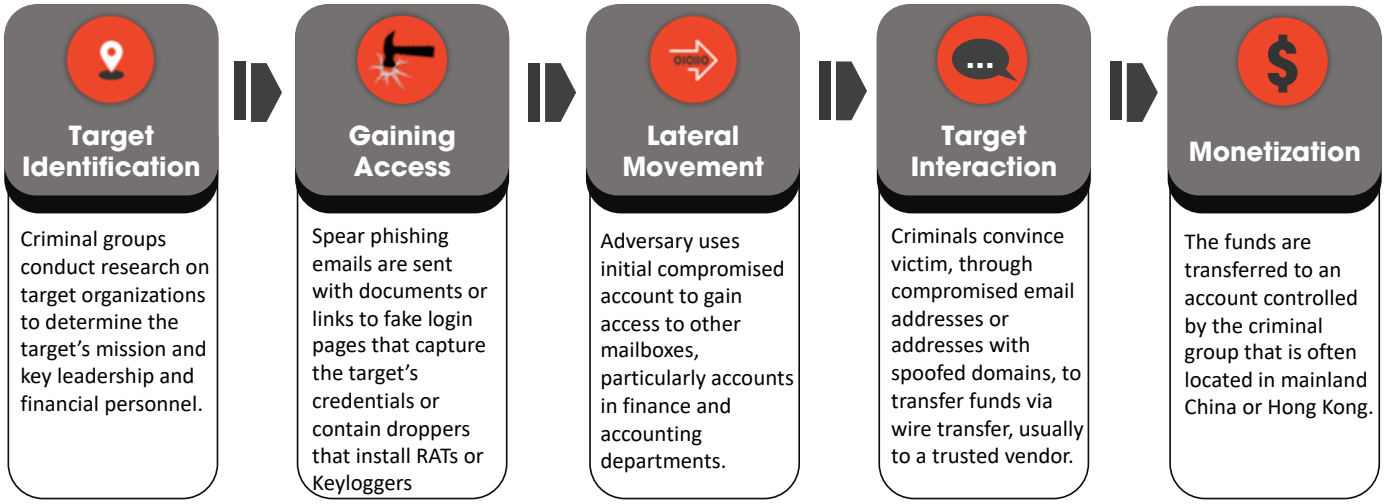



Figure 1. Structure of BEC Fraud

### Chinese Bank Accounts Used for Transfers

There have been multiple open-source reports describing how money stolen through BEC fraud is directed to bank accounts in China, particularly Hong Kong. The IC3 has tracked fraudulent bank transfers to 72 countries and has determined that the majority go to banks in China and Hong Kong. These reports coincide with BEC incidents that the CrowdStrike Services team observed in 2017 where frequent fraudulent wire transfers to financial institutions in Hong Kong took place.

African criminals often travel to mainland China and Hong Kong to open bank accounts or hire local agents to open accounts. One recent arrest of a Nigerian criminal, David ADINDU, shows that his

[2] FBI IC3, "Business E-Mail Compromise: The 3.1 Billion Dollar Scam", 14 June 2016, Bhttps://www.ic3[.]gov/media/2016/160614.aspx

primary task was to set up bank accounts in mainland China and Hong Kong, and that from 2014 to 2016 he lived in both Lagos, Nigeria and Guangzhou, China.

According to one open-source report in November 2017, operators from unlicensed, mainland China banks traveled to Hong Kong to open bank accounts to be used as intermediate collection points for money stolen from BEC operations.[3] The money was then transferred electronically to banks around the world on the same day it was deposited. Hong Kong police stated that the operators who opened the accounts were recruited in mainland China and were offered payment. The process of transferring money to accounts in China and then to additional financial institutions makes tracking and recovering the funds much more difficult for investigators and the companies that have been defrauded.

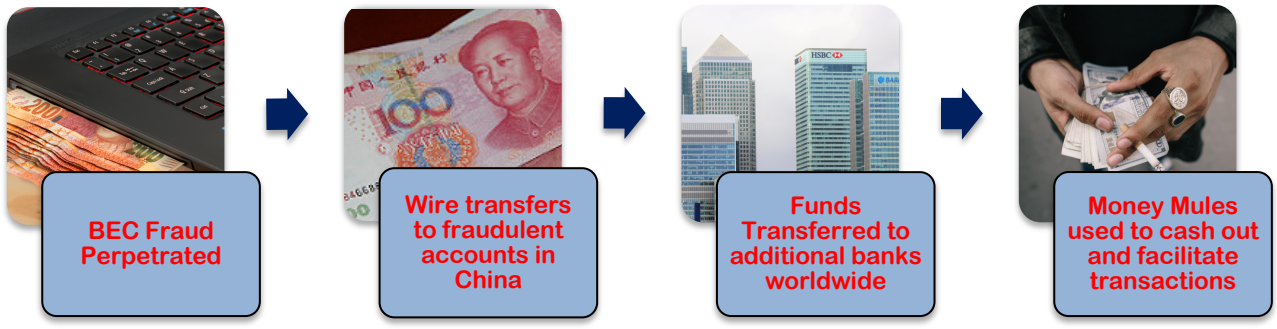



Figure 2. BEC Money Flow

### Role of Romance Scams and Money Mules in BEC

The FBI considers romance scams as a "secondary scheme associated with BEC" because victims of this type of fraud have been used as money mules to cash out or transfer money stolen from BEC.[4] Victims of romance scams tend to be older widowed or divorced persons who become emotionally attached to criminals using an alias that they meet online, often on dating sites.[5] In most romance scams, the victims are enticed to transfer money to their "romeo" to pay for an emergency or similar situation, and in some cases individuals have lost millions of dollars.

Victims of romance scams are also used to facilitate BEC scams. This occurs when victims of romance scams are manipulated to act as money mules for fraudulent money transfers once the money arrives at

[3] South China Morning Post, Clifford Lo, "Millions in laundered cash from email scams filtered through Hong Kong, police say", 28 November 2017, http://www.scmp[.]com/news/hong-kong/law-crime/article/2121985/millions-laundered-cash-email-scams-filtered-through-hong

[4] FBI, "FBI Warns of Rise in Schemes Targeting Businesses and Online Fraud of Financial Officers and Individuals", 29 March 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

[5] FBI, "Romance Scams, Online Imposters Break Hearts and Bank Accounts", 13 February 2017, https://www.fbi[.]gov/news/stories/romance-scams

a bank they can access. The victim then withdraws the funds or transfers them again, taking a portion as payment.

### The Nigerian Connection: A Tradition in eCrime

Nigeria is the most populated country in Africa, and it is a longstanding source of eCrime attacks on targets in generally wealthier countries. While in popular culture the "Nigerian prince" scams are often dismissed for their stylistic crudeness, in reality, Nigerian criminals have been able to steal significant amounts of funds through fraud vectors such as BEC.

There is no information supporting the notion that there is a local malware development scene in Nigeria, as opposed to the reality observed in countries such as Brazil or Russia. Instead, Nigerian criminals have historically tended to either go malware-free (by leveraging spear phishing and social engineering), or to employ free or otherwise widely available (also known as "commodity") malware.

Among the tools known to have been employed by Nigerian criminal actors are keyloggers such as *Predator Pain*, *Hawkeye*, and *Keybase*, and RATs such as *Dark Comet* and *Netwire*. These tools are often used to facilitate BEC fraud at the front end of the scam to gain access and conduct reconnaissance. Keyloggers and RATs are ideal for BEC because they are easy to learn how to use, and because they are capable of harvesting email credentials stored in internet browsers or computer memory.

## Moving from 419 Scams to Business Email Compromise

Younger Nigerian criminals—often called Yahoo Boys—are said to begin their scamming careers while undergraduates at university. There are thousands of undergraduates in Nigeria who participate in online fraud, and it has been estimated that there are approximately five million online scammers in the Lagos region.[6]

Novices typically start off with basic 419 fraud (named after the Nigerian criminal code), also known as advanced-fee fraud, which dates back many years and attempts to lure victims to part with a payment with the promise of a "return' on this investment at a later date. Criminals often contact their victims through emails or SMS messages and provide official-looking documents that complement the scam.

Once confidence is gained, money is requested usually through wire transfers via Western Union or similar services. There are many variations of 419 scams that can utilize employment, taxes, or lottery-related themes. Basic phishing campaigns and romance scams are also popular with younger Nigerian criminals.

As eCrime has evolved over the past decade and become a global issue costing companies and individuals billions of dollars, so have Nigerian cybercriminals; they have moved to BEC scams, which are much more advanced than 419 fraud. Previous industry reporting on Nigerian BEC described a group of criminals, as the "wire wire 1" group, who conducted BEC scams using commodity malware (RATs) and publicly available email services.[7]

---

[6] The Guardian (Nigeria), Samson Ezea, "Prevalence of internet fraud among Nigerian youths", 28 January 2018, https://guardian[.]ng/saturday-magazine/prevalence-of-internet-fraud-among-nigerian-youths/.

[7] Dell Secure Works, "Wire Wire: A West African Cyber Threat", 4 August 2016, https://www.secureworks[.]com/research/wire-wire-a-west-african-cyber-threat.

This group was loosely organized and revolved around an actor who provided knowledge and expertise to the group. Other industry reporting has described BEC campaigns conducted by a singular actor, using the Netwire RAT and Hawkeye keylogger.[8] These reports show that BEC can be perpetrated by groups or an individual, and that the tools are readily available. Additional analysis shows that larger and more sinister Nigerian criminal groups are involved in BEC: Nigerian confraternities.

### Nigerian Confraternities

The first confraternity in Nigeria was the Pyrates confraternity founded at the University of Ibadan, Nigeria in 1952. This confraternity transformed eventually into a secret cult and led to the establishment of splinter confraternities such as Eiye/ Airlords, Black Axe, Sealords, Supreme Vikings, and Mafia Con-fraternity, which followed in the 1970s and 1980s.[9] These con-fraternities revolve around Nigerian universities, where new members are recruited and are often referred to as secret cults. It is estimated that there are approximately 44 secret cults active in Nigeria, with some universities having up to 16 cults on their campuses.[10]


Figure 3. Pyrates Confraternity Logo

Although the original aims of the Pyrates were altruistic, the confraternities that followed and exist today are characterized by extreme violence, cultism, and rampant organized crime. Despite being illegal, these cults have thrived and even expanded overseas to locations in Europe and North America, and they are funded by drug and human trafficking, as well as highly organized and very lucrative cybercrime operations.

## Black Axe Confraternity/Neo Black Movement

The Neo Black Movement (NBM) was founded in 1977 at the University of Benin. NBM claims that it is an officially registered organization in Nigeria, however it is widely considered one and the same as the Black Axe confraternity, and both have been banned by law.[11] NBM maintain that they do not have connections to Black Axe, however is essentially just a different name that acts as a nominal cover for the Black Axe confraternity.

Since its foundation, Black Axe has developed into a formidable criminal organization, and it has developed a hierarchical, inter-state organization while at the same time retaining cult-like tendencies. It is frequently involved in violent, often deadly clashes with other cults, and torture and rape are often

[8] Checkpoint, "Get Rich or Die Trying: A Case Study on the Real Identity behind a Wave of Cyber Attacks on Energy, Mining and Infrastructure Companies", 15 August 2018.

[9] Adewale Rotimi, Nordic Journal of African Studies, "Violence in the Citadel: The Menace of Secret Cults in the Nigerian Universities", 2005, http://www.njas.helsinki[.]fi/pdf-files/vol14num1/rotimi.pdf

[10] Global Sentinel, "Cultism: Top 7 Confraternities in Nigeria and Their History, Beliefs", 5 October 2017, https://globalsentinelng[.]com/2017/10/05/cultism-top-7-confraternities-nigeria-history-beliefs/

[11] Immigration and Refugee Board of Canada, "Nigeria: The Black Axe confraternity, also known as the Neo-Black Movement of Africa, including their rituals, oaths of secrecy, and use of symbols or particular signs; whether they use force to recruit individuals (2009-November 2012)", 3 December 2012, http://www.refworld[.]org/docid/50ebf7a82.html

involved in initiations. There are also reports that Black Axe/NBM has infiltrated the political system in Nigeria in order to influence elections and ensure protection from adverse law enforcement action.[12]

### Organized for eCrime

Black Axe gangs are involved in a multitude of organized crime ventures such as running prostitution rings, human trafficking, narcotics trafficking, grand theft, money laundering, and email fraud/cybercrime. These activities take place in Nigeria, and also are conducted by Black Axe members (a.k.a. Axemen) in Europe and North America. Black Axe maintains pyramidal command structure at the national level, and also operates Black Axe "Zones" (also pyramidal in structure) in foreign locations. These zones typically have a commander or crime boss referred to as an "Oga".

In terms of eCrime, the Oga directs the scams and provides direction to his team. These teams are composed of spammers, catchers, and freelancers.[13] Spammers acquire email lists and operate advanced mail systems. The catchers monitor the responses to the spam campaigns and make first contact with victims (known as a "magas") in order to advance the scam. Freelancers perform additional duties such as assisting with romance scams, acquiring and developing infrastructure, and creating fake documents.

According to open sources, this hierarchy is used by the Black Axe Manchester (UK) zone to conduct numerous types of emails scams. The zone Oga runs a team of scammers that conduct numerous variations of advanced-fee fraud, and he has even set up fraudulent front companies to assist in these operations.[14]

[12] *Ibid*.

[13] bemigho147watch, "Manchester Mafia", 13 February 2015, https://bemigho147watch.wordpress[.]com/2015/02/13/manchester-mafia/

[14] *Ibid*.

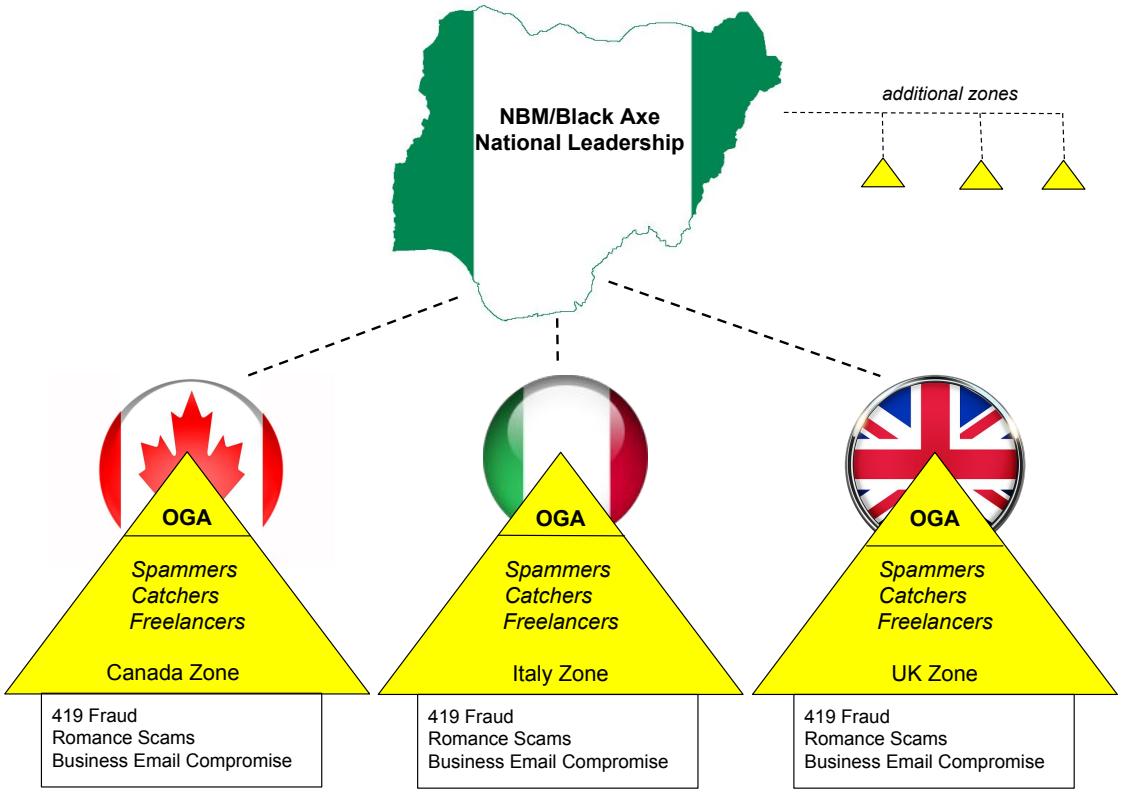



Figure 4. Black Axe Zonal Organization

### Use of Facebook

Black Axe members trade information and ideas on closed Facebook groups; these exchanges include information about phishing, VPN/proxy services, carding, and other eCrime-related topics.[15] Axemen typically do not use their true names in the Facebook groups, employing a rudimentary and basic level of security; however, these accounts often contain information that can be used to garner further information.

The use of Facebook allows Axemen to communicate with members across geographic regions. At this time, CrowdStrike Intelligence cannot confirm that this platform is used to conduct detailed planning for BEC operations, and it is likely more secure and direct forms of communication would be used for these purposes.

[15] Bemuda, "Killing & Scamming: The Neo Black Movement of Africa aka Black Axe Cult", 24 January 2015, https://bemuda.wordpress[.]com/2015/01/24/killing-scamming-the-neo-black-movement-of-africa-aka-black-axe-cult/.


Figure 5. Black Axe Closed Facebook Group

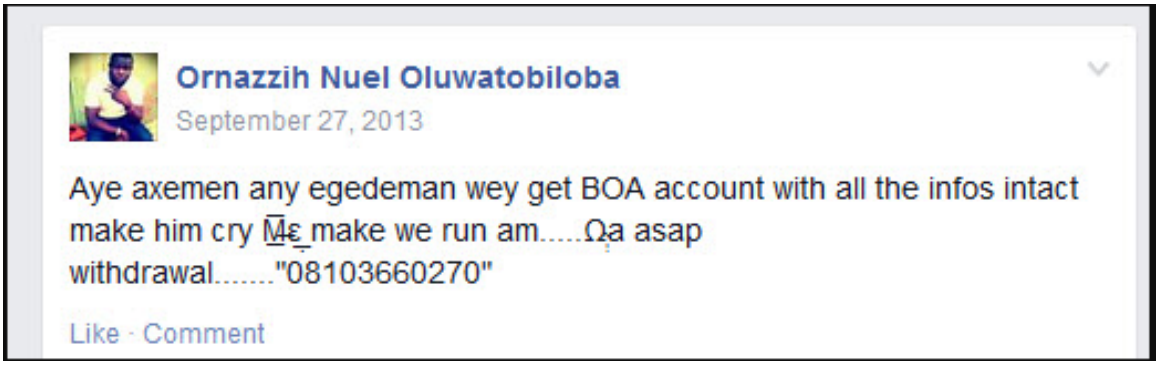



Figure 6. Axeman Posting About Carding Operations[16]

### Black Axe Toronto Zone Member Arrested for eCrime Fraud

Black Axemen do employ a modicum of security online, and they enjoy a certain level of autonomy within Nigeria; as such, prosecuting members of this group poses challenges to law enforcement. However, police in Canada have arrested Black Axe members for conducting romance scams and wire fraud, to include BEC.

In mid-2015, police in Toronto, Canada arrested Akohomen IGHEDOISE, Ikechukwu AMADI, and Lineo MOLEFE on fraud charges for stealing more than $600,000 USD from a Canadian widow through a romance scam that was conducted through the dating site *match[.]com*. Police also charged IGHEDOISE with the crime "money laundering for criminal organization" because they identified him as the bookkeeper for Black Axe's Canada zone.[17]

[16] Bemuda, "Killing & Scamming: The Neo Black Movement of Africa aka Black Axe Cult", 24 January 2015, https://bemuda.wordpress[.]com/2015/01/24/killing-scamming-the-neo-black-movement-of-africa-aka-black-axe-cult/.

[17] Vice News, Tamara Khandaker, "The Notorious Black Axe Has Put Down Roots in Canada", 17 December 2015, https://news.vice[.]com/article/the-notorious-black-axe-has-put-down-roots-in-canada

In addition to this scam, several people in Toronto were defrauded of $1 million USD each through similar scams. That stolen money was wired by Canadians linked to Black Axe (and in some cases, it was delivered directly to Black Axe members.[18]

AMADI and IGHEDOISE were also indicted by the FBI (along with three additional defendants) for conducting wire fraud costing more than $10 million USD. The three additional defendants were U.S. citizens who worked directly with AMADI and IGHEDOISE on a variety of schemes that targeted law firms, ultimately convincing these targets to wire money to accounts that they controlled.

This conspiracy "also employed hackers who compromised both individual and corporate email accounts, ordering wire transfers from brokerage and business accounts to shell accounts controlled by conspirators."[19] Based on these charges, it is evident that this criminal scheme involved BEC fraud in addition to romance scams. All three U.S. defendants were found guilty of these crimes, while AMADI and IGHEDOISE have not appeared in the U.S., as they remain in police custody in Canada.

### Recent Arrests of Nigerian BEC Threat Actors

Apprehending criminals for BEC fraud can be difficult due to the nature of crime on the internet and geographic issues. Despite these difficulties, in 2017, U.S. law enforcement agencies arrested and sentenced numerous Nigerian criminals for perpetrating BEC fraud. BEC fraudsters, once identified, have been arrested attempting to enter the U.S., or when residing in the U.S., often as Visa overstays.

#### Daniel Adekunle OJO

In August 2017, the FBI arrested Daniel Adekunle OJO for conducting BEC scams that allowed him to collect the tax records of thousands of local school employees. OJO, a Nigerian living in the U.S. on an expired visa, was charged with fraud and identity theft for sending phishing emails requesting W-2 tax information to school officials in Connecticut and Minnesota.

OJO impersonated another school district employee and sent phishing emails from AOL and Gmail accounts to school district employees requesting W-2 records, and in at least one instance got a response that allowed him to file 122 fraudulent tax returns. Government officials have stated that the IRS processed an undisclosed amount of the fraudulent returns and deposited approximately $37,000 USD in bank accounts controlled by OJO.[20]

[18] The Globe and Mail, Selena Ross, "Shadowy Black Axe group leaves trail of tattered lives", 12 November 2015, https://www.theglobeandmail[.]com/news/national/shadowy-black-axe-group-leaves-trail-of-tattered-lives/article27244946/

[19] Department of Justice, "Texas Attorney Sentenced To 25 Years In Prison For International Money Laundering Conspiracy," 16 October 2017, https://www.justice[.]gov/usao-mdfl/pr/texas-attorney-sentenced-25-years-prison-international-money-laundering-conspiracy

[20] VOA, "Nigerian Man Charged in US Phishing Scam", 4 August 2017, https://www.voanews[.]com/a/nigeria-us-phishing-scam/3973069.html

### Amechi Colvis AMUEGBUNAM

Amechi Colvis AMUEGBUNAM (a.k.a. Colvis Amue), from Lagos Nigeria, was arrested in 2015 and was sentenced to 46 months in prison in September 2017 for conducting BEC scams that dated back to 2013. AMUEGBUANAM was charged with attempting to steal approximately $3.7 million USD from 10 victims. According to the FBI, the threat actor sent spear-phishing emails that appeared to come from C-suite level executives to employees in the accounting departments of various companies. The emails instructed the recipients to make financial transfers to fraudulent accounts. Investigators connected this activity to AMUEGBUNAM through the PDFs used in the schemes.[21]

Figure 7. AMUEGBUNAM

In mid-August 2014, CrowdStrike Intelligence tied this actor to financial fraud activity using a wire transfer scheme initiated by a spear-phishing email directly targeting a semiconductor manufacturer. In this instance, a Portable Document Format (PDF) file was transmitted to the finance department of a semiconductor manufacturer. The attack targeted the company directly, as this PDF arrived from an email address spoofing a senior official within the organization, using an email address that innocuously added an additional character to the domain of the targeted organization (the domain was registered the day the email was sent to the victim). This PDF provided wiring instructions—in this case, to a bank in Shanghai, China. For more information on this campaign, see CSIT-14098.

### Obinna Kelvin OBIOHA

Figure 8. OBIOHA

Obinna Kelvin OBIOHA was arrested in October 2016 while attempting to enter the U.S., and was sentenced in August 2017 to serve 51 months in prison for conducting wire fraud while in Nigeria. The U.S. government described him as a central figure in Nigerian criminal group that conducted advanced fraud schemes. In 2016, OBIOHA conducted at least 50 fraudulent wire transfers, which resulted in $6.5 million USD being transferred to accounts under his control.

This criminal group was able to monitor victims and identify opportunities to redirect commercial transactions through a common BEC technique of creating email addresses that were almost identical to legitimate addresses. They then sent emails to victims enticing them to proceed with the transaction under their pretense.[22] According to his LinkedIn profile, OBIOHA has a Bachelor of Applied Science degree in statistics as well as Russian language skills.

---

[21] Justice Department, "Nigerian Man Sentenced for Role in "Business Email Compromise" Scheme That Caused $3.7 Million Loss to U.S. Companies", 28 August 2017, https://www.justice[.]gov/usao-ndtx/pr/nigerian-man-sentenced-role-business-email-compromise-scheme-caused-37-million-loss-us

[22] Department of Justice, "Nigerian Man Sentenced to Prison for Hacking and Fraud Scheme", 16 August 2017, https://www.justice[.]gov/usao-ndny/pr/nigerian-man-sentenced-prison-hacking-and-fraud-scheme

### David Chukwuneke ADINDU

In December 2017, David Chukwuneke ADINDU was sentenced to three years in prison for committing BEC wire fraud that convinced thousands of victims to wire approximately $25 million USD to bank accounts that he created in China. One of ADINDU's primary functions in this scam was to set up these accounts in mainland China and Hong Kong. He lived in both Lagos, Nigeria and Guangzhou, China[23] from 2014 to 2016.

## BEC Campaigns Observed by CrowdStrike in 2017

Over the past 12 months, CrowdStrike has typically observed two different types of BEC scams: wire transfer attempts and compromises that have led to follow-on spam campaigns. Regarding fraudulent wire transfers, the criminals typically get caught on the initial attempt, or they get caught on the second attempt, which usually involves a much larger amount than the first attempt. The wire transfer scams that have been observed follow similar patterns in some cases, even though the companies and personnel targeted have varied.

In many BEC cases, CrowdStrike has observed Office 365 (or Google suites) being compromised because 2FA was not enabled. When this happens, the attackers can take over the entire approval chain for Office 365, and then add rules in order to monitor email traffic and intercept messages of employees who may be trying to report suspicious activity.

In general, the majority of these attacks are coming from Nigerian IP addresses, the mailboxes are going to Nigerian IPs, and they are just now starting to use proxies. Although there is not one set of standard tactics for BEC, CrowdStrike, in 2017, has observed numerous BEC campaigns that use tactics mirroring these:

1. A spear-phishing email, often containing a PDF attachment or a link, is sent to a pre-determined individual in the target company. Emails sent to victims seem to be relatively targeted, but generally very simple. They usually contain links to fake DocuSign or One Drive login pages, sometimes hidden behind URL shortening services.
2. Once the PDF is opened in the browser, the link contained in the PDF is visited by the browser. Otherwise, links contained in the emails lead to a phishing site often containing the email address of the targeted account. The email address form field can then be pre-populated with this value.
3. In certain cases, after the initial link is visited, a redirect occurs that lands on DocuSign pages with the option to log into legitimate mail providers such as Office 365. Phishing pages are hosted on what appear to be hacked web servers. They contain login forms for victims to enter their email and password.
4. Browsers are then redirected to legitimate web pages for logging into email services, where user credentials are then stolen. The backend code that collects entered credentials is written in PHP. It forwards the entered data per email to an attacker-controlled email account.

[23] Reuters, "Nigerian man pleads guilty to taking part in global email scams", 14 December 2017, https://www.reuters[.]com/article/us-cyber-fraud/nigerian-man-pleads-guilty-to-taking-part-in-global-email-scams-idUSKBN1E838W

5. The stolen credentials are then used by criminals to access the victim's mailbox from a remote IP address, in some cases the same IP address used in the initial spear phish.
6. The compromised account is then used to gain access to additional mailboxes including accounts typically in the finance and accounting departments. Search queries are then completed for terms such as wire transfer, invoice, payment, CEO, or bank.
7. An email sent from one of the compromised email addresses is then sent to the company's financial institution requesting a wire transfer, in some cases as high as $1M USD.
8. Additional emails from hacked accounts are also sent to the financial institution approving the transaction.
9. Once the payment details are intercepted by the criminals, the account number (or IBAN), name of bank, and SWIFT/BIC codes are changed to a criminally controlled account, typically in Hong Kong or China.

## Case Study: Targeting Supporting Services

In late 2017, a BEC campaign was perpetrated against a firm in the services sector; it involved slightly modified and more sophisticated tactics than those listed above. In this instance, the target company was not compromised, but rather the Office 365 environment of the company's accounting firm was compromised through targeted spear-phishing emails. Reconnaissance was conducted, and information was collected that informed the adversary on target's banking practices.

Simultaneously, the adversary created a spoofed domain that was one letter off from the target firm's true domain. They then started sending instructions with replicated, authentic-looking email headers and footers from the spoofed domain to the accounting firm. Victims were thereby instructed to conduct wire transfers using the target firm's bank. In the course of one week, the criminals were able to induce multiple transactions to bank accounts in China, totaling in the seven figures. Nigerian IP addresses (located in the *Network Indicators* section) were used to access the Office 365 environment and conduct correspondence with the accounting firm.

### Connection to Netwire RAT Campaigns

As mentioned earlier, Nigerian criminals can use keyloggers and RATs as part of their BEC campaigns. Examining the IP addresses from the above BEC case study reveals that there are connections to Nigerian eCrime campaigns using the Netwire RAT that occurred at the same time frame.

Netwire is a full-fledged RAT that is sold in the open community by World Wired Labs and marketed as a legitimate application. Copies of the RAT have been circulating in the criminal underground alongside custom packers and obfuscators to enable both targeted and criminal attacks via spear-phishing campaigns. (For more information on the Netwire RAT, see CSIT-16007).

The anatomy of a typical Netwire attack is the use of a spear-phishing email to deliver a malicious Microsoft Word document that uses an obfuscated macro to obtain the main Netwire payload. The Netwire RAT has a range of highly configurable capabilities including victim file system management, screen capture, keystroke logging, process management, credential stealing, and configuration of the victim as a proxy server. These capabilities make Netwire—and other similar tools—good for supporting BEC campaigns, or for stealing information to be sold to other criminals.

Four of the IP addresses observed in the above BEC case (41.190.2[.]151, 41.190.2[.]249, 41.190.3[.]14, and 41.190.3[.]49) hosted the domains `enitan1759.linkpc[.]net` and/or `entitan.linkpc[.]net` in December 2017. CrowdStrike Intelligence has observed `enitan1759.linkpc[.]net` being used as a Netwire C2 domain in multiple campaigns dating back to mid-2017, and observed `enitan.linkpc[.]net` as far back as 2016 (CSIT-16007).

In previous examples, the Netwire payload was embedded in a Delphi executable that was decoded from a Visual Basic (VB) script. It is currently not clear whether these lures and scripts are from a single group, but there are several overlaps:

- VB script obfuscation technique
- VB script name themes
- Obfuscation techniques in the packed Delphi executable
- Netwire RAT payload (in a few cases the payload is another RAT such as *Quasar* or *NanoCore*)
- C2 overlap

There is an association to Nigeria in these cases, and the main link from these cases to this .NET-malware case is the Netwire RAT with a C2 of `enitan1759.linkpc[.]net`.

CrowdStrike has observed these campaigns affect companies in the energy, travel, financial, and hospitality sectors. These campaigns are started with spear-phishing emails that contain Word document attachments that act as droppers for Netwire, and in some cases for Quasar or NanoCore.

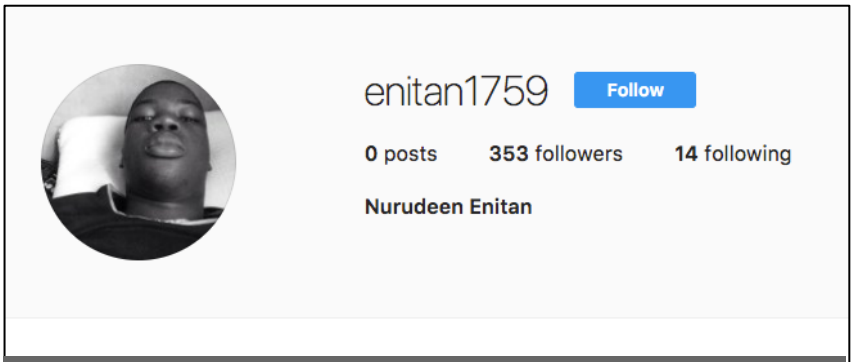
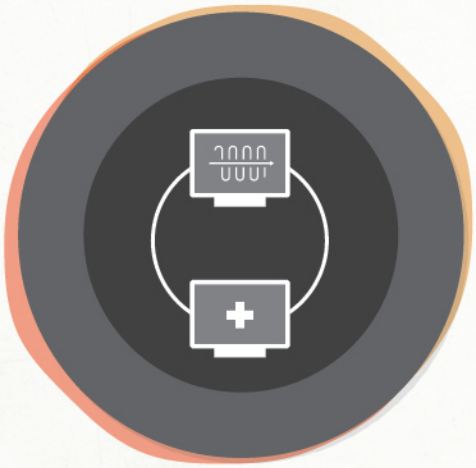


Figure 9. Nurudeen Enitan on Instagram

Conducting research on the string "entitan1759" reveals accounts on Twitter and Instagram with the handle @enitan1759, using the names *Jake* and *Nurudeen Enitan*, respectively. The name *Nurudeen Enitan* can be observed in the metadata of a malicious dropper document (SHA256 hash: `4f8c9d6be8157031ef79478b9906eaf4ae95cd139f7308d2c8d6ccbb8a8bb4df`) that downloads a Netwire sample (SHA256 hash: `ab92de709eb73fa9e5b15608175d4355f6ed56fce9c8291138e3dd2265687bd0`) with the C2 `yachtingconcept.hopto[.]org`. Netwire is often used in conjunction with BEC fraud, and email lures were related to air and sea transportation.



# Mitigation & Remediation

CSIR-18004

# MITIGATION AND REMEDIATION

## INDICATORS OF ATTACK

### Host Indicators

The tables below detail files belonging to the Netwire campaigns including filename, SHA256 hash, and build time when known.

#### Executables

| FILENAME | SHA256 HASH | BUILD TIME (UTC) |
|---|---|---|
| puttyx86.exe | ab92de709eb73fa9e5b15608175d4355 f6ed56fce9c8291138e3dd2265687bd0 | 2014-10-31 03:28:47 |

#### Related Files

| FILENAME | SHA256 HASH |
|---|---|
| 1701251826.doc | 4f8c9d6be8157031ef79478b9906eaf4 ae95cd139f7308d2c8d6ccbb8a8bb4df |

## NETWORK INDICATORS

### Network Artifacts

Below is a list of IP addresses used to conduct BEC fraud as described in this report.

#### IP addresses used to conduct correspondence with targets:

- 197.210.226[.]132 In network 197.210.226.0/24 (ASN 29465 - VCG-AS, NG) Emure-Ekiti, Nigeria
- 197.210.226[.]215 In network 197.210.226.0/24 (ASN 29465 - VCG-AS, NG) Emure-Ekiti, Nigeria
- 197.210.226[.]97 In network 197.210.226.0/24 (ASN 29465 - VCG-AS, NG) Emure-Ekiti, Nigeria
- 197.210.227[.]48 In network 197.210.227.0/24 (ASN 29465 - VCG-AS, NG) Oke Ila, Nigeria
- 197.210.227[.]59 In network 197.210.227.0/24 (ASN 29465 - VCG-AS, NG) Oke Ila, Nigeria
- 197.210.227[.]78 In network 197.210.227.0/24 (ASN 29465 - VCG-AS, NG) Oke Ila, Nigeria
- 197.210.45[.]192 In network 197.210.0.0/16 (ASN 29465 - VCG-AS, NG), Lagos Nigeria

**IP addresses used to access Office 365 accounts:**

- 105.112.28[.]9 In network 105.112.28.0/24 (ASN 36873 - VNL1-AS, NG) Lagos Nigeria
- 105.112.32[.]60 In network 105.112.32.0/24 (ASN 36873 - VNL1-AS, NG) Lagos Nigeria
- 105.112.32[.]98 In network 105.112.32.0/24 (ASN 36873 - VNL1-AS, NG) Lagos Nigeria
- 105.112.33[.]118 In network 105.112.33.0/24 (ASN 36873 - VNL1-AS, NG) Lagos Nigeria
- 105.112.34[.]101 In network 105.112.32.0/20 (ASN 36873 - VNL1-AS, NG) Lagos Nigeria
- 105.112.41[.]117 In network 105.112.41.0/24 (ASN 36873 - VNL1-AS, NG) Lagos Nigeria
- 105.112.41[.]127 In network 105.112.41.0/24 (ASN 36873 - VNL1-AS, NG) Lagos Nigeria
- 105.112.41[.]234 In network 105.112.41.0/24 (ASN 36873 - VNL1-AS, NG) Lagos Nigeria
- 105.112.42[.]183 In network 105.112.42.0/24 (ASN 36873 - VNL1-AS, NG) Lagos Nigeria
- 105.112.45[.]21 In network 105.112.45.0/24 (ASN 36873 - VNL1-AS, NG) Lagos Nigeria
- 105.112.45[.]89 In network 105.112.45.0/24 (ASN 36873 - VNL1-AS, NG) Lagos Nigeria
- 197.210.226[.]116 In network 197.210.226.0/24 (ASN 29465 - VCG-AS, NG) Emure-Ekiti Nigeria
- 197.210.226[.]146 In network 197.210.226.0/24 (ASN 29465 - VCG-AS, NG) Emure-Ekiti Nigeria
- 197.210.227[.]128 In network 197.210.227.0/24 (ASN 29465 - VCG-AS, NG) Oke Ila Nigeria
- 197.210.227[.]178 In network 197.210.227.0/24 (ASN 29465 - VCG-AS, NG) Oke Ila Nigeria
- 197.210.227[.]81 In network 197.210.227.0/24 (ASN 29465 - VCG-AS, NG) Oke Ila Nigeria
- 197.210.24[.]139 In network 197.210.24.0/23 (ASN 29465 - VCG-AS, NG) Nigeria
- 197.210.25[.]222 In network 197.210.24.0/23 (ASN 29465 - VCG-AS, NG) Lagos Nigeria
- 197.210.29[.]84 In network 197.210.29.0/24 (ASN 29465 - VCG-AS, NG) Lagos Nigeria
- 197.210.44[.]117 In network 197.210.0.0/16 (ASN 29465 - VCG-AS, NG) Lagos Nigeria
- 197.210.8[.]50 In network 197.210.0.0/16 (ASN 29465 - VCG-AS, NG) Lagos Nigeria
- 41.190.2[.]151 In network 41.190.2.0/24 (ASN 37076 - EMTS-NIGERIA-AS, NG) Lagos Nigeria
- 41.190.2[.]249 In network 41.190.2.0/24 (ASN 37076 - EMTS-NIGERIA-AS, NG) Lagos Nigeria
- 41.190.3[.]14 In network 41.190.3.0/24 (ASN 37076 - EMTS-NIGERIA-AS, NG) Lagos Nigeria

- 41.190.3[.]49 In network 41.190.3.0/24 (ASN 37076 - EMTS-NIGERIA-AS, NG) Lagos Nigeria

## Infrastructure for Netwire

| INFRASTRUCTURE | CONNECTION TYPE | DESCRIPTION |
|---|---|---|
| enitan1759.linkpc[.]net | TCP | C2 |
| enitan.linkpc[.]net | TCP | C2 |
| yachtingconcept.hopto[.]org | TCP | C2 |

# Conclusion

CSIR-18004

# CONCLUSION

Business email compromise (BEC) has become a massive eCrime challenge; it is essentially a global problem that affects all geographical regions and involves actors conducting fraud on multiple continents. The FBI has estimated that this fraud has resulted in billions of dollars stolen from large and small businesses alike, and CrowdStrike has observed cases were singe BEC cases have resulted in losses in the seven figures.

Many descriptions and advisories or press releases on BEC describe it in relatively simple terms, and the basic construct is simple in nature, which makes the success of the scam more impressive. However, the different variations of BEC that have been crafted show that in its different forms, it is actually a complex series of movements and events that require a multifunctional criminal team. When BEC scams are combined or conducted in conjunction with romance scams, money mule recruitments, and complex money-laundering operations, they present an enormous challenge to law enforcement, businesses, cyber security firms, and even individuals.

These scams should not be thought of separately, but rather as crimes that support one another, and as such they should be considered an advanced form of eCrime. Although the perpetration of Nigerian 419 scams and the use of keyloggers are not as advanced technically as the sophisticated banking Trojans developed and managed by Russian actors, the argument can be made that Nigerian BEC scams are just as advanced given their global scale, the amount of money involved, and the advanced money-laundering techniques that include the use of banks in China.

The arrests of Black Axe personnel in Toronto shed light on a criminal gang that is ruthless, while at the same time extremely organized and dedicated to conducting wire fraud, romance scams, money laundering, and BEC. The emergence this confraternity as a global scamming menace and advanced eCrime threat is alarming. While the online security of these actors is not complete, they take greater security measures than “standard” Nigerian criminals. Furthermore, it has been difficult for law enforcement in countries outside Nigeria to gain an understanding of how Black Axe zones are structured and how they operate. These factors, combined with persistence and tenacity, have allowed fraud conducted by Black Axe and other Nigerian criminals to flourish.

U.S. law enforcement has arrested several Nigerian criminals on BEC fraud over the past few years, and Canadian and Italian law enforcement agencies have had limited success confronting and dealing the Black Axe zones in their respective countries. Yet the magnitude of this criminal threat has only recently begun to be understood. As such, the threat posed by Black Axe and similar groups will remain high for the foreseeable future, and BEC will remain an effective eCrime technique in the near to mid-term.