HOW CLOSED SOURCE INTELLIGENCE AND OPEN SOURCE INTELLIGENCE (OSINT) HELPED LAW ENFORCEMENT UNRAVEL BUSINESS EMAIL COMPROMISE (BEC) SCHEMES – DECONSTRUCTING UNITED STATES V OBINWANNE OKEKE (4:19-mj-00116) PART 1

INTRODUCTION

In its June 2016 issue, Forbes cover picture was that of none other than that of an African – name Obinwanne Okeke, age 28, nationality Nigerian, his rags to riches inside story included in the article titled "Africa's Most Promising Entrepreneur: Forbes Africa's 30 Under 30 for 2016."

Barely a year later, May 2017, Invictus Group of Companies Limited, one of his companies – a total of fourteen of them, ten at home, 2 in Zambia, 1 each in Botswana and South Africa – won "Africa's Most Innovative Investment Company of the Year 2017 Award" from Africa Brand Congress, at the Africa Brand Leadership Merit Award, held in Lagos, Nigeria.

Just four months later, meaning September, Okeke was nominated finalist for the 7th All Africa Business Leaders Award organized by AABLA in partnership with Consumer News and Business Channel Africa (CNBC Africa) – category, Young Business Leader of the Year – West Africa.

Come 2018, Veronique Edward of the BBC interviewed Okeke live, in London, for her show "Focus on Africa" streaming the same on BBC Africa Facebook page, April 26, 2018.

But Forbes was not yet done with him. The journal got back to him two years reckoning from 2016, spotlighting Okeke in its shortlist of "Forbes 100 most Influential Young Africans of the Year 2018."

End of the flight August 2, 2019!

How come? Marshall Ward, FBI Special Agent crashes Okeke's plane, swearing to an affidavit in support of a criminal complaint against the flying magnate to requisition for an arrest warrant, when the success guy was supposed to be boarding a literal flight, this time around – destination home – away from the US, in just a matter of days, August 6, 2019, to be specific. And overnight, August 7, 2019, the warrant was successfully executed and returned. Same day, a federal public defender was appointed for him, and he was remanded in the custody of US Marshalls Service, pending the next hearing. Preliminary detention hearing before Magistrate Judge Theresa Caroll Buchanan earlier scheduled for 2 PM on August 9, 2019 in the Alexandria courtroom 500 was rescheduled for August 12, 2019 before Magistrate Judge Michael S. Nachmanoffin when, for some reason, it did not quite happen. That notwithstanding, the prosecution secured a temporary detention order. And a John Obiora Iweanoge would be appearing for him.

Okeke's third appearance came about August 12, 2019, before Magistrate Judge Michael S. Nachmanoffin in the Alexandria courtroom 400, but Okeke had reason to contest neither his detention nor his prospective trial and so was left with no choice but to sheepishly submit to custody in anticipation of an appearance before a Grand Jury.

And so, June 18, 2020, four years from June 2016, Okeke, the flying star, heard himself pleading guilty to a two-count charge of Conspiracy to Commit Computer Fraud in violation of 10 U.S.C § 1030 and Conspiracy to Commit Wire Fraud in violation of 18 U.S.C § 1349, both contained in the Statement of Facts filed in Court for and on behalf of none other than the eminent and celebrated success, Mr. Obinwanne Okeke!

Sentencing is due come October 22, 2020!

Author: Idara Akpan

FROM GRACE TO GRASS

Obinwanne Okeke, business magnate, born in Ukpor Village, Anambra State of Nigeria, some 565 KM from Abuja, FCT, November 9, 1987, 17th child of a 4th wife, with a roving childhood, ever shuttling between teacher/trader mother and dispersed relatives during school vacations, boarded at 10, orphaned of a dad at 16, holder of a first degree in International Studies and Forensic Criminology from Monash South Africa and a second degree in International Relations and Counter Terrorism with distinction from Monash University Australia, a prolific public lecturer, including TEDx talks, plus one to a distinguished audience at London School of Economics (LSE) Africa Summit in 2018.

Unatrac Holding Limited, the export sales office of Caterpillar heavy industrial and farm equipment, headquartered in the United Kingdom fell victim to Obinwanne Okeke's business email compromise (BEC) scheme climaxing in fraudulent wire transfers amounting to as good as $11 million (eleven million US dollars). A review of the documentation provided by Unatrac representatives took the FBI a whole month, followed by the commencement of investigations in July 2018.

THE PHISHING EMAIL TO UNATRAC'S CHIEF FINANCIAL OFFICER (CFO)

Thereabouts April 1, 2018, Unatrac's CFO was sent a phishing email that masqueraded as a legitimate email from Microsoft Office365 but was a flawless reproduction of the original. Unfortunately, the CFO fell for the social engineering trick when he clicked on the link, was redirected to the spoofed web page, attempted to login and passed on his account username and password to the brains behind the fabrication.

SERIAL ACCESS TO UNATRAC CFO'S ACCOUNT

With the ill-gotten access to both account username and password, the CFO's Office365 account became cannon fodder for the intruder who went on to access the same no less than 464 times primarily from Nigerian internet protocol (IP) addresses between April 6, 2018 and April 20, 2018 as the intruder ransacked emails and digital files at random with a view to coming into information to enable him make a killing.

FOUR CRIMINAL ACTS PERFORMED BY THE INTRUDER

Courtesy of total control over the CFO's account, the intruder:

1. Assumed the CFO's identity to send dishonest wire transfer requests to members of Unatrac's internal financial team
2. Buoyed up the believability of the attached bogus invoices to the email requests
3. stole Unatrac's logos and preformatted invoice templates from the CFO's commandeered account to provide an air of authenticity
4. In cognizance of the fact invoices come from external parties, prepared emails from fabricated external emails, then sent them to the CFO's account before forwarding them to the financial team with his control of the CFO's account as if the CFO had done so himself

THE FAKE INVOICE AND EMAIL FORWARD FROM PAKFEI.TRADE@GMAIL.COM

Sometime on April 19 2018, the intruder sent an email with a fake invoice from pakfei.trade@gmail.com to the CFO's account. Some one hundred and twenty seconds later, the intruder sent the same email to a member of the financial team.

Author: Idara Akpan

A FIFTH CRIMINAL ACT OF THE INTRUDER

Between April 10, 2018 and April 17, 2018, the period of the CFO's account takeover, the intruder either created or modified email filter rules a total of seven times. The idea behind the creation or modification of those rules was to keep the CFO in the dark that his account had been hijacked by denying the CFO access to the replies sent by recipients of the intruders made-up emails as well as diverting genuine emails sent to or sent by members of the financial team marking them as real and stowing them away in a folder other than the inbox!

INTRUDER'S SOCIAL ENGINEERING TRICKS WORK!

The social engineering trick succeeded! Between April 11, 2018 and April 19, 2018, members of Unatrac's financial team acted on the fabricated emails processing around 15 sham payments sometimes to the same account more than once. For example, the financial staff received and processed three invoices to Pakfei Trade Limited valued at $278,470.66; $898,461.17 and $1,957,100.00. In total, nearly $11,000,0000 was sent, all of which went to overseas accounts. When the lid blew open, it was too late to reverse the transactions or recover the funds

SIXTH CRIMINAL ACT OF THE INTRUDER

Following the takeover of the CFO's Microsoft Office365 account, the intruder pillaged the CFO's OneDrive online file storage viewing no less than 13 of his digital files mainly those dealing with his tax records and travel schedule, and in an act that proved to be his undoing, downloaded and emailed one of those files which contained parts of the company's standard terms and conditions to his email address iconoclast1960@gmail.com.

OSINT (WHOIS QUERIES) ON THE EXTERNAL EMAIL ADDRESS

WHOIS queries for iconoclast1960@gmail.com show it as a registrant for several internet domains including emmarlndustries.com which happens to be an intentional misspelling of the domain emmarindustries.com which is likely a legitimate email domain or ASM International Trading, Dubai, UAE an international financial portfolio company that could logically have business relationships with Unatrac. It is a common tactic of subjects who send phishing emails to incorporate one or two intentionally misspelled characters in the hope that the email recipients would not notice and assume that they are communicating with their clients or other legitimate business partners, rather than an unknown third party.

OSINT (WHOIS QUERIES) ON ANOTHER EMAIL ADDRESS

WHOIS queries on info@emmarlndustries.com was linked to five(5) additional domains:

- REDACTED DOMAIN 1,
- REDACTED DOMAIN 2,
- REDACTED DOMAIN 3,
- REDACTED DOMAIN 4,
- REDACTED DOMAIN 5.

REDACTED PERSON 1 of Yorktown, Virginia was named as the registrant for all five (5) of these domains.

REDACTED PERSON 1 DENIES ANY CONNECTION TO ICONOCLAST1960@GMAIL.COM

REDACTED PERSON 1 said he had nothing to do with iconoclast1960@gmail.com and that he has never registered an internet domain and that he was unaware that anyone had used his identity to do so.

INVESTIGATION GOES CLOSED SOURCE

Iconoclast1960@gmail.com was implicated in another email phishing scheme according to an FBI confidential email source who the FBI has absolute confidence in due to his job function/role as a high-level architect, access to raw malware reporting data and the fact that FBI agents have had a chance to observe at work working with irrespective of the fact that his engagements with the FBI have spanned less than a year as at the time of this investigation.

FBI's confidential source was also of the opinion that it was well-nigh impossible for iconoclast1960@gmail.com to be a legitimate account that was being hijacked from its legitimate owner by a malicious actor to perpetuate fraud as the non-legitimate activity on the account would have raised eyebrows and caused the legitimate account owner to reach out to law enforcement. This position was further solidified by the fact that FBI database searches had previously implicated the account in phishing activity.

Another FBI field office had prior to the current investigation come to the realization that iconoclast1960@gmail.com was also involved in the registration of counterfeit domains for phishing purposes, and that a Nigerian provider of domain registration services had transacted domain registration business leading to the provider sending iconoclast1960@gmail.com "Invoice Payment Confirmation" emails no less than twice between February 5, 2016 and June 21, 2018

THE JUDICIAL ARM OF GOVERNMENT GETS INVOLVED IN A BID TO SECURE GOOGLE'S COOPERATION

Some 4 months after the case was reported and 3 months and a few days after commencing investigations, on November 7, 2018, the FBI obtained official records from Google pertaining to the account iconoclast1960@gmail.com in response to a federal search warrant 4:18sw65 issued in the United States District Court for the Eastern District of Virginia. The returns from Google responsive to the FBI's first federal search warrant pertaining to this investigation highlighted that iconoclast1960@gmail.com was a major player in fraud, computer break-ins, trading in compromised credentials, setting up fraudulent wire transfers conspiracies such as the heist against Unatrac in April 2018, and another swindle against the Red Wing Shoe Company of Red Wing, Minnesota of $108,475.55 around about January 9, 2018 and this was independently confirmed by representatives of Red Wing.

The Google returns also included extensive emails and chat messaging with probable co-conspirators about designing and hosting phishing web pages to enable further identity theft scams. Other emails in the Google return contained lists of over 600 captured email account passwords and personally identifiable information like scans of passports and driver's licenses.

Returns of chat messages in the iconoclast1960@gmail.com account revealed that the operator of that account did not act alone, his several co-conspirators included the person behind REDACTED EMAIL 1 as evidenced by chat messages exchanged between December 2017 and November 2018, that discussed the particulars of setting up phishing pages to enable identity theft. In the course of these discussions, iconoclast1960@gmail.com directed REDACTED EMAIL 1 to

design phishing web pages to his specifications to ensure they looked and functioned as closely as possible to their legitimate counterparts.

On January 8, 2018 REDACTED EMAIL 1 and iconoclast1960@gmail.com sent each other emails which contained code for setting up phishing web pages in a bid to demonstrate and test their efficacy. The iconoclast1960@gmail.com account was host to hundreds of emails that can be traced to the script that resulted from those conversations given that they contained stolen login details and concluded with "REDACTED LINE 1."

HOW THE FBI DEMONSTRATED THAT EASTERN DISTRICT OF VIRGINIA'S COURT HAD JURISDICTION

Recall that the FBI obtained its first federal search warrant from the United States District Court for the Eastern District of Virginia on November 7, 2018.The Google returns in response indicated that among the stolen credentials were passwords of accounts belonging to victims located within the Eastern District of Virginia such as January 17, 2018 emails which included passwords belonging to victims located in Mechanicsville, Virginia, and another email dated January 18, 2018 which had a Richmond, Virginia victim's password and also an email dated February 26, 2018 which also held a password belonging to an Ashburn, Virginia victim.

On the basis of the above, the FBI Special Agent concluded that because the capture of these passwords was facilitated by wire communications affecting interstate commerce between the Eastern District of Virginia and locations outside Virginia, there is probable cause to believe that these emails violated Title 18, United States Code, Section 1030(a)(6) (Password Trafficking).

TRUE IDENTITY OF THE ICONOCLAST1960@GMAIL ACCOUNT REVEALED

In addition to conspiratorial conversations, fraudulent web page code, compromised credentials, the returns received from Google also revealed the true identity of the owner of iconoclast1960@gmail.com and indicated that alibabaobi@gmail.com was its listed recovery email and also linked several other accounts to iconoclast1960@gmail.com via login session cookies including notably obinwannem@gmail.com.

ONCE AGAIN INVESTIGATION GOES OPEN SOURCE AND OPEN SOURCE INTELLIGENCE CONNECTS OR MERGES VARIOUS ONLINE IDENTITIES/PERSONA

Open source intelligence on

- obinwannem@gmail.com linked it to the online forum hosted by Nairaland.com and to a Nairaland user named Invictusobi who had listed obinwannem@gmail.com as his contact address;
- the Nairaland.com profile page for Invictusobi linked it to the Twitter username @Invictusobi.
- the Twitter page for @Invictusobi identified the user as Obinwanne Okeke in Abuja, Nigeria
- Obinwanne Okeke associated him with a company called Invictus Group
- the Twitter page also claimed that he maintained an Instagram page with the same username Invictusobi
- Both the Twitter and Instagram pages led to the conclusion that both the Twitter and Instagram pages appeared to be true identity and contained posts as recent as July 2019 (to put this date in context, it should be recalled that this Affidavit was filed on August 2, 2019)

- Okeke's Instagram page found numerous posts indicating that he travels extensively throughout the world

NEXT INVESTIGATION GOES MIXED SOURCE BY COMPARING AND CONTRASTING CLOSED SOURCE AND OPEN SOURCE INTELLIGENCE RECORDS, BRIDGING THE GAP BETWEEN ONLINE AND OFFLINE IDENTITY

On March 31, 2018 Okeke posted to Instagram post claiming that he was in Seychelles. Google's records for March 31, 2018 indicated that there was a login to iconoclast1960@gmail.com account from an IP address 197.158.125.89 which is located in Seychelles.

On April 20, 2018 Okeke stated that he was in England. Google's logs for April 20, 2018 also showed a login to the iconoclast1960@gmail.com account from an IP address 167.98.28.227 in London, England.

Between June 25 – 27, 2018, Okeke claimed that he was in Washington DC. Google's return also reported a login to the iconoclast1960@gmail.com account from IP address 68.33.78.173 located in Washington DC.

Open source intelligence on Okeke's Instagram page uncovered a post-dated July 12, 2018 where Okeke claimed to be in hospital recovering from surgery. That post contained a picture of Okeke lying in a hospital bed with the text "Thank God for seeing the surgery through and making it a successful one." Marshall Ward, FBI Special Agent then searched for the term "hospital" in the chat messages contained in the iconoclast1960@gmail.com account from records provided by Google and found a conversation which appeared to reference Okeke's hospital visit.

Yet other chat messages with iconoclast1960@gmail.com indicate that others often referred to him in his true name or nickname "Obi", "Chief Obi" or "Obinwanne" confirming for a certainty that iconoclast1960@gmail.com is none other than Okeke.

Further confirmation that iconoclast1960@gmail.com is none other than Invictusobi is that official records from Google for iconoclast1950@gmail.com email content included the term Invictusobi twice.

Additionally, content in closed source records, i.e., pictures in his email were posted in open source records, i.e., pictures in his Instagram account and on the same date! There is also the fact that the picture posted on the Instagram account originated from iconoclast1960@gmail.com.

By correlating closed source and open source records, the FBI succeeded in connecting three email accounts to Okeke. On February 27, 2016 iconoclast1960@gmail.com sent an email to alibabaobi@gmail.com (which was the recovery email of iconoclast1960@gmail.com). On March 4, 2016 iconoclast1960@gmail.com forwarded the February 27, 2016 email above to invictusobi@icloud.com. The attachment to both emails corroborated the FBI's findings that the person running all three accounts was involved in identity theft and credit card fraud.

THE JUDICIAL ARM OF GOVERNMENT AGAIN GETS INVOLVED IN A BID TO SECURE GOOGLE'S AND APPLE'S COOPERATION

Let us review the case so far. The case was reported to the FBI around June 2018. Investigations by the FBI commenced around July 2018. The first federal search warrant 4:18sw65 for official records from Google pertaining to the account iconoclast1960@gmail.com was sought for and obtained by the FBI on November 7, 2018 some 4 months after the case was reported and 3 months and a few days after commencing investigations. Having completed a review of those records, new

leads turned up and these needed to be explored as well and so some 5 months and a few days after commencing investigations, and 1 month and 2 weeks after the first federal search warrant was obtained, the FBI once again approached the courts for this time around, not one but 2 search warrants. The second federal search warrant 4:18sw81 for official records from Google for the accounts REDACTED EMAIL 1, alibabaobi@gmail.com and obinwannem@gmail.com was served on the company December 21, 2018. The third federal search warrant 4:18sw83 for official records from Apple for the account invictusobi@icloud.com was served on the company on the same date. The FBI's review of the returns indicates the accounts alibabaobi@gmail.com, obinwannem@gmail.com and invictusobi@icloud.com are all used in true name by Okeke.

An analysis of REDACTED EMAIL 1 records (one of the three email accounts in the second federal search warrant) confirmed the account's involvement in the fraudulent scheme as evidenced by multiple discussions about setting up phishing web pages and to fleece victims of money dishonestly. Google's returns also tied the operator of REDACTED EMAIL 1 through session cookies to several dozen email accounts implicated in other FBI investigation of fraud reports such as REDACTED EMAIL 4.

THE JUDICIAL ARM OF GOVERNMENT GETS INVOLVED YET AGAIN IN A BID TO SECURE GOOGLE'S AND APPLE'S COOPERATION

Having completed a review of the returns for REDACTED EMAIL 1, alibabaobi@gmail.com, obinwannem@gmail.com and invictusobi@icloud.com, more new leads turned up and one of those leads was REDACTED EMAIL 4.

And so once again to stay on the right side of the law, some 11 months after the case was reported and 10 months after the FBI commenced investigations, 6 months and 8 days after returns responsive to the first federal search warrant were received, 4 months and 24 days after returns responsive to the second and third federal search warrant were received, it became necessary to serve a forth federal search warrant from the Eastern District of Virginia on May 19, 2019 for official records from Google for multiple Google accounts including REDACTED EMAIL 4 4:19sw74,. REDACTED EMAIL 5 4:19sw77 AND REDACTED EMAIL 6 4:19sw79.

FINDINGS FROM THE RETURN ON REDACTED EMAIL 4

Some 26 days later, June 10, 2019 Google's return indicated that REDACTED EMAIL 4

- was active,
- that the account was implicated in thousands of fraudulent home repair schemes and
- that there was one merchant in Hampton, Virginia who was defrauded in 2015 of $11,570.00.

FINDINGS FROM THE RETURN ON REDACTED EMAIL 5

Official records from Google pertaining to the account iconoclast1960@gmail.com also indicated that the operator of iconoclast1960@gmail.com interacted with several other co-conspiratorial accounts including REDACTED EMAIL 5 and REDACTED EMAIL 6. Given that both redacted email accounts appeared to be the most significantly involved, the FBI came to the determination that they had to conduct an in-depth investigation into those accounts.

Some of the findings from the Google return on REDACTED EMAIL 5 may be summarized as follows:

- REDACTED EMAIL 5 was active,

- REDACTED EMAIL 5 was linked to REDACTED PHONE NUMBER 1,
- REDACTED EMAIL 5 was also linked to several other email accounts including REDACTED EMAIL 7 via session cookies,
- REDACTED EMAIL 5 and iconoclast1960@gmail.com had extensive discussions,
- the communication between REDACTED EMAIL 5 and iconoclast1960@gmail.com involved trafficking in stolen/compromised accounts and passwords,
- the victims spread across 5 US States,
- the communication between them also zeroed in on certain accounts and specific individuals such as the October 15, 2018 email sent by REDACTED EMAIL 5 to iconoclast1960@gmail.com over an upcoming real estate transaction valued at $585,000.00 that suggested a man-in-the-middle attack to waylay the outstanding balance of $526,000.00 and the December 13, 2018 chat conversations between REDACTED EMAIL 5 and iconoclast1960@gmail.com which identified a third co-conspirator named Kelvin.

FBI immigration database record searches indicated that REDACTED PHONE NUMBER 1 and REDACTED EMAIL 7 were both used by REDACTED PERSON 2 a Nigerian citizen on a visa application for entry into the United States dated November 20, 2018.

Okeke and REDACTED PERSON 2 both traveled to the United States on March 10, 2019.

FINDINGS FROM THE RETURN ON REDACTED EMAIL 6

The FBI also received on June 10, 2019 official records from Google For REDACTED EMAIL 6 in response to a sixth federal search warrant 4:19sw79. The findings from that return maybe summarized as follows:

- REDACTED EMAIL 6 was active,
- REDACTED EMAIL 6 was linked to REDACTED PHONE NUMBER 2,
- REDACTED EMAIL 6 and iconoclast1960@gmail.com had extensive discussions,
- the communication between REDACTED EMAIL 6 and iconoclast1960@gmail.com involved trafficking in stolen/compromised accounts and passwords and attachments and included copies of likely stolen passports,
- the communications between them also zeroed in on certain accounts and specific individuals to target such as the September 14, 2017 email sent by REDACTED EMAIL 6 to iconoclast1960@gmail.com which listed a victim's compromised email account and password and that also named a second user's email account who he claimed "approves transfers" and the name of an employee at the potential victim firm whom REDACTED EMAIL 6 suggested was "probably the accountant"

REASONS ADDUCED IN SUPPORT OF THE ISSUE OF AN ARREST WARRANT

For the above reasons, the affidavit submitted that probable cause exists that Obinwanne Okeke has participated in violations of 18 USC §§ 1030 and 1349.

The results of the investigation were unambiguous that Okeke conspired had with several persons including REDACTED PERSON 2 and REDACTED PERSON 3 to carry out computer fraud and organize fraudulent wire transfers.

The affidavit then provided his date of birth, passport number and nationality as well as the number of times he visits the United States yearly before indicating his next departure date and

requesting that the court authorize an arrest warrant to guarantee his apprehension before his departure from the US complicates the process of law enforcement getting hold of him.

THE ROLE OF OPEN SOURCE INTELLIGENCE

In part two of this paper, technical details as to how open source intelligence helped the FBI came to the conclusion that Okeke had conspired with several individuals to access computers without authorization and used such access to cause the fraudulent wire transfer of such funds will be reviewed.