REPORT

London Blue
UK-Based Multinational Gang Runs BEC Scams like a Modern Corporation
Executive Summary

Agari has uncovered the working methods of a U.K./Nigerian gang with U.S.-based co-conspirators conducting Business Email Compromise (BEC) attacks against companies around the world.

Nigeria has been a hub for scammers since long before the Internet came into wide use, and it remains one of the world’s primary centers for active gangs, including many that are focused on BEC.

But with London Blue, a Nigerian gang has extended its base of operation into Western Europe, specifically into the United Kingdom, where at least two of the primary London Blue members operate. We have also identified 17 additional collaborators located in the United States and Western Europe who are primarily involved in moving stolen funds.

London Blue operates like a modern corporation. Its members carry out specialized functions including business intelligence (lead generation), sales management (assignment of leads), email marketing (semi-customized BEC attack emails), sales (the con itself, conducted with individual attention to the victim), financial operations (receiving, moving and extracting the funds), and human resources (recruiting and managing money mules).

London Blue’s effectiveness depends on working with commercial data brokers to assemble lists of target victims around the world. Doing so gives it the attack volume of a mass spam campaign, but with the target-specific customization of spear-phishing attacks. By combining commercially available tools with criminal tactics, the attackers are able to deliver semi-customized attacks on companies of all sizes in countries located around the world.

During our research into London Blue, we identified a list of more than 50,000 corporate officials generated during a five-month period in early 2018 and used to prepare for future BEC phishing campaigns. Among them, 71 percent were CFOs, 2 percent were executive assistants, and the remainder were other finance leaders.

Targets included companies in a very broad range of sectors, from small businesses to the largest multinational corporations. Several of the world’s biggest banks each had dozens of executives listed. The group also singled out mortgage companies for special attention, which would enable scams that steal real estate purchases or lease payments. The attack emails typically contain no malware, thus rendering them invisible to many of the most common email security measures.

Well over half of the 50,000 potential victim profiles that London Blue compiled in their targeting database were located in the United States. Other countries commonly targeted included Spain, the United Kingdom, Finland, the Netherlands and Mexico. In total, potential targets in 82 different countries were identified in London Blue’s target repository.

Like other BEC gangs, London Blue evolved into BEC attacks after previously focusing on other phishing activities like credential phishing and Craigslist scams.
Table of Contents

Background 4
Uncovering London Blue 5
Evolution of London Blue’s Attack Method 11
A Look Inside London Blue’s BEC Enterprise 14
Conclusion 18
## Background

### BEC Overview

Business email compromise is an advanced email attack that leverages the most common form of identity deception—display name deception—most frequently targeting finance teams to make fraudulent payment requests.

Operational intelligence about BEC targets may be gathered from a variety of open sources such as LinkedIn; however, this report demonstrates that these criminals are also leveraging proprietary marketing services to obtain lists of legitimate business email addresses.

According to the FBI Internet Crime Complaint Center (IC3), BEC is a $12 billion scam. Previous Agari research has demonstrated that BEC is the most popular and most effective email scam—producing 3.97 victims for every 100 initial email responses. With an average payment request of $35,000, BEC is big business for these criminal organizations—and as we will explore in this report, they operate like one too.

BEC attack emails typically contain no malware, thus rendering them invisible to many of the most common email security measures.
Uncovering London Blue

In a move that could be described as felony stupid, London Blue targeted Agari with one of its typical attacks.

Agari CFO Raymond Lim was on a list of 306 target victims London Blue obtained in November 2017. The list, which was generated by a commercial data provider, consisted almost entirely of CFOs, plus other people who had CFO in their title, such as “CEO and CFO” or “Executive Assistant to CFO.”

Initial Discovery of London Blue

In addition to Agari, the list targeted California-based CFO victims at one of the world’s top private universities, a major enterprise data storage company, a famed guitar maker, casinos and hotels, a retirement home, and small and medium-sized businesses of all types.

On August 7, 2018, London Blue sent an attack email to Lim, appearing to come from Agari CEO Ravi Khatod. While the actual sending email account is on the daum.net domain, the display name on the email is Ravi Khatod.

Agari then engaged actively with the attacker, giving us an initial glimpse of the gang that we would widen into a penetrating X-ray.
Ravi,

Raymond is out this week and I will help you with the transfer. Would you please provide me with the transfer details? Also just a reminder, as you may know, all payments go out on Wednesday, which is tomorrow. So if you need to make another transfer or payment, please inform me so that I could take care of them together before tomorrow's cut-off passes.

Best Regards,

Alicia
From: Ravi Khatod <cceeooss@daum.net >

Subject: Re: wire

Please process and code to admin expenses

Bank of America
385 McLean Blvd,
Paterson, NJ 07514

Routing:
Account:

AMOUNT: $25,890

Wellsfargo Bank
420 Montgomery Street,
San Francisco, CA, 94104,

Routing:
Account:

Amount: $22,650

I will have the invoice sent to you shortly. Email me the transfer confirmation as soon as it is done, so I can forward it to the beneficiary as proof of payment. Please acknowledge receipt of this mail

Thanks

Ravi Khatod
Alicia, did you get the wire instructions yet? Please advise

Thanks

Ravi

Ravi,

I processed the Bank of America transfer successfully, the customer should see the wire coming through on her end. Attached is the wire confirmation, please check.

I did try to take care of the Wells Fargo one, but unfortunately, the transfer was rejected by the bank. It seems that there’s something wrong with the recipient account. Would you please ask the customer to double check if the account information is right? Or could the customer provide us a different account?

Best Regards,

Alicia
Alicia, i have just been able to get a different wire instruction regarding the wells Fargo that we could not get sent out. Are you able to process now? Please advise

Thanks

Ravi

Ravi,

Of course, I can help you with that. Send me the wire details and I will process it for you.

Alicia

Agari continued engaging with London Blue to gain more insight into the group and identify additional mule accounts. By gathering information on mule accounts, Agari is able to advise financial services of fraudulent or malicious accounts to help shut them down.
Who is London Blue

Nigeria has been a hub for scammers since long before the Internet came into wide use. The origin of the “Nigerian Prince” advance fee scam dates back to a similar Spanish prisoner scam in the mid-16th century. Today, Nigeria remains one of the world’s primary centers for active gangs, including many who are focused on BEC. In fact, previous Agari research indicates that 90% of BEC groups operate out of Nigeria.

Based on our research, while the primary members of this group likely originated in Nigeria, at least two of them have extended the group’s base operations into Western Europe—specifically into the United Kingdom, hence the first part of the group’s name. In addition to these two primary threat actors located in the U.K., we have identified 17 other potential collaborators located in the United States and Western Europe who are primarily involved in moving stolen funds.

In our analysis of London Blue, we identified the working methods of a group that has taken the basic technique of spear-phishing—using specific knowledge about a target’s relationships to send a fraudulent email—and turned it into massive BEC campaigns.

Each attack email requesting a money transfer is customized to appear to be an order from a senior executive of the company. Conventional spear-phishing requires time-consuming research to gather the info needed for the attack to be successful—identifying individuals with access to move funds, learning how to contact them, and learning their organizational hierarchies. However, commercial lead-generation services have allowed London Blue to short-cut gathering the necessary data for thousands of target victims at a time.

By combining commercially available tools with criminal tactics, attackers based anywhere in the world are able to deliver semi-customized attacks on companies of all sizes located in countries around the world.
Evolution of London Blue’s Attack Methodology

Based on our historical visibility into London Blue, we have been able to observe an evolution in the group’s scamming methodology over time.

2011: Craigslist Scams

Beginning around 2011, the group was heavily involved in Craigslist scams. These scams involved contacting sellers in the United States inquiring about whether an item for sale was still available. Here’s how these scams usually worked:

- If a seller responds, the London Blue actor tells them that they can pay for the item with a certified check, but they won’t be able to pick the item up and will need to use a local “mover.”
- To pay for the mover, the threat actor writes the check for well over the price of the item and asks the seller to send the difference to the “mover” via Western Union.
- A US-based accomplice sends a check to the seller through FedEx or UPS.
- These certified checks are high-quality counterfeits; however, they’re generally not caught by the seller’s bank immediately, so the victim sends the money to the “mover.”

---

To Nick Gorman

Subject Ashley Furniture Living Room Set - $350

Hello, how are you doing today? Just saw this item and would really love to know if it is still available for sale?

Thanks
2015: Credential Phishing

London Blue then transitioned to credential phishing attacks, primarily focused on impersonating web pages used by enterprise users, such as Adobe ID, Dropbox, and Microsoft Office 365. This transition occurred around 2015 when the global surge of BEC attacks was just beginning. Based on the temporal context, it is likely that the purpose of the London Blue’s credential phishing campaigns was to compromise business email accounts in order to send BEC emails to other employees.

Example of a London Blue credential phishing email lure.

Example of a London Blue Adobe credential phishing page.
Once a scammer gets hold of an employee’s email credentials, he can surreptitiously take over the email account and use it for a wide variety of malicious purposes. As an example, the real estate industry has been a prime target of these attacks. A scammer gets into the email of real estate or title agents, and monitors pending real estate sales or lease signings. As the closing date approaches and the payment is about to be made, the scammer sends an email to the buyer or lessor providing an account number for a fraudulent wire transfer. The email appears totally legitimate since it is sent from the actual email account of the real estate or title agent. Once the transfer is made, the money is gone—we call this scam the homeless homebuyer.

Any company that sends invoices is vulnerable to these attacks. Invoices can be sent to actual customers for goods they purchased, using invoice forms identical to the real ones, with instructions to transfer payment to a scammer-controlled account. For companies routinely sending or paying invoices for tens of thousands of dollars, it can be many weeks or even months before they realize they’ve been duped.

Obtaining log-in credentials to a corporate network makes all kinds of attacks easier: early access to earnings reports for public companies, W-2 scams enabled by access to employee salary data, and ransomware.

2016: Business Email Compromise

In early 2016, London Blue evolved their tactics to start sending BEC emails to employees using display name deception. Using this tactic, the group registers free webmail accounts and sets the display name (the apparent name of the sender) to match the person being impersonated. This tactic has continued to be the group’s preferred modus operandi through present day.

<table>
<thead>
<tr>
<th>To</th>
<th>John Tabbot <a href="mailto:jtab@daum.net">jtab@daum.net</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject</td>
<td>Transfer</td>
</tr>
</tbody>
</table>

John, we need to make a transfer today. Let me know if you can process now and i will send info.

Thanks
James

Example of a London Blue BEC phishing email.
A Look Inside London Blue’s BEC Enterprise

Organizational Structure

London Blue operates like a modern corporation. Its members carry out specialized functions including business intelligence (lead generation), sales management (assignment of leads), email marketing (semi-customized BEC attack emails), sales (the con itself, conducted with individual attention to the victim), financial operations (receiving, moving, and extracting the funds), and human resources (recruiting and managing money mules).

- **Lead Generation**: London Blue group members collect and share "leads" to identify potential targets.
- **Open Source Recon**: Additional open source research is likely needed to gather missing information, such as CEO names/email addresses.
- **Testing**: Prior to SEC campaigns, group members send test emails to themselves and other members to make sure attempts are sent and/or received.
- **BEC Attack**: BEC Attack Emails Sent.
- **Mule Account**: Mule accounts used to receive funds are shared to primary actors in the group.
Who Do They Target?

During our research, we identified a file containing a list of more than 50,000 finance executives that was generated over a five month period in early 2018. This list was likely used by London Blue as a massive targeting repository for their BEC attacks. Among them, 71 percent held a CFO title, 12 percent were finance directors or managers, nine percent were controllers, six percent held accounting roles, and two percent had executive assistant titles.
Well over half of the 50,000 potential victim profiles that London Blue compiled in their targeting database were located in the United States. Other countries commonly targeted by London Blue were Spain, the United Kingdom, Finland, the Netherlands, and Mexico. In total, potential targets in 82 different countries were identified in London Blue’s target repository.

Use of Commercial Data Providers to Identify Targets

Like a business, London Blue uses commercial data providers to identify potential targets of their BEC campaigns. Most recently, the group has relied on a San Francisco-based company to generate “leads.” Using this service, London Blue is able to collect comprehensive information about targets, including name, company, title, work email address, and personal email address. All of the potential targets London Blue collects information on have financial roles in their respective companies.

These leads are collated and shared among various members of the group. Notably, much like a sales department targets prospects in specific regions, London Blue focuses on specific states or countries during each of their lead generation runs. Out of the more than 60 distinct lead lists we have identified, more than half of them are finely crafted to collect data on financial targets in nine different U.S. states and seven countries.

Essentially, this data gives the group the initial information needed to start preparing for their phishing campaigns. After collecting this information, the group then likely conducts further open source research to identify the names of CEOs affiliated with the companies they will be impersonating for their BEC attacks.

Attacks in Non-English Languages

London Blue sends attack emails in multiple languages, usually variants on the same message: a fraudulent email from the CEO or CFO asking a lower-level staff member to make an urgent transfer.

<table>
<thead>
<tr>
<th>From</th>
<th>&lt; <a href="mailto:mdceo001@lavabit.com">mdceo001@lavabit.com</a> &gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To</td>
<td></td>
</tr>
<tr>
<td>Subject</td>
<td>Dringend</td>
</tr>
</tbody>
</table>

Koen, müssen wir heute eine Überweisung tätigen. Lassen Sie mich wissen, wenn Sie jetzt verarbeiten können, und ich werde Info senden.

Dank Davy

This is an attempted scam of a Belgian property development company. The email, purporting to be from the company’s managing director, is sent to a finance staff member. It says, “We have to make a transfer today. Let me know if you can process now and I will send info.”
This is an attempted scam of a large property management company based in Stockholm. The email, purporting to be from the company’s CEO, is sent to a finance team member, and says, “We need to send a payment of €23,650 to England today. Let me know if you can process now and I will send info.”

This attack makes the use of display name deception since email platforms and software allow senders to use anything they want as a display name. Email readers or services often show only the display name but not the underlying email address.

**Use of Money Mules, Including Convicted Sex Offenders**

Over the course of our research, we identified 17 individuals being used by London Blue as money mules located in the United States and Western Europe. These money mules are used by the group to receive and move illicit funds gained during their scams.

Notably, at least three of the 17 money mules have criminal records. Two have prior felony convictions for sex-related crimes. The increased difficulty that convicted felons face in finding legitimate jobs—and convicted sex offenders likely face an even greater challenge—may be correlated with the willingness of these individuals to participate in these scams.

One of the transactions we observed involved a money mule in a Western state who received a cashier’s check of more than $20,000 from one of the largest U.S. banks. The transaction had originally been flagged by a local branch of the bank as being potentially fraudulent. But the money mule, a registered sex offender with a lengthy criminal record and experience in the mortgage industry, was able to convince the bank’s loss prevention unit that the transaction was legitimate. The check was then cashed and deposited into another account, presumably to be accessed by the primary London Blue actors.
Conclusion

This report demonstrates that cybercriminal groups continue to evolve and are using formal business strategies and structure to more effectively carry out their scams. London Blue’s use of legitimate commercial sales prospecting tools shows the out-of-box thinking these groups employ to identify new targets. The pure scale of the group’s target repository is evidence that BEC attacks are a threat to all businesses, regardless of size or location.

Appendix A - Email Addresses Associated with London Blue BEC Attacks

abbyss101@aol.com
bluegate000@mailfence.com
bluegate001@yandex.com
bluegate002@naver.com
bluegate010@naver.com
bluegate101@163.com
bluegate102@naver.com
blugate000@lumail.lu
blugate001@naver.com
ceoadmiin@163.com
c eoofficeadmin@gmail.com
c eos.em@mail.com
mdceo001@hush.com
mdceo001@lavabit.com
mdceo002@naver.com

Appendix B - Historical London Blue Credential Phishing URLs

http://arkitecture.ro
http://ih891976.myihor.ru/MicrosoftOutlook/
http://odebrechit.com/images/app/
http://patanjaliayurved.net/1tt.rbqet.netbank.com/
http://servisdropbox.com/
http://www.accat.cat/fotosnoticias/bt/index.htm
http://www.ih1111296.myihor.ru/ouloo00k/OutL00k/
http://www.laras-world.com/source/modules/
http://www.mashablegift.ml/manager/update_mail1/
REPORT

London Blue
April 2019 Update

UK-Based Multinational Gang Evolves Their Tactics, Targeting Asian Users and Spoofing Email Addresses
In December, we published a report on a business email compromise (BEC) group of cybercriminals we call London Blue. In this report, we documented how this group, which has roots in the United Kingdom, evolved its tactics over time, from Craigslist scams to enterprise credential phishing to BEC as they matured into a criminal enterprise that is structured and operates much like a modern corporation. We also discussed how the group uses legitimate commercial services to mass harvest target data for their phishing campaigns, which included a master targeting database containing the contact information of more than 50,000 financial executives. That list was collected over a five-month span in early 2018.

Since the release of our previous report, we have continued to track London Blue’s activities in real time. This report provides an update on how the group has continued to evolve over the last few months, including how they have started targeting new parts of the world and how they are now using new tactics in their BEC campaigns.

How Not to Stay Under the Radar

In our last report, we mentioned that we started investigating London Blue after they targeted Agari CFO Raymond Lim in August 2018. In January, the group made the decision to try their hand at targeting our CFO... again. This time, though, we knew the malicious email was coming. Because of our visibility into London Blue’s operations, we were able to observe the entire lifecycle of the group’s attack chain, from preparation to execution.

Targeting a Cybersecurity Company

Here’s what the lifecycle of London Blue’s BEC attempt against Raymond looked like:

- **January 11, 2019:** Raymond’s contact information, in addition to information for more than 500 other financial executives, was collected by one of the primary London Blue actors using a commercial US-based lead service in the initial preparation stage for BEC campaigns targeting California-based companies.

- **January 13, 2019:** A CSV file containing the raw leads for these identified targets was sent to another London Blue associate for processing. Processing involves organizing and validating the targeting data and supplementing it with open source intelligence to identify a company’s CEO, who is then impersonated during the attack.

- **January 22, 2019:** The associate sent a batch of processed leads back to the primary actor, which contained Raymond’s validated email address and the name of Agari’s CEO at the time. This was the second of two batches of processed leads. The first was returned to the primary actor on January 16, 2019.

- **January 28, 2019:** In preparation for a round of BEC attacks, a test email was sent from an attack email account to one of the group’s central operational email addresses. This test email is likely used to verify that a BEC email will successfully be delivered to a target without being blocked. All BEC groups we have tracked have used similar testing methods prior to launching their campaigns.

- **January 28, 2019:** Three and a half hours after the initial test email, London Blue’s attack email is sent to Raymond, but is blocked by Agari Advanced Threat Protection before it hits the inbox.
In the August 2018 BEC attempt, London Blue used one of the more common BEC ruses, claiming a payment is due to a vendor and a wire transfer needs to be processed ASAP. In the January campaign, however, the group switched tactics and used a mergers and acquisitions theme.

After a generic initial email meant to elicit a response, the London Blue attacker stated that an international vendor accepted an offer for acquisition and, based on the terms of the agreement, 30 percent of the purchase price needs to be paid in advance via wire transfer to a Mexican bank. Of course, until the “acquisition” has been announced publicly, details about the news were not to be shared with anyone else.

Our initial engagement with London Blue during this latest campaign is shown below:

---

**Messages**

From: Ravi Khatod <lockarff1@mailbox.org>
To: Raymond Lim <rlim@agari.com>
Subject: trf

Hi Raymond,

Are you at the office?

Ravi
Hi Ravi,

Raymond has been out of the office this week. He just forwarded the email you sent him earlier this week and wanted me to see if you still needed anything. Please let me know if I can help out.

Thanks,
Luis

Okay, I need you to take care of this personally, I have just been informed that we have had an offer accepted by a new international vendor, to complete an acquisition that I have been negotiating privately for some time now, in line with the terms agreed, we will need to make a down payment of 30% of their total, Which will be $86,000

Until we are in a position to formally announce the acquisition I do not want you discussing this with anybody in the office, any question please email me, can you arrange a wire transfer now?

Thanks
Very exciting! I can absolutely take care of that for you and, don’t worry, I’ll keep the information to myself until we’re ready to announce it publicly.

If you send over the information for the transfer, I can take care of it ASAP.

See account details below, let me know should you need anything.

ACCOUNT NUMBER ......  
ACCOUNT NAME.....  
BANK NAME ......  
CLABE -  
SWIFT CODE .......  
BANK ADDRESS.... MEXICO NUEVO LEON, MEXICO.

I will have the invoice sent to you shortly. Email me the transfer confirmation as soon as it is done so I can forward it to the beneficiary as proof of payment. Please acknowledge receipt of this mail.

Thanks
Transfer sent! The confirmation has been attached for your reference. Please send me the invoice when you get a chance and let me know if any issues arise in the other end.

This sounds like a big deal for us. Any idea when we’ll be going public with the news?
Gazing East into Asia

During our continued monitoring of London Blue, we have observed them collect targeting information for a significant number of additional targets.

London Blue Focuses on Asian Targets

Since November 2018, the group has amassed a new targeting database of nearly 8,500 financial executives from almost 7,800 different companies around the world. Similar to their previous targeting dataset, a plurality of these targets are located in the United States.

That said, one of the notable observations about London Blue’s target selection over the past five months is that many of their targets are located in Asia, an area we have not seen the group target previously. In February, London Blue collected contact information for and launched BEC campaigns against targets in Hong Kong and Singapore. In March, the group targeted employees located in Malaysia.

Interestingly, while the employees targeted by the Asia-focused attacks are located in Asia, the companies they work for are not based in those countries. A review of these targets indicates that nearly all of them work for companies based in the United States, Western Europe, or Australia. This makes sense since the BEC emails we have observed targeting individuals in these countries are written in English and not in the local language.
Evolving Tactics: London Blue Starts Spoofing Target Domains

In late-February, London Blue made a rather dramatic shift in their attack methodology. Rather than simply using a free and temporary email account with an imposter display name to send their BEC emails, a tactic the group has used consistently since 2016, they started spoofing the email address of the target company’s CEO as a way to add a bit more authenticity to their malicious attacks.

Example of a domain spoofed London Blue email targeting a Dutch company

While this is London Blue’s first foray into email spoofing as an attack technique, this is not an uncommon tactic and has been used by scammers for years in BEC campaigns and other types of email-based attacks.

Unsurprisingly, most of the companies we have observed London Blue target using spoofing techniques do not have a DMARC record established. The few targeted companies that do have DMARC records set up only have their policies set to p=none, which only sends failure reports to a specified email address and does nothing to prevent a spoofed email from reaching its intended target.
Conclusion

This report demonstrates that cybercriminal groups continue to evolve and are using formal business strategies and structure to more effectively carry out their scams. London Blue’s use of legitimate commercial sales prospecting tools shows the out-of-box thinking these groups employ to identify new targets. The pure scale of the group’s target repository is evidence that BEC attacks are a threat to all businesses, regardless of size or location.

Appendix A – Email Addresses Associated with London Blue BEC Attacks

Email addresses with asterisks (**) are new since our last report was released in December 2018.

abbyss101@aol.com
admin@com1t.ga**
admin@com1r.ml**
admin@com9g.ml**
afterplay@mailbox.org**
amc11@mailbox.org**
bluegate000@mailfence.com
bluegate001@yandex.com
bluegate002@naver.com
bluegate010@naver.com
bluegate101@163.com
bluegate101@eclipso.me**
bluegate102@naver.com
bluegate231@daum.net**
blugate000@lumail.lu
blugate001@naver.com
ceadmiin@163.com
coeofficeadmiin@gmail.com
ceos.em@mail.com
ceos1@daum.net**
ceoses101@sol.dk**
lockarff1@mailbox.org**
lockarff1@daum.net**
lockup11@mailbox.org**
mdceo001@hush.com
mdceo001@lavabit.com
mdceo002@naver.com
outlookeracct@mailbox.org**
workon1@mailbox.org**
The Agari Cyber Intelligence Division (ACID) is the only counterintelligence research team dedicated to worldwide BEC and spearphishing investigation. ACID supports Agari’s unique mission of protecting communications so that humanity prevails over evil. ACID uncovers identity deception tactics, criminal group dynamics, and relevant trends in advanced email attacks. Created by Agari in 2018, ACID helps to impact the cyber threat ecosystem and mitigate cybercrime activity by working with law enforcement and other trusted partners.

Agari Data, Inc.
950 Tower Lane Suite 2000, Foster City, CA 94404