AGARI CYBER
INTELLIGENCE DIVISION

THREAT INTELLIGENCE BRIEF

The Geography of BEC

The Global Reach of the World's Top Cyber Threat

Executive Summary

Every single day, the Agari Cyber Intelligence Division (ACID) engages with Business Email Compromise (BEC) scammers who try (and fail) to target Agari customers with phishing attacks.

The information contained in this report comes from more than 9,000 active defense engagements conducted by ACID between May 2019 and July 2020. As a result of these engagements, we are able to collect crucial intelligence that allows us to better understand the operations of BEC criminal organizations. This includes the locations of the threat actors who perpetrate these attacks, as well as the money mules who play such an integral role in laundering the proceeds from these crimes.

The purpose of this report is to demonstrate the global reach of BEC attacks. Historically, Nigeria has been the traditional epicenter of social engineering scams, but this report shows that the actors responsible for BEC attacks have branched out in recent years. We identified BEC actors in 50 different countries, yet only half of the scammers we identified were located in Nigeria.

Surprisingly, a quarter of all BEC attackers had a home base in the United States. Nearly half of US-based BEC actors were located in five states: California, Georgia, Florida, Texas, and New York. Looking at the data more granularly, we observed clusters of actors around a handful of metro areas, including Atlanta, GA; New York, NY; Los Angeles, CA; Houston, TX; and Miami, FL.

Money mules, one of the most important components of the BEC financial supply chain, were also observed around the world. Over the course of 15 months, we collected 2,900 mule accounts in 39 countries, through which scammers intended to receive more than $64 million in stolen funds from BEC victims. While 80% of these mule accounts were located in the United States, the requested payment amounts destined for those accounts were significantly lower than other countries. For example, the average amount of payments to US-based mule accounts was $39,500, while payments directed to mule accounts based in Hong Kong were $257,300—more than six times their stateside counterparts.

Within the United States, more than 900 mules were identified across all 50 states, as well as the District of Columbia. While many of these mules are likely to be unwitting victims of other social engineering attacks, from romance scams to work-from-home cons, a significant number of these mules were clustered around a small number of cities, indicating these areas may be hubs of BEC activity in the US. Mirroring the clusters of BEC actors, the top metropolitan areas for money mules in the US were Dallas, TX; New York, NY; Atlanta, GA; Houston, TX, and Los Angeles, CA.

ACID conducted

9,000+

active defensive engagements

BEC actors are located in

50

countries

Nigeria is home to

50%

of all BEC actors

Money mules are found in

39

countries

ACID identified

900

money mules in the US

Table of Contents

"Falling Mugu"

A Historical Look at the Origins of BEC

When we take a step back and look at the history of BEC, most of the seasoned actors have some nexus to Nigeria. It is here, after all, where BEC first gained global notoriety back in 2015, when email fraud rings first began defrauding organizations by impersonating their CEOs and CFOs in email scams targeting employees.

Seemingly overnight, "Are you on desk?" became a cybercriminal sensation as the opening salvo in identity deception attacks, where scammers would instruct unsuspecting employees to wire thousands of dollars out of an organization. Today, email scammers continue to find clever new ways to bamboozle employees into costly mistakes. But to fully understand the evolution of BEC, you have to go back much further, to the early 1990's.

Popular in the 1990s, 419 fraud—aka, Nigerian Prince scams—were the forbearers of today's BEC attacks. In these ploys, scammers sent long emails describing the plight of a long lost relative in Nigeria, and the sender's efforts to unlock untold riches from an inheritance or other large pool of money.

The recipient was promised generous compensation if they could just wire some money to help the sender overcome an impediment to gaining access to the funds. Initially, requests would be for a few hundred dollars, but further obstacles would inevitably arise, with the scammers coaxing more money from victims for as long as they could string them along.

Among West African email rings, a "falling mugu" mindset began to emerge, driven by the notion that if someone can be "tricked," or made to fall "fool" to deceptions, whatever money could be extracted from them was justifiable. With victims thousands of miles away, it was easy to ignore the financial and emotional toll stemming from their scams.

Fast forward to today. BEC is now responsible for 40% of all cybercrime losses—more than $26 billion in losses[1] since June 2016—and has victimized organizations in at least 177 countries[2]. The success of these attacks has led to a continuing stream of new "flavors" of BEC, including Vendor Email Compromise (VEC), committed by cybercriminal organizations like Silent Starling.

Because of the impact of BEC attacks globally, law enforcement in Nigeria has become more aggressive in recent years, which has caused BEC actors to migrate to other countries. Additionally, the significant return on investment from BEC scams has led far more sophisticated Eastern European cybercrime groups, like Cosmic Lynx, to get into the game. This only increases the geographic distribution of BEC attack sources.

Footnotes:

1. https://www.ic3.gov/media/2019/190910.aspx 2. https://www.ic3.gov/media/2019/190910.aspx

A Global Menace

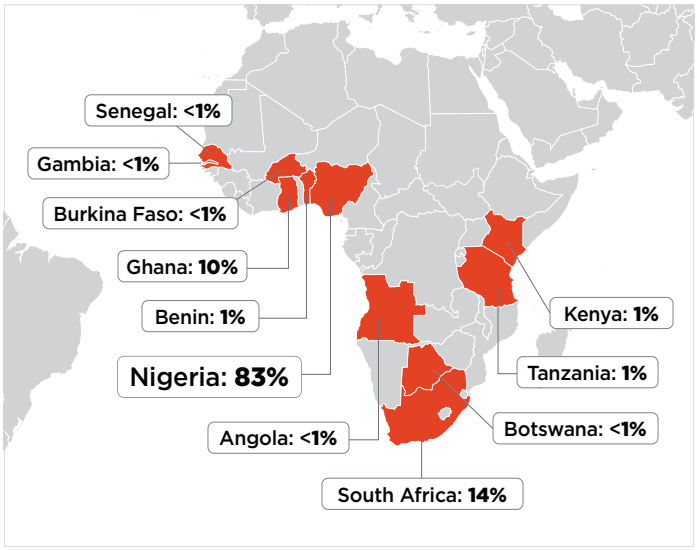
The Locations of BEC Actors Around the World

Of the more than 9,000 active defense engagements we conducted between May 2019 and July 2020, we were able to identify the likely location of the attacker in more than 2,200 cases. These locations do not include engagements where the attacker was likely using a proxy or other methods to anonymize their whereabouts. Our analysis of these locations showed that BEC attackers came from 50 different countries around the globe, demonstrating that these bad actors are not just limited to a small area of the world.

Global locations of BEC threat actors.

Based on our analysis, an unsurprising majority (60 percent) of BEC actors were located in 11 countries in Africa. Eighty-three percent of African attackers, as well as 50% of global BEC actors, hailed from Nigeria. Given the stereotype that BEC attacks overwhelmingly originate from Nigeria, this 50% figure may come as a surprise to some. Yet while the number of BEC threat actors located in Nigeria is far greater than any other country, it is by no means the only base of operations for these scammers.

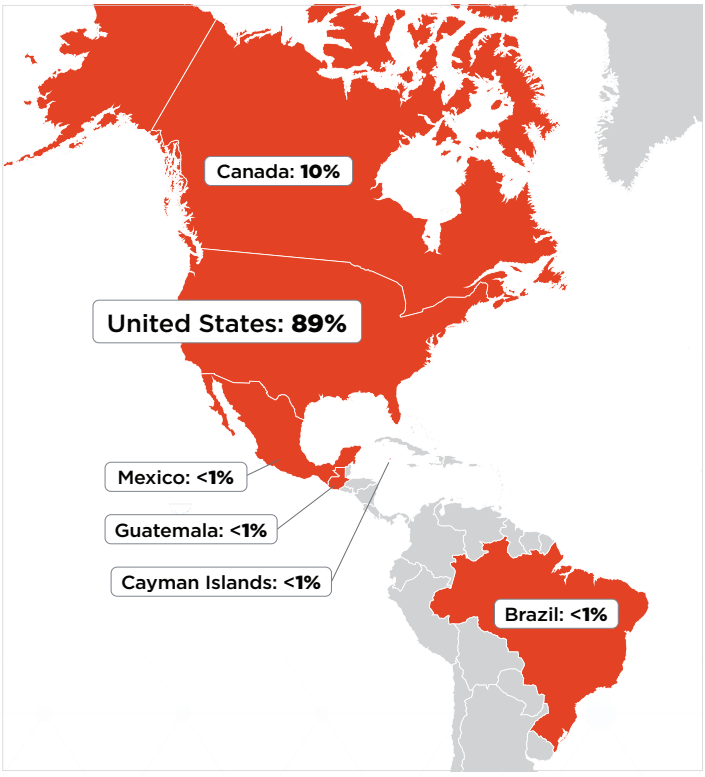
South Africa was home to 14% of the African threat actors observed in our dataset, and was the third-biggest outpost for BEC groups worldwide, representing 9% of the global total. Like Nigeria, South Africa has long been associated with various types of fraudulent activity, but on a smaller scale. Interestingly, South Africa is the only country to see a notable decrease in BEC threat actors during our study. In the last eight months of 2019, 11% of global BEC actors were located in South Africa, but in the first seven months of 2020, this number decreased to just 6%.



BEC actors in Africa.
(Percentages associated with regional distribution.)

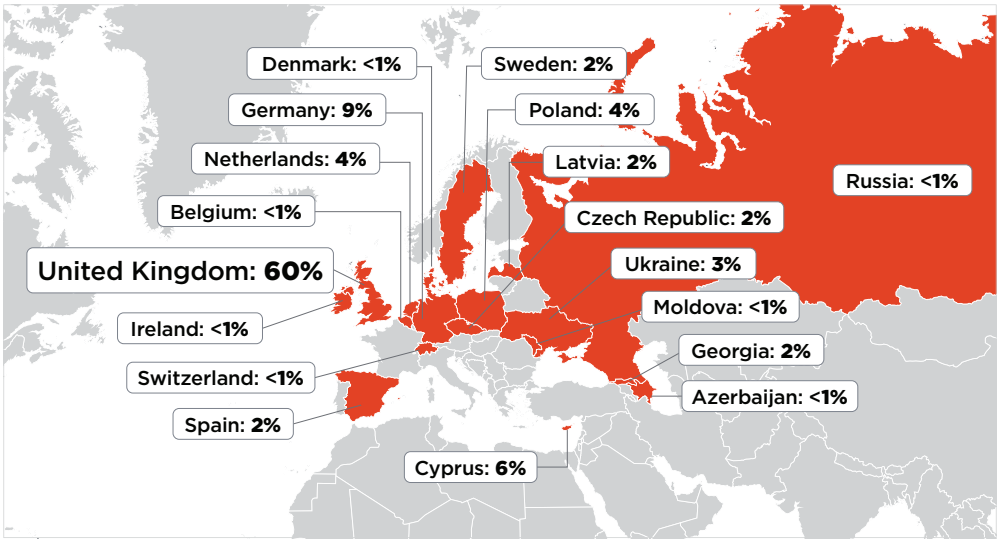
Second only to Africa, 28% of BEC attackers we identified were based in the Americas. While actors were identified throughout North America, Central America, South America, and the Carribean, a disproportionate number of these actors were located in the United States and Canada (10 percent).

The largest source of BEC actors in the Americas was the United States, which was associated with 89% of attackers in the Americas and 25% of threat actors globally. It's well-known that organizations within the United States are preferred targets for BEC actors. Some groups our team has researched, such as Exaggerated Lion, have exclusively targeted US-based businesses, for instance. But it may be surprising to some that a quarter of all BEC actors operate from within the US.



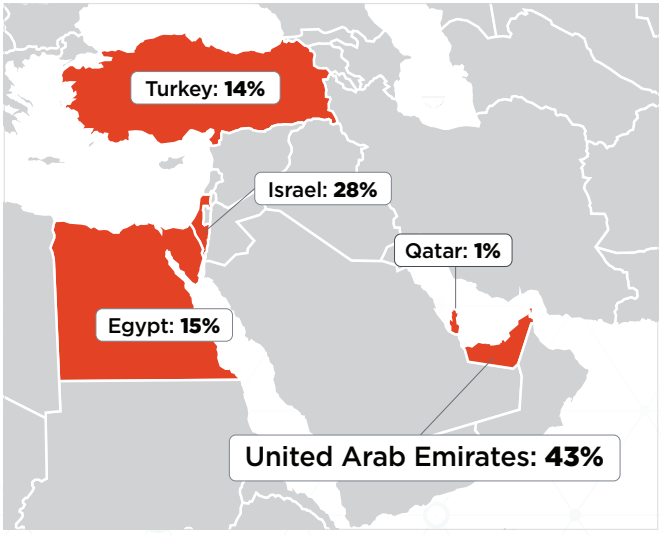
BEC actors in the Americas.

Eighteen countries in Europe were linked to 6% of BEC attackers. The United Kingdom was home to 60% of all European BEC actors, the highest in the region and fourth-highest globally. This includes outfits like London Blue, a cybercriminal organization that gave us insight into the operational structure and targeting strategies of BEC groups. After the UK, the countries with the highest number of BEC actors in Europe are Germany, Cyprus, Poland, and the Netherlands.



BEC actors in Europe.

The Middle East was the home base for 4% of BEC threat actors in our dataset, with the United Arab Emirates being the top source of actors in the region, followed by Israel, Egypt, and Turkey. Dubai in particular has become an emerging hot spot for displaced Nigerian scammers. In June 2020, Ramon Olorunwa Abbas (a.k.a. "Hushpuppi"), a prolific Nigerian fraudster, was arrested in Dubai and extradited to the United States for his alleged role in BEC attacks involving hundreds of millions of dollars filched from companies in the US and Europe[3].

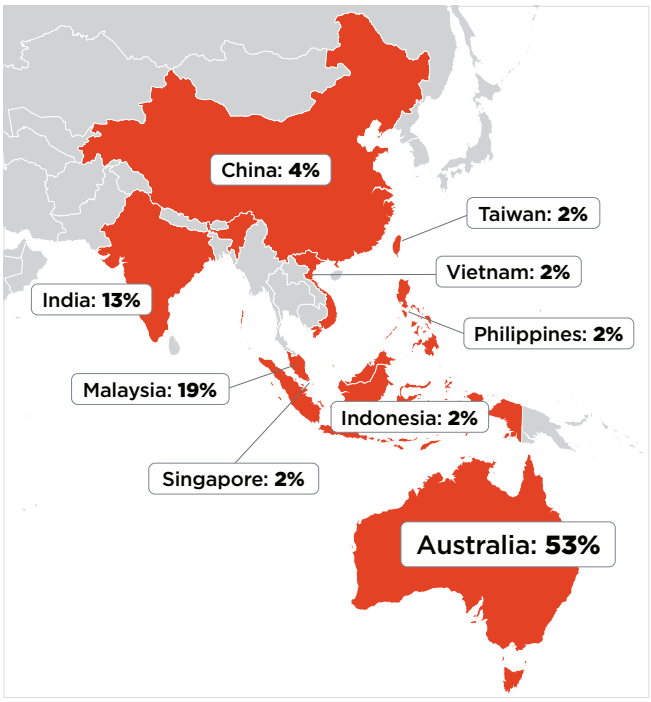


BEC actors in the Middle East.

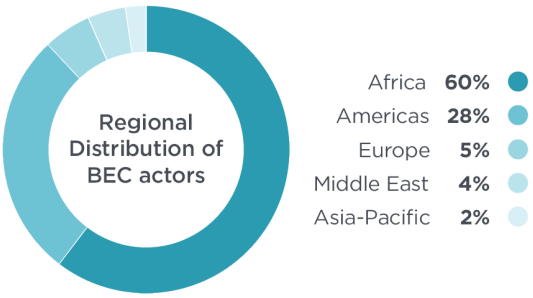
Footnotes:

3. https://www.justice.gov/usao-cdca/pr/nigerian-national-brought-us-face-charges-conspiring-launder-hundreds-millions-dollars

While some APAC nations like Hong Kong have been popular havens for BEC scammers' mule accounts, the region is home turf to the fewest number of BEC actors. Only 2% of the world's BEC attackers operate here, and are distributed across 10 countries. Australia leads the way, with just over half of the malicious actors in the region, followed by Malaysia, India, and China.



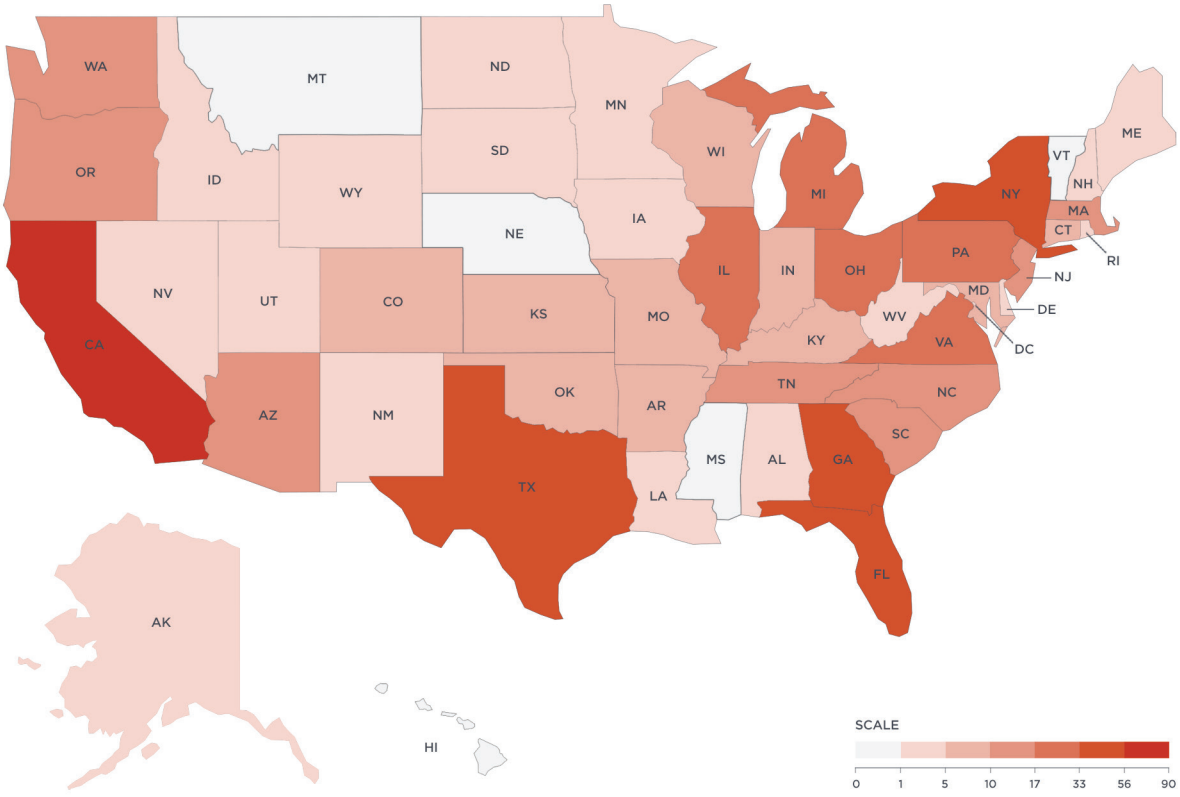
BEC actors in the Asia-Pacific region.



BEC in the USA

The Hidden Threat in Our Backyard

While it's true that a vast majority of BEC attacks are launched from Nigeria, it's worth taking a closer look at the rising number of actors located right here in the United States. A quarter of the BEC actors we identified globally were located in the US, operating in 45 states and the District of Columbia. Nearly half these scammers were located in five states: California, Georgia, Florida, Texas, and New York.



Distribution of BEC actors per state.

Many of the BEC actors in our dataset were clustered around a handful of US cities. The largest of these were based in and around Atlanta, GA, with 7% of all US-based BEC actors operating in this metropolitan area. In March 2020, two dozen individuals were arrested for their involvement in a large-scale fraud operation that included BEC attacks, romance scams, and retirement scams[4]. Most of the individuals arrested in this takedown resided in or around Atlanta.

Footnotes:

4. https://www.justice.gov/usao-ndga/pr/dozens-charged-atlanta-based-money-laundering-operation-funneled-30-million-proceeds

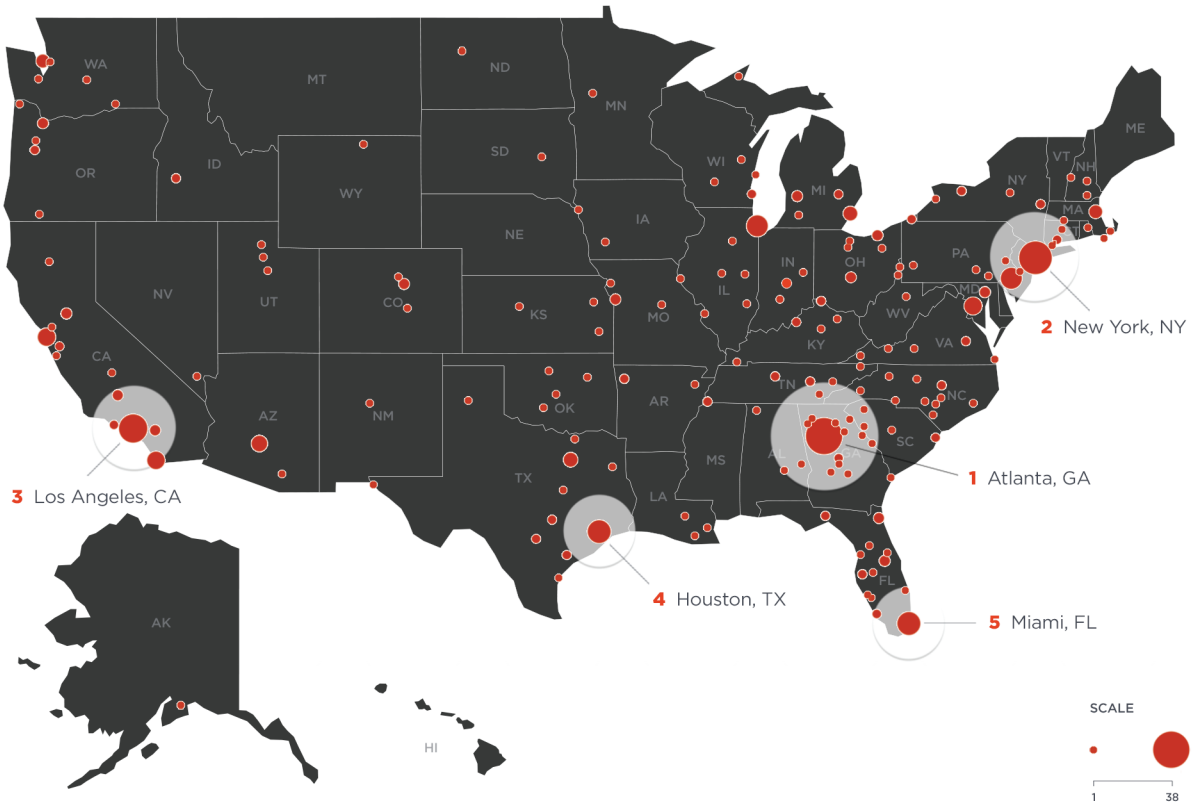
The next largest clusters of BEC actors in the US were around New York, NY; Los Angeles, CA; Houston, TX; and Miami, FL. Nearly a quarter of all US-based BEC attackers were located in these five metropolitan areas. Rounding out the top-10 were Philadelphia, PA; Chicago, IL; San Diego, CA; San Francisco, CA; and Phoenix, AZ. Historical BEC arrests in the US show many of them center around these 10 cities, including Operation reWired[5], a major international law enforcement operation, with 281 arrests of BEC actors worldwide, including 74 in the US.

1	California	15%
2	Georgia	10%
3	Florida	9%
4	Texas	8%
5	New York	6%
6	Pennsylvania	4%
7	Illinois	4%
8	Michigan	4%
9	Ohio	3%
10	Virginia	3%

Top 10 states for BEC actors.

1	Atlanta, GA	7%
2	New York, NY	6%
3	Los Angeles, CA	5%
4	Houston, TX	3%
5	Miami, FL	3%
6	Philadelphia, PA	3%
7	Chicago, IL	3%
8	San Diego, CA	2%
9	San Francisco, CA	2%
10	Phoenix, AZ	2%

Top 10 metro areas for BEC actors.



Locations of BEC actors in the United States.

Footnotes:

5. https://www.justice.gov/opa/pr/281-arrested-worldwide-coordinated-international-enforcement-operation-targeting-hundreds

The BEC Linchpin

How Money Mules are Used in BEC Attacks

When it comes to Business Email Compromise and other related crimes, money mules are the cornerstone and critical infrastructure for successful operations. Without money mules, BEC and related crimes would look and function very differently than how they do today.

Money mules exist in two forms: witting and unwitting. For witting mules, they are fully aware of the legality of their actions, understanding that what they are doing is a crime. In order to help a group steal money, many Nigerians move abroad for the sole purpose of opening businesses or bank accounts to be used in laundering the proceeds from email scams.

On the opposite end of the spectrum, unwitting mules don't have full-scope visibility into the operations of a scam. Unwitting mules are generally socially engineered to commit fraud on behalf of the scammers. These mules are used to perform a variety of different tasks for scammers, including setting up bank accounts, receiving fraudulent payments from BEC victims, printing and sending fraudulent checks, or receiving and reshipping goods. To many unwitting mules, they may have some level of suspicion that the requested task is strange or suspicious; however, they continue to participate in the scheme due to the level of trust that has been built with their handler.

A main source of unwitting mules for BEC actors comes from romance scam victims. Scattered Canary, a prolific Nigerian fraud ring, almost exclusively used a network of romance scam victims to receive stolen funds from BEC attacks. In many cases, these victims are groomed by scammers for months or years, building a solid foundation of trust with the victim. During this time, the scammer will usually con a romance victim out of the money they have and once that well has run dry, the scammer will convert the victim into a money mule to continue victimizing them. Of course, scammers don't come right out and tell a romance scam victim, "Help me steal money." Instead, they convince a romance victim to send them money for another more benign purpose. For example, Exaggerated Lion told romance victims that they needed help receiving a large inheritance that was tied up with lawyers and was being distributed slowly over time.

Another method BEC scammers use to recruit unwitting mules is through work-from-home scams. In these scams, victims respond to what looks to be a legitimate job posting and are "hired" by the scammer. In many cases, these victims go through a formal interview process while the scammers vet their targets. After a victim accepts the "job," they are put to work doing a variety of different tasks, which could include receiving and reshipping goods, receiving "payments" from clients, or printing and sending checks. Of course these tasks are all part of fraudulent schemes the victim is unknowingly a part of. Work-from-home scams have become much more popular this year as the COVID-19 pandemic has caused a significant increase in unemployment,[6] providing scammers with ample resources to capture and move funds as needed. Given the success of recruitment efforts, there are few indications the availability of mules will be constrained anytime soon.

Footnotes:

6. https://www.nytimes.com/2020/09/15/technology/money-mules-fraud-pandemic.html

Dirty Money, Global Networks

The Worldwide Distribution of BEC Money Mules

It is interesting to take a look at the way BEC groups deposit and transfer funds from their scams, as this can often influence the tactics deployed. In our analysis, we discovered some notable trends that again track along geographies.

Because BEC is a global crime, BEC actors need to maintain a cache of money mules in countries around the world. Most of the time, scammers use mules based in the same country as their target to avoid raising suspicions. However, some BEC attackers provide mule accounts in another country for an "international payment." A great example of this is the emergence of Hong Kong as a common destination for these international fraudulent payments.

Between May 2019 and July 2020, we collected more than 2,900 mule accounts from our active defense engagements. In total, more than $64 million was requested to be sent to these mule accounts, located in 39 countries around the world. Eighty percent of the mule accounts we collected were located in the United States, followed by the United Kingdom, Hong Kong, Canada, and Australia.

While we found most mule accounts at US-based banks, the payments requested to be sent to those accounts were significantly lower than other countries. For example, the average amount requested by scammers in BEC attacks where payments are heading to US-based accounts was $39,500, while payments requested to mule accounts based in Hong Kong were $257,300—more than six times higher. In fact, of the top five countries where we saw mule accounts located, only Canada had a lower average requested payment.

Australia	**$45,500**
Canada	**$35,500**
Hong Kong	**$257,300**
United Kingdom	**$46,400**
United States	**$39,500**

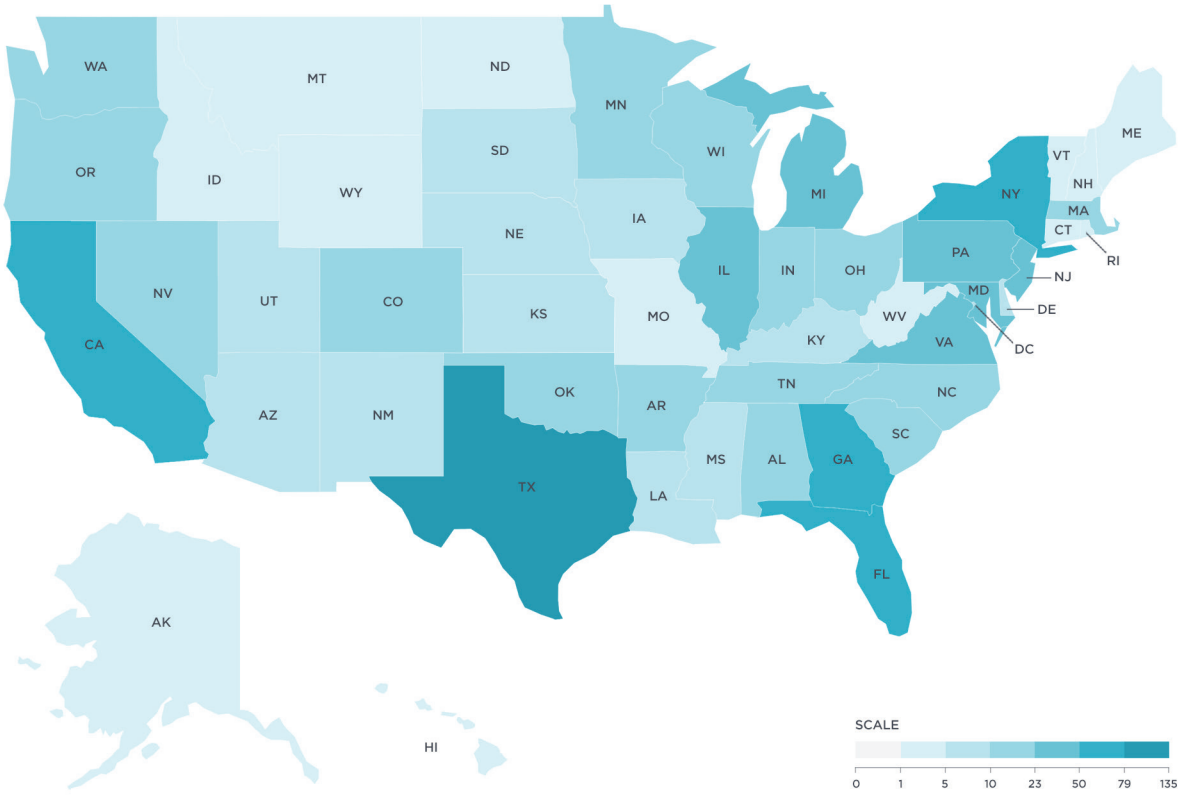
Average BEC payment requests. (US$)

Global locations of BEC money mules.

America's Money Mules

The First Link in the BEC Financial Supply Chain

Within the United States, we identified more than 900 money mules used in BEC scams between May 2019 and July 2020. Demonstrating the point that money mules can be located anywhere, at least one mule was found in every state and the District of Columbia. Many of these individuals are likely to be unwitting victims of romance scams or work-from-home cons. Looking at the parts of the country where mules are clustered, though, provides some interesting insights.



Distribution of BEC money mules per state.

The most common states where US-based mules were located were Texas, California, Georgia, Florida, and New York. These are the same five states that had the highest number of US-based BEC actors, indicating that these states may be hubs of BEC activity in the United States where potential witting mules are located. Texas alone comprised 16% of all mules identified in the US, nearly double California's total.

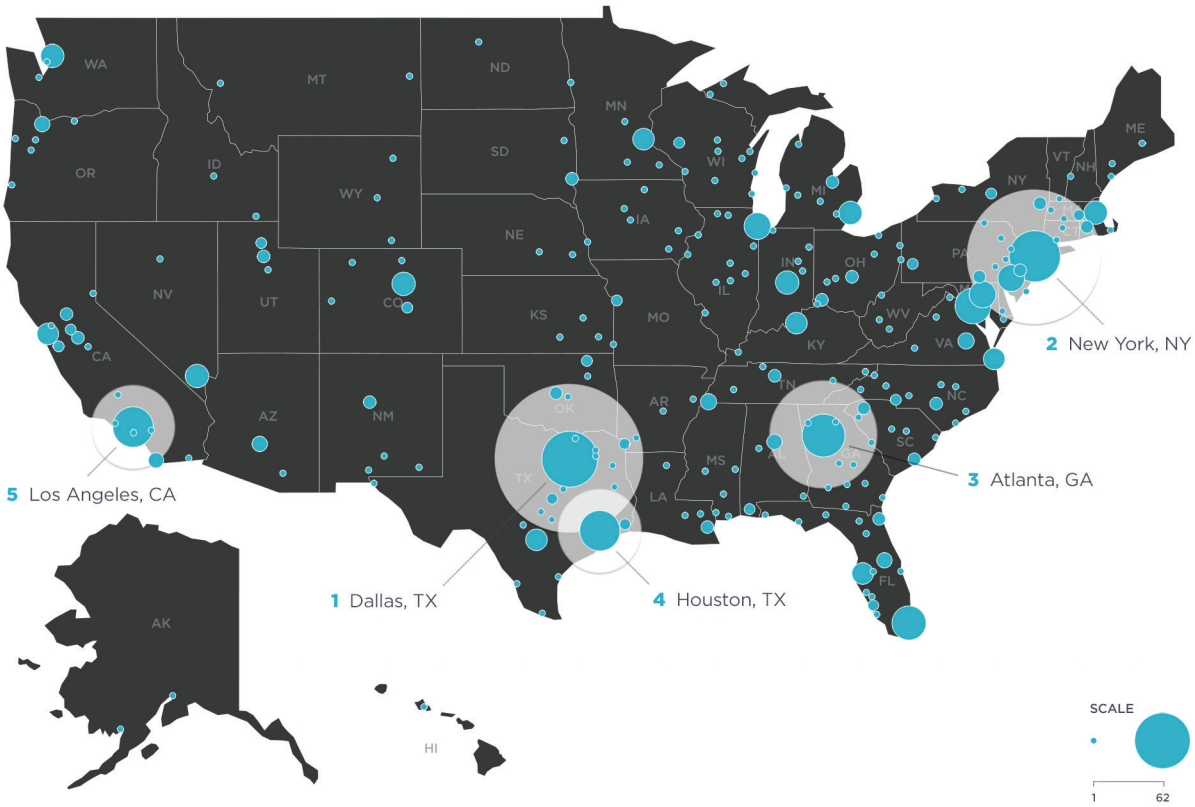
A quarter of US-based mules were clustered in and around four cities: Dallas, TX; New York, NY; Atlanta, GA; and Houston, TX. Interestingly, Dallas, the metropolitan area with the highest number of mules in the US, was not even in the top 10 cities where BEC attackers could be found. Completing the top 10 US metropolitan areas where mules were identified were Los Angeles, CA; Washington, DC; Miami, FL; Baltimore, MD; Chicago, IL; and Philadelphia, PA.

1	Texas	16%
2	California	9%
3	Georgia	7%
4	Florida	7%
5	New York	6%
6	Maryland	4%
7	Pennsylvania	3%
8	Virginia	3%
9	Illinois	3%
10	New Jersey	3%

Top 10 states for BEC money mules.

1	Dallas, TX	7%
2	New York, NY	7%
3	Atlanta, GA	5%
4	Houston, TX	5%
5	Los Angeles, CA	4%
6	Washington, DC	3%
7	Miami, FL	3%
8	Baltimore, MD	2%
9	Chicago, IL	2%
10	Philadelphia, PA	2%

Top 10 metro areas for BEC money mules.



Locations of money mules in the United States.

Conclusion

Historically, BEC and other types of social engineering schemes have had their roots in Nigeria. In recent years, however, pressure from law enforcement has spurred an exodus of some BEC actors out of Nigeria to other countries. Additionally, cybercriminals around the world have recognized the significant ROI in BEC attacks, and have started vying for a piece of the action. BEC actors can now be found in 50 countries, and while half of these actors still have a home base in Nigeria, the geographical distribution of these threat actors is much higher than was just a few years ago. This signals that cybercriminal organizations are healthy, growing, becoming more diversified, and showing little signs of weakness.

Money mules, the central cogs that make BEC attacks so successful, are also geographically dispersed and located in commercial hubs situated for convenience and efficiency. While we have identified mules in 39 countries, the fact that BEC attacks have targeted organizations in at least 177 countries means this is likely just the tip of the iceberg.

While the United States has been a primary target of BEC attacks, it is also home to a significant number of BEC actors. Our analysis shows that a handful of cities, such as Atlanta, Houston, New York, and Los Angeles, may be the main hubs for BEC activity in the US. Meanwhile, the money mules these fraudsters rely on can be found in every US state. And while many of these mules are likely unwitting accomplices, there are clear clusters of potentially complicit mules around some cities, most of which overlap with clusters of US-based BEC actors.

AGARI CYBER
INTELLIGENCE DIVISION

About Fortra's Agari Cyber Intelligence Division

Agari Cyber Intelligence Division (ACID) is the world's only counterintelligence research group dedicated to business email compromise (BEC) investigation and cybercrime abatement. ACID has conducted more than 12,000 active defense engagements with threat actors since May 2019. ACID works closely with CISOs at global enterprises, law enforcement, and other trusted partners to stop identity-based phishing and socially-engineered cybercrimes.

Learn more at acid.agari.com

fta-ag-gd-0922-r1-79d