



AGARI CYBER  
INTELLIGENCE DIVISION

REPORT

# Behind the “From” Lines: Email Fraud on a Global Scale

Ten Cybercriminal Organizations Unmasked

# Executive Summary

## Nigerian Scammers Target American Businesses

Over the course of the past 10 months, using responsible active defense techniques, Agari captured 78 criminal email accounts, belonging to 10 criminal organizations, and containing 59,652 unique email messages. Agari analyzed the contents of these email accounts to investigate the tactics, targets and identities of the criminals. And now, that analysis enables stronger defensive strategies and measures.

What's more, Agari has used this analysis to warn financial institutions about accounts being used for criminal activity, and to provide evidence to law enforcement. Agari has also warned victims, and in at least once case, quick action helped a company recover its money.

One of the more interesting findings from this analysis was that while much of the high-profile cybersecurity news of the past year has involved state sponsors like Russia and North Korea, American businesses and individuals are far more likely to be targeted by Nigerian scam artists.

Nigerian scam artists, traditionally associated with implausible get-rich-quick schemes and other scams of individuals, have become more sophisticated and a significant threat to American businesses. The groups Agari captured began ramping up their business email compromise (BEC) attacks between 2016 and 2018. They have targeted the largest corporations, small businesses, real estate agents, and even hospice care providers with sophisticated, commercially purchased malware.

By compromising these organizations with malware, these criminals can misdirect down payments on homes to steal the life savings of victims, send fake invoices to real customers, reroute product deliveries to false locations to be stolen, and steal sensitive information to target even more victims. By the time the victims realize they have been scammed, their money is long gone.

Even as they move into more sophisticated attacks against businesses, these criminal groups continue duping individuals through rental scams (which yield lucrative revenue) and fraudulent romance (which yields new money mules, in addition to revenue). Among these victims, we found two women who had been bilked out of a half million dollars each. One of them lost her home and was forced to pull her children out of school, while the other appears to have become a knowing accomplice to an online lover who was never real.

"Since I can't send more money, maybe I'm of no use to you now. I certainly feel like that could be the deal here...A realtor is coming over tomorrow to help me list my house for sale. I'm talking to an attorney now about how to keep the collection agencies away and protect my kids. All this time, I'm wondering if I've heard from you for the last time. Please don't let that be the case."

**Romance scam victim, email to her attacker.**

# Table of Contents

Introduction	4
Key Findings	5
Background: Nigerian Princes Really Are From Nigeria	6
Attack Trends: The Business of Email Compromise	14
Criminal Gains: At What Cost?	30
Conclusion: Addressing a Future of Criminal Automation	34

# Introduction

**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.**

Through social engineering, cybercriminals are completely bypassing traditional perimeter defenses. There's no malware to detect, nothing suspicious in the code, nothing unfamiliar in the message—it's just that the person on the other end of the email isn't who they claim to be.

The 2018 Verizon Data Breach Incident Report recognizes that “we're only human” when it comes to social engineering. But this human weakness results in the single most common and costly form of cyberattack. According to Verizon, “phishing and pretexting represent 98% of social incidents and 93% of breaches. Email continues to be the most common vector (96%).” And the FBI reports that BEC has resulted in exposed losses of more than \$5 billion.

It's ironic—and problematic—that many of these attacks are using our own infrastructure against us. Cloud-based email services have commoditized basic email security, but they also offer a low barrier to entry for criminal organizations that want to create dozens of fraudulent accounts to impersonate otherwise trusted identities. Generally, it is more difficult to detect these attacks because they are launched from legitimate infrastructures that traditional security controls have been taught to trust.

Not only are the rewards high for these crimes, the risks are low. These international operations face little consequence in the U.S. for the crimes they commit overseas. However, just like the drug trade, many of these operations make use of U.S.-based mules to aid and abet them. The average U.S. company may be suspicious about wiring money to a Nigerian bank account, but when the bank is in the U.S. (thanks to a mule) it is less likely to raise a red flag.

In short, these criminals have used identity deception and trusted infrastructures to circumvent traditional security. But there is a solution. Thanks to recent advanced in AI-powered defense systems, we can change the equation, turn the tables and fight back against the epidemic of BEC and identity deception—and we must.

This report fills critical gaps in our awareness of these attacks, provides direct insight into the organizations and individuals committing these crimes, and demonstrates the value of proactive protection against identity deception. With this new insight, it is our goal to foster better cooperation and information sharing between law enforcement, the security industry and the organizations they each serve to protect.

# Key Findings

**Despite billions of dollars of investment and major advances in sophisticated security technology, the vast majority of businesses remain utterly vulnerable to BEC attacks, which use identity deception to impersonate a trusted contact.**

- Agari captured 76 criminal email accounts from 10 organized crime groups, containing 59,652 unique messages for analysis. The inception of the accounts ranged from 2009 to 2017.
- Nine out of 10 organized crime groups were based in Nigeria. In many instances, we have been able to identify the real identity of the criminal email accounts because of poor operational security of the organized crime groups.
- After focusing for years on simple romance and rental scams, most of the groups began conducting BEC attacks between 2016 and 2018.
- Most organized crime groups focused on romance scams until the advent of BEC attacks.
- BEC was the most popular attack vector (24% of all attacks, over the life of the accounts), a remarkable finding considering that most of these groups did not begin BEC attacks until 2016 or later.
- BEC attacks require little effort for high reward:
  - The average BEC attack is active for less than three days (a very quick attack), whereas the average romance scam is active for 25 days.
  - BEC has the highest success rate of the tracked attacks, with 0.37 victims per 100 probes. BEC attacks are 10 times more successful if the victim answers an initial probe (3.97 victims per 100 answered probes).
  - The average payment requested across all BEC attacks was \$35,500.
  - BEC attacks have an expected profit of between \$982 to \$5,236 per answered probe, based on previously available FBI IC3 report statistics, making it at least 700 percent more lucrative than a romance scam.
- Agari found man-in-the-middle real estate purchase scams that trick home buyers into wiring their savings to criminals. We also saw a similar attack technique used to compromise a hospice organization.
- Scammers are targeting SMBs and major enterprises, intercepting their invoice payments and directing equipment deliveries to drop sites.
- Organized crime groups make use of legitimate infrastructure and online tools to evade detection and support their operation.
  - Gmail accounts are commonly used for email service.
  - Grammarly is used to correct spelling and punctuation errors.
  - RocketReach and GuideStar are used to find business listings.
  - Match.com and other dating sites are commonly used to target romance scam victims, many of whom become money laundering mules.

## \$35,500

is the average payment requested across BEC attacks

## 3.97%

of people that answer a BEC email become victims

## 24%

of all email scams are BEC

# Background: Nigerian Princes Really Are From Nigeria

**In this section, we will focus on understanding the modus operandi of the perpetrators behind these attacks at both a macro and micro view.**

During the course of our research, Agari identified 78 criminal email accounts from 10 organized crime groups. And this is just the tip of the iceberg. In addition to the 78 criminal email accounts identified by Agari, we have observed communication with 188 more criminal email accounts.

Our researchers were able to access for additional analysis a total of 59,652 messages from the inbox, sent and spam message folders of these criminal email accounts. These messages included communication among members within these organized crime groups, enabling our researchers to correlate their relationships. Our researchers were also able to further assign identity and location because the criminal email accounts were used for personal services, including Facebook and Uber.

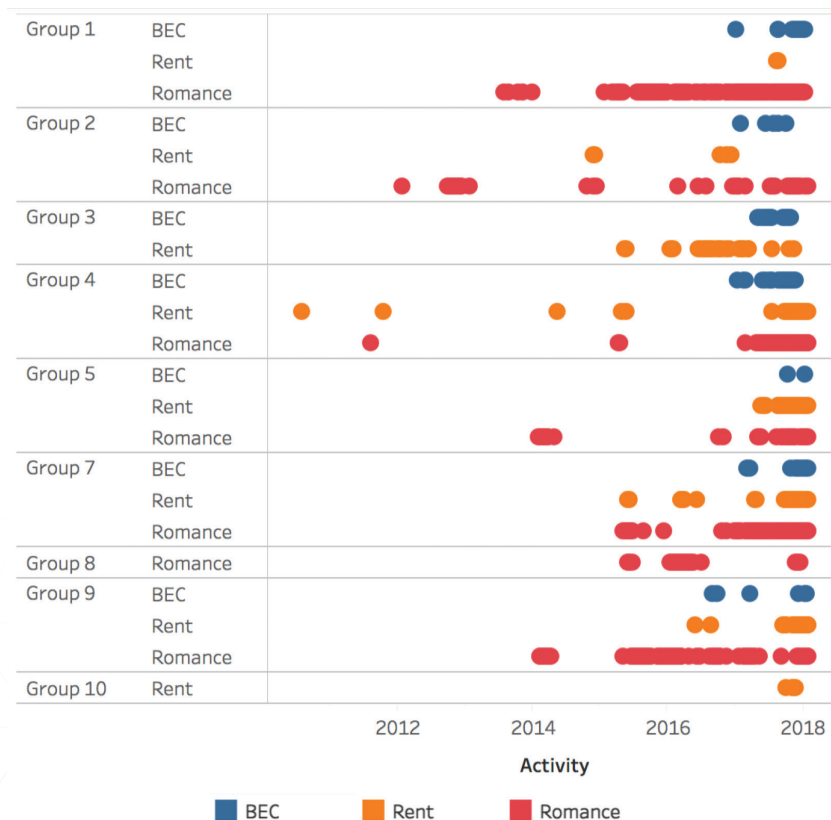
## No Representation Without Taxonomy

Previously, Agari has developed a comprehensive Threat Taxonomy that categorizes and classifies security threats, including email attacks, in a way that makes them easier to understand, anticipate and counter. In this report, we have assigned a similar taxonomy to these organized crime groups.

To create a meaningful characterization of these organizations, an important first step is to identify what is worth measuring. Based on the analysis of the criminal email accounts that Agari has captured, and relative to email-based social engineering crime, we have created the following taxonomy of criminal organizations:

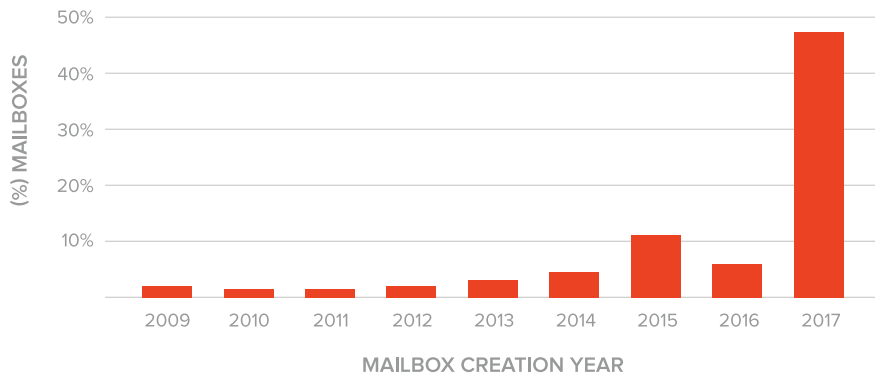
- 1 What?** This dimension highlights the attack vectors that organized crime groups use. We will be covering these attacks in-depth in section two of this report. However, we can briefly state that among the criminal email accounts captured by Agari, BEC was the most common attack vector, corresponding to a quarter of the fraud attempts.
- 2 Where?** Agari determined the location of the criminals, both in terms of their apparent headquarters and in terms of the location of their affiliates. All of the captured criminal email accounts appeared to be headquartered in Africa, and nine out of ten in Nigeria (with the remainder in Kenya). Each of these organized crime groups have confirmed affiliates in either the United States, the European Union, or both. We will further explore this attribution in this section.

- 4 Activity.** The activity descriptor addresses the age of the organization, the volume of criminal attempts, and historical behavior. The average age of the captured criminal email accounts was roughly four and a half years, with the oldest one being ten years old. The volume of attacks was very uneven, with one organized crime group essentially generating the same volume as the remaining nine organizations. In terms of the history, one organization started performing BEC attacks in earnest in 2016 and one in 2018, with all the others starting in 2017. All but one of the organizations started out performing romance scams, and then turned to business email compromise.
- 5 Operations.** We break down the operations of these organized crime groups into operational security, their criminal approach and potential innovation. Proxies and VPNs are popular services among these organized crime groups because they can help hide their true location. Business contact services, such as RocketReach, Crunchbase and GuideStar are popular for their ability to identify targets. Even Grammarly has its place, as it helps the organized crime groups write more effective communications. Our researchers have also identified instances of underground tools and services, such as custom-made malware. We will further explore criminal approach and potential innovation in the next section.
- 6 Impact.** Finally, the impact category describes how these organized crime groups profit. How many confirmed successes did the criminal organizations enjoy, what types of crimes did they correspond to, and what are the estimated gains? We will explore this in more detail in section three of the report. However, we can briefly mention that BEC is the most effective attack vector and attacks are 10 times more likely to succeed when the victim answers an initial probe message, such as “Are you available to make a payment?”



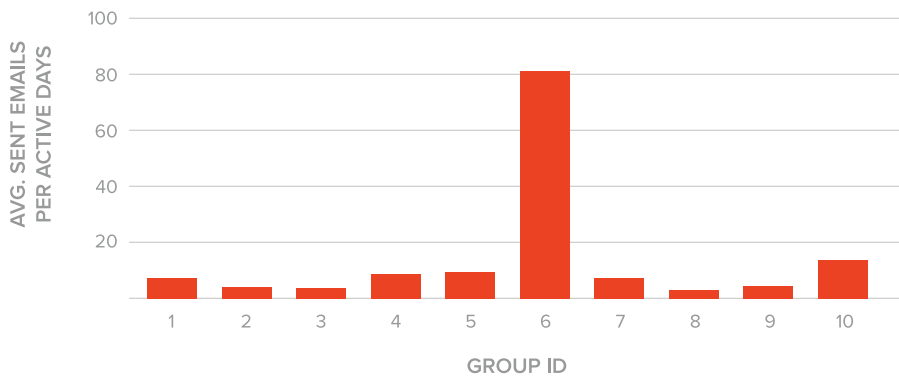
**Figure 1: Development of Major Scam Types within Organized Crime Groups.**

Nearly every organized crime group began with romance scams before turning to business email compromise (BEC) in 2016 or later.



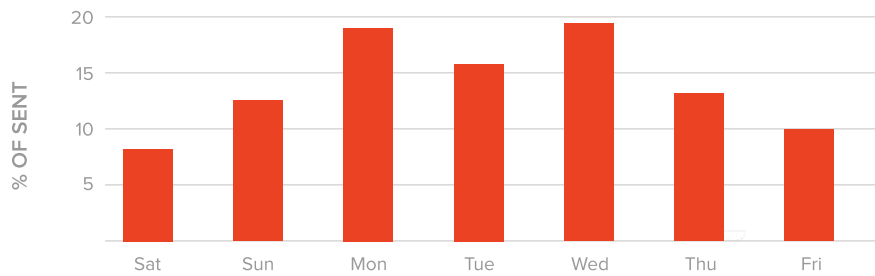
**Figure 2: Origin of Mailbox Creation Year.**

The average age of the captured criminal email accounts was roughly four and a half years, with the oldest one being ten years old.



**Figure 3: Average Sent Emails Per Active Day.**

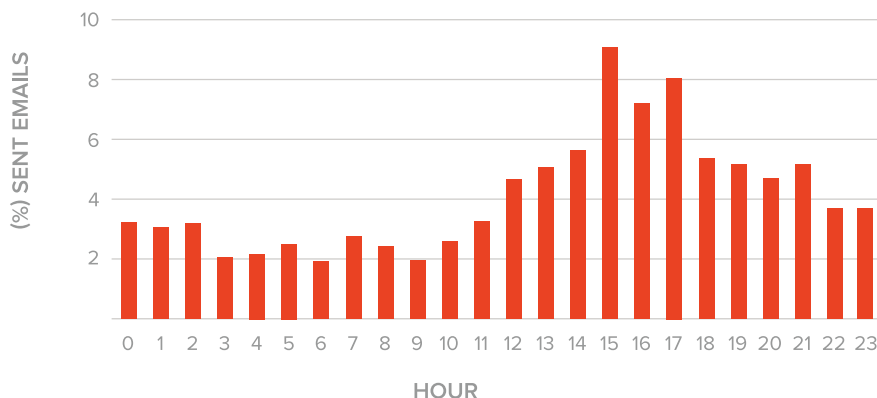
Group Six was the most prolific, sending an average of 81 emails per day during active days



**Figure 4: Distribution of Daily Mailbox Activity.**

Even organized crime groups are working for the weekend; attacks spike at the beginning of the week and taper off by the weekend.





**Figure 5: Distribution of Hourly Mailbox Activity (UTC +1 West Africa).**

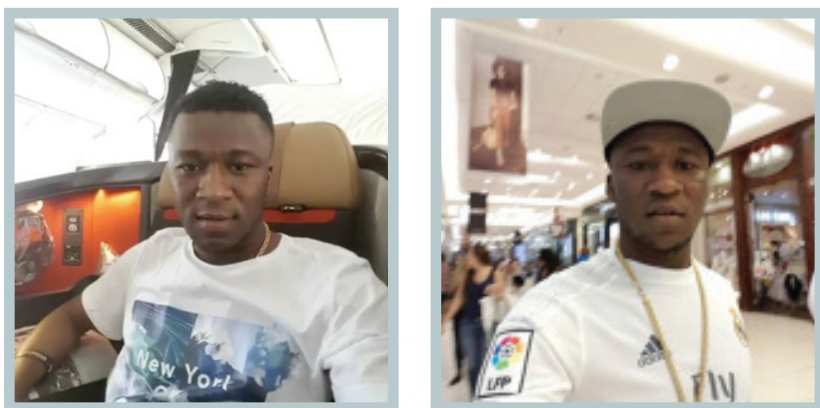
These organized crime groups were most active between 11am - 8pm UTC +1 (West Africa), which coincides with American business hours, 7am - 4pm Eastern.

## Unmasking the Impostors

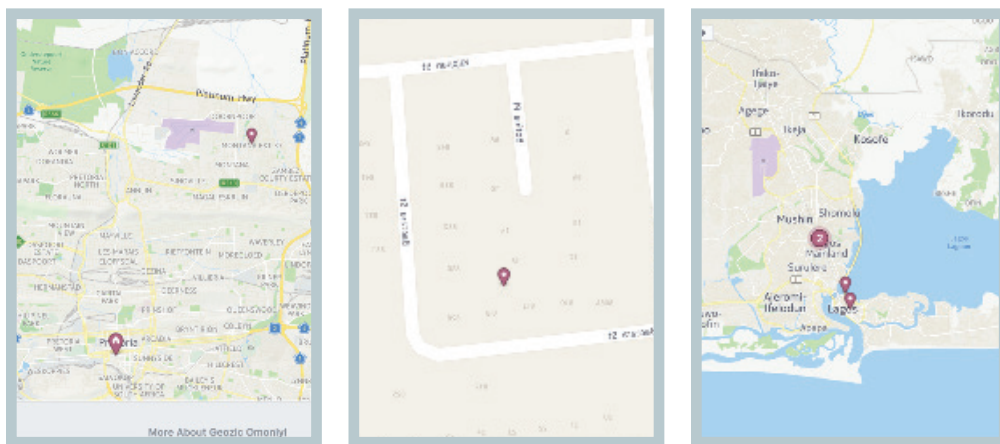
### A One-Man Wolfpack

We can trace the origins of Group One to 2013, when it was focused entirely on romance scams. Our researchers have correlated a primary email account from Group One with two other frequently used email addresses, a male and female alias used in romance scams. Our hypothesis is that Group One may be a single individual managing multiple criminal email accounts. The remainder of the criminal email accounts in Group One are a variation of the same email address, a technique used to circumvent rate limiting on sending email. Among these accounts, we have discovered a plethora of captured email account usernames and passwords, which were stolen using a script created by a third-party actor with the alias “Anthrax.”

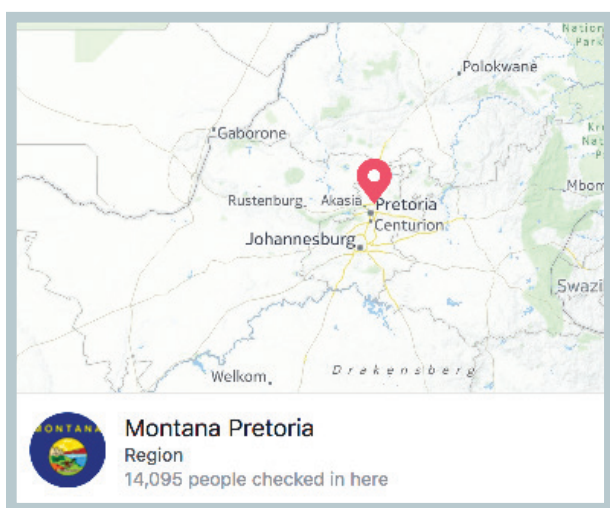
Agari first detected Group One in August 2017 when we intercepted a BEC email to the Chief Accounting Officer of a customer protected by Agari Phishing Defense™. The email used display name deception to make it appear that it was sent by the company’s CEO. This was the start of an attempted BEC scam. We will focus more on Group One, as we unfurl a heartbreaking romance scam initiated by “Jim Blackie.”



**Figure 6:** Pictures of “Jim Blackie” flying first class and in a shopping mall obtained from Facebook accounts linked to the email address used in the romance and BEC scams



**Figure 7:** Facebook Check-ins of Jim Blackie placing him in Lagos, Nigeria.



**Figure 8:** Facebook Check-ins of Jim Blackie placing him in Pretoria, South Africa, which based on email communications may be his residence.

## Define “Ethical” Hacker

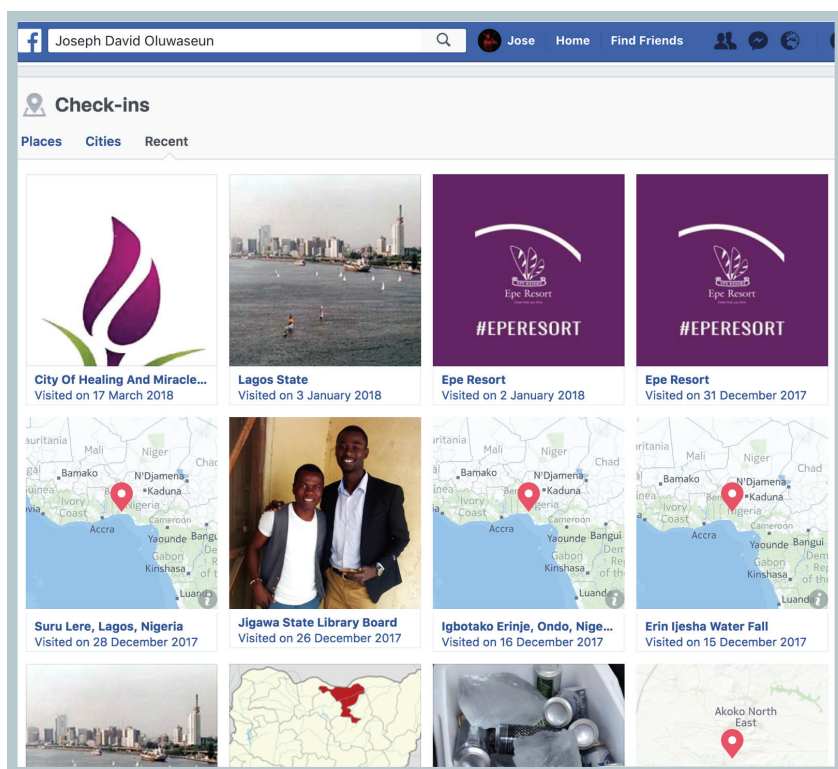
In the world of law enforcement, there’s a concept known as “felony stupid”—that is, an ingeniously orchestrated heist is spoiled when the criminal does something really dumb that leads the authorities right to them. In the analog world, one of the most stunning examples of “felony stupid” is when a perpetrator uses a legitimate personal credit card to rent the getaway vehicle. And the same concept holds true for cybercriminals, especially when criminals access personal services from their criminal email accounts.

Group Nine is particularly egregious in this regard, much to the delight of our researchers. We have been able to correlate a dozen email addresses to this organized crime group, including two that have associated social media profiles with them.

Our researchers have identified one of the attackers as Joseph David Oluwaseun. Oluwaseun describes himself as a graphic designer, brand manager, media strategist and cartoonist living in Dutse, Nigeria. He has also posted multiple public check-ins, which further validate his location in Nigeria.



**Figure 9:** Facebook Profile for Joseph David Oluwaseun.



**Figure 10:** Joseph David Oluwaseun Location Check-Ins.

We have also identified his partner as Abdulwahab Adebawale Ashimi. Ashimi is a self-described blogger, programmer, hacker and founder of SchoolDiary, an education blog. A Whols lookup of SchoolDiary reveals it was registered by the same criminal email account that was captured by Agari. Similarly, he has posted multiple public check-ins, which further validates his location in Nigeria. Ironically, Ashimi recently posted a Udemy Certificate of Completion for “The Definitive Ethical Hacking Course.”

This is just one example of what can be done to turn the tables on seemingly anonymous imposters and cybercriminals—and a great example of what becomes possible when AI-driven defense systems reveal tangible clues for human sleuths to work with.



**Figure 11:** Facebook Profile for Abdulwahab Adebowale Ashimi.



**Figure 12:** Udemy Certificate of Completion for “The Definitive Ethical Hacking Course.”

## A Master Conman, Hiding in Plain Sight

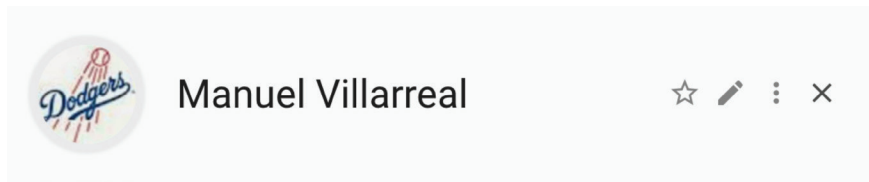
Among the more sophisticated and dangerous of the criminal email accounts we captured is “Master Comann.” Comann uses malware hidden in attachments to penetrate the email systems of real estate agents and other companies, positioning him to do real estate purchase scams and other man-in-the-middle BEC attacks. He also continues to conduct simple romance and rental scams, providing a flow of cash and new mule accounts.

These kinds of cons are not only financially devastating, but also heartbreaking to witness. While it is difficult to identify any one criminal email account as being the most callous, one of Master Comann’s exploits is a contender. He penetrated the email system of an association for hospice care facilities, which provide comfort to the terminally ill. The hospice center, with offices in North Carolina, is a non-profit supporting local hospice facilities and patients. We weren’t able to follow this exploit any further, but believe that once he has access to legitimate email accounts of hospices he could easily attack the families of hospice patients, who will be especially vulnerable at that time.

Master Comann, who appears to be based in Kenya, uses commercially-available malware creation tools that even provided him with tech support when he ran into difficulty. The malware is hard to detect and hard to remove. In November, Agari warned five real estate firms that their email was compromised. Two weeks later, their emails were still forwarding to Comann’s inbox, likely due to persistence of the malware used by Comann.

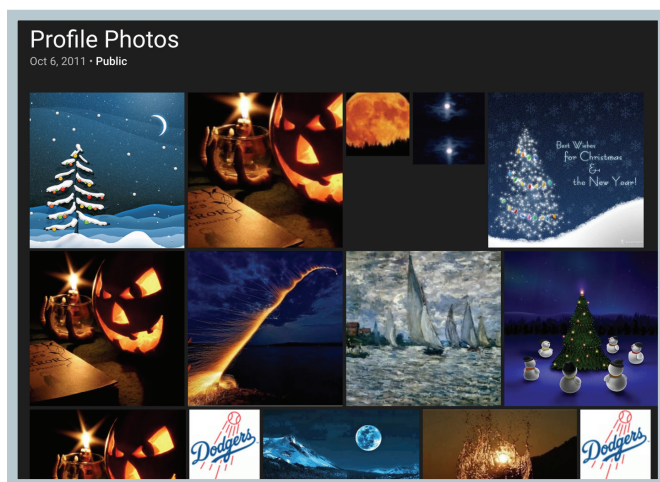


At some point, Master Comann created a Google+ page, featuring the name “Manuel Villarreal” and an L.A. Dodgers avatar.



**Figure 13:** Master Comann's Google+ Account, Registered to “Manuel Villarreal.”

Our researchers identified an additional “Manuel Villarreal” Google+ page with a similar email address to Master Comann (the second “N” was deleted), leading us to believe both addresses were operated by the same person. This secondary account included a link to a Picasaweb photo album with the same L.A. Dodgers avatar.



**Figure 14:** A Picasaweb photo album, presumably associated with Master Comann.

Our researchers were able to determine that this secondary email address was used to create Twitter and Facebook accounts, also with the name “Manuel Villarreal.” These accounts dated back to 2010 and use similarly abstract profile pictures. The majority of the Twitter posts were in Spanish, suggesting that Master Comann may not actually be from (or in) Kenya. Our researchers have strongly correlated evidence indicating that Master Comann is “Manuel Villarreal,” although it is possibly an alias or a stolen identity. If Master Comann truly is “Manuel Villarreal”, our evidence suggests that he is in the United States (perhaps using a VPN or proxy to throw researchers off his trail).

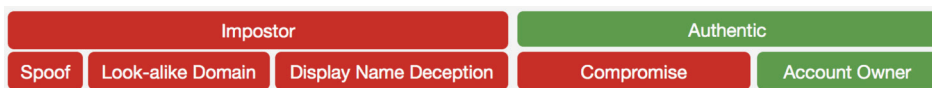
Details like this are instrumental in the work of law enforcement agents who track down, capture and prosecute perpetrators of identity-based crime.

# Attack Trends: The Business of Email Compromise

## Two Types of Trends

It is meaningful to consider trends on two different levels, the technical and the social. In this section we will discuss both, as well as provide some real-world conversations between captured criminal email accounts and their victims.

Technical trends explore the types of identity deception attacks these organized crime groups utilize to generate trust with their victims. Figure 15 below shows the different methods attackers use.



**Figure 15:** A Dimension of Agari's "Threat Taxonomy" Focused on Identity Deception Techniques.

## Social trends relate to whom is being attacked and how.

About 10 years ago, the most common type of fraudulent email was a phishing email, in which an intended victim received an email appearing to come from his or her bank, asking him or her to click on a link to log in. Historically, another common type of fraudulent email was the consumer-facing "Nigerian prince" email. Recently, these email attacks have switched to target enterprises, and most of the time, the attacker attempts to impersonate a colleague or a vendor asking for a transfer of funds.

## What Drives These Trends?

Technical trends are typically driven by improved delivery rates for the attackers, as they learn how to circumvent security controls. Social trends tend to be driven by how quickly attackers discover where to find the most lucrative and most vulnerable targets. By understanding these trends ourselves, we can begin to anticipate where the next wave of attacks is likely to occur and get one step ahead of the wrong-doers.

Still, one must never underestimate the agility and avarice of organized crime. While most criminal organizations are running multiple types of fraud schemes, there are three types that are almost always present: romance scams, rental scams and BEC scams.

These three types of scams are very different, yet complementary, which explains why they are commonly seen together. Romance scams are high-effort, requiring continuous interaction between the criminal and the victim. On average, a criminal email account will send 235 messages across 10 different threads for 25 days during a romance scam. This is a lot of work, but the payoff is not only monetary—many romance scam victims may be converted to money mules (often unwittingly), for use in future attacks.

In comparison, rental scams are short-lived and low-effort, providing a predictable near-term income stream to the criminals. During a rental scam, on average, a criminal email account will send 67 messages across 20 different threads for a mere five days.

But BEC is where the big money lies, and this is where we see the biggest growth in cyberattacks. On average, a BEC attack lasts for less than three days, during which the criminal will send 46 messages across 26 threads. As we will further explore, BEC also has the most victims per probe, making it the most effective of these attacks.

Looking at the relationship between these three types of scams over time, through the lens of 10 criminal organizations observed by Agari, it's plain to see the alarming growth in attacks. It is important to realize that these three types of attacks are just pieces of a larger puzzle. Agari has been able to produce a more complete picture, having captured so many criminal email accounts belonging to these 10 organized crime groups. Many of the observed scams are a variation of the "advance fee" fraud, but with different pitches and different targets. We elaborate on many of these scams in more detail below.

Other types of scams are used as alternative money exit methods, such as "mystery shopper" scams in which the unwitting mule is purchasing gift cards and forwarding the codes of these to the attackers. By studying the longevity of these campaigns, we can infer the likely benefits the different scams present attackers with, allowing us to make predictions about future developments, to assess the comparative levels of sophistication and innovation among criminals, and to suggest effective countermeasures for likely targets.

## Diversification of Scam Activity Within Gangs

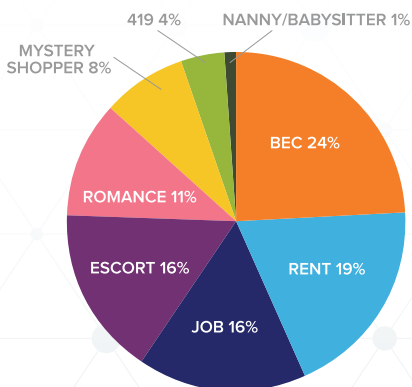
Examination of the attackers' activity shows that BEC scammers are involved in a whole host of other scams. Historically, these organized crime groups have engaged in romance scams, but more recently BEC attacks have emerged as a more lucrative and successful approach.

Even as these criminals have taken on more sophisticated attacks, they have continued romance scams. We believe there are two reasons for this. First, they provide steady cash flow to fund the criminal enterprise while it goes after larger prey. Second, they allow the gang to generate a continuous supply of new money mules who they depend on to retrieve their funds.

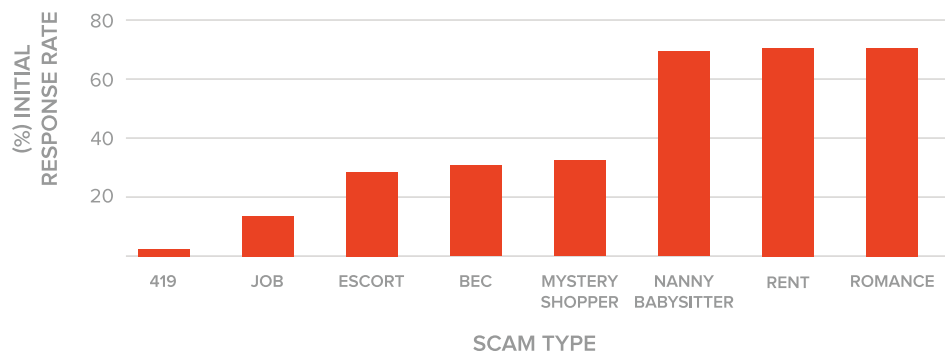
We have also seen a division of labor within some gangs, which seem to run like businesses. One member collects lists of leads and correlates multiple executives within the same company to target in BEC attacks. Another communicates with the targeted victims. A third manages the money flows.

## Prevalence

Our research classified 2,512 discrete attempted scams. We have classified the scams into the following categories, with prevalence noted:



**Figure 16:** Prevalence of Different Attacks. BEC is the most common attack type, indicative of a growing risk since the average age of the accounts was more than four years old, but BEC did not emerge until less than two years ago.



**Figure 17:** Initial Response Rates for Different Types of Scams. These percentages indicate the initial response rate to a variety of attacks, regardless if the attack was ultimately successful or not.

## Money Mules

Parting people from their money isn't necessarily the hardest part of the scammer's job. The real bottleneck is getting the money out of the system. For most North American and European companies, a request to mail a check or wire money directly to an individual in Nigeria would raise more red flags than a payment to a domestic recipient. Meanwhile, banks and other financial intermediaries have tightened their controls over all large wire transfers, especially between unknown senders and receivers, whether to Nigeria or elsewhere.

For that reason, recruiting money mules is a full-time effort for each of the groups we captured. As the scammer groups are typically based overseas, a successful scamming operation is entirely dependent on money transfer techniques that evade suspicion.

A money mule is an individual, generally located in the same country as the victim, who helps the scammer launder stolen money, by methods including routing it through their bank accounts or using iTunes or gift cards. Mules typically begin as unwitting co-conspirators. Over time, they become victims, either through direct financial losses or through falling afoul of law enforcement. Some mules, particularly those recruited through romance scams, become witting co-conspirators, either by refusing to believe their love interest is a scammer, or through blackmail with a threat of turning them in for their role in the scams.

There are two primary sources of money mules: romance scams and work-from-home scams, a type of job scam. These are covered in the section below.

## BEC Attacks

BEC is a type of advanced email attack that inherently relies on the use of identity deception and evades detection by avoiding the use of a detectable payload such as a URL or attachment. Commonly, the criminal will pose as a colleague of the intended victim or as a vendor of the organization of the intended victim, and either ask the intended victim to perform a payment or to send some sensitive data.

There are three different types of identity deception that criminals use to execute a BEC attack: spoofing, look-alike domains and display name deception. Previous Agari research has indicated that 82 percent of BEC attacks use simple display name deception.

In addition to using identity deception, some criminals use corrupted accounts to perform BEC attacks. This gives the criminal access to past interactions between the corrupted user and the intended victim, allowing them to customize the pitch and make it even more believable.



## A Reversal of Fortune

Most BEC attacks proceed in a similar fashion. Criminals leverage business contact databases, social networks and even a company's own website to identify key individuals. In the instance shown below, we captured a criminal email account that was using display name fraud to appear as the president of an entertainment company in Los Angeles.

The attacker sends a simple request to a member of the accounts payable team to determine if his employee is available to make a payment. (The real names and company of the "president" and victim have been redacted.)

From: "President of Company" (Display name deception)
To: "Accounts Payable Victim"
Subject: <b>Due Payment</b>
"Accounts Payable Victim," Are you available to make a payment?

We can see from the next exchange that the target has taken the bait, as the criminal sends a follow-up email to the target. Our research shows that BEC attacks are more than 10 times more likely to succeed after an initial response is received. In this message, our criminal requests an overnight payment for \$64,250:

On Mon, Apr 9, 2018, "Victim" wrote:
HI "President", yes, how can I help?

From: "President of Company" (Display name deception)
To: "Accounts Payable Victim"
Subject: <b>Re: Due Payment</b>
"Accounts Payable Victim," See attached W-9 for vendor details, Overnight a check for \$64,250. e-mail me with tracking# once check is mailed out. Thanks, "President"

As the attack proceeds, accounts payable requests the email address of the vendor to verify her payment. The criminal provides an affiliated email address that will provide the fraudulent bank account information.

×

**On Mon, Apr 9, 2018 , "Accounts Payable Victim" wrote:**

Will do! Also, before we can do that, I need to get her email address so I can email her a link to verify her vendor information. Would you be able to send me her email address when you have a sec?

Thanks!

×

**From:** "President of Company" (Display name deception)

**To:** "Accounts Payable Victim"

**Subject:** **Re: Due Payment**

**Send to** [REDACTED AFFILIATE CRIMINAL EMAIL ACCOUNT]

Again, the criminal faces another obstacle in his play as the accounts payable team does their due diligence, but the criminal responds vaguely enough that it doesn't raise suspicion.

×

**On Mon, Apr 9, 2018 , "Victim" wrote:**


Thanks "President." Also, can you let me know what project this payment is for for coding purposes? Once she approves her vendor information, I'll send you the bill for approval.

×

**From:** "President of Company" (Display name deception)

**To:** "Accounts Payable Victim"

**Subject:** **Re: Due Payment**

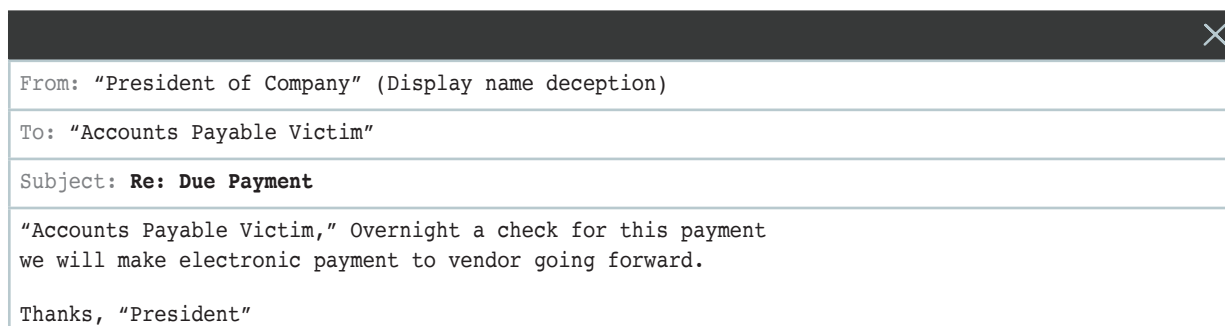
Payment is for consulting. 

It seems this attack is passing the point of no return. The accounts payable team presents the criminal with multiple options for sending payment. This criminal prefers a paper check instead of electronic payment.

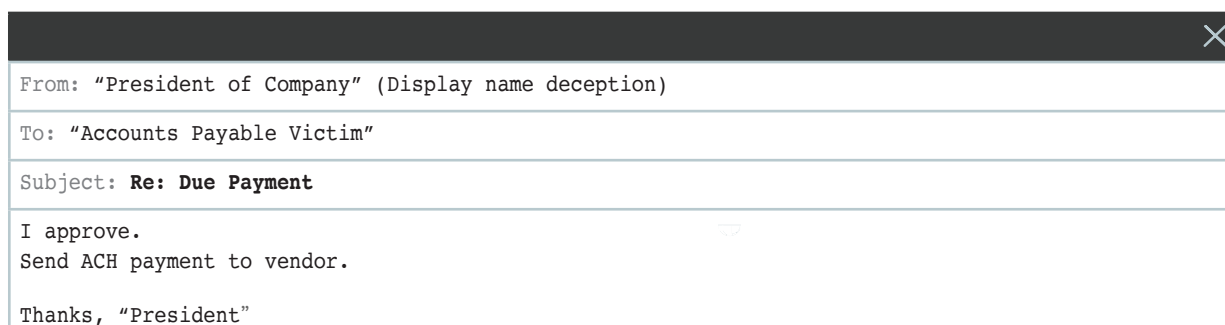
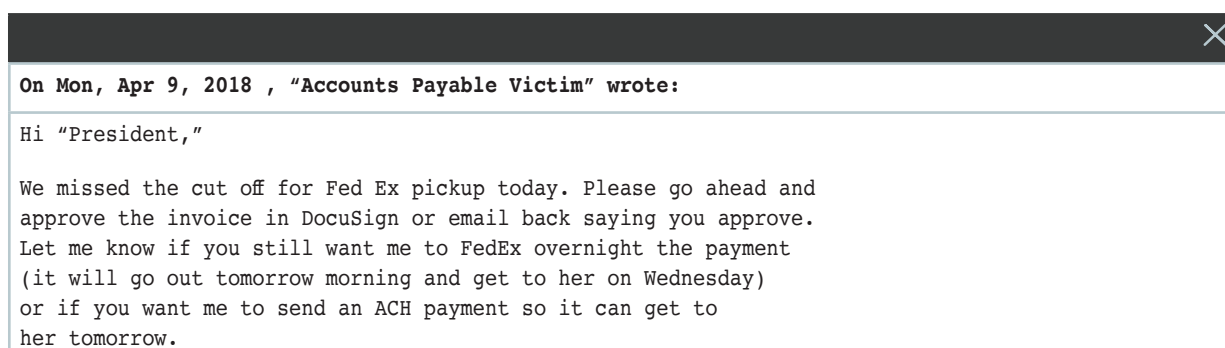
×

**On Mon, Apr 9, 2018, "Accounts Payable Victim" wrote:**

TShe submitted her electronic payment information, so if you would prefer, I could make sure her electronic payment will be processed tomorrow. Otherwise, I am still happy to overnight a check, but wanted to let you know we have that option.



This attack has now reached its final step, as accounts payable has still not realized that “President of Company” is not who he claims to be. This criminal leverages his assumed authority over a woman that presumes he is her boss. These brief exchanges seem all too recognizable as the terse messages that a busy president or CEO would send. The target is all too eager to please her boss and wires payment for the fraudulent charge.



In most cases, this story would end in tragedy (lost funds, potential employee termination, etc.). But this story has a happy ending. In the process of actively monitoring these captured criminal email accounts, an Agari researcher identified this BEC attack and was able to warn the accounts payable team just in time to reverse the wire payment. The response from the victim was a condemnation of the attacker using words too colorful to print. Agari advised the victim to contact her bank immediately to reverse the charge and to file a complaint with the FBI’s IC3 division.

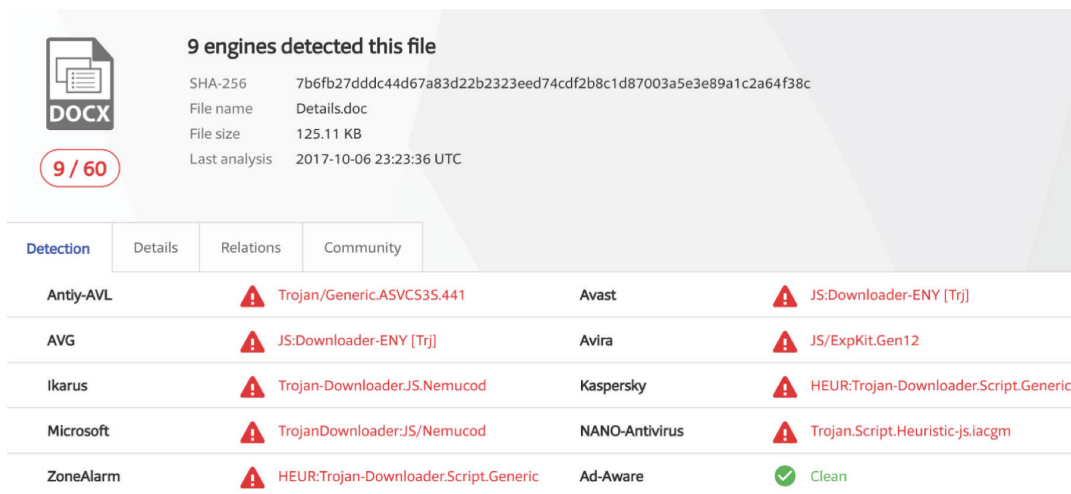
## Real Estate Purchase or Escrow Scams

There are two types of real estate scams—rental scams and purchase scams. Rental scams are a low-cost, high-volume scam. The scammers post an ad for an apartment or vacation rental they don't own, request a deposit and then disappear (savvy security professionals can spot these a mile away on Craigslist). These are more common than purchase scams, as they require less competence to carry out, but they are also less profitable.

Purchase or escrow scams are a sophisticated man-in-the-middle attack, and are especially dangerous, potentially costing victims their life savings. The scammer targets multiple real estate agents or title companies and tricks them into installing malware, which lets him take over the account and begin forwarding all the email to him. He then begins monitoring potential purchases.

When a deal is ready for completion, the scammer sends an email to the buyer purporting to be from an escrow agent or the real estate broker, and provides payment instructions with the scammer's account number. By knowing all the details of the transaction (address, purchase price, the name of the agent, etc.) and knowing when the buyer is expecting instructions, the fraudulent email can be made to look highly convincing even to sophisticated individuals. The victim instructs the bank to wire the money. And in an instant, their down payment—and possibly their life savings—is gone forever.

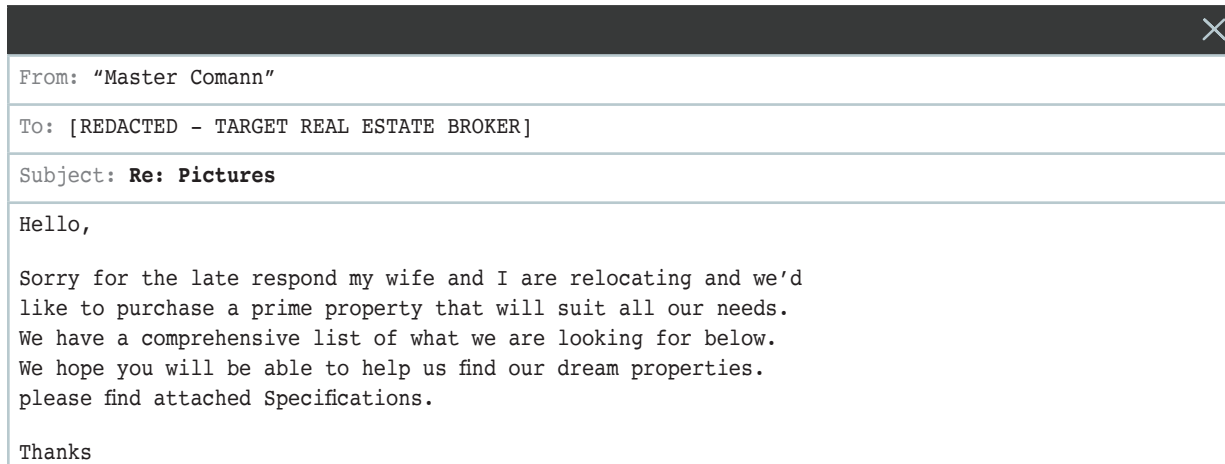
The criminals often use custom malware to compromise the accounts of their launchpad victims. Figure 17 shows our scan of one malware-laden file used by Group Five, made half a year after the malware was purchased.



**Figure 17:**  
A Custom  
Malware  
Sample.

Criminals relying on malware commonly use custom-made malware, purchased on the dark web. Because these are highly tailored pieces of malware that are used only rarely, very few antivirus services are able to detect them. As the figure above shows, one piece of custom malware was only detected by nine out of 60 engines, even six months after it was purchased and deployed.

## Initial Infection Vector



Attached to the email was a Word document infected with malware, and a fake letter from a fake bank, New York Securities Bank, attesting that the buyer has \$400 million on deposit.

The attacker, “Master Comann,” sends variations of this email to many real estate agents. In another example, he has identified himself by forging an alias to the letterhead of a rural Texas hospital.

## W-2 Scams (Identity Theft and Tax Fraud)

In a W-2 scam, the attacker contacts employees in a company’s human resources department with an email appearing to come from the company’s CEO or CFO. The message asks for a copy of the company’s W-2 files. W-2 forms are the Internal Revenue Service (IRS) documents U.S. employers provide to their employees shortly after the end of each year, listing the employee’s earnings, tax withholding, Social Security number and address.

Once they receive that information, the scammers can file fraudulent tax returns to receive a refund check from the IRS. More than 200 employers were victimized by W-2 scams in 2017, compromising the identity of hundreds of thousands of employees, the IRS has reported.

## Nanny Scam

One group runs a nanny scam, where they place an ad for a nanny to care for a disabled child. Respondents are sent a check which they are told to deposit and use a portion of to purchase a wheelchair that the scammer found online. Naturally, the check is bogus and will eventually bounce, but not before the victim has purchased the wheelchair. To make matters worse, the wheelchair ad is also fraudulently placed by the same scammer. After the purchase is made, no goods are shipped.

## Escort Scam

One of the organized crime groups runs an advance fee scam seeking an escort for a wealthy client. Respondents are sent a bogus check for the escort services with an additional amount to be spent with the wealthy client’s “agent” to arrange a hotel room, champagne service, etc. As with other “advance fee” scams, the victim of the attack will either make a payment

to a party associated with the criminal, or refund a portion of a fake check payment in excess of what they needed. The criminal would thereby receive a transfer as a result of sending a fake check, and the victim's bank will charge the victim's account once the scammer's check bounces.

## **Nigerian Letter or 419 Scam**

The grandfather of these attacks, almost always run out of Nigeria, is an email purporting to be from an African government official or prince who offers a large reward in return for helping smuggle millions of dollars out of the country. Once the victim is hooked, he is persuaded to send an advance fee (often in the thousands of dollars) to facilitate the transaction, and then the scammer disappears. These scams are old enough to have originated in physical letters before shifting to email, but have faded considerably as they have become less effective.

## **Job Scams**

Among the varieties we see are “mystery shopper” scams and “work-from-home” scams. These are commonly used by criminals to recruit unwitting money mules or to employ people to “help post ads on Craigslist”—a job description that in reality translates to “help evade security mechanisms deployed by Craigslist.”

## **“Mystery Shopper” Scams**

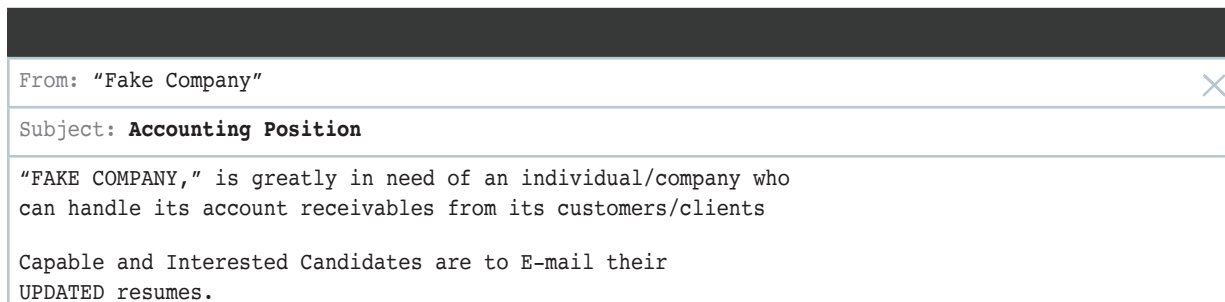
In this scam, ads are placed for mystery shoppers. Respondents are sent a check to cover their shopping task, which is to purchase various gift cards from a particular store. They are asked to fill out a form about their shopping experience, and to forward the gift card codes to the scammer as proof they did indeed perform their task.

A commonly observed shopping task is to receive a wire transfer (usually from a victim in another scam, unbeknownst to the mystery shopper) and to purchase iTunes cards. It might be hard to imagine why a scammer would be so dedicated to filling the gaps in their 70s disco music collection, but with the existence of online services such as paxful.com, the scammers can directly exchange the gift card's value for Bitcoin, essentially turning the iTunes card into a form of pre-paid currency. We have also observed our scammers exchanging Walmart gift cards worth over \$1,000 for Bitcoins, although Amazon, eBay, and Playstation Network gift cards could also have been used in exactly the same way.

Another variation of the mystery shopper scam involves the mystery shopper being sent a check, but for a higher value, commonly \$1800. In this instance the assigned task is to evaluate Walmart, and MoneyGram, the money transfer service. They will be asked to spend \$100 on grocery items for themselves; all the while making a mental note of the experience against some predefined criteria. Once they have completed this stage of the assignment they are asked to deduct their fee of \$300, plus an additional \$40 for the money transfer fee, and then forward the remaining \$1360 on to the next mystery shopper (the scammer). The success of this scam very much hangs upon the check not being spotted to be a forgery, and for the shopper to not get cold feet and wish to return the check as they have suspicions about the legality of the role. As the check eventually bounces, the mystery shopper will realize that the money he or she transferred is lost, but then that is much too late.

## Work-From-Home Scams

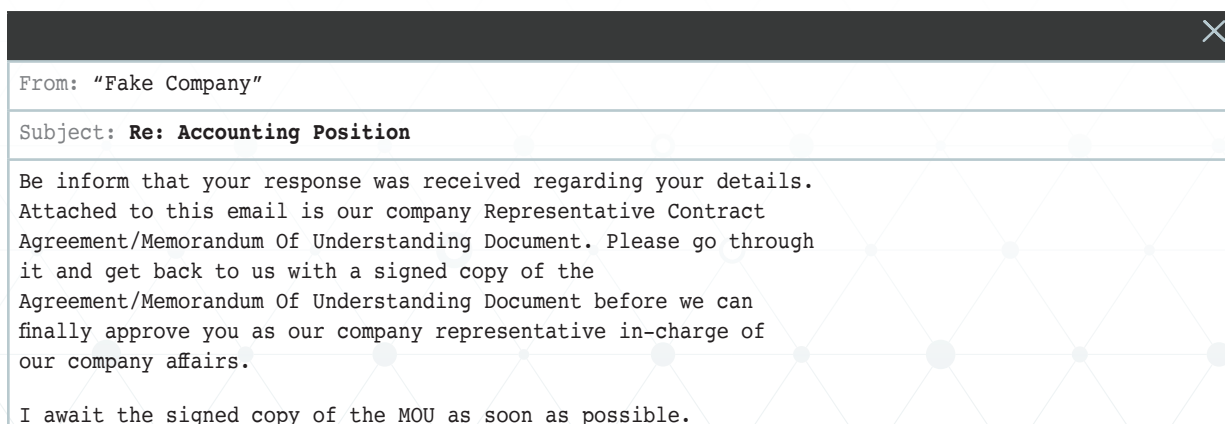
What follows is a real example of a work-from-home scam and our interaction with the scammer. The attacker used fake Japanese names for himself and his company name, which we have redacted. As is typical, it begins with a spam email:



After responding to this email, our researchers received the following email:



After throwing together and sending a mediocre accounting resume, we were soon offered the position of Company Representative with "Fake Company":



After returning the signed MOU, we were soon given our first assignment:

X

From: "Fake Company"

Subject: **Re: Accounting Position**

Prior to your Approval as "Fake Company" representative in-charge of its delinquent account collections/receivables in USA & Canada. Below is the details of your first delinquent account collection on behalf of "Fake Company"

First Official Assignment : You are to contact this customer/client (REDACTED) as your first delinquent account collections on behalf of "Fake Company" Be inform that REDACTED is one of our numerous Customers/Clients that owes our company, although the management "Fake Company" has already spoken to REDACTED regarding your employment as our company representative in-charge of delinquent account collections in USA & Canada and also we have sent him your contact details, informing him to remit all payment they owe "Fake Company" to you as Corporation representative, who is in-charge of our delinquent account collections. You are to contact this delinquent customer/client immediately you receive this message.

Details Of Delinquent Customer/Client are below:

REDACTED (CEO)  
REDACTED  
Tel: Phone: +1-403-555-5555  
Cell ; +1-403-555-8888  
E-mail: REDACTED@redacted.com  
Website:www.redacted.com

FILL OUT THE BELOW FORM AND SEND IT TO HIM ALSO.

Your Business/Company or Personal name to receive payment\_\_\_\_\_

Please confirm address where Payment check is mailed to\_\_\_\_\_

The financial institution check will be processed\_\_\_\_\_

Largest Deposit ever made to this account\_\_\_\_\_

Personal names\_\_\_\_\_

Direct mobile line\_\_\_\_\_

Email\_\_\_\_\_

Be inform that this delinquent customer/client owes our company the sum of \$695,781.00 (Six Hundred And Ninety Five Thousand, Seven Hundred And Eighty One Dollars). So therefore you are to contact this delinquent customer/client via phone and E-mail communication to discuss on how and when their company (REDACTED) intend to remit payment to you, as Company representative. Although REDACTED told our company management that they were ready to remit payment in installment as soon as you establish contact with their company. Also you are to update me on every discussion and contact you establish with this delinquent customer/client.

Note: Attached to this email is the scan copy of "Fake Company" Purchase Agreement and the Purchase Invoice that was used in transacting business between "Fake Company" and REDACTED.

As soon as you are in contact with REDACTED don't hesitate to let us know.

Warm Regards  
"Attacker Alias"  
Director of Administration

At this point we were forced to resign our post, as we could not continue to act as a representative of "Fake Company" without breaking the law.



## Romance Scams

Every organized crime group we captured conducts romance scams in order to find U.S.-based money mules, who aid and abet the foreign scammers by helping them launder money. Most of these money mules are themselves victims, both emotionally and financially. One such mule admitted to the investigating officer that she had been carrying on an online relationship with her handler for six years. She had already given the scammer half a million dollars of her own money, and was paying for a \$250/month business contacts service that her handler used to target companies. She had been contacted by local police in the past, and several of her accounts had been closed at major banks for fraud. Sadly, her story isn't unusual.

Romance scams were the most popular method of money mule recruitment among the groups we captured. While time-consuming, the advantage of the romance scam is the trust built up over time between the scammer and his mule. Thanks to this trust, the mule is far less likely to simply pocket the proceeds. So how does the scam work?

The attack chain is quite straightforward:

- 1 Create a free webmail account.
- 2 Establish a U.S. phone number using Google Voice or a similar service.
- 3 Create a fake Facebook and/or Instagram profile.
- 4 Join one or more online dating websites.
- 5 Use the dating site's search capabilities to target vulnerable individuals.
- 6 Communicate via the dating website just long enough to move the conversation to another medium such as text or email.
- 7 Use mass-marketing email techniques to identify the loneliest, most gullible targets.
- 8 Continue the conversation with the most gullible targets.
- 9 Eventually ask the victim for small sums of money for some contrived hardship.
- 10 Once the victim starts complaining about money, offer them a way to get all of their money back by simply cashing a couple of checks and sending part of the money to the scammer via Moneygram or Western Union.
- 11 Continue pulling the romance scam victim deeper into the scams.
- 12 If the victim wises up, threaten to turn him or her in to law enforcement if he or she does not continue to launder money for the scammer.

## Broken Hearts, Broken Lives

Among the saddest and most heartless of all scams are the romance scams. We captured one long-running exchange between “Jim Blackie” and a divorced American woman with children. Blackie portrayed himself as an expatriate living in Dubai (though the attacker is actually working from Nigeria), and shared photos of attractive individuals (catphish photos) seemingly grabbed from the Internet.

The woman refinanced her home to send money to Blackie. Eventually the creditors closed in, and she was forced to sell her house, pull her children out of school, and move the family in with a friend. She sent Blackie more than \$500,000. All the while, he continued asking her to go out and buy him gift cards. Despite doubts, she persisted in believing he is for real.

×

**On May 7, 2017, at 7:50 PM, “Jim Blackie” wrote:**

How was your day my baby

×

**On Sunday, May 7, 2017, [Victim] wrote:**

It was good. Enjoying time w [child’s name]. Wish you were here babe

×

**On May 7, 2017, at 8:18 PM, “Jim Blackie” wrote:**

I wish that too baby I can’t wait for us to be together as family

×

**On Sunday, May 7, 2017, [Victim] wrote:**

We’ve been saying that for a long long time



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](https://acid.agari.com)**