AGARI CYBER
INTELLIGENCE DIVISION

REPORT

# Scarlet Widow

## BEC Bitcoin Laundry: Scam, Rinse, Repeat

Part 2: Nigeria-Based Scammer Group Targets Nonprofits and Schools; Launders Stolen Gift Cards Through Online Cryptocurrency Exchanges

# Executive Summary

Much of the investigative work done by Agari and others to date has focused on the activities of business email compromise (BEC) gangs going for big scores against big targets: jackpots of tens to hundreds of thousands of dollars, scammed out of medium-sized and large corporations.

Now, Agari has uncovered and documented the practices of a Nigeria-based scammer group, dubbed Scarlet Widow, that has evolved a different strategy. Rather than focusing on corporate targets, which are devoting increased resources to cyber-defenses, the group focuses on more vulnerable sectors such as school districts, universities, and nonprofits, which the group likely believes are softer targets.

## From Rental Fraud to Romance Scams to Tax Refund Diversion

Agari has been gathering information on Scarlet Widow since 2017 and we have documented its evolving operations going back to 2015. In 2015, its focus was on romance scams and property rental fraud. In 2016, Scarlet Widow moved into tax fraud, successfully submitting dozens of fraudulent returns and scoring thousands of dollars in tax refunds with minimal effort. By 2017, like so many West African cybercrime groups, the group moved into the lucrative world of BEC, where it continues to focus its efforts to this day.

Scarlet Widow's preferred targets for BEC scams include academic institutions, including K-12 school districts in the American Midwest and universities in five countries, and nonprofit organizations around the world, ranging from the Boy Scouts of America to the YMCA.

While the bulk of its recent BEC attacks has focused on schools and nonprofits, Scarlet Widow also seems to be preparing for phishing campaigns targeting tax preparation firms. In September 2018, the group began collecting targeting information on thousands of United States-based tax preparers, likely to target these individuals with W-2 BEC attacks prior to tax season.

Like London Blue, the subject of an Agari report in December, this Nigeria-based cybercriminal group operates like a modern sales and marketing organization, building out an entire solution stack to run its scams—including resources for lead generation, email distribution, aliases, falsified documentation used in romance scams, and more.

Since November 2017, Scarlet Widow has gathered targeting information for more than 30,000 individuals associated with more than 13,000 organizations in 12 countries. Most of the leads collected by Scarlet Widow were for employees located in two countries—with 73% in the United States and 20% in the United Kingdom.

# Financial Exfiltration and Money Laundering via Gift Cards and Bitcoin

During our investigation into Scarlet Widow, we observed a shift in the group's cash out methods that parallels trends we are seeing across the entire BEC threat landscape. While the group originally relied on wire transfers in their early BEC scams, they have now transitioned to seeking payment through Apple iTunes and Google Play gift cards.

To launder their proceeds, Scarlet Widow uses a US-based peer-to-peer cryptocurrency exchange called Paxful that—whether wittingly or not—has become a bazaar for West African scam artists. Nigerian scammers are using the exchange to convert fraudulently obtained gift cards into bitcoin for 40 to 80 cents on the dollar.

As a result, within minutes from when a victim emails Scarlet Widow gift cards, they can move the funds beyond the reach of authorities in the victim's country. This avoids the trouble of recruiting and managing local money mules, and eliminates the window when authorities and financial institutions can halt and reverse some wire transfers.

This document is the second of two reports Agari has published on Scarlet Widow. The first report, released on February 13, 2019, focused on the group's history of romance scams.

# Table of Contents

# BEC: Brutally Effective Crime

## Agari's investigation into Scarlet Widow offers a window into today's predominant advanced email threat—business email compromise (BEC).

BEC comes in many forms, but in most cases, the criminals behind these attacks impersonate a senior executive within the targeted company, or a trusted outside partner or supplier.

Whether a stress-inducing missive from the "CEO" demanding an urgent wire transfer, or a time-sensitive request for employee tax records from the "CFO," these malicious emails are used to fool recipients into fulfilling requests before thinking to confirm their legitimacy. The language used in these deceptions and their timing are meant to throw the recipient off kilter just long enough to trick them into revealing sensitive information or making ill-advised payments.

And unfortunately, the cybercriminals are good at what they do. Reported BEC losses in the United States rose 88% between 2016 and 2017, according to the FBI's Internet Crime Complaint Center.

As illustrated by Scarlet Widow's evolution, BEC has become an increasingly tempting line of attack for cybercriminal organizations. The U.S. Securities and Exchange Commission (SEC) in October reported that victims include a publicly traded company that made 14 separate wire payments for fake invoices over the course of several weeks—racking up $45 million in losses. Another paid out $30 million.

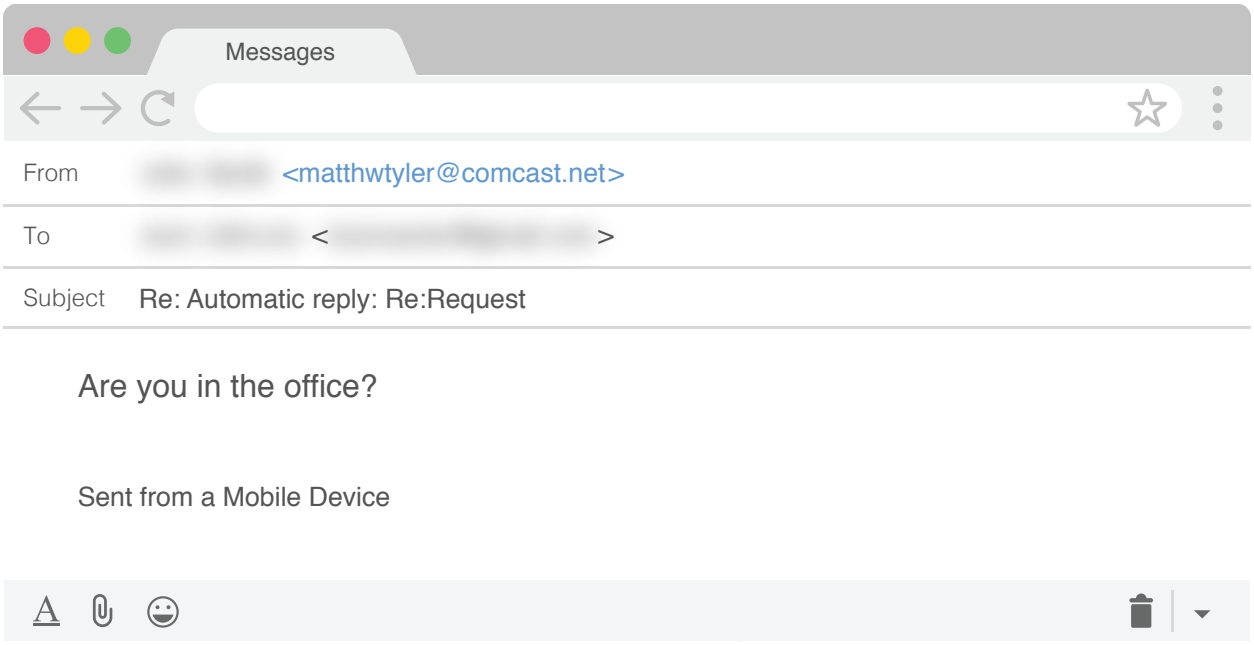
Part of what makes these attacks so difficult to detect is that BEC emails typically contain no malware, thus rendering them invisible to most email security controls in use today.

# Untangling Scarlet's Web

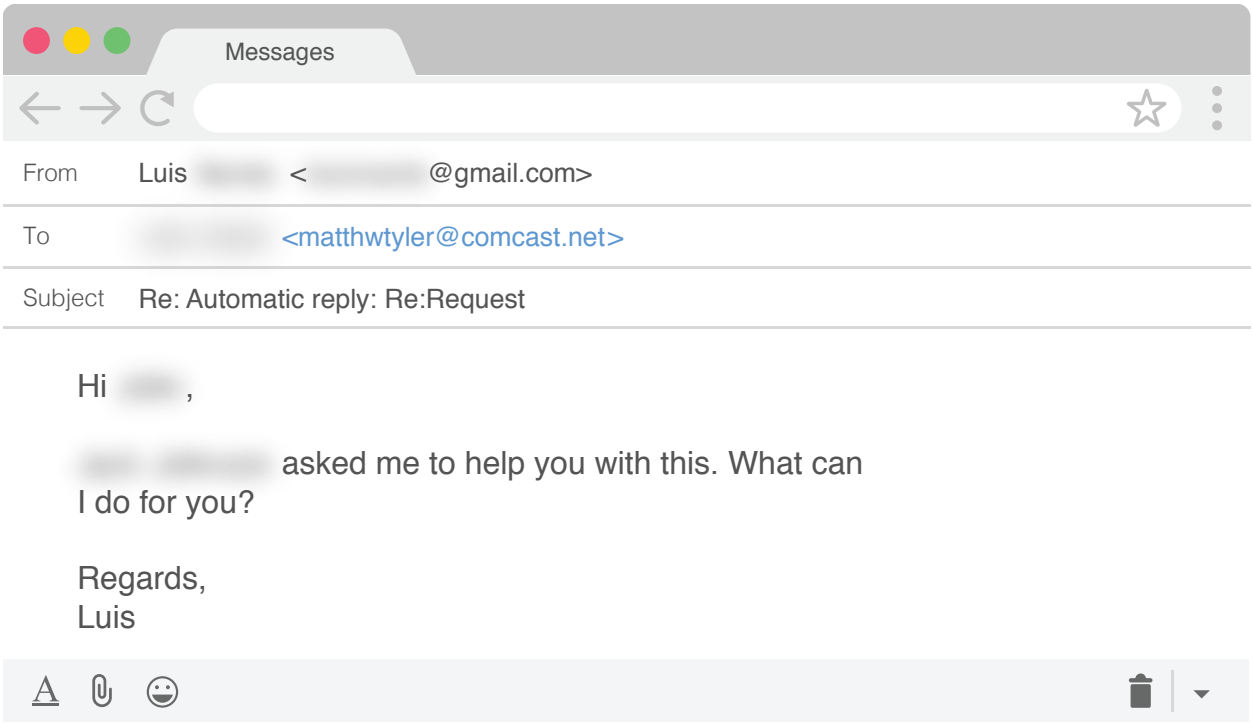
When the VP of Human Resources at an Agari customer was targeted by an attempted BEC scheme, researchers in the Agari Cyber Intelligence Division seized the opportunity.

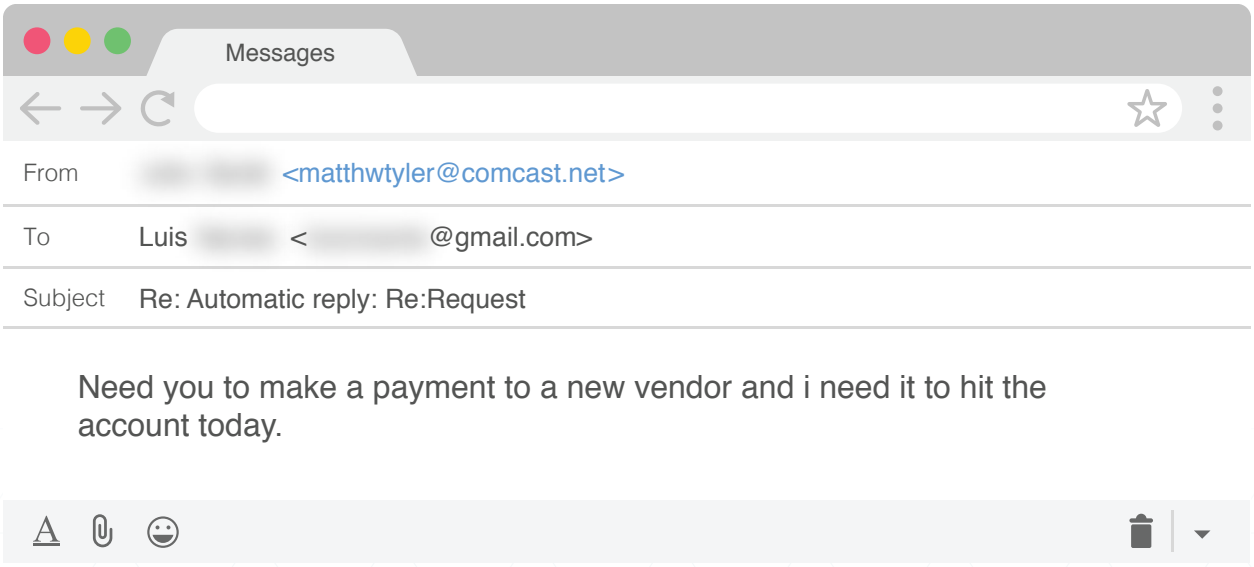
## Scarlet Widow Initiates First Contact

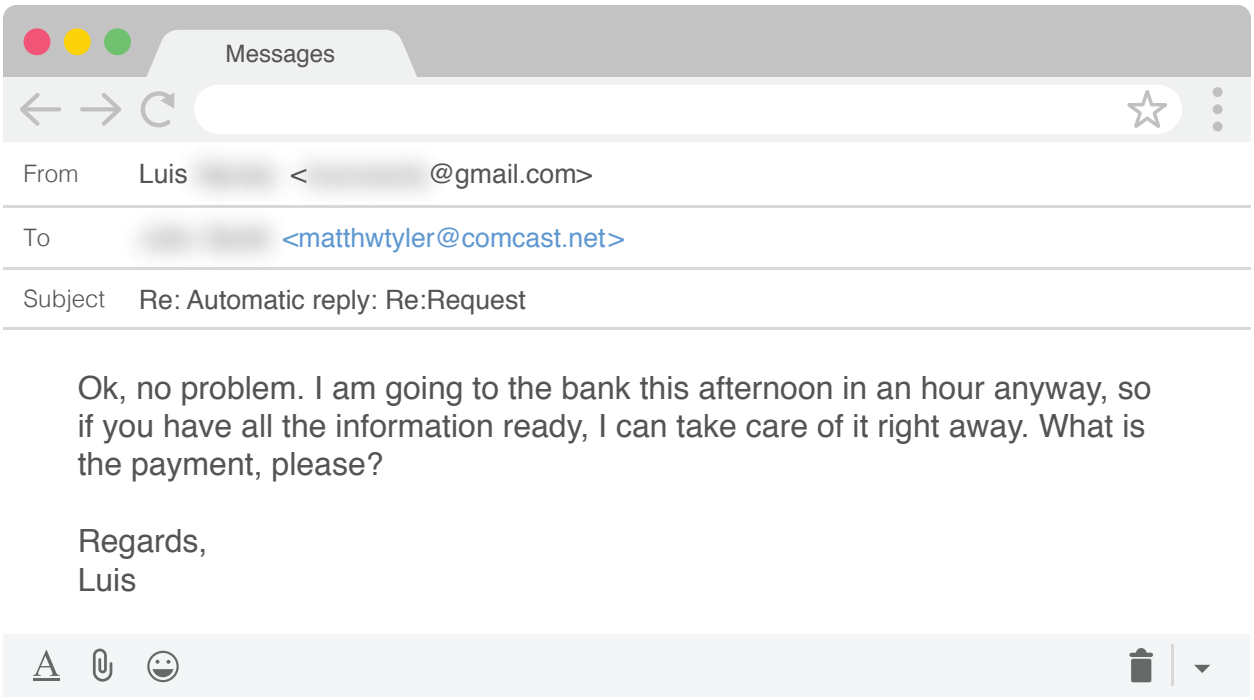
It was the quintessential "CEO" scam, complete with an urgent payment request made via an email to the VP of Human Resources at an Agari customer in November 2017. Like most BEC scams, Scarlet Widow uses display name deception techniques. Using a free and temporary email account—in this case a Comcast address—scammers simply change the display name of the account to the person they are trying to impersonate, which in this instance was the targeted company's CEO.

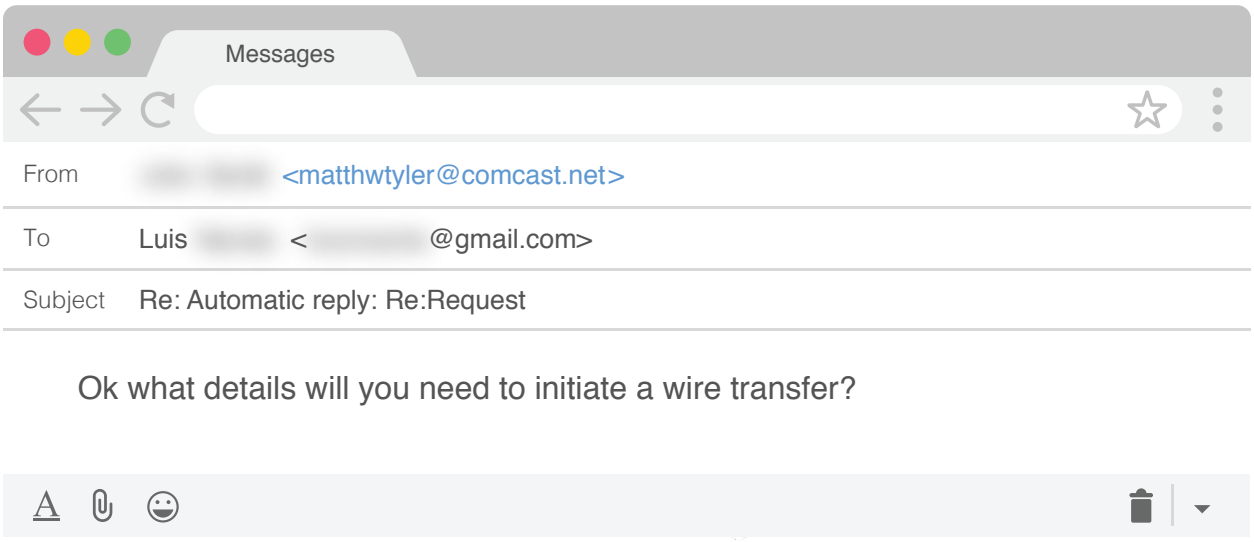


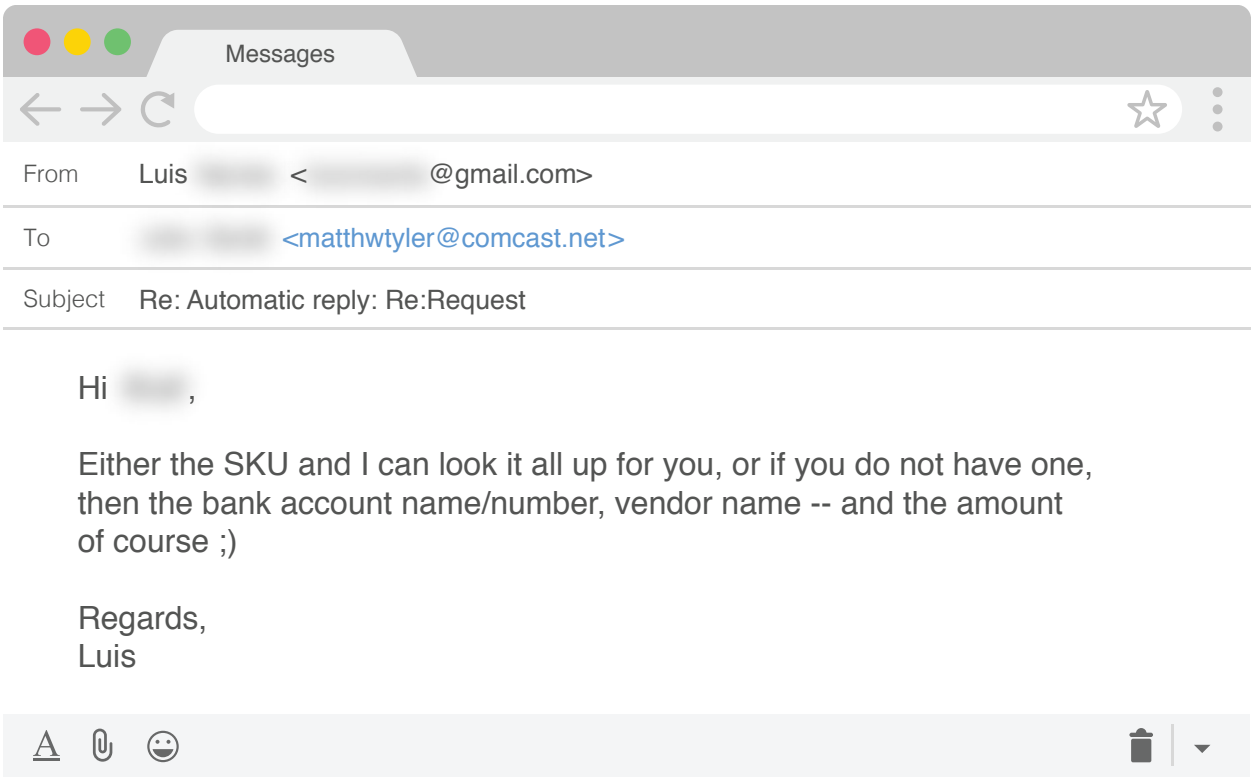
Although the email was blocked by Agari's inbound defenses, the customer contacted ACID researchers to see if we wanted to do any further analysis. Posing as an assistant named "Luis," we began engaging with the fraudster in an attempt to collect additional information about their tactics and infrastructure. What followed was a lengthy conversation that resulted in obtaining a deep insight into a prominent and long-standing Nigerian threat group. The conversation proceeded as follows:

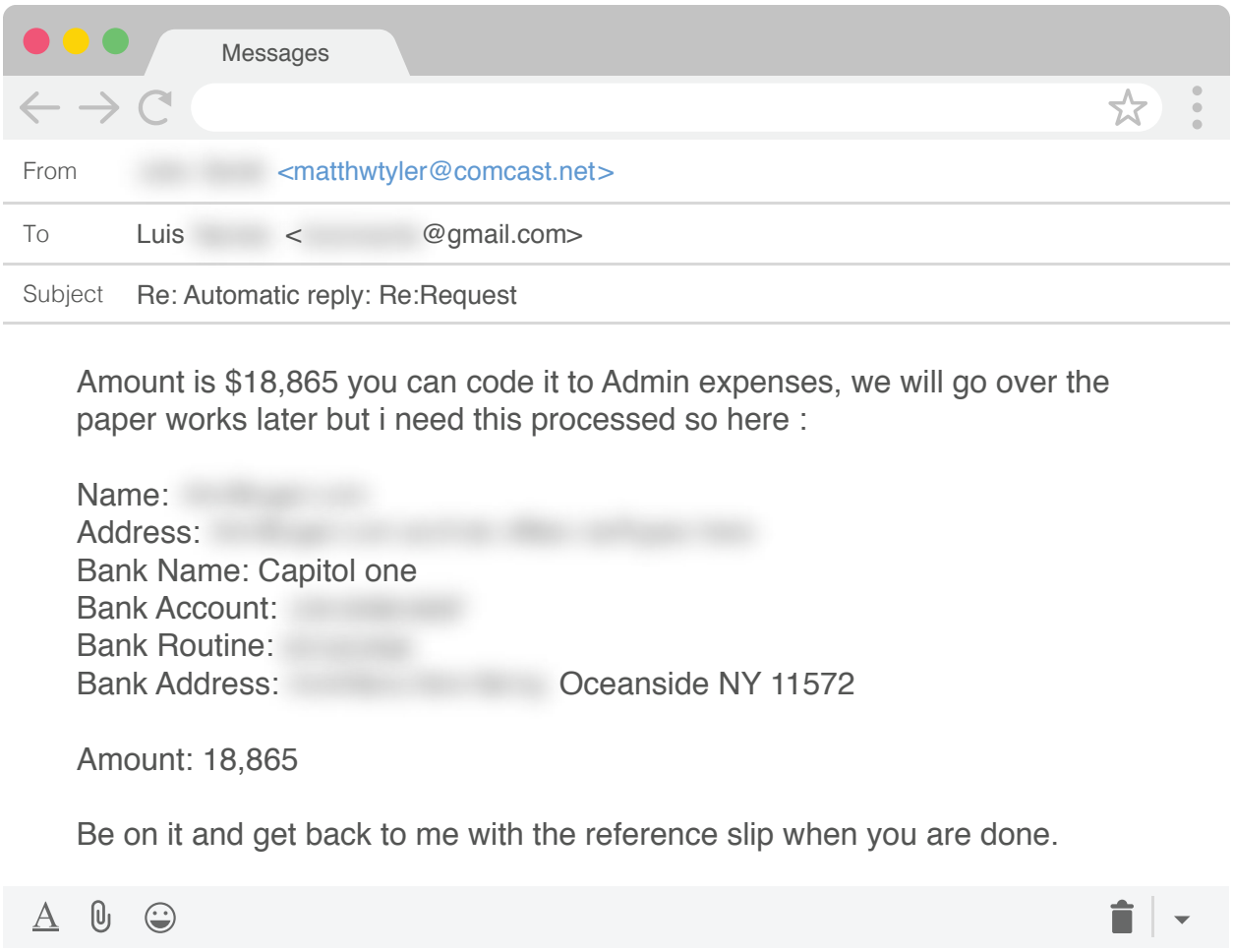



Messages
From Luis [redacted] <[redacted]@gmail.com>
To [redacted] <matthwtyler@comcast.net>
Subject Re: Automatic reply: Re:Request
Ok, no problem. I am going to the bank this afternoon in an hour anyway, so if you have all the information ready, I can take care of it right away. What is the payment, please?
Regards,
Luis


Messages
From [redacted] <matthwtyler@comcast.net>
To Luis [redacted] <[redacted]@gmail.com>
Subject Re: Automatic reply: Re:Request
Ok what details will you need to initiate a wire transfer?


Messages
From
Luis [redacted] <[redacted]@gmail.com>
To
[redacted] <matthwtyler@comcast.net>
Subject
Re: Automatic reply: Re:Request
Hi [redacted],
Either the SKU and I can look it all up for you, or if you do not have one, then the bank account name/number, vendor name -- and the amount of course ;)
Regards,
Luis




After this initial interaction, we continued engaging with Scarlet Widow actors for nearly a month. During this time, we were able to identify a total of nine mule accounts used to receive illicit funds from BEC victims and passed this information to law enforcement and trusted partners. Using a combination of active engagement and other tactics, we were able to gain a deep understanding of the group's history, methods, and primary actors. What follows is an overview of what we uncovered during this investigation.

# Who is Scarlet Widow?
## A Look Behind the Curtain

While much of the high-profile cybersecurity news of the past few years has involved state sponsors like Russia and North Korea, American individuals and businesses are far more likely to be targeted by West African crime groups.

These groups, which frequently hail from Nigeria, account for a significant majority of the social engineering-based cyber attacks that American businesses encounter on a daily basis. In fact, previous Agari research indicates that 90 percent of BEC groups operate out of Nigeria.

To date, we have fully identified three Scarlet Widow actors who top the group's hierarchy, all of whom currently reside in Nigeria. Through extensive research and analysis, we have been able to connect the leaders with specific scams and personas, some of which you will learn about in this report.

### ACTOR 1

**32-YEAR-OLD MALE**
**LIVES IN LAGOS, NIGERIA**

- Specializes in romance scams posing as female models, tax return fraud, and CEO impersonation BEC attacks
- Aspiring record producer who has been promoting reggae music for the past 10 years

### ACTOR 2

**MALE (UNKNOWN AGE)**
**LIVES IN LAGOS, NIGERIA**

- Specializes in vacation rental scams
- Used to be part of an R&B music group
- Describes himself as an "honest down to earth, loving, laid back kind of man"
- Engaged with one son

### ACTOR 3

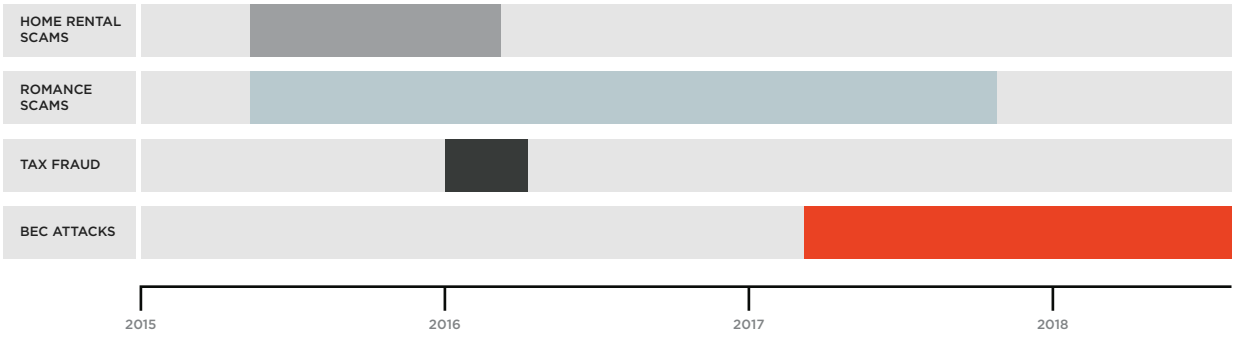
**22-YEAR-OLD FEMALE**
**LIVES IN KWARA, NIGERIA**

- Specializes in BEC lead collection and conducts romance scams posing as an active US military captain
- Recently took a Unified Tertiary Matriculation Examination for college admissions

In addition to these three group members, we have identified information linking at least eight other individuals who have assisted the core group of actors in various ways. Like many other BEC groups, including London Blue—the focus of our most recent intel report—Scarlet Widow actively mines and shares leads and compromised data among other members of its network of operatives. Similar to what we have observed with other groups, Scarlet Widow has a loose structure with central players and tangential actors who are responsible for specific tasks, such as collecting and processing targeting leads for BEC attacks or finding new pictures to use for fictitious personas in romance scams.

# Pathway to BEC:
## Moving Toward the Money

Scarlet Widow has been in operation since at least 2015. Over the past four years, the group has continually evolved its methods, testing new types of fraud and moving to more lucrative scams over time. Based on our historical visibility into Scarlet Widow's operations, we have been able to trace their evolution of criminal schemes over the years.



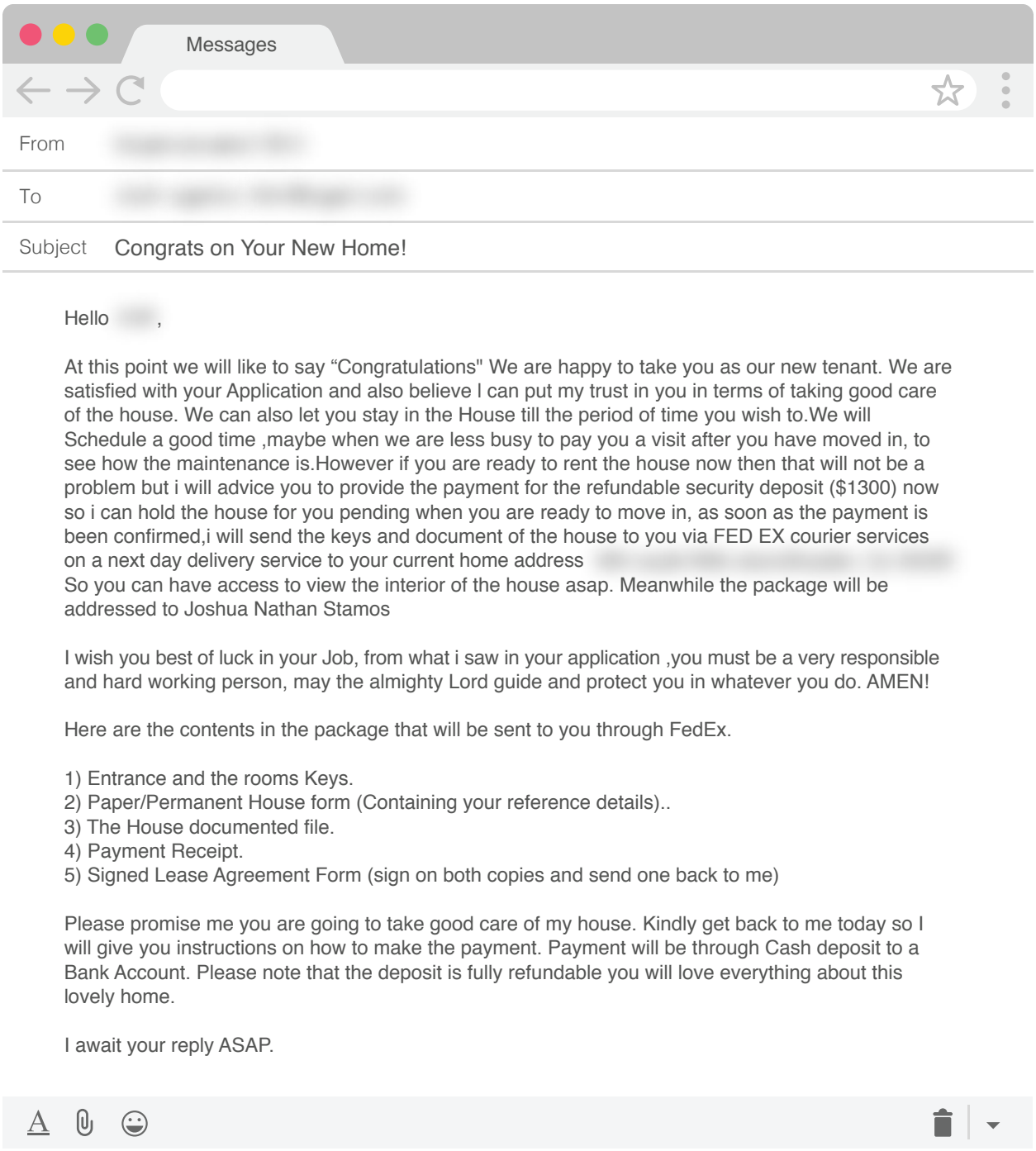

## 2015–2016: Home Rental Scams

Scarlet Widow was heavily involved in a variety of home rental scams throughout 2015 until early 2016, starting with vacation rental scams and then moving to fake tenant scams.

The scam typically followed a set pattern, starting with the group posting an advertisement on Craigslist about a home for rent. Images depicting a desirable property that would have wide appeal were used to generate interest in the rental. Postings were targeted around specific areas of the United States, including Denver; Miami; San Diego; San Francisco; and Sarasota, Florida.

When a prospective renter submitted an inquiry about the availability of the property, they were sent a response that the property was (of course) still available. They were also sent a full description of the property, along with a quote for the cost of the rental, which included a "refundable" security deposit.

Once the victim agreed to the price, they were informed that they must wire money to a bank account in order to confirm the rental—either the entire price of the rental for vacation rentals or the first month's rent plus a security deposit for general rentals. Once the victim sent the rent payment, they were told that they would be sent the keys and other documents for the property. Of course, none of these items were ever sent, leaving the victim swindled out of their money, and without a place to stay.



Messages

From [redacted]

To [redacted]

Subject Congrats on Your New Home!

Hello [redacted],

At this point we will like to say “Congratulations" We are happy to take you as our new tenant. We are satisfied with your Application and also believe I can put my trust in you in terms of taking good care of the house. We can also let you stay in the House till the period of time you wish to.We will Schedule a good time ,maybe when we are less busy to pay you a visit after you have moved in, to see how the maintenance is.However if you are ready to rent the house now then that will not be a problem but i will advice you to provide the payment for the refundable security deposit ($1300) now so i can hold the house for you pending when you are ready to move in, as soon as the payment is been confirmed,i will send the keys and document of the house to you via FED EX courier services on a next day delivery service to your current home address [redacted]
So you can have access to view the interior of the house asap. Meanwhile the package will be addressed to Joshua Nathan Stamos

I wish you best of luck in your Job, from what i saw in your application ,you must be a very responsible and hard working person, may the almighty Lord guide and protect you in whatever you do. AMEN!

Here are the contents in the package that will be sent to you through FedEx.

1) Entrance and the rooms Keys.
2) Paper/Permanent House form (Containing your reference details)..
3) The House documented file.
4) Payment Receipt.
5) Signed Lease Agreement Form (sign on both copies and send one back to me)

Please promise me you are going to take good care of my house. Kindly get back to me today so I will give you instructions on how to make the payment. Payment will be through Cash deposit to a Bank Account. Please note that the deposit is fully refundable you will love everything about this lovely home.

I await your reply ASAP.

Example of Scarlet Widow Rental Scam Email

## 2015–2017: Romance Scams

While still conducting home rental scams, Scarlet Widow began expanding their operations to focus on romance scams, where they would actively search for vulnerable populations on dating sites and then carry on an online relationship with their victims, all while swindling them out of money for plane tickets and other expenses. Key personas for Scarlet Widow include a Texas model living in Paris who they named "Laura Cahill;" a woman in Norway named "Lisa Frankel," who found her ex-boyfriend cheating on her; and "Starling Micheal," a United States Army Captain currently deployed in Afghanistan."

The group's romance scam activity is examined in further detail in Scarlet Widow: Breaking Hearts for Profit, published by Agari in mid-February 2019.

## 2016: Tax Return Fraud

In 2016, Scarlet Widow tried its hand at tax return fraud. Using comprehensive personal information collected from the breach of a Minnesota accounting firm and underground forums, the group filed at least 30 fraudulent tax returns using four different online tax filing services—TaxAct, TurboTax, Efile.com, and TaxHawk—during a two-month period. At least 25 of these fraudulent returns were accepted by the Internal Revenue Service.

To scale their tax fraud operations, Scarlet Widow took advantage of a feature within Gmail to open numerous accounts on tax filing websites linked to email addresses containing strategically placed dots. While all dot variants of a Gmail account direct all email to the same inbox, a vast majority of the rest of the Internet treats each variant as a distinctly separate email address, associated with a unique separate account and identity. Scarlet Widow took advantage of this "feature" to ensure that all correspondence from those accounts were directed to a single Gmail address.

For example, an email like scarletwidow01@gmail.com and scarlet.widow.01@gmail.com both go the same inbox—despite looking like different accounts to an outside service. This allowed Scarlet Widow to conduct their tax fraud schemes more efficiently by not having to monitor and manage numerous different email accounts. Instead, all of their tax fraud information was centralized within a single Gmail account.

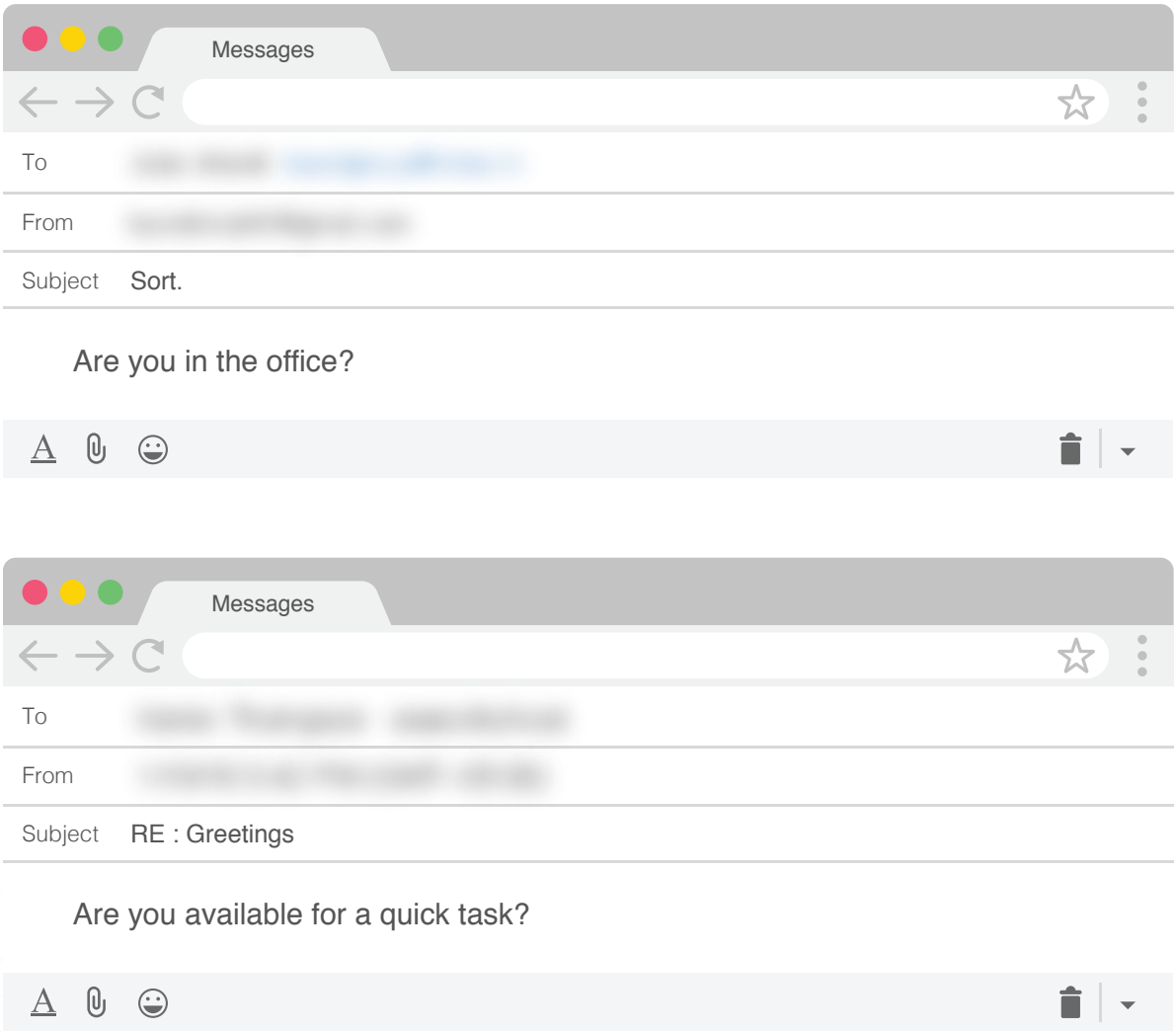
| Subject | Recipient | Date |
|---|---|---|
| Update: 2015 Federal Tax Return Accepted | s.ca.r.l.e.t.w.i.d.o.w.0.1@gmail.com | 2/23/16, 7:03 AM |
| Update: 2015 Federal Tax Return Accepted | sca.r.l.e.t.w.i.d.o.w.0.1@gmail.com | 2/23/16, 7:56 AM |
| Update: 2015 Federal Tax Return Accepted | s.c.ar.l.e.t.w.i.d.o.w.0.1@gmail.com | 2/23/16, 8:51 AM |
| Update: 2015 Federal Tax Return Accepted | sc.ar.l.e.t.w.i.d.o.w.0.1@gmail.com | 2/29/16, 7:40 PM |
| Update: 2015 Federal Tax Return Accepted | s.c.a.r.le.t.w.i.d.o.w.0.1@gmail.com | 3/1/16, 9:43 AM |
| Update: 2015 Federal Tax Return Accepted | s.ca.rl.e.t.w.i.d.o.w.0.1@gmail.com | 3/1/16, 1:57 PM |

Example of Google Dot Accounts Used to Facilitate Tax Return Fraud
(Note: Actual Recipient Email Address Changed)

# 2017–Present: Business Email Compromise

Following a trend seen throughout the cyber threat landscape, Scarlet Widow made its first foray into BEC in March 2017. While romance scams require a great amount of time and effort to continue the con, BEC offers groups like this something revolutionary. Most of the effort comes up front, when groups like Scarlet Widow conduct lead gathering. Once that is done, BEC groups can send phishing campaigns to large number of targets with very little effort and a relatively high ROI. Whereas romance scams are the long con, BEC attacks often yield a similar amount of money in hours—not months.

The tactics Scarlet Widow uses to send their BEC campaigns are quite basic. The group's modus operandi, which has stayed incredibly consistent over time, consists of sending a generically-worded email to targeted victims from a temporary email where the display name is set to an impersonated executive. To date, we have identified 33 different email accounts used by the group to distribute their BEC scams. A list of these email addresses can be found in *Appendix A*.



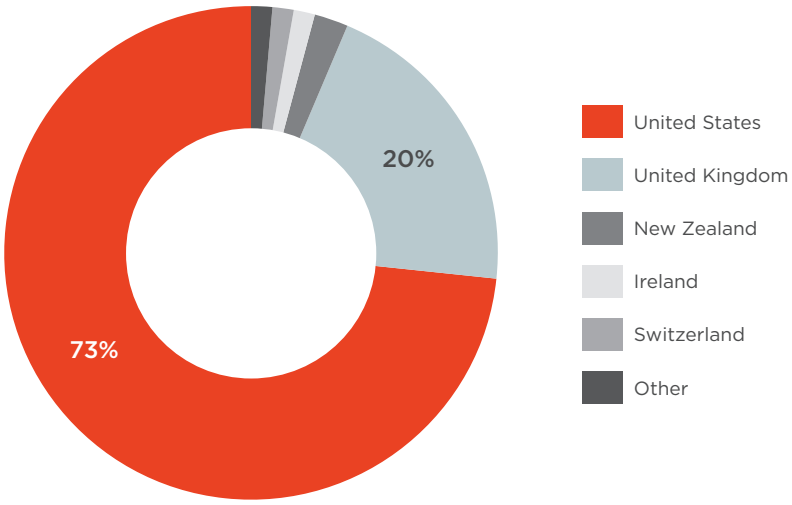

Examples of BEC Emails Sent by Scarlet Widow

# Easy Targets, Easy Money:
## Scarlet Widow's Targets

Since November 2017, Scarlet Widow has gathered targeting information for more than 30,000 individuals associated with more than 13,000 organizations in 12 countries.

Nearly all of the leads collected by Scarlet Widow were for employees located in two countries—with 73% in the United States and 20% in the United Kingdom.

Individuals Targeted by Scarlet Widow by Country




## Targeting Nonprofits

Scarlet Widow has actively targeted the nonprofit sector with their phishing campaigns. More than a quarter of the companies the group has collected targeting information for are charities and other nonprofit organizations. The choice to specifically target these kinds of marks with BEC attacks may indicate that the group believes that they are softer targets than for-profit companies, which typically have greater email security measures in place.

Indeed, while financial institutions and category leaders in other industries have begun hardening defenses in recent years, a general latency in adoption of cybersecurity has been a growing issue in the nonprofit sector. The fundraising capabilities on which this sector depends have not always been matched by suitable protections—at least not in real time.

A review of Scarlet Widow's targeting database shows the diverse array of nonprofits targeted by the group. While the Boy Scouts of America was the nonprofit with the highest number of individual targets at 190, other organizations appear frequently in Scarlet Widow's target database. This list includes a West Coast chapter of the United Way, a nationwide anti-hunger charity, a Texas ballet foundation, a large hospital and physician group in North Carolina, a Midwest Archdiocese of the Catholic Church, a well-known annual arts festival, and numerous chapters of the YMCA.

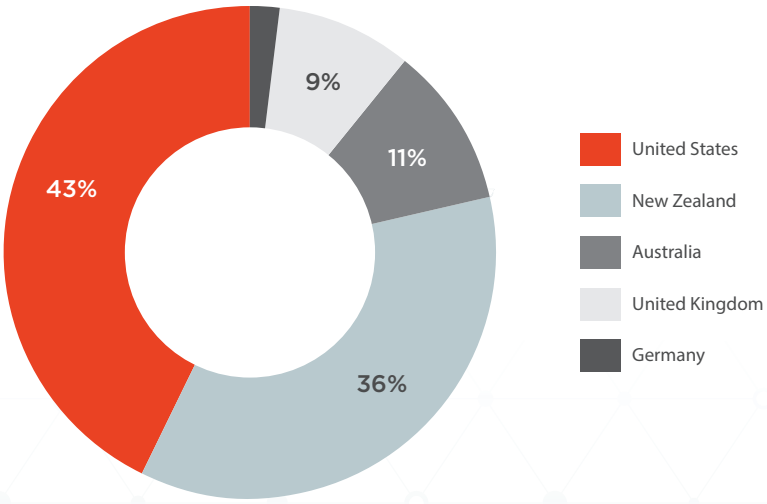
In the United Kingdom, Scarlet Widow secured email addresses for individuals at more than 1,300 large and small nonprofits, including the country's leading children's charity, a large advocacy and support group for the disabled, the national Salvation Army organization, and a family services hub for a borough of London.

It is important to note that while these nonprofits were targeted, the attacks weren't necessarily successful. Any individual email has a low probability of success—previous Agari research found a success rate of 0.37%—with the scam groups depending on a huge volume of attacks to gain a satisfactory return.

## Educational Institutions and Tax Firms Take a Hit

Another sector that Scarlet Widow has specifically targeted with focused BEC attacks is educational institutions. Scarlet Widow's targeting list included more than 1,800 individuals at 660 educational institutions, ranging from rural K-12 school districts in the United States to prominent universities in New Zealand.

Academic Scarlet Widow Targets by Country



Since September 2018, the group has aggressively targeted schools in five countries—New Zealand, the United States, the United Kingdom, Australia, and Germany—with more than 1,600 BEC attacks. Kiwi universities have made up nearly 60% of Scarlet Widow's academic targets during that timeframe.

When targeting academic institutions, Scarlet Widow's tactics change slightly. Instead of impersonating a company CEO and sending an email to a single employee, the group impersonates multiple department heads and sends attack communications to a number of different administrators and coordinators, hoping that one of them will take the bait.

Tax preparation accounting firms have also been a prime target for Scarlet Widow. These companies are attractive targets for BEC scammers looking to obtain W-2s for tax filers, especially before tax season. Over the past eighteen months, the group has collected contact information for more than 9,500 employees at more than 1,500 tax preparation firms. Most of the target data collection for these companies occurred in or around September 2018, likely in preparation for campaigns that have already launched or will launch in early 2019. With a consumer's earnings information, social security number, and other personal information in hand, a scammer can file a false return and collect an electronic refund from the IRS—making this a prime target for easy money.

| Sector | Organizations | Individuals |
|---|---|---|
| Nonprofit | 3,483 | 5,581 |
| Education | 660 | 1,815 |
| Tax Prep | 1,505 | 9,592 |

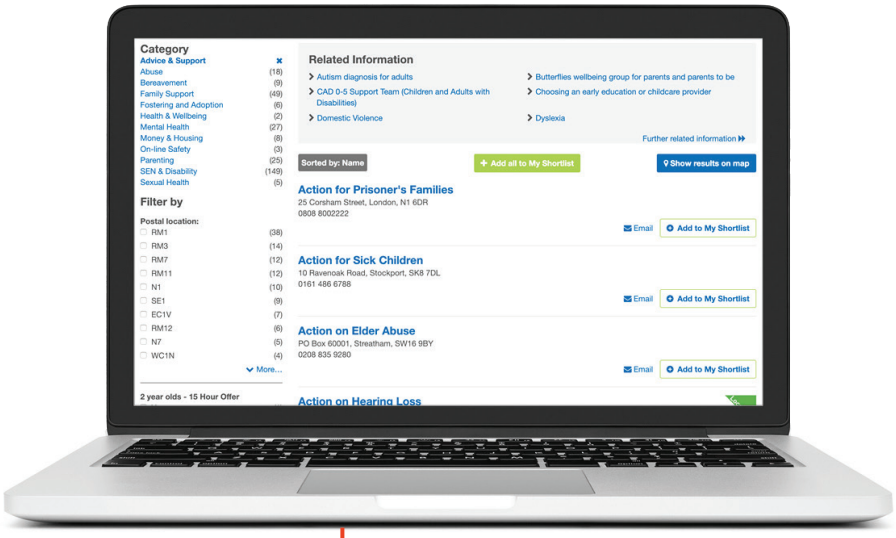
Scarlet Widow Targets since November 2017

# How Scarlet Widow Identifies Its Targets

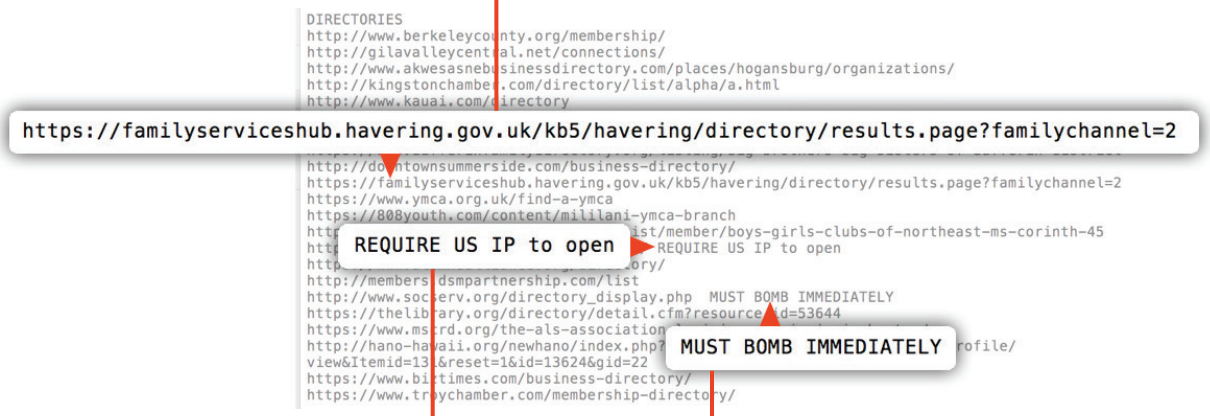
Like other email fraud operations, Scarlet Widow actively collects and shares leads among other members of its network. Similar to other BEC groups we have recently tracked, Scarlet Widow uses legitimate commercial services to identify potential targets. Since 2016, the group has used at least five different online services to collect data for future campaigns. In an effort to be cost-effective, members of the group have taken advantage of free trial periods offered by these services and used them to quickly gather leads during the few days they have access to the service.

While the groups uses commercial tools to identify individual targets within businesses, when Scarlet Widow goes after nonprofit organizations, the group primarily uses publicly-accessible websites to scrape contact information for employees. One of the artifacts that we identified during our research into the group (shown on the next page) provides insight into the tactics the group used to collect information.

Working off a list of identified websites that contain directories of nonprofit organizations, Scarlet Widow uses a web scraper to traverse the online directory and collect email addresses associated with each organization. The group refers to this process as “bombing” an online directory.




Target Online Directory for Scraping




Reminder that a US-based proxy is needed to access the directory.

"Bombing" is the term Scarlet Widow uses to refer to scraping target contact information from an online directory.

How Scarlet Widow Scrapes Target Data from Online Directories

# Laundering Dirty Gift Cards via Bitcoin

While most BEC attacks involve a scammer trying to get a victim to wire money to a mule bank account, there has been an increasing trend of BEC actors using gift cards as a primary mechanism to profit from their attacks. Gift cards are likely becoming an emerging cash out preference for cybercriminals for a number of reasons.

First, successful collaboration between industry researchers, financial institutions, and law enforcement has made the identification and mitigation of suspected mule accounts more impactful, shortening the effective lifespan of these accounts. Using gift cards, cyber threat actors are able to receive illicit funds in a way that does not come into contact with accounts that could get shut down.

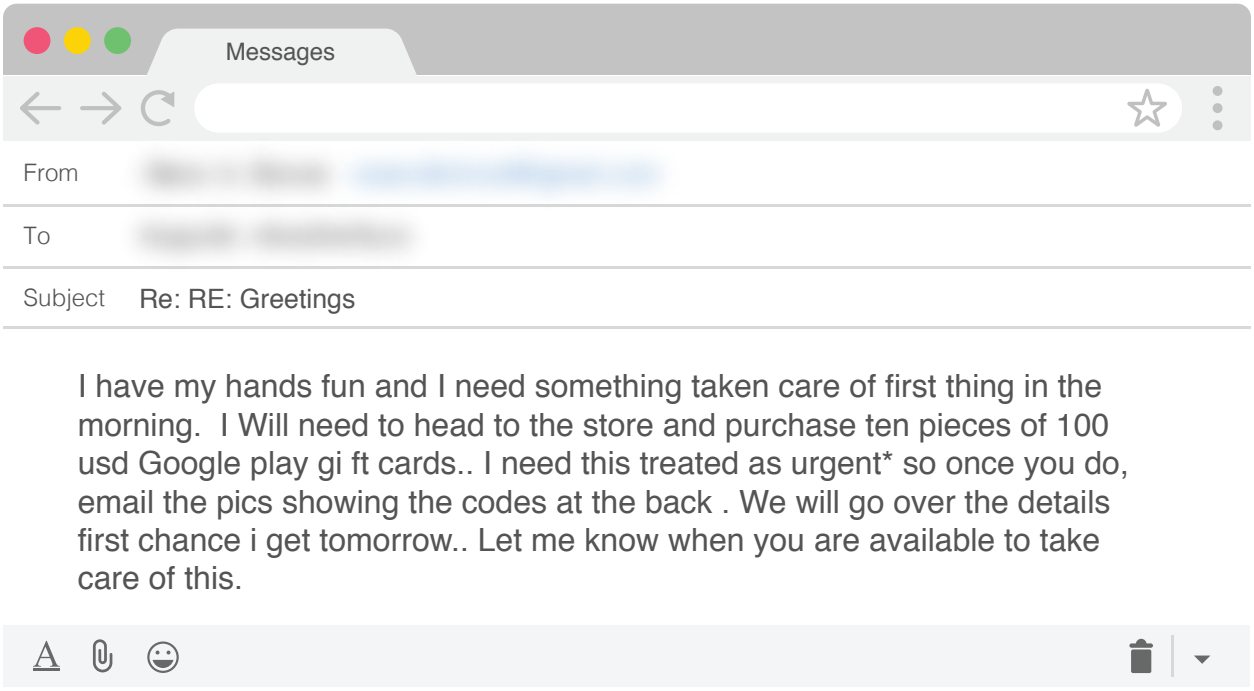
Second, by using gift cards, cybercriminals eliminate the need for a middleman to receive and redirect stolen money. Money mules are individuals that are generally located in the same country as a victim company and help a scammer launder stolen proceeds through their bank account. For their part in the scheme, money mules typically keep a percentage of the stolen funds. Using gift cards, a BEC actor is able to bypass this process and receive the stolen funds directly.

One of the biggest downsides of using gift cards as a cash out mechanism, though, is that the financial gain for an individual attack is typically significantly less than a successful wire transfer. As documented in "Behind the 'From' Lines," the average amount requested in BEC attacks using fraudulent wire transfers is $35,000. The average amount gained through a successful gift card BEC scam, on the other hand, is generally between $1,000 and $2,000.

# Packing Money Into Paxful

Mimicking the BEC threat landscape, Scarlet Widow also evolved their tactics over time. In their early days of BEC scams, Scarlet Widow's preferred technique was to request a wire transfer to a mule bank account under the auspices that a vendor invoice needed to be paid.

But in August 2018, the group's methods changed. Instead of requesting payment to a bank account, the group requested targeted victims to purchase multiple Apple iTunes or Google Play gift cards. While this certainly does not encompass the totality of successful attacks perpetrated by the group, we have directly observed more than $15,000 in gift cards obtained through BEC attacks linked to Scarlet Widow.




Example of a Scarlet Widow BEC Email Requesting Gift Cards

Our observation of Scarlet Widow's 2018 shift to gift cards mirrors findings from a 2018 report from the U.S. Federal Trade Commission. From January through September 2018, gift cards and reload cards were the payment method in 26% of fraud reports, up from just 7% in 2015. "Con artists favor these cards because they can get quick cash, the transaction is largely irreversible, and they can remain anonymous," the FTC noted. Among those who paid a scammer with a gift or reload card, 42% used iTunes or Google Play cards, according to the report.

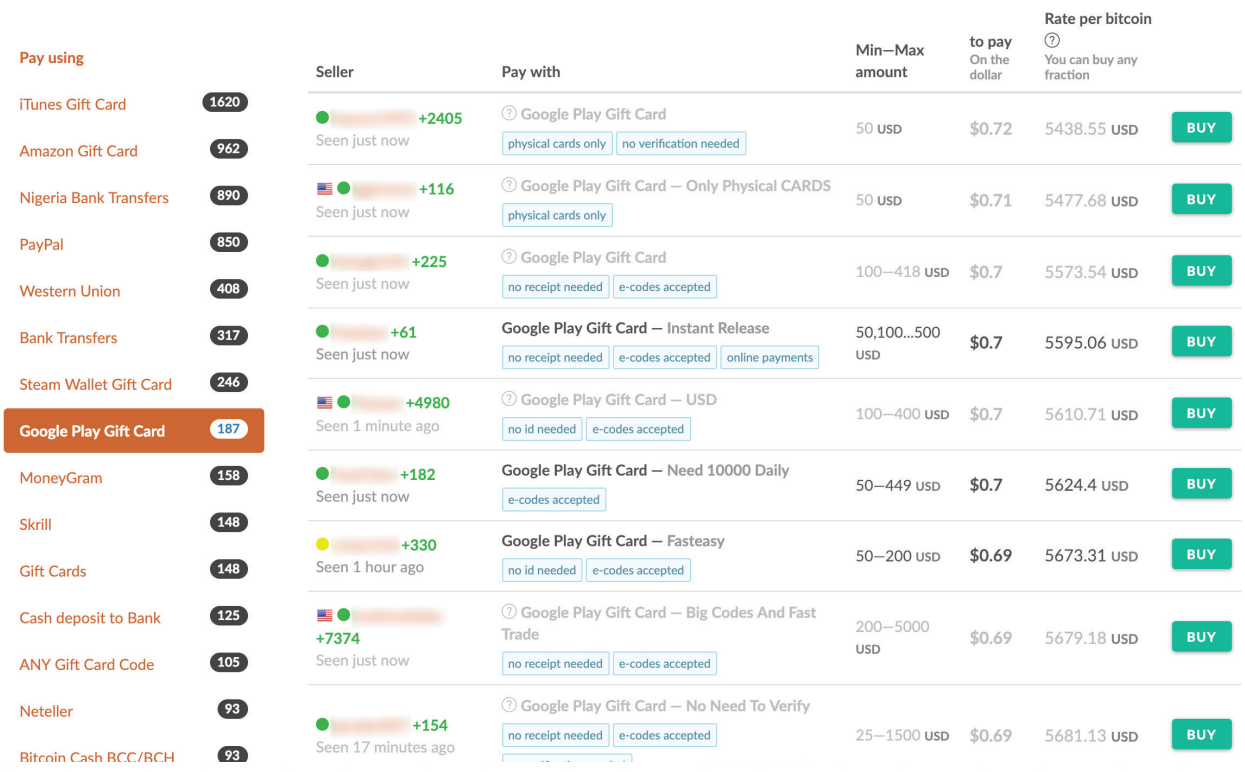
Of course, cybercriminals do not actually want a stash of gift cards, as their ultimate goal is to pad their bank account with actual money. So how do scammers convert these gift cards into cash? Our visibility into Scarlet Widow's operational processes has given us significant insight into how BEC groups launder gift cards through online services.

# Using Legitimate Online Services to Launder Stolen Money

The primary service Scarlet Widow uses to monetize gift cards is Paxful. Paxful is a US-based peer-to-peer marketplace that allows users to buy bitcoin from other users using hundreds of different payment methods, including dozens of different types of gift cards. To trade gift cards on Paxful, though, sellers take a significant hit when it comes to exchange rate. For example, most Apple iTunes gift cards are traded at 40 to 80 cents on the dollar.

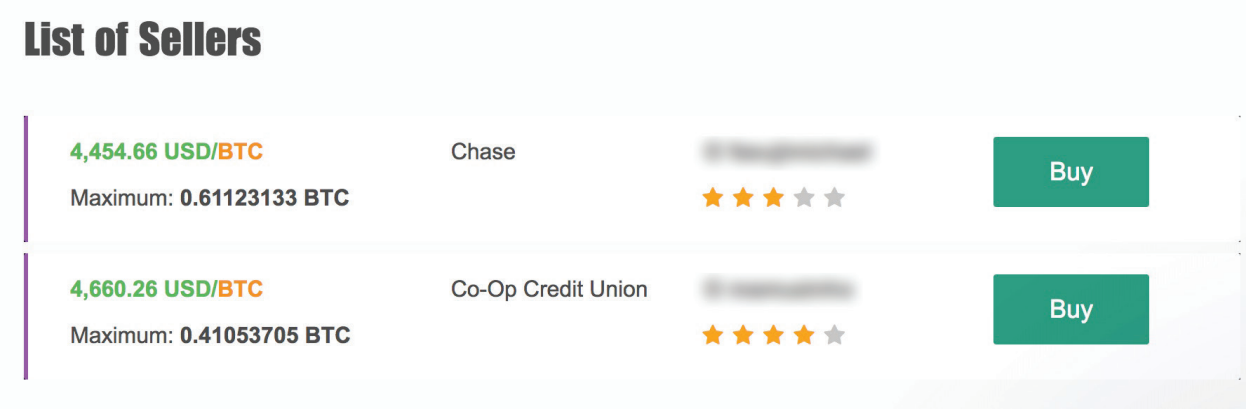
Paxful recently told the online media outlet CoinDesk that it averaged $21 million a week in transactions in 2018—up from $8.5 million in 2017. It attributed the growth in part to its user base nearly tripling in Ghana and more than doubling in Nigeria to more than 300,000 accounts. In fact, African users make up nearly 35% of all Paxful accounts.

Paxful portrays itself as bringing financial services to the world's unbanked, and perhaps they are, but the US-based company has become a bazaar for West African scam artists selling stolen gift cards, as evidenced by our research into Scarlet Widow and other Nigerian-based cybercriminal organizations.



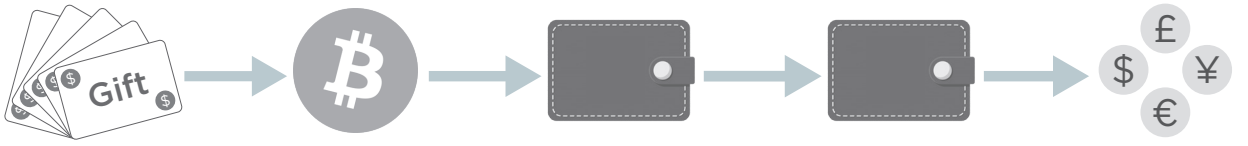

Gift Cards Being Traded on the Paxful Website

After a gift card has been traded for bitcoin, the funds are deposited into a wallet, but the cryptocurrency still needs to be converted into cash. To do this, Scarlet Widow moves bitcoin from their Paxful wallet to a wallet on another peer-to-peer cryptocurrency exchange: Remitano. On Remitano, users are able to advertise their bitcoin for sale and a buyer can purchase the Bitcoin for a specified price via bank transfer.



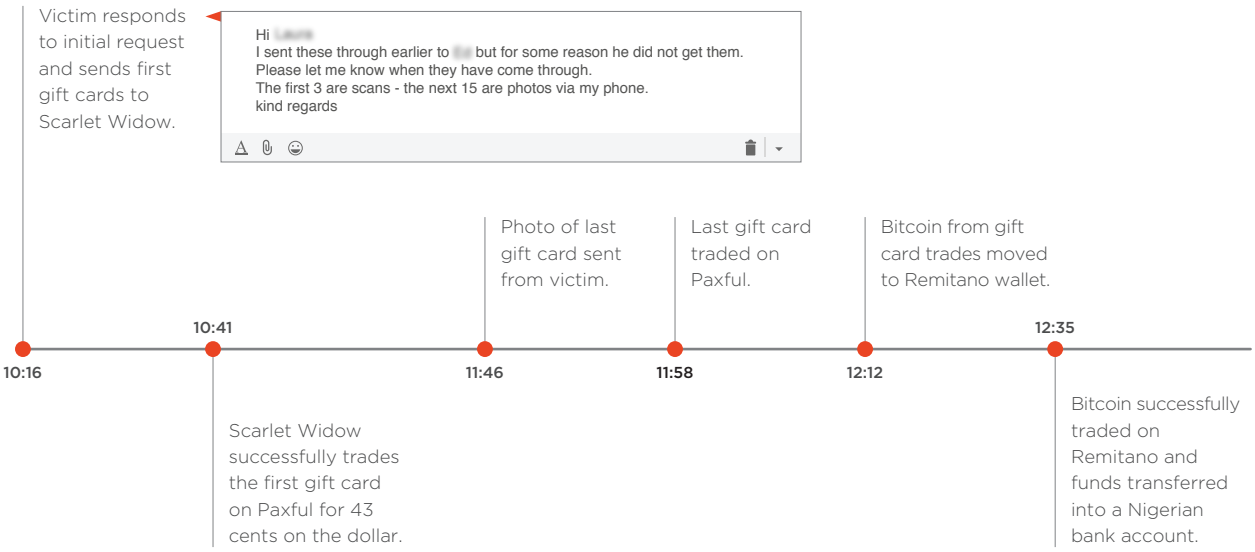

Example of Bitcoin Being Offered for Sale on Remitano

Once the Scarlet Widow actors have exchanged their bitcoin and the buyer's funds are in their bank account, the process of converting illicit gift cards into cash is complete.



# Gone in 120 Minutes

In August 2018, Scarlet Widow successfully attacked an Australian university, a transaction that demonstrates the speed at which group completes the laundering process. Thinking she had received a request from the head of the university's Finance Department, an administrator was tricked into buying $1,800 in Apple iTunes gift cards and sending pictures of the redemption codes to Scarlet Widow. What is fascinating is that we see that upon receiving the gift cards, the group was trading them on Paxful in near real-time. The entire process, from receipt of the first gift card to transferring cash into a bank account, took less than two-and-a-half hours.




In all, $1,800 in Apple iTunes gift cards were converted to $700 in Bitcoin and laundered into a Nigerian bank account in 2 hours, 19 minutes.

# Conclusion

This report demonstrates that cybercriminal fraud rings continue to evolve, and represent a significant financial threat to organizations in every sector across the globe. Scarlet Widow's use of professional prospecting tools, combined with dark web assets, forms the foundation for attacks that easily bypass the email security controls most organizations have in place today. As the criminal element follows the money, these groups will continue to search for new ways to reap large sums through hacking the biggest weakness in any organization's defenses: human beings.

# Appendix A – Email Addresses Associated with Scarlet Widow BEC Attacks

admin@exeoffice.net
beetimes@office01.org
boardgroup@inbox.lv
ceooffice@priateoffice.net
ceooffice0012@comcast.net
ceooffice0212@comcast.net
ceooffice4566@comcast.net
contact@exeoffice.net
contact@officeexe.com
contact@priatemail.com
dept-head@runbox.com
dept-head01@mailbox.org
directivegroup@inbox.lv
director101@comcast.net
directorsoffice@reagan.com
directorsoffice@runbox.eu
discreet@exeoffice.net
execgroup@inbox.lv
execoffice@runbox.com
execofschool@gmail.com
executive.office@comcast.net
executiveceo00@comcast.net
executivemail01@comcast.net
executiveoffice018@comcast.net
info@exeoffice.net
io0oi1@officeexe.com
james.barnes@mailfence.com
Joshy45@exeoffice.net
matthwtyler@comcast.net
mattmatt@exeoffice.net
private@officeexe.com
support@exeoffice.net
vp@shoppingexperience.org

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