AGARI CYBER
INTELLIGENCE DIVISION

THREAT ACTOR DOSSIER

Exaggerated Lion

How an African Cybercrime Group Leveraged G Suite and a Check Mule Network to Build a Prolific BEC Operation

Executive Summary

Business email compromise (BEC) has grown into a billion dollar industry as cybercriminals use look-alike domains and display name deception to trick employees into revealing sensitive information or depositing money into criminally-owned bank accounts. When they can compromise a legitimate email account and use it to send malicious messages, the success rate becomes even greater. And cybercriminals are taking advantage, to the tune of more than $700 million every month.

The Agari Cyber Intelligence Division (ACID) has identified an African cybercriminal organization, which we call Exaggerated Lion, that has been active since at least 2013. Comprised of actors in Nigeria, Ghana, and Kenya, Exaggerated Lion was a prolific check fraud ring before evolving to BEC attacks starting in mid-2017. Since April 2019, we have conducted more than 200 active defense engagements against Exaggerated Lion actors. Our visibility into Exaggerated Lion's operations as a result of these engagements has given us an in-depth look at how their BEC attacks unfold and have evolved over time.

One of the most intriguing aspects of Exaggerated Lion's BEC attacks is their clear preference to use physical checks as a cashout method rather than wire payments, which makes them unique in the BEC threat landscape. The group's history of check fraud and romance scams has resulted in a vast network of check mules across the United States. Over the course of our research into Exaggerated Lion, we have uncovered the identities and locations of 28 check mules, including seven "Tier I" mules who are long-standing romance scam victims that are trusted with large sums of money and interact more extensively with the main Exaggerated Lion actors.

During our research, we identified more than 3,000 individuals employed by nearly 2,100 companies that had been targeted by Exaggerated Lion BEC campaigns between April 2019 and August 2019. All of these targets were located in the United States, in 49 of 50 states and the District of Columbia, an indication of Exaggerated Lion's square focus on American targets.

Over the course of our engagements with Exaggerated Lion, the group evolved their tactics and started using fake invoices and W-9s to inject a sense of authenticity into their attacks. The invoices were created using an easily accessible free invoice generator and the W-9 forms were obtained from the Internal Revenue Service's public website. Since these documents are commonly used in legitimate business transactions, including them gives Exaggerated Lion's attacks a better chance of succeeding without any questions being asked.

Another unique characteristic of Exaggerated Lion's BEC attacks is the use of very long domain names hosted on G Suite containing words that give the appearance that an email was sent from secure infrastructure. Our research has uncovered more than 1,400 domains used by Exaggerated Lion since July 2017 that have been used to launch BEC campaigns. Domains registered by Exaggerated Lion actors comprise more than 10% of all .MANAGEMENT domains that have ever been created and nearly 75% of .MANAGEMENT domains registered with Google.

Table of Contents

Into the Lion's Den
How We Tracked Exaggerated Lion 4

Who is Exaggerated Lion?
A Look Behind the Curtain 7

Checking the Box
How Exaggerated Lion Uses Checks as a Cashout Method 9

Faking it to Make it
How Exaggerated Lion Leverages Fake Documents 13

Putting the "Exaggerated" in Exaggerated Lion
A Look at Exaggerated Lion's BEC Infrastructure 16

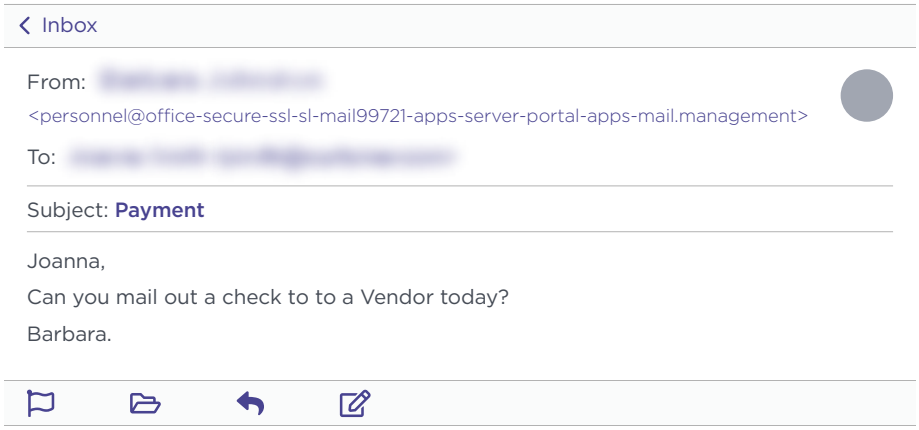
Conclusion
Protecting Yourself Against Lions (and Tigers and Bears) 19

Into the Lion's Den

How We Tracked Exaggerated Lion

Every single day, researchers in the Agari Cyber Intelligence Division engage with dozens of BEC scammers who have tried (and failed) to target our customers. In doing so, we collect rich intelligence that allows us to better understand cybercriminal group operations, discover and track the evolution of their methods over time, unravel the financial infrastructure they use to launder stolen proceeds, and uncover the identities of those involved in the criminal schemes.

Exaggerated Lion is a group that we first started engaging with in April 2019 when we observed an attempted attack targeting an Accounts Payable Specialist at an Agari customer impersonating the company's CEO. Like most BEC attacks, the initial email message was brief and was meant to elicit a response from the target. In this case, the attacker wanted to know if a check could get mailed out to a "vendor."



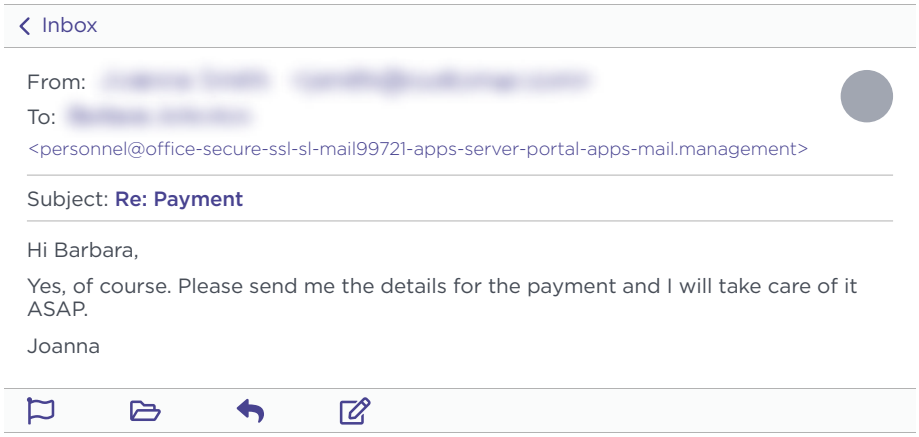
A few things stuck out in this initial message which caught our attention.

First, the domain registered by the attacker to send the initial email was long and quite unique. While it clearly was not mimicking the customer's domain, it seemed to be constructed to appear to come from secure infrastructure.

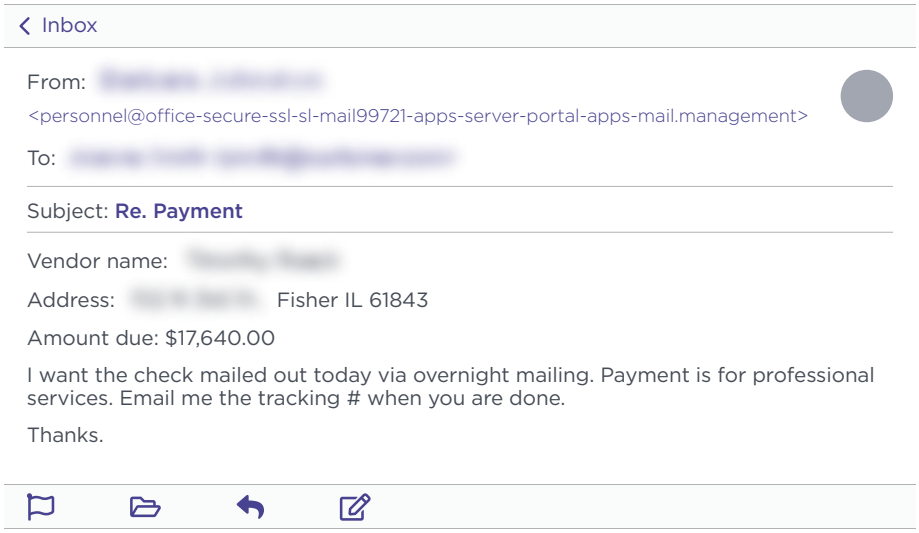
The second aspect of this email that interested us was the request for a physical check to be mailed rather than an electronic wire payment, which is the predominant method requested by BEC scammers in attacks requesting direct payments.

Because of these unique attributes, we decided to conduct a more in-depth engagement with the attacker to learn more about them. We re-crafted a new email conversation with the scammer from a separate persona account, creating new identities for a fake CEO and Accounts Payable Specialist, while recycling the rest of the original email.

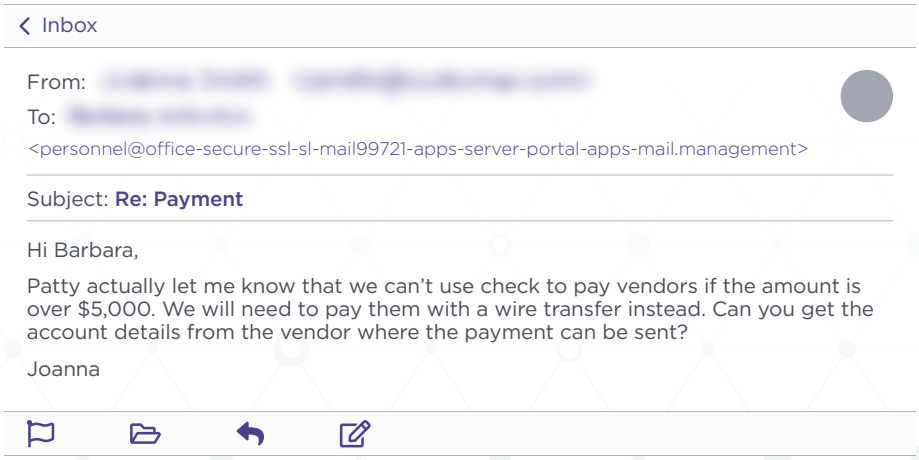
Using this new persona, we responded to the attacker, letting him know that we would, of course, be happy to help him out with his request.



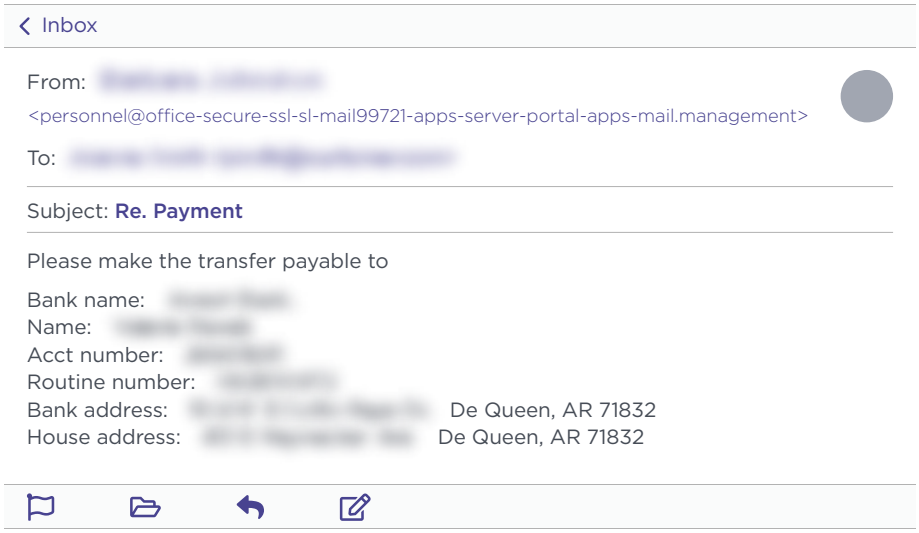
Shortly after sending this email, the Exaggerated Lion actor responded with the name and address of the "vendor" where the $17,640 check should be sent.



Of course, we weren't going to send a check to the scammer's mule, so we informed him that our "CFO" notified us that we will need to send the payment using a wire transfer instead.



Without missing a beat, the scammer quickly replied with the account details for a second mule.



Like other active defense engagements we conduct, we kept the scammer on a leash, continually coming up with a variety of excuses about why our payment attempts kept failing. Using these tactics, we coaxed the scammer to reveal more and more mule accounts that we can then provide to financial institutions for mitigation.

While this was the first interaction we had with Exaggerated Lion, it certainly wasn't the last. Since April 2019, we have conducted more than 200 active defense engagements against Exaggerated Lion actors, which has resulted in the identification of 48 mule accounts used by the group and the identities and locations of 28 check mules, which we have passed to financial partners and law enforcement.

In addition to actively engaging with Exaggerated Lion actors, we used various tools and tactics that allowed us to gain significant insight into the group's background, methods, and primary actors. What follows is an overview of what we discovered during our investigation into Exaggerated Lion.

Who is Exaggerated Lion?

A Look Behind the Curtain

Exaggerated Lion is a cybercriminal organization that has been running scams since at least 2013. Unlike most other BEC organizations we've researched that are centrally located in Nigeria, Exaggerated Lion's primary associates are spread around multiple countries in Africa, including Nigeria, Ghana, and Kenya.

Prior to getting into the BEC game in mid-2017, Exaggerated Lion built a solid foundation of criminal activity, becoming a prominent fixture in the check fraud landscape. Starting in 2014, Exaggerated Lion began their check fraud schemes on Craigslist, using a variety of rental and marketing scams. As the years progressed, Exaggerated Lion's check fraud scams became more sophisticated.

A common check fraud scheme Exaggerated Lion has used for years revolves around the use of a car wrap service. As part of this scam, an Exaggerated Lion actor posts an advertisement on a website or sends emails out to a curated list of recipients with an offer to have the recipient wrap their car with marketing decals for a variety of beverage companies, and in exchange, the recipient would received a fixed amount of money each week. For recipients that responded to Exaggerated Lion's ad, the group would send them a (fake) check that covered the recipient's first month's pay and the money that would get paid to a "specialist" that would come out to wrap the car. After depositing the check, the "employee" (i.e., victim) was told to keep the first month's pay and send the remainder to the specialist via a money order or Western Union. Of course, this specialist did not exist and the money was actually being sent to a money mule or the scammers themselves.

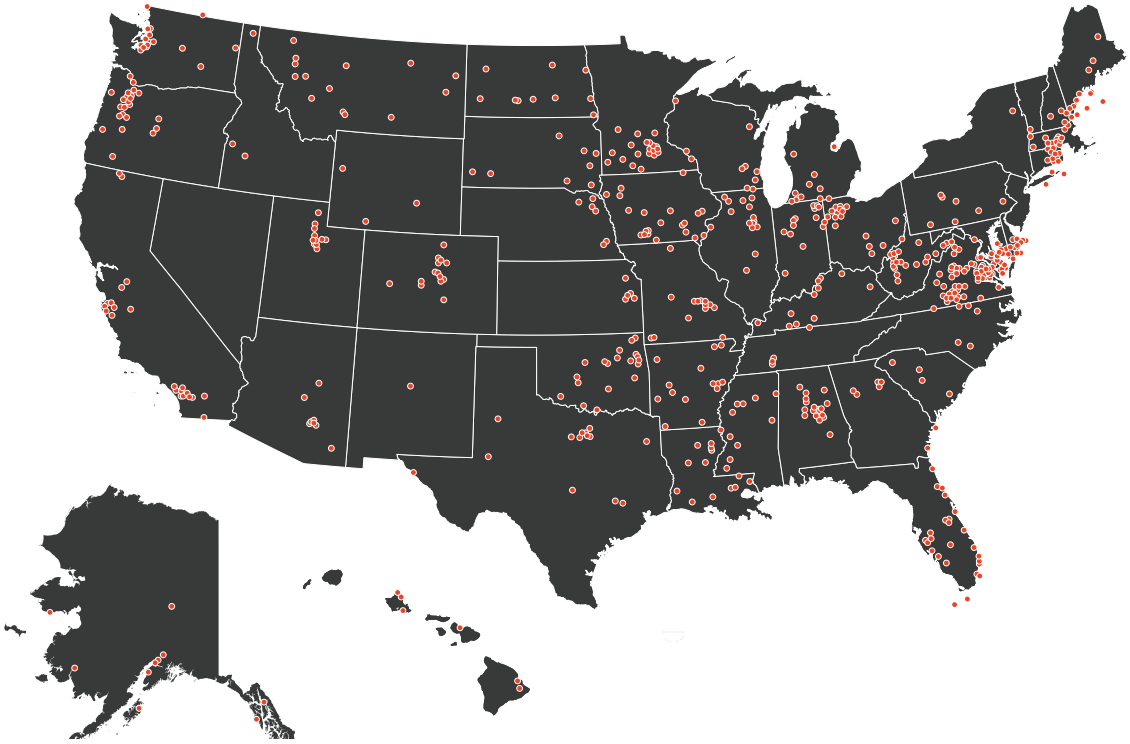
Over the past five years, Exaggerated Lion has sent out thousands of fake checks adding up to millions of dollars in fraudulent funds using this scheme and others like it. As we'll see later in this report, Exaggerated Lion's experience and comfort with checks greatly influenced their tactics once they moved into the world of BEC.

> [redacted] will take full responsibility for placing and remove decal on your car and it will not resort to any damage. Also we have OUT-SOURCED the payment of funds to you to another Agency, so please do not be alarmed by the payment not coming directly from [redacted] Note that a start-up check of $1850 Check payment will be sent to you to cover your first week salary of $700 and also the Specialist fund will be included, Your up front payment would made after you have sent a reply with answer to the questions above and a confirmation email saying we should go ahead and mail out funds and I will like you to send the pictures of the vehicle.

Sample excerpt from an Exaggerated Lion car wrap scam.

During our research, we identified more than 3,000 individuals employed by nearly 2,100 companies that had been targeted by Exaggerated Lion in BEC campaigns between April 2019 and August 2019. While we don't believe this is by any means the totality of Exaggerated Lion's target set during this period, it does give us a good glimpse of where their preferred targets are located. A vast majority of the targets identified held a title that indicates they work in the accounts payable department of an organization. The use of keywords in an employee's title is a common way BEC groups quickly identify targets that are likely to handle transactions they are trying to exploit. While Exaggerated Lion's search terms clearly include "Accounts Payable," we have seen similar keyword searches from BEC groups to identify CFOs and Controllers.

All of these targets were located in the United States, in 49 of 50 states, as well as the District of Columbia. Because the group's preferred cashout method is physical checks, the singular focus on American targets is not surprising, since the use of checks has become much less common in other parts of the world.



Map showing the locations of 3,000 Exaggerated Lion targets

Checking the Box

How Exaggerated Lion Uses Checks as a Cashout Method

One of the most intriguing aspects of Exaggerated Lion's BEC attacks is their clear preference for a victim to send physical checks rather than wire payments, which makes them unique in the BEC threat landscape and is a reflection on the group's long-standing experience in check fraud.

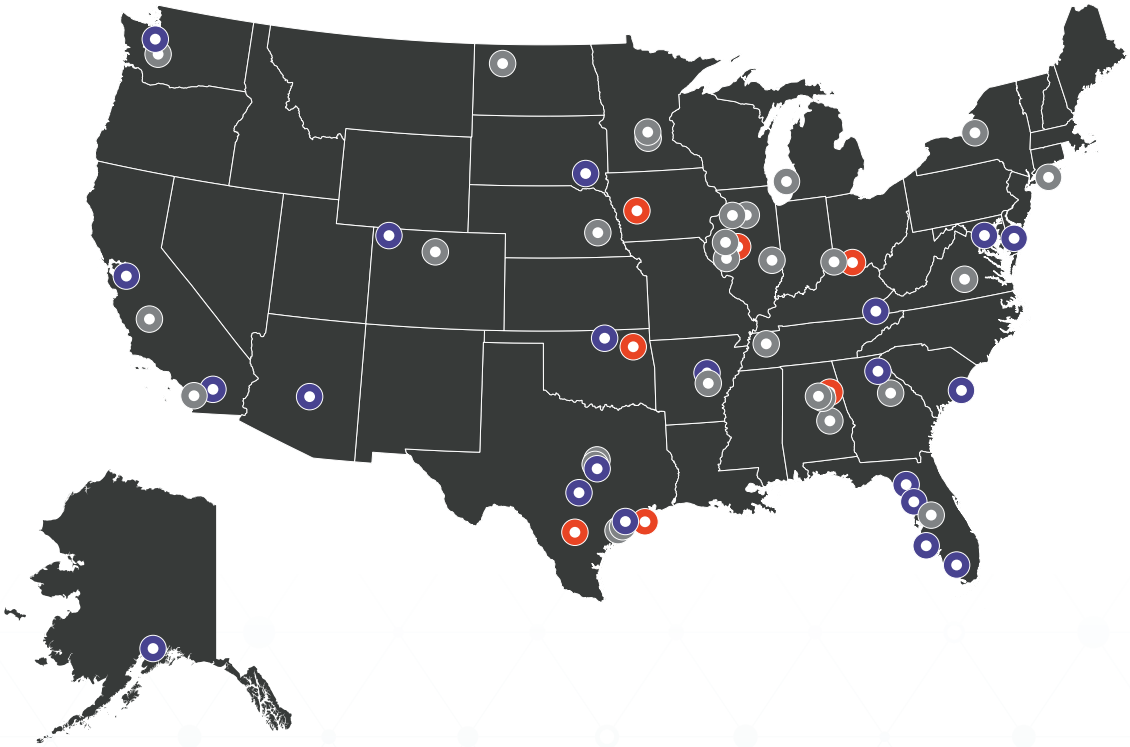
Based on our observations, Exaggerated Lion's network of check mules is primarily comprised of romance scam victims that are likely unwitting to their involvement in a criminal scheme. Instead, these romance-victims-turned-money-mules are told they are helping their romantic partner recover a large inheritance that is tied up with lawyers and is being distributed slowly over time.

Exchange between Exaggerated Lion actor and check mule about fake inheritance.

Our research indicates there are two distinct tiers of mules that Exaggerated Lion uses to receive checks from BEC victims.

Tier I mules are long-standing romance scam victims who are completely invested in their "relationship" with a fictitious Exaggerated Lion persona and have built up a significant amount of trust. They are trusted with larger amounts of money and are usually the ones responsible for sending money directly to the scammers overseas. These mules are comfortable opening new bank accounts and moving funds around to assist Exaggerated Lion actors without questioning why. Due to the level of indoctrination, Tier I mules have difficulty seeing through the fact that they are being scammed, even when presented with evidence that what they are doing is considered fraud. In some cases, these mules will even tell their handler about meeting with law enforcement if they are questioned about their potential involvement in fraudulent activity.

Tier II mules, on the other hand, are the lower tier of mules that are newer to the network and have not developed enough rapport to be trusted with significant components of the BEC process. They are only trusted with smaller amounts of money and instead of sending funds directly to the scammers, they are usually instructed to pass money to other Tier I mules that act as an intermediary. Sometimes, Exaggerated Lion sent Tier II mules fake checks and told them to cash them at the bank, much like the group's classic check fraud schemes, as a way to test the mule's willingness to go along with potentially suspicious requests.

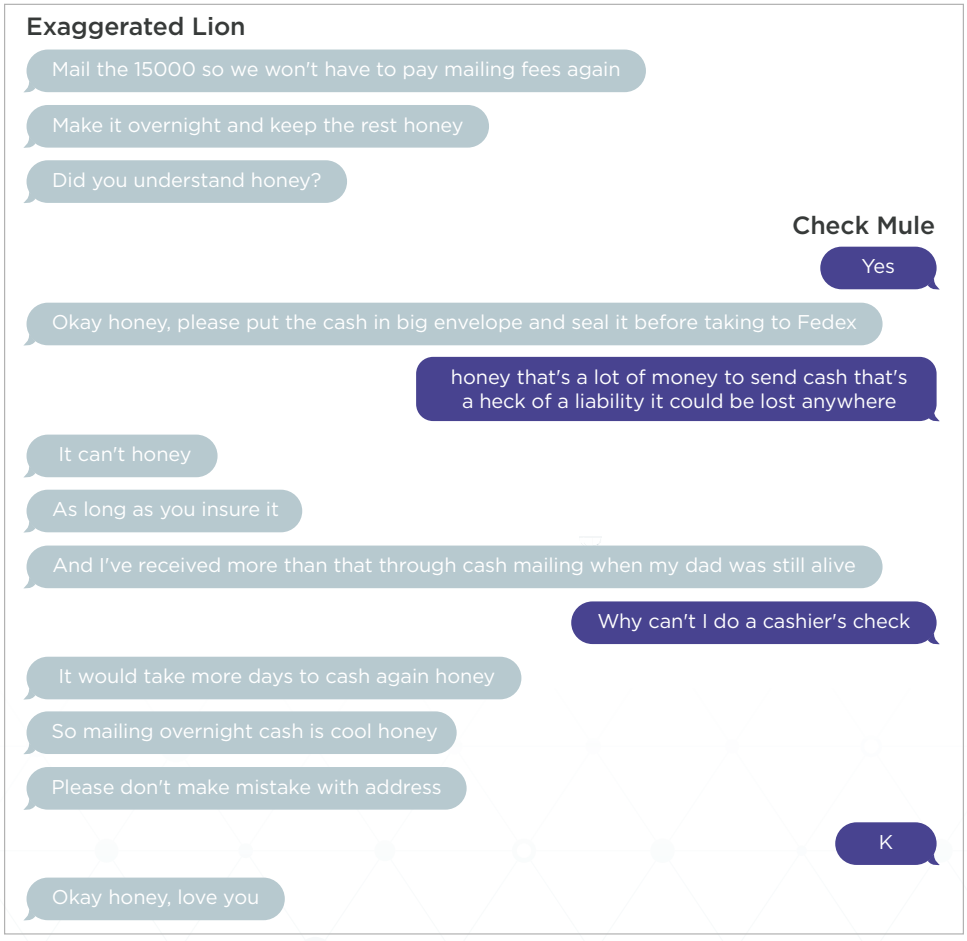


Map of Exaggerated Lion mules in the United States.
Red = Tier I Check Mule, Blue = Tier II Check Mule, Gray = Wire Transfer Mule

So once a company is tricked into sending a check to a "vendor," how does that money get back to the scammer?

Once the check has reached a mule, the check is deposited into a bank account owned by the mule. Because these checks are completely legitimate, they are able to get deposited without any issues, although there are times when the deposit is held for a few days in order to verify the authenticity of the check.

After the check has been successfully deposited into a mule's account, the next step is to get the money to the Exaggerated Lion scammer. As we mentioned previously, if the the money starts with a Tier II mule, Exaggerated Lion will usually ask the mule to send it to a Tier I mule, usually under the guise that the other mule is an inheritance attorney or a client of the scammer, and keep a little money for themselves. A Tier II mule usually sends money to a Tier I mule using a cashier's check or bank transfer, but we have also observed instances where an Exaggerated Lion actor tells a mule to withdraw cash from their account and send it through the mail. In one case, Exaggerated Lion instructed a mule to send $15,000 in cash to another mule via FedEx, which the mule had serious reservations about.



Exaggerated Lion and check mule conversation about sending $15,000 through the mail.

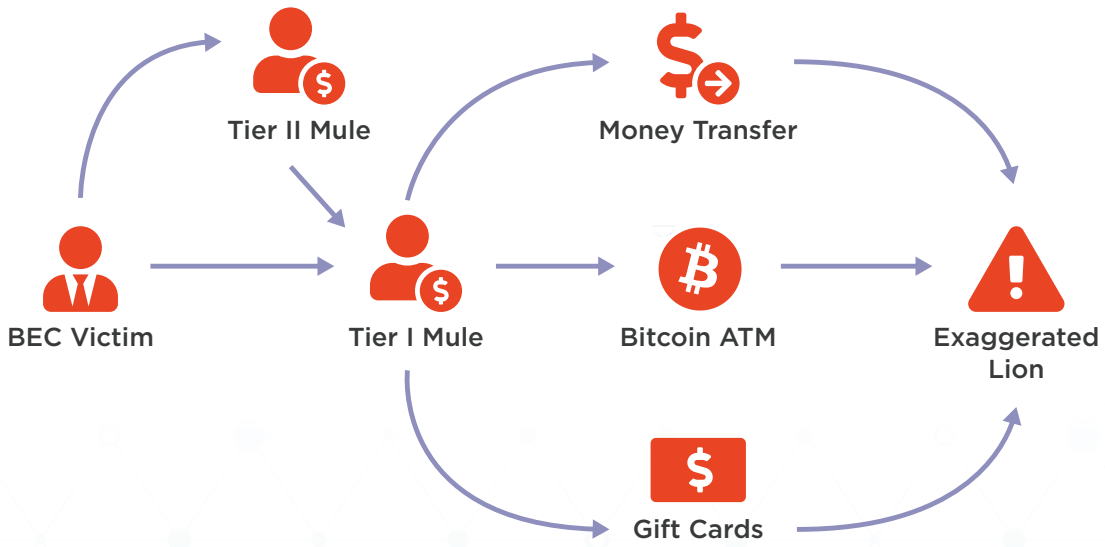
Now that the money has reached a Tier I mule, the next step is to get it into the hands of Exaggerated Lion, which we have observed getting accomplished in a variety of ways.

The first, and most efficient method, is to send funds directly to Exaggerated Lion via Western Union or MoneyGram money transfers. These services have been used by West African scammers for years in a variety of different types of scams. While this is the most direct method of getting money to the scammers, it is also the most risky since these companies are becoming more proactive in identifying potentially suspicious transfers and educating people about fraud risks when they send money overseas.

Another way Exaggerated Lion gets their money is by instructing mules to transfer the money to a bitcoin wallet via a bitcoin ATM machine. Similar to regular ATMs, bitcoin ATMs allow users to deposit and withdraw cash from a bitcoin wallet. The rationale provided by Exaggerated Lion is that they want to avoid "unnecessary bank fees" or "lawyer fees" by not using a regular bank transfer. Once the money has been deposited into a bitcoin wallet, Exaggerated Lion is able to easily transfer the funds to their own bank accounts using a number of different online methods.

The third method used by Exaggerated Lion to launder money through mules is to use gift cards. Mules are told to go purchase a number of specific types of gift cards, expose the code on the back of the cards, and send them pictures of the backs of the cards. Once Exaggerated Lion has received pictures of the cards, they are likely converted to cash through online cryptocurrency exchanges, similar to how cards are laundered in gift card BEC attacks.

By using all of these different types of transfer methods, Exaggerated Lion is likely attempting to evade anti-money laundering efforts.

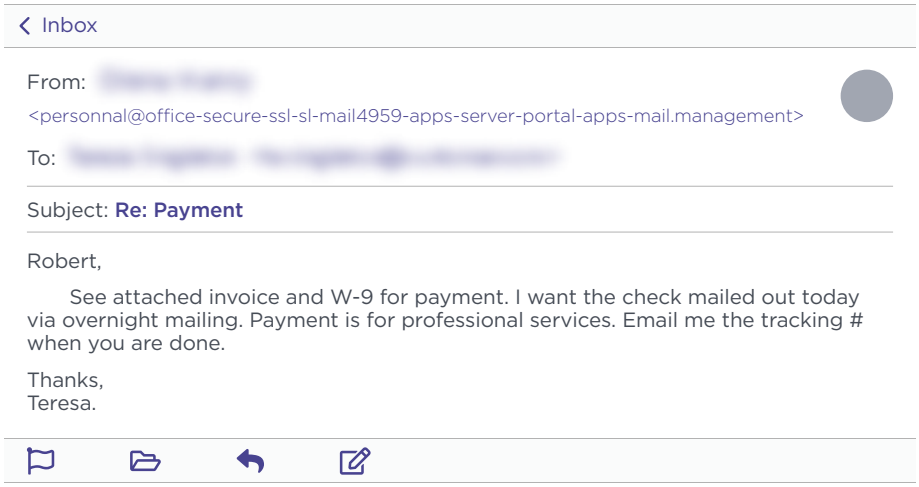


Exaggerated Lion cash out methods.

Faking it to Make it

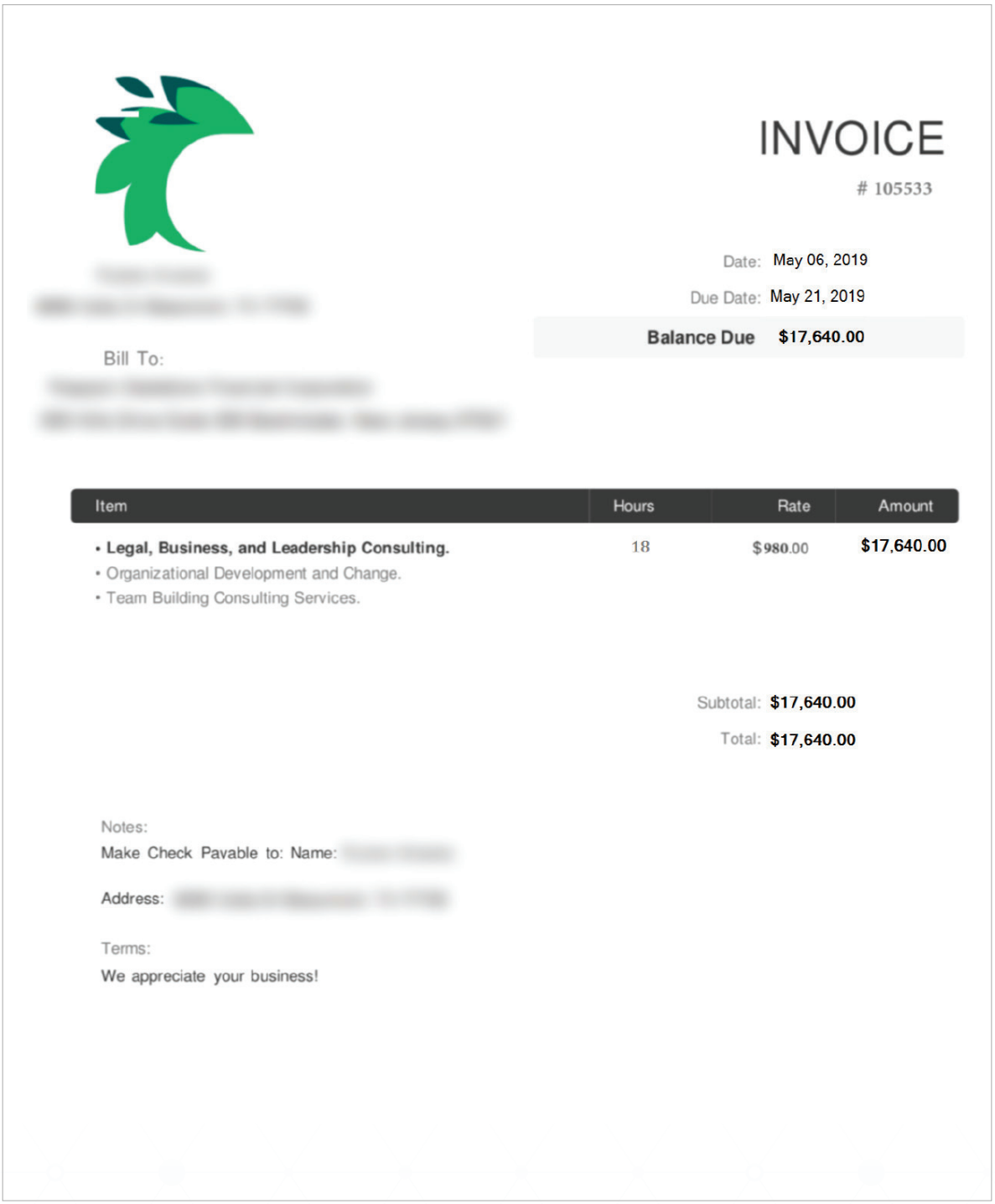
How Exaggerated Lion Leverages Fake Documents

As we continued our engagements with Exaggerated Lion, the group evolved their tactics and started using fake invoices and W-9s to add legitimacy to their attacks. Since these documents are commonly used in authentic business transactions, including them gives the fraudulent request a better chance of succeeding without any questions being asked.



The fake invoices were created using a free invoice generator that can be easily found using a basic Google search. All the Exaggerated Lion actors needed to do was plug in the details for the target company, the mule's contact details, some fake services the "vendor" was supposed to have provided, and the price for the fictional services. The online generator then compiles the details into a legitimate-looking PDF invoice. While Exaggerated Lion generally refers to the payments being meant for "professional services" in their email communications, their fake invoices usually refer to the services rendered as "Legal, Business, and Leadership Consulting."

A W-9 form is used by employers to collect the details of employees or contractors for income-reporting purposes. Fillable versions of the W-9 form are publicly available on the Internal Revenue Service website, which is likely where Exaggerated Lion obtained their copy; however, none of the forms we have observed are current. Most of the W-9 forms used by Exaggerated Lion are from 2017 and some are as old as 2014. In addition to providing a mule's name and address on the W-9 form, Exaggerated Lion also includes the mule's actual social security number on the form, which is notable because it could easily be faked since it's not needed to issue a check for services.



INVOICE

105533

Date: May 06, 2019

Due Date: May 21, 2019

Balance Due **$17,640.00**

Bill To:

Item	Hours	Rate	Amount
• **Legal, Business, and Leadership Consulting.** • Organizational Development and Change. • Team Building Consulting Services.	18	$980.00	**$17,640.00**

Subtotal: **$17,640.00**

Total: **$17,640.00**

Notes:

Make Check Payable to: Name:

Address:

Terms:

We appreciate your business!

Example fake invoice used by Exaggerated Lion.

Form **W-9**
(Rev. November 2017)
Department of the Treasury
Internal Revenue Service

Request for Taxpayer Identification Number and Certification

▶ Go to *www.irs.gov/FormW9* for instructions and the latest information.

Give Form to the requester. Do not send to the IRS.

Print or type. See Specific Instructions on page 3.

1 Name (as shown on your income tax return). Name is required on this line; do not leave this line blank.

2 Business name/disregarded entity name, if different from above

3 Check appropriate box for federal tax classification of the person whose name is entered on line 1. Check only **one** of the following seven boxes.

☒ Individual/sole proprietor or single-member LLC ☐ C Corporation ☐ S Corporation ☐ Partnership ☐ Trust/estate

☐ Limited liability company. Enter the tax classification (C=C corporation, S=S corporation, P=Partnership) ▶ _____

Note: Check the appropriate box in the line above for the tax classification of the single-member owner. Do not check LLC if the LLC is classified as a single-member LLC that is disregarded from the owner unless the owner of the LLC is another LLC that is **not** disregarded from the owner for U.S. federal tax purposes. Otherwise, a single-member LLC that is disregarded from the owner should check the appropriate box for the tax classification of its owner.

☐ Other (see instructions) ▶

4 Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3):

Exempt payee code (if any) _____

Exemption from FATCA reporting code (if any) _____

(Applies to accounts maintained outside the U.S.)

5 Address (number, street, and apt. or suite no.) See instructions.

Requester's name and address (optional)

6 City, state, and ZIP code

7 List account number(s) here (optional)

Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN*, later.

Note: If the account is in more than one name, see the instructions for line 1. Also see *What Name and Number To Give the Requester* for guidelines on whose number to enter.

Social security number

[redacted] – [redacted] – [redacted]

or

Employer identification number

–

Part II Certification

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
2. I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
3. I am a U.S. citizen or other U.S. person (defined below); and
4. The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.

Sign Here Signature of U.S. person ▶ [redacted] Date ▶ 04/15/2019

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

Future developments. For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to *www.irs.gov/FormW9*.

Purpose of Form

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS must obtain your correct taxpayer identification number (TIN) which may be your social security number (SSN), individual taxpayer identification number (ITIN), adoption taxpayer identification number (ATIN), or employer identification number (EIN), to report on an information return the amount paid to you, or other amount reportable on an information return. Examples of information returns include, but are not limited to, the following.

- Form 1099-INT (interest earned or paid)
- Form 1099-DIV (dividends, including those from stocks or mutual funds)
- Form 1099-MISC (various types of income, prizes, awards, or gross proceeds)
- Form 1099-B (stock or mutual fund sales and certain other transactions by brokers)
- Form 1099-S (proceeds from real estate transactions)
- Form 1099-K (merchant card and third party network transactions)
- Form 1098 (home mortgage interest), 1098-E (student loan interest), 1098-T (tuition)
- Form 1099-C (canceled debt)
- Form 1099-A (acquisition or abandonment of secured property)

Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN.

If you do not return Form W-9 to the requester with a TIN, you might be subject to backup withholding. See What is backup withholding, *later.*

8.50 x 11.00 in

Cat. No. 10231X

Form **W-9** (Rev. 11-2017)

Example fake W-9 form used by Exaggerated Lion.

Putting the "Exaggerated" in Exaggerated Lion

A Look at Exaggerated Lion's BEC Infrastructure

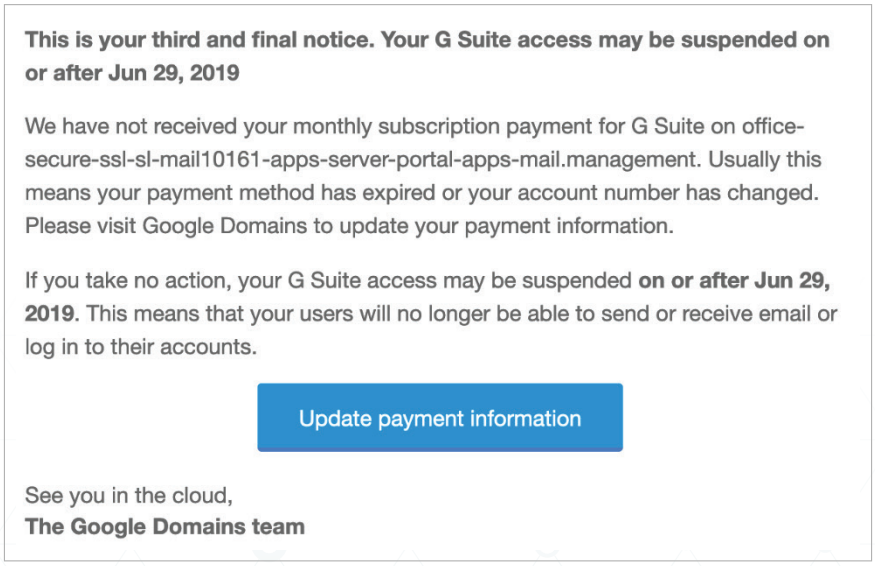
Aside from their use of checks, the other telltale sign of an Exaggerated Lion BEC attack is the unique construction of the infrastructure from where they send their emails. There are two main attributes of Exaggerated Lion's attack email accounts that make them unique: where the domains are hosted and the naming convention of the domains.

Exploiting G Suite

Exaggerated Lion displays a clear preference for using G Suite, Google's enterprise solution for cloud-based email, as a vital part of their delivery infrastructure. We have identified more than 1,400 domains used by Exaggerated Lion dating back to July 2017. Of these domains, 98% of them were registered with Google.

So why would Exaggerated Lion make a conscious choice to use G Suite to host and launch their BEC campaigns?

First, Google doesn't start charging for G Suite until after the first month. This means Exaggerated Lion can create a new G Suite account, add compromised credit card information as a payment method, and effectively have at least a 30-day free trial on each domain they set up. Sure, the compromised credit card may get reported and cut off, so they will receive warnings at the end of the month saying the domain will be suspended if the payment method is not updated, but by then, the effective lifespan of the domain has passed and Exaggerated Lion can simply move on to another account.



This is your third and final notice. Your G Suite access may be suspended on or after Jun 29, 2019

We have not received your monthly subscription payment for G Suite on office-secure-ssl-sl-mail10161-apps-server-portal-apps-mail.management. Usually this means your payment method has expired or your account number has changed. Please visit Google Domains to update your payment information.

If you take no action, your G Suite access may be suspended **on or after Jun 29, 2019.** This means that your users will no longer be able to send or receive email or log in to their accounts.

Update payment information

See you in the cloud,
The Google Domains team

Example suspension notice for an Exaggerated Lion domain.

Second, by using G Suite, Exaggerated Lion doesn't have to worry about setting up any additional infrastructure, such as an SMTP server to send emails. Everything they need is self-contained inside the G Suite environment. It's essentially the easy button to launch BEC campaigns.

Third, by using G Suite, Exaggerated Lion uses a reputable service to maximize the amount of potential emails they can send in a day. With standard Gmail accounts, the most common free webmail provider used to send BEC attacks, a user can only send a maximum of 500 messages a day. Once a G Suite account is out of the trial period, however, it is capable of sending 2,000 messages each day, which is more than enough to do some serious damage, especially considering that most BEC actors still manually send out their BEC emails rather than automating the process.

Registering "Secure" Domains

Less than half of BEC attacks are sent from domains that have been registered by an attacker. Custom domains also give us a glimpse of an attacker's decision-making process because they must make a conscious choice about the domain's name and structure.

Exaggerated Lion has adopted one of the more unique and creative approaches to naming their domains we've seen. Instead of trying to resemble a target's domain or using words that might indicate the domain is associated with a mobile device or telecom provider — two tactics we see quite commonly — Exaggerated Lion prefers to create extremely long domain names consisting of various words separated by hyphens.

office-secure-ssl-sl-mail71521-apps-server-portal-apps-mail.management

mail-offices-execs-ssl-secure-portal.management

admins-office-exec-ssl-secure-server-portal-exec.management

execs-mails-office-ssl-ssl1-secure-server-portal-executives.management

mails-officessl-apps-secureservers-portal-execs.management

Examples of Exaggerated Lion domains.

Usually, when we see long domains like this, they are used to host phishing sites, but there are no indications that Exaggerated Lion has hosted any content — malicious or otherwise — on any of the domains they have registered. For all intents and purposes, these domains are solely used for setting up email accounts to launch BEC attacks.

Some of the common words Exaggerated Lion includes in their domains are “secure,” “ssl,” “portal,” “server,” “apps,” “office,” “mail,” and “executive.” Their strategy seems to be to create domains that would appear to be secure infrastructure associated with a company executive.

A vast majority of Exaggerated Lion’s domains are hosted on the .MANAGEMENT top-level domain (TLD). Again, the use of this TLD is likely to give the domain the aura of belonging to an upper-level executive at a company. Interestingly, the .MANAGEMENT TLD is not one of the more commonly used generic TLDs available. Only around 12,000 domains with the .MANAGEMENT TLD have ever been registered. This means that Exaggerated Lion is associated with more than 10% of all .MANAGEMENT domains that have ever been created (and nearly three-quarters of .MANAGEMENT domains registered with Google).

A full list of domains linked to Exaggerated Lion can be found here*.

*https://www.agari.com/cyber-intelligence-research/whitepapers/acid-agari-exaggerated-lion-url-list.pdf

Conclusion

Protecting Yourself Against Lions (and Tigers and Bears)

Business email compromise has become the predominant cyber threat businesses face today. Since 2016, businesses have lost at least $26 billion as a result of BEC attacks and, based on the most recent FBI IC3 report, losses from BEC attacks grew another 37 percent in 2019. This report shows how cybercriminal groups are continually adapting and developing new and innovative tactics to increase the effectiveness of their crimes. For Exaggerated Lion, their use of physical checks as a cashout mechanism sets them apart from other BEC groups and their evolution to creating fake documents that are commonly used in authentic business transactions to add legitimacy to their scams.

To protect against threats like these, organizations first need to understand and accept the state of today's cyber threat landscape. Most email-based threats today, like BEC attacks, are very simple social engineering attacks that are technically unsophisticated. To effectively protect against these threats, companies need to make sure they have defenses in place that are equipped to detect identity deception attacks that traditional inbound filters are not accustomed to handling. Additionally, organizations should have good internal processes in place, so payment requests, regardless of source, are verified before they are processed.

Since 2016, businesses have lost at least

$26B

as a result of BEC attacks

losses from BEC attacks grew another

37%

in 2019

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