AGARI CYBER
INTELLIGENCE DIVISION

REPORT

London Blue
April 2019 Update

UK-Based Multinational Gang Evolves Their Tactics, Targeting Asian Users and Spoofing Email Addresses

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

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

How Not to Stay Under the Radar

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

Targeting a Cybersecurity Company

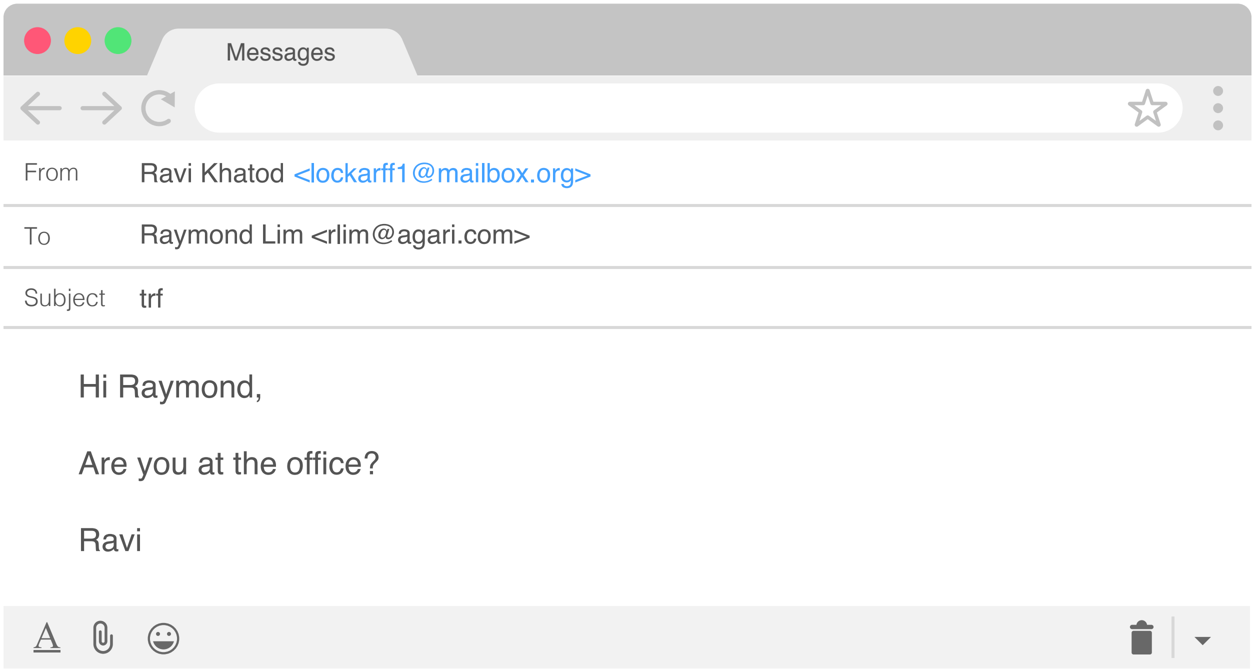
Here's what the lifecycle of London Blue's BEC attempt against Raymond looked like:

- **January 11, 2019:** Raymond's contact information, in addition to information for more than 500 other financial executives, was collected by one of the primary London Blue actors using a commercial US-based lead service in the initial preparation stage for BEC campaigns targeting California-based companies.
- **January 13, 2019:** A CSV file containing the raw leads for these identified targets was sent to another London Blue associate for processing. Processing involves organizing and validating the targeting data and supplementing it with open source intelligence to identify a company's CEO, who is then impersonated during the attack.
- **January 22, 2019:** The associate sent a batch of processed leads back to the primary actor, which contained Raymond's validated email address and the name of Agari's CEO at the time. This was the second of two batches of processed leads. The first was returned to the primary actor on January 16, 2019.
- **January 28, 2019:** In preparation for a round of BEC attacks, a test email was sent from an attack email account to one of the group's central operational email addresses. This test email is likely used to verify that a BEC email will successfully be delivered to a target without being blocked. All BEC groups we have tracked have used similar testing methods prior to launching their campaigns.
- **January 28, 2019:** Three and a half hours after the initial test email, London Blue's attack email is sent to Raymond, but is blocked by Agari Advanced Threat Protection before it hits the inbox.

In the August 2018 BEC attempt, London Blue used one of the more common BEC ruses, claiming a payment is due to a vendor and a wire transfer needs to be processed ASAP. In the January campaign, however, the group switched tactics and used a mergers and acquisitions theme.

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

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



From Ravi Khatod <lockarff1@mailbox.org>

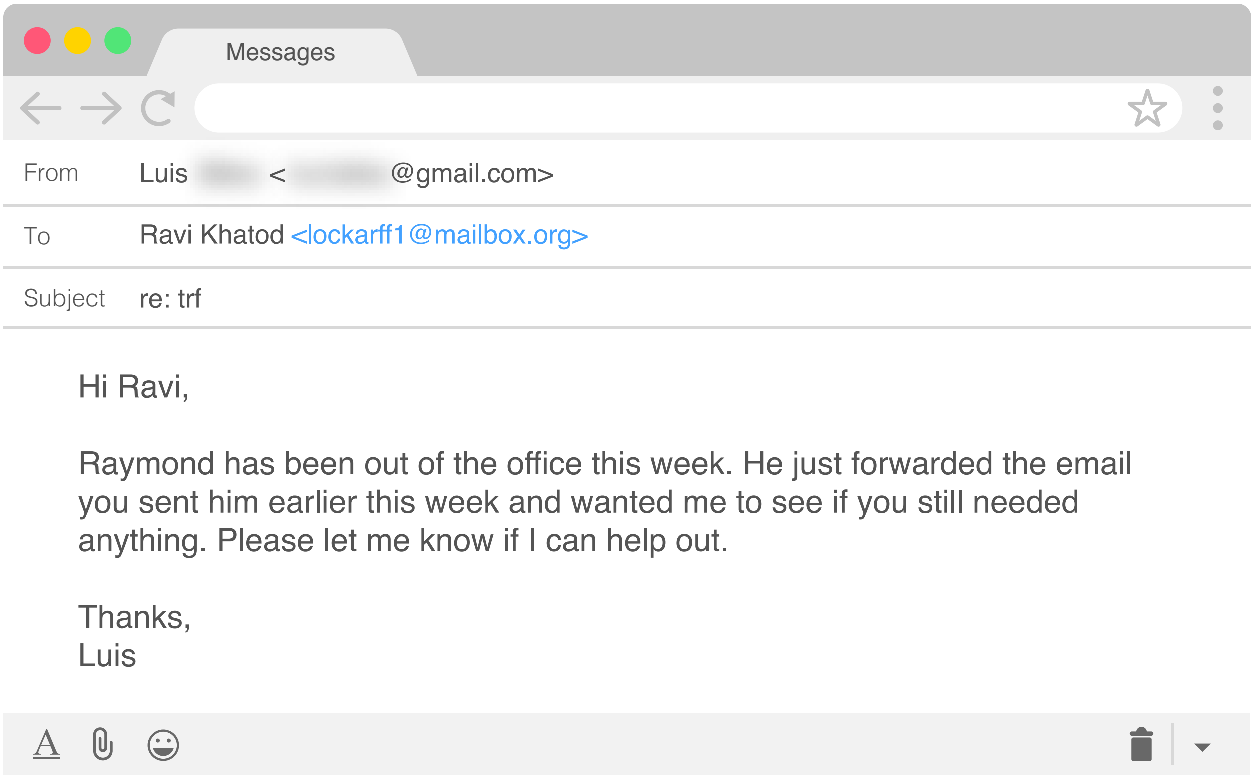
To Raymond Lim <rlim@agari.com>

Subject trf

Hi Raymond,

Are you at the office?

Ravi



From Luis [redacted] <[redacted]@gmail.com>

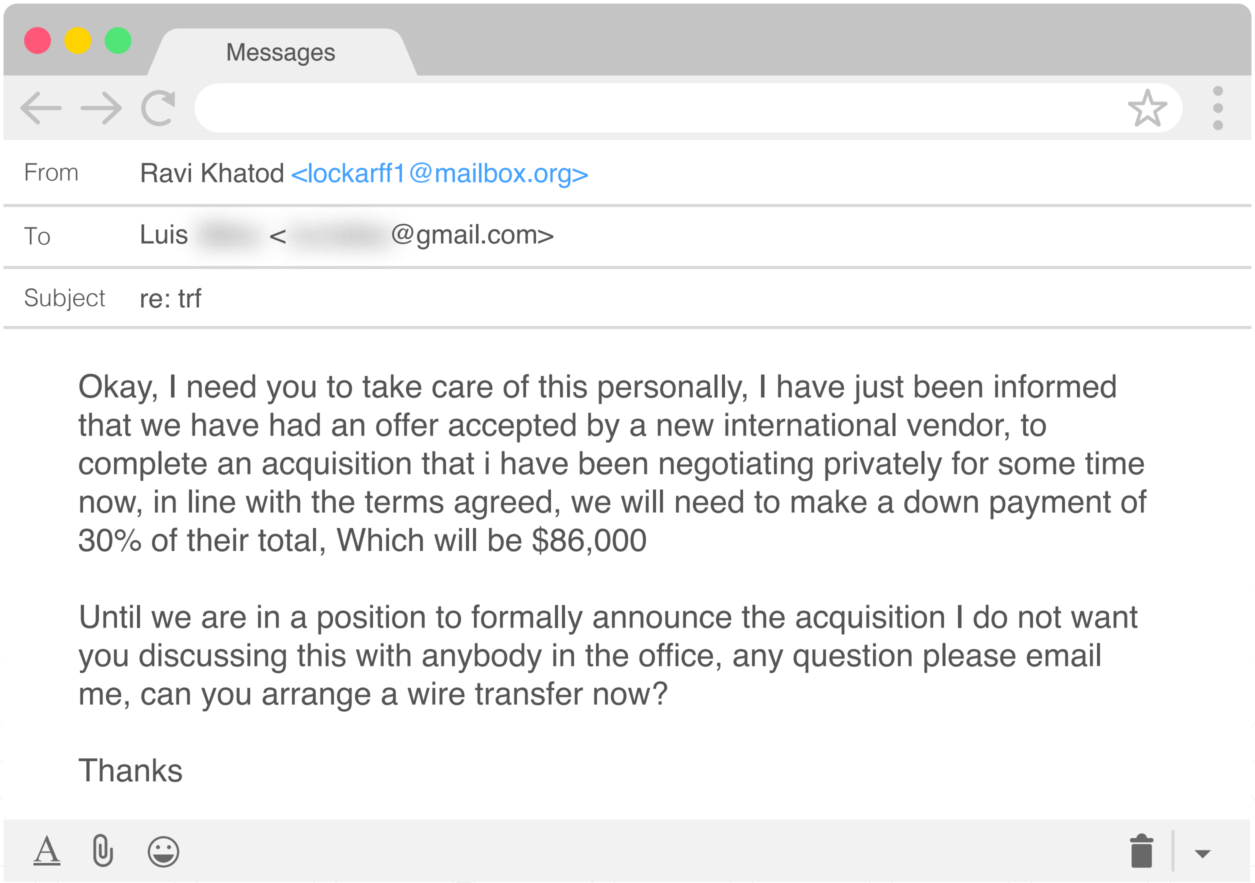
To Ravi Khatod <lockarff1@mailbox.org>

Subject re: trf

Hi Ravi,

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

Thanks,
Luis



From Ravi Khatod <lockarff1@mailbox.org>

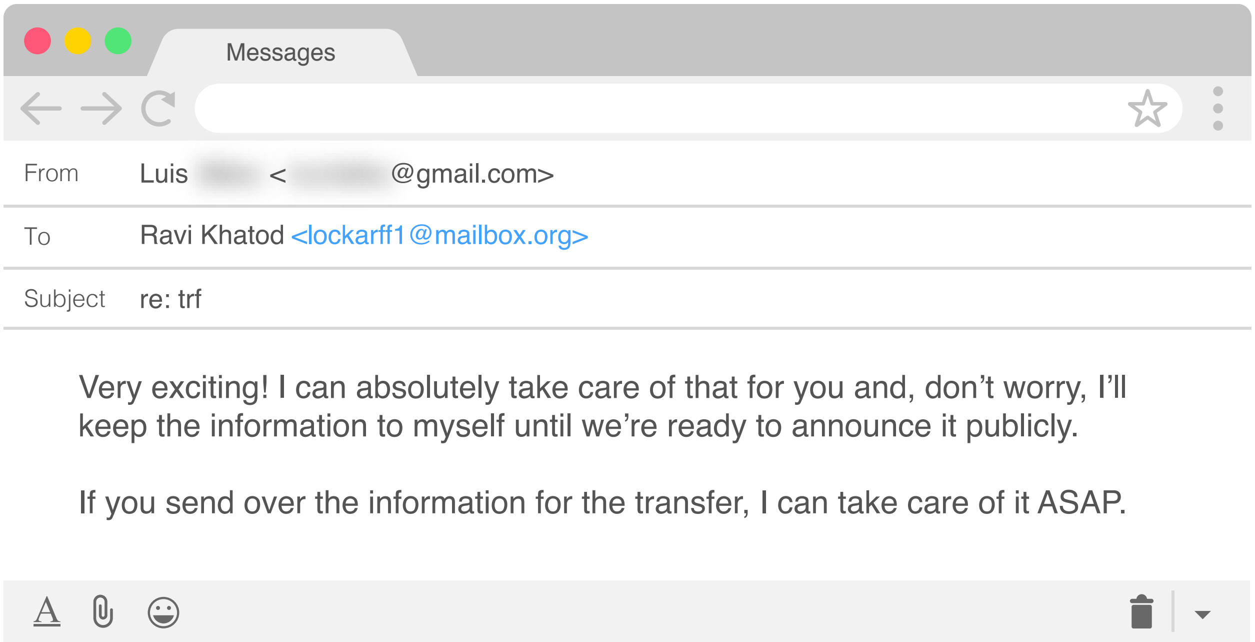
To Luis [redacted] <[redacted]@gmail.com>

Subject re: trf

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

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

Thanks



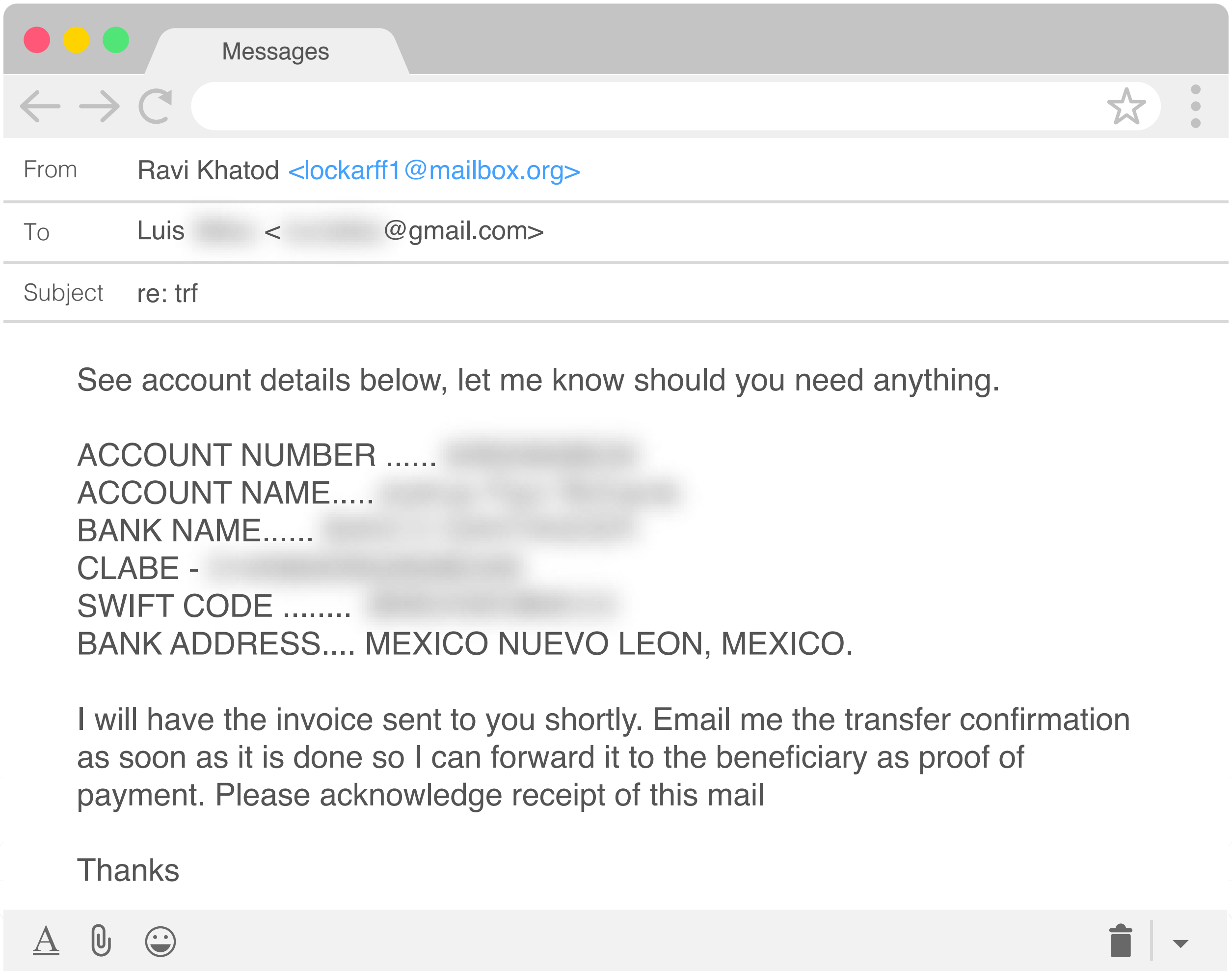
From Luis [redacted] <[redacted]@gmail.com>

To Ravi Khatod <lockarff1@mailbox.org>

Subject re: trf

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

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



From Ravi Khatod <lockarff1@mailbox.org>

To Luis [redacted] <[redacted]@gmail.com>

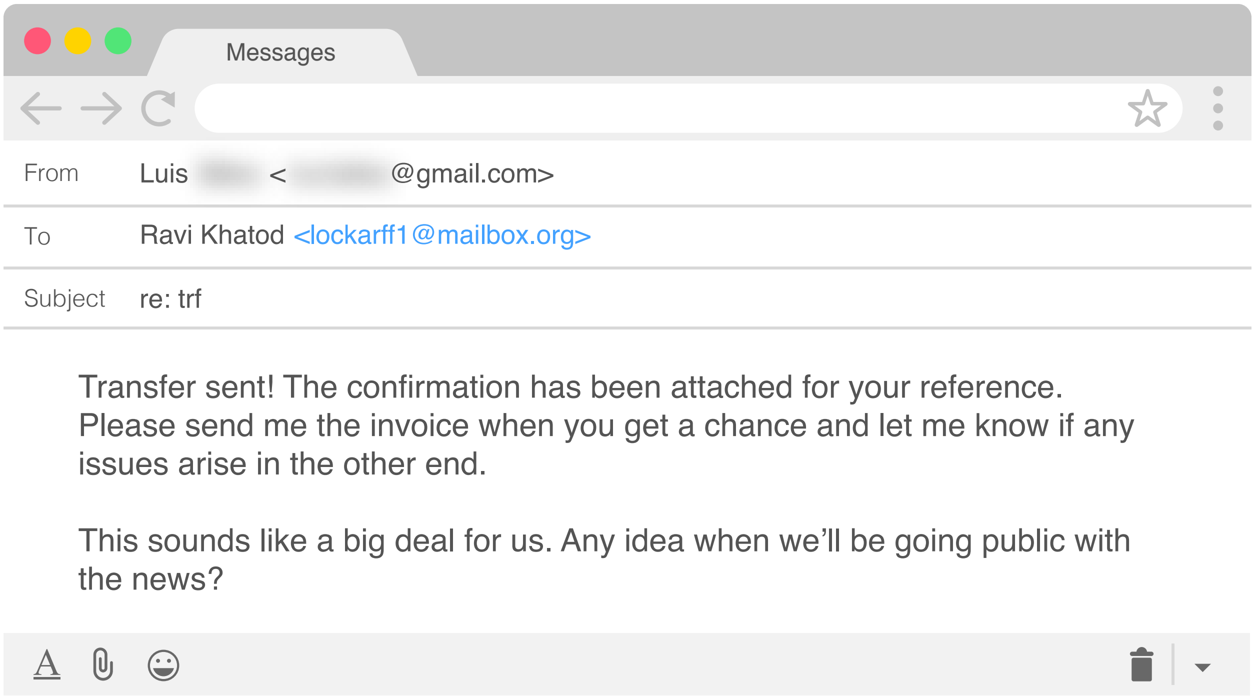
Subject re: trf

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

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

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

Thanks



From Luis [redacted] <[redacted]@gmail.com>

To Ravi Khatod <lockarff1@mailbox.org>

Subject re: trf

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

This sounds like a big deal for us. Any idea when we'll be going public with the news?

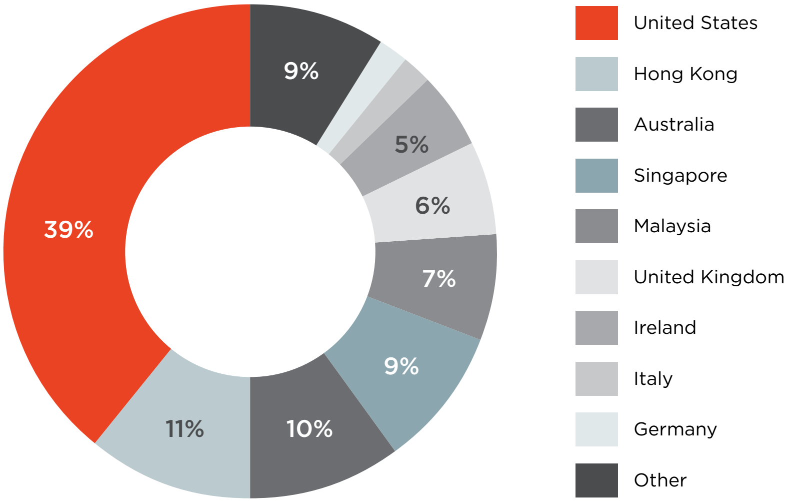
Gazing East into Asia

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

London Blue Focuses on Asian Targets

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

London Blue Target Locations since November 2018

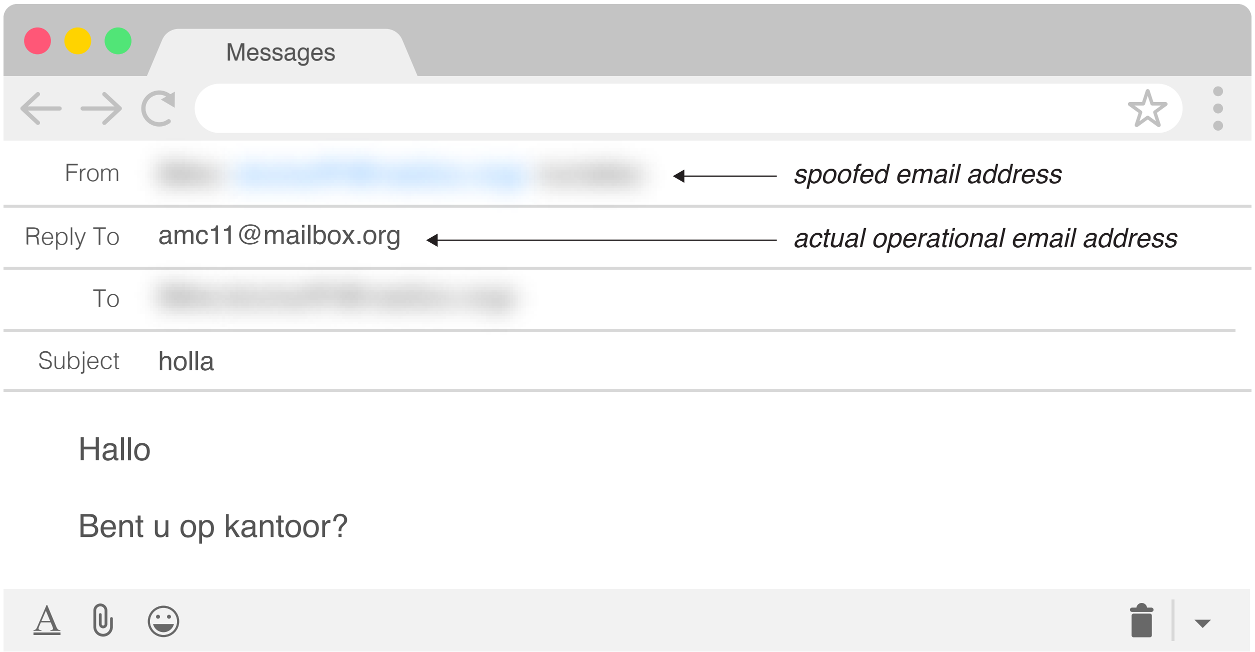


That said, one of the notable observations about London Blue's target selection over the past five months is that many of their targets are located in Asia, an area we have not seen the group target previously. In February, London Blue collected contact information for and launched BEC campaigns against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

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

Evolving Tactics: London Blue Starts Spoofing Target Domains

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



From [redacted]

Reply To amc11@mailbox.org

To [redacted]

Subject holla

Hallo

Bent u op kantoor?

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

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

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

Conclusion

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

Appendix A – Email Addresses Associated with London Blue BEC Attacks

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

abbyss101@aol.com
admin@com1t.ga**
admin@com1r.ml**
admin@com9g.ml**
afterplay@mailbox.org**
amc11@mailbox.org**
bluegate000@mailfence.com
bluegate001@yandex.com
bluegate002@naver.com
bluegate010@naver.com
bluegate101@163.com
bluegate101@eclipso.me**
bluegate102@naver.com
bluegate231@daum.net**
blugate000@lumail.lu
blugate001@naver.com
ceoadmiin@163.com
ceoofficeadmiin@gmail.com
ceos.em@mail.com
ceos1@daum.net**
ceos101@sol.dk**
lockarff1@mailbox.org**
lockarf11@daum.net**
lockup11@mailbox.org**
mdceo001@hush.com
mdceo001@lavabit.com
mdceo002@naver.com
outlookeracct@mailbox.org**
workon1@mailbox.org**

ACID® | AGARI CYBER INTELLIGENCE DIVISION

The Agari Cyber Intelligence Division (ACID) is the only counterintelligence research team dedicated to worldwide BEC and spearphishing investigation. ACID supports Agari's unique mission of protecting communications so that humanity prevails over evil. ACID uncovers identity deception tactics, criminal group dynamics, and relevant trends in advanced email attacks. Created by Agari in 2018, ACID helps to impact the cyber threat ecosystem and mitigate cybercrime activity by working with law enforcement and other trusted partners.

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

AGARI®