Abnormal

THREAT REPORT

Exploring the Rise of Israel-Based BEC Attacks

Executive Summary

Historically, the origin of most business email compromise (BEC) attacks has been West Africa. There's a reason that the "Nigerian Prince" scam became so well known in popular culture! In fact, out of all the BEC attacks the Abnormal team has analyzed since the beginning of 2022, 74% have been based in Nigeria.

But residing in Nigeria certainly isn't a requirement for BEC attackers. Indeed, the subject of this report is a sophisticated threat group based in Israel. And while many BEC actors found in other countries still have a connection back to Nigeria, there are no indications that this threat group has any direct Nigerian ties, making it a notable outlier in the BEC threat landscape.

All of the attacks by this group follow a similar, but effective, formula. The primary pretext in their attacks is that the targeted employee's organization is working through the confidential acquisition of another company and the employee is being asked to help with an initial payment required for the merger. The attacks consist of two stages, each employing a different persona. One is internal, typically the CEO, and the other is external, generally an attorney focused on mergers and acquisitions.

Based on a historical analysis of attacks, we've observed more than 350 BEC campaigns that can be linked to this threat group, dating back to at least February 2021. The frequency of campaigns seems to follow a consistent cyclical pattern, with 80% of attacks occurring during three periods throughout the year.

This threat group does not appear to target specific industries, typical among BEC actors, but it does seem to prefer larger enterprises. Nearly all of the 100+ organizations targeted have been multinational corporations, with offices in various regions around the world, and with annual revenue averaging more than $10 billion a year. Employees in at least 61 different countries across six continents have been targeted.

61

countries where targets are located.

$10+ billion

average annual revenue of a target company.

$712,000

average amount requested in an attack.

Table of Contents

Examining the Locations of BEC Attackers

Traditionally, Nigeria has been the primary epicenter for various types of social engineering scams, including business email compromise attacks.

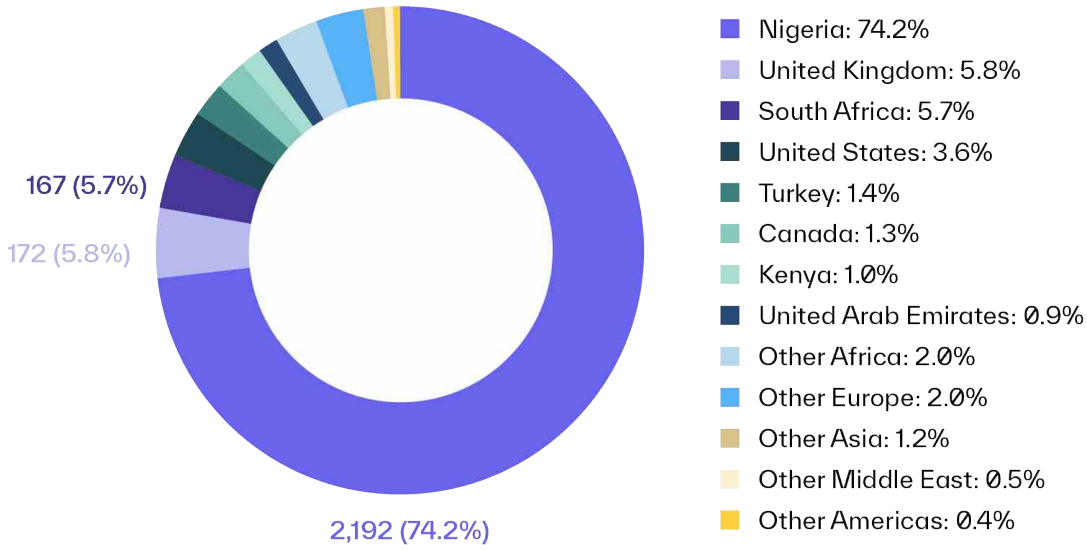
Since the beginning of 2022, we've identified 53 countries in which BEC attackers are operating. These locations are scattered across the globe, showing that BEC actors aren't centralized in a single region of the world.

Map of BEC Actor Locations

Over the past year, three-quarters of the BEC actors we've uncovered have been based in Nigeria. The next most-common country associated with BEC attackers is the United Kingdom, which served as the home base for 5.8% of actors.

Rounding out the top five countries linked to BEC scammers over the past year are South Africa, the United States, and Turkey.

Top Locations for BEC Actors



Interestingly, when you look at the data separated by type of BEC attack, a slightly different picture emerges.

For BEC attacks that request gift cards or a change in payroll banking details, Nigeria is still the clear primary origin for attackers, with 82% and 78% of actors located in the country, respectively. However, this isn't the case for payment fraud as Nigeria is the home base for only 58% of the actors behind this type of attack. Nearly one in five are based in South Africa, which is linked to just 2% of the threat actors who specialize in payroll diversion and gift card requests.

Bucking this historical trend, our analysis of campaigns associated with this threat group over the past two years indicates that the actors are not located in Africa but rather based in Israel. Moreover, while many BEC actors found in other countries still have a connection back to Nigeria, there are no indications that this group has any direct Nigerian ties, making it a notable outlier in the BEC threat landscape.

Analyzing the Targets of the Israel-Based Group

Based on a historical analysis of attacks, this group sent more than 350 BEC campaigns since February 2021. One noteworthy trend is that the group's activity seems to follow a consistent cyclical pattern throughout the year.

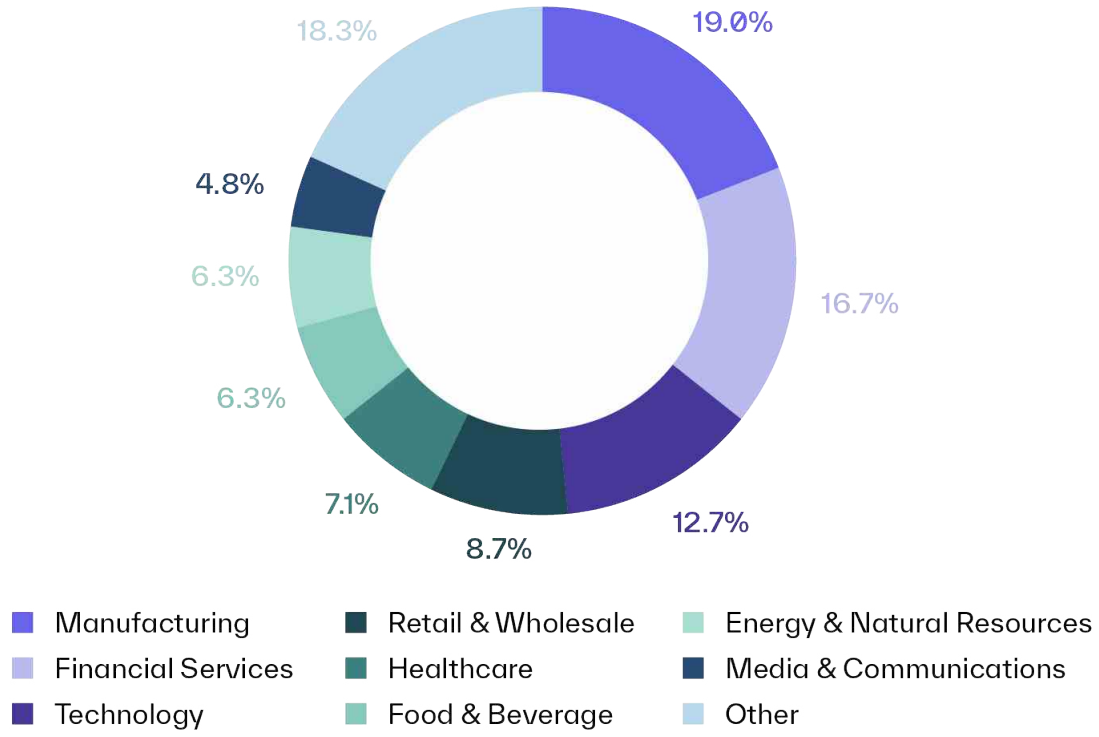
In each of the last two years, the volume of BEC campaigns spiked in March, June-July, and October-December, followed by a lull for two to three months. In fact, 80% of all the observed attacks occurred in one of those six months.

BEC Campaigns by Month

Abnormal

Like most other threat actors that focus on business email compromise, this group is fairly industry agnostic in their targets. They target multiple industries simultaneously, including manufacturing, financial services, technology, retail, healthcare, energy, and media.

Targets by Industry



Although industry doesn't seem to be a factor in their targeting methodology, it's clear that this Israel-based group prefers to target bigger corporations with their campaigns. Nearly all of the 100+ organizations targeted are large, multinational enterprises, with the average annual revenue of each corporation exceeding more than $10 billion a year. Additionally, most of these companies have a global presence with offices in multiple regions around the world.

Abnormal

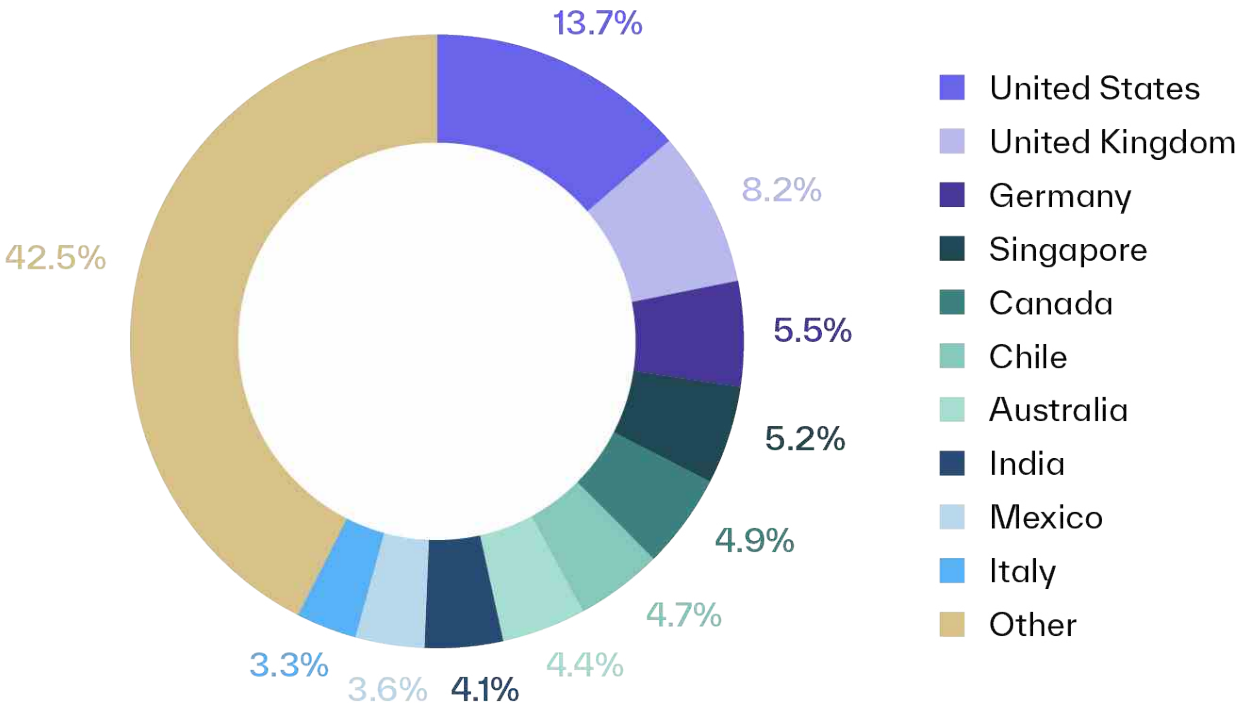
Accordingly, it's no surprise that employees targeted by the group are scattered across the globe. While the targeted companies have headquarters in 15 countries, employees in 61 different countries across six continents have received emails from the group.

Targets by Country

The most common countries in which targets have been located are the United States, the United Kingdom, Germany, Singapore, Canada, and Chile. And while the United States has been where the most targets reside and is a traditional focal point for cybercrime activity, it doesn't make up a disproportionate share of target locations like is the case for many other threat groups.

In fact, a plurality of targets (39%) of this Israel-based group were located across 29 European nations—compared to just 24% of targets based in North America. Nearly one in five targets (18%) were located in Asia.

Targets by Country



A Deep Dive into the Israel-Based BEC Attacks

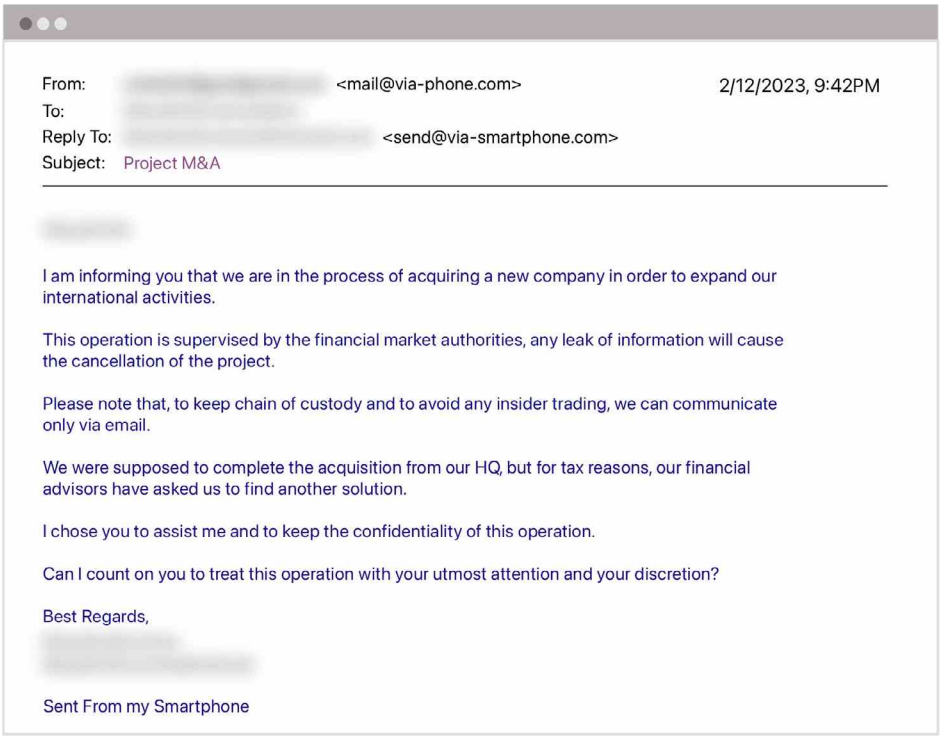
An attack from this group typically consists of two stages, each employing a different persona—one internal and one external. This section walks through attack examples from beginning to end to examine some of the unique tactics used to ensnare victims.

Stage 1: Initial Email and Correspondence

For the Israel-based group, there tends to be a lot of variation in the templates used for the initial email. That said, while the exact text found in opening messages changes frequently, the overall theme has remained the same for years.

In their introductory email, the group most commonly impersonates the CEO of the targeted organization. This first email sets the stage for the rest of the attack, providing some context about the project the targeted employee is being asked to assist with.

The primary pretext used in the attack is that the organization is working through the confidential acquisition of another company. The targeted employee is asked to help with an initial payment required for the merger.



Example of an initial email highlighting the confidentiality theme

One of the main themes throughout the attack is confidentiality. Many of the first few messages stress that the success of the acquisition hinges on the transaction staying a secret. An email may mention that any leak of information about the transaction would result in the cancellation of the project and/or that all communication must be kept to email in order to prevent insider trading and maintain a strict chain of custody.

Of course, the real reason for this "confidentiality" is to prevent the targeted employee from validating the legitimacy of the project with their manager or colleagues.

Targeting Senior Leaders

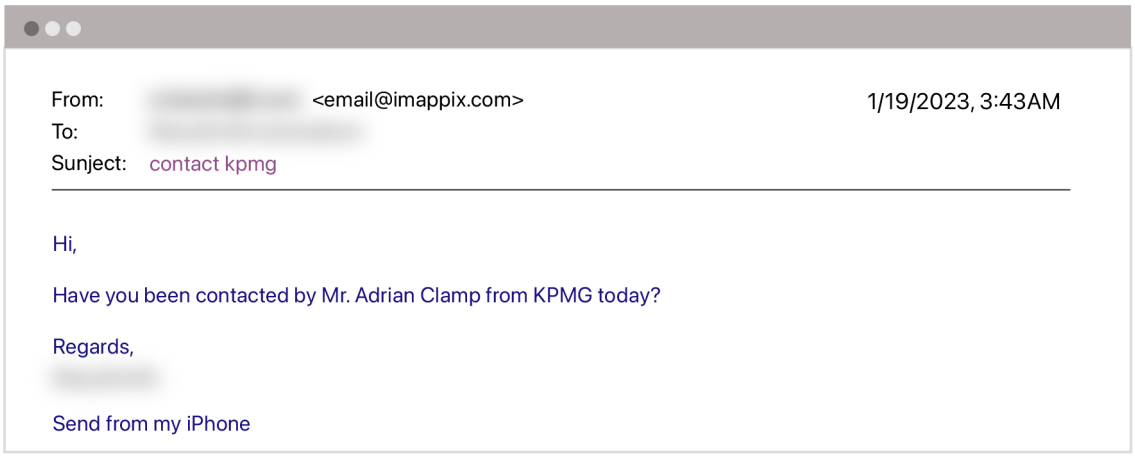
In most other BEC attacks focused on payment fraud, the targeted employees are specialists on the finance or accounting team. However, a vast majority of the employees targeted by this group are company executives or senior leaders that may not necessarily work with payments on a daily basis. This target selection makes sense within the context of the attack for a number of reasons.

First, members of the executive team are likely to send and receive legitimate communications with the CEO on a regular basis, which means an email from the head of the organization may not seem abnormal. Second, based on the stated importance of the supposed acquisition project, it's reasonable for a senior leader at the company to be entrusted to help. And finally, because of their seniority within the organization, there is presumably less red tape that would need to be cut through in order for them to authorize a large financial transaction.

Adding Secondary Personas

Another common thread among these attacks is the use of an external secondary persona whose job it is to "coordinate" the initial payment. In some of the opening messages, the second persona is introduced, asking the recipient whether they've received an email or call from them regarding the project.

All of the secondary personas referenced are real attorneys practicing mergers and acquisitions (M&A) law, usually based out of firms in the United Kingdom. While the impersonated attorneys come from a number of different law firms, the threat group seems to prefer impersonating solicitors at KPMG, a global professional services and consulting firm. KPMG is referenced directly in many of their emails, either in the subject or body of the message.



Follow-up email referencing KPMG

Using Real Domains

To make it seem as if emails are coming directly from the impersonated CEO, two tactics are used. If a targeted organization doesn't have an effective DMARC policy in place, the group spoofs the CEO's email address using the real domain. This approach is most effective because the target would see that the email address matches their own from the same company.

However, if an organization has established a DMARC policy that prevents bad actors from directly spoofing email addresses on their domain, the group updates the sending display name to include the CEO's email address in the display name. Because many email clients only show the sender's display name by default, the use of an extended spoofed display name still has the intended effect of making it appear that a message is sent from the real email address of the impersonated CEO.

From: Jane Smyth <jane.smyth@acme.com> 1/5/2023, 7:40AM
To: ace.jones@acme.com
Reply To: Jane Smyth <jane.smyth@acme.com> <phone@sslmail55.com>
Subject: HQ Project Financial Market Authorities-1001

Ace,

I would like you to be in charge of a matter that needs to be resolved with our appointed legal advisors.

We're currently working on a new acquisition, and Richard Elks, one of our attorneys, was supposed to get in touch with you to provide you all the instructions.

Have you received any email or call?

Best Regards,
Jane Smyth

Sent From my Smartphone

Initial email that spoofs the impersonated CEO's address
NOTE: Names and email addresses have been changed

From: John Smith <john.smith@company.com> <mail@via-phone.com> 2/12/2023, 9:42PM
To: srogers@company.com
Reply To: John Smith <john.smith@company.com> <send@via-smartphone.com>
Subject: Project M&A

Steve,

I am informing you that we are in the process of acquiring a new company in order to expand our international activities.

This operation is supervised by the financial market authorities, any leak of information will cause the cancellation of the project.

Please note that, to keep chain of custody and to avoid any insider trading, we can communicate only via email.

We were supposed to complete the acquisition from our HQ, but for tax reasons, our financial advisors have asked us to find another solution.

I chose you to assist me and to keep the confidentiality of this operation.

Can I count on you to treat this operation with your utmost attention and your discretion?

Best Regards,
John Smith

Sent From my Smartphone

Initial email that uses an extended spoofed display name
NOTE: Names and email addresses have been changed

Languages Used

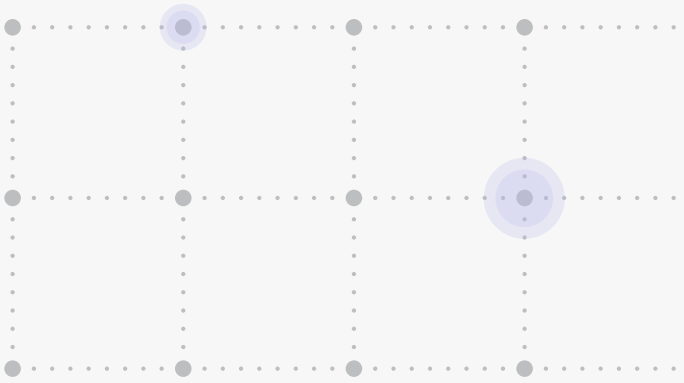
Regardless of where the target is located, most of the malicious emails from this threat group are written in English. Still, a number of attacks were sent in other languages.

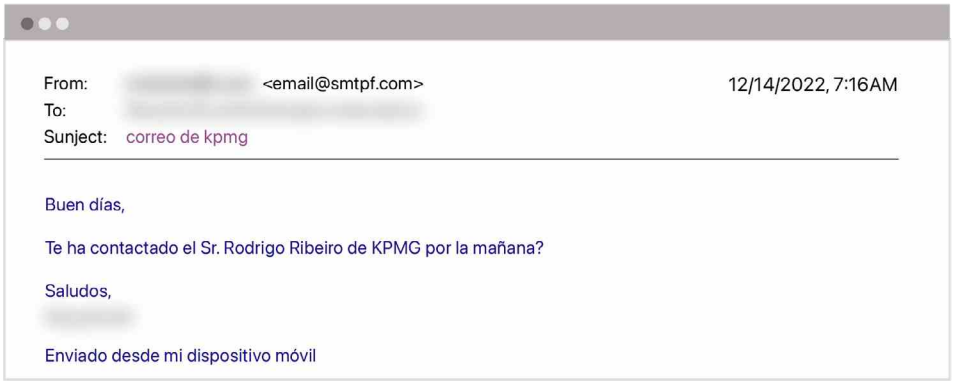
BEC attacks are often translated into other languages to fit in with the communications an employee usually receives. For example, if an employee who typically conducts business in Japanese receives an email from what appears to be their CEO in English, it will likely raise some red flags. But if that email is written in Japanese, it is more likely to blend in with other communications and thus increase the attacker's chance of success.

The most common secondary language we've seen used by this group is Spanish. Interestingly, while a majority of the campaigns targeting employees in South America were written in Spanish, most attacks targeting employees in other Spanish-speaking countries, like Mexico and Spain, were written in English.

Campaigns were also written in other languages, including French, Italian, and Japanese. That said, the use of non-English emails has never been consistent across attacks, and there doesn't seem to be an organizational logic to explain why these threat actors decide to use a different language at a given time.

Additionally, all of the non-English attacks have used short templates, which is a departure from many of the long and detailed English-based attacks typically sent by the group. This likely indicates they don't have access to native non-English speakers, nor do they leverage advanced translation services.





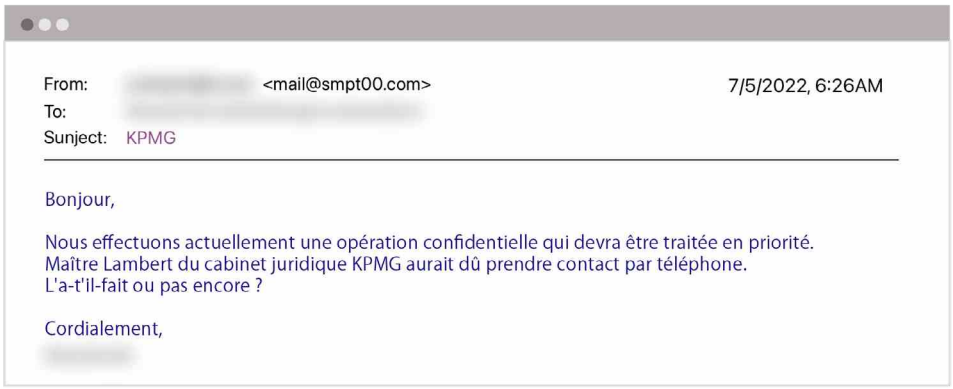
From: [redacted] <email@smtpf.com> 12/14/2022, 7:16AM
To: [redacted]
Sunject: correo de kpmg

Buen días,

Te ha contactado el Sr. Rodrigo Ribeiro de KPMG por la mañana?

Saludos,
[redacted]

Enviado desde mi dispositivo móvil

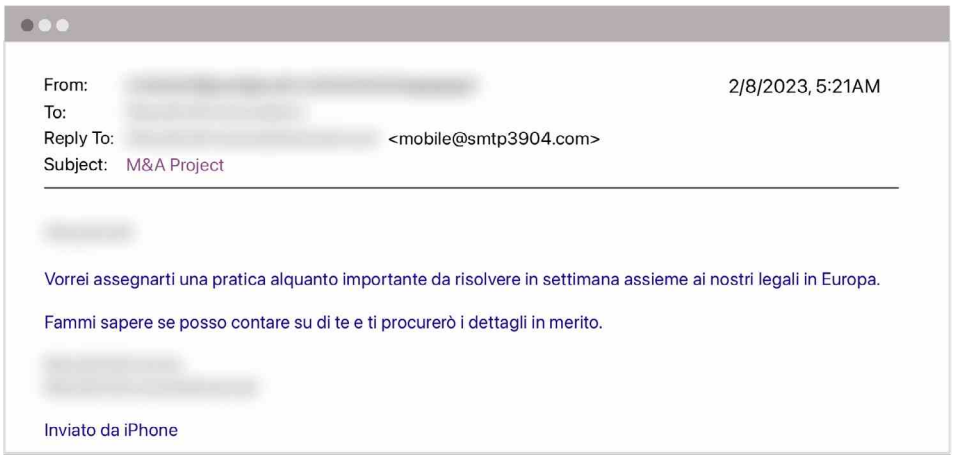


From: [redacted] <mail@smpt00.com> 7/5/2022, 6:26AM
To: [redacted]
Sunject: KPMG

Bonjour,

Nous effectuons actuellement une opération confidentielle qui devra être traitée en priorité.
Maître Lambert du cabinet juridique KPMG aurait dû prendre contact par téléphone.
L'a-t'il-fait ou pas encore ?

Cordialement,
[redacted]



From: [redacted] 2/8/2023, 5:21AM
To: [redacted]
Reply To: [redacted] <mobile@smtp3904.com>
Subject: M&A Project

[redacted]

Vorrei assegnarti una pratica alquanto importante da risolvere in settimana assieme ai nostri legali in Europa.

Fammi sapere se posso contare su di te e ti procurerò i dettagli in merito.

[redacted]

Inviato da iPhone

From: [redacted] < [redacted] @ssl-mail.com> 10/27/2022, 3:26AM
To: [redacted]
Sunject: Finance M&A

[redacted]

今週中に当社が任命した法務アドバイザーと解決すべき件についてを担当をお願いしたいと思います。

ご担当いただけるようでしたら、ご連絡ください。詳細をお知らせいたします。

よろしくお願いします。
[redacted]

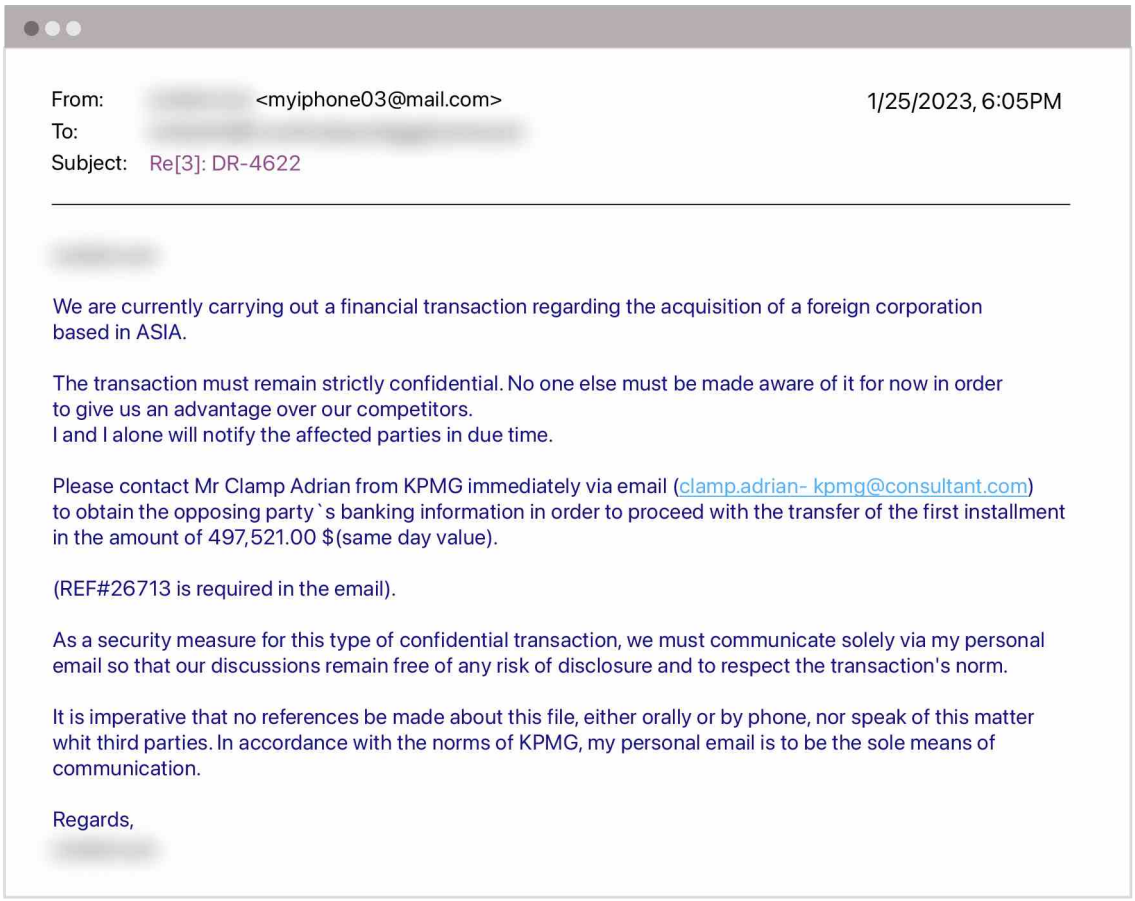
iPhoneから送信

Initial email correspondence in Spanish, French, Italian, and Japanese

Stage 2: Persona Handoff

After the targeted employee responds to the initial email, the attack moves to the next stage. Here, the attacker provides the backstory, explaining that the company being acquired is located in Asia and that the secrecy of the transaction is necessary to ensure an advantage over competitors. Interestingly, the amount requested changes from email to email.

The employee is then asked to contact the attorney referenced in the introductory email to receive bank account details so the initial "installment" payment can be sent. An email address is provided for the attorney, which is usually hosted either on a lookalike domain mimicking the law firm's legitimate domain, or a free mail.com domain like ***consultant.com*** or ***accountant.com***. The email also includes a reference number that the impersonated CEO states must be included in the message to the attorney.



From: [redacted] <myiphone03@mail.com> 1/25/2023, 6:05PM
To: [redacted]
Subject: Re[3]: DR-4622

[redacted]

We are currently carrying out a financial transaction regarding the acquisition of a foreign corporation based in ASIA.

The transaction must remain strictly confidential. No one else must be made aware of it for now in order to give us an advantage over our competitors.
I and I alone will notify the affected parties in due time.

Please contact Mr Clamp Adrian from KPMG immediately via email (clamp.adrian- kpmg@consultant.com) to obtain the opposing party`s banking information in order to proceed with the transfer of the first installment in the amount of 497,521.00 $(same day value).

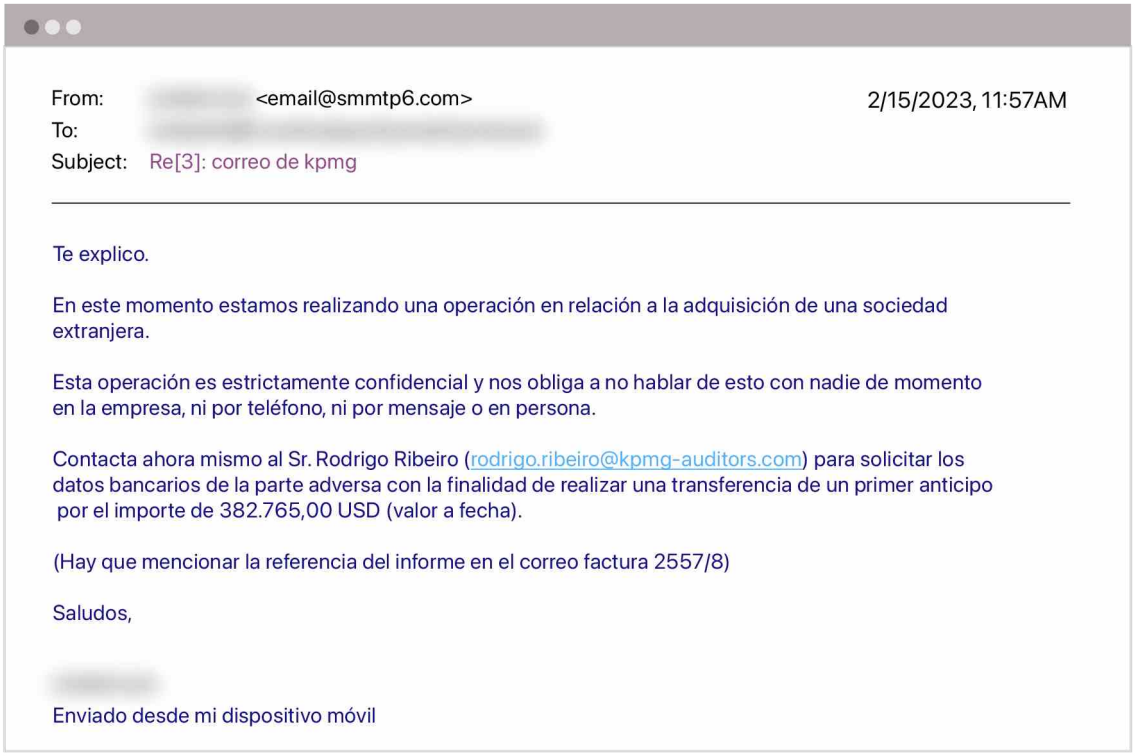
(REF#26713 is required in the email).

As a security measure for this type of confidential transaction, we must communicate solely via my personal email so that our discussions remain free of any risk of disclosure and to respect the transaction's norm.

It is imperative that no references be made about this file, either orally or by phone, nor speak of this matter whit third parties. In accordance with the norms of KPMG, my personal email is to be the sole means of communication.

Regards,
[redacted]

Example follow-up email written in English



From: [redacted] <email@smmtp6.com> 2/15/2023, 11:57AM
To: [redacted]
Subject: Re[3]: correo de kpmg

Te explico.

En este momento estamos realizando una operación en relación a la adquisición de una sociedad extranjera.

Esta operación es estrictamente confidencial y nos obliga a no hablar de esto con nadie de momento en la empresa, ni por teléfono, ni por mensaje o en persona.

Contacta ahora mismo al Sr. Rodrigo Ribeiro (rodrigo.ribeiro@kpmg-auditors.com) para solicitar los datos bancarios de la parte adversa con la finalidad de realizar una transferencia de un primer anticipo por el importe de 382.765,00 USD (valor a fecha).

(Hay que mencionar la referencia del informe en el correo factura 2557/8)

Saludos,

[redacted]
Enviado desde mi dispositivo móvil

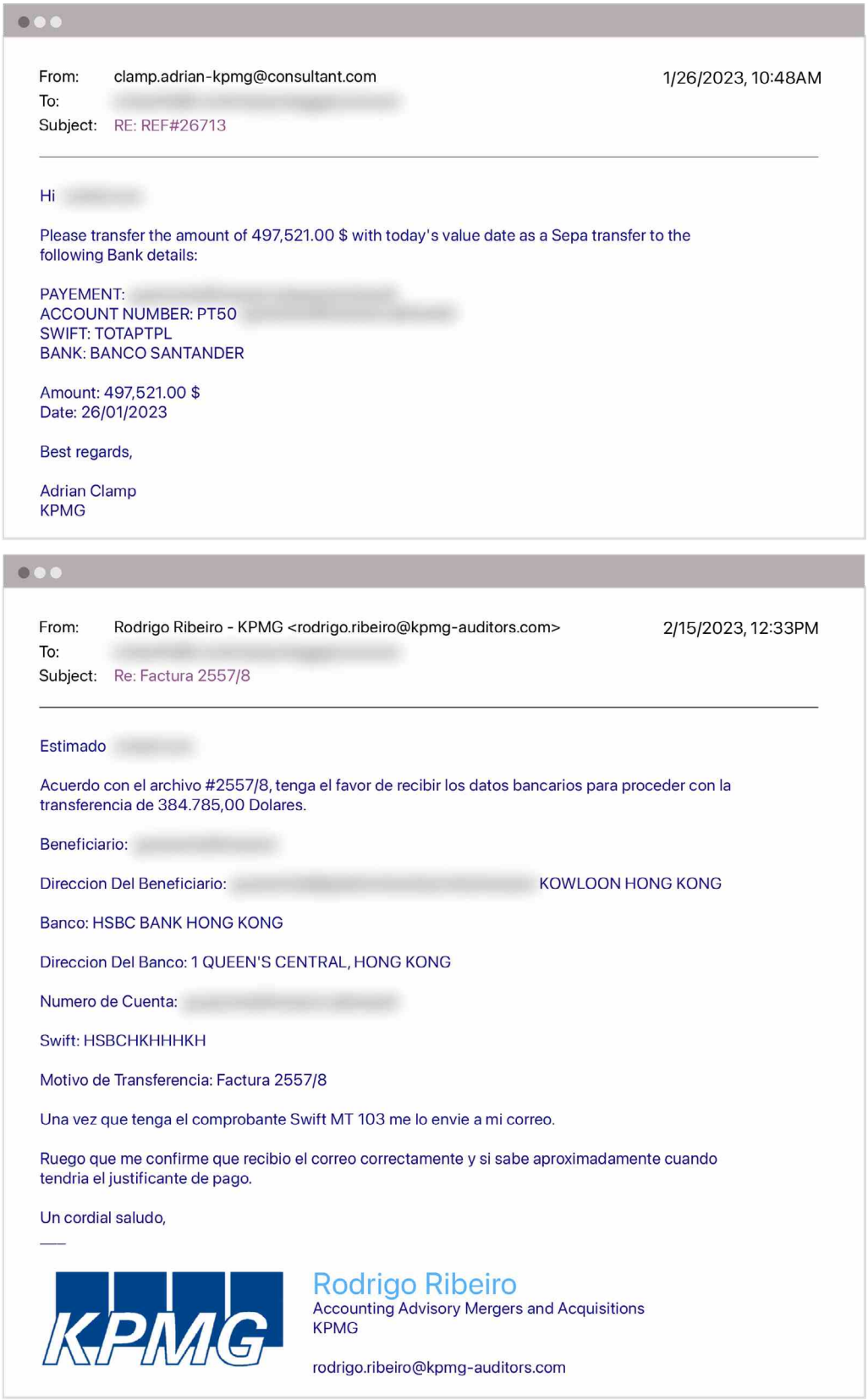
Example follow-up email written in Spanish

If an employee complies and reaches out to the "attorney," they usually receive a quick response—likely because the secondary account is controlled by the same threat actor and they're expecting the message. The reply from the attorney first confirms the amount needed to fulfill the terms of the acquisition. This is where this Israel-based group really stands out in comparison to other BEC threat actors.

An analysis of potential financial impact data across all payment fraud attacks shows the average amount requested is $65,000. In contrast, this group requests an average of $712,000—more than 10 times the average. Because the main theme of these attacks is the acquisition of a company and large sums of money are commonly exchanged in that type of transaction, the amount may not raise any red flags.

Once the amount has been confirmed, the impersonated attorney sends the details for the bank account that will be used to receive the payment. Nearly all of the initial mule accounts provided by the group have been located in Hong Kong, which fits nicely with the pretext that the company being acquired is located in Asia. If the actor is told that a payment to a Hong Kong account isn't possible, they will generally pivot to accounts in other countries, including Portugal and Hungary.

Notably, these threat actors have been hesitant to use mule accounts in the United States or the United Kingdom, likely indicating that they don't have a good mule network there.



From: clamp.adrian-kpmg@consultant.com 1/26/2023, 10:48AM
To:
Subject: RE: REF#26713

Hi

Please transfer the amount of 497,521.00 $ with today's value date as a Sepa transfer to the following Bank details:

PAYEMENT:
ACCOUNT NUMBER: PT50
SWIFT: TOTAPTPL
BANK: BANCO SANTANDER

Amount: 497,521.00 $
Date: 26/01/2023

Best regards,

Adrian Clamp
KPMG

From: Rodrigo Ribeiro - KPMG <rodrigo.ribeiro@kpmg-auditors.com> 2/15/2023, 12:33PM
To:
Subject: Re: Factura 2557/8

Estimado

Acuerdo con el archivo #2557/8, tenga el favor de recibir los datos bancarios para proceder con la transferencia de 384.785,00 Dolares.

Beneficiario:

Direccion Del Beneficiario: KOWLOON HONG KONG

Banco: HSBC BANK HONG KONG

Direccion Del Banco: 1 QUEEN'S CENTRAL, HONG KONG

Numero de Cuenta:

Swift: HSBCHKHHHKH

Motivo de Transferencia: Factura 2557/8

Una vez que tenga el comprobante Swift MT 103 me lo envie a mi correo.

Ruego que me confirme que recibio el correo correctamente y si sabe aproximadamente cuando tendria el justificante de pago.

Un cordial saludo,

—

KPMG

Rodrigo Ribeiro
Accounting Advisory Mergers and Acquisitions
KPMG

rodrigo.ribeiro@kpmg-auditors.com

Examples of follow-up emails containing banking details

Stage 3: Pivot to Phone

In some campaigns, once the attack has reached the second stage, the group has asked to transition the conversation from email to a voice call via WhatsApp. The likely reason for this is to expedite the conversation and move it off of a platform where it could get blocked. This also provides less of a paper trail for the target organization to discover.

Email requesting a switch to WhatsApp

During our research into the group, we recorded one of these calls to understand how this conversation would unfold in a real attack.

The first thing that was immediately noticeable was the accent of the speaker on the other end of the line. As stated earlier, a vast majority of BEC attacks can be attributed to Nigerian threat actors. However, the subject on the phone spoke with a distinct French accent, which was confirmed by the actor himself when he apologized if it was hard to understand him.

> "I'm French, so if there are some words that you don't understand, I'm sorry for my English and my accent."

Abnormal

Similar to the emails that preceded the call, the actor reiterated the need for confidentiality, emphasizing that no one else could know about the acquisition.

> "So please note that this is an extremely confidential operation and nobody besides of [CEO First Name], you, and myself has to know about this acquisition. This operation is ruled by the financial market authority, whose role is to make sure that all the process be in due form. So this is the reason why, uh, we have to keep this strictly confidential until the legal announcement."

During the call, the threat actor, pretending to be the attorney, also walked through the next steps involved in finalizing the acquisition. He inserted various M&A buzzwords to add credibility to his statements, such as needing to sign the "legal acts" or wanting to avoid "insider trading."

> "To sign the legal acts, 1% of the total amount of the acquisition has to be paid. The legal announcement will take place on next week, and then there will be a refund arranged by [CEO First Name]...I will ask [CEO First Name] to prepare the document and I will send it to you, I think, in about 15 or 20 minutes. So please once you proceed with this payment, please send me the proof of payment because I need this document to sign the legal act. Okay. And we are at the end of the operation and I want to avoid any late fees or any insider trading. Okay?"

Prior to this call, we had notified the subject that it wouldn't be possible to send the payment to the Hong Kong bank account he had originally provided. To try to resolve the problem, the actor probed to find a bank that would work for us, eventually settling on a bank in Hungary.

> "So I have received your email that it's not easy for you to proceed to a payment in Asia. That's what you wrote me? So is it easier for you in Europe?...Can you proceed to this payment in Euros or not?...So I will probably send you the bank details of our [Hungarian] bank in Europe."

This first call ended with an understanding that the actor would send new payment account details. The next day, the actor requested another call due to "issues" with the payment. In this second call, the subject employed aggressive pressure tactics to try to resolve the payment issues quickly, implying that the acquisition could be in jeopardy because of the payment delays.

> "So please confirm by email that you have received all the documents and that you can proceed with the payment as soon as possible because we must sign the legal action. We have a huge delay on this operation, so it takes too long from now. So we have to go on...Yes, please, please, very shortly, please. And also we have a big time difference. I'm in London right now, so we have a big time difference. I have to be sure that everything be okay before the weekend."

This was our last phone conversation with the subject, but additional emails were sent over the course of the next few days.

Conclusion: Protecting Your Organization from BEC

This threat group is focused on the same thing as all other BEC actors: making money as quickly and easily as possible. What makes them unique is that they are located in the Middle East rather than Africa—an indicator that BEC is continuing to spread.

The Israel-based group is also unique in that they use executive impersonation to request huge sums of money, a far cry from the hundred dollar gift card requests that comprised the CEO fraud of the past. Even one successful attack each year means they're making more than most people do in a decade—particularly when you consider that all of this money is tax-free. Just one successful attack each month means that these threat actors could be set for life, which is perhaps why they appear to only work a few months each year.

So what can be done to stop these attacks? Security awareness training is essential to ensure that employees know how to spot potentially fraudulent emails like the ones shown here. But even the most security-conscious employees could be tricked by socially engineered lures like these, particularly due to the legitimacy given by the phone calls. And unfortunately, legacy security tools are unlikely to block the initial attacks since they are sent from legitimate domains without suspicious links, malicious attachments, or other traditional indicators of compromise.

As such, organizations should employ a security solution that uses behavioral AI to understand identity, context, and content and baseline known behavior. By understanding what is normal, these platforms can detect and block malicious emails like those sent from this group so that employees never have an opportunity to engage with them. Doing so ensures that your organization stays safe from BEC attacks, as well as malware, ransomware, invoice fraud, credential phishing, and other types of advanced attacks.

Abnormal

Abnormal Security provides the leading behavioral AI-based email security platform that leverages machine learning to stop sophisticated inbound email attacks and dangerous email platform attacks that evade traditional solutions. The anomaly detection engine leverages identity and context to analyze the risk of every cloud email event, preventing inbound email attacks, detecting compromised accounts, and remediating emails and messages in milliseconds—all while providing visibility into configuration drifts across your environment.

You can deploy Abnormal in minutes with an API integration for Microsoft 365 or Google Workspace and experience the full value of the platform instantly, with additional protection available for Slack, Teams, and Zoom. More information is available at abnormalsecurity.com.

Stop Business Email Compromise with Abnormal:

Request a Demo:

abnormalsecurity.com →

Follow Us on Twitter:

@AbnormalSec

Follow Us on LinkedIn:

abnormalsecurity

Appendix: Associated Domains

a-secure[.]cloud
ah-av[.]com
bm-lawyers[.]link
board-ftp[.]com
board-ip[.]com
box-securized[.]com
box-securizing[.]com
ccl2srv[.]com
ccssl3[.]com
cell-secure2[.]online
cellmobile[.]online
company-encrypted[.]com
conf-mail[.]com
corpo-rate[.]xyz
csmtph[.]com
csmtpq[.]com
domaine-encrypted[.]online
ecrypter-webmails[.]com
ecryptor-webmails[.]online
el-jl[.]com
email-secure[.]exchange
emailer-encryptor[.]com
en-oi[.]com
es-ho[.]com
esmtp388[.]com
esmtp94[.]com
fmisystems[.]tech
from-my-iphone[.]com
from-myiphone[.]com
frommobile81[.]com
ho-et[.]com
if-hq[.]com
imap33[.]com
imappix[.]com
incorp-tax[.]com
intern-mail1[.]com
intern-mobile[.]com
intern33[.]com
interncorp[.]tech
internmail[.]tech
intranet-board[.]com
intranet-ip[.]com
io-ic[.]com
io-nc[.]com
ios-smtp[.]com
is-ho[.]com
is-ni[.]com
jl-el[.]com
mail-phone1[.]com
mail039[.]com
mail3495[.]com
mobile039[.]com
mobilefw[.]com
mobilejp[.]co
mx0records[.]com
mx1records[.]co
mx2records[.]co
mxrecords[.]co
mzl-confidential[.]com
outlook-relay[.]com
phone-securemail[.]com
phone-ssl2[.]com
phonesmtp[.]com
pop2sl[.]com
pop3fr[.]com
private-mail1[.]fr
relayformobile[.]com
secure-mobile08[.]com
secure-mobile81[.]com
securemobile02[.]com
securemobile33[.]com
send-phone[.]com
sending-phone[.]com
sendmx-host[.]com
sentfrom-my-iphone[.]com
serveroutlook[.]com
sfp-mx[.]services
smmtp3[.]com
smpt-secure[.]net
smrtapp1[.]com
smrtph[.]com
smtp-mobile02[.]com
smtp-phone[.]com
smtp-secure1[.]com
smtp00[.]com
smtp0039[.]com
smtp007[.]com
smtp0253[.]com
smtp0751[.]com
smtp1223[.]com
smtp129[.]com
smtp203[.]com
smtp220[.]online
smtp2652[.]com
smtp267[.]com
smtp281[.]com
smtp291[.]com
smtp292[.]com
smtp3229[.]com
smtp3306[.]com
smtp34521[.]com
smtp3482[.]com
smtp3904[.]com
smtp394[.]com
smtp399[.]com
smtp433[.]com
smtp483[.]com
smtp4908[.]com
smtp555[.]com
smtp777[.]com
smtp88[.]com
smtp982[.]com
smtpf[.]com
smtpmobile01[.]com
smtpp8[.]com
smtpp88[.]com
ssl-mail[.]com
ssl-mailphone[.]com
ssl-mobilesend[.]com
ssl-phonesend[.]com
ssl-smtp[.]net
ssl-smtp1[.]com
sslmail55[.]com
transfercell[.]tech
verified-market-authority[.]com
via-phone[.]com
via-smartphone[.]com