LMNTRIX

BE THE HUNTER | NOT THE PREY

WHITE PAPER

PROTECTION AGAINST
BUSINESS EMAIL COMPROMISE

2021

LMNTRIX USA.
333 City Blvd West,
18th Floor, Suite 1805
Orange, CA 92868
+1.888.958.4555

LMNTRIX UK.
200 Brook Drive, Green Park,
Reading, RG2 6UB
+44.808.164.9442

LMNTRIX SINGAPORE.
60 KAKI BUKIT PLACE#05-19
EUNOS TECHPARK
+65 3159 0639

LMNTRIX Hong Kong.
14F, Manning House, 38-48
Queen's Road Central, Central,
Hong Kong
+852.580.885.33

LMNTRIX Australia.
Level 32, 101 Miller Street,
North Sydney NSW 2060
+61.288.805.198

lmntrix.com

BUSINESS EMAIL COMPROMISE: A **BILLION-DOLLAR PROBLEM**

Business Email Compromise (BEC) rose to prominence as a scam that cost businesses collectively $1.8 Billion USD in 2020 alone. BEC scams began making headlines towards the end of 2015, but were often wrongly characterized as wire fraud. By the middle of 2016 enough incidents had been detected by security researchers to see what businesses were facing, while it could be considered wire fraud, it was a unique attack method that came to be called BEC.

Some estimates place the total losses suffered by businesses around the globe at $26 Billion USD since June 2016 and businesses from 177 countries have fallen victim to scammers. While putting a figure to the problem certainly helps frame the seriousness of the situation it does little to explain what a BEC scam is. A picture is worth a thousand words.

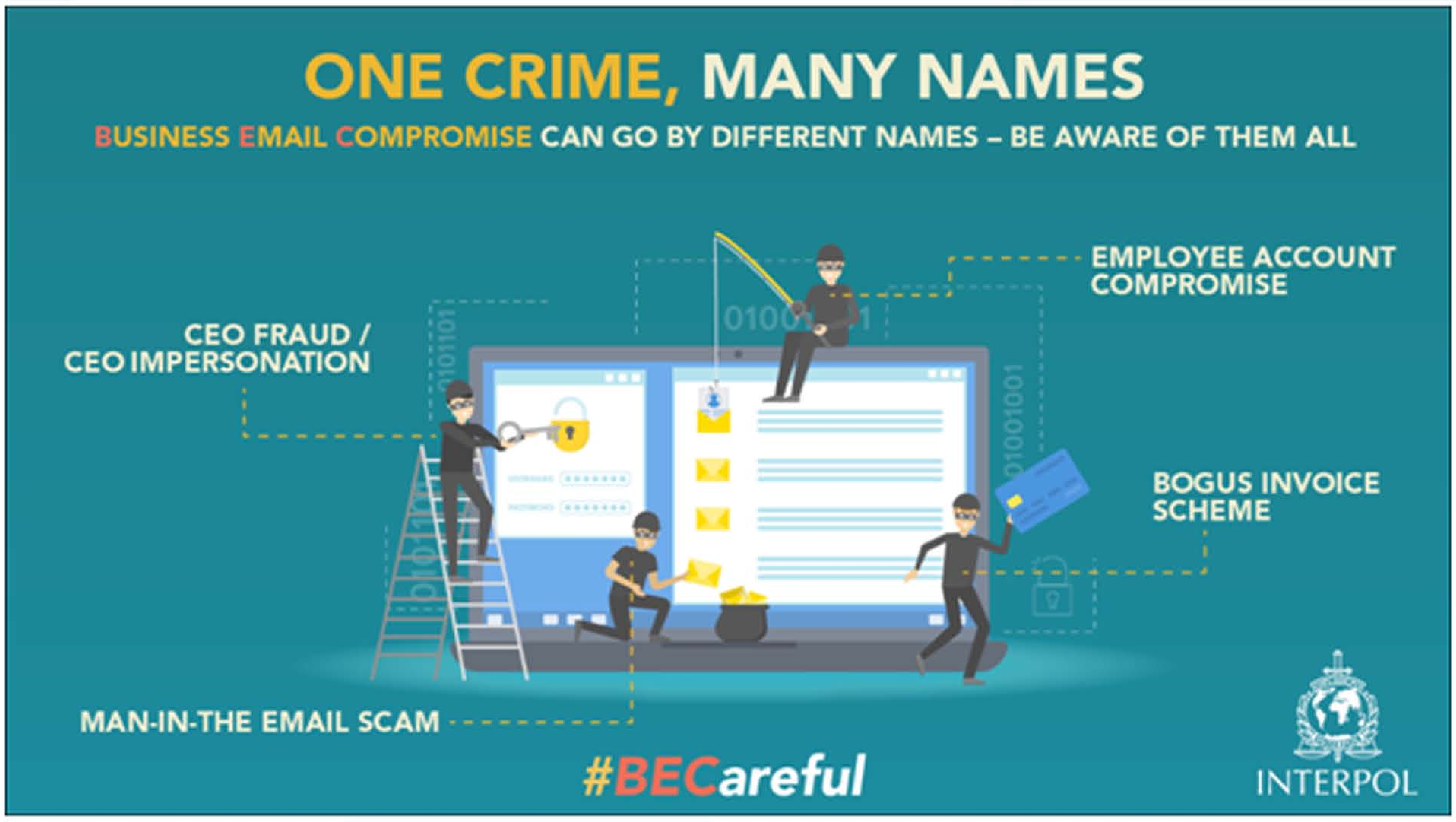

ONE CRIME, MANY NAMES
BUSINESS EMAIL COMPROMISE CAN GO BY DIFFERENT NAMES – BE AWARE OF THEM ALL
EMPLOYEE ACCOUNT COMPROMISE
CEO FRAUD / CEO IMPERSONATION
BOGUS INVOICE SCHEME
MAN-IN-THE EMAIL SCAM
#BECareful
INTERPOL

FIGURE 1 - BUSINESS EMAIL COMPROMISE
Source: Interpol

CONTENTS

Business Email Compromise: A Billion-Dollar Problem 2
BEC and a Working Definition........ 4
Attack Chain........ 5
Phase 1........ 5
Phase 2........ 5
Phase 3........ 5
Real-World Scenarios: Past, Present, and Future........ 6
The Snapchat Incident........ 7
Gift Card Scams........ 7
Present BEC Trends........ 8
COVID-19........ 8
Microsoft Office 365........ 8
Work-From-Home Dangers........ 10
How to best defend against BEC Scams........ 11
The LMNTRIX XDR - BEC Protection Solution........ 12
Protection against account take over and insider risk........ 12
Brand protection and domain fraud visibility........ 13
About LMNTRIX........ 15

FIGURE 1 - BUSINESS EMAIL COMPROMISE 2
FIGURE 2 - BEC LOSSES 2019 4
FIGURE 3 - BEC LOSSES 2020 4
FIGURE 4 - REAL-WORLD SCENARIOS 6
FIGURE 5 - LMNTRIX XDR - BEC PROTECTION SOLUTION........ 12
FIGURE 6 - SPEAR PHISHING........ 13
FIGURE 7 - BUSINESS EMAIL COMPROMISE 14
FIGURE 8 - ACCOUNT TAKEOVER 14

BEC AND A WORKING DEFINITION

Coming up with an exact definition of what a BEC scam is or consists of is difficult as tactics and methods employed by scammers have evolved over the years. This evolution has also brought with it high levels of sophistication as experienced cyber threat groups have seen the potential for profit. This has somewhat muddied attempts to set in stone what a BEC scam is and any definition is likely to be outdated in a few weeks or months.

While providing a definition may be difficult, BEC scams do exhibit a few common characteristics that set them apart from other scams. As to why the scam is referred to as a business email compromise is because the threat actor will compromise the email of a business or a business partner or vendor. The threat actor then sends emails from a compromised account pretending to be a company's CEO or CFO and requests that a payment needs to be made to the banking details provided in the email.

Alternatively, the email is from a trusted vendor or partner requesting payment for services rendered. The threat actor will not only pretend to be a high ranking member of staff within the business but can employ various other social engineering tricks to further add credence to their claims.

If the employee does as instructed, the attack chain is complete. The funds can be transferred to bank accounts controlled by money mules and sent on to be laundered through complex money laundering rings. Over the years Hong Kong has developed the unsavory reputation for being the centre of operations for many of these money mule and laundering rings.

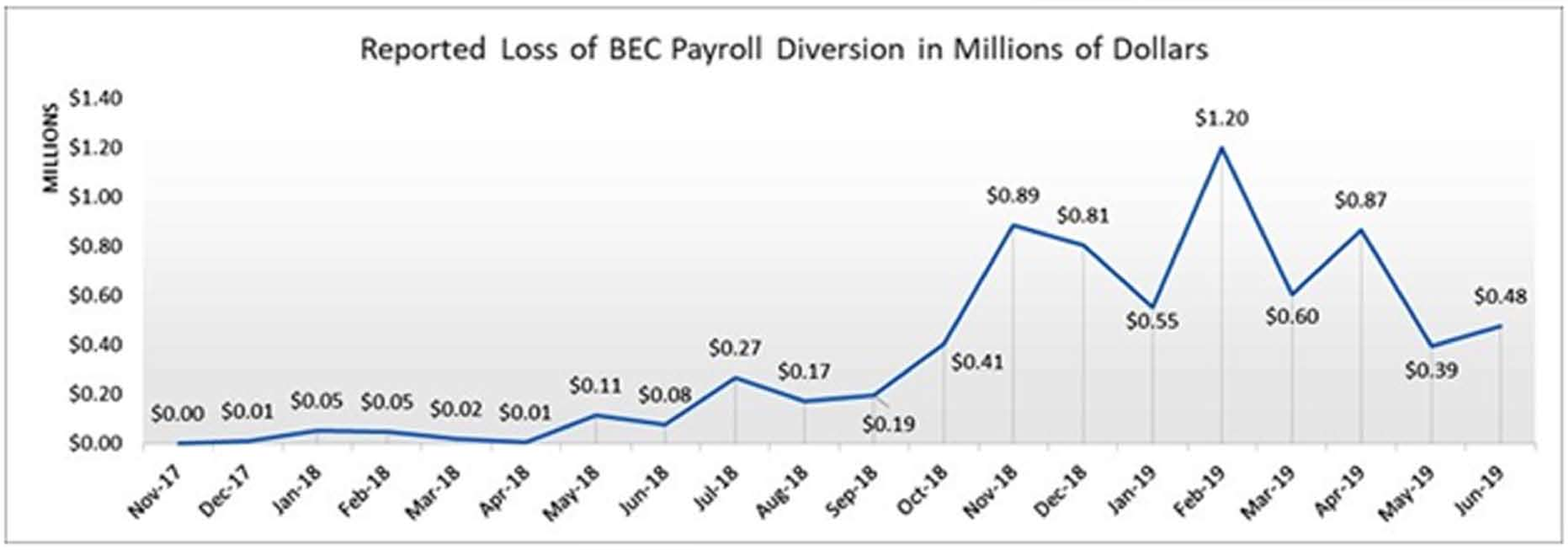


FIGURE 2 - BEC LOSSES 2019.

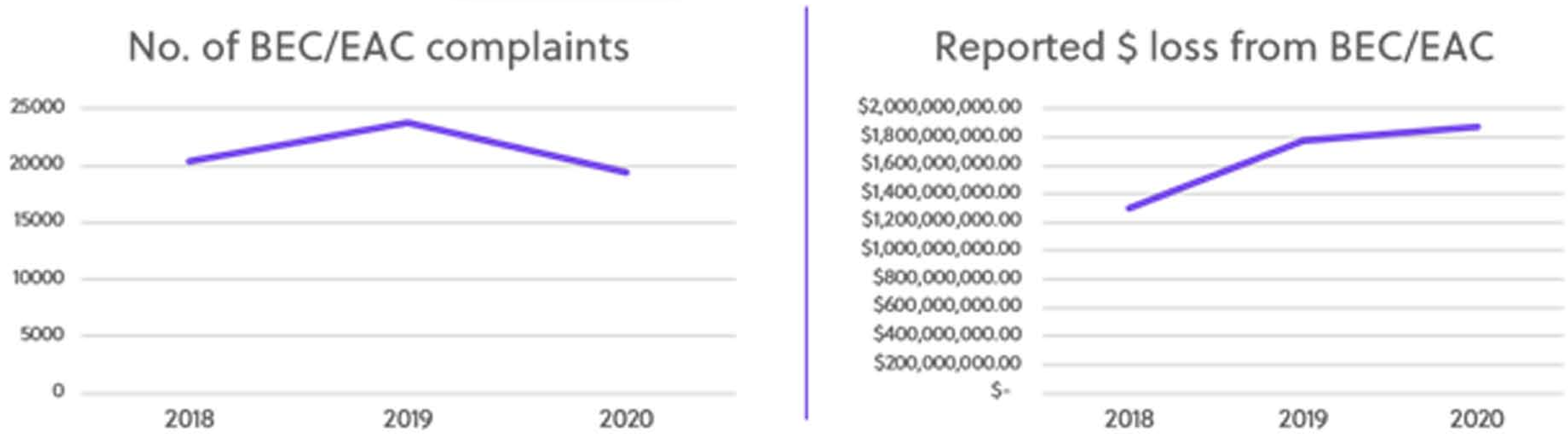


FIGURE 3 - BEC TRENDS 2020

ATTACK CHAIN

From start to finish a BEC scam will move through three phases. Understanding these phases can help businesses detect a scam, especially if detection is done early, in phase 1 or 2 that will be explained below.

Phase 1

- This phase is typically seen as how the threat actor gains initial access to the targeted business.

- This can be done in several ways but researchers have noted several that have been abused enough to be considered popular. These methods have the primary goal of gaining employee credentials so the threat actor gains access to the target's infrastructure, namely email servers or email accounts.

- Methods of gaining credentials include:
  - → Credential harvesting from data dumps and massive data breaches
  - → Spear phishing
  - → Social engineering campaigns designed to trick users into handing over credentials

Phase 2

- This phase is characterized by threat actor looking to gain as much information about the organization and targeted employees.

- This reconnaissance phase allows the threat actor to learn the language, tone, and templates used by the user.

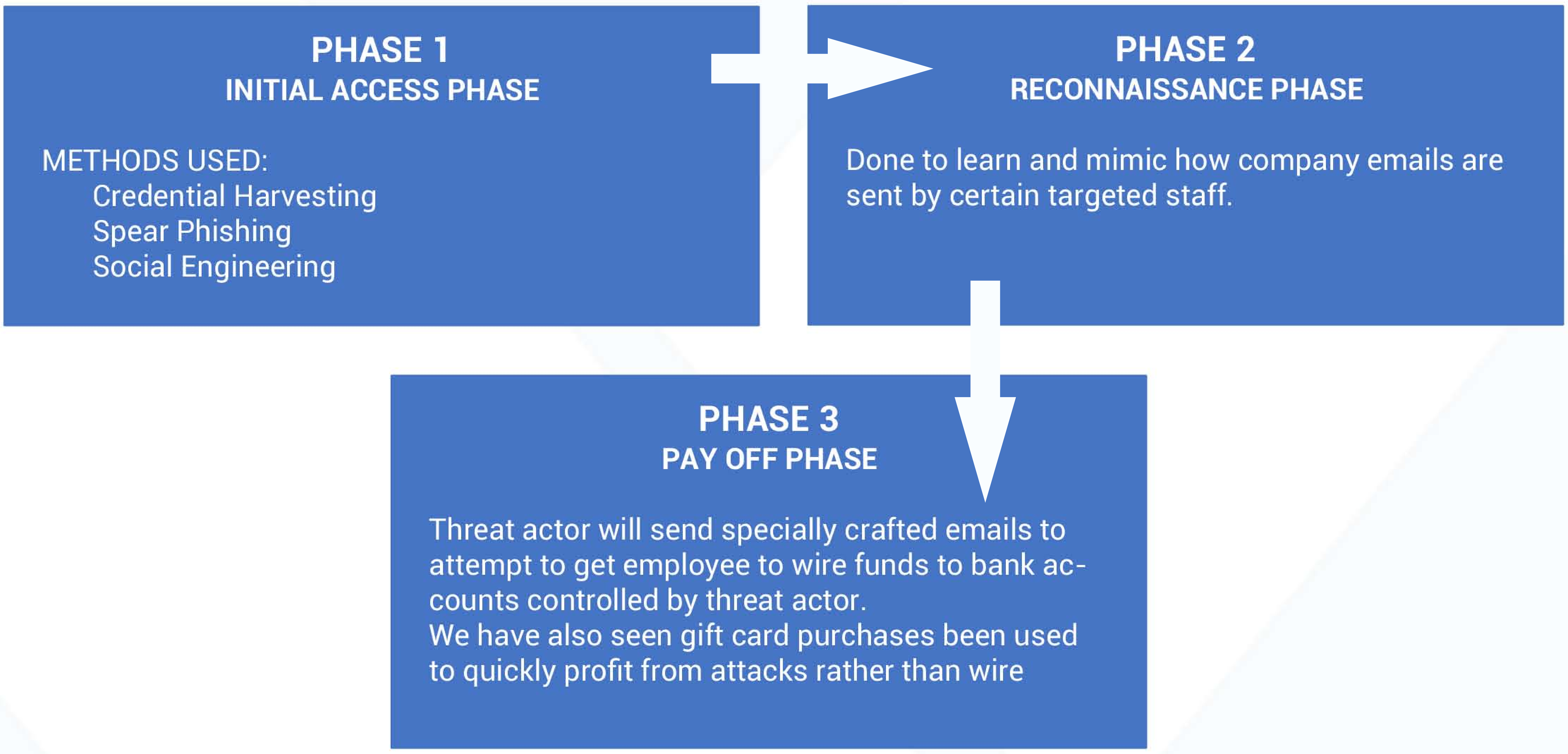
- This phase also allows the threat actor to learn how the targeted user interacts with the infrastructure and other employees.

Phase 3

- This phase is defined by the threat actor trying to profit from the work so far.

- Here the threat actor will send out emails that mimic upper management to get money paid into an account controlled by the threat actor or a money mule in league with the threat actor.

- In the past, we have seen some BEC scams that involve threat actors from registered domains that at first glance will look incredibly similar to the one the business had registered. The chances of success when doing this are slimmer as they will often skip critical steps in the first two phases and rely solely on the similar domain to try and trick the recipient of the email.



PHASE 1
INITIAL ACCESS PHASE

METHODS USED:
- Credential Harvesting
- Spear Phishing
- Social Engineering

PHASE 2
RECONNAISSANCE PHASE

Done to learn and mimic how company emails are sent by certain targeted staff.

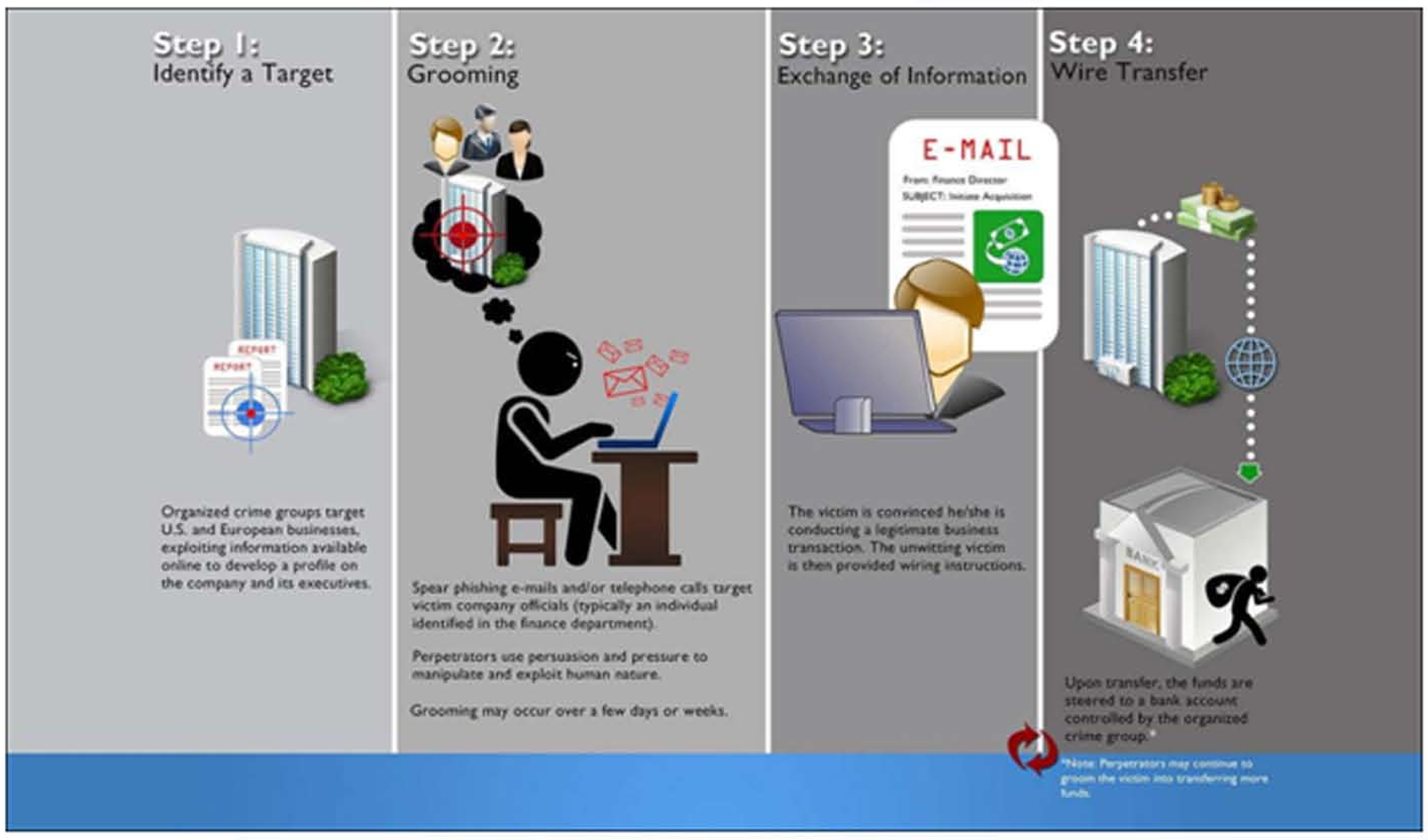
PHASE 3
PAY OFF PHASE

Threat actor will send specially crafted emails to attempt to get employee to wire funds to bank accounts controlled by threat actor.
We have also seen gift card purchases been used to quickly profit from attacks rather than wire

REAL-WORLD SCENARIOS: PAST, PRESENT, AND FUTURE

BEC scams are often seen as the evolution of 419 scams that plagued individual users in the 1990s. Emails from supposed Nigerian princes who would be incredibly generous if they received some help to jump a financial hurdle became one of Nigeria's biggest exports. Nigeria was then to become the epicenter for the BEC tidal wave. This prompted a response from Nigerian law enforcement as well as US law enforcement and while Nigeria is still responsible for an estimated 50% of attacks, other scammers around the globe are now profiting.

With financially motivated cybercrime groups also making use of BEC scam tactics we have seen a wide variety in how scams have been carried out. What follows is a brief look at some import scams that have occurred.



Organized crime groups target U.S. and European businesses, exploiting information available online to develop a profile on the company and its executives.

Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual identified in the finance department).

Perpetrators use persuasion and pressure to manipulate and exploit human nature.

Grooming may occur over a few days or weeks.

The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Upon transfer, the funds are steered to a bank account controlled by the organized crime group.*

*Note: Perpetrators may continue to groom the victim into transferring more funds.

FIGURE 4 - REAL-WORLD SCENARIOS
Source: Federal Bureau of Investigation

THE SNAPCHAT INCIDENT

This was possibly the first high profile case that received public attention and details about the attack were made public in March 2016. The scammer in this instance impersonated the company's CEO and managed to trick an employee into sending payroll information for then current and former employees.

At the time of the incident Snapchat releases a press statement apologizing to employees, noting that,

> "The good news is that our servers were not breached, and our users' data was totally unaffected by this. The bad news is that a number of our employees have now had their identity compromised. And for that, we're just impossibly sorry,"

Information like company payroll contains a wealth of personally identifiable information which can fetch a premium on Dark Web marketplaces. This information can in turn be used to commit identity theft or various other kinds of fraud. Here we see that it is not only payment scammers are after, but sensitive data can be sold off to the highest bidder to generate a profit.

GIFT CARD SCAMS

These scams are remarkably similar to BEC scams in that the scammer will impersonate someone that the victim would perceive as credible. Rather than asking for money to be transferred to an account, the scammer asks for popular retail gift cards to be purchased. Again it is often seen that the scammer will impersonate a CEO and the request for gift cards may be for corporate gifts to loyal customers or for competitions held within the company.

The reason for the scammer wanting a gift card or several is that they can be easily converted to cash. There is no need for complicated wire transfer instructions to be given out and given the prevalence of wire fraud; some companies have become incredibly wary of making transfers. By requesting a gift card the scammer hopes to circumvent any controls the company has placed on wire transfers.

This method of scamming business seemingly exploded in 2018 with the FBI noting.

> "A total of 1,164 complaints were filed with IC3 between January 1st, 2017 and August 31st, 2018 with an adjusted loss of $1,021,919. Although the average reported loss per incident was less than $900, the number of complaints reporting fraudulent gift card requests increased over 1,240% between January 1st, 2017 and August 31st 2018, with over 90% of incidents reported between March and August 2018. This scenario did not register as a measurable trend in 2017."

PRESENT **BEC TRENDS**

COVID-19

Since the global pandemic sent many countries into lockdown and hospitals around the world struggled to treat those infected, scammers were looking to see how best to exploit the terrible scenario. As people were dying BEC scammers were modifying tactics to try and take advantage of the horrible new reality we found ourselves in.

Security researchers detected several ways in which the pandemic was used to scam businesses. Some looked to abuse payroll by asking staff in the payroll department to change the banking details of staff wanting who had changed banks to one that was closer. This appears to be a prudent measure in a time when our freedom of movement was limited. The truth is the scammer impersonated the employee and provided banking details linked to them or their cybercrime organization.

Another cover of the same track was also seen by researchers where employees received emails relating to legal matters concerning COVID-19 and staff. These scams are presented as if they are from attorneys handling a matter and either requires payment for services rendered or personal information pertaining to employees that can then be sold off.

In 2019 the FBI warned,

> "BEC/EAC is constantly evolving as scammers become more sophisticated. In 2013, BEC/EAC scams routinely began with the hacking or spoofing of the email accounts of chief executive officers or chief financial officers, and fraudulent emails were sent requesting wire payments be sent to fraudulent locations. Over the years, the scam evolved to include compromise of personal emails, compromise of vendor emails, spoofed lawyer email accounts, requests for W-2 information, the targeting of the real estate sector, and fraudulent requests for large amounts of gift cards.
>
> In 2019, the IC3 observed an increase in the number of BEC/EAC complaints related to the diversion of payroll funds. In this type of scheme, a company's human resources or payroll department receives an email appearing to be from an employee requesting to update their direct deposit information for the current pay period. The new direct deposit information generally routes to a pre-paid card account."

This warning foreshadowed how many BEC scams would play out this time abusing peoples reaction to the COVID-19 pandemic in order to add legitimacy to their claims.

Microsoft Office 365

In recent times the abuse of Office 365 by BEC scammers has skyrocketed. In one instance the Microsoft Digital Crimes Unit removed 17 malicious domains. The domains are referred to as "homoglyph" domains as they are designed to resemble legitimate domains as much as possible. The domains were used in conjunction with stolen credentials to access Office 365 mail servers to ultimately try and commit wire fraud. The threat actors would observe the internet and email traffic of the victim's business to better mimic how an important figure within the business would operate and communicate.

In May 2021, Microsoft again discovered a BEC scam that compromised several victims and involved the actors typo-squatting 120 different legitimate businesses. Researchers were quick to point out that,

> "We noted that these domains did not have domain privacy enabled, nor were they under the EU's GDPR protections. Each domain used a unique registrant name and email. The registrant names appeared to be auto generated random first names and last names, and the registrant contact email used a free email service such as Gmail or mail.com with accounts that were often simply <first name>.<last name>@gmail.com or similar. Each name was used to register just one domain used in the campaign, which made pivoting to related domains more challenging.
>
> Another observation about this campaign is that the registered domains did not always align with the organization being impersonated in the email. This could have been a mistake on the actor's part, as BEC domains are typically designed to closely mimic the impersonated organization. For example, an actor may register microsoft.xyz or micrrosoft.com, both of which would normally be used to send emails pretending to originate from Microsoft. In this campaign, those types of homoglyphed and typo-squatted domains were used to send emails pretending to originate from a variety of organizations."

This campaign again shows how varied tactics and techniques can be from campaign to campaign. It is also important to note that in this campaign the threat actors attempted to extort gift cards from victims, rather than transfers to a bank account.

Two more new and innovative tactics have been recently seen employed against Office 365 users. The first has become known as a read receipts attack. This is when the scammer manipulates the "Disposition-Notification-To" email header to generate a receipt notification from Office 365. This is done to bypass email security measures as the initial malicious email may be successfully stopped but not the receipt.

The second new attack tactic is known as an Out-of-Office attack. This is when the scammer impersonates another employee but the scammer manipulates the Out-of-Office reply to protocol so that the target ends up sending the Out-of-Office reply to another employee within the organization. Put differently researchers have explained the attack anatomy as the following,

> "A fraudster creates a typical business email compromise (BEC) email, designed to scam a company out of money. However, rather than just sending the email as-is, the scammer manipulates the headers of the email (in this case the "Reply-to:" field) to point to another individual within the targeted organization. So, the email may be sent to one employee (let's call them John), but the "Reply-to" header contains another employee's email address (let's call them Tina).John has his Out-of-office reply enabled, so when he receives the fraudulent email an automatic reply is generated. However, the Out-of-office reply is not sent back to the true sender, but to Tina instead - and includes the extortion text."

Work-From-Home Dangers

One of the biggest dangers faced by businesses regarding BEC scams as well as other malware attacks is the current work-from-home regime. There have been several instances of scammers attacking those forced to work-from-home following COVID-19 lockdowns and regulations.

Scammers know that the drive to work from home has left organizations with many gaps in their security. The distance between the office and the home means that a lot of the software and hardware protections the business invested in will not apply to those working from home. This has given scammers better opportunities to compromise business email servers.

HOW TO BEST DEFEND AGAINST **BEC SCAMS**

There are several easily adopted defensive measures business can take to defend against BEC scams. These include:

- Enable multi-factor authentication, this can prevent a large number of BEC scams as the scammer will be unable to verify themselves from multiple devices simultaneously.
- Monitor geolocation data, this can help analyze and block malicious traffic.
- Require that wire transfers are signed so as to create a paper trail.
- Help educate staff about common BEC tactics including those covered in this document.

While the above points are brief in the extreme, we will look at two broad factors to better help defend against BEC scams. Those being the employee and the organization. When it comes to the employee, as mentioned above, education is key. Make it company policy to adopt a zero-trust policy and to always be skeptical of an email, no matter who it is sent from. When it comes to staff in charge of payments make sure that company policy demands that all banking details be checked, and no matter who the payment request is from it is not rushed, further a company wide ban on gift card purchasing can be enacted. Even if it sounds like banging your head against a wall, insist that company procedures be followed at all times. Empower your staff to trust their instincts, if an email triggers a warning bell within them have them report it to staff who handle cyber security concerns.

The second factor is the organization itself. When developing company policies, make sure high value transactions require sign off by multiple staff. Only work with verified and well established vendor accounts, any changes to their banking details must require a high level of proof and reasoning behind the change. Provide the necessary education alluded to above. Make use of readily accessible technology like SPF / DKIM / DMARC that prevents email spoofing and blocks email traffic from untrusted sources.

THE **LMNTRIX XDR** - BEC PROTECTION SOLUTION

The **LMNTRIX XDR** - BEC Protection Solution approach complements the client's existing security controls to further protect against BEC scams. This is done through our unique API-based architecture that provides our AI engine access to historical email data to learn each user's unique communication patterns. Further, the engine leverages multiple classifiers to map the social networks of every individual inside the company and identifies anomalous signals in message metadata and content.

Our unique approach does not rely on static rules to detect targeted attacks. It relies on data that provides historical statistics on each organization to determine with a higher degree of accuracy whether a certain email is part of a socially engineered attack or account takeover. As an added measure for our clients leveraging Office 365, we have added an extra layer of security to Office 365 email servers. **LMNTRIX XDR** service scans Office 365 accounts, by making use of Office 365's APIs, to protect against advanced threats and spear phishing attacks that hide inside users' mailboxes.

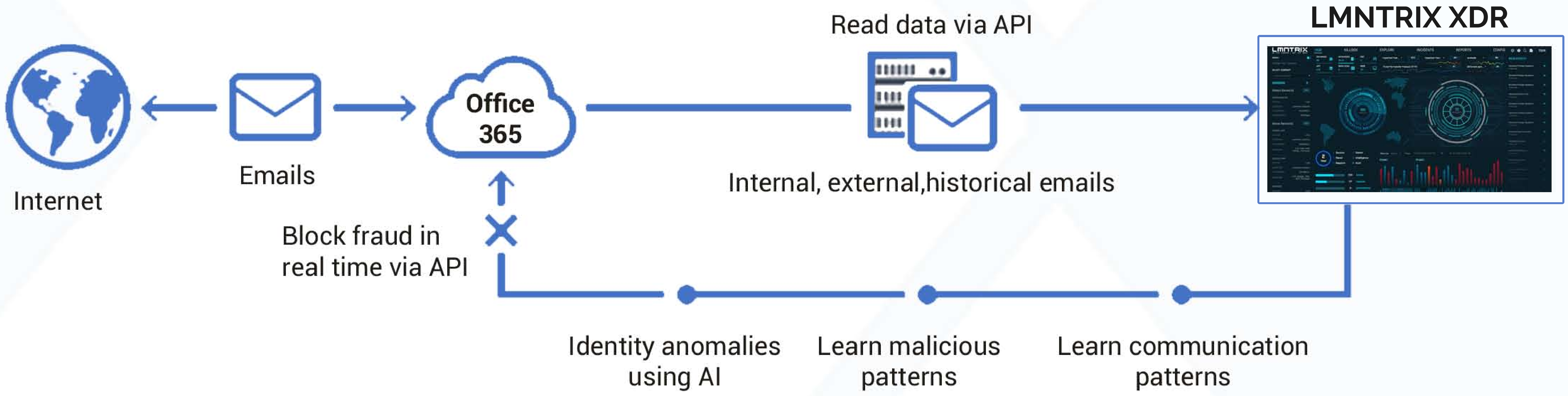

LMNTRIX XDR
Read data via API
Internet
Emails
Office 365
Internal, external,historical emails
Block fraud in real time via API
Identity anomalies using AI
Learn malicious patterns
Learn communication patterns

FIGURE 5 - LMNTRIX XDR - BEC PROTECTION SOLUTION

Protection against account takeover and insider risk

Everyday, legitimate business accounts get compromised due to stolen credentials. Account takeover can remain dormant in your SMB environment for months, with hackers watching and learning before launching their attacks.

The **LMNTRIX XDR's** comprehensive solution to account takeover includes three components: prevention, detection, and remediation. It prevents targeted phishing attacks that bypass traditional email gateways and can lead to harvesting credentials. If an account has been compromised, it detects the anomalous behavior and alerts IT. Finally, it can remediate the attack by removing all of the malicious emails sent by the compromised account from within employee mailboxes with one click.

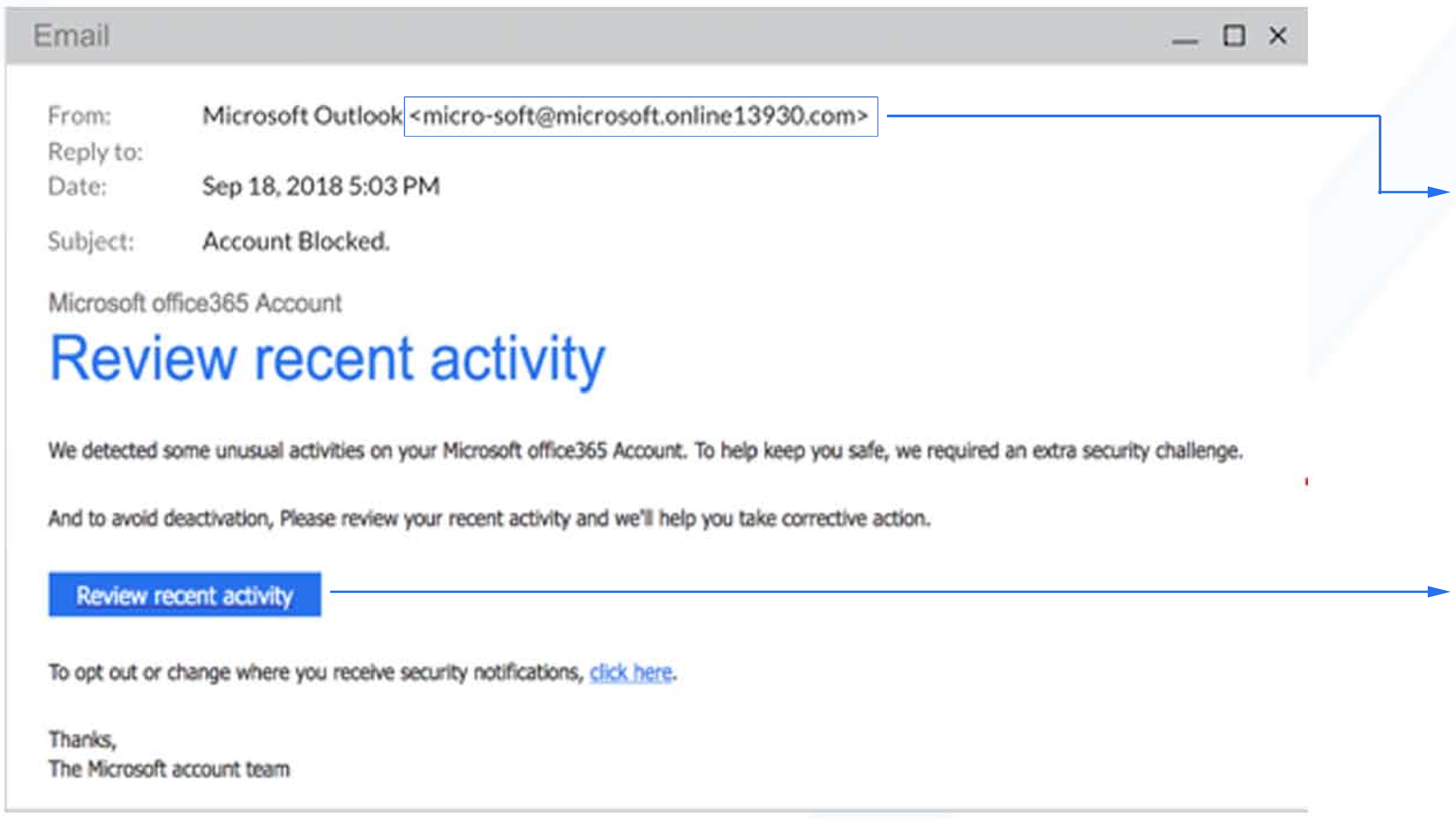
Brand protection and domain fraud visibility

Domain spoofing and brand hijacking are common techniques used by hackers in social engineering attacks. Domain spoofing can be used to target your customer's employees, external partners, and other third parties who might trust their brand. **LMNTRIX XDR** provides complete protection from email domain fraud through DMARC (Domain-based Message Authentication Reporting and Conformance) reporting, analysis, and visibility.

LMNTRIX XDR offers an intuitive wizard to help you easily set up DMARC authentication. Once DMARC is properly configured, it provides granular visibility and analysis of DMARC reports to help you properly set-up DMARC enforcement and reduce the potentialof false-positives enforcements. Well configured DMARC enforcement ensures deliverability of legitimate email traffic and prevents unauthorized spoofing emails.

LMNTRIX XDR detects threats that email gateways can't.

It integrates directly with Microsoft Office 365 APIs to detect attacks coming from both internal and external sources. It uses artificial intelligence to detect signs of malicious intent and deception within every email with virtually no IT administration required.



From: Microsoft Outlook <micro-soft@microsoft.online13930.com>
Reply to:
Date: Sep 18, 2018 5:03 PM
Subject: Account Blocked.

Microsoft office365 Account

Review recent activity

We detected some unusual activities on your Microsoft office365 Account. To help keep you safe, we required an extra security challenge.

And to avoid deactivation, Please review your recent activity and we'll help you take corrective action.

To opt out or change where you receive security notifications, click here.

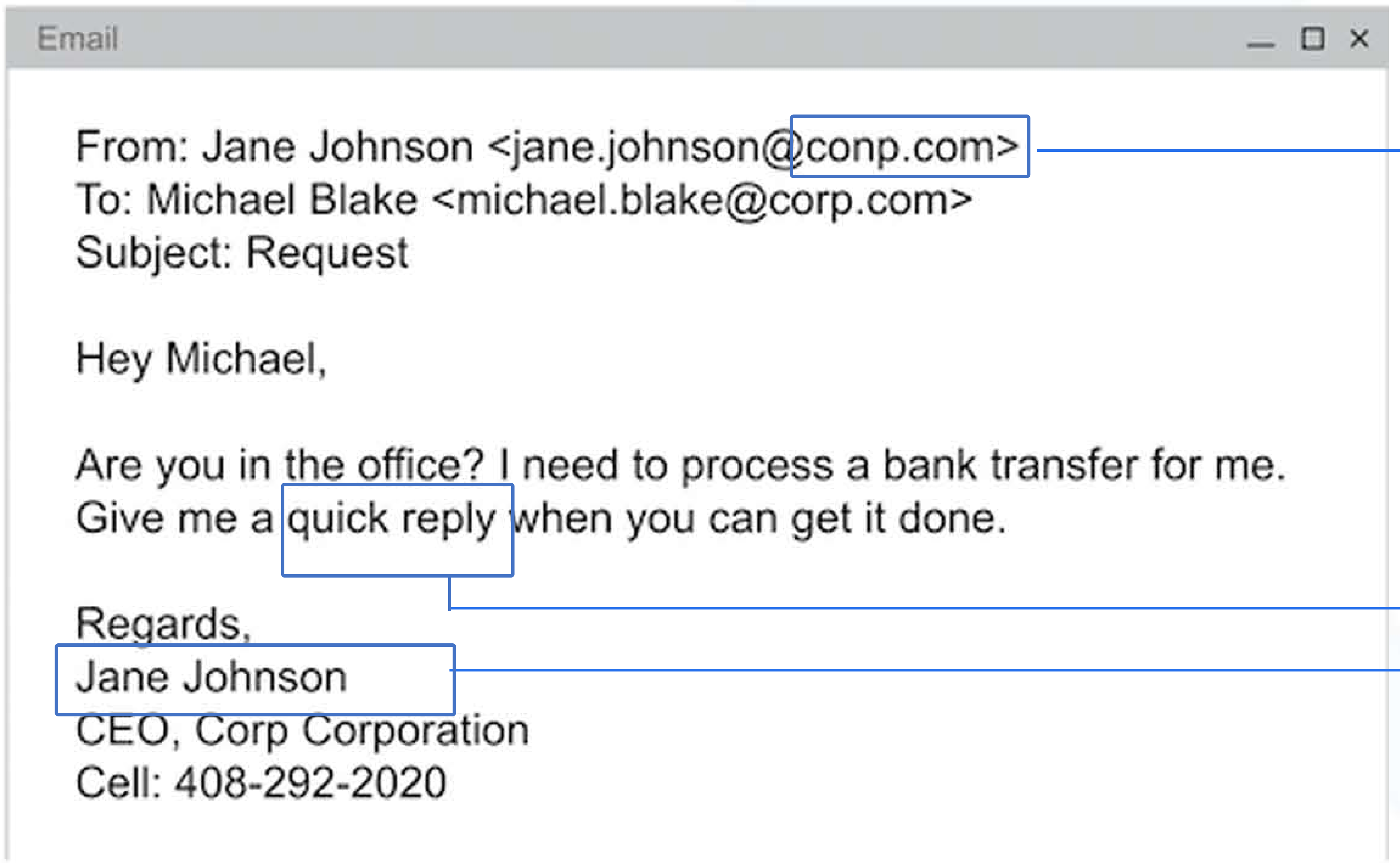
Thanks,
The Microsoft account team

LMNTRX XDR stops spear phishing attack using web impersonation and high reputation links.

Email is not from Microsoft O365

Link to a phishing site hosted on high reputation domain

FIGURE 6 - SPEAR PHISHING



From: Jane Johnson <jane.johnson@conp.com>
To: Michael Blake <michael.blake@corp.com>
Subject: Request

Hey Michael,

Are you in the office? I need to process a bank transfer for me.
Give me a quick reply when you can get it done.

Regards,
Jane Johnson
CEO, Corp Corporation
Cell: 408-292-2020

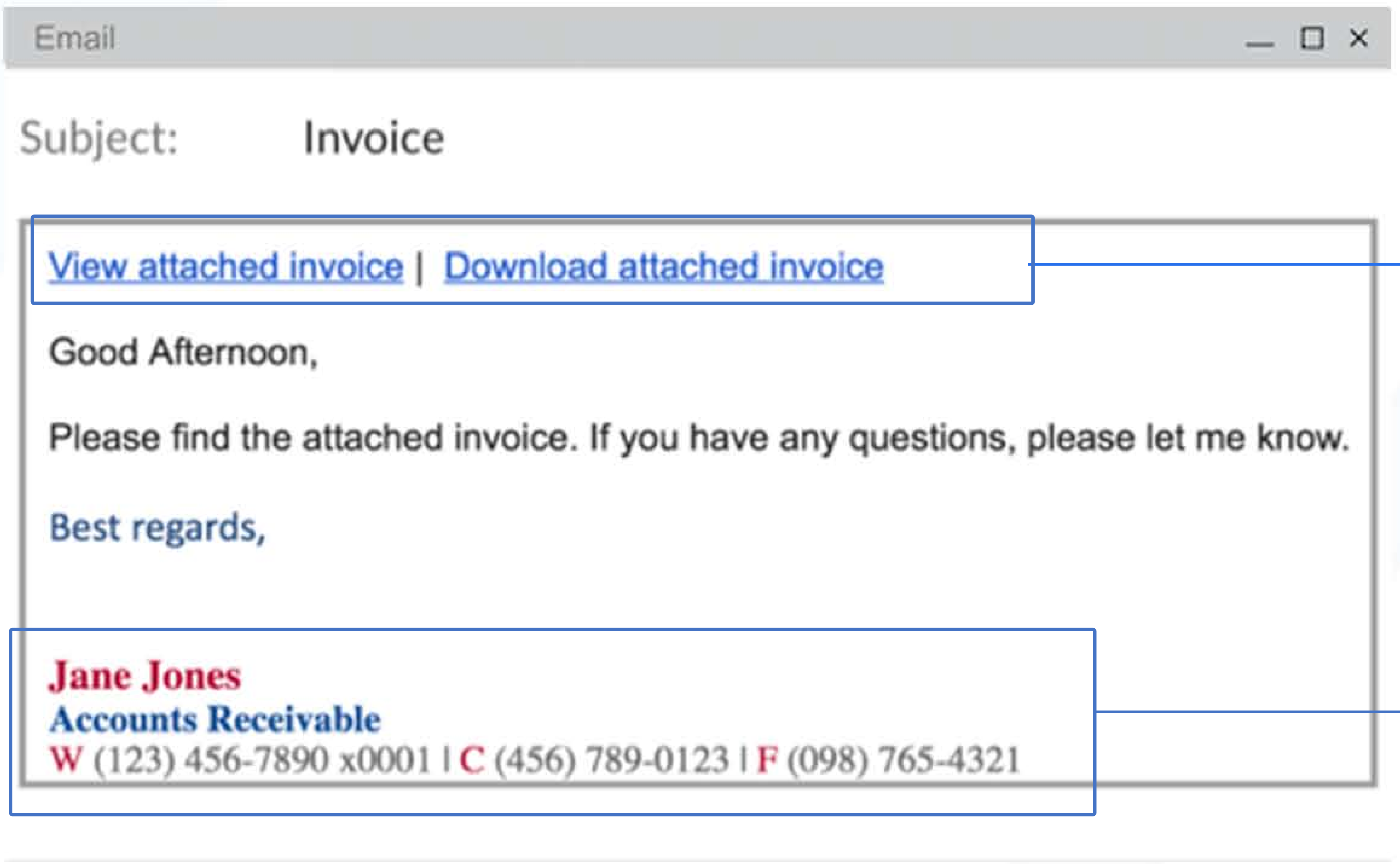
LMNTRIX XDR stops Business Email Compromise and CEO fraud from reaching its intended recipient.

Misspelled sender email domain

Sense of urgency

Wire transfer request is unusual for this employee

FIGURE 7 -BUSINESS EMAIL COMPROMISE



Subject: Invoice

View attached invoice | Download attached invoice

Good Afternoon,

Please find the attached invoice. If you have any questions, please let me know.

Best regards,

Jane Jones
Accounts Receivable
W (123) 456-7890 x0001 | C (456) 789-0123 | F (098) 765-4321

LMNTRIX XDR account takeover attempts and attacks that originates from compromised account.

Suspicious links

Email sent to people this individual doesn't usually communicate with

FIGURE 8 -ACCOUNT TAKEOVER

ABOUT **LMNTRIX**

LMNTRIX was founded by Carlo Minassian, a cybersecurity entrepreneur with over twenty years in the industry. Carlo pioneered MSSP in Australia after seeing a need in the market that few did. He left a secure future with IBM to start a business in his bedroom. He and his team were so far ahead of the curve they struggled at first. Thirteen years later this company, earthwave, had become a Gartner magic quadrant leader and was sold to Dimension Data. Carlo embarked on the journey to globalize the service he had created.

What he discovered over the next three years amazed him. In fact, it really got him worried. On the front lines, engaging with hundreds of organizations worldwide, something was terribly wrong. Instead of getting more secure, companies and organizations were more vulnerable than ever.

What Carlo learned next is the reason **LMNTRIX** exists.

IT'S NOT ABOUT THE MONEY

Yahoo, Target, Sony, RSA, Ebay, Anthem, the US Military, Heartland, Dropbox, JP Morgan Chase, Home Depot, Linkedin, Adobe, the NSA, and a thousand others that shall remain un-named, were investing millions of dollars per annum on their cyber security programs. Many had security forces of hundreds of experts together with shiny SOC's and the latest next generation sandboxes, firewalls, SIEM's, EDR, you name it, but when it mattered . . . They. Just. Didn't. Know.

TOO MANY ALARMS, TOO LITTLE TIME

How could this be? As Carlo travelled the world, he discovered that corporate cybersecurity teams were being defeated by a single enemy. It wasn't the hackers — it was the noise.

All the companies reported one thing: alert fatigue. The shiny boxes and impressive solutions were great at producing alerts, but not so good at telling the signal from the static. Organization's told Carlo they were receiving 300 or more alerts per month from their MSSP, but had no way to tell if the alerts were actual incidents. Their teams lacked the time or skills to respond. The result: alerts were ignored.

The boy had cried wolf too many times. Now the wolf was freely roaming these networks devouring whatever it wanted.

THE ACTION WAS ON THE INSIDE

But it wasn't only alerts.

After a year of research that included surveying 350 companies across multiple regions and dozens of in-depth interviews, Carlo isolated three unmistakable facts at the heart of the problem:

1. Alert Fatigue. Only one percent of all attacks are detected through logs. This is an astounding number and SIEM has proven to be a particular failure. Interviews with IT teams delivered this frustrated indictment of SIEM: "Stupidly Irrelevant Electronic Messaging" (actually they called it something a whole lot worse, but we're too polite to say that here). They said SIEMs produced too many alarms. MSSPs aren't doing much better for those who depend on them. Even medium-sized organizations can receive as many as 200-300 alerts per month from their MSSP and are then left with no idea what to do with them. The result is that alarms drone on while hackers roam free.

2. Lack of Breach Validation. The hackers roam free because companies have no way to confirm if these alerts are actual incidents. It is too time consuming and costly to investigate, and their security teams lack skills to respond to advanced threats. Imagine being told by the police that someone may have broken into your house but it was up to you to investigate further that's the situation most companies are in – it's wrong and needs to be fixed.

3. Fortress Mentality. Even though it should be clear by now that hackers are in the inside, organizations cling to the illusion that cyber security means keeping bad things out. This is about cyber-purity not true cybersecurity. It is a dangerous fantasy that does not reflect the inevitability of cyber intrusion. By holding onto it organizations are unable to respond properly to threats. This mentality is why Gartner is correct in saying the current blocking and prevention techniques are failing, and cybersecurity spending is incorrectly skewed.

So what did these three facts really mean? They meant almost everyone had things inside out.

With the median number of days before a breach was detected at 229 and 67% of companies only learning of a breach when an external entity told them, it was obvious that organizations had to make a mental shift.

They needed to stop fixating on the perimeter and start looking at their network more like an obstacle course where hackers could be deceived, worn down, paralyzed and ultimately thwarted. You protect what matters; they go away empty handed. This was about changing the economics of hacking. Make the cost of the hack impossible for the hackers to justify and you win.

ACTIVE DEFENSE IS BORN

When you make this fundamental shift in thinking, you start to think differently about how to detect and respond to threats. So at **LMNTRIX** we shift your security mindset from "incident response" to "continuous response," wherein systems are assumed to be compromised and require continuous monitoring and remediation.

By thinking like the attacker and hunting on your network and your systems, we allow you to move from being the prey to being the hunter. We then turn the tables on the attackers and change the economics of cyber defense by shifting the cost to the attacker by weaving a deceptive layer over your entire network – every endpoint, server and network component is coated with deceptions. From the instant an attacker penetrates your network, all they can see is an elusive mirage where every single data packet is unreliable. This deceptive environment immobilizes attackers as they are unable to make decisions if the data they've gathered is unreliable.

The **LMNTRIX** Active Defense is a validated and integrated threat detection and response architecture for addressing advanced and unknown threats that bypass an organizations perimeter controls.

We use a combination of advanced network and endpoint threat detection, deceptions everywhere, analytics and global threat intelligence technology. These are complemented with continuous monitoring together with threat hunting both internally as well as on the deep and dark web. It is a fully managed, security analyst delivered service that defends against zero-day attacks, and advanced persistent threats from our cyber defense center, 24 hours a day, 7 days a week.

GREAT SECURITY DOESN'T HAVE TO BE EXPENSIVE

Sometimes cheaper really is better. Carlo realized the secret that the cybersecurity industry didn't want anyone to hear is this: cybersecurity doesn't need to be expensive to be effective. Vendors charge a lot because they can (how better to offset the huge marketing costs that promise the next cybersecurity silver bullet?).

Carlo didn't want **LMNTRIX** to join that crowd, he wanted to sell cyber outcomes not cyber sizzle. That's why **LMNTRIX** runs smart. We hunt where it's quiet, we protect what matters, we use our wits not your pocketbook to deliver genuine protection. We believe you deserve better results, fewer excuses, and the right not to throw your money away because an industry said you must.

YOU ARE PART OF OUR MISSION

We do cybersecurity differently. We're not vendors trying to upsell or consultants hocking advice, we are your cyber bodyguards, outfoxing your potential assailants and keeping what matters safe.

This is a mission that will not only help make you secure and save you money doing it, but will help make everyone safer because by working together we become stronger and more effective. We live in a digital world. What happens on our networks has consequences in our communities. Cyber is simply too important to do alone.

Join us on a journey beyond excuses and into true cybersecurity where the ones being worn down and defeated are the hackers, not us.

Yours In CyberCertainty,
Team LMNTRIX