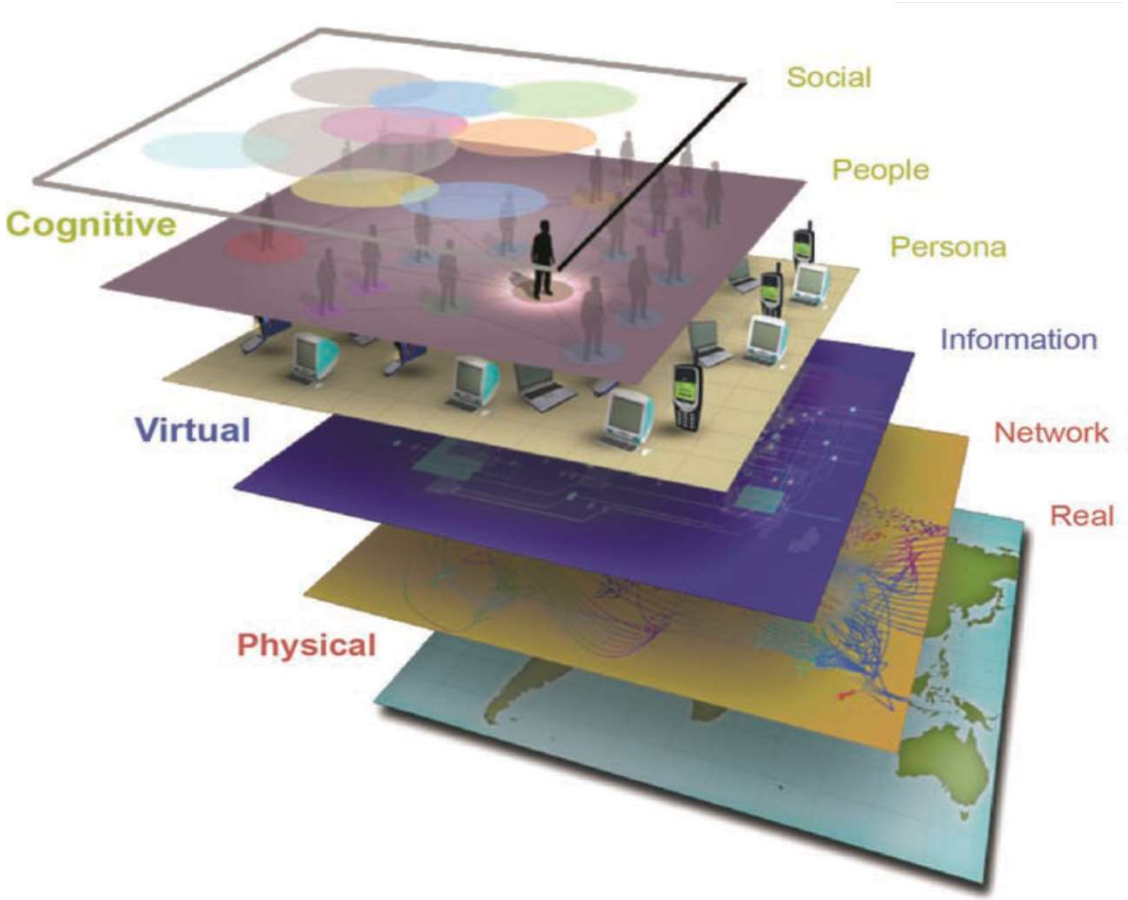
Psychology of Cyber Deception & Frontier Technologies

Dr Francis Gaffney

Senior Director – Mimecast Labs & Future Engineering

Holistic Estimation – Six Layers



Why Do We (Still) Get Deceived?

Physical World… Neuro-Linguistic Programming

Neuro:

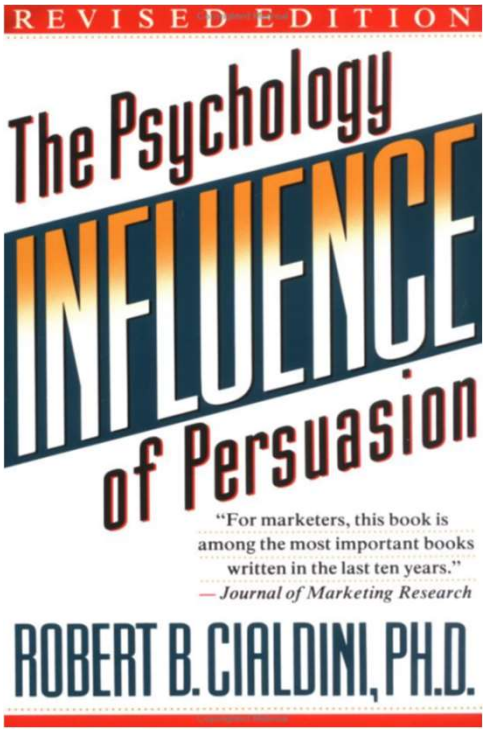
- how we experience and represent the world through our five senses and our neurological processes.

Linguistic:

- the way the language we use shapes and reflects our experience of the world.

Programming:

- training ourselves to think, speak and act in new and positive ways, in order to reach our maximum potential.



Physical World… NLP / Influencers – How to Spot Them

- Change in head position quickly
- Change in breathing
- Body movements
- Touch or cover mouth
- Instinctively cover vulnerable body parts
- Shuffling of feet
- It may be difficult for them to speak
- They may stare without blinking often
- Aggressive gestures

Physical World… NLP / Influencers – How to Spot Them

- The *How* they talk
- Over-emphasis of their truthfulness
- Hedged Statements
- Restating the Question
- Skipping contractions and other normal conversational words
- Using non-specific language, generalised phrases and sweeping statements
- Jump into defensive mode when questioned
- The Avoidance of “I”
- Dodging a direct answer
- Deflecting & Evading
- Embellishing insignificant details while avoiding important ones

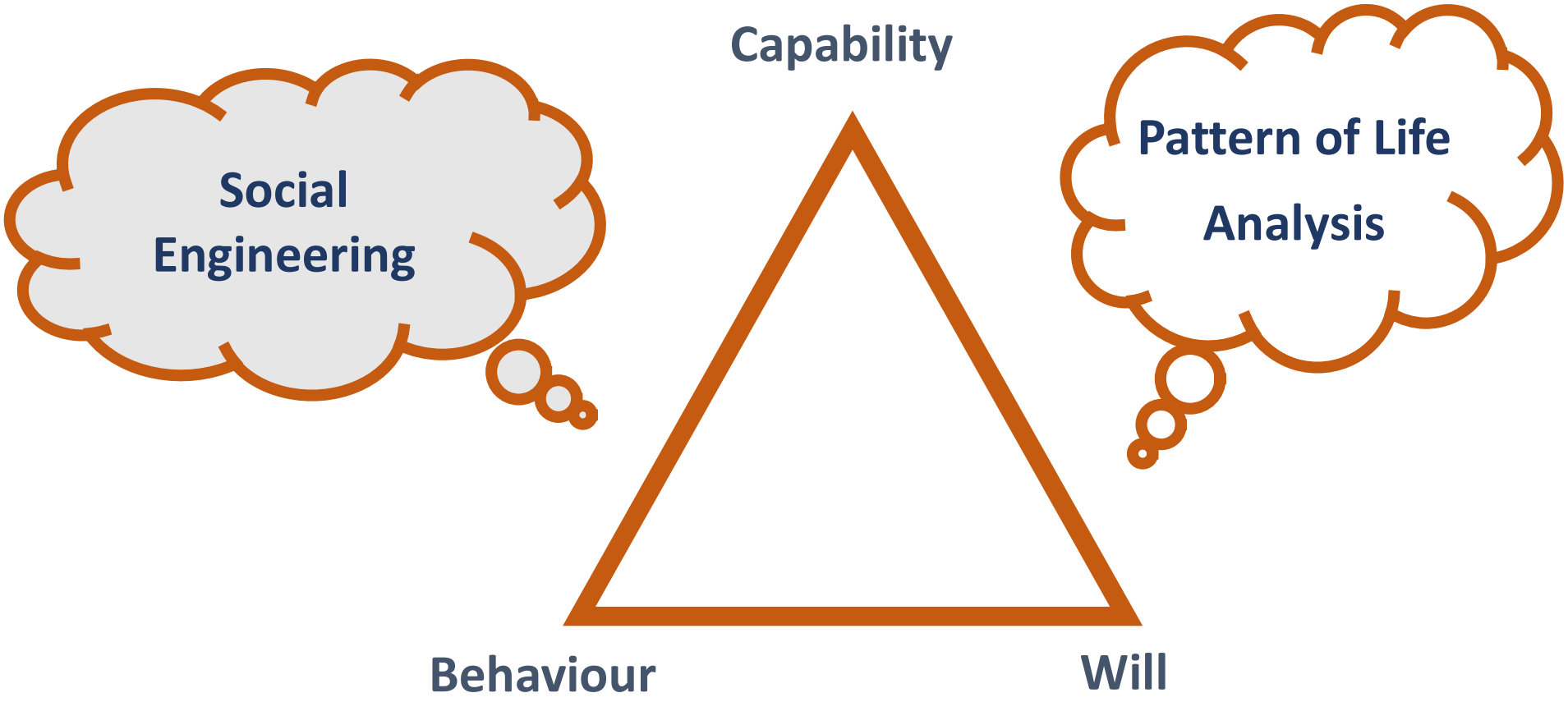
And you will read this last

You will read this first

And then you will read this

Then this one

Deception – “Influence Triangle”



Social Engineering – Pattern-of-Life Analysis

Physical World…

Prince William and Prince Harry's shock: Secret sister found

They are now honouring their mother by building a relationship with their 'forgotten' sibling. - by New Idea

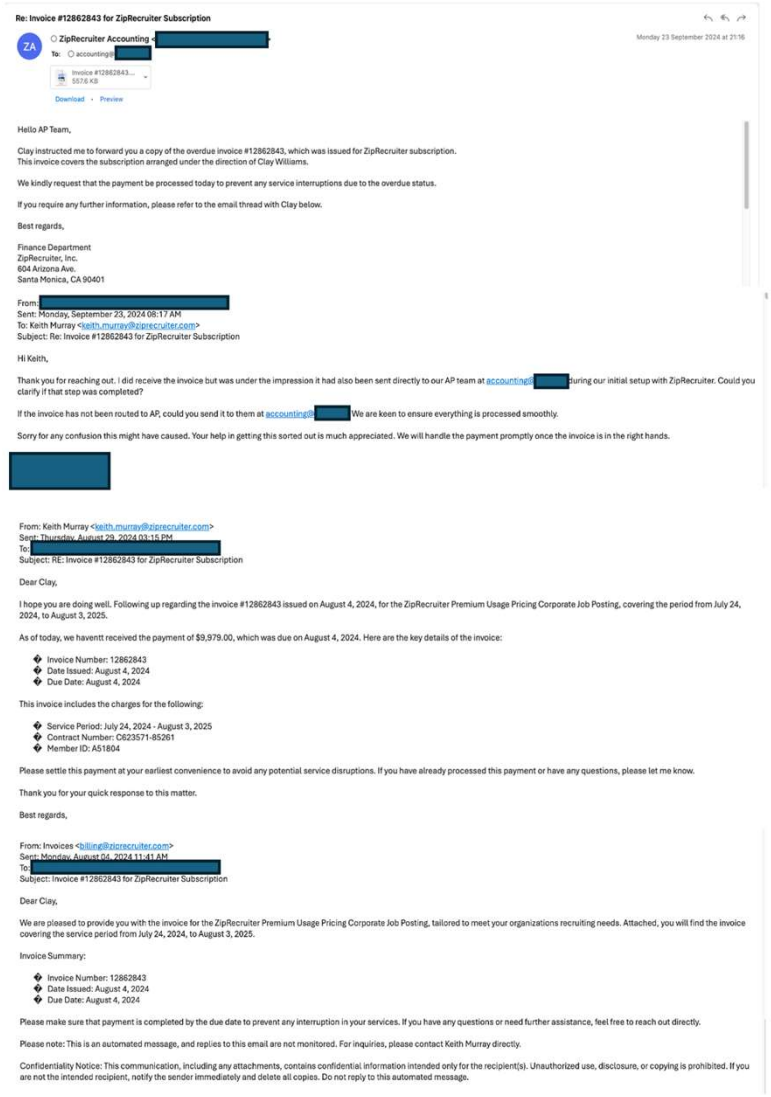
It was Princess Diana's secret dream to give her two sons a sister – now Princes William and Harry are honouring their mother by building a relationship with their 'forgotten' sibling.

Subs
Idea
Save
Subscri
today

delicious.

MCDONALD'S TO STOP SERVING THE BIG MAC

BEC Fake Threads Campaign



4

Re: Invoice #12862843 for ZipRecruiter Subscription

ZA ZipRecruiter Accounting <[redacted]>

To: accounting@[redacted]

Monday 23 September 2024 at 21:16

Invoice #12862843... 5876 KB

Download · Preview

Hello AP Team,

Clay instructed me to forward you a copy of the overdue invoice #12862843, which was issued for ZipRecruiter subscription.
This invoice covers the subscription arranged under the direction of Clay Williams.

We kindly request that the payment be processed today to prevent any service interruptions due to the overdue status.

If you require any further information, please refer to the email thread with Clay below.

Best regards,

Finance Department
ZipRecruiter, Inc.
604 Arizona Ave.
Santa Monica, CA 90401

3

From: [redacted]
Sent: Monday, September 23, 2024 08:17 AM
To: Keith Murray <keith.murray@ziprecruiter.com>
Subject: Re: Invoice #12862843 for ZipRecruiter Subscription

Hi Keith,

Thank you for reaching out. I did receive the invoice but was under the impression it had also been sent directly to our AP team at accounting@[redacted] during our initial setup with ZipRecruiter. Could you clarify if that step was completed?

If the invoice has not been routed to AP, could you send it to them at accounting@[redacted] We are keen to ensure everything is processed smoothly.

Sorry for any confusion this might have caused. Your help in getting this sorted out is much appreciated. We will handle the payment promptly once the invoice is in the right hands.

[redacted]

2

From: Keith Murray <keith.murray@ziprecruiter.com>
Sent: Thursday, August 29, 2024 03:15 PM
To: [redacted]
Subject: RE: Invoice #12862843 for ZipRecruiter Subscription

Dear Clay,

I hope you are doing well. Following up regarding the invoice #12862843 issued on August 4, 2024, for the ZipRecruiter Premium Usage Pricing Corporate Job Posting, covering the period from July 24, 2024, to August 3, 2025.

As of today, we haventt received the payment of $9,979.00, which was due on August 4, 2024. Here are the key details of the invoice:

- Invoice Number: 12862843
- Date Issued: August 4, 2024
- Due Date: August 4, 2024

This invoice includes the charges for the following:

- Service Period: July 24, 2024 - August 3, 2025
- Contract Number: C623571-85261
- Member ID: A51804

Please settle this payment at your earliest convenience to avoid any potential service disruptions. If you have already processed this payment or have any questions, please let me know.

Thank you for your quick response to this matter.

Best regards,

1

From: Invoices <billing@ziprecruiter.com>
Sent: Monday, August 04, 2024 11:41 AM
To: [redacted]
Subject: Invoice #12862843 for ZipRecruiter Subscription

Dear Clay,

We are pleased to provide you with the invoice for the ZipRecruiter Premium Usage Pricing Corporate Job Posting, tailored to meet your organizations recruiting needs. Attached, you will find the invoice covering the service period from July 24, 2024, to August 3, 2025.

Invoice Summary:

- Invoice Number: 12862843
- Date Issued: August 4, 2024
- Due Date: August 4, 2024

Please make sure that payment is completed by the due date to prevent any interruption in your services. If you have any questions or need further assistance, feel free to reach out directly.

Please note: This is an automated message, and replies to this email are not monitored. For inquiries, please contact Keith Murray directly.

Confidentiality Notice: This communication, including any attachments, contains confidential information intended only for the recipient(s). Unauthorized use, disclosure, or copying is prohibited. If you are not the intended recipient, notify the sender immediately and delete all copies. Do not reply to this automated message.

Identified Campaign Details

Examples identified in this detected campaign follow a template. These tactics employ a fabricated email trail, with the first three ‘emails’ placed into the final distributed email. Within that thread the threat actor tends to provide information around a particular service which the targeted organisation owes money for.

Analysis of these initial emails appear to be going to someone very senior in the organisation, with many examples detected showing the name of the organisations CEO as the addressee.

Following the initial fake emails (1 and 2) ‘chasing’ the invoice, there is a fake response added to the trail (3), which appears to emanate from a senior individual in the organisation who approves the invoice and recommends it to be sent to the finance team to act, making payment.

The final email seen (4), is usually the actual email promulgated to the targeted organisation, which contains this fake deceptive thread adding some level of legitimacy and credibility to the request, in a hope that the deception will not be questioned and be processed on the assumed authority given.

BEC Fake Threads Campaign

From: Invoices <billing@ziprecruiter.com>
Sent: Monday, August 04, 2024 11:41 AM
To: [redacted]
Subject: Invoice #12862843 for ZipRecruiter Subscription

Dear Clay,

We are pleased to provide you with the invoice for the ZipRecruiter Premium Usage Pricing Corporate Job Posting, tailored to meet your organizations recruiting needs. Attached, you will find the invoice covering the service period from July 24, 2024, to August 3, 2025.

1 Invoice Summary:

- Invoice Number: 12862843
- Date Issued: August 4, 2024
- Due Date: August 4, 2024

Please make sure that payment is completed by the due date to prevent any interruption in your services. If you have any questions or need further assistance, feel free to reach out directly.

Please note: This is an automated message, and replies to this email are not monitored. For inquiries, please contact Keith Murray directly.

Confidentiality Notice: This communication, including any attachments, contains confidential information intended only for the recipient(s). Unauthorized use, disclosure, or copying is prohibited. If you are not the intended recipient, notify the sender immediately and delete all copies. Do not reply to this automated message.

1 The first 'email' in the fake thread campaign, dated 04 August 2024, alludes to a required invoice payment for a service procured by the targeted organisation.

This fake email is addressed to a senior executive in the organisation in order to add to the deception, and credibility of the ploy.

BEC Fake Threads Campaign

From: Keith Murray <keith.murray@ziprecruiter.com>
Sent: Thursday, August 29, 2024 03:15 PM
To: [redacted]
Subject: RE: Invoice #12862843 for ZipRecruiter Subscription

Dear Clay,

I hope you are doing well. Following up regarding the invoice #12862843 issued on August 4, 2024, for the ZipRecruiter Premium Usage Pricing Corporate Job Posting, covering the period from July 24, 2024, to August 3, 2025.

As of today, we haventt received the payment of $9,979.00, which was due on August 4, 2024. Here are the key details of the invoice:

2

- Invoice Number: 12862843
- Date Issued: August 4, 2024
- Due Date: August 4, 2024

This invoice includes the charges for the following:

- Service Period: July 24, 2024 - August 3, 2025
- Contract Number: C623571-85261
- Member ID: A51804

Please settle this payment at your earliest convenience to avoid any potential service disruptions. If you have already processed this payment or have any questions, please let me know.

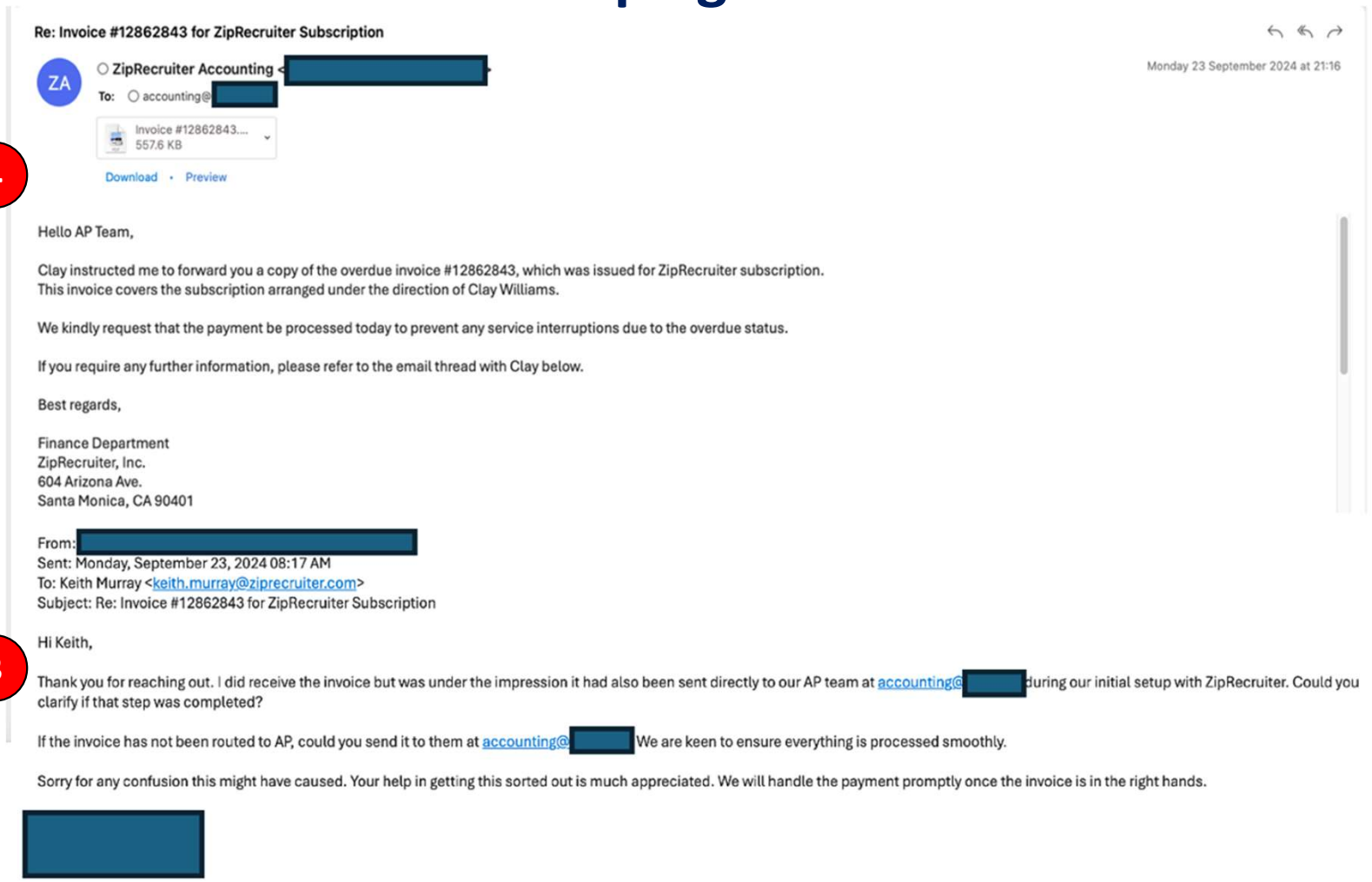
Thank you for your quick response to this matter.

Best regards,

2

The second fake ‘email’ in the thread, dated 29 August 2024, references the first email and is a hastener / reminder for payment to be made as the target organization has seemingly not made payment.
This activity again adds some credibility to the deception, following business practices with payment terms employed by multiple organisations.
Additionally veiled threats of ‘service disruption’ and a need for ‘urgency’ indicate the potential for exploitation of human vulnerabilities.

BEC Fake Threads Campaign



Re: Invoice #12862843 for ZipRecruiter Subscription

ZA ○ ZipRecruiter Accounting <[redacted]

To: ○ accounting@[redacted]

Monday 23 September 2024 at 21:16

Invoice #12862843.... 557.6 KB

Download · Preview

4

Hello AP Team,

Clay instructed me to forward you a copy of the overdue invoice #12862843, which was issued for ZipRecruiter subscription.
This invoice covers the subscription arranged under the direction of Clay Williams.

We kindly request that the payment be processed today to prevent any service interruptions due to the overdue status.

If you require any further information, please refer to the email thread with Clay below.

Best regards,

Finance Department
ZipRecruiter, Inc.
604 Arizona Ave.
Santa Monica, CA 90401

From: [redacted]
Sent: Monday, September 23, 2024 08:17 AM
To: Keith Murray <keith.murray@ziprecruiter.com>
Subject: Re: Invoice #12862843 for ZipRecruiter Subscription

Hi Keith,

3

Thank you for reaching out. I did receive the invoice but was under the impression it had also been sent directly to our AP team at accounting@[redacted] during our initial setup with ZipRecruiter. Could you clarify if that step was completed?

If the invoice has not been routed to AP, could you send it to them at accounting@[redacted] We are keen to ensure everything is processed smoothly.

Sorry for any confusion this might have caused. Your help in getting this sorted out is much appreciated. We will handle the payment promptly once the invoice is in the right hands.

[redacted]

3 Following the initial fake emails 'chasing' the invoice, there is a fake response added to the trail, which appears to emanate from a senior individual in the organisation who approves the invoice and recommends it to be sent to the finance team to act, making payment.

4 The final email seen is usually the actual email promulgated to the targeted organisation, which contains this fake deceptive thread adding some level of legitimacy and credibility to the request, in a hope that it will not be questioned and will be processed for payment, unquestioned, on the assumed authority given.

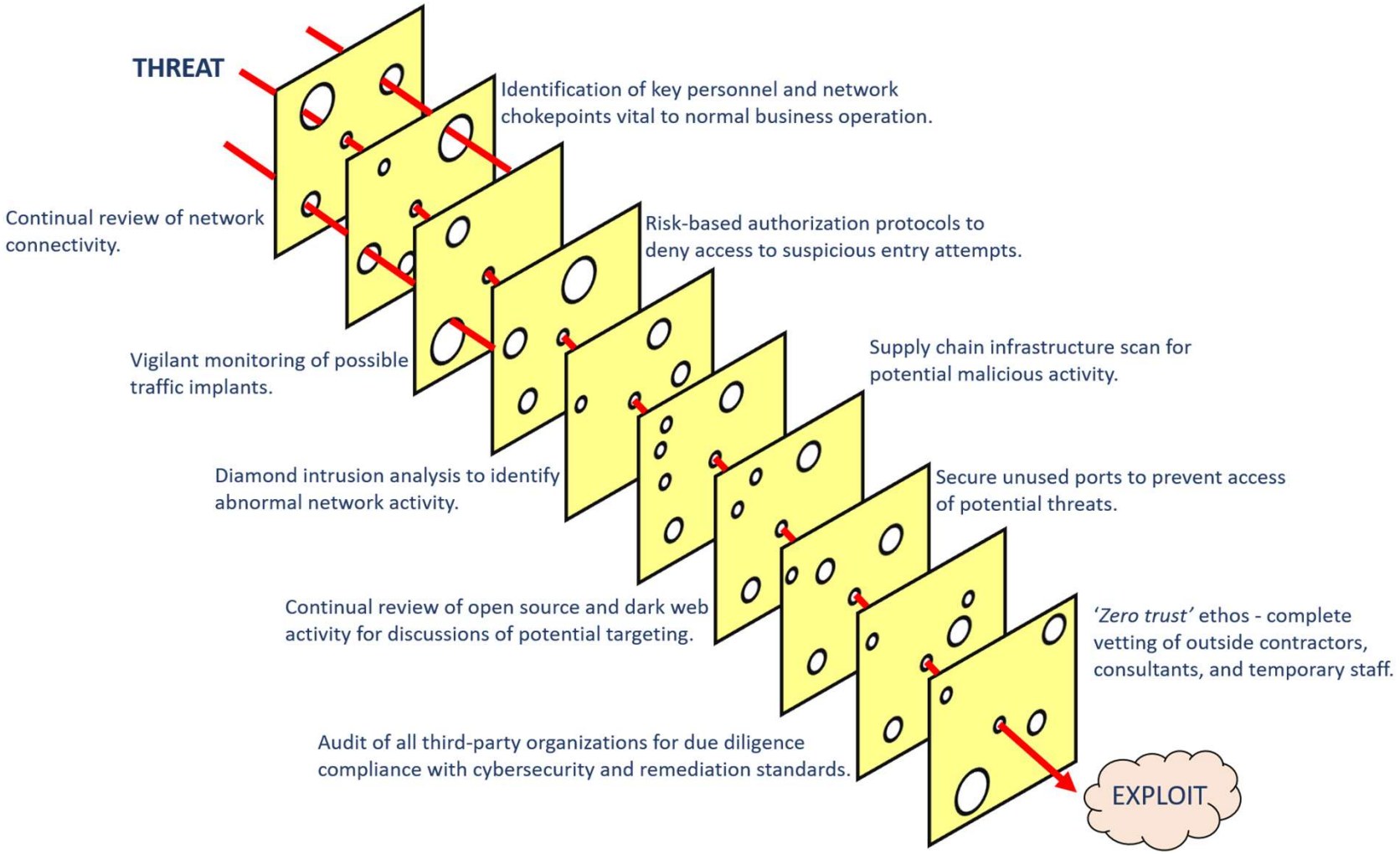
Countering Cyber Deception – AI / eNLP / MLE

Countering Cyber Deception – NLP, TAA, AI, ML…

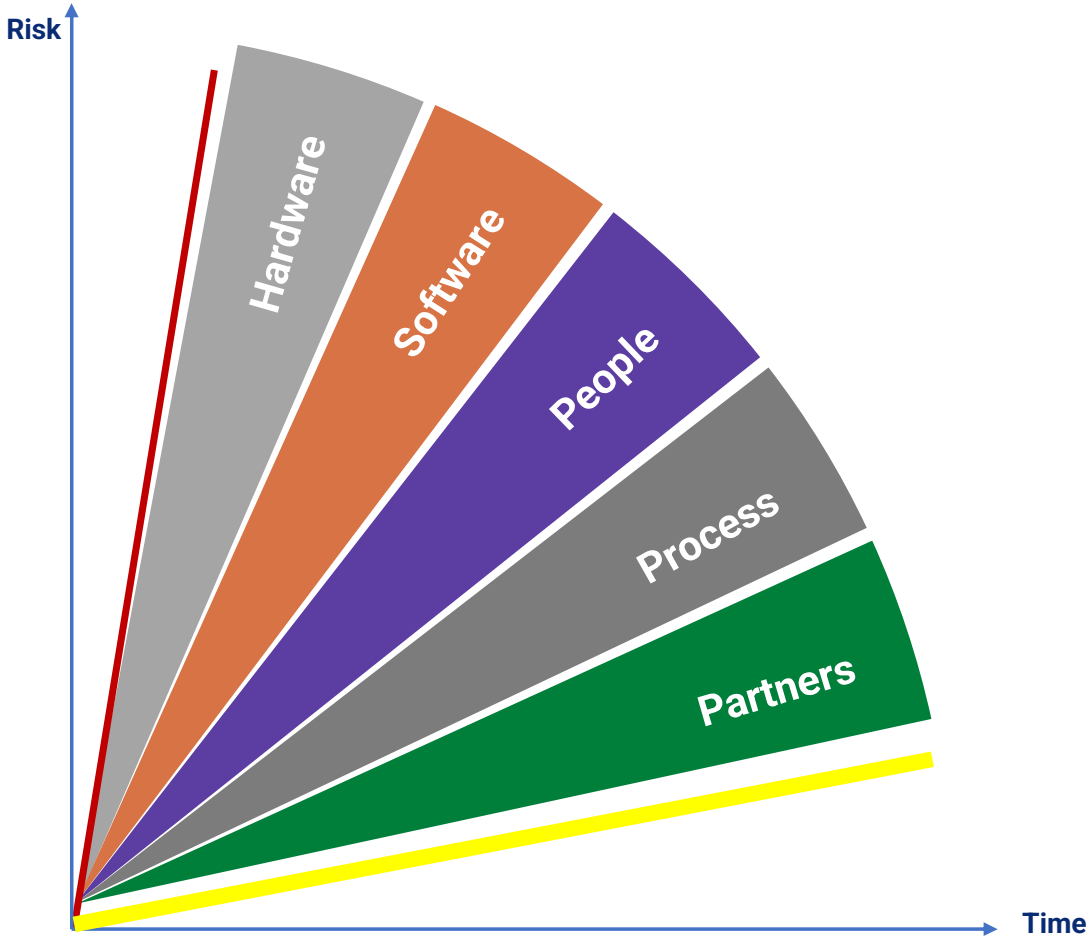
- **Identification of the frequencies of words in phishing and spam e-mails help detect temporal trends.**
- **Entity extraction and parts of speech tagging**
- **User behavior analytics**
- **Automatic VIP detection**
- **Topic identification**
- **Sentiment analysis.**
- Socio-demographic characteristics such as sex, age, language and religion.
- Geographic characteristics such as where the audience lives and how that might impact behaviour.
- Psychographic characteristics such as needs, hopes, concerns and aspirations.
- Audience thoughts, beliefs, knowledge and current actions related to the health or social issue.
- Barriers and facilitators that prevent or encourage audience members to adopt the desired behaviour change.
- Gender and how it impacts audience members' behaviour and ability to change.
- Effective communication channels for reaching the audience.

https://www.aiethicist.org/ai-organizations

Defence in Depth



Target Hardening - Layered Security



Future Concerns

- Structuring of ‘traditional’ security strategies will not be sufficient to maintain the necessary adaptive capability that organisations (with significant risk profiles) must build and maintain to stay ahead in an increasing complex and interconnected world.
- Continued impacts for shadow IT / legacy systems / M&A / BYOD as ongoing hybrid working is normalised
- **Increase in cyber domain concerns will drive an increase in legislation and regulatory activity – esp in cyber insurance markets**
- Attacks via Third Party / Supply Chain will continue to increase in frequency & Impact
- Access Brokerage increase as attack methodology
- Increased use of AI / Ml in developing attack methodologies
- **Ransomware continues**
- Security Stacking of multiple technologies continues to be exploited amid configuration clashes
- Sophisticated Spear Phishing / whaling (via Pattern of Life analysis)
- Increase in attempts to capture data in transit
- Increase in Malware-as-a-service

Thank you


mimecast®
The Connected Human Risk Management Platform