Complexities in Investigating Cases of Social Engineering:

How reverse engineering and profiling can assist in the collection of evidence.

Christina Lekati
Cyber Risk GmbH

Social Engineering

The Basics

“The art and science, of skillfully maneuvering human beings to take action in some aspect of their lives

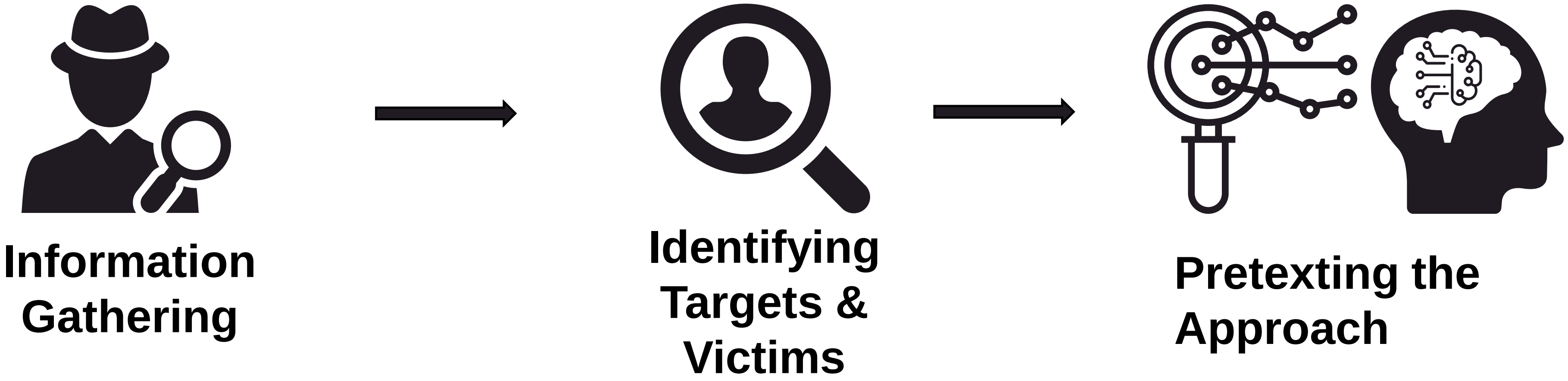
…that may or may not be in the ‘target’s’ best interest.”

-Christopher Hadnagy

Social Engineering

The Typical Backbone of the Attack Strategy

Preparation:

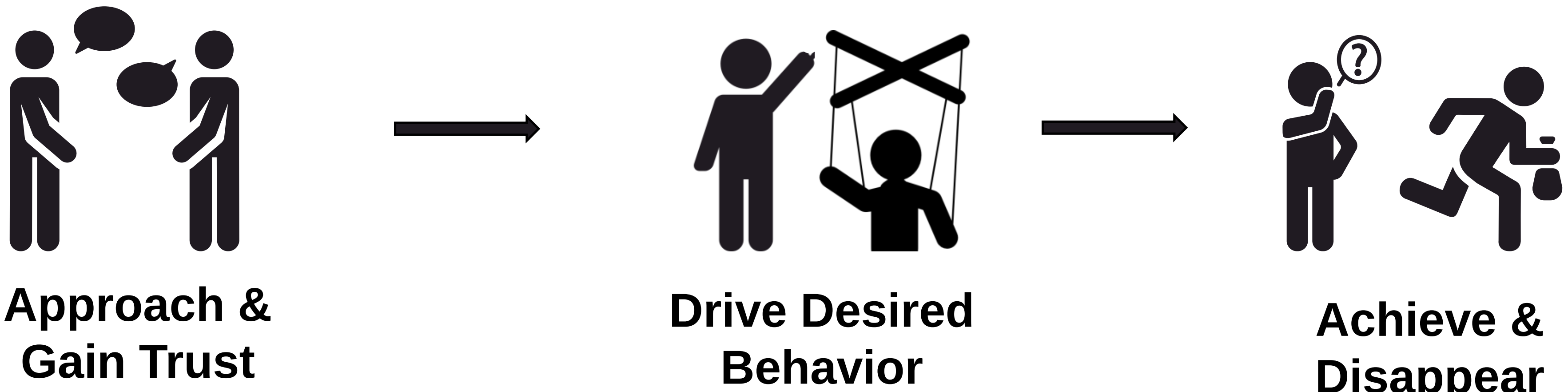


Information Gathering

Identifying Targets & Victims

Pretexting the Approach

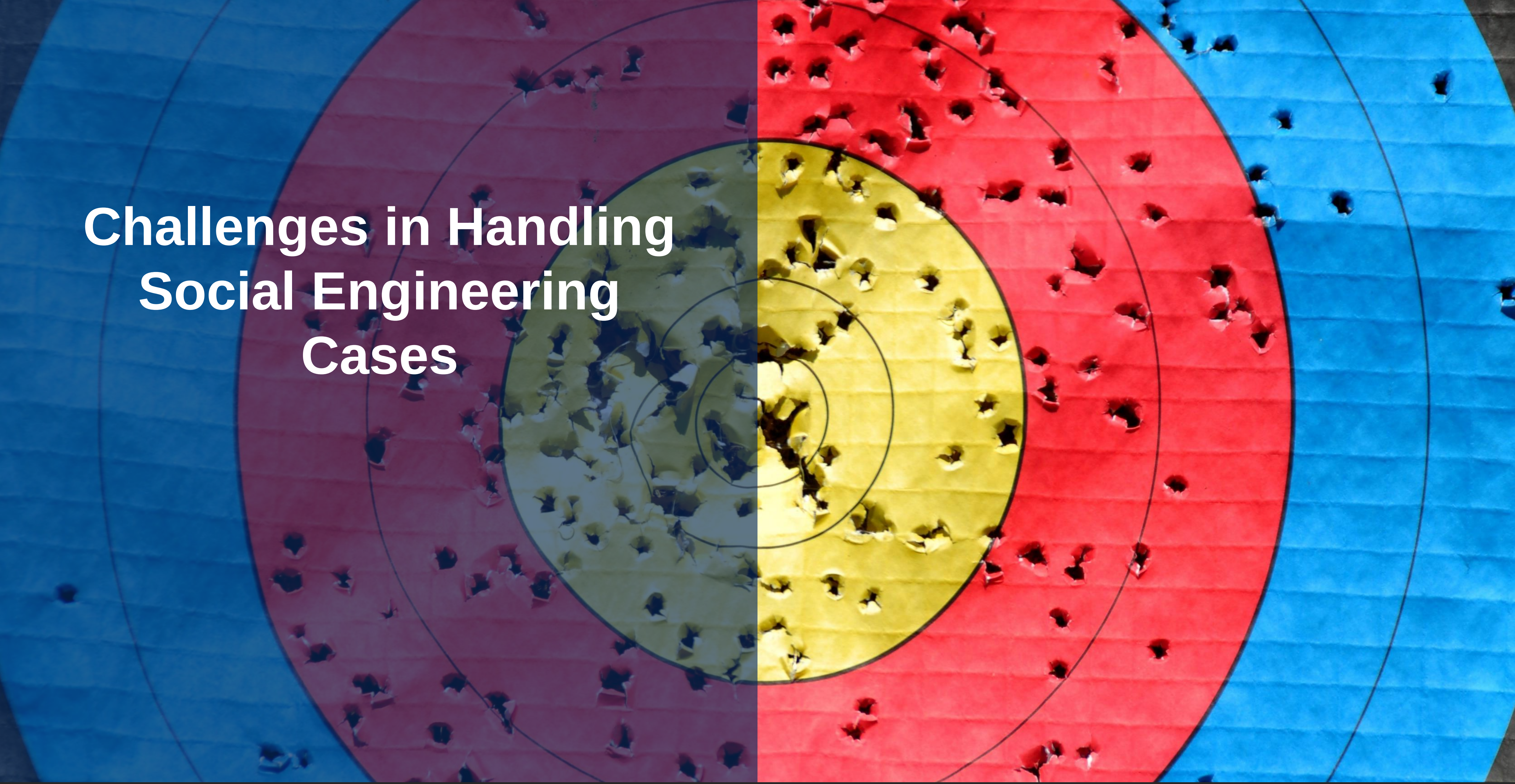
Execution:



Approach & Gain Trust

Drive Desired Behavior

Achieve & Disappear



Challenges in Handling Social Engineering Cases

Case Study: Medidata

How Medidata got tricked

$4.8 million loss from a Social Engineering attack.

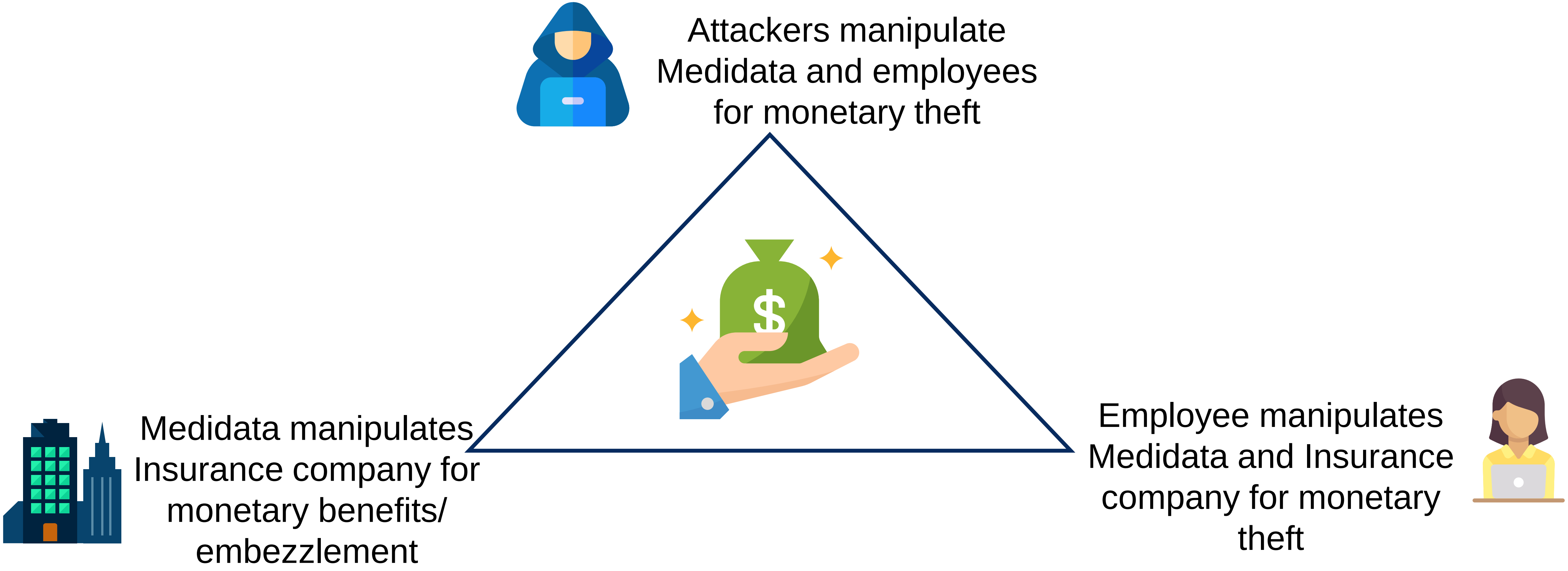
Social Engineering: Quality of Evidence

Leaves mainly weak or non-admissible evidence

- Alleged/ Oral evidence
- Hearsay evidence
- Can manipulation be proved beyond reasonable doubt?
- Many plausible scenarios and interpretations
- …and more

Case Study: Medidata $4.8 million Social Engineering loss

Other Plausible Interpretations



Attackers manipulate Medidata and employees for monetary theft

Medidata manipulates Insurance company for monetary benefits/ embezzlement

Employee manipulates Medidata and Insurance company for monetary theft

Social Engineering: Quality of Evidence

Courts still face difficulties on how to judge and evaluate cases involving mainly Social Engineering.

Providing evidence “beyond reasonable doubt” seems to be the biggest challenge.

But how does one find evidence in Social Engineering cases?

Supporting evidence & leads; tracing back the steps of the offender

Reverse engineer the suspect’s actions?

Traces left through the planning & preparation phase?

- Information used in the attack that were available

  <u>only through certain sources</u>**.**

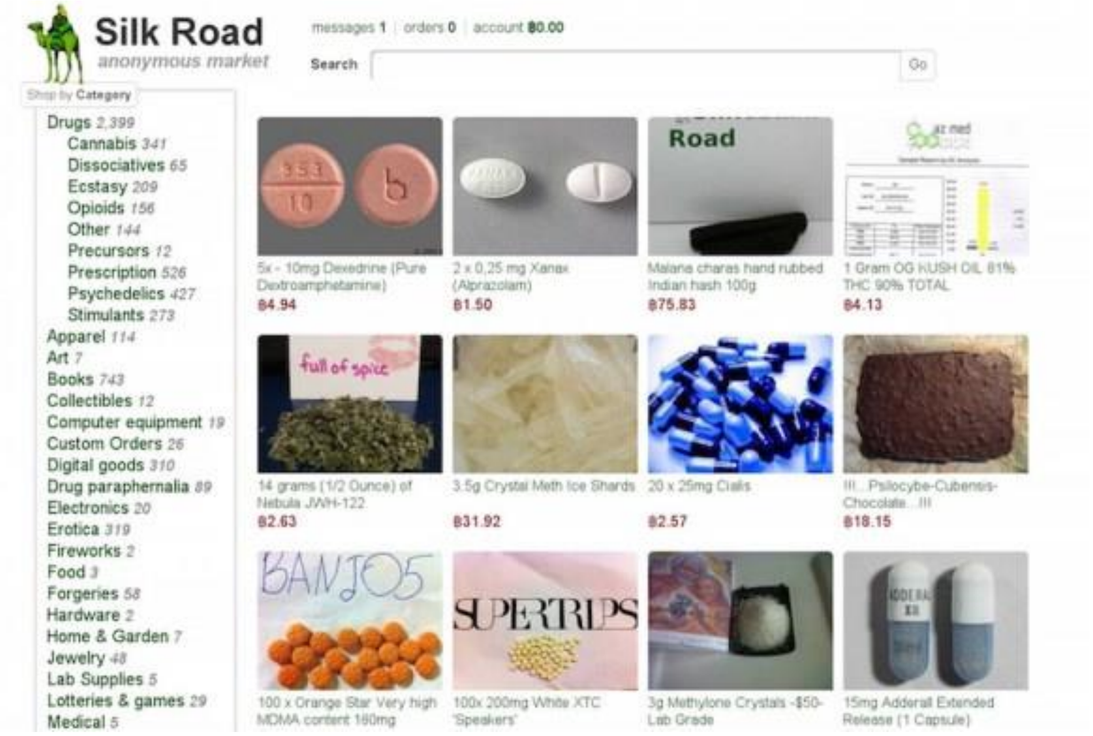
- Did social media assist the attack?

- Forgotten blog posts, forum questions, email addresses and usernames, etc.

- Geolocations, stalking, cyberstalking.

Case Study: Silk Road

Collecting evidence from the preparation phase



Silk Road
anonymous market

messages 1 | orders 0 | account ฿0.00

Search [ ] Go

Shop by Category

- Drugs 2,399
  - Cannabis 341
  - Dissociatives 65
  - Ecstasy 209
  - Opioids 156
  - Other 144
  - Precursors 12
  - Prescription 526
  - Psychedelics 427
  - Stimulants 273
- Apparel 114
- Art 7
- Books 743
- Collectibles 12
- Computer equipment 19
- Custom Orders 26
- Digital goods 310
- Drug paraphernalia 89
- Electronics 20
- Erotica 319
- Fireworks 2
- Food 3
- Forgeries 58
- Hardware 2
- Home & Garden 7
- Jewelry 48
- Lab Supplies 5
- Lotteries & games 29
- Medical 5

5x - 10mg Dexedrine (Pure Dextroamphetamine)
฿4.94

2 x 0,25 mg Xanax (Alprazolam)
฿1.50

Malana charas hand rubbed Indian hash 100g
฿75.83

1 Gram OG KUSH OIL 81% THC 90% TOTAL
฿4.13

14 grams (1/2 Ounce) of Nebula JWH-122
฿2.63

3.5g Crystal Meth Ice Shards
฿31.92

20 x 25mg Cialis
฿2.57

!!!...Psilocybe-Cubensis-Chocolate...!!!
฿18.15

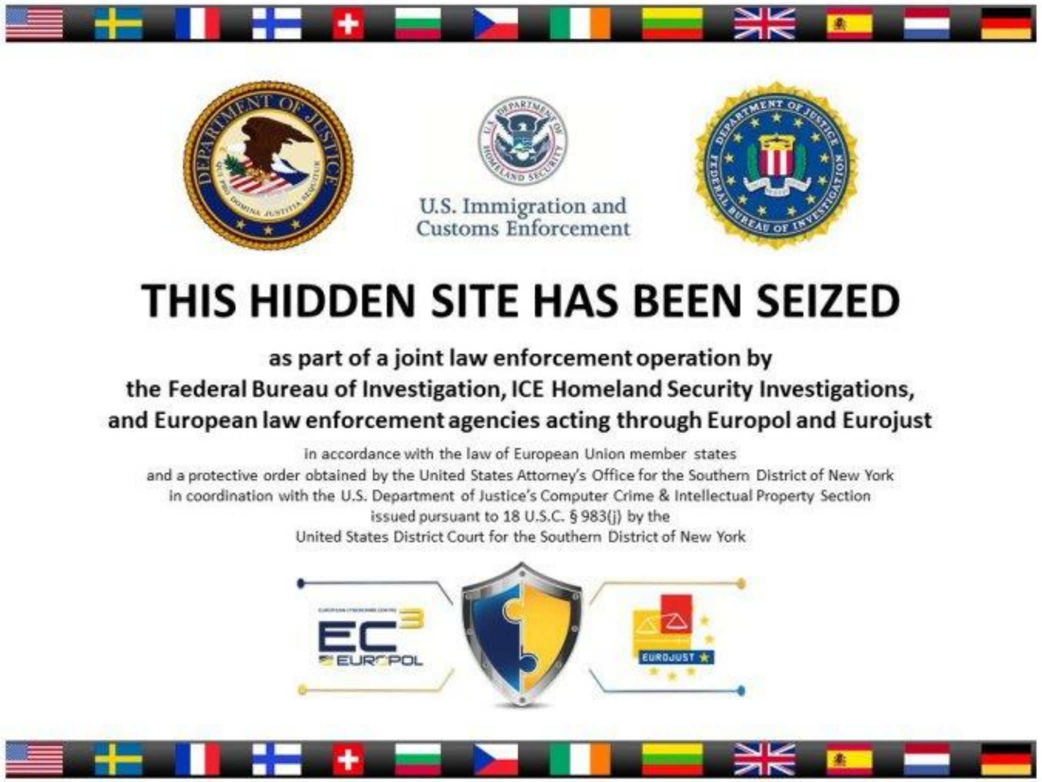
100 x Orange Star Very high MDMA content 180mg

100x 200mg White XTC 'Speakers'

3g Methylone Crystals -$50- Lab Grade

15mg Adderall Extended Release (1 Capsule)

➡



U.S. Immigration and Customs Enforcement

THIS HIDDEN SITE HAS BEEN SEIZED

as part of a joint law enforcement operation by
the Federal Bureau of Investigation, ICE Homeland Security Investigations,
and European law enforcement agencies acting through Europol and Eurojust

in accordance with the law of European Union member states
and a protective order obtained by the United States Attorney's Office for the Southern District of New York
in coordination with the U.S. Department of Justice's Computer Crime & Intellectual Property Section
issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

When digital traces are well covered, look for behavioral mistakes.

Social Engineering

The Typical Backbone of the Attack Strategy

Preparation:

Attacker still feels “invisible” and secure.
Potentially has not decided whether to attack or not.
Potentially is still an amateur, learning how to protect his actions.

Phase of Sloppy Mistakes

Information Gathering
(Reconnaissance)

Identifying Possible Targets & Victims

Pretexting the Approach

Exploitation of Vulnerabilities:

Has prepared and planned for most of his actions.
Has already prepared and strategized into covering his tracks and misleading investigators.

Phase of Careful Action.

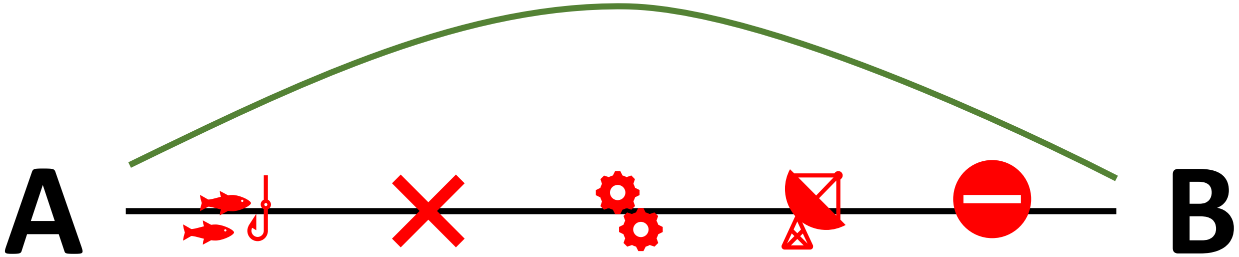
Approach & Gain Trust

Drive Desired Behavior
(Exploitation of Trust & Manipulation)

Achieve Desired Outcome & Disappear

Remember…

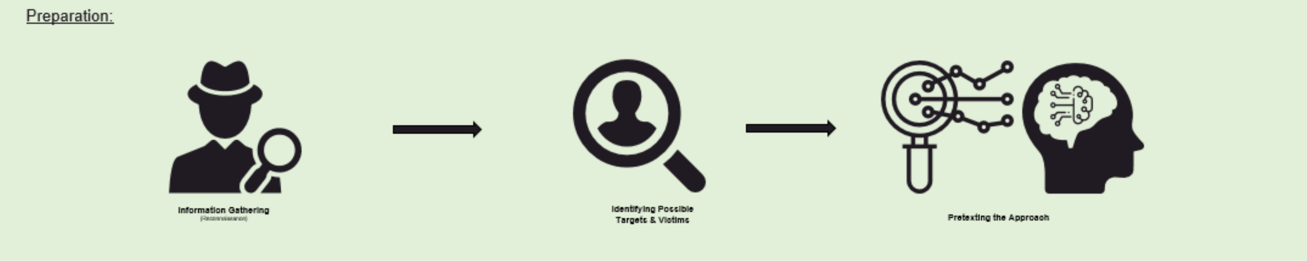
Sometimes, the fastest way from A to B…



…is the unpredicted one.

How do offenders select their victims?

Connecting the Dots



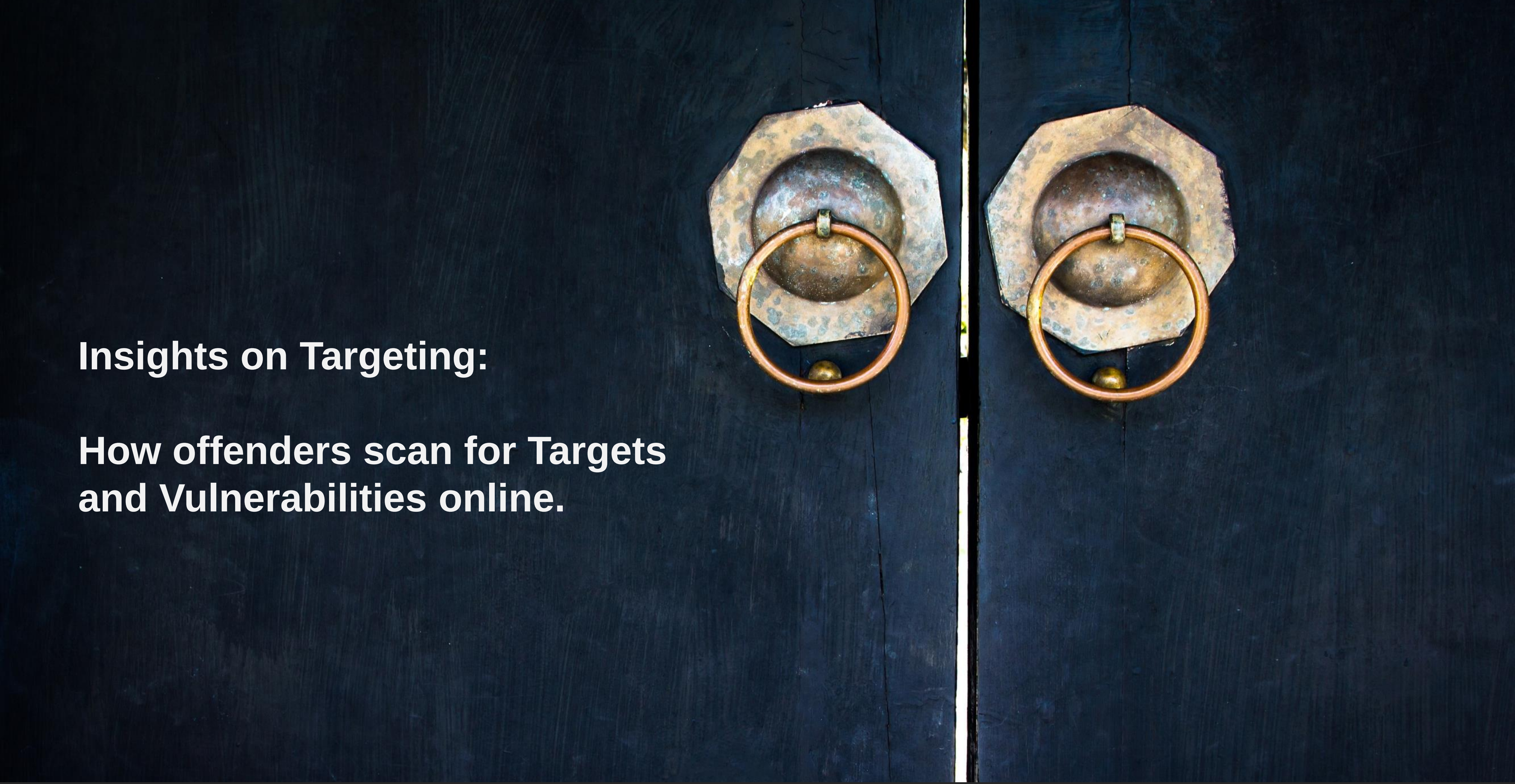
Tracing back an attack:

- The phase of **information gathering, targeting, and planning**.

- Reconnaissance : The attack strategy of the attacker can reveal the steps he took through his **preparation** and reveal **sloppy mistakes**.

- Offenders are still humans: look for **logical possible mistakes**.

- The way a victim was profiled leaves traces in profiling the attacker.



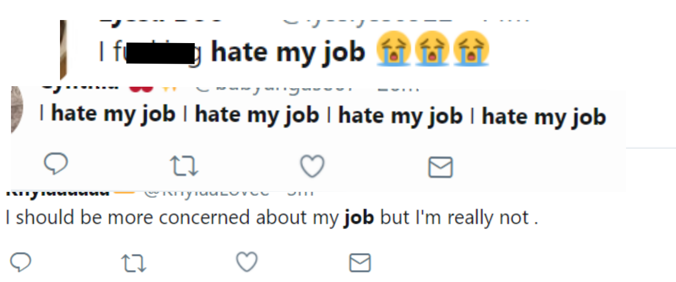
Insights on Targeting:

How offenders scan for Targets and Vulnerabilities online.

Demonstration

Finding Weaknesses and Vulnerabilities

Will not bother protecting the workplace

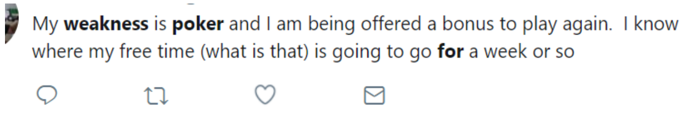


I f[redacted]g hate my job 😭😭😭

I hate my job I hate my job I hate my job I hate my job

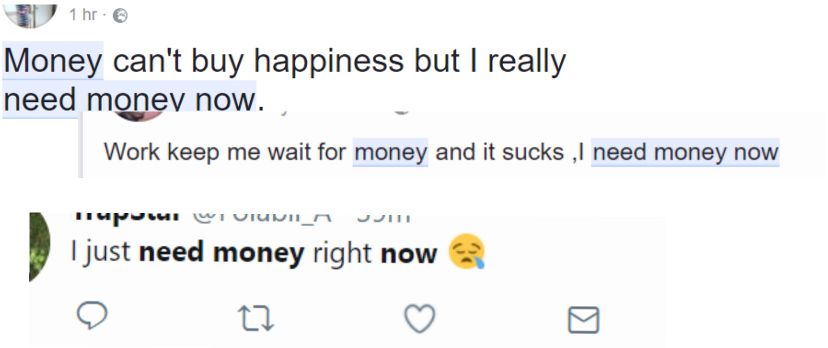
I should be more concerned about my **job** but I'm really not .

Manipulation to feed addictions



My **weakness** is **poker** and I am being offered a bonus to play again. I know where my free time (what is that) is going to go **for** a week or so

Exploit need



1 hr ·

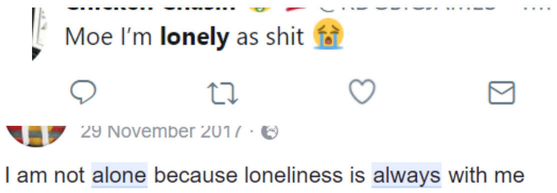
Money can't buy happiness but I really need money now.

Work keep me wait for money and it sucks ,I need money now

I just **need money** right **now** 😪

Vulnerability Exposure Posts

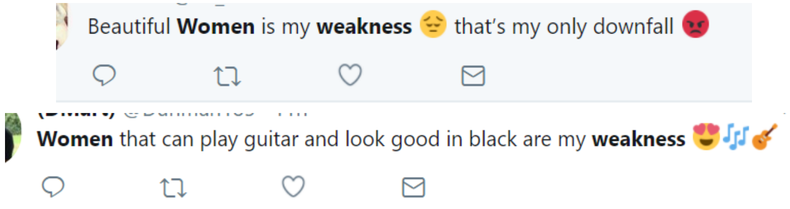
Send romance fraudster



Moe I'm **lonely** as shit 😭

29 November 2017 ·

I am not alone because loneliness is always with me



Beautiful **Women** is my **weakness** 😔 that's my only downfall 😡

Women that can play guitar and look good in black are my **weakness** 😍🎶🎸

WARNING

Insights on Profiling:

How offenders profile potential targets online.

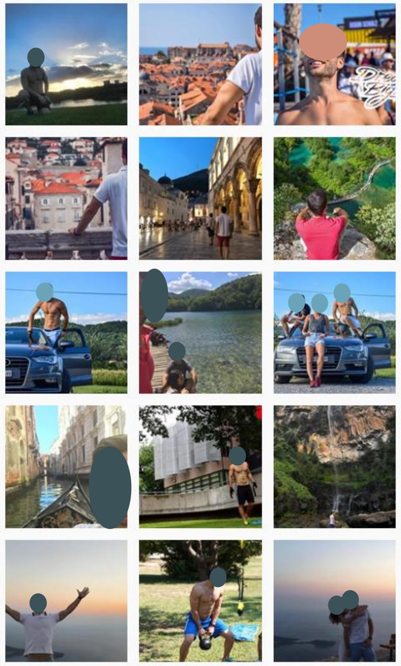
How Key Traits are Being Assessed

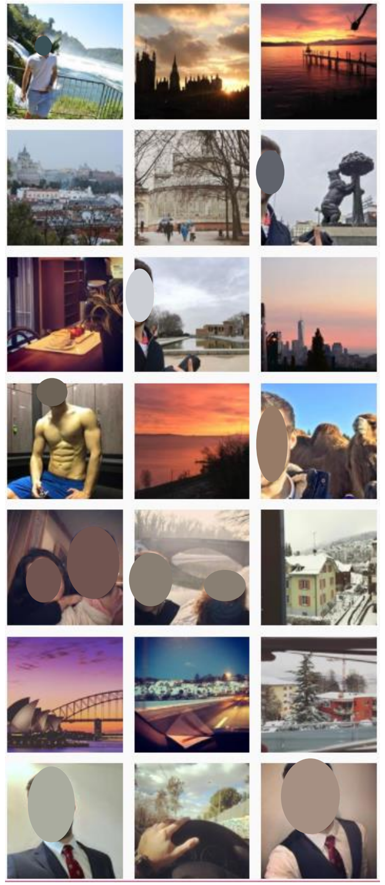
- The overall representation or “Personal Brand”
- Selection of words
- Selection of interests & activities
- Work responsibilities
- Social life indications
- Vulnerabilities

An Example…

Demonstration

Tom’s Profile- What is the overall personal brand?





- Body Language
- Variety of face expressions
- Content (activities)
- Colors
- Locations
- Other people

Demonstration

Profiling Matrix

	Personality Traits	Interests	Wants	Vulnerabilities
Self Image	• Confident • Expressive • Sharing • Euphoric • Enthusiastic	• Fitness • Exploration • Adventure	???	???
Social Life	• Social /Open • Extraverted • Wide social circle	• Travel • Social Events (mostly outdoors)	???	???
Professional Life	???	???	???	???

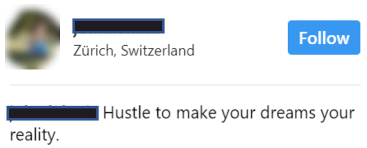
Demonstration

Tom’s Profile- A closer look & verbal expressions

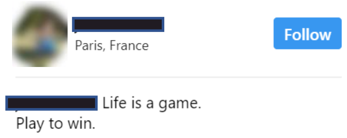
Words.   Patterns.   Expressiveness Style.

Demonstration

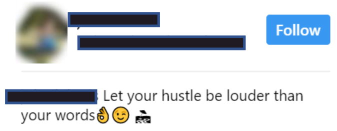
Tom’s Profile- A closer look & verbal expressions


[redacted]
Zürich, Switzerland

[redacted] Hustle to make your dreams your reality.

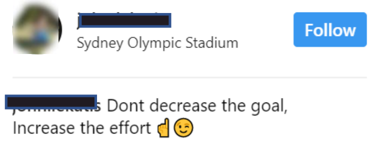

[redacted]
Paris, France

[redacted] Life is a game.
Play to win.

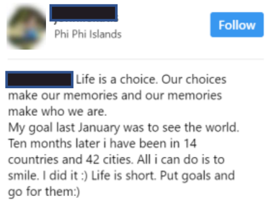

[redacted]

[redacted] Let your hustle be louder than your words👌😉🚣

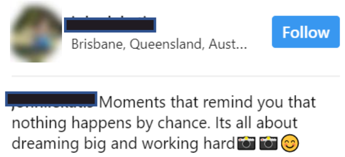
→ Ambition.


[redacted]
Sydney Olympic Stadium

[redacted] Dont decrease the goal,
Increase the effort ☝😉

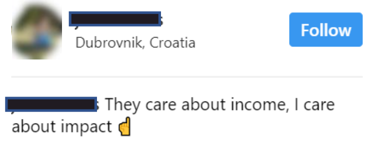

[redacted]
Phi Phi Islands

[redacted] Life is a choice. Our choices make our memories and our memories make who we are.
My goal last January was to see the world. Ten months later i have been in 14 countries and 42 cities. All i can do is to smile. I did it :) Life is short. Put goals and go for them:)

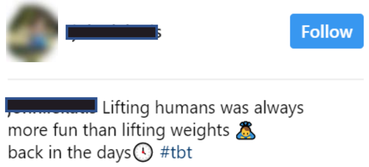

[redacted]
Brisbane, Queensland, Aust...

[redacted] Moments that remind you that nothing happens by chance. Its all about dreaming big and working hard📸📸😊

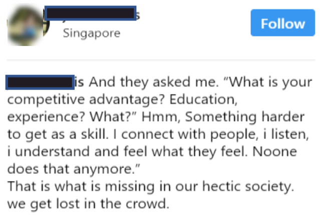
→ Determination.


[redacted]
Dubrovnik, Croatia

[redacted] They care about income, I care about impact ☝

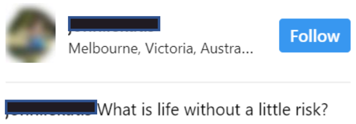

[redacted]

[redacted] Lifting humans was always more fun than lifting weights 🙇
back in the days🕓 #tbt

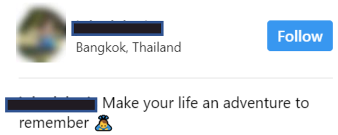

[redacted]
Singapore

[redacted] And they asked me. “What is your competitive advantage? Education, experience? What?” Hmm, Something harder to get as a skill. I connect with people, i listen, i understand and feel what they feel. Noone does that anymore.”
That is what is missing in our hectic society. we get lost in the crowd.

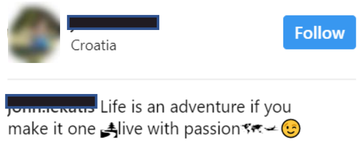
→ Influence.


[redacted]
Melbourne, Victoria, Austra...

[redacted] What is life without a little risk?

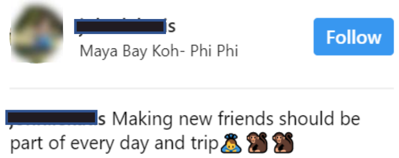

[redacted]
Bangkok, Thailand

[redacted] Make your life an adventure to remember 🙇

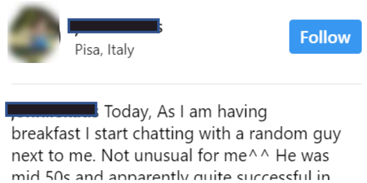

[redacted]
Croatia

[redacted] Life is an adventure if you make it one 🏄live with passion🗺 😉

→ Adventure.


[redacted]
Maya Bay Koh- Phi Phi

[redacted] Making new friends should be part of every day and trip🙇🐒🐒


[redacted]
Pisa, Italy

[redacted] Today, As I am having breakfast I start chatting with a random guy next to me. Not unusual for me^^ He was mid 50s and apparently quite successful in

→ Extraversion.

Demonstration

Profiling Matrix

	Personality Traits	Interests	Wants	Vulnerabilities
Self Image	• Confident • Expressive • Sharing • Euphoric • Enthusiastic • **Determined** • **Hard worker**	• Fitness • Exploration • Adventure • **Growth**	• **Inner peace & happiness** • **Recognition** • **Admiration** • **Advancement**	???
Social Life	• Social /Open • Extraverted • Wide social circle • **Authoritative style of expression**	• Travel • Social Events (mostly outdoors) • **Others' well being**	• **To have positive influence** • **To appeal authoritative** • **To be asked for advice**	???
Professional Life	???	???	???	???

Demonstration

What about the Professional life?? Deductive thinking and more assumptions

	Personality Traits	Interests	Wants	Vulnerabilities
Self Image	• Confident • Expressive • Sharing • Euphoric • Enthusiastic • Determined • Hard worker	• Fitness • Exploration • Adventure • Growth	• Inner peace & happiness • Recognition • Admiration • Advancement	???
+ Social Life	• Social /Open • Extraverted • Wide social circle • Authoritative style of expression	• Travel • Social Events (mostly outdoors) • Others' well being	• To have positive influence • To appeal authoritative • To be asked for advice	???
= Professional Life	• **Front line person** • **Team leader** • **Management**	**Ideally he would have: Challenging job position with a variety of responsibilities and room for growth**	**Consultant?** **Instructor?** **Manager?** **etc**	

Demonstration

What about the Vulnerabilities?? More deductive thinking and assumptions

	Personality Traits	Interests	Wants	Vulnerabilities
Self Image	• Confident • Expressive • Sharing • Euphoric • Enthusiastic • Determined • Hard worker	• Fitness • Exploration • Adventure • Growth	• Inner peace & happiness • Recognition • Admiration • Advancement	• **Failure** • **Ineffectiveness** • **Idleness** • **Triviality**
Social Life	• Social /Open • Extraverted • Wide social circle • Authoritative style of expression	• Travel • Social Events (mostly outdoors) • Others' well being	• To have positive influence • To appeal authoritative • To be asked for advice	• **Rejection** • **Low impact** • **Ignoring**
Professional Life	• Front line person • Team leader • Management	Ideally he would have: Challenging job position with a variety of responsibilities and room for growth	Consultant? Instructor? Manager? etc	

Profiling the Victim

How does a social engineer use all that???

- “Interests” and “Wants” columns: provide fruitful ground to start a conversation and engage the target… Attacker builds rapport, then starts building trust.
- “Vulnerabilities” column: strategically used when likeability cannot drive the desired action or for blackmailing.
- The attacker will adjust his approach according to how the target responds. He has a lot information to work with.
- Knows the patterns of lifestyle, locations, motives, and best time to approach or attack.
- Profiling information help the attacker tailor his pretext to the victim’s personality.

Case study: Targeting victims through social media

- Throughout 2010, a kidnapping ring was targeting victims by scouting through social media.
- Wealthy individuals were preferred: Ransom would be tailored to each victim’s perceived wealth.

Gang’s attack strategy:

- Scouting through social media.
- Profiling targets and selecting vulnerable victims.
- Studying routines and finding patterns to determine best place & method of kidnapping.

Tracing back:

- Information tracing that the target was at place X at time X. (schedule availability, other people, social media, online available information?)

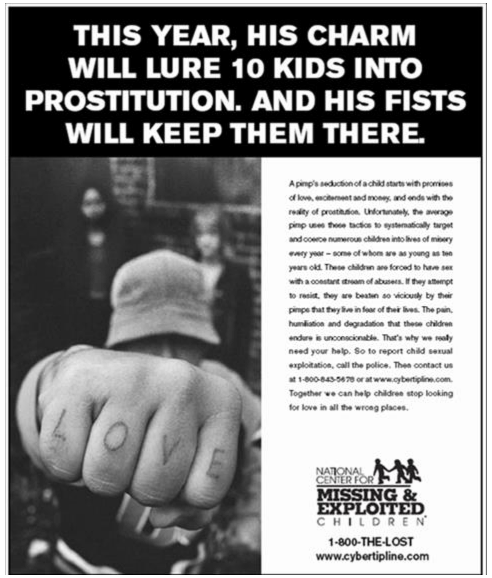
Case study: Targeting victims through social media

Attackers look for patters, but they operate in patterns, too.

The case of “J-Dirt”: Persuading into Juvenile Prostitution

Underground Gangster Crips: Justin Strom’s plan of action:

- Socially engineering juveniles found through social media.
- Turning victims into prostitutes and gang members through “flattery, manipulation and when needed, force”.
- The gang recruited 10 underaged girls online and operated the prostitution ring for 6 years.



THIS YEAR, HIS CHARM WILL LURE 10 KIDS INTO PROSTITUTION. AND HIS FISTS WILL KEEP THEM THERE.

A pimp's seduction of a child starts with promises of love, excitement and money, and ends with the reality of prostitution. Unfortunately, the average pimp uses these tactics to systematically target and coerce numerous children into lives of misery every year – some of whom are as young as ten years old. These children are forced to have sex with a constant stream of abusers. If they attempt to resist, they are beaten so viciously by their pimps that they live in fear of their lives. The pain, humiliation and degradation that these children endure is unconscionable. That's why we really need your help. So to report child sexual exploitation, call the police. Then contact us at 1-800-843-5678 or at www.cybertipline.com. Together we can help children stop looking for love in all the wrong places.

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

1-800-THE-LOST
www.cybertipline.com

Law Enforcement Case Resolution:

- From allege and hearsay – to digital traces and evidence.
- Uncovered: Social media evidence, location evidence, payment traces, surveillance footage and more.
- Enough to connect the dots and provide strong evidence?

Souces: https://archive.org/stream/605416-strom-justin-pacer-2-affidavit-1/605416-strom-justin-pacer-2-affidavit-1_djvu.txt
https://archives.fbi.gov/archives/washingtondc/press-releases/2012/five-alleged-members-of-crips-gang-accused-of-prostituting-high-school-girls

Reverse Engineering the Attacks

Learnings for Law Enforcement

By knowing how a victim was profiled, investigators can…

- Pinpoint the channels and sources of information used by criminals.
- Link the unique information used in an attack with the sources through which they were available.
- Predict potential future targets.
- Narrow down leads and suspects.
- …and more

Profiling the Suspect?

- Patterns in behavior and attack strategies
- Character evidence in intend, motive or opportunity.
- Narrowing down possible suspects
- Acquisition of supportive evidence and leads
- Profile the suspect’s tendencies: better predict future behavior
- Use profiling information for more effective questioning and interrogation
- Use profiling in interrogation to lead to confession

Thank you.

Christina Lekati

Social Engineering Expert

Cyber Risk GmbH

Contact Details:

Christina.lekati@cyber-risk-gmbh.com

Christina Lekati

@ChristinaLekati