

# Analyze, befriend and exploit

## Construct targeted social engineering attacks



# Slides !

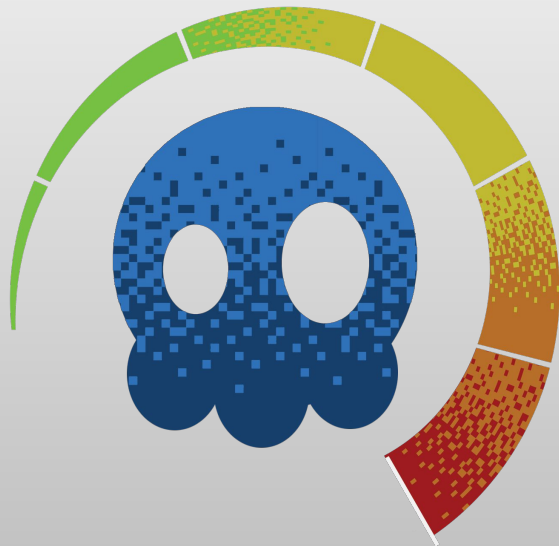


[https://blog.volker-carstein.com/targeted\\_se\\_workshop\\_slides.pdf](https://blog.volker-carstein.com/targeted_se_workshop_slides.pdf)



# Briefing

1. Social engineering basics & definitions
2. Targeted social engineering examples
3. Investigate-Hook-Play-Exit
  - a. Picking your POI
  - b. Defining your persona
  - c. Building your pretext(s)



# Who am I ?



**Volker Carstein (@volker\_carstein)**

- Pentester @  **BSECURE**
- Social engineering, OSINT and infosec (with a preference for Active Directory hacking)
- Speaker @ LeHack, Barbhack, SecSea, AMUSEC

# Social engineering basics

**“Any act that influences a person to take an action  
that may or may not be in their best interest”**



# Social engineering basics

Can be used for *good causes* as well  
as *malicious ones*

## Typical unethical goals

- Money
- Cause or ideology
- Entertainment
- Knowledge
- Ego
- Revenge

## *Empathy*

Most powerful tool in social engineering

SE is used by various kinds of people

- Hackers & Pentesters
- Spies & secret services agents
- Sales people & managers
- Scam artists
- You and me



# Social engineering : definitions

- **(T)SE(A)** = (Targeted) Social Engineering (Attacks)
- **Person of interest/POI** = Target
- **Persona** = Constructed identity/role for the interaction
- **Pretext** = Context of an interaction designed to achieve a goal
- **Burning** a POI = Compromising a persona/alerting the POI of an ongoing attack
- **Elicitation** = Act of obtaining information without directly asking for it
- **Psychological triggers** = Fear, anger, urgency
- **Targeting techniques** = (Social network) spear-phishing, vishing, in-person attack



# Targeted social engineering : Mia Ash



## Mia Ash

Photographer at Mia's Photography

London, Greater London, United Kingdom | Photography

Current	Mia's Photography
Previous	Loft Studios, Clapham Studios
Education	Goldsmiths, University of London

500+  
connections

### Photographer

Mia's Photography

January 2014 – Present (3 years 3 months) | London, United Kingdom

- Lead editor for numerous books, gallery shows, and images for media and multimedia broadcasts
- Consulted as photo editor for various International shows
- Implemented processes and structure for digital archiving, trafficked imagery, and conducted photo research and photo editing for publishing, multimedia, and exhibition projects
- Secured digital image submissions and prepared digital image priming and prepress for multiplatform projects
- Managed writing image use, photographer agreement contracts, and negotiated licensing terms and fees

### Manager, Photo Editing + Image Collection + Special Projects

International League of Conservation Photographers

2009 – 2010 • 1 yr

- Lead editor for numerous books, gallery shows, and images for media and multimedia broadcasts - Selected to edit a Christies Auction House gallery of "Best Nature Photographs of All Time"
- Consulted as photo editor for Conservation International
- Implemented processes and structure for digital archiving, trafficked imagery, and conducted photo research and photo editing for publishing, multimedia, and exhibition projects such as "Freshwater: The Essence of Life"
- Secured digital image submissions and prepared digital image priming and prepress for multiplatform projects
- Managed writing image use, photographer agreement contracts, and negotiated licensing terms and fees

**LinkedIn, Facebook, Instagram, Blogger site for photos, etc.**





# Targeted social engineering : Mia Ash

1. “Mia Ash” posts on LinkedIn and Facebook for “organic” activity
2. “She” interact via LinkedIn with employees from technology, oil/gas, healthcare, aerospace, and consulting organizations. Mid-level employees in technical fields or project management roles.  
Pretext is usually linked to photography
3. Rapport building, escalation of trust, switch to personal email or Facebook
4. “Mia” sends a .xlsx containing the PupyRAT program under a pretext involving scarcity & urgency

# Investigate-Hook-Play-Exit



1. **Investigate**
  - a. Pick a target / POI + Gather information
  - b. Create the persona
  - c. Create the pretext
2. **Hook**
  - a. Establish contact and rapport with POI
  - b. Take control of the interaction (according to plan)
3. **Play**
  - a. Execute the plan
  - b. Accomplish the objective(s)
4. **Exit**
  - a. Close the interaction
  - b. Avoid arousing suspicion

# Step 1 : Picking your POI

- Select a few promising targets, **get as much intelligence as possible**
- Basic information : name, gender, city, DOB, family, friends, work connections
- Position in the company : information access, hierarchical capabilities, etc.
- Hobbies, study places, usual places (bar, sport clubs, etc.)
- Get info via **OSINT** or other social engineering engagements



- Get some easily accessible info, then **pivot** : from “Name”

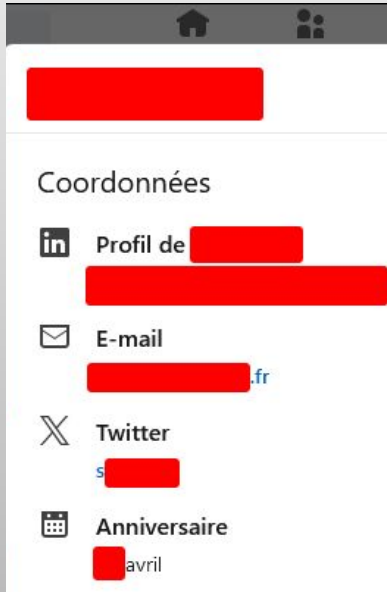


# Analyze, befriend and exploit - GreHack 2023

@volker\_carstein

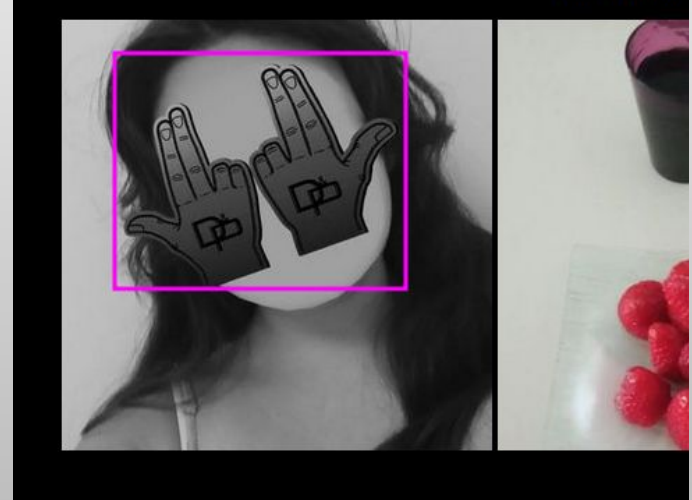
# Step 1 : Picking your POI

- Get some easily accessible info, then **pivot** : from “Social Networks”



# Step 1 : Picking your POI

- Get some easily accessible info, then **pivot** : from “Social Networks”



# Step 1 : Picking your POI

- Get some easily accessible info, then **pivot** : from “Social Networks”



# Step 1 : Picking your POI

- Get some easily accessible info, then **pivot** : from “Email”



HOLEHE



jean.dupont@gmail.com -> Jean Dupont (?)

kazadul@hotmail.fr -> Kazadul (?)







# Step 1 : Picking your POI

- Get some easily accessible info, then **pivot** : from “Linked Companies”

168 sociétés dont le dirigeant porte le nom "J [REDACTED] T"

 "SCI [REDACTED]"  
Location de logements (6820A)  
SIREN : [REDACTED]  
49 [REDACTED]  
[1 dirigeant porte le nom \[REDACTED\]](#)

 "SOCIETE [REDACTED] 16"  
Photocopie, préparation de documents et autres activités spécialisées de soutien de bureau (8219Z)  
SIREN : [REDACTED]  
16 [REDACTED]  
[2 dirigeants portent le nom \[REDACTED\]](#)

<https://societe.com/>

 [REDACTED]  
En instance de chiffrage (0000Z)  
SIREN : [REDACTED]  
14 [REDACTED]  
[2 dirigeants portent le nom \[REDACTED\]](#)

 [REDACTED]  
Location de terrains et d'autres biens immobiliers (6820B)  
SIREN : [REDACTED]  
33 [REDACTED]  
[1 dirigeant porte le nom \[REDACTED\]](#)

# Step 1 : Picking your POI

- Get some easily accessible info, then **pivot** : from “Username”

WhatsMyName Web

Enter the username(s) in the search box, select any category filters & click the search button

Category Filters

Found: 6 Processed: 638 / 632

Show Found Show False Positives Show Not Found Show All

<b>Taringa</b> Username: kazadul Category: social Account Found	<b>tradingview</b> Username: kazadul Category: finance Account Found	<b>Duolingo</b> Username: kazadul Category: hobby Account Found
<b>Trello</b> Username: kazadul Category: social Account Found	<b>TrackmaniaLadder</b> Username: kazadul Category: gaming Account Found	<b>slides</b> Username: kazadul Category: social Account Found



**Maigret**

<https://github.com/soxoj/maigret>



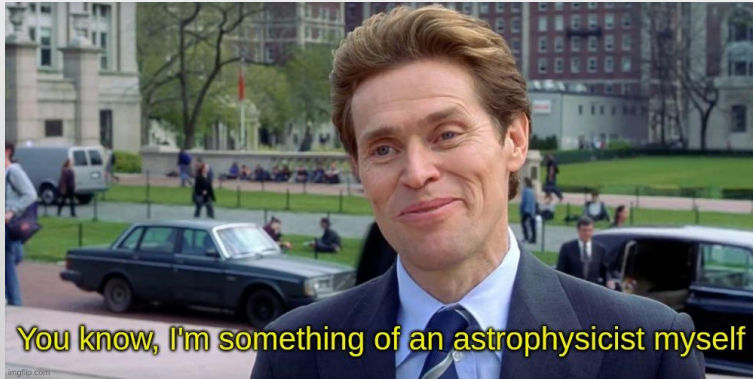
# Step 1 : Picking your POI



# Step 2 : Defining your persona

- **Persona** = Constructed identity/role for the interaction/engagement
- Must be constructed carefully :
  - Basic information : name, gender, city, DOB, family, friends, work connections
  - Already an idea of pretext(s) to play
  - Don't go too far, don't make up too much !
    - “Overproving kills the magic” - Daniel Madison
    - **Truth-default theory** (Malcolm Galdwell)
  - Sock puppets must be regularly active and alimented !

# Step 2 : Defining your persona



## Truth-Default Theory

“our operating assumption is that the people we are dealing with are honest.”

## Tribe mentality

“We like more people that appear to be like us.”

Seem to be from the same “tribe” as your POI.

Use vocabulary, expression, social codes, appearance, etc.



# Step 2 : Defining your persona



- Certainty
- Uncertainty/Variety
- Significance
- Connection/Love
- Growth
- Contribution

## Step 2 : Defining your persona



# Step 3 : Building your pretext(s)

**Pretext** = Context of an interaction designed to achieve a goal

**PREPARE** : Framework for creating a strong pretext (Christopher Hadnagy in *Human Hacking*)

1. **Problem**: Identify the issue you're trying to solve. **What's the goal of the interaction ?**
2. **Result**: Specify your desired outcome. **What would accomplish the goal ?**
3. **Emotional State**: **Identify the emotions you want to see in your subject.** Positive ones ? Negative ones ?
4. **Provocation**: **Anticipate the emotions you need to project** or display in order to generate the desired emotions in your subject.
5. **Activation**: **Define precisely your pretext**, which should be very clear by now.
6. **Rendering**: Determine the specifics of **where, when, and how** best to deliver or render the pretext.
7. **Evaluation**: **Mentally evaluate your pretext** and iteraly improve it, as well as your persona.

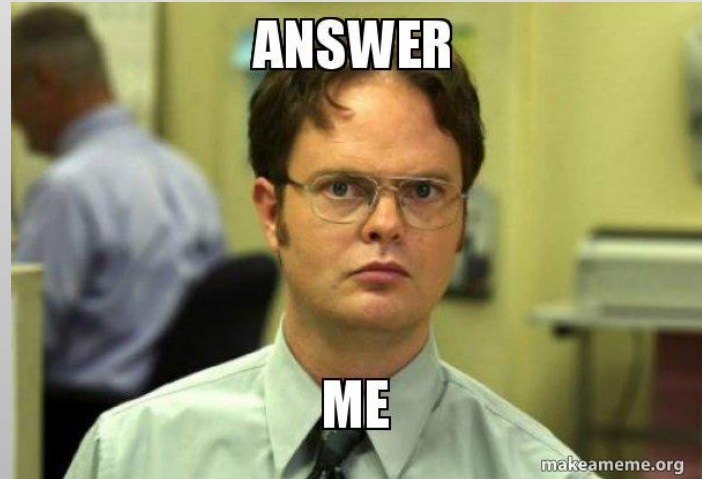


# Step 3 : Building your pretext(s)

- A pretext fails when suspicion is raised, either by blunders or by giving away signals
- Don't try too much to sound convincing
- Let your POI complete your pretext in their head
- Biopsychology : Which hormones/neurotransmitters are in action ?
  - Positive emotions: Dopamine, Serotonin, **Oxytocin**
  - Negative emotions: Cortisol (stress hormone), Adrénaline

# Step 3 : Building your pretext(s)

- **Establish contact** : Hooking POI and creating common ground to get the interaction started
- 4 questions in the POI's mind that must be answered ASAP
  - Who are you ?
  - What do you want ?
  - How long this will take ?
  - Are you a threat ?



# Step 3 : Building your pretext(s)

## Ten techniques to build rapport

(Robin Dreeke in *It's not all about me*)

Establishing artificial time constraints	Validation
Accommodating nonverbal	How ? When ? Why ?
Slower rate of speech	Using quid pro quo
Sympathy or assistance theme	Reciprocal altruism
Ego suspension	Manage expectations

# Step 3 : Building your pretext(s)

**Elicitation** = Process of extracting information from something or someone - NSA

- Open ended -> “What do you think about today’s weather ?”
- Close ended -> “The weather’s beautiful today isn’t it ?”
- Neutral -> “What do you think about today’s weather ?”
- Leading -> “The weather is pretty hot isn’t it ?”
- Assumptive -> “What is the biggest sum you’ve ever stolen from your company ?”

[https://www.dcsa.mil/Portals/91/Documents/CI/DCSA-CI\\_Elicitation\\_2021.pdf](https://www.dcsa.mil/Portals/91/Documents/CI/DCSA-CI_Elicitation_2021.pdf)



# Step 3 : Building your pretext(s)

**Elicitation** = Process of extracting information from something or someone - NSA

- Make illogical/wrong statements
- Help them to assume you know something or someone you don't
- Feign incredulity/Make them justify themselves

[https://www.dcsa.mil/Portals/91/Documents/CI/DCSA-CI\\_Elicitation\\_2021.pdf](https://www.dcsa.mil/Portals/91/Documents/CI/DCSA-CI_Elicitation_2021.pdf)

# Step 3 : Building your pretext(s)

## Seven influence tools

(Robert Cialdini in *Influence*)

- **Reciprocity**
- Concession
- Sympathy & liking
- Korman's self-consistency
- Scarcity
- Social proof
- Authority / Expertise

**Doing something or giving a gift to your person of interest to create an “obligation”**

- Asking a question : this creates an obligation to respond
- Divulging a piece of info : may create an obligation in your POI mind to do the same
- The exchange of gifts and services increase trust, which lead to even bigger gifts and services, etc.

# Step 3 : Building your pretext(s)

## Seven influence tools

(Robert Cialdini in *Influence*)

- Reciprocity
- **Concession**
- Sympathy & liking
- Korman's self-consistency
- Scarcity
- Social proof
- Authority / Expertise

**Conceding on something to make your POI do the same  
(Sometimes considered to be a variation of Reciprocity)**

- The concession must be on something that matters to your POI (remember that empathy is key)
- If your POI refuses something, *give them a choice*: they'll be more likely to comply after

# Step 3 : Building your pretext(s)

## Seven influence tools

(Robert Cialdini in *Influence*)

- Reciprocity
- Concession
- **Sympathy & liking**
- Korman's self-consistency
- Scarcity
- Social proof
- Authority / Expertise

**Your person of interest is more likely to comply to your requests if they like you**

- Tribe mentality
- Compliments/Positive reinforcement
- Cooperation
- Association



# Step 3 : Building your pretext(s)

## Seven influence tools

(Robert Cialdini in *Influence*)

- Reciprocity
- Concession
- Sympathy & liking
- **Korman's self-consistency**
- Scarcity
- Social proof
- Authority / Expertise

**An individual behaves to stay consistent with their decisions, the image they have of themselves and with what others think of them. Failing to stay consistent causes internal conflict.**

- Cognitive routine to avoid too much decision-making
- Commitment escalation
- *Foot-in-the-door technique* : Make your POI agree to something minor to make them agree to something bigger after

# Step 3 : Building your pretext(s)

## Seven influence tools

(Robert Cialdini in *Influence*)

- Reciprocity
- Concession
- Sympathy & liking
- Korman's self-consistency
- **Scarcity**
- Social proof
- Authority / Expertise

### What is rare is desirable

- Make offers limited in time
- Appear busy to make your time seem more valuable
- Implant the idea in your POI that they're special for you by saying them "a little secret"
  - also triggers Reciprocity

# Step 3 : Building your pretext(s)

## Seven influence tools

(Robert Cialdini in *Influence*)

- Reciprocity
- Concession
- Sympathy & liking
- Korman's self-consistency
- Scarcity
- **Social proof**
- Authority / Expertise

**We believe something is good/appropriate if peers think it is**

- “Top 50 songs effect”
- Brand something as popular or validated by known peers of your POI

# Step 3 : Building your pretext(s)

## Seven influence tools

(Robert Cialdini in *Influence*)

- Reciprocity
- Concession
- Sympathy & liking
- Korman's self-consistency
- Scarcity
- Social proof
- **Authority / Expertise**

**We follow and listen more to people appearing to have legitimate authority or expertise**

- Three types of authority
  - Legal
  - Organizational
  - Social
- Appear to be knowledgeable or competent in a domain to be considered as an expert of it

# Step 3 : Building your pretext(s)



- Build at least **2 pretexts**
  - With your goal in mind
  - Tailored for your POI
  - Using your persona
  - Based on the PREPARE framework if possible
  - Applying elicitation & influence techniques
- We'll review your work together

# Example : Company 1 - POI

- **Goal** : Get intelligence about VIP/Company
- **POI**: Aurélie Martin
- Interesting informations
  - Developer
  - Dog lover, vegan, progressive causes
  - Teaches maths, u/girlsdomath2
  - Complains about state of the world on Twitter



# Example : Company 2 - Persona

- **Persona** : Camille Maes
- **Gender** : Female
- **City** : Paris
- **DOB** : 08/07/1997
- Works as a secretary in a law firm
- Wants to retrain in machine learning / code
- Vegetarian wanting to be vegan
- Account on Reddit and Twitter



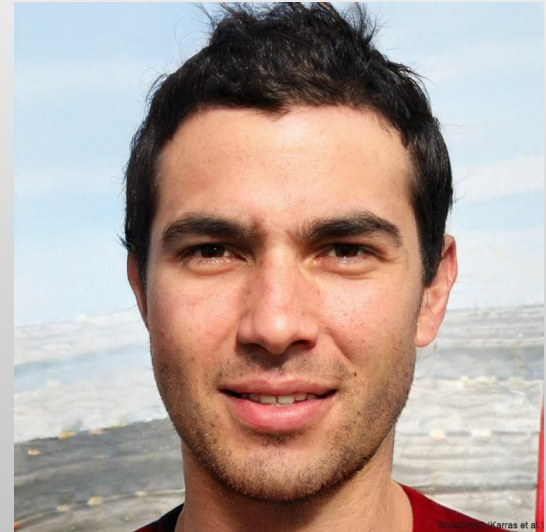
# Example : Company 2 - Pretext 1

1. **Problem:** Getting technological intel on the POI's company
2. **Result:** Befriending the POI and eliciting as much information as possible
3. **Emotional State:** Positive. Wanting to help, form a meaningful connection with fellow woman in tech (or wannabe)
4. **Provocation:** Seem ignorant and curious, put the POI in a “teacher” position, be thankful
5. **Activation:** Interact on social network and escalate interaction by asking questions and taking a mentee approach. Asking simple questions first and slowly transition into “tools of the trade” and “specific work approach” questions. Ask for examples from the POI workplace.
6. **Rendering:** On Reddit and then Discord. Tribe mentality (vegetarian/vegan, work field, gender), open-e. / close-e. questions, validation, wanting to help, make wrong statement, make POI justify
7. **Evaluation:** Ready to go !



# Example : Company 2 - POI

- **Goal** : Deliver payload
- **POI**: Jules Rossi-Schneider
- Interesting informations
  - Engineer
  - Single (Tinder, Fruitz, Bumble, Wyylde)
  - Loves going to the gym



# Example : Company 2 - Persona

- **Persona** : Claire Laurent
- **Gender** : Female
- **City** : Strasbourg, travelling to Finland
- **DOB** : 08/07/1995
- Does Yoga, wants to go to the gym more often
- Works in the movie industry
- Account on Instagram, Tinder, Wyyld



# Example : Company 2 - Pretext 1

1. **Problem:** Starting to befriend the POI on Tinder
2. **Result:** Tinder match, starting discussion, establish legit reason to not meet IRL for now, hinting at a possible meet someday
3. **Emotional State:** Positive. Feeling good, excited, involved in conversation.
4. **Provocation:** Appear excited, wanting to know more, flirting with POI
5. **Activation:** Match POI on Tinder, wait 2-3 days, start conversation, appear friendly and flirty, explaining being in Finland for work but coming back soon, get conversation going
6. **Rendering:** On Tinder chat. Tribe mentality (sport), compliments, reciprocity in info exchange, open-ended question, tapping into “Connection/Love” and “Uncertainty/Variety”
7. **Evaluation:** Ready to go !

# Example : Company 2 - Pretext 2

1. **Problem:** Deliver the payload (via an email attachment)
2. **Result:** Payload delivered without burning the POI
3. **Emotional State:** Positive + Urgency. Feeling good for helping, maybe expect something in return.
4. **Provocation:** Appear stressed/desperate, needing some help from a friend
5. **Activation:** Asking the POI to check/give advice on a work document send on professional email (pretexting that in the urgency we don't remember the personal address of POI). Pretext the document is not working if sent and needing to confirm that. Promise something spicy in return.
6. **Rendering:** Via private message (e.g. Signal) + mail.  
Sympathy, scarcity, reciprocity, tapping into "Significance", wanting to help, be valuable
7. **Evaluation:** Ready to go !



# Conclusion

- Targeted SE attacks are a reality and have a very good ROI for attackers
- Awareness & training are essential to mitigate the effectiveness of targeted SE attacks
- Nobody's perfect, someone's going to make a mistake at some point
- Elicitation, rapport building and influence techniques are as varied as numerous
- Know what you should and shouldn't share or do, for your company's safety as well as your own

