



# SECURITY NEED-TO-KNOWS

*FOR THE FINANCIAL SECTOR*

# CONTENT OUTLINE

## INTRODUCTION

## STATE OF THE FINANCIAL SECTOR

- ATTACKS AGAINST CUSTOMERS
- ATTACKS AGAINST INSTITUTIONS

## REGULATIONS ON THE HORIZON

- GDPR ON DATA PROTECTION
- PSD2 ON OPEN BANKING

## CONFRONTING THE CHALLENGES

- RESPONSE CAPABILITIES
- YOUR PART OF THE PUZZLE



# LET'S GET ACQUAINTED

[DIEDERIK.PERK@FOX-IT.COM](mailto:DIEDERIK.PERK@FOX-IT.COM)

THREAT INTELLIGENCE ADVISOR

AUTHOR/SPEAKER/TRAINER

WEAK SPOT FOR CARTOONS & MEMES

# FROM PAYMENT SYSTEMS TO SURGERY ROOMS

KNOW THE RISK BEFORE IT IMPACTS YOU

# PHYSICAL WORLD NOT SAFE FROM HARM



SECURITY'S JOB IS TO INSPIRE TRUST

CANNOT BE DONE IN ISOLATION

# ISSUES IN AND AROUND THE OFFICE

WHAT DO YOU SEE?

# TWO SIDES OF THE SAME COIN

## Blue Team

Vulnerability-centric  
'Cyber Hygiene'

## Red Team

Threat-centric  
'Active Defense'

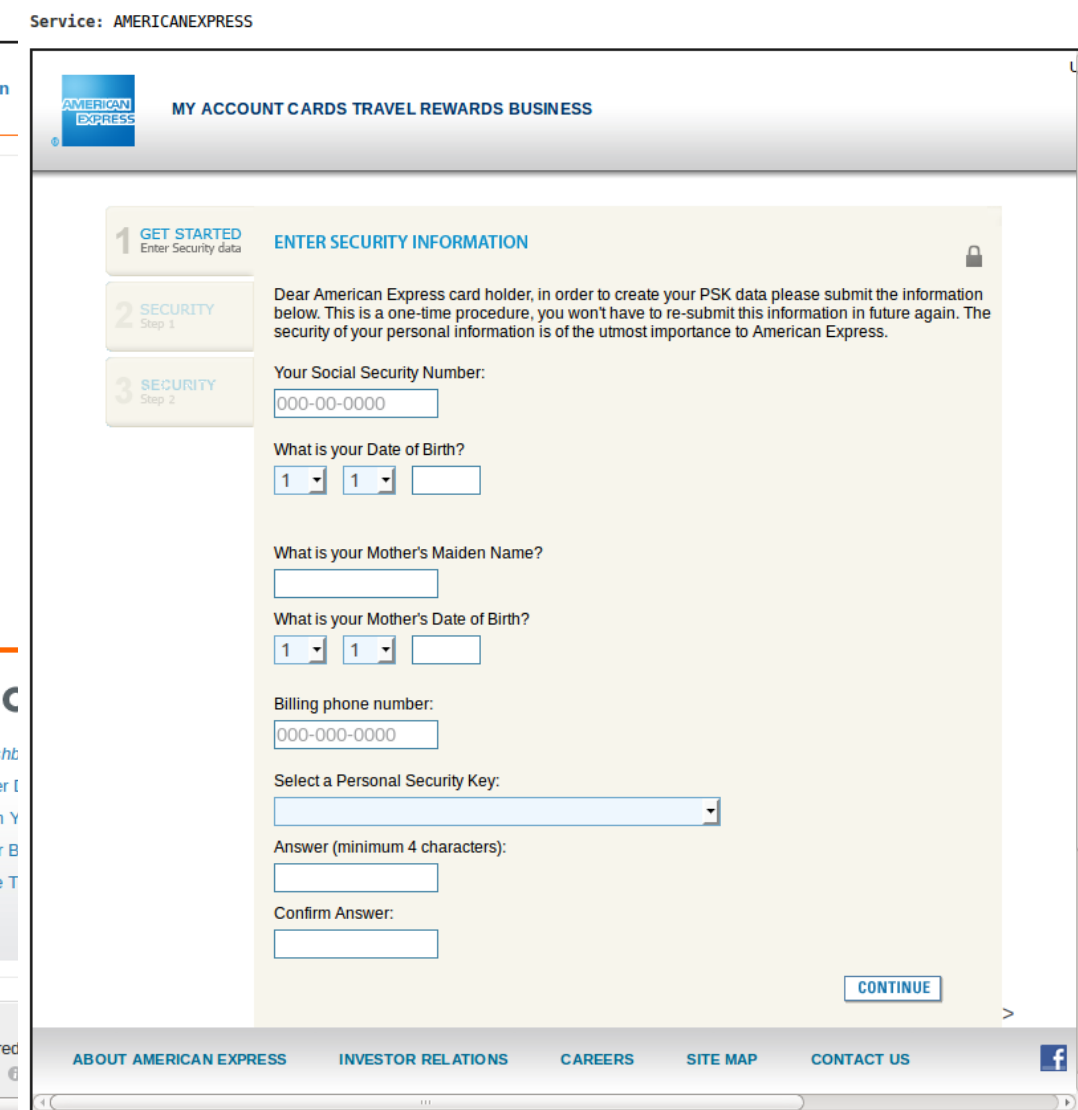
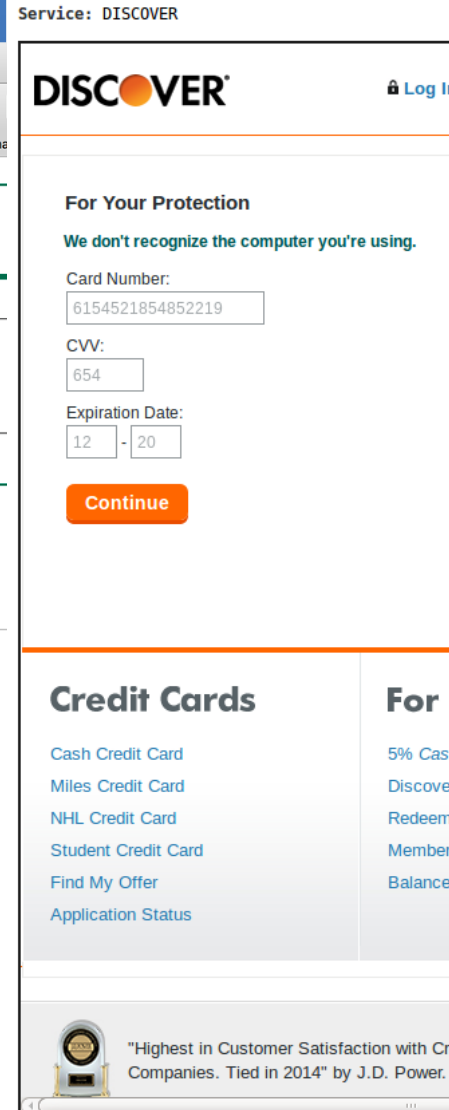
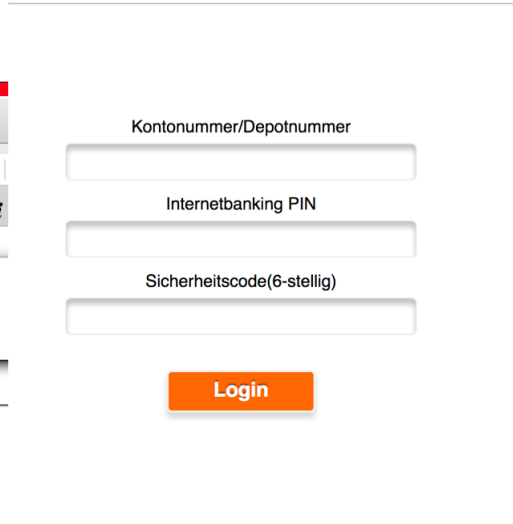
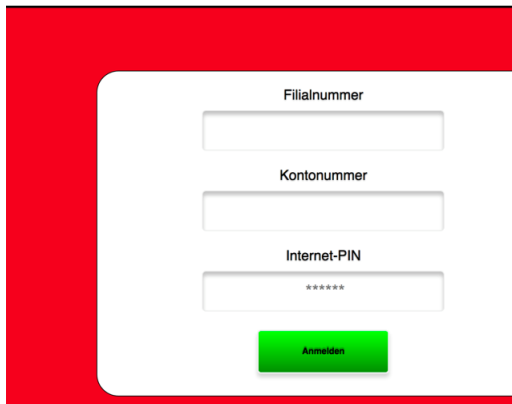
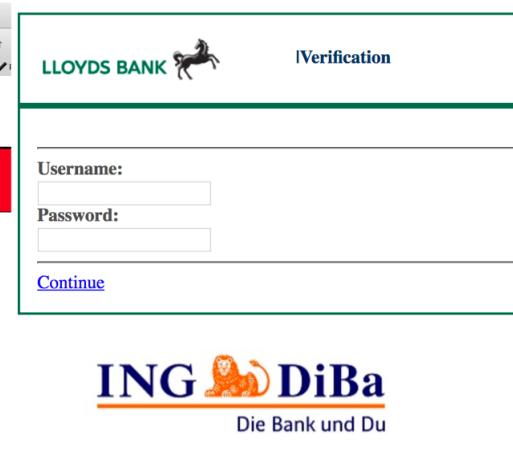
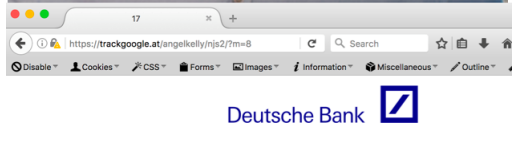
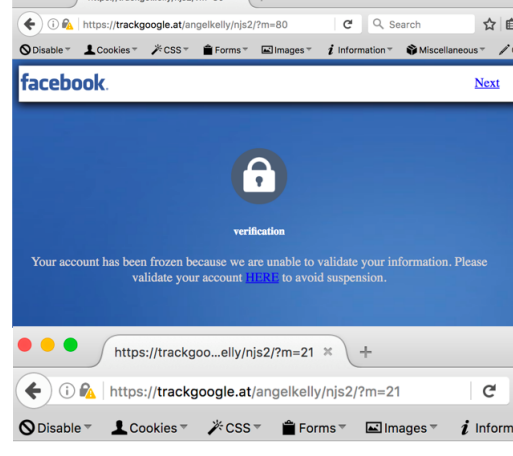
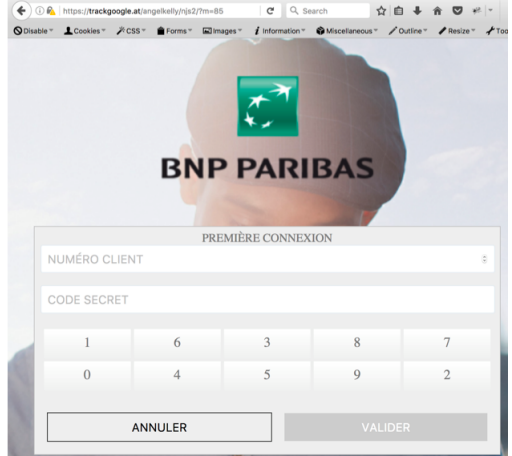




# STATE OF THE FINANCIAL SECTOR

ATTACKS AS A DAILY ROUTINE

# WHEN YOU SEE THIS...

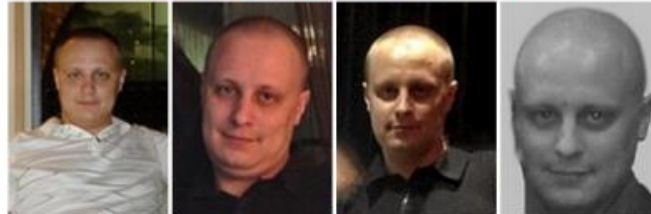


# PORTRAIT OF A MASTER THIEF

**WANTED**  
**BY THE FBI**

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering

## **EVGENIY MIKHAILOVICH BOGACHEV**



Multimedia: Images

### Aliases:

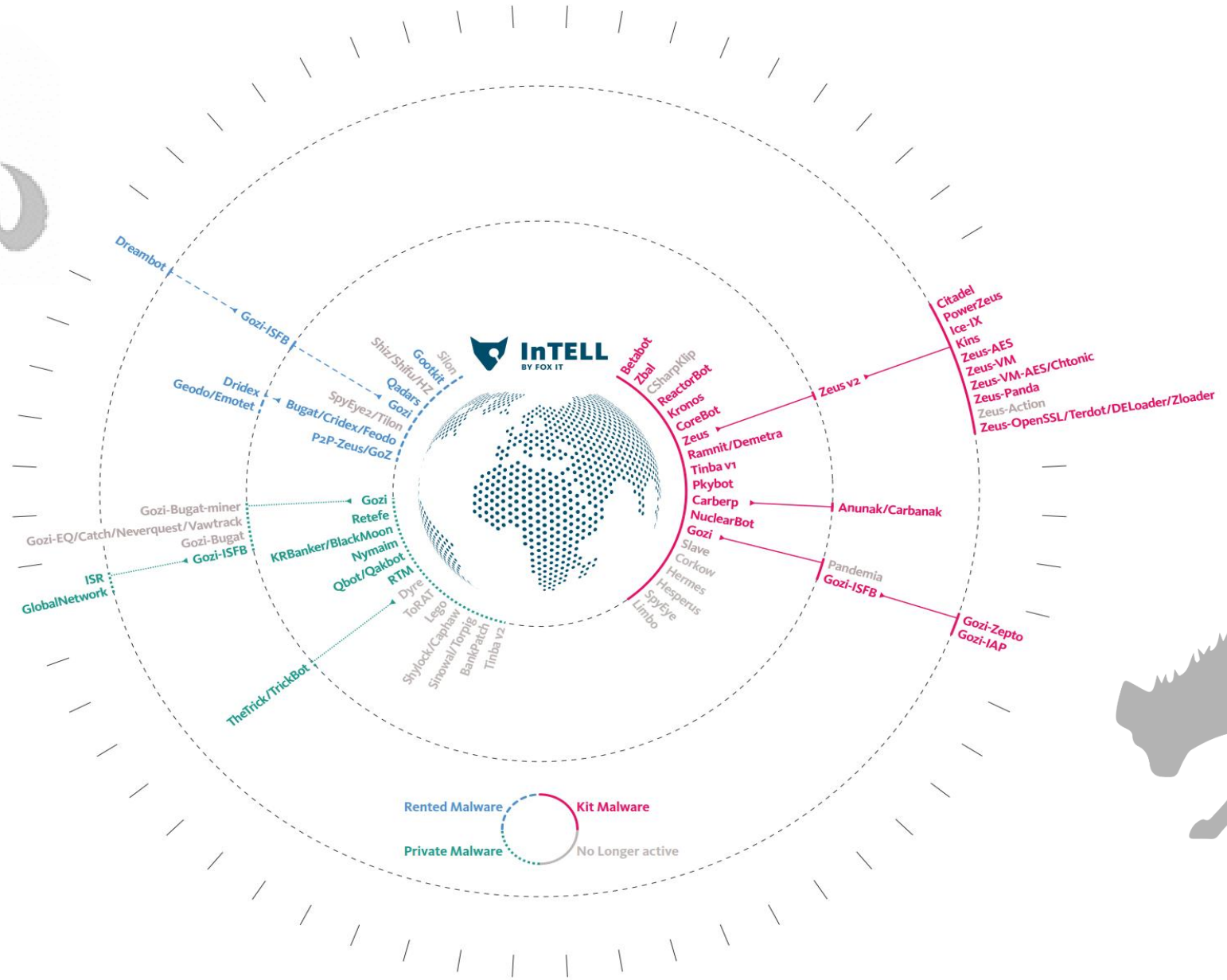
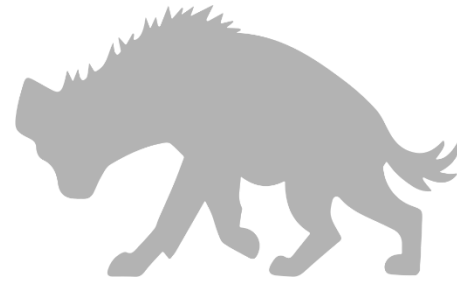
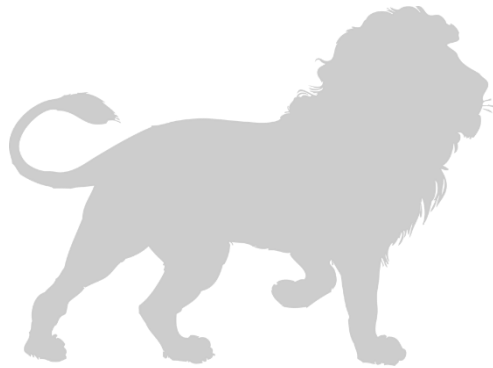
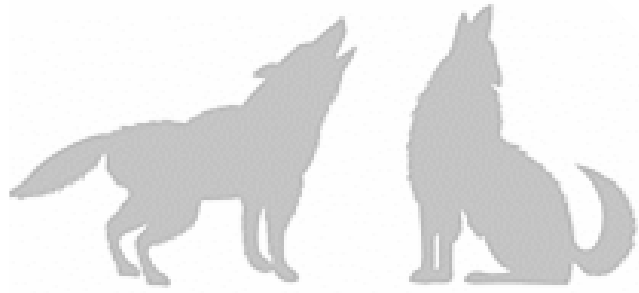
Yevgeniy Bogachev, Evgeniy Mikhailovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

## **DESCRIPTION**

<b>Date(s) of Birth Used:</b>	October 28, 1983	<b>Hair:</b>	Brown (usually shaves his head)
<b>Height:</b>	Approximately 5'9"	<b>Eyes:</b>	Brown
<b>Weight:</b>	Approximately 180 pounds	<b>Sex:</b>	Male
<b>NCIC:</b>	W890989955	<b>Race:</b>	White
<b>Occupation:</b>	Bogachev works in the Information Technology field.		

**Remarks:** Bogachev was last known to reside in Anapa, Russia. He is known to enjoy boating and may travel to locations along the Black Sea in his boat. He also owns property in Krasnodar, Russia.

# FINANCIAL MALWARE LANDSCAPE

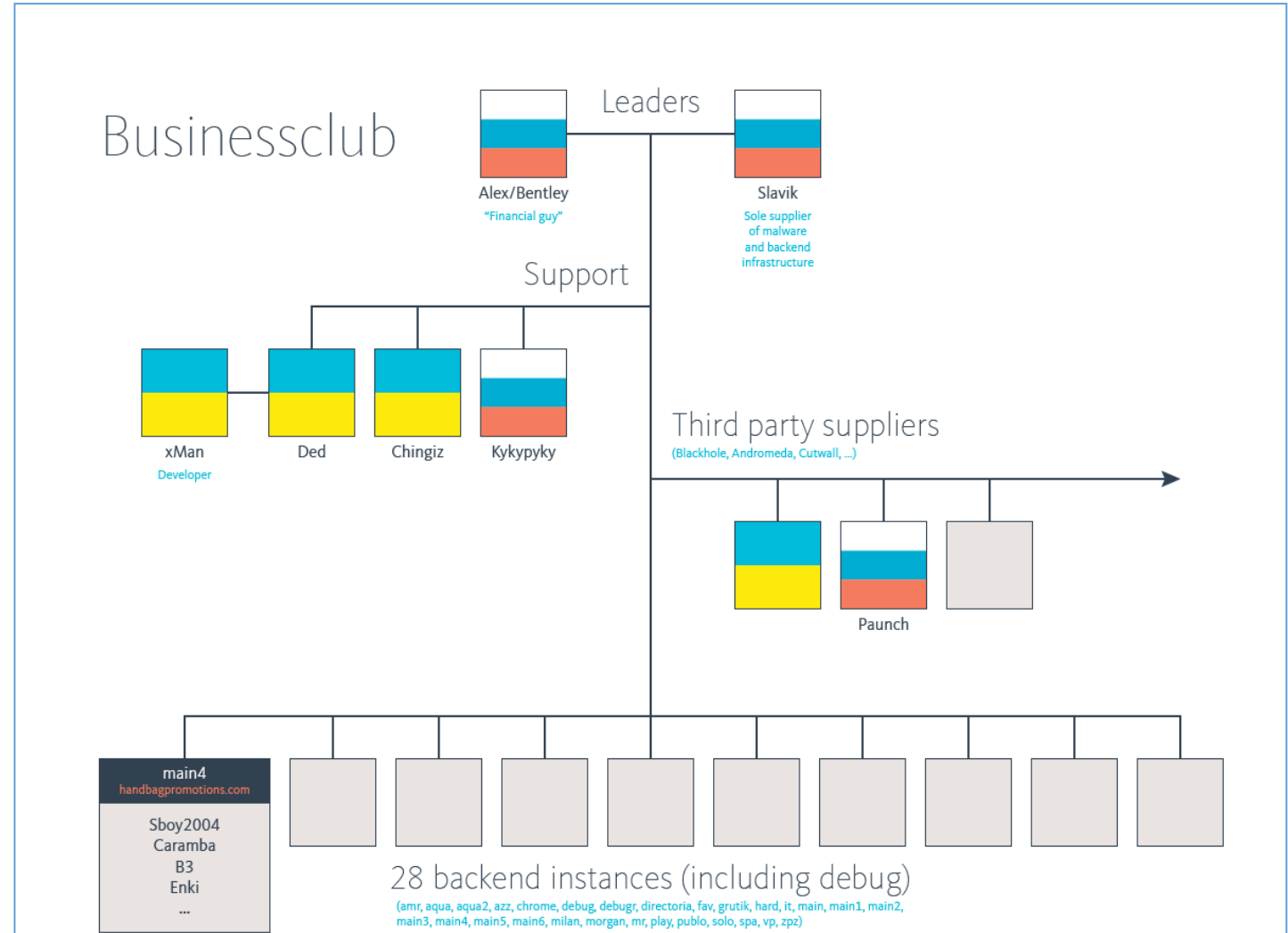


# A FRAUD OPERATION

zeus\_at0m@businessclub.so (11/12)

at0m

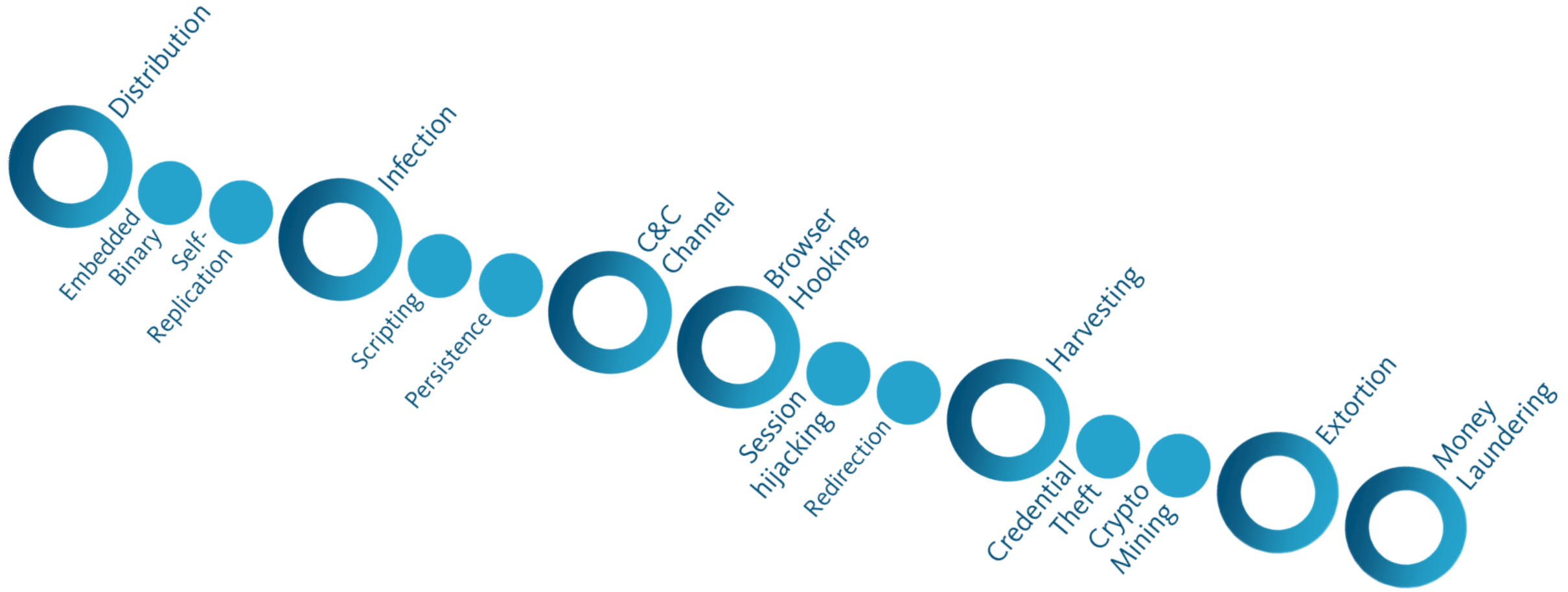
- ▼ Crypter's (2/3)
  - ★ c4y\_2
  - ★ crypt4you
  - ★ mrlapis
- ▼ spam (4/4)
  - ★ dot
  - ★ j.p.morgan
  - ★ roach
  - ★ uho
- ▼ Team leader (2/2)
  - ★ Alex
  - ★ Dear
- ▼ Technical support (3/3)
  - ★ chingiz
  - ★ ded
  - ★ kykypyky



VALUE MAY BE PERCEIVED DIFFERENTLY

NICE GRAPHICS PROCESSING UNIT (GPU) YOU HAVE THERE...

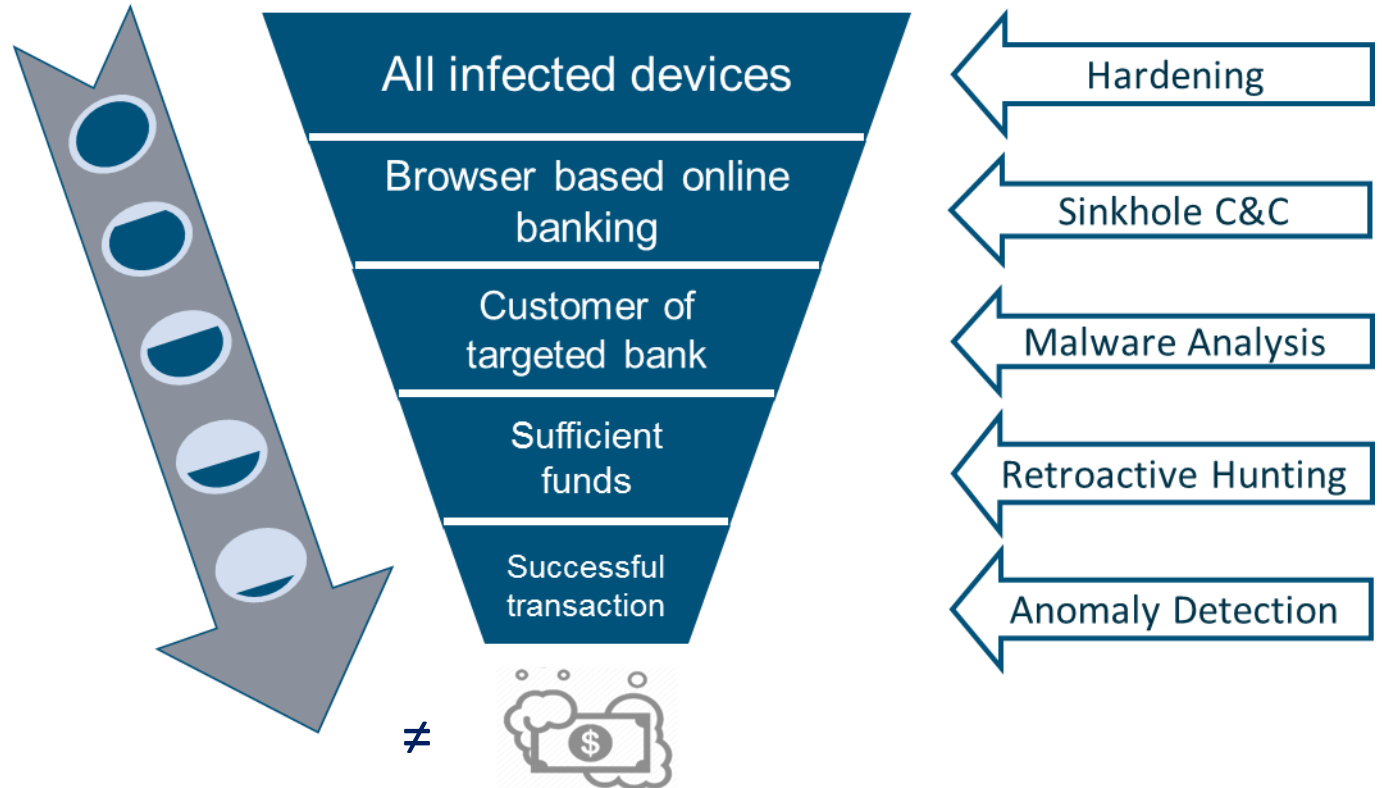
# MULTI STAGE FRAUD ATTACK BY BANKING TROJAN



# CONDITIONS AND COUNTERMEASURES

- Volume
- Velocity
- Veracity

Value

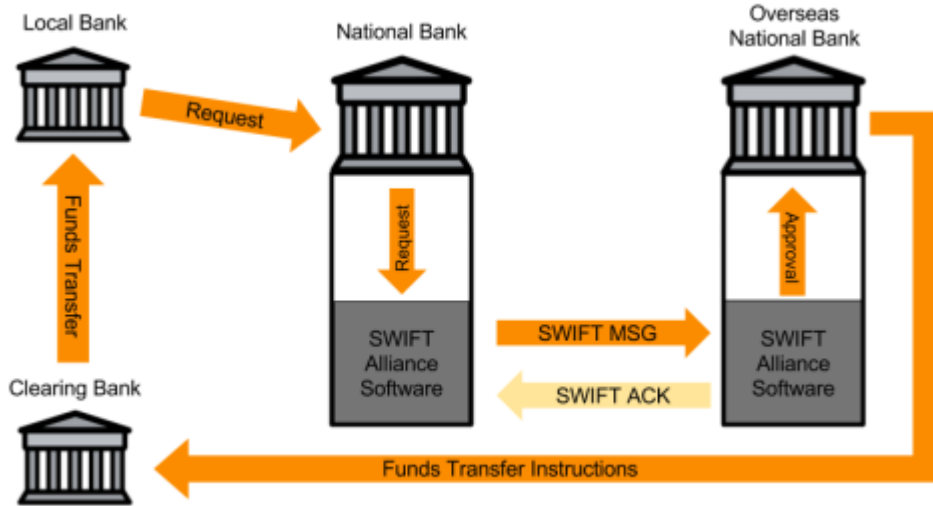




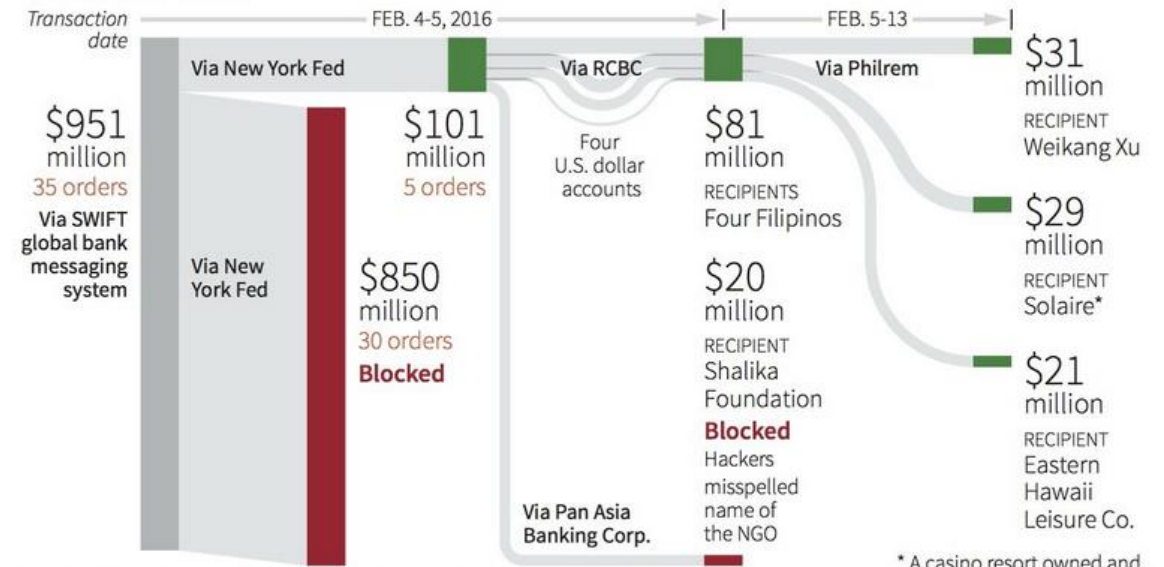
# GOING AFTER BIG FISH

TRANSFER FUNDS OUT FROM WITHIN

# BANK OF BANGLADESH



## THE MONEY TRAIL



Sources: Philippines Court of Appeals documents; Reuters

W. Foo, 31/03/2016

\* A casino resort owned and operated by Bloomberry Resorts

# CARBANAK

## How the Carbanak cybergang stole \$1bn A targeted attack on a bank

### 1. Infection



100s of machines infected in search of the admin PC



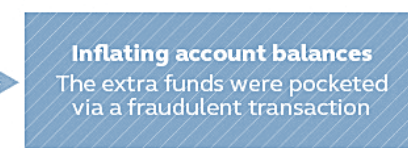
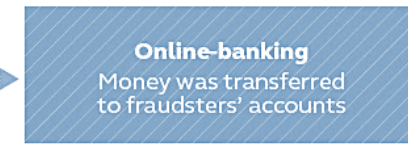
### 2. Harvesting Intelligence

Intercepting the clerks' screens



### 3. Mimicking the staff

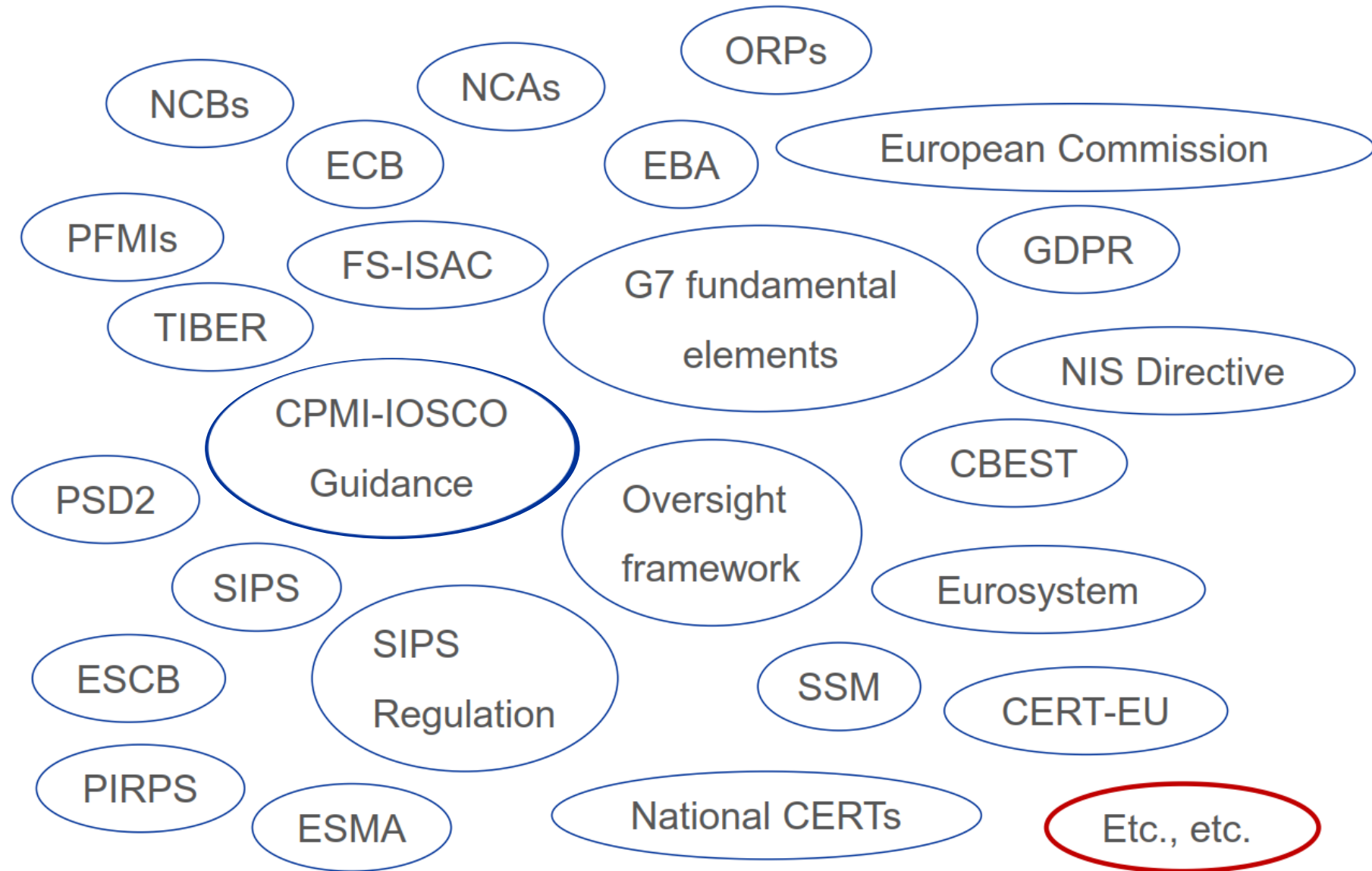
How the money was stolen



# DEVELOPMENTS IN REGULATION

BLAME THE VICTIM?

# Legislation, Guidance, authorities and initiatives....



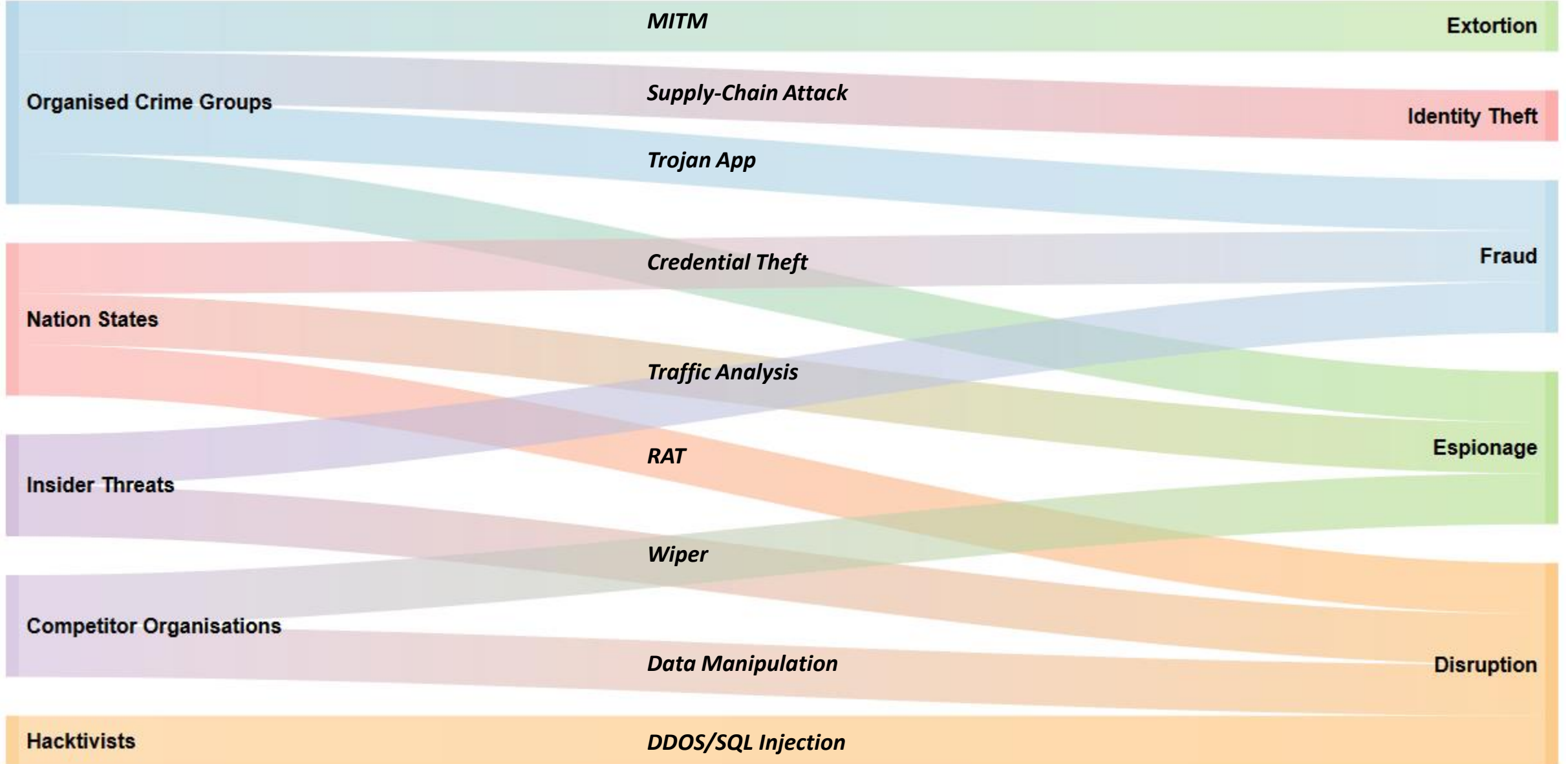
# HOW OPEN IS OPEN BANKING IN TERMS OF SECURITY?

EXPOSURE VS. EXPLOITATION

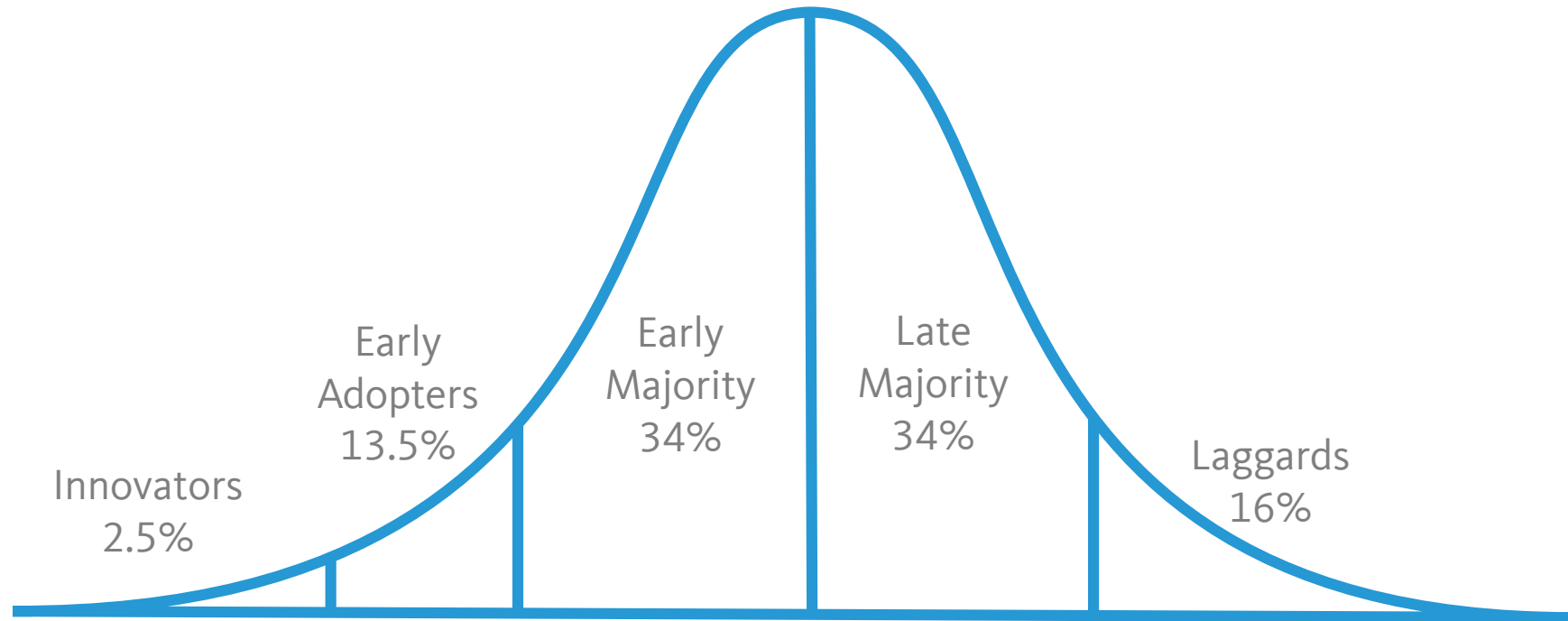
## Threat Actor

## Method

## Result



# ADOPTION RATE



From E.M. Rogers, *Diffusion of Innovations*, 4<sup>th</sup> edition (New York: The Free Press, 1995)



# SCENARIOS AND SIGNPOSTS

## Extortion

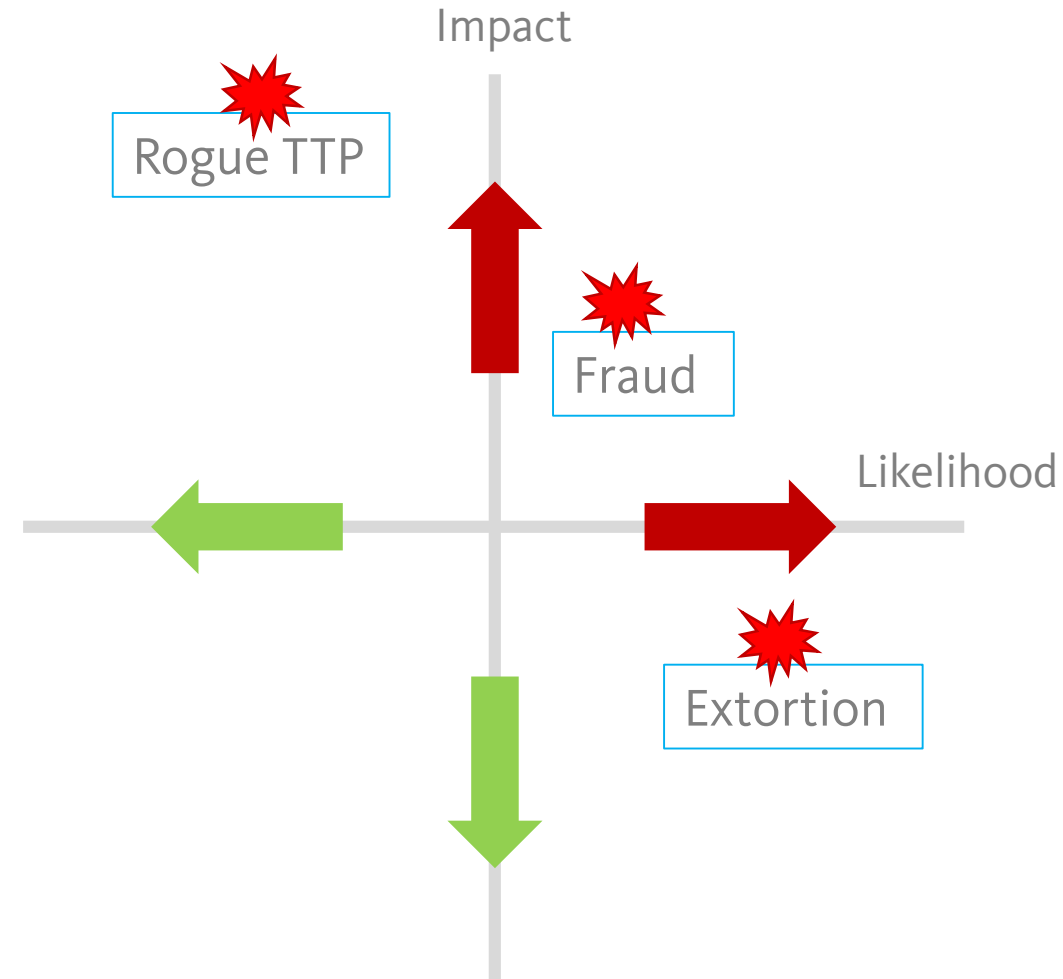
GDPR fine

## Commodity Fraud

Scalable vulnerability

## Rogue TPP spyware

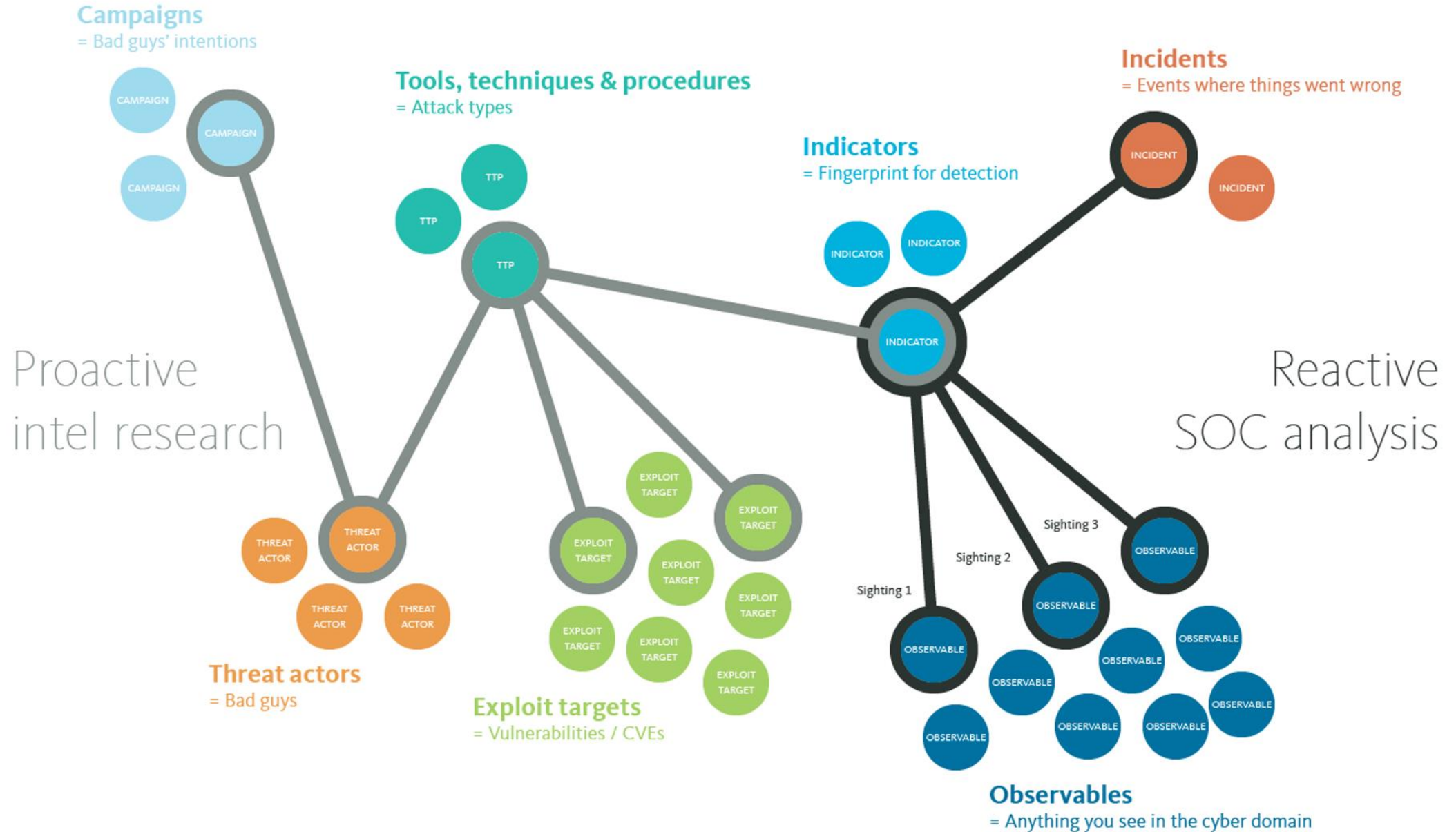
Business model without ROI



# COUNTERING THE ADVERSARY

WHERE THEY RESIDE

# INTELLIGENCE DRIVEN SECURITY



# REAL-TIME RESPONSE CAPABILITY



“EVERY SOLDIER A SENSOR”

WHAT YOU CAN DO



Q & A