FOX IT
part of nccgroup

SECURITY NEED-TO-KNOWS

FOR THE FINANCIAL SECTOR

InTELL
BY FOX IT

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

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

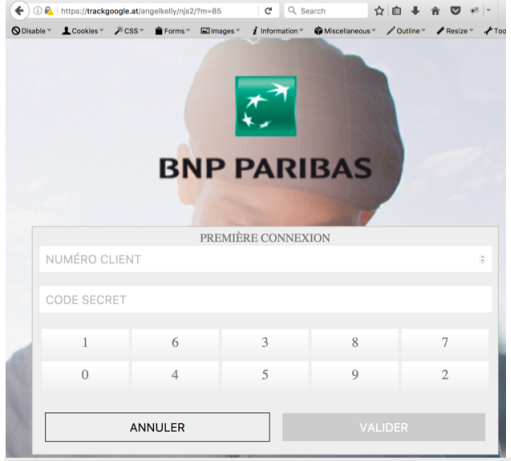
Threat-centric
'Active Defense'

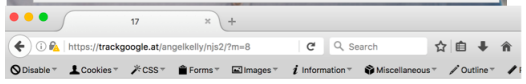
State of the financial sector

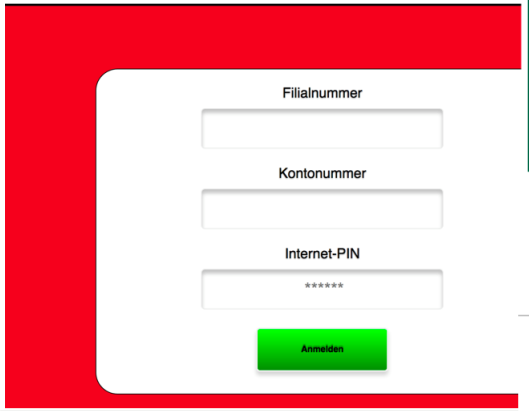
Attacks as a daily routine

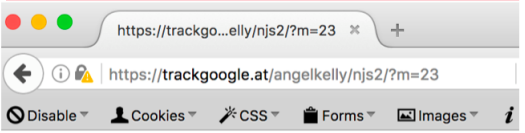
When you see this...

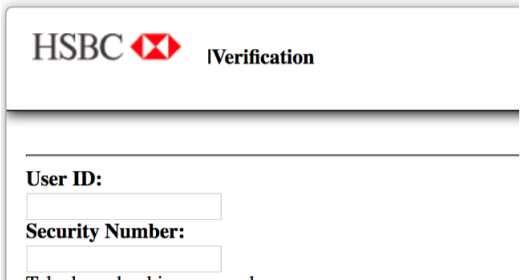
FOX IT
part of nccgroup

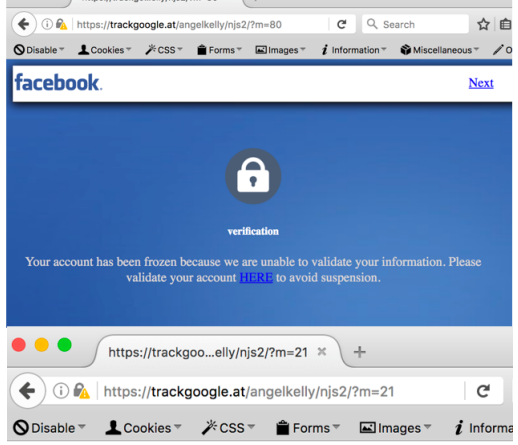


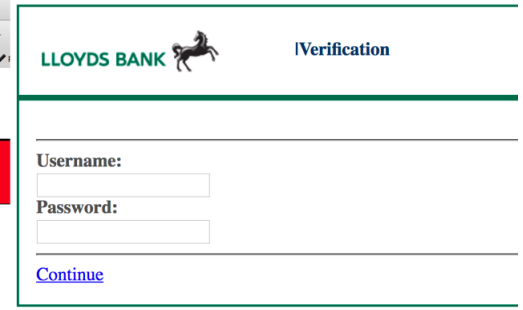


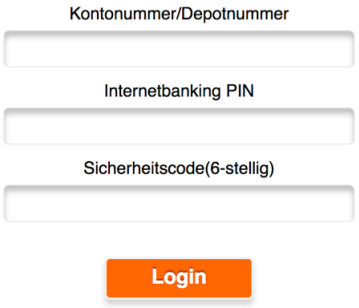




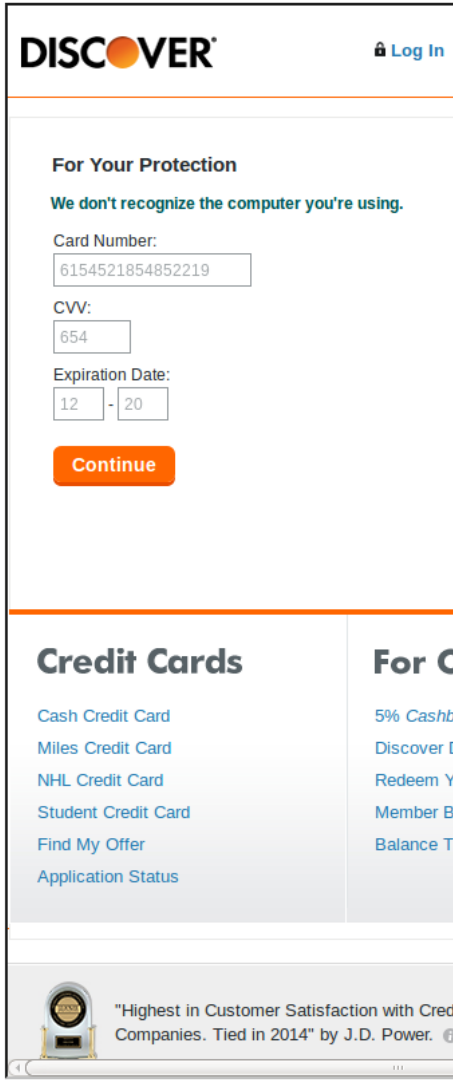






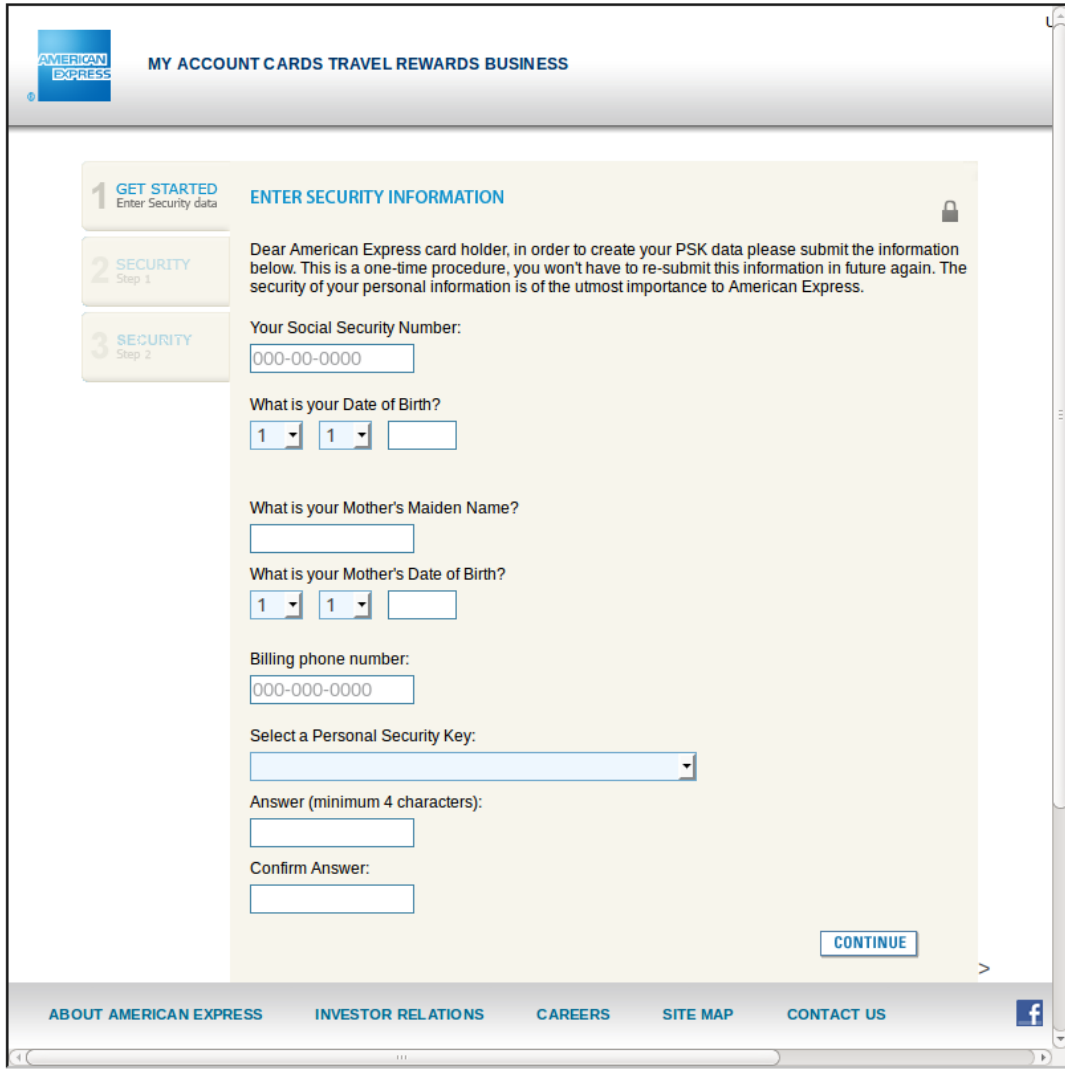


Service: DISCOVER



edit | list

Service: AMERICANEXPRESS



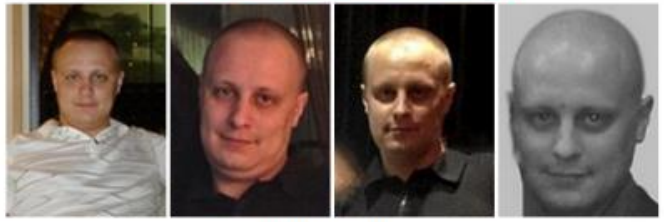
edit | list

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

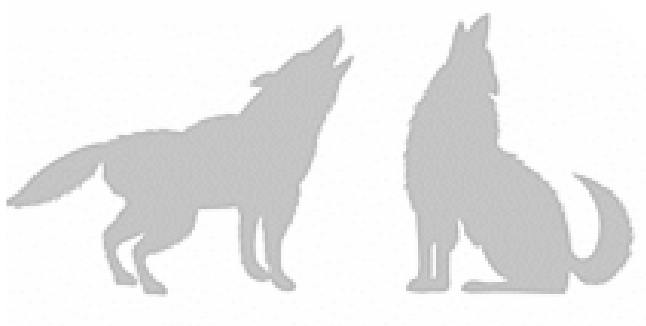
Aliases:
Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

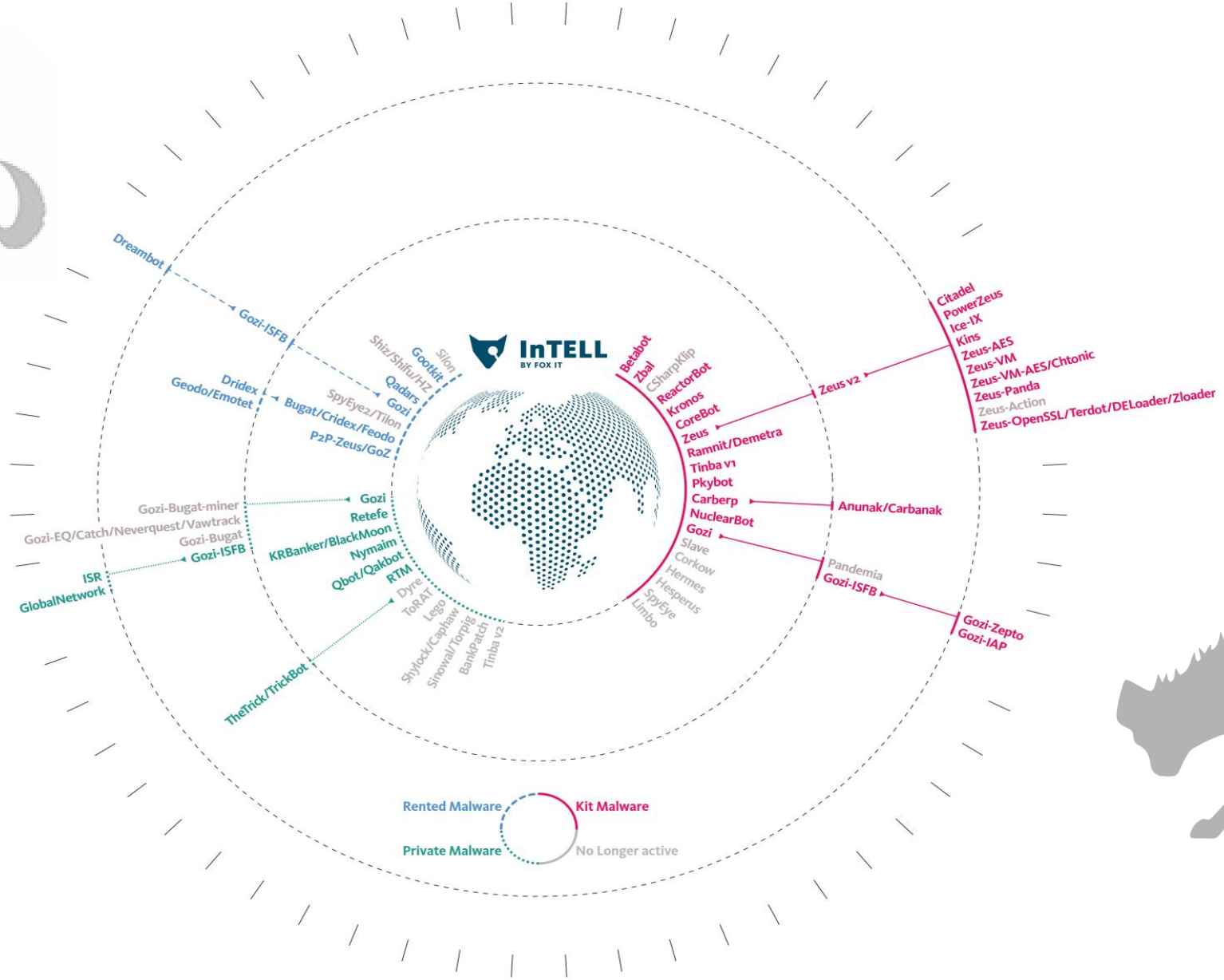
DESCRIPTION

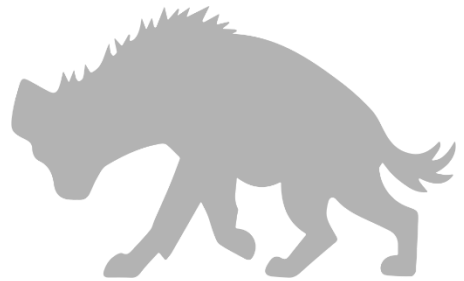
Date(s) of Birth Used:	October 28, 1983	**Hair:**	Brown (usually shaves his head)
Height:	Approximately 5'9"	**Eyes:**	Brown
Weight:	Approximately 180 pounds	**Sex:**	Male
NCIC:	W890989955	**Race:**	White
Occupation:	Bogachev works in the Information Technology field.		

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.

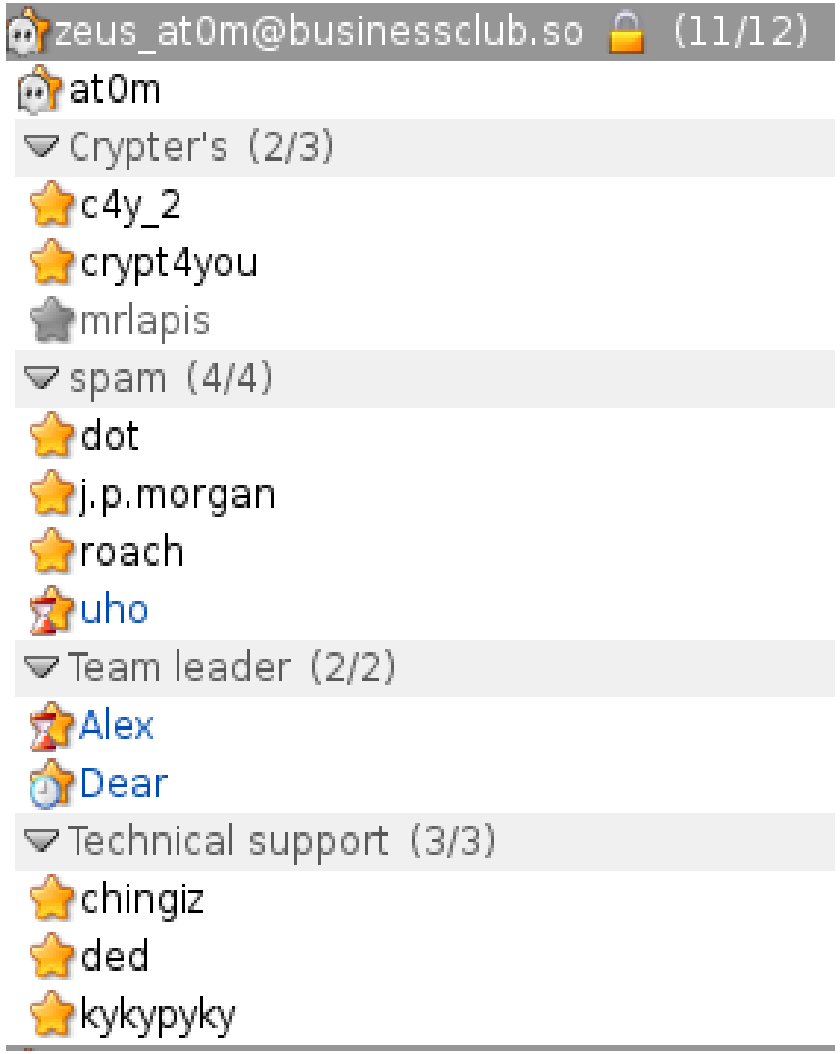
FINANCIAL MALWARE LANDSCAPE

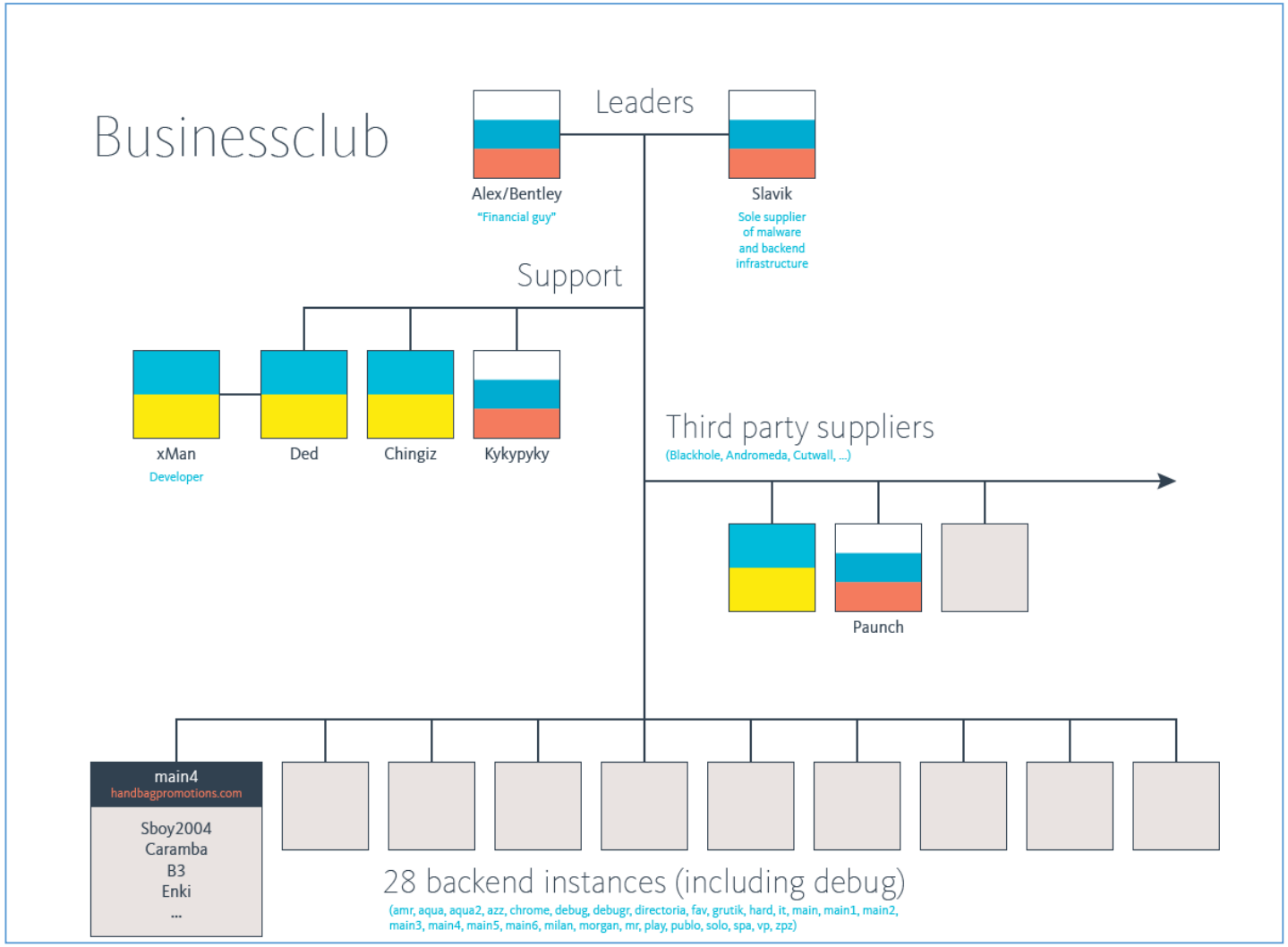






A Fraud operation

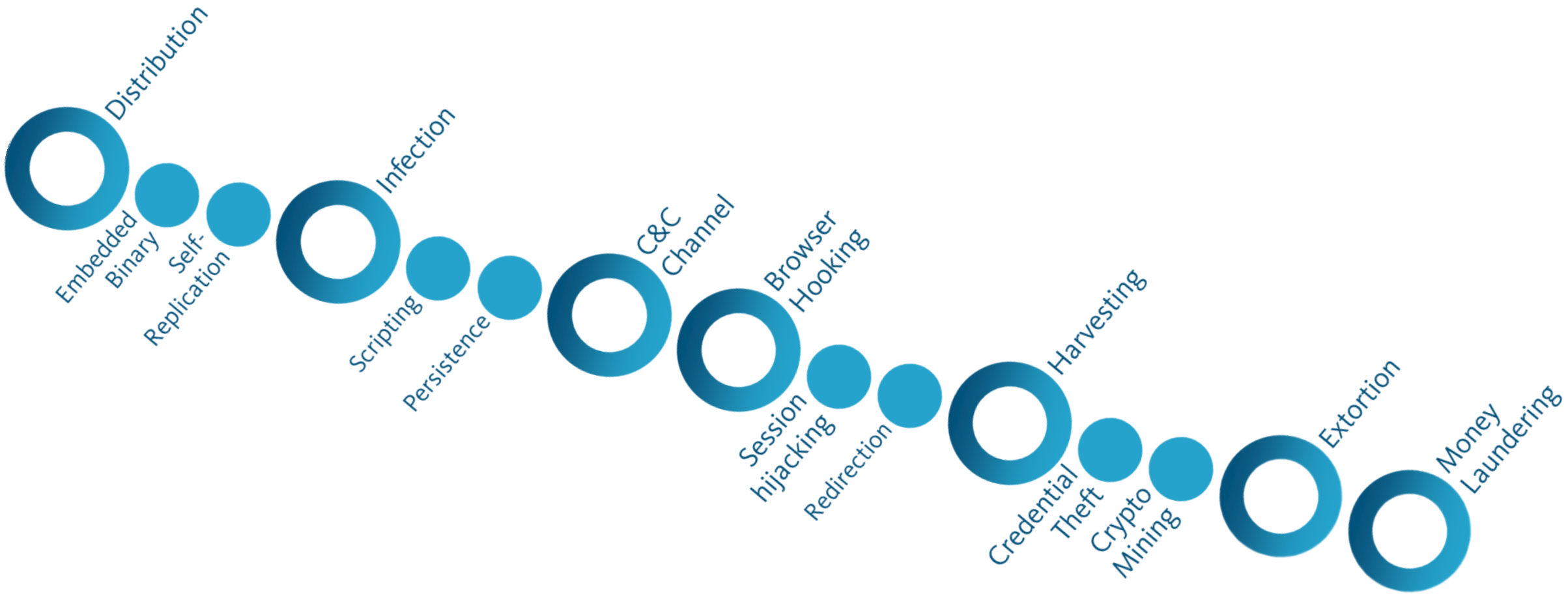




Value may be perceived differently

Nice graphics processing unit (GPU) you have there...

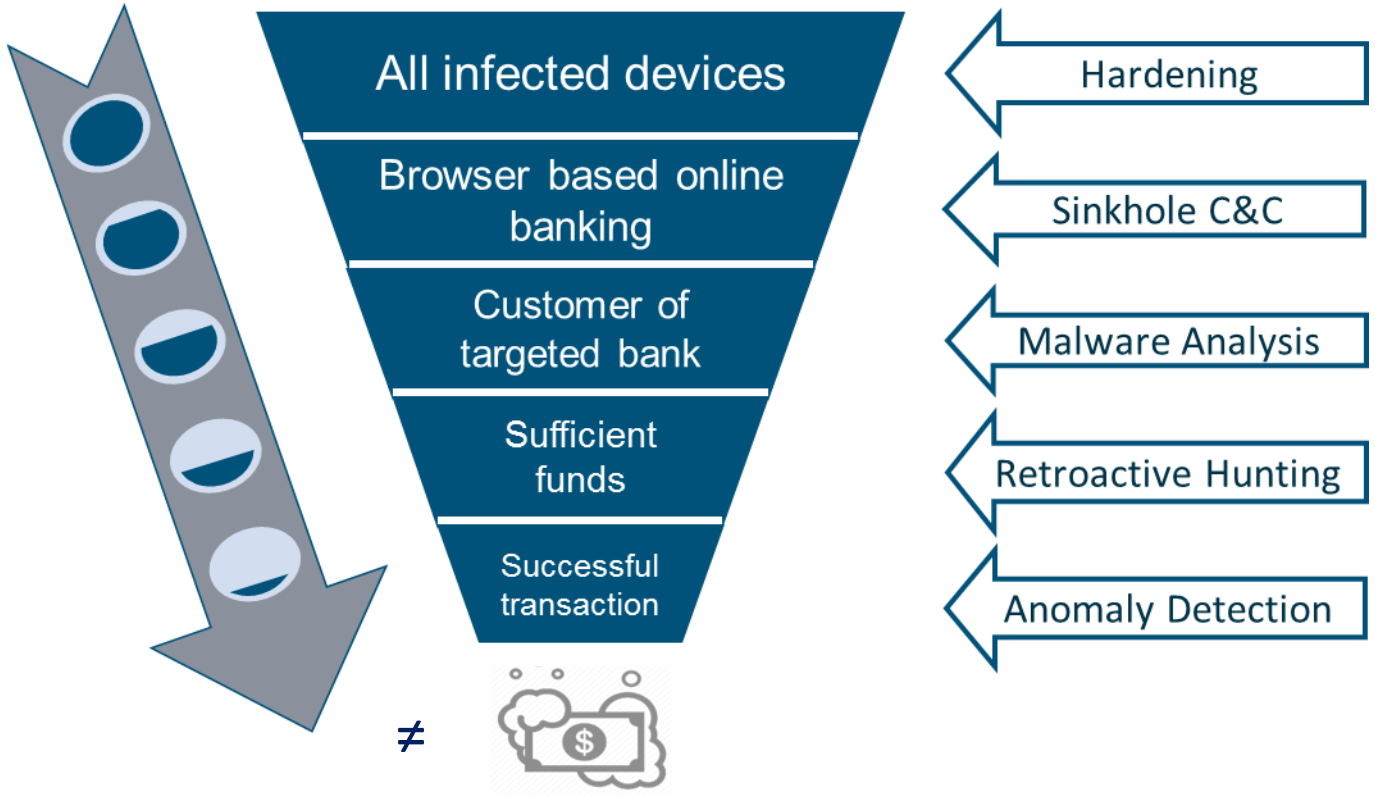
Multi stage Fraud attack by Banking Trojan



Conditions and Countermeasures

- Volume
- Velocity
- Veracity

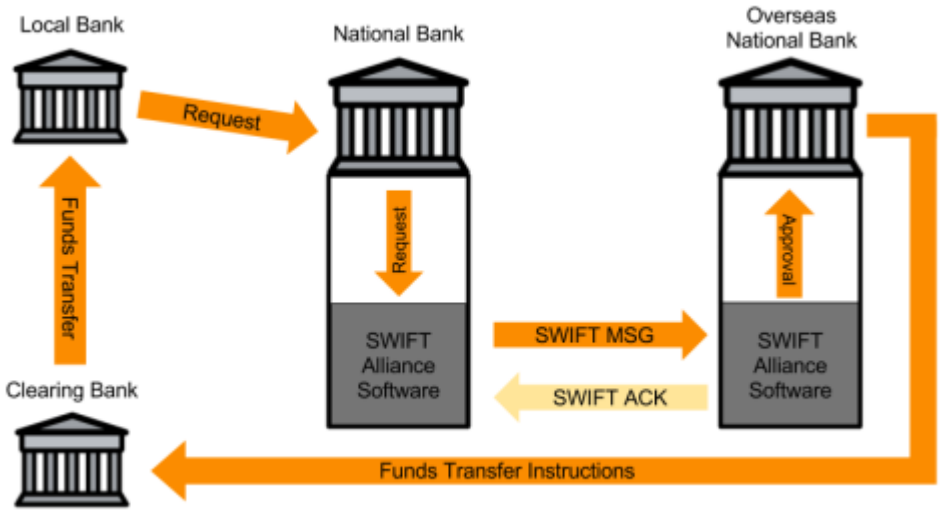
Value

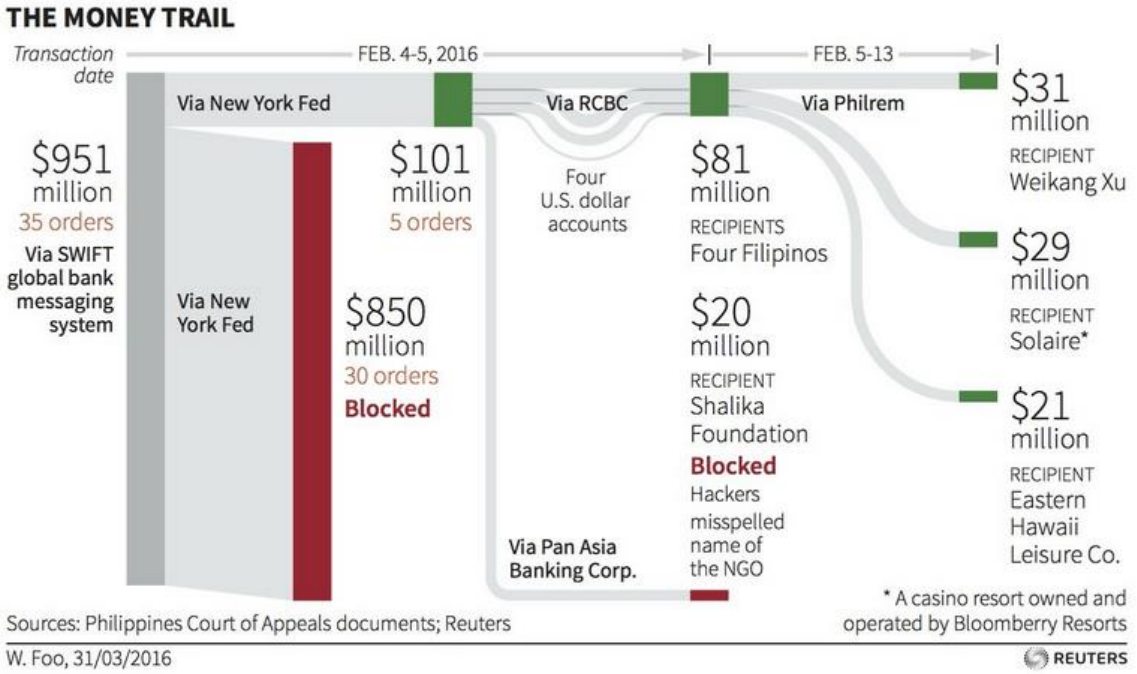


Going after big fish

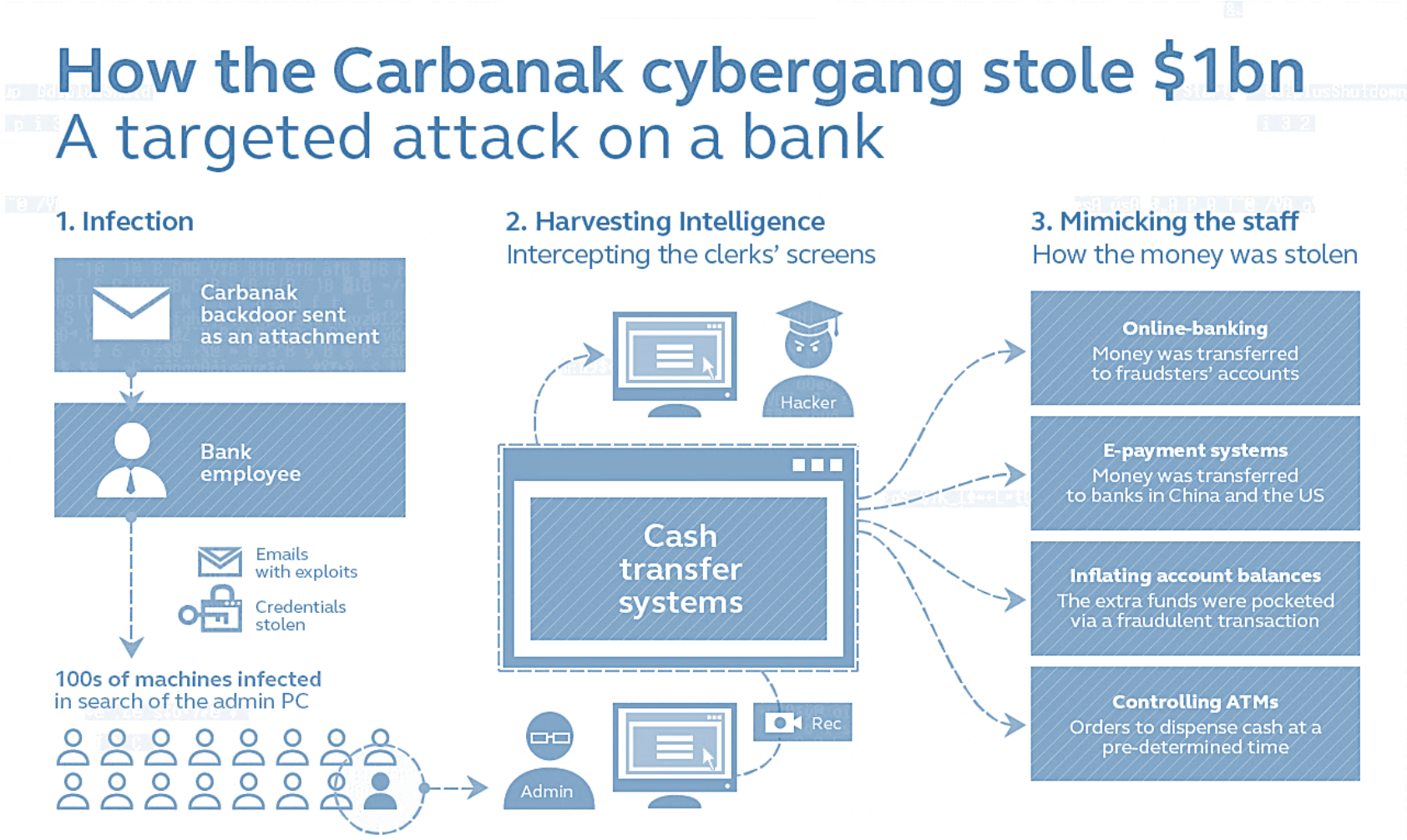
Transfer funds out from within

Bank of Bangladesh





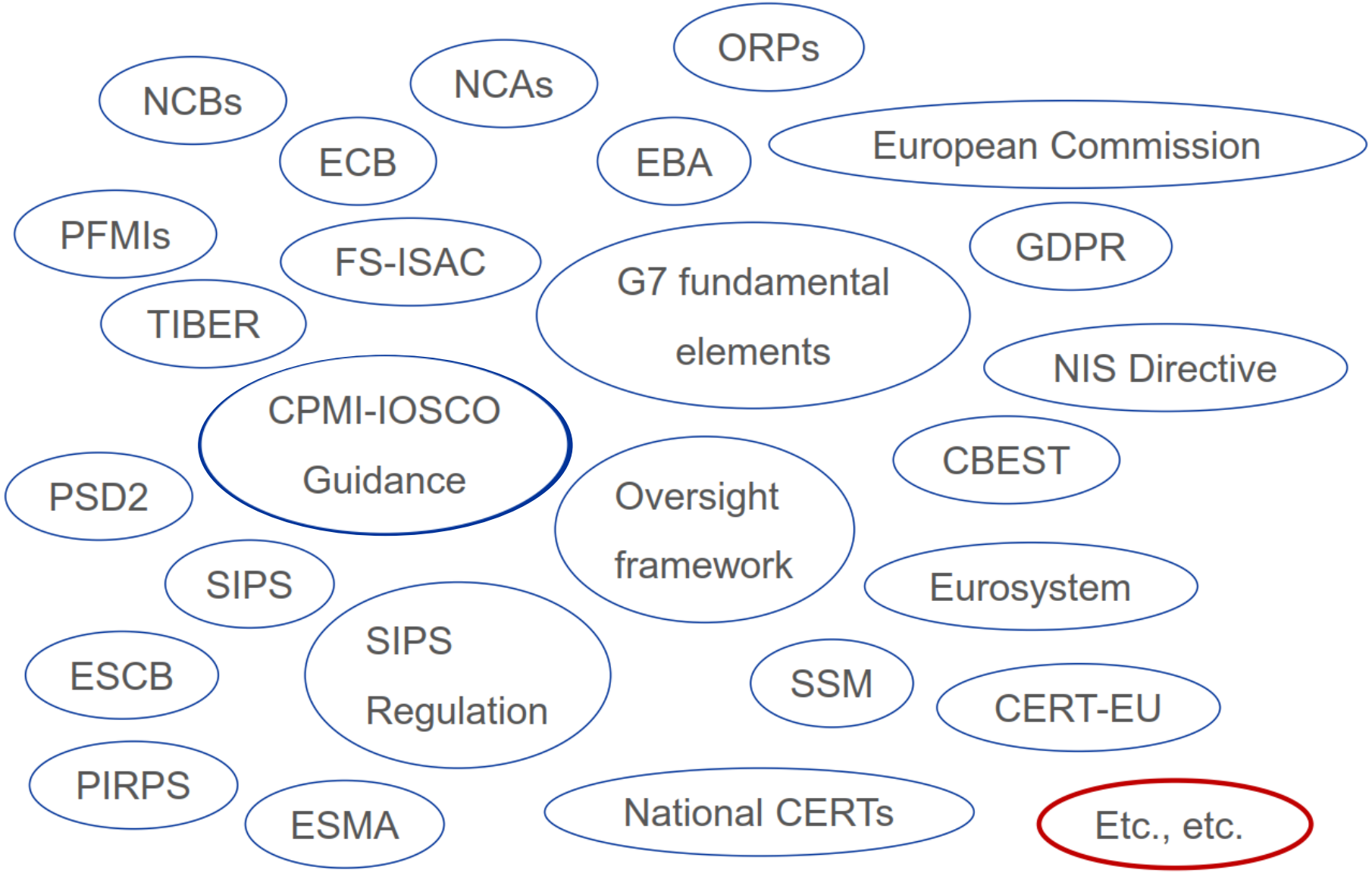
CARBANAK


How the Carbanak cybergang stole $1bn
A targeted attack on a bank
1. Infection
Carbanak backdoor sent as an attachment
Bank employee
Emails with exploits
Credentials stolen
100s of machines infected in search of the admin PC
2. Harvesting Intelligence
Intercepting the clerks' screens
Hacker
Cash transfer systems
Admin
Rec
3. Mimicking the staff
How the money was stolen
Online-banking
Money was transferred to fraudsters' accounts
E-payment systems
Money was transferred to banks in China and the US
Inflating account balances
The extra funds were pocketed via a fraudulent transaction
Controlling ATMs
Orders to dispense cash at a pre-determined time

Developments in regulation

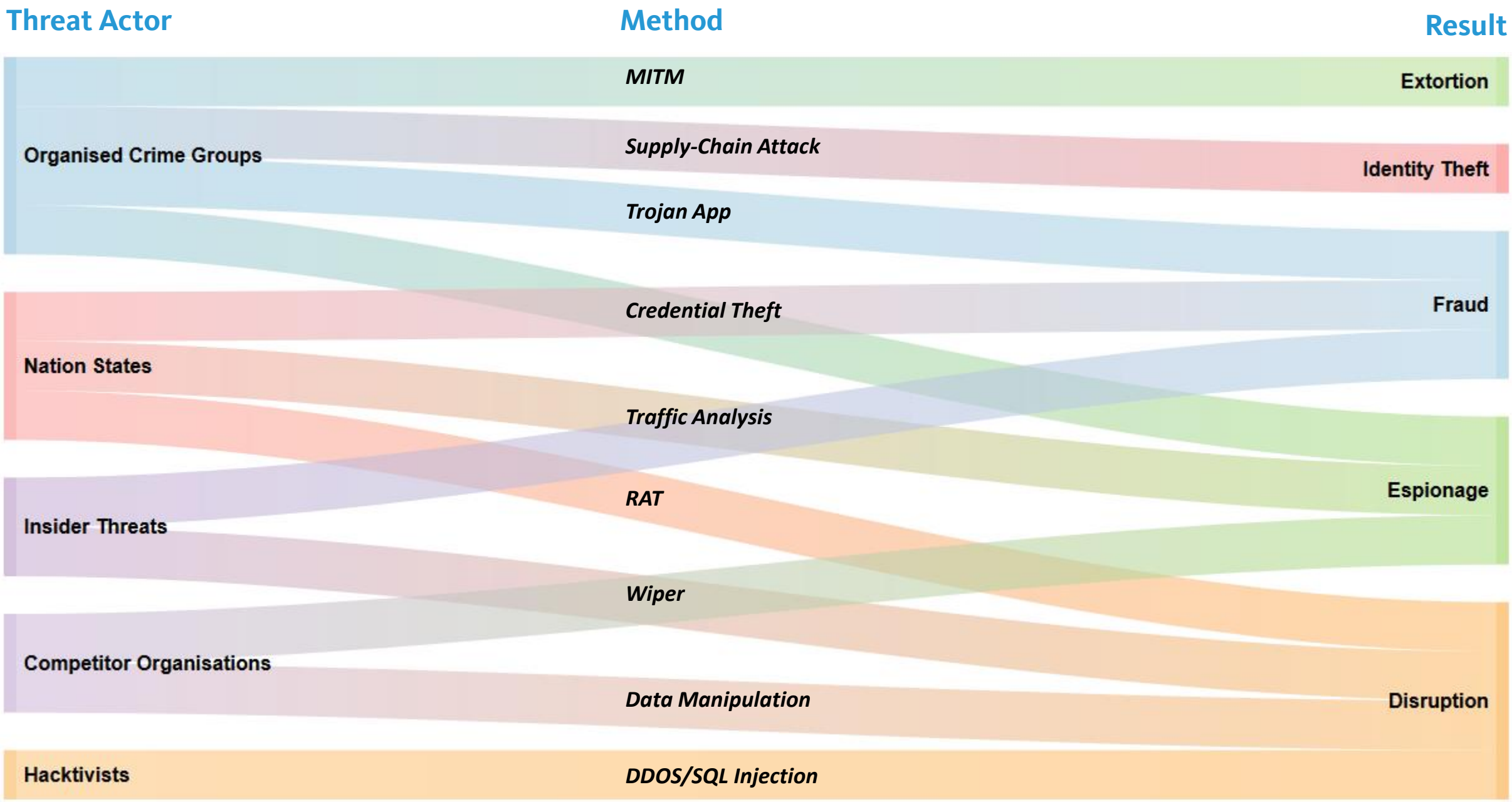
Blame the victim?

Legislation, Guidance, authorities and initiatives....

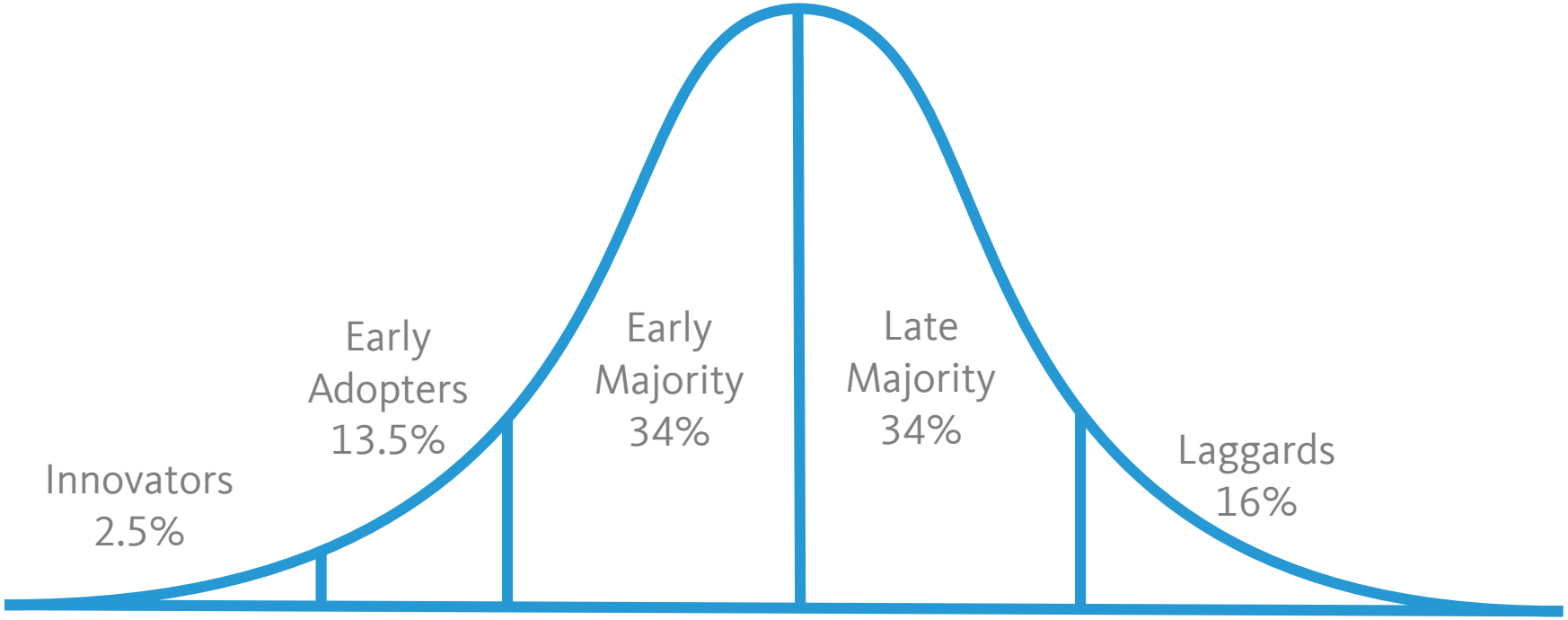


How open is open banking in terms of security?

Exposure vs. exploitation


Threat Actor
Method
Result
Organised Crime Groups
Nation States
Insider Threats
Competitor Organisations
Hacktivists
MITM
Supply-Chain Attack
Trojan App
Credential Theft
Traffic Analysis
RAT
Wiper
Data Manipulation
DDOS/SQL Injection
Extortion
Identity Theft
Fraud
Espionage
Disruption

Adoption Rate



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

Scenarios and signposts

Extortion

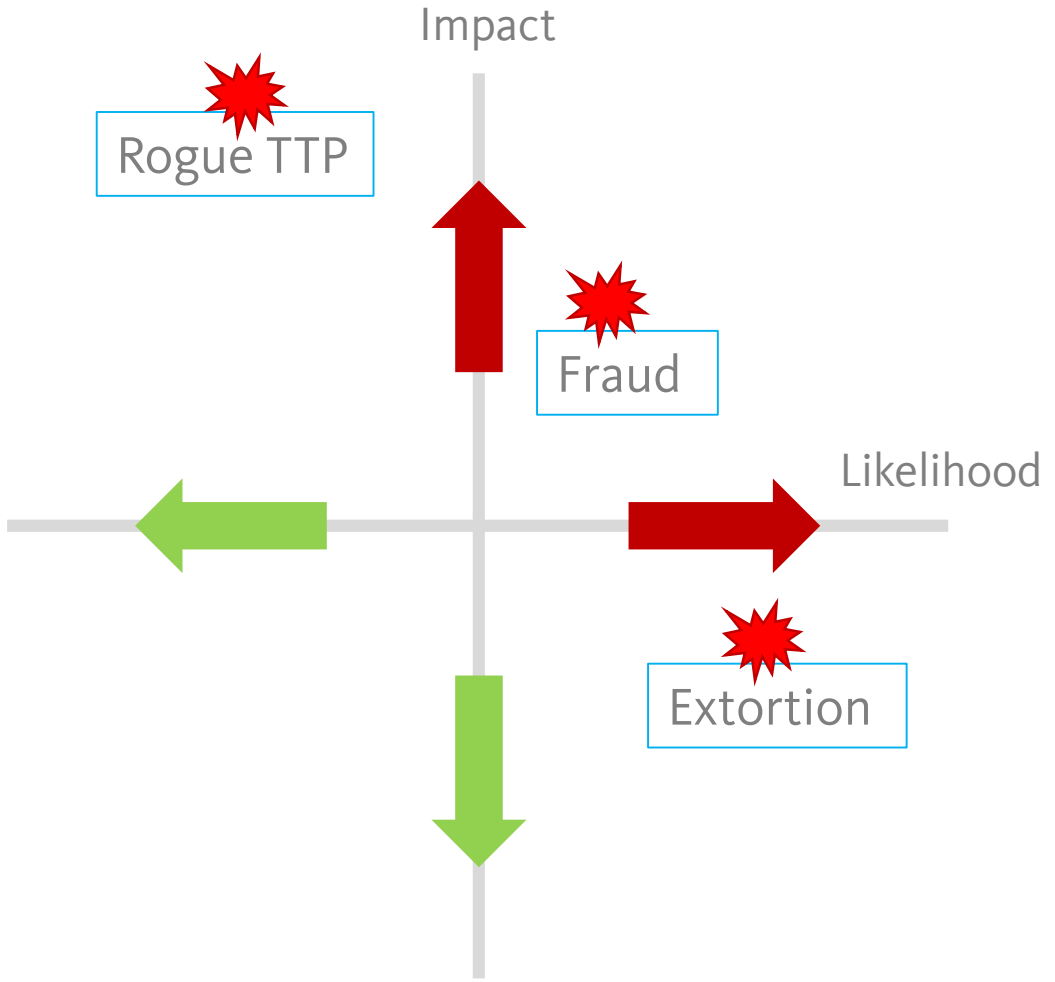
GDPR fine

Commodity Fraud

Scalable vulnerability

Rogue TPP spyware

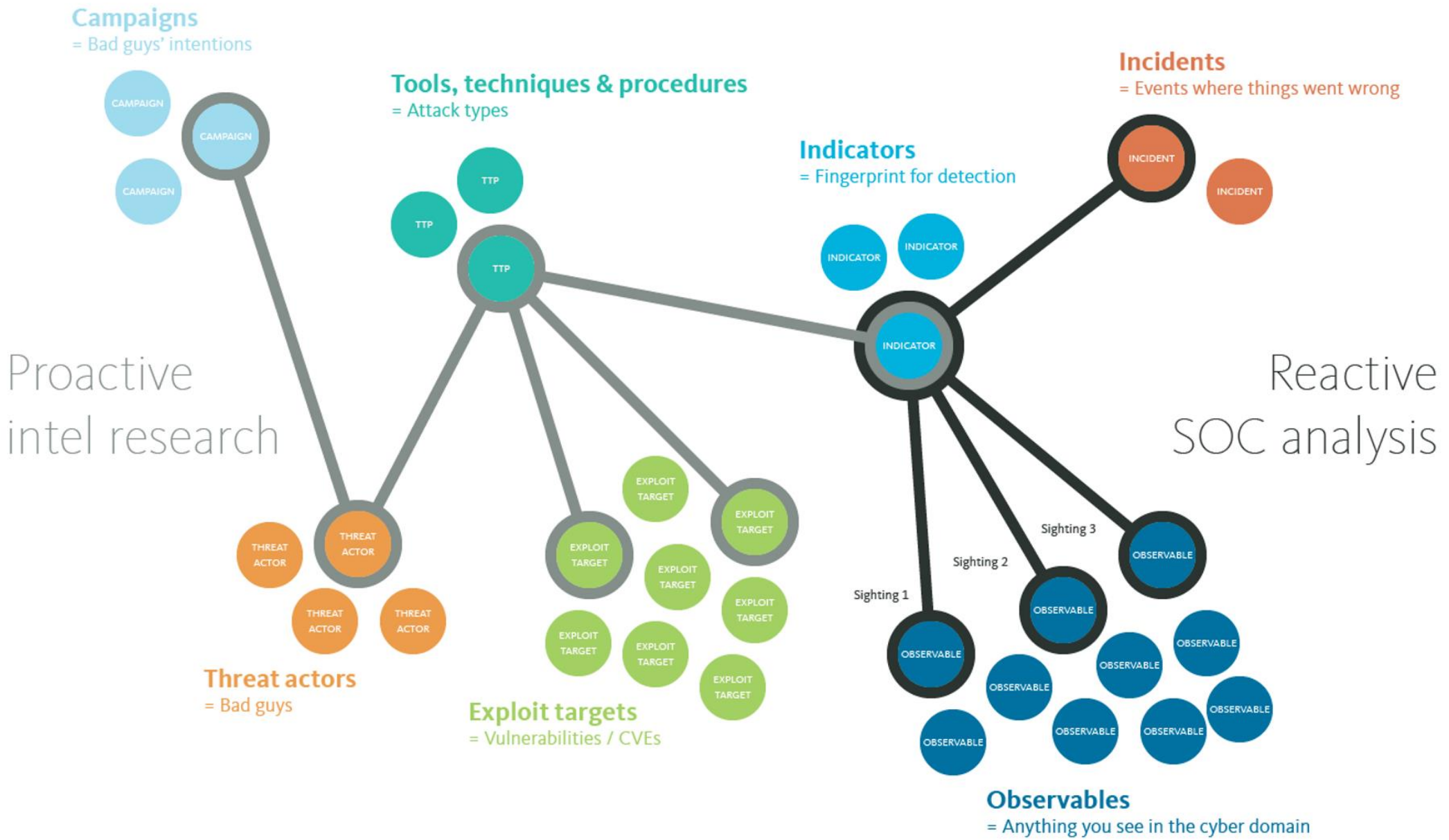
Business model without ROI



Countering the adversary

Where they reside

Intelligence driven security



REAL-TIME RESPONSE CAPABILITY

“Every soldier a sensor”

What you can do

InTELL
BY FOX IT

Q & A