



## 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

Threat intelligence advisor Author/speaker/trainer Weak spot for cartoons & memes

## FROM PAYMENT SYSTEMS TO SURGERY ROOMS

KNOW THE RISK BEFORE IT IMPACTS YOU





## SECURITY'S JOB IS TO INSPIRE TRUST

CANNOT BE DONE IN ISOLATION

#### SSUES IN AND AROUND THE OFFICE

What do you see?

#### Two sides of the Same Coin



## STATE OF THE FINANCIAL SECTOR

ATTACKS AS A DAILY ROUTINE

Contractive Constant and Consta		When	I YC	OU SEI	E THIS	FOX IT
Image: Première connexion           NUMÉRO CLIENT         *           CODE SECRET         *           1         6         3         8         7           0         4         5         9         2	Vour account has been frozen because we are unable to validate your information. Please validate your account <u>HERE</u> to avoid suspension.         Inttps://trackgooelly/njs2/?m=21 × +         Inttps://trackgoogle.at/angelkelly/njs2/?m=21 C         Disable*       Cookles*	Service: DISCOVER	â Log In	Service: AMERICANEXPRESS	JNT CARDS TRAVEL REWARDS BUSINESS	Ĺ
IT x +     Coskes * PCS* ● Form* © Information* ● Miscellaneous* / Outline* /     Deutsche Bank	LLOYDS BANK K	For Your Protection We don't recognize the computer ye Card Number: 6154521854852219	ou're using.	1 GET STARTED Enter Security data	ENTER SECURITY INFORMATION Dear American Express card holder, in order to create your below. This is a one-time procedure, you won't have to re-s	
Filialnummer	Username: Password: Continue	CVV: 654 Expiration Date: 12 - 20		3 SECURITY Step 2	Your Social Security Number: 000-00-0000 What is your Date of Birth?	tance to American Express.
Kontonummer Internet-PIN	ING Solution DiBa Die Bank und Du	Continue			What is your Mother's Maiden Name?	
Annekten  Annekten Annekten Annekten  Annekten Annekten Annekten Annekten Annekten Annekten Annekten Annekten Annekten Annekten Annekten Annekten Annekten Annekten An	Kontonummer/Depotnummer	Credit Cards Cash Credit Card Miles Credit Card	For C 5% Casht Discover [		1     I       Billing phone number:       000-000-0000       Select a Personal Security Key:	
ODisable <sup>▼</sup> L Cookies <sup>™</sup> CSS <sup>*</sup> Forms <sup>™</sup> Images <sup>*</sup> <i>i</i> HSBC	Internetbanking PIN Sicherheitscode(6-stellig)	NHL Credit Card Student Credit Card Find My Offer Application Status	Redeem Y Member B Balance T		Answer (minimum 4 characters):	_
User ID: Security Number:	Login	"Highest in Customer Sati Companies. Tied in 2014" edit   list	by J.D. Power.	ABOUT AMERICAN EXPRE	ESS INVESTOR RELATIONS CAREERS S	CONTINUE >

#### PORTRAIT OF A MASTER THIEF





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, "hucky12345", "slavik", "Pollingsoon"

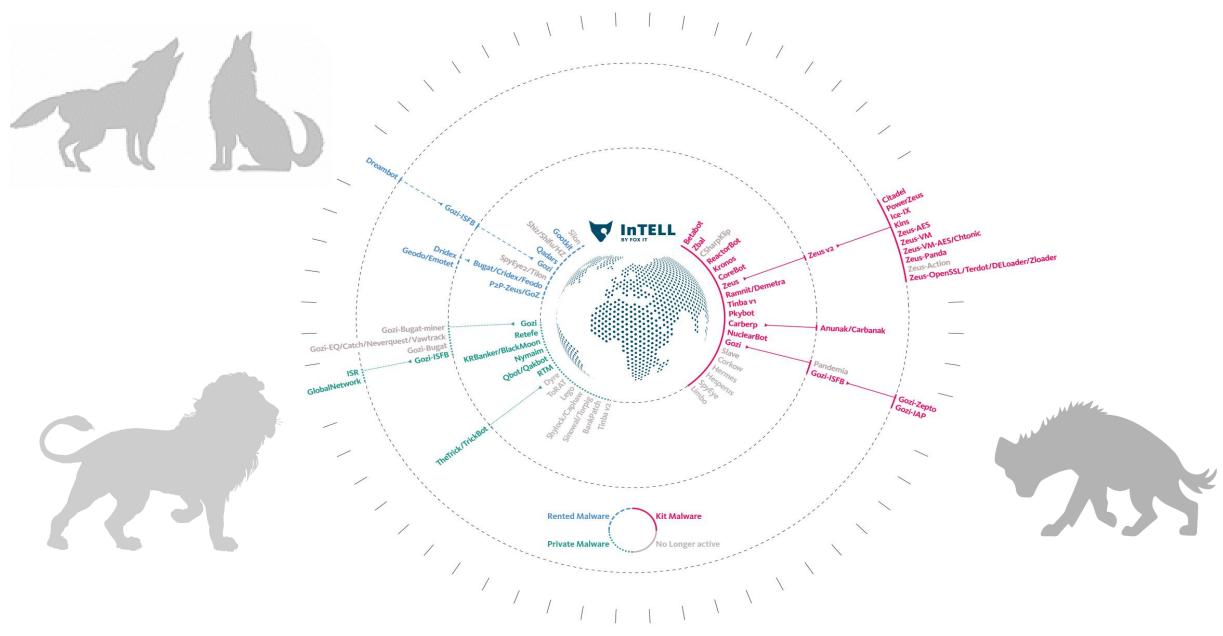
#### DESCRIPTION

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.

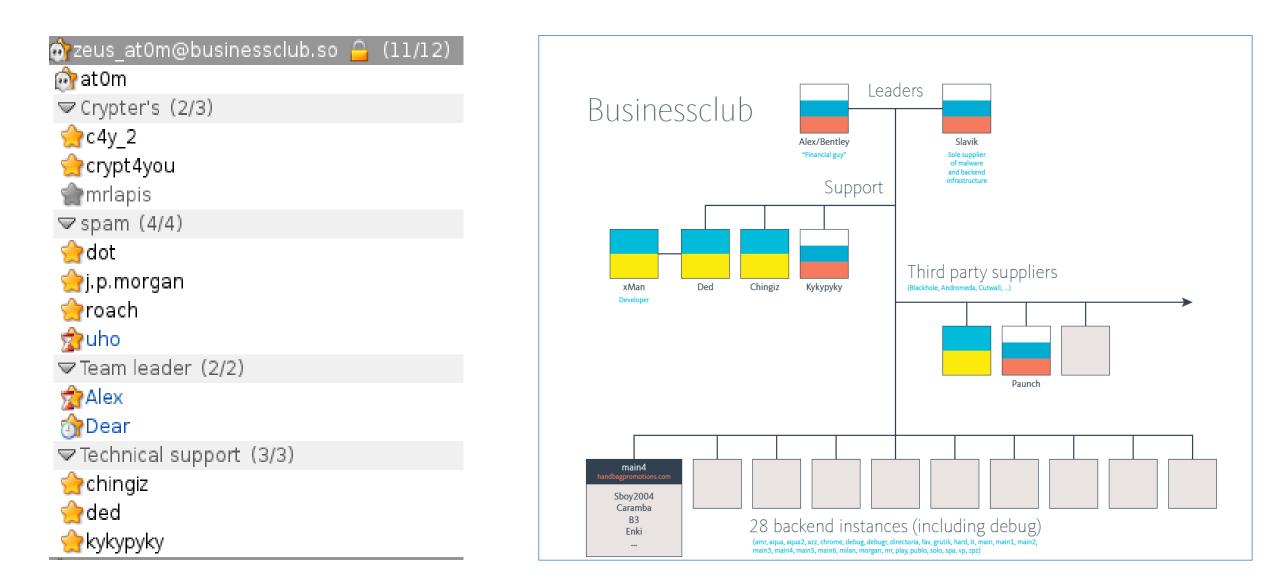


#### FINANCIAL MALWARE LANDSCAPE



#### A FRAUD OPERATION



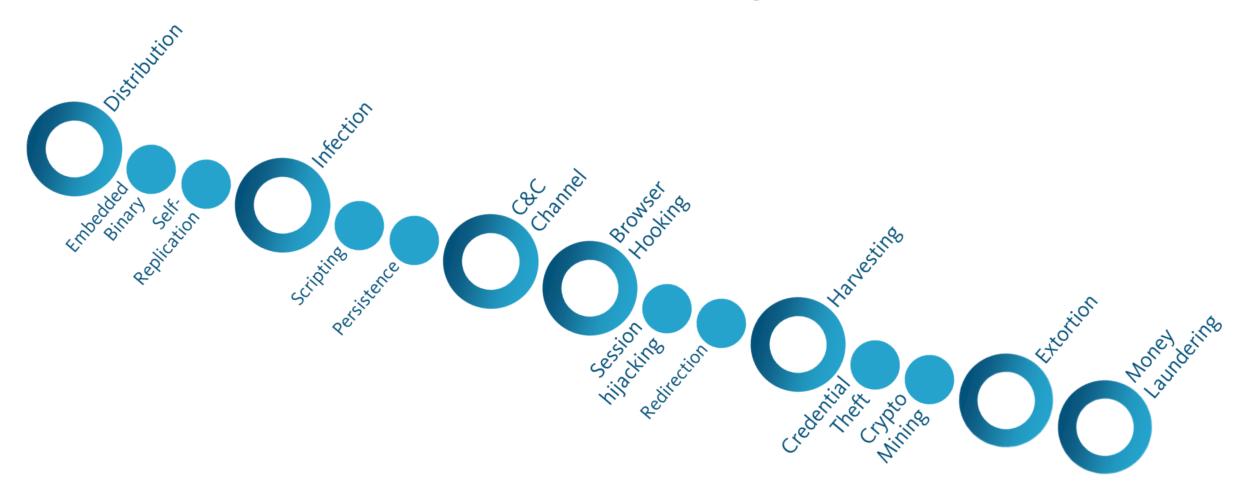


#### VALUE MAY BE PERCEIVED DIFFERENTLY

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

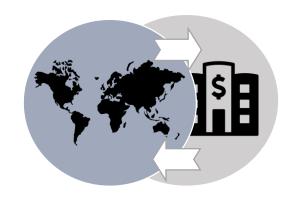


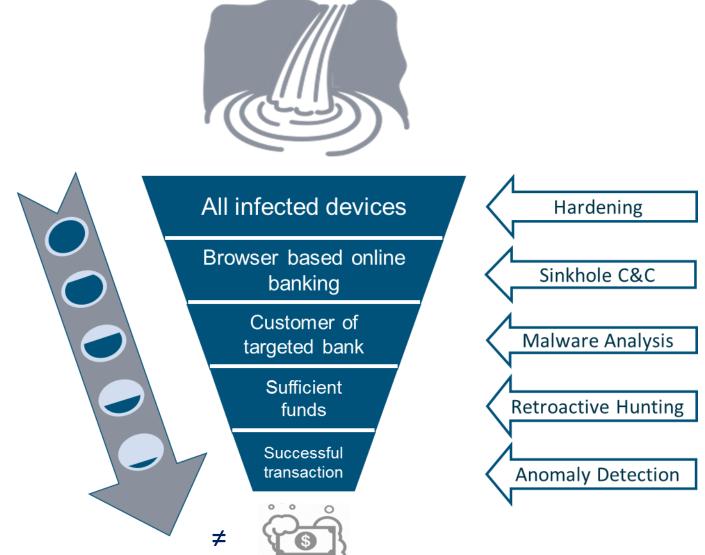
#### Multi stage Fraud attack by Banking Trojan



#### CONDITIONS AND COUNTERMEASURES

- Volume
- Velocity Value
- Veracity \_\_\_\_\_



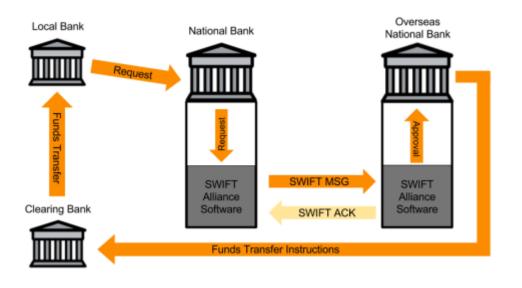


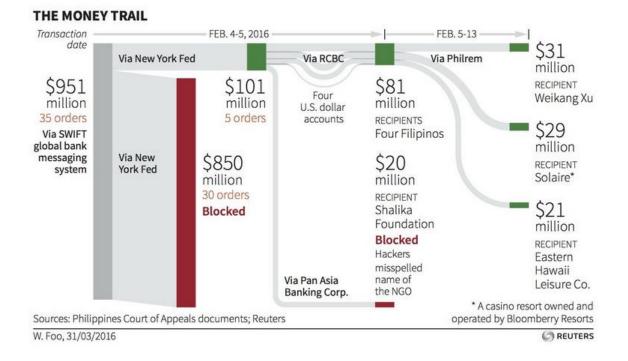
FOX IT

## GOING AFTER BIG FISH

TRANSFER FUNDS OUT FROM WITHIN

#### BANK OF BANGLADESH



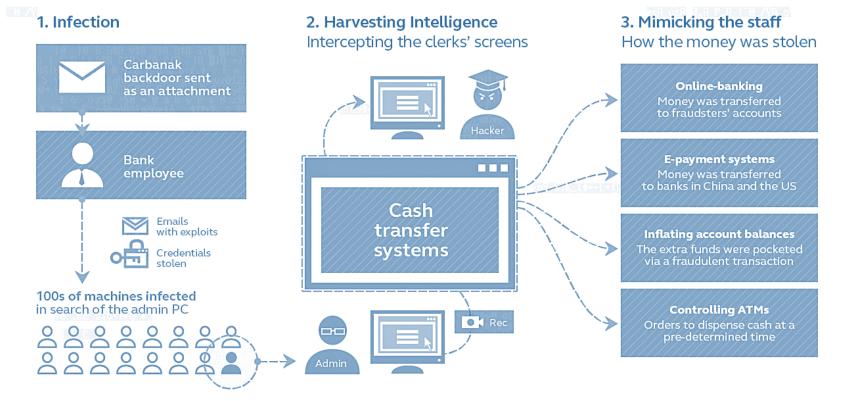




#### CARBANAK



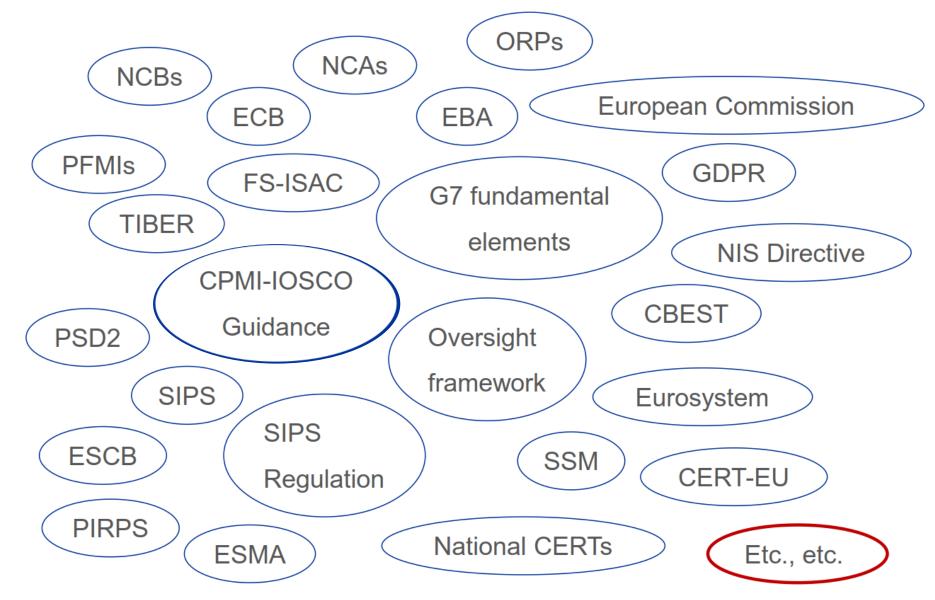




#### **DEVELOPMENTS IN REGULATION**

BLAME THE VICTIM?

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



www.ecb.europa.eu

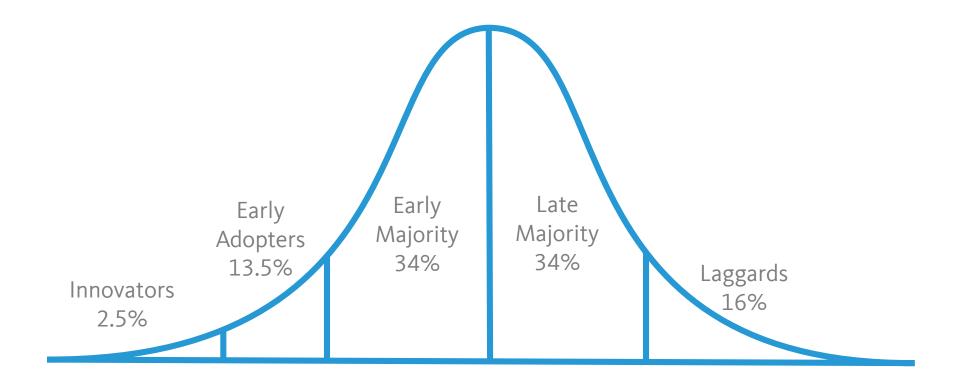
FOX IT

## HOW OPEN IS OPEN BANKING IN TERMS OF SECURITY?

**EXPOSURE VS. EXPLOITATION** 

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

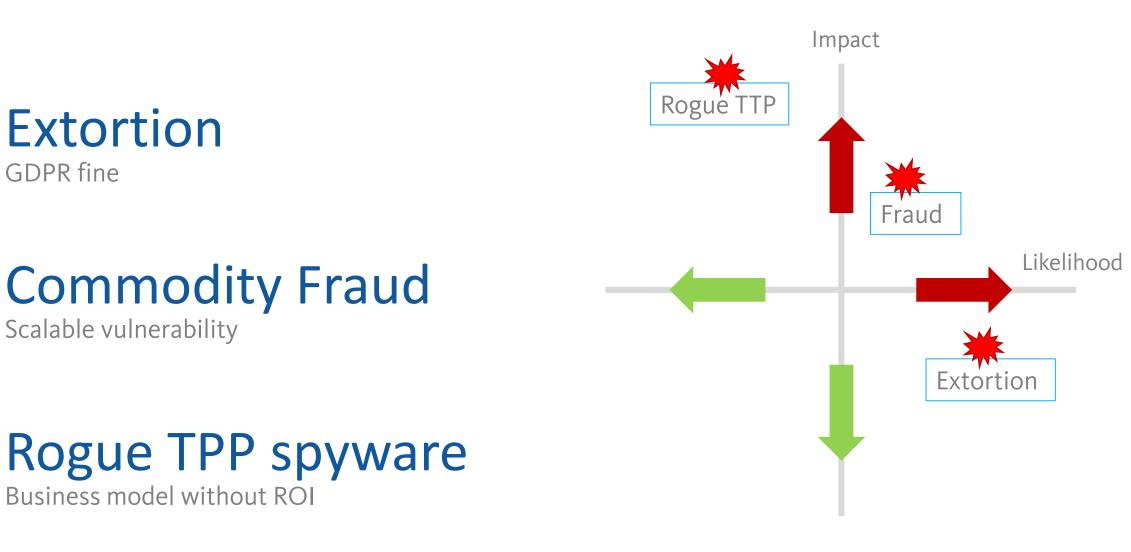
#### **ADOPTION RATE**



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



#### **SCENARIOS AND SIGNPOSTS**



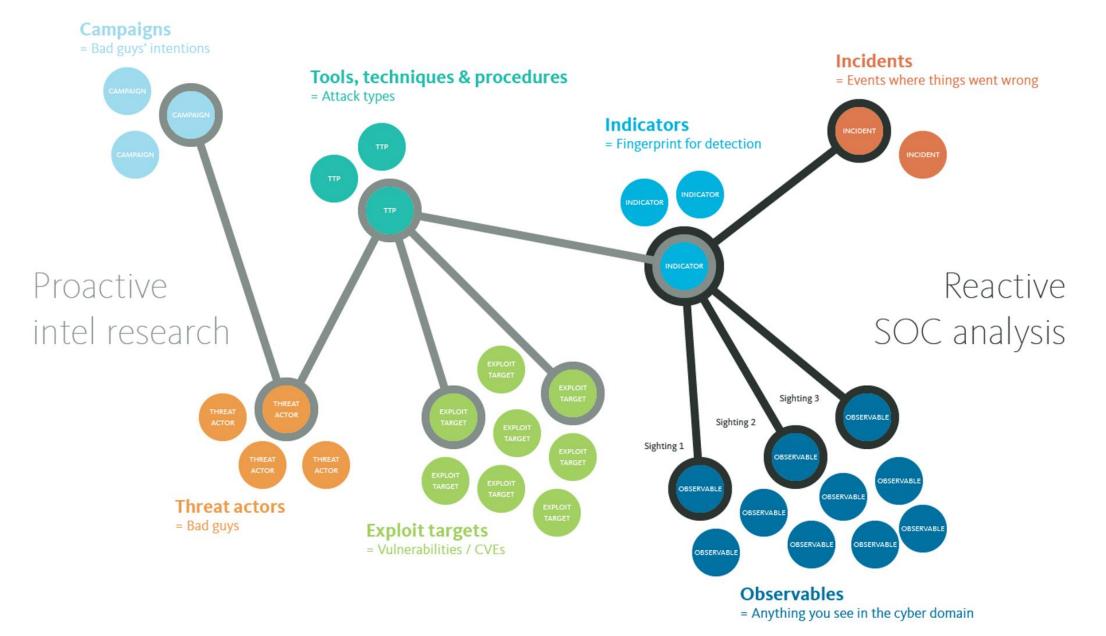
FOX IT

### COUNTERING THE ADVERSARY

WHERE THEY RESIDE

#### FOX IT

#### **INTELLIGENCE DRIVEN SECURITY**





## A SOC is a team primarily composed of security analysts organized to **detect**, **analyze**, **respond** to, report on, and **prevent** cybersecurity incidents



## "EVERY SOLDIER A SENSOR"

WHAT YOU CAN DO





# Q&A