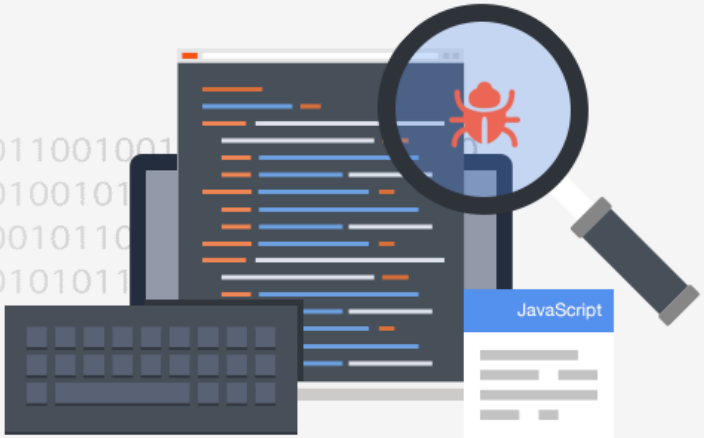
MINDED SECURITY
The Software Security Company

Which Technologies Financial Institutions can adopt for mitigating the risk of malware banking attacks



Matteo Meucci, CEO Minded Security

Agenda

- Introduction to Banking Malware Attacks
- Technologies for mitigating the risk
- Threat modeling approach to manage the attacks complexity

Who am I?

- Matteo Meucci
  - Working on Application Security from 2002
  - OWASP Italy Founder and President from 2005
  - OWASP Testing Guide lead from 2006
  - Founder and CEO at Minded Security the Software Security Company from 2007

1. INTRODUCTION TO BANKING MALWARE ATTACKS

Malware Banking Attacks In Measured Data

1.7 Mil
phished bank users worldwide in 1 month
(Ref Kaspersky)

11 % of overall population victim of phishing
(Ref Verizon)

4381 users attacked by malware in 1 month in U.K.
(Ref Kaspersky)

5% of bank users are infected by some malware (Ref Minded Security)

0.4 % of users of high risk of account takeover
(Ref Minded Security)

0.1 % of are users of critical risk of account takeover
(Ref Minded Security)

Malware Banking & Cyber Threat Agents

Evolution of Cyber-Threat Actors (1995-present)

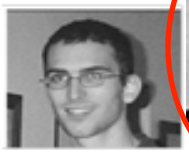
Threat Actors: Occasional Intruders
Motives: Testing and probing Systems and channels, computer disruptions, hacking
Attacks: Exploiting absence of security controls, sniffing data traffic

Threat Actors: Script Kiddies,
Motives: Notoriety and fame, world-wide notoriety spread virus and worms, computer disruptions, profit from botnet- spamming
Attacks: Viruses, Worms, DoS, Buffer Overflow Exploits, Spamming, Sniffing Network Traffic, Phishing emails with viruses

Threat Actors: Fraudsters, cyber-gangs
Motives: Identity Theft, Online and Credit/Debit Card Fraud
Attacks: SQLi, Sniffing Wireless Traffic, Session Hijacking, Phishing, Vishing, Drive by Download, Account take-over, MitM, MiTB, counterfeiting, banking malware, Trojans

Threat Actors: Hacktivists, cyber criminals, country sponsored spies, cyber-warfare actors, fraudsters,
Motives: Political, Stealing Company Secrets, Fraud, Reputation Damage
Attacks: DDoS, APTs, Account Take Over, MitM, MitB,Session Hijacking, Phishing, Web Injections, Banking Malware, POS Malware

Threat Actor (TTP) Tools, Techniques & Procedures Sophistication



Lloyd-Omega (1996)

Levin - Citi (1998)

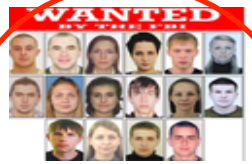
De Guzman- ILOVEYOU virus (2000)

Mafia Boy- DDoS Yahoo, Ebay, CNN (2001)

Ancheta Spam -Botnets (2004)

Jaschan- Sasser Worm (2004)

Gonzales Gang, TJ-Maxx, Heartland Payment Systems, Hannaford Bros (2007)



Bank Trojan Zeus- Russian Cyber-Gang (2010)

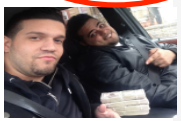
LulzSec DDoS & Sony (2011)

Anonymous, DDoS & Hacking (2011)

Israel-Palestine, DDoS (2012)

AOCE DDoS US Banks (2012)

Taraspov Target POS Malware (2013)

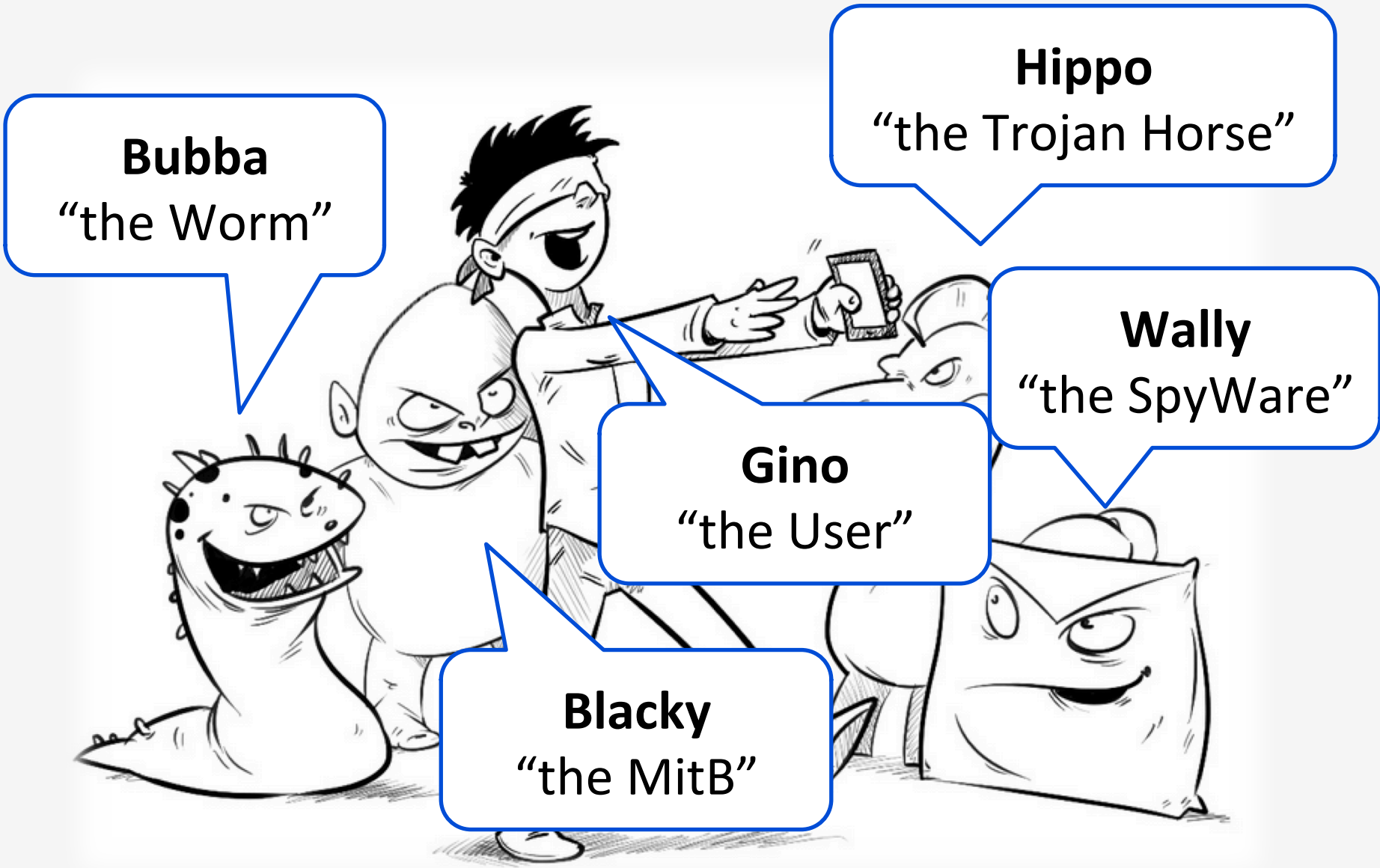


Rodriguez & Yeje $ 45 mil, Rakbank ATM heist (2013)

1995 2000 2005 2010 2015

MINDED SECURITY
The Software Security Company

1.1 THE INFECTION



MINDED SECURITY
The Software Security Company

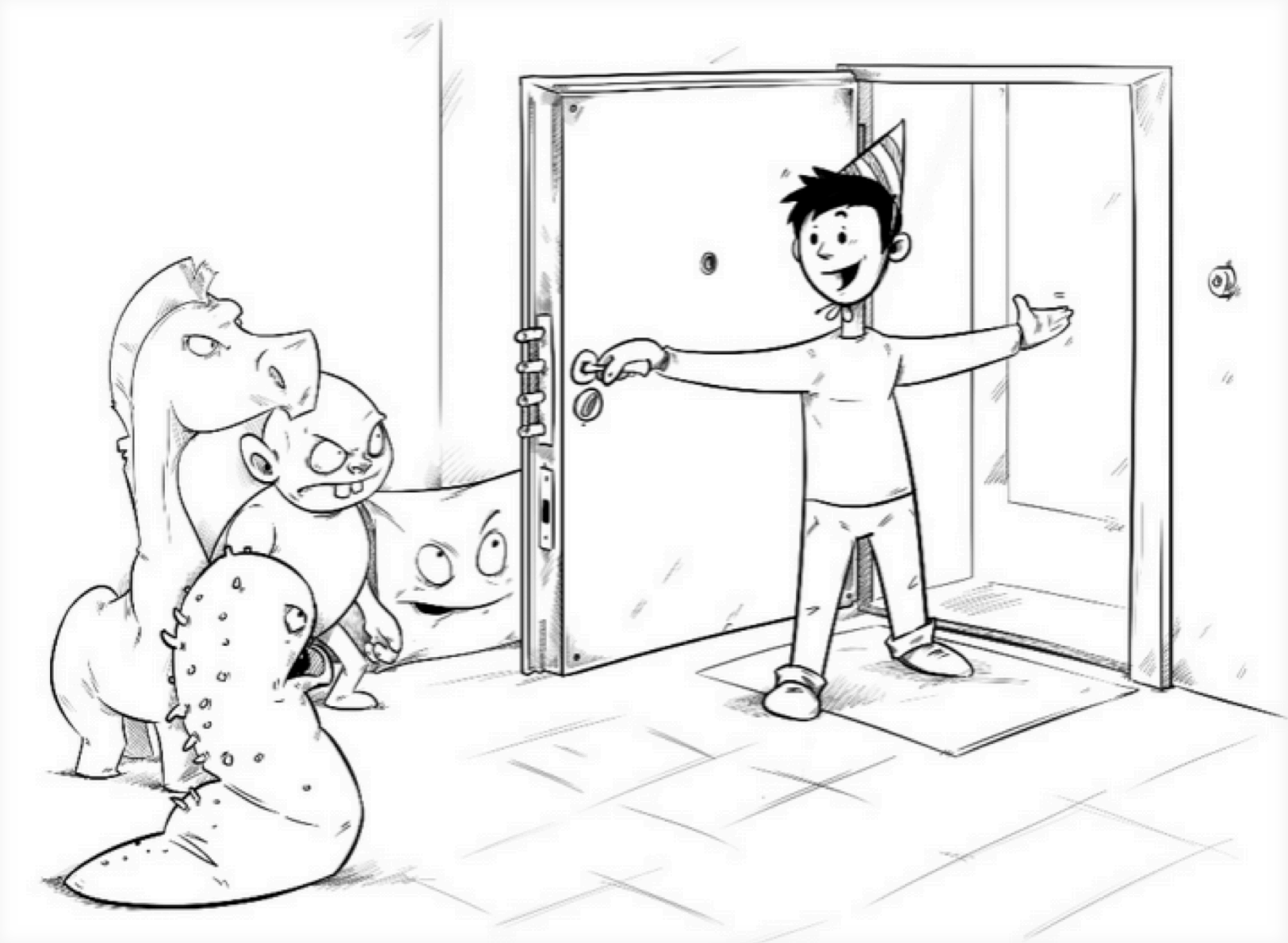
Courtesy of www.securelist.com

Common Malware Features

- Malware is executed on user devices **WITHOUT EXPLICIT** user consent
- They can keep control of the device
- They can halt or damage the user device
- They can alter the user browsing experience
- They can harvest user-data and device information
- They can modify the information on the device

Headline Breaking News

- 23% OF RECIPIENTS NOW OPEN PHISHING MESSAGES AND **11% CLICK ON ATTACHMENTS.** (Verizon data-breach-investigation-report-2015)
- **Users open email Attachments, it's proven!**



MINDED SECURITY
The Software Security Company

Courtesy of www.securelist.com

Real example

Infection Campaigns

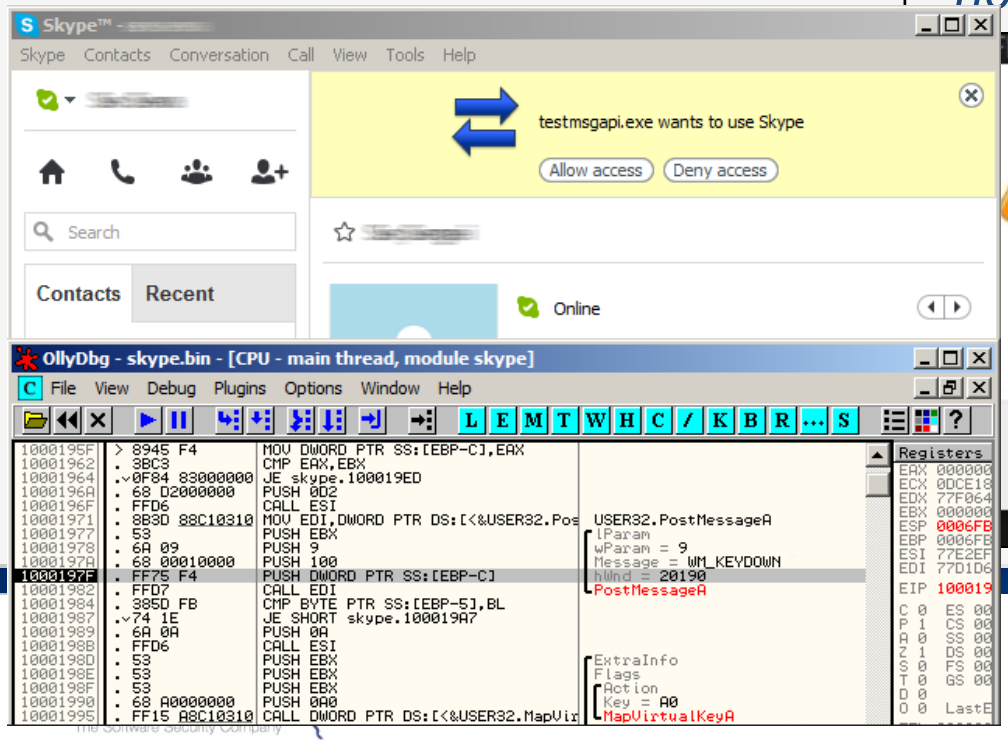
- Email Messages
- Social Network Chats
- Social Engineering
- Infected Websites
- Malvertising

Subject: Invoice 0518900

Dear Customer

Invoice 0518900 can be downloaded at the following address

http://evildomain.Filename.zip?nconto=email



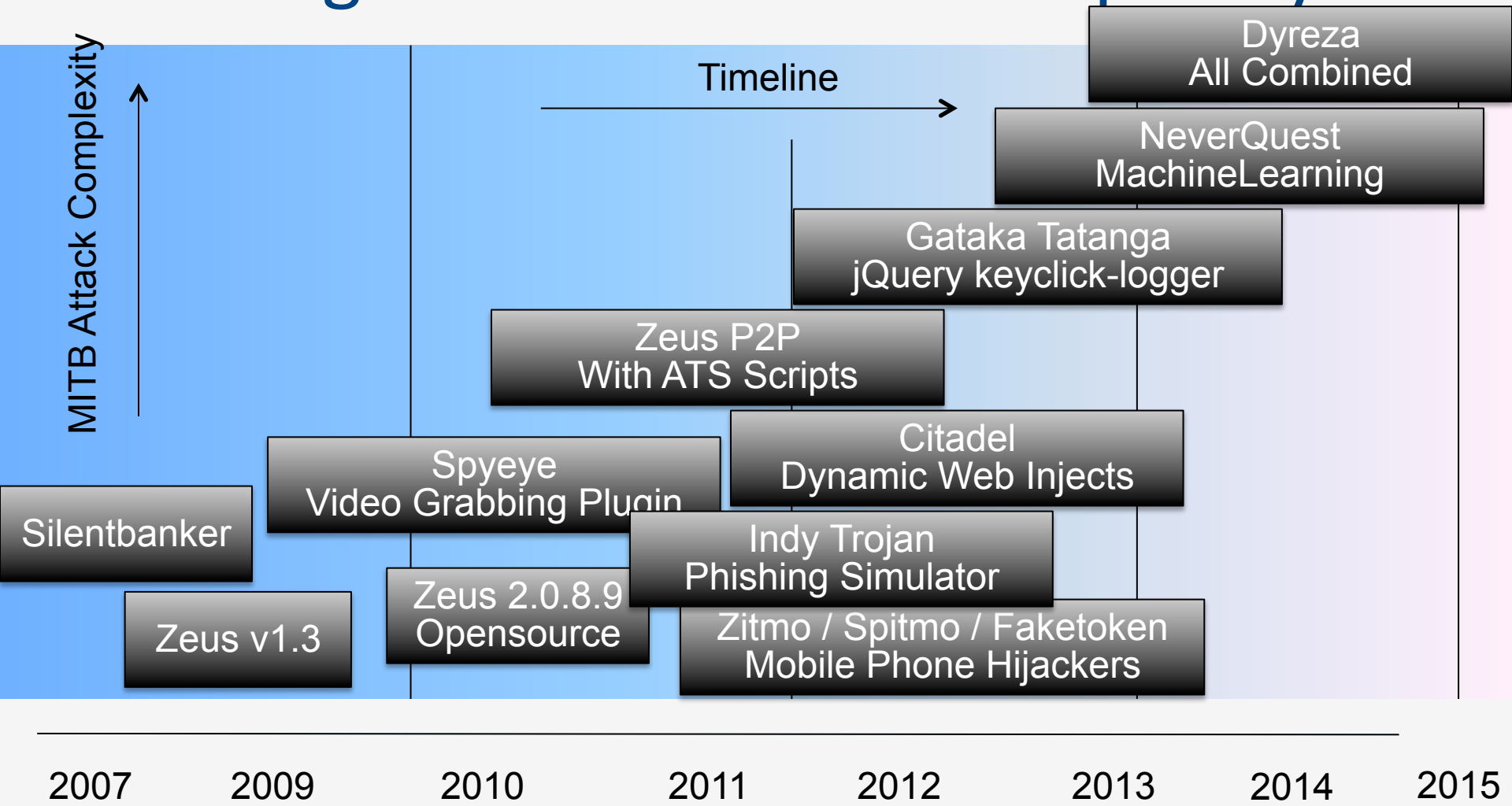
1.2 THE ATTACK

Attacks

- Attacks against bank website are performed through **Man in The Browser**

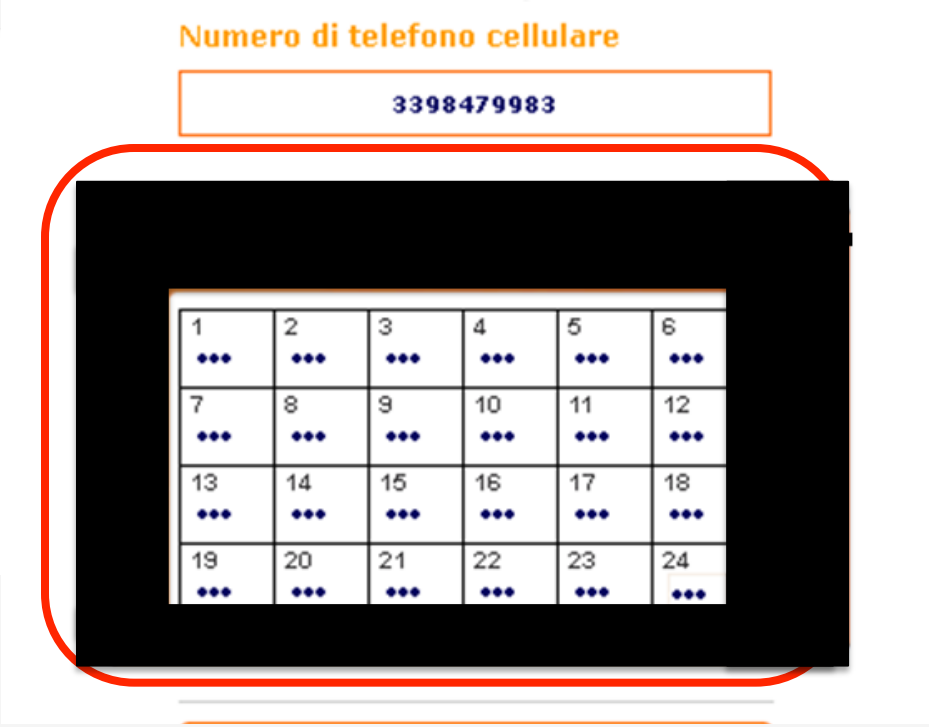
- The Trojan is attached to the browser process and can alter http request and responses
  - Web Injects
  - Request Hijacking
  - Credential Stealing (Keylogging / Screenshotting)
  - OTP Theft → secondary mobile infection

Banking Malware Attack Complexity



Web Fraud *Social Engineering*

- Malware Asks for User disposal credentials
- Attack is customized upon bank authentication process
- Custom Webinjects are often made by professional developers



Banking Malware *Software Solution*

Source: http://cyb3rsleuth.blogspot.co.uk

Citadel 1.3.3 (Spring Edition)

Dropzone (where data is stored)

- Banking Malware Infections need to be controlled remotely
- Bots usually implement a client-server model
- It's unusual that P2P features are used as data channel

Name

Parent Directory
existed_bots.txt
existed_bots_%2F..%2Faaa.txt
existed_bots_atime.it.txt
existed_bots_bancodinapoli.it.txt
existed_bots_bank_name.txt
existed_bots_bmedonline.it.txt
existed_bots_bpmbanking.it.txt
existed_bots_cariparma.it.txt
existed_bots_cartasi.it.txt
existed_bots_chebanca.it.txt
existed_bots_clarisbanca.it.txt
existed_bots_credem.it.txt
existed_bots_fineco.it.txt
existed_bots_gbw1.it.txt
existed_bots_gbw2.it.txt
existed_bots_gbw3.it.txt

Parent D
log_.htm
log_no_c

link=[redacted]
user=6546[redacted]
dob=1[redacted]_03_19[redacted]
fiscale=[redacted]
pin=97[redacted]
coords=
_1=737 _2=638 [redacted]
_7=374 _8=653 _9=387 10=645 11=183 12=651
[redacted] 17=287 18=364
19=159 20=746 21=159 22=476 23=[redacted] 24=

phone=33984[redacted]

Minded Security – A Real Citadel Custom Dropzone

2. TECHNOLOGIES TO MITIGATE WEB FRAUD RISKS

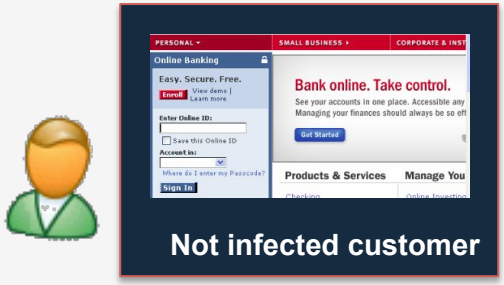
Antimalware Solutions

- Security Strategy should be **Layered**
  - More layers are more difficult to defeat
- Fraud detection should be **transparent to users and attacker**
  - Forcing user into executing some binary is a bad practice. Attackers could ask them to install "***a stronger ;;-))*** " security solution.
- The Solution Should be **Flexible**
  - Malware changes rapidly and the solution should change accordingly
- The Solution should be **modular**
  - Correlation of multiple anomaly detection methods can better detect unknown 0day threats.

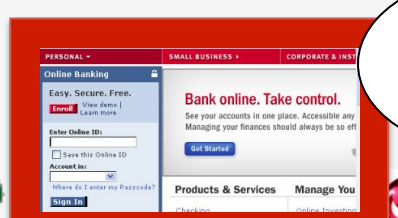
From a banking point of view: the scenario

On-line Banking Fraud Office needs tools to know in real time which users are infected and could be defrauded using the on-line banking service.

AMT Banking Malware Detector: the answer



Not infected customer

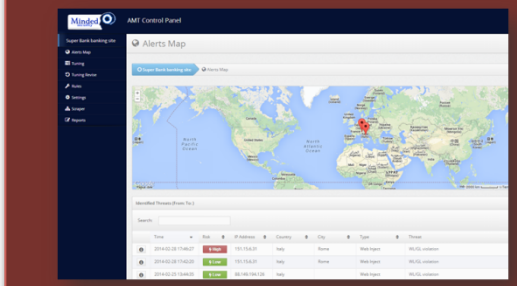


Infected customer

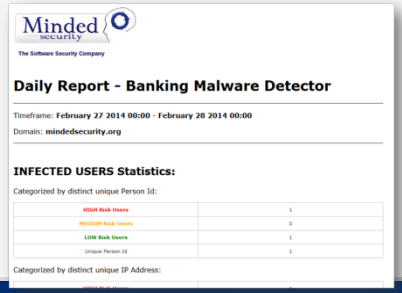
I will modify the IBAN and money data

I would like a technology to identify malware victims before they will be defrauded

On-line Banking



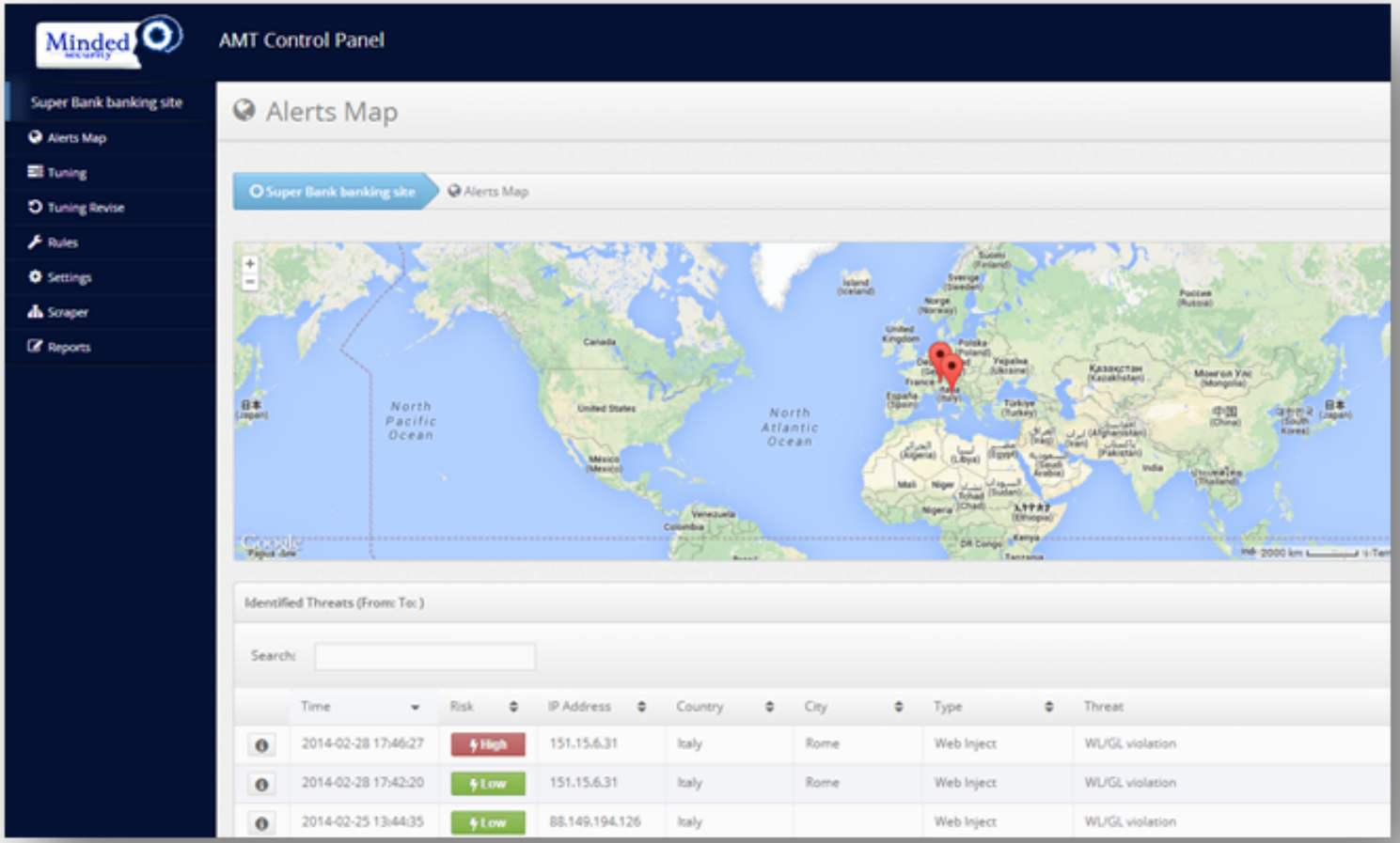
AMT Banking Malware Detector



MINDED SECURITY
The Software Security Company

The AMT – ANTI MALWARE TECHNOLOGY

Agentless and Lightweight, Banking Malware Detector

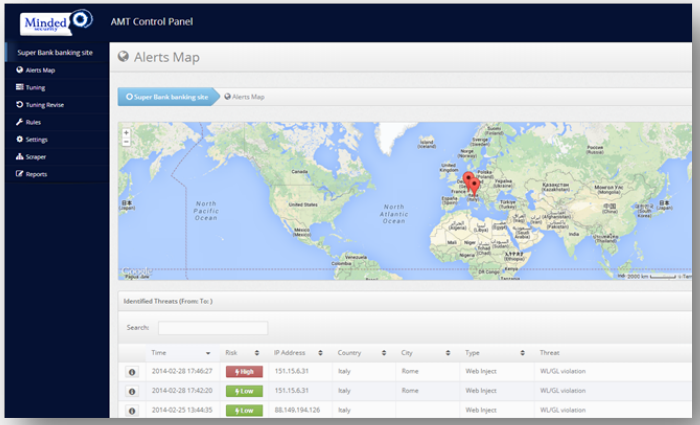


- **Infection alerts: infected users**
- **API for integration of information with customer fraud engine**

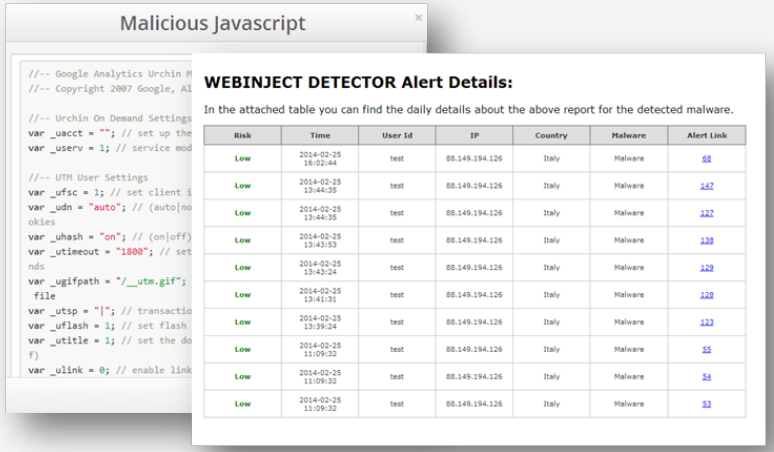
MINDED SECURITY
The Software Security Company

AMT Control Panel

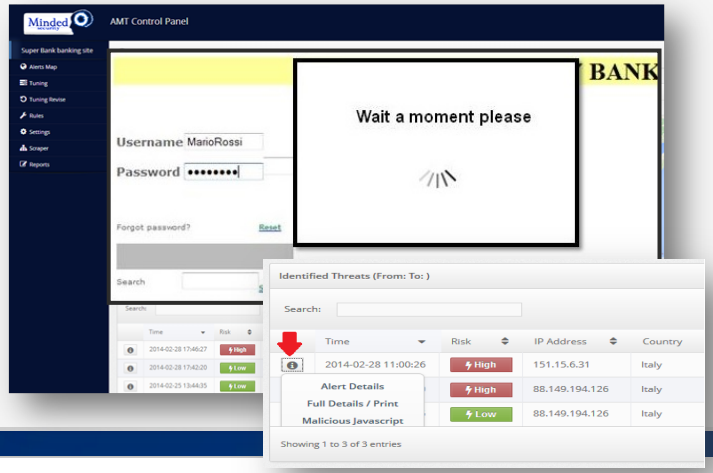
Real time control of user infected



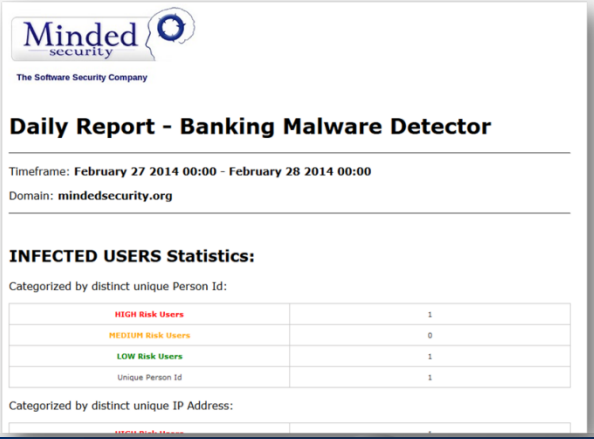
Managing of infected clients risk



Detailed attack information



Daily custom report



MINDED SECURITY
The Software Security Company

Is it Unbreakable?

- Is our technology unbreakable?

Absolutely NO!

- Dyreza bypassed many web fraud detection technology!

3. THREAT MODELING APPROACH TO MANAGE THE ATTACKS COMPLEXITY

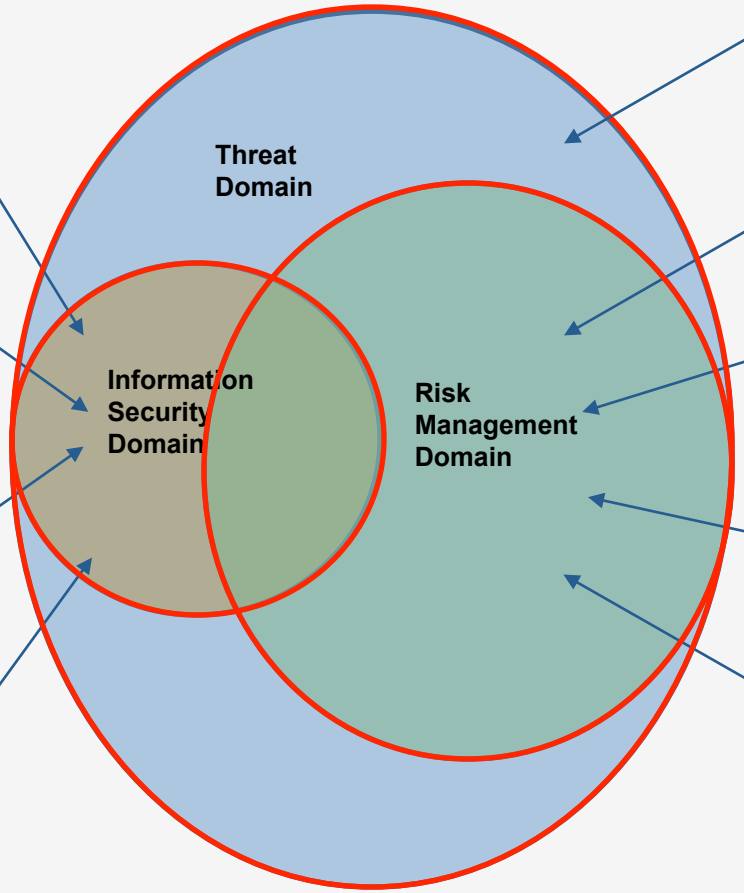
Malware Domains & Risk Assessment Activities

Compliance & Audits

Vulnerability Risk Management

Security Incident Response

Fraud Risk Management



Malware Threat Intelligence

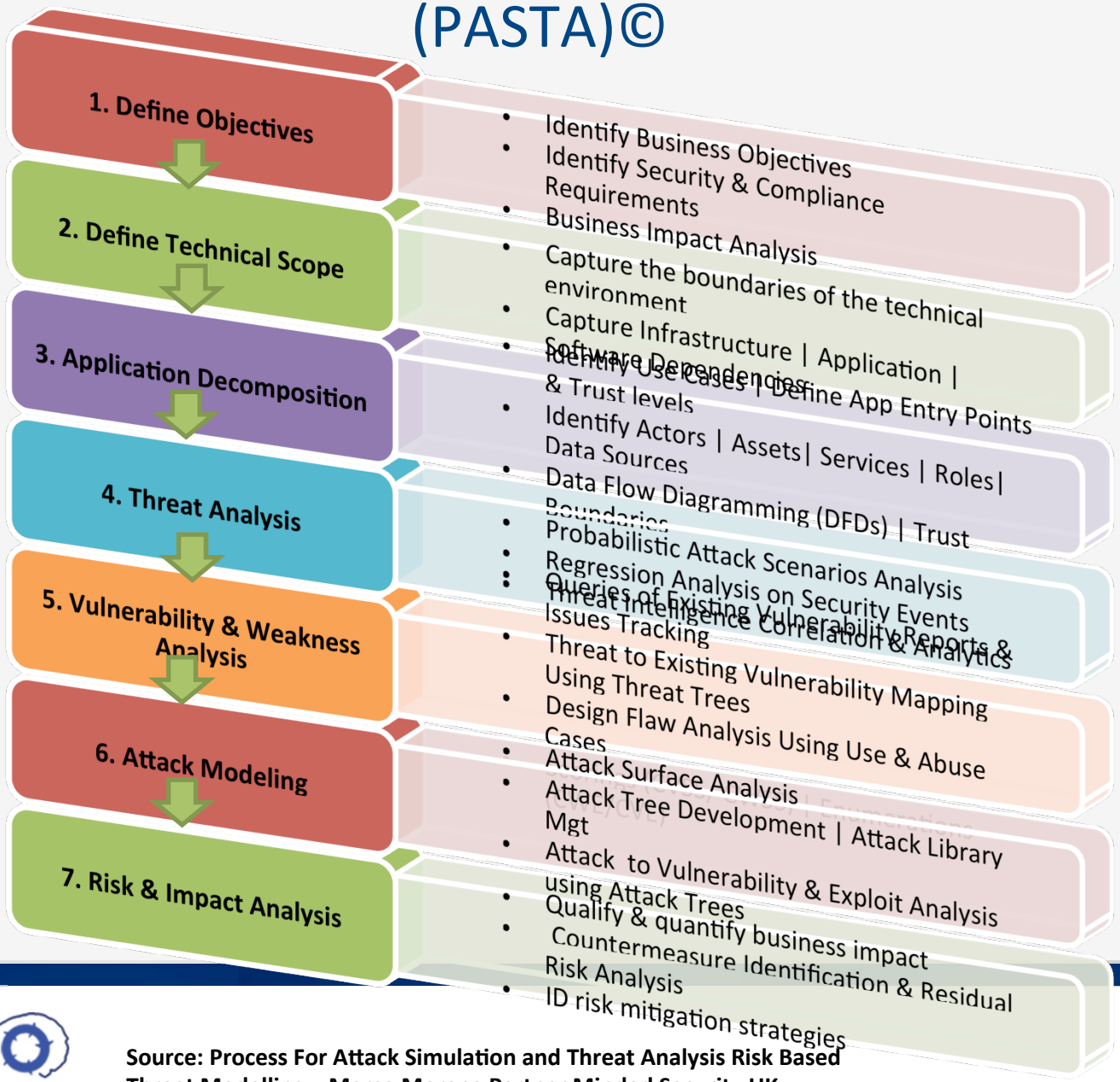
Malware Threat Analysis

Malware Attack Modeling

Malware Attack Simulation & Testing

Malware Risk Management

Process For Attack Simulation And Threat Analysis (PASTA)©



MINDED SECURITY
The Software Security Company

Source: Process For Attack Simulation and Threat Analysis Risk Based Threat Modelling – Marco Morana Partner Minded Security UK

Malware Banking Countermeasures: Requirements

1) Authentication engineered with a threat model of malware attacks such as MitB, MITM

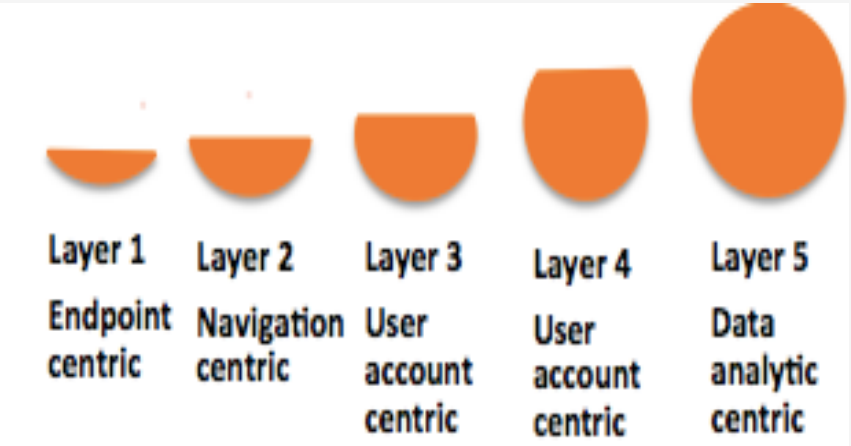
2) Malware web injection detection and automatic Money Transfers Detection

3) Agentless (e.g. no software to download) and scalable

4) Transparent to the user

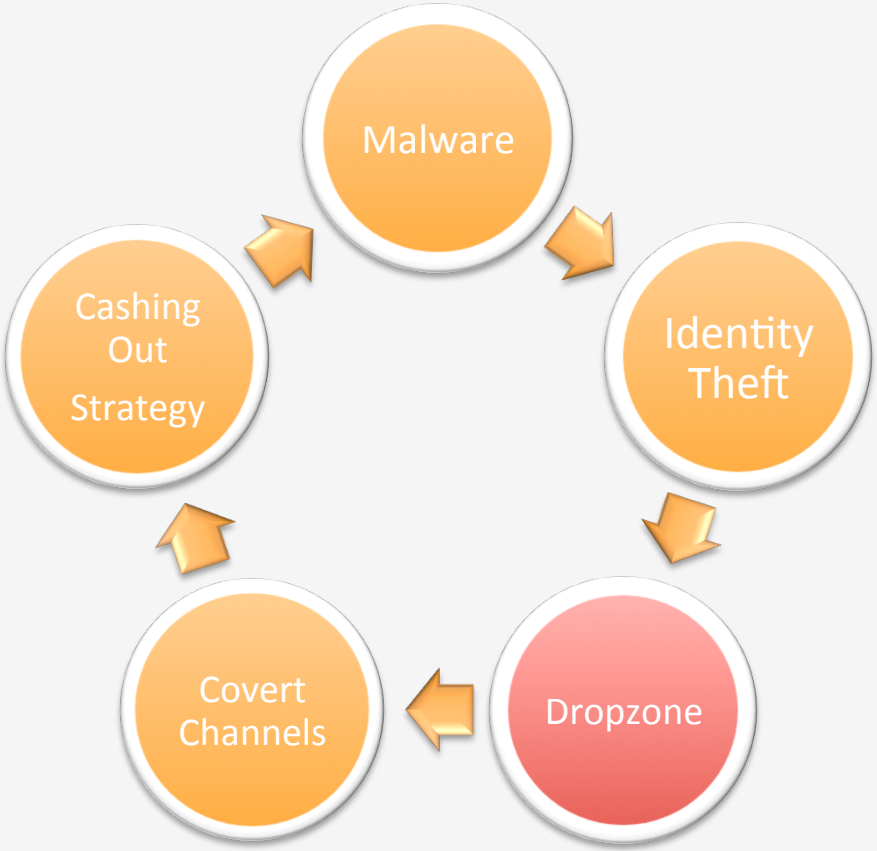
5) Integrated with fraud detection systems and SIEMs

6) Part of multi-layered defense



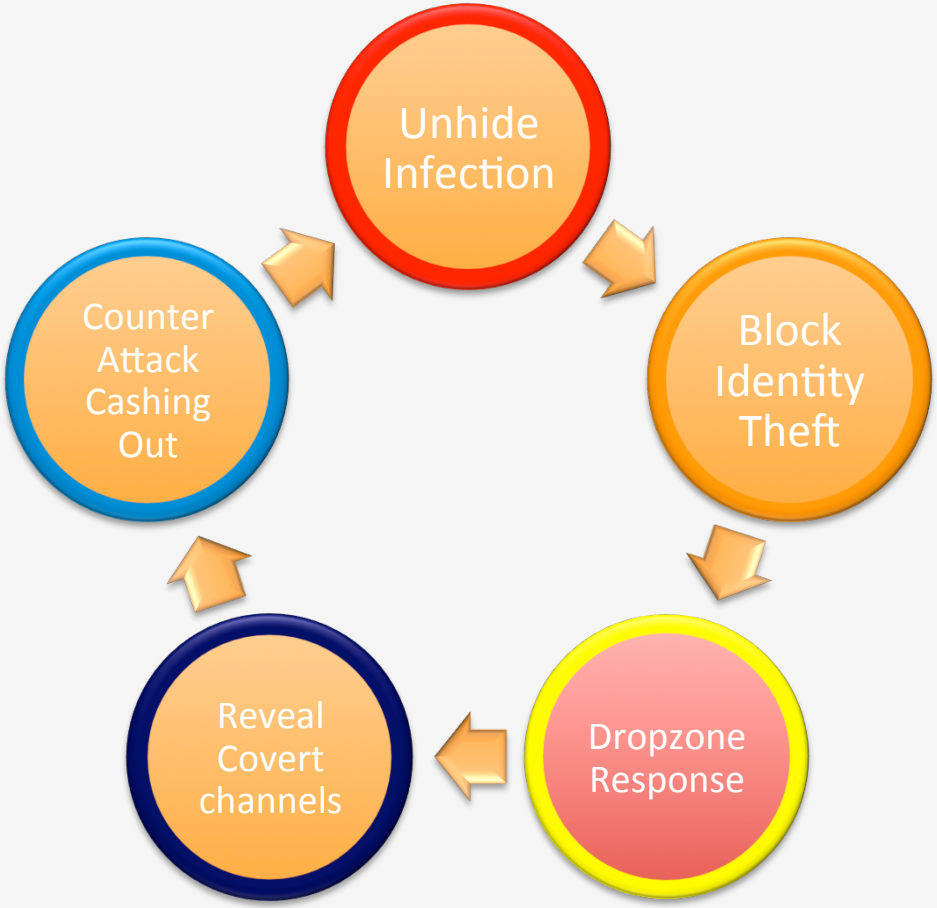
Source Gartner Functional Layers for Web Fraud Detection Tools

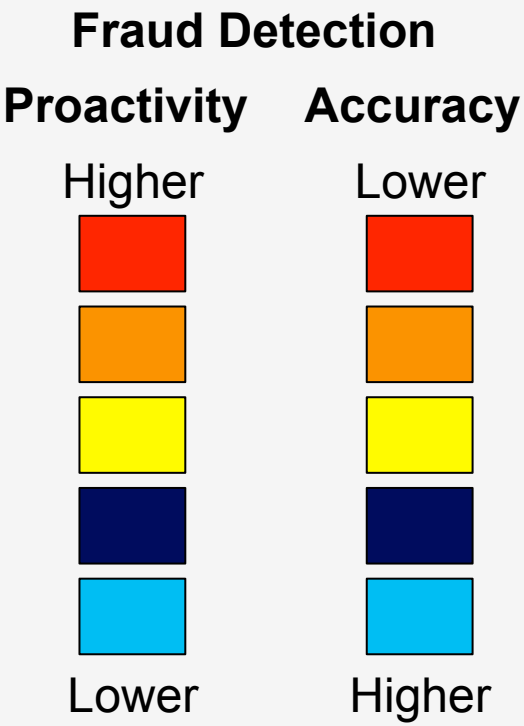
Malware Response Process



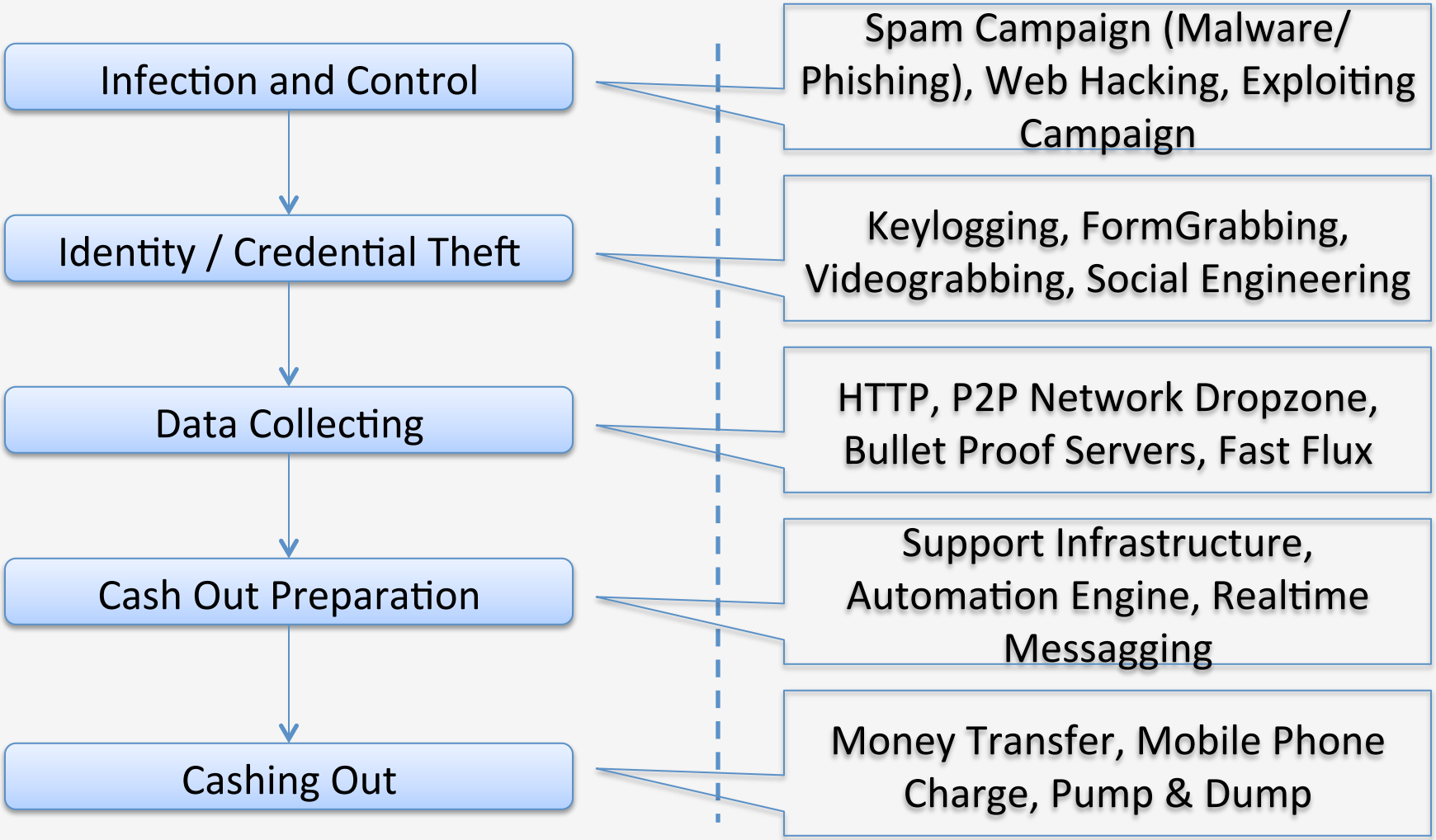
- This is a chain of required steps.
- Attackers need to perform successfully each of these for turning the attack into a monetary gain.
- For this reason the process can be reasonably stopped at any level.

Malware Response Process



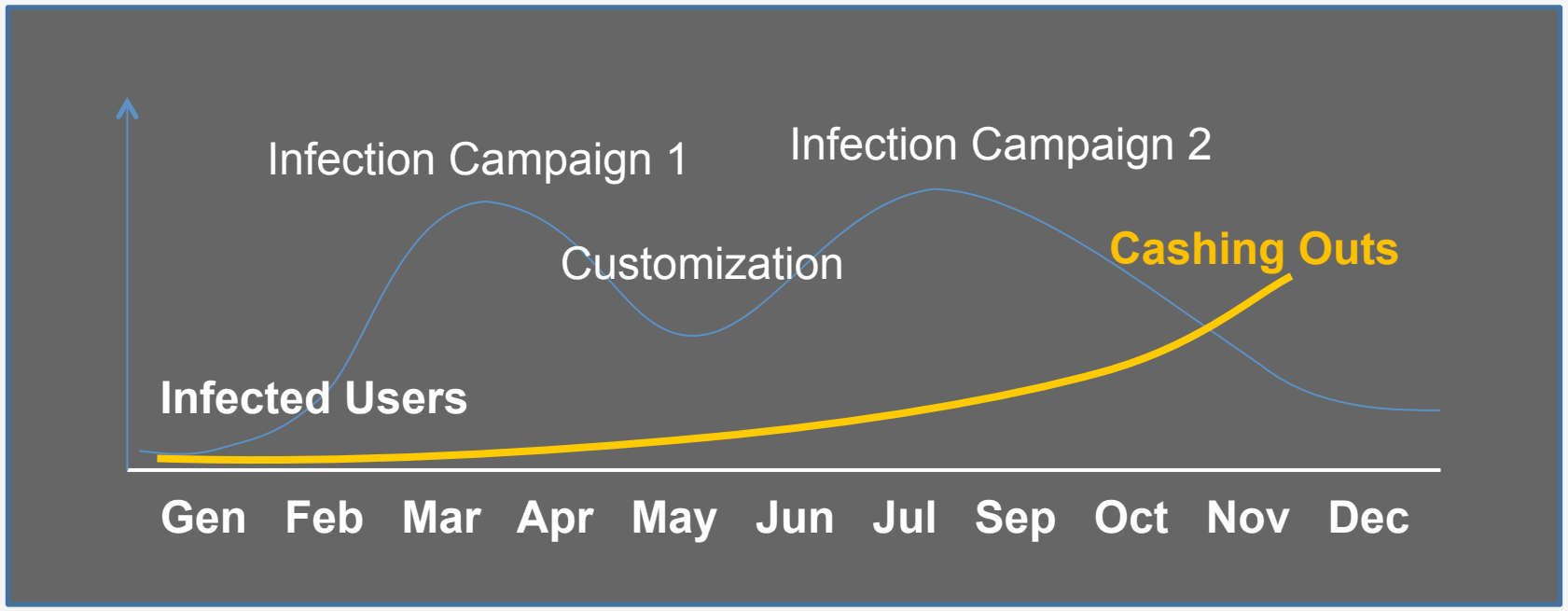


Malware Response Process



Malware Response Process

- Infection floods could happen even months before cashing outs actually occur



Malware Response Process

https://promotion-statistics.mobi/pt/panel.php

whatis my ip

name:
iban:
min:
max:
swift:
comment:

ALL
businesswaybnl.it
inbank.it
inbiz.intesasanpaolo.com
online-smallbusiness.unicredit.it

add

name	iban	swift	min	max	comment	url	timeout	id	
GIAN PIERO LELLI	IT78L0305801604100320306247		2500	10000	bonifico	ALL			delete
Angelo Lombardo	IT23Q0760110300001021873953		2500	10000	HJK4890	ALL			delete
ANGELO SCAROLA	IT82E0558401718000000000780		2500	10000	num 520	ALL			delete
cara salvatore	IT20J0521601634000000002689		750	2500	trasferimento di denaro	businesswaybnl.it			delete
GIUSEPPE SGRO	IT92B0306234210000050016450		2500	10000	C5998FA	inbank.it,inbiz.intesasanpaolo.com,online-smallbusiness.unicredit.it			delete
Franco Giacotto	IT48E0326813000052497370600		2500	15000		ALL	1413177943	UFFICIO-PC_E532648A8984D5E0	delete
Christian Orru	IT47F0305967684510300667272		2500	10000	CODE 117	ALL			delete

MINDED SECURITY
The Software Security Company

Malware Response Process

File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto

AZ | Authorization | shellshock exploit - Cerca co... | Nuova scheda | PANEL

https://derepositories.net/es/

TEST 11-10-2014 09:29:20

ACCOUNTS SETINGS LOGAUT

Statistica

Accounts	Default	Zapros	Block	UnBlock
16	0	3	0	13

Accounts

Link	Login	Pass	Status	Zapros	Dop	Block	Dop	UnBlock	Comment	Save
https://www.sella.it/Autenticazione/step_one.jsp	111111	111111	unblock	Zapros		Block		UnBlock		Save
https://www.sella.it/Autenticazione/step_one.jsp	00482244	0875	unblock	Zapros		Block		UnBlock	bez tokena!!!!!!	Save
https://entreprises.bnpparibas.net/NSAccess	ADMINISTRATOR!TEST264518225D!2422C526		unblock	Zapros		Block		UnBlock	test FR	Save
https://entreprises.bnpparibas.net/NSAccess	BOT_MACHINE_UUID		unblock	Zapros		Block		UnBlock	test FR	Save
https://www.sella.it/Autenticazione/step_one.jsp	54839	1177	zapros	Zapros		Block		UnBlock	Servizio momen	Save
https://www.sella.it/Autenticazione/step_one.jsp	0634744	7272	unblock	Zapros		Block		UnBlock	309,67 EUR crc	Save
https://www.sella.it/Autenticazione/step_one.jsp	33333333	3333	unblock	Zapros		Block		UnBlock		Save
https://www.sella.it/Autenticazione/step_one.jsp	00545527	2007	zapros	Zapros		Block		UnBlock	Id Bot=AFERRA	Save
https://bywebcard.bancopopolare.it/WEBHT/login	2043637	983777	zapros	Zapros		Block		UnBlock		Save
https://youwebcard.bancopopolare.it/WEBHT/logir	9678892	MATTHIAS11	unblock	Zapros		Block		UnBlock		Save
https://www.sella.it/Autenticazione/step_one.jsp	565464	34634634	unblock	Zapros		Block		UnBlock		Save
https://www.sella.it/Autenticazione/step_one.jsp	456897	5566	unblock	Zapros		Block		UnBlock		Save
https://youwebcard.bancopopolare.it/WEBHT/logir	3565455	8855	unblock	Zapros		Block		UnBlock		Save
https://youwebcard.bancopopolare.it/WEBHT/logir	8554522	23255	unblock	Zapros		Block		UnBlock		Save

Console HTML CSS Script DOM Net Cookie Events

Malware Response Process

https://derepositories.net/test1/index.php

.::CC+VBV Grabber

Sat, 11 Oct 2014 14:06:06 (UTC) Options Sign out

Cards | Additional Fields Rules | VBV/MCSC Rules

Refresh | View Details | Delete Card | Delete All Cards | Export To CSV | Reset Holder | Reset All Holders | 1

Site: All
Contry: All
Bank: All
Card Vendor: All
Card Type: All
Card Class: All
Cards Selected: 9
Total Cards: 9

Report Time	IP	Browser	Country	Site	Bank	Type	Card Number	CVV	Exp. Date	Name on Card	Address	City	State	ZIP	Grabbed	Valid State
2014-07-28 12:19:16	69.249.16.188	FF	US	yahoo	BANK OF MONTREAL	MASTERCARD	5191080200358158	324	06/2016	Patricia Lowe	1611 N Jackson St	Wilmington	DE	19806	YES	Checker Disabled
2014-07-28 11:57:55	69.249.16.188	FF	US	yahoo	TD BANK, NATIONAL ASSOCIATION	VISA, DEBIT, CLASSIC	4029445075889507	204	01/2017	Patricia Lowe	1611 N Jackson St	Wilmington	DE	19806	YES	Checker Disabled
2014-07-28 02:50:23	97.124.104.74	IE8	US	yahoo	JPMORGAN CHASE BANK, N.A.	VISA, DEBIT, BUSINESS	4427426016186490	382	08/2017	ERROL VANCE JOHNSON	824 W PASEO WAY	PHOENIX	AZ	85041	YES	Checker Disabled
2014-07-27 14:35:21	174.56.119.191	IE9	US	live	NEW MEXICO EDUCATORS FEDERAL CREDIT UNION	VISA, DEBIT, CLASSIC	4200640004773803	746	09/2016	D L COOK SIMMONS	5126 Camino Vista NW	Albuquerque	NM	87120	NO	Checker Disabled
2014-07-26 21:26:28	198.72.181.44	IE10	US	live	WELLS FARGO BANK, N.A.	VISA, DEBIT	4342562113202343	586	02/2015	Javier Mendez	125 South Mariposa Ave Apt#19	Los Angeles/Koreatown	CA	90004	YES	Checker Disabled
2014-07-25 10:29:57	68.56.184.217	IE10	US	yahoo	LIBERTY SAVINGS BANK, FSB	VISA, DEBIT, CLASSIC	4149970101572459	557	03/2016	Kathryn E Brandow	271 Azure Rd	Venice	FL	34285	NO	Checker Disabled
2014-07-25 05:37:51	24.183.103.213	IE10	US	live	PEOPLES BANK OF ELKHORN	VISA, DEBIT, CLASSIC	4068810040086319	229	12/2014	Sacha Herdt	W3815 County RD A	Elkhorn	WI	53121	YES	Checker Disabled
2014-07-23 04:02:16	70.232.35.165	FF	US	yahoo	WELLS FARGO BANK ARIZONA, N.A.	VISA	4821630200588799	075	07/2018	perry austin jr	4911 145th st	little rock	AR	72206	YES	Checker Disabled
2014-07-12 01:51:05	74.124.102.18	FF	US	live	CAPITAL ONE BANK (USA), NATIONAL ASSOCIATION	VISA, CREDIT, GOLD PREMIUM	4388648772162384	073	01/2017	Michael F. Grenier	east end rd	homer	AK	99603	NO	Checker Disabled

MINDED SECURITY
The Software Security Company

Malware Response Process

https://derepositories.net/test1/index.php

.::CC+VBV Grabber

Sat, 11 Oct 2014 14:07:37 (UTC) Options Sign out

Cards Additional Fields Rules VBV/MCSC Rules

Refresh | View Details | Delete Card | Delete All Cards | Export To CSV | Reset Holder | Reset All Holders

Site: All
Contry: All
Bank: All

Card Vendor: All
Card Type: All
Card Class: All

Cards Selected: 9
Total Cards: 9

Report Time	IP	Browser	Country	Site	Bank	Type	Card Number	CVV	Exp. Date	Name on Card	Address	City	State	ZIP	Grabbed	Valid State
2014-07-28 12:19:16	69.249.16.188	FF	US	yahoo	BANK OF M						1611 N Jackson St	Wilmington	DE	19806	YES	Checker Disabled
2014-07-28 11:57:55	69.249.16.188	FF	US	yahoo	TD BANK, N ASSOCIATI						1611 N Jackson St	Wilmington	DE	19806	YES	Checker Disabled
2014-07-28 02:50:23	97.124.104.74	IE8	US	yahoo	JPMORGAN BANK, N.A.						824 W PASEO WAY	PHOENIX	AZ	85041	YES	Checker Disabled
2014-07-27 14:35:21	174.56.119.191	IE9	US	live	NEW MEXI EDUCATOR CREDIT UN						5126 Camino Vista NW	Albuquerque	NM	87120	NO	Checker Disabled
2014-07-26 21:26:28	198.72.181.44	IE10	US	live	WELLS FAR N.A.						125 South Mariposa Ave Apt#19	Los Angeles/Koreatown	CA	90004	YES	Checker Disabled
2014-07-25 10:29:57	68.56.184.217	IE10	US	yahoo	LIBERTY SA BANK, FSB						271 Azure Rd	Venice	FL	34285	NO	Checker Disabled
2014-07-25 05:37:51	24.183.103.213	IE10	US	live	PEOPLES B ELKHORN						W3815 County RD A	Elkhorn	WI	53121	YES	Checker Disabled
2014-07-23 04:02:16	70.232.35.165	FF	US	yahoo	WELLS FAR ARIZONA,						4911 145th st	little rock	AR	72206	YES	Checker Disabled
2014-07-12 01:51:05	74.124.102.18	FF	US	live	CAPITAL ON (USA), NAT ASSOCIATI						east end rd	homer	AK	99603	NO	Checker Disabled

View Account Details

Details:

Phone: 3027233239
VBV/MCSC (Variant #1): Sirsoth1968
VBV/MCSC (Variant #2): Sirsouth1968
ATM PIN: 1018
Date of Birth (month): 07
Date of Birth (day): 07
Date of Birth (year): 1990

Close

Malware Response Process

https://derepositories.net/ib/model.php#

Startpage

root

Logout

root

Next update in: 0: 10

INTERCEPT

Interception

Account records real-time management

Inject Status: OFF

Linked User: root

Jabber Sender: obamamonkey@jabbim.pl save

Commands: BLOCK x SMS x WAIT x LOGIN x REASK LOGIN INFO x Add Command

MINDED SECURITY
The Software Security Company

The Lessons Learnt from Banking Malware Security Incidents

1. **Banking malware risks are escalating targeting bank customers**:
   Compliance driven controls are not good enough.
   Banks are liable for retail bank customer money losses and exposed to law suits from businesses that experienced money losses.
2. **Banks need to improve web fraud detection controls**:
   Detect malware web injections originating from banking malware
   Simulate malware attacks to identify multi layered controls
3. **Suggested malware banking risk management strategy:**
   Identify the assets at risk
   Adopt a risk-based threat modeling process

References 1/3

- OWASP Top Ten Vulnerabilities
  - http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202010.pdf
- OWASP Testing Guide
  - https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf
- OWASP Application Threat Modeling
  - http://www.owasp.org/index.php/Application_Threat_Modeling
- OWASP Application Security Guide for CISO
  - https://www.owasp.org/index.php/Application_Security_Guide_For_CISOs
- Security Flaws Identification Through Threat Modeling
  - http://www.net-security.org/dl/insecure/INSECURE-Mag-17.pdf
- Real World Threat Modeling Using the PASTA Methodology
  - https://www.owasp.org/images/a/aa/AppSecEU2012_PASTA.pdf
- Threat Modeling of Banking Malware Attacks
  - https://www.owasp.org/images/5/5f/Marco_Morana_and_Tony_UV_-_Threat_Modeling_of_Banking_Malware.pdf
- Software Assurance Maturity Model (SAMM)
  - http://www.opensamm.org/

References 2/3

- Application Threat Modeling Book
  - http://www.amazon.co.uk/Application-Threat-Modeling-Marco-Morana/dp/0470500964
- Manage Your Risk With Application Threat Modeling
  - http://www.myappsecurity.com/wp-content/uploads/2011/09/Manage-Your-Risk-With-ThreatModeler-OWASP.pdf
- How to Design More Secure Online Payment Systems
  - http://www.isaca.org/chapters5/Venice/Events/Documents/ISACAVENICE-OWASP-UNIVE-2013-6%20-%20Morana.pdf
- Writing Secure Software
  - http://securesoftware.blogspot.co.uk/
- Building Security In the SDLC
  - http://www.blackhat.com/presentations/bh-usa-06/bh-us-06-Morana-R3.0.pdf
- Architectural Design Patterns for SSO
  - http://www.owasp.org.cn/OWASP_Conference/2011/10.pdf
- Adapting to evolving cyber attack scenarios: a focus on hacking and malware threats targeting financial applications
  - http://www.owasp.com/images/e/e0/OWASP-eCrime-London-2012-Final.pdf

References 3/3

- Attention, CISOs: Strategy is the Only Security
  - http://www.cio.in/content/attention-cisos-strategy-only-security
- Software Security Assurance
  - http://iac.dtic.mil/csiac/download/security.pdf
- Producing Secure Software With Security Enhanced Software Development Processes
  - http://www.net-security.org/dl/insecure/INSECURE-Mag-16.pdf
- Security Flaws Identification and Technical Risk Analysis Through Threat Modeling, In-secure Magazine, June 2008, Page 85
  - Security Flaws Identification and Technical Risk Analysis Through Threat Modeling, In-secure Magazine, June 2008, Page 85
- Web Application Vulnerabilities And In-secure Software Root Causes
  - http://www.net-security.org/dl/insecure/INSECURE-Mag-17.pdf
  - http://www.net-security.org/dl/insecure/INSECURE-Mag-15.pdf

Questions?

Mail: matteo.meucci@mindedsecurity.com

Corporate Site: www.mindedsecurity.com

AMT Banking Malware Detector:
www.malware-detector.com

Thanks!