FRODI DI NUOVA GENERAZIONE SU CARTE DI CREDITO/DEBITO, NFC & POS ED UTILIZZO DELLA «CYBERCRIME INTELLIGENCE» COME STRUMENTO STRATEGICO DI CONTRASTO

Raoul Chiesa

President, Security Brokers SCpA

European Union Network & Information Security Agency (ENISA), PSG Member

ABI EVENTI

ABI Associazione Bancaria Italiana

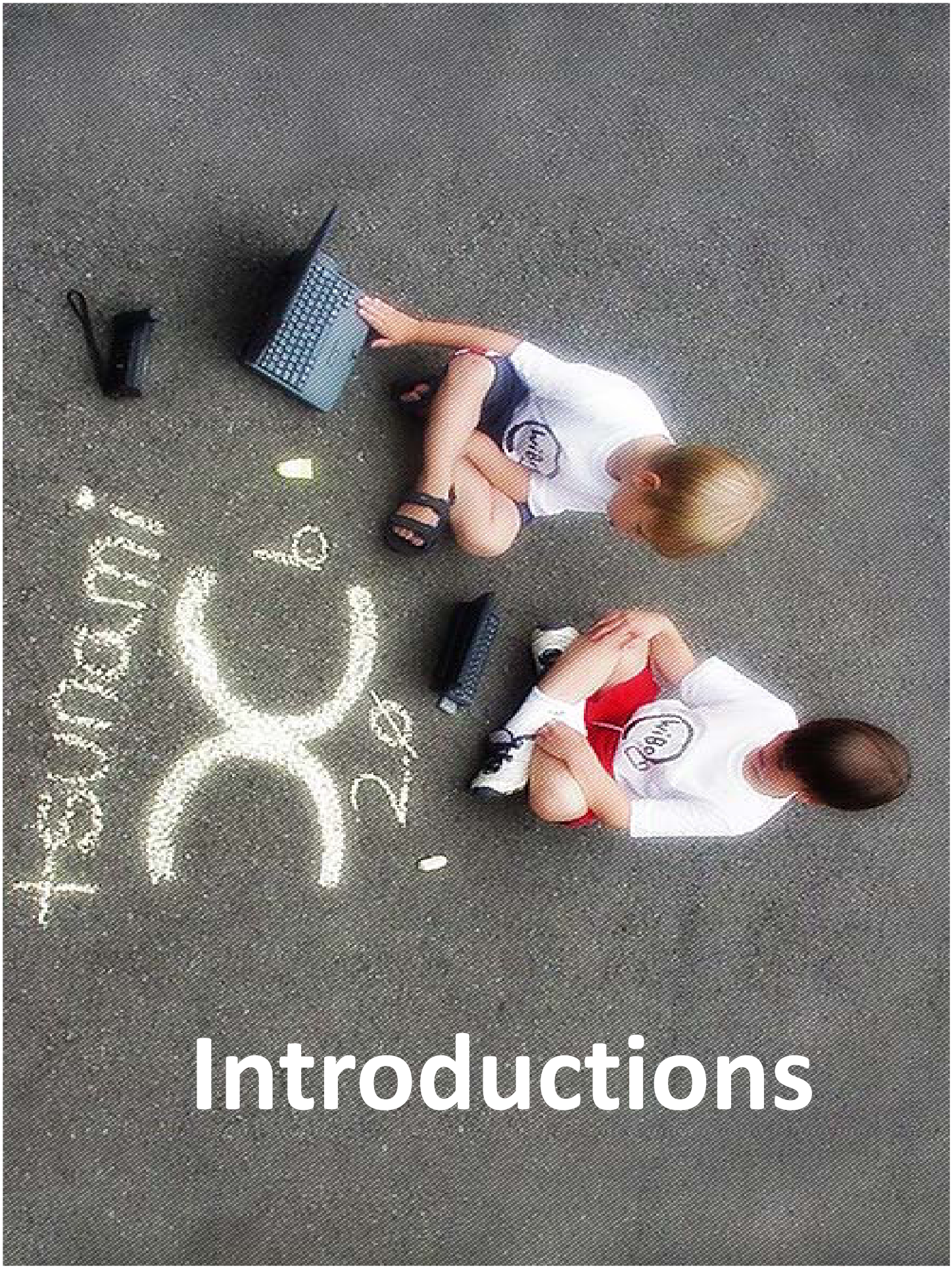
CONSORZIO BANCOMAT

Disclaimer

- The information contained within this presentation **do not infringe** on any intellectual property nor does it contain tools or recipe that could be in breach with known laws.
- The statistical data presented **belongs to** the Hackers Profiling Project by **UNICRI** and **ISECOM**.
- Quoted trademarks belongs to **registered owners**.
- The views expressed are those of the author(s) and speaker(s) and **do not necessary reflect** the views of **UNICRI** or others **United Nations** agencies and institutes, nor the view of **ENISA** and its **PSG** (Permanent Stakeholders Group), neither **Security Brokers**, its **Associates** and **Associated Companies,** and **Technical Partners**.
- Contents of this presentation **cannot be quoted or reproduced**.

Agenda

- Introductions
- Cybercrime
- Evolving scenarios in the counter-fraud Banking Environments:
  - Cards
  - POS
    - mPOS and vPOS: new cash-out approaches
  - NFC
- Cyber Intelligence
  - What can you get?
- Conclusions
- Reading Room
- Contacts
- Extra material: Profiling «Hackers»


Introductions

Il relatore

- President, Founder, **Security Brokers**
- Principal, **CyberDefcon Ltd.**
- Independent Senior Advisor on Cybercrime @ **UNICRI (United Nations Interregional Crime & Justice Research Institute)**
- PSG Member, **ENISA (Permanent Stakeholders Group @ European Union Network & Information Security Agency)**
- Founder, Board of Directors and Technical Commitee Member @ **CLUSIT** (Italian Information Security Association)
- Steering Committee, **AIP/OPSI**, Privacy & Security Observatory
- Member, Co-coordinator of the WG «Cyber World» @ **Italian MoD**
- Board of Directors, **ISECOM**
- Board of Directors, **OWASP** Italian Chapter
- Cultural Attachè and BoD Member for **APWG.EU**
- **Supporter at various security communities**

L'azienda

Security Brokers ScpA

- Ci occupiamo di argomenti estremamente interessanti, forti del know-how frutto di **+20 anni di esperienze** e di **+30 esperti** molto noti a livello mondiale negli ambienti dell'**Information Security** e della **Cyber Intelligence** (ma non solo).

- Le **principali famiglie di servizi** sono riassumibili come segue:
  - **Proactive Security**
    - con forte specializzazione su TLC & Mobile, SCADA & IA, ICN & Trasporti, Space & Air, Social Networks, e-health, […]
  - **Post-Incident**
    - Attacker's profiling, Digital Forensics (Host, Network, Mobile, GPS, etc..), Formazione
  - **Cyber Security Strategic Consulting** (Technical, Legal, Compliance, PR, Strategy)
    - On-demand «Ninja Teams»
    - Security Incident PR Handling & Management
  - **Aspetti psicologici, sociali e comportamentali**
  - **Cyber Intelligence**
    - Cybercrime Intelligence (Banking&Finance, Oil/Gas/Energy, Transportation), Botnet takeovers, takedowns, Cybercriminals bounting, Cyber Intelligence Reports, interfacciamento con CERTs e LEAs/LEOs, servizi di OSINT e di CSINT
  - **Information Warfare & Cyber War** (solo per MoD / GOV / Agenzie di Intelligence)
    - 0-day ed Exploits – Digital Weapons
    - OSINT (Open-source Intelligence in ambito GOV e MIL)
    - CSINT (Closed-source Intelligence in ambito GOV e MIL)

Problemi di terminologia

No common spelling…

„Cybersecurity, Cyber-security, Cyber Security ?”

No common definitions…

Cybercrime is…?

No clear actors…

Cyber – Crime/war/terrorism ?

No common components?…

❑ Nei Paesi di lingua **non anglofona**, il problema di una corretta comprensione delle terminologie **aumenta**.

«Cyber Intelligence»?

- In linea generale, sono pochi gli addetti del settore Finance&Banking che conoscono il reale significato della **Cyber Intelligence**.
- Innanzitutto, dobbiamo **capire cosa significa** "Intelligence".
  - Nei **Paesi anglossassoni**, il termine significa "informazione".
- La "Cyber Intelligence" quindi non è altro che la **raccolta di informazioni dal mondo Cyber**.
- Queste informazioni si chiamano, in gergo, "**feeds**".
  - Principalmente esse provengono da attente osservazioni del mondo del **Cybercrime** (ma non solo).
- La Cyber Intelligence può provenire da **due distinte tipologie di fonti**:
  - **Fonti Aperte** (Open Sources), quindi provenienti da attività di tipo **OSINT** (Open Source Intelligence), manuali, automatiche o "ibride" (automatizzate ma con verifiche manuali da parte di analisti)
  - **Fonti Chiuse** (Closed Sources), quali l'accesso a portali non pubblici, l'infiltrazione per attività "cyber" sotto copertura, l'intercettazione di dati provenienti da diverse fonti (botnet, SIGINT, HUMINT, etc.).


Cybercrime

Cybercrime

«Cybercrime ranks as one of the top four economic crimes»

PriceWaterhouseCoopers LLC Global Economic Crime Survey 2011

"Cybercrime financial turnover apparently scored up more than Drugs dealing, Human Trafficking and Weapons Trafficking turnovers"

Various sources (UN, USDOJ, INTERPOL, 2011)

2013 Financial Turnover, estimation: 12-18 BLN USD$/year

Il crimine di oggi -> Cybercrime

*Hai l'**informazione**, **information**, hai il **potere**..*

Questo avviene semplicemente perché il concetto di "*informazione*" (che oggigiorno risiede su supporti digitali e viaggia in rete) può essere **immediatamente trasformato** in «qualcos'altro»":

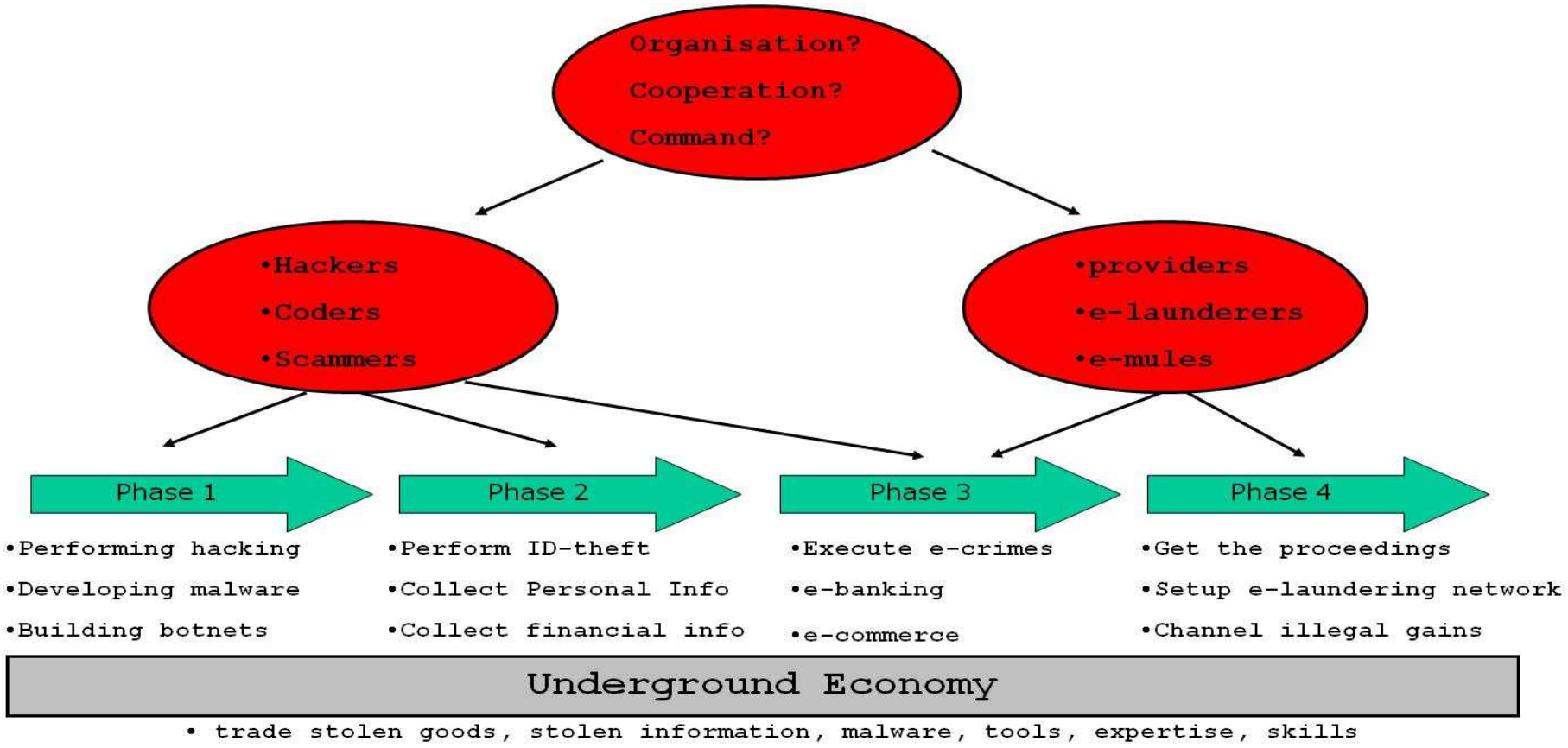
1. **Vantaggio competitivo (geo/politico, business, relazioni personali)**
2. **Informazione sensibile/critica («blackmailing»/ricatto, estorsione)**
3. **Denaro (tecniche di «Cash-out», Black Market & Underground Economy)**

- Ecco perché tutti noi vogliamo «essere sicuri".
- Non è un caso se si chiama «IS» : **Information Security** ☺
  - La **moda** «cyber-prefisso» è d'altr'onde una novità degli **anni recenti**.

Cybercrime: key points

- Il **Cybercrime**:
  - *"utilizzo di strumenti informatici e reti di telecomunicazione*
    - *per l'esecuzione di reati e crimini di diversa natura".*
- **L'assioma alla base dell'intero modello:**
  - *"acquisire diversi insiemi di dati (informazione), tramutabili in denaro."*
- **Punti salienti**:
  - **Virtuale** (modello "a piramide" ed anonimato, C&C, flessibili e scalabili, velocità di spostamento e rebuilding, utilizzo "cross" di prodotti e servizi in differenti scenari e modelli di business)
  - **Transnazionale**
  - Multi-mercato (**acquirenti**)
  - **Diversificazione** dei prodotti e dei servizi
  - **Bassa** "entry-fee"
  - **ROI** (per singola operazione, quindi esponenziale se industrializzato)
  - Tax & (cyber) Law **heaven**

Cybercrime: Modus Operandi (MO)



Esempio di digital underground slang (Cybercrime)

- **Carder** - Slang used to describe individuals who use stolen credit card account information to conduct fraudulent transactions.
- **Carding** - Trafficking in and fraudulent use of stolen credit card account information.
- **Cashing** - The act of obtaining money by committing fraud. This act can be committed in a variety of ways: The term can stand for cashing out Western Union wires, Postal money orders and WebMoney; using track data with PINs to obtain cash at ATMs, from PayPal accounts, or setting up a bank account with a fake ID to withdraw cash on a credit card account.
- **CC** - Slang for credit card.
- **Change of Billing (COB or COBs)** - Term used to describe the act of changing the billing address on a credit account to match that of a mail drop. This act allows the carder full takeover capability of the compromised credit card account and increases the probability that the account will not be rejected when being used for Internet transactions.
- **CVV2** - CVV2 stands for credit card security code. Visa, MasterCard, and Discover require this feature. It is a 3 digit number on the back of the card.
- **DDoS** - Acronym for Distributed Denial of Service Attack. The intent when conducting a DDOS attack is to shut down a targeted website, at least for a period of time, by flooding the network with an overflow of traffic.
- **DLs** - A slang term that stands for counterfeit or novelty driver's licenses.
- **Drop** - An intermediary used to disguise the source of a transaction (addresses, phones etc.)
- **Dumps** - Copied payment card information, at least Track 1 data, but usually Track 1 and Track 2 data.
- **Dump checking** - Using specific software or alternatively encoding track data on plastic and using a point of sale terminal to test whether the dump is approved or declined. This provides carders a higher sense of security for obtaining quality dumps fro those who offer them and also a sense of security when doing in store carding.
- **Full info(s)** - Term used to describe obtaining addresses, phone numbers, social security numbers, PIN numbers, credit history reports and so on. Full Info(s) are synonymous with carders who wish to take over the identity of a person or to sell the identity of a person.
- **Holos** - Slang for the word Holograms. Holograms are important for those who make counterfeit plastic credit cards to emulate an existing security feature.
- **ICQ** - An abbreviation for "I Seek You". ICQ is the most widely used instant messaging system for carders. Popular among Eastern Europeans in their Internet culture, it continues to be used for carding activity.
- **IRC** - An abbreviation for "Internet Relay Chat". IRC is a global system of servers through which users can conduct real-time text-based chat, exchange files, and interact in other ways.
- **IDs** - Slang for identification documents. Carders market a variety of IDs, including bills, diplomas, driver's licenses, passports, or anything that can be used as an identity document.
- **MSR (Magnetic Strip Reader**) - Device that can be used for skimming payment card information and/or encoding track information on plastic.
- Phishing - The extraction of information from a target using a hook (usually an e-mail purporting to be from a legitimate company). Phishers spam the Internet with e-mails in hopes of obtaining information that can be used for fraudulent purposes.
- **POS (Point of Sale)** - Acronym for a terminal through which credit cards are swiped in order to communicate with processors who approve or decline transactions.
- **Proxies** - Term used for proxy servers. The use of proxy servers to mask ones identity on the Internet is widely practiced amongst carders. Many vendors sell access to proxy servers, socks, http, https, and VPN (Virtual Private Networks), which aide in hiding the user's actual IP address when committing fraud or other illegal activity on the Internet.
- **Track 1/Track 2 data** - Track 1 and Track 2 data is the information stored on the magnetic stripe of a payment card that contains the account information.

Evolving scenarios in the counter-fraud Banking Environments

Evoluzione del «perimetro»

- Nel mondo dell'Information Security si chiama «**evoluzione del perimetro**».
- E' la **conseguenza dell'evoluzione tecnologica** e dell'**impatto della c.d. «Digital Society»** sul mondo del business:
  - BYOL (Bring Your Own Laptop)
  - BYOD (Bring Your Own Device)
  - Remote Working
  - Remote Co-Working
  - Social Networks
  - Cloud
  - ……

L'anti-frode di nuova generazione

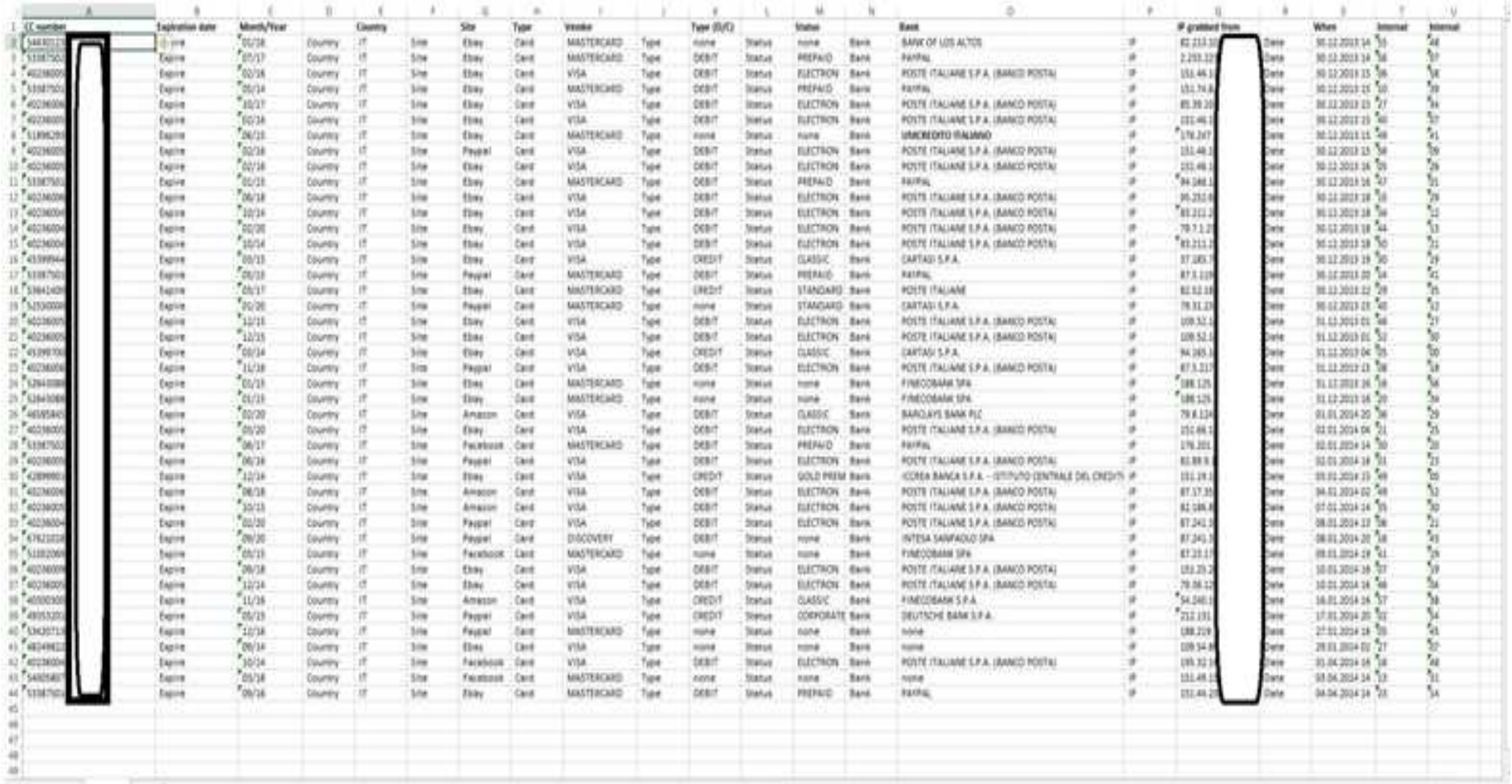
- Allo stesso modo, il mondo bancario ha **dovuto rivedere i propri approcci antifrode**.
- **Oggi** è:
  - (molto) raro che attackers violino i **sistemi mainframe**;
  - (abbastanza) raro che avvengano **violazioni aggirando i sistemi di difesa perimetrale** posti in essere (Firewall, xIDS, etc).
- E' all'ordine del giorno che **TTP** (third-trusted party) vengano violate a scapito dell'istituto bancario e finanziario, come ad esempio i **Card Processing Center** (gli esempi sono purtroppo decine e decine).
- E' all'ordine del giorno che il **cliente finale** dell'istituzione finanziaria venga violato (malware, trojan, key loggers, botnet, etc)
- E' all'ordine del giorno che **dispositivi attended** ed **unattended**, quali **POS** e **Totem di pagamento**, vengano compromessi ed i flussi di carte di credito/debito intercettati.

E-banking (botnet)

Bot ID: 59123a946d2d6ff7af589b1dcf9881e719161db4
Botnet: JUDY
Version: 58
OS Version: Seven x64,SP 1,Lang 1040,ProductType 3,Build 7601
Computer ID UTENTE-PC_05227AE9F7A667719588FBC19FEDF31A
GMT: +1:00
Time start system 00:00:22
Local time 17.03.2014 18:39:51
Report time: 17.03.2014 18:10:09
Country: IT
IPv4: 151.xxx.xxx.xxx
Comment for bot: -
In the list of used: No
Process name: C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE
User of process: Utente-PC\Utente
Enviroment "C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:1484 CREDAT:996370 /prefetch:2
PID 2188
Level 3
Time process 17.03.2014 17:38:31
Lang process 1040
Source: https:/[redacted].it/WEBHT/cc/movimentiConto.do
https://[redacted]t/WEBHT/cc/movimentiConto.do
Referer: https:/[redacted].it/WEBHT/homepage.do
User input: 648112102986638820786l
POST data:

compilazione=S
codContoCorrente=001%7C21809[redacted]

Cards, POS, NFC



CC number	Expiration date	Month/Year		Country		Site	Type	Vendor		Type (D/C)		Status		Bank		IP grabbed from		When	Internet	Internet
5488301[illegible]	Expire	01/18	Country	IT	Site	Ebay	Card	MASTERCARD	Type	none	Status	none	Bank	BANK OF LOS ALTOS	IP	82.213.10[illegible]	Date	30.12.2013 14	33	48
5338750[illegible]	Expire	07/17	Country	IT	Site	Ebay	Card	MASTERCARD	Type	DEBIT	Status	PREPAID	Bank	PAYPAL	IP	2.233.12[illegible]	Date	30.12.2013 14	34	37
4023600[illegible]	Expire	02/18	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	151.44.1[illegible]	Date	30.12.2013 15	36	38
5338750[illegible]	Expire	05/14	Country	IT	Site	Ebay	Card	MASTERCARD	Type	DEBIT	Status	PREPAID	Bank	PAYPAL	IP	151.74.8[illegible]	Date	30.12.2013 15	35	39
4023600[illegible]	Expire	10/17	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	85.39.20[illegible]	Date	30.12.2013 15	37	34
4023600[illegible]	Expire	02/18	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	151.44.1[illegible]	Date	30.12.2013 15	40	37
5189629[illegible]	Expire	06/15	Country	IT	Site	Ebay	Card	MASTERCARD	Type	none	Status	none	Bank	UNICREDITO ITALIANO	IP	176.247[illegible]	Date	30.12.2013 15	48	41
4023600[illegible]	Expire	02/18	Country	IT	Site	Paypal	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	151.44.1[illegible]	Date	30.12.2013 15	38	39
4023600[illegible]	Expire	02/18	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	151.44.1[illegible]	Date	30.12.2013 16	39	26
5338750[illegible]	Expire	01/15	Country	IT	Site	Ebay	Card	MASTERCARD	Type	DEBIT	Status	PREPAID	Bank	PAYPAL	IP	94.168.1[illegible]	Date	30.12.2013 16	47	31
4023600[illegible]	Expire	06/18	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	95.252.6[illegible]	Date	30.12.2013 18	50	29
4023600[illegible]	Expire	10/14	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	93.211.2[illegible]	Date	30.12.2013 18	44	51
4023600[illegible]	Expire	02/20	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	79.7.1.23[illegible]	Date	30.12.2013 18	44	53
4023600[illegible]	Expire	10/14	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	93.211.2[illegible]	Date	30.12.2013 18	50	31
4599994[illegible]	Expire	09/15	Country	IT	Site	Ebay	Card	VISA	Type	CREDIT	Status	CLASSIC	Bank	CARTASI S.P.A.	IP	37.183.3[illegible]	Date	30.12.2013 19	30	29
5338750[illegible]	Expire	09/18	Country	IT	Site	Paypal	Card	MASTERCARD	Type	DEBIT	Status	PREPAID	Bank	PAYPAL	IP	87.3.119[illegible]	Date	30.12.2013 20	54	41
5364140[illegible]	Expire	09/17	Country	IT	Site	Ebay	Card	MASTERCARD	Type	CREDIT	Status	STANDARD	Bank	POSTE ITALIANE	IP	82.52.10[illegible]	Date	30.12.2013 22	29	35
5150000[illegible]	Expire	01/20	Country	IT	Site	Paypal	Card	MASTERCARD	Type	none	Status	STANDARD	Bank	CARTASI S.P.A.	IP	79.31.23[illegible]	Date	30.12.2013 23	40	32
4023600[illegible]	Expire	12/15	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	109.52.1[illegible]	Date	31.12.2013 01	48	27
4023600[illegible]	Expire	12/15	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	109.52.1[illegible]	Date	31.12.2013 01	52	30
4599970[illegible]	Expire	03/14	Country	IT	Site	Ebay	Card	VISA	Type	CREDIT	Status	CLASSIC	Bank	CARTASI S.P.A.	IP	94.165.1[illegible]	Date	31.12.2013 04	55	30
4023600[illegible]	Expire	11/18	Country	IT	Site	Paypal	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	87.3.213[illegible]	Date	31.12.2013 23	58	58
5284308[illegible]	Expire	01/15	Country	IT	Site	Ebay	Card	MASTERCARD	Type	none	Status	none	Bank	FINECOBANK SPA	IP	188.125[illegible]	Date	31.12.2013 16	58	56
5284308[illegible]	Expire	01/15	Country	IT	Site	Ebay	Card	MASTERCARD	Type	none	Status	none	Bank	FINECOBANK SPA	IP	188.125[illegible]	Date	31.12.2013 16	59	56
4659584[illegible]	Expire	02/20	Country	IT	Site	Amazon	Card	VISA	Type	DEBIT	Status	CLASSIC	Bank	BARCLAYS BANK PLC	IP	79.8.124[illegible]	Date	01.01.2014 20	58	59
4023600[illegible]	Expire	09/20	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	151.44.1[illegible]	Date	02.01.2014 04	51	25
5338750[illegible]	Expire	06/17	Country	IT	Site	Facebook	Card	MASTERCARD	Type	DEBIT	Status	PREPAID	Bank	PAYPAL	IP	176.201[illegible]	Date	02.01.2014 14	59	30
4023600[illegible]	Expire	06/18	Country	IT	Site	Paypal	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	82.89.9[illegible]	Date	02.01.2014 14	51	33
4289990[illegible]	Expire	12/14	Country	IT	Site	Ebay	Card	VISA	Type	CREDIT	Status	GOLD PREM	Bank	ICCREA BANCA S.P.A. - ISTITUTO CENTRALE DEL CREDITO	IP	151.19.1[illegible]	Date	03.01.2014 15	59	50
4023600[illegible]	Expire	08/18	Country	IT	Site	Amazon	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	87.17.35[illegible]	Date	04.01.2014 02	49	32
4023600[illegible]	Expire	10/15	Country	IT	Site	Amazon	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	82.186.8[illegible]	Date	07.01.2014 14	55	30
4023600[illegible]	Expire	02/20	Country	IT	Site	Paypal	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	87.241.3[illegible]	Date	08.01.2014 22	58	21
4762103[illegible]	Expire	09/20	Country	IT	Site	Paypal	Card	DISCOVERY	Type	DEBIT	Status	none	Bank	INTESA SANPAOLO SPA	IP	87.241.3[illegible]	Date	08.01.2014 20	58	43
5103206[illegible]	Expire	05/15	Country	IT	Site	Facebook	Card	MASTERCARD	Type	none	Status	none	Bank	FINECOBANK SPA	IP	87.23.15[illegible]	Date	09.01.2014 19	51	29
4023600[illegible]	Expire	09/18	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	151.23.2[illegible]	Date	10.01.2014 16	57	39
4023600[illegible]	Expire	12/14	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	79.38.12[illegible]	Date	10.01.2014 16	48	54
4050030[illegible]	Expire	11/16	Country	IT	Site	Amazon	Card	VISA	Type	CREDIT	Status	CLASSIC	Bank	FINECOBANK S.P.A.	IP	94.240.1[illegible]	Date	16.01.2014 16	57	58
4935320[illegible]	Expire	05/15	Country	IT	Site	Paypal	Card	VISA	Type	CREDIT	Status	CORPORATE	Bank	DEUTSCHE BANK S.P.A.	IP	212.191[illegible]	Date	17.01.2014 20	52	54
5342071[illegible]	Expire	12/18	Country	IT	Site	Paypal	Card	MASTERCARD	Type	none	Status	none	Bank	none	IP	188.219[illegible]	Date	27.01.2014 18	53	43
4824981[illegible]	Expire	09/14	Country	IT	Site	Ebay	Card	VISA	Type	none	Status	none	Bank	none	IP	109.54.8[illegible]	Date	28.01.2014 02	27	32
4023600[illegible]	Expire	10/14	Country	IT	Site	Facebook	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	195.32.1[illegible]	Date	01.04.2014 14	38	48
5405480[illegible]	Expire	05/18	Country	IT	Site	Facebook	Card	MASTERCARD	Type	none	Status	none	Bank	none	IP	151.49.1[illegible]	Date	03.04.2014 14	53	31
5338750[illegible]	Expire	09/16	Country	IT	Site	Ebay	Card	MASTERCARD	Type	DEBIT	Status	PREPAID	Bank	PAYPAL	IP	151.44.2[illegible]	Date	04.04.2014 14	33	54

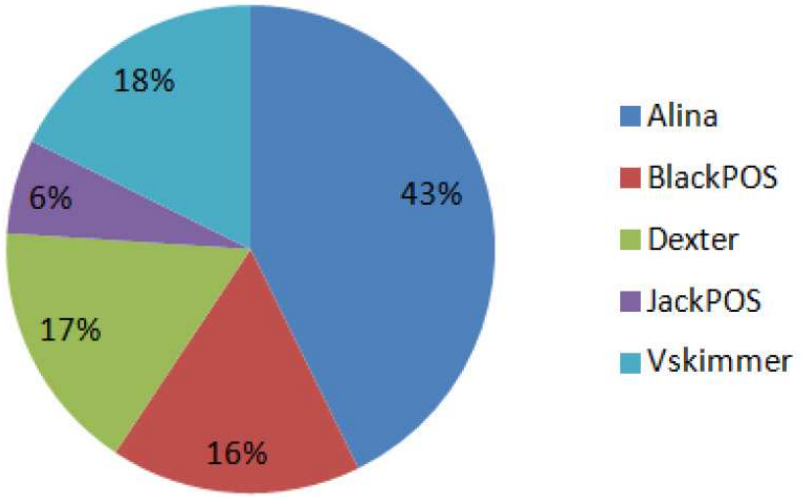
Cards, POS, NFC

#	Card number	Expire	Country	Site	Card	Type	Status	Bank	IP	Date
	4870380	11/16	US	Amazon	VISA	DEBIT	CLASSIC	FIRSTBANK PUERTO RICO	72.50.84.69	02.04.2014 17:18:03
	4111111	06/17	OT	Facebook	VISA	none	none	JPMORGAN CHASE BANK, N.A.	117.208.175.43	02.04.2014 18:32:37
	5213243	11/15	OT	Paypal	MASTERCARD	DEBIT	PLATINUM	TINKOFF CREDIT SYSTEMS	46.42.18.71	02.04.2014 18:56:56
	5588280	08/15	US	Paypal	MASTERCARD	none	STANDARD	CITIBANK SOUTH DAKOTA, N.A.	24.39.157.218	02.04.2014 19:07:52
	5220780	01/17	OT	Facebook	MASTERCARD	none	none	none	92.108.76.166	02.04.2014 20:12:20
	4012888	12/14	GB	Ebay	VISA	none	none	none	81.109.88.31	02.04.2014 21:54:12
	5136482	05/15	FR	Ebay	MASTERCARD	CREDIT	STANDARD	MASTERCARD FRANCE S.A.S.	89.90.10.156	02.04.2014 22:16:42
	4117704	06/16	US	Amazon	VISA	DEBIT	PLATINUM	BANK OF AMERICA, N.A.	216.15.123.114	02.04.2014 22:17:07
	4060012	01/15	OT	Paypal	VISA	DEBIT	CLASSIC	ALPHA BANK	79.167.211.68	03.04.2014 00:13:38
	5256781	11/17	ES	Facebook	MASTERCARD	DEBIT	STANDARD	BANCO NACIONAL DE MEXICO, S.A.	201.141.176.172	03.04.2014 00:45:23
	4117733	12/16	US	Amazon	VISA	DEBIT	PLATINUM	BANK OF AMERICA, N.A.	64.206.92.97	03.04.2014 00:59:09
	4049360	03/17	OT	Paypal	VISA	none	none	none	80.244.19.22	03.04.2014 01:16:02
	4342562	02/17	US	Ebay	VISA	DEBIT	none	WELLS FARGO BANK, N.A.	201.170.244.126	03.04.2014 01:45:08
	4067740	01/15	OT	Ebay	VISA	CREDIT	PLATINUM	BANCO INTERAMERICANO DE FINANZAS, S.A.E.M.A.	200.62.153.210	03.04.2014 01:49:31
	4342562	02/17	US	Ebay	VISA	DEBIT	none	WELLS FARGO BANK, N.A.	201.170.244.126	03.04.2014 01:56:36
	4870380	11/16	US	Amazon	VISA	DEBIT	CLASSIC	FIRSTBANK PUERTO RICO	72.50.87.5	03.04.2014 02:02:29
	4552550	10/13	OT	Facebook	VISA	CREDIT	GOLD PREMIUM	TARJETAS BANAMEX S.A. DE C.V. SOFOM ENTIDAD REGULADA	187.244.40.195	03.04.2014 02:03:47
	5189540	06/15	OT	Facebook	MASTERCARD	none	STANDARD	BANK LEUMI LE-ISRAEL BM	93.173.160.236	03.04.2014 02:13:35
	4537445	09/16	CA	Amazon	VISA	none	none	THE BANK OF NOVA SCOTIA	69.71.69.28	03.04.2014 04:33:31
	6011000	12/19	OT	Facebook	DISCOVERY	CREDIT	PLATINUM	none	186.45.182.9	03.04.2014 05:01:08
	4556321	10/14	OT	Paypal	VISA	CREDIT	CLASSIC	BANK CENTRAL ASIA	125.166.228.196	03.04.2014 05:11:29
	4098513	02/19	OT	Paypal	VISA	DEBIT	ELECTRON	BBVA BANCOMER S.A.	187.205.244.159	03.04.2014 05:25:08
	3749702	06/17	FR	Amazon	AMEX	CHARGE CARD	GOLD	BNP PARIBAS - AIR FRANCE	80.14.51.204	03.04.2014 05:36:44
	4221092	07/20	OT	Paypal	VISA	DEBIT	CLASSIC	ASIA COMMERCIAL BANK	123.18.115.188	03.04.2014 06:27:38
	4870380	11/16	US	Amazon	VISA	DEBIT	CLASSIC	FIRSTBANK PUERTO RICO	72.50.85.69	03.04.2014 07:27:44
	5581588	05/14	US	Paypal	MASTERCARD	none	BUSINESS	JPMORGAN CHASE BANK, N.A.	99.114.149.202	03.04.2014 08:07:51
	4688170	09/21	OT	Paypal	VISA	DEBIT	ELECTRON	ANDHRA BANK	117.207.251.7	03.04.2014 08:32:03
	4216276	10/17	OT	Paypal	VISA	DEBIT	CLASSIC	ICICI BANK LTD	182.64.134.172	03.04.2014 09:27:22
	4386280	08/15	OT	Facebook	VISA	CREDIT	PLATINUM	CITIBANK, N.A.	115.118.167.111	03.04.2014 10:15:05
	5400580	03/18	IT	Facebook	MASTERCARD	none	none	none	151.49.158.230	03.04.2014 14:13:31
	5402052	02/18	ES	Ebay	MASTERCARD	none	STANDARD	BANCO SABADELL S.A.	80.31.18.111	03.04.2014 14:31:52
	4617267	12/17	OT	Facebook	VISA	CREDIT	PLATINUM	CITIBANK (HONG KONG) LIMITED	119.237.130.150	03.04.2014 16:44:04

Cards, POS, NFC

Data Leakage

- POS Device Tampering
- POS Device Infection
- Traffic Analysis



Cards, POS, NFC

"Kartoxa/BlackPOS" & Target Breach

Binary Analysis (March 2013)

```
memset(&v57, 0xCCu, 0x380u);
v88 = 0;
sub_403190(&v87, lpMultiByteStr);
v89 = 0;
v86 = 0;
buff_curr_pos = buffer;
bufend = buffer + bytes_read - 1;
v83 = strstr(lpMultiByteStr, "KAPTOXA");
if ( v83 )
{
  while ( 1 )
  {
    if ( buff_curr_pos >= bufend )
      break;
```

C&C Detection

```
data:00471220 aWwwRee4_7ci_ru db 'www/ree4.7ci.ru/reports/',0 ;
data:00471243 ; char aDun_exe_2[]
data:00471243 aDun_exe_2      db 'dun.exe',0          ; DATA XRI
data:0047124B ; char aOutput_txt_1[]
data:0047124B aOutput_txt_1   db 'output.txt',0       ; DATA XRI
data:00471256 aDun_exe_3      db 'dun.exe',0          ; DATA XRI
data:0047125E ; char aDun_exe_4[]
data:0047125E aDun_exe_4      db 'dun.exe',0          ; DATA XRI
                              db '\svhst.exe',0       ; DATA XRI
data:00471271 aDumpGrabberBuR db 'dump grabber bu ree4.',0
data:00471271                                         ; DATA XRI
data:00471287 aUserDirectoryN db 'user directory name: ',0
data:00471287                                         ; DATA XRI
data:0047129D aDeleteTheFileA db 'Delete the file after reading
```

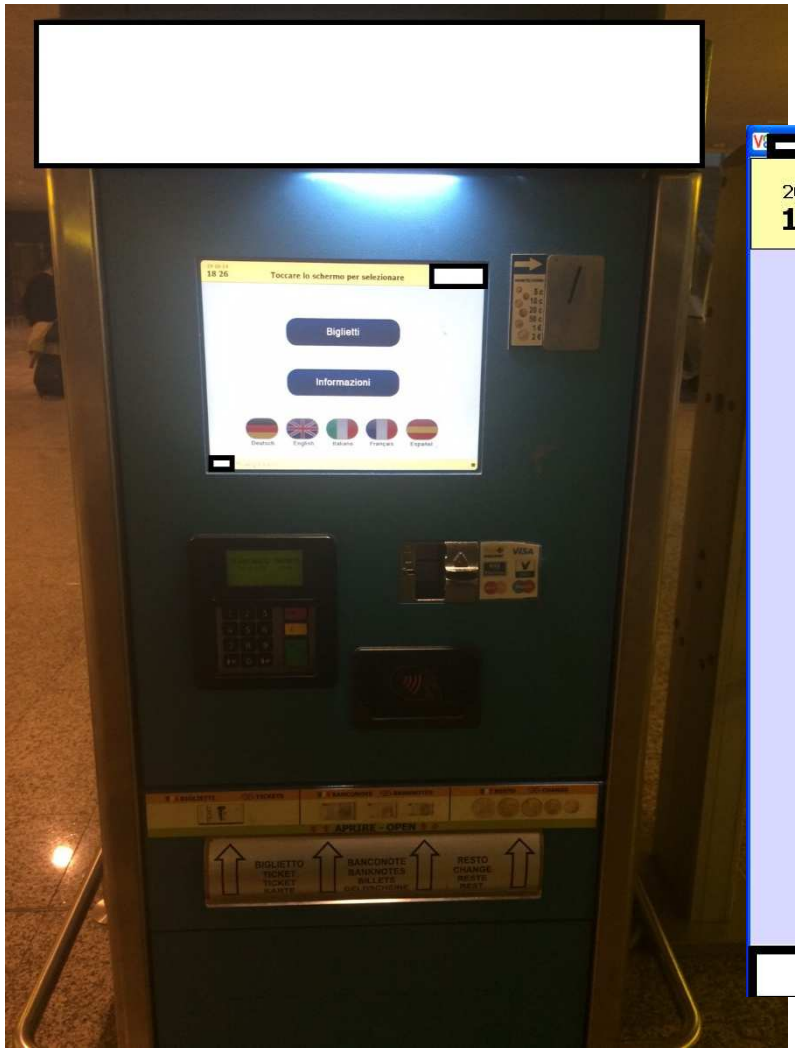
Cards, POS, NFC

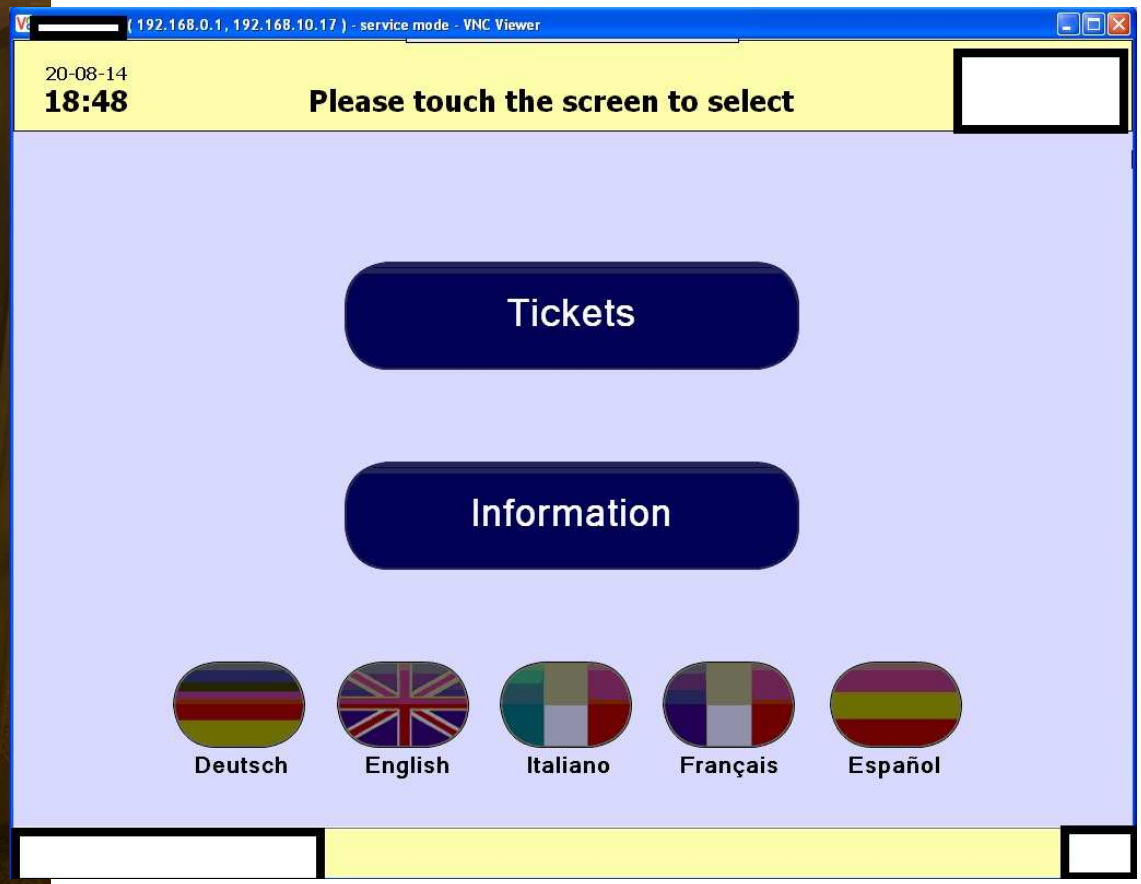
"Kartoxa"/"BlackPOS" Author

"Yes, I have written it, but for security testing ..."

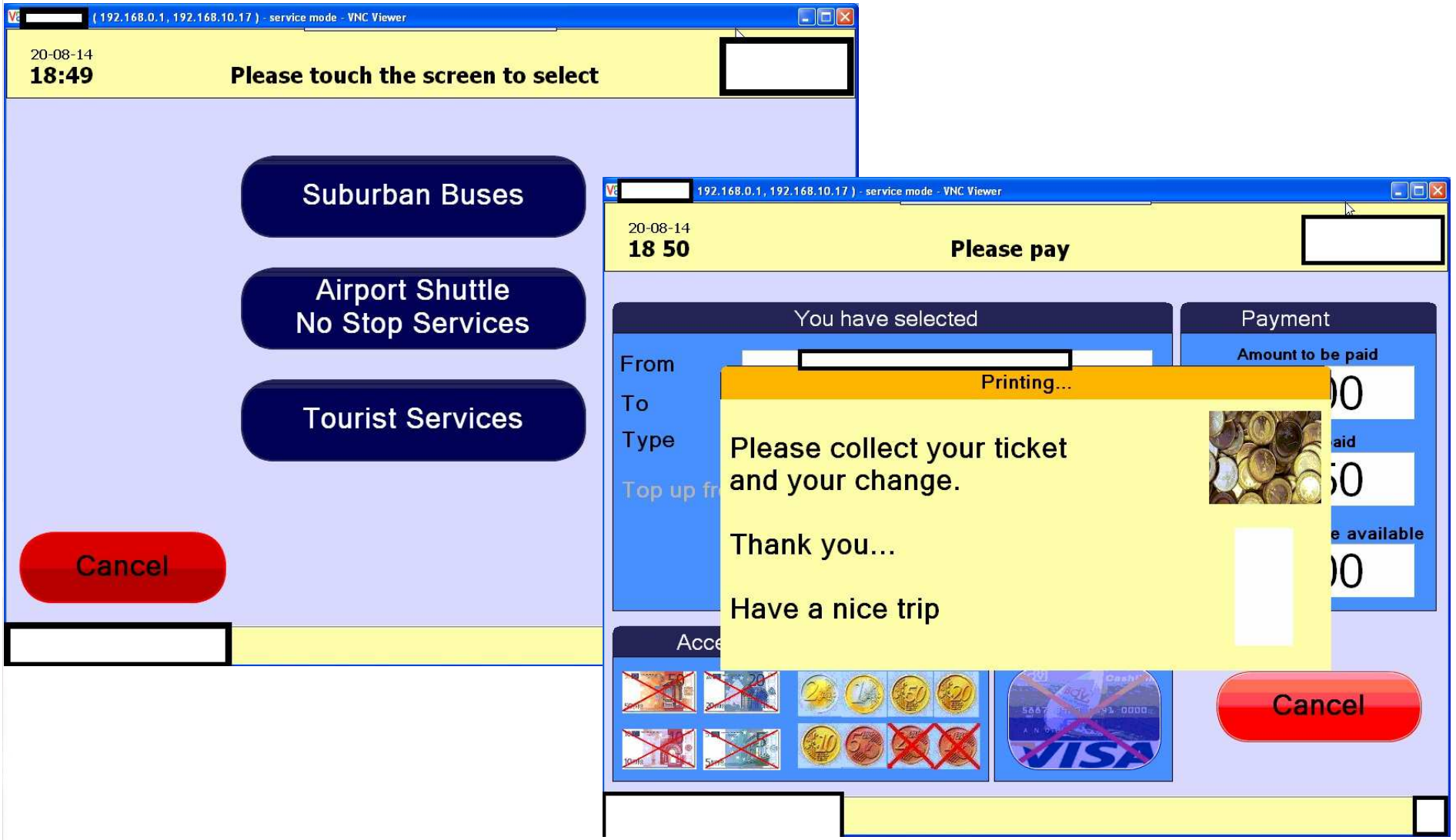
JackPOS, «primi giorni di vita»

Cards, POS (Totem), NFC

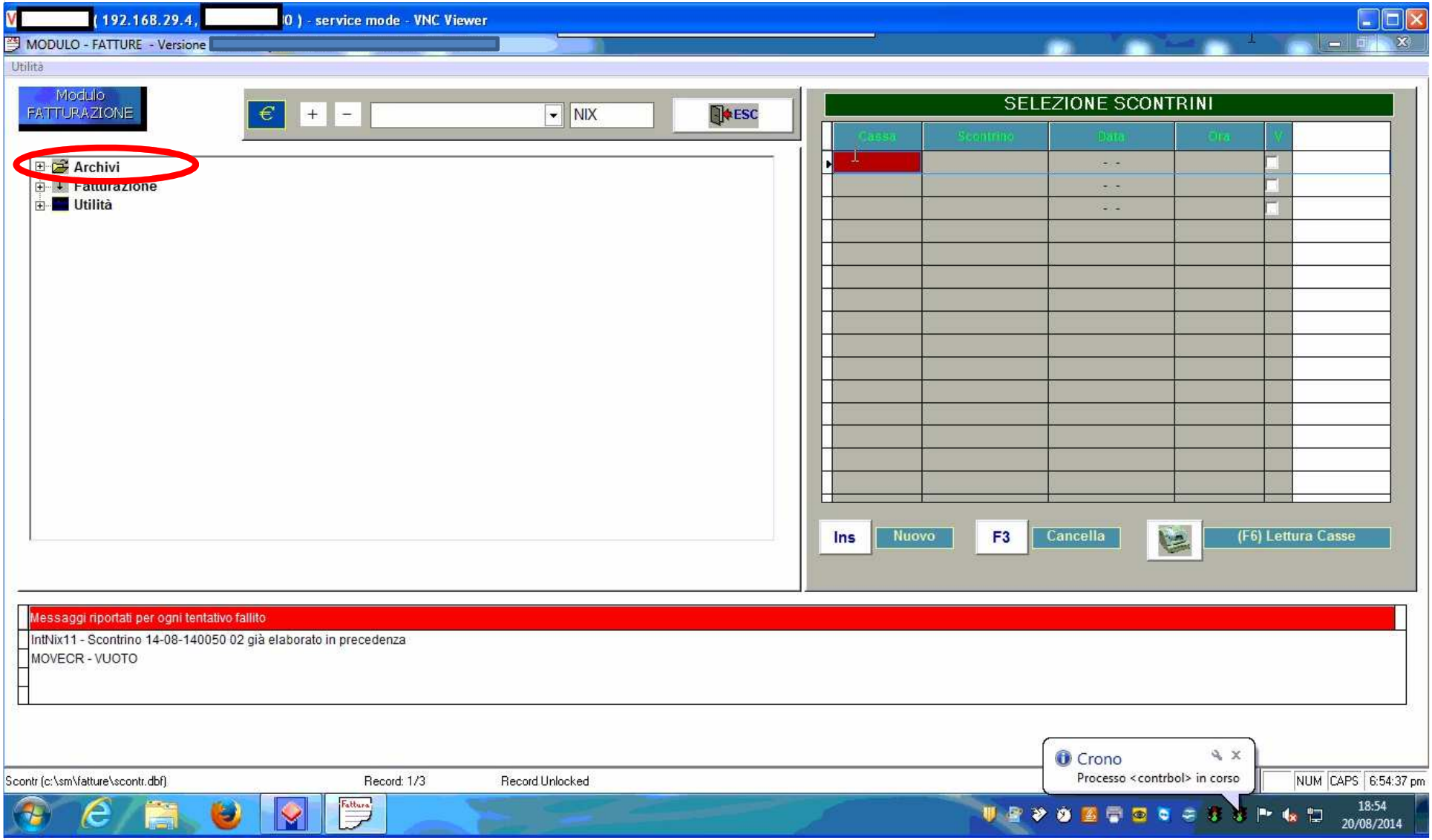




Cards, POS (Totem), NFC



Cards, POS (Totem), NFC



Cards, POS (Totem), NFC

- ANSA, 29 settembre 2014

http://www.ansa.it/sito/notizie/tecnologia/software_app/2014/09/29/parcheggi-e-biglietterie-nuovo-obiettivo-hacker_8c6b810d-c10e-45b7-9fd0-839bff92b5b0.html

EDIZIONI ANSA > Mediterraneo | Europa | NuovaEuropa | Latina | Brasil | English | Realestate

ANSA.it Software&App

Fai la ricerca

Cronaca | Politica | Economia | Regioni + | Mondo | Cultura | Tecnologia

PRIMOPIANO • HI-TECH • INTERNET & SOCIAL • TELECOMUNICAZIONI • SOFTWARE & APP

ANSA.it › Tecnologia › Software & App › Parcheggi e biglietterie, nuovo obiettivo hacker

Parcheggi e biglietterie, nuovo obiettivo hacker

Esperto, carte credito ora clonate da 'totem' casse automatiche

Titti Santamato

29 settembre 2014
20:27
ANALISI

Suggerisci
Facebook
Twitter
Google+
Altri
A+ A A-
Stampa
Scrivi alla redazione

Parcheggi e biglietterie, nuovo obiettivo hacker

CLICCA PER INGRANDIRE

Non solo bancomat, acquisti via Internet e transazioni di e-banking, nel mirino degli hacker ci sono ora le casse automatiche, quelle che comunemente usiamo per fare un biglietto del treno in stazione o per pagare il parcheggio in città. A lanciare l'allarme un team Usa-italiano di esperti nel settore sicurezza.

"Stiamo seguendo da diversi mesi le tracce di svariati gruppi di cybercriminali che si sono specializzati nelle frodi via Pos. Esistono da anni ma quello che è cambiato è il modus operandi di questi gruppi

Cash out


Extracted Track 2 Data
1
Credit Cards Preparation
2
"Money Mules" Orders
3
Converting into real money
4

Cards, POS, NFC

La beffa dei pagamenti con il cellulare all'avanguardia sì, ma facili da hackerare

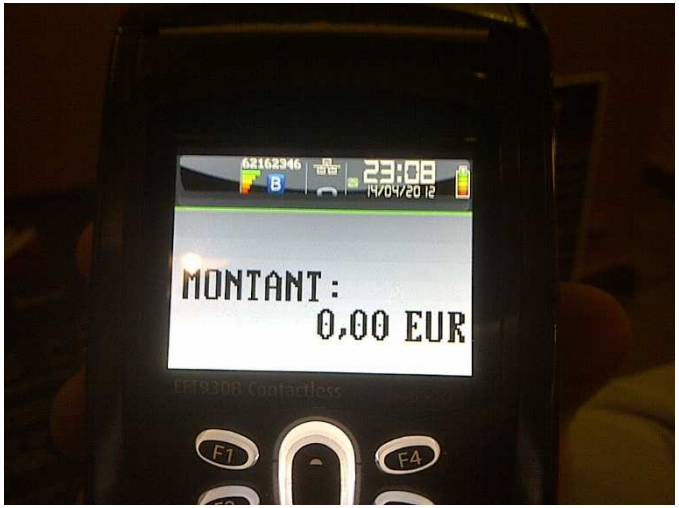
La fretta di introdurre i sistemi Nfc, che permettono di pagare con lo smartphone nei negozi, ha aperto una **falla di sicurezza**: i **dati non vengono crittografati** e quindi **si possono rubare**. Ma **non è un problema dell'Nfc**, garantiscono gli esperti. E in Italia siamo al sicuro, **solo perché ancora non sono attivi questi servizi**.

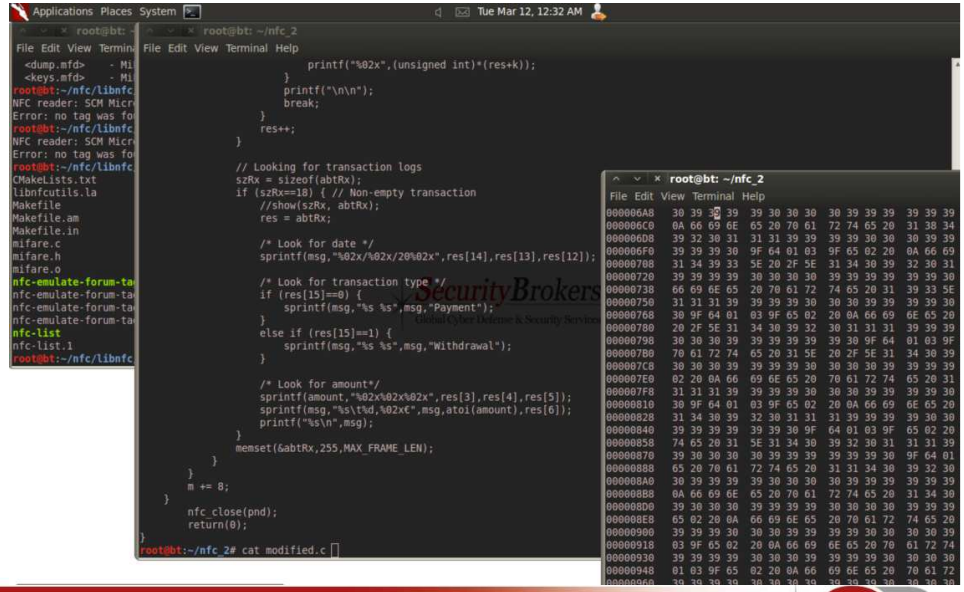
http://www.repubblica.it/tecnologia/2012/08/07/news/rischi_pagamenti_nfc-40330153/?ref=fbpr

By la Repubblica.it - Tecnologia, 7 agosto 2012

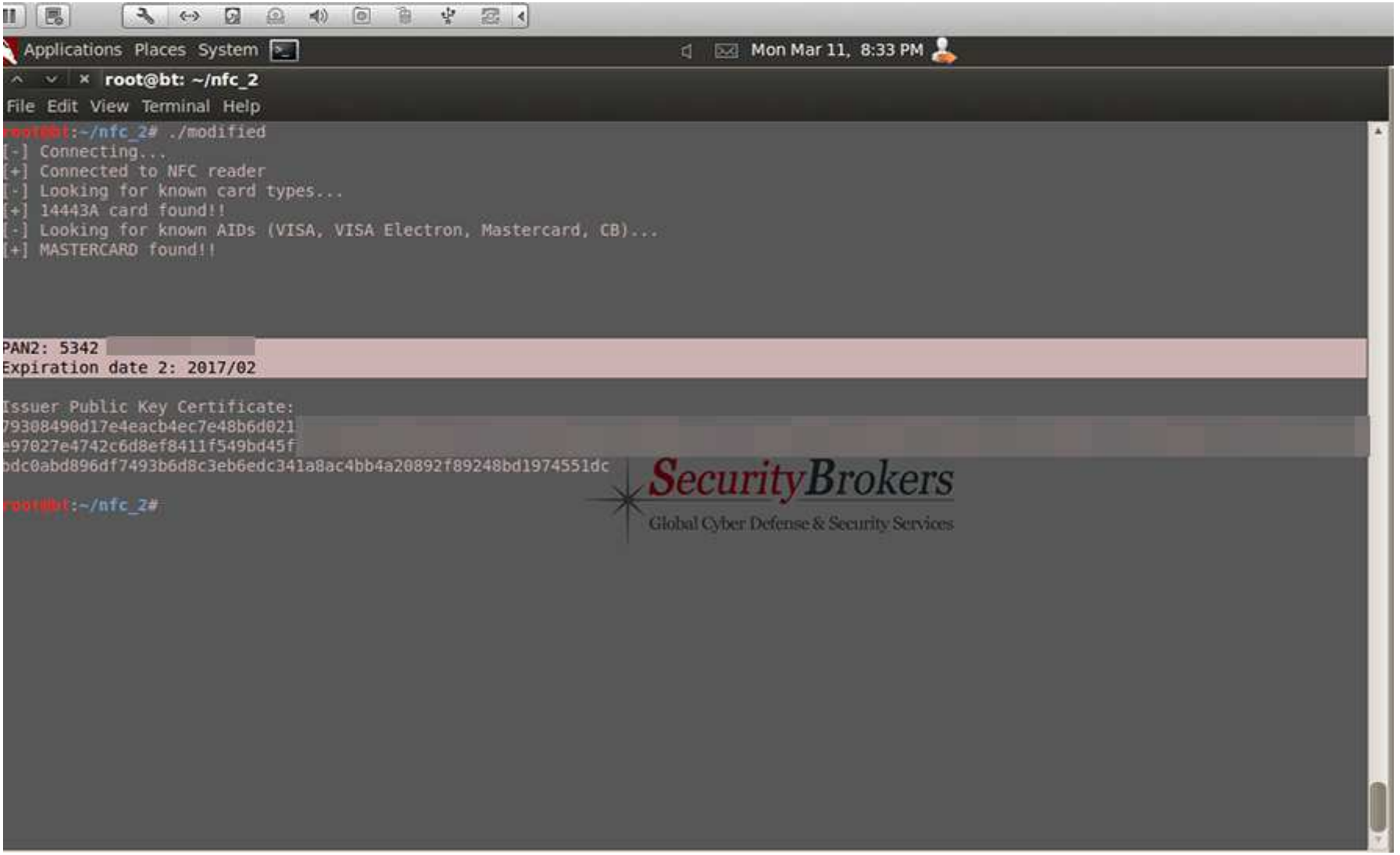
Cards, POS, NFC

Hacking the NFC credit cards for fun and debit ;)





Cards, POS, NFC



Cards, POS, NFC

Vulnerabilities, Problems, Bugs & Misconfigurations

SOFTWARE

- Device Software (Reader & Writer) - Vulnerabilities
- Management Software (UI, Console & GUI) – Core Vulnerabilities
- 3rd Party Clients with influence on the live process of a NFC using box with direct communication as exchange
- GiroGo Card of Sparkasse with last saved 15 trans action readable for attackers

.HARDWARE

- Sniffing (Pocket 4-5cm) via MITM Attack (Mobile Phones)
- Sniffing (DB Wifi) via MITM & Sticker + Chip to skim the data
- Programmable NFC-Tags manipulation for Applications Communication
- Programmable NFC-Chips with manipulated configurations settings
- NFC Protocol – Misconfiguration(s) & Bugs
- Datasecurity breach by saving the last 15 transactions
- CVC3-Codes (Replay Attack Vector)

Cards, POS, NFC

```
$ ./readnfccc
Cardholder name [redacted]
PAN: 4970 [redacted] 2586
Expiration date: 12/2013

07/04/2012 Payment      24,50€
06/04/2012 Payment      73,00€
05/04/2012 Withdrawal   60,00€
05/04/2012 Payment      7,85€
02/04/2012 Payment      6,95€
30/03/2012 Payment      30,00€
30/03/2012 Withdrawal   60,00€
30/03/2012 Payment      59,90€
26/03/2012 Payment      70,00€
24/03/2012 Payment      40,88€
23/03/2012 Payment      108,07€
21/03/2012 Payment      47,00€
20/03/2012 Payment      9,40€
14/03/2012 Payment      48,00€
14/03/2012 Payment      18,35€
14/03/2012 Payment      35,50€
11/03/2012 Payment      21,00€
11/03/2012 Payment      24,50€
11/03/2012 Withdrawal   90,00€
11/03/2012 Payment      45,00€
------------------------
```

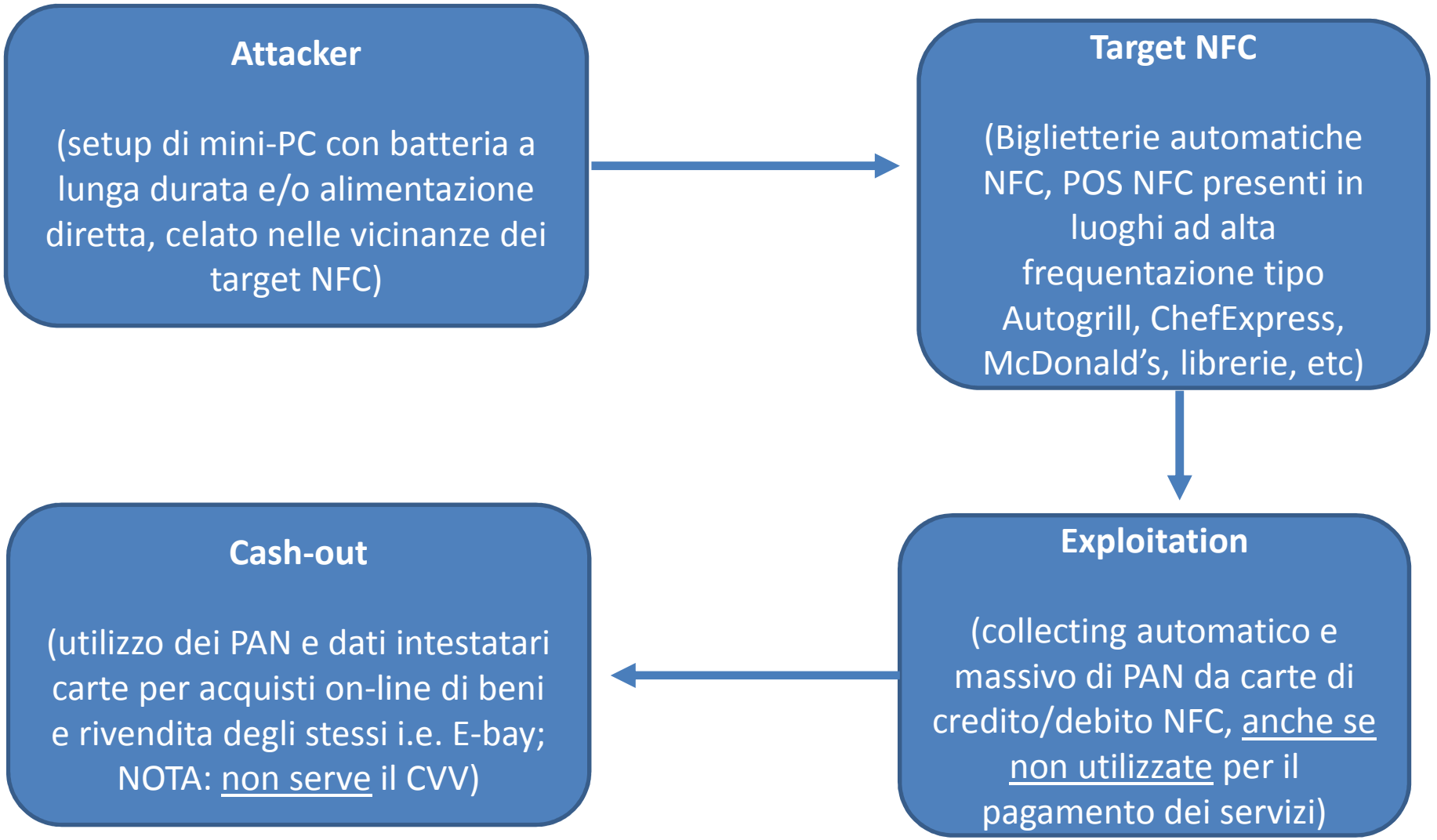
Mass-Carding

La limitazione all'importo pagabile mediante NFC potrebbe causare una **sottovalutazione del problema**.

In realtà, **proprio grazie alla spinta data** dal marketing e dalle promozioni per **invogliare l'utente a pagare con la carta NFC**, si possono disegnare **scenari criminosi** di «Mass-Carding» e conseguente **industrializzazione del cash-out**.

D'altr'onde, basta leggere un libro come «**Kingpin**» (Kevin Poulsen, Hoepli editore) per rendersi conto di come i modelli «classici» di cash-out **si applicano perfettamente** anche ai «dump» di carte NFC-based, **senza dover compromettere** il lettore NFC (POS, etc).

Modello criminoso per il cash-out massivo

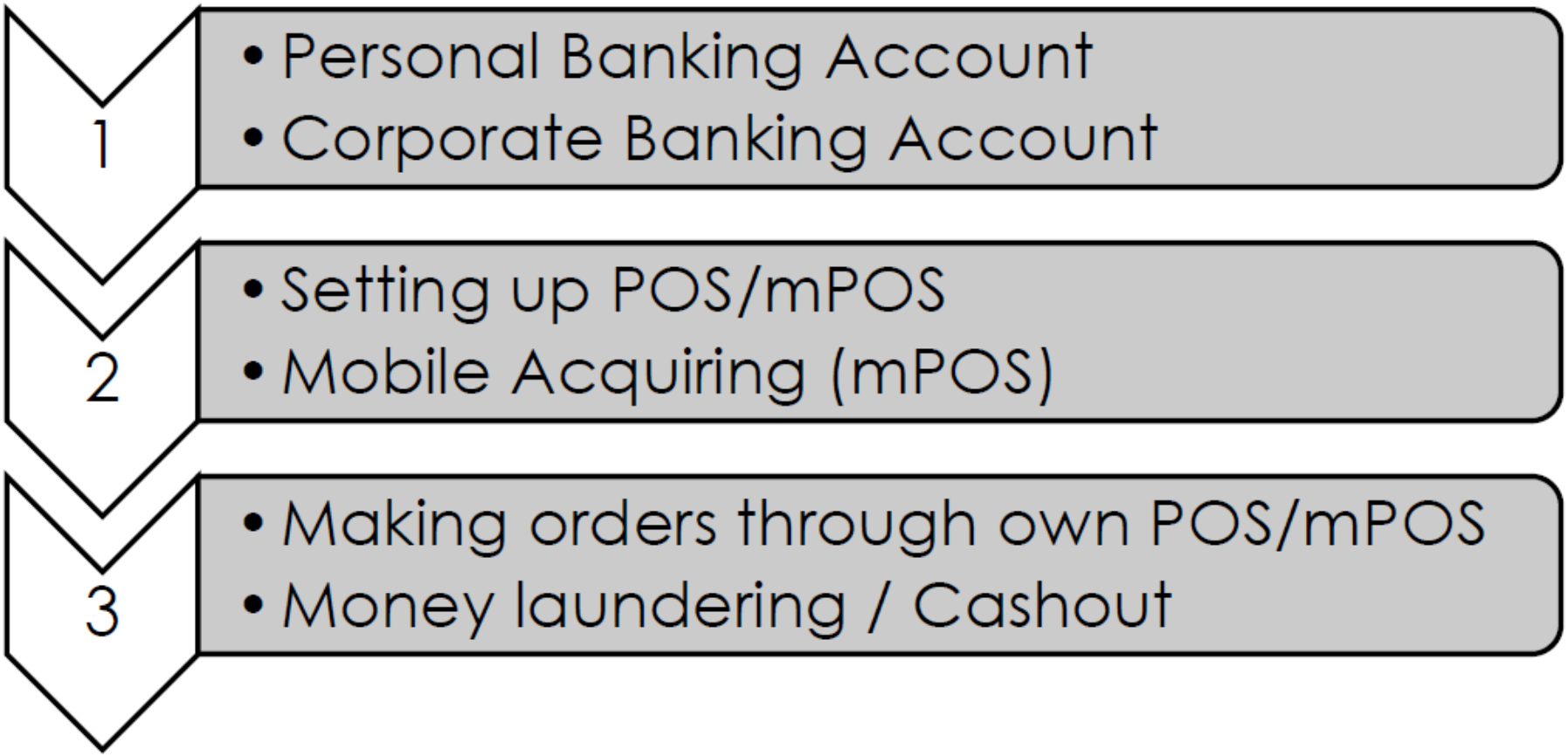


Cosa cambia

- E' all'ordine del giorno che **TTP** (third-trusted party) **vengano violate** a scapito dell'istituto bancario e finanziario, come ad esempio i **Card Processing Center** (gli esempi sono purtroppo decine e decine in tutto il mondo):
  - **Monitoring 24x7 di portali («open» e «chiusi») del Black Market e del mondo del Cybercrime per la pubblicazione di Carte di Credito emesse dal cliente Banca (identificate tramite BIN); identificazione dei Money Mules e C/C utilizzati.**
- E' all'ordine del giorno che il **cliente finale** dell'istituzione finanziaria venga violato (malware, trojan, key loggers, botnet, etc):
  - **Monitoring 24x7 di malicious traffic; intercettazione di Botnet e di sistemi di Command&Control posti alla compravendita delle credenziali e-banking (Token ed OTP inclusi), e-commerce (carte di credito/debito) del cliente finale e credenziali e-mail.**
- E' all'ordine del giorno che **dispositivi attended** ed **unattended**, quali **POS** e **Totem di pagamento**, vengano compromessi ed i flussi di carte di credito/debito intercettati:
  - **Monitoring 24x7 di malicious traffic; intercettazione di Botnet e di sistemi di Command&Control posti alla compravendita degli accessi non autorizzati verso POS e Totem di pagamento.**

Money Laundering mediante POS/mPOS

Modello criminoso per l'auto riciclaggio



Cyber Intelligence: what you get?

Deliverables

✳ Anti Money Laundering Intelligence feed

Monitoraggio di **migliaia di organizzazioni ed individui** coinvolti in **attività fraudolente** e **riciclaggio di denaro** in **tutto il mondo**.

Avere accesso ai feed mette in sicurezza il vostro business e previene i rischi da attività di riciclaggio (Money Mules per il mercato Banking, Gambling, Pharmacy, etc).

✳ Triple «C» feed

Feed sulle **liste di Carte di Credito Compromesse** che vengono «scovate» nei **Black Market** e nel **Digital Underground** e pronte ad essere utilizzate in modo fraudolento.

✳ POS feed

Feed sui **POS** o **reti POS** compromessi, informando sul **numero approssimativo di Carte di Credito** compromesse, **geo-localizzazione** grafica e gli **Indirizzi IP dei terminali infettati**, siano essi **POS**, **Totem**, etc.

Conclusions

Conclusions

- Il mondo bancario deve effettuare un **cambio totale di visione**, ponendo l'attenzione verso nuove tipologie di servizi di informazione, che si pongono a totale supporto dell'antifrode «classica».

- Il Cliente va difeso oltre il classico «perimetro» bancario.

- Mai come oggi è **essenziale essere un passo avanti** al Cybercrime.
  - I benefici per l'istituto bancario possono essere **molteplici**:
    - Immagine
    - Prevenzione frodi
    - Non superamento del tetto coperto dall'insurance
    - …….

Reading room /1

Kingpin: la storia della più grande rapina digitale del secolo, Kevin Poulsen, Hoepli, 2013

Fatal System Error: the Hunt for the new Crime Lords who are bringing down the Internet, Joseph Menn, Public Affairs, 2010

Profiling Hackers: the Science of Criminal Profiling as applied to the world of hacking, Raoul Chiesa, Stefania Ducci, Silvio Ciappi, CRC Press/Taylor & Francis Group, 2009

H.P.P. Questionnaires 2005-2010

Stealing the Network: How to 0wn a Continent, (an Identity), (a Shadow) (V.A.), Syngress Publishing, 2004, 2006, 2007

Stealing the Network: How to 0wn the Box, (V.A.), Syngress Publishing, 2003

Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier, Suelette Dreyfus, Random House Australia, 1997

The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, Clifford Stoll, DoubleDay (1989), Pocket (2000)

Masters of Deception: the Gang that Ruled Cyberspace, Michelle Stalalla & Joshua Quinttner, Harpercollins, 1995

Kevin Poulsen, Serial Hacker, Jonathan Littman, Little & Brown, 1997

Takedown, John Markoff and Tsutomu Shimomura, Sperling & Kupfler, (Hyperion Books), 1996

The Fugitive Game: online with Kevin Mitnick, Jonathan Littman, Little & Brown, 1997

The Art of Deception, Kevin D. Mitnick & William L. Simon, Wiley, 2002

The Art of Intrusion, Kevin D. Mitnick & William L. Simon, Wiley, 2004

@ Large: the Strange Case of the World's Biggest Internet Invasion, Charles Mann & David Freedman, Touchstone, 1998

Reading room /2

The Estonia attack: Battling Botnets and online Mobs, Gadi Evron, 2008 (white paper)

Who is "n3td3v"?, by Hacker Factor Solutions, 2006 (white paper)

Mafiaboy: How I cracked the Internet and Why it's still broken, Michael Calce with Craig Silverman, 2008

The Hacker Diaries: Confessions of Teenage Hackers, Dan Verton, McGraw-Hill Osborne Media, 2002

Cyberpunk: Outlaws and Hackers on the Computer Frontier, Katie Hafner, Simon & Schuster, 1995

Cyber Adversary Characterization: auditing the hacker mind, Tom Parker, Syngress, 2004

Inside the SPAM Cartel: trade secrets from the Dark Side, by Spammer X, Syngress, 2004

Hacker Cracker, Ejovu Nuwere with David Chanoff, Harper Collins, 2002

Compendio di criminologia, Ponti G., Raffaello Cortina, 1991

Criminalità da computer, Tiedemann K., in Trattato di criminologia, medicina criminologica e psichiatria forense, vol.X, Il cambiamento delle forme di criminalità e devianza, Ferracuti F. (a cura di), Giuffrè, 1988

United Nations Manual on the Prevention and Control of Computer-related Crime, in International Review of Criminal Policy – Nos. 43 and 44

Criminal Profiling: dall'analisi della scena del delitto al profilo psicologico del criminale, Massimo Picozzi, Angelo Zappalà, McGraw Hill, 2001

Deductive Criminal Profiling: Comparing Applied Methodologies Between Inductive and Deductive Criminal Profiling Techniques, Turvey B., Knowledge Solutions Library, January, 1998

Malicious Hackers: a framework for Analysis and Case Study, Laura J. Kleen, Captain, USAF, US Air Force Institute of Technology

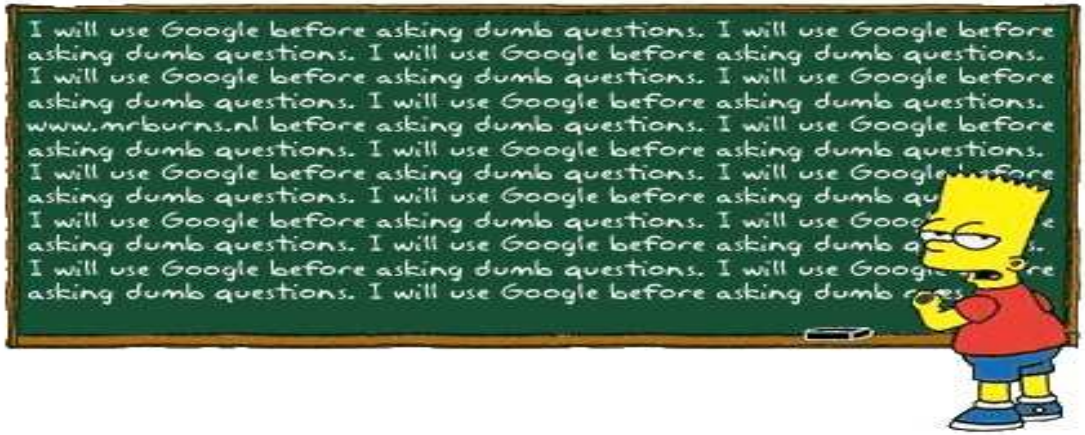
Criminal Profiling Research Site. Scientific Offender Profiling Resource in Switzerland. Criminology, Law, Psychology, Täterpro

Contacts, Q&A

- **Need** anything, got **doubts**, wanna **ask me something**?
  - rc [at] security-brokers [dot] com
  - Public key: http://www.security-brokers.com/keys/rc_pub.asc

Thanks for your attention!

QUESTIONS?



Extra Material

Profiling Hackers

HPP – The Hacker's Profiling Project

HPP V1.0: purposes & goals

unicri
advancing security, serving justice, building peace

Analyse the hacking phenomenon in its several aspects (technological, social, legal, economical) through technical and criminological approaches.

Understand the different motivations and identify the actors involved (who, not "how").

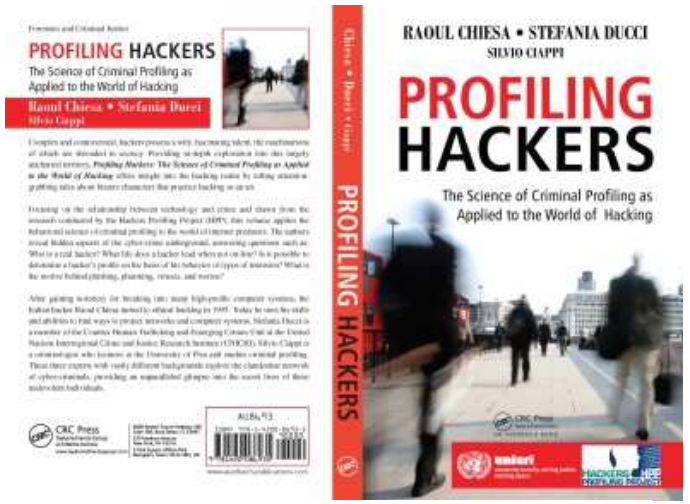
Observe those *true* criminal actions "on the field"

Apply the profiling methodology to collected data (4W: who, where, when, why).

Acquire and disseminate knowledge.

HPP V1.0

- Nel **2004** all'UNICRI abbiamo lanciato l'Hacker's Profiling Project - HPP: http://www.unicri.it/special_topics/cyber_threats/
- Da quell'anno e sino al 2010:
  - **+1.200 questionari** raccolti ed analizzati
  - **9 profili hacker** emersi
  - **Due libri** (uno in inglese)
    - Profilo Hacker, Apogeo, 2007
    - Profiling Hackers: the Science of Criminal Profiling as Applied to the World of Hacking, Taylor&Francis Group, CRC Press (2009)
    - Il **riconoscimento** della nostra **Intelligence nazionale**



unicri
advancing security, serving justice, building peace

SISTEMA DI INFORMAZIONE PER LA SICUREZZA DELLA REPUBBLICA
a protezione degli interessi politici, militari, economici, scientifici ed industriali dell'Italia

Standard di valutazione e correlazione

- Modus Operandi (MO)
- Lone hacker or as a member of a group
- Motivations
- Selected targets
- Relationship between motivations and targets
- Hacking career
- Principles of the hacker's ethics
- Crashed or damaged systems
- Perception of the illegality of their own activity
- Effect of laws, convictions and technical difficulties as a deterrent

Mainly from:
USA
Italy
UK
Canada
Lithuania
Australia
Malaysia
Germany
Brazil
Romania
China

unicri
advancing security, serving justice, building peace

HPP v1.0 - Zoom: correlation standards

Gender and age group

Background and place of residence

How hackers view themselves
Family background

Socio-economic background
Social relationships

Leisure activities

Education

Professional environment
Psychological traits

To be or to appear: the level of self-esteem
Presence of multiple personalities

Psychophysical conditions
Alcohol & drug abuse and dependencies
Definition or self-definition: what is a real hacker?
Relationship data

Handle and nickname

Starting age

Learning and training modalities
The mentor's role

Technical capacities (know-how)
Hacking, phreaking or carding: the reasons behind the choice
Networks, technologies and operating systems
Techniques used to penetrate a system

Individual and group attacks
The art of war: examples of attack techniques
Operating inside a target system
The hacker's signature
Relationships with the System Administrators
Motivations

The power trip
Lone hackers
Hacker groups
Favourite targets and reasons
Specializations
Principles of the Hacker Ethics
Acceptance or refusal of the Hacker Ethics
Crashed systems
Hacking/phreaking addiction
Perception of the illegality of their actions
Offences perpetrated with the aid of IT devices
Offences perpetrated without the use of IT devices
Fear of discovery, arrest and conviction
The law as deterrent
Effect of convictions

Leaving the hacker scene
Beyond hacking

I 9 profili emersi

unicri
advancing security, serving justice, building peace

Profile	OFFENDER ID	LONE / GROUP HACKER	TARGET	MOTIVATIONS / PURPOSES
Wanna Be Lamer	9-16 years "I would like to be a hacker, but I can't"	GROUP	End-User	For fashion, It's "cool" => to boast and brag
Script Kiddie	10-18 years The script boy	GROUP: but they act alone	SME / Specific security flaws	To give vent of their anger / attract mass-media attention
Cracker	17-30 years The destructor, burned ground	LONE	Business company	To demonstrate their power / attract mass-media attention
Ethical Hacker	15-50 years The "ethical" hacker's world	LONE / GROUP (only for fun)	Vendor / Technology	For curiosity (to learn) and altruistic purposes
Quiet, Paranoid, Skilled Hacker	16-40 years The very specialized and paranoid attacker	LONE	On necessity	For curiosity (to learn) => egoistic purposes
Cyber-Warrior	18-50 years The soldier, hacking for money	LONE	"Symbol" business company / End-User	For profit
Industrial Spy	22-45 years Industrial espionage	LONE	Business company / Corporation	For profit
Government Agent	25-45 years CIA, Mossad, FBI, etc.	LONE / GROUP	Government / Suspected Terrorist/ Strategic company/ Individual	Espionage/ Counter-espionage Vulnerability test Activity-monitoring
Military Hacker	25-45 years	LONE / GROUP	Government / Strategic company	Monitoring / controlling / crashing systems

HPP v2.0: cos'è successo?

- E' molto **semplice**…
  - **Stiamo cercando fondi (Donors)**: per le fasi progettuali 3 e 4 abbiamo bisogno di supporto!
    - HW, SW, Analisti, Traduttori

- Abbiamo iniziato nel **2004**: c'erano ancora i «romantic hackers», ma avevamo già previsto «nuovi» attori: **.GOV**, **.MIL, Intelligence.**

- Ci siamo «**persi**»:
  - Hacktivism (!);
  - Cybercriminals al di là dell'approccio «hobbistico» (industrializzazione);
  - Organized Crime (OC);
  - Gli aspetti economici (Follow the Money!!);
  - I Cyberterroristi (esistono veramente?)

unicri
advancing security, serving justice, building peace

HPP v2.0: prossime integrazioni

unicri
advancing security, serving justice, building peace

Going after Cybercriminals:

- **Kingpins & Master minds** (the "Man at the Top")
  - Organized Crime
  - MO, Business Model, Kingpins – "How To"
- **Techies hired by the Organized Crime** (i.e. Romania & skimming at the very beginning; Nigerian cons 419-like; Ukraine Rogue AV; Pharma ADV Campaigns; ESTDomains in Estonia; **POS malware**; etc..)
- **Structure, Infrastructures** (links with Govs & Mils?)
- **Money Laundering: Follow the money** (E-mules & new ways to "cash-out": **mPOS**, **vPOS**, etc..)
- **Outsourcing: malware factories** (Stuxnet? DuQu?? Lingbo? E tutti gli altri…?)

HPP v2.0: prossime integrazioni (esempi)

1. Wannabe/Lamer
2. Script kiddie: under development (Web Defacers, DDoS, links with distributed teams i.e. Anonymous….)
3. Cracker: under development (Hacking on-demand, "outsourced"; links with Organized Crime)
4. Ethical hacker: under development (security researchers, ethical hacking groups)
5. Quiet, paranoid, skilled hacker (*elite*, unexplained hacks? Vodafone GR? NYSE? Lybia TLC systems?)
6. Cyber-warrior: to be developed
7. Industrial spy: to be developed (links with Organized Crimes & Governments i.e. Comodo, DigiNotar and RSA hacks?)
8. Government agent: to be developed ("N" countries..)
9. Military hacker: to be developed (India, China, N./S. Korea, etc.)

X. Money Mules? Ignorant "DDoSsers"? (i.e. LOIC by Anonymous)

unicri
advancing security, serving justice, building peace