SESSIONE PLENARIA: LE NUOVE SFIDE DEL CYBERCRIME

L'evoluzione della sicurezza logica: dal cyber espionage alle frodi massive e globali nel mondo Finance

Raoul Chiesa

President, Security Brokers SCpA

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

- Presentazioni
- Cybercrime
- Evolving scenarios in the counter-fraud Banking Environments:
  - Cards
  - POS
  - NFC
- Cyber Intelligence (open e closed)
- Conclusioni
- Reading Room
- Contacts

Introductions

Il relatore

- President, Founder, Security Brokers
- Principal, CyberDefcon Ltd.
- Independent Senior Advisor on Cybercrime @ UNICRI (United Nations Interregional Crime & Justice Research Institute)
- Fomer 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

- 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:
  - **Experts brokering, guru speaking**
  - **Proactive Security**
    - con forte specializzazione su Banking&Finance, 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 terminologie

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**.

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

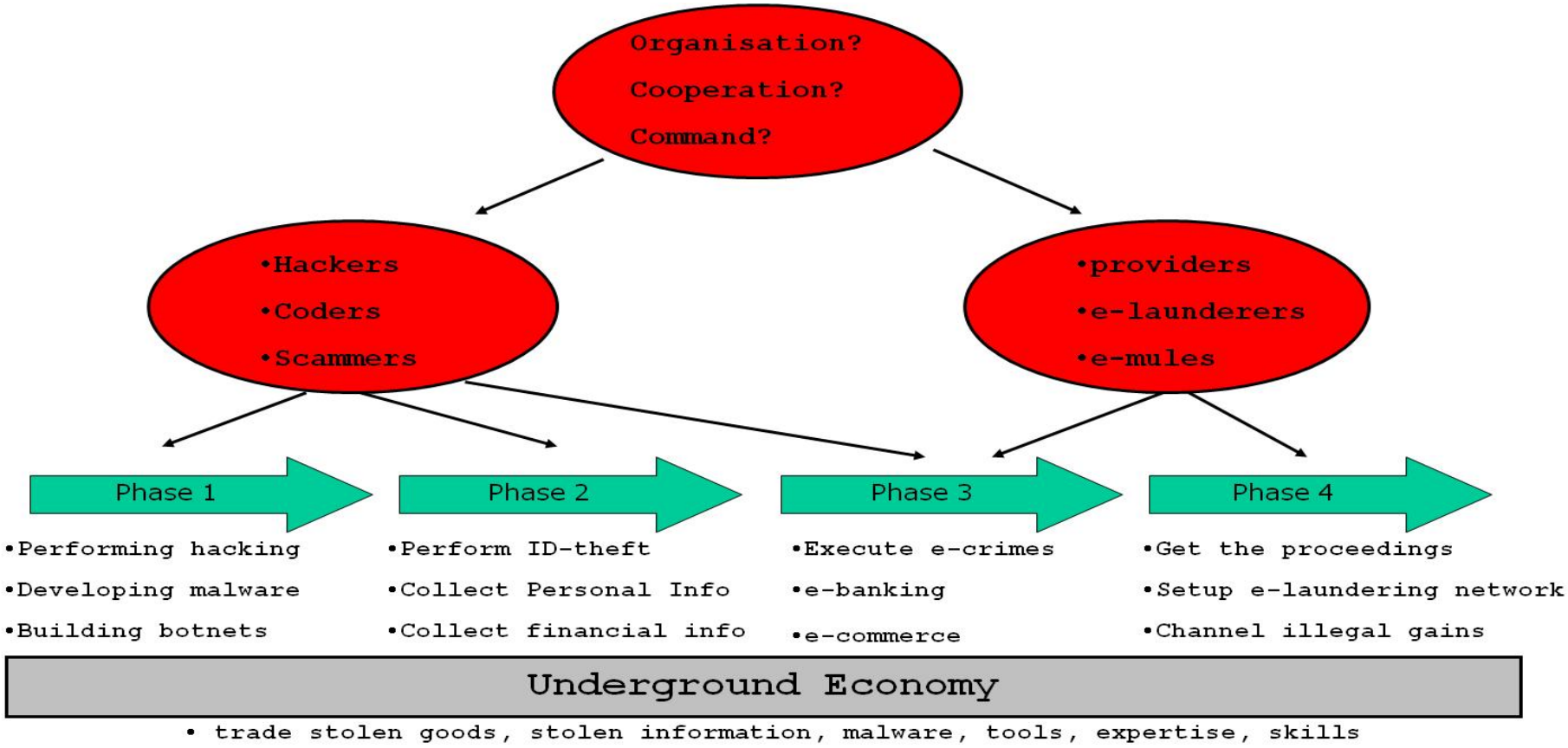
*Hai l'**informazione, information**, hai il **potere**..*

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)**

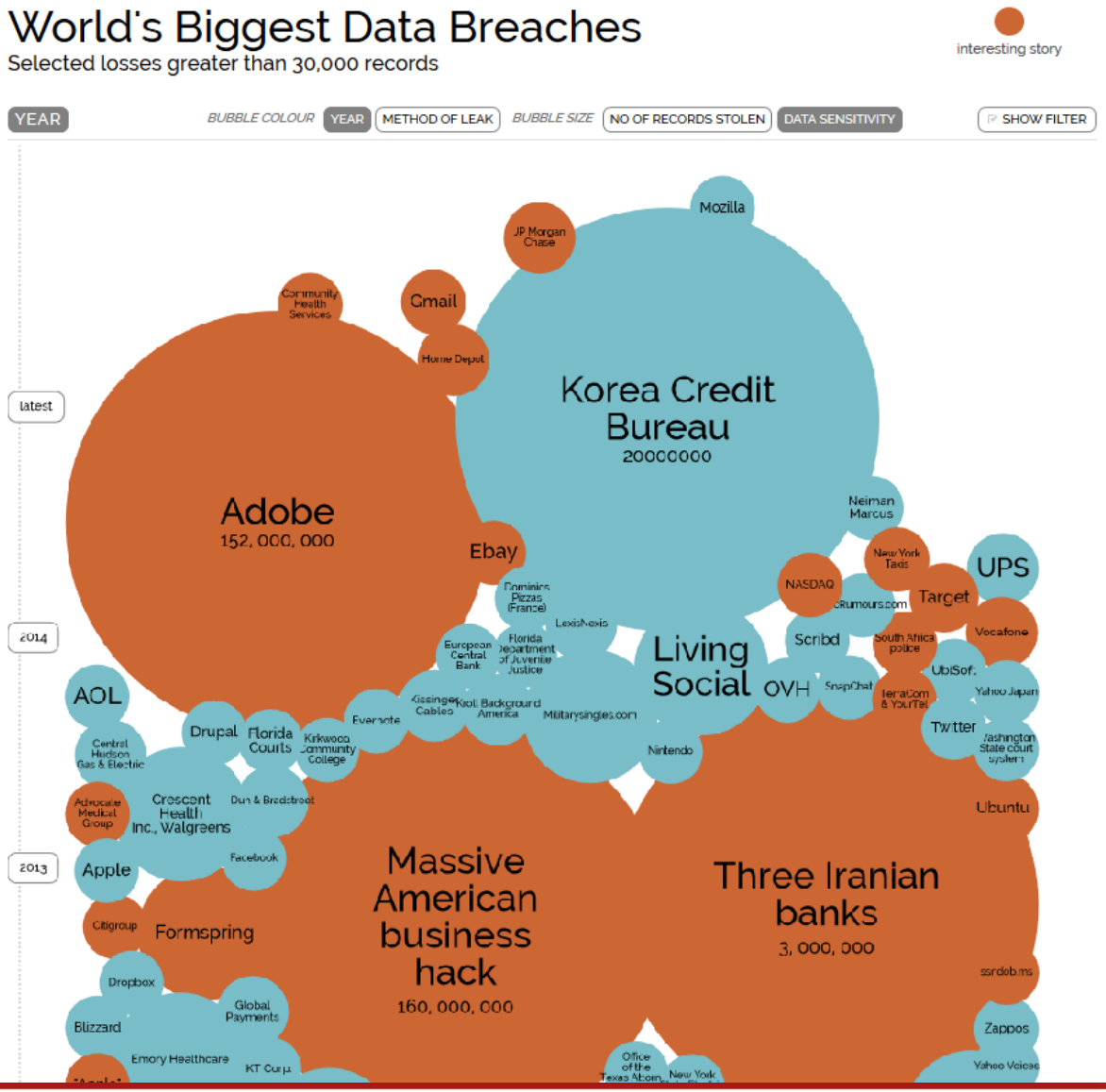
- Ecco perché tutti noi vogliamo «essere sicuri".
- Non è un caso se si chiama «IS» : **Information Security** ☺
  - La **moda** «cyber-prefisso» è d'altr'onde una novità degli **anni recenti**.

Cybercrime: Modus Operandi (MO)



Data Breaches & Cyber Espionage

Data Breach



Filter by...

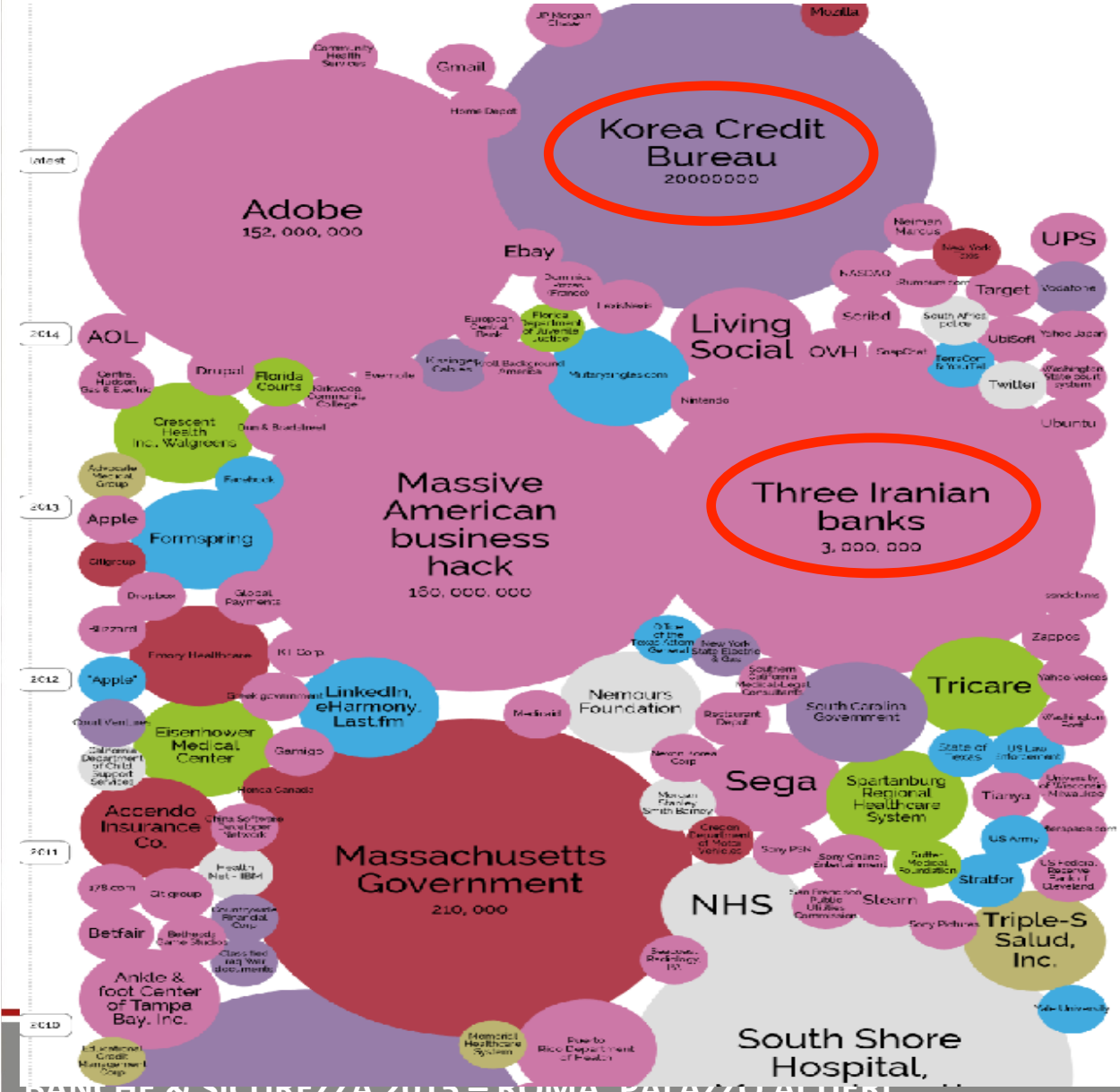
ORGANISATION

- [x] all
- [ ] academic
- [ ] energy
- [ ] financial
- [ ] gaming
- [ ] government
- [ ] healthcare
- [ ] media
- [ ] military
- [ ] retail
- [ ] tech
- [ ] telecoms
- [ ] transport
- [ ] web

METHOD OF LEAK

- [x] all
- [ ] accidentally published
- [ ] hacked
- [ ] inside job
- [ ] lost / stolen computer
- [ ] lost / stolen media
- [ ] poor security

Ops… it wasn't complete!



Filter by...

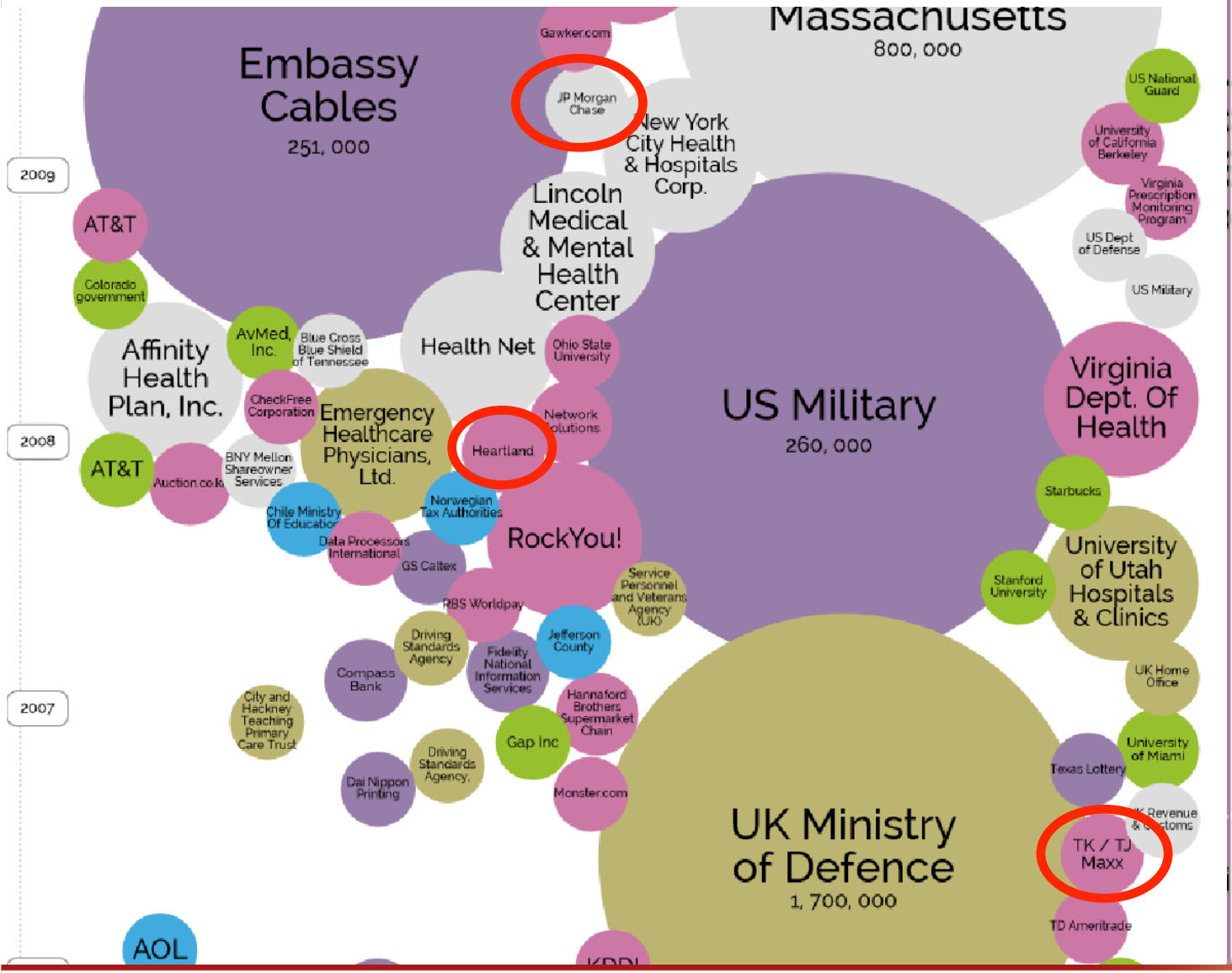
ORGANISATION

- all
- academic
- energy
- financial
- gaming
- government
- healthcare
- media
- military
- retail
- tech
- telecoms
- transport
- web

METHOD OF LEAK

- all
- accidentally published
- hacked
- inside job
- lost / stolen computer
- lost / stolen media
- poor security

Ops… it wasn't complete!



Filter by...

ORGANISATION

- all
- academic
- energy
- financial
- gaming
- government
- healthcare
- media
- military
- retail
- tech
- telecoms
- transport
- web

METHOD OF LEAK

- all
- accidentally published
- hacked
- inside job
- lost / stolen computer
- lost / stolen media
- poor security

Ops… it wasn't complete!

Filter by...

ORGANISATION

- all
- academic
- energy
- financial
- gaming
- government
- healthcare
- media
- military
- retail
- tech
- telecoms
- transport
- web

METHOD OF LEAK

- all
- accidentally published
- hacked
- inside job
- lost / stolen computer
- lost / stolen media
- poor security

La nostra analisi

- Le «world's biggest data breaches» sono state **così tante**, dal 2004 ad oggi, **che non stanno nemmeno su un'unica pagina** ☹
- Maggiori dettagli qui:
  - http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
- Stiamo parlando di un'escalation **senza fine**
- **Nessuno ne è escluso. Non più**
  - Inoltre, **iniziamo a dipendere davvero tanto dal M2M**
- **Informazione = Potere**.
  - Il **danno causato da queste violazioni** è spesso difficile da calcolare
  - Danni **operativi, di business, di immagine, economici** (**rimborsi** ai clienti, **multe dalle Authority**).

La nostra analisi / 2

Insieme al mio team abbiamo **analizzato tutti questi incidenti**.

I **Key drivers** al **successo** degli **attaccanti** possono essere riassunti come segue:

- **Lack of professionally-run Security Testings** (penetration test, ethical hacking, compliance check).
- **Lack of segregation** on **internal networks**.
- **Missing for a correct, centralized management** of **SSH keys**, both **external and internal ones.**
- **Missing of tools** for **Data Leak Prevention (DLP)** on **encrypted connections (SSH tunnels).**
- **Missing of the right sources for Cyber Intelligence (OSINT, Closed-sources)**
- **Lack of internal awareness.**
- **Lack or total miss of tools, methodologies and trainings on Digital Forensics.**
- **Poor programming / Lack of Secure Coding.**

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

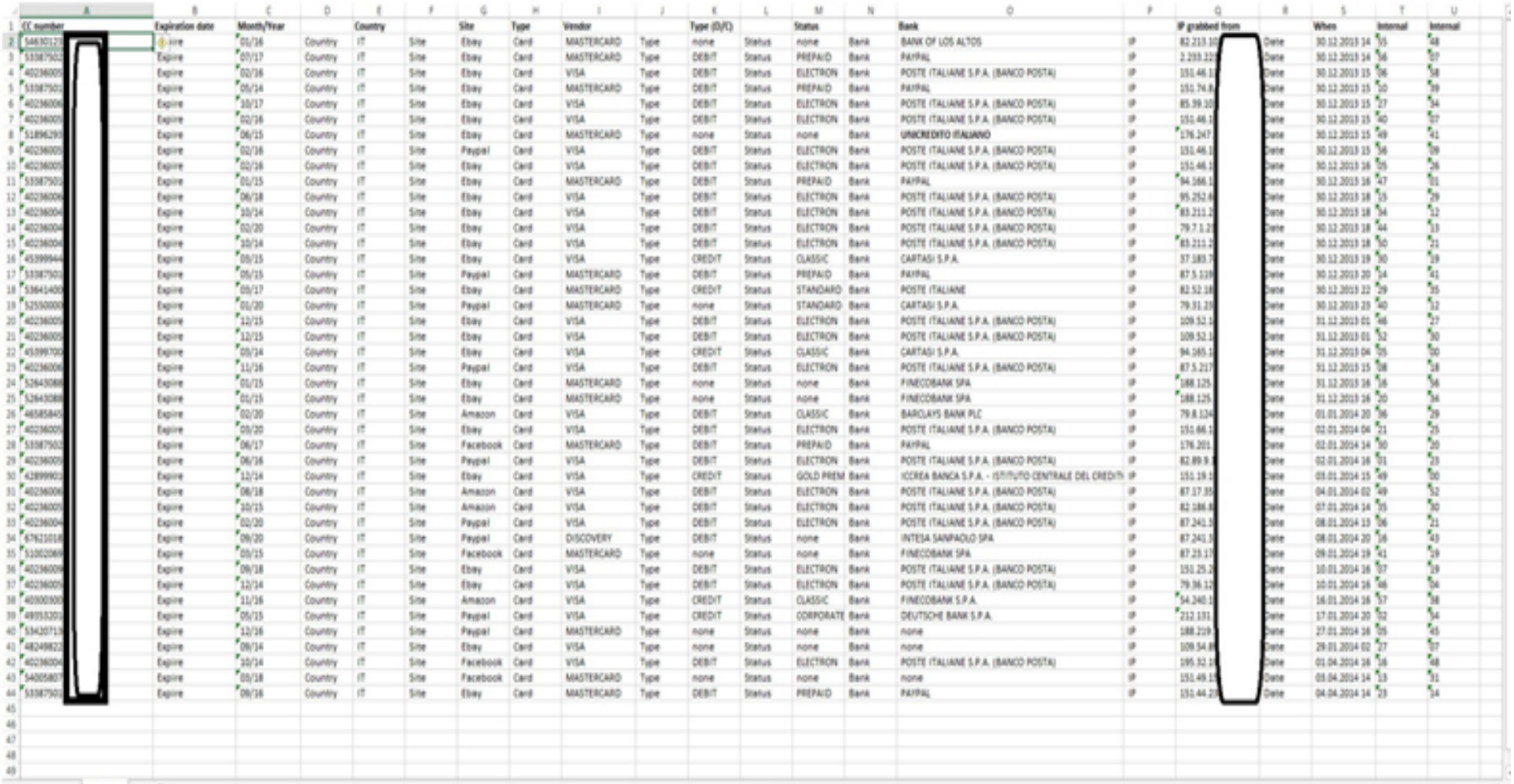
- Allo stesso modo, il mondo bancario ha **dovuto rivedere i propri approcci antifrode**.
- **Oggi** è:
  - (molto) raro che attackers violino i **sistemi mainframe**;
  - (abbastanza) raro che avvengano **violazioni aggirando i sistemi di difesa perimetrale** posti in essere (Firewall, xIDS, etc).
- 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
[redacted] 1040
Source: https://you[redacted]olare.it/WEBHT/cc/movimentiConto.do
https://youwebcard.b[redacted]BHT/cc/movimentiConto.do
Referer: https://youwebcard.bancopopolare.it/WEBHT/homepage.do
User input: 6481121029866388207861
POST data:

compilazione=[redacted]
codContoCorrente=001%7C2180%7C2180002578

Cards, POS, NFC



CC number	Expiration date	Month/Year		Country		Site	Type	Vendor		Type (D/C)		Status		Bank		IP grabbed from		When	Internal	Internal
5446301270	Expire	01/16	Country	IT	Site	Ebay	Card	MASTERCARD	Type	none	Status	none	Bank	BANK OF LOS ALTOS	IP	82.213.10	Date	30.12.2013 14	55	48
5338750	Expire	07/17	Country	IT	Site	Ebay	Card	MASTERCARD	Type	DEBIT	Status	PREPAID	Bank	PAYPAL	IP	2.193.225	Date	30.12.2013 14	56	07
4023600	Expire	02/16	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	151.46.1	Date	30.12.2013 15	06	58
5338750	Expire	05/14	Country	IT	Site	Ebay	Card	MASTERCARD	Type	DEBIT	Status	PREPAID	Bank	PAYPAL	IP	151.74.8	Date	30.12.2013 15	10	39
4023600	Expire	10/17	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	85.39.10	Date	30.12.2013 15	27	54
4023600	Expire	02/16	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	151.46.1	Date	30.12.2013 15	40	07
5189629	Expire	06/15	Country	IT	Site	Ebay	Card	MASTERCARD	Type	none	Status	none	Bank	UNICREDITO ITALIANO	IP	176.247	Date	30.12.2013 15	49	41
4023600	Expire	02/16	Country	IT	Site	Paypal	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	151.46.1	Date	30.12.2013 15	56	09
4023600	Expire	02/16	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	151.46.1	Date	30.12.2013 16	05	26
5338750	Expire	01/15	Country	IT	Site	Ebay	Card	MASTERCARD	Type	DEBIT	Status	PREPAID	Bank	PAYPAL	IP	94.166.1	Date	30.12.2013 16	47	01
4023600	Expire	06/18	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	95.252.8	Date	30.12.2013 18	15	29
4023600	Expire	10/14	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	83.211.2	Date	30.12.2013 18	34	12
4023600	Expire	02/20	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	79.7.1.2	Date	30.12.2013 18	44	13
4023600	Expire	10/14	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	83.211.2	Date	30.12.2013 18	50	21
4539999	Expire	03/15	Country	IT	Site	Ebay	Card	VISA	Type	CREDIT	Status	CLASSIC	Bank	CARTASI S.P.A.	IP	37.183.7	Date	30.12.2013 19	30	19
5338750	Expire	05/15	Country	IT	Site	Paypal	Card	MASTERCARD	Type	DEBIT	Status	PREPAID	Bank	PAYPAL	IP	87.5.119	Date	30.12.2013 20	14	41
5364140	Expire	03/17	Country	IT	Site	Ebay	Card	MASTERCARD	Type	CREDIT	Status	STANDARD	Bank	POSTE ITALIANE	IP	82.52.18	Date	30.12.2013 22	29	35
5255000	Expire	01/20	Country	IT	Site	Paypal	Card	MASTERCARD	Type	none	Status	STANDARD	Bank	CARTASI S.P.A.	IP	79.31.23	Date	30.12.2013 23	40	12
4023600	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	Date	31.12.2013 01	46	27
4023600	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	Date	31.12.2013 01	52	30
4539970	Expire	03/14	Country	IT	Site	Ebay	Card	VISA	Type	CREDIT	Status	CLASSIC	Bank	CARTASI S.P.A.	IP	94.165.1	Date	31.12.2013 04	05	00
4023600	Expire	11/16	Country	IT	Site	Paypal	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	87.5.217	Date	31.12.2013 15	08	18
5264308	Expire	01/15	Country	IT	Site	Ebay	Card	MASTERCARD	Type	none	Status	none	Bank	FINECOBANK SPA	IP	188.125	Date	31.12.2013 16	16	56
5264308	Expire	01/15	Country	IT	Site	Ebay	Card	MASTERCARD	Type	none	Status	none	Bank	FINECOBANK SPA	IP	188.125	Date	31.12.2013 16	20	54
4658584	Expire	02/20	Country	IT	Site	Amazon	Card	VISA	Type	DEBIT	Status	CLASSIC	Bank	BARCLAYS BANK PLC	IP	79.8.124	Date	01.01.2014 20	36	29
4023600	Expire	03/20	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	151.66.1	Date	02.01.2014 04	21	25
5338750	Expire	06/17	Country	IT	Site	Facebook	Card	MASTERCARD	Type	DEBIT	Status	PREPAID	Bank	PAYPAL	IP	176.201	Date	02.01.2014 14	30	20
4023600	Expire	06/16	Country	IT	Site	Paypal	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	82.89.9	Date	02.01.2014 16	31	23
4289990	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	Date	03.01.2014 15	49	00
4023600	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	Date	04.01.2014 02	49	52
4023600	Expire	10/15	Country	IT	Site	Amazon	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	82.188.8	Date	07.01.2014 14	03	50
4023600	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	Date	08.01.2014 13	06	21
6762101	Expire	09/20	Country	IT	Site	Paypal	Card	DISCOVERY	Type	DEBIT	Status	none	Bank	INTESA SANPAOLO SPA	IP	87.241.3	Date	08.01.2014 20	26	43
5100206	Expire	03/15	Country	IT	Site	Facebook	Card	MASTERCARD	Type	none	Status	none	Bank	FINECOBANK SPA	IP	87.23.17	Date	09.01.2014 19	41	29
4023600	Expire	09/18	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	151.25.2	Date	10.01.2014 16	07	19
4023600	Expire	12/14	Country	IT	Site	Ebay	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	79.36.12	Date	10.01.2014 16	46	04
4090030	Expire	11/16	Country	IT	Site	Amazon	Card	VISA	Type	CREDIT	Status	CLASSIC	Bank	FINECOBANK S.P.A.	IP	54.240.1	Date	16.01.2014 16	57	38
4895532	Expire	05/15	Country	IT	Site	Paypal	Card	VISA	Type	CREDIT	Status	CORPORATE	Bank	DEUTSCHE BANK S.P.A.	IP	212.131	Date	17.01.2014 20	02	54
5342071	Expire	12/16	Country	IT	Site	Paypal	Card	MASTERCARD	Type	none	Status	none	Bank	none	IP	188.219	Date	27.01.2014 16	05	45
4824982	Expire	09/14	Country	IT	Site	Ebay	Card	VISA	Type	none	Status	none	Bank	none	IP	109.54.8	Date	29.01.2014 02	27	07
4023600	Expire	10/14	Country	IT	Site	Facebook	Card	VISA	Type	DEBIT	Status	ELECTRON	Bank	POSTE ITALIANE S.P.A. (BANCO POSTA)	IP	195.32.15	Date	01.04.2014 16	16	48
5400580	Expire	03/18	Country	IT	Site	Facebook	Card	MASTERCARD	Type	none	Status	none	Bank	none	IP	151.49.15	Date	03.04.2014 14	13	31
5338750	Expire	09/16	Country	IT	Site	Ebay	Card	MASTERCARD	Type	DEBIT	Status	PREPAID	Bank	PAYPAL	IP	151.44.27	Date	04.04.2014 14	23	14

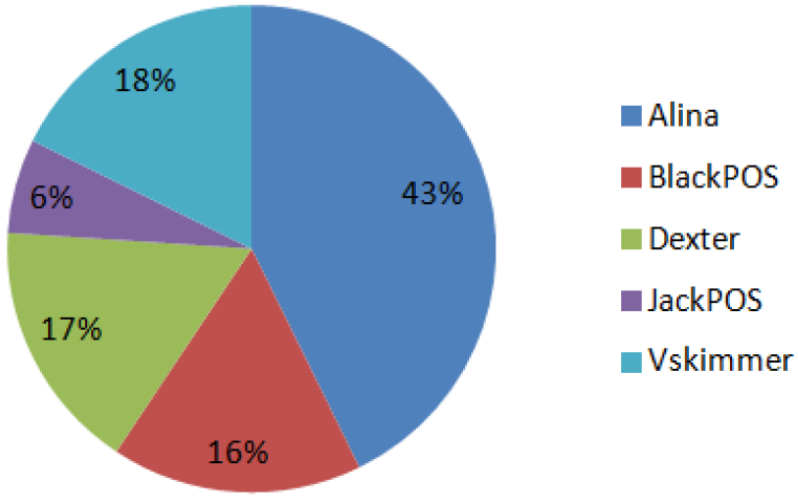
Cards, POS, NFC

#	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

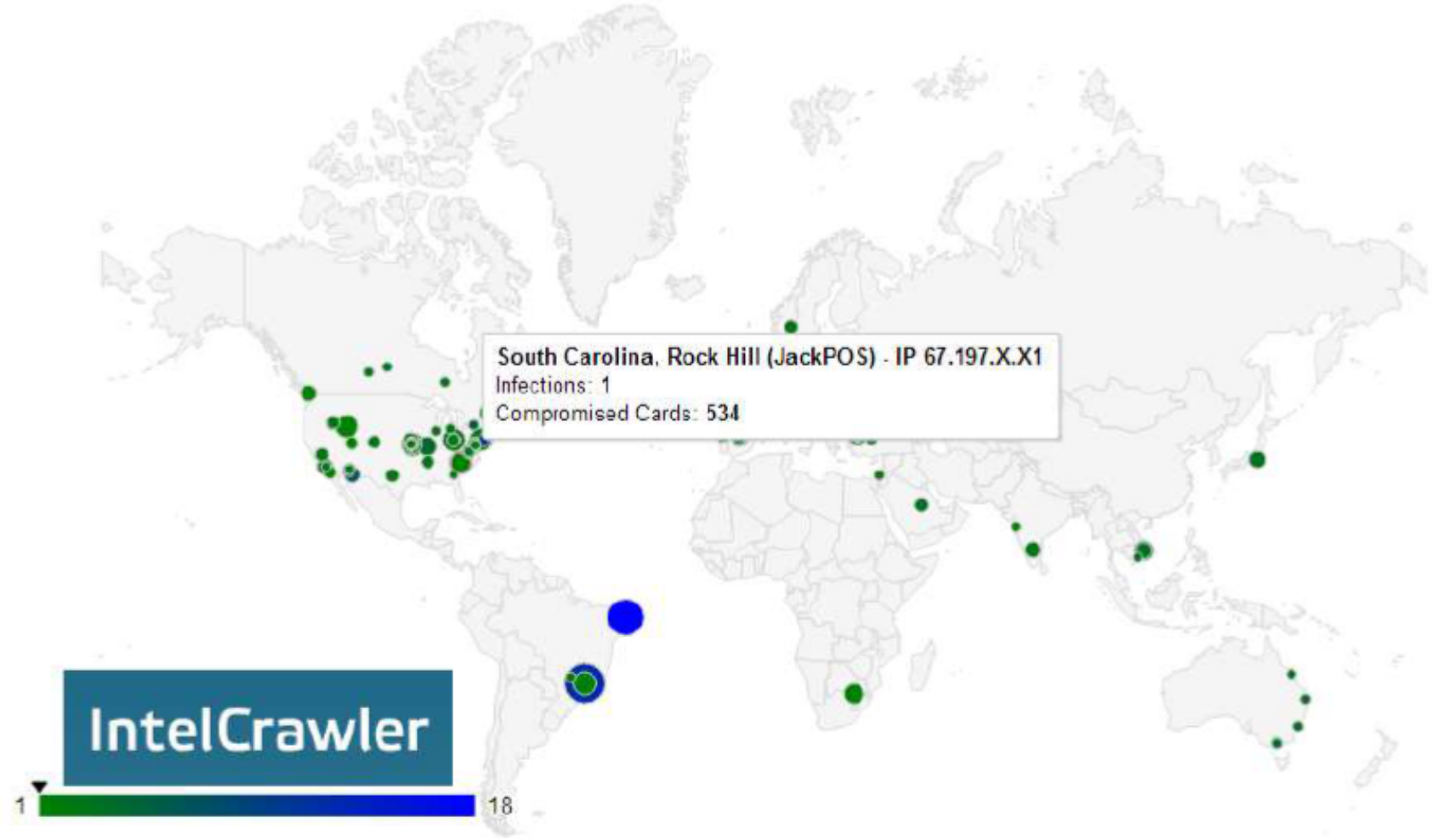
```
data:00471224 aWwwRee4_7ci_ru db 'www/ree4.7ci.ru/reports/',0 ;
data:00471243 ; char aDun_exe_2[]
data:00471243 aDun_exe_2      db 'dun.exe',0          ; DATA XRI
data:0047124B ; char aOutput_txt_1[]
data:0047124B aOutput_txt_1   db 'output.txt',0       ; DATA XRI
data:00471256 aDun_exe_3      db '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

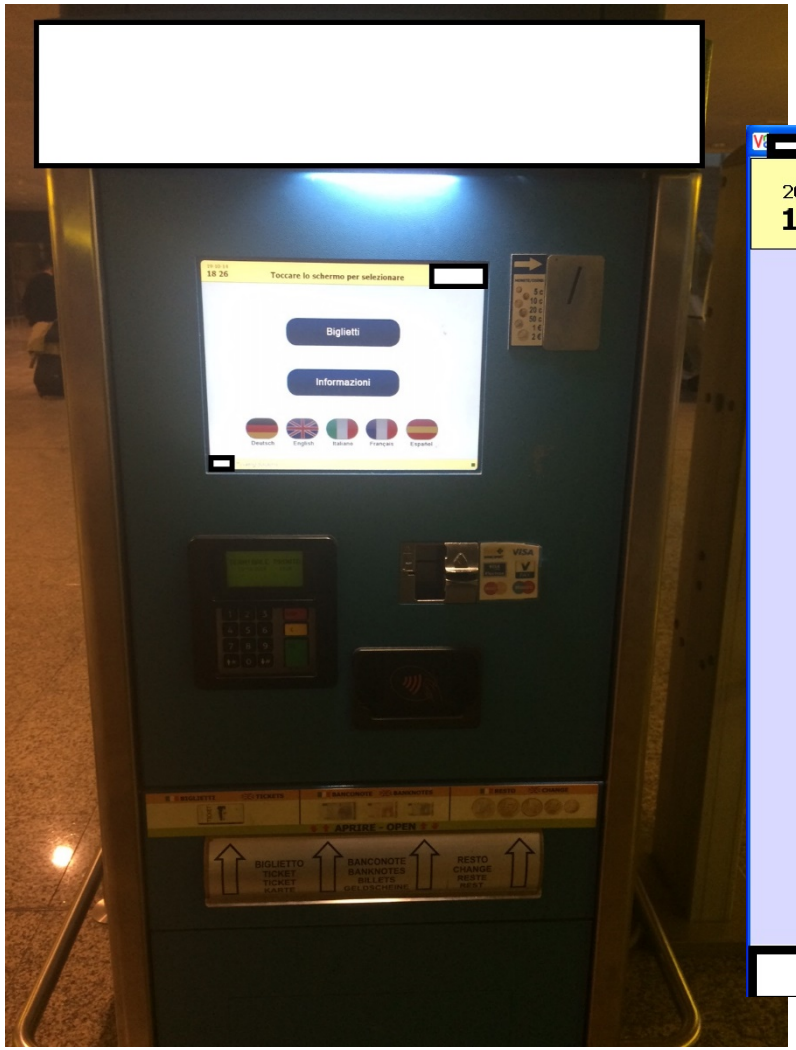
"Kartoxa"/"BlackPOS" Author

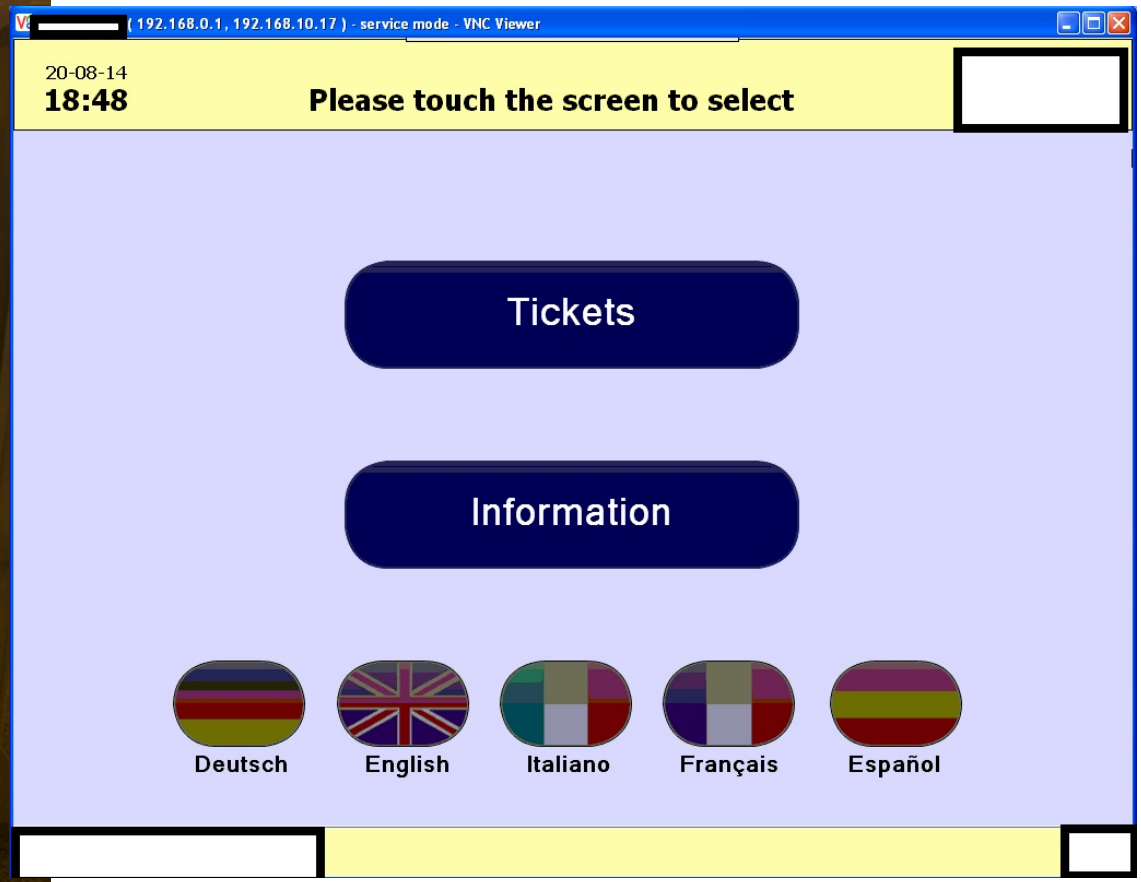
"Yes, I have written it, but for security testing ..."

JackPOS, «primi giorni di vita»

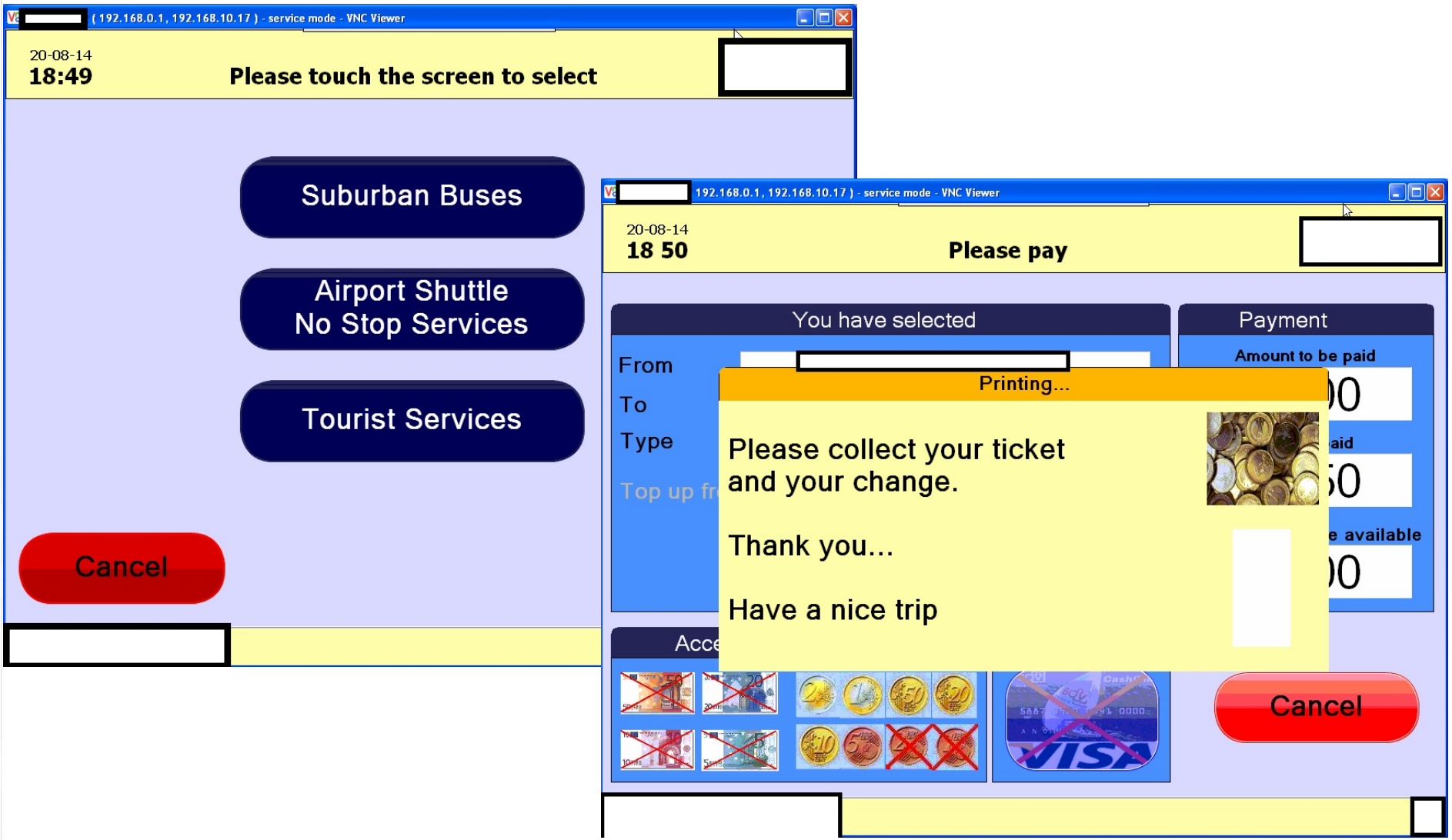


Cards, POS (Totem), NFC

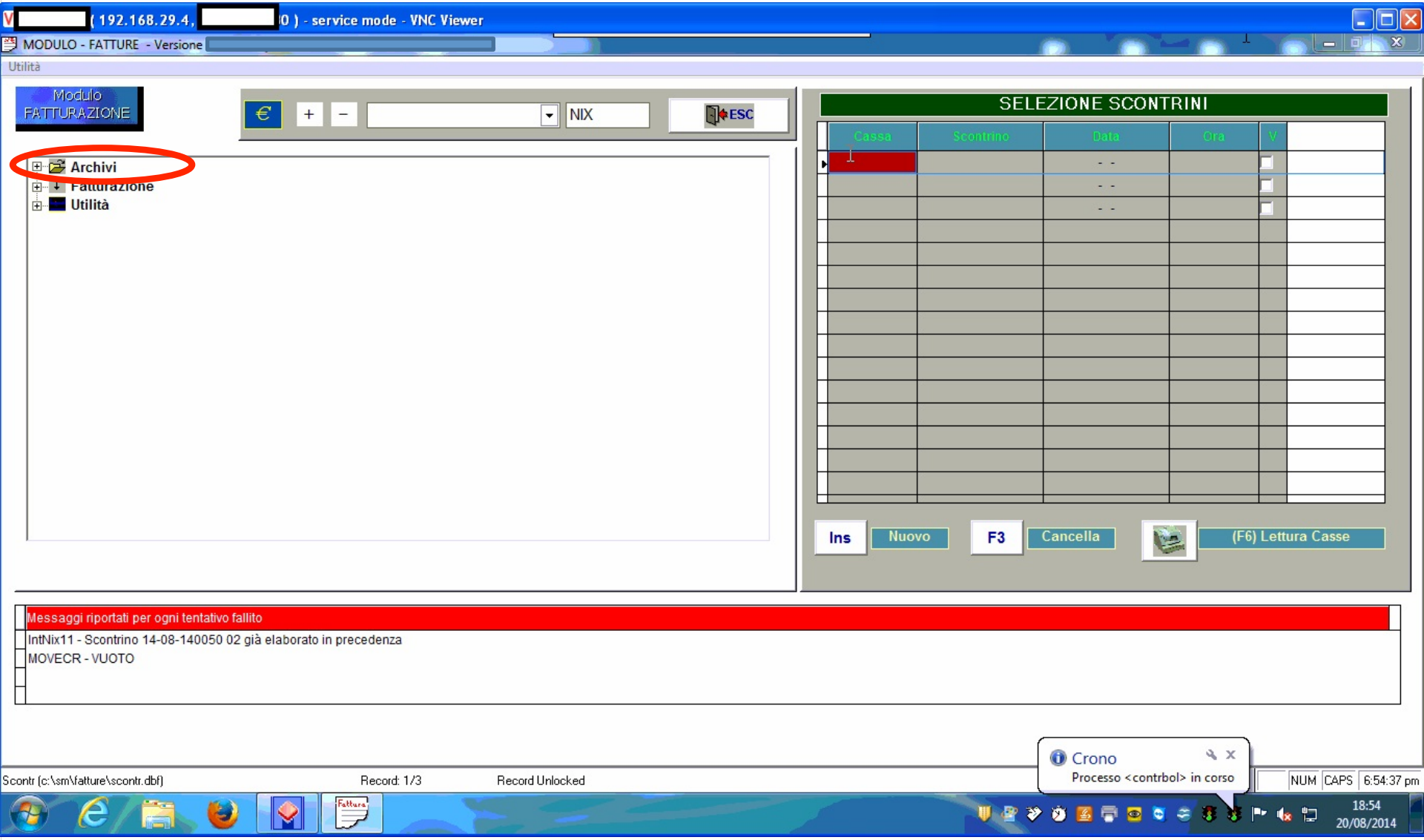




Cards, POS (Totem), NFC



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

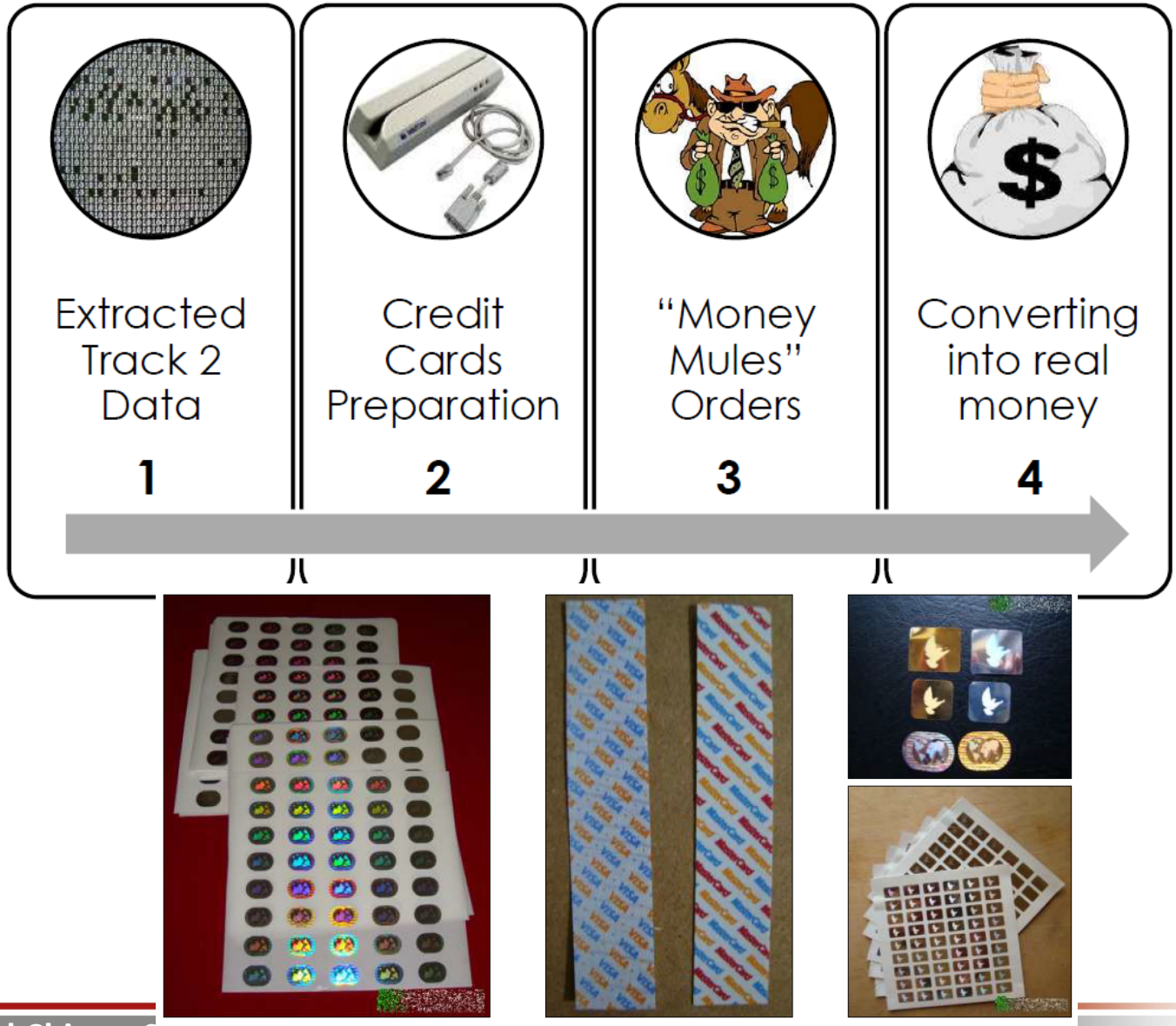
Parcheggi e biglietterie, nuovo obiettivo hacker

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

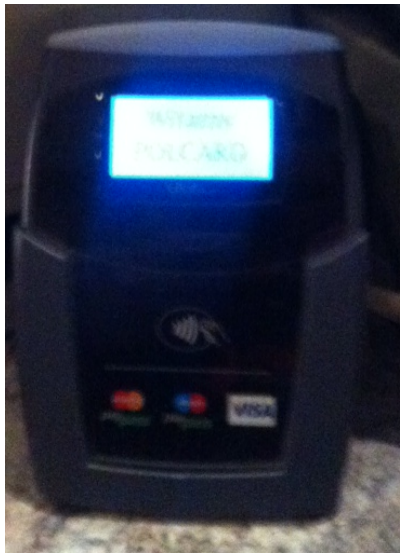
La fretta di introdurre i sistemi Nfc, che permettono di pagare con lo smartphone nei negozi, ha aperto una **falla di sicurezza**: i **dati non vengono crittografati** e quindi **si possono rubare**. Ma **non è un problema dell'Nfc**, garantiscono gli esperti. E in Italia siamo al sicuro, **solo perché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

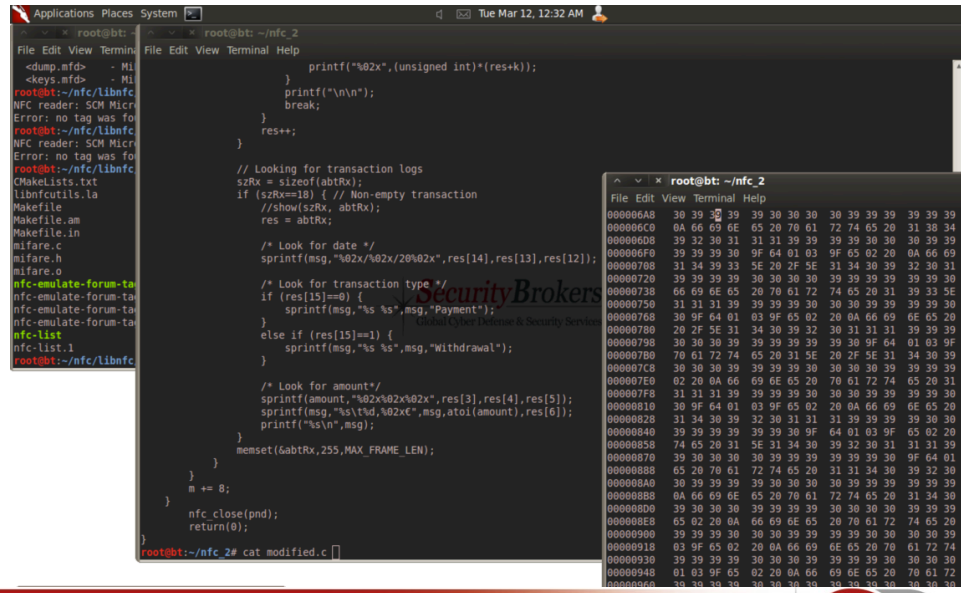
http://www.repubblica.it/tecnologia/2012/08/07/news/rischi_pagamenti_nfc-40330153/?ref=fbpr

By la Repubblica.it - Tecnologia, 7 agosto 2012

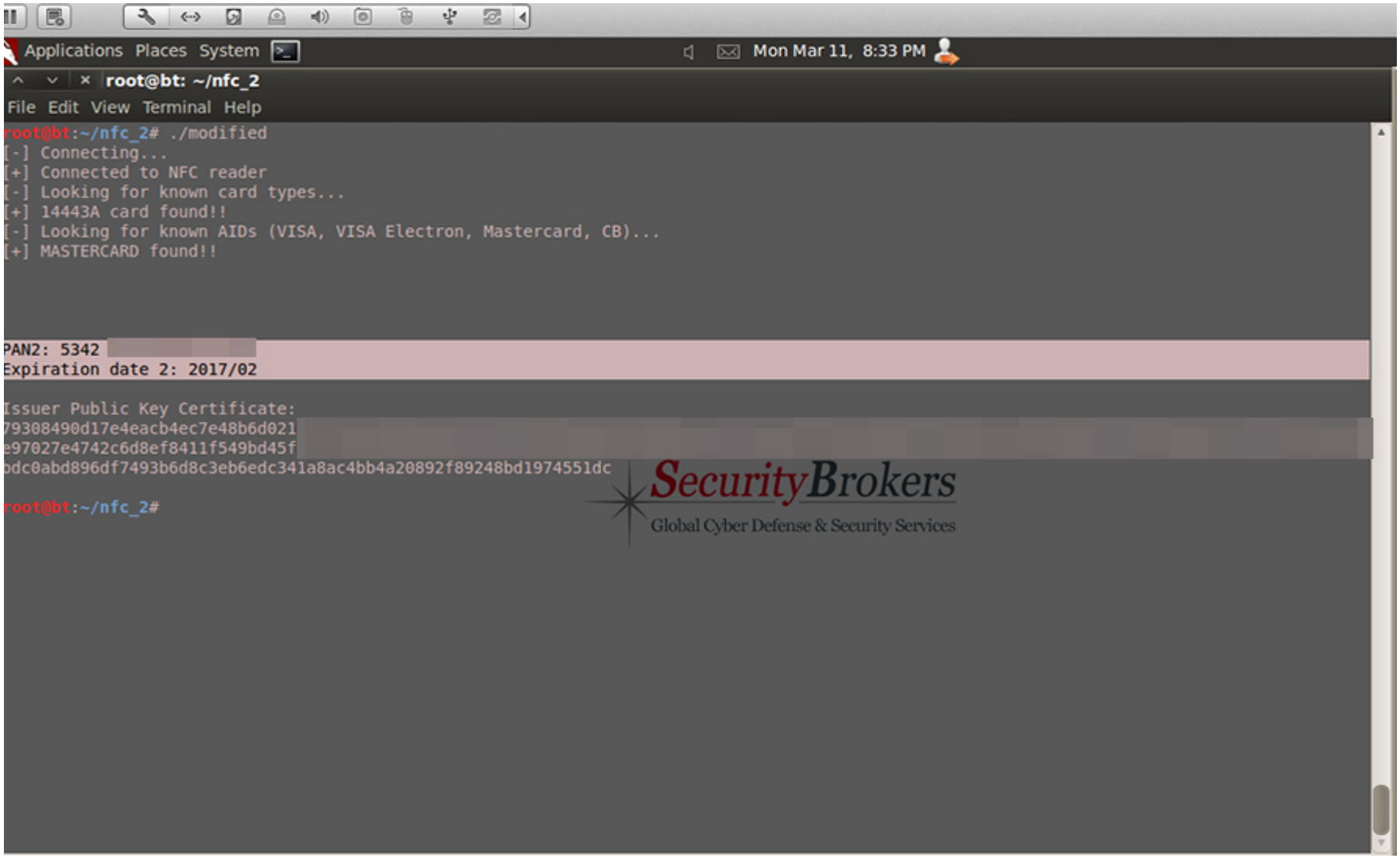
Cards, POS, NFC

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€
------------------------
```

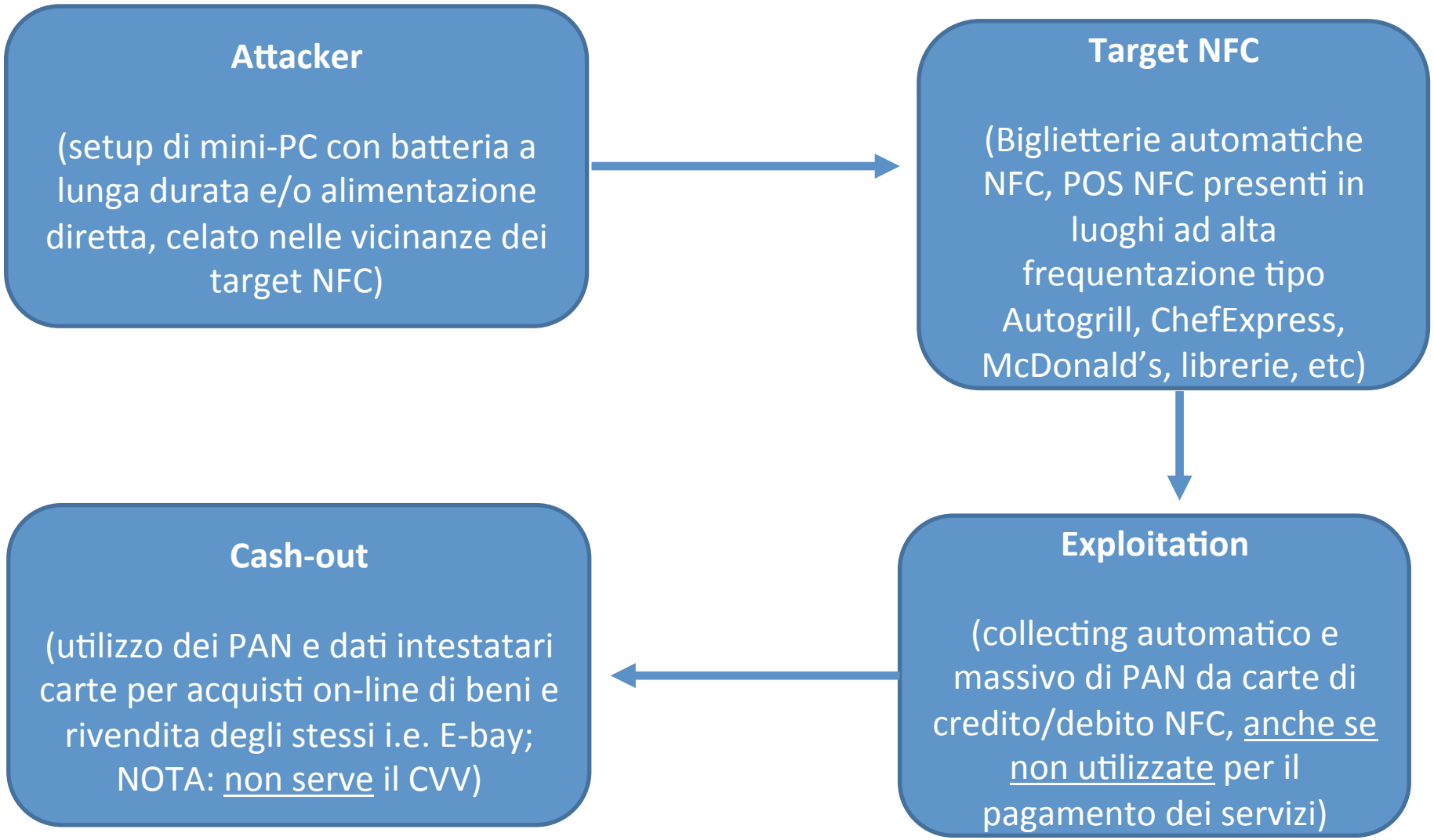
Mass-Carding

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.**

Cyber Intelligence: what you get?

«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.).

Deliverables (closed-source Intelligence)

✴ 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.

Conclusioni

Conclusioni

- 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

Spam Nation, Brian Krebs, 2014

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?