SecurityBrokers
GLOBAL CYBER DEFENSE & SECURITY SERVICES

PUBLIC RELEASE

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

Raoul Chiesa

Founding Partner, President, Security Brokers SCpA

The Innovation Group
Innovating business and organizations through ICT

IntelCrawler

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)**
- Former 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
- Former 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, Cybercrime Infrastructures Takedowns, Cybercriminals bounting, Cyber Intelligence Reports, interfacciamento con CERTs e LEAs/LEOs, servizi targeted 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**: c'è "***molta confusione***".

- Innanzitutto, dobbiamo **capire cosa significa** "Intelligence".
  - Nei **Paesi anglosassoni**, 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: **Cyber Espionage rings/gangs**, **Information Warfare**).

«Cyber Intelligence»?

I feeds

- 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.)

Ogni altra tipologia di fonti (i.e.: logs di Firewall, Antivirus, xIDS, IPS, etc…) **non porta alla Cyber Intelligence nè ai "feeds"**, ma si chiama semplicemente "correlazione di log".


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)**

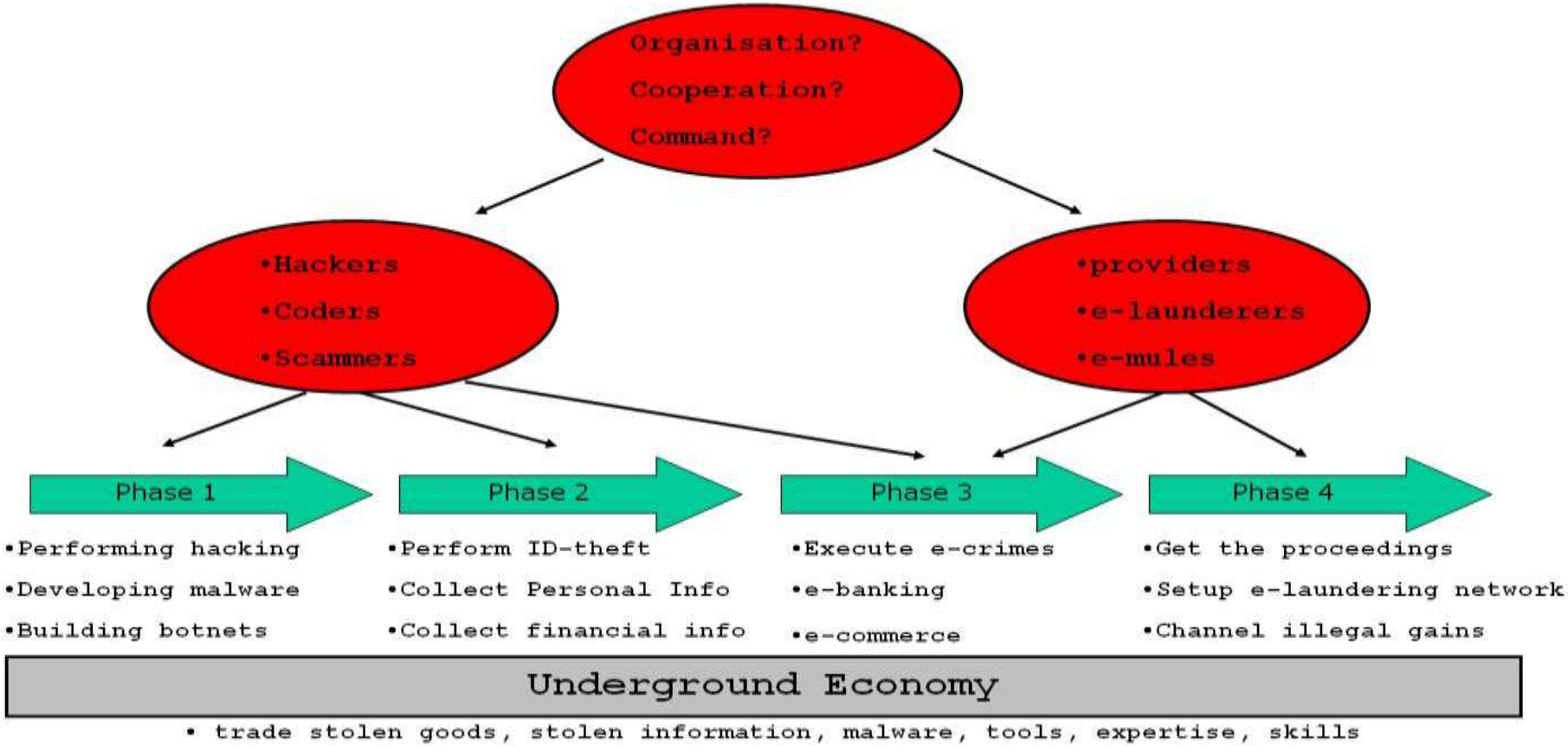
- Ecco perché tutti noi vogliamo «essere sicuri".

- Non è un caso se si chiama **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.

Altri esempi di «slangzzz»

L33T 5P33K

- first use was to play with moderators on BBS'es and that was in age of 1kBd modems
- Very unstable really - live
- present in many languages – even google ;)
- it's not about *gangsta* talk ☺

Altri esempi di «slangzzz»

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4	6	o	|)	3	]=	6	/-/	1	_|	|X	1	|v|	||	0	|*	(_,)	2	5	7	M	\/	\/\/	%	j	2
/\	8	<	|o	&	ph	&	[-]	!	/	|<	£	em	^/	()	|o	()	12	$	+	|_|	\/	vv	><	`/	~/
@	13	(	∂	€	)	(_+	]-[	|	]	|(	1_	]V[	//\\//	oh	|°	O_	|?	z	-|-	Y3W	\\//	'//	X	`(	%
/-\	I3	(	])	£	|=	9	)-(	eye	¿	h	|	(T)	/\/	[]	|^(o)	<|	/2	§	1	L|		\\'	)(	-/	>_
^	|3	(c)	[)	ë	(=	C-	(-)	3y3	</		|_	[V]	[\]	p	|>	9	I2	ehs	']['	µ		\^/	ecks	'/	5
aye	ß		I>	[-	I=	gee	:-:	ai	(/		lJ	nn	<\>	¤	|"	O,	|^	es	†	[_]		(n)	*	Ψ	7_
∂	P>		|>	|=-		(Y,	|~|	¡	_7		//\\//\\	(\)	Ω	?	(,)	|~			_/		\V/	*	φ	
ci	|:		?			(_-	|-|	][	_)		|\/|	[]\		9	(),	1z			_\		\X/	)(	λ	
λ	!3		T)			cj	]~[	:	¿			/\/\	// []		[]Þ	¶	(r)			/_/		\\|/	ex	Ч	
Z	(3		0				)(	]				(u)	/V		|°		|2			(_)		_|_/		¥	
	/3		ß				?					(V)	¤		|7		[z					\\//\\//			
	)3		c1				)-(					(\/)	[]\[]		q		|`					_:_/			
	]3						#					/|	]\[		þ		12					(/\)			
												^^	~		¶		Я					]I[			
												/|/|			ⁿ		|2					LL1			
												//.			|Þ		.-					UU			
												.\\					¤					Ш			
												/^^\										ч			
												/V\													
												[]\/[]													
												|^^|												

Altri esempi di «slangzzz»

Russian letters

А а	а а	a	a	Р р	р р	r	er
Б б	б б	b	be	С с	с с	s	es
В в	в в	w	we	Т т	т т	t	te
Г г	г г	g, h	ge	У у	у у	u	u
Д д	д д	d	de	Ф ф	ф ф	f	ef, fe (pot.)
Е е	е е	je, ie, e	je	Х х	х х	ch	cha
Ё ё	ё ё	jo, io	jo	Ц ц	ц ц	c	ce
Ж ж	ж ж	ż	że	Ч ч	ч ч	czi	czie
З з	з з	z	ze	Ш ш	ш ш	sz	sza
И и	и и	i, y	i	Щ щ	щ щ	śś	ssia
Й й	й й	j	j, i krátkoje	Ъ ъ	ъ ъ	-	twiórdyj znak, jer
К к	к к	k	ka	Ы ы	ы ы	y	y
Л л	л л	ł	el'	Ь ь	ь ь	-	mjákkij znak, jer'
М м	м м	m	em	Э э	э э	e	e abarótnoje
Н н	н н	n	en	Ю ю	ю ю	ju, iu	ju
О о	о о	o, -a	o	Я я	я я	ja, ia, i	ja
П п	п п	p	pe				

Altri esempi di «slangzzz»

Examples :

- KoHTpbl Hy6bl
- Y %username% 4utbl 100 o\o, AgmuH 3a6aHb ero
- Admin cmeHu map, 3ae6aJIo
- odd noobs
- User … cheats I 100%, admin ban him
- Admin change tar, I lost it

Altri esempi di «slangzzz»

Number code introduction

- 1 = 要 to want
- 2 = 爱 to love
- 3 = 想 to miss or to want
- 4 = 死 to die *(bad luck)*
- 5 = 我 I, me
- 7 = 亲 to kiss
- 8 = 發 prosperity (good luck)
- 0 = 你 you
- Examples:
  - 514 = 我要死 I want to die
  - 56 = 无聊 bored
  - 5366 = 我想聊聊 I want to chat
  - 282 = 饿不饿 hungry?
  - 555 = 呜呜呜 refers to: the sound of crying
  - 520 = 我爱你 I love you → Chinese Valentine Day is May 20th ☺
    - And what 520-2 means?

!!! 3Q = thanks (San-Q)

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' invece 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). Ah, però **tutti** PCI-DSS certified! ☹
- 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)

SLIDE NON PRESENTE NELLA VERSIONE PUBBLICA DI QUESTA PRESENTAZIONE

Cards, POS, NFC

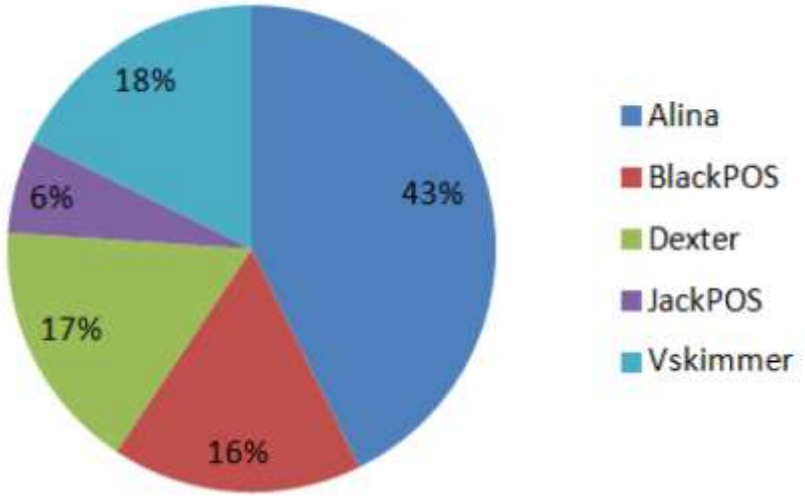
SLIDE NON PRESENTE NELLA VERSIONE PUBBLICA DI QUESTA PRESENTAZIONE

Cards, POS, NFC

SLIDE NON PRESENTE NELLA VERSIONE PUBBLICA DI QUESTA PRESENTAZIONE

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

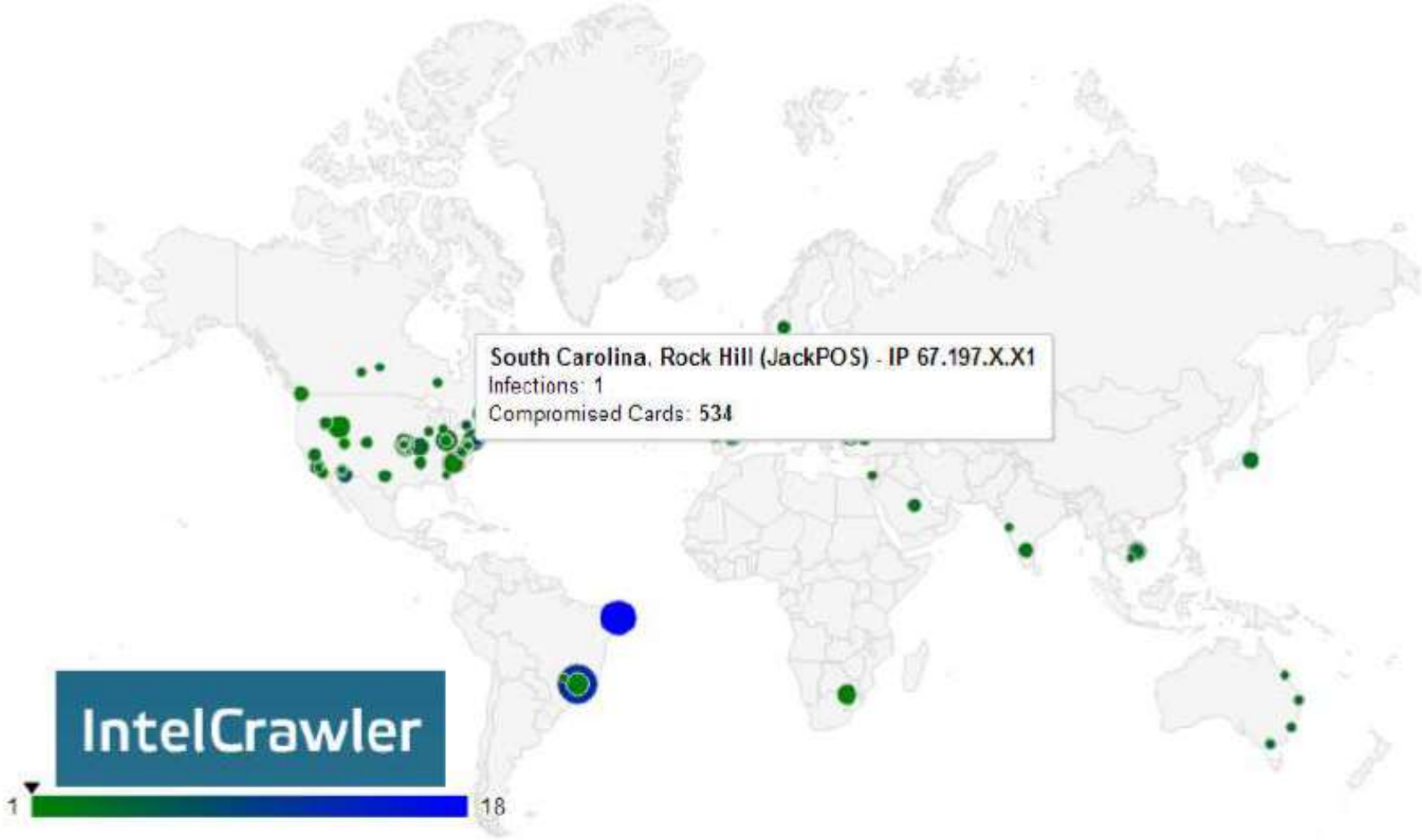
```
data:00471228 aWwwRee4_7ci_ru db 'www/ree4.7ci.ru/reports/',0 ;
data:00471243 ; char aDun_exe_2[]
data:00471243 aDun_exe_2      db 'dun.exe',0          ; DATA XRI
data:0047124B ; char aOutput_txt_1[]
data:0047124B aOutput_txt_1   db 'output.txt',0       ; DATA XRI
data:00471256 aDun_exe_3      db '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

SLIDE NON PRESENTE NELLA VERSIONE PUBBLICA DI QUESTA PRESENTAZIONE

Cards, POS (Totem), NFC

SLIDE NON PRESENTE NELLA VERSIONE PUBBLICA DI QUESTA PRESENTAZIONE

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

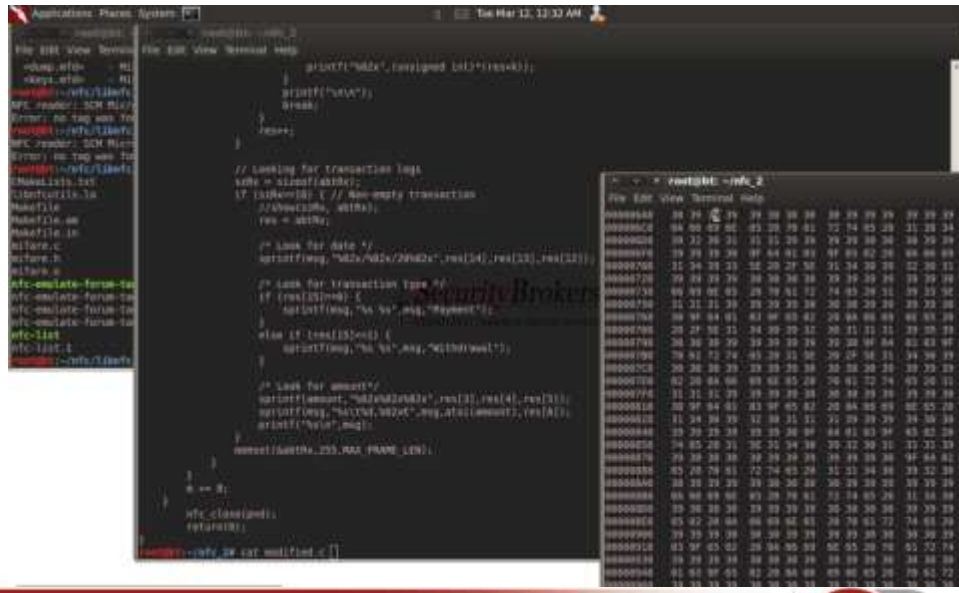
La fretta di introdurre i sistemi Nfc, che permettono di pagare con lo smartphone nei negozi, ha aperto una **falla di sicurezza**: i **dati non vengono crittografati** e quindi **si possono rubare**. Ma **non è un problema dell'Nfc**, garantiscono gli esperti. E in Italia siamo al sicuro, **solo perché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

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

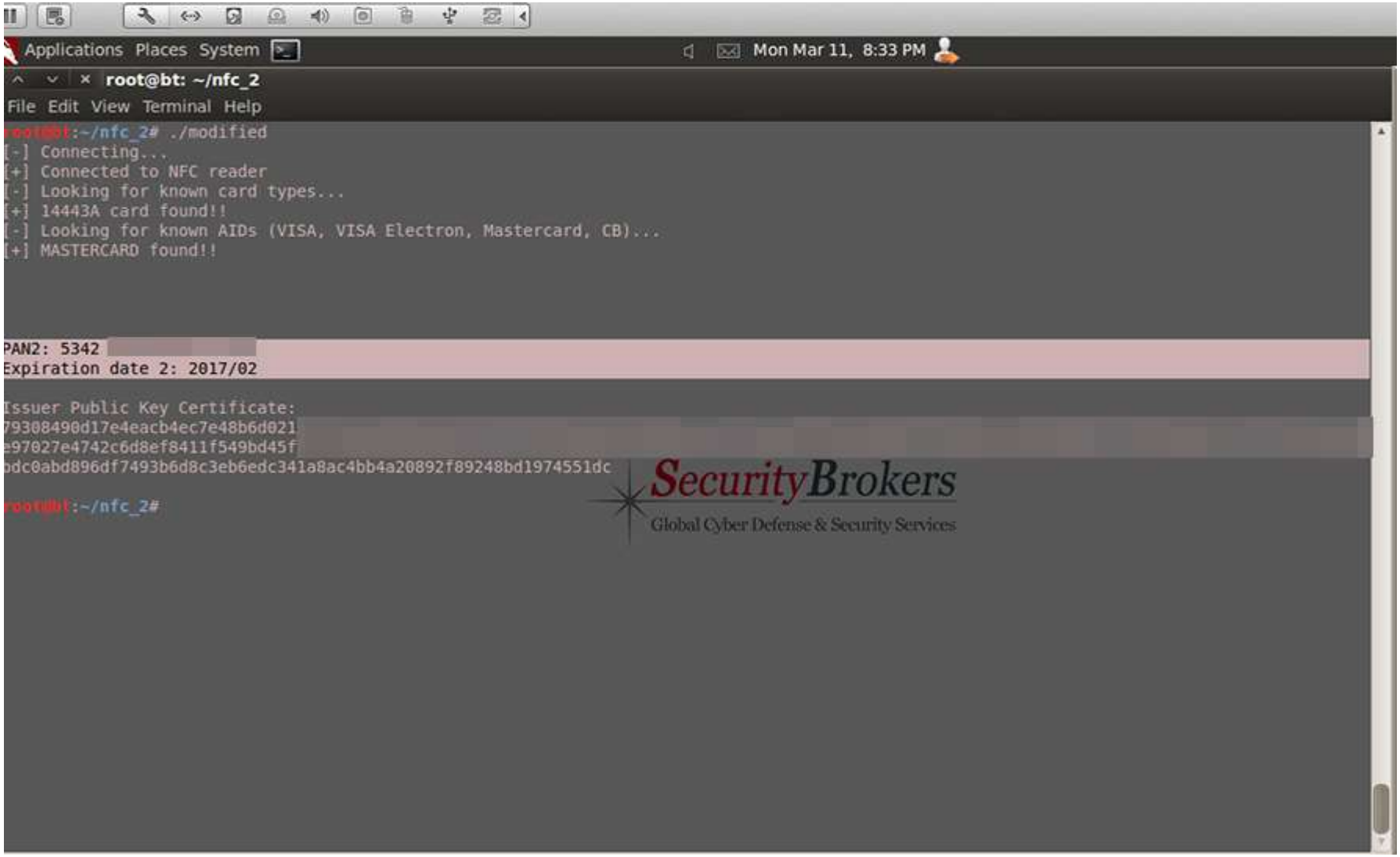
By la Repubblica.it - Tecnologia, 7 agosto 2012

Cards, POS, NFC

Hacking the NFC credit cards for fun and debit ;)



Cards, POS, NFC



Cards, POS, NFC

SLIDE NON PRESENTE NELLA VERSIONE PUBBLICA DI QUESTA PRESENTAZIONE

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

Attacker

(setup di mini-PC con batteria a lunga durata e/o alimentazione diretta, celato nelle vicinanze dei target NFC)

Target NFC

(Biglietterie automatiche NFC, POS NFC presenti in luoghi ad alta frequentazione tipo Autogrill, ChefExpress, McDonald's, librerie, etc)

Exploitation

(collecting automatico e massivo di PAN da carte di credito/debito NFC, anche se non utilizzate per il pagamento dei servizi)

Cash-out

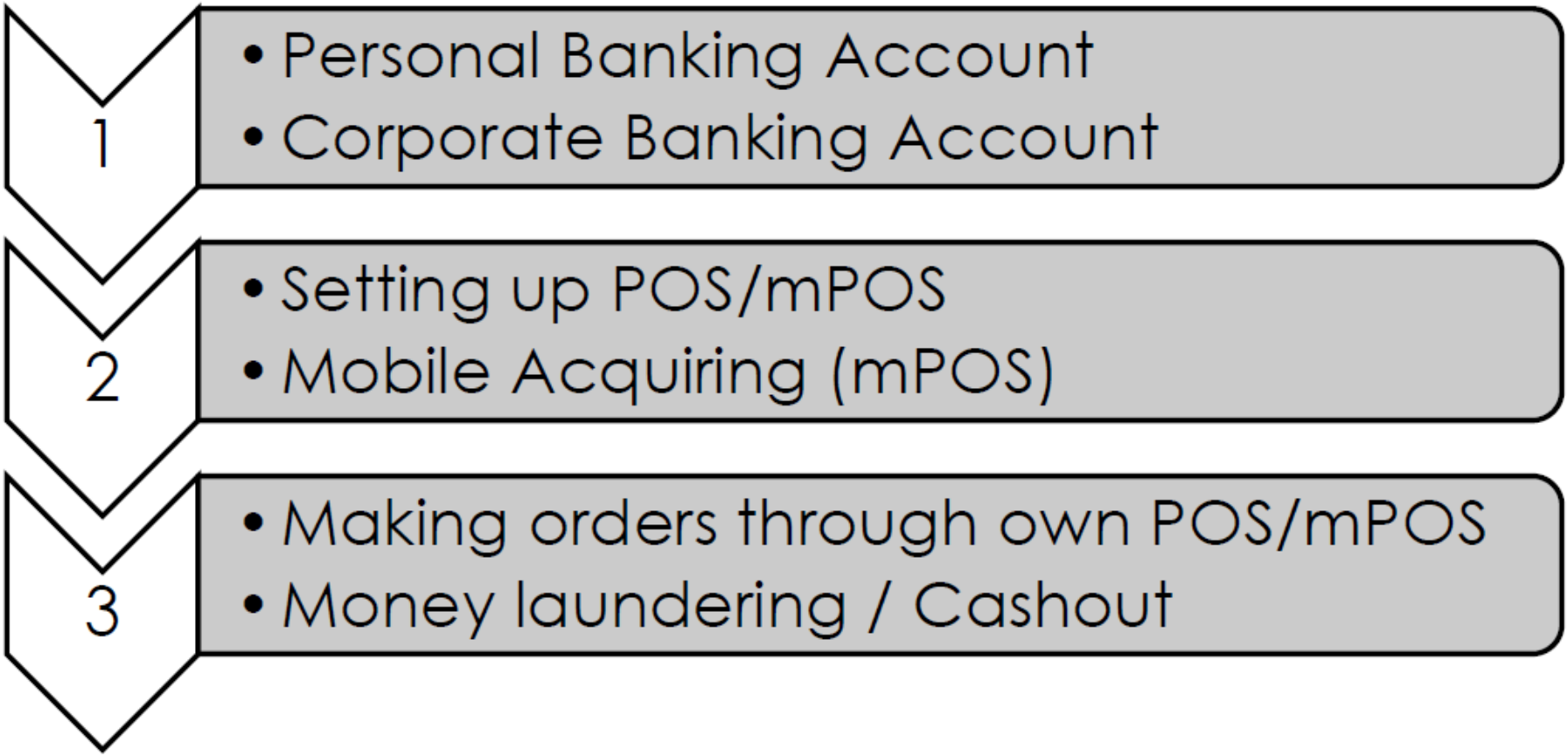
(utilizzo dei PAN e dati intestatari carte per acquisti on-line di beni e rivendita degli stessi i.e. E-bay; **NOTA: non serve il CVV**)

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 (estratto, non completo!)

✶ 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

Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door, Brian Krebs, 2015

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 / of Intrusion, Kevin D. Mitnick & William L. Simon, Wiley, 2002/2004

@ 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

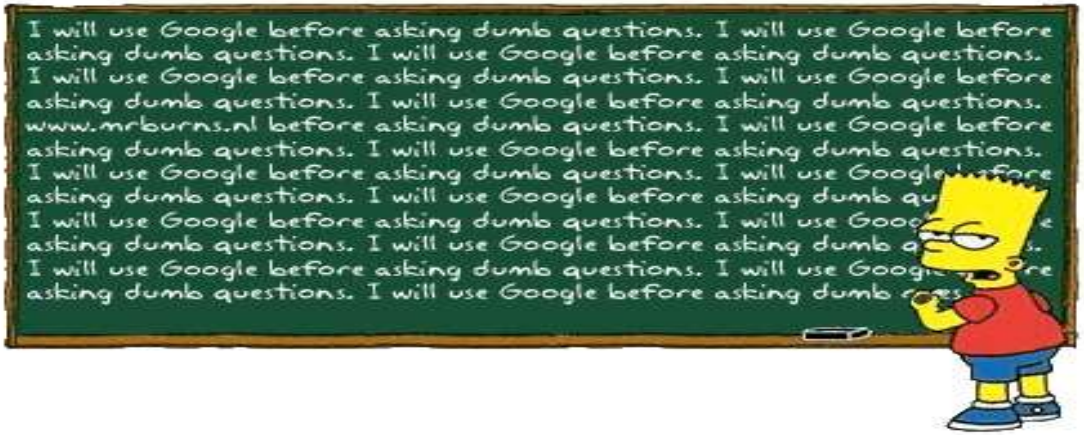
Criminal Profiling Research Site. Scientific Offender Profiling Resource in Switzerland. Criminology, Law, Psychology, Täterpro

Contacts, Q&A

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

Thanks for your attention!

QUESTIONS?



Extra Material

Profiling Hackers

HPP – The Hacker's Profiling Project

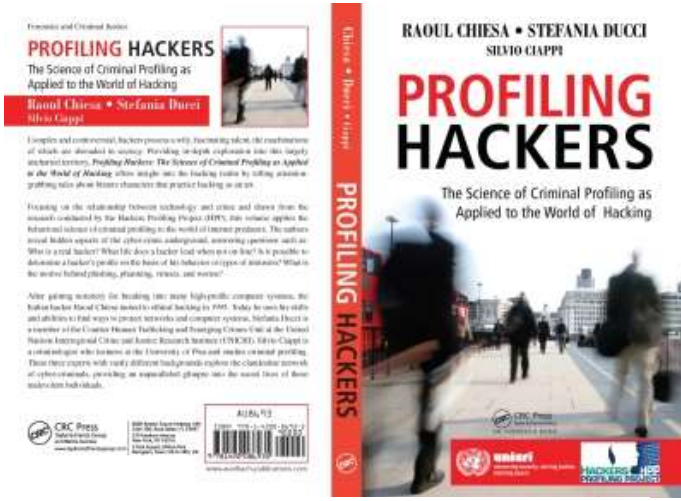
HPP V1.0: purposes & goals

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

unicri
advancing security, serving justice, building peace

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