Public Release for
HES 2011 delegates

From the good, old hacking days to nowadays cybercrime: what happened??

A presentation by Raoul Chiesa
Senior Advisor, on Cybercrime

United Nations - Interregional Crime and Justice Research Institute (UNICRI)

Hackito Ergo Sum

2011

HES 2011 – Hackito Ergo Sum
Key Note Talk - Day 3

Paris, April 9th 2011

Disclaimer

- The information contained in this presentation **does not** break any intellectual property, nor does it provide detailed information that **may be in conflict with** recent controversial French laws.

- Registered brands belong to **their legitimate owners.**

- The opinion here represented are my **personal ones** and **do not necessary** reflect the **United Nations** nor **UNICRI or ENISA and ENISA's PSG** views.

Agenda

- ✓ # whois
- ✓ Introduction and Key Concepts
- ✓ Yesterday’s hacking VS today’s crime
- ✓ Hacking eras and Hacker’s generations
- ✓ Cybercrime
- ✓ Hackers…
- ✓ Profiling the enemy: the Hackers Profiling Project (HPP)
- ✓ Hacking, today: Underground Economy
- ✓ What’s next? The Dark Links
- ✓ Cybercrime: the responses
- ✓ Conclusions

#whois

Who am I?

ph-neutral
0x0 0x1 0x2 0x3 0x4 0x5 0x6 0x7 0x8 0x9 0xa 0xb 0xc 0xd 0xe
blackhat
whitehat
-[c0d3 and p4r7y]-
Talks

Raoul “Nobody” Chiesa

- Old-school Hacker from **1986 to 1995**
- Infosec Professional since **1997 @ Mediaservice.net**
- **OSSTMM** Key Contributor; **HPP** Project Manager; **ISECOM International Trainer**
- Co-founder of **CLUSIT**, Italian Computer Security Association (CLUSI* : Belgium, France, Luxembourg, Switzerland)
- Member of **TSTF.net** – Telecom Security Task Force, **APWG**, ICANN, etc
- I work **worldwide** (so I don’t get bored ;)
- My **areas of interest**: Pentesting, SCADA/DCS/PLC, National Critical Infrastructures, Security R&D+Exploiting weird stuff, , Security People, X.25, PSTN/ISDN, Hackers Profiling, Cybercrime, Information Warfare, Security methodologies, vertical Trainings.

mediaservice.net

ISECOM

Clusit Associazione Italiana per la Sicurezza Informatica

OWASP The Open Web Application Security Project

TSTF.net Telecom Security Task Force

ICANN

opsi aip

unicri advancing security, serving justice, building peace

APWG Committed to Wiping Out Internet Scams and Fraud

- Basically, I do not work in this field just to get my **salary every month** and pay the home/car/whatever loan: **I really love it** ☺

What is UNICRI?

United Nations Interregional Crime & Justice Research Institute

A United Nations entity established in 1968 to support countries worldwide in crime prevention and criminal justice

UNICRI carries out applied research, training, technical cooperation and documentation / information activities

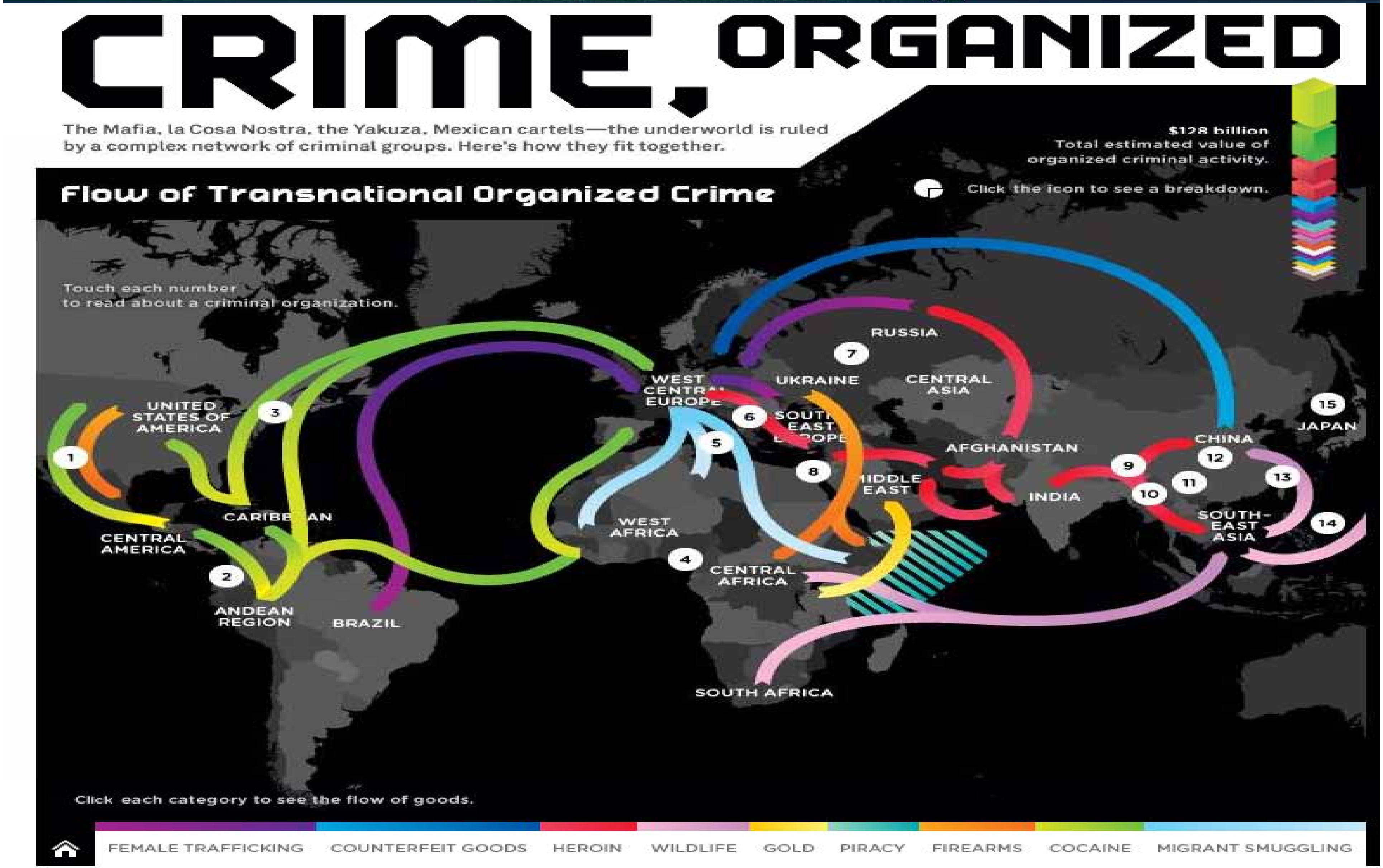
UNICRI disseminates information and maintains contacts with professionals and experts worldwide

Emerging Crimes Unit (ECU): cyber crimes, counterfeiting, environmental crimes, trafficking in stolen works of art…

Fake Bvlgari &Rolex
Viagra & Cialis (ak

Water syst

Guess how they update each others?
Email, chat&IM, Skype…



CRIME, ORGANIZED

The Mafia, la Cosa Nostra, the Yakuza, Mexican cartels—the underworld is ruled by a complex network of criminal groups. Here's how they fit together.

$128 billion
Total estimated value of organized criminal activity.

Click the icon to see a breakdown.

Flow of Transnational Organized Crime

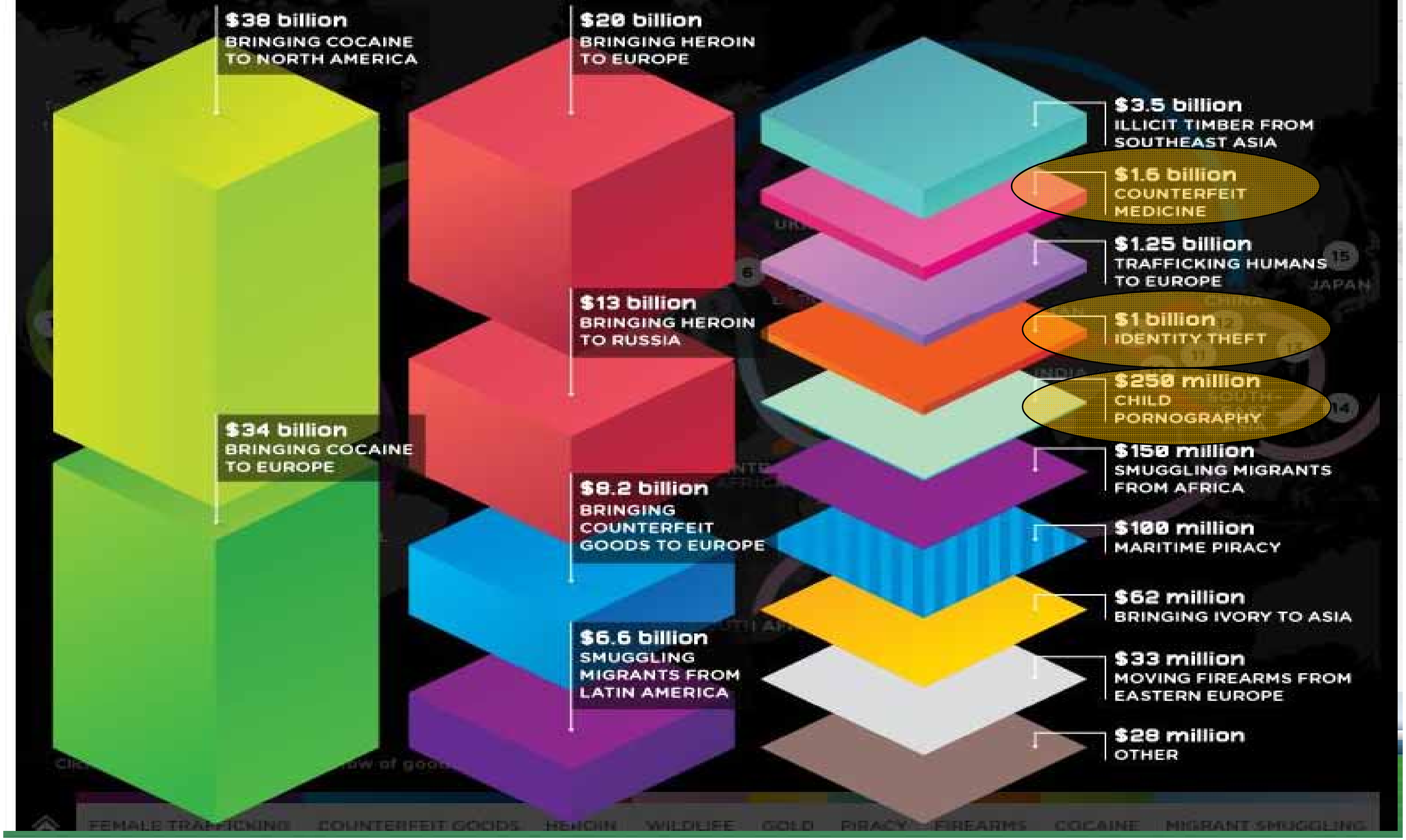
Touch each number to read about a criminal organization.

Click each category to see the flow of goods.

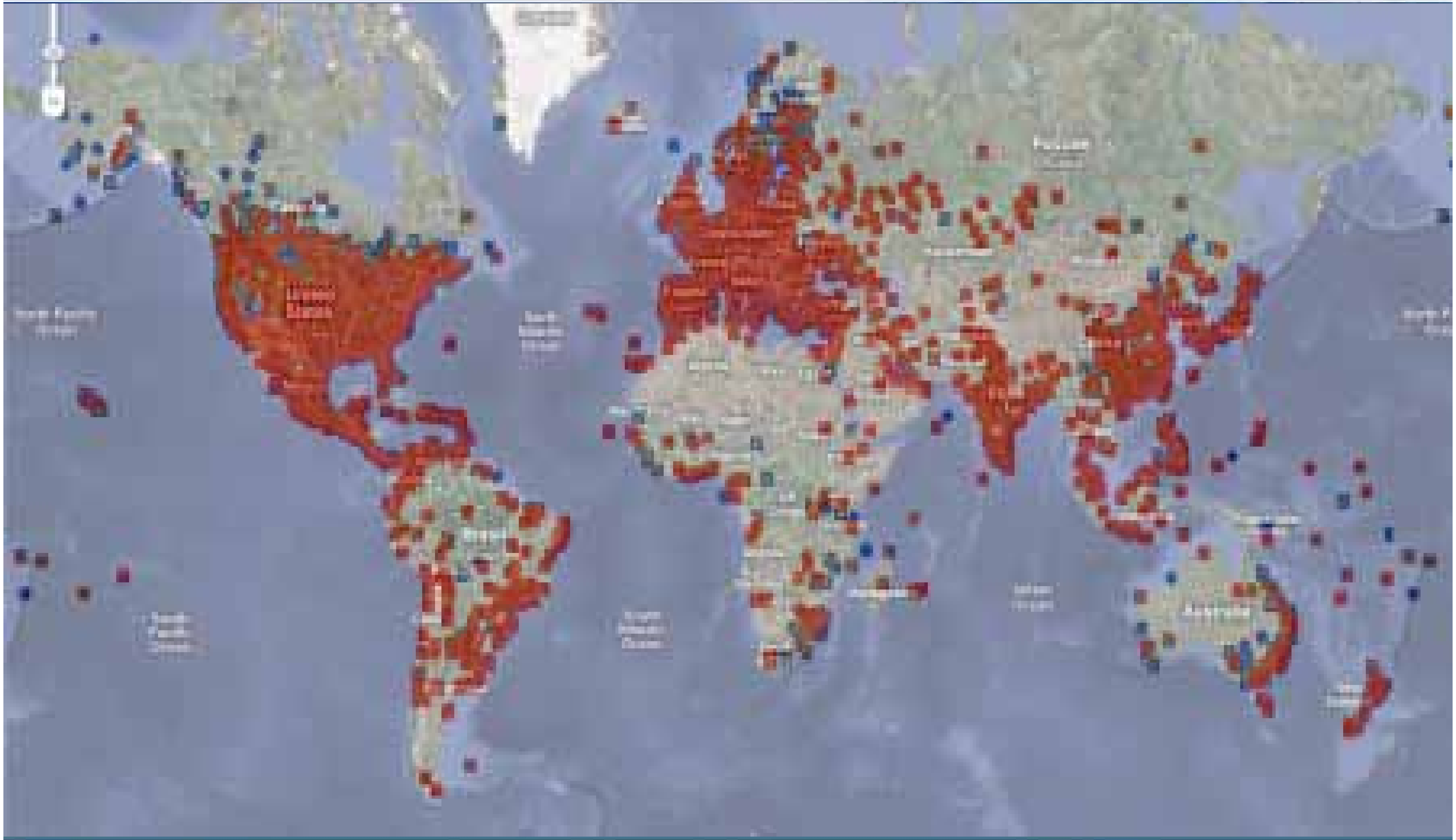
Drugs earn the most and cause the most violence.

$125 billion
Total estimated value of organized criminal activity.

ESTIMATED VALUE OF CRIMINAL ACTIVITIES, BY TYPE

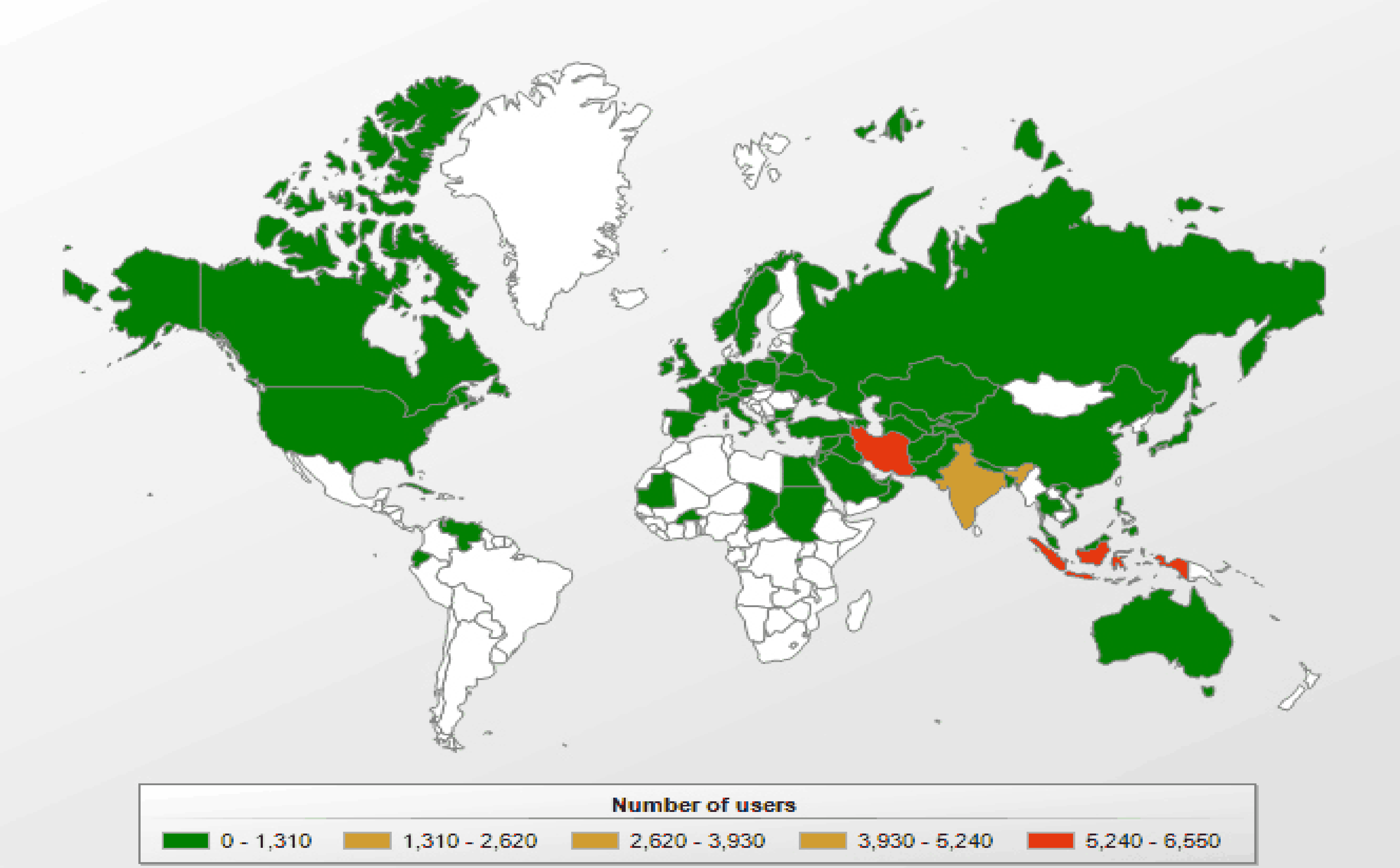


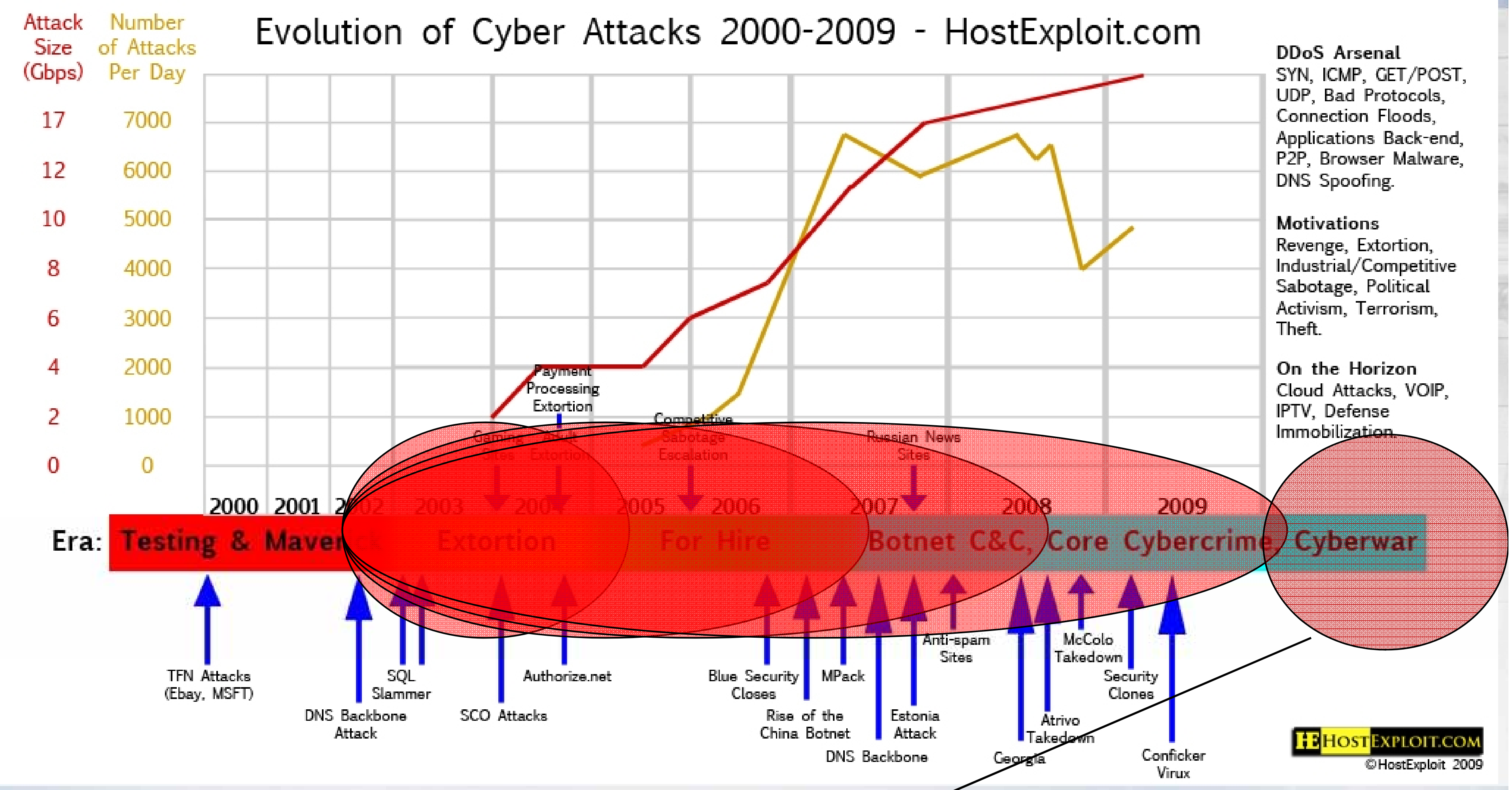
Conficker (December 2009)



Stuxnet (December 2010)

Rootkit.Win32.Stuxnet geography





Evolution of Cyber Attacks 2000-2009 - HostExploit.com

DDoS Arsenal
SYN, ICMP, GET/POST, UDP, Bad Protocols, Connection Floods, Applications Back-end, P2P, Browser Malware, DNS Spoofing.

Motivations
Revenge, Extortion, Industrial/Competitive Sabotage, Political Activism, Terrorism, Theft.

On the Horizon
Cloud Attacks, VOIP, IPTV, Defense Immobilization.

Talk for the next year ;)

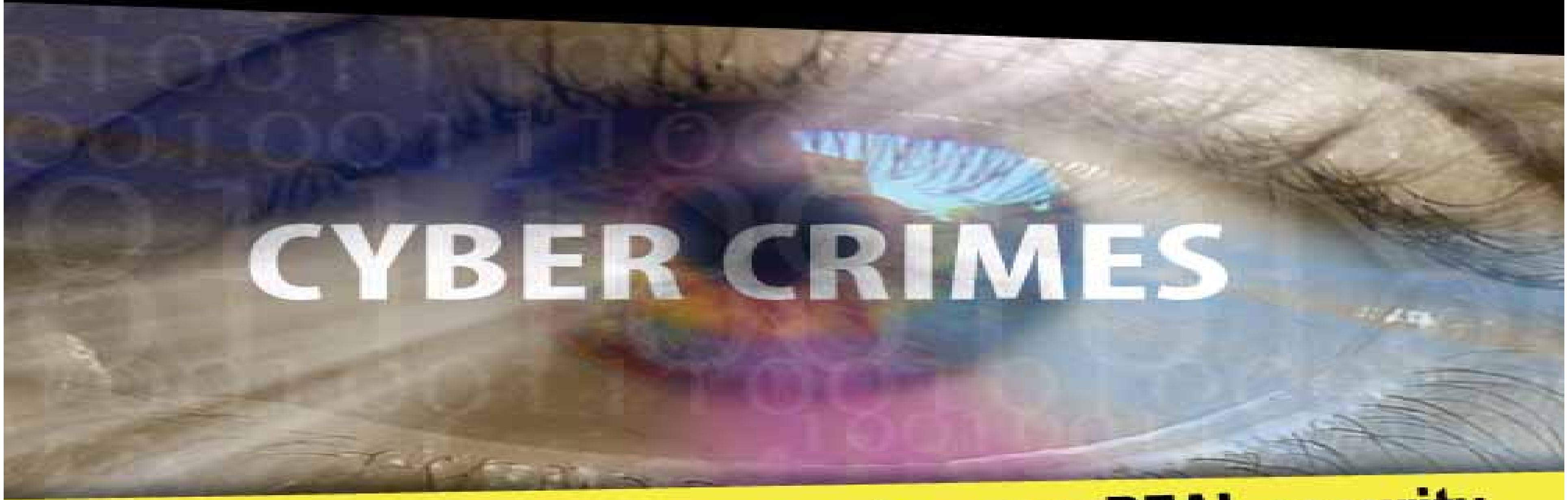
Overview on UNICRI projects against cybercrime

- Hackers Profiling Project (HPP)
- SCADA & NCI’s security
- Digital Forensics and digital investigation techniques
- Cybersecurity Trainings at the UN Campus

unicri
advancing security, serving justice,
building peace

mediaservice.net
CORPORATE SECURITY & IMAGE

FIRST COMPREHENSIVE TRAINING PROGRAMME on



evaluating new threats, assessing your REAL security

- Information Security (InfoSec)
- Hacker Profiling Project (HPP)
- Digital Forensics
- SCADA and NCI

2011

From February 2010 @ UN Campus in Turin, Italy

www.unicri.it/wwd/cybertraining

Strategic relationships and Information-sharing Networks, in order to fight cybercrime

Along the years we have been able to build a network of **special** relationships and **direct** contacts with the following **organizations**, working towards **specific areas of interest** and **shared research topics**:
(this list is may not complete due to NDAs)

Slide or text not supplied with the Public Release of this talk: you should have attended HES 2011 to see this!

Yesterday and today’s Hacking

Crime->Yesterday

“**Every new technology, opens the door to new criminal approaches**”.

- The relationship between **technologies and criminality** has always been – since the very beginning – characterized by a kind of “competition” between the good and the bad guys, just like cats and mice.

- As an example, at the beginning of 1900, when **cars** appeared, the “bad guys” started **stealing them (!)**

- ….the police, in order to contrast the phenomenon, defined the **mandatory use** of car plates…

- ….and the thieves began **stealing the car plates** from the cars (and/or falsifying them).

Crime->Today:Cybercrime

- **Cars** have been substituted by **information**

*You got the **information**, you got the **power**..*

(at least, in **politics**, in the **business world**, in our **personal relationships…**)

- Simply put, this happens because the "*information*" can be **transformed at once** into "something else":

✓ **Competitive advantage (reputation)**

✓ **Sensible/critical information (blackmailing)**

✓ **Money**

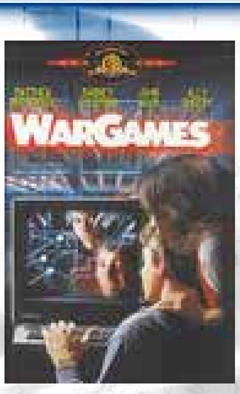
- … **that's why** all of us we want to "*be secure*".

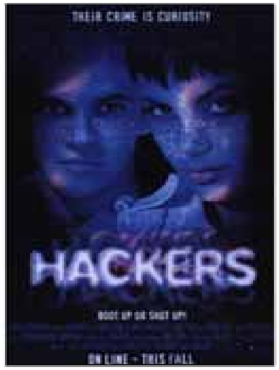
- It's not by chance that it's named "IS": **Information Security** ☺

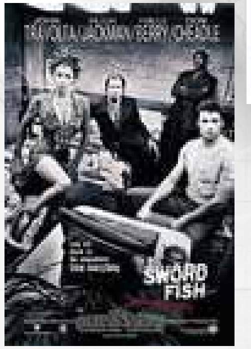
Hacking eras & Hackers’ generations

Things changed…

- **First generation** (70's) was inspired by the **need for knowledge**
- **Second generation** (1980-1984) was driven by **curiosity** plus the knowledge starving: the only way to learn OSs was to **hack them**; later (1985-1990) hacking becomes a **trend**.
- The **Third one** (90's) was simply pushed by the **anger for hacking**, meaning a mix of **addiction**, **curiosity**, **learning new stuff**, **hacking IT systems and networks**, **exchanging info** with the **underground community**. Here we saw new concepts coming, such as hacker's e-zines (Phrack, 2600 Magazine) along with BBS
- **Fourth generation** (2000-today) is driven by **angerness** and **money**: often we can see subjects with a very low know-how, thinking that it's "cool & bragging" being hackers, while they **are not interested** in hacking & phreaking history, culture and ethics. Here hacking meets with politics (**cyber-hacktivism**) or with the criminal world (**cybercrime**).







€, $

Cybercrime: why?

- **QUESTION:**
  - May we state that cybercrime – along with its many, many aspects and views – can be **ranked as #1** in **rising trend** and **global diffusion** ?

- **ANSWER(S):**
- Given that all of you are attendees and speakers here today, I would say that we **already are on the right track** in order **to analyze the problem** ☺

- Nevertheless, some **factors** exist for which the spreading of “e-crime-based” attacks **relays**.

- Let’s take a look at them.

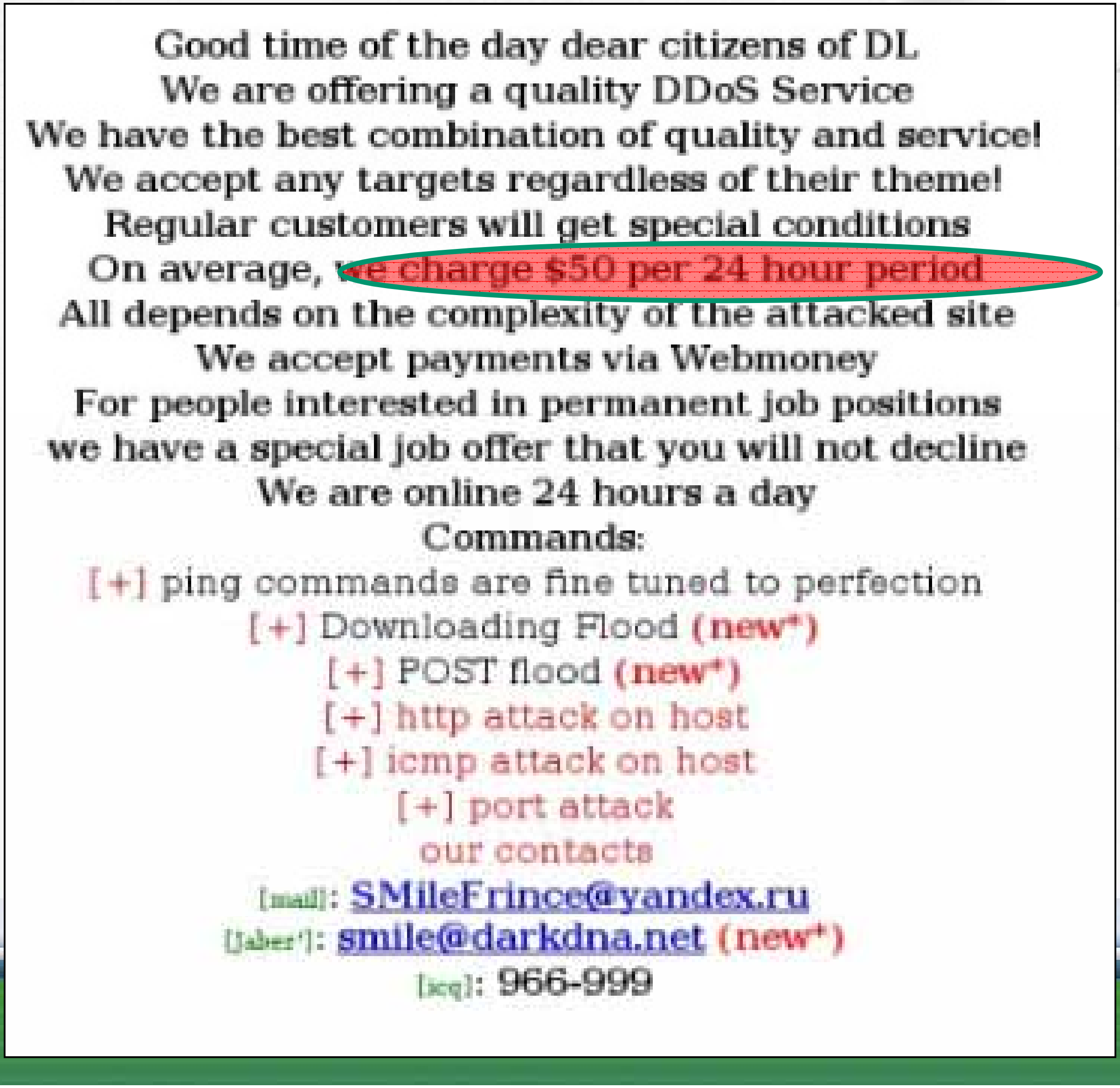
Reasons / 1

- 1. There are **new users, more and more every day**: this means the total amount of **potential victims** and/or attack vectors is increasing. → **Thanks to broadband...**

- 2. **Making money**, “somehow and straight away”. → **WW Economical crisis…**

- 3. Technical know-how public availability & ready-to-go, even when talking about average-high skills: that’s what I name “**hacking pret-à-porter**” → **0-days, Internet distribution system / Black Markets**

Darkness DDoS botnet



Good time of the day dear citizens of DL
We are offering a quality DDoS Service
We have the best combination of quality and service!
We accept any targets regardless of their theme!
Regular customers will get special conditions
On average, we charge $50 per 24 hour period
All depends on the complexity of the attacked site
We accept payments via Webmoney
For people interested in permanent job positions
we have a special job offer that you will not decline
We are online 24 hours a day

Commands:

[+] ping commands are fine tuned to perfection
[+] Downloading Flood (new*)
[+] POST flood (new*)
[+] http attack on host
[+] icmp attack on host
[+] port attack

our contacts
[mail]: SMileFrince@yandex.ru
[Jaber']: smile@darkdna.net (new*)
[icq]: 966-999

Reasons / 2

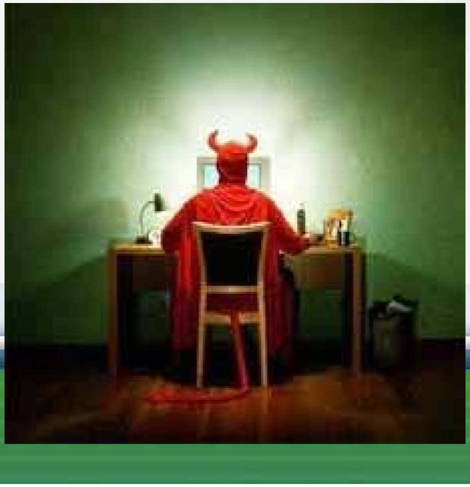
- 4. It’s **extremely easy** to recruit “idiots” and set up **groups**, molding those adepts upon the **bad guy’s needs** (think about e-mules) ⟶ **Newbies, Script Kiddies**

- 5. “They will **never bust me**” ⟶ **Psycology, Criminology**

- 6. **Lack of violent actions** ⟶ **Psycology and Sociology**

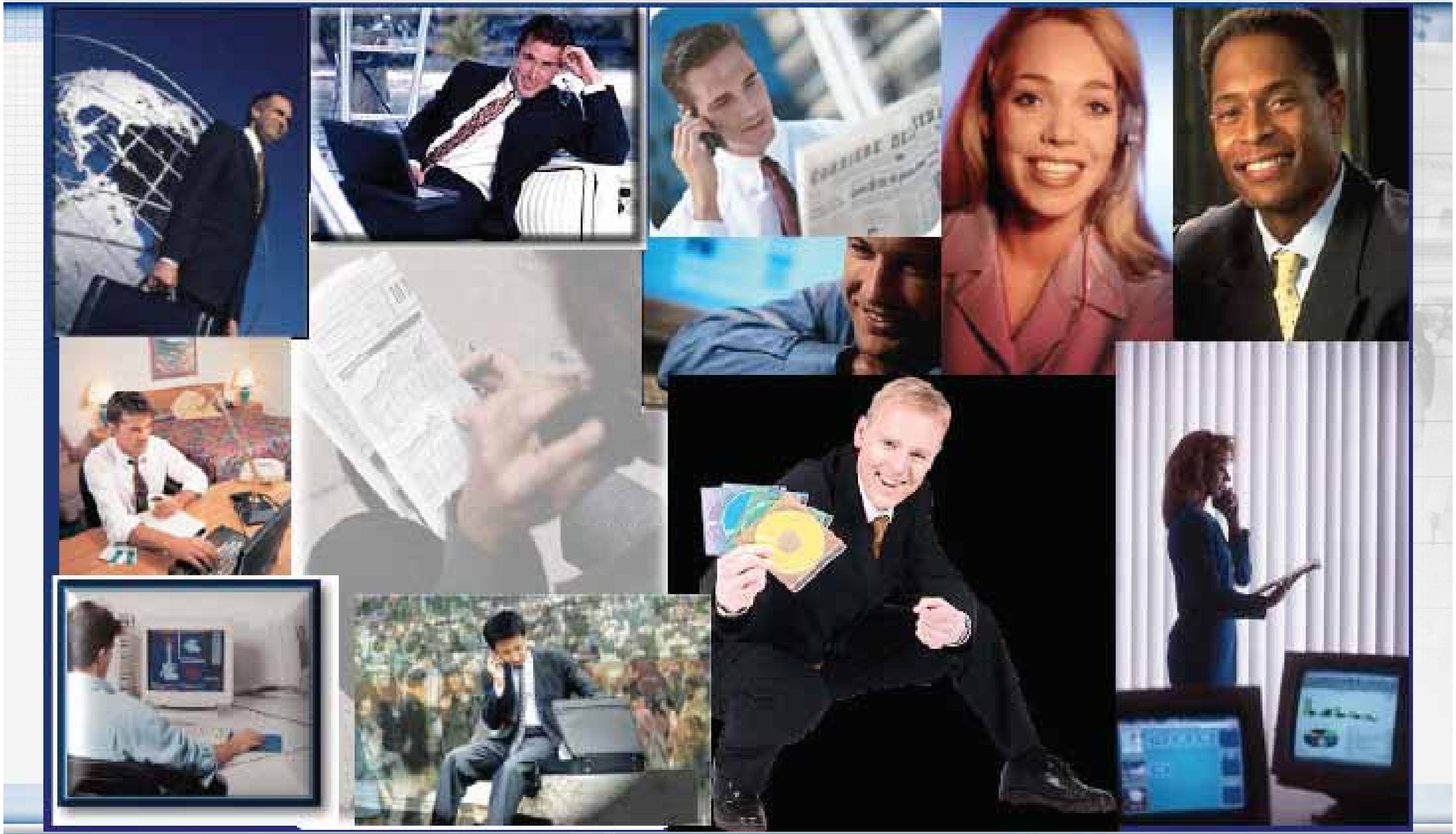
What the heck is changed then??

- What’s really changed is the **attacker’s typology**
- From “bored teens”, doing it for “*hobby and curiosity*” (obviously: during night, pizza-hut’s box on the floor and cans of Red Bull)….
- ...to teenagers and adults not mandatory “ICT” or “hackers”: they just **do it for the money**.
- What’s changed is the **attacker’s profile**, along with its **justifications, motivations and reasons**.
- **Let’s have a quick test!**



Hackers in their environment

“Professionals”



There’s a difference: why?

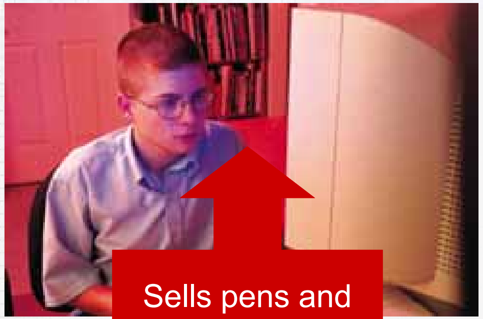
- Why were the guys in the first slide **hackers**, and the others **professionals** ?
- Because of the **PCs** ?
- Because of their “**look**” ?
- Due to the **environments** surrounding them ?
- Because of the “**expression** on their faces” ?

Surprise!
Everything has changed

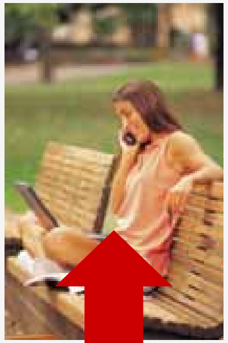
- Erroneus media information **pushed “normal people” minds** to run this approach

- Today, sometimes the **professionals** are the real **criminals**, and **hackers “the good guys”…** (Telecom Italia Scandal, Vodafone Greece Affair, etc…)

Some more examples…

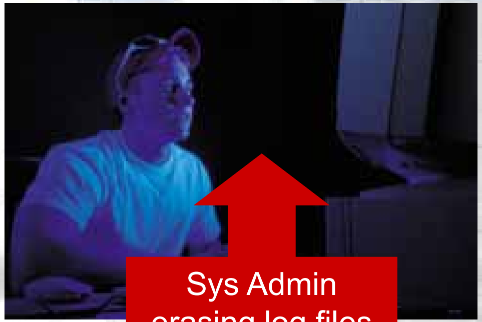


Sells pens and toner on e-bay that he steals at work.



Laughing with a friend over corporate photos she found on your unprotected wi-fi network.

Forwards emails from boss to her reporter friend ever since she didn't get that bonus.



Sys Admin erasing log files after downloading movies all night.

Changing the timestamps on tax records to prepare for an audit.

Understanding Hackers

- It’s **extremely important** that we understand the so-called “hacker’s behaviours”
  - **Don’t limit yourself** to analyse attacks and intrusion techniques: let’s analyze their **social behaviours**
- Try to identify those **not-written rules** of hacker’s subculture
- Explore hacker’s **social organization**
- Let’s zoom on those **existing links** between hacking and organized crime

Welcome to HPP

Hackers

The term hacker has been heavily misused since the 80's; since the 90's, the mainstream have used it to justify every kind of "IT crime", from lame attacks to massive DDoS

Lamers, script-kiddies, industrial spies, hobby hackers….for the mass, they are all the same

From a business point of view, companies don't clearly know who they should be afraid of. To them they're all just "hackers"

Hackers: a blurred image

Yesterday: hacking was an emerging phenomenon – unknown to people & ignored by researchers

Today: research carried out in “mono”: → one type of hacker: ugly (thin, myopic), bad (malicious, destructive, criminal purposes) and “dirty” (asocial, without ethics, anarchic)

Tomorrow (HPP is the future): inter-disciplinary studies that merge criminology and information security → different *typologies* of hackers

HPP purposes

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

Understand the different motivations and identify the actors involved

Observe those *true* criminal actions “in the field”

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

Acquire and disseminate knowledge

Project phases – starting: September 2004

1 – Theoretical collection:
Questionnaire

2 – Observation:
Participation in IT underground security events

3 - Filing:
Database for elaboration/classification of data (phase 1)

4 - Live collection:
Highly customised, new generation Honey-net systems

5 – Gap analysis:
of data from: questionnaire, honey-net, existing literature

6 – HPP "live" assessment
of profiles and correlation of modus operandi through data from phase 4

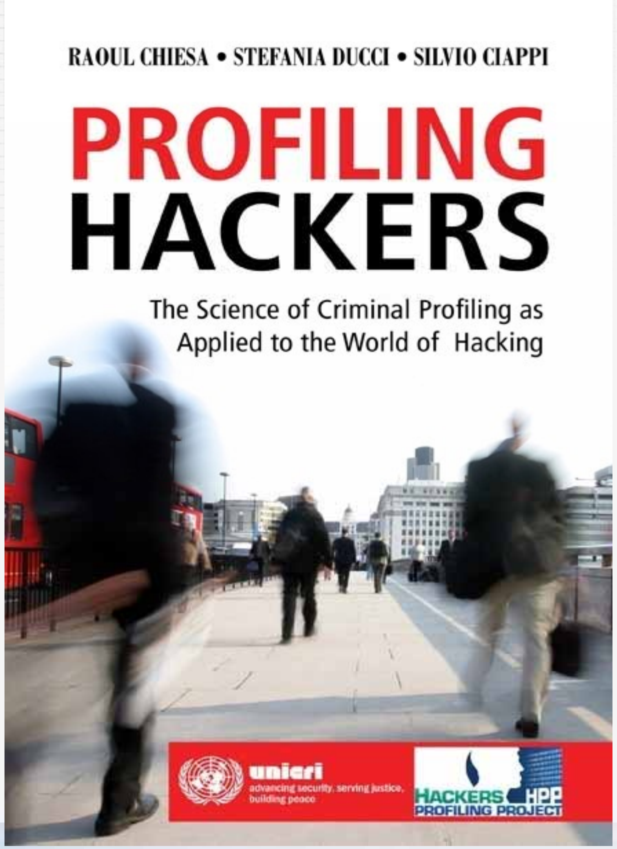
7 – Final profiling:
Redefinition/fine-tuning of hackers profiles used as "de-facto" standard

8 – Diffusion of the model:
elaboration of results, publication of the methodology, raising awareness

Project phases - detail

PHASE	CARRIED OUT		DURATION	NOTES
1 – Theoretical collection	YES	ON-GOING	16 months	Distribution on more levels
2 – Observation	YES	ON-GOING	24 months	From different points of view
3 – Filing	ON-GOING		21 months	The hardest phase
4 – “Live” collection	TO BE COMMENCED		21 months	The funniest phase ☺
5 – Gap & Correlation Analysis	YET TO COME		18 months	The Next Thing
6 – “Live” Assessment	PENDING		16 months	The biggest part of the Project
7 – Final Profiling	PENDING		12 months	“Satisfaction”
8 – Diffusion of the model	PENDING		GNU/FDL ;)	Methodology’s public release

Profiling Hackers – the book



RAOUL CHIESA • STEFANIA DUCCI • SILVIO CIAPPI

PROFILING HACKERS

The Science of Criminal Profiling as Applied to the World of Hacking

unicri
advancing security, serving justice, building peace
HACKERS PROFILING PROJECT
HPP

Content

- Introduction to criminal profiling and cyber-crime
- To be, to think and to live like a hacker
- The Hacker's Profiling Project (HPP)
- Who are hackers? (Part I-II)

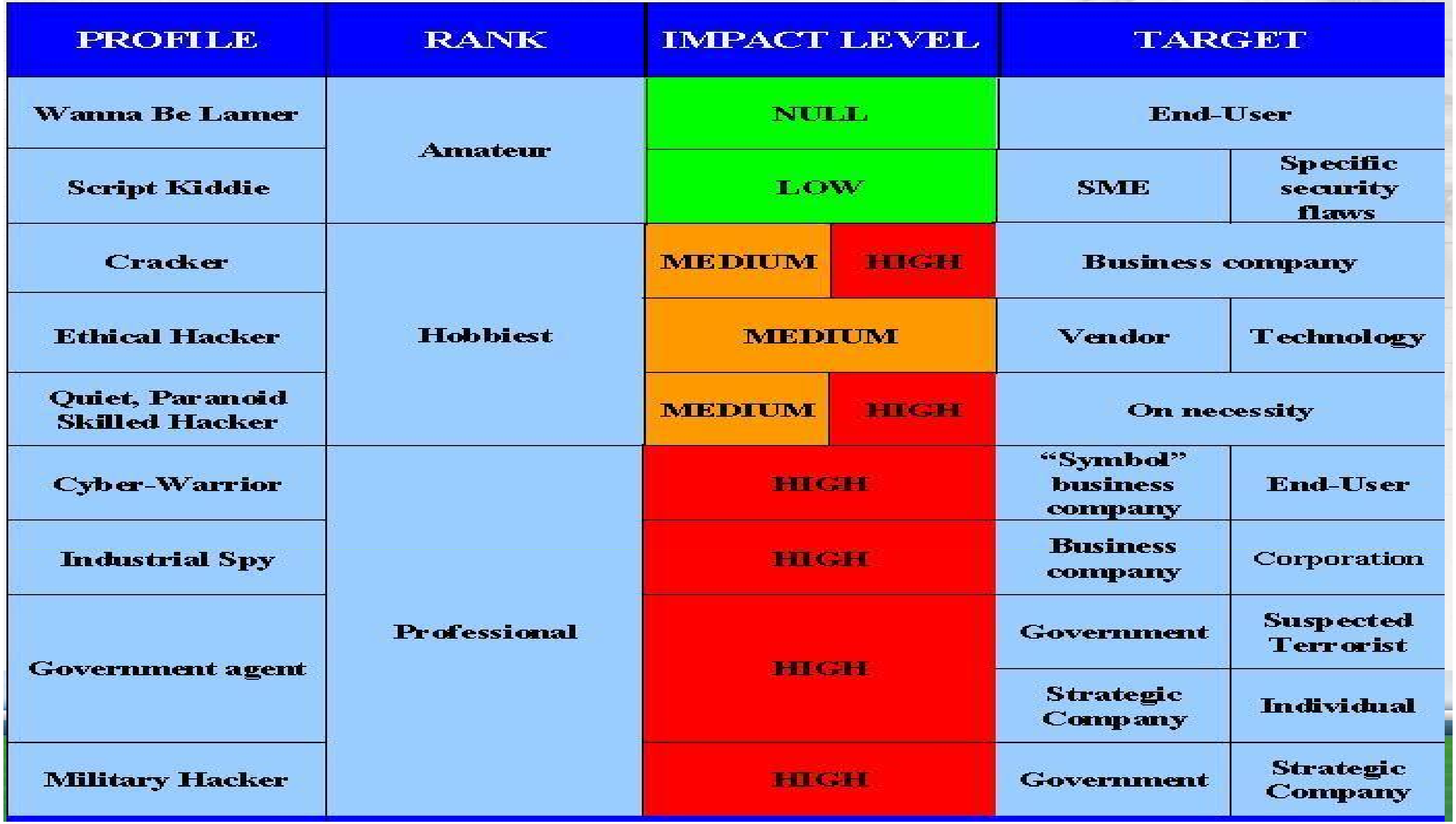
Who is it for?

Professionals involved in the networking activity, police detectives, university professors and students of law interested in criminal psychology as well as primary school and high school teachers dealing with potential hacker students. More in general, this book is designed for anyone interested in understanding the mechanisms behind cyber crimes and criminal psychology.

Evaluation and correlation standards

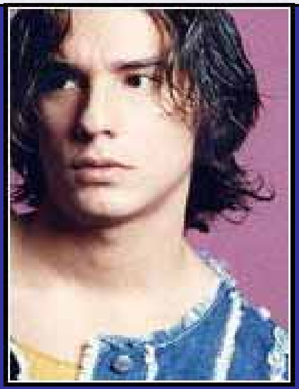
- Modus Operandi (MO)
- Lone hacker or as a member of a group
- Motivations
- Selected targets
- Relationship between motivations and targets
- Hacking career
- Principles of the hacker's ethics
- Crashed or damaged systems
- Perception of the illegality of their own activity
- Effect of laws, convictions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

Detailed analysis and correlation of profiles – table #1



PROFILE	RANK	IMPACT LEVEL	TARGET	
Wanna Be Lamer	Amateur	NULL	End-User	
Script Kiddie		LOW	SME	Specific security flaws
Cracker	Hobbiest	MEDIUM HIGH	Business company	
Ethical Hacker		MEDIUM	Vendor	Technology
Quiet, Paranoid Skilled Hacker		MEDIUM HIGH	On necessity	
Cyber-Warrior	Professional	HIGH	"Symbol" business company	End-User
Industrial Spy		HIGH	Business company	Corporation
Government agent		HIGH	Government	Suspected Terrorist
			Strategic Company	Individual
Military Hacker		HIGH	Government	Strategic Company

The Hackers Profiling Project (HPP)



Detailed analysis and correlation of profiles – table #2

	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 powe / 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

Ok Raoul… so what ?!?

Hacking, today

Numbers

- **285 million records** compromised in 2008 (source: Verizon 2009 Data Breach Investigations Report)

- **2 Billion of US dollars:** that's **RBN**'s 2008 turnover

- **+80 MLN of US$**: **IMU**'s **2010 Turn Over**

- **3 Billion of Euros**: **worldwide** Cybercrime **turnover in 2010** (?)

- **+148% increasing in ATM frauds: more than 500.000.000 € business each year**, just in Europe (source: ENISA "ATM Crime Report 2009")

- **.......bla bla bla**

- Uh ?!? **RBN** ? WTH??

RBN

- **Russian Business Network**
- It’s **not that easy** to explain what it is...
- First of all, cybercrime **IRL means**:
  - ✓ **Phishing & co**
  - ✓ **Malware (rogue AVs, driven-by attacks, fake mobile games, + standard stuff)**
  - ✓ **Frauds & Scams**
  - ✓ **DDoS Attacks**
  - ✓ **Digital Paedophilia (minors rather than <10 children pornography)**
  - ✓ **Generic Porn (who would bother for 10 bucks lost??)**
  - ✓ **On-line games (those fake web sites)**

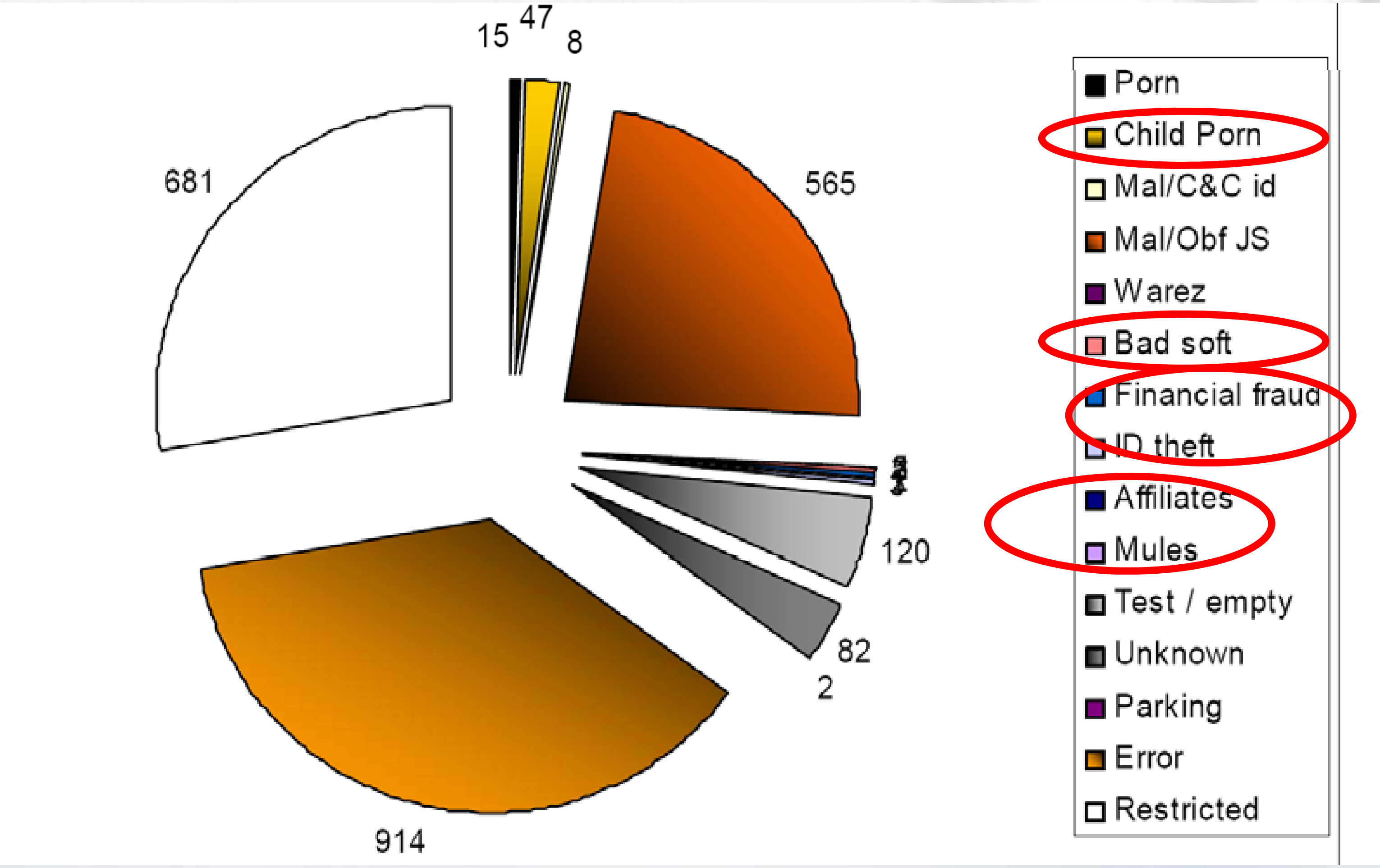
RBN & phishing

- David Bizeul (Head of CERT at Societe Generale, France) wrote an excellent study on RBN. One page was so interesting:

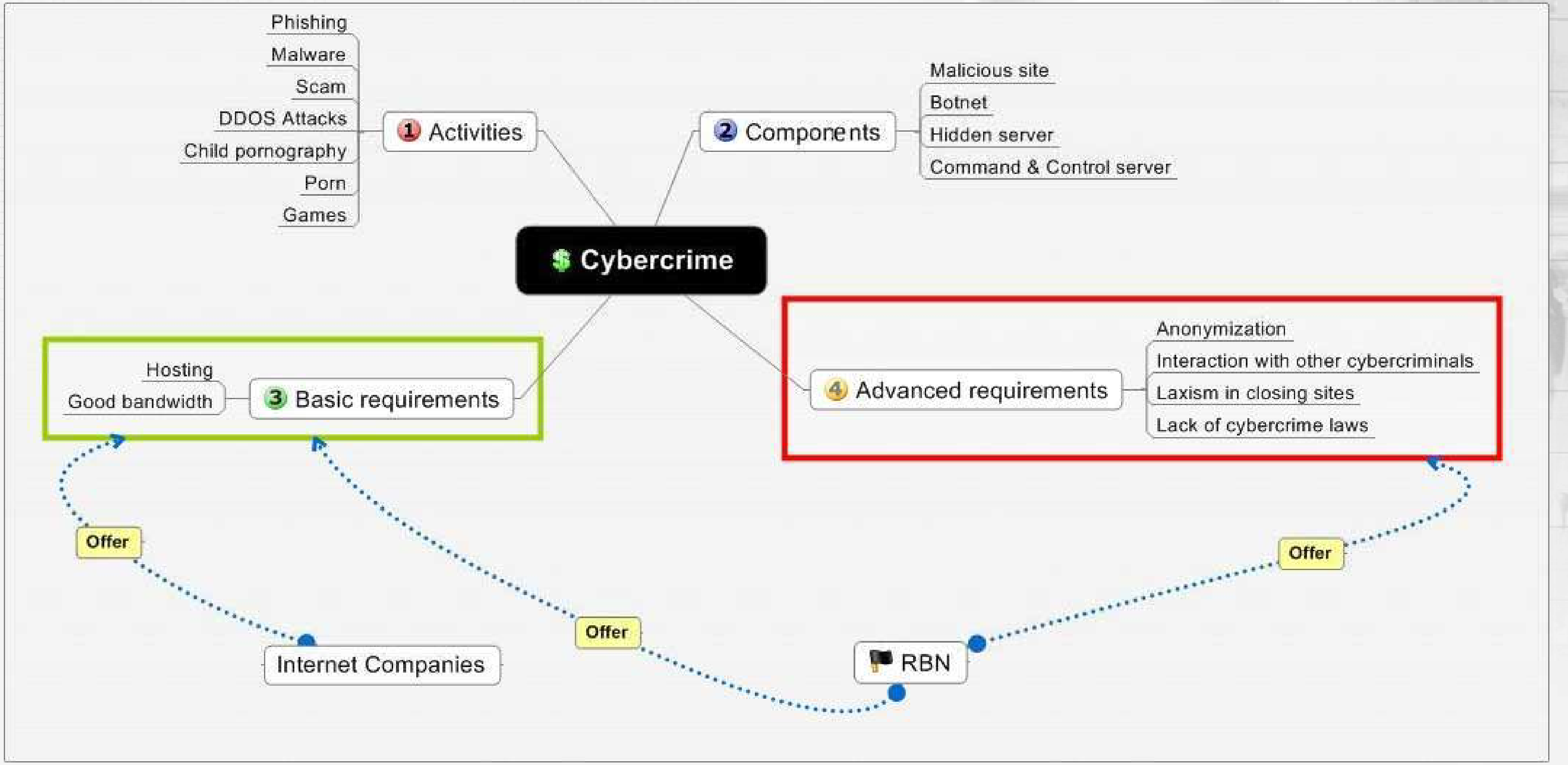
http://194.146.207.18/config

```
storage_send_interval="600" config_file ="$_2341234.TMP" storage_file ="$_2341233.TMP" www_domains_list =
"pageshowlink.com" redirector_url ="citibusinessonline.da-us.citibank.com /cbusol/uSignOn.do  {www}
/usa/citibusiness.php  2 0 3" redirector_url = "*fineco.it  /fineco/PortaleLogin {www} /it/fineco.php 2  0 3"
redirector_url = "onlineid.bankofamerica.com /cgi-bin/sso.login.controller*  {www} /usa/boa_pers/sso.login.php
2  0  2" redirector_url = "onlinebanking-nw.bankofamerica.com /login.jsp*  {www} /usa/boa_pers/sso.login.php
2 0 2" redirector_url = "online.wellsfargo.com  /signon* {www} /usa/wellsfargo.php 2  0 2" redirector_url =
"ibank.barclays.co.uk /olb/*/LoginPasscode.do  {www} /uk/barc/LoginPasscode.php 2  0 2" redirector_url =
"*ebank.hsbc.co.uk /servlet/com.hsbc.ib.app.pib.logon.servlet.OnLogonVerificationServlet {www}
/uk/hsbc/hsbc.php 2  0 2" redirector_url = "online*.lloydstsb.*  /miheld.ibc {www} /uk/lloyds/lloyds.php 2  0 2"
redirector_url = "*halifax-online.co.uk /_mem_bin/UMLogonVerify.asp  {www} /uk/halifax.co.uk.php  2  0  3"
redirector_url = "olb2.nationet.com /signon/SinglePageSignon_wp1.asp*  {www} /uk/nationwide.php 2  0 3"
redirector_url = "webbank.openplan.co.uk /core/webbank.asp  {www} /uk/woolwich.co.uk.php 2 0 3" #DE
redirector_url = "meine.deutsche-bank.de /mod/WebObjects/dbpbc.woa/*  {www}
/de/deutsche-bank.de/login.php 2  0 3" redirector_url = "banking.postbank.de /app/login.prep.do*  {www}
/de/postbank/postbank.de.php 2  0 3" redirector_url = "portal*.commerzbanking.de /P-
Portal/XML/IFILPortal/pgf.html*  {www} /de/commerzbanking/login.php 2  0 2" redirector_url = "www.dresdner-
privat.de /servlet/P/SSA_MLS_PPP_INSECURE_P/pinLogin.do  {www} /de/dresdner-privat/pers.php 2  0 3"
redirector_url = "www.dresdner-privat.de /servlet/N/SSA_MLS_PPP_INSECURE_N/pinLogin.do  {www}
/de/dresdner-privat/corp.php 2  0 3"
```

What about the other IP addresses?

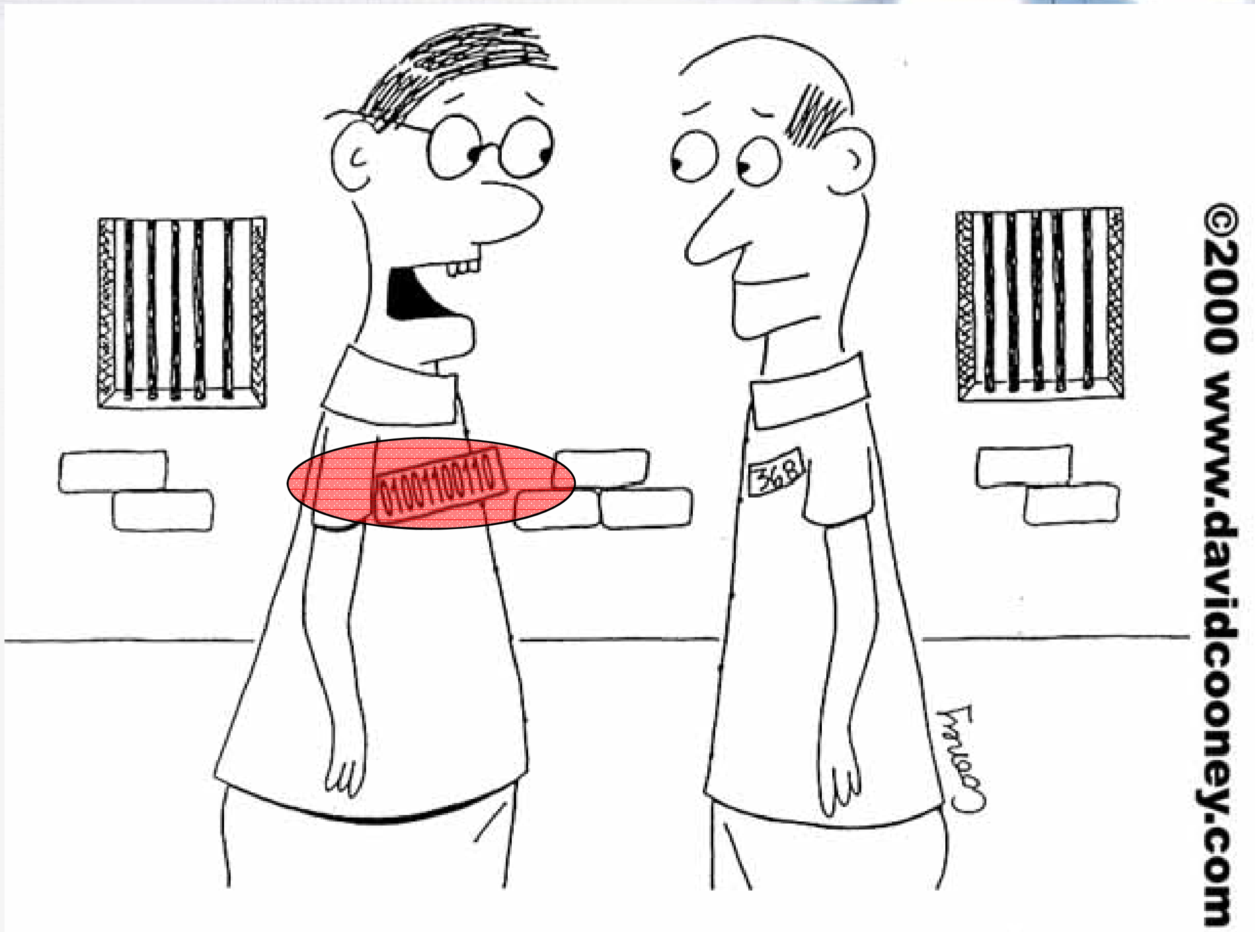


RBN's model


Phishing
Malware
Scam
DDOS Attacks
Child pornography
Porn
Games
1 Activities
2 Components
Malicious site
Botnet
Hidden server
Command & Control server
$ Cybercrime
Hosting
Good bandwidth
3 Basic requirements
4 Advanced requirements
Anonymization
Interaction with other cybercriminals
Laxism in closing sites
Lack of cybercrime laws
Offer
Offer
Offer
Internet Companies
RBN

Underground Economy

“Cybercriminals”



"How’d you know I was in for cyber crime?"

UE

- Underground Economy is the concept thanks to which we will not experience anymore – in the **next future** – “bank robbings”
- Nowadays the ways in order **to fraud and steal money** are SO MANY. And, the world is just full of **unexperienced, not-educated users**.
- What is needed is to “clean” the money: money laundering. They need the **mules**.

UE: the approach

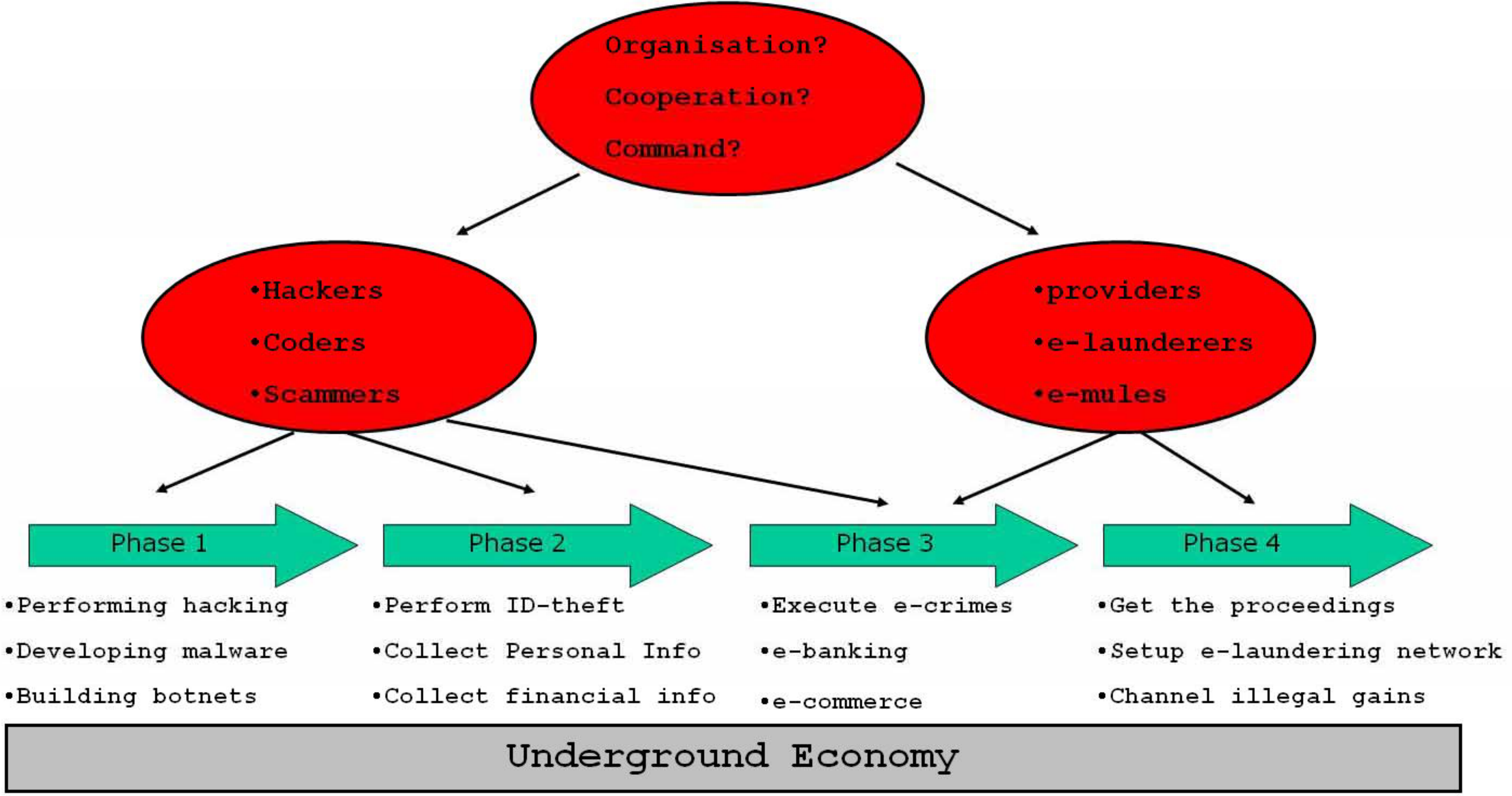
1. **Basics: Malware and Botnets**
   Create the malware, build the botnet

2. **Identity theft**
   Stealing personal and financial credentials (e-banking)

3. **Running the e-crime**
   i.e.: e-Banking attacks and e-commerce frauds (Ebay docet)

4. **Money laundering**
   Setup money laundering's networks

UE Business Model



Organisation?

Cooperation?

Command?

- Hackers
- Coders
- Scammers

- providers
- e-launderers
- e-mules

Phase 1

- Performing hacking
- Developing malware
- Building botnets

Phase 2

- Perform ID-theft
- Collect Personal Info
- Collect financial info

Phase 3

- Execute e-crimes
- e-banking
- e-commerce

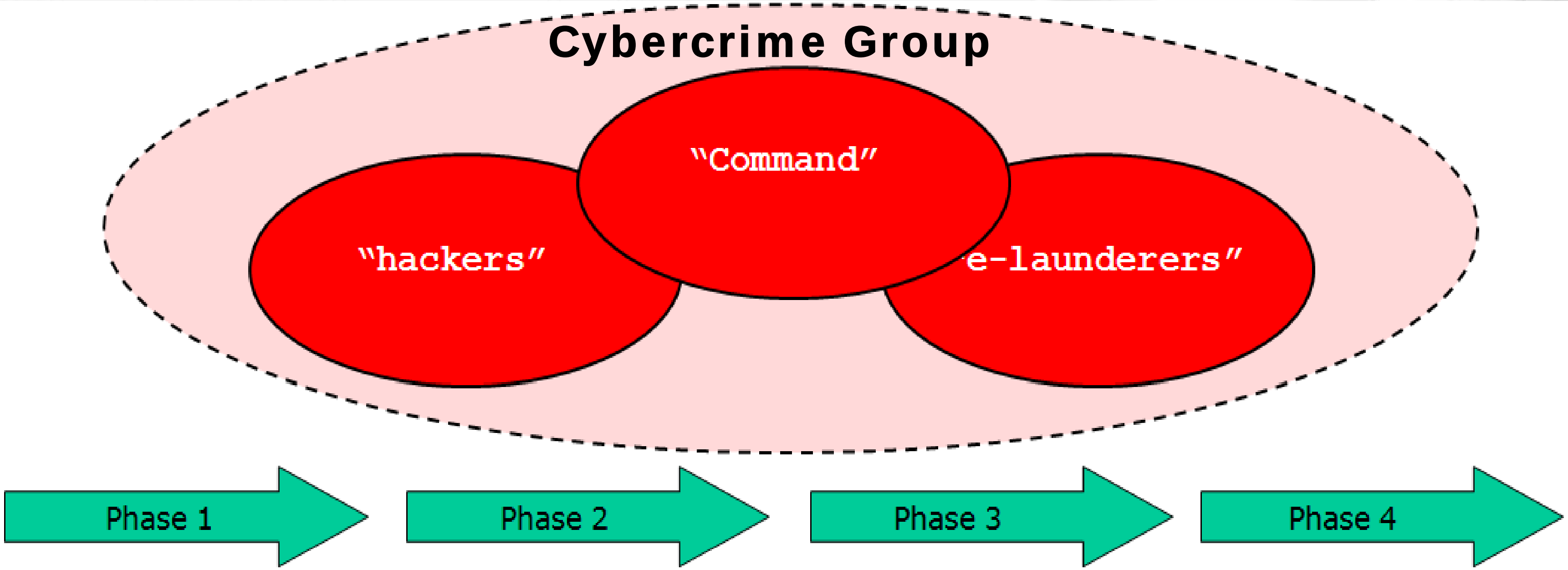
Phase 4

- Get the proceedings
- Setup e-laundering network
- Channel illegal gains

Underground Economy

- trade stolen goods, stolen information, malware, tools, expertise, skills

UE Cooperation Model



Cybercrime Group

“hackers”

“Command”

e-launderers”

Phase 1

- Performing hacking
- Developing malware
- Building botnets

Phase 2

- Perform ID-theft
- Collect Personal Info
- Collect financial info

Phase 3

- Execute e-crimes
- e-banking
- e-commerce

Phase 4

- Get the proceedings
- Setup e-laundering network
- Channel illegal gains

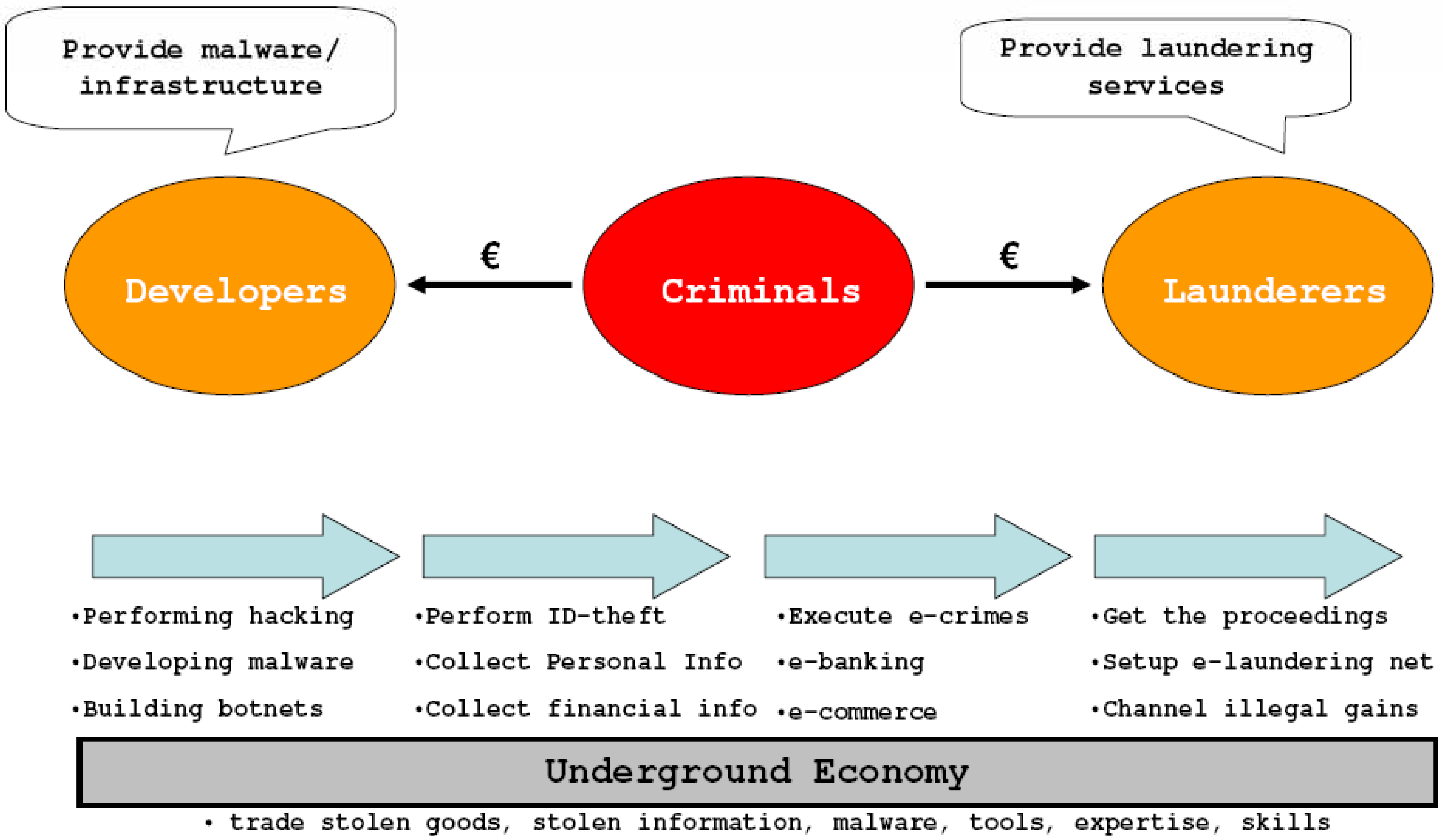
Underground Economy

- trade stolen goods, stolen information, malware, tools, expertise, skills

Surprise.... ☹

- This was happening last time **one year ago**.
- Now there's **IMU** (Innovative Marketing Ukraine) and other **"spare" organized crime gangs**.
- So, they've **changed their business model** (!)

Cybercrime Business Model II



Provide malware/ infrastructure

Provide laundering services

Developers

€

Criminals

€

Launderers

- •Performing hacking
- •Developing malware
- •Building botnets

- •Perform ID-theft
- •Collect Personal Info
- •Collect financial info

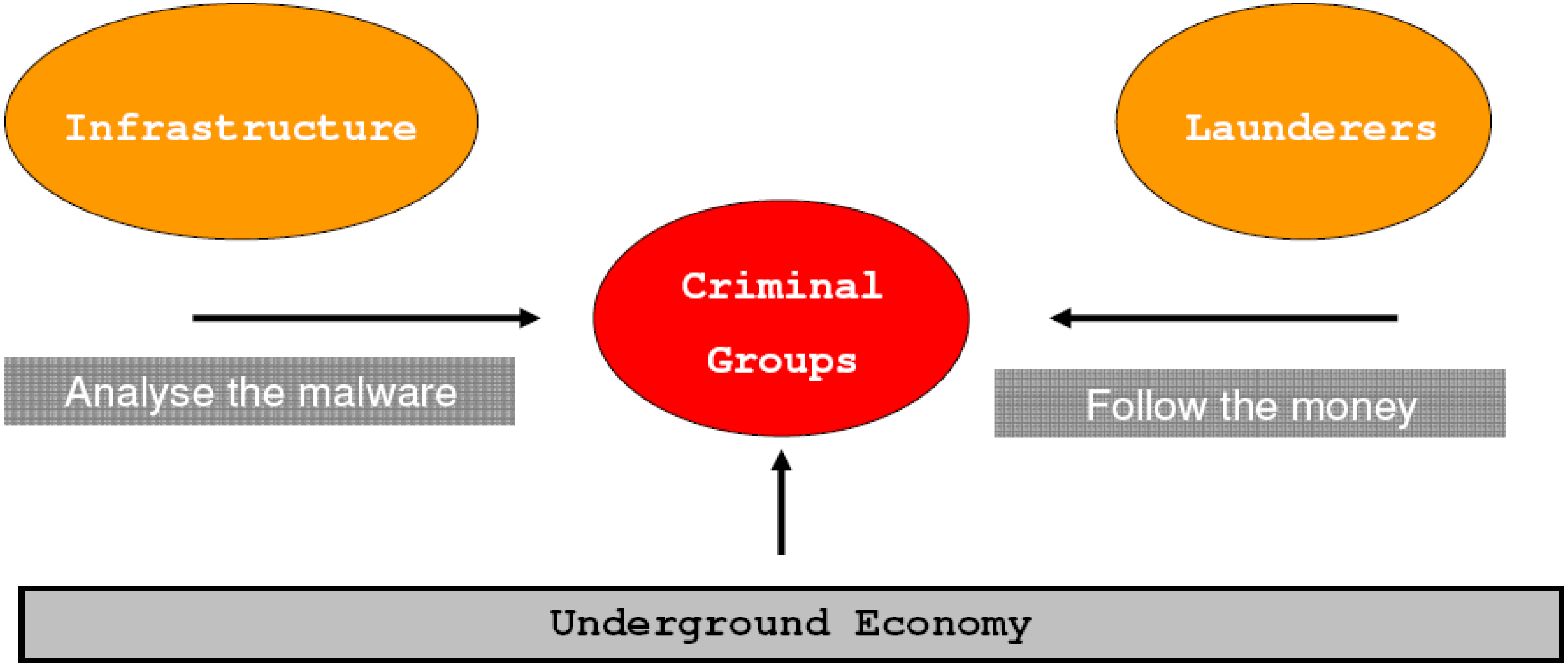
- •Execute e-crimes
- •e-banking
- •e-commerce

- •Get the proceedings
- •Setup e-laundering net
- •Channel illegal gains

Underground Economy

- trade stolen goods, stolen information, malware, tools, expertise, skills

Investigative Opportunities



Infrastructure

Launderers

Criminal Groups

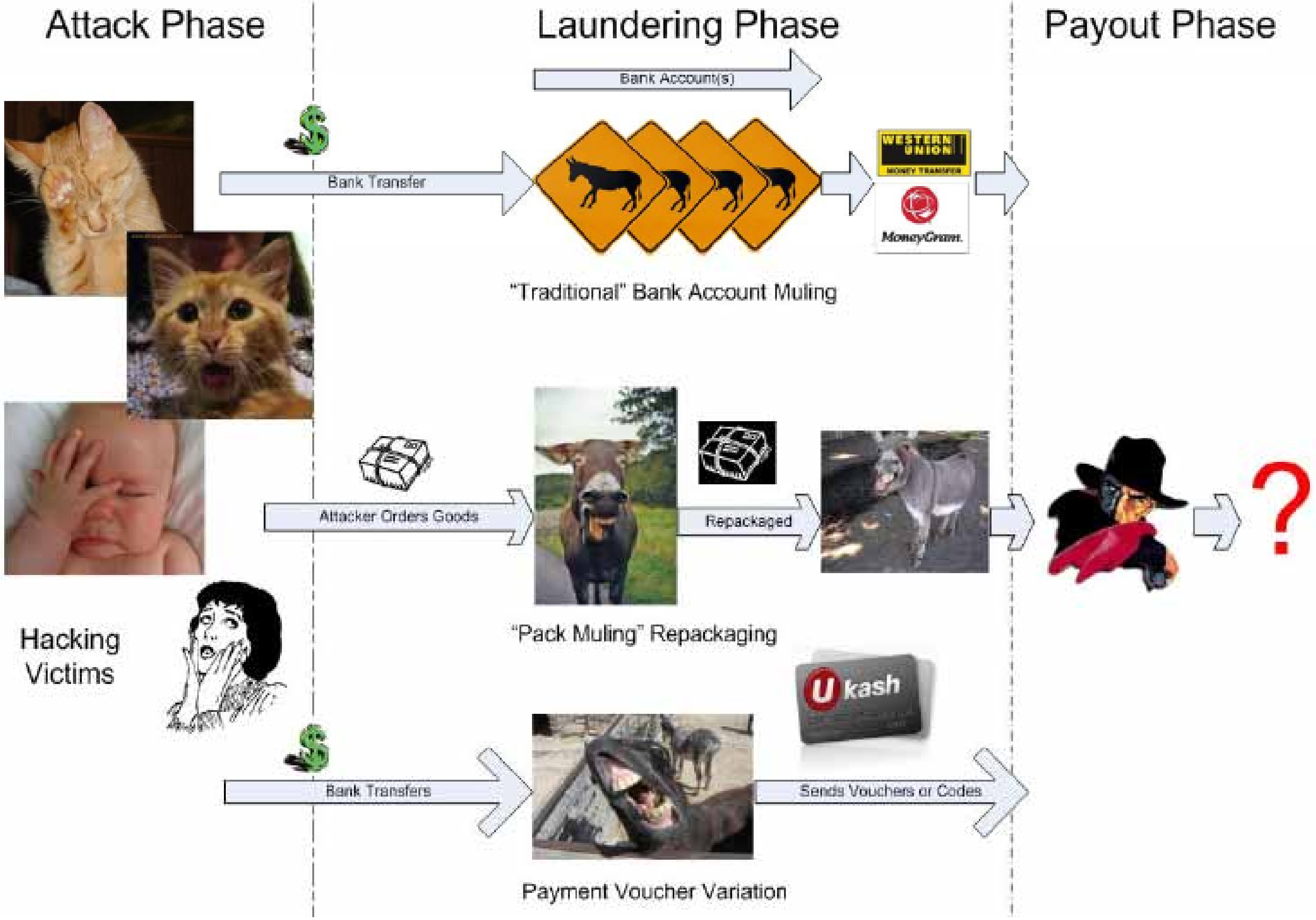
Analyse the malware

Follow the money

Underground Economy

- trade stolen goods, stolen information, malware, tools, expertise, skills

Follow the money!



Who’s beyond ?

- Next slides will contain images from real Law Enforcement operations, as well as undercover operations.

- Please, stop video recording, no pictures and….DO NOT DO THIS AT HOME ! ;)

- Thanks.

Carding 101

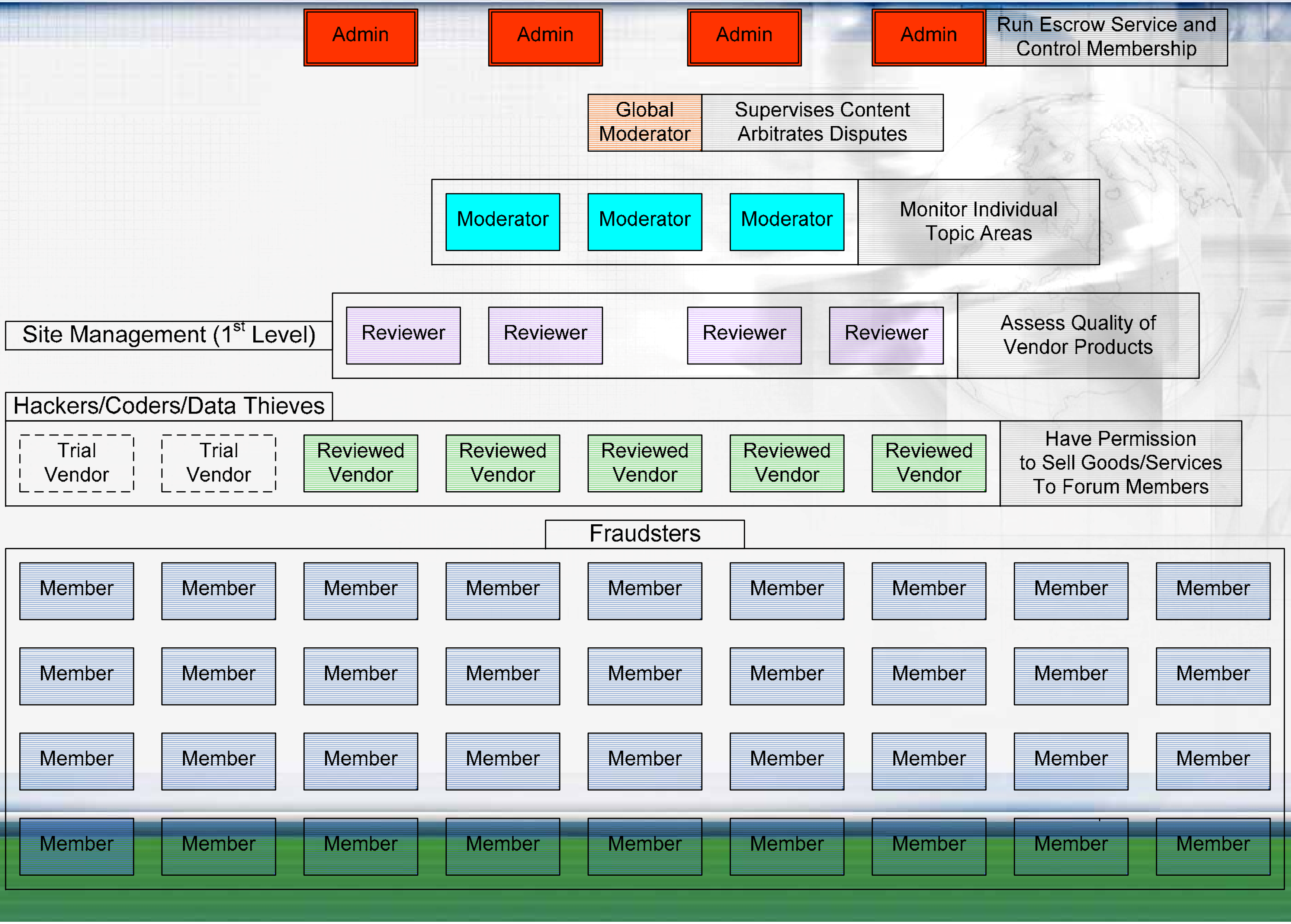
Slide or text not supplied with the Public Release of this talk: you should have attended HES 2011 to see this!

Who lays behind this ?

Slide or text not supplied with the Public Release of this talk: you should have attended HES 2011 to see this!

Slide or text not supplied with the Public Release of this talk: you should have attended HES 2011 to see this!

The organizational model



Admin Admin Admin Admin

Run Escrow Service and Control Membership

Global Moderator

Supervises Content Arbitrates Disputes

Moderator Moderator Moderator

Monitor Individual Topic Areas

Site Management (1st Level)

Reviewer Reviewer Reviewer Reviewer

Assess Quality of Vendor Products

Hackers/Coders/Data Thieves

Trial Vendor Trial Vendor Reviewed Vendor Reviewed Vendor Reviewed Vendor Reviewed Vendor Reviewed Vendor

Have Permission to Sell Goods/Services To Forum Members

Fraudsters

Member Member Member Member Member Member Member Member Member

Member Member Member Member Member Member Member Member Member

Member Member Member Member Member Member Member Member Member

Member Member Member Member Member Member Member Member Member

Who's beyond?

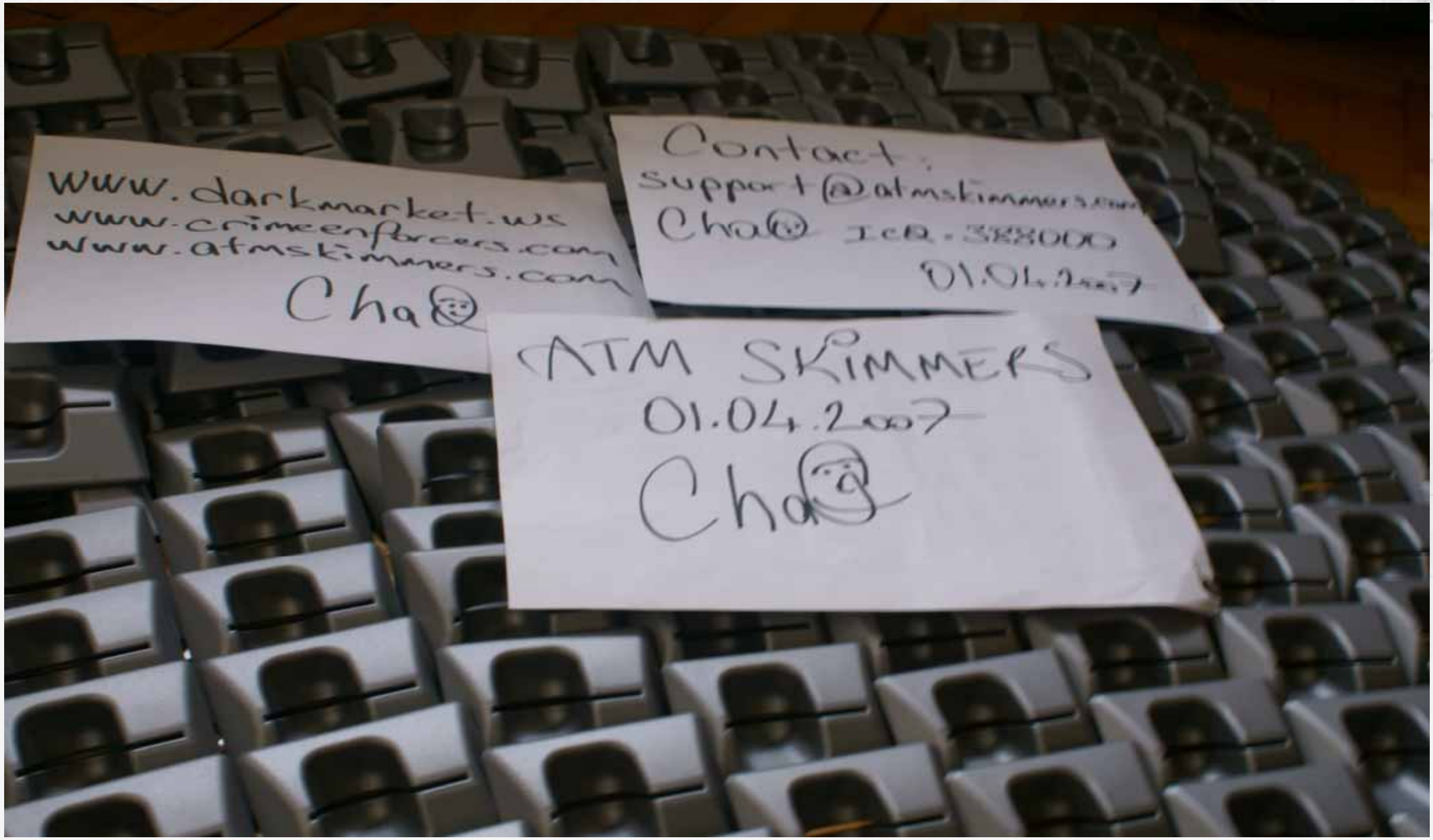
Slide or text not supplied with the Public Release of this talk: you should have attended HES 2011 to see this!

Who's beyond ?

Slide or text not supplied with the Public Release of this talk: you should have attended HES 2011 to see this!

Slide or text not supplied with the Public Release of this talk: you should have attended HES 2011 to see this!

Who’s beyond?


www.darkmarket.ws
www.crimeenforcers.com
www.atmskimmers.com
Cha
Contact:
support@atmskimmers.com
Cha ICQ: 388000
01.04.2007
ATM SKIMMERS
01.04.2007
Cha

Early Arrests

Markus Kellerer aka Matrix001

& Five Others, May 2007-Oct. 2007

Germany

Co-Founder

Renu Subramaniam aka JiLsi

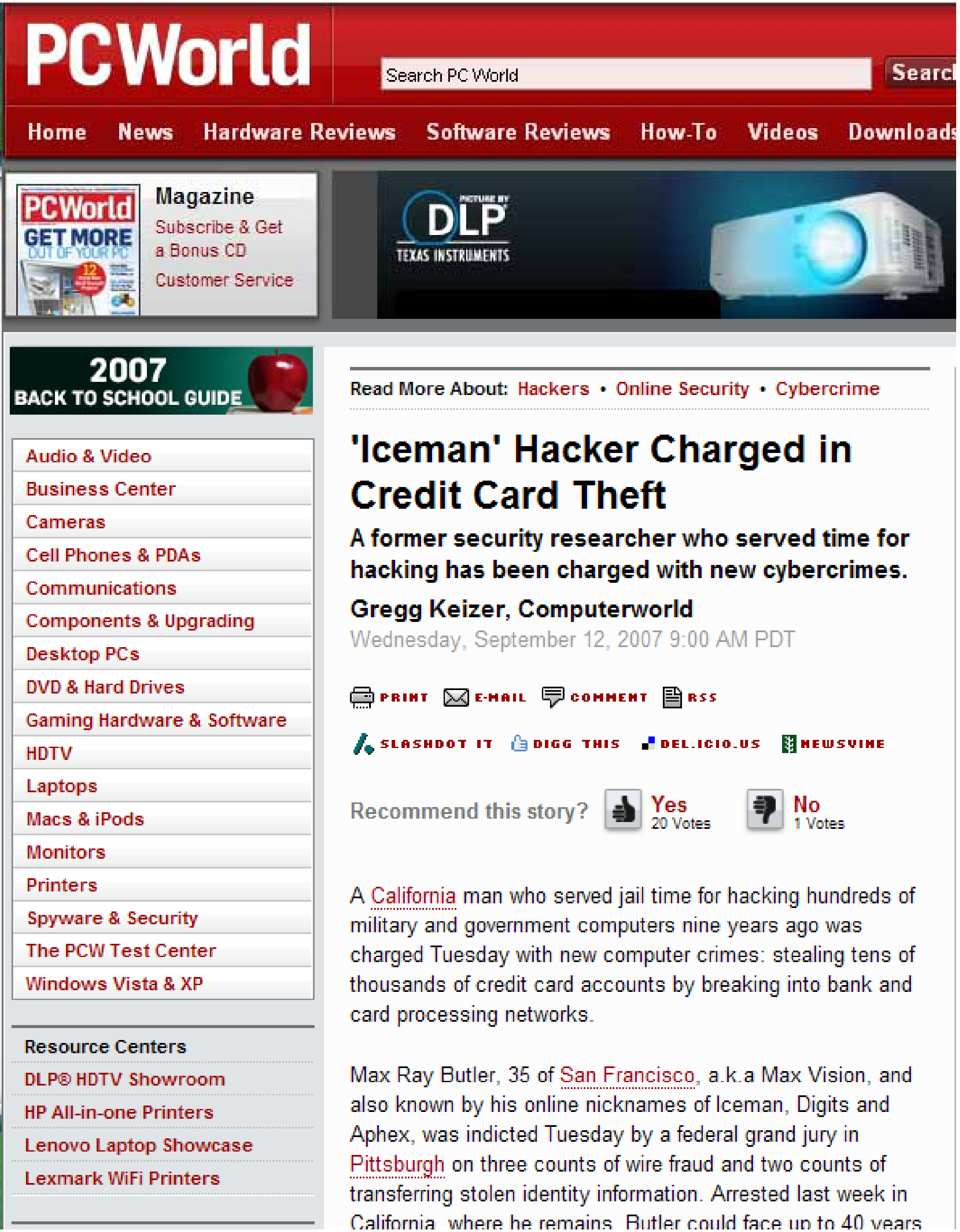
July 2007

United Kingdom

Founder

Santa Clara County Sheriff

Max Butler, aka Iceman
September 2007
San Francisco/Richmond
Founder of CardersMarket
$86 Million in actual Fraud Loss



'Iceman' Hacker Charged in Credit Card Theft

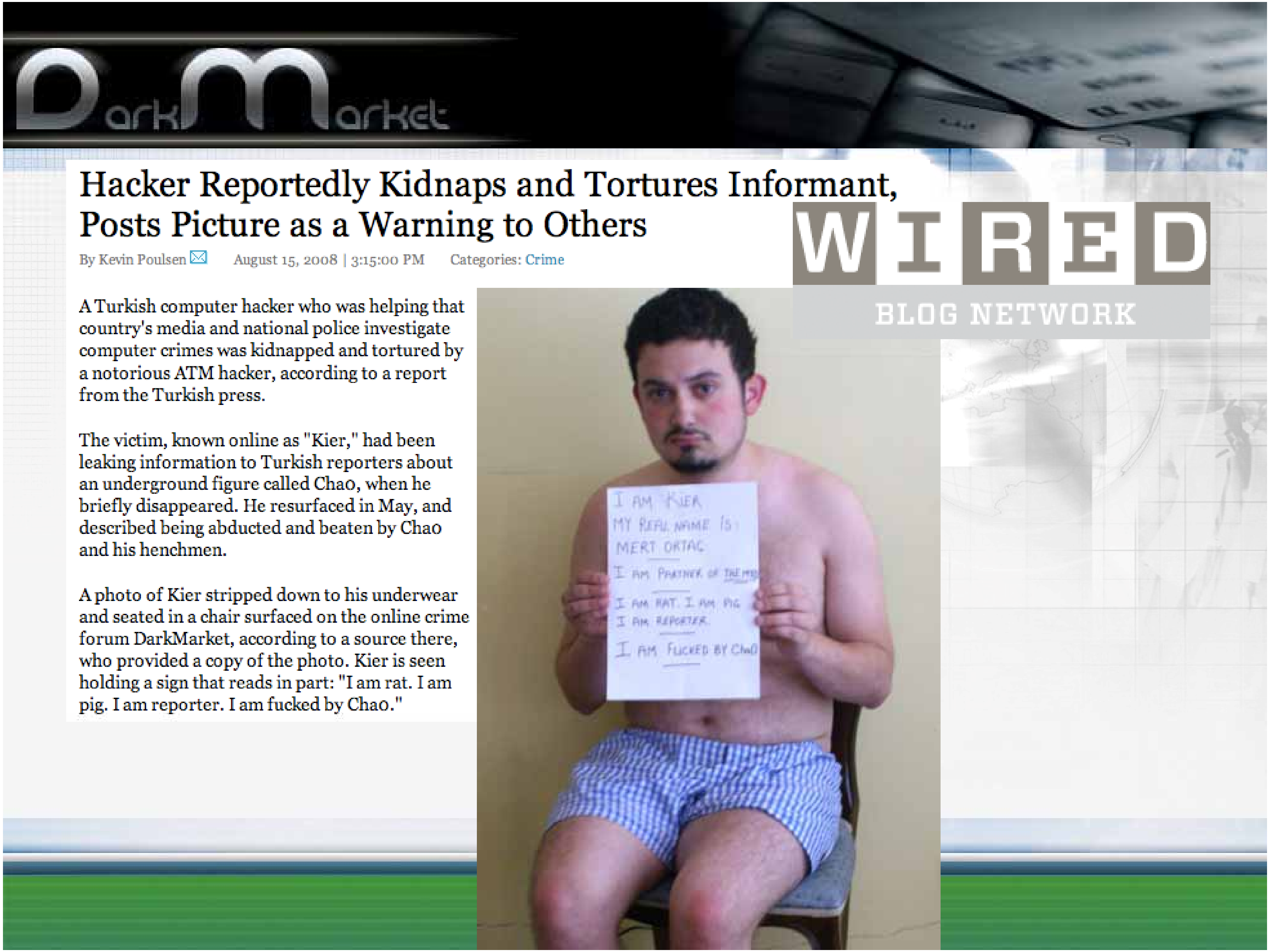
A former security researcher who served time for hacking has been charged with new cybercrimes.

Gregg Keizer, Computerworld

Wednesday, September 12, 2007 9:00 AM PDT

A California man who served jail time for hacking hundreds of military and government computers nine years ago was charged Tuesday with new computer crimes: stealing tens of thousands of credit card accounts by breaking into bank and card processing networks.

Max Ray Butler, 35 of San Francisco, a.k.a Max Vision, and also known by his online nicknames of Iceman, Digits and Aphex, was indicted Tuesday by a federal grand jury in Pittsburgh on three counts of wire fraud and two counts of transferring stolen identity information. Arrested last week in California, where he remains, Butler could face up to 40 years



DarkMarket

WIRED

BLOG NETWORK

Hacker Reportedly Kidnaps and Tortures Informant, Posts Picture as a Warning to Others

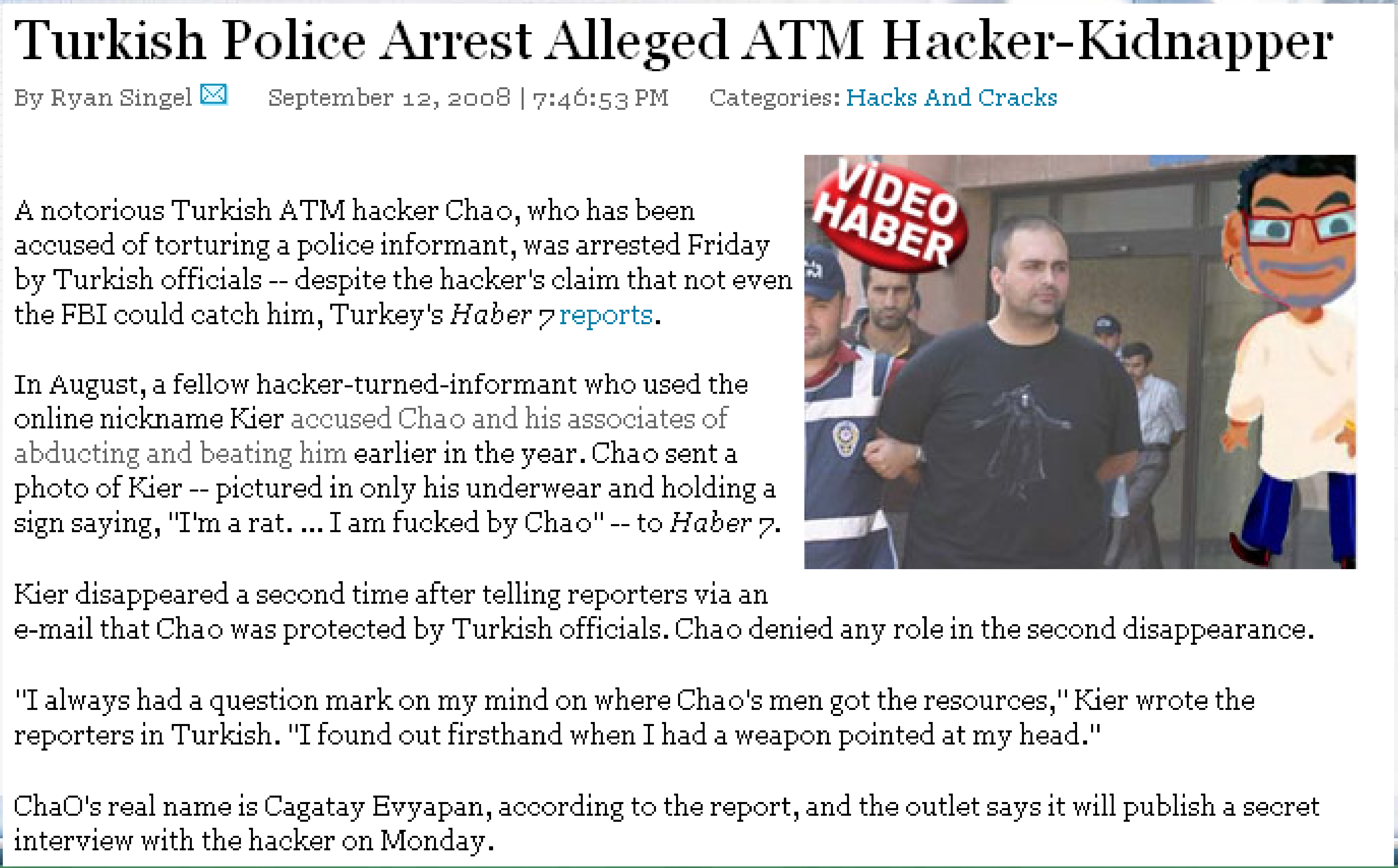
By Kevin Poulsen ✉ August 15, 2008 | 3:15:00 PM Categories: Crime

A Turkish computer hacker who was helping that country's media and national police investigate computer crimes was kidnapped and tortured by a notorious ATM hacker, according to a report from the Turkish press.

The victim, known online as "Kier," had been leaking information to Turkish reporters about an underground figure called Chao, when he briefly disappeared. He resurfaced in May, and described being abducted and beaten by Chao and his henchmen.

A photo of Kier stripped down to his underwear and seated in a chair surfaced on the online crime forum DarkMarket, according to a source there, who provided a copy of the photo. Kier is seen holding a sign that reads in part: "I am rat. I am pig. I am reporter. I am fucked by Chao."

DarkMarket



Turkish Police Arrest Alleged ATM Hacker-Kidnapper

By Ryan Singel ✉ September 12, 2008 | 7:46:53 PM Categories: Hacks And Cracks

A notorious Turkish ATM hacker Chao, who has been accused of torturing a police informant, was arrested Friday by Turkish officials -- despite the hacker's claim that not even the FBI could catch him, Turkey's *Haber 7* reports.

In August, a fellow hacker-turned-informant who used the online nickname Kier accused Chao and his associates of abducting and beating him earlier in the year. Chao sent a photo of Kier -- pictured in only his underwear and holding a sign saying, "I'm a rat. ... I am fucked by Chao" -- to *Haber 7*.

Kier disappeared a second time after telling reporters via an e-mail that Chao was protected by Turkish officials. Chao denied any role in the second disappearance.

"I always had a question mark on my mind on where Chao's men got the resources," Kier wrote the reporters in Turkish. "I found out firsthand when I had a weapon pointed at my head."

ChaO's real name is Cagatay Evyapan, according to the report, and the outlet says it will publish a secret interview with the hacker on Monday.

Who’s beyond?

Slide or text not supplied with the Public Release of this talk: you should have attended HES 2011 to see this!

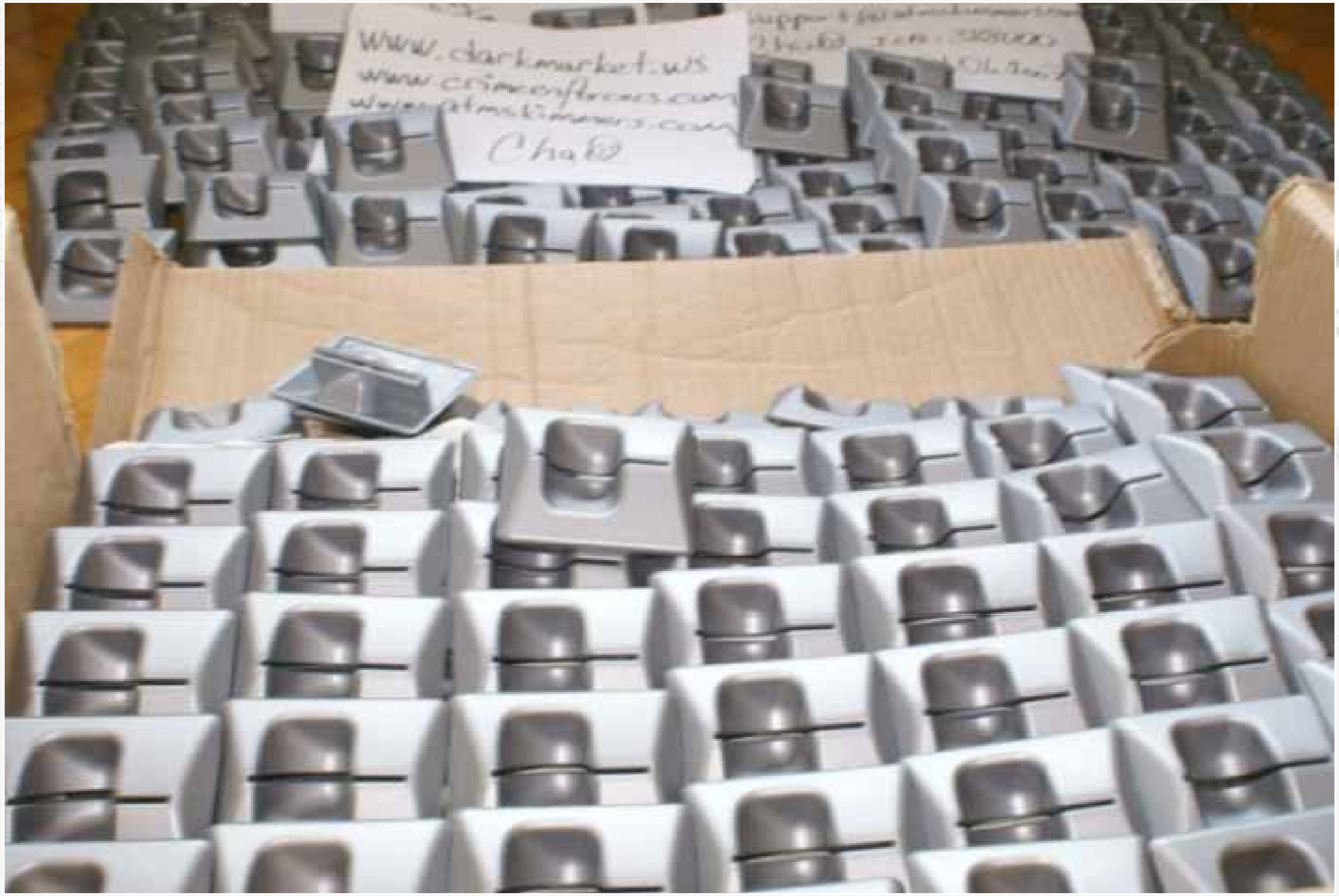
Who's beyond?

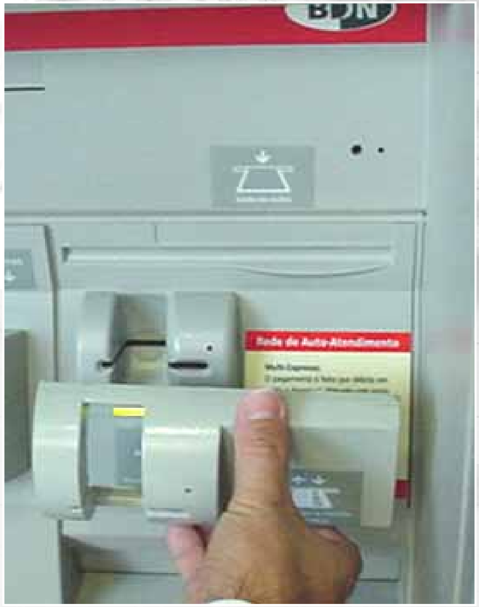
Slide or text not supplied with the Public Release of this talk: you should have attended HES 2011 to see this!

Chi c’è dietro ?

Slide or text not supplied with the Public Release of this talk: you should have attended HES 2011 to see this!

Who's beyond?


www.darkmarket.ws
www.crimesoftrees.com
www.atmskimmers.com
Cha@


BDN
Rede de Auto-Atendimento

Le feste per "i dealer"

Slide or text not supplied with the Public Release of this talk: you should have attended HES 2011 to see this!

Girls, money, cars..

Slide or text not supplied with the Public Release of this talk: you should have attended HES 2011 to see this!

Girls, money, cars..

Slide or text not supplied with the Public Release of this talk: you should have attended HES 2011 to see this!

Videoclip Romania (2010)

Hi-Tech Crime Police Unit enters in ATM Skimmer factory

Some more bad guys…

(thanks to Jon Orbeton, PayPal US, Hi-Tech Fraud Department)

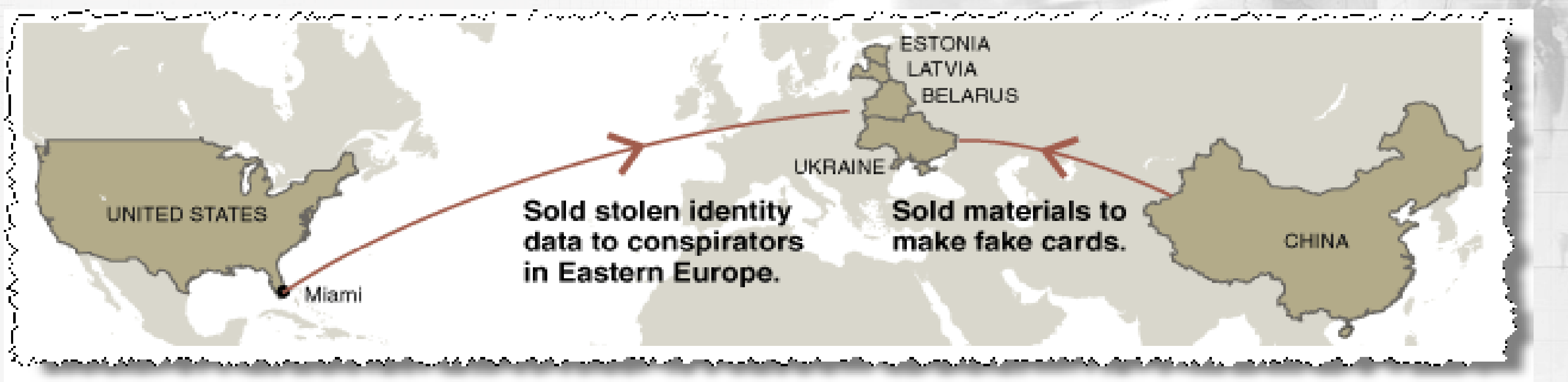
NOTE: the following slides will NOT be published

NOTE: PLEASE DO NOT SHOOT ANY PICTURES

Global Trail of an Online Crime Ring

The New York Times

"Agents connected the ICQ user name to an e-mail address at a Russian-based Internet provider…"



ESTONIA
LATVIA
BELARUS
UKRAINE
UNITED STATES
Miami
CHINA
Sold stolen identity data to conspirators in Eastern Europe.
Sold materials to make fake cards.

"Open sources can provide up to 90% of the information needed to meet most U.S. intelligence needs" *-- Deputy Director of National Intelligence, Thomas Fingar*

Image: NY Times

Cybercriminals

We must investigate the *Disease*, not just the *Symptoms*

Malware is extensively reverse engineered --

Slide or text not supplied with the Public Release of this talk: you should have attended HES 2011 to see this!

Yet the organizations that release it are often ignored…

Online to Real-Life

Slide or text not supplied with the Public Release of this talk: you should have attended HES 2011 to see this!

Online to Real-Life

Money Mules

Slide or text not supplied with the Public Release of this talk: you should have attended HES 2011 to see this!

Online to Real-Life

Slide or text not supplied with the Public Release of this talk: you should have attended HES 2011 to see this!

Online to Real-Life

Slide or text not supplied with the Public Release of this talk: you should have attended HES 2011 to see this!

Rogue AV: Bakasoftware Kingpin

Slide or text not supplied with the Public Release of this talk: you should have attended HES 2011 to see this!

Pharma Programs: Glavmed

Slide or text not supplied with the Public Release of this talk: you should have attended HES 2011 to see this!

RedEye

Slide or text not supplied with the Public Release of this talk: you should have attended HES 2011 to see this!

RedEye

Slide or text not supplied with the Public Release of this talk: you should have attended HES 2011 to see this!

Slide or text not supplied with the Public Release of this talk: you should have attended HES 2011 to see this!

Final toughts

- The hacking world has **not always been linked** to those true criminal actions.

- Those **researches carried out until now**, have **not properly snapshot** the hacking world and its "tunings".

- At the same time, nowaday's **hacking is moving** (transforming?) towards crime. **And, different elements began working together** (see next slides).

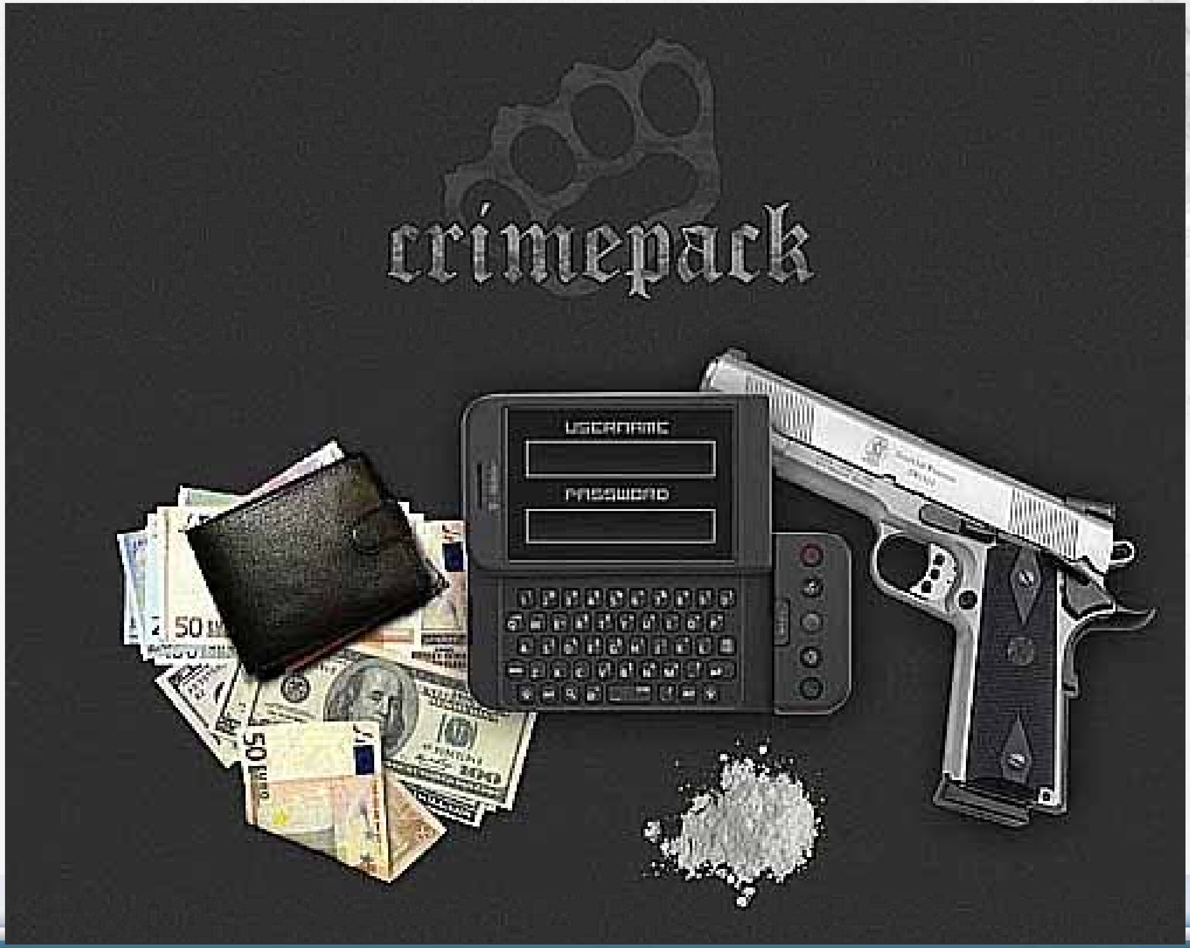
- Cybercrime and Underground Economy problem **is not** "a tech-people issue": rather, it is an issue for **ALL of us**, representing an impact on the countries' ecosystem that could reveal itself as **devastating**.

- Also, **forget** fighting cybercrime on **your own**: **you just can't**.

- That's why my last slides are on **cybercrime's answers** and **VTFs** (Virtual Task Forces).

Extras for HES!

What's next? The Dark Links



Human Organs trafficking

- **September 2010**, Asti (North-West of Italy)

- Police was eavesdropping on phone calls from and to the “Capo dei Capi” of a **Nigerian gang**, specialized in **cloned credit cards** and **elite cars theft**.

- In one of this calls, a guy said to the Boss: “the Kidneys are ready”.

- So, what we have here? Organized Crime “buying” Human Organs from Nigeria – using the money gathered from cybercrime – then selling into EU (!).

La storia

Traffico di organi da Lagos a Torino

Un boss intercettato mentre parla con i suoi complici

Insospettabili

Coinvolti manager di Asti e Torino

Il covo dei [illegible]

Coke for cards?

- **March/May 2010**, Turin (North-West of Italy)
- Turin has got the **biggest Romania’s community** of Italy.
- We also have a **very big Nigeria’s community**.

- Historically, **Romenian gangs drive the business of ATM skimmers**…
- …and **Nigerian the Cocaine business**.

- After a joined FBI/US Secret Service/Interpol/Italian Postal Police operation, the Romanians decided to “**sell**” **the business** to Nigerians.
- **Cloned cards** were **paid with Cocaine**.

- This happens because the Romenians also **run the prostitutes business**…
- …and, prostitute’s **customers want coke as well**.

- Compared to these guys, **Scarface was nearly a kid** ☹

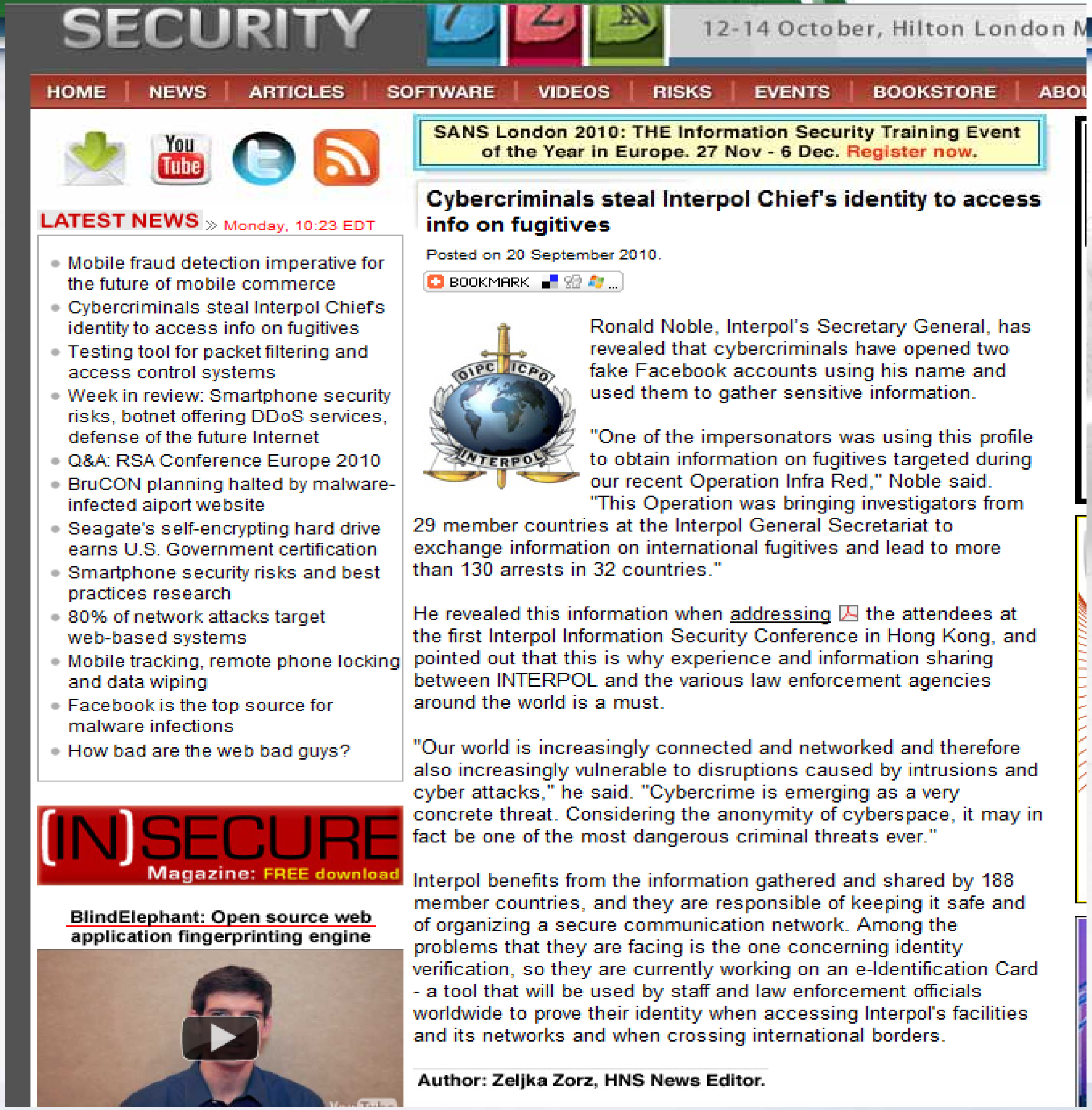
Cybercrime: the answers

- Cybercrime is typically a **transnational** crime, borderless, that includes so **many actors** and **different roles**.
- That's why you just can't think about a **single answer**.
- Instead, it is **necessary** to **think** and **act** in a **distributed approach**, creating **Virtual Task Forces (VTFs)**.
- It is **essential the collaboration among** Law Enforcement, Internet community, Finance sector, ISPs and carriers (voice & data), vertical groups, in order to identify a specific group, malware or facilitator.
- From the **investigative point of view**, challenges are the following:
  - ✓ Analyze the malware
  - ✓ Map the infrastructure
  - ✓ Eavesdrop/Intercept/Sniff the communication and/or the links
  - ✓ Explore the executed attacks
  - ✓ Identify the developers and its crime-rings.

Vertical Groups & VTFs

- That’s why, along these years, Vertical Groups have been raised, among which we can list the following:
  - ✓ Team Cymru
  - ✓ APWG –Anti Phishing Working Group
  - ✓ IEEE-SA
  - ✓ Shadow Server Foundation
  - ✓ UNICRI – Emerging Crimes Unit
  - ✓ Host Exploit
  - ✓ Cyberdefcon
  - ✓ ………..
- …working along with :
  - ✓ INTERPOL
  - ✓ EUROPOL
  - ✓ “Hi-Tech Crimes” groups into each National LEAs

While..you better watch out!



LATEST NEWS » Monday, 10:23 EDT

- Mobile fraud detection imperative for the future of mobile commerce
- Cybercriminals steal Interpol Chief's identity to access info on fugitives
- Testing tool for packet filtering and access control systems
- Week in review: Smartphone security risks, botnet offering DDoS services, defense of the future Internet
- Q&A: RSA Conference Europe 2010
- BruCON planning halted by malware-infected aiport website
- Seagate's self-encrypting hard drive earns U.S. Government certification
- Smartphone security risks and best practices research
- 80% of network attacks target web-based systems
- Mobile tracking, remote phone locking and data wiping
- Facebook is the top source for malware infections
- How bad are the web bad guys?

BlindElephant: Open source web application fingerprinting engine

Cybercriminals steal Interpol Chief's identity to access info on fugitives

Posted on 20 September 2010.

BOOKMARK

Ronald Noble, Interpol's Secretary General, has revealed that cybercriminals have opened two fake Facebook accounts using his name and used them to gather sensitive information.

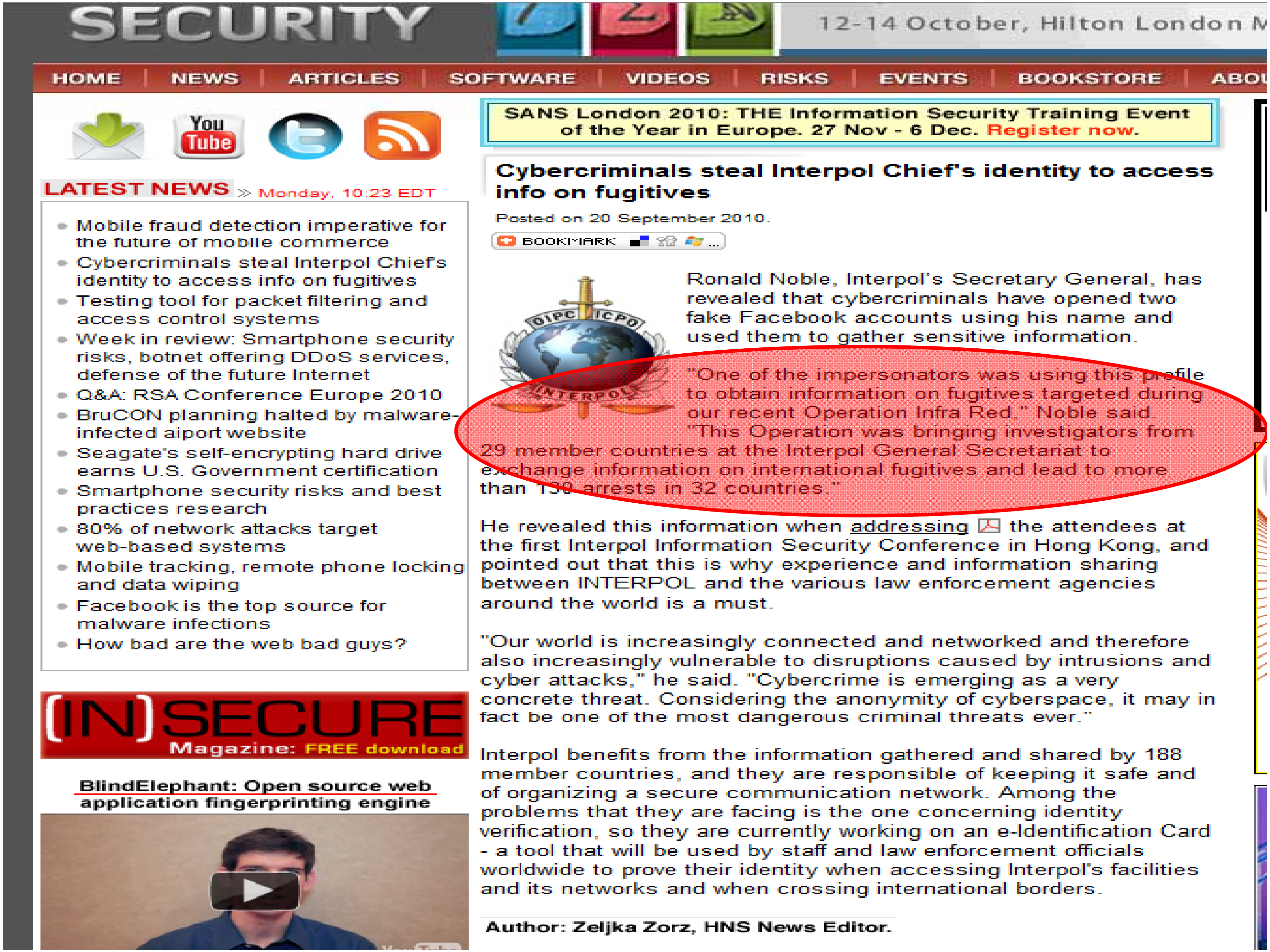
"One of the impersonators was using this profile to obtain information on fugitives targeted during our recent Operation Infra Red," Noble said. "This Operation was bringing investigators from 29 member countries at the Interpol General Secretariat to exchange information on international fugitives and lead to more than 130 arrests in 32 countries."

He revealed this information when addressing the attendees at the first Interpol Information Security Conference in Hong Kong, and pointed out that this is why experience and information sharing between INTERPOL and the various law enforcement agencies around the world is a must.

"Our world is increasingly connected and networked and therefore also increasingly vulnerable to disruptions caused by intrusions and cyber attacks," he said. "Cybercrime is emerging as a very concrete threat. Considering the anonymity of cyberspace, it may in fact be one of the most dangerous criminal threats ever."

Interpol benefits from the information gathered and shared by 188 member countries, and they are responsible of keeping it safe and of organizing a secure communication network. Among the problems that they are facing is the one concerning identity verification, so they are currently working on an e-Identification Card - a tool that will be used by staff and law enforcement officials worldwide to prove their identity when accessing Interpol's facilities and its networks and when crossing international borders.

Author: Zeljka Zorz, HNS News Editor.



LATEST NEWS » Monday, 10:23 EDT

- Mobile fraud detection imperative for the future of mobile commerce
- Cybercriminals steal Interpol Chief's identity to access info on fugitives
- Testing tool for packet filtering and access control systems
- Week in review: Smartphone security risks, botnet offering DDoS services, defense of the future Internet
- Q&A: RSA Conference Europe 2010
- BruCON planning halted by malware-infected aiport website
- Seagate's self-encrypting hard drive earns U.S. Government certification
- Smartphone security risks and best practices research
- 80% of network attacks target web-based systems
- Mobile tracking, remote phone locking and data wiping
- Facebook is the top source for malware infections
- How bad are the web bad guys?

Cybercriminals steal Interpol Chief's identity to access info on fugitives

Posted on 20 September 2010.

BOOKMARK

Ronald Noble, Interpol's Secretary General, has revealed that cybercriminals have opened two fake Facebook accounts using his name and used them to gather sensitive information.

"One of the impersonators was using this profile to obtain information on fugitives targeted during our recent Operation Infra Red," Noble said. "This Operation was bringing investigators from 29 member countries at the Interpol General Secretariat to exchange information on international fugitives and lead to more than 130 arrests in 32 countries."

He revealed this information when addressing the attendees at the first Interpol Information Security Conference in Hong Kong, and pointed out that this is why experience and information sharing between INTERPOL and the various law enforcement agencies around the world is a must.

"Our world is increasingly connected and networked and therefore also increasingly vulnerable to disruptions caused by intrusions and cyber attacks," he said. "Cybercrime is emerging as a very concrete threat. Considering the anonymity of cyberspace, it may in fact be one of the most dangerous criminal threats ever."

Interpol benefits from the information gathered and shared by 188 member countries, and they are responsible of keeping it safe and of organizing a secure communication network. Among the problems that they are facing is the one concerning identity verification, so they are currently working on an e-Identification Card - a tool that will be used by staff and law enforcement officials worldwide to prove their identity when accessing Interpol's facilities and its networks and when crossing international borders.

Author: Zeljka Zorz, HNS News Editor.

Must-read books / 1

During the different phases of bibliography research, the Authors have made reference (also) to the following publications and on-line resources:

- **H.P.P. Questionnaires 2005-2011**
- **Kingpin: How One Hacker Took over The Billion Dollar Cyber Crime Underground**, Kevin Poulsen, Crown Publishers, 2011
- **Fatal System Error: the Hunt for the new Crime Lords who are bringing down the Internet**, Joseph Menn, Public Affairs, 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

Must-read books / 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

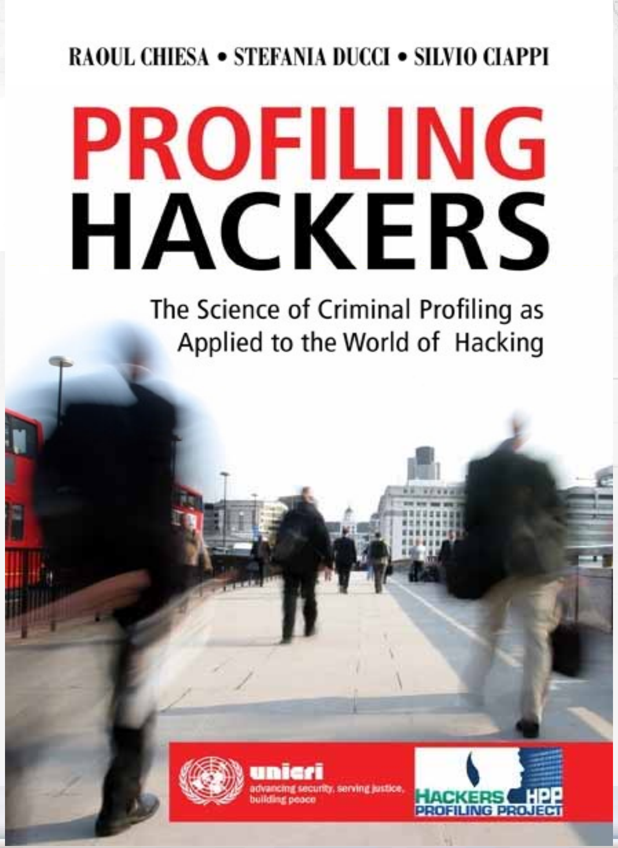
Malicious Hackers: a framework for Analysis and Case Study, Laura J. Kleen, Captain, USAF, US Air Force Institute of Technology

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

Must-read books / 3

- **Profiling Hackers: the Science of Criminal Profiling as applied to the World of Hacking**
- **ISBN: 978-1-4200-8693-5-90000**

unicri
advancing security, serving justice,
building peace



RAOUL CHIESA • STEFANIA DUCCI • SILVIO CIAPPI

PROFILING HACKERS

The Science of Criminal Profiling as Applied to the World of Hacking

unicri advancing security, serving justice, building peace

HACKERS PROFILING PROJECT HPP

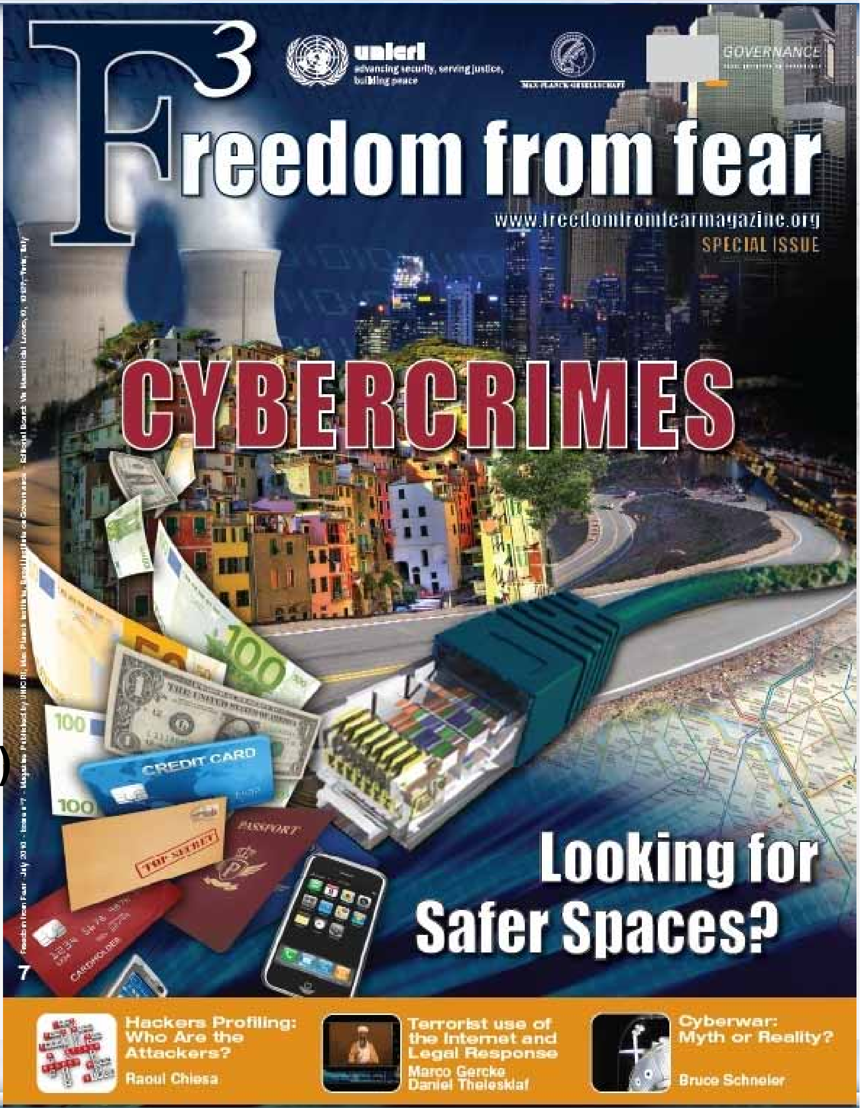
And...a gift for you all here! ☺

Get your own, FREE copy of “F3” (Freedom from Fear, the United Nations magazine) issue #7, totally focused on Cybercrimes!

DOWNLOAD:

www.FreedomFromFearMagazine.org

Or, email me and I will send you the full PDF (10MB)


F3
unicri
advancing security, serving justice, building peace
MAX PLANCK GESELLSCHAFT
GOVERNANCE
Freedom from fear
www.freedomfromfearmagazine.org
SPECIAL ISSUE
CYBERCRIMES
CREDIT CARD
PASSPORT
TOP SECRET
7
Looking for Safer Spaces?
Hackers Profiling: Who Are the Attackers?
Raoul Chiesa
Terrorist use of the Internet and Legal Response
Marco Gercke
Daniel Thelesklaf
Cyberwar: Myth or Reality?
Bruce Schneier

Contacts, Q&A

Raoul Chiesa

E-mail: chiesa@UNICRI.it

Thanks folks!

UNICRI Cybercrime Home Page:

http://www.unicri.it

http://www.unicri.it/emerging_crimes/cybercrime/