

Underground Economy: why we should be fully-updated on this topic: InfoSec players, Finance world, citiziens.

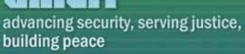
A NFP Talk by Raoul Chiesa Senior Advisor, Strategic Alliances & Cybercrime Issues

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









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 actual laws.

security, serving justice

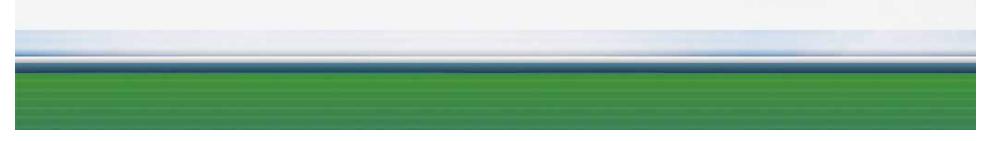
- Registered brands belong to their legitimate owners.
- The opinion here represented are my personal ones and do not necessary reflect the United Nations nor UNICRI views.
- NO: I will not rob ATMs upon request! ;)

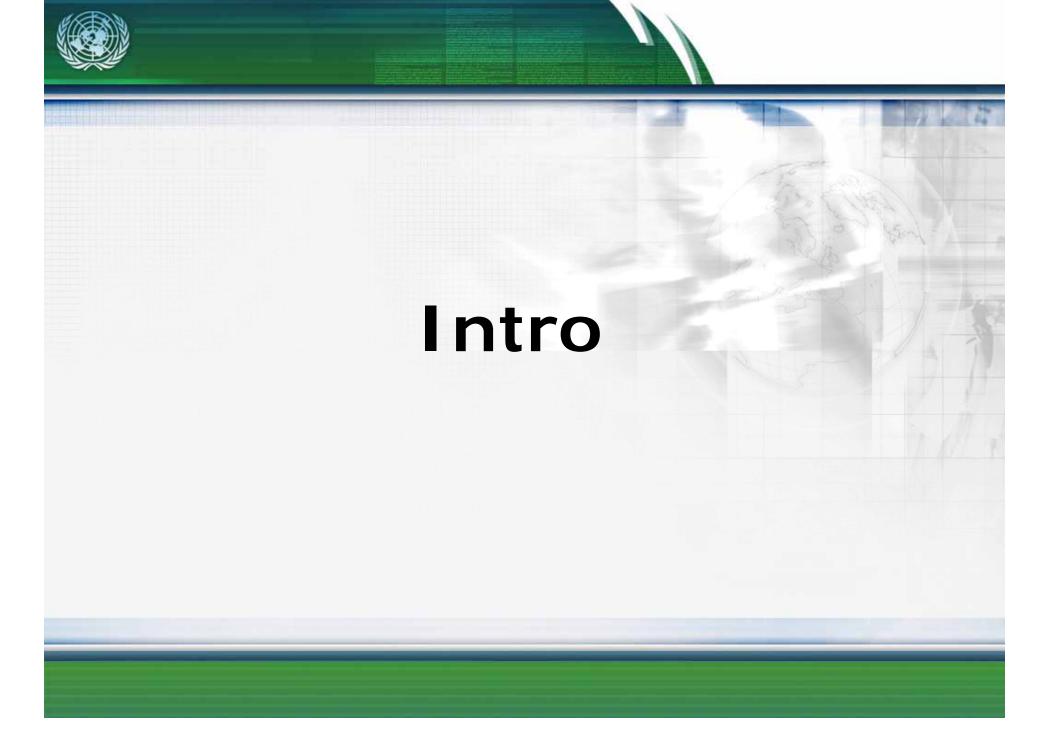
Agenda

mer

dvancing security, serving justice,

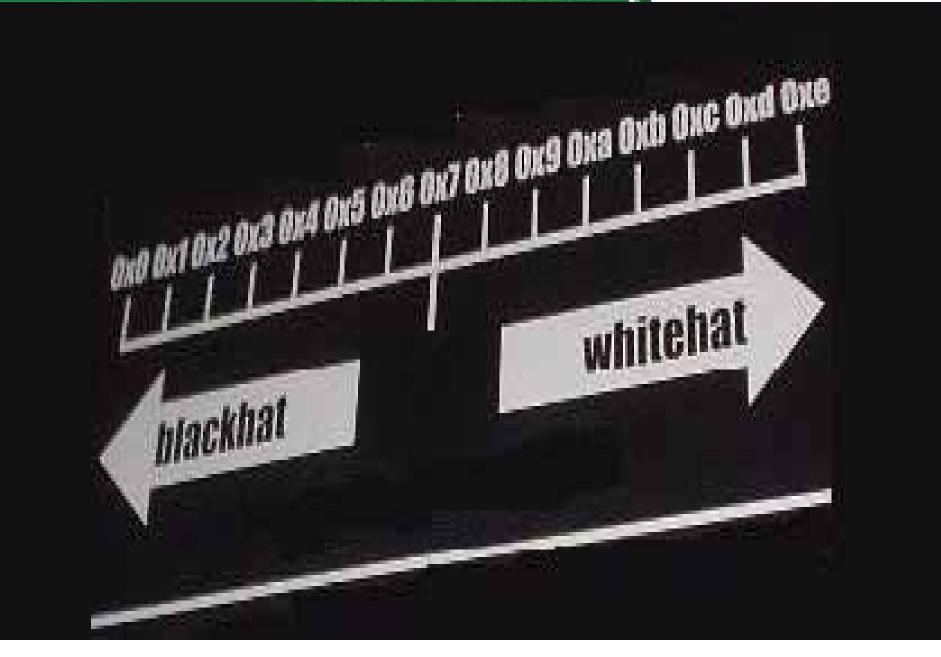
- ✓ # whois raoul
- ✓ #whois UNICRI
- ✓ Yesterday's hacking VS today's crime
- ✓ Hacking eras and Hacker's generations
- ✓ Cybercrime
- ✓ Profiling the enemy
- ✓ Hackers...
- ✓ Hacking, today: Underground Economy (highly sanitized)
- ✓ <u>CENSORED</u>
- ✓ Conclusions







Who am I?





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
- Founder of CLUSIT, Italian Computer Security Association (CLUSI* : Belgium, France, Luxembourg, Switzerland)
- Member of TSTF.net Telecom Security Task Force
- 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, Hacker's Profiling, Cybercrime, Information Warfare, Security methodologies, specialized Trainings.



ig security, serving justice.



mediaserv

ISECON

Associazione Italiana
ver la Sicurezza Informatica

eb Application Security Project

 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 ⁽²⁾





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

Counter Human Trafficking and Emerging Crimes Unit: cyber crimes, counterfeiting, environmental crimes, trafficking \in stolen works of art...

Water syste

Fake Bvlgari &Rolex Viagra &Cialis (aka

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



UNICRI & Cybercrime



Overview on UNICRI projects against cybercrime

Hackers Profiling Project (HPP)

SCADA & CNI's security

Digital Forensics and digital investigation techniques

Cybersecurity Trainings at the UN Campus



advancing security, serving justice, building peace



FIRST COMPREHENSIVE TRAINING PROGRAMME on

CYBER CRIMES

evaluating new threats, assessing your REAL security

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

From February 2010 🤕 UN Campus in Turin, Italy

www.unicri.it/wwd/cybertraining

Yesterday and today's Hacking





advancing security, serving justice, building peace

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).





advancing security, serving justice, building peace

Crime->Today:Cybercrime

Cars have been substituted by information (I'm not drunk. Yet ;)

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
- ✓ Sensible/critical information
- ✓ Money
- ... that's why all of us we want to "be secure".
- It's not by chance that it's named "IS": Information Security ③

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).





• 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 attendes and speakers here at CONfidence 2.0, I would answer that we already are on the right track in order to analyze the problem ^(C)
- Nevertheless, some factors exist for which the spreading of "e-crime"-based attacks relays.
- Let's take a look at them.

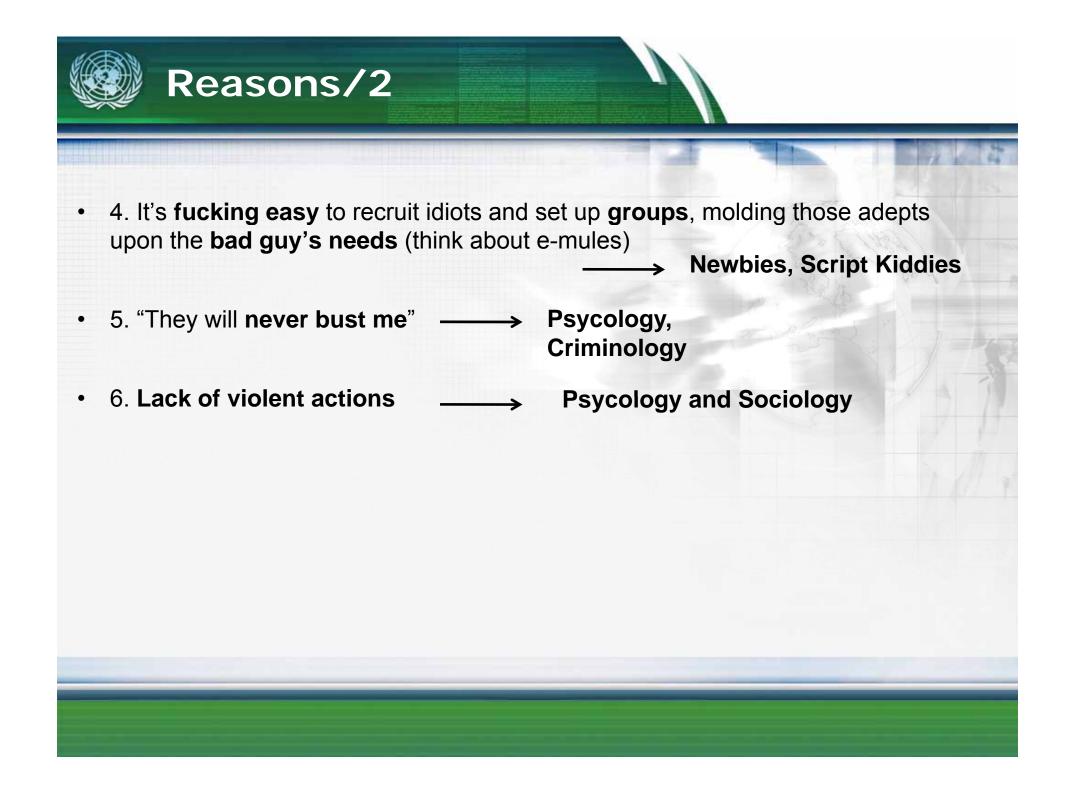
Reasons/1

- 1. There are **new users, more and more every day**: this means the total amount of **potential victims** and/or attack vectors is increasing.
- 2. **Making money**, "somehow and straight away".
- 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"

→ Thanks to broadband...

→ Economical crisis...

→ 0-days, Internet distribution system



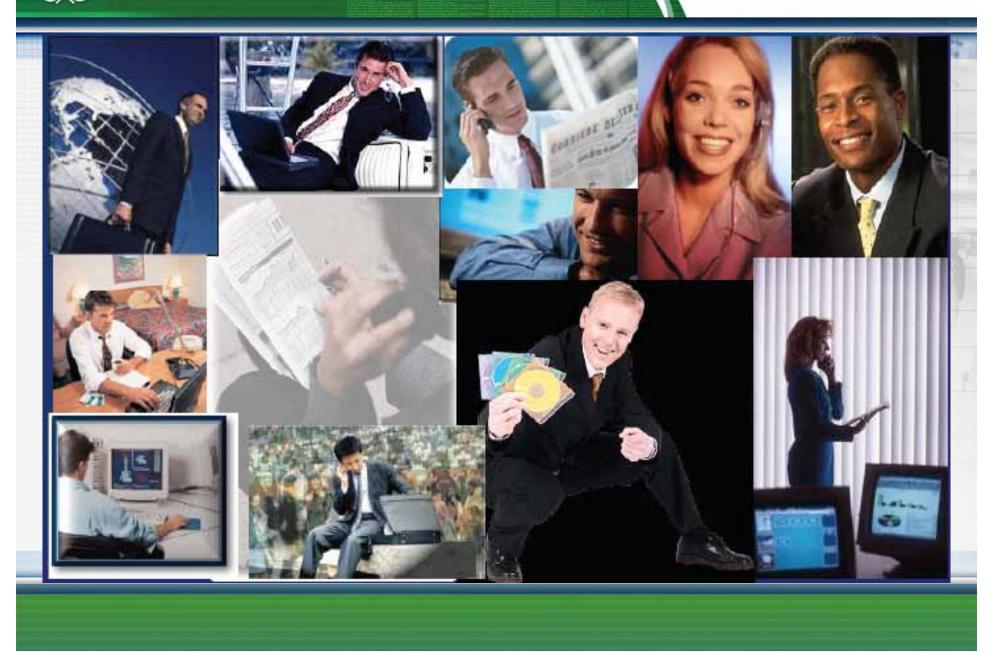
What the heck is changed then??

- 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 do a quick test!









There's a difference: why?

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



- Erroneus media information pushed your mind to run this approach
- Sometimes today the professionals are the real criminals, and hackers "the good guys"... (Telecom Italia Scandal, Vodafone Greece Affair, etc...)



- 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 sof hacker's subculture
- Explore hacker's **social organization**
- Let's zoom on those existing links between hacking and organized crime

Ok Raoul... so what ?!?



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

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

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

•





Russian Business Network

- Not that easy explaing what it is...
- First of all, cybercrime IRL means:

✓ Phishing

RBN

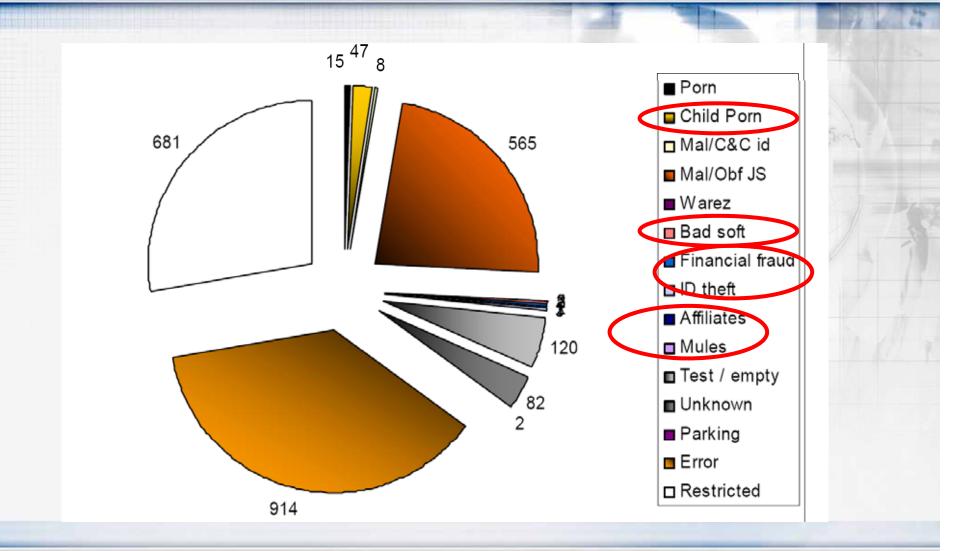
- ✓ Malware (rogue AVs, game sites, casinos, + standard stuff)
- ✓ Frauds & Scams
- ✓ DDoS Attacks
- ✓ Children pornography
- ✓ Generic Porn
- ✓ On-line games (Tomasz may comment out here ;)

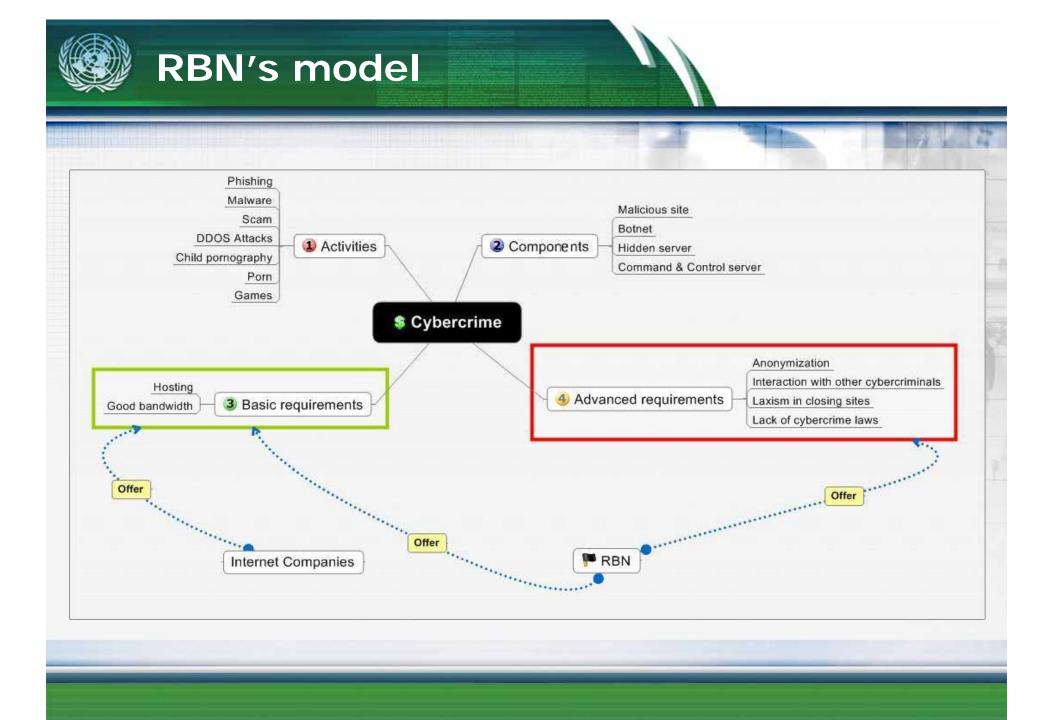
RBN & phishing

David Bizeul wrote an excellent study on RBN. One page was so interesting: http://194.146.207.18/config

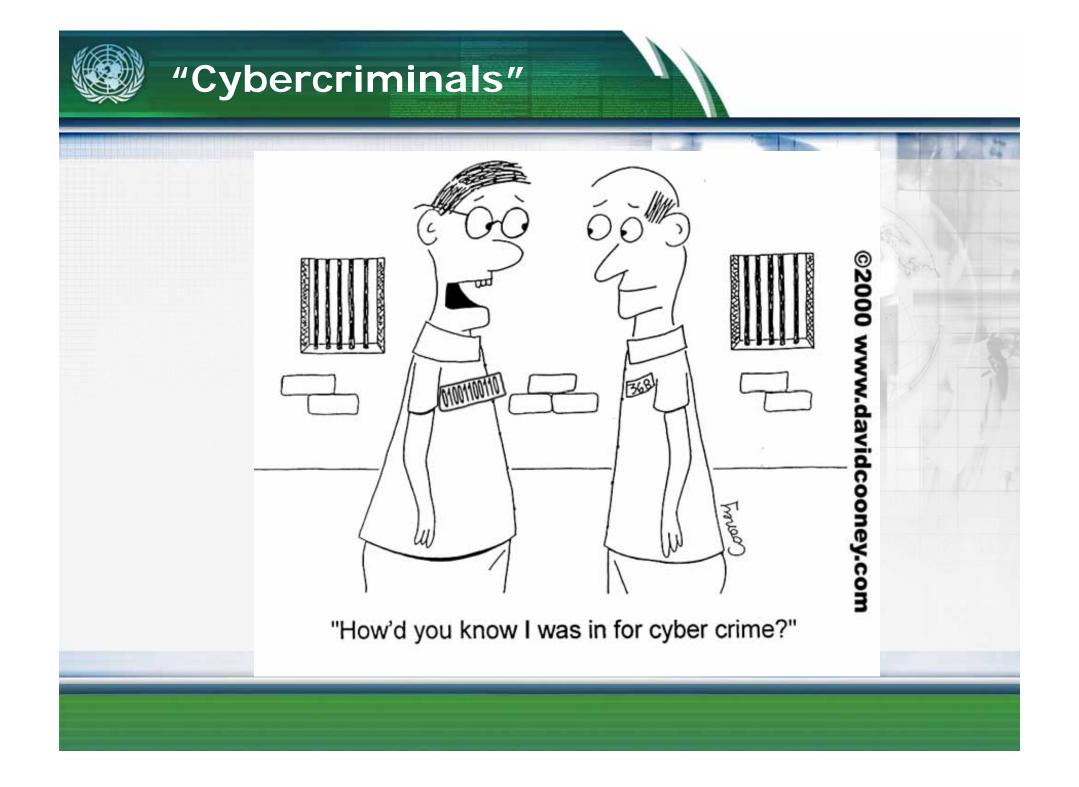
storage send interval="600" config file ="\$ 2341234.TMP" storage file ="\$ 2341233.TMP" www domains list = "pageshowlink.com" redirector url ="citibusinessonline.da-us.citibank.com" /cbusol/uSignOn.do {www} /usa/citibusiness.php 2 0 3" redirector_url = "*fineco.it /fineco/PortaleLogin {www} /it/fineco.php 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/dresdnerprivat/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?





Underground Economy





UE

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



- 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



Who's beyond ?

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

Please, stop video recording, no pictures-

Thanks.

This material is not available: you should have attended CONfidence 2.0 to see this !

What's next ?



advancing security, serving justice, building peace

ATM frauds generations

- "Generation 0": gun & thief, or "kick & run".
- 1st generation is basically the skimming, and/or cloning cards hacked from the Internet, shops & retailers, etc (but EMV and PCI-DSS are there now)
- The on-going fraud on Diebold ATMs (trojanized the OS of the ATM) IMHO is just a 2nd generation fraud
- Some months ago a smart bank hired us. They didn't ask for a "standard" pentest. They gave us a full ATM LAB to play with, for a whole month (God exists!)
- That's how we got to 3rd generation ATM fraud...
- We contributed to ENISA's ATM Crime paper (5% of what we discovered).
- The "embarassing" attack....(see next slide)
- NOTE: All of our attacks are not public, nor "on sale": sorry!

ATM 3rd generation frauds

□ The embarassing attack



unicri

ding peace

advancing security, serving justice,

This is the end, my friends



Final toughts

- The hacking world has not always been linked to those true criminal actions
- Just like FX said yesterday about router's security, it seems that ATM vendors (where the money is) just don't care about the security of their products (a fucking MS Windows cage is really not enough!)
- Basically, they are still thinking that skimming is their sole and unique threat (wrong)
- What they are doing **right now** just as it's happening with Internet routers! -. is adding "gadgets" and fuctions, that basically enlarge the chance of mistakes, bugs, attack vectors, etc (coin dispenser, new "routings" towards telcos, charity, etc..)
- At the same time, nowaday's hacking is moving (transforming?) towards crime.
- 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.

Questions or happy hour time?



Contacts, Q&A

Raoul Chiesa

E-mail: chiesa@UNICRI.it

Thanks folks!



UNICRI Cybercrime Home Page: http://www.unicri.it/wwd/cyber_crime/index.php

http://www.unicri.it