United Nations
Interregional Crime and Justice
Research Institute

The New Cybercriminals
HPP: Hackers' Profiling Project

HACKERS HPP
PROFILING PROJECT

United Nations
Interregional Crime and Justice
Research Institute

Agenda

- Introduction
- HPP V1.0 (first phase)
- HPP V2.0 (second phase)
- Conclusion
- Contacts

United Nations
Interregional Crime and Justice
Research Institute

About UNICRI

UNICRI is a United Nations entity created in 1968 and mandated by the United Nations Economic and Social Council to assist intergovernmental, governmental and non-governmental organizations in the field of crime prevention and criminal justice.

UNICRI activities

UNICRI's Emerging Crimes Unit tackles organized crime involvement in both established and emerging forms of crime and implements programs for the protection of vulnerable people. Particularly, the Institute deals with:

- **Cybercrime**
- Counterfeiting
- Trafficking in persons
- Environmental crimes
- Corruption
- Victims' assistance

United Nations
Interregional Crime and Justice
Research Institute

UNICRI strategy on cyber threats

Specifically, the activities of the Emerging Crimes Unit regarding cybercrime concentrate on:

- Profiling of hackers and cybercriminals
- Evolution of the criminal business model: organized crime links
- Analysis of cybercriminals' modus operandi
- Comprehensive evaluation of case studies

Cyberspace = Growing Opportunities for Crime

"Organised crime is a multi–billion euro business in Europe and it is growing in scale. The further expansion of Internet and mobile technologies, the proliferation of illicit trafficking routes and methods as well as opportunities offered by the global economic crisis, have all contributed to the development of a more potent threat from organised crime".

(Rob Wainwright, Director of Europol)

United Nations
Interregional Crime and Justice
Research Institute

Cybercrime “crime ranking” & direct incoming analysis

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

PriceWaterhouse Coopers LLC, Global Economic Crime Survey 2011

“2011 Cybercrime financial turnover apparently scored up more than Drugs dealing, Human Trafficking and Weapons Trafficking turnovers”

Various sources (UN, USDOJ, INTERPOL, 2011)

Financial Turnover, estimation: 6-12 BLN USD$/year

Group IB Report 2011

United Nations
Interregional Crime and Justice
Research Institute

What is cybercrime? Many possible definitions – no widely accepted one

Any conduct proscribed by legislation and/or jurisprudence that:

(a) is directed at computing and communications technologies themselves;

(b) involves the use of digital technologies in the commission of the offence; or

(c) involves the incidental use of computers with respect to the commission of other crimes.

What is cybercrime? (from a technical point of view)

Cyber crime encompasses any criminal act dealing with computers and networks Additionally, cyber crime also includes traditional crimes conducted through the Internet.

Few examples:

- **Identity theft** (Personal Info)
- **Financial fraud** (Financial Info theft: online banking, CC/CVV, «fullz», etc)
- **Hacking** (E-commerce, e-banking, Credit Processing Centers)
- **Malware** (Virus, Worm, Spyware, Key Loggers, Rogue AV, Botnets, Mobile)
- **Hacking on request**
- **DDoS attacks** (Blackmail, Hacktivism)
- **Spam**
- **Counterfeiting** (medicines, luxury, products&services)
- **Gambling** (Money laundering, fake & not Gov-authorised websites (i.e. Italy -> AAMS)
- **Pornography** (fake websites, etc)
- **Child pornography**
- **Harassment** (Cyberstalking, Cyberbullying, Cybergrooming, ….)

United Nations
Interregional Crime and Justice
Research Institute

Why has cybercrime become so pervasive?

- Extremely **profitable**.
- Very low infrastructure cost and readily available attack tools.
- Barriers to prosecution combined with **weak laws** and sentencing.
- **Anonymity** and financial lure has made cyber-crime more attractive.
- Separation between the physical and virtual world.
- “Hacking prèt-à-porter”.
- **Organized cybercrime groups** can conduct operations without ever making physical contact with each other.

United Nations
Interregional Crime and Justice
Research Institute

Hackers' Profiling Project (HPP V1.0)

Hacking eras & generations

- **First generation** (1970's): driven by need for knowledge.
- **Second generation** (early 1980's): driven by curiosity and need for knowledge; later on (1985-1990) hacking becomes a trend.
- **Third generation** (1990's): driven by addiction, curiosity, establishing networks, information sharing.
- **Fourth generation** (2000-to present): driven by eagerness and money. Here hacking meets with politics (**cyber-hacktivism**) or with the criminal world (**cybercrime**).

Misha Glenny (Author of “McMafia” and “Dark Market”) while speaking about HPP at TED 2011

http://www.youtube.com/watch?v=6gSwRHScq6M&feature=player_detailpage#t=341s

United Nations
Interregional Crime and Justice
Research Institute

HPP Hacker's Profiling Project purposes

- **Apply** the profiling methodology to collected data
- **Analyse** the hacking phenomenon in its several aspects (technical, psychological, social, economical) through an interdisciplinary approach.
- **Identify** the different motivations of the actors involved.
- **Observe** the criminal activity in context
- **Acquire** and disseminate knowledge.

unicri
United Nations
Interregional Crime and Justice
Research Institute

Project phases - starting September 2004

1 – Theoretical collection:
Questionnaire, Existing literature

2 – Observation:
Participation in IT underground security events

3 - Filing:
Database for elaboration/classification of data (phase 1/phase 4)

4 - Live collection:
Highly customized, new generation Honeynet systems

5 – Gap analysis:
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

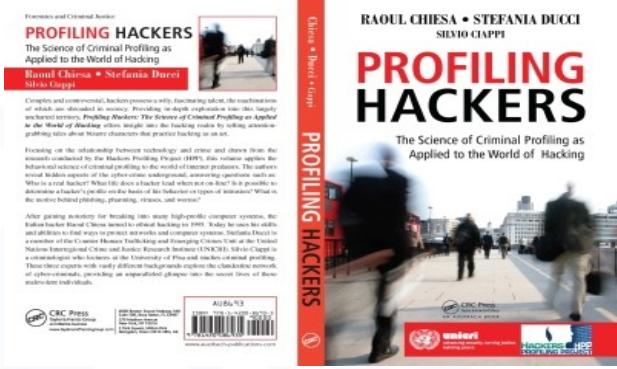
8 – Diffusion of the model:
elaboration of results, publication of the methodology, raising awareness

United Nations
Interregional Crime and Justice
Research Institute

Variables

- Modus Operandi
- Isolated VS Collective activities
- Motivations
- Selected targets
- Career
- Ethics
- Crashed or damaged systems
- Perception of illegality
- Effect of laws, convictions and technical difficulties as a deterrent

United Nations
Interregional Crime and Justice
Research Institute



HPP V1.0 (first phase)

In 2004 the Hacker's Profiling Project – HPP was launched.

Outcomes: over 1.200 questionnaires collected & analyzed in several countries (US, Italy, UK, Canada, Lithuania, Australia, Malaysia, Germany, Brazil):

- 9 Hacker's profiles emerged
- 2 books: 1) Profilo Hacker, Apogeo, 2007; 2) Profiling Hackers: the Science of Criminal Profiling as Applied to the World of Hacking, Taylor&Francis Group, CRC Press (2009).

Hackers or…cybercriminals?

Low level hackers "script-kiddies"

- Phishing, Remote low-level social engineering attacks
- Insiders
- Disgruntled Employees

High-level, sophisticated hackers, organized crime-medium/high level

- Hobbyist Hackers
- Unethical security guys (Telecom Italia and Vodafone Greece Scandals)
- Structured/Unstructured Attacks

Industrial Espionage-Terrorism

- Foreign Espionage
- Hacktivists
- Terrorist Groups
- State Sponsored Attacks

United Nations
Interregional Crime and Justice
Research Institute

The new Hackers Profiling Project (HPP V2.0)

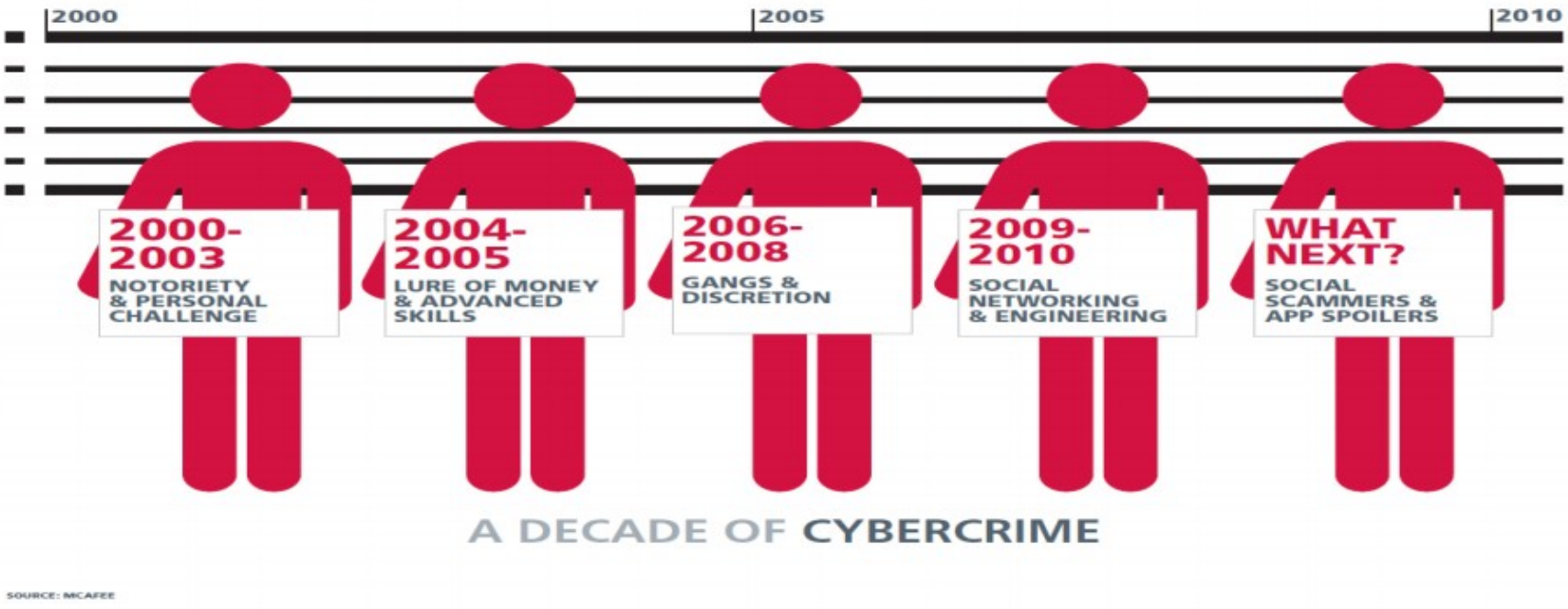
"I urge you to be more innovative when it comes to emerging threats such as cyber-crime, environmental crime and counterfeiting, we must stay one step ahead of the criminals. We must also be more effective in stopping the money flows enabled by corruption and money-laundering"

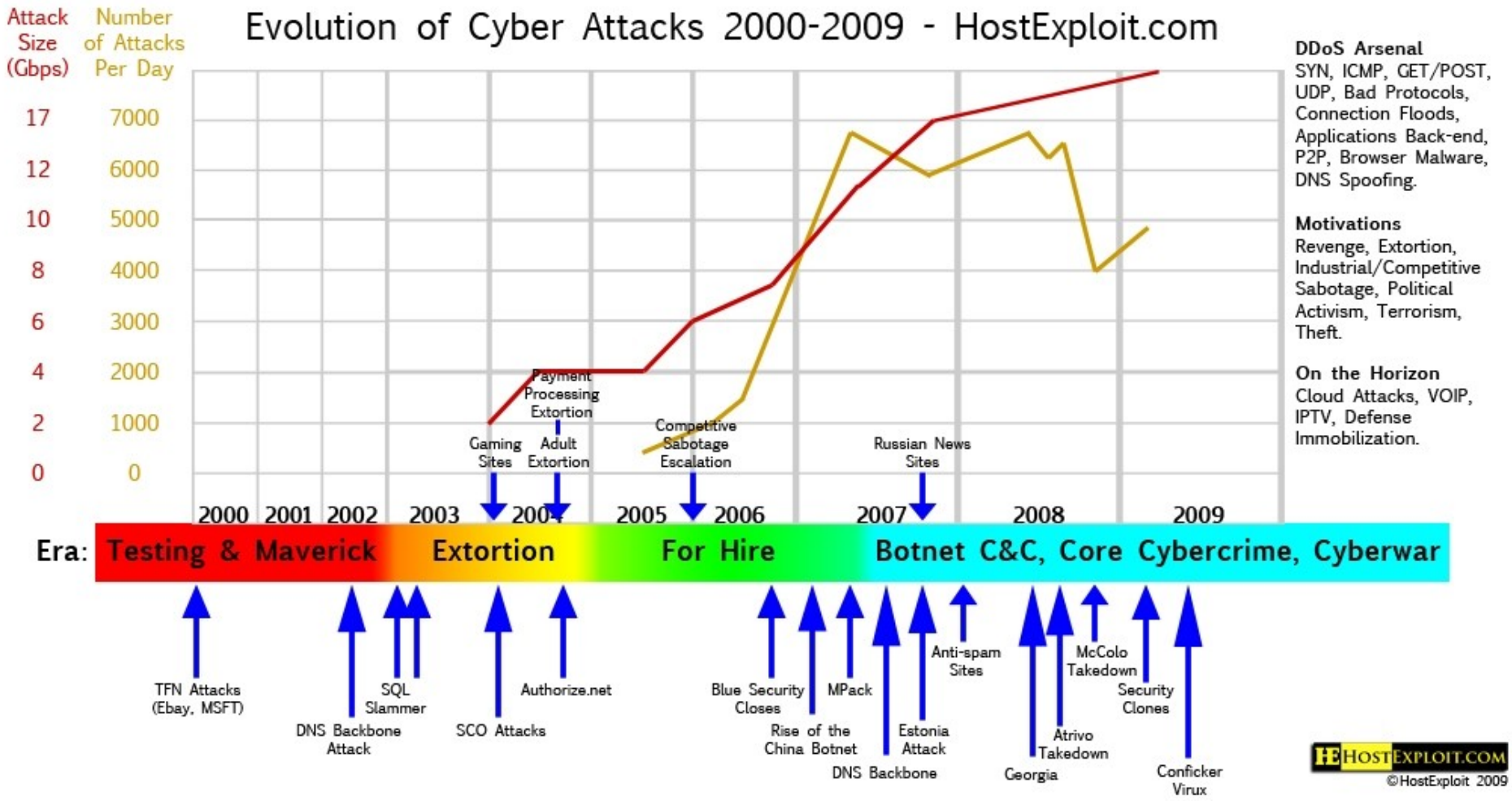
Ban Ki-moon, 2010

United Nations
Interregional Crime and Justice
Research Institute

The day money became the focus of malware is the day the Internet changed

Graham Ingram, AusCERT GM




Evolution of Cyber Attacks 2000-2009 - HostExploit.com
Attack Size (Gbps)
Number of Attacks Per Day
17
12
10
8
6
4
2
0
7000
6000
5000
4000
3000
2000
1000
0
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
Payment Processing Extortion
Gaming Sites
Adult Extortion
Competitive Sabotage Escalation
Russian News Sites
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.
Era:
Testing & Maverick
Extortion
For Hire
Botnet C&C, Core Cybercrime, Cyberwar
TFN Attacks (Ebay, MSFT)
DNS Backbone Attack
SQL Slammer
SCO Attacks
Authorize.net
Blue Security Closes
Rise of the China Botnet
MPack
DNS Backbone
Estonia Attack
Anti-spam Sites
Georgia
Atrivo Takedown
McColo Takedown
Security Clones
Conficker Virux
HOSTEXPLOIT.COM
©HostExploit 2009

United Nations
Interregional Crime and Justice
Research Institute

Who are the actors of the new scenarios?

- Are they politically or financially-motivated?
- Are they actively working with new and unconventional “digital tribes” rather than traditional organized crime groups?
- Are they actively or simply passively working with O.C. groups in order to support their activities?

United Nations
Interregional Crime and Justice
Research Institute

HPP V2.0: aims

- **Look into** new actors involved in cybercrime
- **Identify emerging trends**: hacktivism, organised crime, white collar crime (financial crime)

United Nations
Interregional Crime and Justice
Research Institute

HPP V2.0 Upcoming goals

- Understand new hackers' behaviors.
- Explore the evolving hackers' social, "business" and (possibly) criminal organization.
- Analyze malware in order to map the infrastructure.
- Build the model to test the hackers' behavior in a safe environment.
- Analyze the executed attacks.
- Identify the developers and their crime-rings.

HPP V2.0: phases & activities

- **1. Literature review & Evidence collection**
- **2. Honeypots & Honeynets (H&H)**
  a) design, setup and delivery
  b) defining the collection approach of data existing from H&H
  c) monitoring / acquiring data
  d) analysis
  e) correlation
  f) different outputs
    - Non-technical papers
    - Technical analysis papers
- **3. Gap analysis between data from Project phases 1 and 2**
- **4. HPP new emerged profiles assessment**
  a) specific papers on single profiles
  b) final profiling
  c) diffusion as GNU/FDL (Methodology, Profiles)
  d) new publication

United Nations
Interregional Crime and Justice
Research Institute

Conclusion

The results of HPP V2.0 will be showcased all around the world at public and private Security Events, including media visibility under the UN flag.

United Nations
Interregional Crime and Justice
Research Institute

Why it is important to invest on HPP

- Research carried out so far has **not properly portrayed** the hacking world and its patterns.
- Nowadays hacking is evolving towards **global crime**.
- Cybercrime is inherently **transnational**.
- Cybercrime and Underground Economy are **collective** issues: their societal impact could be devastating.
- **Collaboration** among Law Enforcement, Internet community, Finance sector, ISPs and carriers (voice & data) is crucial.

HPP's donorship added values

Opportunities:

- Obtain fresh and unique data on illegal cyber activities
- Notify and investigate trends
- Find the gaps (Laws, business models, money laundering)

Advantages:

- UNICRI's indipendence from the business market
- International visibility

Contacts

- Francesca Bosco: bosco@unicri.it
  Project Officer
- Raoul Chiesa: chiesa@unicri.it
  Consultant

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