H.P.P.
the Hackers Profiling Project: a general overview

hack.lu 2006

19°-21° October 2006

Project Leaders
Raoul Chiesa
raoul@ISECOM.org
Dr. Stefania Ducci
stefania@ISECOM.org

Document Keywords

HPP General Overview, HPP Introduction, Cybercrime, Hackers Profiling, Criminal Profiling, Honeypots, Honeynets, Computer Intrusions, IT & ICT Attack's Anatomy, IT & ICT frauds.

Disclaimer

- This presentation is copyrighted by Raoul Chiesa and Stefania Ducci (©) 2004-2006 and cannot be modified or partially reproduced without quoting the authors.
- The use of this document is under ISECOM's document licensing.
- The information contained within this presentation does not infringe on any intellectual property nor does it contain tools or recipe that could be in breach with known laws.
- Quoted trademarks belongs to registered owners.

Agenda

Who we are

Introduction to the H.P.P. Project

The questionnaire

The first outputs

Hackers Profiling Grid

Evaluation and correlation standards

Detail analysis and correlation of profiles

Conclusions

Bibliography and references

Contacts

Project Leaders

Raoul Chiesa

- ***Director of Communications*** at ISECOM
  - **Institute for Security and Open Methodologies** (Est. 2002)
  - Originally called the Ideahamster Organization (Est. 2001)
  - **Non Profit Organization** Registered in Spain and U.S.A.
  - **Open Source Community** Registered OSI
- **Project Manager for H.P.P., OSSTMM Key Contributor**
  - OPST, OPSA, ISECOM Authorized International Trainer
- ***Professor of IT Security*** at various Universities & Masters (Italy)
- ***Board of Directors Member*** at I**SECOM**, **CLUSIT**, **Telecom Security Task Force** (TSTF.net)

Project Leaders

Dr. Stefania Ducci

Stefania has a **University degree in Law** (University of Bologna - 2002), and a **Master degree in Criminology** (University of Turin - 2003).

She works for **UNICRI** (United Nations Interregional Crime And Justice Research Institute), a UN agency, dealing with crime and criminal justice.

In 2004 she began collaborating with Raoul Chiesa on **personal basis**. The studies carried out in team formed the core of H.P.P. Project.

For the Hacker's Profiling Project, Stefania has used an **independent research approach**, providing her support and cooperation during her spare time, fascinated by the huge research possibilities and professional evolution offered by the Project.

Her principal interest consists in reading hacking and "classic" criminal profiling books.

The ISECOM Mission

- Our Mission:
  - To provide global, practical, useable security knowledge and knowledge-tools to solve problems caused by insecurity, privacy violations, ethical violations, and poor safety measures.
- Our Audience:
  - Governments, Corporations, Organizations (OSSTMM, HPP)
  - Professionals and quasi-professionals (Rules of Engagement, Metrics)
  - College students (Academic Alliance Program)
  - Teens and pre-teens (Hacker Highschool)

The ISECOM Projects

- **OSSTMM** – The Open Source Security Testing Methodology Manual
- **RAVs** – The Security Metrics
- **BIT** – Business Integrity Testing Methodology Manual
- **OPRP** – Open Protocol Resource Project
- **SIPES** – Security Incident Policy Enforcement System
- **SPSMM** – The Secure Programming Standards Methodology Manual
- **STICK** – Software Testing Checklist
- **ISM 3.0** – Information Security Maturity Model
- **HHS** – Hacker High School
- **HPP** – Hacker’s Profiling Project **New!**

Scope

- **This presentation will intentionally focus on a general introduction to the Hacker's Profiling Project (HPP).**
- **Further public versions of the HPP are already available upon request and identification, since we are still covering the project's core-development phases.**
- **At this time, the following releases of the HPP presentation have been developed:**
  - ✓ Basic
  - ✓ Compact (this one)
  - ✓ Standard
  - ✓ Full
  - ✓ HPP Book # 1 (under development; expected JAN 2007)
- **The HPP Presentations and Questionnaires are available in the following languages:**
  - ✓ English
  - ✓ Italian
  - ✓ Greek (translation in progress)
  - ✓ Rumenian (translation in progress)
  - ✓ German (under development)
  - ✓ Russian (partnership in progress)
  - ✓ Spanish (under development)
  - ✓ French (partnership in progress)

Agenda

Who we are

Introduction to the H.P.P. Project

The questionnaire

The first outputs

Hackers Profiling Grid

Evaluation and correlation standards

Detail analysis and correlation of profiles

Conclusions

Bibliography and references

Contacts

The “cybercrime”

Dealing with “hacking-related” security problems from more than a decade, in the last years we observed with deep attention a series of phenomenon defined by us “worrying”:

✓ A dramatic decrease of the so called “window of exposure”, which is the time between the elaboration of “0-day” exploits and their use in massive attacks and/or distributed at worldwide level;

✓ Dangerous synergies among technologically advanced personalities, classic criminality (national and transnational) and terrorism;

✓ Continuous increase of the dependence between national stability (critical national infrastructures, homeland security, telecommunications, fundamental services, etc.) and the ICT Security issues.

Nevertheless, often the cybercrime and hi-tech crime phenomena are analysed in a wrong manner.

The H.P.P. Project

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

In this connection, we want to analyse the "cybercrime problem" by using an approach completely different from the ones used till now, going directly to the source.

In fact, the H.P.P. Project is aimed at:

- Analysing the hacking phenomenon – technological, social and economic – in its several aspects, through both technical and criminological approaches.
- Understanding the different motivations and identifying the actors involved;
- Observing "in the field" the (true) criminal actions;
- Applying the profiling methodology to the collected data;
- Learning by the acquired knowledge and disseminating it.

The H.P.P. Phases

The H.P.P. Project started in September 2004 and became an official ISECOM project on June 2006. Till now, we have identified 8 different project phases.

Phase 1 **THEORICAL COLLECTION**
Elaboration and Distribution of the questionnaire, in different forms and towards different targets

Phase 2 **OBSERVATION**
Participation to “IT underground security” events (EU, Asia, USA, Australia) identyfing correct research partners

Phase 3 **FILING**
Creation of a Data-base for the classification elaboration of data collected during Phase 1

Phase 4 **“Live” COLLECTION**
Elaboration and activation of Honey-Net Systems of new generation and highly customized

Phase 5 **G&C ANALYSIS**
Gap-Analysis and Correlation among datas collected through the questionnaire, Honeynets and profiles deducted from the existing literature on the topic

Phase 5/A **HCP “live” ASSESSMENT (24X7)**
Continuous assessment of profiles and correlation of modus operandi, through data collected in Phase 4

Phase 6 **FINAL REPORTING**
Redefinition and fine-tuning of different hacker and profiles previously used as a “standard de-facto”

Phase 7 **DIFFUSION OF THE MODEL**
Final elaboration of results, drafting and publication of the methodology, raising awareness (white papers, lectures, company awareness, training)

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 point of views
3 – Filing	ON-GOING (PLANNING)		Planning: 3 months Implementation & Fine Tuning: 18 months	The hardest phase
4 – “Live” collection	ON-GOING (EXISTING LAB)		Planning: 3 months Implementation: 18 months	The funniest phase ☺
5 – Gap & Correlation Analysis	NO		18 months	The Next Thing
5/A – “Live” Assessment	NO		16 months	The biggest part of the Project
6 – Final Profiling	NO		12 months	“Satisfaction”
7 – Diffusion of the model	NO		GNU/FDL ;)	Methodology’s public release

Agenda

Who we are

Introduction to the H.P.P. Project

The questionnaire

The first outputs

Hackers Profiling Grid

Evaluation and correlation standards

Detail analysis and correlation of profiles

Conclusions

Bibliography and references

Contacts

The HPP Questionnaire

- **Module "A"**

Personal data (gender, age, social status, family context, study/work)

- **Module "B"**

Relational data (relationship with: the Authorities, teachers/employers, friends/colleagues, other hackers)

- **Module "C"**

Technical and criminological data (target, hacking techniques and tools, motivations, ethics, perception of the illegality of their own activity, crimes committed, deterrence)

All the questions allow anonymous answers

HPP QUESTIONNAIRE - the delivery

✓ **3 questionnaire typologies:**

❑ **Level 1**: Full Release

25 pages, Modules A, B and C expected as “fully completed” (all fields are mandatory)

❑ **Level 2**: Compact Release

10 pages, Modules A, B and C to be partially completed (some fields are mandatory)

❑ **Level 3**: Basic Release

3 pages, Modules A and C to be partially completed, often uncorrected (few mandatory fields.)

✓ **3 delivery levels:**

❑ **Known and/or verified, “directly” or not (the QoQ is extremely high), IRL and on-line.**

❑ **Underground/hacking general contacts (the QoQ is medium), on-line.**

❑ **Focused IT Magazines, Other (the QoQ is low), hard-copy and on-line.**

The questionnaire: excerpts

a) Sex:

Male

Female

b) Age:

c) Title of study (please, indicate the last):

Primary school leaving-certificate

Secondary school leaving-certificate

Professional qualification

Degree

Beyond (master, PhD, specialisation, etc.)

d) Country and place of residence (if you don't wish to specify your city, please, indicate the geographical area of residence). Specify also if you live in a village and, in the latter case, if this is far or not from a big urban centre.

(a) There are other persons in your family who are (or were)interested in IT?

Yes

No

(b) Are there other persons in your family who practise (or have practised) hacking/phreaking?

a) Awareness of your hacking/phreaking activity:

1)

(a) Among your acquaintances, who is (or was) aware of your hacking/phreaking activity? (teachers, employer(s), schoolmates, colleagues, friends, other members of the underground world, partner, and so on).

d) Hacking, phreaking, carding:

1) Do (or Did you) practise:

- hacking Yes No

- phreaking Yes No

e) Kinds of data nets, technologies and operative systems targeted and tools used:

1) On what kind of data nets and technologies do (or did) you practise hacking/phreaking? For example: Internet, X.25, PSTN/ISDN, PBX, Wireless, "mobile" nets (GSM/GPRS/EDGE/UMTS), VoIP.

The questionnaire: answer’s examples

Q: Do you obey to the hacker’s ethics? If not, why?

A: I obey to my ethics and to my rules, not in ethics in general. The reason for that is that I don’t like to obey in what other people is obeying, ethics are like rules and laws, other people are writing them for you and even if some times they sound fair and correct, always behind the sweet and hypnotic words there is a trap for personal freedom. I am not a sheep to follow rules ethical or legal in general.

Q: How do you perceive your hacking/phreaking activity: legal or illegal?

A: I don’t accept the terms legal and illegal, for accepting this terms means that I have the same point of view with people who have nothing common with me.

Ok, I’ll try to be more specific for helping you in this question. For me my activities are legal, for the others are illegal.

Agenda

Who we are

Introduction to the H.P.P. Project

The questionnaire

The first outputs

Hackers Profiling Grid

Evaluation and correlation standards

Detail analysis and correlation of profiles

Conclusions

Bibliography and references

Contacts

Hackers: an image still blurred

- ❑ **Yesterday:** hacking as an emerging phenomenon, unknown to people and ignored by researchers.
- ❑ **Today:** several researches and analysis about hacking and hackers but carried out in "mono": from a psychological, sociological, or criminological perspective, particularly after the so called Hacker Crackdown → according to them, there is only one type of hackers, seen as ugly (thin, myope), bad (malicious, destructive and/or criminal purposes) and "dirty" (asocial, without ethics, anarchic).
- ❑ **Tomorrow:** inter-disciplinary studies that put together criminology with information security → different typologies of hackers if we consider: action modalities (alone or in a group), technical skills, motivations, purposes, targets, obedience or not to the so called "Hacker Ethics".

A new perspective: first data from the "HPP 2004/06" questionnaires (1)

- Hackers are generally intellectually brilliant, creative, decided and resolute
- They are angry and rebel towards Authorities and narrow-minded people, seen as a menace for civil liberties
- Hacking as: 1) a technique, a way of life with curiosity and a way to challenge themselves; 2) a tool of power useful to raise people's awareness on political and social problems
- Usually they are motivated by the love for knowledge; but there are also hackers that have lucrative purposes and, therefore, practice phishing/pharming, carding and industrial espionage
- Preferred targets: military/governmental systems; corporations; telcos; schools and Universities, but also end-users and SMEs
- The biggest part of hackers (with a low level of technical skills) are deterred by technical difficulties: they prefer "easy" O.S.s such as Linux or Windows – elite hackers instead are stimulated only by systems considered "inviolable" (*BSD, Solaris, HP/UX, *VMS, IOS, Symbian) and by protocols...

A new perspective: first data from the “HPP 2004/06” questionnaires (2)

- They lay the blame of their attacks on SysAdmins (or on designers), because they were not able to protect the systems properly (or to design/define in a *safe* way a protocol or a standard)
- Ethical hackers usually advise SysAdmins of the discovered system's vulnerabilities (or contribute to fix the security flaw), but generally only after communicating them to the other members of the underground world
- Ethical hackers want to increase systems' security and raise SysAdmins' awareness and attention on these issues
- Ethical hackers take possession of the violated systems and defend them from other attacks, making them secure
- Ethical hackers don't crash systems (if it happens is due only to their inexperience) and they don't steal/delete/change data

Agenda

Who we are

Introduction to the H.P.P. Project

The questionnaire

The first outputs

Hackers profiling Grid

Evaluation and correlation standards

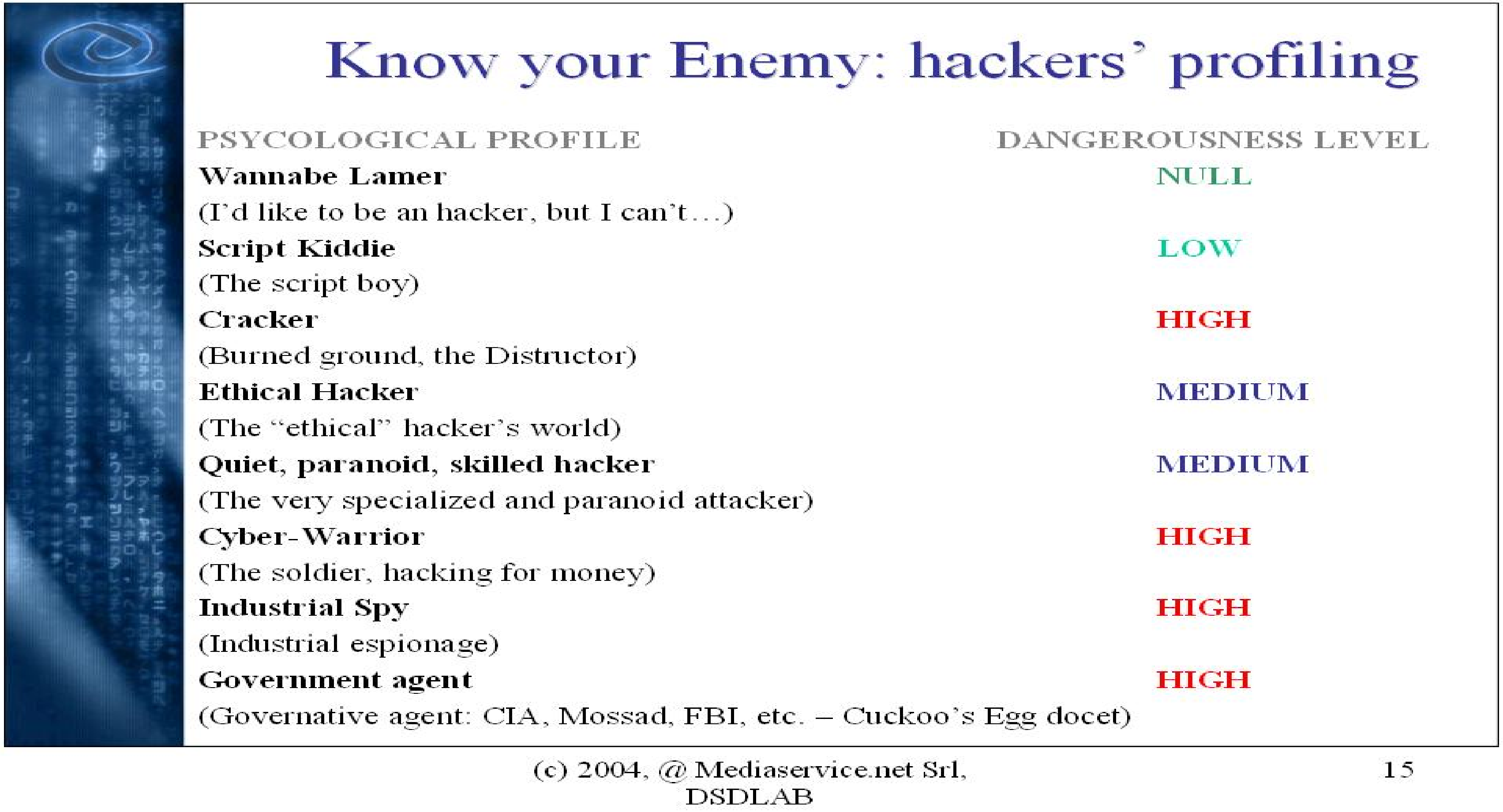
Detail analysis and correlation of profiles

Conclusions

Bibliography and references

Contacts

HPP Grid: the starting point



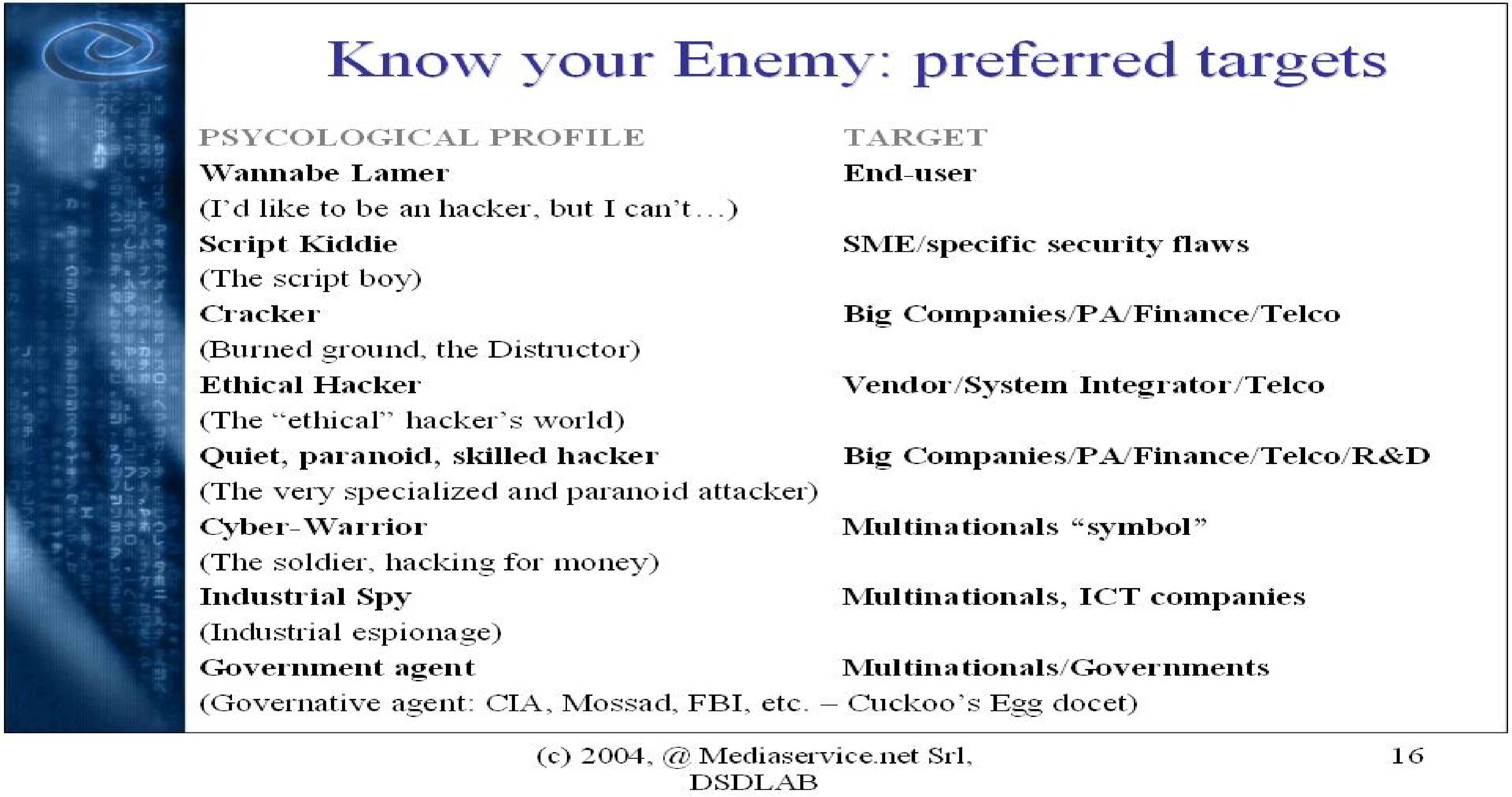
Know your Enemy: hackers' profiling

PSYCOLOGICAL PROFILE	DANGEROUSNESS LEVEL
Wannabe Lamer (I'd like to be an hacker, but I can't…)	NULL
Script Kiddie (The script boy)	LOW
Cracker (Burned ground, the Distructor)	HIGH
Ethical Hacker (The "ethical" hacker's world)	MEDIUM
Quiet, paranoid, skilled hacker (The very specialized and paranoid attacker)	MEDIUM
Cyber-Warrior (The soldier, hacking for money)	HIGH
Industrial Spy (Industrial espionage)	HIGH
Government agent (Governative agent: CIA, Mossad, FBI, etc. – Cuckoo's Egg docet)	HIGH

(c) 2004, @ Mediaservice.net Srl,
DSDLAB

15

HPP Grid: yesterday

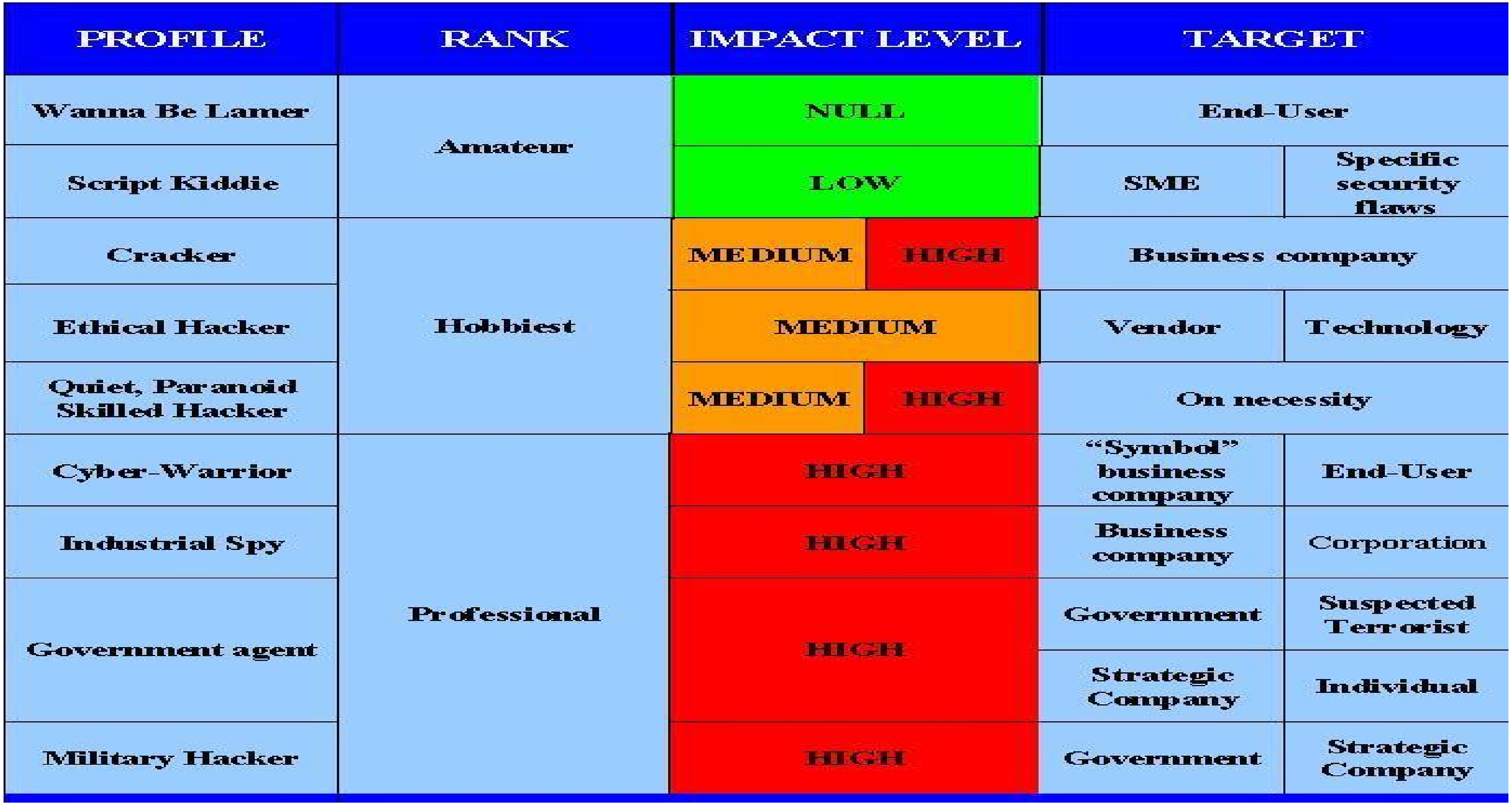


Know your Enemy: preferred targets

PSYCOLOGICAL PROFILE	TARGET
Wannabe Lamer (I'd like to be an hacker, but I can't…)	**End-user**
Script Kiddie (The script boy)	**SME/specific security flaws**
Cracker (Burned ground, the Distructor)	**Big Companies/PA/Finance/Telco**
Ethical Hacker (The "ethical" hacker's world)	**Vendor/System Integrator/Telco**
Quiet, paranoid, skilled hacker (The very specialized and paranoid attacker)	**Big Companies/PA/Finance/Telco/R&D**
Cyber-Warrior (The soldier, hacking for money)	**Multinationals "symbol"**
Industrial Spy (Industrial espionage)	**Multinationals, ICT companies**
Government agent (Governative agent: CIA, Mossad, FBI, etc. – Cuckoo's Egg docet)	**Multinationals/Governments**

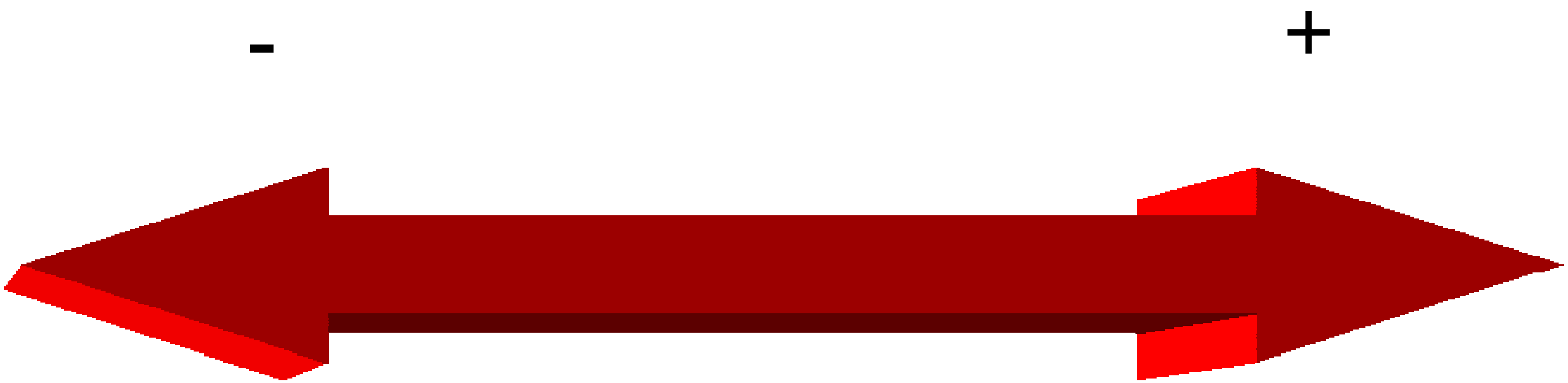
(c) 2004, @ Mediaservice.net Srl, DSDLAB 16

HPP Grid: today



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

Level of technical skills



Wannabe Lamer

Script Kiddie

Cracker

Ethical hacker

Q.P.S. Hacker

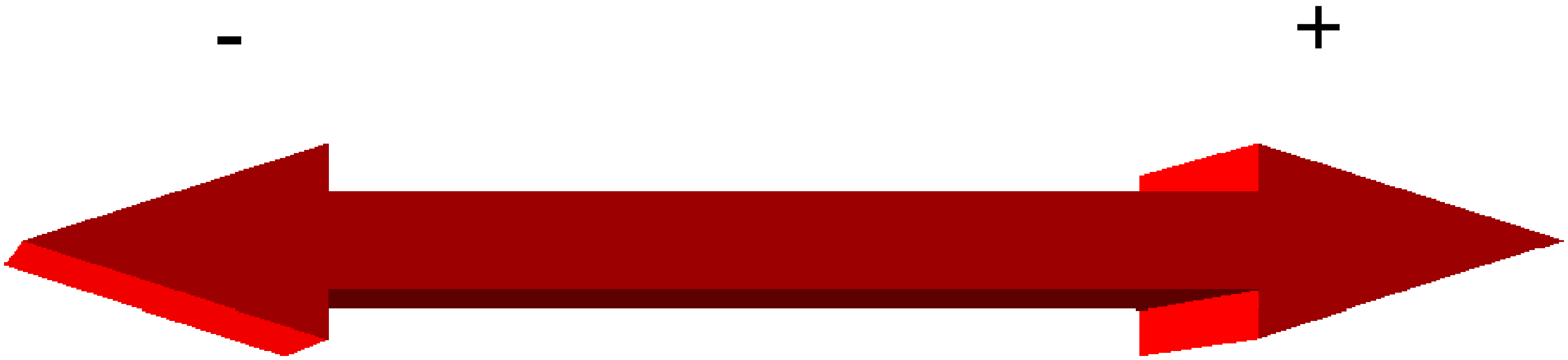
Cyber-Warrior

Industrial spy

Government Agent

Military Hacker

Level of dangerousness



Wannabe Lamer

Script Kiddie

Ethical Hacker

Q.P.S. Hacker

Cracker

Cyber-Warrior

Industrial spy

Government Agent

Military Hackers

Agenda

Who we are

Introduction to the H.P.P. Project

The questionnaire

The first outputs

Hackers profiling

Evaluation and correlation standards

Detail analysis and correlation of profiles

Conclusions

Bibliography and references

Contacts

Evaluation and Correlation standards

- This release of HPP presentation does not cover this chapter.
- The Evaluation and Correlation standards have been based, as for now, on the following fields:
  - ✓ Modus Operandi
  - ✓ Lone Hacker or as a Member of a Group
  - ✓ Motivations
  - ✓ Main Targets
  - ✓ Hacker career and selected targets
  - ✓ Relations between targets and motivations
  - ✓ Fundamentals principles of the so-called “Hacker Ethics”
  - ✓ Crashed or Damaged Systems
  - ✓ Perception pf the illegality of the own activity
  - ✓ Deterrence effect of Laws, Convictions and Technical Difficulties
- The Evaluation and Correlation standards are available to the public, upon request.

Agenda

Who we are

Introduction to the H.P.P. Project

The questionnaire

The first outputs

Hackers profiling

Evaluation and correlation standards

Detail analysis and correlation of profiles

Conclusions

Bibliography and references

Contacts

Detail Analysis and Correlation of the profiles

- This presentation will list a resume of all the analysed profiles and the correlations made.
- Since this is a compact version of the HPP presentation, here we will not fully detail the final profiling core.
- The “ID cards” and the detailed profiling and correlation elements at this time are freely available, upon identified request.

Detail Analysis and Correlation of the profiles: the "ID" card

ID cards are composed by the results gained from the following fields:

- ✓ *Hacker Typology*
- ✓ *Offender ID*
- ✓ *Lone or Group Hacker*
- ✓ *Target*
- ✓ *Motivations & Purposes*
- ✓ *Obedience to the "hacker ethics"*
- ✓ *Crashing or Damaging systems ?*
- ✓ *Perception of the illegality of their own activity*

and

- ✓ *Deterrence effect to:*
  - ✓ ***Laws***
  - ✓ ***Convictions suffered by other hackers***
  - ✓ ***Convictions suffered by them***
  - ✓ ***Technical difficulties approach***

The ID Card "puzzle"

Hacker top-level typologies view

1. Wannabe Lamer
2. Script kiddie: under development (Web Defacers, ….)
3. Cracker: under development (Web Defacers, malicious hackers, phishers, …)
4. Ethical hacker: under development (security researcher, hacker groups)
5. Quiet, paranoid, skilled hacker
6. Cyber-warrior: to be developed
7. Industrial spy: to be developed
8. Government agent
9. Military hacker

Detail Analysis and Correlation of the profiles: Table # 1

	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

Detail Analysis and Correlation of the profiles: Table # 2

	OBEDIENCE TO THE "HACKER ETHICS"	CRASHED / DAMAGED SYSTEMS	PERCEPTION OF THE ILLEGALITY OF THEIR OWN ACTIVITY
Wanna Be Lamer	NO: they don't know "Hacker Ethics" principles	YES: voluntarily or not (inexperience, lack of technical skills)	YES: but they think they will never be caught
Script Kiddie	NO: they create their own ethics	NO: but they delete / modify data	YES: but they justify their actions
Cracker	NO: for them the "Hacker Ethics" doesn't exist	YES: always voluntarily	YES but: MORAL DISCHARGE
Ethical Hacker	YES: they defend it	NEVER: it could happen only incidentally	YES: but they consider their activity morally acceptable
Quiet, Paranoid, Skilled Hacker	NO: they have their own personal ethics, often similar to the "Hacker Ethics"	NO	YES: they feel guilty for the upset caused to SysAdmins and victims
Cyber-Warrior	NO	YES: they also delete/modify/steal and sell data	YES: but they are without scruple
Industrial Spy	NO: but they follow some unwritten "professional" rules	NO: they only steal and sell data	YES: but they are without scruple
Government Agent	NO: they betray the "Hacker Ethics"	YES (including deleting/modifying/stealing data) / NO (in stealth attacks)	
Military Hacker	NO: they betray the "Hacker Ethics"	YES (including deleting/modifying/stealing data) / NO (in stealth attacks)	

Detail Analysis and Correlation of the profiles: Table # 3

DETERRENCE EFFECT OF:	LAWS	CONVICTIONS SUFFERED BY OTHER HACKERS	CONVICTIONS SUFFERED BY THEM	TECHNICAL DIFFICULTIES
Wanna Be Lamer	NULL	NULL	ALMOST NULL	HIGH
Script Kiddie	NULL	NULL	HIGH: they stop after the 1st conviction	HIGH
Cracker	NULL	NULL	NULL	MEDIUM
Ethical Hacker	NULL	NULL	HIGH: they stop after the 1st conviction	NULL
Quiet, Paranoid, Skilled Hacker	NULL	NULL	NULL	NULL
Cyber-Warrior	NULL	NULL	NULL	NULL: they do it as a job
Industrial Spy	NULL	NULL	NULL	NULL: they do it as a job

Agenda

Who we are

Introduction to the H.P.P. Project

The questionnaire

The first outputs

Hackers profiling

Evaluation and correlation standards

Detail analysis and correlation of profiles

Conclusions

Bibliography and references

Contacts

Conclusions

The hacking world has not always been linked to criminal actions;

The researches carried out till today have not depicted properly a so complex, hierarchical and in continuous evolution phenomenon as the underground world;

The application of a profiling methodology is possible, but it needs a 360° analysis of the phenomenon, by analysing it from four principal point of views: Technological, Social, Psychological, Criminological;

We still have a lot of work to do and we need support: if by ourselves we have reached these results, imagine what we can do by joining our forces and experiences !

The Hacker’s Profiling Project is open to collaborations and research partnerships.

HPP Next Steps

GOALS

✓ Data-base delivery

✓ Honey-Net systems delivery

WHAT WE NEED

✓ Looking for **contributors** (attack logs, hacking tales, experience)

✓ Looking for **volunteers** (log analysis, forensics analysis, reverse engineering)

✓ Researching of **sponsors** and funds raising

CHALLENGES

✓ Identification and evaluation of vectors, techniques and attack-tools

✓ Data-correlation and identification of patterns

✓ Release of the methodology at a *draft* level and starting of the HPP_IRP (Hackers Profiling Project Internal Review Process)

✓ Public release of the HPP 1.0 methodology

Considerations

✓ **The whole HPP Project** is self-funded and based on independent research methodologies.

✓ Despite many problems, we have been carrying out the Project for **two years**.

✓ The final methodology is going to be released under **GNU/FDL** and distributed through the ISECOM.

✓ **It is welcomed** the research centres, public and private institutions, and governmental agencies' interest in this research project.

✓ We think that we are **developing something beautiful**...

...**something that does not exist**...

...and it seems – really – **to have a sense** ! :)

✓ It is not a simply challenge. However, **we think to be on the right path**.

Agenda

Who we are

Introduction to the H.P.P. Project

The questionnaire

The first outputs

Hackers profiling

Evaluation and correlation standards

Detail analysis and correlation of profiles

Conclusions

Bibliography and references

Contacts

Bibliography and References (1)

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

. **The H.C.P. Questionnaires (2004-2005)**

. **Stealing the Network: How to 0wn a Continent**, (AA.VV), Syngress Publishing, 2004

. **Stealing the Network: How to 0wn the Box**, (AA.VV.), 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 e Joshua Quinttner, Harpercollins, 1995

. **Kevin Poulsen, Serial Hacker**, Jonathan Littman, Little & Brown, 1997

. **Takedown: sulle tracce di Kevin Mitnick**, John Markoff e 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 and William L. Simon, Wiley, 2002

. **The Art of Intrusion**, Kevin D. Mitnick and William L. Simon, Wiley, 2004

. **@ Large: the Strange Case of the World's Biggest Internet Invasion**, Charles Mann & David Freedman, Touchstone, 1998

. **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

. **SecurityFocus.com** (BugTraq, VulnDev), **Mitre.org** (CVE), **Isecom.org** (OSSTMM), many "underground" web sites & mailing lists, private contacts & personal friendships, the Academy and Information Security worlds

Bibliography and References (2)

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

- **Compendio di criminologia**, Ponti G., Raffaello Cortina, 1991
- **Criminalità da computer**, Tiedemann K., in "Trattato di criminologia, medicina criminologica e psichiatria forense", voumel X, "Il cambiamento delle forme di criminalità e devianza", Ferracuti F. (by), 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
- **Criminal Profiling Research Site. Scientific Offender Profiling Resource in Switzerland. Criminology, Law, Psychology**, Täterpro

Acknowledgements

The H.P.P. Project's Authors would like to thank for their contribution, support and time:

- **Key People:** Sentinel, Dr. Elisa Bortolani, Job De Haas, Kevin D. Mitnick, Mayhem, Venix, FX.
- **Events, Associations and Organizations**: HITB, *SecWest, Italian Hackmeeting, SysCan, MOCA, BLACKHAT, RUXCON, EUROSEC, CLUSIT, ISACA (Italian Chapter), OWASP meetings (Italian Chapter), ISO 27001 IUG (Italian Chapter), BellUA, Telecom Security Task Force, Phrack, 2600 Magazine, Xcon/Xfocus Team, Security Task Force Consortium.
- **Mailing lists**: SecurityFocus.com, Full-Disclosure, sikurezza.org, italian LUGs, private m.ls.
- **Gurus**: Raist, Raptor, Inode, Synack, Cla'75, Lamerone, Dialtone, Pete Herzog, Stefano Chiccarelli, Emmanuel Gadaix, Dr. Gabriele Faggioli, Trek/3K, Phlippe Langlois, Gabriella Mainardi, Antonis Anagnostopoulos, Marco Tracinà, Sentinel, Vittorio Pasteris, Pietro Gentile, Fabrizio Ciraolo, Alessandra Vitagliozzi, Jim Geovedi, Anthony Zboralski, the Grugq, Fabrice Marie, Roelef9 from SensePost, Dhillon Kannabhiran.

Special thanks to:

Daniele Poma, Andrea "Pila" Ghirardini, Andrea Barisani, Fabrizio Matta, Marco Ivaldi, Dr. Angelo Zappalà, Anna Masera, D.ssa Angela Patrignani, Prof. Ernesto Savona, Dr. Andrea Di Nicola, Patrizia Bertini, Dr. Mario Prati, Dr. Raffaella D'Alessandro, Ettore and Federico Altea, Vincenzo Voci, Massimiliano Graziani, Dr. Mimmo Cortese, Lapo Masiero, Simona Macellari, Amodiovalerio "Hypo" Verde, Paolo and Giorgio Giudice, Salvatore Romagnolo, Avv. Annarita Gili, Raffaela Farina, Enrico Novari, Laura Casanova De Marco, Fabrizio Cirilli, Eleonora Cristina Gandini, Dr. Alessandro Scartezzini, Stavroula Ventouri, Rosanna and Francesca D'Antona, Dr. Alberto Pietro Contaretti, Dr.ssa Alicia Burke, Andrey Buikis, Flaminia Zanieri and "the nano", Giovanni Lo Faro, Carla Fortin, Mirko "Mitch" Arcese, Lidia Galeazzo, Freddy "Seabone" Awad, Margherita Bo, Matteo Curtoni and Maura Parolini, Veronica Galbiati, Maya and Barbara "Wolf", Loren Goldig, Alessandro "Cyberfox" Fossato, Laura Di Rauso, Silvia Luzi.

HPP Partnerships

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

❑ **Here we list the HPP signed partnerships as of October 2006.**

✓ **Supporting Organizations**

hack in the box
Keeping Knowledge Free

APOGEOnline

Clusit
Associazione Italiana per la Sicurezza Informatica

WEB-HACK
>> GLOBAL HACKING IN PROGRESS...

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

Phenoelit
host: http://www.phenoelit.de

✓ **Project Sponsors**

mediaservice.net
CORPORATE SECURITY & IMAGE

alba
Alba S.T. srl

APOGEO

Agenda

Who we are

Introduction to the H.P.P. Project

The questionnaire

The first outputs

Hackers profiling

Evaluation and correlation standards

Detail analysis and correlation of profiles

Conclusions

Bibliography and references

Contacts

Links, contacts, Q&A

Hacker's Profiling Project home page:

- **http://www.isecom.org/hpp**

Hacker's Profiling Project *Questionnaires Home* for EU:

- **http://hpp.recursiva.org/**

Hacker's Profiling Project *Questionnaires Home* for ASIA:

- **http://hpp.hackinthebox.org/**

QUESTIONS ?

Project Leaders:

- Raoul Chiesa, Director of Communications

raoul@ISECOM.org

- Dr. Stefania Ducci, Independent Criminal Researcher

stefania@ISECOM.org