

INFOSECURITY ITALIA 2007

7 Febbraio 2007, Sala Azzurra

- HPP -

Hacker's Profiling Project: Risultati Survey 2004-2006

Raoul Chiesa (OPST, OPSA)

CLUSIT, ISECOM, TSTF, OWASP-IT

Board of Directors Member

D.ssa Elisa Bortolani (psicologa)

*Ricercatrice, Università di Verona,
Dipartimento di Psicologia e
Antropologia culturale*

Alessio "mayhem" Pennasilico

CLUSIT, AIPSI, AIP

Disclaimer

- Il seguente materiale è protetto da copyright, appartenente a Raoul Chiesa, Dr.ssa Stefania Ducci, D.ssa Elisa Bortolani, Alessio Pennasilico (©) 2004-2007, e non può essere modificato o riprodotto parzialmente senza quotare gli autori.
 - Questa presentazione non contiene informazioni che violano la proprietà intellettuale o che riguardano strumenti o indicazioni che possano essere in violazione delle leggi esistenti.
 - I marchi industriali indicati appartengono ai loro proprietari registrati.
-

Agenda

Chi siamo

Introduzione al progetto H.P.P.

Il questionario

I risultati ad oggi emersi

Hackers profiling

Conclusioni

Contatti

Agenda

Chi siamo

Introduzione al progetto H.P.P.

Il questionario

I risultati ad oggi emersi

Hackers profiling

Conclusioni

Contatti

Il team

- Un gruppo di esperti indipendenti, specializzati su singole tematiche:
 - Sicurezza delle informazioni
 - Psicologia
 - Criminologia
 - Sociologia
 - Core Team:
 - D.ssa Elisa Bortolani
 - Raoul Chiesa
 - Stefania Ducci
 - Alessio “mayhem” Pennasilico
-

ISECOM



- Teens and pre-teens (Hacker Highschool)

ISECOM: Key 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 (www.hackerhighschool.org)
 - **HPP – Hacker's Profiling Project** (www.isecom.org/hpp)
-

Agenda

Chi siamo

Introduzione al progetto H.P.P.

Il questionario

I risultati ad oggi emersi

Hackers profiling

Conclusioni

Contatti

Il “cybercrime”

Occupandoci di problematiche di sicurezza “hacking-related” da oltre un decennio, in questi ultimi anni abbiamo osservato con attenzione una serie di fenomeni che ci sentiamo di definire “preoccupanti”:

- ✓ Drammatica diminuzione della c.d. “window of exposure”, ovvero il tempo che trascorre dalla stesura di exploit “0-day” sino al loro utilizzo in **attacchi massicci** e/o distribuiti a livello mondiale;
- ✓ **Pericolose sinergie** tra personalità tecnologicamente avanzate, criminalità classica (nazionale ed internazionale) e terrorismo;
- ✓ Continua **crescita della dipendenza** tra la stabilità nazionale (infrastrutture critiche nazionali, homeland security, telecomunicazioni, servizi di base, etc.) e le problematiche di ICT Security.

Ciò nonostante, spesso i fenomeni del cybercrime e degli hi-tech crime vengono **analizzati in maniera errata**.

Il progetto H.P.P.

Abbiamo allora voluto analizzare il “**problema del cybercrime**” utilizzando un approccio completamente diverso da quelli individuati sino ad oggi: andando cioè **direttamente alla fonte**.

Il progetto H.P.P. si pone infatti l'obiettivo di:

- Analizzare il fenomeno – tecnologico, sociale ed economico – dell'hacking nelle sue mille sfaccettature, mediante **approcci sia di tipo tecnico che criminologico**;
 - Comprimerne le **differenti motivazioni** ed **individuare gli attori** chiamati in causa;
 - **Osservare** “sul campo” le (**vere**) azioni criminali;
 - **Applicare** la metodologia di profiling ai dati raccolti;
 - **Apprendere** dalle conoscenze acquisite e **divulgarle**.
-

Le fasi progettuali

Il progetto H.P.P. ha avuto inizio nel **settembre 2004**. Ad oggi, sono state definite **8 distinte fasi progettuali**.

<p>Fase 1 RACCOLTA TEORICA</p> <p>Progettazione e Distribuzione del questionario, in diverse forme e verso target differenziati.</p>	<p>Fase 5 G&C ANALYSIS</p> <p>Gap-Analysis e Correlazione tra i dati raccolti attraverso il questionario, i dati provenienti dalle HoneyNet ed i profili ricavati dalla letteratura in materia.</p>
<p>Fase 2 OSSERVAZIONE</p> <p>Partecipazione ad eventi di “IT underground security” (EU, Asia, USA, Australia).</p>	<p>Fase 5/A HPP “live”ASSESSMENT (24x7)</p> <p>Assessment continuo dei profili e correlazione del modus operandi, tramite i dati provenienti da Ph. #4.</p>
<p>Fase 3 ARCHIVIAZIONE</p> <p>Creazione di un Data-Base per la classificazione e l’elaborazione dei dati raccolti da Fase 1.</p>	<p>Fase 6 PROFILING FINALE</p> <p>Ridefinizione e fine-tuning dei diversi profili hacker precedentemente utilizzati come “standard de-facto”.</p>
<p>Fase 4 RACCOLTA “live”</p> <p>Progettazione e messa in produzione di sistemi HoneyNet di nuova generazione ed altamente customizzati.</p>	<p>Fase 7 DIFFUSIONE DEL MODELLO</p> <p>Elaborazione finale dei risultati emersi, stesura e pubblicazione della metodologia, sensibilizzazione (white papers, conferenze, company awareness, formazione).</p>

Fasi progettuali: dettaglio

FASE	ESEGUITA		DURATA	ANNOTAZIONI
1 – Raccolta Teorica	SI	IN CORSO	16 mesi	Distribuzione si più livelli
2 – Osservazione	SI	IN CORSO	24 mesi	Sotto diverse forme
3 – Archiviazione	IN CORSO (PROGETTAZIONE)		Progettazione: 3 mesi Produzione & Fine Tuning: 18 mesi	La fase più difficile
4 – Raccolta “live”	IN CORSO (LAB ESISTENTE)		Progettazione: 3 mesi Produzione: 18 mesi	La fase più divertente ☺
5 – Gap & Correlation Analysis	NO		18 mesi	The Next Thing
5/A – Assessment “live”	NO		16 mesi	Il grosso del lavoro
6 – Profiling Finale	NO		12 mesi	“Satisfaction”
7 – Diffusione del modello	NO		GNU/FDL ;)	Metodologia

Perché HPP piace ?

- Ce lo spiega Alessio !



Agenda

Chi siamo

Introduzione al progetto H.P.P.

Il questionario

I risultati ad oggi emersi

Hackers profiling

Conclusioni

Contatti

Questionario “HCP” - Hackers' Criminal Profiling

- Modulo “A”

Data personali (genere, età, status sociale, contesto familiare, studio/lavoro)

- Modulo “B”

Dati relazionali (rapporto con: Autorità, insegnanti/datori di lavoro, amici/colleghi, altri hacker)

- Modulo “C”

Dati tecnici e criminologici (target, modalità di attacco e tools, motivazioni, etica, percezione della illiceità della loro attività, reati commessi, deterrenza)



Tutte le domande
permettono
risposte anonime

QUESTIONARIO “HCP” - La somministrazione

✓ **2 tipologie di questionario:**

□ **Livello 1:** Completo

25 pagine, Moduli A, B e C completi (tutti i campi obbligatori)

□ **Livello 2:** Compatto

10 pagine, Moduli A, B e C parzialmente completi (selezione di alcuni campi obbligatori)

✓ **3 livelli di somministrazione:**

□ **Conosciuti e/o verificati, indirettamente o meno (QoQ estremamente alto)**

□ **Testate specializzate, cartacee ed on-line (QoQ medio)**

□ **Altro (QoQ basso)**

Il questionario: alcuni estratti

a) Sesso:

Maschio

Femmina

b) Et :

c) Titolo di studio (segnare l'ultimo conseguito):

Licenza elementare

Licenza di scuola media inferiore

Qualifica professionale

Diploma di scuola media superiore

Diploma di laurea

Oltre (master, dottorato di ricerca, specializzazione, ecc.)

d) Nazione e luogo di residenza (se non vuoi precisare la tua citt , per favore, indica l'area geografica di residenza). Specifica anche se vivi in una citt  o in un paese e, in quest'ultimo caso, se questo   lontano o meno da un grande centro urbano.

a) Conoscenza della tua attivit  di hacking/phreaking:

1)

(a) Tra le persone che conosci, chi   (o era) a conoscenza della tua attivit  di hacking/phreaking? (insegnanti, datore/i di lavoro, compagni di scuola, colleghi, amici, altri membri del mondo underground, partner, ecc.).

d) Hacking, phreaking, carding:

1) Pratichi (o Praticavi):

- l'hacking S  No

- il phreaking S  No

e) Tipologie di reti dati, tecnologie e sistemi operativi su cui operi (o operavi) e strumenti impiegati:

1) *Su quali tipologie di reti dati e tecnologie "fai" (o "facevi") hacking/phreaking? Ad esempio: Internet, X.25, PSTN/ISDN, PBX, Wireless, reti "mobili" (GSM/GPRS/EDGE/UMTS), VoIP.*

(a) Ci sono altre persone nella tua famiglia che si interessano (o interessavano) di informatica?

S 

No

(b) Ci sono altre persone nella tua famiglia che praticano (o praticavano) l'hacking/il phreaking?

Il questionario: alcune risposte

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.

Il questionario: alcuni commenti

- *Buon hack*
- *La trovo un'idea particolare, spero otterrete buoni risultati*
- *Divertente, l'avrei preferito in SSL, pratico.*
- *Nice job !*
- *Cambieranno veramente gli stereotipi sugli Hacker? spero di si*
- *Ben fatto. Speriamo di vedere i risultati pubblicati presto online. Si renda conto che sta facendo un censimento che puo' essere utilizzato in molti modi, speriamo bene. Non lo utilizzi solamente per il suo libro, ripeto: pubblichiamo tutto online. Così facendo darà veramente un buon tema di discussione a tutti gli utenti.*

- *Bel progetto....ma realizzabile veramente?*
- *Carino. Spero che questi dati siano usati a fin di bene, per far capire che l'hacking etico non è reato ma, anzi, una forma di volontariato. Sarebbe bello poter proporre ai singoli forme di \"ciao, provo la security del tuo sito. Non combino danni, ti aiuto a sistemarli\". baci & abbracci*
- *Non mi è piaciuta la definizione di hacking legata esclusivamente ad attività illegali. All'inizio ho compilato il questionario avendo in mente l'hacking che svolgo normalmente per lavoro tutti i giorni, poi però ho deciso di assecondarvi e ho risposto tenendo presente la vostra definizione un po' forzata. Avrei ritenuto più giusto considerare \"hacking\" tutto il processo creativo che c'è attorno alla scoperta di vulnerabilità, creazione di exploit e penetrazione nei sistemi, non per forza illegali. Per essere (o aspirare ad essere) hacker non c'è bisogno di commettere per forza azioni illecite. Tanti hacker moderni lavorano nella piena legalità e contribuiscono allo stesso modo (e anche in maniera migliore) allo sviluppo delle tecnologie.*

Il questionario: osservazioni

- Il progetto HPP **non** si basa esclusivamente sui questionari ricevuti per la stesura e l'elaborazione delle metodologie di profiling ;)
 - Conseguentemente, alcuni profili sono stati elaborati in seguito ad incontri personali con hacker appartenenti a categorie specifiche.
 - La fase 1 e la fase 2 di HPP sono quindi state propedeutiche alle successive fasi progettuali.
 - Il numero di questionari, consigli, commenti, auguri ci ha sinceramente stupito. Ed un po' commosso.
-

Il questionario: considerazioni tecniche

- Grande attenzione verso i dati dei rispondenti
 - Cifrare ? Sì, grazie
 - Gestione dei log
 - Affidabilità
-

Agenda

Chi siamo

Introduzione al progetto H.P.P.

Il questionario

I risultati ad oggi emersi

Hackers profiling

Conclusioni

Contatti

Hackers: un'immagine non ancora nitida

- **Ieri:** hacking come **fenomeno emergente**, sconosciuto alle masse e ignorato dagli studiosi.
 - **Oggi:** diverse ricerche ed analisi su hacking ed hackers ma **eseguiti in “mono”**: profilo psicologico, o sociologico, o criminologico, soprattutto in seguito ai cd. Hacker Crackdown → un'unica tipologia di hackers, visti come brutti (mingherlini, miopi), cattivi (intenti sempre malvagi, distruttivi e/o criminali) e “sporchi” (asociali, privi di etica, anarchici).
 - **Domani:** studi interdisciplinari che **coniugano la criminologia con la sicurezza informatica** → diverse tipologie di hacker se si considerano: le **modalità di azione** (da solo/a o in gruppo), le **capacità tecniche**, le **motivazioni**, gli **scopi**, i **target**, l'adesione o meno alla cd. “**etica hacker**”.
-

Una nuova prospettiva: i primi dati dei questionari “HPP 2004/06” (1)

- Persone di regola intellettualmente **brillanti, creative, decise e risolte**
 - Provano **rabbia e ribellione verso le Autorità e la chiusura mentale**, viste come una minaccia per le libertà civili
 - **Hacking come: 1) tecnica e modo di vivere** con curiosità e voglia di mettersi alla prova; **2) strumento di potere** utile per sensibilizzare le masse su problemi politici e sociali
 - Di solito sono spinti dall'**amore per la conoscenza**; non mancano tuttavia coloro che hanno **fini di lucro** e si dedicano perciò al **phishing/pharming**, al **carding** o allo **spionaggio industriale**
 - Target preferiti: **sistemi militari/governativi; grandi corporazioni; telco; scuole e Università**, ma anche gli **utenti finali e le PMI**
 - La **maggior parte degli hacker (di basso livello tecnico) sono scoraggiati da sistemi difficili da penetrare**: preferiscono S.O. “facili” come Linux o Windows – gli hacker più capaci invece sono stimolati solo da sistemi considerati “inviolabili” (*BSD, Solaris, HP/UX, *VMS, IOS, Symbian) e dai protocolli...
-

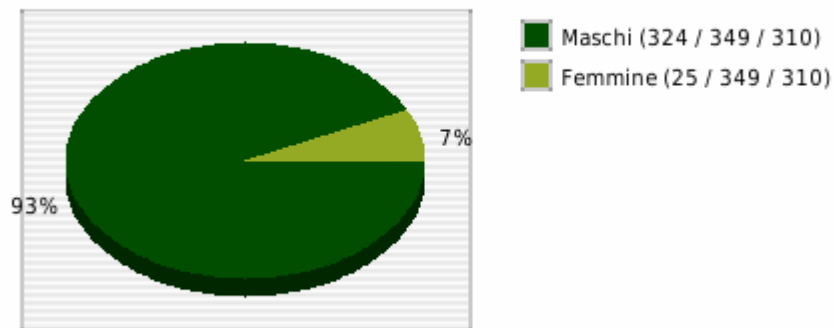
Una nuova prospettiva: i primi dati dei questionari “HPP 2004/06” (2)

- Scaricano la colpa dei loro attacchi sui SysAdmin (o sui progettisti), in quanto non sono stati capaci di proteggere adeguatamente il sistema (o di progettare/definire in maniera *sicura* un protocollo o uno standard)
 - Gli hacker etici sono soliti avvisare il SysAdmin delle vulnerabilità riscontrate nel sistema (o contribuire al fix della security flaw), ma in genere solo dopo averle comunicate agli altri membri dell'underground
 - Gli hacker etici vogliono migliorare la sicurezza dei sistemi ed accrescere la consapevolezza e l'attenzione verso tali problematiche da parte dei SysAdmin
 - Gli hacker etici fanno proprio il sistema penetrato e lo difendono da altri attacchi rendendolo sicuro
 - Gli hacker etici non fanno crashare il sistema (se non accidentalmente per inesperienza) e non rubano/cancellano/modificano dati
-

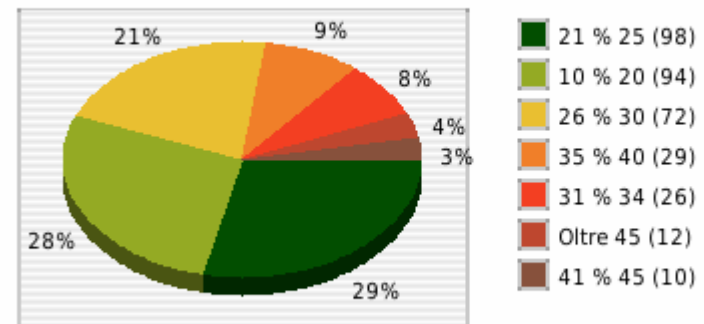
Qualche numero + “hackpies”

- Siccome alla gente “piacciono tanto le torte”, le abbiamo fatte anche noi 😊

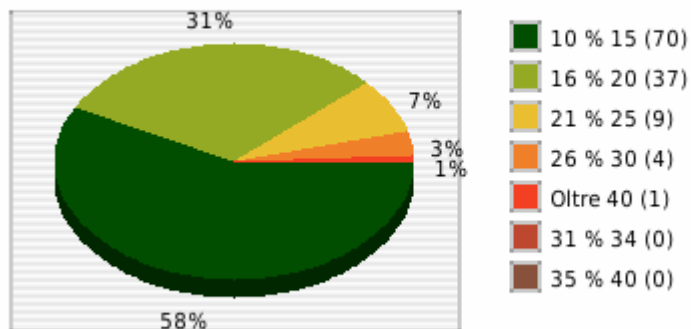
Sesso



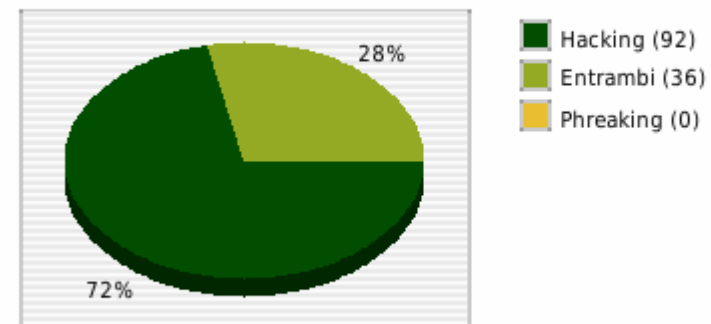
Eta' [Totali: 341, Nulli: 318]



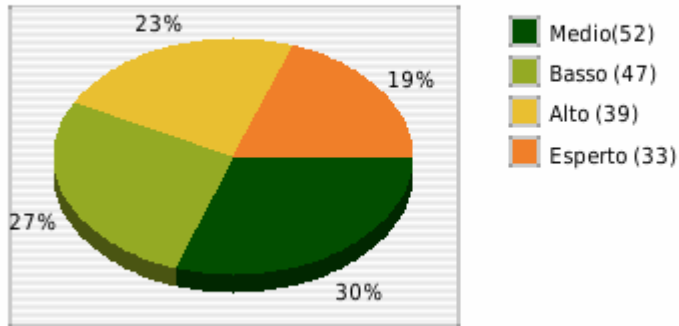
Eta' di inizio hack [Totali: 125, Nulli: 531]



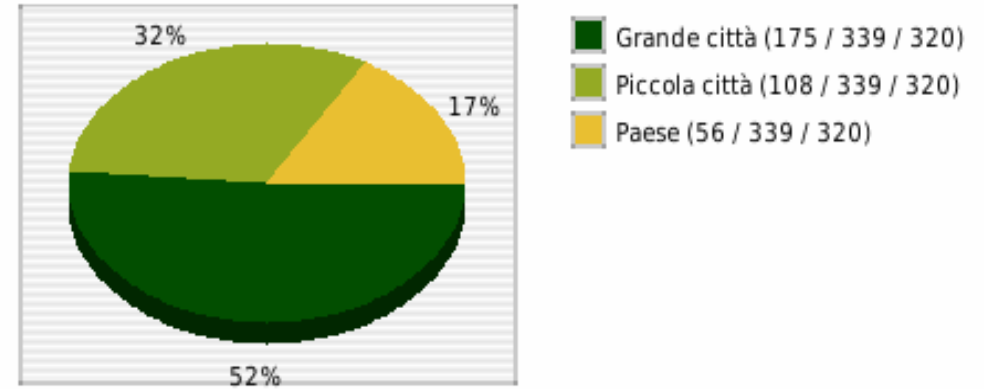
Pratichi? [Totali: 128, Nulli: 528]



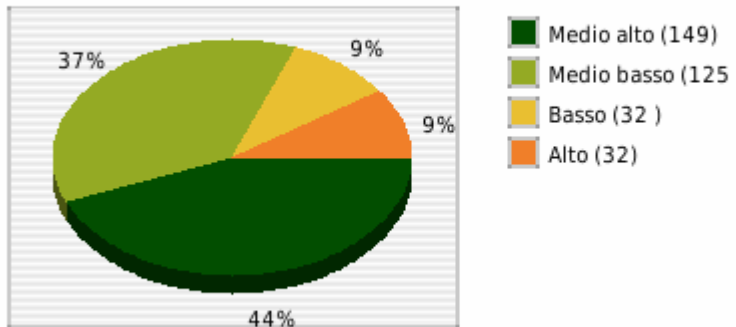
Capacita' tecniche [Totali: 171, Nulli: 521]



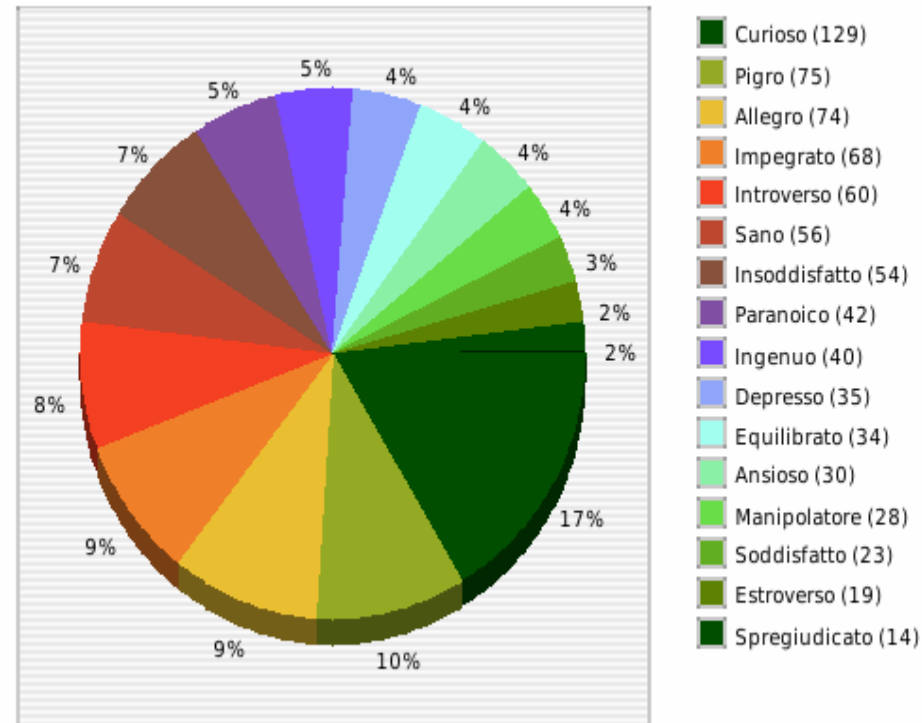
Dove



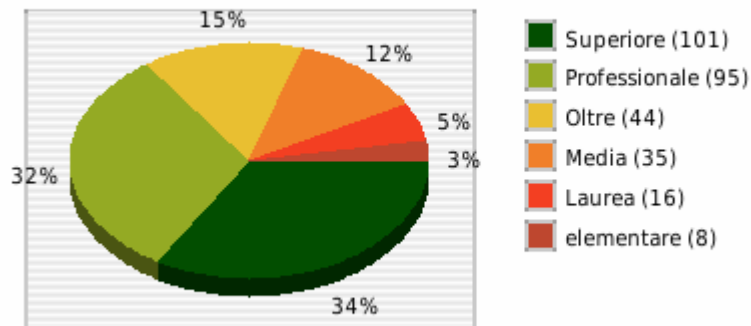
Status socio-economico [Totali: 338, Nulli: 321]



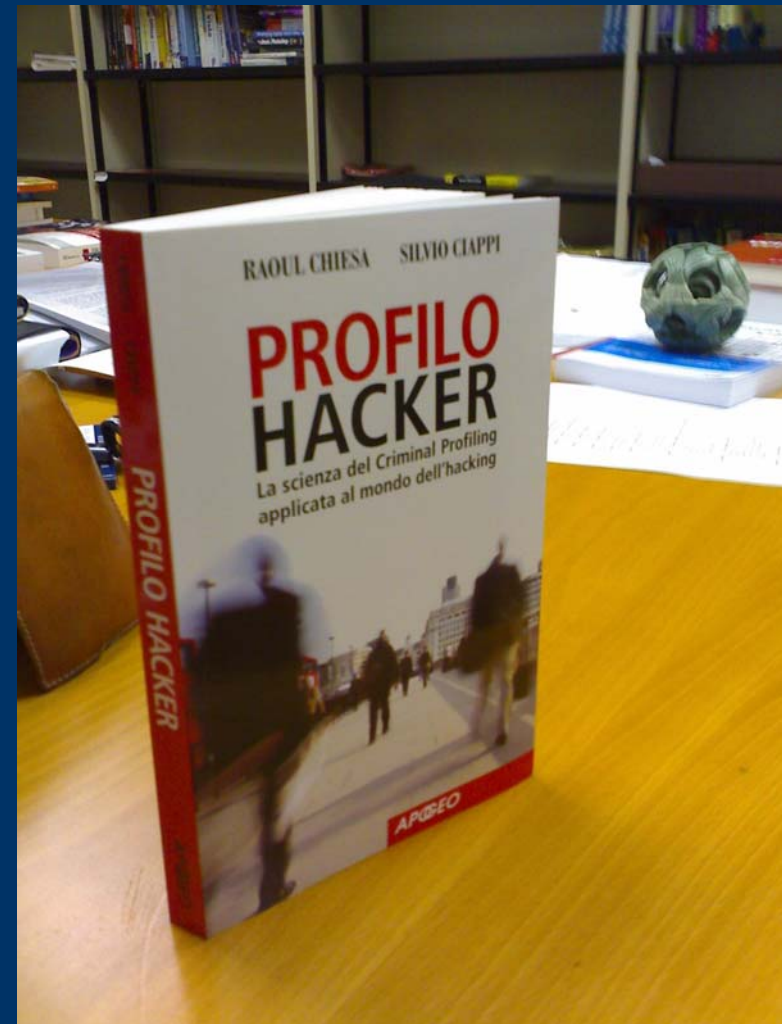
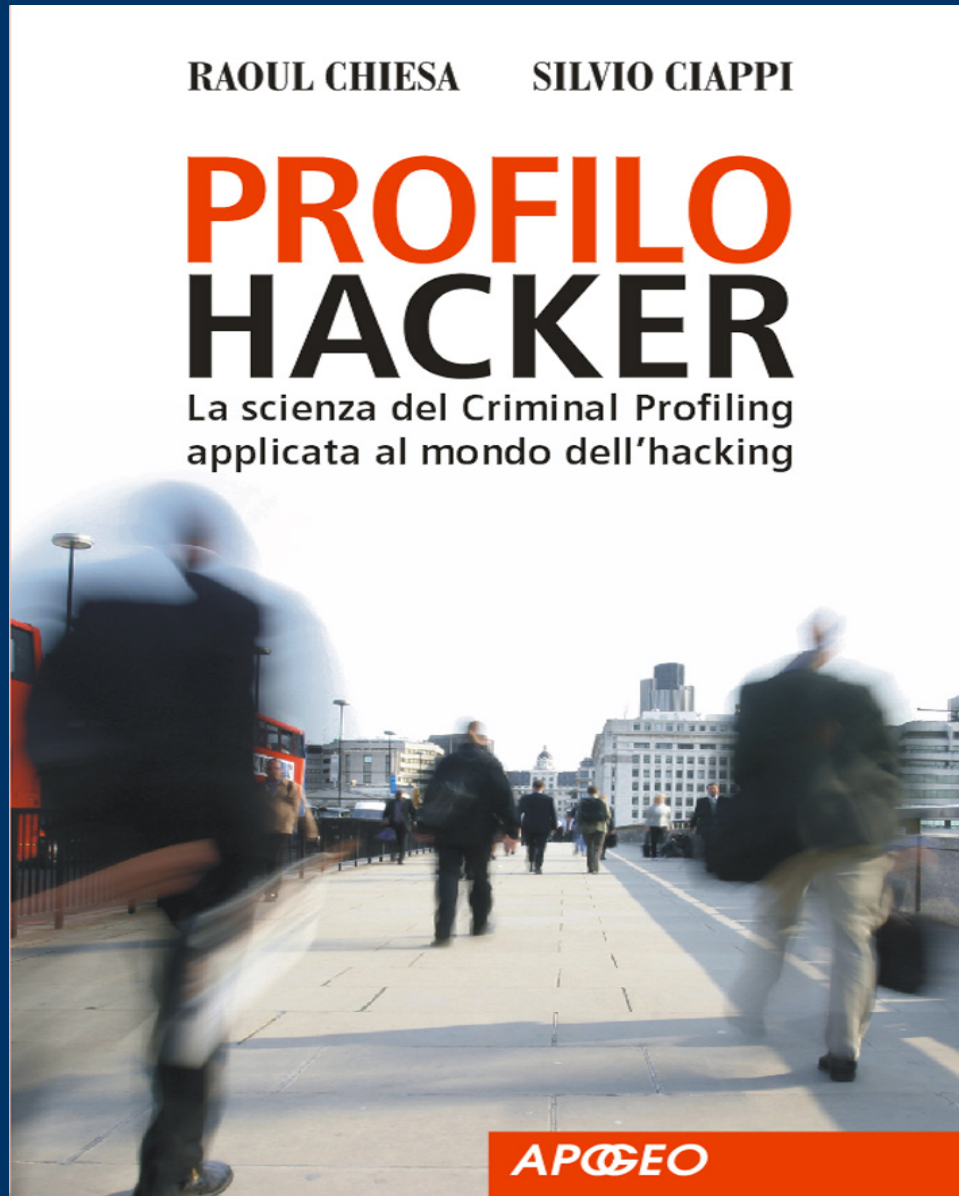
Personalità



Titolo di studio [Totali: 299, Nulli: 354]



Dal progetto on-the-road al “diario di bordo”: Profilo Hacker, il libro



Agenda

Chi siamo

Introduzione al progetto H.P.P.

Il questionario

I risultati ad oggi emersi

Hackers profiling

Conclusioni

Contatti

Hacker's Criminal Profiling: starting point



Know your Enemy: hackers' profiling

PSYCHOLOGICAL PROFILE

DANGEROUSNESS LEVEL

Wannabe Lamer

NULL

(I'd like to be an hacker, but I can't...)

Script Kiddie

LOW

(The script boy)

Cracker

HIGH

(Burned ground, the Distructor)

Ethical Hacker

MEDIUM

(The "ethical" hacker's world)

Quiet, paranoid, skilled hacker

MEDIUM

(The very specialized and paranoid attacker)

Cyber-Warrior

HIGH

(The soldier, hacking for money)

Industrial Spy

HIGH

(Industrial espionage)

Government agent

HIGH

(Governative agent: CIA, Mossad, FBI, etc. – Cuckoo's Egg docet)

Hacker's Criminal Profiling: yesterday



Know your Enemy: preferred targets

PSYCHOLOGICAL PROFILE

Wannabe Lamer

(I'd like to be an hacker, but I can't...)

Script Kiddie

(The script boy)

Cracker

(Burned ground, the Distructor)

Ethical Hacker

(The "ethical" hacker's world)

Quiet, paranoid, skilled hacker

(The very specialized and paranoid attacker)

Cyber-Warrior

(The soldier, hacking for money)

Industrial Spy

(Industrial espionage)

Government agent

(Governative agent: CIA, Mossad, FBI, etc. – Cuckoo's Egg docet)

TARGET

End-user

SME/specific security flaws

Big Companies/PA/Finance/Telco

Vendor/System Integrator/Telco

Big Companies/PA/Finance/Telco/R&D

Multinationals "symbol"

Multinationals, ICT companies

Multinationals/Governments

Hacker's Criminal Profiling

PROFILE	RANK	IMPACT LEVEL		TARGET	
Wanna Be Lamer	Amateur	NULL		End-User	
Script Kiddie		LOW		SME	Specific security flaws
Cracker	Hobbyist	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
		HIGH		Strategic Company	Individual
Military Hacker		HIGH		Government	Strategic Company

Motivazioni

1. Per **intelligente curiosità**, e quindi per imparare e conoscere
 2. Per **amore per la tecnologia**
 3. Per **dimostrare di** essere brillanti e intelligenti
 4. **Divertimento**, gioco
 5. Perché è **noioso usare il computer in maniera normale** (tanto sono capaci tutti: e quindi come faccio a distinguermi dagli altri? Semplice, usandolo in modo non convenzionale)
 6. Perché **adorano risolvere problemi**
 7. Per **migliorare i computer**, renderli più potenti e facili da usare
 8. Per spirito d'avventura, **per l'adrenalina che si prova**, dovuta al rischio di essere scoperti, all'ebbrezza del proibito, od al fatto di possedere il sistema
-

Motivazioni

1. Perché **annoati** dalla routine
 2. Romanticismo, **tradizione**, mito
 3. Per **attrarre l'attenzione dei mass media** sperando di diventare famosi
 4. Per **danaro**
 5. Per **rabbia** e frustrazione
 6. Per **ragioni ideologiche** (politiche, sociali, ecc.)
 7. Per il **cameratismo** presente all'interno della comunità hacker
 8. Per **fuggire da un ambiente familiare** conflittuale e/o **da una realtà sociale alienante**
 9. Per **professione** (esperti di sicurezza informatica, cyber-warriors, spie industriali, agenti governativi e military hackers)
-

Motivazioni

1. Come strumento per **difendere le libertà civili** degli hackers nel cyberspazio e, più in generale, di tutti gli utenti
 2. Per difendere le libertà, soprattutto di informazione, rendendo le **informazioni libere**, accessibili a tutti, e quindi sconfiggere il monopolio della comunicazione e della cultura (knowledge addiction)
 3. Per fornire un servizio condividendo accessi che essi ritengono che dovrebbero essere liberi (**lotta al monopolio delle telecomunicazioni**)
 4. Per preservare la (propria ed altrui) privacy dalle **intrusioni delle Autorità**
 5. Per volontà di **accrescere il livello di sicurezza** delle reti e dei sistemi informatici
 6. Per un **atteggiamento anti-establishment**, anti-autorità (in particolare militare-industriale), facendo così trionfare l'individuo sulla collettività
 7. Per **ribellione**: sfida verso le autorità, rappresentate non solo dalle Autorità in senso stretto (forze dell'ordine ed agenzie governative in genere), ma anche da quelle in senso lato (system administrators, genitori ed adulti in genere), al fine di mostrare loro il “potere hacker” e sentirsi superiore ad esse
-

Evoluzione generazionale delle motivazioni

- La **prima generazione (fine anni '70)** era spinta dalla **sete di sapere**
 - La **seconda (prima metà anni '80)** era spinta dalla **curiosità, unita alla sete di sapere** e al fatto che molti sistemi operativi e reti/sistemi erano apprendibili unicamente bucadoli; più tardi, verso la **seconda metà degli anni '80**, il fenomeno unisce fattori di **moda trend**
 - La **terza (anni '90)** era spinta dalla semplice **voglia di fare hacking**, inteso come un **insieme di curiosità, voglia di imparare e conoscere cose nuove, intenzione di violare sistemi informatici, scambio di informazioni con la comunità underground**. E' in questa fase che si formano i primi gruppi di hackers, che nascono le e-zine hacker e che si propagano i BBSs
 - La **quarta (2000)** è mossa dalla **rabbia**: si tratta spesso di soggetti con scarse conoscenze tecniche, ma che trovano gagliardo e di moda essere degli hackers, non conoscono o non sono interessati alla storia, alla cultura ed all'etica del phreaking e dell'hacking. Qui l'hacking si mescola alla politica e diventa così uno strumento di **cyber-hacktivism**
-

Targets principali

- **Sistemi/siti di enti governativi, in particolare militari**
 - **Grandi corporazioni (soprattutto finanziarie), che amministrano funzioni critiche per la sicurezza o l'economia nazionale**
 - **Critical National Infrastructures (Autostrade, Acquedotti, P.A., L.E.A.)**
 - **Società di telecomunicazione, di servizi Internet, o che producono componenti hardware/software**
 - **Scuole e Università (questi ultimi di solito usati come launchpad per lanciare attacchi a target finali)**
-

Percezione della illegalità della propria attività

- **Sanno che** ciò che fanno è reato
 - **Non si sentono dei criminali**, nè considerano criminale fare hacking, o comunque non lo vedono come un grave reato come ad es. rubare
 - **Non sempre sono consapevoli** delle conseguenze economiche dei loro attacchi
 - Gli hackers etici considerano la loro **condotta moralmente accettabile** proprio perché seguono dei principi etici
 - Si tratta secondo loro di **reati senza vittima** perché pensano di non danneggiare nessuno
 - Ritengono **ingiusto dover finire in prigione** per quello che hanno fatto
 - Non sentono **nè pentimento nè rimorso** per le loro azioni
-

Efficacia deterrente delle leggi, delle condanne e delle difficoltà tecniche

- *Efficacia deterrente: nulla* => usano i gaps delle leggi per aggirarle
 - L'introduzione di leggi più severe sui computer crime e i continui raid della polizia li hanno fatti diventare più sofisticati e paranoici => da comunità aperta ed amichevole l'underground è divenuto un circolo chiuso ed elitario dove la diffidenza ha preso il posto della collaborazione => hacking come fenomeno meno visibile e percepibile => maggiore presenza di hacker solitari
-

Efficacia deterrente delle leggi, delle **condanne** e delle difficoltà tecniche

- *Efficacia deterrente: scarsa* (soprattutto se si tratta della prima condanna e/o se il soggetto è dipendente dall'hacking o se lo fa per fini di profitto) => alcuni continuano a fare hacking anche sotto processo o mentre sono braccati dalla polizia => *si sentono invincibili e sono consapevoli del fatto che ormai non hanno più nulla da perdere (hacking addiction)*
 - *le condanne inflitte agli hackers, per la maggior parte, **non hanno alcun effetto deterrente sugli altri membri del mondo underground.** Il loro spiccato ego e la illimitata fiducia nelle proprie capacità li porta a credere che essi non commetteranno mai gli errori che hanno portato all'arresto di altri hackers*
-

Efficacia deterrente delle leggi, delle condanne e delle **difficoltà tecniche**

- ***Efficacia deterrente: nulla** (soprattutto per gli hacker d'elite e per quelli motivati dalla sete di conoscere)*
 - *Costituendo una sfida, diventano uno **stimolo in più ad entrare in un dato sistema**, e più il sistema è difficile da penetrare, più si divertono*
-

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

Chi siamo

Introduzione al progetto H.P.P.

Il questionario

I risultati ad oggi emersi

Hackers profiling

Conclusioni

Contatti

Conclusioni

Il mondo dell'hacking **non è sempre stato legato** ad azioni di tipo criminoso;

Le ricerche ad oggi eseguite non hanno “reso giustizia” ad un **mondo complesso, gerarchico, in continua evoluzione;**

L'applicazione di una metodologia di profiling **è possibile**, ma richiede un'analisi a 360° del fenomeno, analizzandolo da quattro principali punti di vista: **Tecnologico, Sociale, Psicologico, Criminologico;**

Abbiamo ancora **molto lavoro da fare e ci serve aiuto:** se da soli siamo riusciti ad arrivare sino a qui, immaginate **cosa potremmo fare unendo le forze e le esperienze !**

Il progetto H.P.P. è **aperto alle collaborazioni.**

Next Steps

▣ **OBIETTIVI**

- Delivery del Data-Base
- Delivery dei sistemi Honey-Net

▣ **NECESSITA'**

- Ricerca volontari (analisi log, analisi forensi, reverse engineering)
- Ricerca sponsor

▣ **SFIDE**

- Identificazione e peso di vettori, tecniche e tools di attacco
 - Correlazione dei dati e stesura su modelli
 - Rilascio della metodologia allo stato *draft* ed Attivazione del processo di internal review
 - Rilascio pubblico della metodologia HPP 1.0
-

Riflessioni

- **Tutto** il progetto è ad oggi auto-finanziato e basato su metodologie di ricerca indipendenti.
 - Nonostante le continue problematiche, andiamo avanti da **due anni**.
 - La metodologia finale sarà rilasciata sotto **GNU/FDL** e veicolata tramite l'ISECOM.
 - L'interesse da parte di centri di ricerca, istituzioni pubbliche e private ed agenzie governative è **ben accetto**.
 - Pensiamo di stare **costruendo qualcosa di bello...**
...qualcosa che non c'è...
...e che pare – addirittura – abbia un senso ! :)
 - Non è una sfida semplice, ma **riteniamo di essere sulla giusta strada.**
-

Ringraziamenti

Gli autori del progetto H.P.P. si sentono di ringraziare per il loro contributo, supporto e tempo dedicato:

- **Key People:** Dr.ssa Elisa Bortolani, Job De Haas, Kevin D. Mitnick, Mayhem, Venix.
- **Events, Associations and Organizations:** HITB, *SecWest, Italian Hackmeeting, SysCan, MOCA, BLACKHAT, RUXCON, EUROSEC, CLUSIT, ISECOM, 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, private m.l.
- **Gurus:** Raist, Raptor, Inode, Synack, Cla'75, Lamerone, Dialtone, Pete Herzog, Stefano Chiccarelli, Emmanuel Gadaix, Avv. Gabriele Faggioli, Trek/3K, Philippe Langlois, Gabriella Mainardi, Antonis Anagnostopoulos, Marco Tracinà, Sentinel, Vittorio Pasteris, Pietro Gentile, Fabrizio Ciruolo, Alessandra Vitagliozi, Jim Geovedi, Anthony Zboralski, the Grugq, Fabrice Marie, Roelef9 from SensePost, Dhillon Kannabhiran.

Un ringraziamento particolare, infine, va a:

• Daniele Poma, Andrea “Pila” Ghirardini, Andrea Barisani, Fabrizio Matta, Marco Ivaldi, Dr. Angelo Zappalà, D.ssa Angela Patrignani, Patrizia Bertini, Dr. Mario Prati, Vincenzo Voci, Massimiliano Graziani, Dr. Mimmo Cortese, Lapo Masiero, Simona Macellari, Salvatore Romagnolo, Avv. Annarita Gili, Raffaella Farina, Enrico Novari, Fabrizio Cirilli, Stavroula Ventouri, Dr. Alberto Pietro Contaretti, Dr.ssa Alicia Burke.

Partner e Sponsor della ricerca



Agenda

Chi siamo

Introduzione al progetto H.P.P.

Il questionario

I risultati ad oggi emersi

Hackers profiling

Conclusioni

Contatti

End of Story

Now that we have all this useful information, **it would be nice to do something with it.** (Actually, it can be emotionally fulfilling just to get the information. This is usually only true, however, if you have **the social life of a glass of water.**)

Unix Programmer's Manual.



Contatti

Raoul “Nobody” Chiesa

raoul@ISECOM.org

D.ssa Elisa Bortolani

elisa@recursiva.org

Alessio “mayhem” Pennasilico

mayhem@recursiva.org

Grazie
per
l'attenzione !

Domande?

<http://hpp.recurativa.org>

<http://hpp.antifork.org>

<http://hpp.web-hack.ru>

<http://hpp.hackinthebox.org>

Fill the questionnaire!

