Cyber- ~~Security~~ Crime & Hackers Profiling

VERSIONE PUBBLICA

Presentazione di Raoul Chiesa

Founder, Strategic Alliances, @ Mediaservice.net

PSG Member, ENISA (European Network & Information Security Agency)

Senior Advisor, Strategic Alliances & Cybercrime Issues, GCU (Global Crimes Unit)
United Nations - Interregional Crime and Justice Research Institute (UNICRI)

unicri
advancing security, serving justice, building peace

Disclaimer

- Le informazioni contenute in questa presentazione **non infrangono** alcuna proprietà intellettuale, nè contengono strumenti o istruzioni che potrebbero **essere in conflitto** con la vigente legislazione.

- La presentazione nella sua versione **pubblica** non conterrà alcune slide, immagini e grafici relative ad **operazioni sotto copertura**.

- I dati statistici qui presentati appartengono all'**Hackers Profiling Project** (HPP).

- I marchi registrati appartengono ai **rispettivi proprietari**.

- Le opinioni qui espresse sono quelle dell'autore e **non rispecchiano necessariamente** quelle dell'UNICRI, di altre agenzie delle Nazioni Unite o dell'ENISA.

mediaservice.net
CORPORATE SECURITY & IMAGE

Nella mente dell'hacker

unicri
advancing security, serving justice, building peace

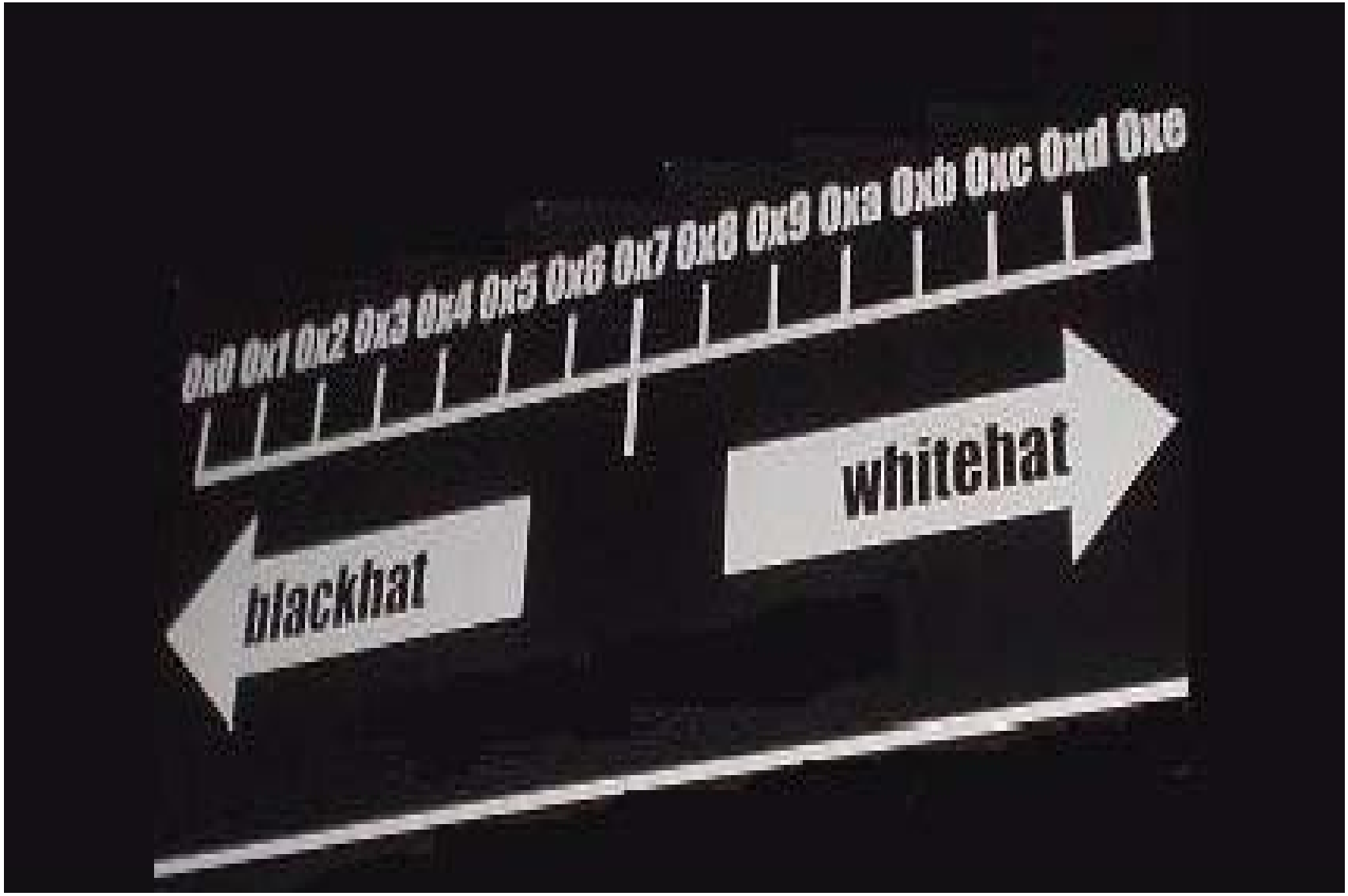
Agenda

- ✓ Chi sono
- ✓ UNICRI, ENISA
- ✓ L'hacking di ieri, il crimine di oggi
- ✓ Hacking: le date storiche
- ✓ Cybercrime
- ✓ Profiling the enemy
- ✓ Hackers…
- ✓ HPP: l'Hackers Profiling Project
- ✓ Some stats (hackpies)
- ✓ Hacking, oggi: Underground Economy
- ✓ Conclusioni
- ✓ References: libri da leggere
- ✓ Contatti, Q&A

mediaservice.net
CORPORATE SECURITY & IMAGE

Introduzione

Chi sono ?



mediaservice.net
CORPORATE SECURITY & IMAGE

Raoul Chiesa

❑ Hacker dal 1986 al 1995, quando vengo arrestato per una lunga serie di violazioni informatiche presso istituzioni ed enti ad alta criticità, nel corso dell'operazione "Ice Trap" condotta dalla S.C.O., Criminalpol, Interpol ed FBI.

❑ Da allora il mio approccio all'ICT Security è maturato: nel 1996 inizio ad occuparmi professionalmente di ethical hacking e, nel 1997, fondo insieme a Daniele Poma la @ **Mediaservice.net**, società di consulenza vendor-independent molto nota a livello europeo.

❑ Sono inoltre socio fondatore del **CLUSIT** (Associazione italiana per la sicurezza informatica), dove ricopro anche la carica di membro del Comitato Direttivo (C.D.) e del Comitato Tecnico Scientifico (C.T.S.). Membro del Board of Directors **ISECOM** (Institute for Security and Open Methodologies), **TSTF** (Telecom Security Task Force) e del Capitolo Italiano di **OWASP** (Open Web Applications Security Project). Infine, sono membro dell'**ICANN** e consulente sul cybercrime alle Nazioni Unite per l'**UNICRI** (United Nations Interregional Crime and Justice Research Center), membro del PSG in ENISA.

mediaservice.net
CORPORATE SECURITY & IMAGE

Clusit
Associazione Italiana per la Sicurezza Informatica

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

TSTF.net
TELECOM SECURITY TASK FORCE

OWASP
The Open Web Application Security Project

ICANN

opsi aip

unicri
advancing security, serving justice, building peace

enisa
European Network and Information Security Agency

mediaservice.net
CORPORATE SECURITY & IMAGE

UNICRI

unicri
advancing security, serving justice, building peace

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
- Global Crimes Unit (Former "Counter Human Trafficking and Emerging Crimes Unit"): cyber crimes, counterfeiting, environmental crimes, trafficking in stolen works of art…

Fake Bvlgari &Rolex, b
&Cialis (aka SI

Water sys

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

mediaservice.net
CORPORATE SECURITY & IMAGE

UNICRI & Cybercrime

unicri
advancing security, serving justice, building peace

Overview dei progetti UNICRI contro il cybercrime

- Hackers Profiling Project (HPP)
- SCADA & sicurezza delle ICN (CNIs)
- Digital Forensics e tecniche di Computer Crimes Investigation
- Corsi ONU sulla Cybersecurity
- Digital Anti-paedophilia (with ITU: COP)
- Spam Analysis (economical model and organized crime, with ITU)

HACKERS PROFILING PROJECT

ITU International Telecommunication Union

mediaservice.net
CORPORATE SECURITY & IMAGE

unicri
advancing security, serving justice, building peace

What is ENISA?

- **E**uropean **N**etwork & **I**nformation **S**ecurity **A**gency
- ENISA is the **EU's response to security issues** of the European Union
- "Securing Europe's Information Society**"** is **our motto**
- In order to accomplish our mission, we work with EU Institutions and Member States
- ENISA came into being following the adoption of **Regulation (EC) No 460/2004** of the **European Parliament** and of the **Council** on **10 March 2004**. Operations started on **September 2005**, after moving from Brussels to Crete, and with the arrival of staff that were recruited through **EU27-wide competitions** with candidates coming from **all over Europe**.
- ENISA is helping the **European Commission**, the **Member States** and the **business community** to **address**, **respond** and especially to **prevent** Network and Information Security **problems**.
- The Agency also **assists the European Commission** in the technical preparatory work for **updating and developing Community legislation** in the field of Network and Information Security.
- I'm a Member of ENISA's PSG – **Permanent Stakeholders Group**.

mediaservice.net
CORPORATE SECURITY & IMAGE

Relazioni strategiche, per combattere il cybercrime

unicri
advancing security, serving justice, building peace

Nel corso degli anni siamo stati in grado di creare una rete di **relazioni speciali** e **contatti diretti** con le seguenti **organizzazioni**, all'interno di **aree di interesse e ricerca comuni**:

(this list is may not complete due to NDAs)

- **APWG – Anti Phishing Working Group (USA)**
- **AFP – Australian Federal Police**
- **ANZ-Australia/New Zealand Bank Association**
- **AUSCert (Australia)**
- **Brand Protect (Canada)**
- **CLUSIT**
- **CNNIC – China Internet Network Information Center (China)**
- **COE (Council of Europe, EU)**
- **CSIS (Center for Strategic and International Studies, WW)**
- **CYBEX (Spain)**
- **EUROPOL**
- **FBI Academy (Quantico, USA)**
- **FBI IC3, Cyber Division (Washington DC, USA)**
- **GCSC (Global Center for Securing Cyberspace, Canada)**
- **Google (WW)**
- **INTERPOL**
- **ISECOM (WW)**
- **ITU – International Communication Union (Switzerland)**
- **Immunity (USA)**
- **JP CERT (Japan)**
- **KPMG (EU)**
- **McAfee (WW)**
- **ESET (WW)**
- **LPI Canada**
- **@ Mediaservice.net**
- **Microsoft (WW)**
- **MyCERT (Malaysia)**
- **NAUSS (Naif Arab University for Security Sciences, Saudi Arabia)**
- **NCIS (USA)**
- **OpenBSD Development Team**
- **OpenCERT (WW)**
- **PayPal (USA)**
- **Polish Police Academy (PL)**
- **@ PSS**
- **RACVIAC SE (Croatia)**
- **RSA (USA)**
- **Team CYMRU (WW)**
- **Trend-Micro (WW)**
- **Verisign (WW)**

mediaservice.net
CORPORATE SECURITY & IMAGE

Hacking,
ieri ed oggi

Hacking: ieri

Il crimine, nel passato (crime)

"**Ogni nuova forma di tecnologia,**
apre la strada a nuove forme di criminalità".

- Il rapporto tra **tecnologia e criminalità** è stato, da sempre, caratterizzato da una sorta di "gara" tra buoni e cattivi.
- Per esempio, agli inizi del '900, con l'avvento dell'**automobile**, i "cattivi" iniziarono a **rubarle**.
- ….la polizia, per contrastare il fenomeno, definì l'**adozione obbligatoria** delle targhe (car plates)…
- ….ed i ladri iniziarono a **rubare le targhe** delle auto (o a falsificarle).

Il crimine, oggi

unicri
advancing security, serving justice, building peace

(Cyber)crime

- Le automobili sono state sostituite dalle informazioni.

Hai l'informazione, hai il potere.

(Quantomeno, nella **politica**, nel **mondo del business**, nelle **relazioni personali…**)

- Questo, semplicemente perché l'informazione è immediatamente trasformabile in:

1. **Vantaggio competitivo**
2. **Informazione sensibile/critica**
3. **Denaro**
4. **Ricatto**

- Esempi ? (…imbarazzo della scelta ;)
  - **Regione Lazio**
  - **Calciopoli**
  - **Scandalo Telecom Italia**
  - **Attacco Vodafone Grecia**
  - **Vittorio Emanuele di Savoia**
  - **Vallettopoli + Scandalo Escorts**
  - **Corona**
  - **McLaren/Ferrari**
  - **…….**

mediaservice.net
CORPORATE SECURITY & IMAGE

Le date storiche

Le Ere dell'hacking…

unicri
advancing security, serving justice, building peace

I

- '60 Hacking Roots: MIT & TMRC
- '70 Phone Phreaking and Captain Crunch (Wozniak & Jobbs)

II

- '80: Hacking Message Boards and Hacking Groups
- 1983: War Games, Kids Games
- 1984: Ezines-> Phrack & 2600 The Hacker's Quarterly
- 1986: Use a computer, go to Jail (CFAA: Computer Fraud & Abuse Act)
- 1988: RTM: Internet is NOT secure (?) / The WANK Worm
- 1989: CCC & KGB (Spy Game ?)
- 15 JAN 1990: the Big Black Out (AT&T Intl. Phone System Crash, MOD& LOD)

III

- 1990: Operation Sundevil (The Hacker's Crackdown)
- 1993: Buy a car or hack one ? -> Kevin Poulsen and the L.A. gangs

IV

- 1994: Hacking tools
- 1994: (Italia) Italian Crackdown (FidoBust)
- 1995: K.D. Mitnick & Tsutomu Shimomura ("IP Spoofing is not practically applicable")
- 1998: CdC & Back Orifice / Gulf War & Israeli Connection (The Analyzer)
- 1999: Steal money, get died (China)
- 2000: Yahoo, Amazon, Ebay DDoS Attacks: International Hacking Scene says NO

…e le loro generazioni

- 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 "bucandoli"; più tardi, verso la seconda metà degli anni '80, il fenomeno unisce fattori di **moda e 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 le BBS.
- La quarta (2000) è mossa dalla rabbia e dal denaro: 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 (**cyber-hacktivism**) e soprattutto alla criminalità (**cybercrime**).

€, $

Cybercrime: perché?

- Il cybercrime, in tutti i suoi molteplici aspetti, può essere ritenuto il business criminale più in ascesa del momento e con i più elevati margini di futura diffusione?
- Se siamo tutti qua oggi, direi che siamo sulla buona strada per analizzare questa problematica…
- La diffusione dei crimini perpetuati attraverso la rete si basa però su una serie di fattori.
- Analizziamoli insieme.

Motivazioni/1

- 1. Il numero sempre crescente di *navigatori novizi*, quindi l'**aumento delle potenziali vittime** o vettori → **W la banda larga…**
- 2. Il crescente bisogno di **far soldi** "in qualche modo e subito" → **C'è crisi…**
- 3. La diffusione del know-how tecnico, anche di livello medio-alto, **preconfezionato** → **0-days**

Motivazioni/2

- 4. L'**estrema facilità** con cui è possibile formare gruppi e reclutare nuovi adepti da plasmare secondo le **proprie esigenze** → **Newbies, Script Kiddies**
- 5. La radicata illusione di **non poter essere scoperti** → **Psicologia, Criminologia**
- 6. L'**assenza di atti violenti** → **Psicologia e Sociologia**

Il progetto HPP: Hackers Profiling Project

Profiling

- Tutto quanto vi abbiamo mostrato sino ad ora, ha fatto sì che i profili degli attori "classici" non fossero sempre applicabili al "mondo virtuale".

- Inoltre, profili **decisamente diversi** hanno iniziato **dialoghi** (che ne pensi di…?), **scambio di informazioni** (io ti dico di X, tu mi dici di Y ?), **mercato nero** (0-day), **ingaggi** (hacking su commissione).

Che cosa è cambiato ?

- Quello che è cambiato è la **tipologia di attaccante**.

- Da "*ragazzini annoiati*", che lo facevano per "*hobby e curiosità*" (rigorosamente alla notte, con la pizza nell'angolo e la lattina di Red Bull)….

- ...a ragazzini, adolescenti ed adulti, non necessariamente di impronta "ICT" né tantomeno "hacker" che, semplicemente, lo **fanno per denaro**.

- E' dunque cambiato il **profilo dell'attaccante** ed, ovviamente, sono cambiate le loro **motivazioni**.

Understanding Hackers

- E' ***tremendamente importante*** che noi comprendiamo i c.d. computer hackers
  - **Non limitiamoci** agli attacchi ed alle tecniche di intrusione, ma analizziamone anche il **comportamento sociale**
- Identifichiamo le **regole non scritte** della subcultura hacker
- Esploriamo l'**organizzazione sociale** degli hackers
- Approfondiamo i **legami esistenti** tra hacking e criminalità

unicri
advancing security, serving justice, building peace

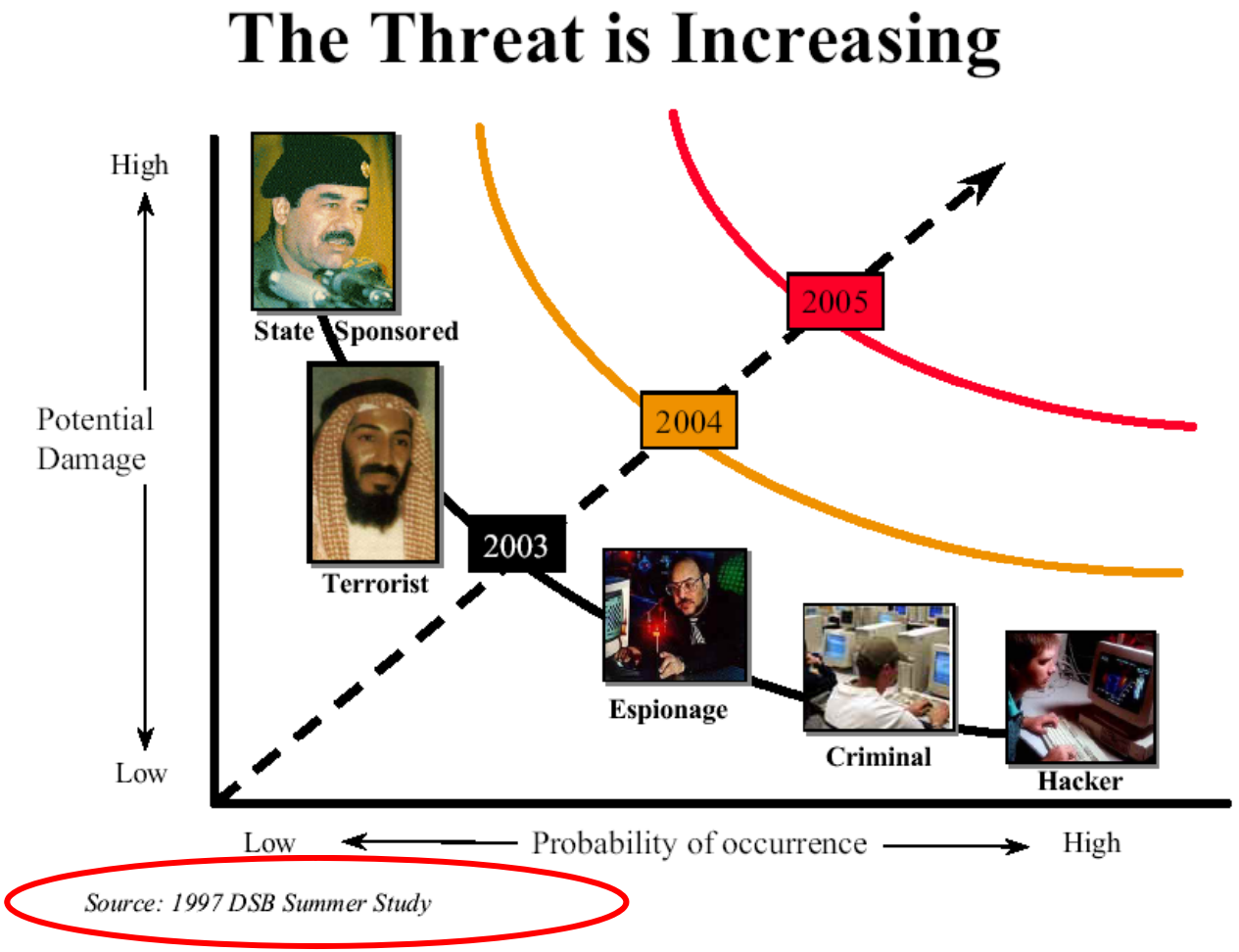
Profiling the Enemy: problematiche

- Le classiche metodologie di criminal profiling spesso **non sono** applicabili al "mondo virtuale" (e.g. "geographical profiling").
- Esistono poi differenti problematiche di tipo **tecnologico**, **etico** e **legislativo**.
- Infine, quanto sopra va applicato ad un "nemico **sconosciuto**", che **evolve rapidamente** (insieme alla tecnologia): una **minaccia non statica**.
- Ecco perché **non è sempre possibile** applicare i profili dei "classici attori del crimine" al mondo del cybercrime.
- ***"Infine, profili molto differenti l'uno dall'altro hanno iniziato a dialogare (cosa pensi di questo…?), a scambiarsi informazioni (io ti dico di X, tu dimmi di Y), ad operare nel mercato nero (0-day), ad accettare ingaggi (hacking su commissione)."***

mediaservice.net
CORPORATE SECURITY & IMAGE

Uno studio

Nuovi attori, nuovi collegamenti ☹



Torniamo all'hacking...

unicri
advancing security, serving justice, building peace

"Hackers"

Il termine hacker è stato lungamente abusato sin dagli anni '80; dagli anni '90, i media lo hanno utilizzato per giustificare qualunque tipologia di "IT Crime", da un banale attacco di phishing sino ad azioni di DDoS devastanti.

"Lamers", script-kiddies, spie industriali, hacker per hobby... Per le masse, sono tutti uguali. Ma non è così....anzi!

Da un punto di vista professionale, le aziende non hanno ancora capito "di chi hanno paura". Per loro, sono semplicemente, tutti quanti, "hackers".

mediaservice.net
CORPORATE SECURITY & IMAGE

Hackers

unicri
advancing security, serving justice, building peace

Macro-tipologie di attaccanti

- **Low-level hackers: “script-kiddies” per vulnerabilità pubbliche note e/o specifiche**
  - ✓ (kind of “NEW”) Phishing, Remote low-level Social Engineering Attacks
  - ✓ Insiders (user/supervisor/admin)
  - ✓ Disgruntled Employees
- **High-level, sophisticated hackers, Organized Crime: attacchi a medio ed alto livello**
  - ✓ Hobbyist hackers
  - ✓ Unethical “security guys” (Telecom Italia and Vodafone Greece scandals)
  - ✓ Unstructured attackers (SCAMs, medium & high-level hi-tech frauds,VISHING …)
  - ✓ Structured attackers (“the italian job”, targeted attacks)
- **Spionaggio Industriale, Terrorismo**
  - ✓ Foreign Espionage
  - ✓ Hacktivist (unfunded groups)
  - ✓ Terrorist groups (funded groups)
  - ✓ State sponsored attacks

mediaservice.net
CORPORATE SECURITY & IMAGE

The Hackers Profiling Project (HPP)

unicri
advancing security, serving justice, building peace

Obiettivo di HPP

Analizzare il fenomeno hacking nei suoi svariati aspetti (tecnologico, sociale, economico), attraverso approcci tecnici e criminologici.

Comprendere le differenti motivazioni ed identificare gli attori chiamati in causa.

Osservare "sul campo" le vere azioni criminose.

Applicare la metodologia di profiling ai dati raccolti (4W: *who, where, when, why*)

Acquisire e disseminare la conoscenza. A tutti. *Gratuitamente*, con un *modello aperto* (GNU/FDL)

mediaservice.net
CORPORATE SECURITY & IMAGE

The Hackers Profiling Project (HPP)

unicri
advancing security, serving justice, building peace

Fasi progettuali – inizio: Settembre 2004

1 – Theoretical collection:
Questionnaires (10 languages)

2 – Observation:
Participation in IT underground security events, worldwide

3 - Filing:
Database for elaboration/classification of data gathered from phases 1 and 4

4 - Live collection:
Highly customized, "NG" Honeynet systems

5 – Gap analysis:
of data gathered from questionnaire, NG honeynets, 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

mediaservice.net
CORPORATE SECURITY & IMAGE

The Hackers Profiling Project (HPP)

unicri
advancing security, serving justice, building peace

Total received questionnaires: #1200

Full questionnaires filled out - #500*

Compact questionnaires filled out - #573*

***since September 2006**

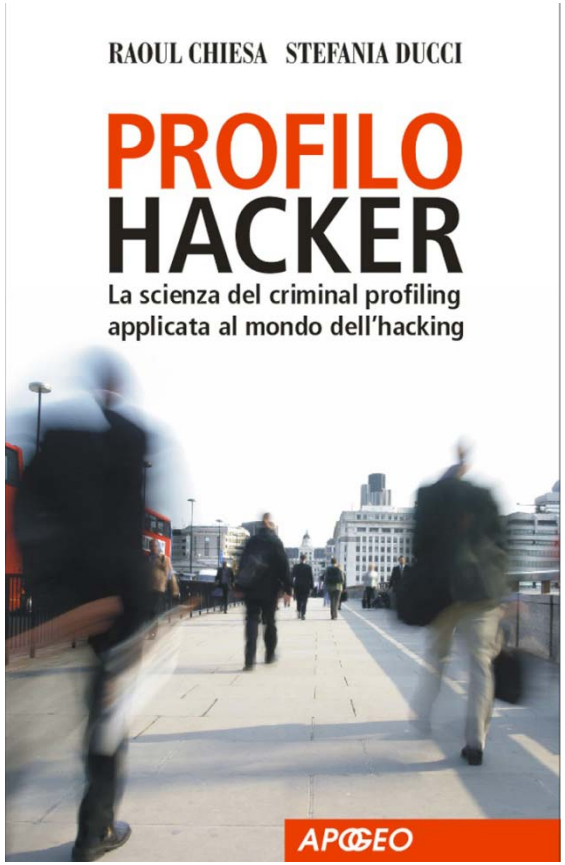
Mainly from:
USA
Italy
UK
Canada
Lithuania
Australia
Malaysia
Germany
Brazil
Romania
China

mediaservice.net
CORPORATE SECURITY & IMAGE

The Hackers Profiling Project (HPP)

unicri
advancing security, serving justice, building peace

Profiling Hackers – il libro/1



Content

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

Who is it for?

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

mediaservice.net
CORPORATE SECURITY & IMAGE

The Hackers Profiling Project (HPP)

unicri
advancing security, serving justice, building peace

Profiling Hackers – il libro/2

Contents

mediaservice.net
CORPORATE SECURITY & IMAGE

The Hackers Profiling Project (HPP)

unicri
advancing security, serving justice, building peace

Dettaglio e correlazione dei profili – Tabella #1

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

mediaservice.net
CORPORATE SECURITY & IMAGE

The Hackers Profiling Project (HPP)

unicri
advancing security, serving justice, building peace

Dettaglio e correlazione dei profili – Tabella #2

PROFILE	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

mediaservice.net
CORPORATE SECURITY & IMAGE

The Hackers Profiling Project (HPP)

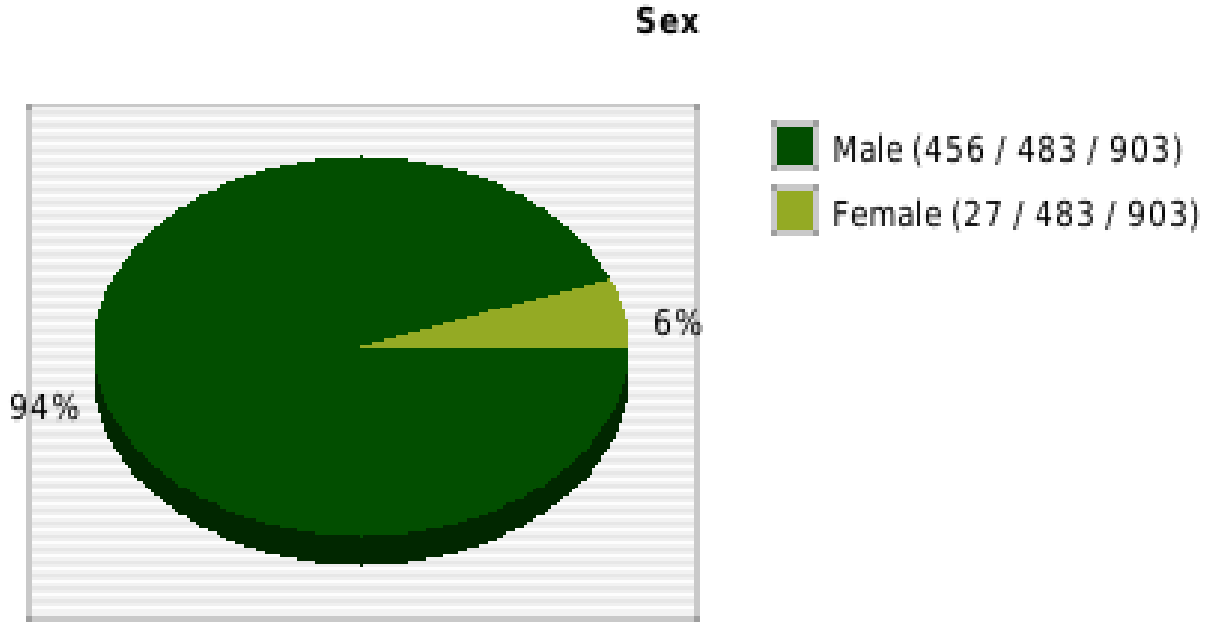
unicri
advancing security, serving justice, building peace

Dettaglio e correlazione dei profili – Tabella #3

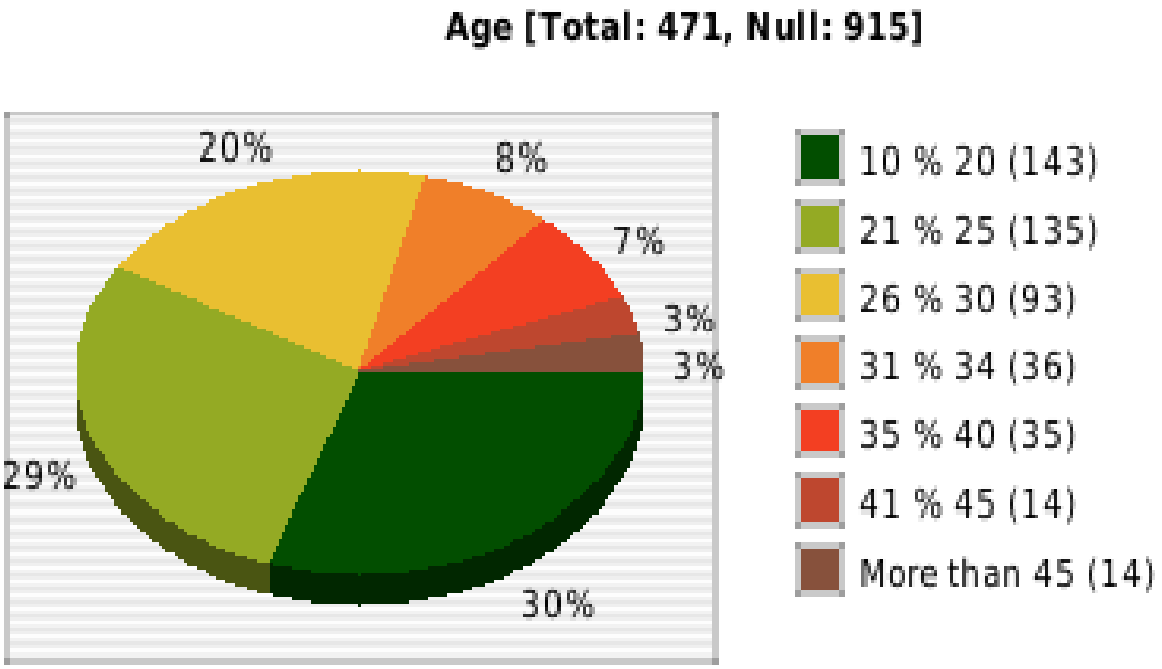
DETERRENCE EFFECT OF:	LAWS	CONVICTIONS SUFFERED BY OTHER HACKERS	CONVICTIONS SUFFERED BY THEM	TECHNICAL DIFFICULTIES
Wanna Be Lamer	NULL	NULL	ALMOST NULL	HIGH
Script Kiddie	NULL	NULL	HIGH: they stop after the 1st conviction	HIGH
Cracker	NULL	NULL	NULL	MEDIUM
Ethical Hacker	NULL	NULL	HIGH: they stop after 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

mediaservice.net
CORPORATE SECURITY & IMAGE

The Hackers Profiling Project (HPP)



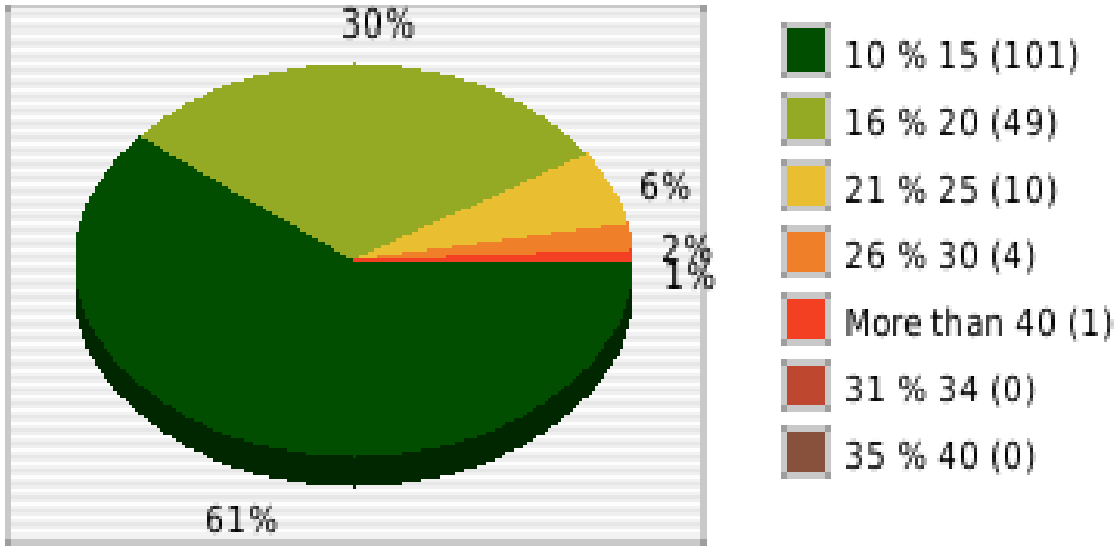
The Hackers Profiling Project (HPP)



The Hackers Profiling Project (HPP)

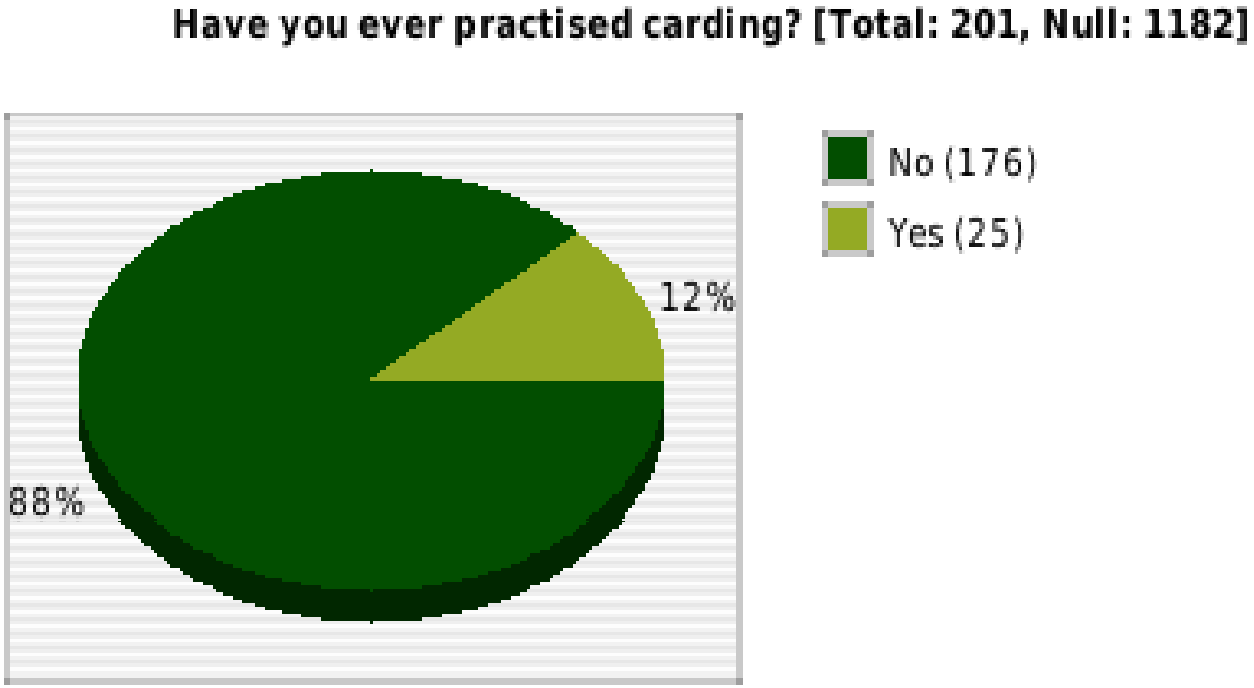
unicri
advancing security, serving justice, building peace

Age that you started with hacking [Total: 171, Null: 1212]

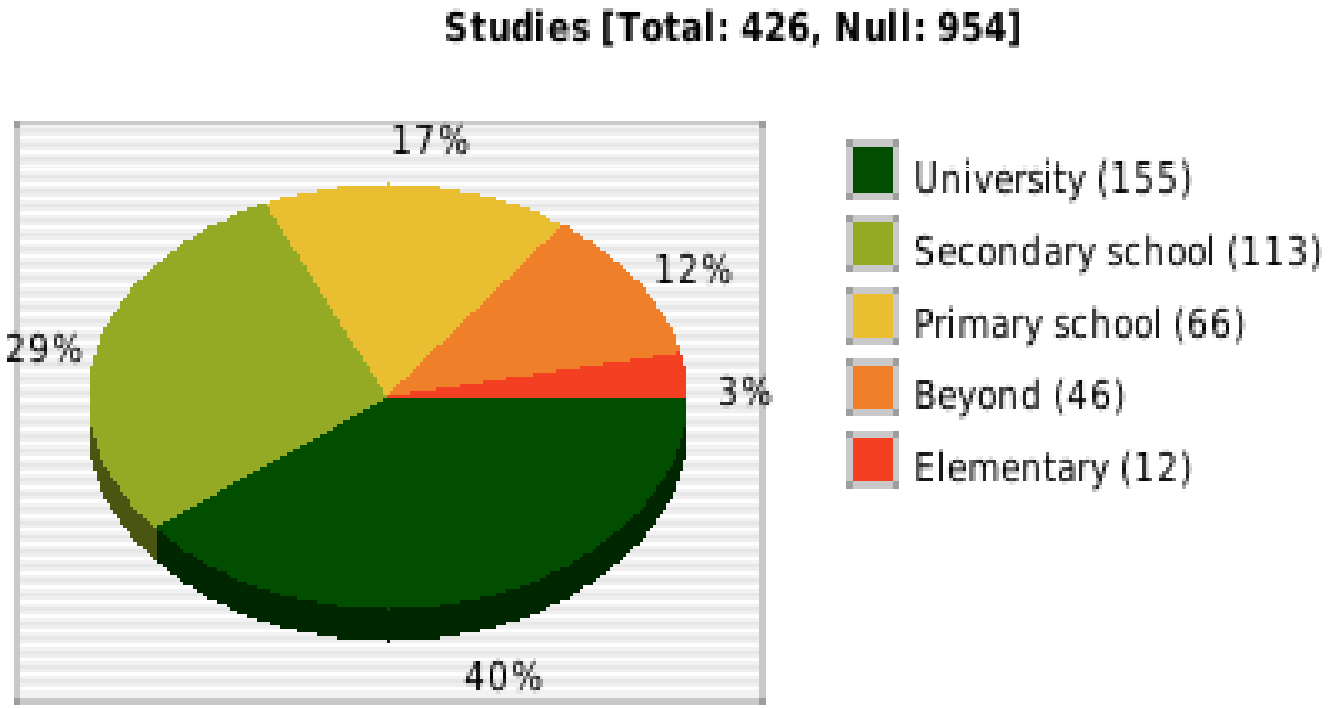


mediaservice.net
CORPORATE SECURITY & IMAGE

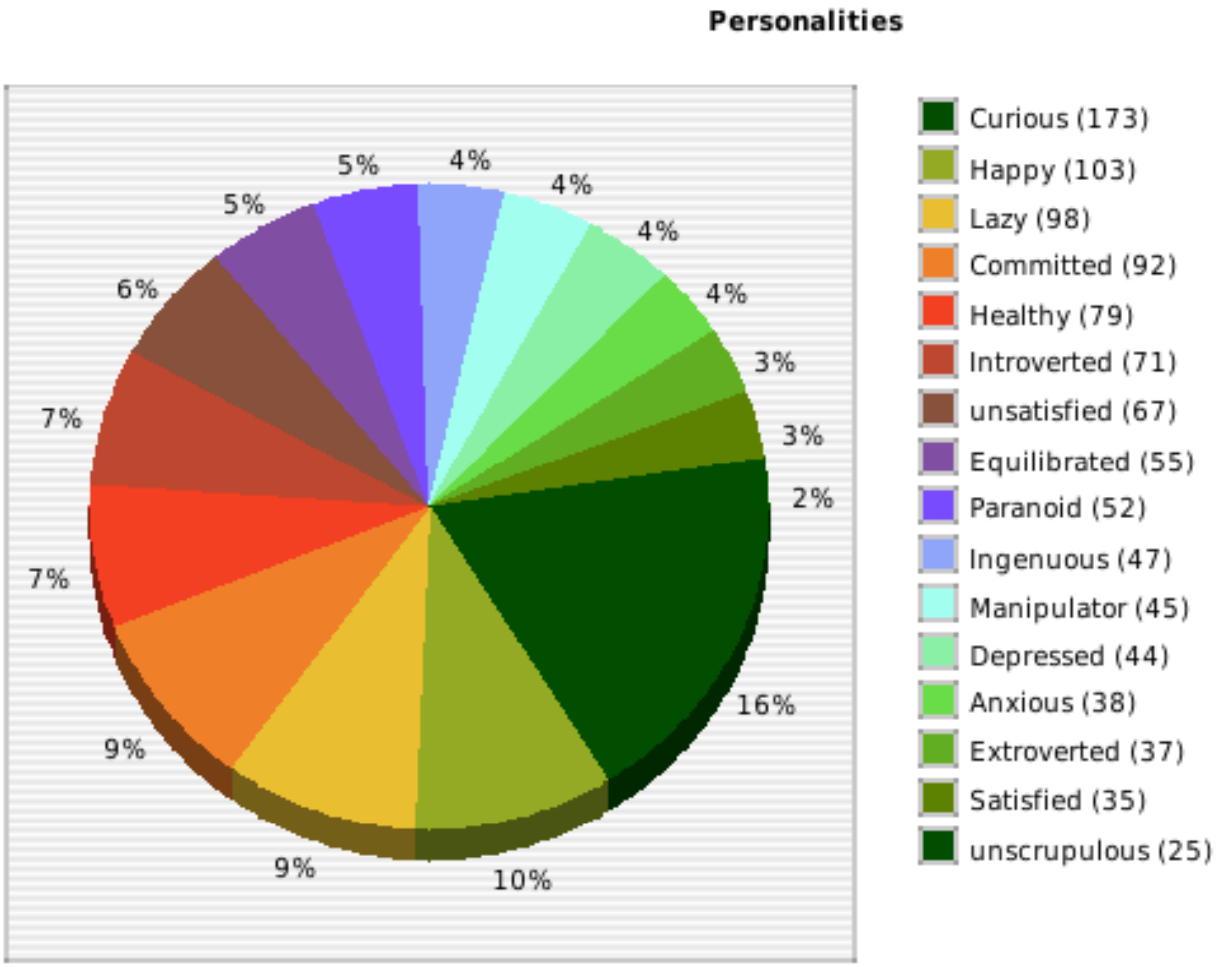
The Hackers Profiling Project (HPP)



The Hackers Profiling Project (HPP)



The Hackers Profiling Project (HPP)



L'hacking, oggi

unicri
advancing security, serving justice, building peace

Cifre

- **285 milioni di record** compromessi nel 2008 (fonte: Verizon 2009 Data Breach Investigations Report)
- **2 miliardi di dollari**: il fatturato 2008 di *RBN*
- **+148% di incremento nelle truffe ai bancomat**: giro di **500 milioni di euro all'anno**, solo in Europa. (fonte: ENISA "ATM Crime Report 2009")
- **.....**

- Uh ?!? **RBN** ? Cos'è ??

mediaservice.net
CORPORATE SECURITY & IMAGE

RBN

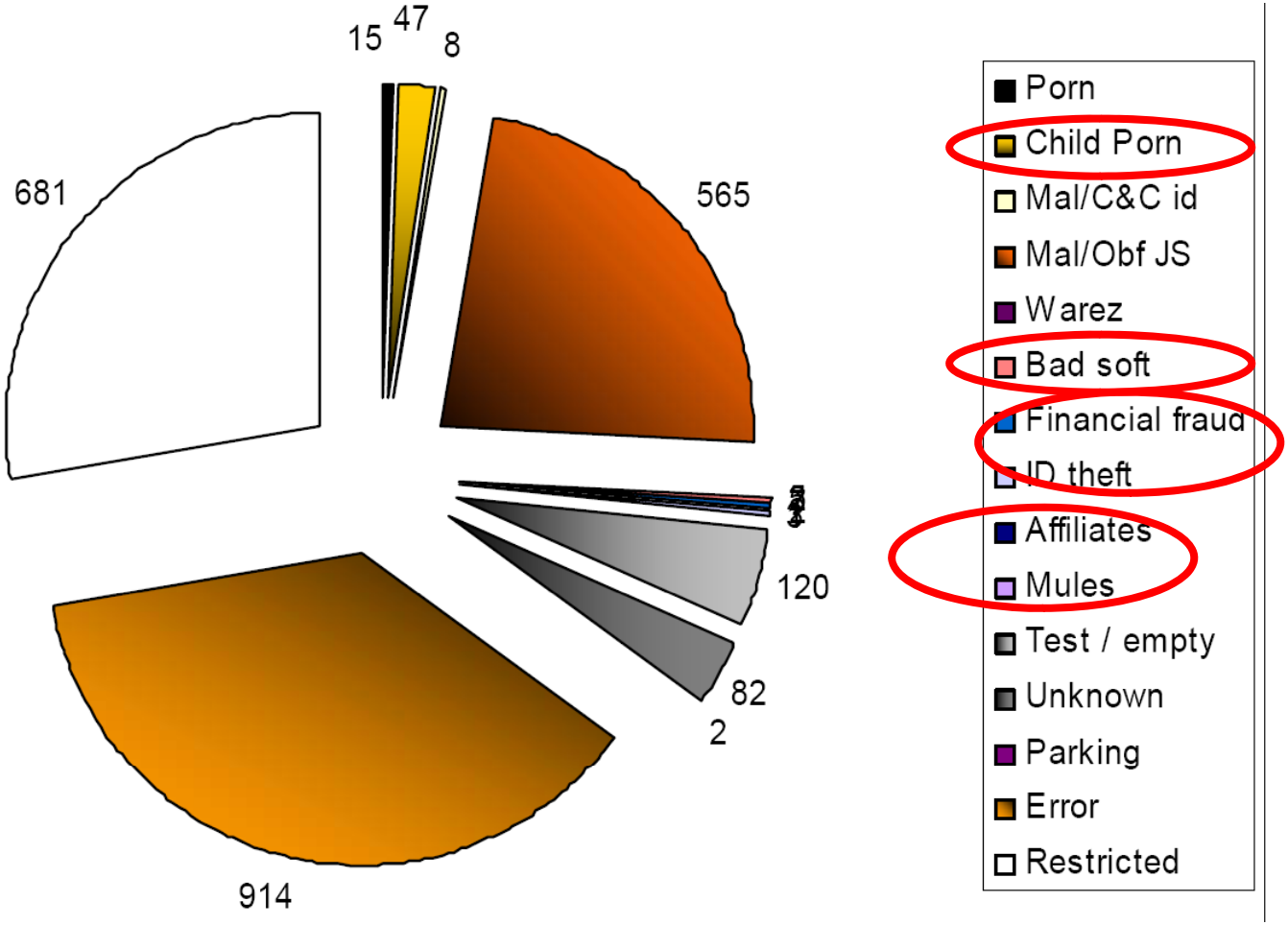
- Acronimo di **Russian Business Network**
- E' difficile spiegare **che cos'è**...
- Innanzitutto, **identifichiamo** come si **traduce materialmente** il cybercrime:
  - ✓ **Phishing**
  - ✓ **Malware**
  - ✓ **Frodi** (scams)
  - ✓ **Attacchi DDoS**
  - ✓ **Pornografia minorile ed infantile**
  - ✓ **Porno generico**
  - ✓ **Giochi on-line**

RBN & il phishing

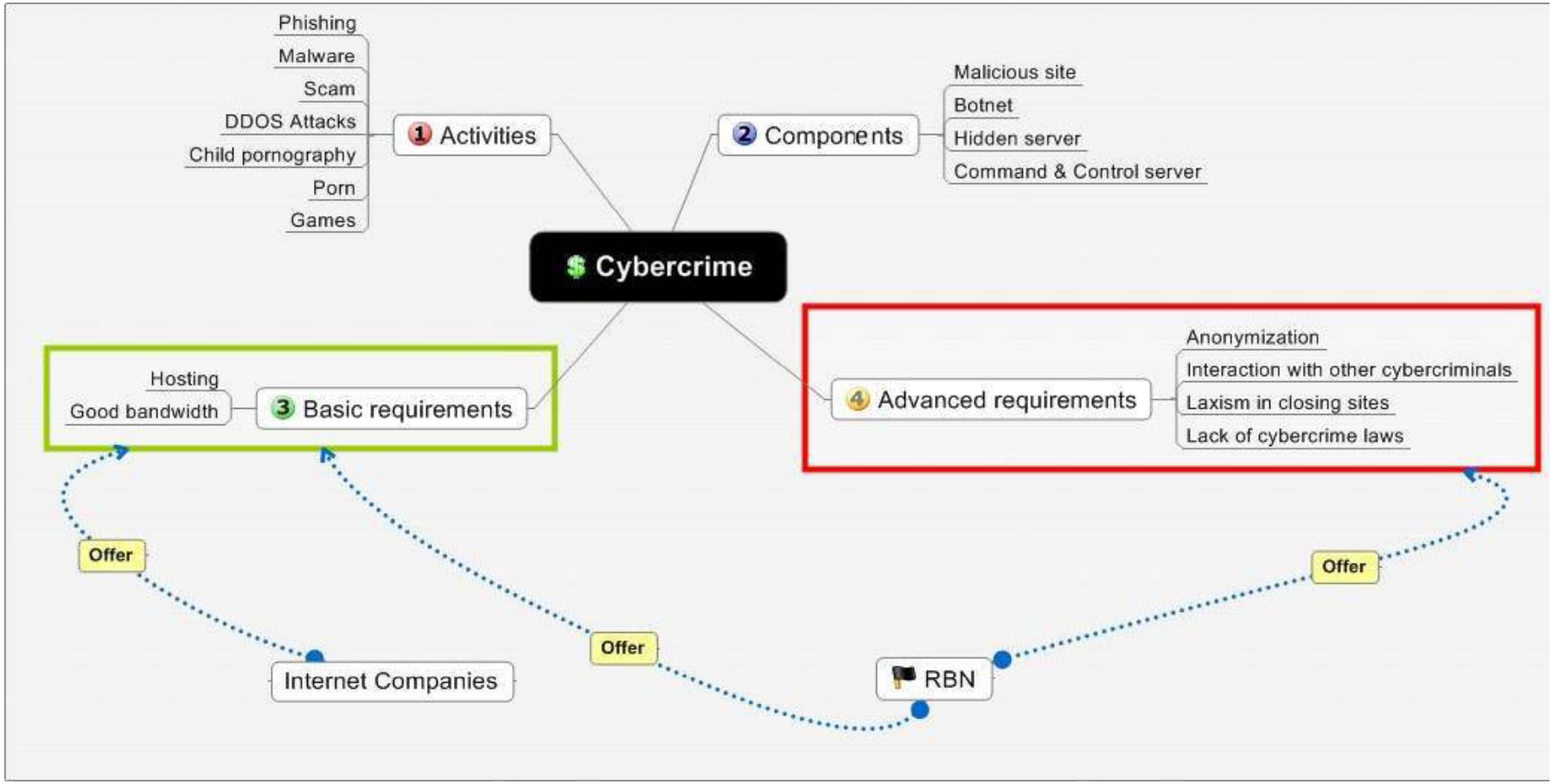
- Un giorno David Bizeul ha preso un IP a caso di RBN. E' arrivata questa pagina da: **http://194.146.207.18/config**

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

Cosa c'era sugli altri IP?



RBN nei fatti...



Underground Economy

“Cybercriminals”

UE

- L'Underground Economy è il concetto per il quale, nel **prossimo futuro, non si faranno più** "rapine in banca".
- Oggigiorno, i mezzi per **frodare** e **rubare** denaro sono **molteplici**. E gli **utenti inesperti** sono tanti.
- Ciò che serve è "pulire" il denaro. Servono i **muli**.
- E' in questo senso che **ci si sta dirigendo**. E la **crisi economica** non è certo di aiuto...

UE: l'approccio

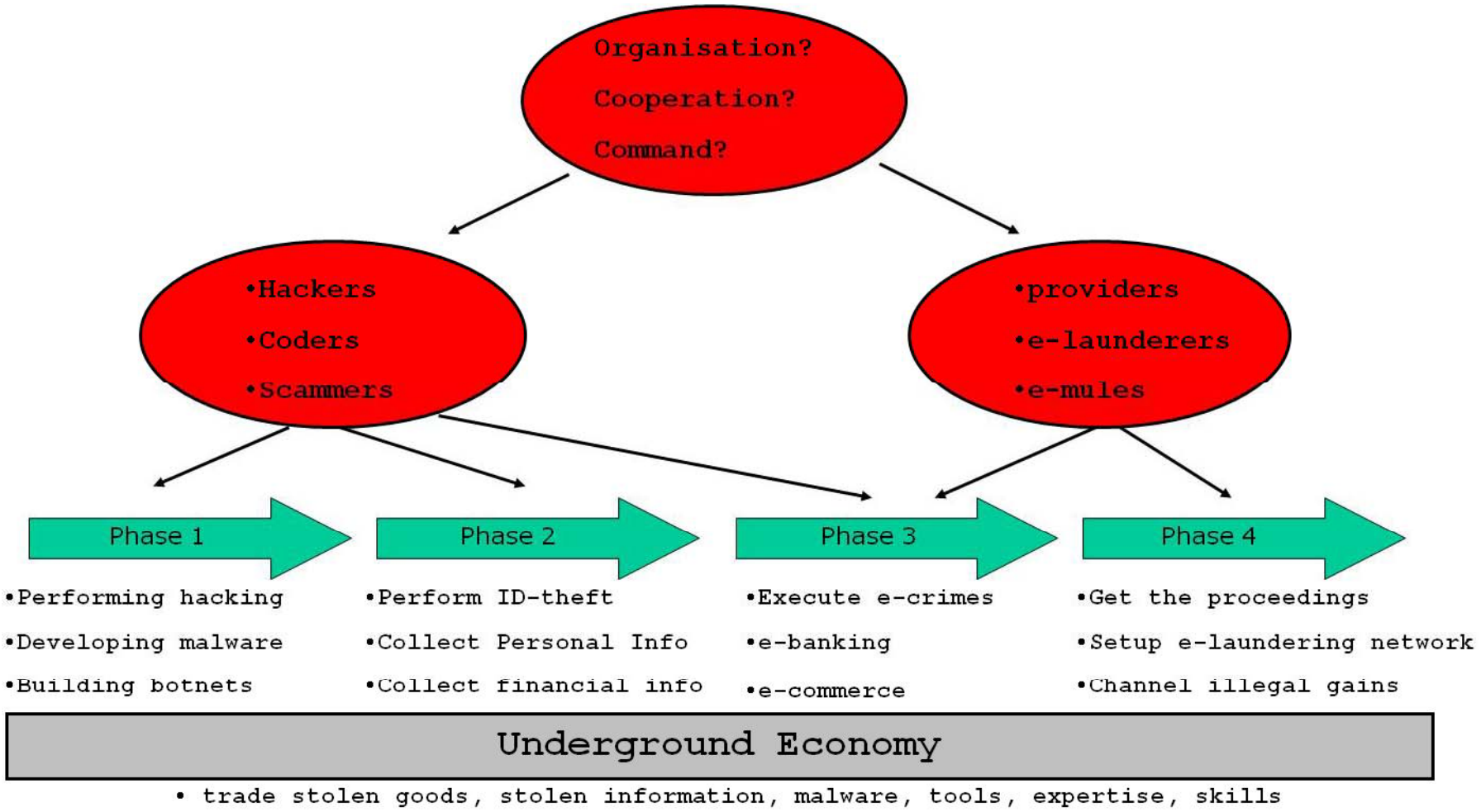
1. **La base: Malware e Botnet**
   Creare il malware, costruire le botnet

2. **Furto di Identità** (Identity theft)
   Furto di credenziali personali e finanziare (e-banking)

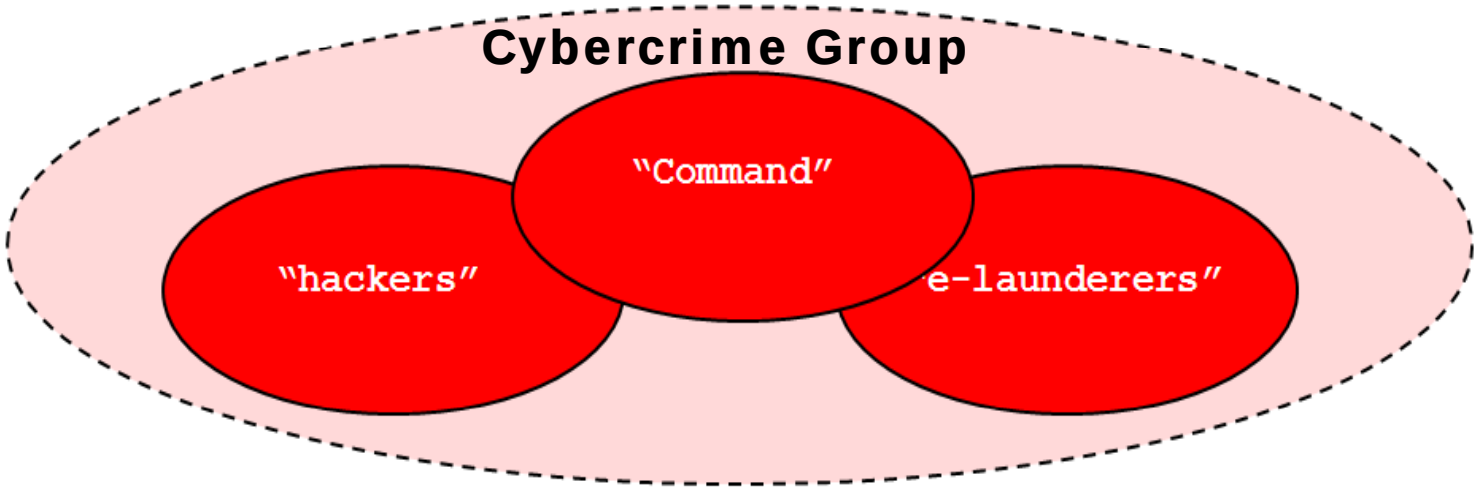
3. **Esecuzione dell'e-crime**
   Esempio: attacchi e-Banking e frodi/truffe e-commerce (Ebay docet)

4. **Riciclaggio di denaro** (Money laundering)
   Setup dei network di money laundering

UE Business Model



UE Cooperation Model



Phase 1	Phase 2	Phase 3	Phase 4
•Performing hacking	•Perform ID-theft	•Execute e-crimes	•Get the proceedings
•Developing malware	•Collect Personal Info	•e-banking	•Setup e-laundering network
•Building botnets	•Collect financial info	•e-commerce	•Channel illegal gains

Underground Economy

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

Chi c’è dietro ?

mediaservice.net
CORPORATE SECURITY & IMAGE

Chi c’è dietro ?

unicri
advancing security, serving justice, building peace

NON DISPONIBILE NELLA VERSIONE PUBBLICA

mediaservice.net
CORPORATE SECURITY & IMAGE

Chi c’è dietro ?

unicri
advancing security, serving justice, building peace

NON DISPONIBILE NELLA VERSIONE PUBBLICA

mediaservice.net
CORPORATE SECURITY & IMAGE

Chi c’è dietro ?

unicri
advancing security, serving justice, building peace

NON DISPONIBILE NELLA VERSIONE PUBBLICA

mediaservice.net
CORPORATE SECURITY & IMAGE

Banner “pubblicitari” (!)

unicri
advancing security, serving justice, building peace

NON DISPONIBILE NELLA VERSIONE PUBBLICA

mediaservice.net
CORPORATE SECURITY & IMAGE

Chi c’è dietro ?

unicri
advancing security, serving justice, building peace

NON DISPONIBILE NELLA VERSIONE PUBBLICA

mediaservice.net
CORPORATE SECURITY & IMAGE

Early Arrests

unicri
advancing security, serving justice, building peace

Markus Kellerer aka Matrix001

& Five Others, May 2007-Oct. 2007 Germany

Co-Founder

mediaservice.net
CORPORATE SECURITY & IMAGE

Renu Subramaniam aka JiLsi

July 2007

United Kingdom

Founder

Early Arrests

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

mediaservice.net
CORPORATE SECURITY & IMAGE

unicri
advancing security, serving justice, building peace

PCWorld

Search PC World

Home | News | Hardware Reviews | Software Reviews | How-To | Videos | Downloads

Magazine
Subscribe & Get a Bonus CD
Customer Service

2007 BACK TO SCHOOL GUIDE

- Audio & Video
- Business Center
- Cameras
- Cell Phones & PDAs
- Communications
- Components & Upgrading
- Desktop PCs
- DVD & Hard Drives
- Gaming Hardware & Software
- HDTV
- Laptops
- Macs & iPods
- Monitors
- Printers
- Spyware & Security
- The PCW Test Center
- Windows Vista & XP

Resource Centers
- DLP® HDTV Showroom
- HP All-in-one Printers
- Lenovo Laptop Showcase
- Lexmark WiFi Printers

Read More About: Hackers • Online Security • Cybercrime

'Iceman' Hacker Charged in Credit Card Theft

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

Gregg Keizer, Computerworld
Wednesday, September 12, 2007 9:00 AM PDT

PRINT E-MAIL COMMENT RSS
SLASHDOT IT DIGG THIS DEL.ICIO.US NEWSVINE

Recommend this story? Yes 20 Votes No 1 Votes

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

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

Early Arrests

unicri
advancing security, serving justice, building peace

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

WIRED BLOG NETWORK

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

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

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

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

mediaservice.net
CORPORATE SECURITY & IMAGE

Early Arrests

Turkish Police Arrest Alleged ATM Hacker-Kidnapper

By Ryan Singel | September 10, 2008 | 7:46:00 PM | Categories: Hacks And Cracks

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

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

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

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

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

Chi c’è dietro ?

unicri
advancing security, serving justice, building peace

NON DISPONIBILE NELLA VERSIONE PUBBLICA

mediaservice.net
CORPORATE SECURITY & IMAGE

Chi c’è dietro ?

unicri
advancing security, serving justice, building peace

NON DISPONIBILE NELLA VERSIONE PUBBLICA

mediaservice.net
CORPORATE SECURITY & IMAGE

Chi c’è dietro ?

unicri
advancing security, serving justice, building peace

NON DISPONIBILE NELLA VERSIONE PUBBLICA

mediaservice.net
CORPORATE SECURITY & IMAGE

Chi c’è dietro ?

NON DISPONIBILE NELLA VERSIONE PUBBLICA

Le feste per “i dealer”

unicri
advancing security, serving justice, building peace

NON DISPONIBILE NELLA VERSIONE PUBBLICA

mediaservice.net
CORPORATE SECURITY & IMAGE

Girls, money, cars..

unicri
advancing security, serving justice, building peace

NON DISPONIBILE NELLA VERSIONE PUBBLICA

mediaservice.net
CORPORATE SECURITY & IMAGE

Girls, money, cars..

unicri
advancing security, serving justice, building peace

NON DISPONIBILE NELLA VERSIONE PUBBLICA

mediaservice.net
CORPORATE SECURITY & IMAGE

This is the end,my friends

unicri
advancing security, serving justice, building peace

Conclusioni

- Il mondo dell' hacking **non è sempre stato legato** ad azioni criminali;
- Ciò nonostante, l'hacking oggi si sta muovendo (**trasformando?**) verso la **criminalità**, organizzata o "fatta in casa".
- Le ricerche portate avanti sino ad oggi **non hanno propriamente fotografato** un fenomeno così **complesso**, **gerarchico** ed in continua evoluzione come quello del mondo underground;
- L'applicazione di una metodologia di profiling **è possibile**, a patto che venga effettuata un'**analisi a 360°** del fenomeno, con **differenti punti di vista**: **Tecnologico, Sociale, Psicologico e Criminologico**;
- Il problema del Cybercrime e dell'Underground Economy **non è** "una questione per tecnici": è un **problema di TUTTI**, e l'**impatto sul Sistema-Paese** può essere **devastante**.
- **What's next?** *Automotive hacking*, attacchi **mirati** ad *infrastrutture critiche*, *satellite hacking*, *SS7 fuzzying*, *0-days&black market*, *mobile malware*, *frodi ATM* .

mediaservice.net
CORPORATE SECURITY & IMAGE

Per chi vuole saperne di più

Bibliografia e Referenze (1)

Questionari **H.P.P., 2005-2010**

Fatal System Error: the Hunt for the new Crime Lords who are bringing down the Internet, Joseph Menn, Public Affairs, 2010

Stealing the Network: How to 0wn a Continent, (an Identity), **(a Shadow)** (V.A.), Syngress Publishing, 2004, 2006, 2007

Stealing the Network: How to 0wn the Box, (V.A.), Syngress Publishing, 2003

Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier, Suelette Dreyfus, Random House Australia, 1997

The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, Clifford Stoll, DoubleDay (1989), Pocket (2000)

Masters of Deception: the Gang that Ruled Cyberspace, Michelle Stalalla & Joshua Quinttner, Harpercollins, 1995

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

Takedown, John Markoff and Tsutomu Shimomura, Sperling & Kupfler, (Hyperion Books), 1996

The Fugitive Game: online with Kevin Mitnick, Jonathan Littman, Little & Brown, 1997

The Art of Deception, Kevin D. Mitnick & William L. Simon, Wiley, 2002

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

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

Per chi vuole saperne di più

Bibliografia e Referenze (2)

The Estonia attack: Battling Botnets and online Mobs, Gadi Evron, 2008 (white paper)

Who is "n3td3v"?, by Hacker Factor Solutions, 2006 (white paper)

Mafiaboy: How I cracked the Internet and Why it's still broken, Michael Calce with Craig Silverman, 2008

The Hacker Diaries: Confessions of Teenage Hackers, Dan Verton, McGraw-Hill Osborne Media, 2002

Cyberpunk: Outlaws and Hackers on the Computer Frontier, Katie Hafner, Simon & Schuster, 1995

Cyber Adversary Characterization: auditing the hacker mind, Tom Parker, Syngress, 2004

Inside the SPAM Cartel: trade secrets from the Dark Side, by Spammer X, Syngress, 2004

Hacker Cracker, Ejovu Nuwere with David Chanoff, Harper Collins, 2002

Compendio di criminologia, Ponti G., Raffaello Cortina, 1991

Criminalità da computer, Tiedemann K., in Trattato di criminologia, medicina criminologica e psichiatria forense, vol.X, Il cambiamento delle forme di criminalità e devianza, Ferracuti F. (a cura di), Giuffrè, 1988

United Nations Manual on the Prevention and Control of Computer-related Crime, in International Review of Criminal Policy – Nos. 43 and 44

Criminal Profiling: dall'analisi della scena del delitto al profilo psicologico del criminale, Massimo Picozzi, Angelo Zappalà, McGraw Hill, 2001

Deductive Criminal Profiling: Comparing Applied Methodologies Between Inductive and Deductive Criminal Profiling Techniques, Turvey B., Knowledge Solutions Library, January, 1998

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

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

Domande?

unicri
advancing security, serving justice, building peace

Contatti, Q&A

Raoul Chiesa

E-mail: chiesa@UNICRI.it

Sito ufficiale di HPP :
http://www.isecom.org/hpp

Questionari HPP:
http://hpp.recursiva.org

http://www.unicri.it

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

Grazie per l'attenzione!

mediaservice.net
CORPORATE SECURITY & IMAGE