



Italian Black Hats Speech

(INFOSECURITY ITALIA 2002)

Italian Black Hats Association

<http://www.blackhats.it>

Seminario Tecnico:

Presentazione della giornata

Milano, 24/1/2002, Sala Cadamosto

Copyright

Questo insieme di trasparenze è protetto dalle leggi sul copyright e dalle disposizioni dei trattati internazionali.

Il titolo ed i copyright relative alle trasparenze (ivi inclusi, ma non limitatamente a, ogni immagine, fotografia, animazione, video e testo) sono di proprietà degli autori indicati.

Le trasparenze possono essere riprodotte ed utilizzate liberamente dagli istituti di ricerca, scolastici ed universitari afferenti al Ministero della Pubblica Istruzione per scopi istituzionali, non a fine di lucro.

Ogni altro utilizzo o riproduzione (ivi incluse, ma non limitatamente a, le riproduzioni a mezzo stampa, su supporti magnetici o su reti di calcolatori) in toto o in parte è vietata, se non esplicitamente autorizzata per iscritto, a priori, da parte dell'autore.

L'informazione contenuta in queste trasparenze è ritenuta essere accurata alla data della pubblicazione. Essa è fornita per scopi meramente didattici e non per essere utilizzata in progetti di impianti, prodotti, ecc.

L'informazione contenuta in queste trasparenze è soggetta a cambiamenti senza preavviso. Gli autori non si assumono alcuna responsabilità per il contenuto di queste trasparenze (ivi incluse, ma non limitatamente a, la correttezza, completezza, applicabilità ed aggiornamento dell'informazione).

In ogni caso non può essere dichiarata conformità all'informazione contenuta in queste trasparenze.

In ogni caso questa nota di copyright non deve mai essere rimossa e deve essere riportata anche in utilizzi parziali.

▶ INDEX

09.30: Presentazione

- the Italian **Black Hats** Association
- Gli interventi tecnici della mattinata

09.45 Hacking e Sicurezza

- Un po' di storia
- L'evoluzione e la crescita
- Sikurezza.org

10.00: INTERVENTO I

Sovversioni del protocollo Tcp/IP: attacchi e contromisure

10.45: INTERVENTO II

Buffer Overflow e dintorni

11.45: INTERVENTO III

Smart Card e Java Card

12.45 Tavola Rotonda

13.15 Q&A, Contacts, Thanks

13.30 Chiusura lavori

▶ SPEAKERS

- **Fabio Pietrosanti aka Naif**
- **Raoul Chiesa aka Nobody**
- **Igor Falcomatà aka Kobaiashi**
- **Marco Ivaldi aka Raptor**

• **Matteo Falsetti aka Fusys**

• **Nicola Bonelli aka Awgn**

• **Francesca Fiorenza aka Kiai**

**Naif, Nobody, Kobaiashi,
Raptor, Fusys, Awgn, Kiai, Nail,
Gigi Sullivan, Vecna**

The Italian Black Hats Association

What we do

Blackhats.it è una comunità di ricerca **sorta spontaneamente**, formata da un gruppo di dieci persone: hackers, esperti di security, alcuni che lavorano nel mondo dell'I.T., altri impegnati come ricercatori, Professionisti della sicurezza informatica, provenienti da aziende e realtà diverse, con **forti legami al mondo underground ed alla filosofia hacker**, i quali si dedicano a migliorare la sicurezza della rete Internet: lo fanno per proprio conto e con risorse proprie, dedicando il loro tempo personale a questa passione.

Who we are

Al momento i Black Hats italiani sono :

naif@blackhats.it, **nail@blackhats.it**, **nobody@blackhats.it**, **raptor@blackhats.it**,
fusys@blackhats.it, **sullivan@blackhats.it**, **awgn@blackhats.it**, **kiai@blackhats.it**,
claudio@blackhats.it, **koba@blackhats.it**.

Altre figure si aggiungeranno nel tempo, in quanto Blackhats.it è una **comunità aperta** a tutti coloro i quali vedono l'I.T. Security da **punti di vista differenti dai canoni standard**, lontano dai legami e dagli obblighi commerciali e vicino alla filosofia Open Source.

Gli interventi tecnici della mattinata

- **Hackers, chi sono ? Underground & Security Research (30 mins)**
(TECH LEVEL: base)
- **Sovversioni del protocollo TCP, attacchi e contromisure (45 mins)**
(TECH LEVEL: medium)
- **Buffer Overflow e dintorni (60 mins)**
(TECH LEVEL : medium/high)
- **Smart Card (Java Card) (60 mins)**
(TECH LEVEL : medium/high)
- **Tavola Rotonda (30 mins)**
- **Q&A, Contacts, Thanks (15 mins)**

Hacking e Sicurezza: un po' di storia

•THE ROOTS, le origini:

Anni '60: i "topi di laboratorio", distribuiti tra MIT, UCLA e BERKELEY, creano le fondamenta dell'attuale Internet

•SOME HISTORY:

Anni '70: nascono le reti pubbliche a commutazione di pacchetto (X.25)

Anni '80: Phrack e 2600 Magazine vedono la luce. Negli USA proliferano i gruppi hackers (LOD, MOD, ...), in Europa nasce il CCC

Anni '80: X.25 hacking, Phreaking (blue boxes, PBXs, calling cards), Internet Hacking (.mil, .gov targets)

Anni '90: Hacker's Crackdowns (USA, 1990, Italy, 1994)

Anni '90: >1995, Commercial Internet (Italy: VOL)

Oggi: cos'è diventato l'"hacking"? L0pht went to @ Stake...

Oggi: IP stacks embedded in "non-standard devices" (cellulari, domotica)

Domani: Networking everywhere... (?)

Hackers: i mass-media li descrivono così...

Il giovane è uno dei responsabili degli accessi abusivi alle più importanti banche dati pubbliche

Roma indagava sul pirata informatico

L'hacker sedicenne di Siracusa era già nel mirino del sostituto procuratore Corasaniti

avrebbe consentito la vendita di Guignard e ceduti alle locali di cui parte delle reti Fininvest

La sua intrisa, ha firmato un'intesa con la tv della Romania.

Marco Mele

Criminalità informatica: sei arresti e sette fermi Operavano in tutta Italia

ROMA — Dall'Italia si erano introdotti per via telematica a mezzo di estorsione e di truffa, in sistemi di banche, società, enti e francesi. Che di fronte alla gravità del fenomeno, hanno chiesto la collaborazione della Polizia italiana. Così ieri, al termine di un lungo e pesante lavoro di "perquisizione" informatica, gli uomini della sezione criminale informatica del servizio centrale operativo hanno eseguito sei arresti, sette fermi e decine di sequestri di materiale informatico.

E' un'operazione di hackers, cui sono stati coinvolti i reati di associazione per delinquenza, truffa e frode, operava a Roma, Milano, Torino, Venezia, Siracusa, Cremona, Firenze, Matera e Varese. Gli arrestati sono un dipendente dell'Inps di

Tradito dalla presunzione il baby-genio del computer

Una moda senza regole

Sono entrati nella rete del Csi e hanno cambiato le parole-chiave impedendo l'accesso ai dipendenti Forse la minaccia arriva da Alessandria

no limitati a lasciare messaggi, una specie di firma dell'intrusione. «Adesso il problema è più grave. Noi non pensavamo che i pirati o il pirata riuscissero a bloccare l'accesso in quella parte di rete».

tizzare». E Picchioni aggiunge: «Servizi segreti? Falange Armata? Siamo alla Fantapolitica». E al Centro di calcolo stanno già tracciando una sorta di identikit del pirata: «Qualche traccia c'è - spiega Rovaris - anche se teoricamente

Corriere della Sera

CRONACHE ITALIANE

Ventisei indagati, quasi tutti ragazzi, tra Veneto, Piemonte, Emilia e Sicilia per reati informatici

Una trentina i baby-pirati

Andrea, l'«hacker»: non volevo fare danni a Bankitalia

Hackers: le aziende li “usano” così...

Carlo non svuota le tasche dei suoi genitori. S'introduce in rete e si impossessa dei dati.

Per sfida o per noia, gli hackers, sempre più numerosi, minacciano la vostra rete. Tra pirateria, vandalismo e spionaggio, gli attacchi contro le aziende si moltiplicano ogni anno. Identificazione, accessi autorizzati, protezione dei dati... Bull, esperta in sicurezza informatica, fornisce soluzioni e servizi completi per garantire l'integrità della vostra rete. Con Internet, è sempre più facile raggiungervi. Con Bull, le vostre informazioni restano sicure. www.bull.it

Bull
NETWORKS OF CONFIDENCE

Campagna pubblicitaria BULL

E PENSATE DI FERMARLO CON UNA PASSWORD?

(Rickard Kust - Hacker)

CON BUSINESS FULL SECURITY DI TELECOM ITALIA POTETE DARE ALLA VOSTRA RETE AZIENDALE UNA NUOVA SICUREZZA. IN OGNI MOMENTO.

BUSINESS FULL SECURITY Nel mondo on line c'è una parola chiave che vale più di molte altre: sicurezza. Perché una volta che dati, informazioni e segreti aziendali sono in rete, la loro vulnerabilità aumenta in maniera esponenziale. Ed è per questo che Telecom Italia ha creato Business Full Security. Grazie alle più avanzate tecnologie di security e al know how del più grande operatore italiano di telecomunicazioni, Business Full Security offre soluzioni complete, modulari per dare una risposta a ogni esigenza di sicurezza nei diversi contesti operativi di ogni azienda. Blocco di accessi indesiderati, protezione del Web aziendale, interscambio sicuro di dati e documenti: queste sono solo alcune delle soluzioni che Business Full Security può sviluppare, grazie anche a una solida organizzazione integrata creata appositamente per questa offerta.

Per saperne di più chiamateci al "Numero Verde della Sicurezza" 800 777 333 e visitate il sito www.security.telecomitalia.it www.telecomitalia.it

TELECOM FULL BUSINESS. CON LE AZIENDE VERSO NUOVE IMPRESE.

Campagna pubblicitaria Telecom Italia (FBS)

O così...

:) HACK EDUCATION

Partecipa anche tu al Corso di

"HACKERS"

Sistemi di sicurezza informatici

Ti insegniamo a diventare
un "HACKER" per
difenderti dagli hackers.



DIVENTA UN PROFESSIONISTA DELLA SICUREZZA INFORMATICA.

Infoline 02.28.97.03.80 - 02.46.82.24 - Fax 02.26.89.46.40

Corsi per Personal Computers:

*Windows - Word - Excel - Access - PowerPoint - Visual Basic - Photoshop
Flash - Dreamweaver*

C.p.s. computers - Via Dei Transiti 21 - Cps.computers@libero.it

"Perchè comprare tutto il corso se posso acquistare anche solo una lezione se voglio?"

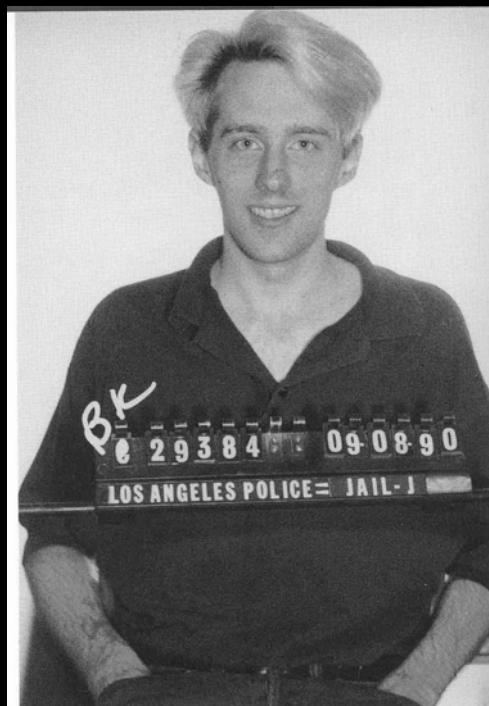
sponsored by Hacknsecurity
sponsored by www.e-webeditor.com
Bianca Cappelletto Carabini - Padova

Graphic by : HACKPublishing - HackerWalker - Iron Subed

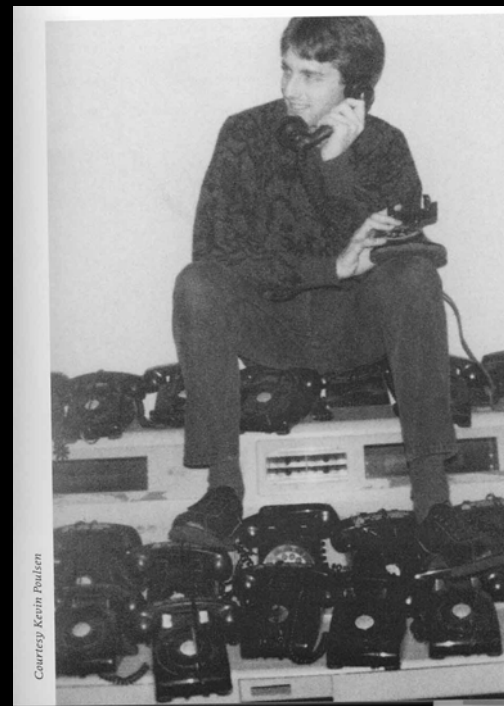
Hackers: ma in realtà sono così...



Kevin Poulsen a 8 anni



Kevin Poulsen (1° arresto)



Kevin Mitnick



**K. Mitnick
(ultimo arresto)**

O così...



Hacking e Sicurezza: l'Evoluzione e la Crescita

•Single Celebrities

Kevin D. Mitnick, Susan Thunder

Kevin L. Poulsen

•Company Celebrities

10pht/@ stake

Aleph1, SecurityFocus: ARIS & SIA

Hacking e Sicurezza: riferimenti

Historical Books

- **The Cuckoo's Egg. Clifford Stoll, ENG**

Forse il primo libro vero sull'hacking e sugli hackers, ha creato un caso.

(recensione su <http://www.apogeeonline.com/webzine/2001/07/10/01/200107100101>)

- **The Watchman: the twisted life and crimes of serial hacker Kevin Poulsen. Jonathan Littman, ENG**

Phreaking e Må Bell nel '90

(recensione su <http://www.apogeeonline.com/webzine/2000/11/29/01/200011290101>)

- **Sulle tracce di Kevin. Markoff/Shimomura, Sperling & Kupfler, ITA**

La storia di Kevin Mitnick - e quindi la prima generazione statunitense di hackers ed azioni di hacking - ma attraverso la *personale* visione di Shimomura, quello che l'ha arrestato.

- **The Fugitive Game: Online with Kevin Mitnick. Jonathan Littman, ENG.**

Stesso argomento di prima, ma scritto in modo obiettivo, avvincente e meno di parte.

- **Spaghetti Hacker, Chiccarelli & Monti, Ediz. Apogeo, ITA**

il primo ed unico libro italiano sull'hacking nostrano: la scena degli anni '90 descritta con capacità ed analisi legale di alcuni reati informatici secondo il nostro codice di procedura penale

Hacking e Sicurezza: Sikurezza.org

- E' nata per essere un luogo di incontro per professionisti, hacker e appassionati di sicurezza informatica
- Ospita numerose mailing list "security related" (moderate) in italiano (ml@, crypto@, openbsd@, progetto@, ...)
- E' un punto di contatto tra aziende, comunità di ricercatori ufficiali, ricercatori indipendenti ed underground digitale
- Ospita alcuni progetti "security related" sviluppati da ricercatori italiani ed è disponibile per ospitarne altri
- Ospita una pagina dove le aziende e gli enti possono pubblicare offerte di lavoro nell'ambito della sicurezza e del networking
- Non ha finalità commerciali ed è gestita da volontari

Hacking e Sicurezza: Sikurezza.org

- ml@sikurezza.org..... sicurezza informatica "full disclosure"
vulnerabilità presunte o teoriche di software e loro dimostrazione, richieste di informazioni o aiuto, pareri e qualsiasi altra cosa sia "security related"
- crypto@sikurezza.org..... crittografia e criptoanalisi
algoritmi, teoria, pratica ed implementazioni di sistemi di crittografia e qualsiasi altra cosa sia "crypto related" anche in ambito non strettamente informatico
- openbsd@sikurezza.org.. utenti .it del sistema operativo OpenBSD
<http://www.openbsd.org>, Free, Functional & Secure
- progetto@sikurezza.org... Discussione del progetto sikurezza.org
coordinamento, nuove proposte, idee, etc.

SIKUREZZA.ORG
Italian Security Mailing List

<http://www.sikurezza.org/ml.html>

Hacking e Sicurezza: Sikurezza.org

storia:

- progetto attivo da 2 anni
- ~4700 messaggi distribuiti
- ~2-400 messaggi al mese
- ~2400 iscritti
- ~10-15mila visite/mese web
- frequentata da tutti i membri di blackhats.it e numerosi altri ricercatori e sviluppatori .it
- scopi dichiaratamente tecnici, di ricerca e di sperimentazione

futuro:

- Nuove mailing list (devel@, ?)
- Più spazio ai progetti di sviluppatori italiani
 - homepage
 - mailing list
 - cvs?
- Migliorare l'usabilità del sito
 - motore di ricerca con opzioni avanzate
 - possibilità di iscrizione online
 - faq e documenti per chi inizia
 - ?

Contacts

Italian Black Hats Association

Hackers, chi sono ?

Underground & Security Research

24 gennaio 2002, Infosecurity Italia

Relatori:

Fabio Pietrosanti

naif@blackhats.it

Raoul Chiesa

nobody@blackhats.it

Igor Falcomatà

koba@blackhats.it

Marco Ivaldi

raptor@blackhats.it

BlackHats.it

General Infos: info@blackhats.it