

BY RAOUL CHIESA and DR STEFANIA DUCCI

CYBERCRIME is a science that studies and analyses the criminal behaviour when dealing with the Information Technology world.

Computer-based crimes evolved significantly since the 80s and one international espionage tale is detailed in Clifford Stoll's book, *The Cuckoo's Egg*.

Today, just like with Sun-Tzu's *Art of War* – it is extremely important to know your enemy. Even before defining the budgets (both from an economical and a technological point of view) to be assigned for IT security in a company or government core infrastructure, it is important to know and understand the threat.

The beginning

When looking at "hacking-related" security incidents over the past decade, some rather worrying trends have surfaced that has driven both of us (*see sidebar*) to develop a more in-depth analysis of the hacking scene and the hacker culture.

Today, there is a dramatic decrease in the "window of exposure," or the time between the disclosure of a new attack or exploit and their use in massive attacks and/or distribution worldwide, as compared to attacks seen a few years ago.

Nevertheless, the hacking world has not always been linked to criminal actions (unlike today) and

the research carried out up till now has not managed to properly depict the complex, hierarchical and "continuous evolution" of the underground world.

Indeed, if we consider the studies and research carried out so far, we can see that in the past hacking has been seen as an emerging phenomenon, unknown to people and ignored by most researchers.

Today there are several leading papers about hacking and hackers outlined from several unique perspectives including psychological, sociological, or criminological.

However, according to these studies, there is only one type of hacker which is usually depicted as male, mostly young and antisocial with only malicious or destructive intent. This as we know is not really 100% true.

The application of a profiling methodology in the study of high-tech crime is possible, however it requires a 360° view of the phenomenon, by analysing it from four principal perspectives: Technological, social, psychological, and criminological.

Delving deep into the hacker culture

BIOGRAPHIES

Raoul Chiesa



A HACKER from 1986 to 1995, Raoul Chiesa was arrested in 1995 during a police operation called "Ice Trap," carried out by S.C.O. (Central Operative Service of the national Italian police), Criminalpol, Interpol and the FBI, after a long series of IT violations towards highly critical institutions and agencies.

From that time on his approach to ICT (information and communications technology) security has changed: In 1996 he began working towards ethical hacking and from 1997, he has been co-ordinating the Tiger Team of @ Mediaservice.net, a security consulting and vendor-independent group which is well known in Europe.

He is also a founder of CLUSIT (Italian Association for Information Technology Security) and member of the Management Committee of ISECOM (Institute for Security and Open Methodologies), TSTF (Telecom Security Task Force) and OWASP Italian Chapter (Open Web Applications Security Project).

Dr Stefania Ducci



SHE has a University degree in Law (University of Bologna - 2002), and a Masters degree in Criminology (University of Turin - 2003). She has been working for UNICRI (United Nations Interregional Crime and Justice Research Institute) since September 2003.

In 2004 she began collaborating with Raoul Chiesa on the Hackers' Profiling Project, for which she has used an independent research approach, providing her support and co-operation during her spare time, fascinated by the huge research possibilities and professional evolution offered by the project.

The Hacker Profiling Project phases

Phase 1 THEORETICAL COLLECTION

Elaboration and distribution of the questionnaire, in different forms and towards different targets.

Phase 2 OBSERVATION

Participation at "IT underground security" events (European Union, Asia, the United States, Australia).

Phase 3 FILING

Creation of a database for the classification and elaboration of data collected during Phase 1.

Phase 4 "Live" COLLECTION

Elaboration and activation of a new generation of highly customised Honey-Net Systems.

Phase 5 G&C ANALYSIS

Gap-analysis and correlation among data collected through the questionnaire, Honey-Nets and profiles deducted from literature on the topic.

Phase 6 HCP "live" ASSESSMENT (24x7)

Continuous assessment of profiles and correlation of modus operandi, through data collected in Phase 4.

Phase 7 FINAL PROFILING

Redefinition and fine-tuning of different hacker profiles previously used as the "standard de-facto."

Phase 8 DIFFUSION OF THE MODEL

Final elaboration of results, drafting and publication of methodology, raising awareness (white papers, lectures, trainings).

The purpose of our research project consists therefore in analysing the underground world through an interdisciplinary lens that, behaving like a prism, will reveal the existence of different categories of external attackers, as well as their subcategories and border-line entities. This is possible by putting together the areas of criminology with IT security.

The early results

The first results of our Hacker Profiling Project (HPP) have shown that different typologies of hackers exist if we consider action

modalities (whether the attacker works alone or in a group), technical skills, motivation, purpose, targets, adherence to the so called "Hacker Ethics" and so on.

Our research applies an approach completely different from the ones still in use, going directly to the source by observing "hackers in the field" and in a sense the "true" criminal actions.

HPP kicked off way back in September 2004, and comprised eight phases – theoretical collection, observation, filing, "live" collection, gap-analysis and correlation, "live" assessment, final profiling, and diffusion of the model (*see table*).

The first two phases are being finalised, while the third and fourth stages are still on-going.

The questionnaire is online and available on the Hack in the Box website (<http://hpb.hackinthebox.org>).

Note: Chiesa and Ducci will be in Kuala Lumpur for the sixth Hack in The Box Security Conference, from Sept 18-21 at The Westin Hotel, and will introduce for the first time – both in Asia and worldwide – the complete results of their research activities.

To register for the conference, call (03) 2039-4724, or surf to <http://conference.hitb.org/hitbsecconf2006kl>.

Nokia offers MoRAN to telcos

NOW that 3G (third-generation) mobile services are gaining momentum in the Malaysian telecommunications sector and new players seeking ways to manage costs and provide optimum service, Nokia has announced a solution that aims to do just that.

Since May 2001, Nokia has been helping to drive the development of 3G in several markets with MoRAN, a Multi-Operator Radio Access Network solution enabling a 3G network shared by several operators while still retaining control over individual licensed frequencies, radio cells, and services.

Nokia said operators can enjoy the advantages of network sharing and provide their own service portfolio to their subscribers at the same time.

In addition, the solution will enable operators to provide cost-effective 3G services in areas where traffic may be initially low at the startup phase.

"We find that sharing Radio Access Network elements and all related equipment between two operators, together with site sharing, can bring savings of up to 40% of the Radio Access Network capital and operational expenditures," said Bill Chang, managing director of Nokia Malaysia.

"This is important in the initial coverage building phase of 3G networks where investment in coverage is substantial and the early traffic and revenues are not in balance to begin with."

Nokia recently shared its

MoRAN solution with some of the 3G-licensed operators in this country.

"It gave us the opportunity to demonstrate how it can boost network building through enabling savings to the mobile infrastructure industry, operators and future subscribers alike," Chang said.

Nokia also announced that its 3G infrastructure is based on open standards, platforms and interfaces for a smooth evolution to commercial 3G services. It includes integrated end-to-end solutions, including charging, security, network management and service control applications.

www.nokia.com.