Cyber Weapons in 2011:
An F-16 just flew over a First World-War Battlefield

Presented by:
Raoul Chiesa
Senior Advisor on Cybercrime Issues at the United Nations Interregional Crime & Justice Research Institute (UNICRI)

Member of the Permanent Stakeholders Group (PSG)
@ European Network & Information Security Agency (ENISA)

Design & Concept:
Jart Armin & Raoul Chiesa

HITB, Amsterdam, May 19th, 2011
Agenda

* Disclaimer
* The Authors
* Introduction, Reasons for this talk
  * Bye bye, Wargames...
  * Evolution of Cyber Attacks
  * Information Warfare
  * Shared points between Cybercrime & InfoWar
  * Countries at stake
* New concepts for a new era
  * The Paradigm Shift
  * Digital Weapons comparison
  * A case study: Stuxnet
* Q&A
* Extra Material (Stuxnet technical details)
© Jart Armin & Raoul Chiesa, 2011
The Authors - Raoul “nobody” Chiesa

* On the IT underground scene since 1986
* Advisor @ UNICRI since 2004
* ENISA PSG (2010-2012)
* Founder, @ Mediaservice.net - Independent Security Advisory Company.
* Founder, Board of Directors at: CLUSIT (Italian Information Security Association), ISECOM, OWASP Italian Chapter
* TSTF.net Associate Partner
* Member: ICANN, OPSI/AIP, EAST
* Supporting: Team Cymru, APWG, ...
Independent Security Expert & Malware researcher
Senior Partner at CyberDefcon
Specialized in Cyber threats analysis and Cybercrime intelligence for Internet industry and government agencies
Well-known ‘cause of his exposure and analysis on RBN (Russian Business Network) - hostexploit.com, RBNexploit.com
Introduced as “one of the world’s top hacker hunters” by RU.TV
Heavily mentioned in Thomas Menn’s book, “Fatal System Error” (2010) along with Steve Santorelli (Team Cymru) and other nice folks!
In 1983, the movie “Wargames” went out.

At least 2 generations of teenagers began “playing hacking” because of this movie.

In the script, the lead character was nearly able to launch a “global termo-nuclear” war.

All of us we’ve used to laugh at that movie...

Nevertheless, the IT attacks launched in the last 25 years, still mainly relay on the hacking-techniques shown in the movie.

It’s the history, played in “repeat mode”.
- Hacking with friends

- Wardialling PSTN & Toll-Free / Port Scanning / X.25 scanning

- ...Getting access.
5 years later...

1988!!
THE CUCKOO'S EGG
TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE

CLIFF STOLL

"A SPY STORY FOR THE 90's -- AND IT'S ALL TRUE."
— Tom Clancy

© Jart Armin & Raoul Chiesa, 2011
* Reasons for this talk

* Speaking along with a lot friends, it looks like the “.mil” world developed a deep interest towards these topics...

- 2001/2002: First interest shown back from USA (after 9/11), focused on hacker’s resources in order to attack and/or infiltrate Al Qaeda;
- 2003-2005: observed a huge escalation of USA and Israel Secret Services, asking for 0-days, seeking for information resources among elite hackers, asking for Iran & Pakistan hacking;
- 2005: China’s attacks to USA go public, escalating during 2007-2010 (UK, Germany, France, Italy);
- 2008/2010: USA & Canada leading (since the last 2/3 years), an increasing attention related to National Critical Infrastructures, followed by UK, EU, Israel, India, Australia;
- 2010: Italian Committee for the National Security of the Republic audited myself (March/May);
- 2009/2010: NATO Cyber Coalition running CyberDefense 2010 (+CyberShot 2009/2010) along with C4 Command (Rome);
- 2011: Swiss Cyber Storm III.

- TODAY - Intelligence Agencies hiring “leet hackers” in order to:
  - Buy/develop 0-days;
  - Launch attacks on terrorists and/or suspected ones;
  - Protect National Security;
  - Informing & Training Local Governments.

* Thus, hackers becoming kind of “e-ambassadors”, “e-strategy consultants” towards .mil and .gov environments, or “e-mercenaries”, training “e-soldiers”...

© Jart Armin & Raoul Chiesa, 2011
Introduction

* Just like along the years you’ve got used to words such as:
  * “Paranoia” (that’s into your DNA, hopefully!)
  * “Information Security” (198x)
  * “Firewall”, “DMZ” (1994/5)
  * “Pentesting” (1996/7)
  * “xIDS” (2001-2003)
  * “SCADA&NCIs” (2008-201x)
  * “PCI-DSS” (2009-201x)
  * Botnets (2008-2010)
  * etc. etc.

* ...in the next (five to ten) years, you will hear non-stop about:
  * NGC - Next Generation Cybercrime
  * CyberWar
  * Information Warfare
  * NGW - Next Generation Warfare

© Jart Armin & Raoul Chiesa, 2011
<table>
<thead>
<tr>
<th><strong>OFFENDER ID</strong></th>
<th><strong>LONE / GROUP HACKER</strong></th>
<th><strong>TARGET</strong></th>
<th><strong>MOTIVATIONS / PURPOSES</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Wanna Be Lamer</td>
<td>GROUP</td>
<td>End-User</td>
<td>For fashion, it's “cool” =&gt; to boast and brag</td>
</tr>
<tr>
<td>Script Kiddie</td>
<td>GROUP: but they act alone</td>
<td>SME / Specific security flaws</td>
<td>To give vent of their anger / attract mass-media</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>attention</td>
</tr>
<tr>
<td>Cracker</td>
<td>LONE</td>
<td>Business company</td>
<td>To demonstrate their power / attract mass-media</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>attention</td>
</tr>
<tr>
<td>Ethical Hacker</td>
<td>LONE / GROUP (only for fun)</td>
<td>Vendor / Technology</td>
<td>For curiosity (to learn) and altruistic purposes</td>
</tr>
<tr>
<td>Quiet, Paranoid, Skilled</td>
<td>LONE</td>
<td>On necessity</td>
<td>For curiosity (to learn) =&gt; egoistic purposes</td>
</tr>
<tr>
<td>Hacker</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber-Warrior</td>
<td>LONE</td>
<td>“Symbol” business company / End-User</td>
<td>For profit</td>
</tr>
<tr>
<td>Industrial Spy</td>
<td>LONE</td>
<td>Business company / Corporation</td>
<td>For profit</td>
</tr>
<tr>
<td>Government Agent</td>
<td>LONE / GROUP</td>
<td>Government / Suspected Terrorist/ Strategic company / Individual</td>
<td>Espionage / Counter-espionage / Vulnerability test / Activity-monitoring</td>
</tr>
<tr>
<td>Military Hacker</td>
<td>LONE / GROUP</td>
<td>Government / Strategic company</td>
<td>Monitoring / controlling / crashing systems</td>
</tr>
</tbody>
</table>

*Hackers Profiling (2004-2011)*

© Jart Armin & Raoul Chiesa, 2011
No more “Wargames”
   (even if: Wargames 2010 went out, and Bruce Willis got the support of an “hacker” in the latest Die Hard): the “romantic hackers” are gone, forever 😞

Then Stuxnet appeared
   (May-June 2010).

...and everything changed.

WHY??
   An unexpected attack.
   An unexpected target (SCADA, Nuclear Plant).
   The very first time something like this was happening.
What is Information WarFare?

* Very simply, we are speaking about the so-called Warfare, applied to the cyberspace.

* Defending information and communication networks, acting like a deterrent towards “information attacks”, while not allowing the enemy to do the same.

* So we are speaking about “Offensive Information Operations”, built against an adversary, “till being able to dominate the information during a war contest.”

Uh? Stopping a Nuclear Plant is not “dominate information”…
* Information WarFare: why?

* It is an extremely new and dynamic war scenario, where those metrics and views used before it are now really obsolete.

* Typically, these operations are decentralized while anonymous.

* The “entry fee” cost is extremely low, while it supplies a huge power.

* ...and after all, there’s always the possibility of denying what has happened..

* Think about Estonia, Georgia...what will be next?

© Jart Armin & Raoul Chiesa, 2011
PC Zombies (botnets) -> they take advantage of the “standard user”, both in a Corporate or home (broadband) scenario.

“0-days”: until today, all of them were on MS Windows + ad-hoc exploiting.

(attacker’s perspective) Nothing changes that much. There’s more chances to hack 1000 broadbands users instead of 10.000 PCs from a company’s network.

It’s still the digital weapon they need in order to launch attacks (DDoS, Keyloggers, 0-Days, etc).
*Being military “trendy”*

**OUT 😊**

- Single operational pic
- Autonomous ops
- Broadcast information push
- Individual Stovepipes
- Task, process, exploit, disseminate
- Multiple data calls, duplication
- Private data
- Perimeter, one-time security
- Bandwidth limitations
- Circuit-based transport
- Single points of failure
- Separate infrastructures
- Customized, platform-centric IT

**IN 😊**

- Situational awareness
- Self-synchronizing ops
- Information pull
- Collaboration
- Communities of Interest
- Task, post, process, use
- Only handle information once
- Shared data
- Persistent, continuous IA
- Bandwidth on demand
- IP-based transport
- Diverse routing
- Enterprise services
- COTS based, net-centric capabilities

**Scouting elite hacker parties?**

© Jart Armin & Raoul Chiesa, 2011
### Countries at stake

<table>
<thead>
<tr>
<th>Low Risk</th>
<th>Average Risk</th>
<th>High Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>Brazil</td>
<td>China</td>
</tr>
<tr>
<td>UK, Canada, France, Germany, Switzerland, Italy</td>
<td>Israel, Palestinian National Authority</td>
<td>North Africa / Africa generally speaking (WW Soccer Games 2010)</td>
</tr>
<tr>
<td></td>
<td>Zimbabwe</td>
<td>India, Pakistan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>North Korea (DPRK)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>South Korea</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Iran</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kyrgyzstan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Myanmar</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Russia, Estonia, Georgia</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rwanda</td>
</tr>
</tbody>
</table>

© Jart Armin & Raoul Chiesa, 2011
...it’s outta there. Already. Now.

<table>
<thead>
<tr>
<th>Summary of nation-state cyberwarfare capabilities</th>
<th>China</th>
<th>India</th>
<th>Iran</th>
<th>N. Korea</th>
<th>Pakistan</th>
<th>Russia</th>
</tr>
</thead>
<tbody>
<tr>
<td>Official cyberwarfare doctrine</td>
<td>X</td>
<td>X</td>
<td></td>
<td>Probable</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Cyberwarfare training</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Cyberwarfare exercises/simulations</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Collaboration with IT industry and/or technical universities</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>IT road map</td>
<td>likely</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information warfare units</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Record of hacking other nations</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

“North Korea will soon attack many countries using IT attacks, since they have the best hackers of the whole world.”

Uh?!? Seriously??

That’s weird, when speaking about a country which is totally isolated from the Internet, where its “cellular network” recalls more a DECT infrastructure...(no BTSs out of PongYang).

See Mike Kemp’s slides from CONfidence 2010 @Krakow.
New concepts, for a new era
"In the very near future many conflicts will not take place on the open field of battle, but rather in spaces on the Internet, fought with the aid of information soldiers, that is hackers. This means that a small force of hackers is stronger than the multi-thousand force of the current armed forces."

Former Duma speaker Nikolai Kuryanovich, 2007
Cyber War
Cybercrime to Cyberwar: Tools of the Trade

- Botnet & drone armies
- DDoS
- Trojans & Worms
- Malware
- Server hacking
- Encryption
- Extortion & Ransom
- Man in the Middle

© Jart Armin & Raoul Chiesa, 2011
Countries

* Russia
* USA
* France
* Israel
* UK
* China
* India
* Pakistan
* Ukraine
* Malware Factories

Activities

* Cyber crime tools
* Communications Intelligence
* National knowhow defence
* Transition from Industrial tools
* Hired Cyber mercenaries
* Industrial espionage
* Counter cyber attacks
* Cyber army
* Botnet armies
* Contract developers (x 4 worldwide)
Countries

* UN Member States = 197
* Vulnerable?
* 197 !!!!

Weapon Vulnerability

* Hacking
* DDoS
* Botnets
* Defacement
* Web site Hijacking & Redirection
* DNS & BGP hijacking
* BlackEnergy
* Darkness

* Stuxnet

* Nations exposed to Cyber Weapons
Why? The Paradigm Shift

Paradigm Shift

Old Paradigm

New Paradigm

Threat intensity

Terror infiltration

Classical wars between armies

Ballistic missiles
NBC
WMD

Short
Medium
Long range

August 4, 2002

The Role of Technology in the Transformation of Warfare
*Cyberwar: the weapons of choice*
* Cyberwar - The Weapons of Choice

Black Energy

* Cluster Bomb

Stuxnet

* Cruise Missile
**Comparison of Weapons**

**Black Energy**
- Multiple targets, loud and noisy
  - Massive DDoS
  - Loss of digital communication
  - Cloning of state communications
  - Create confusion

**Stuxnet**
- Laser Guided, precision, and stealth
  - Compromise infrastructure
  - Industrial Sabotage
  - Loss of confidence in systems
  - Create confusion
The "Ad"

Good time of the day dear citizens of DL
We are offering a quality DDoS Service
We have the best combination of quality and service!
We accept any targets regardless of their theme!
Regular customers will get special conditions
On average, we charge $50 per 24 hour period
All depends on the complexity of the attacked site
We accept payments via Webmoney
For people interested in permanent job positions
we have a special job offer that you will not decline
We are online 24 hours a day
Commands:
[+] ping commands are fine tuned to perfection
[+] Downloading Flood (new*)
[+] POST flood (new*)
[+] http attack on host
[+] temp attack on host
[+] port attack
our contacts
[email]: SMileFirce@yandex.ru
[email]: smile@darkdna.net (new*)
[sec]: 966-999

"Fire-Power"

* 30 bots overwhelm an average web site
* 1,000 bots - large web site
* 5,000 bots - even when using anti-ddos, blocks, and other preventive measures
* 15,000 bots can theoretically bring down vkontakte.ru (Russian Facebook)
* Example of Conficker worm reached 10.5 million bots

© Jart Armin & Raoul Chiesa, 2011
*Entering Cyber War?*
*A case study: Stuxnet (facts)*

- Stuxnet is a specialized malware, **solely** targeting:
  - **SCADA systems** running Siemens SIMATIC WinCC. Such systems monitor and control industrial technology and infrastructure.
  - **SIMATIC Siemens STEP 7** software for process visualization and system control.
- Uses **several vulnerabilities** in the underlying MS Windows operating system for infection and propagation.
- Infection works via **USB-drives** or **open network shares**.
- **Hides the content** of the malware on infected systems.
- Allows **full remote control** & P2P capabilities.
- **Only Siemens SCADA Step 7** & in particular centrifuges.
* An example: Stuxnet (speculations)

* Industrial sabotage
* Cyberwar tool kit
* USA, Israel, India, China…….who else? Maybe the Aliens?? ;)
* Atomstroyexport (TrojanDownloader.Agent.IJ trojan)
* 19790509 in the Windows registry (US & USSR sign Salt 2 treaty, limiting nuclear weapons) - not a US date format
* Experiment gone wrong
* PoC (proof of concept)
Cyber Weapons - Stuxnet
An F16 just flew over a 1st World War Battlefield
* A new class and dimension of malware
* Not only for its complexity and sophistication
* The attackers have invested a substantial amount of time and money to build such a complex attack tool (average: 1 MLN US$)
* Can be considered as the "first strike", i.e. one of the first organized, well prepared attacks against major industrial resources
* MITM (man in the middle) attacks on PLCs, industrial devices, and embedded systems
* Potential associated with Wi-Fi & for radio-frequency identification (RFID) hacking, - “smart-meter” hijacking and much more (think about SCADA-related industry: Water Companies, Energy Power plants, Highways, etc, etc.)
*The first time* that mass-media wrote about “Industrial Automation & SCADA security”.

*Stuxnet “helped”, Intelligence Agencies & Military Forces to think about “the next [IT] war” - also helping government contractors.

*Stuxnet helped also security researchers to “track back the attack” to a state sponsored attack tool.

*Stuxnet may be a basis for future extortion.

*Blueprint for the next generation of malware.*
* It looks like IRAN has been “attacked” again (?)

* “IRAN has detected a second spy virus designed to harm government systems, a senior Iranian military official said.”
  * http://topics.bloomberg.com/iran/

* “Iran announces discovery of new cyber attack, started by mistake from a strange PDF sent by friends of mine.”
*Then suddenly the “news” disappeared....?!!
* Avoiding being a victim of cyberwar

**Control of:**

* Cybercrime (learning from it, then applying its logic to InfoWar)
* Critical industrial infrastructures & contractors
* Over reliance on single routing of communications
* MITM (man in the middle) - gaps in the IT and Industrial Automation systems
* Mobile computing & thumb drives
* Important Internet servers and national communications infrastructure
* Improved Encryption & access
CyberDefcon - Cybercrime Clearing House & EU Early warning Coalition

UNICRI - United Nations Interregional Crime and Justice Research Institute

ENISA - the European Network and Information Security Agency

The opinions hereby expressed are those of the Authors and do not necessarily represent the ideas and opinions of the United Nations, the UN agency “UNICRI”, ENISA, ENISA PSG, nor others.
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

Emerging Crimes Unit (ECU): cyber crimes, counterfeiting, environmental crimes, trafficking in stolen works of art...

Fake Bvlgari & Rolex, Viagra & Cialis (aka SPAM)

Water systems with "sensors"…

Guess how they update each others?

Email, chat&IM, Skype…
Overview on UNICRI projects against cybercrime

- Hackers Profiling Project (HPP)
- SCADA & NCI’s security (CIP)
- Digital Forensics and digital investigation techniques
- Cybersecurity Trainings at the UN Campus

© Jart Armin & Raoul Chiesa, 2011
*Ad-hoc Trainings on SCADA security at the United Nations*
FIRST COMPREHENSIVE TRAINING PROGRAMME on

CYBER CRIMES

evaluating new threats, assessing your REAL security

- Information Security (InfoSec)
- Hacker Profiling Project (HPP)
- Digital Forensics
- SCADA and NCI

http://www.unicri.it/emerging_crimes/cybercrime/

From February 2011 @ UN Campus in Turin, Italy
On Hacker’s Profiling
The Hackers Profiling Project (HPP)

HPP purposes

- Analyse the hacking phenomenon in its several aspects (technological, social, economic) through technical and criminological approaches
- Understand the different motivations and identify the actors involved
- Observe those true criminal actions “in the field”
- Apply the profiling methodology to collected data (4W: who, where, when, why)
- Acquire and disseminate knowledge

© Jart Armin & Raoul Chiesa, 2011
The Hackers Profiling Project (HPP)

**Project phases - starting: September 2004**

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Theoretical collection: Questionnaire</td>
</tr>
<tr>
<td>2</td>
<td>Observation: Participation in IT underground security events</td>
</tr>
<tr>
<td>3</td>
<td>Filing: Database for elaboration/classification of data (phase 1)</td>
</tr>
<tr>
<td>4</td>
<td>Live collection: Highly customised, new generation Honey-net systems</td>
</tr>
<tr>
<td>5</td>
<td>Gap analysis: of data from: questionnaire, honey-net, existing literature</td>
</tr>
<tr>
<td>6</td>
<td>HPP “live” assessment of profiles and correlation of modus operandi through data from phase 4</td>
</tr>
<tr>
<td>7</td>
<td>Final profiling: Redefinition/fine-tuning of hackers profiles used as “de-facto” standard</td>
</tr>
<tr>
<td>8</td>
<td>Diffusion of the model: elaboration of results, publication of the methodology, raising awareness</td>
</tr>
</tbody>
</table>

© Jart Armin & Raoul Chiesa, 2011
The Hackers Profiling Project (HPP)

<table>
<thead>
<tr>
<th>PHASE</th>
<th>CARRIED OUT</th>
<th>DURATION</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - Theoretical collection</td>
<td>YES</td>
<td>ON-GOING</td>
<td>16 months</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Distribution on more levels</td>
</tr>
<tr>
<td>2 - Observation</td>
<td>YES</td>
<td>ON-GOING</td>
<td>24 months</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>From different points of view</td>
</tr>
<tr>
<td>3 - Filing</td>
<td>ON-GOING</td>
<td></td>
<td>21 months</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The hardest phase</td>
</tr>
<tr>
<td>4 - “Live” collection</td>
<td>TO BE COMMENCED</td>
<td></td>
<td>21 months</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The funniest phase 😊</td>
</tr>
<tr>
<td>5 - Gap &amp; Correlation Analysis</td>
<td>YET TO COME</td>
<td></td>
<td>18 months</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The Next Thing</td>
</tr>
<tr>
<td>6 - “Live” Assessment</td>
<td>PENDING</td>
<td></td>
<td>16 months</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The biggest part of the Project</td>
</tr>
<tr>
<td>7 - Final Profiling</td>
<td>PENDING</td>
<td></td>
<td>12 months</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“Satisfaction”</td>
</tr>
<tr>
<td>8 - Diffusion of the model</td>
<td>PENDING</td>
<td>GNU/FDL</td>
<td>12 months</td>
</tr>
<tr>
<td></td>
<td></td>
<td>;</td>
<td>Methodology’s public release</td>
</tr>
</tbody>
</table>

© Jart Armin & Raoul Chiesa, 2011
The Hackers Profiling Project (HPP)

Profiling Hackers - the book

RAOUL CHIESA • STEFANIA DUCCI • SILVIO CIAPPI

PROFILING HACKERS
The Science of Criminal Profiling as Applied to the World of Hacking

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.

ISBN: 978-1-4200-8693-5-90000
The Hackers Profiling Project (HPP)

Evaluation and correlation standards

- ModusOperandi (MO)
- Lone hacker or as a member of a group
- Motivations
- Selected targets
- Relationship between motivations and targets
- Hacking career
- Principles of the hacker’s ethics
- Crashed or damaged systems
- Perception of the illegality of their own activity
- Effect of laws, convictions and technical difficulties as a deterrent

© Jart Armin & Raoul Chiesa, 2011
## The Hackers Profiling Project (HPP)

### Detailed analysis and correlation of profiles - table #1

<table>
<thead>
<tr>
<th>PROFILE</th>
<th>RANK</th>
<th>IMPACT LEVEL</th>
<th>TARGET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wanna Be Lamer</td>
<td>Amateur</td>
<td>NULL</td>
<td>End-User</td>
</tr>
<tr>
<td>Script Kiddie</td>
<td></td>
<td>LOW</td>
<td>SME</td>
</tr>
<tr>
<td>Cracker</td>
<td></td>
<td>MEDIUM-HIGH</td>
<td>Business company</td>
</tr>
<tr>
<td>Ethical Hacker</td>
<td>Hobbieist</td>
<td>MEDIUM</td>
<td>Vendor</td>
</tr>
<tr>
<td>Quiet, Paranoid Skilled Hacker</td>
<td></td>
<td>MEDIUM-HIGH</td>
<td>On necessity</td>
</tr>
<tr>
<td>Cyber-Warrior</td>
<td></td>
<td>HIGH</td>
<td>“Symbol” business company</td>
</tr>
<tr>
<td>Industrial Spy</td>
<td></td>
<td>HIGH</td>
<td>Business company</td>
</tr>
<tr>
<td>Government agent</td>
<td>Professional</td>
<td>HIGH</td>
<td>Government</td>
</tr>
<tr>
<td>Military Hacker</td>
<td></td>
<td>HIGH</td>
<td>Government</td>
</tr>
</tbody>
</table>
### The Hackers Profiling Project (HPP)

#### Detailed analysis and correlation of profiles - table #2

<table>
<thead>
<tr>
<th>Profile</th>
<th>OFFENDER ID</th>
<th>LONE / GROUP HACKER</th>
<th>TARGET</th>
<th>MOTIVATIONS / PURPOSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wanna Be Lamer</td>
<td>9-16 years &quot;I would like to be a hacker, but I can't&quot;</td>
<td>GROUP</td>
<td>End-User</td>
<td>For fashion, it's &quot;cool&quot; =&gt; to boast and brag</td>
</tr>
<tr>
<td>Script Kiddie</td>
<td>10-18 years The script boy</td>
<td>GROUP: but they act alone</td>
<td>SME / Specific security flaws</td>
<td>To give vent of their anger / attract mass-media attention</td>
</tr>
<tr>
<td>Cracker</td>
<td>17-30 years The destructor, burned ground</td>
<td>LONE</td>
<td>Business company</td>
<td>To demonstrate their power / attract mass-media attention</td>
</tr>
<tr>
<td>Ethical Hacker</td>
<td>15-50 years The “ethical” hacker's world</td>
<td>LONE / GROUP (only for fun)</td>
<td>Vendor / Technology</td>
<td>For curiosity (to learn) and altruistic purposes</td>
</tr>
<tr>
<td>Quiet, Paranoid, Skilled Hacker</td>
<td>16-40 years The very specialized and paranoid attacker</td>
<td>LONE</td>
<td>On necessity</td>
<td>For curiosity (to learn) =&gt; egoistic purposes</td>
</tr>
<tr>
<td>Cyber-Warrior</td>
<td>18-50 years The soldier, hacking for money</td>
<td>LONE</td>
<td>“Symbol” business company / End-User</td>
<td>For profit</td>
</tr>
<tr>
<td>Industrial Spy</td>
<td>22-45 years Industrial espionage</td>
<td>LONE</td>
<td>Business company / Corporation</td>
<td>For profit</td>
</tr>
<tr>
<td>Government Agent</td>
<td>25-45 years CIA, Mossad, FBI, etc .</td>
<td>LONE / GROUP</td>
<td>Government / Suspected Terrorist/ Strategic company/ Individual</td>
<td>Espionage/ Counter-espionage Vulnerability test Activity-monitoring</td>
</tr>
<tr>
<td>Military Hacker</td>
<td>25-45 years</td>
<td>LONE / GROUP</td>
<td>Government / Strategic company</td>
<td>Monitoring / controlling / crashing systems</td>
</tr>
</tbody>
</table>
Must-read books / 1

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

- **H.P.P. Questionnaires 2005-2011**
- **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 Own the Box, (V.A.),** Syngress Publishing, 2003
- **Takedown**, John Markoff and Tsutomu Shimomura, Sperling & Kupfler, (Hyperion Books), 1996
- **The Fugitive Game: online with Kevin Mitnick**, Jonathan Littman, Little & Brown, 1997
Must-read books / 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
- 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
- Compendio di criminologia, Ponti G., Raffaello Cortina, 1991
- Criminal Profiling Research Site. Scientific Offender Profiling Resource in Switzerland. Criminology, Law, Psychology, Täterpro

© Jart Armin & Raoul Chiesa, 2011
And...a gift for you all here at HITB AMS! 😊

Get your own, FREE copy of “F3” (Freedom from Fear, the United Nations magazine) issue #7, totally focused on Cybercrimes!

DOWNLOAD:
www.FreedomFromFearMagazine.org

Or, email me and I will send you the full PDF (10MB)
Light zooms on Stuxnet
*Stuxnet - Attacked System - Normal Operation*
*Stuxnet - Attacked System
MITM - Attack Mode
*Stuxnet - Attacked System
MITM - Pass Thru Mode
<table>
<thead>
<tr>
<th>Export #</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Infect connected removable drives, starts RPC server</td>
</tr>
<tr>
<td>2</td>
<td>Hooks APIs for Step 7 project file infections</td>
</tr>
<tr>
<td>4</td>
<td>Calls the removal routine (export 18)</td>
</tr>
<tr>
<td>5</td>
<td>Verifies if the threat is installed correctly</td>
</tr>
<tr>
<td>6</td>
<td>Verifies version information</td>
</tr>
<tr>
<td>7</td>
<td>Calls Export 6</td>
</tr>
<tr>
<td>9</td>
<td>Updates itself from infected Step 7 projects</td>
</tr>
<tr>
<td>10</td>
<td>Updates itself from infected Step 7 projects</td>
</tr>
<tr>
<td>14</td>
<td>Step 7 project file infection routine</td>
</tr>
<tr>
<td>15</td>
<td>Initial entry point</td>
</tr>
<tr>
<td>16</td>
<td>Main installation</td>
</tr>
<tr>
<td>17</td>
<td>Replaces Step 7 DLL</td>
</tr>
<tr>
<td>18</td>
<td>Uninstalls Stuxnet</td>
</tr>
<tr>
<td>19</td>
<td>Infects removable drives</td>
</tr>
<tr>
<td>22</td>
<td>Network propagation routines</td>
</tr>
<tr>
<td>24</td>
<td>Check Internet connection</td>
</tr>
<tr>
<td>27</td>
<td>RPC Server</td>
</tr>
<tr>
<td>28</td>
<td>Command and control routine</td>
</tr>
<tr>
<td>29</td>
<td>Command and control routine</td>
</tr>
<tr>
<td>31</td>
<td>Updates itself from infected Step 7 routines</td>
</tr>
<tr>
<td>32</td>
<td>Same as 1</td>
</tr>
</tbody>
</table>

*Stuxnet - The DLL export paths*

© Jart Armin & Raoul Chiesa, 2011
Stuxnet - checking the correct target
Stuxnet - main injection process

Ref: Joel Langill
Stuxnet - Stolen Certification A & B

SYSTEM32\MRXCLS.SYS
* VirusBlokAda - Belarus
* Symantec - Exploring Stuxnet's PLC Infection Process
* Pierre-Marc Bureau : ESET - Stuxnet Under the Microscope, an analysis of Stuxnet
* F-Secure - Stuxnet Questions and Answers
* Joel Langill of ENGlobal, CSFI - Stuxnet Infection Video, Tofinosecurity
* Ralph Langner’s - Stuxnet is a directed attack -- 'hack of the century'
* VB Conference in Vancouver
* Ruben Santamarta, March 2011, RootedCon (Madrid, Spain)

*Stuxnet - Community Resources*