Cybercrime, Cyber-Espionage, Information Warfare and “Cyber War”: the fil-rouge which connects the dots

Raoul “Nobody” Chiesa
Expert
Disclaimer

- The information contained within this presentation do not infringe on any intellectual property nor does it contain tools or recipe that could be in breach with known laws.
- The statistical data presented belongs to the Hackers Profiling Project by UNICRI and ISECOM.
- Quoted trademarks belongs to registered owners.
- The views expressed are those of the author(s) and speaker(s) and do not necessary reflect the views of UNICRI or others United Nations agencies and institutes, nor the view of ENISA and its PSG (Permanent Stakeholders Group), neither Security Brokers.
- Contents of this presentation may be quoted or reproduced, provided that the source of information is acknowledged.
Agenda

- Introductions
- The scenarios and the Actors
- Profiling «Hackers»
- Information Warfare
- Cyber Espionage case study
- Conclusions
- References, Q&A
The Speaker

- President, Founder, **Security Brokers**
- Principal, **CyberDefcon Ltd.**
- Independent Senior Advisor on Cybercrime @ **UNICRI (United Nations Interregional Crime & Justice Research Institute)**
- Former PSG Member (2010-2012 / 2013.2015) @ **ENISA (Permanent Stakeholders Group @ European Union Network & Information Security Agency)**
- Founder, Board of Directors and Technical Commitee Member @ **CLUSIT (Italian Information Security Association)**
- Steering Committee, **AIP/OPSI, Privacy & Security Observatory**
- Former Member, Co-coordinator of the **WG «Cyber World» @ Italian MoD**
- Cultural Attachè, **APWG European Chapter (APWG.EU)**
- Board of Directors, **ISECOM**
- Board of Directors, **OWASP Italian Chapter**
- **Supporter at various security communities**
The Security Brokers

- We deal with extremely interesting, niche topics, giving our strong know-hows gained from +20 years of field experience and from our +30 experts, very well known all over the world in the Information Security and Cyber Intelligence markets.

- Our Key Areas of services can be resumed as:
  - **Proactive Security**
    - With a deep specialization on TLC & Mobile, SCADA & IA, ICN & Transportation, Space & Air, Social Networks, e-health, [...]
  - **Post-Incident**
    - **Attacker’s profiling**, Digital Forensics (Host, Network, Mobile, GPS, etc.), Trainings
  - **Cyber Security Strategic Consulting** (Technical, Legal, Compliance, PR, Strategy)
    - On-demand «Ninja Teams»
    - Security Incident PR Handling & Management
  - **Psychological, Social and Behavioural aspects** (applied to cyber environments)
  - **Cybercrime Intelligence**
    - Botnet takeovers, takedowns, Cybercriminals bounting, Cyber Intelligence Reports, Technical & Operational support towards CERTs and LEAs/LEOs, [...]
  - **Information Warfare & Cyber War** (only for MoDs & Intelligence Agencies)
    - Specialized Trainings, Attack&Defense Labs, more...
    - 0-day and Exploits – Digital Weapons
    - OSINT

October 26-27, Istanbul, Turkey
In the Information Security (InfoSec) world, we have a tremendous problem: the terminology.

- Each term has different meanings, depending on the context and the actor.

This is not enough, tough: in the last years a new trend come out, which is adding the prefix “cyber” to most of the terms.

- Nevertheless, a lot of (huge) doubts still persist, even in your own national language!
No common spelling...

„Cybersecurity, Cyber-security, Cyber Security ?”

No common definitions...

Cybercrime is...?

No clear actors...

Cyber – Crime/war/terrorism ?

No common components?...

In those non English-speaking countries, problems with correctly understanding words and terms rise up.
The scenario(s) and the Actors
Crime -> Today

You got the *information*, you got the *power*..

(at least, in *politics*, in the *business world*, in our *personal relationships*...)

- Simply put, this happens because the “*information*” can be *transformed at once* into “something else”:
  1. Competitive advantage
  2. Sensible/critical information (blackmailing)
  3. Money

- ... *that’s why* all of us we want to “*be secure*”.

- It’s not by chance that it’s named “*IS*”: *Information Security* 😊
Cybercrime

- **Cybercrime:**
  
  “The use of IT tools and telecommunication networks in order to **commit crimes** in **different manners**.”

- **The axiom of the whole model:**
  
  “**acquiring different types of data (information), which can be transformed into money.**”

- **Key points:**
  
  - Virtual (pyramidal approach, anonymity, C&C, flexible and scalable, moving quickly and rebuilding fast, use of “cross” products and services in different scenarios and different business models)
  - Transnational
  - Multi-market (buyers)
  - Differentiating products and services
  - Low “entry-fee”
  - ROI /Return of Investment (on each single operation, which means that, exponentially, it can be industrialized)
  - Tax & (cyber) Law heaven
Why?

“2013 Cybercrime financial turnover apparently scored up more than Drugs dealing, Human Trafficking and Weapons Trafficking turnovers”

Various sources (UN, USDOJ, INTERPOL, 2013)

Financial Turnover, estimation: 12-18 BLN USD$/year

«Cybercrime ranks as one of the top four economic crimes»

PriceWaterhouseCoopers LLC
Global Economic Crime Survey 2011
We are speaking about an ecosystem which is very often underevaluated: most of times, Cybercrime is the starting or transit point towards different ecosystems:

- Information Warfare
- Black Ops
- Cyber Espionage
- Hacktivism
- (private) Cyber Armies
- Underground Economy and Black/Grey Markets
  - Organized Crime
  - Carders
  - Botnet owners
  - 0days
  - Malware factories (APTs, code writing outsourcing)
  - Lonely wolves
  - “cyber”-Mercenaries
Profiling Actors
New Actors joined in

- Cybercrime and Information Warfare have a very wide spectrum of action and use intrusion techniques which are nowadays, somehow, available to a growing amount of Actors, which use them in order to accomplish different goals, with approaches and intensity which may deeply vary.

- All of the above is launched against any kind of targets: Critical Infrastructures, Governative Systems, Military Systems, Private Companies of any kind, Banks, Medias, Interest Groups, Private Citizens....
  - National States
  - IC / LEAs
  - Organized Cybercrime
  - Hacktivists
  - Industrial Spies
  - Terrorists
  - Corporations
  - Cyber Mercenaries

Everyone against everybody
The world is changing... (?)

→ Geopolitical shift: 2013 - Map of ITU Dubai General Assembly December (red=not signed; black=signed)

Source: Flavia Zappa, Security Brokers, 2013
Welcome to HPP!
HPP V1.0

• Back in **2004** we launched the Hacker’s Profiling Project - HPP:
  http://www.unicri.it/special_topics/cyber_threats/

• Since that year:
  – **+1.200 questionnaires** collected & analyzed
  – **9 Hackers profiles** emerged
  – **Two books** (one in English)
    • Profilo Hacker, Apogeo, 2007
### Evaluation & Correlation standards

<table>
<thead>
<tr>
<th>Modus Operandi (MO)</th>
<th>Hacking career</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lone hacker or as a member of a group</td>
<td>Principles of the hacker’s ethics</td>
</tr>
<tr>
<td>Motivations</td>
<td>Crashed or damaged systems</td>
</tr>
<tr>
<td>Selected targets</td>
<td>Perception of the illegality of their own activity</td>
</tr>
<tr>
<td>Relationship between motivations and targets</td>
<td>Effect of laws, convictions and technical difficulties as a deterrent</td>
</tr>
</tbody>
</table>

---

October 26-27, Istanbul, Turkey

Istanbul 2015 FIRST Technical Colloquium & TRANSITS Training
The scenario

- **Everything»evolved», somehow...**
- Here’s what the **United Nations** says (Hacker’s Profiling Project):

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

October 26-27, Istanbul, Turkey

Istanbul 2015 FIRST Technical Colloquium & TRANSITS Training
HPP V2.0: what happened?

• **VERY simple:**
• **Lack of funding:** for phases 3&4 we need support!
  – HW, SW, Analysts, Translators
• We started back in **2004:** «romantic hackers», + we foreseen those «new» actors tough: .GOV, .MIL, Intelligence.
• We **missed out:**
  – Hacktivism (!);
  – Cybercriminals out of the «hobbystic» approach;
  – OC;
  – The financial aspects (Follow the Money!!);
  – Cyberterrorists (do they really exist?)
Information Warfare (Cyberwar?) and the evolution of the 0-days market
October 26-27, Istanbul, Turkey
The DUMA knew it, long time ago....

"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
Hackers as a National Resource?

- A couple of years ago I’ve dig into a research from an Hungarian security researcher from HP
- His idea was weird!

- Should we consider hackers as “the enemy” / “troubles”...
- ...Or, may they represent an opportunity for Governments??
  - Patriot’s Hackers
  - Think about bloggers and North Africa (Egypt, Tunisia, Morocco) / GCC Area (Gulf Countries)
  - Think about IRAN and Twitter
  - See the potentialities?

Hackers in the national cyber security
Feds Seek a Few Good Hackers

War on terrorism distracts cybercops from routine hacking, and even encourages alliances.

By Andrew Brandt, PCWorld Aug 4, 2004 4:00 am

Attention, hackers: Uncle Sam wants you.

And hackers are answering the call, or at least listening. A well-attended session at the recent Defcon 12 hackers’ conference was “Meet the Feds,” a recruitment presentation by a group of federal cybercrime law enforcement agents, who fielded questions from would-be cybercops.

“We’re looking for good, talented people. We need a lot of help,” said Jim Christy, director of the Defense Department’s Cyber Crime Center.

“The Department of Defense understands how important computers are to defending the United States, and is always on the lookout for good people,” said Alvin Wallace, a supervisory special agent with the Air Force’s Office of Special Investigations.
Hacker 'Mudge' gets DARPA job

by Elinor Mills

February 10, 20:04:00 AM PST

Zatkoff, a respected hacker known as "Mudge," has been tapped to be a program manager at DARPA, where he will be in charge of funding research designed to help give the U.S. government tools needed to protect against cyberattacks, CNET has learned.

Zatkoff will become a program manager in mid-March within the Strategic Technologies Office at DARPA (Defense Advanced Research Projects Agency), which is the research and development office for the Department of Defense. His focus will be cybersecurity, he said in an interview with CNET on Tuesday.

One of his main goals will be to fund researchers at hacker spaces, start-ups, and boutiques who are most likely to develop technologies that can keep security systems up to date. He wants to see revolutionary changes, not evolutionary ones, he said.

He's also looking at giving a big push to research and development, which will be more advanced to match the progress of cyberattacks. "We can't wait for industry to catch up to cyber attacks," he said.
Making “Cyber War”...

- equipment to mimic target network
- dummy run on similar network
- sandbox zero-days

- "dummy list" of "ID-10T" for phishing
- background info on organisation (orgchart etc.)
- Primer for sector-specific social-engineering
- proxy servers
- banking arrangements
- purchase attack-kits
- rent botnets
- find (trade!) good C&C server
- equipment to mimic target network
- dummy run on similar network
- sandbox zero-days

- purchase 0-days / certificates
- purchase skill-set
- bespoke payload / search terms

- Intelligence/Logistics
- Live/System Discovery
- Detailed Preparations
- Testing & Practice
- Attack Execution

Alexander Klimburg 2012

- Purchase L2/L3 system data
Non-state proxies and “inadvertent Cyberwar”:"

„During a time of international crisis, a [presumed non-state CNE] proxy network of country A is used to wage a „serious (malicious destruction) cyber-attack“ against country B.“

**How does country B know if:**

a) The attack is conducted with consent of Country A (Cyberwar)

b) The attack is conducted by the proxy network itself without consent of Country A (Cyberterrorism)

c) The attack is conducted by a Country C who has hijacked the proxy network? (False Flag Cyberwar)
Back in 2005

- Vodafone Greece 2004 ("The Athens affair")
  - Rootkit on MSC Ericsson AXE
  - Inbound and Outbound Voice calls, SMS in/out, forwarded to 14 “pay-as-you-go” SIM cards (anonymous ones)
  - Olympic Games
  - 14 DEC 2007: Vodafone GR fined with 76M€

The illegally wiretapped cellphones in the Athens affair included those of the prime minister, his defense and foreign affairs ministers, top military and law enforcement officials, the Greek EU commissioner, activists, and journalists.
Ahhhh.... now I get it!

- PRISM and other secret project’s scandals ("the Snowden case")
- NSA’s budgets for black operations revealed
  - http://www.lemonde.fr/technologies/visuel/2013/08/27/plongee-dans-la-pieuvre-de-la-cybersurveillance-de-la-nsa_3467057_651865.html
Will this ever end up?

The Intercept

A DEATH IN ATHENS
Did a Rogue NSA Operation Cause the Death of a Greek Telecom Employee?

Costas Tsalikidis,
Network Planning Manager,
Vodafone-Panafon

Vodafone Greece CEO George Koronias holds documents in April 2006 before the start of a parliamentary committee hearing investigating the phone-tapping scandal. Photo: Louisa Gouliamaki /AFP/Getty Images
Budgets, Black Ops

NSA «black-ops Budget» exposed

- NSA’s “black budget”: 652M$ (2011)
- **231 black operations** known as of today (2011)
- 16 US agencies involved from the US Intelligence community (107,035 employees)

- Targets: US intelligence agencies high priority:
  - Iran
  - Russia
  - China
  - Afghanistan
  - North Korea
  - Syria
  - ....

- Cyber Attacks Unit “GENIE”
- Hacking into foreign systems in order to spy on contents, controlling functions
U.N. Report Calls on Governments to Protect Whistleblowers Like Snowden, Not Prosecute Them
Maybe...... 😊
What happened on September 2013?

Belgian Telco says it was hacked, while reports point to NSA or GCHQ as culprit

http://gigaom.com/2013/09/16/belgian-telco-says-it-was-hacked-while-reports-point-to-nsa-or-gchq-as-culprit/
The on-going one...

The Morning Download: Ukraine Claims Telecom System Hacked

By MICHAEL HICKINS

October 26-27, Istanbul, Turkey

Istanbul 2015 FIRST Technical Colloquium & TRANSITS Training
And the Police, too!

Dutch bill would give police hacking powers

Dutch law enforcement should be allowed to break into computers outside the Netherlands when necessary, the draft bill said.

By Loek Essers
May 2, 2013 06:47 AM ET  Add a comment

IDG News Service - The Dutch government today presented a draft bill that aims to give law enforcement the power to hack into computer systems -- including those located in foreign countries -- to do research, gather and copy evidence or block access to certain data.

Law enforcement should be allowed to block access to child pornography, read emails that contain information exchanged between criminals and also be able to place taps on communication, according to a draft bill published Thursday and signed by Ivo Opstelten, the Minister of Security and Justice. Government agents should also be able to engage in activities such as turning on a suspect's phone GPS to track their location, the bill said.

Opstelten announced last October he was planning to craft this bill.
Dutch Government Seeks to Let Law Enforcement Hack Foreign Computers

Dutch government wants to give law enforcement agencies investigative powers that involve hacking, installing spyware and destroying data

By Lucan Constantin
Fri, October 19, 2012

IDG News Service — The Dutch government wants to give law enforcement authorities the power to hack into computers, including those located in other countries, for the purpose of discovering and gathering evidence during cybercrime investigations.

In a letter that was sent to the lower house of the Dutch parliament on Monday, the Dutch Minister of Security and Justice Ivo Opstelten outlined the government’s plan to draft a bill in upcoming months that would provide law enforcement authorities with new investigative powers on the Internet.

According to the letter, the new legislation would allow cybercrime investigators to remotely infiltrate computers in order to install monitoring software or to search them for evidence. Investigators would also be allowed to destroy illegal content, like child pornography, found during such searches.

These investigative powers would not only cover computers located in the Netherlands, but also computers located in other countries, if the location of those computers cannot be determined.
Global, dirty business

• “Mass interception of entire populations is not only a reality, it is a secret new industry spanning 25 countries.”

• “It's estimated that the global computer surveillance technology market is worth $5 billion a year.”

  — ITALY: >300M/year
Who do you wanna sell (your 0days) to?
The pricing debate

- What about this? (CHEAP but LAME, India’s ones)
The pricing debate

http://www.theregister.co.uk/2014/11/11/german_spooks_want_millions_to_buy_0day_vulns/

October 26-27, Istanbul, Turkey

Istanbul 2015 FIRST Technical Colloquium & TRANSITS Training

47
The pricing debate

German spies want millions of Euros to buy zero-day code holes

Because once we own them, nobody else can ... oh, wait

By Richard Chirgwin, 11 Nov 2014  Follow 2,717 followers

Germany’s spies have come under fire for reportedly seeking funds to find bugs — not to fix them, but to hear them.

According to The Register, Germany’s national intelligence service, the country’s BND — its federal intelligence service — wants €300 million in funding for what it calls the Strategic Technical Initiative. The total sum of €49 million of that will be spent seeking bugs in SSL and HTTPS.

The BND is shopping for zero-day bugs not to fix them, but to exploit them. Instead of report them and face drawn criticism from NGOs, the Pirate Party, and the Chaos Computer Club (CCC), German Pirate Party president Stefan Kürmertold The Register people should hear governments more than cyber terror.

Kürmann is also critical of the strategy on the basis that governments shouldn’t be helping fund the grey market for security vulnerabilities, a sentiment echoed by the CCC.

http://www.theregister.co.uk/2014/11/11/german_spooks_want_millions_to_buy_0day_vulns/
Black Market?
Grey Market?
White Market?
Prices ranging from thousands to millions?

WTH?!?!?!
0-day Markets

Grey Market (underground)

White (?) Market

Software

Black Market (Cybercrime)

Software Rel x.y.z

0-day

«Bug»

Patch

Vendors
CERT (ICS-CERT)
National Institutions
A different (more serious?) approach

<table>
<thead>
<tr>
<th>Public Knowledge of the vulnerability</th>
<th>Buyer’s typology</th>
<th>0-day Exploit code + PoC Cost: Min/Max</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IS = IT Security companies</td>
<td>10K – 50K USD</td>
</tr>
<tr>
<td>Y</td>
<td>IS</td>
<td>10K – 50K USD</td>
</tr>
<tr>
<td>Y</td>
<td>INT</td>
<td>30K – 150K USD</td>
</tr>
<tr>
<td>Y</td>
<td>MIL</td>
<td>50K – 200K USD</td>
</tr>
<tr>
<td>Y</td>
<td>OC</td>
<td>5K – 80K USD</td>
</tr>
<tr>
<td>N</td>
<td>ALL</td>
<td>X2 – X10</td>
</tr>
</tbody>
</table>
## A different (more serious?) approach

<table>
<thead>
<tr>
<th>Public Knowledge of the vulnerability</th>
<th>Vulnerability relays on:</th>
<th>Buyer’s typology</th>
<th>0-day Exploit code + PoC Cost: Min/Max</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Operating System (OS)</td>
<td>IS = IT Security companies</td>
<td>40K – 100K</td>
</tr>
<tr>
<td></td>
<td>Major General Applications (MGA)</td>
<td>INT = Intelligence Agencies for Governmental use (National Security protection)</td>
<td>100K – 300K</td>
</tr>
<tr>
<td></td>
<td>SCADA-Industrial Automation (SCADA)</td>
<td>MIL = MoD/related actors for warfare use</td>
<td>100K – 300K</td>
</tr>
<tr>
<td>Y</td>
<td>OS</td>
<td>OC</td>
<td>40K – 100K</td>
</tr>
<tr>
<td>Y</td>
<td>MGA</td>
<td>INT</td>
<td>100K – 300K</td>
</tr>
<tr>
<td>Y</td>
<td>SCADA</td>
<td>MIL</td>
<td>100K – 300K</td>
</tr>
<tr>
<td>N</td>
<td>OS</td>
<td>MIL</td>
<td>300K – 600K</td>
</tr>
<tr>
<td>N</td>
<td>SCADA</td>
<td>MIL</td>
<td>400K – 1M</td>
</tr>
</tbody>
</table>
Cyber Espionage: a case study from India
Cyber Espionage

- The **complexity** and the **infrastructural and operating costs** of espionage (in the wide sense of the term) dramatically lowered down along the years, because of the IT revolution and the so-called “Digital Society”.
- In most of the cases, the **information** sits on (also, or “just”) on **digital storages** and **travels over the Net**.
- As a first effect, the **concept of “stealing” doesn’t exist anymore** (it’s virtual) and we must speak about **copying** the information (espionage approach):
  - What is “still there”, is “safe”;
  - More time needed to realize the “theft”; 
  - Less time needed to transfer or reselling the information -> cashing out.
- (public) incidents do happen both in the **private** and **public** (even **Military** and **Governmental**) business:
  - insiders (drivers: political, ethics, religious, fame and mass media, corruption, blackmail, ignorance);
  - contractors (external suppliers, consultants, VPN and RAS access, etc);
  - “competitors” (civilian and military) both **State-Sponsored** and **Independent**.
Massive Cybercrime + Industrial Espionage

The case study
- Our counter-cybercrime internal team works closely with different security communities (APWG, Host Exploit, Global Security Map, Team Cymru, etc...) which run concrete actions such as information sharing, botnets takedowns, international digital investigations, supporting and coordinating with different Law Enforcement Agencies in those involved countries (since the crime is global).
- One year ago, some members of these communities alerted about suspicious activities, not public known.

Weird aspects
- The world-famous «Chinese espionage» wasn’t involved
- Technical level and quality of the used tools: medium-low.
- Serial industrialization of the whole operational chain of the APT attacks (Advanced Persistent Threats).
- Full outsourcing of the attack.
- MO (Modus Operandi) organized by steps: Social Engineering based (phone calls, emails), then target exploitation (spear phishing).
- A very important and scaring sign of those synergies between Cybercrime and Cyber Espionage worlds.
- Something like a «prêt à portér» of digital espionage.
Operation Hang Over

- Repeated, targeted malicious activities, “targeted attack infrastructure” type.
  - New and different MO:
    - low-quality (.doc + .exe!!)
    - Very noisy;
    - Persistent;
    - Not executed by a single person.
  - Attacks and actions (apparently) originated from India.
  - Operating infrastructure since at least 3 years (mostly 4).

- We are speaking about a specific cybercrime service sold by an IT Security company based in India (AppPin Security Group...ever heard about?).

- Targets public known:
  - Telenor (Norway)
  - Bumi PLC (Indonesia)

- Targets found later:
  - ENRC (UK) – Energy National Research Center
  - Porsche (Austria)
  - Private companies from different markets in USA, Germany, etc
How this started?

Snorre, team leader, told us the following

“The op started with Telenor intrusion, we received md5s and cc info from TN via NorCert.

We then started looking into the case on our own initiative.

We were quickly able to connect the case with others, just googling the http request string returned lots of hits, and we used our own databases to get a lot more.

Dns reqs in combination w malware behavior info was one of the main mapping methods, but we also used other tricks, for example tracking bad guys through shodan. They often tanked their vps images identically, meaning we could see identical esmtp banners on different ip ranges.

Generally, the Hangover op was large-scale, over many arenas, but minimal complexity.

And I suspect it is not the only one ongoing in that region.

Snorre”

(Source: email exchange with Snorre Fagerland, Norman Shark, May-June 2013)
GUI pret-à-portèr

Direction to use aMatrix software

1. In First step, you start with Server Configuration module. In here you can configure Payloads, exploits and social engineering webpage, also create folder according to corresponding Payload, Exploits and social Engineering webpage on FTP server using its credentials and upload its exe's, html's and any other files inside the folder.

2. In second step, you start with New project and following the preceding steps to perform attack on victim. OR you can start with Existing project, if you want to use the existing project.

3. In third step, Report viewing, here you can see the complete details of sender, targetted person, types of attack etc.

4. In fourth Step, You can start with Monitor section:-
   - FTP Server Management - Here you can see the details of created folders and uploaded files inside the folder.
   - RAT (Remote Administration Tool) - With this, you can use Dragon Eye to take any desktop remotely, command shells are also provided to take control of remote machine.

5. In fifth steps, Utilities Section where different tools are provided to perform operation.

6. In sixth step, you can start with Web Scanner & Web Attack, which helps you to scan any URL and helps in getting its request and response URL, through this you can also perform attack by exploiting them. For more about this, you can learn it from help section of Web scanner & Web Attack of aMatrix software.

NOTE:- We have provided you about 50 templates in (C:\Program Files\Matrix frm) folder to use it while sending mail to the victim. You can also add some new templates according to your convenience while performing attack.

Copyright 2010-2011 Appin Security Group
GUI

In Server Configuration of Exploit, you can create the exploit by choosing payload server UserName, providing Exploit name, browse to choose bin file and select payload link from the combobox and then click OK. After that choose Exploit server UserName and providing Exploit description. You can also create a folder on local machine as well as on server through FTP and upload file inside it.
The «Big Picture»

Domain map of the attack infrastructure. Yellow and orange nodes constitute domains, blue are IP addresses, and purple are autonomous systems (AS). Green nodes are domains that are not part of any attack pattern, but are interesting in this context.
Conclusions
Conclusions

- Everything has changed.

- You just cannot fight on your own this war anymore. You may win a single battle, while it won’t be enough.
  - If you are insecure, I will be insecure too....

- Information Sharing, Security Awareness, Attacker’s Profiling, balanced InfoSec approach & processes: this is what you need.

- Ask for technical solutions from the Security Industry, be compliant with security standards and regulations, but don’t forget both taking from and giving back to the security communities.
A gift for you all here! 😊

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)
Spam Nation, Brian Krebs, 2014
Kingpin, Kevin Poulsen, 2012
H.P.P. Questionnaires 2005-2012
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
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 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
Reading Room /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, Katie Hafner, 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
International press on the case study

Contacts, Q&A

• **Need** anything, got **doubts**, wanna ask me **smth**?
  – rc [at] security-brokers [dot] com

Thanks for your attention!

**QUESTIONS?**
EXTRA Material
**HPPV1.0 - Zoom: correlation standards**

- Gender and age group
- Background and place of residence
- How hackers view themselves
- Family background
- Socio-economic background
- Social relationships
- Leisure activities
- Education
- Professional environment
- Psychological traits
- To be or to appear: the level of self-esteem
- Presence of multiple personalities
- Psychophysical conditions
- Alcohol & drug abuse and dependencies
- Definition or self-definition: what is a real hacker?
- Relationship data
- Handle and nickname
- Starting age
- Learning and training modalities
- The mentor’s role
- Technical capacities (know-how)
- Hacking, phreaking or carding: the reasons behind the choice
- Networks, technologies and operating systems
- Techniques used to penetrate a system

- Individual and group attacks
- The art of war: examples of attack techniques
- Operating inside a target system
- The hacker’s signature
- Relationships with the System Administrators
- Motivations
- The power trip
- Lone hackers
- Hacker groups
- Favourite targets and reasons
- Specializations
- Principles of the Hacker Ethics
- Acceptance or refusal of the Hacker Ethics
- Crashed systems
- Hacking/phreaking addiction
- Perception of the illegality of their actions
- Offences perpetrated with the aid of IT devices
- Offences perpetrated without the use of IT devices
- Fear of discovery, arrest and conviction
- The law as deterrent
- Effect of convictions
- Leaving the hacker scene
- Beyond hacking
<table>
<thead>
<tr>
<th>DETERRENCE EFFECT OF:</th>
<th>LAWS</th>
<th>CONVICTIONS SUFFERED BY OTHER HACKERS</th>
<th>CONVICTIONS SUFFERED BY THEM</th>
<th>TECHNICAL DIFFICULTIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wanna Be Lamer</td>
<td>NULL</td>
<td>NULL</td>
<td>ALMOST NULL</td>
<td>HIGH</td>
</tr>
<tr>
<td>Script Kiddie</td>
<td>NULL</td>
<td>NULL</td>
<td>HIGH: they stop after the 1st conviction</td>
<td>HIGH</td>
</tr>
<tr>
<td>Cracker</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>Ethical Hacker</td>
<td>NULL</td>
<td>NULL</td>
<td>HIGH: they stop after the 1st conviction</td>
<td>NULL</td>
</tr>
<tr>
<td>Quiet, Paranoid, Skilled Hacker</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td>Cyber-Warrior</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL: they do it as a job</td>
</tr>
<tr>
<td>Industrial Spy</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL: they do it as a job</td>
</tr>
</tbody>
</table>
Lesson learned?

I. Information Sharing and PPP (Public, Private Partnerships) are “must-have” in the InfoSec (and “Cybersecurity” 😊) world
   - Gov CERTs
   - Independent Security Communities
   - Investigation speed:
     - Knowing procedures
     - Direct, field experience
     - Network of contacts
   - Concrete and operative collaboration among victims, ISPs and ICT security experts

II. If this happened to a TLC operator in Northern Europe, possibly it happened also in other countries?
   - Did we know it? Did we realize we have been attacked, breached, exfiltrated?

III. The Cyber Espionage world is moving towards the outsourcing of “APT-based” attacks...
   - ... which was already there! The difference is that, now, is incredibly cheap and is coming from India, a country with a hacking know-how which is average good, and has huge experiences with IT outsourcing, very famous because of their prices, much lower than other markets;
   - Sold by a private company: did we investigated on a special, single, isolated case study? Are these the first steps of something bigger?
→ Solutions

- Despite being or not APTs, over the last 3-4 years attacks evolved, focusing on the human factor when dealing with targeted espionage, getting benefits from:
  - Ignorance of the victims (lack of education, basic training, security awareness, simulations);
  - Exposure and visibility on the Social Networks of the companies and its employees;
  - contractors and external suppliers;
  - BYOL (Bring your own device: smartphones, tablets;
  - “remote working”;
  - Lack of dialogue and information exchange with other market players (even competitors!);
  - Lack of procedures (approved, ready-to-go, tested) for Incident Handling, Digital Forensics e overall the “PR Security Management”.

- The “solution?”? There is not a panacea which “fixes everything”. But, good sense, personnel education and being ready to manage such incidents.
  - Speaking with the management, getting the authorizations approved
  - Security Awareness to all of the company’s levels
  - Specific trainings (IT department, software developers, Security department, Blue Team) and practical simulations (at least) yearly (2-3 /year=better)
  - The most important thing: work along with colleagues from different departments, such as Legal, Human Resources, Marketing, Sales!!