Cyber [Crime|War]

Connecting the dots

Iftach Ian Amit
Managing Partner, Security & Innovation
Agenda

- Who am I?
- CyberWar [Attack | Defense]
- CyberCrime [Attack | Defense]
- Past events revisited...
  - Connecting the dots
- Future
Who Am I
This is NOT going to be
Picking up where we left off

At least as far as last year’s research is concerned...
Boss, is this supposed to be on the internet? I think this is from my powerpoint! We probably need to call someone... I think this is from my powerpoint!
Finally declassified... (public domain)

The initial “trace” or lo-jack used (see rabbithole talk from 09)
Hungry yet?

This was just the appetizer...
Question 1: What is this?
Perceptions may be deceiving...

War

Crime
War

- Government / state
- Official backing
- Official resources
- Financing
- Expertise?
- Exploits/Vulns?

Crime

- Private
- semi-official backing (think organized crime)
- Official resources
- Self financing?
- Established expertise (in-house + outsourced)
- Market for exploits
CyberWar

“Cyberwarfare, (also known as cyberwar and Cyber Warfare), is the use of computers and the Internet in conducting warfare in cyberspace.”

Wikipedia
It did not happen yet Estonia being an exception?

“There is no Cyberwar”
This is not the **only** way!

Neither is this...

But civilian are **always** at stake!
Many faces of how CyberWar is perceived...

From McAfee’s “Virtual Criminology Report 2009”

Image caption: “countries developing advanced offensive cyber capabilities”
We’ll focus on current players:

And no, here size does **NOT** matter...
Thoroughly documented activity around cyberwar preparedness as well as military/government agencies with readily available offensive capabilities

Massive recruiting of professional in attack/defense for different departments:

- USCC (United States Cyber Command - includes AirForce, Marines, Navy and Army service components)
- NSA
- Other TLA’s...
Russia

- GRU (Main Intelligence Directorate of the Russian Armed Forces)
- SVR (Foreign Intelligence Service)
- FSB (Federal Security Services)
- Center for Research of Military Strength of Foreign Countries
- Several “National Youth Associations” (Nashi)
China

- PLA (People’s Liberation Army)
  - Homework: read the Northrop Grumman report...
  - General Staff Department 4th Department - Electronic Countermeasures == Offense
  - GSD 3rd Department - Signals Intelligence == Defense
- Yes... Titan Rain...
Iran

- Telecommunications Infrastructure Co.
- Government telecom monopoly
- Iranian Armed Forces
This is going to be very boring... Google data only :-(

- IDF (Israel Defense Forces) add cyber-attack capabilities.
- C4I (Command, Control, Communications, Computers and Intelligence) branches in Intelligence and Air-Force commands
- Staffing is mostly homegrown - trained in the army and other government agencies.
- Mossad? (check out the jobs section on mossad.gov.il...)
CyberWar - Attack

Highly selective targeting of military (and critical) resources

In conjunction with a kinetic attack

OR

Massive DDOS in order to “black-out” a region, disrupt services, and/or push political agenda (propaganda)
CyberWar - Defense

- Never just military
- Targets will be civilian
- Physical and logical protections = last survival act
- Availability and Integrity of services
- Can manifest in the cost of making services unavailable for most civilians
CyberCrime
You want money, you gotta play like the big boys do...
CyberCrime - Attack

- Channels: web, mail, open services
- Targeted attacks on premium resources
  - Commissioned, or for extortion purposes
- Carpet bombing for most attacks
  - Segmenting geographical regions and market segments
- Secondary infections through controlled outposts
  - Bots, infected sites
CyberCrime - target location
CyberCrime - Locations

Major Cybercrime group locations
CyberCrime - Ammunition

≈ APT
Zeus :: Statistics

Information:
Profile: icon
GMT date: 24.04.2008
GMT time: 22:11:51

Statistics:

Zeus :: Bots

Information:
Profile: icon
GMT date: 24.04.2008
GMT time: 22:14:03

Statistics:
Summary

Logs:
	→ Online bots
Remote commands

System:
Profiles
Search with template
Uploaded files

Options:
Profile
Search
Upload

Logout:

---

<table>
<thead>
<tr>
<th>#</th>
<th>CompID</th>
<th>Ver/Botnet</th>
<th>IP</th>
<th>Country</th>
<th>Socks</th>
<th>Proxy</th>
<th>Screenshot</th>
<th>Online time</th>
<th>Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>home_5hm79aabbb8_18ff587</td>
<td>1.0.3.7/0 66.20.176.219</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>28:14:42</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>home_00e01ec4</td>
<td>1.0.3.7/0 70.189.43.6</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>28:14:49</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>e58aeb3f9a6342e_0005cf1f</td>
<td>1.0.3.7/0 76.6.28.134</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>00:59:12</td>
<td>1.015</td>
</tr>
<tr>
<td>4</td>
<td>s0026776334_03c9bf3f</td>
<td>1.0.3.7/0 71.88.41.203</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>11:00:04</td>
<td>0.172</td>
</tr>
<tr>
<td>5</td>
<td>home_cxlfjvjt_3a19fa48</td>
<td>1.0.3.7/0 65.190.70.193</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>28:15:35</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>gabrail_00ebe5b</td>
<td>1.0.3.7/0 75.187.190.246</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>28:15:18</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>mvrd_00151288</td>
<td>1.0.3.7/0 66.24.74.225</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>03:56:03</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>hicks_07ca460dc_0002c847</td>
<td>1.0.3.7/0 74.47.176.92</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>28:14:55</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>e519887_04d613e3</td>
<td>1.0.3.7/0 130.76.32.145</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>28:15:15</td>
<td>2.353</td>
</tr>
<tr>
<td>10</td>
<td>home_039e4185</td>
<td>1.0.3.7/0 67.49.216.74</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>24:28:25</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>your_co2ygtgdl_21340d33</td>
<td>1.0.3.7/0 70.180.173.198</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>03:28:31</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>wa5117d81_000de927</td>
<td>1.0.3.7/0 63.164.145.198</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>23:19:11</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>hewlett_lhydpep_600d1b7d</td>
<td>1.0.3.7/0 67.175.12.315</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>06:04:26</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>e107300_00a07fc7</td>
<td>1.0.3.7/0 130.76.32.182</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>28:14:16</td>
<td>2.484</td>
</tr>
<tr>
<td>15</td>
<td>judy_tf2c4509</td>
<td>1.0.3.7/0 74.227.149.82</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>25:44:29</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td>cade6424_77f66e1</td>
<td>1.0.3.7/0 60.56.242.15</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>00:24:09</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>central_yyuq1of_03fc9472</td>
<td>1.0.3.7/0 206.71.200.121</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>07:03:20</td>
<td>0</td>
</tr>
<tr>
<td>18</td>
<td>bryan_pc_3e13a070</td>
<td>1.0.3.7/0 70.99.25.241</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>01:52:09</td>
<td>0.172</td>
</tr>
<tr>
<td>19</td>
<td>winxp_00021f3a1</td>
<td>1.0.3.7/0 69.246.194.0</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>28:15:32</td>
<td>0.27</td>
</tr>
<tr>
<td>20</td>
<td>wa5117d82_0027e2a1</td>
<td>1.0.3.7/0 62.64.145.198</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>28:15:34</td>
<td>0</td>
</tr>
<tr>
<td>21</td>
<td>private_45878f3_008622ad</td>
<td>1.0.3.7/0 76.68.150.19</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>00:46:55</td>
<td>0</td>
</tr>
<tr>
<td>22</td>
<td>mkres_xtygbenbe_17f5b01f</td>
<td>1.0.3.7/0 75.176.3.31</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>28:14:41</td>
<td>0</td>
</tr>
<tr>
<td>23</td>
<td>tony_f748f42277_00b21f7c</td>
<td>1.0.3.7/0 24.247.72.95</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>03:55:35</td>
<td>60.093</td>
</tr>
<tr>
<td>24</td>
<td>owner_f835edfc_0003f6be</td>
<td>1.0.3.7/0 65.12.136.38</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>03:14:38</td>
<td>0</td>
</tr>
<tr>
<td>25</td>
<td>take_2067du80ff_1c1dfb98</td>
<td>1.0.3.7/0 75.100.123.124</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>28:14:39</td>
<td>0</td>
</tr>
<tr>
<td>26</td>
<td>s002640302_01f52e5f</td>
<td>1.0.3.7/0 74.397.114.250</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>00:02:54</td>
<td>0.219</td>
</tr>
<tr>
<td>27</td>
<td>lovefamily_000d35a</td>
<td>1.0.3.7/0 71.180.88.97</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>02:30:50</td>
<td>0</td>
</tr>
<tr>
<td>28</td>
<td>hub_lab_11_0000dadf</td>
<td>1.0.3.7/0 68.190.65.92</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>00:46:12</td>
<td>0</td>
</tr>
<tr>
<td>29</td>
<td>faniba_05744139</td>
<td>1.0.3.7/0 75.56.211.191</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>28:15:26</td>
<td>0</td>
</tr>
<tr>
<td>30</td>
<td>dorm_0002de02</td>
<td>1.0.3.7/0 74.170.82.94</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>08:40:34</td>
<td>0</td>
</tr>
<tr>
<td>31</td>
<td>d5wccbb1_0005840c</td>
<td>1.0.3.7/0 72.149.8.2</td>
<td>US</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>05:54:22</td>
<td>0</td>
</tr>
</tbody>
</table>
CyberCrime - Defense

- Anti [Virus | Malware | Spyware | Rootkit | Trojan]
  - Seriously?

- Firewalls / IDS / IPS
  - Seriously?
    - Brought to you by the numbers 80, 443, 53...
    - SSL...
How do these connect?

Claim: CyberCrime is being used to conduct CyberWar

Proof: Let’s start with some history...
History - Revisited...

Estonia

You read all about it.

Bottom line: **civilian** infrastructure was targeted. Attacks originated mostly from **civilian** networks.
History - Revisited...

Israel

Cast led 2nd Lebanon war
Palestinian TV hacked - propaganda
Cast-Led, 2nd Lebanon war
(Israel and mid-east)

All attacks on Israeli Arab targets are attributed to hacktivists.
Mid-east crime-war links

ARHack

Hacker forum by day

Cybercrime operations by night
Political post

Buying/Selling cards for 1/2 their balance

Selling 1600 visa cards
History - Revisited...

Georgia

More interesting...

Highly synchronized **Kinetic** and **Cyber** attacks
Targets still mostly **civilian**
Launched from **civilian** networks
Russian Crime/State Dillema

McColo
ESTDomains
Atrivo
Micronnet
RealHost
RBN
Eexhost
Remember Georgia?

- Started by picking on the president...
  
  flood http www.president.gov.ge
  flood tcp www.president.gov.ge
  flood icmp www.president.gov.ge

- Then the **C&C** used to control the botnet was shut down as:
  
  - **Troops** cross the border towards Georgia
  - A few days of silence...
Georgia - cont.

- Six (6) new C&C servers came up and drove attacks at additional **Georgian** sites
  - www.president.gov.ge
  - www.parliament.ge
  - apsny.ge
  - news.ge
  - tbilisiweb.info
  - newsgeorgia.ru
  - os-inform.com
  - www.kasparov.ru
  - hacking.ge
  - mk.ru
  - newstula.info

- BUT - the same C&C’s were also used for attacks on **commercial** sites in order to extort them (botnet-for-hire)

  **Additional sites attacked:**
  - Porn sites
  - Adult escort services
  - Nazi/Racist sites
  - Carder forums
  - Gambling sites
  - Webmoney/Webgold/etc…
History - Revisited...

Iran

2009 Twitter DNS hack attributed to Iranian activity.

Political connections are too obvious to ignore (elections)

Timing was right on:

- UN Council Decisions
- Protests by leadership opposition in Tehran
IRANIAN CYBER ARMY

THIS SITE HAS BEEN HACKED BY IRANIAN CYBER ARMY
iranian.cyber.army@gmail.com
Iran-Twitter connecting dots

- Twitter taken down December 18th 2009
- Attack attributed eventually to cyber-crime/vigilante group named “Iranian Cyber Army”
- Until December 2009 there was no group known as “Iranian Cyber Army”...
- BUT - “Ashiyane” (Shiite group) is from the same place as the “Iranian Cyber Army”
Your Box Own3z By
Behroz_Ice - Q7x - Sha2ow - Virangar - MagicCoder - Mehdy007 - Nitrojen26 - tHe_Mo3tafA - BodyGuard
We Love Iran
Ashiyane Digital Security Team
Greetz: r00t_b0x - Azazel - 0261 - Jok3r - All_eagle - iNJECTOR
and All Ashiyane Defacers

HACKED BY
ASHIYANE
DIGITAL SECURITY TEAM

Enfrontery of blasphemy to Imam Khomeini is what that only you can
do. This is just a warning to your governmental sites!

Your Box Own3z By
Behroz_Ice - Q7x - Sha2ow - Virangar - Nitrojen26 - BodyGuard - tHe_Mo3tafA
MagicCoder - 0261 - All_Eagle - PLUS - Jok3r - System Fehler
We Love Iran
Ashiyane Digital Security Team
Greetz: Azazel - mahrud - N4H and All Ashiyane Defacers
Iran-Twitter - Ashiyane

- Ashiyane was using the same pro-Hezbollah messages that were used on the Twitter attack with their own attacks for some time...
- AND the “Iranian Cyber Army” seems to be a pretty active group on the Ashiyane forums
  www.ashiyane.com/forum

Let’s take a look at how Ashiyane operates...
On [Crime|War] training

Ashiyane forums

WarGames
Wargame targets includes:
What else happened on the 18th?

More recently - Baidu taken down with the same MO (credentials)
Mapping Iran’s [Crime|War]

- Ashiyane
- Iranian Cyber Army
- DDoS
- Botnet Herding
- Site Defacement
- Credit Card Theft
- Strategic Attacks
- $\$$
- US
- UK
- CN

Crime

War
History - Revisited...

China

- Great Chinese Firewall doing an OK job in keeping information out.
- Proving grounds for many cyber-attackers
- Bulletproof hosting (after RBN temporary closure in 2008 China provided an alternative that stayed...
January 12th - Google announces it was hacked by China

Not as in the “we lost a few minutes of DNS” hacked...

“In mid-December we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google” (David Drummond, SVP @Google)
January 12th - Adobe gets hacked. By China.

“Adobe became aware on January 2, 2010 of a computer security incident involving a sophisticated coordinated attack against corporate network systems managed by Adobe and other companies” (Adobe official blog)

Same MO: 0-day in Internet Explorer to get into Google, Adobe and more than 40 additional companies
The only problem so far - the attacks all have the sign of a CyberCrime attack. All the evidence points to known crime groups so far.

“It was an attack on the technology infrastructure of major corporations in sectors as diverse as finance, technology, media, and chemical” (Google enterprise blog)
Criminal groups attack companies in order to get to their data so they can sell it (whether it was commercial or government data!)

**US Response:** “We look to the Chinese government for an explanation. The ability to operate with confidence in cyberspace is critical in a modern society and economy.” (Hillary Clinton, Secretary of State)
The China move:

Use of criminal groups to carry out the attacks provides the perfect deniability on espionage connections (just like in the past, and a perfect response to clinton).

Targets are major US companies with strategic poise to enable state interest espionage.

Information sharing at its best:

State <-> Crime

Win - Win
THE FUTURE (Illustrated)
Summary

**Good**
- Formal training on cybersecurity by nations

**Bad**
- Commercial development of malware still reigns

**Ugly**
- Good meet Bad: money changes hands, less tracks to cover, criminal ops already creating the weapons...
Summary

THE FUTURE

LACK OF LEGISLATION AND COOPERATION ON MULTINATIONAL LEVEL IS CREATING DE-FACTO “SAFE HAVEN” FOR CYBERCRIME. <- FIX THIS!

TREATIES AND ANTI-CRIME ACTIVITIES MAY PROVE TO BE BENEFICIAL. <- NUKES?
Thanks!

Q & A

iamit@iamit.org

pro: iamit@securityandinnovation.com

twitter: twitter.com/iiamit

blog: iamit.org/blog