An investigation into Chinese cybercrime and the underground economy in comparison with the West

Michael Yip
07 December 2010
China’s Internet population is 420 million with only 31.6% penetration.

UK’s Internet population is 51 million but with 82.5% penetration.
Social problems

• 94.9% of Chinese Internet users have monthly salary of 5000 RMB (£479) or below

• Huge inequality in income distribution (urban vs rural)

• Nationwide “admiration” for hacking:
  – Do you want to be a hacker? 86.72% Yes (9031 votes)
  – Should hackers use their skill to make profit? 53.82% Yes (7443 votes)

* The poll is placed on an article about how 18-20 year olds are making tens of thousands of RMB per month in the underground economy
Disgruntle IT industry

- In 2003 – 2009, between 86.4% - 91% of IT employees are unhappy about their salary
- In 2009, IT had the lowest job retention rate
- Typical monthly salaries:
  - Web administration: 800–2000RMB (£75 - £187)
  - Enterprise system admin: 2000–3500RMB (£187 - £328)
  - Software developer (5 yr experience): 12000–15000RMB (£1,146 to £1433)

Cybercrime legislation in China

• The Criminal Law is the primary guideline for prosecution and sentencing (Articles 285 – 7)

• There are gaps and inadequacies e.g. max. punishment for invasion into state systems is < 3 years of imprisonment (Qi et al. 2009)

• From 2000 – 2009, 102 cybercrime offenders were reported in the People’s Daily newspaper but only 13 were reported to have received official punishment. On the other hand, the U.S. has 65% prosecution rate. (Lu et al. 2010)

Booming underground economy?

• The net value of the Chinese underground economy is estimated to be reaching 10 billion RMB (US$1.48 billion)

• Far larger than the estimated value of the Western underground economy US$276 million

• Malware on mobile devices also rising, reaching 1000 variants by the end of 2009

• The value of the mobile malware production chain is conservatively estimated to be around 1 billion RMB (US$148 million)
Why study China?

• The threat of huge breeding ground of cybercriminals

• A potential safe haven with known issues in cooperation with Western law enforcement in tackling cybercrime

• The skill required to make profits in cybercrime is falling – presents an unprecedented opportunity for the poor

• Collapse of traditional boundaries - anyone anywhere can be affected

• Political motivated hacking, “hacktivism” -> cyberwarfare?
Today’s talk

The aim of this talk is to provide an open intelligence report on the state of cyber security in China.

• Hacktivism in China
• Current model(s) of cybercrime
• The Chinese underground economy in detail
Hacking and Hacktivism
“Goodwill” – founder of the Green Army

“Withered Rose” – his group HCPH rumoured to have written malware responsible for many espionage attacks

Source: The Dark Visitor – http://www.thedarkvisitor.com
Xiao Tian – attributed as the leader of a hacker group called “CN Girls Security Team”
Hacking

• Hacking is the essence of cybercrime

• Immensely popular in China

• Approximately 3.8 million registered users across just 19 forums

• Chinese government has begun cracking down on forums promoting malicious hacking in a bid to improve Web security

• Hacktivist groups have volunteered to help out with cleaning out malicious web pages
Chinese hacktivism

- The Chinese politically-motivated hacktivists first appeared in the mid-1990s when Internet first became publicly available in China

- They are a different kind of hacktivists in that they hack to defend the country, not against

- They have a strict code of conduct in not hacking within China

- Hacking is a way for them to voice their opinion on political matters thus not always destructive
“Chinese nationalism is not just about celebrating the glories of Chinese civilization; it also commemorates China’s weakness. This negative image comes out most directly in the discourse of China’s Century of National Humiliation. Chinese books on the topic generally tell the tale of China going from being at the centre of the world to being the Sick Man of Asia after the Opium War (1840) only to rise again with the Communist Revolution (1949)… The discourse of national humiliation shows how China’s insecurities are not just material, a matter of catching up to the West militarily and economically, but symbolic. Indeed, one of the goals of Chinese foreign policy has been to ‘cleanse National Humiliation’.”

Famous groups (1)

- Green Army (绿色兵团):
  - The very first group of Chinese hacktivists
  - Attacked Indonesian websites in response to the Indonesian riots in 1997, which gained media attention and hero status
  - Disbanded in 2000 due to commercialisation into security consultancy (Nsfocus?)
  - May have regrouped on Isbase.net, a forum which uses the exact same name

Famous groups (2)

- Javaphile
  - Founded by a person known as Coolswallow
  - All members were students from Jiaotong University
  - Has a history of attacking foreign websites. The same university is rumoured to be behind the recent attacks on Google CN
  - Coolswallow is alleged to be an information security consultant for China’s Public Security Bureau

Famous groups (2)

Famous groups (3)

- Honker Union of China (中国红客联盟):
  - One of the largest groups after the Green Army disbanded
  - Had around 80,000 members
  - Disbanded in 2004
  - Two groups are found to carry the same name:
    - Chinesehonker.org (honker.net)
    - Cnhonkerarmy.com

Famous groups (3)
Famous groups (3)
China VS Japan – Sept. 2010

• On 7th September 2010, a Chinese fishing boat was detained by Japan near the disputed Diaoyu Island

• The Chinese government was outraged and so were the honkers

A rally call for fellow honkers with list of targets, it is claimed to be a call from the founding members of the Honker Union of China.

附：目标
http://www.kantei.go.jp首相官邸
http://www.jinji.admix.go.jp人事院
http://www.cib.admix.go.jp内阁法制
http://www.sontu.go.jp总理府
http://www.ytcc.admix.go.jp公正取引委員
http://www.npa.go.jp警察庁
http://www.kouchnoi.go.jp宮内庁
http://www.kunaicho.go.jp宮内庁
http://www.somucho.go.jp宮内庁
More on the rally call

- Amateur hackers were also invited
- Ready-made tools were distributed for use by amateurs
- Skilled hackers were responsible for other types of intrusions
- QQ groups were set up for sharing and discussion
- YY Team Voice channel was also used for collaboration
The administrator of honker.net dismisses the rally call

He described such attacks as futile and of low strategic value for the country.

Such attacks would bring unnecessary pressure on the country and an excuse for other nations to attack China.
Cnhonkerarmy.com

- On the other hand, cnhonkerarmy.com announced on the 15th Sept. that they had launched attacks on Japan since 12th Sept. and had achieved success

- Cnhonkerarmy.com also suffered attacks from Japanese hackers in retaliation

- Attacks stopped after intervention from the Chinese government due to increasing pressure from foreign media

- No announcements of any arrests
Cnhonkerarmy.com

Message on defaced websites by cnhonkerarmy.com
Attribution to Chinese government

- No direct link to the Chinese government
- The hacking community is unlikely to be an official part of the Chinese military’s plan on information warfare because:
  - Difficulty in command and control
  - Difficulty in maintaining secrecy and surprise
  - Difficulty in precision targeting
- Rather, the government prefers to recruit talents from the hacking community and universities (e.g. Coolswallow)
Model(s) of cybercrime
Characteristics of cybercrime

- Well organised transnational underground markets with labour specialisation and healthy competition
- Targets the long tail of crime (higher volume, low in value)
Cybercrime in the West

- U.S. and Russian cybercriminals form the majority although there are people from all parts of the world including U.K. and Turkey

- Underground markets mainly exist on online forums but also on IRC channels

- Very well organised and sophisticated

- Hierarchical management preferred (communism?)

- Carding oriented – the unauthorised use of third party credit card details for personal gain
Carding forum - Darkmarket

- Darkmarket founded in the U.K. by JiLSi (Renukanth Subramaniam)
- Around 2500 members
- Shutdown by FBI in 2008 after a lengthy undercover operation
- Resulted in over 60 arrests in a dozen countries including the U.K.
Cybercrime in the West

Hierarchical structure of Western Carding Forums

- **Administrators**: Responsible for the management of the forum and making long-term strategic decisions. They are also responsible for managing the forum members, including rewards and punishments when appropriate.

- **Moderators**: Responsible for the management of the sub-forums within a forum which either fall into their expertise or geographical location. They specify the rules for posts as well as removing inappropriate ones.

- **Reviewers**: The duty of the reviewers is to examine and/or test illicit merchandises as well as services for which members of the forum desire to become a vendor.

- **Reviewed Vendors**: Reviewed vendors are those who have been referenced by reviewers and are deemed as trustworthy.

- **Members**: Members are the users who contribute to the forum and participate in various discussions and activities.
Cybercrime in the China

• Chinese cybercriminals prefer a more decentralised model with little or no central management (democracy?)

• Network of temporal relations rather than a hierarchical system of power delegation and fixed role assignments

• Trading via publicly available tools such as QQ and Baidu Tieba

• Theft of virtual assets more common than carding
  – In 2008, Zhuge et al estimated value of virtual asset trading solely on Taobao is worth approx. 223 million RMB (£20.8 million)
A general model of cybercrime

**ATTACK SERVICES**
- Zero-day exploit finders
- Malware authors
- Botnet herders

**DELIVERY**
- Spammers
- Phishers
- Intruders & Crackers
- Rogue web admins

**FINANCIAL CRIME / IDENTITY THEFT**
- Bank data stealers
- Plastic vendors & encoders
- Identity theft & fraud
- Cashiers
- Scammers
- Carders

**BLENDED SERVICES**
- Rogue Hosting
- Spoof website designers

**TRA好象 ORGANISED CRIMINAL GROUPS**
- Blackmailers
- Gangs/Mafia

**VIRTUAL ASSETS TRADING**
- Game login/envelope traders
- Virtual asset traders

**MONEY LAUNDERING**
- Virtual currency sellers
- Mules/Drops
- Exchangers

Offers services such as:
- VPNs
- SOCKS (encrypted proxies)
- Proxies
- IM server e.g. Jabba server

**NOTE:**
- flow of demand
- potential influence
Money laundering

• To add layers in the flow of money in order to obscure the true source of funding

• Money mules – people who receives and forwards the proceeds of fraud

An advert to recruit Chinese overseas students in the U.K. to act as money mules
The Chinese underground economy
The “visa” bar most popular for carding.

Rippers are also published here.

Baidu Tieba (http://tieba.baidu.com) is a public message board hosted by Baidu.
Adverts are usually short in length.

QQ numbers are left for further negotiations.
QQ IM and Group

Free.

Merge between social groups with IM.

Perfect tool for underground traders.
A Western-like carding forum.

Launched in July but has only 59 registered members to date.
Zombie machines “Flesh Chicken” are sold on Taobao, China’s equivalent to eBay.
Prices (1)

- Carding goods are similarly priced as those observed in the West
- Chinese tracks are more expensive than Western tracks

<table>
<thead>
<tr>
<th>Goods</th>
<th>Western Price (USD)</th>
<th>CN Price (USD) per unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK credit cards + cvv2</td>
<td>$0.50 - $12</td>
<td>Normal - $3.7 - $5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>With 3D - $22 - $44</td>
</tr>
<tr>
<td>US credit cards + cvv2</td>
<td>$0.50 - $12</td>
<td>Normal - $1.7 - $2</td>
</tr>
<tr>
<td>FR credit cards + cvv2</td>
<td>$0.50 - $12</td>
<td>Normal - $5.9</td>
</tr>
<tr>
<td>CN credit cards + cvv2</td>
<td>$0.50 - $12</td>
<td>Normal - $17</td>
</tr>
<tr>
<td>UK 101/201</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>US 101/201</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>FR 101/201</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Japan 101/201</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Dumps</td>
<td>$4 - $150</td>
<td></td>
</tr>
<tr>
<td>Bank logins</td>
<td>$15 - $850</td>
<td></td>
</tr>
<tr>
<td>Dumps</td>
<td>$4 - $150</td>
<td></td>
</tr>
<tr>
<td>Bank logins</td>
<td>$15 - $850</td>
<td></td>
</tr>
<tr>
<td>Bank BOA US</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Balance $7000 = $300</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Balance $14000 = $500</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Balance $18000 = $800</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bank HSBC (US)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Balance $12000 = 400</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Balance $28000 = 1000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bank HSBC (UK)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Balance GBP 8000 = $300</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Balance GBP 17000 = $700</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Prices (2)

<table>
<thead>
<tr>
<th>Services</th>
<th>Western Price (USD)</th>
<th>CN Price (USD) per unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zombie sales</td>
<td>A botnet can be sold for $550 including hosting</td>
<td>$0.11 – $0.22 per zombie</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$15 for 1000 household zombies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$15 for 1500 traffic zombies/Internet café zombies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$15 for 500-700 zombies with webcam control</td>
</tr>
<tr>
<td>DDoS attacks (DDoS 攻击)</td>
<td>$60 - $80 per day</td>
<td>$89 to $298 (24 hour attack)</td>
</tr>
<tr>
<td>Money laundering/Mule service/Cashier</td>
<td>N/A</td>
<td>50:50 split</td>
</tr>
<tr>
<td>Hacking training/tutorial</td>
<td>N/A</td>
<td>$22 to $149 (per student)</td>
</tr>
<tr>
<td>IP address</td>
<td>N/A</td>
<td>10,000 IPs = $18</td>
</tr>
</tbody>
</table>

- Zombie machines are sold/rented individually as well as in batch. Pricing also differs by location as well as webcam control.

- DDoS attacks more expensive than in the West
Track stores such as ltdcc.com eliminates language barriers between Chinese and Western carders.
Conclusion
Conclusion

- Hacking in China is immensely popular and hacktivists are perceived as national heroes
- Chinese government clearly shows leniency towards the hacktivists
- Cybercrime in China is flourishing rapidly, with victims being those in the West
- Chinese cybercriminals do trade with those in the West
- Baidu and QQ are main facilitators of cybercrime in China
Useful literatures


Thank you!