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

Michael Yip
16 December 2010
Internet in China

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)

Inadequate cyber laws

• 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

• Net value 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 (Symantec)

• 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)

Note: exaggeration highly possible
Why study China?

- The threat of huge breeding ground of cybercriminals
- A potential safe haven for Chinese cybercriminals
- 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”
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
Hacking

- Hacking is the essence of cybercrime
- Immensely popular in China
- Approximately 3.6 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
“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”
Chinese hacktivism

- First appeared in the mid-1990s when Internet first became publicly available in China
- Hack to defend their country, not against
- Strict code of conduct in not hacking within China
- Commonly and casually attributed by the foreign media as the masterminds behind cyber attacks on foreign targets e.g. the Florida blackout, 2008
“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.
China VS Japan – Sept. 2010

Lu Wall resindual waste tanks fire trench in the history of the bridge is still crying the passage of time can not erase that period of humiliating history of the network world today when the motherland once again sounded the alarm as a new generation of our
Adhering to the spirit of seventy-seven and Mukden
With our approach
With our thoughts
Firmly back all invaders
Network Security fight for the motherland against Japanese distortion of history and culture in the end.
Japan’s devils on our side to leave the land of peace and tranquility of the various crimes.
As a network of enthusiasts, we should pick up our weapons.
Defend our flag. Bearing in mind that China let the world will never yield to the view of the September 18, 2010 to commemorate the significance of this decision on the day of the major distortions in the Japanese war history. Support the independence of the site for large-scale resistance to the Japanese devils know that the Chinese are no longer sinking. The rise of China today, the face of all of Japan as We deeply regret that, as descendants of us, as anyone with a backbone of the Chinese people, we should not be silent, we should use our own way, to knock Japan ring a loud alarm, not a sign of weakness of the Chinese people!
In this former Honker Union of China (http://www.honker.net) appealed to the patriotic heart of youth, the majority of computer enthusiasts, the majority of hackers and technical personnel, in the September 18 launch network operations in Japan, mainly in the paralysis of various Japanese Great Link router and the major government and commercial Web sites based (to be released when the objectives and modalities)! will also organize our security technology group of Japanese Web sites, hang our banner, and paralysis of the Japanese server, and delete data, to Japan to a heavy blow.
You are willing to participate in this action based on friends to add group members 5,209,614 shares in the group are familiar with weapons and download the DF-5 tactical nuclear missiles. Exe 1.1MB, DDOS strong killertop Edition. EXE 28.5KB, Aladdin UDP attack device v2.1. exe 1.3MB, take the time to use this tool to achieve maximum unity of the skill of the core group members invasion invasion of other methods will be used! Tools for internal special!
See our pre-planning and preparation, and to join our team, and the clan for the record! Long-term target of attack is; United States, Japan, Indonesia, India, Vietnam, Philippines. . Core group of 27,437,332 invited to join the official system

Appendix: Target

http://www.kantei.go.jp prime minister’s residence
http://www.iiuji_admjp.go.jp Institute of Personnel
http://www.jlbj.admjp.go.jp Cabinet Legal
http://www.soifju.go.jp Prime Minister
http://www.jtc.admjp.go.jp members just to take lead
http://www.npajp.go.jp Police Agency
http://www.kroucho.go.jp members of public nuisance and other adjustments
http://www.kunapia.go.jp Imperial Household Agency
http://www.somuchu.go.jp Office of General Services
http://www.stat.go.jp Statistical Office of General Services
http://www.stat.go.jp/1.htm [English]
http://www.hda.go.jp Hokkaido Development Agency [Japan]
Coordination strategies

- List of targets published
- Amateur hackers invited and tools provided for use
- Skilled hackers responsible for other types of intrusions
- QQ groups were set up for sharing and discussion
- YY Team Voice tool was also used for collaboration
- Similar to other national hacktivists e.g. Russians
Chinesehonker.org (honker.net)

• The administrator of honker.net discourages such attacks.

• 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 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

2010年9月7日 中船与日船发生冲撞事件 请日国政府出面道歉！

中国红客联盟
cnhonkerarmy

[Hacked By 中国红客联盟]

5年前没打完的仗，如今我们继续奉陪……

This is just a little warning, Japan please self-respect...
Attribution

• No evidence linking the Chinese government found

• The hacking community 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

• Casual relationships between government and hacktivist groups likely

• Official recruitment
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
Cybercrime in the West

Typical management hierarchy in Western carding forums

Administrators are 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 are 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.

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 are those who have been referenced by reviewers and are deemed as trustworthy.

Members
Cybercrime in the China

- Prefer a more decentralised model with little or no central management (democracy?)
- Networks of temporal relations
- Trading via publicly available tools such as QQ and Baidu Tieba
- Theft of virtual assets more common than carding
- Law enforcement tend to be more focused on tackling the creation and distribution of malware than carding
Panda worm (06-07)

- First time Chinese authorities made arrests over virus attacks
- Highly destructive and caused mass data loss – cost of damage US$ 14 million
- Sold traffic of his website to an envelope (login) stealer Zhang Sun
- Infected machines also automatically downloaded trojans
- Profit of 150,000 RMB (US$ 22,518)

Li Jun – author of the Panda worm was sentenced to 4 years imprisonment
Panda worm (06-07)
“Gentle” Trojan (07-08)

- Targeted online games
- 5.3 million online gaming accounts were stolen within a year
- The authors Lu and Zhang made a profit of 645,000 RMB (US$94,534)
- 11/110 detainees sentenced to <3 years
- Fined 830,000 RMB

The production chain for the Gentle Trojan
A general model of cybercrime

The diagram illustrates the various roles and services involved in cybercrime activities. Key components include:

- **ATTACK SERVICES**
  - Zero-day exploit finders
  - Malware authors
  - Botnet herders
  - Offers products such as:
    - Virus & worms
    - Web-based trojans
    - Conventional trojans
    - Malware generators
    - Phishing kits
  - Offers services such as:
    - VPNs
    - SOCKS (encrypted proxies)
    - Proxies
    - IM server e.g. Jabba server

- **TRADITIONAL ORGANISED CRIMINAL GROUPS**
  - Blackmailers
  - Gangs/Mafia
  - Traditional gangs are not the cybercriminals. Rather, they are engaged in a range of illegal activities in the real world and they are constantly looking for opportunities for profit.

- **FINANCIAL CRIME / IDENTITY THEFT**
  - Scammers
  - Carders
  - Identity theft & fraud
  - They are people who commit financial fraud using stolen credit card data as well as online bank logins.

- **MONEY LAUNDERING**
  - Virtual currency sellers
  - Mules/Drops
  - They purchase large sums of virtual currencies such as WMZ and sell them in smaller quantities to carders.
  - Exchangers
  - They remove the need for identity verifications by the service provid-ers.

**Note:**
- flow of demand
- potential influence

THE UNDERGROUND ECONOMY CHAIN
Chinese underground economy
The “visa” “master” 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.
Forum

A Western-like carding forum.

Launched in July but has only 88 registered members to date.
Zombie machines “Flesh Chicken” are sold on Taobao, China’s equivalent to eBay.
Prices (1)

- Foreign carding goods are similarly priced as those observed in the West
- Chinese tracks are more expensive than Western tracks
Track stores such as ltdcc.com eliminates language barriers between Chinese and Western carders.
### Prices (3)

<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 $15 for 1000 household zombies $15 for 1500 traffic zombies/Internet café zombies $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
Big brother is looking...
Money laundering

- Chinese carders do recruit Chinese overseas students
- Claims to have been in operation for 6 years
- Also acquiring NETELLER accounts because not possible to register from CN
  - £35 – normal
  - £100 – NET+ card
Conclusion
Conclusion

- CN Hacktivists are perceived as heroes and leniency is clearly shown by the government
- Western carders prefer to operate in closed hierarchical forums while Chinese carders prefer to be open and decentralised
- Baidu and QQ are main facilitators of cybercrime in China
- Cybercrime in China is flourishing rapidly, with victims being those in the West
- Chinese and Western carders do trade with each other
Thank you!
Useful literatures


