

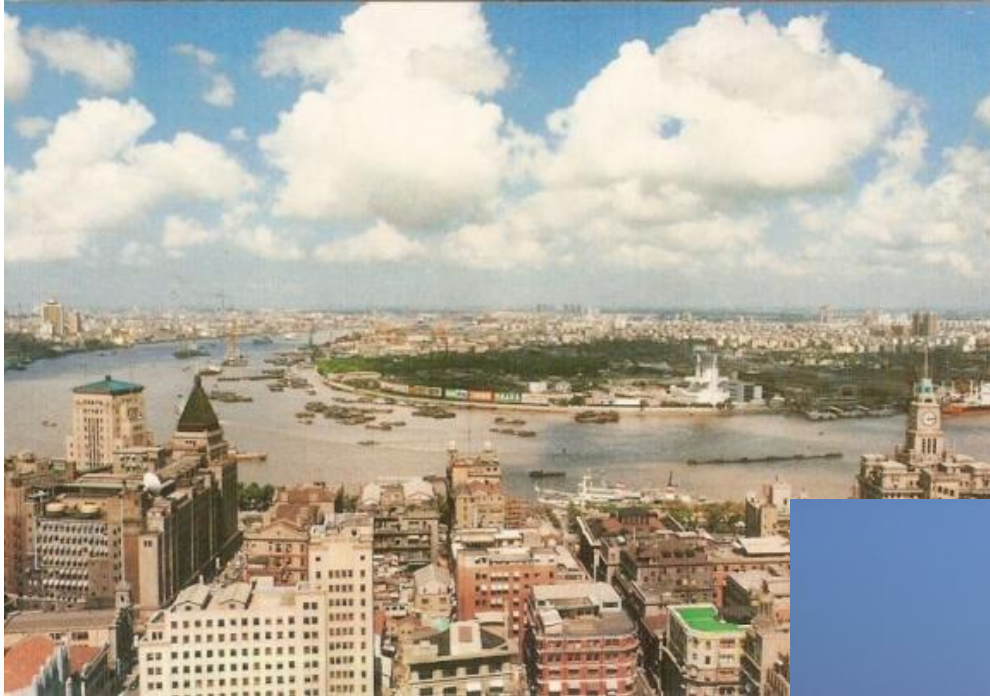
An investigation into Chinese cybercrime

and the underground economy in
comparison with the West

Michael Yip
02 November 2010



1990



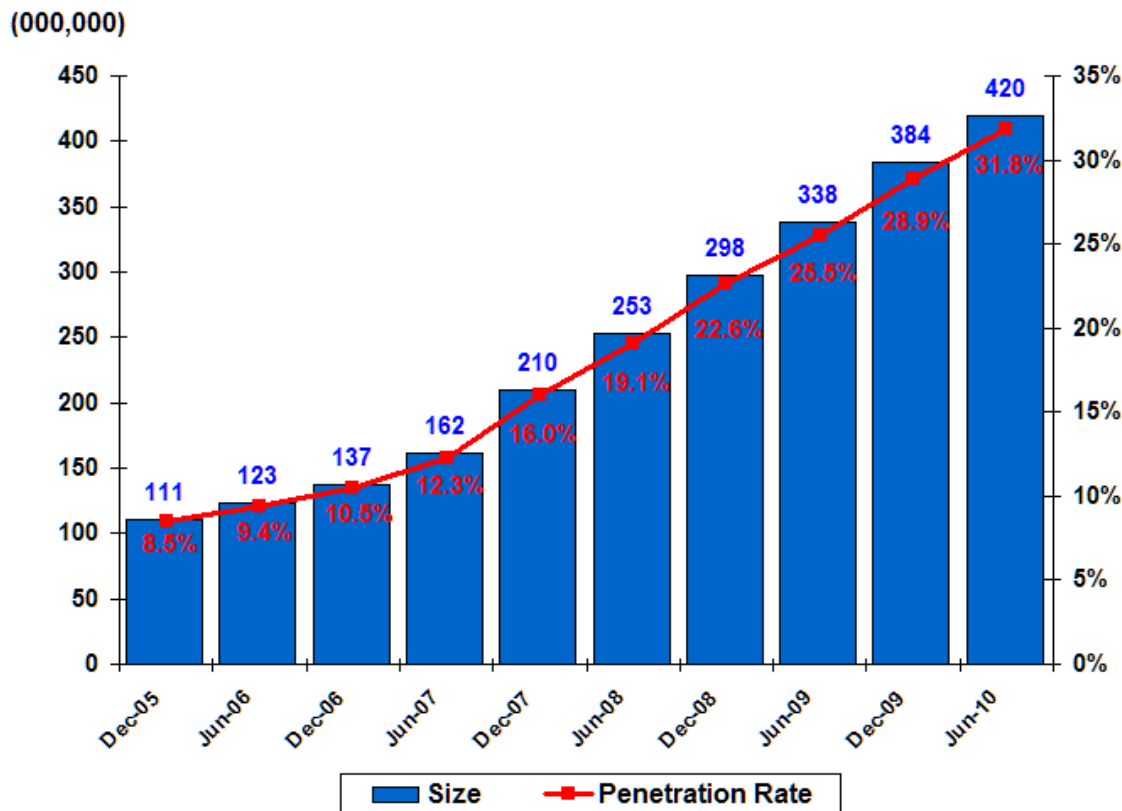
2010



Internet in China



**Chinese Internet Population Growth
(June 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
- Widening income inequality
- Results from an opinion poll on 163.com:
 - 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)

Source: Which level are you at? An investigation into the state of survival for the IT people, CNET News - <http://www.cnetnews.com.cn/2010/0311/1659908.shtml>

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 offenders were reported in the People's Daily newspaper to have committed cybercrime but official punishment was only reported for 13 offenders (Lu *et al.* 2010)

Sources: Lu, H., Liang, B. and Taylor, M. (2010) A Comparative Analysis of Cybercrimes and Governmental Law Enforcement in China and the United States. IN: *Asian Journal of Criminology*. DOI: <http://dx.doi.org/10.1007/s11417-010-9092-5>.
Qi, M., Wang, Y., and Xu, R. (2009) Fighting cybercrime: legislation in China. IN: *International Journal of Electronic Security and Digital Forensics*, Vol. 2(2) pp.219-227. DOI: <http://dx.doi.org/10.1504/IJESDF.2009.024905>

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\$276million
- 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”

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 3.8 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 + hacking

“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**’.”

Source: Callahan, W. (2004) *National Insecurities: Humiliation, Salvation, and Chinese Nationalism*

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

Source: Henderson, S. (2007) *The Dark Visistor*. LuLu Press. Also, his blog at <http://www.thedarkvisitor.com>.

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

Source: Henderson, S. (2007) *The Dark Visistor*. LuLu Press. Also, his blog at <http://www.thedarkvisitor.com>.

Famous groups (2)

PNEUMA COLLEGIUM

牛馬之夜

上海交通大学人文学院
牛马读书社系列讲座

主讲人：彭一楠

信息安全学院研三，资深黑客
牛马社前任召集人
上海市公安局信息安全顾问
国际注册信息系统安全专家(CISSP)
上海恩基网络技术公司运营总监兼安全总监

黑客，
无限赛博空间之王，
那什么是黑客？
黑客有哪些派别？
黑客用什么方式交流？
真正的黑客精神是什么，
和《金刚经》中的佛教思想
又有哪些暗合之处？
世界黑客目前的现状如何，
他们认为什么是对的？
为什么社会工程学
被认为是最有效的攻击手段？

I could be bounded in a nutshell and count myself a king of infinite space.
— Shakespeare, *Hamlet*, Act 2, Scene 2

果壳里的黑客
Hacker in a Nutshell

Poster designed by James LAO, BigCove Studio

地点：陈瑞球楼 114 时间：10月31日 19:00



Peng Yinan a.k.a.
“Coolswallow”

Source: Henderson, S. (2007) *The Dark Visitor*. LuLu Press. Also, his blog at <http://www.thedarkvisitor.com>.

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

Source: Henderson, S. (2007) *The Dark Visitor*. LuLu Press. Also, his blog at <http://www.thedarkvisitor.com>.

Famous groups (3)

红客联盟

首页 新闻中心 安全文档 红客学院

天行健,君子以自强不息

中國紅客

WWW.CHINESEHONKER.ORG

加入我们 join us 登录

论坛 搜索 插件 每日签到 资源中心 导航

H 中国红客联盟 » 首页

请输入用户名 安全提问 登录 注册

2010年11月2日 星期二 午夜好

公告: 红客联盟招贤纳士郑重宣言 (2010-9-12) 新人入门发帖必读 (2010-6-16) 论坛长期招聘版主 (2010-6-16) Nessus平台发布欢迎使用 (2010-6-14)

不是不能见义，怕的是见义而不勇为。一谢觉哉

社区图片	最新主题	最新回复	热门主题	随机精华	论坛明星	活跃会员
	1 中国红客联盟2010.09.18版主会议通知[HUC2010090801] 小5、飘飘	2 中国红客联盟第一届编程大赛[HUC2010090501HD号] 小5、飘飘	3 IP地址攻击工具 重型核武器(DDOS 2011超强版) nss090605073	4 红客联盟招贤纳士郑重宣言: [HUC2010091501号] Lyon	 guohao18	5 中国红客联盟重聚公告[HUC2010100401号] Lyon
	6 对忘月生怨处理公告 Lyon	7 按住两个键，你的电脑就会崩溃 xiaobo518518	8 中国红客联盟官方期刊《红》第一期发布[HUC201010010] fooying			

动态域名怎么办??? 急!!! 急!!! 1 2 3 4 5

今日: 222, 昨日: 1777, 会员: 112022

分区版主: 307724975

互动答疑	原创作品	论坛活动&期刊区
26 today 主题: 4022, 帖数: 28953 最后发表: 2010-11-2	8 today 主题: 247, 帖数: 9175 最后发表: 2010-11-2	0 today 主题: 6, 帖数: 610 最后发表: 2010-10-30

Famous groups (3)



★ 中国红客联盟 · 首页

发帖

你可以注册一个帐号，并以此登录，以浏览更多精彩内容，并随时发布观点，与大家交流。

最新图片

最新主题 最新回复 热门主题



- 1 日本四面树敌恐难承受
- 2 日本民主党干事长下月拟访华 望改善两国关系
- 3 日官员称俄总统视察北方四岛加剧日本困境 汉网-武汉晚
- 4 俄罗斯总统发微博解释登千岛群岛原因 新华网
- 5 外交部:日公布录像不能改变扣中国渔船非法性 京华时
- 6 拿下台湾第一站! 台湾黑客莫装B! ! ! ! ! ! ! ! ! !
- 7 新手上路
- 8 投诉! 我发的新手求助区的帖子为什么给我删了?

论坛版块 论坛动态

今日: 243, 昨日: 1499, 会员: 20118

官方公告

分区版主: 冰儿



行动规划 (今日: 3)

内部事项发布, 以及对外行动在此公布

版主: 冰儿

19 / 3083

中国红客联盟官方杂志《HONKER T ...
lwwh1016 - 半小时前

道，可道，非常道；名，可名，非常名。

中国红客

进入联盟社区

行动规划 部门机构 网站宗旨 成员召回 职位申请 友情连接

红盟原域名: www.chinahonker.com

现改为: 红盟中文域名: www.中国红客联盟.com 红盟英文域名: www.cnhonkerarmy.com

Cnhonkerarmy.com

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.

鉴于2010年9月18日这个有纪念意义的日子
决定对日本各大扭曲抗战历史。拥护台独的站点进行大规模的反抗
让日本鬼子知道中国人不再沉没。中国在崛起
今天,面对日本的种种作为我们深感遗憾,作为炎黄子孙的我们,作为任何一个有骨气的中国人,我们都不应该再沉默了,我们要用我们自己的方式,给日本敲响一个响亮的警钟,中国人民不是软弱可欺的!
在此原中国红客联盟(<http://www.honker.net>)核心号召广大爱国青年,广大电脑爱好者,广大黑客技术人员,于9月18日对日本发动网络作战,主要以瘫痪日本各大干线路由器和各大政府及商业网站为主(到时候会发布目标及方式)!届时还会组织我们的安全技术小组对日本各大网站挂上我们的旗帜,瘫痪日本服务器,删除数据,给日本来一次沉重的打击。
请愿意参加此次行动的朋友到 加群5209614 基础成员请在群共享熟悉武器并下载DF-5战术核导弹.exe 1.1MB, DDOS强力killertop版.EXE 28.5KB, 阿拉丁UDP攻击器V2.1.exe 1.3MB, 用此工具需时间统一才能发挥最大功力,核心入侵组成员将使用其他方法入侵! 工具为内部专用!
去看我们的前期计划和准备,并加入我们的小组,和各战队备案! 长期攻击对象为:美,日,印尼,印度,越南,菲律宾。。
官方核心群27437332 邀请加入制

附: 目标

<http://www.kantei.go.jp>首相官邸
<http://www.jinji.admix.go.jp>人事院
<http://www.clb.admix.go.jp>内阁法制
<http://www.sorifu.go.jp>总理府
<http://www.jftc.admix.go.jp>公正取引委员
<http://www.npa.go.jp>警察厅
<http://www.kouchoi.go.jp>公害等调整委员
<http://www.kunaicho.go.jp>宫内厅
<http://www.somucho.go.jp>总务厅

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

Chinesehonker.org (honker.net)

- 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

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.. .



Message on defaced websites by cnhonkerarmy.com

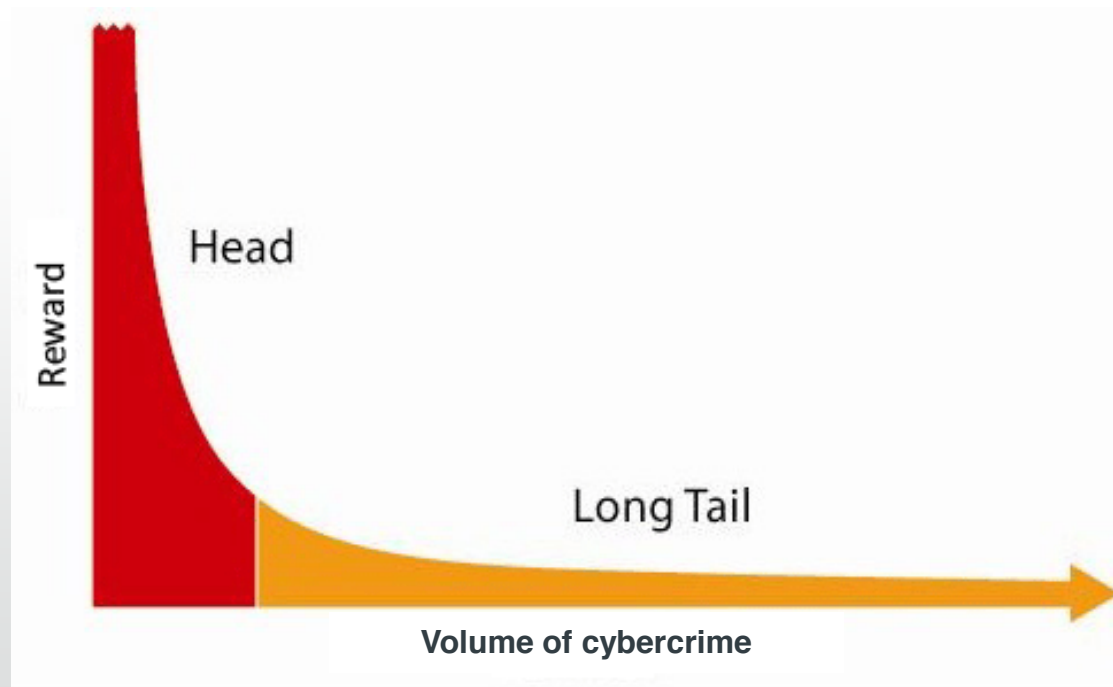
Attribution to Chinese government

- 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 matured
- Hierarchical management preferred
- Carding oriented – the unauthorised use of third party credit card details for personal gain

Carding forum - Shadowcrew

SHADOWCREW FOR THOSE WHO WISH TO PLAY IN THE SHADOWS			
FAQ Search Memberlist Usergroups Register Profile Login to check your private messages Login			
The time now is Tue Sep 03, 2002 5:03 pm shadowcrew Forum Index		View unanswered posts	
Forum	Topics	Posts	Last Post
Discussion Forums			
 Identification Technical discussion on Novelty Identification, 2nd ID, Passports, and the like.	116	667	Tue Sep 03, 2002 4:50 pm Deck 
 Cyberspace Discussion about online anonymity and tools to hide your online presence.	26	89	Tue Sep 03, 2002 4:59 pm Deck 
 Credit Discussion concerning credit cards, credit bureaus, credit reports, and credit services.	9	40	Mon Sep 02, 2002 6:29 pm Deck 
 Qualification Discussion of Diplomas, Employment References, Job searches, Transcript, Etc	4	5	Tue Sep 03, 2002 5:42 am OntheFringe 
 The Lounge Anything goes in this forum. Take your battles and personal matters into the lounge.	13	53	Tue Sep 03, 2002 4:39 pm Deck 
Vendors and Reviews			
 Vendors/Reviews Find out what vendors offer and who delivers.	15	77	Tue Sep 03, 2002 3:33 am NTT 
 Scamming Bastards Tell everyone who ripped you off and maybe save the newbies a few dollars.	5	10	Sun Sep 01, 2002 9:40 pm benq 
Archives			
 Tutorials and How-To's Learn from those who came before you.	57	75	Tue Sep 03, 2002 11:47 am OntheFringe 
Forum BS			
 Forum Discussion Suggestions, complaints, bitches, moans, whatever.	26	182	Sun Sep 01, 2002 10:16 pm fusi0nX 
 Trashed Topics You don't want your thread to end up here!	2	2	Fri Aug 30, 2002 12:37 am kidd 

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.

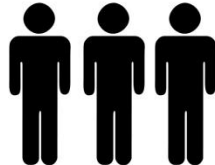
Cybercrime in the West

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.



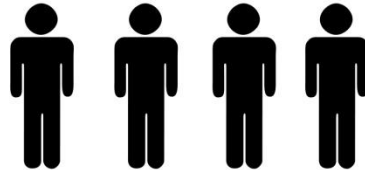
Administrators

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.



Moderators

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.



Reviewers

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



Reviewed vendors



Members

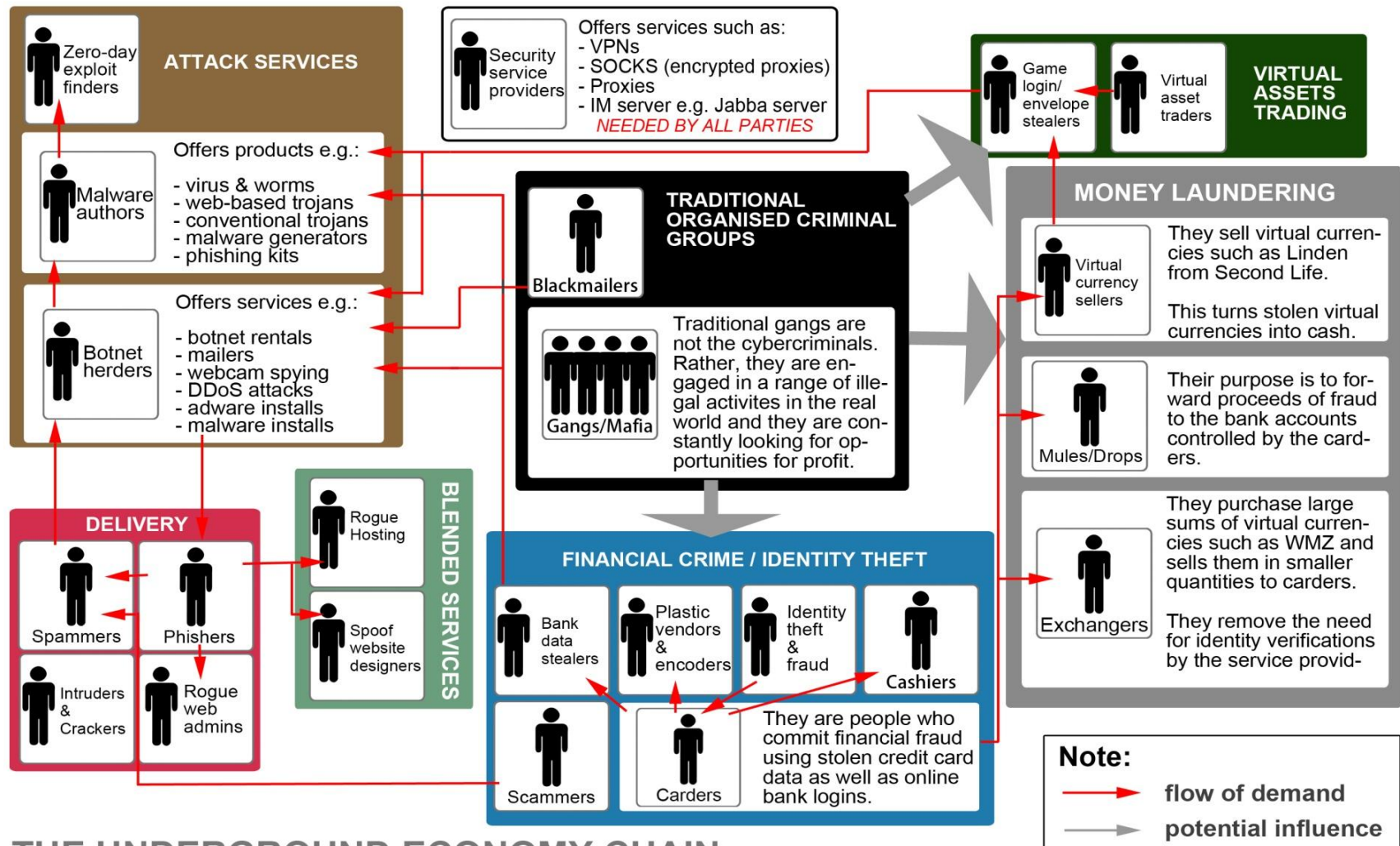
Hierarchical structure of Western Carding Forums

Typical management hierarchy in Western carding forums

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)

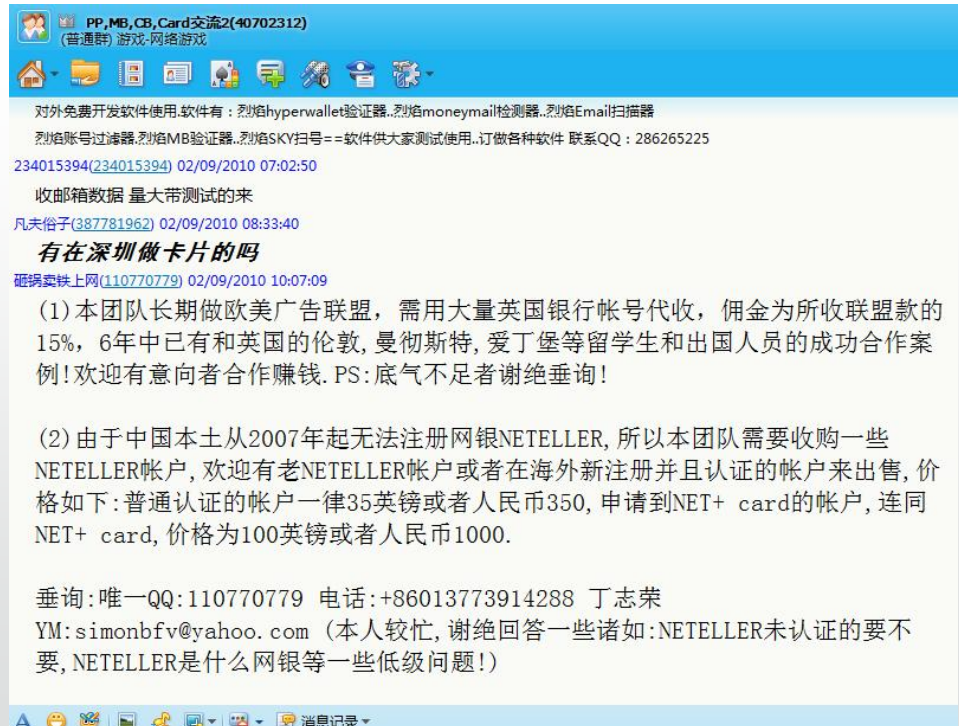
A general model of cybercrime



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



PP, MB, CB, Card交流2(40702312)
(普通群) 游戏-网络游戏

对外免费开发软件使用.软件有:烈焰hyperwallet验证器..烈焰moneymail检测器..烈焰Email扫描器
烈焰账号过滤器..烈焰MB验证器..烈焰SKY扫号==软件供大家测试使用..订做各种软件 联系QQ: 286265225

234015394(234015394) 02/09/2010 07:02:50
收邮箱数据 量大带测试的来

凡夫俗子(387781962) 02/09/2010 08:33:40
有在深圳做卡片的吗

砸锅卖铁上网(110770779) 02/09/2010 10:07:09

(1) 本团队长期做欧美广告联盟, 需用大量英国银行帐号代收, 佣金为所收联盟款的15%, 6年中已有和英国的伦敦, 曼彻斯特, 爱丁堡等留学生和出国人员的成功合作案例! 欢迎有意向者合作赚钱. PS: 底气不足者谢绝垂询!

(2) 由于中国本土从2007年起无法注册网银NETELLER, 所以本团队需要收购一些NETELLER帐户, 欢迎有老NETELLER帐户或者在海外新注册并且认证的帐户来出售, 价格如下: 普通认证的帐户一律35英镑或者人民币350, 申请到NET+ card的帐户, 连同NET+ card, 价格为100英镑或者人民币1000.

垂询: 唯一QQ: 110770779 电话: +86013773914288 丁志荣
YM: simonbfv@yahoo.com (本人较忙, 谢绝回答一些诸如: NETELLER未认证的要不要, NETELLER是什么网银等一些低级问题!)

The Chinese underground economy

Baidu Tieba (1)

Baidu 贴吧 新闻 网页 贴吧 知道 MP3 图片 视频 百科

visa 百度一下 吧内搜索 | 帮助

进入贴吧 进入贴吧 帖子搜索

visa吧 精品区 | 投票区 | 游戏区 | 聊聊天 **NEW** 发表新贴

精品区: visa-vip

点击	回复	标题	作者	最后回复
--	--	警示收费删贴等诈骗行为[公告]	贴吧公告	----
71	4	大量求购欧洲卡~~~月需求3W元	大量求购卡	10-30 大量求购卡
231	17	一手料站 大量 US JP DE 等各国料 寻求合作	诚心求学了	10-30 221.238.38.*
31	0	收山。打包卖一切，通道若干。	218.76.139.*	10-30 218.76.139.*
148	14	有需要的请进	出卡110	10-30 z30058180
34	1	长期销售各国优质卡	joe lin	10-30 222.170.238.*
1009	59	小弟来个猛的，免费收徒弟，这在吧里什么水平？	yes19601230	10-30 221.206.175.*
255	20	招合作人一起赚钱，有胆识的人进来！	218.6.15.*	10-30 221.206.175.*
556	32	大量一手 DE UK VM卡包过 AION 赌场 等等~~(欢迎大家定购)留下你	222.84.164.*	10-30 221.206.175.*
216	5	虚拟Visa卡交易交流	115.193.230.*	10-30 221.206.175.*
257	28	1手高质量US可包过 可测试 过了给钱 需要的留QQ	hszskihh	10-30 a443987778

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.

Baidu Tieba (2)

共有35篇贴子 [1](#) [2](#) [下一页](#) [尾页](#)

大量一手 DE UK VM卡包过 AION 赌场 等等~~ (欢迎大家订购)留下你

» 转贴并收藏

1楼

222.84.164.* 大量一手 DE UK VM卡包过 AION 赌场 等等~~ (欢迎大家订购)留下你们的QQ我经常上来加的

2009-12-14 23:47 [回复](#)

2楼

58.52.202.* 710151152

2009-12-14 23:54 [回复](#)

3楼

117.90.100.* 576-459-338 大量求购包过AION UK卡

2009-12-15 00:16 [回复](#)

4楼

59.62.142.* 大量要欧美能过AION的卡
4 6 2 2 5 7 9 4 1

2009-12-15 00:34 [回复](#)

6楼

819845324

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

登录 注册

Fuck Bank
00 00 00 FUCH THE BANK!

Fuck Bank Web ICQ 验证商家押金全已达：7500¥ 我的快捷通道 搜索 高级

输入用户名 登录 注册
今日:0 | 昨日:0 | 最高日:12 | 标记已读
社区应用 最新帖子 精华区 社区服务 会员列表 统计排行 银行
主题:61 | 帖子:100 | 会员:59 | 新会员:chousan 83%

论坛验证商家、推荐商家火热招募中! 10-07-20

» 无奸不商

版块	主题 / 文章	最后发表
商家推荐 推荐、验证商家介绍 验证、推荐商家申请 与本版介绍商家交易，受本站先行赔付保护。 版主：	8/13	Re:本站首位验证商 .. admin 2010-08-16 19:09
交易中心 站友交易，申请站长先行赔付请按照置顶帖格式发布。 版主：	17/37	回 12楼(admin) 的帖子 花果山猿 2010-10-20 09:59
骗子揭发 欢迎举报各类骗子，让骗子曝光于大众！！ 发布骗子的ICQ QQ 支付宝 WMZ LR等交易联系方式 尽量让新来的朋友少上当。 版主：	6/16	Re:郁闷，刚刚被骗 admin 2010-08-16 19:06

» 知识就是金钱

版块	主题 / 文章	最后发表
DUMP相关 发布关于DUMP相关知识以及技巧 版主：	2/4	我真的不懂，拿1轨 .. admin 2010-09-14 01:42
CV V 相关 发布C V V相关知识与学习文字 版主：	1/1	VISA卡校验值CVV的计 .. admin 2010-08-07 23:56

A Western-like
carding
forum.

Launched
in July but
has only
59
registered
members
to date.

Others

淘宝网

所有分类 > 腾讯QQ专区 > 宝贝详情

肉鸡出售 家鸡出售 保证全是家鸡



分享给好友

收藏该商品

宝贝 店铺

输入您想要的宝贝

Q 搜索

一口价: **0.20** 元

运费: 卖家承担运费

30天售出: **1209** 件 (查看评价)

付款方式: 支付宝卡通 网银支付 找人代付 消费卡
网点支付 支付宝余额

我 要 买: 件 (库存8420件)

立即购买

所在地区: 北京

宝贝类型: 全新

浏览次数: 206次

收藏人气: 1 (类似收藏)

掌柜档案

小贩仔520 给我留言

会员信用

累计信用:

好评率: 85.71%

店铺动态评分

宝贝与描述相符: ★★★★★ 4.6

卖家的服务态度: ★★★★★ 4.7

卖家发货的速度: ★★★★★ 5.0

挑选更多商品
进入掌柜店铺

收藏本店铺 发站内信件

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

Goods	Western Price (USD)	CN Price (USD) per unit
UK credit cards + cvv2	\$0.50 - \$12	Normal - \$3.7 - \$5 With 3D - \$22 - \$44
US credit cards + cvv2	\$0.50 - \$12	Normal - \$1.7 - \$2
FR credit cards + cvv2	\$0.50 - \$12	Normal - \$5.9
CN credit cards + cvv2	\$0.50 - \$12	Normal - \$17
UK 101/201	N/A	Track 101: Classic = \$1.47 per track Gold = \$1.76 per track Platinum = \$2.06 per track Track 201: Classic = \$1.34 to 1.63 per track Gold = \$1.63 to \$2.08 per track Platinum = \$1.93 to \$2.53 per track U.S. Discover = \$15
US 101/201	N/A	Track 101: Classic = \$1.26 per track Gold = \$0.89 to \$1.71 per track Platinum = \$1.19 to \$1.937 per track
FR 101/201	N/A	Track 201: V/M = \$11.9 per track
Japan 101/201	N/A	Track 201: JCB = \$14.89 V/M = \$10.42
Dumps	\$4 - \$150	\$74.46
Bank logins	\$15 - \$850	Bank BOA Us: Balance \$7000 = \$300 Balance \$14000 = \$500 Balance \$18000 = \$800 Bank HSBC (US): Balance \$12000 = 400 Balance \$28000 = 1000 Bank HSBC (UK): Balance GBP 8000 = \$300 Balance GBP 17000 = \$700

Goods	Western prices (USD)	Price (USD) per unit
Trojans (木马)	\$15 - \$40	Target China banks (ICBC and BC): \$22.33
Anti-security(木马免杀)	N/A	Guaranteed effective: For 10 days = \$14.89 For one month = \$29.78 to \$44.67
Trojan generator	N/A	\$4.46 - \$298

Prices (2)

Services	Western Price (USD)	CN Price (USD) per unit
Zombie sales	A botnet can be sold for \$550 including hosting	\$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
DDoS attacks (DDoS 攻击)	\$60 - \$80 per day	\$89 to \$298 (24 hour attack)
Money laundering/Mule service/Cashier	N/A	50:50 split
Hacking training/tutorial	N/A	\$22 to \$149 (per student)
IP address	N/A	10,000 IPs = \$18

- 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

Prices (3)

Home

CC

Notifier

Cart

Orders

Billing

Rules/FAQ

Tickets

Checker

Profile

Logout

Filter:

BINs: (+0.5\$)

Country: US (29041)

State: (+0.5\$) all

City: (+0.5\$) Select state

Zip: (+0.5\$)

Type: All

VISA

Mastercard

Discovery

AmEx

Search

Reset

Cards in DB: 29382

BIN	Name	Exp	City	State	Country	ZIP	Price	
██████	Debi	03/11	██████	██	US	████	1.50+0	
██████	Tiffany	03/11	██████	██	US	████	1.60+0	
██████	tiry	03/11	██████	██	US	████	1.60+0	
██████	Penny	03/11	██████	██	US	████	1.60+0	
██████	Jeannie	03/11	██████	██	US	████	1.60+0	
██████	Jeannine	03/11	██████	██	US	████	1.60+0	
██████	alfred	03/11	██████	██	US	████	1.60+0	
██████	Mindy	03/11	██████	██	US	████	1.60+0	
██████	dawn	03/11	██████	██	US	████	1.60+0	
██████	Janet	03/11	██████	██	US	████	1.60+0	
██████	John	03/11	██████	██	US	████	1.60+0	

Balance: 0.00\$

ADD MONEY!

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

Henderson, S. (2007) *The Dark Visitor – Inside the World of Chinese Hackers*. Lulu Press.

IOSC of the PRC (2010) *The Internet In China*. Available from: http://www.gov.cn/english/2010-06/08/content_1622956.htm#.

Krekel, B. (2009) Capability of the People's republic of China to Conduct Cyber Warfare and Computer Network Exploitation. *U.S.-China Economic and Security Review Commission*. Available from: http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf.

Qi, M., Wang, Y., and Xu, R. (2009) Fighting cybercrime: legislation in China. IN: *International Journal of Electronic Security and Digital Forensics*, Vol. 2(2) pp.219-227. DOI: <http://dx.doi.org/10.1504/IJESDF.2009.024905>.

Zhuge, J. et al. (2008) Studying Malicious Websites and the Underground Economy on the Chinese Web. IN: *Proceedings of the 7th Workshop on the Economics of Information Security (WEIS'08)* Hanover, NH, USA, June 2008. Available from: <http://weis2008.econinfosec.org/papers/Holz.pdf>.

Zhuge, J. et al. (2007) Characterizing the IRC-based Botnet Phenomenon. IN: *Peking University & University of Mannheim Technical Report*. Available from: http://www.honeynet.org.cn/downloads/publication/TR_IRC_Botnet.pdf.

Thank you!