中国互联网信息安全地下产业链调查

诸葛建伟[1]，谷亮[2]，段海新[1]

1 清华大学信息与网络安全实验室，CCERT 应急响应组
2 趋势科技中国公司

摘要：支撑许多网络犯罪的中国互联网信息安全地下产业链经历了多年的快速增长，但始终没有引起中国安全界的足够关注。在本文中，作者对中国互联网信息安全地下产业链进行了一次广泛且深入的结构性调查与实证数据分析，展示出地下产业链的当前情况、内部特征以及发展趋势。作者的测算显示，在 2011 年，由中国互联网信息安全地下产业链造成的总体损失超过 53.6 亿元人民币，监测到地下黑市参与者人数超过 9 万人。在有效的遏制手段出现之前，地下产业链活动与参与者数量仍将呈现出快速增长的态势。作者还进一步验证了监测地下黑市信息有助于对一些正在发生的网络犯罪案件进行早期监控与调查。

关键字：地下产业链；信息安全；网络犯罪；地下黑市

关于作者：

诸葛建伟，博士，清华大学网络与信息安全实验室副研究员，狩猎女神科研团队负责人，CCERT 应急响应组成员。在加入清华大学之前，在北京大学计算机系取得学士与博士学位，并在计算机科学技术研究所担任教学科研工作，历任助理研究员与副研究员。曾获得 IBM 全球博士生英才、微软学者、北京大学五四青年科学奖。目前研究领域为网络与系统安全，研究兴趣包括网络安全威胁监测、安全漏洞分析与利用、恶意代码分析与检测、网络犯罪地下经济链调查等，在国际知名安全会议、国内一级期刊上发表学术论文 30 多篇，截止 2012 年 6 月，Google Scholar 文献引用超过 450 次，H-index 为 11。著有《网络攻防技术与实践》、《Metasploit 渗透测试技术指南》等畅销书籍。

谷亮，趋势科技中国公司资深研究员，目前研究兴趣关注于恶意代码分析、移动安全与网络犯罪地下经济链调查。在天津理工大学取得电子信息工程专业学士学位。

段海新，博士，清华大学网络与信息安全实验室研究员，实验室主任，CCERT 应急响应组负责人，目前在美国伯克利大学国际计算机科学研究所访问研究。在清华大学计算机系取得博士学位。研究兴趣包括网络入侵检测、DNS 安全和匿名通信等。

目　　录

1. 引言

从 2008 年中国互联网网民数量跃居世界第一位以来，中国互联网仍然以惊人的速度快速发展。根据 CNNIC 报告，截至 2011 年 12 月底，中国网民规模突破 5 亿，达到 5.13 亿，其中手机网民规模达到 3.56 亿，即时通讯、网络游戏等沟通娱乐类应用用户规模均超过 3 亿，而网络购物、网络支付、网上银行等电子商务类应用也稳步发展，用户规模均超过 1.6 亿[CNNIC 2012]。而与此同时，中国互联网网民在上网期间则频繁地遭遇到安全威胁，根据腾讯 QQ 电脑管家对 2000 名网民开展的调查问卷显示，45.5%用户曾遭遇即时通讯账户被盗，32%网民遭遇游戏账号被盗号，而遭遇虚假中奖等网络钓鱼信息则更为频繁，最终导致支付被劫持或网银被盗窃的也分别有 5.8%和 5.6%的用户比例[电脑管家年报 2012]。而年底的 CSDN、天涯等网站发生大量用户信息泄露事件引起了社会广泛关注[CSDN 事件 2012]，而 2012 年央视三一五晚会曝光多家银行内部员工出售用户个人资料导致数十位用户网银余额被窃超过 300 多万元的案件[央视 315 2012]，也让互联网个人信息与上网安全成为舆论焦点。

在这些互联网安全威胁的背后，大多有着信息安全地下黑色产业链的身影。由巨额经济利益的驱动，一些网络不法分子使用各种网络犯罪技术手段，并利用目前社会大众在个人信息资料安全和网络安全的各个薄弱环节，组织起具有明确社会角色分工并拥有多重环节的地下产业链，通过各种可能的非法盈利链条危害网民大众的财产安全，攫取大量的非法收入。随着地下产业链的不断发展与壮大，不法分子们也建立了大量隐藏在互联网阴暗角落中的地下黑市。地下黑市为不法分子们提供了产业链中非法商品、服务的交易平台，以及他们之间的通讯平台，是地下产业链赖以运转的联系纽带。

由于信息安全地下产业链以违背法律与社会道德来谋取巨额非法收入，因此很自然地采取隐秘地方式来实施各种在线攻击和利益攫取。然而与毒品贩卖等物理世界犯罪产业链不同的是，信息安全地下产业链以攻击和利用互联网用户盈利，所涉及的非法商品服务以及最终攫取的金钱都可以依赖互联网进行传输与实施，因此这一独特的地下产业链完全依托于互联网，联系整个地下产业链的黑市交易与通讯也大多利用互联网服务与应用。在公开访问的互联网上，信息安全地下产业链通常仅靠一些内部行话术语来保证地下黑市对外界的隐蔽性，为了吸引新的参与者加入并保持黑市的高效运行，地下产业链的黑市是比较开放的，这也为通过黑市监测了解地下产业链提供了可能性，只要研究者对产业链结构进行深入了解并破译内部行话，便可以深入到各个地下黑市中进行观测。而参与黑市的不法分子们则会进一步采用即时通信与论坛匿名用户、冒用身份资料、隐藏 IP 地址等各种方法，来尝试躲避执法部门的追查。

信息安全地下产业链不仅仅在中国互联网上存在，互联网信息技术与应用更加发达普遍的西方发达国家更早出现了地下产业链，也吸引了一些研究者对地下产业链开展监测研究工作[Thomas 2006][Franklin 2007][Holt 2010]，向安全社区和社会大众揭露出地下产业链的存在与危害。

由于中国在互联网应用领域与西方国家的巨大差异，以及中国在经济社会结构、信息安全相关法律法规、网民互联网使用习惯等方面的独特性，中国互联网的信息安全地下产业链经过多年发展与演变，与西方国家有着较大的差别，因此针对中国互联网信息安全地下产业链的深入研究，以及与西方国家的相关研究进行对比，将有助于在全球范围内更好地通过协作来应对地下产业链所驱动的网络犯罪问题。

然而，中国互联网的信息安全地下产业链并没有得到国内安全研究领域的充分关注，国家网络安全监管部门与执法部门在针对造成重大社会影响与危害的网络犯罪案件处理中，已

经了解到地下产业链的存在及其对网络犯罪的推动作用，也进行了一些基础性的总结分析[陈明奇 2006][杜跃进 2007]，一些媒体记者在跟踪报道一些由地下产业链所驱动的网络犯罪案件中，也对地下黑市进行了个案调查和曝光。但均未能采用系统性的研究方法，通过对地下黑市的监测分析与威胁数据统计，全面地揭示出地下产业链的结构、规模与内在规律。本文作者于2007年至2008年初对当时中国互联网上最猖獗的网络虚拟资产盗窃地下产业链进行了结构分析，并通过对地下黑市与虚拟资产公开市场的监测分析，较为系统性地给出了这一主要地下产业链的规模状况与分布规律，同时对这一产业链通过挂马网站植入盗号木马的技术流程进行细致分析，通过抽样检测验证其对中国互联网造成的严重威胁[Zhuge 2008a][Zhuge 2008b]。

本文对之前工作进行了进一步扩展，首次对中国互联网信息安全地下产业链进行全面深入的结构调查与实证数据分析研究。本文主要的贡献点包括：

(1) 对中国互联网的信息安全地下产业链进行全面深入的结构分析，尝试揭示出主要的产业链盈利链条和实施技术手段，并标识出各个产业链盈利链条的环节与角色分工。
(2) 利用国内主流安全厂商、网络安全监管部门的安全威胁统计数据，以及国内相关行业的市场调查报告，首次对中国互联网信息安全地下产业链的整体盈利规模与危害人群进行了细致测算。
(3) 通过对 Web 论坛与 QQ 群方式构建的地下黑市信息进行长期持续监测，给出了中国互联网地下产业链现状、发展规律与趋势分析。
(4) 首次采用公开网络犯罪案件关键信息与地下黑市监测信息的关联分析，验证了监测地下黑市对支持网络犯罪案件调查的支持作用。

本文以下内容将按如下结构组织：第 2 节对中国互联网信息安全地下产业链进行结构分析，第 3 节给出信息安全地下产业链的实证数据分析，第 4 节介绍本文的相关研究工作并进行对比，最后在第 5 节中给出结论。

2. 中国互联网信息安全地下产业链结构

根据对中国互联网信息安全地下产业链盈利模式与关联结构的调查分析，我们将其组织成如**图 1** 所示的地下产业链总体结构，分为真实资产盗窃、网络虚拟资产盗窃、互联网资源与服务滥用、黑帽技术工具与培训这四大产业链，同时给出了它们之间的相互依赖关系，其中黑帽技术工具与培训产业链作为整个产业链的根源，为其他三大产业链都提供了技术基础；而互联网资源与服务滥用产业链则为真实资产盗窃、网络虚拟资产盗窃这两大产业链提供了网络资源条件。产业链的参与者都可以取得现实社会中的非法或不当利益，这也驱使了信息安全地下产业链的不断发展与膨胀。

本节中，我们将从产业链结构分析、角色与行话分析、各个环节技术手段剖析、典型案件研究这几个方面，来对**图 1** 中的四大地下产业链进行深入分析与阐述。

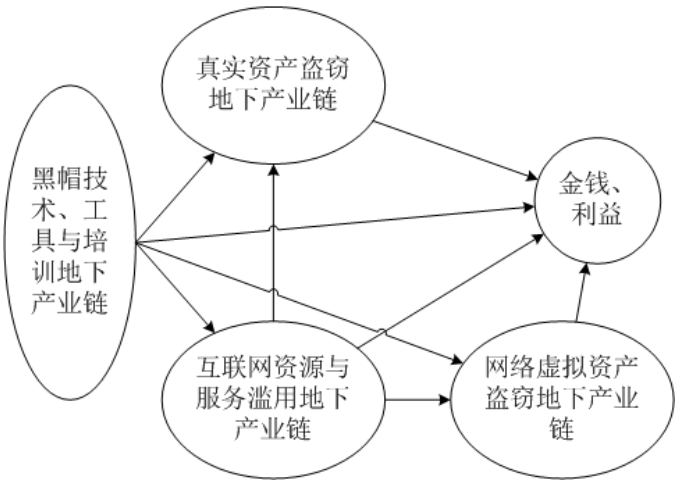


图 1 中国互联网信息安全地下产业链总体结构

2.1 真实资产盗窃地下产业链

真实资产盗窃地下产业链是中国互联网犯罪案件的首要驱动因素，由于直接涉及中国广大网民在互联网上的真实资产与个人财务隐私信息，因此可以为参与地下产业链的网络犯罪者攫取到实际的经济利益回报，并对网民的真实财产安全造成严重危害。

涉及真实资产的网络购物、网上支付、网上银行、旅行预订、网络炒股等商务交易类应用在中国互联网上一直保持稳步发展态势，截止 2011 年底，网络购物用户规模达到 1.94 亿人，使用率提升至 37.8%，网上支付、网上银行、旅行预订、网络炒股用户规模也分别达到 1.67 亿、1.66 亿、0.42 亿和 0.4 亿[CNNIC 2012]。庞大的用户群体以及其中蕴含的巨大财产规模吸引了为数众多的不法分子参与到真实资产盗窃地下产业链中，甘愿冒着被法律制裁的风险，想方设法地通过各种途径来盗窃或骗取网民真实资产，获得非法利益。

2.1.1 真实资产盗窃地下产业链结构分析

通过多年发展，目前中国互联网上的真实资产盗窃地下产业链已经形成了如**图 2** 所示的结构。

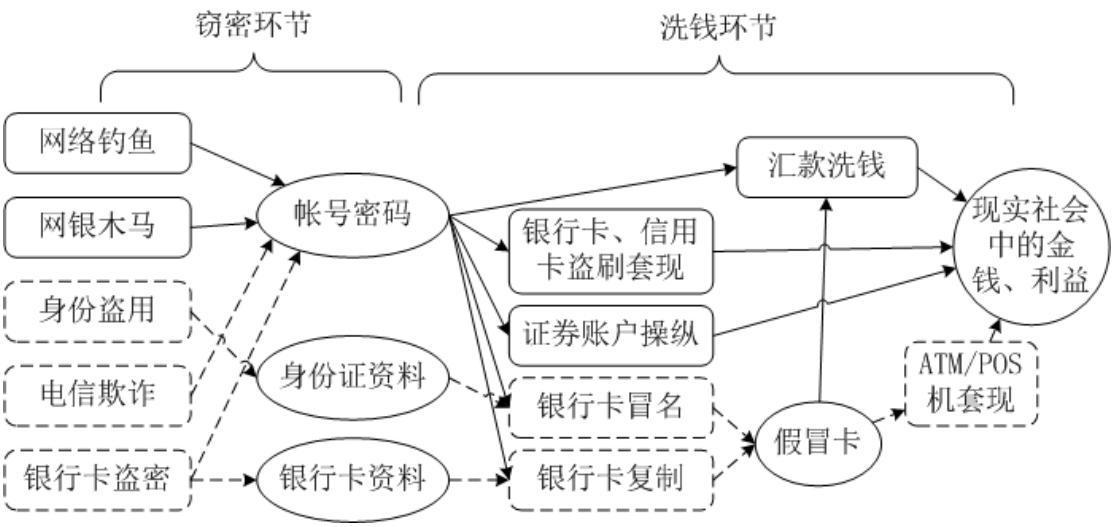


图 2 真实资产盗窃地下产业链结构

互联网上的真实资产主要包括银行账户存款、信用卡的信用额度、网络支付账户余额、股票与基金账户资产等多种类型，而资产所在的账户大都采用账号与密码进行互联网上的访问授权认证，因此这些账号密码就成为了真实资产地下产业链中不法分子首要的攫取对象。而窃取这些账号密码就构成了真实资产盗窃地下产业链的窃密环节。

在中国互联网上，网络犯罪者目前主要使用网络钓鱼（Phishing）和网银木马（Bank Stealing Trojan Horse）这两种技术手段，来尝试获取真实资产账户的账号密码，具体形态包括网银账号卡密、在线支付账号卡密、信用卡号与密码、股票基金账号卡密等。网络钓鱼是一种利用社会工程学和技术手段盗窃消费者个人身份资料和金融账号凭证的身份信息在线窃取活动。而网银木马则是特洛伊木马恶意代码中的一类，以窃取用户网银、信用卡、在线支付、股票证券等账号信息为主要目的。

除了这两种网络技术手段之外，犯罪者还利用了电信诈骗、银行卡盗密等犯罪手段骗取或盗窃账号密码与银行卡磁道等信息。电信诈骗主要借助于电话、手机通讯网络，使用任意显号软件、VoIP 电话、群发短信等技术手段，冒充公安局、银行、法院等工作人员身份实施社会工程学攻击，往往以受害人银行存款资金安全为借口，骗取受害人汇转资金，或给出网银账号卡密信息。银行卡盗密犯罪手段则通过对银行 ATM 机、ATM 门禁、商家 POS 机进行恶意改装，安置读卡器和摄像头，甚至于“山寨”ATM 机，从而套取受害人的账号密码和银行卡资料，最后通过复制卡或假冒卡，在 ATM 机或 POS 机上窃取账户存款或套现。虽然这两种犯罪手段并不属于互联网犯罪的范畴，但与互联网上的真实资产盗窃地下产业链非常紧密地交织在一起，首先这些犯罪手段也充分利用了如 VoIP 电话等互联网技术，同时通过这些犯罪手段窃取的账号密码和银行卡资料也有相当一部分流入了互联网地下黑市中进行交易或合作。因此我们在**图 2** 所示的真实资产盗窃地下产业链中，也包含这些互联网渠道之外的犯罪手段，并采用虚线进行区别表示。

网络犯罪者在获取到真实资产的账号密码信息之后，便会进入洗钱环节，他们会尝试在地下黑市中进行出售，或是通过地下产业链组织起合作性犯罪团伙，进一步对账户中的真实资产进行汇款洗钱、银行卡冒名、银行卡与信用卡盗刷、证券账户操纵等行为，从而最终从中窃取到金钱或非法利益所得。为了躲避执法部门的追查，网络犯罪者通常采用线下的身份盗用手段，购买取得大量身份证资料，并办理假冒银行卡，通过假冒身份进行多次汇款转账的方法，或者假冒卡 ATM 机取现、POS 机套现方式，隐蔽地取得非法收益。

由于涉及银行账户的真实资产盗窃案件危害重大，因此也一直是中国执法部门重点打击

的对象。2011 年，中国公安机关开展了代号为“天网-2011”的打击银行卡犯罪专项行动，重点打击伪卡类、套现类和涉网类等主观恶意程度高、涉案金额大的银行卡犯罪案件，全国共计破获案件2.4万余起,挽回经济损失4亿元。在公安部公布的十大案例中[公安部 2011]，除了 5 项信用卡非法套现案件之外，其他 5 个案件均与互联网真实资产盗窃地下经济链密切相关。例如在浙江湖州“3·28”特大网络信用卡诈骗案中，犯罪团伙从互联网地下黑市购买“网络钓鱼”程序，并以网站出售畅销商品为诱饵实施网络钓鱼，窃取网购顾客的银行卡账号密码资料，然后再实施信用卡盗刷，获取巨额非法所得，而在此案中犯罪团伙使用 QQ 作为联系手段，作案人员分布于 10 个省市，受害人数众多，是一起典型的通过互联网地下产业链组织实施的真实资产盗窃案件。湖南衡阳妨害信用卡管理案中，犯罪嫌疑人利用地下产业链上线提供的他人身份证办理假冒银行卡，公安机关攻击收缴涉案信用卡 8,000 余张，身份证 5 万余张，而每张假冒银行卡以每张 60-80 元价格卖给上线，用于其他犯罪，这是近年来公安机关破获的冒用他人身份信息办理银行卡数量最多的案件，体现了冒用他人身份办理的银行卡在真实资产盗窃地下产业链中的作用。此外还包括通过境外网站购买信用卡资料制作伪卡，并实施刷卡消费或套现的两个案件，缴获伪造境外银行信用卡分别为 1.88 万张和 7,000 余张。

2.1.2 真实资产盗窃地下经济链角色与行话分析

在地下产业链行话中，银行卡账号密码被称为“信封”或“信”，而不法分子用来收取账号密码的电子邮箱、在线 Web 应用程序等则被称为“箱子”。而包含银行卡磁道的窃取信息则通常称为“资料”、“轨道料”，或简称“料”。因此通过窃密环节获得银行卡资料，并在地下产业链中出售的不法分子的角色就被称为“料主”。

而洗钱环节也被称为“洗信”或“洗料”，从事这项活动的角色称为“洗信人”或“洗料人”，而实施伪造复制卡或假冒卡取现套现的过程称为“刷货”，角色称为“车主”（团伙头目）与“车手”（马仔），是整个地下经济链中风险最高的部分，通过非法渠道取得商家 POS 机可提供盗刷或取现资源的角色被称为“机主”。

2.1.3 真实资产盗窃互联网犯罪技术手段剖析

- **针对真实资产账户的网络钓鱼技术手段剖析**

网络钓鱼（Phishing）是目前中国互联网上实施真实资产账户密码窃取最主要的网络犯罪技术手段，并在地下产业链的支持下，形成了“设计—传播—实施”一条龙的完整流程。网络犯罪者通常从地下产业链中购买一些现成的网络钓鱼工具程序，然后针对流行的网银、网购与在线支付等目标网站搭建相似度极高的钓鱼网站，并通过群发邮件或信息等技术手段传播钓鱼网站链接，使用优惠商品、安全借口等社会工程学方法实施钓鱼攻击，诱骗用户登录钓鱼网站并给出账号密码信息。而获得账号密码信息之后，再次通过地下产业链后续环节实施真实资产诈骗或者盗窃。

在“设计制作”环节，目前在黑帽技术、工具与培训地下产业链中已有专门开发各类钓鱼程序的黑帽团伙，只要申请一个域名和网络空间就可以很快建立起钓鱼网站，而这些钓鱼网站大都伪装成网上银行或电子购物网站，与真实网站界面几乎完全一致，并要求访问者提供账号和密码。实施网络钓鱼的不法分子往往会租用国外域名、服务器或网络空间，为相关部门的处理与执法部门的追查增加难度，从而企图躲避法律惩罚。在“传播”环节中，不法分子也会通过地下产业链购买不良网站或流量推广联盟的访问流量，甚至通过购买或黑帽搜索引擎优化技术来获得搜索引擎推广或靠前位置，此外也会利用群发邮件、QQ 等即时通信

软件群发消息、手机短信群发等方式广泛传播钓鱼链接，同时以优惠商品、抽奖或安全等理由吸引用户点击钓鱼链接。而在“实施”环节中，钓鱼程序往往在后台隐秘地记录并传输受害用户输入的账号和密码，而不法分子一旦窃取到有效账号密码，将会立即启动进一步的窃取与诈骗行为。

- **网银木马技术手段剖析**

网银木马是另一种互联网真实资产盗窃的主要犯罪技术手段，与网络钓鱼一样，也在地下产业链支持下形成了分工明确的有组织犯罪流程。网银木马作为黑帽技术、工具与培训地下产业链中的一类主流工具，可以通过地下黑市购买获得。而网络犯罪者也可以借助互联网资源与服务滥用地下产业链的支持，通过僵尸主机植入、软件捆绑、网站挂马、恶意邮件、即时通信群发恶意信息等多种渠道传播网银木马，使得互联网用户主机遭受感染。而一旦主机遭受感染之后，网银木马会静默地在系统中监视用户操作，通过键击记录、截屏录像、窃取数字证书、动态口令窃取、监控 U 盾、嵌入浏览器、篡改网银操作关键数据等技术，来尝试窃取网银账号密码信息，或劫持网银操作。

从 2004 年 4 月国内首个网银木马——“网银大盗”现身网络以来，网银木马也在与反病毒厂商、银行增强安全机制的博弈中不断发展，目前已发展出如下技术手段：

(1) 键击记录：这是网银木马最常见和初步的一种技术手段，往往以后台进程的方式监控用户的浏览器窗口，当发现用户正在访问网银登录或支付页面时，就使用 API 挂钩技术偷偷记录下用户键盘击键信息。

(2) 截屏录像：针对一些网银引入的屏幕小键盘等安全增强机制，网银木马在监控到用户访问网银页面时，使用截屏、桌面录像等技术将用户操作网银时的计算机屏幕录制下来，通过发回给攻击者人工分析出其中的账号密码信息。

(3) 窃取数字证书：对于网银随后普遍引入的数字“软证书”认证机制，网银木马通过控制系统,调用 Windows 操作系统提供接口,从 IE 浏览器证书体系中窃取数字证书。

(4) 动态口令窃取：动态口令是在 60 秒或更短时间内动态产生与时间相关的、不可预测的随机数字组合，网银木马也可以对动态口令进行窃取，并在口令失效时间之内传回攻击者并进行登录使用。

(5) 监控 U 盾：针对目前网银通过 U 盾硬件介质上安全存储数字证书的安全升级机制，最新网银木马具备了监控 U 盾驱动的能力，在被植入主机的用户插入 U 盾交易后还未拔下之机，迅速登录受害人网银并转走存款。

(6) 嵌入浏览器：网银木马将部分代码（通常通过 DLL 注入浏览器，或 Web 层 Javascript 代码）嵌入到受害主机的浏览器中，并以浏览器身份运行，一旦恶意代码能够进入到浏览器的进程中，就有可能在敏感数据被浏览器加密之前截获。

(7) 篡改网银操作关键数据：网银木马通过对网银支付页面中支付金额、支付账号等关键数据进行篡改，或利用第三方支付页面与网银衔接认证缺陷，对第三方支付页面中的网银操作关键数据进行篡改，使得用户进行支付操作后，支付款被恶意劫持到攻击者控制账户，或购买移动通信充值卡等现金等价物套现。

- **洗钱环节技术手段剖析**

在**图 2** 所示的真实资产盗窃地下产业链中，在不法分子窃取账号密码、身份证资料与银行卡资料之后，会进一步通过各种技术手段从中获得非法经济利益，我们将这个环节称为洗钱环节。

洗钱环节的技术手段受着不法分子所窃取到银行卡资料类型、所掌握的技术水平与犯罪资源限制、以及所能接受的法律风险等因素影响，因此非常地多样化，并且往往是通过地下

产业链构成一种非法利益驱动的有组织合作模式。我们也已经总结出了目前流行的几种主要洗钱方式：

(1) 汇款洗钱：在不法分子团伙窃取到网银账号密码（甚至包括软证书或动态口令等认证信息）之后，他们可以通过在线操纵网银账户，将其中存款汇款至其他冒名银行账号的方法，窃取受控账户中的资金。不法分子往往在极短时间内发起多比汇款转账到不同冒名账号，对于网银中设置的汇款最高限额也曾出现过利用银行漏洞实施限额解除的攻击技术，从而造成对受窃网银账户全部资金的瞬间汇转。在涉及跨境汇款洗钱时，网络犯罪者可能还会提供优厚佣金，雇佣“钱骡子”帮其实施跨境汇款，并通过地下钱庄进行资金跨境输送。

(2) 银行卡、信用卡盗刷套现：利用目前国内对 POS 机管理不严格的漏洞，不法分子可以假冒商家名义申请到 POS 机，在窃取到银行卡磁道信息和密码信息后，可以复制出卡片，并在 POS 机上套现。此外，还可以通过产业链的合作印刷出以假乱真的伪造卡，并在银行 ATM 机或商家 POS 机上进行取现或盗刷，在选择盗刷时，往往会去购买诸如金条、首饰、现金卡、充值卡等易于套现的商品。特别是一些支持 VISA、MASTERCARD 等国际支付通道的信用卡，不法分子甚至无需取得磁道信息，即可利用账号、有效期、CVV 等信息，进行信用卡盗刷。

(3) 证券账户操纵：对于窃取到的网络炒股账户的账号密码，不法分子则可以利用股票的高买低卖，将账户中的股金部分地转移至自己控制的股票账户里。中国互联网最早的一起真实资产盗窃案件——“证券大盗”案[证券大盗案 2006]即是通过这一手段，盗买盗卖受窃股民账号中的股票价值 1141.9 万，非法获利 38.6 万。而此次案件也造就了中国互联网犯罪的最高刑法记录——首犯因“盗窃罪”而被判罚无期徒刑。对于受窃的基金账号，也出现过被不法分子进行赎回操作后窃取资金的案例。

(4) 银行卡冒名与复制：无论使用哪种洗钱方法，网络犯罪者都不会使用自己的真实身份与银行卡参与洗钱，而是依靠地下产业链中的冒名银行卡与复制伪造银行卡来隐蔽地洗钱获得非法收入。银行卡冒名与复制伪造都是通过线下渠道来完成。银行卡冒名一般通过收购他人身份证资料（如租用农民工身份证、收购身份证复印件后制作假证等方式），然后在银行柜台中办理冒名的储蓄卡或信用卡。而复制伪造银行卡则通常需要已经窃取到磁道信息，通过一些非法代工工厂制作出伪造的银行卡，甚至可以自己从地下产业链中购置写卡器进行卡复制。

2.1.4 真实资产盗窃典型案件研究

2009 年央视三一五晚会上曝光的“顶狐”案——即“金 X、徐伟 X、徐文 X 等信用卡诈骗盗窃案”，就是一个非常典型的通过地下产业链驱动和组织的互联网真实资产盗窃案件。根据江苏省无锡市滨湖区人民法院对这个案件的初审记录与无锡市中院的二审记录[央视 315 2009]，在此案中，徐伟 X 在地下产业链中的角色为木马编写者与“料主”，开发了“顶狐”木马程序并在互联网上传播，窃取到蔡 X、陶 XX 等多位受害者的网银账号、密码、身份证号、姓名等信息，而金 X 与其女友陆 XX 为“洗料人”，从徐伟 X 处购得“料”，在其中两次作案中将“料”传输给另一位“洗料人”徐文 X，而徐文 X 找到一个具备洗钱技术能力的“车主”龚 XX，由其伪造受害人的身份证与银行卡，并指使某男与某女（“车手”）在银行柜台上注销银行卡后，冒领银行卡实施取现，事后龚 XX 将赃款分成给付给徐文 X 与金 X。金 X 还与另一位“洗料人”方 XX 合作，由方 XX 找到一位网友“哦衲衲”提供黑帽技术服务解除了网银中设置的支付额度限制，然后以转账洗钱方式取得赃款并与金 X 分成。此外，金 X、陆 XX 自己也通过信用卡盗刷方式进行“洗料”，使用受害者信用卡购买游戏点卡后，通

过淘宝点卡经营者陈 X 进行套现。

这个案件充分体现出了互联网真实资产盗窃的地下产业链交互过程，所有主犯均是通过互联网建立起联系和合作关系，在非法经济利益的驱动下，发挥各自角色上的能力，并采用了转账洗钱、信用卡盗刷与假冒银行卡取现等多样化的洗钱方式，攫取银行卡中的资金，而所得赃款也通过地下产业链的经济规律进行分成、支付技术佣金或“料”款，达到了参与各方的利益平衡，也使得这个通过互联网松散组织的犯罪团队一次次地继续配合作案。

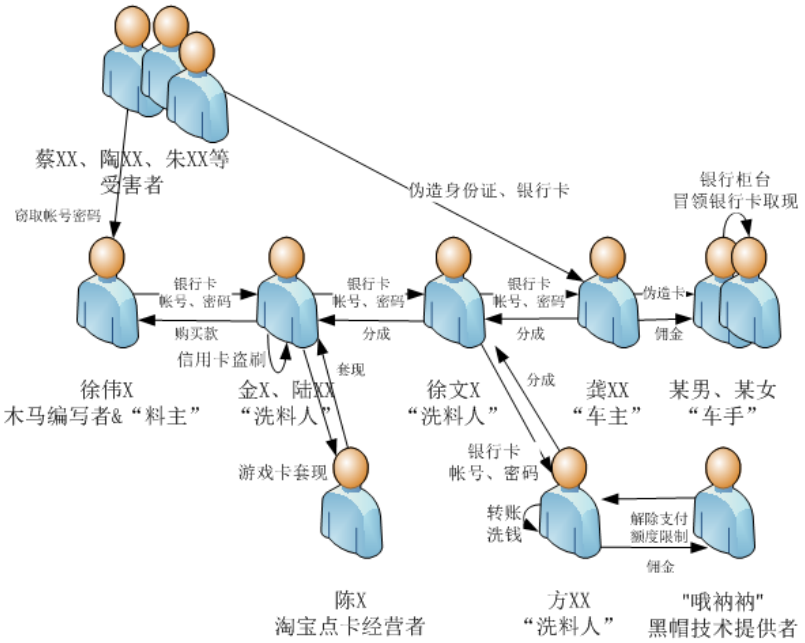


图 3 “顶狐”案件犯罪者角色与关系图

该案件在 2008 年审理之后，在 2009 年 3 月 15 日的央视 315 晚会上进行了曝光[央视 315 2009]，而其中网民为“顶狐”的黑帽——即徐伟 X 也引起了广大网民的极大兴趣，利用了超级人肉搜索，挖掘出了他的很多资料。

“顶狐”案发时 27 岁，广东省惠阳县人，毕业于井冈山师范大学计算机专业。央视 315 晚会上曝光了“顶狐”让人触目惊心的骇客行为，“顶狐”早在 2005 年就是瑞星公布的十大病毒之一“狐狸王”制造者，他通过自己编写“顶狐结巴”木马，疯狂盗取网银、网游、QQ 等各类账户的账号密码，以及网民个人信息，还以免费下载方式，将该木马捆绑至“顶狐下载者”并上传到黑帽网站上，任由下载（目前通过 Google，仍可搜索到大量 2006 年“顶狐”发布的“顶狐下载者”及相关下载页面，如**图 4** 所示例），而“顶狐结巴”木马却背地里将其他黑帽盗取的所有信息，自动回复到他所控制的服务器上。最后警方在抓到“顶狐”时，每天存储到服务器上的窃取账户密码与个人信息量达到 3G 之多。而“顶狐”对盗取到的信息分类整理之后，将密码等信息廉价出售，而网上银行用户信息则仅以 400 元每 G 的低价打包售出。

而“蚂蚁”——即案件中的金 X 正是从“顶狐”那购买这些网上银行用户信息，起初仅仅是通过盗刷方式洗钱，但通过徐文 X 找到“车主”龚 XX 之后，便开始制作假冒银行卡去大额取现，总计盗窃作案七次，盗取人民币 140 余万元，制造了引起公安部高度重视的“3·5”特大网上银行盗窃案。


[系统软件] 顶狐下载者3.5（经测试可以过卡巴，瑞星等各杀毒软件）[复制链接]

哈king 初出茅庐 当前离线
UID 155660 帖子 3 精华 0 蛋花 0 桶 雨点 115 滴 植树 0 棵
威望 7 在线 2小时 注册 2006-9-16 最后 2006-9-16

发表于 2006-9-16 23:50 被查看数:359 | 被回复数:0 | 发短消息 | 查看资料 请输入关键字 搜索 只看该作者 | 字体: 大 中 小 楼主

顶狐下载者3.5 (经测试可以过卡巴，瑞星等各杀毒软件)

顶狐下载者3.5 (经测试可以过卡巴，瑞星等各杀毒软件)

顶狐下载者3.5
http://free5.ys168.com/?heimaomao
3.50更新说明：
重写了随机变种引擎的大部分代码，彻底躲过各大杀软查杀。重新编写了SEH处理程序，动态清除
已执行过的代码(执行之后找不到完整的代码),随机加解密原入口，添加了随机花指令。
由于采用新的变种引擎，经测试可以过卡巴，瑞星等各杀毒软件

基本功能说明：
1、动态注入穿防火墙下载
2、超多项下载，开机自启动
3、功能最全体积最小的下载者
4、过下载拦截者，递归下载直到成功（3次下载中，只要下载成功即下载下一个）
5、全新特色技术，超强免杀.生成服务端绝没有相同代码(随机入口点,随机加密,
随机变换代码,随机加入混淆指令,SEH技术运用),保证生成一次变一次。
升级时间：2006年9月13日
作者：顶狐《TopFox》

图 4 目前仍可搜索访问到的“顶狐”发布“顶狐下载者”的原帖

2.2 网络虚拟资产盗窃地下产业链

中国互联网上的网游和在线娱乐行业在过去十余年中得到了蓬勃发展，而主流网游和在线娱乐系统中都引入了虚拟货币、装备和会员级别等设置，以提升娱乐性并为运营厂商赚取更多盈利。而这些虚拟货币、装备和会员级别大多都由游戏玩家通过真实货币购买，或者投入大量游戏时间赚取，因此对于游戏玩家而言，便是他们在网络空间中的资产。同时通过网络营销渠道，这些网络虚拟资产是可以出售给其他游戏玩家，而转换为现实世界中的金钱货币。因此从这个意义上说，这些网络虚拟资产也具有了实际的价值。然而中国现行法律并没有对虚拟财产的合法性作出明确规定，在《消费者权益保护法》中，网民对虚拟财产的权利也不属于现有的消费者权利中的范畴，虽然在某些判罚案例中会考虑网络虚拟资产的商业价值而将其纳入财产保护范围，但大多数情况下仍难以有效地衡量网络虚拟资产的具体价值，并对其进行有效保护。

地下产业链中的一些不法分子正是利用了这一问题，通过对大众网民的网络虚拟资产进行盗窃与销售，获得非法经济利益，同时又较真实资产盗窃具有更低的法律风险。

2.2.1 网络虚拟资产盗窃地下产业链结构分析

中国互联网上的网络虚拟资产盗窃地下产业链结构如**图 5** 所示，主要包括三个环节：首先是通过网络钓鱼、盗号木马等多种方式窃取网游、娱乐等互联网软件的账号密码；然后通过一个“洗信”环节，利用窃取账号密码登录到账户中，从中窃取虚拟货币、网游装备等网络虚拟资产，或是对一些靓号账户和高级别账户修改认证密码等信息；最后通过网络营销渠道将窃取到的网络虚拟资产出售给游戏玩家，获得现实的金钱与利益。

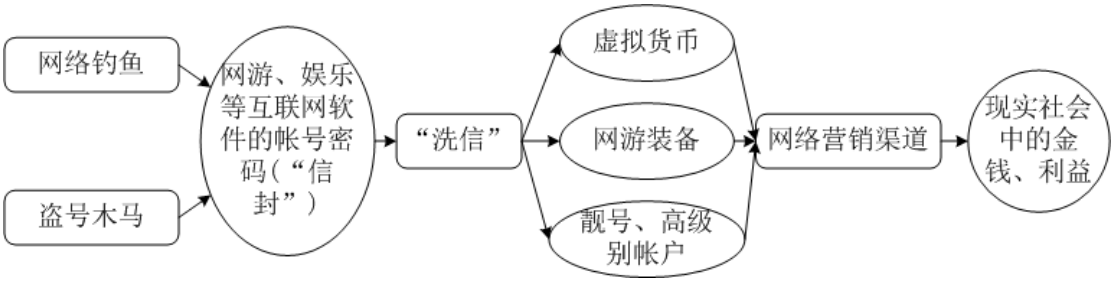


图 5 网络虚拟资产地下产业链结构

2.2.2 网络虚拟资产盗窃地下产业链角色与行话分析

在网络虚拟资产盗窃地下产业链中，各种网游、娱乐软件账户的账号密码也同样被称为“信封”或“信”，而不法分子用来收取账号密码的电子邮箱、在线 Web 应用程序等也被称为“箱子”。通过从木马编写者购买盗号木马，并实施“信封”窃取攻击的黑帽在地下产业链中的角色被称为“木马代理”或“包马人”。而窃取得到“信封”后，通常将其倒卖给地下产业链中的下家——“洗信人”，由他们通过自动化工具或手工方式利用窃取账号密码登录账户，并从中窃取网络虚拟资产，或修改密码控制有价值的账号，这一过程便称为“洗信”。窃取到的网络虚拟资产则出售给“包销商”，由其通过一些公开网络销售渠道出售给游戏玩家，从而套现。

2.2.3 网络虚拟资产盗窃互联网犯罪技术手段剖析

- **针对网络虚拟资产账户的网络钓鱼**

在 2.1.3 节，我们已经剖析了针对真实资产账户的网络钓鱼技术手段，而针对网络虚拟资产账户的网络钓鱼从机制上基本类似，所不同的是针对目标从涉及真实资产的网银、支付等账户变为包含网络虚拟资产的一些网游、娱乐类在线软件账户。从目前的统计结果来看，中国互联网上针对网络虚拟资产账户的网络钓鱼攻击占总体钓鱼攻击的比例相对较小，主要目标是腾讯 QQ，以及盛大、网易等网游厂商。

- **盗号木马**

盗号木马是目前中国互联网上实施网络虚拟资产账号密码盗窃最主流的技术手段，与网银木马类似，针对网游和娱乐在线软件的盗号木马也普遍采用了键击记录、截屏录像、动态口令窃取等技术，来尝试窃取软件登录凭证信息。

由于各个网游和娱乐软件进行账户认证登录处理机制的差异性，因此盗号木马基本上都是针对特定软件进行编写的，但在地下产业链中会出现同一个木马开发工作室对多款主流软件均开发并销售盗号木马的情况，并经常使用同一品牌来进行命名。

由于网游和娱乐软件账户的安全级别较网银与支付类账户较低，盗号木马较网银木马更容易实现一些，在地下产业链黑市中也被称之为“小马”，售价也比网银木马低很多，网银木马售价通常高达几千元甚至上万元，而网游盗号木马的价格则在几百元至上千元区间内。

- **“洗信”**

“洗信”没有什么技术含量，而是需要“洗信人”对网游、娱乐软件中的网络虚拟资产价值和转移方法有较多的认识。他们在使用“信封”成功登录之后，通过大多数网游软件中都提供的交易、拍卖等渠道，将高价值装备、虚拟货币等转移至他们自己控制的账户里。对

于高级别账户，他们还可能通过破解密码保护机制，以达到完全盗号目的。

对于腾讯 QQ 和一些流行网游，为了提高“洗信”效率减少人工操作工作量，地下产业链中也开发出了相应的自动化洗信工具软件。

- **虚拟资产的公开网络营销渠道**

中国互联网上的网游与娱乐软件玩家规模非常庞大，其中也不乏大量沉迷于此，并不惜花费大量金钱购买虚拟货币、网游装备以提升自己游戏和娱乐感受的玩家，他们为网络虚拟资产盗窃地下经济链提供了经济基础。“洗信人”在窃取到大量网络虚拟资产后，通常在地下黑市中出售给“包销商”，由他们在国内主要网络交易平台（如淘宝网）与网游内部交易渠道中销售给终端游戏玩家，获得支撑整个网络虚拟资产盗窃地下产业链运行的资金。

2.2.4 网络虚拟资产盗窃典型案件研究

2007 年湖北省仙桃市人民法院审理的“熊猫烧香”案件[熊猫烧香案 2007]是当年国内最引人关注的网络犯罪案件，也第一次全面地向公众揭示出网络虚拟资产盗窃背后严密的地下产业链。案件主犯李 X 和从犯雷 X 于 2006 年 10 月份制作出“熊猫烧香”病毒，在随后的几个月中通过传播感染了大量“肉鸡”并连接从犯王 X 出资租用的控制网站，而从犯张 X 经过王 X 介绍后购买了李 X 的网站流量，并将盗号木马的自动下载链接挂接至控制网站上，使得感染了“熊猫烧香”病毒的计算机自动访问控制网站时便会感染盗号木马，从而监测窃取网络游戏的账号密码，并通过电子邮件方式发回给张 X。随后张 X 将包含网游账号密码的“信封”，以每个 0.9 至 2.5 元的价格在网上出售，由下家进行“洗信”窃取其中的网络虚拟资产，张 X 先后多次给李 X、王 X 汇款。在该案件中，李 X 获利 145,149 元，王 X 获利 80,000 元，张 X 获利 12,000 元。

在这个案件中，如图 6 所示，李 X 扮演着地下产业链中恶意代码编写者的角色，提供“熊猫烧香”病毒，以及对抗反病毒软件的免杀服务，雷 X 则作为李 X 的黑帽启蒙师傅，为他提供了病毒编写技术的培训与支持，而王 X 和张 X 分别承担了“木马代理”与“包马人”的角色，张 X 通过王 X 从李 X 处购买“熊猫烧香”病毒和受控计算机的安装量，并从地下产业链中购买获得盗号木马，实施盗号木马大规模植入与窃取网游账号密码的攻击过程，并最终将窃取到的“信封”在地下产业链黑市中进行销售而获得非法利益。

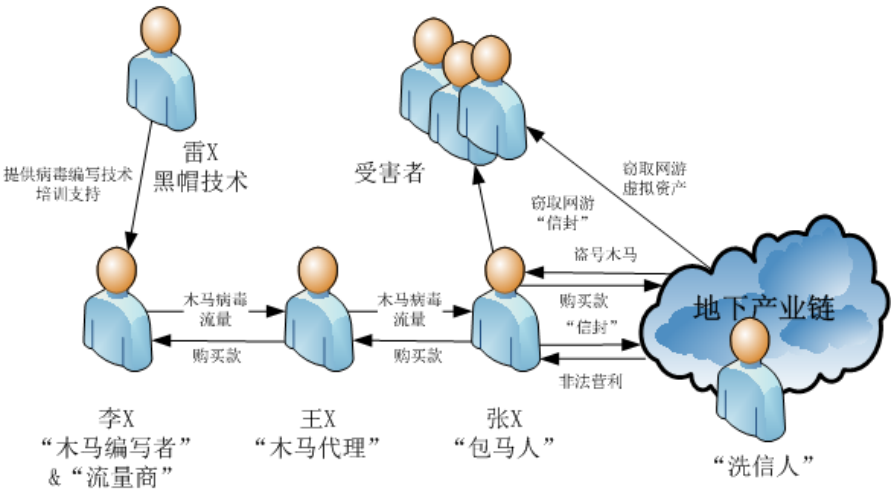


图 6 “熊猫烧香”案件犯罪者角色与关系图

2.3 互联网资源与服务滥用地下产业链

现在的中国互联网上真是“有钱能使鬼推磨，无钱自有鬼驱人”，只要特定的互联网资源和服务能够产生出经济价值，便会有贪婪之徒来窃取他人的资源，或是千方百计地挖掘出互联网服务规则漏洞，通过作弊和滥用服务，来牟取经济利益。即使某些资源与服务对这些贪婪之徒没有任何经济价值，而只要它们对所有者而言非常关键，那他们也会通过破坏、勒索和敲诈来迫使所有者屈服于他们的“淫威”，而不得不交纳赎金。

2.3.1 互联网资源与服务滥用地下产业链结构分析

在缺乏有效法制管理和行业监管下野蛮发展多年之后，目前中国互联网上通过资源与服务滥用来谋取非法经济利益的手段方法已经非常地多样化，也在逐渐形成了许多地下产业盈利链条。我们在**图 7** 中给出了中国互联网资源与服务滥用地下产业链主要结构，主要分为窃取资源和滥用资源两大环节。

在窃取资源环节中，互联网上最重要最普遍的资源就是联网计算机与手机终端，拥有联网计算机与手机资源也就意味着掌握了计算能力、存储空间、网络带宽、IP 地址、网络访问流量、以及上层敏感数据等等其他类型的资源。而在互联网上，拥有更多的资源也就意味着拥有更强的能量，对于网络犯罪者而言，就可以滥用这些能量破坏互联网的合法秩序，从而为他们自己攫取到非法利益。

目前掌握大量联网计算机的主流技术方法便是从本世纪初开始崛起的僵尸网络，可以通过一对多的命令与控制机制，构建出拥有大量受控僵尸主机的庞大“军团”，而让网络犯罪者拥有强大的攻击资源平台。僵尸网络的主要传播技术手段包括恶意邮件/信息、通过系统漏洞“抓鸡”、网站挂马植入、以及恶意捆绑软件等等。以网赚推广名义实施的“挂机”则让一些黑帽们拥有另一种掌握大量联网计算机的手段，这种方式并不是采用非法攻击，而是通过“蝇头小利”配合传销模式，来诱使一些见钱眼开的网民甘愿为人所用，贡献出计算机与网络资源，来参与一些互联网服务滥用的黑帽行为中。联网计算机中特殊的一类——网站服务器还拥有着互联网中具有高度商业价值的资源，也就是网站访问与点击，而这也是让黑帽们垂涎三尺的“宝藏”，他们或者通过“黑站”技术非法取得，或者通过网赚推广名义从地下产业链中廉价购买。此外企业内网关键业务服务器上的敏感数据也是黑帽们尝试攫取或者滥用的对象。

而在智能手机终端平台上，个人计算机所经历过的各种恶意代码形态都已经复现，同时结合智能手机具有更多隐私信息、直接涉及资费与支付等特性，发展出对用户更为致命的安全威胁。智能手机恶意代码传播的主要途径包括恶意捆绑、恶意邮件/信息等。

一旦黑帽们窃取到互联网资源之后，他们便在地下产业链中出售，而由承担产业链中其他角色与分工的恶意攻击者购买并加以利用，通过滥用资源环节中的各种衍化出的盈利链条获得现实世界中的经济利益。

对于僵尸网络控制的僵尸主机，恶意攻击者可以通过下载器进一步植入各种钓鱼程序、网银木马来实施真实资产盗窃，也可以植入钓鱼程序与盗号木马进行网络虚拟资产的盗窃，还可以滥用受控主机的计算与网络资源，通过提供垃圾广告邮件与信息发送服务、发动 DDoS 攻击并勒索敲诈、实施点击广告欺诈、提供刷排名人气投票等服务、窃取情报隐私信息进行销售甚至敲诈等各种盈利途径，取得佣金、黑钱分成、赎金等各种类型的非法收入。通过“挂机”方式的控制主机从技术上完全等同于受控僵尸主机，也同样面临着上述风险，但一般在地下产业链中，为保证传销式推广效果，真正实施“挂机”行为的黑帽们大多不会将合作“挂

机”者作为攻击对象，而是利用这些受控资源攻击第三方，因此盈利模式受限于提供垃圾广告邮件与信息发送服务、发动 DDoS 攻击并勒索敲诈、实施点击广告欺诈、提供刷排名人气投票服务等。然而你不能指望这些黑帽们遵守所谓的“职业道德”，他们在许多时候也会向参与“挂机”的计算机植入各种恶意木马，以窃取更有价值的真实资产、虚拟资产或个人隐私信息。

网站服务器的访问与点击流量在互联网广告这一具有庞大规模的市场板块中具有高度价值，因此黑帽们也会滥用这些资源实施点击广告欺诈、刷排名人气投票来牟取利益，甚至还可以将其利用在窃取资源环节，比如植入挂马链接实施网站挂马攻击等。

在智能手机终端领域，目前通过恶意代码受控手机资源实施地下产业链盈利的模式也发展很快，主要已经拥有：恶意扣费、发送垃圾邮件/信息、点击广告欺诈、软件推广欺诈、刷排名人气投票等服务、以及窃取隐私信息销售或勒索等。

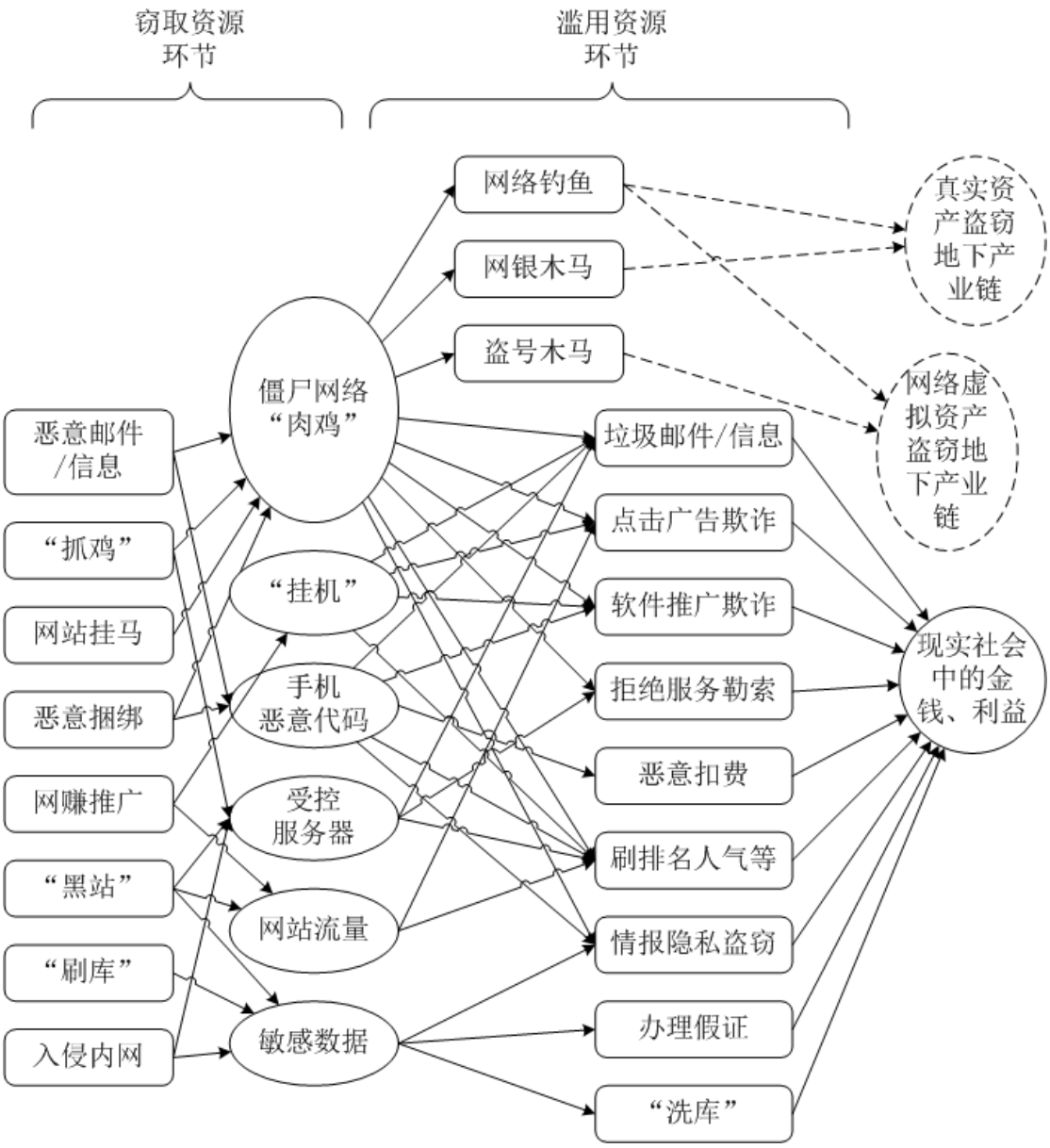


图 7 互联网资源与服务滥用地下产业链

2.3.2 互联网资源与服务滥用地下经济链角色与行话分析

在**图 7** 的互联网资源与服务滥用地下产业链中，通常在窃取资源环节需要参与者掌握一定的黑帽技术，以及拥有相关攻击工具软件与恶意代码，从而能够实施针对联网计算机、服务器、手机等系统资源的攻击，窃取得到大量的系统资源，以及这些系统所关联的网络 IP 地址、访问流量、敏感数据等互联网资源，通过地下产业链黑市进行销售获利。这类参与者是目前中国互联网上由经济利益驱动网络攻击事件的主要源头，在地下产业链中这种参与者角色称为“黑客”（此处带有贬义，指的是对网络进行攻击破坏或窃取资料的人，即黑帽）。

而在利用资源进行互联网服务滥用的环节中，由于从上游产业链中已经提供了现成的工具与大量资源，因此这个环节基本上无需掌握任何黑帽技术，入门门槛很低，同时可以直接通过各种地下盈利渠道取得现实利益，因此吸引了大量网络无业游民参与进来，在各种网络赚钱、非法利益的诱导下，从事这些危害互联网经济与网民利益的黑色活动。由于国内互联网行业方面的监管法律与政策还非常欠缺，因此在这个环节中的一些盈利模式，如垃圾邮件/信息、点击广告欺诈、软件推广欺诈、“刷客”行业、个人隐私信息买卖等都没有相关的法律条款或行政规则进行约束，因此一些缺乏社会与行业道德的企业也参与到地下产业链的灰色地带中，对中国互联网经济的健康发展构成了危害。

2.3.3 互联网资源与服务滥用技术手段剖析

- **服务器远控后门与僵尸网络技术手段剖析**

远控后门（即远程控制后门）是攻击者用来单独控制一台联网主机的命令控制机制，而僵尸网络的基本特性是攻击者与受控主机之间的一对多命令控制机制[诸葛建伟等僵尸网络综述 2008]。目前互联网上远控后门通常只用于控制具有更好的计算性能、存储与网络带宽条件的服务器资源；而对于终端计算机，攻击者普遍利用僵尸网络技术，构建出更加灵活且高效的攻击资源平台。

对服务器进行攻击并植入远控后门的途径主要有“黑站”和入侵内网服务器，分别针对网站服务器和企业内网业务服务器。而用于远程控制服务器的后门类型则包括后门用户账号、远程命令行 Shell 后门、远程桌面控制后门、以及定制远控后门工具软件等。中国互联网地下产业链中最普遍的受控服务器资源是 Windows 网站服务器，并通过标准 Windows 远程桌面进行控制，由于 Windows 远程桌面使用了开放在 TCP 3389 端口上的 RDP 协议，因此此类受控服务器资源在产业链行话中被称为“3389”。

而对互联网用户终端计算机实施攻击并植入僵尸程序的技术手段主要包括：

(1) 恶意邮件/信息：攻击者通过恶意邮件附件、即时通讯软件恶意信息等方式传播僵尸程序，并通常结合社会工程学手段诱使网民运行程序，从而导致终端计算机被感染并加入僵尸网络。

(2) “抓鸡”：攻击者通过主动扫描网络中设置弱密码、存在未打补丁高危安全漏洞的终端计算机，通过口令猜测、安全漏洞远程渗透等技术，攻陷终端计算机并植入僵尸程序。

(3) 网站挂马：攻击者在一些“被黑”网站与购买访问流量的网站上，挂接网页渗透攻击代码，以被动方式等待终端计算机用户访问这些网站页面，并通过这些渗透代码对浏览器及插件安全漏洞的利用，植入僵尸程序。

(4) 恶意捆绑：攻击者在一些合法软件、多媒体文件中捆绑僵尸程序，并通过互联网提

供免费下载，而但终端计算机用户安装这些软件，或播放多媒体软件时，即在背地里植入僵尸程序。

在终端计算机被植入僵尸程序构成僵尸网络时，根据僵尸网络命令控制机制的差异，分为集中式命令控制机制与 P2P 命令控制机制两大类。目前中国互联网地下产业链主要使用的灰鸽子、上兴远控、Ghost 等各种远控软件，大多具有多受控端同时连接一个控制端（称为“上线”）的一对多命令控制特性，因此从技术特性上分析已属于僵尸程序的范畴，并采用了集中式命令控制机制。

- **“挂机”网赚技术手段剖析**

“挂机”网赚是一种处于互联网灰色地带的地下产业链盈利模式，“挂机”网赚项目也乌龙混杂，既有操作规范并具有一定诚信品牌的良性项目，也有为作弊方式提升网站排名提供服务的灰色项目，也不乏大量扰乱互联网广告、投票、推广等在线服务秩序从而牟取不当收益的黑色项目。

良性的“挂机”网赚项目通常需要参与者付出一些时间，来完成软件推送的网络调查问卷、服务推广任务、输入验证码等等，才能获取到少量收益。这种良性项目实质上是参与者通过投入时间与人际关系来获得合理报酬。而那些无人值守的“挂机”项目则往往是利用“挂机”计算机的网络资源，制造出虚假的网络访问流量与页面点击量，可用于作弊提升网站流量排名、实施点击广告欺诈、进行黑帽搜索引擎优化、提供刷人气信誉投票等作弊服务等等。

为了使得项目能够吸引更多的参与者，让运营者取得最大化的经济利益，几乎所有项目都采用了传销式的推广策略，设置了发展下线的提成比例，也就是一旦参与者协助推广吸引其他人参与，就将其视为下线，并获得下线通过项目赚取金额的部分提成。一般的下线提成比例为 5%至 20%之间。这种传销机制的引入使得网赚在互联网地下产业链中异常火热，参与者众多，Google 搜索“网赚”可以查到 2,660 万网页，“挂机网赚”也有 474 万网页，“网赚论坛”则有 451 万网页，虽然参与者众多，但毋庸置疑的是并没有多少参与者能够通过“挂机网赚”赚到较高收入，而利用广大参与者的电脑与网络资源，通过扰乱互联网正常服务秩序而赚取大量不当利益的是这些运营“网赚”项目的地下团队。

几乎所有的无人值守“挂机”软件都提示参与者为了不影响正常运行而关闭反病毒软件，而仅仅通过声明方式宣称不对参与者电脑造成安全危害和使用影响，但这让参与者电脑的安全无法得到有效保障。

- **服务器入侵与攻击技术手段剖析**

针对互联网上的网站服务器及企业内网业务服务器资源，恶意攻击者主要的技术手段包括：

(1) “黑站”：指的是对网站服务器的入侵攻击，主要利用服务器的系统漏洞、弱口令与配置缺陷、Web 应用程序漏洞等不同位置的安全缺陷，取得对网站服务器不同程度的控制权。如利用 XSS 漏洞只能在网站应用程序上植入一些恶意链接，从而攻击网站访问者；而利用 SQL 注入漏洞等可能在网站服务器上植入 Webshell 后门，获得受限用户控制；而再进一步通过提权攻击则可能获得服务器的完全远程控制权限。

(2) 内网服务器入侵：攻击者通过公共互联网，首先攻入同时连接企业内网与互联网的 DMZ 区服务器或网关服务器，然后以其为跳板，渗透进入企业内网，定位并入侵关键的内网业务服务器，取得内网服务器的访问。

(3) “拖库”：指恶意攻击者对网站或业务服务器上包含敏感信息数据库的攻击窃取技术。“拖库”的通常技术步骤为：首先对通过“黑站”或内网服务器入侵技术获取网站或内网服务器的访问，并植入 Webshell、远控等后门工具，然后通过后门进一步利

用服务器本地漏洞进行提权攻击提升至更高权限，最后利用系统权限直接下载备份数据库，或者查找数据库链接后进行数据导出。[瑞星年报 2012]

- **手机恶意代码技术手段剖析**

目前的智能手机终端已经具有类似于个人计算机的开放系统平台和上层应用，这也为手机恶意代码的发展提供了条件。相应于中国智能手机市场最流行的操作系统平台，手机恶意代码目前主要集中在 Android、Symbian 与 Windows Mobile/Windows Phone 7 平台上。

手机恶意代码的主要传播渠道包括恶意邮件/信息、捆绑下载、捆绑预装和 ROM 刷机包等等。恶意邮件/信息渠道通过群发彩信等方式，通过手机通讯录的社交关系进行传播。捆绑下载渠道则是目前最流行的手机恶意代码传播途径，恶意攻击者将手机恶意代码捆绑到正常应用程序中，并通过手机论坛、应用商店、手机下载站进行推广，吸引手机用户安装应用，从而植入捆绑的恶意代码。捆绑预装则是在水货手机、销售存储卡上预先安装带有恶意代码的应用程序。而 ROM 刷机包也是通过捆绑方式，将恶意代码直接植入到提供下载的刷机 ROM 中。

智能手机一旦被植入恶意代码，就会遭受恶意代码所带来的威胁后果，目前中国移动互联网上流行的手机恶意代码主要通过恶意扣费、实施应用软件推广欺诈、参与点击广告欺诈、以及提供广告短信/彩信发送服务来进行直接牟利，或通过手机上的隐私信息窃取销售获得间接利益。

- **滥用资源危害互联网服务环节手段剖析**

通过上述各种资源窃取技术，恶意攻击者可以获取到互联网上的大量联网终端计算机、服务器、智能手机资源，以及系统上的敏感数据内容，之后便可以利用以下多种手段来滥用掌握的这些资源，危害互联网正常服务，来取得不当经济收益。

(1) 广告邮件/信息群发服务

利用控制大量资源为具有商业推广需求的客户提供广告邮件/信息群发服务，这种服务在中国互联网上非常普遍，往往以“精准邮件推广”、“电子邮件营销”、“商务邮件代发”、“广告短信群发”等名义，提供商业付费服务。

而这种服务运营者并不会向客户透露发送邮箱地址及发送邮件资源的来源途径，而是提供代发邮件的服务机制，目前一般的服务价格为 10 万封邮件 1000-2000 元左右（即每封邮件 1-2 分钱），而短信群发一条也只需 3-5 分钱。而实际上大多数此类服务运营者是通过各种渠道获取的电子邮件地址、手机号等用户隐私信息，建立分类邮件地址库与手机号码库，并使用僵尸网络控制的大量终端计算机和手机，参与广告邮件/信息的群发。这种服务也是目前互联网与移动通信中用户遭受大量垃圾广告与信息侵扰的根源所在，同时进行广告邮件/信息群发的受控计算机与手机用户还会更进一步受到网络带宽与通信资费的损失。

(2) 点击广告欺诈

点击广告（CPC）是目前中国互联网上最流行的广告计费模式之一，以百度竞价排名为代表。在百度竞价排名的点击广告模式中，广告主向百度购买一些搜索关键字的排名位置，每次点击付费价格出的越高，就会取得百度搜索结果中越靠前的位置。当互联网用户使用百度搜索这些关键字时，如果点击了结果页面中广告主的链接地址访问其网站时，即被百度进行计费，而广告主也因此获得一个可能的潜在客户。然而点击广告盈利模式的一个致命风险是恶意的自动点击，即不会为广告主带来任何潜在客户，但仍可能导致计费的无效点击。

而实施这种恶意点击的动机也有多种，其一是点击广告商为扩展广告展示渠道和访问流

量，普遍采用联盟方式集成其他网站、软件的用户访问流量，如百度网盟推广、Google AdSense 等，参与这些联盟的一些网站主可以从用户访问流量中点击广告收入中获得利益分成，而一部分网站主为了提高收入，便实施恶意点击手段，来制造出一些无效但计费的点击。另外广告主的恶意竞争对手也可能采用自动点击技术手段，消耗广告主的每日广告限额，从而打击竞争对手广告效果，并让自己的广告排名上升。

虽然点击广告商普遍采用了一些技术手段来识别恶意点击，特别是源自同一 IP 地址与主机的大量自动点击，但是对于使用僵尸网络、“挂机”软件、受控手机终端来实施的恶意点击，由于使用了大量 IP 地址与机器资源，同时会模拟人工点击过程与频率，因此目前广告商的识别防御技术并不能完全对抗，从而使得广告主因此承受点击广告欺诈造成的风险。

地下产业链中的一些僵尸程序插件(如霸王弹窗插件等)、“挂机”软件(如 IP 联盟 707w)中均提供了设置点击广告的功能。例如 2008 至 2009 年在地下产业链中非常流行的霸王弹窗插件是一个采用 HTTP 协议的僵尸程序插件，提供了广告弹窗、隐藏 IE 窗口暗刷流量、后台自动点击广告、刷 ALEXA 排名等多种互联网服务滥用功能，**图 8** 显示了霸王弹窗插件集中的后台管理系统中对于点击广告的配置界面。我们在 2008 年协助部署的 Matrix 中国分布式蜜网系统[Matrix FIRST 2008]中截获了该插件的 1121 个不同变种，并监测到 141 个不同的霸王插件僵尸网络控制信道。

图 8 霸王弹窗插件后台管理系统中的点击广告配置

(3) 软件推广欺诈

中国互联网与智能手机终端上的很多应用软件目前通过广告等方式进行盈利，有些软件甚至具有更为恶劣的流氓行为，而为了使得此类软件具有更大的用户装机量，往往通过地下产业链的 PPI 模式（即按每次安装进行付费）进行软件推广，推广方式包括通过已控制系统的僵尸程序、手机恶意代码进行软件植入和诱骗安装，购买下载类网站的访问流量植入欺骗性链接等等。

根据网秦 2011 年手机安全报告，Android 平台的“远程控制木马”在 Q3、Q4 季度呈现了迅猛增长势头，并在全年以 27.3%的感染比例位居首位。而其中具备恶意传播、推广特征的恶意软件占据了 9.2%的比例， 这类远程控制木马就会自动在手机后台联网接收远程服务器下发的指令，借以下载其制定的恶意推广应用软件。如以网秦 2012 年 1 月 6 日在全球最先截获的一款最新 Android 远程控制木马(a.rogue.PushBot.a)为例，就通过伪装成 Google Dual Core 这一谷歌官方应用，来诱骗用户下载安装。植入手机后会在后台自动联网下载数款用于恶意推广的软件，消耗用户流量，给用户带来经济损失。[网秦木马报告 2012]

(4) 恶意扣费

恶意扣费行为主要出现在可以通过订购 SP 服务直接进行费用支付的手机平台上，也是目前手机恶意代码最流行的盈利行为之一，根据网秦 2011 年手机安全报告，具有该行为的手机恶意代码占总数的 25.5%。[网秦年报 2012]

恶意扣费软件的基本原理为利用技术手段将扣费插件批量伪装成热门应用来诱骗用户下载，装入手机后通过后台强行启动恶意进程来定制 SP 付费业务，而对运营商的订阅二次确认进行自动回复，并拦截业务开通的短信通知，使得用户极易在不知情状态下落入吸费陷阱之中，从而遭受手机资费损失。

安卓吸费王是 2011 年 Android 平台中感染次数最多、传播范围最广和影响范围最大的恶意软件，自 2011 年 2 月被发现以来，目前累计植入超过 700 款 APP 应用之中，同时由于其具备直接扣费威胁用户手机话费安全的特征，也多次被国内媒体重点曝光。[网秦年报 2012]

(5) 勒索敲诈

勒索敲诈是地下产业链中一种性质更加恶劣的盈利方式，恶意攻击者通常利用掌握大量计算与网络带宽资源对目标进行拒绝服务攻击威胁，或是窃取目标的关键隐私信息后以破坏或曝光实施威胁，从而敲诈目标支付“保护费”或者“赎金”。

在中国互联网上，拒绝服务攻击勒索主要针对的是一些严重依赖业务在线运行但本身又处于灰色地带的行业，比如网络游戏私服、网络博彩网站等等。这些地下行业无序化竞争状况也使得很多运营者雇佣黑帽团队对竞争对手服务器或网站进行 DDoS 攻击。2011 年 9 月份，重庆网警召开新闻发布会，称破获一起“黑客”团队勒索私服网游获利 6000 余万元的特大网站犯罪案件[DDoS 私服勒索案 2011]，该案件体现出拒绝服务攻击勒索敲诈从获取广告业务、租用服务器、客服发布广告、网络攻击竞争对手、专门取款小组的一条完备的地下产业盈利链条。

此外窃取目标用户隐私信息后以曝光威胁实施勒索也出现过多起案件，最著名的是央视著名主持人马斌“裸照”被窃并遭敲诈勒索案[马斌案 2010]，犯罪嫌疑人后被警方逮捕并判刑 5 年。除此之外，恶意攻击者还会入侵关键服务器获得企业敏感数据，或传播勒索软件对感染终端计算机上的数据进行加密，之后向数据所有者进行敲诈勒索。这种安全威胁近年来从国外逐步进入中国，也已经给中国互联网带来严重风险。2006 年出现的“敲诈者”病毒是国内最早出现的勒索软件之一[敲诈者案 2006]，感染后会在主机上搜索各种数据文件，对文件进行加密后删除源文件，然后弹出醒目窗口对用户进行勒索敲诈，如**图 9** 所示。

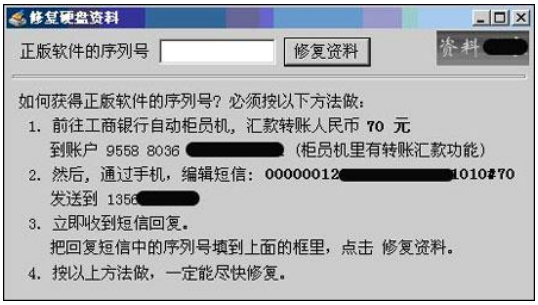


图 9 “敲诈者”勒索软件

(6)“刷客”

中国互联网地下产业链中一种非常普遍的盈利途径是利用大量受控资源来操纵各类互联网在线服务，比如搜索引擎排名、网络购物店铺人气与信誉、软件排名与好评、各种在线投票等等，而这种盈利途径也被称为“刷客”行业。

搜索引擎是目前互联网用户查找并搜索信息最主要的方式，如何在搜索引擎查询结果中获得较高排名是各种商业网站都在考虑的一个关键问题，也由此衍生出大量的搜索引擎优化(SEO)技术手段，而其中一些违反道德甚至法律的被称为黑帽 SEO 技术，比如通过“黑站”在受害网站中植入一些暗链，利用恶意植入大量这些较高 PageRank 值受害网站到推广网站的链接，提升推广网站在搜索引擎中的排名。而网络购物领域也普遍遭受到恶意作弊与操纵，特别是针对这个领域中的市场领先者——淘宝、拍拍、有啊，目前在地下产业链中已经出现了为网店刷排名、人气、信誉的黑帽服务平台，如我拍互动平台（www.webgj.com.cn），该网站采用互刷方式，设计了各种刷客任务，并通过制定发布点赚取、购买与回收的地下黑市行情价格，从中获取差价利益。截止 2012 年 2 月底，该平台会员数量已达 8 万多人，而累计刷钻任务数多达 2245 万个。根据该平台实时资金动态显示，7 个小时内获得会员刷钻消费金额为 1920 元，以此粗略推算每年收入可达到近 240 万元。此外面对类似“刷客”威胁的还包括以苹果 APP Store 为代表的各种手机应用商店排行榜，2012 年 2 月份奇虎 360 旗下所有移动应用遭苹果在惯例检查中下架，也使得这条借助 APP Store 排行牟利的地下黑色利益链浮出水面[360APP 下线事件 2012]。各种网络票选活动也极易遭受地下产业链“刷票”影响，而使得其结果被人为干预和操纵，而无法被互联网网民所接受。“刷客”背后所依靠的则是从互联网中窃取或者通过“网赚”模式集结的大量资源，包括流量、IP、网络“水军”等等。

通过百度搜索“刷票公司”可以查询到 70 多万个网页，而其中占据前 50 页的都是各个“刷票公司”广告网站。而根据一些调查，一些规模较大的刷票公司，年收入均能达到百万元以上，这种刷票作弊行为在中国互联网上的泛滥已经使得各种网络票选、排名都已经失去了诚信，也会让依赖互联网推广的各个相关行业都陷入了无序化恶意竞争，从而失去良性蓬勃发展的机遇。

(7)敏感数据窃取与修改

在通过各种攻击手段取得对联网计算机、服务器和智能手机的控制之后，恶意攻击者可能进一步窃取或者修改系统上的敏感数据，包括个人隐私信息、用户资料数据、商业情报、知识产权、公用事业数据、甚至国家秘密等等。

情报与隐私信息盗窃出售是这条地下产业链中最主要的盈利模式。2009 年央视 315 晚会曾曝光过个人隐私盗取与贩卖的非法产业链，大量真实的个人隐私信息库在互联网上被公开叫卖，而价格非常低廉，仅仅花 100 元就可以买到一千条详细记录了姓名、手机号码、身份证号码等等的个人信息。此外进行非法买卖甚至还包括身份证原件与银行卡等与个人身份密切相关的凭证。这种个人隐私信息在互联网地下产业链中的泛滥助长了进一步的网络犯罪，也为网络犯罪者披上了一层隐秘的外衣。商业情报、企业知识产权甚至国家秘密也可能成为地下产业链中的货品，但由于这些信息的敏感性，很少直接通过互联网的地下黑市进行流通，而更多在是通过地下黑市或线下途径接头之后，通过隐蔽的通讯信道进行沟通。

在取得某些公共事业敏感数据库的控制权之后，恶意攻击者还可能通过蓄意篡改数据库内容而取得非法经济利益，例如某黑帽团体假冒白帽李麒名义提供高考、四六级英语、公务员考试分数修改服务案例[改分案 2010]，2010 年 5 月丰台法院宣判的“孟令建利用木马程序更改计算机证书”案件[计算机证书案 2010]，合肥济南警方联合破获的通过入侵中国教育考试网数据库制售虚假证书与学历案件[假证案 2010]，以及 2003 年福建首例黑帽入侵交

警网络操纵违章记录牟利 10 多万元的案件等[违章记录操纵案 2003]。

2011 年末的 CSDN、天涯、人人等网站用户资料泄露事件让大型互联网网站用户资料库的安全备受质疑，也让用户资料库的“刷库”与“洗库”产业链在网民大众面前所曝光。CSDN、天涯网的用户资料库早在两年前就被入侵窃取，而一直在地下产业链中秘密流通，网名“臭小子”的许某某出于个人炫耀目的，于 2011 年 12 月 4 日在乌云网上发帖称 CSDN 等网站数据密码被泄露，并公布泄露的数据包截图，被公安机关予以训诫。而新浪微博、开心网、7K7K 网站、当当网、凡客诚品等网站均未被入侵。网上公布的上述网站部分账号密码系有人利用网络远程大规模猜测密码所破解（即一种“洗库”方式），实施密码破解的人员身份目前已被锁定，并被公安机关实施抓捕[CSDN 事件 2012]。CSDN 事件曝光后，国内著名白帽黑客龚蔚接收媒体采访时也对地下产业链“洗库”过程进行了介绍[龚蔚 2011]，即对“刷库”获得的数据库中资源进行层层利用，例如在 CSDN 等网站用户资料库泄露事件中，黑帽可能首先针对支付宝、网银、网络购物等账户进行尝试，如果成功即实施真实资产盗窃；第二波则针对腾讯 QQ、网游账户进行破解尝试并窃取网络虚拟资产；再进一步便是对于个人信息、关联手机号、邮件地址的收集，通过将个人信息出售取得利益，这样一层层“洗”下去直至没有价值为止。

2.3.4 互联网资源与服务滥用典型案件研究

江苏省苏州市虎丘区人民法院于 2009 年 11 月份审理的“胡 X、李 X 破坏计算机信息系统案”[剑客案 2009]便是一例由互联网资源与服务滥用地下产业链所驱动的典型案件。根据法院庭审记录：“2009 年 3 月 27 日至 3 月 31 日期间，被告人胡 X、李 X 利用‘剑客压力测试’软件控制大量在线‘肉机’，连续多次通过其控制的攻击器及其‘肉机’以‘DDOS 拒绝服务’的方式向苏州金游数码科技有限责任公司设置在南京龙江机房的游戏平台服务器实施攻击干扰，致使 IDC 网络严重阻塞，无法为客户提供正常服务，最终造成机房内的服务器瘫痪，造成该公司严重损失，并以此为要挟，勒索该公司游戏币‘银子’5 亿两。后两被告人销赃得款人民币 18750 元”。最终法庭以破坏计算机信息系统罪，分别对胡 X 判处有期徒刑二年六个月，对李 X 判处有期徒刑二年四个月。

该案件中涉及的“剑客压力测试”拒绝服务攻击软件在地下产业链黑市中早已流通，而软件编写者曾在百度贴吧中专门开设“jkddos 吧”来推销这款 DDoS 攻击工具软件，并开设“www.jkddos.com”网站进行推广。从图 10 所示 2008 年 12 月 29 日发布的该款攻击工具地下黑市推广帖可以看到：软件编写者不仅仅以 788 元/套的价格出售该款攻击软件，还赠送 500 个僵尸网络“肉鸡”，同时还承接对客户指定网站进行拒绝服务攻击的任务单。而该案件中的被告人则通过地下产业链购得此款攻击软件，以及大量“肉鸡”资源，然后滥用这些在线“肉鸡”资源对网游厂商服务器实施干扰攻击，并以勒索敲诈方式获得网络虚拟资产，并最终通过对网络虚拟资产在网络营销渠道中的套现，取得现实经济利益。该案件中被告人实施拒绝服务攻击勒索敲诈的前提资源是通过地下产业链支持获得的，其犯罪过程也是依照了地下产业链中已形成的一种非法盈利模式，而最后勒索获得的网络虚拟资产也通过地下产业链进行变现，因此，此案是一个能够反映出**图 7** 所示互联网资源与服务滥用地下产业链结构的典型案件。

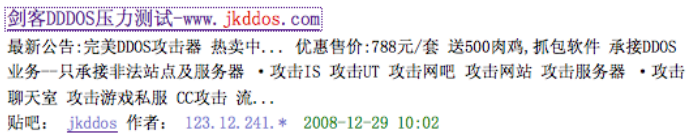

剑客DDDOS压力测试-www.jkddos.com
最新公告:完美DDOS攻击器 热卖中... 优惠售价:788元/套 送500肉鸡,抓包软件 承接DDOS
业务一只承接非法站点及服务器 ·攻击IS 攻击UT 攻击网吧 攻击网站 攻击服务器 ·攻击
聊天室 攻击游戏私服 CC攻击 流...
贴吧： jkddos 作者： 123.12.241.* 2008-12-29 10:02

图 10 剑客压力测试拒绝服务攻击软件在地下黑市中的广告帖

2.4 黑帽技术、工具与培训地下产业链

正如信息技术对信息产业的重要性一样，黑帽技术始终深刻地影响着整个信息安全地下产业链的形成和发展，并渗透到地下产业链中的各个环节，为其运转提供动力。

2.4.1 黑帽技术、工具与培训地下产业链结构分析

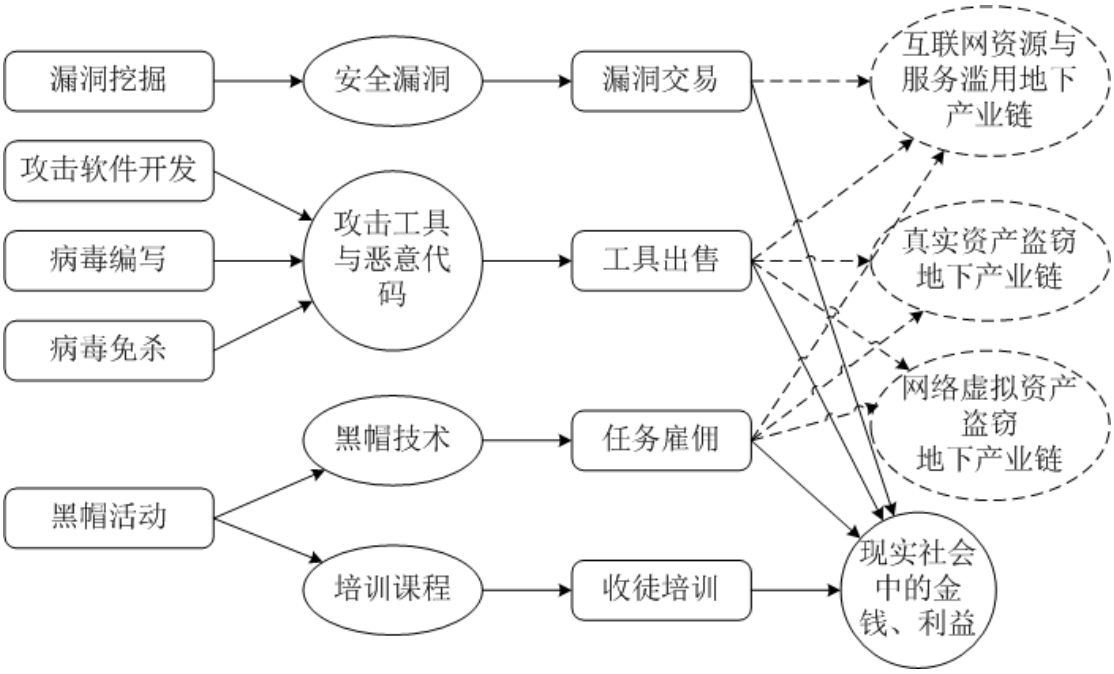


图 11 黑帽技术、工具与培训地下产业链

黑帽技术以产品和服务两种形式存在于地下产业链中。从产品角度来看，黑帽利用自己所掌握的技术来编写各种恶意程序，或者挖掘软件安全漏洞，然后将恶意程序和安全漏洞作为自己的产品出售给另外三条产业链中的不法分子，为他们提供“武器弹药”，使他们有能力从事网络犯罪活动。从服务角度来看，黑帽也会接受临时的雇佣，完成雇主指定的入侵、黑站、窃取个人信息或情报等任务。除此之外，黑帽还透过“收徒”方式将黑帽技术有偿传授给新人，或者借无偿教学名义免费雇佣劳动力，为产业链源源不断地输送新鲜血液。

2.4.2 黑帽技术、工具与培训地下产业链角色与行话分析

在地下产业链行话中，招募黑帽从事网络犯罪活动被称为“黑客任务”。提供黑帽技术培训服务被称为“收徒”；而如果有人想寻求黑帽技术培训服务，一般会发布“拜师”的信息。“马”是木马的简称，一般是以窃取网银、支付、网游等涉及真实资产与网络虚拟资产的软件账号密码为目标的盗号木马，实现此类木马的黑帽称为“木马编写者”，“免杀”则是指逃避安全软件的查杀，是编写木马过程中的重要环节。“0day”则是指尚未有软件厂商的修补补丁的最新软件安全漏洞，通常是未经公开披露，只掌握在漏洞发现者及其出售的少量客户中，是非常宝贵的攻击资源。

2.4.3 黑帽技术、工具与培训环节剖析

- **安全漏洞技术手段剖析**

安全漏洞是指在系统安全流程、设计、实现或内部控制中所存在的缺陷或弱点，能够被攻击者所利用并导致安全侵害或对系统安全策略的违反。安全漏洞存在于计算机的软件、硬件，以及个人与组织的管理流程当中。其中软件安全漏洞是最受黑帽们青睐的，对黑帽而言，软件安全漏洞是他们远程攻击计算机的“便捷暗道”，因为软件安全漏洞可以帮助黑帽绕开受害者系统中的层层安全防护措施，轻而易举地获得系统的控制权，进而实施他们蓄谋已久的各种计划。

由于软件安全漏洞的独特价值，吸引了不少技术精湛的黑客专门挖掘漏洞。漏洞挖掘主要采用源代码审核（白盒测试方法）、逆向工程与补丁比对（灰盒测试方法）、模糊测试（黑盒测试方法）软件测试技术。在模糊测试中，测试者会向目标软件发送大量的带有攻击性的畸形数据，并实时捕捉目标软件在处理这些畸形数据时发出的各种反馈信息，然后综合判断这些反馈信息，以确定在软件中是否存在可以利用的漏洞。从已公布出来的软件安全漏洞来看，比较流行的软件安全漏洞类型分别为缓冲区溢出漏洞、SQL 注入漏洞、跨站脚本攻击漏洞、PHP 远程文件包含漏洞、内存破坏漏洞等。

而黑帽们在挖掘出软件安全漏洞后，大多会将其拿到地下黑市出售，可以获得丰厚的现金回报。软件安全漏洞的价格一般与软件流行程度有关，从几千元到上百万元不等。例如，微软 Windows 操作系统的漏洞是所有漏洞中价格最高的，因为 Windows 是全球最为流行的操作系统，使用者数量非常多；由于 Adobe PDF/Flash 阅读器及播放器也有数量庞大的使用者，其漏洞的价格也非常可观。

- **恶意代码与免杀技术手段剖析**

恶意代码是实现窃取信息、攻击目标等不良意图的计算机指令集。恶意代码的类型包括病毒、蠕虫、木马、后门、僵尸程序等。早先的时候，编写恶意代码要求编写者拥有比较强的程序编写能力，所以人数很少，也限制了恶意代码的数量。后来网络上不断出现一些有意或无意公布出来的恶意程序源代码，促进了恶意代码编写技能的传播，使更多的人加入进来；同时也降低了能力要求，编写者根据源代码稍加改动就可以制造出属于自己的工具，使得恶意代码数量不断攀升。而恶意代码生成器的出现，则实现了恶意代码的自动化大批量生产，导致恶意代码的数量产生了爆发式的增长。恶意代码生成器是专门用来自动化输出恶意代码的工具，例如盗号木马生成器。使用者只需要在生成器中简单地输入一些自定义的参数，便可以在短时间内获得符合自己要求的恶意代码。

黑帽在对外使用恶意代码之前，必须利用一些的技术手段对恶意代码做一定的修改，例如加壳、添加花指令等，以避免被安全软件查杀，增强与安全软件对抗的能力。这种技术手段就是“免杀”。经过免杀处理的恶意代码就可以被交付使用。

- **黑帽教学与培训手段剖析**

网络犯罪“低成本、高回报”的特性吸引了大批的新人源源不断地加入到地下产业链当中，这就产生了大量的学习黑帽技能的需求，黑帽教学与培训便迎合了这样的需求。培训对学员没有要求，不需要学历，不需要经验，也不需要懂英语，只要花上几百元，就能参加培训。黑帽教学与培训都是在网络上来完成的。一部分黑帽会在网站、论坛、聊天工具中散播有偿“收徒”的广告，然后使用聊天工具对学员进行一对一的授课。而最主要的培训方式便是形形色色的“黑客培训网站”，这些培训网站采用会员制方式来招募学员。付费成为会员

之后，学员就可以从网站下载黑帽工具及培训教材，网站和群中会有专门的客服人员随时来为学员答疑解惑。2010 年 2 月，湖北警方摧毁以提供非法控制计算机信息系统程序为主要内容的国内规模最大的黑客培训网站“黑鹰安全网”[黑鹰案 2010]，该网站自 2005 年开办以来，共招收收费会员 12,000 多人，普通会员达到 17 万余人，收取会费逾 700 万元。

2.4.4 黑帽技术、工具与培训典型案件研究

2009 年由公安部挂牌督办的“温柔”系列木马团伙案[温柔木马案 2009]是一起典型的提供黑帽技术与工具的案件。该案涉及全国 16 个省市，涉案人员百余人，金额 3000 多万元，据称占全国盗号木马份额的 50%。

经法院审理查明，2007 年 6 月至 2008 年 8 月间，被告人吕 XX、曾 XX 等为牟利在广东省深圳市，先后编写出国内流行的风云、完美国际、武林外传，QQ 自由幻想等 40 余款网络游戏的木马程序，用于窃取网络游戏玩家的帐号、密码，并由曾 XX 出面寻找合作伙伴帮助销售。2008 年 2 月起，被告人严 XX 接受曾 XX 的委托，将该系列木马程序，以其女友网名“温柔”命名并总代理销售，同时按照不同网络游戏类型由吕 XX 将该木马程序修改后分包给不同的一级代理商张 X、张 XX 等人，并按照包用时间向后者收费，谋取非法利益。至案发前，吕 XX 等人针对不同网络游戏类型开发并销售的“温柔”系列木马程序达 28 款，盗窃游戏账号、密码超过 530 万组。被告人吕 XX、曾 XX 二人共同获利 64.5 万余元，严 XX 及女友共获利 31 万元。吕 XX、曾 XX、严 XX 等 11 名被告人分别因犯提供侵入计算机信息系统程序罪和非法获取计算机信息系统数据罪，被法院一审判处有期徒刑三年至有期徒刑六个月、缓刑一年，拘役六个月，缓刑一年不等的刑罚，法院还分别对被告人并处罚金，总计人民币 83.3 万元。

在本案中，吕 XX 和曾 XX 承担了黑帽地下产业链中的木马编写者角色，编写出大量盗号木马，而严 XX 及女友作为“木马代理”负责“温柔”木马的销售推广，并通过网络发展出张 X、张 XX 等“包马人”，由他们进一步提供到下游产业链，支持针对网游的网络虚拟资产盗窃。

3. 信息安全地下产业链实证分析

3.1 实证分析方法

为了更加深入地调查掌握中国互联网上的信息安全地下产业链现状与发展趋势，我们综合采集了多种不同来源途径的地下产业链信息，进行深入的实证数据分析，从而估计各个产业链的产值规模、威胁人群数量、参与者与业务分布情况等等，并试图揭示出地下产业链与网络犯罪中的直接关联关系。

我们对地下产业链进行调查分析的数据来源包括如下三个渠道。

(1) 国内主流安全厂商与国家安全监管部门的安全威胁监测报告与数据统计资料，我们收集了安天、金山、奇虎360、瑞星、腾讯QQ电脑管家、网秦、知道创宇等安全公司2011年度安全报告及相关专题报告，以及中国反钓鱼网站联盟（APAC）、国家计算机网络应急技术协调中心（CNCERT/CC）、中国国家安全漏洞库（CNNVD）等国家安全监管部门针对不同类型安全威胁的统计数据。

(2) 由地下产业链驱动的网络犯罪案件公开卷宗资料与媒体报道，利用作者单位订阅的法律案件数据库，我们从中搜索并查阅了由地下产业链驱动的典型网络犯罪案件原始法庭卷宗资料，并通过搜素引擎查找了大量与这些案件相关的媒体报道。

(3) 互联网上的地下产业链黑市广告与交流信息，我们对地下产业链进行深入了解之后，定位出了目前中国互联网上主要的地下产业链黑市位置，并对黑市广告与交流信息进行了持续监测。

在这三个数据来源中，前两者均为通过公开渠道可搜索并获取到的信息资源，而地下产业链黑市则是隐藏在互联网之中的秘密信息发布与交流渠道。国外主要国家的地下产业链通常使用IRC实时聊天协议作为黑市广告发布与沟通途径，而由于中国互联网与用户上网行为的独特性，中国互联网地下产业链的广告信息发布与交流途径与国外有着很大的差别，主要采用Web论坛和QQ群进行黑市广告信息发布，而利用QQ私聊方式进行沟通交流，最后的交易支付则主要采用银行汇款和支付宝方式[1]，其中支付宝能够提供交易担保机制，地下产业链参与者在与未建立信任关系的初次合作者进行交易时，往往使用支付宝进行支付。

在目前已经形成了社会角色分工与上下游环节的地下产业链中，参与者希望自己的供需信息能够被更多其他参与者关注到，从而能够以有利条件达成交易获得更丰厚的利益回报，因此地下产业链往往选择采用简单便捷的访问方式来构建网络上的交易黑市环境，而依赖于一些行话术语来尽量地增加地下黑市和广告的隐蔽性。在中国互联网上，主要的地下产业链黑市构建方式包括Web论坛和QQ群两类。

百度贴吧作为中国互联网上最大的中文社区，提供了基于关键字的贴吧组织方式以及松散便捷的登录与发帖机制，因此吸引了地下产业链的大量参与者，通过一些行话术语作为关键字构建用于发布广告信息的地下黑市，例如“料吧”，不知晓地下产业链行话的普通用户极少能访问到这个隐蔽贴吧，而即使偶然进入也无法理解地下黑市广告的含义。而我们通过对地下产业链的深入了解与分析，已经破译了绝大多数行话术语的含义，因此也就可以通过穷举这些行话术语关键字，监测到百度贴吧上绝大多数用于构建地下黑市的贴吧。我们共计搜索了分属于四大产业链的84个行话术语，在百度贴吧中监测到了129个地下黑市贴吧，同时也发现其他26个采用最常见术语的地下黑市贴吧已经被封禁。由于百度贴吧是一个公

[1] 为了躲避执法部门追查，通常使用冒用身份证的银行卡或支付宝账号进行地下产业链交易。

开论坛，并保留全部历史发帖记录，因此我们可以使用爬虫持续监测并抓取这些地下黑市贴吧中的全部信息记录，并插入到数据库中进行统计分析。

而数量更多的地下产业链黑市则基于 QQ 群方式，地下黑市 QQ 群一般通过在 Web 论坛黑市中发布群号与业务类型，或者在 QQ 群名和描述中包含行话术语的方式，吸引地下产业链参与者加入。在申请加入 QQ 群后，QQ 群主会根据申请理由判断申请人是否业内人士，然后决定是否接收进入 QQ 群。我们基于对行话术语的破译，在腾讯 QQ 提供的 QQ 群搜索功能中以行话术语关键字进行搜索。我们共计搜索了 84 个关键字，搜索到 2,738 个 QQ 群，但由于工作量和时间关系，我们仅仅选择性地加入人员规模超过一定阈值的 QQ 群，实施地下黑市监测，我们共加入了 130 个 QQ 群，并于 2012 年 3 月至 5 月份进行了三个月的监测。

在获取地下黑市监测信息后，我们分别针对百度贴吧与 QQ 群编写了数据解析与入库程序，将监测信息插入到 MySQL 数据库中，对于百度贴吧匿名用户的 IP 地址信息，我们采用纯真 IP 定位数据库查询获得这些用户上网 IP 的所在省份、城市与具体位置，补充到数据库中，并进一步在 MySQL 数据库中编写了一系列的消重、标记、分类统计的存储过程，对地下黑市监测信息进行细致深入分析，得到地下产业链黑市规模与发展趋势、参与者规模与分布情况、业务类型分布等监测结果，为更为深入地理解地下产业链提供指导。

在公开渠道收集到安全威胁统计数据与典型网络犯罪案例信息，以及通过黑市监测获取到大量地下产业链广告与交流信息的基础上，我们将在 3.2 节中对地下产业链涉及安全威胁进行实证数据分析，展示各种安全威胁的规模与分布特性，并尝试利用各大地下产业链安全威胁统计数据及相关互联网行业的市场调查报告，估计测算出各大地下产业链的盈利规模与危害范围。在 3.3 节中则主要对地下产业链黑市信息进行细致的实证数据分析，给出地下黑市的内部特征与发展趋势。最后在 3.4 节将对公开渠道典型网络犯罪案件信息与地下黑市监测信息进行关联分析，说明监测地下黑市信息对于网络犯罪侦查与态势监控的支持作用。

3.2 地下产业链涉及安全威胁实证数据分析

在本节中，我们将利用公开渠道收集到的国内主流安全公司的安全报告，以及国家网络安全监管部门对特定安全威胁的统计数据，结合相关互联网商业市场调查报道，分别针对真实资产盗窃、网络虚拟资产盗窃、互联网资源与服务滥用、黑帽技术工具与培训地下产业链，进行相关安全威胁现状分析，并测算各个地下产业链的盈利规模与危害范围。

3.2.1 真实资产盗窃威胁实证分析

在中国互联网上的网络购物领域，淘宝占据了绝对统治地位，据艾瑞咨询最近统计数据显示，2011 年中国网络购物市场交易规模达 7735.6 亿元，较 2010 年增长 67.8%，其中 C2C 交易规模 5944.5 亿元，而淘宝网一家独大，市场份额占到了 90.4%；平台式 B2C 交易规模 955 亿元，其中淘宝商城（已改名天猫）占 53.3%份额[艾瑞购物 2012]。而淘宝网采用支付宝进行网络购物支付，网民用户在使用支付宝时普遍使用网上银行进行账户充值，并在支付宝账户中通常留有一定的余额，有媒体计算淘宝全年日均沉淀资金达到近 60 亿元，此外近 80%的用户倾向于将支付宝与网银绑定以支持“快捷支付”[快捷支付 2011]，这使得安全风险进一步增大。而在网上银行领域，根据艾瑞咨询《2010-2011 年中国网上银行年度监测报告》数据显示[艾瑞网银 2011]，2010 年中国网上银行交易规模达到 549.5 万亿元，同比增长 49.0%，工商银行、农业银行、招商银行在个人网银交易规模占据前三甲，分别占比 36.4%、20.2%和 10.9%，中国银行排名第 6 位，占比 4.4%，但在国际结算业务方面有着绝对优势，排名全球第一。

由于利益导向的原因，中国互联网上的真实资产盗窃地下经济链也将主要攻击目标瞄准了这些占有领先市场份额的网购和网银平台。

- **真实资产盗窃威胁统计分析**

真实资产盗窃已经对中国互联网网民构成了非常普遍的威胁，据 CNNIC 统计，2011 年上半年，有 8%的网民在网上遭遇过网购欺诈或被盗，该群体规模达到 3880 万人，也即每 12 位网民中就有 1 位遭遇过网购欺诈或被盗！[CNNIC 2011]

奇虎 360 与易宝支付联合发布的《2011 年网购支付安全报告》显示[360 网购 2012]，网购与支付安全的威胁主要有网络钓鱼、恶意欺诈和账户被盗三大类，其中网络钓鱼因其技术含量高、隐蔽性好，不易被消费者察觉，因而成为网购与支付安全最大的危害。恶意欺诈就是商户实施诈骗，没有任何技术含量，而账户被盗主要是由于用户不小心或是中了木马导致自己的账户信息被不法分子盗取致使自己的钱财受损。在易宝支付 2011 年投诉中，网络钓鱼、恶意欺诈及账号被盗的比例分别为 89%、8%与 3%，网络钓鱼威胁占据绝对主流的地位。

(1) 网络钓鱼威胁数据分析

根据中国反钓鱼网站联盟（APAC）2011 年工作报告数据显示[APAC 月报 2011]，2011 年全年联盟处理钓鱼网站 40,219 个，我们对每个月 APAC 钓鱼网站处理简报中的数据进行汇总统计之后，得到了如图 12 所示的全年钓鱼网站行业分布图，可以看到与真实资产盗窃或诈骗有关的支付交易（占 81.04%）、金融证券（占 10.16%）、媒体传播（1.81%）等行业排名靠前，且总体占据了超过 93%的比例。钓鱼网站的具体仿冒对象 Top 10 列表如**表 1**：淘宝网以 66.81%绝对优势占据榜首位置，这也其在网络购物市场中的霸主地位相吻合；央视由于《非常 6+1》等涉及中奖栏目的广为人知，也成为了钓鱼网站最看好的“鱼饵”之一，特别是在 2011 年年初和春节期间非常活跃，以 13.56%占据第二位置；网银类网站中排名最靠前的也是市场份额最大的中国工商银行，以 4.69%排名第四位。

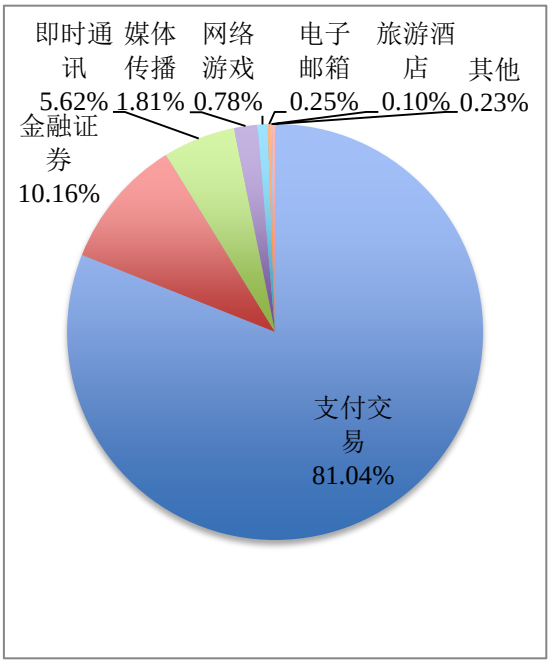


图 12 中国反钓鱼网站联盟 2011 年处理钓鱼网站行业分布图[2]

[2] 数据源为 APAC 网站上公布的 2011 年月度钓鱼网站处理简报，图表基于数据统计结果绘制。

2011 年中国反钓鱼网站联盟处理的钓鱼网站中使用.cn 域名的仅有 207 个，占 0.51%，而使用非.cn 国外域名的则有 40,012 个，占 99.49%。这也反映出网络犯罪者为了躲避法律追查，以及避免国内严格的网站备案流程，往往注册国外域名部署钓鱼网站以实施网络钓鱼攻击，使用最多的是管理比较松散的.tk（25.11%）、.cc（19%）、.pl（12.23%）、.com（11.49%）与.info（10.44%）。

表 1 中国反钓鱼网站联盟 2011 年处理钓鱼网站的仿冒对象排名 Top 10 列表

排名	仿冒对象	钓鱼网站数量	比例
1	淘宝网	26871	66.81%
2	央视	5455	13.56%
3	腾讯	2816	7.00%
4	工商银行	1887	4.69%
5	中国银行	626	1.56%
6	网易	251	0.62%
7	新浪	248	0.62%
8	招商银行	177	0.44%
9	雅虎	154	0.38%
10	盛大	152	0.38%
	其他	1583	3.94%

中国的个人终端安全厂商也普遍在提供的个人安全防护产品中增加了钓鱼网站识别与拦截功能，帮助互联网网民对抗由地下产业链所驱动的网络钓鱼威胁。瑞星、360、金山、腾讯 QQ 电脑管家在最近发布 2011 年安全报告中[电脑管家年报 2012]都包含了对钓鱼网站威胁的拦截统计数据，如**表 2** 所示，由于各家的软件装机量、统计方式、数据精确度等各方面的问题，我们无法也无必要进行横向对比，但可以通过各个厂商的统计情况，及纵向与 2010 年度相比的增长幅度，看出中国互联网上钓鱼网站威胁的大致规模与发展情况。

在截获钓鱼网站数量方面，各厂商的统计数据均显示较 2010 年有非常显著的增长趋势，特别在下半年集中爆发，奇虎 360 于 2011 年截获超过 50 万家钓鱼网站（以网站域名计数），较 2010 年同比增长 259%[360 网购 2012]，而瑞星公司截获 480 万左右钓鱼网站页面（以 URL 计数），较 2010 年同比增长 174%[瑞星年报 2012]。从 APAC 反钓联盟处理钓鱼网站数量规模（4 万）与厂商拦截钓鱼网站数量规模（超过 50 万）的比较，我们可以看出得到有效汇总与处置的钓鱼网站数量只占据了很小的比例，其中一方面原因是钓鱼网站普遍的生命周期都很短，攻击者实施钓鱼攻击后也会很快废弃网站，另一方面大多数钓鱼网站都普遍使用国外域名并架设在国外，这也给快速处理增加了协调成本与处置难度。在拦截访问钓鱼网站人次方面，瑞星为 1.9861 亿人次，奇虎 360 为 21.5 亿人次，金山[金山年报 2012]与腾讯 QQ 电脑管家[电脑管家年报 2012]未提供精确数据，分别宣称为每月 4-11 亿次和下半年 10 亿余次，都均较 2010 年同比显著增长。而与此同时，瑞星、金山、腾讯 QQ 电脑管家统计数据均显示挂马网站威胁呈现下降趋势，钓鱼网站已取代挂马网站成为终端浏览安全的最严重威胁。各厂商对钓鱼网站威胁发展新趋势也都有较为一致的总结，包括以蓬勃发展的网购应用作为最主要的攻击对象，社交网络和即时通信成为钓鱼网站传播的主要途径等。奇虎 360 特别针对网购与支付实施钓鱼攻击的钓鱼网站进行了监测，2011 年 1 月至 11 月共截获购物钓鱼网站 253,188 家，占到所有钓鱼网站的一半以上，而拦截此类钓鱼网站访问量 5.73 亿次。[360 网购 2012]

表 2 国内个人安全厂商对 2011 年钓鱼网站威胁的统计数据

项目	金山	奇虎 360	瑞星	腾讯 QQ 电脑管家
截获钓鱼网站数量	45 万左右[1]	501708[1]	480 万[2]	492 万[2,3]
截获网站较 2010 年同比增长	无 2010 年对应数据	259%[4]	174%	无 2010 年对应数据
截获人次	每月 4 亿~11 亿之间	21.5 亿	1.9861 亿	10 亿余[3]
截获人次较 2010 年同比增长	2010 年最高仅 1000 万次	24%[4]	350%	无 2010 年对应数据
钓鱼网站假冒对象前三	淘宝、中奖、六合彩	网购、中奖、彩票	QQ、“非常 6+1”、淘宝	无数据
1. 按网站域名计数 2. 按 URL 计数 3. 参照腾讯 QQ 电脑管家联合艾瑞咨询发布的《2011 下半年个人网络安全报告》，未有全年数据。 4. 参照奇虎 360 的发布《2010 上半年中国互联网安全报告》，未有全年数据，平均至全年计算。				

(2) 支付账户盗窃威胁数据分析

易宝支付风控中心在 2011 年 1 月至 10 月中接收到 169 次网购市场账户被盗事件的用户投诉[360 网购 2012]，而据数据统计，易宝支付注册用户规模大约为 4200 万，日交易额突破 2 亿元[支付行业 2011a]，以 10%的账户遭窃用户投诉率估计，2011 年账户遭窃造成损失的用户数量大约为 2000 人，占万分之 4.8 左右，与行业调研数据吻合。截至 2011 年 12 月底，我国使用第三方支付的用户账号数超过 10 亿[支付行业 2011b]，以此测算，遭遇支付账户盗窃造成损失的用户规模达到 48 万以上。

- **真实资产盗窃地下产业链规模测算分析**

中国工商银行一直是个人网银客户量最多的银行，也是网络犯罪者实施真实资产盗窃最主要的攻击目标，早在 2006 年 7 月份，中国工商银行大量使用账号密码方式登录的大众版网银客户由于遭遇钓鱼网站、网银木马等攻击而导致网银余额被盗取，当时部分受害者发起了“工行网银受害者集体维权联盟”，通过集体诉讼争取全额赔偿损失。据报道，截止 2006 年 12 月底，“工行网银受害者集体维权联盟”上便有近 500 位受害者实名登记，公布损失达到 350 余万元，最多 38.9 万，最少 100 元，平均每人损失近 7,000 元[工行网银维权 2006]。而 2006 年底中国工商银行个人网银客户数为 2325 万[工行数据 2006]，以 10%网银被盗受害者参与“维权联盟”进行实名登记保守估计，那么将有近 5,000 位客户遭遇网银被窃，占工商银行网银客户总量的万分之二左右，而损失金额估计为 3,500 万元。2011 年 3 月末，工行个人网上银行客户数已超过 1 亿户，达到 1.02 亿[工行数据 2011]，如果网银被窃客户比例和平均失窃金额仍保持 2006 年水平，那么 2011 年估算仅涉及工行的真实资产盗窃损失额便可达 1.53 亿元。以 2011 年工行个人网银市场占有率 36.4%推算[艾瑞网银 2011]，中国网银用户遭受真实资产盗窃的损失总额将达到 4.2 亿元，涉及大约 6 万名受害者。而这仅仅是个保守估计，一些媒体曝光案件中动则几百万，甚至几千万的银行卡盗取盗刷涉案金额，使得我们对国内网银用户的安全性深感担忧，公安部“天网-2011” 打击银行卡犯罪专项行动中共计破获案件 2.4 万余起，挽回经济损失 4 亿元，这也从另一个侧面反映出网银失窃盗刷直接损失规模在数亿元甚至十亿元量级。[公安部 2011]

除了网银账户之外，第三方支付账户余额也可能遭受真实资产盗窃威胁，根据前述对支

付账户盗窃威胁的测算分析，2011 年至少有 48 万人遭遇支付账户金额盗窃损失，另外据金山公司于 2011 年 5 月至 7 月间的 1062 位网购被盗受害者调查，平均每位受害者被盗金额为 3437 元[金山网购 2011]，以此推算第三方支付账号遭受盗窃造成的直接经济损失在 16.5 亿元左右，占 2011 年第三方支付市场规模 21610 亿元[易观 2011]的万分之 7.6。

3.2.2 网络虚拟资产盗窃威胁实证数据分析

网络游戏一直是中国互联网上用户规模最庞大的应用之一，2011 年度中国游戏产业年会发布的《2011 年度中国游戏产业调查报告》显示，去年国内游戏市场规模达 446 亿元，同比增长 34%，同期国内 PC 网游用户达 1.2 亿人，同比增长 9.1%[游戏产业调查 2011]。其中腾讯、网易与盛大作为网游行业的三巨头，分别占据 35.4%、13.9%和 11%市场份额[艾瑞网游 2011]。这些主流网游厂商均采用了虚拟货币充值方式，让玩家获得虚拟货币后进行支付游戏业务、购买游戏道具与装备，同时在游戏内部也往往支持玩家之间的虚拟货币与装备交易。这就使得网游中的虚拟货币与装备具有了现实价值，然而国内法律尚未有明文法律对其进行保护，因此这些虚拟资产就成为了地下产业链的盗窃目标。网游行业老大腾讯游戏直接使用腾讯 QQ 账号进行登录，并支持使用 Q 币来支付各种游戏业务、道具与装备等，因此 Q 币也成为了目前中国互联网上使用范围最广的虚拟货币。这也让腾讯 QQ 账号及账户内 Q 币成为了网络虚拟资产盗窃地下产业链最普遍的交易商品。

根据奇虎 360 发布的《360 网络游戏 2011 上半年安全报告》[360 网游 2011]，2011 年上半年网络游戏安全主要的三大威胁为网络钓鱼欺诈、木马盗号和骗号（通过社会工程学攻击手段），所占比例分别为 53%、38%和 9%。游戏类钓鱼网站累计数量超过 3 万家，超越传统盗号木马方式，成为网游安全的最大威胁，游戏类钓鱼网站主要传播途径集中在假冒 GM（游戏管理员）消息、游戏内消息、论坛及 IM，分别占 80%、11%、5%和 4%，360 共计拦截到 3,862 万次游戏类钓鱼网站访问。中国反钓鱼网站联盟 2011 年统计数据显示腾讯、网易、盛大等主流网游厂商也是钓鱼网站仿冒的主要对象，分别占 7%、0.62%和 0.62%。奇虎 360 在 2011 年上半年新监测到网游盗号木马数量约为 7900 万个，比去年同期下降 19.8%。360 共计拦截并查杀 20.54 亿次网游盗号木马，自 2011 年 3 月份开始，360 观测到网游盗号木马活跃度正在逐渐下降，6 月份更是达到近年新低，显示出网游盗号木马威胁正在衰退。

据 360 统计，上半年网游玩家被盗号的经济损失在 8 亿元左右，占网游市场规模的 5%以内，但 360 并没有在报告中给出具体测算方法。而根据腾讯 QQ 电脑管家对 2000 名网民开展的调查问卷显示，32%网民遭遇过游戏账号被盗号困扰，保守估计其中 10%的网游用户由于盗号而遭受了经济损失，每次平均损失金额为每年网游花费的 371 元，可以测算得出由于网游盗号遭受损失玩家 384 万人，造成直接经济损失金额在 14.2 亿元，占 2011 年网游市场规模的 3.18%。

3.2.3 互联网资源与服务滥用威胁实证数据分析

依照我们对互联网资源与服务滥用地下产业链结构的分析结果，我们从终端主机、智能手机与网站服务器这三类主要的互联网资源，分别对受控木马与僵尸网络、手机恶意代码与网站安全三方面，展开对互联网资源与服务滥用威胁进行实证数据分析。

- **受控木马与僵尸网络威胁统计分析**

反病毒厂商通常只能依靠客户端软件拦截恶意代码感染的数据汇总分析恶意代码疫情情况，而难以监测到真正被木马或僵尸程序控制主机的数量规模。CNCERT/CC 则具有基本覆

盖全网的网络安全监测能力，可以利用主流木马与僵尸程序的网络通讯特征，检测出被控主机与控制服务端的网络通讯行为，因此可以提供出较为全面的受控主机与控制服务端的规模统计数据。

根据 CNCERT/CC 针对 200 至 300 种流行木马与僵尸程序的监测数据[CNCERT/CC 月报 2011]，2011 年每月中国境内被木马或僵尸程序控制的主机 IP 数如图 13 所示，最高在 3 月份达到 182 万，最低为 7 月份的 27 万，平均每月 84.58 万，累计全年 1015 万次，消除重复后为 890 万[CNCERT/CC 年报 2011]。而每月监测到用于控制这些主机的服务器 IP 数如图 14 所示，最高在 12 月份为 39,167 个，最低为 2 月份的 22,100，累计全年近 34 万，其中境内服务器 25.4 万，境外服务器 8.6 万。由于 CNCERT/CC 现有平台的样本监测覆盖面及网络范围仍然不够完备，因此中国境内的受控主机数量还远远不止此数。而数量庞大的受控僵尸主机为中国互联网地下产业链提供了源源不断的后备资源。

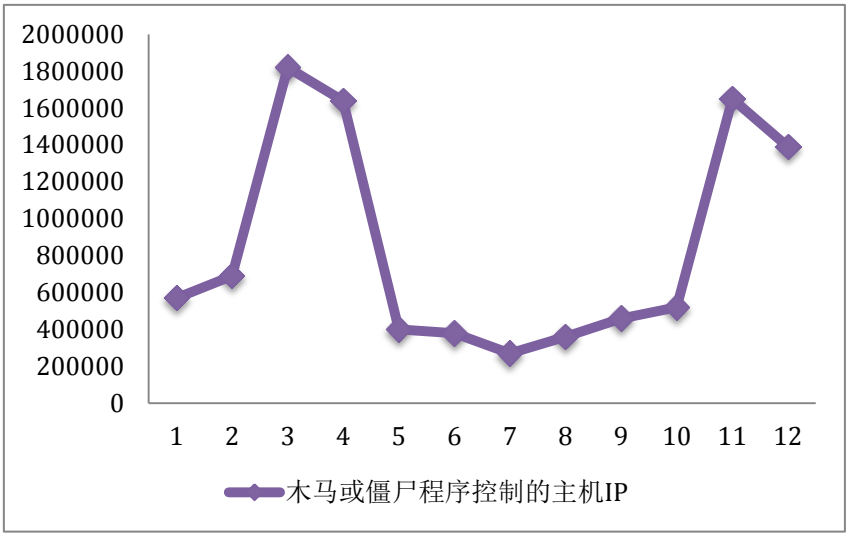


图 13 CNCERT/CC 在 2011 年监测木马或僵尸程序控制主机 IP 趋势图

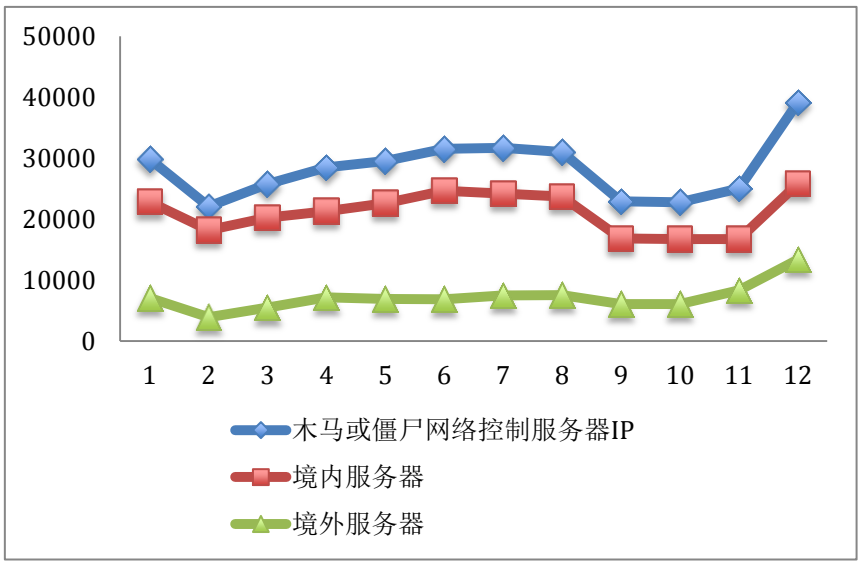


图 14 CNCERT/CC 在 2011 年监测木马或僵尸程序控制服务器趋势图

- **移动终端恶意代码威胁统计分析**

截至 2011 年 12 月底，中国手机网民规模达到 3.56 亿，占整体网民比例的 69.3%，已接近家庭电脑上网网民 3.96 亿的规模[CNNIC 2012]。 2011 年中国智能手机市场最大的改变就是 Android 系统取代诺基亚 Symbian 系统成为最流行的智能手机操作系统，获得了 50.4%的用户关注比例，较 2010 年高出了 36.2%之多，而 Symbian 则从 57.1%下降至 29.3%并已走向末路[智能手机调查 2012]。智能手机恶意代码同样随着这一发展趋势，Android 平台恶意代码也在 2011 年突飞猛进。

国内主要手机安全厂商在 2011 年度安全报告中针对智能手机恶意代码的统计数据（如**表 3** 所示）均显示出手机恶意代码数量迅猛增长，同时 Android 平台恶意代码逐渐超越传统 Symbian 平台恶意代码，成为目前手机恶意代码的主流。在手机杀毒软件市场占据较大份额的金山、奇虎 360 与网秦均拦截了超过千万台次的手机恶意代码感染。而手机恶意代码体现出了由地下经济利益驱动的鲜明色彩，各厂商对样本危害后果的分析数据显示，几乎所有手机恶意代码都具有恶意扣费、隐私信息窃取、远程控制等追求非法经济利益的危害行为。而主要的样本传播途径则包括手机论坛、应用商店、WAP/Web 下载、ROM/存储卡预装等。

据网秦不完全统计，单个手机病毒造成的直接经济损失高达 2,000 万元，而通过山寨机内置恶意软件、或传播手机病毒进行恶意“吸费”行为的手机黑色产业链，保守估计每年收入高达 10 亿元！[网秦估计 2012]2011 年金山手机卫士云安全中心捕获扣费病毒 5670 个，占所捕获新增病毒总数的 24%，感染人群 300 多万，以人均每月被扣费 10 元计算，病毒作者通过扣费病毒全年非法获利高达 3.6 亿元[金山手机 2012]。

表 3 国内手机安全厂商对 2011 年智能手机恶意代码的统计数据

项目	安天	金山	奇虎 360	网秦
手机恶意代码数量	190[1]	23681[2]	8714[2]	24794[2]
Symbian 比例	22.1%(42)	无监测数据	45.8% (3992)	60% (14948)
Android 比例	76.8%(146)	仅针对 Android	54.2% (4722)	38% (9498)
拦截次数	无数据	1037 万	2753 万	1152 万
中国省份分布	无数据	广东、北京、江苏、上海四川	无数据	广东、北京、上海、河南、江苏
危害行为类型前三位	恶意扣费(34%)、信息窃取类(27%)、远程控制(16%)	扣费病毒(24%)、恶意监听软件(15%)、恶意广告软件(14%)	Android:恶意扣费(78%)、隐私窃取(13%)、其他(9%) Symbian:资源消耗(40%)、系统破坏(33%)、恶意扣费(20%)	远程控制(27.3%)、恶意扣费(25.5%)、隐私窃取(16.3%)[3]
传播途径前三位	无数据	无数据	Android:ROM/存储卡预装(29%)、Web/WAP 下载(28%)、应用商店(26%)；Symbian：Web/WAP 下载(75%)、手机论坛(12%)、手机下载站(8%)	手机论坛(24.2%)、应用商店(20.3%)、Web/WAP 下载(17.3%)
1. 按家族计数 2. 按新增样本计数 3. 部分恶意软件同时存在多个危害行为				

- **网站安全威胁统计分析**

根据 CNNIC 统计数据，截止 2011 年底，中国互联网上的网站数量为 230 万，但这仅包含域名注册者在中国境内的网站，大量网站运营者为了免于繁琐的中国互联网网站备案过程，选择在国外注册域名，因此中国互联网上实际网站数量并不止此数，根据知道创宇公司的监测，2011 年共计监测到中国互联网上的网站数量为 553.3 万个。[知道创宇年报 2012]

中国互联网上大量网站由于存在着安全漏洞与配置疏忽，很容易遭受到由地下产业链所驱动的“黑站”攻击，奇虎 360 对 93,233 个网站的采样检测结果显示，存在高危漏洞的网站数占 36%，存在中危漏洞的占 16%，不安全的网站比例超过一半[360 网购 2012]。

在网站遭遇“黑站”之后，普遍的危害后果包括网页篡改、网站挂马、植入黑链和“刷库”，其中前者可以算作灰帽行为，除了为个人赢取黑帽社区中的声望与影响力之外，更多的是出于一些表达诉求与提醒网站安全的动机;而后两种则完全是由地下产业链所驱动的黑帽行为，通过损失网站运营者与访问用户的利益谋取不当收入。

网站挂马从 2006 年开始便成为中国互联网网站最大的安全威胁，在近几年持续高位威胁之后，由于 Windows 主流操作系统平台安全性增强，以及国家网络安全监管部门与各大安全厂商的合力围剿之后，2011 年网站挂马威胁开始呈现出下降趋势，其中瑞星统计数据显示截获挂马网页 URL 数量较 2010 年大幅度减少近 89.74%,但知道创宇仍然监测到了 57,662 个网站被挂马，和 2010 年基本持平，如图 15 中所示，知道创宇监测到的网站挂马数量除了 10 月份与 11 月份由于一些重要系统和软件出现严重安全漏洞，达到 1 万多个的高位，其他月份均维持在 3,000-4,000 之间[知道创宇年报 2012]。这些挂马网站，特别是其中一些访问量较大的重点网站，会对访问网站的终端主机造成严重威胁，一旦终端主机存在挂马页面所利用的安全漏洞并缺乏及时更新反病毒软件的保护，就很可能被植入盗号木马等恶意软件，瑞星、QQ 电脑管家等通过客户端软件截获了数以千万、甚至上亿次挂马网站访问次数。

暗链攻击指的是攻击者在“被黑”网站上植入不可见的隐蔽链接，而这些链接的指向目的并非造成网站运营者与访问终端主机安全风险的挂马网页，而通常是一些需要推广的广告页面，通过暗链攻击，攻击者可以快速提升推广广告页面的 PR 值，从而大幅提升这些页面在搜索引擎检索页面中的排名，即达到 SEO 搜索引擎优化的效果。暗链攻击虽然从表现形式上不对网站和访问用户造成危害，但能够植入暗链已经意味着攻击者可以完全控制“被黑”网站，而如果出现盈利更直接的挂马攻击机会，地下产业链中由经济利益驱动的攻击者完全可能通过出售流量方式，将“被黑”网站用于其他更严重的攻击。由于暗链攻击的隐蔽性，直到 2010 年才由知道创宇在年度安全报告中给出系统的监测统计数据，从而揭示出这种威胁在中国互联网网站中的普遍性。2011 年全年平均每月监测到 171,589 个网站被暗链攻击，累计全年 205.9 万次，如图 15 所示呈现稳步上升趋势。其中私服、医疗、博彩类目标推广网页成为 2011 年暗链攻击排名靠前的三种类型，而私服类网页类型暗链总量，接近于其它类型的总和，医疗类网站也普遍采用暗链攻击此类黑帽 SEO 技术进行推广，这使得我们对中国的医疗现状深感担忧。[知道创宇年报 2012]

表 4 国内安全厂商对 2011 年网站安全威胁的统计数据

项目	奇虎 360	瑞星	QQ 电脑管家	知道创宇
截获挂马网站数量	N/A[1]	347.11 万[2]	246 万[2,3]	57,662[4] (1.04%)
截获量较 2010 年同比增长	N/A	-89.74%	N/A	2%
截获挂马网站访问次数	N/A	8065 万	1.5 亿[3]	N/A
截获次数较 2010 年同比增长	N/A	N/A	N/A	N/A
存在漏洞网站比例	高危 36%	N/A	N/A	N/A

	中危 16%			
植入暗链网站比例	N/A	N/A	N/A	2010：78.7 万次 2011：205.9 万次
1. 将网站挂马拦截都归并入木马病毒拦截中，没有给出单独统计数字 2. 按不同挂马页面 URL 计数 3. 参照腾讯 QQ 电脑管家联合艾瑞咨询发布的《2011 下半年个人网络安全报告》，未有全年数据。 4. 按不同被挂马网站数量计数				

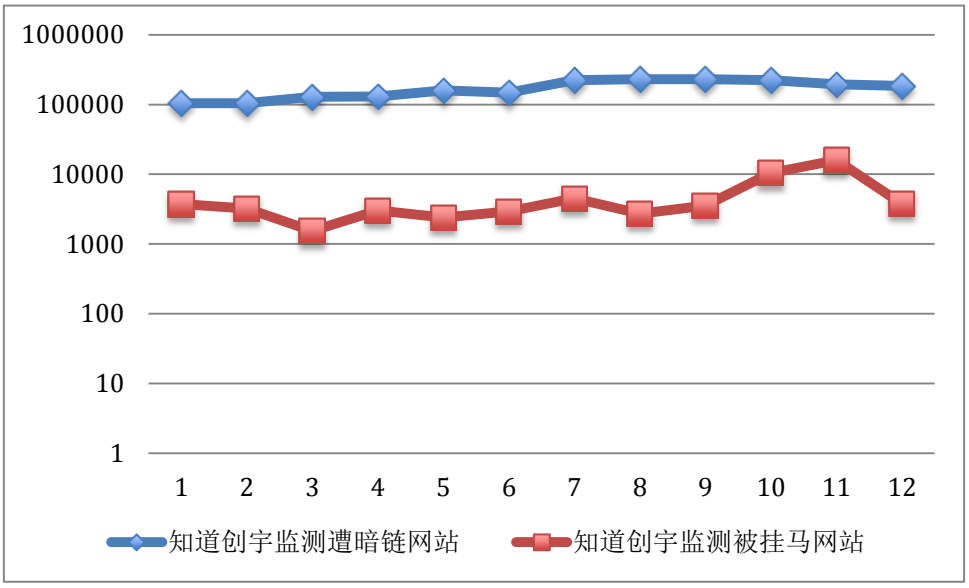


图 15 知道创宇在 2011 年监测到网站安全威胁趋势

3.2.4 黑帽技术与工具威胁实证分析

黑帽技术、工具与培训地下产业链并不直接通过危害互联网用户而牟利，而是通过为其他三条地下产业链提供技术工具支持，获取技术出让、工具销售与服务佣金。国内安全监管部门与安全厂商目前主要针对安全漏洞、恶意代码工具等方面进行监测与数据统计，但尚未对黑帽社区的技术服务与培训进行有效的监控与调查分析。

- **软件安全漏洞威胁数据统计分析**

软件安全漏洞挖掘与利用是黑客技术的精髓，也是黑帽支持地下产业链非法获利的技术源头。负责任的黑客在研究挖掘出安全漏洞之后，会通过 CERT、安全研究组织报告给相应软件厂商，由其进行修复。而黑帽们则更多出于经济利益考虑，选择在地下产业链中出售 0day 安全漏洞，一些 0day 安全漏洞在地下产业链传播一段时间后，会被安全厂商与 CERT 部门截获，从而公开披露漏洞。

国家信息安全漏洞库（CNNVD）与国家信息安全漏洞平台（CNVD）是中国两个由政府部门运营的权威漏洞搜集与发布信息库。CNNVD 在 2011 年收集安全漏洞的月度统计情况如图 16 所示[CNNVD 2011]，全年收集整理安全漏洞数量累计 5595 个，其中危急及高危漏洞 2394 个，占比 42.8%，而在公开披露时尚未有补丁的 0day 安全漏洞数量达到 1401 个，占 25%。CNVD 在 2011 年的收集安全漏洞统计数据如图 17 所示[CNVD 2011a]，与 CNNVD 基本一致，全年收集安全漏洞累计 5547 个，高危安全漏洞 2164 个，占 39%，0day 安全漏洞 1625 个，

占 29.3%，通过公开周报数据[CNVD 2011b]统计 CNVD 在 2011 年共收集私有 0day 漏洞 45 个。

由于 0day 安全漏洞具有的高度价值，因此大量研究挖掘出的 0day 安全漏洞会被秘密地掌握在互联网上各种组织机构、团队和黑客个人手中。目前国外安全公司与机构如 iDefense、TippingPoint 已经构建出如 VCP、ZDI 等安全漏洞市场机制，而国内也在逐渐完善合法的安全漏洞研究与交易市场机制，避免 0day 安全漏洞流入地下黑市，支持地下产业链从而危害互联网安全。但目前国内地下产业链中仍然掌握着较多的 0day 安全漏洞资源，但限于此类信息的私密性及交易的隐蔽性，研究者和安全监管部门都尚无任何途径能够调查统计到地下产业链中 0day 安全漏洞数量规模与交易情况。然而如果被地下产业链利用的 0day 漏洞一旦被公开披露，而软件厂商还尚未来得及发布修补补丁，或刚发布补丁时，往往地下产业链中会抓住这一时间差，出现一个出售 0day 攻击代码工具的高峰期。本文作者曾在[Zhuge 2008a]中针对 2007 年十多个被地下产业链用于网站挂马攻击的安全漏洞进行调查分析，揭示出了地下产业链黑市对新发现漏洞的快速反应情况。

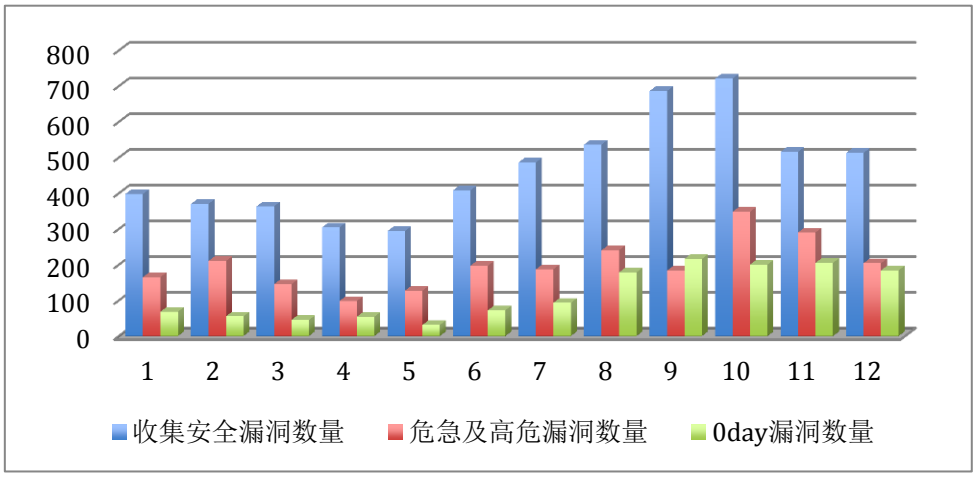


图 16 2011 年 CNNVD 收集安全漏洞月度统计

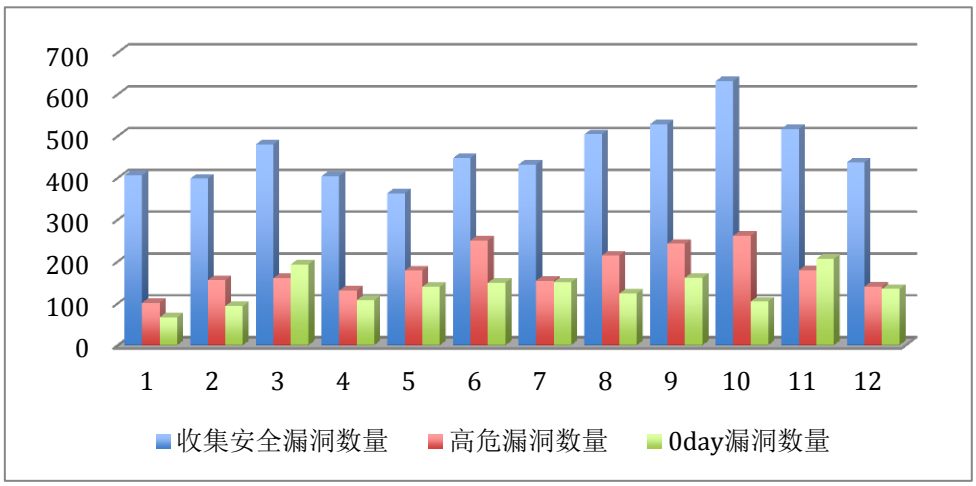


图 17 2011 年 CNVD 收集安全漏洞月度统计

- **恶意代码威胁数据统计分析**

恶意代码是中国信息安全地下产业链中较安全漏洞相比更为常见的交易商品，而由于地下产业链的驱动，以及与主流反病毒厂商的免杀技术博弈，中国互联网上出现的恶意代码样

本数量以惊人速度不断增长，也推动了真实资产盗窃、虚拟资产盗窃与互联网服务滥用等地下产业链的发展。

我们在**表 5** 中总结了安天[安天报告 2012]、金山[金山年报 2012]、奇虎 360[360 年报 2012]、瑞星[瑞星年报 2012]和腾讯 QQ 电脑管家[电脑管家年报 2012]对 2011 年恶意代码威胁的统计数据，由于各厂商均采用文件 MD5 指纹区分恶意程序，并统计不同指纹恶意程序数量作为截获木马病毒数量，随着目前多态与变形恶意程序的流行泛滥，这种计数方式不再能够反映出木马病毒真实家族与变种的流行情况，因此建议厂商能够改进恶意程序识别技术，将同一家族及变种的多态或变形恶意程序进行归并计数，以恶意程序家族数量及变种数量来反映出木马病毒疫情的真实发展情况。安天、奇虎 360 与瑞星统计数据均表明木马病毒截获量与截获次数较 2010 年有显著的增长，仅有金山的统计数据显示木马病毒截获量较 2010 年同比降低 31.5%。在恶意程序流行类型前三位，各厂商虽然分类标准都不尽相同，但均显示木马（尤其是盗号木马）占据了绝对主流的地位。

国家计算机网络应急技术处理协调中心（CNCERT/CC）[CNCERT/CC 月报 2011]也利用其 863-917 网络安全监测系统对网络病毒感染进行全网抽样监测[3]，2011 年全年捕获新增网络病毒 667 个家族 11,523 个不同变种，按月度累计监测到网络病毒感染终端 8,321 万台次，平均每月 693 万台，而其中飞客蠕虫占绝对多数，累计境内感染终端 7,230 万次，平均每月 602.5 万台。

表 5 国内个人安全厂商对 2011 年木马病毒威胁的统计数据

项目	安天	金山	奇虎 360	瑞星	腾讯 QQ 电脑管家
截获木马病毒数量	1153 万[1]	1230 万[1]	10.56 亿[1]	922 万[1]	3.81 亿（下半年）[1,2,4]
截获量较 2010 年同比增长	17%	-31.5%	87.7%[5]	22.9%	无数据
截获次数	无数据	18.25 亿[3]	236.1 亿	11.7 亿	无数据
截获次数较 2010 年同比增长	无数据	无数据	34%[5]	66.4%	无数据
木马病毒类型前三	木马、后门、蠕虫	无数据	广告木马、盗号木马、恶意插件	木马、感染性病毒、后门	盗号木马、病毒、推广木马
1. 按文件 MD5 指纹区分统计 2. 按月度累加 3. 按日均数据推算 4. 参照腾讯 QQ 电脑管家联合艾瑞咨询发布的《2011 下半年个人网络安全报告》，未有全年数据。 5. 参照奇虎 360 的发布《2010 上半年中国互联网安全报告》，未有全年数据，平均至全年计算。					

3.2.5 地下产业链整体规模估计

综合以上对四大信息安全地下产业链的实证数据分析，我们对中国信息安全地下产业链 2011 年整体经济规模做出如**表 6** 中所示的不完全估计。

真实资产盗窃地下产业链威胁网民人群规模为 3880 万，网银账户盗窃与盗刷盈利链条

[3] 网络病毒是特指有网络通信行为的恶意代码，CNCERT/CC 抽样监测 200-300 多种木马、僵尸程序与网络蠕虫。

对约 6 万受害者造成资金损失，保守估计规模为 4.2 亿元；第三方支付账户盗窃与盗刷盈利链条则危害 48 万人，保守估计规模达 16.5 亿元。虚拟资产盗窃地下产业链主要针对网络游戏行业实施，威胁网游用户人群达 3840 万，其中 384 万遭受损失，该产业链保守估计规模为 14.2 亿元。

资源与服务滥用地下产业链的盈利模式更加多样化，也更难以量化测算。本文仅以受控僵尸主机、感染恶意代码手机与被黑“网站”这三种最主要互联网资源进行分类统计与不完全估计。根据 CNCERT/CC 对木马与僵尸程序的监测数据[CNCERT/CC 年报 2011]，2011 年全年累计监测到 890 万台主机受控，以每台受控主机通过垃圾信息发送服务、点击广告欺诈、软件推广欺诈、拒绝服务勒索、各类刷客行为、窃取隐私信息等盈利模式为地下产业链获利 50 元计算，可为地下产业链贡献 4.45 亿元非法收入；根据金山[金山年报 2012]、奇虎 360[360 年报 2012]、网秦[网秦年报 2012]等国内主流手机安全厂商统计数据，2011 年全年累计监测到 4942 万部次手机感染恶意代码，而以每次感染手机通过恶意吸费、软件推广欺诈、垃圾信息发送、窃取隐私信息等各种盈利模式获利 20 元计算，可为地下产业链盈利大约9.9亿元;而根据知道创宇对国内互联网550多万个网站监测结果[知道创宇年报 2012]，共计监测到网站挂马 5.7 万站次，暗链攻击 205.9 万站次（注：按月度监测数量累计），以每次网站挂马平均可为攻击者牟取 500 元收入、每次暗链攻击平均牟取 200 元收入计算，对“被黑”网站资源的滥用可获利 4.4 亿元。

由上述保守估计，可测算得到 2011 年中国信息安全地下产业链整体盈利规模可达 53.6 亿元,即使在考虑安全厂商对网民提供了全方位保护的情况下,仍威胁超过 11,081 万网民，占总体 5.13 亿网民数量[CNNIC 2012]的 21.6%，威胁到 105 万个网站，占总监测网站数量 553.3 万[知道创宇年报 2012]的 19%。

表 6　2011 年中国信息安全地下产业链整体盈利规模不完全估计

产业链	盈利链条	威胁人群规模	遭受损失受害者	保守估计规模
真实资产盗窃	网银账户盗窃与盗刷	3880 万	6 万	4.2 亿
	支付账户盗窃与盗刷		48 万	16.5 亿
虚拟资产盗窃	网游虚拟资产盗窃	3840 万	384 万	14.2 亿
资源与服务滥用	僵尸主机资源滥用	890 万	890 万台次	4.45 亿
	感染手机资源滥用	2471 万[1]	4942 万部次	9.9 亿
	被“黑”网站资源滥用（挂马、暗链等）	105 万网站[1]	210 万站次	4.4 亿
总计		11,081 万网民 105 万网站		53.6 亿
1 安全报告中均仅提供月度消重数据，进行全年累加后重复率以 50%估算。				

再考虑到每个盈利链条的各个上游环节，以及这三大地下产业链对黑帽技术、工具与培训地下产业链的利益反馈，和“刷客”等尚无法估计规模的盈利链产值，中国信息安全地下产业链的整体经济总量或超百亿元，相当于百度、阿里巴巴集团等超大型互联网公司的全年营收规模。

3.3 地下产业链黑市实证分析

在本节中，我们通过监测目前国内互联网最主要的地下产业链黑市，即隐藏于百度贴吧与腾讯 QQ 社区中的一些专门用于地下产业链沟通交流的贴吧与 QQ 群，获取到对地下产业链的一手观测数据，通过实证数据分析来揭示出中国互联网信息安全地下产业链的规模、现状与发展趋势。

3.3.1 地下产业链黑市概况统计分析

百度贴吧作为国内互联网上最大的中文社区论坛，同时采用了基于关键字的论坛组织方式，并支持未经注册用户的匿名访问，地下产业链参与者可以使用业界行话创建出较为隐蔽的交流论坛，也可以非常便捷地发布信息与参与讨论。因此百度贴吧便成为国内信息安全地下产业链黑市的主要聚集地之一。

我们在对国内信息安全地下产业链内部行话进行深入理解与破译基础上，通过搜索了 84 个行话关键字，共计监测到 129 个开放的地下产业链黑市贴吧，具体分布情况如**表 7** 所示。同时在搜索这些行话关键字时，我们也发现百度贴吧已经对 26 个已被安全社区熟知的行话关键字对应的贴吧进行了封禁处理，包括“身份”、“证件”、“洗钱”、“盗号”、“肉鸡”、“木马”、“免杀”、“黑客”等等。这说明百度已经根据一些社区或国家监管部门的反馈，对地下产业链黑市采取了应对措施，但我们的监测数据也表明这种应对措施还不足以触动地下黑市的正常运转。由于百度贴吧保存所有发帖的历史记录并支持匿名浏览，因此我们采用互联网爬虫，对所监测的地下产业链黑市贴吧进行持续的帖子爬取，并编写程序抽取网页中的帖子内容，插入至地下黑市监测数据库中。

百度贴吧中的帖子分为主题帖与回帖两类，主题帖是发起一次讨论会话线程(Thread)的第一个帖子，在贴吧中被记为“第 1 楼”，主题帖发帖人被称为“楼主”，回帖则依据其回复主题帖的先后次序标记“第 n 楼”。如果发帖人注册了百度贴吧会员，发帖人则显示会员昵称，而未经注册的匿名用户发帖时，百度贴吧将记录并在帖子中显示发帖人所在的 C 类 IP 网段。对于每个帖子，我们记录包括发帖时间、标题、内容、发帖人昵称、会员 ID（注册会员）、发帖人上网 IP（匿名用户）、主题帖 ID、楼数等信息项。截止 2012 年 3 月 15 日，我们共计监测到的主题帖数量为 31,8815，总帖子数为 110 多万条。经过对标题与内容均重复的帖子进行消重之后，我们选择 2004 年至 2011 年这 8 年间的 753,806 个帖子作为本文对百度贴吧地下黑市的监测分析数据集。

表 7 百度贴吧中的地下产业链黑市监测数据概况

产业链	搜索关键字	开放贴吧	封禁贴吧	监测主题	比例
真实资产盗窃	21	20	8	28,378	8.90%
网络虚拟资产盗窃	12	40	4	101,269	31.76%
互联网资源与服务滥用 [1]	37	33	11	113,049	35.46%
黑帽技术、工具与培训	14	36	3	76,119	23.88%
总计	84	129	26	318,815	100%
1 “刷客”相关贴吧超过 20 个，主题帖累计超过 100 万，未加入实际监测					

腾讯 QQ 是中国互联网上占据绝对优势地位的即时通信软件，提供的 QQ 群功能支持多人同时在线聊天，发起群主也可以自由控制人员加入和踢出，因而成为了国内地下产业链用来

在线沟通交流最为主要的途径。我们从2012年2月份开始陆续搜索采集地下黑市QQ群列表，并使用多个申请到的QQ号加入到这些QQ群中，进行地下黑市信息的潜伏监听。截止5月份，我们同样采用84个行话关键字，使用腾讯QQ软件中的QQ群搜索功能，共计搜索到描述存在关键字的QQ群82,121个，由于大多数QQ群人数偏少，且腾讯QQ限制每次搜索最多返回300个QQ群，通过人工确认与信息安全地下产业链相关且满足人数限制条件的的地下黑市QQ群共计2,738个。腾讯QQ作为闭源软件，没有提供自动化查询与加入QQ群的接口，同时又对同一QQ号与IP地址每日加入QQ群的数量与频率进行严格限制，由于时间与精力关系，我们仅选择人数规模较大且覆盖面较广的采样监测QQ群集合，通过使用所掌握的行话伪装为地下黑市参与者，成功申请加入了130个地下黑市QQ群。

在加入QQ群后，我们对其中发送的消息进行持续监测和记录，并编写程序将消息记录解析插入到数据库中，同时我们采用了一种对QQ群消息进行会话重组的简单策略，在同一QQ群中的消息间隔在五分钟之内我们视为同一会话，而间隔超过五分钟之后则将发布的消息作为新的会话主题消息。每条QQ群消息记录包括消息发送时间、消息内容、发送者昵称、发送者QQ号、主题消息ID、楼数等信息项。

我们选取2012年3月至5月期间这130个地下黑市QQ群消息作为本文监测分析数据集，包括76,516条消息，23,720个会话，地下黑市QQ群的具体分布情况如**表 8**。

表 8　QQ群地下产业链黑市监测数据概况

产业链	关键字数	发现QQ群	符合条件QQ群	监测QQ群
真实资产盗窃	21	142	128	24
网络虚拟资产盗窃	12	9050	576	12
互联网资源与服务滥用	37	70104[1]	1779	42
黑帽技术、工具与培训	14	2825	562	52
总计	84	82121[2]	2738[3]	130[3]

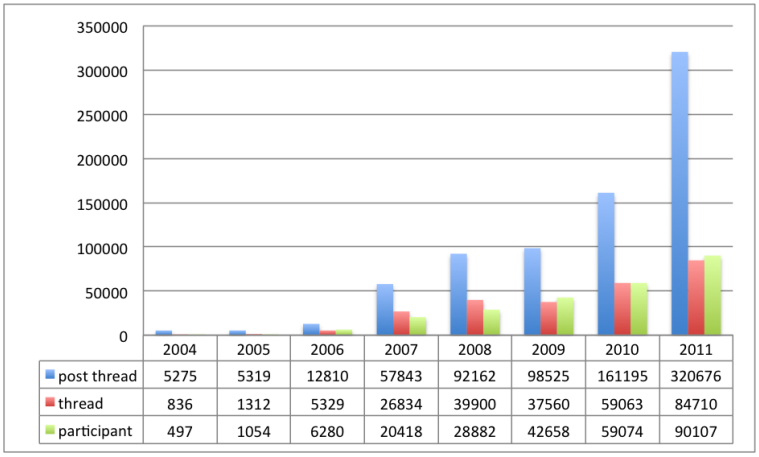
1 其中“刷客”相关QQ群超64,106个，未加入实际监测

2 未经过消重处理

3 经过消重处理

3.3.2　地下黑市行为统计分析

在2004至2011年周期中，我们在百度贴吧地下黑市中共计监测到753,805条帖子，分属于255,544个主题帖会话，每个主题帖会话平均拥有近3条不重复帖子，而参与这些地下黑市贴吧的发帖人有248,970。图 18给出了每年度发帖数、主帖数与参与者数的统计情况，可以作为一个侧面反映出国内信息安全地下产业链的发展过程与趋势，2004年至2005年尚处于发展萌芽状态，参与人数与帖子数量的规模还较小，在2006年至2008年则进入一个飞速膨胀与发展阶段，地下黑市发帖数平均年增长达到184%，2007年猛增352%，在2008年达到一个阶段性高峰。2009 年由于中国出台针对网络犯罪打击的刑法修正案，并通过若干个大案处置对地下产业链形成了一定的威慑效果，因而2009年较2008年的增长并不明显，在主帖数上甚至有所降低。而从2010年至2011年，由于执法部门对网络犯罪与一些不当行为监管打击措施不够到位，地下产业链又开始呈现出快速发展的趋势。2011 年参与百度贴吧地下黑市的人数达到9万多人，发帖数则超过32万，较2010年几乎翻番，达到监测期间内的峰值。如果不采取有效应对措施，预计中国互联网地下产业链仍将保持快速增长趋势。



	2004	2005	2006	2007	2008	2009	2010	2011
post thread	5275	5319	12810	57843	92162	98525	161195	320676
thread	836	1312	5329	26834	39900	37560	59063	84710
participant	497	1054	6280	20418	28882	42658	59074	90107

图 18 百度贴吧地下黑市帖子、主题帖与参与者年度统计数据

监测周期中每个月份的帖子数与主题帖数统计情况如图 19 所示，我们可以从中发现明显的年度周期：其中 1 月份和 2 月份受到中国春节假期等因素影响，是全年的谷底，而 6 月至 8 月份是全年高峰期，部分原因是这一期间庞大的学生群体放暑假，推动网络游戏、网络购物等互联网行业处于活跃期，也会对地下产业链形成需求刺激。

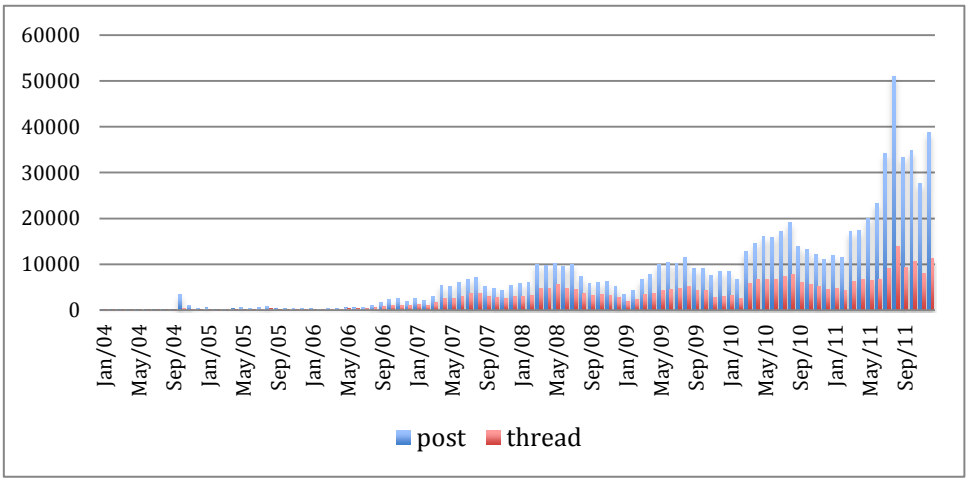


图 19 百度贴吧中地下黑市的帖子与主题数量趋势图

对于地下黑市 QQ 群，我们于 2012 年 3 月份在 130 个 QQ 群中共计监测到 76,516 条消息，分属于 23,720 个不同的会话，监测到使用了 7,996 个不同 QQ 号的参与者。

图 20 显示了每日在地下黑市 QQ 群中监测到的 QQ 消息数、会话数与 QQ 号码数的统计情况，QQ 消息数的峰值达到 5,000，而 QQ 会话数与 QQ 号码数的峰值均在 800 左右（3 月 16 日与 30 日，均为周末）。

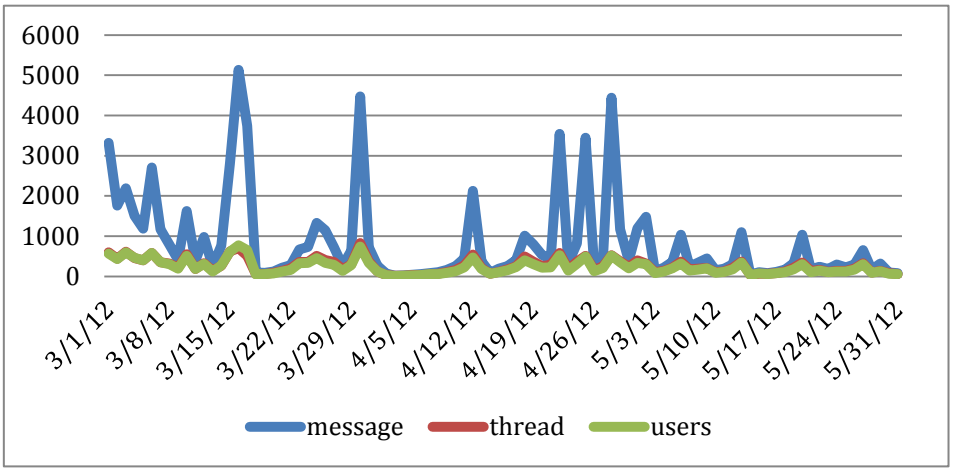


图 20 地下黑市 QQ 群监测数据统计情况

3.3.3 地下黑市参与者分析

- **参与者规模与趋势分析**

如图 21 所示，百度贴吧地下黑市的参与者数量趋势也呈现出同样的年度周期，参与者数量一直呈现增长趋势，平均年增长率为 144.74%，其中 2006 年暴增 495%，即使在主题贴数减少的 2009 年，参与者数量仍快速增长了 47.7%。这反映出地下产业链参与者具有较强的黏着性，在尝到获取高额不法利益的诱使下，将长期参与地下产业链，而执法部门短期运动式的严打行动只会让网络犯罪者暂避风头，但仍通过地下黑市保持沟通联络，在执法部门放松监管与打击力度时重新活跃作案。从图 21 中，我们还可以发现百度贴吧地下黑市的参与者类型构成发生了有趣的变化，在 2010 年之前，采用未经注册用户发帖的匿名参与者比例远大于注册用户，2009 年匿名参与者数量是注册会员参与者数量的 2.59 倍，而 2010 之后，匿名参与者数量急剧下降，而注册会员参与者数量则显著增长，至 2011 年匿名参与者仅有注册会员参与者的 16%。在经过向百度公司的了解之后，确定发生这一变化的原因是百度贴吧在 2009 年底加强了发帖审核机制，只允许用户注册才能进行发帖（仍可以选择匿名发帖）。

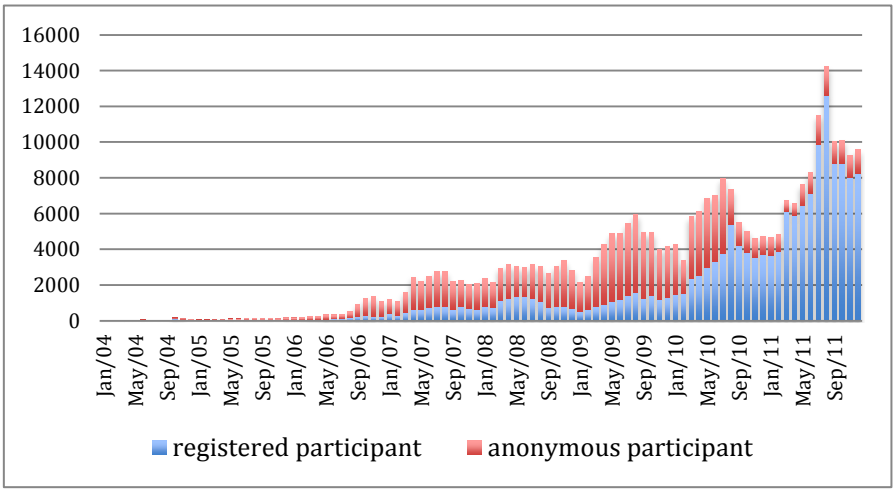


图 21 百度贴吧中地下产业链黑市参与者趋势统计图

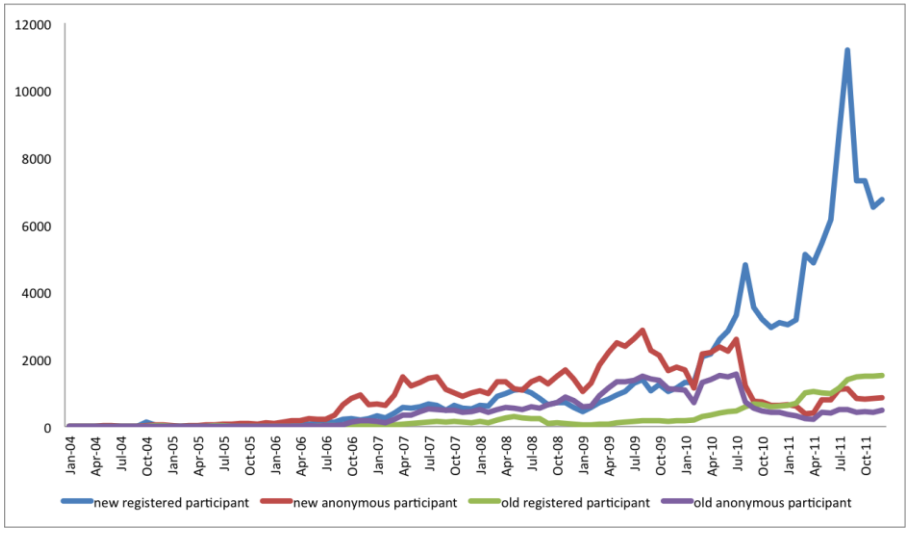


图 22 百度贴吧地下黑市中每月新出现参与者与老参与者数量统计图

通过对每位参与者在地下产业链黑市中的最早出现时间进行分析，我们将在本月出现的参与者标记为“新人”，而在之前月份已出现过的参与者标记为“熟客”，从而给出每月地下黑市“新人”与“熟客”的数量统计情况，如图 22 所示，可以发现地下黑市仍以“新人”居多，尤其是注册会员“新人”，在 2010 年至 2011 年呈现“井喷”式增长势头，这也反映了中国地下产业链仍处于快速发展的阶段，由于前面提到的原因，在 2009 年之后，匿名登录用户无论在“新人”还是“熟客”均快速缩减，而注册用户“熟客”在 2010 年之后处于稳步快速增长趋势，2011 年累计达到 13,857 人，构成了地下产业链黑市中坚力量。

- **参与者联系方式**

在地下黑市，参与者非常普遍地使用腾讯 QQ 号作为联系方式，在帖子标题、内容或发布者昵称中包含 QQ 号，要求广告信息关注者通过 QQ 与其联系。由于 QQ 号并非实名注册，同时在地下产业链中盗窃与销售 QQ 号的行为也非常普遍，因此 QQ 为地下产业链参与者提供了最便捷和隐蔽的在线通讯方式。我们通过在程序中使用正则表达式，匹配 5 位至 11 位数字并通过特定格式与手机号段排除掉手机号码，同时支持匹配中文大写数字，对地下黑市帖子中的 QQ 号进行匹配识别。结果在 753,806 条帖子监测数据集匹配到包含 QQ 号的帖子 420,230 条，占 55.8%；而主题帖中包含 QQ 号的有 138,660，占 56.7%，略高于平均数值；共计监测到 151,903 个参与者共计发布了 144,964 个不同 QQ 号，占总参与者人数的 67.6%。这一统计数据验证了地下黑市普遍采用腾讯 QQ 作为进一步黑市交易联系方式的主要途径。

- **参与者地理分布情况**

根据百度贴吧地下黑市中未经注册匿名用户的 C 类 IP 网段信息，我们采用纯真库查询获得该网段的所属省份、城市与具体地址信息，并进行参与者地理分布的统计。虽然存在部分参与者使用代理隐藏真实上网 IP，以及 IP 地址定位信息不准确等因素，但在目前中国执法部门尚未对地下黑市进行严密监管与打击的情况下，真正在参与地下黑市信息发布与交流时候使用代理机制隐藏 IP 的参与者比例还较少（躲避国内执法部门追查通常会使用国外代理，而我们仅监测到 2.79%匿名参与者使用境外 IP），因此基于参与者发文 IP 地址定位进行参与者地理分布情况统计，能够反映出地下产业链参与者在中国的大致分布情况，还是具有较高的参考价值。

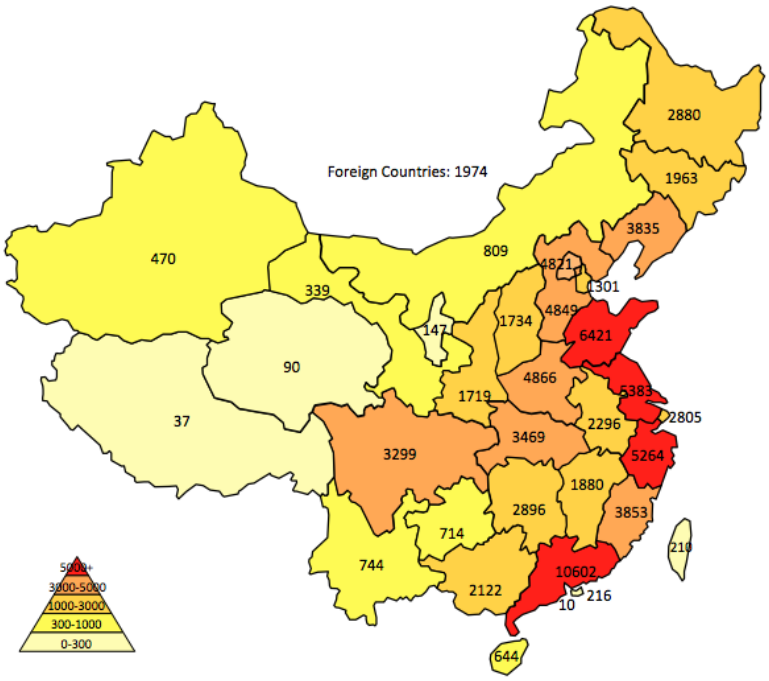


图 23 百度贴吧地下黑市匿名参与者的省份分布情况（注：不反映真实中国版图情况）

图 23 显示了百度贴吧地下黑市中 86,337 个不同 C 类 IP 网段的所在省份分布情况，排名前十位的包括广东、山东、江苏、浙江、河南、河北、北京、福建、辽宁和湖北，大多数为互联网经济发达的沿海省份与重点城市，也包括了人口众多的一些经济较不发达省份。中国大陆境外（包括外国、台湾地区、香港特区与澳门特区）的参与者 IP 网段数量有 2,410 个，占比 2.79%，大部分为地下黑市参与者使用境外代理方式躲避执法部门追查，在地下黑市中也发现少量自称位于境外，可以有恃无恐进行网络犯罪的参与者。

- **参与者行为分析**

对百度贴吧和 QQ 群地下黑市中的参与者，我们还进一步根据参与者昵称、匿名参与者上网 IP 网段、QQ 号等标识信息进行聚类统计，获得每位参与者在地下黑市中的最早出现时间、最近出现时间、活跃时间长度、发帖数、参与会话数量以及参与贴吧/QQ 群数量等行为特征，然后通过对不同类型地下黑市、不同类型参与者的行为特征分析，尝试揭示出地下产业链中的一些内在规律。

不同类型参与者在地下黑市中的活跃时间长度的累计分布函数（CDF）曲线如图 24(a)所示，可以看到：百度贴吧地下黑市参与者中超过 50%的活跃时间长度少于 0.01 小时，50.8%的参与者仅仅发布了一条信息。百度贴吧所有参与者中有 80%的活跃时间长度小于 100 小时，而近 15%的参与者拥有超过 1000 小时（41.7 天）的活跃时间，这些用户通过长期活动积累起一些交易关系与信誉，构成了地下黑市的骨干力量。百度贴吧地下黑市的注册会员参与者与匿名参与者的活跃时间分布也存在着较为显著的差异，近 30%的匿名参与者 IP 网段活跃时间超过 1000 小时，而只有 10%的的注册用户参与者活跃时间超过 1000 小时，其中原因可能是匿名参与者无法变更其上网 IP 地址网段，而注册用户参与者为了躲避追查和关注，在一段时间后会选择变更会员昵称。而在 QQ 群一个月监测记录中，近 40%参与者活跃时间长度少于 0.01 小时，CDF 曲线在 12 小时左右位置出现一个明显的折点，在折点之前参与者百分比较百度贴吧均少 10-15%左右，这也体现出了即时通信软件较 Web 论坛对于提升地下黑市参与者交流活跃度与便捷度的优势，而 12 小时折点之后的 CDF 曲线迅速攀升，这与我们

对 QQ 群仅监测三个月时间（2208 小时）有关。

地下黑市参与者活动的贴吧、QQ 群数量分布情况则如图 24(b)，超过 85%的百度贴吧地下黑市参与者仅出现在一个贴吧中，最活跃参与者则在 34 个贴吧均发布过消息。而对于匿名参与者的 IP 网段，则有 25%以上曾出现在两个以上的贴吧中，其中原因可能包括在同一上网网段可能存在多个匿名参与者，以及地下黑市参与者往往通过注册多个会员账户，或频繁变更昵称，以达到更好的隐蔽性。90%的 QQ 黑市参与者仅出现在一个受监测的 QQ 群中，这可能与我们目前 QQ 群地下黑市监测面较窄相关。

地下黑市参与者的消息发布数量、参与会话数量分布 CDF 分别如图 24(c)与图 24(d)所示，可以看到 QQ 群中的地下黑市参与者发布消息更加活跃，在消息数量小于 16 左右的临界点之前，参与者百分比较百度贴吧均少 10%左右，再次体现出了即时通讯协议对提升地下黑市活跃度的支持作用。而在参与会话数量分布特征方面，QQ 群参与者则和百度贴吧参与者没有明显区别，大致 50%左右的参与者仅参与了一次会话，而 90%以上参与者的会话数均小于 8，这也说明地下黑市主要用于发布广告消息，而承担沟通交流的任务很少，后期的交易洽谈等任务则一般通过 QQ 私聊方式隐蔽进行。

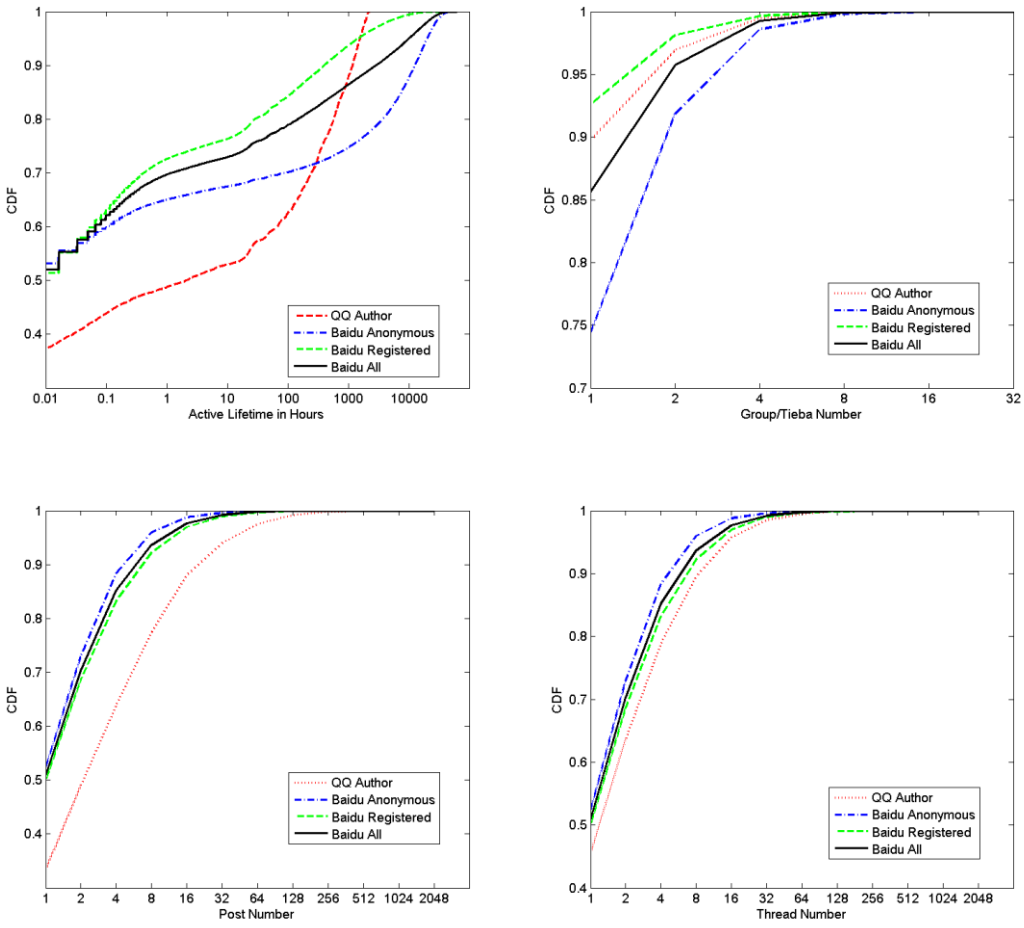


图 24 (a)地下黑市参与者活跃时间分布 CDF 图 (b)地下黑市参与者活动贴吧/QQ 群分布 CDF 图 (c)地下黑市参与者发消息数分布 CDF 图 (d)地下黑市参与者参与会话数分布 CDF 图

3.3.4 地下黑市业务分析

- **地下黑市商品与买卖行为分布情况**

对于百度贴吧地下黑市监测数据集，我们考虑到中文语言切词与语义理解的难度，并注意到地下黑市广告信息中通常使用行话关键字，而且每条广告信息中还会出现多种商品情况，因此并未使用机器学习方法对广告涉及的商品类型与买卖行为类别进行分类，而是利用整理的行话关键字与中文语言习惯人工编写出一些添加标签的 SQL 语句，对地下黑市的广告信息进行商品类型与买卖行为的标记分类。对于一些使用不太独特容易错误关联匹配的行话特殊关键字，如“料”（银行卡资料），我们在匹配关键字时引入排除词（如“料想”、“爆料”等），排除掉无关词的错误匹配与标记，并引入包含词（如“内料”、“外料”等）进一步补充标记，达到对信息的精确标识。对买卖行为的关键字我们也同样引入关键字、排除词与包含词来达到精确标识。

经过对广告信息的商品类型与买卖行为类别进行标识后，共计 369,476 条地下黑市信息被标记了商品类型，出售广告信息数量为 265,980 条次，购买广告信息数量为 118,710 条次，出售与购买广告数量比将近 2:1，其中网络虚拟资产盗窃地下产业链则达到 4:1。真实资产盗窃由于直接违反国家法律，风险度很高，因此广告量较其他三大产业链少一个数量级。

表 9 地下黑市中四大产业链买卖广告信息统计数据

产业链	百度贴吧出售广告信息数	百度贴吧购买广告信息数	百度贴吧供求比例	QQ 群出售广告信息数	QQ 群购买广告信息数	QQ 群供求比例
真实资产盗窃	31,980	17,270	1.85	1,481	86	17.22
网络虚拟资产盗窃	121,191	29,105	4.16	2,,087	128	16.3
互联网资源与服务滥用	119,233	70,872	1.68	5,417	328	16.52
黑帽技术、工具与培训	61,183	44,781	1.37	3,898	217	17.96
未消重总计	333,587	162,028	2.06	12,883	759	16.97
消重后总计	265,980	118,710	2.24	10,816	608	17.79

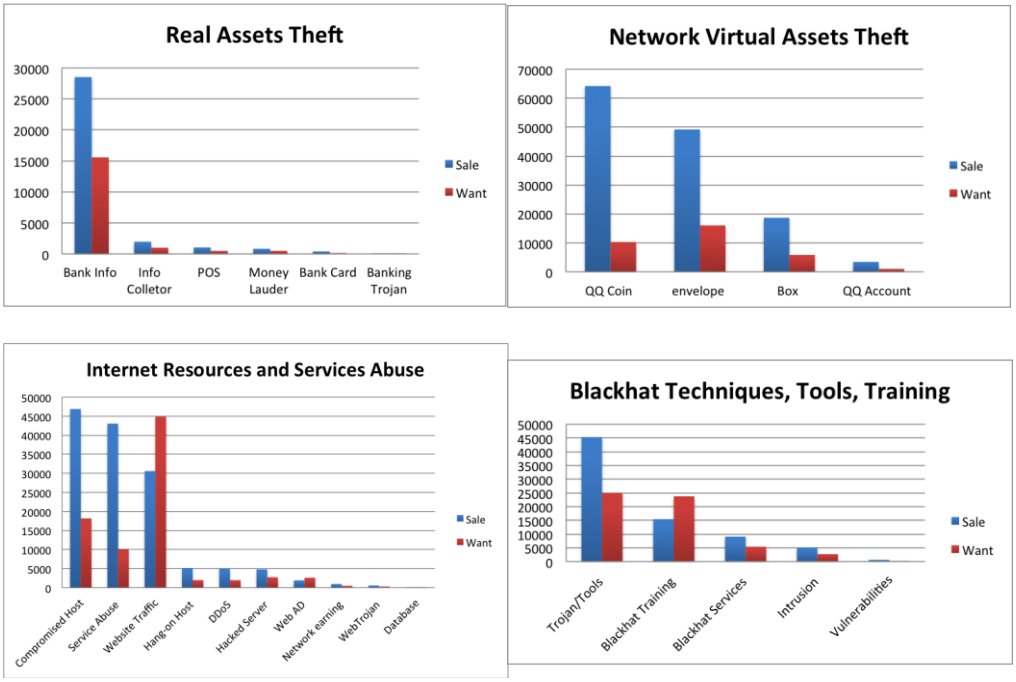


图 25 百度贴吧地下黑市中的商品与服务业务分布图

对于百度贴吧，真实资产盗窃、网络虚拟资产盗窃、互联网资源与服务滥用、黑帽技术工具与培训四大地下产业链的黑市广告信息中主要商品买卖情况如图 25 所示。在真实资产盗窃地下黑市中，最主流的商品是银行卡资料，其次为采集器、POS 机盗刷服务等。网络虚拟资产盗窃地下黑市中，流行商品为 Q 币、“信封”与“箱子”，出售与购买广告数量比均达到了 3 倍以上。而在互联网资源与服务滥用地下黑市中，流行商品分别为受控“肉鸡”，服务滥用业务和网站流量。其中网站流量的购买广告数量超过了出售广告数量达 47%左右，表明地下黑市对这类资源出现了供不应求的现象。黑帽技术工具与培训地下黑市中的主流商品为木马与攻击工具、远程控制软件和黑帽技术培训，其中黑帽技术培训的购买（即“拜师”）广告数量超过了出售（即“收徒”）广告达 54%左右；“拜师”帖的发帖人有 11,439，帖子数量有 23,748 之多，说明大量新人希望学习和掌握黑帽技术，进入到地下产业链当中，这再次表明中国信息安全地下产业链如果不进行有效治理，将继续保持快速增长和泛滥的势头。

- **参与者角色分析**

根据地下黑市参与者发布的广告帖商品标记类型与买卖行为类别，我们可以进一步识别出他们在地下产业链中所承担的角色，并进行分布情况统计分析，从而反映出地下产业链的人员构成情况。

我们监测到发布至少一个广告贴的参与者人数达到 129,968。这些黑市参与者主要角色构成情况见表 15，四大产业链中的参与者比例分别为 16.5%，45.5%，51.6%和 30.5%，注意参与者的活动普遍涉及到多个产业链，因此比例之和会超过 100%。地下经济中参与人数最多的角色为“洗信人”，数量达到 29,916，这个角色基本不需要掌握任何的黑帽技术，于是地下经济中的大量新手会选择这个角色作为他们的起点。

表 10　百度贴吧地下黑市参与者主要角色构成情况

产业链	人数	所占比例	参与者角色	人数	所占比例
真实资产盗窃	21,460	16.5%	料主	14,524	11.1%
			洗料人	8,345	6.4%
网络虚拟资产盗窃	58,963	45.5%	包马人	20,486	15.8%
			洗信人	29,916	23%
互联网资源与服务滥用	67,003	51.6%	“抓鸡人”	16,078	12.4%
			“黑站人”	14,259	11%
黑帽技术、工具与培训	39,605	30.5%	木马作者与木马代理	18,945	14.6%
			0day 漏洞商人	421	0.3%
			黑帽技术培训师	8,140	6.3%
			黑帽技术求学者	11,439	8.8%
	注：可能某一广告信息匹配多个商品，因此计数存在重复。				

- **地下黑市商品价格分析**

在对地下黑市中流行商品进行标定识别之后，我们进一步对产业链中最为重要的五类商品——银行卡资料、信封、肉鸡、网站流量与木马病毒进行价格提取与统计分析。虽然在地下黑市中，大部分广告帖中均没有标明商品定价，但也存在着一小部分帖子中给出了报价。我们采用一些通用的中文句式与价格表达形式，从标记好的广告帖中提取价格信息，根据买卖行为类别分为出售价格与收购价格，并分别计算月度平均价格。由于银行卡资料的特殊性，地下黑市中往往不是采用定价出售的方式，而是采用在窃取存款后进行分成的方式，因此在

少量关于银行卡资料的广告帖中，会给出诸如“55 分账”、“你 6 我 4”此类的分成比例。而其他四类地下黑市流行商品的价格情况如图 26 所示：信封普遍的出售价和收购价均在 1 元-3 元之间，同时在某些月份也不乏有低价倾销的情况发生；网站流量作为一种供不应求的攻击“生产资料”，包含明确收购价的广告信息很多，最高达到 330 元/万 IP 访问，同时而求购价往往高于同期销售价，以获得更多关注度；受控主机（“肉鸡”）价格则根据不同类型肉鸡有所差异，但一般售价都在 0.1 元至 0.5 元之间，这种低廉的价格也说明中国互联网地下产业链掌握着大量的受控计算机资源；木马程序广告以出售为主，价格一般在 100 元至 1000 元之间，而求购广告则往往获取到一些特殊目的的木马或病毒程序，给出的价格一般较高，在我们的监测中，发现的最高求购价为 2,000 元。

对地下黑市主要产业链商品的价格跟踪分析将有助于安全社区分析安全威胁的攻击成本代价，如我们可以通过“肉鸡”价格监控，计算出购买 1,000 个“肉鸡”构成具有一定规模的僵尸网络实施拒绝服务攻击的成本仅需 100-500 元，这为如何部署针对性的安全防范措施提供了参考信息。

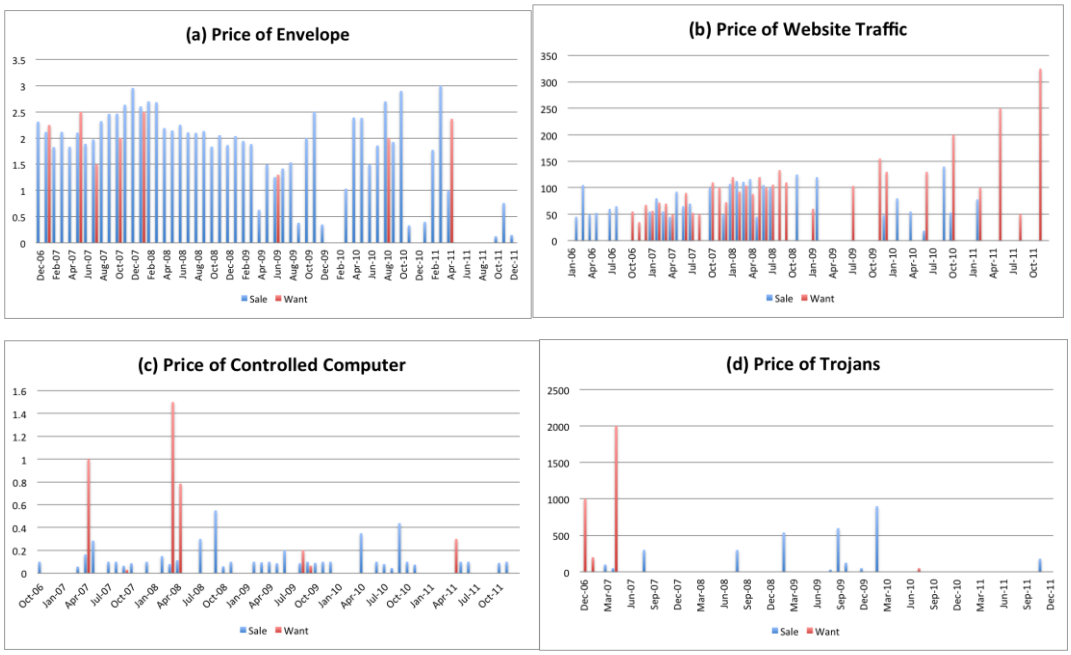


图 26 地下黑市中流行商品的出售与求购价格情况分析

3.3.5 地下黑市中的欺诈行为分析

地下黑市中的主要信息除了广告之外，还存在着大量对其他参与者欺骗行为的举报帖，相当部分的广告帖中也包含了对欺骗行为的警示，这说明地下黑市作为网络犯罪者与不法分子的在线交流市场，充斥着很多不诚信交易与欺诈行为。图 27 显示了一个典型的骗子举报帖，在主题帖中昵称为“大路对长空 999”参与者列出了一位卖家的几个昵称与 QQ 号，宣称被骗了 600 元，并揭露了对方的手机号码、支付宝账号与银行账号信息；而在九天之后的回帖中，一位昵称为“dumps88”的参与者回复辩驳，并宣称对方才是骗子；几天后一位匿名参与者则发帖调侃称“两个都是骗子对咬”。这一典型举报骗子说明地下黑市中确实存在不诚信交易和欺诈行为，而参与者对自身信誉还是比较看重的，在遇到举报时往往通过地下黑市中的辩解与反驳，尝试减轻举报帖对自身信誉的影响，而其他参与者也都在关注这些举报帖，可能在地下黑市交易时往往更慎重地对待未建立信任关系并曾被举报的对象。同时他

们在发布黑市广告时，也时常包含对欺骗行为的警示，如警告“骗子绕道”等。

图 27 一个百度贴吧地下黑市举报骗子的典型帖子

通过对欺骗行为举报与警示的表达模式分析，我们编写了 SQL 语句从地下黑市信息中标记出欺骗举报信息与欺骗警示信息，共计发现 9,651 位参与者发布了欺骗行为举报帖 15,980 条，占所有信息的 2.1%，举报欺骗行为参与者所占比例为 3.9%，即大概 25 位参与者中便有 1 位曾经在地下黑市中遭遇严重欺骗行为并选择了举报。而包含欺骗警示信息的广告帖数量为 27,496 条，占广告帖数量的 7.4%。

上述数据均验证了地下黑市混乱与噪杂的特性，但地下黑市参与者们仍然能够利用后续的 QQ 私聊、担保支付等通讯与交易工具，正常地达成地下产业链中的交易，维持地下产业链的运转。由于后续 QQ 私聊与交易支付过程的隐私性，我们无法进一步深入监测地下产业链的后续环节。

3.4 网络犯罪案件公开信息与地下黑市信息关联实证分析

为了验证地下黑市信息与由地下产业链驱动网络犯罪案件的关联关系，我们进一步选择了前面在四大地下产业链分析中所列举的 4 个典型案件，并通过查阅这些案件的法庭审判卷宗和媒体报道，从中抽取出犯罪人的网名昵称、QQ 号、案件涉及恶意代码与攻击工具名称等具有独特性的关键信息，然后在监测到的百度贴吧地下黑市历史记录库中搜索包含有这些关键信息的帖子记录，并分别获取在案件曝光之前关键信息的最早出现时间、最后出现时间、帖子条数和帖子中的案件追踪线索。

关联分析结果如**表 11** 所示，对于所有 4 个案件，在案件公开曝光之前，我们均能够从地下黑市中搜索到包含有案件关键信息的帖子内容，如 2008 年 4 月 14 日媒体曝光的顶狐案，主要犯罪人网名“Topfox”在百度贴吧地下黑市中可搜索到 98 个帖子，其中最早出现时间为 2005 年 7 月份，而犯罪人之前编写过的恶意代码“顶狐下载者”、“密码解霸”（别称“密码结巴”）、“狐狸王病毒”均在地下黑市中搜索到相关帖子，而最早出现时间可追溯至 2004 年 1 月份，这说明犯罪人在案发被捕之前已经参与地下产业链至少 4 年以上，而对这些相关帖子的细致分析可追踪到犯罪人或同伙销售恶意代码的发布 IP、发布 QQ、支付银行账号等线索，这些线索可以有助于协助执法部门定位并追查犯罪人。而熊猫烧香案、剑客 DDoS 勒索案、温柔木马案也均可以利用案件中的关键信息从地下黑市信息中搜索到相关记录，而最早时间均较案件曝光时间有半年至两年多的提前量，同时地下黑市相关记录均能够为案件追查提供各种类型的线索。

表 11 典型网络犯罪案件与地下黑市信息关联分析表

案件	曝光时间	关键信息	帖子条数	最早出现时间	曝光前最后时间	线索
顶狐案	2008-4-14	Topfox	98	2005-7-8	2008-2-26	
		顶狐下载者	3	2006-11-11	2007-8-15	发布 IP
		密码结巴	290	2004-1-12	2008-4-1	发布 QQ
		密码解霸	346	2004-2-26	2008-4-1	银行账号
		狐狸王病毒	6	2005-6-30	2007-7-5	
熊猫烧香案	2007-2-12	689565	1	2007-1-23	2007-1-23	
		www.krvkr.com	155	2007-1-14	2007-2-10	注册信息
		武汉男生 2005	42	2004-12-22	2007-2-10	个人网站 发布 IP
剑客 DDoS 勒索案	2009-11-27	剑客压力测试	6	2008-12-29	2009-9-24	网站 发布 IP
温柔木马案	2008-8-6	温柔马	128	2008-1-26	2008-8-3	QQ 号

根据上述对 4 个典型网络犯罪案件与地下黑市信息的关联分析结果，我们可以得出监测地下黑市信息能够支持更早地对一些可能发生的网络犯罪案件进行早期监控与预防这一结论。

而对正在发生的网络犯罪事件，地下黑市监测信息中的线索也能够为案件侦查提供帮助。我们也已经基于这段时间对地下黑市的监测信息，跟踪到若干个仍活跃的网络犯罪团队线索，并已经为相关执法部门提供调查线索。

因此，对于网络犯罪事件应急响应组织和执法部门而言，持续跟踪监测地下产业链黑市具有非常重要的实际意义。

4. 相关工作

驱动互联网犯罪的信息安全地下产业链是一个全球性问题。西方经济发达国家的信用卡网络支付、网络购物消费等应用在互联网上较中国发展地更早，因此也更早出现了包括信用卡盗用欺诈、个人信息泄露、互联网资源滥用等盈利模式的信息安全地下产业链。Cymru 的 Rob Thomas 等人[Thomas 2006]较早地揭露出以 IRC 聊天协议网络构建的金融欺诈地下黑市，并通过监测到的大量黑市广告与交流信息案例分析，曝光了地下产业链中的各种交易行为及其危害，但并未系统性地对地下产业链与地下黑市进行结构分析与数据统计。Jason Franklin 等人[Franklin 2007]首次对地下产业链进行监测与实证数据分析，通过对一个活跃 IRC 地下黑市 7 个月的数据收集与归类分析，对地下黑市行为规律、参与者特征、交易商品与服务等进行了细致调查，给出了丰富的数据统计结果，为安全社区对地下产业链驱动的网络安全威胁有了更加深入的认识。本文借鉴了相关方法对地下黑市信息进行实证数据分析，但监测的中国互联网地下黑市的形态与内容均具有独特性，借助于 Web 论坛较 IRC 协议能够保留历史记录的优势，我们得以监测到中国互联网上长达 8 年的地下黑市信息，因而能够对地下产业链的演变情况与发展趋势做出更加全面的分析，此外，本文除了对地下黑市信息进行监测之外，还综合利用了公开渠道发布的 2011 年安全报告、威胁统计数据与网络犯罪案件卷宗，估算了地下产业链的整体盈利规模与危害人群范围，同时也通过典型网络犯罪案件中关键信息与地下黑市监测信息之间的关联分析，证实了监测地下黑市信息对打击网络犯罪的支持作用。

Holt 等人[Holt 2007]对用于盗窃个人信息交易的 6 个 Web 论坛中的 300 个讨论线程进行了定量分析，给出了地下黑市出售商品的类型与分布情况，并对其价格进行了统计分析，进一步分析了黑市参与者及其相关之间的关系，本文选择了被盗银行资料、网游账号密码、受控主机、网站流量与木马这五类分属于不同产业链的地下黑市流行商品，从中国互联网地下黑市长达 8 年的监测数据中进行商品广告价格与供求关系的案例分析，揭示出这些地下黑市商品的价格是随着供求关系而变化，同时与参与者数量密切相关。Cormac Herley 等人[Herley 2010]则认为 IRC 地下黑市是地下产业链的底层市场，里面充斥着很多欺骗性的广告，而对那些并不具备技术能力的产业链新手进行欺骗，从而导致 IRC 黑市的规模估计被夸大。我们在对中国互联网地下黑市的监测过程中也同样发现了地下黑市存在大量举报欺骗性广告和参与者的信息，同时在相当比例的广告信息中均包含对欺骗者的警示，“鱼目混杂”是地下黑市的一个本质特性，但这并不妨碍这些地下黑市成为地下产业链的联系纽带。

后续研究工作分别针对僵尸网络[Stone-Gross 2009] [Li 2009]、网络钓鱼[Cova 2008]、垃圾邮件[Kreibich 2009][Kanich 2008][Levchenko 2011]、点击欺诈[Daswani 2007][Christin 2010]、PPI 方式恶意代码传播[Caballero 2011]等安全威胁背后驱动的地下产业链进行更为深入细致的调查分析，本文针对中国互联网地下产业链的具体情况，分析了上述技术手段在地下产业链盈利链条中的所处环节与作用，并利用公开渠道获取的安全公司与网络安全监管部门威胁数据统计，给出了 2011 年度中国互联网上由地下产业链驱动的各类安全威胁现状分析。

针对于中国互联网信息安全地下产业链，陈明奇等最早于 2006 年给出了一份现状研究，但仅仅列举分析了信息窃取、“黑客”培训、网络游戏打币等七条盈利产业链，但并未对地下产业链的整体结构进行系统分析，也未对地下黑市进行监测与实证数据分析。2007 年 CNCERT/CC 的报告显示，中国互联网“黑色产业链”赢利模式主要包括黑客培训、信息窃取、恶意广告、垃圾邮件、敲诈勒索、网站仿冒等几种，估计年产值已超过 2.38 亿元，造成的

损失则超过 76 亿元，但并未公布测算方法。

本文作者于 2008 年发表的文章[Zhuge 2008]是首次针对中国互联网上的虚拟资产盗窃地下产业链展开系统性的实证数据分析，揭示了虚拟资产盗窃地下产业链的模型结构，并通过对百度贴吧地下黑市与淘宝虚拟资产交易市场信息的监测，分析了这一地下产业链黑市现状，以及参与者规模和分布情况，此外也通过针对中国互联网网站的采样检测，发现了当时被植入恶意木马实施挂马攻击的网站占到 1.49%的高比例，显示了虚拟资产盗窃地下产业链给中国互联网带来的高度安全威胁。

本文对这一工作进行了进一步的扩展，更加全面地分析了地下产业链结构与盈利手段，也借助于国内主流安全厂商与网络安全监管部门近年来发展的各种网络威胁监测平台，对中国互联网信息安全地下产业链的整体盈利规模与危害人群进行了更为细致的测算，此外还对包括 Web 论坛与 QQ 群的地下黑市信息进行了范围更大、时间跨度更长的综合分析，得出了能够反映中国互联网地下产业链近年来发展规律与趋势的更具价值的结果。

5. 讨论与结束语

本文针对中国互联网信息安全地下产业链给进行了全面深入的实证数据分析与调查，但由于地下产业链从事的是违反法律法规和社会道德的不法行为，因此会始终保持在一种较为隐蔽的状态，通过地下黑市监测，我们也仅仅能够观测到地下产业链最为底层的一些交易与交流行为，而诸如0day安全漏洞、商业情报、APT攻击任务等更高层次的地下产业链交易事件则可能通过更具隐蔽的加密在线通讯进行，因此作为研究者，我们无法对地下产业链进行更具全面性的调查。

通过本文的不完全测算与保守估计，中国互联网信息安全地下产业链已发展成真实资产盗窃、网络虚拟资产盗窃、互联网资源与服务滥用和黑帽技术工具培训四大部分数十条盈利链条，2011年整体造成损失规模达53.6亿元，危害到11,081万互联网网民和105万网站。而我们对地下黑市的不完全监测结果也发现：地下黑市无论在发布信息量还是参与者人数都呈现快速增长趋势，2011年至少有9.27万人参与地下黑市，并发布了10万多个主帖38万多帖子，这显示出中国信息安全地下产业链的活跃。此外，我们通过典型网络犯罪案件的公开关键信息与地下黑市监测信息的关联分析，验证了监测地下产业链黑市对于网络犯罪监控与追查的支持作用。因此，国内网络安全监管部门与执法部门非常有必要建设更加全面覆盖面更加广泛的地下产业链监测体系，并在法律授权范围建立对涉及网络犯罪案件参与者进行在线通讯与银行支付等渠道的调查取证分析工作流程，这将有助于更好地通过法律手段打击网络犯罪行为，威慑地下产业链的参与者，从而保护互联网用户的财产与个人信息安全。安全监管与执法部门对地下产业链黑市的监测将有可能促使其向更隐蔽更封闭的方向发展，但这也会给地下产业链的便捷联系与沟通造成阻碍，而对地下产业链黑市的监测与跟踪需要持续进行下去，才能够对其进行持续性的打击。

而应对地下产业链中如网络虚拟资产盗窃、个人隐私信息窃取与互联网服务滥用等尚未触及现有法律条款的灰色盈利链条，当务之急是通过立法手段确立对个人信息与网络资产的保护法案，在我国，公民信息保护法已经酝酿六年，但时至今日仍未正式进入立法程序，在2012年两会期间又成为社会关注和呼吁的焦点，而对于网络虚拟资产保护，虽然有些案件判罚中已经考虑网络虚拟资产的财产特性，从而对盗窃敲诈网络虚拟资产犯罪人做出定罪判罚，但仍未在法律中明确对虚拟资产的保护。

只有在完善的法律法规保障之下，通过网络安全监管与执法部门对地下产业链的更具严密的监测与追查，以及安全厂商对各种威胁提供的全方位保护技术措施，才能够有效遏制目前中国互联网信息安全地下产业链快速发展的趋势，减轻互联网网民遭受网络犯罪的风险与危害。

致谢

感谢北京邮电大学本科生毛骏与北京信息科技大学本科生侯雷杰参与项目数据统计与地下产业链黑市监测。感谢以下业界同仁们提供帮助（排名不分先后）：安天实验室肖新光、李柏松；奇虎360公司赵武、王宇；金山公司李铁军、王海棠；网秦邹仕洪；知道创宇赵伟、杨冀龙。本文部分工作受到国家自然科学基金项目（61003127）资助，在此表示感谢，文章观点只代表作者，不代表资助方。

参考文献

[CNNIC 2012] CNNIC, 第 29 次中国互联网络发展状况统计报告,
http://www.cnnic.cn/research/bgxz/tjbg/201201/P020120116330880247967.pdf
[CSDN 事件 2012] 武汉晚报, CSDN“泄露门”黑客“臭小子”抓到了,
http://news.163.com/12/0111/03/7NF5BVLF00014AED.html
[央视 315 2012] cnBeta.com, 央视 315 晚会曝光多家银行非法出售个人征信报告,
http://www.cnbeta.com/articles/177376.htm
[公安部 2011] 中央政府门户网站, 公安部公布“天网—2011”行动十大案例,
http://www.gov.cn/fwxx/sh/2011-12/30/content_2033631.htm
[证券大盗案 2006] 江民公司, 木马窃号“证券大盗”被判无期,
http://www.pconline.com.cn/pcedu/soft/virus/safe/0605/795936.html
[央视 315 2009] 央视 315 晚会曝光, 个人信息被大量在线出售牟利,
http://boxun.com/news/gb/china/2009/03/200903152322.shtml
[熊猫烧香案 2007] 新华网, “熊猫烧香”案解密网络病毒产业链,
http://news.xinhuanet.com/legal/2007-02/16/content_5745932.htm
[诸葛建伟等僵尸网络综述 2008] 诸葛建伟, 韩心慧, 周勇林, 叶志远, 邹维*. 僵尸网络研究, 软件学报, 19(3):702~715, 2008.
[瑞星年报 2012] 瑞星公司, 瑞星 2011 年度企业安全报告,
http://sec.chinabyte.com/150/12257650.shtml
[Matrix FIRST 2008] 北大计算机研究所狩猎女神项目组获得世界蜜网项目组织最佳团队奖励, http://ercis.icst.pku.edu.cn/modules/blog/?p=31
[网秦木马报告 2012]网秦公司, 网秦 1 月 6 日截获新远程木马 恶意推广快速消耗流量,
http://blog.netqin.com/?p=1948
[网秦年报 2012] 网秦公司, 2011 中国大陆手机安全报告,
http://www.netqin.com/upLoad/File/baogao/20120112.pdf
[DDoS 私服勒索案 2011] 中国日报, 重庆 85 后建黑客团队勒索私服网游获利 6000 余万,
http://news.ifeng.com/mainland/detail_2011_09/21/9354349_0.shtml
[马斌案 2010] 北京娱乐信报, “马斌案”黑客被判 5 年,
http://news.163.com/10/0324/01/62GLE03N000146BB.html
[敲诈者案 2006] 北京晚报, 隐藏用户文档索财 国内截获首例敲诈病毒,
http://tech.qq.com/a/20060614/000047.htm
[360APP 下线事件 2012] 360 安全卫士, 关于 360 应用遭苹果下架一事公告以及苹果公司最新回应, http://bbs.360.cn/3229787/252736083.html
[改分案 2010]新京报, 黑客网站称可改高考成绩：收费 3 千至 1.5 万元,
http://news.xinhuanet.com/digi/2010-07/13/c_12327494.htm
[计算机证书案 2010]北京晚报, 用木马程序帮网友改分 考试院内鬼被判刑 1 年半,
http://news.xinhuanet.com/local/2010-05/13/c_1298129.htm
[假证案 2010]合肥日报, 合肥济南警方联动破获制售假学历大案,
http://news.hefei.cc/n/14440.shtml
[违章记录操纵案 2003]人民网, 福建首例"黑客"入侵破坏交警网信息案告破,
http://www.people.com.cn/GB/other4788/20030115/908075.html
[龚蔚 2011]IT 发发, 什么是洗库，洗库的避免与解决办法,

http://www.itit88.net/document/201201/283.shtml
[剑客案 2009] 人民网, 两小伙搞瘫网站敲诈“5 亿两银子”被判刑,
http://game.people.com.cn/GB/48644/48662/10589122.html
[吸费案 2011] 新华网, 全国首例“手机病毒恶意扣费”案告破 数十万人受害,
http://www.brand-news.cn/news/guonei/0607/19018.html
[温柔木马案 2009] 新华网, 全国最大制售木马案宣判 案犯涉 16 省市百余人,
http://news.xinhuanet.com/legal/2009-12/16/content_12656680.htm
[大小姐木马案 2009] 腾讯网, 刑法修正后首例木马案公诉：3 个月牟利 3000,
http://tech.qq.com/a/20090306/000136.htm
[CNNIC 2011] CNNIC, 第 28 次中国互联网络发展状况统计报告,
http://www.cnnic.net.cn/dtygg/dtgg/201107/W020110719521725234632.pdf
[艾瑞购物 2012] 艾瑞咨询, 2011 年中国网络购物市场分析报告,
http://www.newhua.com/2012/0201/143441.shtml
[快捷支付 2011]网络导报, 快捷支付 后牌照时代的杀手锏,
http://www.techweb.com.cn/news/2011-11-22/1122294.shtml
[工行网银维权 2006] 工行网银受害者集体维权联盟, http://www.ak.cn/liebiao.htm
[APAC 月报 2011] 中国反钓鱼网站联盟, 月报, http://www.apac.org.cn/gzdt/
[工行数据 2006]工行网站, 工商银行再获“中国网上银行测评”第一名,
http://www.51credit.com/HangYe/YeJieDongTai/T-YeJieDongTai/article170072.shtml
[工行数据 2011] 证券时报, 工商银行个人网银客户数过亿,
http://www.p5w.net/today/201104/t3572526.htm
[黑鹰案 2010] 新华网, 湖北警方成功查封国内最大黑客培训网站,
http://news.xinhuanet.com/society/2010-02/08/content_12954507.htm
[艾瑞网银 2011] 艾瑞咨询, 《2010-2011 年中国网上银行年度监测报告》,
http://www.dynamicode.com.cn/Chinese/NewsInfo.Asp?ID=850&ClassID=45
[360 网购 2012] 360 安全中心, 360 联合易宝发布《2011 网购支付安全报告》,
http://bbs.360.cn/5473016/252581925.html?recommend=1
[易观 2011] 易观国际, 中国第三方网络支付安全调研报告,
http://www.docin.com/p-294024153.html
[游戏产业调查 2011] 中国游戏产业网,2011 年中国游戏产业报告,
http://www.cgigc.com.cn/201201/120087820889.html
[艾瑞网游 2011]艾瑞咨询,2011 年第四季度及全年网络游戏核心数据发布,
http://www.iresearch.com.cn/coredata/2011q4_4.shtml
[智能手机调查 2012]互联网消费调研中心, 2011-2012 中国智能手机市场研究年度报告(简版), http://www.docin.com/p-327004323.html
[网秦估计 2012] 网秦, 专家称手机黑色产业链达 10 亿元规模,
http://www.360doc.com/content/10/0613/14/587283_32870083.shtml.
[金山网购 2011] 金山网络, 2011 上半年金山网购安全报告,
http://www.ijinshan.com/download/2011zgwlgwaqbg.pdf
[支付行业 2011a] 2010-2013 年中国第三方支付行业研究报告,
http://blog.csdn.net/tommyhp/article/details/7033884
[支付行业 2011b] 新京报, 2011 年中国第三方支付市场规模翻番 达 21610 亿元,
http://big5.ifeng.com/gate/big5/tech.ifeng.com/internet/detail_2012_02/23/12715156_0.shtml

[360 网游 2011] 360 安全中心, 2011 上半年网络游戏产业安全报告,
http://bbs.360.cn/3229787/250724377.html?recommend=1
[电脑管家年报 2012] 腾讯电脑管家, 2011 下半年个人网络安全报
告,http://guanjia.qq.com/security/report2011
[CNCERT/CC 月报 2011] CNCERT/CC, 2011 年月报,
http://www.cert.org.cn/articles/docs/index.shtml
[CNCERT/CC 年报 2011] CNCERT/CC, 2011 年年报,
http://www.cert.org.cn/publish/main/46/index.html
[CNNVD 2011]中国国家信息安全漏洞库, 2011 年月报,
http://www.cnnvd.org.cn/news/vulreport#
[CNVD 2011a]国家信息安全漏洞共享平台, 2011 年月报, http://www.cnvd.org.cn/.
[CNVD 2011b]国家信息安全漏洞共享平台, 2011 年周报,
http://www.cnvd.org.cn/publish/main/47/index.html
[安天报告 2012]安天安全响应中心, 2011 年互联网信息安全威胁综合报告,
http://www.antiy.com/cn/security/2012/2011_network_security_report.html
[金山年报 2012] 金山网络, 2011 年中国互联网安全研究报告 ,
http://www.ijinshan.com/news/20120217001.shtml
[金山手机 2012] 金山网络, 2011-2012 年度智能手机安全报,
http://www.ijinshan.com/zhuanti/sjaqbg/
[360 年报 2012] 360 安全中心, 2011 中国网络安全报告,
http://w.qhimg.com/images/v2/site/360/2011report/2012.pdf
[知道创宇年报 2012] 知道创宇, 2011-2012 中国互联网网站安全报告,
http://blog.knownsec.com/wp-content/uploads/2012/03/知道创宇 2011-2012 年中国互
联网网站安全报告.pdf
[两高 2011] 检察日报, 关于办理危害计算机信息系统安全刑事案件应用法律若干问题的
解释, http://legal.people.com.cn/h/2011/0830/c226563-3193010425.html
[Thomas 2006] Rob Thomas, Jerry Martin. the underground economy: priceless, USENIX, 31(6), published December 2006, accessed March 2012.
[Franklin 2007] Franklin, J., Paxson, V., Perrig, A., Savage, S.: An Inquiry Into the Nature and Causes of the Wealth of Internet Miscreants. In: Conference on Computer and Communications Security, CCS (2007)., published 2007, accessed March 2012.
[Holt 2010] Thomas J. Holt, Eric Lampke. Exploring stolen data markets online: products and market forces. Criminal Justice Studies: A Critical Journal of Crime, Law and Society. 23(1), 2010., published 2010, accessed March 2012.
[Herley 2010] Cormac Herley, Dinei Florêncio. Nobody sells gold for the price of silver: dishonesty, uncertainty and the underground economy. Economics of Information Security and Privacy 2010, 33-53., published 2010, accessed March 2012.
[Stone-Gross 2009] Brett Stone-Gross, Marco Cova, et al. Your botnet is my botnet: analysis of a botnet takeover. In Proceedings of the 16th ACM conference on Computer and communications security (CCS '09). 635-647, New York, NY, USA, published 2009, accessed March 2012.
[Li 2009] Zhen Li, Qi Liao, Aaron Striegel. Botnet Economics: Uncertainty Matters, Managing Information Risk and the Economics of Security, book chapter, 245-267.

Springer US, published 2009, accessed March 2012.
[Cova 2008] Marco Cova, Christopher Kruegel, and Giovanni Vigna. 2008. There is no free phish: an analysis of "free" and live phishing kits. In Proceedings of the 2nd conference on USENIX Workshop on offensive technologies (WOOT'08). USENIX Association, Berkeley, CA, USA., published 2008, accessed March 2012.
[Kreibich 2009] Kreibich C, Kanich C, Levchenko K, Enright B, Voelker GM, Paxson V and Savage S. Spamcraft: an inside look at spam campaign orchestration. In: Proceedings of the 2nd USENIX conference on Large-scale exploits and emergent threats: botnets, spyware, worms, and more. Boston, MA: USENIX Association, published 2009, accessed March 2012.
[Kanich 2008] Kanich C, Kreibich C, Levchenko K, Enright B, Voelker GM, Paxson V and Savage S. Spamalytics: an empirical analysis of spam marketing conversion. In: Proceedings of the 15th ACM conference on Computer and communications security. Alexandria, Virginia, USA: ACM, 2008. 3-14. , published 2008, accessed March 2012.
[Levchenko 2011] Kirill Levchenko, Andreas Pitsillidis, Neha Chachra, et al, Click Trajectories: End-to-End Analysis of the Spam Value Chain, Proceedings of the IEEE Symposium and Security and Privacy, pages 431 – 446, Oakland, CA, published May 2011, accessed March 2012.
[Daswani 2007] Neil Daswani, Michael Stoppelman. The anatomy of Clickbot.A. In Proceedings of the First Workshop on Hot Topics in Understanding Botnets (HotBots'07). USENIX Association, Berkeley, CA, USA., published 2007, accessed March 2012.
[Christin 2010] Nicolas Christin, Sally S. Yanagihara, and Keisuke Kamataki. Dissecting one click frauds. In Proceedings of the 17th ACM conference on Computer and communications security (CCS '10). ACM, New York, NY, USA, 15-26. , published 2010, accessed March 2012.
[Caballero 2011] Juan Caballero, Chris Grier, Christian Kreibich, Vern Paxson. Measuring Pay-per-Install: The Commoditization of Malware Distribution, Proceedings of the 20th USENIX Security Symposium (Security '11), San Francisco, California, published 2011, accessed March 2012.
[陈明奇 2006] 陈明奇, 中国互联网黑色产业链现状研究. 现代电信科技, 2006(11): 8-11.,
[杜跃进 2007] 21 世纪经济报道, 黑客产业攻击网络愈演愈烈 国家四部委协同作战联手反黑
[Zhuge 2008a] J. Zhuge, T. Holz, C. Song, J. Guo, X. Han, and W. Zou. 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, published June 2008, accessed March 2012.
[Zhuge 2008b] J. Zhuge, Y. Zhou, J. Guo, et al. Malicious Websites on the Chinese Web: Overview and Case Study, 20th Annual FIRST Conference (FIRST' 08), British Columbia, Canada, published June 2008 , accessed March 2012.
[陈明奇 2011] 陈明奇, 我国互联网灰色产业链分析及其法律应对措施. 政法论丛