链滴

# 中国黑客的隐秘江湖

作者：adminis

原文链接：https://ld246.com/article/1440660765633

来源网站：链滴

世界上能称之为顶级黑客的，只有几百人。他们是上帝的宠儿，获得了一把开启网络世界大门的匙，得以窥见网络世界的终极秘密。
他们的名字不会出现在所谓的“顶尖黑客排行榜”中，他们低调于自己的技术世界，就像遁世的士，潜心修炼。
他们被称为网络世界的“神”，纵横江湖，随心所欲。但在现实中，他们依然是被现实研磨的凡。
他们都曾是黑客技术的爱好者，却在利益的岔路口，走向了针锋相对的对立面，一方为攻，一方守。
攻击方可攻陷所有联网电子终端，如入无人之境，他们是黑产链条中的攻城者，月入千万；防守建立起网络安全骨架，与黑产对抗，如果没有他们的守卫，网络将变成黑暗渔场，被黑产肆意捕捞。
金钱和利益就像分水岭，将人性的两个侧面划分得泾渭分明。
白帽黑客的兴起
“你说得不对。”蔡晶晶发言被一位专家打断。
整个圆桌会议的所有目光聚焦到蔡晶晶的身上。他满脸通红，无言以对，仓惶落座。
这是 2001 年的一次“反病毒大会”。当时，尼姆达（nimda）蠕虫病毒肆掠，大量电脑断网。晶晶不过 19 岁，刚进专业网络安全公司“启明星辰”不久，以技术专家的身份出席。
他发言称，其实微软在事发 7 个月前已发布官方补丁，只要修补漏洞就不会造成如此大影响，“明网络管理员没有尽责，事件主因是人为因素”。
未经世故的蔡晶晶不知道，现场就有很多网络管理员。在他们眼中，这个 19 岁少年显然不是在开挑衅是什么。
一位专家毫不留情地打断他的发言。专家认为说，系统应该自动升级，事件主因要归结于安全方不够完善。
当时的蔡晶晶还没有意识到，这件事足以影响他的一生。“蝴蝶效应”的翅膀已然张开，在某种义上，也改变了中国网络安全人才培养的历史。
在 2015 年以前，我们找不到任何关于“蔡晶晶”的报道。经常有人被他女性化的名字给骗了，实他长相斯文，戴着眼镜，是个 80 后帅小伙。
外界虽未耳闻，但在黑客圈子里，“蔡晶晶”是一个无论如何绕不开的名字。你会发现，几乎所黑客和他都多少有些联系。
一个时代的开启需要一个符号。中国产生真正意义上的黑客，应该追溯到 1997 年上海黑客龚蔚goodwell）成立第一个中文黑客站点“绿色兵团”。此时，民间零散的技术爱好者开始集结成群—蔡晶晶也是其中的一员。
2001 年，南海中美发生南海中美撞击机事件，美国率先对中国的网站发动攻击。中国民间黑客自发打响黑客反击战，“绿色兵团”也参与其中。
在战斗过程中，蔡晶晶和几个朋友组建了名为“0x557”的黑客组织。现在来看，这个团队出现众多顶尖黑客，这些人几乎构建了中国的互联网安全骨架。
这场民间力量的黑客抗衡，最终没有赢家。美国黑客导致中国很多网站瘫痪，中国黑客也攻陷了宫网站。但这次“战斗”，让中国黑客切实体会到中美技术的差距，毕竟操作系统、通用协议、编程言，都是英文的，就连互联网都是美国创造的。这种差距让很多中国黑客沉下心来专钻研技术。
蔡晶晶记得，当时有主流媒体发表言论说，号召国内的所有互联网用户用计算机去 ping 倒一个站，“确实无知而可笑”。
黑客大战结束后，蔡晶晶开始专研漏洞挖掘。他发现微软的 IE 浏览器存在一个漏洞，可导致用在观看图片时被注入木马。
蔡晶晶将漏洞提交微软，对方电子邮件回复说，“这是一个程序 bug，但不是一个引起安全问题漏洞”。，年轻气盛的蔡晶晶不干了，他把漏洞细节公布在一个黑客论坛上，“小伙伴们都炸锅了”
微软终于重视到问题的严重性，他们主动找到蔡晶晶，希望他能加入微软安全部门。那时，蔡晶的他，只有 19 岁。
而中国最早的网络安全公司“启明星辰”也发现了蔡晶晶的夺过人之处，邀请他加入。“你可以护咱们国家的网络安全”，中美黑客大战情愫犹在的蔡晶晶，选择了“启明星辰”。
和蔡晶晶一样，当时有很多技术超群的小孩被安全公司发现。他们得到了机会，在一个专业而健的环境中成长。如今，他们已成长为中国网络安全的顶梁柱。
蔡晶晶很快崭露头角。一次，原信产部的网站被入侵，政府让“启明星辰”派出安全专家来“灭”。，蔡晶晶连夜被派过去，到了门口却被保安拦住了。一个穿着 T 恤、趿着拖鞋的小孩怎么可能是

家？尽管年轻，但每次他都用超强的实力证明自己，不久就成为公司的核心力量。
蔡晶晶在“启明星辰”待了的 14 年，一直是黑客团队的负责人。他坚持认为“人为因素”是导安全事件的主因，人才的培养至关重要。蔡晶晶将“0X557”的部分精英拉入“启明星辰”，并培养近百位顶尖安全人才。
这些网络安全防守方的黑客们，被称为“白帽黑客”。“启明星辰”俨然已成为白帽黑客的黄埔校。
某种意义上说，蔡晶晶正是白帽黑客的教父。
黑产的疯狂成长
如同武侠电影中的情景，白帽黑客在网络安全的历史舞台上，一直是白衣胜雪、披风昂飘的侠客象。演对手戏的，则是黑帽黑客：一群神秘而技艺高超的蒙面人。
黑帽黑客的兴起要比晚于白帽黑客晚。2000 年的黑客群体都是侠骨柔情的安全爱好者，他们坚初心、不卑不亢。2000 年后出现的黑客，受到黑产（黑客黑色产业链）的侵染较多。
拖鞋、T 恤、黝黑、清瘦，不修边幅……如果说坐在《创业家》记者面前的这个 85 后小孩，就中国的顶级黑客，可能没有人会相信。
我们管他叫 K。他常年潜伏在网络黑产最幽暗的角落，是黑产链条最上游攻城略地的先锋。他的事听起来像天方夜谭，却能从他身上窥见暴利黑产的疯狂。
和其他 80 后孩子一样，K 是中国第一批互联网用户。他自学成才，四处拜师学艺，最开始也盗盗 QQ，监控一下喜欢女孩的电脑，满足偷窥欲。
K 的天才很快光芒毕现。黑客都会加入一些组织，谈论技术，组成联盟，K 也不例外。因为一些人恩怨，组织负责人将 K 踢了出去，并四处发帖“黑”他。只学了半年技术的 K 找到论坛的漏洞，接接管管理员权限，开始进行报复攻击，把帖子全部锁定，搞黄了一个论坛。
报复的快感，让他尝到技术的甜头。
K 只有初中学历，在现实生活中很难找到好的工作。随着技术能力的增长，他开始有机会涉猎中的黑产。“DDoS 勒索”是他的第一个“玩具”。DDoS（分布式拒绝服务）是一种网络攻击手段，过大量合法的请求占用大量网络资源，以达到瘫痪网络的目的。
形象一点的比喻是，你开了一家小面馆，黑客派了几百号人涌入你的店里，也不消费就霸着场子导致其他顾客根本无法挤进入店里。
“想开业？每个月给我十万 10 万的保护费。”K 勒索的目标是一些电商网站，靠收保护费每月收百万。但他很快就玩腻了，因为 DDoS 技术含量极低，“简直就是浪费我一身的顶级装备。”
互联网迭代速度极快。，新玩意 2009 年后，电子虚拟货币“比特币”兴起。电脑上可以安装挖软件，经过一系列步骤繁琐的特定算法，就能在一定几率上产生“比特币”。市面上有性能强悍的计机作为“比特币挖矿机”销售，但价格不菲。
“天下之大莫非王土，天下的服务器皆可为我所用。，”K 黑进国外一些拥有上万台服务器的大企业，在其后台偷偷运行比特币挖矿软件。
K 坐在黑暗小屋中遥控，几百万台服务器轰隆隆同时启动运算。他在电脑前啃着汉堡喝着可乐，着这支挖矿大军无坚不摧，比特币一个个叮叮当当掉入他的钱袋。在比特币行情最好的年代时期，他月入几百万。
除了比特币，K 偶尔也会盗取一些游戏账号。理论上说，K 几乎可以攻破所有网站，只是投入多时间和精力的问题。如果正面攻击太耗损精力，他会另辟蹊径。
有一次，他制作了一份动过手脚的简历，发给一家安全防守严密的游戏公司的 HR，假装应聘。方一点进去，后门程序自动启动。K 顺利入侵游戏公司内网，洗劫游戏账号，这一单生意让他挣了几万。
中国的地下黑产已组成黑暗的暴利帝国，分工极为明确。大部分黑客的网上攻击行为难以被追踪一些攻击工具和代码都存放在加密硬盘中，电脑一旦重启，硬盘永久锁死，很难取证。即便公安人员入黑客老巢，抓个现行，黑客电源一拔，便再无直接证据。
大部分黑客都是在线下交易环节被抓。黑产圈流行的一句话叫“有命挣，没命花”，高风险带来收益，变现者是利润最丰厚的工种。
大部分黑客都是团队行动，各取所长。，像 K 这种千手观音型黑客并不常见。据 K 透露，顶尖客的月收入可达到几千万美金美元。他们从未出现在媒体中，对自己保护极为严密，很多人挣够钱后就销声匿迹了。
没有硝烟的战场
眼前是一张特殊的世界地图。上面此起彼伏，出现许多亮点。点与点之间，有线条交叉串联。
这是“知道创宇”公司的网络空间实时防御与追踪系统。在这里，可以用上帝视角去俯瞰黑客世

的实时攻防大战。任何一条线，都是一次攻击行为。任何一个点，都是一个攻击目标。这张大网，就网络世界没有硝烟的终极战场。
“这个世界是危险的，不是因为那些邪恶的人，而是因为那些无动于衷的人。”这句话出自爱因坦，也是赵伟的人生信条。
赵伟，“知道创宇”CEO，蔡晶晶创立的“0X557”的成员，也是蔡晶晶的多年挚友。
赵伟像是白帽黑客中的天才人物。他的论点极为超前。他认为真实世界与互联网世界本质上一致都是输入信息，输出信息。一个人获取知识，是在输入信息。一个人创造价值形成理论，是在输出信。因此，他把互联网世界看得和真实世界同等重要。他了解网络世界越深入，就觉得世界越危险，他法做到无动于衷。
在攻防博弈的江湖上，攻守双方，相互之间也“看不上”。
“黑产的那一帮，不算黑客。，他们就是劫匪。你有一把刀，去抢劫手无寸铁的人，就这么回事”赵伟有道德洁癖。有黑产背景的人，纵然才华顶了天了，他也不会接纳到自己团队。
“他们防得住我吗？”K 嗤之以鼻，他甚至觉得，白帽黑客不过是给自己戴高帽的技不如人者。
就像两边开战前相互放狠话，接着就是“沙场上见”。
事实上，黑客江湖的攻击水平远高于防守水平。如同围棋的黑白子博弈，先动手抢占要点的人，会有先手优势。再加上，黑产有暴利的利益驱动，他们整合资源的能力远超防守方。
与一般白帽黑客不同的是，赵伟不是简单防御，而是试图改变网络规则。“任何世界都有规则，有引力，热力学，相对论等等，我们的世界是现在的样子，都是因为这些规则。”赵伟觉得，只有形新的安全规则，才能从本质上扭转攻守局面局势。
2012 年 9 月，“知道创宇”联合腾讯、百度、金山共同创立了“安全联盟”。赵伟试图参与整网络安全产业链，联合对抗黑色黑产。
这个联盟的牛逼之处是，利用“知道创宇”开发的安全产品，可锁定黑客攻击，获取位置，并进一段时间网络行为观察。一旦被打上“黑客”的标签，安全联盟的所有网站都将拒绝其访问。另外，些存在欺诈、钓鱼、盗号等风险的网站，都将被百度搜索背后贴上“风险提醒”标记。
黑产的蛋糕，被赵伟切割得支离破碎。有些黑客前来求饶，请求放行；有些黑客在论坛中扬言 20 万干掉他，利用黑客技术进行人肉搜索，将他的隐私信息全部公开。赵伟的手机每天都接到大量的威短信和恐吓电话，他不得不更换手机，“我感觉来自世界到一种深深的恶意，这种恶意是随时准备要的命。”他请了一位新助理，是跆拳道黑带，身兼保镖职责。
但最让赵伟感受到威胁的是美国斯诺登事件。事件之后，被曝光的“棱镜计划”表明，美国政府可以从电邮、消息、视频、照片、存储数据、甚至语音聊天等全方位对人进行监控。
这就是说，美国已进入“上帝模式”，大数据的挖掘和情报收集，让互联网世界已无死角可言。同时也证明，大数据时代的到来和云计算的运用，让黑客攻击方的能力已无限升级。
赵伟用了一个比喻，互联网世界就像一个海洋渔场，以前用鱼叉捕鱼，现在升级为巨型捕鱼船。成千上万的鱼落入网中，他们可能只挑选其中最肥美、最珍贵的一条，其他再放掉，就这么任性。”
对这个问题上最有发言权的，恐怕是中国最顶尖的白帽子黑客团队 Keen。在国际安全比赛中，们曾因 30 秒找到苹果手机系统漏洞而轰动世界。
Keen 团队从表面上看是攻击的一方，实质是为了寻找漏洞及时修补，攻击的目的是为了更好的防守。Keen 团队已是国际上的最顶尖的漏洞猎手。
Keen 团队创始人王琦（绰号“大牛蛙”）说，大数据时代，我们可以看到明显的攻击（譬如盗银行卡等）将不再是主流，主流的是隐蔽性攻击。
“大数据时代，数据就是钱。”，王琦说。黑客们可以从互联网中盗取各种数据，“地下社工库就是其发展的结果。
社工库的地下暗战
社工库，传说互联网中的地下宝藏。盗取用户数据的黑客们组成了利益联盟，将各种渠道获取的据进行汇总分析。姓名、身份证、银行卡、密码只是最基本的信息，这个底下地下数据库甚至能精细征信、体检、病史、性格爱好等。这些数据可以素描勾勒出被盗用户的完整肖像。
互联网用户数据泄露从未消停，京东用户密码泄露，12306 火车购票网站用户数据满天飞等，这被曝光的数据只是地下社工库中的冰山一角。
只要搜索“社工库”，就能找到一些可查询泄露数据的网站。《创业家》的记者将自己常用的邮和用户名输入，发现密码早已泄露。同时又将几个朋友的邮箱输入，也均能查到外泄密码。
互联网上的用户信息已被扫荡成什么样子，业内有句话叫“十墓九空”，可见已然千疮百孔。</>

近几年，中国互联网金融兴起，P2P 金融遍地开花，以每天新增一两家的速度急速发展。在 K 中，这些公司都是肥肉：有钱，创业型公司，对安全没有重视。他进入这些网站，比进后花园还容易
横扫一片，无往不利。K 进入互联网金融平台的后台，将有价值信息盗取出来，专业术语叫“脱”。
如何从浩如烟海的数据中找到价值信息，K 有一项超出常人的天赋。他的实战经验太多丰富，对与他交过手的安全人员太多，什么的套路和战术，他全了然于胸。他能猜出他们下一步行动，甚至能出管理员密码。
他曾经入侵一家互联网金融公司，在几个 G 的后台数据中，一分钟内准确找到了备份系统的机文件夹。
“我猜到了管理员可能设立的文件夹名字。”就是如此可怕的直觉。
K 转手将用户数据卖给勒索机构，让他们拿着数据去威胁互联网金融公司。“一旦公布数据，公会名誉扫地，甚至面临破产。，因此一般的公司都愿意掏钱，息事宁人。”
数据盗取的另一种合作方式是定制化服务。一些企业想购买竞争对手或合作伙伴的核心数据和用资料，就会让黑客去盗取数据。
“了解黑产后，你会觉得，商业战场没有公平可言。如果你想买到对手的核心数据，只要找到靠的人，2 万元就能搞定。”K 说。
数据的沉淀，则形成了社工库。像 K 这样手头有大量数据的黑客，就会与一些类似的黑客们合作将手头的数据汇总，积累越多，价值越大。
如果说互联网进入大数据时代，那么社工库就是地下非法大数据。现在整理社工库的黑客团伙，在沉淀数据。其详尽已达到可怕的程度，可利用这些数据完整模拟出一个人。目前社工库数据的主要途是高级金融诈骗。
未来的潜能？大数据有多大的潜能，社工库就有多大。
值得庆幸的是，这个世界像赵伟一样的卫道士人并不少。他们试图搭建起核心信息数据的安全城，守住网络的最后阵地。
青藤云安全的 CEO 张福，80 后黑客。他在大学时代就表现出惊人的黑客天赋，毕业后进入盛大昆仑万维等企业掌舵技术和业务安全部门。他是国内为数不多的，打通网络业务研发和安全体系两个域的黑客。
2014 年，张福放弃百万年薪和即将兑现的千万股票，与传奇黑客风宁一起组建了青藤云安全公。他们正在开发一款 SaaS 模式的云端安全产品。这款产品的魅力之处就在于，会根据不同企业的需，自适应构建安全体系。
某种意义上说，青藤云安全的产品也在试图扭转攻防之间的悬殊。传统互联网公司受到攻击，即最终解决，这个经验也不会外传输给下一家别的公司，“所谓“家丑不可外扬”，其封闭性是导致防方成长缓慢的重要原因。但如果 100 家企业用青藤云安全产品，只要其中一家企业挡住攻击，其他家会免受同样威胁，“攻击者批量攻击，我们是批量防御。”
安全产品升级，加固城墙、提高壁垒是一种对战方案。而蔡晶晶提供了另外一种解决途径，他派了更多的援军军队。
2014 年 11 月，工信部电子科技情报所提出，目前我国中国网络安全人才缺口上百万。截止截至 2014 年，我国中国 2500 多所高校中开设“信息安全专业”的只有 103 所，其实博士点、硕士点不到 40 个，每年培养的大学的“信息安全专业”培养的人才不到一万 1 万人。
早在 2012 年，蔡晶晶就意识到了这一点，他离开“启明星辰”自己创业，试图将“启明星辰”累的人才培养经验推广到更多企业，。他的公司推出了“e 春秋”系统，专门用于企业内部的人才培。今年 6 月份，他又推出了“i 春秋”系统，用于培养民间安全人才。“i 春秋”不仅找来业内大牛录教学视频，还提供在线实战和比赛的竞技平台。
如果时间倒流回到 19 岁，蔡晶晶再次面对那位专家，他会说：“我们说得都对。，安全产品需更人性化的设计，安全人才也同等重要。”
“我到底是谁？”
K 最近专注的“生意”，是攻陷国外消费网站，获取用户信用卡数据。国外信用卡消费不需密码他倒手将黑卡卖给盗刷团伙，月入千万。
他没日没夜地加班。以前每天只“工作”4 小时的生活规律完全打破。
他有非干不可的理由。K 说，他交往多年的女朋友最近查出身患绝症。治疗费用是一个天文数字他要为她攒够救命钱。
在互联网上，K 恣意妄为。在现实中，他也有无能为力的时候，只能抓住最后的救命稻草。说他忍也好，说他幼稚也罢，他就是要用洗劫世界的方式，达到他的目的实现自己的目的。上帝给了他一

钥匙，他却把它变成吸金棒。K 没有信仰，他唯一信仰的，就是金钱。当金钱也不是万能的时候，他不知道该信仰什么了。
K 有时也会困惑，不是来自道德的审判，而是对于自我价值的拷问。“我到底是谁？无疑我是自的，我穷尽一生，无非是为了非法窃取别人的所得。我可能就是一个病毒，一个 bug。”
K 说，等女朋友病好了，挣到这辈子花不完的钱，“就退隐江湖，在国外买栋海边别墅，带着她朝大海，春暖花开。”
“你会良心不安吗？”提这样的问题，K 会嘲笑你。，可他并没有安宁。K 一直用黑莓手机，据黑莓拥有世界上最安全的系统，任何人都无法盗取其中信息。K 的黑莓从来不联网，只用来打电话发信。他把自己与网络完全隔离，躲在黑暗角落，谨小慎微地活。他是惶恐的，因为他没有找到“我到是谁”的答案。
至于赵伟，他很明白自己是谁，他也深谙自己的使命，可是同样逃避不了现实的磕碰与研磨。
最大的困扰也是钱。创业初期，资金紧张，赵伟啃了一个月的馒头。他发现，自己一个月最低消是 3000 元，其中 2000 元租房，1000 元生活费，他就每个月只给自己开 3000 元工资。公司每年要经历几次即将倒闭的窘境，赵伟不得不问不向朋友借钱。后来朋友借怕了，他就去借高利贷。借来一百万 100 万现金在办公桌上垒成一座小山。转眼间小山就空了，变成员工的工资。
公司成立至今，开发的安全产品少说也有几十种，可被市场接受活下来的产品也就几种。“我们计的安全产品都太过超前，很多企业根本无法理解。”赵伟说，他能做的，就是反复说服。
“做安全的人真的很苦，我们就是一个保安的角色。”张福说，目前阻碍中国网络安全发展的最障碍，是安全意识不高，“创业型企业第一步就是活下来，安全的需求并不是最主要的。”
张福经过市场调研发现，一个公司建立安全系统，每年至少要投入 100 万。一两个安全人员，些必要的安全产品，这还仅是最低配置。创业型企业基本属于“裸奔”状态，企业的管理者通常不愿支付安全花销，而是抱着侥幸心理。但一旦被攻陷，其影响却是致命的，甚至面临破产。
“没有过切肤之痛，很难意识到安全的重要性，但真正意识到的时候，已为时已晚。”张福说。
赵伟的团队通过扫描曾经发现很多企业的安全漏洞，他们打电话去提醒企业时，对方的态度大都现得无所谓，脾气暴躁点的，就开始谩骂。
市场在一点点吞噬赵伟的理想，但蔡晶晶倒比较乐观。斯诺登事件之后，中国领导人提出：“没网络安全，就没有国家安全。”，对互联网安全的重视，已经上升到国家层面。蔡晶晶认为，这就是络安全春天到来的号角。
2015 年春天，北京高碑店一个没有路名、没有门牌的四合院内，葡萄藤缠绕着小桥流水。远离嚣，辟得一处清凉。
一个叫“神话”项目在这里启动，曾经的顶级黑客王英健，试图用真人秀的方式快速培养信息安人才。学员们每天都在进行封闭式训练，白帽黑客的大牛们，来到这里将毕生所学技艺倾囊相授。除技术，还有坚守良心和正义的执着。培养黑客的过程，就像在创造“神话”。
曾经的黑客教父、绿色兵团的创始人龚蔚告诉《创业家》的记者，属于第一批代黑客的世界已经变，而新生的一代黑客，正在慢慢成长起来。