现在叫我黑客，我会立刻纠正

中国第一代黑客揭秘：借安全漏洞牟利已成黑色产业链

本报记者 **叶薇**

“飞云”（网名）今年38岁，1995年开始接触互联网，是中国第一代黑客。正值互联网安全大会召开，他作为一家主攻网络安全的企业高管参会，感慨万千。“我退出江湖很久了，这个圈子变化太快，很多东西都走样了。”

尽管他不当黑客很多年，但由于长期关注，深谙黑客背后的隐秘产业链。以下为“飞云”的口述。

曾经崇尚自由与高技术

1997年我第一次从美国网站上听说“黑客”这个词。那时大陆中文网站上几乎没有，所有信息都从国外和我国台湾地区获得，我们一帮技术爱好者疯狂搜寻各种关于黑客的信息。

在我们看来，黑客象征自由、高技术，大家都想掌握高超的编程技术，有解决问题和突破限制的欲望。

我们成立了一个论坛，一群爱好者很快聚集在一起，交流互联网安全技术领域的最新资讯、攻防技术的学习心得等。渐渐有人发帖公布一些操作系统和网站的安全漏洞，大家一起研究、破解。我们会寻找一些特定的目标来攻击，只是为了证明自己有挖掘漏洞和入侵的能力，一般进去后马上就出来了。

当时，如果谁发现了漏洞，第一时间会分享给大家。现在很多互联网公司的高管、主管等，大多是从我们那里出来的。

说实话，黑客的主要作用是“建设”，而不是“破坏”。我们一旦找到漏洞，通常都会免费将所知的信息提供给微软、谷歌、苹果等科技公司，协助它们堵塞漏洞。

十年前，别人说我是个黑客，我会觉得很骄傲；十年后，有人说我是黑客，我会立刻纠正他。

地下交易达到商业目的

2005年以后，这个圈子有了特别明显的变化。之前，很少有人炫耀自己攻击了什么网站，更不会有人想用网络技术非法牟利。我们崇尚自由、共享的互联网精神，有一些心照不宣的网络道德标准。

圈子的良好生态逐渐被打破了。起先是一些公司出钱让黑客帮助寻找自己的安全漏洞，然后就发展为地下交易：中间人抢先把漏洞拿走，价格是公司的好几倍。拿走漏洞有很多不可告人的商业用途。

越来越多的黑客，已经把目光从率先发布漏洞的荣誉感转变到利用这些漏洞得到经济利益上。

圈子里把没公布的漏洞叫0DAY漏洞，是指已经被发现、而官方还没发现、没有相关补丁的漏洞。一个0DAY漏洞能换几十个普通漏洞，非常值钱。0DAY还有了网上交易，黑客们通过网上报价出售，一个操作系统或数据库的远程溢出源代码可以卖到上千美元，甚至更高。

现在，全世界都有人找黑客提供服务，有些国家或政府也会向黑客购买信息，他们主要不是为了防堵安全漏洞，而是希望利用漏洞达成目的。泄露美国“棱镜”监控事件的斯诺登，在公布的机密文件中也揭露美国是程序漏洞的其中一个买主。

2011年曾发生过黑客在网上公开了中国最大的开发者社区CSDN网站的用户数据库，600多万个注册邮箱账号和与之对应的明文密码泄露。圈子里都清楚，这些资料早就泄露了，已被用了好多次了。有人为了炫耀就公布了，随后陆续有人跟进，其实公开了就毫无利用价值。

阵地逐渐转向手机用户

这些靠漏洞赚钱的黑客，对网络环境的危害很大。他们惯用的手段一般有：

■ **编写“免杀”木马**　一旦玩家中了这种木马病毒，账号和密码会自动发到一个地址里。他们还为木马程序进行“免杀升级”，这样一来，普通的杀毒软件就算及时更新升级，也没法查杀出这个木马。一般这种都是用来盗取游戏账号卖钱。

■ **偷流量**　要么修改网站内的链接代码，当有人登录一些知名网站等次级链接时，会跳到其目标网站；或者在网站后台做手脚，当有人打开网站时，会自动暗中弹出其目标网站，用户却看不到。一些小网站靠广告赢利，广告商则按点击率给这些网站支付广告费。黑客在后台控制一些知名网站，可为客户瞬间提供几十万的点击率。因此，这些网站难免会遭受攻击。

■ **商业间谍活动**　有个黑客端着笔记本电脑进了一家酒店，第二天他出来的时候，电脑里存着这家酒店所有的客户数据。这是酒店竞争对手给他下的单子，为的是把客户都抢过来。这批数据卖了100多万元。还有一些公司在商业谈判前夕，请黑客去盗竞争对手的“底牌”。

■ **通过网银偷钱**　比这些更黑的生意是通过网银偷钱，但也更危险，很少有人敢在国内做。现在很多黑客把阵地从微软转到安卓、从电脑用户转到手机用户了。越来越多移动恶意程序拥有命令和控制服务器的后门。

这个圈子确实有赚钱多的，我听说有黑客一年赚了5000万元，赚几百万上千万的更多，我身边就有。其实，这些黑客，大多没有正经工作，也不出名。他们都是打工的人，这条产业链上真正的大鱼是渠道商。有人给渠道商下单，他们就雇一些人找黑客谈价钱，这都不知道倒过几次手了。目前市场上有不少中介，专替黑客与买家接洽，赚取高额佣金。

【相关链接】

“云上安全”支招

■ **“老屋”最容易漏水**　PDF、Java、Flash等你所熟悉的程序越来越多的恶意软件利用“盯梢”。因此，个人用户也要学着经常杀毒以修补漏洞，尤其是容易感染的系统老漏洞，时刻保持关注，警惕新的漏洞出现。

■ **一部机坏了一锅粥**　目前针对智能手机有3000种病毒，其中1000多种为木马，恶意应用软件有5万多种，而当所有的手机都能Wi-Fi上网又具备3G上网能力时，一个个手机就相当于把原来保护严实的企业“防火墙”给咬出了缺口。所以尤其对部分敏感单位，并不建议开放Wi-Fi，也不建议用外部U盘。

胡晓晶

图 CFP

防御黑客组织需有国家力量

“曾经密码让我们感觉很安全，但现在密码也保不了你上网！”奥巴马的网络安全智囊、美国智库战略与国际研究中心高级研究员詹姆斯·刘易斯昨天透露，国家网络安全已成国际竞争新战场，目前已有46个国家启动了相关计划，其中12个国家制定了网络攻击部署，且大部分以关键基础设施为目标。他强烈建议，作为全球互联网应用最发达的国家和互联网网民最多的国家，美中两国应从国家层面来合作探讨网络安全问题。

据美国智库信息技术及创新基金会（ITIF）的报告显示，近期由斯诺登触发的美国国安局（NSA）“棱镜”项目被曝光，将导致美国云计算行业损失250至350亿美元，因为这让不少企业觉得“美国云”也不是“保险箱”。为此欧盟也制定出云计算标准，以便绕过美国的服务器，避免可能被监控。

中国计算机网络应急技术处理协调中心最新数据显示：2013年上半年，抽样监测发现我国境内共有693万余台主机感染木马或僵尸程序，较去年同期下降16.0%；但大量感染主机受控于境外服务器，在1.5万个木马和僵尸网络控制服务器中，位于美国地址独占1/3；有1.6万余个境外IP，通过植入后门对境内的3.3万余个网站实施了远程控制。该中心运行管理部负责人王明华指出，应从攻击和防御两大角度来划分国家网络安全责任：如果攻击方为黑客组织，当攻击对象是国家政府和重要基础设施时，防御方应为国家力量；但如果攻击方有国家背景，则其攻击对象无论是政府、企业还是个人，防御方都必须是国家力量。

本报记者 **胡晓晶**

网络安全远非杀杀毒这么简单

只要一个改装的充电器，60秒就能黑掉你的iPhone？只要你敢亮出QQ号，10秒钟别人就能知你真姓大名，连带你的朋友圈？只要小小一个U盘，就能让“固若金汤”的企业内网“破功”，演变成商战“碟中谍”？昨天，由中国互联网协会、中国信息安全测评中心、360等联合主办的2013中国互联网安全大会在京拉开帷幕。作为中国年度规模最大的信息安全盛会，本届大会齐集了来自全球的近百位顶级网络安全高手。

信息泄露威胁近在咫尺

如今的网络安全，远非杀杀毒那么简单：一方面对移动设备安全威胁的捕获、识别、处理，必须依靠云端的计算能力；但另一方面，“云上的开放”，也给“黑客”们留出了足够的“盗梦空间”。

你见过现场版的黑客“钓鱼”吗？昨天，在软件安全分论坛上，子衿晨风科技公司的CEO王清随机邀请一名观众上台，索要后者的QQ号码后加进一段代码，大屏幕上便直接显示出该观众的真实姓名和社交关系网。在移动安全分论坛上，360移动研究院的高级研究员周亚金则演示了恶意程序如何利用定制系统的漏洞来“钓鱼”：远程可控的恶意程序既可伪装成银行短信，亦可“变装”为亲友号码，据悉约有50%的漏洞皆因厂商定制而生。

中国免费安全软件普及

目前，中国还是全球唯一普及免费安全软件的互联网大国。因为免费杀毒应用的普及，在微软今年的《全球个人安全入侵报告》中，中国的恶意软件感染率从原来的“重灾区”降到了“相对安全区”，中国用户的被入侵比例仅为全球平均水平的1/10。不过，上网安全依旧是一个沉重的话题。

在国内最大的互联网安全平台360上，每天截获的手机恶意APP、恶意插件就有2500款，每天拦截各种办证、银行打款垃圾短信将近2亿条，每天截掉的骚扰电话就超过9000万通。360董事长兼CEO周鸿祎坦言，从最近监测到的网络攻击类型和安全事件看，小到为了窃取别人的网上钱包，中到涉及企业的不正当竞争，大到代表着背后的国家利益，网络犯罪远非几十年前老一辈黑客只为秀能力、秀技术的“老黄历”可比。

智能时代面临全新挑战

中国互联网络信息中心（CNNIC）最近发布的《第32次中国互联网络发展状况统计报告》显示：截至今年6月底，中国网民规模已达5.91亿，且有近八成人用手机上网。

中国工程院院士、中国互联网协会理事长邬贺铨指出，下一代互联网将从PC转到手机，甚至各种各样的智能设备、可穿戴设备、智能硬件上，包括家电、汽车、单位里的工业控制设备等等，届时都会面临攻击者的挑战。

未来的安全挑战，不仅出现在你刷微博、看微信、打游戏、收邮件、上淘宝、用网银的时候，也不只是为了盗取密码、钓取信息、偷取钱包，甚至还可能出现在以下场景中：你正为能用手机APP来遥控调节智能照明而自鸣得意，却不料这一新奇系统也有可能受到黑客攻击，被人远程恶意关闭；当你开着新买的混合动力车，殊不知一脚踩上刹车板后，这辆爱车却拒绝停下，只因它的计算机系统已被黑客入侵……信息安全的“攻防战”将永无止境。

本报记者 **胡晓晶**