揭秘技术大神越狱那些事儿

盘古越狱创始人称越狱为名不为利 苹果用户越狱热情消退

近期，一则因越狱导致20多万苹果用户账户被盗的消息又让已经逐渐被很多苹果用户淡忘的“iOS越狱”重新受到了关注。能不断攻破苹果系统的究竟都是什么样的技术大神？什么人还在使用越狱服务？越狱是否真的存在很大安全隐患？第一个完全由中国黑客高手组成的越狱团队——盘古越狱的创始人向记者揭开了越狱背后的那些故事。

什么是越狱

越狱是指开放用户的操作权限，使用户可以随意擦写任何区域的运行状态，只有越狱成功后iPhone的文件系统才处于可读写状态，可以安装和运行未经过官方认证的第三方程序、插件。

越狱优缺点

●优点

1.在原本iOS4.x不越狱时有后台运行功能的基础上，能够使某些不支持后台运行的程序支持后台运行。

2.系统权限很高，可以自己优化系统，可以修改系统文件。可以安装更多拥有高系统权限的软件，例如：与其他设备蓝牙发送文件、短信回执、来电归属地、浏览器下载插件、flash插件等等。

3.可以更换主题、图标、短信铃声等等。

4.可以借助第三方文件管理软件灵活地管理系统或者其他文件，把iphone当移动硬盘（U盘）。

●缺点

1.费电。

2.可能会造成系统不稳定。

3.在新的手机固件版本出来的时候，除非你备份了，否则千万不要及时进行更新。因为每个新版本的固件，都会修复上一个版本的越狱漏洞，使越狱失效。

4.产生小BUG。

5.在使用一些破解插件的同时会出现“白苹果”（白屏）或导致系统不稳定。

A 3个月做出越狱工具

刚刚三十出头的韩争光已经从事网络安全行业超过14年，曾在多家网络安全企业任职，在安全圈子里绝对是“大神”级别的高人。2014年初，正是他和两位好友徐昊、陈小波一起做出了第一版的盘古越狱工具，打破了国外黑客在越狱领域的垄断地位。之后，又陆续有多位业界大神加入了盘古团队。

“能做出完美越狱工具的，一定是黑客高手中的高手。”有业内人士这样评价。的确，盘古团队虽然人数并不多，但核心成员个个是安全领域的传奇人物，网上名称在业内广为人知，但真实身份知道的人却很少。

虽然盘古的第一版越狱工具去年才发布出来，可对于盘古团队中的几个成员来说，越狱是他们早就想尝试的一件事。“早期的几个人都是我十几年的老哥们儿，大家都有兴趣想搞搞iOS的东西。不过后来大家出国的出国，创业的创业，都没时间搞。”韩争光介绍，直到2014年初，他们才真正决心动手去“搞一搞”。

制作第一版iOS越狱工具的韩争光、徐昊和陈小波当时都有各自的工作，也分处不同的地方，陈小波更是远在美国，3人就利用闲暇时间，在网上沟通分工，尝试向号称最安全的苹果iOS系统发起挑战。

3个月之后，3个人实现了中国黑客在iOS越狱领域的突破。从技术上讲，越狱最难的部分是挖掘漏洞不像国外越狱者拥有从第一代iOS越狱开始的工具积累，从零开始的盘古团队在开发越狱工具上花费了大量的时间。

越狱工具做出来后，陈小波建议用“盘古”这个名字，立刻就获得了同伴们的一致认可。“这个名字有两重含义：第一，苹果是一个封闭的生态圈，越狱就是给用户自己控制设备的自由，就像盘古开天辟地；第二，我们也是国内第一个独立完成完美越狱的团队。”韩争光表示。

B 越狱背后的名与利

成功开发出越狱工具，在黑客的圈子里也算是一个“扬名立万”的壮举。虽说盘古团队的几位主要成员在行业里成名已久，可盘古越狱工具发布后，他们还是感觉到越狱给他们带来的变化。“之前参加技术交流活动，都是被称为‘××安全公司专家’，如今都是被叫作‘盘古越狱团队核心成员’，行业知名度和地位都变得更高了。”徐昊说。在一次国际会议上，苹果的技术专家就半开玩笑地对他们说“你们再发布越狱工具不要选择周末，不然我们还得加班”。

越狱带来名气的同时，也带来更多利益上的机会。在发布越狱工具后，盘古团队的成员也萌生出了创业的念头。因为越狱带来的影响，他们也获得了一些大公司和投资方的青睐。不过，对越狱工具的研究和开发，在他们看来只是一种对技术的挑战，出于兴趣的成分更大，并不是用来赚钱的手段。

“如果我们把越狱作为盈利方式，那肯定就去做应用分发的渠道了，而不是像现在这样只做一个越狱工具。我们的主要业务方向还是移动安全。”韩争光说，在他看来，越狱对于如今他们的公司来说，主要意义有两个，一是打响对外的知名度，让更多人知道他们，相信他们的技术实力；二是通过对越狱的研究，对iOS系统和安全性进行研究和分析。

C 用户越狱热情消退

两年前，在苹果用户中，越狱用户的比例还是相当可观的，特别是中国的用户，因为支付习惯、使用习惯等原因，很多人还是喜欢把iPhone越狱后使用。不过，近一两年，越狱的苹果用户越来越少。

韩争光也承认这一点。他介绍，盘古第一个版本的越狱工具，用户使用其进行越狱的设备数量累计超过了一千万。特别是盘古第一个越狱工具针对的是iOS7最后的版本7.1.2，而iPhone4最后支持的系统就是7.1.2，iPhone4用户只能使用盘古的这个工具进行越狱，因此直到今天，这个版本的用户数据还在不断刷新中。但是，从iOS8系统的越狱工具开始，使用量就开始明显少于iOS7了。

韩争光认为，造成越狱用户数量明显减少的原因是用户的越狱硬需求在减小。以前用户越狱，一方面是为了获得更多免费的应用，另一方面是对手机进行更多个性化的设置，如使用更习惯的输入法、更改手机主题、使用可拦截骚扰电话短信的安全软件等。现在，苹果用户不用越狱也能装软件，苹果也开放了对第三方输入法的支持，这些都让用户对越狱的依赖性大大降低了。现在，还在追求越狱的用户，多数是为了更加自由和个性化地使用手机，这些用户多是很专业的玩家，占用户比例并不高。

D 越狱与安全不矛盾

近期让越狱再度成为热点的事件，是一个名为“KeyRaider”的恶意软件家族，这个恶意软件家族主要通过iOS越狱软件Cydia进行传播，攻击越狱版的iPhone，并盗取iPhone用户的个人信息。此外，还针对不同的设备识别码、安全证书以及密钥，向苹果用户推送通知及应用商店购买数据，同时还令部分受影响手机无法使用，直到用户支付赎金为止。目前，受入侵的用户涉及中国、法国、俄罗斯、日本和英国等17个国家，已有超过22.5万个iCloud账号登录信息被窃取，这成为苹果公司历史上规模最大的恶意软件侵害事件之一。

这一安全事件发生后，关于越狱带来不安全性的争议再度被热炒，有一些手机业内人士也对外呼吁，出于安全性考虑，用户应尽量减少对手机进行越狱，否则手机面临的安全风险会变得更高。

对于越狱与安全之间的矛盾，韩争光认为，这其实是两个概念。越狱本身是为了打破苹果的限制，让用户可以安装更多功能强大的插件，同时也降低了一些安全性，就跟Windows一样，用户很自由，但是如果用户不注意的话就很容易中病毒。另外，不越狱也不代表安全，不越狱也可以让这些恶意软件发生作用，但是门槛要高不少。他表示，对于普通用户来说，为了保证安全，使用越狱的iPhone应该像用Windows一样，不可信的应用程序不要乱装。（京华）