浙大学生在顶级黑客大赛上夺冠 十秒钟攻破谷歌智能手机

原来我们身边藏着这么牛的黑客团队:腾讯科恩实验室、浙大AAA战队

本报记者 张冰清 通讯员 周炜

日前,世界顶级黑客大赛Mobile Pwn2Own 2016在日本东京落幕。腾讯科恩实验室以45个积分和215000美元奖金摘得桂冠,获得了"The Master of Pwn"(破解大师)的称号。

这支冠军队伍的主力队员中,有两位来自浙江大学计算机学院——何淇丹是浙大毕业生,目前供职于腾讯科恩实验室;刘耕铭是一名大四学生,主攻信息安全方向。

夺冠消息公布后,浙大cc98论坛出现了一个长达10页的帖子,学弟学妹们对这两个"黑客"大牛膜拜不已。

腾讯科恩实验室队员在比赛现场。

Pwn2Own是世界著名的黑客大赛,由Trend Micro旗下的著名安全项目Zero Day Initiative举办。此次在东京举办的Mobile Pwn2Own重点关注移动操作系统、手机浏览器和手机应用APP的安全性问题。

比赛的目的,是希望参赛者通过某些此前未知的漏洞来侵入各种移动设备,然后将之汇报给相应的设备制造商,以便它们对这些漏洞进行修补和修复。这些做好事的"黑客"也被称为"白帽黑客"。

由于比赛关注点是移动端,所以参赛者瞄准的目标是智能手机。他们将以iPhone6S、Google Nexus 6P和Galaxy S7为硬件目标,完成获取手机内部敏感信息、给手机安装恶意应用程序、固件及破解三个攻击项目。

腾讯科恩实验室第一个拿下的是Google Nexus 6P。他们成功在Nexus 6P安装了恶意应用软件,这为他们赢得102500美元奖金和29个积分。

随后,团队又在iPhone 6S安装了恶意应用软件。但它没能扛得住大家修手机最常用的一招——重启。所以,这只算半个成功,有60000美元奖金,但没有积分。

最后一项,他们再次攻击iPhone 6S,导致手机照片泄露。这样,腾讯科恩实验室最终以45个积分和215000美元奖金的成绩,成为本次比赛的"The Master of Pwn"。

比赛中,有一个数据被外人津津乐道。团队在远程攻破Nexus 6P时,仅仅花了十秒钟的时间。这听起来简直是不可完成的任务。

但其实,攻击代码是赛前早已经准备好的,上场就是操作一下。有人把它比喻成,你先在家写好PPT,然后到现场演讲。胜负取决于你PPT的质量,而不是花多少秒去演讲PPT。

腾讯科恩实验室成立于2016年1月,其成员主要来自于大名鼎鼎的安全研究团队Keen Team。

实验室官网上的一组数据能说明他们有多牛。

据不完全统计,自成立到2016年5月,科恩一共发现主流操作系统、浏览器、应用软件高危漏洞152枚。成员连续4年参加Pwn2Own并获得8个单项冠军。

正在浙大读大四的刘耕铭,当年以丽水市庆元县第一名考入杭州外国语学校,随后进入浙大。在浙大,他加入了一个重要的神秘组织——浙大AAA战队。

AAA是Azure Assassin Alliance的缩写,中文意思是蓝色刺客联盟。何淇丹毕业前,也是AAA战队的成员。

别看着名字挺中二,这个联盟可是聚集了整个浙大最厉害的"黑客"们。团员共有十几人,不全是计算机学院的学生,有些来自数学、生物、电子等专业,全是信息安全的爱好者。

为了保证团员的质量,AAA战队专门设置了一定的准入门槛。他们在网站上放了题目,只有做对一道题,才能获取战队的联系方式,加入组织。

昨天记者联系刘耕铭同学,他的手机依然未通,老师说他还在东京未回杭。

浙大计算机学院白洪欢老师平时和刘耕铭交往密切,他说,刘耕铭可以算得上是AAA战队的灵魂人物。

AAA战队经常南征北战,参加各种信息安全类的比赛。很多比赛要求选手在规定的几十个小时内完成指定任务,由于刘耕铭能力突出,承担了重要的任务,所以常常要熬夜打比赛。

在白洪欢看来,刘耕铭的性格特别适合当一个黑客。他有个性,有耐心,对热爱的事情非常执着。所以还没毕业,他就已经被腾讯科恩实验室挑中,成为其中一员。

师兄何淇丹的经历就更丰富了,除了跟随科恩团队参加国际顶尖赛事,他还于8月份受邀在顶级安全会议BlackHat USA和DEFCON上发表演讲。他把那次拉斯维加斯之行记录在《白帽赌城演讲记》一文里,称两场演讲"解锁了两项人生成就"。

国际微创外科大会西湖峰会,彭淑牖领衔的课题引起关注

如何把肝养大了再手术,"彭家军"们绞尽脑汁

本报讯 日前,由浙江大学医学院附属邵逸夫医院、浙江省医学会主办的国际微创外科大会西湖峰会,在杭州举行,大会顾问、国际著名外科学家彭淑牖教授在主题报告中介绍,把肝养大了再切,是这几年彭教授和他的学生们在努力探索和创新的课题。

把肝养大了再切,是一位德国医生2007年的偶然发现。当时有一位高位肝门胆管癌晚期患者,胆管堵塞,黄胆指数很高,为了减轻患者痛苦,延长患者生命,医生将患者的肝切开,将胆管与肠相接,进行胆汁导流,顺便将对侧的门静脉扎牢,让血液不再流入病变的右肝,以促使病变的右肝萎缩。他所采取的办法,是"临终关怀"式,没想到奇迹出现了,一周后,未病变的余肝迅速增大,使原本无望进行的手术又可以进行了。但是德国医生的两次手术,因为切口大,出血多,对病人伤害较大,病人恢复起来比较慢。

著名外科学家、浙江大学医学院附属邵逸夫医院院长蔡秀军是彭教授的学生,为解决以上种种不足,他和彭教授探讨后,决定用一根"绳子"解决——用一根有弹力的绳子,绕肝脏一周,进行捆扎,阻断了左右肝脏之间的交通血流。有点像手被毒蛇咬到后,为阻止毒素快速扩散,会在伤臂上方扎一根绳子一样。被称为"蔡氏绕肝止血带法"。

著名外科学家、浙江省人民医院肝胆胰外科和微创外科主任洪德飞也是彭教授的学生,他通过微波消融的方法,把肝脏左右交通的毛细血管连同肝脏予以封塞,再通过介入方法,把栓塞剂送进门静脉,也达到了阻止血液流通的目的。

"彭家军"虽然取得了不错的养肝效果,但他们并没有停止探索。彭教授介绍,他们现在可以将栓塞剂送到主血管并通过主血管渗入毛细血管,完全彻底对"敌占区"进行封锁。这实际上是一次手术分两个步骤做,第一步是介入法,对病人几乎不构成影响。而且大大节省了养肝时间,一般养两周,病人就可以进行手术了。

目前,通过这种养肝方法的12例巨型肝肿瘤,余肝全部短期内显著增大,取得成功。

本报记者 薛建国