

王琦:让更多黑客戴上“白帽子”

从微软高管到“创客”

作为暮晨(KEEN)云计算科技有限公司创始人,王琦在安全圈早已鼎鼎有名,人称“大牛蛙”。创业之前,他就曾是微软中国安全响应中心技术负责人,建立了微软在美国总部以外的第一个安全响应中心。但王琦并没有满足,2011年,凭着一腔热血,王琦做了个大胆的决定:创业。对他影响最大的一位素不相识的老前辈:史蒂夫·沃兹。

“他是一个典型的黑客,邋里邋遢,但对电子技术狂热,话少,逆向思维多,不讲究个人卫生,也没什么朋友。”在正常社会里,这类人是不会有社会地位的,甚至不会有丈母娘。但是1972年,沃兹自制了“蓝匣子”,第一次实现了盗打美国电话,十几年后,他和另一个史蒂夫,也就是乔布斯共同成立了苹果公司。

“这就是土壤的力量。”王琦说,沃兹在安全土壤健康的美国和乔布斯成立了苹果公司,如果缺少这样的土壤,这样的天才很可能就走偏成为黑帽子。“我觉得我身边就有很优秀的中国年轻人,但好像还没有土壤让他们被发现、发光发热,我决定培育最正义、最强悍的中国黑客土壤。”带着让黑客正面改变世界的美好愿望,带着几个和沃兹一般木讷、不修边幅,却痴迷技术的哥们,31岁的他建立了KEEN TEAM。“这在IT届里属于大龄创业。”王琦笑道。

在浦东一个几平方米的民居里,王琦定下了一个从来没有被证明可以成功的目标:发现这个世界上最难以发现的最危险漏洞,做到比黑客还要黑,但我们不做坏事,我们要把发现的漏洞报告给厂商修复,让互联网变得更安全。王琦说,黑客分“黑帽子”和“白帽子”,他们这种就叫“白帽子”。

走别人没走过的路

创业之初的两年,生活异常艰难。“勇于承认自身有问题的企业并不多。特别是在国内,很多企业并没有太多安全的意识,对于我们行为的目的性也表示怀疑。”所以,即使辛苦开发出高含金量的安全产品,最终还是陷入低接受度的窘境。

在狭小的出租房里王琦睡了2年沙发,每晚只能睡4个小时。一个年轻同事,拼了几个月哭着对他说:如果你让我考一个证书,我觉得有信心,因为起码有人证明是可实现的,你给我们定了一个从来没有被证明过会成功的目标,我怎么办?

要摆脱困境,王琦找到的又是一条别的中国人没有走过的路——参加世界最顶级安全赛事Pwn2Own,“规格相当于黑客界的奥斯卡、普利策评选,此前从来没有亚洲人参加”。

2013年,KEEN TEAM在东京机场走下飞机,王琦收到了这样一条提醒短信:“你们看清楚比赛规则了吗?”发信人是来参赛的法国队负责人,这个战队过去十年多次夺冠。王琦没有理会,只回复了一个笑脸。但他的内心独白是:“我们吃了两年多上海葱油拌面和小杨生煎来做基础研究和突破,你以为呢?”

一天之后,在比赛现场,KEEN TEAM通过此前从未被发现的漏洞,60秒内从一台全新iPhone上偷出了刚拍的照片。亚洲第一个世界冠军就这样诞生了。

“我们不做别人做不好的,只做别人做不到的!”

尽管光芒背后的窘迫只有王琦知道,“没有银行存款证明,比赛前我们甚至办不了日本签证。”还好一个政府朋友最终为他们做了担保,王琦借钱买了飞机票,才赶上了这班通往世界冠军的飞机。

本报记者 王文佳

在团市委和市档案馆日前主办的“上海青年创新梦想分享会”上,一位身穿黑色连帽衫、牛仔褲的帅小伙格外引人注目。他没有像其他讲演者一样穿着衬衫、西裤,而是用着装让人一眼就记住了他的身份:“黑客”。不过,一上台他就迫不及待地给自己的头衔作了个补充说明——“我这黑可不是黑车、黑心棉的黑,是黑猫警长的‘黑’,我们叫‘白帽子黑客’。”



KEEN 早期团队

“白帽子”也有中国梦

此前,KEEN TEAM 首席科学家吴石就收获了《福布斯》这样的评价:“发现的安全漏洞是整个苹果公司发现漏洞的两倍还多。”王琦说,他清楚,他们要厚积薄发了。

接下来两年的Pwn2Own赛场上,KEEN TEAM 接连夺冠,连续3年5个冠军。去年,在温哥华,他们打出了“KEEN China Team China Dream”(KEEN,中国队,中国梦)的横幅,法国人也竖起了大拇指。

做到攻击的极致,是为了证明有能力保卫我们的网络安全。王琦说,KEEN TEAM

让整个世界看到了中国信息安全的力量,“别因为中国人爱好和平不攻击你们,就来挑衅我们。有我们KEEN在,你敢来吗?”

后来,他们加入了号称全球黑客顶级天团的“Google Project Zero”,做到了更多亚洲人从来没有做到的。现在世界上每一台智能设备,无论是苹果手机、安卓手机甚至PC,每一个上面都有KEEN TEAM 数十到上百个的研究成果。喝着啤酒吃着葱油拌面的时候,王琦经常和队友们说:“瞧,我们保护了全人类。”

别人在炒股他在写代码

成功的背后是常人难以想象的付出。前两届三夺Pwn2Own 冠军的主攻手陈良,在准备去年的Pwn2Own 比赛时,得了肺炎,还坚持每天十几个小时攻坚克难。

今年,凭借30秒攻破Flash,不到60秒攻破PDF 阅读器的傲人成绩,KEEN TEAM 成员Peter 和陆吉辉又夺下Pwn2Own 的2个冠军。

然而比赛后,来不及兴奋和游玩,两位冠军把剩下几天在温哥华的日子都用来睡觉了。几个月来,他们每天工作十五六个小时,甚至春节都没有休息。“前面亏得实在太多了,一天可以连续睡十几个小时。”

有同学说王琦是投机分子,他回驳:

“你们在买房的时候,我在写代码;你们泡妞的时候,我在写代码;你们炒股的时候,我在写代码;你们生了孩子,我还在写代码。”

更可怕的是,这样艰辛的付出,时常还没有任何回报。他们把漏洞反馈给厂商,只是偶尔能拿到酬金,大多时候厂商只是表示感谢。可是用更低端的技术做出盗号木马出售,却可以轻松月入百万。不少好苗子不堪清贫,走上了“黑帽子”的道路。

创业初期,王琦挖人时也只能说:“虽然看不到蛋糕,但你会揉面,他会生火,我们可以先做个馒头出来养活自己,这样至少大家都不会走(做黑帽子)。”

用黑客技术保护世界

但王琦并没有忘记他创业的初衷。“中国很多默默无闻的‘白帽子’缺少的只是土壤。”光是KEEN TEAM,土壤面积还不够。去年,他又发起主办了全球第一个智能安全嘉年华GeekPwn。

通过已经关机的手机自动拍照,监听现场声音;无需木马或钓鱼,让打到别人账户的钱在途中悄无声息转到黑客账户……很多籍籍无名的民间黑客以其偏执的关注点,发现了智能生活中的安全漏洞。按照规则,在现场成功破解系统的选手不仅可以得到奖金,还能拿走被黑掉的设备。“我希望给更多的有才华、热爱技术的年轻人树立正能量

的榜样,让他们看到什么是顶级的安全技术,不要走到邪路上。”

GeekPwn 上,最令人叹服的还是KEEN TEAM 表演的远程控制特斯拉。前行突然变成倒车,甚至熄火。团队为了找到漏洞,特意买了一辆特斯拉,然后和来自车企北京的V2S 团队一起工作了100天才实现了技术突破。

“当时特斯拉发表了声明谴责我们。但是在我们发给他们特斯拉漏洞报告以后,特斯拉总部安全负责人特意飞抵上海,专门给我们送来了四枚限量版代表最高荣誉的安全勋章。”王琦说,那是中国人第一次登上特斯拉



创新 我们在行动

王琦参加的“上海青年创新梦想分享会”主题为“创新,我们在行动”,是团市委和市档案馆共同举办的纪念五四运动96周年主题团日活动,活动当天还有三位来自不同领域的青少年创新代表。

“创新就要不惧失败,因为我们从不相信任何一个伟大的创新是灵光闪现得来的,创新的过程其实就是试错的过程。”

说这话的是中国商用飞机有限责任公司“梦幻工作室”负责人张驰。他所组建的团队曾创造了9个人连续工作40个小时,喝掉22罐红牛的纪录。他们所制造的“灵雀”缩比飞行验证机,经计算能降低传统客机9%的油耗,一旦应用推广,可以为整个航空产业每年降低碳排放42万吨,相当于路上少跑15万辆车。

“只要换一个角度看待学习,创新其实就在我们身边,假如我们能换一个角度看世界,创新就能随时迸发出来。”

上海外国语大学附属外国语学校学生李欣雨今年只有17岁,为了做一台金属记忆发电机,她曾经绕了一万多圈的线圈,手上磨出了老茧。如今她所制作的发电机,能将一碗热水里的热能转化成电能,获得了国家专利。

另一位分享者是上海简米网络科技有限公司(Ping++)创始人金亦冶。年仅29岁的他已经成功入选了中国福布斯30岁以下创业者榜单。将“中国制造”转变为“中国创造”一直是他的信念,4年的留美经历助推了他的梦想,如今他创造了属于自己的创新产品Ping++,这种全新的移动支付接入工具,是连接移动应用和支付通道之间的技术桥梁,他说——

“仅仅是Made in China是远远不够获得别人的尊重的,我们需要的是Created in China。”

安全名人堂。

前阵子,著名的《经济学人》杂志这样评价“白帽子黑客”:“那些极客可能在学校不好过,他们被运动员精英嘲笑,在聚会中被忽视。但现在任何正儿八经的组织想要蓬勃发展都离不开他们。”

王琦则这样评价自己的团队:“一群书呆子,在小黑屋里持续忍耐着寂寞,也终会让世人看到自己的无比潜力、无比热爱、无比坚持、无比努力和无比团结”,王琦说,黑客的每一项创新,都会是一把双刃剑。但他希望通过这一代中国信息安全从业年轻人的努力,让黑客技术的创新变成保护世界的力量。“我们在团队里经常说,安全需要激情,更需要对正义的坚守,未来我们就真的有可能去正面改变世界。”