

黑客少年的“数据帝国”

高中生窃取1亿条公民信息

来到看守所的第27天,刘佳乐(化名)收到了父亲寄来的两三套换洗衣物。当看到包裹里还夹着一件父亲的上衣时,他立刻失声痛哭。

这个刚过18岁生日的年轻人告诉记者,作为中学数学教师的父亲一向小心谨慎,这次准备衣服时,肯定是瞒着母亲,不想让她伤心,才把自己的衣服凑了进来。

刘佳乐是最近网络上刷屏的新闻“高中生窃取1亿条公民信息获利2万”中的当事人。日前,记者在无锡第二看守所与他进行了独家对话。

成就

刘佳乐的老家广东信宜市。“小时候没人陪我玩,经常一个人玩电脑。”刘佳乐的父母是双职工,工作都比较忙。父亲是高中数学教师,很早就教他数学。小学时,刘佳乐就学会了初中的许多知识。不过,性格偏内向的他似乎不太会和同学交往。刘佳乐不愿回忆那段充斥着打架以及师生相处不太融洽的初中三年时光,也不喜欢大多数男孩子喜欢的篮球、足球等活动,唯一让他“稀罕”的是,每晚10点下晚自习,回家后便进入那个可以躲避现实中孤单、还能带来“成就感”的网络世界。

刘佳乐的数学和英语很好,经常逛一些国内外技术帖论坛。高一时,他通过看一些视频和例子,自学掌握了编写软件程序。

一开始,他热衷寻找各商业网站的漏洞。刘佳乐算了一下,仅2018年一年,他就给腾讯、百度、阿里等知名网站找了约有八九个漏洞,通过各大公司的网络应急响应中心进行反馈。

在这些商业网站筑就的“铜墙铁壁”中找到漏洞,而这又是众多毕业于“985”名校的技术大拿没有发现的漏洞,这让刘佳乐感觉“日子特别充实”。尽管每次奖金只有200元,最多的一次奖励是1000元,但他觉得这份成就感与利益无关。

帝国

14岁的刘佳乐在网络论坛里闲逛时,有网友提到了“暗网”。后来,他尝试翻墙,登录暗网网址后,看到了一个不一样的世界。

“卖什么的都有,恐怖色情视频,各种详细的个人信息。”其中,个人信息除名字、地区、生日外,还包括名下房产、银行卡、个人户籍和全家户籍,以及手机信息和手机定位等。

后来,当熟悉的网友找到他,请他帮忙在“暗网”上买户籍信息时,他抱着“体验过程”的想法,帮这个朋友买过几次个人信息。“价格从十几元到上百元不等。”在他看来,买卖双方都是自愿的,自己只是帮忙提供了联系方式的中介。

2017年下半年,刘佳乐在论坛



资料图片

贴吧中看到查询网络用户个人信息的方法,对此产生了兴趣。不出一个月,他便成功编写出一款软件,可通过内置接口,将其对接到百度贴吧,通过撞库的方式,用不同的手机号码不断登录,获取手机号码对应的账户信息。2018年6月,刘佳乐又编写出了一款能够批量获取信息的软件。

他将这款软件分了很多手机号段,在境外租用十几台服务器,搜集的数据会自动导入到租用的网络数据库里。短短不到1个月的时间,他的数据库里便存储了上亿条个人信息。

在网络黑市里,刘佳乐掌握的个人信息库是众多网络黑灰产急需的。有人希望找到在百度贴吧的发帖人,于是提供账号,刘佳乐通过信息库搜索,就能找到账号对应的手机号码。

刘佳乐在境内网络建立起微信群、QQ群,在境外使用“Telegram”等聊天工具,自助编写“信息查询”机器人,将数据库以包月查询的形式向他人兜售,并且通过连接VPN翻墙到境外,以比特币为交易货币贩卖数据库长达两个月,共计获利约两万元。

权力

有人知道刘佳乐有这个数据库后,想花高价购买,但他想:“我怎么知道他买了之后会做什么,但我觉得自己做事是有底线的,骗人害人的事情不会做。”

可是,他不清楚自己非法获取上亿条账号和手机号的行为,已严重触犯了法律。

2018年9月,无锡市惠山区警方接到网友举报,有人在论坛、贴吧等平台售卖公民个人信息以及盗窃信息所用的黑客软件,惠山区警方第一时间立案侦查,跨省抓捕了江西籍26岁犯罪嫌疑人付强(化名)。

付强的网名叫“清风”,曾向网友“i春秋”购买了一款黑客软件用于非法获取公民个人信息,非法获利上千元。“i春秋”就是刘佳乐的

网名。

今年4月,无锡惠山警方前往广东对刘佳乐进行调查。由于他即将迎来高考,在侦查环节公安机关对他采取取保候审措施并准许其参加高考。

但刘佳乐高考落榜了。“自从警察找上门后,情绪经常崩溃”。今年8月,无锡惠山区人民检察院对刘佳乐批准逮捕。

无锡惠山区人民检察院承办检察官徐静超指出,该案数据总量大,非法获取公民个人信息精准,危害公民个人信息安全甚至是国家数据信息安全,现已上诉至法院。不过犯罪嫌疑人犯罪时尚未成年,即使现在是成年人,仍属于未成年人犯罪,应当依法从轻或减轻处罚。

“黑客是一群为技术着迷的人,但也有他们自己的基本理念。”广东警官学院公共管理系主任、珠三角公共安全研究所所长吴兴民,曾花3年时间对黑客进行了专门研究。

在与多名黑客深度访谈后,吴兴民发现黑客的年龄一般都不大,性格偏内向,有时跟同龄人相比显得格格不入,但对于自己的技术极有信心。

吴兴民分析,如今的一些黑客“往往分不清打破技术壁垒和打破信息保护之间的不同,可能严重触犯了法律还不自知”。部分黑客违法犯罪不完全是因为法律意识淡薄。“黑客当然知道非法窃取他人信息是触犯法律,但他所拥有的技术就是他手里掌握的权力。常言说,失去监督的权力必然导致腐败。当这种技术可以给他一种强烈的力量感时,他有可能会觉得我可以,那为什么不呢?”

“当青少年没有完善的知识理论体系支撑时,在接受过多复杂纷乱信息的情况下,他们很容易在选择时陷入迷茫,甚至作出错误的判断。”吴兴民认为,在他们是非观念、辨别能力都还不是很强的情况下,有必要引导,甚至加以一定限制。

《中国青年报》10月29日报道

干涸近300年
“哈拉奇”水域重现

据《北京青年报》10月29日报道 波光粼粼的湖面,茂盛的芦苇丛,在水面上起起落落的白鹭和野鸭——如此美景很难让人联想到这是一片身处沙漠之中的水域,而更难想象的是,作为“倒流河”疏勒河的终端湖,这片名叫“哈拉奇”的水域此前已经干涸了近300年。

近日,甘肃敦煌“哈拉奇”水域在干涸消失近300年后重新出现的消息引发网友关注。

10月28日,记者从敦煌西湖国家级自然保护区管理局了解到,该湖泊是“倒流河”疏勒河的终端湖,之所以能在干涸近300年后重新出现,得益于疏勒河及党河河道恢复与归束工程的完工投用。实际上,从2017年开始“哈拉奇”就开始逐渐恢复,今年雨水充足,所以水面也比较大,达到了5平方公里。“哈拉奇”的重获生机,对于阻止库姆塔格沙漠的东侵,保护敦煌绿洲和敦煌文化具有深远的意义。

28日上午,敦煌西湖国家级自然保护区管理局科研科科长孙志成告诉记者,“哈拉奇”位于敦煌西湖国家级自然保护区西端和库姆塔格沙漠东缘交汇的地方,是疏勒河的尾间。

据史料记载,这里曾经的湿地面积约1000平方公里以上,水域面积约200平方公里,“但是随着环境的变迁,疏勒河发生了部分的退缩、断流,‘哈拉奇’在清代的时候也干涸了,渐渐被东进的库姆塔格沙漠包围,附近的人都叫这里‘北枯沟’”。

如今,“北枯沟”又泛起了水波,而这粼粼波光得益于长期的规划和治理。2011年6月,经国务院批复,总投资47.22亿元的《敦煌水资源合理利用与生态保护综合规划》启动实施。在该规划支持下,酒泉及敦煌地区相继实施灌区节水改造、河道恢复与归束、党河流域水资源监测调度、月牙泉恢复补水、水土保持生态建设等工程。

有了水源,“哈拉奇”附近的野生动植物也开始焕发了生机。孙志成告诉记者,据史料记载“哈拉奇”之前一直都是野骆驼的栖息地,但是由于水源的枯竭,野骆驼几近绝迹。而当“哈拉奇”重新泛起碧波后,野骆驼们再次出现在“哈拉奇”。如今的“哈拉奇”水域,生长着茂盛的芦苇,研究人员不完全统计到的鸟类就有20种左右。

孙志成表示,“哈拉奇”的地理位置就在库姆塔格沙漠的东缘,恢复有水后,水域和植被都对阻止沙漠化有着重要的价值。