“我的12306账户竟有14个陌生人!”

■潘女士3年未用的账户被盗用

■黄牛盯上“沉寂账户”,几元就能买一个

阅读提示

“太可怕了,3年前注册了一个12306网站(中国铁路客户服务中心)的账户,现在却发现账户被人盗用,常用联系人里绝大部分都是不认识的人。”上海市民潘女士非常震惊,自己3年没用的账户,竟然被黄牛(票贩子)拿去刷票了,而且向铁路部门反映,也找不到原因。

随着春运大幕开启,一些不常购票的市民发现他们“沉寂已久”的12306账户信息中出现了一个甚至多个素不相识的人。为什么黄牛会盯上这些“沉寂”的账户,这些账户又通过怎样的渠道落入黄牛手中?

12306网站上线以来,黄牛和官方的博弈就一直在进行,各种身份信息被盗用的情况不断出现。业内人士分析,黄牛确实有可能盗用“沉寂账户”,这些账户因为长时间不用,即使是被不法分子盗用了也很难被发现。

陌生人信息无法删除

1月6日,之前在国外读书的潘女士尝试在12306网站购票。“账户3年前就注册了,但一直没用过。这次原本打算和妈妈周末一起乘高铁去苏州散散心。”但登录12306网站进入个人账户后,潘女士惊讶地发现,她的常用联系人列表中,除了自己之外,居然还有14个素不相识的人,“我看了看名单,年龄最大的60多岁了,最小的才刚刚成年,而且身份证号码也是来自全国各地的。”

有朋友提醒潘女士,她的账户应该是被黄牛盗用了,让她赶紧再查查账户信息。潘女士随后再次点开了她的账户,发现这些陌生人信息是2016年12月14日通过12306官网审核,批量加入到她的账号之中,“我查询后发现,正好就是春运火车票预售前夕,看来是黄牛拿着我的账号,购买春运火车票赚钱。”

潘女士表示,原本想把12306的账户密码更改一下继续购票就算了,反正也没查到有什么损失,但更改密码后,自己却无法删除常用联系人列表中那些陌生人的信息。无奈之下,她只能来到上海火车站的票务中心寻求帮助。“我去了人工售票处的服务台,工作人员表示根据系统规定,要在2017年6月12日以后才可以删除,现在的办法只有注销原账户再重新注册一个新账户。”

12306称未泄露用户信息

潘女士随后致电12306客服热线,想了解自己的账户到底是如何被黄牛盗用的。

“12306客服坚称,我的账户及相关信息不可能是12306网站泄露的,一定是在其他第三方网站泄露的,还说我这种案例并不少见,具体什么原因,客服也说不上来。”潘女士说,她的12306账户是在2014年注册申请的,因为当时还在国外念书,注册之后就没有用其购买过火车票,“不过我在其他的论坛和应用上的确用过12306的账户名及密码。”

记者咨询了12306官方客服,据客服介绍,像潘女士这样账户被盗甚至密码被篡改的状况,可以通过验证的电子邮件或手机重置密码。但是根据常用联系人的身份信息核验状态,标注状态为“已通过”“请报验”“预通过”的常用联系人在180天内不能删除,至于为什么要有180天的限制时间,该客服声称这是规定,但具体原因并不知情。

此外,该客服还表示,一个账户内最多可以添加15名常用联系人,“所以,像潘女士这样联系人列表已满的状况,确实比较麻烦,如果急着购票,只能到铁路车站的服务窗口或相关代售点购票。”

新闻延伸:

“沉寂账户”更易被“撞库攻击”,被盗后难被发现

业内人士分析,黄牛确实有可能盗用了他人的“沉寂账户”,这些账户因为长时间不用,即使是被不法分子盗用了也很难被发现。

12306网站上线以来,黄牛和官方的博弈就一直在进行。曾不断出现各种身份信息被抢注的情况,为防止黄牛利用他人身份信息恶性抢票,2015年6月中旬,12306网站发布公告,称将网站注册用户名下的“已通过”“请报验”“预通过”常用联系人(乘车人)累计上限由原来的100人调整为30人。随后又不断调整,现在上限调整为15人。“这样的话,黄牛如果想要多购票,就需要更多的账户信息和成本。直接盗取‘沉寂账户’,是最为直接的手段了。”业内人士说。

而12306也出现过安全问题。据了解,早在2014年底的春运抢票高峰期间,乌云漏洞平台就发布了高危害等级漏洞报告,报告显示,12306用户资料疑似大量泄露,甚至有明文形式的密码,以及身份证、邮箱等敏感信息。随即又有大量12306用户数据在互联网上传播售卖,包括用户账号、明文密码、身份证、邮箱等。已知公开传播的数据库涉及用户数约14万。

GeekPwn(极棒)实验室网络安全专家宋宇昊表示,像潘女士这样的“沉寂账户”被盗存在多种可能的原因:“比如说她在其他平台上使用的账号密码和在12306上使用的账号密码是同一个,那么别人就可以通过‘撞库攻击’的方法来获得她的12306账号密码。另外一个可能就是病毒,如果她在使用12306账户时,终端里面有恶意程序,她的账户信息也有可能会泄露。”

针对“撞库攻击”,目前国外的一些互联网企业已经有了相应的措施:通过技术手段对异常登录现象进行持续监控,对“撞库攻击”行为进行分析辨别,从而防止用户信息泄露。宋宇昊认为,像潘女士这样长时间不使用的12306账户更容易被“撞库攻击”,因为这些账户用的还是老的用户名和密码,没有经过修改,所以比起新账户或者活跃账户来说,它们在数据库里的重合率一般会更高一些,也就是说“撞库”的成功率会更高一些。不仅如此,这些“沉寂账户”基本都处于荒废状态,被找回的可能性也更小,可以保证黄牛更长时间、更稳定地使用。

有人专门出售账户,几块钱一个,要多少有多少

那么,黄牛到底是从哪里得到了潘女士的账户信息呢?

记者从部分黄牛那里了解到,他们所使用的12306账户除了有用自己身份信息注册的,也有一些是买来的。“5元一个买的,到现在还没出现过什么问题,已经用这些账户抢了不少票。”一名黄牛说。

随后,该黄牛还向记者推荐了几名专门出售12306账户的卖家。记者联系了其中的多名卖家,并表示想要购买12306账户,一名卖家说:“10元一个,要多少有多少。”另外一名卖家则把价格压得更低,但是要求要大批量购入,“2.5元一个,如果一次性购买100个,单价还可以再减掉0.5元。”

而当记者询问这些账户都是从哪里来的时,该卖家支支吾吾地回答:“我们的账户都是定制的,用几年都不会有问题。多的不解释,你自己想吧!”

账户还可以定制?“定制”到底是什么意思?该卖家并没有向记者解释这些问题,他只是保证这些账户不是抢注的,不用担心被找回。而像他这样号称能替别人“定制”账户的卖家,记者在网上还找到了不少。

宋宇昊告诉记者,安全是一个博弈对抗的过程,即使平台采取了很多措施,攻击者也有可能找到另外的方法来达到他们的目的。所以,任何平台都不可能没有安全漏洞,12306也不例外。不过在安全性方面,第三方平台比官方平台泄露信息的风险更大。“不管是从技术上还是从责任意识上来讲,第三方平台肯定都没有官方平台那样强,特别是一些小平台,在保障用户信息安全方面的投入肯定不会太多。”

(胡迎)