细思极恐！验血结果竟可轻易泄露……

《财经调查》曝光信息黑洞！

消费者在享受数字化时代带来的便利时,个人信息也不可避免地留存在了不同的服务平台上。每年盗取、滥用个人敏感信息的犯罪事件并不罕见,到底是谁在背后收集这些数据？这些数据又是怎么流出的?《财经调查》起底非法贩卖个人信息黑色产业链条。

日常停车竟能暴露公民敏感信息?!

这几年,市场上一种被称为“智慧停车”的新业态应运而生。它依托于物联网和大数据技术,覆盖各种类型的停车场,大大提升了居民出行的便利度。停车信息包括了车辆进入和离开某个地点的完整闭环,属于《个人信息保护法》规定的敏感个人信息中的行踪轨迹信息。智慧停车,很智慧,但是够安全吗？

《财经调查》对北京两个采用了“智慧停车”系统的停车场进行了技术检测。驾驶员将车驶入停车场,远在几公里外的专业技术人员,输入车辆的车牌号后,无需身份验证,轻而易举地就获得了车辆所在停车场、车辆入场时间等敏感信息。

在记者采用同样的方式测试第三个“智慧”停车场时,并没有直接显示出车辆的敏感信息,但经过技术专家的辨别,发现这个停车场只是没有在前台显示信息,后台实际上有了应答,返回的数据包里同样有着车辆敏感信息。专家告诉记者,这样的招数只能让消费者不能直接看到。但是,不法分子依然能轻易获取这些敏感的个人信息。

2017年《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》中规定:

非法获取、出售行踪轨迹信息五十条以上,即可入刑;五百条以上即为情节特别严重。

犯罪分子利用停车信息追踪社会车辆 违法安装跟踪器 对公民人身安全造成巨大隐患！

犯罪分子的聊天群里每天在滚动发布着各种车辆的实时停车信息,包括了车牌号、停车场具体地址、进场时间等等。

被犯罪分子“盯上”的车辆一旦进入停车场,显示在群里,几十分钟之内,就会被装上GPS无线定位器,强磁吸附且超长待机。

2023年,安徽砀山网警破获了一起非法获取计算机信息系统数据,侵犯公民个人信息的案件。犯罪分子的突破口,就是全国数千个智慧停车服务系统中的数据接口漏洞。据安徽省砀山县公安局网安大队侦查中队中队长余天龙介绍,全国主流的这些停车场系统,它们都有一个问题是任何一个人都可以为任何一个车辆去缴费。通过批量地在这些停车场系统里面进行模拟缴费,获取返回值进行解析,就可以确定某一台车是不是在某一个停车场系统里面。

据警方介绍,不法分子通过互联网接单,帮助客户寻找指定车辆。在实施犯罪的过程中,正是利用了停车小程序数据接口上的漏洞。之后,短则几分钟,贴手就会找到指定车辆,贴上GPS追踪器。据警方资料显示,贴手每贴一辆车能获利800元到1000元。那些位于上游的入侵停车场数据系统的不法分子更是获利不菲。

这起案件中,安徽砀山网警成功打掉了这个非法获取售卖停车数据的犯罪团伙,抓获犯罪嫌疑人32名,查封远程服务器9台、关键脚本程序5套、车辆位置数据50余万条。

芦云律师向记者介绍,案件中犯罪分子的行为涉嫌非法侵入计算机信息系统,或者是非法获取计算机信息系统数据这样的罪名,那么同时也有可能涉嫌侵犯公民个人信息罪。

2024年10月,法院判决该案系列被告人犯侵犯公民个人信息罪,判决有期徒刑二年至四年不等。

点餐、办卡、订酒店……你的个人信息根本藏不住 就连医院验血的结果别人也能随意查看

眼下,骚扰电话和各类骚扰信息一直是困扰广大消费者的一个问题。最值得注意的是这些推销对消费者的选择,也异常精准。中国电子技术标准化研究院网安中心的何延哲表示,问题就出在API上,它也被称为应用程序接口,这其中与开放、传输数据相关的则被称为数据接口。

购买机票时,输入起点、终点的输入框就是一个接口。消费者进一步点击某个航班,此时这个网页链接,也是一个数据接口。消费者获得服务的过程就是一个个数据接口通过不断与后台进行数据交互来实现的。专家告诉记者,眼下消费市场上的网站和应用程序上,存在着海量的数据接口。仅一个简单的App应用,平均就拥有成百上千个数据接口,一个小型平台,就可能拥有上万个数据接口。恰恰是这些承载着海量数据流转和交互的数据接口正是不法分子眼中的薄弱环节,也逐步成为他们主要攻击的目标。

《财经调查》的记者会同网络安全技术专家,针对不同消费场景中数据接口的使用情况进行了一系列实时测试和深入调查。技术测试分为三步:

第一步:扫描接口

第二步:分析接口开放参数

第三步:检查身份鉴别和授权机制

测试场景一:咖啡茶饮店的手机点餐

测试结果:专家仅仅使用最基础的解码程序,就轻而易举地从小程序的数据接口返回的数据包中,获取了记者下单消费的完整且没有加密的后台数据。这家咖啡店的网络小程序数据接口授权不严密,导致任意人员能轻易获取该企业数据库中用户的个人信息,比如手机号。

测试场景二:运动健身购买月卡

测试结果:专家仅仅使用最基础的解码程序,就顺利通过了该小程序数据接口的用户身份校验,毫无阻拦地就拿到了完整且未加密的用户信息。这其中包括身高、体重、职业、生日等敏感信息。

测试场景三:生活服务-洗衣店

测试结果:这家企业的小程序接口存在一个非常明显的漏洞:当消费者查询的订单号为空的时候,该接口就会返回数据库中所有订单的信息,这几乎让程序平台里的整个用户信息都存在极大的泄露风险。敏感信息包括手机号、姓名和居住地址。

测试场景四:酒店订房

测试结果:这个小程序的接口虽然做了一定的加密措施,但是由于生成的订单号非常有规律,专业人员可以根据规律构造查询指令,也可以很轻易地查看到指定日期的所有订单信息。

测试场景五:医院医疗信息

测试结果:该医院的小程序也属于查询接口授权机制不完善。查询所有患者的化验报告应该要管理员权限才能访问,但是通过这个接口,用普通账号也能查询,医院的小程序在权限等级识别上根本就没有设置任何障碍。