接口随意调用、数据花钱可买……

为何有人总能“轻易”获取隐私信息

近年来,随着数据安全法、个人信息保护法等一系列法律法规相继出台实施,我国信息安全事业取得长足发展。但是,一些掌握大量用户数据的机构在网络安全防护中措施不足,导致用户数据被不法分子窃取。不法分子将获取的用户数据分门别类打上标签,再以诸如“婚恋报告”“风险报告”等形式对外出售,破坏网络安全生态。

相较于过去“打包贩卖”用户敏感数据的方式,当前网络黑市以买家实际需求为导向,以“生成报告”的形式出卖个人信息。为什么我们的个人隐私总能被不法分子“轻易”获取?记者就此展开调查。

1 网络安全形势仍不容乐观

“提供身份证号,可查指定人征信、户籍信息。”“婚姻状态可查,USDT(一种虚拟货币)、微信、支付宝均可支付。”刚刚加入某境外通信软件的聊天群,就有群成员迫不及待发来招徕私信。

在一名卖家发来的“个人信用报告”的预览版中,除姓名、性别、手机号等信息外,还细致记录了每个人的工作岗位、公积金和社保缴纳记录、借贷额度等高度隐私内容。“这些报告可用于精准电话营销。”该卖家说。

来自奇安信的数据显示,2024年全年境内政企机构共发生个人信息泄露风险事件112起,涉及个人信息数据266.9亿条,尽管这一数据较2023年减少54.5%,但是海量的数据泄露问题反映出政企机构的网络安全形势仍不容乐观。

个人信息数据的频繁泄露,不仅严重侵害公民隐私,带来网络诈骗风险,还可能对国家安全带来威胁。“大量个人信息数据的汇聚、关联和再组织,可以形成精准的人物画像,还可以将人与人之间的关系网络描绘出来。这就让不法分子更容易锁定目标群体、找到突破口。”奇安信安全专家裴智勇说。

此外,一些黑灰产还利用大数据和人工智能等技术,抓取和匹配个人的隐私图片和视频。有不法分子声称“只要一张照片就能查询你的另一半有没有外遇”,以此牟取不法利益。“通过网络爬虫技术获取一些网站上的公开视频和图片资料,再进行人脸识别比对,这实际上侵害了当事人的隐私权。”中国科学技术大学网络空间安全学院教授左晓栋说,不法分子有可能利用泄露的个人信息和肖像进行恶意匹配,由此形成的所谓“婚恋报告”也触及法律红线。

2 不法分子利用“数据接口”等渠道窃取数据

在落实网络安全主体责任过程中,过去常见的“拖库”渐渐少了,取而代之的是利用数据接口等渠道进行“蚂蚁搬家”式的个人信息窃取。

姓名、身份证号、手机号、常用地址……在中国电子技术标准化研究院网安中心的一例安全测评中,测试人员发现有6万份订单数据有可能来自某平台的数据接口泄露。

所谓数据接口,就是机构传输、共享数据时输入和输出数据的对接口,也就是数据出入的“大门”。“如果把这扇门看住了,来来往往的数据就都能被调阅。”中国电子技术标准化研究院网安中心测评实验室副主任何延哲告诉记者,一些机构在设置数据接口时缺少身份认证、访问控制等安全措施,导致黑客能够随时“劫持”接口并获取实时数据。

在何延哲及其技术团队以往随机测试的数据接口中,存在安全问题的不在少数。“相较于‘陈年数据’,通过数据接口获取的实时数据更新,在黑灰产上售卖的价格也会更高。”何延哲说。

在某不法论坛网站中,有人开设了专门群组用以分享各类数据接口。通过其所分享的数据接口,不法分子可获取指定人员的社保信息、生育信息、车险购买信息等敏感数据。

各类机构在打造数字化平台时缺乏网络安全思维,部分敏感数据缺乏高等级保护,而通过数据接口窃取数据等不法操作并不需要多高的技术门槛。“有的平台存在安全问题的数据接口长期‘暴露’在外,掌握一些基础攻击手段的黑客就能通过不安全的数据接口直接获取平台最新用户数据。”何延哲说,把数据接口“保护起来”并非难事,不过由于缺乏对数据接口的安全风险监测,机构在大多数情况下难以意识到自己的数据接口可能已经被网络黑灰产恶意利用了。

此外,合作伙伴和机构“内鬼”也是数据泄露的重要渠道之一。2020年7月,某快递企业员工私自向不法分子有偿出借工作账号,致使超过40万条公民个人信息泄露。“各类机构在获取用户数据后,往往会和合作伙伴共享,以获取数据的最大利用价值。”裴智勇说,在数据共享过程中,部分合作伙伴未完全遵守网络安全协议,进而导致用户数据泄露。同时,一些网络黑灰产和机构“内鬼”相勾结,倒卖用户数据。“在互联网知识共享平台上发生的数据泄露事件中,这两种方式占比超过一半”。

一些机构在源头端过度收集用户数据,导致敏感数据过度集中。国内知名个人信息保护专家、清华大学法学院教授劳东燕认为,部分信息收集机构以包括“提升服务体验”在内的各种理由要求用户或消费者“一揽子授权”,是造成数据泄露的根本原因。2021年,个人信息保护法正式实施,其中明确规定“收集个人信息,应当限于实现处理目的的最小范围,不得过度收集个人信息”。“这个‘最小范围’的解释权目前看仍然在收集数据的机构,而不是在用户或者消费者手上”。

3 彻底斩断伸向个人隐私的黑手

随着法律法规的日益完善,近年来我国打击涉公民个人信息犯罪工作成效显著,一批以兜售公民个人信息牟利的不法分子受到法律严惩。

2024年,四川成都警方侦破侵犯公民个人信息、非法控制计算机信息系统等网络犯罪案件1201起,依法采取刑事强制措施1116人;山西长治警方在2024年辗转多地,成功打掉一个特大侵犯公民个人信息及掩饰、隐瞒犯罪所得犯罪团伙,抓获犯罪嫌疑人10名,扣押涉案资金500余万元;同年,安徽合肥警方侦破特大侵犯公民个人信息案,抓获犯罪嫌疑人11名,查获涉案金额120余万元,保护了公民个人信息百万余条……

提升机构网络安全防护能力,构筑数据安全防火墙。裴智勇等专家建议,政企机构应进一步完善网络安全的制度建设,确保责任到岗、到人。在出现网络安全事件后,及时向国家有关部门报告,尽可能减少因数据泄露给用户和社会带来的损失。

减少前端数据收集,从源头降低数据泄露风险。“比如点外卖,有手机号、有地址,确保外卖能送到,就不应该获取其他信息。”劳东燕建议,根据个人信息保护法等法律法规要求,数据收集应遵循“最小必要原则”,有关部门可根据数据实际使用场景,明确相应的数据收集范围,为“最小必要”设定标准。

强化隐私保护意识,对过度收集、滥用数据等行为说“不”。何延哲建议,机构和网络平台等应从用户和消费者角度出发,更加重视个人信息保护,决不能为了蝇头小利出让个人信息权益。对明显存在过度收集用户信息和潜在的侵犯公民个人信息的违法犯罪线索,网络用户可及时向互联网管理部门和公安部门举报。 来源:新华网