“李女士，您所购买的小区最近正在交房，您家装修公司选好了吗？”

“您好，我们银行最近有装修贷产品做活动，利率很优惠，您有需求吗？”

“您家房本快下来了，您有考虑卖房吗？”

……

自从李女士买了房，她的生活就像被跟踪一般，装修公司、银行、中介的各种推销电话每天各种轰炸。大多数人都有过和李女士类似的经历。究其原因，正是信息泄露让我们无形中变身“透明人”。

记者调查发现，从上游个人信息被非法获取、到中游数据在各种黑市交易平台被转手和出售、再到下游各种隐私数据被用于诈骗、勒索，个人信息泄露背后已然形成了一条完整的黑灰产业链，滋生着巨大的非法获利空间，严重威胁着个人、企业甚至国家安全。

“黑客”难躲“内鬼”频现泄露渠道“无孔不入”

个人信息究竟是怎么被泄露的呢？在诸多的信息泄露案背后，不乏“黑客”和“内鬼”的身影。

奇安信数据安全子公司负责人姚磊对《经济参考报》记者表示，黑客可利用在线系统漏洞拖库、利用社工库或者弱口令等撞库，此前出现的QQ群、163邮箱、天涯、万豪、华住等数据泄露事件，均和黑客攻击有关。“部分黑客也可利用移动终端操作系统漏洞、公共WIFI网络漏洞、终端旧设备数据删除不完全等，攻击终端企业数据，造成个人隐私数据泄露。”他说。

除了“黑客”难躲，“内鬼”也频现。北京市朝阳区人民检察院检察官助理陈莹璐告诉记者，就犯罪主体来看，单位内部员工或离职人员，利用职务或工作便利，非法获取或贩卖公民个人信息案件时有发生。她举例称，被告人方某在某网络公司任职期间，非法复制获取公司系统服务器中的公民个人信息10万余条，并出售获利。后该公司在排查中发现该员工账户使用异常，下载大量包含用户信息姓名、身份证、电话等公民个人信息，故报案。据方某供述，其在公司利用爬虫软件获取了数十万条公民个人信息，经筛选、删除敏感信息后，留下姓名、手机号，存入移动硬盘，后从移动硬盘中找信息卖出。

值得注意的是，现实生活中，一些信息泄露途径十分隐秘，无形之中我们就已然变身为“透明人”。

无处不在的摄像头已经成为获取个人生物信息的重要渠道。业内专家表示，个人生物特征数据具有唯一性和不可再生性，一旦被窃取，无法追回和变更，将对个人隐私保护带来极大的、不可逆的风险。人脸信息明文传输，每次刷脸解锁均会反复上传，很容易发生泄露，且识别可靠性差，使用翻拍照片即可轻易破解。

另外，电信运营商、短信通道、第三方平台等也已经成为近些年来不可忽视的泄露渠道。“用户访问客户网站/App的记录被运营商泄露、用户数据被第三方工具或平台泄露、企业下发给用户的短信被第三方短信通道泄露等，都时有发生。”业务情报安全企业永安在线产品经理邹洪志表示。

他对记者说，永安在线最近协助某证券公司发现了一条数据资产泄露渠道，该证券公司的数据并不存在直接泄露，但与其客户相关的资产数据在暗网或Telegram群被持续出售。

“黑灰产人员可以获取到访问过该证券公司官网的用户手机号码，有些还可以获取到用户姓名、运营商、省份、城市等相关数据。”他说，运营商能拿到用户的上网流量，可以通过用户手机号-设备-流量（访问网址）对应上，然后通过内鬼或者某个接口泄露到第三方“大数据营”公司之类去卖。邹洪志说，一些数据卖家明确表示只支持某一家电信运营商，也从侧面证明这些卖家是与运营商合作的。

专家指出，实名制的深入实施让个人信息常与设备、账号绑定，进一步放大了信息泄露的风险。360集团手机安全研究员俞奎表示，某种程度上，身份信息、支付等校验的是设备、账号，而不是本人，即谁掌握了他人的信息，即可实现身份冒充。如果平台遭受黑客攻击，或有内鬼泄露，那么用户交付出去的个人信息用途并不可控。

层层加密无法追踪暗网等平台成信息买卖“大本营”

在一些隐秘的角落，有关个人信息的非法交易“无时无刻”都在进行。“传统的泄露数据大都在QQ、微信以及地下论坛等交易。然而，随着国家对网络空间治理和打击力度的加大，越来越多的泄露数据在‘暗网’这种匿名、匿踪的黑市交易平台出售。”姚磊说。

陈莹璐表示，“暗网”被称为“隐藏的服务器”，其域名数量达到表层网络的400-500倍，运营环节具有全方位的程序保护和复杂的登录方式。犯罪分子借助暗网匿名、无法追踪等特点，并使用赌博平台、虚拟货币进行交易，层层加密为游走在“暗网”的犯罪分子提供了技术上的“保护色”。

记者从业内人士了解到，“暗网”提供各种“查档”、“定位”服务，“查档”指

查询公民的住宿、出行、户籍、车辆、犯罪记录、学籍等各种隐私信息。“定位”则是指可查询各种App位置信息。

记者通过有关渠道获取到一张“暗网”发布帖子的截图。发帖人称，“全国幼儿园至高中、职校以及相关教育机构教师数据，一手出新74800条，数据内容非常详细”。该截图显示，这些个人信息包括教师姓名、手机、邮箱、毕业院校、任教学科、任教学校、教龄等共16个维度的数据。记者随机挑选了两位教师的信息，经电话求证，信息均为其个人真实信息。该帖子发布于2021年1月9日，截至3月25日，该定价为99美元的数据包已有4单成交。

实际上，“暗网“已成个人信息买卖“大本营”。姚磊介绍，2020年以来，在“暗网”出售的部分重要数据包括：2021年1月，印度支付公司Juspay超1亿用户的借记卡、信用卡信息在“暗网”上销售；2020年8月，黑客在“暗网”出售美国1.86亿选民数据；2020年4月，超50万Zoom用户账户在暗网出售；2020年3月，5.38亿条微博用户信息在“暗网”出售，包括用户ID、微博数、粉丝数、关注数、地理位置、手机号等。

滋生诈骗、勒索信息泄露成“精准”犯罪“助推器”

陈莹璐表示，随着经济的快速发展和信息网络的广泛普及，公民个人信息的经济价值日益凸显，导致侵犯公民个人信息的犯罪屡打不绝，且成为了滋生电信网络诈骗、绑架、敲诈勒索等下游犯罪的源头，社会危害日益突出并多发，已经史无前例地成为影响个人甚至国家安全的重要问题。

中国司法大数据研究院社会治理研究中心主任李俊慧对记者表示，通常而言，买卖个人信息，从购买一方来看，一定有特殊用途，不论是进行业务推广，或是实施诈骗犯罪等。因此，个人信息不当泄露或非法买卖一定会给下游犯罪提供帮助。他举例称，在一起个人信息非法买卖案件中，不法分子成立了一家信息咨询公司，通过QQ购买股民电话号码，进行虚假股票营销牟利。公安机关在该公司现场查获股民电话号码约12万条。

“囿于违法所得金额的限制，对于涉公民个人信息犯罪违法所得的追缴与罚金的财产性处罚，却远不足以填平公民个人信息泄露造成的次生危害。”北京市第三中级人民法院副院长辛尚民表示。实践中，行为人利用非法获取的公民个人信息实施的犯罪主要有诈骗罪，比如向不特定对象发送“中奖”信息；合同诈骗罪，比如利用某些理财软件漏洞骗取财物；敲诈勒索罪，比如利用酒店开房记录等住宿信息对相关人员进行勒索。

值得注意的是，数据泄露及贩卖正从单纯的交易数据演变到交易数据访问权限。网

络犯罪分子已将注意力从个人信息转移到了更庞大的数据库——工业企业数据库。黑客利用漏洞窃取企业核心数据，并通过勒索软件加密企业相关设备。随后，这些数据将被进行“双重勒索”，如果不支付赎金不予解锁，同时会泄露被盗数据。尤其是在制造业智能化程度大幅提高的背景下，智能化工控系统（ICS）已成为黑客攻击的目标。

闪捷信息安全战略研究中心发布的《2020年度数据泄漏态势分析报告》显示，2020年受勒索攻击而造成数据泄露事件占所有数据安全事件的15%，成为常态化的数据安全事件。

据此前江苏省南通市警方通报，在“净网 2020”行动中，成功侦破一起由公安部督办的特大制作、使用勒索病毒破坏计算机信息系统从而实施网络敲诈勒索的案件，非法获利的比特币折合人民币500余万元。

华顺信安的创始人、CEO赵武表示，黑客已单纯索取数据行为转向勒索，通过勒索病毒对企业关键信息库加密的方式索要高额虚拟货币，可以短时间获得暴利，又因虚拟货币的匿名性而保护身份不暴露。“企业不同于个人，企业不支付赎金，黑客便泄露企业敏感数据、窃取其知识产权。极端情况下，最严重的攻击可能对制造商工厂和设备造成永久性损失，对企业影响难以估量。”赵武说。

(来源:经济参考报)