裸聊敲诈勒索案件中

技术犯罪人员的发现和证据链的完善

□钱浩 王海容

杀猪盘、虚假投资理财、冒充领导熟人诈骗、冒充客服诈骗等电信网络诈骗犯罪的高发，已经引起社会各界对于电诈犯罪打击治理的关注与重视。而与电信网络诈骗犯罪类似，随着信息网络的快速发展，越来越多的传统犯罪加快向网上蔓延变异，例如裸聊敲诈勒索犯罪。犯罪分子借助信息网络寻找作案目标，通过敲诈、恐吓等手段实现非法牟利，严重破坏经济社会生活秩序和互联网环境秩序，甚至已经可以定义为“涉网黑恶势力”。

裸聊敲诈的被害人作为特定的被害人群体，又有可能造成一些独有的社会矛盾和不安定因素。在日常办理案件的过程中，侦查人员发现裸聊敲诈团伙的首选对象通常为单身男性。嫌疑人通过交友软件筛选特定的被害人后往往得手概率更高，当这类人群的隐私被用作敲诈后会对其身心造成极大的伤害甚至导致一些不可逆的不安定的因素。所以打击和宣传裸聊敲诈势必会成为今后打击网络犯罪的重中之重。

在裸聊敲诈勒索案件的侦办中，侦查人员往往以受害人的资金流向、作案手机号和社交账号作为突破口，并对查明的犯罪嫌疑人开展工作，而对“技术犯罪人员”的打击少之又少。

“技术犯罪人员”作为犯罪环节中的重要组成部分，往往一人服务多个团队，量产软件供其使用。所谓“技术犯罪人员”，涵义相当广泛：包括裸聊App的开发人员、服务器及数据库运维人员人员等。他们往往不再是暧昧地“提供技术帮助”，而是直接利用自己的专业技术参与到犯罪活动中，成为犯罪链条的关键一环。本文将这些“技术犯罪人员”作为研究对象，讨论如何在案件侦查过程中突出其身份、固定犯罪证据以及完善案件证据链。

技术犯罪人员的角色作用

当前阶段主流的裸聊敲诈犯罪全程依托网络进行，有较为完整的产业链，根据所处环节及具体分工，裸聊敲诈犯罪人员主要可以分为以下几类：一是前期引流人员，通常在各类手机交友软件中以交友等名义引导受害人添加指定的微信、QQ、易信、blued等聊天软件账号，这些聊天软件账号的背后实际是由实施敲诈勒索人员在登陆使用；二是技术支持人员，主要是指为裸聊敲诈App的开发、服务器及数据库运维等提供技术服务的人员；三是敲诈勒索人员，即核心犯罪团伙，他们诱导受害人裸聊，以录屏的方式取得裸聊视频，并引导受害人安装运行裸聊敲诈App，此App通常只是一个显示无法安装的程序，通常以“×××控制器”“×××直播室”等名称伪装，以此获取通讯录、实时定位、相册等隐私数据，之后将裸聊视频和隐私数据发送给受害人以勒索财物；四是资金转移人员，负责为核心犯罪团伙转移资金，进行“洗钱”以及支付各种网络要素的费用。

上述第二类技术支持人员负责开发裸聊敲诈专用的App，通常仅具备获取受害人定位、通讯录的功能，传输隐私数据成功后，App即闪退或卡死，对于受害人来说没有使用价值，目前亦有App加入了读写相册等权限等功能，能获取更多受害人隐私信息。技术犯罪人员从服务器运营商处租用服务器，并在服务器中部署源码，搭建网站，通过打包公司的打包软件进行打包，实现App的封装以及分发。当受害人安装、运行了App后，其隐私数据即被抓取。技术犯罪人员可在后台访问数据库，调取受害人隐私数据并提供给实施敲诈勒索的犯罪人员，对于犯罪的成功实施具有直接推动作用，是犯罪活动的一个重要环节。

由于用于犯罪的主网站域名容易被封停、服务器需要到期续费或更换等客观原因，上述开发、运维的技术犯罪人员需要经常更换域名解析、更新网站后台地址，因此通常需要与实施敲诈勒索的核心犯罪团伙之间通过各种方式进行长期密切联系，针对技术犯罪人员的深入侦查研判有利于固定犯罪证据、循线追踪核心裸聊敲诈犯罪团伙。侦查人员可以通过向第三方公司调取证据等方式来获得购买人、租用人、支付人的主体信息，以此为切入口，开展侦查。

资料照片

技术犯罪人员的发现

技术犯罪人员的发现主要依靠对下载链接、Android应用程序包（即apk文件）的静态分析和对App本身的动态分析来提供线索。

1、链接分析

在被害人获取涉案软件时，往往会通过扫描二维码或通过点击链接下载的方式，这些二维码及链接背后可能是第三方的分发下载平台，也有可能是技术人员自建的分发下载平台。第三方平台可以通过正常法律手段获取证据，而自建平台就要通过分析其域名及服务器的信息再做进一步分析。但也往往是这些自建平台的分析，能够获取到技术人员开发的多种软件信息，对后期犯罪事实的认定起到关键作用。

2、静态分析

与一些诈骗App相比，裸聊敲诈App由于实际功能少，因此不需要接入过多的第三方SDK（软件开发工具包），留下的痕迹较少，静态分析环节产生的有效线索主要是对App进行打包的公司及对应注册账号、打包ID和回传地址等。

3、动态分析

动态分析环节产生的有效线索主要是回传地址。对App动态分析的常用工具，有Charles、Fiddler等抓包工具，配合使用Android模拟器或手机真机，进行动态抓包。在获取服务器IP、打包ID等要素后，需要向对应的服务器运营商、打包公司进行调证。除了常规的实名认证信息、支付记录、登录日志，不同的公司还会提供业务相关证据，例如云端打包记录、App前二十用户使用记录、服务器镜像等，对于进一步研判、完善证据链都有重要作用。

技术犯罪人员证据的固定与证据链的完善

1、涉案要素的获取

在一些常见的裸聊敲诈案件中，嫌疑人往往会通过QQ发送一个软件安装包供被害人下载直接安装，但随着QQ自检功能的不断加强，这些安装包在发送过程中即被提示不安全而不能进行传送。开发人员便将软件获取方式改为二维码截图或链接下载，下载地址也是犯罪要素链路上的关键一环，开发人员在完成开发后会将软件上传至三方分发平台或自建分发平台供人下载，绕过了QQ的安全提示，即便浏览器有时会提醒链接可能存在威胁，嫌疑人也会编造理由称因双方的对话内容敏感才遭提醒。被害人扫码或点击后便获取到了涉案软件，这里要区分的是市面上主流的两种操作系统（ios,android)的要素获取方式并不相同，ios系统获取安装包更为复杂，但操作原理与android系统相仿，所以在日常分析中以获取android系统的apk文件为主要依据。

2、前期分析过程中的证据固定

在静态分析过程中，除了获取常规的包名、MD5值、SDK特征码等线索，还需要对裸聊敲诈App获取定位、读写通讯录、相册等敏感权限进行取证固定，这些权限是获取受害人隐私数据的基础，也是App功能性的主要依据。

动态分析过程本身也能反映出App的动态运行特征，实践中发现，在进行动态分析的不同模拟器之间、模拟器与真机之间，对于同一App的适应性以及运行情况都有差别，因此在动态分析时，应当尽量使用不同的载体多次尝试，尽量完整反映、取证固定App的相关信息。此外，可以通过对分析过程全程录屏等方式，记录App动态运行特征，也为证明取证合法合规提供依据。

3、通过服务器镜像分析完善案件证据链

向服务器运营商调证取回的证据材料中包含涉案服务器的镜像，而对服务器镜像进行分析，是完善证据链的关键所在。与此同时，一些服务器的管理面板成为技术人员日常管理多台服务器的重要工具，例如堡塔面板就是技术犯罪人员搭建网站或运行维护服务器常用的控制面板（即通过可视化界面来管理云服务器），一般记录有搭载在该服务器上的域名以及账号的历史管理记录等，如能找到与前期侦查发现相吻合的域名，则可以证实该服务器与裸聊敲诈犯罪的关联性。在此基础上，通过对源码文件进行进一步分析，可以找到更多线索，例如网站后台的账号密码，通过账号密码登录后台，在数据库中可以找到裸聊敲诈案件受害人的隐私信息，使得该服务器与案件的关联性更加明确，整个证据链形成闭环。

通过VMware等软件可以完成绝大多数案件的服务器重建，以此可以设法找到网站后台地址及密码，进入后台。网站后台记录有裸聊敲诈受害人的手机通讯录、短信等隐私数据，是重要的犯罪证据。尽管服务器本身各不相同，但是由于同一时期流通贩卖的源码大同小异，开发、运维人员将源码部署到服务器，修改后台地址，重置账号密码，并使用HBuilder X等编辑器软件进行打包，即可生成了一个新的裸聊敲诈App，因此，同一时期裸聊敲诈的网站后台差别并不大。

4、通过第三方公司调取数据完成拓线

在大量案件中，会碰到使用打包公司等第三方服务公司。向这些公司调取打包账号的注册、付费、打包等记录，在侦破案件过程中可以对案件进行串并及拓线，为侦破类似案件提供依据，形成更广泛的打击。

结论

裸聊敲诈勒索案件中针对技术犯罪人员的侦查过程，从受害人端采集的裸聊敲诈App出发，通过分析找到数据回传地址，研判出服务器IP及运营商后，通过调证取得服务器镜像，在服务器镜像内发现了回传地址域名和受害人隐私数据，结合对服务器运营商、打包公司进行调证，明确开发、运维等技术犯罪人员身份，初步形成了一个证据链的“闭环”，为后续侦查提供了方向。结合对涉案资金流向、作案手机号和社交账号开展工作，以及后续对抓获嫌疑人的审讯、随身电子设备的勘查，进一步完善案件证据链，并将侦查工作逐步向幕后核心犯罪团伙推进。

利用App和信息网络开展的裸聊敲诈犯罪，只是涉网新型犯罪一个缩影。技术犯罪人员是“路走偏”的网络从业者，在利益的趋势下“走捷径赚大钱”，这类人员一般不会开发单一的裸聊敲诈软件，他们会通过网络购买各类诈骗软件源码后部署出售来谋取暴利。裸聊敲诈App相比较于贷款诈骗、虚假投资理财诈骗、虚假博彩等众多犯罪App，是较为简单、基础的一种，这些网站、App背后的技术原理相通，勘查方法也大体相似，裸聊敲诈App的勘查、证据固定技巧对于其他类型的犯罪App、网站的网络流勘查也有一定的借鉴意义。

（作者单位：江苏省苏州市常熟市公安局）

工商银行上海分行金融助力医疗系统疫情防控

3月以来，上海正经历着一场来势汹汹的“倒春寒”。工行上海分行迅速行动，通过金融支持、物资捐赠等方式，全力支持上海医疗机构疫情抗击工作的顺利开展，多措并举保障医疗体系金融服务需求。

为保障医疗机构在疫情时期的金融需求，工商银行上海分行主动了解辖内医疗机构了解金融需求，帮助解决上门收款、代发工资等各类业务，并在全辖范围内增设应急网点，做到快速响应、高效服务，保证了各医疗机构的紧急支付需求。4月14日，工行上海卢湾支行得知黄浦区卫健委需要紧急支付一笔疫情防控费用，统筹用于辖内28家基层医疗卫生机构开展新冠肺炎疫情防控的各类经费支出。卢湾支行立即启动应急服务保障预案，前后用时不到30分钟，便完成了对28家基层医疗卫生机构的专项资金准确、及时、安全拨付到位。

为驰援疫情，工行上海分行各级机构深入防控疫情的第一线，开展了物资的捐赠及慰问工作，黄浦支行第一时间向新建的方舱医院捐赠水果，以保障医务工作者及患者的三餐营养；包括徐汇支行、静安支行在内的多家分支机构主动联系辖内医院、区卫健委、区疾控、医学院等医疗系统单位，向其捐赠生活、抗疫物资，以保证医疗工作者内部工作时的正常起居，保障抗疫工作的稳步进行。据统计，在此次驰援抗疫的过程中，上海分行辖内各分支机构已累计向医疗系统驰援捐赠物资上千万元。此外，还有一批工行员工也积极参与到抗疫志愿服务中，黄浦支行的顾佳颖和杜志康前往仁济医院，作为核酸采集的志愿者，在自助机具服务区为市民提供帮助。