上图：与黑账号不同，黑软件实施违法行为最关键的角色就是黑客。

用自动化程序工具，完成整个流程。“目前我自己手里握有几百万张手机 SIM 卡，可为上万个平台、网站提供服务。”

与黑账号不同，黑软件实施违法行为最关键的角色就是黑客，以黑产活跃的游戏领域为例，黑客通常会对知名 App 做二次打包，将木马程序插入安装包，挂在各大网站供免费下载，只要用户下载了软件，手机自然就会被黑客操纵，进行暗扣话费、刷流量、盗号圈钱等非法行为，甚至复制仿冒银行等大型 App，引诱用户提供账号密码等敏感信息，进而利用钓鱼网站窃取受害人资产。

黑客也瞄准了 App 的广告收益，一般来讲，App 用了广告联盟的插件计算流量进行广告分成。“一个浏览几毛钱或几元钱，一天上下好几百万元的广告收益。在交易过程中，黑客会做成木马小游戏嵌入其中，污染软件并将广告收益账号篡改为黑客自己的账号，从中劫持绝大部分广告收益分成。”张雪松说。

除了黑账号、黑软件的肆意猖獗，恶意平台也是互联网黑灰产业链链接上下游的运转核心。据调查，各类资源、工具以及犯罪手段、经验，都需要通过“恶意平台”来交流、运转。目前，恶意平台分为三类，恶意网站、恶意论坛和恶意群组。以空包交易平台为例，卖家为提高店铺信誉，联合刷手（刷单平台）进行虚假交易时，产生大量非真实的快递订单；恶意论坛则将黑灰产技术、信息卖家与买家聚集在一起，用于存放着大量黑灰产更新资源，成为黑灰产滋生各种犯罪行为的温床。

有案例报道，一个论坛管理员在一个月内通过论坛发布付费教程，非法牟利了近 10 万元。张雪松提醒，只要脱离几个大牌的 App 或平台，原则上都应该谨慎。“像趣步涉嫌金融诈骗被立案调查，根本上是拉人头传销，包装得很前卫，做得也很隐晦，还会和网贷、理财、选股、棋牌等非法网站平台合作，一茬茬地割韭菜。”

据阿里安全归零实验室统计，2018 年活跃的专业技术黑灰产平台多达数百个。服务专业化使得犯罪技术更加平民化，低廉价格也使得黑灰产技术犯罪的成本逐步降低。

找漏洞：技术解决不了全部问题

张雪松接触过各行各业的黑产案例，至今拥有 10 年网络安全研究经验。他认为，彻底打破网络黑产链条，应该从上游“个人信息如何获取”层面上着手解决。而处在互联网技术极速发展的今天，如何铲除“黑账号”生长的土壤，恰恰是掐断源头的关键。

“个人信息失守的核心在于漏洞，黑客的技术正是嫁接在漏洞之上，利用漏洞实现更多权限谋取暴利。”张雪松说，漏洞银行的初衷就是通过众包模式为企业客户寻找漏洞，帮助其用低成本建立起 SRC（安全响应）中心。

简言之，就是在社区里聚集一群“白帽子”，让这些“白帽子”解决企业提出的安全检测需求。“根据安全漏洞大小和数量，对白帽展开定价悬赏，金额从几千元到十余万元不等。”张雪松说，截至目前，平台已有近千家企业和 3 万余名白帽入驻“漏洞银行”。

当企业遭遇黑客攻击时，这群白帽将从“管理漏洞、逻辑漏洞、技术漏洞、机制漏洞、防护漏洞”几个方面找问题。以管理漏洞为例，最经典的攻击方式就是客服攻击，因为有很多网站提供了客服人工的