间谍入侵

数千部手机被恶意软件感染 涉及多国政府工作人员

制图:童玮(豆包AI)

据央视

记者从国家安全部了解到，当前，智能终端已经深深融入生活、学习、工作的各个场景，在带来惊喜和便利的同时，也暴露出一系列风险隐患，如不注意防范，甚至可能危害国家安全。

■链接

“间谍”潜入手机的几种方式

初级方式

诱骗点击陌生链接。

一些木马程序被关联在网站发布的跳转链接，或者伪装在二维码图片中，一旦点击扫描，手机便会“中招”。

进阶方式

伪装成应用软件。

一些木马程序被伪装成手机应用，打着“破解”“翻墙”等噱头诱导大家下载，下载安装这类应用同时也为“间谍”打开方便之门。

高级方式

利用软硬件漏洞。

利用手机硬件设备、操作系统和应用软件的技术漏洞，在目标毫无感知的情况下获取手机控制权，进而实现对目标无声无息的监控。

揭秘终端窃密暗网

今年3月25日，中国网络安全产业联盟(CCIA)发布报告，深度揭示了美国情报机构针对全球移动智能终端实施大规模攻击和长时间的监听窃密活动。智能终端遭非法入侵事件屡有发生，警醒我们当前智能设备已经成为国家级网络战的攻击目标，在这看不见硝烟的战场上，智能设备的安全防线正面临前所未有的挑战。

利用SIM卡软件漏洞“隔空接管”手机。SIM卡是移动通信系统的用户身份识别模块，用于存储用户身份信息与加密密钥。此前曝光的案例显示，攻击者通过发送特殊短信激活SIM卡内置的浏览器，即可远程获取用户位置、窃取短信甚至拨打电话。这种攻击无需物理接触设备，仅利用SIM卡软件的未修复漏洞，便能控制全球超10亿部手机。

利用系统层“零点击”攻击“静默激活”设备。智能终端系统的封闭性曾是安全的代名词。然而，有案例显示，某国公司故意向该国间谍情报机关提供后门，用于在该公司智能手机上植入间谍软件，且已发现数千部感染了恶意软件的智能手机，相关手机使用者包括多国政府工作人员。攻击者可以利用某智能手机操作系统内置的即时通信服务漏洞，无须用户交互即可直接控制手机。

利用手机软件“投毒”“暗度陈仓”窃密。手机预置软件可能暗藏窃密通道。此前曝光的案例显示，某运营商通过在手机中预置网络诊断软件，违规收集用户短信、通话记录等敏感数据。2015年境外媒体披露，“五眼联盟”国家情报部门联合发起“怒角”计划，通过劫持个别有代表性的应用商店的下载链接，将用户下载或更新的应用程序“调包”为已植入间谍软件的应用，使数亿用户不知不觉成为数据泄露源头。

利用移动网络层“强制降级”窃密。移动运营商网络承载着关键信息交互的功能。攻击者通过劫持骨干网络、伪造基站信号、渗透运营商内网等手段，可以在信号“生成—传输—接收”链条中的每个环节植入窃密通道。攻击者将恶意代码注入4G/5G信号，配合伪基站集群强迫手机降级至2G网络，再利用未加密通信窃取敏感数据。

■提示

自觉规范上网行为 做好信息安全防护

日常使用手机过程中，防范潜入手机的“间谍”，不仅关系到个人信息和隐私安全，更事关国家安全。广大人民群众，特别是核心涉密岗位工作人员，要切实提高安全意识，自觉规范上网行为，做好信息安全防护。猎奇心理需杜绝。不使用来路不明的智能电子设备，不点击短信、电子邮件中的陌生链接，不扫描来历不明的二维码，不安装陌生应用软件，不随意连接公共Wi-Fi，不浏览非法网站，及时关闭不必要的共享、云服务功能，养成在官方应用市场下载应用软件的良好习惯。安全意识需提升。不使用手机存储、处理、传输、谈论国家秘密，不在手机上存储核心涉密人员的工作单位、职务、电话号码等敏感信息，不在涉密公务活动中开启和使用手机位置服务功能，不将手机带入保密要害部位、涉密会议和活动场所。防护措施需增强。及时更新手机操作系统和应用程序版本，修复已知安全漏洞，安装可靠安全软件，定期查杀病毒，警惕应用软件敏感和超范围权限请求，及时发现处理手机异常行为。

电视变成窃听器，卡车变杀人工具

美国斑斑劣迹黑料百出，国家计算机病毒应急处理中心和360公司早在2023年便联合发布了一份调查报告。报告揭秘了美国中央情报局(CIA)利用网络攻击他国的相关情况，披露部分发生在中国和其他国家的网络安全典型案件的具体过程，全面深入分析美国中央情报局的网络攻击窃密和相关现实危害活动，以及其对美国成为“黑客帝国”所作的贡献。

从披露的信息看，光是隶属于CIA下设的网络情报中心(CCI)的黑客就超过5000名，这还只是2016年的人员规模。

CIA还针对不同设备“量身打造”窃密工具。就拿家用电器来说，CIA的嵌入式设备分部(EDB)开发了一款名为“哭泣天使”的黑客程序，主要针对三星智能电视。感染这一黑客程序的电视会处于“假关机”状态，人们以为电视已经关闭，但其实它变成了一个窃听器，会记录房间内的对话并通过互联网发送到CIA的服务器。

除了窃听之外，很多黑客程序还被用来做更有针对性的破坏行动。比如，该部门试图侵入小汽车与卡车的控制系统，以便从事暗杀行动。

之所以能够如此精细化地研发各类工具，正是建立在前期无差别的入侵窃密工作之上。

CIA的移动设备分部(MDB)开发了多种针对智能手机的攻击“武器”，被感染的移动设备会向CIA发送用户的地理位置、音频和文本信息，以及在用户不知情的情况下，秘密激活手机的摄像头与麦克风。

根据报告披露，这些部门还研发了针对多款主流操作系统以及路由器的“后门”程序，也就是说，只要CIA愿意，它可以随时利用这些“后门”入侵相关设备。

据统计，到2016年底，CIA下的网络情报中心(CCI)就制造了1000多种黑客系统、木马、病毒和其他“武器化”恶意软件。

随着被披露的真相越来越多，我们也应该越来越警惕，不能让技术放任自流，把世界带向危险的边缘。

随着各国应对措施的提高，某些国家滥用技术而不愿承担责任的日子已经一去不复返了。再执迷不悟，只会不断把破坏规则和秩序的证据拱手展示给世人。

责编/李林惠 编辑/张恒春 版式/童玮 校对/杨进峰 王慧娟