噫

发布于 2016年7月12日 3 天前

作者：1024 链接：http://zhuanlan.zhihu.com/p/21558357 (http://zhuanlan.zhihu.com/p/21558357) 来源：知乎 

这几年安卓系统的普及速度可谓迅猛，一时间各式各样的设备都承载着安卓系统，手机、平板、机顶盒等都忠实地成为了安卓系统的用户。由于安卓系统在移动设备上的使用率最高，而移动设备上存储的数据往往涉及到个人隐私，如手机通讯录、短信内容、拍摄照片、阅读书目、保存文档等，有时更会涉及到经济利益，这诱惑着一些利益集团开始制作基于安卓系统的远程控制程序，即安卓系统木马。

首个安卓系统木马应属2010年出现的“Trojan-SMS.AndroidOS.FakePlayer.a”，这是一个以扣取用户手机话费为目的的盈利性安卓系统木马。随着需要的发展，单纯的盈利性木马已经不是重点，用户的隐私数据才是核心，尤其是具有用户行为监视性的木马最受关注。所谓“用户行为监视性的木马”就是指该类安卓木马能够监视用户的所在、所说、所做。

所在”即用户所处位置在哪里；“所说”即通话内容，聊天内容；“所做”即在操作什么程序，在干什么活动。

这一类的木马由于涉及到用户核心利益，往往经济价值较大，多用于私人侦探、商业窃密等领域，平时很难见到，更不要说了解其核心代码、实现机制。为此，本文将逐步向读者揭秘这些高级安卓木马的核心实现技术，帮助大家更好地了解这些木马实现技术，从而做好对个人隐私的保护，防范该类木马的入侵。本文旨在讨论技术，凡利用本文技术进行违法活动的作者与杂志概不负责。