Noticia en chino / chinese versión

智能手机恶意软件检测系统

马德里卡洛斯三世大学（卡三）的研究人员研发出一种可协助安全分析师保护市场以免用户受到恶意软件侵害的系统。该系统可分析海量手机应用软件以便找到这些恶意软件的源头和家族。

恶意软件（malware）是一种不怀好意的程序，目的是为了在用户不知情的情况下采取行动获得经济利益，如：偷窃用户信息或经济诈骗。“任何设备，无论是传统手机，还是现在的智能手机，甚至是家用洗衣机都可能有恶意软件的存在。”研究人员之一，卡三计算机学院的季耶莫·苏亚雷斯·德·丹吉尔解释道。

由于最近几年来智能手机的热销（比个人电脑问世以来的销售总和还多），恶意软件自然瞄准了这个平台，而且越来越层出不穷，越来越狡诈。“安全分析师和市场管理人员不堪重负，无法对每个应用程序进行彻底监控。”季耶莫·苏亚雷斯·德·丹吉尔说明，并表示恶意软件的发展已经成为一种巨大的产业并拥有整套代码重制体系。“这并不是从无中创造一个程序，而是在已有的程序中结合新的样本。”

卡三研究人员研发的这种系统被命名为 DENDROID，并由某工作室在科学期刊《专家系统及其应用》*Expert Systems with Applications* 上发表。文章阐述了该系统可帮助安全分析师分析海量应用并找到这些恶意软件的源头和家族。此外，如果不能直接对某恶意软件进行归类，也可从该应用的进化树中了解到恶意软件的祖先。“研究人员通常对于其他恶意软件的构成进行再利用，这正好可以构建其族谱。”季耶莫·苏亚雷斯·德·丹吉尔表示。该信息可帮助安全分析师对从未见过的恶意软件进行样本分析。

智能手机中安装的杀毒软件的运行原理是使用签名的监测引擎，从之前观测到恶意软件的特性从而确认其类型。“因此，其效率值得质疑。”季耶莫解释并总结道：“因为智能手机的资源比个人电脑更加有限。此外，恶意软件高频的变化使这些签名无法及时跟进。然而，这种新型系统可以帮助分析师保护市场，而且用户无需完全依赖智能手机的探测器。”

该项目隶属于在此领域对社会有特殊贡献的卡三信息技术安全保护小组（COSEC: www.seg.inf.uc3m.es）。具体而言，该小组近期刚启动一项 IoY（电脑和你 *Internet of You*）安全与隐私的国家级研究项目。

更多信息：

标题：《Dendroid：文本挖掘法对安卓系统恶意软件家族代码结构的分析与归类》
作者：G·苏亚雷斯·德·丹吉尔 G. Suarez-Tangil，J·E·塔比多 J.E. Tapiador，P·佩里斯-洛佩斯 P. Peris-Lopez，J·布拉斯科 J. Blasco
期刊：《专家系统及其应用》，爱思唯尔 Elsevier 出版社
卷 41:4（2014）1104-1117 页
DOI: 10.1016/j.eswa.2013.07.106