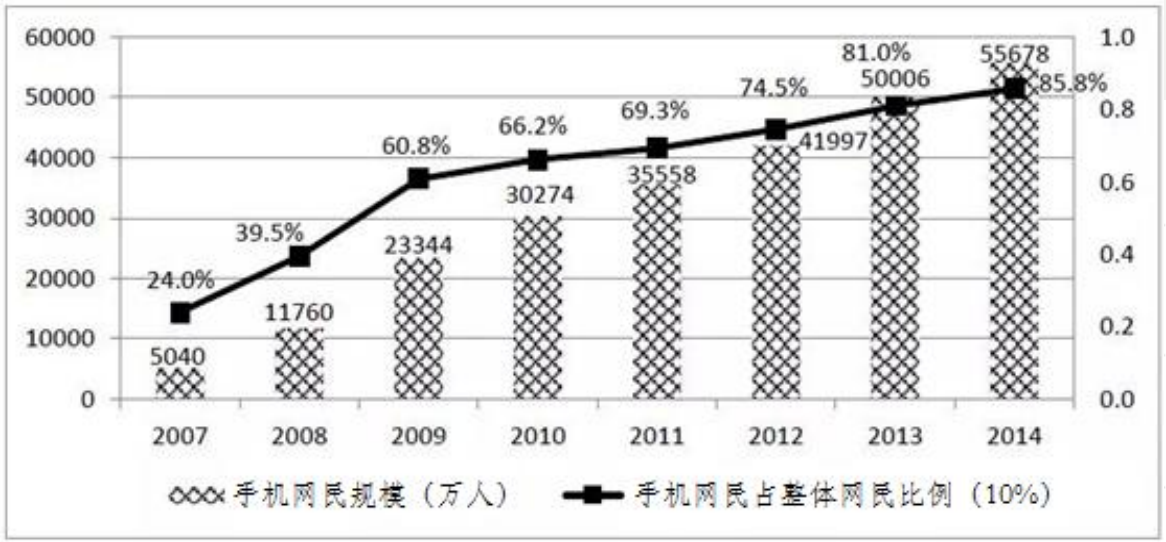
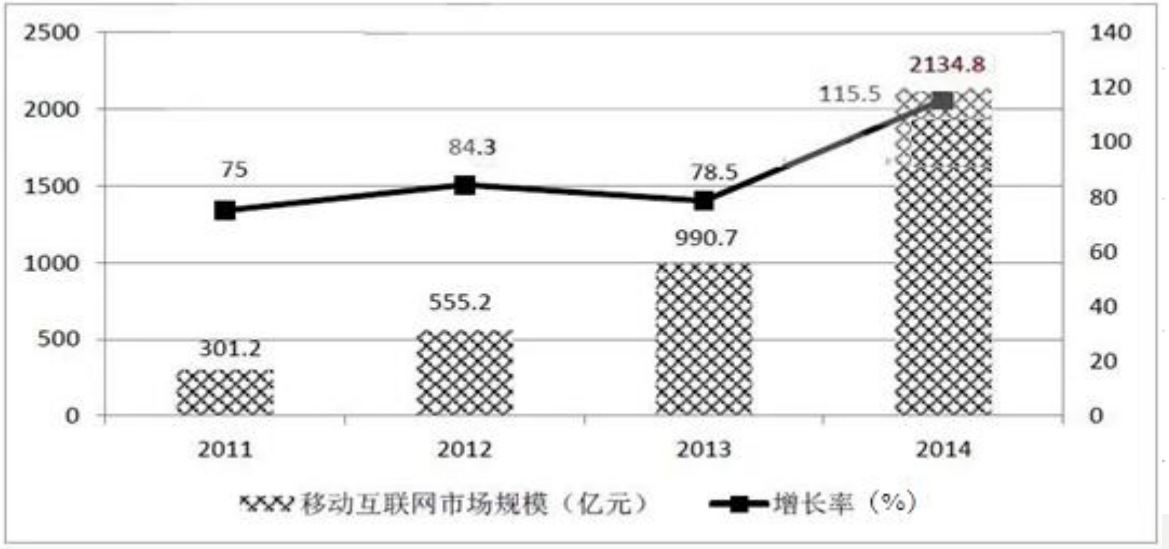
移动App安全检测系统的设计与实现
--Android 篇

江苏通付盾 宋超

通付盾® PayEgis



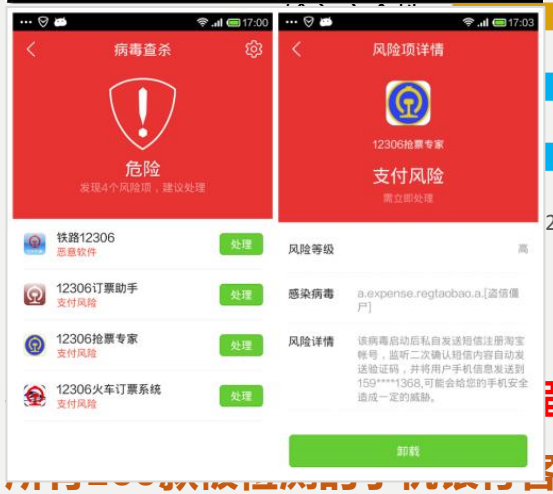


时代背景

- 2014 Google Play的应用数量和开发者数量首次超过App Store，其中Android 应用数量已接近150万，那么2015……
- 2014 中国网民数量突破5亿5千万，手机上网占所有网民上网数量的85%，移动互联网和智能设备只通过短短几年时间就已原因超越PC，那么2015……
- 2014 移动互联网市场规模突破2000亿，增长率达到115.5%；不光有人势，还有钱势；那么2015……

01

移动应用是“互联网+X”的主战场，
安全问题成关注焦点



仿冒应用：窃取网银账号密码及验证码，盗取银行卡余额

手机木马伪装成网银客户端升级助手——应用名为“建行升级助手”、“邮政升级助手”、“平安升级助手”等数十款木马。其结构内容基本一致，并且经过了几个版本的变种完善后，该木马具备了防卸载、躲查杀的超强能力。

二次打包：病毒伪装成订票软件

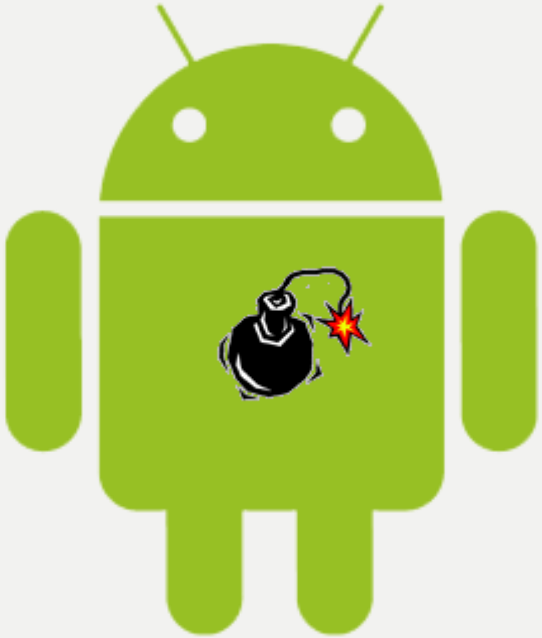
手机病毒被二次打包到12306相关应用中，并散布在各大手机论坛、非安全电子市场供用户下载安装。下载安装后，病毒自动激活，并在后台偷偷运行，用户无法觉察。

20 40 60 80 100 120 140 160 180

注入，反盗版/防二次打包，以及防止验证短信被劫持等方面，

客户端的风险隐患率高达100%

Android寄生兽漏洞（API调用参数设置问题）；Android wormhole漏洞（Android组件或服务权限设置问题）……



02

Android 高性能应用安全扫描器--ARGUS

WHO IS ARGUS ?

通付盾 PayEgis

WHY IS ARGUS ?

通付盾® PayEgis

检测项		数据存储检测>>内容提供者			
分析方案		对APK进行破解后，获取apk源码进行关键词搜索和人工查询			
分析结果		危险			
漏洞详情	结果说明	可以获取源码，通过代码逻辑找到创建数据库、创建表、对表的操作以及保存的数据等信息，可以找到隐私的数据等信息。			
	敏感代码	包名	com.duoduo.util	类名	ae.java
		代码片段			

```
01
02
03 private static boolean b(Activity paramActivity)
04 {
05             ...
06   {
07     ContentResolver localContentResolver = paramActivity.getContentResolver();
08     Uri localUri = Uri.parse("content://com.android.launcher2.settings/favorites?notify=true");
09     String[] arrayOfString1 = { "title", "iconResource" };
10     String[] arrayOfString2 = new String[1];
11
12             ...
13 }
14
15
```

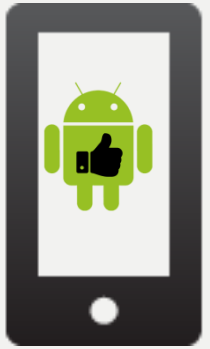
关键字扫描不能叫安全检测！

*30万 ？

HOW ARGUS HELP?

通付盾® PayEgis

passed



ARGUS

1：内容分析，防止监守自盗

2：基于API性能消耗和调用的静态性能消耗分析

谢谢

通付盾®
PayEgis