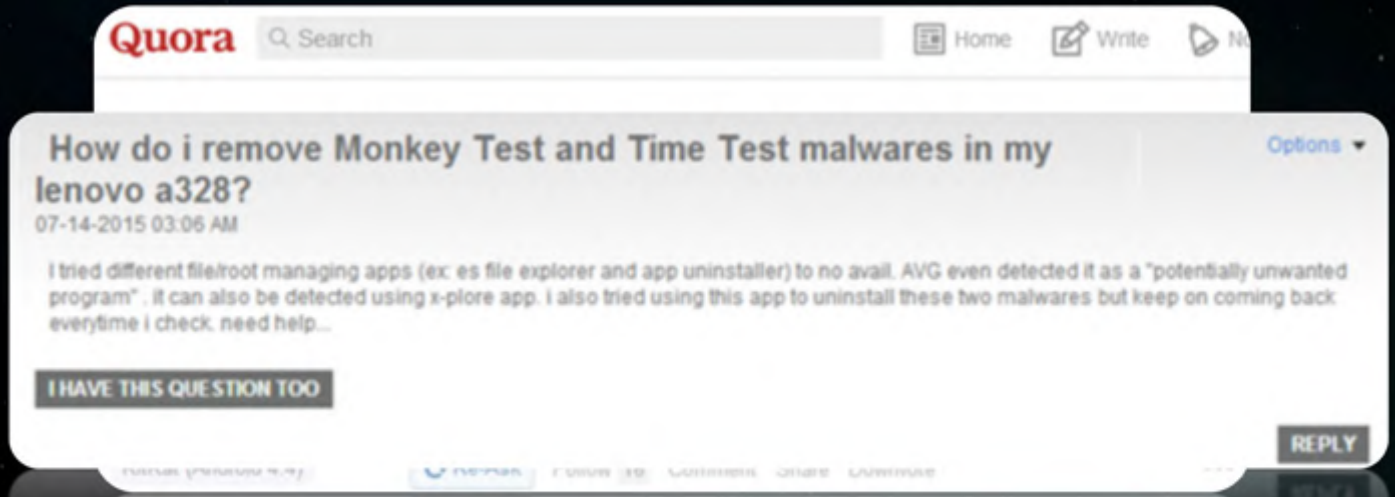
Ghost Push 揭秘

演讲者：邹义鹏
猎豹移动 技术总监

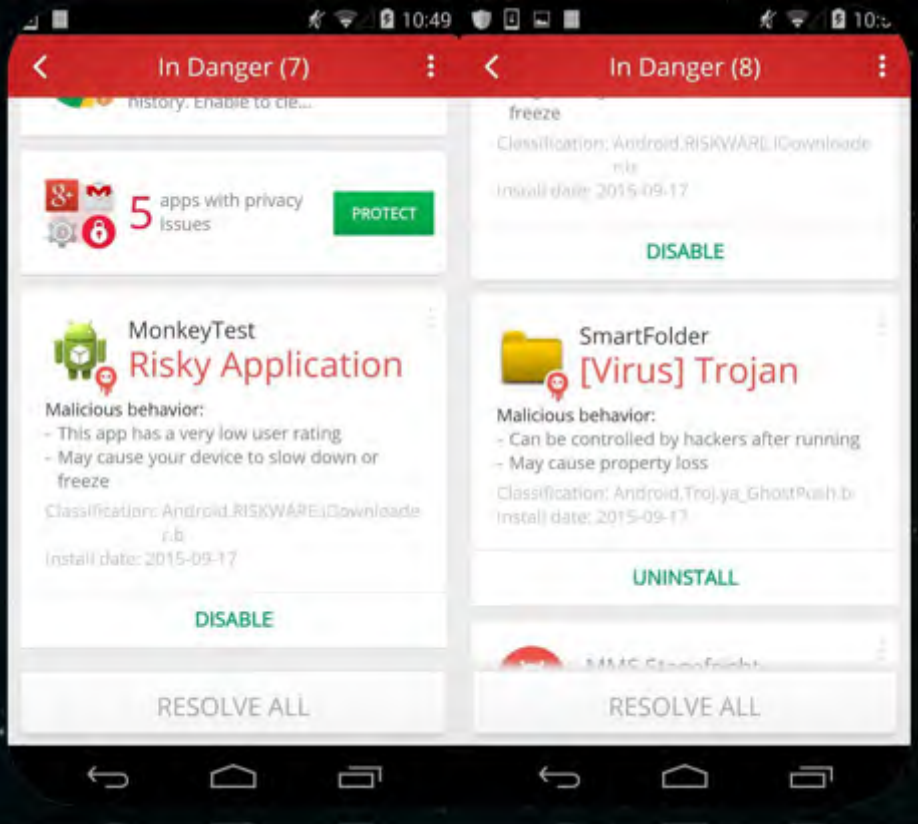
前奏

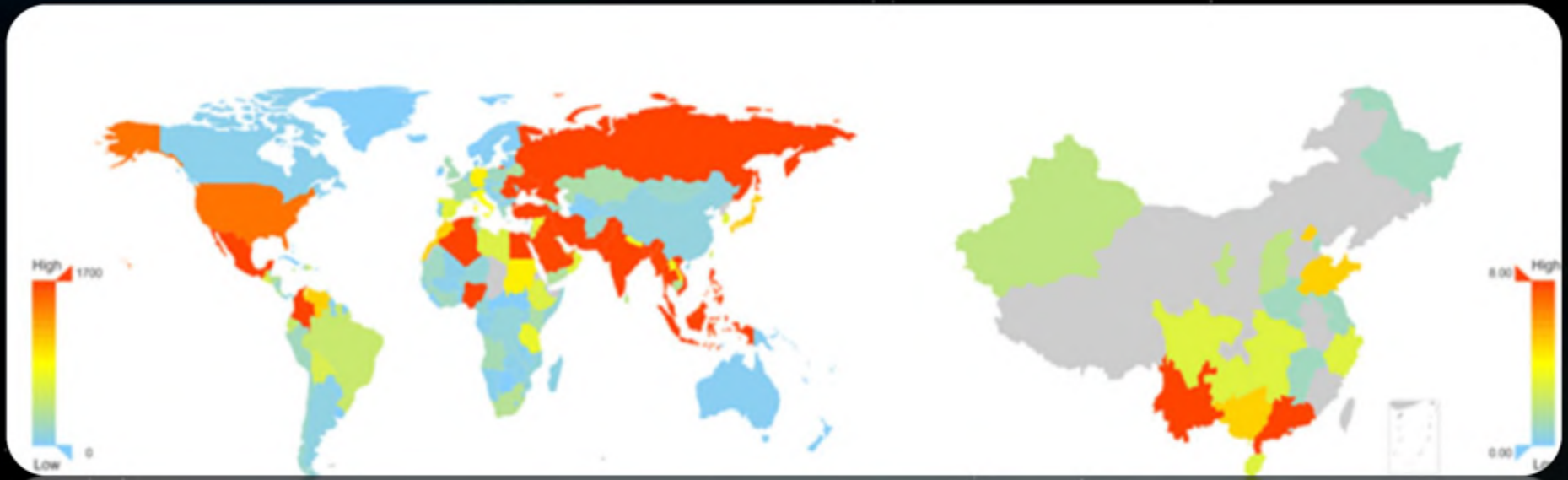
- 时间：2015年7月
  - 用户在论坛反馈无法清除的恶意应用：



目标出现了

- 时间：2015年8月
  - 源头：酷派大神手机用户
  - 现象：在安装官方提供的系统升级包后，被预安装了未知软件：
    - MonkeyTest
    - TimeService





比想象中的影响要大得多...

- 截止到9月18日，该类病毒的每日感染量已经扩大到了最高70万台/天，包括酷派/三星等厂商的3658个品牌、14847种型号机型受影响。
- 感染用户主要分布于东欧、俄罗斯、印度、墨西哥、委内瑞拉、中东、东南亚、中国南部等。

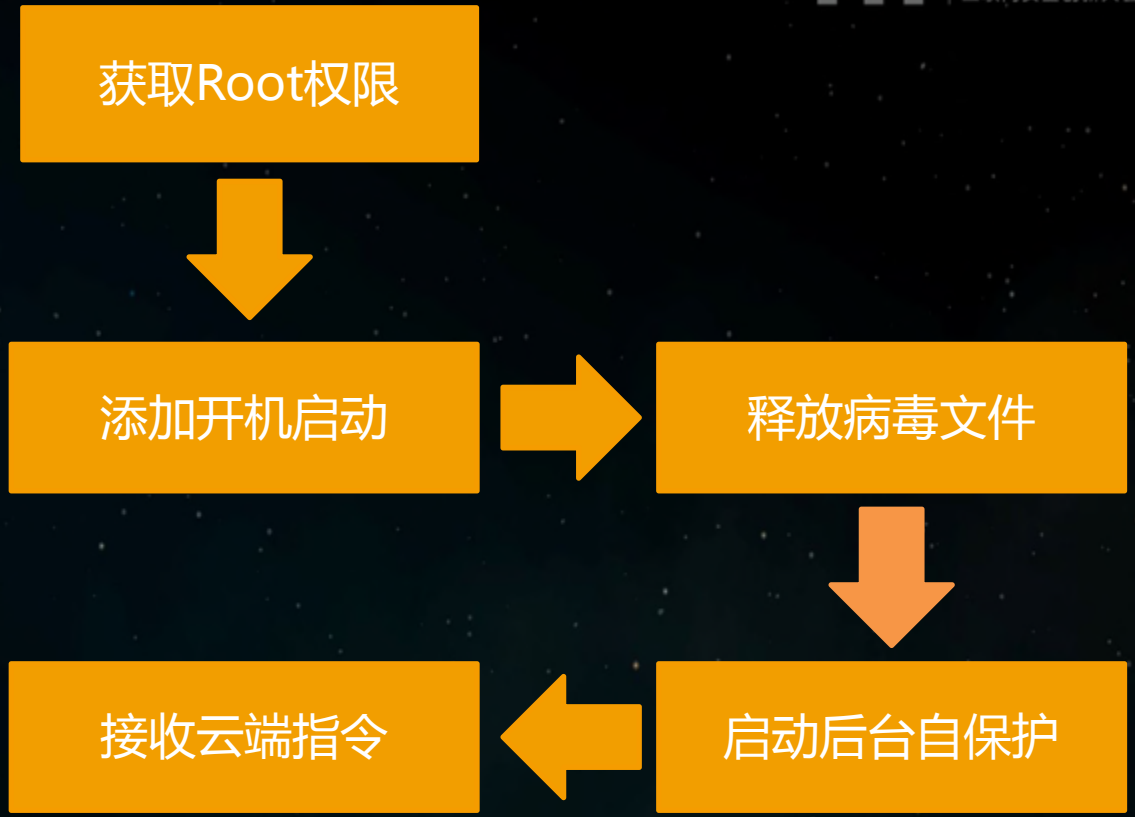
它做了什么...

- 自带Root模块，无法卸载
  - 利用漏洞获取Root（CVE）
- 推送广告
- 静默安装应用

Rootkit	CVE Number
FramaRoot	CVE-2013-6282
TowelRoot	CVE-2014-3153
GiefRoot	CVE-2014-7911 CVE-2014-4322
PingPongRoot	CVE-2015-3636

它是这么干的...

- 云端获取*root*模块
- 替换系统文件，设置开机启动
- 释放文件，安装病毒体到系统目录
- 执行前述的后续动作

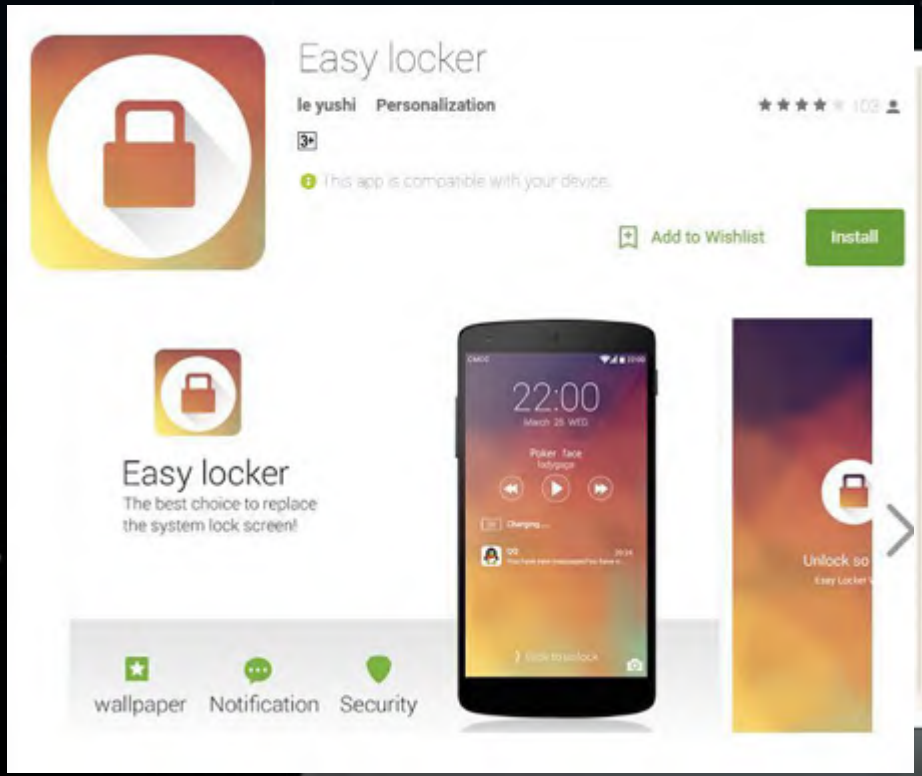


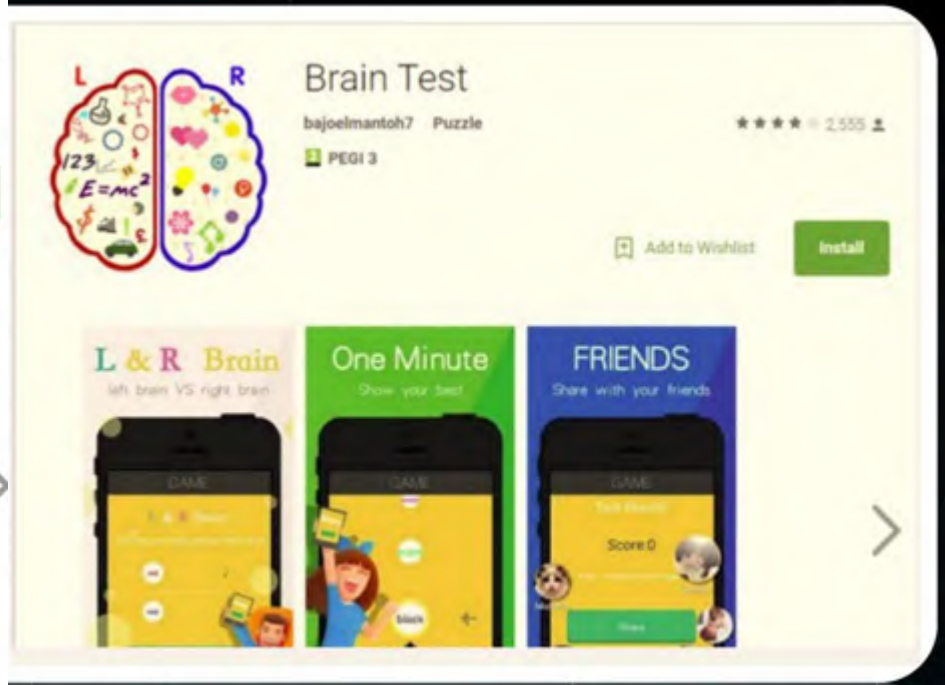
它从哪里来...

应用名：SmartFolder
版本号：101　版本名：1.0.1
证书MD5：ca495b303cca1875165bd6d49b0cafa1
颁发者：C=CN/O=xinyinhe/OU=ngsteam/CN=ngsteam
使用者：C=CN/O=xinyinhe/OU=ngsteam/CN=ngsteam

新银河官网（现在不可用） http://www.ngemob.com
一键ROOT大师 官网http://www.dashi.com/
两个域名使用过同一ip。

它如何遍布全球...


Easy locker
le yushi
Personalization
3+
This app is compatible with your device.
Add to Wishlist
Install
Easy locker
The best choice to replace
the system lock screen!
22:00
wallpaper
Notification
Security


Brain Test
bajoelmantoh7
Puzzle
PEGI 3
Add to Wishlist
Install
L & R Brain
One Minute
FRIENDS
Share with your friends

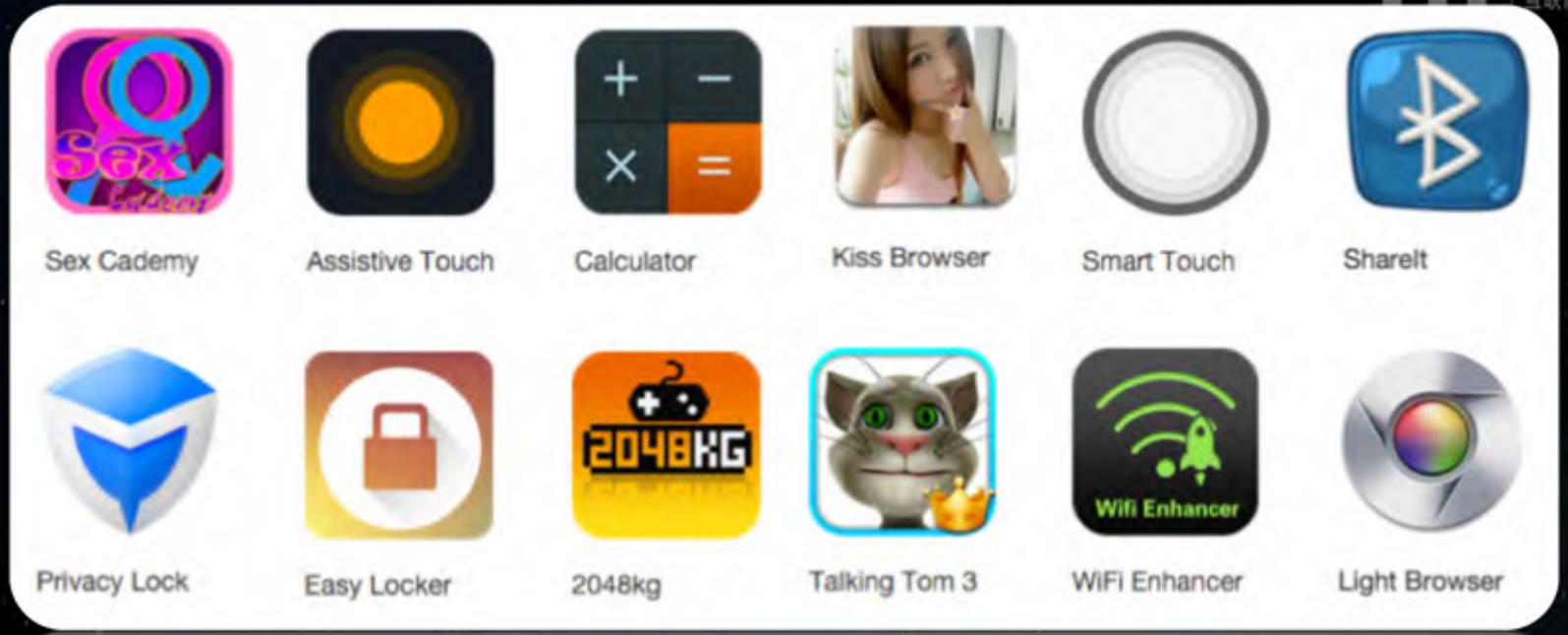
真相 - 只有一个

- 背景：
  - 移动互联网大时代
- 需求：
  - 应用推广 → **灰色产业链**
- 根源：
  - 逐利!

顺藤摸瓜

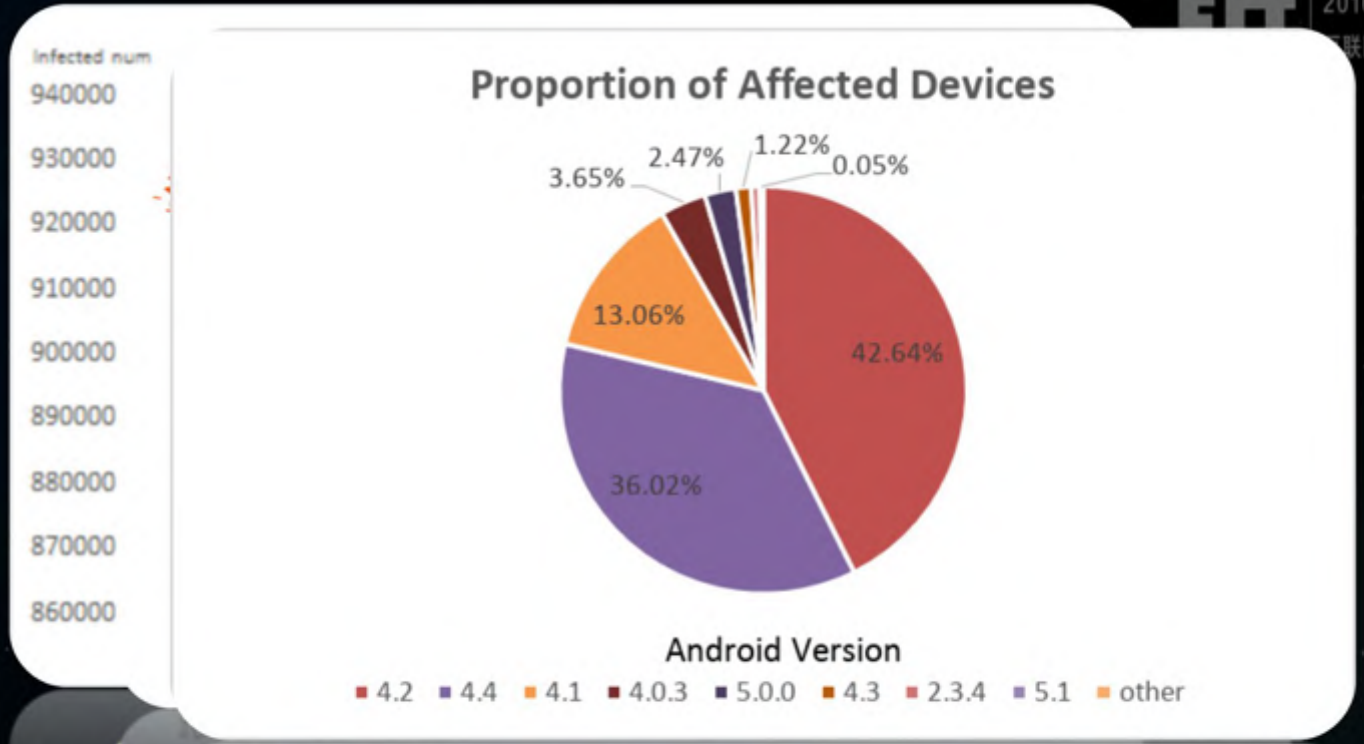
- 更多的Root病毒浮出水面

Date	Warning	Reporter
9.18	Ghost push	Cheetah Mobile
9.21	Braintest	Checkpoint
9.22	Guaranteed Clicks	Fireeye
10.2	RetroTetris	Trend Micro
10.7	Kemoge	Fireeye



更多被感染的APP，包括Google Play市场应用

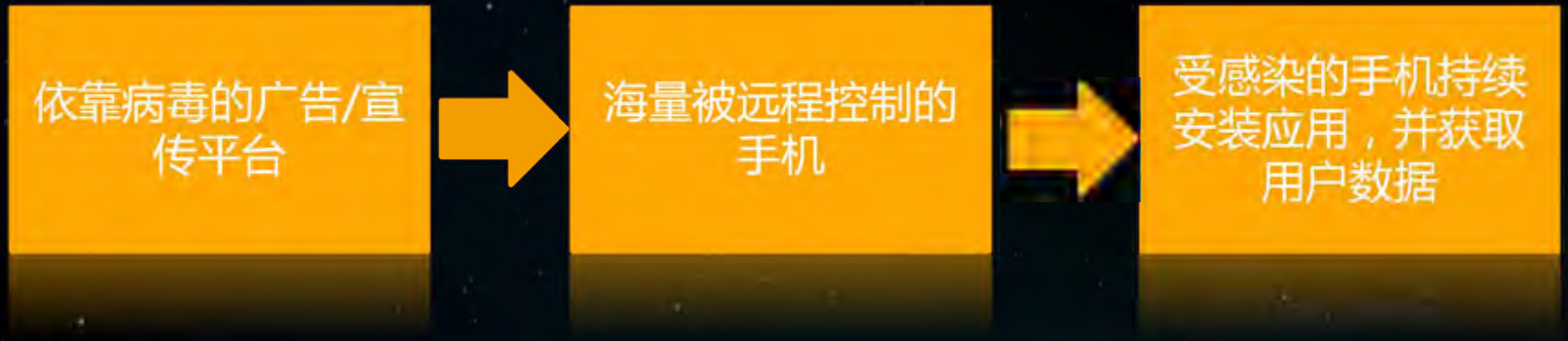
除了Brain Test，更多的应用被发现有感染，以及发现新的病毒变种。



感染量依然持续增加

- 为何东南亚成了重灾区？

越来越多的中国供应商开始在东南亚地区拓展业务，来自中国的病毒作者的商机就在这里



产业链运作方式

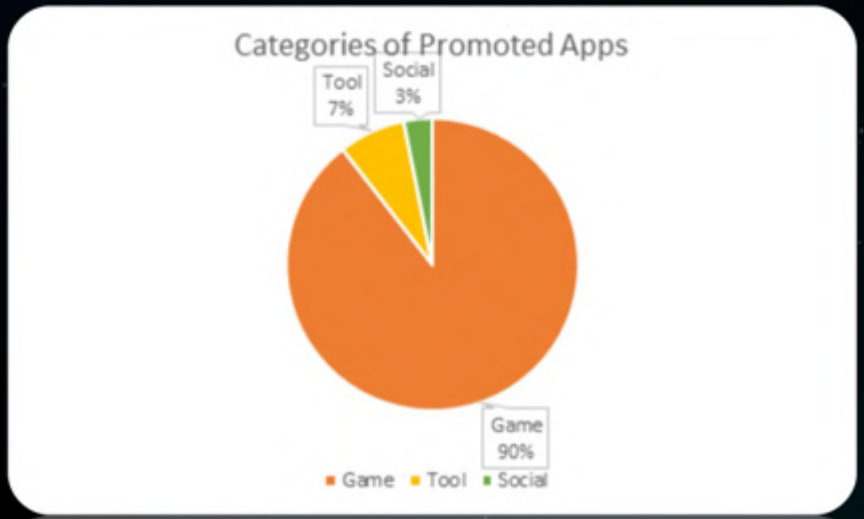
- 利用病毒进行广告/推广
- 获取大量被远控的手机
- 在被感染的手机上静默安装应用并进一步扩大病毒网络

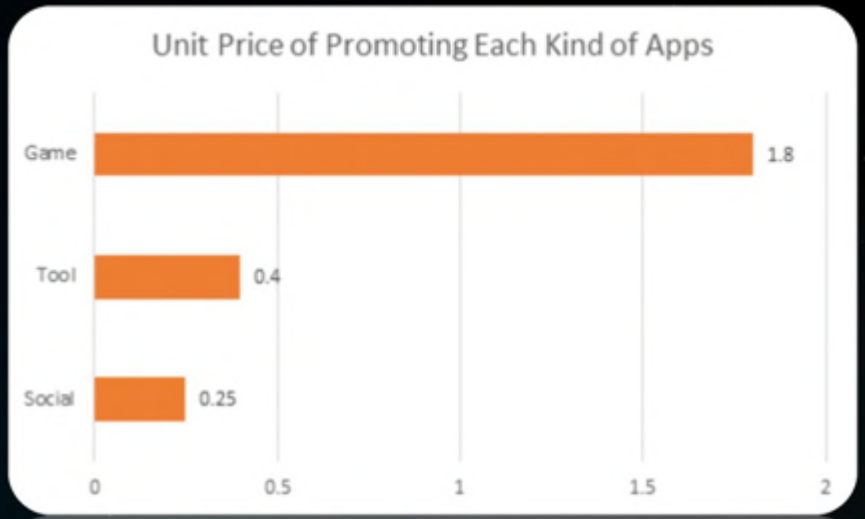
App name	Price($)	Package Name
Magic Rush: Heroes	3.00	com.moonton.magicrush
Empire: Four Kingdoms	2.94	air.com.goodgamestudios.empirefourkingdoms
Dawn of Titans	2.89	com.naturalmotion.dawnoftitans
盜夢英雄（全面公測）	2.80	com.funapps.tw.dmyxob
DomiNations Asia	2.52	com.nexon.dominations.asia.g
Ensogo	2.50	com.ensogo
仙劍奇俠傳-官方正版授權	2.14	com.gm99.pal
武聖的覺醒	2.14	com.zhancheng.sanguolua.google
戰國GOGOGO	2.10	com.kimi.ggplay.zhanguotw
戰姬天下	2.10	com.happyelements.canontwsa.googleplay
百將行	2.08	com.gaeagame.tw.heros100

抓取到的一份应用推广价格清单

事实上，从我们分析到的数据来看，游戏的推广费用是最高的，最高的竟然达到了$3.00/用户！

每天能挣多少钱？





可以计算一下：

平均每台设备3个应用，一个应用平均$1.5，基于感染量保守估计90万，那么收益就是：

$1.5*3*900,000=**$4,050,000** ！！！

启示

- 关于移动互联网安全
  - Ghost Push可能只是冰山一角
  - 利益的驱使催生灰色产业
- 对安全从业者来说
  - 移动端安全问题的挑战
  - 对用户设备&信息的安全保护，任重而道远

谢谢！