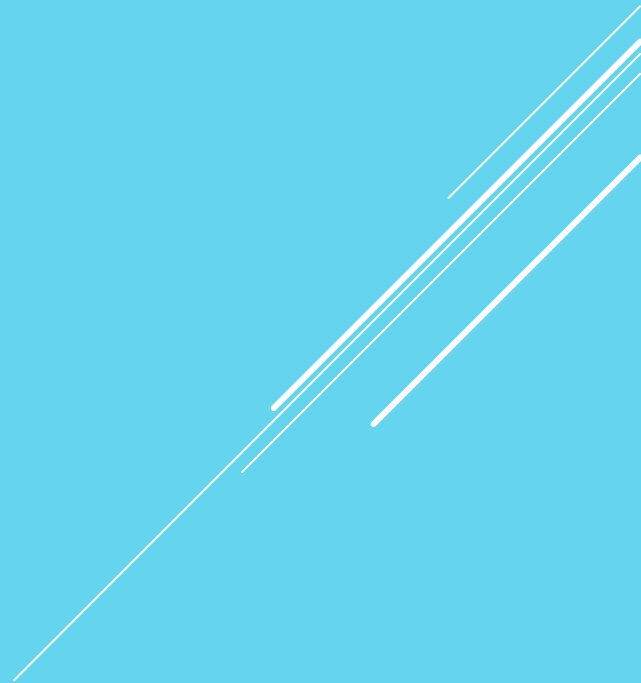


# 全球移动安全趋势分析

猎豹移动安全实验室 苏海峰



# 安卓手机病毒数据分析

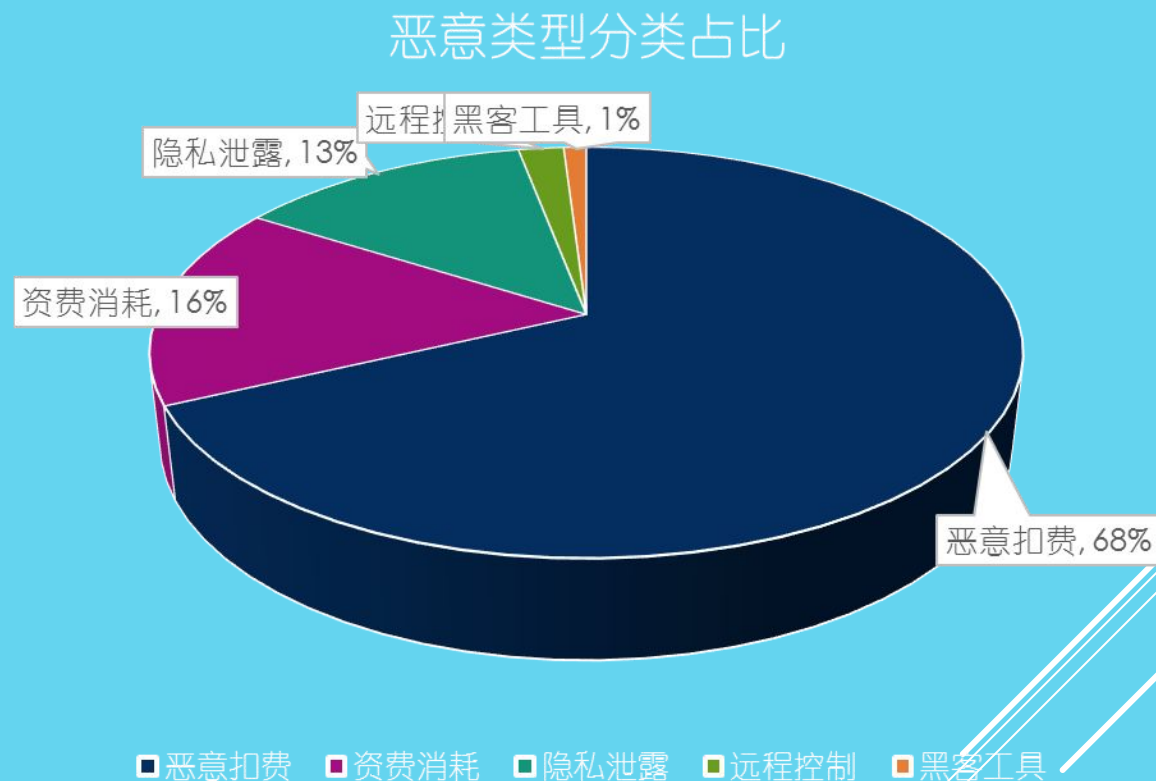




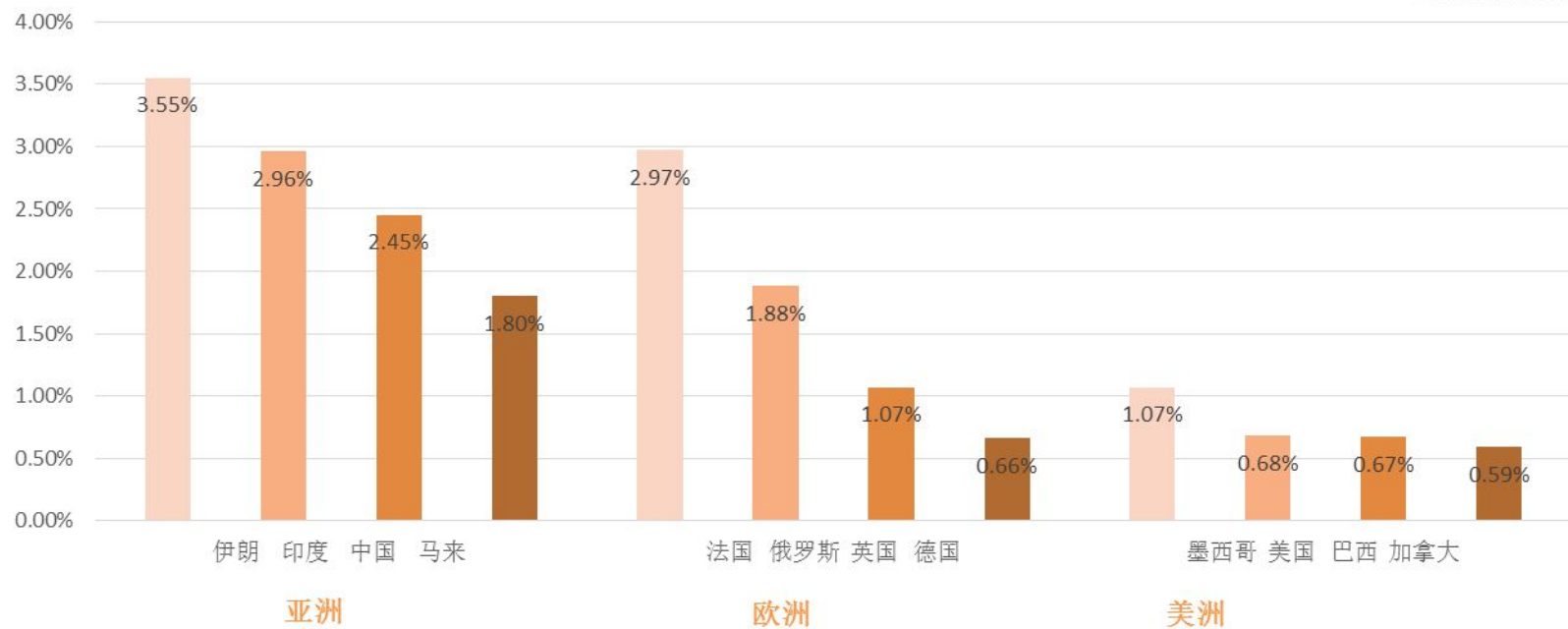
支付及恶意扣费类病毒占据病毒样本的84%

资费消耗类病毒占据第二位，达到16%

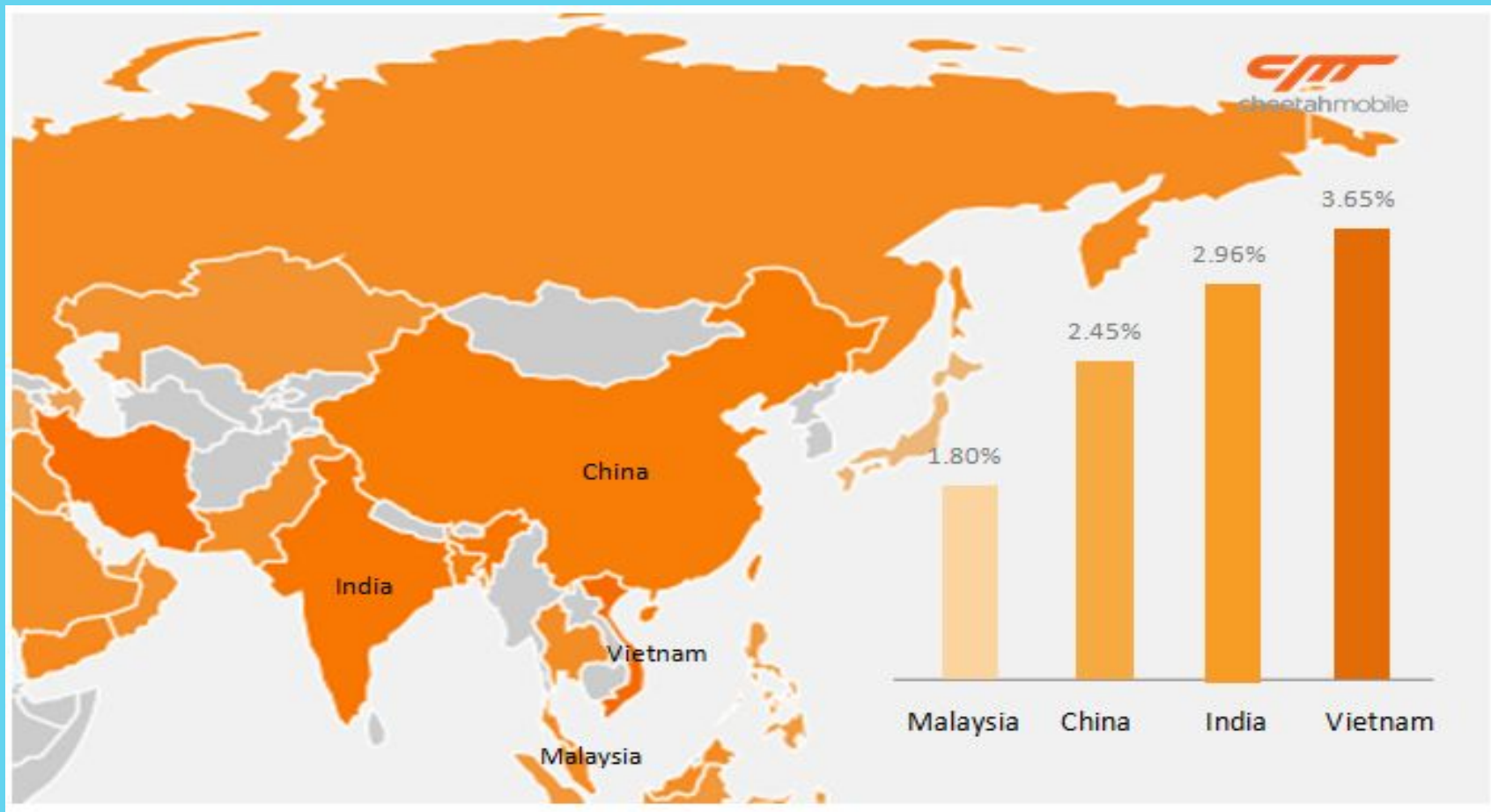
## 病毒样本分类





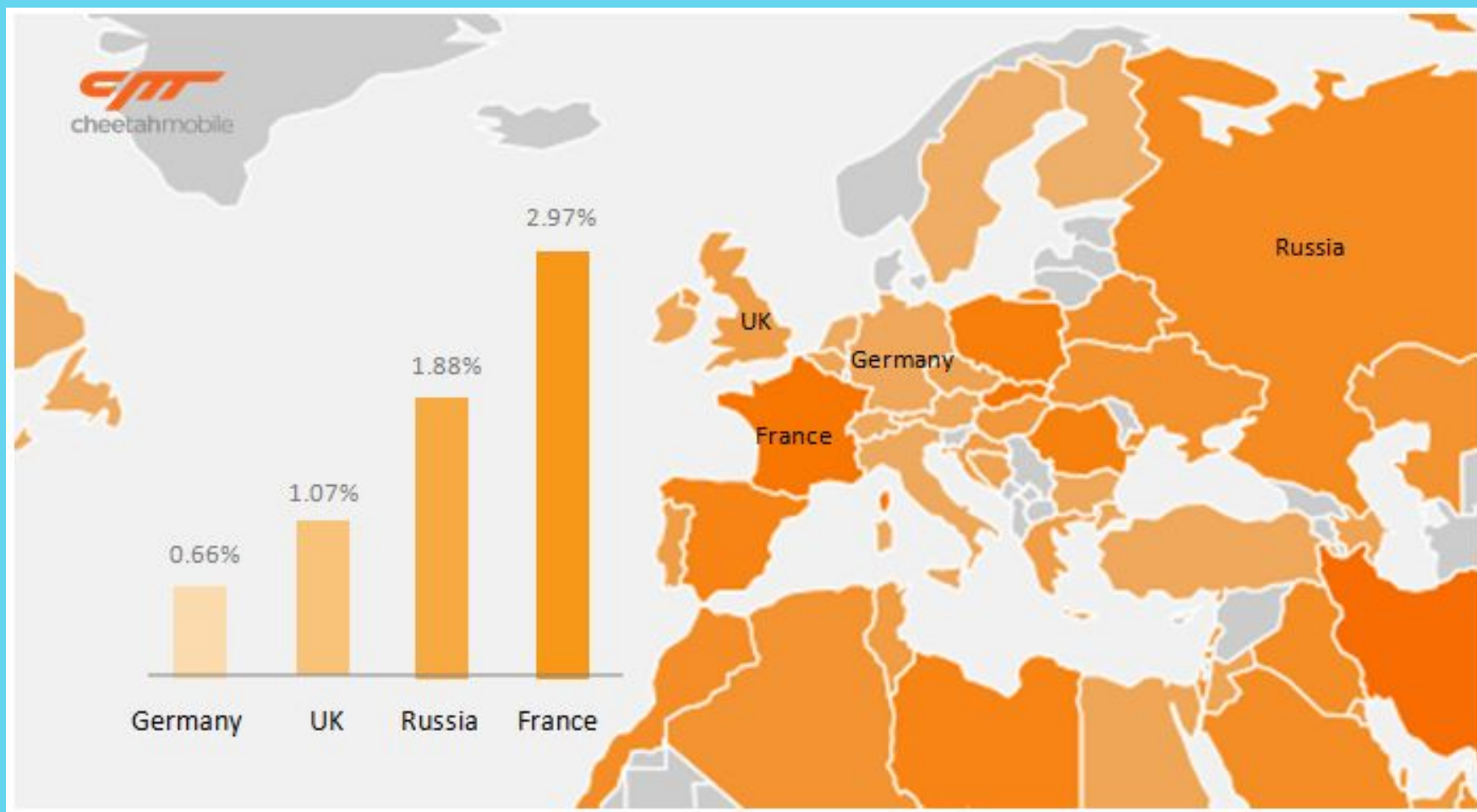


# 全球病毒感染形式

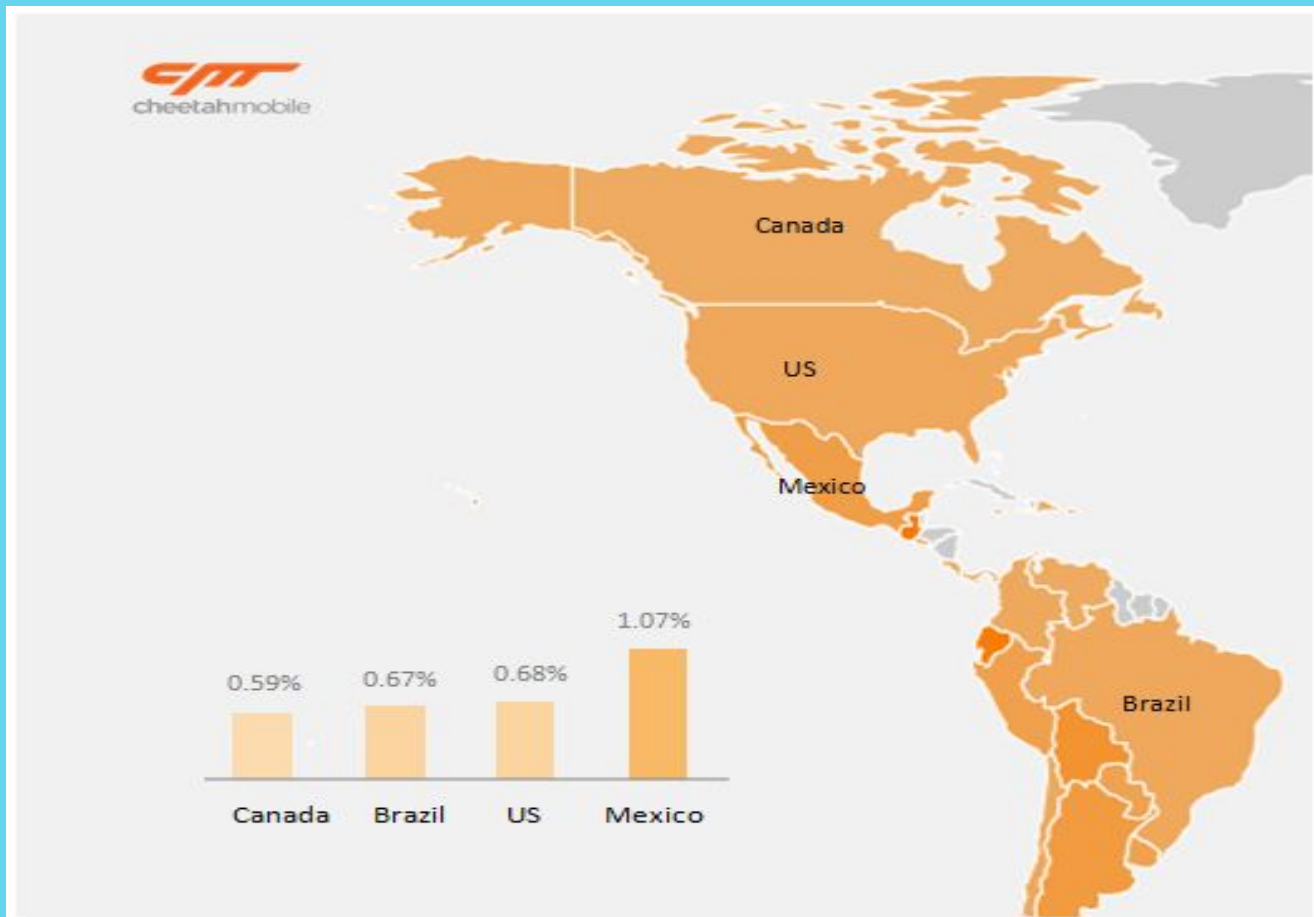


## 亚洲地区病毒感染情况



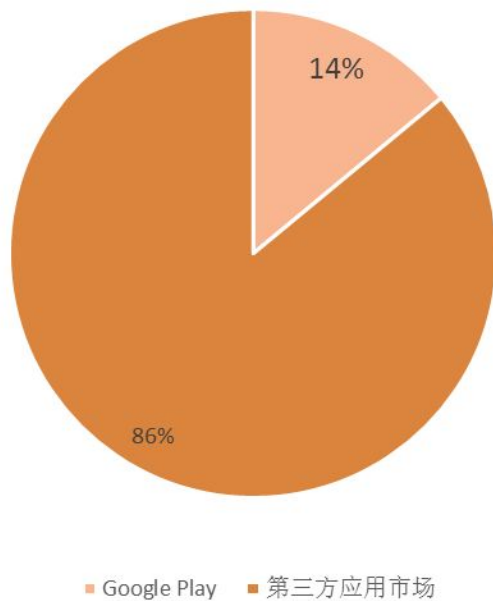


欧洲地区感染情况



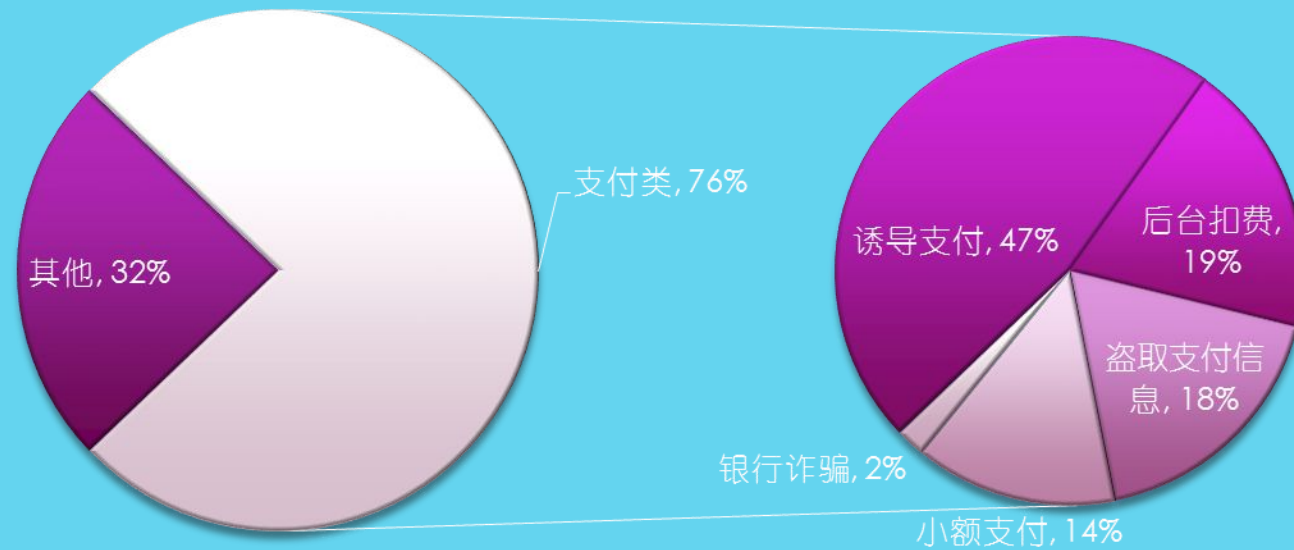
## 美洲地区病毒感染情况

## 安卓手机病毒传播渠道分析

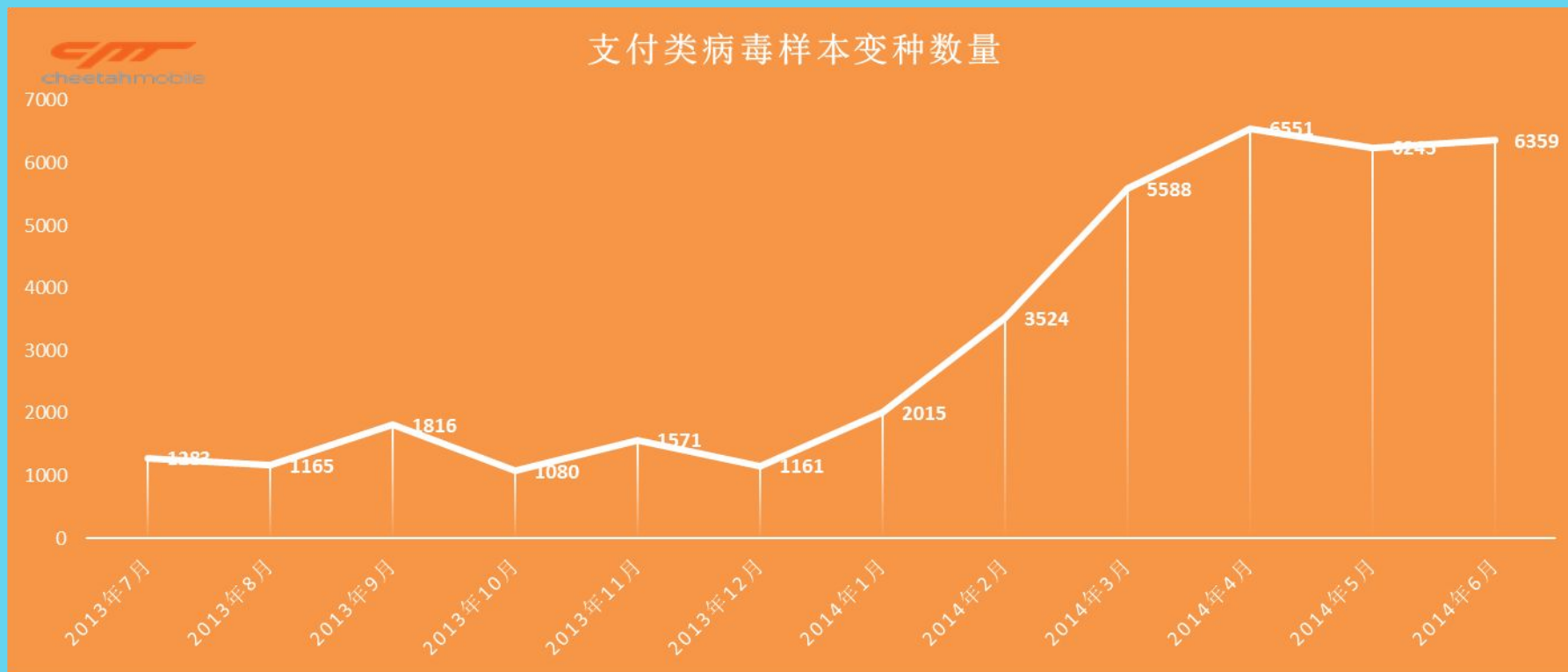


86%的病毒来自于第三方应用市场

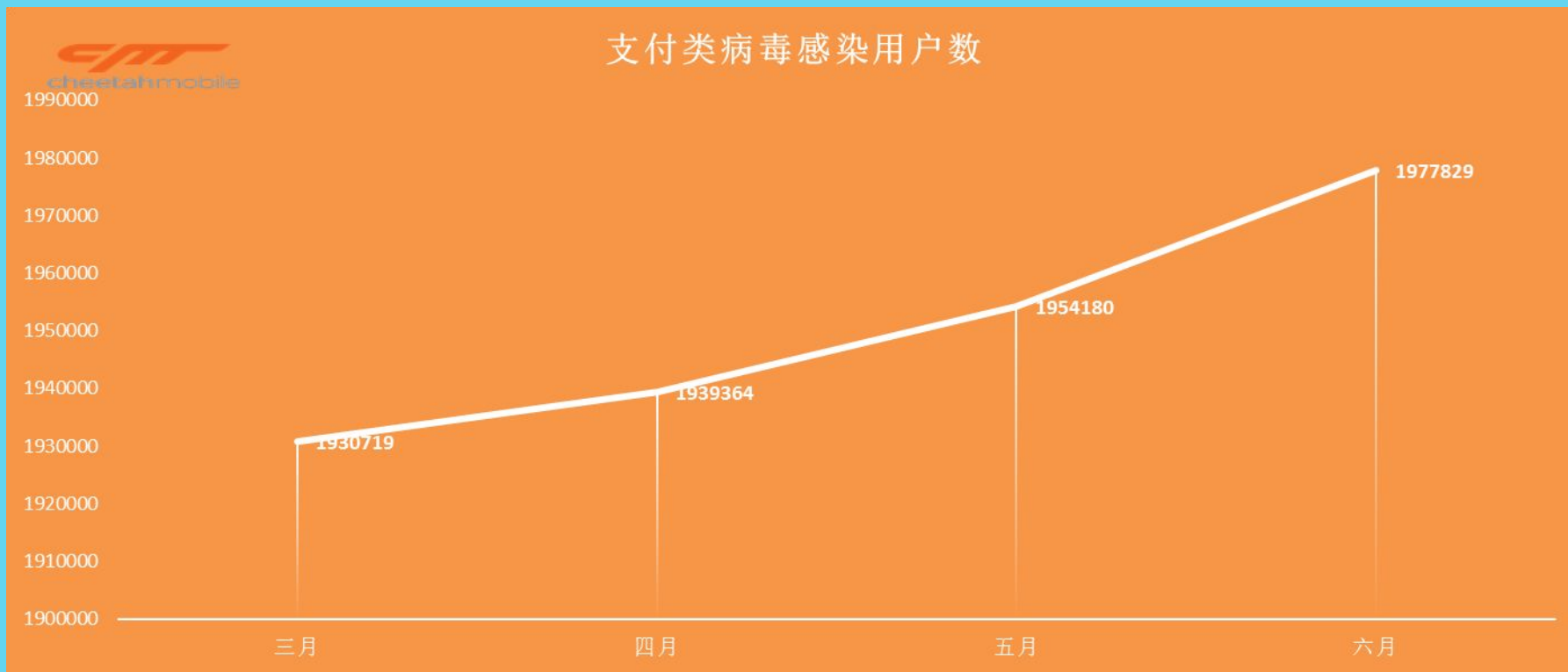
## 病毒分类



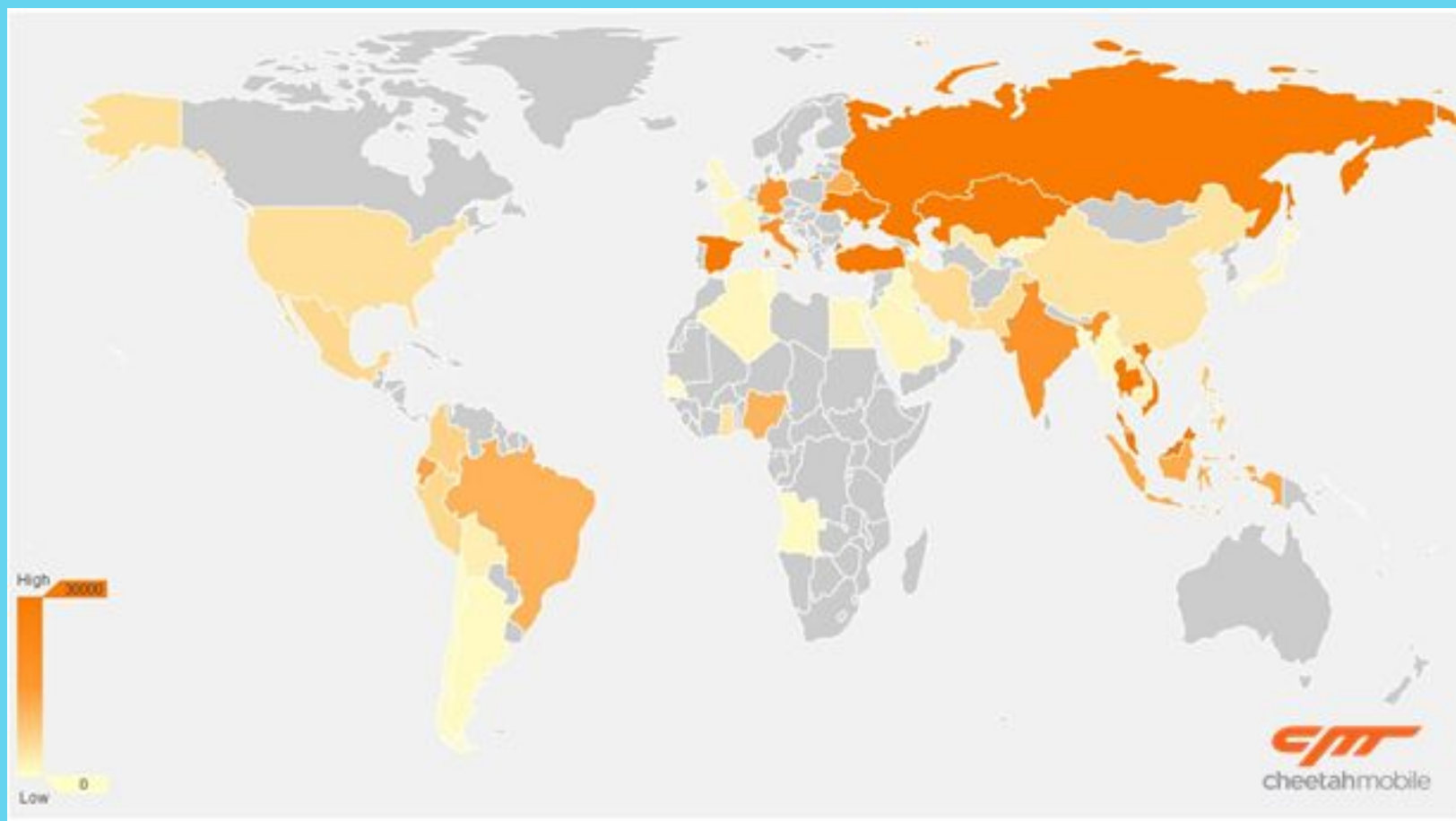
## 支付类病毒分析



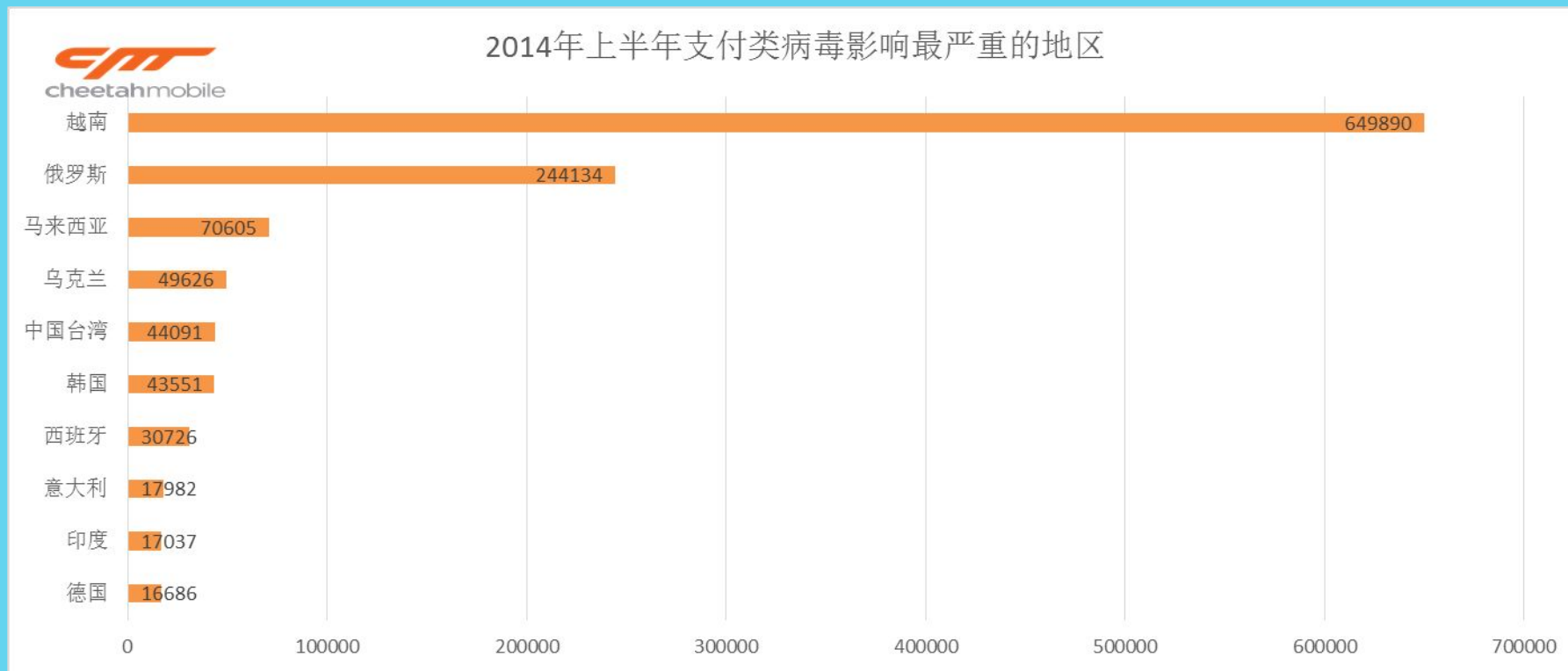
支付类病毒增长4倍



中毒用户持续增长



上半年全球支付类病毒中毒地区分布



上半年支付类病毒高中毒地区





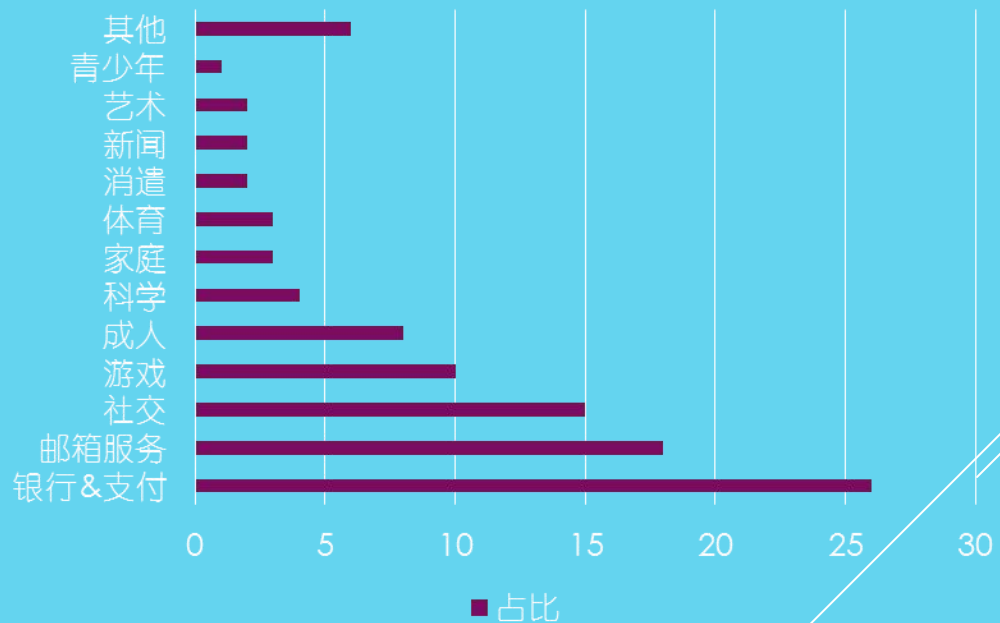
# 心脏出血漏洞

102个国家



1100万台服务器

漏洞网站分类占比情况



## eBay数据泄漏

影响1.45亿用户

登陆账号、邮件地址、联系地址、电话号码以及出生日期



## 携程网信息泄露

### 安全支付日志可下载导致信息泄露

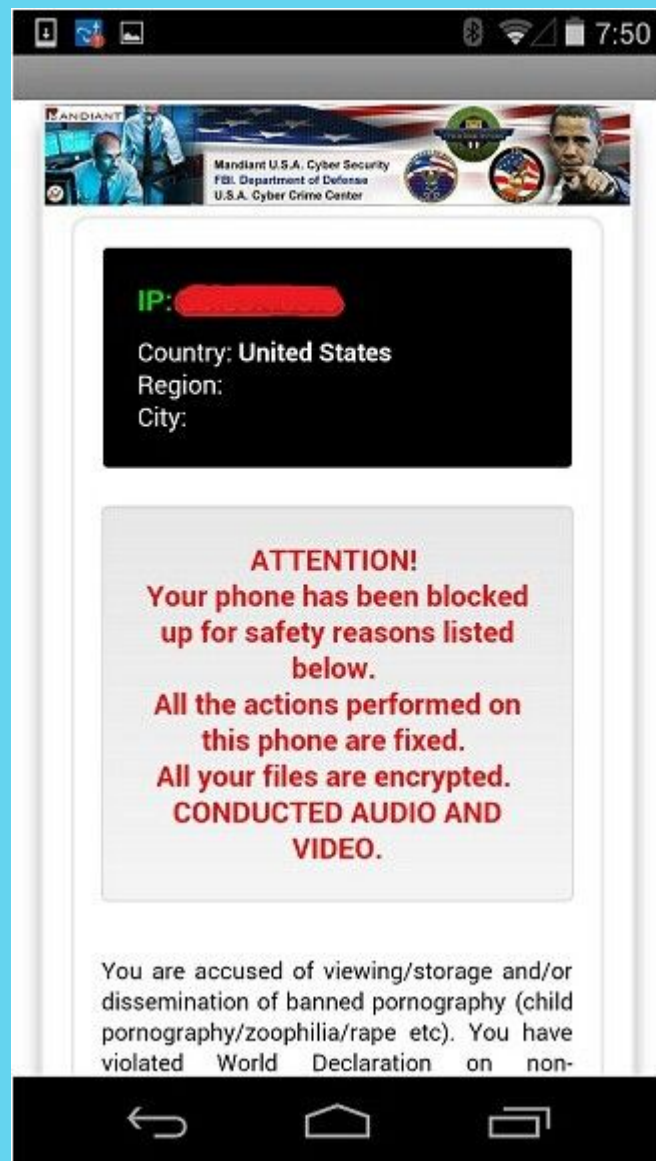
持卡人姓名  
持卡人身份证  
所持银行卡类别（比如，招商银行信用卡、中国银行信用卡）  
所持银行卡卡号  
所持银行卡CVV码  
所持银行卡6位Bin(用于验证支付信息的6位数字)

国家	病毒名称	恶意行为
美国	敲诈者病毒	恶意弹窗,敲诈用户付费，用户无法正常使用手机
台湾区	宅急便病毒	小额支付诈骗病毒，并伴有后台发送短信导致恶意扣费的行为
俄罗斯	顽固木马病毒	伪装成系统应用，无法正常卸载，恶意扣费
中国内陆	手机预装马病毒	伪装成安卓系统服务，窃取用户手机信息

近期爆发的热点病毒

和Windows时代的敲诈者类似  
手机无法正常使用，2s弹窗  
将SD卡中的图片文件加密  
强迫用户交赎金

敲诈者



SD卡加密



弹窗强制  
用户付费

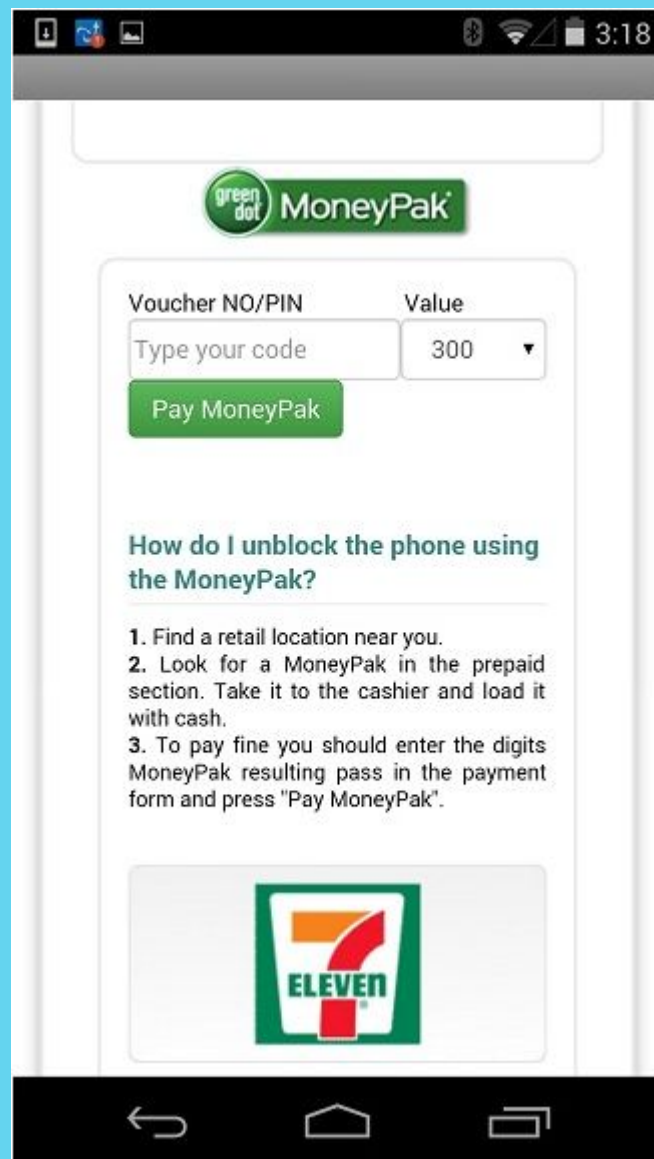


判断用户  
是否付费



卸载

病毒流程



每日**2**万条  
感染**200**万  
中毒率**10%**  
千万级吸费金额



“宅急便”手机病毒

伪装成*GOOGLE* 服务

短信传播，短信中带有机主姓名

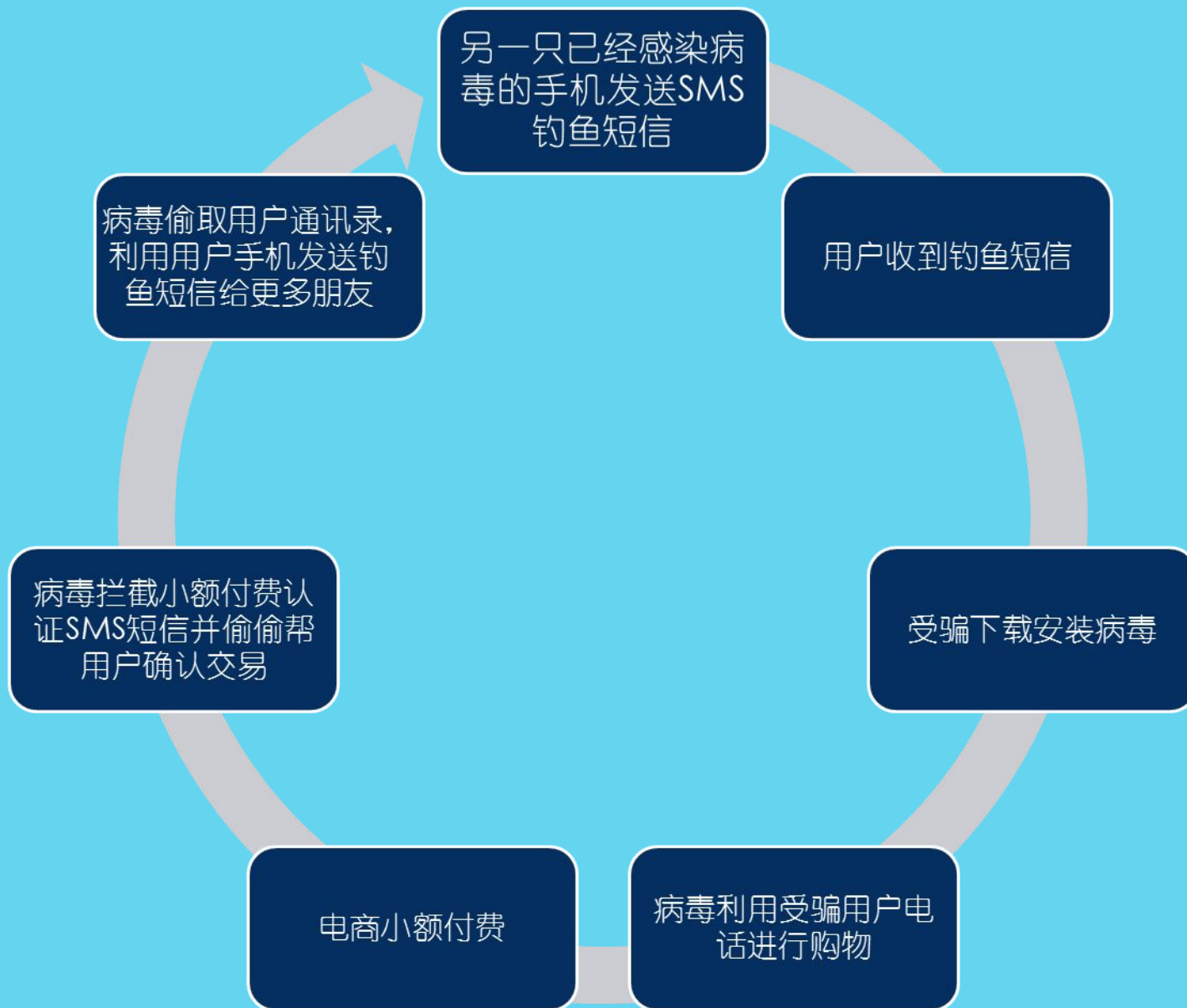
利用小额支付功能盈利

病毒特点





# 盈利模式





## 对抗方式

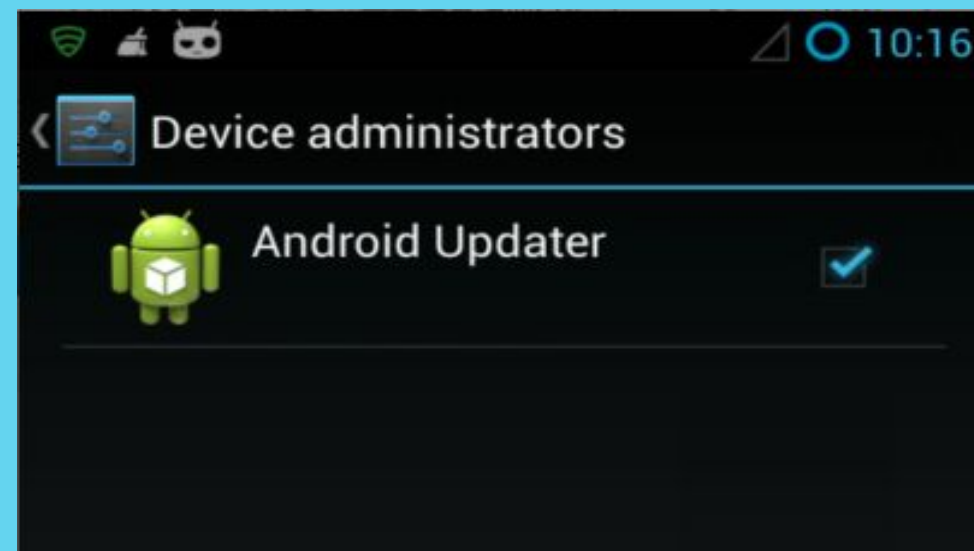
```
graph TD; A[对抗方式] --> B[利用漏洞]; A --> C[在取消时进行干扰]; A --> D[在取消激活后强制激活];
```

利用漏洞

在取消时进行干扰

在取消激活后强制激活

激活成功后不显示在设备管理器  
列表中

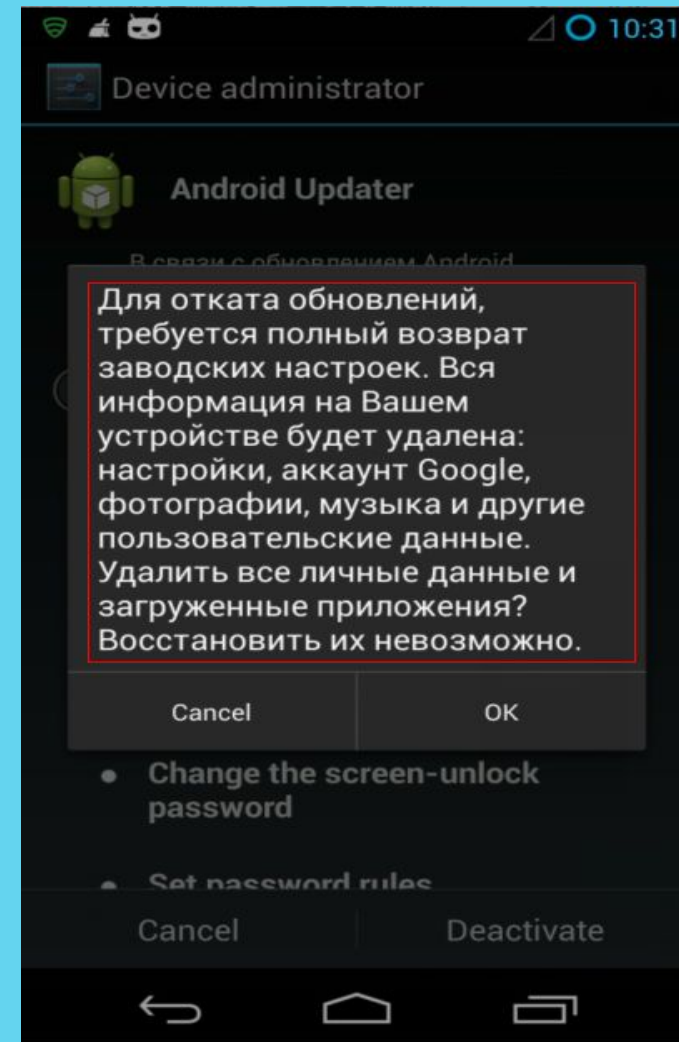


利用漏洞

修改确认对话框里的描述，  
恐吓用户

提示“如果点击确认会导致数据丢失”

取消设备管理器时进行干扰



锁屏

启动一个覆盖全屏的悬浮窗，屏蔽所有按键消息（图）

不断调用激活界面，强制激活



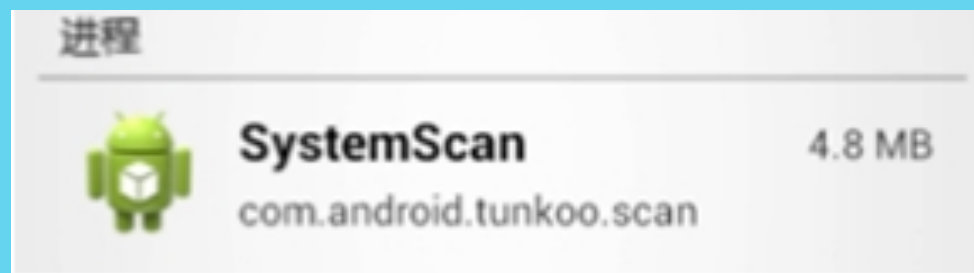
取消设备管理器时的对抗

国家	感染量
Russia	9307
Ukraine	1833
Kazakhstan	1800
Belarus	390
Korea, South	260
Uzbekistan	147
United States of America	67
Kyrgyzstan	48
Azerbaijan	46
Tajikistan	42
Armenia	42
China	38

总感染量

出厂后销售商植入病毒  
无法卸载  
恶意扣费

手机预装马

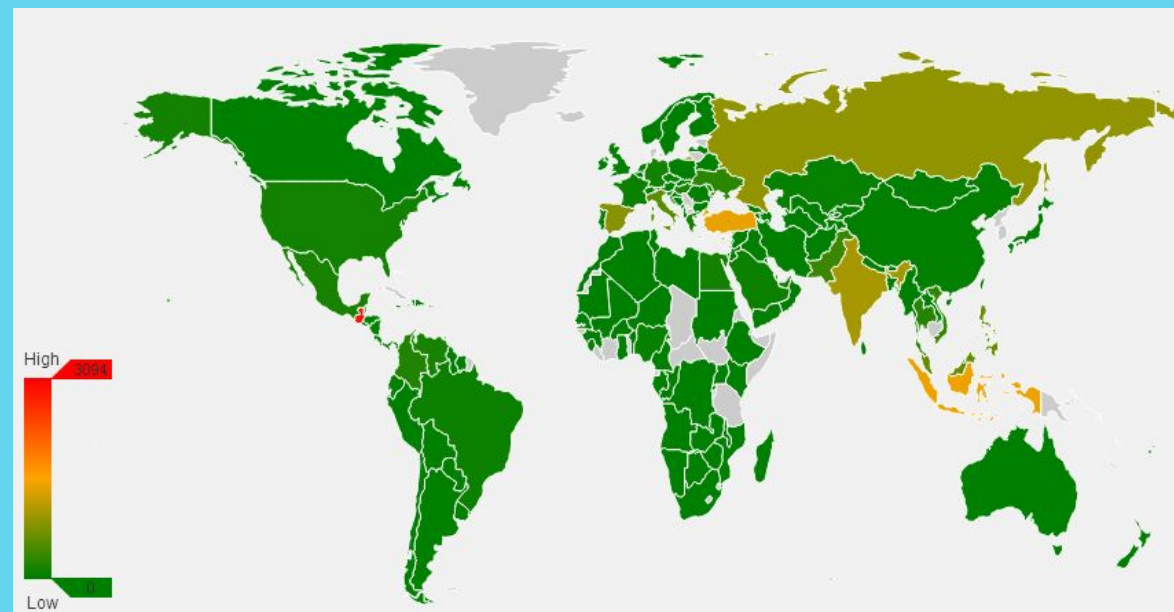




中国制造的山寨含毒手机，几乎卖到了全世界

每日影响用户1.5W人

只能冻结



手机预装马

*Android*下的黑色产业链越来越完善  
山寨手机病毒已形成完整的利益链条  
移动支付的普及将带来更多的安全风险

*APP*市场的安全审查必须更严格

启示

加壳和混淆技术会被病毒普遍应用

病毒将会加强的云端建设，恶意行为更隐蔽

AV厂商必须加强动态分析技术和启发式识别能力

对抗方面

