全球移动安全趋势分析

猎豹移动安全实验室 苏海峰

上半年移动安全的主要特点

- 安卓病毒数量仍然大幅增长
- 支付类病毒表现突出，影响遍布全球
- 以心脏出血漏洞为代表的漏洞攻击影响多个平台

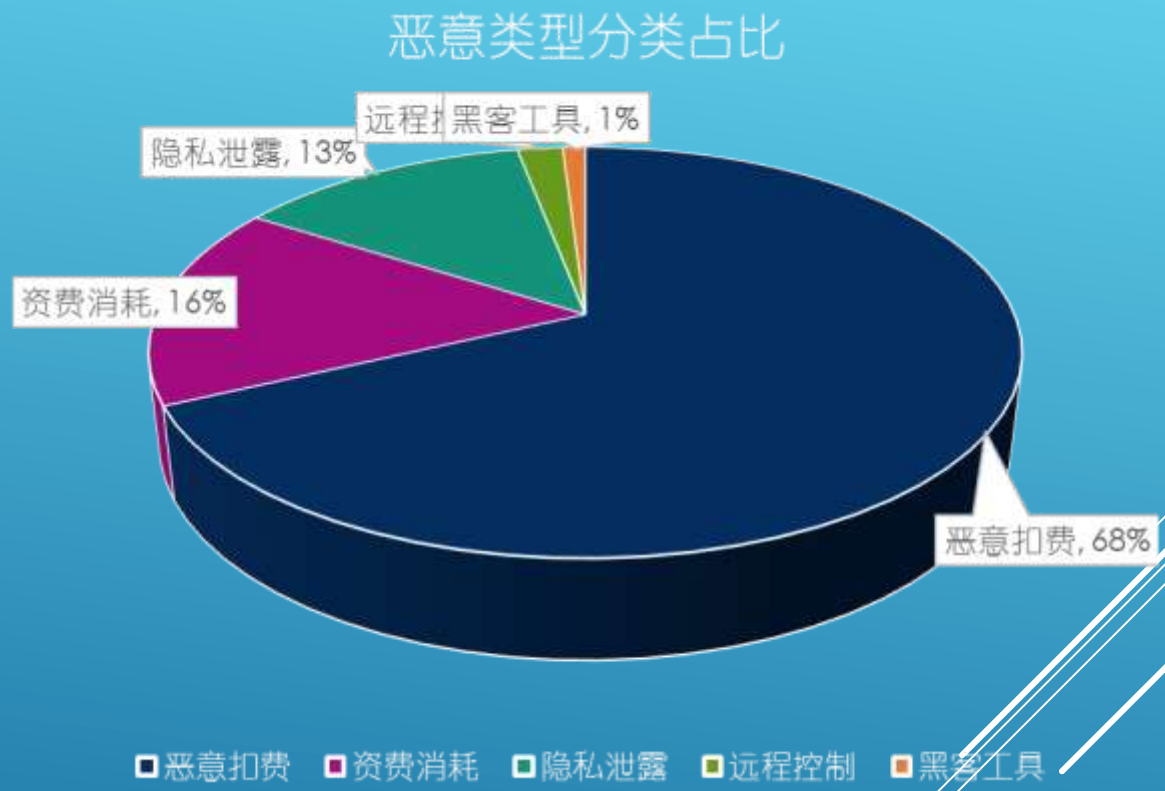
安卓手机病毒数据分析

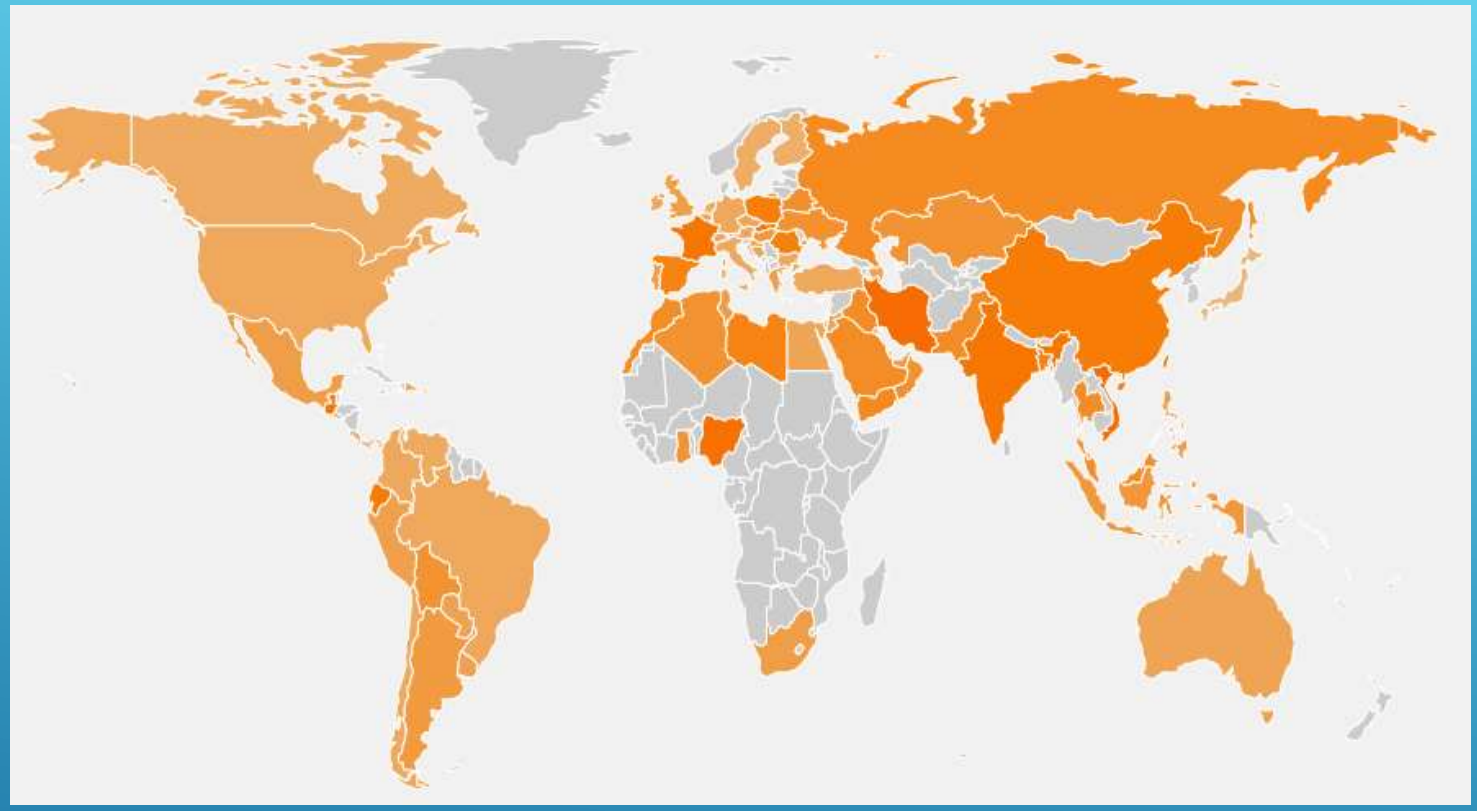
安卓病毒持续迅猛增长

- 截止2014年6月
- 病毒样本总量达215万
- 2012全年的20.5倍
- 2013年全年2.5倍

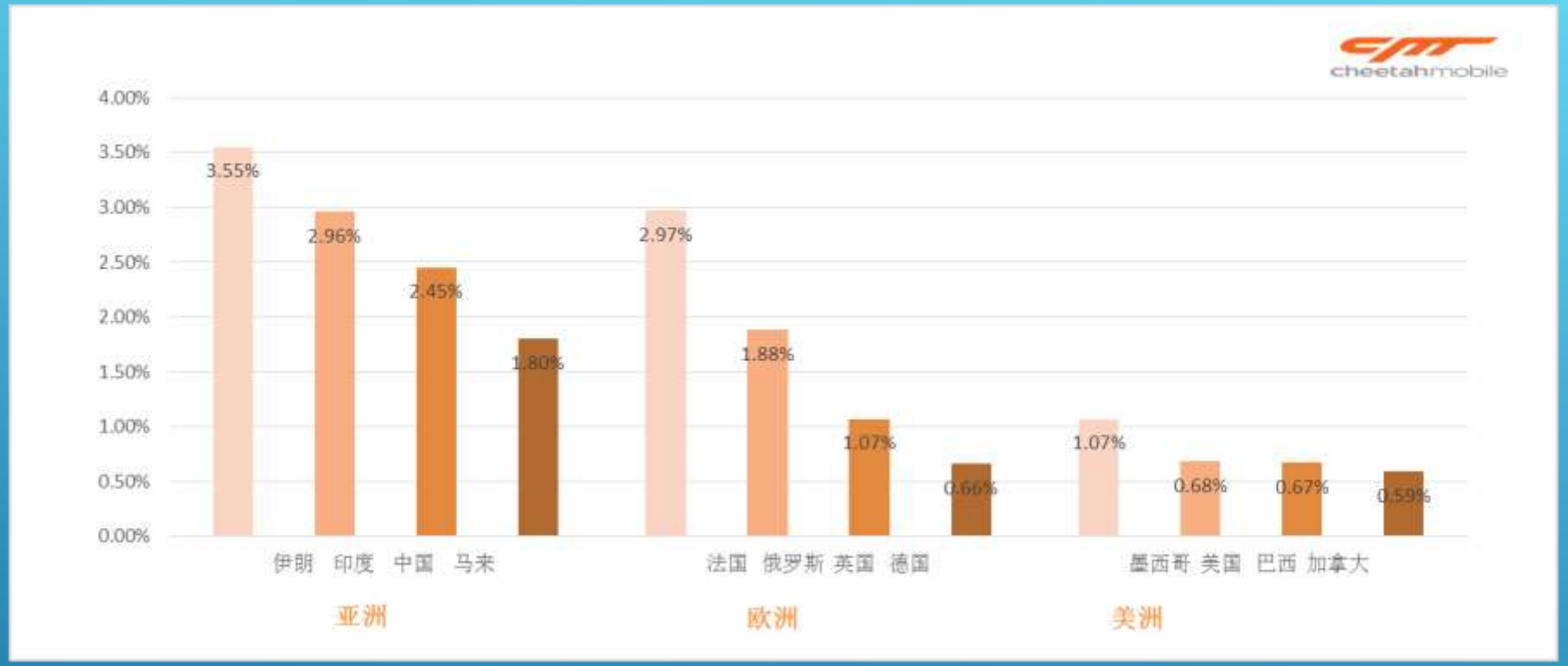
病毒样本分类

- 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%

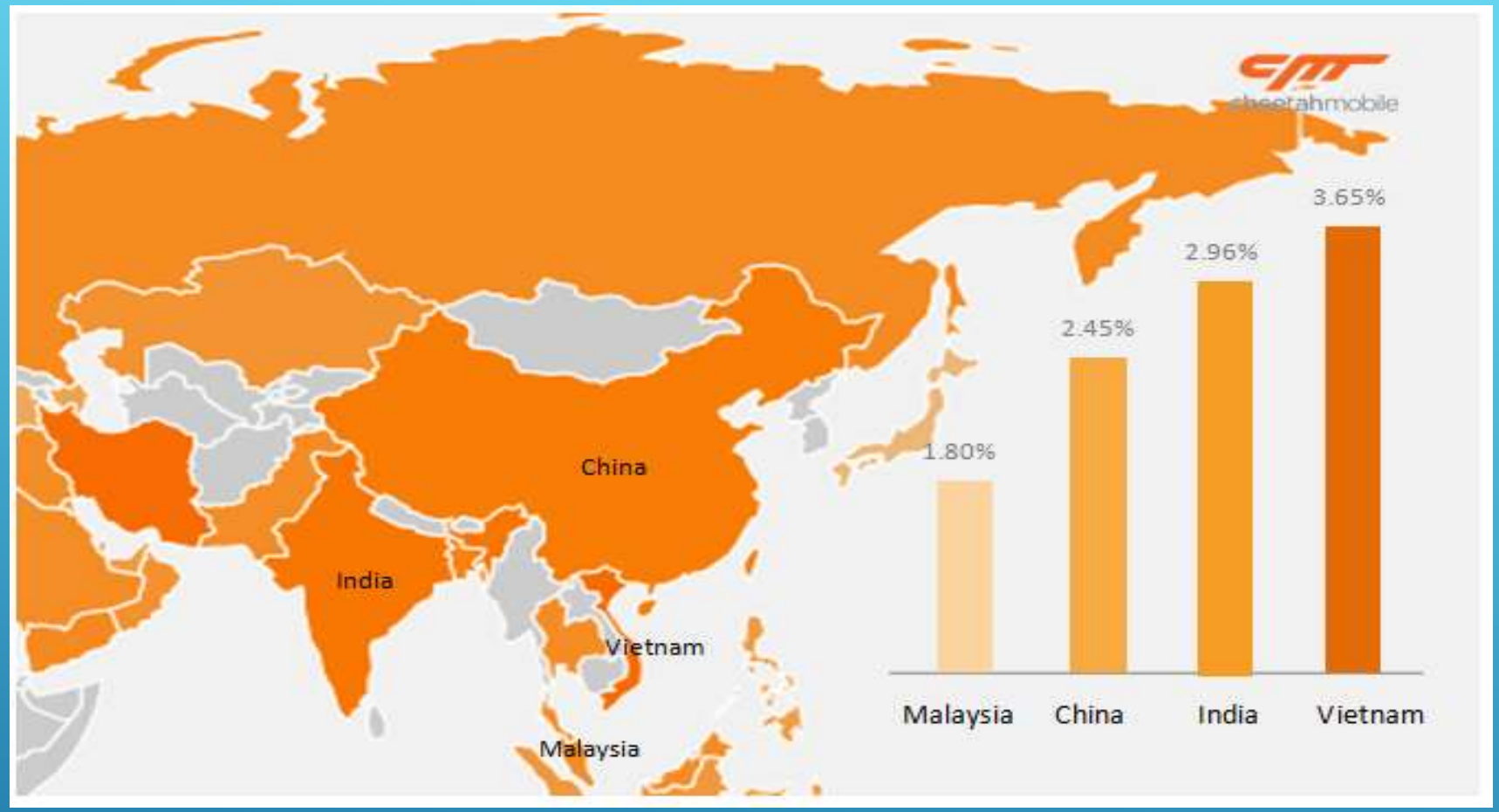




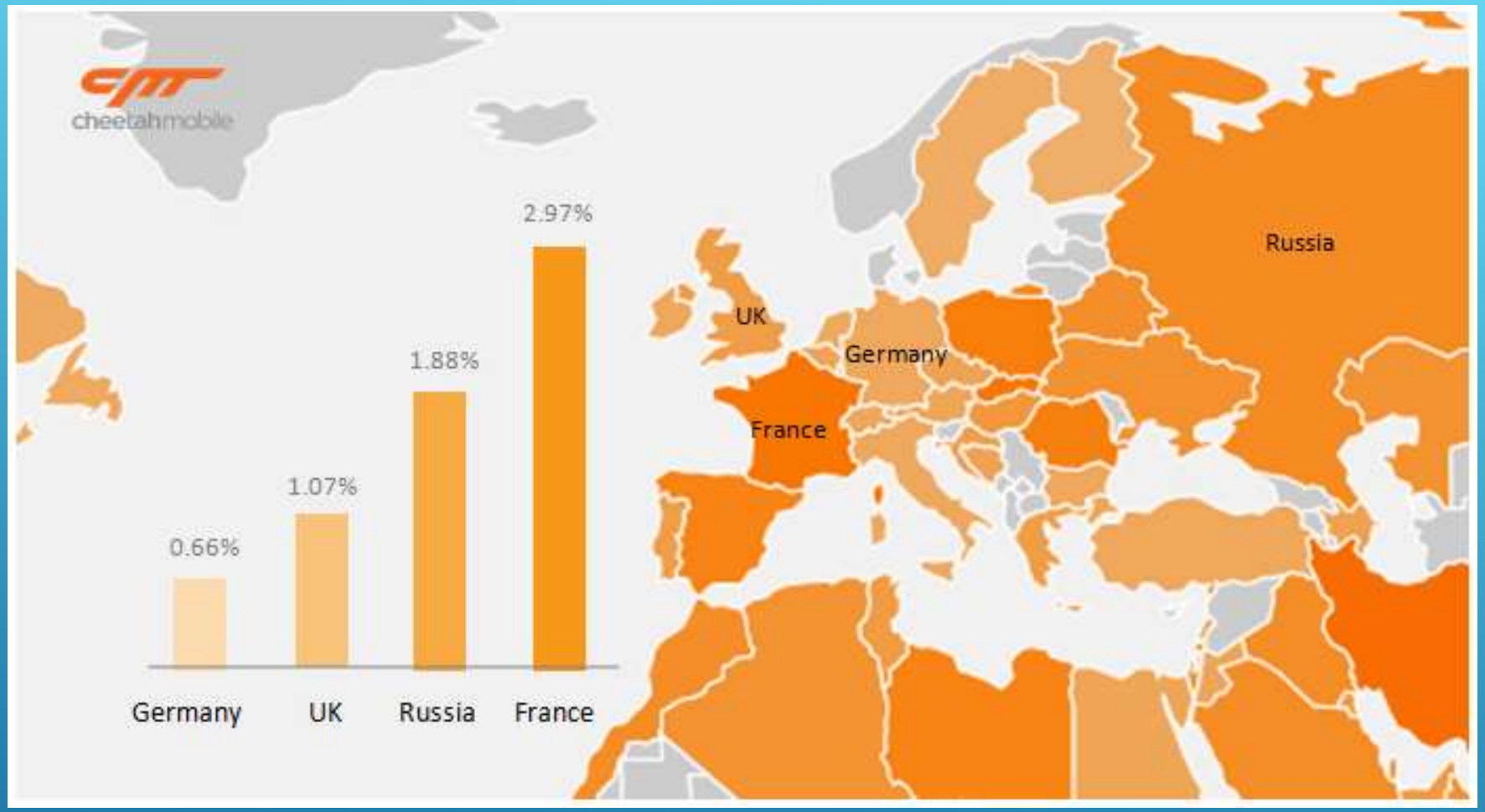
全球病毒感染形式


cheetahmobile
4.00%
3.50%
3.00%
2.50%
2.00%
1.50%
1.00%
0.50%
0.00%
3.55%
2.96%
2.45%
1.80%
2.97%
1.88%
1.07%
0.66%
1.07%
0.68%
0.67%
0.59%
伊朗 印度 中国 马来
法国 俄罗斯 英国 德国
墨西哥 美国 巴西 加拿大
亚洲
欧洲
美洲

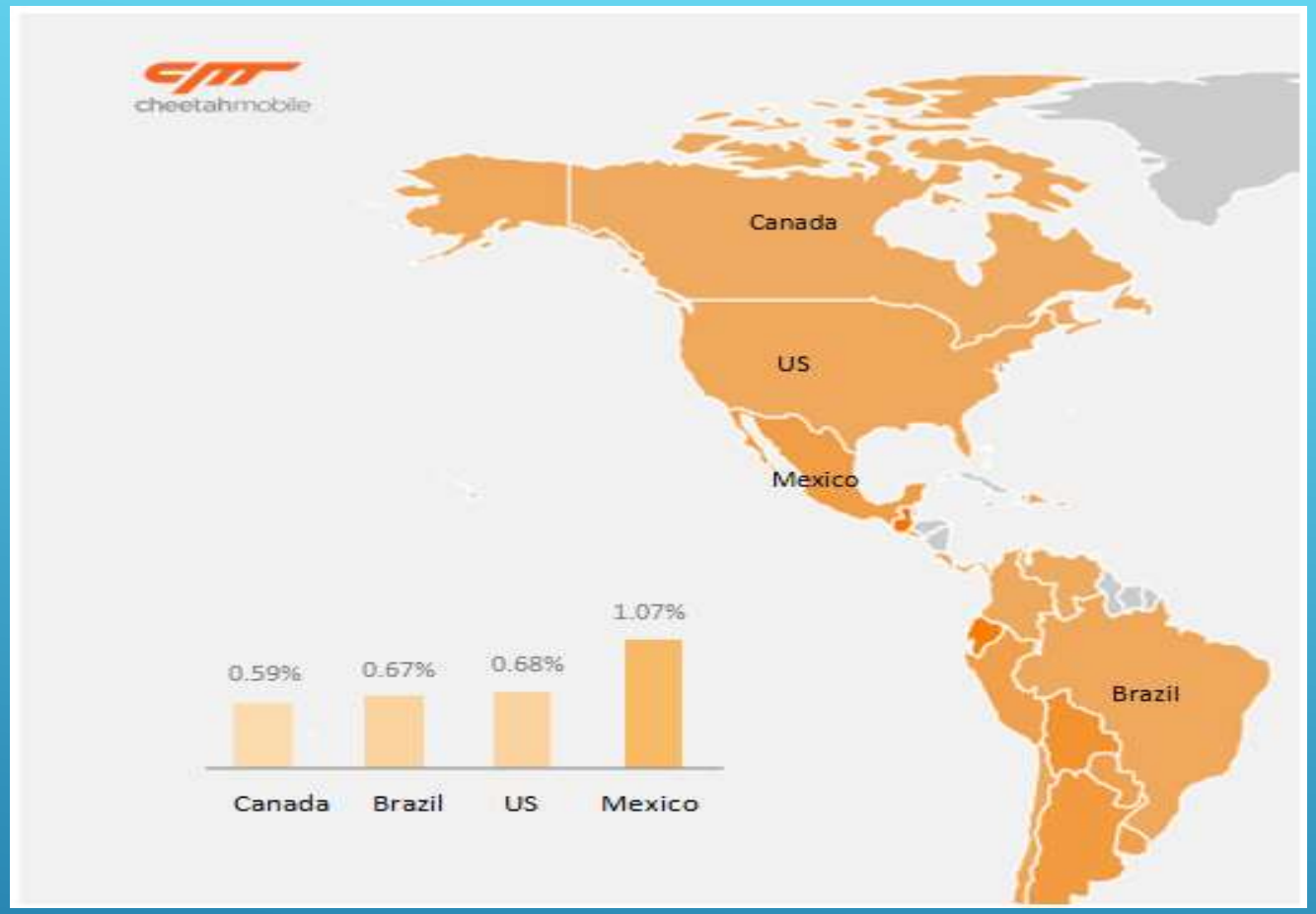
全球病毒感染形式


cheetahmobile
China
India
Vietnam
Malaysia
1.80%
2.45%
2.96%
3.65%
Malaysia
China
India
Vietnam

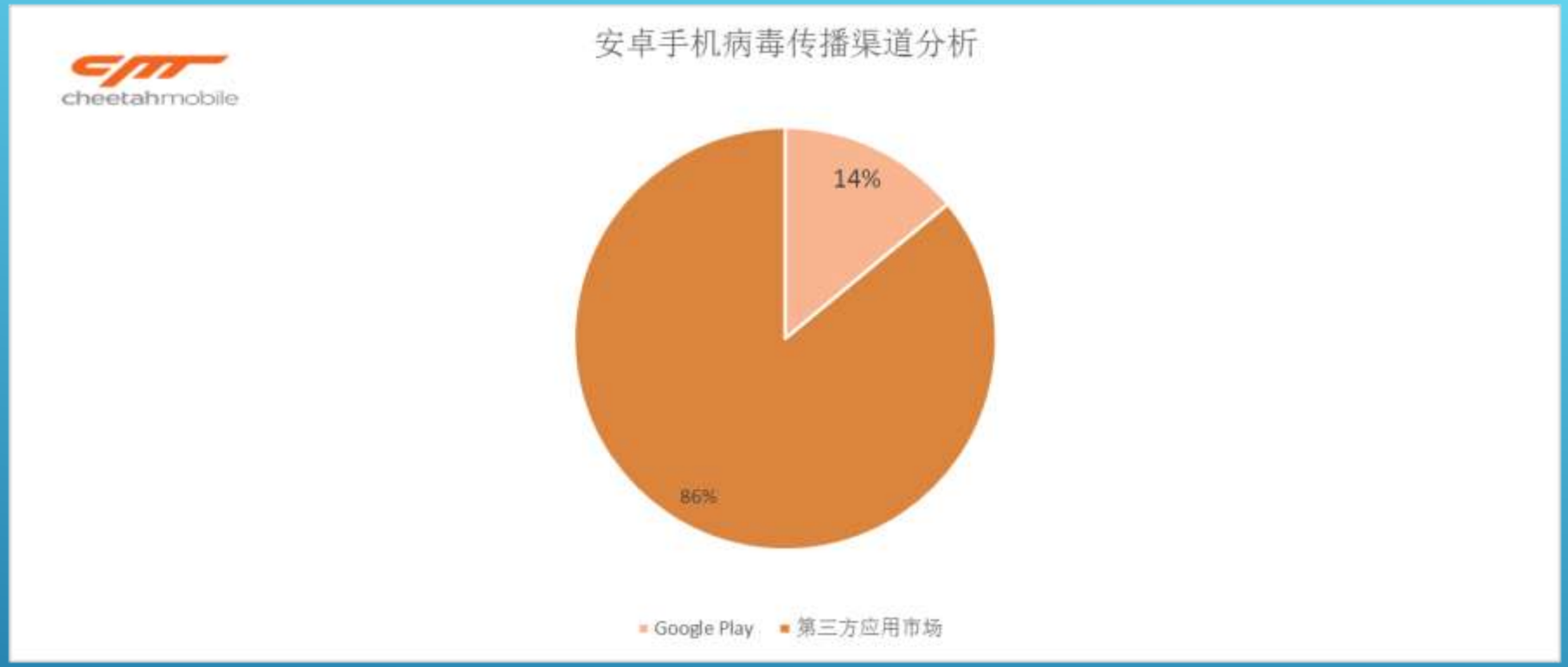
亚洲地区病毒感染情况


cheetahmobile
2.97%
1.88%
1.07%
0.66%
Germany
UK
Russia
France
Russia
UK
Germany
France

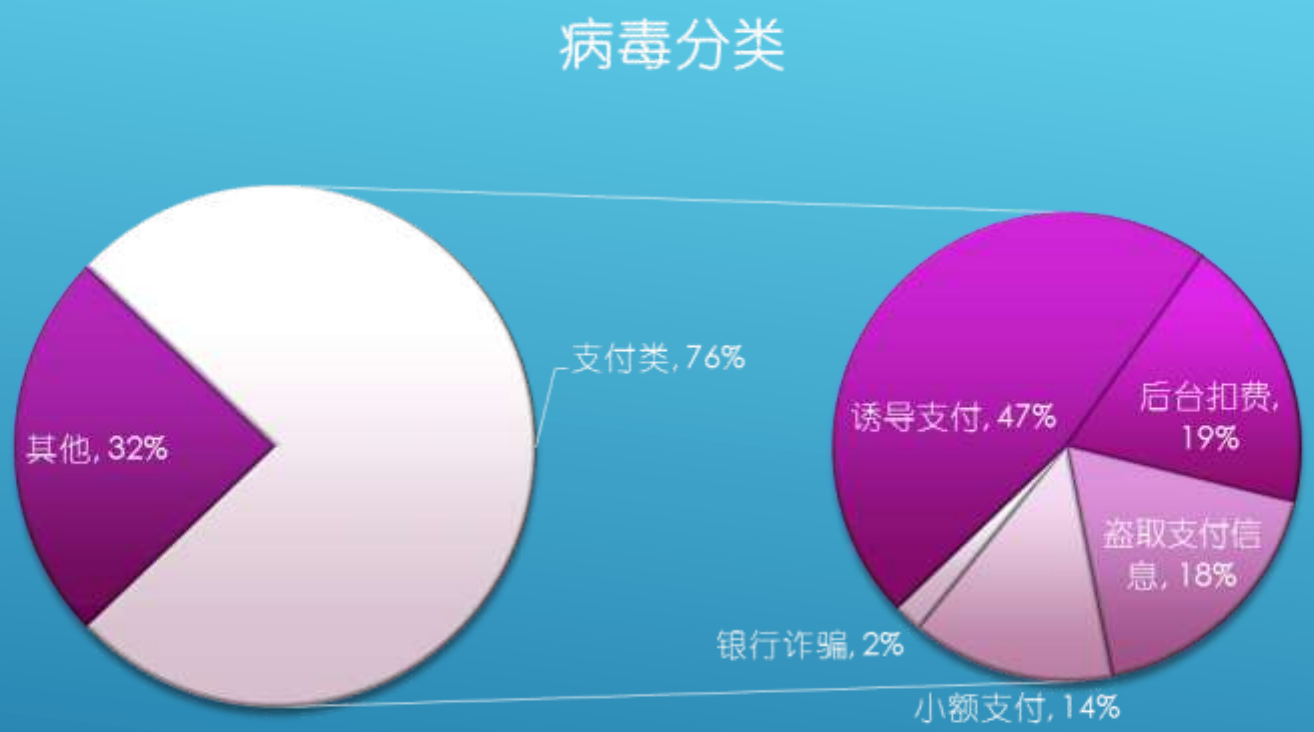
欧洲地区感染情况


cheetahmobile
Canada
US
Mexico
Brazil
0.59%
0.67%
0.68%
1.07%
Canada
Brazil
US
Mexico

美洲地区病毒感染情况



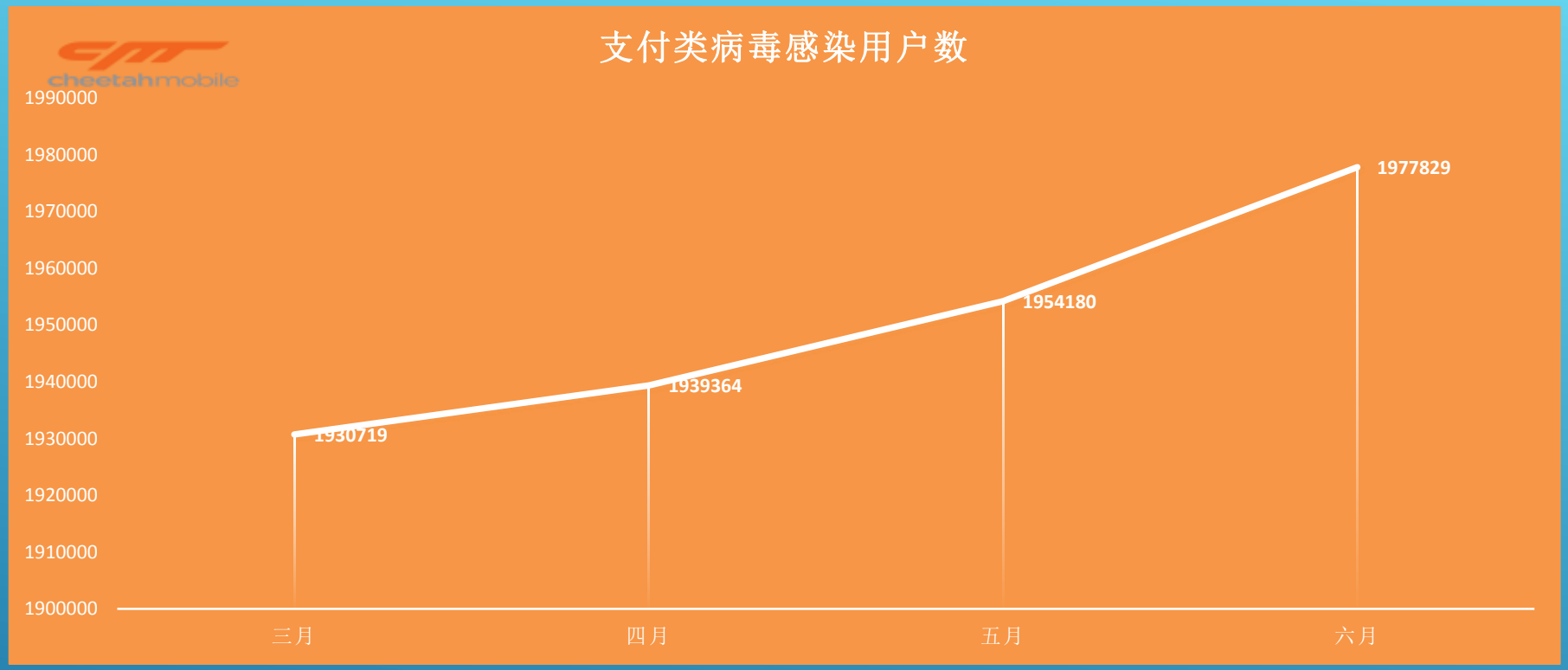
86%的病毒来自于第三方应用市场



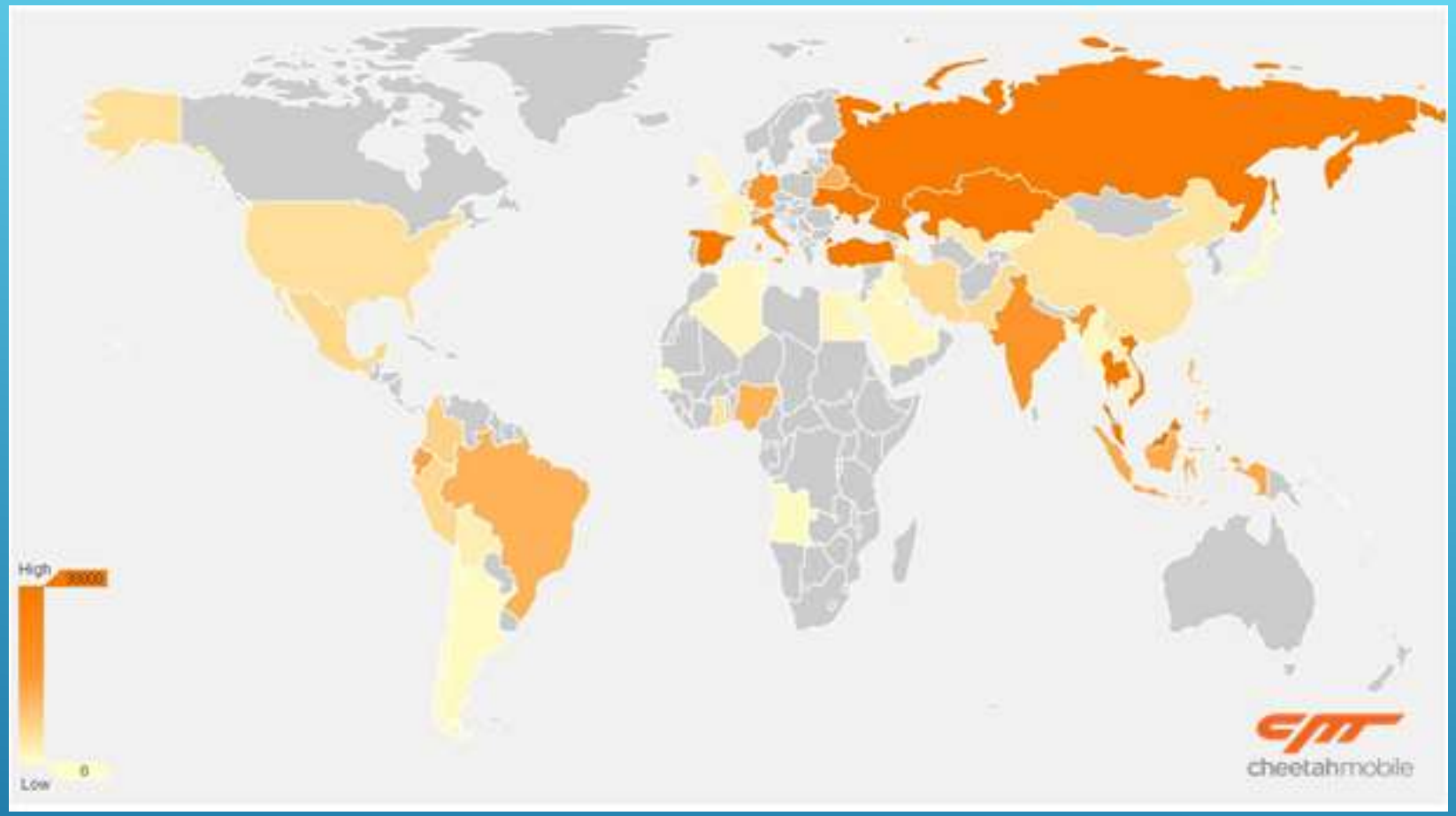
支付类病毒分析


支付类病毒样本变种数量
7000
6000
5000
4000
3000
2000
1000
0
1165
1816
1080
1571
1161
2015
3524
5588
6359
2013年7月
2013年8月
2013年9月
2013年10月
2013年11月
2013年12月
2014年1月
2014年2月
2014年3月
2014年4月
2014年5月
2014年6月

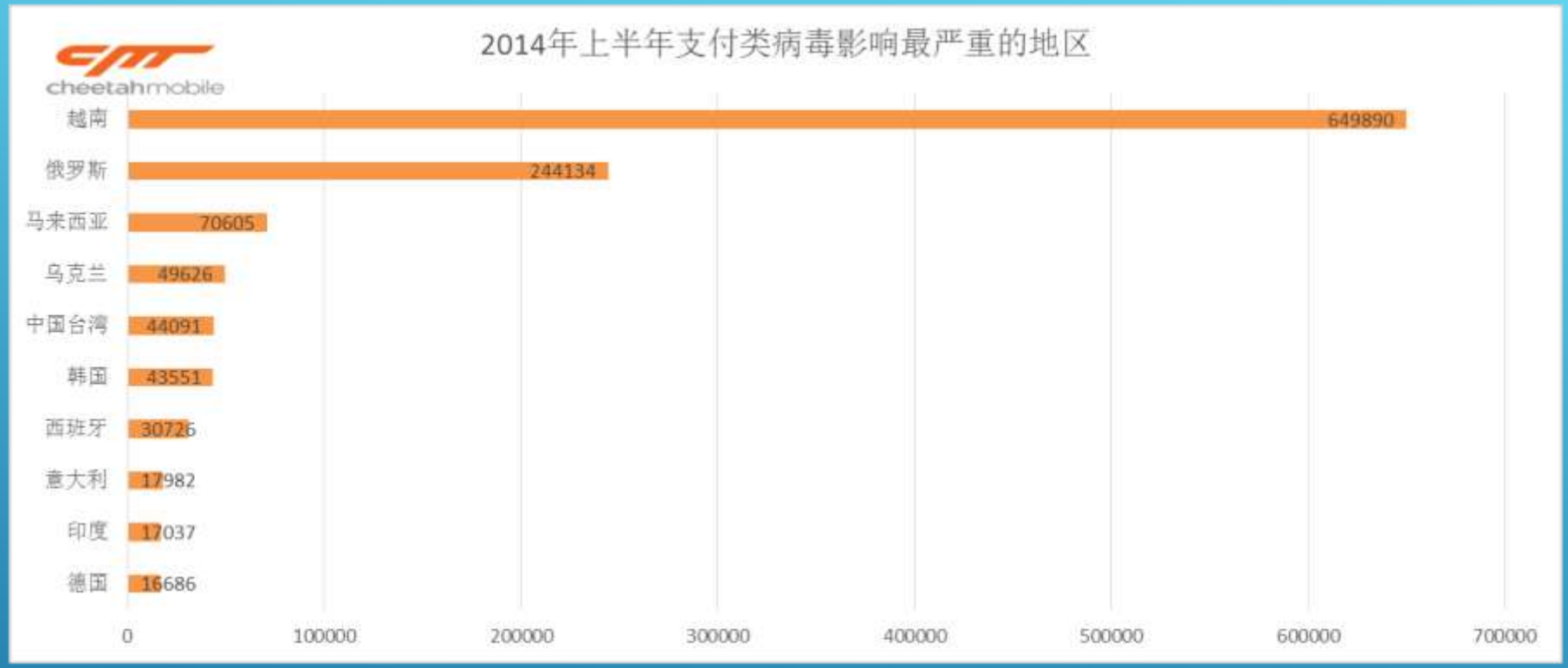
支付类病毒增长4倍


支付类病毒感染用户数
1990000
1980000
1970000
1960000
1950000
1940000
1930000
1920000
1910000
1900000
1930719
1939364
1954180
1977829
三月
四月
五月
六月

中毒用户持续增长



上半年全球支付类病毒中毒地区分布



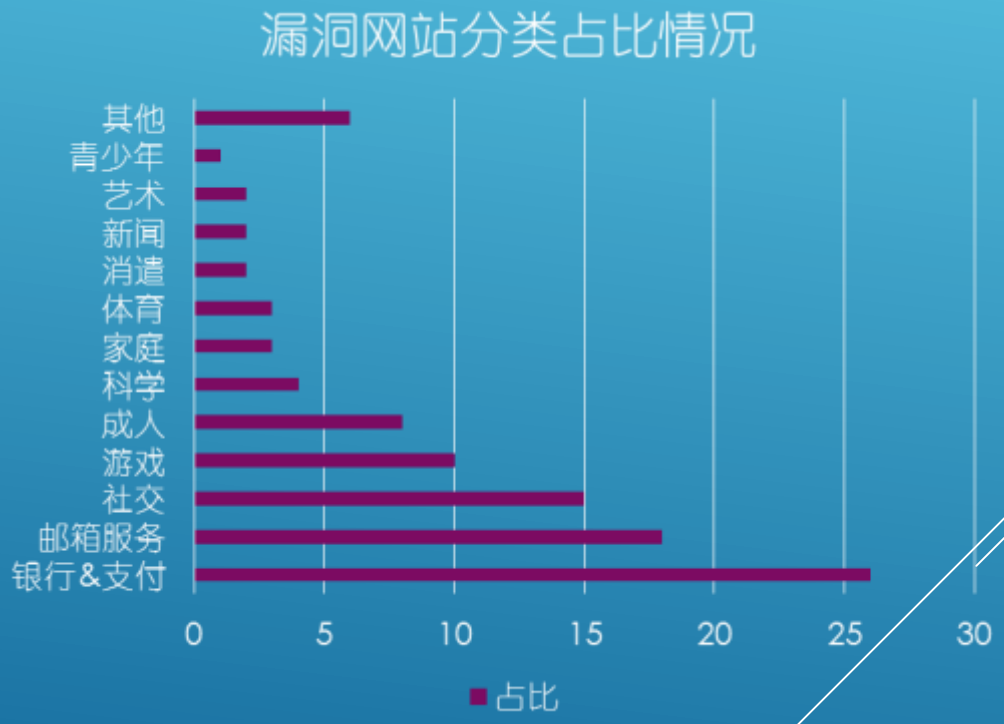
上半年支付类病毒高中毒地区

上半年安全事件与热点病毒回顾

心脏出血漏洞

- 102个国家

- 1100万台服务器



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

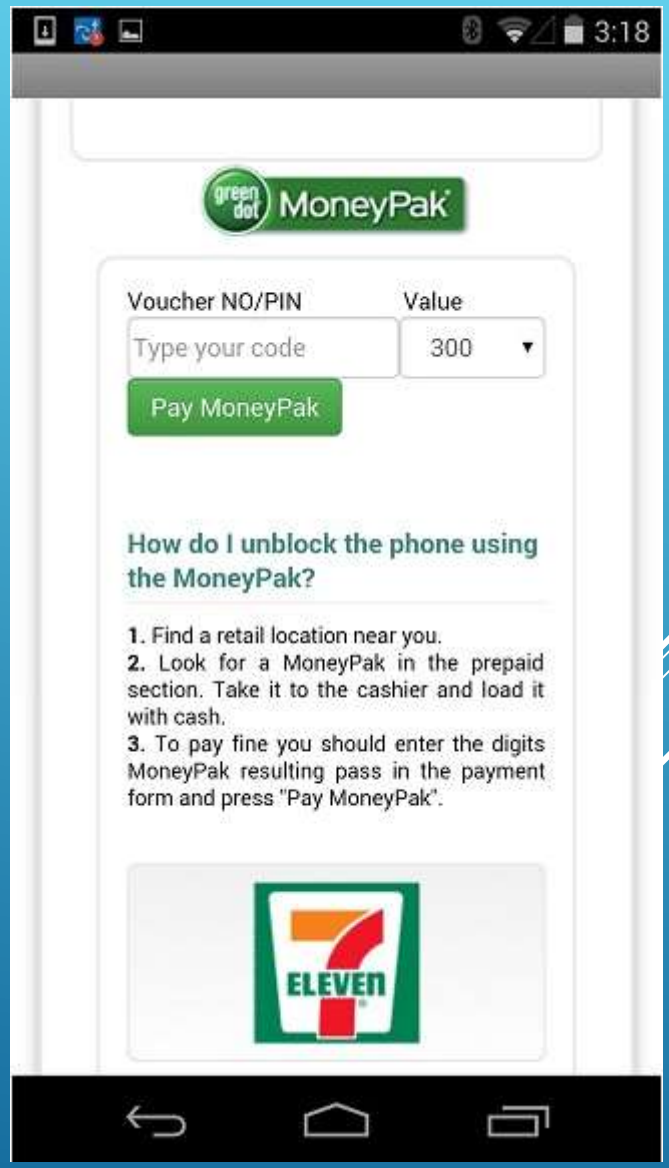
SD卡加密

弹窗强制用户付费

判断用户是否付费

卸载

病毒流程



“宅急便”手机病毒

- 每日2万条
- 感染200万
- 中毒率10%
- 千万级吸费金额

病毒特点

- 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

盈利模式


另一只已经感染病毒的手机发送SMS钓鱼短信
用户收到钓鱼短信
受骗下载安装病毒
病毒利用受骗用户电话进行购物
电商小额付费
病毒拦截小额付费认证SMS短信并偷偷帮用户确认交易
病毒偷取用户通讯录，利用用户手机发送钓鱼短信给更多朋友

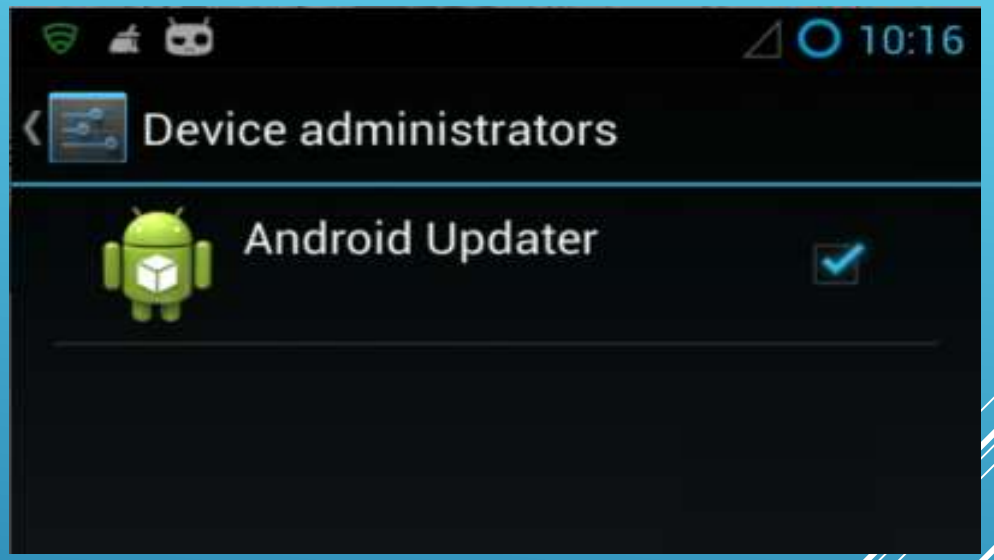
- 俄罗斯感染量最高的病毒类型
- 每日有6000用户中招
- 防毒软件无法卸载
- 必须使用特殊的清毒逻辑

顽固木马系列病毒


对抗方式
利用漏洞
在取消时进行干扰
在取消激活后强制激活

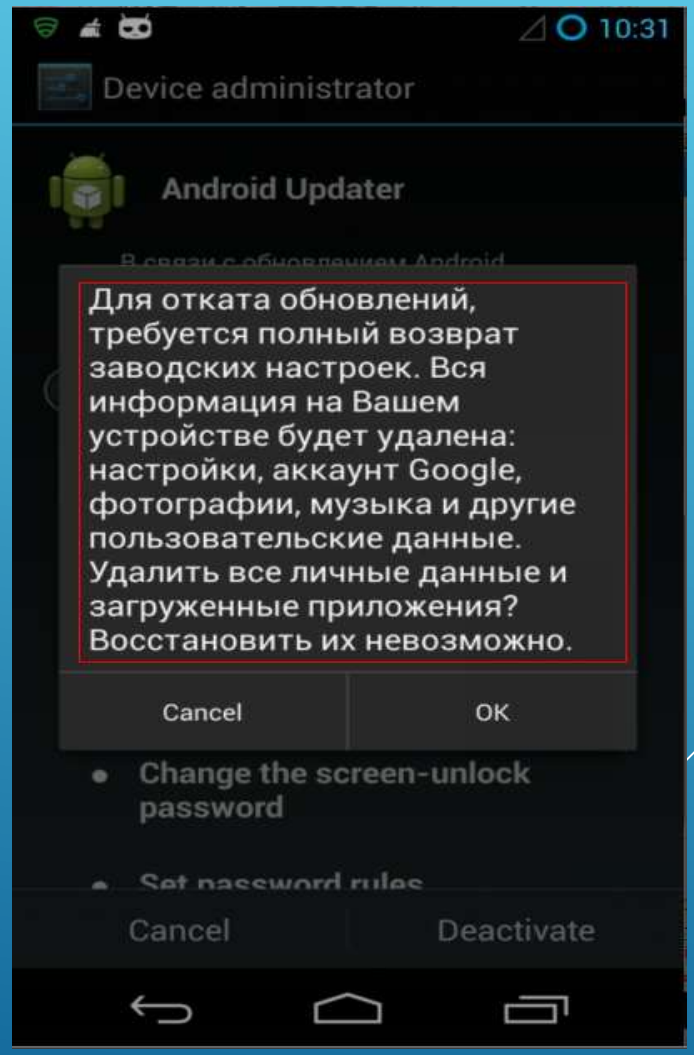
利用漏洞

- 激活成功后不显示在设备管理器列表中



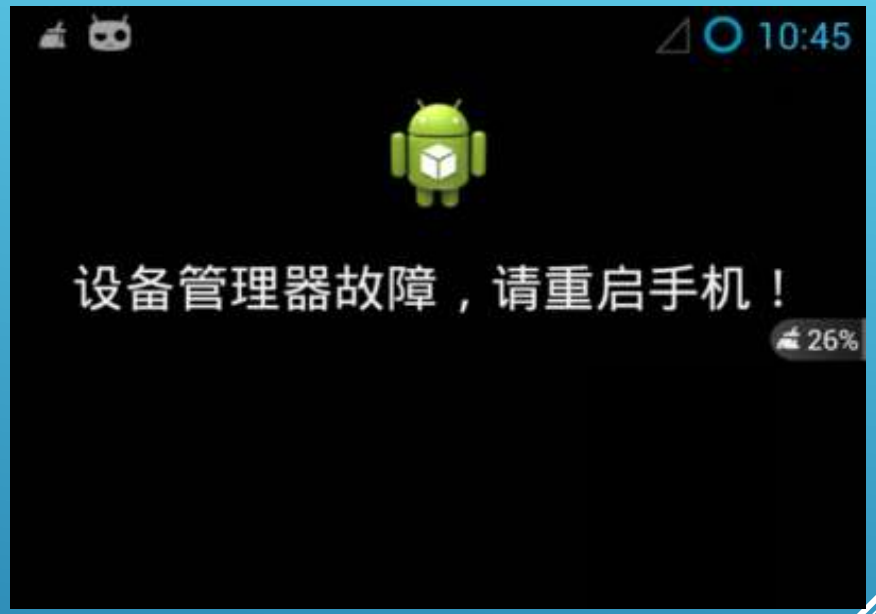
- 修改确认对话框里的描述，恐吓用户
- 提示“如果点击确认会导致数据丢失“

取消设备管理器时进行干扰



取消设备管理器时的对抗

- 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



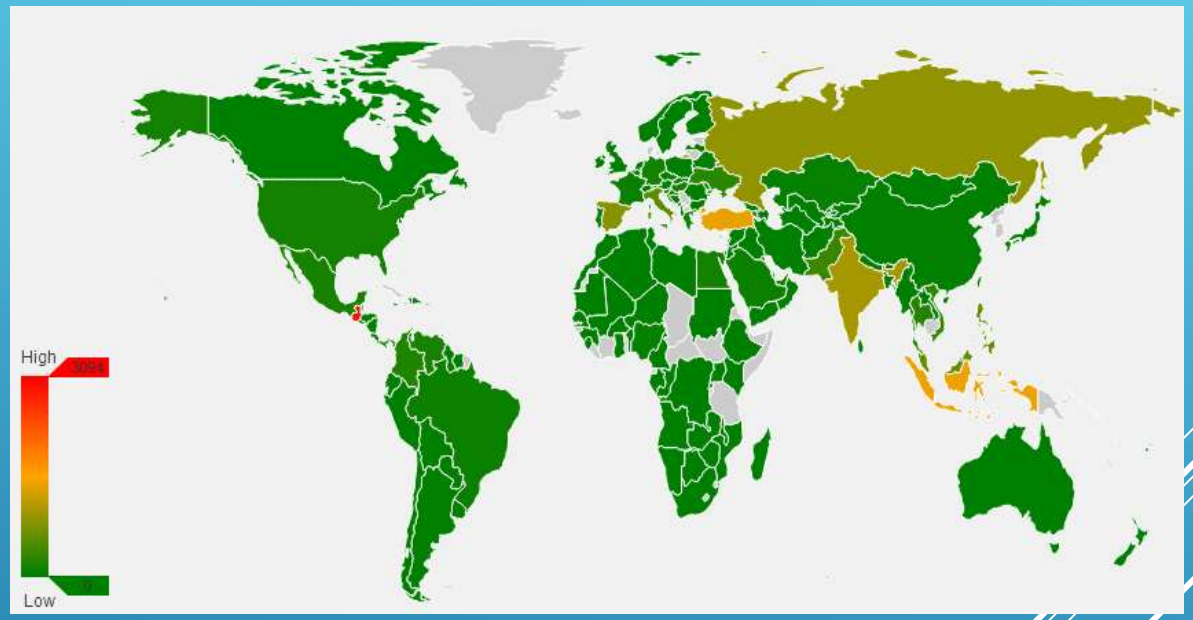
国家	感染量
Russia	9307
Ukraine	1833
Kazakhstan	1800
Belarus	390
Korea, South	260
Uzbekistan	147
United States of America	67
Kyrgyzstan	48
Azerbaijan	46
Tajikistan	42
Armenia	42
China	38

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

谢谢！