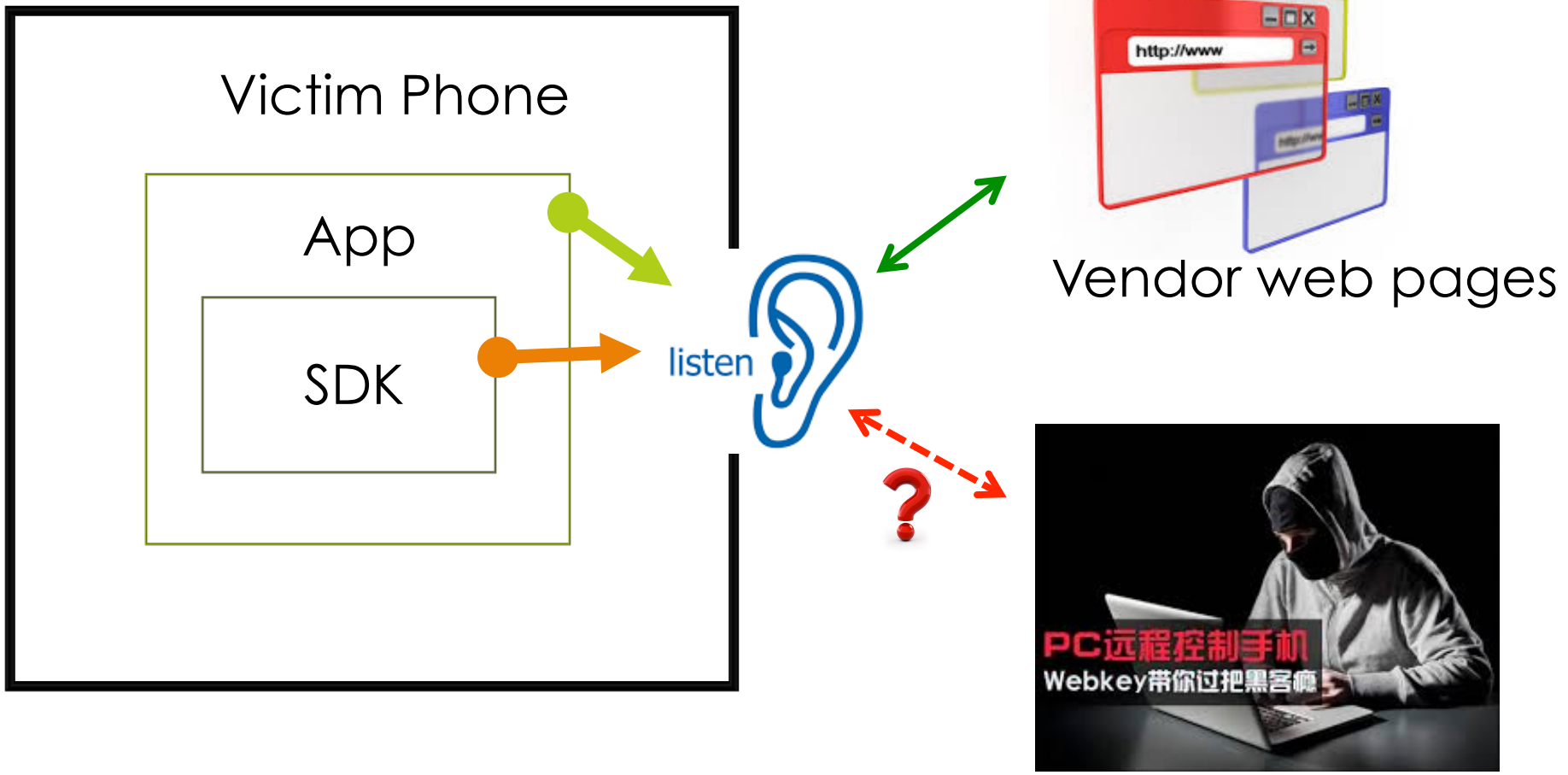
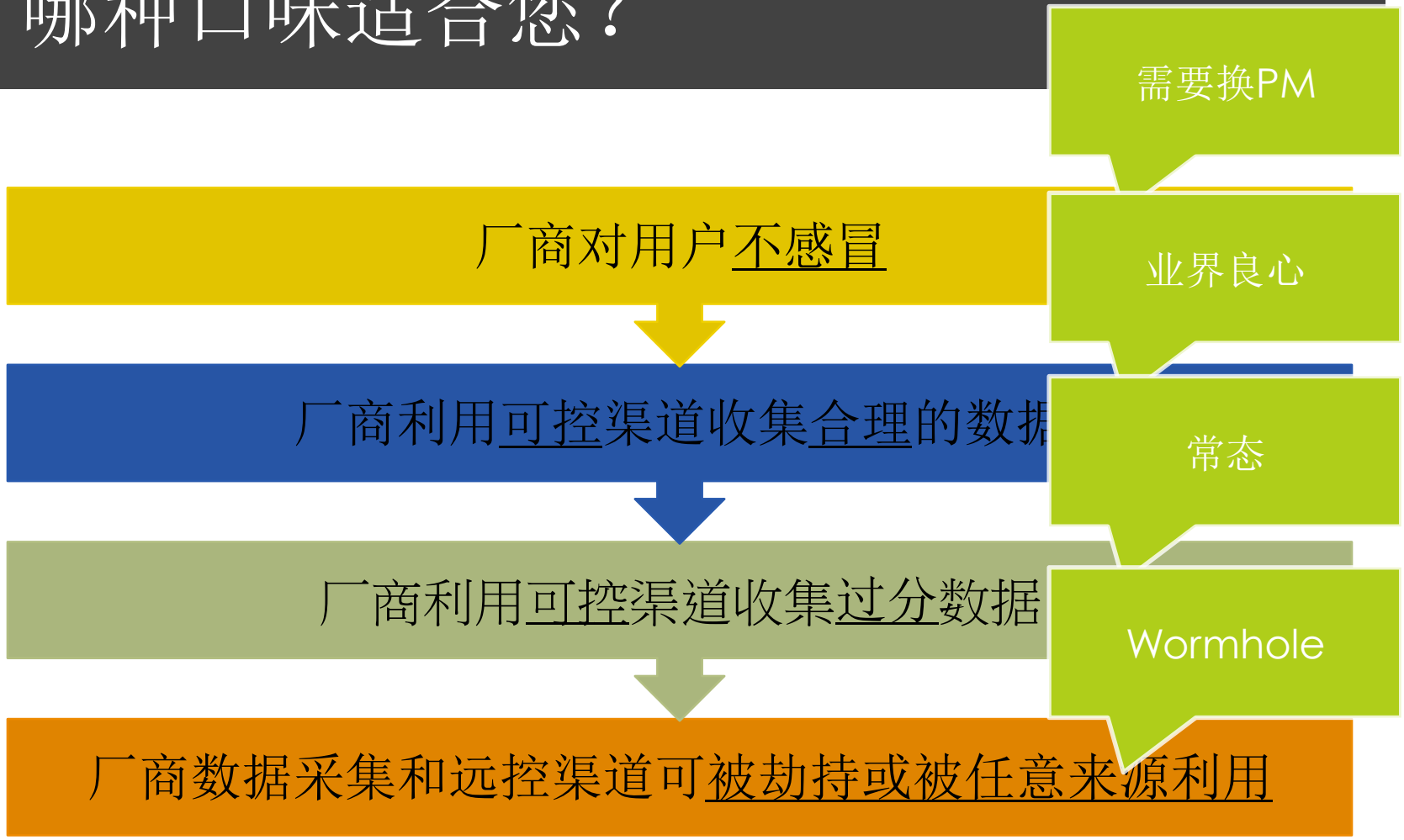
Wormhole 前后一百天

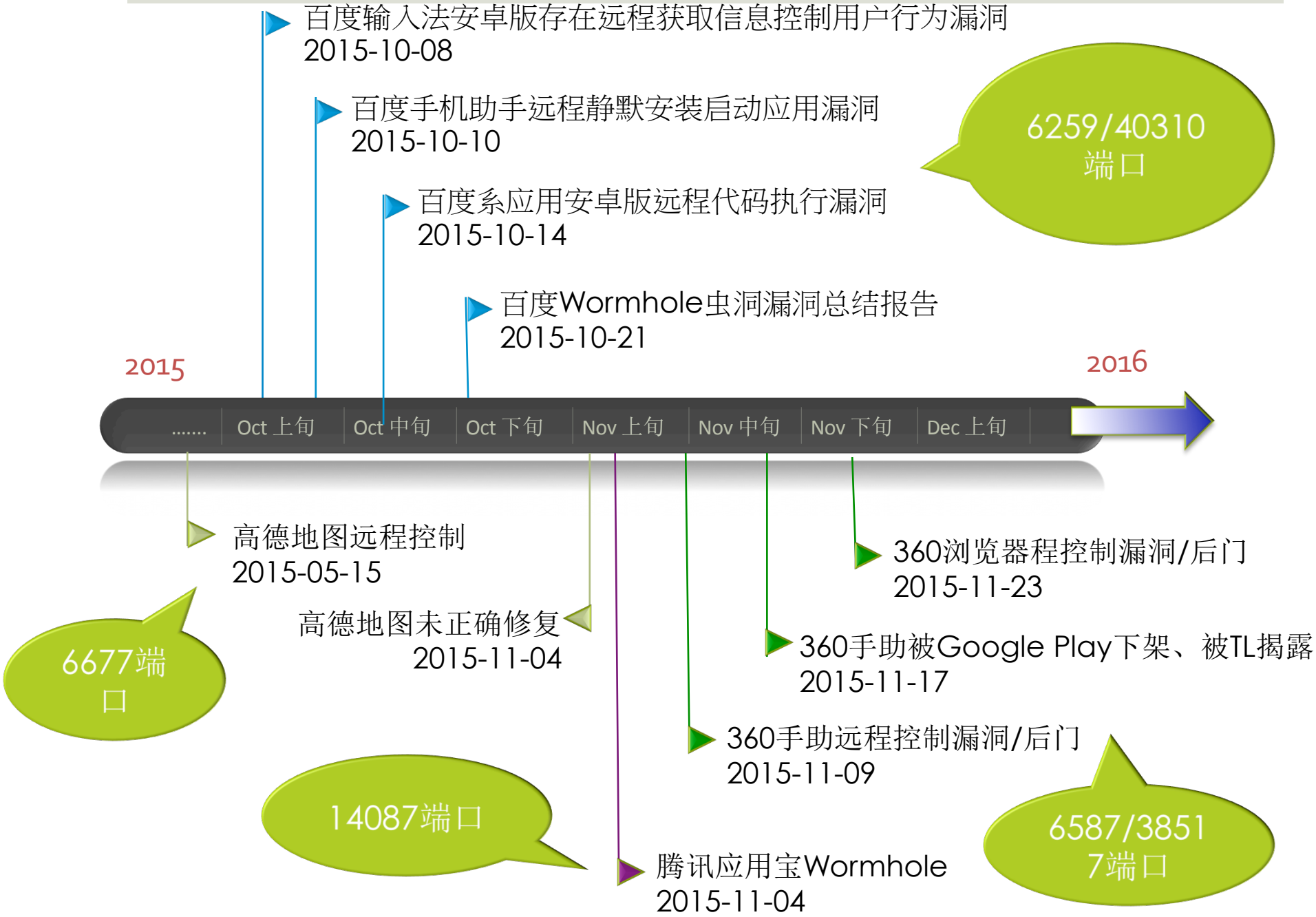
仲震宇 张煜龙 冯侦探 韦韬
Baidu X-Lab | 百度安全实验室

Wormhole Overview



哪种口味适合您？


厂商对用户不感冒
厂商利用可控渠道收集合理的数据
厂商利用可控渠道收集过分数据
厂商数据采集和远控渠道可被劫持或被任意来源利用
需要换PM
业界良心
常态
Wormhole


百度输入法安卓版存在远程获取信息控制用户行为漏洞
2015-10-08
百度手机助手远程静默安装启动应用漏洞
2015-10-10
百度系应用安卓版远程代码执行漏洞
2015-10-14
百度Wormhole虫洞漏洞总结报告
2015-10-21
6259/40310
端口
2015
2016
.....
Oct 上旬
Oct 中旬
Oct 下旬
Nov 上旬
Nov 中旬
Nov 下旬
Dec 上旬
高德地图远程控制
2015-05-15
6677端
口
高德地图未正确修复
2015-11-04
360浏览器程控制漏洞/后门
2015-11-23
360手助被Google Play下架、被TL揭露
2015-11-17
360手助远程控制漏洞/后门
2015-11-09
14087端口
腾讯应用宝Wormhole
2015-11-04
6587/3851
7端口

几种Wormhole现象

- 端口未限制任何来源
- 限制referrer（可以伪造）
- 对命令、访问来源等有所检查（不严谨的话可绕过）
- 使得本地无权限App获得信息或控制权

- WooYun-2015-145365
  - 百度输入法安卓版存在远程获取信息控制用户行为漏洞
- WooYun-2015-145718
  - 百度手机助手远程静默安装启动应用漏洞
- WooYun-2015-146617
  - 百度系应用安卓版远程代码执行漏洞
- WooYun-2015-148406
  - Wormhole虫洞漏洞总结报告

- 端口列表
  - 6259
  - 40310

Tencent 腾讯

- 端口列表
  - 14087
    - 可以远程截图、安装卸载app、操作文件、收集信息

- WooYun-2015-152507
  - 360手机助手设计缺陷可进行部分远程操作
- WooYun-2015-153353
  - wormhole第二弹来袭:360某应用可远程静默安装app
- WooYun-2015-155003
  - 360手机浏览器wormhole漏洞可导致任意命令执行
- Trustlook
  - Yet another Wormhole Vulnerability – Meet the “DimensionDoor”

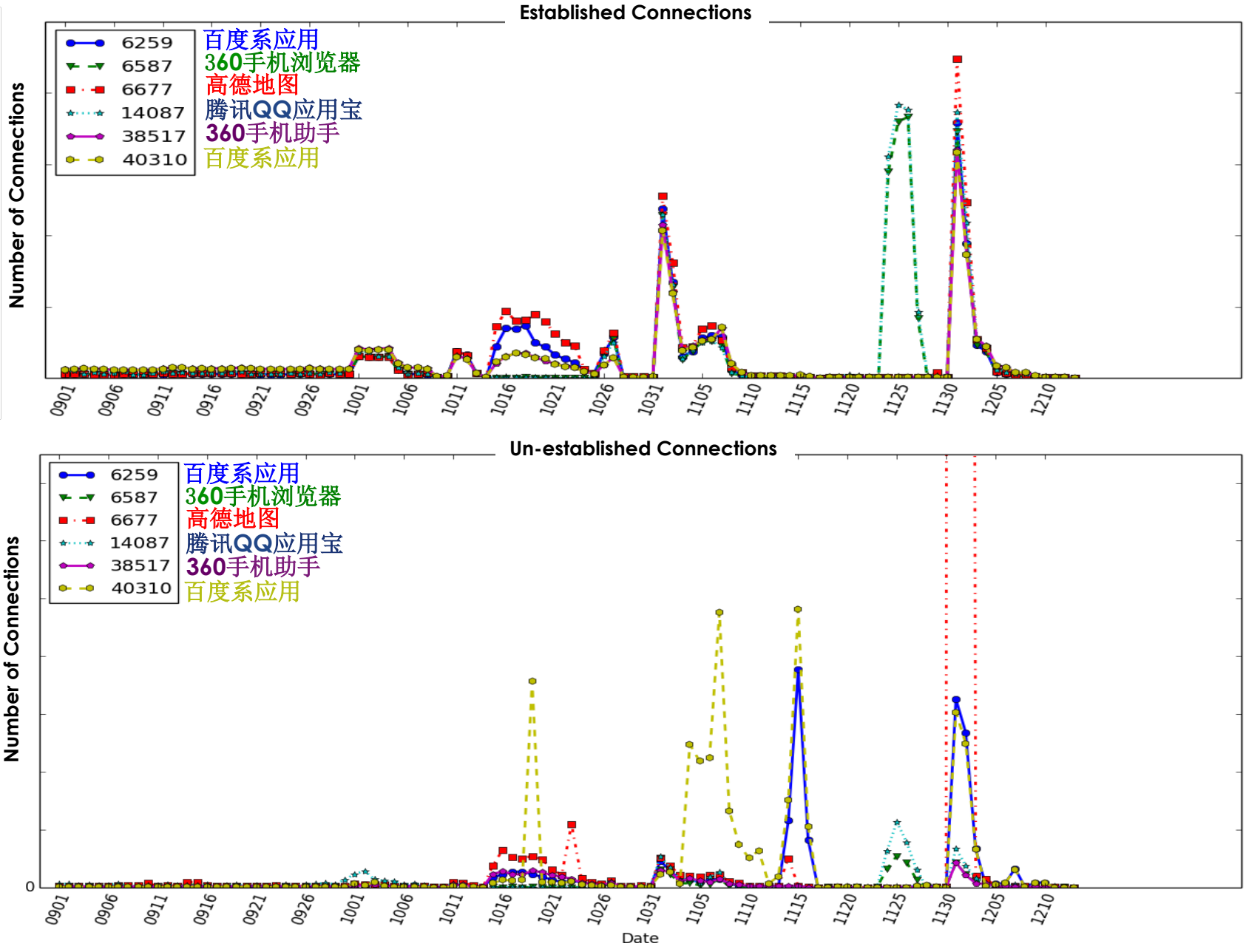
- 端口列表
  - 6587
  - 38517
    - 可以远程控制手机、安装卸载app、打开App、打开网页、搜集信息等

- WooYun-2015-114241
  - 高德地图远程获取手机的敏感信息可远程命令执行
- WormHole分析第二弹（乌云文库）
  - “在验证http_referer时，高德竟然用了contains()这个函数去遍历，修复并不彻底”

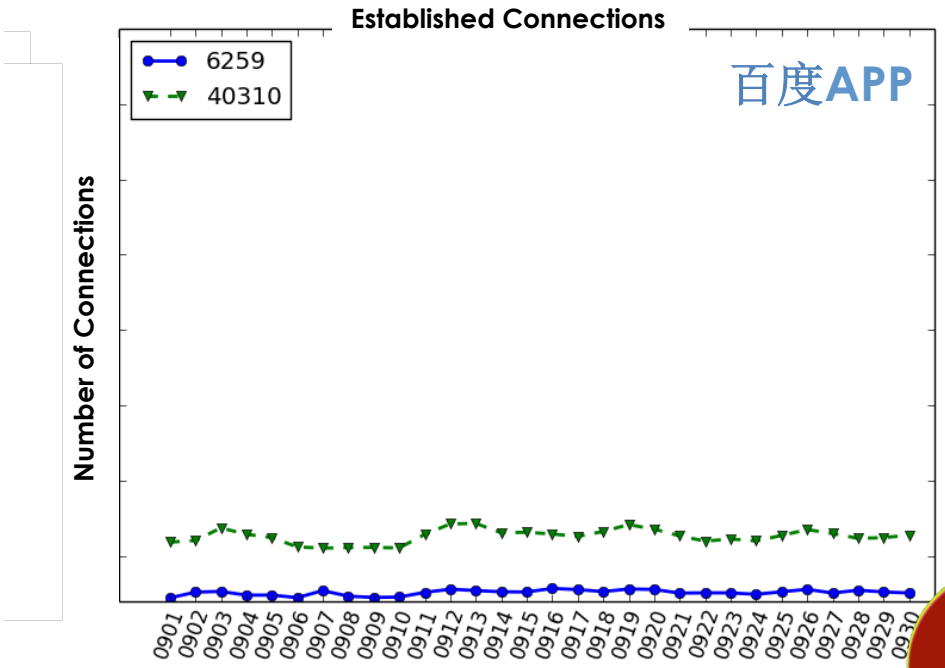
Wormhole端口总结

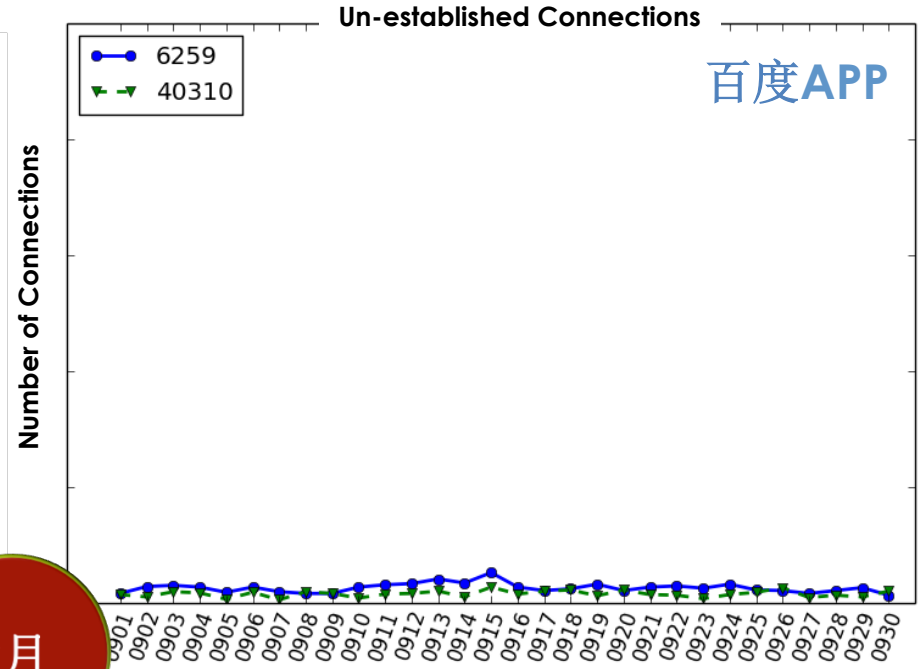
- 百度
  - 6259
  - 40310
- 腾讯
  - 14087
- 高德（阿里）
  - 6677
- 奇虎360
  - 6587
  - 38517

Wormhole tracking (09/01 ~ 12/13)

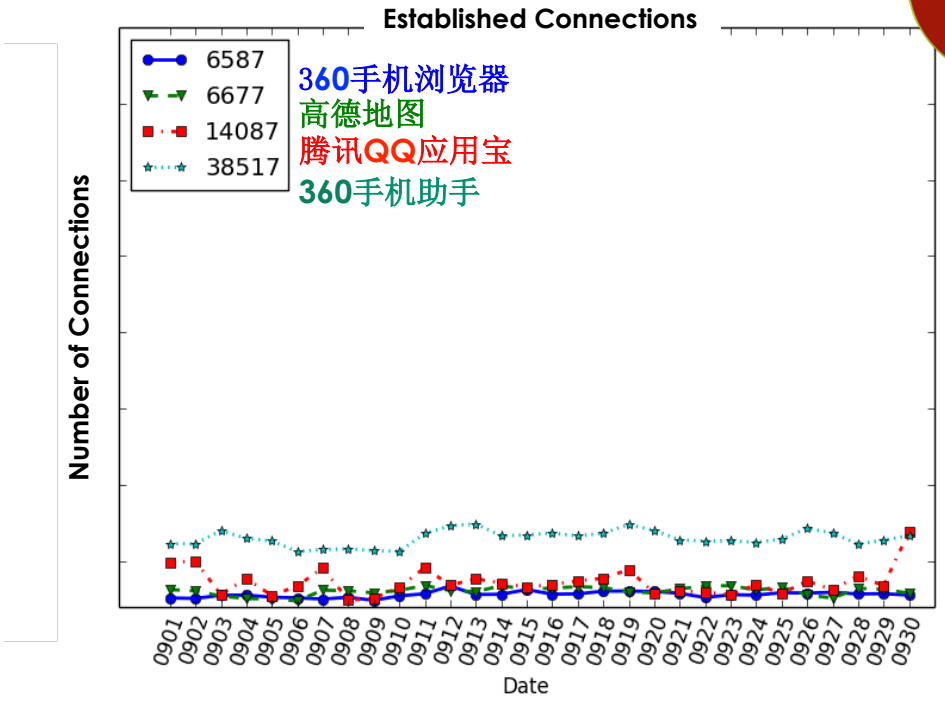


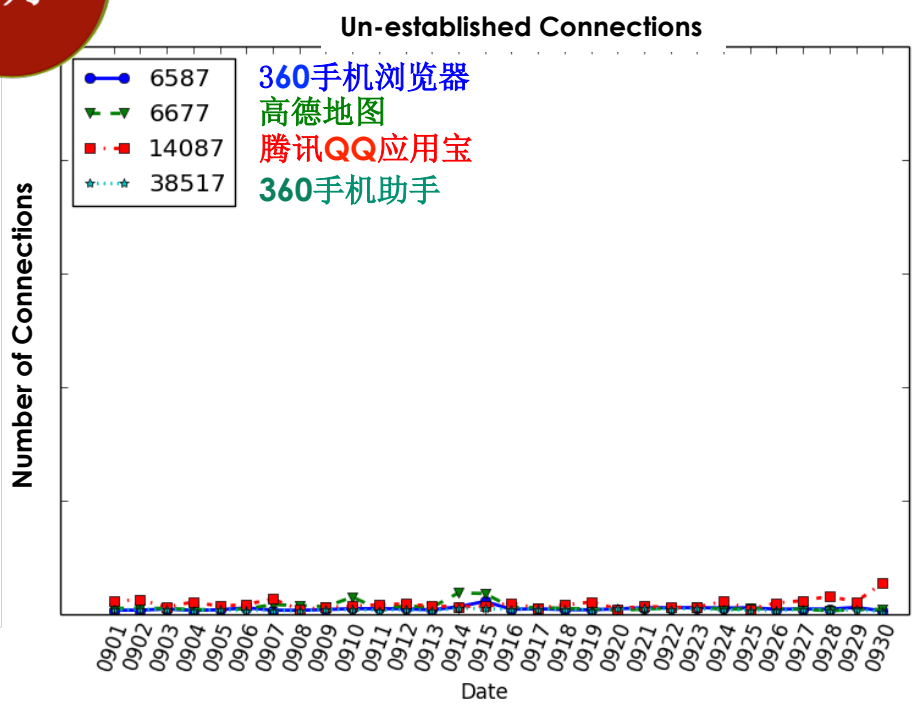
- 百度相关APP与其它厂家APP在四个不同阶段的每天Connections比较

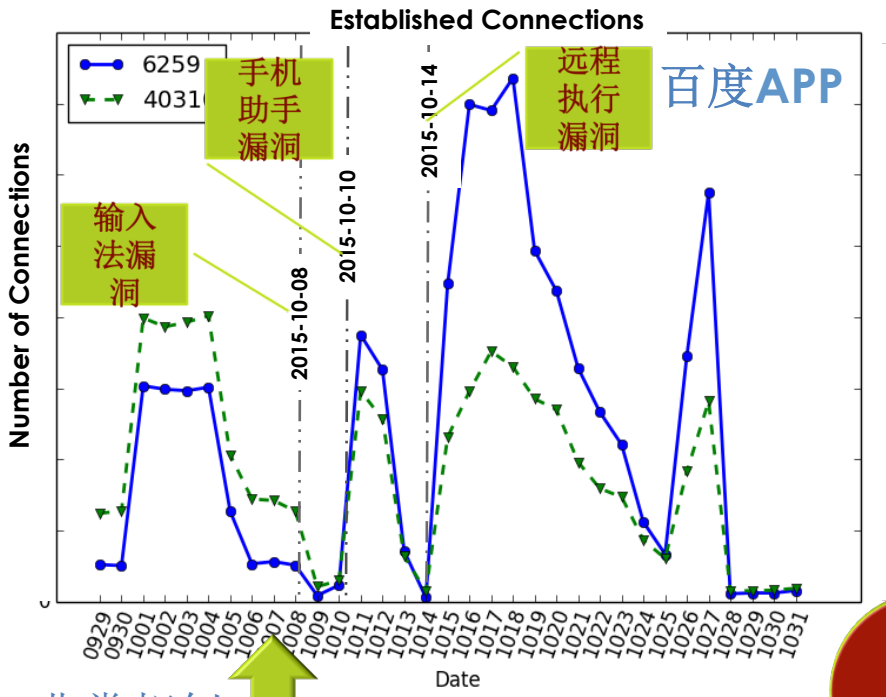

Established Connections
6259
40310
百度APP
Number of Connections

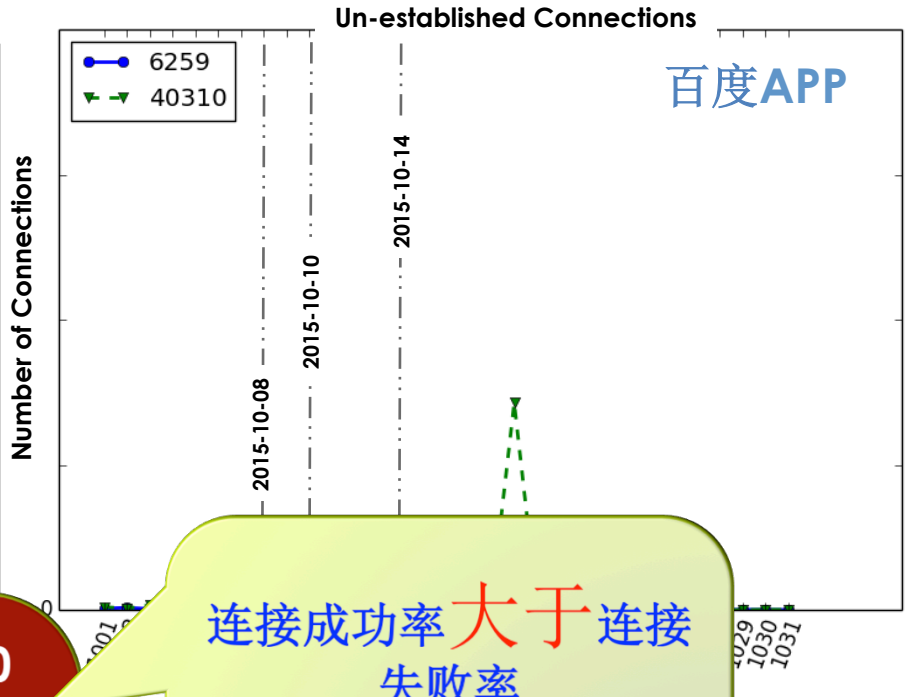

Un-established Connections
6259
40310
百度APP
Number of Connections

9月

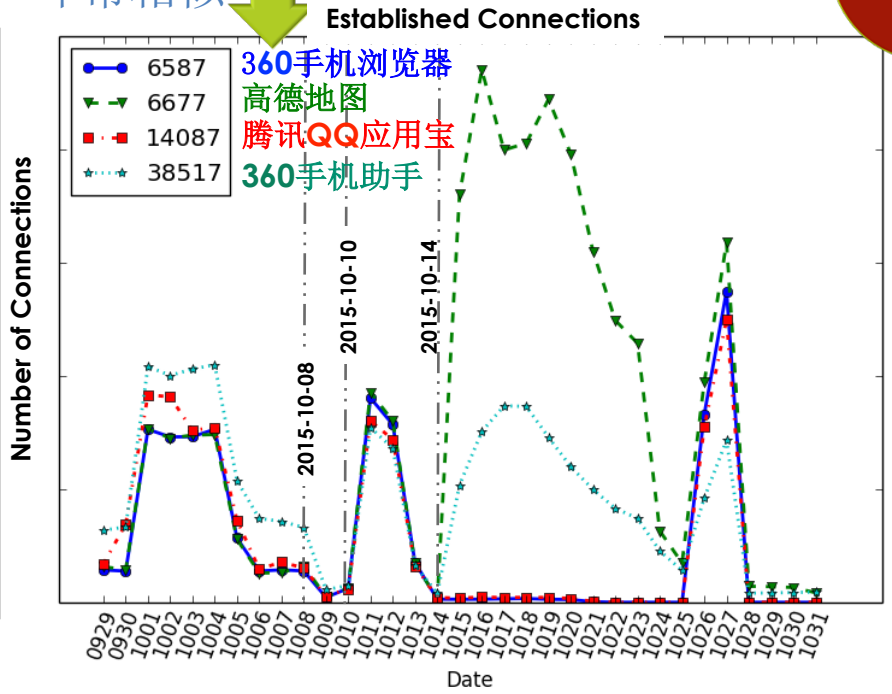

Established Connections
6587
6677
14087
38517
360手机浏览器
高德地图
腾讯QQ应用宝
360手机助手
Number of Connections
Date

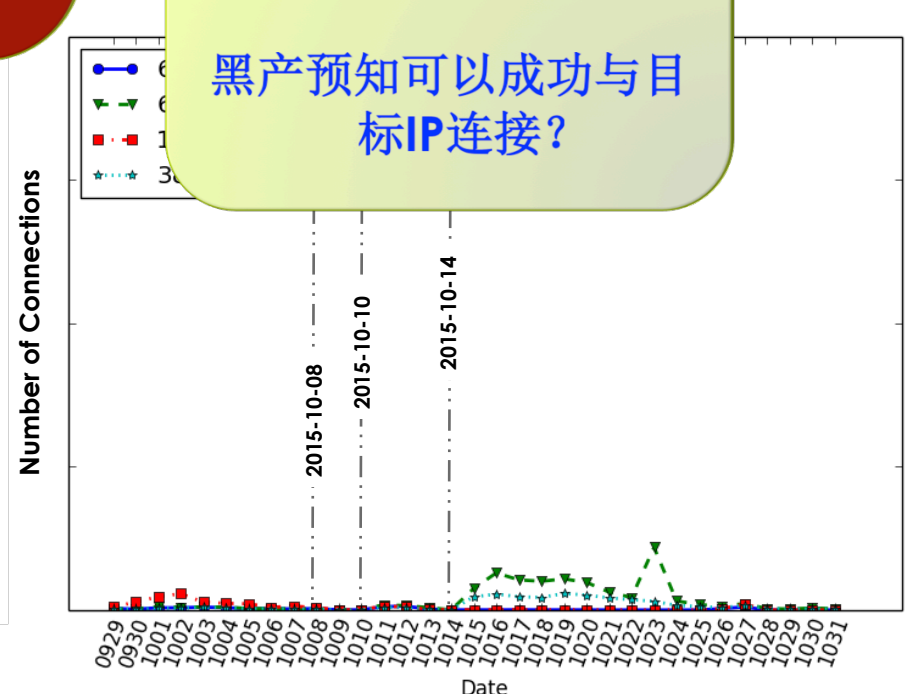

Un-established Connections
6587
6677
14087
38517
360手机浏览器
高德地图
腾讯QQ应用宝
360手机助手
Number of Connections
Date





非常相似



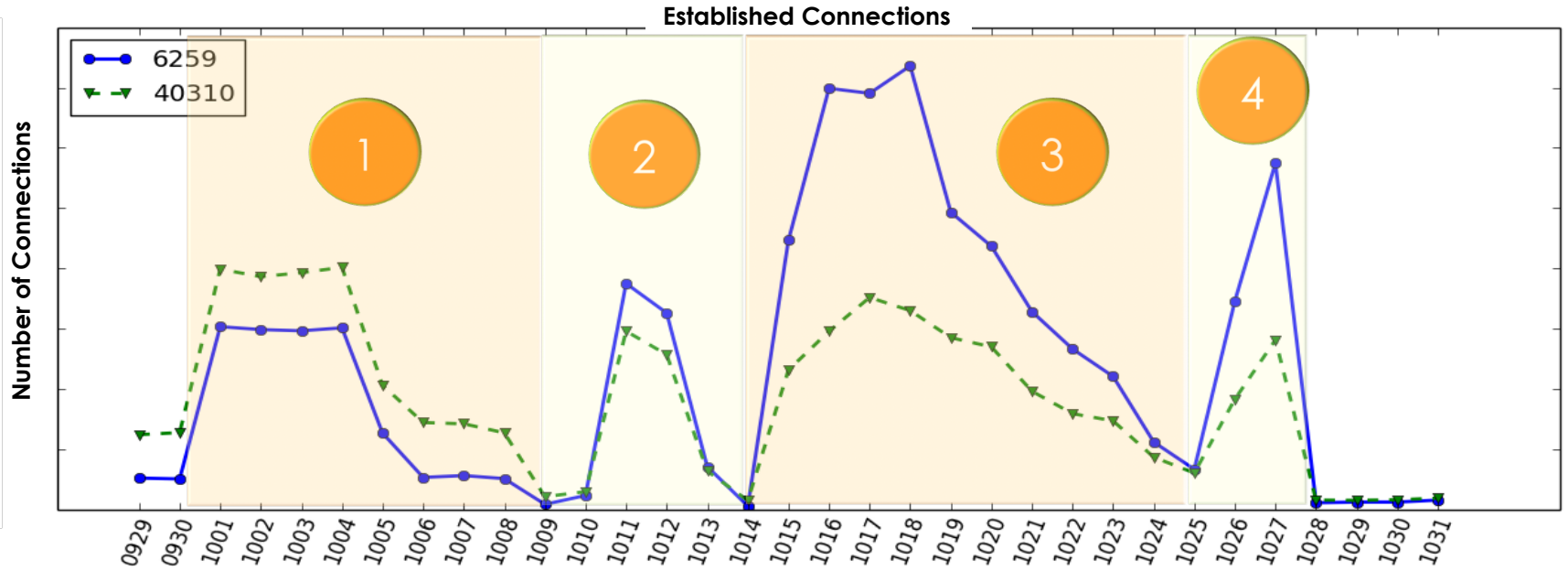


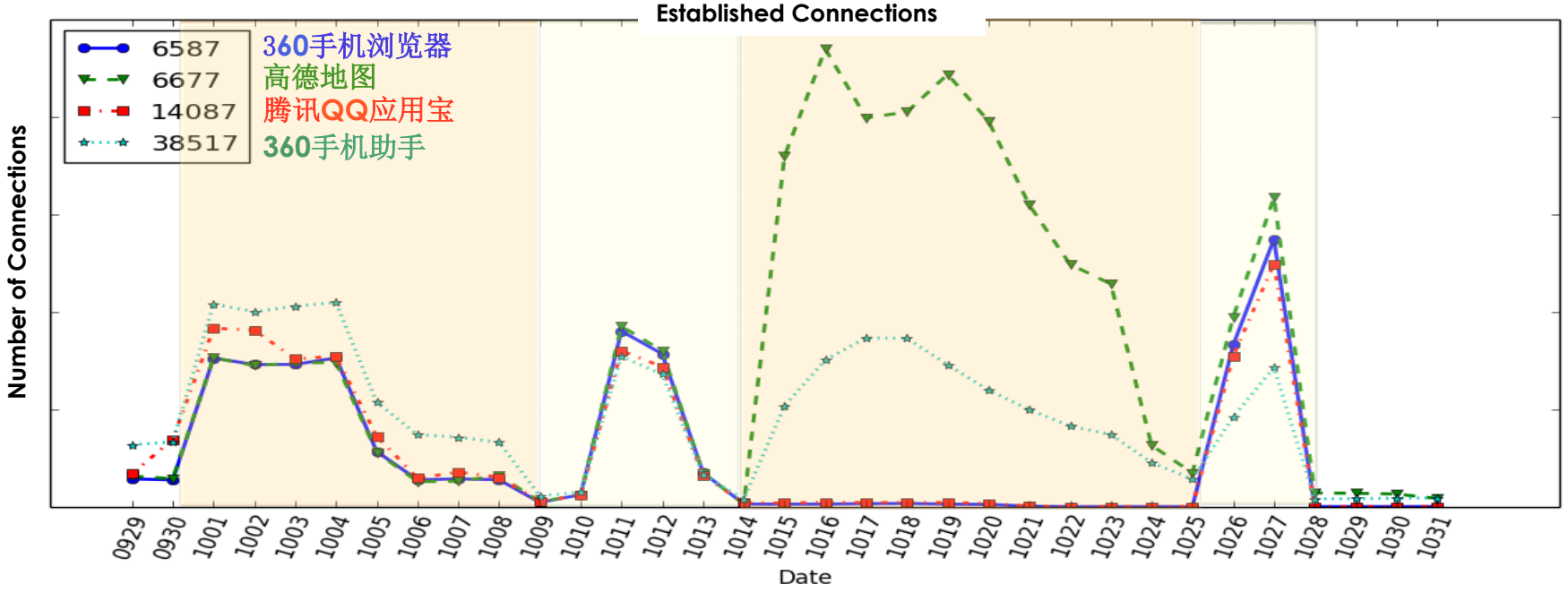
10月

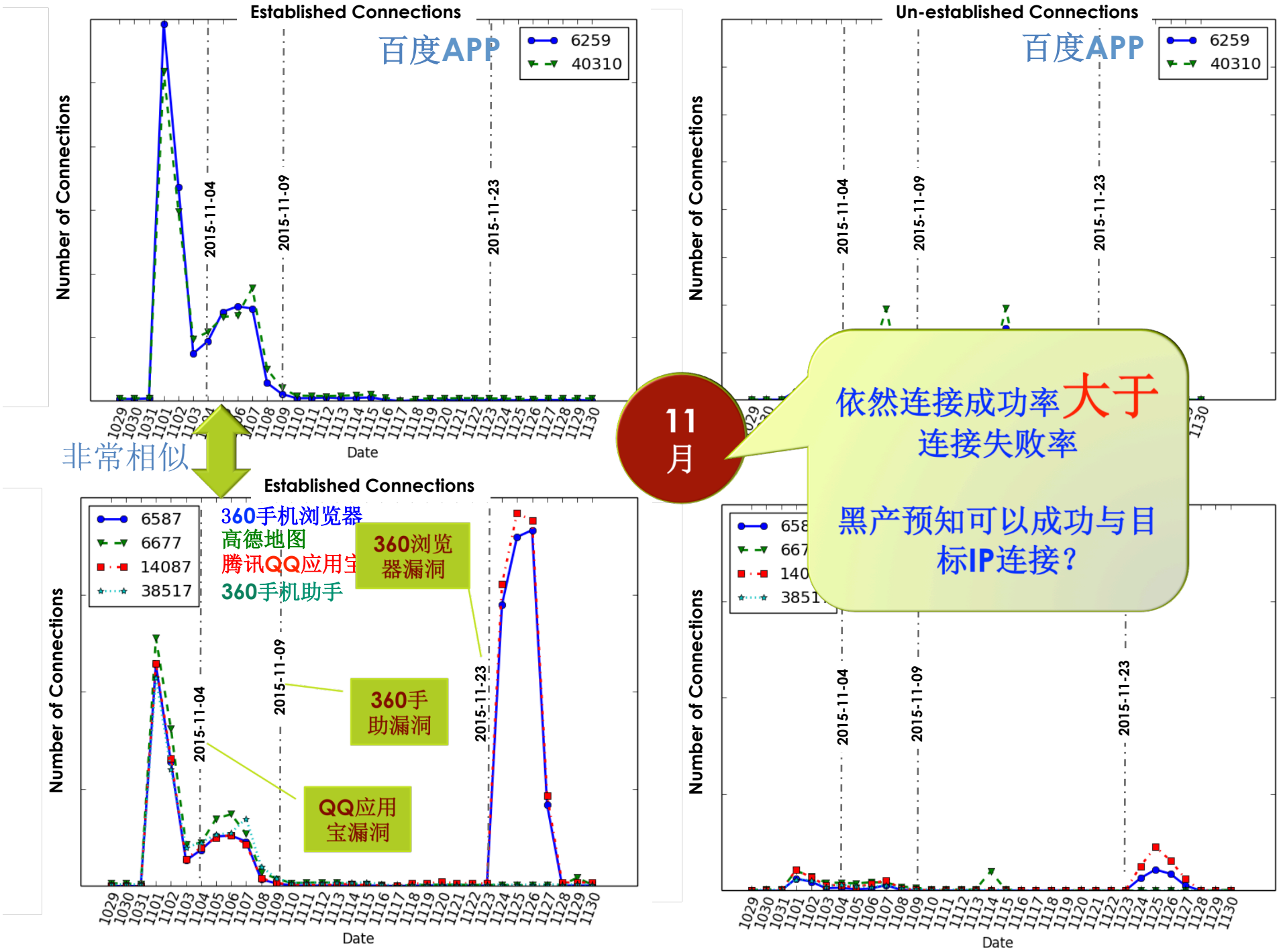
连接成功率大于连接失败率

黑产预知可以成功与目标IP连接？

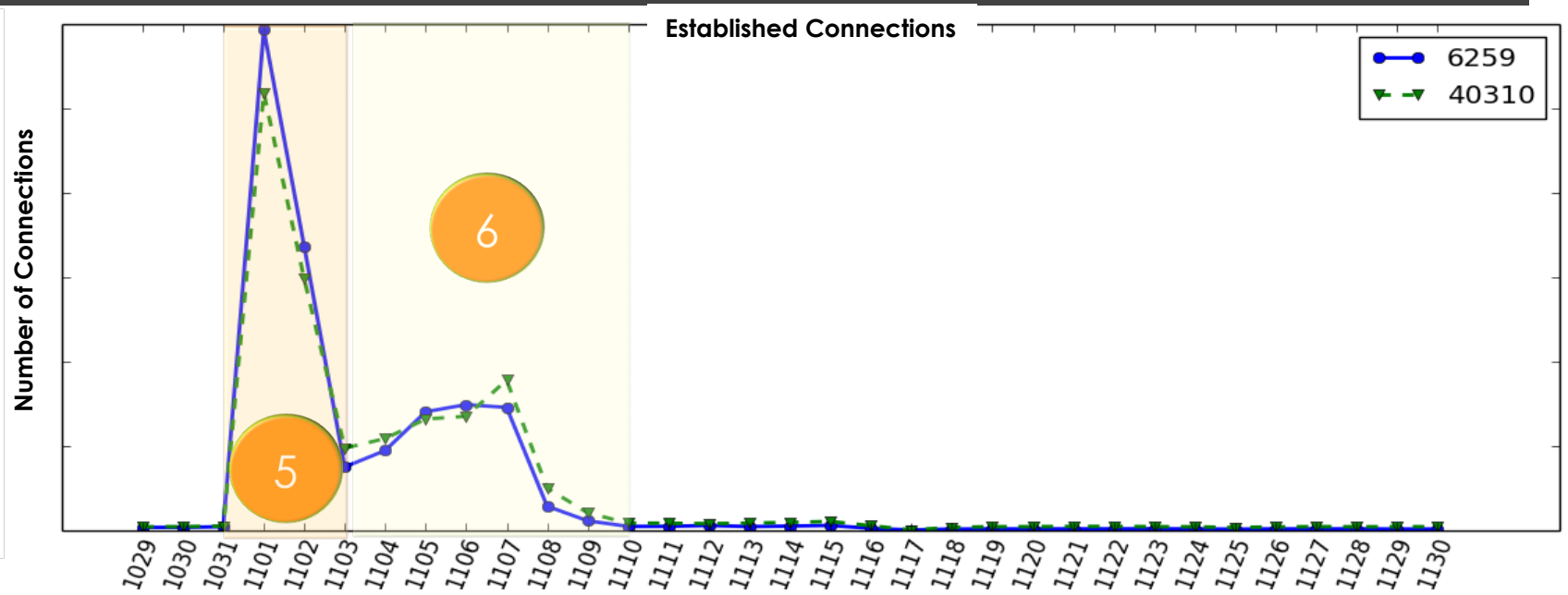
Estimated Campaign Phases —10月

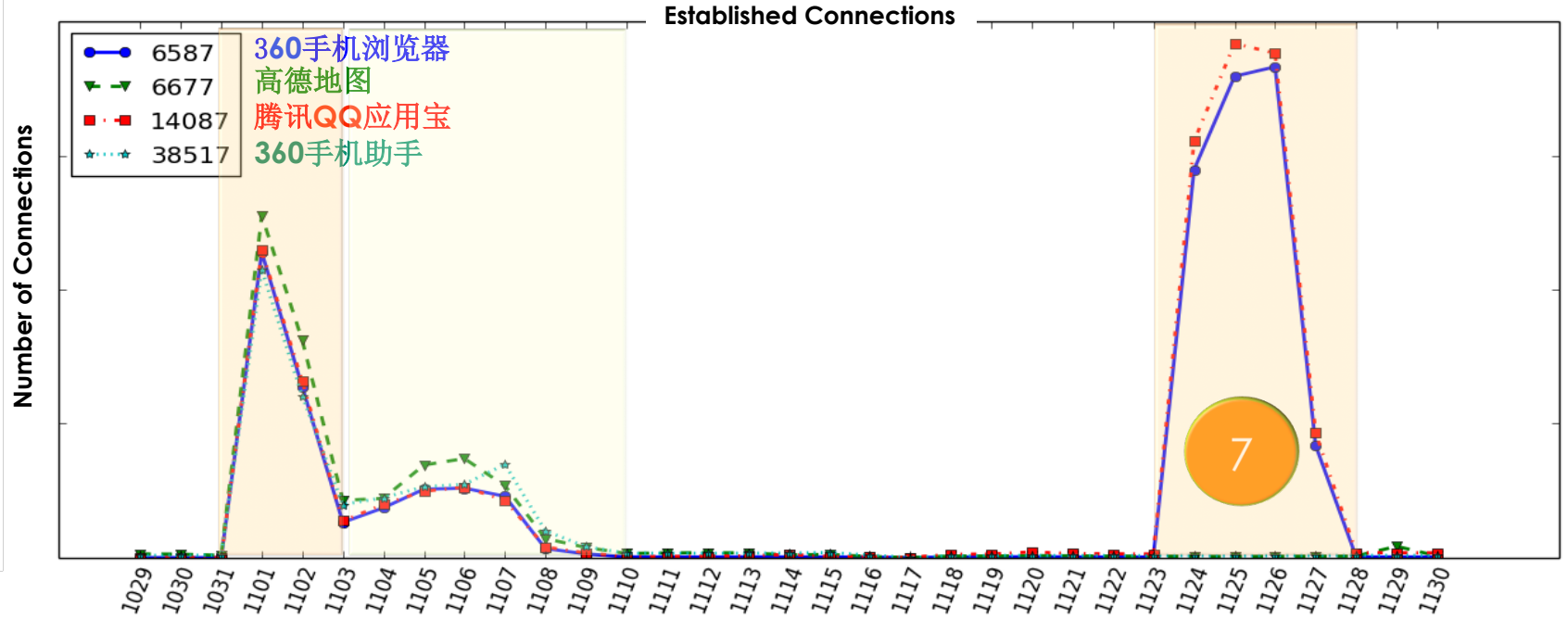


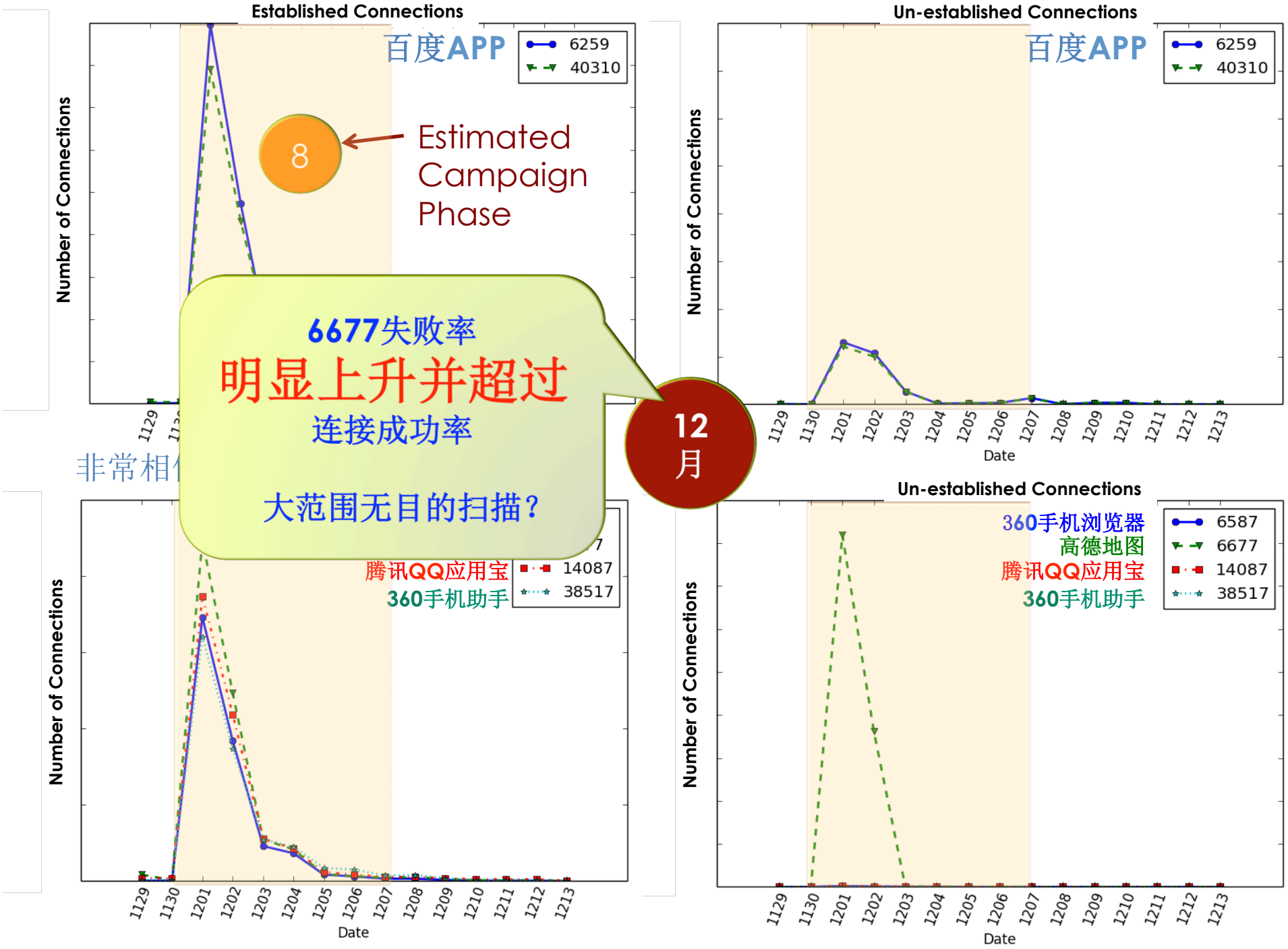



Established Connections
百度APP
6259
40310
Number of Connections
2015-11-04
2015-11-09
2015-11-23
Date
非常相似
Established Connections
6587
6677
14087
38517
360手机浏览器
高德地图
腾讯QQ应用宝
360手机助手
360浏览器漏洞
360手助漏洞
QQ应用宝漏洞
Number of Connections
2015-11-04
2015-11-09
2015-11-23
Date
Un-established Connections
百度APP
6259
40310
Number of Connections
2015-11-04
2015-11-09
2015-11-23
11月
依然连接成功率大于连接失败率
黑产预知可以成功与目标IP连接？
Number of Connections
2015-11-04
2015-11-09
2015-11-23
Date

Estimated Campaign Phases – 11月





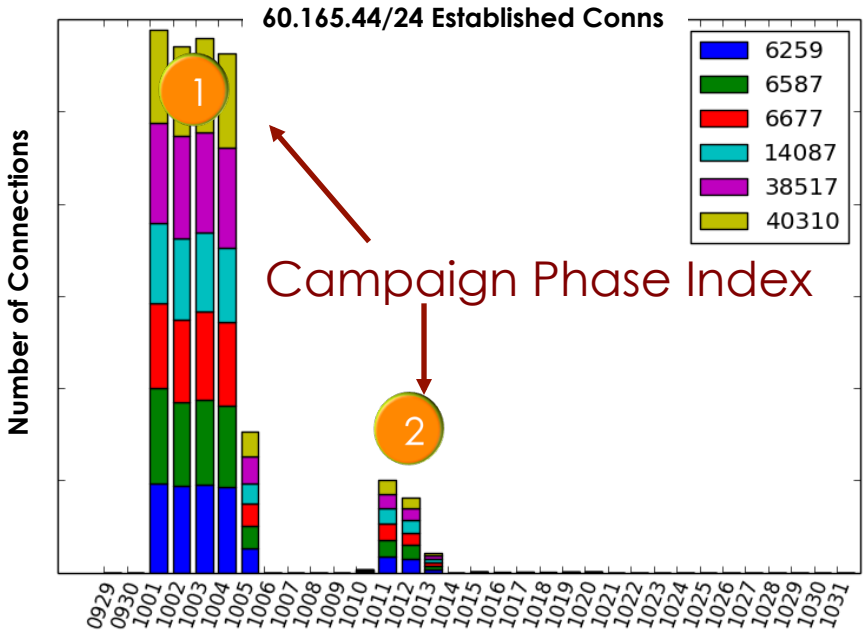

Established Connections
百度APP
6259
40310
Number of Connections
8
Estimated Campaign Phase
6677失败率
明显上升并超过
连接成功率
大范围无目的扫描？
12月
Un-established Connections
百度APP
6259
40310
Number of Connections
1129
1130
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
Date
非常相
腾讯QQ应用宝
360手机助手
14087
38517
Number of Connections
Date
Un-established Connections
360手机浏览器
高德地图
腾讯QQ应用宝
360手机助手
6587
6677
14087
38517
Number of Connections
Date

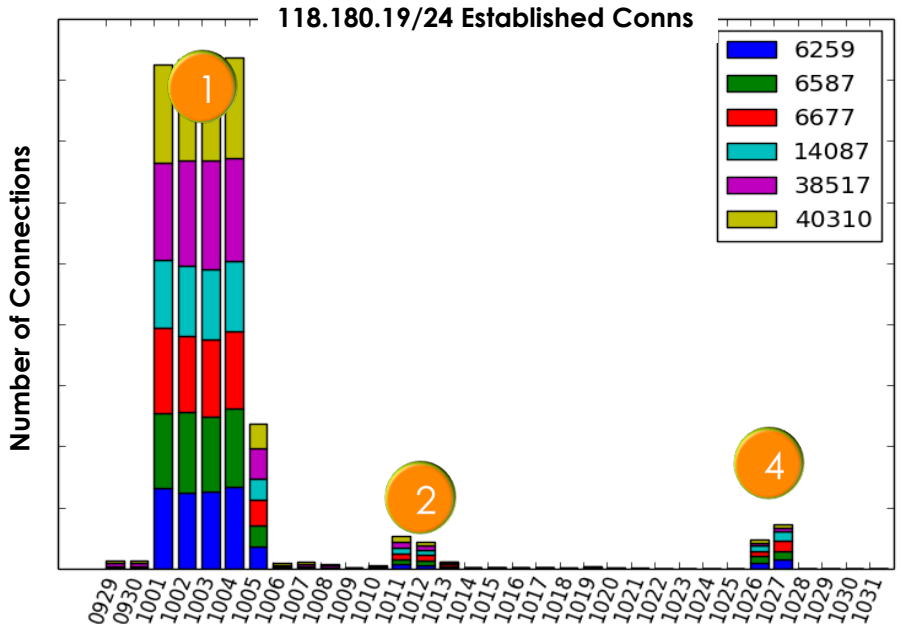
- 扫描源(src ip/subnet)耦合度分析(时间，目标端口维度)

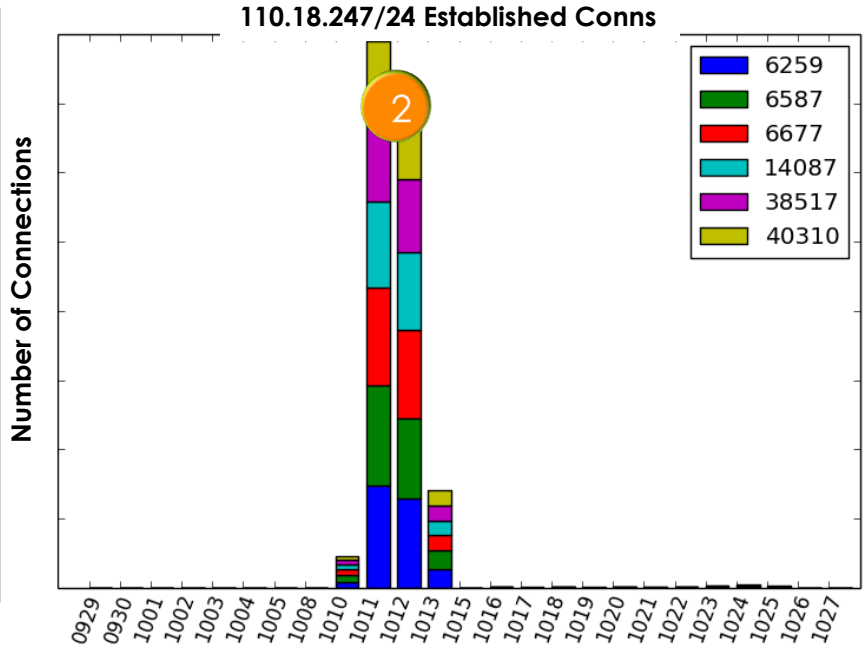
扫描源/24网段在不同端口的重叠性

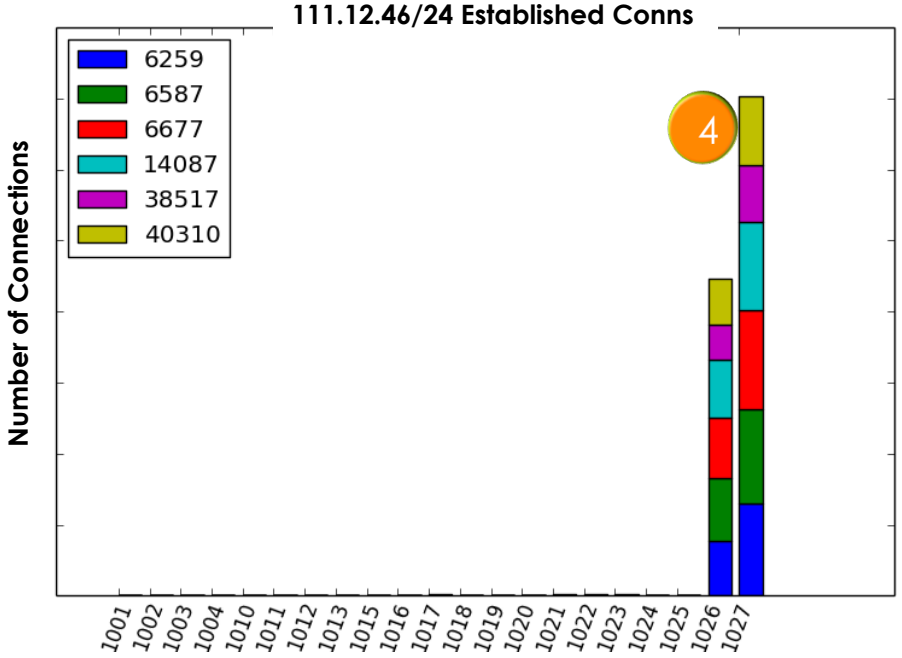
TCP only （established connection）	
端口组合	同时扫描多于 2 个端口的/24 subnet 百分比
[6677, 38517]	9.91%
[6677, 6259]	13.07%
[38517, 6259]	9.57%
[6677, 38517, 6259]	7.34%
[6677, 40310]	9.93%
[38517, 40310]	8.25%
[6259, 40310]	9.63%
[6677, 6259, 40310]	7.37%
[38517, 6259, 40310]	6.28%
[6677, 38517, 6259, 40310]	5.57%

Daily Connections/Port

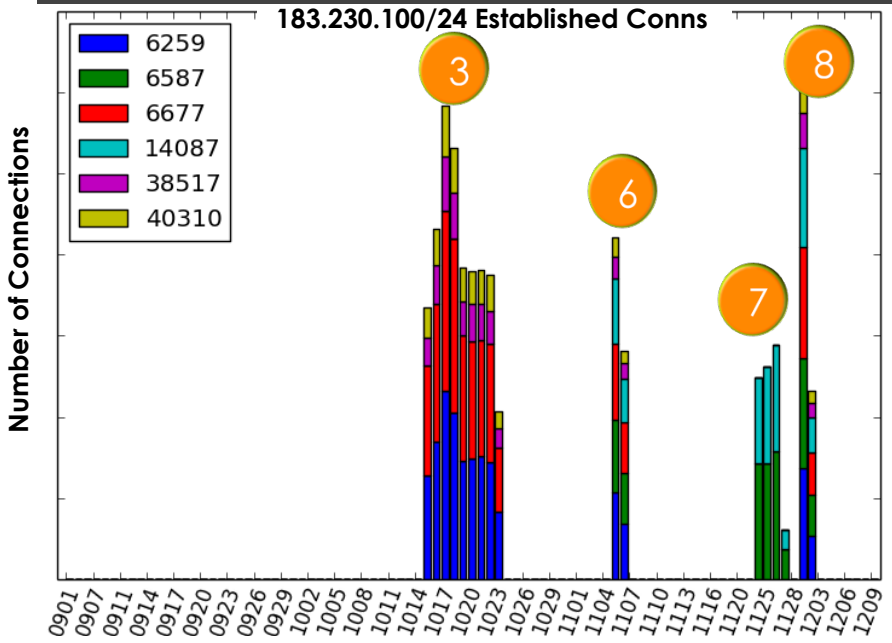


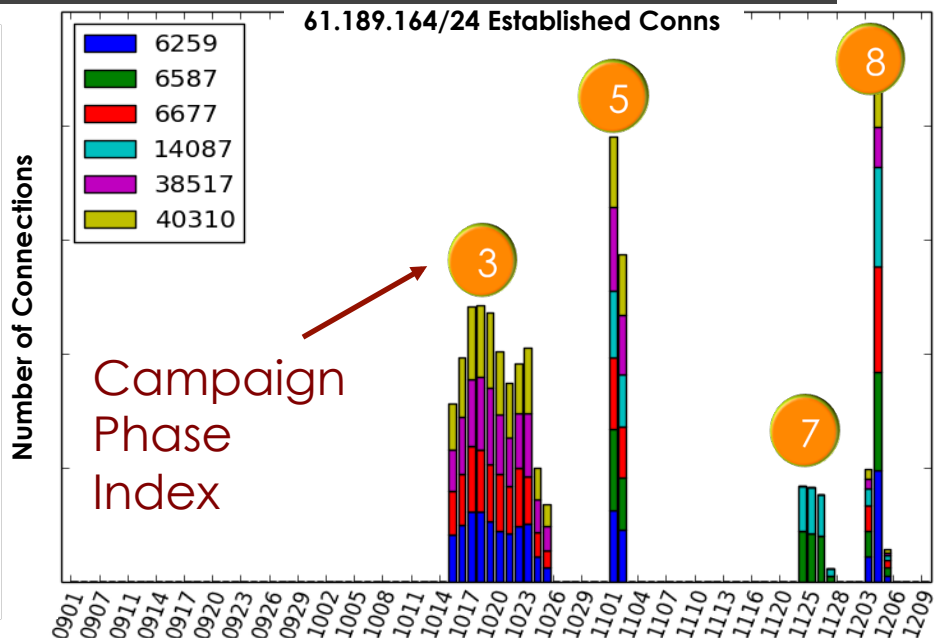


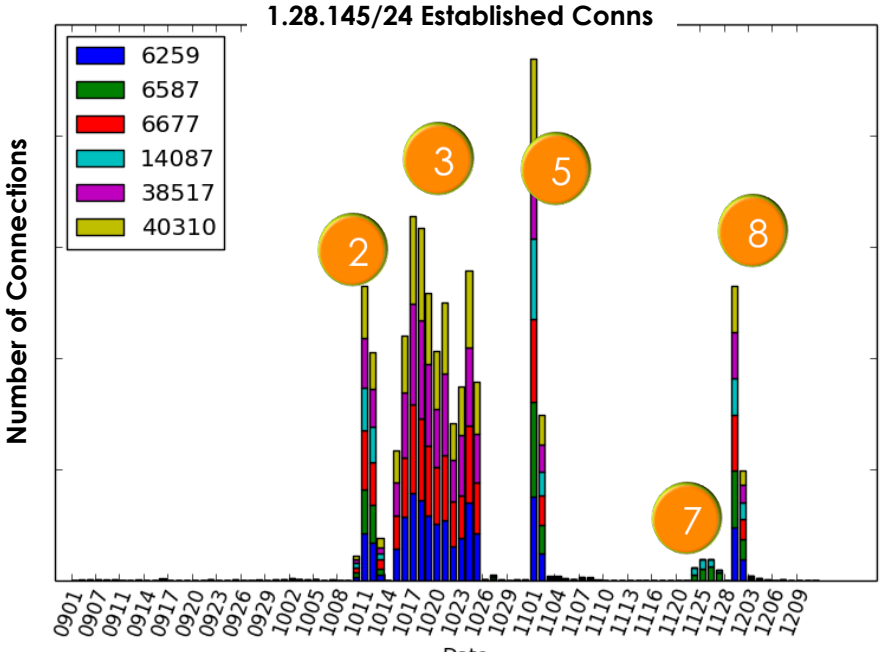


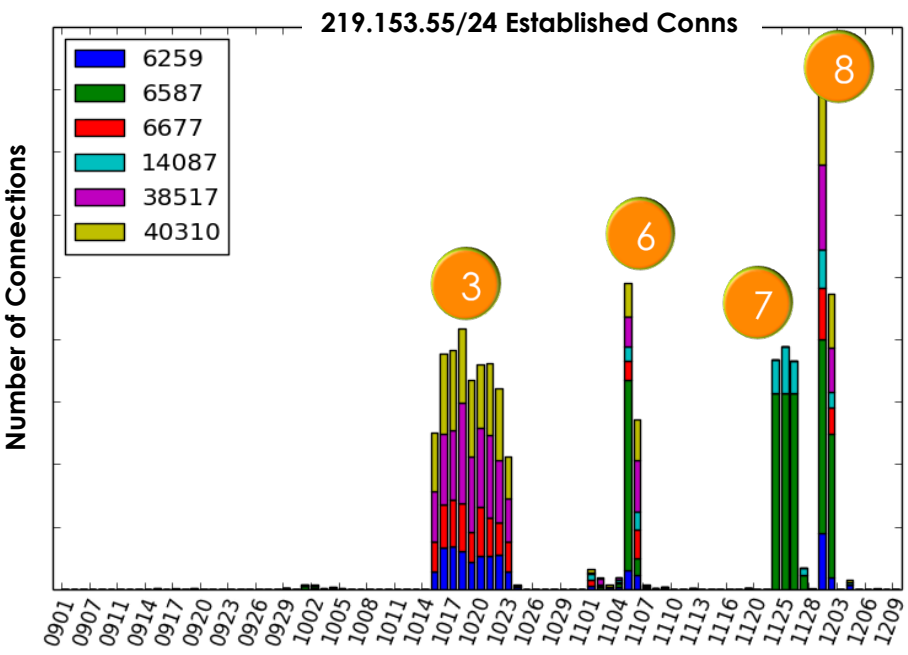


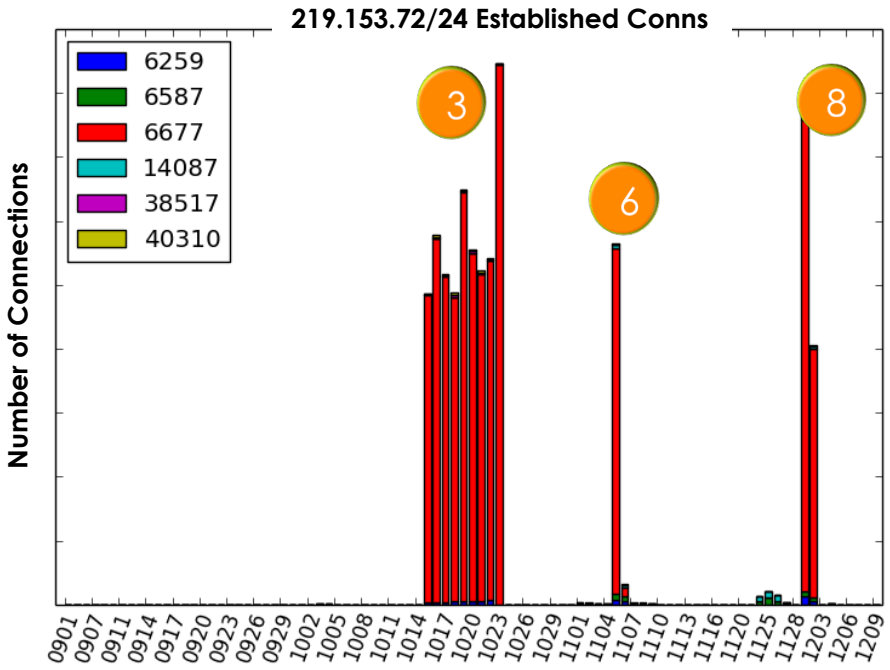
Daily Connections/Port

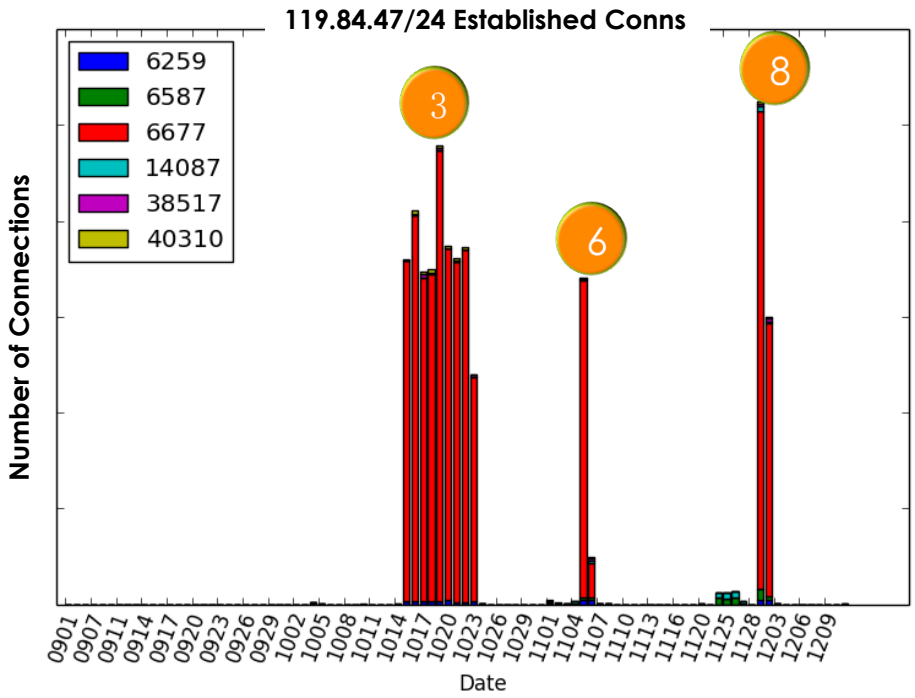


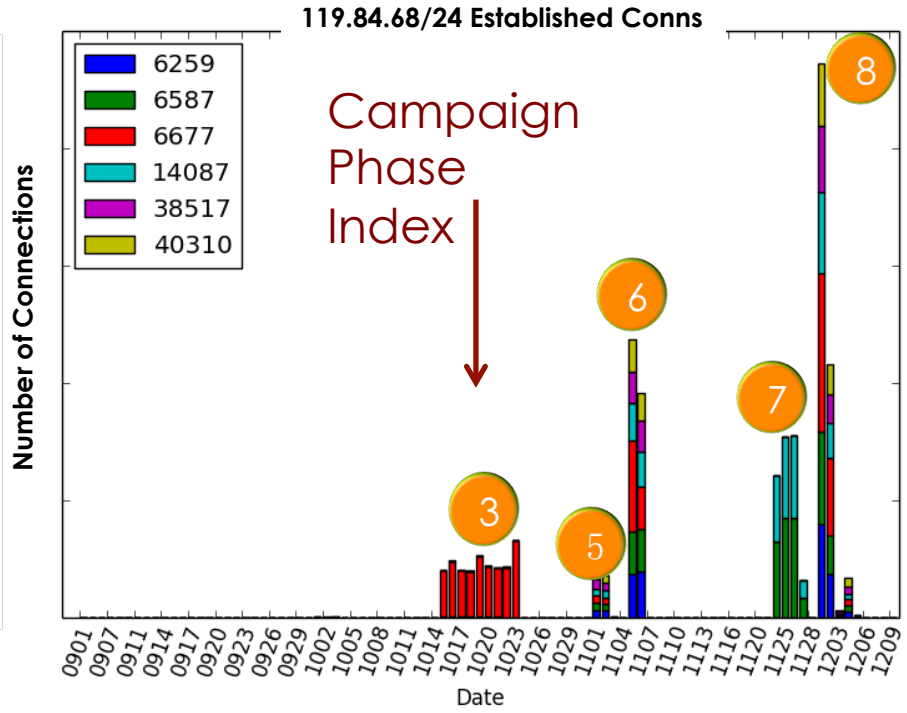






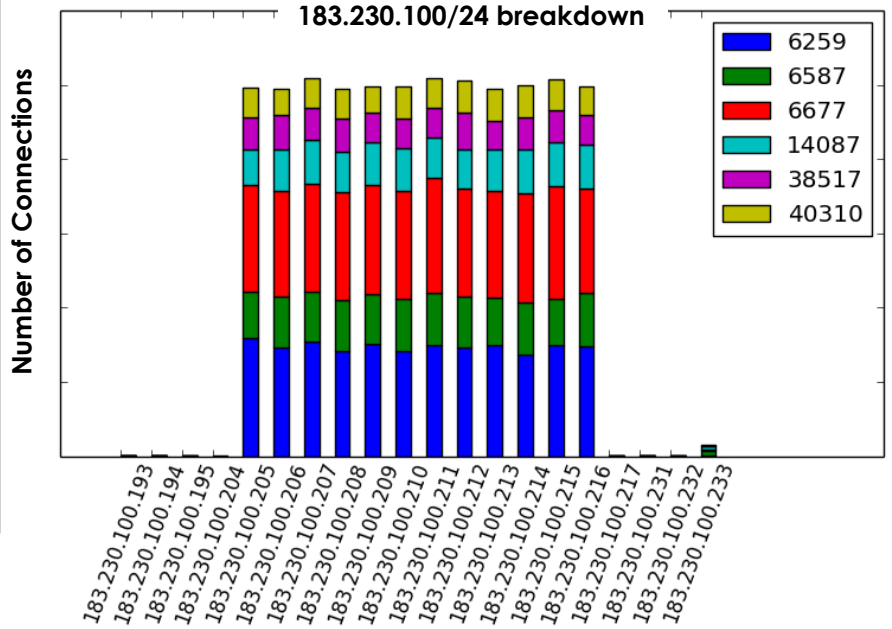


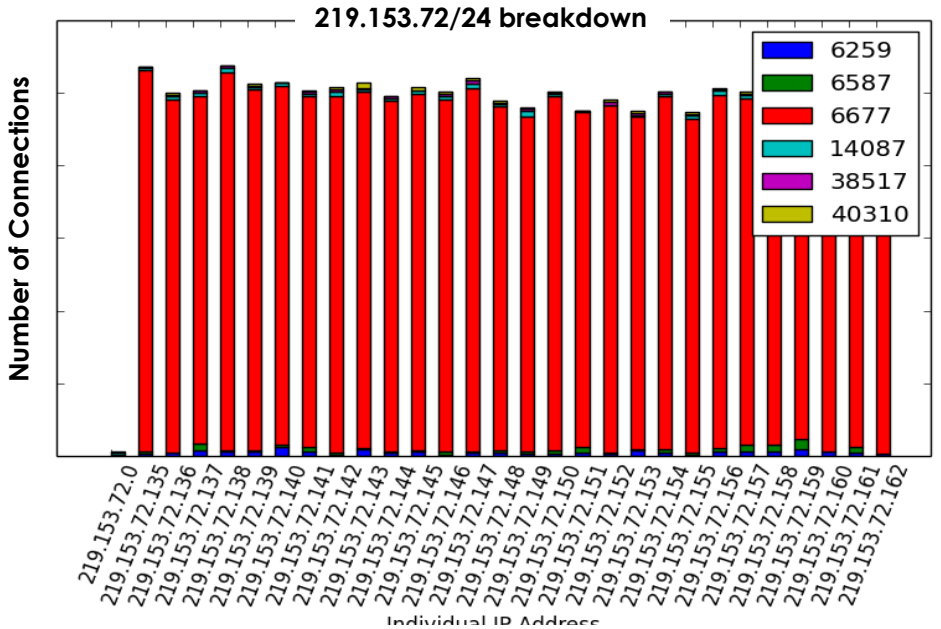


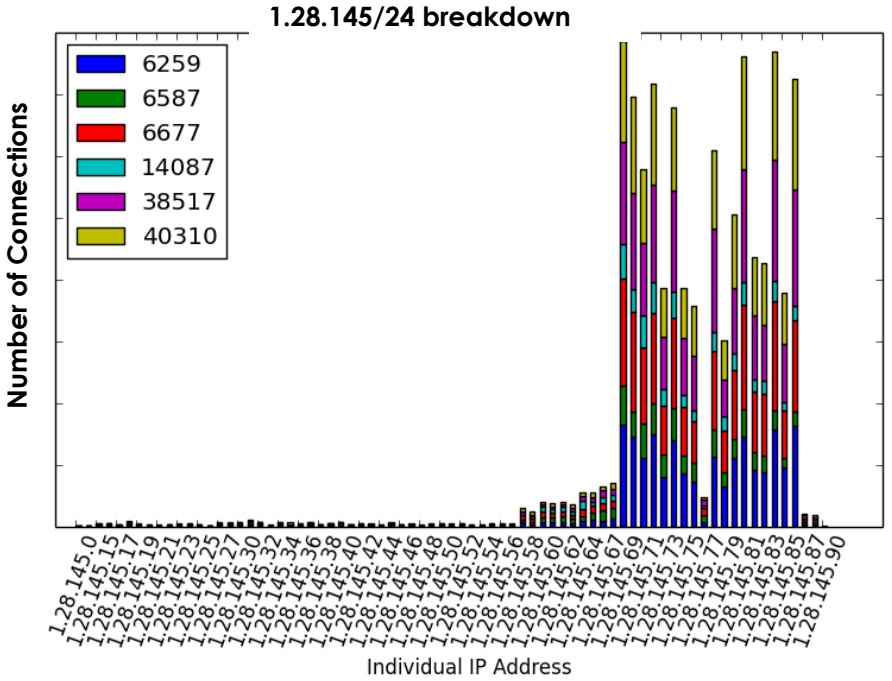


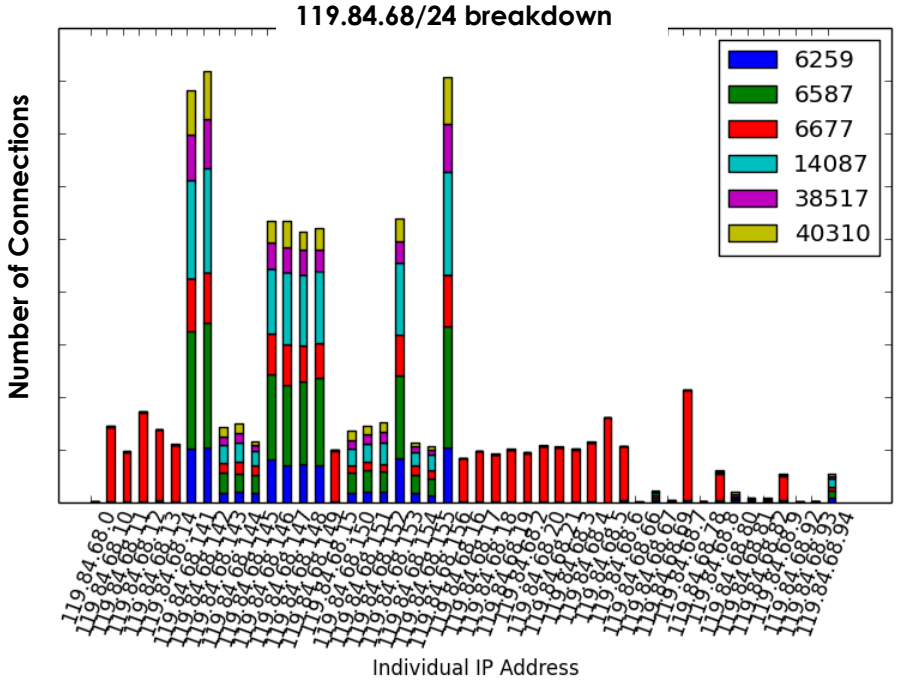
Daily Connections/Port (established connections)

Established Conns/port/IP within /24 subnet

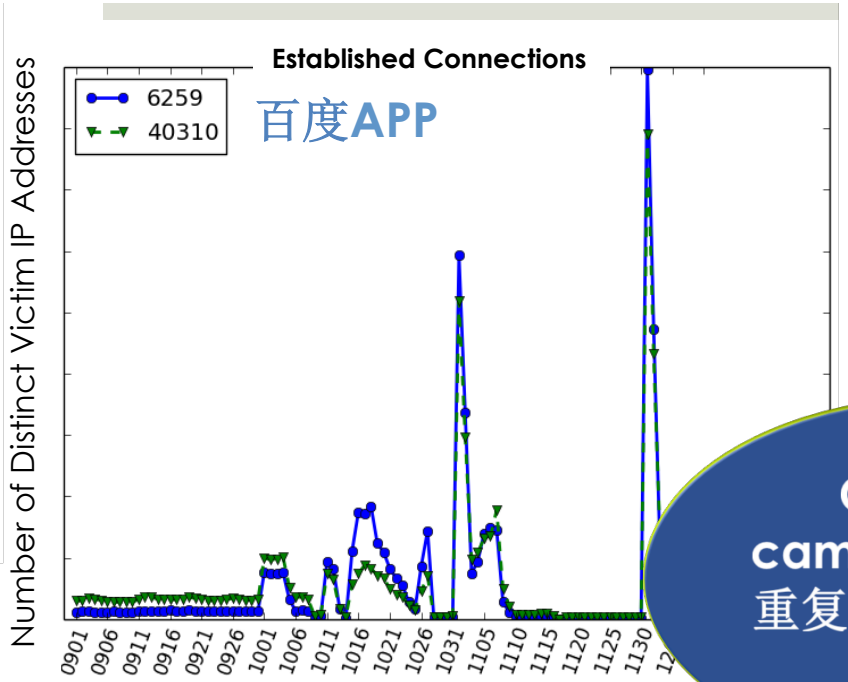


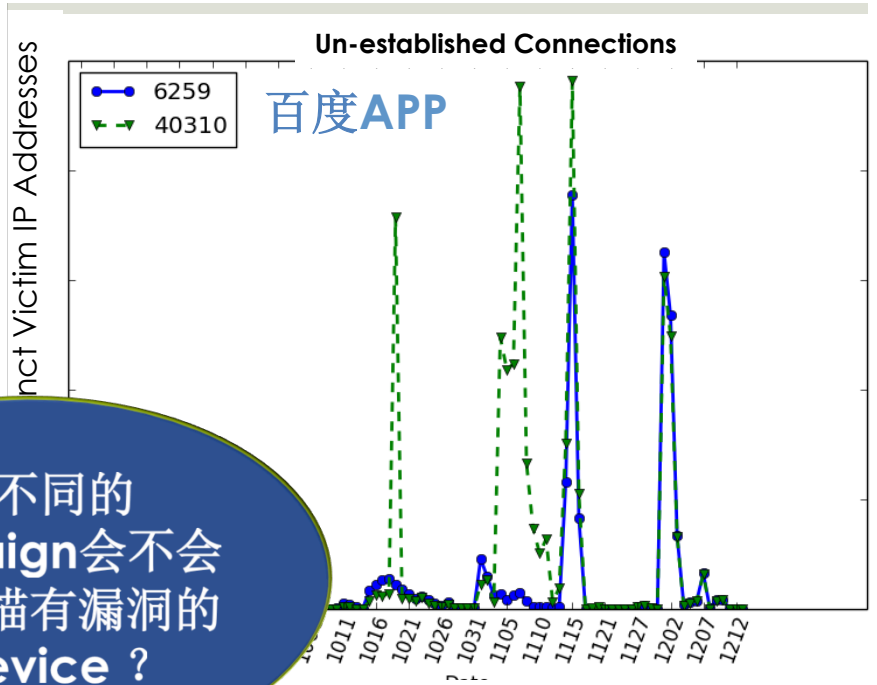




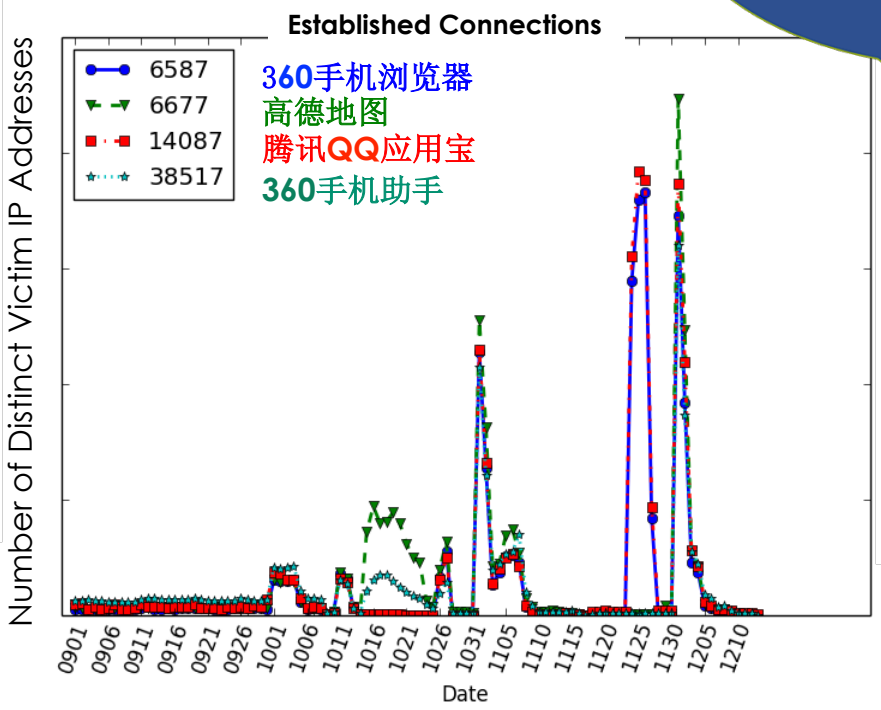


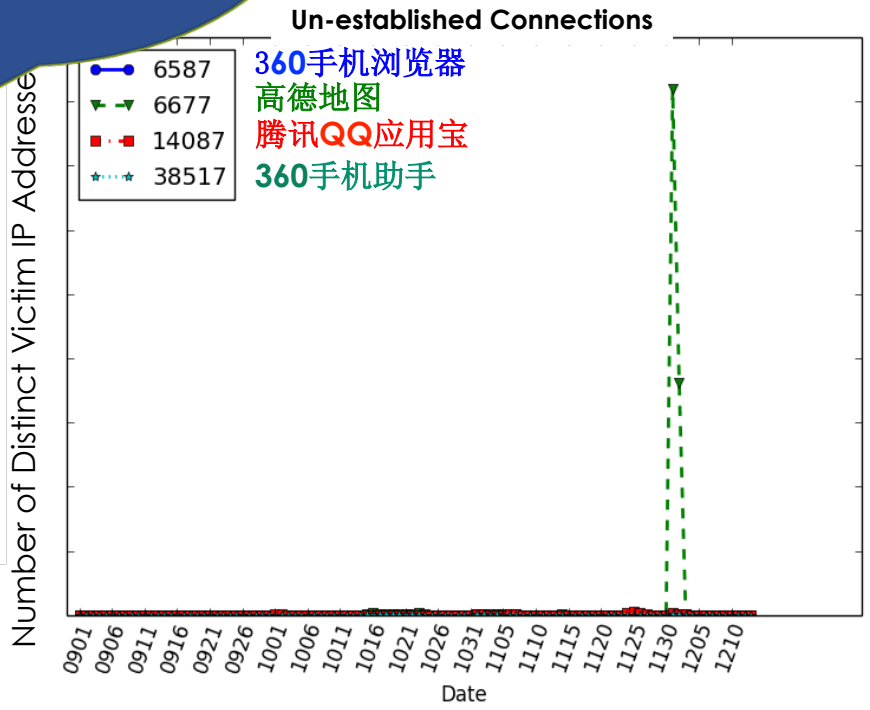
- 被扫描IP(dstip)地址每天数量分布

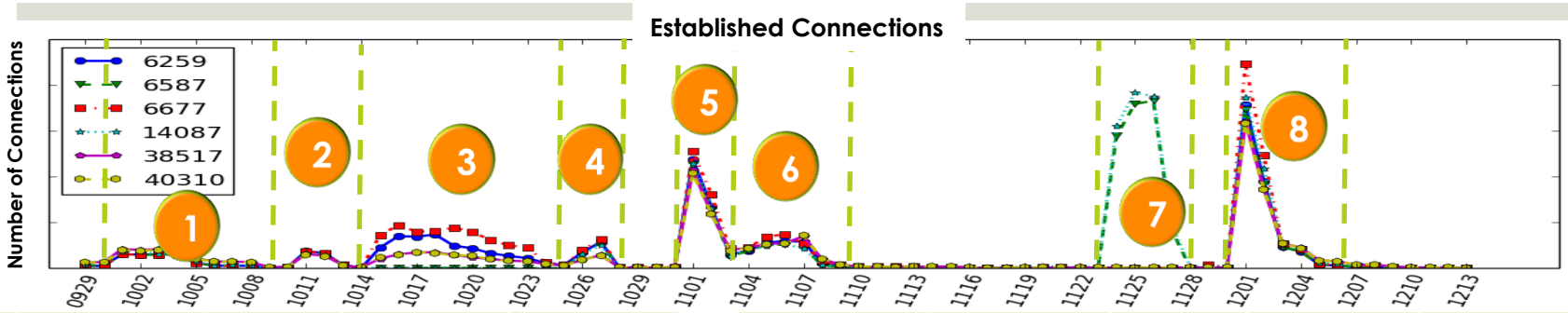




Q: 不同的campaign会不会重复扫描有漏洞的device？







Campaign Pair	# of Distinct Victim IPs	Ratio of Total	Ratio of Campaign [0]	Ratio of Campaign [1]	Campaign Pair	# of Distinct Victim IPs	Ratio of Total	Ratio of Campaign [0]	Ratio of Campaign [1]
[1,2]	9,787	0.25%	1.97%				3%	**20.84%**	8.40%
[1,3]	15,472	0.39%	3.11%				4%	15.25%	7.13%
[1,4]	4,823	0.12%	0.97%				1%	**22.85%**	12.28%
[1,5]	57,758	1.47%	11.61%				7%	**32.67%**	6.09%
[1,6]	42,301	1.08%	8.50%				1%	**35.74%**	8.32%
[1,7]	46,235	1.18%	9.29%				6%	3.12%	0.84%
[1,8]	93,620	2.39%	18.81%				7%	**23.11%**	7.17%
[2,3]	18,731	0.48%	12.71%				6%	**34.73%**	3.74%
[2,4]	2,556	0.07%	1.73%				9%	8.67%	10.05%
[2,5]	40,578	1.04%	**27.53%**				3%	18.49%	**24.64%**
[2,6]	6,569	0.17%	4.46%				8%	**30.67%**	14.18%
[2,7]	32,667	0.83%	**22.17%**				.04%	16.20%	18.61%
[2,8]	45,958	1.17%	**31.18%**	2.49%	[6,8]	190,662	4.86%	**25.91%**	10.32%
[3,4]	26,986	0.69%	7.84%	13.58%	[7,8]	280,586	7.16%	**43.80%**	15.19%

- 不同campaign所针对的目标IP有一定重合，但不显著
- 早期的campaign与 campaign 7，8 有较显著重合。
  - 7可能掌握了很大一部分前期的目标IP / device
  - 8 的特征是大批量wild scan

结论

- 针对高危漏洞，互联网攻击行为特征
  - 超前（漏洞公布前就出现）
  - 及时（漏洞公布24小时之内发起）
  - 大规模响应（漏洞公布之后，被大规模探测或利用）
- 反思
  - 现实：恶意攻击防不胜防，安全业界应对迟缓
  - 互联网安全业界如何在这场arms race中扭转被动局面
  - Brainstorm 如何推动并利用威胁情报，跟踪攻击源头，总结并关联攻击行为从而占得先机

致谢Acknowledgement

衷心感谢长安通信对“wormhole前后一百天”的大力支持。此次也是百度与长安通信在威胁情报领域的第一次联手之作。