iOS系统越狱畅谈

@PanguTeam

议程

- iOS越狱的相关背景
- 盘古越狱的有趣数据
- 越狱开发的要求
- Q&A

iOS的封闭性

- 代码签名
  - 安装/运行
- 沙盒
  - 访问控制
- 内核加密
  - 运行时刻硬件解密
- 系统版本限制

越狱的初衷

- 掌控自己的设备
  - 完全的文件访问
  - 执行任意代码
- 使用扩展插件
  - 突破系统的限制

iOS安全性

- 应用层
  - ASLR / NX / Stack Cookie / AMFI / Sandbox / Entitlement / Code Signing / …
- 内核层
  - KASLR / NX / Stack Cookie / User Space Isolation / Heap Randomization / Free List Protection / …
- ARMv7s/ARM64
- 几乎无法调试内核
- 低碎片化

几种越狱

- Failbreak
  - 仅获取了Root权限，没能修补内核，从而无法运行Mobile Substrate
- Tethered Jailbreak
  - 手机重启后失去越狱状态
- Untethered Jailbreak
  - 在手机重启后仍然能保持越狱状态

越狱的历史

- Saffron (JailBreakMe 3.0) for iOS 4.3.3 (2011.7)
- Absinthe 2.0 for iOS 5.1.1 (2012.5)
- Evasi0n for iOS 6.0-6.1.2 (2013.2)
- Evasi0n7 for iOS 7.0.x (2013.12)
- Pangu for iOS 7.1.x (2014.6)

盘古越狱

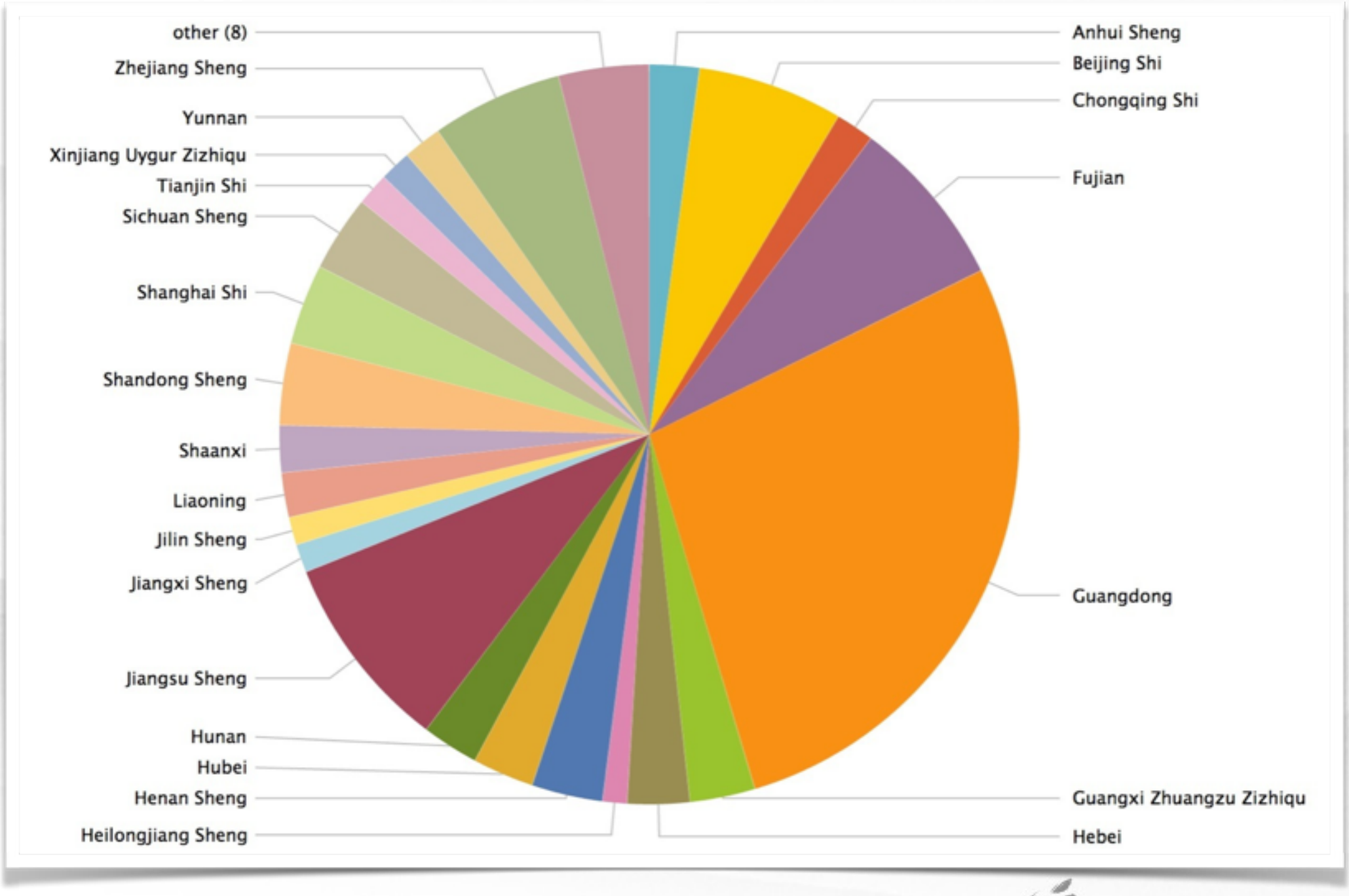
- 发布于2014.6.24日零时
- 全球首个支持 iOS 7.1.x 全设备的完美越狱
- 第一次由中国团队独立研发并公布越狱
- 盘古团队成员

  @dm557 @windknown @OGC557 @Daniel_K4 @曾半仙

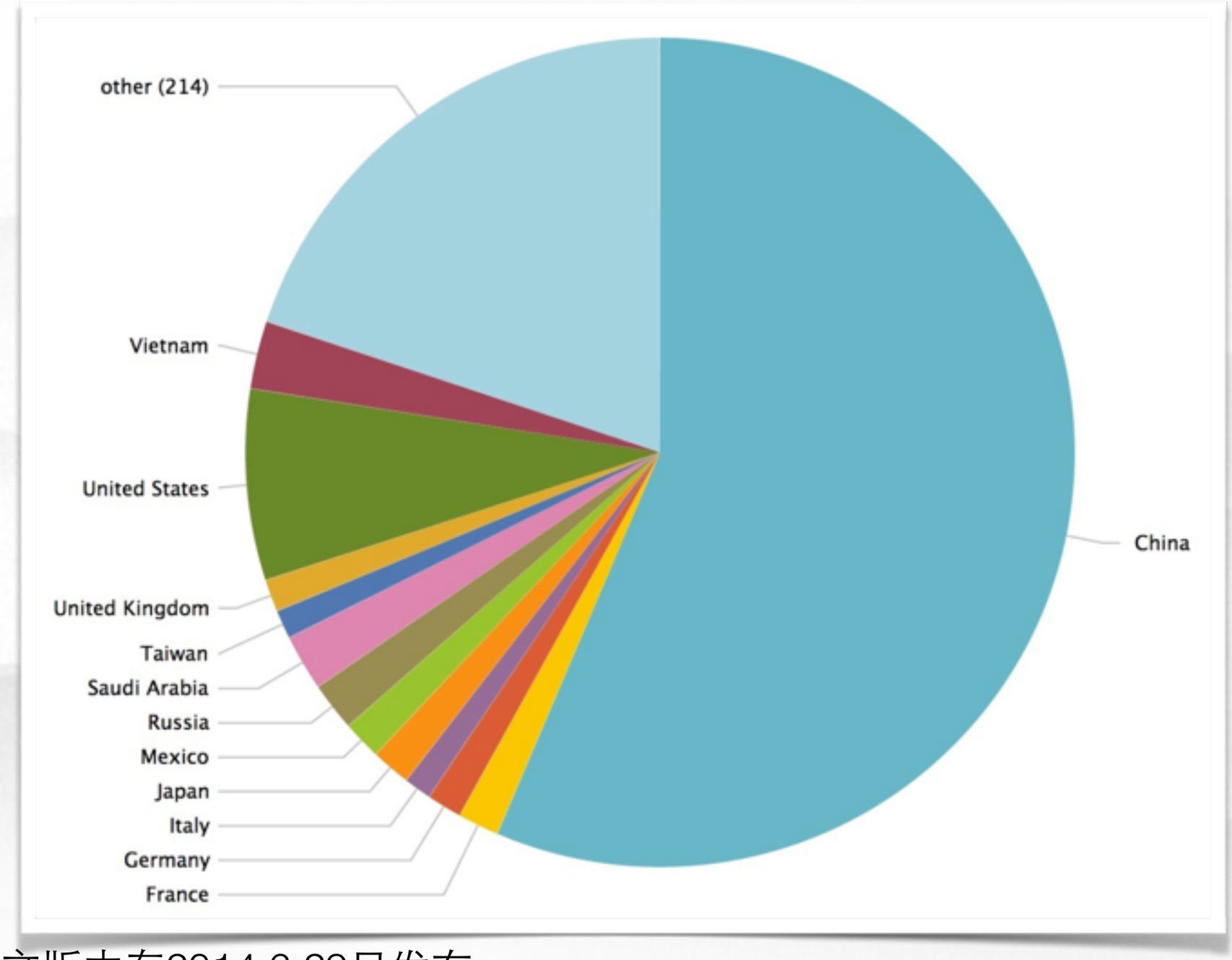
盘古越狱数据

- 以下统计数据截止到**2014.07.02**
- 网站有 **356万** 次浏览量
- 总计 **782万** 次越狱请求
- 尝试对 **205万** 台设备进行越狱
- 成功越狱 **181万** 台设备

国内越狱分布



全球越狱分布



- 注：英文版本在2014.6.29日发布

泄漏的iOS 7.1.2

14/06/24 0:52:18.000 116.251. - - [23/Jun/2014:16:52:18 +0000] "GET /x/?a=2&os=7.1.2&model=iPhone6,1&md5=2EE6382C06A42C8EACE1F0F6F034E70A&version=1.0.0&client=pc HTTP/1.1" 200 2 "-" "Asynchronous WinHTTP/1.0" -

a = 2 | clientip = 116.251 | host = tj | md5 = 2EE6382C06A42C8EACE1F0F6F034E70A | method = GET | os = 7.1.2 | referer = -
req_time = 23/Jun/2014:16:52:18 +0000 | root = x | source = /home/user/log/tj/jb_tj.access.20140623.log | sourcetype = access_combined_wcookie | status = 200
uri = /x/?a=2&os=7.1.2&model=iPhone6,1&md5=2EE6382C06A42C8EACE1F0F6F034E70A&ver... | uri_path = /x/
uri_query = a=2&os=7.1.2&model=iPhone6,1&md5=2EE6382C06A42C8EACE1F0F6F034E70A&versio... | useragent = Asynchronous WinHTTP/1.0

前 10 个值	计数	%
116.251	15	16.304%
65.101.9	10	10.87%
174.94.(	8	8.696%
17.114.7	7	7.609%
17.114.(	6	6.522%
173.72.2	6	6.522%
50.152.2	5	5.435%
99.248.(	5	5.435%
68.43.17	4	4.348%
17.114.9	3	3.261%

来自Apple的请求

查询的 IP: 17.114.[redacted] 来自：美国

GeoIP: Cupertino, California, United States

Apple

值	计数	%
17.114	21	45.652%
17.105	10	21.739%
17.114	6	13.043%
17.114	3	6.522%
17.114	2	4.348%
17.206	2	4.348%
17.114	1	2.174%
17.115	1	2.174%

完美越狱流程

- 代码注入
- 跳出沙盒 / 获取Root权限
- 溢出内核
- Patch内核
- Remount rootfs为可写
- 释放Untether

完美越狱流程

- 重启手机
- 绕过代码签名
- 溢出内核
- Patch内核
- Remount rootfs为可写
- 继续启动系统

应用层攻击

- 内置应用
  - MobileSafari / Mail / Message / …
- 与电脑连接
  - Backup / File Relay / Sync / DDI / …

内核层攻击

- IOKit
- Syscall
- Mach Trap
- Mig System

代码签名绕过

- 内核层 - AMFI
- 应用层 - dyld

Patch内核

- 适配所有设备 - 固定地址偏移不适合
- 智能搜索 - 实时dump出内核后搜索
  - 简单的指令解释器
  - 根据指令特征进行搜索

Jailbreak.

Pangu iOS 7.1-7.1.x

Q & A