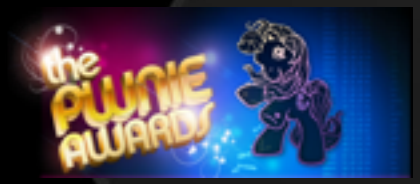
From Good to Best

陈良 I 高级安全研究员

关于我们



- 一群白帽子
- 专注PC及移动端二进制攻防研究
- 四年获得八个Pwn2Own单项冠军
- 科恩联合电脑管家获得世界首个Master of Pwn
- 四个Pwnie Award提名
- 多次在世界级安全峰会上做主题演讲

Pwn2Own

- 世界最难黑客挑战赛
- “不出题的比赛”
- 安全界二进制攻与防的“真实缩影”
- 针对主流浏览器的远程攻击
  - 要求沙盒逃逸 （System/Root可加分）
  - 当天最新版本 （要求使用未知漏洞进行攻击）

KEEN security lab

历届赛况

- James Forshaw：Pwn2Own 2013 Java
- VUPEN： Pwn2Own 2014 IE, Flash, Chrome, Reader
- Geohot：Pwn2Own 2014 Firefox
- Lokihardt：Pwn2Own 2015 IE, Chrome, Safari

KEEN security lab

我们过去的五冠

- Mobile Pwn2Own 2013 iOS 7
- Pwn2Own 2014 OS X Mavericks
- Pwn2Own 2014 Flash
- Pwn2Own 2015 Flash
- Pwn2Own 2015 Adobe Reader
  - 联合电脑管家

KEEN security lab

“失手”的大神们

- VUPEN
  - Pwn2Own 2013 Chrome比赛当天上午漏洞被补
- Lokihardt
  - Pwn2Own 2014 IE项目沙盒逃逸
  - Pwn2Own 2014 Chrome项目与Geohot撞洞
  - Pwn2Own 2016 Chrome项目失败
- Juri
  - Pwn2Own 2015 Chrom项目失败

KEEN security lab

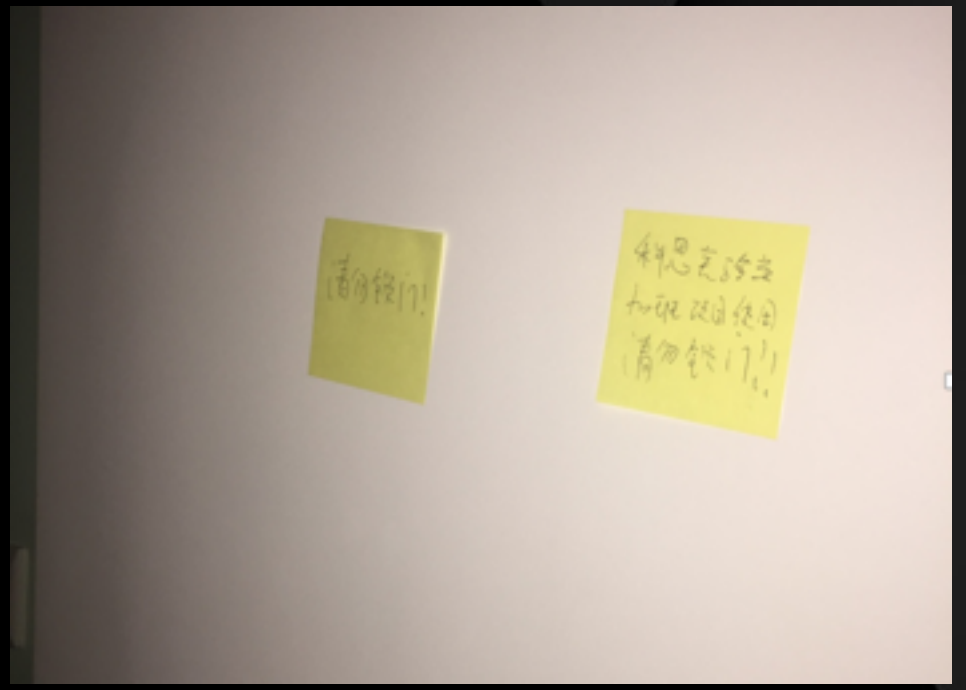
Pwn2Own 2016

- 史上最难Pwn2Own
  - 仅有3次机会， 15分钟内完成
  - 不许任何用户交互
- 参赛项目的调整
- 抽签顺序很重要
- 设立积分制，积分最高团队获得Master of Pwn称号

KEEN security lab

赛前准备

- 三缺一的尴尬
- 向困难挑战
- 春节无休
- 解读新规则
- 第二套方案
- “无赖”的厂商
  - 无限Beta，延时发补丁
  - 悲剧发生
- 奋力一搏
- 报漏洞
- 小遗憾



KEEN security lab

比赛过程

- 不幸运的抽签结果
- 策略调整
- 第二天是关键
- 通宵测试
- 第二天：首战顺利
- Edge决胜局：屏住呼吸一分钟
- 惊叹主办方
- Master of Pwn

KEEN security lab

Pwn2Own 2016比赛结果：Best

- KeenLab联合电脑管家组成的Tencent Security Team Sniper赢得全球首个“Master of Pwn”
  - Sniper Team 斩获Edge Flash Safari三个单项冠军，积分38分获得第一
  - 腾讯安全总共获得4个单项，总分48分

战队	总积分
腾讯安全Sniper战队	38
韩国JungHoon Lee	25
360Vulcan Team	25
腾讯安全Shield战队	10

KEEN security lab

总结

- 热情 + 无畏
- 个人黑客英雄时代已经结束
- 深入的安全研究更依赖团队合作与专业人才的培养

KEEN security lab

谢谢！

KEEN
security
lab