SACC

卓越 5周年 变迁

2013中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2013

大数据下的IT架构变迁

乌云的背后是阳光

乌云平台实践

几个问题

- 我是谁？
- 乌云是什么？
- 为什么要有乌云？
- 乌云改变了什么？
- 已经完成了吗？

我是谁？

- 网名：疯狗（不要笑，严肃！）
- 业余渗透师，web安全爱好者，菜鸟运营
- 9年互联网安全研究经历
- 乌云网联合创始人

何为乌云

- WooYun是一个位于厂商和安全研究者之间的安全问题反馈平台
- 为互联网安全研究者提供一个公益、学习、交流和研究的平台

何为乌云

- 漏洞第一时间通知厂商
- 厂商确认与修复周期
- 对外不主动披露任何信息
- 通用漏洞风险控制与解决渠道（闭环）
- 安全问题开放学习共享

何为乌云


白帽报告漏洞
用户监督并且对企业提出安全需求
企业修复并披露安全问题
企业加强安全建设和提升白帽价值
更多白帽学习和加入这个过程

何为乌云

何为乌云

- This is wooyun

为什么要有乌云

- 对安全研究者进行良性引导
- 安全漏洞的封闭为厂商造成了盲目，甚至恐惧
- 如今与传统互联网的差异为用户带来的影响

传统与改变

- 传统

Microsoft

Adobe

传统与改变

- 现在

传统与改变

- 360任意密码修改漏洞（wooyun-2012-08333）

  -影响用户过千万！

  -修复迅速
  15:36提交 -> 15:52确认 -> 半小时内修复完毕

传统与改变

- 腾讯WEBQQ聊天功能XSS（wooyun-2012-08487）

  - WebQQ用户接收信息即可中招！
  - 云端直接对内容输出进行处理，问题解决了..

传统与改变

- 中国万网任意账号劫持+验证码漏洞 （wooyun-2013-016896）

  -影响域名过百万！
  -修复迅速（新年初夜的疯狂）

- 原来我们的安全根本不掌握在自己手里

传统与改变

- 传统的安全问题：
  - 数据分散在用户端
  - 安全攻击不易于察觉
  - 安全不可控

- 如今的安全问题：
  - 数据都集中在云端
  - 安全攻击易于发现
  - 安全可控

传统与改变

- 化零为整


中国人民银行
100
100
壹佰圆
C0A8657568
100
毛泽东1893-1976
by: haifeng330

封闭与公开

- 甲方 VS 乙方 & 丙方 & 丁方？？？

乌云改变了什么？

- 再说一遍乌云做了什么
  - 漏洞第一时间提交给厂商
  - 通用性问题及时通知其他厂商及安全厂商
  - 社区对安全漏洞进行沟通与讨论
  - 对公众保持公开

乌云改变了什么？

- 厂商得到了什么？

  - 攻击发生前第一时间获取到漏洞信息
  - 其他厂商借鉴及时避免损失
  - 厂商了解自己当前真正的问题所在
  - 公众了解数据安全并对厂商进行监督

- 具体呢？

乌云改变了什么？

- 黑产披露
  - 搜索引擎恶意SEO
  - 病毒、钓鱼
  - 淘宝信誉诈骗

- 漏洞预警
  - ThinkPHP
  - Struts2
  - Dedecms

乌云改变了什么？

- 漏洞趋势
  - CSDN“拖库”事件
  - 任意密码修改（验证码爆破）
  - 商城支付漏洞
  - 开源后门
  - 安全设备漏洞
  - XSS“盲打”
  - …

已经完成了吗？

- 这个互联网有两种安全
  - 真正的安全
  - 掩盖下的安全

已经完成了吗？

- 传统
  - 无视web和云带来的安全变革
- 封闭
  - 收集漏洞并隐藏漏洞细节
- 掩饰
  - 威吓提交者，精力不用在如何修复漏洞，而是琢磨怎么隐藏漏洞上

已经完成了吗？

- 不修复的问题
  - 跨站脚本-可以让战场离得更远（浅谈腾讯架构缺陷） wooyun-2010-011192
  - 一个普通的xss即可沦陷腾讯所有业务

- 真的是为了用户吗？

漏洞回应

厂商回应：

危害等级：高

漏洞Rank：10

确认时间：2012-08-23 09:16

厂商回复：

多谢反馈，正在跟进处理中

已经完成了吗？

- 不修复+频发=？

提交日期	漏洞名称
2013-01-01	[腾讯实例教程] 那些年我们一起学XSS - 21. 存储型XSS进阶 [猜测规则，利用Flash addCallback构造XSS]
2013-01-01	[腾讯实例教程] 那些年我们一起学XSS - 20. 存储型XSS入门 [套现绕过富文本]
2012-12-31	[腾讯实例教程] 那些年我们一起学XSS - 19. 存储型XSS入门 [什么都没过滤的情况]
2012-12-29	[腾讯实例教程] 那些年我们一起学XSS - 18. XSS过滤器绕过 [猥琐绕过]
2012-12-29	[腾讯实例教程] 那些年我们一起学XSS - 17. XSS过滤器绕过 [通用绕过]
2012-12-27	[腾讯实例教程] 那些年我们一起学XSS - 16. Flash Xss进阶 [ExternalInterface.call第二个参
2012-12-26	[腾讯实例教程] 那些年我们一起学XSS - 15. Flash Xss进阶 [ExternalInterface.call第一个参
2012-12-26	[腾讯实例教程] 那些年我们一起学XSS - 14. Flash Xss入门 [navigateToURL]
2012-12-24	[腾讯实例教程] 那些年我们一起学XSS - 13. Dom Xss实例 [Discuz X2.5]
2012-12-20	[腾讯实例教程] 那些年我们一起学XSS - 12. Dom Xss进阶 [路径con]
2012-12-19	[腾讯实例教程] 那些年我们一起学XSS - 11. Dom Xss进阶 [善变iframe]
2012-12-18	[腾讯实例教程] 那些年我们一起学XSS - 10. Dom Xss进阶 [避逅eval]
2012-12-17	[腾讯实例教程] 那些年我们一起学XSS - 9. Dom Xss入门 [隐式输出]
2012-12-14	[腾讯实例教程] 那些年我们一起学XSS - 8. Dom Xss入门 [显式输出]
2012-12-14	[腾讯实例教程] 那些年我们一起学XSS - 7. 宽字节、反斜线与换行符一起复仇记
2012-12-14	[腾讯实例教程] 那些年我们一起学XSS - 6. 换行符复仇记
2012-12-13	[腾讯实例教程] 那些年我们一起学XSS - 5. 反斜线复仇记
2012-12-13	[腾讯实例教程] 那些年我们一起学XSS - 4. 宽字节复仇记 [QQ邮箱基本通用]
2012-12-13	[腾讯实例教程] 那些年我们一起学XSS - 3. 输出在HTML属性里的情况
2012-12-13	[腾讯实例教程] 那些年我们一起学XSS - 2. 输出在<script></script>之间的情况

2012-11-06	腾讯微博存储型XSS漏洞--看我这标题多普通10
2012-10-31	腾讯微博存储型XSS漏洞--看我这标题多普通9
2012-10-22	腾讯微博存储型XSS漏洞--看我这标题多普通8
2012-10-19	腾讯微博存储型XSS漏洞--看我这标题多普通7
2012-10-18	腾讯微博存储型XSS漏洞--看我这标题多普通6
2012-10-17	腾讯微博存储型XSS漏洞--看我这标题多普通5
2012-10-15	腾讯微博存储型XSS漏洞--看我这标题多普通4
2012-10-12	腾讯微博存储型XSS漏洞--看我这标题多普通3
2012-10-12	搜狗一应用存在struts任意代码执行漏洞
2012-10-11	腾讯微博存储型XSS漏洞--看我这标题多普通2
2012-10-11	搜狐微博存储型XSS漏洞二
2012-09-27	腾讯微博存储型XSS漏洞--看我这标题多普通

已经完成了吗？

- 就这些？其实还有...

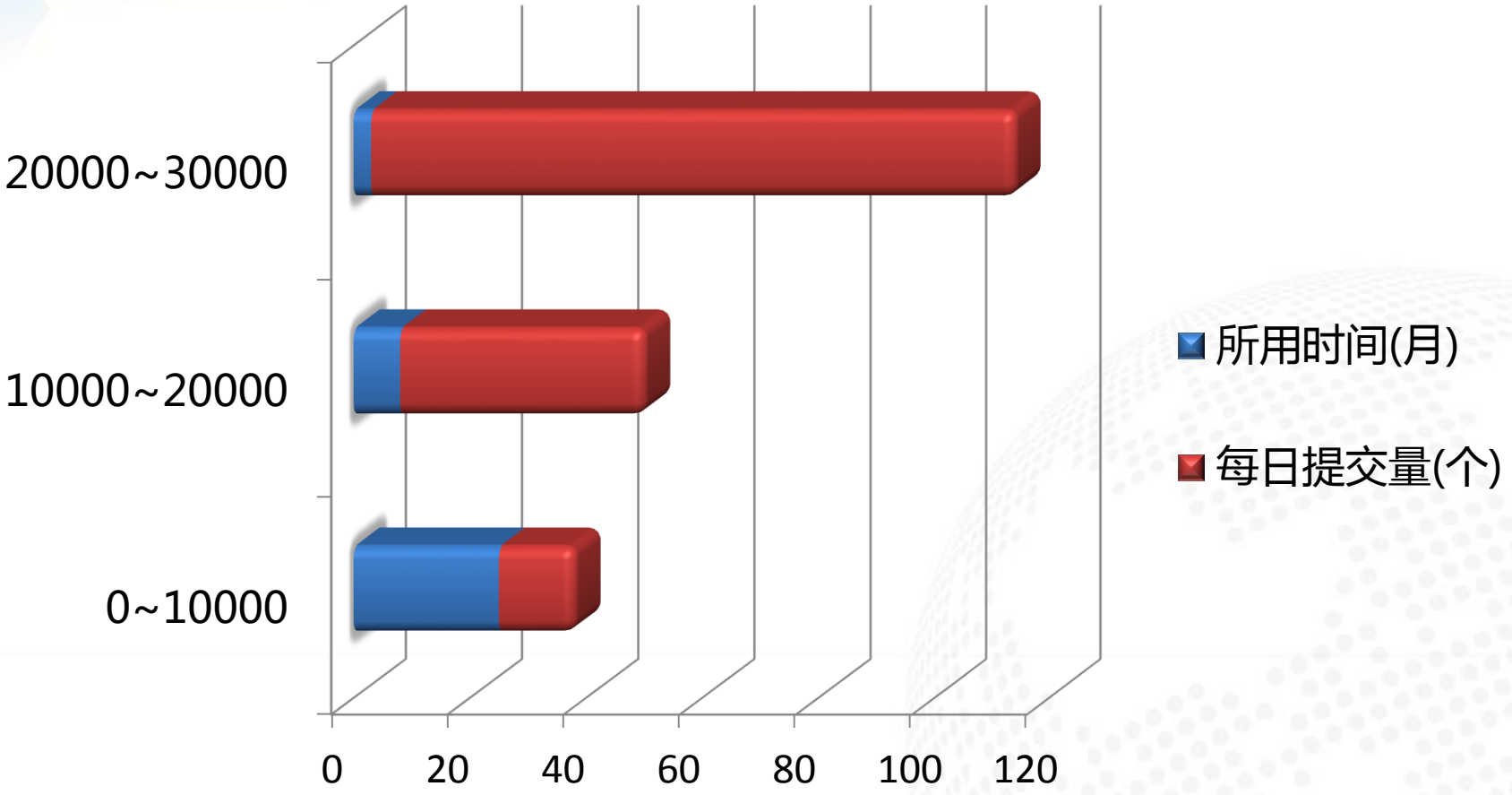
2013-03-31 QQ空间某功能缺陷导致日志存储型XSS - 12
2013-03-31 QQ空间某功能缺陷导致日志存储型XSS - 11
2013-03-26 QQ空间某功能缺陷导致日志存储型XSS - 10
2013-03-25 QQ空间某功能缺陷导致日志存储型XSS - 9
2013-03-24 QQ空间某功能缺陷导致日志存储型XSS - 8
2013-03-22 QQ空间某功能缺陷导致日志存储型XSS - 7
2013-03-20 QQ空间某功能缺陷导致日志存储型XSS - 6
2013-03-19 QQ空间某功能缺陷导致日志存储型XSS - 5
2013-03-18 QQ空间某功能缺陷导致日志存储型XSS
2013-03-18 QQ空间某功能缺陷导致日志存储型XSS
2013-03-17 QQ空间某功能缺陷导致日志存储型XSS
2013-03-16 QQ空间某功能缺陷导致日志存储型XSS

2012-10-22 PKAV腾讯专场 - 5. 两个未修补好的历史遗留XSS，（腾讯微博，WEBQQ各一处）
2012-10-20 PKAV腾讯专场 - 4. QQ群论坛存储型XSS
2012-10-18 PKAV腾讯专场 - 2. 腾讯产品交流平台的一个js文件泄漏了一个url之后
2012-10-18 PKAV腾讯专场 - 1. 腾讯微博私信存储型XSS
2012-09-03 百度100G网盘分享功能存储型XSS
2012-08-11 当 |XSS蠕虫| 与 |QQ系统消息推送| 双剑合璧之后 ...
2012-08-10 漂流瓶：飘来的可能是局长，也可能是XSS，Orz ...

已经完成了吗？

- 只对厂商负责，不对用户负责的行为不叫负责任。

乌云数字


20000~30000
10000~20000
0~10000
0
20
40
60
80
100
120
所用时间(月)
每日提交量(个)

已经完成了吗？

- 乌云人才培养计划
  - 靠谱安全人才...堪比大熊猫...

已经完成了吗？

- 这个问题其实要问大家
- Just wooyun !

Thanks!


SequeMedia
盛拓传媒
IT168.com
www.it168.com
ChinaUnix.net
ITPUB