

[www.qconferences.com](http://www.qconferences.com)

[www.qconbeijing.com](http://www.qconbeijing.com)



QCon北京2014大会 4月17—19日

伦敦 | 北京 | 东京 | 纽约 | 圣保罗 | 上海 | 旧金山

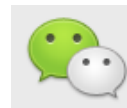
London · Beijing · Tokyo · New York · Sao Paulo · Shanghai · San Francisco

# QCon全球软件开发大会

International Software Development Conference



@InfoQ



infoqchina

软件  
正在改变世界!

# 特别感谢 QCon上海合作伙伴





# 企业安全体系建设

—— 理论与实践

胡珀 腾讯安全中心

# Who am I



## 胡珀 - lakehu

- 07年加入腾讯安全中心
- Web漏洞扫描器、恶意网址检测系统、主机安全Agent系统建设和运营
- 安全事件响应、渗透测试、安全培训、安全评估、安全规范
- 腾讯安全应急响应中心 ( TSRC )

# 目录



**我的安全世界观**

**企业安全体系的建设思路**

**腾讯应用运维安全体系分享**

**挑战 & 未来的想法**

**Q & A**

# 我的安全世界观



原 Serv-U本地权限提升的ASP实现

Author: lake2

原 轻轻绕过

Author: lake2 (http://lake2.0x04.0rd/)

(雷RT占的)

原 伪造发

Author:

程学破解Ema

原 假作真

Author: la

as string

原 PJBlog

Author: l

安全防御比黑客攻击更困难！

安全是业务发展到一定阶段的刚需

安全需要自上而下的重视



原 荐



# 思路 1

## 事件驱动

安全事件

分析提炼

安全工作

发件人:

收件人:

抄送:

主题: 【漏洞知会】安卓签名绕过漏洞知会

邮件

安卓签名绕过漏洞评估报告.doc (225 KB)

CheckShortBug.rar (517 KB)

各位:

近日 Bluebox 公司声称 Android 存在安全漏洞, 99% 设备受影响。恶意开发者可在不破坏特定的恶意操作。目前, 网上已有相应的 PoC 代码公布, 可能已被外部用户恶意利用。该漏洞详情请参见附件中的《安卓签名绕过漏洞评估报告》。

### 【漏洞原理】

- 1、签名校验前会先解压 ZIP 压缩包, 当遇到两个同路径同名文件时, 后者 (正常 dex)
- 2、执行程序时, 会以第一个 dex 文件为准, 导致前者 (恶意 dex) 被执行。

特定的阿拉伯字符 (见附图 1) 上述 iOS 漏洞影响。目前该漏洞

户无法正常使用公司产品; 器、短信应用等。

多家互

发表于:

多家互联

网站部入侵事件



# 思路 2



抓大放小 解决主要矛盾

**HACKED!**



IDC入侵

内网入侵

客户端漏洞

Web漏洞

DDoS

终端漏洞

IDC安全

内网安全

客户端  
安全

应用安全

DDoS防  
御体系

终端安全审计

# 思路 3



## 安全部门的自身定位

*取法于上，仅得为中；取法于中，故为其下*



安全平台部



业务的核心  
竞争力



全面保障业  
务发展



应急响应



QQ安全中心

AQ.QQ.COM 在线生活,安全护航



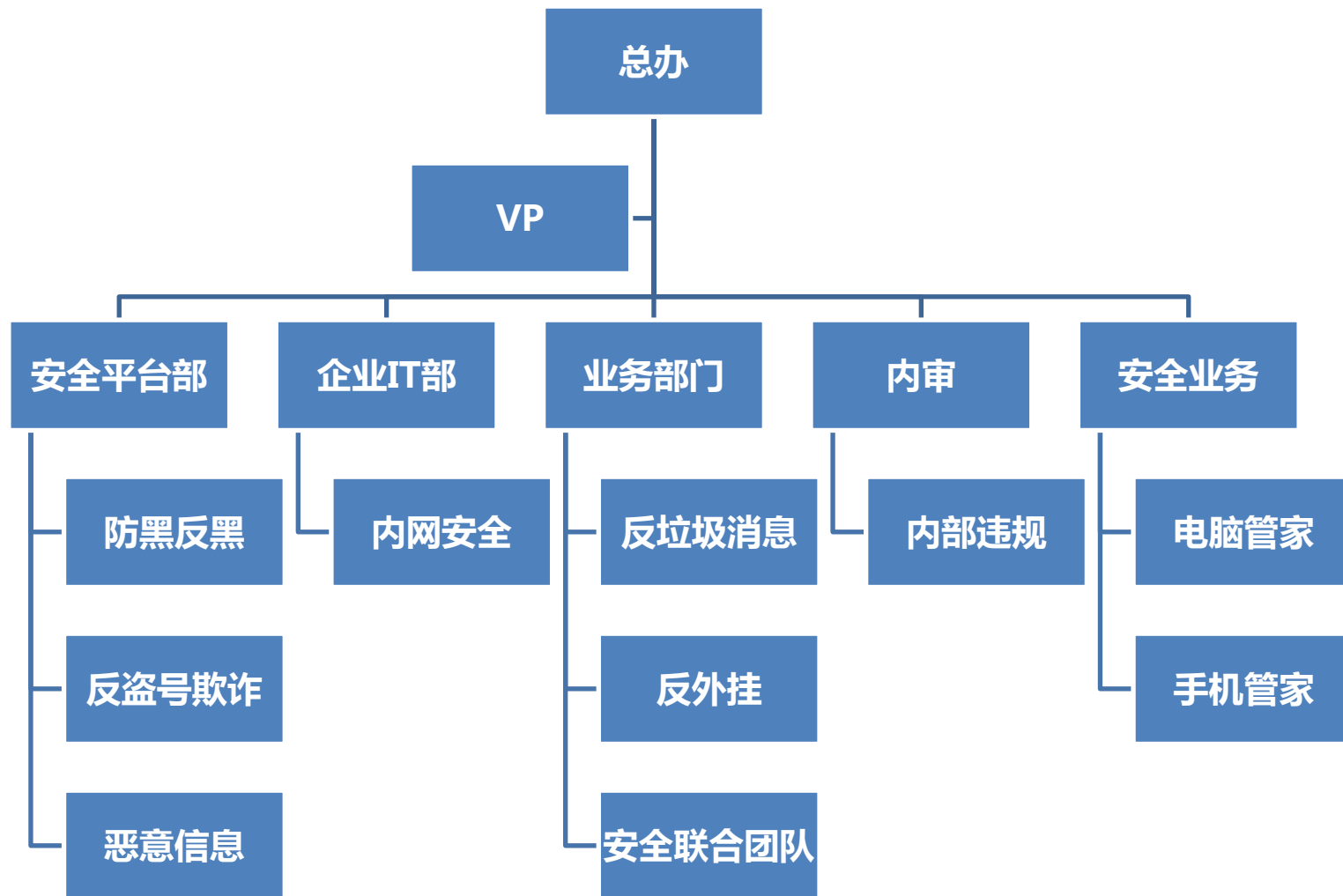
云安全

提供多重可靠防护

免费安全保护

您在购买腾讯云服务后，只需  
开启想要的安全服务，即可免  
费享受相应的安全保护。

# 腾讯安全体系介绍



# 腾讯安全体系介绍



先后组建运维安全团队、  
应用安全团队

2006  
黑客入侵

组建信息安全团队

2008  
不和谐信息

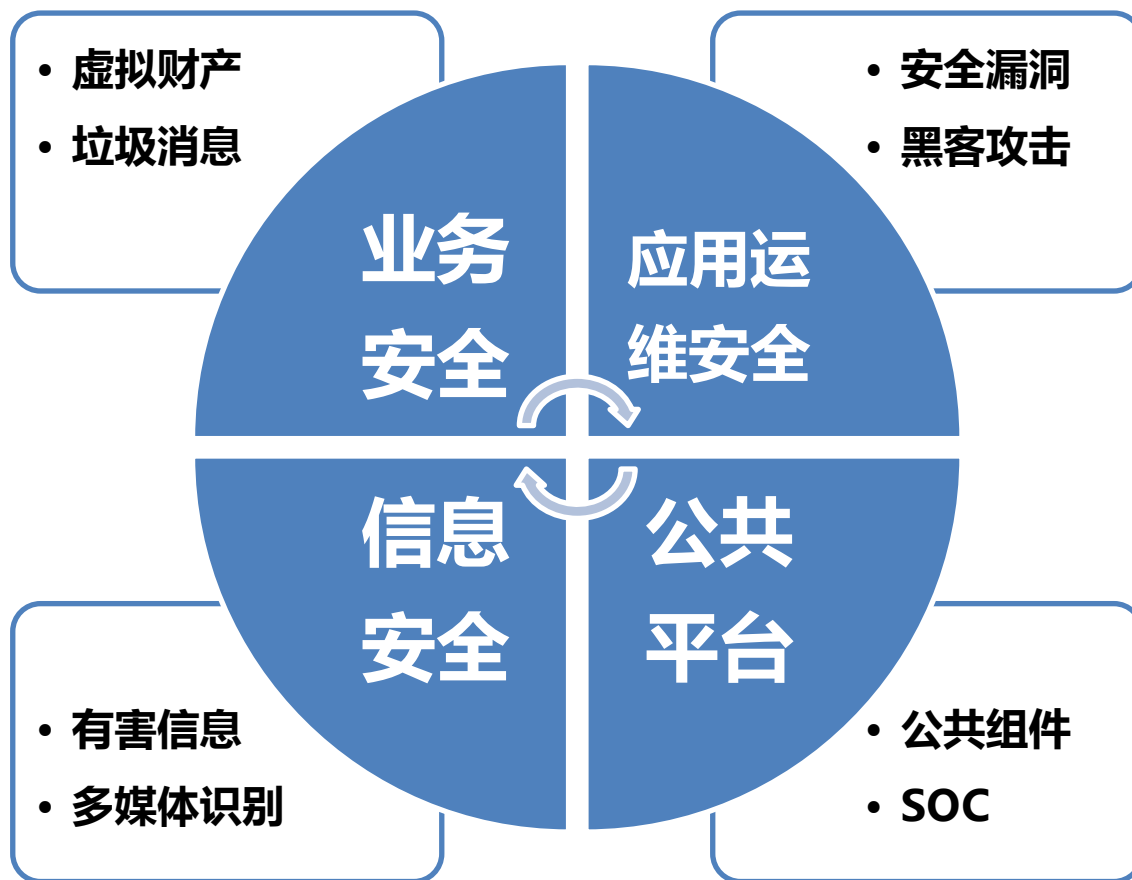
2007  
虚拟财产被盗  
垃圾消息  
欺诈消息

组建业务安全团队

# 腾讯安全体系介绍



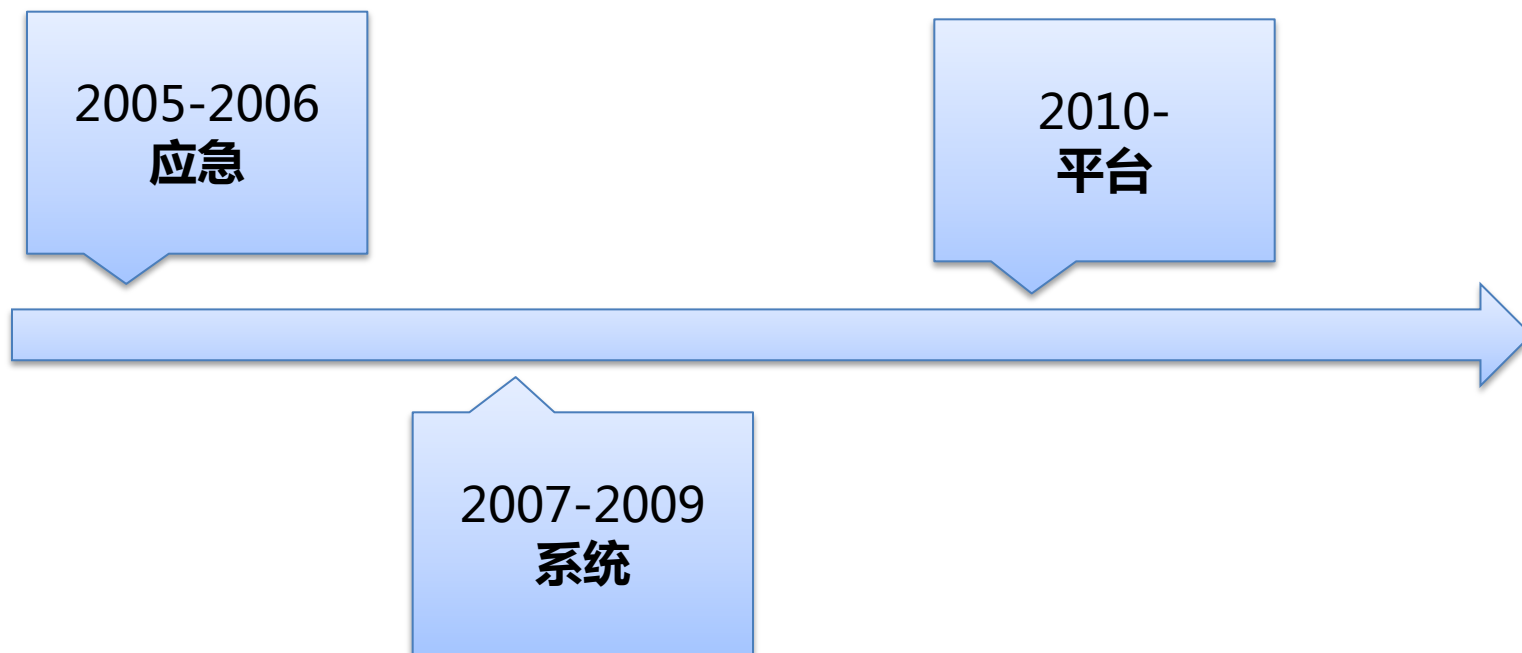
## 关于安全平台部



# 腾讯安全体系介绍



## 腾讯安全中心的几个发展阶段



# 腾讯安全体系分享



## TSDL思想

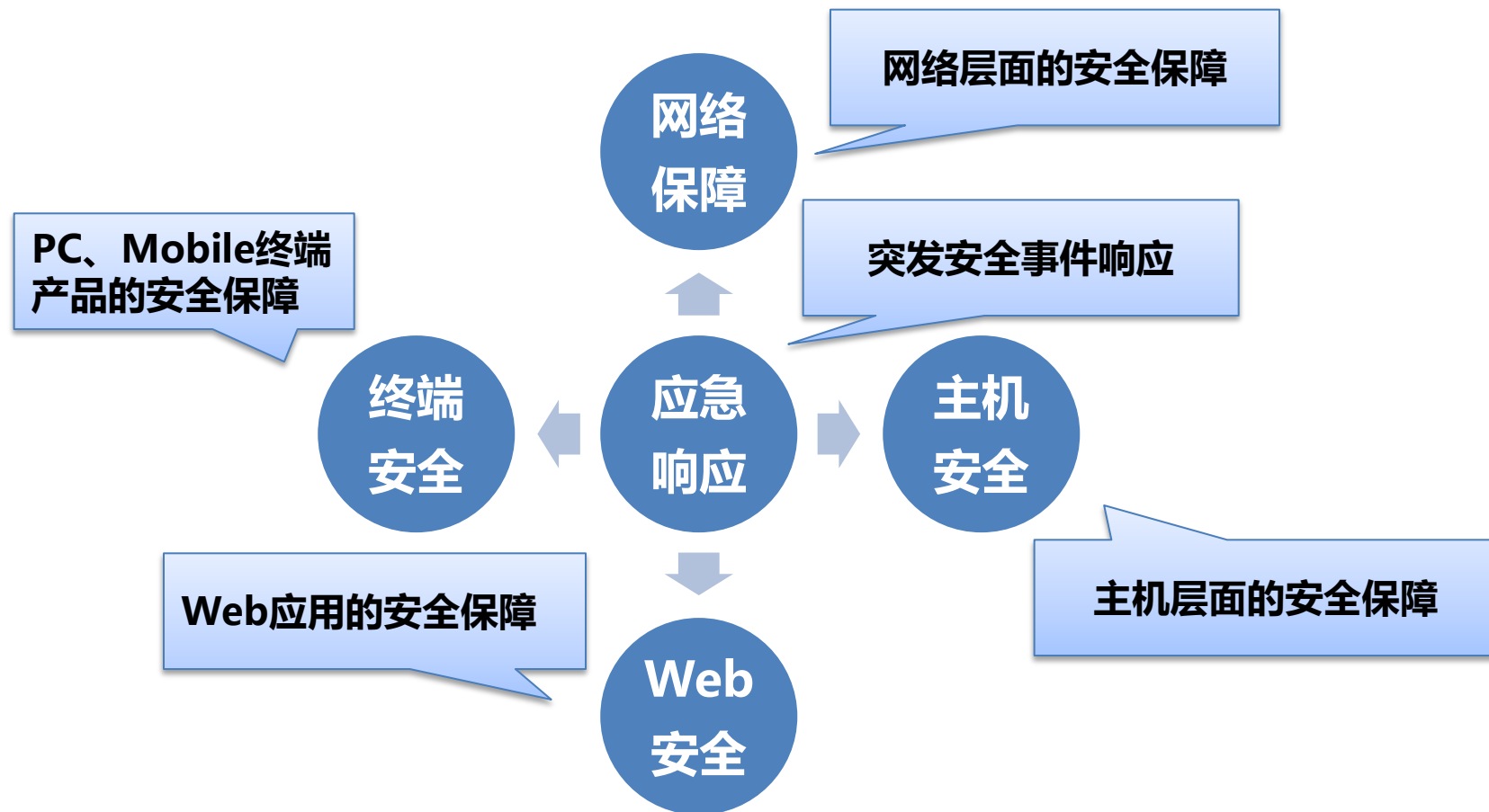




# 腾讯安全体系分享



## 应用运维安全团队架构



# 腾讯安全体系分享



## 网络层威胁场景



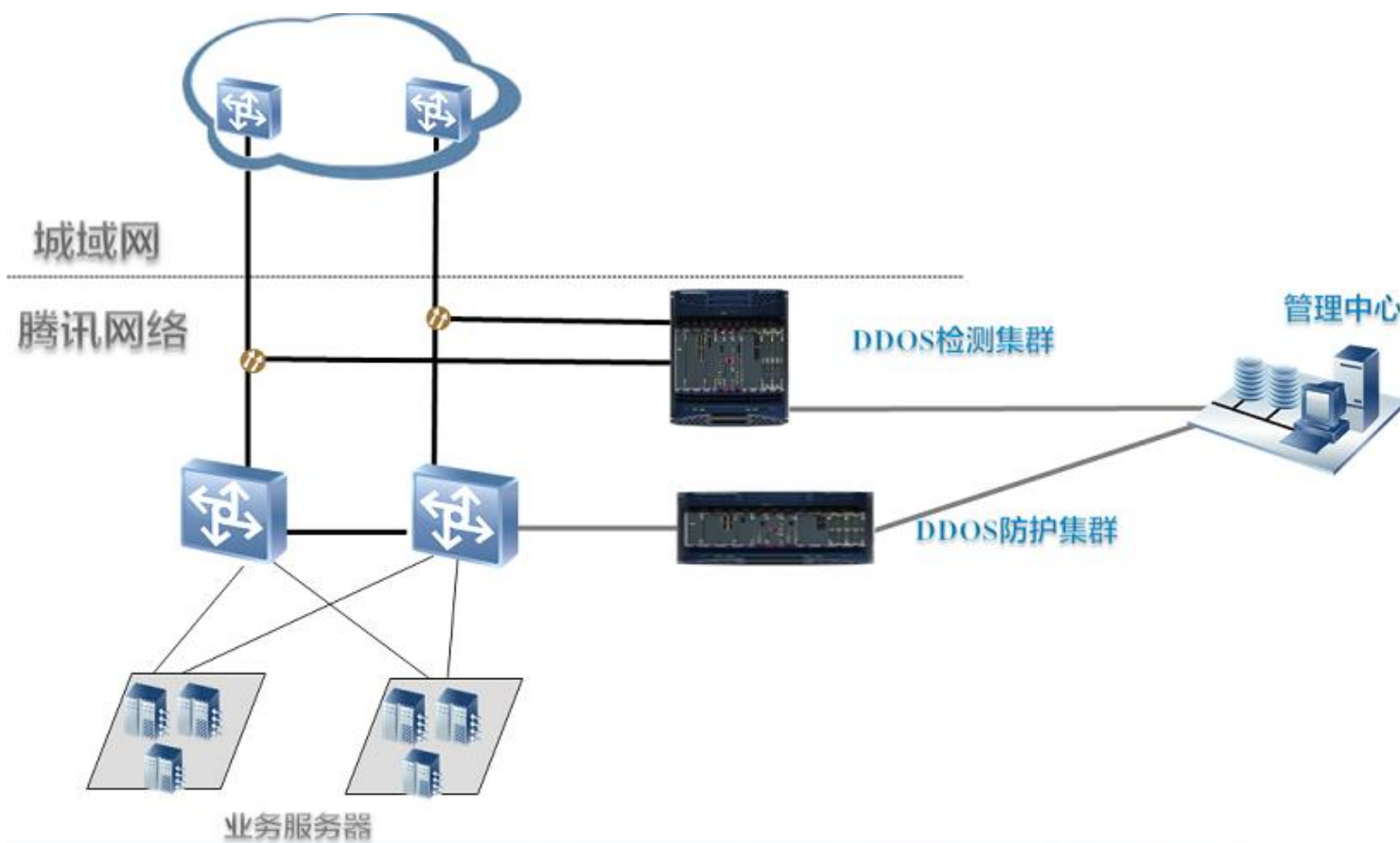
C:\Python25\python.exe

```
WARNING: No route found for IPv6 destination :: (no default route?)
TCP Hijacking Detector by lake2
[+] Sniffing ....
74.125.128.199 has been hijacking !!!   debug info : 145  <-> 139
=>
74.125.128.199 has been hijacking !!!   debug info : 132  <-> 139
74.125.128.199 has been hijacking !!!   debug info : 134  <-> 139
74.125.128.199 has been hijacking !!!   debug info : 209  <-> 139
74.125.128.199 has been hijacking !!!   debug info : 211  <-> 139
=>
security.tencent.com
```

# 腾讯安全体系分享



## 网络安全平台：DDoS检测与防护

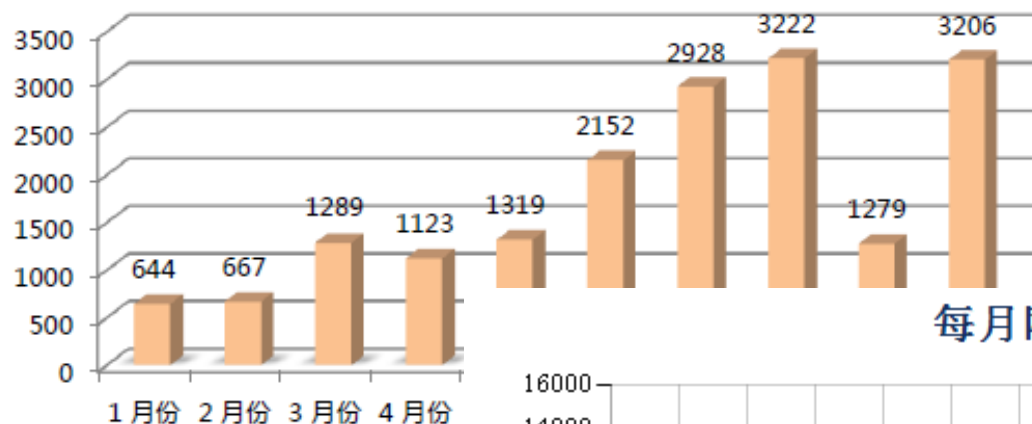


# 腾讯安全体系分享

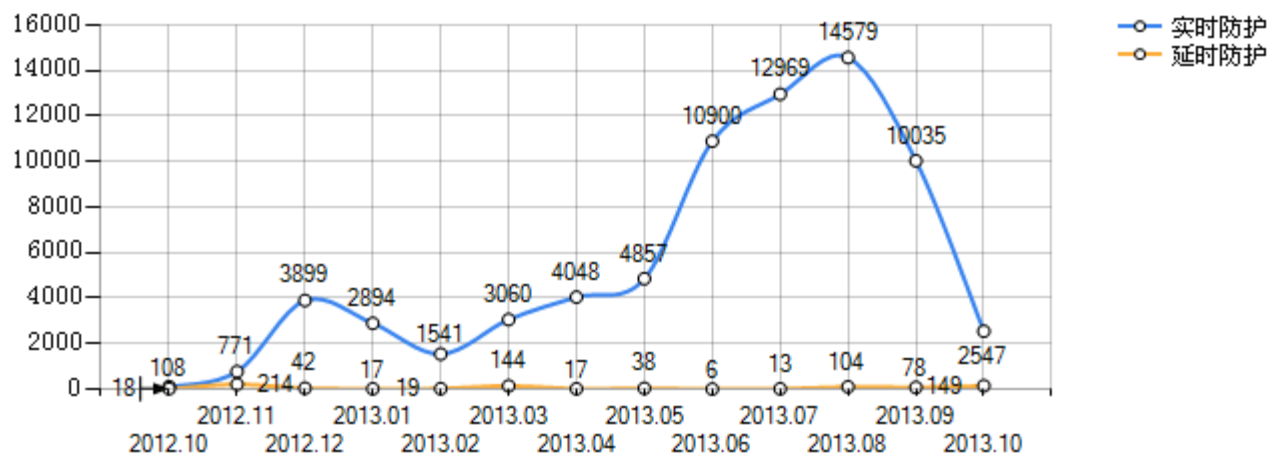


## 网络安全平台：DDoS检测与防护

### 全公司每月网络攻击总次数分析图

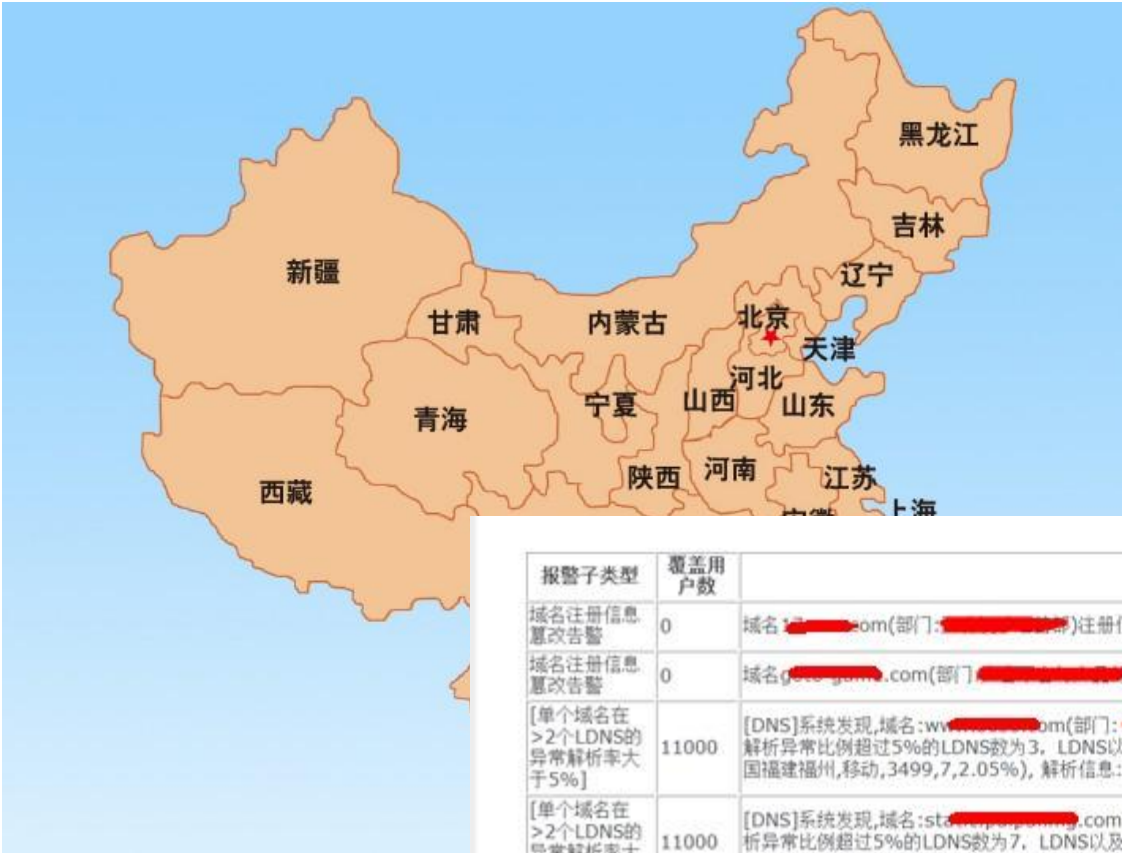


### 每月网络攻击防护分析





## 网络安全平台：DNS解析监测



### 1 ) Local DNS劫持监测

覆盖全国各主要城市Local DNS

### 2 ) 权威DNS篡改

权威DNS监测

报警子类型	覆盖用户数	细节
域名注册信息篡改告警	0	域名 123456789.com(部门: 研发部)注册信息发生变动, 请关注(from: 123456789.com)
域名注册信息篡改告警	0	域名 gds-gsm.com(部门: 市场部)注册信息发生变动, 请关注(from: gds-gsm.com)
[单个域名在>2个LDNS的异常解析率大于5%]	11000	[DNS]系统发现, 域名: www.123456789.com(部门: 研发部)在2.5小时内, 非故障类的解析异常比例超过5%的LDNS数为3, LDNS以及解析的详细信息为(TOP 2): LDNS: 123456789.com(中国福建福州, 移动, 3499, 7, 2.05%), 解析信息: 有风险: 39%;
[单个域名在>2个LDNS的异常解析率大于5%]	11000	[DNS]系统发现, 域名: sta.123456789.com(部门: 市场部)在2.5小时内, 非故障类的解析异常比例超过5%的LDNS数为7, LDNS以及解析的详细信息为(TOP 2): LDNS: 123456789.com(中国福建福州, 移动, 3499, 7, 2.05%), 解析信息: 有风险: 38.7%; security.tencent.com



# 腾讯安全体系分享



## 主机层威胁场景



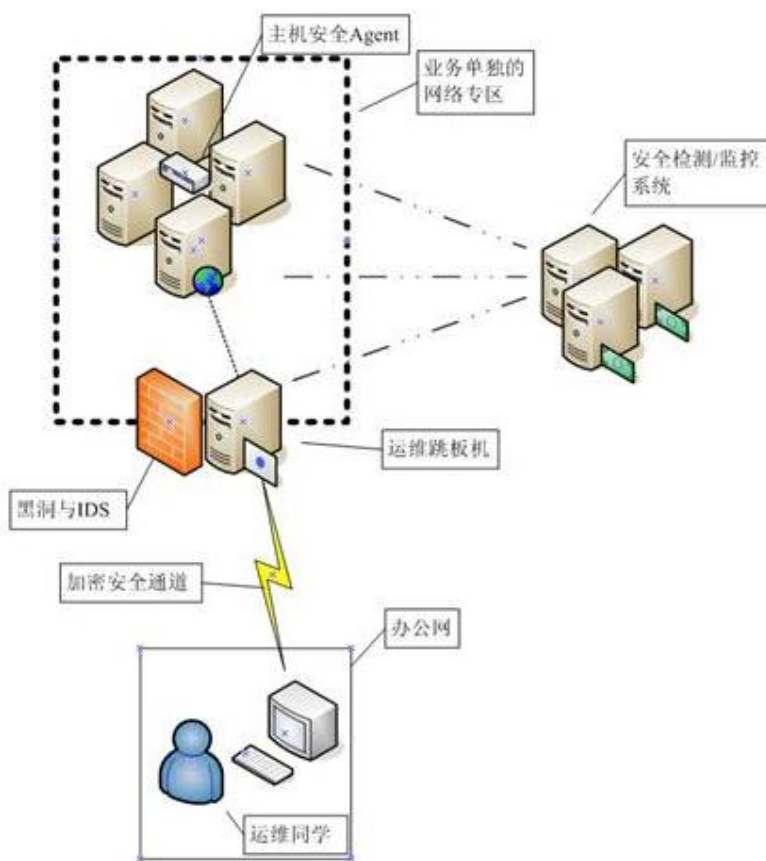
- 2013-07-17 中国联通某分站struts命令执行
- 2013-07-17 易宝支付struts2命令执行漏洞! (已证明)
- 2013-07-17 京东某分站命令执行漏洞
- 2013-07-17 土豆网主站存在struts2命令执行漏洞! (已证明)
- 2013-07-17 51比购网命令执行
- 2013-07-17 京东商城分站存在struts2命令执行漏洞
- 2013-07-17 一号店旗下某网站, struts2命令执行漏洞 (已证明读取到etc/passwd)
- 2013-07-17 京东商城某分站struts2命令执行漏洞
- 2013-07-17 百合网最新struts2任意命令执行漏洞大礼包集合 (方便运维人员集中修复)
- 2013-07-17 京东商城旗下奢侈品as600p, struts2命令执行漏洞 (已证明读取到etc/passwd)
- 2013-07-18 金蝶主站struts2命令执行漏洞

struts2命令执行漏洞

# 腾讯安全体系分享



## 主机安全平台：运维安全整体架构

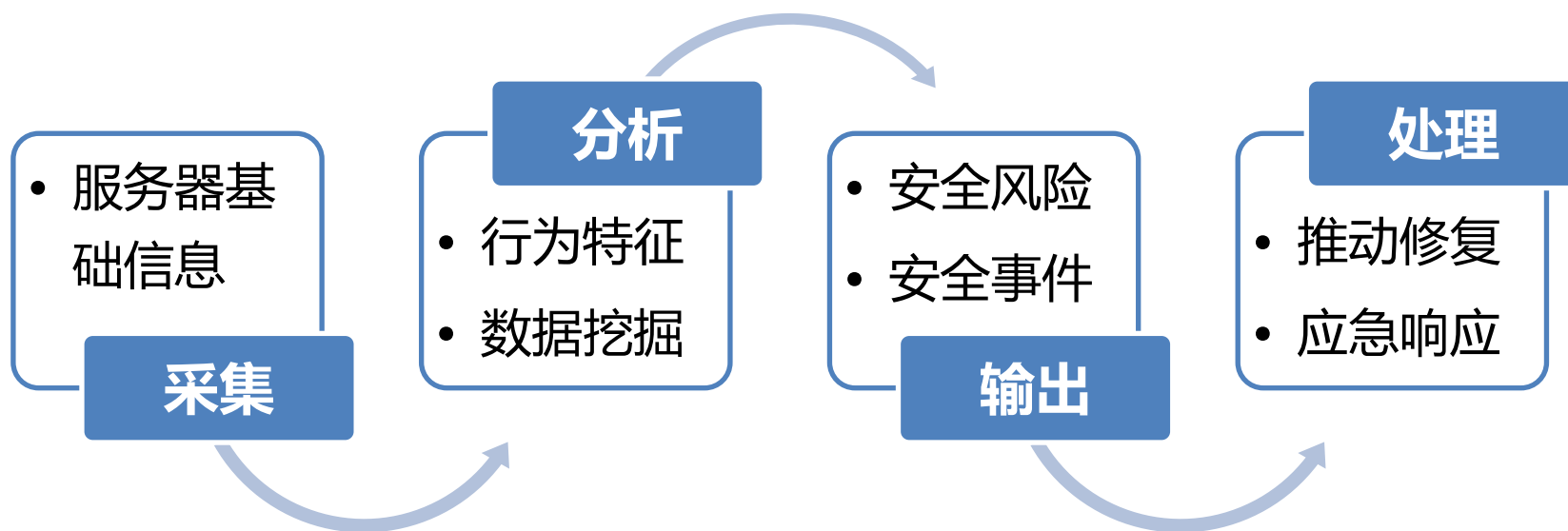




# 腾讯安全体系分享



## 主机安全平台：安全Agent



## 主机安全平台：安全Agent

```
| -firefox---run-mozilla.sh---firefox-bin-+-plugin-containe---{  
|                                     |  
|-gnome-terminal-+-3*[bash]  
|                                     |  
|                                     |-bash--grep  
|                                     |-bash---netcat
```

### 软件版本信息 (共1条)

最终机器	软件	版本	软件路径	配置文件路径
机器ID: 16989 [REDACTED] 2 98	php	5 [REDACTED]	/usr [REDACTED] /ap [REDACTED] so	/usr/l [REDACTED] nf/httpd.conf
	ssh secure shell	3 [REDACTED]	/usr [REDACTED] /sb [REDACTED]	/etc/s [REDACTED] ig
	apache	2 [REDACTED]	/usr [REDACTED] /ap [REDACTED]	/usr/l [REDACTED] nf/httpd.conf

11:05:13  
两分钟都不到...

11:06:21

我正准备看看history

11:06:27

啪的一下就啥都没了。

IP为10.16.8.5的Agent于2011-12-13 14:48:01发现webshell:  
文件路径: /usr/share/agent/htdocs/tsrc/backdoor.php  
分值: 85, 文件属主: root, mtime: 2011-12-13 14:34:02, ctime: 2011-12-13 14:34:02  
部门: 安全中心, 机器负责人: hantingjia  
匹配规则:

**事件描述：**

```
2002: eval(base64_decode("aWYoaXNzZXQ3PjB0T09LSUVbJ2N  
0lFWydjbSddKS4nIDI+JjEnKTtzZXRjb29raVNoPjB0T09LSUVbJ2N  
Y29udGVudHMokSkUJF9DT09LSUVbJ2NwJ10pO29X2Vu  
4001: eval(base64_decode("aWYoaXNzZXQ3PjB0T09LSUVbJ2N  
0lFWydjbSddKS4nIDI+JjEnKTtzZXRjb29raVNoPjB0T09LSUVbJ2N  
Y29udGVudHMokSkUJF9DT09LSUVbJ2NwJ10pO29X2Vu
```

16-06-21

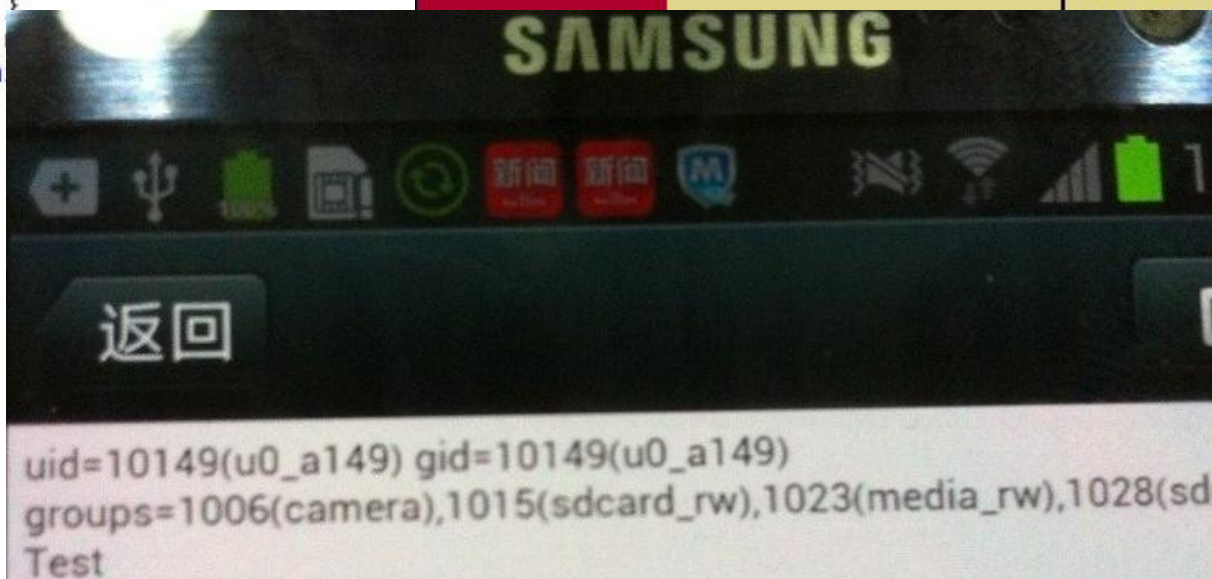
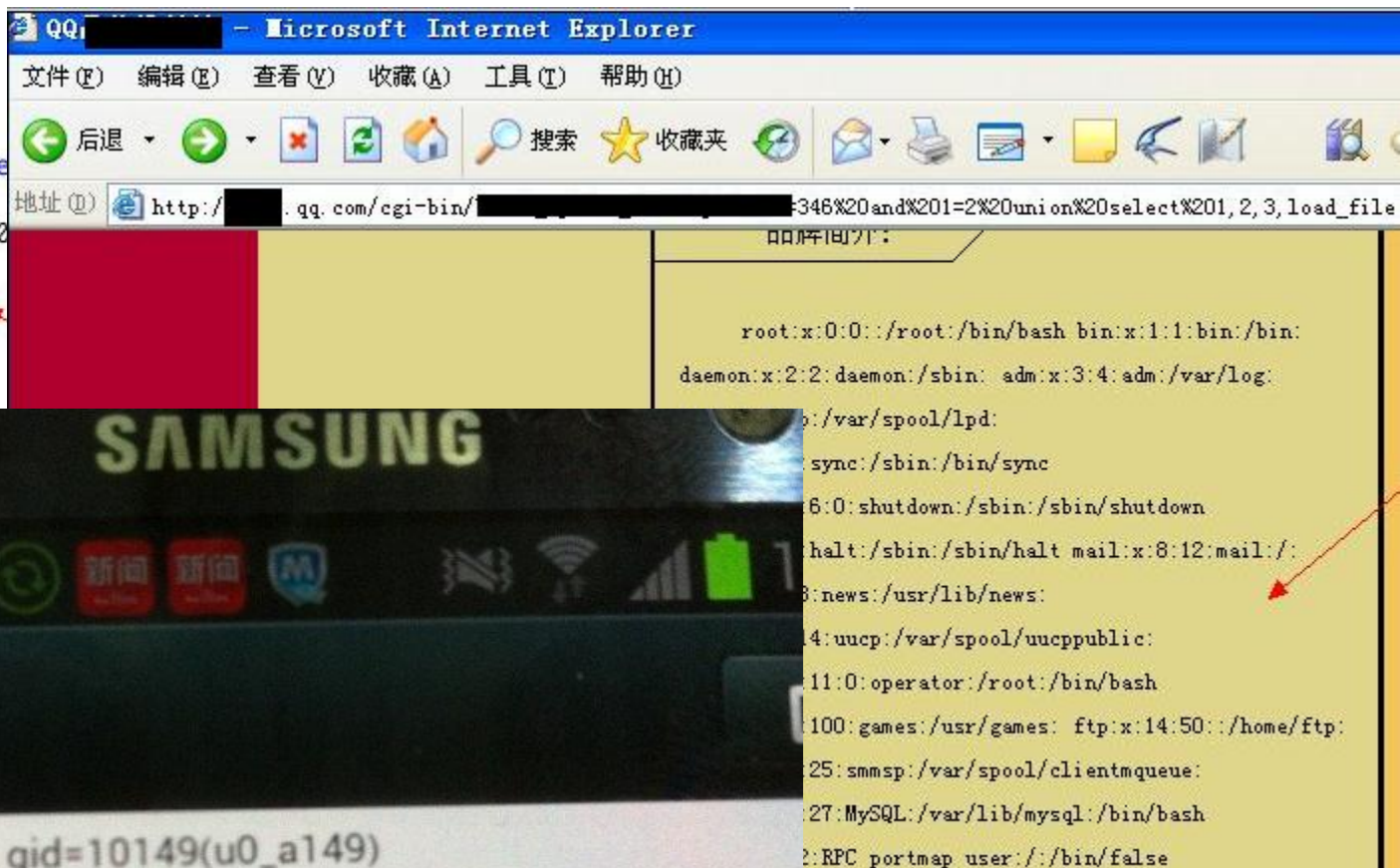
21:25:54

21:25:54

# 腾讯安全体系分享

## 应用安全威胁场景

```
UINT nNum = 0;  
do  
{  
    if (2 != fread(&cTmp, size  
    cBuf[nNum] = (cTmp[0] != 0  
    if (cBuf[nNum] == cKey)  
    {  
        break;  
    }  
} while (1);
```





## 应用安全平台：Web/Server漏洞检测

SQL Injection  
XSS  
CSRF  
JSON Hijacking  
OS Injection  
....

- 远程扫描
- 代码审计

Web



- 远程扫描
- 本地检测

Server



high-risk port  
low version  
remote overflow  
danger config  
weak pwd  
....

# 腾讯安全体系分享



## 应用安全平台：Web/Server漏洞检测

### 腾讯网站安全检测

自定义扫描

自定义扫描 > 域名爬扫

域名爬扫

单CGI扫描

任务查询

帮助中心

漏洞参考标准

风险等级评分标准

添加站点

站点列表 \*

关注人

扫描时间 2013-10-28 09:15:00

设置Host ip

指定UIN登录 uin

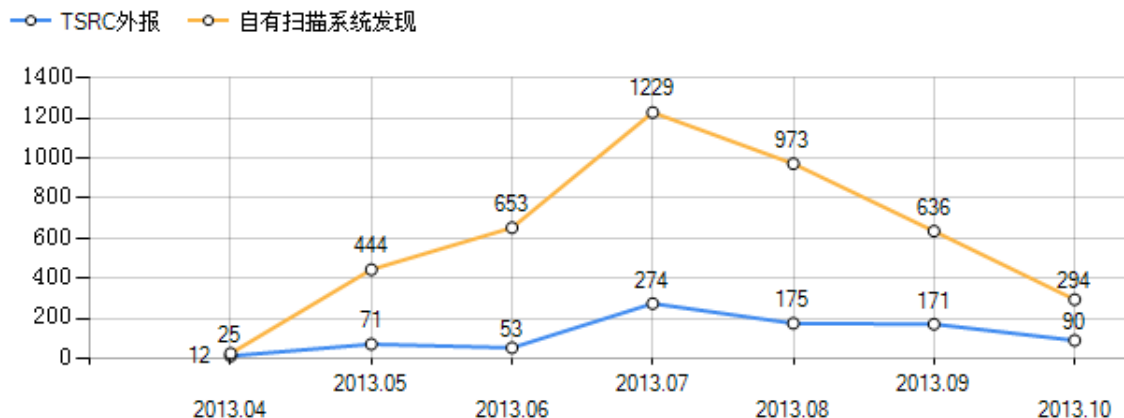
任务通知 ☐ 短信 ☒ RTX

HTTP配置 +

爬虫配置 +

规则配置 -

漏洞月趋势图





## 应用安全平台：客户端漏洞审计

danger func  
danger COM  
DLL Hijacking  
overflow  
....

- 代码审计
- 动态分析
- 静态分析

PC



- 代码审计
- 动态分析
- 静态分析

Mobile



danger func  
storage  
transmission  
组件权限  
....



# 腾讯安全体系分享



## 应用安全平台：客户端漏洞审计

1. 项目名称: QQ [redacted] [Tips: 如果这里没有您的项目名称, 请联系我们, 谢谢](#)

2. 版本: [redacted] [Tips: 仅接受标准的4位版本号, 例如2.1.768.202](#)

3. 负责人: [redacted]

4. 部门: 安全平台部

5. 安装包: [单击选择exe安装包文件](#) [Tips: 限制150M以内, 文件格式限于使用NSIS制作](#)

已上传文件:

6. 静默参数: [redacted] [Tips: 安装包的静默安装参数, 例如: \[redacted\]](#)

7. 安装路径: [redacted] [Tips: 路径不需带盘符, 例如: \[redacted\]](#)

选择子系统

☒ 全部

☒ 二进制文件审计 ☒ ActiveX控件模糊测试 ☒ DLL hijacking

☒ 第三方漏洞审计 ☒ DNS频率审计 ☒ ActiveX污点分析

☒ 统一关键词过滤 ☒ CGI模糊测试 ☒ 可信路径漏洞

SVN路径: [redacted]

☒ C/C++/ObjC语言安全扫描

如果产品包含多个SVN路径, 请以换行或者分号为间隔。  
合理的SVN路径样例: http(s):/[redacted]

SVN路径: [redacted]

☒ Java/Jsp语言安全扫描

如果产品包含多个SVN路径, 请以换行或者分号为间隔。  
合理的SVN路径样例: http(s):/[redacted]

SVN路径: [redacted]

☒ PHP语言安全扫描

如果产品包含多个SVN路径, 请以换行或者分号为间隔。  
合理的SVN路径样例: http(s):/[redacted]

☒ 驱动安全审计

驱动XML路径: [redacted]

[单击选择xml配置文件](#) [Tips: 第一次配置? 请点击这里。](#)

主题: [金剛系统] [redacted] 7.4. [redacted] 00审计结果邮件

附件: QQ [redacted] Setup\_7.4.15653.400\_4375\_CompilerOptions.csv (523 B) QQ [redacted] p\_7.4.15653.400\_4375\_DnsResult.csv (927 B)

二进制文件审计 [redacted] 检查未通过

三方的0个, 所有文件已经审计备案。  
SAFESEH安全编译选项: 0个未开启;  
ASLR安全编译选项: 0个未开启;  
DEP安全编译选项: 1个未开启。  
详情请参考附件:  
QQ [redacted] 4375\_CompilerOptions.csv.

ActiveX控件模糊测试 未发现安装包中包含任何ActiveX控件 检查通过, 未发现安全漏洞和潜在的安全风险

DLL hijacking审计 经过检查, DLL劫持漏洞审计未发现问题。  
同时, 经过模拟DLL劫持审计, 发现以下4个可执行文件在加载模块前未对文件合法性进行校验:

C:\Program Files\Tencent\QQ\bin\QQApplication.exe	rApplication.exe;
D:\Program Files\Tencent\QQ\bin\QQLiveup.exe	erLiveup.exe;
C:\Program Files\Tencent\QQ\bin\QQ.exe	exe;
C:\Program Files\Tencent\QQ\bin\QQ.exe	exe;

请及时以上文性加上文件合法性校验, 以防止恶意代码利用



# 腾讯安全体系分享



## 应用安全平台：WAF

No.	Time	Source	Destination	Protocol	Length	Info
190	9.75939700	10.26.234.31	113.108.12.60	TCP	66	58355 > http [SYN]
197	9.76787600	113.108.12.60	10.26.234.31	TCP	66	http > 58355 [SYN]
198	9.76793000	10.26.234.31	113.108.12.60	TCP	54	58355 > http [ACK]
238	10.0607890	10.26.234.31	113.108.12.60	HTTP	636	GET / HTTP/1.1
239	10.0630830	113.108.12.60	10.26.234.31	TCP	60	http > 58355 [ACK]
240	10.0779570	113.108.12.60	10.26.234.31	TCP	1502	[TCP segment of data stream 0]
241	10.0780740	113.108.12.60	10.26.234.31	TCP	1502	[TCP segment of data stream 0]
242	10.0781050	10.26.234.31	113.108.12.60	TCP	54	58355 > http [ACK]
243	10.0810460	113.108.12.60	10.26.234.31	TCP	1502	[TCP segment of data stream 0]
244	10.0811580	113.108.12.60	10.26.234.31	TCP	1502	[TCP segment of data stream 0]
245	10.0811770	10.26.234.31	113.108.12.60	TCP	54	58355 > http [ACK]
246	10.0812800	113.108.12.60	10.26.234.31	TCP	1502	[TCP segment of data stream 0]
247	10.0833940	113.108.12.60	10.26.234.31	HTTP	762	HTTP/1.1 200 OK
248	10.0834270	10.26.234.31	113.108.12.60	TCP	54	58355 > http [ACK]
432	15.0750180	113.108.12.60	10.26.234.31	TCP	60	http > 58355 [FIN]



WAF



# 腾讯安全体系分享



## 应急响应：struts2 0day漏洞响应的案例

漏洞发现

漏洞分析

更新规则

推动修复

修复完毕

**10:00**

外部报告腾讯某  
站点存在struts  
0day漏洞

**10:40**

掌握漏洞原理及  
检测、修复办法

**10:50**

漏洞扫描器规则  
紧急更新

**11:40**

使用struts站点  
检测完毕，公司  
级安全预警

**18:30**

自有站点全部修  
复

总结&优化

如何快速解决安全风险？WAF

如何防御类似0day？主机agent新特性

# 腾讯安全体系分享



## 应急响应：漏洞奖励计划

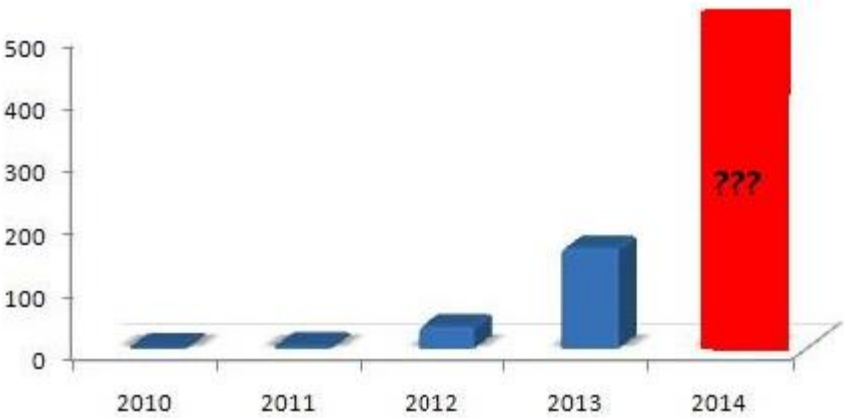


腾讯安全应急响应中心  
Tencent Security Response Center

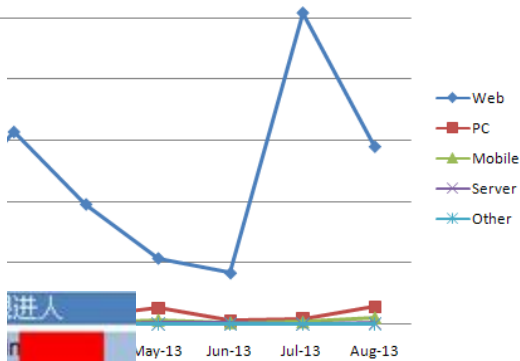
- 2013-09-04 因“腾讯漏洞奖励计划-用户兑换”获得1个“美心月饼”
- 2013-09-01 因“腾讯漏洞奖励计划-用户兑换”获得1个“移动硬盘”
- 2013-08-28 因“腾讯漏洞奖励计划-用户兑换”获得1个“手机”
- 2013-08-12 因“感谢一直以来对TSRC的帮助和支持”，赠送 TSRC 2013年“最佳合作伙伴”奖杯
- 2013-07-19 因“腾讯漏洞奖励计划-用户兑换”获得1个“Andriod手机”
- 2013-05-04 因“腾讯漏洞奖励计划-用户兑换”获得1个“三星GALAXY S4”
- 2013-03-06 因“腾讯漏洞奖励计划-用户兑换”获得1个“雷蛇八爪鱼鼠标”
- 2013-03-06 因“腾讯漏洞奖励计划-用户兑换”获得1个“Q影”
- 2013-03-06 因“腾讯漏洞奖励计划-用户兑换”获得1个“New iPad”
- 2013-02-05 因“提交高质量漏洞”获得1个“白兔”
- 2013-01-14 因“2012年年度突出贡献-漏洞之王”获得1个“金蛇”
- 2013-01-07 因“2012年12月月度奖励-力拔头筹”获得1个“金蛇”
- 2012-12-06 因“2012年11月月度奖励-漏洞猎手”获得1个“金蛇”
- 2012-12-06 因“2012年11月月度奖励-力拔头筹”获得1个“金蛇”
- 2012-11-07 因“2012年10月月度奖励-漏洞猎手”获得1个“金蛇”
- 2012-11-07 因“2012年10月月度奖励-力拔头筹”获得1个“金蛇”
- 2012-11-07 因“2012年10月月度奖励-力拔头筹”获得1个“金蛇”

所属系统  
漏洞扫描

## 腾讯漏洞奖励计划投入金额



TSRC分类漏洞月度统计



Web 漏洞检测	高危漏洞	漏洞扫描	增加按目	Bin
信息泄漏检测	Web 目录	扫描文件	缩包检测	Cal
Web 漏洞检测	Tomcat	漏洞扫描	优化扫描	Bin
			测试文件	
			实现检测	
			漏洞的功	

# 未来的一些想法



## 分享：技术分享、安全服务



当心！您当前使用的APP存在Android WebView 挂马漏洞！  
请不要用这个APP打开不可信的外部链接！

### 【关于腾讯安全漏洞奖励计划】

腾讯一直非常重视产品和业务的安全问题，除了建设专门的

### 免费安全保护

您在购买腾讯云服务后，只需  
开启想要的安全服务，即可免  
费享受相应的安全保护。



云安全

提供多重可靠防护

### 安全服务1：防DDoS攻击

- 腾讯云安全提供专业的防DDoS攻击服务，能够帮您的云服务抵御CC、SYN flood、UDP flood等多种攻击。

### 安全服务2：漏洞扫描

- 腾讯云安全可以定期对您的云服务进行各种安全漏洞检测，并将检测结果及时反馈给您。

### 安全服务3：入侵检测

- 腾讯云安全可以定期对您的云服务进行木马、暗链检测，并将检测结果及时反馈给您。

# 未来的一些想法



国际化：随业务国际化的安全国际化





# 未来的一些想法



联盟：企业安全联盟





**mrhupo@qq.com**

**lakehu@tencent.com**