脱 茧

Coolc

腾讯安全平台部负责人

腾讯T4安全专家

腾讯安全通道会长

腾讯技术委员会常务委员

信息安全决策委员会委员

十年以上的网络安全从业经验。2005年进入腾讯，先后负责过应用运维安全、业务安全、信息安全等领域。曾负责北京奥运会、上海世博、广州亚运会、广电、粮油总局等安全建设工作。

财经观察 **重要的不是赚钱而是防范风险**

中国的潜在增长率可能比十年前少掉一半，这个就是商品界所要面临的新常态。

智库 **再不有效救市则后患无穷**

谭松珩：最佳的救市时机转瞬即逝，我们希望人民银行能够抓住机会，避免中国经济滑入深渊。

代码/名称/拼音 全部

我的自选股 手机版自选股

颜色配置: 红涨绿跌 红跌绿涨

亚太 北美 欧洲 期货 外汇

上证指数	3507.19	-219.93

深证成指	11040.89	-334.71
恒生指数	23516.56	-1458.75
腾安指数	2115.03	-112.40

最近访问股 我的自选股

沪指重挫近6% A股新增十二道救市金牌

未来仍可能会继续表现出持续震荡的态势，在这种市场下追涨杀跌具有非常大的风险...[详细] 522

热点推荐 | 招聘 编辑产品经理 2015互联网金融外滩峰会 白银大赛高手日收益187%

要 闻

李克强主持国务院常务会议:部署整改审计问题

棱镜

9日9夜：峭壁边缘拯救A股

制度的缺憾成为股灾罪魁，由此带来的系统性风险一触即发…[详细]

- 57期：惊魂48小时：A股周一或混战
- 56期：出租车“钓鱼”专车事件调查

财经观察

重要的不是赚钱而是防范风险

中国的潜在增长率可能比十年前少掉一半…[详细]

我们所处的互联网行业
正在乘风破浪，风头正劲

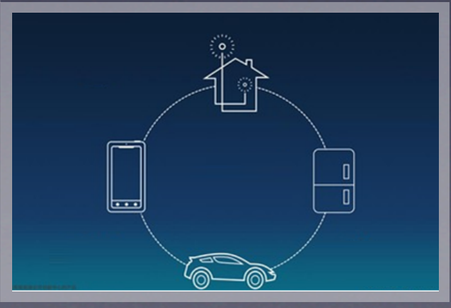
移动互联网

大数据

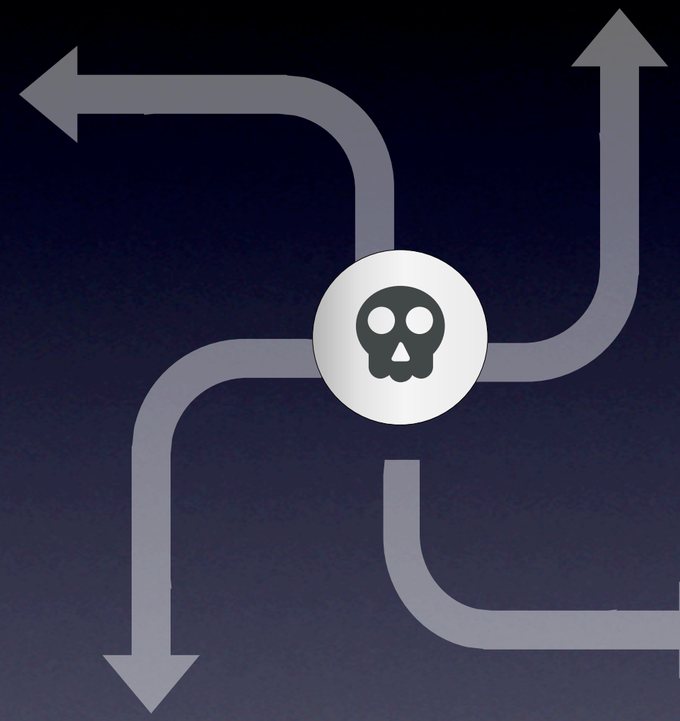
云计算

智能设备

物联网



基础组件安全
漏洞的快速处置
——心脏滴血



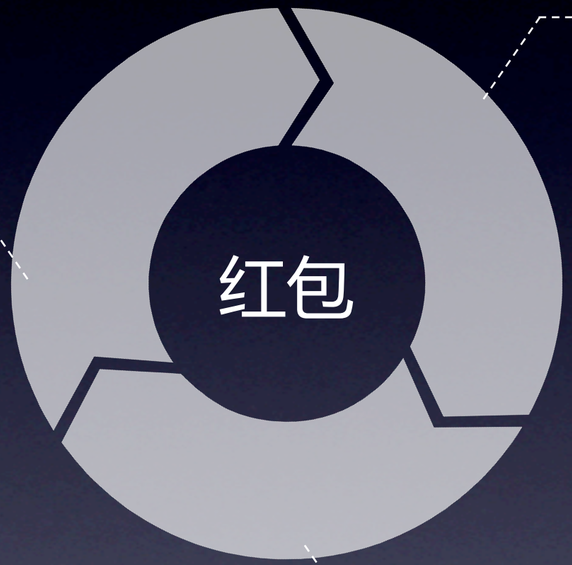
无线业务安全

海量业务环境
下APT攻击的
发现和对抗

泛安全的崛起
——利用互联网金融洗钱
——利用养号和外挂抢红包
——第三方安全

红包的故事

- 10.1亿次微信红包收发总量
- 110亿次摇一摇互动总量
- 8.1亿次/分钟的峰值数据



业务场景复杂

---手Q、微信
---H5、原生
---附件、摇一摇
---个人红包、企业红包

临时变更和紧急扩容

历史包袱

--陈旧系统

攻防对抗Top3

跨站脚本攻击86%、SQL注入7%、身份鉴权类5%、信息显示伪造2%

加固了1.5万台重点活动业务的机器如彩票/红包/微信等

“合买彩票”攻防，拦截恶意请求24万次

黑产团伙Top5

广东
广西
山东
江苏
河南

最终满意的效果
但是**准备好**了吗？

游戏的那些事儿

宙斯盾

腾讯DDoS实时防御系统

2014年全网攻击概况

总攻击次数：150,492 次

最大攻击流量：100 G

最长攻击时间：23 小时 59 分 50 秒

攻击目标业务TOP 5

游戏：72,300 次

DNS：63,222 次

腾讯云：21,021 次

网站：1,370 次

QQ：470 次

攻击时间滚动

区域	业务	攻击类型	流量
天津市	DNS	UDPFLOOD	915 Mbps
深圳市	DNS	DNSFLOOD	150,213 qps
深圳市	DNS	DNSFLOOD	2,361,702 qps
深圳市	DNS	UDPFLOOD	1,640 Mbps
东莞市	游戏	UDPFLOOD	2,794 Mbps
成都市	DNS	DNSFLOOD	106,479 qps
成都市	DNS	DNSFLOOD	1,605,749 qps
成都市	DNS	UDPFLOOD	1,115 Mbps
成都市	DNS	DNSFLOOD	203,717 qps
上海市	DNS	DNSFLOOD	1,830,730 qps
杭州市	DNS	DNSFLOOD	1,728,788 qps

当天最大攻击流量趋势图

当天攻击类型占比

当天累计攻击次数

19,653 次，163倍

暴力破解 839万

Web渗透 197万

取得了满意的效果，但这些科学吗？
真的**准备**好了吗

危机解决了，不等于问题解决

茧

云计算	数据保护、海量攻防对抗
支付安全	自然人和征信 木马对抗预埋
智能设备	隐私保护 经典场景历史重演

到底是真的好，还是在享受红利？

如果跑不赢业务创新，是否是可持续性发展呢？

破茧

速度：谁在等谁，有何种方法可以让安全，跟上业务创新？人 云 数据；要狩猎，不要农耕

视角：安全不应有“门第观念”，兼收并蓄法务、产品设计、风控的理念和做法。拿来主义，当仁不让

人才：行业拥抱变革，人才观更应该拥抱变革，安全会走进更多的行业，也会有更多人走进来改变格局

新红包

人民战争

--利用tsrc的情报体系
--聚焦安全社区、微博和微信朋友圈

海量机器的安全加固和监控

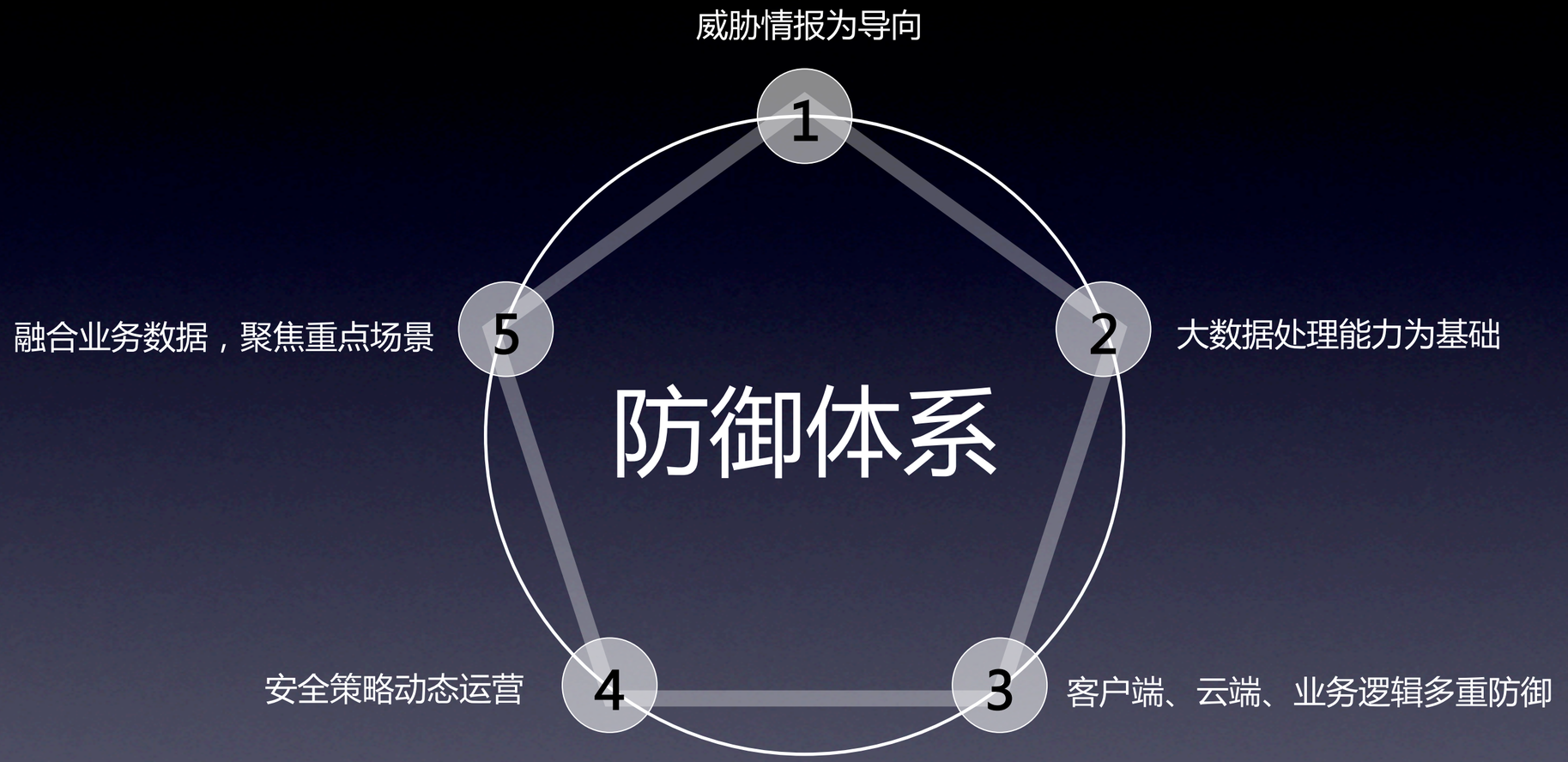
--利用“洋葱”和“门神”构建双保险

融合业务数据构建红包白安全模型

云端安全策略的使用

--客户端存在漏洞无法快速升级
--外挂打击
--假红包打击

舆情的快速反应和掌控


威胁情报为导向
1
2
大数据处理能力为基础
3
客户端、云端、业务逻辑多重防御
4
安全策略动态运营
5
融合业务数据，聚焦重点场景
防御体系


WE ARE ALWAYS ON THE WAY
THANK YOU
Coolc 2015