2016乌云白帽大会・不插电

十年安全路
信息安全的从1到10

信息安全总监 凌云
2016.4

About Me

凌云 10年信息安全从业经验

待过乙方：绿盟科技
也待过甲方：1号店 中国平安等
目前在携程担任信息安全总监
关注电商业务安全，企业研发安全
信息安全，安全产品设计及合规审计
CISA、ISO27001LA认证

目录

信息安全的从1到10

先分类	再摸底	定目标	走起
• 运维安全 • 应用安全 • 业务安全 • 安全合规	• 访谈 • 扫描 • 乌云	• 同行交流 • 我在哪里 • 我要去哪里	• 招人 • 单点突破 • 预埋伏笔

信息安全的从1到10

携程一年时间20 +人　　成长到　40人
50%的人员会开发python, Java。

运维安全　　运维安全工程师，研发工程师
应用安全　　web安全工程师，无线安全工程师
业务安全　　安全分析工程师，安全开发工程师
安全运营　　安全运营人员，安全合规

服务携程3000+人的技术团队。

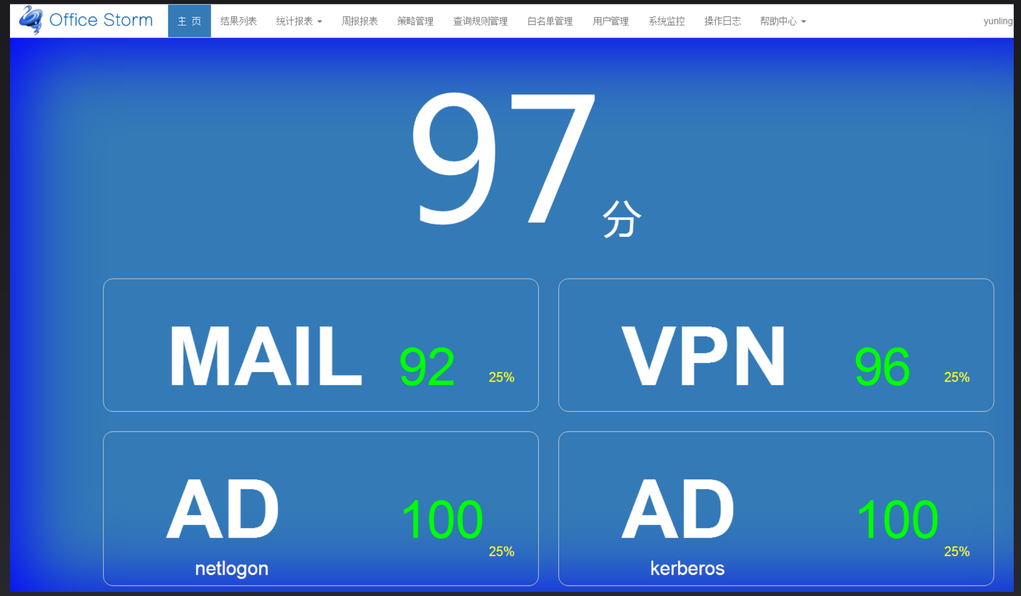
目录

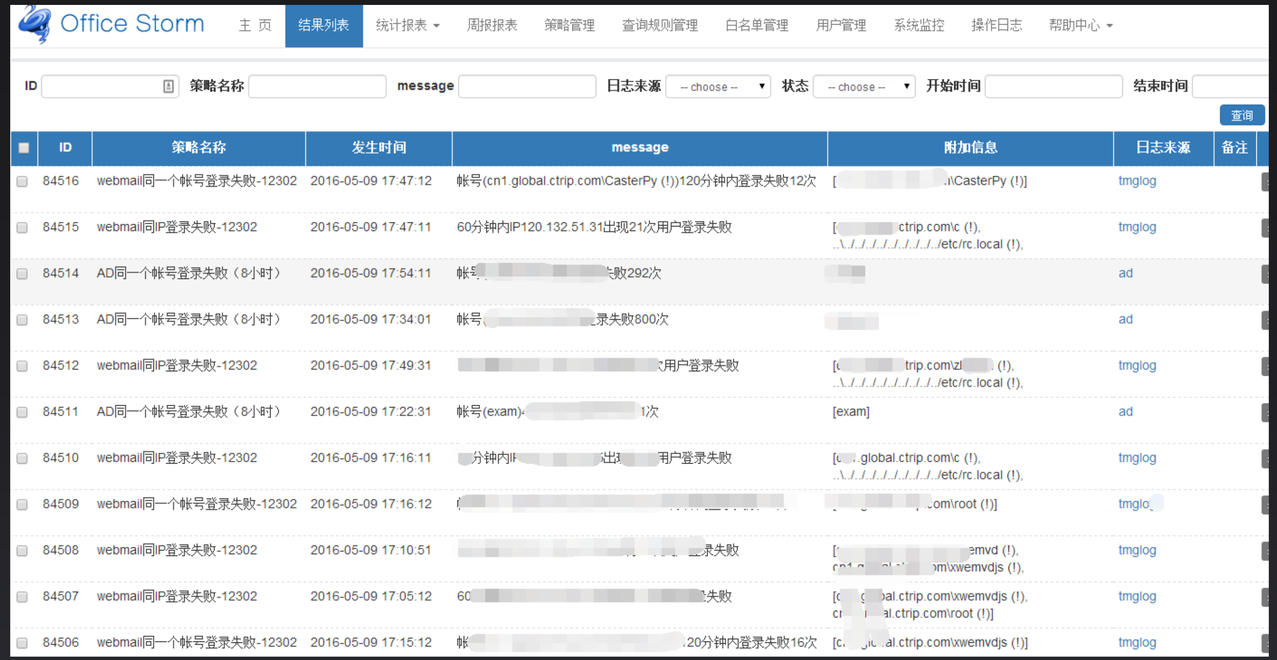
运维安全

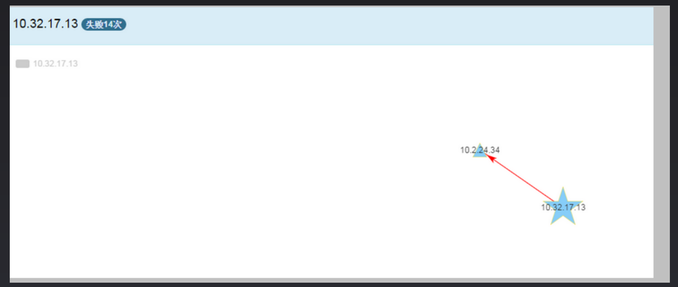
- ✓ 定运维安全规范
- ✓ 安全域划分
- ✓ 巡检弱口令、漏洞
- ✓ 新增主机扫描
- ✓ 日志收集分析
- ✓ 蜜罐
- ✓ OSSEC
- ✓ APT防御
- ✓ ……

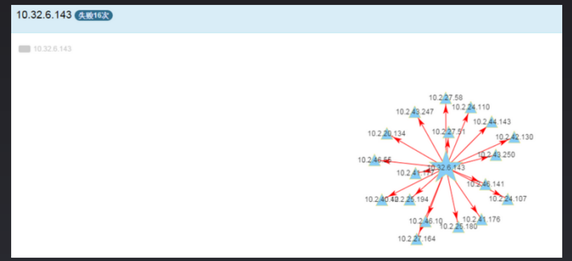
能否加大入侵难度
能否第一时间发现入侵

办公网日志入Storm
规则实时分析
数值化反映
当前安全情况

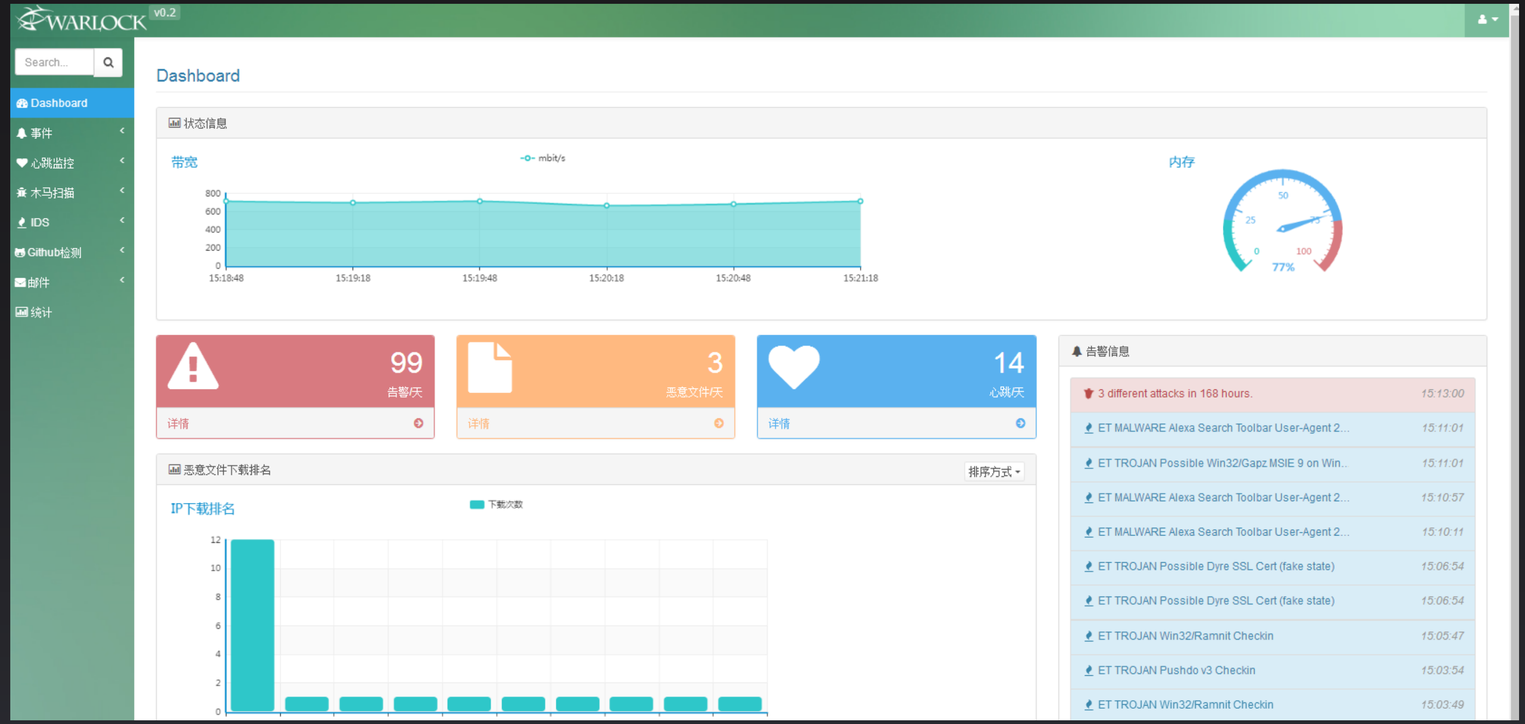








APT监控

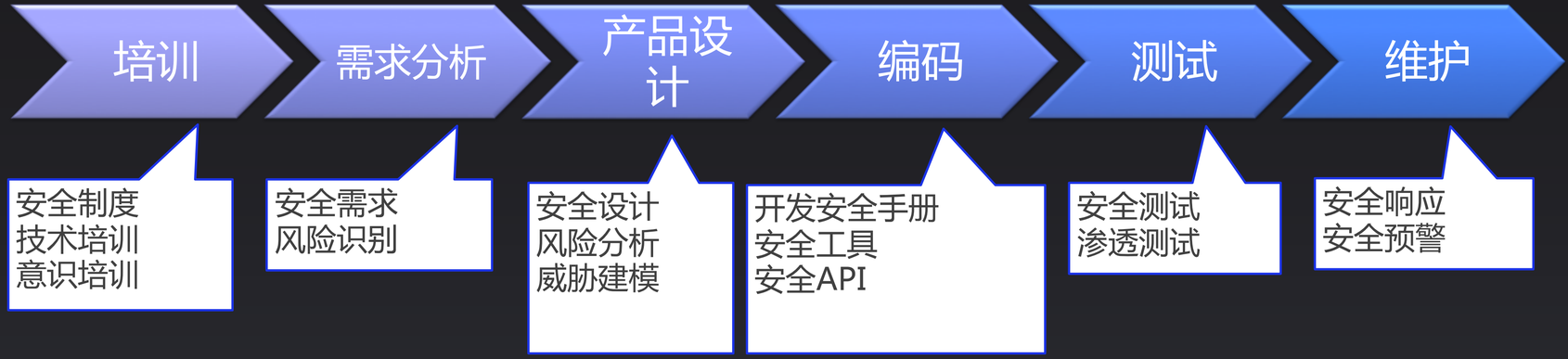

WARLOCK v0.2
Search...
Dashboard
事件
心跳监控
木马扫描
IDS
Github检测
邮件
统计
Dashboard
状态信息
带宽
mbit/s
800
600
400
200
0
15:18:48
15:19:18
15:19:48
15:20:18
15:20:48
15:21:18
内存
50
25
0
100
77%
99
告警/天
详情
3
恶意文件/天
详情
14
心跳/天
详情
告警信息
3 different attacks in 168 hours. 15:13:00
ET MALWARE Alexa Search Toolbar User-Agent 2... 15:11:01
ET TROJAN Possible Win32/Gapz.MSIE 9 on Win.. 15:11:01
ET MALWARE Alexa Search Toolbar User-Agent 2... 15:10:57
ET MALWARE Alexa Search Toolbar User-Agent 2... 15:10:11
ET TROJAN Possible Dyre SSL Cert (fake state) 15:06:54
ET TROJAN Possible Dyre SSL Cert (fake state) 15:06:54
ET TROJAN Win32/Ramnit Checkin 15:05:47
ET TROJAN Pushdo v3 Checkin 15:03:54
ET TROJAN Win32/Ramnit Checkin 15:03:49
恶意文件下载排名
排序方式
IP下载排名
下载次数
12
10
8
6
4
2
0

目录

安全开发生命周期　SDL

什么是SDL？　　Security Development Lifecycle from Microsoft

军事学说法：纵深防御　娱乐化解读：塔防



事前管控，抓大放小

1.身份鉴别	1.1密码支持
	1.2账户策略
	1.3辅助安全设备
2.授权管理	2.1 功能授权
3.访问控制	3.1 系统内访问控制
	3.2 系统外访问控制
4.系统安全审计	4.1 WEB应用访问日志完备性
	4.2 用户认证日志完备性
	4.3 应用操作日志完备性
	4.4 后台日志完备性
	4.5 日志信息安全存储
5.通信安全	5.1 通讯协议
	5.2 通讯安全认证
6.数据安全	6.1 用户数据的输入与输出
	6.2 用户数据保密性
	6.3 用户数据完整性鉴别
	6.4 用户数据的存储
7.抗抵赖	7.1 原发抗抵赖
	7.2 接收抗抵赖
	7.3 数字证书
8.软件容错	8.1 降级容错
	8.2 受限容错
9.资源控制	9.1 内部资源控制
	9.2 外部资源控制

登录注册风险

注册

1. **遍历已注册手机号**
2. 允许弱密码注册
3. 抢注他人手机号
4. 绕过短信验证
5. **注册时可短信炸弹**
6. 批量注册
7. 注册处存在SQL注入、跨站脚本、跨站请求欺骗类漏洞
8. 注册时图形验证码可绕过
9. 邮箱注册时验证值可猜解

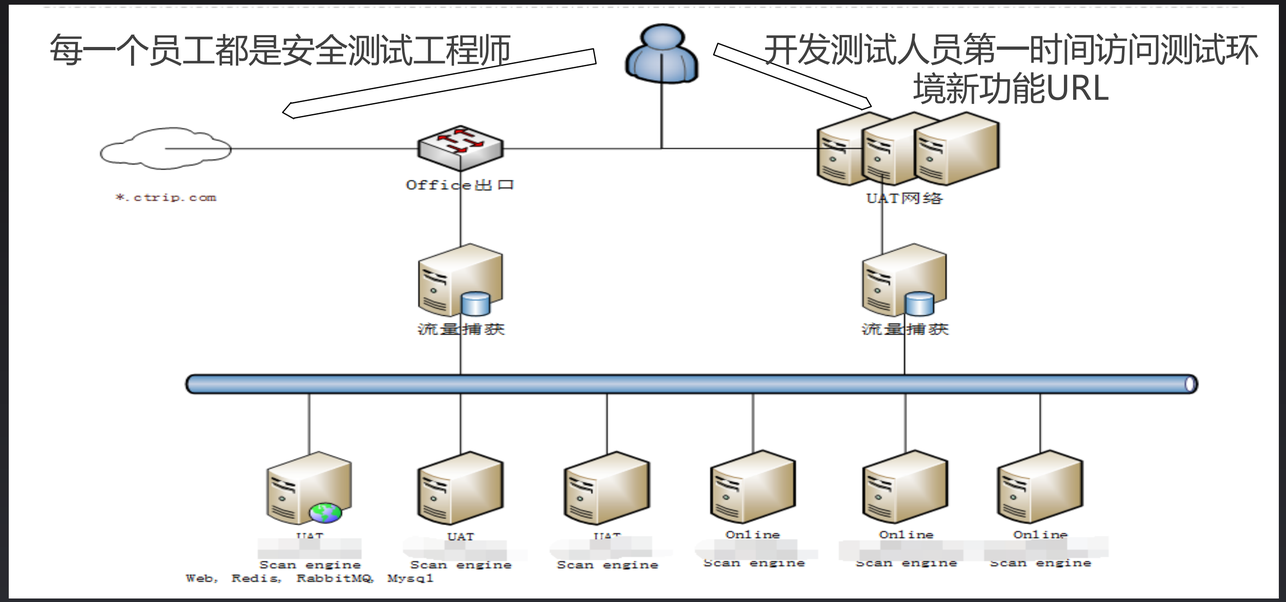
登录

1. 登录处可SQL注入
2. 登录处图形验证码可绕过
3. 登录时短信验证码各类问题，如正确的短信验证码在反回数据包中、爆破、短信轰炸、
4. **登录错误提示过于详细**

事中自动化，扩大覆盖面

CMDB　Git代码库　JIRA　DNS服务器 监控？

我们来点更高大上的黑科技 ——— 被动扫描，主动感知



抓住每一个新功能


HULK
结果列表
统计
规则审核
规则配置
yunling
注销
Online
UAT HULK 运营概览
Day Hour
Thursday, Oct 15, 2015
unique: 9 599
done: 9 571
测试环境有新功能了！
Values
consume unique done
Ctrip.com HULK 运营概览
Day Hour
恩，过了7天上线了
域名TOP 10
120
65
53
45
30
20
20
19
18
18
Values
漏洞等级分布
6.74 %
29.11 %
64.14 %
低 中 高
漏洞类型分布
6.74 %
19.90 %
4.11 %
69.24 %

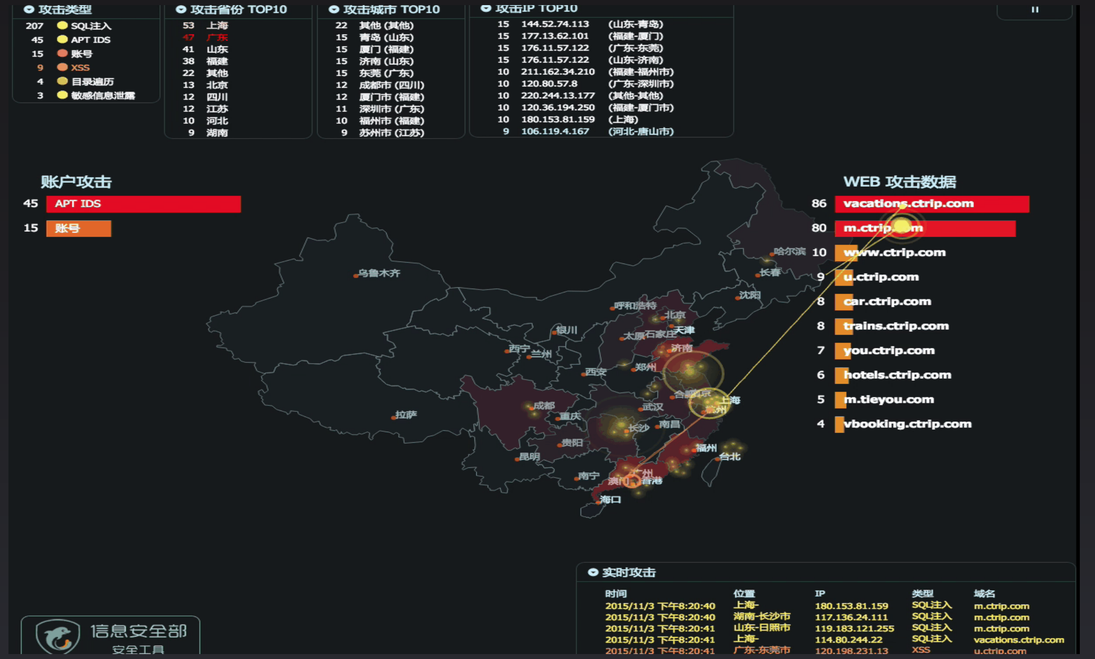
水平权限自动化检测

通过自定义Cookies访问含有订单信息的页面
自动化检测水平权限问题

攻击可视化

通过storm
实时抓取攻击数据
分析“黑客”爱好

并反向验证
网站安全情况



自研WAF


携程Web应用防护系统
欢迎您:vly凌云 退出登录
状态监控
规则策略
统计功能
报表功能
日志明细
变更日志
发布日志
漏报分析
误报分析
攻击日志
切换主题
3D可视化
DASHBOARDS
状态监控
运行状态
86
集群状态
87
集群状态
88
集群状态
89
集群状态
攻击趋势
11000
10500
10000
9500
9000
8500
8000
7500
7000
6500
6000
5500
5000
4500
4000
3500
3000
2500
2000
19:00
22:00
01:00
04:00
07:00
10:00
13:00
16:00

目录

业务安全

1. 扫号撞库
2. 广告劫持
3. 薅羊毛
4. 虚占位/库存
5. 爬虫

xKungFoo2013

| xKungFoo | 会议日程 | 赞助商 | 演讲者 | 往届会议 | 注册 | 联系我们 |

2013年3月23日星期六 第一天		
时间	演讲者	议题
08:00-09:30	会议注册	
xKungFoo开始		
09:30-10:30	王云翔	0day快速分析 - 预知未来，通晓过去
10:30-11:00	魏兴国	CC攻击防御基础介绍
11:00-11:10	休息	
11:10-12:10	杨哲	2013:后无线Hacking时代
12:10-13:30	休息	
13:40-14:10	崔孝晨	From 1 day to forensic
14:10-15:10	林鑫	虚拟机入侵与内存取证
15:10-15:20	休息	
15:20-15:50	魏兴国	动态cookie缓解APP时代的CC攻击
15:50-16:50	麦云	电商安全那点事
16:50-17:00	幸运抽奖	

2013年3月24日星期日 第二天		
时间	演讲者	议题
09:30-10:30	胡文君	基于Android程序通信机制的攻击及防御方法
10:30-11:00	商广明	Android网络安全
11:00-11:10	休息	
11:10-12:10	何晓杰	Android的组件管控与安全
12:10-13:30	休息	
13:40-14:10	方兴	APT攻击的过去、现在和将来
14:10-15:10	潜伏鹰	先进匿名通信网络的设计及其在敏感行动中的应用
15:10-15:20	休息	
15:20-15:50	Benjurry	SDN 改变网络安全格局
15:50-16:50	于旸（TK）	浏览器和本地域
16:50-17:00	幸运抽奖 & xKungFoo 闭幕辞	

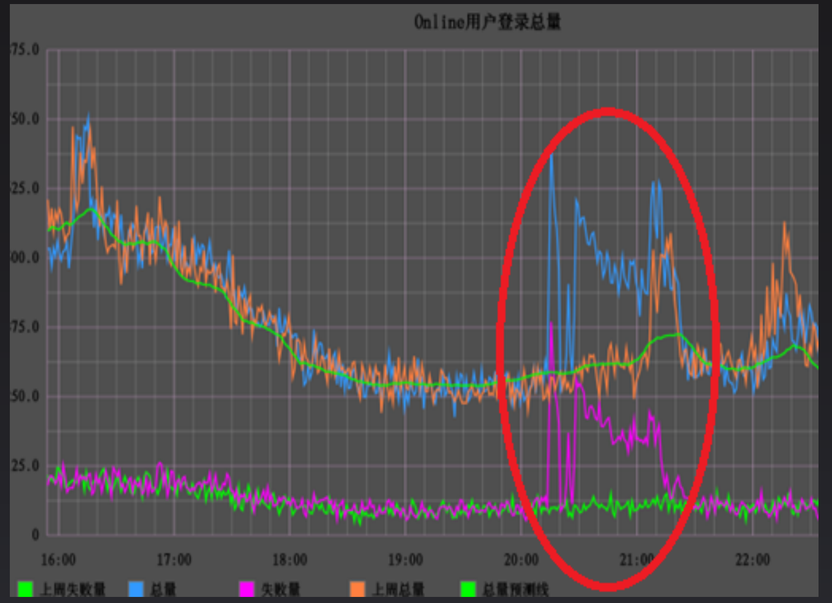
扫号：

威胁用户账号安全的源头

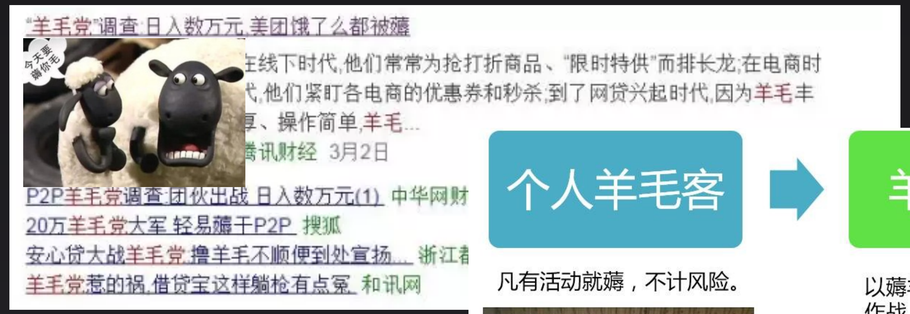
- 资金盗用
- 信息泄漏
- 恶意欺诈

特征：

- IP使用量巨大，可以做到1号1 IP
- 使用外部社工库，密码正确率高
- 可以根据安全措施及时更换策略
- 设备指纹基本伪造，无明显特征



薅羊毛与风险库


"羊毛党"调查 日入数万元 美团饿了么都被薅
线下时代,他们常常为抢打折商品、"限时特供"而排长龙;在电商时
代,他们紧盯各电商的优惠券和秒杀;到了网贷兴起时代,因为羊毛丰
厚、操作简单,羊毛...
腾讯财经 3月2日
P2P羊毛党调查:团伙出战 日入数万元(1) 中华网财
20万羊毛党大军 轻易薅于P2P 搜狐
安心贷大战羊毛党 撸羊毛不顺便到处宣扬... 浙江
羊毛党惹的祸,借贷宝这样躺枪有点冤 和讯网


个人羊毛客
羊毛团伙
集团作战
凡有活动就薅，不计风险。
以薅羊毛为职业，团队作战，分工明确，拥有几百个手机号、身份证、银行虚拟卡，可对同一公司的活动狂薅。
当羊毛党结集10个以上羊毛团伙，资金达到5000万以上时，可利用提现绑架平台，进行"接管"，甚至"搞垮"平台。
安在

谁是小号?

eud7282038da@163.com
pgcf77045140haos@163.com
qhz77413593jiaos4@163.com
xd63576160haoyi6@163.com
zhuoji9683@163.com
lting520@hotmail.com

批量领券拦截

ID	请求时间	用户IP	用户IP地理地址	UID	UserName	手机号归属地	注册间隔时间（ms）	重置密码间隔时间（ms）			Tag	策略ID	更新时间	UA	URL
1695	2016-03-30 11:08:02	112.102.69.27	黑龙江	M354847129	15665808142	济南	1000	121161	[redacted]		批量刷券	活动领券策略1	2016-03-30 11:11:13	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.154 Safari/537.36 LBBROWSER	/mobilecouponws/json/Participate
1694	2016-03-30 11:09:06	1.58.55.80	黑龙江	M354847693	15665758642	济南	1000	62244	[redacted]		批量刷券	活动领券策略1	2016-03-30 11:11:12	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.73 Safari/537.36	/mobilecouponws/json/Participate
1693	2016-03-30 11:08:21	1.58.55.80	黑龙江	M354847284	15665764069	济南	1000	68641	[redacted]		批量刷券	活动领券策略1	2016-03-30 11:11:12	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.73 Safari/537.36	/mobilecouponws/json/Participate
1692	2016-03-30 11:08:11	112.102.69.27	黑龙江	M354847215	15665807486	济南	1000	114238	[redacted]		批量刷券	活动领券策略1	2016-03-30 11:11:12	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.87 Safari/537.36 QQBrowser/9.2.5748.400	/mobilecouponws/json/Participate

沉淀恶意手机号	1000W +	上线3个月
国人常用弱密码	2500+	羊毛党拦截1,219,341次
手机归属地分类	32W+	爬虫拦截689,561次

每张卷平均价值20，使用率2%，被刷优惠卷损失倍数3

1219341*20*2%*3=1,463,209 元

目录

security.ctrip.com

抓痛点，接地气。
有情怀，不收费。

你的想法，我来实现

四大金刚

Github Scan

监控Github代码库，及时发现员工托管公司代码到Github行为并预警，降低代码泄露风险。

风险库

根据不同层面的恶意行为计算风险值，多年沉淀，千万级别手机号码库，帮助企业有效防御羊毛党。

军火库

监控常用软件漏洞发布，对存在POC的漏洞及时预警，帮助用户提早发现高风险安全漏洞。

天眼

跟踪最新互联网泄密事件，发现企业隐私数据被泄露行为，并及时预警。

THANKS


乌云 WooYun


乌云白帽大会 · 2016
不插电