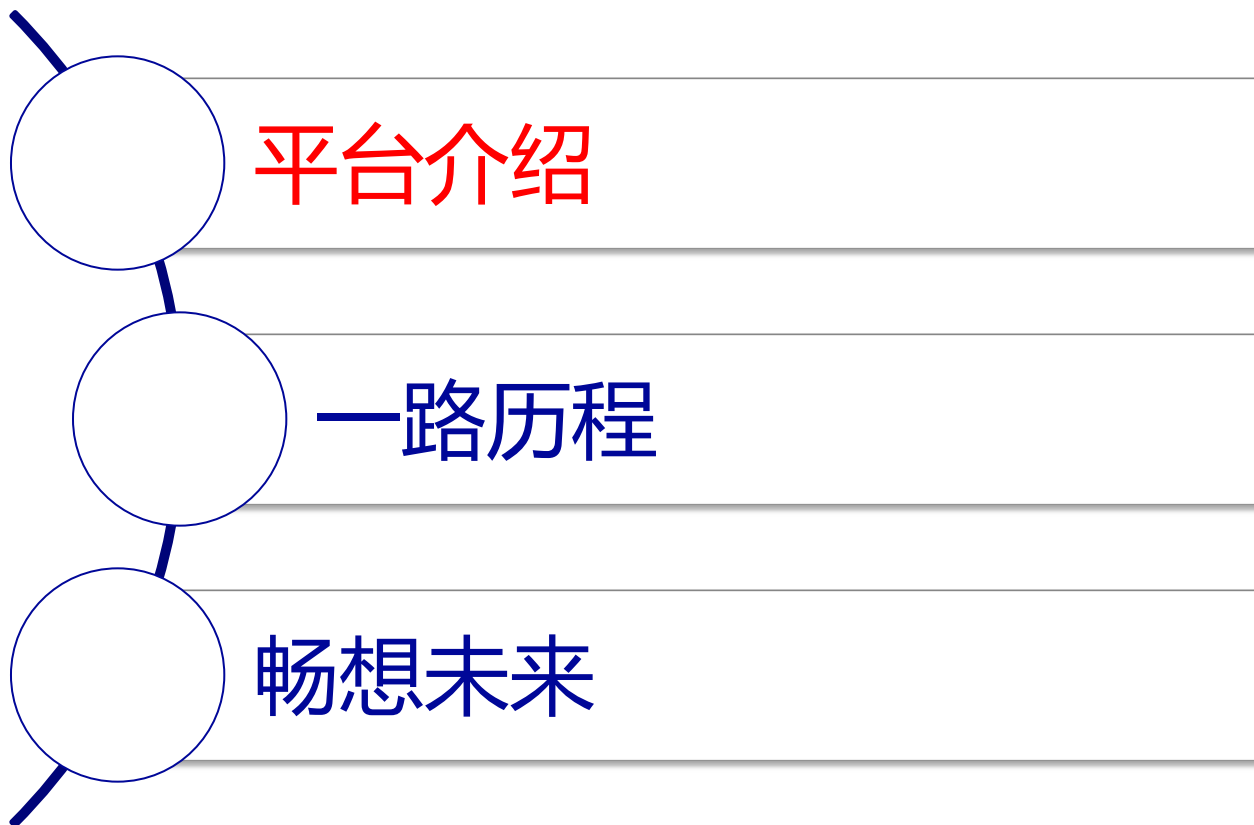


企业SaaS安全服务的瑞士军刀

---携程安全SaaS之路



凌云



楔子1

艺龙遭到黑客攻击，希望更方便的使用到携程已有的一些安全产品

楔子2

行业内黑名单数据交换，需要一个较好的互换机制和渠道

楔子3

乙方产品不接地气，造一些轮子给没有开发能力的甲方使用

谷歌、Facebook、雅虎共享IP黑名单

发布时间：2015-07-26 16:58:00 来源：论坛 作者：红黑联盟 dawnr

A+ A-

关键字：[facebook](#) [谷歌](#) [新闻](#) [雅虎](#)



网络欺诈，尤其是广告欺诈行为很是令人恼火。近日网络科技巨头[Google](#)、[Facebook](#)、[Yahoo](#)公司携手启动了一个新计划，阻止黑名单中IP地址刷web流量。

谷歌将利用IP黑名单过滤爬虫机器人

现在的网络环境中，大部分数据中心流量都是非法流量或机器爬虫产生的。为了遏制这个问题，Trustworthy Accountability Group(TAG)宣布启动一项计划，利用Google内部数据中心的IP黑名单去过滤爬虫机器人。

Google的广告经理Vegard Johnsen表示，这个新的试点项目将使用黑名单过滤掉网络流量机器人和僵尸爬虫，这能减少数据中心很大一部分冗余流量。

像Google这样的科技大公司们都有自己的黑名单，上面列有计算机系统数据中心上可疑的IP地址，这些可疑IP地址会伪装成自然人点击广告等赚取流量费用。Google仅在5月份就阻止了将近8.9%的流量。

地址：<https://security.ctrip.com>



让我们一起做一些互联网公司喜欢的安全小工具

累计接入企业150+ 核心活跃 40+





创建历程



Github scan、风险库上线



2016.1.6

军火库上线



2016.3.31

天眼上线



2016.4.20



2015.12.9

启动立项



30+

2016.3.1



90+

2016.4.6



150+

2016.5.7



Github Scan



当前位置: WooYun >> 搜索结果

搜索关键字: [github](#) (共 772 条记录) [按未公开漏洞的搜索结果](#)

[BUS365官方邮箱密码泄露40W+已发送邮件 \(姓名/身份证/手机号码/座位号/取票码等\)](#)

不知道谁重复...[https://github.com/chuanwang1993/hello-world/blob/24f3bd69cd7cf793c510689233b1b7a18af9ab1c/bus365mngri/conf/applicatio](#)
[mtp.bus365.com.mail.smtp.user=bus365@bus365.com.mail.smtp.pass=2013bus84365.mail.smtp.channel=smtpl](#) 可登陆 已发送邮件中, 都是这样
...改密码, 来个20Rank吧

提交日期: 2016-05-05 作者: 路人甲

[通卡网络账某处信息泄露 \(十多G数据数千万条数据\)](#)

...[https://github.com/lifangzhen/BacKEnd/blob/ft273dca1e734157703e7](#)
录: mongo未授权访问无需输入账号和密码 <mask>*****</mask> 十多G
享, 到现在还没改密码, 这可不行 求20Ra...

提交日期: 2016-05-04 作者: 路人甲

[疑似众安保险某站源码泄露数据库可直连/大量敏感信息](#)

众安保险某站源码泄露数据库可直连大量敏感信息...code 区域[https://github.com/588bd4db7c2e0f750567743/src/main/resources/ideploy.properties](#) code
#database.user=root#database.password=Kingsley6

提交日期: 2016-04-21 作者: 路人甲

[乐友某站jboss存在后门漏洞](#)

RT...[http://wooyun.org/bugs/wooyun-2010-0196219](#) 跟着前人的...[github](#)
on: 1.0.7 [3.J] * --- JexBoss: Jboss verify and EXPloitation Tool --- * ||| @
提交日期: 2016-04-21 作者: 路人甲

[东风本田某供应商交互平台getshell](#)

rt工具 [https://github.com/Xyntax/POC-Tf/blob/master/module/jboss.py..2](#)
* ||| @author: João Filho Matos Figueiredo ||| @contact: joaomatos@gf
提交日期: 2016-04-21 作者: 路人甲

在某漏洞平台搜索GitHub关键字就可以匹配到627条关于GitHub导致的漏洞问题, 其中包含政府机关、企业、医疗、大专院校等各个领域, 其中不乏有京东、唯品会, 万达等知名企业。

羊城晚报 X年X月
万达集团内部绝密资料泄露, 可导致黑客入侵内网漫游

凤凰网 X年X月
步步高商城泄露集团各分店账号密码

新华网 X年X月
某大型知名保险公司泄露数据库账号密码, 测试环境账号密码

新民晚报 X年X月
GitHub代码上传不慎至Uber司机数据库泄露



项目白名单

文件白名单

[添加项目白名单](#)

路径	创建时间
https://github.com/ctripcorp/hermes	2016-01-29 13:06:43
https://github.com/ctripcorp/	2016-01-22 15:41:17
github.com/ctripcorp/zeus	2016-01-18 19:08:35

Github Scan



主题: 您在携程SAAS上关注的github关键词有结果更新

携程云安全

亲爱的 SAAS_GithubScan,

您好, 您关注的关键词 (ctrip password, ctrip mysql, ctrip database, ctrip login, ctrip smtp pass, tieyou, ctripcorp pwd, ctripcorp password, ctrip 密码, ctrip svn) 在携程SAAS的github扫描服务中有更新, 请点击查看!

使用统计

过滤:

搜索

用户名	厂商	爬取数	关键字
bo	恒生电子	378	hundsun password hundsun mysql hundsun database hundsun login hundsun smtp pass
p	完美世界	523	pwd password pwd mysql pwd database pwd login pwd smtp pass pwd.com
sc	Lenovo	774	lenovo password lenovo mysql lenovo database lenovo login lenovo smtp pass
s	联想	776	lenovo password lenovo mysql lenovo database lenovo login lenovo smtp pass
xi	厦门航空	14	xiamenair password xiamenair oracle xiamenair database xiamenair login xiamenair smtp pass xiamenair xiamenair.com xiamenair.com.cn mif.com
su	UFreedom	295	duomi password duomi mysql duomi database duomi login duomi smtp pass
an	启明星辰	408	venustech.com password venustech.com mysql venustech.com database venustech.com login venustech.com smtp pass
o	北京启明星辰	408	venustech.com password venustech.com mysql venustech.com database venustech.com login venustech.com smtp pass
a	蚂蚁金服	473	alipay password alipay mysql alipay database alipay login alipay smtp pass
5	武汉维佳置业有限责任公司	0	weigagroup password weigagroup mysql weigagroup database weigagroup login weigagroup smtp pass
l	福建新大陆科技集团	353	newland password newland mysql newland database newland login newland smtp pass

01 关键字定制

02 智能白名单

03 实时推送

04 多链路爬虫

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



在线下时代,他们常常为抢折扣商品、“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 轻易薅干P2P 搜狐

安心贷大战羊毛党,撸羊毛不顺便到处宣扬... 浙江者
羊毛党惹的祸,借贷宝这样躺枪有点冤. 和讯网

个人羊毛客

凡有活动就薅,不计风险。



羊毛团伙

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。



集团作战

当羊毛党集结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。



谁是小号?

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

RiskRep-风险库系统

[导入风控配置](#)
[手机号数据](#)
[验证码数据](#)
[白名单库](#)
[风险数据](#)
[注册数据](#)
[登录数据](#)
[领券数据](#)
[分账转换](#)
[数据统计](#)
[手机号归属](#)
[用户管理](#)
[账户](#)

起始日期:
 结束日期:
 数据来源:

注册IP:
 UID:
 ClientID:

命中策略:
 Tag:
 密码MD5:

[查询](#) [报表导出](#)

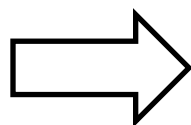
ID	注册时间	注册IP	UID	注册平台	手机号	验证码	邮箱	Tag	策略ID	SourceFrom	ClientID	更新时间
24459242	2016-06-13 18:03:04	119.101.107.113	E395736779	P	97F4...7CC4		y4397351luwen5447@163.com	批量注册	注册策略2	CRM		2016-06-13 18:05:01
24459222	2016-06-13 18:03:27	119.101.107.113	E395736951	P	97F...9...7C		hao6399872wengj@163.com	批量注册	注册策略2	CRM		2016-06-13 18:05:00
24459215	2016-06-13 18:03:19	119.101.107.113	E395736891	P	97...A...37		chao6455170z@163.com	批量注册	注册策略2	CRM		2016-06-13 18:05:00
24459212	2016-06-13 18:03:45	119.101.107.75	E395737111	P	9...7F...AA...437		lu81212duanbe@163.com	批量注册	注册策略2	CRM		2016-06-13 18:05:00
24459188	2016-06-13 18:03:29		M395736984	M	9964...F...3D980A			批量注册	注册策略1	CRM	12001172810023852852	2016-06-13 18:05:00
24459177	2016-06-13 18:0	119.101.107.11	E395736646	P	97F4...19A9...AAEC7CC437		soov7036788sheno@163.com	批量注册	注册策略	CRM		2016-06-13 18:0

ID	手机类型	phone_header	省份	城市	区号	邮编	操作
325253	联通	1554787	内蒙古	巴彦淖尔市			修改 删除
325252	移动	1513380	河北	承德市			修改 删除
325251	联通	1554844	内蒙古	赤峰市			修改 删除
325250	联通	1554775	内蒙古	鄂尔多斯市			修改 删除
325249	联通	1554752	内蒙古	通辽市			修改 删除
325248	联通	1554923	湖北	恩施市			修改 删除
325247	联通	1554847	内蒙古	赤峰市			修改 删除
325246	联通	1554957	湖北	孝感市			修改 删除
325245	移动	1508964	广东	茂名市			修改 删除
325244	联通	1554842	内蒙古	赤峰市			修改 删除
325243	电信	1535463	吉林	四平市			修改 删除
325242	联通	1554841	内蒙古	赤峰市			修改 删除
325241	联通	1554875	内蒙古	呼和浩特市			修改 删除
325240	联通	1319171	河北	邯郸市			修改 删除
325239	联通	1554773	内蒙古	鄂尔多斯市			修改 删除

批量领券拦截

ID	请求时间	用户IP	用户IP地理位置	UID	UserName	手机号归属地	(ms)	(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	9016B BCE4 9DAD	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	9016B BCE4 9DAD	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	9016B BCE4 9DAD	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	9016B BCE4 9DAD	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 +
国人常用弱密码 2500+
手机归属地分类 32W+



上线3个月
羊毛党拦截1,219,341次
爬虫拦截689,561次

每张卷平均价值20，使用率2%，被刷优惠券损失倍数3

$$1219341 * 20 * 2\% * 3 = 1,463,209 \text{ 元}$$

通过SaaS接口方式

进行风险值调用

对外闭源黑名单



The screenshot displays the '携程云安全' (Ctrip Cloud Security) dashboard. The left sidebar contains navigation options: Dashboard, 安全服务 (Security Services), 业务安全 (Business Security), 账号管理 (Account Management), 意见反馈 (Feedback), and 管理设置 (Management Settings). Under '安全服务', there are links for GitHub Scan, 军火库 (Arsenal), 天眼 (Tianyan), and 帮助文档 (Help Docs). The '帮助文档' link is highlighted. The main content area is titled 'SaaS风险值查询接口' (SaaS Risk Value Query Interface) and lists 12 items. The first two items are expanded to show their details.

- 1.1. 功能描述
- 1.2. 接口描述
- 1.3. 访问权限控制
- 1.4. IP白名单说明
- 1.5. 使用次数说明
- 1.6. 签名参数生成
- 1.7. 响应报文说明
- 1.8. SCENE 场景说明
- 1.9. 响应码说明
- 1.10. 风险值说明
- 1.11. 开发指引
- 1.12. 示例信息

1.1. 功能描述
风险值查询接口，根据用户请求参数中的IP或者手机号来获取相应的风险值。

1.2. 接口描述
协议：HTTP
Heads：Content-Type: application/json
域名：http://api-security.ctrip.com/secsaas-service/services/
接口名：risk
格式：JSON
方法：POST

● 互联网风控基础数据中心

登录 申请内测

洞察冰山下的未知

申请内测

FEATURES



PARTNERS

Tencent 腾讯

 Ctrip
携程

为乌云提供底层数据

欢迎合作

主题 携程云安全之军火库扫描服务有结果更新

携程云安全

亲爱的 zhang_jc,

您好，您关注的软件（ [struts](#) ）在携程云安全的军火库扫描服务中有更新，请[点击查看](#)！

历史漏洞

全部 搜索

05月07日	struts	⚡ struts 2.3.14 includeParams 命令执行漏洞	15:49:45
04月30日	struts	⚡ Apache Struts 2.3.28 Dynamic Method Invocation Remote Code Execution Exploit	16:36:18
04月26日	struts2	⚡ Struts2 方法调用远程代码执行漏洞(S2-032)	16:17:35
04月06日	struts	⚡ Apache Struts 2 远程命令执行漏洞(S2-029)	09:50:05

加载更多

自定义关键字，有POC的漏洞才通知
避免劳烦运维频繁打补丁

EXPLOIT
DATABASE



ExploitHub



思考

大量泄漏信息中
是否保护企业用户？

黑客获取这些信息
会攻击哪些地方？

CSDN600万数据泄露

考生信息泄露

天涯网4000万用户隐私信息泄露

机锋被泄露2300万用户信息

iCloud账号被盗引发“好莱坞艳照门”事件

酒店开房记录泄露

12306大量用户数据泄露并在网上传播售卖

海康威视监控设备存在严重漏洞被境外控制

支付宝前员工出售数据

超30省过5000万社保信息泄露

人寿10万保单信息泄露

美国人事电脑遭受黑客入侵，2150万人的信息被窃取

大麦网600万用户信息泄露

.....

跟踪最新泄露事件，识别隐私数据

air@ctrip.com	1qaz2wsx3	6745****
ben@ctrip.com	beni_shen	a06e****
ben@ctrip.com	yzh928	f339****
cj@ctrip.com	wuhero11	lloy****
ck@ctrip.com	lornaly	9911****
cs@ctrip.com	hock	357c****
cy@ctrip.com	gcy0015	gcy1****
cy@ctrip.com	ycy290	3dbc****
cz@ctrip.com	czji	904e****
d@ctrip.com	hktk200216	dd48****
d@ctrip.com	hktk200216	f4df****
d@ctrip.com	N/A	MAHO****
d@ctrip.com	shdita11979	6720****
d@ctrip.com	shdita	805b****
d@ctrip.com	zdwfhy	e9e6****
d@ctrip.com	yogosuny66	e915****
d@ctrip.com	saphiresky1	7953****
d@ctrip.com	fyang	49ba****
d@ctrip.com	gec	0435****

总计 96 条

- 1 动态更新
- 2 智能清洗
- 3 免操作
- 4 实时推送





蜜罐： docker形式开放， SaaS控制台



扫描器： docker形式开放， SaaS控制台



WAF： docker形式开放， SaaS控制台



机器学习： 在线提交

有情怀的安全工具平台

<https://security.ctrip.com>

首席客服 yunling@ctrip.com

谢谢

