看雪 2017 安全开发者峰会

Kanxue 2017 Security Developer Summit

2000-2017

看雪峰會
2017

业务安全的发展趋势及对抗思路

彭巍@威胁猎人

自我介绍

彭巍

- 曾在金山毒霸负责系统查杀引擎开发，解决终端安全问题。
- 2017年初加入威胁猎人团队，专注业务安全相关黑灰产研究及对抗。

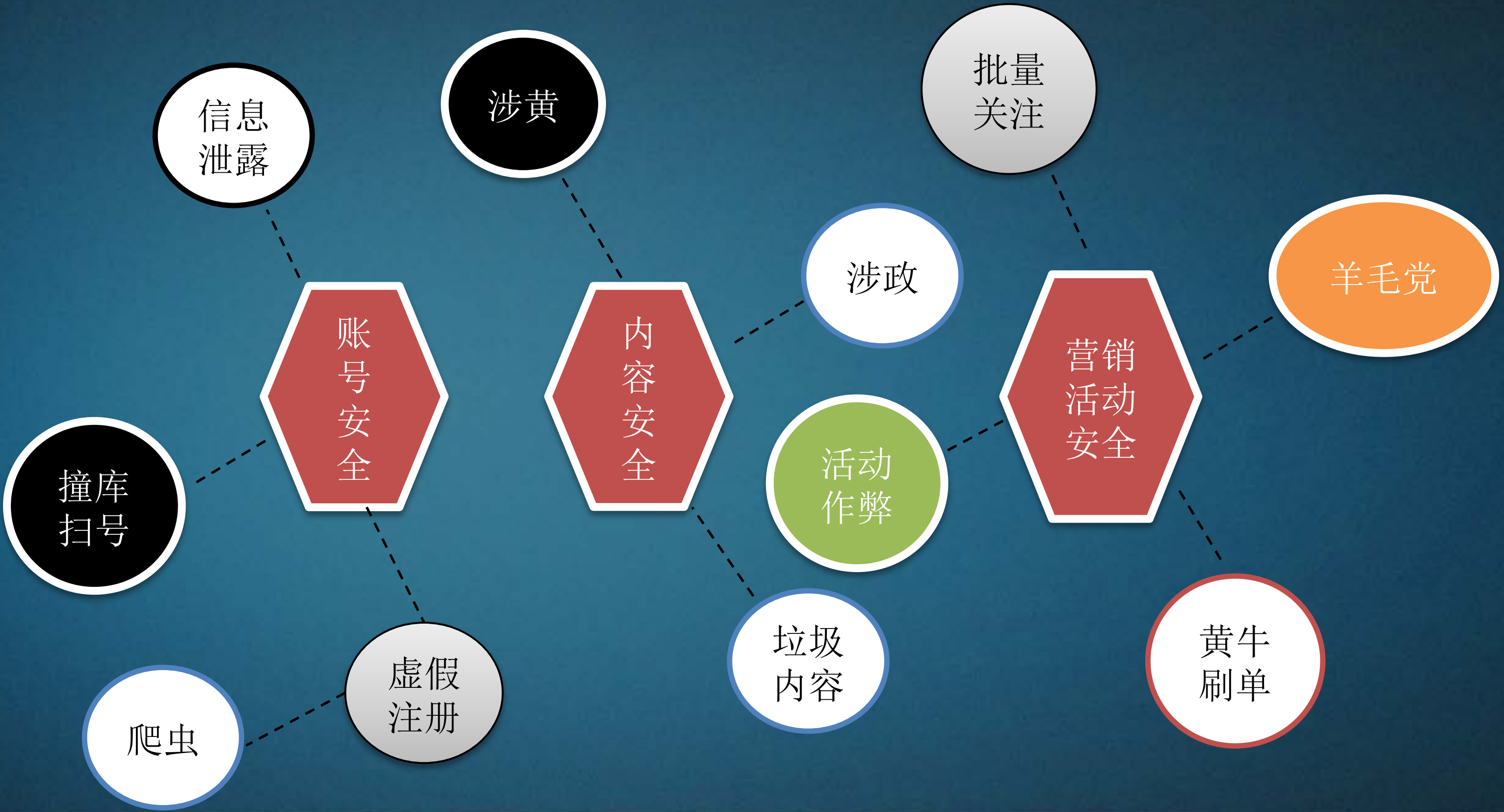
CONTENT 目录

1. 简介
2. 业务安全的昨天与今天
3. 核心问题及对抗思路

PART 1

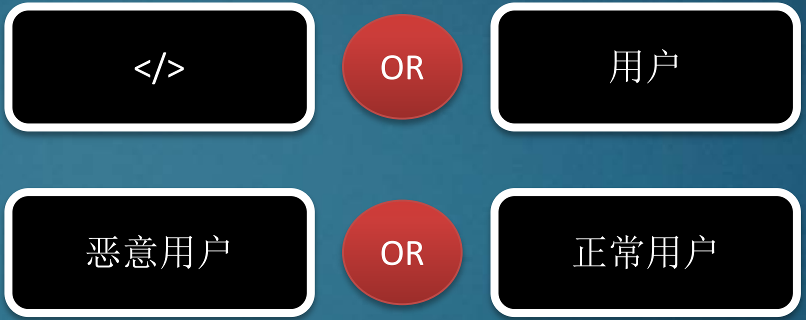
简介

业务安全



信息泄露
涉黄
批量关注
涉政
羊毛党
账号安全
内容安全
营销活动安全
撞库扫号
活动作弊
虚假注册
爬虫
垃圾内容
黄牛刷单

业务安全



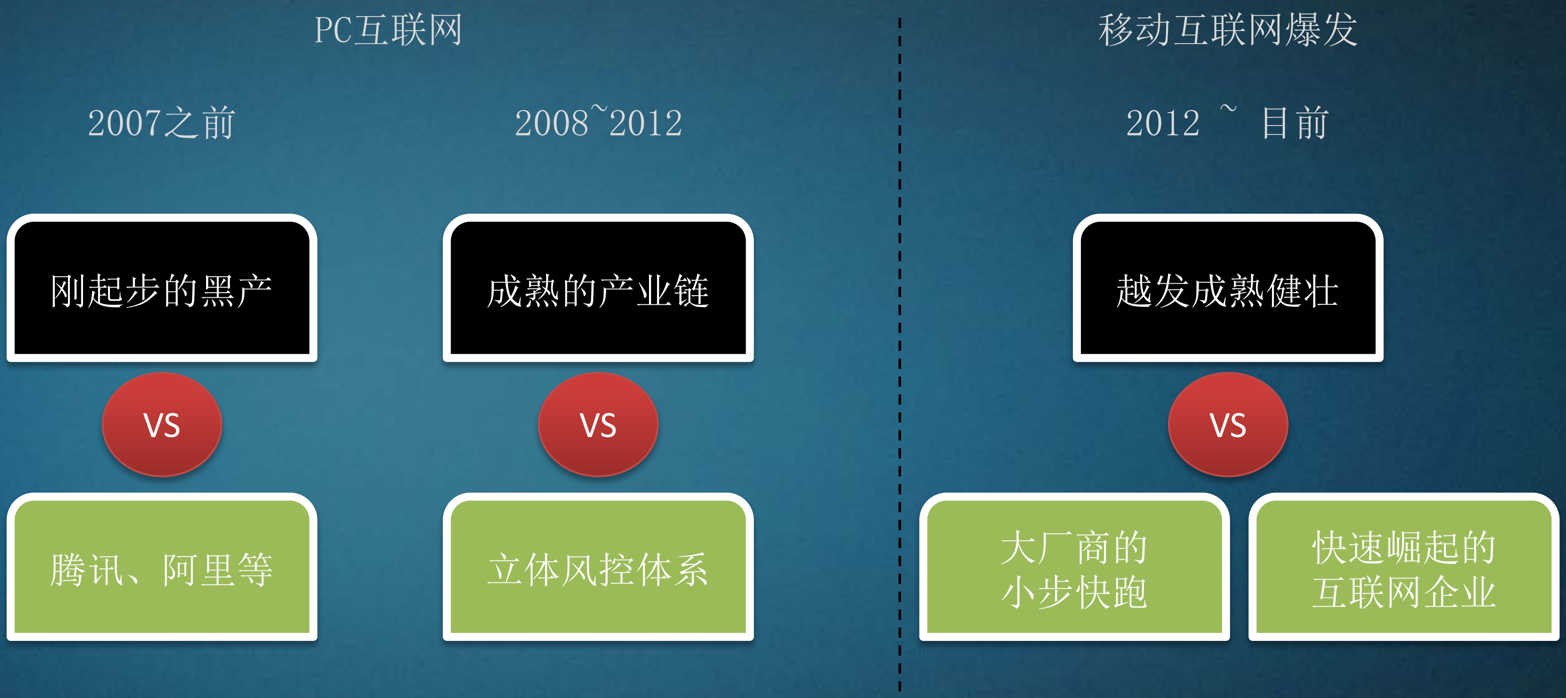
</> OR 用户

恶意用户 OR 正常用户

PART 2

业务安全的昨天和今天

业务安全的昨天



PC互联网

2007之前

刚起步的黑产

VS

腾讯、阿里等

2008~2012

成熟的产业链

VS

立体风控体系

移动互联网爆发

2012 ~ 目前

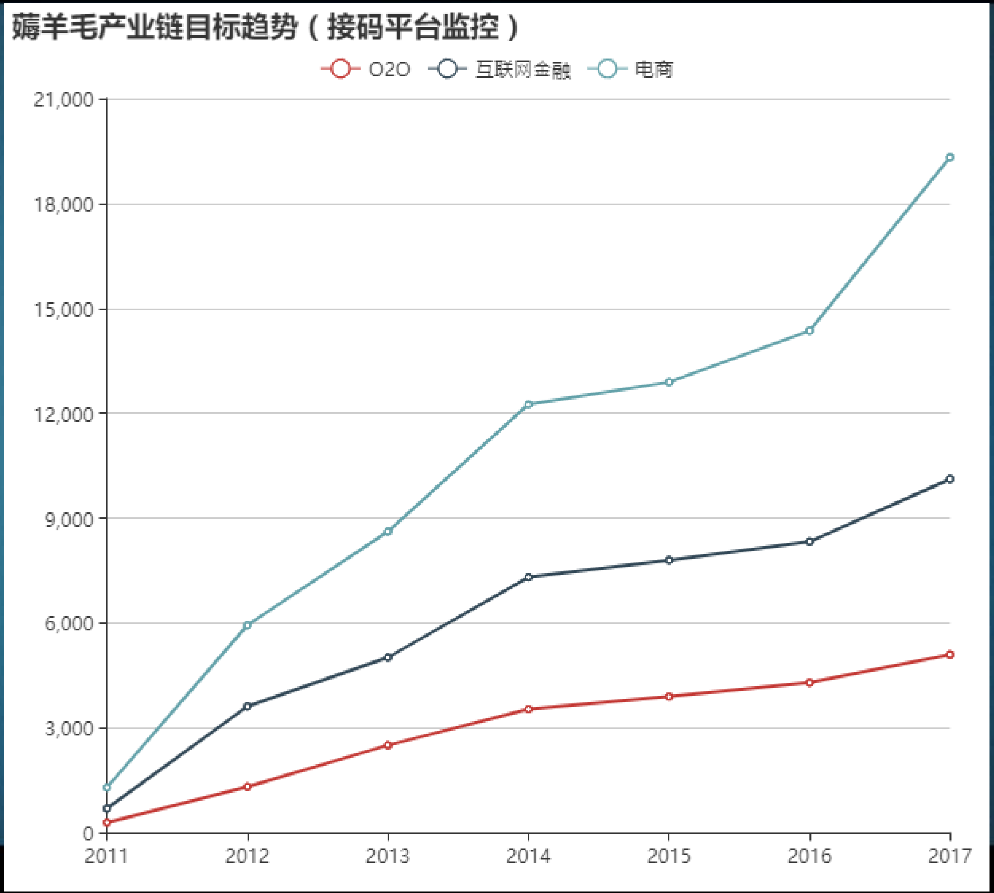
越发成熟健壮

VS

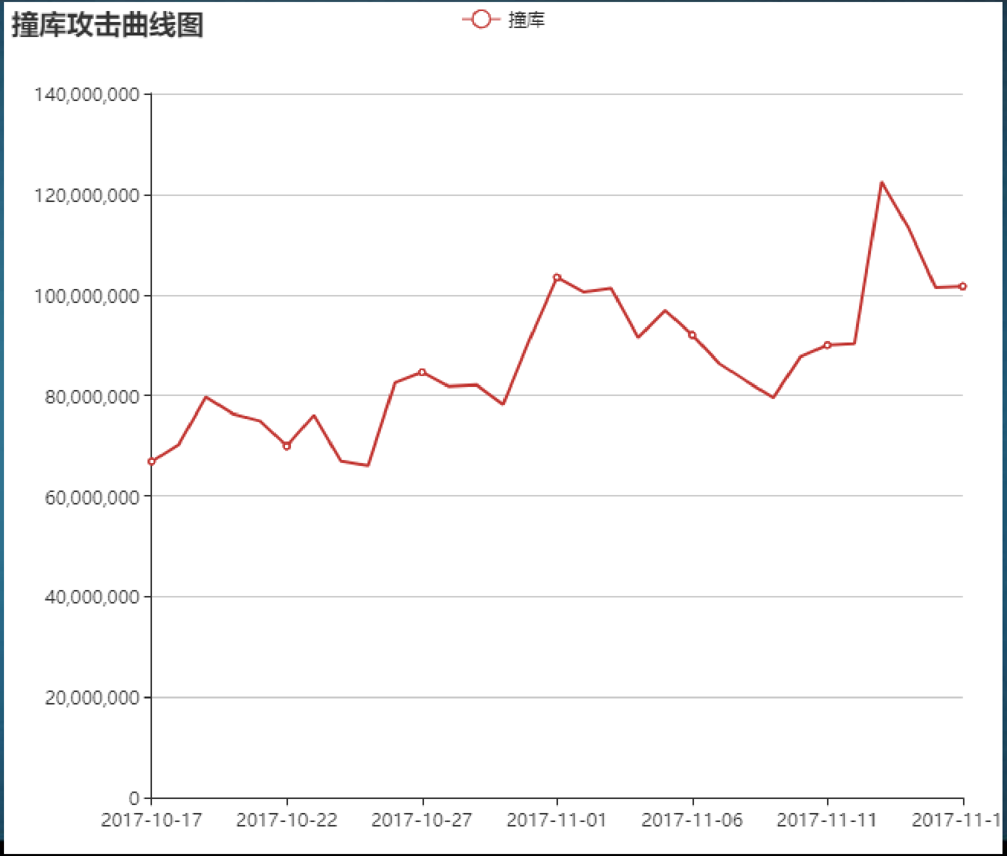
大厂商的
小步快跑

快速崛起的
互联网企业

场景爆发带来业务安全问题陡增

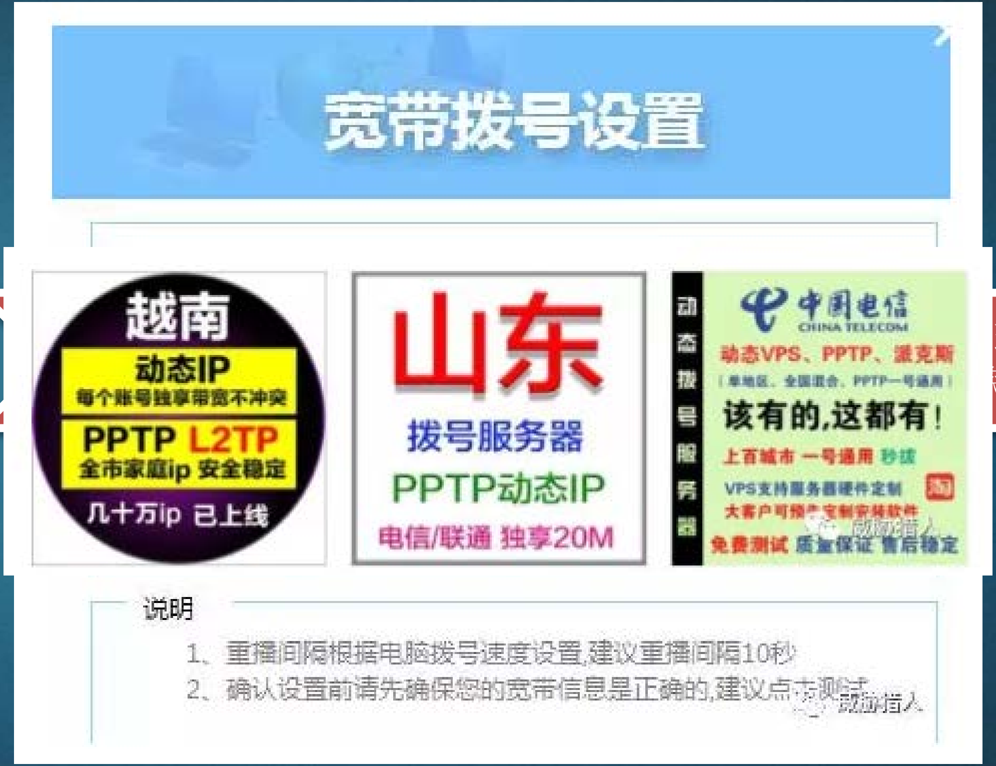


场景爆发带来业务安全问题陡增



场景爆发带来业务安全问题陡增

黑产技术飞跃式的发展 - 秒拨



宽带拨号设置

说明

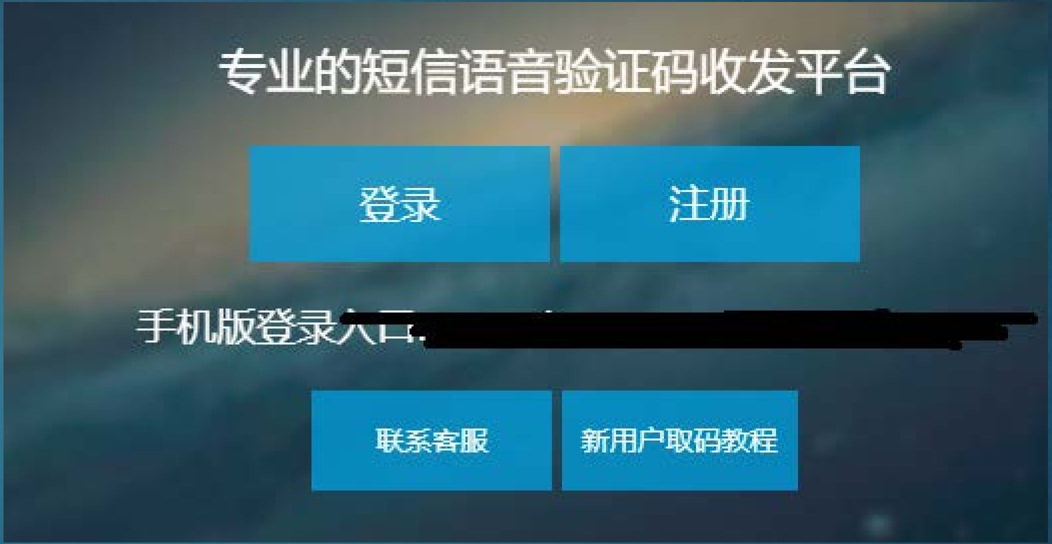
1、重播间隔根据电脑拨号速度设置,建议重播间隔10秒

2、确认设置前请先确保您的宽带信息是正确的,建议点击测试

现

获取

黑产技术飞跃式的发展 - 接码平台

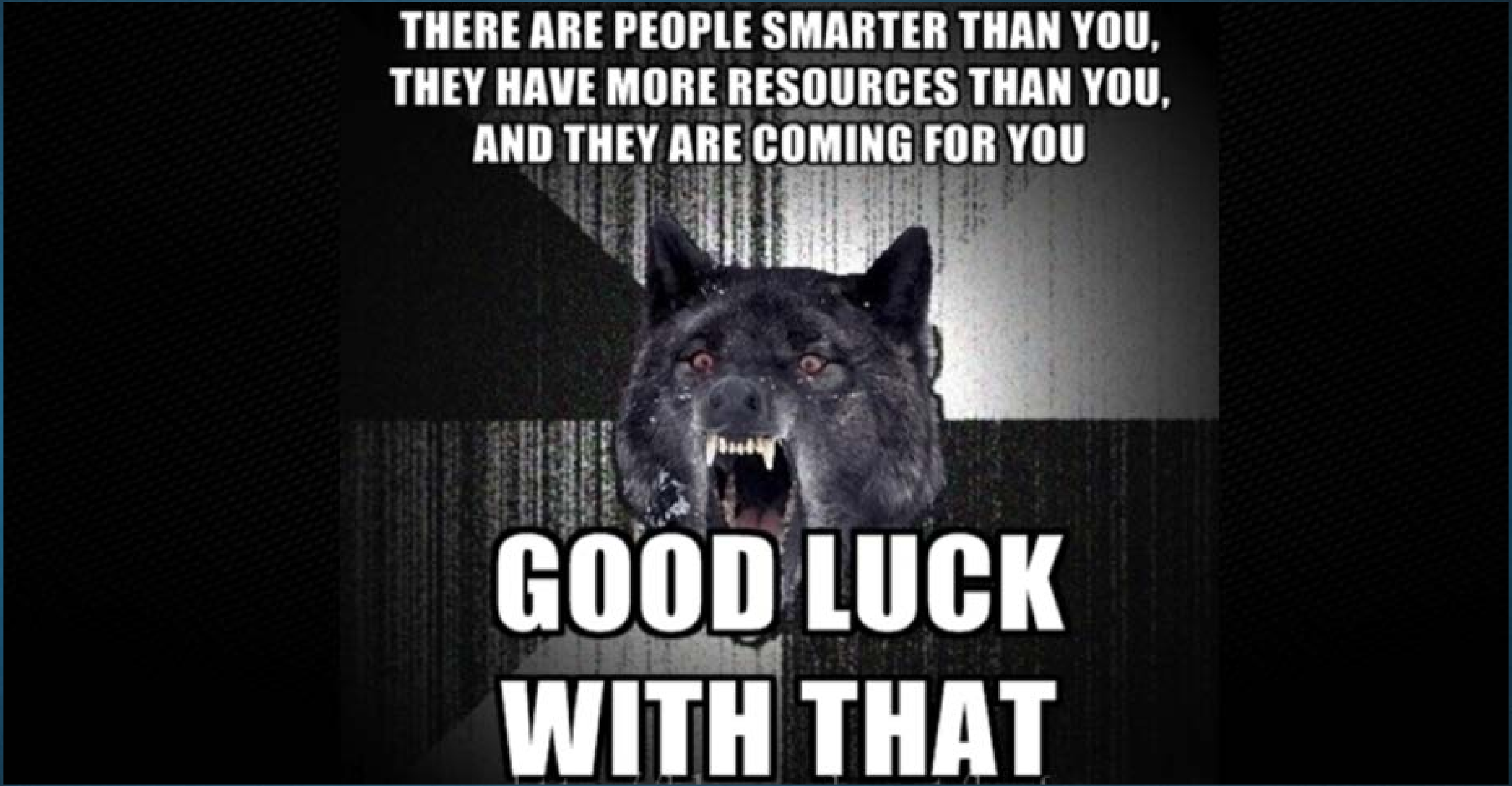


专业的短信语音验证码收发平台

手机版登录入口:[redacted]

PART 3

核心问题及对抗思路


THERE ARE PEOPLE SMARTER THAN YOU,
THEY HAVE MORE RESOURCES THAN YOU,
AND THEY ARE COMING FOR YOU
GOOD LUCK
WITH THAT

攻防双方越趋严重的信息不对称问题

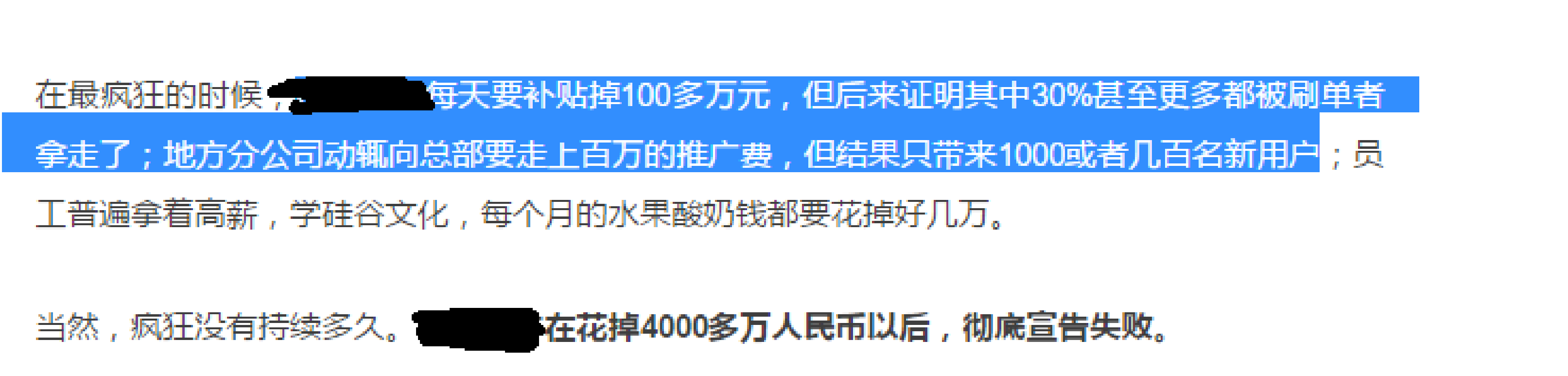
不知道自己被攻击了

攻击平面快速增大

对黑产认知的盲区增大

传统安全管理失控

黑产认识盲区



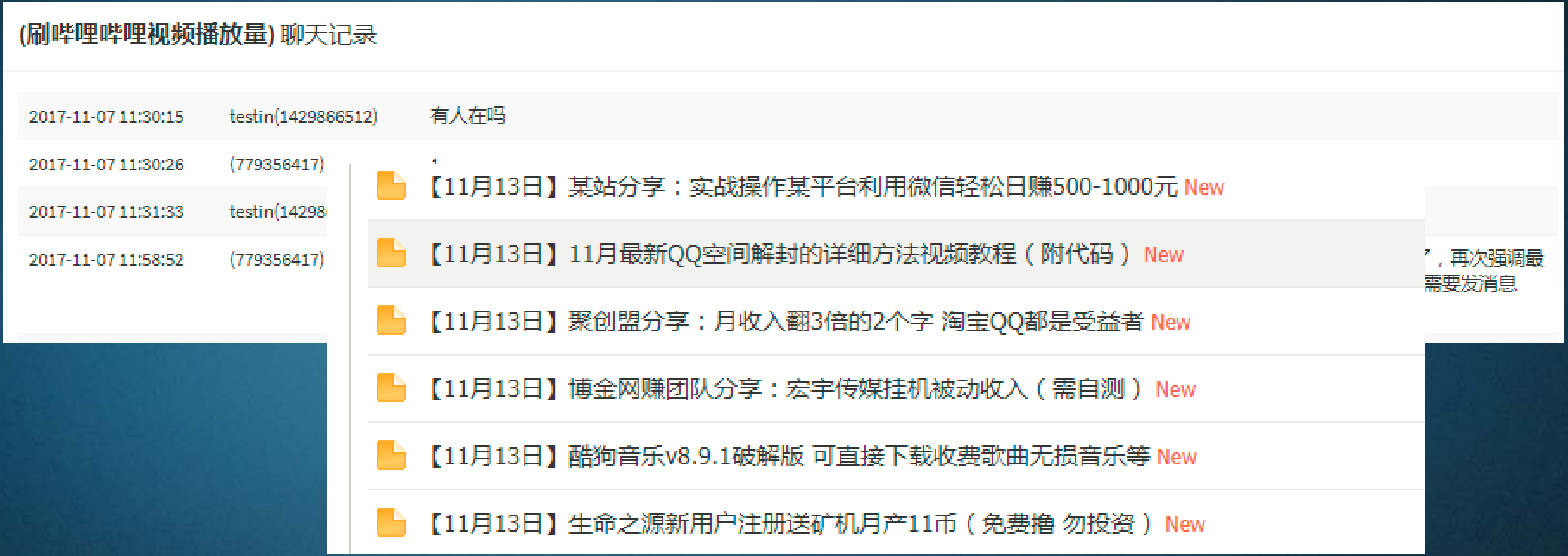
在最疯狂的时候，[redacted]每天要补贴掉100多万元，但后来证明其中30%甚至更多都被刷单者拿走了；地方分公司动辄向总部要走上百万的推广费，但结果只带来1000或者几百名新用户；员工普遍拿着高薪，学硅谷文化，每个月的水果酸奶钱都要花掉好几万。

当然，疯狂没有持续多久。[redacted]**在花掉4000多万人民币以后，彻底宣告失败。**

对抗思路

情报

开源情报

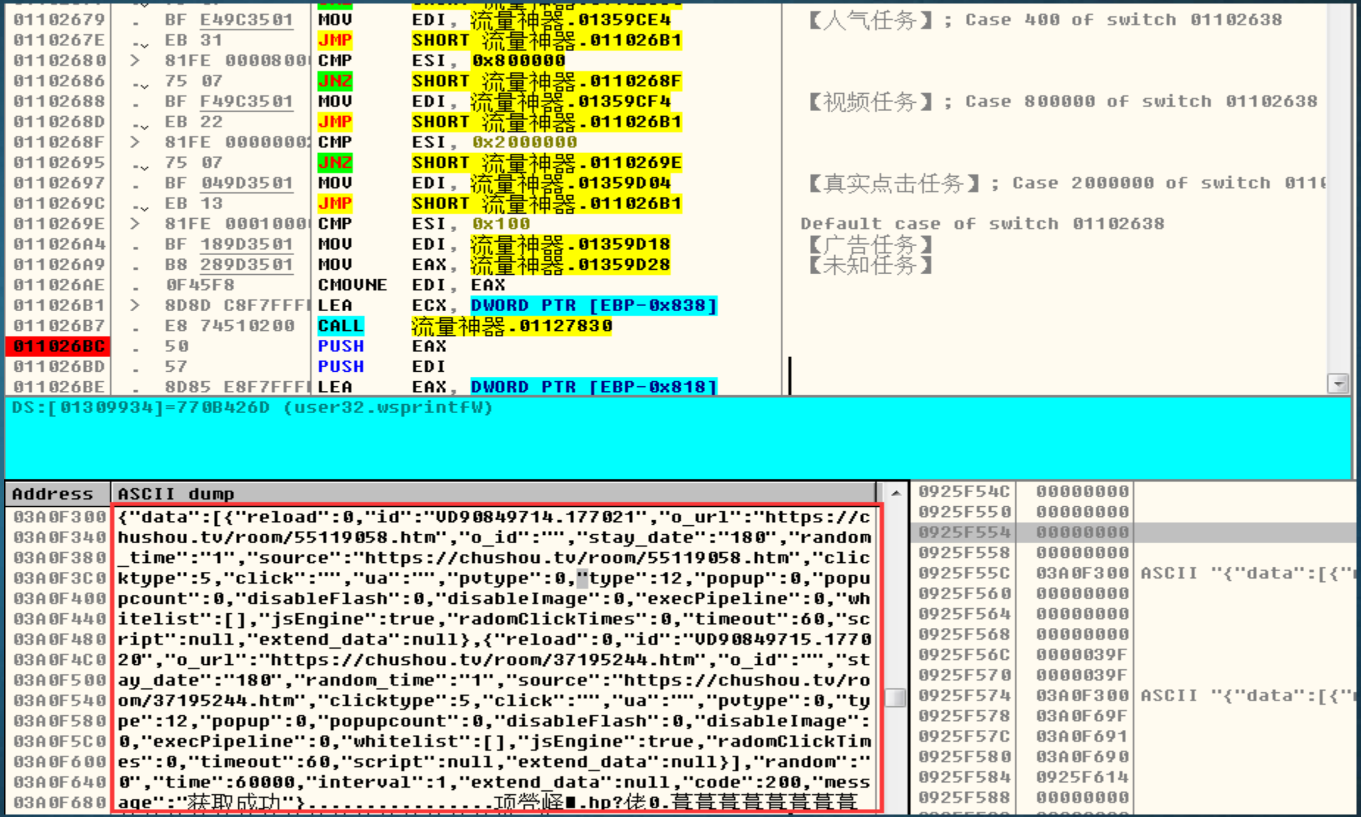


(刷哔哩哔哩视频播放量) 聊天记录

2017-11-07 11:30:15	testin(1429866512)	有人在吗
2017-11-07 11:30:26	(779356417)	
2017-11-07 11:31:33	testin(14298	
2017-11-07 11:58:52	(779356417)	，再次强调最 需要发消息

- 【11月13日】某站分享：实战操作某平台利用微信轻松日赚500-1000元 New
- 【11月13日】11月最新QQ空间解封的详细方法视频教程（附代码） New
- 【11月13日】聚创盟分享：月收入翻3倍的2个字 淘宝QQ都是受益者 New
- 【11月13日】博金网赚团队分享：宏宇传媒挂机被动收入（需自测） New
- 【11月13日】酷狗音乐v8.9.1破解版 可直接下载收费歌曲无损音乐等 New
- 【11月13日】生命之源新用户注册送矿机月产11币（免费撸 勿投资） New

闭源情报



```
01102679  .   BF E49C3501    MOV     EDI, 流量神器.01359CE4
0110267E  .v  EB 31          JMP     SHORT 流量神器.011026B1
01102680  >   81FE 0000800(  CMP     ESI, 0x800000
01102686  .v  75 07          JNZ     SHORT 流量神器.0110268F
01102688  .   BF F49C3501    MOV     EDI, 流量神器.01359CF4
0110268D  .v  EB 22          JMP     SHORT 流量神器.011026B1
0110268F  >   81FE 0000000:  CMP     ESI, 0x2000000
01102695  .v  75 07          JNZ     SHORT 流量神器.0110269E
01102697  .   BF 049D3501    MOV     EDI, 流量神器.01359D04
0110269C  .v  EB 13          JMP     SHORT 流量神器.011026B1
0110269E  >   81FE 0001000(  CMP     ESI, 0x100
011026A4  .   BF 189D3501    MOV     EDI, 流量神器.01359D18
011026A9  .   B8 289D3501    MOV     EAX, 流量神器.01359D28
011026AE  .   0F45F8         CMOVNE  EDI, EAX
011026B1  >   8D8D C8F7FFF(  LEA     ECX, DWORD PTR [EBP-0x838]
011026B7  .   E8 74510200    CALL    流量神器.01127830
011026BC  .   50             PUSH    EAX
011026BD  .   57             PUSH    EDI
011026BE  .   8D85 E8F7FFF(  LEA     EAX, DWORD PTR [EBP-0x818]
```

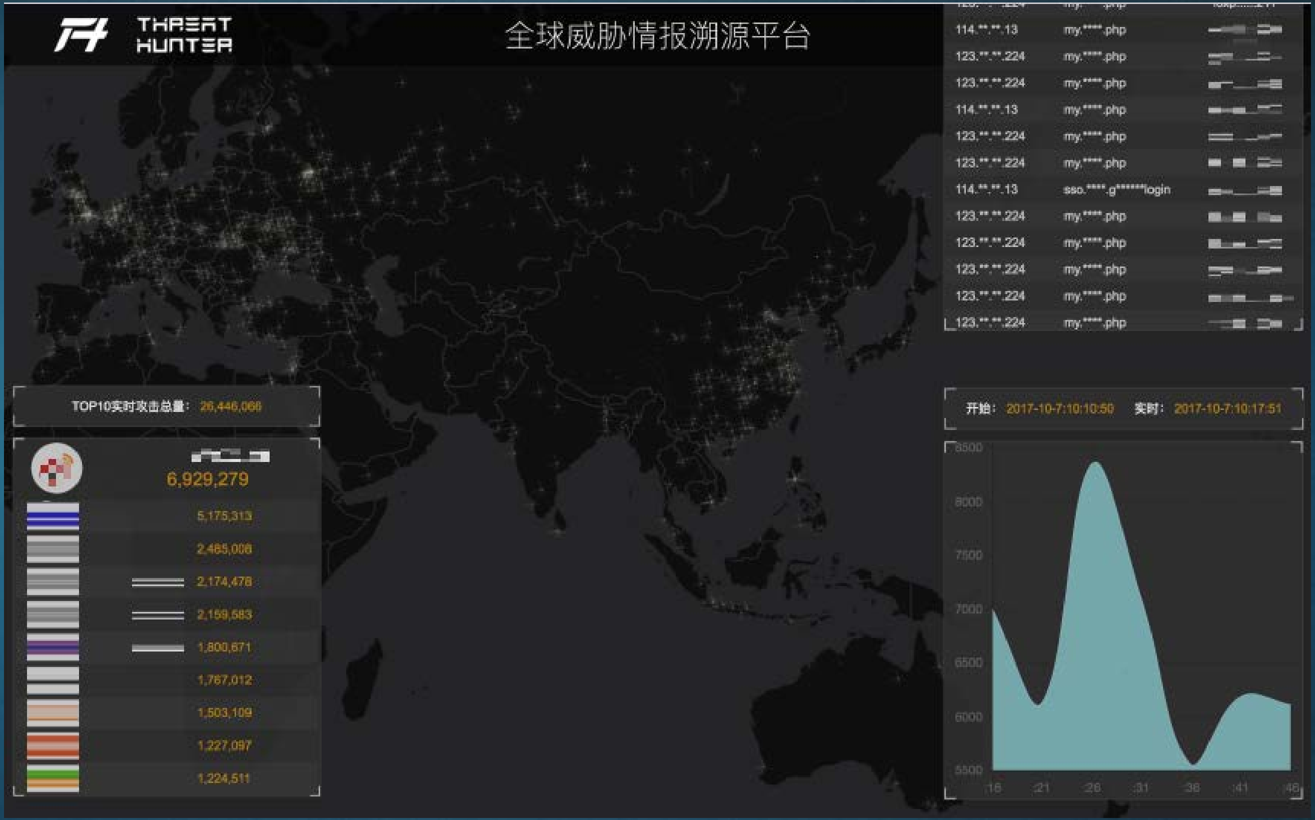
```
【人气任务】; Case 400 of switch 01102638

【视频任务】; Case 800000 of switch 01102638

【真实点击任务】; Case 2000000 of switch 011(

Default case of switch 01102638
【广告任务】
【未知任务】
```

```
DS:[01309934]=770B426D (user32.wsprintfW)
```

```
Address   ASCII dump
03A0F300  {"data":[{"reload":0,"id":"VD90849714.177021","o_url":"https://c
03A0F340  hushou.tv/room/55119058.htm","o_id":"","stay_date":"180","random
03A0F380  _time":"1","source":"https://chushou.tv/room/55119058.htm","clic
03A0F3C0  ktype":5,"click":"","ua":"","pvtype":0,"type":12,"popup":0,"popu
03A0F400  pcount":0,"disableFlash":0,"disableImage":0,"execPipeline":0,"wh
03A0F440  itelist":[],"jsEngine":true,"radomClickTimes":0,"timeout":60,"sc
03A0F480  ript":null,"extend_data":null},{"reload":0,"id":"VD90849715.1770
03A0F4C0  20","o_url":"https://chushou.tv/room/37195244.htm","o_id":"","st
03A0F500  ay_date":"180","random_time":"1","source":"https://chushou.tv/ro
03A0F540  om/37195244.htm","clicktype":5,"click":"","ua":"","pvtype":0,"ty
03A0F580  pe":12,"popup":0,"popupcount":0,"disableFlash":0,"disableImage":
03A0F5C0  0,"execPipeline":0,"whitelist":[],"jsEngine":true,"radomClickTim
03A0F600  es":0,"timeout":60,"script":null,"extend_data":null}],"random":"
03A0F640  0","time":60000,"interval":1,"extend_data":null,"code":200,"mess
03A0F680  age":"获取成功"}................项带哑■.hp?佬0.萁萁萁萁萁萁萁萁
```

```
0925F54C  00000000
0925F550  00000000
0925F554  00000000
0925F558  00000000
0925F55C  03A0F300  ASCII "{"data":[{"
0925F560  00000000
0925F564  00000000
0925F568  00000000
0925F56C  0000039F
0925F570  0000039F
0925F574  03A0F300  ASCII "{"data":[{"
0925F578  03A0F69F
0925F57C  03A0F691
0925F580  03A0F690
0925F584  0925F614
0925F588  00000000
```

闭源情报



THREAT HUNTER

全球威胁情报溯源平台

114.**.**.13	my.****.php	[redacted]
123.**.**.224	my.****.php	[redacted]
123.**.**.224	my.****.php	[redacted]
114.**.**.13	my.****.php	[redacted]
123.**.**.224	my.****.php	[redacted]
123.**.**.224	my.****.php	[redacted]
114.**.**.13	sso.****.g******login	[redacted]
123.**.**.224	my.****.php	[redacted]
123.**.**.224	my.****.php	[redacted]
123.**.**.224	my.****.php	[redacted]
123.**.**.224	my.****.php	[redacted]
123.**.**.224	my.****.php	[redacted]

TOP10实时攻击总量：26,446,066

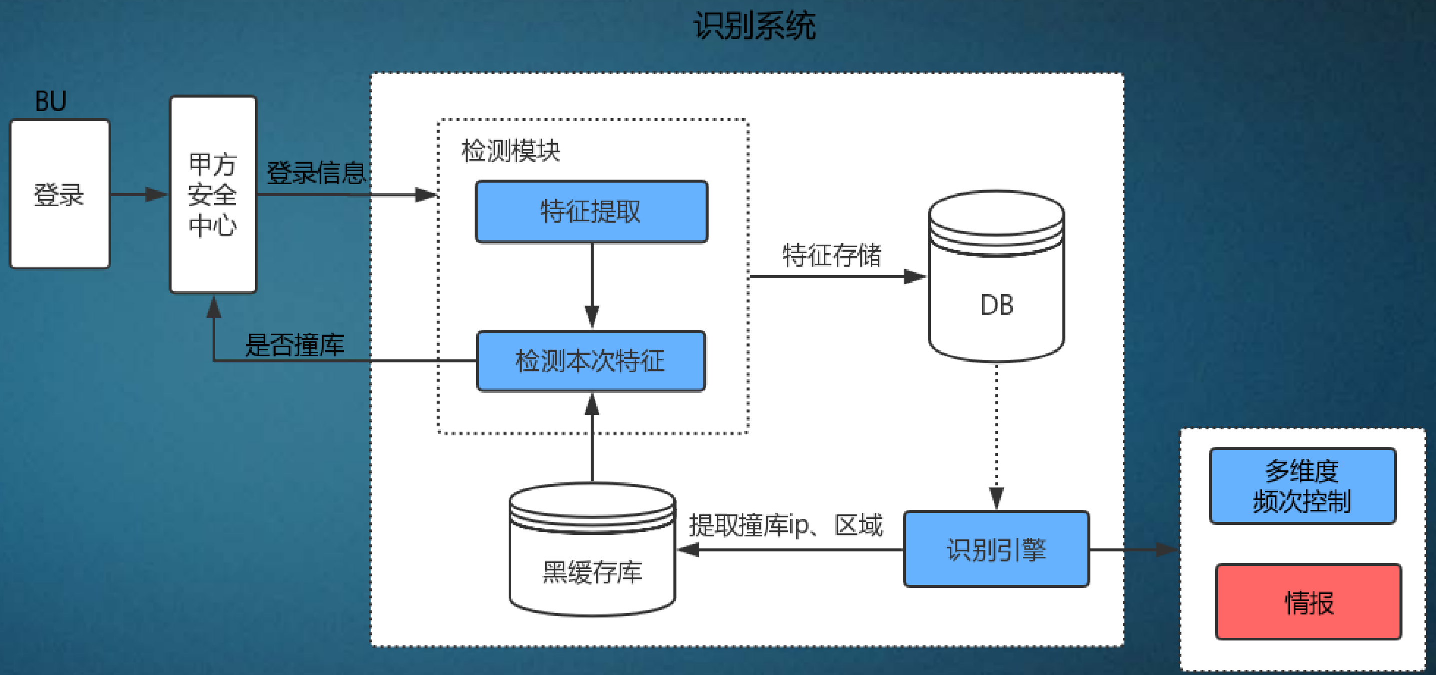
[redacted]	6,929,279
[redacted]	5,175,313
[redacted]	2,465,006
[redacted]	2,174,478
[redacted]	2,159,583
[redacted]	1,800,671
[redacted]	1,767,012
[redacted]	1,503,109
[redacted]	1,227,097
[redacted]	1,224,511

开始：2017-10-7:10:10:50　实时：2017-10-7:10:17:51

情报价值

→

情报结合的撞库识别方案



Thanks