TCSS 2018

中國羊毛黨來襲

你的優惠被吃掉了嗎？

ForceShield .Inc.
Belinda Lai

ForceShield
IoT Defender

Belinda Lai
Security Engineer
belinda.lai@forceshield.com

Work Experience:

- Embedded Engineer in Ruckus
- Security Engineer
  in Institute for Information Industry

Accomplishment:

- Speaker in 2017
  Taiwan Cyber Security Summit
- Speaker in HITCON 2015
  (Hacker in Taiwan Conference)
- A core founder of HITCON GIRLS
  (The first security community for girls in Taiwan)

Certification:

- GIAC Reverse Engineering Malware (GREM) from SANS
- Certified Ethical Hacking course from EC-Council
- ISO 20000-1:2011
- ISO 27001

OUTLINE

羊毛黨介紹

攻擊流程

工具訊息

灰色產業鏈

防禦機制

OUTLINE

羊毛黨介紹

攻擊流程

工具訊息

灰色產業鏈

防禦機制

羊毛黨

- 蒐集各渠道的優惠促銷活動
- 有選擇地參與活動
- 以相對較低成本,零成本換取優惠
- “薅”意为揪、拔除：薅羊毛
- 而關注與熱衷於“薅羊毛”的群體：羊毛黨
- 高流量＋人氣＝合格[illegible]賓人?

ForceShield
IoT Defender

災情頻傳

ofo再遭羊毛黨紅包騙補或將被視作盜刷_財經頻道_新浪網
finance.sina.com/bg/economy/sinacn/20170424/14551590461.html

全民答题背后：羊毛党作弊成风，乱象频发亟待监管
新浪网 - 2018年1月25日

信用卡积分回馈成羊毛党盛宴普通持卡人难享优惠
金融界 - 2018年1月25日
而其他时间抽多少次也不会中，由于放水时间不固定，因此大多是羊毛

支付宝被"薅"走137万！如何从源头根治羊毛党？
CSDN - 2018年1月11日

搜狐

支付宝10亿红包引来"羊毛党" 官方:已处理800个账户
新华网 - 2017年12月31日
这场支付宝自掏10亿发动的红包活动，初衷是普及移动支付，吸引更多
也毫无悬念地引来大批"羊毛党"。现在看来，"羊毛党"的收成也的确丰厚
传的截图，有的支付宝用户在短时间内获取了137.8万元红包，有的获取
包，同时显示还有10万+个红包在来的路上。 支付宝官方近日 ...

还在到处群发抢红包？支付宝已经封了800个账号
搜狐 - 2018年1月2日

13 %

ForceShield
IoT Defender

國內案例

無法結帳網友氣炸

PChome商店街昨凌晨3時推整點搶紅包活動，輸入指定序號，購物滿2千現折1111元，活動一開跑造成系統短暫異常，網友抱怨「網頁當掉」，還有人一連輸入10幾次信用卡資料都無法結帳，遭批「萬人購買，無人成交」、「難怪被蝦皮打趴」。蝦皮和PChome昨均解釋，系統出包因短時間大量湧入人潮所致；但兩業者都不公布業績和熱賣品項資料。

蘋果即時 最新 焦點 熱門 娛樂 愛指網 社會 國際 政治 生活 火線 3C 動物 副刊

鑽電商活動漏洞　3天寄數百空貨袋賺上萬購物金

30518　出版時間：2017/11/15 19:58

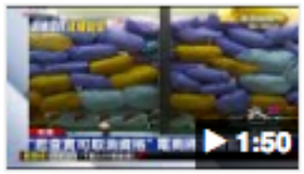
隨貨退差額買賣雙方串通賺蝦皮免運- YouTube

https://www.youtube.com/watch?v=USmYjdLOjo0

2016年10月13日 - 上傳者：台視新聞TTV NEWS

立即訂閱「台視新聞」頻道(http://www.youtube.com/ttvnewsview)，隨時掌握國內外最新、最熱、最夯的新聞影音。 台視新聞新聞官網- http://www.ttv ...

鑽電商漏洞！ 超取回饋20元、賣家自賣自取- YouTube



https://www.youtube.com/watch?v=7TYNC3D_yZU

2017年12月13日 - 上傳者：東森新聞 CH51

雙十二購物節，有電商為了回饋消費者，祭出優惠，只要到超商取貨，不只免運費，還能夠獲得20元購物金，造福消費者，但現在卻傳出有人鑽漏洞，電商平台的個人賣家另 ...

ForceShield

災情多嚴重？

ForceShield

IoT Defender

發展歷程

2013

O2O
電子商務

2014

P2P網路
借貸平台

2015

羊毛黨專業
分工化

2016

平台倒閉潮

2017

打擊羊毛黨聯盟

ForceShield
IoT Defender

OUTLINE

羊毛黨介紹

攻擊流程

工具訊息

灰色產業鏈

防禦機制

工作流程

01

獲得情報

取得各平台
促銷活動

02

準備武器

尋找漏洞
準備工具

03

上緊發條

大量註冊,
登入, 簽到
等前置作業

04

薅羊毛

根據漏洞
搶購平台優惠

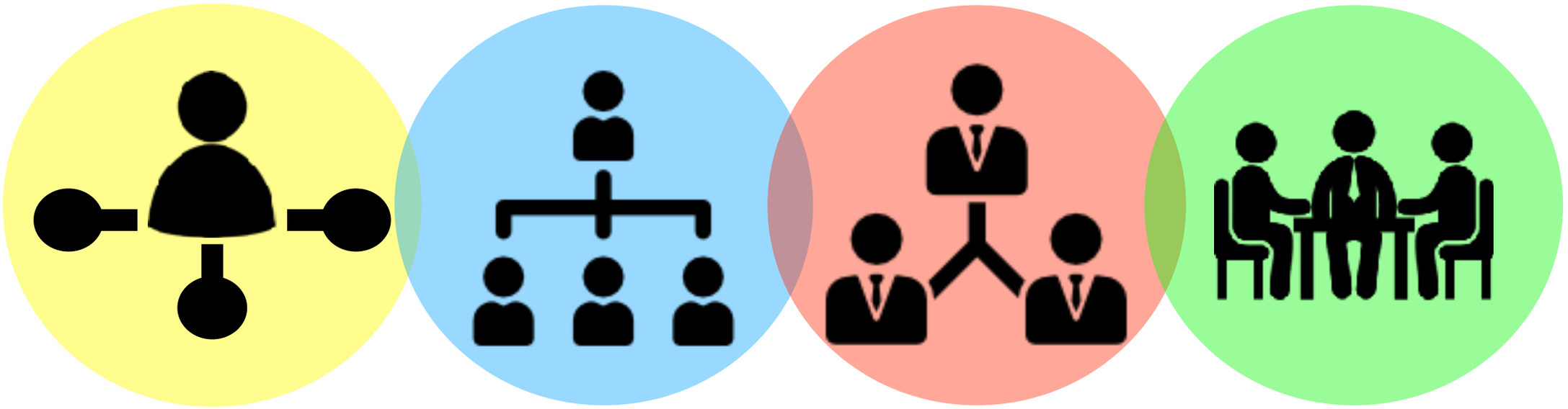
05

轉為現金

將優惠卷
商品,積分等
轉賣或變現

ForceShield
IoT Defender

攻擊者



個人作業

團體戰

專業人士

公司經營

ForceShield

IoT Defender

工具

爬蟲

搜集優惠訊息

搜集個資

釣魚網站,內部泄露

自動化Bot

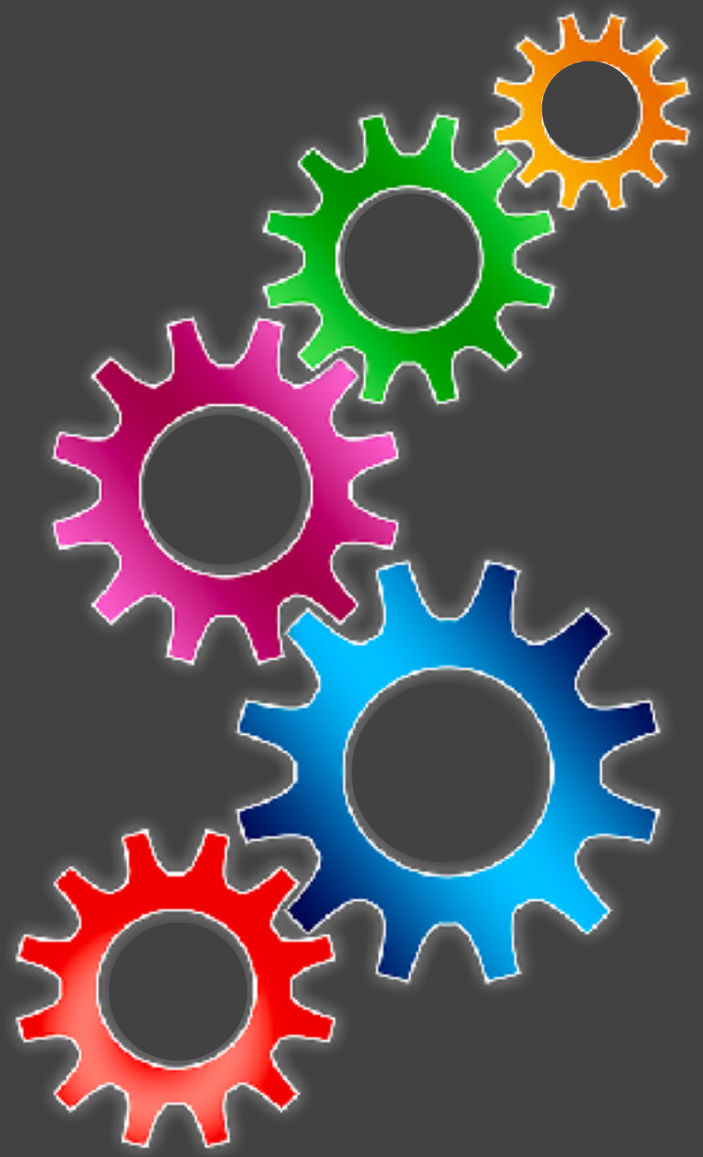
自動化註冊，簽到

自動化Bot

搶優惠，下單

免洗ＩＰ

Proxy, 黑名單繞過



ForceShield
IoT Defender

OUTLINE

羊毛黨介紹

攻擊流程

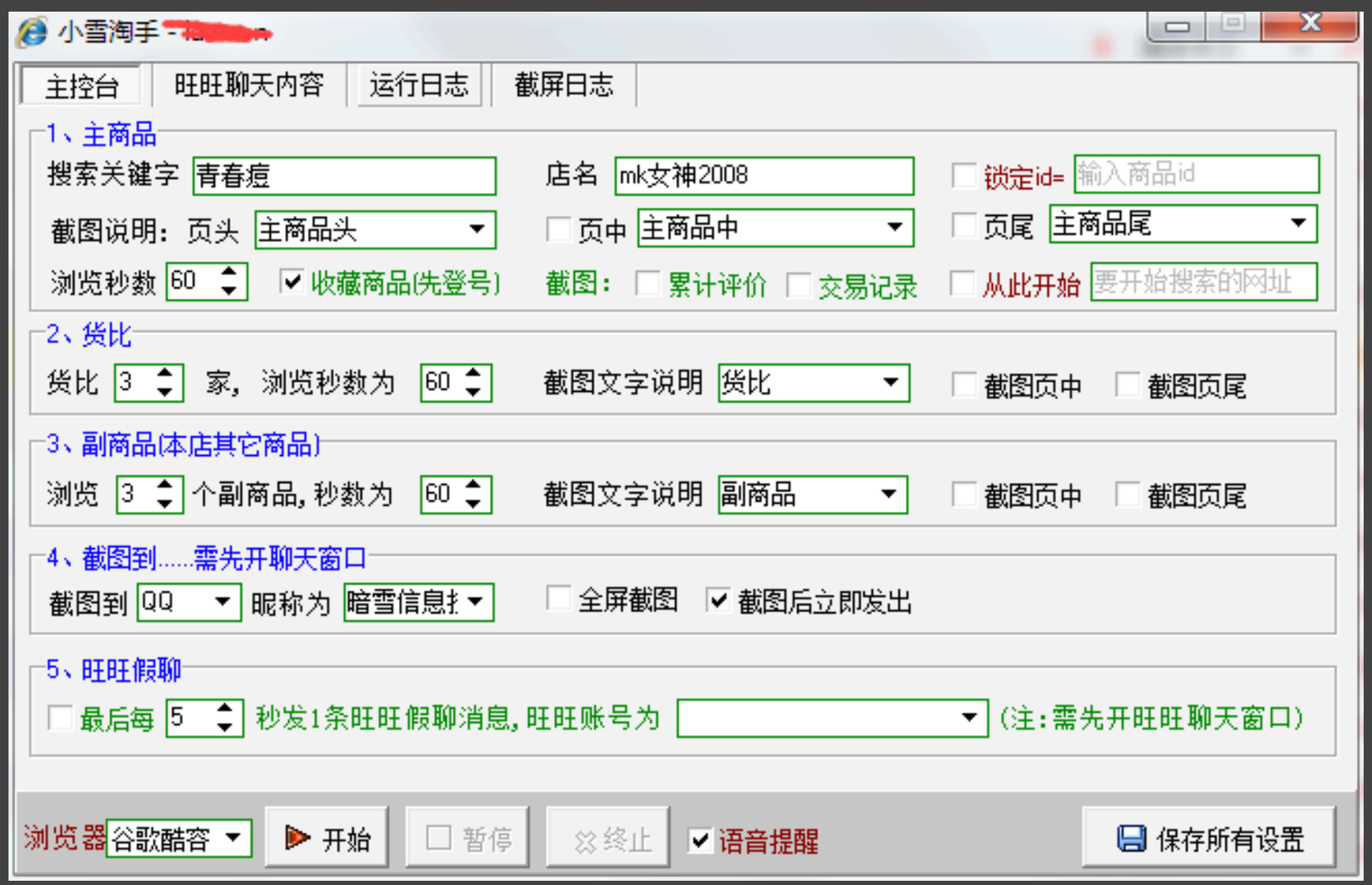
NEWS

工具訊息

灰色產業鏈

防禦機制

工具



- 自動下單
- 關鍵字搜索
- 比價
- 自動截圖
- 機器人聊天
- 副商品瀏覽

ForceShield
IoT Defender

工具

ForceShield
IoT Defender

工具

查排名 淘口令卡首屏 提升排名 淘宝无线查排名 店铺优化-卖家工具

http://shengyitong.net

查排名(maijiagongju.cn)免费淘宝店铺管理工具-卖家服务：一站式卖家服务平台！淘宝无线查排名,打造专业的卖家店铺优化工具箱。

Keywords: 刷流量, 流量软件, 手机刷流量, 卖家工具：手淘查排名

★ ★ ★ ★ ★

卖家工具

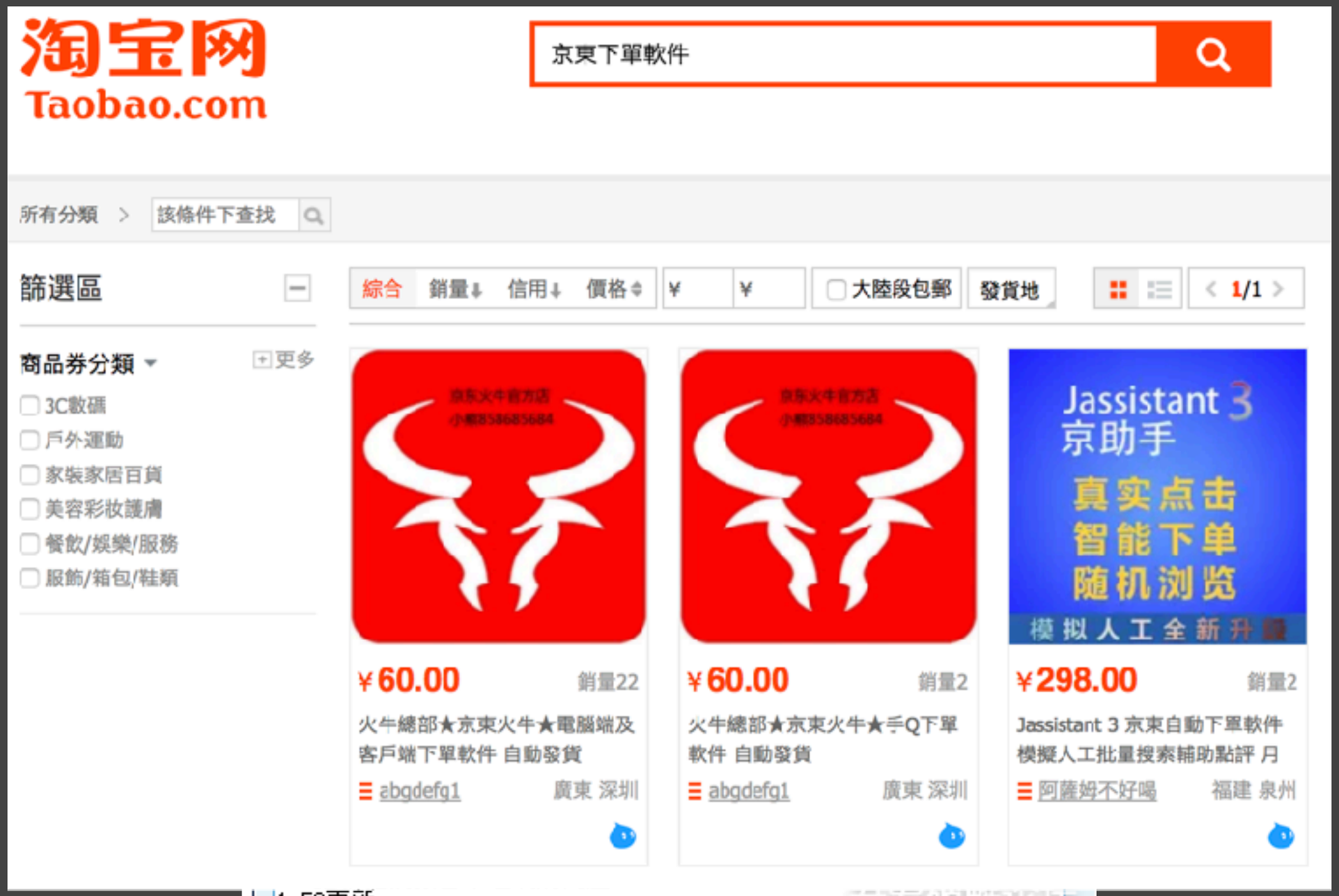
maijiagongju.cn

卖家开店孵化工具箱

ForceShield

IoT Defender

工具

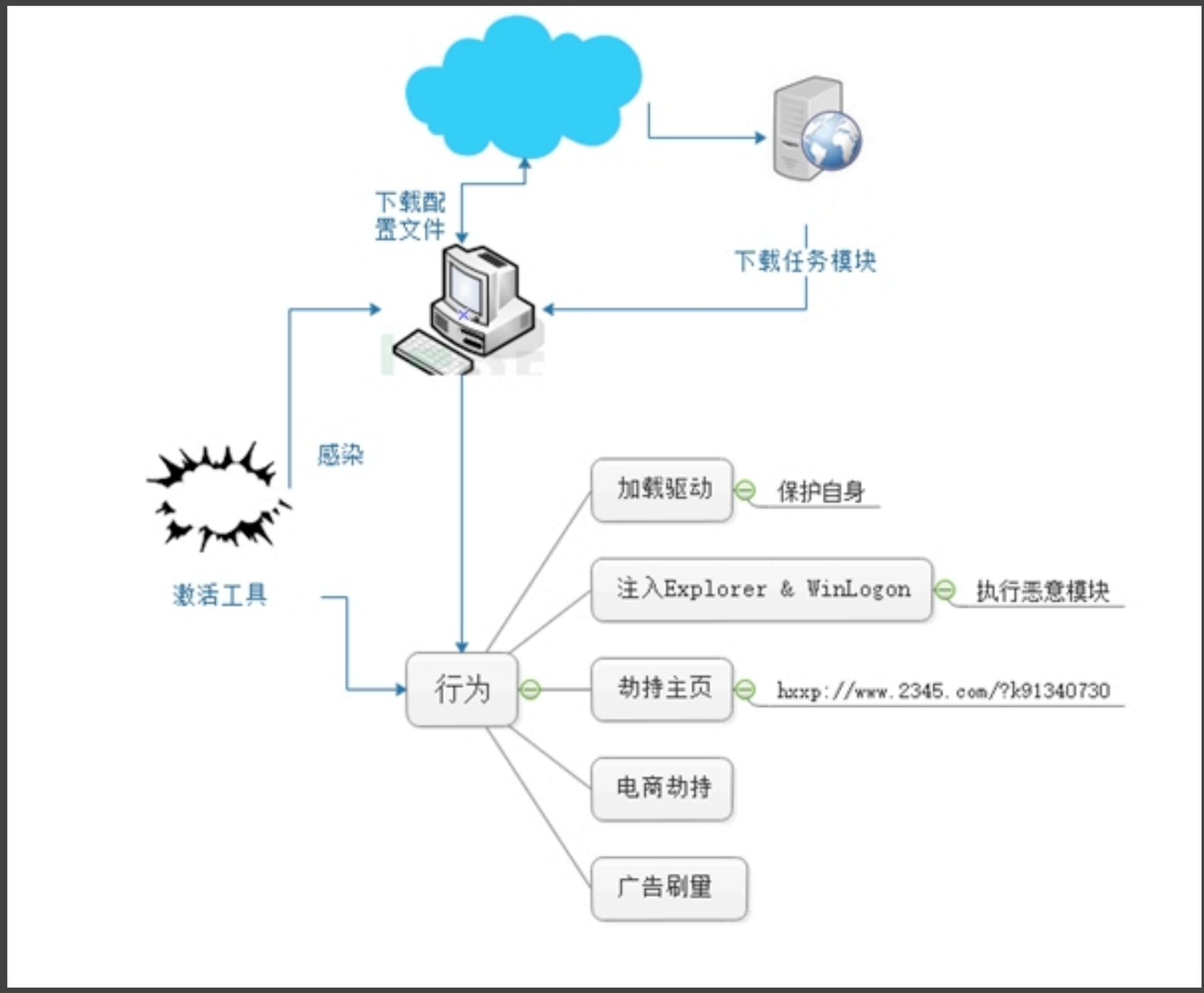


1.52更新
1、更新商品分类树搜索不显示商品名的问题

www.52pojie.cn

ForceShield
IoT Defender

工具



ForceShield
IoT Defender

OUTLINE

羊毛黨介紹

攻擊流程

工具訊息

灰色產業鏈

防禦機制

灰色產業鏈

領頭羊	駭客	卡商	打碼平台	現金收入
訊息分享	尋找漏洞	虛擬帳號	自動化登入	變賣轉現
尋找目標	工具製作	大量個資	破解驗證機制	協助銷贓

ForceShield
IoT Defender

領頭羊

撸了个北美羊毛快报和公众...

站长我就自称羊毛君吧。

中國新聞

首頁 熱點 娛樂 科技 財經 體育 軍事 旅遊 母嬰 更多..

進擊的羊毛黨：近億殭屍手機殺向海外，東南亞欺詐流量佔3成

大陸資訊 | 11月02日

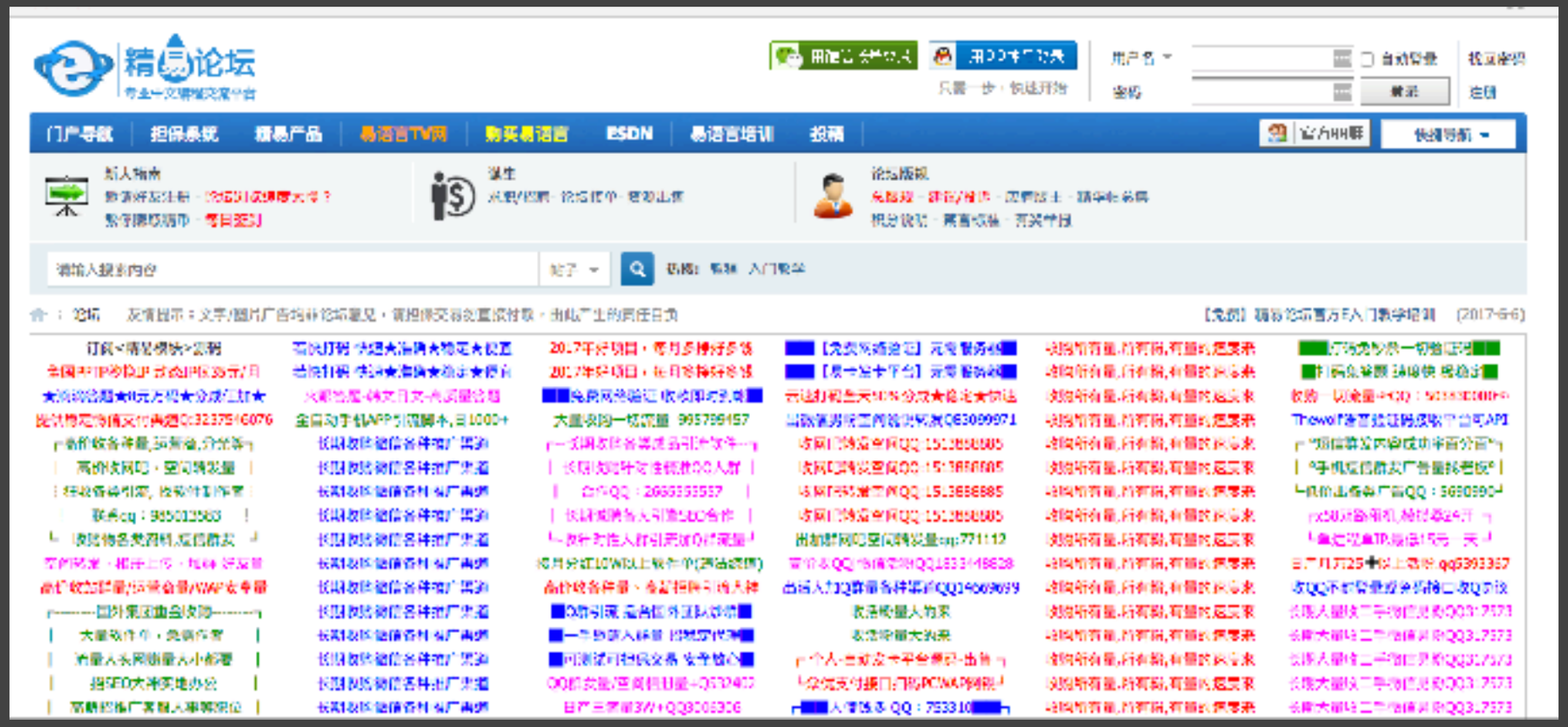
隨著中國互聯網的快速發展，不少公司正大踏步走向海外，阿里系、獵豹、Apus等公司已經在海外嶄露頭角。 在巨大的冰山之下，有更多的黑灰產公司、羊毛黨工作室已經開始...

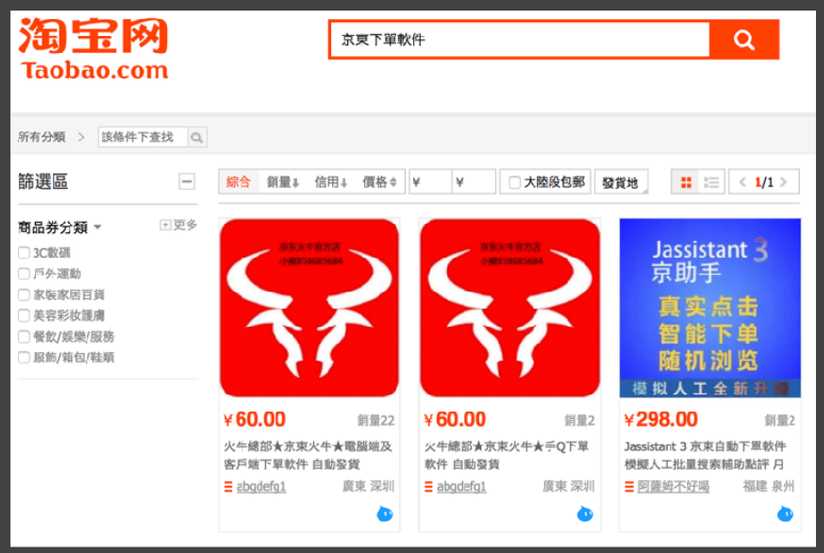
https://www.haoyangmao8.com/ - - 百度快照

ForceShield

IoT Defender

駭客





ForceShield
IoT Defender

卡商

sim卡營運商

整合資源
大量註冊
虛擬帳號

卡商

卡商管理

駭客

竊取大量個資

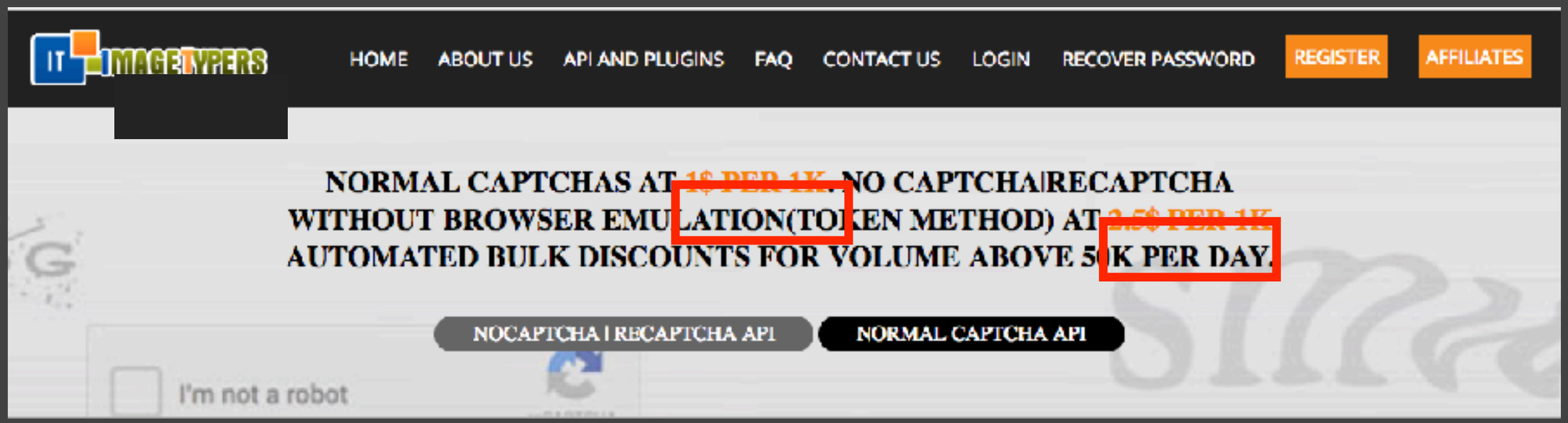
貓池

卡商平台

媒合配對

ForceShield
IoT Defender

打碼平台



ForceShield
IoT Defender

現金收入

- 折扣販售
- 二手市場
- 遊戲幣／點數變賣
- 虛擬錢包
- 虛擬貨幣
- 虛假店家
- 自買自賣

ForceShield
IoT Defender

OUTLINE

羊毛黨介紹

攻擊流程

工具訊息

灰色產業鏈

防禦機制

供應商

活動規劃	活動進行	事後檢討	平時維護
風險控管	追蹤監測系統	限制權益使用範圍	事件演練
規劃活動規則	動態調整	避免優惠被換現	系統維護
部署監測系統	衡量優惠數量	監控權益使用方式	最新攻擊手法
資安威脅評估	加強Server安全	追蹤使用者活動	資安教育訓練

ForceShield
IoT Defender

消費者

不要以身試法

不要貪小便宜

不要下載來路不明的軟體

要保護好自己的個資

ForceShield
IoT Defender

ForceShield

IoT Defender

THANK YOU !

- Reference :
- 中國電信安全幫 《2016年中国网站安全报告》
- 阿里安全 毒眼系列报告之黄牛软件
  http://www.freebuf.com/articles/paper/160726.html
- ASC 2016 移动物联网安全高峰论坛 大数据环境下的 黑产对抗研究
- 金山毒霸安全實驗室 多款 Windows 激活工具捆绑“薅羊毛”病毒
  https://www.leiphone.com/news/201711/K1mg6selYYoFWYwW.html
- 宅客頻道 雙11黑產薅一天吃一年？反“薅羊毛”絕技在此：
  https://weiwenku.net/d/103701610
- 騰訊雲安全 移动APP安全行业报告电商篇：
  http://www.freebuf.com/articles/terminal/128125.html
- 網貸之家 当羊毛党已“老”P2P企业的下一波“流量客”又在何方
  http://www.wdzj.com/zhuanlan/guancha/17-4865-1.html
- 新浪專欄 上亿黑卡在手，撸垮上市公司，羊毛党大揭秘
  http://tech.sina.com.cn/csj/2017-10-23/doc-ifymzqpq3491043.shtml
- 新京報 抢票软件变身黄牛牟利工具 多个账号同时登录：
  https://c.m.163.com/news/a/D8QQ8JU604388CS9.html?spss=newsapp&fromhistory=1
- 中新網 IP变脸：“刷票党、羊毛党”背后有特大黑产团伙
  http://www.chinanews.com/it/2017/11-15/8377105.shtml
- 精易論壇 https://bbs.125.la/
- 當羊毛黨「老了」，P2P的下一波流量客在哪裏？ https://itw01.com/27LE8D9.htmlhttps://itw01.com/27LE8D9.html