ThreatBook

# 安全威胁情报与分析

薛锋, ThreatBook

# 内容

- 自我介绍
- 几个故事
- 什么是威胁情报
- 基础数据
- 威胁情报分析

ThreatBook

# 自我介绍

- 微步在线创始人、CEO。国内首个安全威胁情报公司
- 亚马逊中国首席安全官(CISO)
- 微软互联网安全战略总监
- 耐威实验室技术负责人
- 公安部

ThreatBook

# 琅琊榜


ThreatBook

# 琅琊榜

# 琅琊榜

# 琅琊榜

# 琅琊榜

# 故事一：索尼

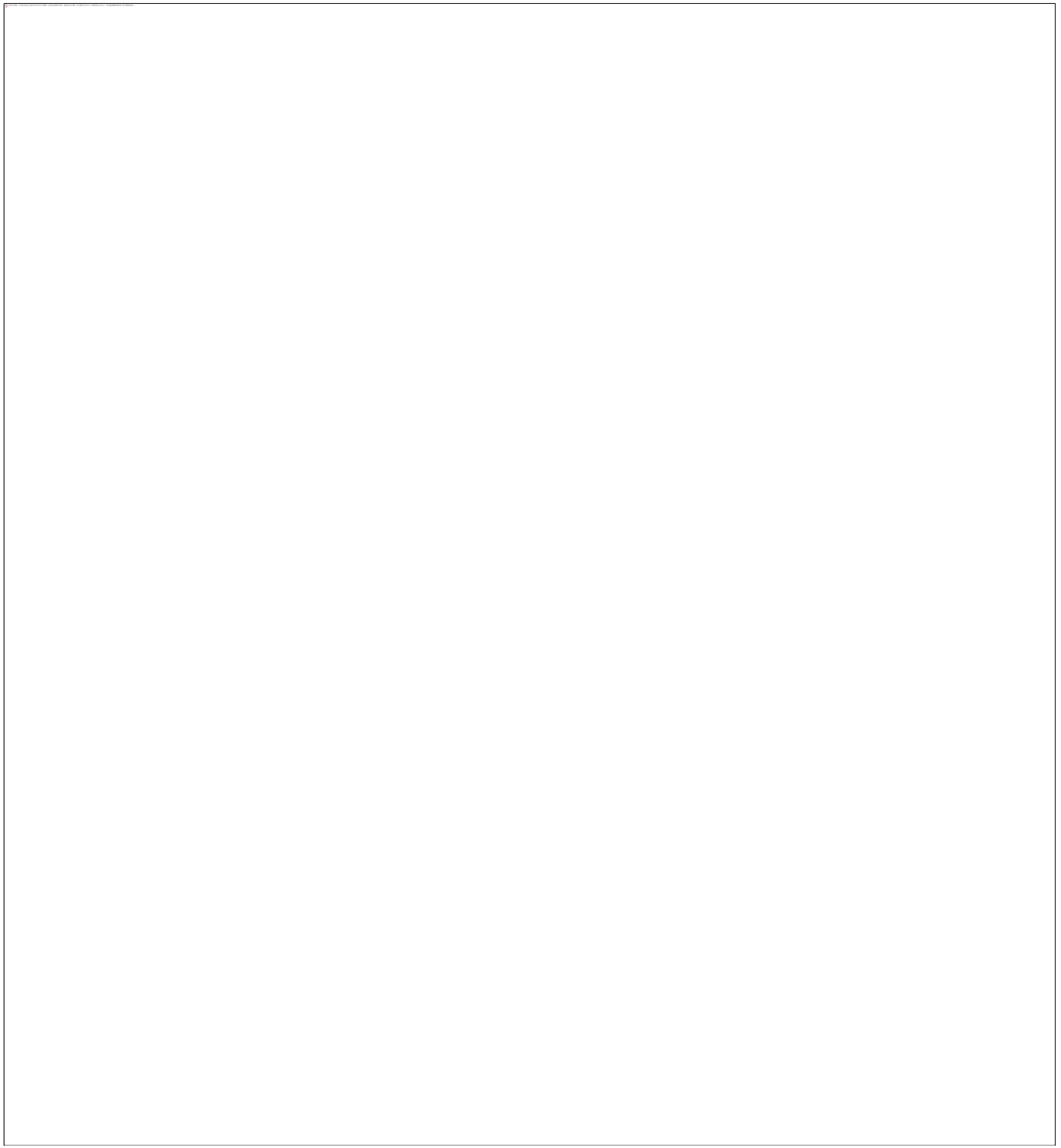
# 故事二：XcodeGhost


ThreatBook

# 故事二：XcodeGhost


ThreatBook

# 故事二：



ThreatBook

# 故事二：XcodeGhost动机

- 疑点一：**XcodeGhost 与 KeyRaider 的关系**

8月，PaloAlto Networks 曾披露过代号为 KeyRaider 的恶意程序盗取了 225000 个 Apple 帐号，报告中提到 KeyRaider 曾向 icloud-analysis.com 发送信息

- 疑点二：**XcodeGhost 与流行的 PC 木马病毒 TrojanSpy 的关系**

2015年3 至 9月 期间，与 XcodeGhost 相关的域名 icloud-analysis.com 和 allsdk.org 都曾指向 IP 地址 50.63.202.48，ThreatBook 通过威胁情报关联分析发现，同一时间段内超过七成的寄生于此 IP 地址的木马病毒属于 TrojanSpy 家族。

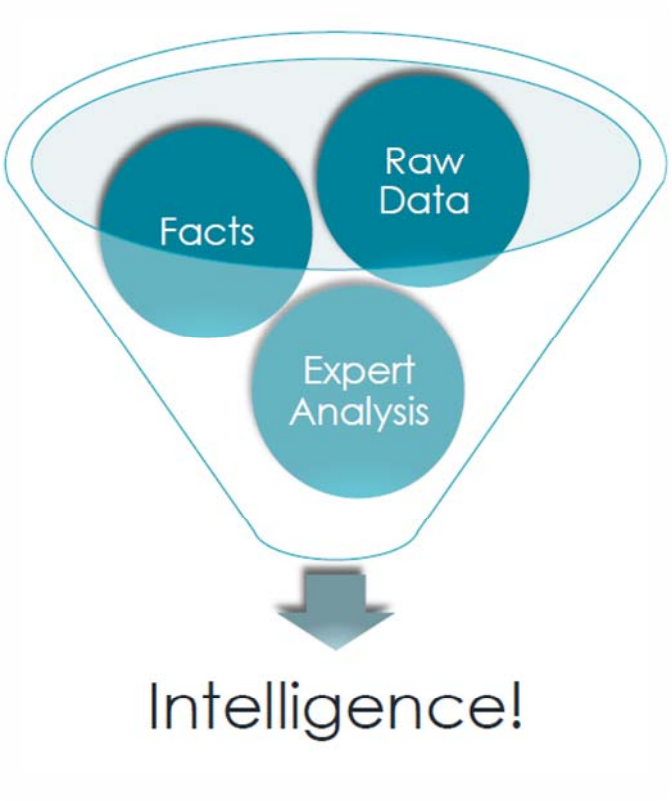
ThreatBook

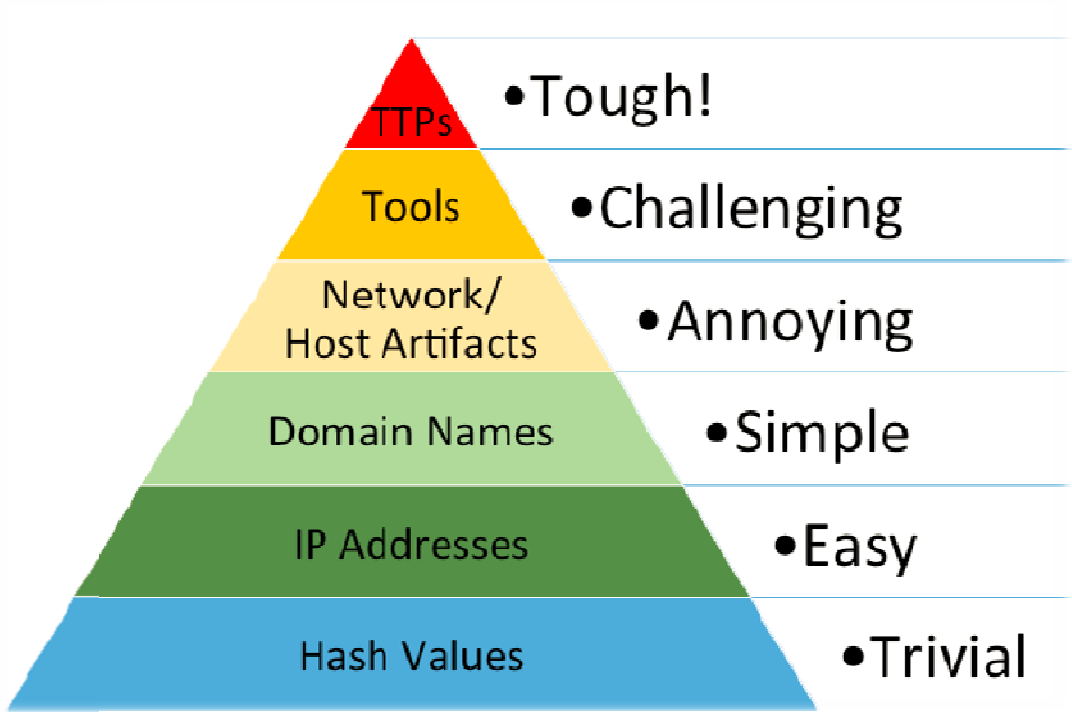
# 故事三

# 故事四：零售行业



# 安全威胁情报




ThreatBook

# 三大原则：防住、检测、保密

## 检测和响应
## Detection and Response

ThreatBook

# 知彼、知己


ThreatBook

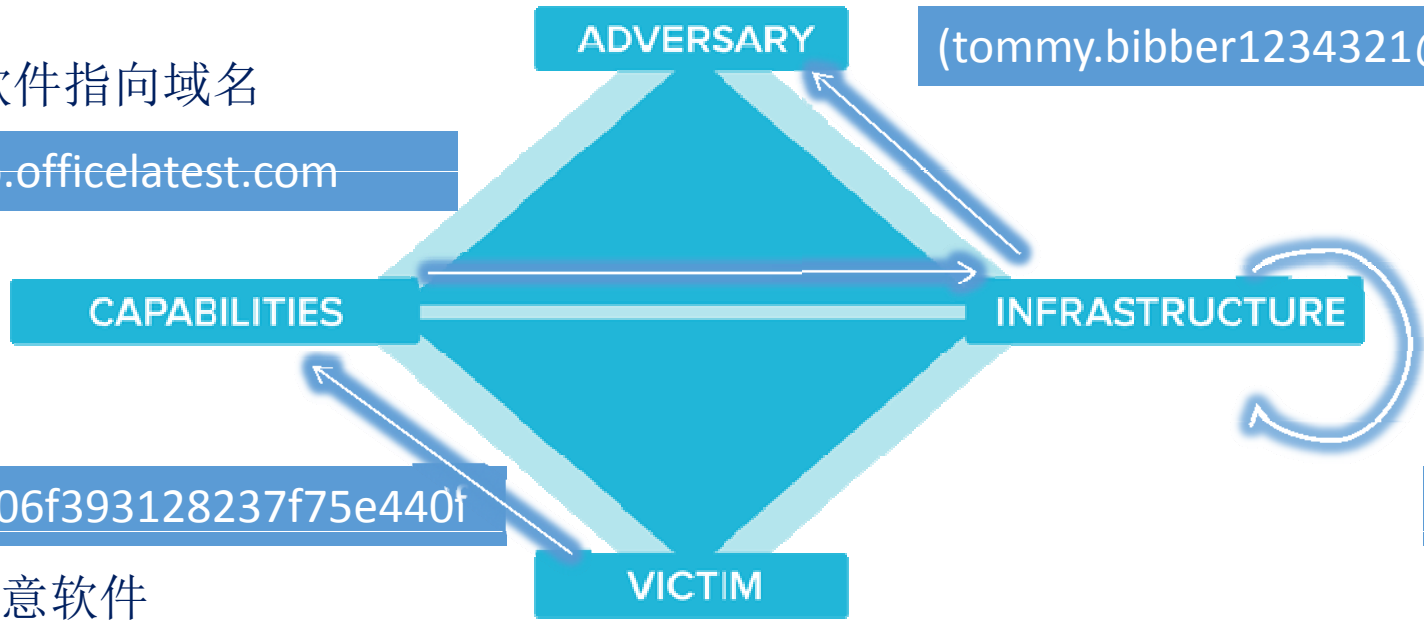
# 钻石模型

(4) 谁？

(tommy.bibber1234321@ddd.com)

(2) 恶意软件指向域名

info.officelatest.com




(3) C2 IP

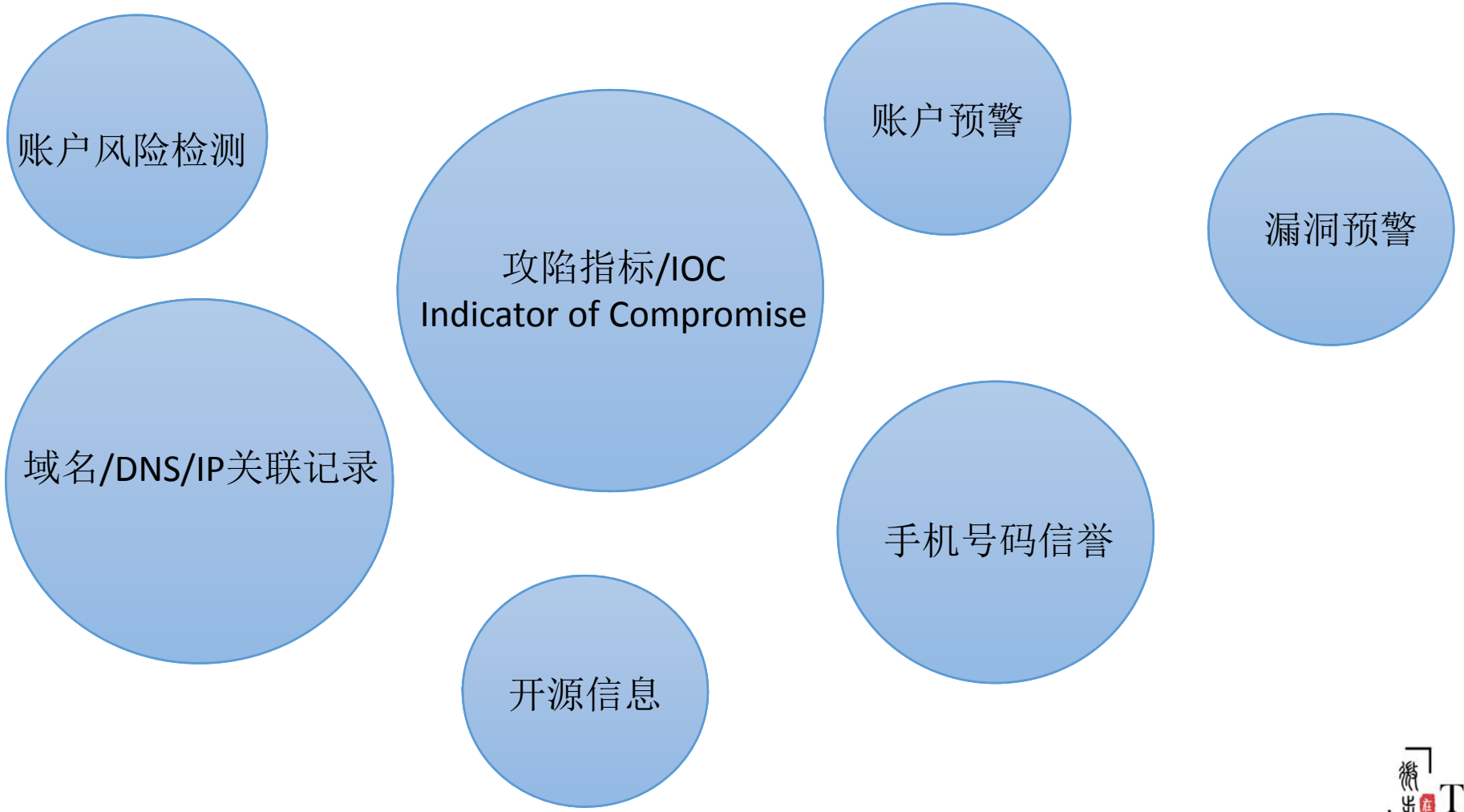
142.91.132.23

0606c10388c306f393128237f75e440f

受害人发现恶意软件

ThreatBook

# 威胁情报在中国




ThreatBook

# 可机读威胁情报示例

Branch: **master** ▾ **schemas** / samples / **CybOX_Domain_Instance.xml**

 **ikiril01** on Dec 20 2013 Updated versions in samples to account for v2.1 update

**3** contributors 

Executable File | 19 lines (18 sloc) | 965 Bytes **Raw** **Blame** **History**

```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <cybox:Observables xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
3      xmlns:cybox="http://cybox.mitre.org/cybox-2"
4      xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
5      xmlns:URIObject="http://cybox.mitre.org/objects#URIObject-2"
6      xmlns:example="http://example.com/"
7      xsi:schemaLocation="
8      http://cybox.mitre.org/cybox-2 ../cybox_core.xsd
9      http://cybox.mitre.org/objects#URIObject-2 ../objects/URI_Object.xsd"
10     cybox_major_version="2" cybox_minor_version="1" cybox_update_version="0">
11     <cybox:Observable id="example:Observable-0b9af310-0d5a-4c44-bdd7-aea3d99f13b6">
12         <cybox:Object id="example:Object-15be6630-b2df-4bf9-8750-3f45ca9e19cf">
13             <cybox:Properties xsi:type="URIObject:URIObjectType" type="Domain Name">
14                 <URIObject:Value>example.com</URIObject:Value>
15             </cybox:Properties>
16         </cybox:Object>
17     </cybox:Observable>
18 </cybox:Observables>
```

# 安全分析云


Virusbook Beta

首页 API 关于

SHA256：d4526f0710fa2

分析日期：2015-09-13 21

云查杀： （还有 4 款

检出率： 7 / 8

| 反病毒软件 |
| --- |
| 安天 ( Antiy ) |
| AVG |
| 腾讯 ( Tencent ) |
| 百度 ( Baidu ) |
| 金山 ( Kingsoft ) |
| 趋势 ( TrendMicro ) |
| IKARUS |
| 360 ( Qihoo 360 ) |

API简介

Public API

Private API

## Private API

VirusBook Private API 为您提供高品质的收费服务。不同于Public API的局限性和低优先级，Private API能为您提供更加全面和便捷的服务。

Private API能返回给您更加详细的查询信息，包括：VirusBook的元数据（文件第一次和最后一次出现的日期、上传次数、上传文件名等），文件工具信息（sigcheck，打包信息，PE结构，沙箱分析等），完整的扫描信息（该文件所有版本的扫描报告，杀毒软件版本和签名更新等）和其它我们能提供的定制信息。

**只要您的行为不对安全产业构成直接或间接的威胁，并且遵守VirusBook隐私条款，您即可将VirusBook Private API用于商业产品和服务中。**

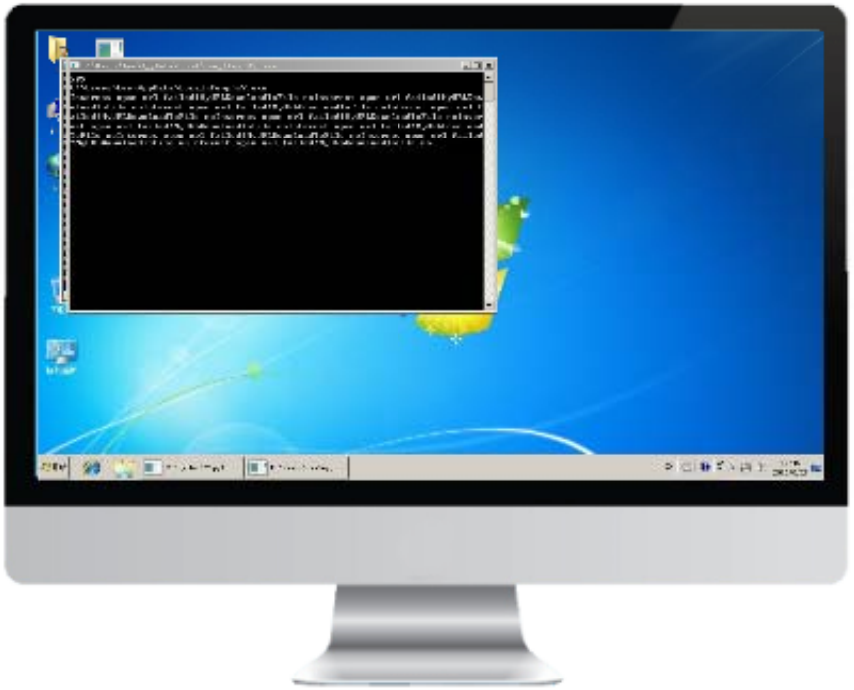
```
import requests
params = {'apikey': '-YOUR API KEY HERE-'}
files = {'file': ('sample.txt', open('sample.txt', 'rb'))}
response = requests.post('https://www.virusbook.cn/api/v1/file/scan', files=files, params=params)
json = response.json()
print json
{
  "response_code": 1,
  "verbose_msg": "Your scan request has been submitted and queued, please come back for the report later.",
  "permalink": "https://www.virusbook.cn/view_report/scan/93a3c629fecfd10c1cf614714efd69b10e89cfcaf94c2609d6
88b27754e4ab41-13593455675",
  "resource": "93a3c629fecfd10c1cf614714efd69b10e89cfcaf94c2609d688b27754e4ab41",
  "scan_id": "93a3c629fecfd10c1cf614714efd69b10e89cfcaf94c2609d688b27754e4ab41-13593455675",
  "sha256": "93a3c629fecfd10c1cf614714efd69b10e89cfcaf94c2609d688b27754e4ab41"
}
```

Book

# 安全分析云

动态分析报告：

## 屏幕截图



# 安全分析云

## 网络分析

▲ 主机通信

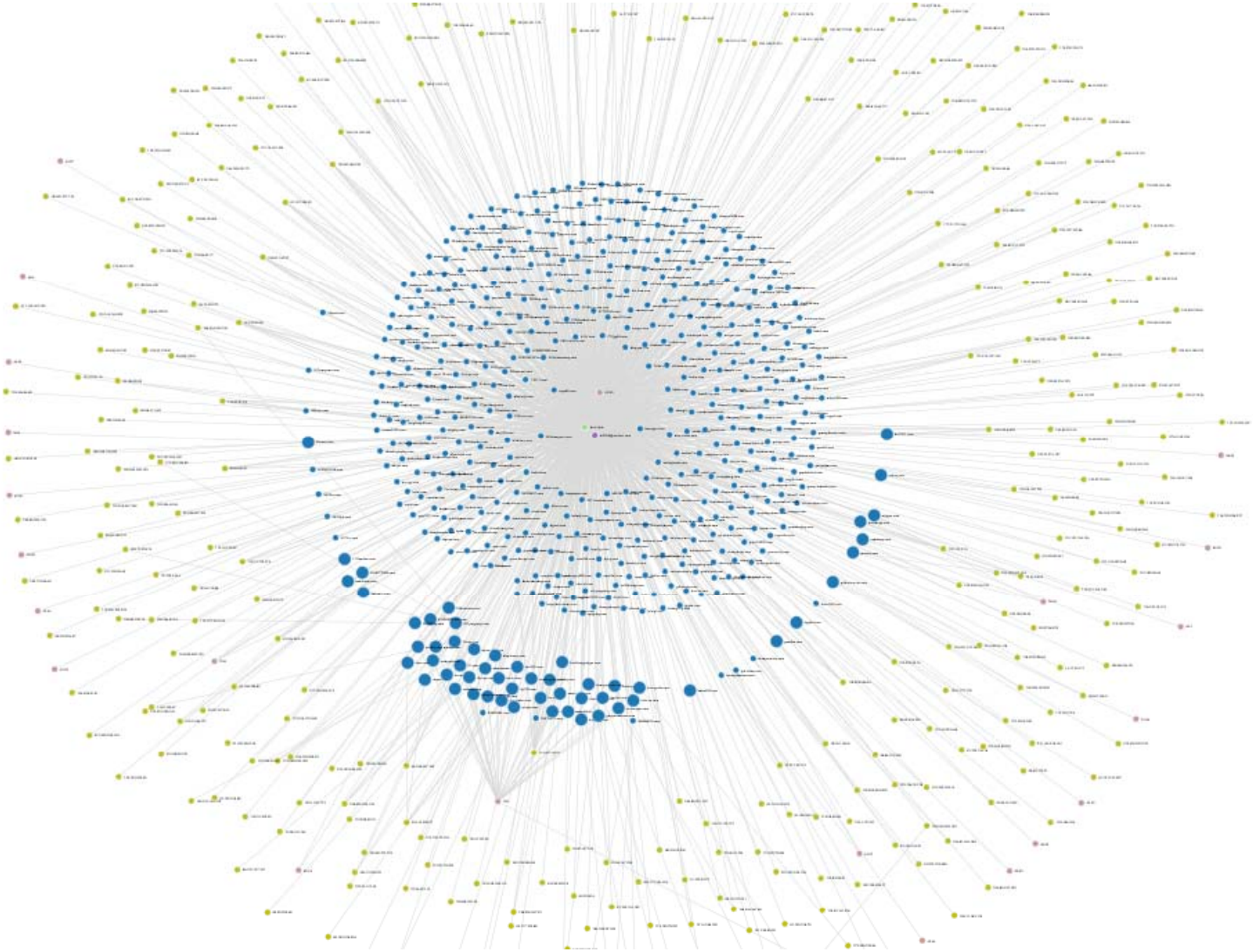
| IP地址 | 位置 | 经纬度 |
| --- | --- | --- |
| 104.41.150.68 | 博伊顿 | -78.3905101,36.665756 |
| 122.49.30.20 | 北京 | 116.3974589,39.9388838 |
| 8.8.8.8 | GOOGLE | |

▲ DNS请求

| 域名 | IP地址 | 位置 | 经纬度 |
| --- | --- | --- | --- |
| dns.msftncsi.com | 131.107.255.255 | 美国 | -89.143509,37.136162 |
| teredo.ipv6.microsoft.com | 94.245.121.251 | 都柏林 | -6.286360,53.334129 |
| asust.5i9u.com | 122.49.30.20 | 北京 | 116.3974589,39.9388838 |

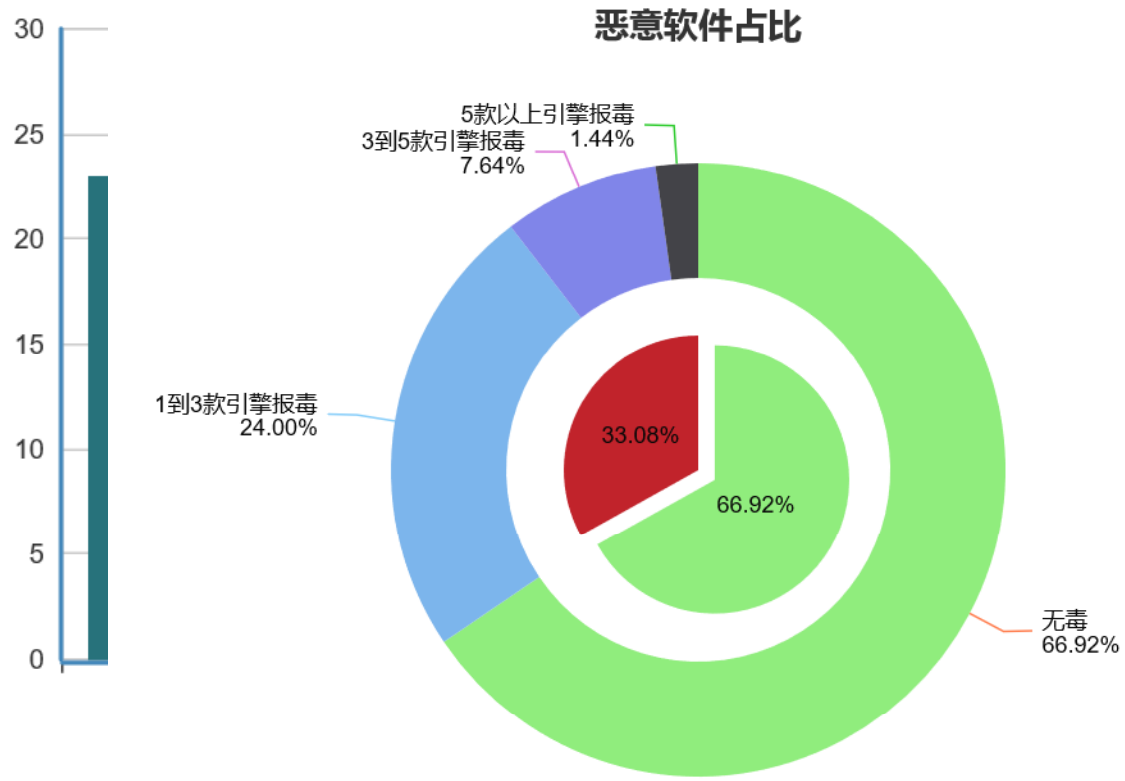

ThreatBook

# 关联



ThreatBook

# 移动互联网安全态势




杀毒引擎查杀数量

| 引擎名称 | 查杀数量 | 占比 |
|---|---|---|
| 小红伞 | 51274 | 29.71% |
| IKARUS | 17318 | 10.04% |
| 大蜘蛛 | 10428 | 6.04% |
| 百度 | 10161 | 5.89% |
| AVG | 9180 | 5.32% |
| 腾讯 | 8013 | 4.64% |
| 趋势 | 1438 | 0.83% |
| 安天 | 1293 | 0.75% |
| 金山 | 943 | 0.55% |
| 火绒 | 621 | 0.36% |
| 360 | 448 | 0.26% |

# 安全分析师

# 威胁情报分析现状

- 分析师需求增大
- 分析师人才短缺
- 缺乏高质量分析交流平台
- 缺乏优质威胁情报信息和基础资源共享
- 分析师缺乏分享动力

# 合作呼吁

- 1. 教育网威胁检测
  - 文件载体检测
  - 网络流量检测
- 2. 威胁分析师
  - 安全分析师激励计划
  - 共同培养安全分析师

ThreatBook

谢谢！

xuefeng@threatbook.cn

微信：XuefengXuefeng

欢迎关注威胁情报公众号：安全威胁情报

ThreatBook