第三届网络安全冬训营 | 朔雪飛揚

ThreatBook

安全威胁情报实战

薛锋, ThreatBook

情报的支撑 攻防的实践

内容

- 自我介绍
- 安全威胁情报
- 威胁情报分析
- 威胁情报落地

自我介绍

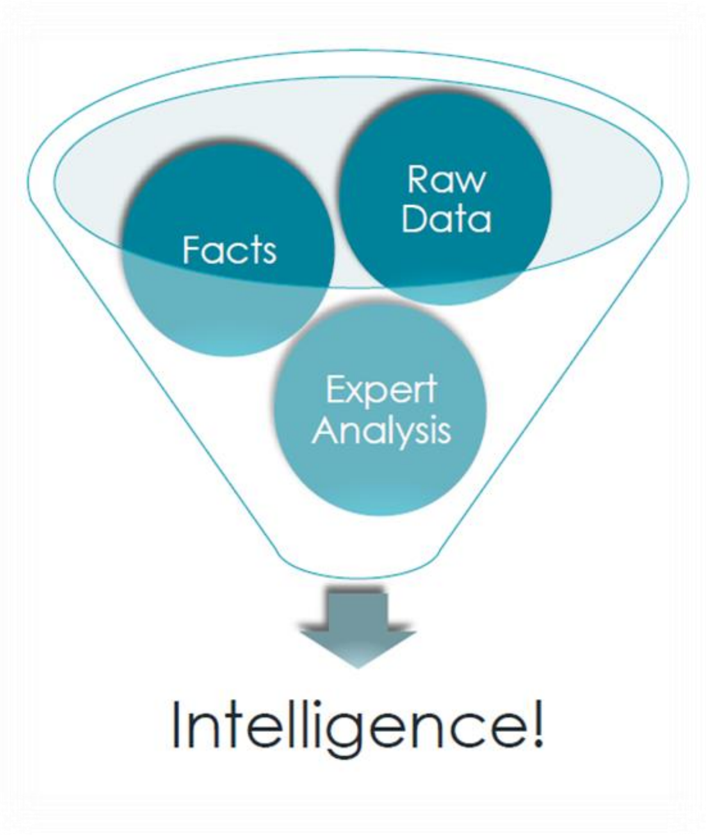
- 微步在线创始人、CEO。国内首个安全威胁情报公司
- 亚马逊中国首席安全官(CISO)
- 微软互联网安全战略总监
- 耐威实验室技术负责人
- 公安部第三研究所

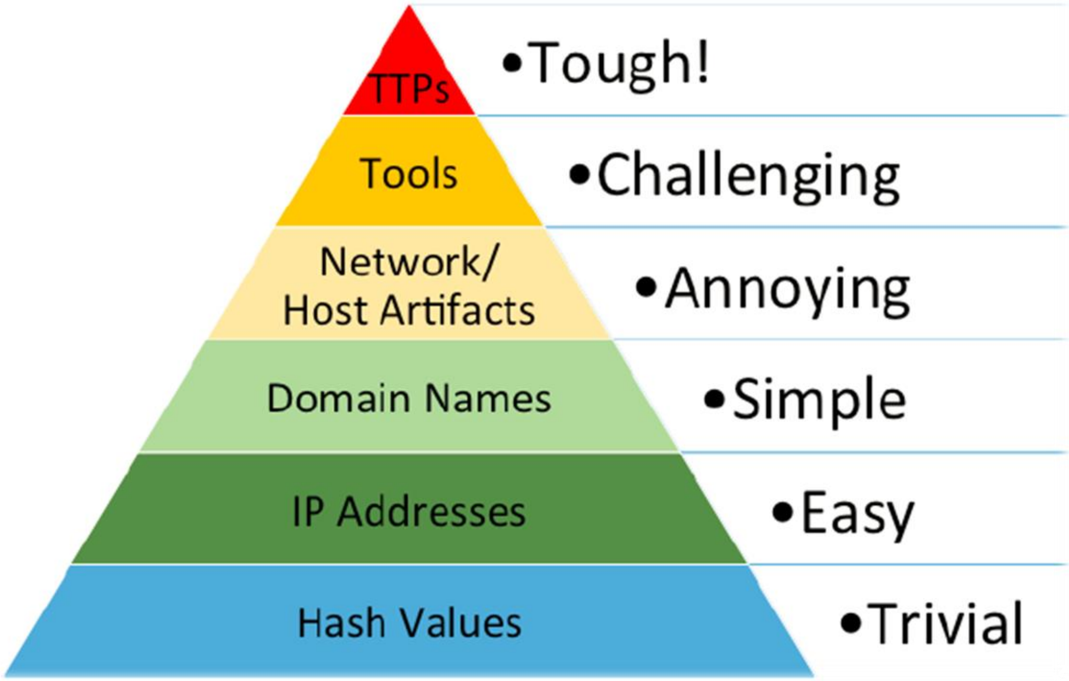
~~社工库~~

~~黑产~~

~~谍报~~

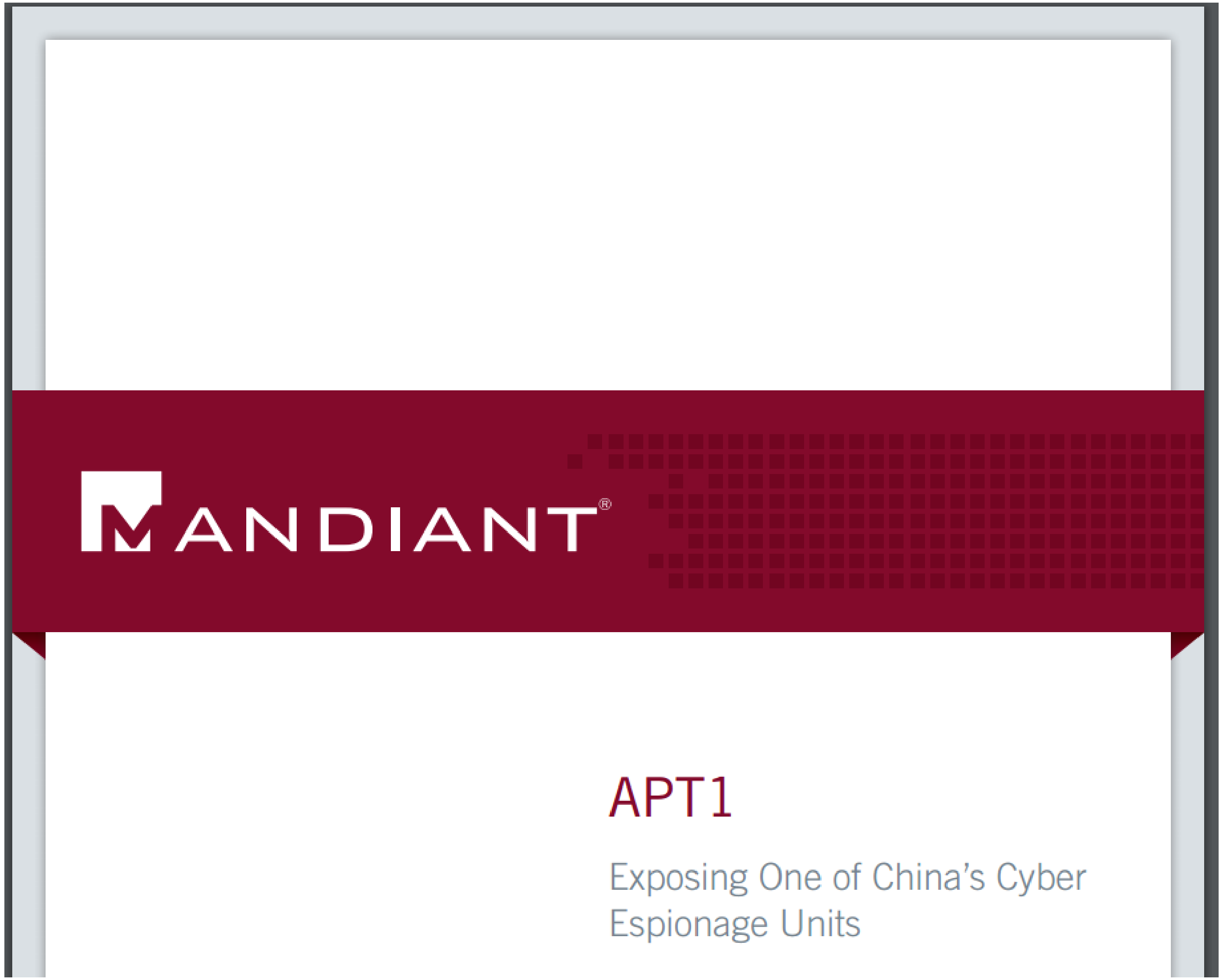
安全威胁情报





ThreatBook

实战一：APT1



MANDIANT®

APT1

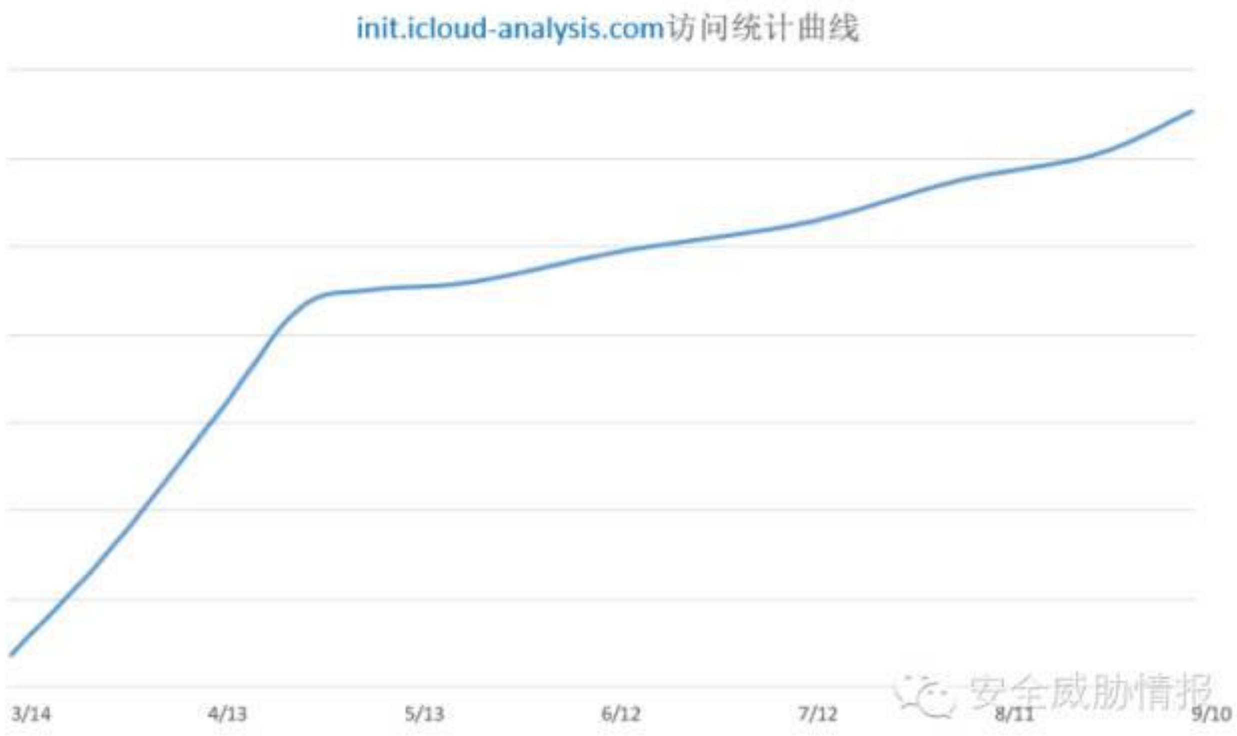
Exposing One of China’s Cyber Espionage Units

实战二：暗黑客栈

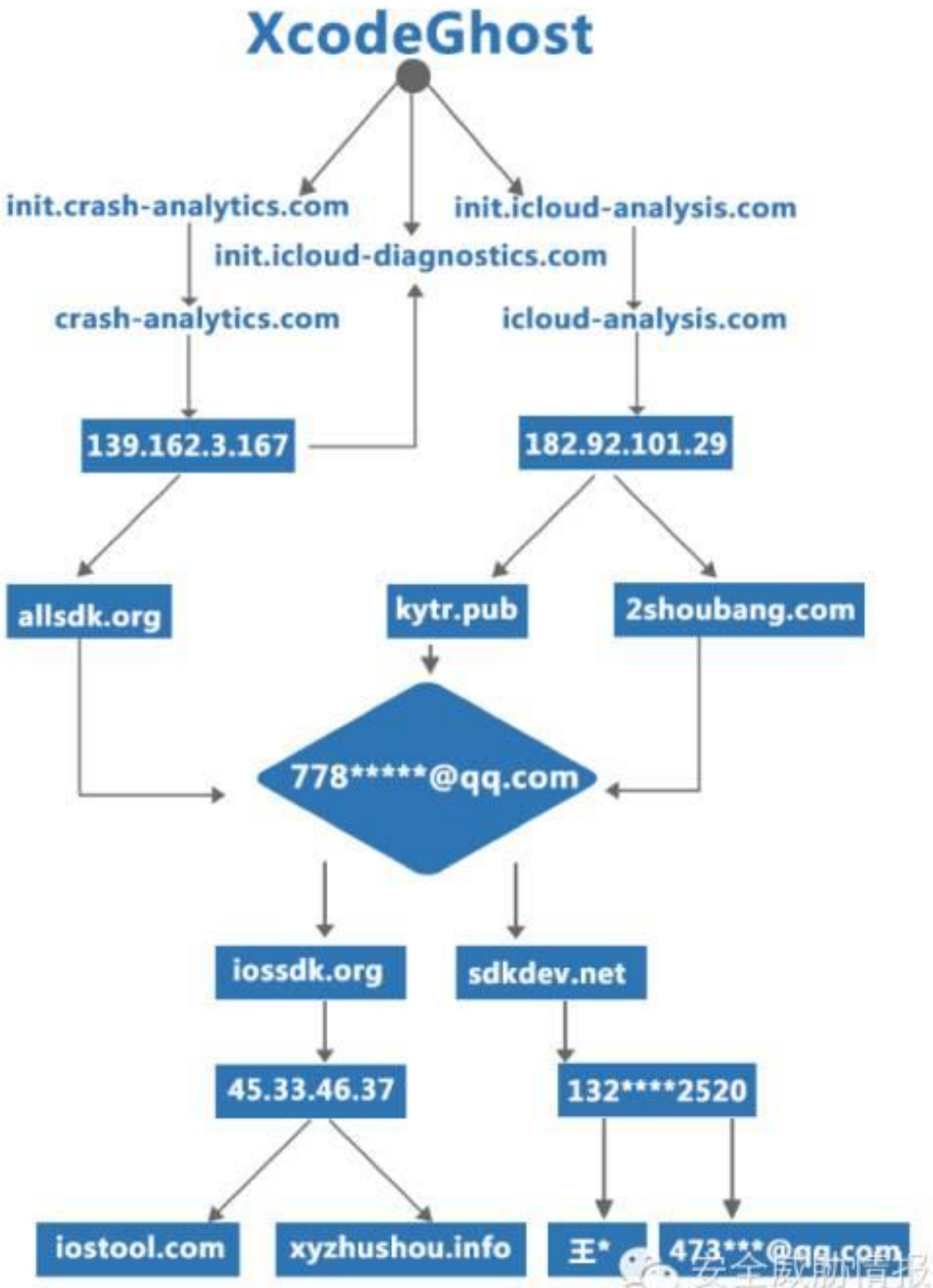
实战三：索尼

实战四：XcodeGhost

实战四：XcodeGhost



实战四：



XcodeGhost

init.crash-analytics.com

init.icloud-diagnostics.com

init.icloud-analysis.com

crash-analytics.com

icloud-analysis.com

139.162.3.167

182.92.101.29

allsdk.org

kytr.pub

2shoubang.com

778*****@qq.com

iossdk.org

sdkdev.net

45.33.46.37

132****2520

iostool.com

xyzhushou.info

王*

473***@qq.com

实战四：XcodeGhost动机

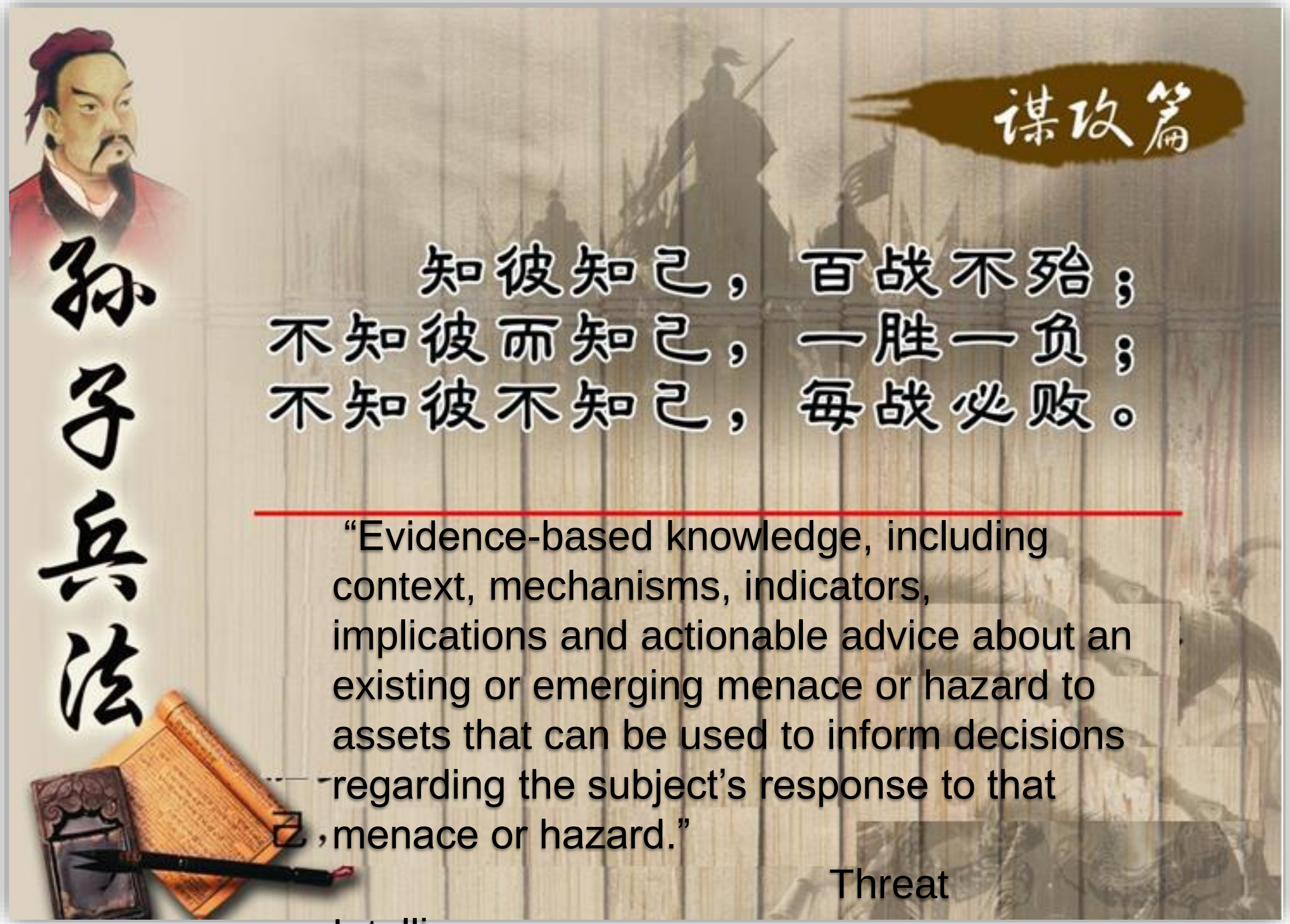
- **疑点一：XcodeGhost 与 KeyRaider 的关系**

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。

知彼、知己



知彼知己，百战不殆；
不知彼而知己，一胜一负；
不知彼不知己，每战必败。

“Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject’s response to that menace or hazard.”

Threat Intelligence

- Gartner

基础能力

数据

分析

数据收集

外部

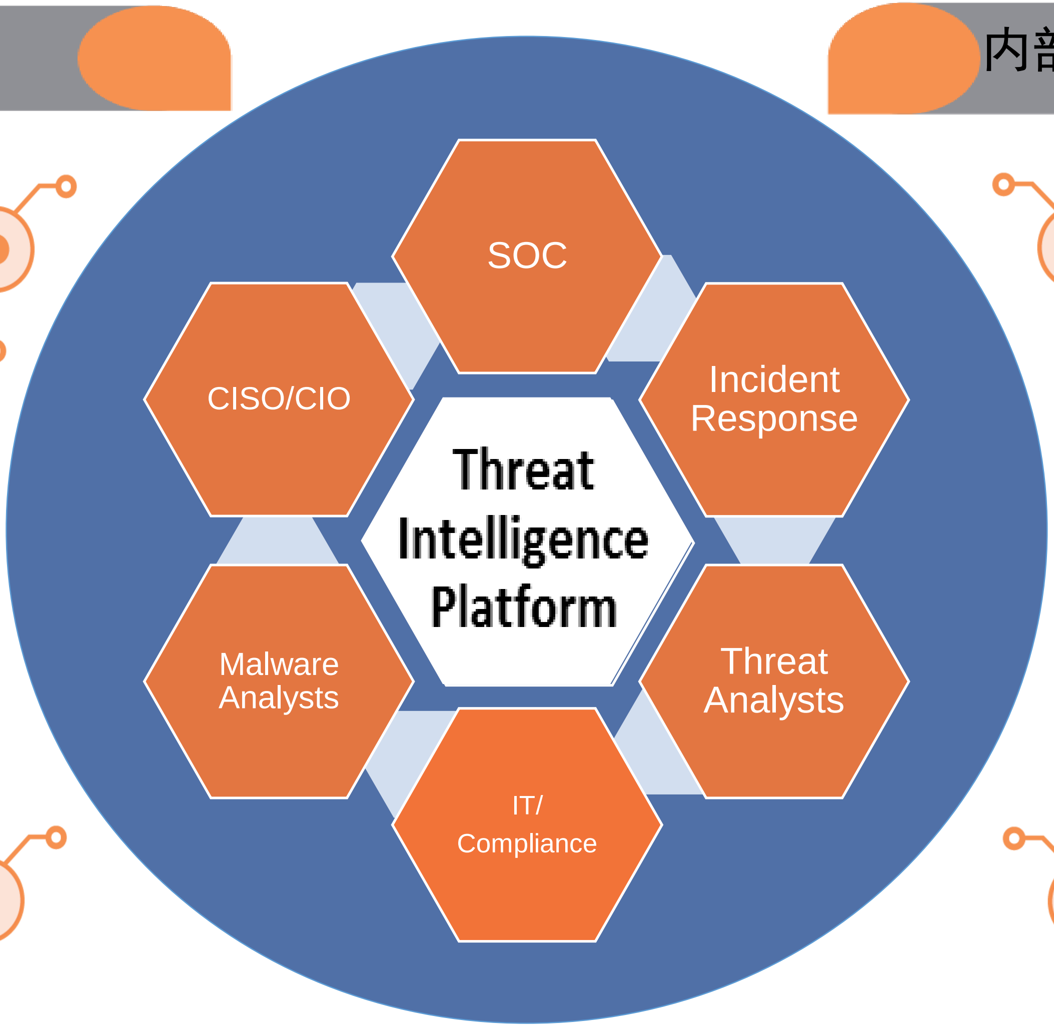
商业情报

开源情报

基础数据

众包情报

其它



内部

DNS日志

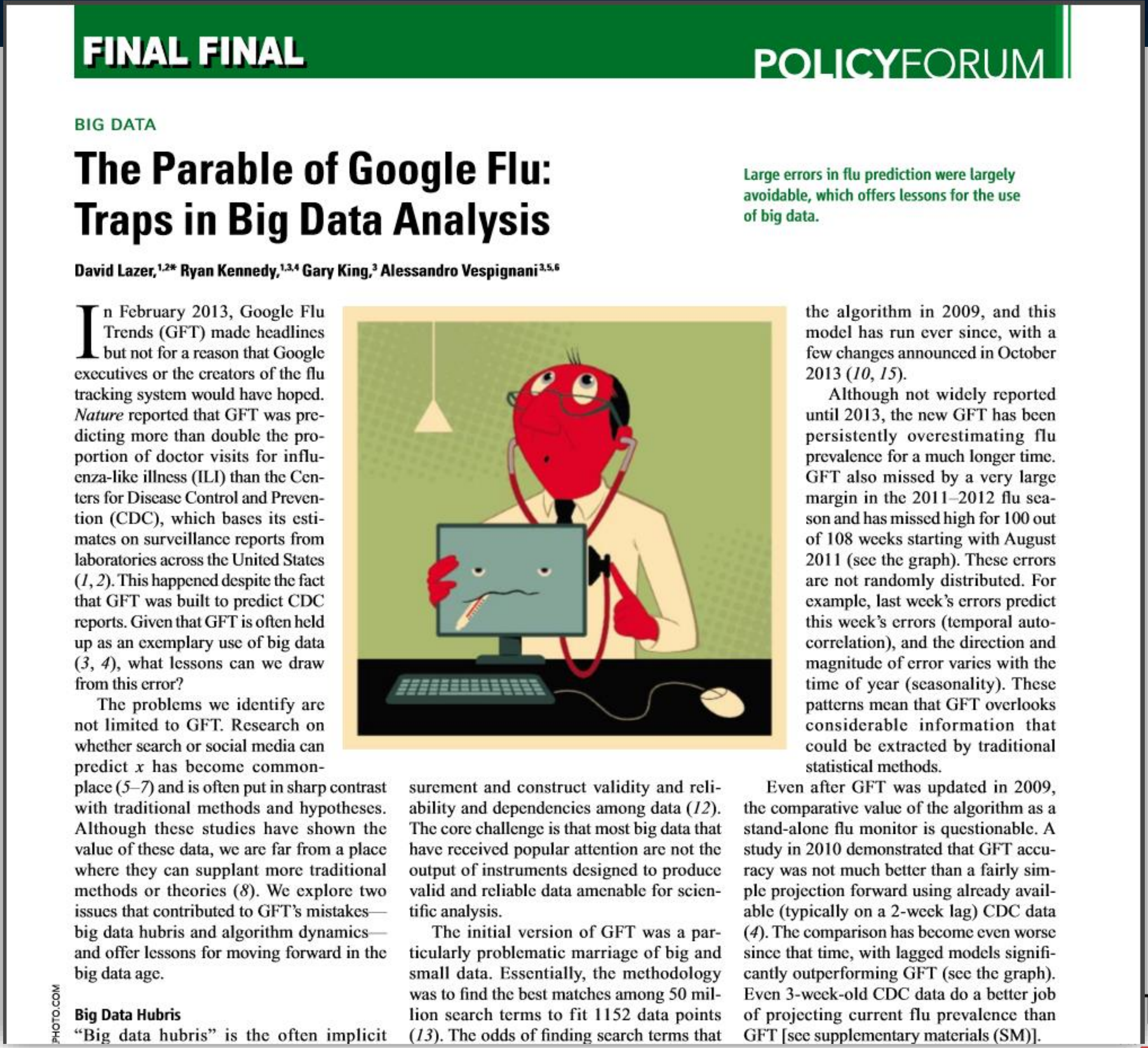
DHCP日志

防火墙日志

Windows日志

各种日志...

数据越大越好?



FINAL FINAL

POLICYFORUM

BIG DATA

The Parable of Google Flu: Traps in Big Data Analysis

Large errors in flu prediction were largely avoidable, which offers lessons for the use of big data.

David Lazer,[1,2*] Ryan Kennedy,[1,3,4] Gary King,[3] Alessandro Vespignani[3,5,6]

In February 2013, Google Flu Trends (GFT) made headlines but not for a reason that Google executives or the creators of the flu tracking system would have hoped. *Nature* reported that GFT was predicting more than double the proportion of doctor visits for influenza-like illness (ILI) than the Centers for Disease Control and Prevention (CDC), which bases its estimates on surveillance reports from laboratories across the United States (*1*, *2*). This happened despite the fact that GFT was built to predict CDC reports. Given that GFT is often held up as an exemplary use of big data (*3*, *4*), what lessons can we draw from this error?

The problems we identify are not limited to GFT. Research on whether search or social media can predict *x* has become commonplace (*5*–*7*) and is often put in sharp contrast with traditional methods and hypotheses. Although these studies have shown the value of these data, we are far from a place where they can supplant more traditional methods or theories (*8*). We explore two issues that contributed to GFT's mistakes—big data hubris and algorithm dynamics—and offer lessons for moving forward in the big data age.

PHOTO.COM

Big Data Hubris

"Big data hubris" is the often implicit

surement and construct validity and reliability and dependencies among data (*12*). The core challenge is that most big data that have received popular attention are not the output of instruments designed to produce valid and reliable data amenable for scientific analysis.

The initial version of GFT was a particularly problematic marriage of big and small data. Essentially, the methodology was to find the best matches among 50 million search terms to fit 1152 data points (*13*). The odds of finding search terms that

the algorithm in 2009, and this model has run ever since, with a few changes announced in October 2013 (*10*, *15*).

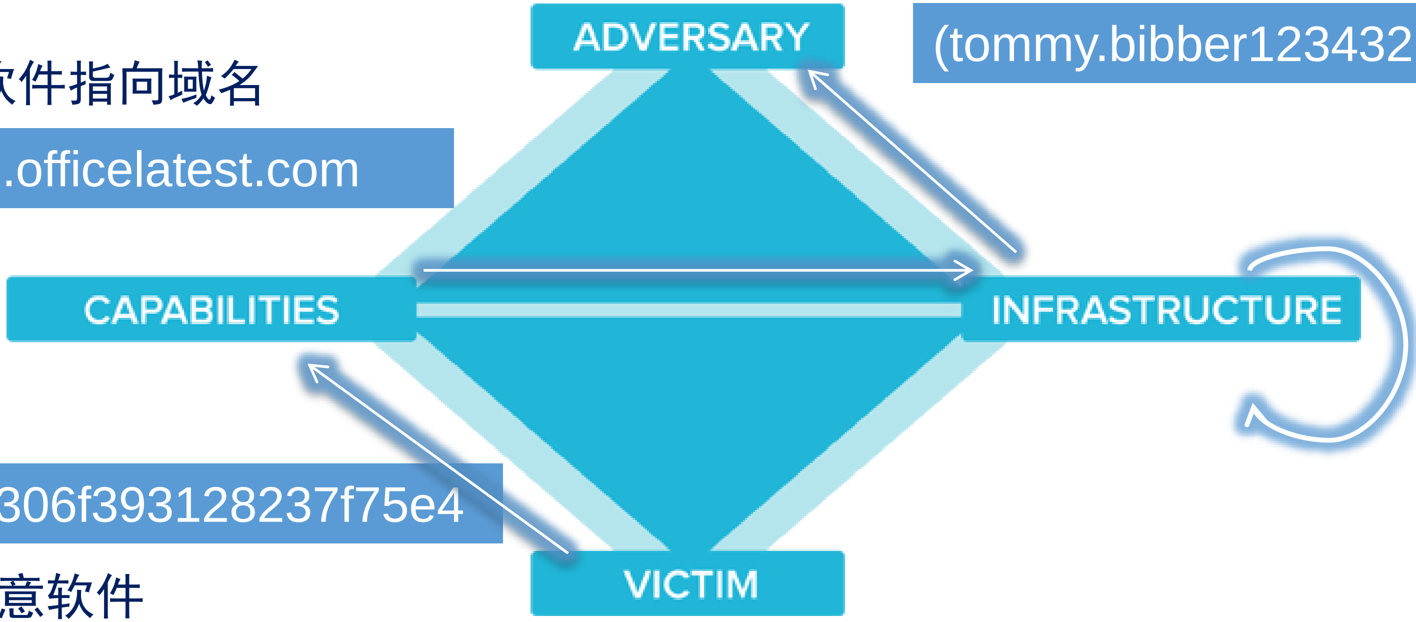
Although not widely reported until 2013, the new GFT has been persistently overestimating flu prevalence for a much longer time. GFT also missed by a very large margin in the 2011–2012 flu season and has missed high for 100 out of 108 weeks starting with August 2011 (see the graph). These errors are not randomly distributed. For example, last week's errors predict this week's errors (temporal autocorrelation), and the direction and magnitude of error varies with the time of year (seasonality). These patterns mean that GFT overlooks considerable information that could be extracted by traditional statistical methods.

Even after GFT was updated in 2009, the comparative value of the algorithm as a stand-alone flu monitor is questionable. A study in 2010 demonstrated that GFT accuracy was not much better than a fairly simple projection forward using already available (typically on a 2-week lag) CDC data (*4*). The comparison has become even worse since that time, with lagged models significantly outperforming GFT (see the graph). Even 3-week-old CDC data do a better job of projecting current flu prevalence than GFT [see supplementary materials (SM)].

分析

ThreatBook

钻石模型



(4) 谁？

(tommy.bibber1234321@ddd.com

(2) 恶意软件指向域名

info.officelatest.com

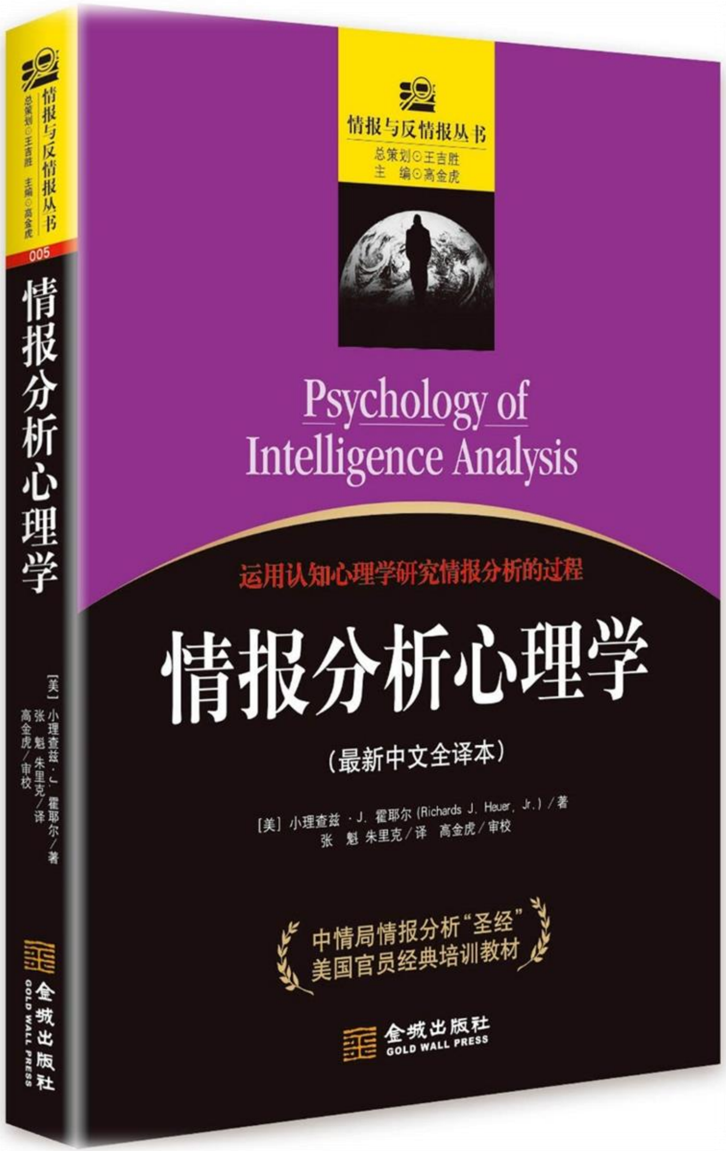
(3) C2 IP

142.91.132.23

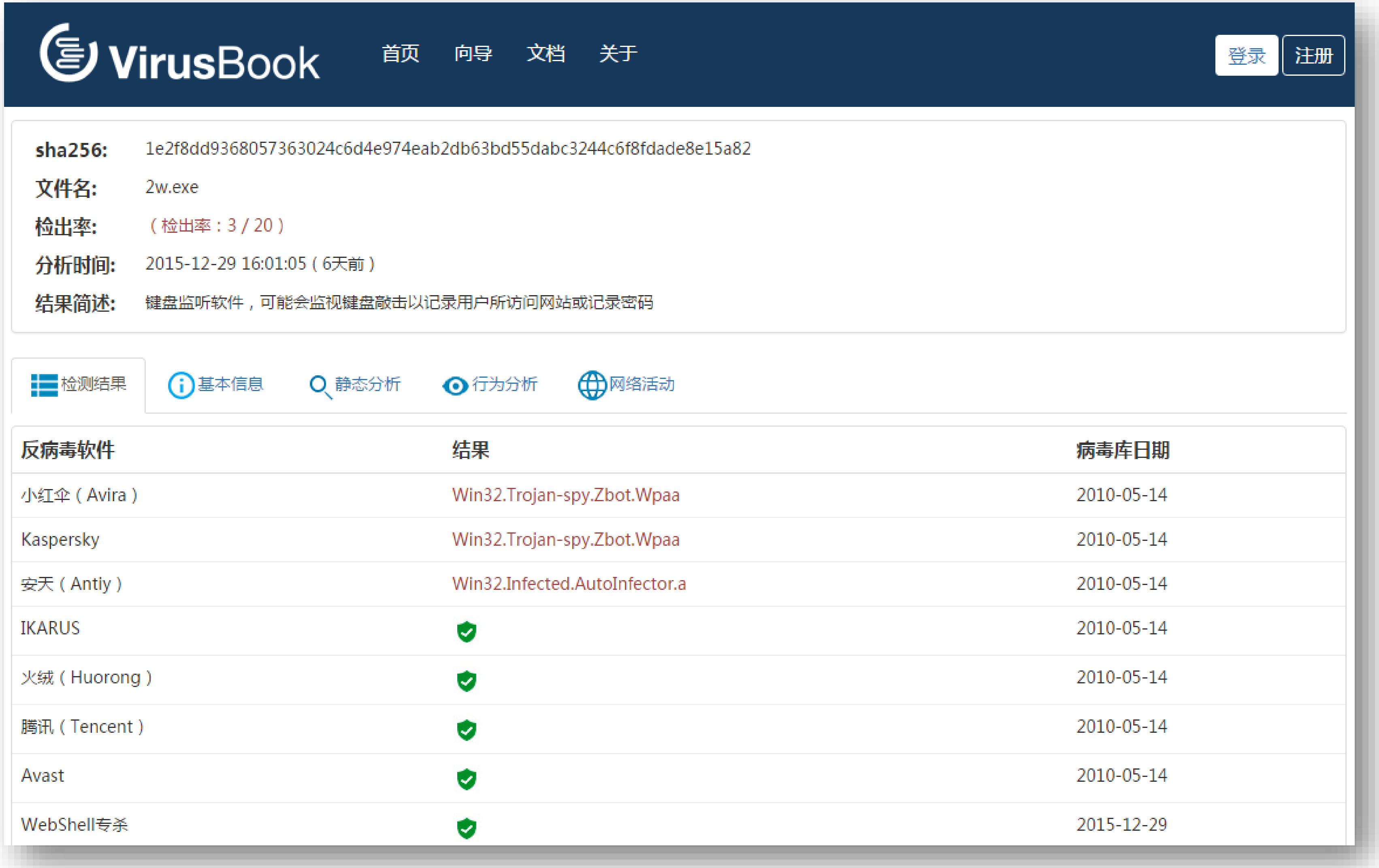
0606c10388c306f393128237f75e4

(1) 受害人发现恶意软件

分析方法论-CIA


情报与反情报丛书
总策划◎王吉胜
主 编◎高金虎
005
情报分析心理学
[美] 小理查兹·J. 霍耶尔/著
张 魁 朱里克/译
高金虎/审校
金城出版社
GOLD WALL PRESS
情报与反情报丛书
总策划◎王吉胜
主 编◎高金虎
Psychology of Intelligence Analysis
运用认知心理学研究情报分析的过程
情报分析心理学
（最新中文全译本）
[美] 小理查兹·J. 霍耶尔 (Richards J. Heuer, Jr.) / 著
张 魁 朱里克 / 译 高金虎 / 审校
中情局情报分析“圣经”
美国官员经典培训教材
金城出版社
GOLD WALL PRESS

威胁分析



sha256: 1e2f8dd9368057363024c6d4e974eab2db63bd55dabc3244c6f8fdade8e15a82

文件名: 2w.exe

检出率: （检出率：3 / 20）

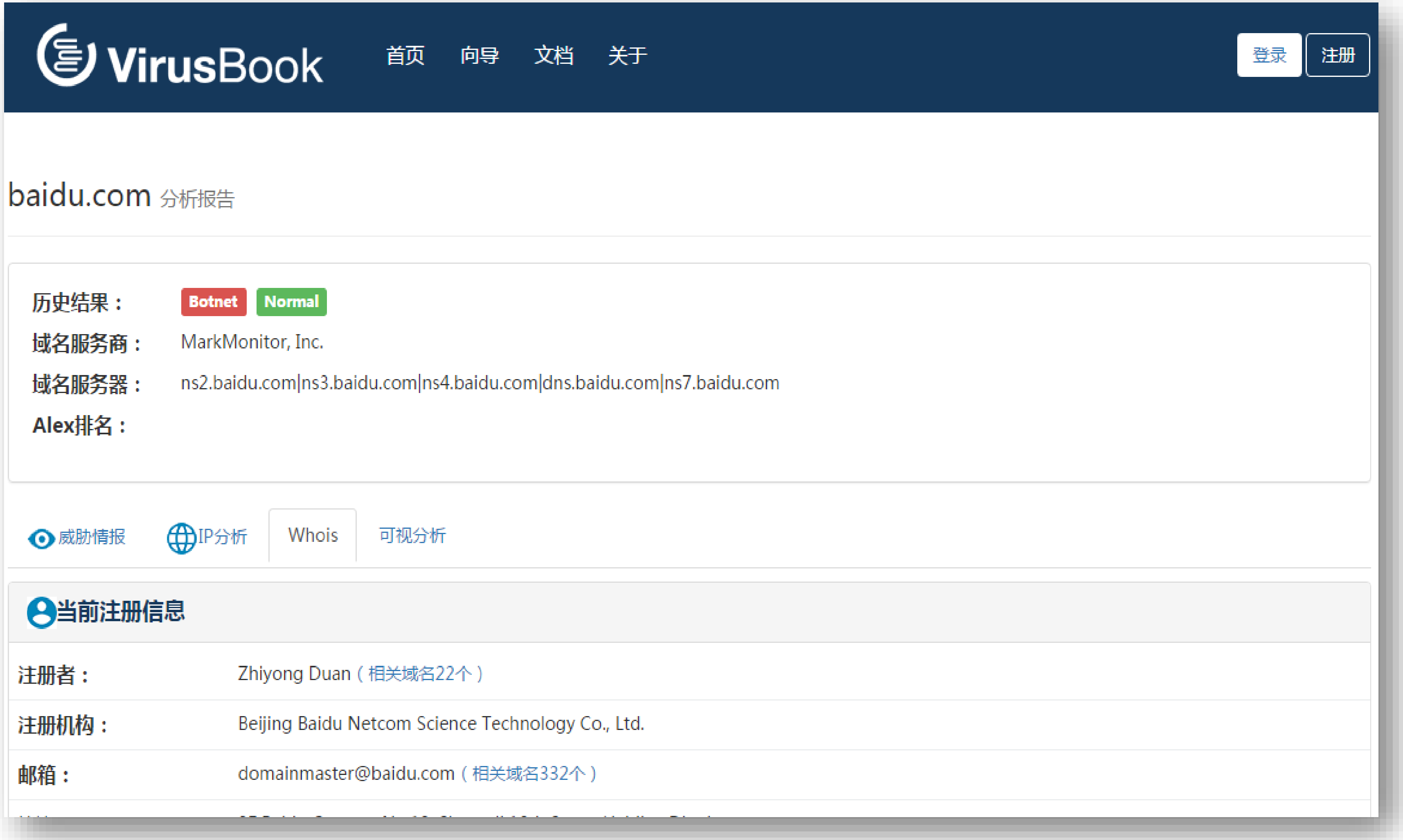
分析时间: 2015-12-29 16:01:05（6天前）

结果简述: 键盘监听软件，可能会监视键盘敲击以记录用户所访问网站或记录密码

反病毒软件	结果	病毒库日期
小红伞（Avira）	Win32.Trojan-spy.Zbot.Wpaa	2010-05-14
Kaspersky	Win32.Trojan-spy.Zbot.Wpaa	2010-05-14
安天（Antiy）	Win32.Infected.AutoInfector.a	2010-05-14
IKARUS	✓	2010-05-14
火绒（Huorong）	✓	2010-05-14
腾讯（Tencent）	✓	2010-05-14
Avast	✓	2010-05-14
WebShell专杀	✓	2015-12-29

ThreatBook

威胁分析



baidu.com 分析报告

历史结果： Botnet Normal

域名服务商： MarkMonitor, Inc.

域名服务器： ns2.baidu.com|ns3.baidu.com|ns4.baidu.com|dns.baidu.com|ns7.baidu.com

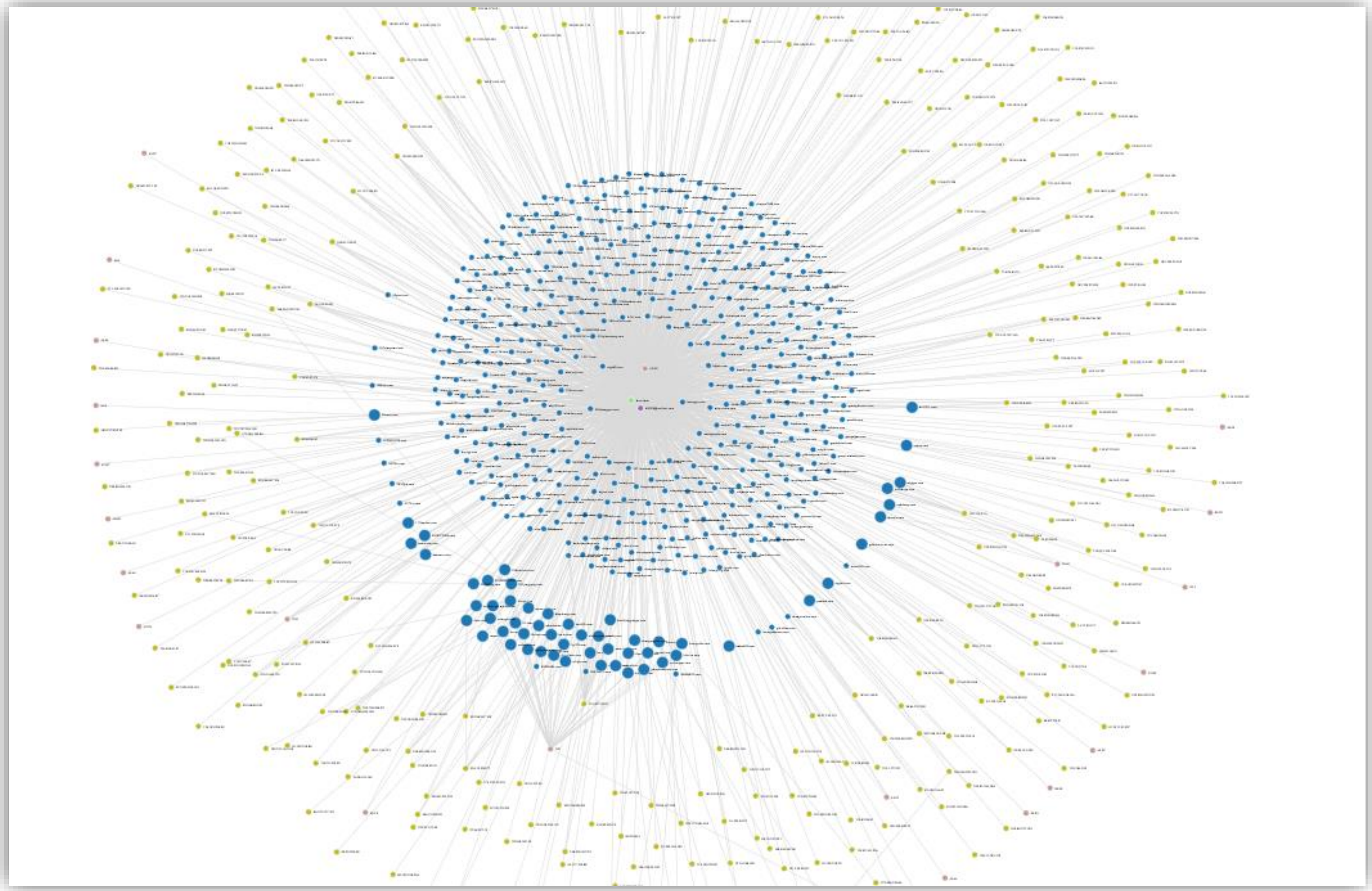
Alex排名：

当前注册信息

注册者：	Zhiyong Duan（相关域名22个）
注册机构：	Beijing Baidu Netcom Science Technology Co., Ltd.
邮箱：	domainmaster@baidu.com（相关域名332个）

ThreatBook

可视化关联分析

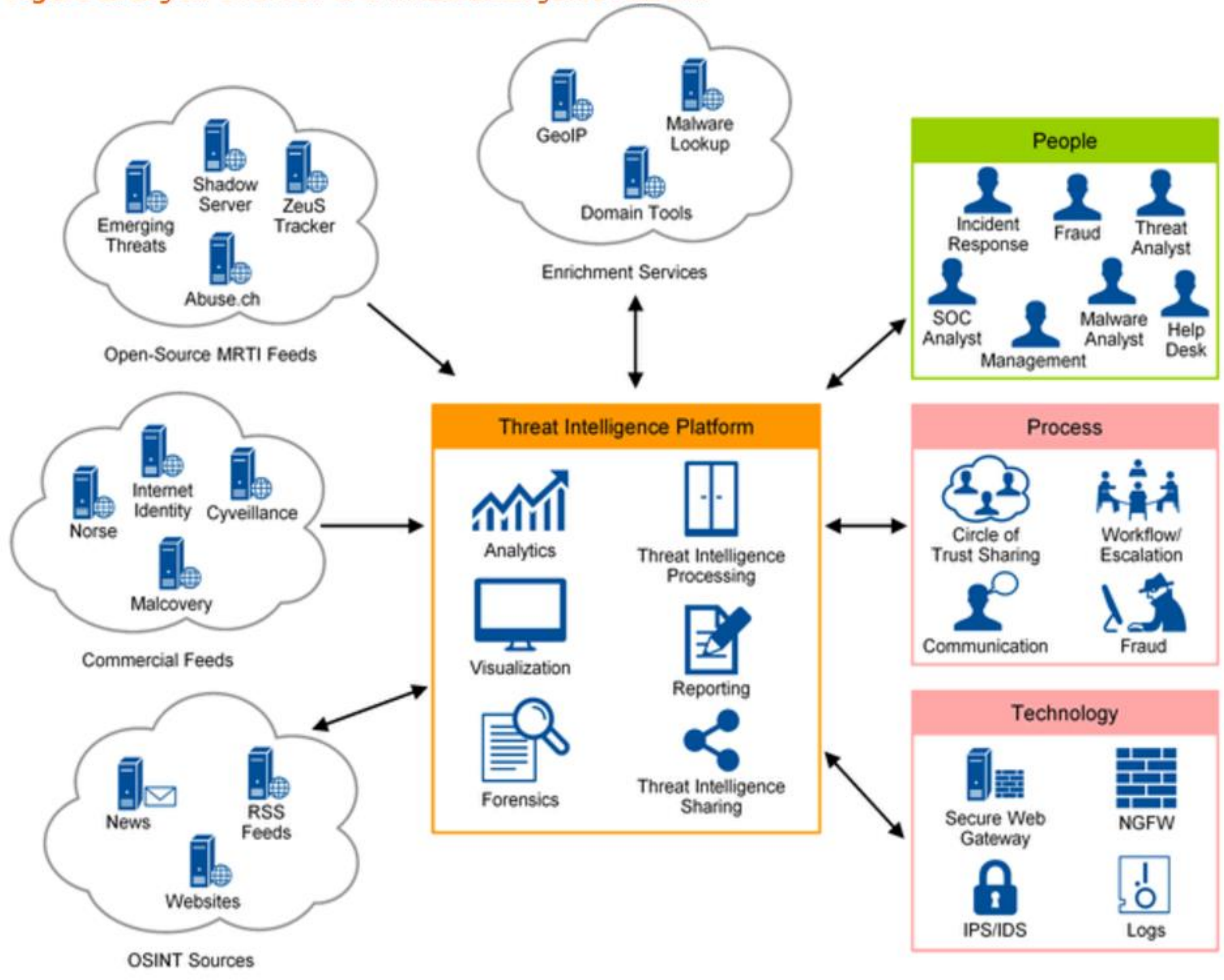


安全分析师

ThreatBook

落地

Figure 1. Logical Overview of a Threat Intelligence Platform



Source: Gartner (December 2014)

谢谢！

Email: xuefeng@threatbook.cn

微信：xuefengxuefeng