



AVAR 2012

HANG ZHOU

Hangzhou JW Marriott Hotel
November 12-14 2012

15th Association Of Anti Virus Asia Researchers
International Conference



提纲

- APT时代的来临
- 回看传统反病毒
- APT给AVER的困扰点
- 应对以及尝试
- APT检测我们还有很多路要走
- 结束

历史事件对比

APT时代的来临



时间对比（蠕虫时代）

病毒名称	释放时间	发现时间
CodeRedII	2001年8月3日	2001年8月3日
冲击波(Blaster)	2003年8月11日	2003年8月12日
震荡波(Sasser)	2004年4月30日	2004年5月1日
Zotob	2005年8月13日	2005年8月16日
Nyxem	2006年1月20	2006年2月3日

时间对比 (APT时代)

病毒名称	释放时间	发现时间
Stuxnet	2009年6月	2010年7月
Duqu	2007年或2008年 ?	2011年8月
Flame	2007年12月之前 ?	2012年5月

Flame

- 模块编译时间2006年，第一个关联域名注册于2007年，模块 WAVESUP3.DRV2007-12-5在欧洲Webroot社区被发现。

Duqu

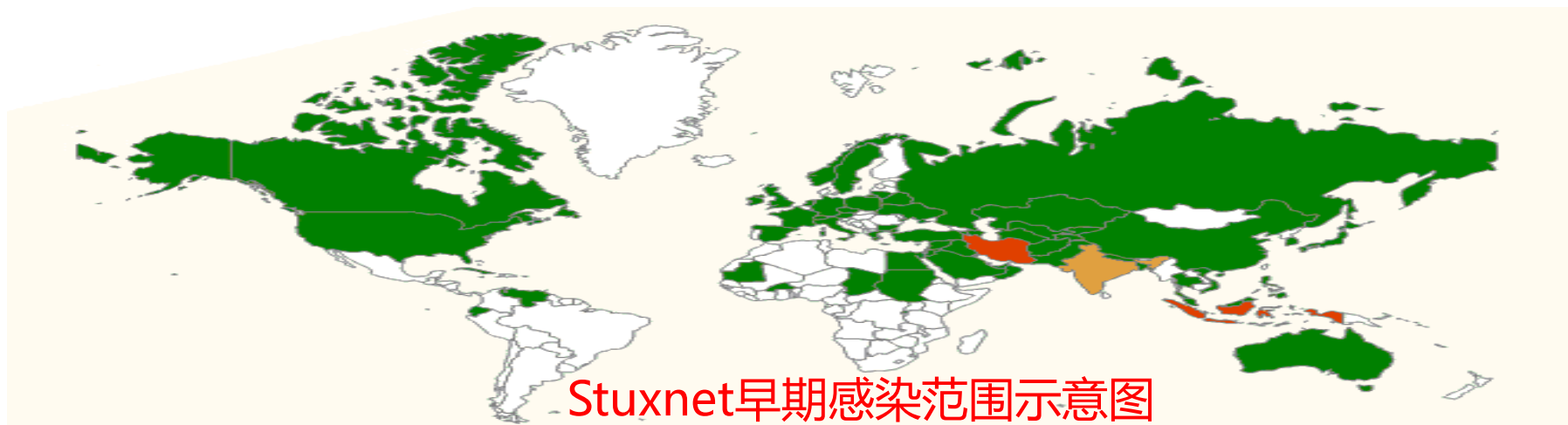
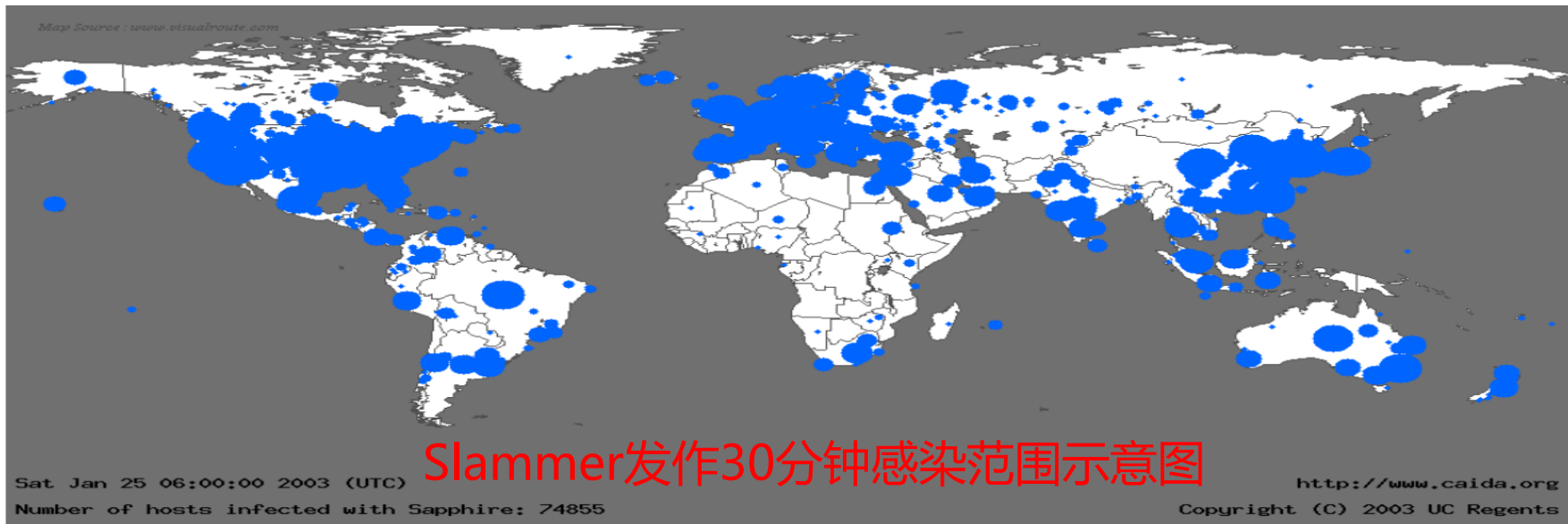
- Duqu中发现多个模块的编译时间为2010-3-11，但有其他事件佐证在2008年甚至更早已经出现。

Stuxnet

- 根据时间戳等信息认为初始时间为2009年6月

疑似事件链

地点对比（蠕虫时代和APT定向性）



“人物”对比（病毒与传统攻击）



病毒：CIH
人物：陈盈豪



病毒：Sasser
人物：Sven Jaschan

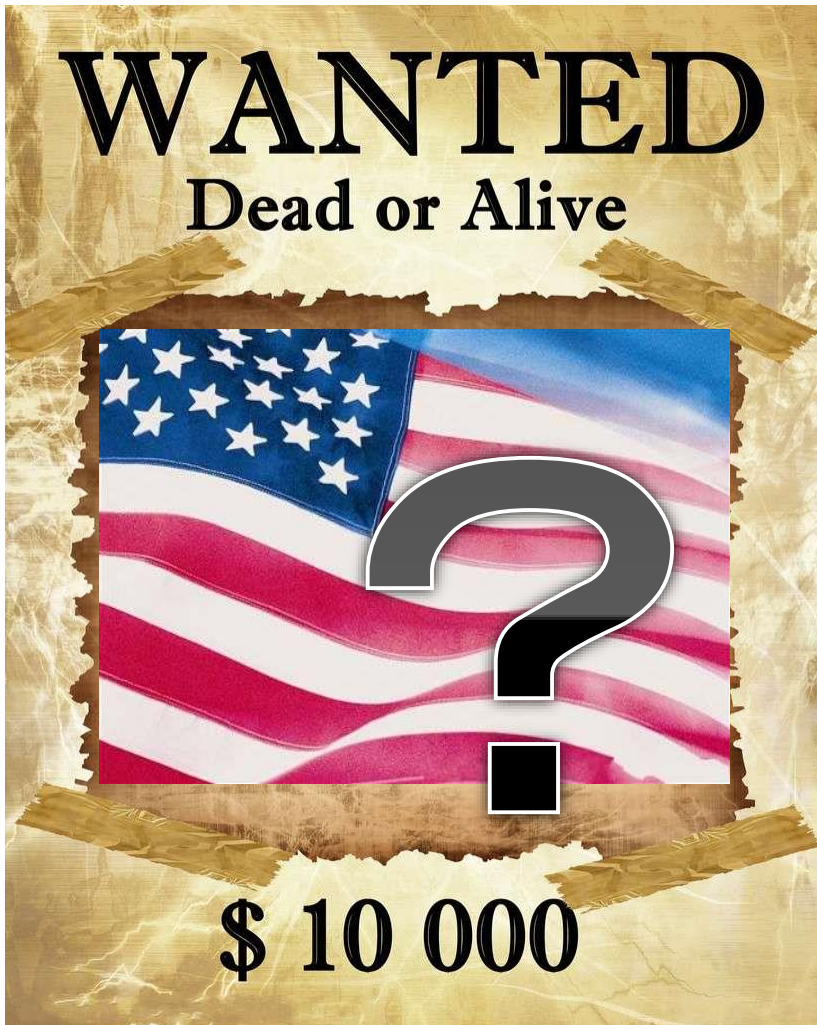


病毒：DNSChanger
人物：Tsatsin



病毒：Mariposa
人物：Iserdo

“人物”对比(APT)



传统反病毒相关说明

回看传统反病毒



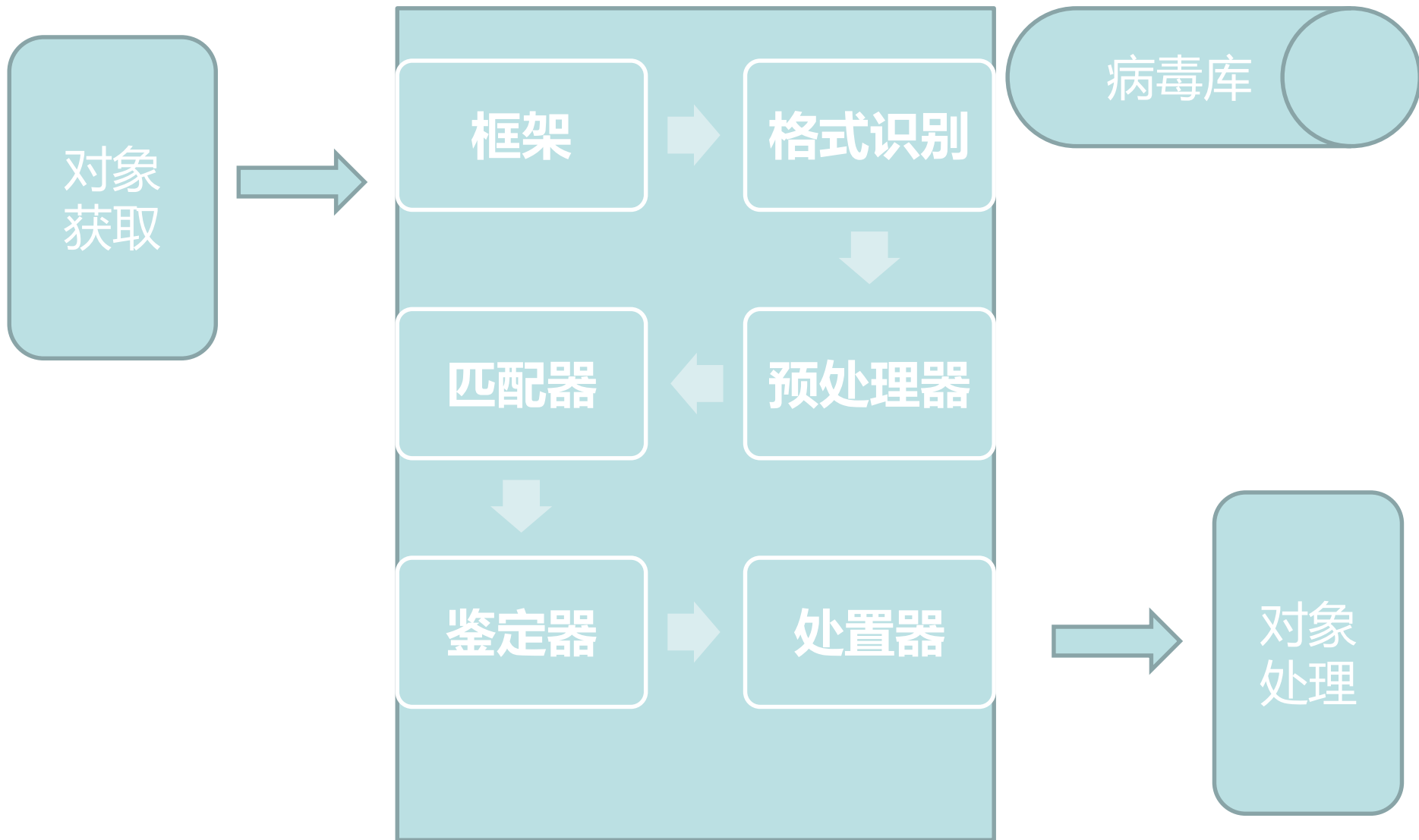
架构的形成（一）

	优点	缺点
样本交换	数量大、质量高	不及时，一些公司比较保守。
用户上报/自动上报	数量大、可能获得流行样本	质量不高，有大量非病毒文件
现场/定向采集	可能获得流行样本	需要特定机会
主动收集	数量较大、质量高	需要人工处理。
流量采集	第一时间捕获传输蠕虫	数量小，代价大
honeypot采集	第一时间捕获扫描蠕虫	数量较小，代价大

架构的形成（二）

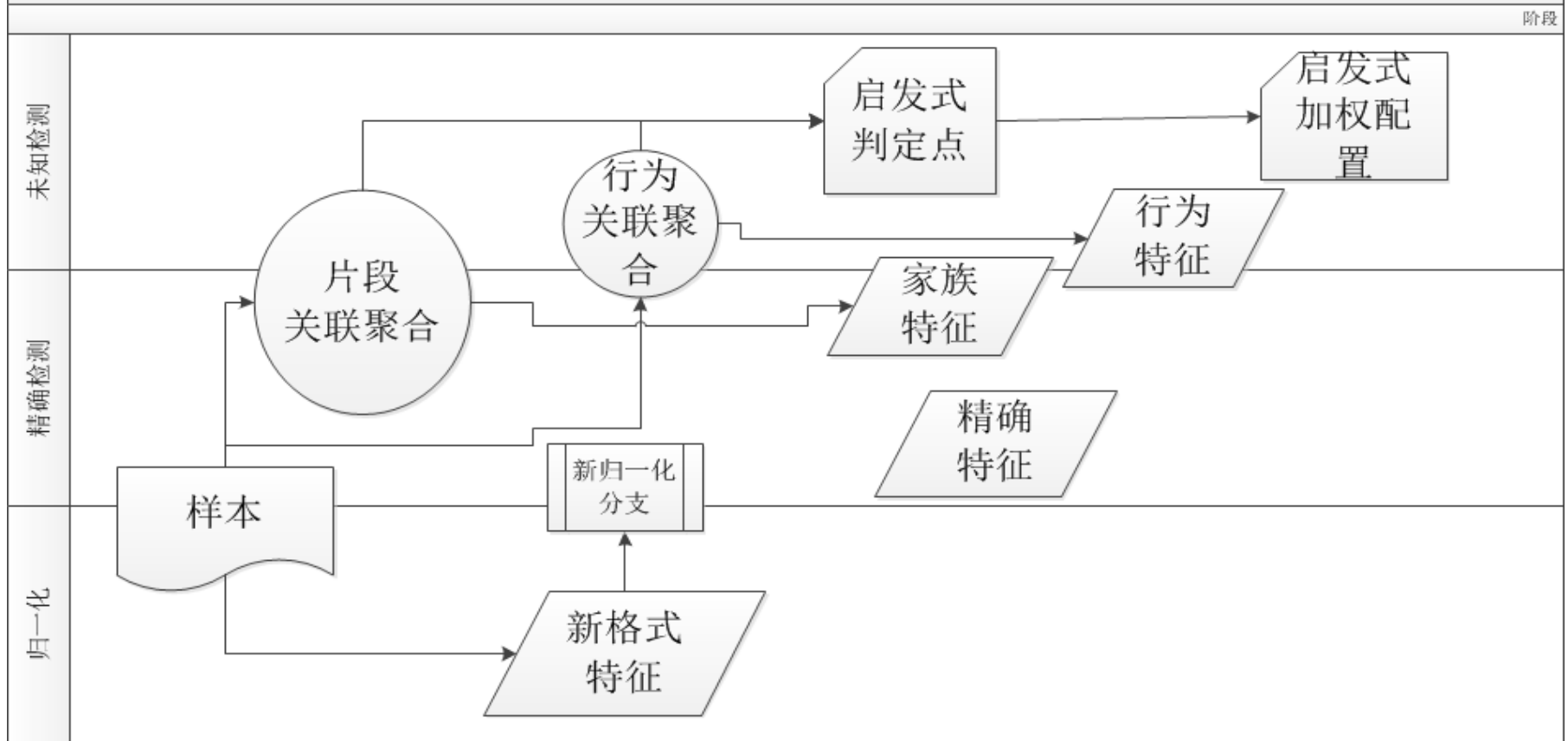
	来源类型	实时性	全面性	完整性	准确性
用户上报	不可控	中	差	差	差
兄弟企业样本交换	不可控	差	好	好	好
现场采集	不可控	中	差	好	中
网站主动收集	不可控	中	差	好	好
诱饵信箱	可控	中	差	中	好
蜜罐系统	可控	好	差	中	好

传统反病毒机理的模型抽象



传统反病毒的模型维护

反病毒引擎核心维护机理示意图




传统反病毒并非一个只有捕获、提取、检测的单循环体制
其自身就有未知检测工作反而被公众忽略

传统反病毒的真正软肋

562 software downloads results for "antivirus"

1 2 3 4 ... 57 Next >

▼ Sponsored match



Vipre Antivirus 2013
Version 6.0 | Added on 09/26/2012

Protect yourself against viruses and malware threats without slowing down your PC.

381,564 total downloads 2,064 last week

User rating
out of 189 reviews


★★★★☆

[Download Now](#)

[Buy Now](#)

[Save to list](#)

▼ Sponsored match



Trend Micro Titanium Maximum Security 2013
Version 6.0.1215 | Added on 09/10/2012

Stop viruses and spyware automatically before they reach your computer.

[Read CNET's review](#)

147,171 total downloads 1,594 last week

Editors' rating
★★★★★

User rating
out of 79 reviews


★★★★☆

[Download Now](#)

[Buy Now](#)

[Save to list](#)

▼ Sponsored match



acdONE Antivirus + Total Security
Version 15.0.33.1409 | Added on 04/03/2012

Protect your computer from emerging e-threats.

6,325 total downloads 383 last week


User rating
out of 2 reviews

★★★★★

[Download Now](#)

[Save to list](#)

▼ Sponsored match



G Data InternetSecurity 2013
Version 2012 | Added on 07/19/2012

Protect your PC against Trojans, viruses, and all kinds of malware.

1,806 total downloads 600 last week

User rating
out of 2 reviews


★★★★★

[Download Now](#)

[Buy Now](#)

[Save to list](#)

▼ Sponsored match



Avast Free Antivirus
Version 7.0.1466 | Added on 08/21/2012

Protect your PC against the latest viruses and spyware.

[Read CNET's review](#)

216,605,103 total downloads 1,290,195 last week

Editors' rating
★★★★★

User rating
out of 23648 reviews

★★★★★

[Download Now](#)

[Save to list](#)



SHA256: 70d030e233bf740f22fc0f934b9eb1bf360bcef47a21b0b6f00a3d3a37690d4a

File name: 1F61D280067E2564999CAC20E386041C

Detection ratio: 37 / 44

Analysis date: 2012-10-20 01:57:09 UTC (0 分钟 ago)

[More details](#)

Analysis [Comments](#) [Votes](#) [Additional information](#)

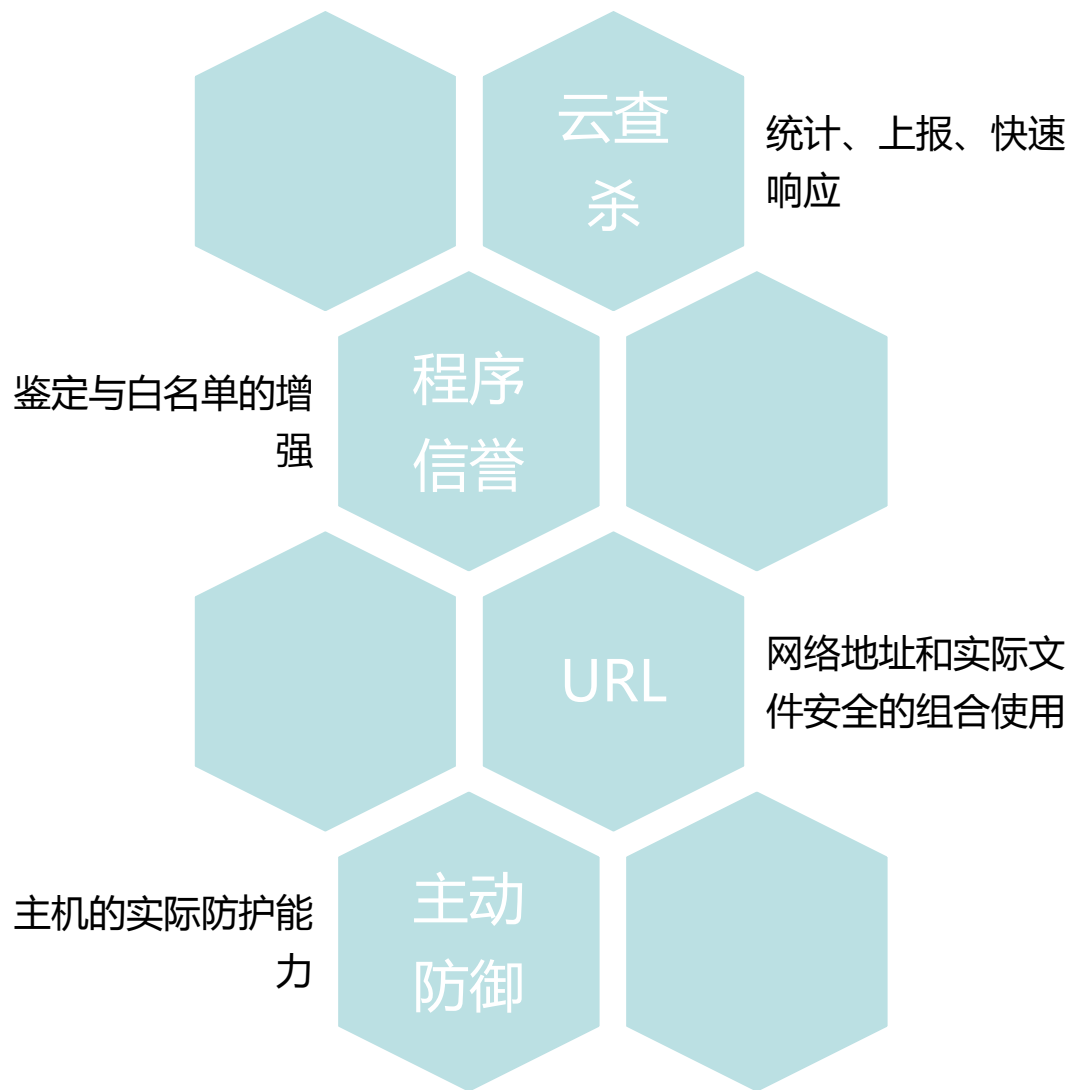
Antivirus	Result	Update
Agnitum	Worm.Flamer17+VSA4dkgdk	20121019
AhnLab-V3	Win32/Flame.worm.29928	20121019
AntiVir	TR/ATRAPS.Gen	20121020
Antiy-AVL	Worm/Win32.Flame.gen	20121020
Avast	Win32:Skywiper-N [Trj]	20121019
AVG	Worm/Flame.A	20121020
BitDefender	Trojan.Flame.A	20121019
ByteHero	-	20121019
CAT-QuickHeal	-	20121019
ClamAV	-	20121019
Commtouch	-	20121020

AV-一种易于获得的安全资源

多引擎扫描工程上已经非常成熟



进步与慌乱

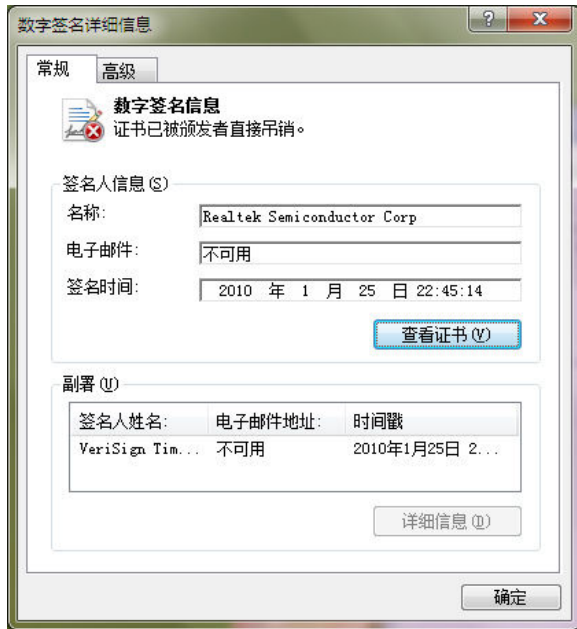


APT融合了病毒相关设计及攻击方法与一身

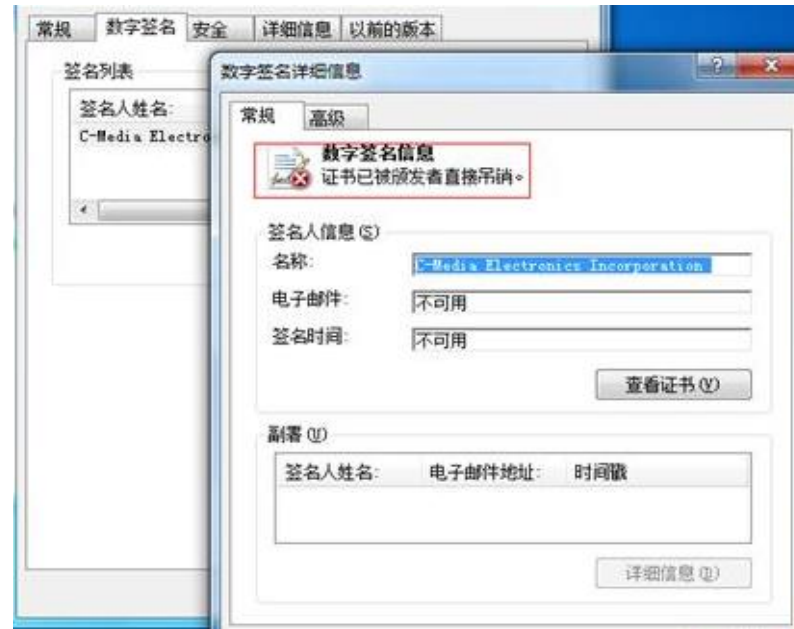
APT给AVER的困扰点

APT颠覆之模型

- APT攻击的不仅是反病毒的技术链条，更是整个信息安全体系的分工模式



Stuxnet



Duqu

APT颠覆之捕获



捕获体系之外??

APT颠覆之隐私

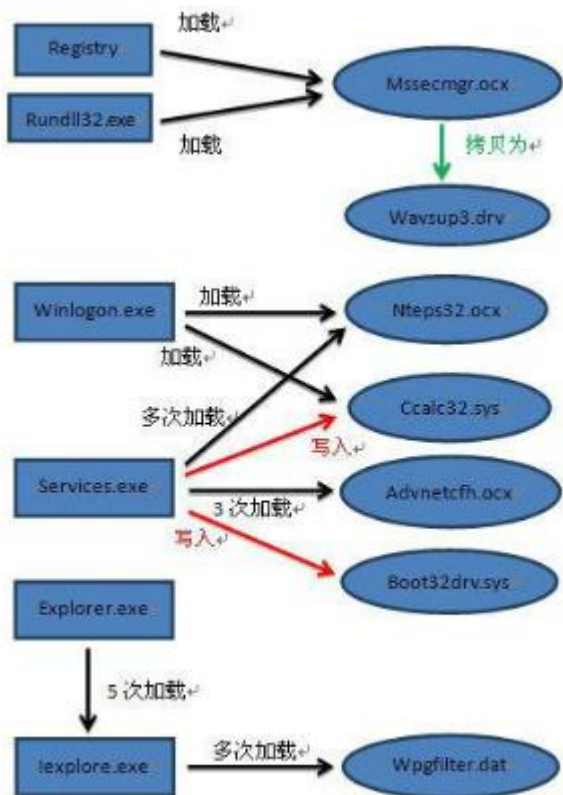
- 当APT以格式溢出为前导...



2011年发生了“RSA Secur ID被窃取”的事件中，黑客发送了名为“2011 Recruitment plan(2011年招聘计划)”的邮件给RSA员工，该邮件附带了一个名为“2011 Recruitment plan.xls”的附件，该附件利用了一个Adobe解析Flash文件格式的漏洞。当它被打开时触发了相应的漏洞，然后执行相应的恶意的代码。

APT颠覆之代价

- 曾经我们认为恶意代码是短小精悍的



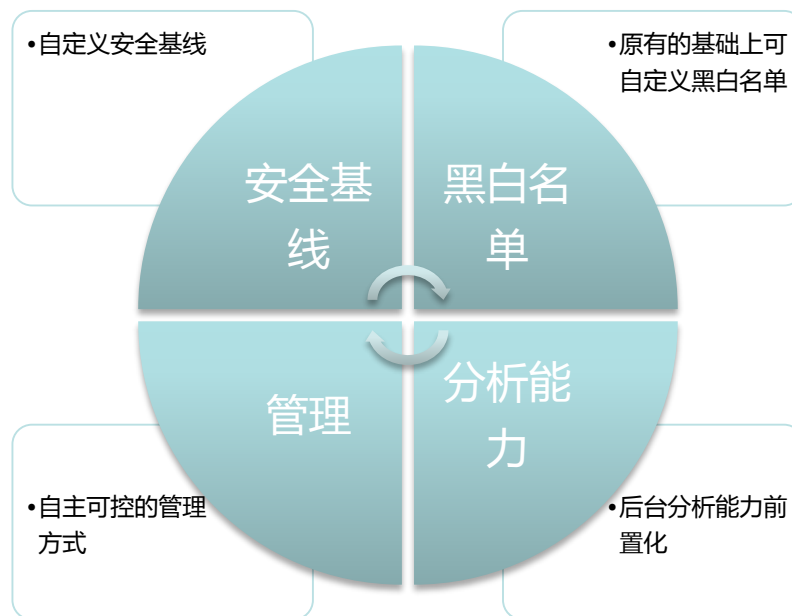
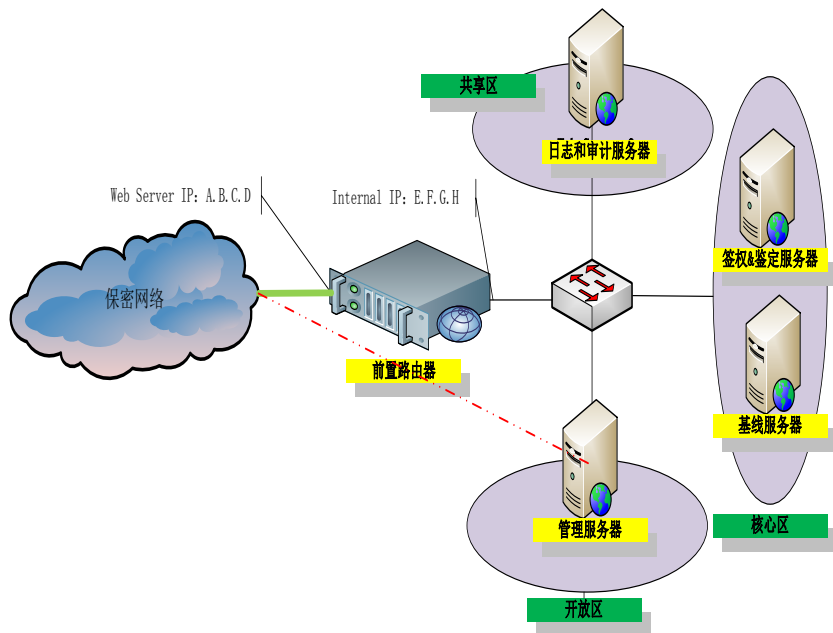
Falme模块共有20M大小，其中包括了大量的函数库，用来处理SSL流量，SSH链接，嗅探，攻击和拦截通讯等。我们用了几个月的时间分析Stuxnet仅500K大小的文件，那么我们需要用几年的时间去完全明白Flame 20M大小的文件？-- 卡巴斯基《Flame病毒问答》

在病毒检测体系上的改进

应对以及尝试

分析能力前置化

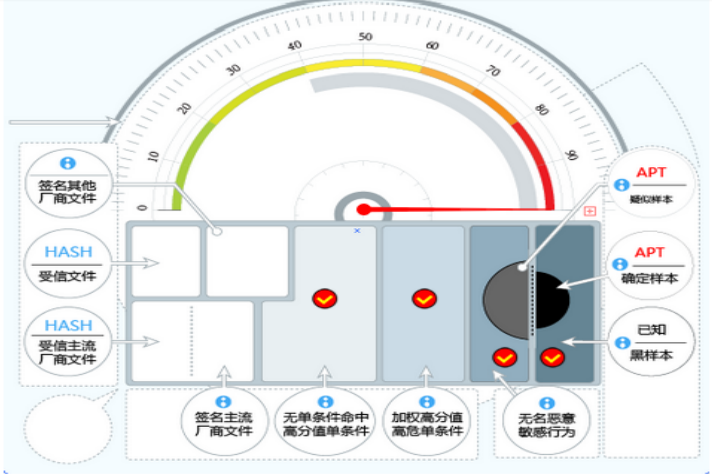
- 私有云平台，具备后台同等的自动化分析能力



判定信息详细化

- 多重的判定信息便于用户的决策

基本信息 检测模块判定 详细结果 静态启发 衍生文件



基本信息(BASEINFO)
Format Name: BinExecute / Microsoft.PE[:X86]
Format ID: 22
Pack Name: Packer_Compression/Dwing.UPACK[:v0.3x]
Pack ID: 1225

详细结果

模块名称	模块缩写	病毒ID	病毒名称
最终检测结果	MALWARE	1204130	Trojan/Win32_OnLineGames.qzh[GameThief]
感染式病毒检测	INFECT	-	-
通用特征检测	ATBM	2242724	Trojan/Win32_WOW.gic[GameThief]
木马检测	ATROJAN	1204130	Trojan/Win32_OnLineGames.qzh[GameThief]
格式漏洞检测	AEXPLOIT	-	-
脚本检测	ASCRIP	-	-
静态启发式检测	VCSII	3357027	VCS/Environment.DigitalFN.a
木马检测5	ATROJANS	-	-

分析手段层次化

- 动、静态信息统计

- 基因特征 str : cmd /c api:deletefile

- Action:delfself

- 不同层次

- 创建文件，创建PE文件，创建DLL文件，创建名字为abc.dll的文件

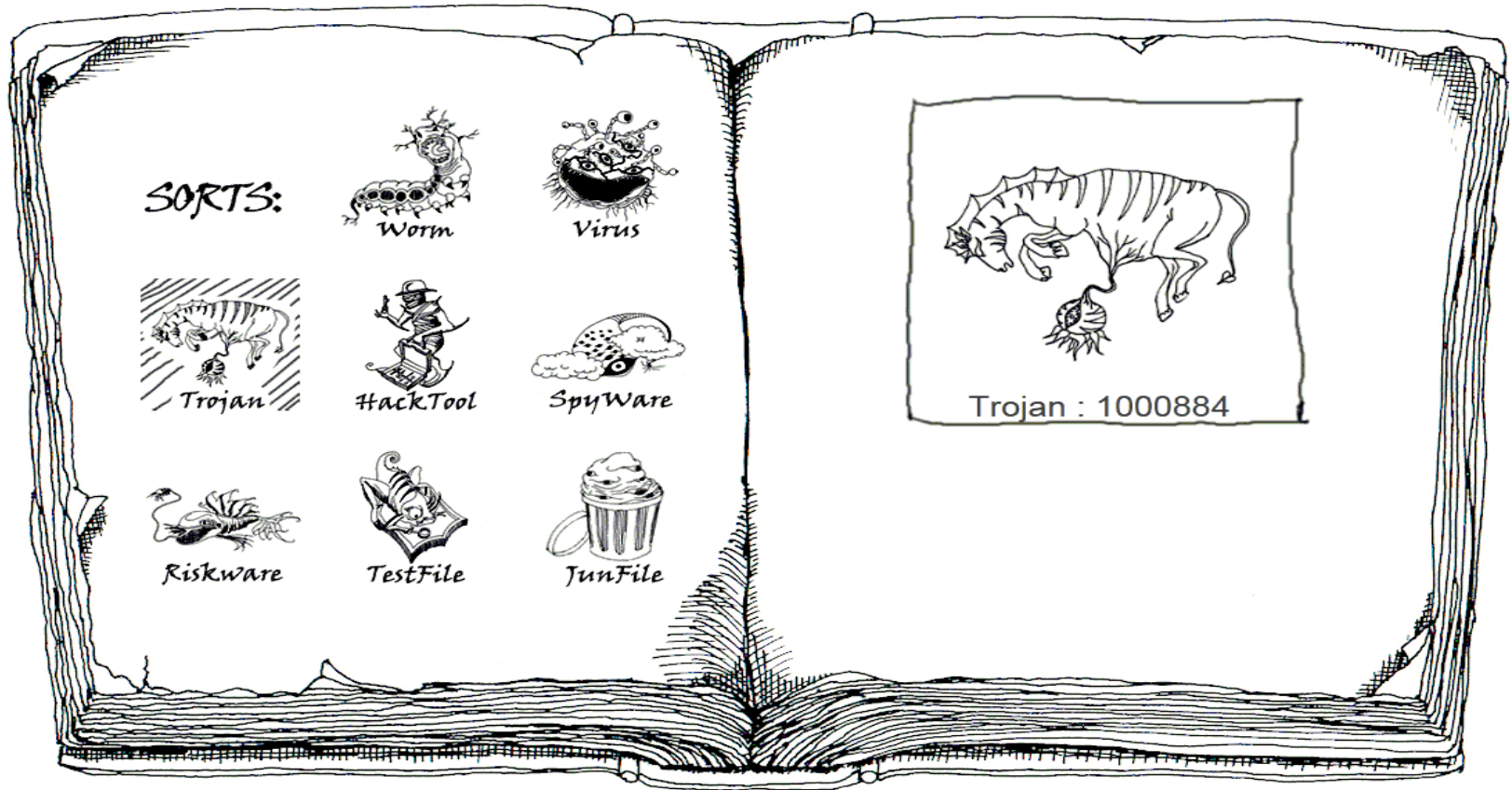
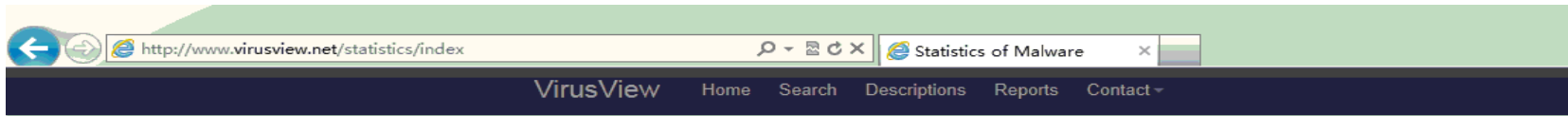
- 黑白样本集合中的概率

- 概率表明覆盖面积

- 黑白概率差异表明基因的权重

$$G = \begin{cases} \frac{P_b - P_w}{P_b + P_w}, & P_w \\ \frac{P_b - P}{P_b - P} & P... \end{cases}$$

病毒档案的建立与教训



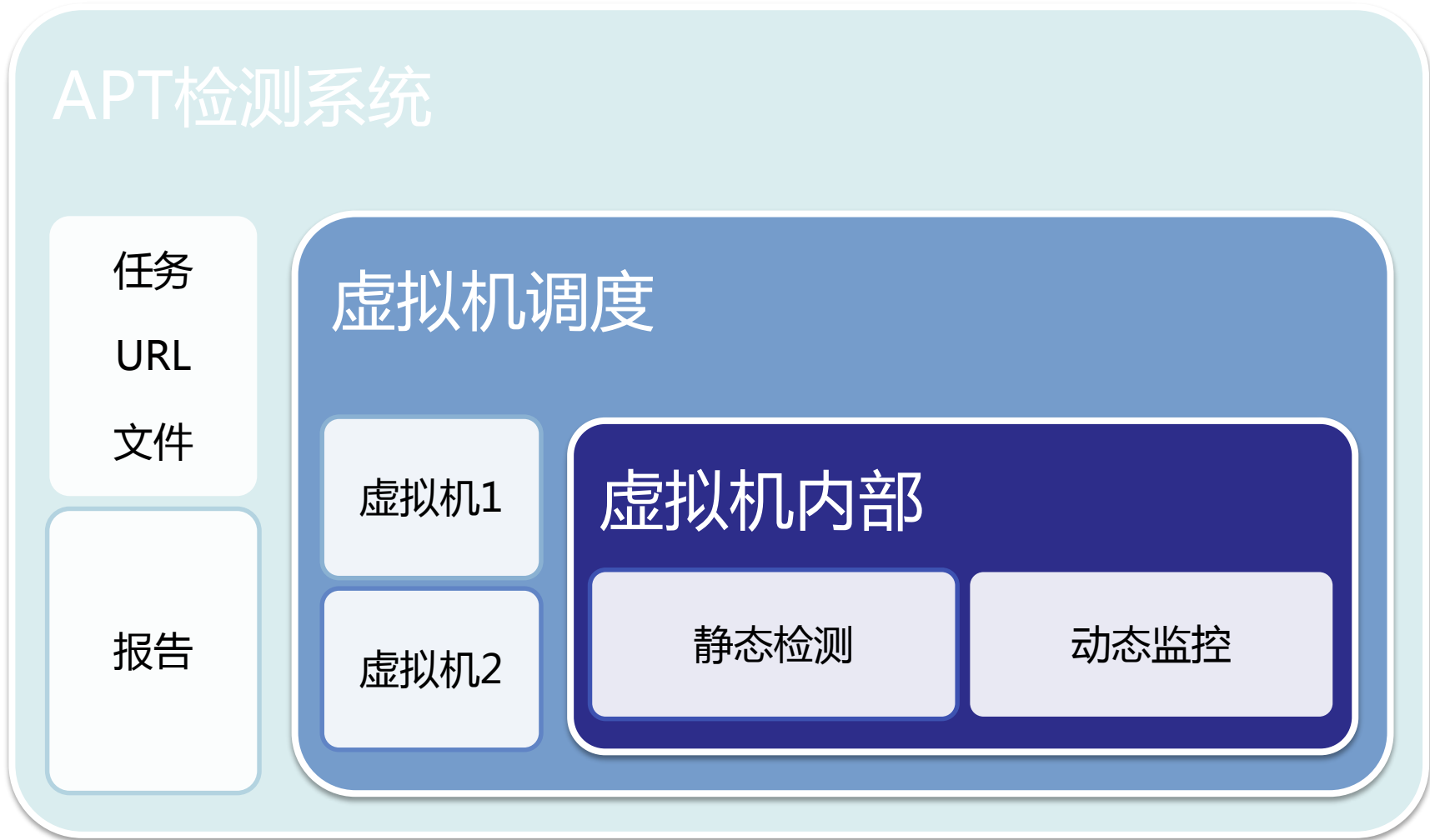
对于检测方法上的尝试

APT检测我们还有很多路要走

APT样本检测



检测系统调度架构



核心模块

监控
进程

衍生
进程

系统
进程

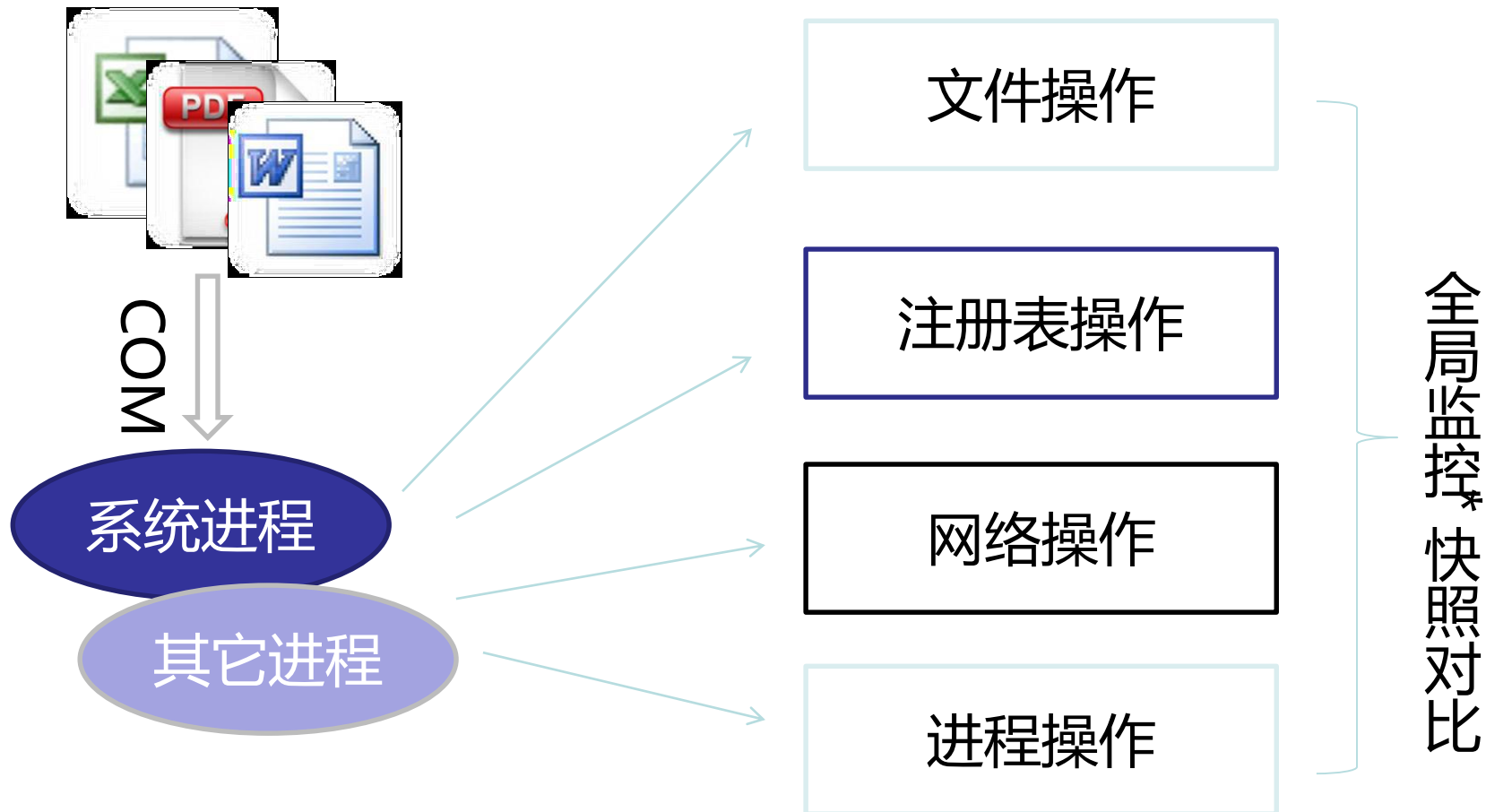
RING3

环境
模拟

Ring0 SSDT TDI 反探测

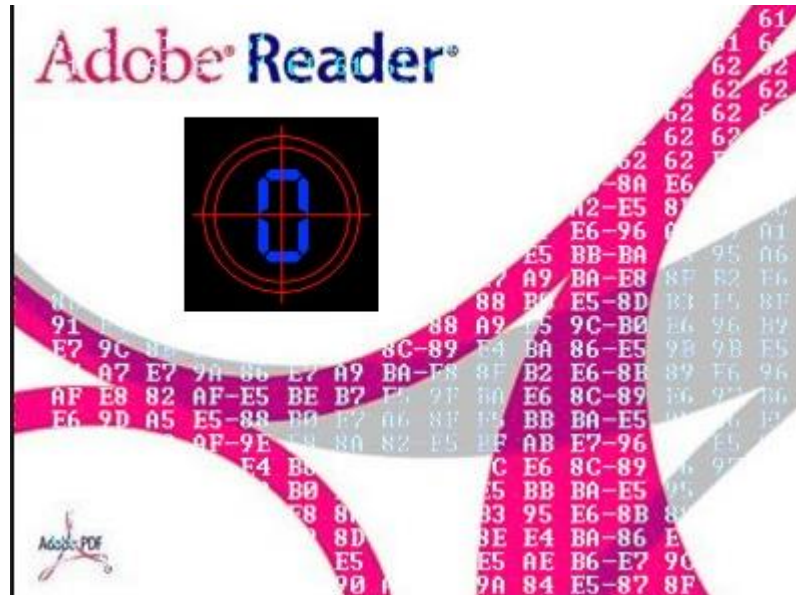


WMI 监控



静态检测

- 格式解析
- 黑白判断
- 决策树
- Shellcode发现
- 堆喷射
- 字符串信息
- 漏洞检测



数据结果分析



转换出更有价值的信息

- 关联分析

- 删除文件->删除自身
- 注册表某位置->启动项
- 创建文件->自复制

- 事件序列

- 创建文件,创建服务,驱动还原
SSDT ->穿主动防御

- 知识库

- 恶意URL

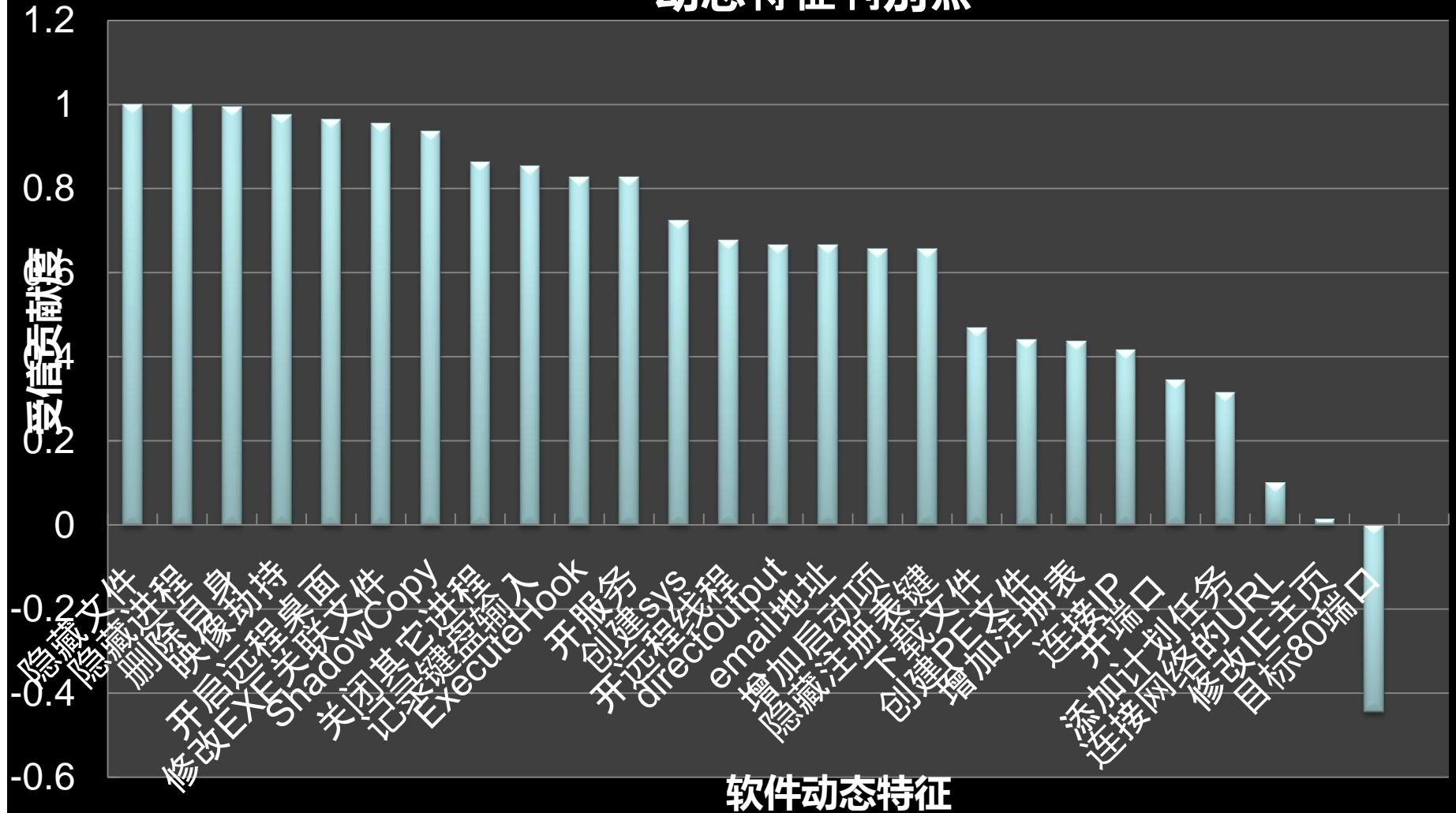
```
0 10 20 30 40 50 60 70 80 90 100
130 </Time>
131 <Time ID="16" logtime="2011-3-23 11:12:53">
132 <PID>1908</PID>
133 <Image>c:\virus\server.exe</Image>
134 <Action>delete</Action>
135 <Path>c:\WINDOWS\system32\drivers\beep.sys</Path>
136 <Type>FILE</Type>
137 <Other>delete file</Other>
138 </Time>
139 <Time ID="17" logtime="2011-3-23 11:12:53">
140 <PID>1908</PID>
141 <Image>c:\virus\server.exe</Image>
142 <Action>MoveFile</Action>
143 <Path>C:\WINDOWS\System32\Drivers\usb20.sys|C:\WINDOWS\System32\Drivers\beep.sys</Path>
144 <Type>FILE</Type>
145 <Other />
146 </Time>
147 <Time ID="18" logtime="2011-3-23 11:12:53">
148 <PID>1908</PID>
149 <Image>c:\virus\server.exe</Image>
150 <Action>OpenService</Action>
151 <Path>Beep</Path>
152 <Type>SERVICE</Type>
153 <Other>SERVICE</Other>
154 </Time>
155 <Time ID="19" logtime="2011-3-23 11:12:53">
```

判别系统

- 可疑行为识别
 - 远程线程序
 - 自删除（主体进程镜像被删除）
 - 注册表自启动位置
 - 其它自启动
 - 注册表敏感位置（劫持）
 - 恶意URL访问(恶意的域名，放马地址等)
 - 恶意IP访问
 - 映像劫持
 - 终止沙软进程
 - 释放驱动反主动防御

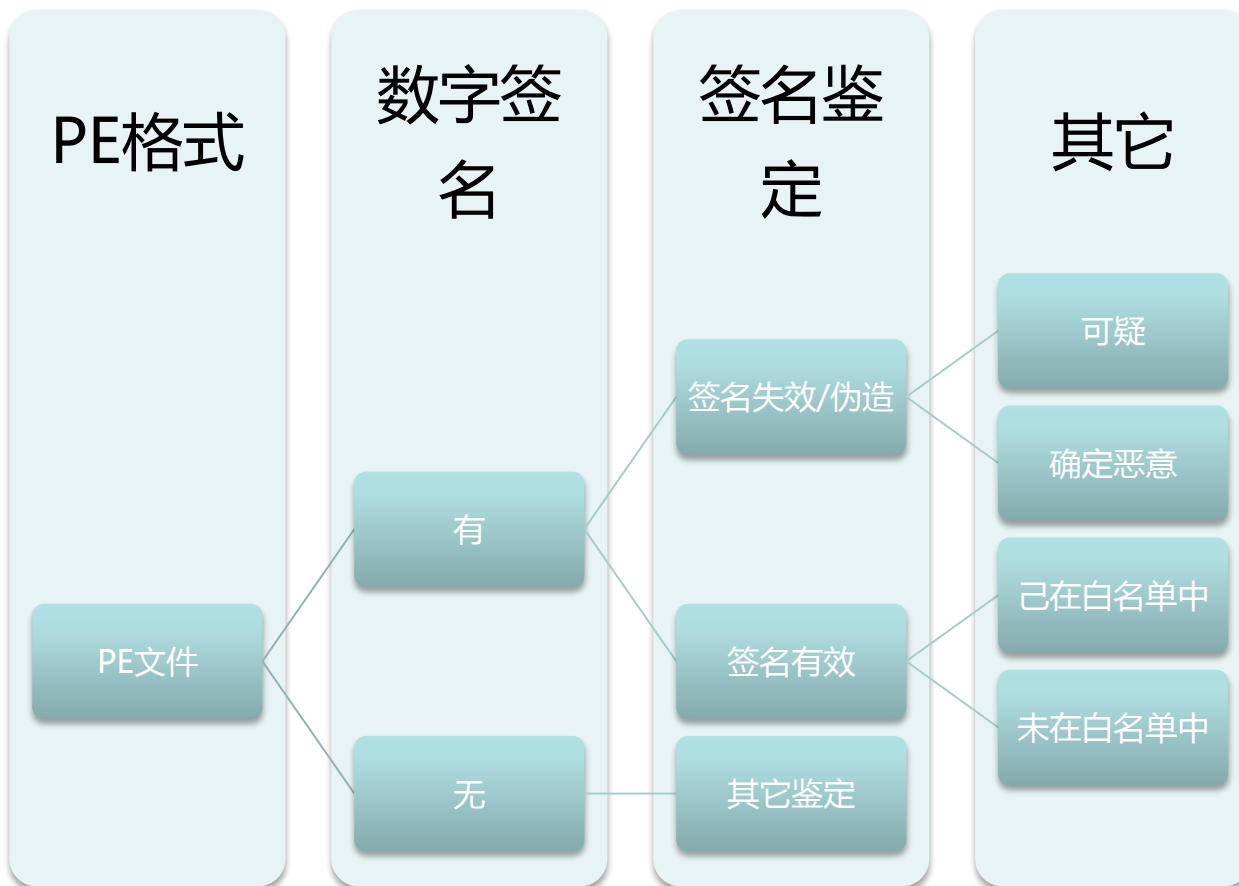
判别系统

动态特征判别点



检测机理—联合判定

- 基于分析结果的联合判定



基因辅助提取

- 动、静态信息统计

- 基因特征 str : cmd /c api:deletefile

Action:delfself

- 不同层次

- 创建文件，创建PE文件，创建DLL文件，创建名字为abc.dll的文件

- 黑白样本集中的概率

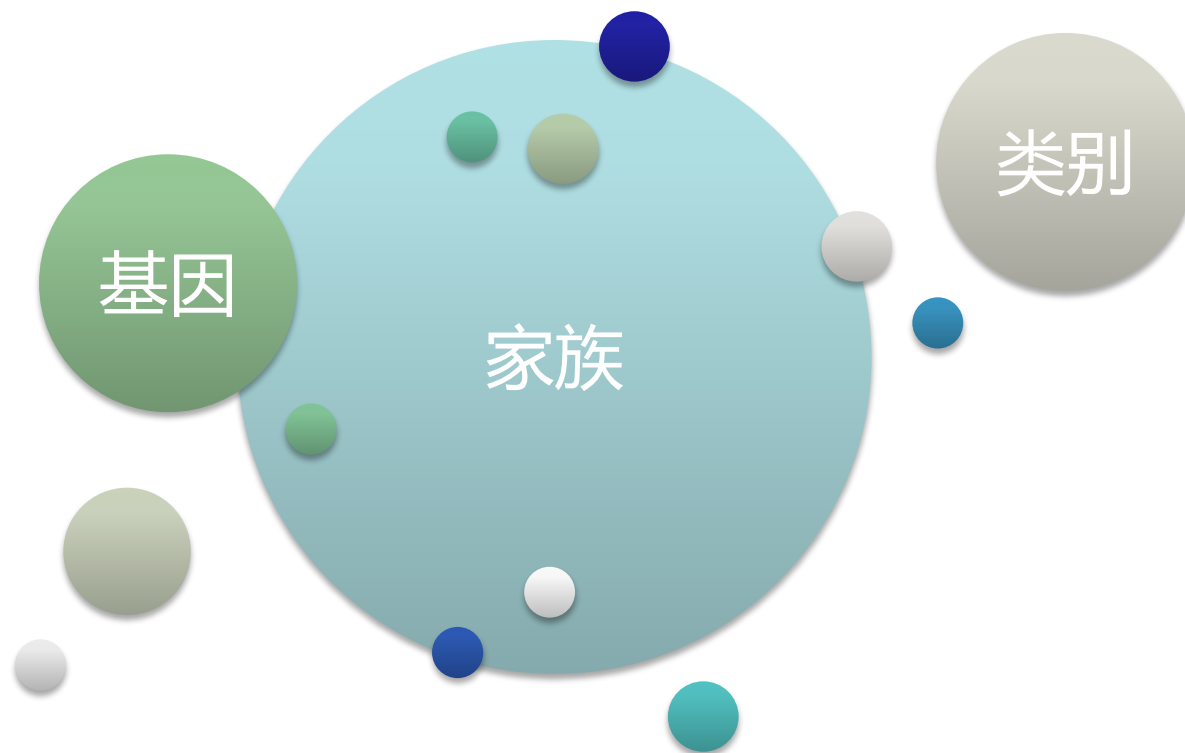
- 概率表明覆盖面积

- 黑白概率差异表明基因的权重

$$G = \begin{cases} \frac{p_b - P_w}{P_b + P_w}, & P_w \\ \frac{p_b - P}{P_b + P}, & P_w \end{cases}$$

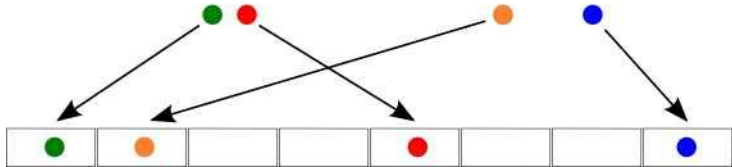
依托海量数据分析自动分类一

- 基因特征向量
- 离群点的分析和处理
- 噪声处理

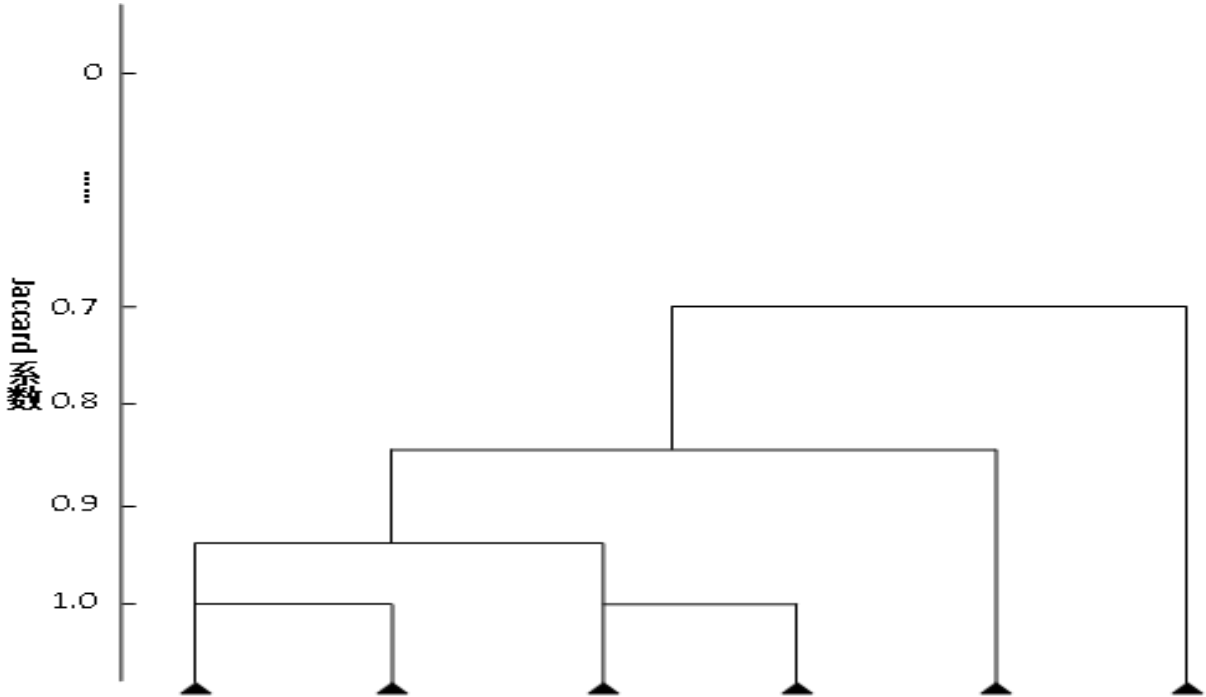


依托海量数据分析自动分类二

general hashing



locality-sensitive hashing



自动化分析响应



一些观点

- APT颠覆了全球主要国家阵营间艰难形成的应急协作体制
- APT是AV厂商一个新的28定律分水岭
- APT在原有的采集+自动化能力的比拼，增加了深度分析能力和耐心的比拼
- APT的大众与小众，必然有产品模式的变化
- APT对抗的本质依然是资源和代价对抗，我们已经输在起跑线上.....

Thanks