ANTIY 安天

AVER反思三部曲之二

走出蠕虫木马地带

——传统反网络恶意代码方法的成因与应对APT的局限

安天实验室 肖新光（江海客）

2013. XDEF. 武汉

个人简介

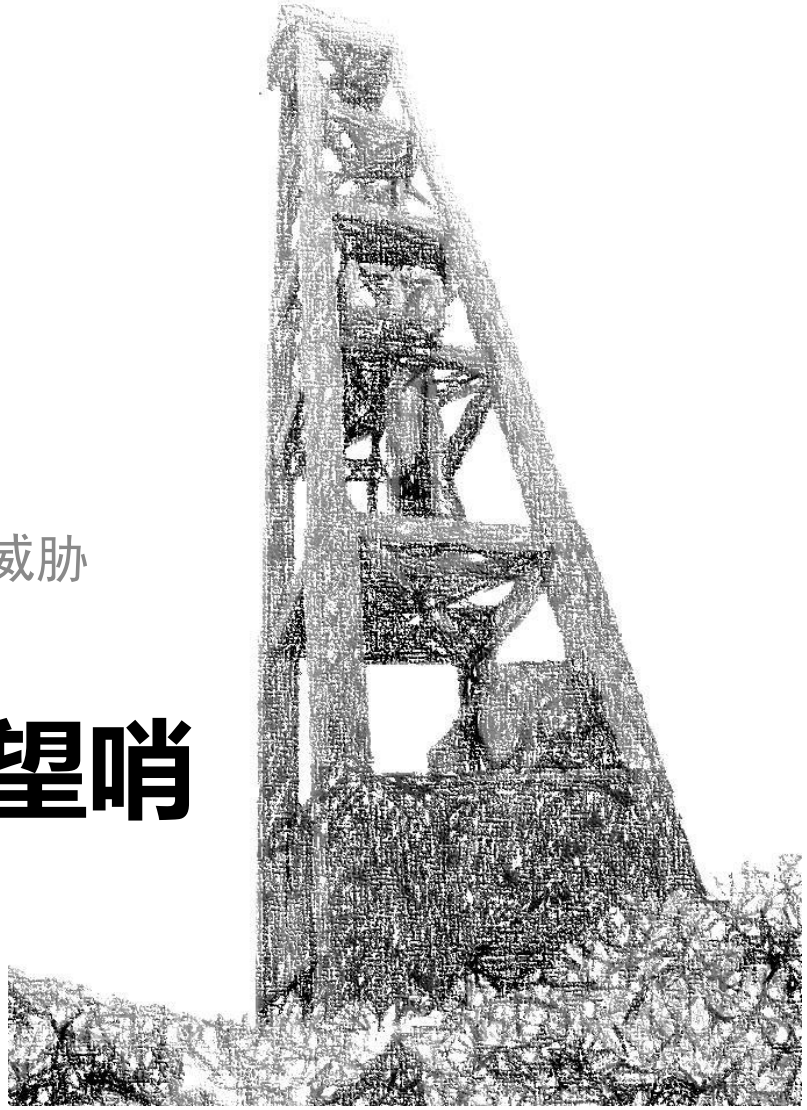
- 中国公民：肖新光
- 安天实验室成员：seak
- 互联网网民：江海客
- 反病毒老兵（Since 1994）

提纲

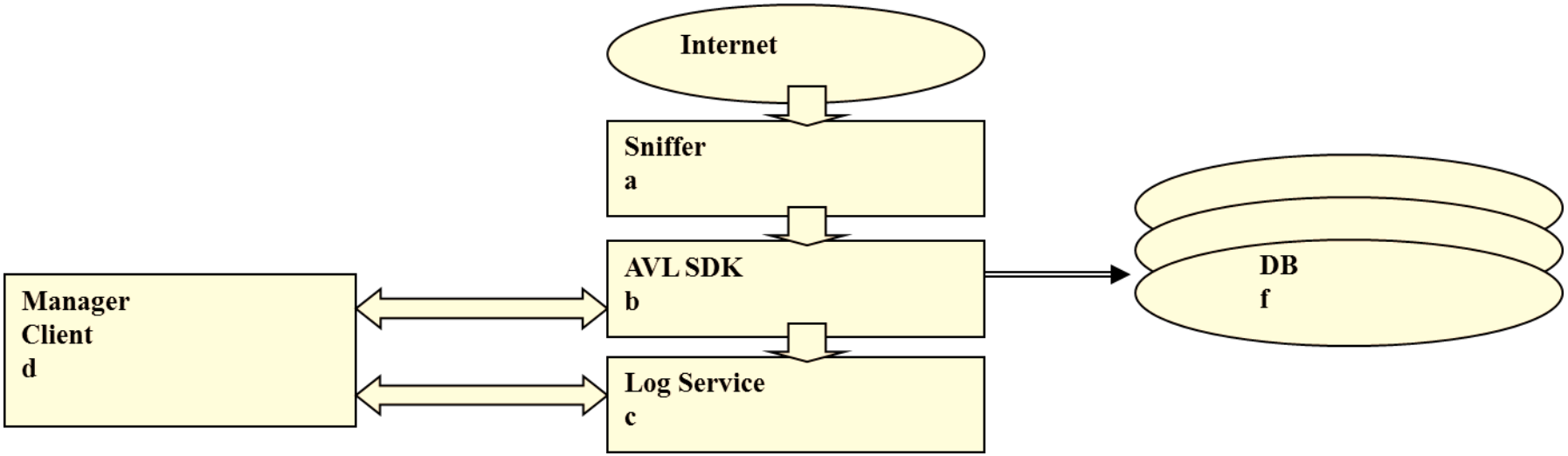
- 网络侧—失守的瞭望哨
- 蜜罐—原始人的陷阱
- 分析流水线—笨拙的蒸汽机
- 展望—再造利器、再造方法

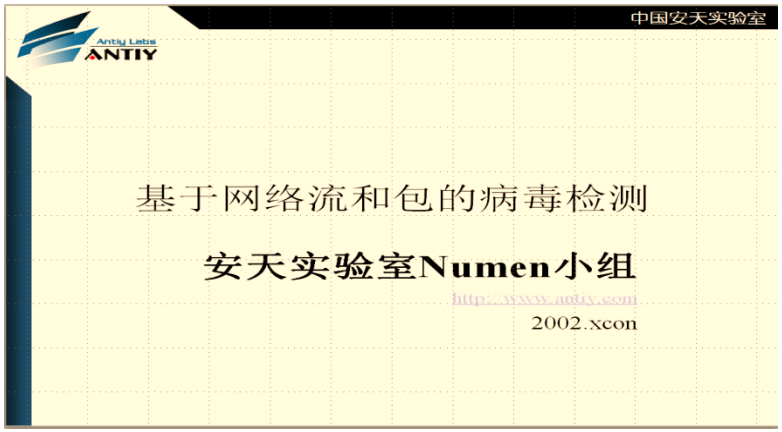
网络侧的检测手段基本是在与蠕虫类威胁斗争中形成和完善的。

网络侧—失守的瞭望哨



重回原点（2002）





2002年12月XCON会议报告

P-A病毒监控预警平台（2002年）
由安天和哈尔滨工业大学共同研制

网络侧设备的发展

超高速、移动网接入

2012

再创新期

2011

2010

成熟期

2009

2008

2007

2006

2005

高速、便携、工具化、细粒度

2004

2003

发展期

成为独立产品形态

2003

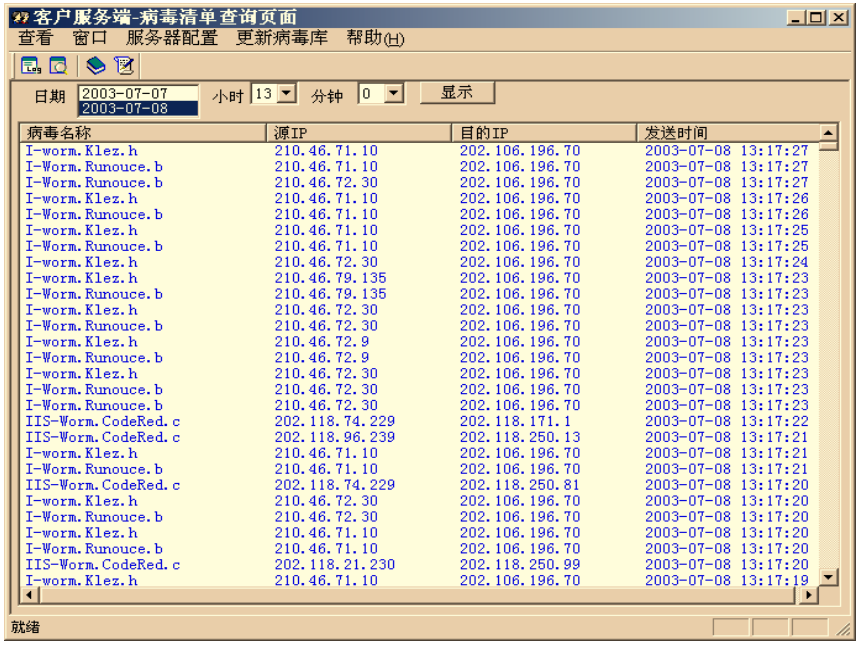
2002

2001

维形期

基本方法论完成

网络侧驱动力-扩散速度



2003年7月8中国教育科研网黑龙江主节点VDS实时数据

2003-7-7病毒扫描日志

统计数据：	
扫描数据流总数：	0
发现病毒体总数：	242573
发现已知病毒总数：	242573
发现未知病毒总数：	0

发现病毒体传输次数排行榜：

名次	病毒名	发现次数
1	I-worm.Klez.h	171267
2	I-Worm.Runouce.b	39661
3	I-Worm.Lentin.i	941
4	I-Worm.Lentin.m	167
5	I-Worm.Sobig.a	67
6	I-Worm.LovGate.f	54
7	I-Worm.Sobig.b	12
8	I-Worm.Sobig.c	2
9	I-Worm.Sobig	1
10	I-Worm.Tanatos.dam	1

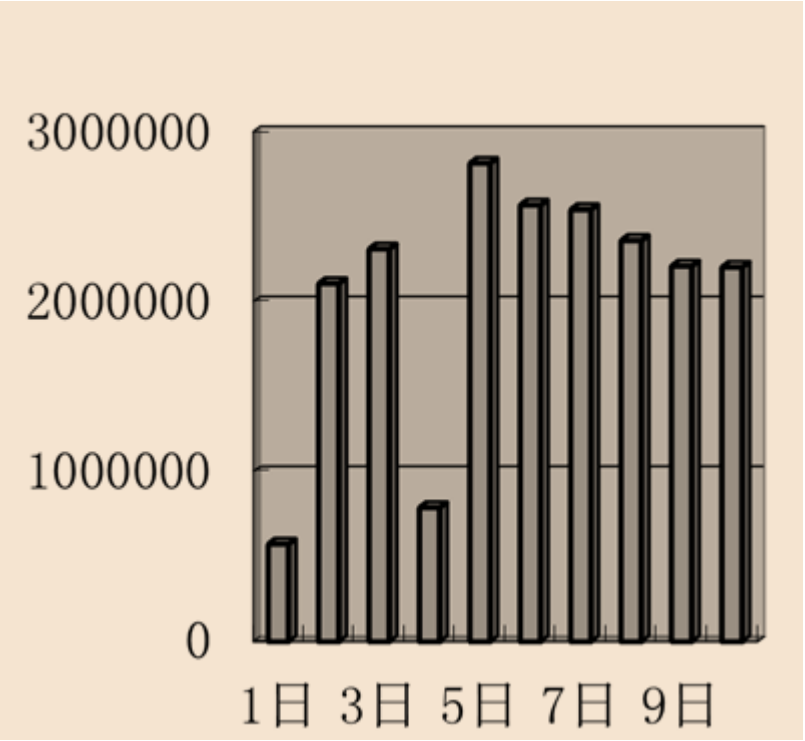
发现病毒体传输次数统计图：

2003年7月7日
中国教育科研网黑龙江主节点VDS日统计数据

驱动力-网络运行压力

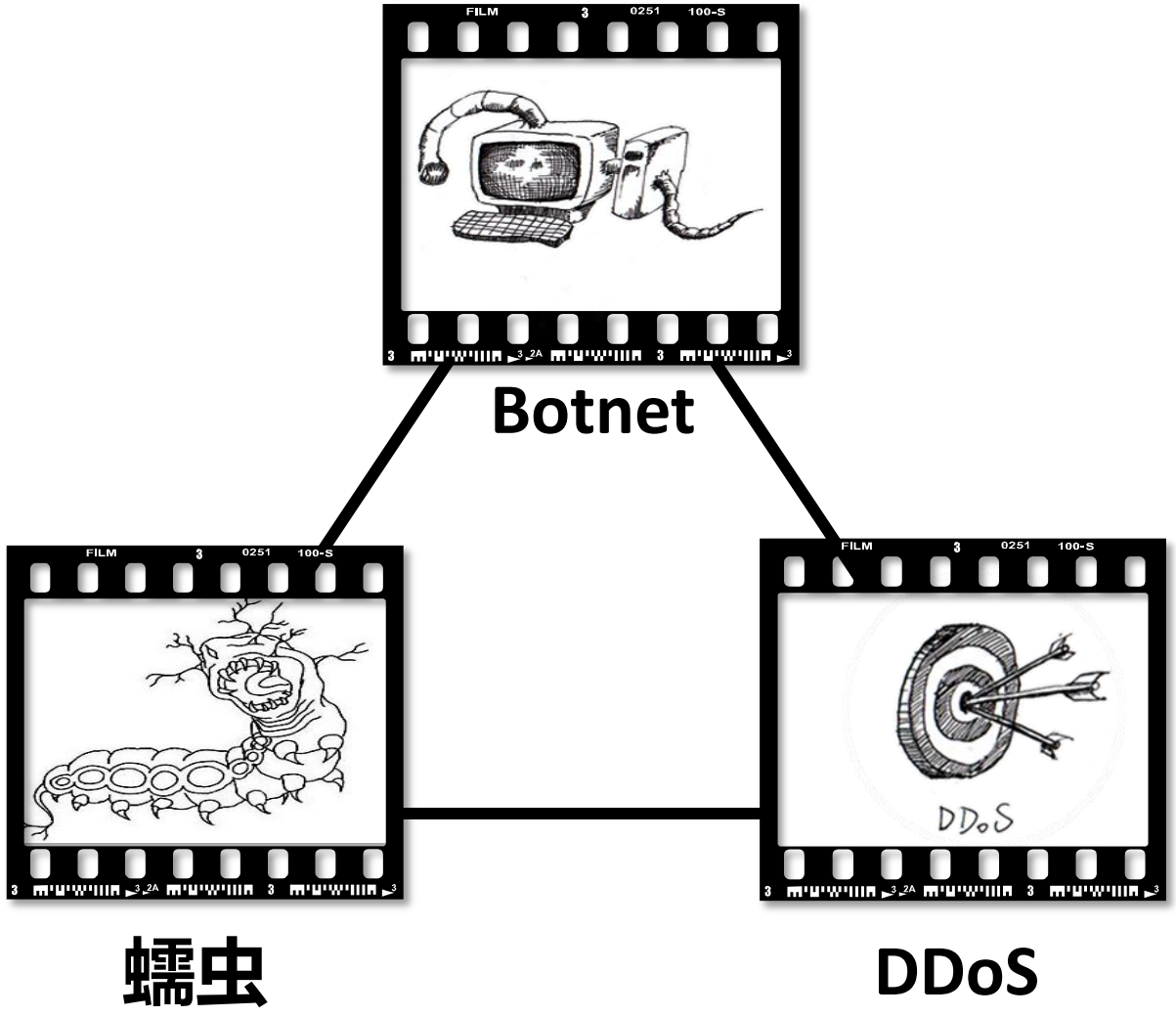
数量排行	名称	接受次数	流量
1	I-Worm.sobig	39006	3.7G
2	I-worm.klez.h	34664	5.6G
3	I-Worm.Runonce	34206	3.0G
合计			12.3G

2003年7月某日
安天在某邮件服务器监控到TOP3蠕虫的情况

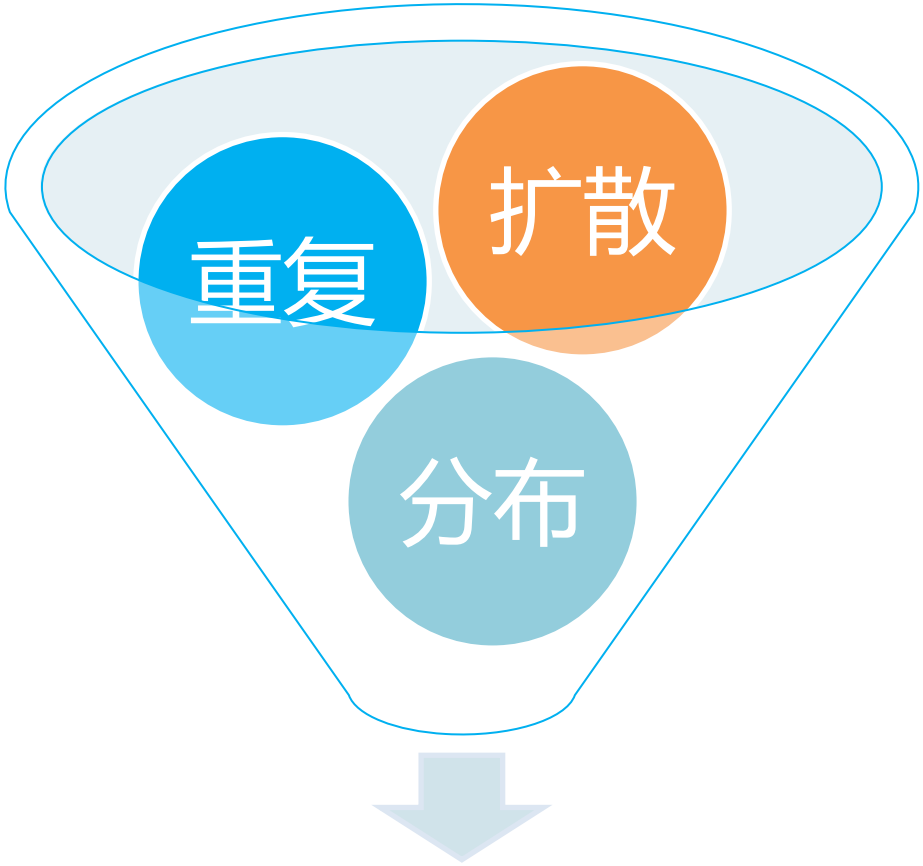


2003年12月上旬
安天在某ISP监控到的Welchian蠕虫扫描数量

[蠕虫时代]威胁集体特点

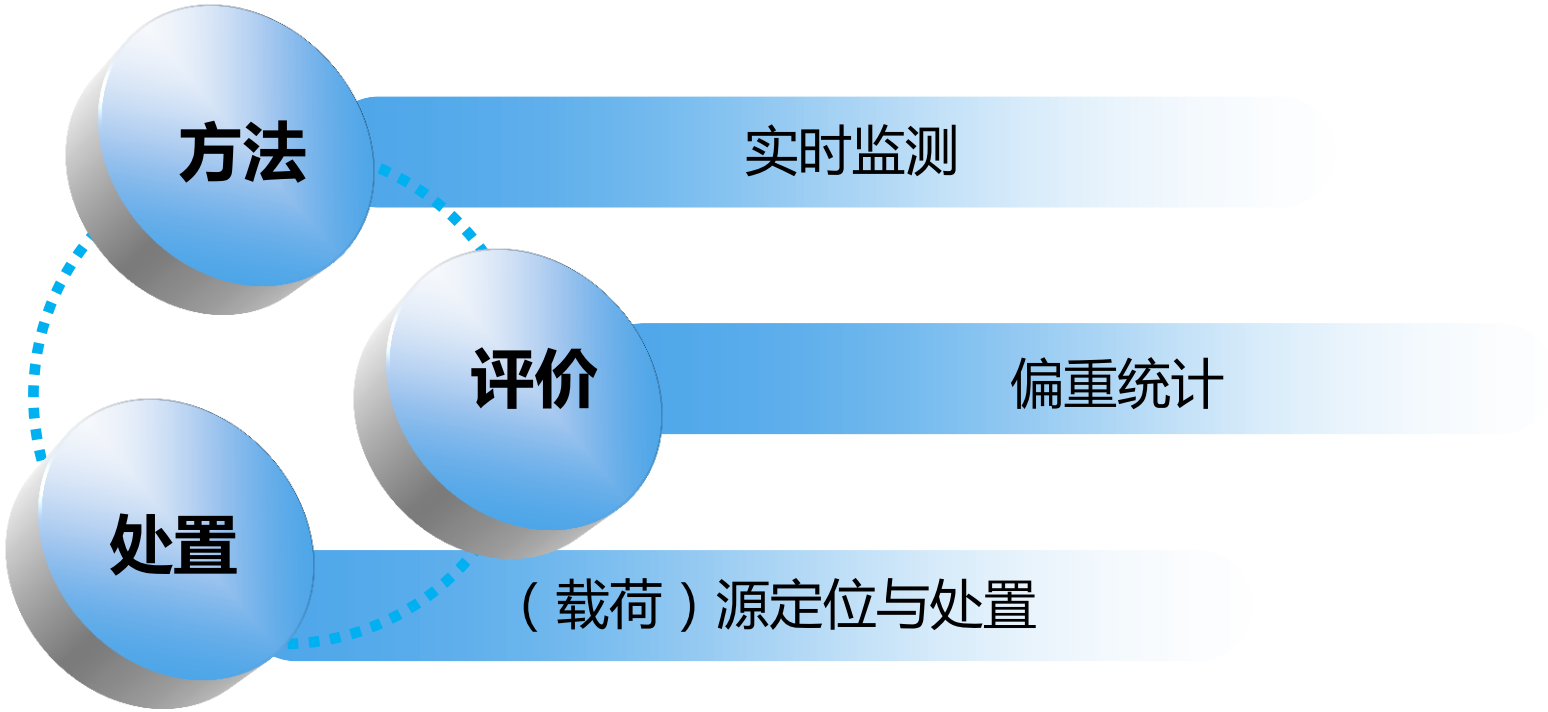


[蠕虫时代]前提假定



检测点

方法关键词



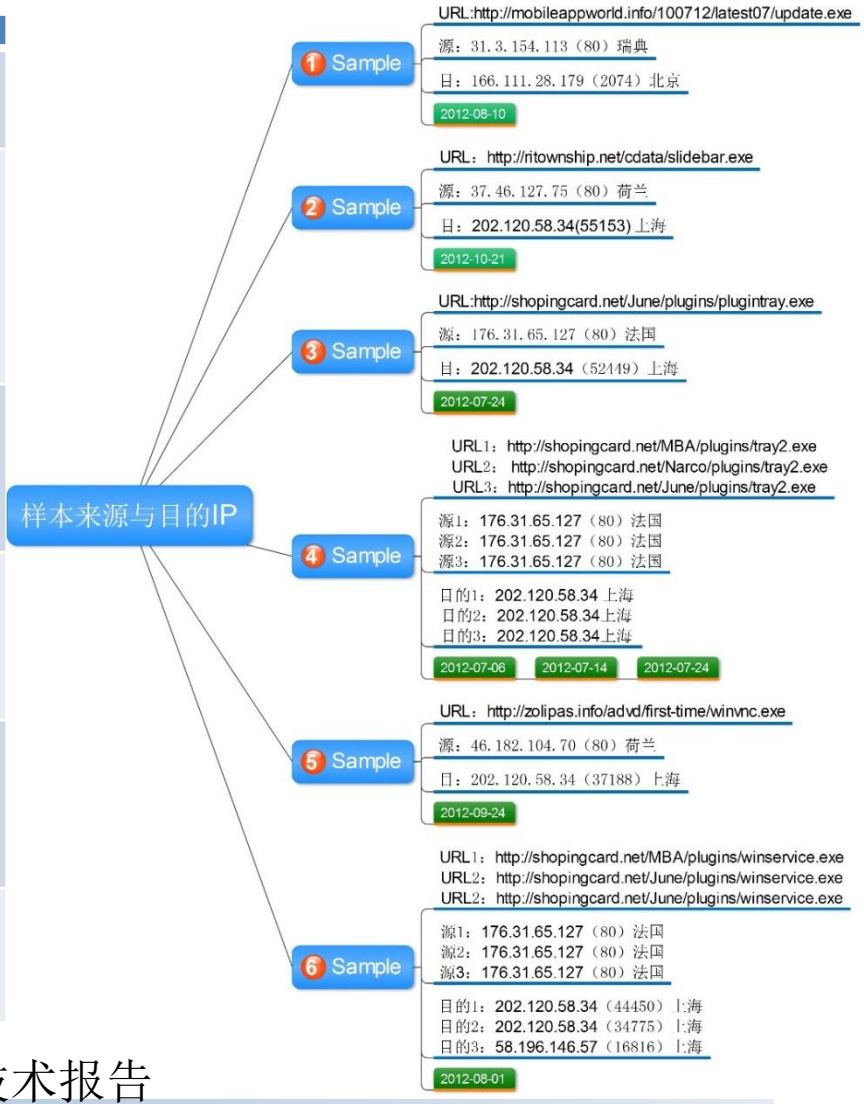
发现病毒体扫描次数排行榜：

名次	病毒名	发现次数	源节点数
1	IIS-Worm.CodeRed.c(Scan)	45513	1023
2	IIS-Worm(Scan)	980	2
3	I-Worm.Nimda(Scan)	577	109

2003年某日中国教育科研网黑龙江主节点扫描蠕虫的数据

APT穿透：以Hangover为例

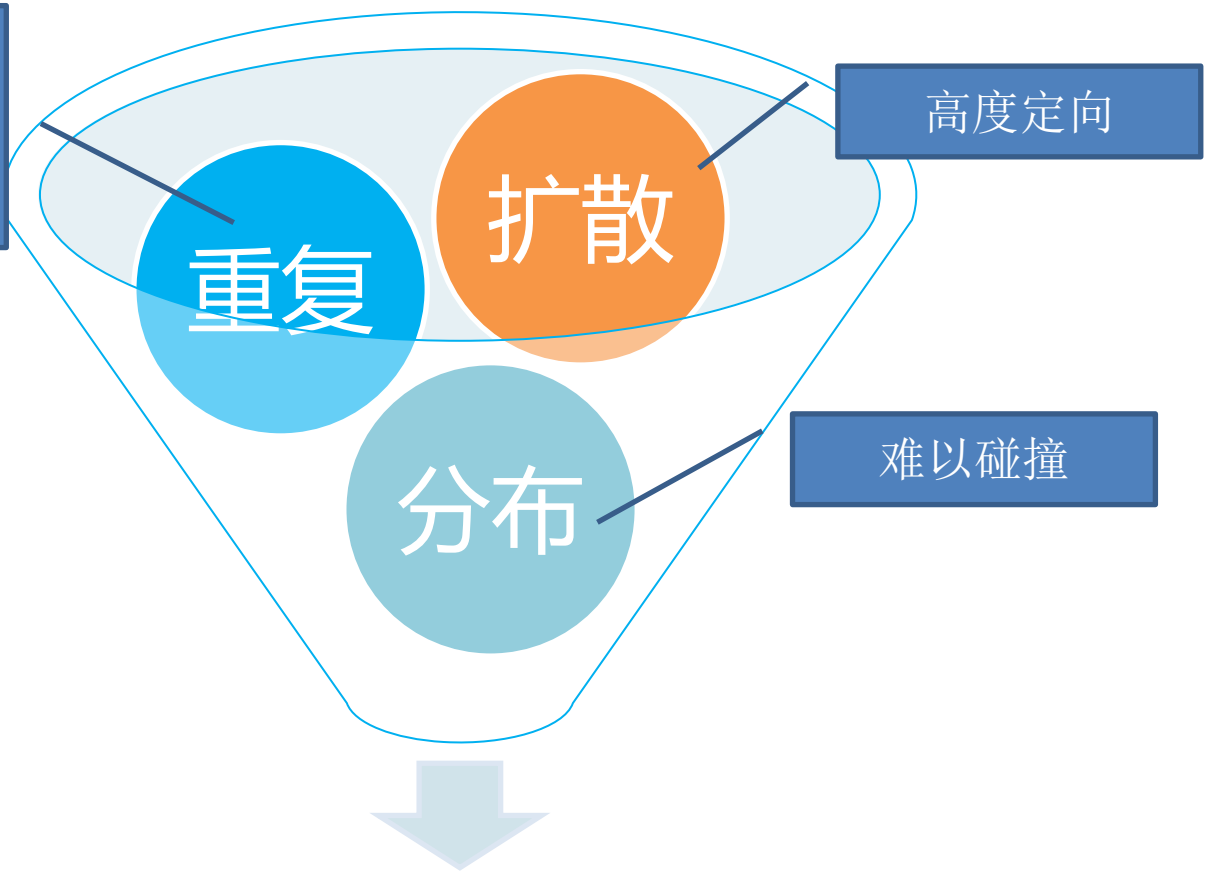
	壳	编译器	主要行为
Sample 1	无	Microsoft Visual Basic 5.0 / 6.0	释放的VBScript脚本,脚本执行后连接远程服务器zolipas.info。（域名失效）.
Sample 2	无	Microsoft Visual Studio .NET 2005 -- 2008	运行后将以下文件设置为Run自启C:\WINDOWS\system32\CatRoot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\slidebar.exe，后续无其他行为
Sample 3	UPX 0.89.6 - 1.02 / 1.05 - 1.24	Dev-C++ 4.9.9.2	运行后在C:\ApplicationData\Prefetch\目录下生存log.txt文件，不断的记录键盘、窗口标题、浏览器搜索内容、计算机用户名等信息。
Sample 4	UPX 0.89.6 - 1.02 / 1.05 - 1.24	Microsoft Visual C++ 7.0	运行后链接域名secureplanning.net欲下载其他恶意代码（URL失效）。
Sample 5	无	Microsoft Visual Studio .NET 2005 -- 2008	运行后在c:\Documents and Settings\Administrator\Local Settings\Application Data\NTUSR\目录下创建文件ntusr1.ini进行键盘记录
Sample 6	无	Dev-C++ 4.9.9.2	样本运行后在C:\ApplicationData\目录下释放logFile.txt文件，收集各种相关扩展名文档名称。



引自2013-08-13日安天内部技术报告

[APT]对网络侧的前提穿透

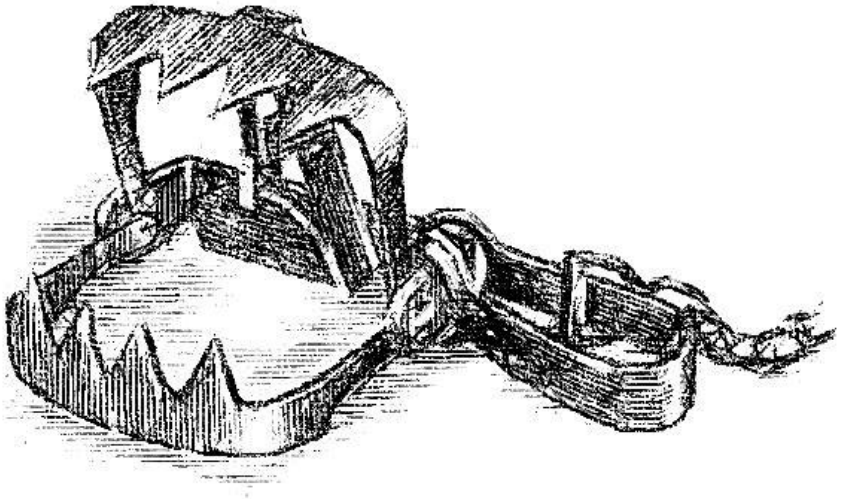
载荷部分很少重放
通讯部分虽然持续，但具有隐蔽性



检测困难

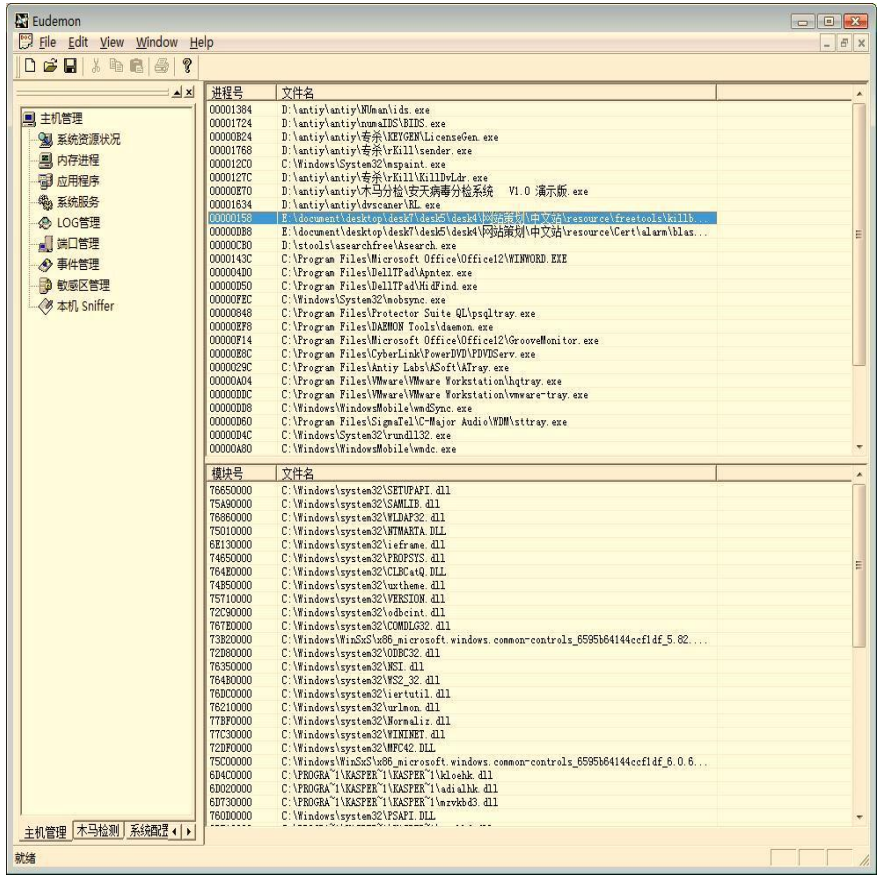
小结

- 过度追求吞吐量、检测速度、以及检测点的完备性拉动原有网络设备的发展。
- 但这并不意味着网络侧设备为应对新威胁做好了准备。



蜜罐——原始人的陷阱

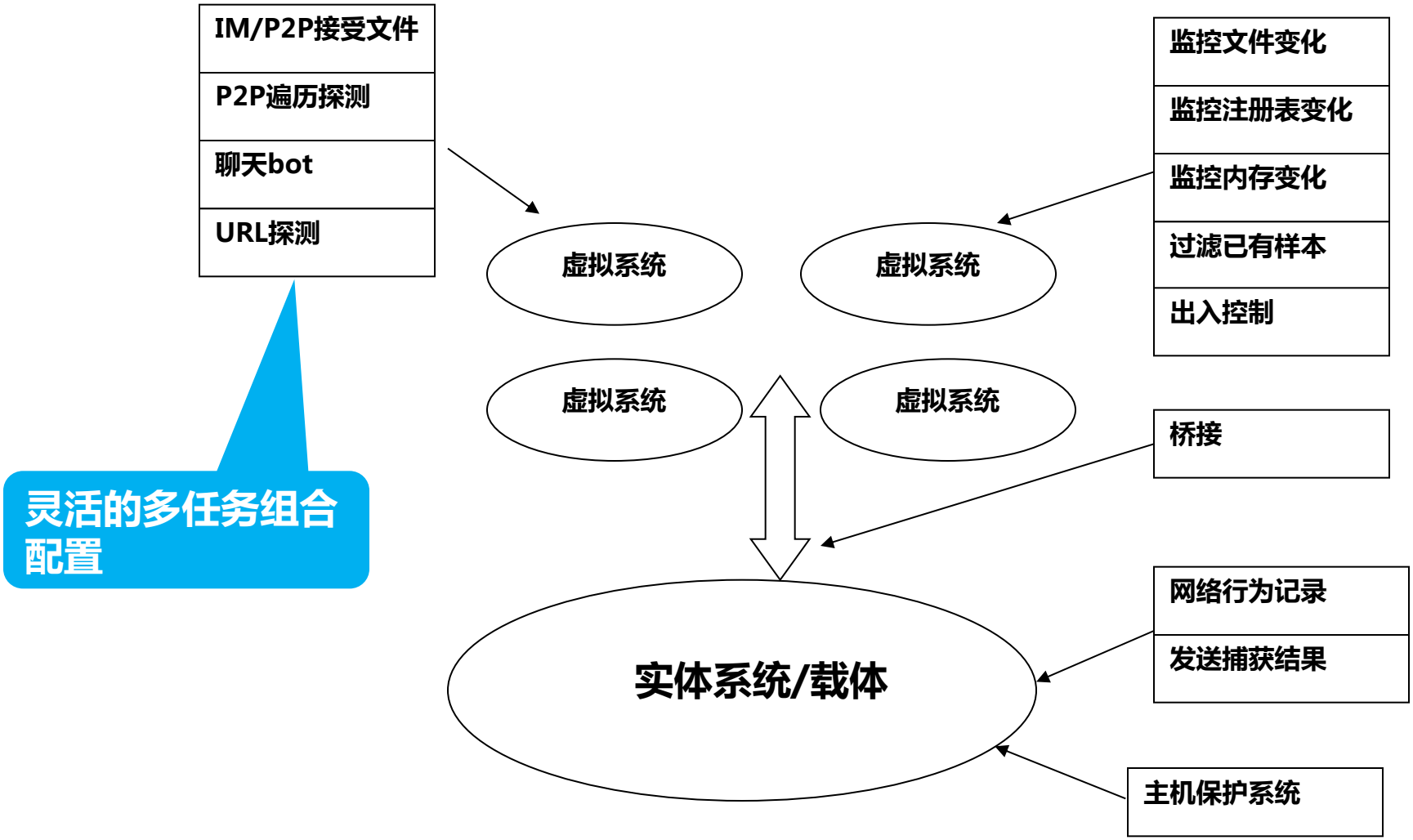
回到原点（2001）



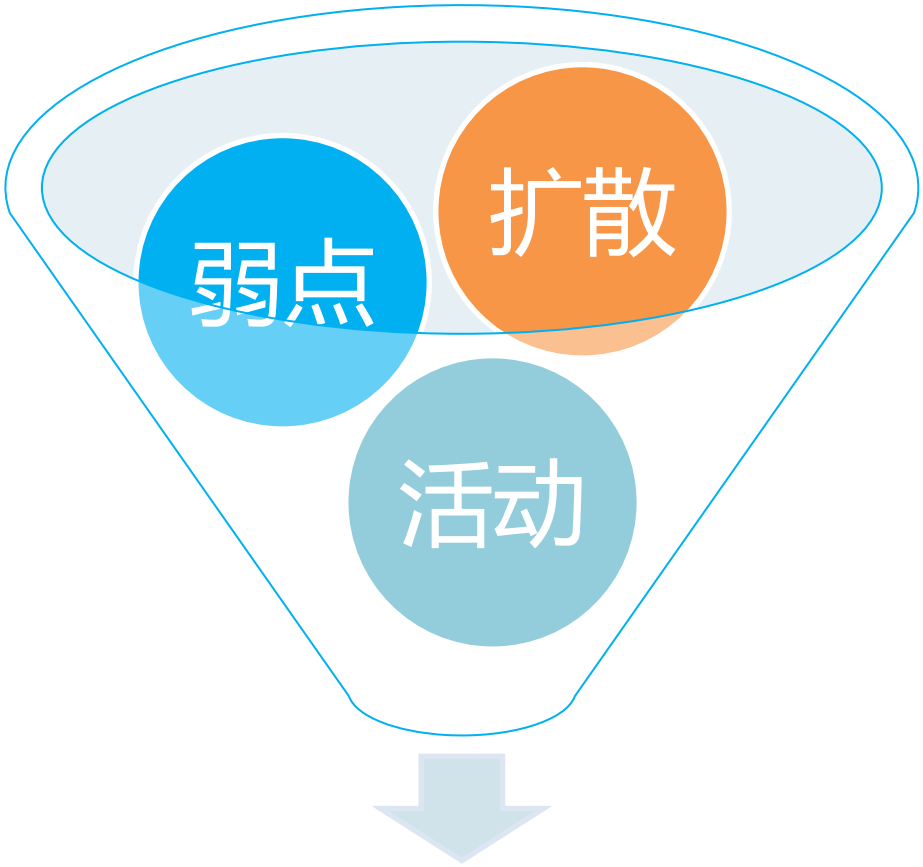
2001年 安天Eudemon主机安全系统
曾捕获CodeRed II蠕虫

2005～2007
基于ARM的低成本虚拟蜜罐系统

糖人的思路

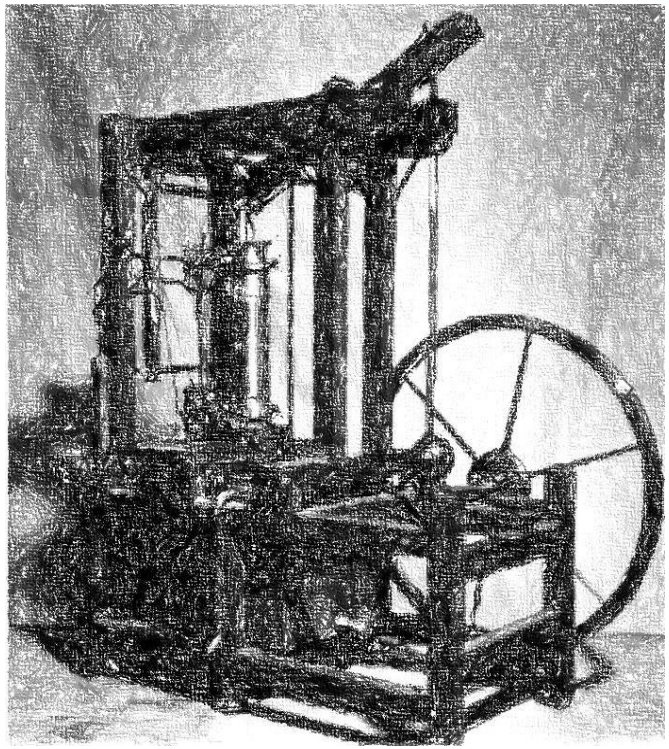

IM/P2P接受文件
P2P遍历探测
聊天bot
URL探测
灵活的多任务组合配置
虚拟系统
虚拟系统
虚拟系统
虚拟系统
监控文件变化
监控注册表变化
监控内存变化
过滤已有样本
出入控制
桥接
网络行为记录
发送捕获结果
实体系统/载体
主机保护系统

[蜜罐]前提假定



小结

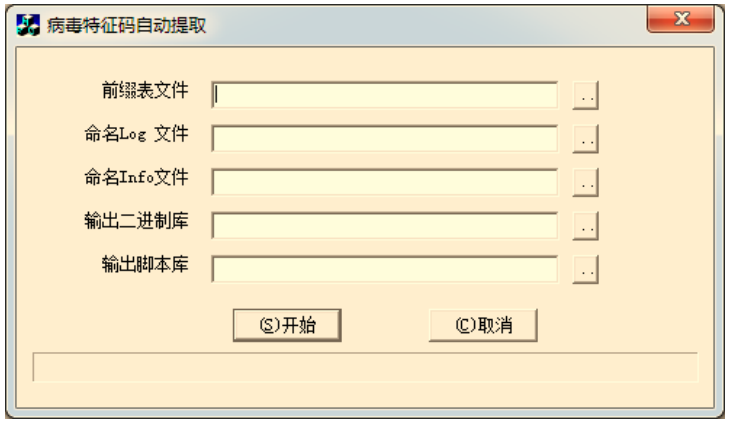
- 在众多在蠕虫时代兴起的安全手段中，蜜罐是最有争议性和临时性的。
- 从捕获价值上来看，其已经远不能与海量的产品客户端部署相比，也不及基于流量的还原。
- 从发现价值来看，其可能在应对大规模扫描探测方面还有一定价值，但其传统思路对APT的价值微乎其微。

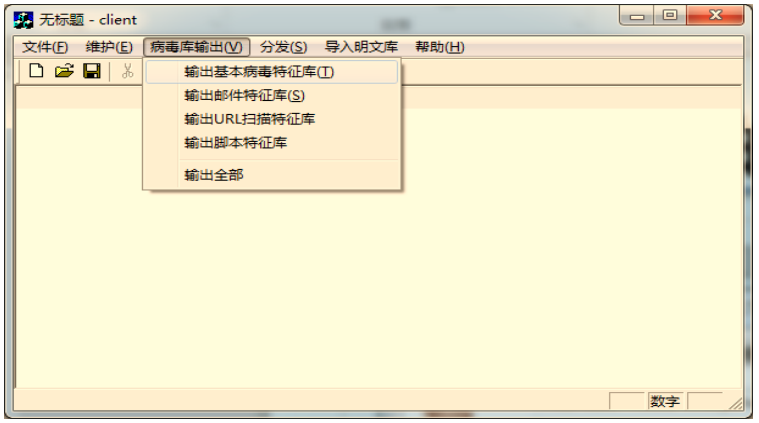


分析流水线——笨拙的蒸汽机

回到原点

名称	类型	大小
Backdoor.Win32.RBot.lo(751B4353).EXe	应用程序	89 KB
Trojan-Downloader.Win32.Small.any(BB830A3D).exe	应用程序	7 KB
Trojan-Dropper.Win32.Microjoin.gen(3B7952EE).exe	应用程序	9 KB
Trojan-Downloader.Win32.Agent.fw(F56A6EE5).exe	应用程序	28 KB
Trojan-Downloader.Win32.Agent.fw(EE556E2A).exe	应用程序	98 KB
not-a-virus.AdWare.180Solutions(D4B5B489).exe	应用程序	92 KB
not-a-virus.AdWare.180Solutions(EF1075C2).dll	应用程序扩展	56 KB
not-a-virus.AdWare.Sahat.l(6EFB6CCE).exe	应用程序	193 KB
not-a-virus.Porn-Downloader.Win32.TibSystems(21A66713).exe	应用程序	27 KB
Virus.MSWord.Xaler.a(6C7C485B).DoC	Microsoft Word ...	62 KB





AutoDistill.exe	2003/7/19 14:26	应用程序	40 KB
AV.LIB	2003/7/4 18:14	LIB 文件	9,904 KB
VirusScan.exe	2003/7/19 14:25	应用程序	40 KB

早期的AV后台是一个以目录管理样本，以本地小工具管理规则的体制

后台发展过程

1986 | 1995

- **产业背景**：操作系统和软件规模本身在初级阶段
- **核心挑战**：最基本的奠基问题。
- **主要成就**：反病毒最基础的形式化

1995 | 2002

- **产业背景**：局网应用成熟、Internet发展
- **核心挑战**：规模和复杂度的增加
- **主要成就**：现代反病毒引擎的成型、特征自动化提取技术（针对非感染式恶意代码）的成熟

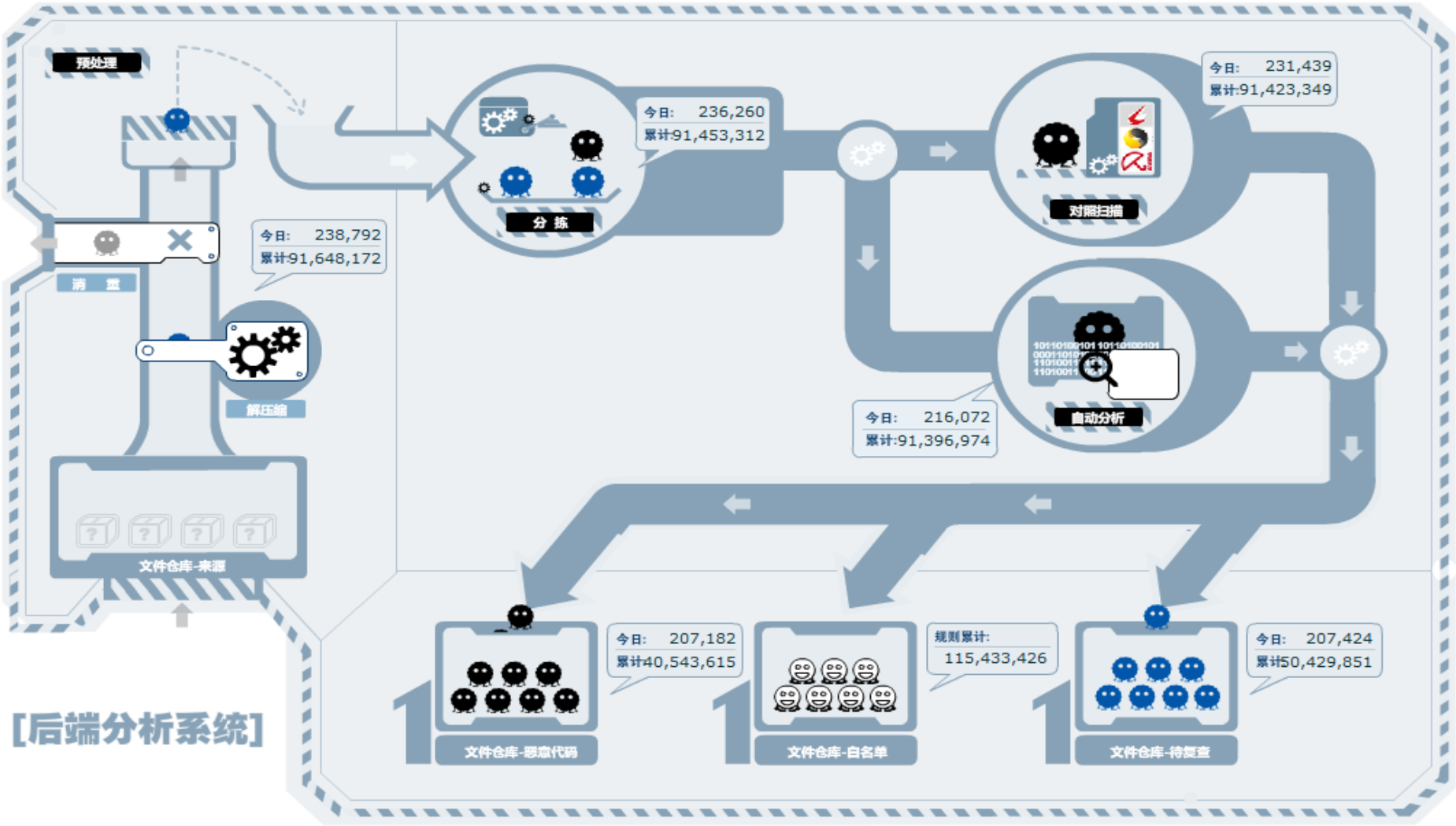
2002 | 2005

- **产业背景**：操作系统日趋复杂、网络主渠道、应用大发展
- **核心挑战**：辨识压力超越处置压力
- **主要成就**：解决分析员作业和样本管理问题

2005 | 2010

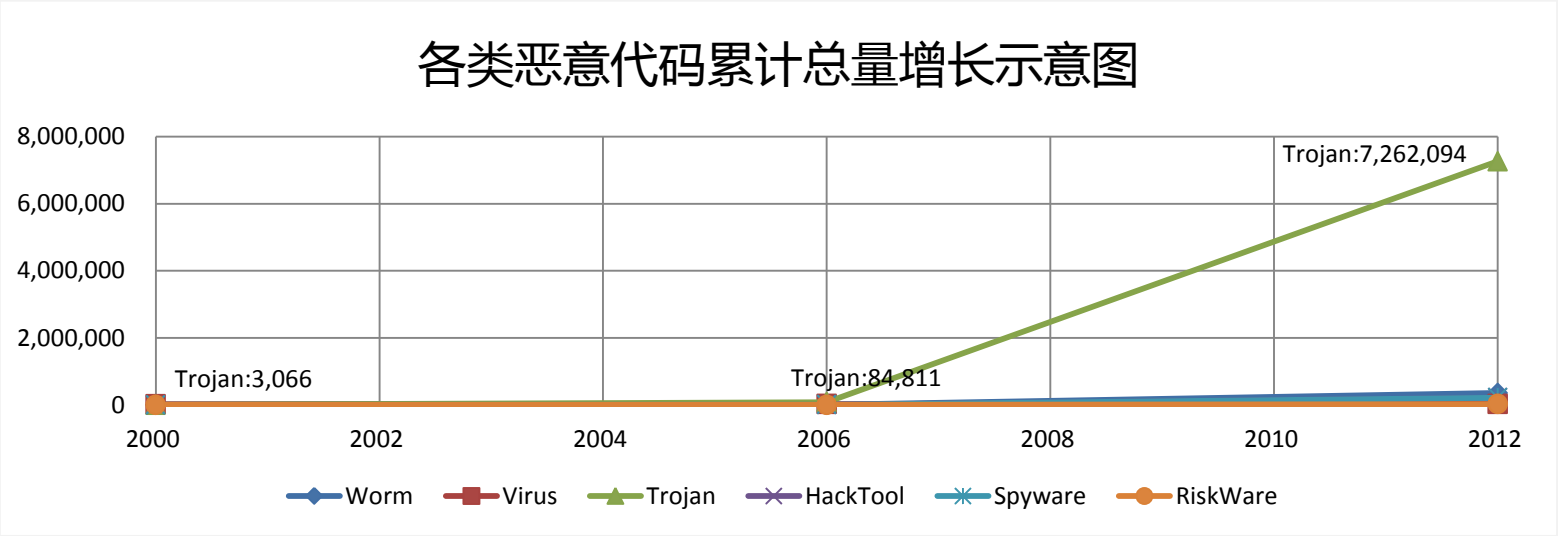
- **产业背景**：网络经济大发展催生地下经济体系，网络计算、云计算、虚拟化成熟
- **核心挑战**：样本和正常应用都以几何级数增长
- **主要成就**：解决海量样本的自动化判定问题

恶意代码的后端分析流水线



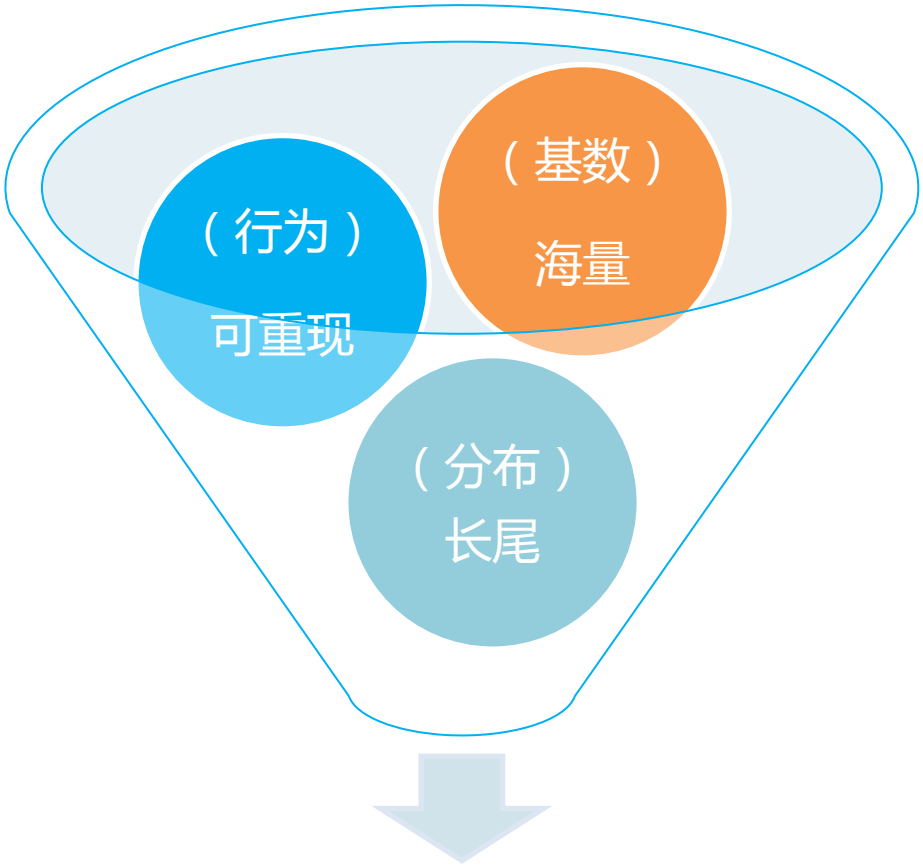
截图2013年11月6日取自安天分析系统

驱动力:木马种类的规模膨胀



统计时间	Worm	Virus	Trojan	HackTool	Spyware	RiskWare
2000/10/24	512	21,006	3,066	260	37	0
2006/11/10	8,109	27,760	84,811	4,968	4,899	88
2012/11/27	354,049	29,940	7,262,094	217,502	214,570	25,800

[木马时代]前提假定



检测点

[木马时代]核心方法.后台时间片

32秒

1分24秒

6分44秒 = ？分？秒

单样本分析报告

导出PDF

概述

行为： 该样本具有删除文件、INFECT、http访问、连接网络、创建文件、释放PE文件.、REGVALUE_MODIFY、MOVE_FILE、独占模式打开、获取计算机名称等行为。

分类： 该样本是木马(Trojan)，木马是一类具有危害主机安全功能，且包含多种恶意行为分类的恶意代码，如：Rootkit、Backdoor、Bot、Downloader、PSW、Clicker等。反病毒厂商通过Trojan的行为进行分类，并在病毒名上标注类似上述的行为标签。原则上是既没有感染其它文件能力也不具备主动传播自身特性的恶意代码。它们的特性是以达成某种目的：如远程监控主机、组建僵尸网络、下载其他恶意代码并运行、窃取主机的各类账号密码信息、刷网站流量等。

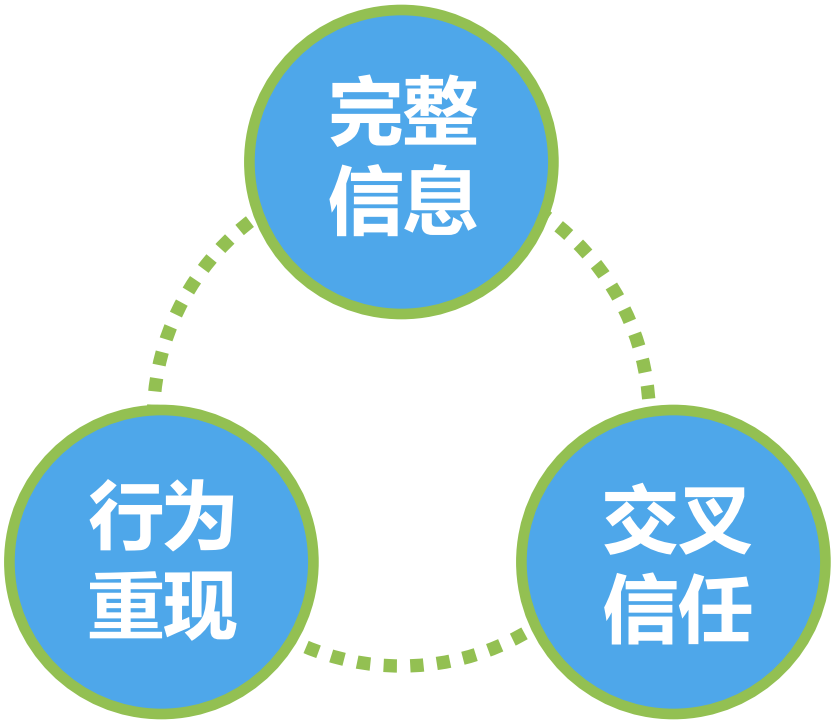
环境： 该样本的运行平台属于操作系统(Win32)，微软Windows32位平台操作系统。运行于微软Windows32位平台操作系统。该系统的代表版本有Win95、Win2k、WinNT、WinXP等，其主要的可执行文件结构是PE格式。

基本信息

原始文件名	VideoAccelerator.exe
恶意判定	含有病毒
病毒名称	Trojan/Win32.Agent.2ab9c7
文件大小	1907.00KB (1,952,768 字节)
文件格式	BinExecute/Microsoft.EXE[:X86]
PE格式	EXE_PEFORMAT
MD5	000009525846FCCDE6194E7F79B61947
SHA1	8D8FE4B20B185702301A86646EC080DF4D0BC5BD
编译器	未成功识别
壳名称	无
来源	amag(1)

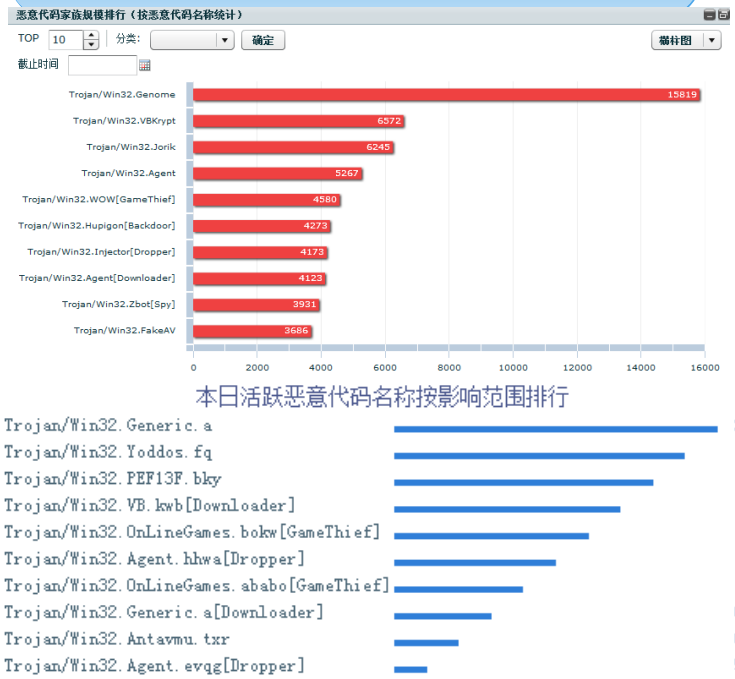
行为分析 多引擎对照扫描 静态分析 动态分析

方法关键词

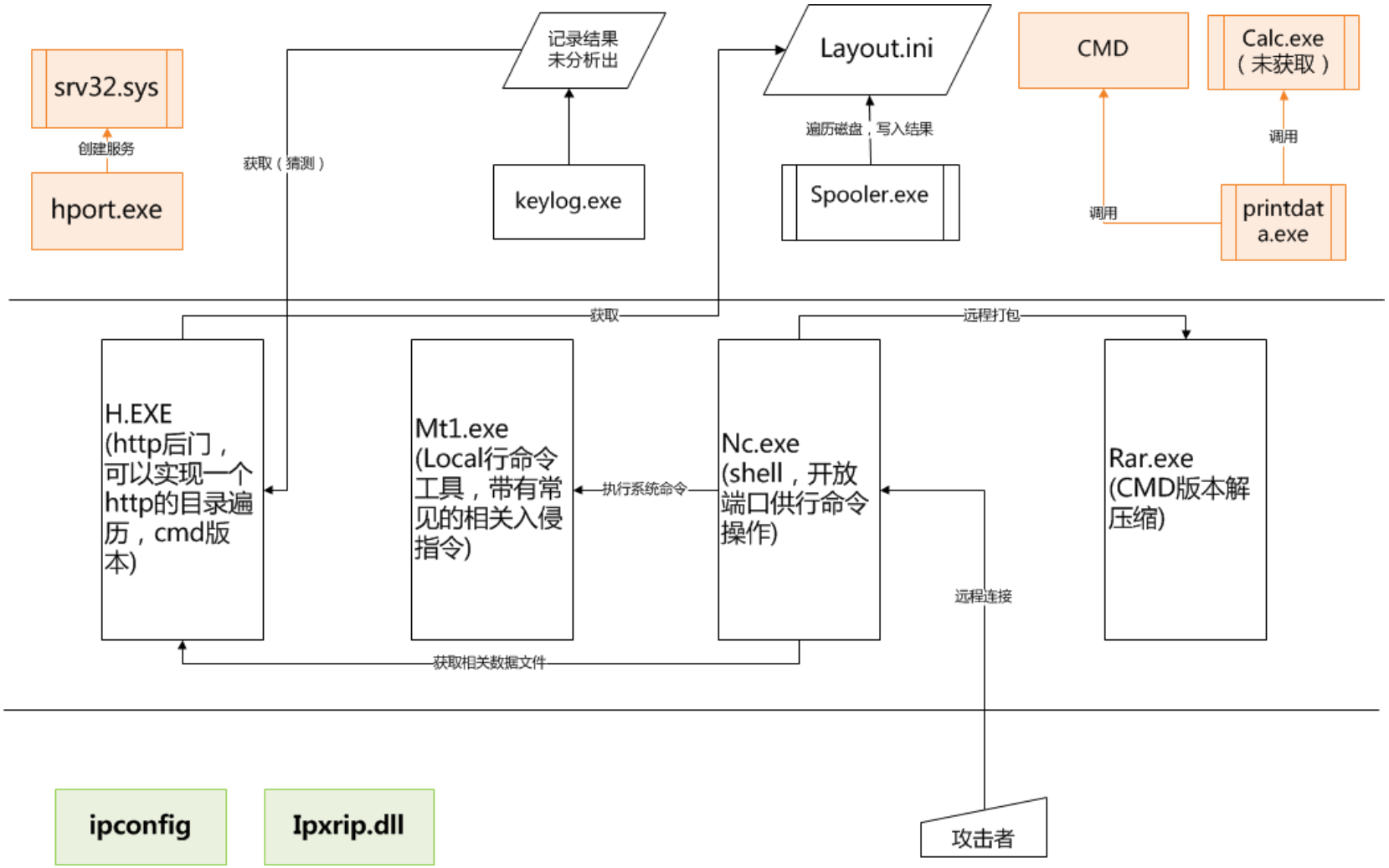


评价指标

- 感染范围
- 变种数量

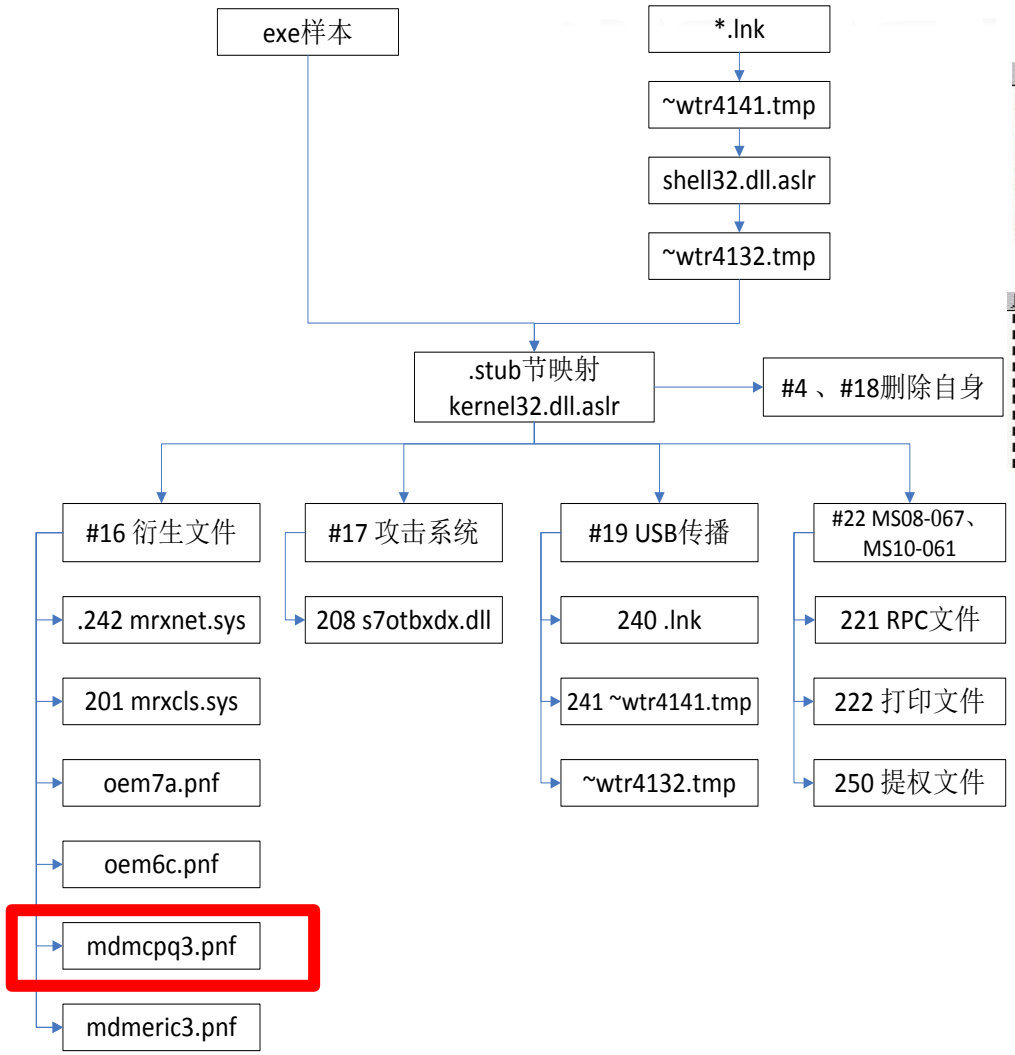


APT穿透：复杂主机场景



2007年11月14日安天对某事件的内部分析报告

APT穿透：之不可浮现



反汇编	文本字串
MOV EBX,Region00.10061B30	{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}
PUSH Region00.10061A80	storage#volume#
MOV EDI,Region00.10061A0C	\\.\
MOV EBP,Region00.10061BCC	%s%s%s#%s
PUSH Region00.10061AA0	storage#volume#1&19f7e59c&0&
PUSH Region00.10061A4C	storage#removablemedia#8&
MOV EBP,Region00.10061BE0	%s%s%x&0&rm#%s
PUSH Region00.10061A18	storage#removablemedia#7&

反汇编	文本字串
PUSH Region00.100618A4	copy of shortcut to.lnk
PUSH Region00.100618D4	copy of
PUSH Region00.100618E8	~wtr4141.tmp
PUSH Region00.10061904	~wtr4132.tmp
PUSH Region00.1005CD1C	*
PUSH Region00.100618E8	~wtr4141.tmp
PUSH Region00.10061904	~wtr4132.tmp
PUSH Region00.1005CD20	global\wkssvcshutdownevent2
PUSH Region00.100618E8	~wtr4141.tmp
PUSH Region00.10061904	~wtr4132.tmp

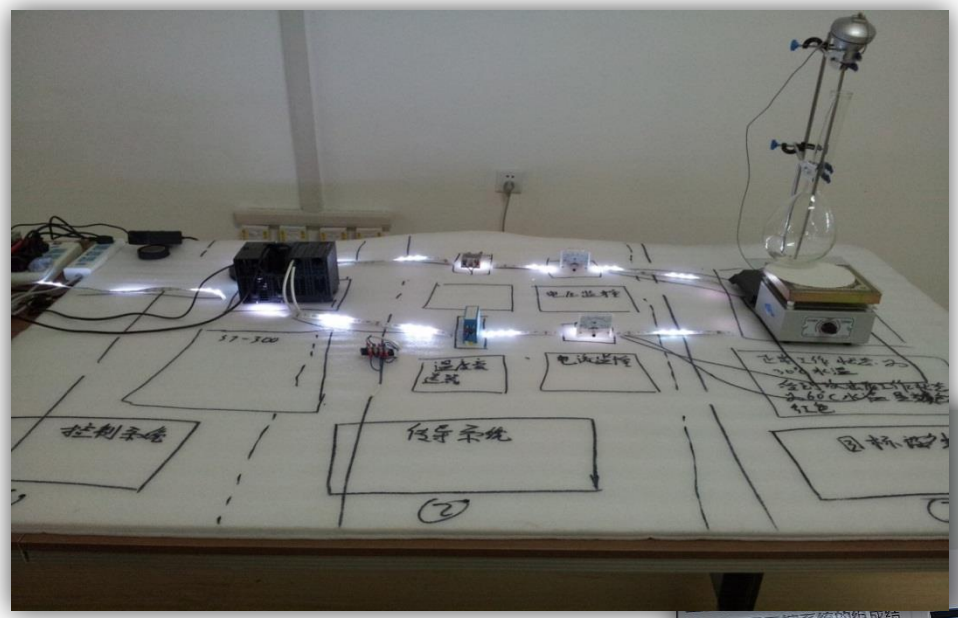
mdmcpq3.PNF

```
          0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00000000h: 09 05 79 AE 14 00 00 00 BF F1 71 D3 44 07 00 00 ; ..y?...狂q餵...
00000010h: 4C 04 00 00 03 00 00 00 01 00 00 00 02 00 00 00 ; L...............
00000020h: 08 00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 ; ................
00000030h: E0 93 04 00 E0 70 72 00 80 84 1E 00 FE 04 00 00 ; 鄴..郧r.€?.?..
00000040h: 01 00 00 00 01 00 00 00 01 00 00 00 80 EE 36 00 ; ............€?.
00000050h: 64 00 00 00 2C 01 00 00 58 02 00 00 84 03 00 00 ; d...,...X...?..
00000060h: 50 46 00 00 08 52 00 00 01 00 00 00 00 00 00 00 ; PF...R.........
00000070h: 00 00 00 00 15 00 00 00 00 00 CB AA 7D A8 CB 01 ; ..........霜}?.
00000080h: 03 00 00 00 40 4B 4C 00 03 00 00 00 00 C0 45 4C ; ....@KL......繾E
00000090h: 9C 51 CD 01 38 31 00 00 00 00 00 00 00 00 00 00 ; 淨?81..........
000000a0h: 00 00 00 00 04 F2 CB 1C 60 5D CB 01 01 00 00 00 ; .....蛩.`]?....
000000b0h: 00 00 00 00 04 F2 CB 1C 60 5D CB 01 00 00 00 00 ; .....蛩.`]?....
000000c0h: 5A 00 00 00 87 00 00 00 01 00 00 00 77 00 77 00 ; Z...?.....w.w.
000000d0h: 77 00 2E 00 77 00 69 00 6E 00 64 00 6F 00 77 00 ; w...w.i.n.d.o.w.
000000e0h: 73 00 75 00 70 00 64 00 61 00 74 00 65 00 2E 00 ; s.u.p.d.a.t.e...
000001e0h: 69 00 65 00 72 00 66 00 75 00 74 00 62 00 6F 00 ; i.e.r.f.u.t.b.o.
000001f0h: 6C 00 2E 00 63 00 6F 00 6D 00 00 00 00 00 00 00 ; l...c.o.m.......
00000200h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
00000210h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ; ................
```

偏移0x6c、0x70、0xc8处的标记位
偏移0x78、0x7c处的时间戳
偏移0x80、0x84处的数值
决定是否进行USB传播，而默认不传播。

为什么Stuxnet USB传播行为不可浮现
引自安天《对Stuxnet蠕虫的后续分析报告》

APT穿透：之场景外延

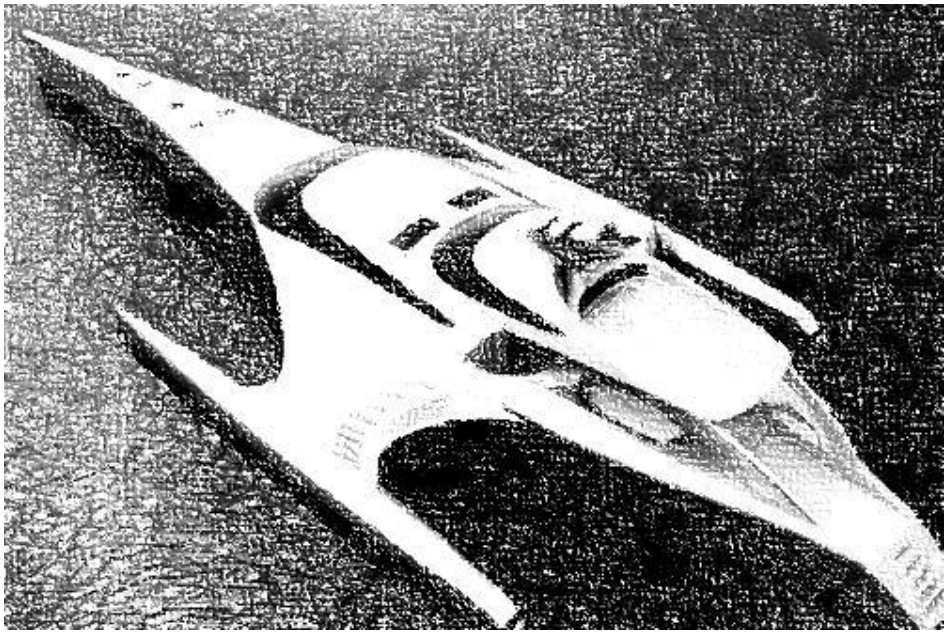


2010年安天搭建的
Stuxnet分析场景

2012年安天搭建的
工控安全演示台

小结

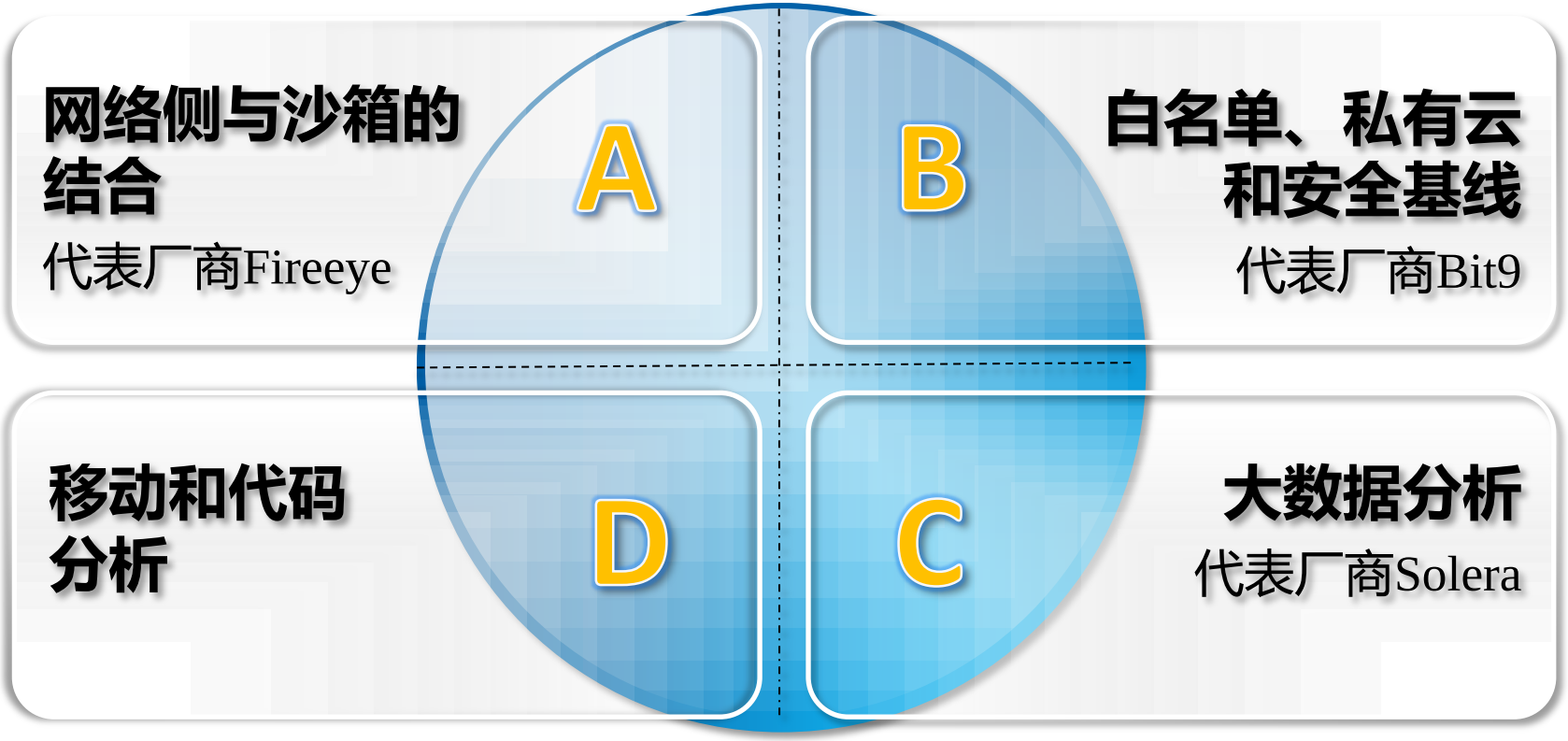
- APT的复杂性是一个分析障碍，但更多的是资源与投入的问题。
- 传统分析流水线并非完全不能有效分析APT样本、也包括定性其为恶意的样本，而是难以将其从海量的黑名单中筛选出来，从而对人工分析作出引导。



一点思考

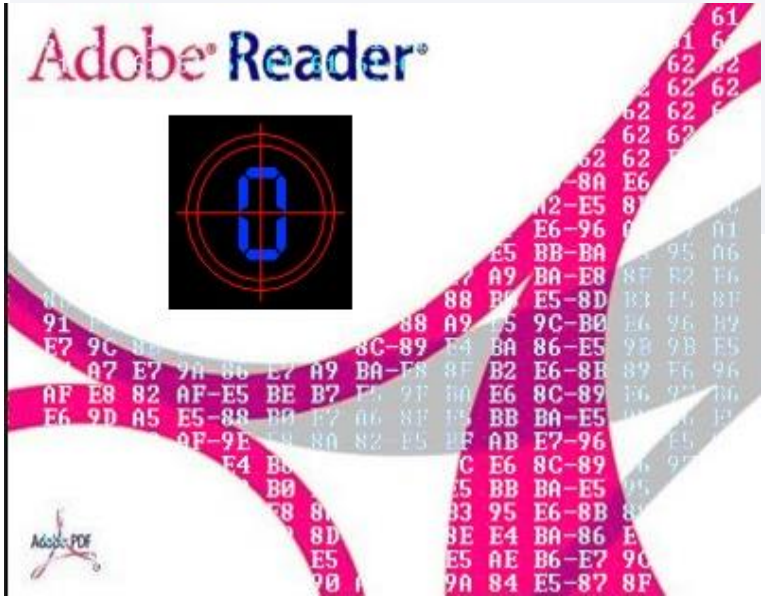
展望——再造利器、再造方法

业内的趋势点

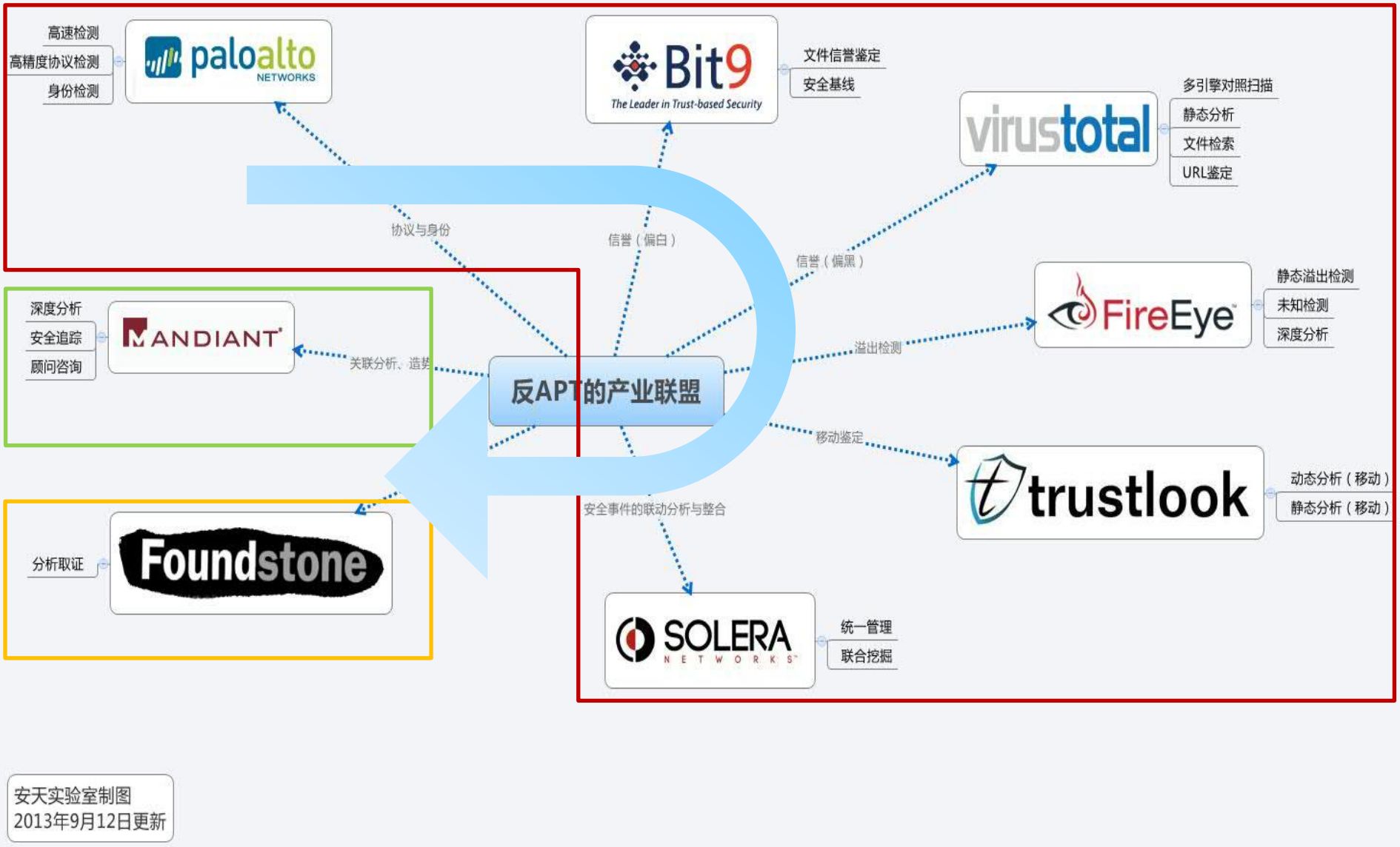

网络侧与沙箱的结合
代表厂商Fireeye
A
B
白名单、私有云和安全基线
代表厂商Bit9
移动和代码分析
D
C
大数据分析
代表厂商Solera

沙箱的再认识


追影的检测方法
环境模拟
环境软件安装
Word、Adobe、IM
移动介质模拟
利用文件夹模拟磁盘，并hook修改磁盘类型
模拟游戏、杀软进程
网络模拟
静态检测
格式解析
特征扫描
Shellcode发现
堆喷射
字符串信息
漏洞检测
行为采集、动态监视
进程创建、终止
远程线程插入
文件操作
注册表创建、设置
网络通信访问
网络数据url
驱动加载


Adobe Reader

美国企业反APT联动机制的启示



安天实验室制图
2013年9月12日更新

尾声：穿越战场

蠕虫已经非常不引人关注，但其并不是被AV击败的，DEP、ASLR和其他的系统环境变化因素是其主因。

云、主动防御对遏制木马起到了很大作用，但并未彻底将其击败，相反木马技术和方法均被APT充分借鉴利用了。

……既然威胁更大的对手已经出现，我们需要穿越战场，在改进武器的同时，我们需要再造方法。

谢谢大家听这份内容不完整的演讲！
后续内容构思中……

2103 11.14~15.上海ISF ！
再续反思……

- 肖新光
- 安天实验室
- http://www.antiy.net
- seak@antiy.com
- Weibo.com/seak