AntiVirus 进化论的浅思

——谨献给安全工作者与病毒斗争的20年

安天实验室 江海客

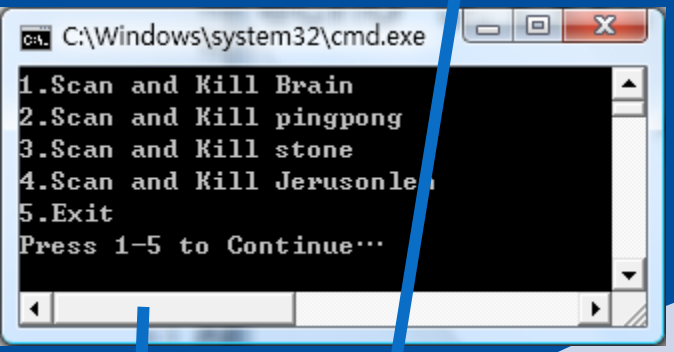
2008/09/21 中国上海

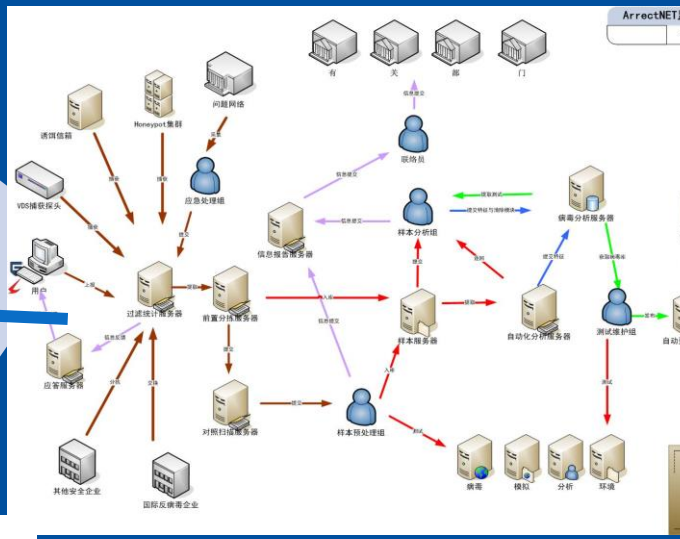
提纲

- AV演进律
- 黑云压城
- 网络反病毒的炼狱
- 终端覆巢下
- 蜜罐生与死
- 总结

AV演进

alert boot (msg"virus-Brain"; content:" |A1 13 04 2D 07 00 A3 13 04 B1 06 D3 E0 8E C0|";)
alert boot (msg"virus-pingpong"; content:" |A1 13 04 2D 02 00 A3 13 04 B1 06 D3 E0 2D C0|";)



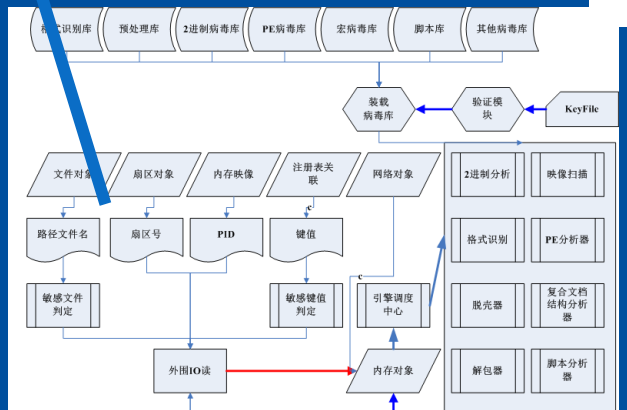


体系建制

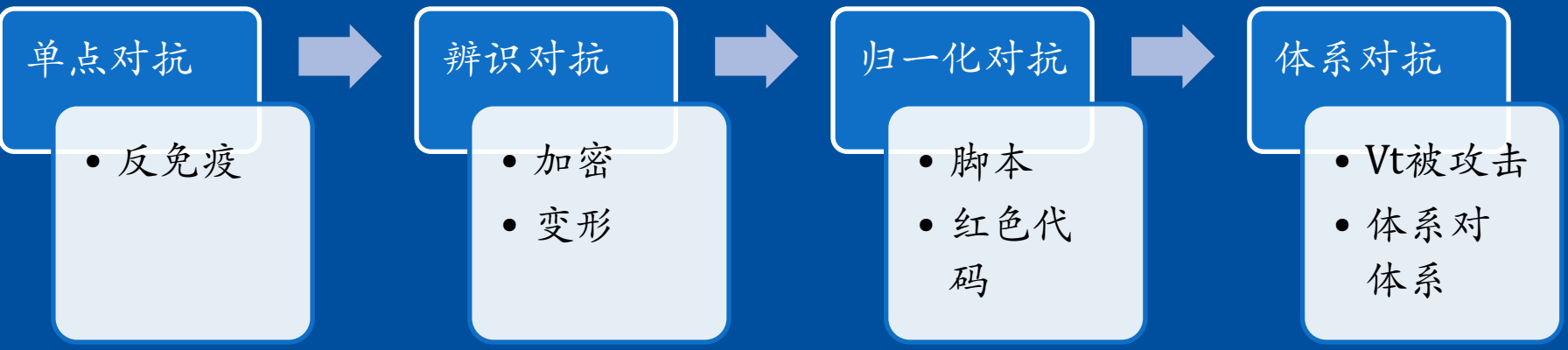
归一化

规则化

单点
对抗



挑战与对抗的同步演进



基本演进方法

直接对抗	• 专杀
功能增加	• Regmon/TDI mon
归纳-归一化	• 从AntiOOB到PFW
回流	• 免疫
前后台转化	• 基于神经网络/决策树未知检测
引入	• UTM增加AV Engine
硬件（设备）化/软件化	• 防毒卡-〉反病毒软件
……	

提纲

- AV演进律
- 黑云压城
- 网络反病毒的炼狱
- 终端覆巢下
- 蜜罐生与死
- 总结

谁在天堂，谁在地狱？

- AV
- 人员数量持续增长
- 捕获体系持续扩大
- 投入不断增加

- VX
- 在2005年之前，出现多个在几天内感染节点数量达到千万的病毒（单变种计算）。
- 而在2005年之后，几乎没有感染数量超过百万的病毒（单变种计算）

2001 VS 2005

	个数	NAV	Panda	Pccillin	MCAFEE	RAV	KAV
Wildlist	156	137	148	154	155	61	154/154
Supplemetal	113	97	101	107	112	38	106/108
Other	4	4	4/4	4	3	1	4
总计	273	238	253	265	270	100	266

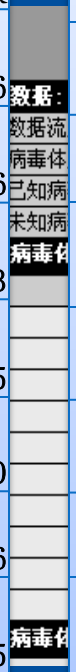
2001年 Popsoft 横向测试，样本取自安天ASTS#6 00-01年度流行库

	个数	江民KV	瑞星	金山	Pc-cillin	诺顿
bot	46	34	31	40	41	40
病毒	21	21	18	17	19	21
黑客工具	39	27	26	27	14	14
间谍软件	6	4	5	3	1	3
木马	281	179	212	206	153	206
蠕虫	31	28	28	28	28	30

2005年 CHIP横向测试，样本取自安天ASTS#6 04-05年度流行库

数量与分布： 2003 vs 2008

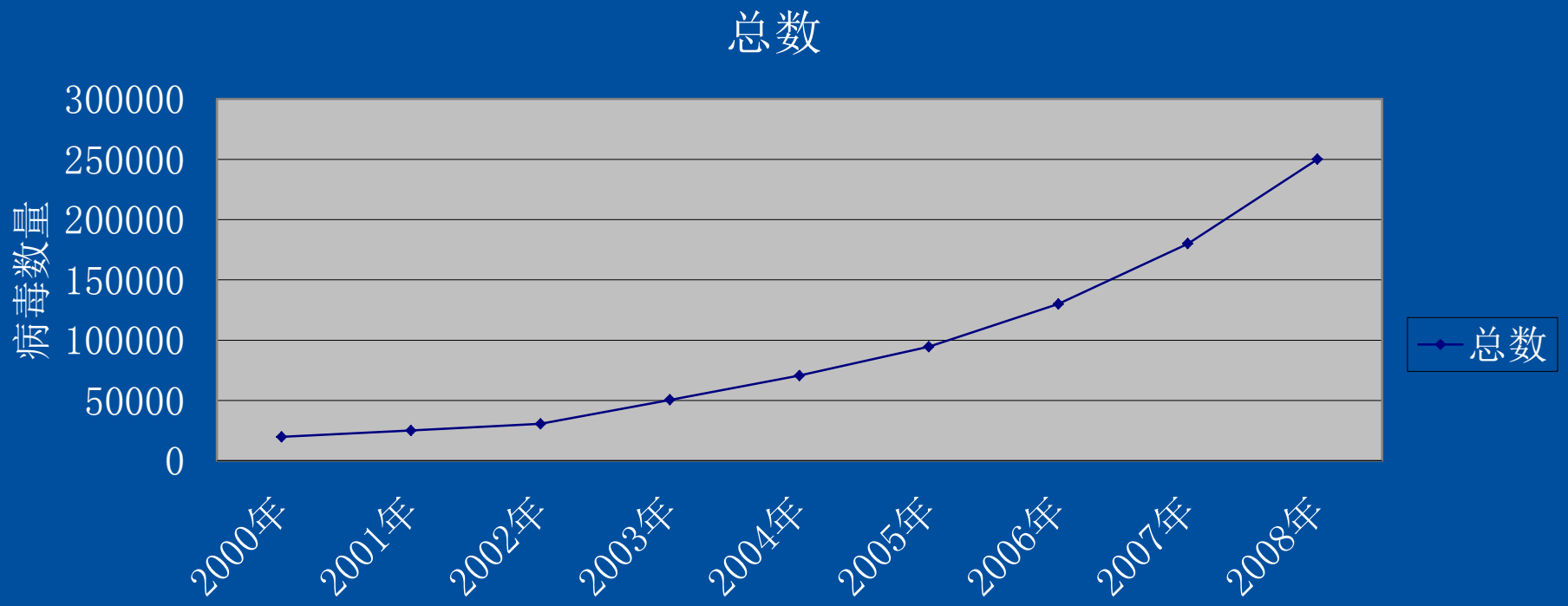
排名	病毒名	7日均数
1	Trojan-Downloader.Win32.Small.suu	50746
2	Trojan-Dropper.Win32.Agent.qgb	50346
3	Trojan-Downloader.Win32.Agent.mkj	20453
4	Trojan.Win32.Agent.iqq	14825
5	Trojan.Win32.KillAV.qo	12690
6	Trojan-Downloader.Win32.Injecter.io	9606
7	Trojan-PSW.Win32.OnLineGames.ynj	9555
8	Trojan-PSW.Win32.OnLineGames.ynd	8276
9	Trojan-PSW.Win32.OnLineGames.ymk	7622
10	Trojan-PSW.Win32.OnLineGames.yvt	7464



排名	病毒名	7日均数
491	Trojan-Clicker.Win32.Delf.cy	121
492	Virus.Win32.AutoRun.z	121
493	Trojan-PSW.Win32.OnLineGames.yml	120
494	not-a-virus:AdWare.Win32.Yokbar.n	120
495	Trojan-PSW.Win32.OnLineGames.tll	119
496	Trojan-PSW.Win32.WOW.arq	119
497	Trojan-PSW.Win32.OnLineGames.cyp	119
498	Trojan.Win32.LaSta	119
499	Trojan-PSW.Win32.OnLineGames.zeb	118
500	Trojan-Spy.Win32.FtpSend.a	118

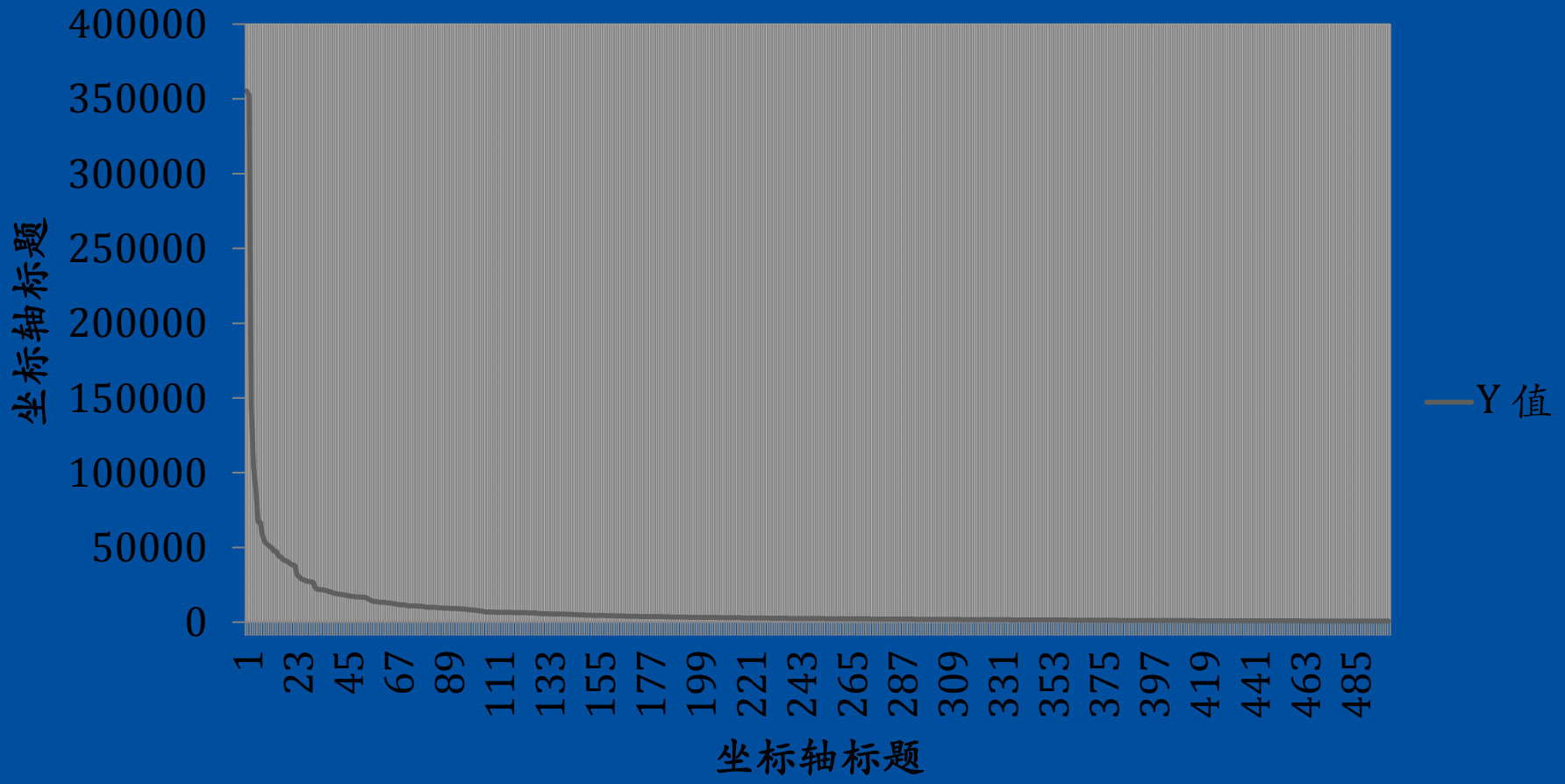
数据来源：20084月1日-7日
ArrectNET全网监控体系统计

数量与分布：病毒总数增长趋势

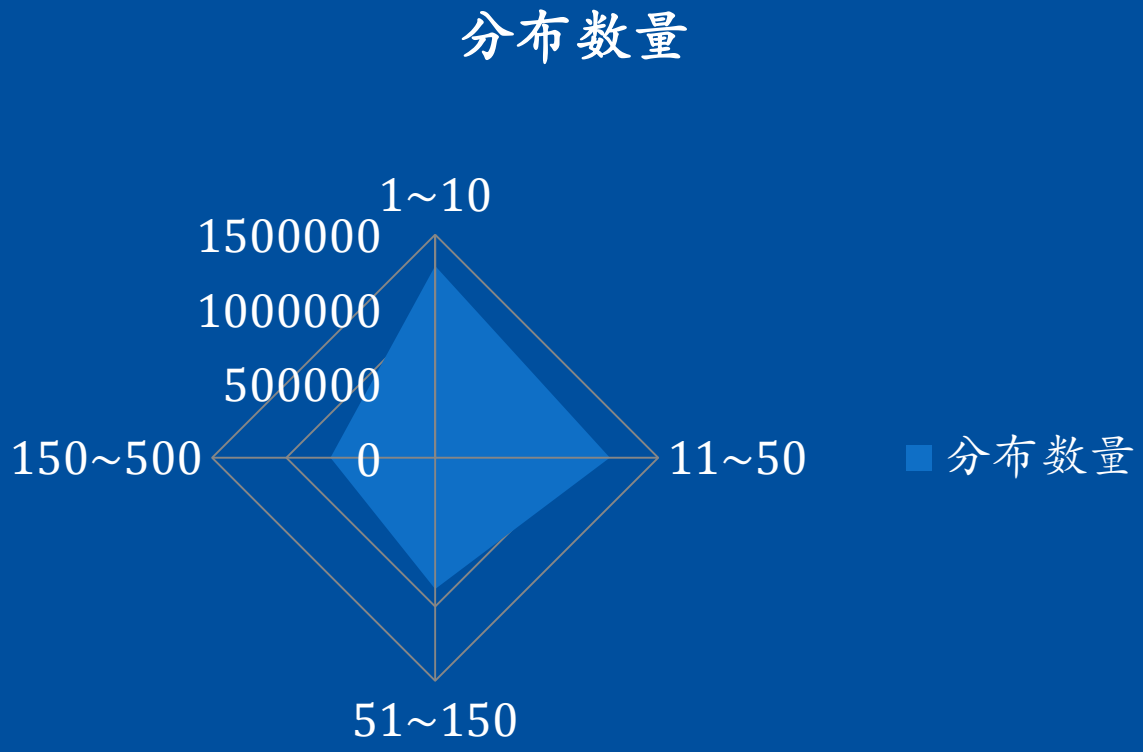


根据统计：从1986年第一个PC病毒产生到2000年底的15年，全球共产生了19836种病毒。而预计到2008年底病毒总数可能突破25万种。

数量与分布：超级长尾



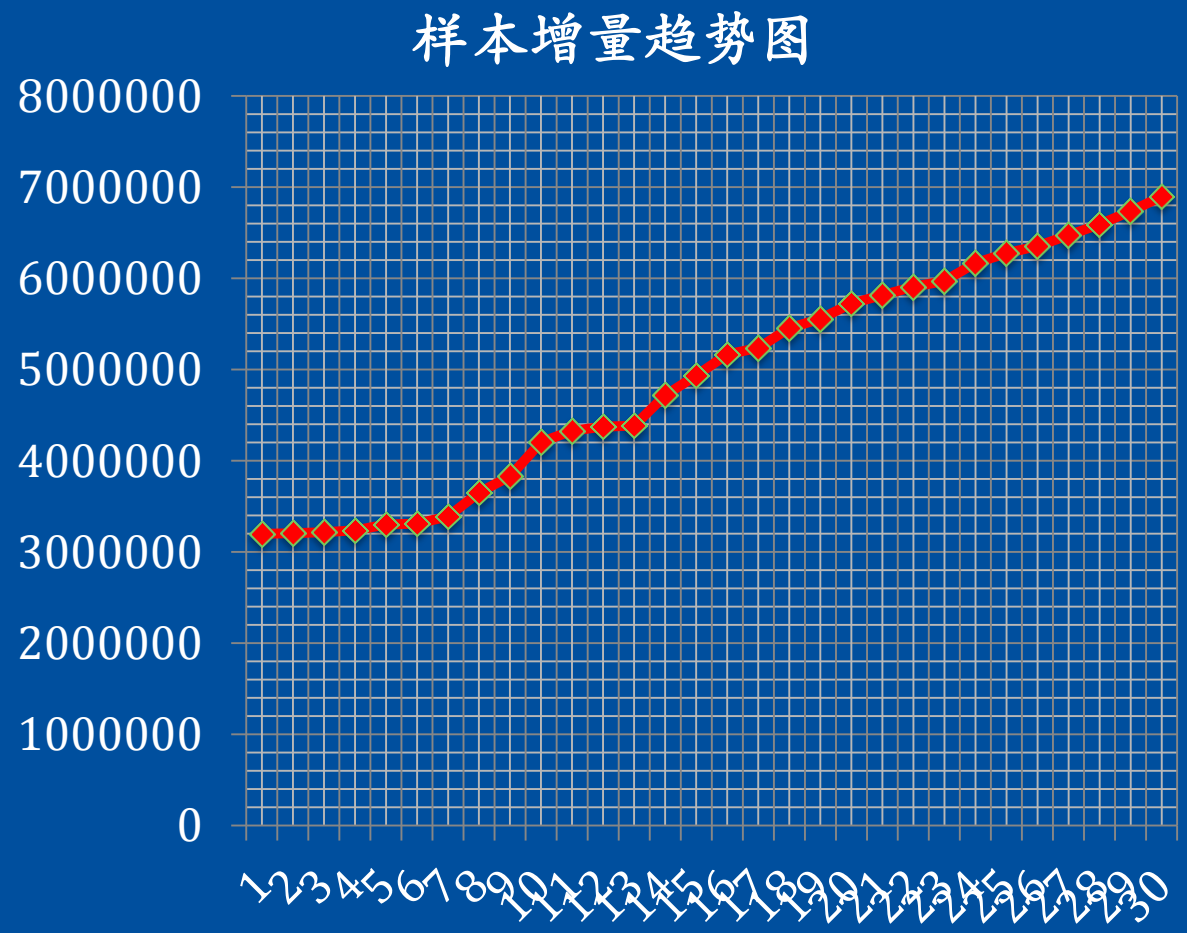
数量与分布：小众化



排名	分布数量
1~10	1288822
11~50	1174053
51~150	883269
150~500	703925

2008的数量膨胀

时间	样本数量
2008.03.01	3198418
2008.03.08	3203641
2008.03.15	3214524
2008.03.22	3235268
2008.03.29	3301003
2008.04.05	3311228
2008.04.12	3387375
2008.04.19	3652374
2008.04.26	3830092
2008.05.03	4204444
2008.05.05	4326955
2008.05.10	4372122
2008.05.17	4382715
2008.05.24	4716174
2008.05.31	4936402
2008.06.07	5165593
2008.06.14	5236535
2008.06.23	5454057
2008.06.28	5556308
2008.07.05	5723758
2008.07.12	5816720
2008.07.19	5906967
2008.07.26	5969311
2008.08.02	6166699
2008.08.09	6275924
2008.08.16	6354377
2008.08.23	6472529
2008.08.30	6593113
2008.09.06	6736621
2008.09.13	6898377



威胁衍生

提纲

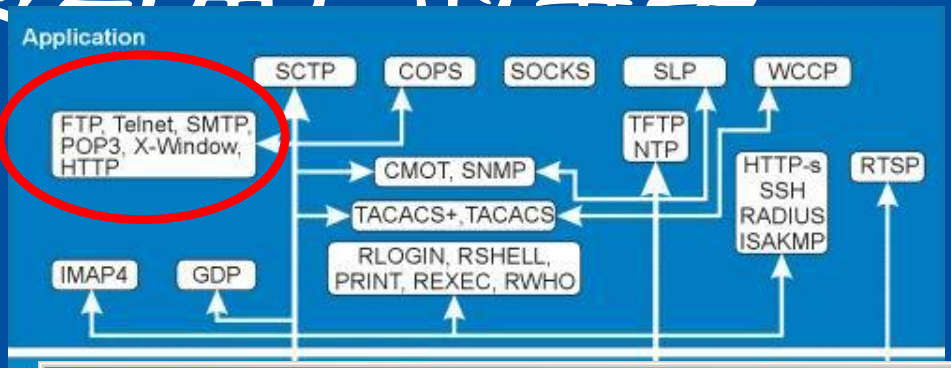
- AV演进律
- 黑云压城
- 网络反病毒的炼狱
- 终端覆巢下
- 蜜罐生与死
- 总结

01-08的演进图

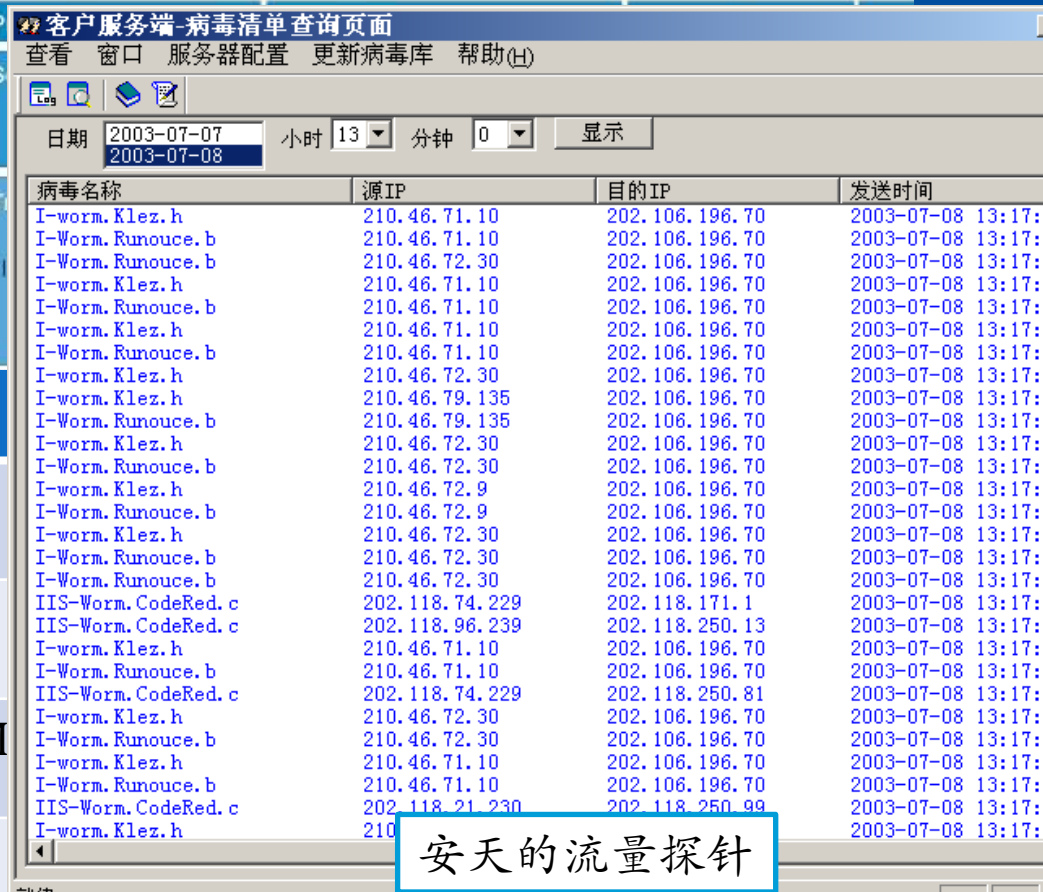
- 1995年，趋势InterScan VirusWall
- 1998，开源IDS系统，snort
- 2000，安天，P-A，全规则病毒检测，zerocopy、并行协议栈应用
- 2007年，卡巴斯基，GPU AV 加速卡

彩页的宣传与用户的事实

- 协议
- 行为与威胁
- 带宽
- 表现
- 效果



产品名称	速率
Iss Proventia M50*	178Mbps
Panda gatedefender 8200*	167Mbps
Fortigate 3600*	200~225M
援引自NSS Group测试数据	



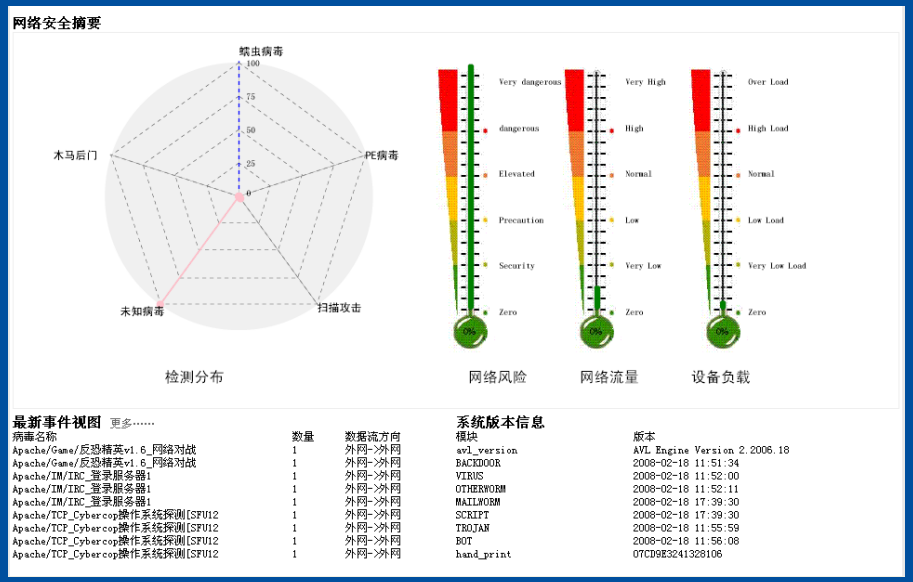
演进-〉速度

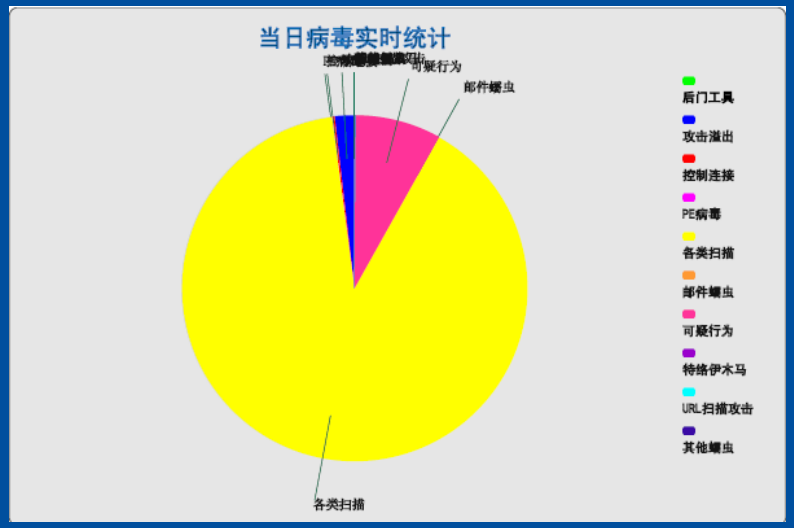
- 算法
  - KMP->单模BM->多模BM
- 加速
  - 算法的优化，减少入口进入
- 剪裁
  - 如何形成更有效的流行规则

演进->应对威胁

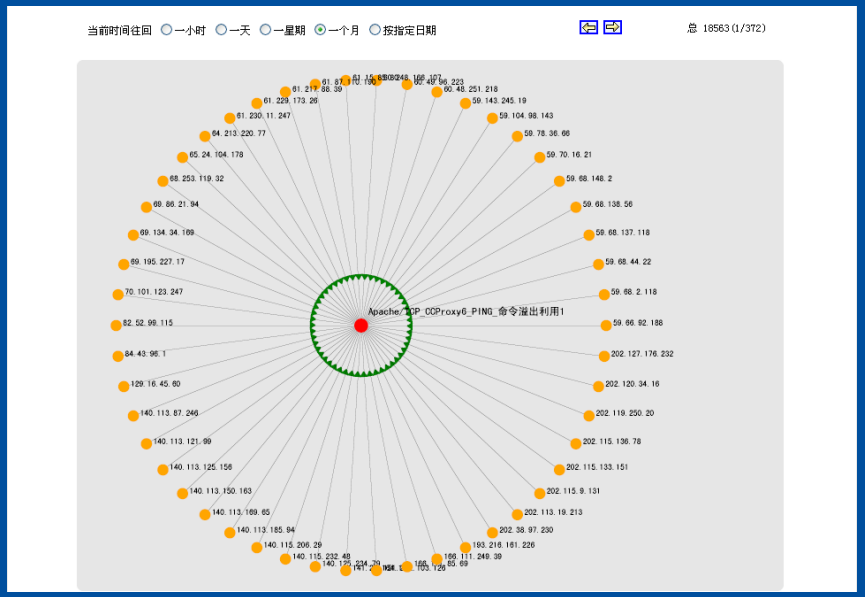
- 演示

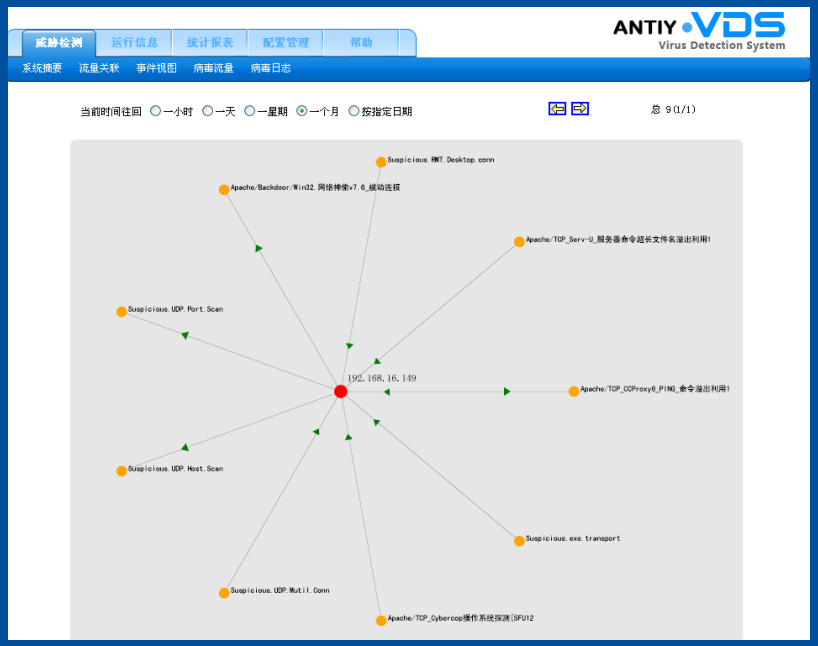
演进->探索表现

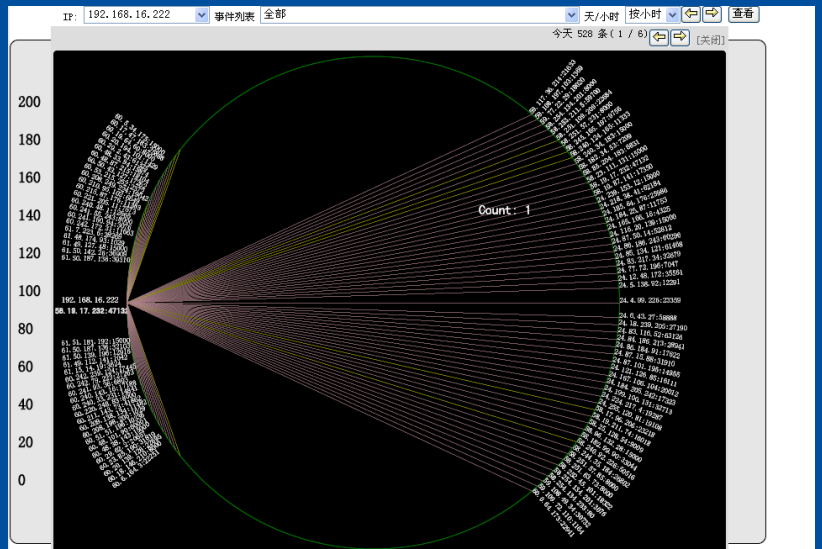




演进->探索方法



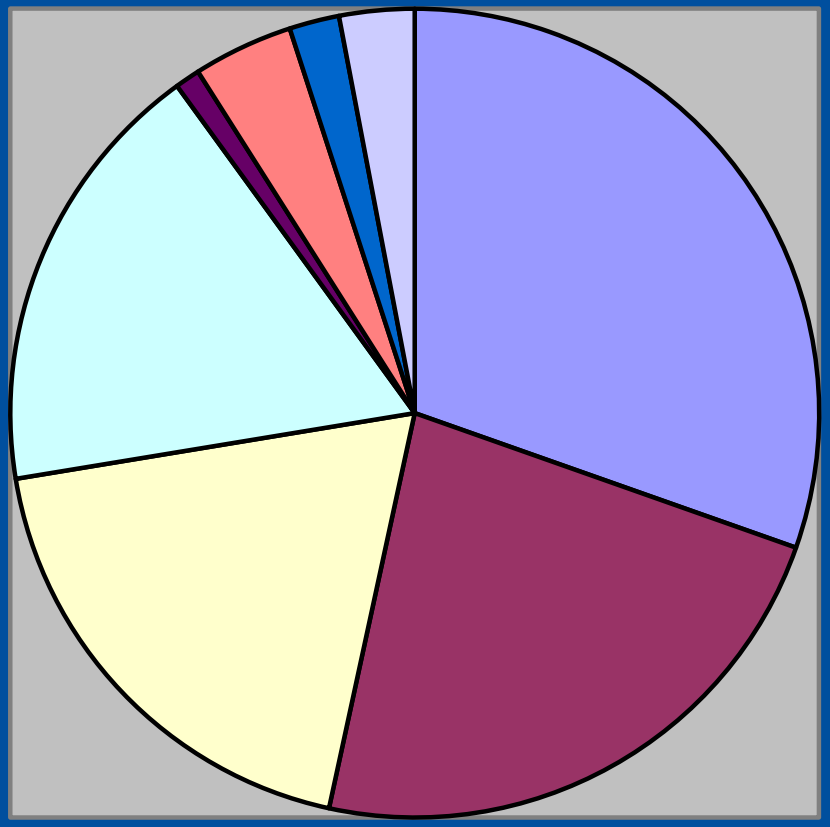




提纲

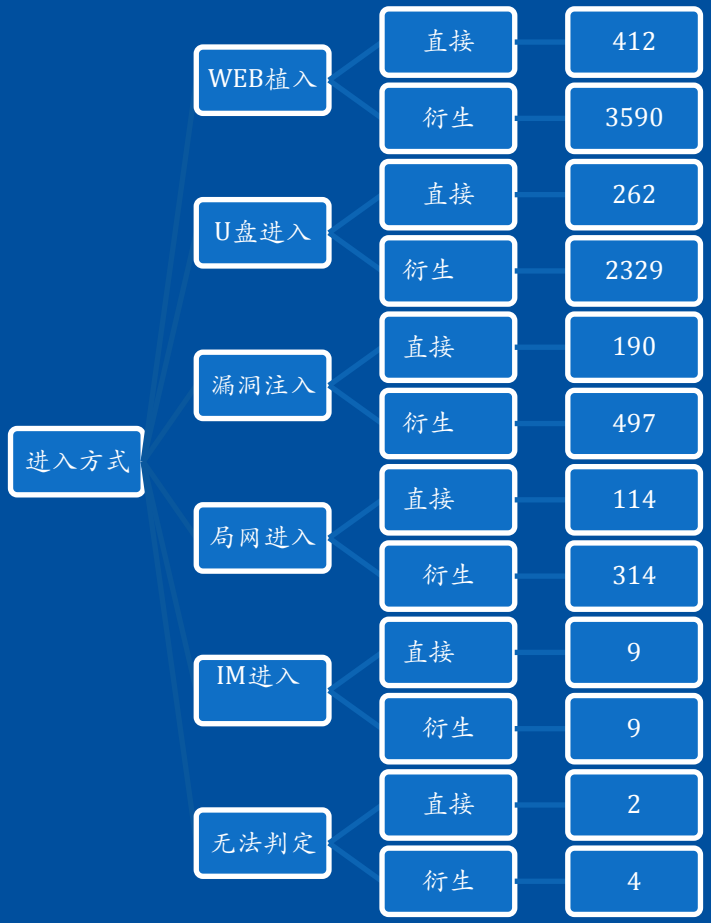
- AV演进律
- 黑云压城
- 网络反病毒的炼狱
- 终端覆巢下
- 蜜罐生与死
- 总结

传播途径：木马是怎么来的



2006年，309例主机木马感染问题跟踪统计。

传播途径：木马是怎么来的（续）



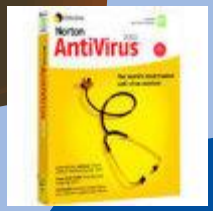
2008年，安天针对7732例样本进入主机方法的细粒度审计。

蔡中案过程

Port:7618

Port:15440

nihao20060808.vicp.net:7619



7分钟

再回犯罪现场

淘宝网 Taobao.com

信息安全每一天

作案手法：精工细作

创建

IP地址
本机信息:操作系统版本
计算机名
工作组
用户名
IE版本
DX版本
CPU速度
物理内存数
屏幕分辨率
开机时间

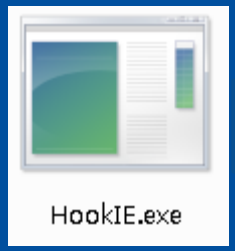
Net localgroup administrators guest /add
net user guest 123

[AutoRun]\r\n
open=svr.exe\r\n
shellexecute=svr.exe\r\n
shell\\Auto\\command=svr.exe\r\n

KEYLOG.....

伪

NETSEND



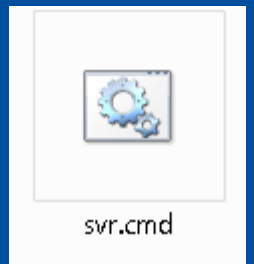
解包

创建

伪装

伪装

伪装



TCP:15440

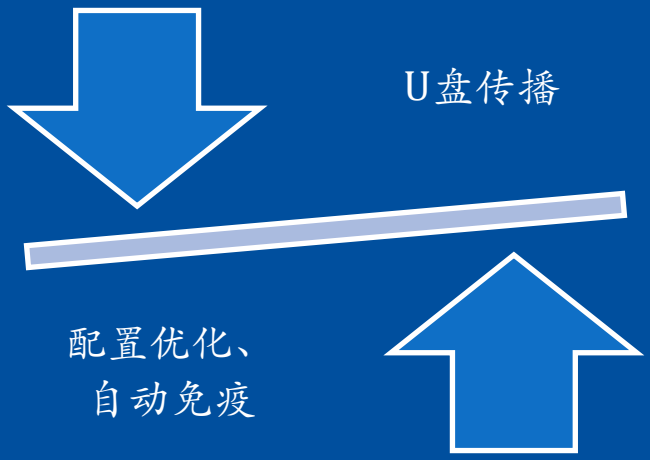
桌面面临什么

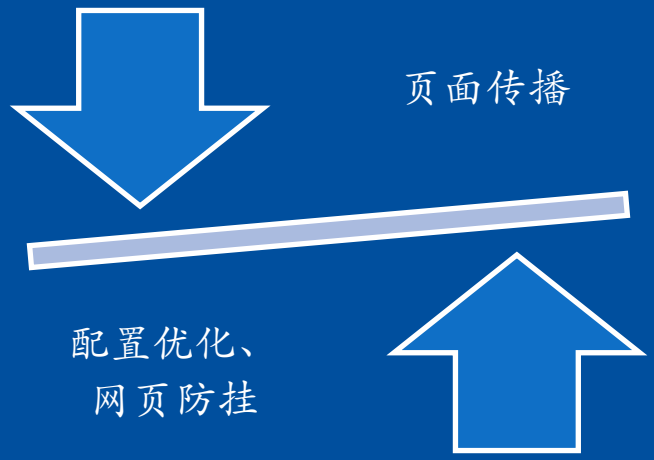
- Anti-AV技术已经高度模块化——一点突破全局崩溃
- Rootkit技术已经逼近极限——一旦进入，即难查出
- 单机链式反应已经不可控——一个程序运行，数十木马执行
- 个案细作——个性化植入方案，超出AV团队采集和分析能力

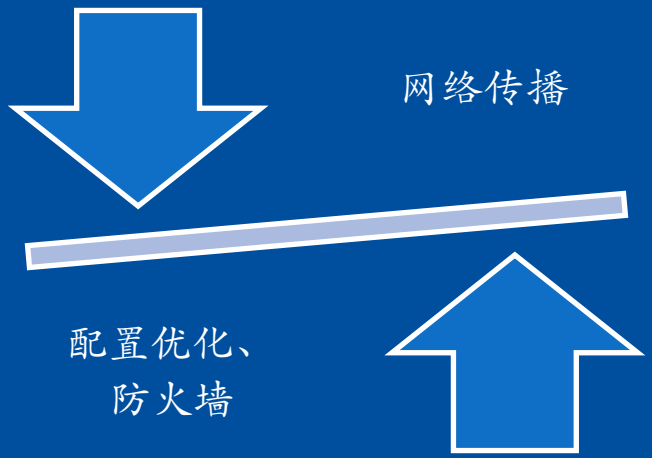
主动防御之生

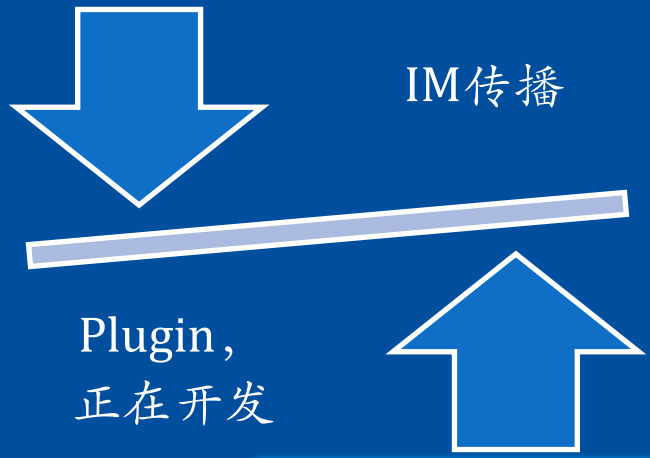
- 主动防御技术本来就是从实时检测发展起来的，却被被当作噱头，而站到特征码技术的对立面。其把行为识别和未知辨识当作key。以为没有已知能力能解决所有问题——幼稚啊！
- 主动防御技术的核心本质，不是智能辨识与处理，而且切断“数据->指令”的链条，和止损“指令”的后果。

从威胁出发的防护





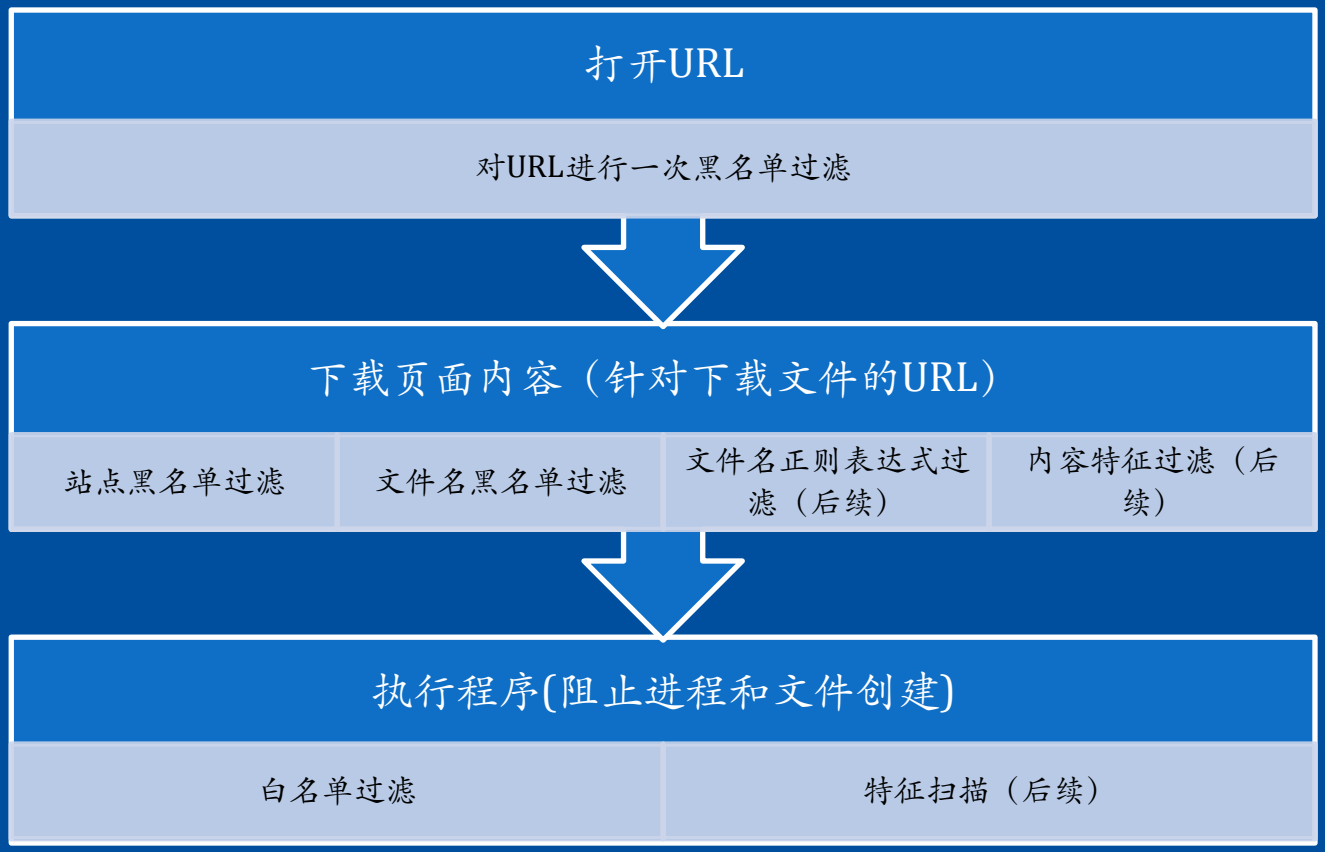




长路漫漫

- 演示当前主流反挂马技术的脆弱性。

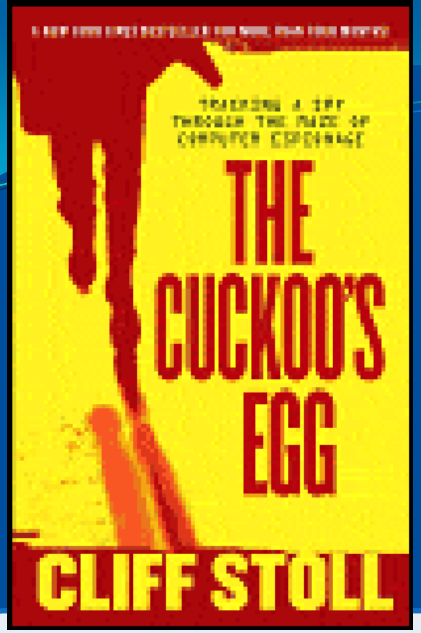
我们的方法：欢迎测试



提纲

- AV演进律
- 黑云压城
- 网络反病毒的炼狱
- 终端覆巢下
- 蜜罐生与死
- 总结

蜜罐演进史



1990-1998

- The Cuckoo’s Egg

1998-2000

- DTK
- Honeyd

2000-2006

- Honeywall CDROM
- Sebek
- Nepenthes
- Capture-HPC
- HoneyC

谁动了我的蜜罐？

- 2003年，安天每日单点蜜罐有效样本获取数量为从20-30个
- 2008年，下降到3-5个。

终端安全趋势的挑战

- DEP、ASLR带来的强大保护能力，极大遏制了针对系统服务的扫描溢出攻击的空间。
- 漏洞从被蠕虫利用，转入黑产定向攻击牟利。
- 静态格式溢出、浏览器和其他客户端传播成为主流。
- 蜜罐的基本存在场景合理性受到了威胁。

核心挑战

- 蜜罐的工作基础是模拟定点目标，守株待兔式的手段。
- 主流攻击链路不以IP为主导，让局面趋于复杂化。原有的大面积扫描、注入正在变成撒网捞鱼式的攻击。

全活动内容上报的挑战

- 典型的上报体系：OSLoader、驱动、服务、进程、模块、IE插件等。
- 海量文件上报+数据频度统计+未知判定+自动化分析机制

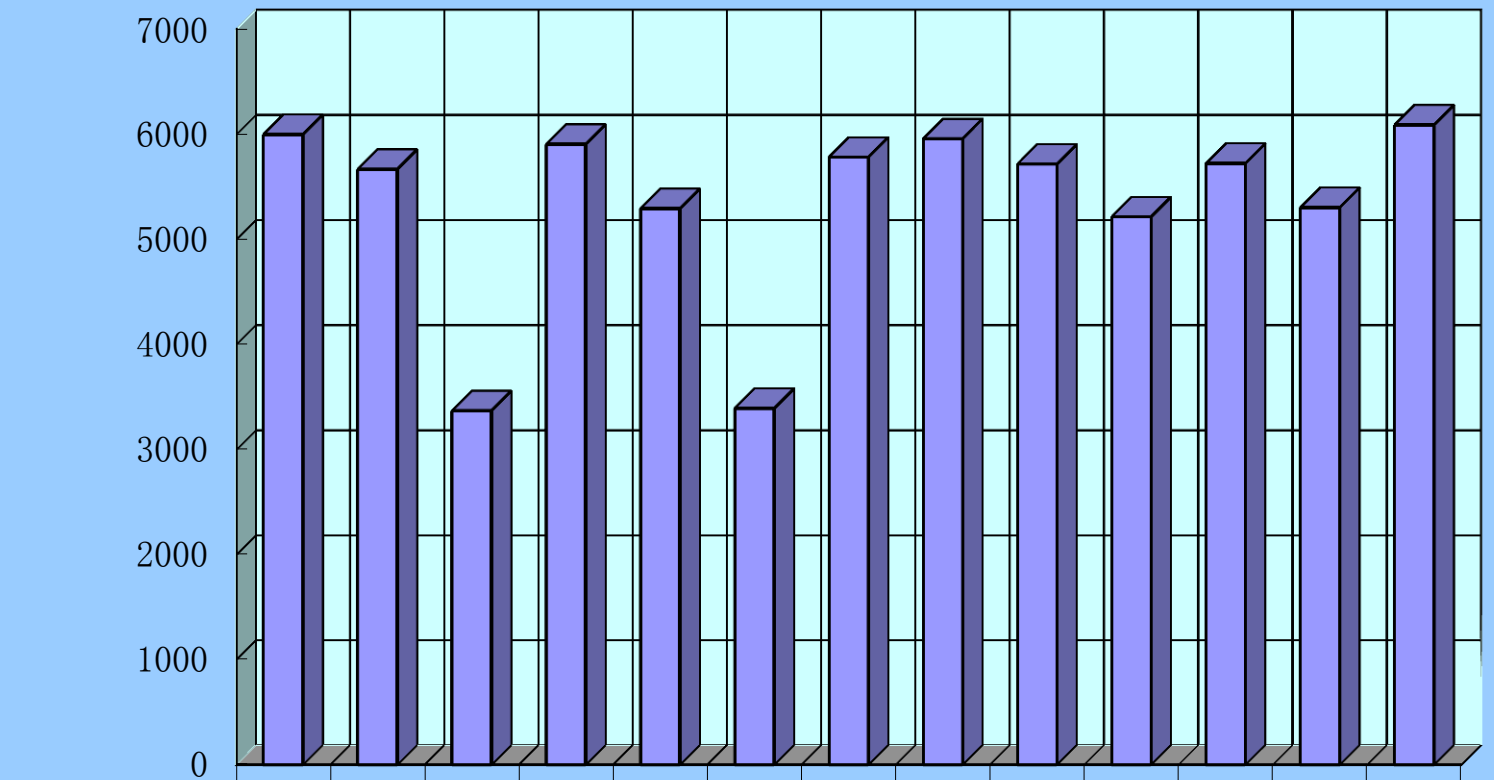
一些代表性的主要分布式上报分析体系

- MS的上报体系
- Eset（NOD32）ThreatSense.Net
- 安天 ArrectNET
- 瑞星“云”计算
- 360safe进程上报体系

挑战点

- 桌面安全产品、安全客户端无以伦比的基础数量规模。
- 实际活动内容。
- 设备和硬件资源零成本。
- 分布式计算零成本

全进程（模块）上报技术对检测率的改善



	安天防线	江民	费尔	金山	驱逐舰	安铁诺	瑞星	avast	NOD32	Norton	趋势	麦咖啡	Kaspersky Anti-Virus
查杀个数6178	6001	5670	3374	5908	5296	3396	5786	5961	5720	5219	5727	5306	6091

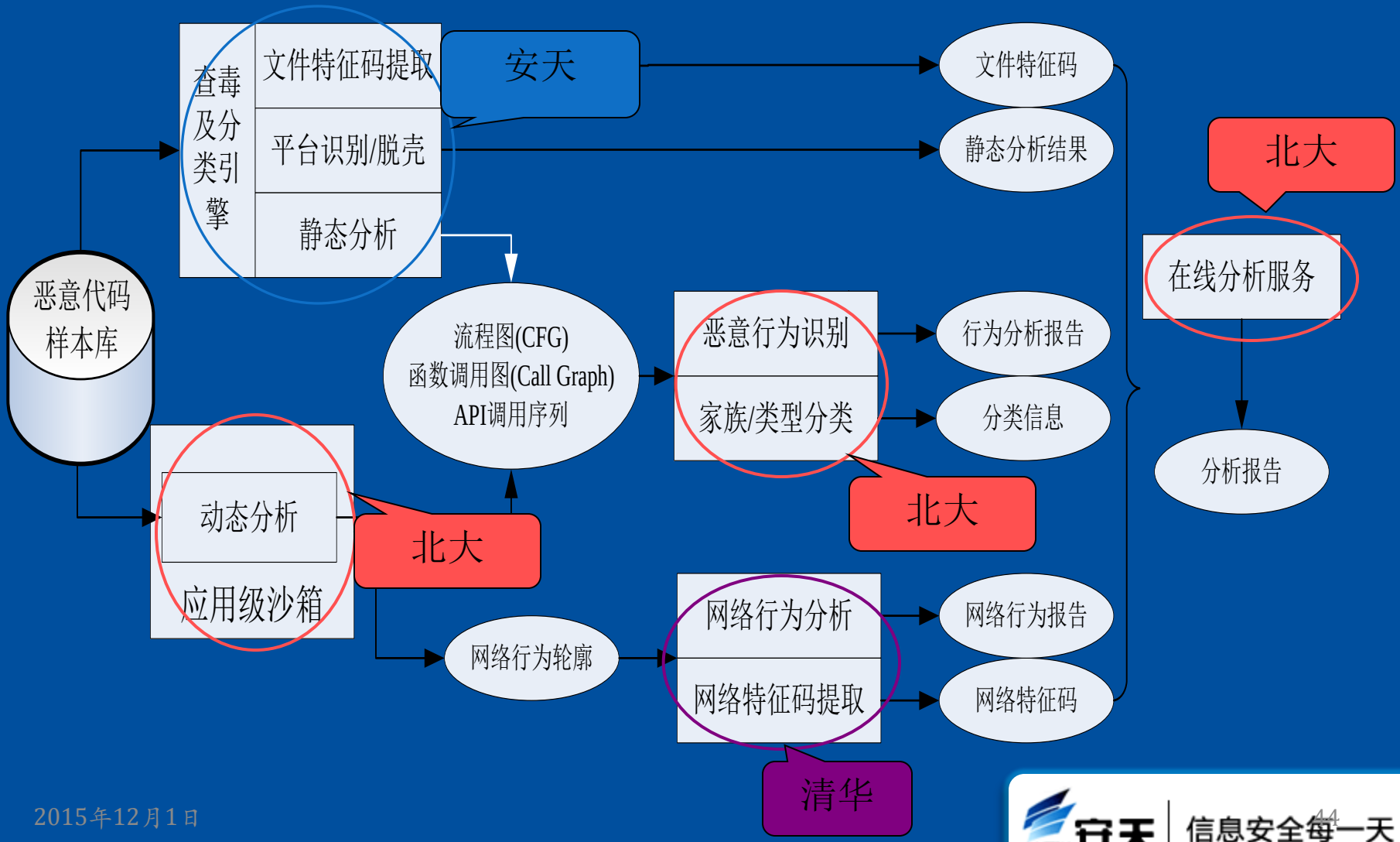
演进-前台->后台

- 趋势——WEB挂马挑战
- 为什么需要样本养殖。（不完备提取、经常变化）
- 样本养殖的主要来源。

样本养殖和分析体系

- 与安天挂马探测体系（猎狐、安天防线）配套的养殖体系
- 北大、清华、安天：自动化行为分析特征提取的研究。
- 公安部上海三所、安天、华师大：海量自动化分析研究

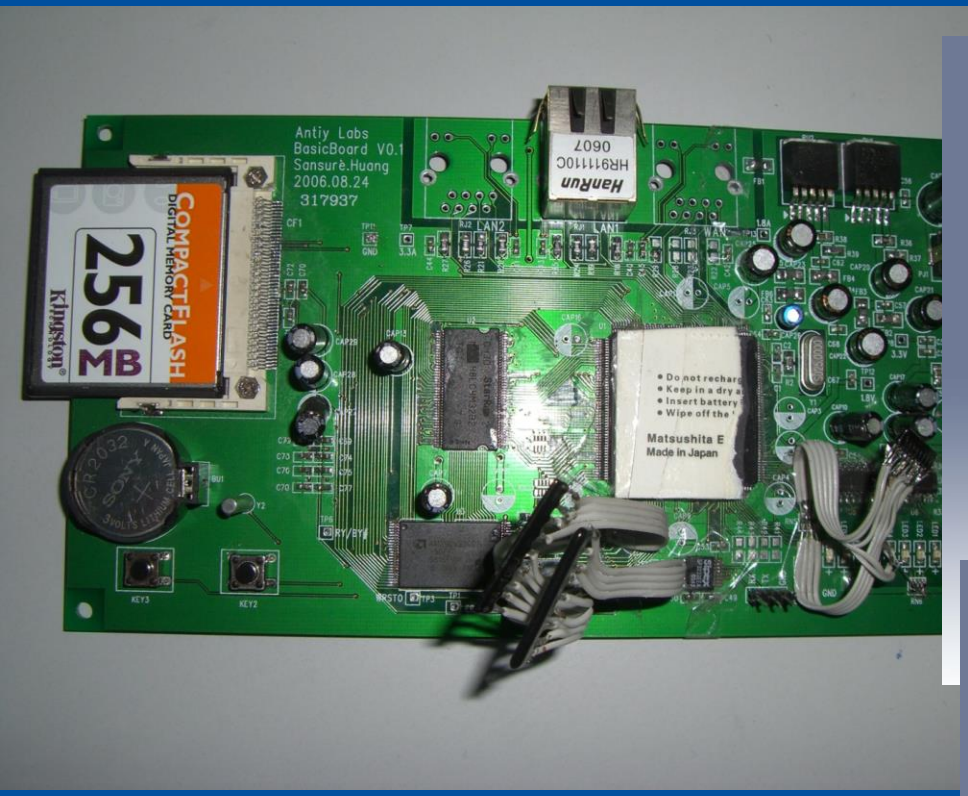
自动化行为分析特征提取研究



演进->设备化

- 实物演示。
- 电路设计介绍
- 软件体系介绍

演进：电信级别密网——蜜池



产品级蜜罐想象图

演进:表现与管理

月度	攻击数量	NO.1漏洞
2008-7	29	MS04-011
2008-6	96	MS03-051
2008-5	102	MS03-039
2008-4	38	MS04-012

今日统计 | 昨日统计

独立源IP个数:132个	捕获样本总数:67个	病毒类别:总数量
网络攻击事件总数:1,223次	捕获新增样本总数:12个	Trojan:780个
库中网络攻击总流量:384.24MB	库中样本总数:1,434个	Backdoor:120个
		Worm:780个
		HackTool:120个
		SpamTool:12个
		Other:128个

当前互联网威胁状况

提纲

- AV演进律
- 黑云压城
- 网络反病毒的炼狱
- 终端覆巢下
- 蜜罐生与死
- 总结

题记

- 每天，当太阳升起来的时候，非洲大草原上的动物们就开始奔跑了。**狮子**妈妈在教育自己的孩子：“孩子，你必须跑得再快一点，再快一点，你要是跑不过最慢的**羚羊**，你就会活活地饿死。”在另外一个场地上，**羚羊**妈妈也在教育自己的孩子：“孩子，你必须跑得再快一点，再快一点，如果你不能比跑得**最快的狮子**还要快，那你就肯定会被他们吃掉。”

题记续

- 而20年来，AVER者们顽强奋争着，在操作系统和信息体系巨变的颠簸舞台上起舞，清理淘汰着攻击威胁和恶意代码的挑战，也被对手所挑战和淘汰着，同时也应付着来自内部阵营的暗箭。
- 也许天下无毒是我们无法达成的目标，但却是我们的信仰。

谢谢大家

- seak@antiy.net