蜜罐技术与分布式蜜罐网络

安天实验室 肖新光

2005年3月

提纲

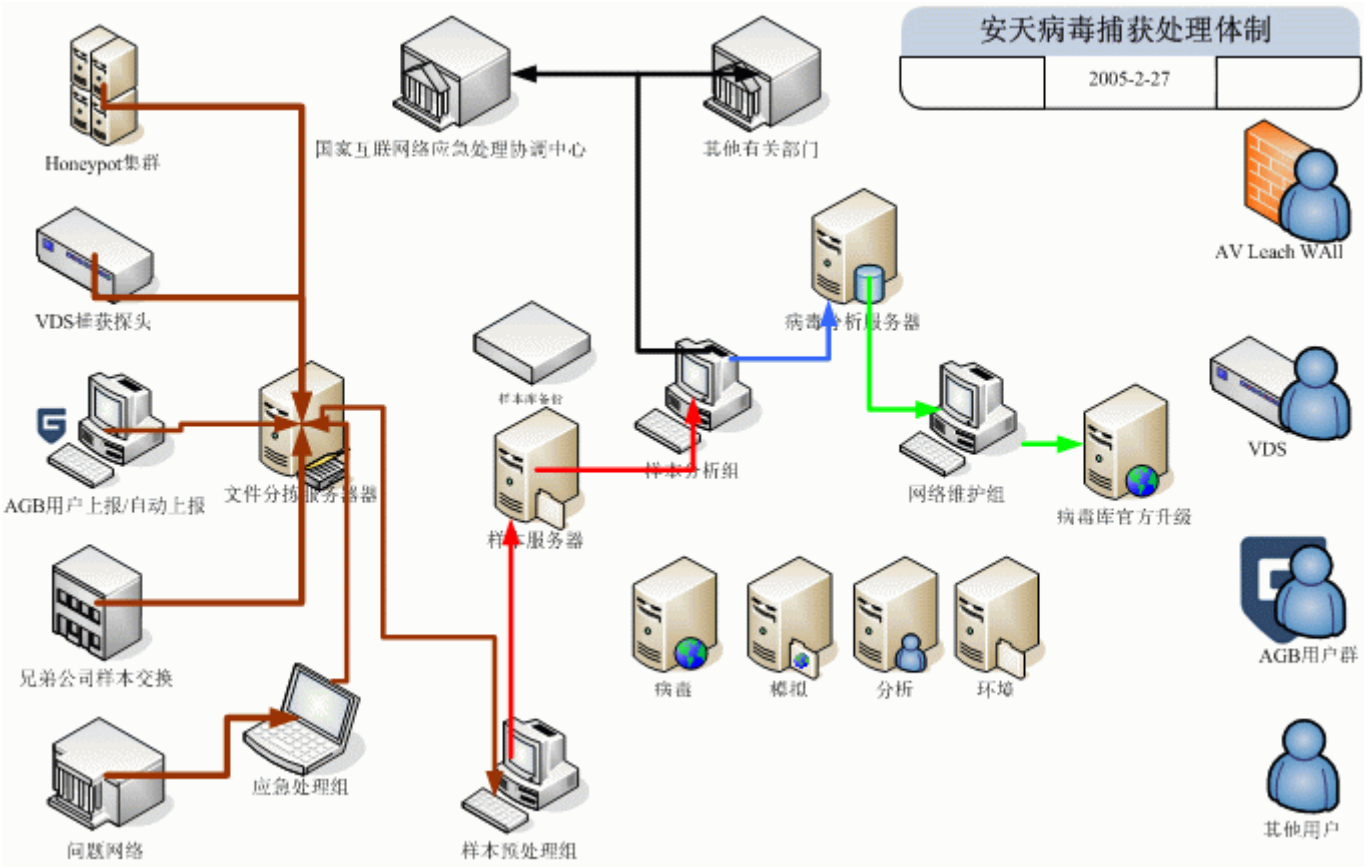
- 蜜罐对蠕虫捕获的价值
- 蜜罐节点实现
- 分布式蜜罐网络与后端分析体制

蜜罐对蠕虫捕获的价值

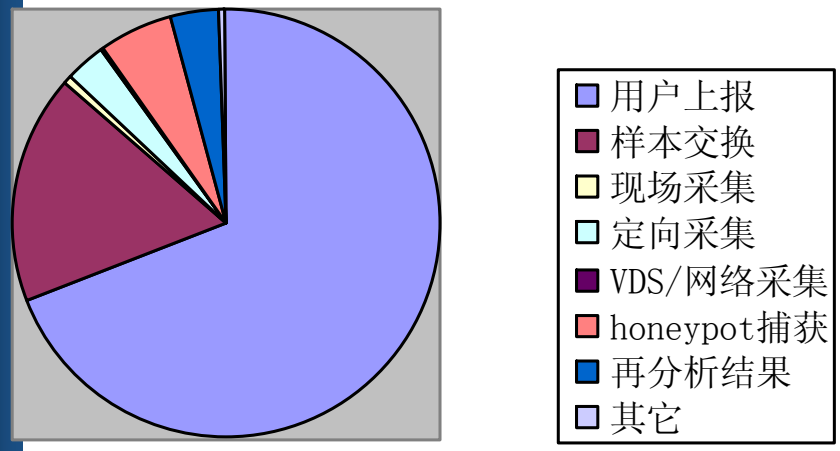
蜜罐与蠕虫捕获

- 蜜罐的与反病毒领域的结合趋势始于2002年，成熟于2004年。
- 与传统蜜罐诱捕与迟滞攻击的作用不同，用于蠕虫捕获的蜜罐完全以获得蠕虫样本为目的。
- 用于蠕虫捕获的蜜罐系统主要针对获取系统控制权且主动传播的扫描溢出/口令猜测型蠕虫样本，使这些蠕虫扫描到蜜罐节点的时候，其样本文件或其他载体形态被获取。

安天病毒捕获流程


安天病毒捕获处理体制
2005-2-27
Honeypot集群
国家互联网络应急处理协调中心
其他有关部门
AV Leach WAll
VDS捕获探头
病毒分析服务器
VDS
AGB用户上报/自动上报
文件分拣服务器
样本分析组
网络维护组
病毒库官方升级
样本服务器
兄弟公司样本交换
病毒
模拟
分析
环境
AGB用户群
应急处理组
问题网络
样本预处理组
其他用户

安天最近7032个样本来源统计



用户上报	68.84%
与国外AV企业交换	17.50%
现场采集	0.50%
定向采集	3.31%
VDS/网络捕获	0.27%
Honeypot捕获	**5.4%**
再分析结果	4.61%
其他	0.52%

不同样本渠道比较

	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。
VDS/网络采集	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**

蜜罐的价值

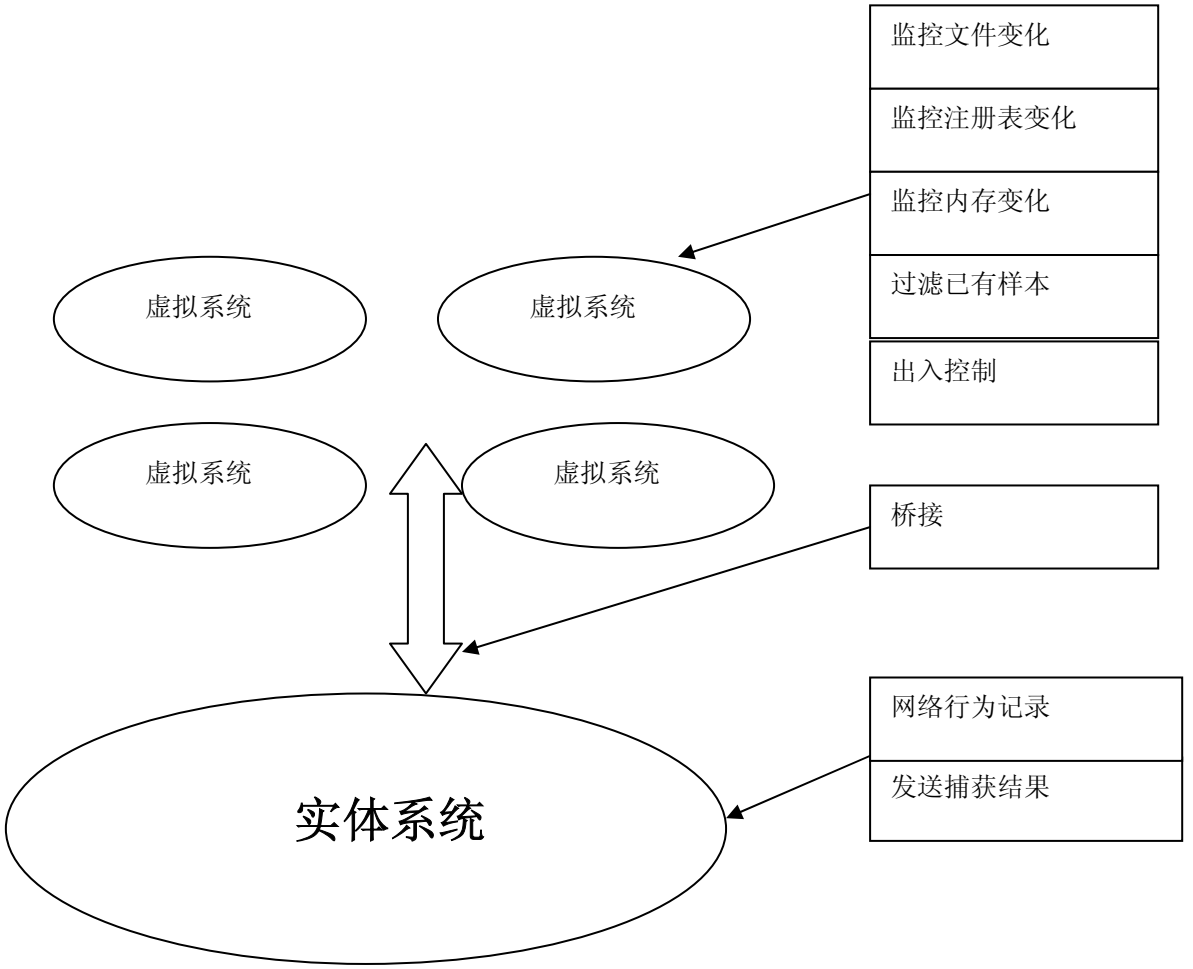
- 蜜罐体系是安天ArrectNET监控网络的重要组成部分，蜜罐获取样本的绝对种类数不大，但意义非凡。
- 蜜罐主要的价值是：第一时间捕获流行的扫描型蠕虫，我们第一时间截获冲击波、震荡波以及他们的变种都依赖于蜜罐体制。
- 此外，蜜罐具有统计意义，能够对流行情况/节点压力进行比较准确的判断和分析。

蜜罐节点的实现

蜜罐的技术要求

- 获得样本
- 记录网络行为、保存系统行为
- 扫进不能扫出，避免成为再感染源和跳板
- 发现新的文件和进程变化
- 排除已有蠕虫
- 发送新文件和内存映像

Antiy Honey pot的结构



技术基础

- AV Leach SDK，细粒度可嵌入的反病毒引擎，全面的病毒检测能力，进行已知病毒过滤
- 单机防火墙技术，程序行为控制，网络出入控制。
- 文件/内存/注册表监控技术。

节点技术的探索

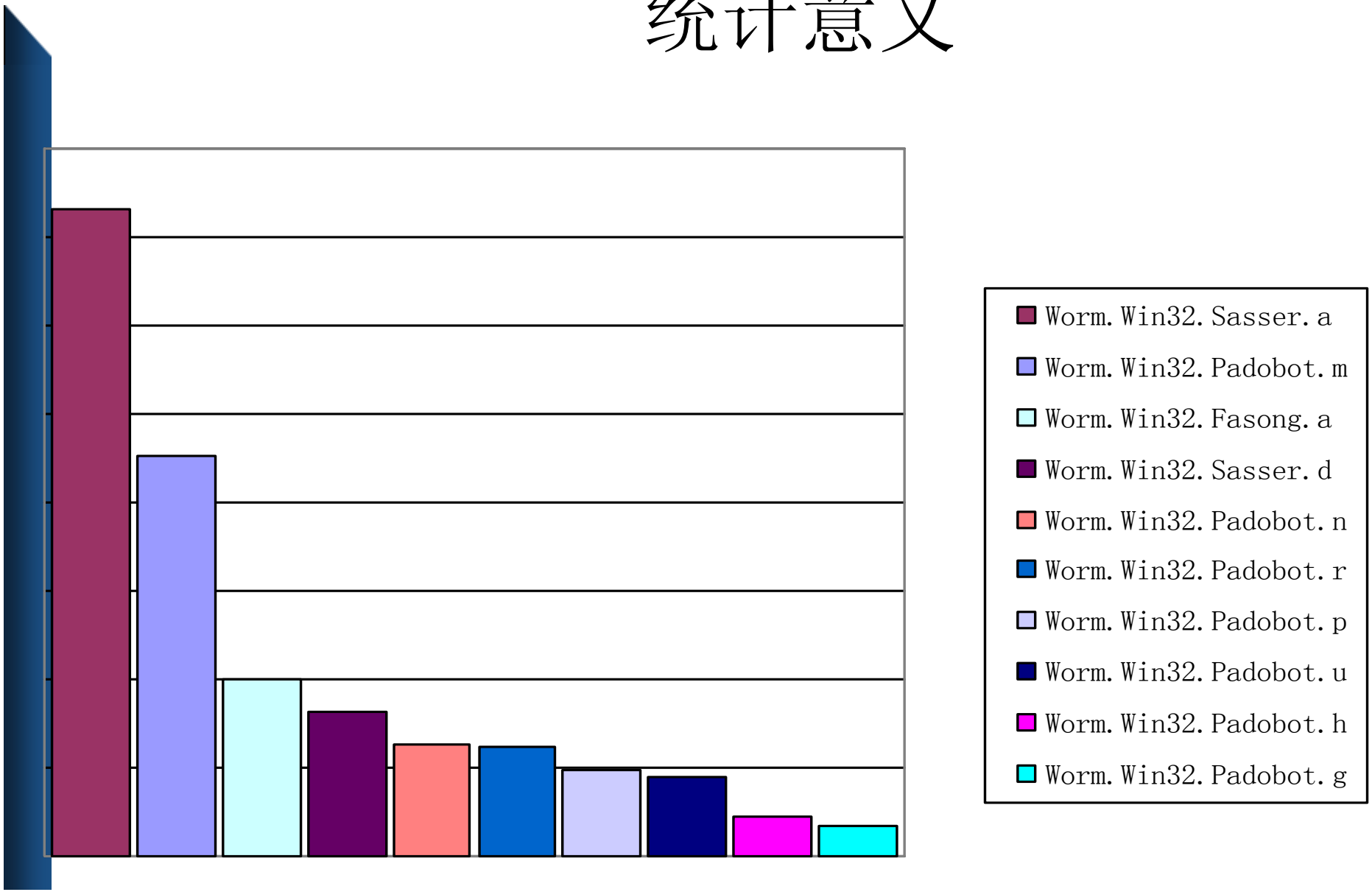
- AI Pot，安天新一代蜜罐。
  通用载体平台
  主动行为模拟
  深度环境构造
  主动应答

分布式蜜罐网/后端分析体制

为什么需要分布式体系

- 蜜罐系统的捕获能力来自于其足够的数量和分布范围
- 统计意义。
- 问题：
- 蜜罐数量的增加带来上报数量的增加，但也相应增加了分析处理的压力。
- 同时维护的压力也大大增加。

统计意义

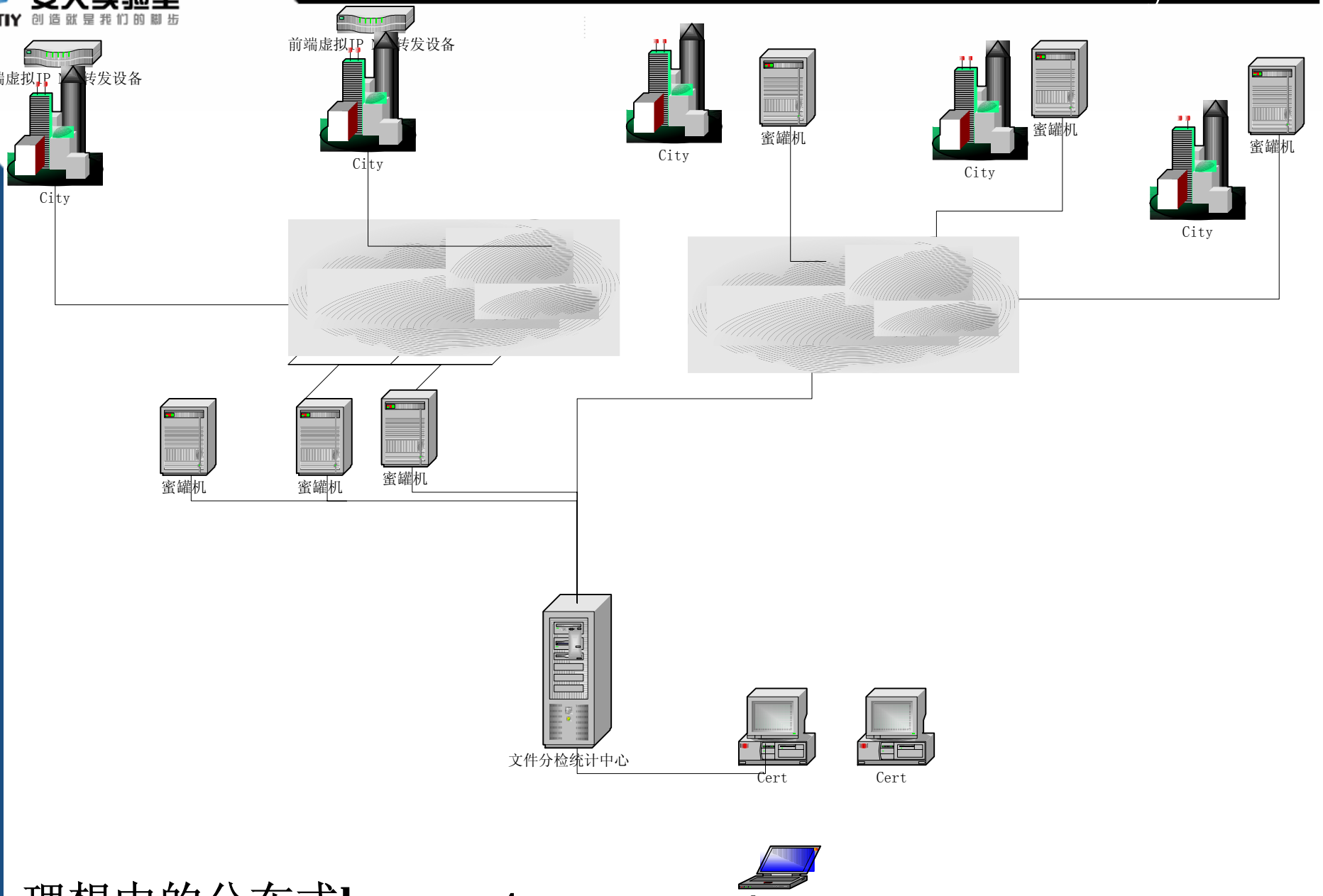

Worm.Win32.Sasser.a
Worm.Win32.Padobot.m
Worm.Win32.Fasong.a
Worm.Win32.Sasser.d
Worm.Win32.Padobot.n
Worm.Win32.Padobot.r
Worm.Win32.Padobot.p
Worm.Win32.Padobot.u
Worm.Win32.Padobot.h
Worm.Win32.Padobot.g

分布体系的关键问题

- 复杂条件部署
- 可管控载体平台
- 结果集汇总
- 规则定义分发
- 批命令执行

分代

- 第一代：分布式设备，集中汇总结果集。
- 第二代：基于前端设备包转发，可以很容易实现复杂IP段的分布部署和实体的集中。
- 第三代：结合两者优点，增加集中分析处理体制。



理想中的分布式honeypot

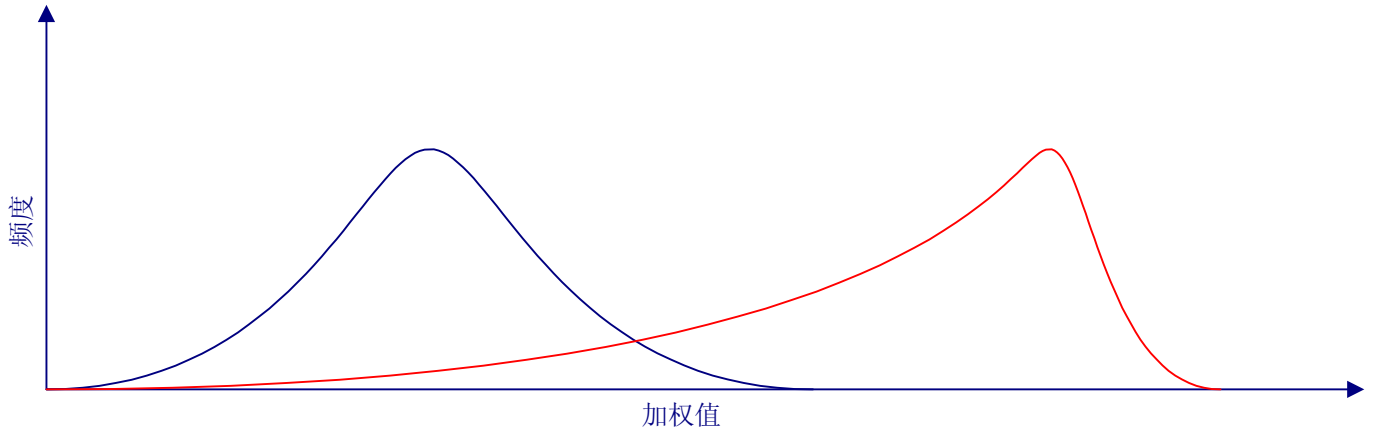
后端分析体制的意义

- 蜜罐和其他样本来源所造成的庞大上报数量，构成了对传统人工分拣方法的挑战。
- 因此必须形成一个具有较强自动前段处理能力的分拣体制。

蜜罐/上报文件的结果集处理

- Step1.黑白名单过滤
- Step2.人工智能分拣
- Step3.人工分析处理

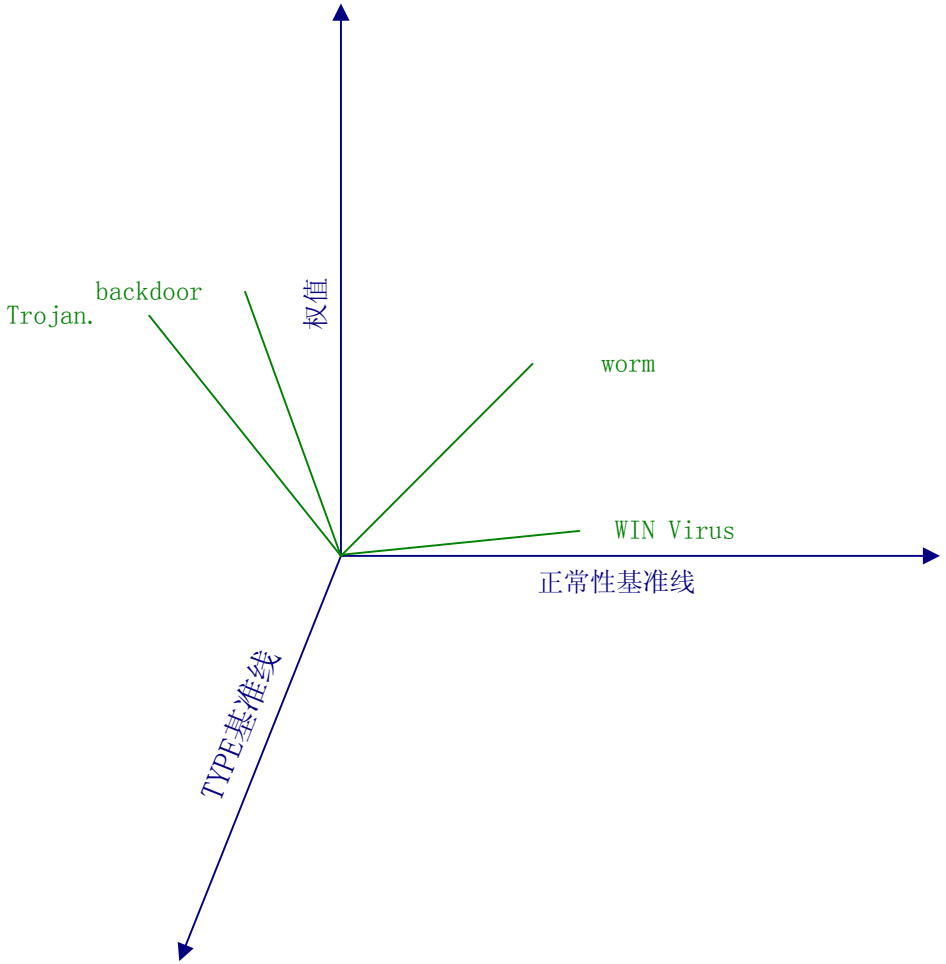
目前的分拣模型



基于神经网络进行正常文件的样本采样。

主要针对木马和脚本病毒。

正在开发分拣模型



- 成分分析+决策树
- 新的分拣模型，不仅可以判定有害性，还可以进行类别分析。

创造就是我们的脚步

- 我们与蠕虫之间的对抗，是一场战争，或者它让我们的信息社会体制崩溃，或者我们扼住蠕虫的咽喉。
- 谢谢各位专家领导的批评指导。
- seak@antiy.net