后“冷战”时代的病毒捕获体制

安天实验室 江海客

2006年.9月于武汉大学

返回索引

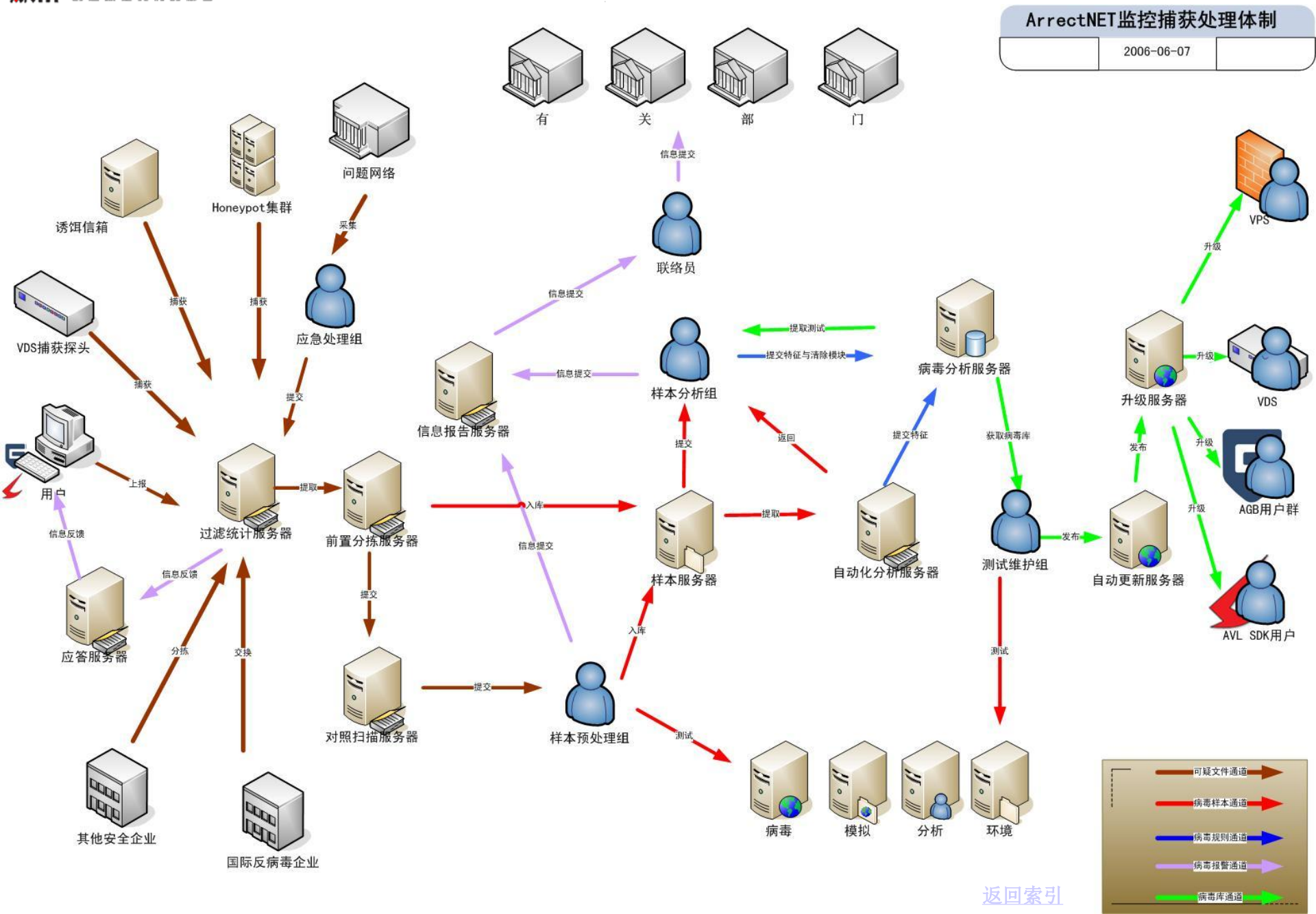
2012补记

- 笔者2006年9月*在武汉大学计算机学院做了本报告，之后PPT并未公开，因笔者拟在2012年武汉大学Xdef安全会议上反思和批判这次报告。因此对错别字做了修改，将当年这些幼稚的思考予以公开。

* 2007年4月，作者在对部分内容进行完善后，曾在哈工大四维讲坛做了第二次同名报告，但本版本仍为第一版内容。

提纲

- 现代AV企业的病毒捕获的体系
- 快速捕获通道的发展与现状
- VX对抗的冷战时代与后冷战时代
- 我们的应对


ArrectNET监控捕获处理体制
2006-06-07
有
关
部
门
问题网络
Honeypot集群
诱饵信箱
采集
捕获
捕获
VDS捕获探头
捕获
应急处理组
提交
用户
上报
过滤统计服务器
提取
前置分拣服务器
信息反馈
信息反馈
应答服务器
分拣
交换
提交
对照扫描服务器
其他安全企业
国际反病毒企业
信息提交
联络员
信息提交
信息报告服务器
信息提交
样本分析组
提交
入库
信息提交
样本服务器
入库
提交
样本预处理组
测试
提取测试
提交特征与清除模块
返回
病毒分析服务器
提交特征
提取
自动化分析服务器
获取病毒库
测试维护组
测试
发布
自动更新服务器
发布
升级服务器
升级
VPS
升级
VDS
升级
AGB用户群
升级
AVL SDK用户
病毒
模拟
分析
环境
可疑文件通道
病毒样本通道
病毒规则通道
病毒报警通道
病毒库通道

返回索引

渠道一览表

- 蜜罐捕获
- 诱饵信箱
- 邮件服务代管
- VDS监控捕获探头
- 客户端抓取
- 问题网络采集
- 原厂和黑客站点监控
- 兄弟CERT组织提供
- 其他企业分拣样本
- 用户主动上报
- 样本志愿者上报
- 国际AV企业交换
- 购买

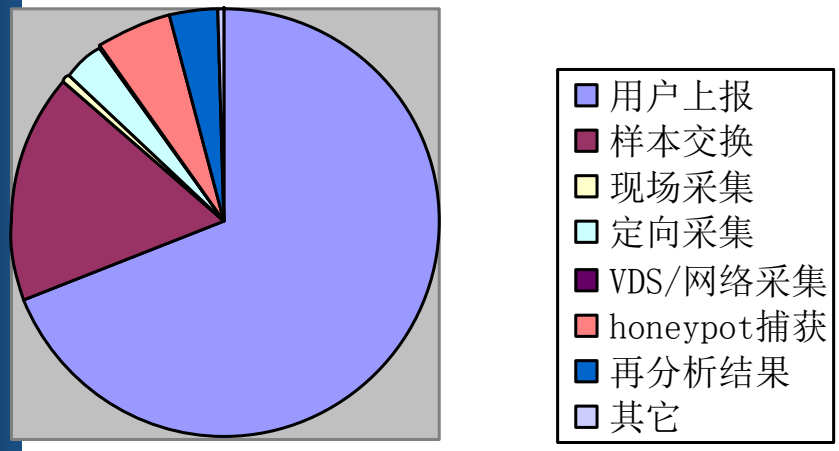
返回索引

部分渠道方法说明

手段	说明
用户上报	通过使用反病毒产品用户上报，是目前反病毒企业获得样本的主要方式。
样本交换	通过等量交换方式从其它公司、个人获得病毒样本
诱饵信箱	通过在各个邮件服务商注册大量邮件的方式，达到邮件蠕虫可能发送到信箱中的效果。
原厂和黑客站点监控	对木马后门的原始发布站点和黑客工具站点追踪下载。
现场采集	通过应急处理工程师在网络安全时间现场采集样本。
蜜罐系统	通过模拟具有漏洞的系统，实现对扫描性

返回索引

安天2004年做的一个统计



各种上报分拣	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%

返回索引

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**

返回索引

目前的常规样本获得手段比较

	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

返回索引

提纲

- 病毒捕获的体系
- 快速捕获通道
- VX对抗的冷战时代与后冷战时代
- 我们的应对

返回索引

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。

蜜罐的价值

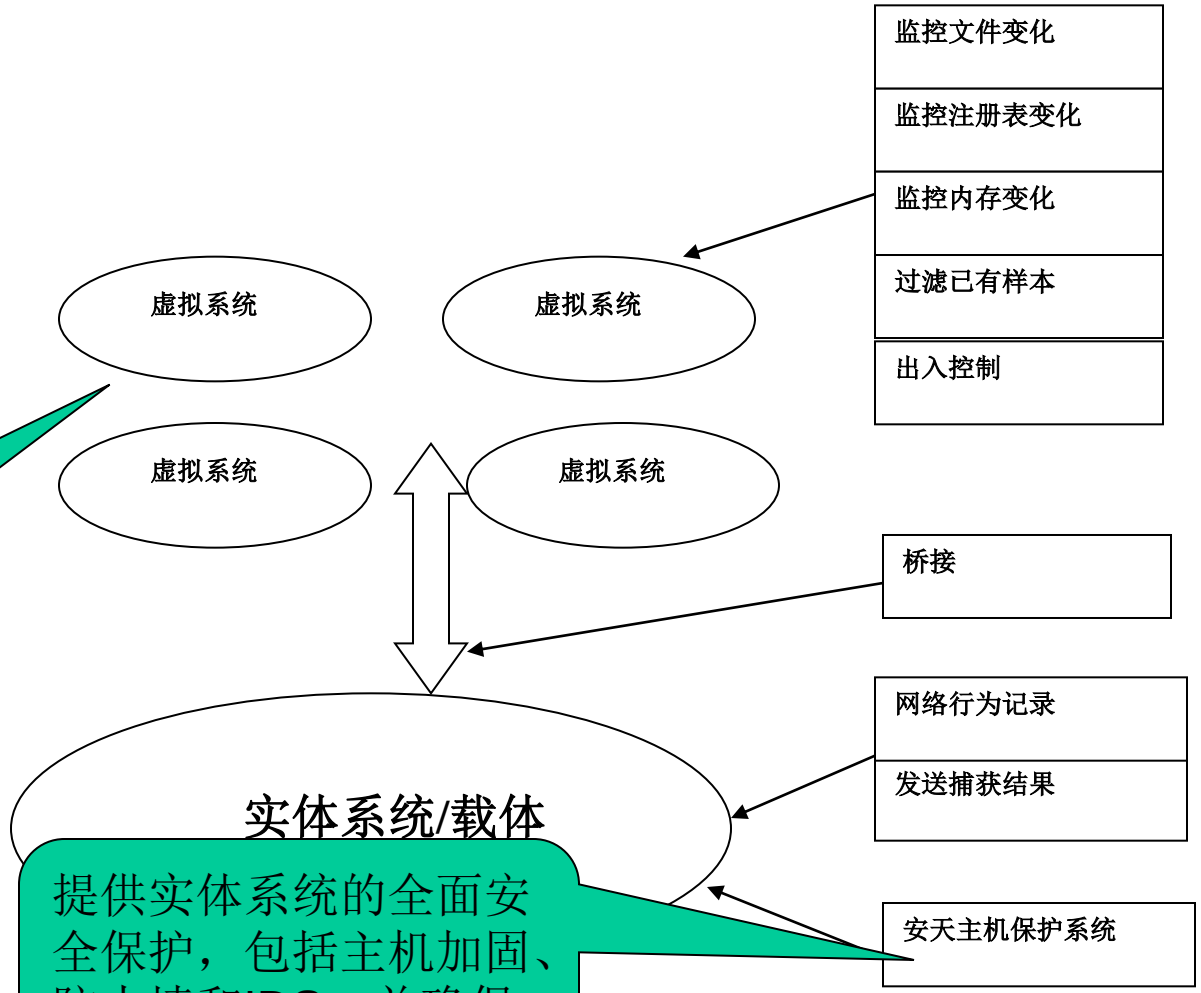
- 蜜罐体系是安天ArrectNET监控网络的重要组成部分，蜜罐获取样本的绝对种类数不大，但意义非凡。
- 蜜罐主要的价值是：第一时间捕获流行的扫描型蠕虫，我们第一时间截获冲击波、震荡波以及他们的变种都依赖于蜜罐体制。
- 此外，蜜罐具有统计意义，能够对流行情况/节点压力进行比较准确的判断和分析。

返回索引

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

安天当前蜜罐的结构



返回索引

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。

返回索引

旁路的价值

- 旁路监控体系是安天ArrectNET监控网络的重要组成部分，旁路监控体系获取样本的数量不大，但对于及时性和态势分析，意义非凡。。
- 旁路主要的价值是：第一时间捕获流行的可还原协议传输型蠕虫，我们第一时间截获多个emial-worm依赖于旁路捕获体制。
- 此外，旁路体制可以起到制导的作用，如发现可疑的URL、发现可疑的EMAIL ADDR等。

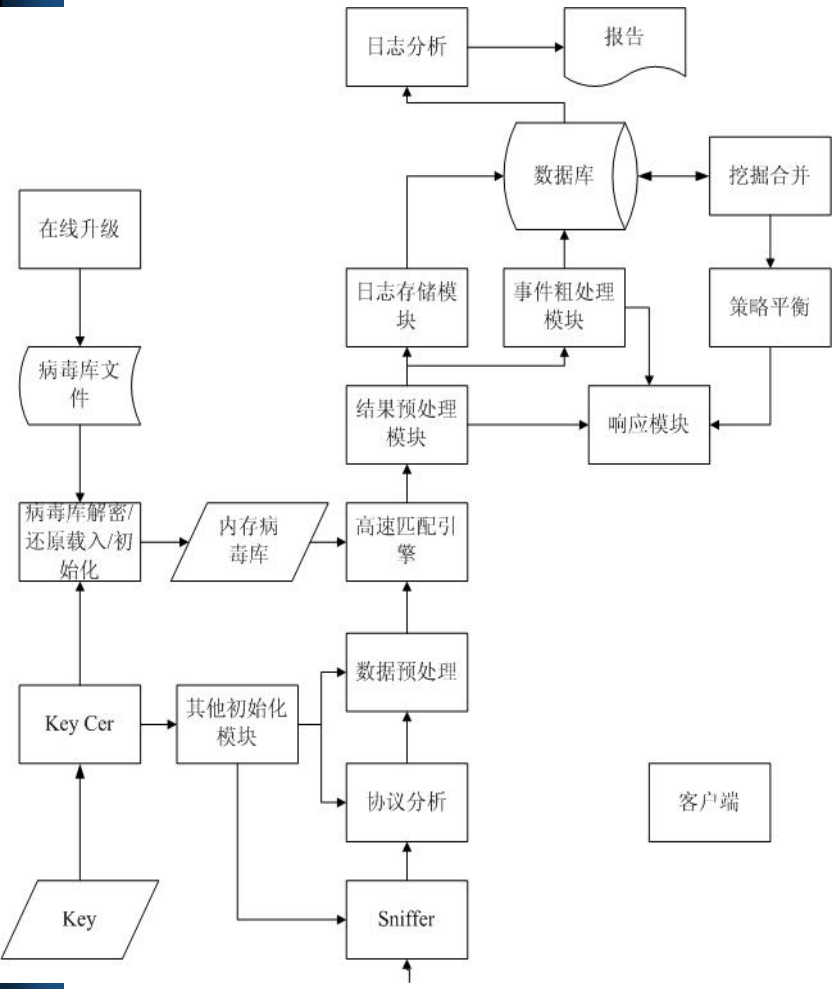
返回索引

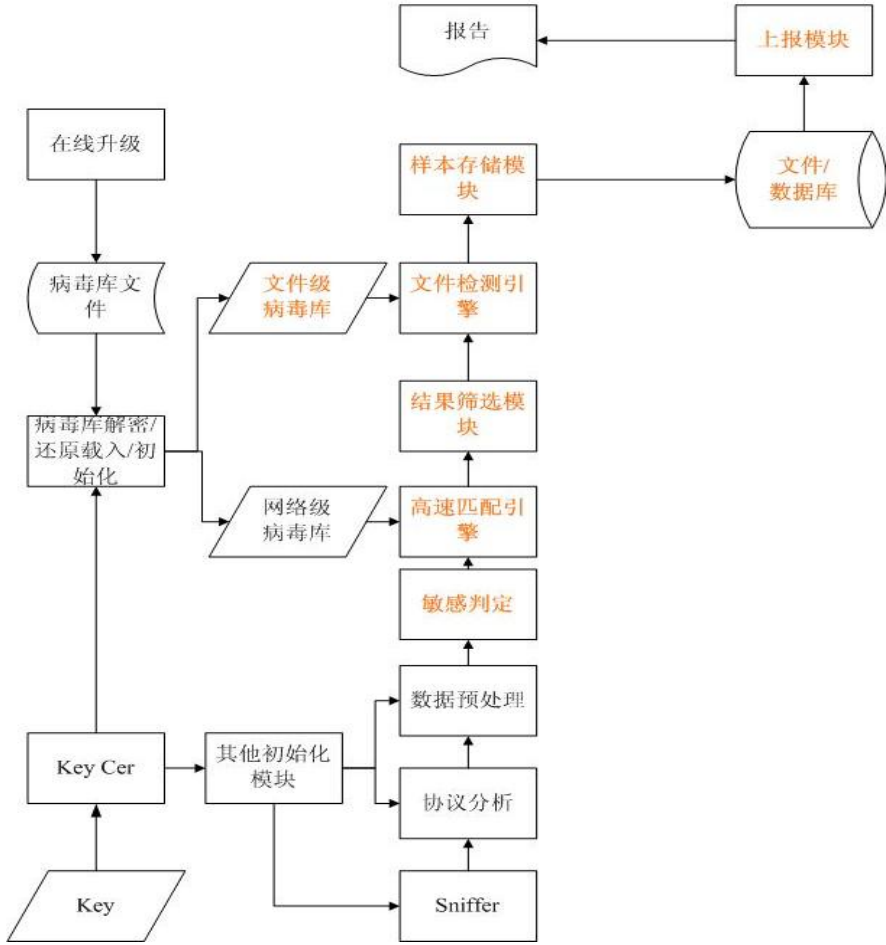
旁路的技术要求

- 高速捕包和协议分析
- 获得样本
- 记录准确的源头
- 排除已有病毒
- 提供新文件和病毒源头

返回索引

旁路捕获探头





VDS体系结构

旁路侧捕获设备

返回索引

总结

- 蜜罐系统可以捕获扫描蠕虫/BOT，主要利用了他们以IP扫描进行寻找目标的特性。
- 由于蠕虫想要形成传播必须呈现足够大的扫描扇面，一般数百个蜜罐节点如果分布足够均匀足以捕获大多数蠕虫。
- 如果解决主动应答和探索的问题，蜜罐系统就可以演化为多功能的安全代理。
- 但对于定向传播的病毒（如mail worm）等则难以捕获。
- 旁路捕获有其无条件特点，但难以解决不可还原协议、加密协议等问题。

返回索引

提纲

- 病毒捕获的体系
- 快速捕获通道
- VX对抗的冷战时代与后冷战时代
- 我们的应对

返回索引

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。
- 而在2005年之后，几乎没有感染数量超过百万的病毒

冷战时代的数据

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

- 2001年度Popsoft横向测试，病毒样本由安天供应。选取的原则是参考wildlist对照命名。
- 测试结果各主流反病毒产品数据均达到90%以上。

返回索引

后冷战时代的数据

	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年度CHIP杂志反病毒横向测试，病毒样本由安天供应。选取的原则是，每类病毒个数的比例关系与2004年度各类新病毒产生的数量比例一致，具体种类的选取遵从用户上报的排行榜，保证了测试所选用的病毒样本均为确实有传播的样本。
- 测试结果各主流反病毒产品对木马检测数据均不理想。

返回索引

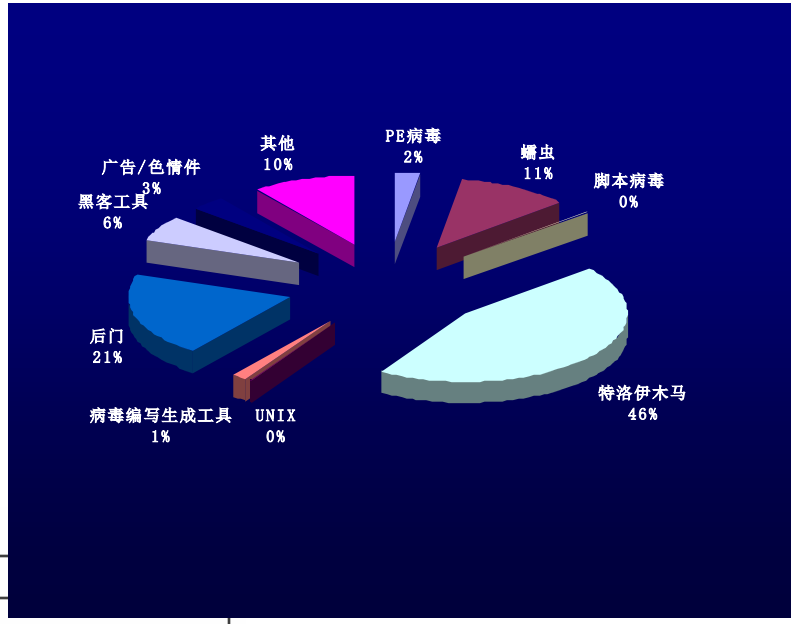
Why?

- Why?
- Why?
- Why?
- Why?

  - 别忘了 M$!!!

数量规模失控化

2004年，安天实验室平均每天接到6523次文件上报，共向病毒库中添加了200,047个新的独立病毒名称（含变种），其中木马类（木马、后门、黑客工具、广告色情件占绝大多数，部分蠕虫也具备木马性质）。而从1986年到2003年病毒数量的总和只有6万种。



2004 年各类病毒的产生数量如下：

PE 病毒	478
UNIX/Linux 系统病毒	33
蠕虫	2239
脚本病毒	81
特洛伊木马	8969
后门工具	4010
黑客工具	1241
广告/色情件	668
其他	2049

根据媒体报道，国内有2200个站点销售原创木马。根据国外机构统计，全球参与木马开发的人员约为50万人。

返回索引

黑客技术泛化

- 溢出技术：条件溢出木马
- 驱动技术：rootkit
- 流文件技术：无载体文件
- 信息伪装技术：非可执行格式

专有化

- 经济利益化/政治利益化促进木马向定向性、专有化发展。
- 从传统的散步行为向定向行为转化，不需要大面积传播也能达到一定目的。

返回索引

传统技术的主要挑战总结

- 数量失控
- 黑客技术
- 伪装技术
- 专有性
- 全面分析响应的工作量趋向不收敛
- 无法对抗各种非常规态木马
- 木马可复用性大大提高
- 采集工作异常困难

结论：木马动摇了AV根基

- 传统AV技术的根本链路是，编制>>流行>>捕获>>处理，捕获是AV的根基！！
- AV机理：以样本满足一定的流行范围或公开发布为基础，立足于后发式的一对一处理。
- 全面捕获已经趋近不可能，分析处理强度也趋向不收敛，必须有全新的思路作为补充。

返回索引

VXER们在干什么？

- 搭建加密的控制和传输协议
- 基于PKI技术的命令分发体系
- 反查杀、反发现、反捕获
- 基于VM技术的木马
- 安全体系能做什么，他们也能做什么
- AV能做什么，他们也能做什么

标志性事件

- Backdoor.Win32.IRCBot.st——一场未遂的911
- DDoS攻击分析者
- 负载均衡
- 降低系统安全等级
- Trojan.PSW.QQpass.jh——
- 智能中止反病毒软件
- 锁定注册表

其他标志事件—总结

- Virus Total被攻击
- WoW木马的反查杀竞赛。

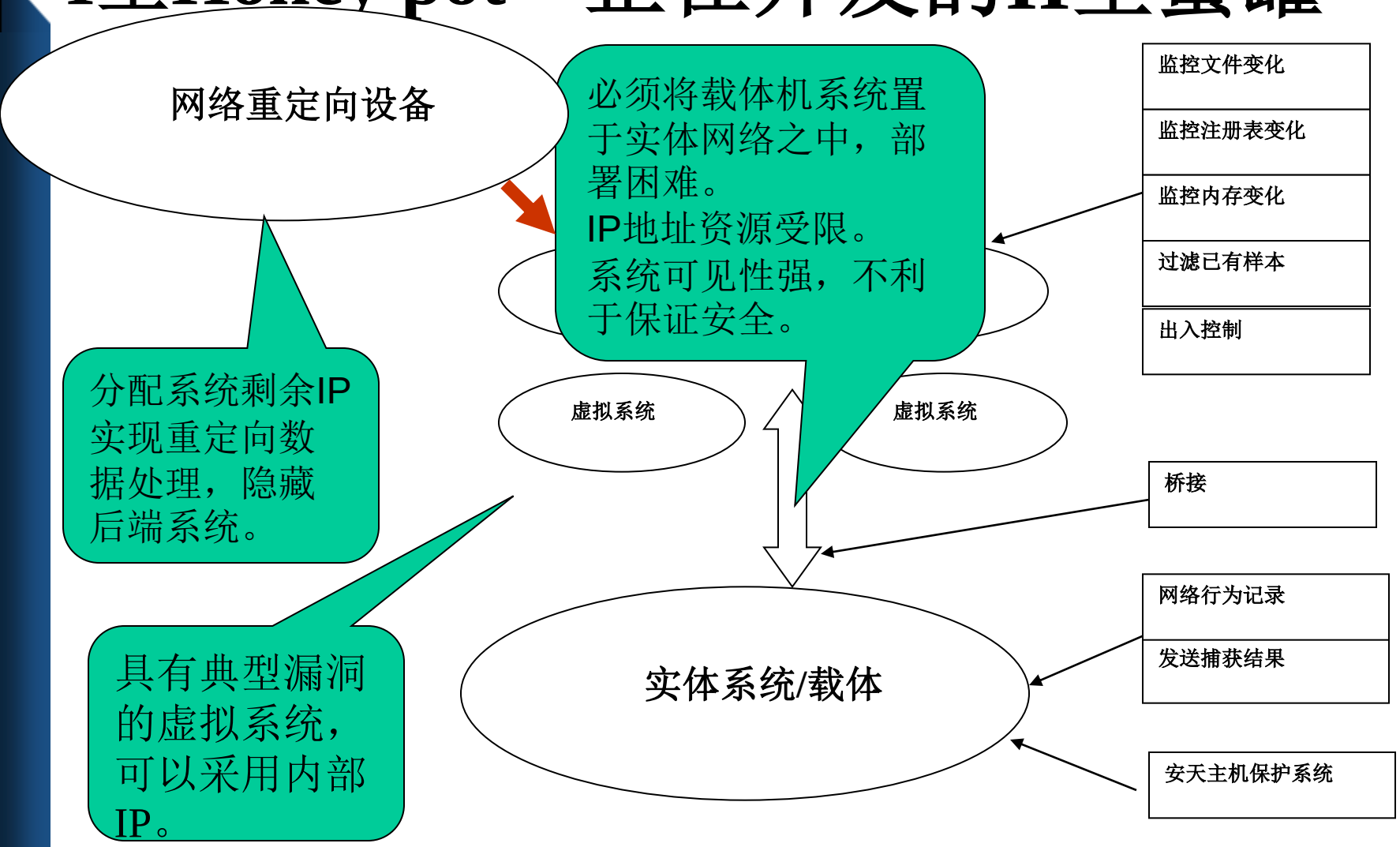
- 新一代的VXER其实并不比他们的前辈富有才华，他们增加的是强烈的目的性，而却没有老的VXER在自然社会面前的负疚感……

提纲

- 病毒捕获的体系
- 快速捕获通道
- VX对抗的冷战时代与后冷战时代
- 我们的应对

返回索引

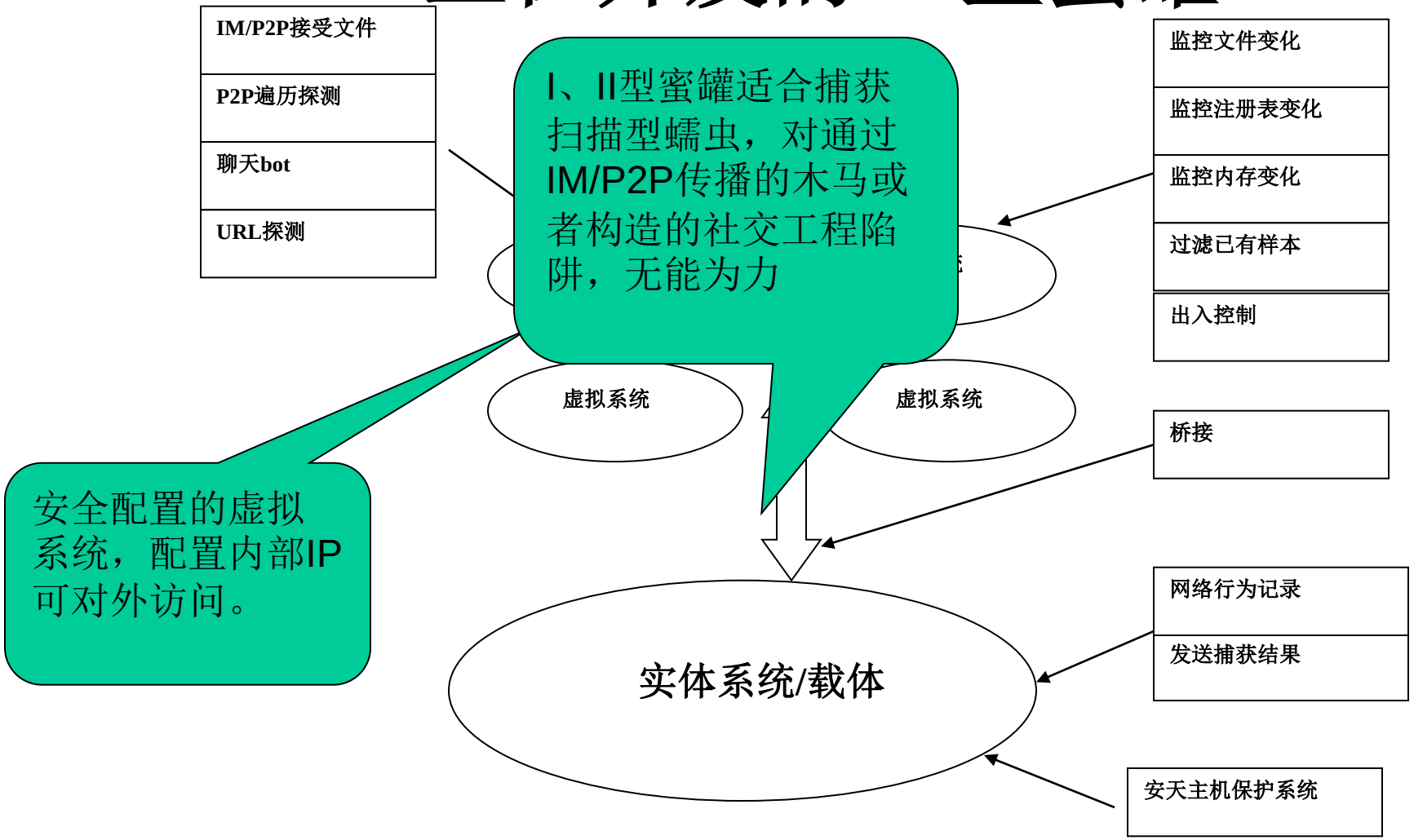
I型Honey pot　正在开发的II型蜜罐



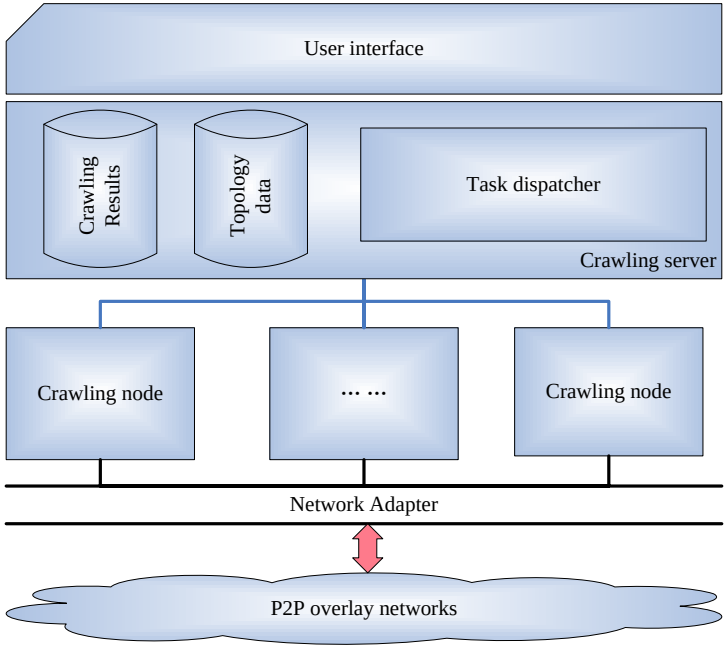
申请书:P16

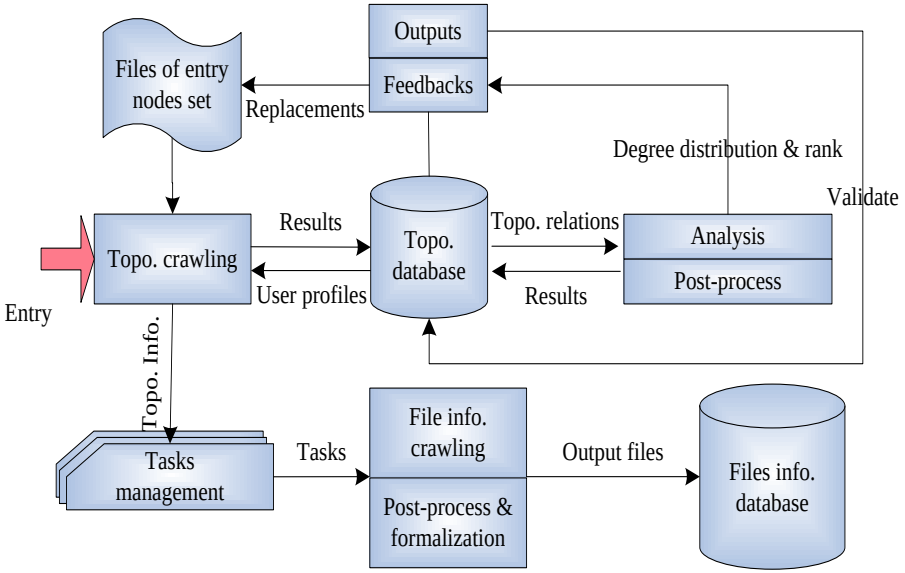
返回索引

正在开发的III型蜜罐



P2P的遍历测试





返回索引

VCS技术

- 客户端即探头的思想
- 行为检测->上报->回避误报问题
- 演示

总结

- 过去的问题
- 不能应答
- 社交工程

- 解决
- 模拟应答
- 社交工程的反识别

返回索引

创造就是我们的脚步

- 谢谢大家！
- 欢迎大家加入与我们并肩战斗！

- seak@antiy.net