蜜罐技术的发展、困局与探索

安天实验室 江海客

提纲

- 蜜罐的历史沿革
- 蜜罐的研究现状
- 蜜罐遇到的技术挑战
- 方向和探索

英英解释

柯林斯英语大词典

honeypot 生词本

['hʌnɪˌpɒt]

n

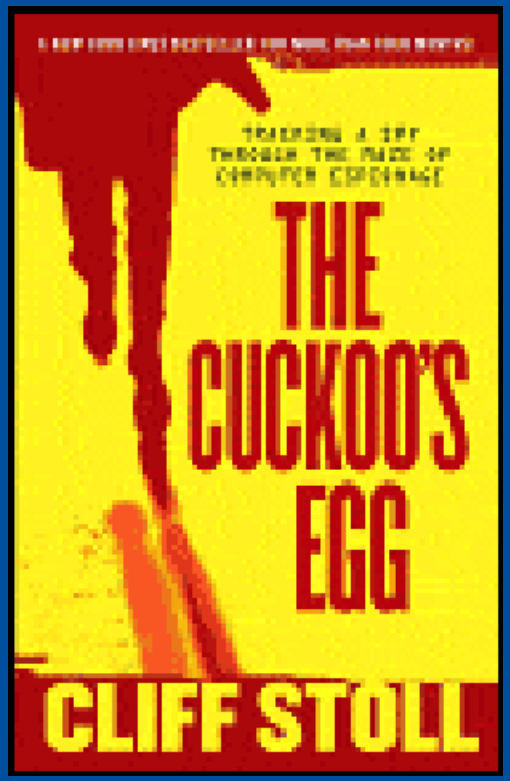
- a container for honey

什么是蜜罐

- 蜜罐是一种安全资源，其价值在于被扫描、攻击和攻陷。——Lance Spiztner

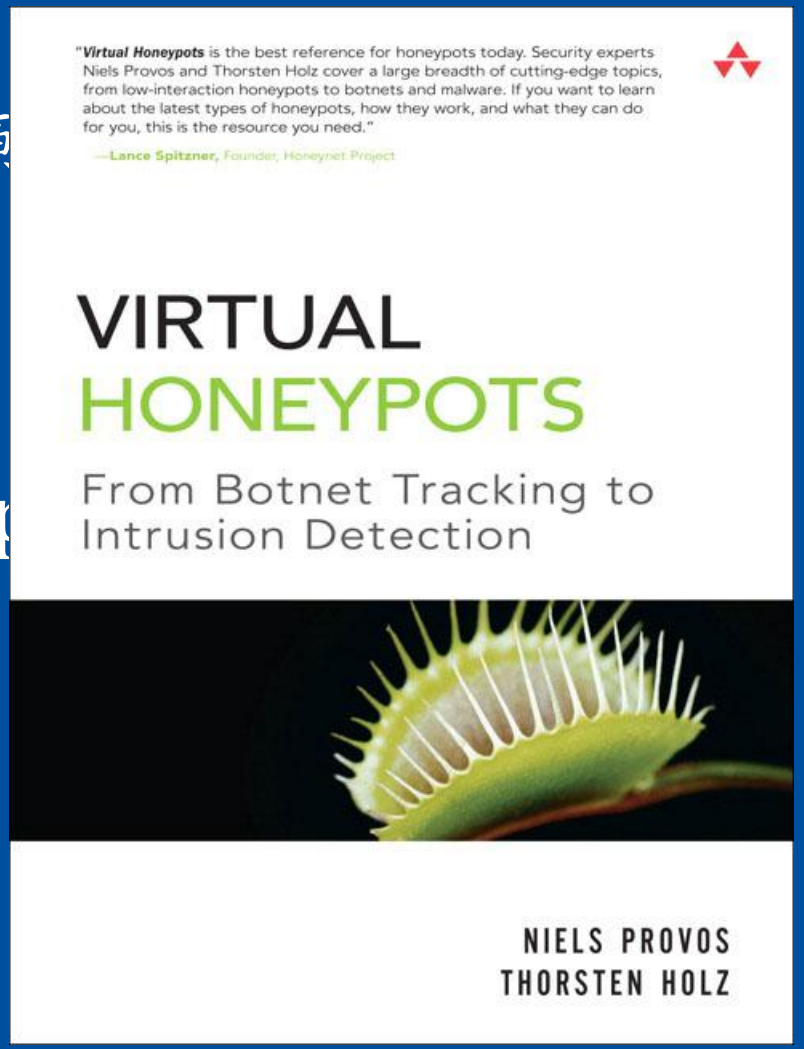
1990-1998，青铜时代

- 1990 年，《The Cuckoo’s Egg》
- 网络管理员自发的时代
- 实体系统



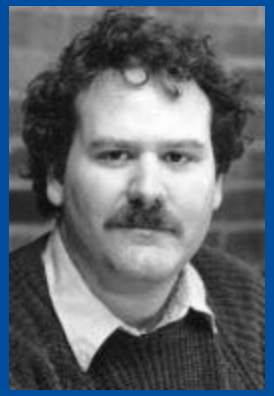
1998-2000，白银时代

- 专门用于欺骗黑客的开源
- DTK（Fred Cohen）
- Honeyd（Niels Provos）
- 蜜罐产品：KFSensor、Sp
- 虚拟蜜罐



小贴士.Fred Cohen

- 反病毒技术领域的第一位大师
- 把病毒一词引入电脑领域
- “对交线法”的天才论证



2000-2006，黄金时代

- 从2000 年之后，安全研究人员更倾向于使用真实的主机、操作系统和应用程序搭建蜜罐，但与之前不同的是，融入了更强大的数据捕获、数据分析和数据控制的工具。
- 样本获取的主流通道

提纲

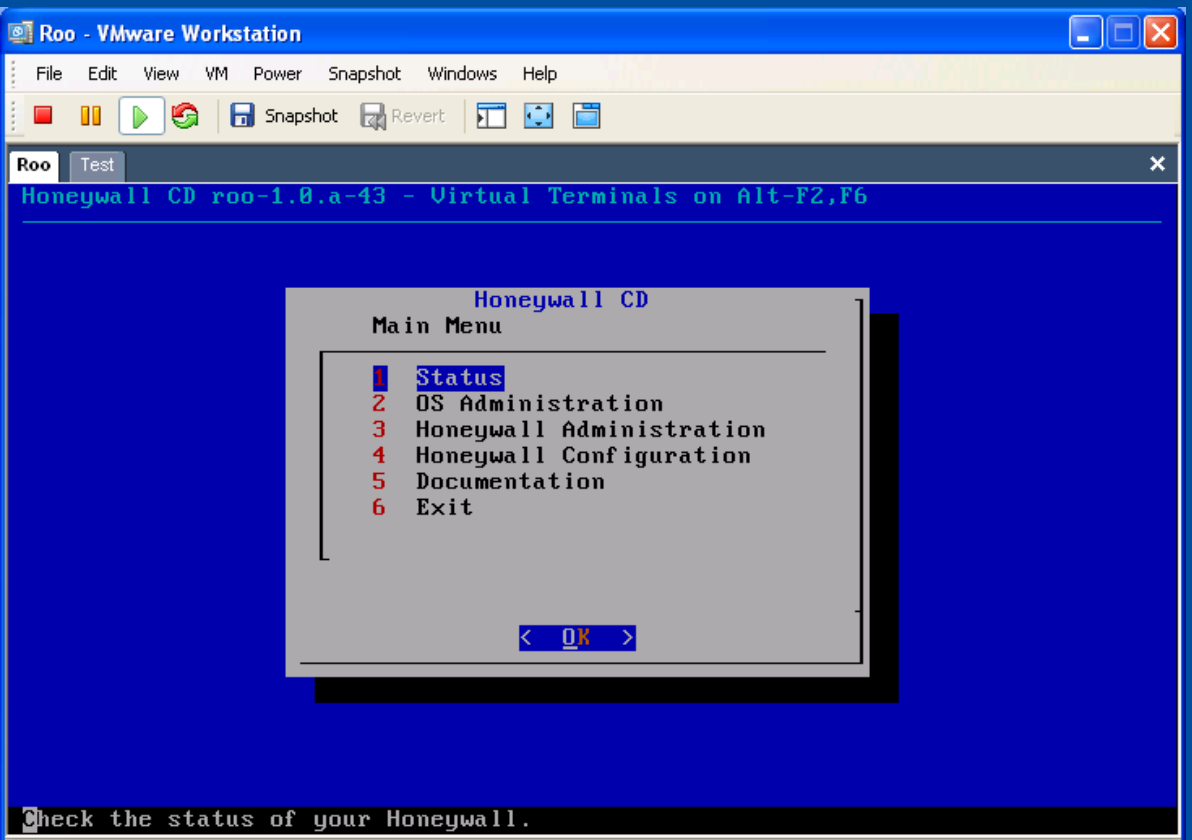
- 蜜罐的历史沿革
- 蜜罐的研究现状
- 蜜罐遇到的技术挑战
- 方向和探索

分类

- 部署目的划分
  - 产品型
  - 研究型
- 交互度的划分
  - 高交互型
  - 低交互型

高交互蜜罐代表介绍

- Honeywall CDROM
- Sebek:



低交互密网介绍

- Nepenthes
- Honeyd:
- Honeytrap:

利用无线节点固化的蜜罐

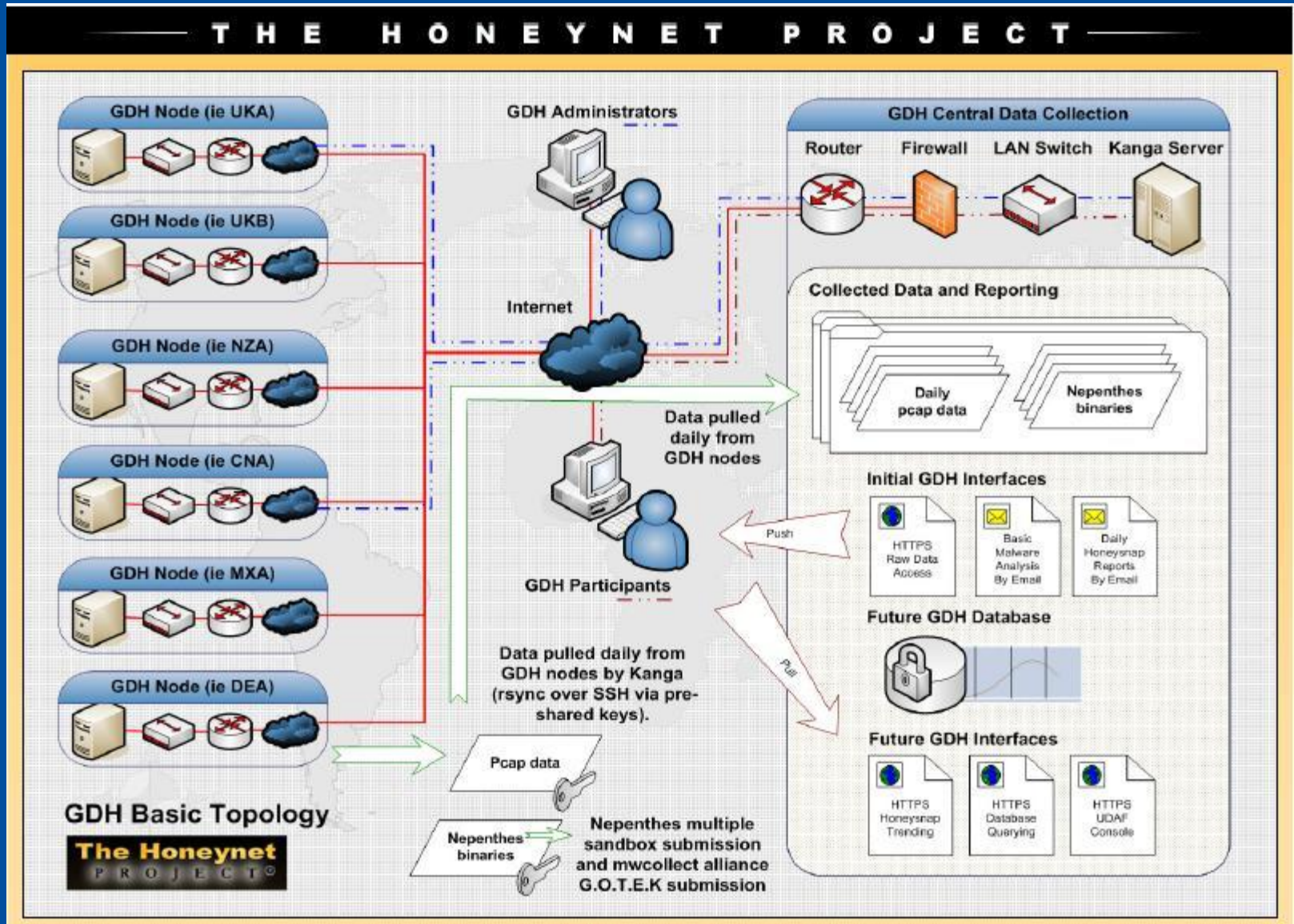
客户端蜜罐

- Capture-HPC
- HoneyC

数据分析工具

- Honeysnap

可以看到的一些开源系统



可以

Display Filters

Limit: 20

Only data from my sensors:

- Magnet Value contains av.clam

+ Add a custom filter.

Filter Bi

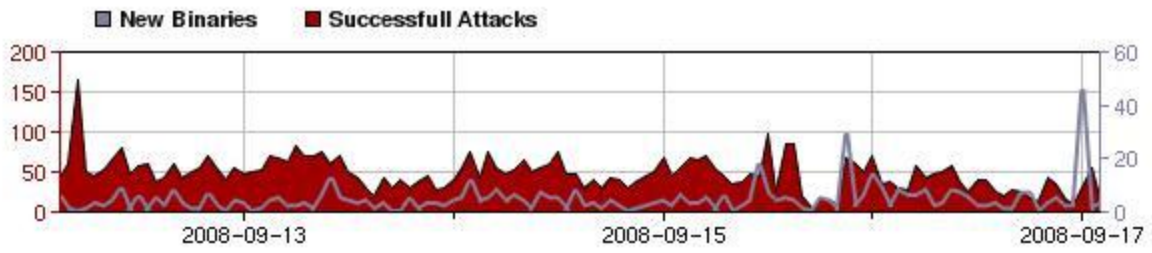
Matching Binaries

Displaying matching samples 1 - 20.

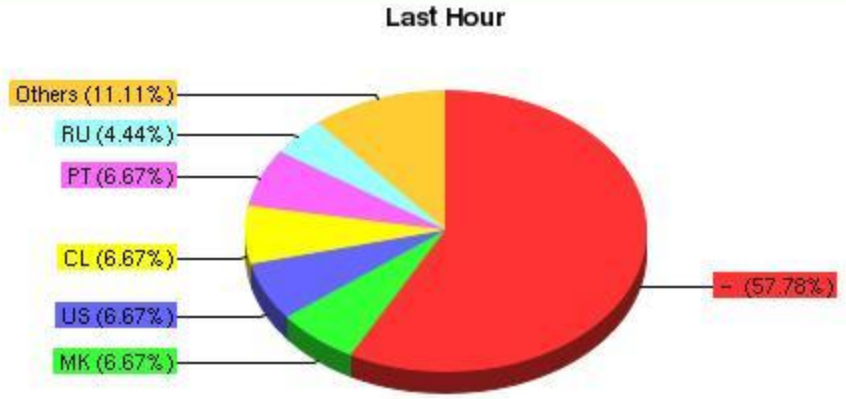
Hits	Samples	PE Hash
1	1	8e7e49098620ccf78bf6cb
1	1	?
6	6	bedf4242974d7a0299319
2	2	ee6d544d4f50628b1bef8
10	10	1c15d334dc0eb44ba335b
90	90	23162437075ae1ed5d33
9	9	ec4461904b376c0338936
52	52	8cb9cb3578438c441f2136
158	56	b2cee2a770dd210bd482a
234	234	b45deba4a88553a5f83e2
175	175	71d1c85ab3e0782717ffbb
169	169	19edc87ad51a1beddc2b9
489	489	ef2123aebf6cf650d300fb4
70	70	63ba4ead6d8c8fcbed355b
4952	4952	9a32e5f3b0f24a1ca07c4ff
1371	271	169f97a27b1e14ccb44503
3181	3181	5b8ff0c3cd58c66a451ea1
9184	9183	a5afdff73e118584e55de9

«

mwcollect Alliance Activity



Attack Source Country Distribution

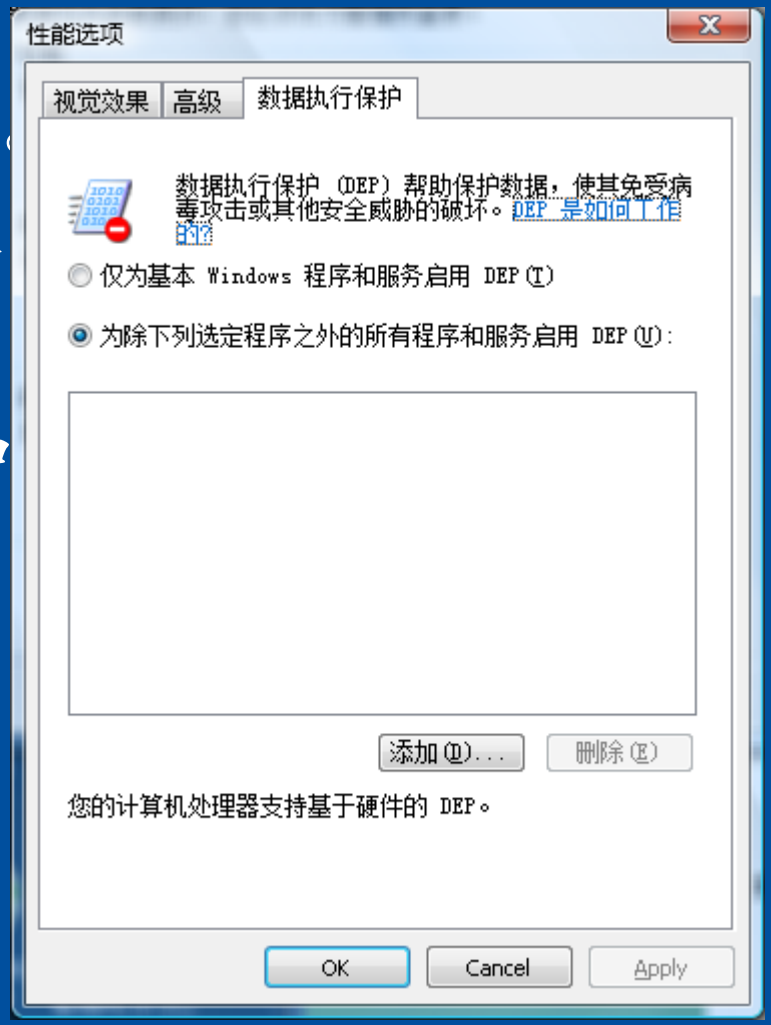


提纲

- 蜜罐的历史沿革
- 蜜罐的研究现状
- 蜜罐遇到的技术挑战
- 方向和探索

终端安全趋势的挑战

- DEP带来的强大保护能力，发生针对windows系统服过DEP的攻击。
- 静态格式溢出、浏览器和成为主流。
- 蜜罐的基本存在原理受到



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

- 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

提纲

- 蜜罐的历史沿革
- 蜜罐的研究现状
- 蜜罐遇到的技术挑战
- 方向和探索

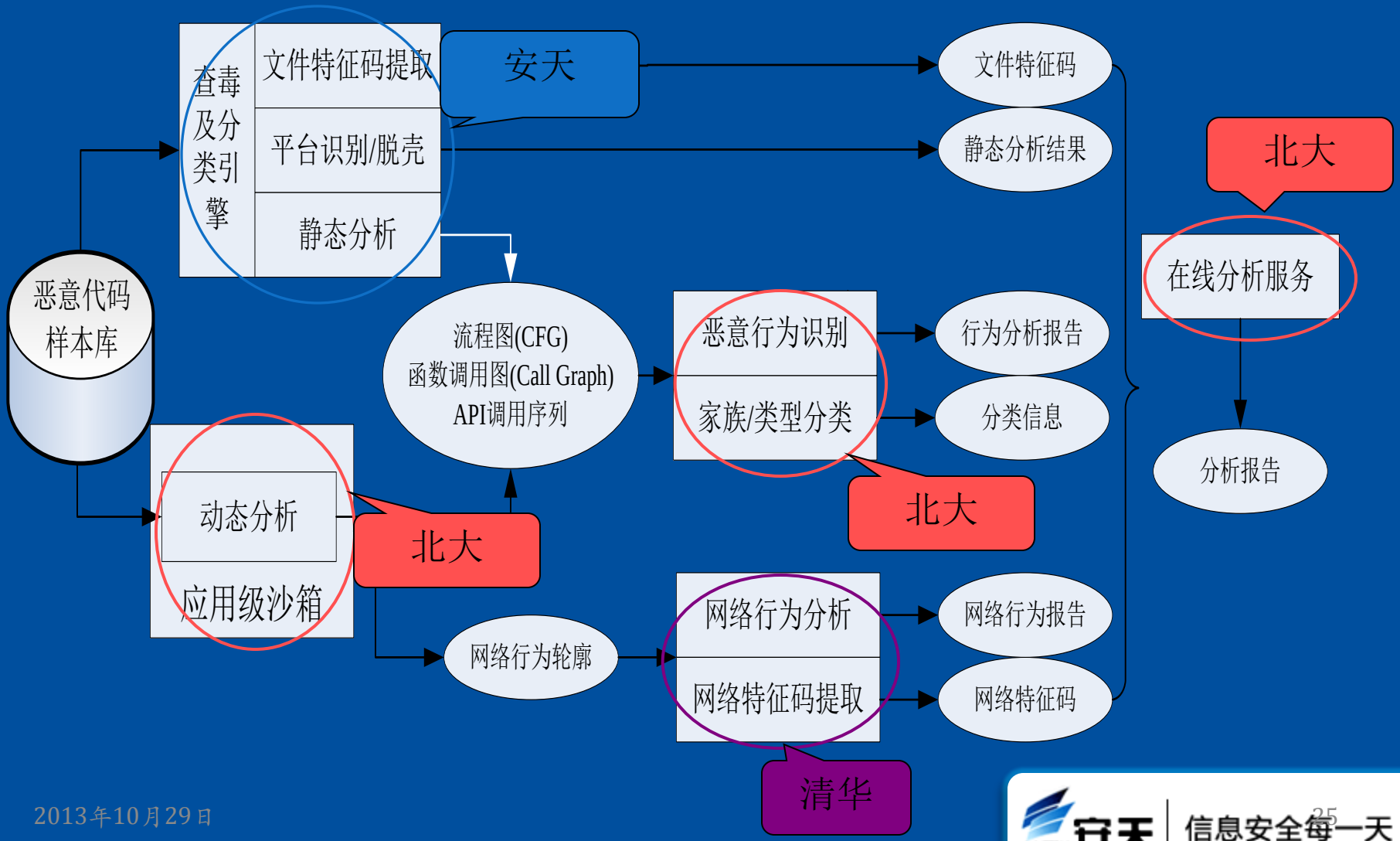
趋势：样本养殖

- 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

- 北大、清华、安天：自动化行为分析特征提取的研究。
- 国家863反入侵防病毒中心、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



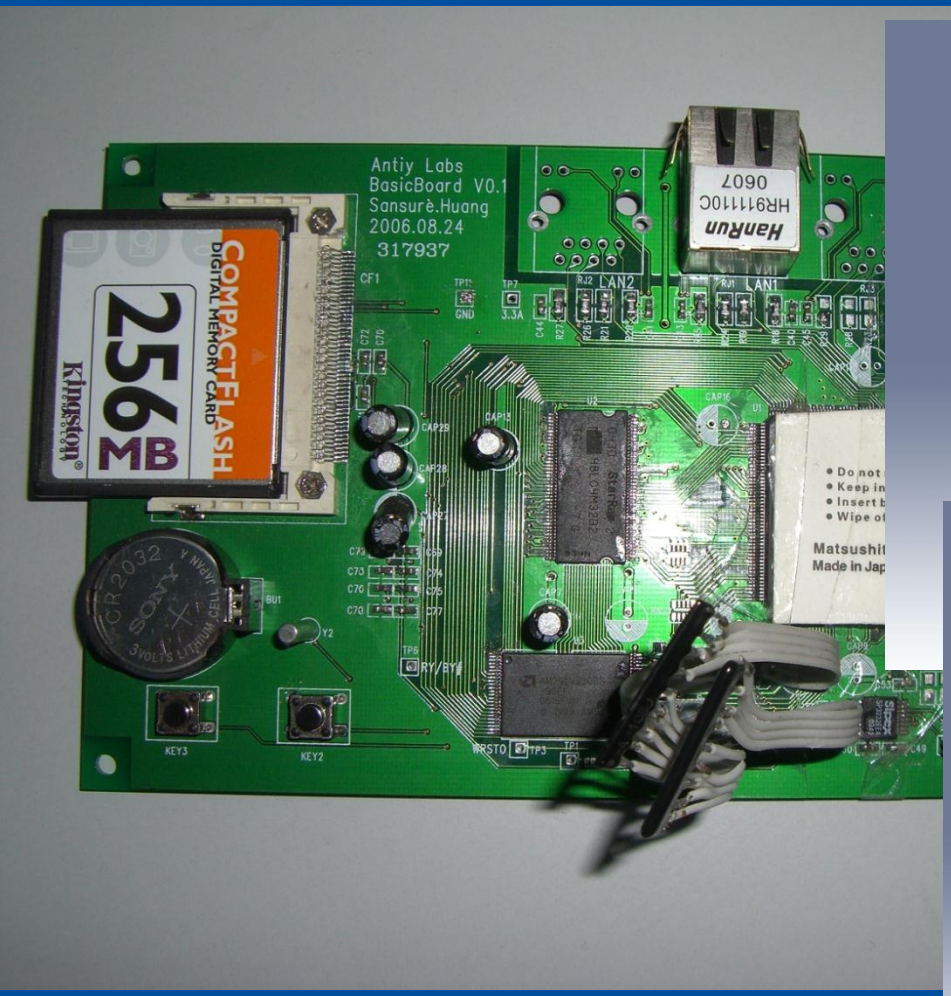
捕风计划

- 捕风计划：是安天于2006年发起的公益性蜜网部署计划。
- 计划划分三期。
- 捕风I:改善国家基础捕获体系。
- 捕风II:高校协同研究计划
- 捕风III：面向民间研究者和民间上报节点。

捕风II:ARM虚拟蜜罐

- 实物演示。
- 电路设计介绍
- 软件体系介绍

电信级别密网——蜜池


Antiy Labs
BasicBoard V0.1
Sansurè.Huang
2006.08.24
317937
COMPACTFLASH
DIGITAL MEMORY CARD
256MB
Kingston
HanRun
LAN2
LAN1
KEY3
KEY2


瑞 风 2
ANTIY HONEYPOT


POOL

管理系统

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

- 数据导入员
- 数据导出员
- ftp下载
- 站点分析员
- 查询用户

捕风II-密网联盟

- 安天计划与武汉大学、清华大学、哈尔滨工业大学等联合发起。
- 每校部署3-5台捕风II蜜罐节点，数据共享。

为信息科学研究提供基础数据。

捕风III:ADSL蜜罐

- 双网卡小型蜜罐网关
- 可以放在AD猫后面，用户系统之前。

Honeybot 糖人

- NPC概念的安全应用。
- 模拟目标价值，诱发攻击。
- 传统体系的结合。

创造就是我们的脚步

- 请各位老师和同学们指正。

- seak@antiy.net