第三讲 蜜罐技术的发展趋势

诸葛建伟
北京大学狩猎女神项目组
The Artemis Project

北京大学计算机科学技术研究所

蜜罐技术的发展趋势

- 分布式蜜罐/蜜网技术
- 应用层蜜罐技术
- 客户端蜜罐技术
- 蜜场技术

蜜罐技术的发展趋势

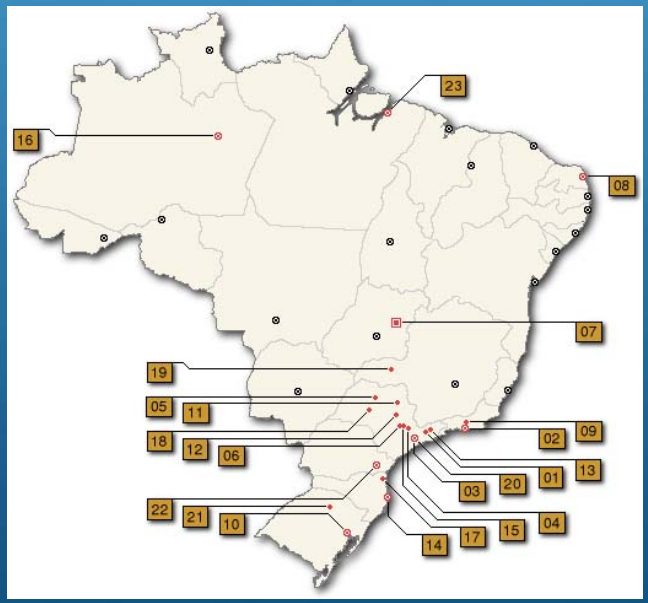
- 分布式蜜罐/蜜网技术
- 应用层蜜罐技术
- 客户端蜜罐技术
- 蜜场技术

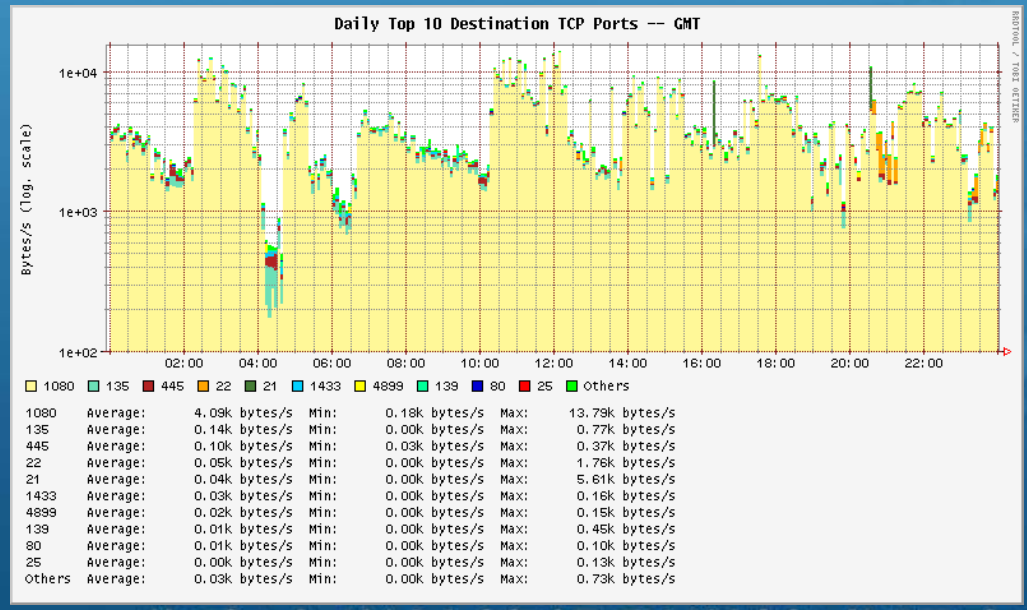
分布式蜜罐技术

- 分布式蜜罐技术
  - 分布式：克服蜜罐监测面小的缺陷，通过分布式部署提高安全威胁监测的覆盖面
  - 引入的技术点
    - 分布式蜜罐捕获数据的汇总
    - 分布式蜜罐的有效部署、配置与管理
    - 对大规模原始攻击数据的深入分析
- 分布式蜜罐项目
  - 巴西蜜罐联盟分布式蜜罐项目
  - LEURRE分布式蜜罐项目

巴西分布式蜜罐项目

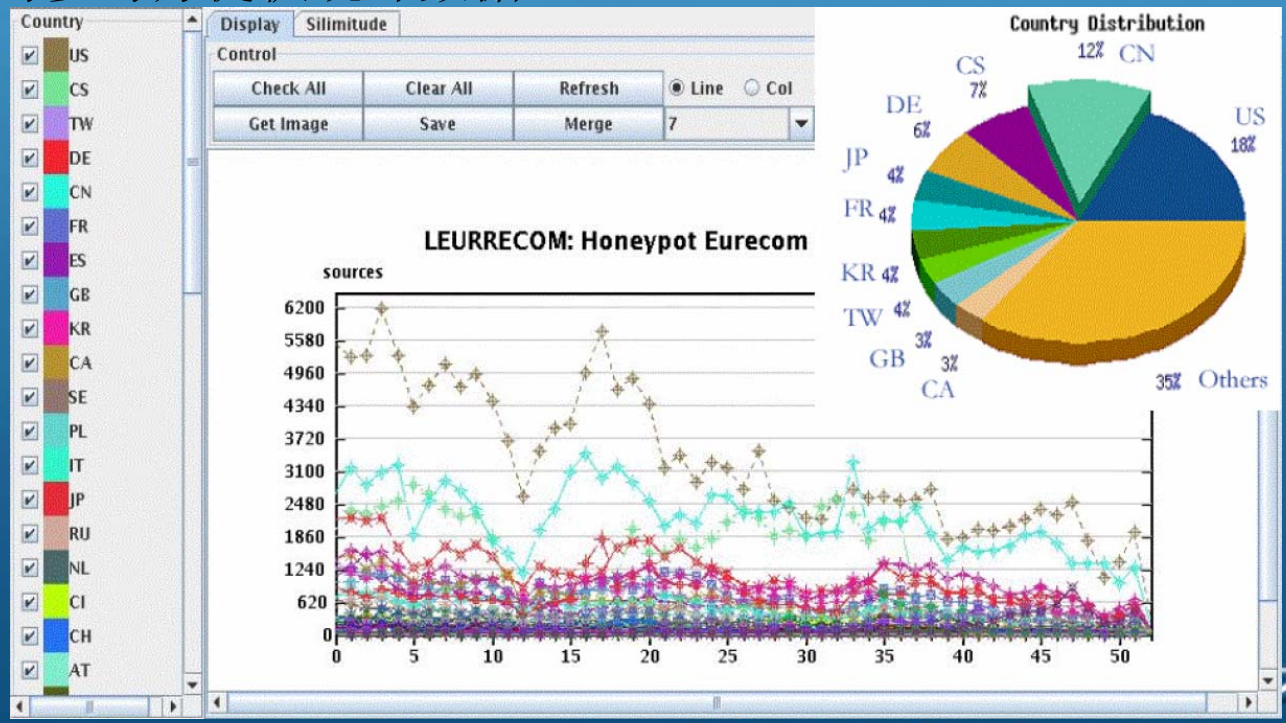
- 巴西分布式蜜罐项目
  - 巴西CERT/巴西蜜网项目组发起创建http://www.honeypots-alliance.org.br/
  - 目前覆盖巴西境内23个城市的40多个节点
  - 基于Honeyd虚拟蜜罐技术构建，可启动光盘，网络连接数据
  - 提供统计分析功能：目标端口、源国家、源OS分布、...





LEURRE分布式蜜罐项目

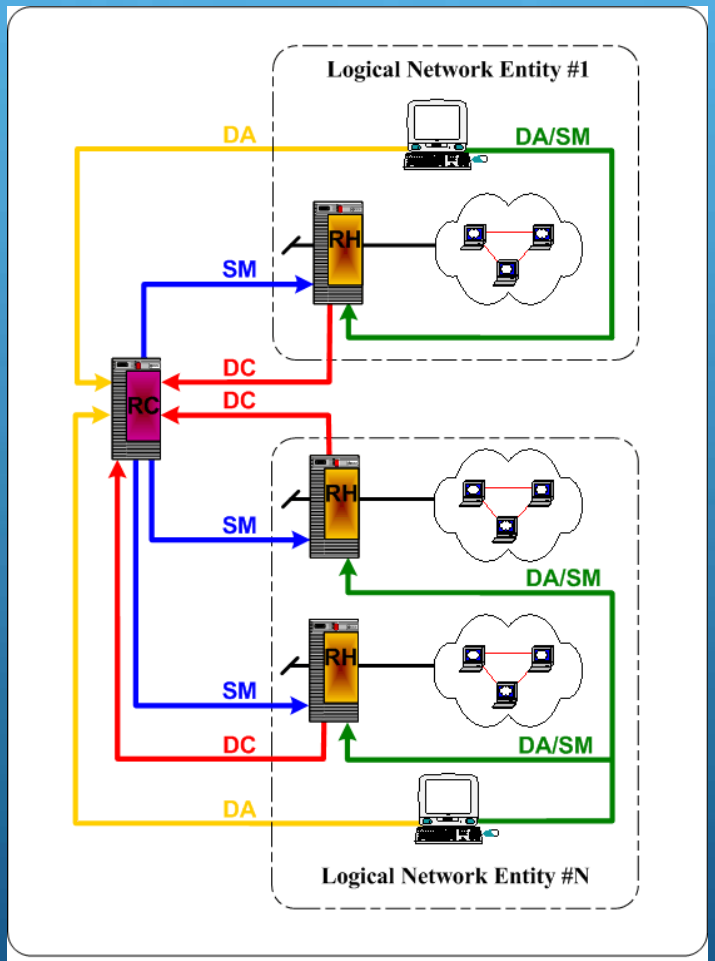
- LEURRE分布式蜜罐项目
  - 欧洲电信蜜罐项目组发起http://www.leurrecom.org
  - 目前拥有来自20多个国家的部署站点，狩猎女神项目组是该项目的参与方
  - 基于Honeyd虚拟蜜罐技术构建，可启动光盘，网络连接数据
  - 为参与方提供统计数据



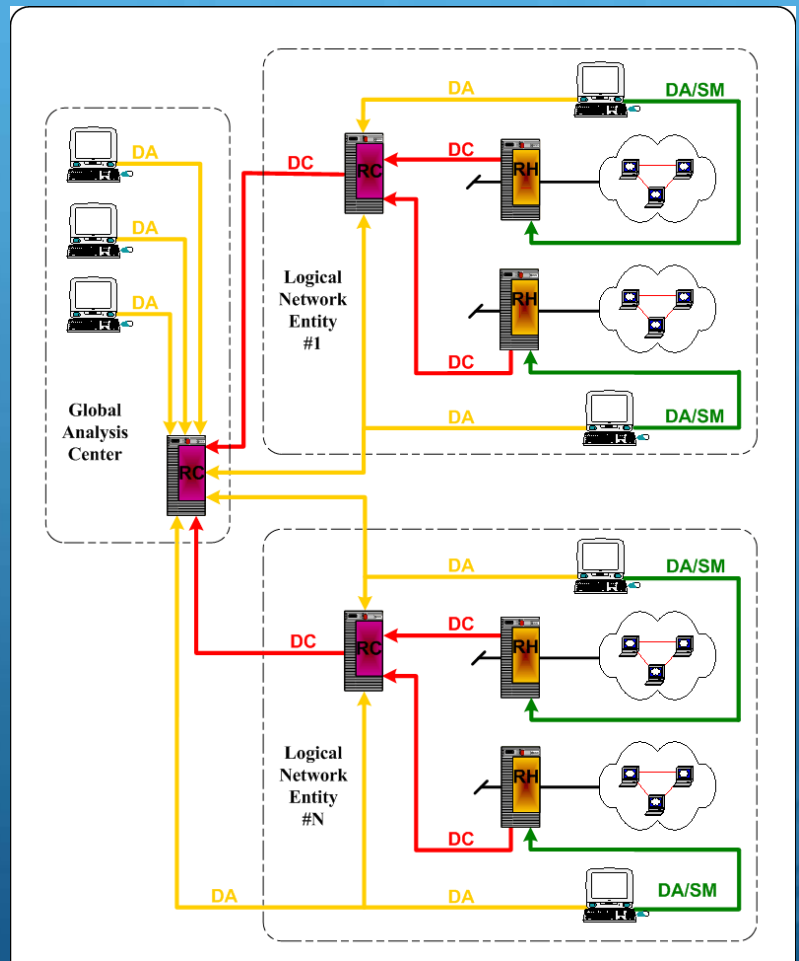
分布式蜜网技术

- 蜜网研究联盟Kanga分布式蜜网项目
  - 基于高交互式蜜罐技术
  - 由多个蜜网站点构成
- 低交互式、高交互式蜜罐相结合的分布式蜜网
  - NoAH欧盟分布式蜜罐项目
  - Matrix中国分布式蜜网项目(狩猎女神项目组、CNCERT/CC)

分布式蜜网构建模式：联邦制 VS. 邦联制



Federated



Confederated

Kanga分布式蜜网项目

- 由世界蜜网研究联盟(HRA)各支成员团队部署的蜜网构成，狩猎女神项目组是国内唯一参与站点
- 基于蜜网技术构建，采用Confederated邦联式
- 2004–2005: 基于第二代蜜网技术的Kanga分布式蜜网系统
- 2006–2007: 基于第三代蜜网技术的Kanga分布式蜜网系统 （升级中...）
- Roo CDROM
  - HoneyWall （单个站点的数据分析服务器）
  - Kanga Server （多个分布式站点的集中数据分析服务器）

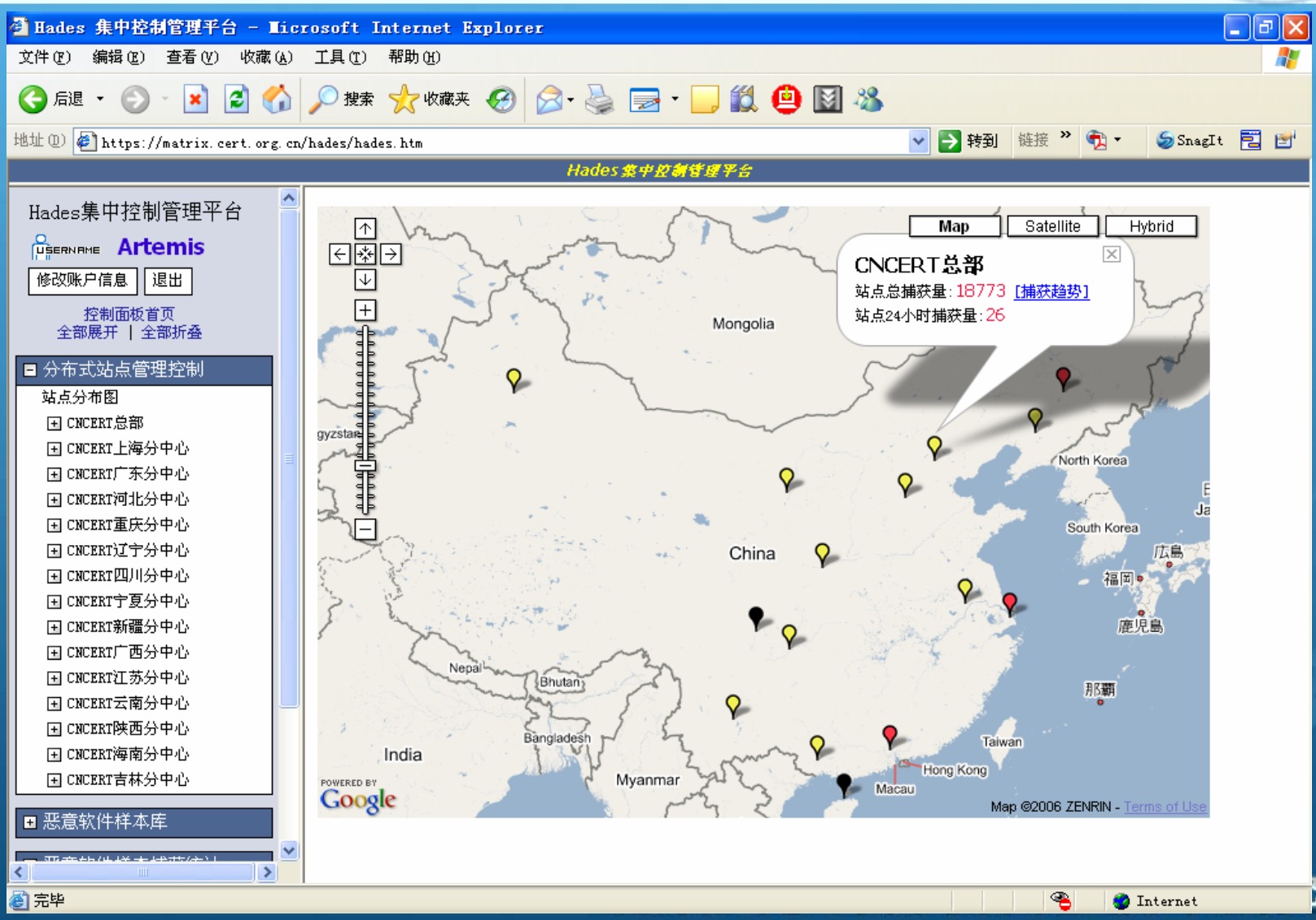
NoAH分布式蜜罐项目

- NoAH分布式蜜罐项目—欧盟第六框架计划项目
  - 项目协调者：FORTH(希腊技术研究基金会)
  - 项目参与方：Alcatel(法国阿尔卡特公司)、DFN-CERT(德国)、ETHZ(瑞士)、TERENA(荷兰)、VT(希腊) 、VU(荷兰阿姆斯特丹大学)
  - 项目周期：2005-2008 经费：243万欧元
  - 项目目标：基于蜜罐技术研发互联网安全监测基础设施，能够对互联网攻击进行检测和预警，为及时准确的响应提供支持。
  - 目前进度：设计阶段，部分原型系统实现如Argos

Matrix中国分布式蜜网项目

- CNCERT/CC发起，由北大狩猎女神项目组具体承担技术研发和部署
  - 2005一，项目经费：目前65万人民币
  - 目前在CNCERT/CC及分中心进行全国范围部署
  - 计划进一步在ISP安全管理部门等进行部署
- 分布式站点组成部件
  - 低交互式虚拟蜜罐一Honeyd/Nepenthes
  - 高交互式蜜罐一虚拟机/物理蜜罐+HoneyBow
  - 蜜网网关
  - 站点管理服务器
- 集中管理控制点
  - 集中管理控制服务器+数据库服务器
  - 恶意代码自动分析平台
  - 僵尸网络跟踪系统

Matrix中国分布式蜜网管理界面



蜜罐技术的发展趋势

- 分布式蜜罐/蜜网技术
- 应用层蜜罐技术
- 客户端蜜罐技术
- 蜜场技术

应用层蜜罐技术

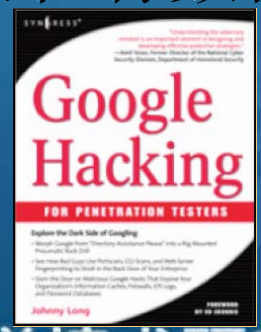
- 应用层攻击越来越普遍
  - 针对Web应用的攻击:
  - 针对数据库的攻击: SQL注入
- 应用层蜜罐技术—针对特定应用，构建对应用层攻击的诱骗环境
  - Web应用—Web Decoy Honeypot
    - Google Hacking Honeypot
    - PHP Honeypot
  - Email应用 — SMTP Decoy Honeypot
    - Jackpot SMTP Fake Server

Web应用的安全威胁

- WWW一直是互联网最为核心的应用
- WWW目前所面临的安全威胁
  - 自动寻找WWW安全漏洞的扫描器
    - nikto
  - WWW上主动传播的蠕虫
    - phpBB蠕虫、Witty蠕虫
  - 针对WWW的自动攻击工具
    - 用于自动获取页面信息的爬虫、自动获取远程控制的黑客工具
  - Google Hacking
    - 通过Google等搜索引擎寻找WWW安全漏洞
  - 手动攻击和渗透测试
    - 更为复杂、更具变化的攻击手段－如SQL注入攻击

Google Hacking

- Google等搜索引擎通过爬取WWW页面，并进行索引，以支持对互联网内容的查询
- Web服务器经常泄漏私有数据
  - 错误的设计和配置
  - 临时性、测试性的共享
  - Google等搜索引擎具有本地cache功能，一旦数据被cache，则数据拥有者将无法控制
- 存在安全漏洞的Web应用程序可被google搜索出
- Google Hacking — 通过Google搜索私有数据和存在安全漏洞的目标Web应用服务
  - Jonny Long (johnny.ihackstuff.com)
  - Google Hack Database (GHDB)



Google Hacking Honeypot

- 攻击者利用GHDB寻找漏洞主机和敏感信息
- Google Hacking Honeypot
  - 2005年2月，Ryan McGeehan
  - 低交互式Web应用层蜜罐
  - 利用GHDB指纹信息模拟存有漏洞的Web应用服务、敏感信息
  - 通过不可见的透明链接减少误报，防止fingerprinting
  - 只能通过爬虫和搜索引擎Bot访问Web站点
  - 保证模拟的Web服务被Google索引并拥有一个较高的page rank

PHP Honeypot Project

- 针对PHP Web应用的低交互式蜜罐
  - 模拟存在漏洞的PHP Web应用，为黑客和恶意代码提供攻击目标
  - 用于对PHP Web应用的安全威胁预警
    - 欺骗攻击者、减慢攻击速度
    - 检测攻击行为
    - 收集恶意代码（木马、蠕虫）
  - 案例
    - 应对Google Hacking攻击－如phpbb蠕虫
    - 应对Web漏洞扫描器－如nikto工具
    - 应对黑客－模拟一个shell，收集攻击指令，获取恶意代码

Jackpot SMTP Honeypot

- SMTP服务器面临安全威胁
  - 垃圾邮件发送者寻找开放的SMTP服务器作为其发送垃圾邮件的Open Relay
- Jackpot SMTP Honeypot
  - 架设一个模拟的SMTP Open Relay
  - 诱骗垃圾邮件发送者，记录其登录SMTP并发送垃圾邮件的过程
  - 垃圾邮件具体内容信息
  - 多个Jackpot可将捕获的垃圾邮件信息记入共享的数据库
  - http://jackpot.uk.net/

蜜罐技术的发展趋势

- 分布式蜜罐/蜜网技术
- 应用层蜜罐技术
- 客户端蜜罐技术
- 蜜场技术

客户端蜜罐技术

- 传统蜜罐/蜜网技术
  - 关注服务器端的安全威胁
- 客户端蜜罐技术
  - 互联网客户端面临的安全威胁越来越严重
    - 浏览器(IE, Firefox, ...)：恶意网站、间谍软件...
    - 邮件客户端(Outlook, Foxmail, ...)：垃圾邮件、病毒邮件...
    - IRC、IM、P2P...
  - 客户端蜜罐(client-side honeypot)
    - 模拟为普通的互联网客户端
    - 主动了解互联网上针对客户端的安全威胁

针对恶意网站/间谍软件的客户端蜜罐技术

- Honeyclient
  - http://www.honeyclient.org/
- HoneyC
  - http://honeyc.sourceforge.net/
- 微软研究院HoneyMonkey项目
  - http://research.microsoft.com/HoneyMonkey/
  - Automated Web Patrol with Strider HoneyMonkeys: Finding Web Sites That Exploit Browser Vulnerabilities, NDSS 2006
- 华盛顿大学
  - A Crawler-based Study of Spyware on the Web, NDSS 2006
- McAfee SiteAdvisor: http://www.siteadvisor.com/
- http://www.stopbadware.org/: 集成到Google

Strider HoneyMonkey

- 微软研究院Strider项目组HoneyMonkey
  - 基于主动客户端蜜罐技术
  - 关注发现攻击浏览器漏洞的恶意网站
  - 通过自动化的Web巡逻实现
    - 使用5000+初始恶意网站url列表：通过搜索引擎搜索hosts文件中的被阻断url列表
    - 测试指定url是否恶意网站：基于虚拟机和沙箱技术检测非预期执行的文件和对系统的修改
    - 虚拟机被感染后，通过revert进行恢复
    - 进一步测试恶意网页中的链接和重定向页面

HoneyMonkey结果

	Number of Unique Exploit URLs	Number of Exploit Sites
Total	752	287
WinXP SP1 Unpatched (SP1-UP)	688	270
WinXP SP2 Unpatched (SP2-UP)	204	115
WinXP SP2 Partially Patched (SP2-PP)	17	10
WinXP SP2 Fully Patched (SP2-FP)	0	0

Figure 1. Numbe **/June 2005 data).**

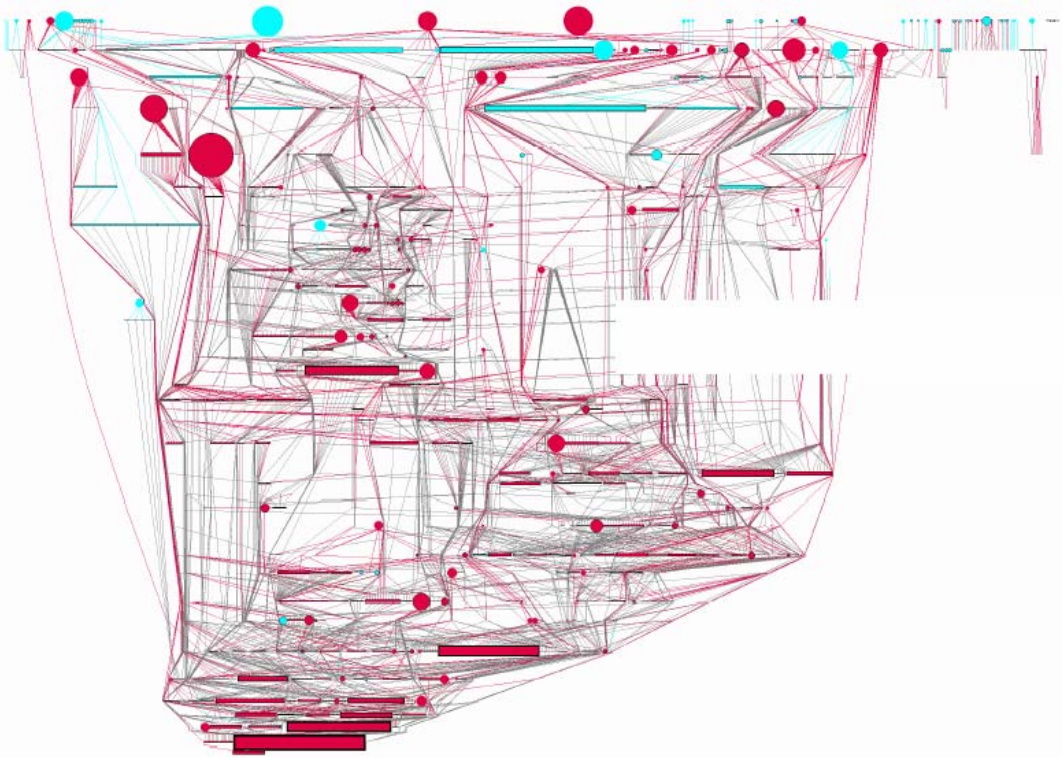
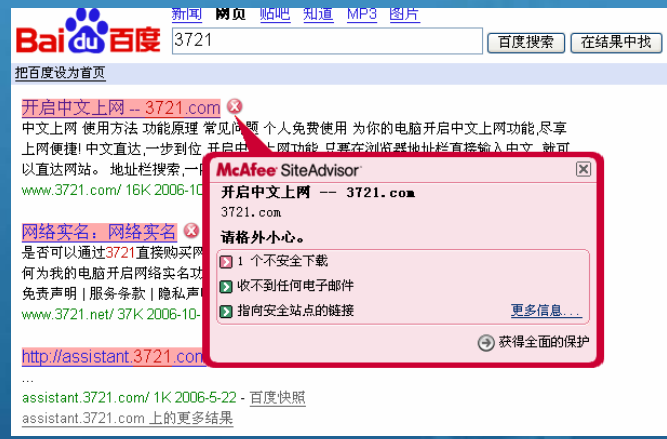


Figure 2. URL-level Topology Graph for WinXP SP1 Unpatched: 688 URLs from 270 sites

McAfee SiteAdvisor

- SiteAdvisor
  - 2005年4月MIT工程师创建
  - 2006年5月被McAfee购买
- 原理
  - 通过客户端蜜罐技术测试网站是否安全(95%访问量网站)
  - 对网站进行安全度评价
    - 是否可安全使用：弹出窗口、干扰
    - 是否可安全下载：有无病毒、间谍软件
    - 是否可安全提交：有无垃圾邮件
    - 是否可安全跳转：是否链接到恶意网站
    - 其他人的意见
  - 提供主流IE、Firefox浏览器插件
    - Google/Yahoo/MSN搜索结果的安全度
    - 帮助用户免受恶意网站、间谍软件侵扰



Email客户端蜜罐技术

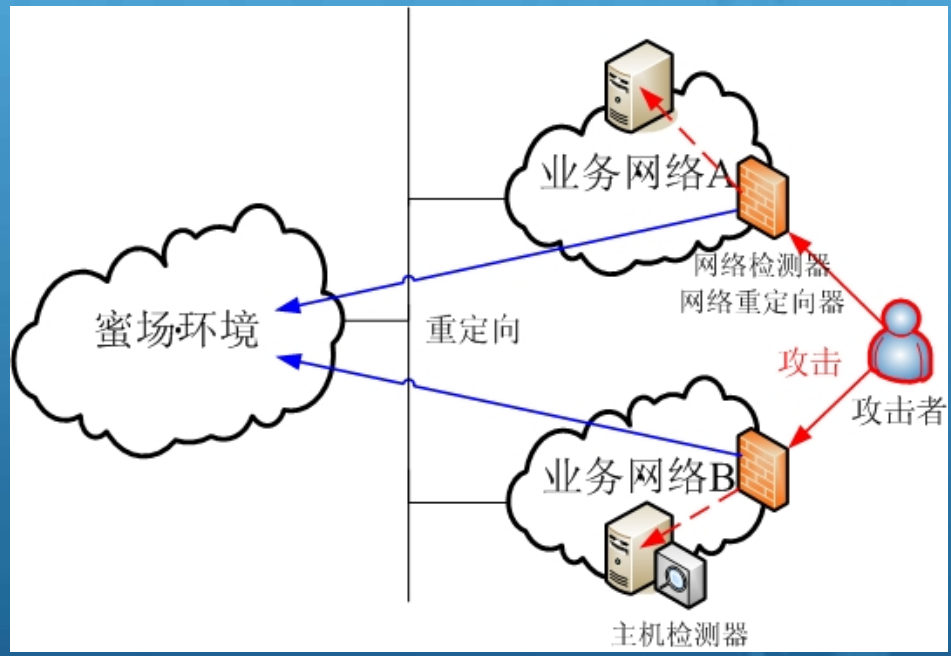
- HoneyEmail
  - 申请无任何业务用途的Email帐号
  - 通过各种途径散播这些Email帐号信息
    - 论坛注册、论坛透明发布等
  - 分析接收到的垃圾邮件、邮件病毒
- PR3(PRoactive PRivacy PRotection) Email Honeypot
  - 提供给某个服务提供商(如论坛)
  - 查看是否有来自其他服务提供商的邮件，以确认服务提供商是否执行其保护隐私承诺
- Email Honeyclient
  - 使用outlook客户端获取email中包含的URL，通过honeyclient下载
  - http://www.honeyclient.org/

蜜罐技术的发展趋势

- 分布式蜜罐/蜜网技术
- 应用层蜜罐技术
- 客户端蜜罐技术
- 蜜场技术

蜜场技术

- 蜜罐-蜜网-蜜场技术的演变过程
- 蜜场技术示意图
  - 结合蜜罐技术和攻击检测技术
  - 部署方式：分布式部署探测器+集中式部署蜜场
  - 面向大规模网络的新型主动防护技术



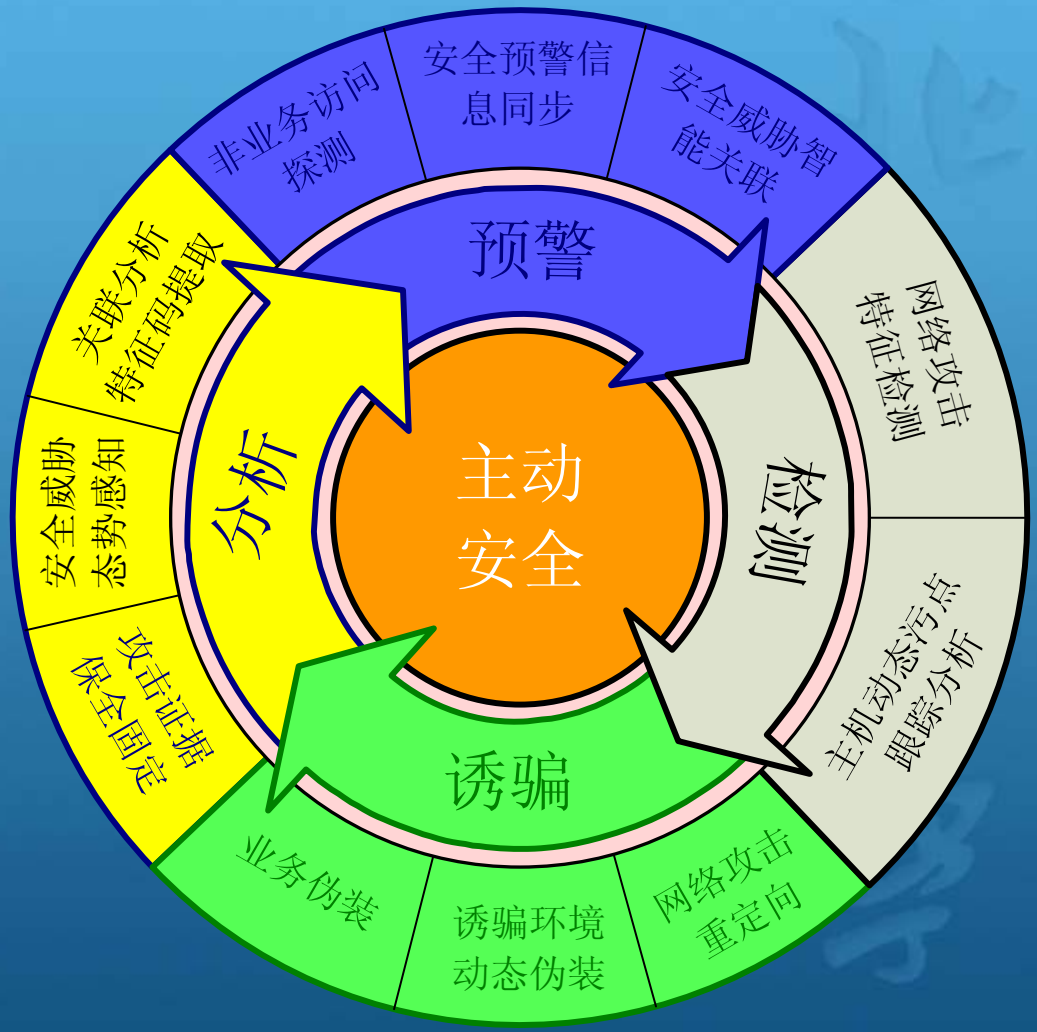
蜜场技术的核心思想

- 结合传统检测技术和蜜罐诱骗技术
  - 通过部署检测器发现针对业务网络的安全威胁
  - 将安全威胁重定向到蜜罐诱骗环境
  - 实施深入的取证分析
- 集中式部署蜜场环境
  - 在SOC安全操作中心集中部署
  - 通过重定向器将安全威胁透明地诱骗到蜜场中
  - 便于部署、维护和攻击取证分析

北京大学

基于蜜场技术构建主动安全体系

- 安全威胁预警
  - 非业务访问探测
  - 安全预警信息同步
  - 安全威胁智能关联
- 安全威胁检测
  - 网络攻击特征检测
  - 主机动态污点跟踪分析
- 攻击诱骗
  - 业务伪装
  - 诱骗环境动态伪装
  - 网络攻击重定向
- 攻击分析
  - 攻击证据保全固定
  - 安全威胁态势感知
  - 关联分析/特征码提取



休息、提问时间

10分钟