

# 网络蠕虫技术研究

郑 辉

清华大学网络中心

CCERT (CERNET Computer Emergency Response Team)

zhenghui@ccert.edu.cn

# 主要内容

- 网络蠕虫的历史
- 网络蠕虫采用的主要技术
- 网络蠕虫防范策略
- 网络蠕虫未来的发展趋势
- CCERT的主要研究成果

# 蠕虫的历史回顾

- Xerox PRAC, 1980年
- Morris Worm, 1988年11月2日
- WANK Worm, 1989年10月16日
- ADM Worm, 1998年5月
- Millennium, 1999年9月
- Ramen Worm, 2001年1月
- Lion Worm, 2001年3月23日
- Adore Worm, 2001年4月3日
- Cheese Worm, 2001年5月
- Sadmin/IIS Worm, 2001年5月
- CodeRed Worm, 2001年7月19日
- Nimda Worm, 2001年9月18日
- Slapper, 2002年9月14日
- Slammer, 2003年1月25日
- Dvldr32, 2003年3月7日
- MSBlaster, 2003年8月12日
- Nachi, 2003年8月18日

# 2004年蠕虫

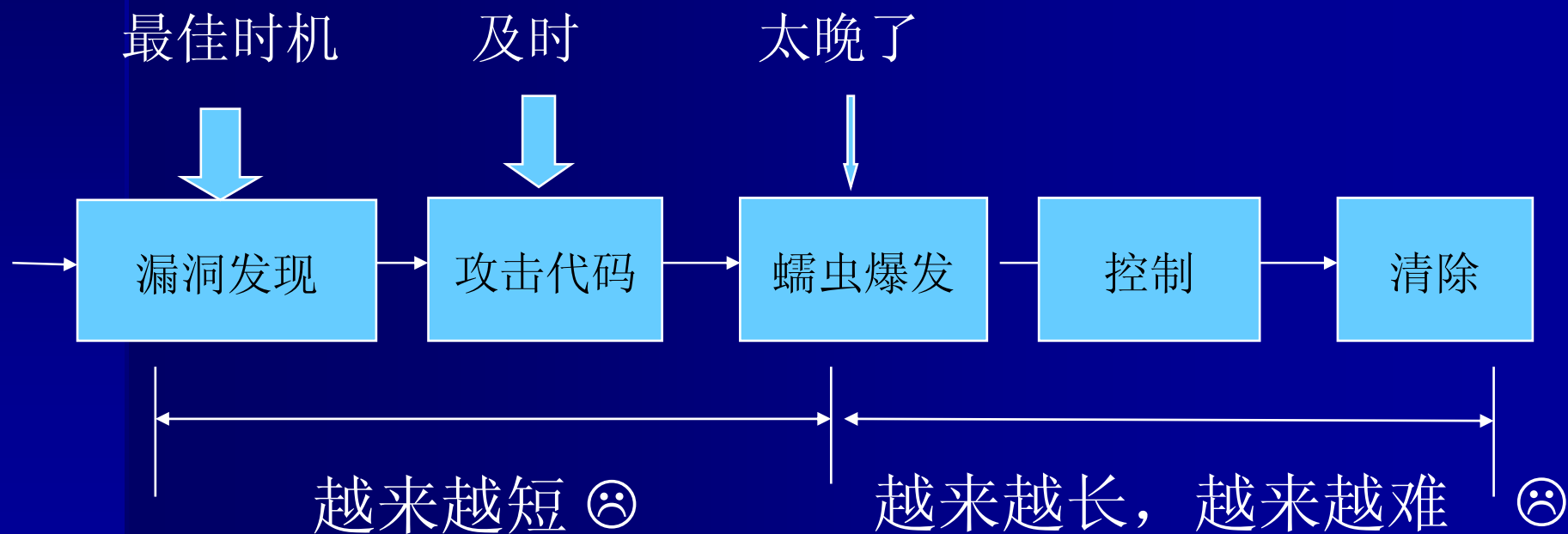
- MyDoom.C 2004年2月9日
- Witty Worm 2004年3月20日
- Sasser Worm 2004年4月30日
- Santy Worm 2004年12月21日

# 恶意移动代码的简单比较

	Internet 蠕虫	病毒邮件	文件系统 病毒	网页脚本	木马
传播速度	极快	快	一般	慢	慢
传播方式	自动	半自动	半自动	人工	人工
影响对象	网络	网络	主机	主机	主机
防治难度	难	难	易	易	一般
经济损失	严重	较大	较大	一般	一般

# 蠕虫的爆发周期越来越短...

- 漏洞公布和蠕虫爆发的间隔越来越短



# 各种恶意移动代码的融合趋势

- 蠕虫、病毒、木马之间的界限已经不再明显；
- 综合使用多种攻击手段：
  - 传播：计算机系统的漏洞、电子邮件、文件共享、Web浏览等
  - 社会工程（social engineering）

# 攻防主体

- 影响网络安全的三支力量
  - Hacker
  - VXer
  - Cracker
- 防范主体
  - 网络运营商、服务提供商、用户；
  - 系统厂商、防毒产品厂商；
  - 科研技术人员、政府主管部门；

# 网络蠕虫采用的主要技术

- 缓冲区溢出
- 口令破解
- 预设信任机制
- 路径限制突破
- ...

# 网络蠕虫防范策略

- 预防阶段
- 检测阶段
- 遏制阶段
- 清除阶段

# 预防阶段

- 补丁管理
  - 搜集、分类;
  - 自动升级机制;
- 漏洞扫描
  - 周期性检测
  - 通知

# 检测阶段

- IDS
- 流量分析

# 遏制阶段

- 封堵
- 延迟
- 疏导

# 清除阶段

- 病毒软件
- 手工
- 打补丁
- 防火墙规则调整

# 网络蠕虫的技术发展趋势

- 结合人工智能技术;
- 动态功能升级技术;
- 多平台传播技术;
- 分布式实体技术;

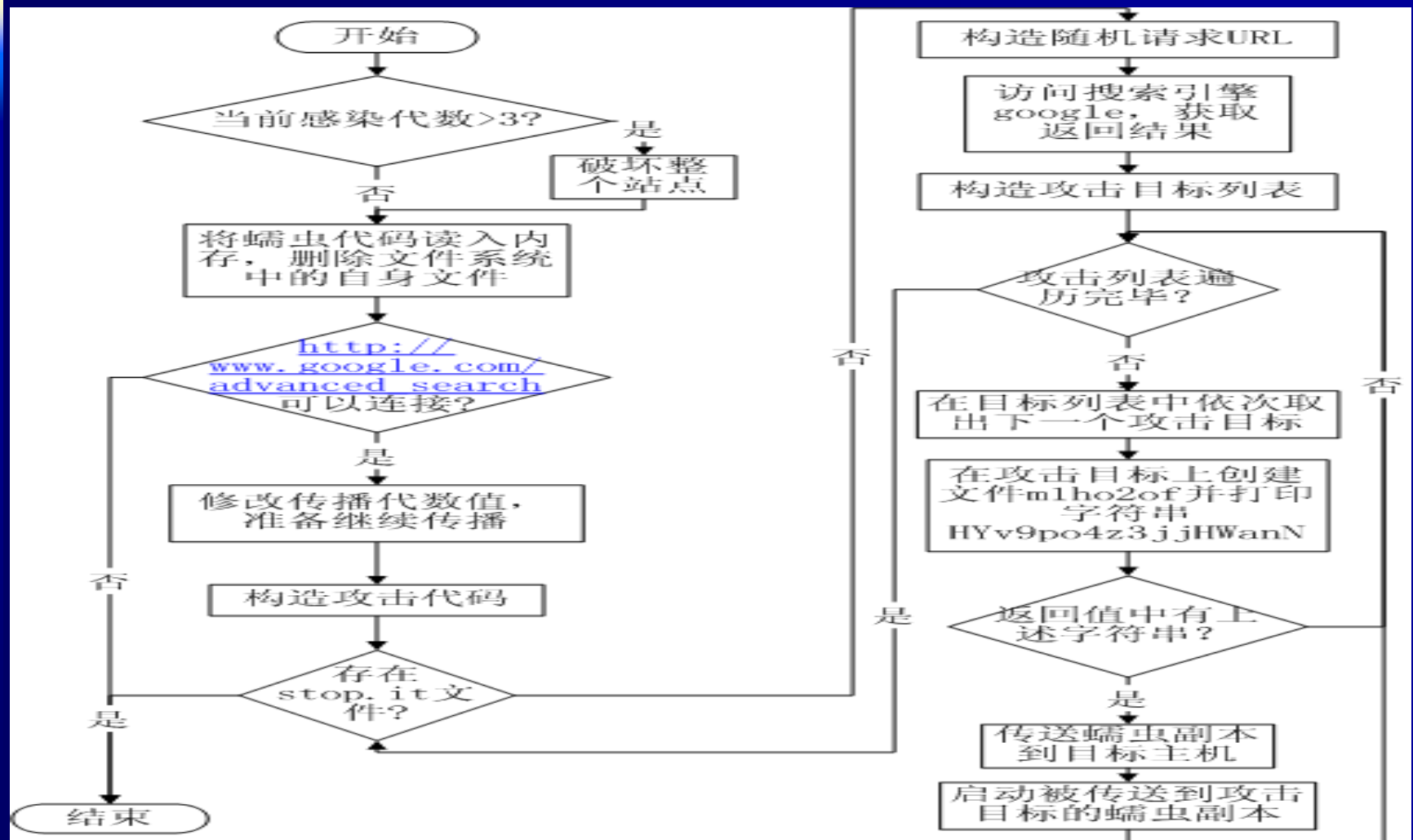
# Santy蠕虫

- 描述：
  - 2004年12月21日发现，截止到12月22日，google可以统计到被santy蠕虫破坏的网站已经达到26000多；
  - 利用论坛系统phpBB的漏洞传播；
- 智能特性：
  - 从搜索引擎google得到攻击站点列表；
- 存在形式：
  - 脚本代码；

# This site is defaced!!!

*NeverEverNoSanity WebWorm generation 25.*

# Santy蠕虫工作流程



# 攻击目标列表构造

- 构造查询请求

- 随机字符插入

- @ts = qw/t p topic/, \$ts[int(rand(@ts))],  
int(rand(30000));

- [http://www.google.com/search?num=100&hl=en&lr=&as\\_qdr=all&q=allinurl%3A+%22viewtopic.php%22+%22topic%3D1234%22&btnG=Search](http://www.google.com/search?num=100&hl=en&lr=&as_qdr=all&q=allinurl%3A+%22viewtopic.php%22+%22topic%3D1234%22&btnG=Search)

- 返回结果处理

- 仅保留IP地址或URL

- 生成攻击目标列表

# Santy.B 蠕虫

## ■ AOL

– 错误:

<http://search.aol.com/aolcom/search?q=viewtopic.php%3Ft%3D1234&Stage=0&page=2>

– 正确:

<http://search.aol.com/aolcom/search?query=viewtopic.php%3Ft%3D1234&Stage=0&page=2>

## ■ Yahoo:

– <http://cade.search.yahoo.com/search?p=viewtopic.php%3Ft%3D1234&ei=UTF-8&fl=0&all=1&pstart=1&b=2>

# Santy.C 蠕虫

- Google

- `http://www.google.com.br/search?q=inurl:*.php?*=1234&start=10`

- Yahoo

- 错误:

- `http://cade.search.yahoo.com/search?p=inurl:*.php?*=1234&ei=UTF-8&fl=0&all=1&pstart=1&b=123`

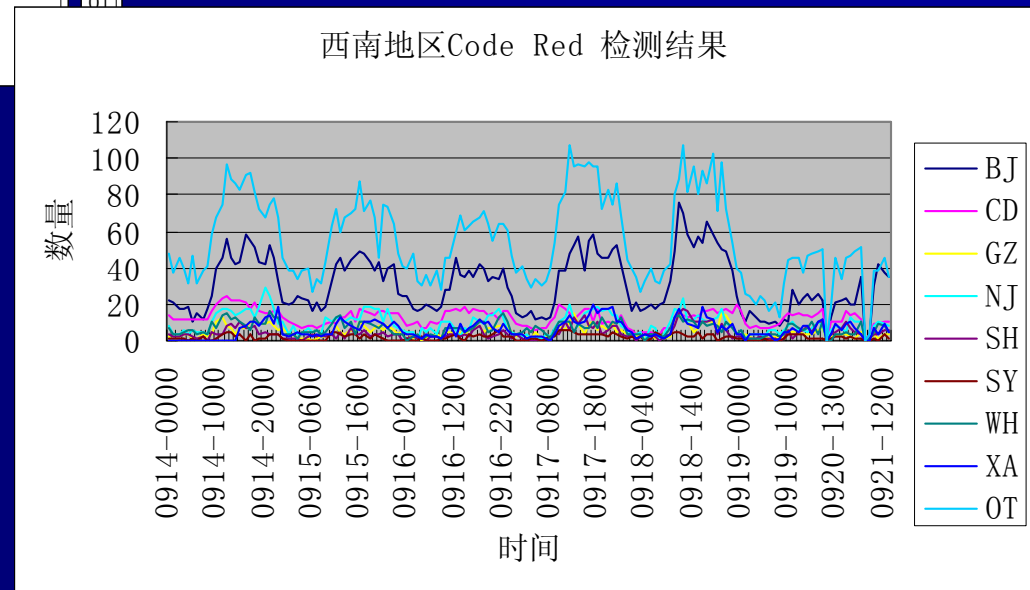
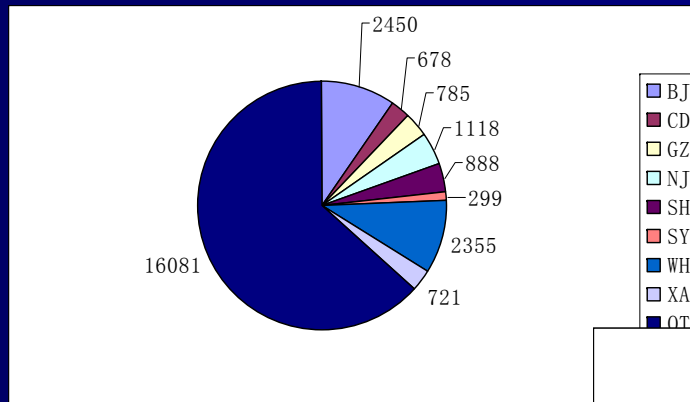
- 正确:

- `http://cade.search.yahoo.com/search?p=*.php?*=1234&ei=UTF-8&fl=0&all=1&pstart=1&b=123`

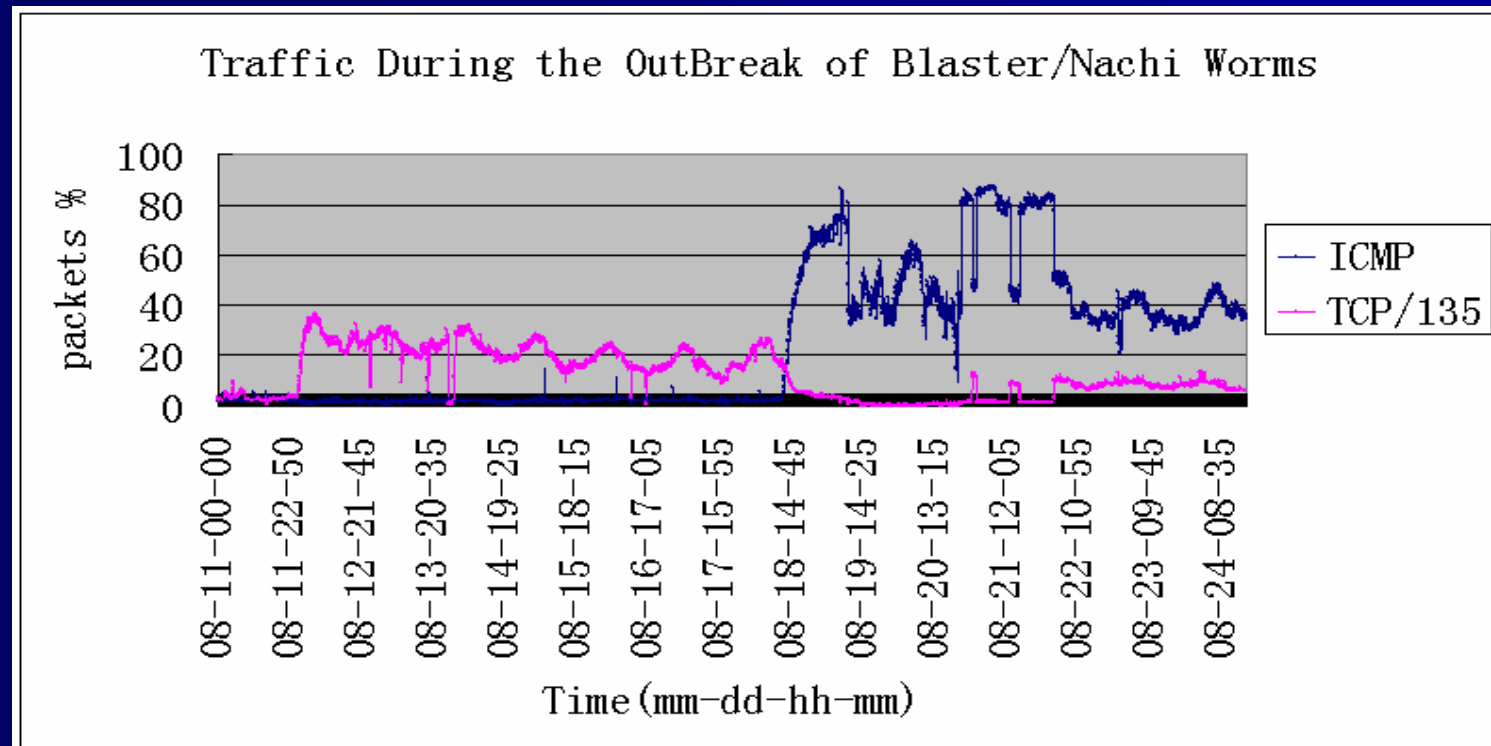
# CCERT的科研优势

- 长期对恶意移动代码研究的积累；
- 迅速有效的响应机制；
- 第一手的网络数据；

# CodeRed蠕虫监测数据



# Blaster & Nachi 监测数据

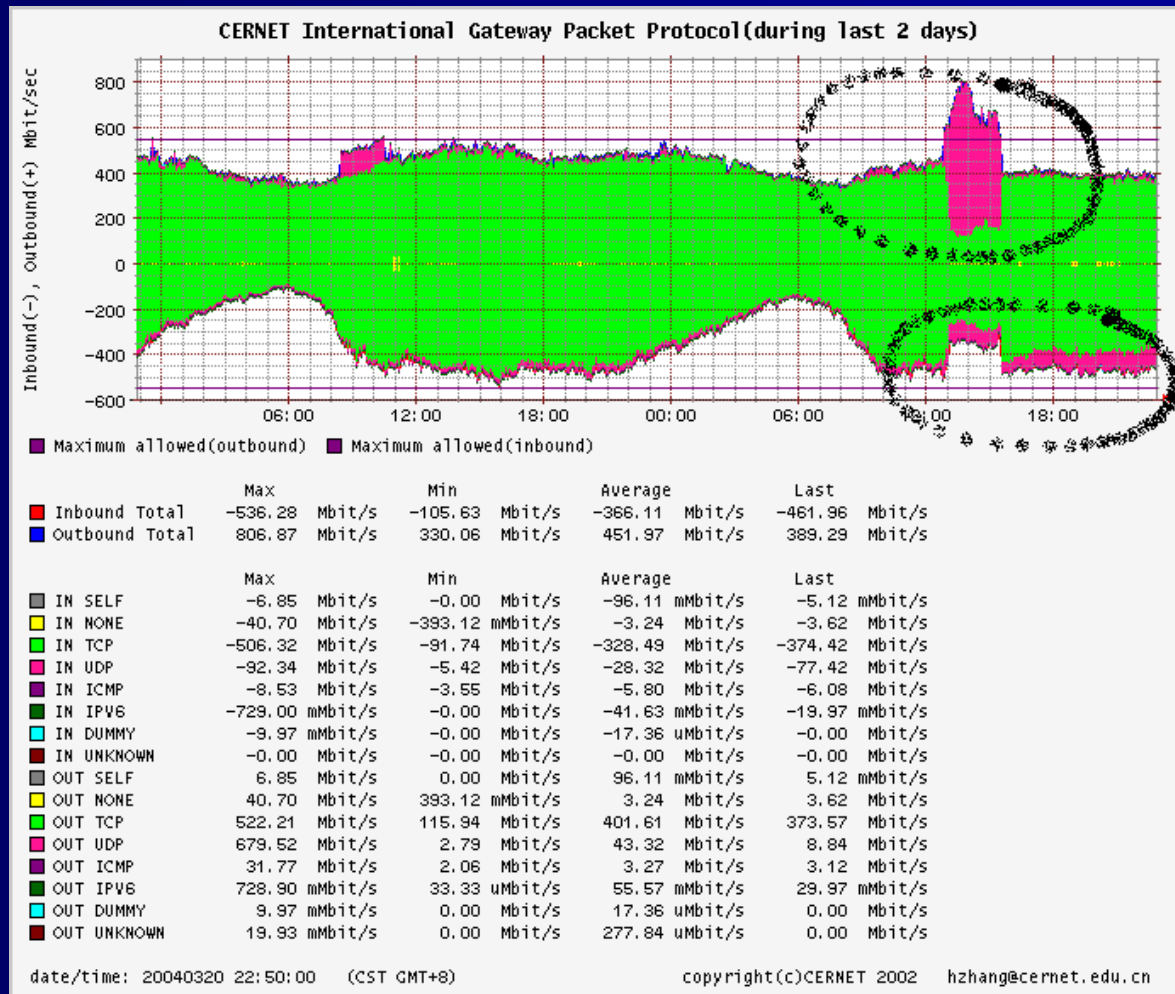


# Sasser蠕虫监测数据



图一、清华校园网 Sasser 蠕虫感染数量统计

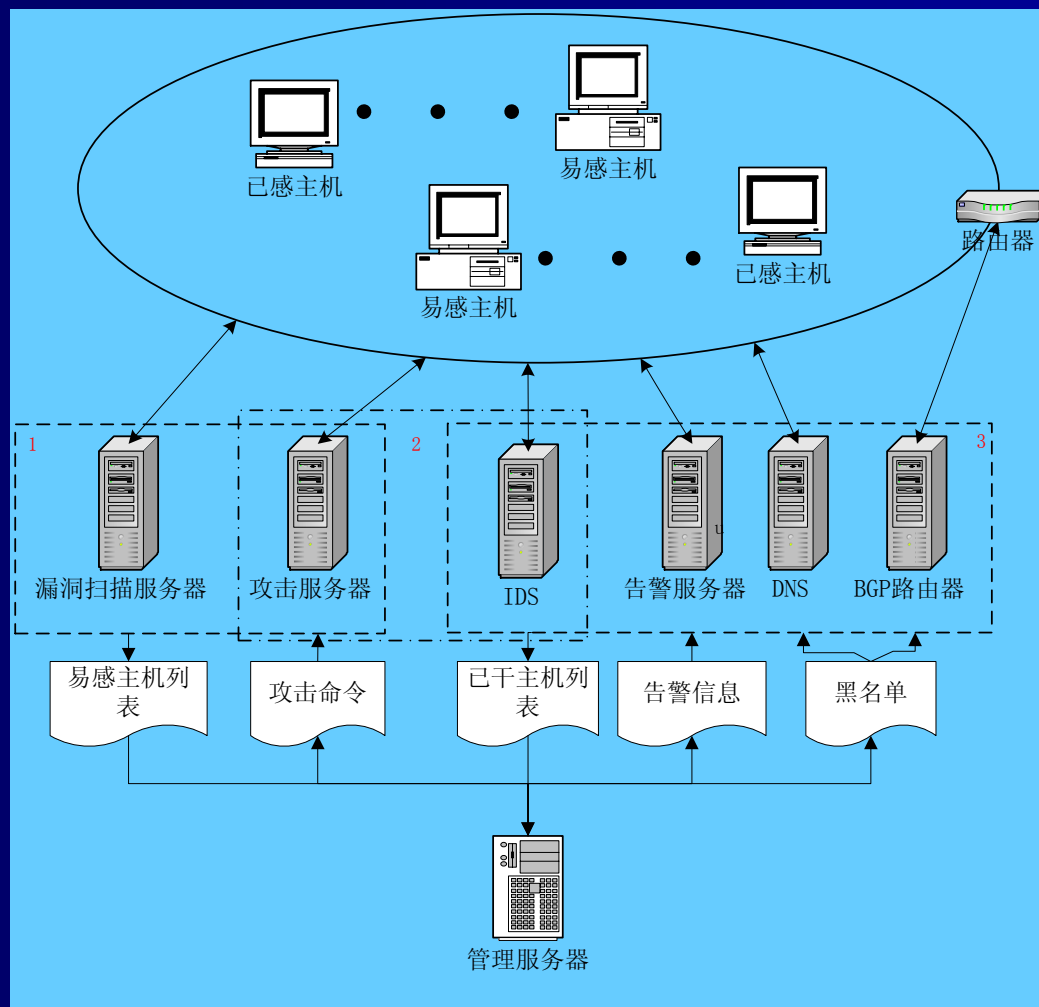
# Witty 蠕虫监测数据



# 主要研究成果

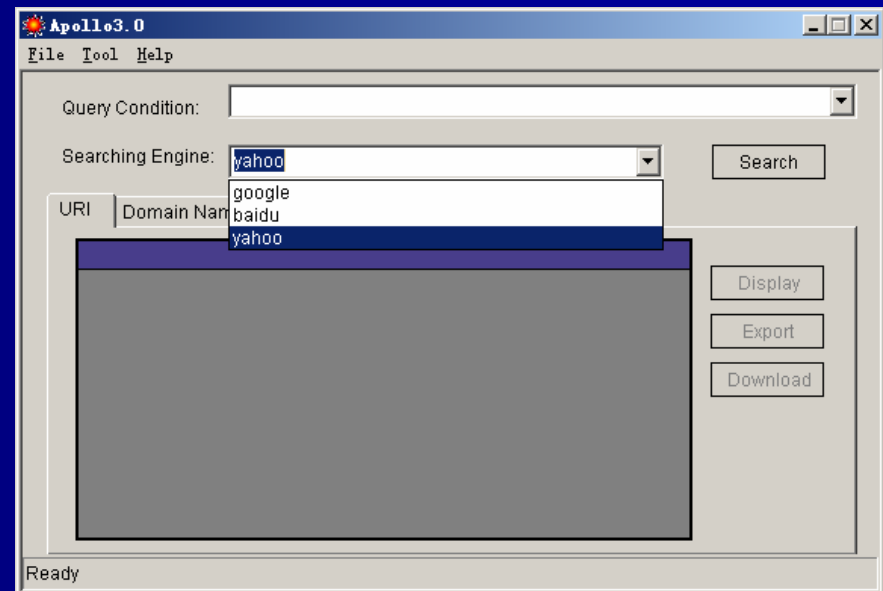
- 针对蠕虫个体
  - 实体结构模型
  - 功能结构模型
- 针对网络
  - 利用DNS服务抑制蠕虫传播
  - Internet 蠕虫主动防治系统

# Internet 蠕虫主动防治系统



# Google Hacking 风险评估工具：Apollo

- Apollo V3.0
  - 多搜索引擎支持；
  - 开放式配置框架；
- Apollo V2.0
  - 基于GHDB的域检测；
  - 全部查询结果支持；
  - 多线程；
  - 日志；
- Apollo V1.0
  - 多语言查询；
  - URL、域名、IP地址导出；
  - 文件下载；
  - GHDB支持；



# Apollo

The screenshot displays the Apollo2.0 application interface. The main window shows a search query "密码 filetype:xls site:cn" and a list of results under the "IP Address" tab. A smaller window in the foreground shows a detailed view of the search results, including a list of URIs and a table of file details.

**Query Condition:** 密码 filetype:xls site:cn

**URI | Domain Name | IP Address**

URI	Domain Name	IP Address
http://www.petrochina.com.cn/chinese/cphfw/iccard/1.xls	www.petrochina.com.cn	202.96.255.90
http://info.cwi.gov.cn/download/mail.xls	info.cwi.gov.cn	211.155.27.140
http://www.itonline.gd.cn/service/doc/host.xls	www.itonline.gd.cn	202.38.64.11
http://www.fj-innofund.gov.cn/jhb/2004_1.xls	www.fj-innofund.gov.cn	211.154.222.19
http://www.qhu.edu.cn/software/username.xls	www.qhu.edu.cn	202.107.194.196
http://www.gs.edu.cn/news/mailusers1.xls	www.gs.edu.cn	202.120.192.44
http://www.gs.edu.cn/news/mailusers.xls	www.gs.edu.cn	218.30.103.84
http://www.mqmt.uestc.edu.cn/UploadFile/200412171121021082.xls	www.mqmt.uestc.edu.cn	210.51.169.143

**Something is wrong?**

大小	类型	修改日期	属性
29 KB	Microsoft Excel...	2005-1-7 9:16	A
32 KB	Microsoft Excel...	2005-1-7 9:16	A
86 KB	Microsoft Excel...	2005-1-7 9:18	A
26 KB	Microsoft Excel...	2005-1-7 9:18	A
21 KB	Microsoft Excel...	2005-1-7 9:18	A
37 KB	Microsoft Excel...	2005-1-7 9:18	A
26 KB	Microsoft Excel...	2005-1-7 9:18	A
164 KB	Microsoft Excel...	2005-1-7 9:18	A
17 KB	Microsoft Excel...	2005-1-7 9:18	A
143 KB	Microsoft Excel...	2005-1-7 9:18	A
99 KB	Microsoft Excel...	2005-1-7 9:18	A
33 KB	Microsoft Excel...	2005-1-7 9:18	A
408 KB	Microsoft Excel...	2005-1-7 9:20	A
125 KB	Microsoft Excel...	2005-1-7 9:20	A
20 KB	Microsoft Excel...	2005-1-7 9:20	A
22 KB	Microsoft Excel...	2005-1-7 9:20	A
19 KB	Microsoft Excel...	2005-1-7 9:20	A
48 KB	Microsoft Excel...	2005-1-7 9:20	A
152 KB	Microsoft Excel...	2005-1-7 9:20	A
89 KB	Microsoft Excel...	2005-1-7 9:21	A
230 KB	Microsoft Excel...	2005-1-7 9:21	A
14 KB	Microsoft Excel...	2005-1-7 9:21	A
281 KB	Microsoft Excel...	2005-1-7 9:21	A
40 KB	Microsoft Excel...	2005-1-7 9:21	A
26 KB	Microsoft Excel...	2005-1-7 9:21	A
121 KB	Microsoft Excel...	2005-1-7 9:21	A
415 KB	Microsoft Excel...	2005-1-7 9:23	A
282 KB	Microsoft Excel...	2005-1-7 9:23	A
76 KB	Microsoft Excel...	2005-1-7 9:23	A
106 KB	Microsoft Excel...	2005-1-7 9:23	A
54 KB	Microsoft Excel...	2005-1-7 9:23	A
157 KB	Microsoft Excel...	2005-1-7 9:23	A
14 KB	Microsoft Excel...	2005-1-7 9:23	A
53 KB	Microsoft Excel...	2005-1-7 9:23	A
41 KB	Microsoft Excel...	2005-1-7 9:23	A
123 KB	Microsoft Excel...	2005-1-7 9:23	A
159 KB	Microsoft Excel...	2005-1-7 9:23	A
120 KB	Microsoft Excel...	2005-1-7 9:23	A

Done

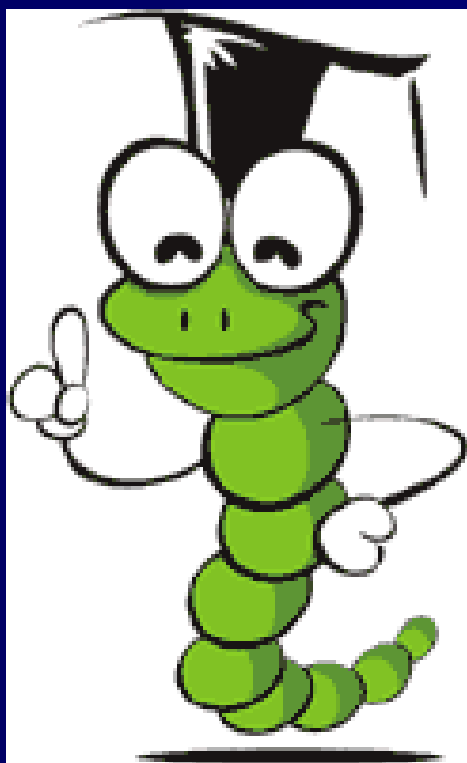
84 个对象

16.8 MB

我的电脑

# References

- 蠕虫的行为特征描述和工作原理分析,  
<http://worm.ccert.edu.cn/doc/spark/WormBehaviorPrincipleAnalysis.pdf>
- Internet蠕虫研究,  
<http://worm.ccert.edu.cn/doc/InternetWormResearch.pdf>
- 大规模网络中Internet 蠕虫主动防治技术研究 -- 利用DNS 服务抑制蠕虫传播,  
<http://worm.ccert.edu.cn/doc/spark/WormDefenseWithDNS.pdf>
- 主动Internet蠕虫防治技术-接种疫苗,  
<http://worm.ccert.edu.cn/doc/Vaccination.pdf>
- Internet蠕虫主动防治系统原理与设计,  
<http://worm.ccert.edu.cn/doc/spark/WormDefenseSystem.pdf>
- 郑辉, Santy蠕虫分析报告。  
<http://worm.ccert.edu.cn/doc/spark/santywormanalysis.doc>
- Mimi, Apollo for Google Hacking,  
<http://worm.ccert.edu.cn/GoogleHacking/Apollo/index.html>



谢谢！