



INFORMATION SECURITY DECISIONS



Hosted by  

Beat Back the Botnets

The Automation of Computer Network Attack

David Dittrich
The Information School/
Center for Information Assurance and Cybersecurity
University of Washington



INFORMATION SECURITY DECISIONS

Hosted by  

Overview


- Where did "bots" come from?
- How do they work?
- How botnets are built
- How are they used for attacking?
- How do you defend against them?
- Botnets in *action!*

INFORMATION SECURITY DECISIONS

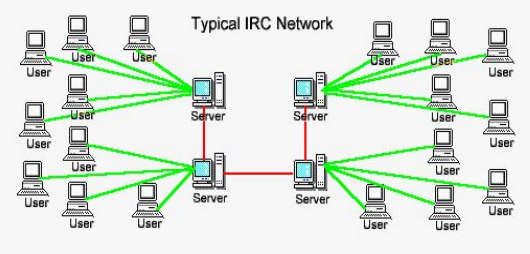
Hosted by  

Where did "bots" come from?

INFORMATION SECURITY DECISIONS

Hosted by  SearchSecurity.com


Internet relay chat



The diagram illustrates a typical IRC network. It consists of several servers connected to each other in a mesh-like structure. Each server is connected to a group of users. The servers are represented by icons of a computer tower and a monitor, while the users are represented by icons of a laptop and a monitor. Green lines represent the connections between users and their local servers, and red lines represent the connections between the servers themselves.

<http://www.newircusers.com/network.html>

INFORMATION SECURITY DECISIONS

Hosted by  SearchSecurity.com

IRC bots


(1) What exactly is an IRC bot?

It is a computer program that logs onto IRC and does things automatically, based upon its programming. Technically, any script or client which has automatic responses could be classified as a bot, even your IRC client such as mIRC for Windows. Although the most commonly accepted definition of an IRC bot is "an unmanned chat-client which idles on a channel and responds automatically to predefined events".

A group of bots which are linked together is called a network or botnet. Bots are linked into botnets for several reasons, such as sharing common user lists and channel settings (who to op, who to ban, etc.), as well as to provide a method to simultaneously control several bots. Botnets also provide an internal chat network similar to, but independent of, IRC. Bot users DCC chat or telnet into a bot and then can have conversations with other bot users on the same botnet, and not have to worry about server lag or splits.

<http://www.irchelp.org/irchelp/misc/botfaq.html#1>


INFORMATION SECURITY DECISIONS

Hosted by  SearchSecurity.com

Original (benign) uses for bots


- Keep track of channel users
- Transfer files automatically
- Enforce kick/ban lists of "bad" users
- Protection from *channel takeovers*

INFORMATION SECURITY DECISIONS

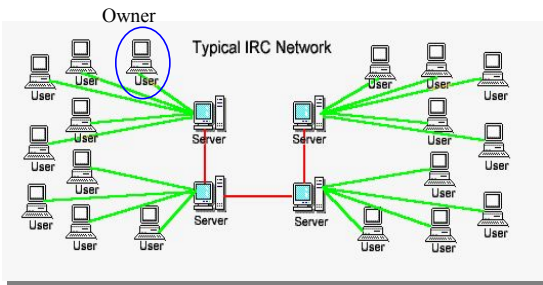
Hosted by  SearchSecurity.com

How do bots work?


INFORMATION SECURITY DECISIONS

Hosted by  SearchSecurity.com

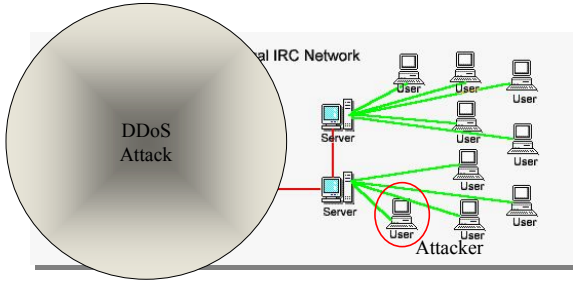
"Net split" attack (before)



INFORMATION SECURITY DECISIONS

Hosted by  SearchSecurity.com

"Net split" attack (after)



INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

"Net split" attack (defense)

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Eggdrop config file

```
#3v- eggdrop v1.1.5 -- kicker -- written Wed Sep 17 12:26:41 1997
ecl-leet f3jd7dg95p6t ofbsh /0 0 0 0
:      *!*eclipse@leet-net.com
:      leet-net.com:6005
:      { created 874462154}
synth 95c8jx6293uy9 ofb /0 0 0 0
-      *!recon@.pulsar.net, *!*eclipse@.pulsar.net
:      alpha.pulsar.net:6005
:      { created 874462189}
stuph tsrntv0lxiw ofb /0 0 0 0
-      *!andrew@.en.com
:      shell.en.com:6005
!!     874505247 #isp-ops
:      { created 874462190}
brutal s2636tx63bvdj ofb /0 0 0 0
-      *!niczak@parodius.com
:      parodius.com:6005
!!     874469770 #telia020
:      { created 874462190}
```

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

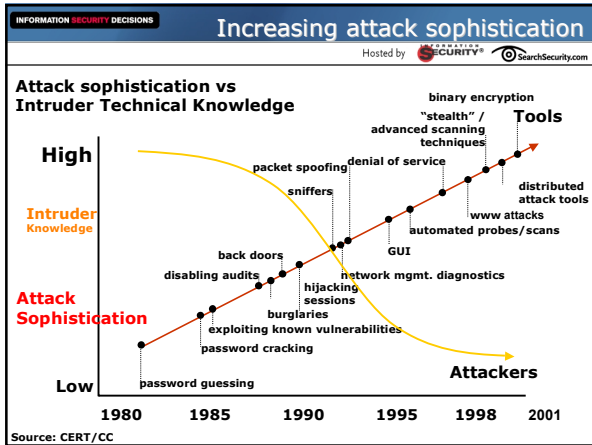
Encrypted communications

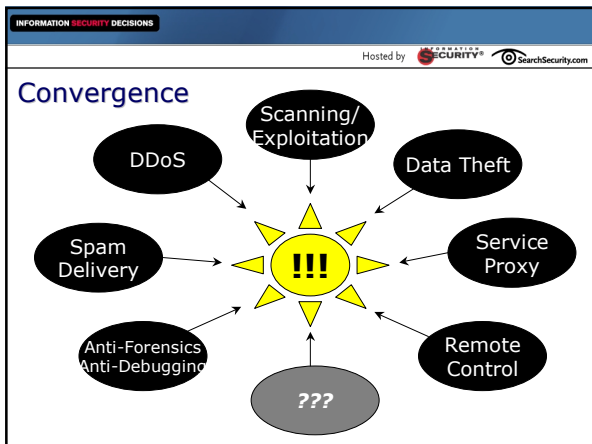
netbots.tcl v1.16 (25 April 1999)
 A secure botnet commands script with encrypted communication. Commands include nethelp, netbots, netinfo, netshell, netserv, netpass, netsave, nethash, netsay, netact, netnotice, netjoin, netpart, netchanset, and netcycle. This is the old standalone version of netbots.tcl, [click here for latest version](#).

INFORMATION SECURITY DECISIONS



Hosted by SearchSecurity.com

My how these bots have grown...







INFORMATION SECURITY DECISIONS

Hosted by  

Early Bot features (1994)

- Channel controls
- Simple file transfers
- Password protected back door



INFORMATION SECURITY DECISIONS

Hosted by  

PrettyPark.exe (1999)

- Email worm/trojan
- Connects to 1 of 13 IRC servers
- Serves as remote access trojan (RAT)
- Rumored to have spam delivery features

INFORMATION SECURITY DECISIONS

Hosted by  



Kaiten bot (2001)

```

/*****
* This is a IRC based distributed denial of service client. It connects to
* the server specified below and accepts commands via the channel specified.
* The syntax is:
* <nick> <command>
* You send this message to the channel that is defined later in this code.
* Where <nick> is the nickname of the client (which can include wildcards)
* and the command is the command that should be sent. For example, if you
* want to tell all the clients with the nickname starting with N, to send you
* the help message, you type in the channel:
* !N* HELP
* That will send you a list of all the commands. You can also specify an
* asterick alone to make all client do a specific command:
* !* SH uname -a
* There are a number of commands that can be sent to the client:
* TRUNMI <target> <secs> - A PUSH/ACK flooder
* FAN <target> <port> <secs> - A SYN flooder
* UDP <target> <port> <secs> - An UDP flooder
* UNKNOWN <target> <secs> - Another non-spoof udp flooder
* NICK <nick> - Changes the nick of the client
* SERVER <server> - Changes servers
* GETSPOOFS - Gets the current spoofing
* SPOOFS <subnet> - Changes spoofing to a subnet
* DISABLE - Disables all packeting from this bot
* ENABLE - Enables all packeting from this bot
* KILL - Kills the knight
* GET <http address> <save as> - Downloads a file off the web
* VERSION - Requests version of knight
* NITLALL - Kills all current packeting
* HELP - Displays this
* IRC <command> - Sends this command to the server
* SH <command> - Executes a command
* Remember, all these commands must be prefixed by a ! and the nickname that
* you want the command to be sent to (can include wildcards). There are no
* spaces in between the ! and the nickname, and there are no spaces before
* the !
*****/

```



INFORMATION SECURITY DECISIONS

Hosted by  

W32/Leaves (Summer 2001)

- Harvests hosts compromised with SubSeven trojan
- Advanced use of encryption
- Synchronizes clocks!?!



INFORMATION SECURITY DECISIONS

Hosted by  

Power bot (August 2001)

- Scans, compromises, proxies, DDoS
- Implements reflected DDoS
- Witnessed
 - 9,106 systems compromised
 - 40 hosts pushing 50Mbps continuous for >2 hours

INFORMATION SECURITY DECISIONS

Hosted by  



Agobot/Phatbot (2004)

Phatbot Feature List
 (Many of these features are also present in Agobot)

- ▶ Has the ability to polymorph on install in an attempt to evade antivirus signatures as it spreads from system to system
- ▶ Checks to see if it is allowed to send mail to AOL, for spamming purposes
- ▶ Can steal Windows Product Keys
- ▶ Can run an IDENT server on demand
- ▶ Starts an FTP server to deliver the trojan binary to exploited hosts - ends the FTP session with the message "221 Goodbye, have a good infection :)"
- ▶ Can run a socks, HTTP or HTTPS proxy on demand
- ▶ Can start a redirection service for GRE or TCP protocols
- ▶ Can scan for and use the following exploits to spread itself to new victims:
 - ▶ DCOM
 - ▶ DCOM2
 - ▶ MyDoom backdoor
 - ▶ DameWare
 - ▶ Locator Service (Update: This exploit appears to be non-functional)
 - ▶ Shares with weak passwords
 - ▶ WebDav
 - ▶ WKS - Windows Workstation Service

<http://www.lurhq.com/phatbot.html>



INFORMATION SECURITY DECISIONS

Hosted by  

Agobot/Phatbot (2004)

- **Update 2004-04-20** - Newer versions of Agobot and Phatbot have added scanner modules for:
 - Bagle virus backdoor
 - CPanel resetpass vulnerability
 - UPnP (MS01-059)
 - MSSQL weak administrator passwords
- Attempts to kill instances of MSBlast, Welchia and Sobig.F
- Can sniff IRC network traffic looking for logins to other botnets and IRC operator passwords
- Can sniff FTP network traffic for usernames and passwords
- Can sniff HTTP network traffic for Paypal cookies
- Contains a list of nearly 600 processes to kill if found on an infected system. Some are antivirus software, others are competing viruses/trojans
- Tests the available bandwidth by posting large amounts of data to the following websites:
 - www.st.lib.keio.ac.jp
 - www.lib.nthu.edu.tw
 - www.stanford.edu
 - www.xo.net
 - www.uwente.nl
 - www.schlund.net
- Can steal AOL account logins and passwords
- Can steal CD Keys for several popular games
- Can harvest emails from the web for spam purposes
- Can harvest emails from the local system for spam purposes



INFORMATION SECURITY DECISIONS

Hosted by  

Agobot NetBIOS password list

admin, Admin, password, Password, 1, 12, 123, 1234, beer, !@#\$, asdfgh, !@#%\$, !@#\$%^, !@#\$%^&, !@#\$%^&*, WindowsXP, windows2k, windowsME, windows98, windoze, hax, dude, owned, lol, ADMINISTRATOR, rooted, noob, TEMP, share, r00t, freak, ROOT, TEST, SYSTEM, LOCAL, SERVER, ACCESS, BACKUP, computer, fucked, gay, idiot, Internet, test, 2003, 2004, backdoor, whore, wh0re, CNN, pwned, own, crash, passwd, PASSWD, iraq, devil, linux, UNIX, feds, fish, changeme, ASP, PHP, 666, BOX, Box, box, 12345, 123456, 1234567, 12345678, 123456789, 654321, 54321, 111, 000000, 00000000, 11111111, 88888888, fanny, pass, passwd, database, abcd, oracle, sybase, 123qwe, fool, server, computer, Internet, super, 123asd, ihavenopass, West, godblessyou, enable, xp, 23, 2002, 2600, 0, 110, 2525, newfy, 111111, 121212, 123123, 1234qwer, 123abc, 007, alpha, 1776, newfie, patrick, pal, administrator, root, sex, god, foobar, 1778, a, aaa, abc, test, temp, win, pc, asdf, secret, drugs, qwer, yxcv, zxcv, home, xxx, owner, login, Login, west, Coordinatore, Administrador, Verwalter, Ospite, administrator, Default, administrator, admins, teacher, student, superman, wmd, supersecret, kids, penis, wwwadmin, database, changeme, dope, test123, user, private, 69, root, 654321, xxyzz, asdfghjkl, mybaby, vagina, pussy, leet, metal, work, school, mybox, box, werty, baby, porn, homework, secrets, x, z, bong, qwertyuiop, secret, Administrateur, abc123, password123, red123, qwerty, admin123, zxcvbnm, poluytrewa, pwd, pass, love, mypc, texas, Texas, Washington, washington, Tennessee, tennessee, jackdaniels, whiskey, whiskey, azerty, poiut, mouse, ordinateur, souris, imprimeur, cederom, cédérom, bière, biere, moonshine, athlon, oil, operon, écran, ecran, reseau, carte, merde, mince, ami, amie, copin, copine, 42, harry, dumbdore, hagrid, potter, hermione, hermine, gryffindor, azkaban, askaban, cauldron, buckbeak, hogwarts, dementor, quidditch, madre, switch, mypass, pw, NULL

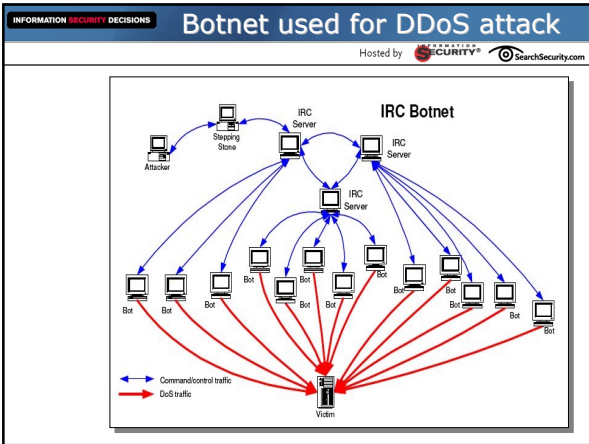
INFORMATION SECURITY DECISIONS

Hosted by  

Relationship to DDoS

(Dates approximated)

Year	Bots (Benign)	Single-source DoS	Classic DDoS (Handler/Agent)	Remote Control Trojans	DDoS Botnets
1996	High	None	None	None	None
1997	High	None	None	None	None
1998	High	Low	None	None	None
1999	High	Low	None	None	None
2000	High	Low	Low	Low	None
2001	High	Low	Low	Low	Low
2002	High	Low	Low	Low	Low
2003	High	Low	Low	Low	Low
2004	High	None	Low	Low	Low
2005	High	None	None	Low	Low



- Advances in C2 & security features**
- Encryption of communications
 - Use of Peer-to-Peer
 - "Swiss Army knife" feature set
 - Polymorphism and Anti-Anti-Virus
 - Anti-forensics/Anti-debugging

Numbers (that are public)

Program	Year	Typical	Largest
<i>Trinoo, Stacheldraht</i>	1999	100s	5,000
Knight	2001	100s	1,500
Power	2001	*	10,000
Leaves	2001	*	23,000
Sdbot, gt-bot, Deloder	2003	1,000s	140,000
Agobot/Phatbot	2004	10,000s	750,000

INFORMATION SECURITY DECISIONS

Hosted by INFORMATION SECURITY SearchSecurity.com

How are botnets built?

INFORMATION SECURITY DECISIONS

Hosted by INFORMATION SECURITY SearchSecurity.com

"It takes malware..."



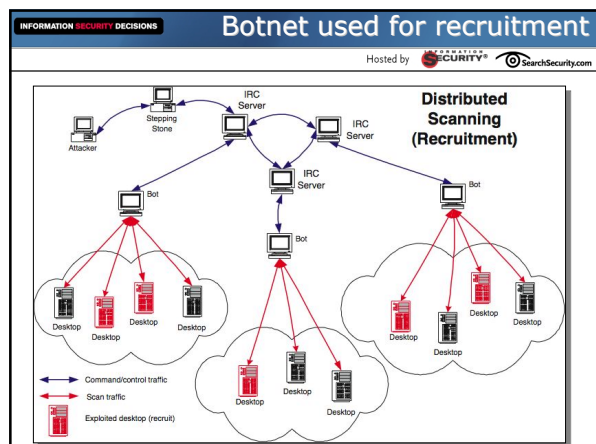
Schwabert

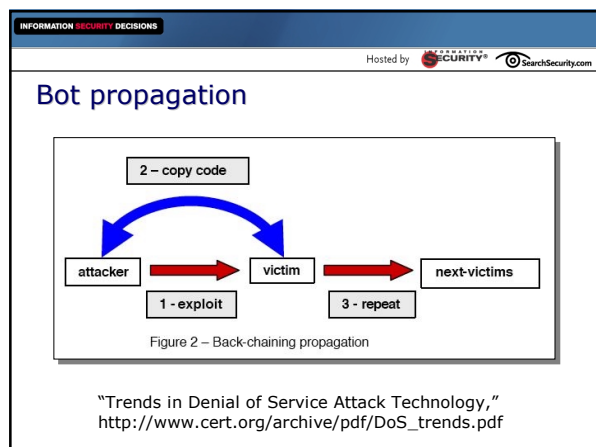
INFORMATION SECURITY DECISIONS

Hosted by INFORMATION SECURITY SearchSecurity.com

Strategies in botnet creation

- Learn about IRC commands and features
- Choose a bot or "blended threat" kit
- Get access to some computers
 - Trade for CCs, other hosts/accounts, or buy
 - Use a virus, trojan horse, or other "sploit"
 - "War drive" to find free wireless access
- Herd your bots
- Try to keep someone from finding/stealing them





Growth of botnets

Hosted by SearchSecurity.com

Alarm growing over bot software

By Robert Lemos CNET News.com April 30, 2004, 9:16 AM PT

Add your opinion [TALKBACK](#) Forward in [EMAIL](#) Format for [PRINT](#)

[Security](#) [MS Windows](#) [Symantec Corp](#) [Microsoft Corp](#)


While many network administrators worry about the next worm, security experts are warning that a more equally damaging threat is slowly gaining networks of computers.

Known as bot software, the remote attack tool and place themselves on vulnerable computer systems silently in the background, letting an attacker snoop to the system while its owner works away, oblige versions of the software created by the security firm let attackers control compromised computers, servers and peer-to-peer networks, command attack other computers and steal information from systems.

Bot stealthiness
Anxiety is understandable, given that Symantec and the Cooperative Association for Internet Data Analysis, or CAIDA--two groups thought to have some of the best data on Internet attacks--both undercounted the extent of the MSBlast infection by an order of magnitude.

The group...

INFORMATION SECURITY DECISIONS


Hosted by  SearchSecurity.com

Phases of botnet/DDoS attacks

- **Phase one: "own" a [bleep!]-load of computers!**
- **Phase two: use them to attack others**
 - DDoS
 - More "owning"
 - Anonymity while doing crimes

INFORMATION SECURITY DECISIONS

The new spammers

Hosted by  SearchSecurity.com

Another site, hosted by the Polish group, offers free credit consultations. Traceroutes to the site, removeform.com, also provided ever-changing results, ranging from a DSL line in Israel to another provided by EarthLink. However, the title of the site's home page consistently read "Yahoo Web Hosting," suggesting it was actually located on a server run by the Internet giant.

According to Tubul, his group uses a special software developed by the Polish group that routes traffic between spammers' websites through thousands of the hijacked computers. The numerous intermediary systems confound tools such as traceroute, effectively laundering the true location of the website. To utilize the service, customers simply configure their sites to use any of several domain-name system servers controlled by the Polish group, Tubul said.

While the price may be steep, such services "definitely" will frustrate antispyammers and others who try to track down the true address of rogue Internet sites, according to Joe Stewart, a security researcher with Ludwig.

"I wish we could get a list of the names of the people who are using these services," said Stewart. "About all you can do is try to follow the money -- sign up for whatever it is they're selling and try to figure out who's behind the whole thing."

The use of such stealth hosting techniques has become widespread among spammers, according to Steve Linford, leader of the Spamhaus Project, which maintains a blacklist of known junk e-mail operations. Linford blamed the development of the new methods on the recent alliances between spammers and computer crackers.

"Hackers used to detest spammers, but now that spamming has become such a big business, it's suddenly cool to be a spammer," Linford said. He said the junk e-mail business has also recently attracted "engineers who have been laid off or fired, and people who really know what they're doing with networking and DNS."

INFORMATION SECURITY DECISIONS

... and fraudsters

Hosted by  SearchSecurity.com

Phishing attacks powered by 'just five' zombie networks

Grime Wearden
ZDNet UK
October 20, 2004, 18:10 BST

All phishing attacks launched across the Internet come from one of just five networks of zombie PCs, according to research published by security firm CiperTrust this week.

CiperTrust based its claim on data collected from companies that use its IronMail messaging security product. By analysing phishing emails to find the IP addresses of the computers that sent them, CiperTrust says it found that every day a different set of around 1,000 zombie computers were used to deliver phishing emails.

Phishing emails typically purport to come from a major financial institution, and try to trick the recipient into visiting a fake Web site and revealing their banking details.

By monitoring which computers were involved with which phishing attacks, CiperTrust concluded that each one was part of one of five zombie networks, also called botnets. A zombie PC is one that has been secretly taken over by a malicious hacker, typically when the user falls victim to a virus.

"Phishing attacks represent a collaboration of the world's most skilled hackers and organised crime -- instead of breaking into the bank to take money, phishers are tricking users into handing over their account information, or rather the electronic keys to the vault," said Paul Judge, chief technology officer at CiperTrust, in a statement.

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

The new gangsters

DDoS protection racket targets online bookies

By [John Leyden](#)
Published Monday 26th November 2001 15:47 GMT

Organised criminals are using distributed denial of service (DDoS) attacks to force online bookmakers into protection rackets, a British security consultancy says.

Victims are subjected first to a network-based denial of service attack, which can render their site unavailable for a time. When this ceases, they are approached by an "Internet security consultancy" which promises that attacks can be stopped, in return for a monthly payment.

DDoS extortion attempts according to Neil Brown, technical director of the consultancy.

Requests for payment from the criminals involved appeared to go through Russia, though the provenance of the gang, or gangs, is uncertain. Firms who

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Assoc. of Remote Gambling Operators (ARGO)

- **US\$73M paid in extortion in 2004**
- **US\$10K - \$40K per attack (some multiple)**
- **Each attack lasts hours to > 1 week**
- **518,000 "computers" used in one attack**
- **3 arrested in July 2004**
 - By following the \$\$, not by traceback
 - Several gangs still active worldwide

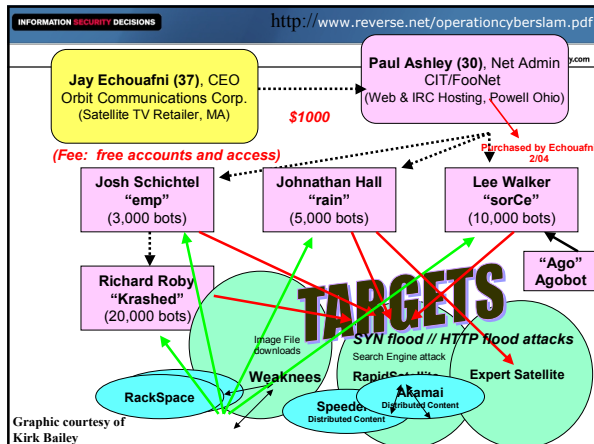
"Gambling Sites, This Is A Holdup: Organized criminal hackers threaten to paralyze their networks if they don't pay up," Business Week, http://www.businessweek.com/magazine/content/04_32/b3895106_mz063.htm

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Phatbot DDoS attack methods

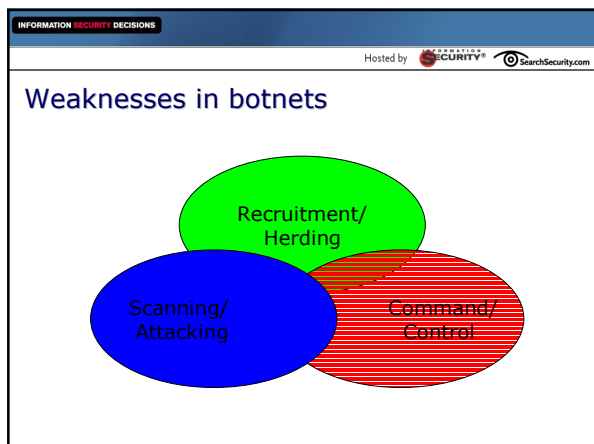
- **Two types of SYN floods, UDP & ICMP**
- **"Targa"**
(random IP protocol, fragmentation, and frag offset)
- **"Wonk"**
(one SYN packet followed by 1023 ACK packets)
- **HTTP**
(single GET w/delay in hours, or recursive GET)
- **Many attacks support various spoofing**
(/16, /24 or all 32 bits)





INFORMATION SECURITY DECISIONS Hosted by SearchSecurity.com

Strategies in botnet defense

- Learn about IRC commands and features
- Learn about bots, DDoS, other malware
<http://staff.washington.edu/dittrich/misc/ddos, and book>
- Gain data collection and analysis skills
 - Host forensics
 - Network forensics
 - Reverse engineering, programming, scanning, etc.
- Analyze traffic flows, patterns
- Key goals: *Identify structure and C2 methods*





INFORMATION SECURITY DECISIONS

Hosted by  

How bot herders attempt to evade detection

- Conceal malware on hosts
- Obfuscate bot host names in C2 traffic
- Tactical botnet herding
- Advanced features



INFORMATION SECURITY DECISIONS

Hosted by  

Concealment on hosts

- Rootkits
- Window hiding (old mIRC bot trick)
- Packers and "Cryptors"
(<http://www.woodmann.com/crackz/Packers.htm>)
- NTFS alternate data streams
(<http://securityfocus.com/infocus/1822>)



INFORMATION SECURITY DECISIONS

Hosted by  

Obfuscation of bot host names

- dR-XI33ch408@IRCSoulZ-24267.vt.edu
- dR-Amazing-11@201.129.63.IRCSoulZ-11894
- [uNi]-Gangsta-047@29655c0f.2486bca.dhcp4.washington.edu
- [AC]Codec@1f49225e.385a42df.297f4433.27ad84c0.IP
- tMp-C031@WarezX.biz
- [w4a]-050@455216627A4331AD666E4E0E7E1x



INFORMATION SECURITY DECISIONS

Hosted by  

Tactical botnet herding

- **Dynamic DNS to point to servers**
- **Channel hopping**
- **Server hopping**
- **Code swapping**
- **Redirection or feedback via HTTP**
- **Combine the above**

INFORMATION SECURITY DECISIONS



Hosted by  

Advanced bot hardening

- **Detection of virtual machine use**
- **Detection of debugger use**
- **Defeat ptrace**
- **Binary encryption**
- **Encryption of C2**

(Reverse Engineering skills helpful)

INFORMATION SECURITY DECISIONS

Hosted by  

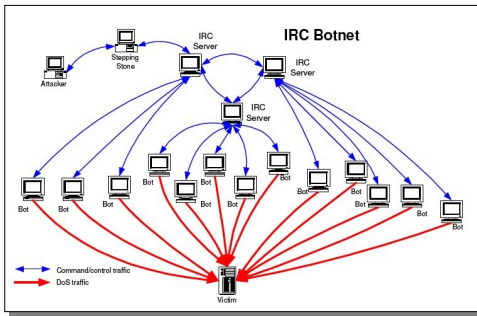
How to identify and dismantle bots

- **Identify your role in botnet**
- **Identify C2 traffic, channels, nicks**
- **Identify vulnerability being exploited and malware being used**
- **Produce detailed report (and preserve evidence)**
- **Enlist cooperation of other sites in cleaning up bots, handlers, caches, etc.**
- **Report to CERT/CC and federal law enforcement**

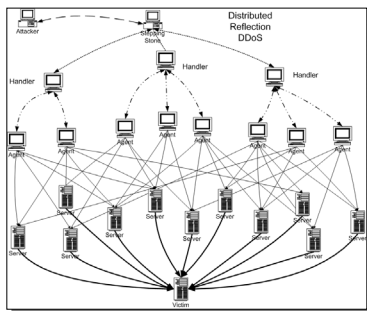
Identifying your role in a botnet

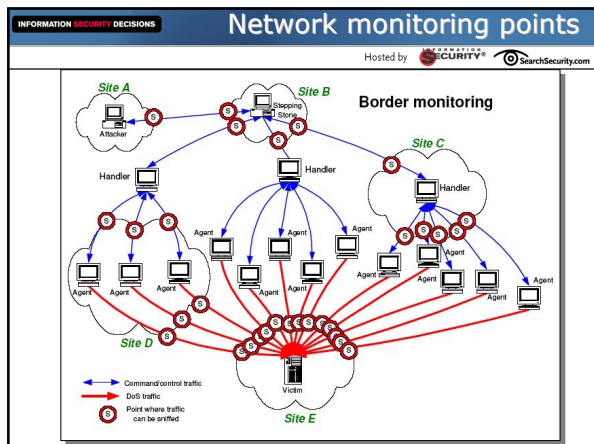
- **Two phases of attack**
Phase 1: Massive ownage
Phase 2: Mayhem
- **Stepping stone?**
- **Handler?**
- **Agent?**
- **Victim of secondary attack?**

Prototypical IRC botnet



Reflected DDoS attack





INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Putting it together

- **Need to get from Site E to Site A**
- **Speed is essential**
- **Cooperation required**
- **Accurate data a must**

Legend:
 - Blue arrow: Command control traffic
 - Red arrow: DDoS traffic
 - Red circle: Point where traffic can be sniffed

INFORMATION SECURITY DECISIONS



Hosted by SearchSecurity.com

I'm not a network engineer ...

... nor do I play one on TV. But if *you* are:



- "ISP Security: Real World Techniques," by Gemberling, Morrow & Greene
<http://www.nanog.org/mtg-0110/greene.html>
- Team Cymru web site
<http://www.cymru.com>
- "Managing the Threat of Denial of Service," CERT/CC
http://www.cert.org/archive/pdf/Managing_DoS.pdf

INFORMATION SECURITY DECISIONS

Hosted by  

Botnets in action



INFORMATION SECURITY DECISIONS

Hosted by  

Nmap scan

```
Starting nmap 3.45 ( http://www.insecure.org/nmap/ ) at 2004-03-23 19:29 PST
Insufficient responses for TCP sequencing (0), OS detection may be less accurate
Interesting ports on d-192-168-8-150.dhcp.washington.edu (192.168.8.150):
(The 39434 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE
413/tcp   open  auth
435/tcp   open  merpc
439/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
497/tcp   open  dantz
1050/tcp  open  java-or-OTGfileshare
11009/tcp open  unknown
39158/tcp open  unknown
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows XP Professional SP1 or Windows 2000 SP3
Nmap run completed -- 1 IP address (1 host up) scanned in 661.742 seconds
```

INFORMATION SECURITY DECISIONS

Hosted by  

Services provided by bot

```
(As a side note, it is generally unwise to connect to services
running on compromised hosts, as it is unclear what function they
provide and whether the connection will be noticed. A tactic
that works in these cases to minimize the danger of exposure of
an analysts workstation is to use a static IP address that is used
for no other reason than to make connections to untrusted hosts,
for precisely this reason. During this analysis, I simply
forgot to do it this time. My bad, as you will see in a moment.)

Connecting to port 11009 elicits a prompt:

<----->
220 Bot Server (Win32)
<----->

Connecting to port 39158 elicits a stream of bytes. The type is
not recognized by "file":

<----->
39158.bin: data
<----->
```

INFORMATION SECURITY DECISIONS

Hosted by SECURITY SearchSecurity.com

Speed tests

```

2004/03/23 21:27:00.73370 192.168.9.100:8145 -> 212.227.147.70:80 [MP]
50 4f 63 54 30 2f 20 48 54 54 50 2f 31 2e 30 0d POST / HTTP/1.0.
0a 48 6f 73 74 3a 20 77 77 77 2e 63 63 68 6c 75 .Host: www.schlu
6e 64 2e 6e 65 74 0d 0a 43 6f 6e 74 05 6e 74 0d .Content-Len: 204800...
4c 65 6e 67 74 68 3a 20 32 30 34 38 30 30 0d 0a .Length: 204800...
0d 0a 67 67 67 67 67 67 67 67 67 67 67 67 67 67 .....
c7 67 67 67 67 67 67 67 67 67 67 67 67 67 67 .....
07 67 67 67 67 67 67 67 67 67 67 67 67 67 67 .....
[duplicate lines deleted]

2004/03/23 21:27:02.46514 192.168.9.100:8257 -> 66.96.192.201:80 [MP]
50 4f 63 54 30 2f 20 48 54 54 50 2f 31 2e 30 0d POST / HTTP/1.0.
0a 48 6f 73 74 3a 20 77 77 77 2e 62 75 72 73 74 .Host: www.zburnt
2e 6e 65 74 0a 0d 6f 6e 74 05 6e 74 0d 6c 65 .Content-Length:
6e 67 74 68 3a 20 32 30 34 38 30 30 0d 0a 0d 0a .Length: 204800...
8c 8c 8c 8c 8c 8c 8c 8c 8c 8c 8c 8c 8c 8c 8c .....
8c 8c 8c 8c 8c 8c 8c 8c 8c 8c 8c 8c 8c 8c 8c .....
[duplicate lines deleted]

2004/03/24 10:52:31.474564 192.168.10.5:1028 -> 212.227.147.70:80 [MP]
50 4f 63 54 30 2f 20 48 54 54 50 2f 31 2e 30 0d POST / HTTP/1.0.
0a 48 6f 73 74 3a 20 77 77 77 2e 63 63 68 6c 75 .Host: www.schlu
6e 64 2e 6e 65 74 0d 0a 43 6f 6e 74 05 6e 74 0d .Content-Len: 204800...
4c 65 6e 67 74 68 3a 20 32 30 34 38 30 30 0d 0a .Length: 204800...
0d 0a 38 38 38 38 38 38 38 38 38 38 38 38 38 38 .....8888888888888888
38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 .....8888888888888888
38 38 38 38 38 38 38 38 38 38 38 38 38 38 38 .....8888888888888888
[duplicate lines deleted]

2004/03/24 10:52:40.010703 192.168.10.5:1031 -> 38.9.51.9:80 [MP]
50 4f 63 54 30 2f 20 48 54 54 50 2f 31 2e 30 0d POST / HTTP/1.0.
0a 48 6f 73 74 3a 20 77 77 77 2e 63 6f 67 65 6e .Host: www.copen
74 63 6f 2e 63 6f 6a 0d 0a 43 6f 6e 74 05 6e 74 .Content-Length: 204800...
0d 0a 00 00 33 33 33 33 33 33 33 33 33 33 33 33 .....3333333333333333
33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 .....3333333333333333
33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 .....3333333333333333
[duplicate lines deleted]

```

INFORMATION SECURITY DECISIONS

Analysis of speed test

```

DumpFile: phatbot-test.dump
FileSize: 0.23MB
Id: 200403230525
StartTime: Tue Mar 23 05:25:13 2004
EndTime: Tue Mar 23 05:25:19 2004
TotalTime: 6.18 seconds
TotalCapSize: 0.22MB CapLen: 1514 bytes
# of packets: 321 (226.36KB)
AvgRate: 279.76Kbps stddev:159.76K PeakRate: 435.06Kbps

### IP flow (unique src/dst pair) Information ###
# of flows: 2 (avg, 160.50 pkts/flow)
Top 10 big flow size (bytes/total in %):
91.8% 8.2%

### IP address Information ###
# of IPv4 addresses: 2
Top 10 bandwidth usage (bytes/total in %):
100.0% 100.0%

### Packet Size Distribution (including MAC headers) ###
<<<<
[ 32- 63]: 122
[ 64- 127]: 4
[ 128- 255]: 1
[ 512- 1023]: 68
[ 1024- 2047]: 129
>>>>

```

INFORMATION SECURITY DECISIONS

Scanning with Phatbot

Hosted by SECURITY SearchSecurity.com

```

[scan_addnetrange] Adds a CIDR block to the bot net work scanning
list. (It is not clear if this is acted on by
all bots, or just specific individual bots.)

#####
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.login
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.scan_addnetrange 165 .0/0/16 10000
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.scan_addnetrange 139 .0/0/16 10000
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.scan_addnetrange 143 .0/0/16 10000
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.scan_addnetrange 139 .0/0/16 10000
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.scan_addnetrange 128 .0/0/16 10000
#Planet-3812AD55.dip.t-dialin.net NICK :
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.scan_addnetrange 128 .0/0/16 10000
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.scan_addnetrange 128 .0/0/16 10000
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.scan_addnetrange 137 .0/0/16 10000
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.scan_addnetrange 138 .0/0/16 10000
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.scan_addnetrange 139 .0/0/16 10000
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.scan_addnetrange 213 .0/0/16 10000
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.scan_addnetrange 145 .0/0/16 10000
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.scan_addnetrange 145 .0/0/16 10000
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.scan_addnetrange 145 .0/0/16 10000
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.scan_starttail
#Planet-3812AD55.dip.t-dialin.net QUIT :Connection reset by peer
#Planet-3812AD55.dip.t-dialin.net MODE #test2 +o
#Planet-3812AD55.dip.t-dialin.net QUIT :Max SendP exceeded
#Planet-3812AD55.dip.t-dialin.net MODE #test2 +o
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.login
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.scan_clearnetranges
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.scan_reset_netranges
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.scan_starttail
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.login
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.scan_addnetrange 144 .0/0/16 10000
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.scan_addnetrange 143 .0/0/16 10000
#Planet-3812AD55.dip.t-dialin.net PRIVMSG #test2 :.scan_addnetrange 143 .0/0/16 10000

```

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

The victims...

- "Politehnica" University of Bucharest, Hungary
- Aachen University of Technology, Aachen, Germany
- Academic Medical Centre, Amsterdam, The Netherlands
- Albert-Ludwigs-Universität Freiburg, Germany
- Czech Technical University, Prague
- Fachhochschule Albstadt-Sigmaringen, Germany
- Fachhochschule Augsburg, Germany
- Fachhochschule Easingen, Germany
- Fachhochschule Konstanz, Germany
- Fachhochschule Worms, Germany
- Hochschule fuer Technik, Ulm, Germany
- Hogeschool Brabant, The Netherlands
- Hogeschool Rotterdam & Omstreken, The Netherlands
- Hogeschool van Amsterdam, The Netherlands
- Hogeschool van Utrecht, The Netherlands
- Humboldt-Universität zu Berlin, Germany
- Johann Wolfgang Goethe-Universität Frankfurt, Germany
- Philipps-Universität Marburg, Germany
- Physikalisches Technische Bundesanstalt, Germany
- Rechenzentrum der Universität Jena, Germany
- Technische Universität Berlin, Germany
- Technische Universität Dresden, Germany
- Universität Augsburg, Germany
- Universität Bamberg, Germany
- Universität Bremen, Germany
- Universität Duisburg-Essen, Germany
- Universität Karlsruhe, Germany
- Universität Konstanz, Germany
- Universität Münster, Germany
- Universität Oldenburg, Germany
- Universität Stuttgart, Germany
- Universität Würzburg, Germany
- Université de Fribourg, Switzerland
- Université de Liège, Belgium
- Université de Valenciennes, France
- Universiteit van Amsterdam, The Netherlands
- University College London, UK
- University of Applied Sciences, Weingarten, Germany
- University of Cooperative Education, Mannheim, Germany
- University of Cooperative Education, Ravensburg, Germany
- University of Cooperative Education, Stuttgart, Germany
- University of Hamburg, Germany
- University of Innsbruck, Austria
- University of Liverpool, UK
- University of London, UK
- Westsächsische Hochschule, Zwickau, Germany

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Collateral damage...

- Amsterdam Airport Schiphol, The Netherlands
- DESY Zeuthen, Germany
- DeTeLine GmbH, Berlin, Germany
- Dr. Ing. h.c. F. Porsche AG, Germany
- Dutch Railways Network, Utrecht, The Netherlands
- EDS International B.V., The Netherlands
- Materna GmbH, Dortmund, Germany
- Ministerie van Binnenlandse Zaken, The Hague
- Ministerie van Sociale Zaken en Werkgelegenheid, The Hague
- Saudi Online Network, Riyadh, Saudi Arabia
- Shell Information Technology International, SA Telecom
- Siemens AG, World Headquarter, Munich, Germany
- Swisscom Fixnet, Berne, Switzerland
- Swisscom IP-Plus, Berne, Switzerland
- Unilever Research Laboratorium, The Netherlands
- Unilever Research Vlaardingen, The Netherlands

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Proxying IRC traffic

```
The bot on 192.168.11.2 appears to be using a wildly different port for its IRC command and control, and a different IRC server and channel that the bots described earlier:

-----
T 2004/03/25 11:33:08.398815 192.168.3.50:54481 -> 192.168.11.2:1053 [AP]
:[ASS]lbtb!A5Sjbtb@147.26.169.*** QUIT :Connection reset by peer..:[ASS]bcv
zy!A5Sbcvz@147.26.235.*** QUIT :Connection reset by peer..
-----
T 2004/03/25 11:33:08.566118 192.168.3.50:54481 -> 192.168.11.2:1516 [AP]
:[ASS]jlliof!A5Sjlliof@147.26.220.*** QUIT :Connection reset by peer..:[ASS]o
tmf!A5Sotef@147.26.169.*** QUIT :Connection reset by peer..:[ASS]uvxb!A5Suv
xb@147.26.169.*** QUIT :Connection reset by peer..:[ASS]jnymx!A5Sjnymx@147.
26.169.*** QUIT :Connection reset by peer..:[ASS]ehnh!A5Sehnh@147.26.199
.*** QUIT :Connection reset by peer..:[ASS]vdfc!A5Svdfc@147.26.235.*** QUIT
:Connection reset by peer..:[ASS]gab!A5Sgab@147.26.169.*** QUIT :Connect
ion reset by peer..
-----
T 2004/03/25 11:33:08.566361 192.168.3.50:54481 -> 192.168.11.2:1053 [AP]
:[ASS]lbtb!A5Sjbtb@147.26.220.*** QUIT :Connection reset by peer..:[ASS]o
tmf!A5Sotef@147.26.169.*** QUIT :Connection reset by peer..:[ASS]uvxb!A5Suv
xb@147.26.169.*** QUIT :Connection reset by peer..:[ASS]jnymx!A5Sjnymx@147.
26.169.*** QUIT :Connection reset by peer..:[ASS]ehnh!A5Sehnh@147.26.199
.*** QUIT :Connection reset by peer..:[ASS]vdfc!A5Svdfc@147.26.235.*** QUIT
:Connection reset by peer..:[ASS]gab!A5Sgab@147.26.169.*** QUIT :Connect
ion reset by peer..
-----

```

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Uptime of bots

bot.longuptime Shows uptime of bots in long form.

```

! @Planet-3B12AD55.dip.t-dialin.net PRIVMSG #test2 :.bot.longuptime
-qtJung1! -qtJung2AD5Df42.4A4A88925.67E83863.IP PRIVMSG #test2 :uptime: 7d 12h 53m
-mjctxyl! -mjctxyl@Planet-11D13A85.u.usf.edu PRIVMSG #test2 :uptime: 6d 12h 35m
-nauvyp1! -nauvyp1@Planet-2FE0C63A.physics.utoledo.edu PRIVMSG #test2 :uptime: 40d 11h 12m
-rnhcjpup! -rnhcjpup@Planet-342A65D7.u.usf.edu PRIVMSG #test2 :uptime: 16d 9h 56m
-lijemaul! -lijemaul@Planet-056467f.physics.utoledo.edu PRIVMSG #test2 :uptime: 20d 9h 36m
-rbkzjztd! -rbkzjztd@Planet-295C68E.utoledo.edu PRIVMSG #test2 :uptime: 35d 0h 30m
-gkhrnu! -gkhrnu@Planet-27BE6697.resnet.ua.edu PRIVMSG #test2 :uptime: 36d 8h 58m
-fgntcz! -fgntcz@Planet-ABC4985.kaist.ac.kr PRIVMSG #test2 :uptime: 26d 13h 34m
-cobprbrv! -cobprbrv@Planet-2FC6A514.usf.edu PRIVMSG #test2 :uptime: 6d 10h 6h
-cocbea! -cocbea@2F082997.9320C6D7.16D9D19D.IP PRIVMSG #test2 :uptime: 7d 6h 49m
-zckybjb! -zckybjb@Planet-1091B569.law.lsu.edu PRIVMSG #test2 :uptime: 33d 6h 54m
-nvfkau! -nvfkau@Planet-280B0983.stern.nyu.edu PRIVMSG #test2 :uptime: 27d 8h 10m
-pdzurhkl! -pdzurhkl@Planet-1B4E83D9.ew.utoledo.edu PRIVMSG #test2 :uptime: 21d 24h 18m
-cuphka! -cuphka@Planet-F2C1955.memphis.edu PRIVMSG #test2 :uptime: 47d 6h 24m
-ernuth! -ernuth@Planet-194BD172.bio.nau.edu PRIVMSG #test2 :uptime: 32d 7h 11m
-lymqbae! -lymqbae@Planet-2C425D41.ucr.edu PRIVMSG #test2 :uptime: 21d 11h 31m
-ekyjcdal! -ekyjcdal@ky022F022E.262733EF.16D0D19D.IP PRIVMSG #test2 :uptime: 20d 5h 22m
-rxhgkd! -rxhgkd@Planet-26779967.memphis.edu PRIVMSG #test2 :uptime: 7d 8h 38m
-gfzzh! -gfzzh@Planet-1A82C5E4.memphis.edu PRIVMSG #test2 :uptime: 27d 7h 20m
-gaqznr! -gaqznr@Planet-215AE305.neurosurgery.utoledo.edu PRIVMSG #test2 :uptime: 12d 12h 5h
-lijemaul! -lijemaul@Planet-18F590A.ccc.clonisia.edu PRIVMSG #test2 :uptime: 15d 9h 57m
-zmfpcxc! -zmfpcxc@Planet-623D00F.1c.utoledo.edu PRIVMSG #test2 :uptime: 22d 13h 25m

```

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Uptimes

```

$ cat -n | grep -F "#test2 :uptime:" | sort -n
#test2 :uptime: 11d 11h 0m
#test2 :uptime: 11d 14h 2m
#test2 :uptime: 12d 14h 3m
#test2 :uptime: 12d 12h 5m
#test2 :uptime: 13d 12h 4m
#test2 :uptime: 13d 1h 57m
#test2 :uptime: 14d 2h 3m
#test2 :uptime: 14d 3h 16m
#test2 :uptime: 15d 8h 16m
#test2 :uptime: 15d 12h 25m
#test2 :uptime: 20d 5h 22m
#test2 :uptime: 20d 9h 35m
#test2 :uptime: 20d 7h 5m
#test2 :uptime: 21d 11h 31m
#test2 :uptime: 21d 11h 16m
#test2 :uptime: 21d 12h 16m
#test2 :uptime: 21d 13h 54m
#test2 :uptime: 27d 10h 12m
#test2 :uptime: 27d 7h 20m
#test2 :uptime: 27d 8h 10m
#test2 :uptime: 28d 12h 14m
#test2 :uptime: 28d 7h 11m
#test2 :uptime: 28d 9h 39m
#test2 :uptime: 28d 9h 39m
#test2 :uptime: 29d 0h 30m
#test2 :uptime: 29d 0h 30m
#test2 :uptime: 35d 0h 30m
#test2 :uptime: 36d 8h 58m
#test2 :uptime: 40d 11h 12m
#test2 :uptime: 41d 12h 12m
#test2 :uptime: 41d 12h 12m
#test2 :uptime: 47d 6h 24m
#test2 :uptime: 7d 12h 53m
#test2 :uptime: 7d 22h 5m

```

#test2 :uptime: 48d 11h 15m

INFORMATION SECURITY DECISIONS

Hosted by SearchSecurity.com

Thanks and questions

- Contact: **Dave Dittrich**
IA Researcher
The Information School/
Center for Information
Assurance & Cybersecurity

dittrich@u.washington.edu
<http://staff.washington.edu/dittrich/>

