

Today's Modern Network Killing Robot

Viki Navratilova
viki@uchicago.edu
Network Security Officer
The University of Chicago

How to Create a Network Killing Robot

- Slap together different technologies
 - Borrow from the strengths of each
- Make it easy for lots of people to use (AOL effect)
 - Means giving up 'I am an elite hacker' snobbery
- Widely distribute it to non-tech people
- Automate everything
- Distribute as much as you can over the Internet
 - Reduces single point of failure
- Give people the ability to express themselves through the tools

IRC & DOS, two great tastes that taste great together

- IRC (I Repeat Classes)
 - Widely available networked benign application
 - (relatively) effective way to fulfill need to socialize
 - Easy to use application
- DOS (Denial of Service Tools)
 - Effective way to communicate emotions to others
 - Lots of engineering effort goes into DOS tools
 - Always evolving in response to new ways to block them

A Brief History of Denial of Service Attacks

Early DOS attacks

■ ping of death

- Simple network flood
- either single very large ping packet, or a flood of large or small ping packets

■ smurf attack

- Amplified network flood
- widespread pings with faked return address (broadcast address)



■ syn flood

- Overload the machine instead of the network
- Send a bunch of SYN packets to a host on different ports to open a connection, and don't finish opening the connection

Honey! I think
our network is
having another
Smurf attack!



Julie
©2000

Distributed Denial of Service (DDOS) Tools

- trinoo,stacheldracht
 - faked source ip address
 - easy to spot and filter
 - Much more devastating than old DOS tools
 - Harder to track back to the attacker
 - Made famous in the media when cnn.com, yahoo.com, ebay.com DOS'ed for several hours
 - Generally required breaking into each DDOS drone by hand to install the DDOS software

A Brief History of IRC Bots

eggdrop bot - Jeff Fischer, 1993

- download from www.eggheads.org
- usually used to mind irc channels
when their human ops weren't there
- windows port is called windrop
- still widely used today





bnc - the bnc group

- IRC server proxy
- found on a lot of compromised machines in the wild
- hides your IP, so you are protected from DOS attacks and exploits
- you select port, password, max # of users, and hosts.allow for ips
`/server shell.server.com portnumber password`
- good for anonymizing trash talking and IRC-based attacks
- everyone sees the IP address of the BNC server
- if people attack your BNC server
 - slows down your IRC connection and might disconnect you from IRC temporarily
 - your computer is safe

Parallel Evolution of Two Tools

IRC

- irc scripts (aliases for sending files)
- irc bots for file sharing & keeping the channel op'd while you're away
- netsplits would accidentally give people ops
- channel wars break out & netsplits are caused manually to give ops
- irc bots start to keep the channel up during netsplits
 - two bots fight it out, the one on the better server wins
- irc bots themselves start to cause netsplits
- irc bots start to attack (pax0r) individuals (be polite!) (started in mid '90's)
- irc bots used to be mostly unix are now mostly windows
- people write scripts to automatically scan, break in, and install irc bots (eggdrop)

Denial of Service

- Becomes common later than IRC
- starts simply by poorly written software or shell scripts
 - CS students accidentally fork bombing
 - too many wgets taking down a server
- network dos (started in mid '90's – Clinton Conspiracy?)
 - simple network flood - ping of death
 - amplified network flood - smurf attack
 - overloading machine instead of network - syn floods
- distributed dos
 - dos itself becomes scripted & remotely controlled
 - trinoo, stacheldracht make the news
 - setting it up (breaking-in & downloading) is mostly done manually
- IRC & DOS come together when people realize they can use irc to control what were once known as zombie machines

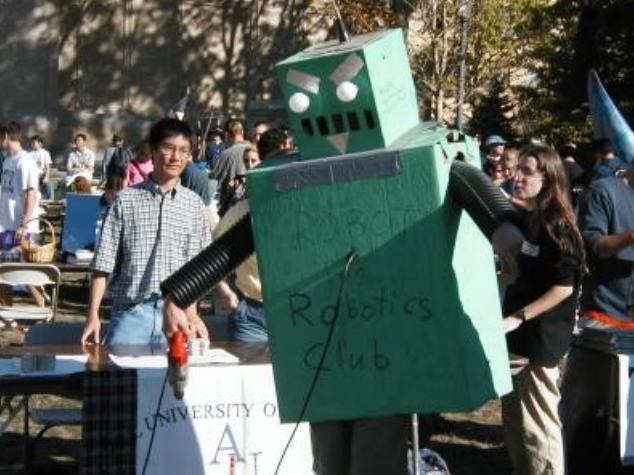
Today's Modern Network Killing Robot

- irc bots control everything in one handy package
 - scan, break in, carry out dos attacks on demand
- having so many machines that DOS on demand makes the dos attacks into ddos attacks
- These networks of DOS'ing machines are called DOSnets

DoSnet tools



- immigrant child labor became expensive, so people started automating DDOS by using robots
- harder to filter because they come from all over
- may or may not use spoofed source addresses, not necessary because individual botnet nodes are cheap to replenish
- little to no media coverage, so users and sysadmins are largely unaware of how widespread they are
- hide in legitimate IRC traffic, no special ports



DoSnet tools

- botnet Masters & bots can hide in channels that most people can't see (hidden channel, appears the channel is empty from outside, special characters in channel name, etc.)
- infection of hosts with botnets is much easier than before, no more need for children in sweatshops to individually compromise each host for a traditional DDOS drone network
- DoSnet botnets are much more flexible than DDOS drones
- Dosnet bots can include various programs so they can run almost anything
 - examples: Ping of death, fragmented IGMP flood, flood irc channels,etc.

DoSnet Methods of Infection



- trojaned file containing a bot sent through e-mail via attachment
- web browser exploits (usually IE) download a small executable invisibly to a desktop, which then downloads a bot and runs it in stealth mode
- blank or weak admin password, password is guessed, script logs on, download and runs bot
- looking for something currently infected with another trojan such as SubSeven

evilbot

- backdoor windows trojan
 - copies itself to the \Windows\System folder
 - adds itself to the registry (who doesn't?)
 sysyemdl %system%\sysedit.exe
 HKEY_LOCAL_MACHINE\Software\
 Microsoft\Windows\CurrentVersion\Run
- backdoor is accessible via IRC
- attacks other computers using IRC

gtbot (global threat bot) - Sony, mSg, & DeadKode, 2009



- renamed mirc client containing various mirc bot scripts
- runs in stealth mode using HideWindow program
- often downloaded by people on irc who are tricked into thinking it's a clean mirc client, or installed on a compromised machine as the payload of the automated compromise
- supports plugins, so adding in programs to do extra stuff (like sending fragmented ICMP packets) is easy

gtbot on irc

- connects to a channel on an IRC network & waits for commands from the bot master
- commands include:

!scan

usage:

!scan <ip.*> <port>

!scan 1.1.1.* 31337

example : **!scan 128.135.75.103 31337**

!fileserver.access

no usage, if the address of the user = %master, then they can spawn an fserve from the root of C:\.

!up

attempts to op the \$nick in the current channel.

- **!info**
- no usage, gives information about the client such as:
- date, time, os (which type of windows), uptime, number of .mp3s, number of .exe's, number of .mpg's, number of .asf's
- and which url the client it currently viewing.

!clone.c.flood
constant flood, sets a timer to continually flood a channel or nick.

!flood.stop
stops the above flood.

!super.flood
another flood type.

!super.flood.stop!
stops the above flood.



!portscan
usage:
!portscan <ipaddress> <startport> <endport>

!update
attempts to get an update from a webpage, if your address
matchs %master.
usage:
!update <url>

gtbot registry key settings

- - adds registry key to make sure it starts at boot, such as:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "WHVLXD"
■ Type: REG_SZ
■ Data: C:\<folder gtbot is in>\WHVLXD.exe
- - modifies mirc registry key values:
HKEY_CLASSES_ROOT\ChatFile\DefaultIcon "(Default)"
■ Old data: "C:\MIRC\MIRC.EXE"
■ New data: "C:\<folder gtbot is in>\TEMP.EXE"
- HKEY_CLASSES_ROOT\ChatFile\Shell\open\command "(Default)"
■ Old data: "C:\MIRC\MIRC.EXE" -noconnect
■ New data: "C:\<folder gtbot is in>\TEMP.EXE" -noconnect
- HKEY_CLASSES_ROOT\irc\DefaultIcon "(Default)"
■ Old data: "C:\MIRC\MIRC.EXE"
■ New data: "C:\<folder gtbot is in>\TEMP.EXE"
- HKEY_CLASSES_ROOT\irc\Shell\open\command "(Default)"
■ Old data: "C:\MIRC\MIRC.EXE" -noconnect
■ New data: "C:\<folder gtbot is in>\TEMP.EXE" -noconnect
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\mIRC
"UninstallString"
■ Old data: "C:\MIRC\MIRC.EXE" -uninstall
■ New data: "C:\<folder gtbot is in>\TEMP.EXE" -uninstall



How to remove gtbot

- if you have this on machine, odds are good that you have other problems & other backdoors installed
- download a tool such as Lockdown Corp's LockDown 2000 or their free scanning tool SwatIt!
- delete the registry key it created to make it start up after every boot
 - make a backup of your registry first
 - mirc registry keys shouldn't affect system operation, so they don't have to deleted



How to remove gtbot (cont.)

- can either reboot and kill the bot files
- look for a mirc.ini file in a place where it shouldn't be, and probably delete the entire folder that contains the mirc.ini file if it looks like it's been created by the bot
- doing a search for all the mirc.ini files on your system should reveal all the bots on your machine (sometimes hidden in windows font directory)
- should only have one mirc.ini file for each legitimately installed version of mirc

How to remove gtbot (cont.)

- possible to hexedit the bot so it starts up off another file name other than mirc.ini, so looking for mirc.ini may not always work
- or can kill the process and delete the files
- be sure the process has stopped running before you delete anything
- if one opens on your desktop, close it using the X at the top of the window
- some bots signal destructive routines if someone types something into them
- don't use a bot for chat

sdbot

- copies itself somewhere to the Windows System directory or a subdirectory
- connects to IRC servers & joins pre-selected IRC channel (hardcoded)
- receives control commands from its master such as:
 - download files
 - execute remote files
 - act as IRC proxy server
 - join IRC channels
 - send /msgs on IRC
 - sending UDP & ICMP packets to remote machines
- can remove by using something like McAfee or F-Secure Anti-Virus
 - can also try deleting individual files, but that might trigger all sorts of destructive triggers like deleting c:\ or the windows\system\ folder, etc.



Demonstration



Ways to Detect a Botnet on Your Network



- subscribe to a mailing list like FIRST,
 - require membership
 - members regularly watch internet-wide trends in bot activity and notify members
- look for flows to port 6667
 - look for timing
 - incoming microsoft-ds (445) to machine A, soon afterwards machine A starts outgoing irc (6667) traffic
- Use an IDS like Snort
 - generally unencrypted traffic, so easy to spot if you know what strings to look for
 - because of bot variations, bots can get around this
 - some bot variations encrypt their traffic



use packeteer

- look for top dcc talkers
- high traffic indicates an irc bot, may or may not be a DDOS botnet bot

look for machines with irc traffic and lots of udp or icmp traffic

- really noticeable only when the botnet is attacking

see people joining irc channels with formulaic nicknames

- they get kicked and re-join later with similar nickname and same IP address as before
- may or may not be a DDOS botnet bot



Angie Mason 2009

URLs for further reading

- bot scanners, bot information, interviews with IRC ops and backdoor authors
<http://bots.lockdowncorp.com/>
- gtbot information
 - including lots of documentation on variants
 - lists of files each variant installs & file sizes & registry key mods to help you find them on your machine<http://golcor.tripod.com/gtbot.htm>
- download sdbot
<http://wintermarket.org:81/~sd/sdbot/news.shtml>
- download gtbot & a bunch of others and their variants
<http://www.weblinxorz.com/bots/bots.html>

More urls...

- download eggdrop
<http://www.eggheads.org>
- download BNC
<http://www.gotbnc.com/>
<http://bnc ircadmin.net/>

I for one, welcome our new robot masters.
Questions?

