Botnets

Secret Puppetry With Computers

Balaji Prasad T.K (bpt@email.arizona.edu)
Nupur Maheshwari (nupurm@email.arizona.edu)
Department of Computer Science
University of Arizona

April 22, 2012

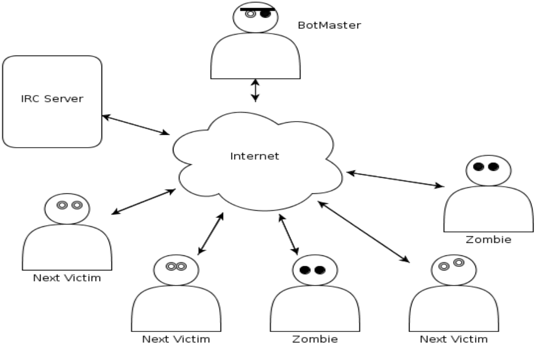
1. What are Botnets?
2. Technical Overview
3. Compare and Contrast
4. Detection and Prevention
5. Evolution and Conclusion

Introduction

A botnet is a network of *zombie* computers which are remotely controlled by a *botmaster*. Components:

- Botmaster
- Zombies
- Communication Channel
- Servers

Botnet Overview



Facts and Stats

- 83% of global spam
- 3 million botnets, 100 spams per minute
- Only 3 survived from 2010
- Why no Linux Botnets?

Bot Stories

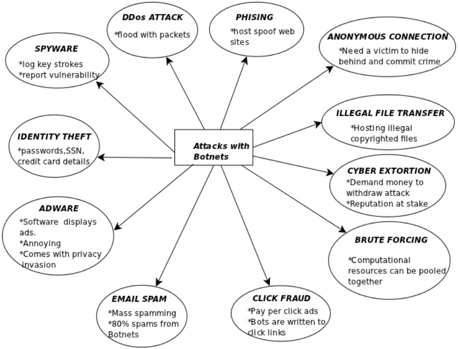
- Wiki Leaks -Used Botnet for campaign

  http://news.techworld.com/security/3252663/anonymous-uses-30000-pc-strong-botnet-in-wikileaks-campaign/

- App Stores - Marketing

Botnets Threat Landscape

- Have managed to bring down websites of biggies like cia.gov(US cental investigation agency), SOCA.gov (British serious organised crime agency)) etc
- Here is a list of what you can do:



Attacks with Botnets

DDos ATTACK
*flood with packets

PHISING
*host spoof web sites

ANONYMOUS CONNECTION
*Need a victim to hide behind and commit crime

SPYWARE
*log key strokes
*report vulnerability

ILLEGAL FILE TRANSFER
*Hosting illegal copyrighted files

IDENTITY THEFT
*passwords,SSN, credit card details

CYBER EXTORTION
*Demand money to withdraw attack
*Reputation at stake

ADWARE
*Software displays ads.
*Annoying
*Comes with privacy invasion

BRUTE FORCING
*Computational resources can be pooled together

EMAIL SPAM
*Mass spamming
*80% spams from Botnets

CLICK FRAUD
*Pay per click ads
*Bots are written to click links

Historically (in)Famous

StormBot:

- Jan 2007
- fighting-back capabilities
- Spam with Subject - 230 dead as storm batters Europe
- Affected: private computers in Europe and US

Conflicker:

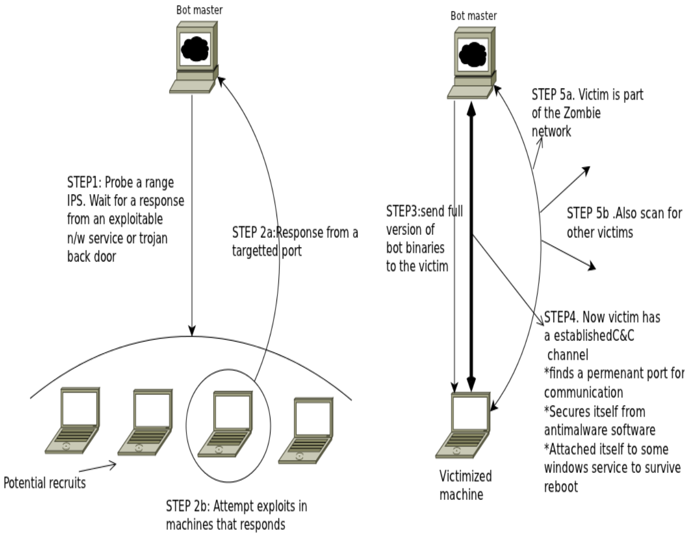
- Nov 2009
- RPC Request
- Buffer overflow
- Affected: French Navy, United Kingdom Ministry of Defence, Manchester City council's system and police network, German army systems

ZeusBot:

- July 2007
- drive-by-downloads and Phising scams
- Affected: Bank of America, NASA, Monster.com, ABC Oracle, Play.com, Cisco, Amazon, an BusinessWeek

1. What are Botnets?
2. Technical Overview
3. Compare and Contrast
4. Detection and Prevention
5. Evolution and Conclusion

How They Recruit



STEP1: Probe a range IPS. Wait for a response from an exploitable n/w service or trojan back door

STEP 2a:Response from a targetted port

STEP 2b: Attempt exploits in machines that responds

STEP3:send full version of bot binaries to the victim

STEP4. Now victim has a establishedC&C channel
*finds a permenant port for communication
*Secures itself from antimalware software
*Attached itself to some windows service to survive reboot

STEP 5a. Victim is part of the Zombie network

STEP 5b .Also scan for other victims

How They Differ

Virus Vs. Worm Vs. Botnet

http://www.youtube.com/watch?v=XlSc8W5VaR8

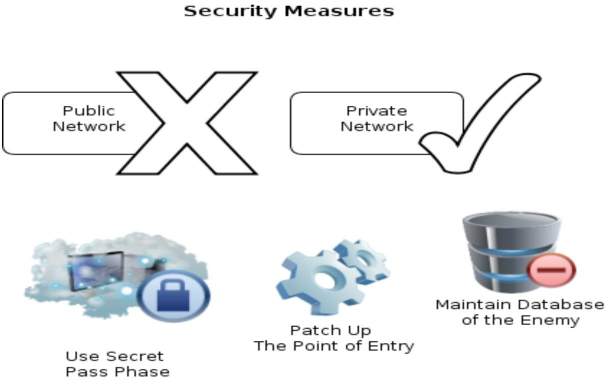
How They Propogate

- Scan the network
- Send spam mails
- Drive-by download
- Install malware

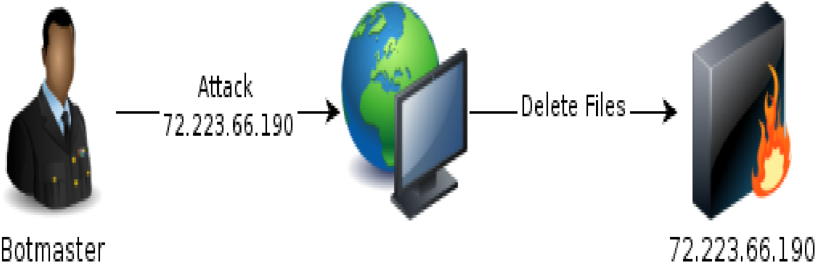
How They Obfuscate

- Encryptation
- Mutation
- Encoded Peer List

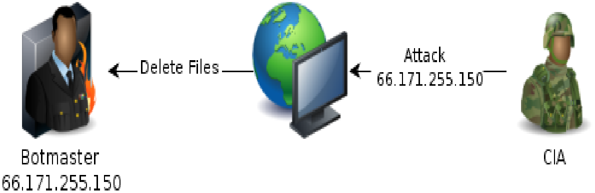
Botnet obfuscation mechanisms



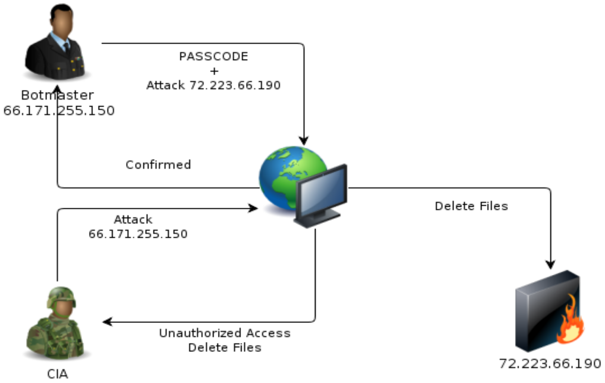
Use a Passcode



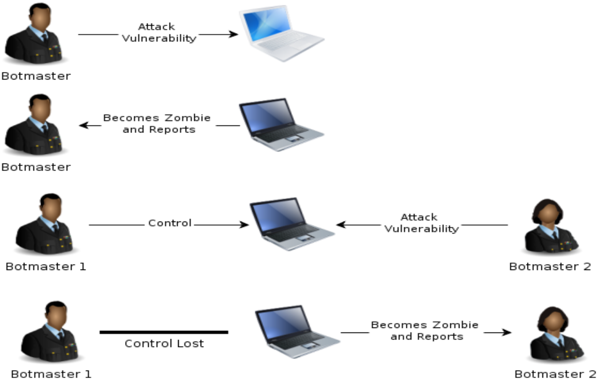
Use a Passcode



Use a Passcode



Patch Up

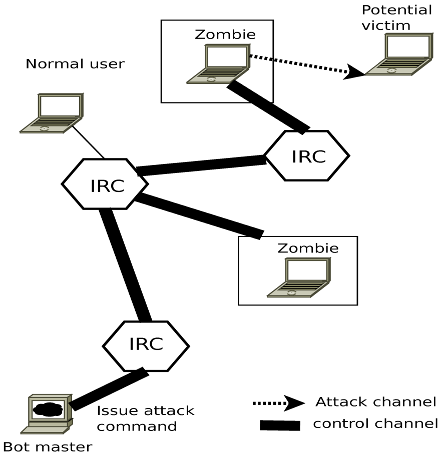


Attack Vulnerability
Botmaster
Becomes Zombie and Reports
Botmaster
Control
Attack Vulnerability
Botmaster 1
Botmaster 2
Control Lost
Becomes Zombie and Reports
Botmaster 1
Botmaster 2

Command and Control

- IRC - Internet Relay Chat
- P2P - Peer-to-Peer
- Web Based

Command and Control - IRC



IRC C&C

Command and Control - P2P

P2P -based:

- IRC-based botnets have centralized master which is single point of failure
- In P2P based C&C Botmaster can use any of the nodes to pass commands or collect information from other nodes in the Botnet

Web-based:

- Botnets evolved to use HTTP and HTTPS protocols for C&C - The bots talk to a web server acting as their master
- Distinct advantage to the adversary as HTTP ports are always enabled
- This C&C merges well with the normal traffic to provide obscurity

1. What are Botnets?
2. Technical Overview
3. **Compare and Contrast**
4. Detection and Prevention
5. Evolution and Conclusion

Anatomy of 2 High Profile Bots

AgoBot

- Also known as Phatbot - oldest known bots
- IRC based bot with a huge arsenal of exploits
- Ability to launch DDoS attacks and harvest passwords through key logging and traffic sniffing

SDBot

- Known since 2002-Hundreds of variants providing a wide range of capabilities
- Core code is very compact when compared to AgoBot with just 2000 lines of C code
- Extension of code to add a newer capability is very straightforward - also diffuses accountability of the creator.

Botnet Control Mechanism

AgoBot

bot.execute & Makes the bot execute a specific .exe
bot.sysinfo & Echo the bots system information
bot.status Echo bot status information
bot.nick & Changes the nickname of the bot
bot.open & Opens a specified file
bot.remove & Removes the bot from the host

SDBot uses commands like

- Ping & Pong
- Join request to establish IRC connection
- Commands sent by the master include:KICK, NICK, PART.
- All other commands will be sent as part of the PRIVMSG,NOTICE or TOPIC IRC messages

Host Control Mechanism

AgoBot

- Secure the system
- Harvest commands
- Pctrl commands
- Inst commands

SDBot

- Download
- Kill thread
- Sysinfo
- Execute
- Update

Attack Mechanism

AgoBot

- Scans for backdoors left by *other* worms
- Exploits RPC Buffer Overflow in windows
- Brute force SQL servers
- DDos

SDBot

- Capabilities are relatively benign
- Creator can disown
- Extends to UDP and ICMP
- udp/ping <host to attack>
  $< portno.ofpackets >< packetsize >$

Obfuscation and deception mechanism

AgoBot

- Swapping consecutive bytes
- Rotate left / Rotate right
- Polymorphic encoding
- Looked for debuggers
- Installed virtual machines
- Kills antivirus processes
- Alters DNS servers of the AV/SW companies

SDBot did not have any such capabilities.

1. What are Botnets?

2. Technical Overview

3. Compare and Contrast

4. Detection and Prevention

5. Evolution and Conclusion

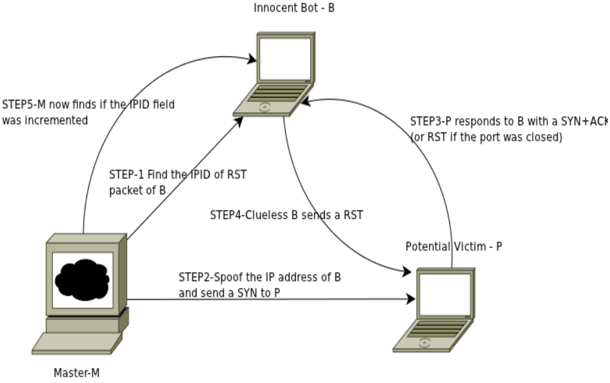
Anomaly based detection

- Scanning involves sending TCP SYN and other control packets to find open ports
- Calculate TCP work weight - fraction of TCP packets that were control packets

$$w = (\mathrm{SYN_n} + \mathrm{ACK_n} + \mathrm{FIN_n})/\mathrm{TCP_n}$$

- Anomalous values caught. Won't work with **"Idle scanning"**

What is Idle scanning?

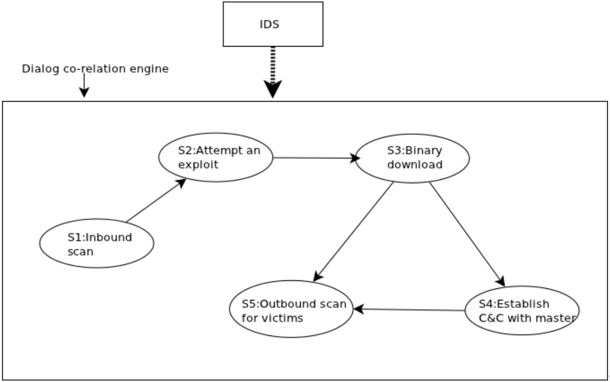

Innocent Bot - B
STEP5-M now finds if the IPID field was incremented
STEP3-P responds to B with a SYN+ACK (or RST if the port was closed)
STEP-1 Find the IPID of RST packet of B
STEP4-Clueless B sends a RST
Potential Victim - P
STEP2-Spoof the IP address of B and send a SYN to P
Master-M

Idle scanning Detection

- we can form a *Host Exposure Map* which captures the host-port combinations of the connections in which the host generally involves.
- Data should be obtained by initially training the system and capturing the pattern.
- Any activity on the host which doesn't fall in the Exposure Map can be reported.

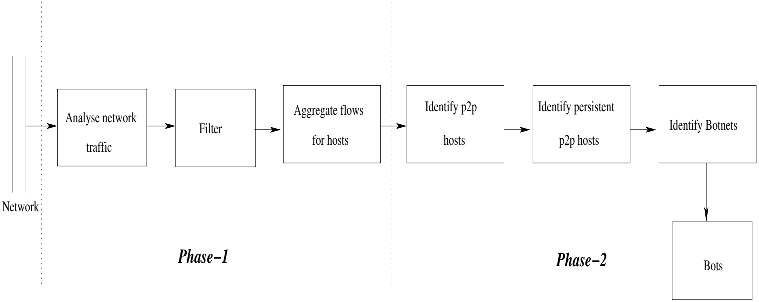
Detection by dialog co-realation

- The victimized host goes into specific states during interaction with master
- The dialog co-relation engine sits at the perimeter of the network and make use of the services of *Intrusion Detection Systems(IDS)*


IDS
Dialog co-relation engine
S2:Attempt an exploit
S3:Binary download
S1:Inbound scan
S5:Outbound scan for victims
S4:Establish C&C with master

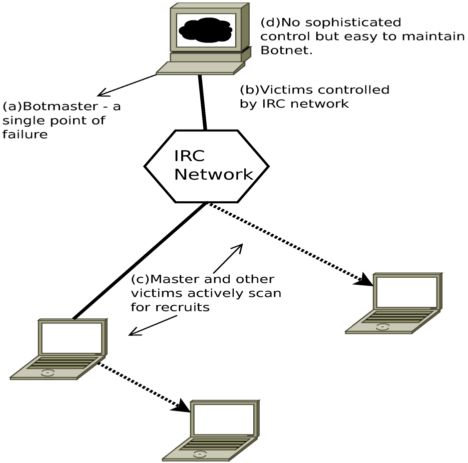
p2p Botnet Detection

- First process involves detection of hosts in the network that involve in p2p communication - Statistical Finger printing
- Separation of legitimate p2p hosts from the malicious ones - persistence pattern and interaction pattern



1. What are Botnets?
2. Technical Overview
3. Compare and Contrast
4. Detection and Prevention
5. Evolution and Conclusion

Evolution of botnets



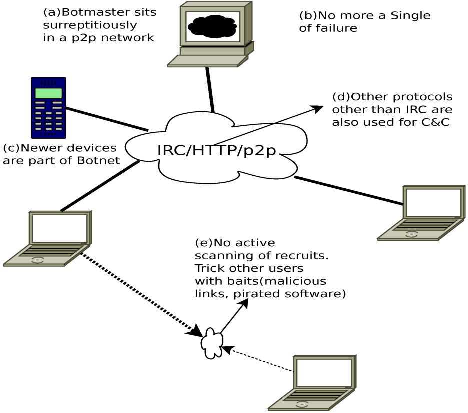
(d)No sophisticated control but easy to maintain Botnet.

(a)Botmaster - a single point of failure

(b)Victims controlled by IRC network

(c)Master and other victims actively scan for recruits

Evolution of Botnets


(a)Botmaster sits surreptitiously in a p2p network
(b)No more a Single of failure
(c)Newer devices are part of Botnet
(d)Other protocols other than IRC are also used for C&C
IRC/HTTP/p2p
(e)No active scanning of recruits. Trick other users with baits(malicious links, pirated software)

Conclusion

- Security begins from personal responsibility.
- Install *security updates* for OS, browser etc promptly
- Don't visit untrusted links
- Avoid using peer-to-peer software
- *Block JavaScript*
- *Watch your ports* for unexpected inbound and outbound traffic.

http://www.youtube.com/watch?v=SubxMZxhiKo