# BOTNETS

## Information Security in Systems & Networks
## Public Development Program

### Sanjay Goel
### University at Albany, SUNY
### Fall 2006

12/4/2006
Sanjay Goel, School of Business and New York State Center for
Information Forensics and Assurance, University at Albany
1

# Botnets

## Agenda

- What are botnets?

- How are they constructed?

- Who is responsible for botnets?

- How can botnets be detected?

# Botnets

## What are bots?

- Bots are automated scripts that are designed to perform specific operations

- Good bots are used for housekeeping functions in networks such as robotic helpers in instant-messaging systems.

- Malicious bots, however, open up a victim's machine to remote access.

    - A majority of bots use IRC networks and network shares to propagate and communicate with the controller through and IRC channel.
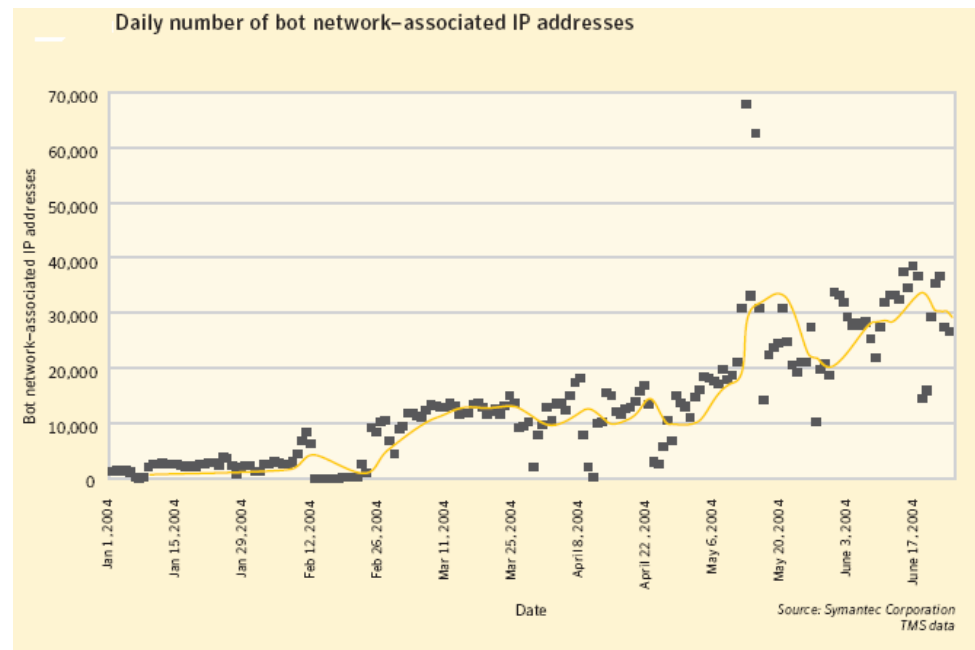
# Botnets

## Description

- Zombies or botnets are computers that have been compromised by attackers, generally through the use of Trojans, allowing these compromised systems to be remotely controlled.
- Collectively, these systems are manipulated to create the high traffic flow necessary to create a DDoS attack.

**Richard Clark (Former security advisor to the White House)**

*"The number of botnets has gone in the last year from 2,000 to about 30,000," said Clarke, now chairman of Good Harbor Consulting. "I don't know what the average number of machines is per botnet, but you can bet it's in the thousands. The only thing I know they are good for is denial-of-service attacks. Even if people aren't reporting it, you know they are having it."*



Daily number of bot network–associated IP addresses

Source: Symantec Corporation TMS data

# Botnets

## Rise of the Botnets

*September 20, 2004, The Register*

**Rise of the Botnets:** The first half of 2004 saw a huge increase in zombie PCs. Also called bots, their average numbers monitored by security firm Symantec rose between January and June from under 2,000 to more than 30,000 per day - peaking at 75,000 on one day.

Richard Archdeacon, Symantec's director of technical services, said: "Bot networks create unique problems for organizations and individual PC users as systems can be automatically upgraded with new exploits very quickly, allowing attackers to outpace efforts to patch or download security updates. We saw a steady increase in the number of bots during the reporting period. Variants of the 'Gaobot' family alone accounted for 67,000 submissions."

**Source:** http://www.theregister.co.uk/2004/09/20/rise_of_the_botnets/

# Botnets
## Problem

- Research estimates millions of computers currently compromised and participating in botnets

  - How do we defend against botnets?

  - How do botnets function?

  - How do we track the owner of the botnet?

  - How can we take control of the botnet so the owner can no longer perform command and control functions?

  - How do we identify and reclaim all the compromised hosts that participate as a drone?

# Botnets

## Why is Managing Bot Attacks Difficult?

- Botnet software can be easily upgraded to include new exploits targeting new vulnerabilities.
- Bot networks are often better able to exploit new vulnerabilities than worms, as propagation code is not needed to use the exploits in a bot network.
- This simplifies the incorporation into the bot network of exploits written by third parties.
- Any number of exploits can be included, making differentiation of bot network attacks from targeted attacks by a single attacker difficult.
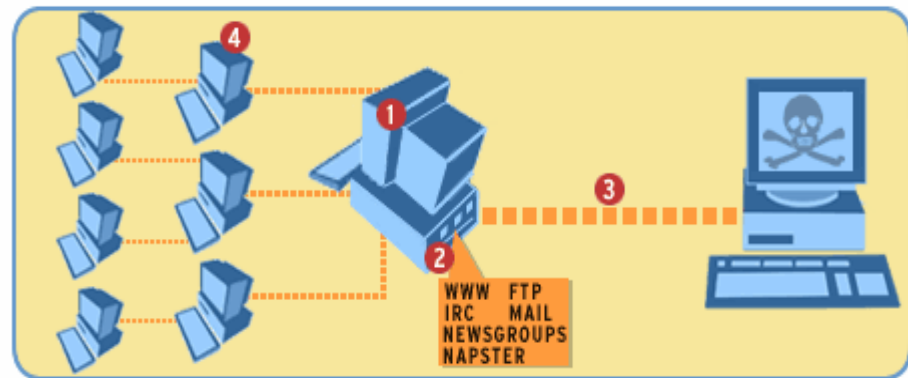
# Botnets
## Attacks

- Distributed Denial-of-service Attacks

- Spamming

- Sniffing Traffic

- Keylogging

- Installing Advertisement Add-ons

- Google Adsense Abuse

- Spreading New Malware

- Attacking IRC Chat Networks

- Manipulating Online Polls/games

- Mass Identity Theft

# Botnets

## DDoS

- At its most basic level, a Distributed Denial of Service (DDoS) attack overwhelms the target system with data, such that the response from the target system is either slowed or stopped altogether.
  - In order to create the necessary amount of traffic, a network of zombie or bot computers is most often used.

- Common techniques to facilitate a Distributed Denial of Service attack are:
  - HTTP GET requests
  - SYN Floods.
  - UDP Fragment Attacks
  - ICMP Floods
  - Ping of Death.

# Botnets
## DDoS, cont'd.

- GET attack works by repeatedly sending a request for a specific page to the target server
- Example: MyDoom worm DDoS attack on SCO.com
  - An machine infected with MyDoom sent multiple (64) http requests every second to the SCO.com server
  - Thousands of machines were infected with MyDoom
  - All these machines acting in conjunction saturated the capacity of the SCO.com server, knocking it offline for several days.

# Botnets
## Incident (Commercial DDoS Attack)

### *United States v. Jay R. Echouafni et al. (Operation Cyberslam)*

***Summary***: On August 25, 2004, a federal grand jury in the Central District of California indicted Jay R. Echouafni, Chief Executive Officer of Orbit Communication Corporation in Massachusetts, and five other individuals on multiple charges of conspiracy and causing damage to protected computers, after Echouafni and a business partner allegedly hired computer hackers to launch relentless distributed denial of service ("DDOS") attacks against Orbit Communication's online competitors.

**The massive computer networks used to launch the DDOS attacks were allegedly created through the use of computer worms that proliferated throughout the Internet and compromised thousands of vulnerable computers.** The infected computers, known as "zombies," were then allegedly used by the co-conspirators to attack the victim computer systems by flooding the systems with massive amounts of data. Echouafni, a U.S. citizen of Moroccan origin, fled from the United States and is the target of an international manhunt led by the FBI. Operation Cyberslam was investigated by the FBI and United States Secret Service with the assistance of the London Metropolitan Police Service and the FBI Legal Attache in the United Kingdom.                     **Source:** http://www.usdoj.gov/criminal/fraud/websnare.pdf

# Botnets
## Socks Proxy

- Bots may also be able to open a SOCKS v4/v5 proxy (a generic proxy protocol for TCP/IP) based networking applications on a compromised machine.
    - When an application client needs to connect to an application server, the client connects to a SOCKS proxy server.
    - The proxy server connects to the application server on behalf of the client, and relays data between the client and the application server.
    - For the application server, the proxy server is the client
- After enabling the SOCKS proxy, the machine can be used for network tasks such as email.
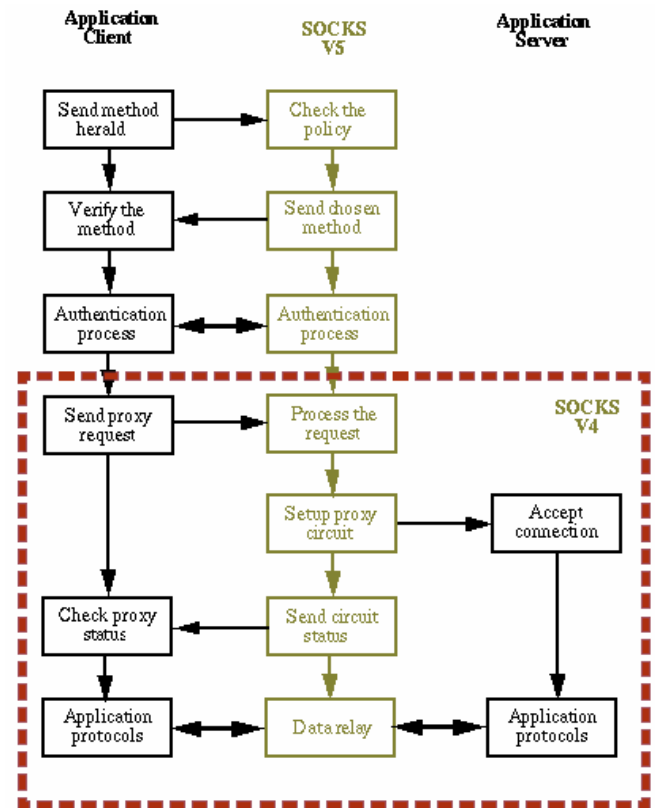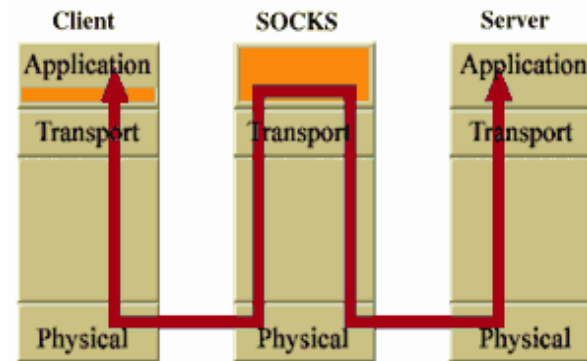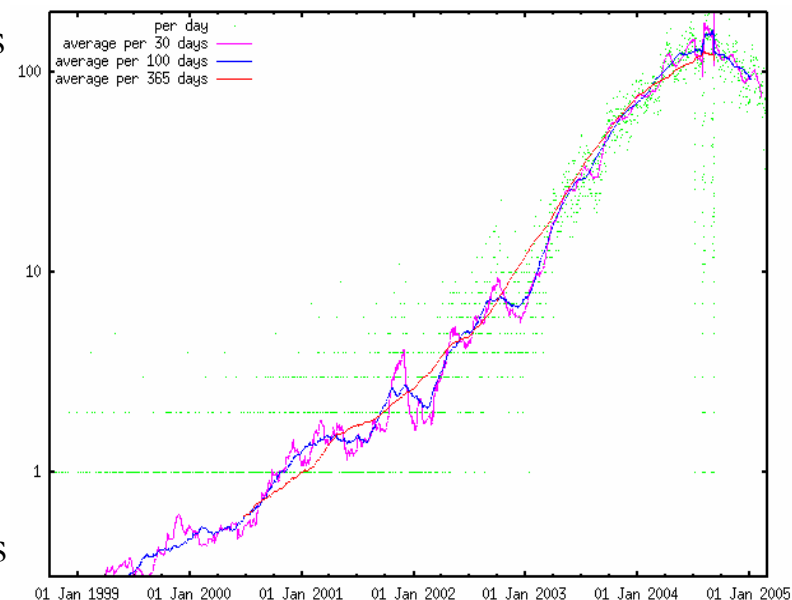
# Botnets
## SPAM

- The word SPAM means "Unsolicited Bulk Email".
  - Unsolicited means that the Recipient has not granted verifiable permission for the message to be sent.
  - Bulk means that the message is sent as part of a larger collection of messages, all having substantively identical content.

  **Source:** http://www.spamhaus.org/news.lasso?article=9

- 90% of all email traffic in the World is SPAM

- The amount of SPAM is growing exponentially with time

- Spurt in the SPAM in the 2000's can be attributed to the rise of the botnets

- Reduction of SPAM recently is attributed to filtering

- Virus writers sell botnets to spammers for $0.10/compromised PC



**Source:** http://wwwhome.cs.utwente.nl/~ptdeboer/misc/SPAM.html

# Botnets
## Phishing

- The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

- The e-mail directs the user to visit a website where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.
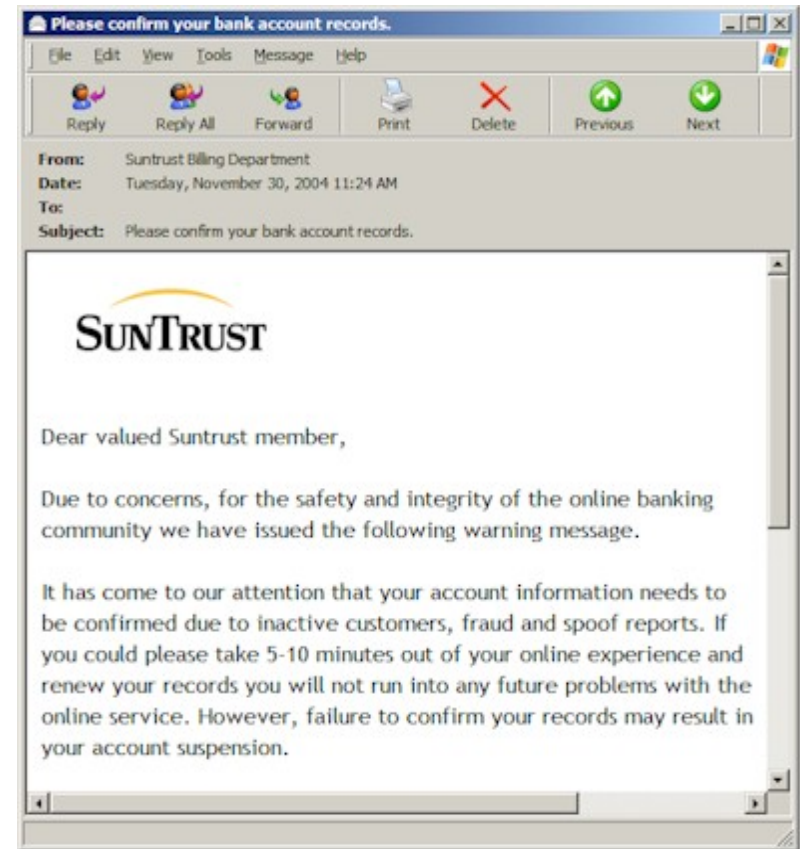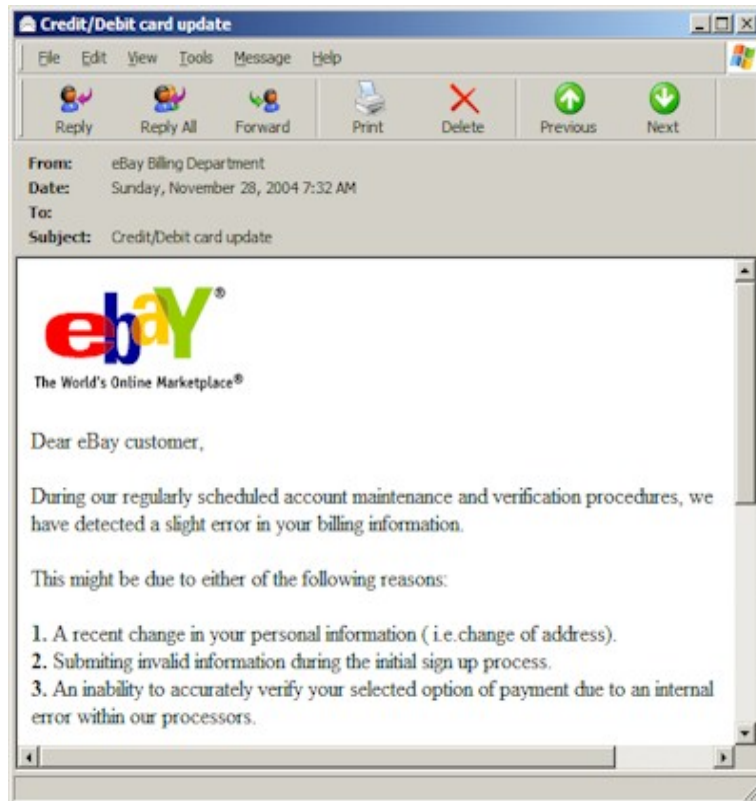
**Source:** Webopedia

# Botnets
## Phishing (Incidents)

**In the eBay** phishing scam, users received e-mails supposedly from eBay claiming that the user's account was about to be suspended unless he clicked on the provided link and updated the credit card information that eBay already had.





**SunTrust** e-mail claimed that the inactive users should update all the information to keep their accounts current.

# Botnets

## Incidents

### October 20, 2004 ZDNet UK by Graeme Wearden

**Phishing attacks powered by 'just five' zombie networks**:

Reseach carried out by Ciphertrust has found that phishing emails come from groups of 1,000 hijacked computers belonging to one of five botnets

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

CipherTrust 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, CipherTrust says it found that every day a different set of around 1,000 zombie computers were used to deliver phishing emails.

More than 32 percent of these zombies were based in the US, and 16 percent in the Republic of Korea. The remaining 52 percent of phishing zombies were spread across 98 other countries, with just over 4 percent based in the UK.

CipherTrust also found that 70 percent of zombie PCs are also used to send SPAM, which confirms the views of anti-SPAM expert Steve Linford.

**Source:** http://news.zdnet.co.uk/internet/security/0,39020375,39170848,00.htm

# Botnets
## Phishing (Create Infections)

*July 23, 2004 Sophos (Munir Kotadia)*

**Suicidal Osama Bin Laden' recruits a zombie army:** A new way of enticing users to open a Trojan horse called Hackarmy was discovered by antivirus firm Sophos on Friday after it was posted on several Internet news groups. The message claims to contain pictures taken by CNN journalists of Osama Bin Laden's suicide but, once the file is opened, it installs a Trojan horse that effectively recruits the infected machine into the ***author's zombie army***, which can then be used to distribute SPAM or launch DDoS attacks.

**Sample message:**

```
Osama Bin Laden was found hanged by two CNN
journalists early Wednesday evening. As
evidence they took several photos, some of
which I have included here. As yet, this
information has not hit the headlines due to
Bush wanting confirmation of his identity but
the journalists have released some early
photos over the internet. <url removed>
```

# Botnets
## Incidents (Spreading Porn)

### October 1, 2003 (Brett Glass, ExtremeTech)

**Don't Let Your PC Become a Porn Zombie:** **More than a thousand Windows PCs were hijacked recently, unbeknownst to their owners, to send SPAM and distribute pornography.** This was done via a Trojan known as Migmaf (migrant Mafia) that turned their machines into proxies, or relay points, which hid the real servers involved. The victim machines, controlled from afar, are often called zombies. Here's how to keep your PC from becoming a zombie in the service of spammers, pornographers, and malicious hackers.

It's important to understand that although mainstream news coverage of such exploits is a recent development, these activities have been occurring practically since the general public was allowed to use the Internet in the early 1990s. Back then, hackers who wanted to cover their tracks would take control of machines running certain programs that let Windows-based PCs share Internet connections. They'd then use these machines as proxies for their attacks on other systems. When investigators tried to trace the break-ins, they would find only the Windows machine, which kept no record of the hacker's whereabouts

**Source:** http://www.pcmag.com/article2/0,1759,1265383,00.asp

# Botnets
## Sniffing & Keylogging

- Bots can also use packet sniffers to observe data (text) passing across a compromised machine.

  - Used primarily to retrieve sensitive information like usernames and passwords.

  - If a machine is compromised by more than one botnet once packet sniffing allows to gather the key information of the other botnet making it possible to "steal" another botnet

- If the compromised machine uses encrypted communication channels (e.g. HTTPS or POP3S), sniffing the network packets is useless.

  - In such case, keyloggers are installed on hacked machines to retrieve sensitive information using filtering mechanisms (e.g. "I am only interested in key sequences near the keyword 'paypal.com'")
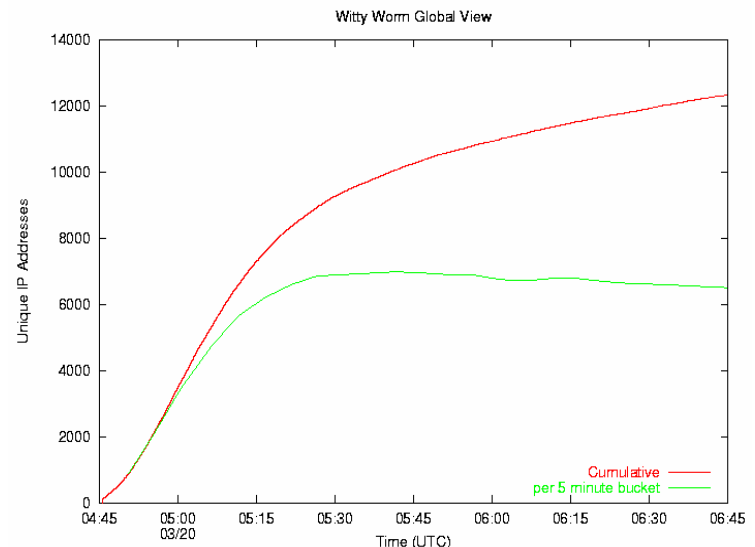
# Botnets
## Spreading Malicious Code

- Usually botnets are used to spread new bots which requires tem to download and execute a file via HTTP or FTP.

- Email viruses can be easily spread using a botnet as well
  - A botnet with 10.000 hosts which acts as the start base for the mail virus allows very fast spreading and thus causes more harm.

*March 2004, Colleen Shannon & David Moore*

**The Spread of the Witty Worm:** The Witty worm, which attacked the ICQ protocol parsing implementation in ISS products is suspected to have been initially launched by a botnet due to the fact that the attacking hosts were not running any ISS services.



Witty Worm Global View

# Botnets
## Installing Adware

- Adware is any software application that generates advertisements such as pop-up windows or hotlinks on Web pages that are not part of a page's code.

    – It can changes the home page & search engine to sites that earn income from various advertisers.

    – This income is dependent on, for example, how many people visit the adware site, or how many people click on the links or advertisements at the site.

    – These ads are legitimate if they are displayed with the consent of the user however, many adware programs do not give users enough notice or control.

- Botnets set up a fake website with some advertisements.

    – The operator of this website negotiates a deal with some hosting companies that pay for clicks on ads.

    – With the help of a botnet, these clicks can be "automated" so that instantly a few thousand bots click on the pop-ups.

    – This process can be further enhanced if the bot hijacks the start page of a hacked machine so that the "clicks" are executed each time the victim uses the browser

# Botnets
## Inflate Ad Revenues

- Botnets can also be used to inflate advertisement revenues
  - Google's AdSense program offers companies the possibility to display Google ads on their own website.
  - Companies earn money based on the clicks on these ads
  - An attacker can abuse this program by leveraging his botnet to click on these advertisements in an automated fashion and artificially incrementing the click counter.
  - This kind of usage for botnets is relatively uncommon, but not a bad idea from an attacker's perspective
- Adware vendors estimate they make $2-7 per infected PC

**Source** http://www.eecs.utoledo.edu/~jwalden/talks/hackers101.html
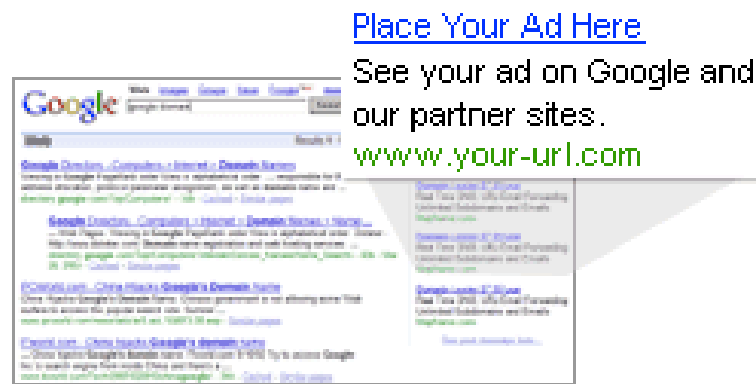
# Botnets
## Incidents (Adwords)

**Botnets strangle Google Adwords campaign:** Researchers have discovered a way to shut down or seriously impair a Google Adwords advertising campaign by artificially inflating the number of times an ad is displayed. By running searches against particular keywords from compromised hosts, attackers can cause click-through percentage rates to fall through the floor.

This, in turn, causes Google Adwords to automatically disable the affected campaign keywords and prevent ads from being displayed. By disabling campaign keywords using the technique, cyber criminals could give their preferred parties higher ad positions at reduced costs, according to click fraud prevention specialists Clickrisk.

**Source:** http://www.theregister.co.uk/2005/02/03/google_adwords_attack/

**Start gaining new customers in less than 15 minutes.** Google AdWords ads connect you with new customers at the precise moment when they're looking for your products or services. The Google Network reaches more than 80% of Internet users. With Google AdWords you create your own ads, choose keywords to help us match your ads to your audience and pay only when someone clicks on them.
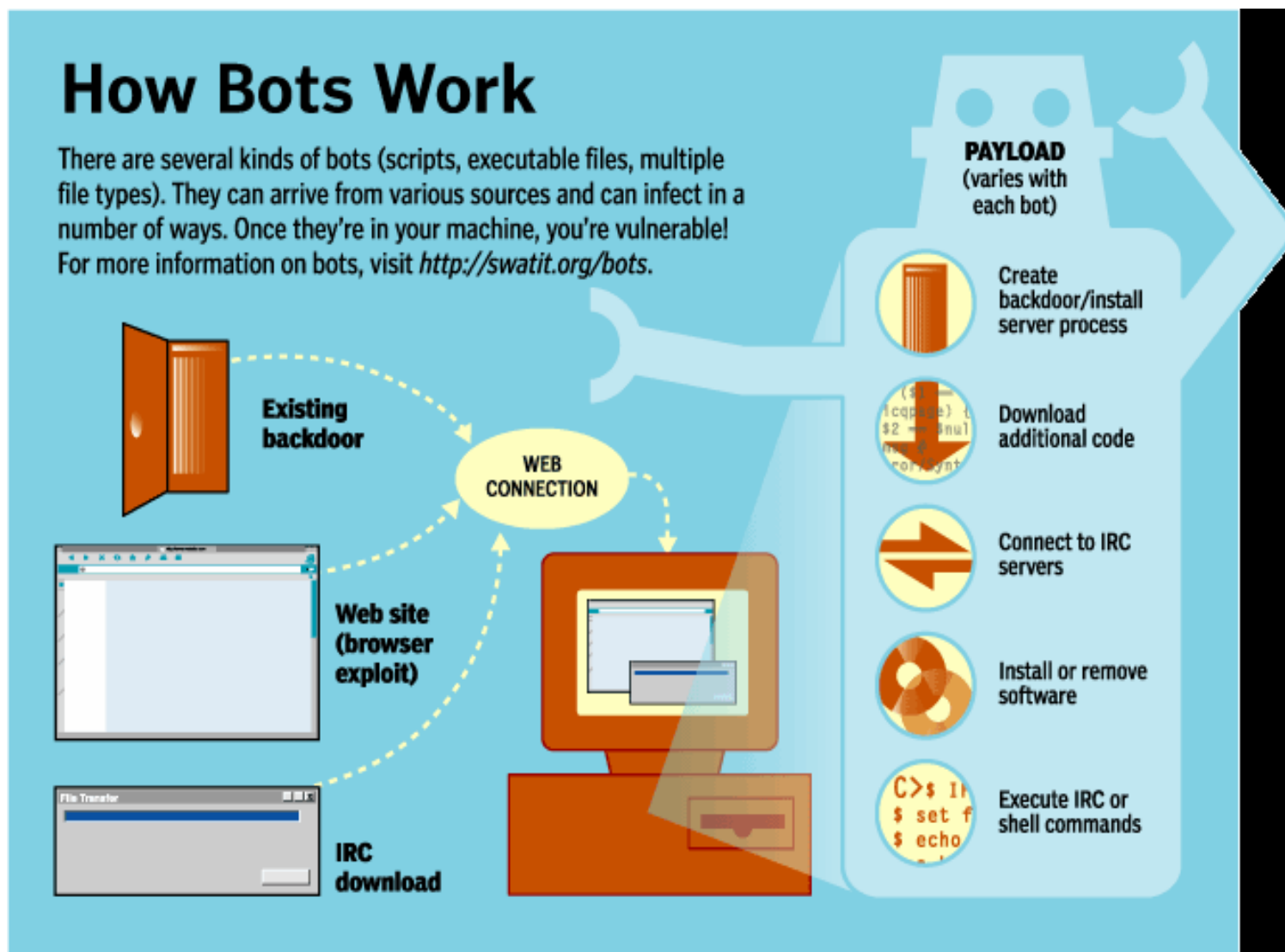
# Architecture & Types

# Botnets

## How Botnets Work?

# Botnets
## Agobot/Phatbot/Forbot/XtremBot

- Most well known bot (500 versions of Agobot)
  - Written in C++ with cross platform capability
  - Highly modular design allowing extensions to the design
  - Uses libpcap (packet sniffing library) and and Perl Compatible Regular Expressions (PCRE) to sniff and sort traffic
  - Well organized user interface

  - Provides rootkit capabilities to hide traffic

  - Makes reverse engineering harder since it includes functions to detect debuggers and virtual machines

  - Use IRC to communicate with controller
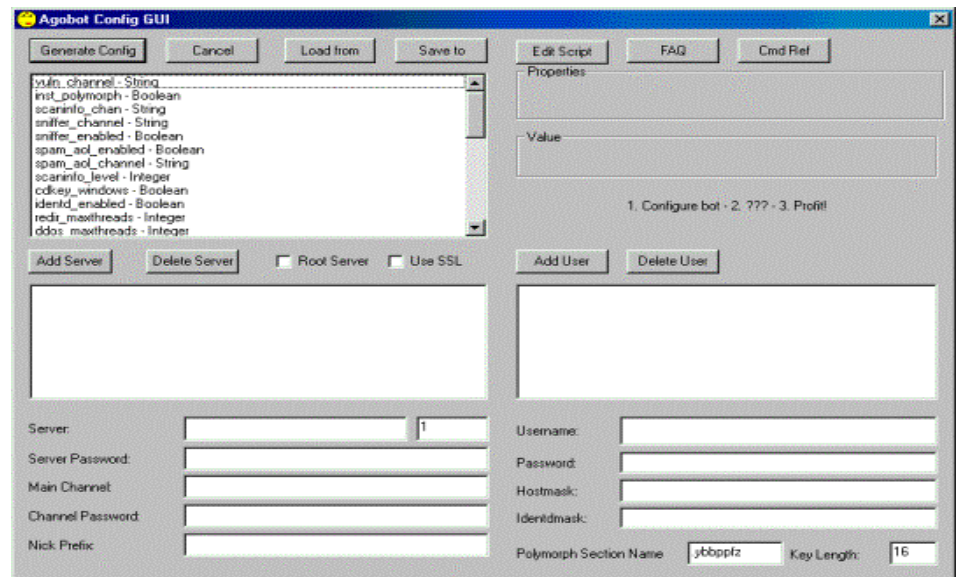
# Botnets
## How Do They Work?

- Machine infected with worm attempts to infect vulnerable computers
    - Scans the subnet to find vulnerable computers
    - Infects the vulnerable computers via various exploits and copies itself onto them

- Vulnerabilities it Exploits
    - WebDav (MS03-007)
    - RPC-DCOM (MS03-039)
    - LSASS (MS04-011)
    - Unprotected windows shares
    - Weak passwords on windows shares
    - MyDoom backdoor

```
O O O                192.168.2.2: 192.168.2.2 #TheName
192.168.2.2        #TheName                                      op
pop: 2                                                          Nick
    ***: You have joined the channel                           TheOper
    ***: xjbe945 (~xjbe945@192.168.2.3) has joined the channel xjbe945
TheOper: .login ago pass
TheOper: .bot.login adnan pass
TheOper: .login adnan pass
xjbe945: Password accepted.
TheOper: bot.execute 1 notepad.exe
TheOper: .bot.execute 1 notepad.exe

                                                          Msg    Query
                                                          Whois  Kick
```

# Botnets
## Description

Controller
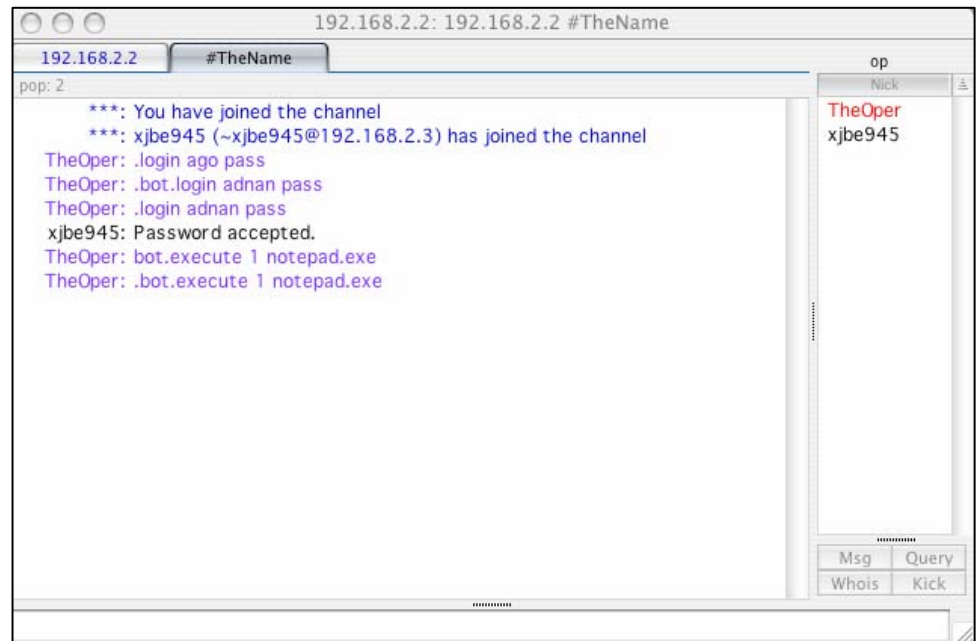
Hacker uses password to connect to the IRC Channel and to send commands to the zombie computers

Controller Sends Commands to the Zombie machines through IRC Channel

Private Channel

IRC Servers

IRC Channels

User Machines

Infected Machines Connect to Specific IRC Channel
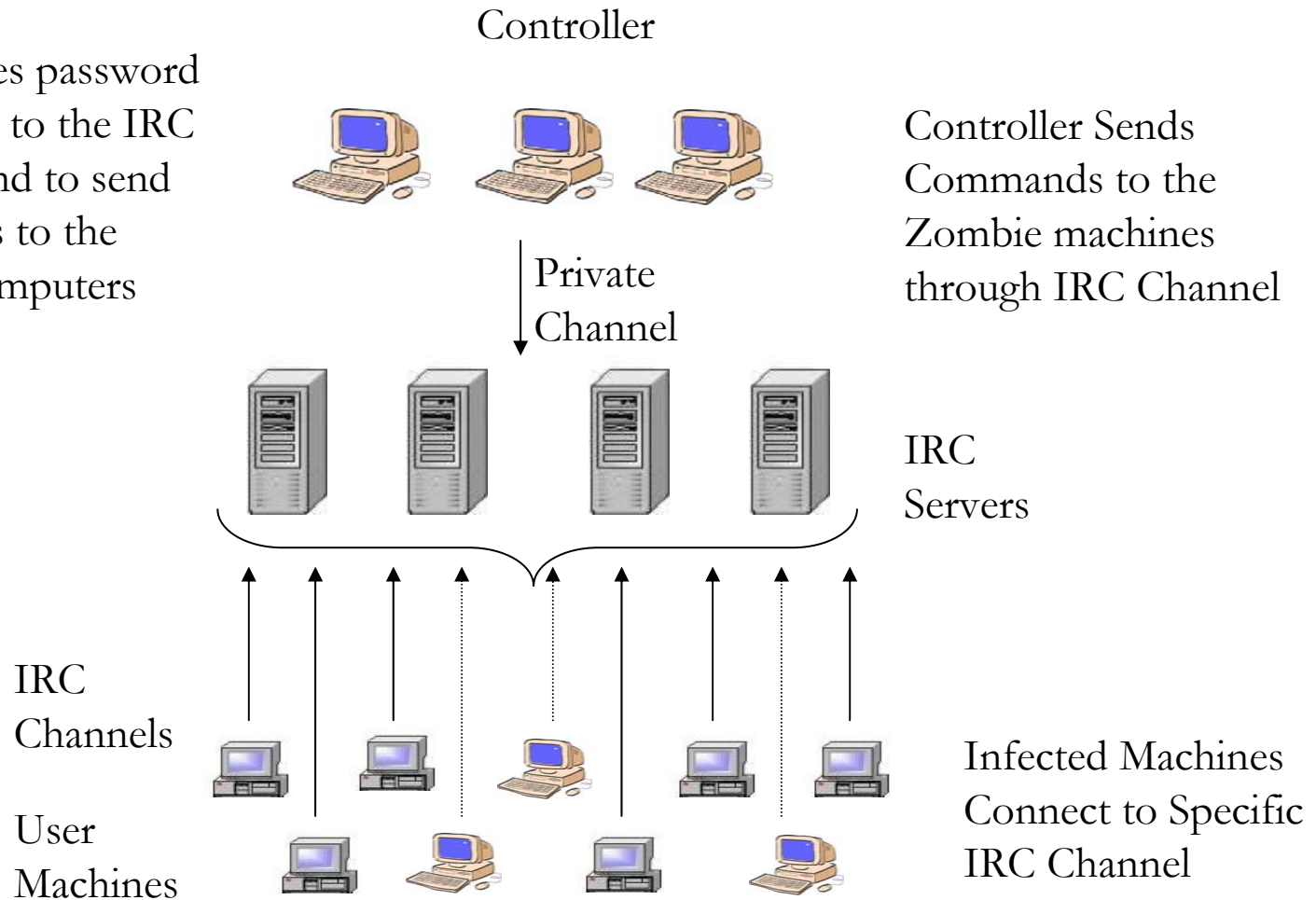
# Botnets
## Propagation & Control

- Every infected machine has a copy of the available servers list
- Uses simple IRC client to connect to an IRC channel and waits for commands
- Controller connects to same IRC channels and issues commands
- Usually, every module connects to different IRC channel (Chat rooms).
- Often botnets have distributed control
  - If one controller is disabled an alternate controller can replace it

# Botnets
## Agobot (Where to get it?)

- Origin
  - Written by 21 year old guy who calls himself Ago
  - Built on sdbot (one of the first irc bots)
  - Uses many known windows vulnerabilities to spread
  - Very modular
  - Easy to build and control
- Source
  - Source code is available on the internet
    - www.networkpunk.com
    - www.gigen.tk
  - Total download size is 50MB
  - Toolkit has a graphical user interface
  - Can be used to create custom trojans in minutes
  - New exploits can be added very quickly as they become available

# Botnets

## SDBot/RBot/UrBot/UrXBot/...

- Currently most active malware with 840 variations

- Written in poor C and also published under the GPL.

- Used for creating variants such as RBot, RxBot, UrBot, UrXBot, JrBot

- The source code of this bot is not very well designed or written. It offers similar features to Agobot, although the command set is not as large, nor the implementation as sophisticated.

- The latest, W32/Rbot.KZ, uses weak passwords on network shares and on three Microsoft vulnerabilities (MS03-007, MS04-011, and MS04-012).

- SDBot.AB can accomplish several tasks

    – Steal product license keys for a wide range of computer games

    – Perform a DoS attack against a target host, retrieve system information, connect to a URL, upload and download files, execute programs, log keystrokes, sniff network packets, conduct port scans against other computers, or steal the Windows Product ID.

# Botnets
## mIRC-based Bots (GT-Bots)

- mIRC itself is a popular IRC client for Windows.

- GT is an abbreviation for *Global Threat* and this is the common name used for all mIRC-scripted bots.

- These bots launch an instance of the mIRC chat-client with a set of scripts and other binaries.

- Libraries include

  - *HideWindow* executable to make the mIRC instance unseen by the user.

  - The other binaries are mainly Dynamic Link Libraries (DLLs) linked to mIRC that add some new features the mIRC scripts can use.

  - The mIRC-scripts, often having the extension ".mrc", are used to control the bot.

  - They can access the scanners in the DLLs and take care of further spreading. GT-Bots spread by exploiting weaknesses on remote computers and uploading themselves to compromised hosts (filesize > 1 MB).

# Botnets
## Other Bots

- **DSNX Bots**

  The Dataspy Network X (DSNX) bot is written in C++ and has a convenient plugin interface. An attacker can easily write scanners and spreaders as plugins and extend the bot's features. Again, the code is published under the GPL. This bot has one major disadvantage: the default version does not come with any spreaders. But plugins are available to overcome this gap. Furthermore, plugins that offer services like DDoS-attacks, portscan-interface or hidden HTTP-server are available.

- **Q8 Bots**

  Q8bot is a very small bot, consisting of only 926 lines of C-code. And it has one additional noteworthiness: It's written for Unix/Linux systems. It implements all common features of a bot: Dynamic updating via HTTP-downloads, various DDoS-attacks (e.g. SYN-flood and UDP-flood), execution of arbitrary commands, and many more. In the version we have captured, spreaders are missing. But presumably versions of this bot exist which also include spreaders.

- **kaiten**

  This bot lacks a spreader too, and is also written for Unix/Linux systems. The weak user authentication makes it very easy to hijack a botnet running with kaiten. The bot itself consists of just one file. Thus it is very easy to fetch the source code using wget, and compile it on a vulnerable box using a script. Kaiten offers an easy remote shell, so checking for further vulnerabilities to gain privileged access can be done via IRC.

- **Perl-based bots**

  There are many different version of very simple based on the programming language Perl. These bots are very small and contain in most cases only a few hundred lines of code. They offer only a rudimentary set of commands (most often DDoS-attacks) and are used on Unix-based systems.

# Detection & Defense

# Botnets
## Hard to Detect

- IRC servers are on infected machines

- Hackers connect to IRC servers to control the botnet

- It is very hard to locate every IRC server

- Users on the channel are invisible

- Can't we monitor the activity?
  - Hard to determine who is controller and who is zombie
  - Even if we did, it is hard to locate them
  - Even if we did, most countries do not have laws against hackers

# Botnets

## What to do if you suspect your machine has become a zombie?

- Check if your hosts file has been rewritten?
  - C:\winnt\system32\drivers\etc (Check timestamp)
- See if you have a lot of unidentified connects to the system?
  - Open a command prompt (Start → Run → cmd)
  - Observe At the command prompt type netstat -an.
  - Take a look at the devices that are listed. Do you recognize all of the ips?
- Go into windows task manager and check for any processes that you don't recognize.
- Check the registry entries
  - HKEY_LOCAL_MACHINE → software → Microsoft → windows →current version.
  - You should see run and run once and run services and check for entries that you don't recognize or look suspicious?

**Source:** http://channels.lockergnome.com/windows/archives/20041012_is_your_computer_part_of_a_botnet.phtml

# Botnets
## Protection: Anti-virus

- Make sure that the latest virus definitions for your specific anti virus software are installed.
    - The leading anti virus software providers are working on circumventing the latest cracker techniques.

- There is a lag between the time a virus is released to the time when the virus signature is added to the database
    - It is easy to create variants of the virus that have a different signature which can pass undetected

# Botnets
## Protection: Packet Filtering

- Use Egress and Ingress filtering
  - Filtering inbound traffic is called Ingress filtering
  - Filtering outbound traffic is called Egress filtering.

- Most worms will install a backdoor on the compromised host for malicious users to connect to, or will establish a connection with a server (IRC on Agobot case).

- Most of the time these backdoors will use high network ports.
  - Business entities must carefully decide the services they need and only allow the ports for those services to use the outbound/inbound connections.
  - In case worms use port 80 (web traffic) for backdoors Egress and Ingress filtering fails to protect the network.

# Botnets
## Protection: Proxies

- Employ proxies for outbound connection.

  - Proxies can be configured to analyze the traffic and drop connections that are not suitable for the type of traffic we want our users to use.

  - For instance, one can install web proxy and configure it in a way that it will only allow "web traffic".

  - This proxy will successfully stop Agobot virus running on port 80 to make an outbound connection because IRC traffic is fundamentally different than web traffic.

  - This works if IRC traffic is not encrypted. There are many known worms today which ssl encrypt the traffic. In this case proxies will fail.

- Another advantage of proxy is that hosts on the subnet can not communicate with outside world directly

  - They have to make a request to the proxy and proxy will forward the traffic.

  - This will stop most of the today's worms because they all assume that they can make an outbound connection directly. But, it is very straight forward to get the proxy information from host machines configuration files and use that information to establish an outbound traffic.

# Botnets
## Protection: HIDS

- Installing Host Intrusion Detection Systems (HIDs) on each machine on the subnet will allow everybody to monitor their connections and block the ones that are not legitimate/not needed.

- For this to work the users need to be educated about communication networks.

- Currently, most of the users don¹t even know what a "port" is making the education task very onerous

# Botnets
## DDoS

- A SYN Flood is an aborted handshake.
    - Internet communications use a three-way handshake where initiating client initiates with a SYN, the server responds with a SYN-ACK, and the client then responds with an ACK.
    - In this attack sends an attacker sends the SYN from a spoofed ip-address which results in the SYN-ACK being sent to a non-requesting address. The server then waits for the ACK response to no avail.
    - When large numbers of these aborted SYN packets are sent to a target, the server resources are exhausted and the server succumbs to the SYN Flood DDoS.