Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Bots &; Botnet: An Overview

Using thousands of zombie machines to launch distributed denial of service attack against enterprise and government internet resources by attackers is becoming dangerously common trend. Recently, there is a growing trend towards attackers, using Internet Relay Chat (IRC) networks for controlling & managing infected internet hosts. This paper provides an overview of malicious bot, a remotely controlled trojan which infects internet hosts and is remotely controlled by attacker via private IRC channels. The paper provides...

Copyright SANS Institute
Author Retains Full Rights

AD
CounterTack
Counter Tack Active Forensics
for In-Progress Attacks
GET THE WHITE PAPER NOW >>>

Bots & Botnet: An Overview

Ramneek Puri
August 08, 2003
GSEC Practical Assignment Version 1.4b
Option 1 – Research on Topics in Information Security

Abstract

Using thousands of zombie machines to launch distributed denial of service attack against enterprise and government internet resources by attackers is becoming dangerously common trend. To create this army of zombie internet hosts, attackers typically infect machines of home users having broadband access to internet,' networks maintained by universities & small enterprises, with remotely controlled trojans. Owners of these machines are typically profiled as users with relatively low internet security awareness and limited resources to defend their internet infrastructure. Recently, there is a growing trend towards attackers, using Internet Relay Chat (IRC) networks for controlling & managing infected internet hosts. This paper provides an overview of malicious bot, a remotely controlled trojan which infects internet hosts and is remotely controlled by attacker via private IRC channels.

The paper provides brief background into underlying IP protocol, IRC (RFC 2810) and covers the terms used to explain the operations of bots, the elements involved in malicious bots infection, insight into possible uses of bot infected machines by attackers. How & why an attacker chooses a target system to infect, describes the process of malicious bot infecting a system & attacker remotely controlling the infected system via IRC channels, list & characteristics of some of known bots, takes a look at how bots could be used as part of information warfare strategy, provide recommendations for home user & system admin to prevent, detect & respond to malicious bot activity.

Introduction

The internet by its inherent characteristic, comprise of finite resources and attackers have traditionally exploited this by exhausting computer & network services with illegitimate requests, thereby denying the legitimate access to these services. The model for denial of service attack has evolved from single attacker machine against single target machine to multiple attacker machines flooding requests to single target. The later DDoS model was refined by attackers by using multiple handlers for directing & managing large number of hosts against a single target.

The tools & technology for denial of service attack has evolved over a period of time, they are readily available & easy to use. In their paper [CERT, DOS_TRENDS] "*Trends in Denial of Service Attack Technology*" George M. Weaver & Kevin J. Houle from CERT® Coordination Center have discussed model, where attackers infect large number of internet hosts with remotely

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

controlled trojans & direct them against DDoS targets via handlers, as the most common attack technique. Interestingly, the use of handler to manage & direct large number of zombie hosts (infected systems under attacker control) has in recent years, largely been replaced by Internet Relay Chat (IRC) networks, acting as attacker's virtual command & control centers.

Wide ranging popularity of IRC network & services help attackers to obscure their activities & evade detection in disguise of legitimate IRC traffic. The infected hosts connect to attacker hosted IRC channels called "bots "& network of these bots connect to an IRC channel forms a "botnet".

'Bots' are analogous to 'agent' that in traditional DDoS models infect host machine & maintain access for attackers to control them via 'handlers' analogous to 'botnets', while referring to IRC networks. Typically, a bot when installed on a victim machine establishes outbound connections to a standard IRC network service port & joins attacker private channel. Public IRC networks such as Efnet, Undernet or DALnet, provide attackers with stable, scalable infrastructure to maintain, expand, manage & control their bots army.

IRC networks provide attackers easy & flexible ability to control hundreds or even thousands of bots (malicious program on individual infected machine). It also helps them to obscure their identity, making task of tracking the source of attack by sys-admins & law enforcement agency much more difficult.

According to Australian CERT, [AuCERT] advisory reference--AA-2002.03, the criteria attackers use to select victims for the purpose of bots infection is that of high-bandwidth and high-availability. The potential targets are not limited to university servers, but also home broadband users and Internet Service Providers. Additionally, there is growing practice of using IRC based trojans & backdoors for file sharing over IRC channels i.e. "distributing pirated intellectual property".

There are likely hundreds or perhaps thousands of highly configurable, customizable bot packages freely available on the internet. They range from self written task specific codes to of-the-shelf executables used by script kiddies. The common protection provided against bot infection by anti-virus packages is limited to known bot variants.

Background

IRC is an internet protocol developed by Jarkko Oikarinen of Finland in 1988, with basic function to allow people connected anywhere on the Internet to join in real-time text based discussions. Each discussion is on a "channel," and many people can join at once. According to [IRC RFC] RFC 2810, "The IRC (Internet Relay Chat) protocol has been designed over a number of years for use with text based conferencing. The IRC Protocol is based on the client-server model, and is well suited to running on many machines in a distributed fashion. A typical setup involves a single process (the server) forming a central point for clients (or other servers) to connect to, performing the required message delivery/ multiplexing and other functions. "

A typical IRC setup consists of a user running an "IRC client" program which connects to a "server" in an IRC network. All servers are interconnected and

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

pass messages from user to user over the IRC network. One server can be connected to several other servers and up to hundreds of clients. Default TCP service port for IRC is 6667 and generally IRC servers listen on port range of 6000-7000, though it could be configured to run on any TCP port.
In one of the communications mode available on IRC networks multiple IRC clients [MIRC] connect to IRC servers to form a logical grouping referred to as *channel*. The communication sent by each client to IRC server is pushed to all other IRC clients that are connected to that channel.

The term *bot* is derived from "ro-bot ". Bot is a generic term used to describe a script or set of scripts designed to perform predefined functions in automated fashion. Bots are used by search engines to spider online website content & by online games to provide virtual opponents. e.g. the games sometimes we play against computer while online, bot act as our artificial opponents. [DALNET] More specifically on IRC network bot's function in channels include managing access lists, move files, share users, share channel information, anything else if right scripts are added.

In summary, IRC bots are automated and controlled by events which could be commands given in a channel by other IRC bot or client with necessary privileges.

Elements of Typical IRC Bot Attack

Bots in its malicious mutation are used by attackers to infect victim machines after they have been compromised or the victim machine user is tricked into performing the installation. The bots on installation joins the configured IRC channel & waits for attackers command. The figure below shows typical IRC bot attack and the elements involved.

- *Bot*: is typically an executable file, capable of performing a set of functions, each of which could be triggered by a specific command. A bot when installed on victim machine copies itself into a configurable install directory & changes system configuration to start each time system boots. For windows platform the bots may add its instance to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\, the typical size of a compressed bot is less than 15kb in size. An off-the-shelf bot generally used by less sophisticated attacker can be downloaded from warez site on internet & edited to include, desired remote IRC server to connect, remote TCP port to use for this connection, channel to join on that server and authentication password referred to as 'key' to gain access to attackers private channel. A more sophisticated attacker can even manipulate the bot characteristics like files created after installation and install directory where the bot files reside after installation. One important point to note is that bots are not the exploits for OS or application, they are the payload carried by worms or means used to install backdoor once a machine has been comprised.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

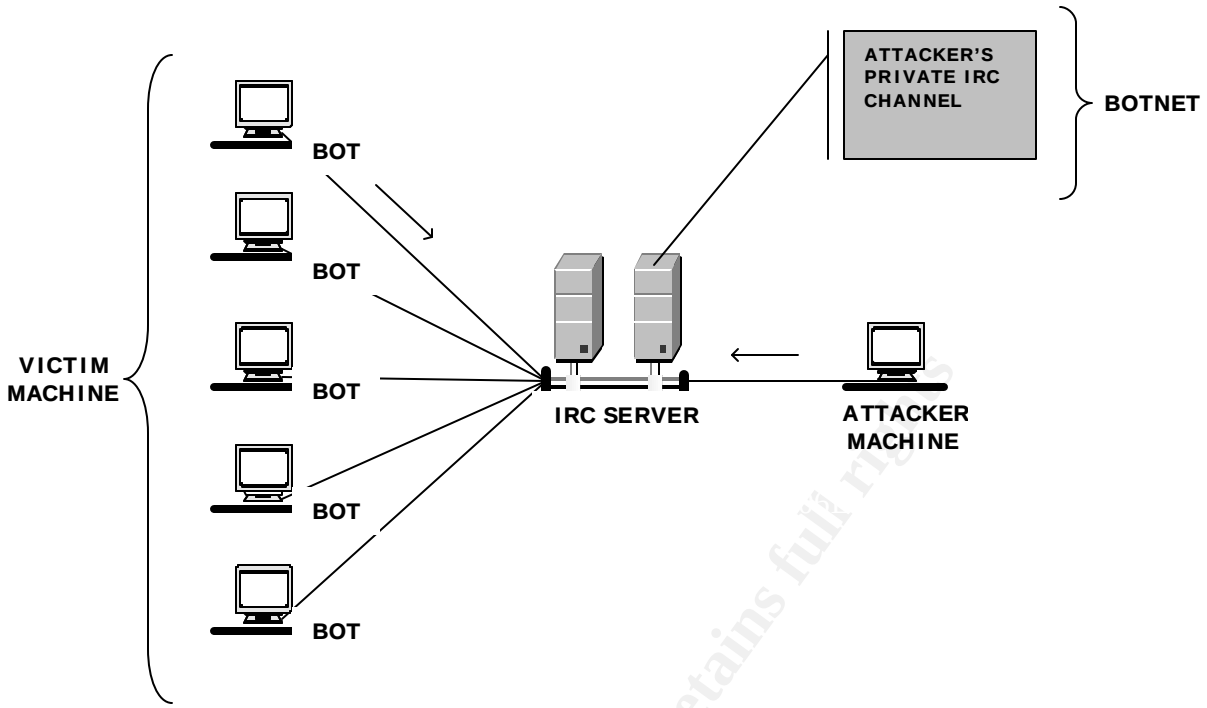


Figure 1: Elements of typical IRC BOT Attack

- *Victim machine*: is the compromised internet host on which the malicious bot is installed after the attacker has exploited an application or operating system vulnerability or has duped the user into executing a malicious program. Once infected the target host are also referred to as Zombies.
- *Attacker*: is the one that configures the bot, it comprises a machine to install a malicious bot, controls & directs the bots once it joins the designated IRC channel.
- *Control channel*: is a private IRC channel created by the attacker as rendezvous point for all the bots to join once they are installed on infected machine & are online, it comprises of a channel name & a password 'key' to authenticate.
- *IRC Server:* is a server providing IRC services, this could be a legitimate public service provider like DALNET etc. or another attacker's compromised machine.
- *Botnet*: All the bots once connected to control channel form a botnets i.e. network of bots, awaiting the attacker command.

Malicious use of Bots & Botnet

Following are some of the malicious activity performed by attackers using bots & botnets.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- *Distributed denial of service attacks*: This is the foremost reason for using malicious IRC bots by attackers. The attacker could command its army of zombie machines through botnets, to send large size stream of UDP packets or large size stream of ICMP requests or flood TCP sync requests to target servers, against which the DDoS is directed. [AuCERT] With hundreds or even thousands of bots at its command the attacker is able to choke the bandwidth of target server thus denying the server to cater legitimate service requests.
- *Secondary local infection*: with installation of bots the attacker takes the complete control of victim machine, the attacker could further download & install key logger or trojan to gather valuable information from the infected host, like online banking passwords, credit card numbers or any other personal information stored on compromised machine.
- *Trade bandwidth*: another interesting use of infected machine is trading of bandwidth of high speed bots (infected machine with "always on", broadband connection to internet) between hacker communities.
- *Backdoor*: bots are installed on compromised machines as backdoors to maintain access after the exploit, especially if there is already legitimate IRC traffic in the network. Attacker could configure the bots to use same remote TCP port as used by legitimate IRC traffic, thereby reducing the chances of detection by sys-admins.
- *Host illegal data:* In a growing trend attackers are using the malicious bots to make victim machine part of file sharing networks & [CNET] use their storage space to host illegal files, software, pirated movies, especially in case the infected host happens to be server with large storage space connected via a high speed internet link. [AuCERT] The IRC bots (such as Iroffer) are designed specifically for file-sharing over IRC.

Additionally, tracking of actual attacker that installs malicious bot on victim machine and uses it for illegal activity is quite difficult & seldom pursued by ISPs or sys-admins. It might be clear from above, the destructive use of bots & botnet is restricted only by attacker's imagination & could involve the infected machine into host of illegal activities.

Prime Targets/Victims

The host connected to internet that are most desired by attackers, thereby most vulnerable to bots infection are less monitored, high bandwidth, home computers or university servers. [NETSYS]

- *High bandwidth*: one of the most sorts after internet hosts by attackers are machines connected to internet by broadband access, giving attackers large cumulative attack bandwidth to target servers for DDoS or host pirated files or software.
- *Availability*: the attacker prefers machines that are "always on", highly available to carry out their commands round the clock.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- *Low user awareness & monitoring capability:* Users with low internet security awareness & with limited resources to invest in access control devices are specially targeted for bots infection. Lack of updated operating system and/or application in addition to non-existence of access control devices like firewall gives the attacker the opportunity to break into system & maintain the bots over a long period of time without being identified or traced.
- *Location*: the attacker target machines, which are geographically far away from their own location & with relatively low probability of law enforcement officers being able to trace the bots back to attacker.

The typical profile that fits the above criteria is that of a residential broadband connection or university servers those are connected to internet via broadband connection & are most of the time available i.e. 'on'.

The attackers generally target residential broadband connectivity providing ISP subnets or university subnets that have low or no access control devices, with minimal monitoring of internet connection.

Bots Infection & Control Process

The section describes process in stages, of attackers using the bots, customizing it as per their need, exploiting the victim host, infecting it with malicious bot & controlling the bots to attack the other targets or use it as zombies to above discussed means.

Coding/Editing: the process starts by depending on attacker's skills, by either editing known bots available on the internet warez sites or writing own code with primary configurable component being, IRC server where the bot will connect once installed on victim machine, remote IRC TCP service port to connect, private channel name to join, password or key to authenticate the bots access to that private channel. Additionally, depending on the specific bot used, the attacker may change the location & name of file that is placed on directory of infected machine. Further the attacker may choose to use dynamic or multiple channels that a bots joins so that to maintain access to their botnet army in case they are banned from a specific IRC server. To achieve this, the attackers generally use service providers like dyndns.com or no-ip.com to associate dynamic ip mapping to IRC server for bots to join.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

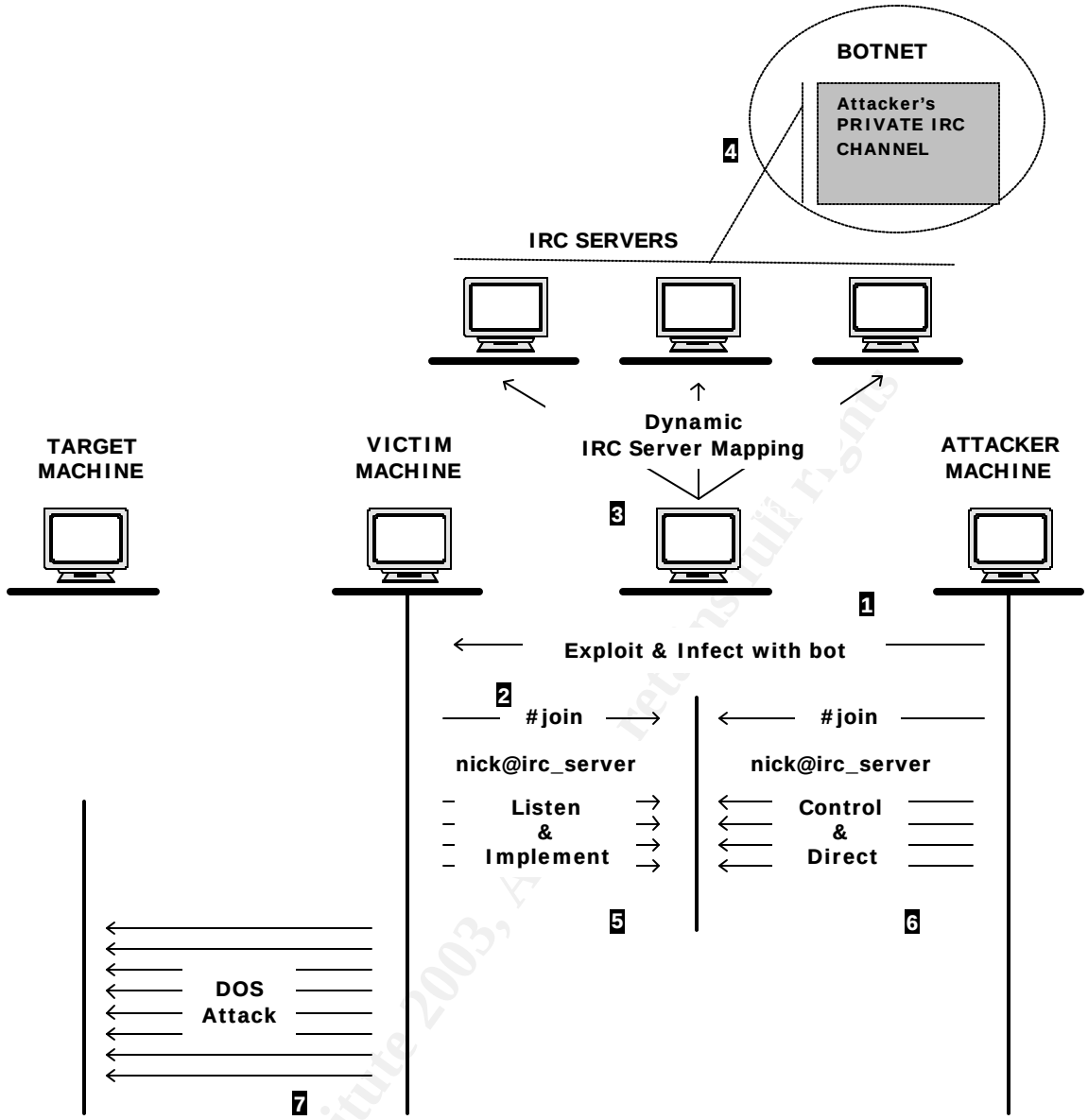


Figure 2: Bots Infection & Control Process

The figure above shows a single instance of bot infection, the process is replicated over large number of hosts to create army of bots or zombie machines.

The attacker, attempts to infect the victim machines with bots through either exploiting some operating system/application vulnerability or trick the user into executing a malicious program leading to bots installation. *(1)* Typical way for attacker infecting mass group of internet hosts is to use exploit code of recently disclosed vulnerability, [NDNN] use it to gain access to victim machine and install bots as backdoor to maintain that access. The described process could be automated by using a directed worm that will scan a target subnet for known vulnerability, exploit the largely un-patched systems & infect them with malicious bot. [ZDNET] Other way is to exploit unpatched web applications & trick the user into executing some malicious program or virus leading to bots infection. User

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

could install an IRC client with trojan inside that while doing all legitimate tasks of IRC client also installs a bot on user machine.

After the bot installs on victim machine it copies itself to install directory & updates the registry keys in case of windows platform. In next stage, *(2)* the bot attempts to connect to IRC server with a randomly generated nick name i.e. the unique name or handle representing that bot in attacker's private channel. The bot uses the 'key', authentication password to *join* the attacker's private IRC channel.

Further many times the attackers use public IRC servers for these activity & could be banned by IRC administrators, thus loosing their botnet army. To avoid this, attacker sometimes use service providers like dyndns.com or no-ip.com to *(3)* dynamically map their bots with multiple IRC servers.

Once *(4)* the bot is installed on victim machine, it joins the attackers channel with unique nick name, as part of attacker's botnet army awaiting instructions *(5)*

Often as these bots join the IRC channel the attacker will log into them *(6)* with a complex and sometimes encrypted access password, ensuring that the bots cannot be controlled by others and making it harder for someone to hijack the botnet. After the access has been accepted the attacker may direct & remotely control the action of large number of infected zombies via this botnet to stage attack against other targets *(7)* or use it for other described malicious activities.

Described above is the process for a single instance of bot infection & control, the process could be replicated over large number of hosts to create army of bots or zombie machines.

Some Known Bots

Listed below are some of the commonly used malicious bots freely available on internet for Microsoft windows platform.
The list available at http://www.simovits.com/trojans/trojans_action.html provides brief description & major characteristics of IRC bots.

GTbot

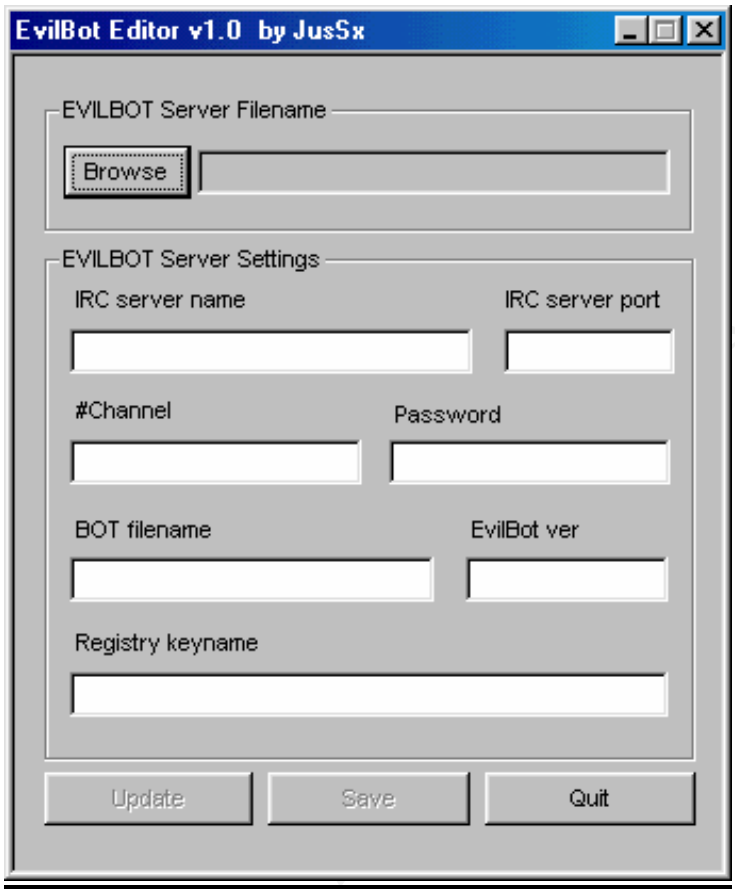
As per the analysis provided at http://swatit.org/bots/gtbot.html primary characteristics of this variant of GTbot are

- uses the legitimate mIRC program as its main carrier.
- easy to rewrite or edit, develop own variations.

Aliases: W32.IRCBot,
Ports: configurable
Use: Remote Access / IRC trojan
Registers: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
Platform: Windows 95, 98, ME, NT, 2000 and XP.

Evilbot

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



Screen capture of EvilBot v1.0 editor from
http://www.megasecurity.org/trojans/e/evilbot/Evilbot_a.html

Typical size of compressed file: 15.904 bytes
Ports: 6667 (port can be changed)
Use: Remote Access / IRC trojan / Distributed DoS tool / Downloading trojan
Registers: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\
Platform: Windows 95, 98, ME, NT, 2000 and XP.
For further information please refer to
http://securityresponse.symantec.com/avcenter/venc/data/pf/backdoor.evilbot.html

SlackBot
Aliases Backdoor.Slackbot, DDOS/Slack, Troj/Slack, Slack,
Ports: 6667 (port can be changed)
Files: Slackbot.zip - Slackbot1_0.zip - Zwbv.exe - Sbconfig.exe -
Uses: Remote Access / IRC trojan / Distributed DoS tool / Downloading trojan
Registers: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\
Platform: all windows, together with IRC software.

Botnet Role in Information Warfare

Botnet or army of high speed bots can be effectively used to quietly maintain the capability of high value DDoS attack & to launch coordinated network attacks

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

at any desired time as directed by control master through attacker. "Cable bots " phrase used in hacker community to describe bots installed on compromised hosts connected to internet via high speed broadband links acting like zombies waiting for a trigger from its controller, provide attacker large cumulative bandwidth to exploit & deny access to adversary's computer based services. In a corporate or government espionage scenario, one can envision an attacker silently gathering proprietary information over a long period completely unnoticed.

Defending Against Bots & Botnet

Defense against bots infection & attack could be classified in three stages prevention, detection & response as explained by Jim Jones in his paper on " *Botnet: Detection and Mitigation* " [FEDCIRC] and following section explains the same from the perspective of home user & sys-admin, details of each stage follows

- *Prevention stage*: recommends the measures a user or admin could take to prevent their system or network from bots infection. This stage outlines the preventive measures the home user and sys-admin could implement against bots infection.
- *Detection stage*: the measures user and sys-admin could employ to identify a malicious bots activity on machine or in network. It outlines general guidelines that could be used to observe & verify suspected malicious bots activity.
- *Response stage*: recommends the action that home user, sys-admin could take in response to bots infecting machine or network.

Home User: prevention

- General awareness about online security & privacy is must for all online users. High level of user awareness is best course in preventing malicious bots from infecting computers.
- As described earlier most prevalent way of infection by malicious bots is compromising the host by exploiting the known vulnerability in OS or installed applications. Following vendor guidelines regarding safe use, patch & updates for installed OS & application could act as first & most critical line of defense and prevent system from being compromised in the first place.
- Refer to web resources like cert.org section IV of "Home Network Security" http://www.cert.org/tech_tips/home_networks.html for best practice for home users.
- Activate & avail the auto-patch update facility provided with popular OS & applications [CERT, 2001]
- Practice safe handling of common web application like web mail, instant messaging & web browser.
- Use & regularly update anti-virus software.
- Bots available on net for different OS are configurable & could be manipulated to evade anti-virus detection, thus for more comprehensive

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

defense strategy deployment of personal firewall on “always on “host with broadband connection to internet is recommended.

Home User: detection

- The default port for IRC service is TCP port 6667 as mentioned in the previous sections & same may be checked on Microsoft windows OS machine by

  C:/windows> netstat –an

  And output of

  TCP your.machine.ip remote.irc.server.ip :6667 ESTABLISHED

  could indicate malicious traffic if there is no IRC client installed & activated by the user. Many IRC servers also listen on tcp port range of 6000-7000. [COMMODON]

  But it should be kept in mind that as discussed before various bots could be configured to use other TCP ports.
- Slow network response, unexpectedly high volumes of traffic, traffic on unusual ports, and unusual system behavior could indicate towards presence of malicious software including bots.
- Anti-virus software is able to detect & respond to known type of bots.
- Online resource for scanning your system may be employed like Symantec online security checker- will scan the system for open common trojan ports [SYMANTEC]

Home User: response

- The user should disconnect any compromised machine from both the internet and any local network as soon as the user realizes it's been compromised. This helps limit the potential damage both to user’s own systems (remote attackers can no longer gain access) and to other systems on the internet (user’s machine cannot be used to attack others). It's important to physically disconnect the machine from the network.
- Update anti-virus software; check your OS & application vendor site for latest patches. The attacker could have used some new vulnerability to compromise the system. [CERT. 2001]
- An anti-trojan tool may be required if updated anti-virus is not able to detect & remove the infected file.
- If the user stores bank or credit card details on PC, the user should immediately inform the appropriate organization.
- Any password or secure data stored or used on PC should be assumed to have been compromised and changed at once. This includes ISP access passwords, FTP, email and website passwords as well as any other service used, which requires a secure login.
- If unresolved, contact technical support personal with details of problem.

Sys-Admin: prevention

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- General awareness about online security & privacy is must for all online users. High level of user awareness is best course in preventing malicious bots from infecting computers.
- Follow vendor guidelines regarding safe use, patch & updates for installed OS & application.
- Remain informed of latest vulnerabilities by referring to web resources like cert.org & sans.org, subscribe to bugtraq mailing list.
- Activate & avail the auto-patch update facility provided with popular OS & applications.
- Practice & implement safe handling of common web applications like mail services, instant messaging & web browser.
- Use & regularly update anti-virus software.
- Implement access control measures & regularly monitor the generated logs.

Sys-Admin: detection

- In addition to detection techniques used by home user on host itself sys-admins could employ network based techniques.
- Regularly monitor logs generated by perimeter defense devices & analyze the internet traffic for anomalies. [FEDCIRC]
- High network latency or volumes of traffic, traffic on unusual ports and unusual system behavior could indicate presence of malicious software including bots in network. Use network packet sniffer to identity the subnet/machine generating malicious traffic. Both network & host based techniques could be used to confirm the presence of bots. Packet sniffer could help in determining the extend to infection in network, once identified, control the spread of bots by isolating the malicious network subnet, use Windows command line utility like 'netstat' to verify IRC activity on host and 'fport' available at http://www.foundstone.com/knowledge/proddesc/fport.html to map tcp connection established on system to program making that connection. [Dave Dittrich]
- Analysis the logs generated by network sniffer could be used for finding the IRC server used, name of attacker's private channel, authentication key if the communication is in clear text & not encrypted
- Scan individual identified machine for presence of malware like bots itself and other installed backdoors.
- Detail analysis & procedure for detection of bots activity in network subnet could be referred from
  - Dave Dittrich, University of Washington
    - "Dissecting Distributed Malware Networks "
      url: http://security.isu.edu/ppt/pdfppt/Core02.pdf
    - Security Incidents: World-wide distributed DoS and "warez" bot networks (fwd)::Security focus mailing list Date: May 03 2002
      url: http://lists.insecure.org/lists/incidents/2002/May/0026.html

Sys-Admin: response

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- In addition to response measures suggested for home user, sys-admins could initiate action to control the spread of bots, like by isolating the malicious network subnet.
- [FEDCIRC] Preserve the data on the affected system and relevant system logs like Firewalls, Mail servers, IDS, DHCP server, proxy.
- Assess extend of infection by identifying the number of machines infected with bots in subnet, through data collected via network packet sniffer.
- Contact your computer incident response team.

Trends

Use of IRC networks to control zombie machines has seen an emergence of new generation of DDoS tools and new trends in their application. In their paper [CERT, DOS_TRENDS] "*Trends in Denial of Service Attack Technology*" George M. Weaver & Kevin J. Houle from CERT® Coordination Center outline the impact of Internet Relay Chat (IRC) network on attackers ability to manage & control large army of bots. Here are some of the major points.

Survivability – A major consideration for attackers, who would like to evade detection & maintain access to compromised and bots infected systems for as long as possible. Internet Relay Chat protocol being a popular & widely used service, bots on infected system establish an outbound connection to attacker IRC channel using legitimate IRC network service port, thereby leaving their communication undetected by simple network port scanners. Large public IRC networks are used by attackers to host these botnets and use service providers like dyndns.com & no-ip.com to dynamically map bots to multiple IRC severs. Discovery of a single bots infected machine may lead no further than the identification of one or more IRC servers and channel names used by the attacker, enabling them to maintain access to their botnets even when they are banned from that IRC service provider network. Thus, IRC based botnets are difficult to trace & take down, than traditional DoS network models.

Infection & Propagation—from attackers scanning each victim machine for vulnerability & exploiting the hole to install bots, has given way to sophisticated, deliberate, well directed worms that automatically scan, exploit and infect the target network subnet using latest remote exploits for popular end user windows operating system. The trends are towards large scale infection or attempts to infect when a new remote exploit becomes publicly available.

Use -- there is growing practice of using bots infected machines in addition to DDoS network, as part of file sharing network over IRC channels for distributing pirated intellectual property which may include movies, mp3, software and warez, with possible civil/criminal ramifications for end users, associated with hosting and therefore having control or possession over pirated intellectual property, willingly or otherwise.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Conclusion

There have been limited developments in DoS methodologies (ICMP flood, UDP flood, stream of TCP requests) but the technologies related to propagation & management of these attacks have evolved over time. The IRC network model has provided attackers, with very limited knowledge of underlying technologies, to edit readily available known bots to create large botnets that are scalable, automated but equally dangerous with old DoS flooding algorithms. With time to exploit becoming shorter and automation of bots propagation & infection becoming common, is leading to rise in both blind targeting & selective targeting of specially Windows end-users, with high speed, highly available hosts on internet. IRC-based trojans and similar tools are gaining popularity, bots infected hosts & DDoS networks operated via botnets are creating new challenges for the internet.

Proactive defense lies in raising the awareness towards internet security & privacy issues for end users, following the best practices for managing & using online host, thereby preventing the systems to be infected in the first instance. Reactive abilities include using a packet sniffer, monitoring firewall, reverse engineering the trojan binaries, scripts and configuration files. However, none of these, in isolation are effective. The diligent, informed & responsible online users are the most real & effective defense against such attacks.

List of References

[CERT, 2001] Author(s): Jeff Carpenter, Chad Dougherty, Shawn Hernan
CERT® Advisory CA-2001-20
"*Continuing Threats to Home Users"* Original release",
July 20, 2001
URL: http://www.cert.org/advisories/CA-2001-20.html

[AuCERT] Australian CERT advisory reference--AA-2002.03
(File-Sharing Activity Part 2 of 2) –
"*Increased intruder attacks against servers to expand illegal file sharing networks* ", 20 May 2002
URL: http://www.auscert.org.au/render.html?it=2229&cid=1

[FEDCIRC] Jones, Jim. FEDCIRC
"*BotNets: Detection and Mitigation",* February 2003
URL: http://www.fedcirc.gov/library/documents/botNetsv32.doc

[CERT DOS_TRENDS]
Kevin J. Houle, George M. Weaver, in collaboration with:
Neil Long, Rob Thomas. CERT® Coordination Center
"*Trends in Denial of Service Attack Technology* "v1.0,
October 2001
URL:http://www.cert.org/archive/pdf/DoS_trends.pdf

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[Dave Dittrich] Dittrich, Dave. University of Washington
"*Dissecting Distributed Malware Networks* "
URL: http://security.isu.edu/ppt/pdfppt/Core02.pdf

[INSECURE] Dittrich, Dave. University of Washington,
insecure.org mailing list
Security Incidents: World-wide distributed DoS and "warez" bot networks (fwd): May 03 2002
URL: http://lists.insecure.org/lists/incidents/2002/May/0026.html

[ZDNET] Leibhan, Rachel, "*Chat 'bots' may be hacker tool*"
ZDNet Australia
May 10, 2002, 10:55 BST
URL: http://news.zdnet.co.uk/story/0,,t269-s2109962,00.html

[IRC RFC] Contributors: Matthew Green, Michael Neumayer, Volker Paulsen, Kurt Roeckx, Vesa Ruokonen, Magnus Tjernstrom, Stefan Zehl
Internet Relay Chat: Architecture Request for Comments: 2810
April 2000
URL: http://www.irchelp.org/irchelp/rfc/rfc2810.txt

[MIRC] Vonck, Tjerk.
IRC FAQ., *"Introduction to IRC for people using Windows"*
URL: http://www.mirc.com/ircintro.html

[DALNET] *"Just What Is a Botnet?" By Curve*
January, 2003 Issue
URL: http://zine.dal.net/previousissues/issue22/botnet.php

[CNET] Vamosi, Robert, Associate editor, CNET Software
"Pirated movies now playing on a server near you",
5 August 2002
URL: http://reviews.cnet.com/4520-3513_7-5021079-1.html

[NETSYS] URL: http://www.netsys.com/library/papers/DDoS-ircbot.txt

[NDNN] Posted by "tj"
"*Dangers in BotNets?"*
February 22, 2003
URL: http://www.ndnn.org/blog/archives/2003_02.html

[COMMODON] "*How do I detect them?"* By 'mynetstat'
URL: http://www.commodon.com/threat/threat-detect.htm

[SYMANTEC] Symantec security check

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

URL: http://security.symantec.com/sscv6/home.asp?j=1&langid=ie&venid=sym&plfid=23&pkj=BINJESLHFEPGEVVSDUX.
CERT® Coordination Center
"Home Network Security"
June 22, 2001 Initial Release
URL: http://www.cert.org/tech_tips/home_networks.html

"Trojan list sorted on action"
URL: http://www.simovits.com/trojans/trojans_action.html

GT Bot (*Global Threat*)
URL: http://swatit.org/bots/gtbot.html

© SANS Institute 2003, Author retains full rights

Last Updated: June 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**