How the botnet works

One of the most effective and popular DDoS attacks today is based on hundreds of computers being hijacked (ie zombies). These zombies are often controlled and managed through IRC networks, which are used to call them

One of the most effective and popular DDoS attacks today is based on hundreds of computers being hijacked (ie zombies). These zombies are often controlled and managed through IRC networks, using so-called botnets. In this article we will look at some ways hackers can use to attack and hijack target computers, and some effective countermeasures to protect computers against dangerous threats. always lurking around.

We will learn about :

• How are bot and botnet; how they work.
• The most common components in bots.
• How a host can be attacked and hijacked.
• Effective preventive measures and how to deal with their destructive activities.

What should you know?

• How malware works (malware) such as trojans, worms, .
• Mechanism used in DDoS attack type.
• Understand the basic concepts of TCP / IP, DNS and IRC.

' ***How the robot wars - Botnet works*** ', is the name of a hacker world (**Robot Wars - How Botnets Work** , author *Massimiliano Romano* , *Simone Rosignoli* , *Ennio Giannini*).

At the end of the 19th century as well as the beginning of the millennium, the rapid development of a number of different attack strategies aimed at the network was marked. DDoS, ie Distributed Denial of Services, the notorious distributed distributed denial of service form was born. Similar to the DoS brother (denial of service attack), DDoS is widely distributed, mainly due to their simplicity but very difficult to detect. There has been a lot of shared coping experience, with a small amount of knowledge about it, but today DDoS is still a serious threat, a dangerous tool of hackers. Let's learn about DDoS and its legacy product: botnet attacks.

Introducing Bot and Botnet

Bot stands for *robots* , ie automation programs (rather than robotics as we still call them) that are frequently used in the Internet world. It is defined that the spider used by online search engines, website mapping and software that meets IRC requirements (like eggdrop) is a robot. Programs that automatically respond to events outside the internal network are also called robots. In this article, we will be interested in a specific type of robot (or bot as the commonly called short name) IRC bot. IRC bot uses IRC networks as a communication channel to receive commands from remote users. For example, the user is an attacker, and the bot is a Trojan horse. A good

programmer can easily create some of his own bots, or rebuild from available bots. They can easily hide before basic security systems, then spread quickly in a short time.

IRC

IRC is the short name for *Internet Relay Chat* . It is a protocol designed for communication in the form of real-time chat mode (eg RFC 1459, RFC updates 2810, 2811, 2812, 2813) based on the client-server architecture. Most IRC servers allow free access, regardless of the user. IRC is an open network protocol based on TCP (*Transmission Control Protocol*), sometimes enhanced with SSL (*Secure Sockets Layer*).

An IRC server connects to another IRC server in the same network. IRC users can contact both in public (on channels) or private (one-on-one) forms. There are two basic access levels to the IRC channel: user level (operator) and operator level (operator). Users who create a private channel will become moderators. A moderator has more privileges (depending on the type of mode set up by the original operator) compared to the regular user.

IRC bots are treated as a normal user (or operator). They are daemon processes, which can run some operations automatically. The process of controlling these bots is usually based on sending commands to establish a communication channel implemented by the hacker, with the main purpose being vandalism. Of course, bot administration also requires authentication and licensing mechanisms. Therefore, only owners can use them.

An important component of these bots are events that they can use to spread quickly to other computers. Building a careful plan for an attack program will help get better results in shorter time (such as invading more computers). Some *n* bots connect to a single channel waiting for commands from an attacker called a botnet.

Not long ago, *zombie* networks (another name of a bot being hacked) were often controlled through proprietary tools developed by deliberate hackers themselves. Over time, they are aimed at remote control. IRC is considered to be the best tool for launching attacks thanks to its flexibility, ease of use, and especially common servers that can be used as a means of communication. IRC provides a simple way to control hundreds and even thousands of bots simultaneously. It also allows an attacker to cover up his true identity with some simple tricks like using anonymous proxies or forging IP addresses. But it is because of this that they leave traces for server administrators to follow.

In most cases of bot attacks, victims are primarily single computer users, university servers or small business networks. The reason is because computers in these places are not closely monitored and often leave the network protection layer completely blank. These user objects often do not build their own security policies, or if they are not complete, only locally in some parts. Most personal computer users who connect ADSL lines are not aware of the dangers around them and do not use security software such as personal antivirus or firewall tools.

Bot and their applications

The ability to use bots and their applications for computers that are hijacked completely depends on the attacker's creativity and skills. Let's see some of the most popular applications.

DDoS

Botnets are frequently used in *Distributed Denial of Service* (DDoS) attacks. An attacker can control a large number of computers with remote control at a remote station, exploit their bandwidth and send a connection

request to the destination machine. Many networks become very bad after suffering these attacks. And in some cases, the culprit is found as soon as the vandalism is in progress (as in the dotcom war).

Distributed Denial of Service (DDoS) attacks

DDoS attack is a variant of Foolding DoS (Denial of service overflow). The purpose of this form is to cause the network to overflow, using all possible bandwidth. The attacker will then have all the huge bandwidth on the network to overflow the target website. That is the best way to launch attacks to put multiple computers under control. Each computer will provide its own bandwidth (for example, for personal PC users connecting ADSL). All will be used once, and therefore, disperse the attack on the destination website. One of the most common types of attacks is done through the use of TCP protocol (a connection-oriented protocol), called *syn* TCP *flooding* . Their behavior is to send at the same time a huge number of requests for TCP connection to a Web Server (or any other service), overflowing server resources, resulting in bandwidth overflow and blocking Let other users open their own connection. The result is simple but really dangerous! The results are similar when using UDP protocol (a connectionless protocol).

The hackers also spend a lot of time and effort to invest to improve their attack methods. Today, computer network users like us are facing far more sophisticated techniques than traditional DDoS attacks. These techniques allow an attacker to control an extremely large number of hijacked computers (zombies) at a remote station that simply needs to use the IRC protocol.

Spamming (spam spread)

Botnet is an ideal tool for spammers (spammers). They have been and will be used both to exchange collected e-mail addresses and to control spam delivery mechanisms in the same way as DDoS attacks. Spam is sent to the botnet, then distributed through bots and from there spread to the computer being hijacked. All spammers take anonymity and all the consequences are computer damage.

Sniffing and Keylogging

The bots can also be used effectively to enhance the classical art of sniffing. If you monitor the amount of data transmitted, you can determine the incredible number of information transmitted. It could be a user's habits, TCP packet payloads and some other interesting information (such as passwords, user names). The same is true for keylogging, a form of collecting all the information on the keyboard when the user types in the computer (e-mail, password, bank data, PayPal account, etc.).

Stealing identity

The methods mentioned above allow an attacker to control a botnet to collect a huge amount of personal information. Data can be used to build fake identities, then take advantage to be able to access personal accounts or perform many other activities (possibly preparing for many other attacks) that people bear the consequences no one else is the owner of the information.

Possession of illegal software

This is the final form, but not the end. Computers that are bot-type attacks can be used as dynamic archives of illegal documents (pirated software, pornographic images, etc.). Data is stored on the hard drive while ADSL users are unaware.

There are many, many other types of applications developed based on botnets (such as paying for each click to use a program, phishing, hijacking HTTP / HTTPS connection .), but all are listed. It will probably take hours. The bot itself is just a tool with the ability to easily assemble and adapt to all activities that require placing single control on a large number of computers.

Different types of bots

Many types of bots have been built and allow downloads to be available across the Internet. Each type has its own special components. We will look at some of the most popular bots and discuss their main components and distinguishing factors.

GT-Bot

All GT (*Global Threat*) bots are based on the popular IRC client type for Windows called mIRC. The core of these bots is to build the mIRC script (script), which is used to control the operation of the remote system. This bot launches an advanced client session with control scripts and uses a second application, usually HideWindows to hide mIRC from the target computer user. An additional DLL will add some new components to mIRC so that scripts can dominate many different aspects of the computer being hijacked.

Agobot

Agobot is one of the most popular bot types used by professional crackers (craker). They are written in C ++ language and released as GPL license. Interesting point in Agobot is the source code. Being highly modularized, Agobot allows adding new functions easily. It also provides many hidden mechanisms on user computers. The main components of Agobot include: NTFS *Alternate Data Stream* , NTFS *Killer* , and *Polymorphic Encryptor Engine* . Agobot provides sorting and sniffing capabilities. Protocols other than IRC can also be used to control this type of bot.

DSNX

Dataspy Network X (DSNX) is also written in the C ++ language and source code based on GPL copyright. In this type of bot has a new feature is a simple plug-in architecture.

SDBot

SDBot is written in C language and also uses GPL copyright. Unlike Agobot, the source code of this bot is very clear and the software itself has a limited amount of functionality. But SDBot is very popular and has been developed into many different variants.

Elements of an attack

Figure 1 shows the structure of a typical botnet:

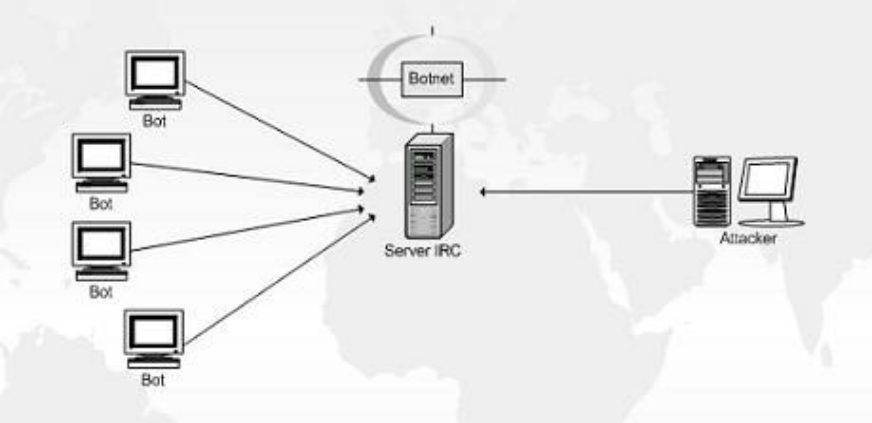


Figure 1 : Structure of a typical botnet

• First, an attacker will spread trojan horse to many different computers. These computers become zombies (the computer is hijacked) and connect to the IRC server to hear more commands coming up.

• The IRC server can be a public machine on one of the IRC networks, but it can also be a dedicated machine installed by an attacker on one of the hijacked machines.

• The bots running on the computer are hijacked, forming a botnet.

A specific example

The attacker's activity can be divided into four different stages:

1. Create
2. Configuration
3. Attack
4. Control

The *Create* phase depends heavily on the attacker's skills and demands. If they are professional hackers, they may consider writing their own bot code or simply expanding it, customizing the existing one. The amount of bot available is very large and its configuration is high. Some also allow for easier operation via a graphical interface. This stage is not difficult, usually for those new to the profession.

The *Configuration* stage is to provide IRC server and information channel. Once installed on a controlled computer, the bot will connect to the selected host. The attacker first enters the required data to limit bot access, secure the channel and ultimately provides a list of licensed users (who can control the bot). At this stage, the bot can be further modified, such as defining attack methods and destinations.

The *Attack* phase is to use a variety of techniques to spread bots, both directly and indirectly. Direct forms may be exploiting vulnerabilities of operating systems or services. Also indirectly is to deploy some other software for dark work, such as using deformed HTML file to exploit Internet Explorer vulnerability, using some other malicious software distributed through horizontal networks row or through exchange of DCC (*Direct Client-to-Client*) file on IRC. Direct attacks are usually done automatically through worms (worms). All the work these worms have to do is find the subnet of the vulnerable system and insert the bot code. Each compromised system

will then continue to execute the attack program, allowing the attacker to record the previously used resource and gain plenty of time to search for another victim.

The mechanism used to distribute bots is one of the main reasons for causing so-called Internet *background noise* . Some main ports are used for Windows, namely Windows 2000, XP SP1 (see Table 1). They seem to be the target of hackers' favorite, because it is easy to find a Windows computer that has not been fully patched or does not install firewall software. This case is also very popular with home computer users and small businesses, which often ignore security issues and always connect to broadband Internet.

Service Port 42 WINS (Host Name Server) 80 HTTP (IIS or Apache vulnerability) 135 RPC (Remote Procedure Call) 137 NetBIOS Name Service 139 NetBIOS Session Service 445 Microsoft – DS – Service 1025 Windows Messenger 1433 Microsoft – SQL – Server 2745 Bagle backdoor worm 3127 MyDoom backdoor worm 3306 MySQL UDF (User Definable Functions) 5000 UPnP (Universal Plug and Play)

Table 1 : List of ports associated with service vulnerabilities

The *Control* Stage consists of several operations performed after the bot has been installed on the target machine in a selected folder. To boot with Windows, bot updates the registry keys, typically HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun . The first thing the bot does after being successfully installed is to connect to an IRC server and link to the control channel using a password. Random nickname on IRC. The bot is then ready to wait for commands from the master application. The attacker must also use a password to connect to the botnet. This is necessary so no one else can use the provided botnet.

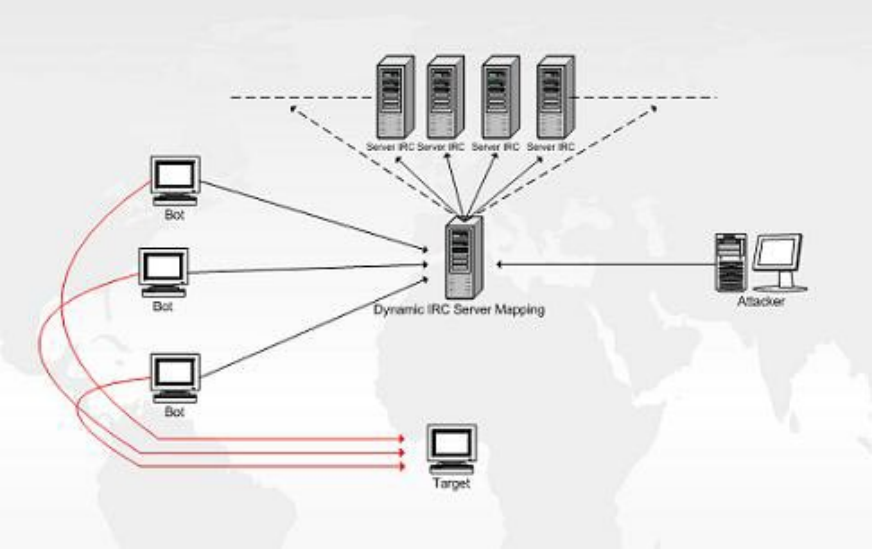


Figure 2 : Hardening botnet technique

IRC not only provides a means to control hundreds of bots, but also allows attackers to use various techniques to hide their true identities. That makes dealing with attacks difficult. But fortunately, due to their natural characteristics, botnets always generate suspicious traffic, facilitating easy detection by a number of known models or models. That helps IRC administrators detect and intervene in a timely manner, allowing them to remove botnets and unnecessary abuse on their systems.

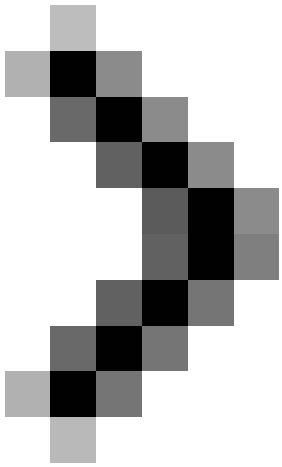
Before this situation, attackers were forced to think of another way, improving the C&C (*Control and Command*) technique into a hardening botnet. In this new technique, bots are usually configured to connect to multiple servers, using a dynamic mapping hostname. As a result, the attacker can easily switch the bot to the new server, still completely in control even if the bot has been detected. Dynamic DNS services like dyndns.com or no-IP.com are often used in this type of attack.

Dynamic DNS

A dynamic DNS (like RFC 2136) is a domain linking system with dynamic IP addresses. Users connecting to the Internet via modem, ADSL or cable usually do not have a fixed IP address. When a user object connects to the Internet, the network service provider (ISP) assigns an unused IP address taken from the selected area. This address is usually left untouched until the user stops using that connection.

This mechanism helps network service providers (ISPs) make the most of the ability to exploit IP addresses, but hinder the audience who needs to perform certain services over the Internet for a long time. , but not using a static IP address. To solve this problem, dynamic DNS was released. The provider will create a dedicated program service, send signals to the DNS database each time the user's IP address changes.

To hide the operation, the configured IRC channel limits access and hide operations. Typical IRC models for botnet channels are: + k (requires entering a password when using the channel); + s (not shown on the list of public channels); + u (only the operator is displayed on the user list); + m (only users with + v audio status can send messages to the channel). Most attackers use personal IRC servers, encrypting all communications on the channel. They also tend to use more personalized variants of the IRC server software, configured to listen on standard external ports and use the edited version of the protocol, to a regular IRC client Can connect to the network.



How the botnet works (Last part)

You finished reading the article "**How the botnet works**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
