Impacts, threats and incidents caused by Botnets

Christian Matthias Fulz
University of Applied Sciences, Ingolstadt
olz1983@gmail.com
Matthias.Fulz@kaspersky.de

October 29, 2009
This Paper will give an introduction to what botnets are, how they are controlled and why it is important to keep an eye on the development of botnets.

It will go deeper into detail as to what security issues are exploited in spreading the bots over the world, what kinds of Command & Control-Servers there are to control the bots, and it will explain some scenarios in the way botnets are used.

Furthermore, the paper will introduce the most popular botnets and some impacts and incidents that were caused by them. It will also describe details of the malware-tools responsible for this efficiency, and take a look at what directions the trends could be heading in the future.
# Contents

1 Introduction .......................... 4  
   1.1 What a botnet is. .......................... 4  
   1.2 Controlling the botnet. .......................... 4  
   1.3 Why botnets are so dangerous. .......................... 4  

2 Details of botnets .......................... 6  
   2.1 Spreading the bots .......................... 6  
      2.1.1 Emails. .......................... 6  
      2.1.2 Downloads .......................... 6  
      2.1.3 Exploits. .......................... 6  
      2.1.4 Manual installation. .......................... 6  
   2.2 Administration of botnets. .......................... 6  
      2.2.1 Internet Relay Chat (IRC) .......................... 7  
      2.2.2 Instant Messaging (IM) .......................... 7  
      2.2.3 WEB (HTTP, HTTPS, etc.) .......................... 7  
      2.2.4 Decentralized / Peer-to-Peer (P2P). .......................... 8  
   2.3 Usage of botnets .......................... 8  
      2.3.1 Spam .......................... 8  
      2.3.2 Cyber-Extortion .......................... 8  
      2.3.3 Anonymous Internet-Connections. .......................... 9  
      2.3.4 Illegal file transfers. .......................... 9  
      2.3.5 Sniffing traffic .......................... 9  
      2.3.6 Key-logging. .......................... 9  
      2.3.7 Brute-forcing .......................... 9  
      2.3.8 Other .......................... 9  

3 Some known botnets .......................... 10  
   3.1 History of botnets .......................... 10  
   3.2 The Storm-Bot .......................... 10  
      3.2.1 Some details of the Storm-Bot .......................... 10  
   3.3 Conficker .......................... 11  
      3.3.1 Some details of Conficker .......................... 11  
   3.4 A short look into the future. .......................... 11  
   3.5 Conclusion .......................... 11
1 Introduction

1.1 What a botnet is

A botnet is a network built from hijacked computers, also called zombies or bots. The owners of the captured systems are normally unaware of this situation, and the computer's network/local resources and also the local files used remotely by the crackers for their own aims, which have the control over the botnet.

Generally the hijacked systems will connect automatically to a so-called Command- and Control-Server, which is used to send the orders to the single computers in the botnet.

1.2 Controlling the botnet

The malware which is installed on the bots to take control of them needs to be able to direct a connection to the Command and Control-Server.

This is normally done from the client site (the bot) to the server site (the C&C). This is the usual way to bypass firewalls which are nowadays installed into in every router at home.

The most common ways to connect to C&C-Servers is to use well known protocols such as IRC (Internet Relay Chat) or, more and more, the HTTP protocol (Hypertext Transfer Protocol).

Normally, the connection over the IRC is lasting, and it is not easy to assemble the infrastructure needed to control the botnet. The benefit is that the bots will execute the orders without delay and the operator will receive a response from the zombies immediately.

In comparison to the IRC controlled botnet the HTTP variant is easier to set up as only a web server is needed for the bots to connect to and request their orders as necessary. This type of traffic is also more difficult to realize, as all usual Internet traffic to websites is the same, and that constitutes about 50% of all the traffic worldwide [1].

1.3 Why botnets are so dangerous

There are botnets out there which have many hundreds of thousands of nodes. This is pure power as only a few individuals control them.

Nowadays, nearly everyone has an ADSL-like connection at home with about 40KB/s upstream to the Internet. There is no way to protect critical systems effectively against DdoS attacks initiated from so many zombies simultaneously. In most cases it would be enough to start an attack from a few hundred or few thousand systems in order to bring almost every server down, so that it won't be able to handle incoming connections.

One of the biggest problems is that most users don't even know that their systems are being hacked and are no longer under their own control. There are still many computers connected to the Internet which are not at all well enough protected or secure. Many users don't update their computers or even use an antivirus program.

One big problem from the social perspective is that if there is a big botnet created, the law doesn't allow it to be remotely destroyed again. The Storm botnet was reverse engineered from some hackers

who were able to take control over nodes belonging to the network [2]. The problem is that even if there is such a way to take control over a botnet, and it is possible to remotely delete the Trojans and fix the security hole so the malware can’t be installed again, this would be legally treated the same way as if it were criminal. It would be necessary to contact the owner of the system first and ask for his permission.

2 Details of botnets

2.1 Spreading the bots

Extending the botnet is done by installing the malware program on systems which aren’t connected to the botnet. The goal is to get as many computers under control as possible. The installation of the malware is done without the knowledge of the system's owner and it is important to hide the Trojan and its activity so it will not be discovered.

2.1.1 Emails

One way to install the malware on systems is to send out many spam emails with the program attached to the email, and to let it be executed by the recipient. The emails may even lead to a website in which the Trojan is embedded.

2.1.2 Downloads

The Trojan could be attached to a tool or program which the user wants to download and execute on his system. Mostly these are files which are cracks for programs or games, even dangerous, as many users will even ignore the warnings of anti-virus-programs in such a special situation.

2.1.3 Exploits

Installation of bots is executed by exploiting security holes in the Operating System or programs like Browsers, Email-Clients, Instant-Messengers etc. In most cases, if a malware tool uses this installation path, it is combined with the functionalities of computer-worms so as to spread automatically to other systems.

In some cases the user needs to interact (click on a link of a website) to execute the malware. There are other ways to execute the bots automatically by loading a website (drive-by-infection). Even popular websites are cracked and infected by Trojans.

2.1.4 Manual installation

The bot is installed manually after breaking into a system. This mostly happens on servers, as they have better connections than "home systems", and as they are mostly 24/7 online it is profitable to look for holes in their system security.

2.2 Administration of botnets

There are different ways to control the botnets. This paper will introduce the most common ways used to administer zombies.
2.2.1 Internet Relay Chat (IRC)
This is one of the oldest ways to control the botnet. Every single bot connects to an IRC Server whose address is included in the malware tool. The zombies will receive their orders via a defined IRC Channel.

Advantages
The orders sent to the bots are answered immediately and the botnet administrator receives them without any delays.

Disadvantages
It is not easy setting up an IRC Infrastructure capable of controlling a botnet, and the traffic isn’t so usual nowadays that an administrator can easily accomplish this by.

2.2.2 Instant Messaging (IM)
This variant is nearly the same as the IRC botnet, but it uses common IM Services such as AOL, MSN or ICQ. Such botnets are not very popular as they have many disadvantages (see below).

Advantages
The traffic is used by many (most) users to communicate with other people who are spread throughout the world and connected to and by the Internet. It is therefore very difficult recognizing that the traffic comes from a bot and not from a normal user.

Disadvantages
Every single bot needs its own IM account and these accounts can’t be created automatically by bots as the service provider is normally using something like captchas to disguise the creating of an account.
All bots could share one account to connect to a network and receive orders, but then they need to share the connection time as well, and therefore the whole botnet would react very slow.

2.2.3 WEB (HTTP, HTTPS, etc.)
This is a fast developing type of botnet. The bots connect to a web server and receive their orders. After execution they send back their answers (data) to the web server.

Advantages
This is the most common traffic in the Internet, so it is very hard to accomplish. Also, this traffic is permitted in nearly every company. In comparison to a bot which attempts using protocols like IM or IRC, which are often disallowed in companies, a HTTP bot won’t attract attention.
It doesn’t take a lot to assemble a botnet utilizing the HTTP protocol. This botnet could be controlled via a web interface which is accessible from nearly everywhere in the world with an Internet connection.
This type of botnet can easily bypass each personal firewall. It doesn’t identify (no actual signature etc.) the bot as malware because the tools often utilize Operating System Functions such as Internet Explorer (Windows) to connect to the C&C –server, and such functions are mostly permitted by the personal firewalls.
Disadvantages
The botnet depends on the C&C server, and if the server is localized and deleted by a provider the botnet can’t be controlled anymore. Many botnets use more than one C&C server so they are not dependent to one server. There are even ways to use random domains which are updated from time to time on the botnet, and therefore so the C&C server addresses will be changed in the process.

2.2.4 Decentralized / Peer-to-Peer (P2P)
A decentralized botnet doesn’t need a C&C server as each zombie is connected to a few other bots belonging to the network.
To control such a network the administrator only needs to have access to one bot in the network (he could use his own system and connect it to the botnet). The systems send the received orders to their neighbors.

Advantages
Because there is no need for a C&C server, the botnet is much harder to neutralize and very stable after creation.
Furthermore, the traffic is hard to recognize for home users as many are using different P2P-Networks to exchange files with others (EMule, BitTorrent, etc).

Disadvantages
To develop such a botnet it requires a very detailed knowledge of programming and networks. The biggest problem is that each bots needs the addresses of a few other zombies in order to send the orders to them. In most cases this type of botnet is combined with a C&C server to make the addresses of the bots known to other systems connected to the botnet. This server is normally integrated in the botnet.

2.3 Usage of botnets
Botnets are used for many types of criminal actions, as for example in sending Spam or starting DDoS attacks.

2.3.1 Spam
This seems to be one of the most common usages of botnets. Because broadband -connections nowadays have about 40+KB/s upload, a system is able to send many spam emails in a few hours. The spam emails often do not directly belong to the botnet administrator, as the botnets are often hired to other people for money, who are responsible for the spam emails.
A big advantage in using botnets to send spam emails is that if a system is sending many spam -emails, its address will be added to an email server blacklist and the emails of one will be rejected. By using many different computers with many different addresses this protection can be partially circumvented.
A recent study [1] established that about 87% of all spam emails are sent by botnets (Q3 2009).

2.3.2 Cyber Extortion

Botnets are often used to steal money. Zombies are used to launch a DDoS attack on the servers of companies critical for them. The bots request so many connections to the server until it handles a real connection request from customers of the company. To stop the attack, the criminals demand money and most companies pay it, because this is often cheaper than the downtime of the servers. And because of this situation, and even the damage to the company’s image, they don’t call the police. DDoS attacks can be besides used for political needs, and the targets are often political servers of governmental institutions. This is very dangerous as other countries can use them as a means of provocation.

2.3.3 Anonymous Internet Connections

Botnets can be used for accessing the Internet anonymously. A criminal can use bots to break into other systems and hide the real origin of the attacker.

2.3.4 Illegal file transfers

The botnet could be used for illegal file hosting and/or exchange. Many systems have 500+GB hdds built in, so there is a lot of space for storing files on them. Botnets can be used to host illegal material, such as child pornography spread over many systems and exchanged for money. When such material is hosted on a botnet and found by institutions such as the police, there will only be a few systems out of action as the real origin of the files are hidden behind the botnet.

2.3.5 Sniffing traffic

Botnets can be used to sniff clear text traffic of the captured system, mostly usernames and passwords. If the bot is compromised by another malware and connected to more than one botnet, it could be that this traffic is analyzed in order to steal another botnet or parts of it.

2.3.6 Keylogging

With encrypted data streams such as HTTPS, POP3S etc., many bots can log each user input. Encrypted data cannot be read by sniffing so the passwords, etc. are logged directly from the keyboard of the user. With “intelligent” filters the criminals are able to effectively log the login details. For example, when the bot "tell me all information a few lines before and after paypal.com" runs on thousands of systems, a lot of accounts can be easily harvested.

2.3.7 Brute forcing

Botnets could be used as “supercomputers” to brute force logins or encryption keys. Nowadays, one medium-power system can attempt a few hundred keys/passwords a second depending on what the required brute force. By using many thousands of computers simultaneously, the time needed per single combination can be essentially decreased.

2.3.8 Other

In general there are so many ways to used botnets for criminal actions that only the creativity of the person who wants to use a botnet marks the limit.
3 Some known botnets

3.1 History of botnets[1]

The history of botnets began in 1998 with the first malware tools (NetBus and BackOrifice), which encompassed many functions for controlling infected systems remotely. At this time the infected computers acted as servers and waited for incoming connections. When criminals connected to systems they were able to control nearly every function of the system remotely (depending on the programmed functions of the malware-tools). The infected computer often sent an email to the cracker when it was connected to the Internet with the actual IP-Address of the system.

By 2000 malware was able to control more than one system simultaneously. The next step was to allow the systems to initiate connection to the controller of the bots. The first real botnets used the IRC protocol to be controlled by a C&C server and receive their orders from the cracker. This was at first done by hackers (perhaps just for fun or as proof-of-concepts), but the so-called black hats (crackers) used these ideas to create botnets for illegal profit. The user password protected IRC channels to which the bots were connected and controlled them through special IRC messages.

In a further step, the C&C servers were moved to the Internet and used standard web technologies such as HTTP connections and remote control features that were integrated into the operating system. Web oriented botnets are very popular. They can be controlled by nearly every device (even mobile and smartphones) with an Internet connection.

One of the most dangerous botnet types is the P2P-botnet. Because this type of botnet is independent of centralized C&C servers there is no single point of failure which can be used to destroy the botnet. Crackers used to experiment longer in the past on this type of botnet, but the first real P2P-botnet turned up in 2007, the StormNet.

3.2 The Storm Bot

The Storm botnet is one of the most famous and popular botnets, appearing in 2007. This was a P2P-botnet. No expert was able to find out the real size of the botnet but some estimated that there could have been between 50000 and 10 Million zombies controlled by the criminals that created it.

3.2.1 Some details of the Storm bot

The Storm bot was designed to protect itself against many threats to the network itself. As an example, it had automated functions to attack (DDoS) systems that tried to scan for or delete the malware on other systems that were already infected[2].

Another interesting feature of the Storm worm is that many versions were released in a short space of time. Partially, the developers released hundreds or thousands of variants of the malware each week to overwhelm the Antivirus-Companies by the amount of new versions[3].

Also, the Storm botnet was "fighting back" against security researchers. It was able to find out when someone tried to analyze it by probing it's Command&Control servers and started DDoS attacks against them to bring their Internet access down for days[4].

3.3 Conficker

Another popular P2P-Botnet was assembled on a malware called Conficker. It was so well designed that it was able to even break into systems that belonged to the military.

It spread through the systems using a security hole in the windows systems, which allowed it to run code remotely on the victims' systems. It even used the opportunity to spread itself through using network shares so that it was able to obtain access from an infected system and also exploit the autostart functionality of USB-Sticks or external HDDs.

3.3.1 Some details of Conficker

On January 19 2009, the security company F-Secure reported that about 9 million systems were already infected by the Conficker worm[5].

On February 13 2009, the worm arrived at the German military ("Bundeswehr"), and a few agencies were disconnected from the network[6].

It also reached the French air force and was responsible for a delay in the performance of duties for a few days.[7].

A good analysis of the Conficker worm can be found at: "http://mtc.sri.com/Conficker/".

3.4 A short look into the future

In the future, botnets will become more dangerous than ever. It could be that new devices resources and technologies will be aimed at by malware –developers, such as mobile and smartphones. These types of devices could become attractive zombies. They are nearly 24/7 online as people nowadays (especially business people) need to be always reachable. Also, more and more mobile-devices are getting flat-rates to access the Internet whole the time. Also such small mobile devices have more and more functions built in so that they are nearly the same as a computer in their daily use (emails, calendar, navigation etc.). This type of device is often connected to a computer to synchronize contents, and this could be exploited to spread malware across different systems if the viruses are cross-platform developed.

3.5 Conclusion

This paper discusses some interesting aspects of botnets and gives an perspective as to why botnets are so dangerous. It is very important to help users so they know about the threats which comes from this type of malwares history has proven that when such a botnet already exists it is very hard to destroy it again.