Botnet Future Trend

Amin Hosseinian Far, Hamid Jahankhani, Rouzbeh Ghazihesami

School of Computing, IT & Engineering,
University of East London, UK
danial@fastermail.com, hamid.jahankhani@uel.ac.uk

1School of Engineering & Mathematical Sciences,
City University London, UK

Abstract: Botnets are one of the most dangerous threats on the web. They operate like a distributed network and have two main components: the Botnet (or Zombies) and the Botmaster. Their target is to steal valuable information from business (which constitutes the majority of attacks) as well as individuals. There are four main Botnet topologies: Hierarchical, Multi-server, Star, and Random (or Mesh). The work towards security against Botnets is not mature enough due to the extensive operation of Botnet Trojans and lack of necessary knowledge about them. The lack of a standard approach towards Botnet confrontation as exists in many other Internet threats such as Viruses, Malware, etc. is one of the main problems within the Internet system. Governmental rules and regulations regarding internet use do not exist or are too weak within countries such as China, Russia, and Brazil, which has in turn led to these countries becoming global centers for Botnet administration. This paper aims to review Botnet future trend and why industry-wide standard needs to developed to combat these threats.

1. Introduction

Security is a concept that has steadily grown in importance in recent years as a result of the globalization and mass market economy of the world. This is even more importance in information technology which has had to adapt to rapid changes in the industry and cope with the lessons of several high profile exploits of server and data vulnerabilities with personal, political and commercial repercussions. The image of the hacker before the year 2000 was more about individuals partaking in such activity for fun, excitement and the thrill, competition or the possibility of fame. With the rapid development of the complexity of user interaction with the internet, however, hacking activity has also evolved. Many victims may now lose their credit card information, their emails, and other valuable information which may have adverse financial consequences; though direct financial transactions are not the only method of abuse of personal information, Figure 1. Such security breaches caused by a Botnet attacker or team of attackers will be considered in this paper.

2. Characteristics of the Botnets

Botnet Trojan Horses can be considered as one of the newest threats to the Internet. This type of Trojan was first introduced across the internet in the late 90’s. [1]

The Trojan architecture is highly similar to that of initial Trojans, but their purpose and the way they operate in the network is significantly different from those initial types of attacks, both in intent and in procedure. Botnets can infect a few systems and up to several million computers in a network in order to obtain valuable data regarding individuals and organizations. In one of most recent research works performed by the
Kaspersky lab team it has become clear that targets are normally chosen from businesses and not personal users; though personal computer users can also be affected by Trojans. The general structure of a botnet follows a botmaster that has the responsibility of controlling and managing the infected machines. The machines which are infected will send data to the botmaster by means of machine resources. The action can be easily triggered by a simple click of the user, although research is ongoing about trigger types in Botnet Trojan Horses.

One of the main characteristics of botnets is that they have a very robust infrastructure in the Command and Control-CnC- section. This is another factor that differentiates them from other malware activities. In some other malicious activities the communication between nodes exists, but is dissimilar to Botnet communication.

There are different communication topologies, which we can generally categorize as follows:
1. Star
2. Multi-Server
3. Hierarchical
4. Random

Each presents a mixture of advantages and drawbacks, and each may be used by different attackers.

The main advantage of Star is that it allows for direct communication between the botmaster, the Botnet Trojan, and the agent. It can, however, be easily found and removed by the system administrator. It can be imagined as when each Botnet node is granted access to the main phone line of each network node and tries to communicate directly to the centre, Figure 2.
Compared to Star, the multi-server topology provides a better risk management scheme. In the case of failure in one of the servers, the other servers are able to continue the job. It can also cover a greater geographical area. Different powerful servers in different locations of the world can cover specific number of Botnet nodes. The main drawback is the higher cost and effort of initialization of such a system, Figure 3.
In the hierarchical topology the Botnet server provides greater security due to the management of information through nodes of different levels in place of constant direct centralized communication between all the nodes, and is thus less vulnerable to being dismantled; although there are delays during the command and control procedures due to the natural data transfer structure of the system, Figure 4.

![Hierarchical topology](image)

**Figure 4: Hierarchical topology, source [2]**

The centralized system is removed in this scheme and becomes similar to the Mesh network topology. Each Botnet node communicates directly with other nodes. There are latencies associated with the longer data transfer path, but it is also much more secure and more resistant to being shut down, Figure 5.

![Random topology](image)

**Figure 5: Random topology, Source [2]**
There are a number of known attack types that seems to be favourites in most Botnet attacks. Distributed DoS (Denial of Service) is one the most important ones that has the potential to completely disrupt business activities, given the increasing importance of IT systems in the day to day running of many businesses nowadays. A DoS attack can be identified when exceptionally high levels of activities are posted to the main machines of a network in order to stop them from serving other users. The Botnet systems that comprise many servers distributed throughout the Internet give the idea of a distributed network that has different nodes with each node performing a part of the job by using its machine resources.

Phishing is a technique through which Botnets exploit users. Phishing involves scanning the activity of vulnerable servers in order to be able to steal passwords or other crucial identifying information.

Identity theft is another tactic which Botnets exploit users by stealing their valuable information such as passwords, usernames etc. This information are either used instantly or sold as a batch to third parties.

Finally, Adware are the most important and the main tool most Botnet Trojans employ. They are automatically downloaded by the victim’s machine by many different predefined triggers based on the victim’s machine specifications. There is an ongoing research in the area of trigger types that allow first for Botnets to place themselves into a machine, and then to activate and send information from the victim’s machine.

Threats from Botnets are gaining in publicity and importance as hacking develops into a complex fraud and financial tool, rather than the more basic and passive reasons such as simple excitement it was initially founded upon. Early attacks such thwart has now evolved to more sophisticated attacks. Cyber security is an ongoing war against a variety of attack types and malicious software. Different attackers use different technologies and tactics in order to gain access to a network of computers, to which different Internet security companies similarly employ different security structures, with varying degrees of effectiveness.

Considering 1 million machines infected by the same Botnet Trojan in a very short time of under 10 minutes requires a standardize security features which would protect different individuals and businesses which are using different security software. Even if the nodes are recovered by some Internet security packages, others may still be operable under the control of the Botnet administrator. In terms of Internet laws and regulations, it is also worth noting there is no accepted globally standardized regulation operable by all countries. This then allows attackers to attack different users in specific geographical areas and jurisdictions dependent on local developments in security structure.

3. Proposed solutions for Botnets

A proposal is to standardize Botnet detection strategies within nodes and servers across security companies. When computer viruses were introduced, the anti-virus industry emerged so that dozens of companies currently offer security solutions. The same applies to firewall and anti-spyware software. The sudden emergence of so many security systems has meant that security strategies vary greatly between companies.
There would naturally be difficulties introducing such a system from scratch but the capability of detecting the Botnet codes can be added to many anti-virus systems.

Tracking the servers and the attackers within different geographical areas is also another issue that needs integrated laws and regulation accepted by all countries.

There are several security systems available for monitoring, control, and protection against Botnet Trojans. The analysis shows that the security systems available vary across system traits. Some existing security solutions for Botnets are offered by the following:

- **Engate:** Engatelabs Corporation which is a Security Company has announced that they have come up with a system that stops Botnet activities. The proactive nature of their system is reminiscent of the software agent systems that had autonomicity in performing tasks towards their target. [4] It should be a challenging system development process as weak performance by the system may collapse the normal activities of the business network.

- **Messagelabs:** The Messagelabs Corporation suggests various techniques in order to protect businesses and individuals from Botnet threats. They range from user training modules to completely managed network security systems.[6] The Californian based McColo ISP has recently done a very interesting experiment which gives us a very good understanding of Botnets. As per regular Botnet structures, they set up an IRC server and monitored Botnet activities through their servers. They noticed that there was a substantial number of Botmasters working through their server. They suggested that after diminishing the server’s activity, the Botnet activities will also have to rapidly diminish. Soon after they disabled the server, the Botnet activities on the web decreased substantially, but after a while it gradually began to increase again. The conclusion from this experiment was that Botnet Trojan activities are rising rapidly among current Internet systems and that what we should be worried about is that it would not necessarily be a sufficient security measure to attempt to stop botnet activities by stopping the servers that are responsible for Botnet activities. In the same research, it was found that the source of most of the attacks were generally from countries such as Russia, Brazil and China. The suggestion here being that the solution may very well lie in encouraging the liable systems within these countries to act against such activities in order to limit their impact on the web structure. Standardization of Internet laws has the potential to consolidate such measures and make it significantly more difficult for criminals to bypass global measures by proxy of local deficiencies.

**Conclusion**

Botnet attacks are currently escalating and the severity of the attacks is at its worst. The work done in the area of security against and removal of, Botnet Trojans has not been sufficient and each company continues to head towards their own discrete strategies. The proposal here is to consolidate technical strategies used against Botnet Trojans by developing an industry-wide standard. Changes in laws and regulations in certain jurisdictions would therefore be needed in order to allow for an effective front to minimize the harm caused by web criminals.
Given that some of the most notorious internet wide viruses and Trojans, such as the Blaster worm (which was developed by an 18 year old) and the Netsky and Sasser (also developed by an 18 year old) worms, were created by teenagers rather than gangs of organized professional coders, it is evident that education is an area that needs to be addressed with regards to web security and its implications for business as well as individuals.

References


