A Literature Survey About Recent Botnet Trends

GÉANT 3 JRA2 T4: Internal deliverable
Emre YÜCE
ULAKBİM, Turkey
emre@ulakbim.gov.tr

June 19, 2011

Abstract

Today botnets are seen to be one of the main sources of malicious activity. Rapidly growing botnets find new methods for spreading malicious codes and launching attacks. The main goal of this document is to give a brief information about the latest botnet trends which include botnet architectures used, botnet attacks and latest botnet behaviours.

1 Introduction

Botnet is defined as a collection of software "robots" that run on host computers autonomously and automatically, controlled remotely by an attacker or attackers [1]. Botnets are used for malicious activity like distributed denial of service (DDOS) attacks, identity theft, sending spams and phishing attacks.

In the past, the concept of bots did not include harmful behaviour by default. Studying the evolution of bots and botnets provides insight into their capabilities. One of the original uses of computer bots was to assist in Internet Relay Chat (IRC) channel management [2]. IRC is a chat system that provides one-to-one and one-to-many instant messaging over the Internet. Users can join a channel on an IRC network and communicate with

groups of other users. Managing busy channels is a time consuming job, so channel operators created bots to help in management of popular channels. Bots gradually have been developed into a comprehensive tool which operates as an IRC channel operator, e.g. Eggdrop was written in 1993 to assist channel operators. [3] In time IRC bots with malicious purposes appeared. The goal of these bots was to attack other users and servers. These attacks include flooding attacks (i.e. DoS). The bots are used both for hiding the source address of the attack and distributing the attacks (i.e. using multiple bots grouped together).

In order to strengthen the effect of the attack against larger targets, botnet masters needed to increase the number of bots. Since nobody wants to be a part of a botnet willingly, botnet masters had found ways to spread the malicious code. At the beginning, bot infection was not an automated process and needed human interaction such as downloading software that includes a malicious code or opening a malicious software attached e-mail. Today bot infection process has become more automated. For example, SDBot [4] can propagate using techniques such as open file shares, p2p networks, backdoors left by previous worms and exploits of common Windows vulnerabilities such as WEBDAV [5], DCOM RPC [6] and LSASS [7]. Besides, the attack and the communication capabilities of bots have been improved. For example Agobot [8] has a wide range of attack capabilities including DoS attacks, proxy for spam, GRE tunneling and password sniffing.

Outline The remainder of this document is organized as follows. Section 2 investigates commonly used botnet architectures, their advantages and disadvantages. Morover recent botnet trends are presented in this chapter. Section 3 focuses on overview of threats which includes DoS/DDoS attacks, spams, identity theft. Finally, Section 4 gives the conclusions.

2 Botnet Architectures

Botnets are generally characterized with respect to the C&C (command and control) mechanism used for communication. C&C mechanism specifies how the bots retrieve the commands from the botmasters. Botmasters require stealth and speed while sending their commands to the bots. There are many types of C&C mechanism but centralized and P2P botnets are the most commonly seen types whereas hybrid and unstructured C&C mechanisms are

investigated as different approaches.

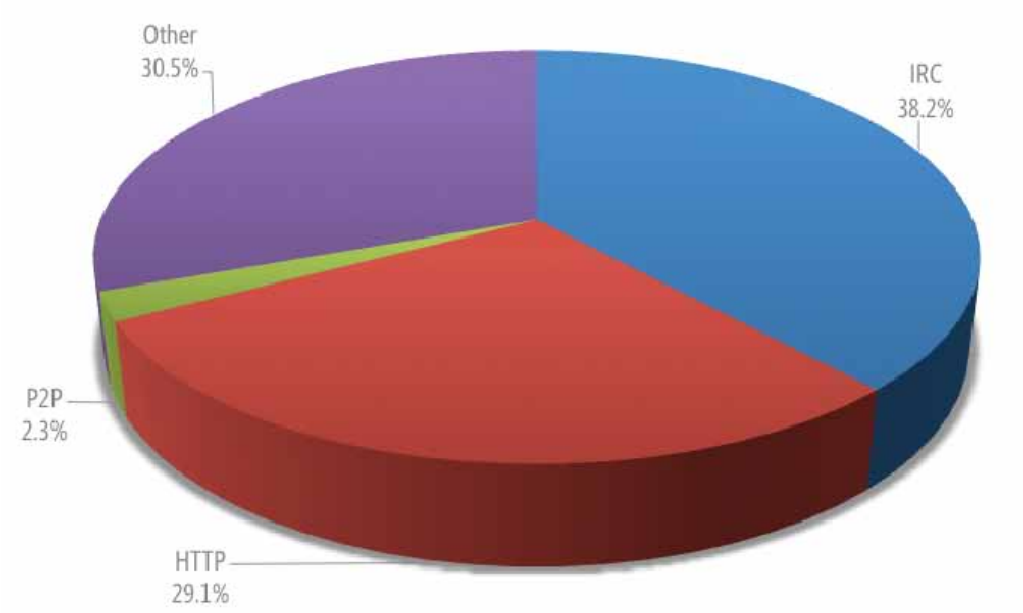

Figure 1: C&C mechanisms used by botnet families in 2Q10 [9]

2.1 Centralized

Centralized C&C architecture is the most commonly used botnet architecture. In this architecture, botmasters use central servers to issue their commands to the selected sets of bots. Bots act as clients where the botnet is built using the client-server scheme. Internet Relay Chat (IRC) and HTTP are the most common protocols used in centralized communication. There are two advantages of using centralized C&C architecture. Firstly, this architecture is based on a client-server scheme which is easy to implement using centralized communication channels. Secondly, latency is a critical measure for highly synchronized tasks, e.g. DDoS attacks. Centralized botnets have low latency as their routing information is clear for each bot and each bot is directly connected to the server.

However centralized networks have its drawbacks for botnet masters too. First disadvantage is about detection. Centralized communication is easier

to detect than non-centralized since bots are using similar traffic patterns for communication. For example, DNS queries may give a clue to detect a centralized botnet. Fast-flux networks are used to hide actual hosts behind the C&C servers. Fast-flux is a technique that allows the attackers to manage an ever-changing mapping between the DNS name and the IP address behind it. Another disadvantage is that if a bot is detected, disrupting the connection of a centralized botnet is easier, e.g. disrupting the communication of central server will lead the whole botnet network to crush.

An example centralized botnet structure is given in Figure 2. Botnet operator controls the bots by injecting the commands to the central server.

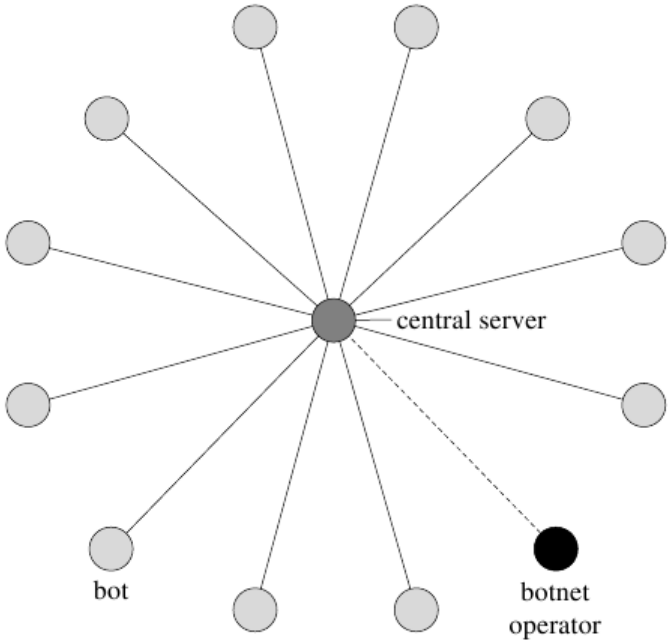

Figure 2: Centralized C&C Structure [10]

2.2 IRC

IRC C&C architecture is most commonly used communication channel in centralized botnets. All bots connect to a single IRC server to listen for

commands. After they establish the connection to the server, they join a specific channel using the standard IRC protocol. All communication works like a normal IRC chat conversation in a language that bots can interpret and process the commands. Botmasters are able to push their commands through these channels. As a result the latency between issuing a command and execution by the bot is very low. Moreover, IRC servers can work together to give access IRC clients for reaching an IRC network via multiple IRC servers. This enables botmasters to handle large number of bots. Another issue using IRC is authentication. When a bot is joining to a channel, botmaster authenticates the bot to keep outsiders from joining the botnet. At the same time, bot authenticates the botmaster to protect bots being overtaken by defenders or other botnet operators.

Commonly known examples of IRC bots may be given as Agobot and SDbot. Agobot is a modular IRC bot for Win32 / Linux which has several thousands of variants. Most of the Agobot variants have the features namely: packet sniffing, keylogging, changing its own code (polymorphic code), installing rootkits, information harvesting (email addresses, software product keys, passwords etc.), and performing DDoS attacks. SDbot, also known as Zobot, is a computer worm which uses security vulnerabilities in Microsoft operating systems and is known to spread on TCP port 445. It is observed that the malware has installed some spyware to the bots it has infected.

2.3 HTTP

HTTP is another popular communication protocol used by botnets. If HTTP is used as communication protocol, botmaster cannot send command its bots immediately, instead, he/she leaves malicious instructions on a web server that bots may later fetch and execute. While using HTTP, bots need to query dedicated web sites regularly for getting new commands. Even if this pull mechanism leads to higher communication latencies, botmasters prefer HTTP since it creates less suspicious traffic for managing bots.

There is another approach which uses malicious web servers to create puppetnets. This approach aims to remotely instruct browsers to orchestrate actions including DoS attacks, worm propagation and reconnaissance scans without directly harming the browser's host machine. It is observed that attackers may create a powerful botnet like activity which may cause significant damage depending on the popularity of the malicious web server

and user browsing behaviours. As seen in Figure 3, web clients connect to a malicious web server and receive attack instructions that redirect them to the victim site.

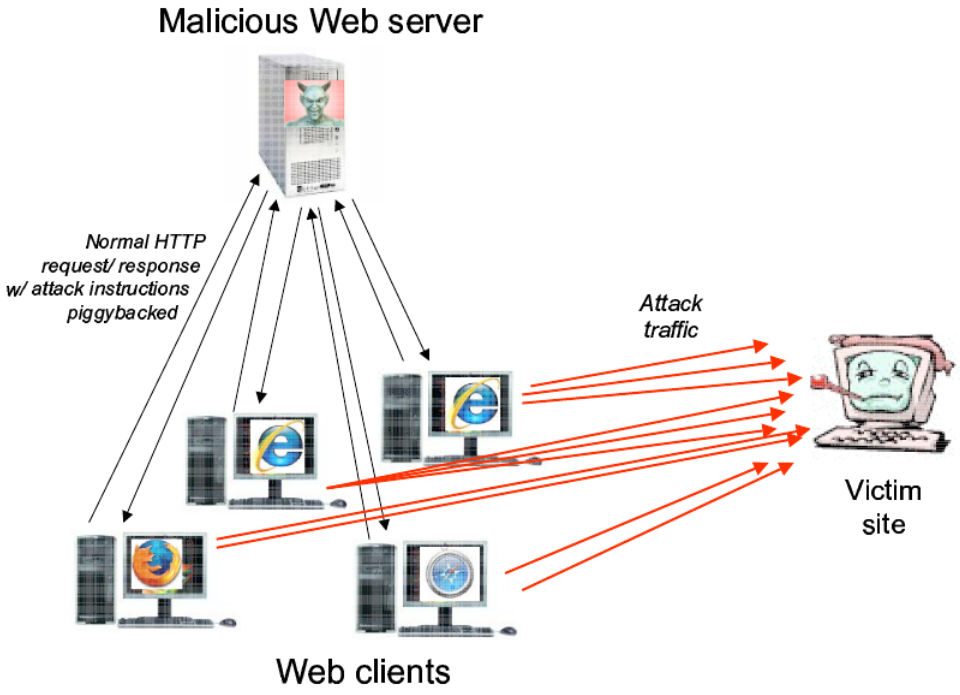

Figure 3: DDoS using puppetnets [11]

Zeus botnet is the most popular botnet using HTTP as the communication protocol. The various Zeus' botnets are estimated to include millions of compromised computers around the world. Zeus botnet uses the Zeus Trojan horse which is spread mainly through drive-by downloads and phishing schemes. Zeus botnet is mainly used to steal critical information including login credentials to email accounts, financial services etc. Since May 2011 source code of Zeus has been leaked. This will led more complex malwares to be produced, e.g. Zeus Trojan may be merged with Spy Eye Trojan.

The bot named Spyeye, which is published in early 2011, is aiming to take over the info stealing business. Moreover, the Spyeye malware has a built in function to Kill the ZeuS botnet and eliminate the competition. The main task of the malware is to steal bank accounts, credit cards, ftp

accounts and other sensitive data from the victim's computer. Just like the ZeuS Trojan, the Spyeye aims to have a stealthy approach and report back to its command/control center.

2.4 P2P

P2P C&C architecture which gained attraction lately, has no central server. Each bot is a peer acting as a server and a client at the same time. Bots connect to each other when they join the botnet. In order to achieve this goal, bots has a list of known peers. Bots try to connect using the list and when a connection established bots exchange their lists to have an improved connectivity.

An example P2P C&C architecture is given in Figure 4. As seen in the figure, the botnet operator acts as a peer which makes the detection of the botnet operator harder.

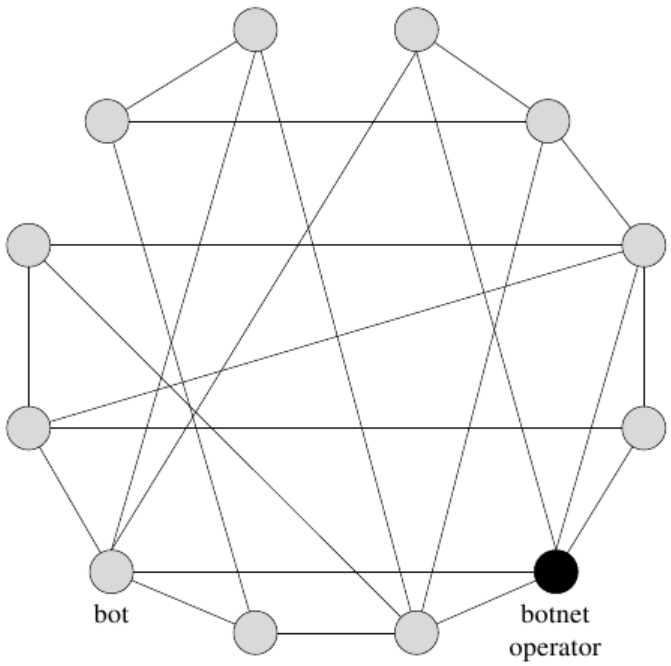

Figure 4: C&C structure in a P2P botnet [10]

P2P botnets are more resilient than centralized botnets. In other words, removing a bot from a P2P botnet hardly affects the communication where botnet totally depends on the server in centralized architecture. Moreover, detection of P2P botnets using traffic analysis is difficult because of its distributed structure. However, when compared to the other architectures, P2P botnets have a higher latency which is the delay between issuing a command and execution of the command by the bots. Also the synchronization of bots is another drawbackin P2P botnets due to this latency.

One of the examples of the P2P botnets is the Storm Botnet. The Storm botnet is a remotely controlled network that has been linked by the Storm Worm, a Trojan horse spread through spam emails. It is estimated that the Storm botnet was running on anywhere from 1 million to 50 million computer systems by September 2007. The Storm botnet's operators control the system via peer-to-peer techniques, making external monitoring and disabling of the system more difficult, since there is no central C&C server in the Storm botnet that can be shut down. Besides, the botnet also makes use of encryption techniques to hide the traffic content from outsiders.

2.5 Current Trends

As seen in the previous sections botnets may be used in a wide area including DDoS attacks, spams, identitiy thefts and click frauds. To be able to deal with these threats one should understand the way how the attackers may improve their malware and hence botnet structures. It is interpreted that P2P botnet architecture is gaining attention because its less detectable and more resilient. Also hybrid models may be used in the future which has the advantages of both centralized and P2P structures. Furthermore, botnets tend to be as specific as possible to the task they are assigned to do: for example, there are spam-only botnets, like Conficker and DDoS-only botnets like the Mariposa botnet, while multipurpose botnets, like the Zeus botnet, are decreasing.

Centralized and P2P botnet architectures both have advantages and disadvantages. In theory, both approaches can be used together in the same topology. This approach has not been seen in the wild yet but there are proposed hybrid structures including subbotnets which communicate using P2P protocols. In that structure all subbotnets are connected to central server through one of the peers. If one of the subbotnets is detected, this will not affect the other subbotnets. However, existence of a central server is again

the disadvantage of this structure.

Another approach takes the P2P concept to the extreme and is based on the principle that every peer knows about only one peer. In this structure when a bot has received a message, it will randomly search the internet and when it finds another peer then it will pass the message to the other bot. This will give less information about the botnet infrastructure however latency will be very high.

Another point is that large botnets will be aggressive in capturing more computers for their kingdom. Botnets will attempt to steal seats from their competition, patching the computers they take over so to defend themselves against other thieves. An example of this situation is seen in the SpyEye botnet interface which has an option namely "Kill Zeus". If this option is selected, Spyeye malware will disinfect the computer from Zeus malware, then it will make the computer join the Spyeye botnet.

Social networks are becoming the command points for botnets. It is known that social networks are used as a spread channel since users trust links and contents coming from social networks. The usage of social networks as a command point is observed in Svelta malware. As seen in the Figure 5, a twitter account, named upd4t3, is used for this purpose and commands/web addresses are sent as tweets from this account in base64 encoded form. The infected bots are the followers of this twitter account and they are programmed to convert base64 encoded tweets into the commands of the server. Furthermore, Twitter is hit by XSS vulnerabilities which enable users to post javascript code in a tweet. Also, bogus Facebook applications are used to steal personal information or make users fill surveys.

Similar to the SETI programs where you can donate some of your computer's processing capacity to search for alien intelligence, some bot nets are becoming opt-in so that you can participate in politically-based botnet activity. One of the example of these groups is Anonymous group which manages approximately 90.000 bots, some of them have been volunteered to be a bot by downloading and executing a file. When the Wikileaks document archive web site is published in 2010, Anonymous has announced its support for Wikileaks and launched DDoS attacks against companies who have an anti-wikileaks behavior.

In addition to these attacks, which require synchronized work and mass activity like DDoS attacks, botnets have been used for stealing critical information. For his purpose small botnets, down to 10 computers, are created and used effectively. These small botnets are harder to detect. Moreover,

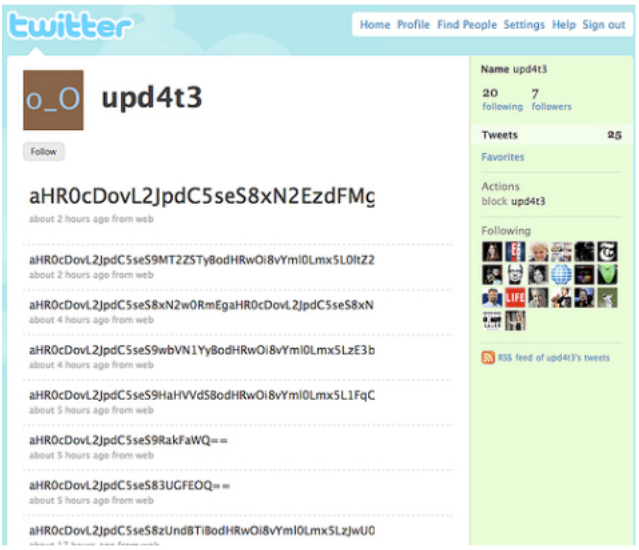

Figure 5: upd4t3 twitter account used to issue commands to bots

rather than using phishing attacks, it is getting common to use malware to capture user credentials while doing banking or other critical activity.

The discovery of Stuxnet in the second half of 2010 gives clues about the evolution of the malware. Stuxnet is a Windows worm targets industrial systems. It is the first kind of worm that includes a programmable logic controller (PLC) rootkit. It's observed that the worm has used four 0-day vulnerability and a vulnerability that had been used by the Conficker worm. The attacks those target industrial systems show that sources other than financial and personal ones, are also under threat.

Last but not least, the mobile device market, including smartphones and tablet PCs, is rapidly growing which makes mobile devices as a new target for attackers. Moreover mobile device users are less careful about updating and securing their devices. A new variant of Zeus malware has been observed that is targeting Nokia phones which use Symbian OS. This malware aims to defeat online banking two-factor authentication by monitoring the SMS sent by the bank. Another example of attack on mobile devices is a rogue application for Android called "Movie Player" which secretly sends SMS messages to a premium rate number, costing the end user several dollars per message. In addition to this application, there are other rogue applications that are

stealing personal information held on the phone. Making the application market approval more restricted is not a very effective solution. Although Apple's iOS platform is a closed system and application approval process for Application Store is restrictive, there are many vulnerabilities discovered for iPhone including the jailbreak vulnerability which removes the restriction on which applications can be installed. It is expected that as smartphone and tablet platform usage grows, the malware targeting mobile platforms will increase.

3 Overview of Threats

Botnets may be used in various criminal activities ranging from DoS/DDoS attacks to stealing confidential data. Botnet operator may rent the botnet or he may use the botnet for his own purposes like spreading malware to extend the botnet or harvest email addresses. Some of the common usage of botnets is discussed throughout this section.

3.1 DoS/DDoS

DoS/DDos attacks are one of the oldest types of botnet activities. A DoS attack or DDoS attack is an attempt to make a computer resource unavailable to its intended users. Although the methods, motives and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. In such an attack bots simultaneously perform actions to bring the target down. Due to large bandwith and source that can be deployed within a botnet, botnets are well feasible for large scale DDoS attacks. These DDos attacks may include exhaustive search queries or HTTP floods, TCP SYN, UDP or ICMP floods.

3.2 Spam

Spam is unsolicited and bulk email sent without the verified permission of the receiver. Delivery failure messages, misdirected messages and messages from system administrators are examples of unsolicited emails which are not spam.

Today most of the spam sent is originated from bots. A bot in the Lethic botnet has the capacity of sending between 12.000 – 60.000 messages per hour. Two popular botnets Grum and Cutwail have been used to sent 39,9 billion and 74 billion spam a day respectively in first quarter of 2010. These statistics show that botnets are intensively used for spamming. Botnet operators may rent the botnet to spammers, also botnet operators may use the spam functionality of the botnets' themselves by sending out malicious software as attachments or sending links to malicious web sites to expand their botnet.

Spammers crawl web sites to harvest email addresses or they may buy email lists from others on the market. These methods will result in low quality email addresses such that they may be unused email addresses or they may be trap email addresses which will enable the network operators to block the source IP addresses. Hence bots are used to harvest email addresses. For instance Win32/Waledac, HTTP botnet, searches for email addresses on compromised machines. If the harvested email addresses include demographic information such as name and address they are considered more valuable.

3.3 Click Fraud

Advertising on the Internet mostly depends on a pay-per-click structure. This system is abused by leveraging botnets. Botnet operator sets up a web site and places advertisements which are working in a pay-per-click fashion. Then botnet operator arranges the bots to automatically click on these advertisements. The pay-per-click marketer will pay for these illegitimate clicks without gaining any sales. Also botnet operators may change the home page of the compromised computer to the related web site and make them click the ads every time the browser is opened. It is observed that approximately 16% clicks on search engine advertisements are fraudulent. In addition to the usage in advertisements, click frauds are used in manipulating online polls, games or click counters.

3.4 Identity and Data Theft

Botnet operators may search the compromised computers using their malware in order to gather data like bank account credentials, email addresses, product keys for games or software products. Also industrial espionage is

another activity that botnets are used. The methods to gather these data include key logging, sniffing the traffic or using phishing attacks.

3.5 Spreading Malware

Another common usage of botnets is spreading malware which is mostly used to extend the botnet by infecting new computers. To spread a malware attacker generally sends spams using bots. These spams include a link to the file directly which is again hosted on the botnet or a link to a website which automatically installs a malware leveraging a vulnerability in the browser. Latter may be achieved by a tactic called drive-by-download which installs the malware to the user's computer only by visiting a malicious website. Attackers use social engineering techniques to make users click the links in the spams such as disguising the message as news digest with provocative headlines or as a message coming from a friend including interesting photos taken together.

4 Conclusions

Current botnet trends, referencing the advantages and disadvantages, are discussed in this document. Among different botnet architectures it is observed that P2P architectures are getting popular because they are less detectable and more resilient. In addition hybrid architectures are seen which utilize the advantages of both centralized and P2P arcitectures. It is seen that as user behaviours change so do botnets. Social networks, usage of mobile devices are hot topics and botnets are also starting to use these technologies. Bots communicating over twitter or bots targeting smartphones or tablet PCs are examples of this usage.

Although the botnet architectures vary, the malicious activites that botnets are used for does not change much. DoS/DDos attacks, spams, identity theft and spreading malware are still at the top of the list. A new item added to this list may be manipulating industrial systems using a programmable logic controller (PLC) rootkit that targets industrial systems. This shows that industrial systems are also under threat like financial and personal data.

References

[1] Zhaosheng Zhu, Guohan Lu, Yan Chen, Zhi Judy Fu, Phil Roberts, and Keesook Han. Botnet research survey. *32nd Annual IEEE International Computer Software and Applications Conference*, pages 967–972, 2008.

[2] J. Oikarinen and D. Reed. Rfc1459 internet relay chat protocol, May 1993.

[3] Eggdrop: Open source irc bot. `http://www.eggheads.org`, 1993.

[4] Mcaffee. w32/sdbot worm. `http://vil.nai.com/vil/content/v\\_100454.htm`, 2003.

[5] Microsoft webdav vulnerability. `http://www.microsoft.com/technet/security/bulletin/ms03-007.mspx`, 2003.

[6] Microsoft dcom rpc vulnerability. `http://www.microsoft.com/technet/security/bulletin/ms03-026.mspx`, 2003.

[7] Microsoft lsass vulnerability. `http://www.microsoft.com/technet/security/bulletin/ms03-011.mspx`, 2004.

[8] Computer associates, win32.agobot. `http://www3.ca.com/securityadvisor/virusinfo/virus.aspx?id=37776`, 2004.

[9] Microsoft security intelligence report, 2010.

[10] Christian Rossow, Christian J. Dietrich, and Prof. Dr. Norbert Pohlmann. Botnets – literature survey and report, December 2009.

[11] Spiros Antonatos, Periklis Akritidis, Vinh The Lam, and Kostas G. Anagnostakis. Puppetnets: Misusing web browsers as a distributed attack infrastructure. *ACM Trans. Inf. Syst. Secur. 12*, December 2008.