6-5-2009

Study of Botnets and Their Threats to Internet Security

M. Tariq Banday
University of Kashmir, sgrmtb@yahoo.com

Jameel A. Qadri
BC College of North West London, scorpiojameel@yahoo.com

Nisar A. Shah
University of Kashmir, nassgr@yahoo.com

芽|Sprouts Working Papers on Information Systems ISSN 1535-6078

Study of Botnets and Their Threats to Internet Security

M. Tariq Banday
University of Kashmir, India

Jameel A. Qadri
BC College of North West London, UK

Nisar A. Shah
University of Kashmir, India

Abstract
Among all media of communications, Internet is most vulnerable to attacks owing to its public nature and virtually without centralized control. With the growing financial dealings and dependence of businesses on Internet, these attacks have even more increased. Whereas previously hackers would satisfy themselves by breaking into someoneâ s system, in today's world hackers' work under an organized crime plan to obtain illicit financial gains. Various attacks than include spamming, phishing, click fraud, distributed denial of services, hosting illegal material, key logging, etc. are being carried out by hackers using botnets. In this paper a detailed study of botnets vis-a-vis their creation, propagation, command and control techniques, communication protocols and relay mechanism is presented. The aim of this paper is to gain an insight of security threats that users of Internet are facing from hackers by the use of malicious botnets.

Keywords: Botnet, Bot, Internet Security, Spam, Phishing, DDoS, Identity Theft, IRC

Permanent URL: http://sprouts.aisnet.org/9-24

Reference: Banday, M.T., Qadri, J.A., Shah, N.A. (2009). "Study of Botnets and Their Threats to Internet Security ," . *Sprouts: Working Papers on Information Systems*, 9(24). http://sprouts.aisnet.org/9-24

BOTS AND BOTNETS

The term bot, derived from "ro-bot" in its generic form is used to describe a script or set of scripts or a program designed to perform predefined functions repeatedly and automatically after being triggered intentionally or through a system infection. Although bots originated as a useful feature for carrying out repetitive and time consuming operations but they are being exploited for malicious intent. Bots that are used to carry out legitimate activities in an automated manner are called benevolent bots and those that are meant for malicious intent are known as malicious bots. Benevolent bots among various other activities are used by search engines to spider online website content and by online games to provide virtual opponent (Cooke & et al – 2005).

The first bot program Eggdrop created by Jeff Fisher in 1993 originated as a useful feature on Internet Relay Chat (IRC) (Green & et al – 2000) for text based conferencing on many machines in a distributed fashion. In a typical IRC setup (Oikarinen & Reed – 1993), a user running an IRC client program connects to an IRC server in an IRC network. The default TCP service port for IRC is 6667 and generally IRC servers listen on port range of 6000-7000, though servers could be configured to run on any TCP port. All servers are interconnected and pass messages from one user to other. As IRC gained popularity among Internet users, attacks on IRC started, initially due to curiosity or seeking fame and later for illicit financial gain, resulting in its misuse. An IRC malicious bot program runs on an IRC host or client each time it boots in a hidden manner and controlled by commands given by other IRC bot(s). It is typically an executable file with a size of less than 15 KB in its compressed form. An IRC host computer running an IRC bot malware program becomes a Zombie or a drone (Choo – 2007). The first malicious IRC bot, Pretty Park Worm that appeared in 1999 contained a limited set of functionality and features, such as the ability to connect to a remote IRC server, retrieve basic system information e.g. operating system version, login names, email addresses, etc. (Puri – 2003). However, bots extend the basic functions of their predecessors and have become a very powerful tool in building large computer armies which is the key difference between bots and other programs like viruses and worms. This very large pool of such Zombie hosts running bot programs form a large network called a botnet run under the command and control of a single or a group of hackers known as botmaster. Any host on Internet that is compromised by the botmaster becomes part of this botnet. A typical botnet comprises of thousands of Zombie hosts and thus poses a tremendous threat to the Internet security and privacy (Schaffer – 2006). For creating a bigger and safer botnet that could remain up and running for large duration without detection, most vulnerable to bot infection are less monitored, high bandwidth home computers or University Servers (Vogt, Aycock & Jacobson – 2007). According to (MessageLabs - 2009) various notorious botnets that have been reported in the literature include Storm, Srizbi, Cutwail, Gheg, Mega-D, ASPROX, Rustuch, Warezor, Doubot, Ozdok, Xarvester and Bagle. Their estimated size of these botnets in terms of number of bot malware compromised computers varies from a few bots to a million bots. The average spam emails send through these bots per day ranges from a million messages to more than ten billion messages.

BOTNET CREATION AND PROPOGATION

The process of building a botnet requires minimum technical and programming skills. Besides this, some IRC channels offer specialized training programs (Lanelli & Hackworth –

2005) for creation, propagation and use of botnets. A brief two stage overview of building a botnet is outlined in this section.

Bot Creation

This stage largely depends on skills and requirements of an attacker. The attacker may choose to write its own code or simply extend or customize an existing bot. Readymade and highly configurable bots with step by step instructions on how to compromise systems are sold on Internet. The instructions include instructions to obtain packaging exploits, simple character and graphical user interfaces, and various other tools for gaining backdoor entry into networks (Barford & Yagneswaran – 2006). The bot code generally contains configurable components that include IRC server and channel information, remote IRC TCP service port, the location and name of the bot code file in the infected machine, and other components permitting the botmaster to dynamically change the attack behavior and to hide itself, list of botmasters and their credentials. The values pertaining to these components are supplied to the bots by the botmaster(s) using various Command and Control techniques (Barford & Yagneswaran – 2006).

Bot Propagation

In this stage vulnerable systems and tools to exploit them are located which are then used to gain backdoor access to these systems facilitating installation of bot malware by uploading or commanding the victim machine to download a copy of the bot malware (Shannon & Moore – 2004). This infection stage involves use of various direct and indirect techniques to spread bot malware. These include attack through software vulnerabilities, vulnerabilities caused by other infections, social engineering through the use of email, instant messaging and malicious web page content. The bot malware is also propagated through peer to peer networks, open file sharing, and direct client to client file exchange. Bot malware uses FTP, TFTP, HTTP protocol based services to infect computers and spread it until a desired strength of botnet is assembled (Choo – 2007). Botnets are also created by other botnets called seed botnets.

BOTNET COMMAND AND CONTROL (C&C) TECHNIQUES

Once bot malware is recruited on the victim machines, the botmaster has to discover these bot malware infected machines. Once discovered, the botmaster needs to control these victim machines through some form of communication to carry out the desired operations. One simple possible method of communication between bots and botmaster is through a direct control message communication link. However, such a direct link can easily locate the botmaster and as such this type of communication is not used. Instead several organized command languages and control protocols called botnet Command and Control (C&C) techniques are used to operate botnets remotely. Communication between bots and the C&C machine is the weakest link in a botnet, without which the victim cloud does not behave as a coordinated network (Barford & Yagneswaran – 2006). C&C system of botnets is unique and unlikely to change among bots and their variants, however; attackers are continuing to adapt and look for new botnet communication channels. In this section we discuss three different categories of command and control techniques namely centralized, peer to peer and random.

Centralized Command & Control (C&C) Technique

This C&C technique uses a central high bandwidth host called C&C server to forward messages between various bots (Govil & Dayanand – 2007). The C&C server in a botnet is a compromised computer that runs certain network services like IRC, HTTP, etc and which rallies the commands issued by the botmaster to each host in the botnet that join the C&C server channel. Botnets use various mechanisms to protect their communications which include the use of passwords set by the botmasters. The centralized C&C is most predominant C&C technique and many bots including *AgoBot, RBot, SDBot, SpamThru* and *Zotob* use this C&C technique. There are several advantages of using centralized C&C techniques out of which easy availability and greater productivity are most predominant. A great amount of resources are available online to create a C&C based botnet that include IRC server and IRC bot scripts, simple CUI and GUI customization interfaces, etc. Centralized C&C allows controlling of as many bots as possible and thus maximizes the profit of the botmaster. Small message latency and lack of adequate countermeasures in fighting against botnets especially on unprotected and unmonitored networks have also motivated the botnet operators to use centralized C&C technique. The only drawback of centralized C&C technique is that C&C server is the weakest point in the entire botnet link as all communication passes through this single point. Once the central location is discovered, the entire botnet can be easily neutralized.

P2P Command & Control (C&C) Technique

The peer to peer C&C technique uses P2P communication with no real central server to forward messages between botnets which makes it more resilient to failures in the network (Cooke & et al – 2005). Unlike centralized C&C technique, P2P C&C technique is much harder to discover and destroy; even if one or more bots are neutralized, the botnet still continues to operate. Further, an anonymous P2P technique may be used to make it even more difficult to detect. However the botnet size supported by P2P systems is generally very low in comparison to centralized systems, which makes profit oriented botmasters to avoid using P2P technique. Also the propagation latency and guaranteed message delivery is lacking in P2P systems. Some examples of botnets that use P2P C&C technique include *Phatbot* and *Sinit*.

Random Command & Control (C&C) Technique

The idea of random C&C technique has been presented by Evan Cooke (Cooke & et al – 2005), however no botnet has been reported to have used this C&C technique. In this C&C technique no bot can know about the existence of more than one other bot thus making the detection of the botnet very difficult. A botmaster or a bot can send an encrypted message randomly which may be intercepted by other bot and a conversation could begin. In this command and control technique message latency is very high, however; unlike other command and control techniques it lags guaranteed message delivery.

BOTNETS COMMUNICATION PROTOCOLS AND RALLY MECHANISMS

The command and control techniques described above use various communication protocols (Rajab & et al – 2006) and rally mechanisms (Govil & Dayanand – 2007). Botnets make use of some well defined network communication protocols that include more importantly IRC protocol, HTTP protocol and other protocols like IM and P2P protocols. The communication protocols used in botnets provide an understanding of the botnets origin and the

possible software tools that may be used by the botnet. Besides this, knowledge of communication protocol used by a botnet provides an understanding for decoding the communication that takes place between bots and the botmasters.

In an IRC protocol based botnet, the C&C server is installed as an IRC service on a host computer and botmaster creates a channel on the C&C server. The bots connect to this channel, receive commands from the botmaster and execute these instructions to carry out various types of malicious functions. The flexibility of IRC protocol to be used as a group communication or private communication system makes it possible for botmaster to command all bots or selectively select a group of bots in a botnet to carry out a malicious activity.

Although IRC protocol is the most predominant method used in botnets, yet the monitoring of IRC traffic and the installation of firewalls to reduce the chances of falling victim to a botmaster, some botnets have been using different communication protocols including HTTP, IM and P2P protocols. IM and P2P protocols are used for creating botnet of relatively small size but HTTP protocol is used to create a large sized botnet. Although HTTP traffic generated by botnets is different from the normal HTTP traffic, yet it is difficult to detect it because it hides itself within huge legitimate HTTP traffic.

Bots include either hard coded C&C server IP addresses or hard coded domain names to connect to the C&C servers. Inclusion of hard coded C&C server IP addresses with bot code makes it easy to detect, block the C&C server and neutralize the entire botnet. In order to evade detection, this type of rally mechanism is not used in bots. Bots include hard coded domain names assigned by dynamic DNS providers, so that even if the C&C server IP address is located botmaster can update the dynamic DNS entry to map the server at some other address and continue operating the botnet. Some botmasters operate their own unauthorized distributed DNS servers that are used to resolve the IP addresses of the C&C servers.

SECURITY THREATS FROM BOTNET

With the growing sophistication of botnets and highly skilled and organized botmasters, a powerful threat as that from viruses, Trojan horses, network intrusion, worms and other familiar cyber threats (McCarty – 2003) persists to the Internet security and privacy. Botmasters are more numerous, sophisticated, harder to identify, have better tools and very large size of bot armies and thus can command the individual zombies to carry out various types of attacks that include but is not limited to distributed denial of services (DDoS), spamming, phishing, identity theft, click fraud, hosting of illegal material, disseminating malicious code, and a variety of other possible attacks (McKewan – 2006). Several studies and reports that include (Kandula & et al – 2005), (McAfee – 2005), (AHTCC – 2006), (Dunn – 2005), (David – 2006), (FCAC – 2006) and (Biever & Celeste - 2004) have reported the use of botnets in carrying out several types of attacks on one or the other service available on the Internet.

Distributed Denial of Services (DDoS)

Denial of Services (DoS) attack is an attempt on a computer system or network to make unavailable the computational resources to its intended user. A Distributed DoS (DDoS) attack is a DoS attack which involves use of multiple compromised systems to cause a loss of service to its intended users by depleting the bandwidth and other computational resources of the target system or network. Bandwidth depletion and resource depletion are two main variants of DDoS attacks. Flooding and reflection attacks are two primary types of bandwidth depletion attacks.

Bandwidth depletion involves flooding a target machine with unwanted traffic as an attempt to overwhelm the processing power of the target machine. Flooding attack involves sending multiple packets to some target website simultaneously to congest traffic. The reflection attack involves sending many packets to many computers with a spoofed source address. Resource depletion also called protocol exploitation involves a target that specifically attempts to deplete resources on the targeted computer or cause it to become unstable and crash. To launch a DDoS attack using botnet has several advantages that include magnifying impact of the attack without the requirement of any source IP address spoofing. A DDoS attack on the DNS servers of United States Department of Defense has been reportedly carried out in Feb, 2006.

Spamming

Loosely defining spam is any message or posting, regardless of its content, that is sent to multiple recipients who have not specifically requested the message (Opt-In). Spam can also be multiple postings of the same message to newsgroups or list servers that are not related to the topic of discussion. A person engaged in spamming is called spammer. Spam in blogs called blog spam or comment spam is a form of search engine spamming done manually or automatically by posting random comments, promoting commercial services, to blogs, wikis, guestbooks, or other publicly-accessible online discussion boards. Any web application that accepts and displays hyperlinks submitted by visitors may be a target of Link Spam. This is the placing or solicitation of links randomly on other sites, placing a desired keyword into the hyperlinked text of the backlink. Blogs, guest books, forums and any site that accepts visitors' comments are particular targets and are often victims of drive-by spamming, where automated software creates nonsense posts with links that are usually irrelevant and unwanted. Link spam dishonestly and deliberately manipulates link-based ranking algorithms of search engines like Google's PageRank to increase the rank of a web site or page so that it is placed as close to the top of search results as possible. Spam generally refers to email, rather than other forms of electronic communication. The term spim, for example, is used for unsolicited advertising via Instant Messaging. Spit refers to unsolicited advertising via Voice Over Internet Protocol (VOIP). Unsolicited advertising on wireless devices such as cell phones is called wireless spam.

Spammers use various techniques and tools that include spoofing, spam botnets (Husna & et al – 2008), open proxies, open mail relays, untraceable Internet connections, and bulk email tools for sending unsolicited bulk email. Spammers operate as a creative group who work through secret networks to meet and share email addresses. The two most effective approaches to gather or harvest emails are to monitor Internet use and to ask for email addresses. Some of the most popular methods of email harvesting are guessing, purchased lists, legitimate email lists, web pages, white/yellow page sites, web & paper forms, usenet posts, web browser, hacking, user profiles, irc and chat rooms. The significant increase in the spam volume mostly due to botnets has been the key development in the year 2008 (MessageLabs - 2009).

Phishing and Identity Theft

Phishing is used to describe spoof emails and other technical ploys to trick receipts into giving up their personal or their company’s confidential information such as social security number, financial account credentials and other identity and security information. Some phishing emails look extremely professional and realistic, while others are crude and badly constructed but have a common goal to steal information through deception. This form of identity theft (McCarty – 2003b) employs both social engineering and technical subterfuge to steal account

access information, identity or other proprietary information that can be sold on to third party via specialized chat rooms established specifically for this purpose. Selling the information onwards reduces the risk of being apprehended by minimizing the direct link between the hacker and those using the information to gain unauthorized access to accounts and profiting from them. Social engineering schemes use spoofed emails to lead customers to counterfeit websites designed to trick recipients into divulging financial data. Technical subterfuge schemes plant crime ware onto computers to steal credentials directly using keylogging systems. Pharming crimeware misdirects users to fraudulent sites or proxy servers, typically through Domain Name System (DNS) hijacking or poisoning. The term "phishing" evolved from the word "fishing" and follows a very similar approach. Fraudsters and scammers, the "fishermen", send out large quantities of deceptive emails, the "bait", to mostly random address across the Internet.

Phishing is a serious and increasingly prolific form of spam, and is one of the main tactics employed in business and consumer identity theft. Phishing actually comprises of two online identity thefts which are the identity of the target company and its unsuspecting customers. Target Company is commonly a bank, online payment service or other reputable business organization. A typical phishing attack is made up of two components: an authentic looking email and a fraudulent Web page. This form of spam of email frequently has a professional look that includes company logos, colors, graphics, font styles, and other elements to successfully spoof the sender. The content of the phishing email is usually designed to confuse, upset, or excite the recipient. Typical email topics include account problems, account verifications, security updates/upgrades, and new product or service offerings. Recipients of email are prompted to react immediately and click on a link provided in the email body, which actually directs them to the phishing Web page. The intent is to lure recipients into revealing sensitive information such as usernames, passwords, account IDs, ATM PINs, or credit card details. Like the phishing email, the phishing Web page almost always possesses the look and feel of the legitimate site that it copies, often containing the same company logos, graphics, writing style, fonts, layout, and other site elements. This spoofed Web page may also include a graphical user interface (GUI) intended to lure the user into entering their bank account information, credit card number, social security number, passwords, or other sensitive information. Either the phisher, or an anonymous remote user that is sent the information, can then use the stolen information. Phishing approaches used for identity thefts are constantly growing and new variants are tried and used to attack business organizations, financial institutions, and customers. Some of the most prevalent types of phishing and identity theft attacks include deceptive phishing, malware based phishing, key loggers, screen loggers, session hijacking, web Trojans, hosts file poisoning, system reconfiguration attacks, data theft, DNS-based phishing also called pharming, content injection phishing, man-in-the-middle phishing, search engine phishing, spear phishing, vishing or voice phishing.

The phishing "ecosystem" consists of a collection of individuals who play various roles within the phishing space, ranging from the financially-motivated botnet creators to those who actively pursue and prosecute the cybercriminals. In this ecosystem, a large industry of buying and selling - a "microeconomy" - exists within the phishing underground, involving botnet creators, perpetrators, and enablers. However, these three player groups are complex and intertwined: a single individual or multiple perpetrators can play separate or simultaneous roles. Botnets, with an army of thousands of bots awaiting their instructions can use packet sniffers to watch for sensitive information like usernames and passwords on the machine it has intruded and accordingly send this to the botmaster (FCAC – 2006).

Click Fraud

Some of the advertisements appearing on the websites are charged by the website operators on the basis of pay per click revenue model wherein an advertiser is charged on the basis of the number of clicks made by visitors on the advertisement appearing in a website. Any mechanism that is used to increment this click counter in an automated or artificial manner is click fraud. For illicit financial advantages botmaster can increment the click counter in an artificial manner by commanding bots under its control to send web requests that represent clicks on Internet advertisements. Botnet based click fraud is harder to detect because botnet comprises of large number of geographically dispersed IP addresses and *click through pattern matching* wherein geographical locations of IP addresses from each click are monitored fails. Click fraud activity generates large volumes of revenue for attackers and their customers but at the same time poses a great threat to both the advertisers and the content providers and thus is considered as an emerging threat to e-commerce. Several examples of use of botnet in facilitating click fraud have been reported wherein the content provider had to pay huge amount to settle the lawsuit alleging the content providers of overcharging the advertiser. One such recent example has been reported in July 2006 where Google agreed to pay US$ 90 million to settle such a lawsuit. Another example involving the use of botnet to facilitate the click fraud can be found in (McKewan – 2006).

Hosting illegal material and disseminating malicious code

Illegal material such as child pornographic (Olagunju et al – 2008) pictures, videos and other such material, pirated software or code to crack the licensed software, pirated e-books, pirated games, etc. can be stored as a dynamic repository on a bot compromised computer by the botmaster. Often this illegal material contains malicious code in the form of malware like viruses, Trojan horses, worms and others like spyware and adware. All bots contain functionality that allows FTP, TFTP, and HTTP downloads and execution of binaries. This is the primary method used by botnets to update their malicious code; however it is not limited to this alone but can be used to download any file botmaster commands it to. This ability of bots to download and install any binary is often used to install additional malware like Viruses, Trojan Horses, worms and other malicious code like spyware and adware. A malware is an undesired code surreptitiously introduced into a computer system to harm it. Spyware is software that is used to collect personal information about users without their informed consent. Adware is software with advertizing functions that are integrated into or bundled with a software package to recover the costs of programming or reduce or even provide the software free of cost to users. However adware may often take the form of spyware in which the users' activity is tracked by the software and sold without the consent or knowledge of the user.

Other Security Threats

Although botmasters need not to be highly technical yet some are skilled, organized and are getting smarter day by day. Further, they have thousands of bot compromised computers at their disposal and thus can launch variety attacks other than those detailed above. Online games and polls can easily fall victim to botnets where bots can manipulate the results. Bots can be levered to steal the online software license by transferring the same to some other computer. Key loggers can be deployed with bots to retrieve sensitive and secret data. Bots can use packet sniffing to watch for clear text data passing by compromised machines and retrieve sensitive data

such as usernames and passwords. Botnets can setup a fake website with advertisements thus leading to click fraud. Bots are used to download and execute harmful executive files via FTP or HTTP and thus spread new malware and viruses. The growing access to Internet through mobile phones can prompt hackers to attack cellular network system and create botnets on this system which may cause inconvenience to millions of cell phone users.

BOTNET PREVENTION, DETECTION AND DISRUPTION

Botnets present significant new challenges for the Internet community as the attackers come up with new and improved tools. Protection against falling victim to a botnet and detecting the location of botmaster is very challenging owing to various facts that include i) the mechanism used in constructing and maintenance of botnets and that used in its possible attack are independent of each other, ii) Every Zombie in a botnet is a source of attack and iii) Botnets remain in a silent state until they are leveraged to launch a specific attack (Strayer & et al – 2006).

Preventing a system on Internet from falling victim to a botnet requires a high level of awareness about online security and privacy. Besides this, the system must be kept up to date by installation of various Operating System updates and patches. Use of pirated software, games, and other illegal material available online are always a source of malicious code and thus presents a grave security threat and as such users should restrict themselves from accessing such web sites. Further, software firewalls and antivirus/anti-spyware programs should be installed and periodically updated on systems to prevent them from being infected. (Jones & Jim - 2003), (Carpenter & et al – 2001). The use of CAPTCHA tests has been suggested for website and other services for prevention against bots and other malicious agents.

Detecting the bot activity on a system or on a network is dominant to the study of botnets. The use of honeypot has been the most popular method of setting a trap to detect botnet activity (HoneyNet – 2005). Honeypot is generally an isolated and protected system that appears to be part of a network and having valuable information stored on it. It allows itself to be infected by a bot and become part of botnet. The honeypot is next used to capture the bot malware and detect the bot controller. Various reactive and proactive techniques have been suggested to detect and identify botnets. Detection of botnet by monitoring the network and host activity in terms of number of users per channel service ports used or abnormal ratio of invisible to visible users, etc have been suggested. In (Strayer & et al – 2006) examination of flow characteristics such as bandwidth, duration and timing is suggested for detection of botnet C&C activity. (Cooke & et al – 2005) suggests use of secondary bot behavior such as propagation and attack for detecting botnets. In (Akiyama& et al – 2007) three metrics namely relationship, response and synchronization have been proposed for detecting botnets through analyzing their behavior.

On detecting a botnet immediate mitigation goals are to neutralize the zombie by removing the bot infection and more importantly to disrupt the C&C Server of the entire botnet. Disrupting the botnet C&C server is significant because bot infected system is only part of very large zombie army controlled by C&C Server and thus disrupting this controller will reutilize the entire botnet.

CONCLUSION

Increasing number of Internet users and its commercial character naturally bring in proportionate number of criminal minded people to the scene who pose potential threats to legitimate users, Internet infrastructure and timeliness of services offered by it. The aim of this paper is to document Internet Security threats so that general understanding about the malicious users and the malware is increased. The paper presents a detailed study of technology involved in the design and control of botnets and threats posed by them. The main focus of this paper is Botnet which enfolds all other attacks in one way or the other. The paper has not presented any solution to the Internet Security threats but hopefully will generate an intense interest among researchers to undertake research in this area.

REFERENCES

AHTCC. (2006). International Internet Investigation nets arrest. Australian High Tech Crime Centre Media Release. http://www.ahtcc.gov.au/news_and_information/media_releases/nat_060322internetarrest.pdf accessed May 17, 2008.

Akiyama, M., Kawamoto, T., Shimamura, M., Yokoyama, T., Kadobayashi, Y. & Yamaguchi, S. (2007). A Proposal for metrics for botnet detection based on its cooperative behavior. Proceedings of the 2007 International Symposium on Applications and the Internet Workshops (SAINTW'07), IEEE Computer Society. http://doi.ieeecomputersociety.org/10.1109/SAINT-W.2007.14 accessed June 8, 2008.

Barford, P. & Yagneswaran, V. (2006). An Inside Look at Botnets. In Special Workshop on Malware Detection, Advances in Information Security, Springer, 2006, http://pages.cs.wisc.edu/~pb/botnets_final.pdf accessed July 8, 2008.

Biever & Celeste. (2004). How Zombie Networks Fuel Cybercrime. New Scientist. http://www.newscientist.com/article.ns?id=dn6616 accessed June 8, 2008.

Carpenter, J., Dougherty, C. & Hernan, S. (2001). Continuing Threats to Home Users, CERT Advisory, CA, http://www.cert.org/advisories/CA-2001-20.html accessed May 8, 2008.

Choo, KK. R. (2007). Zombies and Botnets. Trends & Issues in crime and Criminal Justice, 333. http://www.aic.gov.au/publications/tandi2/tandi333.pdf accessed July 18, 2008.

Cooke, E., Jahanian, F. & McPherson, D. (2005). The zombie roundup: understanding, detecting, and disrupting botnets. Proceedings of SRUTI '05 Workshop, USENIX Association, Berkeley CA, 35–44. http://www.usenix.org/events/sruti05/tech/full_papers/cooke/cooke.pdf accessed June 8, 2008.

David, L. (2006). Phishing expedition at heart of AT&T hacking. San Francisco Chronicle. http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/09/01/BUGVBKSUIE1.DTL accessed May, 8, 2008.

Dunn, JE. (2005). Botnet chaos shut down hospital. Techworld, May 5, 2005. http://www.techworld.com/security/news/index.cfm?NewsID=5951 accessed May 17, 2008.

FCAC (2006). FCAC Cautions Consumers About New Vishing Scam. Financial Consumer Agency of Canada. http://www.fcac-acfc.gc.ca/eng/media/news/default.asp?postingId=218 accessed June 8, 2008.

Govil, J. & Dayanand, M. (2007). Examining the criminology of bot zoo. In proceedings of ICICS 2007, 1-6. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&isnumber=&arnumber=4449633 accessed March 22, 2009.

Green, M., Neumayer, M., Paulsen, V., Roeckx, K., Ruokonen, V., Tjernstrom, M. & Zehl, S. (2000). Internet Relay Chat: Architecture Request for Comments: 2810. http://www.irchelp.org/irchelp/rfc/rfc2810.txt accessed July 18, 2008.

HoneyNet. (2005). Know your enemy: Tracking botnets. The Honeynet Project. http://www.honeynet.org/papers/bots/accessed July 18, 2008.

Husna, H., Phithakkitnukoon, S., Palla, S. & Dantu, R. (2008). Behavior analysis of spam botnets. COMSWARE 2008, 246-253. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&isnumber=&arnumber=4554418 accessed March 22, 2009.

Jones & Jim. (2003). BotNets: Detection and Mitigation. FEDCIRC. http://www.fedcirc.gov/library/documents/botNetsv32.doc accessed May 8, 2009.

Kandula, S., Katabi, D., Jacob, M. & Berger, A. (2005). Botz-4-Sale: Surviving Organized DDoS Attacks that Mimic Flash Crowds. Proceedings of 2nd Symposium on Networked Systems Design and Implementation, Boston, MA, http://nms.lcs.mit.edu/papers/killbots.pdf accessed May 17, 2008.

Lanelli, N., & Hackworth, A. (2005). Botnets as a vehicle for online crime. CERT Coordination Center, Pittsburgh PA, http://www.cert.org/archive/pdf/Botnets.pdf accessed June 13, 2008.

McAfee. (2005). McAfee virtual criminology report. McAfee, Santa Clara CA. http://www.softmart.com/mcafee/docs/McAfee%20NA%20Virtual%20Criminology%20Report.pdf accessed May 17, 2008.

McCarty, B. (2003). Automated Identity Theft. IEEE Security & Privacy, 1(5): 89-92.

McCarty, B. (2003b). Botnets : Big and Bigger. IEEE Security & Privacy, 1(4): 87-90.

McKewan, A. (2006). Botnes: Zombies get Smarter, Network Security, 6: 18-20.

MessageLabs. (2009). MessageLabs Intelligence: 2008 Annual Security Report. http://www.messagelabs.com/mlireport/MLIReport_Annual_2008_FINAL.pdf accessed March 23, 2009.

Oikarinen J. & Reed, D. (1993). Internet Relay Chat Protocol RFC 1459. Network Working Group. http://rfc.sunsite.dk/rfc/rfc1459.html accessed July 28, 2008.

Olagunju, Amos O. (2008). Harmonizing the Interests of Free Speech, Obscenity and Child Pornography on Cyberspace: The New Roles of Parents, Technology and Legislation for Internet Safety. Paper presented at the Oxford Round Table on "The Regulation of Cyberspace: Balancing the Interests. Available online at: http://www.eric.ed.gov/ERICWebPortal/contentdelivery/servlet/ERICServlet?accno=ED502269 accessed March 22, 2009.

Puri, R. (2003). Bots & botnet: An overview. SANS Institute. http://www.sans.org/rr/whitepapers/malicious/1299.php accessed June 8, 2008.

Rajab, M. A., Zarfoss, Monrose, J. F., & Terzis, A. (2006). A multifaceted approach to understanding the botnet phenomenon. In Internet Measurements Conference (IMC)2006. http://www.imconf.net/imc-2006/papers/p4-rajab.pdf accessed June 14, 2008.

Schaffer, GP. (2006). Worms and viruses and botnets, oh my!. IEEE security & privacy 4(3), 52–58.

Shannon, C. & Moore, D. (2004). The spread of the witty worm. Security & Privacy Magazine, 2(4): 46-50.
Strayer, W. T., Walsh, R., Livadas, C. & Lapsley, D. (2006). Detecting Botnet with Tight Command and Control. ARO/DARPA/DHS Special Workshop on Botnet.
Vogt, R., Aycock, J. & Jacobson, M. (2007). Army of botnets, proceedings of 14th Annual Network and Distributed System Security Symposium (NDSS).

芽|Sprouts

Working Papers on Information Systems | ISSN 1535-6078

Office:
Sprouts
University of Amsterdam
Roetersstraat 11, Room E 2.74
1018 WB Amsterdam, Netherlands
Email: admin@sprouts.aisnet.org

芽|Sprouts