BOTNETs: A Network Security Issue

From Definition to Detection and Prevention

Engr. Umar Iftikhar[1], Engr. Kashif Asrar[2], Dr. Maria Waqas[3], Dr' Syed Abbas Ali[4]
Computer and Information Systems Engineering Department
NED University of Engineering and Technology
Karachi, Pakistan

***Abstract*—With the technological advancements in the field of networking and information technology in general, organizations are enjoying the technological blessings and simultaneously under perpetual threats that are present in the form of attacks, designed especially to disable organizations and their infrastructure, as the gravest cyber threats in recent times. Compromised computers or BOTNETs are unarguably the most severe threat to the security of internet community. Organizations are doing their best to curb BOTNETs in every possible way, spending huge amount of their budget every year for available hardware and software solutions. This paper presents a survey on the security issues raised by the BOTNETs, their future; how they are evolving and how they could be circumvent to secure the most valuable resource of the organizations which is data. The compromised systems may be treated like viruses in the network which are capable of performing substantial loss to the organization including theft of confidential information. This paper highlights the parameters that should be considered by the organizations or Network administrators to find out the anomalies that may point to the presence of BOTNET in the network. The early detection may reduce the impact of damage by taking timely actions against compromised systems.**

***Keywords*—BOTNET; malware; drones; zombies; threats**

I. Introduction

The emerging and rapidly growing internet era has led the mankind to an exceptional world of facilitation where one can find endless social and economic benefits. On the other hand, this technology has introduced numerous challenges. Despite of various advanced security methodologies, the network security threats are continuing to evolve day by day.

Network security can be described as the actions taken for the protection of the network. Usually, these actions safeguard the usability, reliability, integrity and safety of the data and network. Operative security in networks is capable of addressing various types of threats as well as prevents them from entering or spreading into the network.

There are numerous types of threats that are being faced by network security. Some of them are Trojan horses, viruses and worms, spyware, malware, BOTNETS, zero- hour attacks, hacker attacks, DoS (Denial of Service) attacks, data interception and theft, identity theft, etc. [1].

This paper deals with a review of a very important network security issue that is BOTNET. The paper begins with the demonstration of network security issues in section [I] and explaining some of the important threats in network security due to the BOTNETS. Botnet administrators can moreover run them as a commercial operation for creating a distress for the organization especially those who rely more on the IT infrastructure for their business continuity in Section II. Threats immerged due to the existence of BOTNETS are mitigated by major operations that require significant worldwide participation in Section III.

A. What is BOTNET?

The terminology BOTNET is extracted from the term bot that is the short form for the robot. Intruders use different tricky techniques to distribute malicious software that is capable of converting a computer into bot or zombie. When such a situation arises in which a computer is being controlled not by user but by a hacker, it performs several suspicious tasks on internet without the knowledge of the user.

In other words, the collections of several computers that are associated to perform suspicious tasks using malicious software are termed as BOTNETs.

Attackers usually utilize the bots to infect huge number of computers. These computers form a group known as BOTNET. These zombies can be utilized to spread out spam emails, distribute viruses, attack the servers, and commit various kinds of fraud and cybercrimes [2].

The size of BOTNET is variable that is it can be small or large. The size of BOTNET depends upon the sophistication and complexity of the bots that are used. A large BOTNET consist of tens and hundred thousand zombies. While on the other hand, a smaller BOTNET comprised of a few thousand of zombies.

The owner whose computer has become the zombie, do not know that the affected computer and all of its resources are being remotely controlled, subjugated and misused by an single or a group of malware runners that uses Internet Relay Chat (IRC) as a substantial tool for these malicious attacks. There are several kinds of malwares and malicious software and applications that have already trapped and are continuing to trap the internet. Large bots use their own spreaders to spread the viruses while smaller kinds of bots do not possess such capabilities. The whole scenario of BOTNETs is illustrated in Fig. 1 [3].

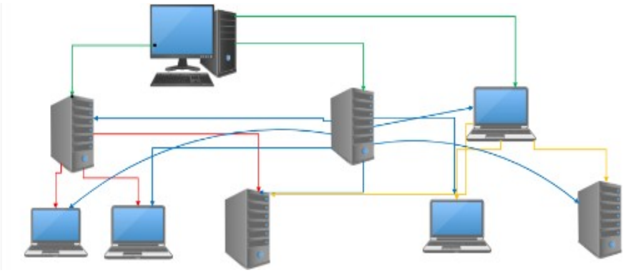

Fig. 1. BOTNET Central Command.

B. Formation of BOTNET

BOTNETs are formed with a use of an IT tool known as “drones”. These drones penetrate into an open computer through internet that has low security measures. When a drone penetrates into a computer that computer becomes a “Zombie Computer”. Now that zombie computer acts like a BOTNET that is being controlled centrally by a BOTNET owner. The zombie computer runs malicious software itself and the owner of infected computer doesn’t know that the computer is being trapped and became a BOTNET [4].

The whole group of BOTNETs is being controlled centrally by the herder that is actually a BOTNET owner. The more increment in the size of the BOTNETs, the larger is the impact of BOTNETs on internet. In other words, herder gets stronger and stronger as more and more computers are affected by this malware 5].

C. Propagation of BOTNET

The BOTNETs propagate through various bot software that contains spreaders. This spreader in the bot software automates the job of IP addresses scanning for various susceptible software holes. Once the holes are found by software, the unsecured and defenseless machines are attacked and infected by this bot software, and this pattern continues thus resulting in increasing the number of infected computers. With each new machine infected by the drones, the BOTNET becomes more and more powerful to infect more machines. The one and only difference between a bot and worm is the presence of a unifying control mechanism [6].

Command and Control Tools for BOTNET:

A large number of infected machines are useless without some controlling mechanism. The command and control (C&C) mechanism provides the interface between the BOTNET and the herder. The C&C get commands from herder and control the bots.

The BOTNETs are traditionally been controlled using Internet Relay Chat (IRC). This framework is the most popular one because of its easiness, tractability and ease of administration. IRC is a global and commonly used communication standard over the internet and can be easily modified for any specific purpose. Bot software has the tendency to connect the infected computer to IRC server and accept instructions from centrally controlled channel (herder). The herders have rights to use current chat service and network or they can implement their own separate server for control by using the IRC daemon [7].

D. Mitigation of BOTNET

In today’s high tech era, where internet has penetrated into the lives of humans and made the world a global village, BOTNETs are of major concerns and can be very dangerous if they are in a very large number. With drone population counting as 60,000 – 80,000, the access and the control that herders can have over the largest network giants is incredible and gigantic.

Therefore, the best possible way to diminish BOTNETS is to prevent and block them from establishing at initial stages. If malware is controlled from propagation and infection into the system, BOTNETs would no longer remain the serious threat to the network security. The owner of the computer should take care of the system itself by properly patching and licensing the software and systems, otherwise their computers can be easily transformed into BOTNETs. The mitigation of BOTNETs is further illustrated in Fig. 4 [8].

II. Application of BOTNETs

BOTNET damages magnificently, the security of businesses and individuals the data and resources of an infected computer losses its legitimate user’s control. Most of the users store their sensitive information on their personal machines. If the security of this machine is compromised, the attacker can easily harvest that sensitive and confidential data. Bot herders used to sell or rent their BOTNETs to those who want to perform hacker activities.

The strong penetrating capability and strength of BOTNETs, give attacker more and more power on the internet. With the increase in number of BOTNETs, the control over compromised systems of the herder becomes stronger thus performing more complicated, advance and typical activities that internet has never seen before.

Some of the severe applications of BOTNETs are discussed below:

A. Click Fraud

BOTNETs can be utilized to engage in Click Fraud. In this type of scam, the bot software used to navigate different websites on browser and automatically click on advertisements. Now consider about a herder having a bot network of several thousand computers and stealing a large amount of money from online advertisement organizations that pay small amount on each click. With a large network, each click for few times, returns heavy amount of money. As the clicks are coming from each separate entity distributed across the globe, so investigators can’t find out that this is a scam [9].

B. Distributed Denial of Service (DDoS)

BOTNETs are used to remunerate confrontation on various computers over the network accessing the internet by completely trapping and saturating its bandwidth and various other resources. Such DDoS attacks can disable the access the web pages for a long span of time. While considering the financial organizing, this delay of accessibility places a marvelous and enormous burden on financial operators that are unable to service their customers.

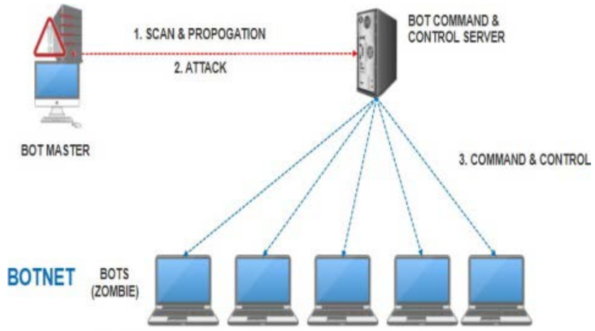

Fig. 2. Distributed Denial of Service (DDoS).

Another type of attack comes under the umbrella of DDoS where the attackers demand for the payment to free the attacked resources and allow the traffic to flow again. This type of attack is known as Extortion attacks. The complete illustration can be referred from Fig. 2 [10].

C. *Key logging and Mass Identity Theft*

Key logging is the technique that is used to record the sequence of the key pressed. This can be done by installing the key logger software. This is encryption software that is used to gather the sequence of keys pressed by the user. This includes the personal information of the user and passwords. This is one of the important reasons behind the massive PayPal account theft for past several years.

Bots can also be utilized by the attacker as an agent for mass identity theft. This involves methods of phishing or pretending to be the agent of a company and enforcing the Client to give their personal information like password and credit card numbers. The phishing technique is implemented by spam emails in which a fake link is given for the renowned financial or online transaction website that traps the client to submit the personal information.

Despite of key logging, many bots allow the herder to completely access the file system. This enable the herder to modify and transfer any file, can read any personal document stored in the user’s computer and can upload the malicious files [11].

D. *Traffic Monitoring and Spamming*

BOTNETs are utilized by using the TCP/IP proxy protocol for several applications of network. After the IP of a computer is compromised, bot commander can use this IP to propagate the massive spams, malware, phishing and fraud email to various email address. This is achieved by stealing an IP address of any bot and in conjunction with other bots, the bot commander send these massive spam emails.

Also, a zombie can act as a packet sniffer to monitor the traffic and ongoing activities over the network with the help of infected machines. Typically these sniffers look for the username and passwords for different accounts which a bot commander can use later for its personal interests [12].

E. *Warez*

Another application of the BOTNETs is Warez. Warez is technique in the world of hacking that is being used for stealing the licenses of the software or applications. BOTNETs possess the tendency to steal, store or propagate Warez. They can do this by scanning the hard drives of the infected machines looking for the software and applications that are licensed. After successful searching, the herder can easily transfer or duplicate that license and can distribute over the internet thus violating the copyrights of the software. The illustration of Warez in Fig. 3 [13].

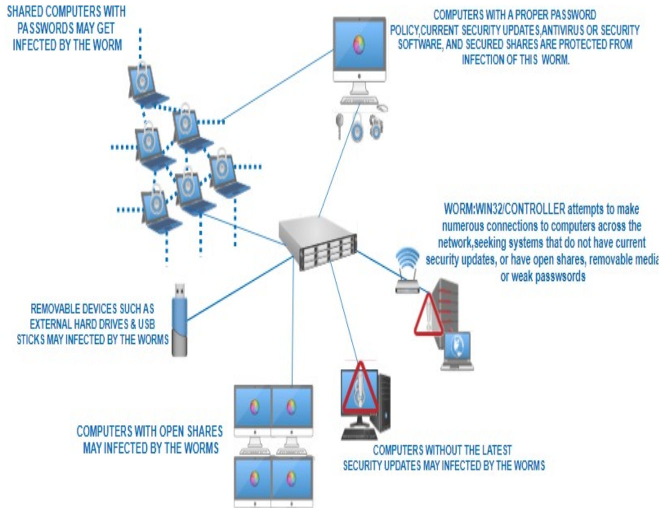
SHARED COMPUTERS WITH PASSWORDS MAY GET INFECTED BY THE WORM
COMPUTERS WITH A PROPER PASSWORD POLICY,CURRENT SECURITY UPDATES,ANTIVIRUS OR SECURITY SOFTWARE, AND SECURED SHARES ARE PROTECTED FROM INFECTION OF THIS WORM.
WORM:WIN32/CONTROLLER attempts to make numerous connections to computers across the network,seeking systems that do not have current security updates, or have open shares, removable media or weak passwsords
REMOVABLE DEVICES SUCH AS EXTERNAL HARD DRIVES & USB STICKS MAY INFECTED BY THE WORMS
COMPUTERS WITH OPEN SHARES MAY INFECTED BY THE WORMS
COMPUTERS WITHOUT THE LATEST SECURITY UPDATES MAY INFECTED BY THE WORMS

Fig. 3. Illustration of Warez.

III. BOTNET Detection and Prevention

The detection and prevention of BOTNETs is of immense importance as it is one of the major issues of the network security.

A. *Detection of BOTNETs*

The detection of BOTNETs is typical and very much difficult. The reason is that bots used to operate within a network or infected machine without prior information to the owner [15]. However there are some common indications while the routine functioning of the machine from which the owner can identify whether the machine is under attack or not. These indications are listed below:

1) Usage of Internet Relay Chat (IRC) by monitoring the traffic.

2) Time to time multiple connection attempts with known C&C servers.

3) Multiple machines generating identical DNS requests.

4) Outgoing SMTP traffic becomes very high.

5) Unexpected popups.

6) Slow processing speed, processor utilization is at extreme while no certain heavy application is running.

7) High and repetitive spikes in the data traffic over the network. Particularly Port 6667 that is used for IRC. Port 25 usually used for spam emails. Port 1080 used by proxy servers.

8) Outbound messages send by user without any knowledge like on email, instant messengers, social media, etc. with the name of owner.

9) Internet access becomes unavailable for no reason. Web pages couldn’t be accessed [5, 7, 14, 16].

B. Prevention from BOTNETs

There are various method, techniques and measures that the owner of the infected machine can take to avoid the BOTNET attacks. The major concerned in transforming a normal machine to a BOTNET is malware. The measures described below mainly focuses on how to avoid malware. In other words, if malware are being stopped from penetration into a machine the chances of transforming a machine into BOTNET gets lower extensively.

Recommended practices from different network security providers are summarized below:

1) Installation and enabling of Windows Firewall: The users should always install a recommended firewall and must keep that firewall enabled especially when accessing the internet. As firewall block many network based threats.

2) Disabling the Auto-Run option: The auto-run option in the windows must be disabled or it must be enabled with the permission of user. The user must know that which software is installing on the machine. If auto-run option is enabled, it will automatically install the software without the permission of the user.

3) Breaking password Trusts: While taking in consideration the local accounts, especially the account with a local network administrator, it is really important to isolate and eliminate the threats by making a judicious policy for the implementation of the local network. By disabling the computer's capability to automatically connect to the other networks that are closer in the path, the property of BOTNET to make itself multiple will be eliminated.

4) Network Compartmentalization: In various computing environments, the workstations don't communicate with each other within the same vicinity or the departments. Disabling this feature will help in prevention of BOTNETs spreading feature up to a great extent. The network administrators should establish VLANs and ACLs between several sub networks to minimize the exposure. Although this approach is not much appreciable, but it fits in the environment where there is a mix voice and data communication.

5) Providing Least Privilege: A central control mechanism must be implemented in a network where every user must not be given the administrative rights. This approach can minimize the propagation of the malware to infect the individual machines as the user have very limited and specific privileges.

6) Installation of Host-based Intrusion Prevention Application: IT managers should focus on taking additional measures for the security and protection by adding vulnerability to the specified network layers for example at points of contact between specific hardware and the software. Although this approach cannot fix the technicalities but still it prevents the system not to be exploited easily. Also these types of security applications are very expensive and very much typical to deploy.

7) Enhancement in the Monitoring of Traffic over Network: The monitoring of the network traffic can play a very essential part in preventing the BOTNET attacks. The enhancement and routine scheduling of the network traffic monitoring is essential and Network administrator must concentrate of that very seriously.

8) Filtering of data that is outgoing from Network: BOTNETs use to communicate with bot commander through remote severs. The agencies must stop these communications by prohibiting the unwanted traffic leaving from the network. A very essential tool for this purpose is Egress Filtering. Agencies should deploy Data Loss Prevention (DLP) solution.

9) Usage of Proxy Servers: Although it is impossible to block all the outbound traffic, but forcing the outbound traffic using a proxy server provides agencies a secondary choke point to monitor and control the out-bound data that is accessing the web.

10) Monitoring of queries generated by DNS: The workstations responds to DNS queries in a way is a pre sign of warning that workstation can get infected by a drone. Particularly, the responses with very low time-to live values should be seriously monitored by the network administrator. Monitoring helps the network administrator to act early as the attack gets stronger infecting a large are or might be whole network [17 – 21].

IV. Conclusion

BOTNETs are one of the most severe threats in the domain of network security. This paper addressed some of the attention-grabbing aspects of BOTNETs and provided a viewpoint as to why BOTNETs are so much dangerous and harmful in the field of network security. Hence it becomes very essential to aware the users regarding the threats that can be caused from this type of malware.

After the study and analysis, it was concluded that creation and prevention of BOTNETs can be considered as the cold war between the intruders that creates the BOTNETs and preventers that counters the attacks. The security experts are focusing on the prevention of new attacks making use of regression techniques in unsupervised learning algorithms to identify the malicious traffic pattern.

References

[1] Geer, "Malicious bots threaten network security," Computer, vol. 38, no. 1, pp. 18–20, Jan. 2005.

[2] Z. Zhu, G. Lu, Y. Chen, Z. Fu, P. Roberts, and K. Han, "Botnet Research Survey," in Computer Software and Applications, 2008. COMPSAC '08. 32nd Annual IEEE International, 2008, pp. 967–972.

[3] B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, and G. Vigna, "Your botnet is my botnet: analysis of a botnet takeover," presented at the Proceedings of the 16th ACM conference on Computer and communications security, 2009, pp. 635–647.

[4] "R. Vogt, J. Aycock, and M. Jacobson, Jr. Army of Botnets, 14th Annual Network and Distributed System Security Symposium, 2007, pp. 111-123. Reprinted in Chapter 10 of Botnets: A Cyber Threat, S. Puneet, ed., Icfai University Press, 2008, pp. 171-199." .

[5] Y. H. Moon, E. Kim, S. M. Hur, and H. K. Kim, "Detection of botnets before activation: an enhanced honeypot system for intentional infection and behavioral observation of malware," Secur. Commun. Netw., vol. 5, no. 10, pp. 1094– 1101, Oct. 2012.

[6] D. Dagon, C. C. Zou, and W. Lee, "Modeling Botnet Propagation Using

Time Zones.," in ResearchGate, 2006.

[7] W. T. Strayer, R. Walsh, C. Livadas, and D. Lapsley, "Detecting Botnets with Tight Command and Control," in Proceedings 2006 31st IEEE Conference on Local Computer Networks, 2006, pp. 195–202.

[8] "Measurements and Mitigation of Peer-to-Peer-based Botnets: A Case Study on Storm Worm." [Online]. Available: https://www.usenix.org/legacy/event/leet08/tech/full_papers/holz/holz_html/. [Accessed: 29-Sep-2015].

[9] B. J. Jansen, "Click Fraud," Computer, vol. 40, no. 7, pp. 85–86, Jul. 2007.

[10] F. Lau, S. H. Rubin, M. H. Smith, and L. Trajkovic, "Distributed denial of service attacks," in 2000 IEEE International Conference on Systems, Man, and Cybernetics, 2000, vol. 3, pp. 2275–2280 vol.3.

[11] M. Bailey, E. Cooke, F. Jahanian, Y. Xu, and M. Karir, "A Survey of Botnet Technology and Defenses," in Conference For Homeland Security, 2009. CATCH '09. Cybersecurity Applications Technology, 2009, pp. 299– 304.

[12] H. R. Zeidanloo, A. Bt Manaf, P. Vahdani, F. Tabatabaei, and M. Zamani, "Botnet detection based on traffic monitoring," in 2010 International Conference on Networking and Information Technology (ICNIT), 2010, pp. 97–101.

[13] D. Dagon, G. Gu, C. P. Lee, and W. Lee, "A Taxonomy of Botnet Structures," in Computer Security Applications Conference, 2007. ACSAC 2007. Twenty- Third Annual, 2007, pp. 325–339.

[14] K. Anestis, R. Brian, and H. David, "Wide-scale Botnet Detection and Characterization."

[15] P. Barford and V. Yegneswaran, "An Inside Look at Botnets," in Malware Detection, M. Christodorescu, S. Jha, D. Maughan, D. Song, and C. Wang, Eds. Springer US, 2007, pp. 171–191.

[16] W. Lee, C. Wang, and D. Dagon, Botnet Detection: Countering the Largest Security Threat. Springer Science & Business Media, 2007.

[17] K. A. Cole, R. L. Silva, and R. P. Mislan, "All Bot Net: A Need for Smartphone P2P Awareness," presented at the International Conference on Digital Forensics and Cyber Crime, 2011, pp. 36–46.

[18] "Indian Journals." [Online]. Available: http://www.indianjournals.com/ijor.aspx?target=ijor:ij mt&volume=1&issue=3&article=004. [Accessed: 29- Sep- 2015].

[19] M. R. Thakur, D. R. Khilnani, K. Gupta, S. Jain, V. Agarwal, S. Sane, S. Sanyal, and P. S. Dhekne, "Detection and prevention of botnets and malware in an enterprise network," Int. J. Wirel. Mob. Comput., May 2012.

[20] N.-Y. Lee and H.-J. Chiang, "The research of botnet detection and prevention," presented at the Computer Symposium (ICS), 2010 International, 2010, pp. 119– 124.

[21] "The Analysis of Botnet Transmission Model and the Prevention & Cure Methods--《Journal of Changzhou Institute of Technology》2008 年 06 期." [Online]. Available: http://en.cnki.com.cn/Article_en/CJFDTOTAL- CZGB200806009.htm. [Accessed: 29-Sep-2015].