ISSN 2349-9842, Volume 1, Issue 1, March 2014

INTERNATIONAL JOURNAL OF INNOVATIVE TRENDS AND EMERGING TECHNOLOGIES

DISCLOSURE OF BOTNET IN DNS USING ANOMALY APPROACH WITH HONEYPOT TECHNIQUE

[1]R.C.JENI GRACIA, [2]A.M.ARULRAJ

[1]M.E Student, Dhaanish Ahmed College Of Engineering,Email:jenigracia89@gmail.com

[2]Associate Professor, Dhaanish Ahmed College Of Engineering, Email:arulmtech@yahoo.co.in

Abstract--Botnet is the stealthy messaging communication in the network of compromised computers, that is controlled by a remote attacker using Domain Name System (DNS) as a stealthy botnet command and control channel. User intention-based Anomaly detection approach is used to identify anomalous DNS traffic on a infected host. It is used to detect the deviations of the host, which is infected by the botmaster. The Honeypot technique is to prevent the communication between the botmaster and the bot(infected host). This technique has the data control facilities to control traffic of outgoing suspicious connections. This experiments show that the User intention-based Anomaly detection is effective in detecting the infected host and the Honeypot technique gives the best performance in preventing the malware that happens by the botmaster.

Index Terms- Botnet, DNS, Anomaly detection , Honeypot technique

1 INTRODUCTION

A botnet is a network of computers on the Internet, has been compromised and is under the influence of a coordinated group of malware instances. Bots in the network run without the owners' knowledge, and send out transmissions (viruses) to other computers on the Internet. Botnets are controlled by a 'bot-master' through command-and-control (C&C) channels.

Although previously very common, IRC(Internet Relay Chat) command and control servers have fallen in popularity among botnet owners because IRC network traffic is easy to detect and may be easier to distinguish from other types of traffic, such as HTTP. In contrast to IRC, HTTP command and control methods are less interactive and responsive. HTTP command and control mechanisms can be prevented mainly by blocking access to domains that are known to serve as command and control systems.

DNS as carrier for botnet Command and Control seems to be getting popular. Regarding its usage as botnet C&C, DNS has not been seen so far. In network environments, DNS is usually one of the few protocols – if not the only one – that is allowed to pass without further ado. Thus botnet using DNS as Command and Control benefit from the fact that currently there is no specifically tailored detection mechanism, raises the probability for the botnet to remain undetected. Due to their immense size, they pose a severe threat to the community. With the help of honeypot technique can observe the people who form botnet.

The User intention based anomaly detection approach is used to detect malware behaviour at runtime. It is used for privacy preserving data leak detection. It detects what/who downloads files on the computer, where the packet is from, what/who causes outbound traffic and where the keystroke is from. The sensitive information from botnet that enables us to place a fake bot into a botnet.

The required information include:

- The IP-address of DNS and port number (optional) password to connect to DNS-server.
- Nickname of bot and identity structure.
- Channel to join and (optional) channel password.

A honeypot is tough to define because it is a new and changing technology and it can be involved in different aspects of security such as avoidance, detection and information gathering. It is unique in more general technology and does not solve a specific security problem. A honeypot is a highly flexible tool with applications in such areas as network forensics and intrusion detection. The purpose of this paper use the following definition: a honeypot is a security resource whose value lies in being probe about attack.

To maximize the strength of honeypot and minimise the risks involved in it, deployment should be carefully planned. The subsequent is a set of common honeypot deployment strategies:

1. Install honeypot alongside regular production servers. The honeypot will likely need to mirror some real data and services from the production servers in order to irresistible attackers.

2. Pair each server with a honeypot and direct suspicious traffic destined for the server to the honeypot.

3. Build a honeynet, which is a network of honeypot that imitate and replicate as actual or fictitious network.

However, honeypot do have their drawbacks, because they only track and capture activity that directly interacts with them, they cannot detect attacks against other systems in the network. By placing the honeypot in front of firewall, the risk for the internal network does not increase. The danger of having a compromising system behind the firewall is eliminated. This could be a special problem as soon as no additional firewalls are used to shield some resources or if the IP is used for authentication. A honeypot will attract and generate a lot of undesirable traffic like port scans or attack patterns.

By placing a honeypot outside the firewall, such event don't get logged by the firewall and an internal IDS system won't generate alerts. A lot of alerts would be generated on the firewall or IDS. Probably the biggest merits of the firewall or IDS, as well as any other resources, is that they haven't to be adjusted because the honeypot is outside the firewall and viewed as any other machine on the external network. Running a honeypot does not increase the risk of the internal network nor does it introduce new risks.

. Botnet with a Random topology (i.e., a dynamic master-slave or peer-to-peer relationship) have no centralized C&C infrastructure. Commands are injected in to the botnet via any bot agent. These commands are often "signed" as authentic, which tells the agent to automatically propagate the commands to all other agents.

Random botnet are highly resilient to shut down and hijacking because they lack centralized C&C and employ multiple communication paths between bot agents.It is often easy to identify members of the botnet by monitoring a single infected host and observing the external host to which it communicate with.

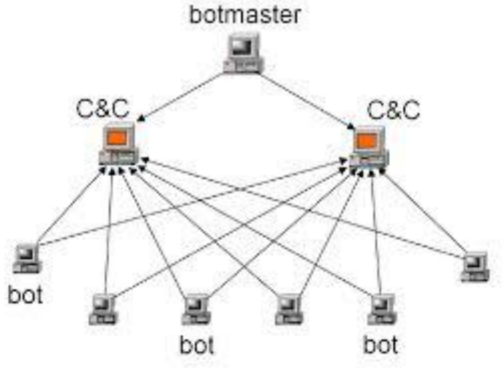

Fig 1.Architecture Botnet

The topology in multiple layers of DNS fluxing and redirection make some botnet highly resilient to shutdown or enumeration.

Our work systematic addresses using networking and data mining techniques.The technical contributions are summarized as follows:

- The Legitimate DNS is detected by the queries from the botmaster by the Botnet query detection algorithm.
- The detected queries from the botmaster is denied by the honeypot technique. It also deny the suspicious connections to the legitimate DNS.
- We propose this method to detect, from where the attack is, and also find the IP address of the attacker and deny it.

2 RELATED WORK

Serveral researches have been proposed to efficiently detect the legitimate DNS. In[2] EXPOSURE, a system that employs large-scale, passive DNS analysis techniques to detect domains that are involved in malicious activity. In our approach, based on the features that we have identified and a training set that contains known benign and malicious domains, it train a classifier for DNS names. It is beneficial only to monitor the use of the DNS system on a large-scale that indicate that a certain name is used as part of a malicious operation. A determined attacker who knows how EXPOSURE works could try to avoid the specific features and behavior that are looking in DNS traffic.In proposed processing the deviation in the system can be detected using Anomaly method. In this, the legitimate website can be detected by the traffic occurs by queries send from botmaster.

In[7],recent malicious attempts are intended to get financial benefits through a large pool of compromised hosts, which are called software robots or simply bots. It is remotely controllable by a server and can be used for sending spam, stealing personal information and launching DDoS attacks. The main contribution of this is to the development of an anomaly-based botnet detection mechanism by monitoring group activities in DNS traffic. The mechanism uses the information of IP headers and that enables to detect botnet, even though they uses SSH(Secure Shell) or any other channel encryption methods. But in the proposed system, User Intention based anomaly detection technique is used to detect the deviation of the user system that happens by the executable event.

Hao Zhang et al [12] proposed User Intention-Based Traffic Dependence Analysis for Anomaly Detection. They explain a novel approach that can be used for detecting anomalous traffic on a host. This scheme investigates direct and indirect dependencies in how a user interacts with applications and how applications respond to the user's requests following the specifications of the applications. By enforcing an application's correct responses to user actions, they are capable to identify vagabond events. Vagabond events are nothing but to outbound network events that are not generated by any user actions and may hence be due to anomalies.

Bait'n'Switch [7] is a honeypot response mechanism that redirects the attacker from valuable targets to a honeypot system. Bait'n'Switch is realized as a Snort inline extension. Whenever a successful attack is detected, the IDS drops the packets of the first attack and all further traffic from the host that initiated the attack is rerouted to a dedicated honeypot This process is hidden from the attacker so that he does not realize that he is not communicating with the original target anymore. The attacker's further interaction with the honeypot can later be analyzed and the production system is the protected from the attacker's further actions. The system reacts on attacks that are described in an IDS signature database and can therefore only react on previously known attacks.

In[6],it describe a new tool called DeWare (standing for detection of malware) for detecting the onset of infection delivered through vulnerable application. In this, it defines rules for identifying dependency between the system events and the user actions that initiate them. The host-based security protection against unauthorized system events. The stealthy events such as executable downloading and execution are detected.

It detects the legitimate websites that occurs malware, also control and confine their access to the file systems. Overhead of queries makes the network connection slow and sometimes it makes the connection cut off. In proposed system, the executable file can be detected using anomaly detection strategy and the queries from the botmaster can be blocked.

In[4],using k-Means clustering and a Euclidean Distance based classifier, it classifies DNS transactions of malware concerning DNS-C&C.It detects malware concerning DNS C&C usage based on DNS traffic.It detect the bot , that use DNS as the carrier by analysing the traffic. A technique is present to distinguish between DNS-based C&C and regular DNS communication in real world DNS traffic. Classifier that can distinguish purely malicious communication into DNS-based C&C and regular DNS communication. In proposed processing, the traffic can be detected by the user intention based anomaly detection method, it finds the deviation due to the traffic of queries.

The overall performance of various other techniques, methods and algorithms is not so far efficient.The detection of the traffic is done and also the executable events can be found. In proposed,the legitimate DNS which is used by the hackers is detected by the honeypot technique.

3 PROPOSED METHODOLOGY

1. Displaying links in legitimate DNS

Displaying links on Domain Names, links will contain some malware programs. By clicking that links malware programs sends our credential information to the attackers(bot master).The bot master can take over the control of the hacked Domain Names to get the up-to-date details. The legitimate DNS can display the links like logos, photographs or other images, location maps and similar items.

2. User hacked details

An admin user has full access to perform any operation on all organization accounts of which the admin user is a member. It can also set or reset an admin user's password, activate or reactivate on admin user, and get an admin user's activity feed. In this ,it shows the details of the user name, time and date of the user who enter into it. And the hacked domain name ,IP address can be seen in the list of hacked details of domain name.

3. Affecting Malwares

Domain Name has malware program, domain users click that link and automatically our credentials is send to hacker, they has to receive new attack commands and updates from attacker, or to submit stolen data. A C&C channel for a malware program needs to be reliable, redundant, non-centralized, and easily disguised as legitimate traffic.

Many malware operators used the Internet Relay Chat protocol (IRC) or HTTP servers to pass information. Malware operators constantly explore new stealthy communication mechanisms to evade detection. HTTP based C&C is difficult to distinguish from legitimate web traffic.

4. Finding Malwares:

The executable event which sends the credential information to the botmaster is detected. Because of queries from the botmaster to bot, traffic is occurred. DNS queries are usually issued by a host with temporal proximity. Data packets sent to and from a server in tunneled mode[1] .The deviation of the user's system can be found by using the anomaly detection method.And the Domain name used by the hackers can also be found.

5.Avoiding Malwares and Performance Evaluation

DNS-based stealthy command and control channel can be very powerful for attackers, the need for further research by defenders in this direction. Many websites contain content from multiple independent domains due to third-party content delivery, advertisements, or content mash up attackers. The honeypot technique is used to deny the communication to the botmaster. It deny the suspicious connections of the legitimate Domain Names. It also finds the botmaster who hack the user system and the details of the other Domain Names.

4 MITIGATION AND COUNTERMEASURE

In this section, countermeasures are chosen for a given attack scenario. The countermeasure serves the purpose of 1)Protecting the users system from being compromised and 2) making attack behavior stand prominent so that the attackers' actions can be identified.

System	Type of Attack	Number of Attack	sucessful
ns@me	Cmd.exe exploit	578	✓
ns@me	Code Red and similar	65	
ns@me	RPC based attacks	10	
ns@me	FTP based attacks	5	

Types of attack through botnet that compromised the user system.These attack can be blocked by the honeypot technique to the it@me system.

5 SYSTEM DESIGN

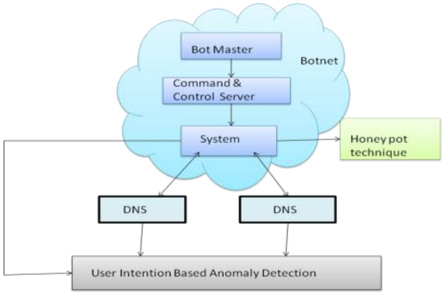

Fig 5.1:Architecture diagram for Botnet, honeypot technique,user intention-based anomaly detection method.

6 CONCLUSION AND FUTURE ENHANCEMENT

DNS based botnet C&C is more stealthy than application-based C&C and such a C&C system also beneficals from the decentralization of DNS. In this,the infected domain names causes malware to other domain names and makes it as a network to get the details from the Domain Names. The User intention based anomaly detection approach found out the infected Domain Names by the traffic caused by the bot master. The Honeypot technique blocks and avoids the suspicious connection from the infected Domain Names to explore the botnet.

Botnet use the Domain Name System to spread the malware into the host.It can be improved by how the honeypot technique can be used efficiently and avoid their exposure to botnet. In the future, the botnet can be detected and prevented in the mobile network.

7 REFERENCES

[1]Kui Xu,Member,IEEE, Patrick Butler,Sudip Saha,and Danfeng(Daphne)Yao,"DNS for Massive-Scale Command and Control,Member,IEEE june 2013.

[2]L. Bilge, E. Kirda, C. Kruegel, and M. Balduzzi, "Exposure:Finding Malicious Domains Using Passive DNS Analysis," Proc.18th Ann. Network and Distributed System Security Symp. (NDSS),Feb. 2011.

[3]D. Dagon, "Botnet Detection and Response, the Network Is theInfection," Proc. Domain Name System Operations Analysis and Research Center Workshop, 2005.

[4]C.J. Dietrich, C. Rossow, F.C. Freiling, H. Bos, M. van Steen, and N.Pohlmann, "On Botnets that Use DNS for Command and Control,"Proc. European Conf. Computer Network Defense, Sept. 2011.

[5]R. Villamarı´n-Salomo´n and J.C. Brustoloni, "Identifying Botnets Using Anomaly Detection Techniques Applied to DNS Traffic,"Proc. IEEE Fifth Consumer Comm. and Networking Conf. (CCNC),2008.

[6]K. Xu, D. Yao, Q. Ma, and A. Crowell, "Detecting Infection Onset with Behavior-Based Policies," Proc. Fifth Int'l Conf. Network and System Security (NSS), Sept. 2011.

[7] Alberto Gonzalez Jack Whitsitt. Bait'n'Switch. Technical report, Team Violating , http:// baitnswitch.sf.net.

[8] E. Kartaltepe, J. Morales, S. Xu, and R. Sandhu, "Social Network-Based Botnet Command-and-Control: Emerging Threats and Countermeasures," Proc. Eighth Int'l Conf. Applied Cryptography and Network Security (ACNS), pp. 511-528, 2010.

[9] M.V. Horenbeeck, "DNS Tunneling," http://www.daemon.be/maarten/dnstunnel.html, 2013.

[10] X. Hu, M. Knysz, and K.G. Shin, "Measurement and Analysis of Global IP-Usage Patterns of Fast-Flux Botnets," Proc. 30th Ann. Int'l Conf. Computer Comm. (INFOCOM), 2011.

[11]P. Butler, K. Xu, and D. Yao, "Quantitatively Analyzing Stealthy Communication Channels," Proc. Ninth Int'l Conf. Applied Cryptographyand Network Security (ACNS '11), pp. 238-254, 2011.

[12] D. Dagon, "Botnet Detection and Response, the Network Is the Infection," Proc. Domain Name System Operations Analysis and Research Center Workshop, 2005.

[13] DeNiSe, http://c0re.23.nu/c0de/snap/DeNiSe-snap-20021026.tar.gz, 2013.

[14] X. Shu and D. Yao, "Data-Leak Detection as a Service," Proc. Eighth Int'l Conf. Security and Privacy in Comm. Networks(SECURECOMM), Sept. 2012.

[15] K. Singh, S. Sangal, N. Jain, P. Traynor, and W. Lee, “Evaluating Bluetooth as a Medium for Botnet Command and Control,” Proc.Int’l Conf. Detection of Intrusions Malware Vulnerability Assessment (DIMVA), 2010.

[16] K. Singh, A. Srivastava, J.T. Giffin, and W. Lee, “Evaluating Email’s Feasibility for Botnet Command and Control,” Proc. IEEE Int’l Conf. Dependable Systems Networks with FTCS and DCC (DSN),pp. 376-385, 2008.

[17] D. Stefan, C. Wu, D. Yao, and G. Xu, “Cryptographic Provenance Verification for the Integrity of Keystrokes and Outbound Network Traffic,” Proc. Eighth Int’l Conf. Applied Cryptography and Network Security (ACNS), June 2010.