International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 4, Number 1 (2014), pp. 11-14

http://www. irphouse.com /ijict.htm

Generating a New Forensic Methodology to Investigate, Tracks Left by Hackers on Remote Access Trojan: (Fast Flux Network)

Dinesh.D

M.TECH-Information Security & Computer Forensic,
Department of Information Technology, SRM University, Chennai.

Abstract

Hacker, the word become so special all around the globe. The entire world plans to plot the community as the digital criminals who work for their benefits for money and their own desires ,hence it is to be considered because of activities such as Cyber Terrorism,Cyberthreats and so on. At this moment we should clearly get deep to the core how they actually commit in these crimes, as a result we can clearly understand the people with extreme knowledge and proficiency upon digital and computer intelligence. Many security mechanisms and surveillances techniques are taken by security professionals to plot their whole community and get them down. As a result in order to prevent their community they formulated a new methodology to keep hide their identity and fashionably they fabricated a new BOTNETmechanism said to be *Fast Flux Network (*FFN). Hereby, upon my research i Generate a forensic methodology to identify the attacker by the tracks he left on compromised host by generating a new system to monitor DNS ,Binaries, IP's records as inspired by ROKSO.

1. Introduction

One of the biggest threat to the internet users are malware which got priority now-a-days by enriching their terms by BOTS. BOT's are generally robots which are mean to do any work commanded by its master.BOTNET's collection (or) group of BOT's which are spread all through the network and works depend upon their commands done by the master, who spread it.Hence,these slaves are being pupated by master using Command and Control Servers***(C&C's).***In earlier times these servers are centralized and hence once by annihilating the binaries of botnet.exe it is easy for

forensic investigator to detect.Now-a-days it has been enriched by de-centralized***C&C's***so it becomes highly undetectable and it will be still resilience and sty anonymously by slaying numerous slave host as a proxy layer .This kind of ***C&C's*** are taken advantage and used by ***FFN's.***

1.1 Fast Flux Networks

Imagine a domain with 'n' number of IP addresses which can toggle in a very small time span denoted to be TTL .The hacker mainly uses this idea to generat*e fast flux network* a multiple numerous IP addresses in every 300ms for one domain. The hacker mainly host the phishing page or scam redirects to this web server which is malicious. Fast Flux Network is simply a domain with numerous multiple IP's.For example if a BOT client wanted connect to a network it gives a request, but the request is redirected to the DNS server which gives a reply with multiple IP's where they lay a proxy path to malicious webserver where an phishing pages are hosted.

1.2 How it is benefit to Hacker

Consider a situation where attacker post his Phishing pages to the webserver which can be done by changing the CName of the DNS.The victim who become slave to the C&C will be directed to the malicious webserver where the fastflux network is fabricated and hence by directing to the web server his/her IP addresses is added to the list for the toggling of IP address as discussed before and also there is an another chance to make use of the that particular host for the main attacking launch pad. When investigator starts his investigation it is very hard to plot him, because the ***C&C's*** that hacker mainly uses is away from the victim machine by laying many BOT clients as a proxy Path .MotherHost for the herding the bots is away from the network.So,it becomes a stealth proof for attacker and he makes use of this Fast Flux Network.

2. Detection Mechanism

2.1 Tradational Measures

Passive detection mechanisms are followed by security professionals and investigators to analysis behavior of bot.One great method handled are Intrusion Detection System(IDS),Intrusion Prevention System(IPS).Where this mechanism provide both on Network and even on Host .Hence forth the packets which enter both system and host is forwarded to the Analysis system which makes a blacklist of the entries and update to the firewall server which provides a registry of malware packets which is abstracted from the characteristic of their respective Binaries.

2.2 LOBSTER Inspiration

When the network size becomes bigger and inspection of packets through IDS,IPS is highly risk because due to the traffic load is high because of scalability of the network. Here comes the LOBSTER *(Large Scale Monitoring of Broadband based on Internet Infrastructure)* which has an architecture of de-centralized passive sensors to monitor the traffic of packets and their behaviors on the network. The main advantage of these

de-centralized architecture is if any one server is responsible for monitoring and it face the problem of traffic load the traffic is routed to the nearest lobster server by load-balancing system. So, the efficiency of monitoring is enhanced for administrators and investigators.

2.3 Sink-Holing

Technical countermeasure to take down the malicious webserver hosted by hacker done by he investigators. This is a simple analysis method by routing the traffic of the malicious server to the server made ditto, similar by the investigators with same static IP addresses.hence, thro and flow of data records of that particular malicious server is monitored by the investigators.

2.4 DNS Cache Snooping

Generally when user request domain for the service the request is taken to domain name system, this DNS system looks for the requested service where it looks for the requested domain and reply the user upon their request this conversation is stored in cache of DNS ,so when the same user request the same URL it provides a fast and reliable connection for the user i.e. The temporary storage of the particular domain,which is generally created by DNS based upon number of request and traffic routed to the particular domain.Here,the investigator installs a new inspection agent to annihilate and analyze the cache of each and every request by user upon domain.

This method of snooping of DNS provides a great scope of forensically investigate and to clearly monitor the flow of malicious data flow record packets.Hence,it is stored on snooping agent and those records are useful for fabricating a list of IP addresses and can be coined as a black list.

3. Proposal of Forensic System

3.1 ROKSO

(Register of Known Spam Operation)is a database of "Hard-core spam gangs" and their history of servers, databases and list of IP addresses which are used to spam.Which was created by SPAMHAUS(*www.spamhaus.org*).This database is taken in control of many ISP's to make their data more secured .ROKSO holds the collection of files related to spam and cyber threat malware binaries and the servers and domain in SBL and XBL as archives.

The above process of being moving to chest of ROKSO and determination of black list is done by examining the IP header, CNAME ,AS records and so on.

3.2 Analysis System on In and Out flow records

Analysis system which exactly works like the Network Interface Card,the system i proposed can be a useful for both the individual users and also to the investigator.When,normally user request for the service from the public network he/she uses browser as a medium .from where the REQ packet is sent .Now,this packet is moved to the system is proposed where it directs to the chest of ROKSO where it holds the list of black list and white list entries of DNS that checks the requested

packet whether,is mentioned on its database.The list of DNS information on ROKSO is stored on DNSBL(*Domain Name System Black List*) and DNSWL(*Domain Name System White List*).This practice of happening can be even vice versa,when some malicious spam mails and executable files which is initiated by any BOT master around the world will be monitored by SPAMHAUS and updated to the ROKSO,once updated the same is forwarded to analysis system that we installed on host.So,it never let the malicious entry ..Hence, user who is trying to connect the public network, the request packet is moved to the chest of ROKSO and check for its threat severity viz. Good, Bad or none. The same happens when the ACK and REP packets from any domain or host are trying to the chest of ROKSO and risk factor of particular properties are analyzed.

4. Conclusion

Hereby, I conclude that the forensic system i proposed would be a great solution of deploying a security mechanisms to the individual user and the larger network .This interface system can be even built on micro ships which can be compatible to every operating system especially designed to defend from spamming and also to peel the anonymity of the attacker's in fast-Flux networks.

5. Acknowledgement

Hence,i acknowledge that upon the inspiration of Honey pot,LOBSTER infrastructure i proposed my research work.To my extent of my knowledge i hope this would even help layman to access his physical assets and credentials in a well secured manner.

References

[1] Know yourenemy: Fast Flux Service Network. technical report ,July2007.
[2] atlat.arbor.net(ATLAS ARBOR Networks)
[3] ENISA(European Network and Information Security Agent)by Daniel Plohmann,Elmar Gerhard’s.
[4] See P. Mocka Petris, “RFC 1034: Domain names - concepts and facilities”, Nov. 1987,
[5] http://www.faqs.org/rfcs/rfc1034.html, and P. Mockapetris, "RFC 1035: Domain names -implementation and specification",