On Inferring Autonomous System Relationships In The Internet

shyamala.R(M.E,CSE)

vels university,chennai

sheelagowr.P(M,E,CSE)

Assistant professor ,vels university

Abstract-The Internet is affected by malicious activities from spam and phishing to malware and distributed denial of service. Much of it thrives on armies of compromised hosts, or botnet. The DDOS attack can be prevented by using a new technique called as token validation technique which can be automatically generated by the server, when the request is being made by the user. So that the attackers cannot run a massive number of queries through the victim search engine which makes the server down. The phishing attack can be prevented by using a new technique known as one time password (OTP) technique. OTP is a password that is valid for only one login session. The users receive the OTP via their mobile phone. This technique prevents the attackers from collecting sensitive information such as credit card number and account number. Attackers maintain the complete control of their botnet, and can conduct file stealth, file flooding, file erase attacks. This paper proposes an effective detection and prevention using honeypot.

Keywords:- Autonomous system, Botnet, DDOS, Honeypot, Phishing

I.Introduction:

The Internet is affected by malicious activities from spam and phishing to malware and distributed denial of service. Autonomous system consists of groups of compromised system used for malicious purposes on the internet. The blacklist is used to determine the Malicious AS. These blacklists either contains host names or IP addresses to be black listed. DDOS is characterized by an explicit attempt by an attacker to prevent the legitimate user from using resources. The phishing is a fake site attempts to collect sensitive data such as login credentials, credit card numbers, account numbers and social security numbers.

The overlay network enables IP Address among participating AS routers. The BGP as a vehicle for information exchange among AS that are participating in the scheme. The BGP routers periodically use update message to exchange routing information with each other.

The identification of the neighbor AS (Server or Peer) in the overlay network that has the responsible for the BGP update message that indicated this overlay neighbor in the topology. The building an overlay network of Autonomous System consists of in DDOS, Phishing, Botnet.

DDOS Attack consists of webpage through which Attackers attack the victim Web servers by HTTP GET requests (e.g., HTTP Flooding) and pulling large image files from the victim server in overwhelming numbers via the BGP Router. In

another instance, attackers run a massive number of queries through the victim's search engine or database query to bring the server down. Very large number of attackers simultaneously accesses a popular website, which produces a surge in traffic to the website and might cause the site to be virtually unreachable.

Phishing Attack detects the Phishing page through the application. It follows some terms to find the phishing pages, a request for personal details and redirecting the URL. It also noticed that phishers have spoofed sender's request and ask the victims not to reply the details. The BGP contains IP addresses, autonomous system numbers, organizations or customers that are associated with these resources. The client sends the request to the server via the BGP Router on the URL that is contained within the phishing request.

Botnet Attack consists of the bot master infects the peers that are the initial bots. Then, the initial bots infect the other bots in their peer list. The bots in the bot net sends the information about the bots in their peer list to the specified bot (that is called as 'Sensor Host'). This sensor host is determined by the bot master. The bot master retrieves the peer list information submitted by each bots in the botnet from the sensor host. The bot master can attack the bots in the botnet. Attackers maintain the complete control of their botnet, and can conduct file stealth, file flooding, file erase attacks. In computer security, honeypot is a general an effective attack detection technique. A honeypot is a special constructed or network trap designed to attract and detect malicious attacks.

II. Existing system

The existing system handles the web based attacks DDOS and Phishing. To prevent the DDOS attack, new technique has been introduced known as token validation. This token is automatically generated by the server, while the request is being made by the user. So the attackers cannot run a massive number of queries through the victim's search engine to bring the server down. The one time password helps prevent phishing attack. OTP is a password that is valid for only one login session. The users receive the OTP via their mobile phone. This technique prevents the attackers from collecting sensitive information such as credit card number and account number.

A. Disadvantages of Existing System

- OTPs are difficult for human beings to memorize.
- A cell phone may be lost, damaged, or stolen.
- In addition to threat from hackers the mobile phone operator becomes part of the mobile phone operator becomes part of the trust chain. In case of roaming, more than one using this information may mount a man-in-the-middle attack.
- Sometimes the server considers the legitimate user as a attacker.

III. Proposed work

In this section we have defined a model which will provide the following extension.

A.Usage of Botnets for Flooding Attacks:

A denial-of service(DoS) attack is an attempt by attackers to prevent an information service's legitimate users from using that service. In a DDoS attack, these attempts come from a large number of distributed hosts that coordinate to flood the victim with an abundance of attack packets simultaneously. The attackers may the botnets and other alternatives to launch the attack.

B. Bots:

The attacker uses the bots to generate huge number of packet to attack the victim by sending these huge packets as large traffic to generate flooding attack. The attacker first identifies the compromised servers in terms of security and controls the systems which are under the control of these compromised servers. The compromised system under the servers knows as the bot. normally the attacker communicates the bots by using the Internet Relay Chat (IRC) . IRC is the public network there the user can enter and communicate each other or with the groups openly.

The attacker launches the DDoS attacks through the bot by sending the commands using these IRC network. The DDoS attacks can be blocked or the detection can not be possible, but by identifying the IRC server one can block the packet to the victim.

C. Botnet:

Internet is the globally established network where different users or systems exist and provide the better scalability and openness to the users in terms of services. The open accessing of the internet allows different threats and one of the major threats is from large number of compromised computers also called as bots or Zombies and the group of these computers called as Botnet. By using these botnets the attackers performs the attacks on the victims by simply sitting in house, from offices or organization and any private or public network around the world. Every botnet or the group of compromised bots is controlled by a master commonly called as attacker or hacker. These botnets conduct various attacks which includes DDoS, e-mail spamming, key logging, click fraud, and spreading any malware to the victim. Compared to any attack the botnets consist s of pool of compromised bots and these are capable to conduct or damage the victim tremendously with collective power or capacity than the individual attacker. Example for these type of attacks are flooding, flash crowd and ports scan attacks there the attacker uses the botnet power to generate the large numbe of traffic to blocks the victim resources.

Attacking Behavior: During the preparation an attack, botnets normally generate a large amount of malicious traffic, which in turn can make possible of easy detection. Understanding the attacks require the attacking behavior and a lot more information can reveal important intelligence including the nature of botnet, purpose of hackers and the origin of hackers. The attacking behaviours can defined from the following four aspects:

- Infecting new hosts
- Stealing personal information
- Phishing and spam proxy
- DDoS

D. Infecting new hosts: Botnets often selects new hosts using same ways as the virus and worms do for attack. The method that botnets use to compromise new hosts is through social engineering and distribution of malicious emails. In general the botnet distributes the malware using the mail attachment. Scoail engineering techniques are used to trap computer users into executing the malware, which leads to the compromise of hosts.

Stealing sensitive information: Recent botnets have employed complicated tools to steal sensitive user information from compromised hosts. The most commonly used tools for stealing sensitive information at victim systems are keyloggers and network traffic sniffers. Keyloggers modify host operating system to spy on user activities and store user key strikes. Network traffic sniffers monitor network traffic sent over the subnet of the compromised host. The sensitive data is logged by these tools and then compiled into digested formats. Periodically , the data will be sent to their bot master various communication channels. Some commonly used methods are data through a designed IRC channel created by a botnet and in emails to a designated email address.

Sending spam: Botnets are widely used to broadcast spam for different attack purposes. Two major advantages for hackers to use botnets to distribute spam are that the victims cannot trace the spam back to the source for legal action, and botnets can distribute a much larger volume of spam because of the aggregate computing power and vast availability of bandwidth. While some spam is used into visiting certain malicious websites, which install malware on their computers by exploiting Internet browser vulnerabilities.

E. Distributed denial of service: A DDoS attack is probably one of the oldest botnet attack mechanisms. In the infancy of botnets, hacker began using botnets to launch DDoS attack against a number of large organization to consume all of their available platform CPU cycles and available bandwidth, effectively slowing their services down to crawl, or knowing out their services altogether.

F. Honeypots:

A honeypot is an effective tool for observing and understanding the behavior of intruder's tactics and intensions. A honeypot checks every packet transmitted to/from it, giving it the ability to collect highly determined and less noisy datasets for network attack analysis. Honeypots are trick computer resources set up for the purposes of monitoring and logging the activities of entities that probe, attack or compromise them. Honeypots can have many shapes and sizes, examples include dummy items in a database, low-interaction network components like preconfigured traffic sinks, or full-interaction hosts with real operating system and services.

Honeypot reduces the burden on the servers or the system in terms of detection and logging. By capturing the small data sets of high volume it reduces the false positive and also captures the unknown attacks.

IV. Proposed system:

The proposed system honeypot provide a mechanism for detecting and preventing botnet based attacks like file flooding, file stealth and file erase. Botnet attack consists of the bot master infects the peers that are the initial bots. Then the initial bots infect the other bots in their peer list. The bots in the botnet sends the

information about the bots in their peer list to the specified bot (that is called as 'Sensor Host'). This sensor host is determined by the bot master. The bot master retrieves the peer list information submitted by each bots in the botnet from the sensor host. Attackers maintain the complete control of their botnet, and can conduct file stealth, file flooding, and file erase attacks. Among those uncompromised systems the high configuration system acts as a honeypot.

A.Benefits of proposed system

- The honeypot is used to detect and prevent the botnet attacks.
- It reduces the burden of server (or) the system in terms of detection and logging.
- It effectively understands the behavior of intruder's tactics and intensions.
- It shows the peer list to its defenders.
- It deletes the peer list of the bot in its peer list.

V. Results:

Figure 1 shows Bot Master Works like infect, report, update, and retrieve

Figure 2 and 3 shows the work of bots.

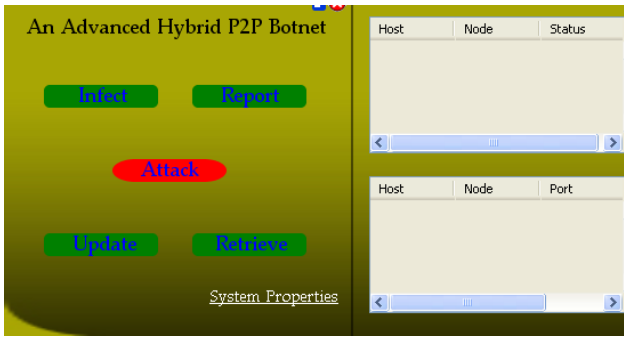

Fig 1: botmaster

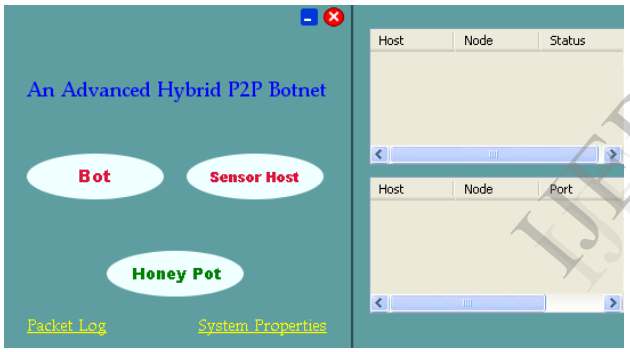

Fig 2:bot 1

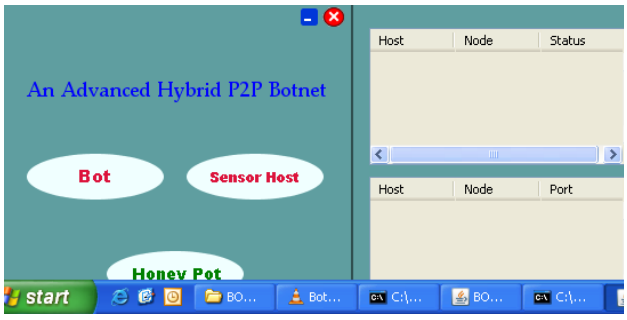

Fig 3: bot2

VI. Conclusion and Future Scope:

In the future, honeypots are going to become a critical weapon in a security professional's arsenal. Honeypot have the ability to catch new hacker toolkits and scripts, and are able to reduce the effectiveness of these tools in the wild by allowing security practitioners the capability to analyze these new tools. As we know in the security field we have a viable arms race between the discovery and exploitation of vulnerabilities and patching those discovered vulnerabilities. Security professionals can use honeypots to delay the time between when vulnerability is found and when that vulnerability is exploited by a malicious intruder. Also, security professionals can use to develop better methods and skills by gaining invaluable knowledge from watching an actual attack in progress.

A. Future Scope:

- In this implementation, we have not included the latest rules for virus and worms detection. This system can be exclusively designed for worm detection, so that the prevention can be made easier.
- Up gradation in hardware and software will result in a faster response time to detect unauthorized access.

References

[1] Craig A.shue, Andrew J.kalafut minaxi Gupta "Abnormally Malicious Autonomous System and Their Internet Connectivity".

[2] Cliff C-ZOU, Rgan cunningham "Honey pot-Aware advanced Bot net Construction and Maintenance".

Stone-gross.B, C.Kruegel, K.Almeroth, A.Moser, and E.Kirda, "FIRE: Finding Rogue Networks", in proc.ACSAC,2009, pp.231-240.

[3]Ramachandran.A and eamster,"Understanding the network level behavior of Spammers," in proc.ACMSIGOMM,2006,pp.291-302.

[4] “Route Views project”, University of Oregon Advanced Network Technology Center, Eugene, OR [Online]. Available: http:// www.routerviews.org/.

[5] Feldmann.A, O.Maennel,Z.M.Mao,A.Berger and B.Maggs,”Locating internet routing instabilities” in Proc. ACM SIGCOMM,2004, pp 205-218.

[8]“Malware block list,” Malware Patrol[Online]. Available:http://www.malwarepatrol.net//.

[9]“PhishTank”,OpenDNS,sanFrancisco,CA[Online].Available:http://www.spamhaus.org/xbl/index.lassc.

[10]“SURBL,”[Online].Available: http://www.surbl.org/.

[11] “Viruswatch mailing list,” NETpilot GmbH,Munich Germany [Online]. Available:http://lists.clean-mx.com/cgi-bin/mailman/listinfo/viruwatch

[12] X.Dimitropouos, D.Krioukov, M.Fomenkov, B.Huffaker, Y.Hyun, K.C.Claff, and G.Riley”AS relationship: Inference and validation, “ Comput, Common, Rev., vol.37, no. 1,pp 29-40 , Jan 2007.

[6] Kent.s, C.Lynn, and K.Seo “Secure border gateway protocol (S-BGP)” IEEE J.Sel.Areas Commun,Vol.18, no.4, pp.582-592,Apr.2000.

[7] Lanz Spitzner, Know Your Enemy: Learning with User-Mode Linux Building Virtual Honeynets using UML, , 20 December, 2002.