INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 4 (2017) PAGES 2282 - 2286
RECEIVED : 20.07.2017 PUBLISHED : 16.08.2017

Aug 21, 2017

A SURVEY ON DISTRIBUTED DENIAL OF SERVICE ATTACKS NETWORK APPLICATION

[1]R.Poornimadevi, M.Phil Scholar, Dept of computer science and Applications, KMG College of Arts & Science, Gudiyatham,

[2]V.S. Vinitha Janani Associate Professor PG and Research Dept of computer science and Applications, KMG College of Arts & Science, Gudiyatham.

Abstract:

During my research for this thesis ,In a DDoS attack, the attack uses widely distributed zombies to send a large amount of traffic to the target system, thus preventing legitimate users from accessing to network resources. At the same time, in recent years here are increasing interests in using path identifiers*PIDs* that identify paths between network entities as inter- domain routing objects, since doing this not only helps addressing the routing scalability and multi-path routing issues but also can facilitate the and adoption of different routing architectures. For instance, Godfrey *et al*. proposed pathlet routing ,which networks advertise the *PIDs* of paththroughout the Internet and a sender in the network constructs its select pathlets into an end-to-end source route.

Keywords: DDoS Attack, Inter Domain, PID.

1. INTRODUCTION

This research investigates the denial of service problem, in the context of services provided over a network, and contributes to improved techniques for modelling, detecting, and preventing denial of service attacks against these services. While the majority of currently employed denial of service attacks aim to pre-emptively consume the network bandwidth of victims, a significant amount of research effort is already being directed at this problem. This research is instead concerned with addressing the inevitable migration of denial of service attacks up the protocol stack to theapplication layer.Of particular interest is the denial of service resistance of key establishment protocols Along with the base technologies of PIDs and dynamic path identifiers, the thesis highlights and discusses the importance of supporting technologies like integration, Big Data analytics and Develops that enhance the business value of convergence. the conclusion, summarizes the whole work and pointsout its benefits and deficits. It also discusses the next steps that could be taken to improve the outcome. It sets questions for further work in this topic.

2. RELATED WORK

Distributed Denial of Service (DDoS) floodingattacks are one of the biggest concerns for security professionals.DDoS flooding attacks are typically explicit attempts to disrupt legitimate users' access to services. Attackers usually gain accessto a large number of computers by exploiting their vulnerabilitiesto set up attack armies (i.e., Botnets). Once an attack army hasbeen set up, an attacker can invoke a coordinated, large-scaleattack against one or more targets. Developing a comprehensive defense mechanism against identified and anticipated DDoSflooding attacks is a desired goal of the intrusion detection andprevention research community. Botnets can have hundreds of various implementations. IRC-based, Web-based, and P2P-based. Since the first two categories have been widely used to launch DDoS flooding attacks, we briefly explain them and introduce some of the tools that have been used in each category.

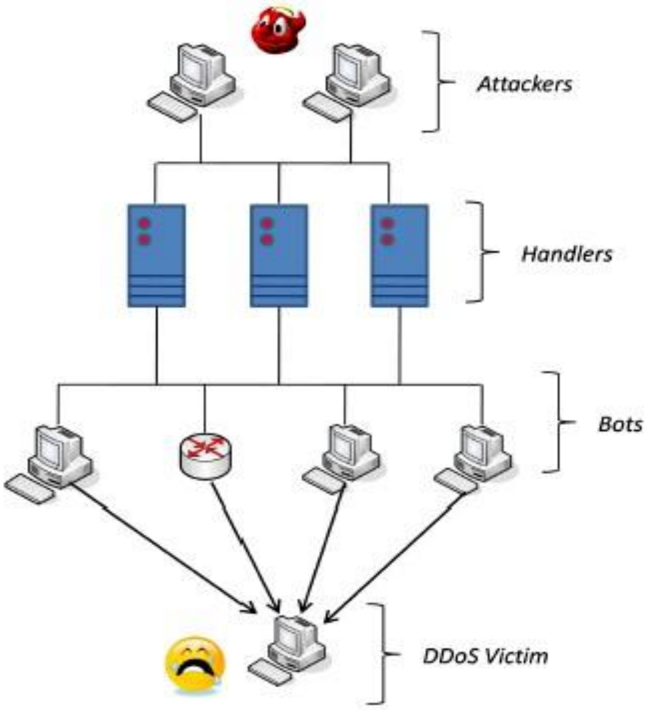

Fig.1. Elements of a Botnet

Some of the botnets could also provide their customers with some additional malicious services. For instance, McAfee reports that in a recent DDoS attack incident against South Korean government websites, the botnet that was used to launch the attack had employed resiliency techniques in order to evade its capture. The code also had destructive capabilities in its payload to destroy the compromised hosts, whenever required, by overwriting and deleting all the data on the hard drive. Usually by the time a DDoS flooding attack is detected, there is nothing that can be done except to disconnect the victim from the network and manually fix the problem. DDoS flooding attacks waste a lot of resources (e.g., processing time, space, etc.) on the paths that lead to the targeted machine; hence, the ultimate goal of any DDoS defense mechanism is to detect them as soon as possible and stop them as near as possible to their sources.

3. NETWORK ATTACKS

As the Internet becomes increasingly important as a business infra structure, the number of attackson it, especially denial-of-service attacks such as TCP SYN flooding,Teardrop,and Land,grows. Because of the weaksecurity in TCP/IP, we must take responsibility for protecting our own sitesagainst network attacks. The purpose of IP traceback is to identifythe true IP address of a host originatingattack packets. Normally, we can do thisby checking the source IP address field ofan IP packet.Because a sender can easily forge this information, however, it can hide itsidentity.

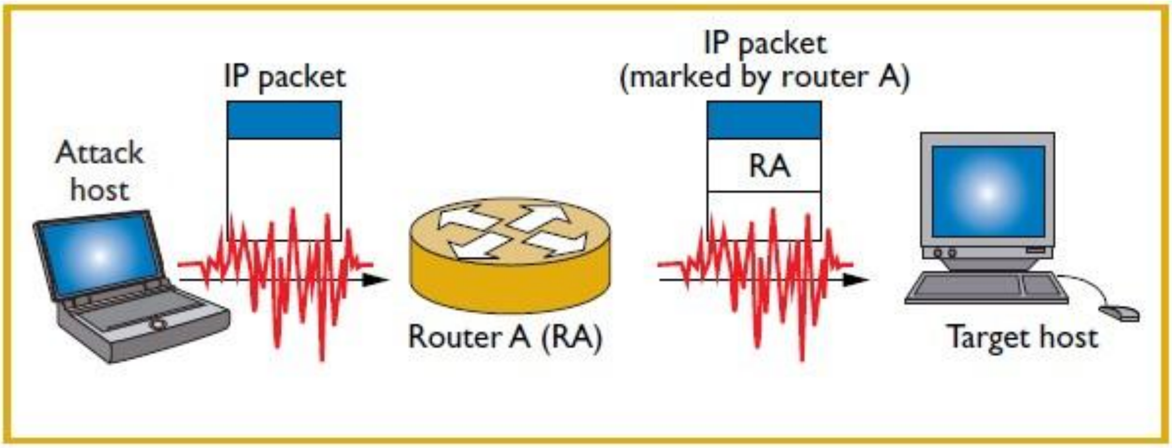

Fig.2. Packet marking.As packets travel through the network

If we can identify the true IP address ofthe attack host, we can also get information aboutthe organization, such as its name and the net-work administrator’s e-mail address, from whichthe attack originated. In packet marking, which is illustrated in Figure , packets store information about each router they pass as they travel through the network. The recipient of the marked packet can use this router information to follow the packet’s path to its source. Routers must be able to mark packets, however, without disturbing normal packet processing. With IP’s record route option, for example, the IP packet can store router addresses in its option field. Firewalls are widely used to protect networks against attacks, especially those coming from the Internet. Usually, firewalls control access based on source IP address, destination IP address, protocol type, source port number, and destination port number. For example, we can configure a firewall to deny any access to a WWW server except for WWW access using HTTP (destination port number 80). If an attacker attempts to exploit the WWW server using HTTP, however, the firewall cannot prevent it.

4. ANALYSIS

DDOS attacks can be mitigated through the use on on-premise inline devices, cloud based scrubbing solutions or a careful combination of these two technologies. IT shows that commercial customers are the most common target of volumetric attacks. These attacks, as we have discussed, are quick, easy and cheap to run and are commonly above 1Gbps in size. This means when choosing the right solution, organizations must be able to mitigate large volumes of traffic that would ordinarily swamp their ISP connection. In our view based on the global developments in DDoS attacks, a hybrid approach provides the most robust, cost-effective solution – providing the confidence that your investment will allow you to manage any incident, whatever the scale, at a predictable, budgeted cost. The company was being threatened with blackmail and approached NTT Security for emergency advice and assistance to mitigate what could have been a catastrophic attack for the business. DoS attack tools are commonly deployed on compromised systems. This deployment depends on the presence of exploitable vulnerabilities on systems and the ability of intruders to exploit those

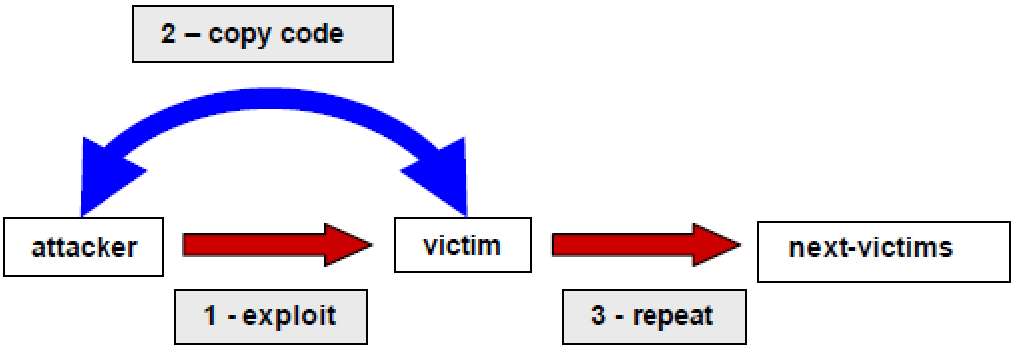

Figure 2 – Back-chaining propagation

vulnerabilities. We have seen an increase in the sophistication and use of 10 automated attacks, the use of blind targeting, and selective targeting of Windows-based systems and routers. Its intruders have developed and employed a higher degree of automation in multiple aspects of DoS attack technology deployment. we have seen a movement toward tools that automate scanning, exploitation, deployment, and propagation. Such tools a reactively being used to deploy DoS attack tools. Its attacks are usually highly automated and involve little human interaction during the execution of the attack. They also tend to be highly vulnerability-specific, often targeting systems that are vulnerable to one or a small number of particular exploitations. Other criteria are less central to the design and success of attacks based on blind targeting. It may or may not incorporate high degrees of automation and vulnerability-specificity. Selective targeting is generally based on using some criteria other than the target operating system or potentially exploitable vulnerabilities to select a target or target sector for attack. It were installed on carefully selected unix-based hosts. Systems were often manually tested for network connectivity, regular levels of network traffic, and available bandwidth before being used as handlers or agent in a DDoS network.

CONCLUSION

We have presented a number of real world examples of phishing attacks and the typical activities performed by attackers during the full lifecycle of such incidents. All the information provided was captured using high interaction research honey pots, once again proving that honey net technology can be a powerful tool in the areas of information assurance and forensic analysis. In each incident phishers attacked and compromised the honey pot systems, but after the initial compromise their actions differed and a number of techniques for staging phishing attacks were observed.In this thesis, I envision that these fundamental new capabilities will enable network security seamlessly utilize the cloud to obtain the resource benefits without incurring delays and jitter and without worrying about attack. By thus empowering network security computing will be able to break free of the fundamental constraints that have been keeping us from transform many areas of wireless services. We envision the future of applications will be built on top of a rich eco-system of basic network attack security.

REFERENCES

[1] J. Francois, I. Aib, and R. Boutaba, “Firecol: a Collaborative ProtectionNetwork for the Detection of Flooding ddos Attacks,” *IEEE/ACM Trans.onNetw.*, vol. 20, no. 6, Dec. 2012, pp. 1828-1841.

[2] OVH hosting suffers 1Tbps DDoS attack: largest Internet has everseen. [Online] Available: https: //www.hackread.com/ovh-hostingsuffers-1tbps- ddos-attack/.

[3] 602 Gbps! This May Have Been the Largest DDoS Attack in History.http://thehackernews.com/2016/01/biggest-ddos-attack.html.

[4] S. T. Zargar, J. Joshi, D. Tipper, "A Survey of Defense MechanismsAgainst Distributed Denial of Service (DDoS) Flooding Attacks," *IEEECommun.Surv.&Tut.*, vol. 15, no. 4, pp. 2046 - 2069, Nov. 2013.

[5] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denialof Service Attacks that Employ IP Source Address Spoofing," *IET Internet RFC 2827*, May 2000.

[6] K. Park and H. Lee, "On the Effectiveness of Route-Based PacketFiltering for Distributed DoS Attack Prevention in Power-Law Internets,"In*Proc. SIGCOMM'01*, Aug. 2001, San Diego, CA, USA.

[7] A. Yaar, A. Perrig, D. Song, "StackPi: New Packet Marking and Filtering Mechanisms for DDoS and IP Spoofing Defense," *IEEE J. on Sel. Areasin Commun.*, vol. 24, no. 10, pp. 1853 - 1863, Oct. 2006.

[8] H. Wang, C. Jin, K. G. Shin, "Defense Against Spoofed IP Traffic Using Hop-Count Filtering," *IEEE/ACM Trans. on Netw.*, vol. 15, no. 1, pp. 40 - 53, Feb. 2007.