CLASSIFYING WEBSITES FOR QUANTIFYING DDOS ATTACK IMPACTS

N.Srihari Rao[1], K.Munidhanalakshmi[2], Y.Sirisha[3], V.Shashidhar Reddy[4], and T.Geetha Sri[5]

[1,2,3]Assistant Professor, CSE Department, BIET Hyderabad, Telangana, India
[4]Student, ECE Department, BIET Hyderabad, Telangana, India
[5]Student, CSE Department, BIET Hyderabad, Telangana, India.

Abstract: Internet is the base infrastructure on which the distributed system of World Wide Web (WWW) is built. World Wide Web is a well organized collection of very large number of web pages with certain group of web pages forming a specific web site hosted on a web server. Any website with few or many web pages can be DDoSed to disable the web servers from serving legitimate users. But, through observation it can be perceived that some web servers are almost unaffected or affected but not manifested through these attacks. Therefore, these kinds of websites need not plan for and deploy DDoS protection mechanisms in reality. We conducted a detailed study on the existing websites on the Internet for classifying them into various categories which facilitates the quantifying of DDoS attack impacts on these websites.

Keywords: DDoS Attacks, Flash crowd, Hyper Text Transfer Protocol (HTTP), Attack Impact, DDoS Protection Vendors.

I. INTRODUCTION

For the WWW, there are two types of users. First category consists of legitimate users, which means these are the users without any malicious intent but with original requests to fetch information from web servers. The second category is of malicious users, which means these are the users with the intent of destroying the web servers and making the original web services not available to the legitimate users. The name of the condition that occurs due to the second category of users is Denial-of-Service (DoS) attacks [1]. If the malicious users select large number of systems that are distributed and vulnerable on the Internet and compromise these webservers, then we call such an attack Distributed Denial-of-Service (DDoS) attack.

1.1 Attack Model

Attacker sits on an anonymous and remotely located system in order to avoid being detected. A large number of distributed and vulnerable systems on the Internet [2] that are selected and compromised are called attack agents. Generally, attackers with some motivation to attack the web servers will set up an attacking system, which consists of a master program installed on it and running some vulnerability detection software in a wide range of unprotected and normal computers. Systems that are found with some vulnerability will be selected and installed with attack agent software. When the attacker wants to attack a particular web server, he may use command and control software to trigger the agents to send a flood of traffic towards the target. The agents generate packets with source addresses as original or fake source IP addresses based on the attacker's option. Also, the agents include the actual IP address of the victim in the destination field of request packets in order to send attack packets to the victim. In this way, large collection of agents will make the victim allocate different types of resources unnecessarily to these fake agent requests. Hence, the resources present at the victim web server will be consumed, legitimate users will be denied the services, and the victim goes to crash state.

1.2 Motivation

There exist different types of websites driven with different motivations. Some websites may target for making money, gaining popularity, personal satisfaction, or malicious purposes [3]. We want to classify all the general and currently existing websites into different categories at two levels. First level represents commonness of many second level categories (i.e. these are subcategories). Currently, there exists DDoS protection solutions [4] from many vendors but the process for evaluation of the DDoS protection necessity is not formalized as per our thorough research. Hence, we liked to concentrate on the problem of quantifying the DDoS attack impact and hence the degree of the necessity to install and deploy DDoS defense mechanisms for these different categories of websites.
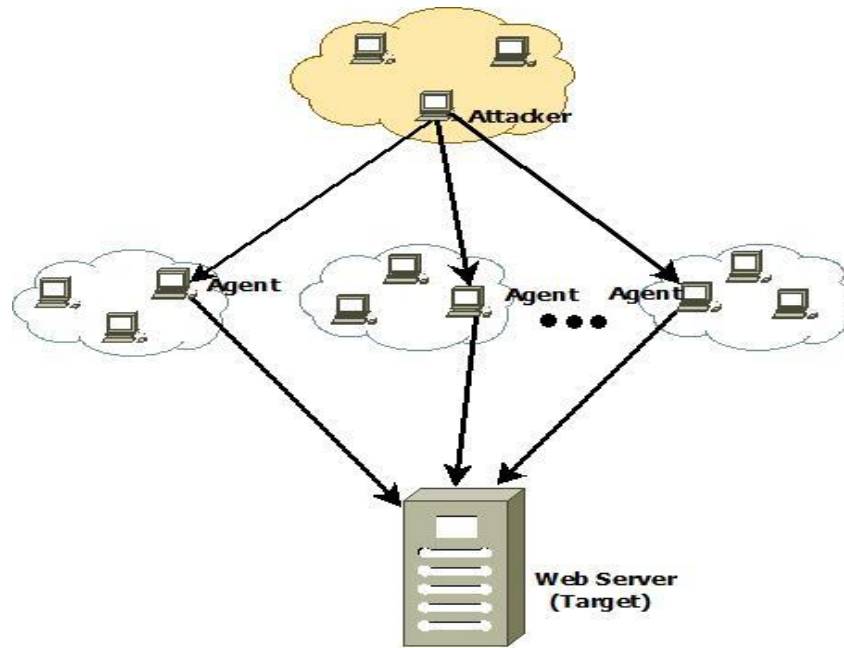
Figure 1. Attacker, Agents, and Victim in the Attack Model

II. RELATED WORK

DDoS protection becomes a necessity if the website that serves the users faces DDoS attacks and owner of the website feels and imagines the negative impact on his website in certain definable terms. Therefore there must be some mechanism to assess the impact on a website and evaluate the need for DDoS defense for that website in the presence of potential victims (persons). Currently, in the DDoS defense industry there are many DDoS Protection vendors [5] each of which has different mechanisms to back website owners and support availability of web servers to its users. The DDoS Protection solutions are currently provided by companies like Akamai, Verisign, Radware, Cloudflare, Arbor, Nexusguard, DOSarrest, F5 Networks, Neustar, Imperva Incapsula etc.

III. A CLEAN CLASSIFICATION OF VARIOUS WEBSITES ON THE INTERNET

After analyzing the (whole) types of websites that exist on the Internet, we came up with the clean classification of various websites. This classification facilitates the quantifying of DDoS attack impacts on these websites. Table 1 presents the detailed benefits and beneficiary categories for different types of websites on the Internet.

Table 1. Detailed Benefits and Beneficiary Categories for Different Types of Websites [7]

S.No	Website Category	Website Sub-Category	Description	General Owners of this Website	This Website is Useful for	Incentives from hosting this Website	WebsiteType ID (for effective
1	Money making sites	E-commerce site	Offers goods and services for online sales and offers online transactions for such sales	Some private company or an individual	Website Owners as sellers, Buyers	Money through advertising, and transactions	WWWA001
		Affiliate website	Sells or facilitates the sale of a third party's product	Some private company or an individual	Seller, Website Owners, Users	Money through advertising	WWWA002
		Affiliate agency website	Displays its custom content as well as content from other content providers for an agreed fee.	Some private company or an individual	Seller, Website Owners, Users	Money through advertising	WWWA003
		Classified ads site	Publishes offers of or requests for jobs, houses, apartments, used cars, and the like.	Some private company or an individual	Website Owners, Employers, Buyers, Sellers	Money through advertising	WWWA004
		Content site	Creates and distributes the original content	Some private company or an individual	User community, Website owners	Money through subscriptions and advertising	WWWA005
2.	Advertising-for-money sites	Crowdfunding site	Works as a platform to attract pre-purchase of products or donations from audience to fund the projects	Some organization or an individual	Website owners	Funding for projects, money through donations	WWWB001
		Brand-	Creates an online experience	Some	Website owners,	Money through	WWWB002

		building site	of brand but does not sell anything through these sites	organization or an individual	sellers	brand building and advertising	
3.	Advertising only not-for-money sites	Celebrity site	Includes information that elevates the personality figure of a celebrity or a public figure.	An individual	Website Owners, celebrity, fans	Personal elevation, reputation for being on the web	WWWC001
		Personal website	Contains information about an individual or a small group that he wishes to include	Individual	User community, Website owners	Personal elevation, reputation for being on the web	WWWC002
		Political site	Includes information about a certain candidate, political party, political humor. It may campaign for elections or may stage people's voice on political views.	Some organization or an individual	User community, Website owners	Personal elevation, reputation for being on the web	WWWC003
4	Service cum Advertising sites/ Service cum money collecting sites/ Service cum donation making sites	Social networking site (Community site)	People can use these sites to build social networks or social relations with other people who share similar personal or career interests, activities, backgrounds or real-life connections. People can share media such as pictures, videos, music, blogs, games and web applications etc with others.	Some private company or an individual	User community, Website Owners	Money through advertising, reputation from serving	WWWD001
		News site	Distributes news, politics, and commentary	News organizations	User community, Specific news organization	Money through advertising, reputation from serving	WWWD002
		Dating sites	People can find other people looking for a long-term, short-term relationships like dating, or short encounters or friendship	Some private company or an individual	User community, Website owners	Money through advertising and online site registrations, personal impression through user's satisfaction	WWWD003
		Photo sharing sites	Digital photos can be shared with the online community	Some private company or an individual	User community, Website owners	Money through advertising, reputation from serving	WWWD004
		Media sharing sites	Enables users to upload and view multimedia content	Some organization or an individual	User community, Website owners	Money through advertising, reputation from serving	WWWD005
		Gallery website	Useful as a gallery such as an art gallery or photo gallery	Some organization or an individual	User community, Website Owners	Money through advertising and subscription, reputation from serving	WWWD006
		Forum website	Conversations can be held by users in the form of posted messages	Some organization or an individual	User community, Website owners	Money through advertising, reputation from serving	WWWD007
4		Question and Answer (Q&A) site	People can ask questions and get answers on this site.	Some organization or an individual	User community, Website owners, Sellers	Money through advertising, reputation from serving	WWWD008
		Review site	Product or service reviews may be posted by the users on this site	Some organization or an individual	User community, Website owners, Sellers	Money through advertising, reputation from serving	WWWD009
		Religious site	Places of worship may be advertised in this site. Follower's faith may be encouraged through inspirations using this site.	Some organization or an individual	User community, Website owners	donations through advertising, reputation from serving	WWWD010
		Mirror website	Website that is a replication of another website. It is useful in the case of spikes in user visitors and provides multiple sources of the same information. Provides reliable access to large downloads.	Some organization or an individual	User community, Website owners	Money through advertising, reputation from serving	WWWD011
		Search engine site	Provides useful links to the material or particular web	Some organization or	User community, Website owners,	Money through advertising,	WWWD012

			sites relevant to particular keywords	an individual	sellers	reputation from serving	
		P2P/Torrents website	Torrent files are indexed in this site	Some organization or an individual	User community, Website owners	Money through advertising, reputation from serving	WWWD013
		Archive sites (Data Repository sites)	Preserve important and valuable electronic content that is thought to be no longer existing in future	Some organization or an individual	User community, Website owners	Money through subscriptions, advertising, reputation from serving	WWWD014
		Blog (Web log)	Provides for online diaries that include discussion forums, editorial section of a news paper to express blogger's ideas on anything, blog about a certain subject	Some organization or an individual	User community, Website owners, sellers	Money through advertising, reputation from serving	WWWD015
	Service cum Advertising sites/ Service cum money collecting sites/ Service cum donation making sites	Webmail site	Provides a web mail service	Some organization	User community, Website owners, sellers, buyers	Money through advertising, online services, and reputation from serving	WWWD016
		Web portal	Works as a beginning point or gateway to other useful resources on the internet or intranet	Some organization or an individual	User community, website owners, sellers, buyers	Money through advertising, online services, and reputation from serving	WWWD017
		Government Payment Service sites	Enable online transactions for payments for various services offered, penalties to specific organizations.	Specific government	Citizens, Specific government	Money, Respect and reputation from serving	WWWD018
		Comparison website	Provides information to compare different products or services online	Some organization or an individual	User community, website owners, sellers, buyers	Money, Respect and reputation from serving	WWWD019
		Job Portal	Shares information about latest job openings to job seekers	Some organization or an individual	Employees, employers, user community, website owners, sellers, buyers	Money from enrollment in the web site, reputation from serving	WWWD020
5	Service and self-advertising sites	School site	Teachers, students, or administrators can post information related to the events at their schools.	Specific institution	User community, Website owners	Money through self-advertising, reputation from serving	WWWE001
		Business information website	Provides information to the public about the company rather than transacting business or providing other services.	Specific organization	User community, Specific organization	Money through advertising, reputation from serving	WWWE002
6	Service sites	Government Information sites	Local, departmental, state, or national governments of a country can offer varieties of information on rights and rules for its citizens.	Specific government	All levels of governments, Citizens	Respect and reputation from serving	WWWF001
		Non-profit Corporate sites	Offers free services to its user community	Specific organization	User community, Specific organization	Reputation from serving	WWWF002
		Wiki site	Users collaboratively edit the content meant for multipurpose	Specific organization	Website owner, user community	Reputation from serving	WWWF003
7	Malicious sites	Attack sites	Attack computers which visit this site for the first time by downloading a file.	Some organization or an individual	Website owner	Loss for User community to fulfill his malicious intentions	WWWG001
		Gripe sites	Used to criticize a person, place, corporation, government or institution	Some organization or an individual	Website owner	Loss for criticized people to fulfill his malicious intentions	WWWG002
		Phishing sites	Used to fraudulently acquire sensitive information such as credit card details, and passwords by pretending to be a trustworthy person or business in an electronic communication	Some organization or an individual	Website owner	Loss for user community to fulfill his malicious intentions, and money through fraud	WWWG003
		Fake news websites	Publish fake news stories, in order to deceive visitors and profit from advertising	Some organization or an individual	Website owner	Loss for user community to fulfill his	WWWG004

						malicious intentions, money through fraud	
		Scraper sites	Duplicate the contents of another site without permission from that site and earns revenue from advertising or in other ways	Some organization or an individual	Website owner	Loss for the original site to fulfill his malicious intentions	WWWG005
		Shock sites	Include images and other material which is offensive to the majority viewers	Some organization or an individual	Website owner	Loss for the user community to fulfill his malicious intentions	WWWG006
8	Entertain ment and money making sites	Humor sites	Satirizes, parodies or amuses the audience	Some organization or an individual	User community, Website owners	Money through advertising, charges for entertaining content	WWWH001
		Gaming websites (Gambling websites)	Allows users to play online games such as rummy, gambling etc.	Some organization or an individual	User community, website owners	Money through advertising, gaming charges, money betting	WWWH002

The current need of the hour is to devise mechanisms that have the ability to determine whether a particular website on the Internet requires DDoS protection plan. In order to do this, DPVs base their judgements for DDoS protection-necessity on certain factors. Intuitively, according to the degree of DDoS-protection-requirement we can put the website categories from high to low in the order of:

1. Money Making Sites
2. Advertising for Money Sites
3. Service cum Advertising Sites
4. Entertainment and Money Making sites
5. Service and Self-advertising sites
6. Advertising-only not for Money sites
7. Service Sites

However, malicious sites need not be protected because they are under the control of hackers who are cyber criminals. These malicious sites need to be strongly opposed from existing and operating in the cyber world in order to keep the cyber world free of cyber criminal activities. Currently, standard evaluation procedure or mechanism does not exist for determining the degree of necessity for DDoS protection. Hence we like to take up the task of devising a set of standard evaluation criteria for determining the degree of DDoS defense necessity.

IV. CONCLUSIONS AND FUTURE SCOPE

We considered almost all the different types of websites that exist on the Internet for our exhaustive study that facilitates in quantifying the DDoS attack impacts and therefore the degree of necessity of DDoS Protection for various categories of web sites. We highlighted the least projected but, significant features till now of the websites that are actually very much useful to envisage the requirement or non requirement for subscription to the DDoS Protection services. We perceived that not all web servers are equally affected or damaged [11] through DDoS attacks as some web servers are almost unaffected or affected but not manifested through these attacks. Therefore these kinds of web sites need not plan for and deploy DDoS protection mechanisms in reality. We would like to propose a framework that acts as an intelligent recommender in the hands of DDoS Protection Vendors (DPVs) for recommending/non recommending the clients who look for or approach for DDoS Protection plans for their websites.

REFERENCES

[1] N.Srihari Rao, K.Chandra Sekharaiah, A.Ananda Rao. (2016) "A Survey of Discriminating Distributed DoS Attacks from FlashCrowds." in Springer Computer Science Proceedings, CCIS Series (SmartCom 2016), pp. 733-742.

[2] N.Srihari Rao, K.Chandra Sekharaiah, A.Ananda Rao. (2017) "A Survey of Distributed Denial of Service (DDoS) Defense Techniques in ISP Domains." in 5th International Conference on Innovations in Computer Science and Engineering (ICICSE-2017).

[3] J.Ramesh Babu, K.Chandra Sekharaiah, N.Srihari Rao. (2017) "Adaptive Management of Cybercriminal, Maladaptive Organizations, in the Offing, that Imperil the Nation." in Tech-Report-JNTUH-CHANDRG-RB-NSRAO-1.

[4] N. Srihari Rao, Prof. K. Chandra Sekharaiah and Prof. A. Ananda Rao, An Approach to Distinguish the Conditions of Flash Crowd Versus Ddos Attacks and to Remedy a Cyber Crime. International Journal of Computer Engineering and Technology, 9(2), 2018, pp. 110-123.

[5] Top 10 Distributed Denial of Service (DDoS) Protection Vendors https://www.esecurityplanet.com/products/top-ddos-vendors.html

[6] Why do you need on-premise DDoS protection? URL: https://www.arbornetworks.com/blog/insight/why-do-you-need-on-premise-ddos-protection/

[7] Cloudflare Pricing http://www.Cloudflare.com/plans

[8] Protect Against DDoS Attack, URL: https://www.cloudflare.com/ddos/

[9] DDoS Protection Services by Business.Com Editorial Staff URL: https://www.business.com/categories/best-ddos-protection-services/