Distributed Denial of Service (DDoS)

Clarence Kimbrell Jr.

Cyber Security

CYSE 250

Old Dominion University

Abstract

The majority of us who use the internet or technology daily hardly ever think of the huge risk we are taking just by turning them on. Since the majority of the time people will not be affected by mass hacker attacks are information breaches. Although they occur thousands if not millions of times every day which should not be a surprise to anyone, and it is usually shocking when you are affected by it. When we access the internet, we are lending our trust to businesses and cooperation with little to no sort of agreement that our information is the top priority. This should frighten most people because this shows that everyone is vulnerable to attacks at any level of security, no matter what precautions were taken. Massive websites like Facebook, Twitter, and Yahoo have all fallen victim to these types of attacks. Those companies only spend millions of United States dollars trying to prevent these types of occurrences and still fall short.

Introduction

Most older generations will have concluded that the internet is not only a miracle but a privilege and service. Younger adults and kids of today's generation have yet to realize this because they grew up with technology their entire lives. Since the internet and technology are so widespread and can reach from the furthest points on earth and join them together, you eventually going to

run into people with malicious intent. This is a small group of people but as the saying goes the minority makes the loudest noise. This is a good thing because it will expose how easy it is for some hackers to get around millions of U.S. dollars in equipment to prevent such attacks. This cycle of hacking will sadly never end and will only keep getting more intense and threatening. The most famous attacks that occur thousands if not millions of times a day are the following phishing, bait and switch, key logging, and denial of service attacks. In this paper, we will discuss famous attacks, understand how they work, and prevention.

Distributed Denial of Service

Distributed Denial of Service is a common practice among hackers that overload a server with requests. There have been countless distributed denial-of-service attacks throughout the history of the internet, and they are only getting worse. They are so common that most people know the act of it by its acronym DDoS, but most people do not know what the term exactly means. The main focus is to restrict access to a program, server, or even household internet connection. These attacks have been in the media showing how vulnerable major corporations are. Some of these types of attacks even have been recorded to prevent areas of a population. Many hackers that choose this method of disruption are seeking something in return that no person or company should have to agree to. That is why nearly every company that has an online presence is seeking a way to prevent such things that could potentially ruin a business or hurt a group of individuals.

According to many sources on the attacker's side of the distributed denial of service, there is little to no arrangement or preparation. Attackers seek to find easily exploitable systems or flaws in security measures and use them to begin and maintain distributed denial of service attacks. An unsecured site or a household could become rapidly disrupted by the mass amounts of requests or packets being sent to them. This can cause permanent damage to a server for a business or a router in a household in some cases. As stated earlier since the internet is so widespread spread

anyone can simply look up the tools necessary to conduct one of these attacks and wreak havoc on anything they so wish.

There have been thousands of recordings of distributed denial of services around the world since the internet is practically everywhere. The most famous one occurred very recently in 2020 and was carried out on one of the world's biggest companies, Google. These types of attacks as stated previously are only going to occur more often and they are going to be more threatening. The biggest known distributed denial of service attack only occurred last year which should be a wake-up call to everyone that uses the internet or technology on a day-to-day basis. In the years to come and potentially even this year, there will be some type of distributed denial of service attack to overthrow the one that was carried out on Google just last year. Hackers in China were able to find a hole in Google's security and conducted a distributed denial of service attack that sent two point five terabytes of packets flooding Google's servers.

Known Methods

There are countless types of distributed denial of services attacks and only a few have been documented. It is very hard to keep a list of known types because they change so often. Consider the scenario where an attack occurs, then the organization or website that is the victim will resolve the issue and prevent that certain type of attack. In the future, they could still be attacked by using a different method so it leaves websites, organizations, and businesses still vulnerable. We have documented a few similar attacks and classified them. They are the following, application layer attack, volume-based attack, and protocol attack. Application attacks are when attackers target the web server and seek vulnerabilities in Windows. Volume-based attacks are the attacks that most people think of when they hear the term distributed denial of service. This floods the bandwidth of a server or router with packets and disrupts the flow of intercepting packets. Lastly, protocol attacks disturb server resources for the victim's web server. Each one of these categories has hundreds of different known methods of use. For example, the Ping of Death is a volume-based attack that sends the maximum packet size repeatedly until the web

server crashes. Most if not all web servers cannot withstand such mass amounts of packets per second that it will try processing them and lead them to fail. Smurf attacks fall under the category of protocol attacks. They are when a large number of packets are being sent to a victim's web server and creating fake ping messages. This type of attack can last days on end if the attacks so which. So big corporations and businesses need to be prepared and monitor collected data. Another attack is called a TCP SYN Flood it is also called a three-way handshake. An attacker sends fake packets to a victim and hopes that it establishes a connection then is sent to a web server so it creates a three-way handshake. Once a connection is established it allows a hacker to flood the web server through a victim's packets. These are just the known methods of distributed denial of service attacks. New ones are being developed nearly every day and carried out without documentation to the public until years after the problem is solved.

Prevention

It is hard to believe that most distributed denial of services by big corporations or companies are undetected. As more time passes the complexity of these attacks is only getting more in-depth. Most companies or corporations wish it could be as easy as installing an antivirus but to prevent these types of attacks they need to completely create something from the ground up to even make a difference. Many companies and businesses are using this listed software that is built specifically for distributed denial of service, and they are Indusface AppTrana, SolarWinds Security Event Manager, and countless others. ShadowNet is another great tool that many organizations use, its first goal in distributed denial of service is to detect the problem before it gets out of hand. It monitors the number of packets being received and it keeps note of a large number of packets to see if it will keep increasing. This ensures that ShadowNet can provide lightning-fast results and with great accuracy when detecting an attack rather than leaving it to the servers that host businesses' websites. Most if not all prevention systems put in place follow a relatively similar model that can be altered to their needs. Some are designed specifically from attacks they have received in the past and others try to protect themselves from future attacks

they have not experienced. They are simpler things that can be done without needing to completely create a new defense system and they are, congestion restraints, minimizing collateral damage, and accessible tracebacks. These few things can prevent or hinder an attacker's chances of performing a direct denial of service attack. One thing that needs to be known about implementing security measures they need to be distributed just as the attacks are. Many reports state that there is no end-all system or software that can be put in place to provide ongoing, forever-lasting security. That is why it is so important for companies to update security measures as frequently as possible.

Conclusion

As we all know now distributed denial of service is a common practice among hackers and people with malicious intent. Cooperation and businesses need to understand when they fall victim to these types of attacks it puts everyone involved at risk not just the server in question. There are many ways that they can implement these new strategies to combat this, and prioritize it, and make it the most important. The internet is often referred to as the wild west and there is never going to be a shortage of attacks and crimes committed over the internet. More people should understand all forms of internet security before lending their trust to big-name businesses and corporations that time and time again fall victim to all forms of attacks. Simply just stating that there are precautionary measures is not enough they need to provide evidence for their claims as often as possible. All in all, these distributed denial of service attacks are being prevented every day and will continue to go on as long as we use technology.

References:

Bhandari, A., Sangal, A. L., and Kumar, K. (2016) Characterizing flash events and distributed denial-of-service attacks: an empirical investigation. *Security Comm. Networks*, 9: 2222– 2239. doi: 10.1002/sec.1472.

Bhardwaj, Ketan, et al. "Towards IOT-Ddos Prevention Using Edge Computing - Usenix." *Towards IoT-DDoS Prevention Using Edge Computing*, 2021, https://www.usenix.org/system/files/conference/hotedge18/hotedge18-papers-bhardwaj.pdf.

F. Lau, S. H. Rubin, M. H. Smith, and L. Trajkovic, "Distributed denial of service attacks," Smc 2000 conference proceedings. 2000 ie International Conference on Systems, Man, and Cybernetics. 'cybernetics evolving to systems, humans, organizations, and their complex interactions' (cat. no.0, 2000, pp. 2275-2280 vol.3, doi: 10.1109/ICSMC.2000.886455.

Mahjabin T, Xiao Y, Sun G, Jiang W. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks. December 2017. doi:10.1177/1550147717741463

Mirkovic, J. (2003). *D-WARD: Source-end defense against distributed denial-of-service attacks* (Order No. 3121225). Available from ProQuest Dissertations & Theses Global. (305341918). http://proxy.lib.odu.edu/login?url=https://www.proquest.com/dissertations-theses/d-ward-source-end-defense-against-distributed/docview/305341918/se-2?accountid=12967

Mohd Azahari Mohd Yusof, et al. "Detection and Defense Algorithms of Different ... - Ijetch.org." *Detection and Defense Algorithms of Different Types of DDoS Attacks*, Oct. 2017, http://www.ijetch.org/vol9/1008-ED003.pdf.

Muhammad Asad, Muhammad Asim, Talha Javed, Mirza O Beg, Hasan Mujtaba, Sohail Abbas, DeepDetect: Detection of Distributed Denial of Service Attacks Using Deep Learning, *The Computer Journal*, Volume 63, Issue 7, July 2020, Pages 983–994, https://doi.org/10.1093/comjnl/bxz064

Osanaiye, O., Cai, H., Choo, KK.R. *et al*. Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing. *J Wireless Com Network* **2016,** 130 (2016). https://doi.org/10.1186/s13638-016-0623-3

Paul Rubens, et al. “How to Prevent DDoS Attacks: 6 Tips to Keep Your Website Safe.” *ESecurityPlanet*, 28 Jan. 2021, www.esecurityplanet.com/networks/how-to-prevent-ddos-attacks-tips-to-keep-your-website-safe/.

Salim, M.M., Rathore, S. & Park, J.H. Distributed denial of service attacks and its defenses in IoT: a survey. *J Supercomput* **76,** 5320–5363 (2020). https://doi.org/10.1007/s11227-019-02945-z

Sekar, Vyas, et al. “Lads: Large-Scale Automated Ddos Detection System.” *Check out the New USENIX Web Site.*, 9 May 2006, www.usenix.org/legacy/event/usenix06/tech/full_papers/sekar/sekar_html/.

S. T. Zargar, J. Joshi and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," in IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2046-2069, Fourth Quarter 2013, doi: 10.1109/SURV.2013.031413.00127.