ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

EVOLUTION OF DDOS ATTACKS IN STRATEGY AND TACTICS

M.PadmavathyM.Sc (CS)., M.Phil.,
Research Scholar, Department of Computer Applications,
School of Information Technology, Madurai Kamaraj University,
Palkalainagar, Madurai – 625021.
E-Mail: padmaphd1@gmail.com

Dr. M. Ramakrishnan, M.E., Ph.D., Ph.D.
Professor and Head Department of Computer Application
Chairperson - School of Information Technology Madurai Kamaraj University
Madurai – 625 021.

Abstract

The volume, size and sophistication of distributed denial of service (DDoS) attacks are increasing rapidly, which makes protecting against these threats an even bigger priority for all enterprises. A DDoS attack may sound complicated, but it is actually quite easy to understand. A common approach is to "swarm" a target server with thousands of communication requests originating from multiple machines. In this way the server is completely overwhelmed and cannot respond anymore to legitimate user requests. Another approach is to obstruct the network connections between users and the target server, thus blocking all communication between the two – much like clogging a pipe so that no water can flow through. Attacking machines are often geographically-distributed and use many different internet

connections, thereby making it very difficult to control the attacks. This can have extremely negative consequences for businesses, especially those that rely heavily on its website; E-commerce or SaaS-based businesses come to mind. Most attackers have moved to using HTTP-controlled command servers or have even started using peer-to-peer (P2P) networks...

Key Words: (DDoS), Distributed Denial of Service, Peer-to-Peer, (P2P), attacks.

I. Evolution of DDoS attacks

A few years ago, DDoS attacks were mostly conducted using large botnets to directly flood the target with traffic. Now, we often see the use of amplification attacks through open third-party services or botnets of hijacked servers, which have more bandwidth than compromised computers. But common botnets still play an important role in DDoS attacks.[1] In the past, many DDoS bots were controlled through Internet Relay Chat (IRC) channels. In recent years, most attackers have moved to using HTTP-controlled command servers or have even started using peer-to-peer (P2P) networks to make their attack infrastructure more resilient against takedowns. [4] In order to make it harder for static signatures to be applied for filtering traffic, modern attack scripts randomize every possible part of their traffic. **For example**, in application layer attacks, **HTTP** requests' user agent string is varied and **HTTP GET** requests call on random Web pages. Newer versions of these attacks also allow the attacker to use specific bots in a certain region to perform the attacks. If the bots are in the same geolocation as the target, it makes it even harder to filter the malicious traffic early in the network chain, as one DDoS mitigation tactic for local businesses is to simply drop every connection from foreign countries. [2] Some attackers have started to impersonate Google Bots with their requests as they believe that the target will not filter these bots out. Of course, smart prevention systems are easily able to identify the fake bots by verifying
the source IP address and the frequency of their visits. As a result, this is not a tactic to be worried about, but it highlights how attackers are experimenting with new ideas to bypass DDoS protection mechanisms. Sometimes, even the servers of DDoS protection services are hijacked for attacks.
Instead of attacking the targets directly, attackers have been increasingly targeting connected resources.
The most obvious example is to attack the **domain name system (DNS) server** responsible for resolving the target's domain. If all name servers are not responding over a long time, then users will not be able to reach the company's website, as they don't know the site's IP address.
A prime example of this was the attack against the Chinese registry, which pulled many .cn websites offline for several hours. But some attackers have also started to attack the hardware along the path, such as proxies or gateway solutions in front of Web servers. Attackers are getting smarter at finding the weakest link and attacking this possibly unprotected resource instead. They
can even breach the physical world as well. In August 2014, attackers cut the fiber optic cables of a network provider in

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

Germany, pushing160,000 users offline for multiple hours. Another DDoS attack evolution seen in recent years is how mobile malware has started to include DDoS functionality as well. [3] Of course, unless the mobile devices have 4G connectivity, the bandwidth resources are quite limited. But even if the devices don't have 4G, they can still be used to perform application-layer attacks as, for example, the Dendroid toolkit for Android malware demonstrates. In addition, there are standalone DoS tools available for smartphones, like Android.Loicdos—a mobile version of Low Orbit Ion Canon (LOIC)—and Slowloris. In these cases, the user manually installs and deliberately executes the stress test tools. [1] Attackers also have gained an increased interest in the reverse attack, where the victim's phone is flooded with inbound telephone calls. This type of attack rose in popularity after a presentation on the technique at a recent security conference.

In **general**, we see that attackers are trying to leverage every angle to attack their target from multiple sides from various devices. [2] The bandwidth at their disposal has grown over the years and is combined with customized application-level attacks against Web applications. DDoS attacks have long since moved from a single method used by frustrated **"script kiddies"** to an attack technique used by various professional groups.

II. Denial of Service Concepts

As the name implies, DDoS encompasses the coordinated activities of multiple Denial of Service (DoS) agents and tools. The general concepts of DoS are simple – cause an action upon a computer or networked device which results in other processes, resources or activities floundering and failing to adequately respond. DoS attacks can take on many forms depending upon the target system and objectives of the attacker. For example, an attacker may deny their victims the ability to log into their computer systems by intentionally supplying multiple incorrect passwords until the application locks the accounts out. [4] At the other end of the spectrum, an example would be the mid-1990's "ping of death" – in which an attacker sends a specially crafted network packet (in this case an overly large ping packet) – resulting in multiple victim machines crashing and eventually rebooting.

While many DoS attack techniques have their own nuances and specific naming conventions (e.g. ICMP flooding, teardrop attacks, reflected attacks, etc.), [2]

III. The Distributed DoS Attack

DoS attacks can take on many forms depending upon the target system and objectives of the attacker.Compared to the many classes of complex threats routinely encountered by businesses, DDoS tends to be inelegant and one of the most easily recognized attacks. [1] While the threat may be one of the most commonly encountered and discussed, many people are unaware of the fact that the label of "DDoS" encompasses multiple attack techniques – each with their own nuances and effect on the designated target.

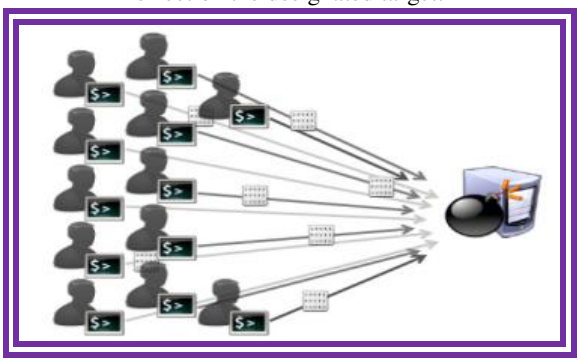

Fig 1: Multiple attackers launch their DoS payloads to constitute a DDoS attack.

- **Volume-based DoS attacks** — Also called a "volumetric" attack, volume-based DoS attacks represent the most common type of threats. [1]The hacker floods the website or network with a high volume of packets or connections, which overwhelms the network equipment, servers or bandwidth resources. In the past, criminals would recruit volunteers to launch these attacks. [4] Today, the most common technique uses "botnet," the hacker commandeers a gang of "zombies" – Internet-compromised machines and sends span emails or performs other criminal acts.
- **Application DoS attacks** — This type of attack can target many different applications, but tend to target HTTP the most. Requiring fewer network connections to achieve its objective, application-focused DDoS attacks aim to exhaust web servers and services. Simply launching numerous HTTP POSTS or HTTP GETs could exhaust an application or web server. These attack also target application like DNS and Voice over IP (VoIP).
- **Low-rate DoS (LDoS) attacks** — This malicious code seeks out weaknesses and design flaws in your network.

IV. DDoS attacks: 5 strategies for defending your network

Malicious programs like Slowloris allow the hacker to take down a web server with minimal bandwidth requirements and without the need to launch numerous attacks simultaneously. Here are some methods that have proven effective in combating DoS attacks.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

1. Bandwidth oversubscription.
One of the most common measures employed to alleviate DoS attacks may also be one of the most expensive. Bandwidth oversubscription may be one of the most effective ways to account for attacks that can be 10x or 100x greater than standard traffic levels. [3]You should frequently review this component of your plan because as bandwidth becomes cheaper you should increase your capacity to build your buffer.

2. Internal system reinforcement.
This method may be something as straightforward as implementation of additional layers of firewall protection or re-configuration of both the operating system and applications. For example, you can ensure that you have the correct number of nodes on your Linux server to configure the appropriate number of Apache worker threads, which makes it more difficult for a malicious attack to bring down your server.

3. Monitor network traffic.
The most effective way to detect when a system comes under DoS attack is by monitoring applications and network traffic. Numerous threat detection tools have the ability to monitor netflow data from routers and other data sources to determine your traffic baseline. [2] Monitoring traffic lets you determine poor application performance occurs due to attacks or it has its basis in service provider outages. You will also be able to identify legitimate traffic from attacks.
Your security administrator should review the following information:

- ✓ Traffic levels
- ✓ Application performance
- ✓ Anomalous behavior
- ✓ Protocol violations
- ✓ Web server error codes

Typical monitoring tools employ BGP or other mechanisms that filter out noise and pass the clean traffic further into the network. [1] These tools provide instant visibility into DoS attacks and can detect volumetric attacks and more subtle attacks such as Slowloris.

4. Upstream blackholing.
Companies depend mostly on traffic of the TCP format as oppose to UDP traffic. Implement a solution that deflects UDP traffic by use router backholding to reroute traffic away from the intended target.

5. Third party provider.
Many companies employ third-party service provides to provide the assistance when traffic becomes overwhelming. [3] Through the implementation of a DNS-based redirect service or a BGP-based service, the contractor will provide the necessary protection if the network suffers a sustained attack. CDN providers also fit this bill because they can help organizations stay online during a DoS attack.

V. Conclusion

DDoS attacks are constantly evolving in terms of their technology, sophistication level, and tactics.These attacks are easy to carry out and do not require great knowledge or access to zero-day vulnerabilities. Application-layer attacks, which target the Web application, are gaining in importance as well as they are difficult to mitigate. They will become even more important in the future as often, attackers adapt their methods during an attack in an attempt to bypass any short term defense mechanism. In the future, we might see more DDoS attacks coming from mobile devices or even the Internet of Things, but this is currently not happening on a large scale. In this paper, we are discussed about the evolution of ddos attacks in strategy and tactics**.**

VI. REFERENCES

1) **The Top 10 DDoS Attack Trends, Discover the Latest DDoS Attacks and Their Implications, www.imperva.com. © Copyright 2015, Imperva All rights reserved. Imperva and SecureSphere are registered trademarks of Imperva.**
2) **The continued rise of DDoS attacks, Candid Wueest, Principal Software Engineer,Version 1.0 – October 21, 2014, 13:00 GMT. www.symantec.com. Copyright © 2014 Symantec Corporation. All rights reserved.**
3) **Understanding the Modern DDoS Threat by Gunter Ollmann, VP of Research, Damballa. ID.30.104.0511,Copyright © 2011, Damballa, Inc. All rights reserved worldwide.**
4) **DDoS attacks: 5 strategies for defending your networkBy Charles Herring on 3 June, 2015.**