xahive

CYBERSECURITY CYBER-ATTACK SERIES

DISTRIBUTED DENIAL-OF-SERVICE (DDoS)

Prepared by Keith J. Gomes, J.D., Ph.D.

What is a Distributed Denial-of-Service (DDoS) attack?

A distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

The flood of incoming messages to the target system essentially forces it to shut down, thereby denying access to legitimate users. A typical DDoS attack begins by the hacker exploiting a vulnerability in one computer system and making it the DDoS master. The attack master (also known as the botmaster) identifies and infects other vulnerable systems with malware. Eventually, the hacker instructs the controlled machines to launch an attack against a specified target. DDoS attacks are most common for large companies, however, smaller companies can also be targeted or fall victim to such attacks if another organization on their network is targeted.

The machines which are under the control of an intruder are called zombies or bots, and a group of such computers is known as a botnet or a zombie army. Both Kaspersky Labs and Symantec have identified botnets – not spam, viruses, or worms – as the biggest threat to Internet security (Rouse, Distributed denial-of-service attack (DDoS) 2013).

The Aim of a DDoS attack

DDoS attack typically serve as means to extort money or disrupt the operations of a private or government enterprise. They are designed to target any aspect of a business and its resources, and can easily:

- disable a specific computer, service or an entire network
- target alarms, printers, phones or laptops
- hit system resources like bandwidth, disk space, processor time or routing information
- execute malware that affects processors and triggers errors in computer microcodes
- exploit operating system vulnerabilities to drain system resources
- crash the operating system (DDoS) 2013).

The cost of carrying out DDoS has dropped significantly in cost thus making it easier for anyone to launch an attack: organized crime, blackmailers, disgruntled ex-employees or competitors. Anyone can be a victim (Rubens 2016).

Types of DDoS attacks

There are three main types of DDoS attacks. It is important to note that, however, that these types of DDoS attacks are often used in conjunction with one another to compromise a single target.

Type #1: Network-centric/volumetric attacks

This type of attack is the most common type of DDoS attack accounting for about 65% of the total reported. These attacks use bots and botnets to flood the network layers with a substantial amount of seemingly legitimate traffic. This consumes an excessive amount of bandwidth within and/or outside of the network and causes network operations to become extremely slow or to not work at all. These kinds of attacks are more difficult to mitigate than attacks from a single source since they essential mob a network from multiple sources. Volumetric attacks come in a variety of forms, including:

- **User Datagram Protocol (UDP) Floods.** Random ports on a server are flooded with UDP packets, causing the server to repeatedly check for and respond to non-existent applications at the ports. As a result, the system is unable to respond to legitimate applications.
- **ICMP floods.** A server is flooded with ICMP echo requests from multiple spoofed IP addresses. As the targeted server processes and replies to these phony requests, it is eventually overloaded and unable to process valid ICMP echo requests**.**

Type #2. Application-layer attacks

Application-layer attacks comprise about 17% of all reported DDoS attacks. They target web application packets in order to disrupt the transmission of data between hosts. For example, an HTTP Flood – the most common application-layer attack – uses botnets to force a target to expend an excessive amount of resources when responding to a HTTP request. HTTP floods and other application-layer DDoS attacks mimic human-user behavior making them much more difficult to detect than other types of attacks. Also, application layer attacks can also come from a single machine, which causes less traffic to be generated and therefore is harder to detect. HTTPS and SMTP are also commonly targeted, although less often that HTTP. Web-based email apps, WordPress, Joomla, and forum software are good examples of application specific targets.

Type #3. State-exhaustion/protocol attacks

State-exhaustion or protocol attacks target the connection state tables in firewalls, web application servers, and other infrastructure components. They account for about 20% of reported DDoS attacks. One of the most common state-exhaustion attacks (especially in the nineties) was the **ping of death,** in which a 65,536-byte ping packet is defragmented and sent to a target server as fast as possible. Once the target reassembles the large packet, a buffer overload typically occurs. In the likely scenario that the target attempts to respond to the pings, even more bandwidth is consumed, eventually causing the targeted system to crash (Calyptix 2015; RivalHost 2013).

More Examples of Forms of DDoS Attacks (RivalHost 2013)

SYN Flood	*Transmission Control Protocol (TCP) connections use what is referred to as a "three-way handshake" to work. First, a "synchronize", or SYN message, is sent to the host machine to start the conversation. Next, the request is "acknowledged" by the server. It sends an ACK flag to the machine that started the "handshake" process and awaits for the connection to be closed. The connection is completed when the requesting machine closes the connection. A SYN flood attack will send repeated spoofed requests from a variety of sources at a target server. The server will respond with an ACK packet to complete the TCP connection, but instead of closing the connection the connection is allowed to timeout. Eventually, and with a strong enough attack, the host resources will be exhausted and the server will go offline.*
Reflected Attack	*A reflected attack is where an attacker creates forged packets that will be sent out to as many computers as possible. When these computers receive the packets they will reply, but the reply will be a spoofed address that actually routes to the target. All of the computers will attempt to communicate at once and this will cause the site to be bogged down with requests until the server resources are exhausted.*
Peer-to-Peer Attacks	*Peer-to-Peer servers present an opportunity for attackers. Instead of using a botnet to siphon traffic towards the target, this exploits a peer-to-peer server to route traffic to the target website. This redirects people using the file-sharing hub to the target website until the website is overwhelmed and sent offline.*
Nuke	*More common in the past, in this kind of attack, corrupt and fragmented ICMP packets are sent via a modified ping utility to keep the malicious packets to be delivered to the target. Eventually, the target machine goes offline.*
Slowloris	*This kind of attack was used in the 2009 Iranian Presidential election. Slowloris is a tool that allows an attacker to use fewer resources during an attack. During the attack connections to the target machine are opened with partial requests and allowed to stay open for the maximum time possible. It will also send HTTP headers at certain intervals. This adds to the requests, but never completes them – keeping more connections open longer until the target website is no longer able to stay online.*
Degradation of Service Attacks	*The purpose of this attack is to slow server response times. Generally, a DDoS attack seeks to take a website or server offline, however in a degradation of service attack, the goal here is to slow response time to a level that essentially makes the website unusable for most people. Zombie computers are leveraged to flood a target machine with malicious traffic that will cause performance and page-loading issues. These types of attacks can be difficult to detect because the goal is not to take the website offline, but to degrade performance. They are often confused with simply an increase in legitimate website traffic.*
Unintentional DDoS	*Unintended distributed denial of service happens when a spike in web traffic causes a server to not be able to handle all of the incoming requests. The more traffic that occurs, the more resources are used. This causes pages to timeout when loading and eventually the server will fail to respond and go offline.*
Multi-Vector Attacks	*Multi-vector attacks are the most complex forms of distributed denial of service (DDoS) attack. Instead of utilizing a single method, a combination of tools and strategies are used to overwhelm the target and take it offline. Multi-vector attacks will often target specific applications on the target server, as well as flood the target with a large volume of malicious traffic. These attacks are the most difficult to mitigate because the attack comes in different forms and targets different resources simultaneously.*
Zero Day DDoS	*A "Zero Day" based attack is simply an attack method that to date has no patches. This is a general term used to describe new vulnerabilities and exploits that are still new.*

Determining if your system has suffered a DDoS attack

- *There was a 180% percent increase in the total number of DDoS attacks in 2015 compared to 2014.*

- *The online gaming sector is currently the most susceptible to attack, accounting for 50% of all DDoS attacks. Software and technology companies suffered about 25% of all DDoS attacks, with Internet and telecoms companies suffering just 5% of DDoS attacks (Rubens 2016).*

It can be difficult to determine if a website is down due to legitimate traffic, rather than an attack. However, if slow or denied service continues for days rather than a spike during a campaign, this might be a sign of a DDoS attack. Unfortunately, a user cannot simply check to see if all of the traffic is coming from one IP, as the exact purpose of a DDoS is to have traffic coming from multiple sources (Grange 2014).

DDoS attacks include the following symptoms:

- Unusually slow network performance (extremely slow opening files or accessing other websites)
- Unavailability of a particular website
- Inability to access other websites
- High increase in the number of spam emails (sometimes called an ‘e-mail bomb’)
- If the same source address is asking or sending requests for the same data before (Time to Live) has passed (Sullivan).

Preventing a DDoS attack

- Nominate a DDoS leader in your company who is responsible for acting should you come under attack.
- Keep systems as secure as possible with regular software updates, online security monitoring and monitoring of data flow to identify any unusual or threatening spikes in traffic.
- Since DDoS attacks can also be perpetrated by simply cutting a cable or dislodging a plug that connects your website's server to the internet, due diligence is also required in physically monitoring connections is recommended.
- It generally makes sense to have more bandwidth available to your Web server than you ever think you are likely to need. That way, you can accommodate sudden and unexpected surges in traffic. This will not stop a DDoS attack but it may give you a few extra minutes to act before your resources are overwhelmed.

- Some technical measures that can be taken to partially mitigate the effect of an attack, especially in the first minutes, include the following that may buy time as a DDoS attack ramps up:
    - rate limit the router to prevent the Web server being overwhelmed
    - add filters to tell the router to drop packets from obvious sources of attack
    - timeout half-open connections more aggressively
    - drop spoofed or malformed packages
    - set lower SYN, ICMP, and UDP flood drop thresholds.
- Call your ISP (or hosting provider if you do not host your own Web server), tell them you are under attack and ask for help. Keep emergency contacts for your ISP or hosting provider readily available so this can be done quickly.
- For very large attacks, the best chance of staying online is to use a specialist DDoS mitigation company (Rubens 2016; Sullivan).

References

Calyptix. 2015. "DDoS Attacks 101: Types, targets, and motivations." *Calyptix.* April 26. Accessed July 20, 2016. http://www.calyptix.com/top-threats/ddos-attacks-101-types-targets-motivations/.

Grange, David. 2014. "How to tell if you've been hit by a DDoS attack, and 5 ways to be prepared." *IT Pro Portal.* June 3. Accessed July 29, 2016. http://www.itproportal.com/2014/03/06/how-tell-if-youve-been-hit-ddos-attack-and-how-respond/#ixzz4F6gBNBfM.

Kramer, David. n.d. "Buffer overflow." *Search Security.* Accessed July 12, 2016. http://searchsecurity.techtarget.com/definition/buffer-overflow.

RivalHost. 2013. "12 Types of DDoS Attacks Used By Hackers." *RivalHost.* February 28. Accessed July 20, 2016. https://www.rivalhost.com/12-types-of-ddos-attacks-used-by-hackers/.

Rouse, Margaret. 2013. "Distributed denial-of-service attack (DDoS)." *Search Security.* May. Accessed July 12, 2016. http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack.

—. 2007. "IP spoofing (IP address forgery or a host file hijack)." *Search Security.* June. Accessed July 12, 2016. http://searchsecurity.techtarget.com/definition/IP-spoofing.

Rubens, Paul. 2016. "6 Tips for Fighting DDoS Attacks." *eSecurity Planet.* January 25. Accessed July 29, 2016. http://www.esecurityplanet.com/network-security/5-tips-for-fighting-ddos-attacks.html.

Sullivan, Megan. n.d. "8 Types of Cyber Attacks Your Business Needs to Avoid." *Intuit.* Accessed July 13, 2016. http://quickbooks.intuit.com/r/technology-and-security/8-types-of-cyber-attacks-your-business-needs-to-avoid/#sm.000mbhe2m17qedtvq9n2kph7kl57f.