CENTER FOR INTERNET SECURITY®

INTEGRATED INTELLIGENCE CENTER

# TECHNICAL WHITE PAPER

William F. Pelgrin, CIS President and CEO

# Guide to DDoS Attacks

December 2014

*Authored by: Lee Myers, SOC Analyst*

This Center for Internet Security (CIS) Multi-State Information Sharing and Analysis Center (MS-ISAC) document is a guide to aid our partners in their remediation efforts of Distributed Denial of Service (DDoS) attacks.

A Denial of Service (DoS) attack is an attempt to make a system unavailable to the intended user(s), such as preventing access to a website. This is accomplished when an attacker successfully consumes all available network or system resources, usually resulting in a slowdown or server crash. Whenever multiple sources are coordinating in the DoS attack, it becomes known as a DDoS.

MS-ISAC regularly observes two methods of DDoS attacks: Standard and Reflection.

A Standard DDoS attack occurs when attackers are able to send a very large amount of malformed network traffic directly to a target server or network. One of the ways an attacker can accomplish this is by using a botnet to send the traffic. A botnet is a large number of victim computers, or zombies, connected over the Internet, that communicate with each other and can be controlled from a single location. When an attacker uses a botnet to perform the DDoS attack, they send instructions to some or all of the zombie machines connected to that botnet, thereby magnifying the size of their attack, making it originate from multiple networks and possibly from multiple countries.

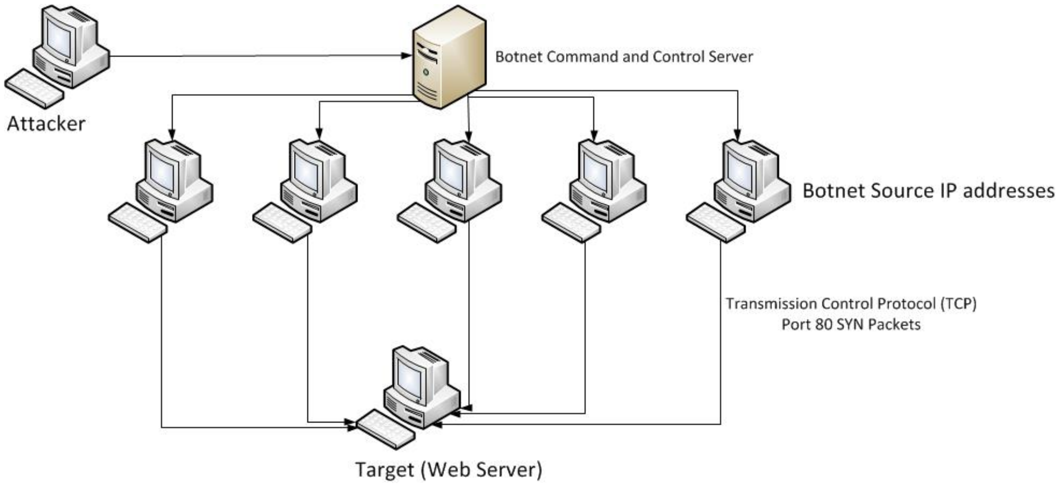
Attacker
Botnet Command and Control Server
Botnet Source IP addresses
Transmission Control Protocol (TCP)
Port 80 SYN Packets
Target (Web Server)

**Figure 1: Example Standard DDoS SYN Flood**

*Image Source: Lee Myers, Center for Internet Security*

A Reflection DDoS attack occurs when attackers spoof their IP address to pose as the intended victim and then send legitimate requests to legitimate public-facing servers. The responses to these requests are sent to the intended victim and originate from legitimate servers.

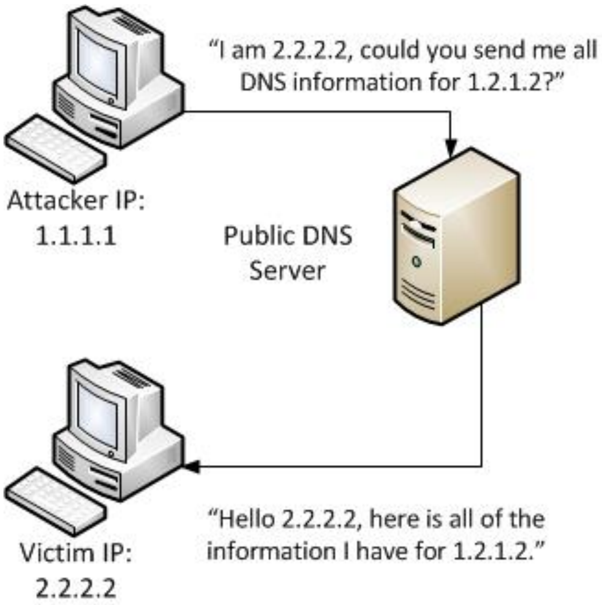
"I am 2.2.2.2, could you send me all DNS information for 1.2.1.2?"
Attacker IP: 1.1.1.1
Public DNS Server
"Hello 2.2.2.2, here is all of the information I have for 1.2.1.2."
Victim IP: 2.2.2.2

**Figure 2: Example DNS Reflection DDoS with Amplification**
*Image Source: Lee Myers, Center for Internet Security*

In addition to these methods, a technique used by attackers to increase the effectiveness of their attack is called Amplification. Usually used in conjunction with Reflection attacks, Amplification is whenever the response that is sent to the victim is larger than the request that is sent from the attacker.

In addition to the use of botnets, there are tools that are freely available online that malicious actors can use to perform DDoS attacks. Most of these tools were originally designed by legitimate organizations to be stress testers, and have since become open source. Popular examples of these tools include the Low Orbit Ion Cannon (LOIC) and the High Orbit Ion Cannon (HOIC). These tools can be downloaded, installed, and utilized by anyone who wishes to be a part of an on-going DDoS operation. With the goal of consuming all available bandwidth allocated to the target, the LOIC sends large amounts of TCP and UDP traffic, while the HOIC specifically sends HTTP traffic. Other examples of tools that can be used to perform DDoS activities include Metasploit, Pyloris, and Slowloris.

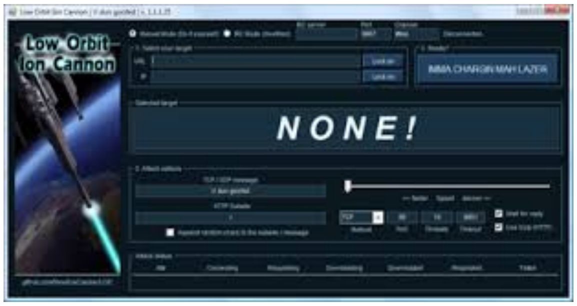
Low Orbit Ion Cannon
IMMA CHARGIN MAH LAZER
NONE!

**Figure 3: Image of the LOIC Graphical User**
***Image Source: en.wikipedia.org***

While the main purpose behind a DDoS is the malicious consumption of resources, different attackers may use different techniques to generate the traffic necessary for an effective DDoS. A lone actor with a botnet at their disposal may use that botnet to orchestrate the attacks. However, botnets are also available for hire, with operators charging minimal fees for short duration attacks. A group of actors working together may choose to use the same type of free tool, rather than trying to gain access to a botnet. Attacks like these are usually less successful, as it is difficult to coordinate enough attackers for the effect to be noticeable.

## Standard DDoS Attack Types

### SYN Flood:

A SYN Flood is one of the most common forms of DDoS attacks observed by the MS-ISAC. It occurs when an attacker sends a succession of Transmission Control Protocol (TCP) Synchronize (SYN) requests to the target in an attempt to consume enough resources as to make the server unavailable for legitimate users. This works because a SYN request is used to open network communication between a prospective client and the target server. When the server receives a SYN request, it responds acknowledging the request, and then holds the communication open as it waits for the client to acknowledge the open connection on the client’s end. However, in a SYN Flood attack the client acknowledgement never arrives, thus tying up the server resource until the connection times out. A large number of incoming SYN requests to the target server will eventually exhaust all available server resources and result in a successful DDoS attack.

***Recommendations:***

- To identify a SYN Flood, investigate network logs and locate the TCP SYN flag. We recommend using either Tcpdump or Wireshark.
    - TCP SYN packets are normal, and are not on their own indicative of malicious activity. Look for a large number of SYN packets coming from a large number of sources over a short period of time.
- Once an attack is identified, try to leverage your upstream network service provider in order for them to mitigate the activity before it reaches your network.
- To help minimize the impact of successful SYN Flood attacks, define strict “TCP keepalive” and “maximum connection” rules on all perimeter devices, such as firewalls and proxy servers.
    - On some firewall devices, you can enable “SYN cookies” to help mitigate the effects of a SYN Flood. When this is enabled, the firewall will validate the TCP connection between client and server before traffic is actually passed to the server. When the attackers never send a final acknowledgement of the open connection, the firewall will drop the connection.

### UDP Flood:

A User Datagram Protocol (UDP) Flood is very similar to a SYN Flood in that an attacker uses a botnet to send a large amount of traffic to the target server. The difference is that this attack is much faster, and rather than attempting to exhaust server resources, it is attempting to consume all of the available bandwidth on the server's network link, thereby denying access to legitimate users. The attack works because a server that receives a UDP packet on a network port, such as 50555/UDP, will check for an application that is listening on that port. If there is nothing listening on that port, it will reply to the sender of the UDP packet with an Internet Control Message Protocol (ICMP) Destination Unreachable packet. During an attack, a large number of UDP packets arrive, each with various destination ports, then the server is forced to process each one, and in most cases, respond to each one. This can quickly lead to the consumption of all available bandwidth.

***Recommendations:***

- To identify a UDP Flood, investigate network logs and look for a large number of inbound UDP packets over irregular network ports coming from a large number of source IP addresses.
    - There are many legitimate services that use UDP for their network traffic. Common UDP ports are 53 (DNS), 88 (Kerberos), 137/138/445 (Windows), and 161 (SNMP). When investigating a DDoS attack, look for UDP traffic with high numbered network ports (1024+).
- Once an attack is identified, try to leverage your upstream network service provider in order for them to mitigate the activity before it reaches your network.
- To mitigate the effect of UDP Flood attacks, define strict rules on your perimeter network devices, like firewalls, to only allow inbound traffic on ports that are required.

UDP Flood Variant using Reflection: Fraggle DDoS Attack

A Fraggle attack is an alternate method of carrying out a UDP Flood attack. In a Fraggle attack, the attacker uses the target's IP address as their own, which is called spoofing, and then sends UDP echo (port 7) requests to the character generation port (port 19) of the broadcast IP address for a public network on the Internet. The broadcast IP address of a network will send any traffic that it receives to all other IP addresses within its network. Therefore, when the UDP echo request is received by the broadcast IP address, it is then forwarded on to all live computers on its network. Each of those computers think that these echo requests are coming from the target IP address, and therefore send their responses to the target rather than back to the attacker. The result of this is a large number of unsolicited UDP character generation traffic being sent to the target of the DDoS, resulting in the consumption of available bandwidth.

## ICMP Flood:

An ICMP Flood occurs when an attacker uses a botnet to send a large number of ICMP packets to a target server in an attempt to consume all available bandwidth and deny legitimate users access. This attack works when a large number of sources are able to send enough ICMP traffic as to consume all available bandwidth of the target's network. An example of this could be the "ping" command. This command is primarily used to test network connectivity between two points on a network. However, it is possible to supply this command with different variables to make the ping larger in size and occur more often. In using these variables correctly, and with enough source machines initiating the traffic, this traffic will eventually lead to the consumption of all available bandwidth.

***Recommendations:***

- To identify an ICMP Flood, investigate network logs and look for a large amount of inbound ICMP traffic from a large number of sources.
    - Depending on what tool you are using to investigate your logs, you can identify ICMP packets either by the protocol being displayed in the graphical user interface, such as with WireShark, or you will notice that no port information is available, as ICMP does not use network ports like TCP or UDP do.
    - If you are using a tool that displays the network protocols as numbered values, ICMP is protocol 1.
    - There are also ICMP type and code fields that identify what ICMP traffic is being sent or received. For a complete list of these types and codes, please see hxxp://www.nthelp.com/icmp.html
- Once an attack is identified, try to leverage your upstream network service provider in order for them to mitigate the activity before it reaches your network.
- To mitigate some of the damage of ICMP Flood attacks, block ICMP traffic at perimeter network devices such as routers. Additionally, set a packet-per-second threshold for ICMP requests on perimeter routers. If the amount of inbound ICMP traffic exceeds this threshold, the excess traffic is ignored until the next second. This will effectively keep your network from being overrun with ICMP traffic.
    - Note: The above step will not stop a determined ICMP Flood. If there is enough inbound traffic to exhaust the bandwidth between the upstream network provider and the perimeter device filtering ICMP, legitimate traffic may be dropped, or delayed to the point of a DOS. If this is the case, it is necessary to contact the upstream network service provider in order to have this ICMP activity dropped at their level before it reaches your network link.

ICMP Flood Variant using Reflection: Smurf Attack

A Smurf attack is an alternate method of carrying out an ICMP Flood attack. In a Smurf attack, the attacker uses the target's IP address as their own, which is called spoofing, and then sends ICMP ping requests to the broadcast IP address of a public network on the Internet. The broadcast IP address of a network will send any traffic that it receives to all other IP addresses within its network. Therefore, when the ICMP ping request is received by the broadcast IP address, it is then forwarded on to all live computers on its network. Each of those computers think that these ping requests are coming from the target IP address and therefore send their responses to the target rather than back to the attacker. The result of this is a large number of unsolicited ICMP ping replies being sent to the target of the DDoS, resulting in the consumption of available bandwidth.

# Reflection DDoS Attack Types

## NTP Reflection Attack with Amplification:

A Network Time Protocol (NTP) DDoS attack occurs when the attacker uses traffic from a legitimate NTP server to overwhelm the resources of the target. NTP is used to synchronize clocks on networked machines and runs over port 123/UDP. An obscure command, monlist, allows a requesting computer to receive information regarding the last 600 connections to the NTP server. An attacker can spoof the target's IP address and send a monlist command to request that the NTP server send a large amount of information to the target. These responses will typically have a fixed packet size that can be identified across a large number of responses. Because the response from the NTP server is larger than the request being sent from the attacker, the effect of the attack has been amplified. When an attacker spoofs the target's IP address and then sends the monlist command to a large number of Internet-facing NTP servers, the amplified responses will all be sent back to the target. This will eventually result in the consumption of all available bandwidth.

***Recommendations:***

- To identify a NTP Reflection Attack with Amplification, investigate your network logs and look for inbound traffic with a source port of 123/UDP and a specific packet size.
- Once identified, try to leverage your upstream network service provider and provide them with the attacking IP addresses and the packet sizes used in the attack. Upstream providers can place a filter at their level that will drop inbound NTP traffic using the specific packet size that you are experiencing.
- Along with remediating inbound attacks, take the following preventative measures to ensure that your NTP servers are not used to attack others.
    - If you are unsure if your NTP server is vulnerable to being used in an attack, follow the instructions available at OpenNTP: hxxp://openntpproject.org/
    - Upgrade NTP servers to version 2.4.7 or later, which removes the monlist command entirely, or implement a version of NTP that does not utilize the monlist command, such as OpenNTPD.
    - If the server cannot be upgraded, the monlist query feature can be disabled by adding "disable monitor" to your ntp.conf file and restarting the NTP process.
    - Implement firewall rules that restrict unauthorized traffic to the NTP server.

## DNS Reflection Attack with Amplification:

A Domain Name System (DNS) DDoS attack occurs when the attacker manipulates the DNS system to send an overwhelming amount of traffic to the target. A DNS server is used to resolve IP addresses to domain names. This allows the average Internet user to type an easily remembered domain name into their Internet browser, rather remembering the IP addresses of websites. A DNS Reflection attack occurs when an attacker spoofs the victim's IP address and sends DNS name lookup requests to public DNS servers. The DNS server will then send the response to the target server, and the size of the response depends on the options specified by the attacker in their name lookup request. To get the maximum amplification, the attacker can use the word “ANY” in their request, which returns all known information about a DNS zone to a single request. When an attacker spoofs a target’s IP address and sends DNS lookup requests to a large number of public DNS servers, the amplified responses are sent back to the target and will eventually result in the consumption of all available bandwidth.

As DNS is a necessary service, there is no way to prevent this attack.

***Recommendations:***

- To identify if a DNS Reflection Attack with Amplification is occurring, investigate network logs and look for inbound DNS query responses with no matching DNS query requests.
    - DNS queries are normal, and are themselves not indicative of an attack.
- Once an attack is identified, try to leverage your upstream network service provider in order for them to mitigate the activity before it reaches your network.
- Along with remediating inbound attacks, disable DNS recursion, if possible, by following the guidelines provided by your DNS server vendor (BIND, Microsoft, etc). This will ensure that your DNS servers are not used to attack others.

## WordPress Pingback Reflection Attack with Amplification:

WordPress is a popular Content Management System (CMS) that is used to develop and maintain websites and blogs. A function of WordPress sites is called the Pingback feature. This feature is used to notify other WordPress websites that you have put a link to their website on your website. Sites using WordPress automate this process, and maintain automated lists linking back to sites that link to them. These “pingbacks” are sent as Hypertext Transfer Protocol (HTTP) POST requests to the /xmlrpc.php page, which is used by WordPress to carry out the pingback process. By default, this feature downloads the entire webpage that contains the link that triggered the pingback process. An attacker can locate any number of WordPress websites and then send Pingback requests to each of them containing the URL of the target web site, resulting in each of those WordPress websites sending requests to the target server requesting the download of the web page. A large number of requests to download the webpage can eventually overload the target web server.

***Recommendations:***

- To identify a WordPress Pingback Reflection attack with Amplification, investigate your network logs and look for a large number of inbound TCP traffic over port 80 from a large number of sources. The traffic will be HTTP GET requests for random values such as “?5454545=6767676”. This bypasses the cache and forces a full-page reload for every packet.
- Once an attack is identified, try to leverage your upstream network service provider in order for them to mitigate the activity before it reaches your network.
- At the time of this writing, there is no way to prevent this inbound traffic as on its own it is normal web traffic. However, there is a way to ensure that your own WordPress websites are not used to attack others. To do this, WordPress offers a tool that is available for download that will disable the pingback feature of XMLRPC. This tool can be found at the following link: hxxp://wordpress.org/plugins/disable-xml-rpc-pingback/.

  - Instead of downloading this tool, you could also create a plugin for the website that adds a filter which will manually unset the pingback function of XMLRPC. An example of this plugin can be found at hxxps://blog.cisecurity.org/wordpress-pingback-feature-being-used-in-ddos-attacks/

## General Recommendations and Mitigation Strategies

The recommendations for DDoS attacks vary depending on what type of attack you are experiencing. However, the following generic recommendations are guidelines for DDoS mitigation, which will reduce the impact of attempt DDoS attacks, and enable you to respond to successful DDoS attacks more quickly when they do occur.

- Establish and maintain effective partnerships with your upstream network service provider and know what assistance they may be able to provide you in the event of a DDoS attack. In the event of a DDoS attack, the faster that they can implement traffic blocks and mitigation strategies at their level, the sooner your services will become available for legitimate users.
- Consider also establishing relationships with companies who offer DDoS mitigation services.
- If you are experiencing a DDoS attack, provide the attacking IP addresses to your upstream network service provider so they can implement restrictions at their level. Keep in mind that Reflection DDoS attacks typically originate from legitimate public servers. This is important information to ascertain when examining network logs during an attack. Use tools such as the American Registry for Internet Numbers (ARIN) (https://www.arin.net) to lookup the source IPs involved in the attack. Otherwise, you may block traffic from legitimate networks or servers.
- Enable firewall logging of accepted and denied traffic in order to determine where the DDoS may be originating.
- Define strict “TCP keepalive” and “maximum connection” on all perimeter devices, such as firewalls and proxy servers. This will help with SYN Flood attacks from being successful.
- Consider port and packet size filtering by the upstream network service provider.
- Establish and regularly validate baseline traffic patterns (volume and type) for public-facing websites.
- Apply all vendor patches after appropriate testing.
- Configure firewalls to block, as a minimum, inbound traffic sourced from IP addresses that are reserved (0/8), loopback (127/8), private (RFC 1918 blocks 10/8, 172.16/12, and 192.168/16), and otherwise listed in RFC 5735. This should be requested at the ISP level as well.
- Tune public-facing server processes to allow the minimum amount of processes or connections necessary to effectively conduct business.
- Configure firewalls and intrusion detection/prevention devices to alarm on traffic anomalies.
- Configure firewalls to accept only that traffic detailed in your organization’s security policy as required for business purposes.

**About the Multi-State Information Sharing and Analysis Center (MS-ISAC):**

The MS-ISAC is the focal point for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. The MS-ISAC 24x7 cyber security operations center provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response.

For more information please visit http://msisac.cisecurity.org/

**Tra**