



MULTI-STATE
Information Sharing
& Analysis Center™

**TECHNICAL
WHITE PAPER**

June 2016

Guide to DDoS Attacks

Authored by:

Lee Myers, Senior Manager of Security Operations

Christopher Cooley, Cyber Intelligence Analyst

This Multi-State Information Sharing and Analysis Center (MS-ISAC) document is a guide to aid partners in their remediation efforts of Distributed Denial of Service (DDoS) attacks. This guide is not inclusive of all DDoS attack types and references only the types of attacks partners of the MS-ISAC have reported as experiencing.

TABLE OF CONTENTS:

Introduction.....	2
<u>Standard DDoS Attack Types:</u>	
SYN Flood.....	4
UDP Flood.....	5
ICMP Flood.....	6
HTTP GET Flood.....	7
<u>Reflection DDoS Attack Types:</u>	
NTP Reflection Attack with Amplification.....	8
DNS Reflection Attack with Amplification.....	9
Wordpress Pingback Reflection Attack with Amplification.....	10
SSDP Reflection Attack with Amplification.....	11
Microsoft SQL Reflection Attack with Amplification.....	12
General Recommendations and Mitigation Strategies.....	13

INTRODUCTION

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. A successful DoS attack 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 attack.

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

A Standard DDoS attack occurs when attackers send a substantial 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.

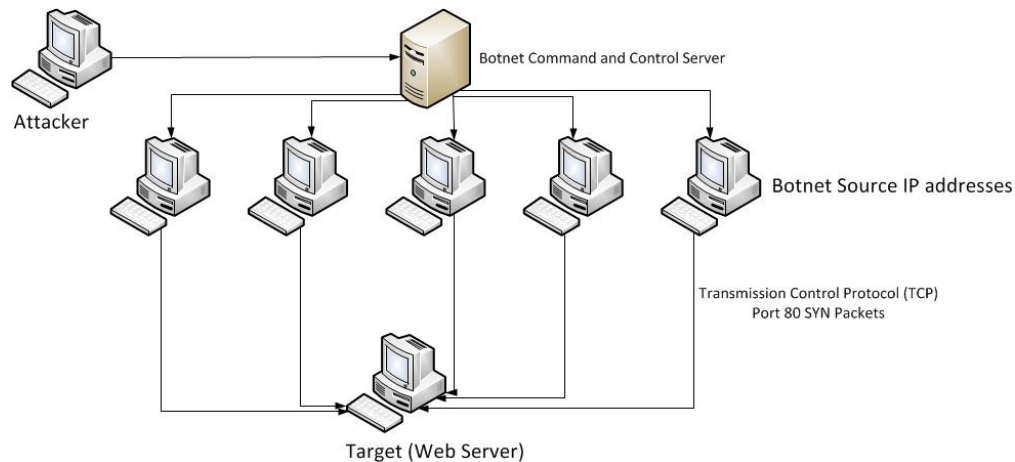


Figure 1: Example Standard DDoS SYN Flood
Image Source: Center for Internet Security

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.

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 occurs when the response that is sent to the victim is larger than the request that is sent from the attacker.

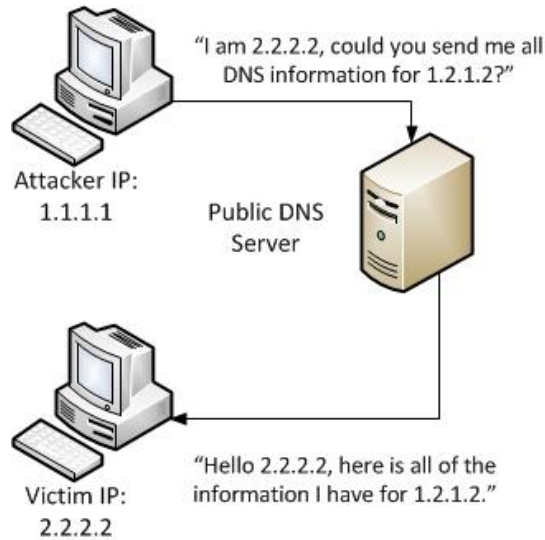


Figure 2: Example DNS Reflection DDoS with Amplification
Image Source: Center for Internet Security

In addition to the use of botnets, some tools are freely available online that cyber threat actors can use to perform DDoS attacks. Most of these tools were originally designed to be stress testers and have since become open source tools used to conduct DDoS attacks by amateur cyber threat actors. 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 ongoing DDoS attack. With the goal of consuming all available bandwidth allocated to the target, the LOIC sends significant amounts of Transmission Control Protocol (TCP) and User Datagram Protocol (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.

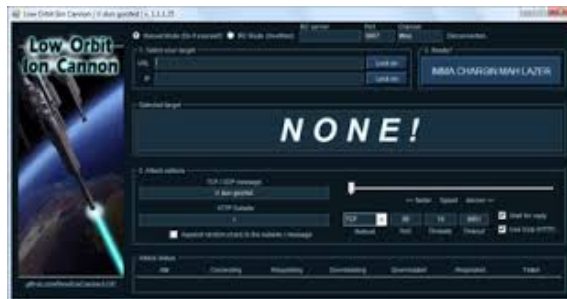


Figure 3: Image of the LOIC Graphical User
Image Source: en.wikipedia.org

While the main purpose behind a DDoS attack 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 TCP Synchronize (SYN) requests to the target in an attempt to consume enough resources to make the server unavailable for legitimate users. This works because a SYN request opens network communication between a prospective client and the target server. When the server receives a SYN request, it responds acknowledging the request and holds the communication open while it waits for the client to acknowledge the open connection. However, in a successful SYN Flood, the client acknowledgment never arrives, thus tying up the server's resources until the connection times out. A large number of incoming SYN requests to the target server exhausts all available server resources and results in a successful DDoS attack.

Recommendations:

- To identify a SYN Flood, investigate network logs and locate the TCP SYN flag. Tcpcmdump or Wireshark may work for this purpose.
 - TCP SYN packets are normal and are not necessarily indicative of malicious activity. Look for a large number of SYN packets coming from multiple sources over a short period.
- If you identify an attack, 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 appliances, you can enable "SYN cookies" to help mitigate the effects of a SYN Flood. Enabling SYN cookies forces the firewall to validate the TCP connection between client and server before traffic is passed to the server. When attackers never send a final acknowledgment of the open connection, the firewall drops the connection.

Slowloris Attacks: While Slowloris is a DoS tool that can be easily accessed by threat actors, the term Slowloris is also used to describe a type of DoS attack. Slowloris attacks attempt to establish multiple TCP connections on a target web server, and hold them open for as long as possible by sending partial requests, very similar to a SYN Flood.

Variation of SYN Flood: ESSYN/XSYN Flood

An ESSYN Flood, also known as an XSYN Flood, is an attack designed to target entities using stateful firewalls. The attack works when a large number of unique source IP addresses all attempt to open connections with the target destination IP. Each new connection from a unique source IP creates a new entry in the firewall state table. The purpose of this attack is to create more unique connections than there is space for in the firewall's state table. Once the table is full, the firewall will not accept any additional inbound connections, denying service to legitimate users attempting to access the destination IP.

Variation of SYN Flood: PSH Flood

A Push (PSH) Flood involves sending a large number of TCP packets with the PSH bit enabled. The purpose of a PSH packet is to bypass packet buffering, which allows for the efficient transfer of data by ensuring packets are filled to the maximum segment size when multiple packets are sent over a TCP connection. If the PSH bit is enabled, it indicates the packet should immediately be sent to the application. In normal circumstances, this does not present an issue, however when a significant number of PSH packets are sent to a target server, there is a potential to overload its resources, creating a DoS situation.

UDP Flood

A UDP Flood is very similar to a SYN Flood in that an attacker uses a botnet to send a significant 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 seeks 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, checks for an application that is listening on that port. If nothing is listening on that port, it replies 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. This forces the server to process each one, and in most cases, respond to each one. This type of attack 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.
 - Many legitimate services 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+).
- If you identify an attack, try to leverage your upstream network service provider in order for them to mitigate the activity before it reaches your network.
- To minimize the effect of UDP Flood attacks, define strict rules on your perimeter network devices, like firewalls, to allow only 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, the request is then forwarded on to all live computers on the 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 can send enough ICMP traffic 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. By using these variables correctly, and with enough source machines initiating the traffic, it is possible to consume all of the available bandwidth.

Recommendations:

- To identify an ICMP Flood, investigate network logs and look for a significant 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 displayed in the graphical user interface, such as with WireShark. When analyzing ICMP traffic you will notice that no port information is available, as ICMP does not use network ports like TCP or UDP.
 - 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 <http://www.nthelp.com/icmp.html>
- If you identify an attack, 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. Packet-per-second thresholds effectively keep your network from being overrun with ICMP traffic.
 - Note: The above step does 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 to have 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.

HTTP GET Flood

An HTTP GET Flood occurs when an attacker, or attackers, generate a significant number of continuous HTTP GET requests for a target website in an attempt to consume enough resources to make the server unavailable for legitimate users. In this case, the attacking IP addresses never wait for a response from the target server, despite the server attempting to respond to all incoming requests. This results in connections being left open on the web server. A large enough number of incoming HTTP GET requests to the target web server eventually exhausts all available server resources and results in a successful DDoS attack.

Recommendations:

- To identify an HTTP GET Flood, investigate network logs and look for a large number of inbound traffic from a significant number of source IP addresses with a destination port of 80 and a protocol of TCP. The packet data should also begin with "GET". We recommend using either Tcpcdump or Wireshark.
 - HTTP GET requests are normal and are not on their own indicative of malicious activity. Look for a large number of identical GET requests coming from a large number of sources over a short period. The same source IP addresses should re-send the same GET requests rapidly.
- If you identify an attack, leverage a DDoS mitigation service provider for the best results in mitigating this activity.
- It is difficult to set up proactive security measures to block against this attack, as legitimate traffic is used to carry it out. Often, rate based protections are not sufficient to block this attack, and the source IP addresses of the attack are part of a large botnet, so blocking every source IP is not efficient and may include legitimate users.
 - One solution that may help mitigate this type of attack is to use a Web Application Firewall (WAF). HTTP Floods often exhibit trends that a correctly configured WAF filters and blocks without blocking legitimate access to the web server.

HTTP GET Flood Variation: HTTP POST Flood

Another HTTP Flood incorporates the use of the HTTP POST request instead of GET. This attack works because it forces the web server to allocate more resources in response to each inbound request. A large number of these requests could tie up enough server resources as to deny legitimate users access to the web server.

REFLECTION DDoS ATTACK TYPES

NTP Reflection Attack with Amplification

A Network Time Protocol (NTP) reflection 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 typically have a fixed packet size that can be identified across a large number of replies. Since the response from the NTP server is larger than the request sent from the attacker, the effect of the attack is 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 are sent back to the target. This eventually results 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 have the ability to place a filter at their level that forces inbound NTP traffic, using the specific packet size that you are experiencing, to drop.
- 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 whether or not your NTP server is vulnerable to being utilized in an attack, follow the instructions available at OpenNTP: <http://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 you are unable to upgrade your server, disable the monlist query feature 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) Reflection attack occurs when the attacker manipulates the DNS system to send an overwhelming amount of traffic to the target. DNS servers resolve IP addresses to domain names allowing the average Internet user to type an easily remembered domain name into their Internet browser, rather than 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 then sends 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.

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.
- If you identify an attack, 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.). In doing so, this ensures that your DNS servers are not used to attack others.
 - Instructions for disabling recursion can also be found at Team Cymru: <http://www.team-cymru.org/Services/Resolvers/instructions.html>.
 - To discover if any of your public DNS servers may be used to attack others, use the free test at openresolverproject.org.

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, which is used to notify other WordPress websites that you have put a link to their website on your site. 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 web page 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 with the URL of the target website, 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 web page 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 appears as HTTP GET requests for random values such as “?5454545=6767676”. This request bypasses the cache and forces a full-page reload for every packet.
- If you identify an attack, 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 WordPress websites are not used to attack others. To do this, WordPress offers a tool that is available for download that disables the pingback feature of XMLRPC. Download the tool at the following link: <http://wordpress.org/plugins/disable-xml-rpc-pingback/>.
 - Alternatively, you can create a plugin for the website that adds a filter that manually disables the pingback function of XMLRPC. An example of this plugin can be found at <http://blog.cisecurity.org/wordpress-pingback-feature-being-used-in-ddos-attacks/>

SSDP Reflection Attack with Amplification

The Simple Service Discovery Protocol (SSDP) is commonly used for the discovery of Universal Plug and Play (UPnP) devices. UPnP is a series of networking protocols that allows networking devices to discover and connect with one another, without user intervention. Using SSDP, Simple Object Access Protocol (SOAP) is used to deliver control messages to UPnP devices. A SSDP reflection attack occurs when an attacker spoofs the victim's IP address and sends crafted SOAP requests to open UPnP devices on the Internet. These devices then send their responses to that victim IP address. Depending on how the attacker crafted the request, the response could be amplified by a factor of 30 from a single request.

According to OpenSSDPProject.org, there are over 80 million devices on the Internet that are vulnerable to UPnP and SSDP related exploits. When an attacker spoofs a victim's IP address and sends crafted SOAP requests over SSDP to a large number of public UPnP devices, the amplified responses are sent back to the victim, eventually resulting in the consumption of all available bandwidth.

Recommendations:

- To identify if an SSDP Reflection Attack with Amplification is occurring, investigate network logs and look for inbound source port 1900/UDP (SSDP) traffic from a large number of source IP addresses.
- 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, take the following preventative measures to ensure that your UPnP devices are not used to attack others.
 - If you are unsure if any devices on your network could be employed in an attack, follow the instructions available at OpenSSDP to check: <http://openssdpproject.org/>
 - It is also recommended to block outbound port 1900/UDP traffic at your border routers, and restrict UPnP to the internal network if required.

Microsoft SQL Reflection Attack with Amplification

Microsoft (MS) Structured Query Language (SQL) is a popular application used to manage relational databases. Database servers using MS SQL are sometimes left on external IP addresses so that they can be accessed remotely over the Internet. A MS SQL reflection attack occurs when an attacker spoofs the target's IP address and then sends crafted requests to public-facing MS SQL servers using the MS SQL Server Resolution Protocol (MC-SQLR), which listens on port 1434/UDP. The response from the database server contains information about the database instances running on the server as well as how to connect to each one. Depending on the configuration of the database server, and the number of database instances on the server, the response to the client request could be amplified by a factor of 25 for a single request.

Attackers can send scripted MC-SQLR requests, spoofing the target's IP address, to a large number of public-facing MS SQL servers. The amplified responses are sent back to the target, possibly resulting in the consumption of all of the target's available bandwidth.

Recommendations:

- To identify if a MS SQL Reflection Attack with Amplification is occurring, investigate network logs and look for inbound source port 1434/UDP (MC-SQLR) traffic from a large number of source IP addresses. In some instances, it may be possible to identify a particular payload signature.
- If you identify an attack, try to leverage your upstream provider in order for them to mitigate the activity before it reaches your network.
- If possible, block inbound connections to port 1434/UDP or filter connections to allow only trusted IP addresses.
- Along with mitigating inbound attacks, take the following steps to prevent your MS SQL server from being used as a reflector in attacks against others:
 - Use ingress and egress filters on firewalls to block SQL server ports. Port 1434/UDP should be open only if there is an identified need for the service. If the port is open, it is recommended that traffic be filtered to allow only trusted IP addresses.
 - SQL servers that have only one database instance running do not need to run MS-SQLR. If you are running only one database instance, disable MS-SQLR.
 - As of Microsoft SQL Server 2008 the feature is disabled by default. However, earlier versions require administrators to disable this service manually. If you are running an older version of the software and there is not a need for MS-SQLR, disable it. If it is determined that MS-SQLR is needed, consider adding an additional layer of security, such as requiring authentication via SSH or VPN, in front of the service.

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 reduce the impact of attempted 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 case of a DDoS attack, the faster a provider 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. It is important to ascertain to whom an IP belongs to when examining network logs during an attack. Use tools such as the American Registry for Internet Numbers (ARIN) (<https://www.arin.net>) to look up 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 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 recommendation assists with keeping 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), unassigned DHCP clients (169.254.0.0/16), multicast (224.0.0.0/4) and otherwise listed in RFC 5735. This configuration 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 only to accept traffic detailed in your organization’s security policy as required for business purposes.
- Consider setting up Out-of-Band access, Internet and telephony, to an incident management room to ensure connection in the event of a DDoS attack that disrupts normal connectivity.

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/>