the Availability Digest

www.availabilitydigest.com
@availabilitydig

Surviving DNS DDoS Attacks

November 2013

DDoS attacks are on the rise. A DDoS attack launches a massive amount of traffic to a website to overwhelm it to the point that it no longer can function. The website does not have the resources or network bandwidth to respond to legitimate requests from its users. Results can include lost revenues, lost customers, and lost brand reputation.

A particularly sensitive system in a company's web infrastructure is its DNS server. The DNS server responds to requests to convert URLs to IP addresses so that messages can be sent to target systems over the Web. Without its DNS server, a company cannot communicate with the outside world.

Secure64's DNS Authority[1] (www.secure64.com) is a dedicated, authoritative DNS name server that is designed to be self-protecting. It identifies and blocks attack traffic while continuing to respond to DNS queries from legitimate sources.

Bigger DDoS Attacks Are Coming More Frequently

Early on, most DDoS attacks generated about 10 gigabits-per-second (gbps) of malicious traffic. However, the severity of DDoS attacks is increasing to the point where malicious traffic is now measured in the hundreds of gigabits per second. The frequency of attacks is also increasing. The number of attacks increased 53% from 2011 to 2012.

Two notable examples reported in the Digest were attacks against U.S. banks and Spamhaus:

- In September, 2012, in retaliation for the anti-Islamic YouTube video "Innocence of Muslims, Islamic hackers launched massive DDoS attacks against several U.S. banks that took down their online banking portals for over a day each. In December, they repeated their attacks; and they have vowed to continue the attacks until the video is removed from the Internet.[2] Their attacks so far have generated up to 70 gbps of malicious traffic – enough to overwhelm most web sites.

- In March of 2013, Spamhaus was hit with the most massive DDoS attack yet reported – a malicious data rate of 300 gbps! Spamhaus is a firm that maintains a blacklist of spam-generating sites and sells the list to corporations, government agencies, and ISPs so that they can block traffic from these sites. One of the web sites on the blacklist is CyberBunker. It is CyberBunker that is suspected of launching the attack.[3]

[1] Surviving DNS DDoS Attacks, *Secure64 White Paper*. Available at www.secure64.com.

[2] Islamic Hacktivists Attack U.S. Banks, *Availability Digest*; October 2012.
http://www.availabilitydigest.com/public_articles/0710/bank_attacks.pdf
DDoS Attacks on U.S. Banks Continue, *Availability Digest*; January 2013.
http://www.availabilitydigest.com/public_articles/0801/more_bank_attacks.pdf

[3] History's Largest DDoS Attack?, *Availability Digest*; April 2013.
http://www.availabilitydigest.com/public_articles/0804/spamhaus.pdf

Current Defenses Against DDoS Attacks

To defend against DDoS attacks directed at their DNS servers, companies have invested in more sophisticated firewalls and Intrusion Prevention Systems (IPS), and they have over-provisioned their networks and DNS servers for sufficient capacity to ward off attacks. However, these solutions add cost, complexity, and latency to the network.

Router ACLs (access control lists) can be used to block attack traffic once it has been identified, but they do not detect DDoS attacks on their own. Traditional firewalls pass or block traffic from ranges of IP addresses, but they are not designed to analyze the traffic that passes through them. This makes them unable to defend against protocol exploits or UDP or TCP flood attacks. Though IPS appliances do a good job of detecting invalid packets, they cannot detect attacks that employ valid packets like UDP and TCP floods.

DNS Attacks and Their Mitigation with Secure64 DNS Authority

The Secure64 DNS Authority server detects several types of DNS attacks and mitigates them to protect the DNS server. Attacks can be categorized either as protocol exploit attacks or flood attacks. Flood attacks include TCP SYN floods, illegal DNS packet floods, UDP floods, and TCP floods.

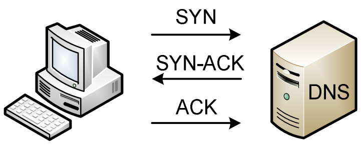
Protocol Exploits

Protocol exploits send illegal IP or TCP traffic to a target DNS server in an attempt to cripple the I/O driver that is handling the network traffic.

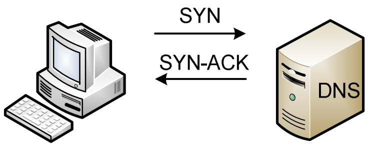
These attacks are easily mitigated by DNS Authority by simply testing the I/O driver for all combinations of invalid traffic. Malformed packets or invalid combinations of header bits are dropped immediately. Packet types that are protected include ARP packets, MAC packets, TCP packets, and IP packets.

TCP SYN Flood

A TCP SYN flood corrupts the three-way handshake used by TCP to establish a connection. In this protocol, the connection initiator sends a SYN request. The target system responds with a SYN-ACK indicating that it is ready to establish a connection. The initiator sends an ACK to complete the connection.



Connection Establishment Protocol



TCP SYN Flood Attack

During a TCP SYN flood, the attacker sends a SYN request to the victim DNS server with a spoofed sending address. The victim system responds with a SYN-ACK, but the attacker does not send the final ACK. Nor does the spoofed sender, since it receives the SYN-ACK but knows that it did not send the SYN. The victim machine allocates resources to the pending connection and holds them for several minutes before timing out. By sending a flood of SYN requests to the victim, the attacker can quickly consume all of the connection resources of the victim system, preventing it from establishing any new connections with external systems.

The Secure64 DNS Authority server protects against TCP SYN flood attacks by not allocating connection resources until the three-way handshake is complete. When a SYN is received, a small pre-connection entry is made in a data structure and begins to age. If the final ACK is received before the timeout, resources are allocated and the connection is completed. If the final ACK is not received, the pre-connection entry is deleted.

Thus, no critical resources are allocated until the connection protocol has been completed, and TCP SYN floods have no effect on the system. Established connections continue to operate normally.

In addition, the DNS Authority server limits the number of incoming SYNs to 100,000 per second.

Illegal DNS Packet Floods

DNS reflection is a particularly vicious type of attack since it can generate massive amounts of malicious data sent to the victim DNS server with only a relatively small amount of effort on the part of the attacker. DNS reflection was used in the recent attack on Spamhaus, referenced earlier, to generate a DDoS attack of 300 gbps.

DNS reflection depends upon DNS open resolvers. An open resolver is a DNS server that will respond to a request from any source. The attacker sends DNS requests to resolve an address to multiple open resolvers with the spoofed source IP address of the victim DNS server. The open resolver DNS system will return its response to the victim DNS server, thus potentially overwhelming it. The reason that this is a particularly vicious attack is that the DNS response message is about 100 times as big (about 3,000 bytes) as the request message (about 30 bytes). Therefore, the attacker can generate a massive amount of malicious traffic by generating only 1% of that traffic.

Years ago, DNS open resolvers were recognized as a security issue; and efforts were made to close all DNS resolvers. Unfortunately, busy network administrators are not particularly incentivized to update their DNS servers. There are still about 27 million open resolvers on the Internet, and their IP addresses are known.

To mitigate DNS packet floods, the Secure64 DNS Authority server takes advantage of the fact that its job is to respond to queries, not to get query responses. The I/O driver rejects any DNS query responses received by the DNS server's configured DNS IP addresses and ports and allows only properly formatted DNS queries to be delivered to the server. Thus, the massive attack by a flood of DNS responses never reaches the DNS server.

UDP Data Floods

Similar to the illegal DNS packet floods described above that overwhelm a DNS server with false DNS query responses, UDP floods overwhelm a DNS server with false DNS queries. The attacker uses a botnet (a network of compromised computers) to make more requests of a DNS server than it can handle. This causes the DNS server to drop inbound UDP DNS requests. Thus, legitimate users cannot get service reliably from their DNS server. The source addresses of the botnet are spoofed so that they cannot be filtered.

Protection against UDP floods are more difficult to handle than the previously described attacks since the DNS server is being bombarded with what appears to be legitimate traffic. The DNS Authority server protects itself from these floods through automatic IP-based rate limiting and configurable aggregate rate limiting:

- The aggregate number of UDP packets per second can be limited.
- The number of UDP packets per second can be limited from each source IP address.
- If the packet rate from a given source exceeds the designated limit, the IP address is blacklisted and all of its incoming packets are dropped.
- If the flood from a blacklisted IP address drops off, the IP address is removed from the blacklist to ensure that a spoofed address does not block a real user.
- Repeat offenses result in faster blacklisting than the initial offense.

If the aggregate packet rate should be exceeded, DNS Authority will begin to drop packets on a probabilistic basis to maintain the incoming packet rate at the configured limit. This may result in the loss of some good traffic, but the server can remain available to much of the good traffic and to administrators.

TCP Data Floods

Similar to the UDP floods described above, TCP floods cause the DNS server to refuse to establish new connections. Thus, legitimate users cannot get service reliably from their DNS server. The source addresses of the botnet are spoofed so that they cannot be filtered.

For TCP traffic, DNS Authority tracks resource usage (specifically, network buffers) to detect and block specific overload situations. Data sources that are consuming more than their fair share of system resources are detected and blocked. TCP traffic rules include the following:

- The aggregate number of packets in the network buffers can be limited.
- The number of TCP packets per second can be limited from each source IP address.
- Administrators can specify that trusted TCP traffic is not subject to mitigation.
- If the packet rate from a given source exceeds the designated limit, DNS Authority issues a TCP Reset (RST) packet to block the attacker.

If the aggregate packet rate should be exceeded, DNS Authority will begin to drop packets on a probabilistic basis in a manner that maintains the distribution of network-buffer resources. As with UDP flood control, this may result in the loss of some good traffic, but the server can remain available to much of the good traffic and to administrators.

Test Results

The Secure64 DNS Authority server was tested by ExtremeLabs, an independent test laboratory. The tests and their results included the following:

Protocol Exploits

The DNS Authority server was placed under a nominal load of legitimate traffic, and then subjected to an ARP flood in which the DNS server was flooded with inaccurate ARP protocol-based information at an increasing rate.

The DNS Authority server remained 100% responsive to legitimate queries while mitigating the ARP flood attack until the total data rate saturated the Gigabit connection at 830 Mbps of traffic.

TCP SYN Floods

The DNS Authority server was placed under a legitimate traffic load while TCP SYNs were generated from a number of source systems at an increasing rate.

The DNS Authority server remained 100% responsive to legitimate queries while mitigating the SYN flood attack until the total data rate saturated the Gigabit connection at 830 Mbps of traffic.

Illegal DNS Packet Floods

The DNS Authority server was placed under a maximum load of 102,000 legitimate queries per second. It was then subjected to a DNS reflection attack of approximately 150,000 packets per second (about 82 Mbps of attack traffic).

The Secure64 DNS Authority server was able to answer 100% of the 102,000 legitimate queries per second while dropping the reflected DNS reflection attack.

UDP and TCP Data Floods

To test DNS Authority's response to UDP floods, a botnet directed a high volume of legitimate DNS queries at the victim DNS server. The DNS Authority server blocked this traffic and maintained 100% availability.

Secure64 published no test results for TCP floods.

Summary

Secure64 DNS Authority is a self-protecting DNS server that detects and blocks a wide variety of DDoS attacks with little if any degradation of service. DNS Authority can reduce the need to overprovision server resources and eliminates the need to protect servers with network security devices.

DNS Authority does not use BIND, the open-source freeware that is often used for DNS security. The problem with BIND is that a new vulnerability is found every few weeks requiring patching. Secure64 built its own operating system and does not use BIND.

The DNS Authority server uses multiple defenses to mitigate DDoS attacks. These attacks include protocol exploits, TCP SYN floods, reflected DNS attacks, and UDP and TCP data floods. Testing by an independent testing lab showed that DNS Authority survived without incident all but the UDP and TCP floods. In these cases, DNS Authority continued to service most legitimate requests; though some requests were dropped and had to be repeated.

Funded in part by the Department of Homeland Security, Secure64's products are sold worldwide by both Secure64 and HP. According to Secure64, it never has had a customer experience any down time due to a DDoS attack.