DNS Amplification Attacks on the Rise

Domain Name System (DNS) amplification attacks are a type of powerful distributed denial-of-service (DDoS) reflection attack that have a long history dating back to the "Smurf" attack in 1997. Today's DNS amplification attacks are even stronger, can slow down Internet access and cause significant damage to the intended target.

Breaking records: DNS attacks spike HUGE numbers

The NSFOCUS research team, which tracks and analyzes trends in cyber security, found that DNS amplification attacks are being adopted more frequently. On May 30, 2013, the DNS amplification DDoS attack (DrDoS) in history hit the financial sector with traffic up to 167Gbps. The attack started on May 27 and was aimed at the real-time trading platforms of financial institutions.

DoS attacks can be roughly classified into three types, based on their targets and layers:

- Network layer - attacks on network bandwidth resources
- Transmission layer - attacks on connection resources
- Application layer - attacks on computing resources

DNS attacks mainly occur at the network layer. In this scenario, the network interface bandwidth of a server or data packet processing capacity of Internet infrastructure (for example, a router or switch) has an upper limit. When the number of arriving or transiting network packets exceeds the upper limit, it can cause network congestion or a slow response. DDoS attacks at the network layer send a large number of network packets by using widely distributed zombie hosts (slave computers), exhausting all bandwidth resources of the target so that normal requests will not receive timely and effective responses.

Shutting Down Spamhaus

DNS amplification attacks follow the general principle of reflection attacks and have particular features of the DNS protocol.
Attackers can initiate a DDoS attack at the network layer via Ping Flood or User Datagram Protocol (UDP) Flood. However, this is an inefficient method that also makes it easy to find the attack sources. Attackers can hide sources by using forged source IP addresses, but the DDoS reflection attack technology is a better approach.

During the DDoS attack on Spamhaus in March 2013, attackers mainly used DNS amplification attack technology to increase traffic to an unprecedented level of 300 Gbps, affecting even the response time of the local Internet.

**Snapshot of a DDoS Reflection Attack**

The following figure shows the relationship between DDoS attacks on network bandwidth resources, connection resources, and computing resources.

DDoS reflection attacks, which target at network bandwidth, use routers or servers to respond to requests, thus reflecting the attack traffic and hiding the attack sources.
During a DDoS reflection attack, the attacker sends a large number of data packets by controlling zombie hosts at the control end. These data packets are directed through the servers or routers that are used as reflectors, cloaking the source IP address and mimicking the IP address of the intended target. The reflector thinks that the data packet is a request originally sent by the attack target itself, causing it to respond. When a large number of response packets are sent to the intended target, a DDoS attack is generated.

To initiate a DDoS attack, the attacker needs to find a large number of reflectors on the Internet. For certain types of reflection attacks, this is not a difficult task. For an ACK reflection attack, the attacker needs to find servers that only enable their TCP ports, which widely exist on the Internet.

As compared with DDoS attacks that directly forge source IP addresses, DDoS reflection attacks add an extra step, thus making it more difficult to identify the attack sources.

**DNS Amplification Attack**
DNS amplification attack is a typical type of DDoS reflection attack which reflectors amplify network traffic.

DNS, a distributed database that can map domain names and IP addresses mutually, is a core service of the Internet. It enables people to access the Internet without having to remember the IP strings that are directly read by computers. DNS uses TCP port 53 and UDP port 53, and mainly complies with UDP.

Usually, a DNS response packet is larger than a DNS query packet. By taking advantage of an ordinary DNS query request, an attacker can amplify the attack up to tenfold. A more effective approach is Extension Mechanisms for DNS (EDNS0), which is the DNS extension mechanism defined in RFC 2671.

Before the advent of EDNS0, the maximum size of a DNS response packet was limited to 512 bytes. When the size of a response packet is greater than 512 bytes, the excess size may be discarded, or the TCP is used to establish a new connection to send the DNS response packet again, depending on the implementation of the DNS service. Neither of these two modes is conducive to amplifying the attack traffic.

In EDNS0, the structure of each DNS packet is extended; specifically, the OPT Resource Record (RR) field is added. The OPT RR field contains the maximum size of a UDP packet that can be processed by the client. When responding to a DNS query request, the server resolves and records the size, generating the appropriate response packet.

Attackers initiate effective DNS amplification attacks by means of Domain Information Groper (DIG) and EDNS0.

---

1 RFC 2671: Extension mechanisms for DNS (EDNS) is a specification for expanding the size of several parameters of the Domain Name System (DNS) protocol. The first set of extensions was published in 1999 by the Internet Engineering Task Force as RFC 2671, also known as EDNS0.
The attacker sends dig query requests to the widely distributed open DNS resolvers, sets the UDP packet size contained in the OPT RR field to a large value (for example, 4096) and mirrors the source IP address of the query requests as the IP address of the attack target. After receiving the query requests, the DNS resolvers send the resolution results to the attack target. When a large number of resolution results arrive at an attack target, the target network is congested and runs slowly, thus causing a DoS attack.

The size of a DNS query request packet sent by the attacker is usually 60 bytes, and the size of a returned result packet is usually more than 3,000 bytes. Therefore, this attack mode can achieve amplification of at least 50-fold. In extreme cases, a 36-byte query request can lead to a response of 3,000 to 4,000 bytes. In other words, the attack traffic can be amplified by 100-fold.

**Attacking Conditions: DNS amplification attack**

The method of DNS amplification attacks are similar to DDoS reflection attacks, except that the network services provided by reflectors and amplifiers must meet certain conditions.

First, there is an asymmetry between the amount of request data and amount of response data in the Network Service Protocol (NSP) provided by the reflectors. The amount of response data should be
greater than that of request data. The greater the ratio, the higher the amplification factor and the more significant the impact is.

Secondly, amplification attacks often use protocols that require no authentication or handshaking. If the protocol used requires authentication or handshaking, the process cannot be implemented, making it impossible to launch subsequent attacks. Therefore, most amplification attacks are initiated over UDP-based network services.

Finally, the popularity of network services used by amplifiers determines the scale and severity of the DDoS attack. Assume that a certain network service is authentication-free and provides a very good amplification effect, but it is rarely deployed on the Internet.

Assume that a certain network service is authentication-free and provides a very good amplification effect, but it is rarely deployed on the Internet. This means the network service cannot be used to amplify the attack traffic significantly, failing to achieve the level of a DDoS attacks and function as a DDoS attack amplifier.

Protection Methods

The protections against DNS amplification attacks can be classified into three types:

- **Protecting Devices that Enable DNS Service**

  First, identify whether the DNS services on the device are necessary. If they are not, disable the DNS services.

  If the DNS services are required, take measures to reinforce the authentication of requests. For example, the DNS services should respond to only the DNS resolution requests that are submitted by an ISP or are generated inside the network, rather than the DNS resolution requests that are submitted by any PC on the Internet. Finally, restrict the maximum size of each DNS response packet and discard oversized response packets directly. DNS amplification attacks can be prevented as long as you effectively protect devices that enable DNS services.

- **ISPs Filter Data Packets with Forged Source IP Addresses**

  Attackers can send data packets with forged source IP addresses, which is the root cause of DDoS attacks at the network layer. By forging source IP addresses, attackers can not only initiate DDoS
reflection and amplification attacks, but effectively hide the attack sources. If an ISP can filter the data packets with forged source IP addresses, and thus exclude such data packets from the Internet, DDoS attacks at the network layer can be prevented.

RFC 2827/BCP 38 highly recommends ingress filtering to block network attacks with forged source IP addresses. Regrettably, only a few companies and ISPs follow the recommendations. Network attacks with forged source IP addresses can be thoroughly prevented only when all devices on the Internet comply with the recommendations.

- **Diluting and Cleaning Attack Traffic by Using Anycast Technology**

Through DDoS amplification attack technology, traffic can be amplified significantly. Attack traffic of such a large scale needs to be cleaned on multiple centers in a distributed manner, thus spreading and diluting the attack traffic. Subsequently, each cleaning center performs this function on the attack traffic.

Anycast technology is a feasible solution, spreading attack traffic to different cleaning centers. In a normal environment, Anycast can ensure the request data of a user is routed to the nearest cleaning center. In case of a DDoS attack, Anycast can effectively dilute the attack traffic to the network infrastructure of the defender. In addition, each cleaning center declares the same IP address, and attack traffic is not converged to a single position. The attack mode changes from multi-to-one attacks to multi-to-multi attacks, thus preventing a single-point bottleneck in the network. After the attack traffic is diluted, it becomes relatively easier for centers to perform conventional cleaning and blocking on the attack traffic.

**Conclusion**

DDoS reflection attacks are a type of DDoS attack aimed at the network layer. These attacks generate the attack traffic by taking advantage of the asymmetry between request data and response data in the NSP, authentication-free network services and extensive deployment of network services.

One of the common DDoS reflection attack technology is used to initiate DNS amplification attacks. Other protocols and network services can also be used as an auxiliary means to increase the traffic of DDoS amplification attacks.
To attain the most effective protection against DDoS reflection attack, and DNS amplification attack protective measures should be taken in three respects: attack source, amplifier and attack target.
For more information about NSFOCUS products and services, please contact the NSFOCUS sales

NSFOCUS
TEL: +86 10 68438880
EMAIL: info@nsfocus.com

NSFOCUS US
TEL: +1 408 907 6638
EMAIL: info-us@nsfocus.com

NSFOCUS Japan
TEL: +81 3 6206 8156
EMAIL: info-jp@nsfocus.com

For more information visit NSFOCUS Website: www.nsfocus.com

"NSFOCUS" is the trademark of NSFOCUS Information Technology Co., Ltd.

NSFOCUS enjoys all copyrights with respect to all textual narrations, document formats, illustrations, photographs, methods, processes and other contents, unless otherwise specified, which shall be governed by relevant property rights and copyright laws. Without written permission of NSFOCUS, any individual or institution shall be prohibited to copy or quote any section herein in any way.

**About NSFOCUS**

NSFOCUS is a proven global leader in active perimeter network security for service providers, data centers, and corporations. It focuses on providing network security solutions including: carrier-grade Anti-DDoS System, Web Application Firewall, and Network Intrusion Prevention System - all designed to help customers secure their networks and corporate-critical information. More detailed information is available at http://www.nsfocus.com.