Defending the DNS Infrastructure

The DNS (Domain Name System) protocol is a critical part of the Internet's control plane, providing name resolution functionality and supporting other capabilities that are taken for granted such as load-balancing and internet traffic management. The availability of DNS is key for anyone providing services or content across the Internet; if the DNS infrastructure is unavailable or slow, the user experience would be impacted to the point of "no internet service".

Challenge

A good example of the devastating effects an attack targeting DNS infrastructure can have was the well-publicized Mirai botnet campaigned against DYN at the end of 2016.

DYN, now a part of Oracle, is a provider of DNS services to a number of well-known Internet brands, and when its infrastructure was hit by a number of massive DDoS attacks in a very short period of time, millions of users could no longer reach the web properties of those brands.

Although the DDoS attacks did not target the web servers and infrastructure of the affected companies directly their URL's could not be resolved into IP addresses. As a result and for all practical purposes, these websites were not reachable by users and appeared to be down.

The attack against DYN DNS infrastructure used an application-layer DDoS vector known as "water-torture" where the Mirai botnet generated DNS queries for millions of random hosts such as aaaa. Netflix.com, bb.Netflix.com, ccccc.Netflix.com and so on. This put a huge load on the Authoritative DNS infrastructure, in this case provided by DYN, causing it to become unavailable for genuine user queries.

As well as being a target for sophisticated application-layer DDoS attacks such as the DYN example, DNS infrastructure can also be leveraged to generate large-scale volumetric attacks using a technique known as reflection-amplification. DNS reflection-amplification attacks have historically been some of the largest volumetric attacks seen across the Internet, measuring hundreds of Gbps in size. Reflection-amplification takes advantage of the following:

- DNS predominantly uses the connectionless UDP transport layer protocol, so a user can send a query without an initial handshake being required.
- Many DNS resolvers will respond to queries originating from anywhere. There are millions of these around the world.
- DNS responses can be many times the size of the initial query resulting in amplification factors of 10s or 100s of times.

DNS reflection-amplification attacks involve an attacker botnet sending queries to a number of DNS servers (usually the low thousands in number) for a domain with multiple DNS records (an ANY query results in all of these records being returned). This will result in a large response. The 'trick' is that the bots will generate the DNS queries using the source IP address of the intended DDoS victim. The DNS servers will innocently send their large responses back to the victim, with the traffic volume being many multiple times larger than that generated by the original botnet. This is reflection-amplification.

Solution

To defend against DDoS attacks targeting DNS services, it is key to quickly detect any kind of DNS vector attack; both application-layer and volumetric reflection-amplification types. By leveraging Arbor Sightline and Arbor Sightline With Sentinel to provide the visibility and fast detection at Layer-3/4 via Netflow and Layer-7 with Smart Data, NETSCOUT® is uniquely positioned to protect DNS infrastructure.

Arbor Sightline and Sentinel are at the heart of the NETSCOUT Smart Visibility and Protection Solution. The use of Netflow, BGP and SNMP allows the system to detect within seconds any DNS volumetric attack such as the reflection-amplification type, giving the infrastructure provider the means to react and defend in a real-time manner. With the addition of CyberStream, the Arbor Sightline and Sentinel system will consume and analyze Smart Data, providing the Layer-7 visibility to detect faster and more effectively any of the DNS application-layer DDoS vectors such as "water-torture", DNS malformation, NXDOMAIN, etc.

To close the loop on how to defend against DNS DDoS attacks, it is necessary to consider the appropriate techniques to mitigate these attacks in a holistic way.

An orchestrated, automated and integrated mitigation is the cornerstone of NETSCOUT's Mitigation Without Borders. This approach consists of combining different capabilities and systems that provide NETSCOUT with a distinctive positioning and competitive advantage:

- Utilizing the capabilities in the network infrastructure to defend against DNS DDoS volumetric attack vectors via BGP Flowspec.
- Enabling Network Operators to leverage inter-operator signaling capabilities to collaborate in the mitigation of DNS DDoS attacks, and defend against the attacks as close to the source as possible.
- Deploying the industry-leading Arbor Threat Mitigation System (TMS) to deal with complex DNS DDoS application-layer attacks. This scalable software solution allows for the most surgical mitigation capability, and the most cost-effective mitigation engine in the market.

Summary

Protecting the Internet DNS infrastructure is a big component of NETSCOUT's Guardians of the Connected World mission. Without this key Internet enabler, the way people and companies communicate, work and collaborate would be drastically and negatively affected.

By leveraging NETSCOUT's technologies, expertise plus experience in protecting the worldwide DNS infrastructure, Service Providers and Enterprises can count on having the Internet "always on" keeping customers and stakeholders connected.

NETSCOUT®

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us