ANATOMY OF A DDoS ATTACK AGAINST THE DNS INFRASTRUCTURE
ANATOMY OF A DDOS ATTACK AGAINST THE DNS INFRASTRUCTURE

The Domain Name System (DNS) is part of the functional infrastructure of the Internet and part of the Internet’s “trust” framework. Without these nameservers, the huge investments in hardware, software and applications that organizations make cannot be found and accessed by customers. Unfortunately, because the DNS is a key piece of infrastructure, it is often targeted by malicious players. Distributed Denial of Service (DDos) attacks targeting the DNS is a specific type of DDoS attack that exposes vulnerabilities in the DNS system. This whitepaper provides an explanation for this specific type of attack.

A DDoS attack is used to bring down a system without leveraging the attackers own system. This helps the attacker to avoid discovery. While this form of attack doesn’t always attempt to gain access to an organization’s data, it can be used maliciously by bad actors to deny resources or inhibit services to a targeted system. Moreover, DDoS attacks in general are on the rise globally and were up 50 per cent in 2013 (Akamai report) with some attacks generating sustained bandwidth in the hundreds of gigabits and for several hours or days. DNS DDoS attacks are a smaller percentage of all DDoS attacks, but fully one-third of companies have reported a customer-impacting attack of this type (source: Arbor 2013 report in security).

HOW DOES THE DOMAIN NAME SYSTEM (DNS) WORK?

The Domain Name System (DNS) provides the core backbone of the Internet by providing the map between easily-readable hostnames (i.e. www.cira.ca) and IP addresses (192.228.29.1) by way of resource records. It is essential to the operation of the Internet by enabling the use of logical, human-readable names for locations rather than complex IPv4 or IPv6 addresses. It additionally provides mappings to things like mail servers, SIP servers, redirects, digital signatures, and more.

The DNS is a distributed database organized as a tree of interconnected nodes (server or server clusters) where each node is a partition of the database. Nodes are delegated to designated authorities and there can be only one authority for a node or group of nodes. The DNS is a critical part of the Internet’s trust framework and functionality and as such is often a target for malicious activity.
HOW A DNS DDOS ATTACK WORKS

Before getting into the mechanics of a DNS-based DDoS attack versus other forms of DDoS attacks, it is worth noting that these attack scenarios can generically describe an attack that applies to the DNS or to an application or web server.

The DNS DDoS attack typically uses three elements in the hackers tool chest: spoofing, reflection and amplification. Since the attacker’s goal is either to saturate a nameserver, or to target another server, these elements of the attack are typically distributed across many open DNS resolvers. Reflection is used to increase the number of queries while amplification comes in when the reflecting server answers the relatively small query with a much larger response.

In the case of the DNS, the problem is compounded because a very small query (<100 bytes) can be amplified (to 50X and up) to generate thousands of bytes in response.

Let’s look a little closer. If the attacker wanted to attack a target DNS server then it would use all the botnet zombies in his network to issue DNS request messages for an amplification record from open recursive servers. If the recursive nameserver has not received a request before then they issue their own request to a compromised server to get the amplification record. The open recursive servers think they are sending a response to the botnet host that generated the query, but it has spoofed the IP address of the attack target. So the organization’s server never issued a request but it is now being bombarded with responses. Making matters worse, because the response is amplified, it is broken into fragments that need to be reassembled at the destination, putting further strain on the target.

There is another scenario, which we will call amplifier exhaustion. It occurs when the organization isn’t the target in the attack, but an unwitting accomplice. Their nameservers are being used in an attack on another server and in the process the bandwidth or resources of the nameserver are being taken up. Maintaining a good DNS architecture is important because it helps protect the organization while also ensuring that it is a good Internet citizen.

Just over 1/3 of companies report DNS DDoS Attacks (Source: Arbor Networks 2013 report on Security).
DNSSEC is a secure handshake protocol for domain names that is used to validate that a user is connecting to a website or service associated with the domain name. It helps to address man-in-the-middle type of attacks. This is distinct from SSL which uses a similar set of protocols to secure the actual communications once they have been initiated.

DNSSEC has rapidly gained adoption by top level domain registries and as of 2014 is beginning to gain more rapid traction across the rest of the Internet with players like Comcast and Google actively promoting its benefits. However, as it does, DNSSEC has the potential to further amplify a DDoS attack because the additional bytes for sending keys can further increase the amplification.

In the example shown we see that without DNSSEC the server provides a 62 byte response to a 72 byte query. With DNSSEC a similar query generates 241 bytes (281 bytes on the wire) to an 83 byte question, or an amplification factor of 341 per cent in this example. Depending on the how the query is crafted a larger amplification is possible with the implication that any DNS server can be used for an attack:

### HELPING TO MITIGATE THE PROBLEM WITH AN ANYCAST DNS INFRASTRUCTURE

Several players in the industry are trying to get the (tens of millions of) open recursive DNS resolvers cleaned-up by focusing on the networks that have them and getting the resolvers shut down. However, this is an extremely challenging global problem that is caused by the inadvertent behaviour of both individuals and corporations. Rather than trying to solve the global issue, there is a more immediate and active response that an IT department can take, and that is to add capacity and redundancy to their DNS. One tool for building out the DNS infrastructure is to use anycast servers.

Anycast DNS servers enable organizations to deploy a set of DNS servers across the globe that all have the same IP address. Since one of the features of anycast DNS is that queries are responded to by the geographically closest server, attacks against one node will only impact customers in that region. Maintaining two or more anycast clouds on different infrastructure and network connectivity provides for even more in-region redundancy to help mitigate the impact of an attack or other outage.

In addition to solving the global risk, if a business has a large domestic component then locating a few high bandwidth international nodes can help to protect your local traffic from an attack that originates off shore. Why? Because the global attack will be soaked-up by the geographically closest off-shore server leaving your domestic ones unaffected.

Even if a global DNS server is brought down, by the time the attack moves to a new node the old one can be back online. In effect it becomes a world-wide game of whack-a-mole on the DNS servers that aren’t delivering content to your most important market or region anyway.
DEPLOYING AN ANYCAST DNS NETWORK

A global company may elect to run one or more anycast clouds to serve its markets. This involves placing enterprise infrastructure and redundancy in the corporate datacenters or branch offices. For very large companies, this approach may be preferred as it gives a high degree of control over the deployment. However, it is costly, and when enterprise-class equipment is used for the DNS, the service is often over-provisioned and represents a non-optimized use of resources.

Alternatively, there are DNS service providers that organizations can use to outsource their DNS. In these instances their DNS is on shared equipment with other companies but can be protected by enterprise-class SLAs and service.

And finally, because of the way anycast is architected, there is the option to combine some in-house infrastructure with one or more best-of-breed secondary solutions. This provides redundancy and capacity for organizations where access to the website is critical.

D-ZONE ANYCAST DNS SERVICE - HELPING IT DEPARTMENTS AND SERVICE PROVIDERS WHO ARE SUPPORTING ORGANIZATIONS WITH A LARGE AMOUNT OF CANADIAN TRAFFIC TO PROTECT AGAINST DDOS ATTACKS

The D-Zone Anycast DNS service is the most robust secondary solution for Canadian traffic available on the market today. It provides redundant, high bandwidth nodes located in IXPs in Canada to answer queries for Canadian traffic. This provides very low latency and helps to keep Canadian web traffic inside Canada’s borders. In addition to these benefits, it serves global markets and helps protect your traffic from DDoS attacks against the DNS by locating high bandwidth global nodes in International Internet hubs. Since a small number of major attacks originate from within Canada, this helps protect your organization from outages due to malicious activity.

Figure: With a single unicast server, when the node goes down or gets hacked, you disappear from the Internet. Anycast allows other nodes in the network to serve traffic.

For more information on how the D-Zone Anycast DNS solution can be used by your organization please contact us today by visiting cira.ca/d-zone

ABOUT CIRA

The Canadian Internet Registration Authority (CIRA) manages Canada’s .CA domain name registry as a 100 per cent up time service for Canadians and Canadian organisations. In addition to stewardship over .CA, CIRA develops and implements policies that support Canada’s Internet community and the .CA registry internationally.