BUILDING A BETTER
ONLINE CANADA

ANATOMY OF A DDOS ATTACK AGAINST THE DNS INFRASTRUCTURE

Protect your business

01-13-2016

ANATOMY OF A DDOS ATTACK AGAINST THE DNS INFRASTRUCTURE

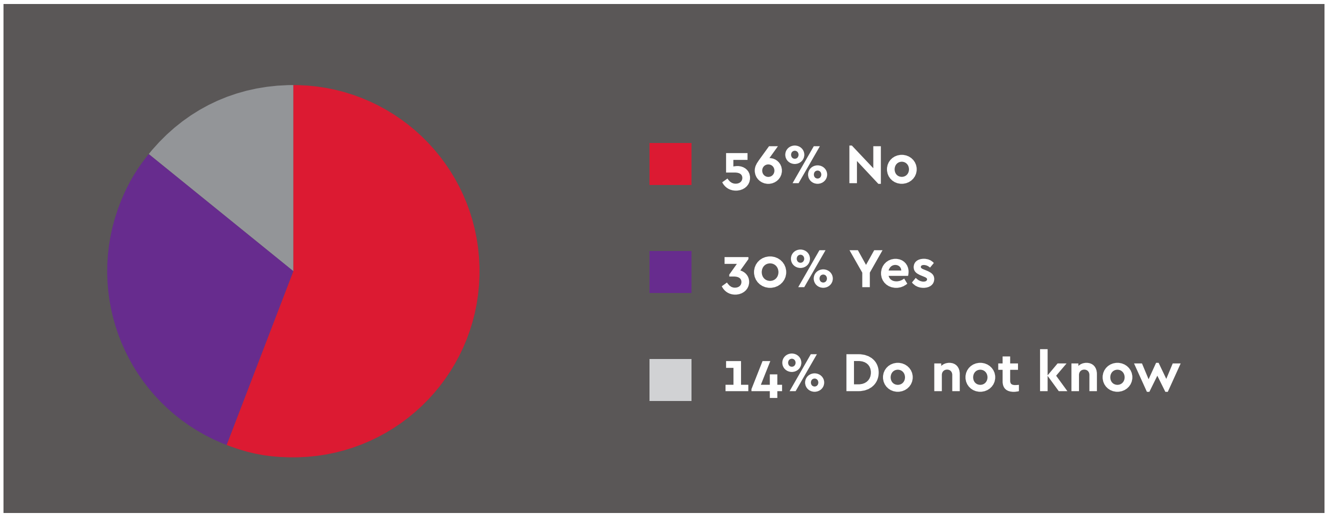
The Domain Name System (DNS) is part of the functional infrastructure of the Internet and part of the Internet's "trust" framework. Without these nameservers, the huge investments in hardware, software and applications that organizations make cannot be found and accessed by customers. Unfortunately, because the DNS is a key piece of infrastructure, it is a piece is 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 solution brief provides an explanation for this specific type of attack.

A distributed denial of service (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, on its own, doesn't attempt to gain access to an organizations data, it can be used maliciously by bad actors to deny resources or inhibit services to a targeted system. Moreover, DDoS attacks in general have been on the rise globally for years and 2016 was no exception. One of the largest ever targeting the DNS occured against Dyn DNS servers in October 2016 and used IoT devices to generate up to 1 TB of traffic. Fully one-third of DNS operators have reported a customer-impacting attack of this type (source: Arbor 2016 Worldwide Infrastructure Security Report). For service providers, this number jumps to 50%!

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.

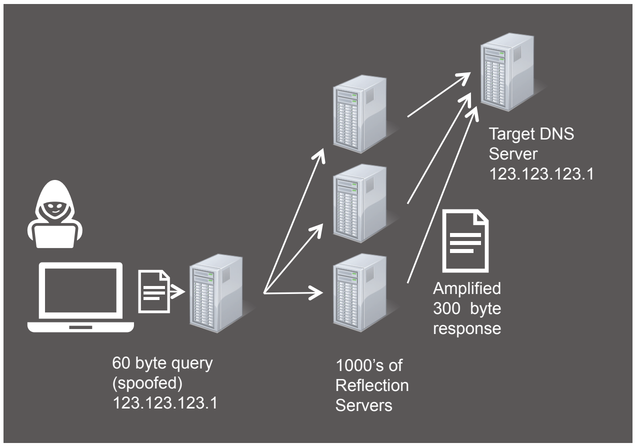
The DNS is a distributed database organized as a tree of interconnected nodes (server or server clusters) where each node is a partition of the database. Nodes are delegated to designated authorities and there can be only one authority for a node or group of nodes.



1/3 of companies report DNS DDoS Attacks (Source: Arbor Networks 2016 Worldwide Infrastructure Security Report)

HOW A DNS DDOS ATTACK WORKS

The DNS DDoS attack uses three elements: spoofing, reflection and amplification. Since the attacker's goal is to saturate a nameserver, these elements of the attack are typically distributed across many open DNS resolvers by using botnets. Using spoofing the attacker sends a large number of queries to tens of thousands of DNS servers where the source IP address is spoofed to the DNS server(s) of the target organization. These servers then reflect the attack from the source to the target. The 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.

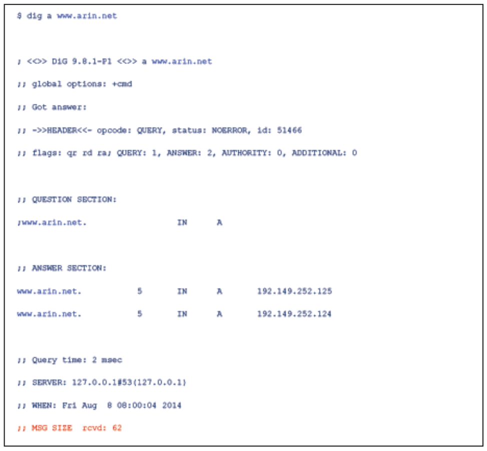

Target DNS Server 123.123.123.1
Amplified 300 byte response
60 byte query (spoofed) 123.123.123.1
1000's of Reflection Servers

Anatomy of a DNS DDoS attack showing spoofing, reflection, and amplification

This is distinct from other types of DDoS against the application layer, in that the host organizations servers may not be directly involved in the solution to the threat. For instance, the response may not be something that can be simply filtered by a firewall's typical features. 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.

THE POTENTIAL ROLE OF DNSSEC

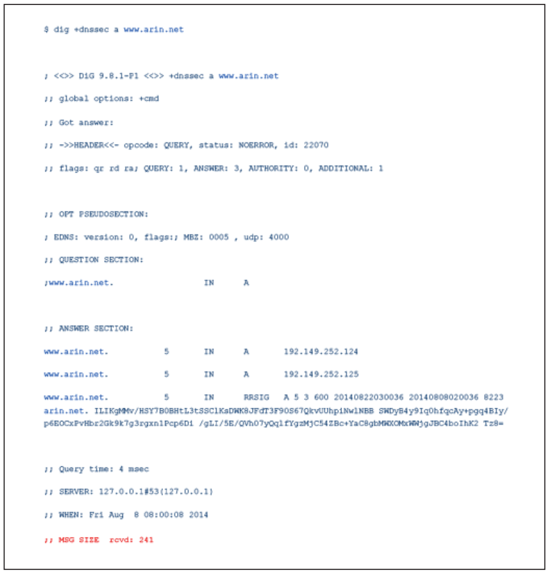
DNSSEC is a secure handshake protocol for domain names that is used to validate that the website the user expects to be accessing is the one that they are accessing. It helps to address a problem that has been around since the dawn of the Internet, and helps to prevent man in the middle type of attacks. 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 Microsoft and Google actively promoting its benefits. However, as it does, it has the potential to further amplify a DDoS attack because the additional bytes for sending keys can further increase the amplification.



```
$ dig a www.arin.net


; <<>> DiG 9.8.1-P1 <<>> a www.arin.net

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51466

;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0


;; QUESTION SECTION:

;www.arin.net.                  IN      A


;; ANSWER SECTION:

www.arin.net.           5       IN      A       192.149.252.125

www.arin.net.           5       IN      A       192.149.252.124


;; Query time: 2 msec

;; SERVER: 127.0.0.1#53(127.0.0.1)

;; WHEN: Fri Aug  8 08:00:04 2014

;; MSG SIZE  rcvd: 62
```

Without DNSSEC

In the following example, we see that without DNSSEC the server provides a 62 byte response to a 72 byte query. With DNSSEC the exact same 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. And depending on the how the query is crafted a larger amplification is possible:



```
$ dig +dnssec a www.arin.net


; <<>> DiG 9.8.1-P1 <<>> +dnssec a www.arin.net

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22070

;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1


;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; MBZ: 0005 , udp: 4000

;; QUESTION SECTION:

;www.arin.net.                  IN      A


;; ANSWER SECTION:

www.arin.net.           5       IN      A       192.149.252.124

www.arin.net.           5       IN      A       192.149.252.125

www.arin.net.           5       IN      RRSIG   A 5 3 600 20140822030036 20140808020036 8223
arin.net. ILIKgMMv/HSY7B0BHtL3tSSClKsDWK8JFdT3F90S67QkvUUhpiNwlNBB SWDyB4y9IqOhfqcAy+pgq4BIy/
p6EOCxPvHbr2Gk9k7g3rgxnlPcp6Di /gLI/5E/QVh07yQqlfYgzMjC54ZBc+YaC8gbMWXOMxWWjgJBC4boIhK2 Tz8=


;; Query time: 4 msec

;; SERVER: 127.0.0.1#53(127.0.0.1)

;; WHEN: Fri Aug  8 08:00:08 2014

;; MSG SIZE  rcvd: 241
```

With DNSSEC

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 allow them and getting them to shut them down. However, this is an extremely challenging global problem that is caused by the inadvertent behaviour of both individuals and corporations. The rapid growth in IoT devices is likely to compound the matter further. Rather than trying to solve the global issue, there is a more immediate and active response to the problem for an IT department.

For application-layer DDoS attacks IT departments focus on their server infrastructure by, for example, limiting responses to packets that are too large, dropping responses altogether, rate limiting traffic, or blocking traffic from certain servers entirely. These types of tactics are an important part of the solution, but one that does not solve the problem against the DNS. For the DNS a tactic which has been successfully deployed by domain name registries and many large organizations is the use of Anycast technology.

Anycast DNS servers enable organizations to deploy a set of DNS servers across the globe that can all resolve the 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.

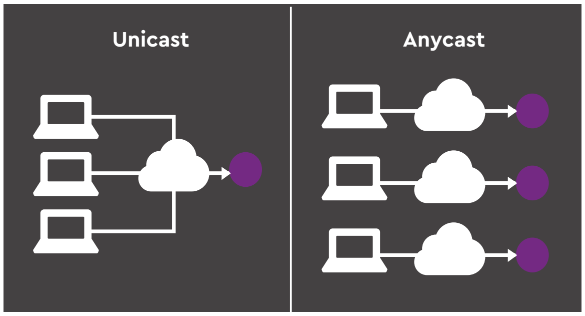
In addition to solving the global risk, if a business has a large domestic component then locating a few high bandwidth local nodes can help to protect your local traffic from an attack that originates off-shore. Why? Because the global attack will be soaked-up by the geographically closest off-shore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

A global company may elect to run several distinct Anycast clouds each serving a different market.

To do this we recommend using one or more dedicated DNS solution providers that have services to help them geo-focus their DNS traffic. The other benefit of using redundant suppliers is that your overall network can be more resilient and faster.



Unicast doesn't provide the redundancy of anycast

Alternatively, if an organization prefers to in-source their authoritative DNS infrastructure then it can be built and managed in organizational data centers. Even in this scenario, using a 3rd party backup via Anycast is a cost-effective way to help protect the network.

And finally, because of the way anycast is architected, there is the option to combine some in-house infrastructure with one or more bestof-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 at key IXP's in Canada to answer queries for Canadian traffic with very low latency and helps to keep Canadian web traffic in Canada's borders. In addition to these benefits, it 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 to protect your organization from outages due to malicious activity.

LEARN MORE

For more information on how an 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 delivers DNS services around the world and develops and implements policies that support Canada's Internet community and the .CA registry internationally.