Security Whitepaper

DNS Resource Exhaustion

Arlyn Johns
October, 2014
DNS is Emerging as a Desirable Target for Malicious Actors

The current threat landscape is complex, rapidly expanding and advancing in sophistication. Initially, when many organizations built their security systems, risks and attacks were simple by today’s standards. Now, many of those security systems are just outmatched, especially when it comes to protecting DNS.

Criminals have discovered that DNS is often an unwatched back door, making invasion into an organization’s network much too easy. Further, DNS resource exhaustion is a key threat area where we see growth. The open nature of DNS makes leveraging it for Resource Exhaustion highly desirable for the bad guys.

Overview

This document describes a new DNS DDoS threat that is emerging, how you can detect it, and what actions you can take to avoid it. This attack attempts to overload the DNS infrastructure of its intended target, thereby rendering it nonoperational. And as DNS is critical to almost all modern communication over the Internet, taking down the target's DNS services essentially takes down their ability to access the Internet. But there is also collateral damage from this attack that can negatively affect your own DNS infrastructure.

Attack Details

In order to perform this attack, the attacker must first have registered a domain and designated the intended target’s name server as the authoritative server for that domain or use an existing domain whose authoritative server is already the intended target.

Then using a botnet of compromised machines, the attacker directs the machines to send a flood of requests through a botted machine's ISPs' recursive name servers. Additionally the attacker may flood requests through any known open resolvers that may reside within an ISP's network. Each request will contain a unique, randomized, and non-existent sub-domain of the previously registered domain (ex. kbsruxixqf.www.500sf.com, adujqzutahyp.www.500sf.com).

Because of the uniqueness of the sub-domains, each request will then trigger a recursive lookup against the target's name server. As the attack grows in size, the amount of requests hitting the intended target's name servers grows as well. Eventually the target's DNS
infrastructure will buckle under the load, either from system resource depletion, network saturation or both.

Under the Hood

As these attacks rage on, the unwilling participants may not show any major symptoms. Perhaps they will notice some additional load or bandwidth over normal usage patterns. But as these turf wars escalate in intensity and duration, ISPs are more and more likely to get caught in the cross-fire. CPU, memory, and bandwidth are being consumed handling these malicious lookups. How much depends on the size of the attack and the resources of the victim, but for many ISPs already running within constrained resource environments, this unwanted additional load can begin to push things closer to the edge.

Take for example the charts seen in Figure 1 and Figure 2, generated by analyzing DNS traffic at an ISP during a half-hour period when an attack was taking place.
Here you can see an attack against the DNS infrastructure hosting 500sf.com, a domain registered in China. Over half of all outstanding requests are tied up servicing requests for 500sf.com sub-domains. Most of these requests either timeout or take several seconds to return results. Each request is also taking up space in the cache which could cause premature ejection of valid domains resulting in longer lookup times.

During this time roughly 15 Mb/s is devoted solely to handling these malicious requests. That may not seem like much, but consider that the target DNS infrastructure is likely not provisioned to handle the heavy load that is being placed on it for all the participating resolvers combined. An attack on a larger, better equipped target, or multiple targets simultaneously, would be able to consume additional bandwidth before falling over.
Traffic analyzed from the following day show a similar attack occurring, but this time against two targets, 7098.com and sf277.com as seen in Figure 3 and Figure 4 below.

What is interesting about these charts is that after about 15 minutes into the analysis the attacker shifts resources being used against sf277.com over to attack 7098.com. This coordination suggests that there is a single command and control structure managing both attacks.
What Makes this all Possible?

A major source of DNS infrastructure abuse comes from open resolvers residing within the ISP's own network. Open resolvers are typically commodity devices used for home networking that are misconfigured to allow access from outside the local network. These devices are independently managed and are often running out-of-date firmware with known exploits. This is a difficult problem for ISPs to address because they have limited control, if any, over these devices, and no way to separate legitimate from malicious traffic.

The other major source of abuse comes from compromised machines. Compromised machines are costly to remediate, and ISPs are hesitant to take broader action in fear of upsetting their customers.

How You can Protect Yourself?

There are some precautions you can take as a DNS administrator to help mitigate the effects of resource exhaustion attacks. Some of these precautions include:

Restrict packets with spoofed source IP addresses from exiting your network (See BCP 38). Although this doesn't directly benefit the implementer, it is a good practice for running a hygienic network and being a good net citizen.

Monitor your recursive DNS servers looking for anomalous behavior such as:

- Spikes in the number of unique sub-domains being queried.
- Spikes in the number of timeouts or delayed responses from a given name server.

When detected, a synthetic response can be generated for the misbehaving domains through a DNS RPZ modification. Vendors such as Spamhaus, SURBL, and others offer DNS RPZ feeds to help protect against malicious domains as they begin to be reported. And, apply per-domain rate limits for lookup requests from clients within your network.
Nothing Beats Real-Time

Protecting your DNS infrastructure from outside attack can be a daunting and thankless task. It involves accurate monitoring and regular maintenance in order to prevent malicious activity entering or leaving your network. And although some of this work can be automated, much of it requires human interaction that is resource intensive and often reactive at best.

The Cloudmark Security Platform for DNS provides automatic, real-time detection and prevention of resource exhaustion and other DNS-related threats. Cloudmark’s patented solutions deliver immediate, adaptive and predictive protection from ever-evolving network threats with proven, carrier-grade scalability and operability, assuring business continuity while lowering infrastructure costs. Cloudmark leverages big data analytics from locally collected data and from our Global Threat Network—the world’s most comprehensive repository of global threat intelligence. Cloudmark protects more than 120 tier-one customers, including AT&T, Verizon, Swisscom, Comcast, Cox and NTT and more than 1 billion subscribers worldwide.