SECURITY
SERVICES

DNSSEC:

How Savvy Attackers Are Using Our Defenses Against Us

neustar®

In Neustar's **April 2016 Security Operations Report**, we shared the troubling rise of DDoS attacks that exploited and abused the Domain Name System Security Extensions (DNSSEC) to amplify DNS reflection attacks. After mitigating the attacks and deconstructing the DDoS battles, we began to analyze other domains that could be exploited for DDoS attacks and found some disturbing trends.

ANATOMY OF A DNSSEC REFLECTION ATTACK

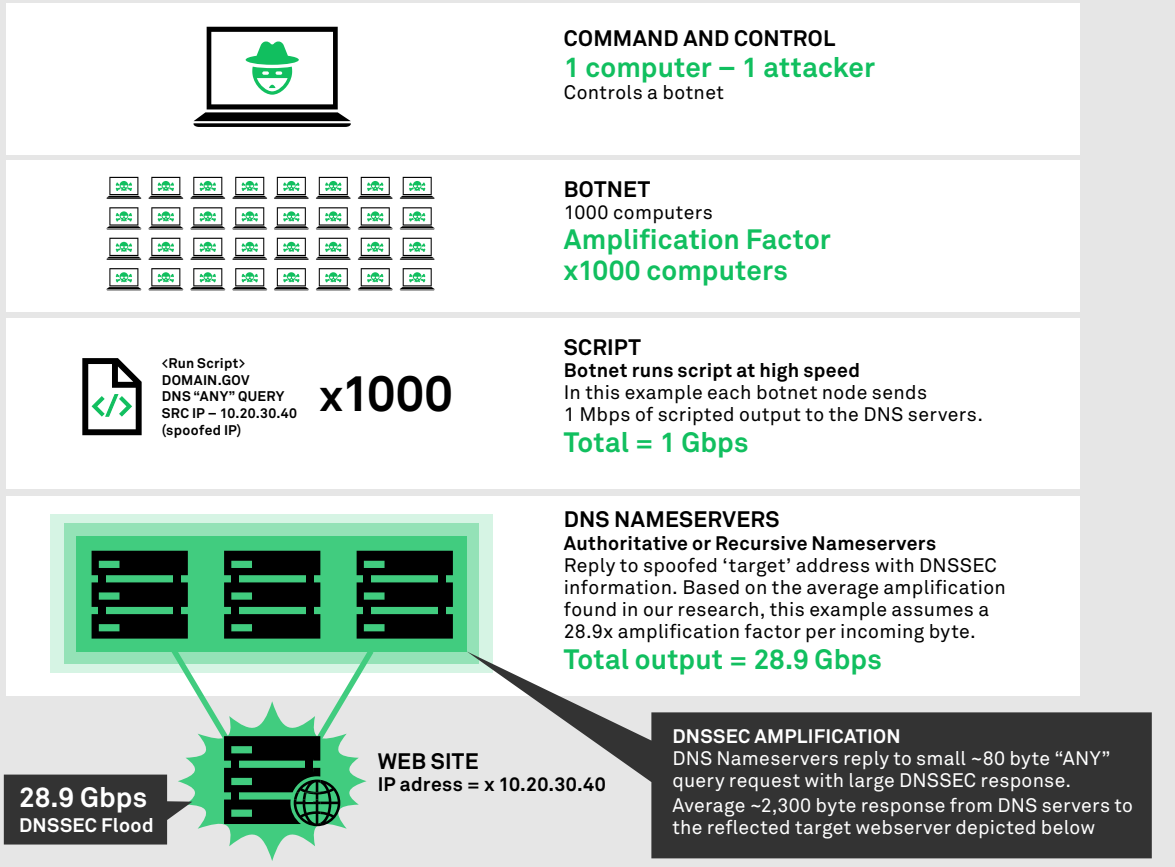
Assuming the hacker has amassed a botnet of 100 or even 1000 infected computers, they just need to know which website they want to attack and get that website's IP address—which is fairly simple in most cases.

Once the attacker has the target's IP address, they'll use the botnet to run a script that spoofs the Source IP address and replaces it with the known IP address of the website. The botnet then executes the script using the "ANY" query.

The DNSSEC nameservers reply to the target IP address with a massive response. Since the attacker spoofed the IP address, the attack script fools the nameservers into reflecting the DNSSEC response towards the target. That is the "Reflection" part of the attack that is made possible by the unverified nature of the UDP protocol.

DECONSTRUCT: DNSSEC REFLECTION ATTACK

(Please note that the IP addresses and domain names used below are fictional)



BACKGROUND

DNS is a necessary, yet vulnerable layer of the Internet that translates user understandable names (e.g. URLs) into IP addresses that are understood and accepted by Internet routers and computers. Unfortunately, hackers discovered a way to insert bogus answers into the query/response scheme of normal DNS. This sinister discovery can redirect unsuspecting users to counterfeit websites that are often infected malware, or a hacker "taunt" site.

As a means to combat this issue, DNSSEC was designed to provide integrity and authentication to an otherwise insecure DNS system. Though not widely adopted across the public Internet, DNSSEC is mandated and used in certain sectors like the government. DNSSEC uses complex digital signatures to provide a level of protection to the DNS transaction. The result when you convert a normal DNS record over to one signed with DNSSEC is an extraordinary amount of additional information stored in the zone.

With digital hashed signatures and complex key exchanges, DNSSEC records are considerably larger than standard DNS. Yes, they are more secure, but their sheer size can also be misused as a DDoS amplifier. Here's the rub: if DNS is not properly secured, signed and authenticated, then it is vulnerable to cache poisoning and similar malicious redirections attacks. But when DNSSEC is in place, the domain can become a powerful amplifier for DDoS attacks.

So far in 2016, Neustar is seeing a large number of these DNSSEC based UDP amplification attacks. To understand how the DNSSEC attacks were being launched, we conducted an experiment that is outlined below:

APPROACH

In June of 2016, we attempted to replicate the methodology and thought process of an attacker who would use DNSSEC to augment DDoS strikes. We located 1,349 domains in a certain high-adoption community and checked for DNSSEC records. We then ran DNS queries from four separate and independent open recursive servers—not run by Neustar—to look for DNSSEC nameservers that responded to queries using the DNS command "ANY," which is a favorite malicious query used by hackers. If the DNSSEC zones replied to the "ANY" query, the amplified response was exponentially larger than that from a normal DNS reply.

After using four recursive servers to test the domains for DNSSEC vulnerabilities, we averaged the real byte response from the DNSSEC signed zones that answered to the "ANY" query. We then compared the response to an estimated DNS query of 80 bytes, a conservative figure based on research and packet analysis. Since attacks are all different, there is no exact figure for the query size. By assuming our query size was 80 bytes, this gave us a baseline to measure the attacker's return on investment (amplification factor) for the different domains that met the criteria.

FINDINGS

Of the 1,349 domains that we examined, 1,084 were signed with DNSSEC and responded to the "ANY" query. Which means: **80% of the domains in this one community could be repurposed as a DDoS amplifier and used maliciously.**

OTHER FINDINGS:

28.9x
The average amplification factor for a DNSSEC signed zone.

17,377 bytes
The largest amplification response across all domains

2313 bytes
The average response "return on investment" for an 80-byte query

neustar

IMPLICATIONS

If left unprotected from "ANY" queries, DNSSEC poses a serious threat as a DDoS amplifier. For the average company with a modest DDoS defense, a DNSSEC-based flood attack could easily knock their website offline, and possibly give the attacker free access to their infrastructure. DNSSEC attacks can also serve as smokescreens, or distractions to hide the hacker's real intent to insert malware or mask the exfiltration of sensitive information.

There are also significant ramifications for the domain owner. If they pay for DNS by the query, such attacks could significantly drive up their DNS bill. Additionally and more seriously, their domain could become a useful filter for ISPs or other DDoS mitigation networks.

If a blunt filter were applied to block all DNS traffic from a particular domain, then it would simultaneously solve one problem while creating another. On one hand, applying the filter could stem the attack, but it also eliminates legitimate DNS queries from getting through—a nightmare scenario for e-commerce businesses or companies that depend on their website for sales.

Although ISPs and DDoS mitigation networks try their best to allow legitimate traffic to flow through, there is no guarantee of what may happen when network integrity is at stake, especially in the case of a large flood. The best practice is to avoid owning an exploitable DNSSEC signed domain or risk a large swath of the Internet being unable to resolve legitimate DNS queries for your domain because of an ISP DDoS filter.

For organizations that use and rely on DNSSEC, Neustar recommends ensuring that your DNS provider does not respond to the "ANY" queries or has some mechanism in place to identify and stop misuse.

ABOUT NEUSTAR

Neustar, Inc. (NYSE: NSR) is the first real-time provider of cloud-based information services, enabling marketing and IT security professionals to promote and protect their businesses. With a commitment to privacy and neutrality, Neustar operates complex data registries and uses its expertise to deliver actionable, data-driven insights that help clients make high-value business decisions in real time, one customer interaction at a time.

More information is available at **www.neustar.biz**.

neustar®