IT Security

DDoS strike on Spamhaus highlights need to close DNS open resolvers

By Patrick Lambert
April 2, 2013, 5:30 AM PDT

Takeaway: Patrick Lambert breaks down the Spamhaus DDoS attack and some of the controversies that have ensued. What isn't up for debate — fixing the open resolver flaw on DNS servers.

Last week, news went around the world about one of the biggest Distributed Denial of Service (DDoS) attacks in history, launched against a site called Spamhaus, in which attackers not only went after the organization's website itself, but also its providers and some Tier 1 Internet exchanges as well, causing potential collateral damage. Since then however, the situation has only become more complex, with rumors flying around that the attack was not as bad as reported, and hints on who might be behind it, along with what could be done to prevent future attacks.

Why Spamhaus?

Most people have no idea what the Spamhaus Project is. This group of security researchers and IT pros work in the background, alongside many Internet providers and network administrators, in an effort to cut down on email spam. According to its mission statements, Spamhaus was founded in 1998 as a nonprofit organization dedicated to fighting spam. It is run by volunteers and works alongside law enforcement agencies like the FBI, email providers, and networks around the world. In reality, the way they fight spam is by maintaining large blacklists. These are lists of source addresses such as mail servers and websites, where they believe spam is coming from. These blacklists use DNS to block access from these sources, and are updated in real time. Because so many networks and providers use those blacklists, over 1.4 billion people are affected by them. This means that if an IP address is added to a Spamhaus blacklist, a large percentage of the Internet users will instantly be unable to receive anything from that source address. Needless to say, this has huge consequences.

Spamhaus is loved by many, since they have succeeded in bringing down the levels of spam that travel through the Internet. However, it also has a lot of enemies, and is the center of many controversies. The reason is that they have final say on which sites appear in their database. If they decide one particular business is sending spam, and they add their server to the blacklist, that will greatly affect the company's ability to do business. The site does offer ways to get a case reviewed and potentially get removed from the list, but many still feel that Spamhaus is acting as judge, jury and executioner. So as a result, Spamhaus is often the victim of attacks.

How the attack happened

Spamhaus already has a strong infrastructure that allows them to deal with normal attacks, but on March 18th they started to see a very large attack that they could not handle. So they contacted CloudFlare, a content delivery network that specializes in these types of attacks - since then, CloudFlare has published an account of events. Basically, they used their worldwide Anycast network to spread the DDoS attack over a large number of data centers. Even though the total bandwidth from the attack reached close to 300 Gbps, which is massive and would bring down any normal network, they still managed to cope because of their redundancies. However, the attackers did not stop there.

Seeing that they could not bring down Spamhaus or CloudFlare, they decided to attack their providers, and then the nodes upstream. However, because CloudFlare is so big, those upstream nodes are actual Tier 1 Internet backbones, so in essence the attackers ended up flooding crucial Internet exchange points such as the London Internet Exchange, Amsterdam Internet Exchange, and Hong Kong Internet Exchange. These are the core exchange points of the Internet where all of the large networks peer with each other, and while those have enough bandwidth to cope with such an attack, if all of the traffic comes in through a single port, it can easily slow down access for customers, in this case millions of people.

Controversy about the impacts felt

After the attack and CloudFlare's post, Gizmodo posted a fairly controversial post titled "That Internet War Apocalypse Is a Lie." Basically, they claimed that CloudFlare was greatly exaggerating their claims that this attack was seriously impacting the Internet backbone. They say the account of events was overly dramatic, perhaps made to sell CloudFlare's DDoS protection services. They say that Internet charts do not show services being slow on that day, and talk about how Internet backbones can support Tbps of bandwidth, an order of magnitude higher than what was felt. Since then there have been backs and forths, with CloudFlare countering saying that because some Internet exchange IPs can be publicly known, such an attack could actually disrupt crucial switches, and so on.

The problem of open resolvers

Regardless of whether part of the Internet was disrupted, or this was just affecting a couple of companies, the fact remains that a 300 Gbps attack is really big, much bigger than what most companies can cope with. The reason that bad guys can create such massive attacks is because of a *specific flaw in how many DNS servers are configured*. By default, DNS can make use of something called a resolver, which will reply with information about a particular address, domain name or site name, and send that information back. Unfortunately, the Internet is filled with open resolvers, DNS servers that will return this information to anyone who asks. Add to that the fact that spoofing an IP address is trivial, and you have a massive issue.

The way the attack goes is that the attacker spoofs his or her originating IP to be the website they want to hit. Then, they ask many of these open resolvers for a lot of information. These servers will then return the information, but not to the attacker, instead to the site being attacked. In

essence, you end up directing between ten times to a hundred times as much data as you are sending out. So to create a 300 Gbps attack you would only need 3 Gbps of bandwidth. The DNS servers across the Internet would do the rest, and your real IP would never be seen by the target, which is another plus for the bad guys. The Open Resolver Project is attempting to bring light to this issue, and tracked over 27 million open resolvers across the Internet. The only real fix is for the administrators of all these servers to correctly secure them. There are tips and recommendations on the project's website to help secure those servers.

Who did this

It is still unknown who is behind the SpamHaus attack, however the hosting provider Cyberpunker is suspected of having sponsored the attack after it was added to the blacklist. As for who did the actual flooding, the New York Times posted about a potential suspect, Sven Olaf Kamphuis from Denmark, who has recently talked about his wish to bring SpamHaus down and describes himself as an Internet freedom fighter. He is described as the prince of spam, someone who hates authority, and former partners of his said he does not care about collateral damage at all. Since then, he has appeared on TV claiming that he is not behind the attack.

Bottom line

The authorities are now investigating the Spamhaus attack, but regardless of whether they manage to find the guilty party or not, there is no doubt that future attacks of this scale - or even bigger — will keep happening. The only true solution is for all of those DNS resolvers to be fixed, but in the meantime, redundant Internet connections, DDoS protection services, and content delivery networks are just some of the elements that can help a network cope with such an attack.