the Availability Digest

www.availabilitydigest.com

History's Largest DDoS Attack?

April 2013

From March 18th through March 28th, Spamhaus, a spam-filtering site, was swamped with up to 300 gigabits per second (gbps) of traffic in the largest reported Distributed Denial of Service (DDoS) attack in the history of the Internet. How was this amount of traffic generated?

The answer is that a well-known flaw in DNS servers known as open resolvers was used to generate the massive amount of malicious traffic. Spamhaus survived the attack by enlisting the services of a DDoS protection vendor that spread the traffic over its 23 worldwide data centers.

Spamhaus

Spamhaus is a Swiss/British anti-spam watchdog group. It is a nonprofit organization run by volunteers, and it works alongside law enforcement agencies such as the FBI (the U.S. Federal Bureau of Investigation), email providers, and networks around the world.

Spamhaus provides a blacklist of IP addresses for servers that are determined by Spamhaus to host email spammers. The list is updated in real time and is provided to ISPs, corporations, and spam-filtering vendors. The lists are typically used by the DNS servers of these organizations to restrict incoming information from spamming sites.

It is estimated that 1.4 billion Internet users are protected by the Spamhaus blacklist. This means that 1.4 billion users cannot receive anything from a listed site. Though Spamhaus provides a procedure for a listed site to clear its name and be removed from the list, it is understandable that the management of any site on the blacklist will be very unhappy with Spamhaus.

Spamhaus has weathered many DDoS attacks from disgruntled sites but not of any magnitude that affected it. It maintains a very distributed infrastructure to withstand such attacks. However, in late March, 2013, it was buffeted by a massive DDoS attack that threatened its survival.

The Attack by CyberBunker

CyberBunker

CyberBunker, named for its headquarters in an old NATO five-story bunker, is a Dutch web site that claims that it will host anything but child pornography and terrorism-related content. The CyberBunker web site is designated a spam site by Spamhaus and is on the Spamhaus blacklist.

The owner of CyberBunker is Sven Olaf Kamphuis. He calls himself the "Minister of telecommunications and foreign affairs for the Republic of CyberBunker." A Facebook post of his contains the statement:

> "Yo anons, we could use a little help in shutting down illegal slander and blackmail censorship project 'spamhaus.org,' which thinks it can dictate its views on what should and should not be on the internet."

Kamphuis submits that Spamhaus abuses its position not to stop spam but to exercise censorship without a court order. He is currently being investigated by Dutch authorities for the ensuing attacks on Spamhaus but has not been charged. He claims his innocence. However, Dutch Internet hosting service, Greenhost, discovered digital footprints of one of his companies in the DDoS attack.

The Initial Attack

The attacks on Spamhaus began on March 18, 2013. In the beginning, they were rather weak and had little effect on Spamhaus' operations. The attacks started out with a data rate of 10 gbps. Spamhaus' distributed architecture allowed it to continue providing its services with little performance impact.

The attacks then escalated to 75 gbps on March 19th. This level of attack became a serious threat to Spamhaus. Its web site was substantially unreachable, and it could not update its lists. It reached out to CloudFlare, an Internet security firm, for help weathering the attack.

CloudFlare to the Rescue

Headquartered in Silicon Valley, CloudFlare is an Internet security firm that maintains 23 data centers around the world. It spread the Spamhaus attack among its data centers, allowing Spamhaus services to resume.

CyberBunker immediately included CloudFlare in its attack, and the DDoS data rate increased to an unprecedented 300 gbps. CloudFlare also was able to distribute this level of DDoS attack among its data centers without affecting its other customers, and Spamhaus continued in operation.

Escalating the Attack to the Heart of the Internet

CyberBunker did not give up at this point. It moved from attacking Spamhaus and CloudFlare to attacking the critical Internet infrastructure upon which these companies depend.

The Internet is a collection of networks (thus its name) all connected together using peering relationships. Company intranets connect to Tier 2 networks that purchase bandwidth from Tier 1 networks. Tier 1 networks include such companies as AT&T, Verizon, Sprint, and Deutsche Telekom and provide their own networks. Tier 1 networks can route traffic to and from all of their Tier 2 networks and are themselves interconnected via Internet Exchanges (IXs) along with other major networks. In this way, packets can move across the Internet from any source to any destination.

CyberBunker began attacking the upstream peers and exchanges used by Spamhaus and CloudFlare. This included their Tier 2 providers, the Tier 1 providers to which the Tier 2 providers were connected, and the associated Internet Exchanges. The London IX (LINX), Amsterdam IX (AMS-IX), German IX (DE-CIX), and Hong Kong IX (HKIX) were all attacked. Every network attached to an attacked IX was also affected.

Though these networks and interchanges can handle terabits of data per second, any one port is typically limited to about 100 gbps of traffic. Thus, depending upon the distribution of traffic, Internet performance in these areas were affected to various degrees.

Most of the Internet that was impacted was in Europe. Some estimated that hundreds of millions of people were affected, though others noted that there did not seem to be any uproar over Internet performance during the period of the attacks.

The attacks finally stopped (at least for now) on March 28th. They had been going on for almost two weeks.

How Significant is 300 gbps?

For DDoS attacks, 300 gbps is a massive attack. Typical attacks are measured in the 10 gbps range. The recent attack on U.S. online banking portals in retaliation for the YouTube video "Innocence of Muslims" reached an unprecedented rate at that time of 70 gbps.[1]

The Spamhaus attack was the first reported DDoS attack of such a magnitude. In fact, the data rate may well have exceeded 300 gbps – this was the upper limit of the measurement capability of CloudFlare's instrumentation.

The Net Effect

The distributed-processing resources that Spamhaus and CloudFlare were able to deploy helped to reduce the impact on them. Spamhaus continued to distribute its black list, and CloudFlare continued to service its other customers.

There were certainly ripples of disruption in Europe as servers moved mountains of junk traffic over the Internet. However, the impact may not have been as great on other Internet users as CloudFlare publicly indicated. Gizmodo claimed that CloudFlare was exaggerating the impact on the Internet in order to sell its DDoS services. CloudFlare countered that since some IX IP addresses are well known, successful attacks can be launched. These attacks are a warning for the future.

The DNS Flaw – Open Resolvers

The question remains – how did the attackers achieve such high DDoS data rates? Typical DDoS attacks use botnets of PCs that are capable of generating only a few gbps of data.

The attacks on U.S. banks increased this data rate by an order of magnitude. The attackers achieved this by two means. First, they used a network of PCs provided by volunteers – all those equally infuriated by the YouTube video. This was a massive number of PCs – far more than a normal infected botnet would provide. Second, they were able to infect servers and put them into service. A large server can generate the traffic of thousands of PCs.

But CyberBunker did not have a cadre of sympathetic PC users. It instead used a long-recognized flaw in DNS servers. This flaw is known as the DNS open resolver.

In the early days of the Internet, a DNS server would resolve an address from any source by returning an IP address associated with a URL. It did not have to be a request from its administrative domain or from another DNS server. This type of DNS server is known as an open resolver. Recognizing this as a security hole, newly installed DNS servers now will respond only to requests from their own administrative domains or from other DNS servers for public-facing services.

However, network managers around the world have been slow to upgrade their DNS servers – it's not a very high priority for them. The result is that there are still 27 million DNS open resolvers on the Internet.

[1] Islamist Hacktivists Attack U.S. Banks, *Availability Digest*; October 2012.
http://www.availabilitydigest.com/public_articles/0710/bank_attacks.pdf
DDoS Attacks on U.S. Banks Continue, *Availability Digest*; January 2013.
http://www.availabilitydigest.com/public_articles/0801/more_bank_attacks.pdf

The use of these open resolvers to generate a massive amount of malicious traffic is straightforward. It is called DNS reflection. The attacker sends a request to an open resolver for information concerning a URL address. The open resolver DNS server responds with data concerning that destination. However, the attacker has spoofed the requesting address to be that of its victim. Thus, the DNS information is returned to the victim.

This is like mailing information to thousands of companies with the victim's return address on the back of the envelope. The result is that when the organizations reply, the victim is swamped with a landslide of useless data.

The success of a reflection attack depends upon the relative size of the request message and that of the response message. A typical DNS request message is about 30 bytes. A typical DNS response message contains about 3,000 bytes – a 100:1 amplification factor. Thus, to generate 300 gbps of DDoS data, the attacker only needs to generate 3 gbps – a fairly trivial data rate.

The Future of DDoS Attacks

What Can We Expect?

Lists of DNS open resolvers have been passed around the Internet on network security lists for the last few years to help administrators identify and correct them. The Spamhaus attack is the first time that this flaw has been used for a major attack, and it is the first time that the full extent of the problem has been made public. We now can expect other hackers to utilize this same DNS flaw to launch major attacks.

Could one day a nation-state or a terrorist group cripple the entire worldwide Internet using a DNS reflection DDoS technique? Devastation of an unprecedented scale might result. Let's hope that we can act to close this security hole before we have to face such a situation.

What Can We Do?

The first thing we can do to solve the problem is to get rid of all of the DNS open resolvers. The Open Resolver Project has been set up to identify the remaining open resolvers (27 million of them so far) and to prepare procedures for system administrators to modify their DNS servers to eliminate the flaw. Unfortunately, little incentive exists for administrators to add this task to their busy workload.

Until the open resolvers are secured, a company can take some steps to help mitigate the impact of an attack:

- It can ensure that it has sufficient redundant Internet connections to be able to route traffic in the middle of a major DDoS attack.

- It can subscribe to a DDoS protection service such as CloudFlare (there are many others) that can spread the malicious traffic across multiple data centers to minimize its impact.

- It can contract with content-delivery networks to provide a degree of protection from DDoS attacks by using their large distributed server infrastructures to absorb traffic.

- It can implement the provisions of BCP 38 for its network. This Internet specification allows only traffic that originated in a network to be sent out of the network. Consequently, sender addresses cannot be spoofed (at least, not to addresses out of network).

Summary

Gone are the days when a major data-center failure followed by a failover fault to another data center was the only way to lose all IT services. DDoS attacks now can have the same impact. However, recovery time is not a matter of minutes or hours as backups are brought up. Rather, recovery time is up to the attacker.

Companies must now take into account this type of data-center failure, and the Business Continuity Plan must deal with the continuation of services when system response times have become so long that IT is unable to support the company's operations.

Acknowledgements

Material for this article was taken from the following sources:

Spamhaus Hit with 'Largest Publicly Announced DDoS Attack' Ever, Affecting Internet Users Worldwide, *Huffington Post*; March 27, 2013.
BIGGEST DDoS ATTACK IN HISTORY hammers Spamhaus, *The Register*; March 27, 2013.
The Biggest Cyber Attack in History Is Taking Place Right Now, *Business Insider*; March 27, 2013.
The DDoS That Almost Broke the Internet, *CloudFlare Blog*; March 27, 2013.
Firm Is Accused of Sending Spam, and Fight Jams Internet, *The New York Times*; March 28, 2013.
Authorities Investigate CyberBunker "minister" over cyber attacks, *Slash Gear*; March 30, 2013.
Is the Spamhaus DDoS Attack Over?, *Security Watch*; March 30, 2013.
Spamhaus DDoS Spotlights DNS Server Security Challenge, *Dark Reading*; April 2, 2013.
DDoS strike on Spamhaus highlights need to close DNS Open Resolvers, *Tech Republic*; April 2, 2013.
Spamhaus DDoS was just a warning shot, *Fierce Telecom*; April 2, 2013.