the Availability Digest

www.availabilitydigest.com
@availabilitydig

# Verisign DDoS Mitigation Services

December 2013

Distributed Denial of Service (DDoS) attacks are increasing in frequency and size. The number of DDoS attacks increased over 50% from 2011 to 2012. Of more concern is their size. The volume of malicious traffic generated by a DDoS attacker has grown from five gigabits per second (Gbps) to over 300 Gbps in the past year.



This volume of malicious traffic cannot be handled by the ordinary organization. The only reasonable defense is to turn to a cloud-based DDoS mitigation service that can spread the malicious traffic across several data centers and return cleansed traffic to the victim.


Verisign provides cloud-based DDoS mitigation services. We look at the DDoS attack challenge and Verisign's solutions in this article.

## What is a DDoS Attack

A DDoS attack floods a web site with so much traffic that it is unable to provide reasonable responses to its users. These attacks can cripple an organization's entire online operation, from email to e-commerce. This threatens an organization's ability to carry on its business and may damage its brand. In addition to a poor customer experience, the downtime caused by a DDoS attack can have severe financial penalties.

Successful DDoS attacks are not just a matter of creating so much malicious traffic that the organization's network bandwidth is consumed. Though this is certainly one method of attack, there are several layers of attacks that are more sophisticated.[1] DDoS attacks can be launched at different layers of the Internet stack. In addition to consuming bandwidth, attacks can force an application to consume resources by flooding it with requests for apparently legitimate services.

For instance, a SYN flood with spoofed client addresses requests connections with a server by sending it a SYN message. The server assigns resources to the pending connection and responds with a SYN-ACK message. However, neither the attacker nor the spoofed sender ever sends an ACK message to complete the connection. The server holds its connection resources for several minutes before releasing them. Ultimately, the server runs out of connection resources and cannot respond to further connection requests from legitimate users.

An HTTP flood makes legitimate requests of a web site, such as downloading a web page. Ultimately, the attacker has either consumed all of the web server's connections or has put such a load on the web server that it cannot respond to any further requests.

[1] Anatomy of a DDoS Attack, *Availability Digest*; April 2013.
http://www.availabilitydigest.com/public_articles/0804/ddos_anatomy.pdf

These are just a sampling of DDoS attack methods used by hackers. DDoS attacks are now in the province of amateurs. Publicly available tools allow anyone to launch a DDoS attack against a target web site.

The high volume of traffic is generated by botnets. A botnet is a collection of infected computers controlled by a botnet master. Upon command from the master, the computers in the botnet bombard the victim system with the master's attacks of choice. Targets include web servers, DNS servers, application servers, routers, firewalls, and network bandwidth. Publicly available tools and information-sharing sites make it easy for an attacker to learn from each successive wave of attacks what defenses the victim is deploying and to plan further attacks to avoid these defenses.

There are many reasons for DDoS attacks. Unlike typical malware, the purpose of a DDoS attack is not to steal data or to redirect the actions of a computer. Rather, DDoS attacks may be launched for activism, for revenge, for competitive brand damage, or for extortion.

The second half of 2012 saw a series of major attacks against U.S. banks that were launched by activists.[2] An Islamic group calling themselves the Izz ad-Din al-Qassam Cyber Fighters attacked several major banks over the offensive video entitled "Innocence of Muslims" that had been posted on YouTube. They vowed to continue the attacks until the video was removed. They launched a second wave of attacks a few months later. These attacks were the largest seen up to this point, lasting a day or more and generating about 70 Gbps of malicious traffic.

Then in early 2013, the largest DDoS attack ever seen was launched against Spamhaus, a company that specializes in creating a black list of spammers used by ISPs and corporations to block spam. Spamhaus added CyberBunker to its list.[3] In retaliation, CyberBunker launched a massive DDoS attack against Spamhaus. Three-hundred Gbps of data were directed at the Spamhaus web sites, and the attack lasted several days. Spamhaus managed to survive the attack by using the cloud-mitigation services of CloudFare, which also was attacked by CyberBunker in retaliation.

## Current DDoS Defenses

A survey conducted by IDG Research Services that polled 160 IT and network technicians and line-of-business executives found that two-thirds had experienced at least one DDoS attack in the last year, and 11% had been attacked six times or more. About half of the respondents were using on-premises appliances such as firewalls and intrusion-detection devices to thwart DDoS attacks. Less than half of the respondents were confident that they could detect a DDoS attack. Even fewer felt that they could defeat one.

There are four typical approaches to DDoS protection:

- Do-it-yourself – Increase bandwidth or write scripts to try to filter bad traffic. This approach is simple but generally ineffective.

- Specialized on-premises appliances – These appliances sit in front of servers and routers to detect and filter malicious traffic. They are costly to buy and to operate, require constant attention to keep current, and cannot defend against volumetric attacks.

- Rely on the ISP – ISPs have more bandwidth than individual organizations. However, many organizations use multiple ISPs to avoid a single point of failure, and attack traffic is difficult to manage if it is distributed across multiple ISPs.

[2] Islamic 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
[3] History's Largest DDoS Attack?, *Availability Digest*; April 2013.
http://www.availabilitydigest.com/public_articles/0804/spamhaus.pdf

- Use cloud-mitigation providers – Cloud-mitigation providers provide massive amounts of bandwidth at multiple sites around the Internet. They scrub malicious traffic and send only clean traffic to the victim. Cloud-mitigation providers incorporate several mitigation strategies and can identify attack tactics to determine the optimum defense strategy to use.

## Preparing for a DDoS Attack

More and more companies are realizing that it is when, not if, a DDoS attack is going to happen. There are several important steps that should be taken to detect and mitigate an attack.

- Gather proper metrics so that a DDoS attack can be distinguished from other malfunctions that may be affecting the system's performance. Appropriate metrics include inbound and outbound traffic, server metrics (CPU load, network and disk activity, memory usage, etc.), top URLs being requested, and HTTP to HTPPS ratios.

- Define a clear escalation path. What tools are in place to alert pertinent personnel? Who is to be contacted for mitigation service? Notify upper management and support and customer service personnel that an attack is underway and that there may be a potential outage. An outages email list is a good place to start.

- Provide layered filtering of malicious traffic. Filtering for bandwidth floods, SYN-ACK floods, HTTP floods, and other attack tactics are all different. Filters should be in place to protect against any known DDoS flood.

- Address application and configuration issues. DDoS attackers are excellent at detecting problems in applications, particularly those concerning performance tuning and configuration. Do application load testing to see that networks and databases are configured optimally. Check that there are enough connections available for the web servers.

- Protect your DNS system.[4] This is probably the most overlooked of all recommendations since a company's DNS system is largely transparent to developers and operations personnel. DNS systems are a very common target of DDoS attackers. If a company cannot resolve the addresses of its web sites, no one can reach these sites.

## Cloud-Based DDoS Mitigation Services

Simply increasing bandwidth to survive a DDoS attack is no longer an acceptable solution. DDoS malicious traffic must be spread across multiple cooperating data centers that are configured to handle massive attacks.

Furthermore, filtering malicious traffic has become a very complex task requiring the skills of specialists. As new attack tactics are discovered, new filters must be developed and put in place. This is a continuing, complicated, and costly undertaking.

These observations lead to the importance of cloud-based mitigation services. The advantages that a cloud-based service brings to DDoS mitigation are many:

- Cloud-mitigation service providers provide multiple data centers with massive amounts of network capacity capable of distributing massive DDoS attacks across many data centers.

- They invest in skilled personnel dedicated to the task of staying abreast of the latest security threats and assault tactics.

[4] Surviving DNS DDoS Attacks, *Availability Digest*; November 2013.
http://www.availabilitydigest.com/public_articles/0811/secure64.pdf

- They provide multiple layers of filtering for all kinds of DDoS attacks.
- They provide monitoring services to quickly detect a DDoS attack so that defenses can be put in place before the company suffers an outage.
- They provide DNS hosting services to protect the DNS systems from attack.
- They provide effective DDoS protection on a 24x7 basis.

Some companies who are considering cloud-mitigation services have some concerns that should be addressed before following this path. One is the security of data being transmitted to and from the cloud during an attack. The other is the compatibility of the cloud with the company's existing technology.

## DDoS Mitigation by Verisign

Verisign has for fifteen years operated the infrastructure for a portfolio of top level domains, including .com, .net, .tv, .edu, .gov, .jobs, .name, and .cc. More to the point of this article, it also offers cloud-based DDoS mitigation services and managed DNS services.

Verisign provides two complimentary DDoS defensive services – DDoS Monitoring Service and DDoS Mitigation Service. Though either can be purchased separately, full DDoS protection is only available with the joint use of both services.

### *Verisign DDoS Monitoring Service*

Verisign's DDoS Monitoring Service provides via a single Dashboard a view of traffic activity and traffic patterns across a company's entire network. This view is continually monitored by Verisign's experienced professionals for signs of unusual activity, giving them the capability to quickly detect a DDoS attack and to initiate migration strategies.

The Monitoring Service collects sample packets from switches, routers, and other devices to establish a baseline of normal traffic. These traffic measurements are sent to a correlation engine for threat detection, alerts, and reporting. The client company has continual access to Verisign DDoS specialists for advice, questions, and investigations of unusual traffic detected by the company.

Verisign continually analyzes attack patterns around the world to identify emerging attack strategies.

### *Verisign DDoS Mitigation Service*

When malicious traffic is detected, harmful traffic is redirected to a Verisign mitigation site. If the Verisign DDoS Monitoring Service is being used, Verisign will detect the attack and will redirect traffic to its site. If the client is not using the Monitoring Service, the client company is responsible for detecting the attack and for rerouting its traffic to a Verisign mitigation site.

Redirection requires the availability of a DNS server to resolve the company's URLs and to change the IP addresses from the company's web sites to ports on Verisign's mitigation data centers. Thus, the protection of a company's DNS system is paramount to effective DDoS attack mitigation. The use of Verisign's managed DNS services is one option to ensure a functioning DNS system when an attack begins.

At the Verisign mitigation site, specialist DDoS teams scrub the redirected traffic to remove malicious content and to return cleansed traffic to the client web site. Scrubbing traffic is accomplished via the use of layered filters as described earlier. Many of these filters are Verisign's proprietary filters, and some are third-party filters.

By filtering malicious traffic, Verisign stops cyberattacks before they have a chance to affect the online operations of the victim company. The Verisign DDoS Mitigation Service eliminates the need to over-provision network bandwidth to keep up with increasing attack volumes

***Verisign Best Practices***

In summary, Verisign protects a company from DDoS attacks via a set of best practices:

- It provides centralized data monitoring that shows an enterprise's entire network traffic patterns in one place so that DDoS attacks can be quickly detected.
- It provides a network of large data centers with massive network and compute capacity to handle any size of a DDoS attack.
- It builds in scalability and flexibility in its networks and data centers to make sure systems will perform properly under attacks.
- It employs experienced researchers with hands-on experience dealing with botnets, recognizing malicious traffic, defending against DDoS attacks, and changing mitigation tactics rapidly to combat changing attack tactics.
- It uses layered filtering to return clean traffic to the client company with minimum latency.
- It ensures that there is a clear escalation path to involve pertinent corporate personnel as an attack progresses.
- It provides managed DNS services to ensure that a company's web sites can always be reached.
- It works with its client companies to address application and configuration issues that would make it easy for an attacker to take down an application.
- It helps its client companies prepare for downtime by testing contingency plans for short and long-term outages

***A Case Study***

A leading online retailer experienced a crippling DDoS attack on its two main ecommerce web sites. It was unable to ward of the attack using its onsite in-house systems and services. It called on Verisign for attack mitigation and rerouted all of its traffic to Verisign's global cloud-mitigation network. At this point, it had restored its own network bandwidth.

The attack came in multiple waves. It began as a SYN-ACK attack with a network volume of 250 Mbps. Once the attacker became aware that this attack was being successfully defended, it increased the traffic volume within thirty minutes by an order of magnitude to 2.3 Gbps.

As mitigation of this attack became successful, the attackers shifted to HTTP floods that attempted to call up web pages from the company's servers. When Verisign rendered these attacks ineffective, the attackers turned to SSL attacks that targeted encrypted credit-card transaction traffic. Verisign engineers determined that the attackers were making malformed requests inside the SSL payload and quickly updated its mitigation filters to drop these requests. At this point, the attacks stopped.

This case study shows the importance of Verisign's massive network capacity, the power of its layered filtering techniques, and the importance of a skilled staff to make swift changes to defense strategies.

## Summary

DDoS attacks are on the rise in both frequency and size. It is imperative that companies be prepared for an eventual attack, as the question is no longer if they will be attacked but when they will be attacked.

There are several things that a company can do to prepare itself to defend against a DDoS attack on its online services, including increasing its bandwidth and investing in a variety of defensive appliances within its data center. However, with the increasing size of DDoS attacks, it is becoming more likely that these approaches will prove inadequate.

The best strategy is to arrange with a cloud-mitigation service provider to be available to take over defense against an attack if the company's own defenses become overwhelmed. The company's compromised traffic is sent to the data centers of the cloud-mitigation provider, and the provider returns clean traffic to the victim company. Verisign's cloud-mitigation services are an excellent example of the benefits of a cloud-mitigation defense against DDoS attacks.

## Acknowledgements

In addition to the previously referenced papers, information for this article was taken from the following Verisign white papers:

What is a DDoS Attack?
DDoS Attacks Threaten Every Enterprise
Five Steps to Prepare for a DDoS Attack
Thwarting DDoS Attacks with Cloud Defenses
DDoS Monitoring Service
DDoS Mitigation Service