DDoS Attacks &

Prevention Primer

A whitepaper looking into DDoS and prevention methodologies and technologies.

Netscylla Cyber Security Ltd
GB 10571639

Address:
Telecom House,
125-135 Preston Road, Brighton,
East Sussex,
United Kingdom, BN1 6AF

Introduction

What is DDoS?

DDoS is a Distributed Denial of Service - an attempt to make a computer resource unavailable to its intended users. Although types of DoS attack may vary, it generally consists of the efforts of a person or group of people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS attacks typically target large enterprises that have come under focus from the main-stream media; sites or services hosted on high-profile web or name servers can become targeted with abnormal amounts of high traffic.

Outcomes of a DDoS attack

One common method of attack involves saturating the target machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable.

Another outcome of attacks in regards to cloud-based infrastructure, is the cost of maintaining these web-services becomes unsustainable in its current architecture or unaffordable: Inappropriately configured auto-scaling groups, might suddenly scale outwards and upwards; generating high operational costs for the business that could cause severe financial implications.

In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

Table of Contents

Understanding the types of DoS attacks

There are several types of DDoS attacks. Below we will cover the two most common attacks: Typical Flood and DNS (or nameserver) flood attacks.

Typical flood attacks

A typical flood attack is a type of DoS attack in which a large number of requests are sent to a targeted server with the aim of overwhelming that device's ability to process and respond. Either, the firewall protecting the targeted server can become exhausted as a result of flooding, resulting in a denial-of-service to legitimate traffic. Or the application can run out of resources trying to resolve the users request, resulting in a resource-exhaustion where user requests can no longer be adequately processed for a response.

How does a flood attack work?

A flood can be thought of in the context of a hotel receptionist routing calls. First, the receptionist receives a phone call where the caller asks to be connected to a specific room. The receptionist then needs to look through the list of all rooms to make sure that the guest is available in the room and willing to take the call. Once the receptionist realises that the guest is not taking any calls, they have to pick the phone back up and tell the caller that the guest will not be taking the call. If suddenly all the phone lines light up simultaneously with similar requests then they will quickly become overwhelmed.

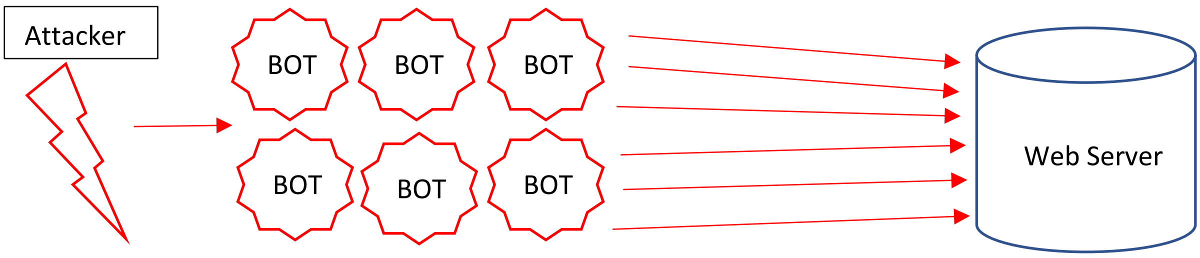

Figure 1: Example where an attacker controls a botnet that can launch a DoS attack against a web server with too much traffic (flood DoS).

As each new request is received by the server, it goes through steps in order to process the request, utilising server resources in the process. When responses are transmitted, each packet will include the address of the source. During this type of DDoS attack, an attacker will generally not use their own real address, but will instead spoof the source address of the request, impeding the attacker's true location from being exposed and potentially saturated with the response packets from the targeted server.

As a result of the targeted server utilising resources to check and then respond to each received UDP packet, the target's resources can become quickly exhausted when a large flood of requests are received, resulting in denial-of-service to normal traffic.

How is a UDP flood attack mitigated

Most operating systems limit the response rate of ICMP packets in part to disrupt DDoS attacks that require ICMP response. One drawback of this type of mitigation is that during an attack legitimate packets may also be filtered in the process. If the UDP flood has a volume high enough to saturate the state table of the targeted server's firewall, any mitigation that occurs at the server level will be insufficient as the bottleneck will occur upstream from the targeted device.

A DNS (or Nameserver) Flood

Domain Name System (DNS) services are essentially a “phonebook” of the Internet; they convert easy to remember names into sequences of digits known as IP addresses – how machines and computers talk to each other on the Internet. A DNS flood is a type of distributed denial-of-service attack (DDoS) where an attacker floods a particular domain’s DNS servers in an attempt to disrupt DNS resolution for that domain. If a user is unable to find the phonebook, it cannot lookup the address in order to make the call for a particular resource. By disrupting DNS resolution, a DNS flood attack will compromise a website, API, or web application's ability respond to legitimate traffic. DNS flood attacks can be difficult to distinguish from normal heavy traffic because the large volume of traffic often comes from a multitude of unique locations, querying for real records on the domain, mimicking legitimate traffic.

How does a DNS flood attack work?

The function of the Domain Name System is to translate between easy to remember names (e.g. example.com) and hard to remember addresses of website servers (e.g. 192.168.0.1), so successfully attacking DNS infrastructure makes the Internet unusable for most people. DNS flood attacks constitute a relatively new type of DNS-based attack that has proliferated with the rise of high bandwidth Internet of Things (IoT) botnets like Mirai. DNS flood attacks use the high bandwidth connections of IP cameras, DVR boxes and other IoT devices to directly overwhelm the DNS servers of major providers. The volume of requests from IoT devices overwhelms the DNS provider’s services and prevents legitimate users from accessing the provider's DNS servers.

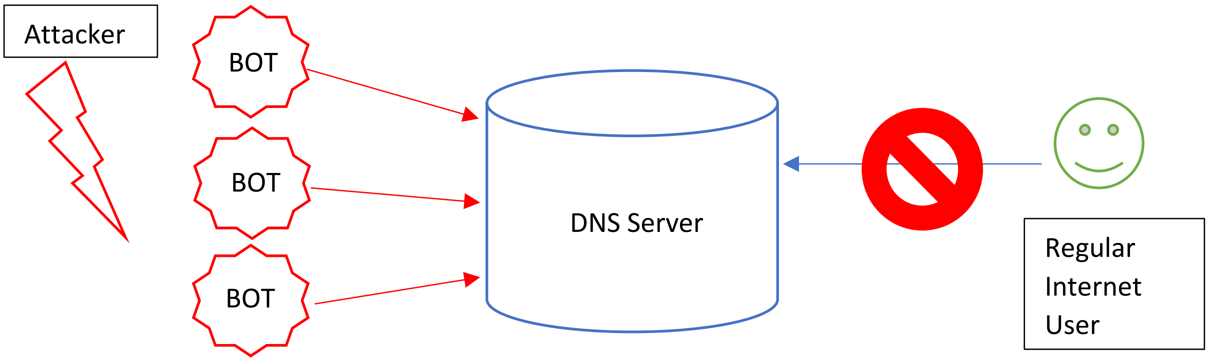

Figure 2: Simple example of a DNS DoS attack, where the user fails to get a DNS response from the DNS service

DNS flood attacks differ from DNS Amplification Attacks. Unlike DNS floods, DNS amplification attacks reflect and amplify traffic off unsecured DNS servers in order to hide the origin of the attack and increase its effectiveness. DNS amplification attacks use devices with smaller bandwidth connections to make numerous requests to unsecured DNS servers. The devices make many small requests for very large DNS records, but when making the requests, the attacker forges the return address to be that of the intended victim. The amplification allows the attacker to take out larger targets with only limited attack resources.

How can a DNS Flood attack be mitigated?

DNS floods represent a change from traditional amplification-based attack methods. With easily accessible high bandwidth botnets, attackers can now target large organizations. Until compromised IoT devices can be updated or replaced, the only way to withstand these types of attacks is to use a very large and highly distributed DNS system that can monitor, absorb, and block the attack traffic in real-time.

What to do in the event of a DDoS Attack?

DDoS Preparation Checklist

1. Understand no organisation is safe. It's not about if you will be attacked, but about when.
2. Make sure detection tools are optimally located. Remember, you can only protect against what you can detect.
3. Make sure your security strategy is implemented into policies and procedures and that your staff are prepared with specially defined roles and responsibilities.
4. Perform on-going tests and evaluations of your systems and of new technologies that are available in the market. For example:
    a. Verify whether your organization could bene t more from an out-of-path implementation of some of your detection tools.
    b. Evaluate the implementation of a hybrid solution to protect your organization during attacks that saturate the internet pipe.
5. Make sure your staff knows the Incident Response procedure and have an available easy-to-locate list of people to contact when under attack. If you are at risk of having a public website down, prepare an explanation and apology for an inconvenience message.
6. Don't implement multiple detection tools from different vendors, unless these different tools are able to "communicate" with one another and pass relevant information for optimal detection.

DDoS Under Current Attack Checklist

1. Don't panic!
2. Don't decide what to do before consulting your in-house/provider's emergency response team.
3. Don't transfer traffic to the cloud scrubbing centre unless you are close to pipe saturation.
4. Don't ignore customers and make sure someone reassures them even during the attack.
5. Contact the in-house and/or vendor's Emergency Response Team to make sure best decisions are carried out. If you depend on an ISP vendor, contact them now.
6. Define the detection point, attack type and tool, and decide on best mitigation process.
7. Make sure every step of the attack is documented.
8. Have a spokesperson ready to provide information to your customers during the attack (via alternative media such as social media).

Post DDoS Attack & Prepare Lessons Learnt

1. Perform a damage control analysis and review reports and forensics, learn what went wrong so you can better prepare for future attacks. Investigate everything.
2. Optimise your security architecture. Make sure you analyse and evaluate every aspect of the attack. Adapt technologies, policies and solution strategies.
3. Notify customers/press with relevant details. Online businesses should consider a marketing campaign to win back the hearts of disappointed customers.
4. Make sure your reports and forensics information are available in case it is needed for law enforcement investigation.
5. Don't think for one second that when the attack is over you can sit back and relax.
6. Don't delay implementing the outcomes of the attack investigation, be it security strategy, technology solutions, policies, roles and responsibilities, and anything else important to your business.

Defending against DDoS attacks

Volume Based Attacks

Use an ISP or Cloud-service provider that can execute a scrubbing service.

What is a scrubbing service?

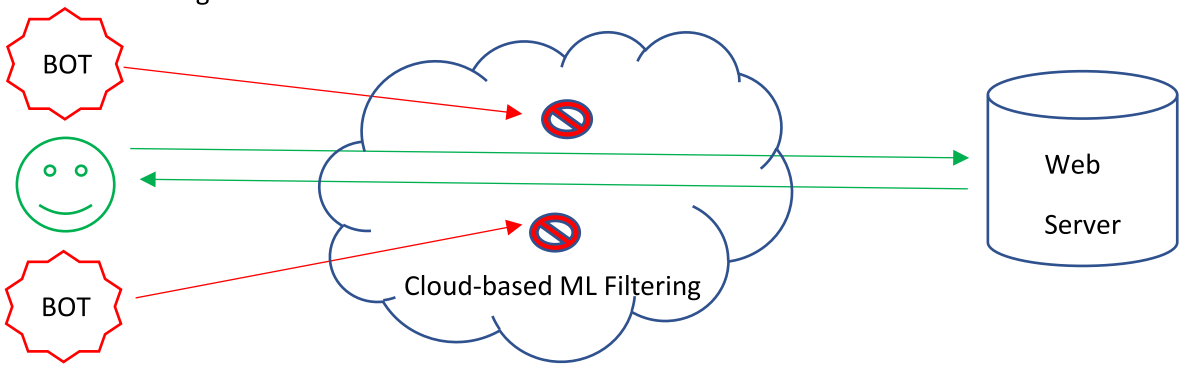

Figure 3: Example of a cloud-based (Machine Learning) scrubbing service, that filters bots, but permits legitimate traffic

As traffic enters a scrubbing centre, it is triaged based on a various traffic characteristics and possible attack methodologies. Traffic continues to be checked as it traverses the scrubbing centre to confirm the malicious traffic has been fully removed. Clean traffic is then returned to your application with little to no impact to the end user.

Protocol Attacks

Depending on the technology and network design, you can try filtering known bad addresses, or temporarily the known sources of attack.

This can be as simple as adding additional firewall deny rules, or NACLs in cloud-based providers. Stripping malicious traffic at the network level reduces the load on your application servers.

The downside of this defence is that if your firewall appliance is under sever-load or itself a DDoS, your normal users will still struggle to connect and request resources from your web application or services, despite being healthy hosts and fully operational.

Application Layer Attacks

With the advancement of Next-Generation Firewalls (NGFW), or through the use of existing Web Application Firewall (WAF) appliances and/or technologies; Consider updating your signatures to the latest version and enabling a number of appropriate WAF rules to block layer-7 and application-based attacks, that may consume additional resources.

Depending on your application; consider implementing captchas or other input-based challenges such as 2FA, and rate-limiting API's to reduce the throughput of malicious input-based attacks. Machine learning is a new technology, that can analyse user behaviour, and then dynamically block known bad bots from accessing your applications.

Appendix A: How to Evaluate a Vendor for DDoS & Cyber-Attack Mitigation

These set of questions can be used to evaluated the ability for the vendor to provide high-quality DDoS detection (Reminder: prevention is not 100% guaranteed against modern advancements in DDoS type attacks):

Area of Assessment	Functionality Provided?
Type(s) of Detection Available	Net flow
	Layer 7 Header-less Mode
	Open flow
	Coverage of OWASP Vulnerabilities
	Packet Layer 3/4
	Inputs/Signals from Other Mitigation Tools
	Packet Layer 7 Header Required
Deployment Model Options	In-Line
	Cloud Scrubbing Centre – Asynchronous
	OOP – Synchronous
	Software Defined Networking (SDN)
	Hybrid Cloud Options
	Virtual Deployment Options
	Internal Scrubbing Centre – Asynchronous
	Feeds from Partners/Works with Other Vendors' Signals
Time – This section evaluates the categories required for modern attack detection:	Real-Time Options
	Signalling/Automatic Options (for Advanced Application Attacks)
	Signalling/Automatic Options (for Cloud Diversion)
Reporting & Response – This section evaluates the categories required for controlling and reporting modern attack detection	Real Time
	Detection Support Response – Real Time
	Historical Data
	Detection Support Response – On-Site Options
	Forensic Reports
	Integrated Reporting with Cloud Portal
	Intelligence Reporting
	Ability to Discern Legitimate vs. (that is, can detect before attack) Illegitimate Traffic in Real Time
	How good is the vendor at mitigation?
Quality – Does the vendor over-mitigate or under-mitigate the threats? How many technologies are leveraged to assist?	Rate-Only
	HTTP Server-Based Protections
	Routing Techniques
	HTTP OWASP-Based Protections
	Rate Behaviour Only
	Hybrid Signalling/Cloud Scrubbing Centre Coordination
	SSL Protections
	Heuristic Behaviour
	HTTP Redirects

	Statistical Behaviour
	JavaScript Challenge & Response
	Cloud Challenge Response
Updates & Signatures – How are they managed?	Signatures – Custom Real Time
	Signatures – Static with Update Service

Appendix B: Known Historical (D)DoS attacks

As attack technology evolved, so have motivations and participants. Recent years have brought a continuous increase in the number of DDoS attacks—fuelled by changing and increasingly complex motivations.

Event	Year	Description
Major Political Attacks	2014	Energetic Bear malware targets US and Canadian critical infrastructure providers as part of cyber espionage attack
	2014	Mobile news application provider Feedly is taken down by series of DDoS attacks
	2014	Hacktivist group #OpHackingCup takes down Brazil World Cup website
	2012-2013	Operation Ababil targets financial institutions
Activism, rise of anonymous, State sponsored	2011-2012	Operation Tunisia, Operation Sony, Operation Syria, Operation MegaUpload, Operation Russia, Operation India, Operation Japan etc.
	2010	Operation Payback, Avenge Wikileaks' Assange
	2009	Attacks on Facebook, Twitter, Google
	2009	Attacks on Iranian government websites
Political agenda, criminal extorsion	2009	Attacks South Korean and American websites + Washington Post, NYSE
	2009	Attacks on UltraDNS, Register.com, the Pirate Bay
	2008	Attacks on Georgian government sites
	2007	Cyber attacks target Estonia, an early example of cyber warfare

	2018	GitHub – Worlds Largest DDoS attack 1.35Tbps at peak
Democratisation of DDoS	2016	Mirai – Utilising vulnerable IoT devices to launch DDoS
	2003	MyDoom attacks 1M computers, Attacks on ClickBank and Spamcop, Worm blaster, Attack on Al-Jazeera website during Iraq war
	2002	Attack on Internet's DNS Root servers DoS reflected tools
	2000	FBI site taken down, Seattle's Oz.net down, Attacks on eBay, Yahoo, Etrade, Buy.com, Amazon, Excite.com, CNN
	1999	Trinoo, Tribe Flood Network, Stacheldraht, Shaft University of Minnesota taken down
Pre 2000 Attacks	1997-1998	Smurf attacks; First DDoS tools - Teardrop, Boink, Bonk, WinNuke
	1996	First SYN Flood
	1988	Morris Worm, AOL's Punters