US SIGNAL®

DISTRIBUTED DENIAL OF SERVICE (DDoS)

UNDERSTANDING AND MITIGATING ATTACKS

201 Ionia Ave, Grand Rapids, MI 49503 | 866.2.SIGNAL | ussignal.com

PAGE
2

Table of Contents

Introduction

In today's digital world, cyber-attacks have practically become commonplace. Among the most frequent and costly are denial of service (DoS) attacks. A DoS attack attempts to "deny service" to a web site, application or other online resource by making it unavailable to its intended users. While they don't try to breach an organization's security perimeter, DoS attacks do cause costly downtime and often camouflage other malicious activities.

Distributed denial of service (DDoS) attacks are a particularly damaging kind of DoS attack. They employ multiple, distributed resources to take down websites and other services. The distribution of those resources makes it much more difficult to identify and block their source.

Compounding the challenge is the fact that DDoS attacks require little knowledge of computers or networks. A fast-growing online marketplace for DDoS attack services and tools makes it possible for just about anyone to launch an attack, expanding the pool of potential assailants. Not surprisingly, suppliers of DDoS attack services and tools are continually developing new attack methods and incorporating increasingly powerful vectors into their offerings to take advantage of what can be called the "commodization" of cyber-attacks.

The Internet of Things (IoT) is likely to usher in even more DDoS attacks. The potential was already demonstrated in 2016 when cyber-criminals used thousands of hacked devices, mostly internet-connected cameras, to force a well-known security website to go offline by flooding it with an unprecedented amount of traffic[1].

Despite what seems like an unsurmountable battle, there are ways that companies can reduce the chance of being victims of DDos attacks, as well as mitigate the damage if they are. The purpose of this whitepaper is to provide an overview of some of them, as well as offer insight into how and why DDoS attacks occur.

Know Your DoS from Your DDoS

While DoS and DDoS are sometimes used interchangeably, they are different types of attacks. A DoS attack is an attempt to render a technical service, such as a website, application or network, unusable and unavailable to a user. Typically, a single computer and internet connection are used to flood a server with packets (TCP / UDP). By overloading the targeted server's bandwidth and other resources, the server becomes inaccessible and the website or whatever else is hosted there is blocked.

A DDoS attack works much the same way but involves multiple computers and connections to prevent system access. The computers behind the attack are often distributed across a wide geographic range or even around the world. Because the target server in a DDoS attack is overloaded by multiple sources, it's extremely difficult to mitigate. DDoS attacks

[1] Michael Hiltzik, Los Angeles Time. "Cybersecurity expert Brian Krebs was silenced by a huge hacker attack. That should terrify you." October 5, 2016. http://www.latimes.com/business/hiltzik/la-fi-hiltzik-iot-cybersecurity-20160928-snap-story.html

are almost always high-traffic events, commonly measured in gigabits per second (Gbps) or packets per second (PPS). The largest network layer assaults can exceed 200 Gbps. However, 20 to 40 Gbps are enough to completely shut down most network infrastructures.

Attackers can use any of a wide variety of tactics and tools to generate the traffic necessary for a DDoS attack. If they have access to a botnet — a network of internet connected devices such computers or smartphones whose security has been breached and are being controlled by a third party, they may use that to orchestrate the attacks. Or, they may hire botnets from operators who charge fees for short duration attacks.

Still others take advantage of the variety of tools available online, many of which are free. Most were originally developed as stress testers but have since become open source tools for launching DDoS attacks. Among them are the Low Orbit Ion Cannon (LOIC) and the High Orbit Ion Cannon (HOIC). The LOIC sends Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) traffic. The HOIC sends HTTP traffic.

There are numerous ways to classify the various types of DDoS attacks, but most usually are one of two types: standard or reflection.

Standard DDoS Attacks

A standard DDoS attack occurs when attackers send a substantial amount of network traffic directly to a target server or network, often using a botnet. When attackers use botnets in a DDoS attack, they send instructions to some or all the “zombie” machines connected to that botnet. That magnifies the size of the attack because it originates from multiple networks, even multiple geographic areas.

Among the most common type of standard DDoS attack is a SYN Flood, which takes place when an attacker sends a succession of SYN requests to the target. When the server receives a SYN request, it acknowledges the request and holds the communication open while it waits for the client to acknowledge the open connection. The client acknowledgment never arrives in a SYN Flood, which ties up the server’s resources until the connection times out. A UDP Flood is similar, but rather than trying to exhaust server resources, it tries to consume all the available bandwidth on the server’s network link.

Another type of standard DDoS attack is the ICMP Flood. An attacker uses a botnet to send a large number of ICMP packets to a target server to consume all available bandwidth and prevent users from accessing the server. With an HTTP GET Flood, the attacker generates continuous HTTP GET requests for a target website to the extent that enough resources are consumed to make the server unavailable.

Reflection DDoS Attacks

A reflection DDoS attack occurs when attackers make their IP address look like it is that of the target. They tend send legitimate requests to public-facing servers. The responses to the requests, originating from those servers, are sent to the real victim. Reflection DDoS attacks often employ amplification to increase their effectiveness. The byte count of traffic received by the victim is much larger than that of the traffic sent by the attacker, which "amplifies" the sending power of the attacker.

An example is a Network Time Protocol (NTP) reflection attack, in which an attacker uses traffic from a legitimate NTP server to consume all a target's resources. The attacker can spoof the target's IP address and send a monlist command to request the NTP server to send a large amount of information to the target. The response from the NTP server exceeds that of the request sent from the attacker, so the effect of the attack is amplified.

Another common type of reflection DDoS attack is the Domain Name System (DNS) reflection attack. An attacker spoofs the victim's IP address and sends DNS name lookup requests to public DNS servers. The DNS servers then send responses to the target server. To maximize the amplification, the attacker can use the word "ANY" in their request so all known information about a DNS zone is sent in response to a single request. This will eventually consume all available bandwidth.

Other types of DDoS reflection attacks include those associated with specific functions within WordPress, the content management system, and Microsoft (MS) Structured Query Language (SQL), an application used to manage relational databases.

Why DDoS Attacks Happen

The goals and motivation behind DDoS attacks, like most types of cyber-attacks, vary. While the reasons "why" are less important than the "how," understanding the various rationales can help in developing a comprehensive mitigation strategy. Extortion seems to be the prevalent driver behind most recent DDoS attacks but others are the result of:

- Punishment for not giving in to extortion attempts
- Politically or socially motivated "hacktivism"
- Cyber vandalism
- Rivalry between "online gangs," in which groups engaged on Internet-based malicious activities use DDoS attacks against each other
- Anti-competitive business practices
- Attempts to distract from other malicious activities

- Human error or non-malicious actions that an organization's employees took by mistake
- Curiosity about just how much damage can be done
- Simple maliciousness

Attack Trends

Perspectives on DDoS trends vary, depending on those observing and analyzing them. According to Nexusguard, a company specializing in DDoS mitigation, there was an 83% increase in the volume of DDoS attacks in 2016 compared to 2015.[1] A closer look at that 83% shows that the increase is evenly distributed between application and network attack vectors. However, a report issued by Imperva, an application and data security firm, showed application layer attacks becoming more common. The company noted the number of attacks in Q4 reached an all-time high, with an average of 889 application layer assaults per week.[2]

Somewhat surprisingly, Verisign, an internet security firm, saw a 23% decrease in attacks during the first quarter of 2017.[3] It is likely that the lull in DDoS activity was only temporary. The company did note the average peak attack size increased 26% compared to the previous quarter. The largest, highest intensity DDoS attack observed by Verisign was a multi-vector attack that peaked over 120 Gbps and around 90 million packets per second (Mpps). The attack sent a flood of traffic to the targeted network exceeding 60 Gbps for more than 15 hours. It consisted primarily of TCP SYN and TCP RST floods of varying packet sizes and employed one of the signatures associated with the Mirai IoT botnet.

Attackers also launched sustained and repeated attacks against their targets, with Verisign observing that almost 50 percent of customers who experienced DDoS attacks in Q1 2017 were targeted multiple times during the quarter.

Cybersecurity and anti-virus provider Kaspersky Lab noted a sharp increase in the number and proportion of TCP DDoS attacks for first quarter of 2017, from 10.36% to 26.62%. The increase was attributed to greater botnet activity by the Yoyo, Drive and Nitol families.[4]

UDP and ICMP attacks also grew significantly, from 2.19% to 8.71% and from 1.41% to 8.17% respectively. Yoyo and Darkrai activity were blamed, although Darkrai bots also began conducting more UDP attacks. The company noted a considerable decline in the share of SYN DDoS (48.07% vs. 75.33%) and HTTP (from 10.71% to 8.43%) attacks.

According to Arbor Networks , a network security company, the largest number of DDoS attacks in 2016 peaked at 800 Gbps (gigabit per second), compared to only 500 Gbps in 2015.[5] The company reported that 558 of the DDoS attacks it observed last year were over 100 Gbps (as opposed to 223 in 2015), while 87 of them exceeded 200 Gbps (only 16 did in 2015). The company estimates that attacks will reach 1.2 Tbps by the end of 2017.

[1] Nexusguard. DDoS Threat Report Reflection Attacks, Q2 2016. https://www.nexusguard.com/hubfs/Nexusguard_DDoS_Threat_Report_Q2_2016.pdf?hsCtaTracking=a7b724c7-8f07-4470-a228-1d310cec53d3%7C094963d0-3d7c-42db-aec2-e87f44496355

[2] Imperva Global DDoS Threat Landscape Report 2015-2016. https://lp.incapsula.com/rs/804-TEY-921/images/2015-16%20DDoS%20Threat%20Landscape%20Report.pdf

[3] Verisign Distributed Denial of Service Trends Report, Volume 4, Issue 1 – 1st Quarter. https://www.verisign.com/assets/report-ddos-trends-Q12017.pdf

[4] Securelist. Alexander Khalimonenko, Oleg Kupreey, DDOS attacks in Q1 2017. May 11, 2017. https://securelist.com/ddos-attacks-in-q1-2017/78285/

[5] Securelist. Alexander Khalimonenko, Oleg Kupreey, DDOS attacks in Q1 2017. May 11, 2017. https://securelist.com/ddos-attacks-in-q1-2017/78285/

However, if any single trend stands out in 2016 and 2017, it is the emergence of IoT botnets, such as Mirai, as the drivers behind incredibly high-volume DDoS attacks. Multiple cases have been reported of IoT devices and Linux servers being infected with Rakos malware. Linux servers often have distinct vulnerabilities but no protection from a reliable security solution, making them susceptible to bot infection.

The potential for widespread destruction is particularly unnerving given the proliferation of IoT devices. An attack launched by the BASHLITE IoT botnet in Brazil last year reached 400 Gbps without using any form of amplification or reflection.

Yet another emerging trend is the increasing complexity of attacks as exemplified by the combined attack (SYN + TCP Connect + HTTP-flood + UDP flood) on the Moscow stock exchange. The attack was distinctive because of its rare multi-vector nature, combined with relatively low power (3 Gbps). Another attack launched against the Portuguese police force employed vulnerabilities in reverse proxy servers to generate attack traffic. The perpetuators may have been attempting to hide the real source of the attack. New types of botnets were used, consisting of vulnerable reverse proxies, were used to generate traffic.

Best Practices for DDoS Attack Mitigation

As has been seen with other information security-related threats and associated technologies, DDoS mitigation seems to be an all or nothing approach for many companies. Most fall into one of four broad categories:

1. Has been attacked and has implemented a strategy
2. Has been attacked and has not implemented a strategy
3. Will be attacked and had implemented a strategy
4. Will be attacked and has not implemented a strategy

Many companies fall into the “Has been attacked but has not implemented a strategy” category because they haven’t found a cost-effective means of implementing the required response plans, technologies and staffing support. Regardless of available budget and technical expertise, there are some measures that all companies should have in place.

The type of DDoS attack plays an important role in how you reduce its effects. However, knowing your critical systems and being able to tell if they are being attacked, is an important first step. If you don’t know how, your security or firewall vendors have documentation on that subject.

The following general best practices also provide a good starting point for developing a DDoS response and mitigation strategy.

1. Create a Risk Profile.

One of the first steps in minimizing your organization's risk of a DDoS attack is to create a risk profile. Start by answering the following questions:

- Why would we be a good candidate to attack?
- Are we in a high-risk industry such as online gaming, software and technology, financial services, etc.?
- What do we have that someone might want?
- What enemies or aggressive competitors do we have?
- What activities are happening on our systems that might make us a target?
- How would a DDoS attack affect our business?
- What are our potential threat vectors and how should they be characterized and prioritized?
- How long could we go without systems affected by a DDoS attack?

2. Develop an Incident Response Plan.

An incident response plan is essential for helping your organization respond quickly if a DDoS attack occurs. To create one:

- Identify what your critical systems are and understand how to tell if they are being attacked. Signs of a DDoS attack may include, but aren't limited to: unusually slow network performance opening files or accessing websites, the unavailability of a website, or a dramatic increase in the number of received spam emails.
- Request any relevant documentation on DDoS attack mitigation and prevention from your security or firewall vendors, or managed security providers.
- Compile a list of people to help in the event of an attack. Include members of your company's executive management team, your internet service provider (ISP), internal and external information security experts, and law enforcement professionals, including from the FBI.
- Determine your strategies for dealing with an attack. Can you shut down services or implement your DR plan? Can your ISP block the traffic? If so, what does it need from you to make it happen?

3. Establish and Maintain Effective Partnerships.

One of the most important partnerships to forge is with your upstream network service provider. Know what assistance your provider can give in the event of a DDoS attack.

If you experience a DDoS attack, provide the attacking IP addresses to your upstream network service provider so it can implement restrictions at its level. Keep in mind that DDoS reflection attacks typically originate from legitimate public servers. It is important to ascertain to whom an IP belongs to when examining network logs during an attack. Use tools such as the American Registry for Internet Numbers (ARIN) to look up the source IPs involved in the attack. Otherwise, you may block traffic from legitimate networks or servers.

The faster your provider can implement traffic blocks and mitigation strategies at its level, the sooner your services will become available for legitimate users.

Whether it be a DDoS protection provider, your local ISP or a cloud-hosting provider, for better or worse, you will not be able to effectively handle attacks without these partners. Engage them to understand what they can do to help and where gaps may remain.

Also make sure to understand what your role is, what your partners' roles are, and where the demarcation point is. From a general information security perspective, the following matrix can help you understand if all areas are addressed and who is responsible. Use something similar to make sure you have identified all your systems, the associated security measures and who is responsible for them.

Figure 1.1

Cloud Provider Responsibility
Customer Responsibility

	Physical	Technical		Management
		Control Plane	Data Plane	
Application	–	–	–	–
Middleware	–	–	–	–
Database	–	–	–	–
Operating System	–	–	–	–
Compute and Memory	–	–	–	–
Storage	–	–	–	–
Internet	–	–	–	–
Data Center LAN/WAN	–	–	–	–
Facilities	–	–	–	–

4. Employ Your Existing Security Capabilities.

Chances are you already have DDoS mitigation and prevention capabilities or access to them via a provider. Take time to understand what you have, what you can do, and what others can do for you.

- The security appliances you currently use may have features to assist with DDoS detection and prevention. Know what they are and how they work. Enable them if aren't already on.
- Configure firewalls and intrusion detection/prevention devices to alarm on traffic anomalies.
- Make sure firewalls only accept traffic detailed in your organization's security policy as required for business purposes.
- Set firewalls to block, as a minimum, inbound traffic sourced from IP addresses that are reserved (0/8), loopback (127/8), private (RFC 1918 blocks 10/8, 172.16/12, and 192.168/16), unassigned DHCP clients (169.254.0.0/16), multicast (224.0.0.0/4) and otherwise listed in RFC 5735. This configuration should be requested at the ISP level as well.
- Enable firewall logging of accepted and denied traffic to determine where the DDoS may be originating.
- Many ISPs can help with DDoS mitigation and prevention by blocking traffic to or from specific Internet hosts. Check with your ISP to learn about the options.
- Taking hosts offline or moving them to disaster recovery facilities can mitigate issues. In addition, you can shed certain services that are being attacked to protect the services that aren't under attack. That will require triaging your services and knowing which ones are the most important.

5. Plan Your Defense.

Take steps to better defend your company against DDoS attacks. Among them:

- Implement a routing protocol like Border Gateway Protocol (BGP), so you can block or re-route traffic yourself. This will allow you to send routing information to your service provider dynamically and have more control over the situation.
- Tap the expertise of others. Attend local ISC2 events and speak with other companies about what works and what doesn't. Involve your network service providers in your planning, testing, and event management. Work with law enforcement, including the FBI. The InfraGard program, a partnership between the FBI and members of the private sector, provides resources to help you stay abreast of attack events and learn about emerging solutions without vendor bias.

- Move your security perimeter as far from your network as possible, into your services providers' colocation data center or to a security solution hosted by your provider if possible. This transfers the problem of DDoS attacks into the provider's network.

- Move web-based services to the cloud. Most cloud services employ DDoS mitigation technologies and best practices. They also have more internet bandwidth available so they are better able to absorb larger DDoS attacks than end users can.

- Make sure you understand what your role is in defending against DDoS threats, what the service provider's role is, and where the demarcation point is. Use the table in Figure 1.1 to determine if all areas are addressed and who is responsible.

US Signal at Your Service

DDoS prevention can be a complicated, sometimes expensive endeavor. It doesn't have to be when you work with US Signal.

US Signal has extensive experience in dealing with DDoS attacks. Our team can help your company develop a strategy best suited to its business needs and budgetary parameters, drawing from our robust portfolio of customizable cloud and colocation solutions, data protection services, and network services. To learn more now, call 866.2. SIGNAL or email info@ussignal.com

About the Author

Aaron Shaver, PhD

Aaron Shaver leads US Signal's long-term technology vision, and is responsible for its strategic customer partnerships, university collaboration, industry thought leadership and advanced technical solutions.

He has more than 20 years of experience in telecommunications, data center design and information security. Aaron holds a doctorate in information assurance and computer science and a master's degree in information security. His research has focused on disaster recovery and mitigation.