A Layperson's Guide To DoS Attacks

A Rackspace Whitepaper

RACKSPACE® HOSTING | 1 FANATICAL PLACE | SAN ANTONIO, TX 78218 U.S.A.

rackspace®
the open cloud company

Table of Contents

1. Introduction

Flood! Ping of death! Teardrop! The terminology used by security experts may cause you to avoid wanting to learn more about it. But today's business is fueled by the Internet, and your organization is running mission-critical applications on the web. It may be up to you and your team to ensure that your sites continue to connect you with your customers, end users, suppliers and partners. Since DoS attacks are increasing in frequency, size and notoriety, it is important to gain a basic understanding of this type of Internet threat.

Just as entities across the world are increasingly leveraging the Internet to conduct legitimate business, we are also seeing a sharp rise in the amount of internet attacks that seek to steal, disrupt or disable access to resources and systems. These attacks jeopardize the operation of the enterprise by disrupting sales, causing productivity loss and degrading brand image. Organizations should implement actions to protect not only against the short term effects such as site disruptions and business losses, but also against the long term effects such as brand image and reputation loss.

The goal of this white paper is to inform and educate business users, particularly those who are not immersed in the world of information security or Denial-of-Service (DoS) attacks.

2. An Introduction to DoS and DDoS Attacks

According to the Imperva Hacker Intelligence Report, "a DoS attack aims to 'take down' a site in order to make it inaccessible to its users. This may cause serious financial damage to the site, both directly and indirectly by damaging its reputation."[1]

A DoS attack aims to 'take down' a site in order to make it inaccessible to its users.

DoS attacks have evolved and the Distributed-Denial-of-Service (DDoS) attack has emerged. The main difference between a DoS and DDOs attack is that a DoS attack uses one computer and one internet connection while a DDoS attack uses a large number of computers and internet connections that are often distributed globally. In DDoS attacks, an individual or organization takes control of hundreds, thousands and even millions of computers that are then used to target other systems. In a DDoS attack the victims comprise both the targeted system as well as all the systems that the perpetrator maliciously gains control over and uses to launch the attack. Since the victim gets flooded by incoming traffic spread across many different points of origin, it is very difficult to differentiate between legitimate and malicious traffic. For simplicity, we will refer to DoS and DDoS as "DoS" for the rest of this document.

Historically, DoS attacks focused on the network and server layers (the lower layers) of the technology stack. Over time, these attacks have been moving higher up the stack, targeting the Web application layer as well. Defending against attacks targeting the web application layer is more complex. According to Imperva, over the last few years, attackers have moved "their DoS attacks up the stack and into the Web application layer in order to decrease costs, as Web app DoS is more efficient and avoids detection as many anti-DoS solutions are traditionally focused on lower layers."[2]

Industry reports indicate that DoS attacks are growing in number.

Industry reports indicate that DoS attacks are growing in number. Information collected by Rackspace corroborates the same trends. In line with industry trends, we are also seeing an increase in the magnitude of DoS attacks.

3. Types of DoS Attacks

In simple terms, DoS attacks affect systems or networks by exhausting resources or exploiting vulnerabilities. DoS attacks may be broadly classified into different types based on the techniques used by the attackers. In its Hacker Intelligence Report, Imperva categorizes DoS attacks as IP attacks on the network bandwidth, TCP attacks on the server sockets, HTTP attacks on the Web server threads and Web application attacks on CPU resources.[3]

Some of the older types of DoS attacks include the Flood Attack, Ping of Death attack, SYN attack, Teardrop attack and Smurf attack.

- In Flood attacks, an attacker deliberately sends more traffic to a server than it can handle with the objective of making it unavailable to users.
- The Ping of Death attack takes advantage of a weakness in the early implementations of the TCP/IP protocol. In those early versions, sending a ping packet that was larger than specified would crash the system.
- SYN attacks exploit vulnerabilities in the TCP/IP protocol with the objective of exhausting server resources so that it is does not respond to legitimate traffic.
- The Teardrop attack involves sending corrupted IP packages to confuse and crash the targeted system.

DoS attacks have been evolving rapidly and newer threats are a much more advanced class of attack. "The challenge with [application-layer attacks] is that these attacks are harder to detect; they're more stealthy, they don't generate a large network bandwidth but they're equally capable of taking down a network,"[4] according to Arbor Networks.

Newer forms of DoS attacks avoid signature-based defenses, leaving networks vulnerable. A few examples of these types of threats include:

- ICMP Flood or Smurf, in which an attacker depends on misconfigured network devices and uses a fake source IP address that makes it appear as if the attack is coming from inside the network.
- Slowloris is a highly targeted attack that enables one web server to take down another web server by holding open the maximum number of web connections for as long as possible. It does this in a stealthy mode without visibly affecting other services or ports on the target network.
- Zero-day DDoS attacks refers to attacks that target new or unknown vulnerabilities for which a fix may not be currently available.

4. Defending Against DoS Attacks

One of the consequences of the variety of DoS attacks is that it has become challenging for protection technology to keep up. As a result, an organization's defense strategy will depend on the specific situation at hand, because no single approach will be capable of defending against the variety of DoS attacks.

Others seem to agree. According to Gartner's Anton Chuvakin, "No single type of a security safeguard can reliably stop all DoS attacks, and thus, enterprise DoS defense strategy must involve multiple components and safeguard types." He goes on to state that "the defense calculus for denial of service is different because no organization can prevent or block all DoS attacks on its own."[5]

A layered approach leveraging multiple technologies, security experts and security processes can provide a more effective protection to help mitigate the risks from DoS attacks.

Rackspace hosts systems for thousands for customers and offers a range of defense mechanisms to help protect customers' hosted environments. The technology components of a DoS defense strategy may include the following:

- Firewalls and Load Balancers: These provide basic threat prevention and protection with features like Blocking, Whitelisting, Packet Inspection, and Virtual Private Networks.
- Intrusion Detection & Prevention Systems (IDS): An IDS inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack. An IDS also watches for attacks that originate from inside a system. The primary difference between an IDS and Intrusion Prevention System (IPS) is that in addition to detecting intrusions, an IPS also actively blocks intrusions.
- Web Application Firewalls (WAF): A WAF inspects web traffic and dynamically learns from incoming traffic and adapts to allow legitimate traffic. Unlike traditional firewalls, WAFs have the ability to inspect http and https traffic.
- DDoS Mitigation Services: Rackspace DDoS Mitigation Services is a hardware-based program that helps keep customer systems online in the event of a DDoS attack. Features include network-wide packet scanning, granular traffic analysis, server-level anomaly detection and a three layer approach to help detect, identify and filter hostile traffic 24x7x365. When an attack occurs, DDoS processing is offloaded from the customer's configuration to the Rackspace infrastructure allowing the customer to continue to do business as usual even during the attack. The Rackspace DDoS Mitigation Service includes expertise from trained security technicians who recommend mitigation techniques and take action when attacks occur. While we cannot guarantee that your system won't be attacked, we recommend our DDoS Mitigation Services to customers who want to a higher level of protection and faster recovery from DDoS attacks.

5. Conclusion

Dealing with DoS and DDoS attacks has become one of the costs of internet applications and infrastructure. These attacks tend to be sophisticated, and no single approach can be effective against all forms of attack. Attacks are highly situational and avoidance can never be guaranteed. However, a comprehensive and pragmatic security policy, together with a combination of mitigation technologies and assistance from experienced security and network technicians, can help provide guidance and mitigate risks.

This paper is just an overview of DoS and DDoS attacks. We hope that it has helped you start to understand the challenges you may face as you deploy your cloud application or hosted solution. If you would like to have a deeper conversation based on the specific business and technical needs of your application, don't hesitate to reach out to Rackspace. Our Fanatical Support® personnel are ready to help.

6. Notes

1.-3. Imperva's Hacker Intelligence Initiative, Monthly Trend Report #12 (September 2012)

4. TechTarget (SearchSecurity) article "DDoS attacks growing in size, break attack bandwidth barrier, Arbor Networks says" (February 7, 2011)

5. Gartner Report: "Denial of Service: A Comparison of Defense Approaches" by Anton Chuvakin

DISCLAIMER

This whitepaper is for informational purposes only and is provided "AS IS." We strongly recommend that you engage additional expertise in order to further evaluate applicable requirements for your specific environment.

RACKSPACE MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, AS TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS DOCUMENT AND RESERVES THE RIGHT TO MAKE CHANGES TO SPECIFICATIONS AND PRODUCT/SERVICES DESCRIPTION AT ANY TIME WITHOUT NOTICE. RACKSPACE RESERVES THE RIGHT TO DISCONTINUE OR MAKE CHANGES TO ITS SERVICES OFFERINGS AT ANY TIME WITHOUT NOTICE. USERS MUST TAKE FULL RESPONSIBILITY FOR APPLICATION OF ANY SERVICES AND/OR PROCESSES MENTIONED HEREIN. EXCEPT AS SET FORTH IN RACKSPACE GENERAL TERMS AND CONDITIONS, CLOUD TERMS OF SERVICE AND/OR OTHER AGREEMENT YOU SIGN WITH RACKSPACE, RACKSPACE ASSUMES NO LIABILITY WHATSOEVER, AND DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO ITS SERVICES INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT.

Except as expressly provided in any written license agreement from Rackspace, the furnishing of this document does not give you any license to patents, trademarks, copyrights, or other intellectual property.

Rackspace, Fanatical Support, and/or other Rackspace marks mentioned in this document are either registered service marks or service marks of Rackspace US, Inc. in the United States and/or other countries. Third-party trademarks and tradenames appearing in this document are the property of their respective owners. Such third-party trademarks have been printed in caps or initial caps and are used for referential purposes only. We do not intend our use or display of other companies' tradenames, trademarks, or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.