SOLUTIONARY®
RELEVANT . INTELLIGENT . SECURITY

White Paper

In Denial?...Follow Seven Steps for Better DoS and DDoS Protection

In Denial?...Follow Seven Steps for Better DoS and DDoS Protection

Contents

Introduction

Sometimes it's just easier to ignore lingering problems that don't seem to be going away. However, denial and even benign neglect can leave organizations ill prepared to deal with threats. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are often perceived as low-tech nuisances that many security practitioners simply hope to avoid. Unfortunately, hope is not a strategy. The Solutionary Security Engineering Research Team (SERT) is observing more DDoS attacks targeting large and small enterprises, not less. In addition, DoS/DDoS attack capabilities today are more sophisticated, varied and potent. Even with a large attack surface to defend and a continuous arms race against cyber criminals, organizations can't afford to ignore important steps for protecting themselves against DoS/DDoS attacks.

DoS/DDoS attack capabilities today are more sophisticated, varied and potent. Even with a large attack surface to defend and a continuous arms race against cyber criminals, organizations can't afford to ignore important steps for protecting themselves against DoS/DDoS attacks.

DoS/DDoS attacks vary in type and method, so there's no silver bullet for stopping all of them. However, a proactive, layered defense and sound guidelines can help prevent these attacks and minimize their impact. The following seven steps can help to mitigate impact from DoS/DDoS attacks, including:

1. Conduct an enterprise risk assessment.
2. Create an action plan for preparing for, and responding to, DoS/DDoS attacks.
3. Gather information about infrastructure components.
4. Understand ISP options for DoS/DDoS detection and defense.
5. Implement and tune mitigation technology.
6. Review lessons learned after a DoS/DDoS attack.
7. Leverage monitored and managed security services.

Typical DoS/DDoS Attack Scenario

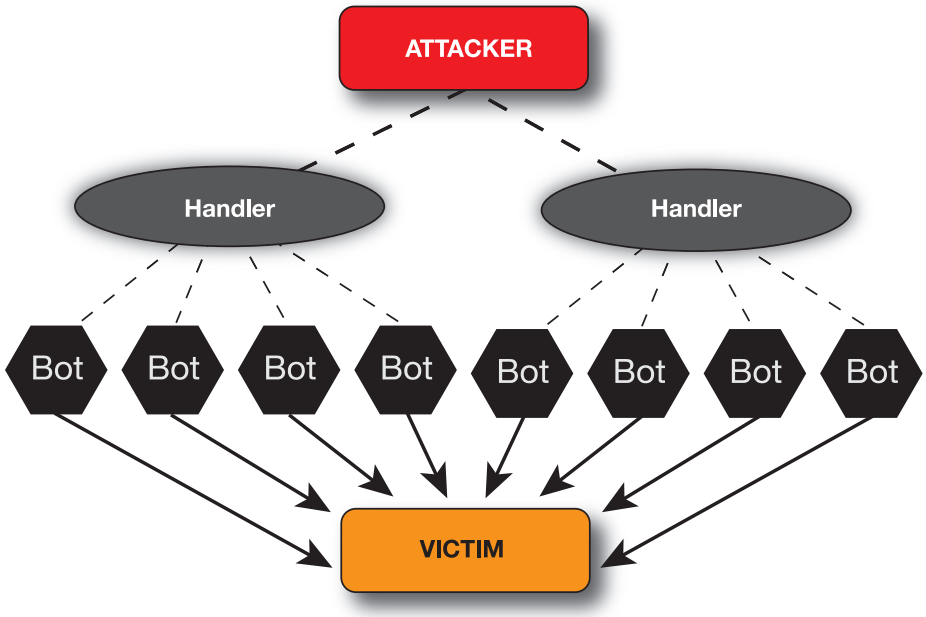
DoS/DDoS have been around for some time. In many cases, they remain successful because organizations have not updated their incident response plans nor tuned their mitigation technologies. These attacks used to primarily consist of high-volume, traffic-flooding techniques targeting service providers. But now techniques are varied, and many enterprises find themselves in the crosshairs for a variety of reasons. A malicious actor could employ a DoS attack as a diversion while going after valuable information in an e-commerce database. DoS/DDoS can also be used to cover up spam

and fraudulent activity, or hold a company hostage by taking out its critical Internet communications. Hacktivist groups in particular are using DoS and DDoS attacks to paralyze, punish and influence targeted victims. These attacks can also disrupt and hamper a company's detection and response to a more covert attack on information or intellectual property. Here is an example of how a typical traffic-flooding DoS attack may be waged against a target:

1. A phishing email or malicious hyperlink directs unsuspecting users to a website where their machines become infected with malware and are placed under the control of a malicious actor.

2. Unbeknownst to the users, the compromised machines (often referred to as bots or zombies) await instructions from the bot controller to attack a target. These bots often remain idle for days or months before they are instructed to attack.

3. At the bot controller's command, the compromised machines launch DoS and/or DDoS attacks against the target, often via UPD ports 53, 80, 443, 514, or TCP ports 80 and 443, 110.



DDoS Attack Architecture

4. The target system or systems are deluged with traffic and subsequently forced offline (targets are usually a Web server or other high profile asset).

Today, DDoS attacks vary in method and presentation. While some DDoS attacks are designed to saturate bandwidth and infrastructure, other categories of DDoS include session-based attacks, simulation replay and amplification. Attackers are using amplification to dramatically increase the traffic volume received by the target, and to deplete the target's resources more quickly. These attacks use Domain Name Server (DNS) spoofed requests and public recursive servers, leveraging innocent bystanders as well as bots.

Some DoS attacks act as slow resource consumers. They do not produce an exceptionally high amount of traffic, but consume resources methodically, making them much harder to detect. In the DoS category, attacks like Slowloris enable a single machine to take down another machine's web server without large amounts of bandwidth or adverse effects on unrelated services and ports. Slowloris sends partial HTTP requests to hold web server connections open. This form of attack is relatively stealthy compared to others that use flooding to overwhelm servers and infrastructure, in that the web server remains inaccessible, but all other services remain intact. It's also particularly effective against thread-based web servers.

The Seven Steps to Bettter DoS/DDoS Protection

Step 1: Conducting an Enterprise Risk Assessment

The first step in any sound defense against DoS and DDoS attacks is to conduct an enterprise risk assessment. This powerful exercise can assess the probability of a DoS/DDoS attack and identify the most likely targets. It will also consider the impact of an attack and estimate the potential loss to the organization, in terms of downtime, damage to reputation, impact on monitoring, communications, forensics costs, connectivity, restoration and other factors. A complete enterprise risk assessment will go beyond addressing only DoS/DDoS threats to considering the organization's entire threat surface and individualized risk. Most importantly, an enterprise risk assessment helps inform IT security investments and risk reduction activity, so security dollars are invested where they will have the most impact.

Step 2: Create an Action Plan

Once under a DoS/DDoS attack, it's too late to determine responses and next steps. Being proactive is the key to preparing against an attacker's next move. An action plan documents how to prepare for a DoS/DDoS attack and how to respond should an attack occur. The action plan must include different strategies and levels of effort based on the intensity of the attack and response warranted. For example, in the case of a successful DDoS attack that takes down the entire company, a powerful action like "drop all inbound traffic to the external Web site" may be recommended while business

functions for the rest of the organization are restored and defense countermeasures are organized. The action plan should identify a chain of command and key areas of responsibility within the organization, and it should be updated and tested on a regular basis.

Step 3: Gather Information about Infrastructure Components

Solutionary security researchers and practitioners find many companies are not fully leveraging capabilities in their current security infrastructure to prevent attacks. It's important to periodically baseline, test and document the protection capabilities available in currently-installed security solutions. Some components of the infrastructure may already have DoS/DDoS prevention capabilities. Organizations can improve defenses and maximize reaction time by identifying the components able to detect, defend and prevent DoS/DDoS attacks—and those with particular vulnerabilities to DoS/DDoS. For example, many network products have capabilities to thwart DoS/DDoS attacks, including routers, web application firewalls and intrusion prevention systems. Ensure those systems are being monitored 24/7.

Many network products have capabilities to thwart DoS/DDoS attacks, including routers, web application firewalls and intrusion prevention systems. Ensure those systems are being monitored 24/7.

Step 4: Understand ISP Options for DoS/DDoS Defense

In line with the enterprise risk assessment and action plan, it's important to establish communication channels and response processes with all parties that could be involved in a DoS/DDoS attack. This especially pertains to the Internet Service Provider (ISP). In some situations, a DDoS attack completely saturates an organization's bandwidth, rendering all other controls ineffective. In preparation for such an outcome, organizations need to establish contacts with their ISP and outline communication processes should ISP intervention become necessary. This information should be clearly documented and easily referenced in case of an attack. If possible, test the plan/processes with the ISP to become more prepared for an attack.

It's also wise to understand the ISP's options for detecting and defending against DoS/DDoS attacks. Does the ISP offer DoS/DDoS protection services? Can the ISP provide proactive and reactive support, and blocking rules to protect against common DoS/DDoS attack vectors? If they do, and it's affordable, purchase these options for added

protection. Make sure that the Service Level Agreement in place with the ISP is well-understood. It would be most unfortunate to discover that the ISP has 24 hours to respond once the organization is under an active DDoS attack.

Step 5: Implement and Tune Mitigation Technology

As discussed in step three, information gathering will help to better implement and tune mitigation technology across the entire infrastructure. Here are a few examples of how to leverage technology and network components for more effective DoS/DDoS detection and prevention:

- Implement appropriate blocking/shunning rules on the IDS/IPS and firewall to address volume-based and packet-based DoS/DDoS attacks. Drop fragmented and non-standard traffic at the Internet router and implement rate limiting threshold triggers.
- Limit traffic by implementing access control lists on border routers. This provides an additional layer of protection to the infrastructure and reduces the traffic handled by firewalls.
- Limit Internet-facing services and protocols. Ensure all services and protocols exposed to the Internet are absolutely necessary and block all others.
- Harden configuration settings for firewalls and routers. Some recent DDoS attacks investigated by Solutionary used known techniques to evade router access controls lists by utilizing fragmented packets in the attack. To limit the effectiveness of attacks using evasive techniques and/or attempting to take advantage of known weaknesses, configure and harden routers and firewalls according to published best practices, such as those provided by the Center for Information Security (CIS) -- http://www.cisecurity.org/.
- Encryption is highly recommended to protect sensitive data while in transit, but can also be helpful to attackers. Improperly implementing SSL termination points can make detection capabilities blind to attacks. Organizations should implement encryption capabilities whenever possible, but consideration for monitoring communications should also be considered.

To limit the effectiveness of attacks using evasive techniques and/or attempting to take advantage of known weaknesses, configure and harden routers and firewalls according to published best practices, such as those provided by the Center for Information Security (CIS) -- http://www.cisecurity.org/.

- Continuously tune security controls so they meet the needs of the infrastructure. It is not efficient to implement and forget; continuous tuning can make a big difference in detection effectiveness.

Step 6: Review Lessons Learned After a DoS/DDoS Attack

Having a plan in place prior to an attack is paramount. But it's equally important to conduct a post-attack debrief in which key participants review the lessons learned and use them to implement changes to the action plan. Most attackers hit a target in waves, so the after-attack review can be critical to improving defenses and reducing the impact of the next attack. The lessons and changes should be documented and implemented as soon as possible. It's a good idea to include the managed security service provider (MSSP), ISP and any other relevant parties in post-attack debriefs.

One of the most simple, yet effective, approaches to a post-attack review is to separate the actions and procedures into the categories, "sustain" and "improve." Organizations can assess the organization's and/or team's communication during a DoS/DDoS attack, the chain of command, the mitigation technology, the hardware and software availability, and more according to the "sustain" and "improve" criteria. "Sustain" refers to practices and actions that worked well, and "improve" covers areas that require some tweaking to be more effective at defending against DoS/DDoS attacks.

Step 7: Leverage Monitored and Managed Services

Partnering with a managed security service provider (MSSP) can provide early warning and critical infrastructure protection from DoS/DDoS attacks. MSSPs have experience dealing with these attacks and can implement emergency actions to minimize their impact. With 24/7 monitoring and management of critical assets, IDS/IPS, web application firewalls, and network firewalls, an MSSP can provide early detection of DoS/DDoS attacks and take immediate steps to mitigate them. A proactive approach and time monitoring can help defend the network 7 days a week, 24 hours a day. An MSSP can also help with the previous steps, including conducting an enterprise risk assessment, creating an action plan, and implementing and monitoring enhanced

Partnering with a managed security service provider (MSSP) can provide early warning and critical infrastructure protection from DoS/DDoS attacks. MSSPs have experience dealing with these attacks and can implement emergency actions to minimize their impact.

security controls in the organization's environment. Leverage the MSSP's expert resources to create a layered DoS/DDoS defense that can help detect and prevent the latest attacks.

If the organization is believed to be a target for DDoS attacks, investigate purpose-built DDoS solutions to meet the specific needs and areas of risk. This can include building relationships with cloud-based security providers to understand the boarding process and how this delivery model may benefit the organization in preventing successful DDoS attacks.

About Solutionary

Solutionary is the leading pure-play managed security services provider. Solutionary reduces the information security and compliance burden, delivering flexible managed security services that align with client goals, enhancing organizations' existing security program, infrastructure and personnel. The company's services are based on experienced security professionals, global threat intelligence from the Solutionary Security Engineering Research Team (SERT) and the patented ActiveGuard service platform. Solutionary works as an extension of clients' internal teams, providing industry-leading customer service, patented technology, thought leadership, years of innovation and proprietary certifications that exceed industry standards. This client focus and dedication to customer service has enabled Solutionary to boast a client retention rate of over 98%. Solutionary provides 24/7 services to mid-market and global, enterprise clients through two security operations centers (SOCs) in North America. For more information, visit www.solutionary.com.

Learn More

To learn more about our SERT research and findings about DoS/DDoS attacks, ways to implement ***the seven steps to better DoS/DDoS protection,*** and Solutionary's capabilities for detecting and preventing these attacks, please contact Solutionary at info@solutionary.com or 866.333.2133.

Contact Solutionary at: info@solutionary.com or 866-333-2133

SOLUTIONARY

Solutionary.com

Solutionary, Inc.

9420 Underwood Ave., 3rd Floor

Omaha, NE 68114