US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Cyber Security Tip
Understanding Distributed-Denial-of-Service Attacks

Overview

One of the most significant cyber threats to businesses, local and federal government agencies is the Distributed-Denial-of-Service attack (DDoS). A Distributed Denial of Service attack (DDoS) occurs when an attacker commands a number of computers to send numerous requests to a target computer. The overwhelming flood of requests to the website or computer network can cause it to shut down or fail to handle the requests of legitimate users, much like a rush hour traffic jam on the freeway. This type of attack can completely disrupt an organization's operations until the network is able to be restored. Understanding the basic concept and methods of a DDoS attack can help operators of both large and small networks mitigate the severity of the attack.

The DDoS Threat

DDoS attacks are easy to carry out and they can often garner widespread media attention, making them a popular tool for anyone wishing to interfere with an organization's web-based and even e-mail services. Attackers often employ "botnets," or networks of compromised computers to use as soldiers in a DDoS attack. Criminal software or "crimeware" has become increasingly available on cyber black markets that can enable a potential adversary to rent a botnet to execute a DDoS attack. Most recently the group Anonymous encourages it's followers to use DDoS software that members can install on their own computers to participate in a DDoS attack, essentially voluntarily participating in cause to disrupt an organizations internet operations.

The goal of a DDoS attack is usually to limit, disrupt, or prevent access to a particular network resource or web service. While the worst case scenario of a DDoS is a failure of the operating system and a crash of the computer system, some common symptoms of a DDoS are:

- A particular web or e-mail resource becoming unavailable
- Slow network performance
- Inability to access some network resources

Best Practices

The best defense for any attack or emergency is to have a plan and this also applies to cyber attacks. A basic understanding of DDoS attack concepts, a list of potential responses and a few key phone numbers will prepare the administrators of even the smallest networks to lessen the damage of a DDoS.

- Assess your organization's risk for a DDoS. If your organization relies heavily on web-based services consider the potential impact to your operations if hit by a DDoS.

- Develop a checklist of actions to take the event of a DDoS and have contact information for your Internet Service Provider ISP and your web hosting providers readily available. If you use a web host for your services, be familiar with their DDoS mitigation polices and plans.

- Be familiar with the services your ISP might offer to mitigate a DDoS such as, temporarily increasing your bandwidth, switching your IP address, and blocking attacking IP addresses.

- Understand your normal amounts of daily network traffic as well as the performance of your system. Many types of DDoS attacks may not actually bring the site down but can significantly reduce service. Properly configured performance monitoring can be a major help in detecting an attack early.

- Separate or compartmentalize critical services:

    - Separate public and private services
    - Separate intranet, extranet, and internet services
    - Create single purpose servers for each service such as HTTP, FTP, and DNS

- Review US-CERT cyber Security Tip Understanding Denial of Service Attacks

Please contact US-CERT at (888) 282-0870 or soc@us-cert.gov if you have any questions.

Document FAQ

What is a TIP? A Technical Information Paper (TIP) is issued for a topic that is more informational in nature, describing an analysis technique, case study, or general cybersecurity issue. Depending on the topic, this product may be published to the public website.

If this document is labeled as UNCLASSIFIED can I distribute it to other people? Yes, this document is intended for broad distribution to individuals and organizations interested in increasing their overall cybersecurity posture.

Can I edit this document to include additional information? This document is not to be edited, changed or modified in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov