Before, during and after a denial of service attack, what should you do?

What to do when the site is subject to denial of service attacks, how to prevent DoS, DDoS, save the site from a denial of service attack? Here are some helpful tips for you.

Hackers have a lot of ways to perform a denial of service attack on targeted targets. If you don't know much about DDoS denial of service and distributed denial of service (DDoS) attacks, please read the article: Learn about DoS and DDoS denial of service attacks

A denial of service attack can occur with any website, at any time, so when you own a website, you should be prepared for psychological and preventive, remedial and preventive measures. they don't fall into a passive position, get the site out of the DoS, DDoS attack quickly.

Before being denied Denial of DoS / DDoS service

- Even if you own a small website, you should have knowledge about DoS / DDoS. If it is an organization, a small group needs at least one person to master this type of attack, technology companies that provide services to small and medium-sized companies or individuals working as IT, an IT group in an organization. The greater the need to have in-depth knowledge of DoS / DDoS, DoS / DDoS types, their attack methods and always know what to do if that happens.

- Establish relationships with Internet service providers (ISPs). This does not mean the relationship with the guy who sells the service to you, but the technical support team. If possible, ask for a meeting with them to discuss how they handle your traffic, what is the 24/7 phone number of the network operating room (NOC), who is responsible in that room? Can they help you if DDoS or other attacks happen?

- Think of Overprovisioning Bandwidth: In general, wider bandwidth for web servers is more beneficial than you think. With overprovisioningbandwidth you can cope with sudden, unexpected changes in traffic, which can be increased by advertising campaigns, a famous person sharing a website or being promoted on media. the media. Try to increase the system's ability as much as possible. Not many organizations have the ability to do this, if you can, feel lucky. After analyzing traffic to the site in a few months, you will know how much capacity your system needs, taking the level of the highest traffic multiplied by 10, if possible to increase to 100 even 500% the better. This is not the method to prevent all DDoS attacks, but it can ensure the hardware can withstand small attacks or give you some time to act before resources are exhausted and the system crashes. to dump.

- Setting up remote monitoring and warning system. We assume that you have a DDoS monitoring tool on your site that can detect and other abnormalities, which is great. But when DDoS is blocked, the links are saturated or your system is offline, unable to send notifications or emails, so how to get a warning? The solution is remote

monitoring. Link the phone to the website's account to receive alerts at all times.

- Hard to update news on technology and security sites such as TipsMake.com, join the famous IT forum to know the large-scale attacks, the spread of malware in the area wide, then plan to prevent it before.

What should DDoS do?

Identify early DDoS attacks

If you are running the server yourself, you need to determine when your system is being denied a service attack. Because the more you know, the sooner you can prevent a better attack. To be able to do this, you should familiarize yourself with the profile of your normal traffic, the more you know about the amount of normal traffic, the easier it is to detect abnormalities of traffic. Most denial-of-service attacks start with a sudden increase in traffic and are useful to distinguish the increase in traffic that comes from legitimate users or attacks. It is a good idea to have a person responsible for handling attacks like this.

Gather information about the attack

You need to know what type of denial of service you are being attacked, the source of specific traffic and systems being targeted.

Enhance Network Perimeter protection

This applies when you run your web server yourself. There are several technical measures that can be taken to mitigate the impact of the attack, especially in the first minutes, and one of them is quite simple. For example, you can:

1. Prevent source IPs (remember to keep all information about these IPs as they may be legitimate, counterfeit or phantom IPs)
2. Set the rate limit on the router to prevent the web server from overflowing
3. Add filters to the router to remove packets from specified attack sources
4. Timeout stronger half-open connections
5. Ignore disfigured or tampered packets
6. Set flood thresholds for SYN, ICMP, and lower UDP

These steps have been effective in the past, but with the increasingly sophisticated DoS / DDoS attack, these actions are much more than just giving you some time to deal.

1. Black Nurse - DDoS technology makes it possible for a normal laptop to take down a server as well

Call your Internet provider or provide a host

The next step is to call your ISP or host provider if you do not operate your web server yourself, tell them you are being attacked and need help. Try to provide as much information as you know. Ask them if they can change their IP address. This is the time to have the relationship mentioned above, call and act as quickly as possible.

Depending on the extent of the attack that the ISP or host provider may have discovered it or they are also beginning to suffer from the attack. The site can tolerate DoS / DDoS better if the web server is placed in large

storage centers instead of running itself. Because their data center has a higher bandwidth link and a better router capacity than your own company or self-running company. Their employees also have a lot of experience to deal with attacks than you.

Depending on the service provider, some ISPs do not have any protection for customers, but many of them have the necessary tools to protect customers. When a customer is attacked they will turn off the site, redirect traffic to "black hole" or block traffic to their network to protect the remaining customers. And the target of the attacker was successful, the site was offline. Then, return the website online, the ISP or host host can redirect traffic to a filter to remove malicious packets before the valid packets are sent to the web server of the site. .

Check the whole system

Continuously check the entire system to ensure the on-going attack is not a misleading arrow to create another attack, or cause more serious problems for affected systems.

What should you do after DoS / DDoS attack?

- Collect all logs during the attack, consider where the traffic is coming from and the type of traffic sent. Work with ISPs to get as much information about the attack as possible. From there determine the location of IP addresses and contact these IP ISPs so they know they have been abused.

- If the attack has serious consequences or signs of crime, contact the police, let them know what happened so they can continue to investigate everything.

- Again check the entire system to make sure everything is operating normally, no parts are compromised.

- Change all passwords.

Hope the article can help you somewhat!