What to do once your device has been compromised with DoS/DDoS

By. Jacob Ibrahim Juma

Collaborator, CyberShield Tanzania inc.

CYBERSHIELD

WHERE AWARENESS UNLOCK SECURITY

What is Denial of service (DOS)

This is the one among the cyber-attacks in which the hacker attempts to make the computer network, services or other IT resources unavailable to the intended users. Thes lead to some one fail to access the web server. It is attempted by flooding the target host with traffic until fail to accept further request, some time force it to shot down and make it unavailable. If multiple devices used to flood the target, then is called Distributed denial of service (DDOS) but if one is kwon as denial of service (DOS).

detecting DDOS/DOS

The best way to detect and identify a DoS attack would be via network traffic monitoring and analysis.

Network traffic can be monitored via a firewall or intrusion detection system. An administrator can set up the network rules to monitor the traffic in the network, so that hi or she can be alerted in case anomalous traffic load is detected, and identify the source of the problem so that to drop network connection to the attacker.

Technically, the process and mechanism vary from one network to device and larger company networks attach prevention method

WHY DoS or DoS

People with different motive can initiate DoS attack to someone device or network due to several reasons not limited to; -

There are various motivations behind launching a Distributed Denial of Service (DDoS) attack on another network, and the reasons can vary based on the attacker's objectives. Some common motivations include:

Financial Gain

Extortion is a common motive behind DDoS attacks. Attackers may demand payment from the target in exchange for stopping the attack.

Competitive Advantage

In some cases, businesses or individuals might launch DDoS attacks against their competitors to disrupt their online services and gain a competitive edge.

Hacktivism

Hacktivists may conduct DDoS attacks to make a political or social statement. They target organizations or websites that they perceive as opposing their beliefs or ideals.

Revenge

Individuals or groups may launch DDoS attacks as a form of revenge against an individual, organization, or community they feel wronged by.

Political Motivations

Nation-states or politically motivated groups may conduct DDoS attacks as a means of cyber warfare, aiming to disrupt the operations of rival nations or organizations.

Distraction for Other Attacks

DDoS attacks are sometimes used as a distraction strategy. While the target is dealing with the DDoS attack, attackers may exploit vulnerabilities in other areas of the network for more serious attacks.

Testing and Demonstrations

Some individuals or groups may launch DDoS attacks to test their hacking skills, demonstrate their capabilities, or simply for the thrill of causing disruption.

Ideological or Personal Reason

Attackers may be motivated by personal beliefs, ideologies, or personal grievances against a particular target.

What is the impact.

On personal life and aspect, Personal Network Impact, a Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack on a personal network can have immediate and disruptive consequences. Users may find themselves unable to access the internet, experience connectivity issues with online services, and face disruptions in communication through email and social media. The attack can overload and render personal devices unresponsive, causing frustration and potential privacy concerns. In some instances, attackers may exploit the situation for financial gain, demanding a ransom from the targeted individual.

For enterprise networks, the impact of DoS or DDoS attacks is more severe, with service disruptions leading to significant downtime for critical systems and applications. This downtime translates into financial losses, productivity declines, and potential damage to the organization's reputation. Customers may lose trust in the business due to extended service interruptions, and there's a risk of data breaches or other cyber threats taking advantage of the chaos caused by the DDoS attack. Organizations may also face increased operational costs related to implementing DDoS protection measures and conducting forensic analyses. Legal consequences and supply chain disruptions further compound the challenges enterprises encounter in the aftermath of such attacks.

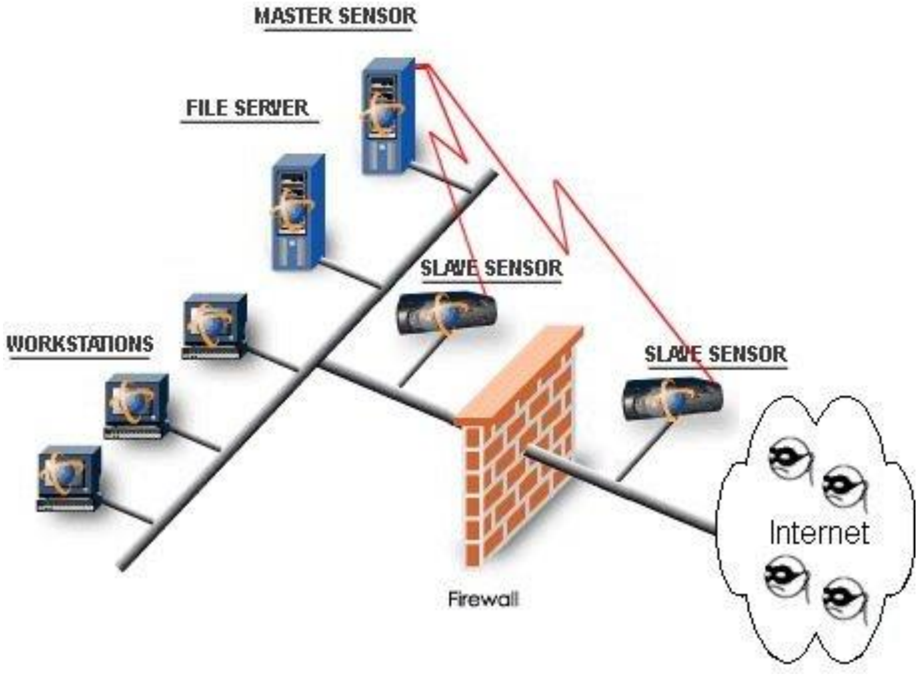
How can do we prevent DDO/DOS

There is no empty room to relax at this situation, but here are several ways that can help you to avoid the incident of such kind.

Preventing DDOS/DOS attack for enterprises network

Firewall and Intrusion Detection System:

Monitor network traffic via a firewall or intrusion detection system. An administrator can set up the network rules to monitor the traffic in the network, so that he or she can be alerted in case anomalous traffic load is detected, and identify the source of the problem so that to drop network connection to the attacker.

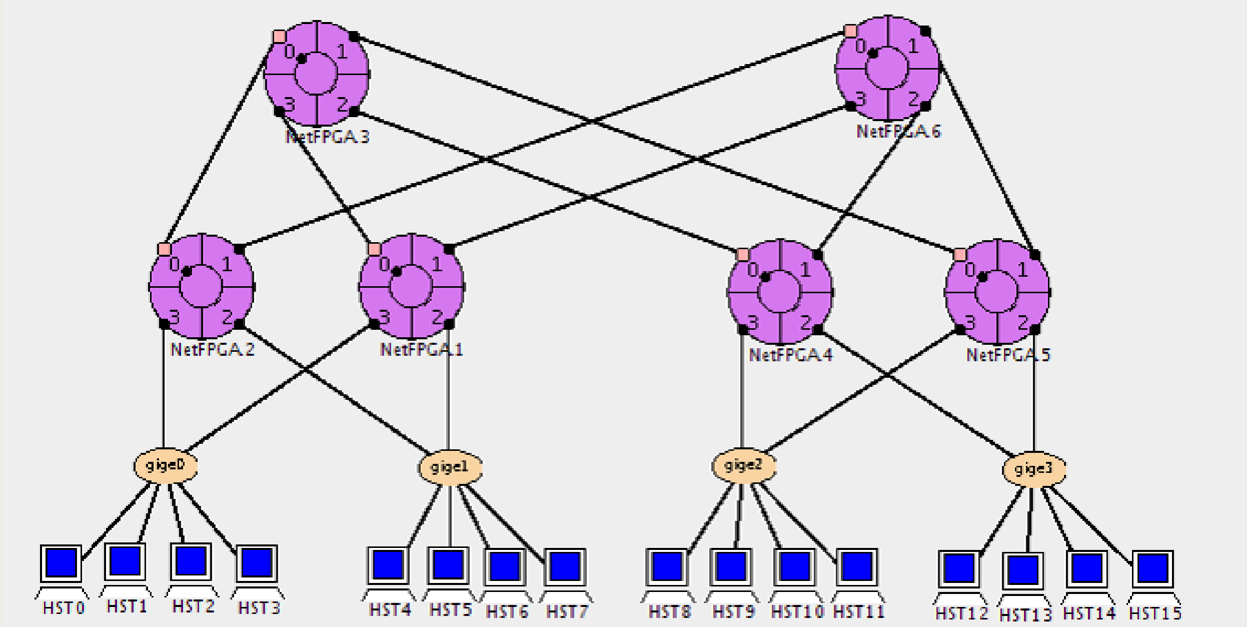


1. **Antivirus software:**

   Installing the antivirus software to detect and prevent malware that can be used to launch denial of service (DOS) attack.

2. **Segmentation**:

   Segment your network into smaller, more manageable pieces, to limit the impact of a DoS attack.



3. **Traffic Distribution**:

   Distribute your traffic across multiple servers, to prevent a single server from being overwhelmed.

4. **Blocking**: Block traffic from known or suspected malicious sources, to prevent DoS traffic from reaching its target.

Preventing personal devices from DDOS/DOS attack.

Below are some specific steps you can take to help protect your Android smartphone from potential DoS attacks:

i. Install a Reliable Security App

Use a reputable antivirus and security app from a trusted provider. These apps can help detect and block malicious activities.

ii. Keep Software Updated

Regularly update your Android operating system and all installed applications to patch vulnerabilities and improve security.

iii. Use a Firewall App

iv. Consider using a firewall app for Android that allows you to control the network traffic going in and out of your device.

v. Be Cautious with Apps

Only download apps from official app stores, such as Google Play. Avoid sideloading apps from untrusted sources, as they may contain malicious code.

vi. Review App Permissions

vii. Review the permissions requested by apps before installing them. Avoid granting unnecessary permissions that could potentially be exploited in an attack.

viii. Enable Do Not Disturb Mode

Use the Do Not Disturb mode to silence notifications and reduce the impact of continuous alerts that may accompany a DoS attack.

ix. Limit Background Processes

In your device settings, limit the number of background processes and apps running in the background to conserve resources and reduce the impact of a potential attack.

x. Use a VPN. Consider using a Virtual Private Network (VPN) to encrypt your internet connection and protect against certain types of attacks.

xi. Stay Informed

Stay informed about the latest security threats and best practices for mobile security. Follow security updates from Android and your device manufacturer Connect to Secure Wi-Fi Network

xii. Avoid connecting to unsecured Wi-Fi networks. Use encrypted Wi-Fi connections, and consider using a VPN when connecting to public Wi-Fi.

xiii. Enable Google Play Protect. Ensure that Google Play Protect is enabled. This feature scans apps for malware and helps keep your device secure.

What can I do if my device has been compromised with DDOS/DOS

If your device has been compromised with a DDoS attack, it is important to take immediate action to prevent further damage. Here are some steps you can take:

1. **Disconnect from the Network**: Disconnect your device from the network to prevent the attacker from continuing the attack.

2. **Contact Your ISP**: Contact your Internet Service Provider (ISP) to report the attack and seek assistance.

3. **Configure Your Server**: Configure your server to limit the number of requests at a given time

Get FREE security tips and tools

There's a wide range of FREE CyberShield tools that can help you to stay safe – on PC, Mac, iPhone, iPad & Android devices, take time to use them in adherence to available regulations. Sign up for our weekly journal here

We're Here to Help

Helping you stay safe is what we're about – so, if you need to contact us, get answers to some FAQs or access our technical support team. Feel free to reach us

CyberShield Tanzania inc.

Email: info@cybershield.ac.tz

Contact: +255-228696953

Dar es salaam Tanzania.