gosafeonline
A monthly infocomm security newsletter

Monthly Newsletter – Issue No. 2012-12

Denial of Service

Denial of Service (DoS) attack refers to the attempt to prevent the availability of computer information or services to its intended users. An attacker is able to prevent you from accessing email, websites, online accounts (banking, etc) or any other services. In some cases, a DoS attack forces websites accessed by millions of people to cease operation and cost the targeted person or company time and money. The most common way to perform a DoS attack is when an attacker "floods" a network or server with as many request and data as possible.

When you access a particular website through your browser, you are sending a request to the website's server to transmit data to your computer. As the server can only process a limited number of requests at a time, your request will not be processed in the event that an attacker sends a very large amount of requests to the server concurrently, beyond what the server can handle. This is known as DoS.

An attacker is also able to utilize spam email messages to perform a similar attack on your email account. Our corporate or personal email accounts are usually allocated with a fixed storage quota. If an attacker floods our email inbox with many spam email messages or email messages with huge attachments, our available storage space would be used up and we would be denied from receiving legitimate messages.

Distributed Denial of Service (DDoS) attack on the other hand, is launched by an attacker through the use of an army of computers to attack the victim computer or server, to deny them in providing resources or services to its intended users. The attack is "distributed" because it utilises multiple computers, including yours, to perform the denial of service. To perform a DDoS attack, the tactic of botnet or a collection of inter-connected computers is most often used.

Botnets or zombies are computers that are remotely controlled by an attacker stealthily, as their security defenses have been breached. Computers that do not have the appropriate security measures such as anti-virus software or firewall in place are common victims of botnet. The attacker is able to control your computer in sending huge amount of request and data to a particular website or email address once it is compromised.

DDoS is a popular attack method since numerous machines produce more attack traffic as compared to a single machine, and thousands of attacking machines are more difficult to trace and turn off. Identifying a DoS or DDoS attack is not easy as users often confuse attacks with usual technical problems with the network or systems maintenance delays.

Symptoms of Botnet / Zombie Computers

The symptoms of computers that have been compromised to serve as a botnet or zombie in a DoS/DDoS attack are very similar to other malware infection. A user may detect if a computer is infected with malware by looking out for the following symptoms:

- Unusually slow network performance (opening files or accessing websites)
- Unavailability of a particular website
- Inability to access any website
- Dramatic increase in the number of spam emails sent and received

Recovering from an attack

IN the unfortunate event that your computer has been compromised and became a zombie or you suspect that you or your organization is targeted by a DoS/DDoS attack, apart from contacting SingCERT to report the incident and for further advice, you may use the following steps to recover from a DoS/DDoS attack

1. **Backup Your Computer:** Save your important files, applications and data on a DVD, CD or clean external hard drive.

2. **Turn Off All Networks:** Unplug all network cable connections from your computer and turn off the Wi-Fi. If you are using a laptop, use the Wi-Fi switch to turn off the Wi-Fi as the hacker's malware may show you that the connection is off when it is still connected.

3. **Format Computer And Reinstall Operating System:** Format your computer and reinstall your operating system using your original OS disks. Be sure to download all updates and patches after installation.

4. **Reinstall Antivirus, Antispyware, And Other Security Software Prior To Any Other Programs:** Install and update all security related software. Ensure that your software is up to date before loading other applications containing malware that might go undetected if your virus signatures are not current.

5. **Run Scans:** Run antivirus, antispyware, and antirootkit scanners on your computer to detect and remove any malware residing in your computer.

6. **Scan Your Data Backup Disks And Copy Them Back To Your Computer:** Scan your data files before copying them back to your computer.

Tips to Mitigate DoS or DDoS attack

1 Install and Maintain Antivirus Software	✓ Installing an antivirus software and configure automatic update of the latest virus definitions helps to detect and remove the malware from your computer, thereby preventing it from becoming a zombie.
2 Install and Configure Network Protection	✓ Firewall: Limit the type of traffic that can pass through and filter out unwanted content or suspicious traffic.
3 Follow Good Security Practices for Distributing Email Address and Apply Email Filters	✓ Don't give your email address out arbitrarily. ✓ Use filters to block certain addresses or to only allow email from addresses on your contact list. ✓ Don't follow links in spam messages. ✓ Disable automatic downloading of graphics in HTML mail as many spammers send HTML email with a linked graphic file to track recipients who had viewed the email message. ✓ Use privacy settings on social networking sites to restrict the viewing of your email address.

Interesting Reads

- Denial of Service Attacks:
  http://www.cert.org/tech\-tips/denial_of_service.html
- Botnet:
  http://en.wikipedia.org/wiki/Botnet
- What to do in a Denial of Service attack:
  http://netsecurity.about.com/od/disasterrecovery/a/I-Ve-Been-Hacked-Now-What.htm
- Firewall, IDS and IPS:
  http://www.securitywizardry.com/index.php/products/ids-and-ips.html

www.gosafeonline.sg

www.facebook.com/gosafeonline

Published by: iDA SINGAPORE

A member of: GOsafeonline.sg Cyber Security Awareness Alliance

In the next issue...

Learn about the use of one time pin (OTP) for two factor authentication (2FA).

Let us know what you like about this newsletter and what we can do to better serve your infocomm security awareness needs.

If you have any enquiries or feedback for our newsletter, do write to us at contact_us@gosafeonline.sg.

BE AWARE, RESPONSIBLE AND SECURE!