Zombies and Botnets

What is a Zombie?

Zombie computer (Zombie or Bot) is a computer connected to the Internet that has been compromised and controlled by an attacker without user's consent.

What is a botnet?

Zombie network (Botnet) refers to a network of zombie computers under the remote control by an attacker. Attackers control their botnets through some command and control centres to perform illegal activities.

How to become a zombie?

Under what circumstances may your computer become a zombie?

If your computer is infected by malicious code such as Trojan Horse, your computer may be controlled by an attacker and may become a zombie.

Symptoms of Infection

When a computer becomes a zombie, the following symptoms will probably appear: Computer can be operated properly and the computer does not hang. The processing speed of computer will slow down, the network usage will increase, unknown files will appear on the computer or unknown programs will be executed.

Potential Security Threats & Impacts

An attacker usually controls the zombies in a botnet remotely and secretly to steal data from the zombies, and to perform malicious activities in the Internet including:

- Sending spam emails

- Attacking other computers and servers

Attackers can control thousands of zombies in a botnet and perform massive attack to the same target at the same time, which can make the system hang and trigger a Denial of Service (DoS). Botnet is a severe threat to both network security and data protection of user.

General Preventive Measures

To prevent your computer from becoming a zombie, you should:

- Pay attention to the security measures of using the Internet, for example:
  - Do not open or reply to a suspicious email or email from an unknown source. Delete it immediately.
  - Pay attention when opening email attachments.
  - Do not visit suspicious websites, follow their links and download files or software from these websites.
- If you discover any abnormal behavior on your computer, it means that your computer may have already been infected by malicious code or have already become a zombie.
- Please disconnect the computer from the network, check and scan the computer with anti-virus software immediately.
- Furthermore, you must apply basic security measures on your computer, including installing anti-malicious code software (such as anti-virus software), firewall and latest security patches, scheduling a weekly full scan and enabling the Auto Update feature of relevant software.

It is difficult to detect botnets since zombies are widely distributed. Internet Service Providers, Multi-national Law Enforcement Agencies or Computer Emergency Response Teams should work together to find out the hidden attackers.

To learn more about information security, please visit the InfoSec website at: http://www.infosec.gov.hk