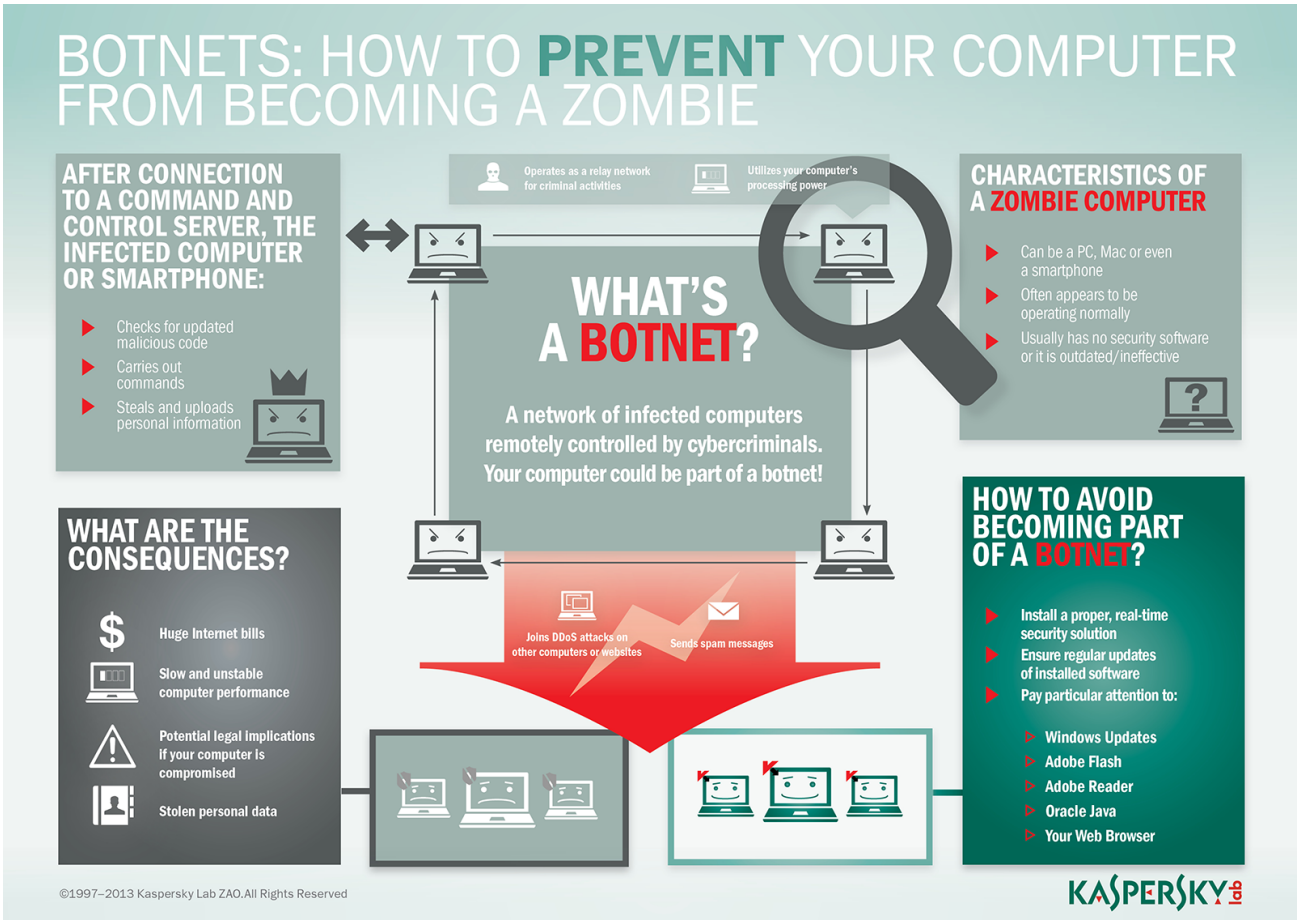
What is a Botnet?



The word Botnet is formed from the words ‘robot’ and ‘network’. Cybercriminals use special Trojan viruses to breach the security of several users’ computers, take control of each computer and organise all of the infected machines into a network of ‘bots’ that the criminal can remotely manage.

How Botnets can impact you

Often, the cybercriminal will seek to infect and control thousands, tens of thousands or even millions of computers – so that the cybercriminal can act as the master of a large ‘zombie network’ – or ‘bot-network’ – that is capable of delivering a Distributed Denial of Service (DDoS) attack, a large-scale spam campaign or other types of cyberattack.

In some cases, cybercriminals will establish a large network of zombie machines and then sell access to the zombie network to other criminals – either on a rental basis or as an outright sale. Spammers may rent or buy a network in order to operate a large-scale spam campaign.

How to prevent your computer becoming part of a Botnet

Installing effective anti-malware software will help to protect your computer against Trojans and other threats.

Kaspersky Lab has award-winning anti-malware solutions for:

- Windows PCs
- Apple Macs
- Linux computers