6 ways to combat botnets

Botnet is a growing threat in today's Internet world, but we have many ways to deal with it. In this article, TipsMake.com will show you 6 ways

Botnet is a growing threat, but we have many ways to deal with it. In this article, TipsMake.com will show you 6 quite professional ways to fight back botnets.

Hire a Web filtering service

Web filtering service is one of the best ways to fight bots. These services scan websites when they see unusual behavior or dangerous code actions and block that site from users.

Websense, Cyveillance and FaceTime Communications are typical examples. All will check the Internet in real time to find websites that are suspected of dangerous actions such as downloading JavaScript and other scams outside the boundaries of normal web browsing. Cyveillance and Support Intelligence also provide services that tell about website organizations and detected ISPs that have malware, so hacked servers can be repaired in time.

Convert browser

Another way to prevent bot intrusion is to not use a browser. Internet Explorer or Mozilla Firefox are the two most popular browsers and so are also the browsers that the malware focuses on. The same is true for operating systems. According to statistics, Macs are safe botnet operating systems because most of them are aimed at Windows.

Disable scripts

Another way is to disable the browser from general scripts (scripts), which can make it difficult for some employees to use custom and web-based applications in their work.

Deployment of intrusion detection and intrusion prevention systems

Another method is to adjust IDS and ISPs so that they can find activities similar to botnets. For example, a computer that suddenly encounters a problem with Internet Relay Chat is completely suspicious. Just like connecting to remote IP addresses or unreasonable DNS addresses. While this problem is difficult to detect, we have another way of discovering when an unexpected attraction is detected in SSL traffic on a computer, especially in unusual ports. That may be the channel that the botnet has hijacked.

Therefore, we need an ISP to check for unusual behavior to instruct HTTP-based attack alerts and remote call procedures, Telnet- and protocol spoofing address solutions, attacks. Other public. However, we should note that many ISP sensors use signature-based detection, which means that attacks are only added to the database when they are detected. Therefore ISPs must update in time to recognize these attacks, otherwise the detection will be invalid.

Content protection created by users

Your own website activities must also be protected to avoid being unintentional accomplices to malware writers. Public blogs and corporate forums should be restricted to text only.

If your site is needed for file exchange members, it must be set up to allow file types to be limited and secure, for example with files with .jpeg or .mp3 extensions. (However, malware writers have started targeting MP3 players).

Use software tools

If you find that the computer is infected, the system has no best way to deal with this situation. You don't have to fear that because companies like Symantec confirm that they can detect and wipe out the most dangerous rootkit infection. The company has launched a new technology in Veritas, VxMS (Veritas Mapping Service, Veritas Mapping Service), offering an anti-virus scanner that bypasses the Windows File System API, which is controlled by the operating system. caused a vulnerability by a rootkit. VxMS directly accesses raw files of Windows NT File System. In addition, other antivirus software companies that are trying to combat this rootkit include McAfee and FSecure.