Docket #: S06-260

Host-Based Detection of Remotely Controlled Malware

Stanford researchers have patented a method for detecting malicious bots, programs that are installed as viruses on a computer and then proceed to execute malicious commands from another remote computer. Using bot behavioral characteristics, the method identifies a wide range of known or previously unknown malicious software and then prevents it from carrying out commands. The method analyzes process behavior in real time in order to detect bot activity; it overcomes shortfalls and can detect, eliminate, and prevent bots from executing commands - without previous knowledge of any specific malicious software, and without a need for identifying and characterizing the software. Furthermore, this invention produces very low false positives and it will not interfere with beneficial programs. This improved detection software is very valuable to both corporations and individuals, and should greatly help to prevent spamming, denial of service attacks against websites, and identity theft, which are commonly carried out by bot networks.

Stage of Development - Prototype

Applications

- **Malware detection** for:
  - Personal and business computers
  - Networked computers (specifically at universities and corporations)

Advantages

- **More effective**:
  - Not vulnerable to syntactic or semantic differences in an executable that enables bot variants to evade signature-based methods.

    - Detects malware using generic bot behaviors that do not change from one bot to another – **does not require malware list** or analysis of previously identified and captured malware.
    - Extremely **low false positives** for tested innocuous programs
- **User transparent** – does not interfere with user experience or system performance, nor require significant system resources.
- **Helps prevent: spamming, denial of service attacks** against websites, and **identity theft**

Publications

- Mitchell, John C., and Elizabeth A. Stinson. "Detection of malicious programs." U.S. Patent 7,870,610, issued January 11, 2011.
- Stinson, Liz, and John Mitchell. "Host-based, run-time win32 bot detection." RO-DARPA-DHS Special Workshop on Botnets, 2006.
- Stinson, Elizabeth, and John C. Mitchell. "Characterizing bots' remote control behavior." In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pp. 89-108. Springer, Berlin, Heidelberg, 2007.

Innovators

- John Mitchell
- Elizabeth Stinson

Licensing Contact

Imelda Oropeza

Senior Licensing Manager, Physcial Sciences

Email