



Powerful Automated Malware Analysis

Your Weapon: Sunbelt CWSandbox

Rapidly analyze behavior of malware - including infected trojans, Office documents, browser helper objects (BHOs), malicious URLs and more - by executing the code inside a controlled environment!

In today's security landscape, malicious applications are rampant across the Internet and are distributed via Windows exploits, email, questionable or compromised websites, and more. In order for security vendors and enterprise service providers to better thwart these malicious threats, the thorough analysis of malware applications is essential in developing signatures that prevent these applications from installing on end user machines.

Analyzing these malicious applications can be done in different ways, and a key method for countering malware is to study their behavior (dynamic analysis) - how the applications are executed, what system changes are made, what network traffic is generated and the severity level of the threat - all in a safe and controlled environment. Sunbelt CWSandbox provides the leading tool on the market for this dynamic analysis. This revolutionary tool allows researchers to analyze the behavior of suspected viruses, trojans and other malware by executing the code inside a controlled environment then recording what Windows API calls it makes.

Further, anything from infected Office documents to malicious URLs and Flash ads can be analyzed by creating the appropriate Windows sandbox environment.

A fraction of the time of conventional research

With Sunbelt CWSandbox, the automatic analysis and classification of malware samples is conducted in a fraction of the time of conventional research. This research automation enables technology

providers to build malware signatures more quickly and bring them to market faster. Additionally it gives enterprise service and security providers the ability to proactively protect against current and evolving malware threats that may present risks to their customers and end users.

How CWSandbox Works

Using automated behavior analysis, CWSandbox leverages unique technology for the automatic behavior analysis of malware. CWSandbox provides fast and autonomous analysis

of large volumes of malware samples in a short period of time. It can facilitate the automatic collection of malware from different inputs including Nepenthes (a tool for automated collection of autonomously-spreading malware), a web server/interface, or a directory. Once malware is dropped into the database, the sandbox can then execute analysis and monitoring. When enough information about the malware is collected, the CWSandbox terminates the malware application and analyzes the collected data.

