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.

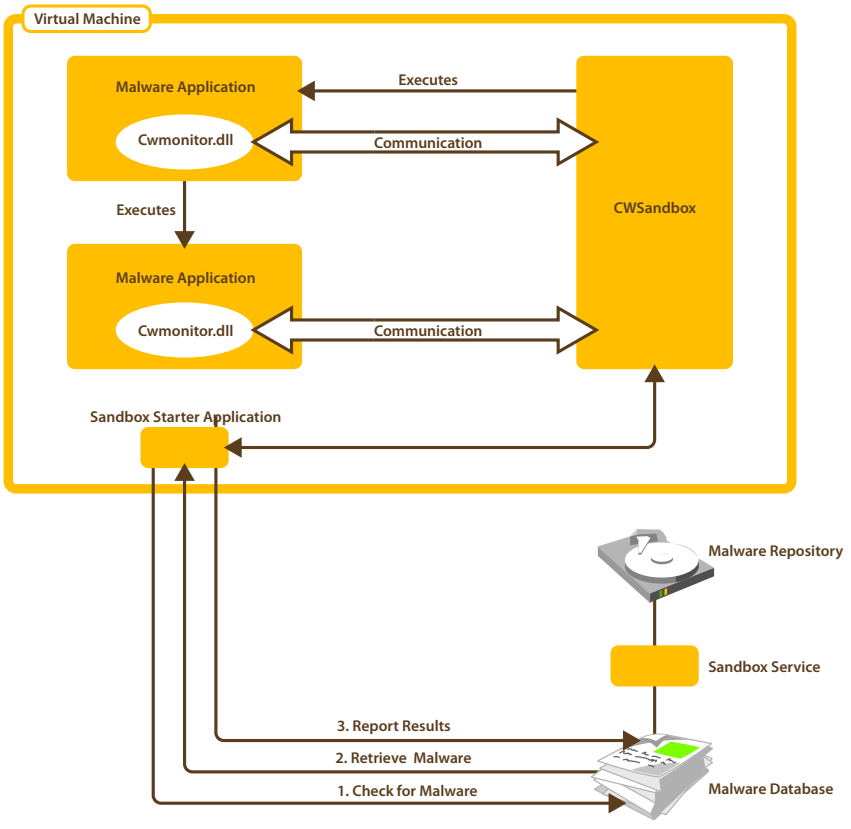
Further, anything from infected Office documents to malicious URLs and Flash ads can be analyzed by creating the appropriate Windows sandbox environment.

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.



Sunbelt Software

Monitoring

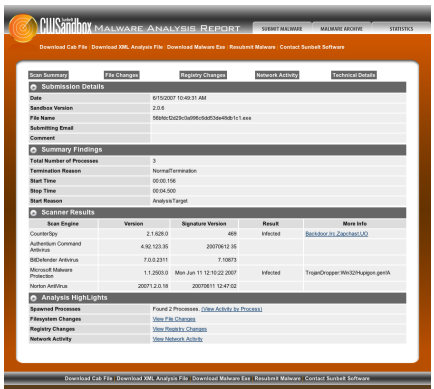
In Windows, nearly all accesses to the system resources are done via the Windows API. The API offers functions to access the file system and the registry, to execute other applications or to install, start or stop Windows services. It also offers the WinSock functions, which are normally used to communicate via TCP/IP-networks, such as the Internet. The API is implemented by different DLLs, located in the Windows system directory.

Because CWSandbox injects code to monitor behavior much like malware injects code into the systems it infects, many malware applications can detect processes that are trying to shut it down. CWSandbox has been hardened to minimize detection so that malware doesn't recognize it is being monitored.

CWSandbox monitors the Windows system resources including the file system, registry and other applications with special attention to communication resources. CWSandbox logs and reports in extensive detail any network activity and HTTP, FTP, SMTP and IRC connections.

Analysis and Reporting

After monitoring is complete, CWSandbox performs a granular analysis to provide better readability of the data collected. The analysis captures resource events which include API calls, WinSock, packets, and more. Reports on the results of the analysis are XML files and can be automatically parsed with XSL templates to generate HTML or text reports. The reports provide information on the list of newly created files and registry entries, as well as any processes that were launched by the malware application. The reports can be emailed automatically to the submitter or administrator, stored in the database or presented in the web interface.



CWSandbox reports granular analysis of malware data

CWSandbox not only analyzes the given malware, but also all other processes that are started or infected by the malware. For example: a lot of malware creates a thread in the context of the Windows Explorer and then performs its malicious functions from within Windows Explorer, Word and other Office applications, or an Office document as the infection vector. These functions are provided for additional analysis in these scenarios:

- CWSandbox can optionally store all the files that are created by the malware, such as regular files, temporary files, or those downloaded from the Internet.
- CWSandbox can additionally create a "dump" file for each analyzed process for further investigation.
- External debuggers can be linked in for memory dumps and the results integrated in the reports. By the same fashion, command line antivirus scanners, third party packet capture tools and more can be linked and integrated.

See CWSandbox in Action

To see how the CWSandbox technology works, simply visit www.sunbeltsandbox.com to upload malware samples and receive the analysis results in minutes.*

For more information on how you can leverage the Sunbelt CWSandbox technology for your organization's research efforts, please contact Sunbelt Business Development at oemsales@sunbeltsoftware.com or call 888-688-8457 x 650.

Highlights

- **Automated installer emulates user interaction with malware applications**
- **Sophisticated scripting and automatic file associations**
- **Supports analysis of:**
  - **Trojans**
  - **Rootkit installers**
  - **Bots**
  - **Infected Office documents**
  - **Browser Helper Objects (BHOs)**
  - **Browsing specified URLs**
  - **And more**
- **Multiple OS support, including Vista**
- **Integrates with a variety of scanners and debuggers**
- **Includes several powerful add-on utilities:**
  - **Sunbelt command-line malware scanner**
  - **Packet capture utility**
  - **Sunbelt PE analyzer**
- **Optional Threat Track data feeds from our Threat Center**

Technical Specifications

CWSandbox has been tested on Windows 2000/2003 and Windows XP. Running it on other operating systems may require modifications. Contact us for more details.

- **Supported Databases: MySQL, MS SQL**
- **VMWare is supported for running CWSandbox instances on a single machine or cluster**
- **Recommended minimum hardware configuration: Xeon 3+Ghz CPU, 2+Gig RAM**
- **Recommended options: Sunbelt Personal Firewall per instance for terminating potential outbound malware traffic**

  Faronics Deep Freeze Enterprise for restoring "clean" images

**Due to heavy load the public site does not support: URL or BHO analysis, zipped files, or analysis of infected documents. Please contact us directly for sample analysis of files other than Win32 PE (portable executable) format.*

33 N. Garden Ave., Suite 1200, Clearwater, FL 33755 | Tel: 1-888-688-8457 or 727-562-0101 | Fax: 727-562-5199 | www.sunbeltsoftware.com | Email: oemsales@sunbeltsoftware.com