AntiHook SDK 3.0 Feature List

Document version 1.1, 9 Mar. 06

Please Note: This document is "pre-release". It lists the expected features of the released software, but the actual features in the final release may be subject to change without notice.

AntiHook SDK 3.0 is a highly functional security software product based on kernel mode protection that controls what software is running on a user's machine.

AntiHook detects and prevents attacks in real-time.

The AntiHook solution is unique - it does not rely on lists of known Malware, so no updates are required and no connection to a server or the internet is required either - the protection is virtually built into the operating system.

AntiHook SDK 3.0 offers the following features:

Feature	Description
Trusted baseline with core Windows operating system.	AntiHook eliminates any race with Rootkits and Malware that have been installed before or after AntiHook as it takes a unique approach to retrieve and compute the core OS function entry points that might be compromised. AntiHook establishes a static trusted baseline with the operating system kernel. This technique ensures that all filters installed by AntiHook are called first before any other filters. AntiHook is therefore more advanced in this area compared to other anti-spyware products. AntiHook provides an effective defence that ensures that AntiHook will "get there first" even in the event a hidden Rootkit is already installed on the machine.
Self-protection and Self-recovery.	AntiHook can detect and block Rootkits and Malware which are attempting to disable AntiHook or to modify Windows System Service Dispatch table or other Windows structures. It blocks malicious applications attempting to unload or stop the AntiHook SDK driver and service…it protects itself! In addition to this AntiHook implements a sophisticated mechanism for recovering critical system structures that have been modified.
Starting of applications and programs.	This feature allows the framework to put restrictions on what applications execute on a user's machine.
Terminating and Suspending of critical security applications.	An important feature that keeps the integrity of the operating system by protecting critical security applications (e.g. Firewall, Anti-virus, and Anti-spyware software) from being terminated or disabled.
Blocks hiding of critical OS components.	The key point of hiding a process is that it allows an attacker to create an undetectable backdoor that cannot be discovered using standard process tools like Process Explorer or Windows Task Manager or even Anti-rootkit software. For example the Hacker Defender rootkit installs hidden backdoors, registers as a hidden system service and installs a hidden system driver. AntiHook can detect and block hiding of operating system critical components such as processes, drivers and DLL's.
Stop attacks intended to modify processes.	Malicious software can execute code in a remote program and perform remote injection of code through standard Win32 API or other native APIs called from within Rootkits or other malicious programs. AntiHook provides protection against this. Here are some of the areas of the process modification monitoring functionality:

Feature	Description
	• reading/writing to process memory • reading/modifying process module information • creating remote threads • opening and manipulating thread handles • attaching a debugger to processes • suspending the execution of a thread in an external process • setting the execution context of a thread in an external process
Ability to detect and block kernel and user land Rootkits.	All the rootkits referred from www.rootkit.com are detected and blocked. If AntiHook SDK driver is installed after a rootkit it still allows the detection of the rootkit.
Service/driver installation.	AntiHook detects the installation of kernel mode Rootkits that integrate and then maliciously alter the Windows operating system.
User mode hooking by modifying IAT or EAT.	AntiHook can detect and stop user mode IAT/EAT hooking.
Start-up applications and DLL's	AntiHook can detect the registration of programs and DLLs for loading on PC start-up or when the user logs on to the system.
System-wide Windows Hooks	Malicious software can install system-wide Windows hooks by using standard Win32 APIs or native APIs. AntiHook can detect and prevent this by monitoring if software attempts to hook SetWindowsHookEx, NtUserSetWindowsHookEx or all related API's.
Registry modifications	AntiHook can protect a user's machine by detecting and stopping applications which are attempting to modify critical registry settings. Registry keys to be monitored are configurable and can be changed by client dynamically. Read/Write/Delete filters are configurable via the SDK API.
Attaching a debugger to another process.	AntiHook can detect and prevent a debugger being attached to a process. This solution can protect the user's machine from any sort of "debugging related" attacks.
Event Logging	Full logging functionality is provided, facilitating consistent logging and instrumentation practices, both within an application and across the enterprise. The AntiHook SDK integrates with the MS Enterprise Library's Logging Application Block as well as SQL databases.
No reboot is required when the Framework is installed on the end-user machine	It is not necessary to reboot the client PC after installation and at the same time no functionality of AntiHook is compromised.
No freezing behaviour	Timeout/default behaviour is implemented for the cases when the caller of the SDK doesn't return from the event handler/callback or the monitored process locks up.
Pre-execution and post-execution processing handlers to modify system behaviour.	When a callback is registered then the AntiHook SDK provides the ability to alter any Win32 API / Native API argument or return value before returning control to the application. For example the SDK client can change the value of the CreateProcess function to return an error. A client security application could subscribe to AntiHook SDK service to handle a set of events the framework fires each time when something happens in the operating system. All events are blocking, therefore until the event handler returns execution flow the interrupted application is suspended. In addition to this, "**timeout based**" behaviour allows the framework to abort "**long running callbacks**". AntiHook SDK implementation is multithreaded so multiple events can be fired to client applications.

AntiHook SDK 3.0 can be also used to isolate malicious activity and "fix" the behaviour of already infected machines.

AntiHook SDK 3.0 addresses significant problems not being solved by AV/Anti-Spyware and Firewall software.

It allows less-than-security-savvy users who visit all types of Web sites and run any downloaded program to keep working without exposing their home or corporate PC to serious risks.

AntiHook SDK 3.0 offers several levels of security protection targeting different end-users with different technical backgrounds:

Security Mode	Description
Advanced mode	Allows an experienced user/administrator to customise the behaviour of the operating system, fine tune what software should be allowed and what should be blocked.
High Security	This is an option blocks all undefined events and can be used in high risk environments and un-trusted user environments.
Low Risk Friendly Environment	When running in this mode, AntiHook performs its validation for all existing rules and allows anything that hasn't been defined. Typically this can be used in highly trusted environments.
Custom	A combination of High Security mode and Low Risk Friendly Environment mode that allows an administrator to specify high security or low risk mode for specific processes/applications. For example AntiHook can run in High Security mode for Skype/IE/IM/Google Desktop etc. and in the same time run in Low Risk mode for Sygate, Zone Alarm, Norton Security, and others.
Allow all	This is a just simple pass-through mode that records all events that occurred on the system.

AntiHook SDK 3.0 provides a user friendly event monitoring system by logging all suspicious events to a file or SQL database.

The Enterprise version of the product allows system administrators to train the system, define custom rules, and maintain users and groups using Advanced Management Tool.

For more information please contact InfoProcess at info@infoprocess.com.au