

Hypersight Rootkit Detector

A New-Generation Rootkit Detector

North Security Labs

www.northsecuritylabs.com

Introduction

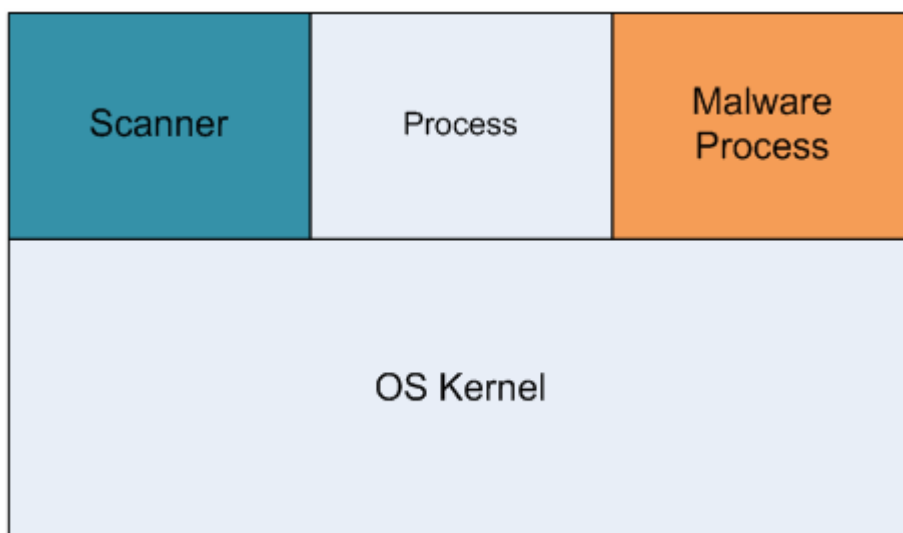
Highly sophisticated rootkit technologies are making it into malicious software more and more over time. Rootkit technology allows hiding malware on a PC from legitimate users and antivirus scanners. As a technology, rootkits are not malicious, yet they are frequently used to block malware from being detected. The rootkits are quite complex to develop, but they are gaining popularity among the hackers who implement rootkit technologies in their viruses, Trojan horses, spam bots, spyware and so on.

Detecting rootkits is not easy. There were no universal solutions up until now to reliably detect kernel-mode rootkits. All current security products fail to detect and combat the newest rootkits.

Types of Information Security Systems

There are several types of information security systems. The different types are not carved in stone, and there are many systems that combine two or more types in one product.

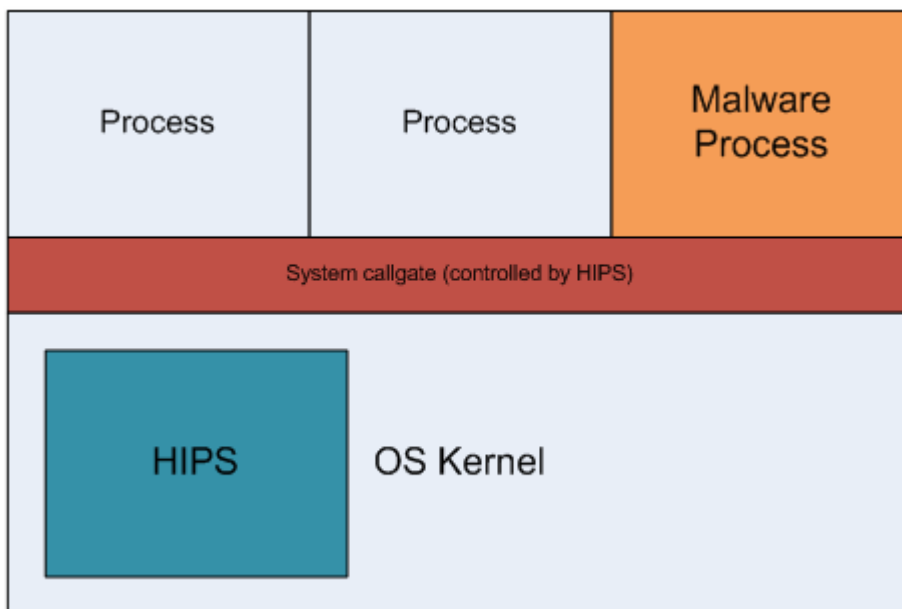
1. Signature Scanners.



This type defines classic antivirus programs. The antiviruses analyze executable code in the computer's memory and on the hard disks in an attempt to identify malicious software using pre-defined code sequences, signatures, checksums, or by using heuristics. These systems were the first to

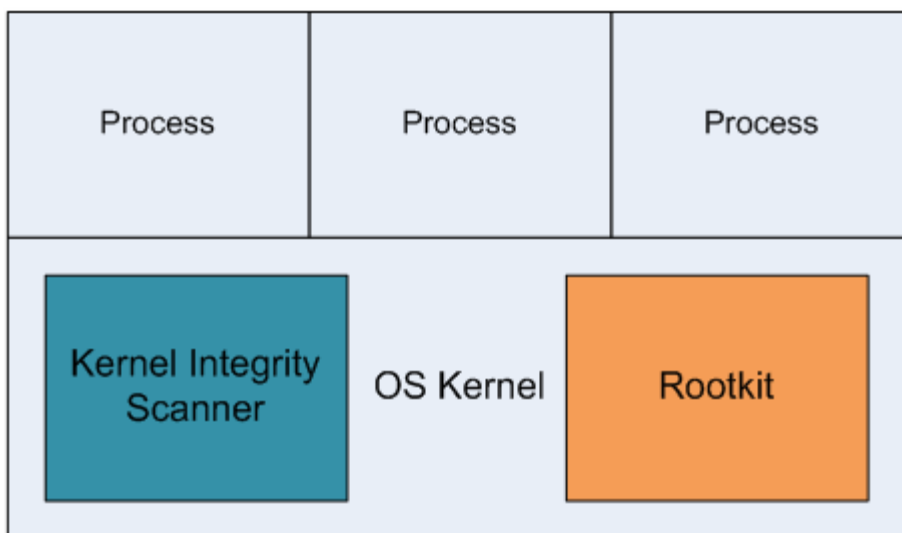
emerge in the early days of computers. Unfortunately, these systems are completely helpless against even basic rootkits as the latter use masking techniques that are designed specifically to defeat antiviruses.

2. Host Intrusion Prevention Systems, HIPS.



HIPS systems are a type of anti-rootkit blocking solutions. HIPS reside in the system kernel, blocking malicious actions of lower-privileged user-mode processes. These anti-rootkits are effective against user-mode rootkits that are already installed. They can also prevent installation of a kernel-mode rootkit. Unfortunately, HIPS cannot help against kernel-mode rootkits that are already running in the system.

3. Kernel Integrity Scanners.

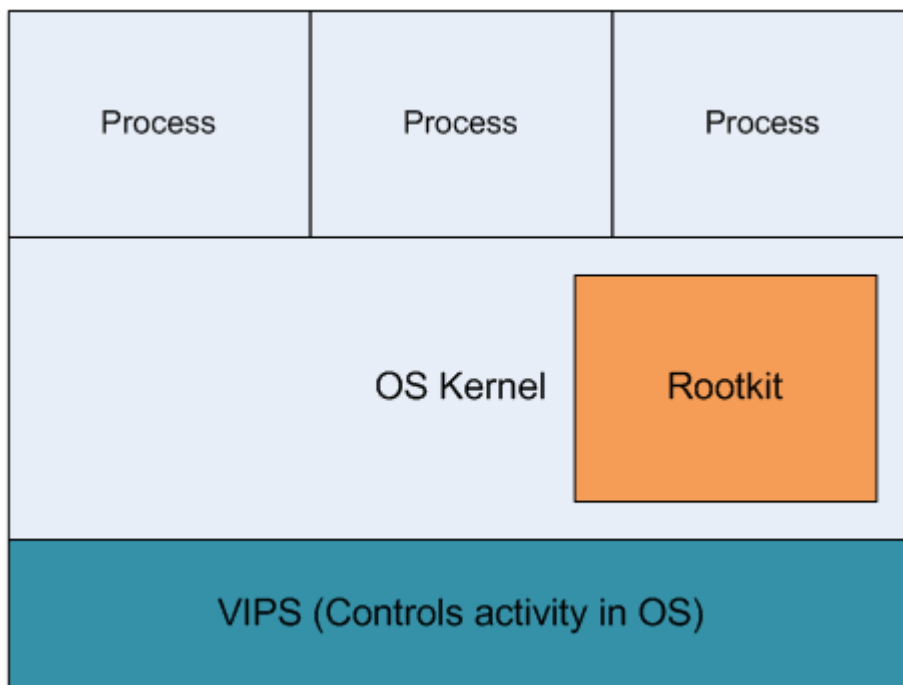


The recently emerged class of anti-rootkits attempts to detect rootkit activities by monitoring the results such as detecting changes in system code and low-level system structures. The integrity scanners are vulnerable, complex and highly specialized to detect only certain types of rootkits. The complexity of modern operating systems does not allow for effective integrity monitors, as there are just too many system structures and too much code to control. The integrity scanners work in the OS kernel with the same level of privileges as rootkits they are attempting to detect. Competing with the rootkits on the

same level of privileges makes them vulnerable to rootkit attacks and useless against the newest rootkits.

We have defined a brand-new class of information security systems.

4. Virtual Intrusion Prevention System, VIPS.



VIPS uses hardware virtualization technology that allows gaining a higher level of privileges over kernel-mode rootkits. The system works as a hypervisor on supported CPUs. The operating system itself works in a virtual machine that is controlled by VIPS from the outside. Suspected rootkit activities are intercepted by VIPS in order to notify the user. The malicious code can be isolated in a secure 'sandbox'. Rootkits are running with lower privileges, and stand no chances against the anti-rootkit.

Hypersight Rootkit Detector – the first VIPS

Hypersight Rootkit Detector is a brand-new product designed to detect malicious activities in the operating system kernel. The following operating systems are supported: Windows 2000, Windows XP, Windows Server 2003.

Hypersight Rootkit Detector is a virtual machine monitor. Hypersight Rootkit Detector kernel runs as a hypervisor when the computer starts. The kernel controls critical operations and is completely transparent to the operating system and all software.

Hypersight Rootkit Detector monitors and intercepts the following actions classified as being potentially dangerous:

- Attempts to modify page table. This activity is typical for 'shadow walker' rootkits that hide themselves in the computer memory.

- Attempts to modify read-only kernel modules. Most rootkits exhibit this behavior.
- Attempts to modify GDT and IDT. Typical for 'shadow walker' and other rootkits.

All of the above activities are illegal operations in Microsoft operating systems. These operations are not allowed in Windows Logo certified drivers. However, most rootkits are attempting to perform one or more of these actions. Some information security and copy-protection systems are also using these technologies.

Hypersight Rootkit Detector intercepts every action from the list and notifies the user about the driver that attempted to perform the action, thus solving the task of detecting kernel-mode rootkits. Note that kernel integrity scanners are generally unable to do the same.

Rootkits are performing the following activities to circumvent memory write-protection:

- Resetting write-protection bit (CR0.WP)
- Mapping memory sections with write privileges (calls to MmMapLockedPages, MmMapLockedPagesSpecifyCache)
- Accessing physical system memory via \Device\PhysicalDrive object

Hypersight Rootkit Detector kernel intercepts all attempts to circumvent memory write-protection.

Hypersight Rootkit Detector intercepts and blocks all attempts of switching into hypervisor mode. So far there are few rootkits using hardware virtualization, including Blue Pill and Vitriol.

VIPS Development

Virtual Intrusion Prevention Systems (VIPS) can successfully protect against most kernel-mode rootkits. Hardware virtualization is a powerful technology allowing detecting and blocking malicious actions attempted by rootkits. However, relying on hardware virtualization alone is not enough to completely protect a PC. A complex protection system must harmoniously combine methods implemented in all four types of information security systems.