Host-based Intrusion Prevention System (HIPS)

White Paper

Document Version (esnhips 14.0.0.1)
Creation Date: 6th Feb, 2013

Host-based Intrusion Prevention System (HIPS)

Few years back, it was relatively easy to determine and decipher malicious programs, using predefined signatures to detect viruses, worms, trojans, and similar malware. Now a days, trends of malicious threats have changed a lot and malicious program writers use advance technology to deceive traditional ways of preventing malicious threats like anti-virus, firewall etc.

Like mentioned above, in the past, Anti-Virus vendors primarily relied on signature based detection. This method, although reliable, was entirely dependent on virus signatures. The way malware writers succeeded in evading signature based protection, most Anti-virus vendors have started evolving different techniques to mitigate these types of attacks. Anti-virus vendors were forced to rethink and adapt themselves in order to prevent latest malware trends and need to be one step ahead of malware writers. To combat these threats, HIPS technology was developed.

eScan Security solution features Host-based Intrusion Prevention System (HIPS). This system is designed to detect unwanted and malicious program activity and block it in real-time.

Definition of HIPS:

It is a method employed within or by security software critical systems are protected against malware and actions taken by malware. Starting from the network layer all the way up to the application layer, HIPS protects from known and unknown malicious attacks. HIPS analyze the characteristics of the host machine and the various events that occur within the host, for suspicious activities.

Why it is better than IDS/Network IPS and Anti-Virus/Anti-Spyware?

An IDS/Network IPS has the capability to tell you exactly what has happened on the network. Major drawback is that it cannot stop an attack from happening. An event must occur before it will send an alert that there has been an intrusion. An IDS/ Network IPS is good for alerting and recovery purposes, but unfortunately cannot prevent an attack from happening.

Anti-virus and anti-spyware vendors have made great achievements in how they scan for viruses, trojans, worms, and spyware, rootkits, but still rely heavily on signatures. This is where the protection is weak. If somebody does not send samples of an attack or the vendor does not discover the new virus or spyware, a signature cannot be created for it. Yes, they do scan and stop known viruses, spyware, but they lack the ability to stop the unknown or zero-day threat which is where everybody is the most vulnerable.
HIPS protect hosts in ways that other types of protection cannot. This is not to say that IDS/Network IPS, antivirus, and anti-spyware are not needed. We should employ multi-layer protection, so that if one layer fails, the other one should prevent it.

eScan 11 - HIPS:

eScan 11 implements HIPS at Network layer, transport layer & application layer. The implementation is "dynamic" at the network and transport layer. But, at the application layer, it is more like static. The eScan firewall drivers, owing to network analysis features implemented within it, provides HIPS at the network layer. Our MWL Technology, by continuously analyzing traffic emanating from browsers, email clients, etc., provides HIPS at the transport layer. And, at the application layer, our Proactive Scan, which statically analyzes executables to check if an "executable" is suspicious or not, provides the HIPS functionality.

eScan 14 - HIPS:

HIPS on eScan 14 is essentially the same, but it has been improvised a lot, with additional protection layers being added. For example, eScan's Firewall also now monitors for concurrent connections from any host and can do portscan blocks. This is again part of HIPS, which has become necessitated owing to the large-scale aggressive attacks seen on an open network. Again, at the application layer, we have implemented both Static and Dynamic monitoring of executables, which will ensure that 90% of unknown malware and zero-day threats are blocked, based on the behavior patterns of programs.

Every executable that is run on the host machine, is continuously monitored at the kernel level, and sometimes at the user level. This means that every call that a PE based binary makes, is given a score. General calls, which are used by normal applications, are given no scores. But any calls, which are suspicious in nature, for example,

- Detect VM environment
- Modify sensitive registry keys
- Detect debugging environment
- Calls to change permissions or elevate privileges
- Communicate to an unknown external entity
- File-system modifications (binaries, SAM files, ACLs, system databases)
- Memory modifications
- Creating threads into a remote binary. etc.

are given a high score. When the combined analysis of scores reach a specific threshold level, the binary is treated as "suspicious" and execution of the same will suspended. At the same time, a database of such objects is also maintained along with the nature of modifications by given set of executables.

Updates are regularly provided by eScan to "whitelist" certain executables which are known for such activities, but are relatively safe. This ensures that legitimate executables, known for such actions, are not marked as suspicious.

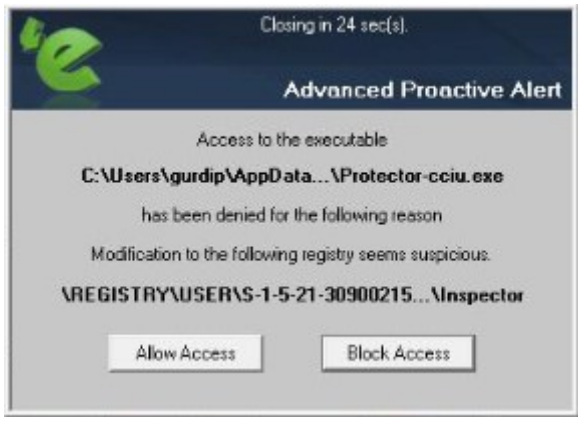
eScan 14's dynamic HIPS at application level, blocks 90% of unknown malware.

How to configure HIPS in eScan products?

A layman always not aware of different technologies, keeping this fact in mind, eScan team enabled best configuration settings for HIPS technology. By default, HIPS is enabled in eScan products. It is a combination of eScan Firewall and Proactive Behavior monitoring technology plus endpoint security.

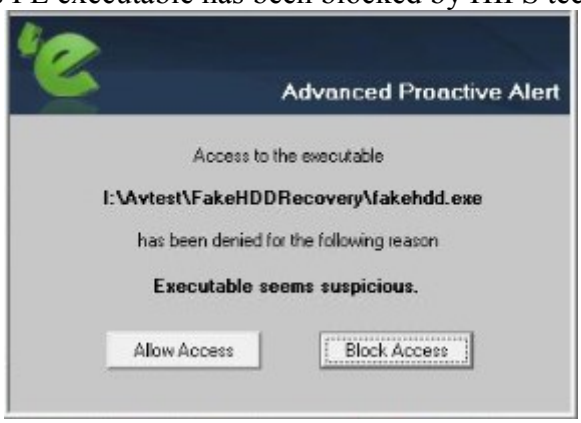
HIPS settings are in interactive mode, so whenever an unknown threat is detected an alert will be displayed to the user. By doing this we have taken precautions to minimize false positives and more accuracy while detecting suspicious activities.

If eScan HIPS detects any suspicious activity it will alerts shown as below

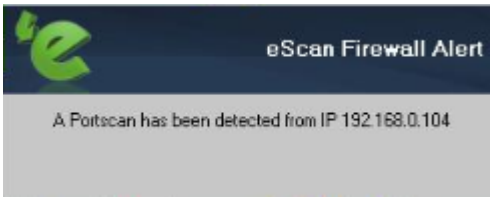


You can see from the above image it stops modification in the registry from a suspicious application called protector-cciu.exe

Below alert shows you the suspicious PE executable has been blocked by HIPS technology



From below image we can see an attempt of port scanning has been blocked by eScan Firewall.



Hence eScan HIPS technology gives complete security for your digital life.