

Securing the Uncertain

BITDEFENDER'S B-HAVE PROACTIVE TECHNOLOGY
FOR DEFENSE AGAINST VERSATILE THREATS

Today's Malware Challenge

The security landscape has changed markedly during recent years and the risks which businesses now face are very different to those of yesteryear. Until recently, malware creation was the domain of the amateur teenage malcontents desire on earning a reputation; today, it is created by skilled criminal coders intent on earning a buck. This commercial exploitation of the malware industry has served to drive both the frequency and the sophistication of attacks.

Malware has now reached epidemic levels

With more than 3,000 strains being identified each day during 2007¹, it has become extremely difficult for vendors of entirely signature-based security solutions to keep the pace. Currently, there are more than 1 million known strains of malware in the wild.

Malware attacks have become increasingly sophisticated

Yesterday's risks were relatively basic and usually easily mitigated. Today's risks are far more sophisticated and are specifically designed to exploit the shortcomings of traditional security architectures:

- Transient polymorphic threats can elude detection by both antivirus solutions and Intrusion Detection/Prevention Systems (IDSs and IPSs) which rely on reactive signatures.
- Script-based web attacks cycle through multiple vulnerabilities until an exploitable weakness is found. They increasingly utilize packaged modules to conceal their malicious payloads.
- Fragmentation, interleaving and SQL injection techniques can be used to bypass the static, deep-packet architectures of many perimeter defense solutions.
- Laptops, other mobile computing and storage devices can all act as vectors; they can be used to carry malware into the network in a manner that completely bypasses perimeter security solutions.
- Rapid distribution methods are used to compromise as many systems as possible in the shortest possible time, before security vendors can release an update with the new signature.
- The time elapsed between the discovery of a threat and the release of a vendor update can amount to several hours or even days and constitutes a window of risk during which systems remain vulnerable.
- Infected computers are increasingly networked in the so-called botnets². This strategy is a highly effective way to update the malicious code residing on the compromised machines since it decreases the useful lifetime of a virus signature – some bot families get updated daily.
- Some malware is now being targeted at specific individuals or organizations. Such attacks may not come to the attention of security vendors as quickly as those targeting the Internet in general, delaying an update release with the new signature and thus expanding the window of risk.

In short, today's technically advanced malware is exposing the intrinsic limitations of security solutions which rely solely on reactive signatures. That is not to say that such solutions have become obsolete; on the contrary, reactive signature-based detection still remains the most accurate and computationally efficient method of detecting threats. However, for the previously mentioned reasons, reactive signatures alone are not enough and must be complemented with some other form of detection which:

¹ Malware quietly reaching epidemic levels: http://www.darkreading.com/document.asp?doc_id=143424

² Botnet is a coined term derived from robot network. A botnet might be understood as a collection of malicious software robots (abbreviated bots), whose purpose is to run different kind of computer applications controlled by the owner or the disseminator of the software robot source, on a group of compromised computers, usually connected to the Internet.

1. Reduces the window of risk between the discovery of a threat and the release of a threat signature update;
2. Is immune to evasion techniques such as polymorphism.

Current Solutions for Security Limitations

Present days answers to the listed security constraints rely mostly on a method called **Heuristic Detection**.

What Is Heuristic Detection?

Heuristic detection works on the principle that if a program exhibits malware-like characteristics and/or behavior, then probably it is malware. Viruses and malware tend to perform specific actions – which the legitimate programs do not usually perform –thus making them detectable. While the idea may sound simple, the technology behind the process is actually exceedingly complex.

Classic signature-based scanners maintain a database of malware signatures (byte sequences extracted from malware samples) against which files are checked. Should a file be found to contain a byte sequence that matches a signature in its database, the file is assumed to be infected.

Heuristic scanners also maintain a database of signatures but, unlike traditional scanners, each signature represents a particular characteristic or behavior which malware is known to exhibit.

Here's an example of how heuristic detection can work to detect a phishing attack utilizing PayPal™. To be able to open PayPal's website, a computer first needs to find PayPal's IP address. To do this, the computer checks its Hosts file to see whether the IP number is listed (the Hosts file contains a listing which maps host names to their corresponding IP address). Should the IP address be found, it is used to open the website. Should no IP address be found, the computer tries to determine it by contacting a Domain Name Server (DNS) computer. A phishing attack alters the Hosts file enabling the malware to direct users to an unexpected site – a person entering `www[dot]paypal[dot]com` into their address bar would be directed to a phishing website created to extract people's PayPal account information. There are relatively few legitimate programs that modify the Hosts file, so it is reasonably safe to assume that any program seeking to do this, in fact, malware.

Types of Heuristic Detection

There are two types of heuristic scanner: static and dynamic. Both rely on “behavior signatures” to identify malware, but that is where the similarity ends.

Static scanners examine a program's structure and programming logic to establish the actions that are likely to be performed and whether any of those actions matches a possible malware behavior.

Dynamic scanners, however, actually execute the program in a virtual environment in order to establish exactly what actions the program performs and whether any of those actions match malware behavior.

There are pros and cons to each method. Because the malware creators often use encryption and other obfuscation techniques to disguise their code, it can be extremely difficult for a static scanner to determine the actions that a program performs. To overcome this, static scanners attempt to identify other characteristics, such as the presence of the decryption routines that may indicate whether a program is malicious or not. This certainly helps improve accuracy, but it still means that static scanners have only limited visibility into the actions that a program actually performs.

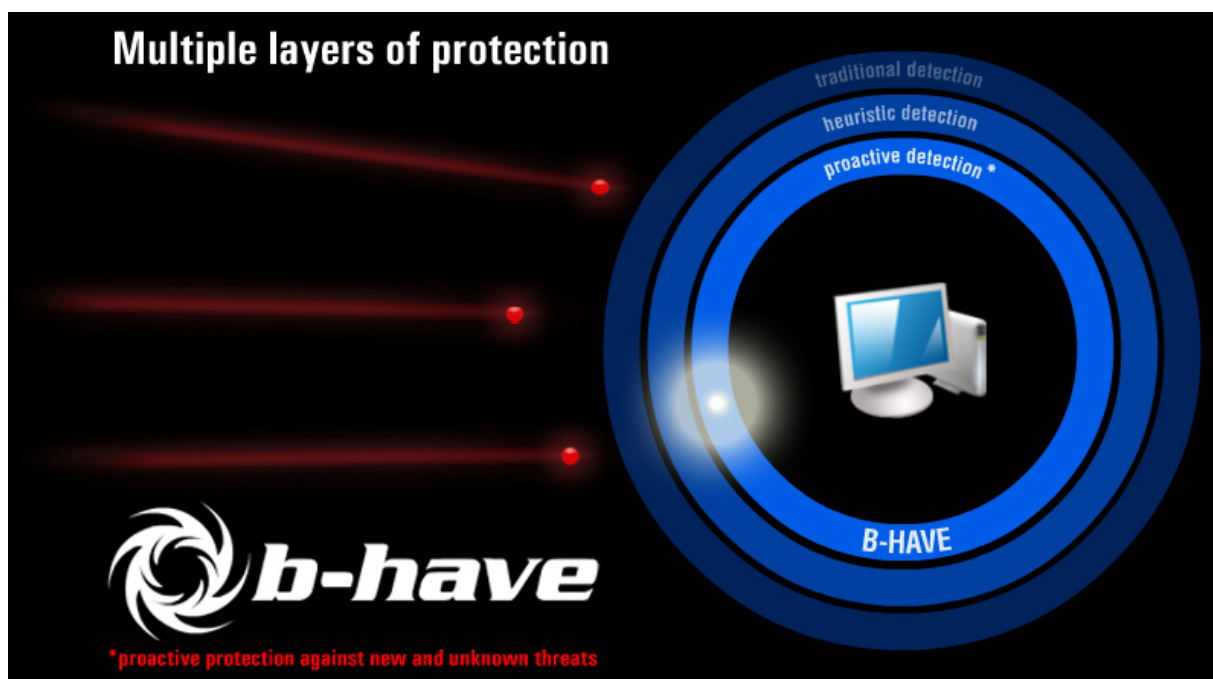
On the other hand, dynamic scanners have no visibility constraints, but instead suffer from a different problem. The virtual environment previously mentioned is, in effect, a computer inside a computer, and therefore requires additional resources. Furthermore, executing a program and analyzing its behavior is often a time consuming process which degrades system performance up to that point that impacts on operational viability.

In addition, heuristic detection is an inexact science and it can be extremely difficult for vendors to strike the right balance between detecting a high percentage of threats and keeping down the incidence of misclassifications. The operational viability of heuristic solutions has long been limited by false positives – valid programs misidentified as threats. This can cause business interruptions, extensive help desk and customer support, but also an extremely high total cost of ownership (TCO).

The ideal heuristic solution should combine the speed of a static scanner with the detection capabilities of a dynamic scanner, while keeping a high degree of accuracy. This is exactly what BitDefender® has managed to achieve with the B-HAVE technology.

BitDefender's B-HAVE – the Alternative Advanced Protection

BitDefender's B-HAVE is a dynamic heuristic scanner especially engineered and designed to complement current security technology and provide superior proactive protection while also overcoming the architectural limitations inherent in many other dynamic solutions.



A Comprehensive Approach

B-HAVE creates a virtual, self-contained computer. A system emulator builds a virtual environment, including a set of virtual hardware devices, mimicking the configuration of a typical PC. The virtual environment is completely isolated from the actual PC, its operating system and other installed applications. Any program can be launched in the virtual environment and its behavior and characteristics catalogued with absolutely zero risk to the host. To determine whether a program is malicious or not, B-HAVE checks for those characteristics known to be associated with the malware. For instance, a program may be deemed to be malicious if it attempts to modify certain files, read from or write to a sensitive area of the memory or create a file that is a product of a known virus.

When you attempt to use an un-trusted program, B-HAVE delays the launching until the program's behavior and characteristics are analyzed and catalogued in the virtual environment. If no malicious actions are detected, B-HAVE starts the program normally; if, on the other hand, a suspect conduct is present, B-HAVE automatically quarantines or deletes the application (depending on the options you choose).

In addition, B-HAVE provides you and your system with the following security benefits:

- generic unpacking methods which provide 0-day unpacking support for new packers

- Visual Basic Runtime Engine for proactive detection of visual basic viruses
- COM support in order to fully emulate VB viruses
- very good static unpacker support
- platform independent: it runs on Windows as well as on all Linux and FreeBSD flavors
- BAT/CMD emulation embedded in the virtual machine.

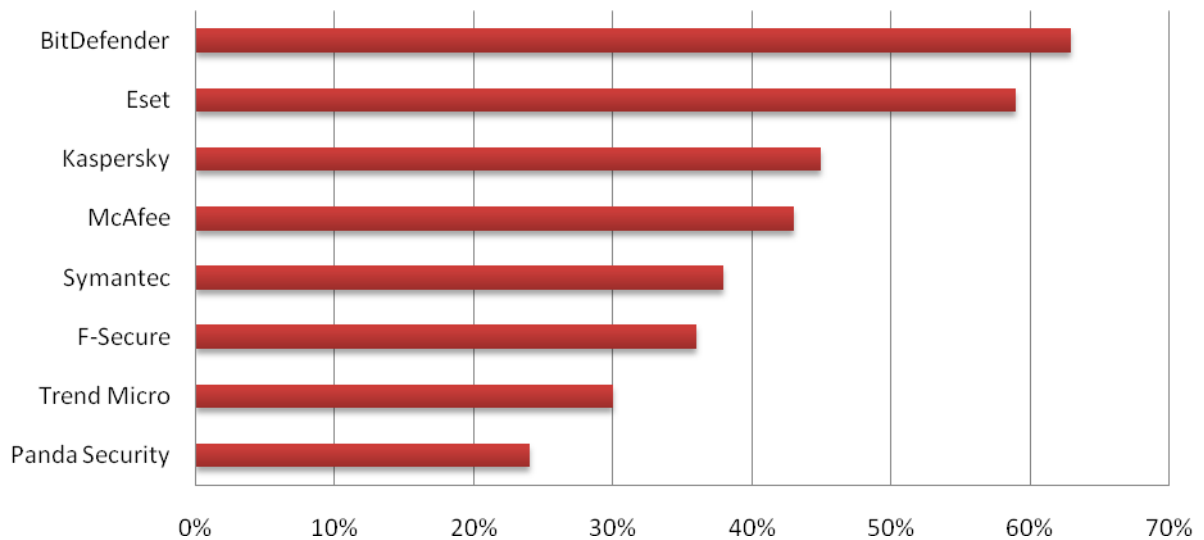
Accuracy and Precision

BitDefender's B-HAVE keeps the right balance between accuracy and precision, by providing a solution which detects a high percentage of threats without generating a high number of false positives and without compromising performance. False positives are avoided by a combination of classic and modern engineering solutions, such as:

- a database of known harmless files, such as samples of installed software or (multi)media files;
- a decision-making mechanism which helps you maintain your system's and files health. To keep you safe, B-HAVE flags by default any potential harmful behavior. You can further choose whether to drill-down the system check, by sending the suspicious file to the BitDefender antivirus lab, while also keeping it quarantined, or to release it from the quarantine, if is known to be harmless.

Thus, B-HAVE provides immediate and proactive protection against new and emerging threats. Independent testing carried out in January 2008 by Anti-Malware Test Lab³, showed that B-HAVE heuristics detected 63% of threats, without needing a signature update.

Proactive antivirus protection test



³ Proactive antivirus protection test <http://www.anti-malware-test.com/?q=node/39>

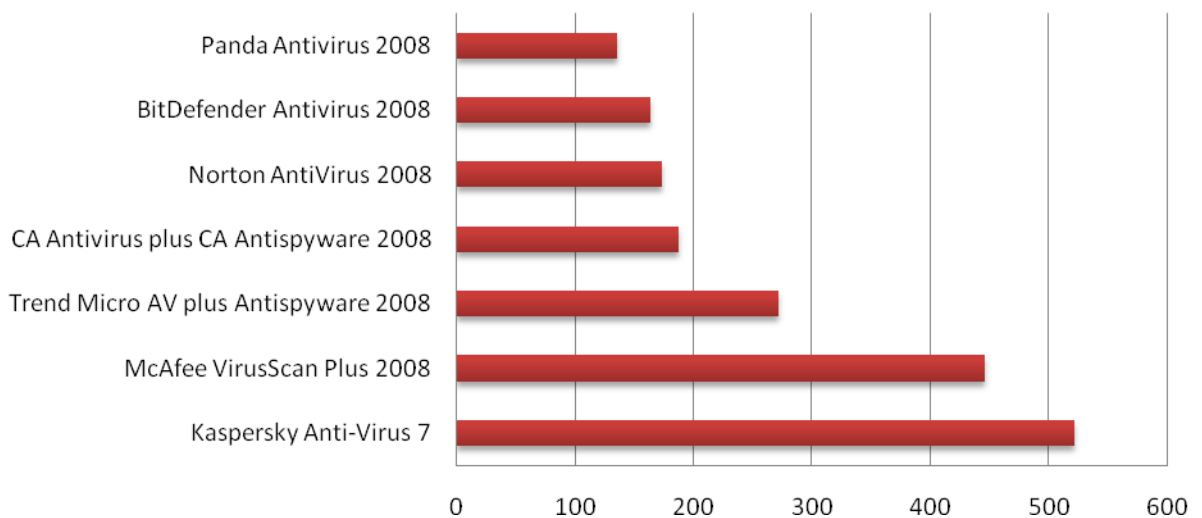
Dynamic Security for Dynamic Threats

To avoid performance degradation, B-HAVE maintains a list of known code sequences, packing methods and system calls which are functionally emulated by an acceleration routine which dramatically decreases the time it takes to execute known code sequences in the virtual environment.

To further reduce B-HAVE's impact on the system resources, you have the option to trust programs and exclude them from scanning.

Although it might seem a long and tortuous process, B-HAVE completes it in just a fraction of a second, displaying the ongoing actions and possible course you might want to follow. The same Anti-Malware Test Lab, proved that B-HAVE's complex heuristics rank among the top three competitors, as you can see from the chart below.

Scan speed (seconds)



About BitDefender

BitDefender is the creator of one of the industry's fastest and most effective lines of internationally certified [security software](#). Since our inception in 2001, BitDefender has continued to raise the bar and set new standards in proactive threat prevention. Every day, BitDefender protects tens of millions of home and corporate users across the globe—giving them the peace of mind of knowing that their digital experiences will be secure. BitDefender solutions are distributed by a global network of value-added distribution and reseller partners in more than 100 countries worldwide. More information is available [on our security solutions' site](#).