BITDEFENDER ACTIVE VIRUS CONTROL:
PROACTIVE PROTECTION AGAINST NEW AND EMERGING THREATS

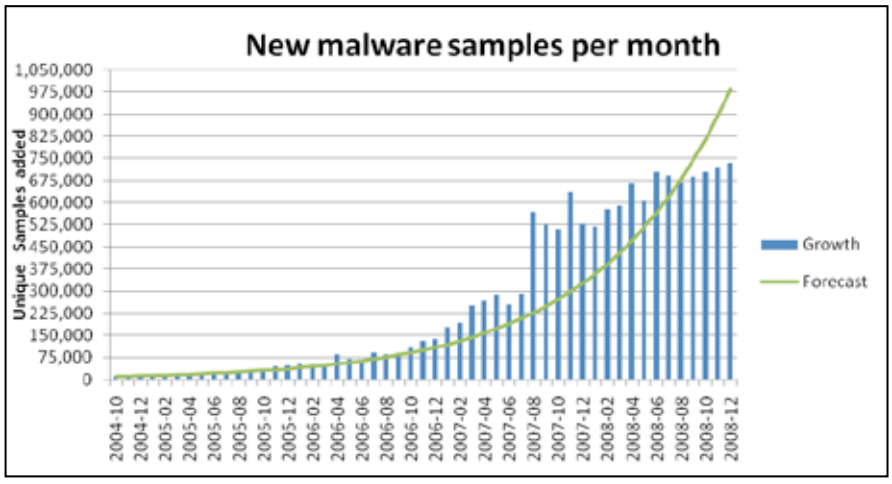
Why you should read this white paper

With new and variant strains of malware emerging at an unprecedented rate, heuristic malware detection has become an increasingly critical line of defence against threats. BitDefender Active Virus Control® is an innovative proactive technology which uses advanced heuristic methods to achieve extremely high detection rates of new viruses.

This white paper explains why such protection is necessary and provides a technological overview of the detection methodologies used by BitDefender solutions.

The state of malware

Keeping computers secure and protected against viruses and other forms of malware has never been harder. With more than half a million new and variant strains of malware emerging each month, tracking and mitigating each threat has become an enormously challenging task for all security vendors.



Source: av-test.org : More than half a million new and variant malware strains are discovered each month.

Compounding the problem is the fact that both malware and the mechanisms used to deliver it have become increasingly sophisticated. Trusted websites can be compromised and used to launch complex script-based attacks that cycle through multiple exploits, advanced packaging methods

are deployed in order to conceal malicious payloads and rootkits are used to make malware completely invisible to both the operating system and security software. Malware can also actively disable known security software at the time of install and during operation by constantly trying to overwhelm or kill antivirus or software firewall processes.

Additionally, social networking websites such as Facebook, MySpace and Twitter provide criminals with new opportunities for exploitation and can enable malware to spread faster than ever before. Whereas a virus may once have taken days or even weeks to propagate, it can now reach millions of computers in hours.

Combined, these factors make it exceptionally difficult to effectively detect and block malware using conventional methods and technology.

Profits up the ante

The driver for the increase in the volume and complexity of malware has been money. In the past, viruses were created by teenagers in order to earn notoriety; today, malware is created by criminals to earn a living. And there are substantial sums to be made. Spam, phishing, pump-and-dump schemes and data-stealing Trojans and keyloggers can net their creators enormous sums. To put it simply, malware has evolved into multimillion dollar, multinational industry.

This commercialization has also resulted in a significant change in the nature of malware. Whereas old-style viruses made no effort to conceal their presence on a system, today's malware is much stealthier and often uses sophisticated technology in order to remain hidden. The longer malware can remain undetected, the more likely it is to be able to successfully steal personal information or to be able to continue to cause the compromised computer to act as a spambot.

What does this mean? Simply that if your computer becomes infected with malware, you may well never know about it – until, that is, you notice unexplained transactions on your bank statement.

Furthermore, as the criminals are able to use their enormous profits to fund malware development, a vicious circle has been created: the more money the criminals make, the better their malware becomes; and the better their malware becomes, the more money the criminals make. For example, in November 2009, the FBI's Internet Crime Complaint Center (IC3) issued an intelligence note warning that sophisticated malware has been used to harvest corporate online banking credentials and that, "As of October 2009, there has been approximately $100 million in attempted losses." With such enormous sums at stake, it is obvious that the criminals have both the motivation and the financial means to develop ever better malware.

Heuristics: detecting tomorrow's threats today

As mentioned previously, the exponentially increasing volume of malware creates real challenges for security vendors: ensuring a timely response to each new and variant strain of malware to emerge is, as you can probably imagine, far from easy. And yet it is absolutely critical that the response be timely – with malware able to spread so rapidly, a slow or delayed response could lead to an enormous number of computers being compromised.

The real problem, however, is that no matter how speedily vendors respond, there is always a gap between the time that a new threat is released into the wild and the time that end-users' computers are "immunized" against that threat via the release of a signature. This gap represents a window during which systems remain vulnerable – and, with more than half a million new and variant strains of malware emerging each month, the number of such windows has become substantial!

Heuristics is a form of proactive detection that closes the window during which computers are vulnerable. Conventional detection relies on signatures. These signatures are snippets of code extracted from actual malware samples and are used by antivirus programs to perform pattern-matching. The problem with this method is that it takes time to produce the signature: antivirus

vendors need to obtain a sample of the malware, develop a signature and then push that signature to users – and this leads to the creation of the window mentioned above. Heuristic detection also relies on signatures but rather than being simple fingerprints, these signatures specify actual behaviours which may indicate that an application is malicious. This works because malicious programs inevitably attempt to perform actions that legitimate applications do not. Examples of suspicious behaviour would include attempting to drop files, disguise processes, replication or executing code in another process's memory space. Because heuristic scanners look for behavioural characteristics rather than relying on simple pattern-matching, they are able to detect and block new and emerging threats for which a signature or fingerprint has yet to be released.

In order to protect computers, the majority of heuristic scanners, including the BitDefender B-HAVE heuristic engine, temporarily delay applications from starting while the code is executed in a virtual environment that is completely isolated – or sandboxed - from the real computer. If no suspicious behaviour is observed, the computer is instructed to start the application normally. If, on the other hand, suspicious behaviour is observed, the computer is instructed to block the program. The entire process happens in fractions of a second and so has practically no impact on either the user's experience or performance.

While this approach certainly enhances security considerably, it nonetheless has a couple of shortcomings. Firstly, programs can only be run in the virtual environment for a short period as, obviously, it would not be acceptable to delay launch by any substantial amount of time. This means that malware can avoid detection simply by delaying performing any malicious actions. Secondly, a program that has already been checked (and is, therefore, trusted) could be exploited and either modified in-memory, while running, or used to launch a malware process with its own credentials.

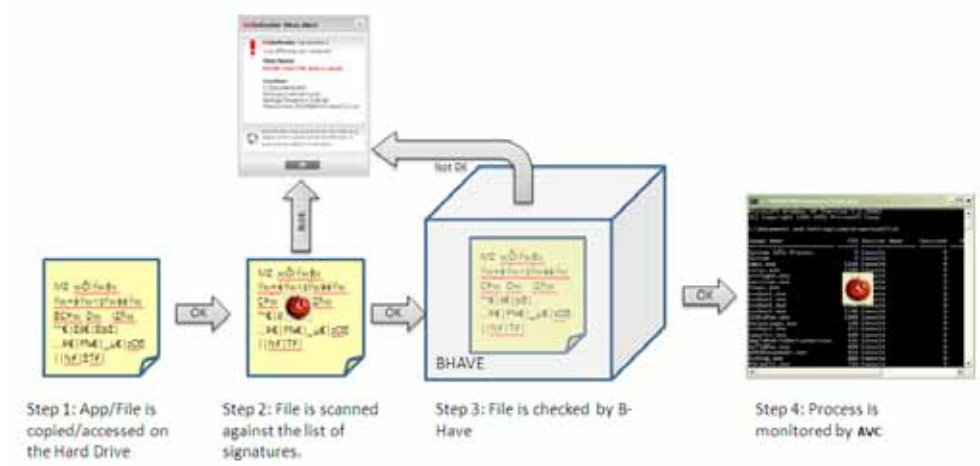
To address these shortcomings, BitDefender has introduced a new technology in its 2010 product line" BitDefender Active Virus Control.

BitDefender Active Virus Control: heuristic detection advances to the next level

Active Virus Control is a new feature in the BitDefender 2010 product line, which includes BitDefender Antivirus 2010, BitDefender Internet Security 2010 and BitDefender Total Security 2010.

In order to provide maximum security, all BitDefender 2010 products use a four step scanning sequence:

- **Step 1:** Each time a file is accessed, copied or downloaded via the Web, email or instant messenger, the file is intercepted by either the BitDefender File System driver or the appropriate proxy and sent for scanning.
- **Step 2:** The file is checked against the BitDefender Signature Database (a database of malware "fingerprints") that is continually updated on an hourly basis. If the file contents match one of the signatures, the product automatically tries to disinfect the virus. If this action fails, the file is moved to the quarantine folder. If no signature is matched, the file is passed to B-HAVE to be checked.
- **Step 3:** B-Have checks the file by running it in a virtual environment inside the BitDefender Engine. If the file exhibits suspicious, malware-like activity, B-Have reports the file as malicious. If not, the file is declared clean and the relevant process is allowed to run.
- **Step 4:** Active Virus Control monitors the actions of the processes (specific processes) as they are running on the computer. It looks for signs specific to viruses and gives a certain score for each of these actions. When the overall score for a process reaches a given threshold, the process is reported as harmful and, depending on the user profile, it is either terminated or the user is prompted to specify the action that is to be taken (depending on the mode in which BitDefender is being run).



The BitDefender Scanning Sequence

Unlike B-HAVE and other heuristic scanners, Active Virus Control monitors everything applications do for as long as they are active and so cannot be defeated by the delaying tactics that some advanced malware deploys. Additionally, this constant monitoring also prevents malware from exploiting or hijacking already trusted applications.

How Active Virus Control works: a technology overview

Active Virus Control continuously monitors all running applications and processes, except:

- Processes specifically excluded from monitoring by the user (white-listed processes).
- System processes such as crss.exe, lsass.ese or smss.exe that are known to be clean.
- All processes loaded before the Security Service (vsserv.exe).
- On Windows XP 64-bit and Windows 2003 64-bit system, Active Virus Control monitors only processes running in 64-bit mode (processes running in 32-bit mode are not monitored).

Applications and process are continuously monitored for as long as they are active for signs of suspicious, malware-like activity, including:

- Not waiting for or requesting any form of user interaction
- Not displaying any type of user interface when executing or terminating the execution
- Copying or moving files in C:\Windows\ or C:\Windows\System32\
- Having an unrelated type of icon - for example, a process that has a folder icon
- Executing code in another processes' space in order to run with higher privileges
- Running files that have been created with information stored in the binary file
- Self-replicating
- Creating an auto-start entry in the registry
- Attempting to hide from process enumeration applications
- Dropping and registering drivers in C:\Windows\System32\

As legitimate applications will sometimes perform one or more of these actions (such as creating an auto-start entry), Active Virus Control does not determine a process to be malicious based on any single action; instead, it keeps a running score and only categorizes an application as malicious when a certain threshold is reached. This minimizes the incidence of misidentifications (false-positives) avoiding unnecessary intervention by the user.

Active Virus Control greatly increases the detection rate of evasive stealth malware

In internet testing, 63.5% of the malware samples which were not detected by either the standard BitDefender scanning engine or by B-HAVE *were* detected by Active Virus Control. Given that B-HAVE is one of the most advanced and effective heuristic scanning engines on the market, it is clear that Active Virus Control has the ability to provide substantially better protection than other solutions and to drastically reduce the risk of a system being compromised by a new or emerging threat.

Conclusion

The criminals that create malware have become increasingly sophisticated in terms of the methods that they use in order to minimize the likelihood of their malicious programs being detected by heuristic scanners. Some malware is even able to detect when it is being run inside a virtual machine and delay displaying performing any malicious actions until it has determined to be clean and launched in the real computing environment. Compounding the challenge is the fact that determining whether or not an application is malicious based on the actions it performs is a far from straightforward process. For example, an application that will erase the hard disk may be a perfectly legitimate system tool. However, if that application attempts to mislead users into running it back - masquerading as an image or some other harmless type of file - then it may well be malware.

Active Virus Control is BitDefender's response these challenges. It represents a brand new layer of security between the computer and potentially malicious code, providing users with a previously unprecedented degree of protection.

About BitDefender

BitDefender is the creator of one of the industry's most secure and 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 at www.bitdefender.com.