

Bitdefender[®]

Advanced Threat Control

Proactive Protection Against
New and Emerging Threats

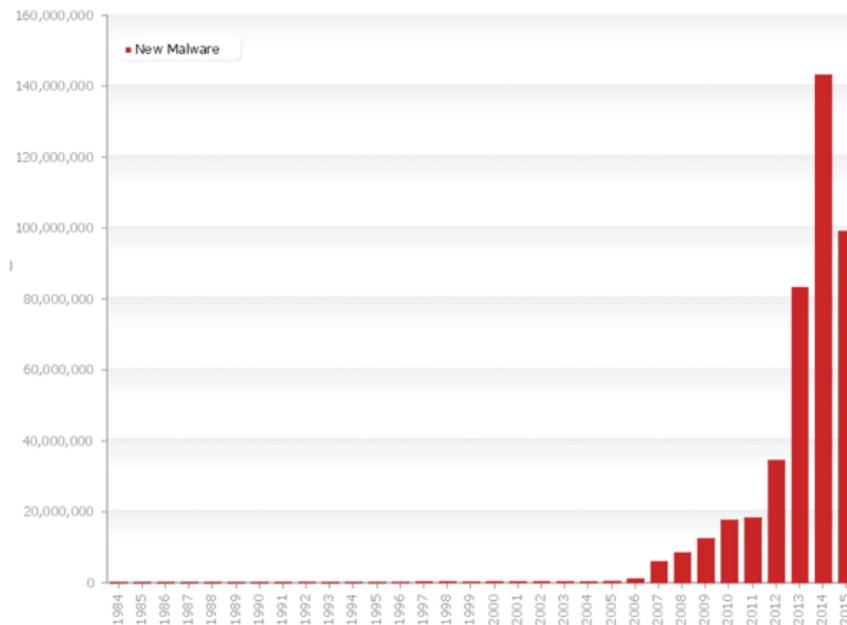


Why You Should Read this White Paper

The continuous rise of new threats has left traditional security mechanisms both ineffective and unreliable in providing adequate defense. Today's pervasive threats have increased in complexity, making prevention, detection, and remediation difficult for traditional security software.

Bitdefender Advanced Threat Control is a proactive and dynamic detection technology, based on monitoring processes and system events, and tagging of suspicious activities. It has been designed to act against unknown threats based on their behavior. This white paper explains why such protection is necessary and provides a technological and technical overview of the detection methodologies used by Bitdefender.

Modern Malware Require New Countermeasures



Source: av-test.org: More than 12 million new and variant malware strains are discovered each month

Keeping computers secure and protected against threats has never been harder. With more than 12 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.

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 to conceal malicious payloads. These malware can also actively disable known security software at the time of installation and during operation by killing antimalware or software firewall processes.

Social networking websites such as Facebook and Twitter provide cybercriminals with personal data for exploitation through social engineering and can enable malware to spread faster than ever. If a malware 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.



Money matters

The main driver for the increase in both volume and complexity of such threats has been money. Historically, viruses were created by teenagers seeking notoriety and recognition for their coding skills. Today's malware is created by criminals to earn a living and even generate substantial profit. Spam, phishing, pump-and-dump schemes and data-stealing Trojans and keyloggers can net their creators an enormous income. Malware has evolved into a multinational and multimillion dollar industry with practitioners just as skilled and versed in security matters, as experts working in the security industry.

These monetization patterns have also significantly changed the nature of today's threats. For instance, if your computer becomes infected with one such threat, you may not realize it until unexplained transactions occur on your bank statement or it starts consuming more processing resources than usual. As 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 and more sophisticated their malware becomes; and the better their malware becomes, the more money the criminals make. Cybercrime costs the global economy about \$445 billion every year, with damages to businesses caused by intellectual property theft exceeding \$160 billion, according to the Center for Strategic and International Studies (CSIS) report published on Jun 9, 2014. 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

Ensuring a timely response to each new threat can become more than challenging. However, it is critical to be prompt, as the new variants of malware can spread rapidly. A slow or delayed response could lead to a large pool of computers being compromised and the potential data loss or impact on the affected network infrastructure could be disastrous.

The challenge is that, regardless of how fast security vendors react, there is always a gap between the time a new threat is released into the wild and the time computers are "immunized" against that threat via a signature update. The gap between initial moments when a threat can affect systems until the fix is disseminated creates a window of opportunity for malicious actors. With more than 12 million new malware samples emerging each month, chances are the window of opportunity favors the attacker.

Conventional detection relies on signatures. Anti-malware signatures are code snippets extracted from malware samples and used by antimalware programs to perform pattern-matching. The problem with this method is that it takes time to produce the signature: antimalware vendors need to obtain a sample of the malware, develop a signature, then push that signature to users

Heuristics are a form of proactive detection that closes the window during which computers are vulnerable. Rather than relying on signatures or binary or code fingerprints, heuristic detection relies on complex algorithms that specify actual patterns and behaviors, which may indicate that an application is malicious. This works because malicious programs inevitably attempt to perform actions in a context that legitimate applications do not. Examples of suspicious behavior would include attempting to drop files or disguise processes, or injecting or executing code in another process's memory space. Because heuristic detection looks for behavioral characteristics rather than relying on simple pattern-matching, it can detect and block zero-day threats, for which a signature or fingerprint has yet to be released.

To protect computers, most heuristic detection technologies, 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 behavior is observed, the computer is instructed to start the application normally. On the other hand, if suspicious behavior is observed, the program is blocked from executing. The entire process happens in fractions of a second, so has practically no impact on either the user experience or perceived performance. To be even more effective, Bitdefender uses application reputation, a form of white listing, and can thus employ more lightweight heuristics for applications that are known likely to be safe. Application reputation is kept intact for false positives with frequent updates from Bitdefender cloud.

While this approach certainly enhances security considerably, it 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 introduced Active Virus Control in 2010 (now known as Advanced Threat Control technology).



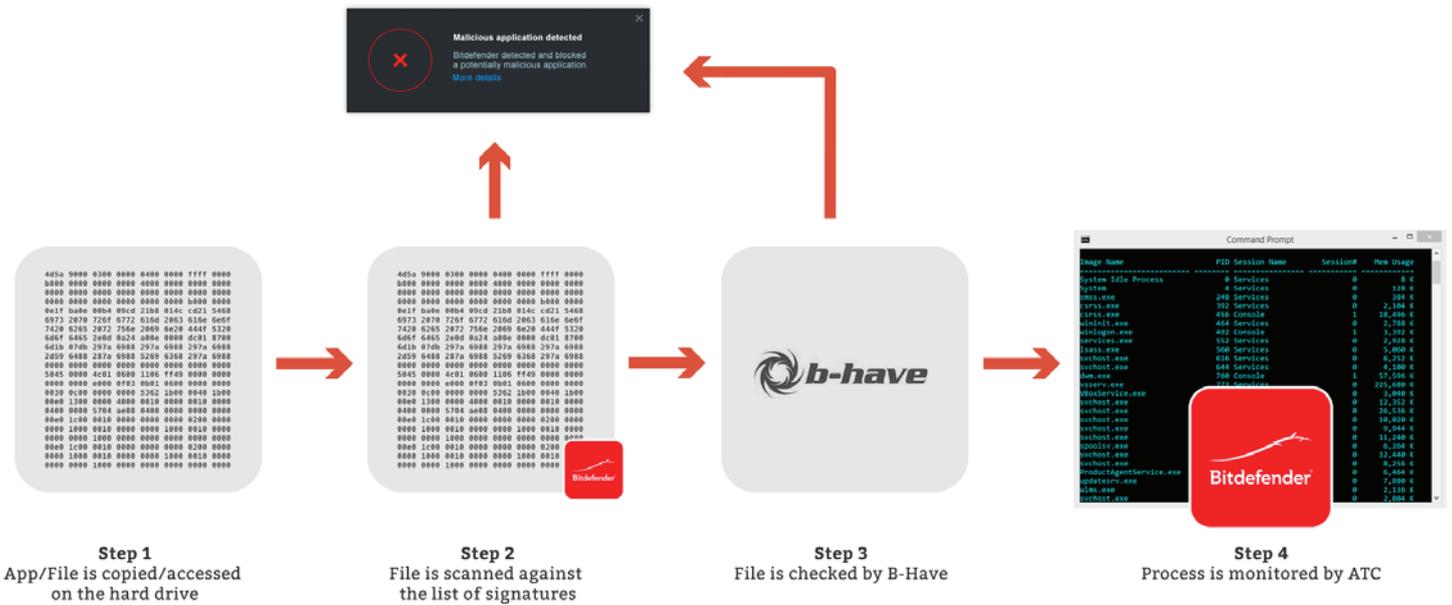
Bitdefender Advanced Threat Control: Heuristic detection advances to the next level

Step 1: Each time a file is accessed, copied or downloaded via web, email or instant messenger, it 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 updated hourly. If the file’s content matches one of the signatures, the product automatically tries to disinfect the threat. If this action fails, the file is moved into quarantine. If no signature is matched, the file is sent to B-HAVE to be checked.

Step 3: B-Have checks the file by running it in a virtual environment inside the Bitdefender Engine designed to emulate the behavior or an actual computer. If the file exhibits suspicious, malware-like activity, B-Have reports the file as malicious. If not, the file is declared clean and the process is allowed to run;

Step 4: Advanced Threat Control monitors actions of specific processes as they are running in the OS. It looks for behavior specific to malware and assigns a score for each process based on its actions and the context in which those were done. When the overall score for a process reaches a given threshold, the process is reported as harmful. Depending on the user profile, it is either terminated to isolate and remediate the threat or the user is prompted to specify the action that is to be taken (depending on the settings profile of the Bitdefender product). User profiles are product-specific. Usage of user profiles may vary in products.



The Bitdefender Scanning Sequence

Unlike B-HAVE and other heuristic detection, Advanced Threat Control constantly monitors processes. This way a delayed execution of malware can be detected and remediated. Constant monitoring prevents malware from exploiting or hijacking already trusted applications.



Leveraging signatures and heuristics with collective intelligence and machine learning

Bitdefender's security cloud, the Bitdefender Global Protective Network (GPN) is essential in leveraging information about newly discovered threats in a fast and efficient manner. In less than 3 seconds after a new threat is discovered using B-Have or ATC, the Global Protective Network ensures even systems on the other side of the globe will detect it.

Having a central threat intelligence Cloud that is always up-to-date and can be accessed by any system also greatly reduces the need for local signatures databases that burden and slow down computers.

Bitdefender's Global Protective Network (GPN) performs 11 billion queries per day, and uses reflective models and advanced machine learning algorithms to extract malware patterns, ensuring real-time protection against any threat. The system detects, anticipates and takes action to neutralize even the newest dangers anywhere in the world. It updates the reputation of apps, email sources and websites, and broadcasts alerts.

How Advanced Threat Control Works: A Technology Overview

Advanced Threat Control continuously monitors all running applications and processes. To extend the flexibility and performance there are some exceptions:

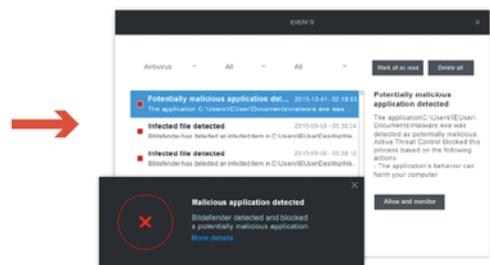
- White-listed processes that are specifically excluded from monitoring by the user
- Validated system processes that have been tagged by Bitdefender Application Reputation to be clean.



Step 1
ATC monitors running process
 • for each process ATC keeps a score
 • each important action taken by the process affects its score



Step 2
ATC detected malwareapp.exe as a possible malicious application
 • MalwareApp.exe score reached the threshold



Step 3
ATC notifies the user that an application was detected and automatically blocks it

Active applications and processes are continuously monitored for suspicious behaviors, like:

- Copying or moving files in System or Windows folders or limited access disk locations
- Executing or injecting code in another processes' space to run with higher privileges
- Running files that have been created with information stored in the binary file
- Self-replication
- Creating an auto-start entry in the registry, accessing or executing illegal operations on registry locations that require elevated privileges
- Dropping and registering drivers

As legitimate applications will sometimes perform one or more of these actions (such as creating an autostart entry), Advanced Threat

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 incidences of misidentification (false-positives), avoiding unnecessary intervention by the user.

How ATC protects against ransomware

In recent years, ransomware has ranked among the most prevalent and damaging cyber-attacks. The rise of crypto-ransomware in particular has been due to the success cyber-criminals have had in extorting money from their victims.

Spurred by the lure of financial gain, attackers are continuously investing time and effort in developing and refining new variants of crypto-ransomware. Many of these new variants are successful because they use different attack vectors, files and vulnerabilities and are often designed to be polymorphic. This has allowed the attacks to elude most antimalware solutions as they rely mostly for detection on signatures for known families of ransomware.

On top of malware signatures for known ransomware, Bitdefender products rely on Advanced Threat Control to detect new ransomware. The continuous monitoring and advanced behavioral detection available in ATC have been highly effective in detecting new attacks as, despite the mutations and differences, most ransomware tries to take similar actions.

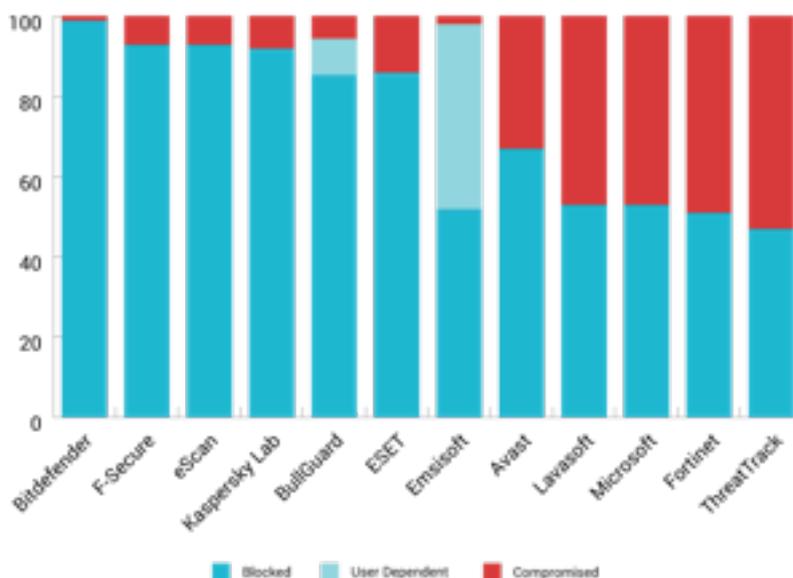
The superior heuristic detection capabilities of ATC has been proven in independent tests and this reflects also on the ability to detect ransomware. To enhance detection even more and to keep up with the development of new ransomware, dedicated heuristics are constantly added to ATC after studying and identifying specific behavior.

Advanced Threat Control greatly increases detection rate of evasive or new malware

Advanced Threat Control drastically reduces the risk of a system being compromised by a new or emerging threat.

The efficiency of Bitdefender Advanced Threat Control can be best demonstrated by Heuristic or Behavioral tests, such as the AV-Comparatives, Proactive Protection Test. The independent report tests leading AV/Antimalware products against new or zero-day malware and ranks their performance based on their ability to block malware samples. Because the threats are new, traditional signatures are useless, and so detection relies solely on the heuristic technologies.

In the 2015 test, Bitdefender outperformed all other solutions, blocking 99% of the samples, with the nearest competitor blocking 93% of the samples. .



AV-Comparatives, Behavioral/Heuristic Detection Test, 2015.



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 detection. Some malware is even able to detect when it is being run inside a virtual machine and delay performing any malicious actions until it has been 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.

Advanced Threat Control is Bitdefender's response to these challenges. It represents a layer of security between the computer and potentially malicious code, providing users with a previously unprecedented degree of protection.

Bitdefender delivers security technology in more than 100 countries through a cutting-edge network of value-added alliances, distributors and reseller partners.

Since 2001, Bitdefender has consistently produced market-leading technologies for businesses and consumers and is one of the top security providers in virtualization and cloud technologies. Bitdefender has matched its award-winning technologies with sales alliances and partnerships and has strengthened its global market position through strategic alliances with some of the world's leading virtualization and cloud technology providers.

All Rights Reserved. © 2015 Bitdefender. All trademarks, trade names, and products referenced herein are property of their respective owners.
FOR MORE INFORMATION VISIT: enterprise.bitdefender.com

