Solution Paper

unfollow the traditional

Bitdefender®
Active Threat Control

Proactive Protection Against New and Emerging Threats

Why You Should Read this White Paper

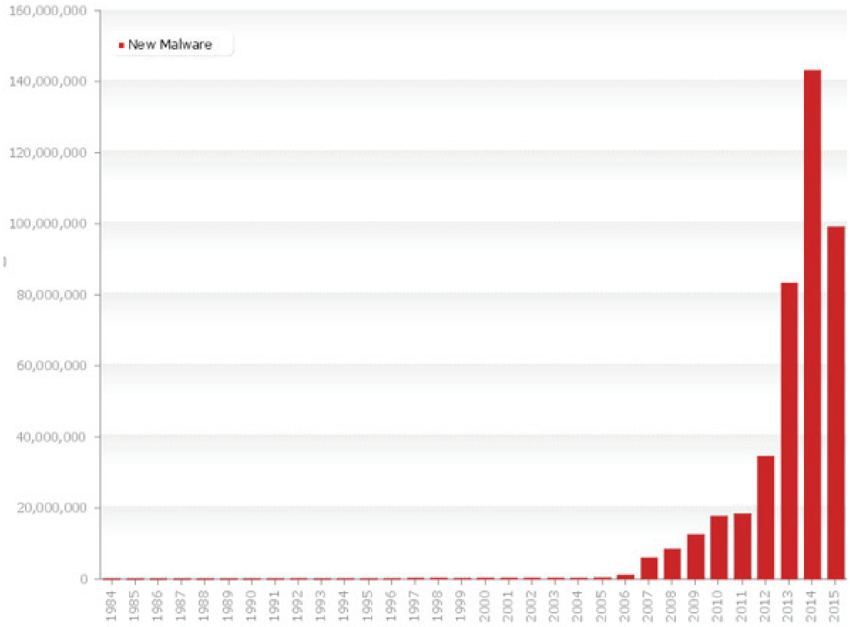
The unprecedented rise of new threats has deemed traditional security mechanisms both ineffective and unreliable in providing adequate defense. Today's pervasive threats have increased in complexity, making prevention, detection, and remediation difficult for traditional security software.

Bitdefender Active Threat Control is a pro-active and dynamic detection technology, based on monitoring processes and system events, and tagging suspicious activities. It has been designed to act against never-before-seen threats based on their behavior.

This white paper explains why such protection is necessary and provides technological and technical overview of the detection methodologies used by Bitdefender products.

Modern Malware result to new countermeasures against threats

Keeping computers secure and protected against threats 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 14 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. These malware can also actively disable known security software at the time of install and during operation by constantly trying to overwhelm or kill antimalware or software firewall processes.

Social networking websites such as Facebook and Twitter provide criminals with new opportunities for exploitation through social engineering and can enable malware to spread faster than ever before. 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 leading to the increase in both volume and complexity of such threats has been money. Historically, viruses were created by teenagers in order to earn notoriety and gain 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 amount of income. Malware has evolved into a multinational and multimillion dollar industry that's just as skilled and versed in security matters, as experts working in the security industry.

These monetization patters have also resulted in a significant change in the nature of today's threats. For instance, if your computer becomes infected with one such threats, 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 to 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 that the response should be prompt, as the new variants of malware are able to 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 unquantifiable.

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 half a million new malware samples emerging each month, chances are the window of opportunity is favor of 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, and then push that signature to users – and this leads to the creation of the window mentioned above.

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 look for behavioral 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.

To protect computers, the majority of heuristic detection, 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 and so has practically no impact on either the user experience or perceived performance. In order to be even more effective, Bitdefender uses application reputation, a form of white listing, for having 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 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 introduced Active Virus Control in 2010 (former name of Active Threat Control technology).

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

Starting with 100 heuristics in 2010, Active Threat Control has been developed to have more than 300 to date. They are constantly fine-tuned, updated, and improved by a dedicated team of security researchers and engineers form Bitdefender Labs. In order to provide maximum security, all Bitdefender products using Active Threat Control follow a four step scanning sequence:

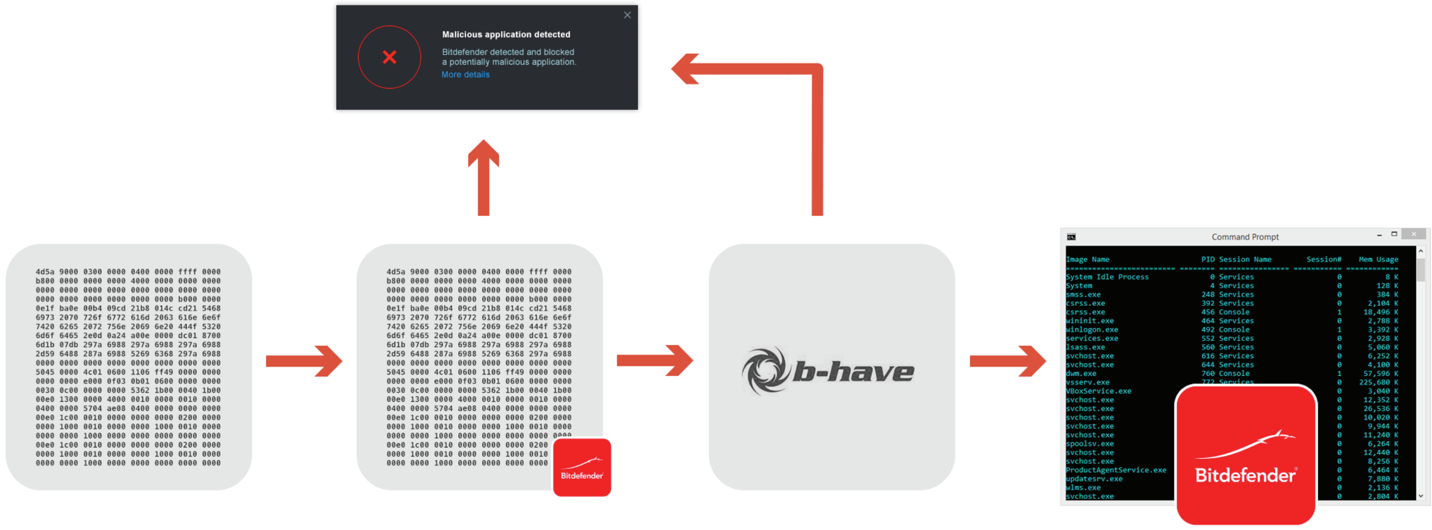
Step 1: Each time a file is accessed, copied or downloaded via Web, Email or Instant Messenger, the file is intercepted by either the Bitdefender File System driver or the appropriate proxy and sent for scanning;

Step 2: The file is checked against the Bitdefender Signature Database (a database of malware "fingerprints") that is updated in an hourly basis. 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-HAVE1 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: Active 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.

Bitdefender proprietary technology for detecting threats.



Malicious application detected

Bitdefender detected and blocked a potentially malicious application.

More details

```
4d5a 9000 0300 0000 0400 0000 ffff 0000
b800 0000 0000 0000 4000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 b000 0000
0e1f ba0e 00b4 09cd 21b8 014c cd21 5468
6973 2070 726f 6772 616d 2063 616e 6e6f
7420 6265 2072 756e 2069 6e20 444f 5320
6d6f 6465 2e0d 0a24 a00e 0000 dc01 8700
6d1b 07db 297a 6988 297a 6988 297a 6988
2d59 6488 287a 6988 5269 6368 297a 6988
0000 0000 0000 0000 0000 0000 0000 0000
5045 0000 4c01 0600 1106 ff49 0000 0000
0000 0000 e000 0f03 0b01 0600 0000 0000
0030 0c00 0000 0000 5362 1b00 0040 1b00
00e0 1300 0000 4000 0010 0000 0010 0000
0400 0000 5704 ae08 0400 0000 0000 0000
00e0 1c00 0010 0000 0000 0000 0200 0000
0000 1000 0010 0000 0000 1000 0010 0000
0000 0000 1000 0000 0000 0000 0000 0000
00e0 1c00 0010 0000 0000 0000 0200 0000
0000 1000 0010 0000 0000 1000 0010 0000
0000 0000 1000 0000 0000 0000 0000 0000
```

Command Prompt

```
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0        128 K
smss.exe                       248 Services                   0        384 K
csrss.exe                      392 Services                   0      2,104 K
csrss.exe                      456 Console                    1     18,496 K
wininit.exe                    464 Services                   0      2,788 K
winlogon.exe                   492 Console                    1      3,392 K
services.exe                   552 Services                   0      2,928 K
lsass.exe                      560 Services                   0      5,060 K
svchost.exe                    616 Services                   0      6,252 K
svchost.exe                    644 Services                   0      4,100 K
dwm.exe                        760 Console                    1     57,596 K
vsserv.exe                     772 Services                   0    225,680 K
VBoxService.exe                                               0      3,040 K
svchost.exe                                                   0     12,352 K
svchost.exe                                                   0     26,536 K
svchost.exe                                                   0     10,020 K
svchost.exe                                                   0      9,944 K
svchost.exe                                                   0     11,240 K
spoolsv.exe                                                   0      6,264 K
svchost.exe                                                   0     12,440 K
svchost.exe                                                   0      8,256 K
ProductAgentService.exe                                       0      6,464 K
updatesrv.exe                                                 0      7,880 K
wlms.exe                                                      0      2,136 K
svchost.exe                                                   0      2,804 K
```

Step 1
App/File is copied/accessed on the hard drive

Step 2
File is scanned against the list of signatures

Step 3
File is checked by B-Have

Step 4
Process is monitored by ATC

The Bitdefender Scanning Sequence

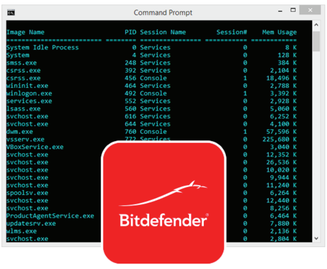
Unlike B-HAVE and other heuristic detection, Active Threat Control constantly monitors processes. This way a delayed execution of malware can be detected and remediated. Constant monitoring prevents malware from exploiting or hijacking already trusted applications.

[1]

How Active Threat Control Works:
A Technology Overview

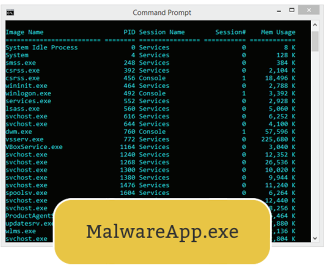
Active Threat Control continuously monitors all running applications and processes. To extend the flexibility and performance there are some exceptions:

- 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.



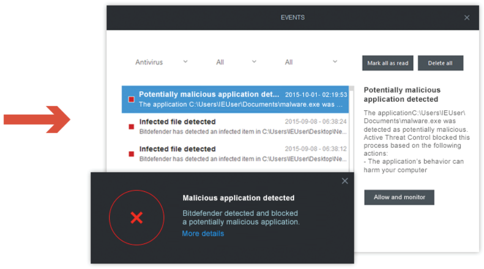
```
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0        128 K
smss.exe                       248 Services                   0        384 K
csrss.exe                      392 Services                   0      2,104 K
csrss.exe                      456 Console                    1     18,496 K
wininit.exe                    464 Services                   0      2,788 K
winlogon.exe                   492 Console                    1      3,392 K
services.exe                   552 Services                   0      2,928 K
lsass.exe                      560 Services                   0      5,060 K
svchost.exe                    616 Services                   0      6,252 K
svchost.exe                    644 Services                   0      4,100 K
dwm.exe                        760 Console                    1     57,596 K
vsserv.exe                     772 Services                   0    225,680 K
VBoxService.exe                                               0      3,040 K
svchost.exe                                                   0     12,352 K
svchost.exe                                                   0     26,536 K
svchost.exe                                                   0     10,020 K
svchost.exe                                                   0      9,944 K
svchost.exe                                                   0     11,240 K
spoolsv.exe                                                   0      6,264 K
svchost.exe                                                   0     12,440 K
svchost.exe                                                   0      8,256 K
ProductAgentService.exe                                       0      6,464 K
updatesrv.exe                                                 0      7,880 K
wlms.exe                                                      0      2,136 K
svchost.exe                                                   0      2,804 K
```

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



```
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0        128 K
smss.exe                       248 Services                   0        384 K
csrss.exe                      392 Services                   0      2,104 K
csrss.exe                      456 Console                    1     18,496 K
wininit.exe                    464 Services                   0      2,788 K
winlogon.exe                   492 Console                    1      3,392 K
services.exe                   552 Services                   0      2,928 K
lsass.exe                      560 Services                   0      5,060 K
svchost.exe                    616 Services                   0      6,252 K
svchost.exe                    644 Services                   0      4,100 K
dwm.exe                        760 Console                    1     57,596 K
vsserv.exe                     772 Services                   0    225,680 K
VBoxService.exe               1164 Services                   0      3,040 K
svchost.exe                   1240 Services                   0     12,352 K
svchost.exe                   1268 Services                   0     26,536 K
svchost.exe                   1300 Services                   0     10,020 K
svchost.exe                   1380 Services                   0      9,944 K
svchost.exe                   1476 Services                   0     11,240 K
spoolsv.exe                   1604 Services                   0      6,264 K
svchost.exe                                                         12,440 K
svchost.exe                                                          8,256 K
ProductAgent                                                          ,464 K
updatesrv.exe                                                         ,880 K
wlms.exe                                                              ,136 K
svchost.exe                                                           ,804 K
```

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



Potentially malicious application det... 2015-10-01- 02:19:53
The application C:\Users\IEUser\Documents\malware.exe was ...

Infected file detected 2015-09-08 - 06:38:24
Bitdefender has detected an infected item in C:\Users\IEUser\Desktop\Ne...

Infected file detected 2015-09-08 - 06:38:12
Bitdefender has detected an infected item in C:\Users\IEUser\Desktop\Ne...

Potentially malicious application detected

The applicationC:\Users\IEUser\Documents\malware.exe was detected as potentially malicious. Active Threat Control blocked this process based on the following actions:
- The application's behavior can harm your computer

Malicious application detected

Bitdefender detected and blocked a potentially malicious application.

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

- Active applications and processes are continuously monitored suspicious behaviors, like:
- Copying or moving files in System or Windows folders or limited access disk location
- Executing or injecting 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-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), Active 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.

Active Threat Control increases the detection rate of malware

A large quantity of malware samples is detected by Active Threat Control. Given that B-HAVE is one of the most advanced and effective heuristic scanning engines on the market, it is clear that Active Threat Control has the ability to provide substantially better protection than other solutions. It drastically reduces 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 detection. 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 Threat Control is Bitdefender's response 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.

FOR MORE INFORMATION VISIT: enterprise.bitdefender.com

BD-Business-Oct.12.2015-Tk#: 70594