Malwarebytes Anti-Exploit Administrators Guide

Version 1.01

25 February 2014

Notices

Malwarebytes products and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. You may copy and use this document for your internal, reference purposes only.

This document is provided "as-is." The information contained in this document is subject to change without notice and is not warranted to be error-free. If you find any errors, we would appreciate your comments; please report them to us in writing.

The Malwarebytes logo and Malwarebytes Anti-Exploit are trademarks of Malwarebytes Corporation. Windows, Windows 8, Windows 7, Windows Vista, Windows XP, Windows Server 2008 and Windows Server 2003 are registered trademarks of Microsoft Corporation. All other trademarks or registered trademarks listed belong to their respective owners.

Copyright © 2014 Malwarebytes Corporation. All rights reserved.

Contents

This page left intentionally blank

1.0 Introduction

Every week, new financial, state-sponsored and cyber-espionage targeted attacks are discovered. These sophisticated advanced persistent threats use arsenals of vulnerability exploits which have been weaponized to steal confidential information and trade secrets. Organizations remain infected while security companies rush to develop signature updates for an outdated security model.

As software vulnerabilities are discovered and disclosed, traditional approaches to securing of companies and users are based mostly on blacklisting. This applies to binaries (antivirus), spam, network attacks (IDS/IPS) and web filtering (IP/URL blacklisting). When it comes to software vulnerabilities, most vendors focus on detection on a *per attack* or *per vulnerability* basis, as it is easier to create signatures for something that is known and that can be studied in a lab.

Unfortunately, this approach is reactive in nature and does not provide enough protection as proven by the fact that new breaches are discovered on a daily basis. Existing security solutions are slow to react, since they need to be patched by receiving up-to-date malware or network attack signatures in order to provide an effective defense. While the reactive signature approach provides good and specific identification of existing attacks, it is extremely ineffective in protection against new and unknown attacks.

After researching thousands of vulnerability exploits, Malwarebytes has developed an innovative patent-pending technology that is able to detect if a shielded application is being exploited maliciously, without relying on blacklisting, whitelisting or sandboxing. By preventing the most dangerous phase of a vulnerability exploit – the execution of malware – Malwarebytes Anti-Exploit (MBAE) can protect against known and unknown zero-day arbitrary code execution vulnerability exploit attacks in a simple to use, install-and-forget endpoint security solution.

Malwarebytes Anti-Exploit protects against targeted attacks and corporate cyber-espionage. It protects where traditional security measures fail. It consists of an innovative patent-pending application shielding technology which prevents malicious exploits from compromising computers through software vulnerabilities.

Malwarebytes Anti-Exploit is vulnerability-agnostic. Unlike intrusion detection and prevention products, once an application is protected by Malwarebytes Anti-Exploit, the shielded application cannot be exploited through any of its present or future zero-day vulnerabilities. Unlike other vulnerability and intrusion detection products, Malwarebytes Anti-Exploit does not require a patient-zero infection.

Malwarebytes Anti-Exploit is malware-agnostic. Unlike antivirus and security suites, Malwarebytes Anti-Exploit does not care if the malicious payload (trojan, rootkit, rogue antivirus, virus, bot, etc.) is known and detected by antivirus signatures, heuristics or by any other means. Malwarebytes Anti-Exploit prevents malicious shellcode and payload from executing even if antivirus products cannot detect it. Malwarebytes Anti-Exploit detects what antivirus products normally miss, making it the perfect companion to traditional antivirus and security suites.

Malwarebytes Anti-Exploit is the most complete anti-exploit (or exploit mitigation) tool in the market. Unlike other similar tools, Malwarebytes Anti-Exploit incorporates multiple protection layers, which in turn are made up of multiple techniques which work in harmony to block exploit attempts at different stages of the vulnerability attack. All techniques are 100% generic and do not depend on any type of blacklisting signature updates, white-listing or sandboxing, making it extremely reliable and resilient to known as well as unknown zero-day vulnerability exploit attacks. In fact, Malwarebytes Anti-Exploit has been proven to stop hundreds of zero-day attacks without any previous knowledge of the vulnerability or the exploit.

- **Layer 1: Protection Against Operating System Security Bypasses** – This is the first and foremost protection against exploits. It consists of multiple advanced memory protection techniques to detect exploit attempts which try to bypass built-in operating system protections such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR). Examples of these techniques are attempts to bypass operating system protections using Return Oriented Programming (ROP) techniques and other such exploit techniques.
- **Layer 2: Memory Caller Protection** – This protection layer incorporates multiple memory techniques to prevent exploit code from executing from memory, such as from specific or special memory areas.

- **Layer 3: Application Behavior Protection –** This protection layer is the last defense against exploit attempts. In case an exploit is able to bypass all memory protections and/or uses sandbox escape techniques such as those typically used in Acrobat Reader and Java exploits, this layer prevents applications protected by Malwarebytes Anti-Exploit from dropping and executing the malicious payloads.

2.0 System Requirements

Following are minimum requirements for a computer system on which Malwarebytes Anti-Exploit may be installed. Please note that these requirements do not include any other functionality that the computer is responsible for.

- **Operating System:** Windows 8.1, Windows 8, Windows 7, Windows Vista, Windows XP (Service Pack 3), Windows Server 2003, Windows Server 2008. All operating systems are supported in both 32 and 64-bit editions.
- **CPU:** 800 MHz or faster
- **RAM:** 256 MB (512 MB or more recommended)
- **Free Disk Space:** 10 MB (initial, log retention may influence this number)
- **Screen Resolution:** 800x600 or higher

This page left intentionally blank

3.0 Program Installation

Malwarebytes Anti-Exploit may be installed locally via the GUI-based setup program, or remotely using a command line-based installer. For both methods, the process begins by procuring a copy of Malwarebytes Anti-Exploit. If you do not have a copy of the program in your possession, it can be downloaded from the Malwarebytes website (**https://www.malwarebytes.org/antiexploit/**) or by contacting your Malwarebytes representative.

3.1 GUI-based Installation

Malwarebytes Anti-Exploit is packaged in a single setup file, which contains all necessary components required to install, configure and operate the program. Double click on the setup file – mbae-setup-1.01.0.1000.exe – to begin installation. The installation process uses standard installation steps, which are itemized here:

- Select language to be used for installation, then click **OK** to continue.
- Installation greeting message. Click **Next** to continue.
- Read and accept the License Agreement, then click **Next** to continue.
- Read the Information panel showing new features and changes, then click **Next** to continue.
- Confirm/select alternate installation location, then click **Next** to continue.
- Select location for program shortcuts, then click **Next** to continue.
- Choose whether a desktop icon will be created, then click **Next** to continue.
- Confirm installation options, then click **Install** to continue.
- Click **Finish** to acknowledge that installation has completed.

3.2 Command Line Installation

In addition to the conventional GUI-based installation, Malwarebytes Anti-Exploit may also be installed remotely from the command line. Using this method, command line parameters can be used to tailor the install to your individual needs. As with the GUI-based installer, the process revolves around use of the setup file – mbae-setup-1.01.0.1000.exe. Command line parameters are not case-sensitive. You may specify their usage with upper or lower case characters. They are shown here in upper case for clarity.

3.2.1 Installer Command Line Switches

The following command line parameters can be used as part of the Malwarebytes Anti-Exploit installation process.

/DIR=path	Set program installation path. The default path is **`%ProgramFiles%\Malwarebytes Anti-Exploit`** (32-bit OS) or **`%ProgramFiles(x86)%\Malwarebytes Anti-Exploit`** (64-bit OS).
/LOG	Creates log file "Setup Log YYYY-MM-DD #001.txt" in **`%TEMP%`** directory
/SP-	Disables the "This will install... Do you wish to continue?" prompt at the beginning of Setup.
/VERYSILENT	Suppress installation windows and perform default install (unless /DIR is specified).
/SUPPRESSMSGBOXES	Instructs Setup to suppress message boxes. Effective only when combined with '/VERYSILENT'.
/NORESTART	Instructs Setup not to reboot even if necessary.

3.2.2 Examples of Command Line Installation

As mentioned previously, this installation model allows a system administrator to install Malwarebytes Anti-Exploit on one or more remote computers, and enables the usage of command line parameters to tailor the installation to his corporate needs. Three examples are shown here to illustrate how this method may be used.

```
psexec \\targetcomputer -u DOMAIN\administrator -p mypassword -d
       \\FILESERVER\Installers\mbae-setup-1.01.0.100.exe /log /SP- /VERYSILENT
       /SUPPRESSMSGBOXES
```

In the above example, psexec is being used to install Malwarebytes Anti-Exploit on *targetcomputer*. Authentication is required, and is provided by inclusion of the –u and –p parameters. Background operation is specified with the –d switch. A Malwarebytes Anti-Exploit installer file stored on a fileserver is being used here.

```
psexec \\* -u DOMAIN\administrator -p mypassword -d
       \\FILESERVER\Installers\mbae-setup-1.01.0.100.exe /log /SP- /VERYSILENT
       /SUPPRESSMSGBOXES
```

In the above example, *psexec* is being used to install Malwarebytes Anti-Exploit on all computers in the domain. **Please note** the target computer's specification here has been replaced with a wildcard. This allows Malwarebytes Anti-Exploit to be installed on all computers in the domain through a single execution of the installer. All other components of this command are identical to the previous example.

```
[network_agent] mbae-setup-1.01.0.100.exe /log /SP- /VERYSILENT
       /SUPPRESSMSGBOXES
```

In the above example, Malwarebytes Anti-Exploit is being installed to a remote computer using an existing network management agent.

Following installation, a setup log will be found in the **%TEMP%** directory of each computer, in the format:

```
Setup Log yyyy-mm-dd #001.LOG
```

yyyy-mm-dd corresponds to the installation date, supplemented by a sequence number (if there was more than one installation on the same computer. You can verify that Malwarebytes Anti-Exploit is installed and running following successful installation by the presence of the Malwarebytes Anti-Exploit icon in the Windows system tray.

3.2.3 Uninstaller Command Line Parameters

The uninstaller can also be used with command line parameters which tailor behavior to your individual needs. The uninstaller filename is unins000.exe. Following installation, it can be found in the Malwarebytes Anti-Exploit directory. If the default installation path was used, this location is **%ProgramFiles%\Malwarebytes Anti-Exploit** (32-bit OS) or **%ProgramFiles(x86)%\Malwarebytes Anti-Exploit** (64-bit OS). The uninstaller must be executed from this location.

/VERYSILENT — When specified, the uninstaller operates in the background. No visible indication of the process will be displayed before, during or after the uninstallation. Shared files which are no longer used are deleted automatically without prompting. Any critical error messages will still be shown on the screen. If a restart is required and the '/NORESTART' command is not used (see below), the uninstaller will reboot without asking.

/SUPPRESSMSGBOXES — Instructs the uninstaller to suppress message boxes. Only has an effect when combined with '/VERYSILENT'.

/LOG — Causes a log file to be created in the user's **%TEMP%** directory detailing file uninstallation and [UninstallRun] actions taken during the uninstallation process. This can be a helpful debugging aid. The log file is created with a unique name based on the current date. (It will not overwrite or append to existing files.) Information contained in the log file is technical in nature and is not intended to be understandable by end users. It is also not designed to be machine-parseable. The file format is subject to change without notice.

/NORESTART — Instructs the uninstaller not to reboot even if necessary.

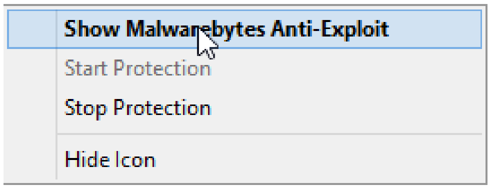
As with the command line installation model, uninstallation may be performed using *psexec* or a network agent of your choice. Individual computers are specified by the names assigned to them. Uninstallation may be performed on all computers by using a "*" wildcard in place of the computer name.

4.0 User Interface

There are two methods by which users may communicate with Malwarebytes Anti-Exploit. The first method is the graphical user interface (GUI). The GUI is available to (a) users who have installed Malwarebytes Anti-Exploit themselves, or (b) on computers where Malwarebytes Anti-Exploit has been installed by system administrators and have been granted GUI privileges by the system administrator. If the system administrator has disallowed access to the user interface (thus preventing interaction with the program), the user interface will simply be unavailable. Please see Section 5 for further information in this area. Modification of operational settings via the GUI is only available to local users with administrator privileges.

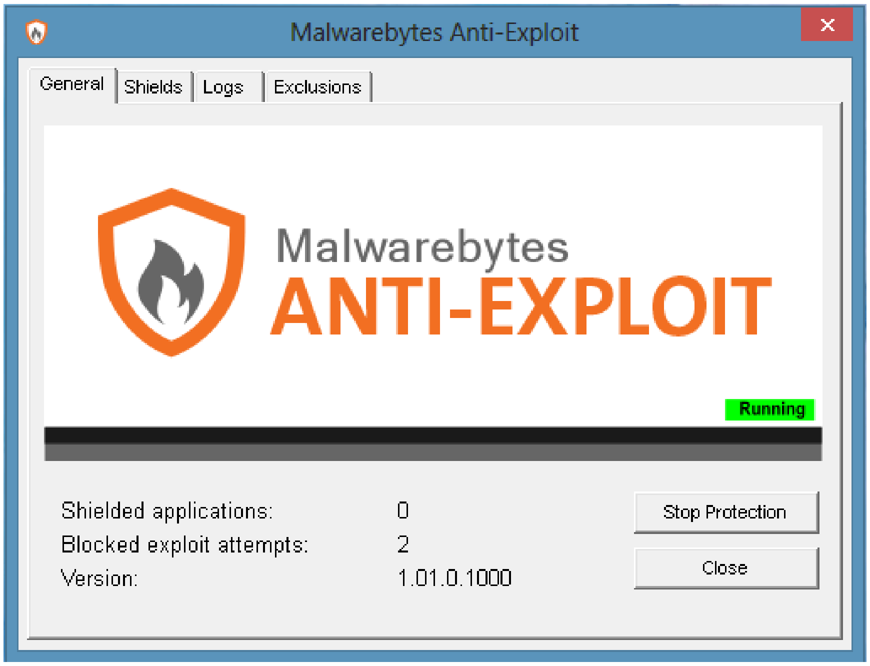
4.1 System Tray

Clicking the Malwarebytes Anti-Exploit icon in the system tray will display the menu shown below.



4.2 General Tab

The screenshot below shows the Malwarebytes Anti-Exploit main screen. It is visible initially after installing Malwarebytes Anti-Exploit (local installation only), or if launched from the system tray (as shown above). As mentioned previously, an installation performed by a system administrator may deny GUI privileges to a local user, so access to this screen may be denied based on that criteria.



Shielded applications: 0

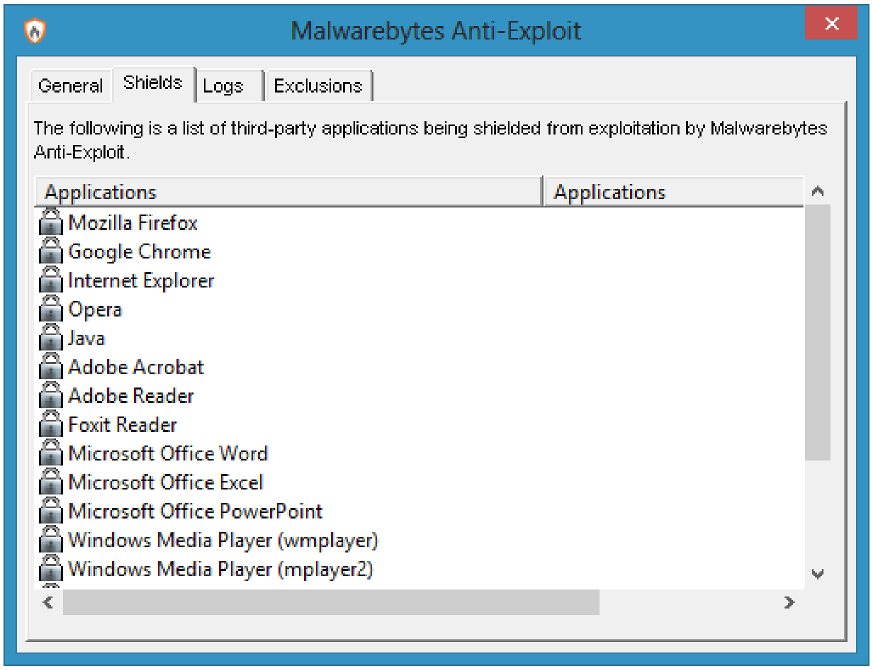
Blocked exploit attempts: 2

Version: 1.01.0.1000

Information presented in the GUI is spread across four tabs, the remaining three tabs are accessible from the *General* tab (shown here). This tab provides general status, allows users to close the interface, and allows local admins to start or stop protection.

4.3 Shields Tab

The *Shields* tab provides a visible indication of the installed applications which can be protected by Malwarebytes Anti-Exploit. The appearance of the padlock next to the application's name is an indicator of what is being protected. Let's demonstrate that.

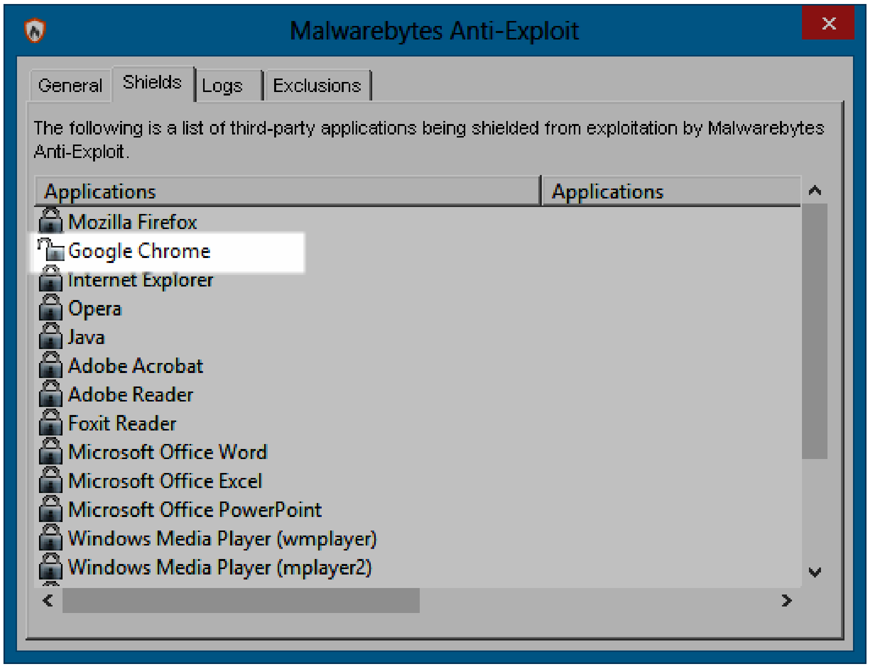


The following is a list of third-party applications being shielded from exploitation by Malwarebytes Anti-Exploit.

Applications	Applications
Mozilla Firefox	
Google Chrome	
Internet Explorer	
Opera	
Java	
Adobe Acrobat	
Adobe Reader	
Foxit Reader	
Microsoft Office Word	
Microsoft Office Excel	
Microsoft Office PowerPoint	
Windows Media Player (wmplayer)	
Windows Media Player (mplayer2)	

4.3.1 Unshielded Applications

If an application has been unshielded (i.e. protection has been turned off), a subtle change is visible on this tab. Here, protection has been removed from the Google Chrome browser application via the command line. This will be discussed more fully in Section 5. Please note the highlighted area in this screenshot.



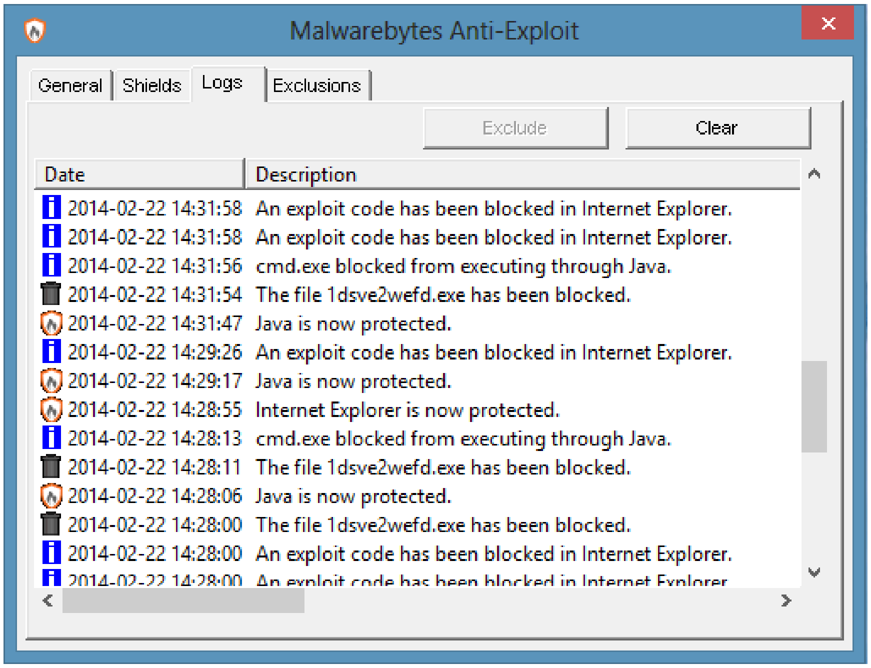
The following is a list of third-party applications being shielded from exploitation by Malwarebytes Anti-Exploit.

Applications	Applications
Mozilla Firefox	
Google Chrome	
Internet Explorer	
Opera	
Java	
Adobe Acrobat	
Adobe Reader	
Foxit Reader	
Microsoft Office Word	
Microsoft Office Excel	
Microsoft Office PowerPoint	
Windows Media Player (wmplayer)	
Windows Media Player (mplayer2)	

The padlock icon to the left of Google Chrome is now unlocked. This is a direct result of unshielding the application, and is a visible indicator to the user that this application is unprotected.

4.4 Logs Tab

The Logs tab provides a list of events related to operation of Malwarebytes Anti-Exploit. All events are displayed in reverse chronological order. There is no provision for changing the order of displayed events.



```
Date                 Description
ℹ 2014-02-22 14:31:58  An exploit code has been blocked in Internet Explorer.
ℹ 2014-02-22 14:31:58  An exploit code has been blocked in Internet Explorer.
ℹ 2014-02-22 14:31:56  cmd.exe blocked from executing through Java.
🗑 2014-02-22 14:31:54  The file 1dsve2wefd.exe has been blocked.
🛡 2014-02-22 14:31:47  Java is now protected.
ℹ 2014-02-22 14:29:26  An exploit code has been blocked in Internet Explorer.
🛡 2014-02-22 14:29:17  Java is now protected.
🛡 2014-02-22 14:28:55  Internet Explorer is now protected.
ℹ 2014-02-22 14:28:13  cmd.exe blocked from executing through Java.
🗑 2014-02-22 14:28:11  The file 1dsve2wefd.exe has been blocked.
🛡 2014-02-22 14:28:06  Java is now protected.
🗑 2014-02-22 14:28:00  The file 1dsve2wefd.exe has been blocked.
ℹ 2014-02-22 14:28:00  An exploit code has been blocked in Internet Explorer.
ℹ 2014-02-22 14:28:00  An exploit code has been blocked in Internet Explorer.
```

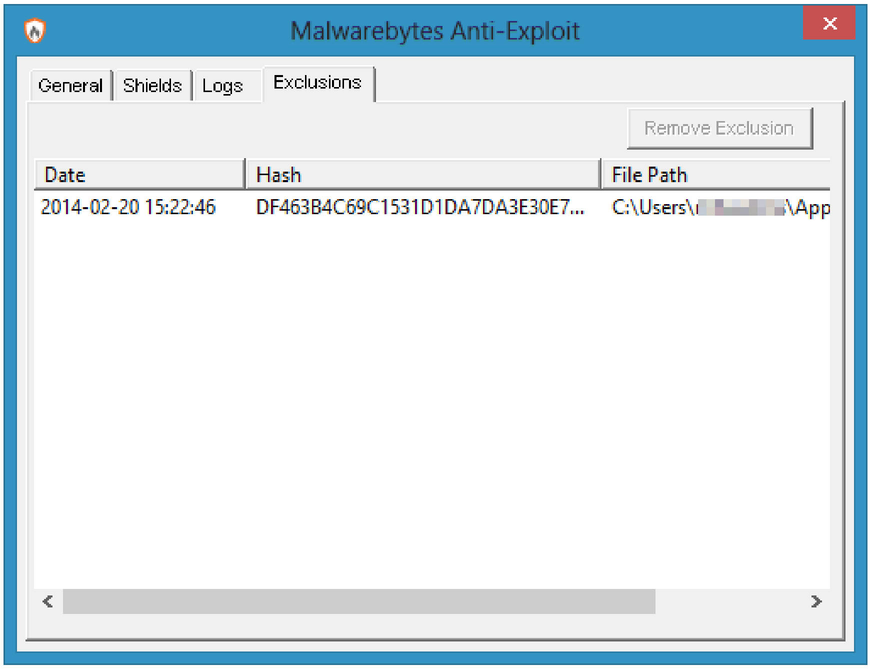
You will note three different icons being displayed to the left of the system date. These indicate the category of information being displayed, and are provided as a quick method of focusing your attention. The information categories are:

ICON	**MEANING**
🛡	Information pertaining to protection status of individual applications.
ℹ	Malwarebytes Anti-Exploit has blocked an exploit attempt. Full details of the blocking techniques used are available in file *mbae-alert.log* (see Section 8 for information on system logs).
🗑	Malwarebytes Anti-Exploit has prevented the specified program from delivering a malicious payload, according to Layer 3 mitigation techniques. For entries of this type, the program's file path and MD5 hash are also displayed for verification purposes. As a local admin, if you are familiar with the program and trust it, you can highlight the log entry and click the **Exclude** button to prevent it from being blocked in the future. **Please note** that an exclusion is based specifically on the MD5 hash of the program, and not the name of the program. If a new version of a trusted program is released using the same file name, the MD5 hash of the new version will be different than the old (excluded) version, and the previous exclusion will no longer be honored.

All information presented here is also available in system logs (to be discussed in Section 8 of this guide). If you are a local admin, you may clear this display of events shown here by clicking the **Clear** button. **Please note** that this only clears the display in the user interface. System logs remain intact.

4.5 Exclusions Tab

The *Exclusions* tab is a list of all programs which are being excluded from anti-exploit testing. Entries here may be a direct result of what Malwarebytes Anti-Exploit had considered to be an exploit attempt in the past. The exclusion shown here was added by a local admin, because the program is trusted and considered safe.



Date	Hash	File Path
2014-02-20 15:22:46	DF463B4C69C1531D1DA7DA3E30E7...	C:\Users\[redacted]\App

Referring to the *Logs* tab (above), this specific program was evaluated as a Layer 3 exploit attempt. Because it is known to be safe, it was excluded. As a result of that exclusion, an entry for the program was immediately created here on the *Exclusions* tab.

5.0 Command Line Interface

Earlier in this guide, it was shown how system administrators could use *psexec* (or other network management tools) as a means of installing Malwarebytes Anti-Exploit onto remote computers with a command line-based setup program. The same capability exists for day-to-day operation and management of remote computers, using a program named *mbam-cli*. This program is installed as part of the Malwarebytes Anti-Exploit package. When used to control Malwarebytes Anti-Exploit, it needs to execute with SYSTEM privileges. It is designed to manage program operations, and provides additional functionality not available in the GUI interface. Additionally, it has the capability to override any settings made to the remote computer *locally* using the GUI interface. Let's look at *mbam-cli* with a focus on the options which it provides.

5.1 mbae-cli Parameters

A single parameter may be used with each execution of an *mbae-cli* command, and an error code will be returned in response to the command. The following is a list of all parameters that can be used as part of an *mbae-cli* command.

/START Starts protection

/STOP Stops protection

/STATUS Checks program status (start/stopped).

/NOALERT Configures client to not show alert popup windows upon exploit detection.

/ALERT Configures client to show alert popups (and toggles status if a /NOALERT command had been sent). This is a default setting.

/NOGUI Configures client to prevent display of the traybar icon or GUI on client machines. If the user attempts to execute Malwarebytes Anti-Exploit manually, it will not launch.

/GUI Shows the traybar icon and GUI (and toggles status if a /NOGUI command has been issued). This is a default setting.

/SHIELD Shields a specific application. Must be used with correct application name. Example: "/SHIELD iexplore".

CLI SWITCH	DISPLAY NAME
iexplore	Internet Explorer
firefox	Mozilla Firefox
chrome	Google Chrome
opera	Opera
java	Java
acrobat	Adobe Acrobat
acrord32	Adobe Reader
foxitreader	Foxit Reader
winword	Microsoft Office Word
excel	Microsoft Office Excel
powerpnt	Microsoft Office PowerPoint
wmplayer	Windows Media Player (wmplayer)
mplayer2	Windows Media Player (mplayer2)
vlc	VLC Player
winamp	Winamp Player
quicktimeplayer	QuickTime Player
helpctr	Microsoft Help and Support Center
winhlp32	Windows Help
wscript	Windows Script Host

/UNSHIELD Unshields a specific application. Must be used with correct application name.

/EXCL-ADD Adds a new file to the local exclusion list. The MD5 hash of the excluded file is required as a parameter.

Example: `mbae-cli /EXCL-ADD F6C75620A1A77241C4E810C2409BADC9`

/EXCL-DEL Deletes a local exclusion. The MD5 hash of the excluded file is required as a parameter.

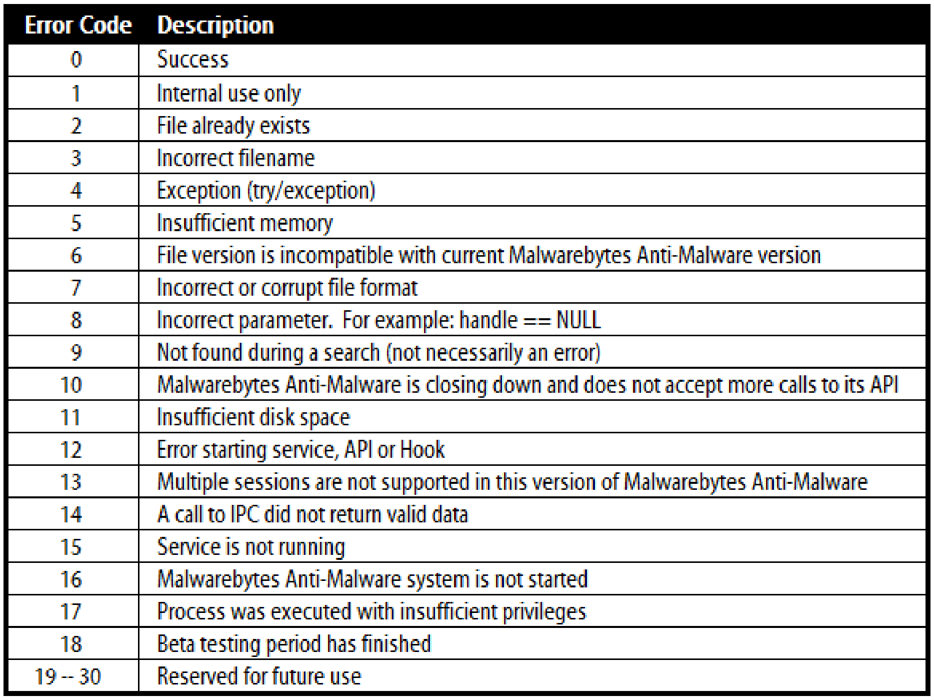
Example: `mbae-cli /EXCL-DEL F6C75620A1A77241C4E810C2409BADC9`

/EXCL-LIST <*out*> Lists exclusions previously added by mbae-cli.exe (does not include user-created local exclusions). Output is a plain text file (specified by filename <*out*>) containing a list of MD5 hashes, one per line.

Please note references here to MD5 hashes. For those who are unfamiliar, these are unique 128-bit signatures which represent both data and the order of data in a file. Virtually any modification made to a given file will result in a different hash. Malwarebytes Anti-Exploit uses MD5 hashes as a way of representing a file to be excluded or included, because the hash is much more specific than simply a file name and/or file path. An internet search will yield many free programs that can generate reliable MD5 hashes for your files.

5.2 mbae-cli Error Codes

Following is a list of all error codes that Malwarebytes Anti-Malware will return in response to commands which have been executed. Error codes may be evaluated based on testing of environmental variable **`%ERRORLEVEL%`**.



Error Code	Description
0	Success
1	Internal use only
2	File already exists
3	Incorrect filename
4	Exception (try/exception)
5	Insufficient memory
6	File version is incompatible with current Malwarebytes Anti-Malware version
7	Incorrect or corrupt file format
8	Incorrect parameter. For example: handle == NULL
9	Not found during a search (not necessarily an error)
10	Malwarebytes Anti-Malware is closing down and does not accept more calls to its API
11	Insufficient disk space
12	Error starting service, API or Hook
13	Multiple sessions are not supported in this version of Malwarebytes Anti-Malware
14	A call to IPC did not return valid data
15	Service is not running
16	Malwarebytes Anti-Malware system is not started
17	Process was executed with insufficient privileges
18	Beta testing period has finished
19 -- 30	Reserved for future use

As the above table shows, the first error code (error code 0) means the operation was successful. In most cases, it will be the desired response to an mbae-cli command. Error codes 19 through 30 have been allocated but are not currently in use. Any error code returned value higher than 30 is a Microsoft operating system error, and has been shifted higher by 30 (i.e. error code 47 is actually Microsoft error code 17).

5.3 mbae-cli Examples

Perhaps the best way to illustrate usage of mbae-cli is to provide examples of how it can be used. These examples are simplistic in nature, and have been chosen to illustrate successful and unsuccessful results. In both cases, mbae-cli is being executed from the Windows command line interface (cmd.exe), invoked with Administrator privileges. The system prompt will be displayed in abbreviated form for clarity.

5.3.1 Start Malwarebytes Anti-Exploit

In the first example, we will start Malwarebytes Anti-Exploit protection, verify success/failure, and repeat the process.

```
1:      C:\>mbae-cli /start

2:      C:\>echo %errorlevel%
        0

3:      C:\>mbae-cli /start

4:      C:\>echo %errorlevel%
        0
```

In line 1, protection was started. The error code (line 2) was returned as 0, indicating success. Another start command was issued in line 3, and the error code returned indicated success again. While protection had been successfully started already, the second attempt did not consider the original state – only that the intent was to start protection and that the result was as intended.

5.3.2 Locally Exclude a File from Malwarebytes Anti-Exploit Protection

In this example, a file will be added to the local exclusion list. In order to do this, a MD5 hash of the file was required to properly identify the file, and this was calculated prior to execution of this example. Once the file has been added to the local exclusion list, a second attempt will be made to perform the same operation.

```
1:      C:\>mbae-cli /excl-add 02cc452c1972995048eac6f3ae4477f6

2:      C:\>echo %errorlevel%
        0

3:      C:\>mbae-cli /excl-add 02cc452c1972995048eac6f3ae4477f6

4:      C:\>echo %errorlevel%
        2
```

Line 1 shows the command to exclude a file, with the file's MD5 hash used for identification purposes. Interrogating the error code shows a successful exclusion. Line 3 is a second attempt to exclude the file. Line 4 returns error code 2. Referring to the above table, error code 2 corresponds to the error "File already exists."

This page left intentionally blank

6.0 Exclusions

Usage of mbae-cli.exe is intended to be performed by a system administrator, whether it be from the command line, or via scripts executed from a network agent. Commands executed in this manner have higher privileges than those executed from within the Malwarebytes Anti-Exploit graphical interface. These primarily relate to the treatment of exclusions. Following are important distinctions to keep in mind.

1. Not all detections can be excluded. Only Layer 3 detections with file name, path and MD5 can be excluded.
2. Local exclusions added by endpoint users via the GUI must include MD5, file name and path.
3. Global exclusions added by administrator via mbae-cli.exe only include MD5 and will not show up in the GUI EXCLUSIONS tab.
4. Local exclusions may have different file names/paths even though they share the same MD5 (i.e. same file).
5. In case (4) the first added exclusion file name and path will be shown (only for local exclusions).
6. If a user or administrator tries to add an exclusion with the same MD5 as a previously-added exclusion, an error message will be returned ("file is already excluded") or error code (in the case of mbae-cli.exe).
7. An administrator may delete via mbae-cli.exe a local exclusion previously added by the user.
8. A local user may not delete a global exclusion added by administrator via mbae-cli.exe.

This page left intentionally blank

7.0 Verifying Program Functionality

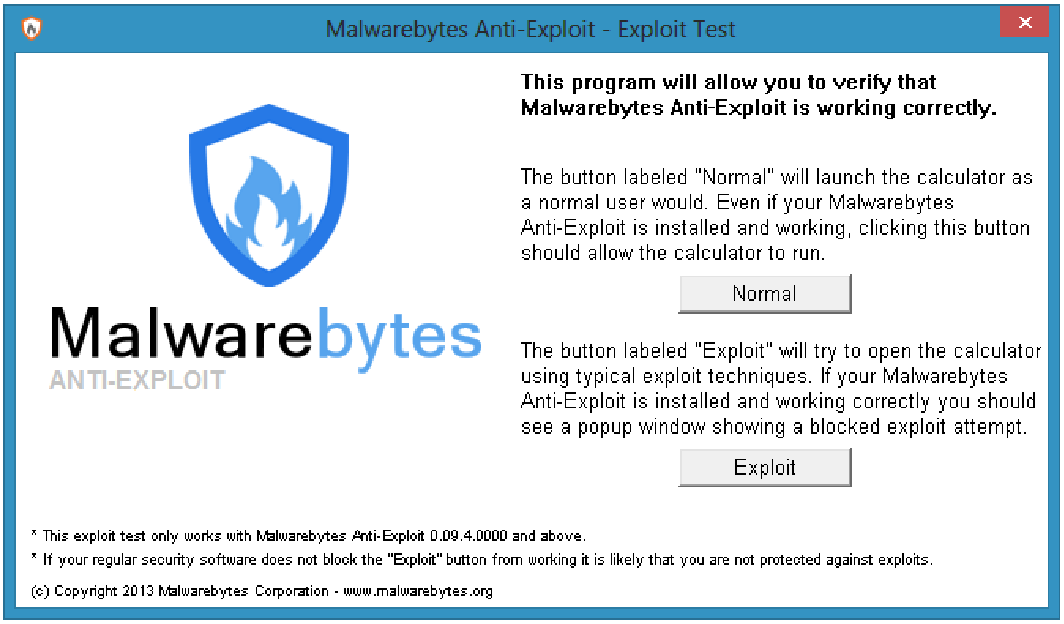
After installing Malwarebytes Anti-Exploit, you may wish to run a few tests so that you can see for yourself that it is doing its part to protect you and your computer. There are two methods you can use to confirm its functionality.

7.1 Exploit Tester

Malwarebytes has made a simple exploit tester available for separate download on our public forums. The forum post provides a download link, as well as an explanation of the exploit tester's behavior. The link to read about (and download) the tester is:

https://forums.malwarebytes.org/index.php?showtopic=139368

After downloading and extracting the exploit tester to a directory of your choice, double click it to launch the tester. You will see the exploit tester as shown below.



This program will allow you to verify that Malwarebytes Anti-Exploit is working correctly.

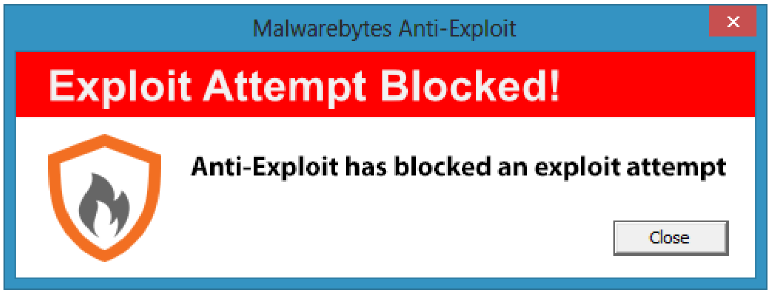
The button labeled "Normal" will launch the calculator as a normal user would. Even if your Malwarebytes Anti-Exploit is installed and working, clicking this button should allow the calculator to run.

The button labeled "Exploit" will try to open the calculator using typical exploit techniques. If your Malwarebytes Anti-Exploit is installed and working correctly you should see a popup window showing a blocked exploit attempt.

* This exploit test only works with Malwarebytes Anti-Exploit 0.09.4.0000 and above.
* If your regular security software does not block the "Exploit" button from working it is likely that you are not protected against exploits.

(c) Copyright 2013 Malwarebytes Corporation - www.malwarebytes.org

The screenshot provides instructions which allow you to perform the test. After clicking the Exploit button, you will see results of the test, as shown below.



Exploit Attempt Blocked!

Anti-Exploit has blocked an exploit attempt

This is the same message that you would see during normal program operation if an exploit attempt has been detected and blocked.

7.2 DLL Injection Verification

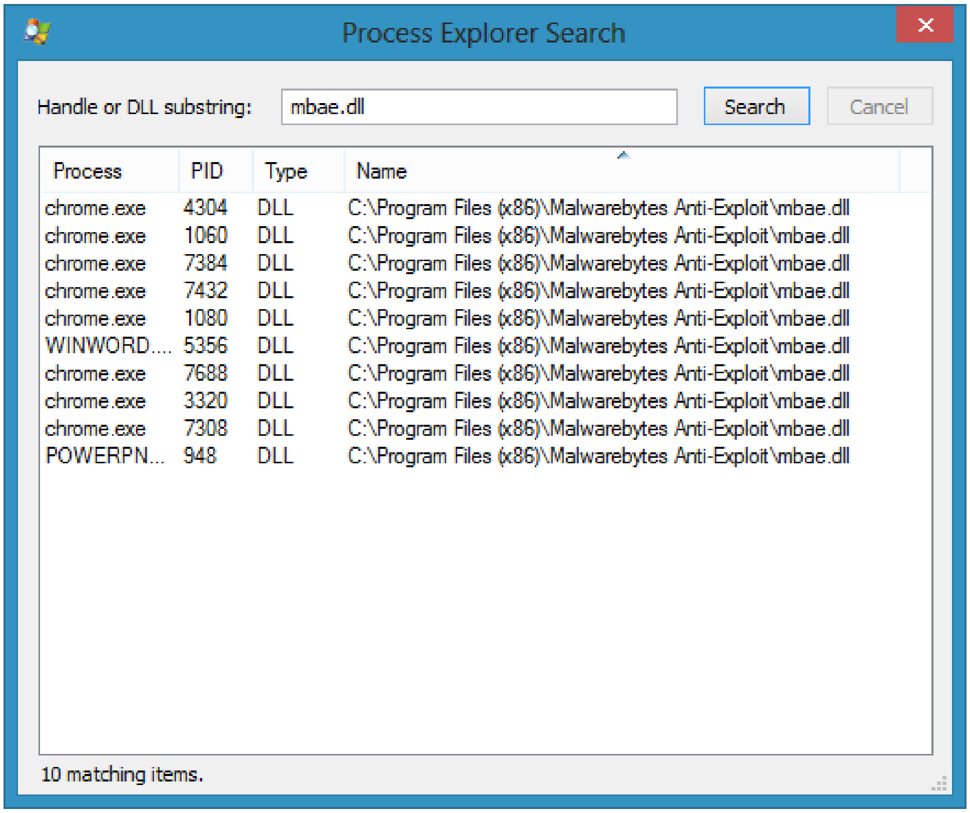
This method – which is also described in the forum post (referred to in the previous section) – provides a more technical approach to verifying Malwarebytes Anti-Exploit functionality. When protecting an application, Malwarebytes Anti-

Exploit uses a method referred to as DLL Injection. This method allows Malwarebytes Anti-Exploit to monitor input/output functionality of protected programs to guard against potentially malicious activity.

You can use a task management utility such as Process Explorer to view running processes and tasks. It is downloadable at the following link:

http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx

The utility's Find function will allow you to investigate DLL usage in running processes. The screenshot below shows an example of this.



Handle or DLL substring: mbae.dll

Process	PID	Type	Name
chrome.exe	4304	DLL	C:\Program Files (x86)\Malwarebytes Anti-Exploit\mbae.dll
chrome.exe	1060	DLL	C:\Program Files (x86)\Malwarebytes Anti-Exploit\mbae.dll
chrome.exe	7384	DLL	C:\Program Files (x86)\Malwarebytes Anti-Exploit\mbae.dll
chrome.exe	7432	DLL	C:\Program Files (x86)\Malwarebytes Anti-Exploit\mbae.dll
chrome.exe	1080	DLL	C:\Program Files (x86)\Malwarebytes Anti-Exploit\mbae.dll
WINWORD....	5356	DLL	C:\Program Files (x86)\Malwarebytes Anti-Exploit\mbae.dll
chrome.exe	7688	DLL	C:\Program Files (x86)\Malwarebytes Anti-Exploit\mbae.dll
chrome.exe	3320	DLL	C:\Program Files (x86)\Malwarebytes Anti-Exploit\mbae.dll
chrome.exe	7308	DLL	C:\Program Files (x86)\Malwarebytes Anti-Exploit\mbae.dll
POWERPN...	948	DLL	C:\Program Files (x86)\Malwarebytes Anti-Exploit\mbae.dll

10 matching items.

Here, we have run a search for mbae.dll. This is the dynamic link library (DLL) that Malwarebytes Anti-Exploit uses to inject itself into applications which have been designated for protection. In this instance, there are ten protected processes as shown in search results.

8.0 Logs

Malwarebytes Anti-Exploit maintains operational information in a number of program logs. A few of these logs are pertinent here, as they maintain dynamic information on the application. In addition, you may be called upon to provide information from these logs to Malwarebytes Technical Support if you require technical support. These logs are stored in **%AllUsersProfile%\Malwarebytes\Malwarebytes Anti-Exploit**. That translates to:

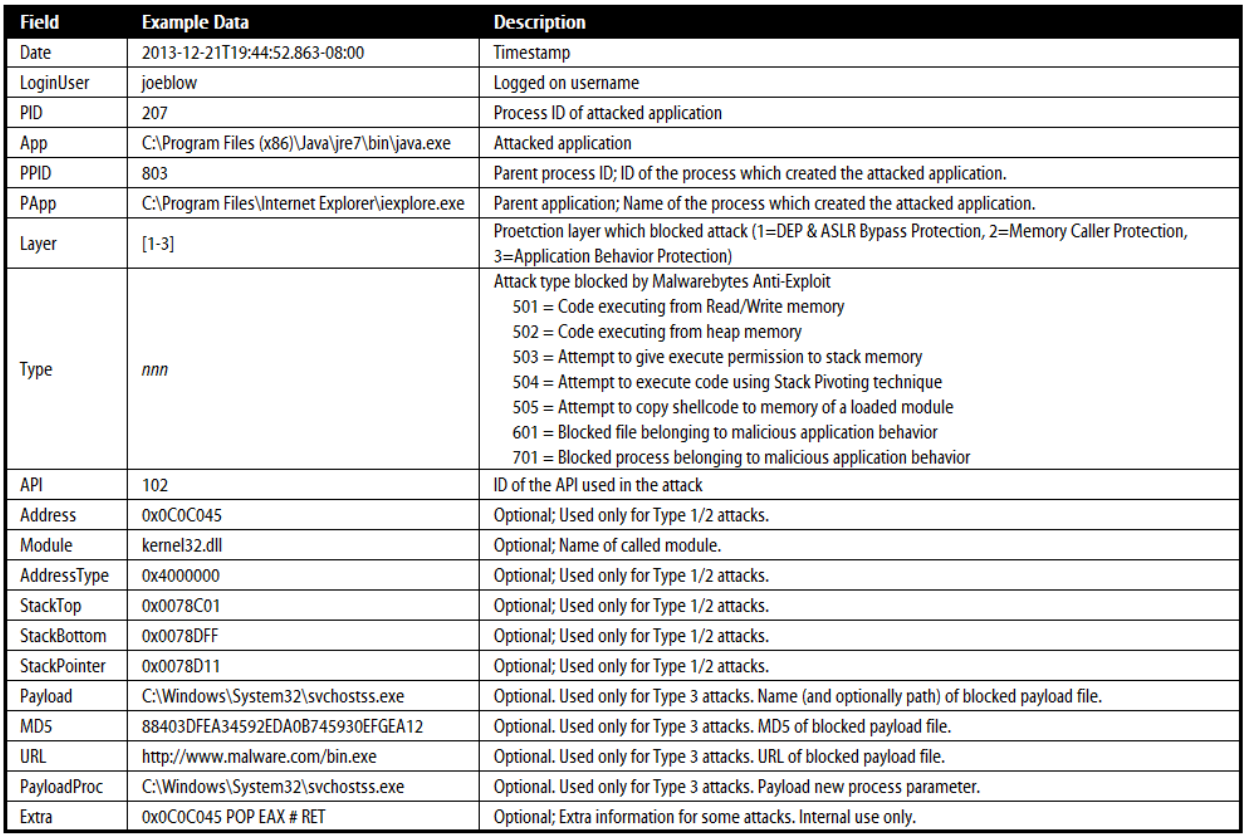
Windows XP:	**C:\Documents and Settings\All Users\Application Data\Malwarebytes\Malwarebytes Anti-Exploit**
Windows Vista/7/8:	**C:\ProgramData\Malwarebytes\Malwarebytes Anti-Exploit**

Please note that **%AllUsersProfile%** may map to a different directory on a computer that is configured for a language other than English. Following is a complete listing of all log files related to Malwarebytes Anti-Exploit.

Log File	Purpose
applications.dat	List of protected applications.
exclusions.dat	Whitelist. Files excluded by the user or administrator.
mbae-alert.log	Alert details; Can be imported into centralized reporting platform.
mbae-default.log	Internal troubleshooting information.
mbae-service.log	System events and information; Can be imported into centralized reporting platform.
mbae-config.dat	Global Settings; Protection enabled, GUI enabled, Alerts enabled, etc.
mbae-report.dat	Report displayed by GUI application.
mbae-svc.dat	Report pending to be notified to GUI application.
mbae-protector.xpe	For use by Malwarebytes Tech Support for troubleshooting.

8.1 mbae-alert.log

This file contains detailed information pertaining to each event Malwarebytes Anti-Exploit has acted in response to.



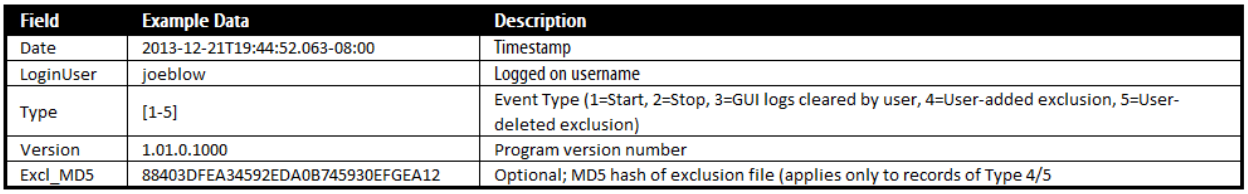
Field	Example Data	Description
Date	2013-12-21T19:44:52.863-08:00	Timestamp
LoginUser	joeblow	Logged on username
PID	207	Process ID of attacked application
App	C:\Program Files (x86)\Java\jre7\bin\java.exe	Attacked application
PPID	803	Parent process ID; ID of the process which created the attacked application.
PApp	C:\Program Files\Internet Explorer\iexplore.exe	Parent application; Name of the process which created the attacked application.
Layer	[1-3]	Proetction layer which blocked attack (1=DEP & ASLR Bypass Protection, 2=Memory Caller Protection, 3=Application Behavior Protection)
Type	*nnn*	Attack type blocked by Malwarebytes Anti-Exploit 501 = Code executing from Read/Write memory 502 = Code executing from heap memory 503 = Attempt to give execute permission to stack memory 504 = Attempt to execute code using Stack Pivoting technique 505 = Attempt to copy shellcode to memory of a loaded module 601 = Blocked file belonging to malicious application behavior 701 = Blocked process belonging to malicious application behavior
API	102	ID of the API used in the attack
Address	0x0C0C045	Optional; Used only for Type 1/2 attacks.
Module	kernel32.dll	Optional; Name of called module.
AddressType	0x4000000	Optional; Used only for Type 1/2 attacks.
StackTop	0x0078C01	Optional; Used only for Type 1/2 attacks.
StackBottom	0x0078DFF	Optional; Used only for Type 1/2 attacks.
StackPointer	0x0078D11	Optional; Used only for Type 1/2 attacks.
Payload	C:\Windows\System32\svchostss.exe	Optional. Used only for Type 3 attacks. Name (and optionally path) of blocked payload file.
MD5	88403DFEA34592EDA0B745930EFGEA12	Optional. Used only for Type 3 attacks. MD5 of blocked payload file.
URL	http://www.malware.com/bin.exe	Optional. Used only for Type 3 attacks. URL of blocked payload file.
PayloadProc	C:\Windows\System32\svchostss.exe	Optional. Used only for Type 3 attacks. Payload new process parameter.
Extra	0x0C0C045 POP EAX # RET	Optional; Extra information for some attacks. Internal use only.

Following is a sample of how log data appears in its native format. Please note that all data is surrounded by quotation marks for consistent handling by other programs. Each log record is a single line of data. It is shown in multiple lines due to line wrapping.

```
"2013-12-21T19:44:52.863-08:00";"joeblow";"207";"C:\Program Files
(x86)\Java\jre7\bin\java.exe";"803";"C:\Program Files\Internet
Explorer\iexplore.exe";"3";"701";"102";"0x0C0C045";"kernel32.dll";"0x4000000";"
0x0078C01";"0x0078DFF";"0x0078D11";"C:\Windows\System32\svchostss.exe";"88403DF
EA34592EDA0B745930EFGEA12";"http://www.malware.com/bin.exe";"C:\Windows\System3
2\svchostss.exe";"0x0C0C045 POP EAX # RET"
```

8.2 mbae-service.log

This file contains detailed information pertaining to administration of Malwarebytes Anti-Exploit. Contents of this file are of value if troubleshooting a Malwarebytes Anti-Exploit control issue.



Field	Example Data	Description
Date	2013-12-21T19:44:52.063-08:00	Timestamp
LoginUser	joeblow	Logged on username
Type	[1-5]	Event Type (1=Start, 2=Stop, 3=GUI logs cleared by user, 4=User-added exclusion, 5=User-deleted exclusion)
Version	1.01.0.1000	Program version number
Excl_MD5	88403DFEA34592EDA0B745930EFGEA12	Optional; MD5 hash of exclusion file (applies only to records of Type 4/5

Five sample records are shown here, illustrating each of the event types.

```
"2013-12-21T19:44:52.863-08:00";"joeblow";"1";"1.01.0.1000";""

"2013-12-21T21:10:45.123-08:00";"joeblow";"2";"1.01.0.1000";""

"2013-12-25T08:08:08.008-08:00";"joeblow";"3";"1.01.0.1000";""

"2013-12-26T21:15:35.321-
08:00";"joeblow";"4";"1.01.0.1000";"88403DFEA34592EDA0B745930EFGEA12"

"2013-12-26T23:22:06.566-
08:00";"joeblow";"5";"1.01.0.1000";"88403DFEA34592EDA0B745930EFGEA12"
```

Appendix A – File List

Following is a list of all log, configuration and program files associated with Malwarebytes Anti-Exploit

Folder Name: **%AllUsersProfile%\Malwarebytes\Malwarebytes Anti-Exploit**
Created by: Installer, with read, write and modify permissions for all "authenticated users".

Log/Config File	Purpose
applications.dat	List of protected applications
exclusions.dat	List of excluded files; Files are marked as known *goodware*
mbae-alert.log	Alert details; Described in Section 8.1
mbae-default.log	Internal troubleshooting information
mbae-service.log	System events and information; Described in Section 8.2
mbae-config.dat	Global Settings: Protection enabled, GUI enabled, alerts enabled, etc.
mbae-report.dat	Report displayed by the user interface
mbae-svc.dat	Report pending to be notified to the user interface
mbae-protector.xpe	For use by Malwarebytes Tech Support for troubleshooting

Folder Name (32-bit): **%ProgramFiles%\Malwarebytes Anti-Exploit**
(64-bit): **%ProgramFiles(x86)%\Malwarebytes Anti-Exploit**
Created by: Installer, with default permissions.

Program File	Purpose
changelog.txt	Changelog for the current version
license.rtf	End User License Agreement (EULA)
mbae-svc.exe	Windows service which implements all backend functionality
mbae.dll	Protection DLL (32-bit)
mb-lib.dll	Malwarebytes libraries for telemetry function and others in the future.
mbae64.dll	Protection DLL (64-bit)
mbae.exe	Graphical user interface (GUI)
mbae64.exe	Used for injection and uninjection of 64-bit processes
mbae-api.dll	DLL that implements the API for 32-bit processes
mbae-api64.dll	DLL that implements the API for 64-bit processes
mbae-cli.exe	Implements the command line interface
mbae.sys	32-bit kernel hooking module
mbae64.sys	64-bit kernel hooking module
uninsXXX.dat	Installation information for uninstaller
uninsXXX.exe	Uninstaller