Malwarebytes
BREACH REMEDIATION

Forensic Timeliner
Administrator Guide

Version 4.0

10 September 2020

Notices

Third Party Project Usage

Malwarebytes software is made possible thanks in part to many open source and third party projects. A requirement of many of these projects is that credit is given where credit is due. Information about each third party/open source project used in Malwarebytes software – as well as licenses for each – are available on the following page.

https://service.malwarebytes.com/hc/en-us/articles/4414986433683

Sample Code in Documentation

The sample code described herein is provided on an "as is" basis, without warranty of any kind, to the fullest extent permitted by law. Malwarebytes does not warrant or guarantee the individual success developers may have in implementing the sample code on their development platforms. You are solely responsible for testing and maintaining all scripts.

Malwarebytes does not warrant, guarantee or make any representations regarding the use, results of use, accuracy, timeliness or completeness of any data or information relating to the sample code. Malwarebytes disclaims all warranties, express or implied, and in particular, disclaims all warranties of merchantability, fitness for a particular purpose, and warranties related to the code, or any service or software related there to.

The Malwarebytes Protection Strategy

Malwarebytes' products incorporate several prevention features which utilize a layered defense strategy to protect you against malware threats which you face daily. Each layer is designed to disrupt the attack chain at a different stage. While all Malwarebytes products are highly effective in dealing with attacks that are becoming all too commonplace, we can only assure your protection when you take advantage of the full product suite, allowing each prevention layer to do the job they are best suited for.

It's your data. Protect it wisely!

Table of Contents

Introduction

Malwarebytes Forensic Timeliner (timeliner.exe, or "*Timeliner*") is a standalone tool, used to generate and display forensic system timelines on Windows systems. It is written in C++ using the Windows API, and is packaged as a single portable Windows executable (EXE) that runs on all modern versions of Windows (Win7 SP1 through Windows 10 clients, 32/64-bit, Server 2008 through Server 2012 R2 (32/64-bit), and has no dependencies other than standard Windows DLLs. *Timeliner* must be run either as SYSTEM or as a local administrator on the machine.

Timeliner is intended to be used to retrospectively discover and display indicators of prior malware infection, notably the malware's source (when was the malware first created/downloaded/encountered, and where did it come from) and the malware's effects (what other files or artifacts did the malware create, delete, or modify). *Timeliner's* data sources are chosen to help answer these specific questions. For example, the browser history data sources might indicate where on the Internet some malware was downloaded from, and the USN Journal data source might indicate what files the malware might have dropped on the system when executed.

What's New

The following changes have been made in this version of *Malwarebytes Forensic Timeliner*:

- Add valid SSL Certificates while deploying/unzipping Timeliner to fix expired certificates.
- Ensure proper activation by verifying Machine ID Check is complete prior to termination of redemption process.

Key Features

The following are key features included in *Timeliner*:

- Collect and Export Windows full system historical timeline from many data sources
- Supported log formats include CSV and Event log (CEF)
- Ability to filter/exclude events that may be uninteresting or irrelevant from data sources

System Requirements

Following are minimum requirements for an endpoint on which *Timeliner* may be installed. Please note that these requirements do not include other functionality that the endpoint is responsible for.

- **Operating System:** Windows 10, Windows 8.1, Windows 8, Windows 7, Windows Server 2012/2012 R2, Windows Server 2008/2008 R2.

  PLEASE NOTE: Windows servers using the Server Core Installation process are specifically excluded

- **CPU:** 800 MHz or faster
- **RAM:** 4 GB (8 GB or more recommended)
- **Free Disk Space:** 1 GB (Note: Output files can exceed 200MB each time *Timeliner* is executed)
- **Screen Resolution:** 800x600 or higher
- **Active Internet Connection**, for license validation and client updates
- **USB 2.0 Port** (optional, depending on deployment method)

External Access Requirements

If your company's Internet access is controlled by a firewall or other access-limiting device, you must grant access for *Timeliner* to reach Malwarebytes services. Please assure access is available for:

https://keystone.mwbsys.com
https://telemetry.malwarebytes.com

Using Malwarebytes Forensic Timeliner

Timeliner is designed specifically for use by IT staff. It may be deployed to an endpoint by local insertion of a USB drive which contains the program, or by pushing the program out to the endpoint using psexec, Powershell, or any other deployment method which you may currently use.

License Key Status

Timeliner uses a license key, which was provided to you upon your purchase of the client. Once registered, the license key is considered active for 14 calendar days – unless a different time interval was specified at time of purchase. Each time the client is used on an endpoint, license status is checked. If your license deactivates (times out), you cannot perform critical operations that the client is intended for. If this occurs, you must re-register the client. This is to prevent unauthorized use of the client. There is no additional cost to re-register the client.

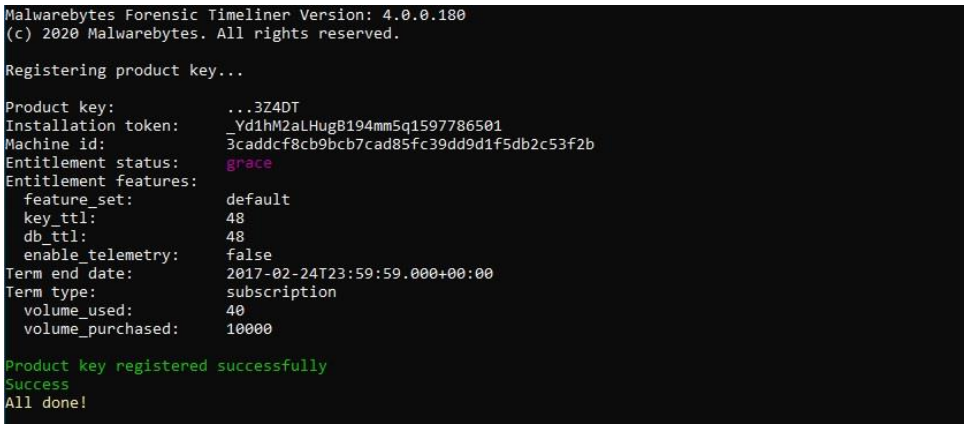
Getting Started

Getting started with *Timeliner* is very simple. Malwarebytes Forensic Timeliner is shipped as a single executable file (**`timeliner.exe`**). When this executable is run for the first time on the endpoint, it will extract all program and configuration components. Once all components have been extracted, the program is available for use on the endpoint.

Using an endpoint with a live Internet connection, access an elevated Windows command line prompt (run as Administrator) and issue the following commands:

```
timeliner.exe register –key:<prodkey>
```

Please note: You must substitute your license key for **`<prodkey>`** in the above example. The screenshot below shows what you can expect to see for a successful client registration.



Operations

The basic functionality of *Timeliner* is to:

1. Generate a full system historical timeline from the available data sources
2. Search that timeline for particular events by date/time or filename/path
3. Filter out events that may be uninteresting or irrelevant
4. Print out remaining relevant events to a CSV file or send them to an external log system (SIEM, Syslog)

When searching a timeline (Step #2, above), *Timeliner* can be run in one of four basic modes of operation:

1. **[-all]:** outputs a full system timeline,

2. **[-target ...]:** searches for a particular filename or path, or website name or partial path
3. **[-date ...]:** searches for a particular date/time
4. **default:** searches for events today (equivalent to **-date NOW**).

For full details of usage and command line syntax, see the documentation provided by running **timeliner.exe** (the program name with no arguments).

Data Sources

Timeliner utilizes Windows data sources to generate historical timelines for malware incursions and potential incursions. All data sources are subclasses of the **TimelineSource** abstract class. The following is a list of data sources which are added to the timeline, in alphabetical order.

DATA SOURCE	PURPOSE
ADS (aka. AlternateData)	An Alternate Data Stream is a Windows feature that is often used for hiding malicious code. It is also used for many legitimate purposes. Only files with alternate data streams are added to the timeline.
AppCompatCache	This is a record of file name, size, last modification and last execution. While a listed file may not have been actually executed, its existence in cache shows that Windows has interacted with the file.
ChromeBrowserHistory	This provides the Chrome browser history of visited websites.
EventLog	This is a record of user login, logout and system startup events
FirefoxBrowserHistory	This provides the Firefox browser history of visited websites.
IEBrowserHistory	This provides the Internet Explorer browser history of visited websites.
JavaCache	This is a record of all loaded Java applets as recorded by Java's IDX Cache.
Jumplist	Jumplists are lists of recently opened files which are available to an application from the Windows Start Menu.
MFT	The Master File Table contains a record of known file creation times.
MRU	The Most Recently Used List is a chronological record of files which have been opened or accessed.
MUICache	The MUI Cache contains a list of applications which have been executed.
NetworkMap	This is a record of all networked drives which have served as mapped drives for the endpoint.
Prefetch	Prefetch entries aid in speeding up launch of an application. They also contain a record of DLLs used by an application as well as the most recent run time of the application.
RecentFiles	This is a record of shortcuts (*.lnk files) to files recently executed by the user.
RegistryModified	This is an aggregate record of last-modified dates for a variety of registry keys.
Schedule Task	This is a record of tasks which have been scheduled for later or periodic execution.
Shellbags	This is used to enumerate past mounted volumes, deleted files, and user actions.
ShimCache	Used in conjunction with AppCompatCache, this source contains a record of files which have created processes during execution.
USBDrives	This is a record of all USB key attach/detach events
UserAssist	The UserAssist registry key allows determination of how, when and how often programs are launched, on a user-by-user basis.

USN Journal	Uses the Update Sequence Number Journal (change log) to identify all file create, delete, and rename events.
WinShares	This is a record of folders whose read/write access rights have been changed to make the folder available to others.

Notes about individual data sources:

- The **USN Journal** is a circular buffer, and typically contains data for only the last 3-5 days of operation. Based on activity level on the endpoint in question, data may cover more *or* less time.
- The registry data sources (**ShimCache**, **UserAssist**, **MUI**, and **MRU**) are only sometimes present and reliable. They are not complete lists of executed programs. Windows does not maintain a complete list of executed programs.
- **Prefetch** is our most reliable indicator of execution, but it is disabled by default when Windows is installed on a solid-state drive (SSD).

…and some notes about data sources as a whole…

- Because many data sources used by *Timeliner* are ephemeral (notably the **USN Journal**, a circular buffer of unknown size), *Timeliner* should be run as soon as possible after a compromise, but before an anti-malware scan or remediation (which can destroy many indicators used by *Timeliner*).
- Browsers (notably Chrome and Firefox) should be closed during a *Timeliner* run. If left open, their history files will be locked and unavailable to Timeliner.
- In order to retrieve timeline events from all user accounts on the machine, *Timeliner* loads user HKCU registry hives (ntuser.dat) into temporary storage under HKU.
- In order to retrieve timeline events from both x86 and x64 native views of the registry on 64-bit versions of Windows, *Timeliner* disables Wow64 redirection for both the registry and the filesystem. Registry redirection is disabled in individual calls to *RegOpenKeyEx*, while filesystem redirection is disabled explicitly by calls to *Environment::DisableFilesystemRedirection* from *Main*.
- Windows API calls are used to read both the MFT and the USN Journal.
- Timeline events with unknown dates are currently stored at "time 0", or "0000-00-00 00:00:00". These events appear in timelines constructed using the **"collect -date"** switch, unless **"settings -exclude.timeBefore"** is specified (default).

Event Logging

When *Timeliner* executes, it produces a log (CSV format) which you may save to a filename of your choice. The screenshot below is a sample from a log produced by *Timeliner.*

Log Time	Data Source	File Path	Event Type	Detail
2018-11-27T07:00:18.364000-05:00	ADS	C:\ProgramData\TEMP	alternate data	ADS name list: 792D4CF1
2018-10-24T07:32:00.930000-04:00	ADS	C:\temp\Upload.url	alternate data	ADS name list: StreamedFileState
2018-10-03T17:19:18.283000-04:00	BagMRU	Desktop\Shared Documents Folder (Users Files)\source\repos\Drawing_Fractal_Images\	Validating_the_Histogram\	ShellBags
2018-10-03T17:19:18.267000-04:00	BagMRU	Desktop\Control Panel\All Control Panel Items\		ShellBags
2018-12-23T13:41:51.597000-05:00	ChromeHistory	http://www.google.com/	website visited	
2018-12-23T13:41:51.019000-05:00	EventLog	CLW-2801$	user logoff	
2018-12-23T13:41:51.019000-05:00	EventLog	CLW-2801$	user logon	
2018-12-23T13:41:51.019000-05:00	EventLog		system startup	
2018-12-23T13:41:50.910000-05:00	EventLog	jsmith	user logoff	
2018-12-23T13:41:50.910000-05:00	EventLog	UMFD-1	user logon	
2018-12-23T13:41:50.020000-05:00	EventLog	DWM-1	user logon	
2018-12-23T13:41:50.020000-05:00	InternetExplorerHistory	file:///C:/work	website visited	
2018-12-23T13:41:50.020000-05:00	InternetExplorerHistory	https://support.office.com/client/results?NS=OUTLOOK&Version=16&Lcid=1033&SysLcid	website visited	
2018-12-23T13:41:49.926000-05:00	JumpListFiles	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe --win-jumplist-action=r	JumpLists	5d696d521de238c3
2018-12-23T13:41:49.926000-05:00	MFT	C:\Windows\Prefetch\TIMELINER.EXE-BDC6A321.pf	file created	
2018-12-23T13:41:49.926000-05:00	MRU	C:\Users\jsmith\Desktop\2018-10-16-CLW-2801.zip	file executed	
2018-12-23T13:41:49.723000-05:00	Prefetch	C:\WINDOWS\SYSTEM32\WIN32U.DLL	file executed	
2018-12-23T13:41:49.723000-05:00	Prefetch	C:\WINDOWS\SYSTEM32\SAMCLI.DLL	file executed	
2018-12-23T13:41:48.801000-05:00	Prefetch	C:\WINDOWS\SYSTEM32\WIN32U.DLL	file executed	
2018-12-23T13:41:48.801000-05:00	Prefetch	C:\WINDOWS\SYSTEM32\WINDOWS.SECURITY.AUTHENTICATION.ONLINEID.DLL	file executed	
2018-12-23T13:41:48.801000-05:00	Prefetch	C:\WINDOWS\SYSTEM32\SAMCLI.DLL	file executed	
2018-12-23T13:41:48.645000-05:00	Prefetch	C:\PROGRAM FILES\MALWAREBYTES\ANTI-MALWARE\MBAE64.DLL	file executed	
2018-12-23T13:41:48.645000-05:00	RecentFiles	C:\Users\jsmith\Documents\Malwarebytes Forensic Timeliner 1.01 Administrator Guide.	file executed	
2018-12-23T13:41:48.645000-05:00	RegistryModified	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{5e164bc1-00dc	registry key (subkey or value) modified	
2018-12-23T13:41:47.817000-05:00	USNJournal	\\?\C:\Users\jsmith\AppData\Local\Temp\etilqs_SChSaTQz1YqahZM	file created	
2018-12-23T13:41:47.817000-05:00	USNJournal	\\?\C:\ProgramData\Malwarebytes\MBAMService\LOGS\mbae-protector.xpe	file written	
2018-12-23T13:41:47.583000-05:00	USNJournal	\\?\C:\ProgramData\Malwarebytes\MBAMService\config\MbamClientConfig.json	file truncated	
2018-12-23T13:41:47.583000-05:00	USNJournal	\\?\C:\Users\jsmith\AppData\Local\Microsoft\Windows\Caches\cversions.3.db	file overwritten	
2018-12-23T13:41:47.192000-05:00	USNJournal	\\?\C:\Users\jsmith\AppData\Roaming\Microsoft\Windows\CloudStore\Store\3BDD44B	file security changed	
2018-12-23T13:41:47.192000-05:00	USNJournal	\\?\C:\Users\jsmith\AppData\Local\MicrosoftEdge\SharedCacheContainers\MicrosoftEd	file renamed FROM (deleted)	
2018-12-23T13:41:47.192000-05:00	USNJournal	\\?\C:\Users\jsmith\AppData\Local\MicrosoftEdge\SharedCacheContainers\MicrosoftEd	file renamed TO (created)	
2018-12-23T13:41:46.958000-05:00	USNJournal	\\?\C:\Users\jsmith\AppData\Local\MicrosoftEdge\SharedCacheContainers\MicrosoftEd	file attributes changed	
2018-12-23T13:41:46.958000-05:00	USNJournal	\\?\C:\Users\jsmith\AppData\Local\Microsoft\Group Policy\History\{688CF64C-9E86-486	file created	
2018-12-23T13:41:46.958000-05:00	USNJournal	\\?\C:\Users\jsmith\AppData\Local\Microsoft\Group Policy\History\{688CF64C-9E86-486	file written	

Event Logging to syslog

Timeliner integrates very easily into a corporate network, allowing simplified deployment to endpoints as well as subsequent forensic analysis. That includes event logging using industry-standard methods. We have implemented logging using CEF (Common Event Format), and output is tailored to the ArcSight Security Intelligence platform and others which support CEF.

Pages 7-8 describes settings which control logging to your existing SIEM. While *Timeliner* automatically generates output files for each program execution, CEF logging is only performed after the feature has been enabled and properly configured.

Command Line Parameters

Timeliner supports a variety of command line parameters, which can be used from a command prompt, batch file or script. When used from a script, additional commands may be required to support the scripting model being used.

Conventions

The command line structure uses modifiers. These are shown as hyphens (-) immediately preceding parameters. Multiple modifiers may be combined with a parameter. When multiple parameters are used, they must be separated by spaces. In addition, the following conventions are used:

- **text without brackets or braces**
  Items you must type as shown
- **<text inside angle brackets>**
  Required information for which you must supply a value
  Example: **timeliner.exe <*parameter_1*>**
- **[text inside square brackets]**
  Optional items
  Example: **timeliner.exe [*parameter_1*]**
- **Grouping of dots (…)**
  A set of specifications
  Example: **timeliner.exe <*parameter _1*> [*parameter_2*] … [*parameter_n*]**
- **{text inside braces}**
  A set of required items; choose one from the list provided
  Example: **timeliner.exe {0 | 1 | 2 | 3}**
- **vertical bar (|)**
  Separator between mutually exclusive items; choose one
  Example: **timeliner.exe <0 | 1 | 2 | 3>**

Command Line Overview

Timeliner commands are specified in the following format:

timeliner.exe { version | register | errorout | collect | settings } [*options*]

Following is a list of high-level commands which may be executed. Each command is detailed beginning on the next page.

version	Displays the program version number.
register	Using your license key, this unlocks the features of *Malwarebytes Forensic Timeliner*. This will also show license status.
errorout	Specifies where error output is directed to.
collect	Defines specifications to be used for data collection, followed by collection itself.
settings	Used to specify universal program settings. These settings are persistent, and are used for program settings which tend to be constants.

In addition, you may type **timeliner** without any additional specifications to see a list of valid commands. This list will span multiple windows if the command line is launched to its default size, so you will achieve best results by stretching the window to show more command line dialog at one time.

Command Line Reference

Commands listed here are listed individually. These are primarily used by a system administrator via script, batch file, GPO update, or Remote Desktop. The admin may configure *Timeliner* to operate as a remote task while the endpoint is not in use. When executed from a script, additional commands may be required to support the scripting model being used.

version

Usage:

timeliner.exe version

Purpose:

Displays the program version number.

Parameters:

none

register

Usage:

timeliner.exe register [-key:<*prodkey*>]

Purpose:

Specifies the unique license key assigned to the partner or customer. This is passed to the licensing server for validation to ensure it is active (non-expired). **A live Internet connection is required.** If the key is valid and the license is active, it will also display status about the license (expiration date, volume purchased, volume used, etc.).

If the key is active, the local installation will operate with this status for 14 calendar days (or the time interval specified in your Malwarebytes license agreement). This "Last Known Good" status is persisted on the USB or wherever the binaries are stored. This allows the USB installation to work as if it were fully registered on offline endpoints or without needing the key.

If **-key** is not specified, license status and the expiration date/time are displayed. **Please note:** If the key is not active, the user may not update threat signature databases, scan for malware, list quarantine contents, or restore files from quarantine.

Parameters:

-key:<*prodkey*>

Specification of <*prodkey*>, the license key assigned to the user.

errorout

Usage:

timeliner.exe [[–console:{on | off }] [–delete] [–errlog:< *file*>] | [–reset]]

Purpose:

Specifies where error output will be directed to. Values set using this command will persist until they are cleared or modified. Issuing this command without arguments will display current settings.

Parameters:

–console:{off | on}

Specifies if error output is displayed on the console. Default value is ON.

–delete

Deletes the output file, if it exists. This command uses the default error log location, unless the error log location has been changed using the **–errlog** switch.

–errorlog:<*file*>

Specifies the log location for error output. This will overwrite any previously-specified location. If <*file*> contains any embedded spaces, please enclose <*file*> in double quotes (“). The default location is **.\logs\MBBR-ERROUT.TXT**.

–reset

Reverts settings associated with this command back to default values.

collect

Usage:

timeliner.exe collect [-all]
[-target:<*string*>]
[-date:<*dateString*>]
[-output:<*fileName*>]
[-excludeTypes:<*eventTypes*>]
[-includeTypes:<*eventTypes*>]

Purpose:

Collects forensic data related to possible malware incursions based on criteria specified by the user here. System data may be specified by inclusion of text strings, date/time, and may be set to include or exclude specified event types. Specifications provided here are often changed, so they are not included in **settings**.

Parameters:

-all

All available system data will be collected.

-target:<*string*>

Text string to be searched for in the path, or details data fields (See the sample log File). The string is not case-sensitive. Only data containing this string in the path, or details will be collected.

-date:<*dateString*>

The earliest date/time that data will be collected for. The format for <*dateString*> is:

`yyyy-mm-dd hh:mm:ss.msec`

All times are local time, and use the 24-hour “military” clock. If a time is not specified, the beginning of the day is used (0 h, 0 m, 0 s, 0 ms). **Please note** that exclude times (before and after, as specified in **settings**) use this parameter as a reference to the date/times that they represent.

-output:<*fileName*>

Filename which will contain requested data after collection. If a filename is specified, it will override the default filename and save the output file to the program home directory unless a different directory is specified as part of the filename. The default log filename is:

`forensic-log-<hostname>-<yyyy>-<mm>-<dd>-<hh>-<mm>-<ss>`

-excludeTypes:<*eventType_1*>[,*eventType_2*,*eventType_n*]

Event types to be excluded from data collection. When multiple event types are listed, they should be separated by commas. You may use **-excludetypes** or **-includetypes** during a single instance of data collection, but not both.

Event Message types which may be specified are:

CollectStartEvent	CollectEvent	CollectEndEvent

CollectEvent types which may be specified are:

AlternateData	FileRenamedFrom	RegistryKeyModified

FileAttributesChanged	FileRenamedTo	Shares
FileCreated	FileSecurityChanged	SystemStartup
FileDeleted	FileTruncated	
	USBDriveAttachedDetached	
FileEncryptedDecrypted	FileWritten	UserLogoff
FileExecuted	JumpLists	UserLogon
FileExecutedSubsequent	NetworkMap	WebsiteVisited
FileOverwritten		

-includeTypes:<*eventType_1*>[,*eventType_2*,*eventType_n*]

Event types to be included in data collection. When multiple event types are listed, they should be separated by commas. You may use **-excludetypes** or **-includetypes** during a single instance of data collection, but not both. See parameter **-excludetypes** for a list of event types which may be specified.

settings

Usage:

timeliner.exe settings [-exclude.browserTIF:true | false]
[-exclude.oprphaned:true | false]
[-exclude.temporary:true | false]
[-exclude.goodDirs:true | false]
[-exclude.recycled:true | false]
[-log.enabled:true | false]
[-log.server:<host>]
[-log.port:<port>]
[-log.netprotocol:<tcp|udp>]
[-log.syslogformat:<default|hp>]
[-log.allevents:on|off]
[-log.events:<eventname>:on|off]
[-log.test]
[-log.clear]
[-exclude.export:<filename>]
[-exclude.import:<filename>]
[-exclude.timeBefore:<time>]
[-exclude.timeAfter:<time>]
[-exclude.installBefore:<time>]
[-proxy.clear]
[-proxy.enabled:true|false]
[-proxy.server:<host>]
[-proxy.port:<port>]
[-proxy.user:<user>]
[-proxy.password:<password>]
[-proxy.useauth: true|false]
[-useStaticURLs: true|false]
[-color:on|off]
[-resetAll]

Purpose:

This parameter allows a user to define settings that will be used as default specifications for all executions of *Timeliner*. While these settings may be modified at any time, they are typically rather static in nature. Typing **"timeliner.exe settings"** with no additional parameters will display current program settings.

Parameters:

-exclude.browserTIF:true | false

Determines whether browser Temporary Internet Files (TIF) are excluded (true) or included (false). The default value is false. A list of all folders containing Temporary Internet Files can be found in Appendix A.

-exclude.orphaned:true | false

Determines whether orphaned file entries are excluded. Orphaned files sometimes come into existence after they have been deleted, their parent directory entry has been deleted, and the space used by the parent directory entry in the Master File Table has been reallocated. The default value is true.

-exclude.temporary:true | false

Determines whether temporary files and folders are excluded (true) or included (false). The default value is false.

-exclude.goodDirs:true | false

Determines whether activity for *known good* folders is excluded from data collection. These folders are listed as [well-known folders] in Appendix A. The default value is true. **Please note** that when gathering data for specific directories (rather than the default "*all*" directories), you may wish to change the value of this parameter to false.

-exclude.recycled:true | false

Determine whether contents of the Windows Recycle Bin is excluded. The default value is false.

-log.enabled:true | false

Specifies whether program execution is logged to a syslog server. All data utilizes a CEF (Common Event Format) standard. If this parameter is set to *true*, the syslog *host* IP/FQDN and *port* number must also be specified before event logging can take place. The default value is false.

-log.server:<host>

IP address or Fully-Qualified Domain Name (FQDN) of a syslog server which will receive event logs generated by *Timeliner*. A valid *port* number must also be specified before logging can take place.

-log.port:<port>

Valid port number for the syslog server which will receive event logs generated by *Timeliner*. A valid syslog *host* specification must also be specified before logging can take place.

-log.netprotocol:<tcp|udp>

Specifies whether the TCP or UDP protocol is used to send data to a syslog server. TCP is the default.

-log.syslogformat:<default|hp>

Set syslog CEF format to Default or HP format.

-log.allevents:on|off

Sets all syslog logging for all events On or Off. All events are on by default.

-log.events:<eventname>:on|off

Enables/disables syslog logging for each individual potential event which may be logged

-log.test

Responds with a text message indicating success or failure in communicating

-log.clear

Clears all Log settings.

-exclude.export:<filename>

Filename that the exclusion list is exported to, typically to allow editing of the list. Filename must be a valid Windows path/filename. If the filename includes embedded spaces, the entire filename must be surrounded by double quotes (“).

-exclude.import:<filename>

Filename that the exclusion list is imported from. Filename must be a valid Windows path/filename. If the filename includes embedded spaces, the entire filename must be surrounded by double quotes (“).

-exclude.timeBefore:<relative time>

Exclude data collection for records written to data sources before the specified time. The default value is 1d (one day). You may specify time increments with letters w (weeks), d (days), h (hours), m (minutes), s (seconds) or l (lower case L, representing milliseconds). **Please note** the following:

- All time increments are relative to the date/time specified in **collect –date**.
- You may combine multiple time specifications (i.e. 1w2d).
- You may collect data for time windows by combining **timeBefore** and **timeAfter**.

-exclude.timeAfter:<relative time>

Exclude data collection for records written to data sources after the specified time. The default value is 1d (one day). You may specify time increments with letters w (weeks), d (days), h (hours), m (minutes), s (seconds) or l (lower case L, representing milliseconds). **Please note** the following:

- All time increments are relative to the date/time specified in **collect –date**.
- You may combine multiple time specifications (i.e. 1w2d).
- You may collect data for time windows by combining **timeBefore** and **timeAfter**.

-exclude.installBefore:<relative time>

Exclude data collection for files created before the specified time. The default value is 7d (seven days). You may specify time increments with letters w (weeks), d (days), h (hours), m (minutes), s (seconds) or l (lower case L, representing milliseconds). Please note that time increments are relative to the time that collection begins.

[-proxy.clear]

Clear all existing proxy settings

[-proxy.enabled:true|false]

Specifies whether a proxy server is required to access the licensing server. If this parameter is set to *true*, the proxy server host IP/FQDN and port number must also be specified. If authentication is required for proxy access, the user name and password associated with the user name must also be specified. The default value is false (disabled).

[-proxy.server:<host>]

IP address or Fully-Qualified Domain Name (FQDN) of a proxy server used to access the licensing server. If this parameter is specified, the port must also be specified. If proxy usage is disabled, this parameter is ignored.

[-proxy.port:<port>]

Valid port number for the proxy server used to access the licensing server. If proxy usage is disabled, this parameter is ignored.

[-proxy.user:<user>]

User name when proxy usage is enabled and authentication is required. If a password is required, it must also be specified. If proxy usage is disabled, this parameter is ignored.

[-proxy.password:<password>]

Password for user when proxy usage is enabled. If proxy usage is disabled, this parameter is ignored.

[-proxy.useauth: true|false]

Enable/disable authentication.

[-useStaticURLs: true|false]

Enable/disable use of static URLs for registering and updates.

[-color:on|off]

Turn color display on or off.

[-resetAll

Reset all settings to defaults.

Logging events to syslog

Malwarebytes Forensic Timeliner integrates very easily into a corporate network, providing highly effective results in the detection and remediation of threats on endpoints. That integration has been extended further through the addition of event logging using industry-standard methods. Based on user requests, we have implemented logging using CEF (Common Event Format), and more specifically, output is tailored to the ArcSight Security Intelligence platform and others which support the CEF format.

This section of the guide is devoted to detailed descriptions of how we have implemented event logging, so that you may easily understand log results and customize reporting in your specific environment.

Construction of a Log Entry

All event logs use a standardized format, which consist of an external logger prefix, a header and an extension. They are described as follows:

- **syslog prefix:** A mandatory entry that is applied for compliance with syslog standards. It includes:
    - **Event date**, including month, day and year, in the format (e.g. **Jul 15 2015**)
    - **Event time**, using 24-hour clock, in the format **hh:mm:ss** (e.g. **12:25:40**)
    - **Hostname** which logs pertain to (e.g. **SFO-VM1234.internal.contoso.com**)
- **Header:** Mandatory fields which identify the product/client generating log entries. Vendors may use non-standard field names for these fields, but their usage must correspond to fields and their order within the log record.
    - **CEF Version**, in the format "CEF:<*version*>". <*version*> is a single-digit, and is used for compliance with the ISO 8601 CEF standard as well as to specify how remaining data should be interpreted.
    - **Device Vendor** identifies the vendor of the product/client which is generating log entries. As it pertains here, this will be "Malwarebytes"
    - **Device Product** identifies the product/client which is generating log entries. As it pertains here, this will be "Malwarebytes Breach Remediation"
    - **Device Version** identifies the product/client version. Malwarebytes Forensic Timeliner is identified not only by the version of the executable, but also by each major components used in conjunction with the program. All components which follow the executable program version are bounded by square brackets. Those components are:
        - Swiss Army Knife
    - **Signature ID** is a unique numeric identifier which Malwarebytes has assigned to each event message type. A full list of all Signature IDs can be found later in this section.
    - **Name** is a simple text description for each Collection Event that corresponds to a specific Signature ID
    - **Severity** is the relative importance of any event, with 1 being the least important and 10 representing a critical event.
- **Extension:** This is a series of fields which are not mandatory by CEF standards. These fields represent values that each vendor select for inclusion in their event logs. Because these fields are not mandatory, vendors will commonly use non-standard field names, and may also include labels for the non-standard fields. If a customer elects to use these labels, this would improve readability of log information, though the same label used by multiple vendors may also create confusion for the user.

Mapping Malwarebytes Fields to CEF Format

As mentioned previously, log entries are comprised of three separate sections. The *syslog prefix* and *Header* are mandatory, and must conform to rigid standards. The *extension* provides flexibility that vendors require to capture important details related to their products/clients, while still conforming to CEF standards. Malwarebytes is no exception.

CEF Field Usage

sorted by CEF Standard Field Name

	CEF Standard Field Name	Malwarebytes Field Name	Type	Description -or- Explicit Value
CEF Header				
	deviceEventClassId	EventId	integer	Event type
	deviceProduct	ProductName	string	Product name
	deviceVendor	Company	string	Product vendor's name
	deviceVersion	ProductVersion	string	Product version
	Name	EventName	string	Event name
	Severity	Severity	integer	Severity (1=min, 10=max)
CEF Extension				
	act	Action	string	Action taken with regard to malware
	cat	MalwareCategory	string	Either "pu" or "virus"
	cs1	MalwareName	string	Name of detected malware
	cs2	MalwareHash	string	MD5 hash of detected malware
	cs3	SessionId	string	UUID for each MBBR session
	cs4	MalwareClass	string	Identifies object type containing malware
	cs5	CommandLine	string	Command with arguments executed by user
	deviceMacAddress	MACAddress	MAC	MAC address of host where MBBR runs
	dvchost	Hostname	string	Hostname where MBBR runs
	end	DateTime	time	Event End Date/Time
	filePath	FilePath	string	Location of detected malware
	msg	*	string	Multi-purpose text string
	outcome	Result	string	"succeeded", "failed" Scan commands also allow "stopped", "cancelled"
	rt	DateTime	time	Event Date/Time
	start	DateTime	time	Event Start Date/Time
	suser	UserName	string	Name of user who runs MBBR

As mentioned previously, *msg* is a multi-purpose field. The CEF format provides six fields which may contain custom data, that which the vendor has determined to be important with relation to their product/client, but does not conform to a standard CEF field. Malwarebytes utilizes five of these six fields, and also utilizes *msg* to provide more robust log content. Its usage in each log message will be detailed in the next section.

Timeliner Log Events

Malwarebytes Forensic Timeliner currently generates log entries for nine different event categories. This section of the guide describes each of those categories in detail. The following table lists fields which are common to all log entries created by *Malwarebytes Forensic Timeliner*.

	CEF Standard Field Name	Malwarebytes Field Name	Description -or- Explicit Value
CEF Header			
	deviceVendor	Company	"Malwarebytes"
	deviceProduct	ProductName	"Malwarebytes Forensic Timeliner"
	deviceVersion	ProductVersion	Version of program
CEF Extension			
	cs3	SessionId	UUID for each Timeliner session
	dvchost	Hostname	Hostname where Timeliner runs
	deviceMacAddress	MACAddress	MAC address of host where Timeliner runs
	cs5	CommandLine	Command with arguments executed by user
	outcome	Results	"succeeded", "failed" Scan commands also allow "stopped", "cancelled"
	suser	UserName	Name of user who runs Timeliner

In addition to these common fields, the following events utilize several fields specific to the event being logged. The remainder of this section is devoted to descriptions of each of these events.

3000 – CollectStartEvent

3000	CollectStartEvent	Generated when a Collect command is initiated		
	EventName	Severity	Fields	Mapping
	CollectStarted	1	CollectType(string)	msg **Format:** "start=%s" **Value(s):** none
			Time	start

3001 – CollectEvent

3001	CollectionEvent	Generated when a Collect Event occurs		
	EventName	Severity	Fields	Mapping
	CollectArtifact	1	Action	act
			LogTime	cs1 real-time
			Data Source	cs2
			File Path	cs3
			Event Type	cs4
			Detail	cs5

3002 – CollectEndEvent

3002	CollectEndEvent	Generated when a Collect command ends		
	EventName	Severity	Fields	Mapping
	CollectEnded	1	CollectedCount(int)	msg **Format:** "end=%s msg=CollectedCount:%d" **Value(s):** CollectionCount(int)
			Time	start

Further reading

Malwarebytes recommends that you obtain a copy of the following document from ArcSight. It is a detailed guide pertaining to the CEF logging format, as well as their recommendations targeted to users and developers.

Implementing ArcSight CEF *(Revision 20, dated 05 June 2013)*
https://protect724.hp.com/docs/DOC-1072

Appendix A: Data Source Exclusions

Default settings for excluded folders used by *Timeliner* are listed below. You can add (exclude from reporting) or remove (include in reporting) an excluded folder at will. To add a new folder to be excluded, simply insert it after a new line in the corresponding folder section. Only one folder may be listed per line, and the allowable wild card is '*'. To remove an excluded folder, you may delete it or put a semicolon in front of the folder entry. To include a subfolder under an excluded folder, you must insert it under the excluded folder and put a '+' in front of the folder entry. Here is an example:

\Windows\AppCompat	Do not report on files in this folder tree
+*\Windows\AppCompat\Programs*	Report on files in this folder tree

To bring the new settings into effect, please run:

```
timeliner setting -exclude.import:<filename>
```

Where **<filename>** is the name of the file which the exclude list was previously exported to. This method provides granularity to allow inspection of the file system.

[well-known folders]

\.git
*.obj
*.lck
*\pagefile.sys
*\Config.Msi
\$Extend
\System Volume Information
\Users\sshd_server
\Users\NTUSER.DAT*
\Windows\AppCompat
\Windows\AppReadiness
\Windows\assembly
\Windows\Boot
\Windows\Fonts
\Windows\IME
\Windows\inf
\Windows\Logs
*
\Windows\Installer
\Windows\L2Schemas
\Windows\Microsoft.NET
\Windows\Microsoft .NET
\Windows\PolicyDefinitions
\Windows\Registration
\Windows\rescache
\Windows\ServiceProfiles
\Windows\Servicing
\Windows\SoftwareDistribution
\Windows\System32\catroot
\Windows\System32\catroot2
\Windows\System32\config
\Windows\System32\DriverStore\FileRepository
\Windows\System32\GWX
\Windows\System32\LogFiles
\Windows\System32\MsDtc
\Windows\System32\spool
\Windows\System32\spp
\Windows\System32\sru
\Windows\System32\Sysprep
\Windows\System32\Tasks\Microsoft
\Windows\System32\wdi
\Windows\System32\wbem\Performance
\Windows\System32\wbem\Repository
\Windows\Winsxs
\AppData\Local\Packages\Microsoft.
\AppData\LocalLow\Microsoft
\AppData\Roaming\Microsoft\Windows\Themes
\ProgramData\Microsoft
+*\ProgramData\Microsoft\Windows\Start Menu*
\Microsoft\Windows\Sqm
\Microsoft\Windows\Recent\AutomaticDestinations
\Microsoft\Windows\Recent\CustomDestinations
\SystemIndex\Indexer\CiFiles
\3M
\Acronis
\Adobe
\Apple Computer
\ArcSoft
\ASUS
\ATI Technologies
\AVAST Software
\Avira
\Bonjour
\Box
\Box Sync
\Broadcom
\Carbonite

\CCleaner
\Cisco Systems
\Cisco
\Citrix
\Common Files\Adobe
\Common Files\Apple
\OpenSSH
\OpenVPN Technologies
\Panda USB Vaccine
\QuickTime
\Realtek
\Reference Assemblies

[well-known folders] (continued)

\Common Files\Java
\Common Files\Microsoft Shared
\Common Files\VMware
\COMODO
\CrashPlan
\CyberLink
\Dell
\Dropbox
\EPSON Software
\Fiddler2
\Fitbit Connect
\Foxit Reader
\G Data
\Google
\Hewlett-Packard
\HP
\Intel
\Internet Explorer
\iPod
\iTunes
\Java
\Kaspersky Lab
\LANDesk
\LastPass
\Lenovo
\Logitech
\Malwarebytes Anti-Exploit
\Malwarebytes Anti-Malware
\McAfee
\Microsoft Analysis Services
\Microsoft Games
\Microsoft Office 15
\Microsoft Office
\Microsoft Silverlight
\Microsoft SQL Server Compact Edition
\Microsoft SQL Server
\Microsoft Sync Framework
\Microsoft Synchronization Services
\Microsoft Visual Studio 8
\Mozilla
\Mozilla Firefox
\Mozilla Maintenance Service
\NVIDIA Corporation
\Reference Assemblies\Microsoft
\SAMSUNG
\Sandboxie
\Seagate
\Skype
\Sophos
\Spotify
\Stardock
\Steam
\Symantec
\TAP-Windows
\TeamViewer
\TechSmith
\TextPad 5
\Thunderbird
\TOSHIBA
\Trend Micro
\uTorrent
\USOShared
\USOPrivate
\VideoLAN
\VLC
\VMware
\WebEx
\Webroot
\Western Digital
\WindowsApps
\Windows Defender
\Windows Journal
\Windows Kits
\Windows Mail
\Windows Mail
\Windows Media Player
\Windows Multimedia Platform
\Windows NT
\Windows Photo Viewer
\Windows Portable Devices
\Windows Sidebar
\WindowsPowerShell
\WinRAR
\WinZip
\Wireshark
\Yahoo!

[temporary folders]

*.tmp
\Temp

*.temp

[browserTIF folders]

\Firefox
\Chrome
\Cache
\Temporary Internet Files
\Content.IE5
\History.IE5
\Cookies
\INetCache
\INetCookies
*.sbstore
*.cache
*.pset
*\Windows\System32\IE11WIN10_*

[recycle bin folders]

\RECYCLER
\RECYCLED
\$Recycle.Bin

Appendix B Mapping Data Sources to Event Types

The following list maps the event types which data may be collected for, and the data sources where this data originated.

Available filtering event types are:

EVENT TYPE	DATA SOURCE
AlternateData	ADS
FileAttributesChanged	USN Journal
FileCreated	MFT
	USN Journal
FileDeleted	USN Journal
FileEncryptedDecrypted	USN Journal
FileExecuted	AppCompatCache
	JavaCache
	MRU
	MUICache
	Prefetch
	RecentFiles
	RegistryLoadPoints
	ShimCache
	UserAssist
	WinJob
FileExecutedSubsequent	ShimCache
FileOverwritten	USN Journal
FileRenamedFrom	USN Journal
FileRenamedTo	USN Journal
FileSecurityChanged	USN Journal
FileTruncated	USN Journal
FileWritten	USN Journal
JumpLists	JumpListFiles
NetworkMap	NetworkMap
RegistryKeyModified	RegistryLoadPoints
Shares	WinShares
SystemStartup	EventLog
USBDriveAttachedDetached	USBDrives
UserLogoff	EventLog
UserLogon	EventLog
WebsiteVisited	ChromeBrowserHistory
	FirefoxBrowserHistory
	IEBrowserHistory