TREND MICRO

# 5.5 Deep Discovery Analyzer

## Syslog Content Mapping Guide

Breakthrough Protection Against APTs and Targeted Attacks


Endpoint Security


Network Security


Protected Cloud

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

http://docs.trendmicro.com



Document Part No.: APEM57272/151216

Release Date: December 2015

Protected by U.S. Patent No.: Patents pending.

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp

# Table of Contents

## Index

# Preface

## Preface

Learn more about the following topics:

# Documentation

The documentation set for Deep Discovery Analyzer includes the following:

**TABLE 1. Product Documentation**

| DOCUMENT | DESCRIPTION |
|---|---|
| Administrator's Guide | PDF documentation provided with the product or downloadable from the Trend Micro website.<br><br>The Administrator's Guide contains detailed instructions on how to configure and manage Deep Discovery Analyzer, and explanations on Deep Discovery Analyzer concepts and features. |
| Installation and Deployment Guide | PDF documentation provided with the product or downloadable from the Trend Micro website.<br><br>The Installation and Deployment Guide contains information about requirements and procedures for planning deployment, installing Deep Discovery Analyzer, and using the Preconfiguration Console to set initial configurations and perform system tasks. |
| Syslog Content Mapping Guide | PDF documentation provided with the product or downloadable from the Trend Micro website.<br><br>The Syslog Content Mapping Guide provides information about log management standards and syntaxes for implementing syslog events in Deep Discovery Analyzer. |
| Quick Start Card | The Quick Start Card provides user-friendly instructions on connecting Deep Discovery Analyzer to your network and on performing the initial configuration. |
| Readme | The Readme contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, known issues, and product release history. |

| Document | Description |
|---|---|
| Online Help | Web-based documentation that is accessible from the Deep Discovery Analyzer management console.<br><br>The Online Help contains explanations of Deep Discovery Analyzer components and features, as well as procedures needed to configure Deep Discovery Analyzer. |
| Support Portal | The Support Portal is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Support Portal, go to the following website:<br><br>http://esupport.trendmicro.com |

View and download product documentation from the Trend Micro Online Help Center:

http://docs.trendmicro.com/en-us/home.aspx

# Audience

The Deep Discovery Analyzer documentation is written for IT administrators and security analysts. The documentation assumes that the reader has an in-depth knowledge of networking and information security, including the following topics:

- Network topologies
- Database management
- Antivirus and content security protection

The documentation does not assume the reader has any knowledge of sandbox environments or threat event correlation.

# Document Conventions

The documentation uses the following conventions:

**TABLE 2. Document Conventions**

| CONVENTION | DESCRIPTION |
|---|---|
| UPPER CASE | Acronyms, abbreviations, and names of certain commands and keys on the keyboard |
| **Bold** | Menus and menu commands, command buttons, tabs, and options |
| *Italics* | References to other documents |
| `Monospace` | Sample command lines, program code, web URLs, file names, and program output |
| **Navigation** > **Path** | The navigation path to reach a particular screen<br>For example, **File** > **Save** means, click **File** and then click **Save** on the interface |
|  **Note** | Configuration notes |
|  **Tip** | Recommendations or suggestions |
|  **Important** | Information regarding required or default configuration settings and product limitations |
|  **WARNING!** | Critical actions and configuration options |

# About Trend Micro

As a global leader in cloud security, Trend Micro develops Internet content security and threat management solutions that make the world safe for businesses and consumers to exchange digital information. With over 20 years of experience, Trend Micro provides top-ranked client, server, and cloud-based solutions that stop threats faster and protect data in physical, virtual, and cloud environments.

As new threats and vulnerabilities emerge, Trend Micro remains committed to helping customers secure data, ensure compliance, reduce costs, and safeguard business integrity. For more information, visit:

http://www.trendmicro.com

# Chapter 1

# Introduction

The Deep Discovery Analyzer Syslog Content Mapping Guide provides information about log management standards and syntaxes for implementing syslog events in Trend Micro Deep Discovery Analyzer.

To enable flexible integration with third-party log management systems, Deep Discovery Analyzer supports the following syslog formats:

| Log Management System | Description |
|---|---|
| Common Event Format (CEF)<br><br>For details, see *Syslog Content Mapping - CEF on page 2-1* | CEF is an open log management standard created by HP ArcSight.<br><br>Deep Discovery Analyzer uses a subset of the CEF dictionary. |
| Log Event Extended Format (LEEF)<br><br>For details, see *Syslog Content Mapping - LEEF on page 3-1* | LEEF is an event format developed for IBM Security QRadar.<br><br>Deep Discovery Analyzer uses a subset of the LEEF dictionary. |
| Trend Micro Event Format (TMEF)<br><br>For details, see *Syslog Content Mapping - TMEF on page 4-1* | TMEF is a superset of log fields that allow a third-party syslog collector to better control and mitigate detection events provided by Deep Discovery Analyzer. |

# Terminology

| TERM | DESCRIPTION |
|---|---|
| CEF | Common Event Format |
| LEEF | Log Event Extended Format |
| TMEF | Trend Micro Event Format |

# Chapter 2

# Syslog Content Mapping - CEF

The following tables outline syslog content mapping between Deep Discovery Analyzer log output and CEF syslog types:

# CEF Virtual Analyzer Analysis Logs: File Analysis Events

**TABLE 2-1. CEF Virtual Analyzer Analysis Logs: File Analysis Events**

| CEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| Header (logVer) | CEF format version | CEF: 0 |
| Header (vendor) | Appliance vendor | Trend Micro |
| Header (pname) | Appliance product | Deep Discovery Analyzer |
| Header (pver) | Appliance version | Example: 2.5.0.1161 |
| Header (eventid) | Signature ID | 200119 |
| Header (eventName) | Description | Sample file sandbox analysis is finished |
| Header (severity) | Severity | 3 |
| cn1 | GRID is known good | • -1: GRID is unknown<br>• 0: GRID is not known good<br>• 1: GRID is known good |
| cn1Label | GRID is known good | GRIDIsKnownGood |
| cn2 | ROZ rating | • -1: Unsupported file type in ROZ<br>• 0: No risk found<br>• 1: Low risk<br>• 2: Medium risk<br>• 3: High risk<br><br>**Note**<br>Other negative values refer to errors. |

| CEF Key | Description | Value |
|---|---|---|
| cn2Label | ROZ rating | ROZRating |
| cn3 | PCAP ready | • 0: PCAP is not ready<br>• 1: PCAP is ready |
| cn3Label | PCAP ready | PcapReady |
| cs1 | Sandbox image type | Example: win7 |
| cs1Label | Sandbox image type | SandboxImageType |
| cs2 | Malware name | Example: HEUR_NAMETRICK.A |
| cs2Label | Malware name | MalwareName |
| cs3 | Parent SHA1 | Example: A29E4ACA70BEF4AF8CE75AF5 1032B6B91572AA0D |
| cs3Label | Parent SHA1 | ParentFileSHA1 |
| deviceExternalId | Appliance GUID | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536 |
| dvc | Appliance IP address | Example: 10.1.144.199 |
| dvchost | Appliance host name | Example: localhost |
| dvcmac | Appliance MAC address | Example: 00:0C:29:6E:CB:F9 |
| fileHash | SHA1 | Example: 1EDD5B38DE4729545767088C5 CAB395E4197C8F3 |
| fileType | True file type | Example: RIFF bitmap file |
| fname | File name | Example: excel.rar |
| fsize | File size | Example: 131372 |
| rt | Analysis time | Example: Mar 09 2015 17:05:21 GMT+08:00 |

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Analyzer|5.5.0.1202|2001
19|Sample file sandbox analysis is finished|3|rt=Feb 27 20
15 09:49:06 GMT+00:00 dvc=10.204.191.249 dvchost=DDAN dvcm
ac=EC:F4:BB:C6:F1:D0 deviceExternalId=758B04C9-F577-4B8A-B
527-ABCB84FDAC83 fname=Invoice_06202013_QBK.exe fileHash=C
F1A6CF231BDA185DEBF70B8562301798F286FAD fileType=WIN32 EXE
 fsize=117248 cs1Label=SandboxImageType cs1=win8 cs3Label=
ParentFileSHA1 cs3=FF47AEE003778AA51E0326F53EF235C96D71D7C
A cn1Label=GRIDIsKnownGood cn1=-1 cn2Label=ROZRating cn2=3
 cs2Label=MalwareName cs2=TSPY_FAREIT.WT cn3Label=PcapRead
y cn3=1
```

# CEF Virtual Analyzer Analysis Logs: URL Analysis Events

**TABLE 2-2. CEF Virtual Analyzer Analysis Logs: URL Analysis Events**

| CEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| Header (logVer) | CEF format version | CEF: 0 |
| Header (vendor) | Appliance vendor | Trend Micro |
| Header (pname) | Appliance product | Deep Discovery Analyzer |
| Header (pver) | Appliance version | Example: 2.5.0.1161 |
| Header (eventid) | Signature ID | 200126 |
| Header (eventName) | Description | URL sandbox analysis is finished |
| Header (severity) | Severity | 3 |

| CEF Key | Description | Value |
|---|---|---|
| cn2 | ROZ rating | • -1: Unsupported file type in ROZ<br>• 0: No risk found<br>• 1: Low risk<br>• 2: Medium risk<br>• 3: High risk<br><br>**Note**<br>Other negative values refer to errors. |
| cn2Label | ROZ rating | ROZRating |
| cn3 | PCAP ready | • 0: PCAP is not ready<br>• 1: PCAP is ready |
| cn3Label | PCAP ready | PcapReady |
| cs1 | Sandbox image type | Example: win7 |
| cs1Label | Sandbox image type | SandboxImageType |
| deviceExternalId | Appliance GUID | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536 |
| dvc | Appliance IP address | Example: 10.1.144.199 |
| dvchost | Appliance host name | Example: localhost |
| dvcmac | Appliance MAC address | Example: 00:0C:29:6E:CB:F9 |
| fileHash | SHA1 | Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3 |

| CEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| request | URL | Example: http://www.rainking.net/?utm_campaign=4-21-2014 \|http://images.rainking.net/eloquaimage |
| rt | Analysis time | Example: Mar 09 2015 17:05:21 GMT+08:00 |

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Analyzer|5.5.0.1202|2001
26|URL sandbox analysis is finished|3|rt=Feb 27 2015 09:3
6:26 GMT+00:00 dvc=10.204.191.249 dvchost=DDAN dvcmac=EC:
F4:BB:C6:F1:D0 deviceExternalId=758B04C9-F577-4B8A-B527-A
BCB84FDAC83 request=http://www.baidu.com:80/ fileHash=ACB
5175554463DD2ADBDFF78AD82C7D6BB8C8B6B cs1Label=SandboxIma
geType cs1=win8 cn2Label=ROZRating cn2=0 cn3Label=PcapRea
dy cn3=1
```

# CEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

**TABLE 2-3. CEF Virtual Analyzer Analysis Logs: Notable Characteristics Events**

| CEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| Header (logVer) | CEF format version | CEF: 0 |
| Header (vendor) | Appliance vendor | Trend Micro |
| Header (pname) | Appliance product | Deep Discovery Analyzer |
| Header (pver) | Appliance version | Example: 2.5.0.1161 |
| Header (eventid) | Signature ID | 200127 |
| Header (eventName) | Description | Notable Characteristics of the analyzed sample |

| CEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| Header (severity) | Severity | 6 |
| cs1 | Violated policy name | Example: Internet Explorer Setting Modification |
| cs1Label | Violated policy name | PolicyCategory |
| cs2 | Violated event analysis | Example: Modified important registry items |
| cs2Label | Violated event analysis | PolicyName |
| cs3 | Sandbox image type | Example: win7 |
| cs3Label | Sandbox image type | SandboxImageType |
| deviceExternalId | Appliance GUID | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536 |
| dvc | Appliance IP address | Example: 10.1.144.199 |
| dvchost | Appliance host name | Example: localhost |
| dvcmac | Appliance MAC address | Example: 00:0C:29:6E:CB:F9 |
| fileHash | SHA1 | Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3 |
| fileType | True file type | Example: RIFF bitmap file |
| fname | File name | Example: excel.rar |
| fsize | File size | Example: 131372 |
| msg | Details | Example: Source: ATSE \nDetection Name: TSPY_FAREIT.WT\nEngine Version: 9.755.1246\nMalware Pattern Version: 11.501.90 |
| rt | Analysis time | Example: Mar 09 2015 17:05:21 GMT+08:00 |

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Analyzer|5.5.0.1202|2001
27|Notable Characteristics of the analyzed sample|6|rt=Feb
 27 2015 09:49:06 GMT+00:00 dvc=10.204.191.249 dvchost=DDA
N dvcmac=EC:F4:BB:C6:F1:D0 deviceExternalId=758B04C9-F577-
4B8A-B527-ABCB84FDAC83 fname=Invoice_06202013_QBK.exe file
Hash=CF1A6CF231BDA185DEBF70B8562301798F286FAD fileType=WIN
32 EXE fsize=117248 cs1Label=PolicyCategory cs1=Malformed,
 defective, or with known malware traits msg=Source: ATSE\
nDetection Name: TSPY_FAREIT.WT\nEngine Version: 9.755.124
6\nMalware Pattern Version: 11.501.90 cs2Label=PolicyName
cs2=Detected as known malware
```

# CEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

**TABLE 2-4. CEF Virtual Analyzer Analysis Logs: Deny List Transaction Events**

| CEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| Header (logVer) | CEF format version | CEF: 0 |
| Header (vendor) | Appliance vendor | Trend Micro |
| Header (pname) | Appliance product | Deep Discovery Analyzer |
| Header (pver) | Appliance version | Example: 2.5.0.1161 |
| Header (eventid) | Signature ID | 200120 |
| Header (eventName) | Description | Deny List updated |
| Header (severity) | Severity | 3 |
| act | The action in the event | • Add<br>• Remove |

| CEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| cs1 | Deny List type | • Deny List IP/Port<br>• Deny List URL<br>• Deny List File SHA1<br>• Deny List Domain |
| cs1Label | Deny List type | type |
| cs2 | Risk level | • Low<br>• Medium<br>• High<br>• Confirmed Malware |
| cs2Label | Risk level | RiskLevel |
| deviceExternalId | Appliance GUID | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536 |
| dhost | Destination host name | Example: dhost1 |
| dpt | Destination port | Value between 0 and 65535 |
| dst | Destination IP address | Example: 10.1.144.199 |
| dvc | Appliance IP address | Example: 10.1.144.199 |
| dvchost | Appliance host name | Example: localhost |
| dvcmac | Appliance MAC address | Example: 00:0C:29:6E:CB:F9 |
| end | Deny List expired time | Example: Mar 09 2015 17:05:21 GMT+08:00 |
| fileHash | SHA1 | Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3 |

| CEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| request | URL | Example: http://www.rainking.net/?utm_campaign=4-21-2014 \|http://images.rainking.net/eloquaimage |
| rt | Log generation time | Example: Mar 09 2015 17:05:21 GMT+08:00 |

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Analyzer|5.5.0.1202|2001
20|Deny List updated|3|rt=Feb 27 2015 09:49:41 GMT+00:00 d
vc=10.204.191.249 dvchost=DDAN dvcmac=EC:F4:BB:C6:F1:D0 de
viceExternalId=758B04C9-F577-4B8A-B527-ABCB84FDAC83  cs1La
bel=type cs1=Deny List File SHA1 end=Mar 29 2015 09:49:06
GMT+00:00 act=Add fileHash=CF1A6CF231BDA185DEBF70B85623017
98F286FAD cs2Label=RiskLevel cs2=High
```

# Chapter 3

# Syslog Content Mapping - LEEF

The following tables outline syslog content mapping between Deep Discovery Analyzer log output and LEEF syslog types:



**Note**

When using the LEEF log syntax, separate event attributes with <009> as a tab delimiter.

# LEEF Virtual Analyzer Analysis Logs: File Analysis

**TABLE 3-1. LEEF Virtual Analyzer Analysis Logs: File Analysis**

| LEEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| Header (logVer) | LEEF format version | LEEF: 1.0 |
| Header (vendor) | Appliance vendor | Trend Micro |
| Header (pname) | Appliance product | Deep Discovery Analyzer |
| Header (pver) | Appliance version | Example: 2.5.0.1161 |
| Header (eventName) | Event Name | FILE_ANALYZED |
| deviceGUID | Appliance GUID | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536 |
| deviceMacAddress | Appliance MAC address | Example: 00:0C:29:56:B3:57 |
| deviceProcessHash | Parent SHA1 | Example: A29E4ACA70BEF4AF8CE75AF5 1032B6B91572AA0D |
| devTime | Log generation time | Example: Jan 28 2015 02:00:36 GMT+08:00 |
| devTimeFormat | Time format | MMM dd yyyy HH:mm:ss z |
| dvc | Appliance IP address | Example: 10.1.144.199 |
| dvchost | Appliance host name | Example: localhost |
| fileHash | SHA1 | Example: 1EDD5B38DE4729545767088C5 CAB395E4197C8F3 |
| fileType | True file type | Example: RIFF bitmap file |
| fname | File name | Example: excel.rar |

| LEEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| fsize | File size | Example: 131372 |
| gridIsKnownGood | GRID is known good | • -1: GRID is unknown<br>• 0: GRID is not known good<br>• 1: GRID is known good |
| malName | Malware name | Example: HEUR_NAMETRICK.A |
| pcapReady | PCAP ready | • 0: PCAP is not ready<br>• 1: PCAP is ready |
| pComp | Detection engine / component | Sandbox |
| rozRating | ROZ rating | • -1: Unsupported file type in ROZ<br>• 0: No risk found<br>• 1: Low risk<br>• 2: Medium risk<br>• 3: High risk<br>**Note**<br>Other negative values refer to errors. |
| sev | Severity | Value between 0 and 10 |

**Note**

When using the LEEF log syntax, separate event attributes with <009> as a tab delimiter.

Log sample:

```
LEEF:1.0|Trend Micro|Deep Discovery Analyzer|5.5.0.1202|FILE
_ANALYZED|devTime=Feb 28 2015 02:45:48 GMT+00:00<009>devTimeF
ormat=MMM dd yyyy HH:mm:ss z<009>sev=3<009>pComp=Sandbox<009>
```

```
dvc=10.204.191.249<009>dvchost=DDAN<009>deviceMacAddress=EC:F
4:BB:C6:F1:D0<009>deviceGUID=758B04C9-F577-4B8A-B527-ABCB84FD
AC83<009>fname=Invoice_06202013_QBK.exe<009>fileHash=CF1A6CF2
31BDA185DEBF70B8562301798F286FAD<009>deviceProcessHash=FF47AE
E003778AA51E0326F53EF235C96D71D7CA<009>malName=TSPY_FAREIT.WT
<009>fileType=WIN32 EXE<009>fsize=117248<009>deviceOSName=win
8<009>gridIsKnownGood=-1<009>rozRating=3<009>pcapReady=1
```

# LEEF Virtual Analyzer Analysis Logs: URL Analysis

**TABLE 3-2. LEEF Virtual Analyzer Analysis Logs: URL Analysis**

| LEEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| Header (logVer) | LEEF format version | LEEF: 1.0 |
| Header (vendor) | Appliance vendor | Trend Micro |
| Header (pname) | Appliance product | Deep Discovery Analyzer |
| Header (pver) | Appliance version | Example: 2.5.0.1161 |
| Header (eventName) | Event Name | URL_ANALYZED |
| deviceGUID | Appliance GUID | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536 |
| deviceMacAddress | Appliance MAC address | Example: 00:0C:29:56:B3:57 |
| deviceOSName | Sandbox image type | Example: win7 |
| devTime | Log generation time | Example: Jan 28 2015 02:00:36 GMT+08:00 |
| devTimeFormat | Time format | MMM dd yyyy HH:mm:ss z |
| dvc | Appliance IP address | Example: 10.1.144.199 |
| dvchost | Appliance host name | Example: localhost |

| LEEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| fileHash | SHA1 | Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3 |
| pcapReady | PCAP ready | • 0: PCAP is not ready<br>• 1: PCAP is ready |
| pComp | Detection engine / component | Sandbox |
| rozRating | ROZ rating | • -1: Unsupported file type in ROZ<br>• 0: No risk found<br>• 1: Low risk<br>• 2: Medium risk<br>• 3: High risk<br><br>**Note**<br>Other negative values refer to errors. |
| sev | Severity | Value between 0 and 10 |
| url | URL | Example: http://1.2.3.4/query?term=value |

**Note**

When using the LEEF log syntax, separate event attributes with <009> as a tab delimiter.

Log sample:

```
LEEF:1.0|Trend Micro|Deep Discovery Analyzer|5.5.0.1202|URL_
ANALYZED|devTime=Feb 27 2015 09:36:26 GMT+00:00<009>devTimeFo
rmat=MMM dd yyyy HH:mm:ss z<009>sev=3<009>pComp=Sandbox<009>d
vc=10.204.191.249<009>dvchost=DDAN<009>deviceMacAddress=EC:F4
:BB:C6:F1:D0<009>deviceGUID=758B04C9-F577-4B8A-B527-ABCB84FDA
```

```
C83<009>fileHash=ACB5175554463DD2ADBDFF78AD82C7D6BB8C8B6B<009
>deviceOSName=win8<009>url=http://www.baidu.com:80/<009>rozRa
ting=0<009>pcapReady=1
```

# LEEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

**TABLE 3-3. LEEF Virtual Analyzer Analysis Logs: Notable Characteristics Events**

| LEEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| Header (logVer) | LEEF format version | LEEF: 1.0 |
| Header (vendor) | Appliance vendor | Trend Micro |
| Header (pname) | Appliance product | Deep Discovery Analyzer |
| Header (pver) | Appliance version | Example: 2.5.0.1161 |
| Header (eventName) | Event Name | NOTABLE_CHARACTERISITICS |
| deviceGUID | Appliance GUID | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536 |
| deviceMacAddress | Appliance MAC address | Example: 00:0C:29:56:B3:57 |
| deviceOSName | Sandbox image type | Example: win7 |
| devTime | Log generation time | Example: Jan 28 2015 02:00:36 GMT+08:00 |
| devTimeFormat | Time format | MMM dd yyyy HH:mm:ss z |
| dvc | Appliance IP address | Example: 10.1.144.199 |
| dvchost | Appliance host name | Example: localhost |
| fileHash | SHA1 | Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3 |

| LEEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| fileType | True file type | Example: RIFF bitmap file |
| fname | File name | Example: excel.rar |
| fsize | File size | Example: 131372 |
| msg | Details | Example: Process ID: 884 \nFile: %TEMP% \~DF7A0C28F4D7D9E792.TMP \nType: VSDT_ERROR |
| pComp | Detection engine / component | Sandbox |
| ruleCategory | Violated policy name | Example: Internet Explorer Setting Modification |
| ruleName | Violated event analysis | Example: Modified important registry items |
| sev | Severity | Value between 0 and 10 |

**Note**

When using the LEEF log syntax, separate event attributes with <009> as a tab delimiter.

Log sample:

```
LEEF:1.0|Trend Micro|Deep Discovery Analyzer|5.5.0.1202|NOTA
BLE_CHARACTERISTICS|devTime=Feb 28 2015 02:46:33 GMT+00:00<00
9>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>sev=6<009>pComp=Sa
ndbox<009>dvc=10.204.191.249<009>dvchost=DDAN<009>deviceMacAd
dress=EC:F4:BB:C6:F1:D0<009>deviceGUID=758B04C9-F577-4B8A-B52
7-ABCB84FDAC83<009>fname=a254i.doc<009>fileHash=7A75D6934C5CD
AAF6CA13F8FA4CA03E46DAA7623<009>fileType=Microsoft RTF<009>fs
ize=86016<009>ruleCategory=File drop, download, sharing, or r
eplication<009>ruleName=Deletes file to compromise the system
 or to remove traces of the infection<009>msg=Process ID: 884
\nFile: %TEMP%\~DF7A0C28F4D7D9E792.TMP\nType: VSDT_ERROR
```

# LEEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

**TABLE 3-4. LEEF Virtual Analyzer Analysis Logs: Deny List Transaction Events**

| LEEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| Header (logVer) | LEEF format version | LEEF: 1.0 |
| Header (vendor) | Appliance vendor | Trend Micro |
| Header (pname) | Appliance product | Deep Discovery Analyzer |
| Header (pver) | Appliance version | Example: 2.5.0.1161 |
| Header (eventName) | Event Name | DENYLIST_CHANGE |
| act | The action in the event | • Add<br>• Remove |
| deviceExternalRiskType | Risk level | • Low<br>• Medium<br>• High<br>• Confirmed Malware |
| deviceGUID | Appliance GUID | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536 |
| deviceMacAddress | Appliance MAC address | Example: 00:0C:29:56:B3:57 |
| devTime | Log generation time | Example: Jan 28 2015 02:00:36 GMT+08:00 |
| devTimeFormat | Time format | MMM dd yyyy HH:mm:ss z |
| dhost | Destination host name | Example: dhost1 |
| dpt | Destination port | Value between 0 and 65535 |
| dst | Destination IP address | Example: 10.1.144.199 |

| LEEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| dvc | Appliance IP address | Example: 10.1.144.199 |
| dvchost | Appliance host name | Example: localhost |
| end | Report end time | Example: Mar 09 2015 17:05:21 GMT+08:00 |
| fileHash | SHA1 | Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3 |
| pComp | Detection engine / component | Sandbox |
| sev | Severity | Value between 1 and 10 |
| type | Deny List type | • Deny List IP/Port<br>• Deny List URL<br>• Deny List File SHA1<br>• Deny List Domain |
| url | URL | Example: http://1.2.3.4/query?term=value |

**Note**

When using the LEEF log syntax, separate event attributes with <009> as a tab delimiter.

Log sample:

```
LEEF:1.0|Trend Micro|Deep Discovery Analyzer|5.5.0.1202|DENY
LIST_CHANGE|devTime=Feb 28 2015 02:50:03 GMT+00:00<009>devTim
eFormat=MMM dd yyyy HH:mm:ss z<009>sev=3<009>pComp=Sandbox<00
9>dvc=10.204.191.249<009>dvchost=DDAN<009>deviceMacAddress=EC
:F4:BB:C6:F1:D0<009> deviceGUID=758B04C9-F577-4B8A-B527-ABCB8
4FDAC83<009>end=Mar 30 2015 02:45:48 GMT+00:00<009>act=Add<00
9>fileHash=CF1A6CF231BDA185DEBF70B8562301798F286FAD<009>devic
eExternalRiskType=High<009>type=Deny List File SHA1
```

# Chapter 4

# Syslog Content Mapping - TMEF

The following tables outline syslog content mapping between Deep Discovery Analyzer log output and TMEF syslog types:

# TMEF Virtual Analyzer Analysis Logs: File Analysis Events

**TABLE 4-1. TMEF Virtual Analyzer Analysis Logs: File Analysis Events**

| TMEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| Header (logVer) | TMEF format version | CEF: 0 |
| Header (vendor) | Appliance vendor | Trend Micro |
| Header (pname) | Appliance product | Deep Discovery Analyzer |
| Header (pver) | Appliance version | Example: 2.5.0.1161 |
| Header (eventid) | Signature ID | 200119 |
| Header (eventName) | Description | FILE_ANALYZED |
| Header (severity) | Severity | 3 |
| cn1 | GRID is known good | • -1: GRID is unknown<br>• 0: GRID is not known good<br>• 1: GRID is known good |
| cn1Label | GRID is known good | GRIDIsKnownGood |
| cn2 | ROZ rating | • -1: Unsupported file type in ROZ<br>• 0: No risk found<br>• 1: Low risk<br>• 2: Medium risk<br>• 3: High risk<br><br>**Note**<br>Other negative values refer to errors. |

| TMEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| cn2Label | ROZ rating | ROZRating |
| cn3 | PCAP ready | • 0: PCAP is not ready<br>• 1: PCAP is ready |
| cn3Label | PCAP ready | PcapReady |
| deviceGUID | Appliance GUID | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536 |
| deviceMacAddress | Appliance MAC address | Example: 00:0C:29:6E:CB:F9 |
| deviceOSName | Sandbox image type | Example: win7 |
| deviceProcessHash | Parent SHA1 | Example: A29E4ACA70BEF4AF8CE75AF5 1032B6B91572AA0D |
| dvc | Appliance IP address | Example: 10.1.144.199 |
| dvchost | Appliance host name | Example: localhost |
| fileHash | SHA1 | Example: 1EDD5B38DE4729545767088C5 CAB395E4197C8F3 |
| fileType | True file type | Example: RIFF bitmap file |
| fname | File name | Example: excel.rar |
| fsize | File size | Example: 131372 |
| malName | Malware name | Example: HEUR_NAMETRICK.A |
| pComp | Detection engine / component | Sandbox |
| rt | Analysis time | Example: Mar 09 2015 17:05:21 GMT+08:00 |

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Analyzer|5.5.0.1221|2001
19|FILE_ANALYZED|3|rt=Jun 26 2015 05:29:57 GMT+00:00 pComp=
Sandbox dvc=10.204.70.173 dvchost=DDAN deviceMacAddress=00:
0C:29:69:19:03 deviceGUID=6EDFB737-5EBA-42B7-8D2E-D0789F19F
EF4 fname=Establishes_uncommon_connection fileHash=0C450F48
E48CEF0B161C254C9E57816CD20FA918 deviceProcessHash=A754E779
292F392AE7692D0D2A55D2ECB71B5332 malName=BKDR_NORAWEC.SMG f
ileType=UPX EXE fsize=149504 deviceOSName=fsdf cn1Label=GRI
DIsKnownGood cn1=-1 cn2Label=ROZRating cn2=3 cn3Label=PcapR
eady cn3=1
```

# TMEF Virtual Analyzer Analysis Logs: URL Analysis Events

**TABLE 4-2. TMEF Virtual Analyzer Analysis Logs: URL Analysis Events**

| TMEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| Header (logVer) | TMEF format version | CEF: 0 |
| Header (vendor) | Appliance vendor | Trend Micro |
| Header (pname) | Appliance product | Deep Discovery Analyzer |
| Header (pver) | Appliance version | Example: 2.5.0.1161 |
| Header (eventid) | Signature ID | 200126 |
| Header (eventName) | Description | URL_ANALYZED |
| Header (severity) | Severity | 3 |

| TMEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| cn2 | ROZ rating | • -1: Unsupported file type in ROZ<br>• 0: No risk found<br>• 1: Low risk<br>• 2: Medium risk<br>• 3: High risk<br><br>**Note**<br>Other negative values refer to errors. |
| cn2Label | ROZ rating | ROZRating |
| cn3 | PCAP ready | • 0: PCAP is not ready<br>• 1: PCAP is ready |
| cn3Label | PCAP ready | PcapReady |
| deviceGUID | Appliance GUID | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536 |
| deviceMacAddress | Appliance MAC address | Example: 00:0C:29:6E:CB:F9 |
| deviceOSName | Sandbox image type | Example: win7 |
| dvc | Appliance IP address | Example: 10.1.144.199 |
| dvchost | Appliance host name | Example: localhost |
| fileHash | SHA1 | Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3 |
| pComp | Detection engine / component | Sandbox |

| TMEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| request | URL | Example: http://www.rainking.net/?utm_campaign=4-21-2014 \|http://images.rainking.net/eloquaimage |
| rt | Analysis time | Example: Mar 09 2015 17:05:21 GMT+08:00 |

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Analyzer|5.5.0.1221|2001
26|URL_ANALYZED|3|rt=Jun 26 2015 05:24:26 GMT+00:00 pComp=San
dbox dvc=10.104.70.173 dvchost=DDAN deviceMacAddress=00:0C:29
:69:19:03 deviceGUID=6EDFB737-5EBA-42B7-8D2E-D0789F19FEF4 req
uest=https://wx.qq.com:443/ fileHash=BA4AA53108D98F5195D1F490
D05716F0B6D7B7EA deviceOSName=fsdf cn2Label=ROZRating cn2=-14
 cn3Label=PcapReady cn3=0
```

# TMEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

**TABLE 4-3. TMEF Virtual Analyzer Analysis Logs: Notable Characteristics Events**

| TMEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| Header (logVer) | TMEF format version | CEF: 0 |
| Header (vendor) | Appliance vendor | Trend Micro |
| Header (pname) | Appliance product | Deep Discovery Analyzer |
| Header (pver) | Appliance version | Example: 2.5.0.1161 |
| Header (eventid) | Signature ID | 200127 |
| Header (eventName) | Description | NOTABLE_CHARACTERISITICS |
| Header (severity) | Severity | 6 |

| TMEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| deviceGUID | Appliance GUID | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536 |
| deviceMacAddress | Appliance MAC address | Example: 00:0C:29:6E:CB:F9 |
| deviceOSName | Sandbox image type | Example: win7 |
| dvc | Appliance IP address | Example: 10.1.144.199 |
| dvchost | Appliance host name | Example: localhost |
| fileHash | SHA1 | Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3 |
| fileType | True file type | Example: RIFF bitmap file |
| fname | File name | Example: excel.rar |
| fsize | File size | Example: 131372 |
| msg | Details | Example: ATSE\nDetection Name: TROJ_FAM_00004f2.TOMA \nEngine Version: 9.826.1078\nMalware Pattern Version: 11.749.92 |
| pComp | Detection engine / component | Sandbox |
| rt | Analysis time | Example: Mar 09 2015 17:05:21 GMT+08:00 |
| ruleCategory | Violated policy name | Example: Internet Explorer Setting Modification |
| ruleName | Violated event analysis | Example: Modified important registry items |

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Analyzer|5.5.0.1221|2001
27|NOTABLE_CHARACTERISTICS|6|rt=Jun 26 2015 05:24:01 GMT+00:0
0 pComp=Sandbox dvc=10.204.70.173 dvchost=DDAN deviceMacAddre
ss=00:0C:29:69:19:13 deviceGUID=6EDFB737-5EBA-42B7-8D2E-D0789
F19FEF4 fname=Sends_email fileHash=1A37D76D3669FC0BF0CBAABB3C
149BAC43491663 fileType=WIN32 EXE fsize=92160 ruleCategory=Ma
lformed, defective, or with known malware traits ruleName=Det
ected as probable malware msg=Source: ATSE\nDetection Name: T
ROJ_FAM_00004f2.TOMA\nEngine Version: 9.826.1078\nMalware Pat
tern Version: 11.749.92 deviceOSName=fsdf
```

# TMEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

**TABLE 4-4. TMEF Virtual Analyzer Analysis Logs: Deny List Transaction Events**

| TMEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| Header (logVer) | TMEF format version | CEF: 0 |
| Header (vendor) | Appliance vendor | Trend Micro |
| Header (pname) | Appliance product | Deep Discovery Analyzer |
| Header (pver) | Appliance version | Example: 2.5.0.1161 |
| Header (eventid) | Signature ID | 200120 |
| Header (eventName) | Description | DENYLIST_CHANGE |
| Header (severity) | Severity | 3 |
| act | The action in the event | • Add<br>• Remove |

| TMEF KEY | DESCRIPTION | VALUE |
|---|---|---|
| cs1 | Deny List type | • Deny List IP/Port<br>• Deny List URL<br>• Deny List File SHA1<br>• Deny List Domain |
| cs1Label | Deny List type | type |
| deviceGUID | Appliance GUID | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536 |
| deviceMacAddress | Appliance MAC address | Example: 00:0C:29:6E:CB:F9 |
| deviceExternalRiskType | Risk level | • Low<br>• Medium<br>• High<br>• Confirmed Malware |
| dhost | Destination host name | Example: dhost1 |
| dvc | Appliance IP address | Example: 10.1.144.199 |
| dvchost | Appliance host name | Example: localhost |
| end | Report end time | Example: Mar 09 2015 17:05:21 GMT+08:00 |
| fileHash | SHA1 | Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3 |
| pComp | Detection engine / component | Sandbox |
| rt | Log generation time | Example: Mar 09 2015 17:05:21 GMT+08:00 |

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Analyzer|5.5.0.1221|2001
20|DENYLIST_CHANGE|3|rt=Jun 26 2015 05:55:02 GMT+00:00 pComp=
Sandbox dvc=10.204.70.17 dvchost=DDAN deviceMacAddress=01:0C:
29:69:19:03 deviceGUID=6EDFB737-5EBA-42B7-8D2E-D0789F19FEF4 c
s1Label=type cs1=Deny List Domain end=Jul 26 2015 05:47:16 GM
T+00:00 act=Add dhost=ns1.player1352.com deviceExternalRiskTy
pe=High
```

# Index


**TREND MICRO INCORPORATED**

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: APEM57272/151216