



# 5.6 TREND MICRO™ Deep Discovery Inspector

Service Pack 1

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>

Trend Micro, the Trend Micro t-ball logo, Deep Discovery Advisor, Deep Discovery Analyzer, Deep Discovery Inspector, and Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2020. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM58907/191227

Release Date: June 2020

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](mailto:docs@trendmicro.com).

Evaluate this documentation on the following site:

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

## **Privacy and Personal Data Collection Disclosure**

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that Deep Discovery Inspector collects and provides detailed instructions on how to disable the specific features that feedback the information.

<https://success.trendmicro.com/data-collection-disclosure>

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Notice:

<https://www.trendmicro.com/privacy>

# Table of Contents

## **Chapter 1: Introduction**

|                   |     |
|-------------------|-----|
| Terminology ..... | 1-2 |
|-------------------|-----|

## **Chapter 2: Revisions**

## **Chapter 3: Syslog Content Mapping - CEF**

|  |      |
|--|------|
| CEF Threat Logs .....  | 3-2  |
| CEF Disruptive Application Logs .....                        | 3-7  |
| CEF Web Reputation Logs .....                                | 3-9  |
| CEF System Logs .....  | 3-13 |
| CEF Virtual Analyzer Logs: File Analysis Events .....        | 3-15 |
| CEF Virtual Analyzer Logs: Notable Characteristics Events .. | 3-17 |
| CEF Virtual Analyzer Logs: Deny List Transaction Events .... | 3-19 |

## **Chapter 4: Syslog Content Mapping - LEEF**

|  |      |
|--|------|
| LEEF Threat Logs .....                                       | 4-2  |
| LEEF Disruptive Application Logs .....                       | 4-9  |
| LEEF Web Reputation Logs .....                               | 4-12 |
| LEEF System Logs .....                                       | 4-16 |
| LEEF Correlation Incident Logs .....                         | 4-17 |
| LEEF Virtual Analyzer Logs: File Analysis Events .....       | 4-20 |
| LEEF Virtual Analyzer Logs: Notable Characteristics Events   | 4-22 |
| LEEF Virtual Analyzer Logs: Deny List Transaction Event .... | 4-24 |

## **Chapter 5: Syslog Content Mapping - TMEF**

|  |      |
|--|------|
| TMEF Threat Logs .....   | 5-2  |
| TMEF Disruptive Application Logs .....                           | 5-11 |
| TMEF Web Reputation Logs .....                                   | 5-15 |
| TMEF System Logs .....   | 5-20 |
| TMEF Correlated Incident Logs .....                              | 5-22 |
| TMEF Virtual Analyzer Logs: File Analysis Events .....           | 5-24 |
| TMEF Virtual Analyzer Logs: Notable Characteristics Events ..... | 5-26 |
| TMEF Virtual Analyzer Logs: Deny List Transaction Events .....   | 5-28 |
| TMEF Retro Scan Report Logs .....                                | 5-30 |
| TMEF Retro Scan Detection Logs .....                             | 5-31 |

# Preface

## Preface

Learn more about the following topics:

- *Documentation on page iv*
- *Audience on page v*
- *Document Conventions on page v*
- *About Trend Micro on page vi*

## Documentation

The documentation set for Deep Discovery Inspector includes the following:

**TABLE 1. Product Documentation**

| DOCUMENT                          | DESCRIPTION  |
|-----------------------------------|--|
| Administrator's Guide             | The Administrator's Guide contains detailed instructions on how to configure and manage Deep Discovery Inspector, and explanations on Deep Discovery Inspector concepts and features.  |
| Installation and Deployment Guide | The Installation and Deployment Guide contains information about requirements and procedures for planning deployment, installing Deep Discovery Inspector, and using the Preconfiguration Console to set initial configurations and perform system tasks.  |
| Syslog Content Mapping Guide      | The Syslog Content Mapping Guide provides information about log management standards and syntaxes for implementing syslog events in Deep Discovery Inspector.  |
| Quick Start Card                  | The Quick Start Card provides user-friendly instructions on connecting Deep Discovery Inspector 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.   |
| Online Help                       | <p>Web-based documentation that is accessible from the Deep Discovery Inspector management console.</p> <p>The Online Help contains explanations of Deep Discovery Inspector components and features, as well as procedures needed to configure Deep Discovery Inspector.</p>                                    |
| Support Portal                    | <p>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:</p> <p><a href="http://esupport.trendmicro.com">http://esupport.trendmicro.com</a></p> |



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

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

## Audience

The Deep Discovery Inspector 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 |
| <b>Bold</b>    | Menus and menu commands, command buttons, tabs, and options                     |
| <i>Italics</i> | References to other documents   |
| Monospace      | Sample command lines, program code, web URLs, file names, and program output    |

| CONVENTION   | DESCRIPTION   |
|--|---|
| <b>Navigation &gt; Path</b>  | The navigation path to reach a particular screen<br><br>For example, <b>File &gt; Save</b> means, click <b>File</b> and then click <b>Save</b> on the interface |
|  <b>Note</b>      | Configuration notes   |
|  <b>Tip</b>       | Recommendations or suggestions  |
|  <b>Important</b> | Information regarding required or default configuration settings and product limitations  |
|  <b>WARNING!</b>  | 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>

Trend Micro and the Trend Micro t-ball logo are trademarks of Trend Micro Incorporated and are registered in some jurisdictions. All other marks are the trademarks or registered trademarks of their respective companies.

# Chapter 1

## Introduction

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

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

| LOG MANAGEMENT SYSTEM  | DESCRIPTION  |
|--|--|
| Common Event Format (CEF)<br>For details, see <a href="#">Syslog Content Mapping - CEF on page 3-1</a>         | CEF is an open log management standard created by HP ArcSight.<br><br>Deep Discovery Inspector uses a subset of the CEF dictionary.                              |
| Log Event Extended Format (LEEF)<br>For details, see <a href="#">Syslog Content Mapping - LEEF on page 4-1</a> | LEEF is an event format developed for IBM Security QRadar.<br><br>Deep Discovery Inspector uses a subset of the LEEF dictionary.                                 |
| Trend Micro Event Format (TMEF)<br>For details, see <a href="#">Syslog Content Mapping - TMEF on page 5-1</a>  | 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 Inspector. |

## Terminology

| <b>TERM</b> | <b>DESCRIPTION</b>                |
|-------------|-----------------------------------|
| CEF         | Common Event Format               |
| LEEF        | Log Event Extended Format         |
| TMEF        | Trend Micro Event Format          |
| CCCA        | Command and Control Contact Alert |

# Chapter 2

## Revisions

There were no revisions for version 5.6 SP 1.



## Chapter 3

### Syslog Content Mapping - CEF

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

- *CEF Threat Logs on page 3-2*
- *CEF Disruptive Application Logs on page 3-7*
- *CEF Web Reputation Logs on page 3-9*
- *CEF System Logs on page 3-13*
- *CEF Virtual Analyzer Logs: File Analysis Events on page 3-15*
- *CEF Virtual Analyzer Logs: Notable Characteristics Events on page 3-17*
- *CEF Virtual Analyzer Logs: Deny List Transaction Events on page 3-19*

## CEF Threat Logs

**TABLE 3-1. CEF Threat Logs**

| CEF KEY            | DESCRIPTION              | VALUE  |
|--------------------|--------------------------|--|
| Header (logVer)    | CEF format version       | CEF: 0   |
| Header (vendor)    | Appliance vendor         | Trend Micro  |
| Header (pname)     | Appliance product        | Deep Discovery Inspector   |
| Header (pver)      | Appliance version        | Example: 3.8.1181  |
| Header (eventid)   | Event ID                 | Example: 8   |
| Header (eventName) | Description              | Example: Packed executable file copied to a network administrative share   |
| Header (severity)  | Severity                 | <ul style="list-style-type: none"> <li>• 2: Informational</li> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul> |
| act                | The action in the event  | blocked or not blocked   |
| app                | Protocol                 | Example: HTTP  |
| c6a1               | Interested IPv6          | Example: 2001:0:0:1::21  |
| c6a1Label          | Interested IPv6          | InterestedIPv6   |
| c6a2               | Source IPv6 address      | Example: 2001:0:0:1::21  |
| c6a2Label          | Source IPv6 address      | Source IPv6 Address  |
| c6a3               | Destination IPv6 address | Example: 2001:0:0:1::21  |
| c6a3Label          | Destination IPv6 address | Destination IPv6 Address   |
| c6a4               | Peer IPv6 address        | Example: 2001:0:0:1::21  |
| c6a4Label          | Peer IPv6 address        | PeerIPv6   |



| CEF KEY  | DESCRIPTION             | VALUE  |
|----------|-------------------------|--|
| cat      | Event category          | Example: File  |
| cnt      | Total count             | Example: 1   |
| cn1      | CCCA detection          | 0 or 1   |
| cn1Label | CCCA detection          | CCCA_Detection   |
| cn3      | Threat type             | <ul style="list-style-type: none"> <li>• 0: Malicious content</li> <li>• 1: Malicious behavior</li> <li>• 2: Suspicious behavior</li> <li>• 3: Exploit</li> <li>• 4: Grayware</li> </ul> |
| cn3Label | Threat type             | Threat Type  |
| cs1      | Mail subject            | Example: hello   |
| cs1Label | Mail subject            | MailSubject  |
| cs2      | Malware name            | Example: HEUR_NAMETRICK.A  |
| cs2Label | Malware name            | DetectionName  |
| cs3      | Host name               | Example: CLIENT1   |
| cs3Label | Host name               | HostName_Ext   |
| cs4      | File name in archive    | Example: mtxlegih.dll  |
| cs4Label | File name in archive    | FileNameInArchive  |
| cs5      | CCCA log is detected by | Example:<br>GLOBAL_INTELLIGENCE or<br>VIRTUAL_ANALYZER or<br>USER_DEFINED  |
| cs5Label | CCCA log is detected by | CCCA_DetectionSource   |

| CEF KEY                      | DESCRIPTION  | VALUE  |
|------------------------------|--|--|
| cs6                          | Attack Phase   | <ul style="list-style-type: none"> <li>Intelligence Gathering</li> <li>Point of Entry</li> <li>Command and Control Communication</li> <li>Lateral Movement</li> <li>Asset and Data Discovery</li> <li>Data Exfiltration</li> <li>Nil (no applicable attack phase)</li> </ul> |
| cs6Label                     | Attack Phase   | pAttackPhase   |
| destinationTranslatedAddress | Peer IP  | Example: 10.1.144.199  |
| deviceDirection              | Packet direction   | <ul style="list-style-type: none"> <li>0: Source is external</li> <li>1: Source is internal</li> <li>2: Unknown</li> </ul>   |
| deviceExternalId             | Appliance GUID   | Example: 6B593E17AFB7-40FB8B28-A4CE-0462-A536  |
| devicePayloadId              | An extendable field.<br>Format: {threat_type}:{log_id}:{with pcap file captured}{:extensions}*<br>* indicates optional | Examples: <ul style="list-style-type: none"> <li>With pcap file captured: 2:10245:P</li> <li>Without pcap file captured: 2:10245:</li> </ul>   |
| dhost                        | Destination host name  | Example: dhost1  |
| dmac                         | Destination MAC  | Example: 00:0C:29:6E:CB:F9   |
| dpt                          | Destination port   | Value between 0 and 65535  |
| dst                          | Destination IP address   | Example: 10.1.144.199  |
| duser                        | Mail recipient   | Example: duser1  |

| CEF KEY                  | DESCRIPTION               | VALUE  |
|--------------------------|---------------------------|--|
| 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:1EDD5B38DE47295457670<br>88C5CAB395E4197C8F3 |
| filePath                 | File path                 | Example: SHARE\\                                     |
| fileType                 | Real file type            | Example: 1638400                                     |
| flexNumber1              | vLANId                    | Example: 4095  |
| flexNumber1Label         | vLANId                    | vLANId   |
| fname                    | File name                 | Example: excel.rar                                   |
| fsize                    | File size                 | Example: 131372                                      |
| oldFileHash              | Mail attachment SHA1      | Example:1EDD5B38DE47295457670<br>88C5CAB395E4197C8F3 |
| oldFileName              | Mail attachment file name | Example: excel.rar                                   |
| oldFileSize              | Mail attachment file size | Example: 150000                                      |
| oldFileType              | Mail attachment file type | Example: 1638400                                     |
| requestClientApplication | User agent                | Example: IE  |
| request                  | URL                       | Example: http://1.2.3.4/query?<br>term=value         |
| rt                       | Log generation time       | Example: Mar 09 2015 17:05:21 GMT<br>+08:00          |
| shost                    | Source host name          | Example: shost1                                      |
| smac                     | Source MAC                | Example: 00:0C:29:6E:CB:F9                           |
| sourceTranslatedAddress  | Interested IP             | Example: 10.1.144.199                                |
| src                      | Source IP address         | Example: 10.1.144.199                                |

| CEF KEY | DESCRIPTION | VALUE                     |
|---------|-------------|---------------------------|
| spt     | Source port | Value between 0 and 65535 |
| suid    | User name   | Example: User1            |
| suser   | Mail sender | Example: suser1           |

### Log sample:

```

CEF:0|Trend Micro|Deep Discovery Inspector|5.0.1329|0|
Eicar_test_file
- HTTP (Response)|8|dvc=172.22.9.32
dvcmac=00:50:56:AD:03:BD
dvchost=localhost deviceExternalId=E9A3FA433916-
4738984C-A4BF-84A0-D603
rt=Jun 22 2017 09:42:47 GMT+08:00 app=HTTP
deviceDirection=1
dhost=172.22.9.5 dst=172.22.9.5 dpt=57908
dmac=00:50:56:82:e7:a9
shost=172.22.9.54 src=172.22.9.54 spt=80
smac=00:50:56:82:c6:ae
cs3Label=HostName_Ext cs3=172.22.9.54 cs2Label=
DetectionName
cs2=Eicar_test_file fname=eicarcom2.zip fileType=
262340608
fsize=308 requestClientApplication=Wget/1.12 (linux-gnu)
act=not blocked cn3Label=Threat Type cn3=0
destinationTranslatedAddress=172.22.9.5
fileHash=BEC1B52D350D721C7E22A6D4BB0A92909893A3AE
cs4Label=FileNameInArchive cs4=eicar.com
sourceTranslatedAddress=172.22.9.54
cnt=1 cat=Malware cs6Label=pAttackPhase cs6=Point
of Entry flexNumber1Label=vLANId flexNumber1=4095
request=http://172.22.9.54/eicarcom2.zip
devicePayloadId=0:143:P

```

## CEF Disruptive Application Logs

**TABLE 3-2. CEF Disruptive Application Logs**

| CEF KEY            | DESCRIPTION              | VALUE  |
|--------------------|--------------------------|--|
| Header (logVer)    | CEF format version       | CEF: 0   |
| Header (vendor)    | Appliance vendor         | Trend Micro  |
| Header (pname)     | Appliance product        | Deep Discovery Inspector   |
| Header (pver)      | Appliance version        | Example: 3.8.1181  |
| Header (eventid)   | Signature ID             | 100120   |
| Header (eventName) | Description              | Deep Discovery Inspector detected this protocol in your monitored network.   |
| Header (severity)  | Severity                 | <ul style="list-style-type: none"> <li>• 2: Informational</li> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul> |
| app                | Protocol                 | Example: HTTP  |
| c6a1               | Interested IPv6          | Example: 2001:0:0:1::21  |
| c6a1Label          | Interested IPv6          | InterestedIPv6   |
| c6a2               | Source IPv6 address      | Example: 2001:0:0:1::21  |
| c6a2Label          | Source IPv6 address      | Source IPv6 Address  |
| c6a3               | Destination IPv6 address | Example: 2001:0:0:1::21  |
| c6a3Label          | Destination IPv6 address | Destination IPv6 Address   |
| c6a4               | Peer IPv6 address        | Example: 2001:0:0:1::21  |
| c6a4Label          | Peer IPv6 address        | PeerIPv6   |
| cnt                | Total count              | Example: 1   |

| CEF KEY                      | DESCRIPTION   | VALUE  |
|------------------------------|---|--|
| cn3                          | Threat type   | 6  |
| cn3Label                     | Threat type   | ThreatType   |
| destinationTranslatedAddress | Peer IP   | Example: 10.1.144.199  |
| deviceDirection              | Packet direction  | <ul style="list-style-type: none"> <li>0: Source is external</li> <li>1: Source is internal</li> <li>2: Unknown</li> </ul>         |
| deviceExternalId             | Appliance GUID  | Example: 6B593E17AFB7-40FB28-A4CE-0462-A536  |
| devicePayloadId              | An extendable field.<br>Format: {threat_type};{log_id};{with pcap file captured}{:extensions}*<br>Examples: | <ul style="list-style-type: none"> <li>With pcap file captured: 2:10245:P</li> <li>Without pcap file captured: 2:10245:</li> </ul> |
| dhost                        | Destination host name   | Example: dhost1  |
| dmac                         | Destination MAC   | Example: 00:0C:29:6E:CB:F9   |
| 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   |
| flexNumber1                  | vLANId  | Example: 4095  |
| flexNumber1Label             | vLANId  | vLANId   |
| rt                           | Log generation time   | Example: Mar 09 2015 17:05:21 GMT +08:00   |

| CEF KEY                 | DESCRIPTION       | VALUE                      |
|-------------------------|-------------------|----------------------------|
| shost                   | Source host name  | Example: shost1            |
| smac                    | Source MAC        | Example: 00:0C:29:6E:CB:F9 |
| sourceTranslatedAddress | Interested IP     | Example: 10.1.144.199      |
| spt                     | Source port       | Value between 0 and 65535  |
| src                     | Source IP address | Example: 10.1.144.199      |

### Log Sample:

```

CEF:0|Trend Micro|Deep Discovery Inspector|5.0.1329|
100120|Deep
Discovery Inspector detected the protocol in your
monitored network.|2|dvc=172.22.9.32 dvcmac=
00:50:56:AD:03:BD
dvchost=localhost deviceExternalId=E9A3FA433916-
4738984C-A4BF-84A0-D603
rt=Jun 22 2017 10:06:24 GMT+08:00 app=eDonkey
deviceDirection=1 dhost=10.1.100.223 dst=10.1.100.223
dpt=4662 dmac=00:0c:29:a7:72:74 shost=10.1.117.231
src=10.1.117.231 spt=39933 smac=00:30:da:2d:47:32
cn3Label=Threat Type cn3=6 sourceTranslatedAddress=
10.1.117.231
destinationTranslatedAddress=10.1.100.223 cnt=1
flexNumber1Label=vLANId flexNumber1=4095
devicePayloadId=6:11:P

```

## CEF Web Reputation Logs

**TABLE 3-3. CEF Web Reputation Logs**

| CEF KEY         | DESCRIPTION        | VALUE       |
|-----------------|--------------------|-------------|
| Header (logVer) | CEF format version | CEF: 0      |
| Header (vendor) | Appliance vendor   | Trend Micro |

| CEF KEY            | DESCRIPTION              | VALUE  |
|--------------------|--------------------------|--|
| Header (pname)     | Appliance product        | Deep Discovery Inspector   |
| Header (pver)      | Appliance version        | Example: 3.8.1181  |
| Header (eventid)   | Signature ID             | 100101   |
| Header (eventName) | Description              | Example: Dangerous URL in Web Reputation Services database - HTTP (Request)  |
| Header (severity)  | Severity                 | <ul style="list-style-type: none"> <li>• 2: Informational</li> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul> |
| app                | Protocol                 | Example: HTTP  |
| c6a1               | Interested IPv6          | Example: 2001:0:0:1::21  |
| c6a1Label          | Interested IPv6          | InterestedIPv6   |
| c6a2               | Source IPv6 address      | Example: 2001:0:0:1::21  |
| c6a2Label          | Source IPv6 address      | Source IPv6 Address  |
| c6a3               | Destination IPv6 address | Example: 2001:0:0:1::21  |
| c6a3Label          | Destination IPv6 address | Destination IPv6 Address   |
| c6a4               | Peer IPv6 address        | Example: 2001:0:0:1::21  |
| c6a4Label          | Peer IPv6 address        | PeerIPv6   |
| cn1                | CCCA detection           | 0 or 1   |
| cn1Label           | CCCA detection           | CCCA_Detection   |
| cn2                | Score                    | Example: 49  |
| cn2Label           | Score                    | WRSScore   |
| cn3                | Threat type              | Example: 5   |



| CEF KEY                      | DESCRIPTION      | VALUE  |
|------------------------------|------------------|--|
| cn3Label                     | Threat type      | Threat Type  |
| cs1                          | Mail subject     | Example: hello   |
| cs1Label                     | Mail subject     | MailSubject  |
| cs2                          | Category         | Example: Gambling  |
| cs2Label                     | Category         | URLCategory  |
| cs3                          | Host name        | Example: CLIENT1   |
| cs3Label                     | Host name        | HostName_Ext   |
| cs4                          | Attack Phase     | <ul style="list-style-type: none"> <li>• Intelligence Gathering</li> <li>• Point of Entry</li> <li>• Command and Control Communication</li> <li>• Lateral Movement</li> <li>• Asset and Data Discovery</li> <li>• Data Exfiltration</li> <li>• Nil (no applicable attack phase)</li> </ul> |
| cs4Label                     | Attack Phase     | pAttackPhase   |
| destinationTranslatedAddress | Peer IP          | Example: 10.1.144.199  |
| deviceDirection              | Packet direction | <ul style="list-style-type: none"> <li>• 0: Source is external</li> <li>• 1: Source is internal</li> <li>• 2: Unknown</li> </ul>   |
| deviceExternalId             | Appliance GUID   | Example: 6B593E17AFB7-40FB28-A4CE-0462-A536  |

| CEF KEY                  | DESCRIPTION  | VALUE  |
|--------------------------|--|--|
| devicePayloadId          | An extendable field.<br>Format: {threat_type};<br>{log_id};{with pcap file<br>captured}{:extensions}*<br>Examples:<br>• With pcap file captured:<br>2:10245:P<br>• Without pcap file captured:<br>2:10245: |  |
| dhost                    | Destination host name  | Example: dhost1                              |
| dmac                     | Destination MAC  | Example: 00:0C:29:6E:CB:F9                   |
| dpt                      | Destination port   | Value between 0 and 65535                    |
| dst                      | Destination IP address   | Example: 10.1.144.199                        |
| duser                    | Mail recipient   | Example: duser1                              |
| 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                   |
| flexNumber1              | vLANid   | Example: 4095                                |
| flexNumber1Label         | vLANid   | vLANid                                       |
| request                  | URL  | Example: http://1.2.3.4/query?<br>term=value |
| requestClientApplication | User agent   | Example: IE                                  |
| rt                       | Log generation time  | Example: Mar 09 2015 17:05:21 GMT<br>+08:00  |
| shost                    | Source host name   | Example: shost1                              |
| smac                     | Source MAC   | Example: 00:0C:29:6E:CB:F9                   |
| sourceTranslatedAddress  | Interested IP  | Example: 10.1.144.199                        |
| spt                      | Source port  | Value between 0 and 65535                    |
| src                      | Source IP address  | Example: 10.1.144.199                        |

| CEF KEY | DESCRIPTION | VALUE           |
|---------|-------------|-----------------|
| suser   | Mail sender | Example: suser1 |

Log sample:

```

CEF:0|Trend Micro|Deep Discovery Inspector
|5.0.1329|100101|Ransomware
URL in Web Reputation Services database - HTTP
(Request)|8|dvc=172.22.9.32 dvcmac=00:50:56:AD:03:BD
dvchost=localhost deviceExternalId=E9A3FA433916-4738984
C-A4BF-84A0-D603
rt=Jun 22 2017 10:00:17 GMT+08:00 cs3Label=HostName_Ext
cs3=ca95-1.winshipway.com cn2Label=WRSScore cn2=49
cn3Label=Threat Type cn3=5 dmac=00:16:c8:65:98:d5
shost=172.22.9.5 src=172.22.9.5 spt=41757
smac=00:50:56:82:e7:a9
sourceTranslatedAddress=172.22.9.5
cn1Label=CCCA_Detection
cn1=1 request=http://ca95-1.winshipway.com/
requestClientApplication=Wget/1.12
(linux-gnu) app=HTTP deviceDirection=1
dhost=150.70.162.115
dst=150.70.162.115 dpt=80 cs2Label=URLCategory
cs2=Ransomware destinationTranslatedAddress=
150.70.162.115
cs4Label=pAttackPhase cs4=Command and Control
Communication flexNumber1Label=vLANId flexNumber1=4095
request=http://ca95-1.winshipway.com/
devicePayloadId=5:17:

```

## CEF System Logs

**TABLE 3-4. CEF System Logs**

| CEF KEY         | DESCRIPTION        | VALUE  |
|-----------------|--------------------|--------|
| Header (logVer) | CEF format version | CEF: 0 |

| CEF KEY            | DESCRIPTION           | VALUE  |
|--------------------|-----------------------|--|
| Header (vendor)    | Appliance vendor      | Trend Micro  |
| Header (pname)     | Appliance product     | Deep Discovery Inspector   |
| Header (pver)      | Appliance version     | Example: 3.8.1181  |
| Header (eventid)   | Signature ID          | <ul style="list-style-type: none"> <li>• 300102</li> <li>• 300999</li> </ul>   |
| Header (eventName) | Description           | Example: The system time setting has been changed.   |
| Header (severity)  | Severity              | <ul style="list-style-type: none"> <li>• 2: Informational</li> <li>• 4: Warning</li> <li>• 6: Severe</li> </ul> Example: 2 |
| c6a2               | Source IPv6 address   | Example: 2001:0:0:1::21  |
| c6a2Label          | Source IPv6 address   | Source IPv6 Address  |
| deviceExternalId   | Appliance GUID        | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536  |
| duser              | Action by             | Example: admin   |
| 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   |
| outcome            | Outcome               | <ul style="list-style-type: none"> <li>• Success</li> <li>• Failure</li> </ul> Example: Success                            |
| rt                 | Log generation time   | Example: Mar 09 2015 17:05:21 GMT +08:00   |
| src                | User IP address       | Example: 10.1.1.1  |

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Inspector|3.8.1175|300999|The system time setting has been changed.|2|dvc=10.201.156.143 dvcmac=00:0C:29:A6:53:0C dvchost=ddi38-143 deviceExternalId=6B593E17AFB7-40FBBB28-A4CE-0462-A536 rt=Mar 09 2015 16:46:08 GMT+08:00
```

## CEF Virtual Analyzer Logs: File Analysis Events

**TABLE 3-5. CEF 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 Inspector  |
| Header (pver)      | Appliance version  | Example: 3.8.1181   |
| Header (eventid)   | Signature ID       | 200119  |
| Header (eventName) | Description        | Sample file sandbox analysis is finished.   |
| Header (severity)  | Severity           | 3 (fixed value)   |
| cn1                | GRID is known good | <ul style="list-style-type: none"> <li>• 0: Bad file</li> <li>• -1: Unknown file</li> <li>• 1: Good file</li> </ul>                     |
| cn1Label           | GRID is known good | GRIDIsKnownGood   |
| cn2                | ROZ rating         | <ul style="list-style-type: none"> <li>• 0: No risk</li> <li>• 1: Low risk</li> <li>• 2: Medium risk</li> <li>• 3: High risk</li> </ul> |

| CEF KEY          | DESCRIPTION           | VALUE  |
|------------------|-----------------------|--|
| cn2Label         | ROZ rating            | ROZRating  |
| cn3              | PcapReady             | Example: 0   |
| cn3Label         | PcapReady             | PcapReady  |
| cs1              | Sandbox image type    | Example: win7  |
| cs1Label         | Sandbox image type    | SandboxImageType   |
| cs2              | Virus name            | Example: HEUR_NAMETRICK.A                                |
| cs2Label         | Virus name            | MalwareName  |
| cs3              | Parent SHA1           | Example:<br>1EDD5B38DE4729545767088C5CAB<br>395E4197C8F3 |
| cs3Label         | Parent SHA1           | ParentFileSHA1   |
| deviceExternalId | Appliance GUID        | Example: 6B593E17AFB7-40FBBB28-<br>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:<br>1EDD5B38DE4729545767088C5CAB<br>395E4197C8F3 |
| fileType         | True file type        | Example: WIN32 EXE                                       |
| fname            | File name             | Example: excel.rar                                       |
| fsize            | File size             | Example: 131372  |
| rt               | Analysis time         | Example: Mar 09 2015 17:05:21 GMT<br>+08:00              |

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Inspector|3.8.1181|200119|S
ample file sandbox analysis is finished|3| rt=Mar 11 2015 06
:51:46 GMT-04:00 dvc=10.201.156.143 dvchost=ddi38-143 dvcmac
=00:0C:29:A6:53:0C deviceExternalId=D2C1D6D20FF8-4FC98F92-25
EB-D7DA-AF0E fname=Tomb Raider.rar fileHash=1E4677A1EF1FBAD1
1F8D06A9DAD8103C2CE861A9 fileType=RAR fsize=131372 cs1Label=
SandboxImageType cs1=MAK_win7sp1en_offices_noab_TL cn2Label=
ROZRating cn2=1 cn1Label=GRIDIsKnownGood cn1=-1 cs2Label=Mal
wareName cs2=HEUR_NAMETRICK.A cn3Label=PcapReady cn3=0
```

## CEF Virtual Analyzer Logs: Notable Characteristics Events

**TABLE 3-6. CEF 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 Inspector                          |
| Header (pver)      | Appliance version       | Example: 3.8.1181                                 |
| Header (eventid)   | Signature ID            | 200127  |
| Header (eventName) | Description             | Notable Characteristics of the analyzed sample    |
| Header (severity)  | Severity                | 6 (fixed value)                                   |
| cs1                | Violated policy name    | Example: Suspicious network or messaging activity |
| cs1Label           | Violated policy name    | PolicyCategory                                    |
| cs2                | Analysis violated event | Example: Uses spoofed version information         |
| cs2Label           | Analysis violated event | PolicyName  |

| CEF KEY          | DESCRIPTION           | VALUE  |
|------------------|-----------------------|--|
| deviceExternalId | Appliance GUID        | Example: 6B593E17AFB7-40FB28-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:<br>1EDD5B38DE4729545767088C5CAB<br>395E4197C8F3 |
| fileType         | True file type        | Example: WIN32 EXE                                       |
| fname            | File name             | Example: excel.rar                                       |
| fsize            | File size             | Example: 131372  |
| msg              | Details               | Example: The file has no company information.            |
| rt               | Analysis time         | Example: Mar 09 2015 17:05:21 GMT +08:00                 |

### Log sample:

```
CEF:0|Trend Micro|Deep Discovery Inspector|3.8.1181|200127|N
otable Characteristics of the analyzed sample|6|rt=Mar 11 20
15 05:00:26 GMT-04:00 dvc=10.201.156.143 dvchost=ddi38-143 d
vcmac=00:0C:29:A6:53:0C deviceExternalId=D2C1D6D20FF8-4FC98F
92-25EB-D7DA-AF0E fname=DTAS_WIN32_07 fileHash=672B1A8ADB412
C272CCA21A214732C447B650349 fileType=WIN32 EXE fsize=290304
cs1Label=PolicyCategory cs1=Deception, social engineering ms
g=The file has no company information. cs2Label=PolicyName c
s2=Uses spoofed version information
```



## CEF Virtual Analyzer Logs: Deny List Transaction Events

**TABLE 3-7. CEF 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 Inspector  |
| Header (pver)      | Appliance version       | Example: 3.8.1181   |
| Header (eventid)   | Signature ID            | 200120  |
| Header (eventName) | Description             | Deny List updated   |
| Header (severity)  | Severity                | 3 (fixed value)   |
| act                | The action in the event | Add or Remove   |
| cs1                | Type                    | <ul style="list-style-type: none"> <li>• Deny List IP/Port</li> <li>• Deny List URL</li> <li>• Deny List File SHA1</li> <li>• Deny List Domain</li> </ul> |
| cs1Label           | Type                    | type  |
| cs2                | Risk level              | <ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> <li>• Confirmed malware</li> </ul>                                    |
| cs2Label           | Risk level              | RiskLevel   |
| deviceExternalId   | Appliance GUID          | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536   |

| CEF KEY  | DESCRIPTION            | VALUE  |
|----------|------------------------|--|
| dhost    | Destination host name  | Example: iplasticalsex.ru                                |
| 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      | Report end time        | Example: Mar 09 2015 17:05:21 GMT +08:00                 |
| fileHash | SHA1                   | Example:<br>1EDD5B38DE4729545767088C5CAB<br>395E4197C8F3 |
| request  | URL                    | Example: http://1.2.3.4/query?<br>term=value             |
| rt       | Analysis time          | Example: Mar 09 2015 17:05:21 GMT +08:00                 |

### Log sample:

```
CEF:0|Trend Micro|Deep Discovery Inspector|3.8.1181|200120|Deny List updated|3|rt=Mar 11 2015 07:15:45 GMT-04:00 dvc=10.201.156.143 dvchost=ddi38-143 dvcmac=00:0C:29:A6:53:0C deviceExternalId=D2C1D6D20FF8-4FC98F92-25EB-D7DA-AF0E cs1Label=type cs1=Deny List Domain end=Apr 10 2015 07:15:35 GMT-04:00 a ct=Add dhost=iplasticalsex.ru cs2Label=RiskLevel cs2=Medium
```

# Chapter 4

## Syslog Content Mapping - LEEF

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

- [LEEF Threat Logs on page 4-2](#)
- [LEEF Disruptive Application Logs on page 4-9](#)
- [LEEF Web Reputation Logs on page 4-12](#)
- [LEEF System Logs on page 4-16](#)
- [LEEF Correlation Incident Logs on page 4-17](#)
- [LEEF Virtual Analyzer Logs: File Analysis Events on page 4-20](#)
- [LEEF Virtual Analyzer Logs: Notable Characteristics Events on page 4-22](#)

**Note**

In LEEF log syntax, separate event attributes with a tab delimiter, <009>.

---

## LEEF Threat Logs

**TABLE 4-1. LEEF Threat Logs**

| LEEF KEY              | DESCRIPTION                    | VALUE  |
|-----------------------|--------------------------------|--|
| Header (logVer)       | LEEF format version            | LEEF: 1.0  |
| Header (vendor)       | Appliance vendor               | Trend Micro  |
| Header (pname)        | Appliance product              | Deep Discovery Inspector   |
| Header (pver)         | Appliance version              | Example: 3.8.1181  |
| Header (eventName)    | Event Name                     | <ul style="list-style-type: none"> <li>• MALWARE_DETECTION</li> <li>• MALWARE_OUTBREAK_DETECTION</li> <li>• SECURITY_RISK_DETECTION</li> </ul> |
| act                   | The action in the event        | blocked or not blocked   |
| aggregatedCnt         | Aggregated count               | Example: 1   |
| aptRelated            | Indicates an APT-related event | 0 or 1   |
| botCommand            | BOT command                    | Example: COMMIT  |
| botUrl                | BOT URL                        | Example: trend.com   |
| cccaDestination       | CCCA address                   | Example: 10.1.144.199  |
| cccaDestinationFormat | CCCA type                      | <ul style="list-style-type: none"> <li>• IP_DOMAIN</li> <li>• IP_DOMAIN_PORT</li> <li>• URL</li> <li>• EMAIL</li> </ul>                        |
| cccaDetection         | CCCA detection                 | 0 or 1   |

| LEEF KEY                  | DESCRIPTION             | VALUE  |
|---------------------------|-------------------------|--|
| cccaDetectionSource       | CCCA log is detected by | <ul style="list-style-type: none"> <li>GLOBAL_INTELLIGENCE</li> <li>VIRTUAL_ANALYZER</li> <li>USER_DEFINED</li> </ul>        |
| cccaRiskLevel             | CCCA Risk Level         | <ul style="list-style-type: none"> <li>0: Unknown</li> <li>1: Low</li> <li>2: Medium</li> <li>3: High</li> </ul>             |
| channelName               | Channel name            | Example: IRCChannel1   |
| chatUserName              | Nickname                | Example: IRCUser1  |
| cnt                       | Total count             | Example: 1   |
| compressedFileName        | File name in archive    | Example: mtxlegih.dll  |
| detectionType             | Detection type          | <ul style="list-style-type: none"> <li>0: Known detection</li> <li>1: Unknown detection</li> <li>2: OPS detection</li> </ul> |
| deviceDirection           | Packet direction        | <ul style="list-style-type: none"> <li>0: Source is external</li> <li>1: Source is internal</li> <li>2: Unknown</li> </ul>   |
| deviceGUID                | Appliance GUID          | Example: 6B593E17AFB7-40FB8B28-A4CE-0462-A536  |
| deviceMacAddress          | Appliance MAC address   | Example: 00:0C:29:6E:CB:F9   |
| deviceRiskConfidenceLevel | Confidence level        | <ul style="list-style-type: none"> <li>1: High</li> <li>2: Medium</li> <li>3: Low</li> <li>0: Undefined</li> </ul>           |

| LEEF KEY        | DESCRIPTION                                  | VALUE   |
|-----------------|--|---|
| devTime         | Log generation time                          | Example: Mar 09 2015 17:05:21 GMT +08:00  |
| devTimeFormat   | Time format                                  | MMM dd yyyy HH:mm:ss z  |
| dhost           | Destination host name                        | Example: dhost1   |
| dOSName         | Destination host OS                          | Example: Android  |
| dst             | Destination IP address                       | Example: 10.1.144.199   |
| dstGroup        | Network Group assigned to a destination host | Example: monitor1   |
| dstMAC          | Destination MAC                              | Example: 00:0C:29:6E:CB:F9  |
| dstPort         | Destination port                             | Value between 0 and 65535   |
| dstZone         | Destination zone                             | <ul style="list-style-type: none"> <li>• 0: Not in monitored network</li> <li>• 1: In monitored network and trusted</li> <li>• 2: In monitored network and untrusted</li> </ul> |
| duser           | Mail recipient                               | Example: duser1   |
| dUser1          | Destination user name 1                      | Example: admin  |
| dUser1LoginTime | Destination user log on time 1               | Example: Mar 09 2015 17:05:21 GMT +08:00  |
| dUser2          | Destination user name 2                      | Example: admin  |
| dUser2LoginTime | Destination user log on time 2               | Example: Mar 09 2015 17:05:21 GMT +08:00  |
| dUser3          | Destination user name 3                      | Example: admin  |
| dUser3LoginTime | Destination user log on time 3               | Example: Mar 09 2015 17:05:21 GMT +08:00  |
| dvc             | Appliance IP address                         | Example: 10.1.144.199   |

| LEEF KEY         | DESCRIPTION                  | VALUE  |
|------------------|------------------------------|--|
| dvchost          | Appliance host name          | Example: localhost                                   |
| evtCat           | Event category               | Example: Suspicious Traffic                          |
| evtSubCat        | Event subcategory            | Example: Email                                       |
| fileHash         | SHA1                         | Example:1EDD5B38DE4729545767088C5CAB395E4197C8F3     |
| filePath         | File path                    | Example: SHARE\\                                     |
| fileType         | Real file type               | Example: 1638400                                     |
| fname            | File name                    | Example: excel.rar                                   |
| fsize            | File size                    | Example: 131372                                      |
| hackerGroup      | Hacker group                 | Example: Comment Crew                                |
| hackingCampaign  | Hacking campaign             | Example:Aurora                                       |
| hostName         | Host name                    | Example: CLIENT1                                     |
| interestedIp     | Interested IP                | Example: 10.1.144.199                                |
| mailMsgSubject   | Mail subject                 | Example: hello                                       |
| malFamily        | Malware family               | Example:Duqu   |
| malName          | Malware name                 | Example: HEUR_NAMETRICK.A                            |
| malType          | Malware type                 | Example: MALWARE                                     |
| mitigationTaskId | Event task ID for mitigation | Example:<br>dc036acb-9a2e-4939-8244-dedbda9ec4ba     |
| msg              | Description                  | Example: HEUR_NAMETRICK.A - SMTP (Email)             |
| oldFileHash      | Mail attachment SHA1         | Example:<br>1EDD5B38DE4729545767088C5CAB395E4197C8F3 |

| LEEF KEY                 | DESCRIPTION                    | VALUE  |
|--------------------------|--------------------------------|--|
| oldFileName              | Mail attachment file name      | Example: excel.rar   |
| oldFileSize              | Mail attachment file size      | Example: 150000  |
| oldFileType              | Mail attachment file type      | Example: 1638400   |
| pAttackPhase             | Primary attack phase           | <ul style="list-style-type: none"> <li>• Intelligence Gathering</li> <li>• Point of Entry</li> <li>• Command and Control Communication</li> <li>• Lateral Movement</li> <li>• Asset and Data Discovery</li> <li>• Data Exfiltration</li> <li>• Nil (no applicable attack phase)</li> </ul> |
| pComp                    | Detection engine/<br>component | Example: VSAPI   |
| peerIP                   | Peer IP                        | Example: 10.1.144.199  |
| proto                    | Protocol                       | Example: SMTP  |
| protoGroup               | Protocol group                 | Example: SMTP  |
| ptype                    | Application type               | IDS  |
| requestClientApplication | User agent                     | Example: IE  |
| riskType                 | Potential risk                 | <ul style="list-style-type: none"> <li>• 0: Known risk</li> <li>• 1: Potential risk</li> </ul>   |
| ruleId                   | Rule ID                        | Example: 52  |
| sAttackPhase             | Secondary attack phase         | Example: Point of Entry  |



| LEEF KEY        | DESCRIPTION                             | VALUE   |
|-----------------|---|---|
| sev             | Severity                                | <ul style="list-style-type: none"> <li>• 2: Informational</li> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul>  |
| shost           | Source host name                        | Example: shost1   |
| sOSName         | Source host OS                          | Example: Android  |
| src             | Source IP address                       | Example: 10.1.144.199   |
| srcGroup        | Network Group assigned to a source host | Example: monitor1   |
| srcMAC          | Source MAC                              | Example: 00:0C:29:6E:CB:F9  |
| srcPort         | Source port                             | Value between 0 and 65535   |
| srcZone         | Source zone                             | <ul style="list-style-type: none"> <li>• 0: Not in monitored network</li> <li>• 1: In monitored network and trusted</li> <li>• 2: In monitored network and untrusted</li> </ul> |
| suid            | User name                               | Example: User1  |
| suser           | Mail sender                             | Example: suser1   |
| sUser1          | Source user name 1                      | Example: admin  |
| sUser1LoginTime | Source user log on time 1               | Example: Mar 09 2015 17:05:21 GMT +08:00  |
| sUser2          | Source user name 2                      | Example: admin  |
| sUser2LoginTime | Source user log on time 2               | Example: Mar 09 2015 17:05:21 GMT +08:00  |
| sUser3          | Source user name 3                      | Example: admin  |

| LEEF KEY        | DESCRIPTION               | VALUE  |
|-----------------|---------------------------|--|
| sUser3LoginTime | Source user log on time 3 | Example: Mar 09 2015 17:05:21 GMT +08:00   |
| threatType      | Threat type               | <ul style="list-style-type: none"> <li>• 0: Malicious content</li> <li>• 1: Malicious behavior</li> <li>• 2: Suspicious behavior</li> <li>• 3: Exploit</li> <li>• 4: Grayware</li> </ul> |
| url             | URL                       | Example: http://1.2.3.4/query?term=value   |
| vLANid          | VLANID                    | Value between 0 and 4095   |

### Log sample:



#### Note

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

```
LEEF:1.0|Trend Micro|Deep Discovery Inspector|3.8.1175|SECURITY_RISK_DETECTION|devTimeFormat=MMM dd yyyy HH:mm:ss z<009>
ptype=IDS<009>dvc=10.201.156.143<009>deviceMacAddress=00:0C:29:A6:53:0C<009>dvchost=ddi38-143<009>deviceGUID=6B593E17AFB7-40FBBB28-A4CE-0462-A536<009>devTime=Mar 09 2015 11:58:24 GMT+08:00<009>sev=6<009>protoGroup=HTTP<009>proto=HTTP<009>vLANId=4095<009>deviceDirection=1<009>dhost=www.freewebs.com<009>dst=216.52.115.2<009>dstPort=80<009>dstMAC=00:1b:21:35:8b:98<009>shost=172.16.1.197<009>src=172.16.1.197<009>srcPort=12121<009>srcMAC=fe:ed:be:ef:5a:c6<009>malType=MALWARE<009>AttackPhase=Point of Entry<009>fname=setting.doc<009>fileType=0<009>fsize=0<009>ruleId=20<009>msg=HEUR_NAMETRIC.K.A - SMTP (Email)<009>deviceRiskConfidenceLevel=2<009>url=http://www.freewebs.com/setting3/setting.doc<009>pComp=CAV<009>riskType=1<009>srcGroup=Default<009>srcZone=1<009>dstZone=0<009>detectionType=1<009>act=not blocked<009>threatType=1<009>interes
```

```
tedIp=172.16.1.197<009>peerIp=216.52.115.2<009>hostName=www.
freewebs.com<009>cnt=1<009>aggregatedCnt=1<009>cccaDestinati
onFormat=URL<009>cccaDetectionSource=GLOBAL_INTELLIGENCE<009
>cccaRiskLevel=2<009>cccaDestination=http://www.freewebs.com
/setting3/setting.doc<009>cccaDetection=1<009>evtCat=Callbac
k evtSubCat=Bot<009>pAttackPhase=Command and Control Communi
cation
```

## LEEF Disruptive Application Logs

**TABLE 4-2. LEEF Disruptive Application Logs**

| LEEF KEY           | DESCRIPTION           | VALUE  |
|--------------------|-----------------------|--|
| Header (logVer)    | LEEF format version   | LEEF: 1.0  |
| Header (vendor)    | Appliance vendor      | Trend Micro  |
| Header (pname)     | Appliance product     | Deep Discovery Inspector   |
| Header (pver)      | Appliance version     | Example: 3.8.1181  |
| Header (eventName) | Event Name            | DISRUPTIVE_APPLICATION_DETECT<br>ION   |
| aggregatedCnt      | AggrCount             | Example: 1   |
| cnt                | Total count           | Example: 1   |
| deviceDirection    | Packet direction      | <ul style="list-style-type: none"> <li>• 0: Source is external</li> <li>• 1: Source is internal</li> <li>• 2: Unknown</li> </ul> |
| deviceGUID         | Appliance GUID        | Example: 6B593E17AFB7-40FBBB28-<br>A4CE-0462-A536  |
| deviceMacAddress   | Appliance MAC address | Example: 00:0C:29:6E:CB:F9   |
| devTime            | Log generation time   | Example: Mar 09 2015 17:05:21 GMT<br>+08:00  |

| LEEF KEY      | DESCRIPTION                                  | VALUE   |
|---------------|--|---|
| devTimeFormat | Time format                                  | MMM dd yyyy HH:mm:ss z  |
| dhost         | Destination host name                        | Example: dhost1   |
| dOSName       | Destination host OS                          | Example: Android  |
| dst           | Destination IP address                       | Example: 10.1.144.199   |
| dstGroup      | Network Group assigned to a destination host | Example: monitor1   |
| dstMAC        | Destination MAC                              | Example: 00:0C:29:6E:CB:F9  |
| dstPort       | Destination port                             | Value between 0 and 65535   |
| dstZone       | Destination zone                             | <ul style="list-style-type: none"> <li>• 0: Not in monitored network</li> <li>• 1: In monitored network and trusted</li> <li>• 2: In monitored network and not trusted</li> </ul> |
| dvc           | Appliance IP address                         | Example: 10.1.144.199   |
| dvchost       | Appliance host name                          | Example: localhost  |
| interestedIp  | Interested IP                                | Example: 10.1.144.199   |
| msg           | Description                                  | Example: Deep Discovery Inspector detected the protocol in your monitored network   |
| pComp         | Detection engine/ component                  | Example: VSAPI  |
| peerIP        | Peer IP                                      | Example: 10.1.144.199   |
| proto         | Protocol                                     | Example: SMTP   |
| protoGroup    | Protocol group                               | Example: SMTP   |
| ptype         | Application type                             | IDS   |

| LEEF KEY   | DESCRIPTION                             | VALUE   |
|------------|---|---|
| sev        | Severity                                | <ul style="list-style-type: none"> <li>• 2: Informational</li> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul>  |
| shost      | Source host name                        | Example: shost1   |
| sOSName    | Source host OS                          | Example: Android  |
| src        | Source IP address                       | Example: 10.1.144.199   |
| srcGroup   | Network Group assigned to a source host | Example: monitor1   |
| srcMAC     | Source MAC                              | Example: 00:0C:29:6E:CB:F9  |
| srcPort    | Source port                             | Value between 0 and 65535   |
| srcZone    | Source zone                             | <ul style="list-style-type: none"> <li>• 0: Not in monitored network</li> <li>• 1: In monitored network and trusted</li> <li>• 2: In monitored network and not trusted</li> </ul> |
| threatType | Threat type                             | 6   |
| vLANid     | VLANID                                  | Value between 0 and 4095  |

Log sample:



**Note**

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

```
LEEF:1.0|Trend Micro|Deep Discovery Inspector|3.8.1175|DISRU
PTIVE_APPLICATION_DETECTION|devTimeFormat=MMM dd yyyy HH:mm:
ss z<009>dvc=10.201.156.143<009>deviceMacAddress=00:0C:29:A6
:53:0C<009>dvchost=ddi38-143<009>deviceGUID=6B593E17AFB7-40F
```

```
BBB28-A4CE-0462-A536<009>ptype=IDS<009>devTime=Mar 09 2015 14:20:38 GMT+08:00<009>sev=2<009>protoGroup=STREAMING<009>proto=WMSPP<009>vLANId=4095<009>deviceDirection=1<009>dhost=12.190.48.13<009>dst=12.190.48.13<009>dstPort=80<009>dstMAC=00:17:9a:65:f3:05<009>shost=192.168.33.2<009>src=192.168.33.2<009>srcPort=35125<009>srcMAC=00:16:6f:a1:3d:7a<009>msg=Deep Discovery Inspector detected the protocol in your monitored network.<009>pComp=CAV<009>threatType=6<009>srcGroup=Default<009>srcZone=1<009>dstZone=0<009>interestedIp=192.168.33.2<009>peerIp=12.190.48.13<009>cnt=1<009>aggregatedCnt=1
```

## LEEF Web Reputation Logs

**TABLE 4-3. LEEF Web Reputation Logs**

| LEEF KEY            | DESCRIPTION             | VALUE   |
|---------------------|-------------------------|---|
| Header (logVer)     | LEEF format version     | LEEF: 1.0   |
| Header (vendor)     | Appliance vendor        | Trend Micro   |
| Header (pname)      | Appliance product       | Deep Discovery Inspector  |
| Header (pver)       | Appliance version       | Example: 3.8.1181   |
| Header (eventName)  | Event Name              | WEB_THREAT_DETECTION  |
| cccaDetection       | CCCA detection          | 0 or 1  |
| cccaDetectionSource | CCCA log is detected by | <ul style="list-style-type: none"> <li>• GLOBAL_INTELLIGENCE</li> <li>• VIRTUAL_ANALYZER</li> <li>• USER_DEFINED</li> </ul> |
| cccaRiskLevel       | CCCA Risk Level         | <ul style="list-style-type: none"> <li>• 0: Unknown</li> <li>• 1: Low</li> <li>• 2: Medium</li> <li>• 3: High</li> </ul>    |

| LEEF KEY         | DESCRIPTION                                  | VALUE   |
|------------------|--|---|
| deviceDirection  | Packet direction                             | <ul style="list-style-type: none"> <li>• 0: Source is external</li> <li>• 1: Source is internal</li> <li>• 2: Unknown</li> </ul>  |
| deviceGUID       | Appliance GUID                               | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536   |
| deviceMacAddress | Appliance MAC address                        | Example: 00:0C:29:6E:CB:F9  |
| devTime          | Log generation time                          | Example: Mar 09 2015 17:05:21 GMT +08:00  |
| devTimeFormat    | Time format                                  | MMM dd yyyy HH:mm:ss z  |
| dhost            | Destination host name                        | Example: dhost1   |
| dOSName          | Destination host OS                          | Example: Android  |
| dst              | Destination IP address                       | Example: 10.1.144.199   |
| dstGroup         | Network Group assigned to a destination host | Example: monitor1   |
| dstMAC           | Destination MAC                              | Example: 00:0C:29:6E:CB:F9  |
| dstPort          | Destination port                             | Value between 0 and 65535   |
| dstZone          | Destination zone                             | <ul style="list-style-type: none"> <li>• 0: Not in monitored network</li> <li>• 1: In monitored network and trusted</li> <li>• 2: In monitored network and not trusted</li> </ul> |
| duser            | Mail recipient                               | Example: duser1   |
| dvc              | Appliance IP address                         | Example: 10.1.144.199   |
| dvchost          | Appliance host name                          | Example: localhost  |
| hostName         | Host name                                    | Example: CLIENT1  |

| LEEF KEY                 | DESCRIPTION                                | VALUE  |
|--------------------------|--|--|
| interestedIp             | Interested IP                              | Example: 10.1.144.199  |
| mailMsgSubject           | Mail subject                               | Example: hello   |
| msg                      | Description                                | Example: Dangerous URL in Web Reputation Services database - HTTP (Request)  |
| pComp                    | Detection engine/<br>component             | Example: VSAPI   |
| peerIP                   | Peer IP                                    | Example: 10.1.144.199  |
| proto                    | Protocol                                   | Example: SMTP  |
| protoGroup               | Protocol group                             | Example: SMTP  |
| ptype                    | Application type                           | IDS  |
| requestClientApplication | User agent                                 | Example: IE  |
| riskScore                | Score                                      | Example: 49  |
| sev                      | Severity                                   | <ul style="list-style-type: none"> <li>• 2: Informational</li> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul> |
| shost                    | Source host name                           | Example: shost1  |
| sOSName                  | Source host OS                             | Example: Android   |
| src                      | Source IP address                          | Example: 10.1.144.199  |
| srcGroup                 | Network Group assigned<br>to a source host | Example: monitor1  |
| srcMAC                   | Source MAC                                 | Example: 00:0C:29:6E:CB:F9   |
| srcPort                  | Source port                                | Value between 0 and 65535  |



| LEEF KEY   | DESCRIPTION | VALUE   |
|------------|-------------|---|
| srcZone    | Source zone | <ul style="list-style-type: none"> <li>0: Not in monitored network</li> <li>1: In monitored network and trusted</li> <li>2: In monitored network and not trusted</li> </ul> |
| suser      | Mail sender | Example: suser1   |
| threatType | Threat type | 5   |
| url        | URL         | Example: http://1.2.3.4/query?term=value  |
| urlCat     | Category    | Example: Gambling   |
| vLANid     | VLANID      | Value between 0 and 4095  |

Log sample:



#### Note

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

```
LEEF:1.0|Trend Micro|Deep Discovery Inspector|3.8.1175|WEB_T
HREAT_DETECTION|devTimeFormat=MMM dd yyyy HH:mm:ss z<009>dvc
=10.201.156.143<009>deviceMacAddress=00:0C:29:A6:53:0C<009>d
vchost=ddi38-143<009>deviceGUID=6B593E17AFB7-40FBBB28-A4CE-0
462-A536<009>ptype=IDS<009>devTime=Mar 09 2015 14:06:36 GMT+
08:00<009>sev=6<009>protoGroup=HTTP<009>proto=HTTP<009>vLANI
d=4095<009>deviceDirection=1<009>dhost=www.freewebs.com<009>
dst=216.52.115.2<009>dstPort=80<009>dstMAC=00:1b:21:35:8b:98
<009>shost=172.16.1.197<009>src=172.16.1.197<009>srcPort=121
21<009>srcMAC=fe:ed:be:ef:5a:c6<009>hostName=www.freewebs.co
m<009>msg=Dangerous URL in Web Reputation Services
database - HTTP (Request)<009>url=http:
//www.freewebs.com/setting3/setting.doc<009>
pComp=TMUFE<009>srcGroup=Default<009>
srcZone=1<009>dstZone=0<009>urlCat=
```

```
Disease Vector<009>riskScore=49<009>threatTy
pe=5<009>interestedIp=172.16.1.197<009>
peerIp=216.52.115.2
```

## LEEF System Logs

**TABLE 4-4. LEEF System Logs**

| LEEF KEY           | DESCRIPTION           | VALUE  |
|--------------------|-----------------------|--|
| Header (logVer)    | LEEF format version   | LEEF: 1.0  |
| Header (vendor)    | Appliance vendor      | Trend Micro  |
| Header (pname)     | Appliance product     | Deep Discovery Inspector   |
| Header (pver)      | Appliance version     | Example: 3.8.1181  |
| Header (eventName) | Event Name            | <ul style="list-style-type: none"> <li>• PRODUCT_UPDATE</li> <li>• SYSTEM_EVENT</li> </ul> |
| deviceGUID         | Appliance GUID        | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536  |
| deviceMacAddress   | Appliance MAC address | Example: 00:0C:29:6E:CB:F9   |
| devTime            | Log generation time   | Example: Mar 09 2015 17:05:21 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   |
| msg                | Description           | Example: The system time setting has been changed.   |
| ptype              | Application type      | IDS  |

| LEEF KEY | DESCRIPTION | VALUE  |
|----------|-------------|--|
| sev      | Severity    | <ul style="list-style-type: none"> <li>• 2: Informational</li> <li>• 4: Warning</li> <li>• 6: Severe</li> </ul> Example: 2 |

Log sample:



#### Note

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

```
LEEF:1.0|Trend Micro|Deep Discovery Inspector|3.8.1175|SYSTEM_EVENT|dvc=10.201.156.143<009>deviceMacAddress=00:0C:29:A6:53:0C<009>dvchost=ddi38-143<009>deviceGUID=6B593E17AFB7-40FB
BB28-A4CE-0462-A536<009>ptype=IDS<009>devTimeFormat=MMM dd y
yyy HH:mm:ss z<009>sev=2<009>msg=The system time setting has
been changed.<009>devTime=Mar 09 2015 16:46:08 GMT+08:00
```

## LEEF Correlation Incident Logs

**TABLE 4-5. LEEF Correlation Incident Logs**

| LEEF KEY           | DESCRIPTION         | VALUE                          |
|--------------------|---------------------|--------------------------------|
| Header (logVer)    | LEEF format version | LEEF: 1.0                      |
| Header (vendor)    | Appliance vendor    | Trend Micro                    |
| Header (pname)     | Appliance product   | Deep Discovery Inspector       |
| Header (pver)      | Appliance version   | Example: 3.8.1181              |
| Header (eventName) | Event Name          | SUSPICIOUS_BEHAVIOUR_DETECTION |

| LEEF KEY             | DESCRIPTION            | VALUE  |
|----------------------|------------------------|--|
| data0                | Correlation data 0     | Additional attribute values  |
| data1                | Correlation data 1     | Additional attribute values  |
| data2                | Correlation data 2     | Additional attribute values  |
| data3                | Correlation data 3     | Additional attribute values  |
| data4                | Correlation data 4     | Additional attribute values  |
| data5                | Correlation data 5     | Additional attribute values  |
| data6                | Correlation data 6     | Additional attribute values  |
| data7                | Correlation data 7     | Additional attribute values  |
| data8                | Correlation data 8     | Additional attribute values  |
| data9                | Correlation data 9     | Additional attribute values  |
| deviceDirection      | Packet direction       | <ul style="list-style-type: none"> <li>• 0: Source is external</li> <li>• 1: Source is internal</li> <li>• 2: Unknown</li> </ul> |
| deviceGUID           | Appliance GUID         | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536  |
| deviceMacAddress     | Appliance MAC address  | Example: 00:0C:29:6E:CB:F9   |
| devTime              | Log generation time    | Example: Mar 09 2015 17:05:21 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   |
| interestedHost       | Interested host name   | Example: trend.net   |
| interestedIp         | Interested IP          | Example: 10.1.144.199  |
| interestedMacAddress | Interested MAC address | Example: 00:0C:29:6E:CB:F9   |

| LEEF KEY        | DESCRIPTION                    | VALUE  |
|-----------------|--------------------------------|--|
| interestedUser  | Interested user name 1         | Example: user1   |
| interestedUser2 | Interested user name 2         | Example: user2   |
| interestedUser3 | Interested user name 3         | Example: user3   |
| pComp           | Detection engine/<br>component | Correlation  |
| proto           | Protocol                       | Example: SMTP  |
| pType           | Application type               | IDS  |
| ruleId          | Rule ID                        | Example: 52  |
| ruleName        | Rule name                      | Example: This host has responded to DNS queries.   |
| sev             | Severity                       | <ul style="list-style-type: none"> <li>• 2: Informational</li> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul> |
| threatName      | Threat name                    | Example: Malicious Bot   |
| threatType      | Threat type                    | Example: Malware-related   |
| userGroup       | User group                     | Example: Default   |

Log sample:



#### Note

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

```
LEEF:1.0|Trend Micro|Deep Discovery Inspector|3.8.1181|SUSPICIOUS_BEHAVIOUR_DETECTION|devTimeFormat=MMM dd yyyy HH:mm:ss z<009>deviceMacAddress=00:0C:29:A6:53:0C<009>dvchost=ddi38-143<009>pComp=Correlation<009>dvc=10.201.156.143<009>pType=I
```

```
DS<009>deviceGUID=D2C1D6D20FF8-4FC98F92-25EB-D7DA-AF0E<009>d
evTime=Mar 11 2015 22:05:50 GMT-04:00<009>sev=2<009>interest
edIp=172.16.0.100<009>interestedHost=172.16.0.100<009>inter
stedMacAddress=00:0c:29:70:45:...36<009>ruleId=47<009>ruleNa
me=This host has responded to DNS queries.<009>threatType=Un
registered Service<009>threatName=Unregistered DNS Server<00
9>proto=DNS Response<009>userGroup=Default<009>deviceDirecti
on=1
```

## LEEF Virtual Analyzer Logs: File Analysis Events

**TABLE 4-6. LEEF File Analysis 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 Inspector                                 |
| Header (pver)      | Appliance version     | Example: 3.8.1181  |
| Header (eventName) | Event Name            | FILE_ANALYZED  |
| deviceGUID         | Appliance GUID        | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536            |
| deviceMacAddress   | Appliance MAC address | Example: 00:0C:29:6E:CB:F9                               |
| deviceOSName       | Sandbox image type    | SandboxImageType   |
| deviceProcessHash  | Parent SHA1           | Example:<br>1EDD5B38DE4729545767088C5CAB<br>395E4197C8F3 |
| devTime            | Analysis time         | Example: Mar 09 2015 17:05:21 GMT<br>+08:00              |
| devTimeFormat      | Time format           | MMM dd yyyy HH:mm:ss z                                   |
| dvc                | Appliance IP address  | Example: 10.1.144.199                                    |

| LEEF KEY        | DESCRIPTION         | VALUE   |
|-----------------|---------------------|---|
| dvchost         | Appliance host name | Example: localhost  |
| fileHash        | File SHA1           | Example:<br>1EDD5B38DE4729545767088C5CAB<br>395E4197C8F3  |
| fileType        | True file type      | Example: WIN32 EXE  |
| fname           | File name           | Example: excel.rar  |
| fsize           | File size           | Example: 131372   |
| gridIsKnownGood | GRID is known good  | <ul style="list-style-type: none"> <li>• 0: Bad file</li> <li>• -1: Unknown file</li> <li>• 1: Good file</li> </ul>                     |
| malName         | Virus name          | Example: HEUR_NAMETRICK.A   |
| pcapReady       | PCAP ready          | Example: 1  |
| pComp           | Detection source    | <ul style="list-style-type: none"> <li>• Sandbox</li> <li>• UDSO (User-Defined Suspicious Objects)</li> </ul>                           |
| rozRating       | ROZ rating          | <ul style="list-style-type: none"> <li>• 0: No risk</li> <li>• 1: Low risk</li> <li>• 2: Medium risk</li> <li>• 3: High risk</li> </ul> |
| sev             | Severity            | 3 (fixed value)   |

Log sample:



**Note**

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

```
LEEF:1.0|Trend Micro|Deep Discovery Inspector|3.8.1181|FILE_
ANALYZED|devTime=Mar 11 2015 07:36:27 GMT-04:00<009>devTimeF
ormat=MMM dd yyyy HH:mm:ss z<009>sev=3<009>pComp=Sandbox<009
>dvc=10.201.156.143<009>dvchost=ddi38-143<009>deviceMacAddre
ss=00:0C:29:A6:53:0C<009>deviceGUID=D2C1D6D20FF8-4FC98F92-25
EB-D7DA-AF0E<009>fname=mwsoemon.exe<009>fileHash=89DE67C5220
91EE259533D9CBDDF37DDB8C8D636<009>malName=Possible_Virus<009
>fileType=WIN32_EXE<009>fsize=59392<009>deviceOSName=MAK_win
7sp1en_offices_noab_TL<009>gridIsKnownGood=-1<009>rozRating=
1<009>pcapReady=1
```

## LEEF Virtual Analyzer Logs: Notable Characteristics Events

**TABLE 4-7. LEEF 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 Inspector                      |
| Header (pver)      | Appliance version     | Example: 3.8.1181                             |
| Header (eventName) | Event Name            | NOTABLE_CHARACTERISTICS                       |
| 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                                 |
| devTime            | Analysis time         | Example: Mar 09 2015 17:05:21 GMT +08:00      |
| devTimeFormat      | Time format           | MMM dd yyyy HH:mm:ss z                        |
| dvc                | Appliance IP address  | Example: 10.1.144.199                         |



| LEEF KEY     | DESCRIPTION             | VALUE  |
|--------------|-------------------------|--|
| dvchost      | Appliance host name     | Example: localhost                                       |
| fileHash     | File SHA1               | Example:<br>1EDD5B38DE4729545767088C5CAB<br>395E4197C8F3 |
| fileType     | True file type          | Example: WIN32 EXE                                       |
| fname        | File name               | Example: excel.rar                                       |
| fsize        | File size               | Example: 131372  |
| msg          | Details                 | Example:<br>www.chapisteriadaniel.com                    |
| pComp        | Detection source        | Sandbox  |
| ruleCategory | Violated policy name    | Example: Internet Explorer Setting<br>Modification       |
| ruleName     | Analysis violated event | Example: Modified important<br>registry items            |
| sev          | Severity                | 6 (fixed value)  |

Log sample:



**Note**

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

```
LEEF:1.0|Trend Micro|Deep Discovery Inspector|3.8.1181|NOTAB
LE_CHARACTERISTICS|devTime=Mar 11 2015 05:00:26 GMT-04:00<00
9>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>sev=6<009>pComp=S
andbox<009>dvc=10.201.156.143<009>dvchost=ddi38-143<009>devi
ceMacAddress=00:0C:29:A6:53:0C<009>deviceGUID=D2C1D6D20FF8-4
FC98F92-25EB-D7DA-AF0E<009>fname=DTAS_WIN32_07<009>fileHash=
672B1A8ADB412C272CCA21A214732C447B650349<009>fileType=WIN32
EXE<009>fsize=290304<009>ruleCategory=Suspicious network or
messaging activity<009>ruleName=Queries DNS server<009>msg=0
```

```
12webpages.com<009>deviceOSName=MAK_win7sp1en_offices_noab_T
L
```

## LEEF Virtual Analyzer Logs: Deny List Transaction Event

**TABLE 4-8. LEEF 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 Inspector   |
| Header (pver)          | Appliance version       | Example: 3.8.1181  |
| Header (eventName)     | Event Name              | DENYLIST_CHANGE  |
| act                    | The action in the event | <ul style="list-style-type: none"> <li>• Add</li> <li>• Remove</li> </ul>  |
| deviceExternalRiskType | Risk level              | <ul style="list-style-type: none"> <li>• Low</li> <li>• Medium</li> <li>• High</li> <li>• Confirmed malware</li> </ul> |
| deviceGUID             | Appliance GUID          | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536  |
| deviceMacAddress       | Appliance MAC address   | Example: 00:0C:29:6E:CB:F9   |
| devTime                | Analysis time           | Example: Mar 09 2015 17:05:21 GMT +08:00   |
| devTimeFormat          | Time format             | MMM dd yyyy HH:mm:ss z   |
| dhost                  | Destination host name   | Example: insta-find.com  |

| LEEF KEY | DESCRIPTION          | VALUE   |
|----------|----------------------|---|
| dpt      | Remote port          | Value between 0 and 65535   |
| dst      | Remote IP            | Example: 10.1.144.199   |
| 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 | File SHA1            | Example:<br>1EDD5B38DE4729545767088C5CAB<br>395E4197C8F3  |
| pComp    | Detection source     | Sandbox   |
| sev      | Severity             | 3 (fixed value)   |
| type     | Deny List type       | <ul style="list-style-type: none"> <li>• Deny List IP/Port</li> <li>• Deny List URL</li> <li>• Deny List File SHA1</li> <li>• Deny List Domain</li> </ul> |
| url      | URL                  | Example: http://1.2.3.4/  |

### Log sample:



#### Note

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

```
LEEF:1.0|Trend Micro|Deep Discovery Inspector|3.8.1181|DENYL
IST_CHANGE|devTime=Mar 11 2015 05:00:42 GMT-04:00<009>devTim
eFormat=MMM dd yyyy HH:mm:ss z<009>sev=3<009>pComp=Sandbox<0
09>dvc=10.201.156.143<009>dvchost=ddi38-143<009>deviceMacAdd
ress=00:0C:29:A6:53:0C<009>deviceGUID=D2C1D6D20FF8-4FC98F92-
25EB-D7DA-AF0E<009>end=Apr 10 2015 05:00:26 GMT-04:00<009>ac
```

```
t=Add<009>dhost=ourdatatransfers.com<009>deviceExternalRiskT  
ype=High<009>type=Deny List Domain
```

# Chapter 5

## Syslog Content Mapping - TMEF

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

- *TMEF Threat Logs on page 5-2*
- *TMEF Disruptive Application Logs on page 5-11*
- *TMEF Web Reputation Logs on page 5-15*
- *TMEF System Logs on page 5-20*
- *TMEF Correlated Incident Logs on page 5-22*
- *TMEF Virtual Analyzer Logs: File Analysis Events on page 5-24*
- *TMEF Virtual Analyzer Logs: Notable Characteristics Events on page 5-26*
- *TMEF Virtual Analyzer Logs: Deny List Transaction Events on page 5-28*

## TMEF Threat Logs

**TABLE 5-1. TMEF Threat Logs**

| TMEF KEY           | DESCRIPTION             | VALUE  |
|--------------------|-------------------------|--|
| Header (logVer)    | TMEF format version     | CEF: 0   |
| Header (vendor)    | Appliance vendor        | Trend Micro  |
| Header (pname)     | Appliance product       | Deep Discovery Inspector   |
| Header (pver)      | Appliance version       | Example: 3.8.1181  |
| Header (eventid)   | Event ID                | <ul style="list-style-type: none"> <li>• 100100</li> <li>• 100118</li> <li>• 100119</li> </ul>   |
| Header (eventName) | Event Name              | <ul style="list-style-type: none"> <li>• MALWARE_DETECTION</li> <li>• MALWARE_OUTBREAK_DETECTION</li> <li>• SECURITY_RISK_DETECTION</li> </ul> |
| Header (severity)  | Severity                | <ul style="list-style-type: none"> <li>• 2: Informational</li> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul>                 |
| act                | The action in the event | blocked or not blocked   |
| app                | Protocol                | Example: HTTP  |
| appGroup           | Protocol group          | Example: HTTP  |
| compressedFileHash | Compressed file SHA1    | Example:<br>1EDD5B38DE4729545767088C5CAB<br>395E4197C8F3   |
| compressedFileName | File name in archive    | Example: mtxlegih.dll  |

| <b>TMEF KEY</b>    | <b>DESCRIPTION</b>             | <b>VALUE</b>   |
|--------------------|--------------------------------|--|
| compressedFileType | Compressed file type           | Example: 0   |
| cnt                | Total count                    | Example: 1   |
| cn1                | CCCA detection                 | 0 or 1   |
| cn1Label           | CCCA detection                 | CCCA_Detection   |
| cn2                | Indicates an APT-related event | 0 or 1   |
| cn2Label           | Indicates an APT-related event | APT Related  |
| cn3                | Potential risk                 | <ul style="list-style-type: none"> <li>• 0: Known risk</li> <li>• 1: Potential risk</li> </ul>   |
| cn3Label           | Potential risk                 | Deep Discovery_PotentialRisk   |
| cn4                | Threat type                    | <ul style="list-style-type: none"> <li>• 0: Malicious content</li> <li>• 1: Malicious behavior</li> <li>• 2: Suspicious behavior</li> <li>• 3: Exploit</li> <li>• 4: Grayware</li> </ul> |
| cn4Label           | Threat type                    | Deep Discovery_ThreatType  |
| cn5                | Aggregated count               | Example: 1   |
| cn5Label           | Aggregated count               | AggregatedCnt  |
| cn6                | CCCA Risk Level                | <ul style="list-style-type: none"> <li>• 0: Unknown</li> <li>• 1: Low</li> <li>• 2: Medium</li> <li>• 3: High</li> </ul>   |
| cn6Label           | CCCA Risk Level                | CCCA_RiskLevel   |

| TMEF KEY | DESCRIPTION                             | VALUE   |
|----------|---|---|
| cn7      | Heuristic flag                          | <ul style="list-style-type: none"> <li>• 0: Non-heuristic detection</li> <li>• 1: Heuristic detection</li> </ul>  |
| cn7Label | Heuristic flag                          | HeurFlag  |
| cs1      | Channel name                            | Example: IRCChannel1  |
| cs1Label | Channel name                            | IRCChannelName  |
| cs2      | Nickname                                | Example: IRCUser1   |
| cs2Label | Nickname                                | IRCUserName   |
| cs3      | Host name                               | Example: CLIENT1  |
| cs3Label | Host name                               | HostName_Ext  |
| cs4      | Network Group assigned to a source host | Example: monitor1   |
| cs4Label | Network Group assigned to a source host | Deep Discovery_SrcGroup   |
| cs5      | Source zone                             | <ul style="list-style-type: none"> <li>• 0: Not in monitored network</li> <li>• 1: In monitored network and trusted</li> <li>• 2: In monitored network and untrusted</li> </ul> |
| cs5Label | Source zone                             | Deep Discovery_SrcZone  |
| cs6      | Detection type                          | <ul style="list-style-type: none"> <li>• 0: Known detection</li> <li>• 1: Unknown detection</li> <li>• 2: OPS detection</li> </ul>  |
| cs6Label | Detection type                          | Deep Discovery_DetectionType  |
| cs7      | BOT command                             | Example: COMMIT   |
| cs7Label | BOT command                             | BOT_CMD   |



| <b>TMEF KEY</b> | <b>DESCRIPTION</b>                           | <b>VALUE</b>  |
|-----------------|--|---|
| cs8             | BOT url                                      | Example: trend.com  |
| cs8Label        | BOT url                                      | BOT_URL   |
| cs9             | Network Group assigned to a destination host | Example: monitor1   |
| cs9Label        | Network Group assigned to a destination host | Deep Discovery_DstGroup   |
| cs10            | Destination zone                             | <ul style="list-style-type: none"> <li>• 0: Not in monitored network</li> <li>• 1: In monitored network and trusted</li> <li>• 2: In monitored network and untrusted</li> </ul> |
| cs10Label       | Destination zone                             | Deep Discovery_DstZone  |
| cs11            | CCCA log is detected by                      | <ul style="list-style-type: none"> <li>• GLOBAL_INTELLIGENCE</li> <li>• VIRTUAL_ANALYZER</li> <li>• USER_DEFINED</li> <li>• RELEVANCE_RULE</li> </ul>                           |
| cs11Label       | CCCA log is detected by                      | CCCA_DetectionSource  |
| cs12            | CCCA address                                 | Example: 10.1.144.199   |
| cs12Label       | CCCA address                                 | CCCA_Destination  |
| cs13            | CCCA type                                    | <ul style="list-style-type: none"> <li>• IP_DOMAIN</li> <li>• IP_DOMAIN_PORT</li> <li>• URL</li> <li>• EMAIL</li> </ul>   |
| cs13Label       | CCCA type                                    | CCCA_DestinationFormat  |

| TMEF KEY                  | DESCRIPTION  | VALUE   |
|---------------------------|--|---|
| deviceDirection           | Packet direction   | <ul style="list-style-type: none"> <li>• 0: Source is external</li> <li>• 1: Source is internal</li> <li>• 2: Unknown</li> </ul>                        |
| deviceGUID                | Appliance GUID   | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536   |
| deviceMacAddress          | Appliance MAC address  | Example: 00:0C:29:6E:CB:F9  |
| devicePayloadId           | An extendable field.<br>Format: {threat_type}:{log_id}:{with pcap file captured}{:extensions}*<br>* indicates optional | <p>Examples:</p> <ul style="list-style-type: none"> <li>• With pcap file captured: 2:10245:P</li> <li>• Without pcap file captured: 2:10245:</li> </ul> |
| deviceRiskConfidenceLevel | Confidence level   | <ul style="list-style-type: none"> <li>• 1: High</li> <li>• 2: Medium</li> <li>• 3: Low</li> <li>• 0: Undefined</li> </ul>                              |
| dhost                     | Destination host name  | Example: dhost1   |
| dmac                      | Destination MAC  | Example: 00:0C:29:6E:CB:F9  |
| dOSName                   | Destination host OS  | Example: Android  |
| dpt                       | Destination port   | Value between 0 and 65535   |
| dst                       | Destination IP address   | Example: 10.1.144.199   |
| duser                     | Mail recipient   | Example: duser1   |
| dUser1                    | Destination user name 1  | Example: admin  |
| dUser1LoginTime           | Destination user log on time 1   | Example: Mar 09 2015 17:05:21 GMT +08:00  |
| dUser2                    | Destination user name 2  | Example: admin  |

| <b>TMEF KEY</b> | <b>DESCRIPTION</b>             | <b>VALUE</b>                                     |
|-----------------|--------------------------------|--|
| dUser2LoginTime | Destination user log on time 2 | Example: Mar 09 2015 17:05:21 GMT +08:00         |
| dUser3          | Destination user name 3        | Example: admin                                   |
| dUser3LoginTime | Destination user log on time 3 | Example: Mar 09 2015 17:05:21 GMT +08:00         |
| dvc             | Appliance IP address           | Example: 10.1.144.199                            |
| dvchost         | Appliance host name            | Example: localhost                               |
| evtCat          | Event category                 | Example: Suspicious Traffic                      |
| evtSubCat       | Event sub category             | Example: Email                                   |
| externalId      | Log ID                         | Example: 11                                      |
| fileHash        | SHA1                           | Example:1EDD5B38DE4729545767088C5CAB395E4197C8F3 |
| filePath        | File path                      | Example: SHARE\\                                 |
| fileType        | Real file type                 | Example: 1638400                                 |
| fname           | File name                      | Example: excel.rar                               |
| fsize           | File size                      | Example: 131372                                  |
| hackerGroup     | Hacker group                   | Example: Comment Crew                            |
| hackingCampaign | Hacking campaign               | Example: Aurora                                  |
| hostSeverity    | Host Severity                  | Example: 4                                       |
| interestedIp    | Interested IP                  | Example: 10.1.144.199                            |
| mailMsgSubject  | Mail subject                   | Example: hello                                   |
| malFamily       | Malware family                 | Example: Duqu                                    |
| malName         | Malware name                   | Example: HEUR_NAMETRICK.A                        |
| malType         | Malware type                   | Example: MALWARE                                 |

| TMEF KEY         | DESCRIPTION                  | VALUE  |
|------------------|------------------------------|--|
| messageld        | Message ID                   | Example:<br><20090130042416.7060505@jovencitasvirigenes.com.ar>  |
| mitigationTaskId | Event task ID for mitigation | Example:<br>dc036acb-9a2e-4939-8244-dedbda9ec4ba   |
| oldFileHash      | Mail attachment SHA1         | Example:<br>1EDD5B38DE4729545767088C5CAB395E4197C8F3   |
| oldFileName      | Mail attachment file name    | Example: excel.rar   |
| oldFileSize      | Mail attachment file size    | Example: 150000  |
| oldFileType      | Mail attachment file type    | Example: 1638400   |
| pAttackPhase     | Primary attack phase         | <ul style="list-style-type: none"> <li>• Intelligence Gathering</li> <li>• Point of Entry</li> <li>• Command and Control Communication</li> <li>• Lateral Movement</li> <li>• Asset and Data Discovery</li> <li>• Data Exfiltration</li> <li>• Nil (no applicable attack phase)</li> </ul> |
| pComp            | Detection engine/component   | Example: VSAPI   |
| peerIP           | Peer IP                      | Example: 10.1.144.199  |
| ptype            | Application type             | IDS  |
| reason           | Reason                       | Example: ["Protocol: 4"]   |
| request          | URL                          | Example: http://1.2.3.4/query?term=value   |

| <b>TMEF KEY</b>          | <b>DESCRIPTION</b>       | <b>VALUE</b>   |
|--------------------------|--------------------------|--|
| requestClientApplication | User agent               | Example: IE  |
| rt                       | Log generation time      | Example: Mar 09 2015 17:05:21 GMT +08:00   |
| ruleId                   | Rule ID                  | Example: 52  |
| ruleName                 | Description              | Example: Email message sent through an unregistered SMTP server  |
| sAttackPhase             | Secondary attack phase   | <ul style="list-style-type: none"> <li>• Intelligence Gathering</li> <li>• Point of Entry</li> <li>• Command and Control Communication</li> <li>• Lateral Movement</li> <li>• Asset and Data Discovery</li> <li>• Data Exfiltration</li> <li>• Nil (no applicable attack phase)</li> </ul> |
| shost                    | Source host name         | Example: shost1  |
| smac                     | Source MAC               | Example: 00:0C:29:6E:CB:F9   |
| sOSName                  | Source host OS           | Example: Android   |
| spt                      | Source port              | Value between 0 and 65535  |
| src                      | Source IP address        | Example: 10.1.144.199  |
| suid                     | User name                | Example: User1   |
| suser                    | Mail sender              | Example: suser1  |
| sUser1                   | Source user name 1       | Example: admin   |
| sUser1LoginTime          | Source user log on time1 | Example: Mar 09 2015 17:05:21 GMT +08:00   |
| sUser2                   | Source user name 2       | Example: admin   |

| TMEF KEY        | DESCRIPTION               | VALUE                                    |
|-----------------|---------------------------|--|
| sUser2LoginTime | Source user log on time 2 | Example: Mar 09 2015 17:05:21 GMT +08:00 |
| sUser3          | Source user name 3        | Example: admin                           |
| sUser3LoginTime | Source user log on time 3 | Example: Mar 09 2015 17:05:21 GMT +08:00 |
| vLANId          | VLANID                    | Value between 0 and 4095                 |

### Log sample:

```

CEF:0|Trend Micro|Deep Discovery Inspector|
5.0.1329|100100|
MALWARE_DETECTION|8| ptype=IDS dvc=172.22.9.32
deviceMacAddress=00:50:56:AD:03:BD dvchost=localhost
deviceGUID=E9A3FA433916-4738984C-A4BF-84A0-D603
rt=Jun 22 2017 09:42:47 GMT+08:00 appGroup=HTTP
app=HTTP vLANId=4095 deviceDirection=1 dhost=172.22.9.5
dst=172.22.9.5 dpt=57908 dmac=00:50:56:82:e7:a9
shost=172.22.9.54 src=172.22.9.54 spt=80
smac=00:50:56:82:c6:ae
cs3Label=HostName_Ext cs3=172.22.9.54
malName=Eicar_test_file
malType=Virus fname=eicarcom2.zip fileType=262340608
fsize=308 ruleId=0 ruleName=Eicar_test_file -
HTTP (Response) deviceRiskConfidenceLevel=0 cn3Label=Deep
Discovery_PotentialRisk cn3=0 cs4Label=Deep
Discovery_SrcGroup
cs4=Default cs5Label=Deep Discovery_SrcZone cs5=1
cs9Label=Deep Discovery_DstGroup cs9=Default
cs10Label=Deep
Discovery_DstZone cs10=1 cs6Label=Deep
Discovery_DetectionType
cs6=0 request=http://172.22.9.54/eicarcom2.zip
requestClientApplication=Wget/1.12 (linux-gnu)
pComp=VSAPI act=not blocked cn4Label=Deep
Discovery_ThreatType
cn4=0 peerIp=172.22.9.5
fileHash=BEC1B52D350D721C7E22A6D4BB0A92909893A3AE

```

```

compressedFileName=eicar.com interestedIp=172.22.9.54
cnt=1 dosName=Linux cn5Label=AggregatedCount
cn5=1 evtCat=Malware evtSubCat=Trojan cn2Label=APT
  Related cn2=0 pAttackPhase=Point of Entry externalId=143
cn7Label=HeurFlag cn7=0 compressedFileType=327680
compressedFileHash=3395856CE81F2B7382DEE72602F
798B642F14140 hostSeverity=8 reason=["Malware:
Eicar_test_file"] devicePayloadId=0:143:P

```

## TMEF Disruptive Application Logs

**TABLE 5-2. TMEF Disruptive Application Logs**

| TMEF KEY           | DESCRIPTION         | VALUE  |
|--------------------|---------------------|--|
| Header (logVer)    | TMEF format version | CEF: 0   |
| Header (vendor)    | Appliance vendor    | Trend Micro  |
| Header (pname)     | Appliance product   | Deep Discovery Inspector   |
| Header (pver)      | Appliance version   | Example: 3.8.1181  |
| Header (eventid)   | Signature ID        | 100120   |
| Header (eventName) | Event Name          | DISRUPTIVE_APPLICATION_DETECTION   |
| Header (severity)  | Severity            | <ul style="list-style-type: none"> <li>• 2: Informational</li> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul> |
| app                | Protocol            | Example: HTTP  |
| appGroup           | Protocol group      | Example: HTTP  |
| cnt                | Total count         | Example: 1   |

| TMEF KEY        | DESCRIPTION                                  | VALUE   |
|-----------------|--|---|
| cn4             | Threat type                                  | 6   |
| cn4Label        | Threat type                                  | Deep Discovery_ThreatType   |
| cn5             | Aggregated count                             | Example: 1  |
| cn5Label        | Aggregated count                             | AggregatedCnt   |
| cs4             | Network Group assigned to a source host      | Example: monitor1   |
| cs4Label        | Network Group assigned to a source host      | Deep Discovery_SrcGroup   |
| cs5             | Source zone                                  | <ul style="list-style-type: none"> <li>• 0: Not in monitored network</li> <li>• 1: In monitored network and trusted</li> <li>• 2: In monitored network and not trusted</li> </ul> |
| cs5Label        | Source zone                                  | Deep Discovery_SrcZone  |
| cs9             | Network Group assigned to a destination host | Example: monitor1   |
| cs9Label        | Network Group assigned to a destination host | Deep Discovery_DstGroup   |
| cs10            | Destination zone                             | <ul style="list-style-type: none"> <li>• 0: Not in monitored network</li> <li>• 1: In monitored network and trusted</li> <li>• 2: In monitored network and not trusted</li> </ul> |
| cs10Label       | Destination zone                             | Deep Discovery_DstZone  |
| deviceDirection | Packet direction                             | <ul style="list-style-type: none"> <li>• 0: Source is external</li> <li>• 1: Source is internal</li> <li>• 2: Unknown</li> </ul>  |



| TMEF KEY         | DESCRIPTION   | VALUE  |
|------------------|---|--|
| deviceGUID       | Appliance GUID  | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536  |
| deviceMacAddress | Appliance MAC address   | Example: 00:0C:29:6E:CB:F9   |
| devicePayloadId  | An extendable field.<br>Format: {threat_type};<br>{log_id};{with pcap file<br>captured}{:extensions}*<br> | Examples: <ul style="list-style-type: none"> <li>• With pcap file captured:<br/>2:10245:P</li> <li>• Without pcap file captured:<br/>2:10245:</li> </ul> |
| dhost            | Destination host name   | Example: dhost1  |
| dmac             | Destination MAC   | Example: 00:0C:29:6E:CB:F9   |
| dOSName          | Destination host OS   | Example: Android   |
| 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   |
| externalId       | Log ID  | Example: 11  |
| interestedIp     | Interested IP   | Example: 10.1.144.199  |
| msg              | Description   | Example: Deep Discovery Inspector detected the protocol in your monitored network.   |
| pComp            | Detection engine/<br>component  | Example: VSAPI   |
| peerIP           | Peer IP   | Example: 10.1.144.199  |
| ptype            | Application type  | IDS  |
| rt               | Log generation time   | Example: Mar 09 2015 17:05:21 GMT +08:00   |

| TMEF KEY | DESCRIPTION       | VALUE                      |
|----------|-------------------|----------------------------|
| shost    | Source host name  | Example: shost1            |
| smac     | Source MAC        | Example: 00:0C:29:6E:CB:F9 |
| sOSName  | Source host OS    | Example: Android           |
| spt      | Source port       | Value between 0 and 65535  |
| src      | Source IP address | Example: 10.1.144.199      |
| vLANId   | VLANID            | Value between 0 and 4095   |

### Log sample:

```

CEF:0|Trend Micro|Deep Discovery Inspector|5.0.1329|
100120|
DISRUPTIVE_APPLICATION_DETECTION|2|dvc=172.22.9.32
deviceMacAddress=00:50:56:AD:03:BD dvchost=localhost
deviceGUID=E9A3FA433916-4738984C-A4BF-84A0-D603
ptype=IDS rt=Jun 22 2017 10:06:24 GMT+08:00 appGroup=P2P
app=eDonkey vLANId=4095 deviceDirection=1
dhost=10.1.100.223
dst=10.1.100.223 dpt=4662 dmac=00:0c:29:a7:72:74
shost=10.1.117.231 src=10.1.117.231 spt=39933
smac=00:30:da:2d:47:32 cn5Label=AggregatedCount
cn5=1 msg=Deep Discovery Inspector detected the
protocol in your monitored network. cn4Label=Deep
Discovery_ThreatType cn4=6 cs4Label=Deep
Discovery_SrcGroup
cs4=Default cs5Label=Deep Discovery_SrcZone cs5=1
cs9Label=Deep Discovery_DstGroup cs9=Default
cs10Label=Deep
Discovery_DstZone cs10=1 interestedIp=10.1.117.231
peerIp=10.1.100.223 pComp=CAV cnt=1 externalId=11
devicePayloadId=6:11:

```

## TMEF Web Reputation Logs

**TABLE 5-3. TMEF Web Reputation Logs**

| TMEF KEY           | DESCRIPTION         | VALUE  |
|--------------------|---------------------|--|
| Header (logVer)    | TMEF format version | CEF: 0   |
| Header (vendor)    | Appliance vendor    | Trend Micro  |
| Header (pname)     | Appliance product   | Deep Discovery Inspector   |
| Header (pver)      | Appliance version   | Example: 3.8.1181  |
| Header (eventid)   | Signature ID        | 100101   |
| Header (eventName) | Event Name          | WEB_THREAT_DETECTION   |
| Header (severity)  | Severity            | <ul style="list-style-type: none"> <li>• 2: Informational</li> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul> |
| app                | Protocol            | Example: HTTP  |
| appGroup           | Protocol group      | Example: HTTP  |
| cn1                | CCCA detection      | 0 or 1   |
| cn1Label           | CCCA detection      | CCCA_Detection   |
| cn2                | Score               | Example: 49  |
| cn2Label           | Score               | Score  |
| cn4                | Threat type         | 5  |
| cn4Label           | Threat type         | Deep Discovery_ThreatType  |

| TMEF KEY  | DESCRIPTION                                  | VALUE   |
|-----------|--|---|
| cn6       | CCCA Risk Level                              | <ul style="list-style-type: none"> <li>• 0: Unknown</li> <li>• 1: Low</li> <li>• 2: Medium</li> <li>• 3: High</li> </ul>  |
| cn6Label  | CCCA Risk Level                              | CCCA_RiskLevel  |
| cs3       | Host name                                    | Example: CLIENT1  |
| cs3Label  | Host name                                    | HostName_Ext  |
| cs4       | Network Group assigned to a source host      | Example: monitor1   |
| cs4Label  | Network Group assigned to a source host      | Deep Discovery_SrcGroup   |
| cs5       | Source zone                                  | <ul style="list-style-type: none"> <li>• 0: Not in monitored network</li> <li>• 1: In monitored network and trusted</li> <li>• 2: In monitored network and not trusted</li> </ul> |
| cs5Label  | Source zone                                  | Deep Discovery_SrcZone  |
| cs9       | Network Group assigned to a destination host | Example: monitor1   |
| cs9Label  | Network Group assigned to a destination host | Deep Discovery_DstGroup   |
| cs10      | Destination zone                             | <ul style="list-style-type: none"> <li>• 0: Not in monitored network</li> <li>• 1: In monitored network and trusted</li> <li>• 2: In monitored network and not trusted</li> </ul> |
| cs10Label | Destination zone                             | Deep Discovery_DstZone  |

| TMEF KEY         | DESCRIPTION  | VALUE   |
|------------------|--|---|
| cs11             | CCCA log is detected by  | <ul style="list-style-type: none"> <li>GLOBAL_INTELLIGENCE</li> <li>VIRTUAL_ANALYZER</li> <li>USER_DEFINED</li> <li>RELEVANCE_RULE</li> </ul> |
| cs11Label        | CCCA log is detected by  | CCCA_DetectionSource  |
| deviceGUID       | Appliance GUID   | Example: 6B593E17AFB7-40FB8B28-A4CE-0462-A536   |
| deviceMacAddress | Appliance MAC address  | Example: 00:0C:29:6E:CB:F9  |
| devicePayloadId  | An extendable field.<br>Format: {threat_type}:<br>{log_id};{with pcap file<br>captured}{:extensions}*<br>Examples: | <ul style="list-style-type: none"> <li>With pcap file captured:<br/>2:10245:P</li> <li>Without pcap file captured:<br/>2:10245:</li> </ul>    |
| dvc              | Appliance IP address   | Example: 10.1.144.199   |
| dvchost          | Appliance host name  | Example: localhost  |
| deviceDirection  | Packet direction   | <ul style="list-style-type: none"> <li>0: Source is external</li> <li>1: Source is internal</li> <li>2: Unknown</li> </ul>                    |
| dhost            | Destination host name  | Example: 'dhost1  |
| dmac             | Destination MAC  | Example: 00:0C:29:6E:CB:F9  |
| dOSName          | Destination host OS  | Example: Android  |
| dpt              | Destination port   | Value between 0 and 65535   |
| dst              | Destination IP address   | Example: 10.1.144.199   |
| duser            | Mail recipient   | Example: duser1   |
| externalId       | Log ID   | Example: 11   |

| <b>TMEF KEY</b>          | <b>DESCRIPTION</b>             | <b>VALUE</b>   |
|--------------------------|--------------------------------|--|
| hostSeverity             | Host Severity                  | Example: 4   |
| interestedIp             | Interested IP                  | Example: 10.1.144.199  |
| mailMsgSubject           | Mail subject                   | Example: hello   |
| msg                      | Description                    | Example: C&C Server URL in Web Reputation Services database - HTTP (Request)   |
| pAttackPhase             | Primary attack phase           | <ul style="list-style-type: none"> <li>• Intelligence Gathering</li> <li>• Point of Entry</li> <li>• Command and Control Communication</li> <li>• Lateral Movement</li> <li>• Asset and Data Discovery</li> <li>• Data Exfiltration</li> <li>• Nil (no applicable attack phase)</li> </ul> |
| pComp                    | Detection engine/<br>component | Example: VSAPI   |
| peerIp                   | Peer IP                        | Example: 10.1.144.199  |
| ptype                    | Application type               | IDS  |
| reason                   | Reason                         | Example: ["Protocol: 4"]   |
| request                  | URL                            | Example: http://1.2.3.4/query?term=value   |
| requestClientApplication | User agent                     | Example: IE  |
| rt                       | Log generation time            | Example: Mar 09 2015 17:05:21 GMT +08:00   |
| sAttackPhase             | Secondary attack phase         | Example: Point of Entry  |
| shost                    | Source host name               | Example: shost1  |

| TMEF KEY | DESCRIPTION       | VALUE                      |
|----------|-------------------|----------------------------|
| smac     | Source MAC        | Example: 00:0C:29:6E:CB:F9 |
| sOSName  | Source host OS    | Example: Android           |
| spt      | Source port       | Value between 0 and 65535  |
| src      | Source IP address | Example: 10.1.144.199      |
| suser    | Mail sender       | Example: suser1            |
| urlCat   | URL category      | Example: C&C Server        |
| vLANId   | VLANID            | Value between 0 and 4095   |

### Log sample:

```

CEF:0|Trend Micro|Deep Discovery Inspector|5.0.1329|
100101|WEB_THREAT_DETECTION|8|dvc=172.22.9.32
deviceMacAddress=00:50:56:AD:03:BD dvchost=localhost
deviceGUID=E9A3FA433916-4738984C-A4BF-84A0-D603
ptype=IDS rt=Jun 22 2017 10:00:17 GMT+08:00
cs3Label=HostName_Ext
cs3=ca95-1.winshipway.com cs4Label=Deep
Discovery_SrcGroup
cs4=Default cs5Label=Deep Discovery_SrcZone cs5=1
cs10Label=Deep Discovery_DstZone cs10=0 cn2Label=Score
cn2=49 cn4Label=Deep Discovery_ThreatType cn4=5
dmac=00:16:c8:65:98:d5 shost=172.22.9.5 src=172.22.9.5
spt=41757 smac=00:50:56:82:e7:a9 interestedIp=172.22.9.5
cn1Label=CCCA_Detection cn1=1 msg=Ransomware URL
in Web Reputation Services database - HTTP (Request)
request=http://ca95-1.winshipway.com/
requestClientApplication=Wget/1.12
(linux-gnu) pComp=TMUFE appGroup=HTTP app=HTTP
vLANId=4095 deviceDirection=1 dhost=150.70.162.115
dst=150.70.162.115 dpt=80 urlCat=Ransomware
peerIp=150.70.162.115
sOSName=Linux cn6Label=CCCA_RiskLevel cn6=3
cs11Label=CCCA_DetectionSource
cs11=RELEVANCE_RULE externalId=17 hostSeverity=8
reason=["URL: http://ca95-1.winshipway.com/"]

```

```
pAttackPhase=Command and Control Communication
devicePayloadId=5:17:P
```

## TMEF System Logs

**TABLE 5-4. TMEF System Logs**

| TMEF KEY           | DESCRIPTION           | VALUE  |
|--------------------|-----------------------|--|
| Header (logVer)    | TMEF format version   | CEF: 0   |
| Header (vendor)    | Appliance vendor      | Trend Micro  |
| Header (pname)     | Appliance product     | Deep Discovery Inspector   |
| Header (pver)      | Appliance version     | Example: 3.8.1181  |
| Header (eventid)   | Signature ID          | <ul style="list-style-type: none"> <li>• 300102</li> <li>• 300999</li> </ul>   |
| Header (eventName) | Event Name            | <ul style="list-style-type: none"> <li>• PRODUCT_UPDATE</li> <li>• SYSTEM_EVENT</li> <li>• PRODUCT_UPDATE</li> </ul>       |
| Header (severity)  | Severity              | <ul style="list-style-type: none"> <li>• 2: Informational</li> <li>• 4: Warning</li> <li>• 6: Severe</li> </ul> Example: 2 |
| deviceGUID         | Appliance GUID        | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536  |
| deviceMacAddress   | Appliance MAC address | Example: 00:0C:29:6E:CB:F9   |
| duser              | Action by             | Example: admin   |
| dvc                | Appliance IP address  | Example: 10.1.144.199  |
| dvchost            | Appliance host name   | Example: localhost   |



| TMEF KEY | DESCRIPTION         | VALUE   |
|----------|---------------------|---|
| engType  | Engine name         | Example: Advanced Threat Scan Engine for Deep Discovery (Linux, 64-bit)                         |
| engVer   | Engine version      | Example: 10.300.1040  |
| msg      | Description         | Example: The web console timeout setting has been changed.                                      |
| outcome  | Outcome             | <ul style="list-style-type: none"> <li>• Success</li> <li>• Failure</li> </ul> Example: Success |
| patType  | Pattern name        | Example: Deep Discovery Malware Pattern   |
| patVer   | Pattern version     | Example: 14.271.92  |
| ptype    | Application type    | IDS   |
| rt       | Log generation time | Example: Mar 09 2015 17:05:21 GMT +08:00  |
| src      | User IP address     | Example: 10.1.1.1   |

### Log sample:

```

CEF:0|Trend Micro|Deep Discovery Inspector
|3.85.1156|300999|SYSTEM_EVENT|2|ptype=IDS
dvc=172.22.9.12 deviceMacAddress=00:50:56:
AD:CC:EE dvchost=localhostdeviceGUID=
DBD38FFC70B4-41C792BE-D671-0040-8B1D
rt=Mar 10 2017 17:03:31 GMT+08:00
msg=The threat detection setting
has been changed. duser=admin
outcome=Success src=172.17.0.250

```

## TMEF Correlated Incident Logs

**TABLE 5-5. Correlation Incident Logs**

| TMEF KEY           | DESCRIPTION                        | VALUE  |
|--------------------|------------------------------------|--|
| Header (logVer)    | TMEF format version                | CEF: 0   |
| Header (vendor)    | Appliance vendor                   | Trend Micro  |
| Header (pname)     | Appliance product                  | Deep Discovery Inspector   |
| Header (pver)      | Appliance version                  | Example: 3.8.1181  |
| Header (eventid)   | Signature ID                       | 100127   |
| Header (eventName) | Event Name                         | SUSPICIOUS_BEHAVIOUR_DETECTION   |
| Header (severity)  | Severity                           | <ul style="list-style-type: none"> <li>• 2: Informational</li> <li>• 4: Low</li> <li>• 6: Medium</li> <li>• 8: High</li> </ul> |
| app                | Protocol                           | Example: HTTP  |
| cs1                | Interested group                   | Example: Default   |
| cs1Label           | Interested group                   | DD_InterestedGroup   |
| cs2                | Malware server address             | Example: 10.1.144.199  |
| cs2Label           | Malware server address             | Malware_Server_IP_Address  |
| cs3                | Number of downloaded malware files | Example: 1   |
| cs3Label           | Number of downloaded malware files | Number_of_Malware_Files_Downloaded   |
| cs10               | Malware name                       | Example: HEUR_NAMETRICK.A  |
| cs10Label          | Malware name                       | Malware_Name   |

| TMEF KEY             | DESCRIPTION                    | VALUE  |
|----------------------|--------------------------------|--|
| deviceDirection      | Packet direction               | <ul style="list-style-type: none"> <li>• 0: Source is external</li> <li>• 1: Source is internal</li> <li>• 2: Unknown</li> </ul> |
| deviceGUID           | Appliance GUID                 | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536  |
| deviceMacAddress     | Appliance MAC address          | Example: 00:0C:29:6E:CB:F9   |
| dvc                  | Appliance IP address           | Example: 10.1.144.199  |
| dvchost              | Appliance host name            | Example: localhost   |
| interestedHost       | Interested host                | Example: trend.net   |
| interestedIp         | Interested IP                  | Example: 10.1.144.199  |
| interestedMacAddress | Interested MAC                 | Example: 00:0C:29:6E:CB:F9   |
| interestedUser       | Interested user 1              | Example: user1   |
| interestedUser2      | Interested user 2              | Example: user2   |
| interestedUser3      | Interested user 3              | Example: user3   |
| pComp                | Detection engine/<br>component | Correlation  |
| peerHost             | Peer host                      | Example: 10.1.144.199  |
| peerIp               | Peer IP                        | Example: 10.1.144.199  |
| ptype                | Application type               | IDS  |
| rt                   | Log generation time            | Example: Mar 09 2015 17:05:21 GMT +08:00   |
| ruleId               | Rule ID                        | Example: 52  |
| ruleName             | Description                    | Example: Email message sent through an unregistered SMTP server  |

| TMEF KEY   | DESCRIPTION | VALUE                            |
|------------|-------------|----------------------------------|
| threatName | Threat name | Example: Malware File Downloaded |
| threatType | Threat type | Example: Malware-related         |

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Inspector|3.8.1181|100127|S
USPICIOUS_BEHAVIOUR_DETECTION|2|dvc=10.201.156.143 deviceMac
Address=00:0C:29:A6:53:0C dvchost=ddi38-143 pComp=Correlatio
n ptype=IDS deviceGUID=D2C1D6D20FF8-4FC98F92-25EB-D7DA-AF0E
rt=Mar 11 2015 22:05:50 GMT-04:00 deviceDirection=1 interest
edIp=172.16.0.100 interestedHost=172.16.0.100 interestedMacA
ddress=00:0c:29:70:45:36 ruleId=47 ruleName=This host has re
sponded to DNS queries. threatType=Unregistered Service thre
atName=Unregistered DNS Server app=DNS Response cs1Label=DD_
InterestedGroup cs1=Default peerHost=172.16.1.141 peerIp=172
.16.1.141
```

## TMEF Virtual Analyzer Logs: File Analysis Events

**TABLE 5-6. TMEF 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 Inspector |
| Header (pver)      | Appliance version   | Example: 3.8.1181        |
| Header (eventid)   | Signature ID        | 200119                   |
| Header (eventName) | Event Name          | FILE_ANALYZED            |
| Header (severity)  | Severity            | 3 (fixed value)          |

| TMEF KEY          | DESCRIPTION           | VALUE   |
|-------------------|-----------------------|---|
| cn1               | GRID is known good    | <ul style="list-style-type: none"> <li>• 0: Bad file</li> <li>• -1: Unknown file</li> <li>• 1: Good file</li> </ul>                     |
| cn1Label          | GRID is known good    | GRIDIsKnownGood   |
| cn2               | ROZ rating            | <ul style="list-style-type: none"> <li>• 0: No risk</li> <li>• 1: Low risk</li> <li>• 2: Medium risk</li> <li>• 3: High risk</li> </ul> |
| cn2Label          | ROZ rating            | ROZRating   |
| cn3               | PCAP ready            | 0 or 1  |
| 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:<br>1EDD5B38DE4729545767088C5CAB<br>395E4197C8F3  |
| dvc               | Appliance IP address  | Example: 10.1.144.199   |
| dvchost           | Appliance host name   | Example: localhost  |
| fileHash          | File SHA1             | Example:<br>1EDD5B38DE4729545767088C5CAB<br>395E4197C8F3  |
| fileType          | True file type        | Example: 1638400  |
| fname             | File name             | Example: excel.rar  |
| fsize             | File size             | Example: 131372   |

| TMEF KEY | DESCRIPTION      | VALUE   |
|----------|------------------|---|
| malName  | Malware name     | Example: SWF_Lfm.926  |
| pComp    | Detection source | <ul style="list-style-type: none"> <li>Sandbox</li> <li>UDSO (User-Defined Suspicious Objects)</li> </ul> |
| rt       | Analysis time    | Example: Mar 09 2015 17:05:21 GMT +08:00  |

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Inspector|3.8.1181|200119|FILE_ANALYZED|3|rt=Mar 11 2015 07:38:04 GMT-04:00 pComp=Sandbox dvc=10.201.156.143 dvchost=ddi38-143 deviceMacAddress=00:0C:29:A6:53:0C deviceGUID=D2C1D6D20FF8-4FC98F92-25EB-D7DA-AF0E fname=multiple_mask.swf fileHash=643DBF968EF3BECD9A73CF1DCF44006BC46E15F7 malName=SWF_Lfm.926 fileType=Macromedia Flash fsize=9400 deviceOSName=MAK_win7splen_offices_noab_TL cn2Label=ROZRating cn2=3 cn1Label=GRIDIsKnownGood cn1=-1 cn3Label=PcapReady cn3=1
```

## TMEF Virtual Analyzer Logs: Notable Characteristics Events

**TABLE 5-7. TMEF 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 Inspector |
| Header (pver)    | Appliance version   | Example: 3.8.1181        |
| Header (eventid) | Signature ID        | 200127                   |

| TMEF KEY           | DESCRIPTION             | VALUE  |
|--------------------|-------------------------|--|
| Header (eventName) | Event Name              | NOTABLE_CHARACTERISTICS                                  |
| Header (severity)  | Severity                | 6 (fixed 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           | File SHA1               | Example:<br>1EDD5B38DE4729545767088C5CAB<br>395E4197C8F3 |
| fileType           | True file type          | Example: 1638400   |
| fname              | File name               | Example: excel.rar                                       |
| fsize              | File size               | Example: 131372  |
| msg                | Details                 | Example:<br>www.chapisteriadaniel.com                    |
| pComp              | Detection source        | Sandbox  |
| rt                 | Analysis time           | Example: Mar 09 2015 17:05:21 GMT<br>+08:00              |
| ruleCategory       | Violated policy name    | Example: Internet Explorer Setting<br>Modification       |
| ruleName           | Analysis violated event | Example: Modified important<br>registry items            |

### Log sample:

```
CEF:0|Trend Micro|Deep Discovery Inspector|3.8.1181|200127|N
OTABLE_CHARACTERISTICS|6|rt=Mar 11 2015 05:00:26 GMT-04:00 p
Comp=Sandbox dvc=10.201.156.143 dvchost=ddi38-143 deviceMacA
```

```
address=00:0C:29:A6:53:0C deviceGUID=D2C1D6D20FF8-4FC98F92-25
EB-D7DA-AF0E fname=DTAS_WIN32_07 fileHash=672B1A8ADB412C272C
CA21A214732C447B650349 fileType=WIN32 EXE fsize=290304 ruleC
ategory=Suspicious network or messaging activity ruleName=Qu
eries DNS server msg=012webpages.com deviceOSName=MAK_win7sp
len_offices_noab_TL
```

## TMEF Virtual Analyzer Logs: Deny List Transaction Events

**TABLE 5-8. TMEF 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 Inspector  |
| Header (pver)      | Appliance version       | Example: 3.8.1181   |
| Header (eventid)   | Signature ID            | 200120  |
| Header (eventName) | Event Name              | DENYLIST_CHANGE   |
| Header (severity)  | Severity                | 3 (fixed value)   |
| act                | The action in the event | Add or Remove   |
| cs1                | Deny List type          | <ul style="list-style-type: none"> <li>• Deny List IP/Port</li> <li>• Deny List URL</li> <li>• Deny List File SHA1</li> <li>• Deny List Domain</li> </ul> |
| cs1Label           | Deny List type          | type  |



| TMEF KEY               | DESCRIPTION           | VALUE  |
|------------------------|-----------------------|--|
| deviceExternalRiskType | Risk level            | <ul style="list-style-type: none"> <li>Low</li> <li>Medium</li> <li>High</li> <li>Confirmed malware</li> </ul> |
| deviceGUID             | Appliance GUID        | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536  |
| deviceMacAddress       | Appliance MAC address | Example: 00:0C:29:6E:CB:F9   |
| dhost                  | Destination host name | Example: insta-find.com  |
| dpt                    | Remote port           | Value between 0 and 65535  |
| dst                    | Remote IP             | Example: 10.1.144.199  |
| 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               | File SHA1             | Example:<br>1EDD5B38DE4729545767088C5CAB<br>395E4197C8F3   |
| pComp                  | Detection source      | Sandbox  |
| request                | URL                   | Example: _http://1.2.3.4/query?<br>term=value  |
| rt                     | Analysis time         | Example: Mar 09 2015 17:05:21 GMT +08:00   |

### Log sample:

```
CEF:0|Trend Micro|Deep Discovery Inspector|3.8.1181|200120|D
ENYLIST_CHANGE|3|rt=Mar 11 2015 07:15:45 GMT-04:00 pComp=San
dbox dvc=10.201.156.143 dvchost=ddi38-143 deviceMacAddress=0
0:0C:29:A6:53:0C deviceGUID=D2C1D6D20FF8-4FC98F92-25EB-D7DA-
AF0E cs1Label=type cs1=Deny List URL end=Apr 10 2015 07:15:3
```

```
5 GMT-04:00 act=Add request=http://zalepivmordu.ru:80/ deviceExternalRiskType=Medium
```

## TMEF Retro Scan Report Logs

**TABLE 5-9. TMEF Retro Scan Report Logs**

| TMEF KEY               | DESCRIPTION                   | VALUE   |
|------------------------|-------------------------------|---|
| Header (logVer)        | TMEF format version           | CEF: 0  |
| Header (vendor)        | Appliance vendor              | Trend Micro                                   |
| Header (pname)         | Appliance product             | Deep Discovery Inspector                      |
| Header (pver)          | Appliance version             | Example: 3.8.1181                             |
| Header (eventid)       | Signature ID                  | 100133  |
| Header (eventName)     | Event Name                    | RETROSCAN_REPORT                              |
| Header (severity)      | Severity                      | 8   |
| callback_attempt_num   | Number of callback attempts   | Example: 20                                   |
| cnc_host_num           | Number of C&C hosts           | Example: 1                                    |
| compromised_client_num | Number of compromised clients | Example: 1                                    |
| deviceGUID             | Appliance GUID                | Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536 |
| firstCallbackTime      | First callback time           | Example: Mar 09 2015 17:05:21 GMT +08:00      |
| lastCallbackTime       | Last callback time            | Example: Mar 09 2015 17:05:21 GMT +08:00      |
| report_id              | Report ID                     | Example: 74c15fe0-90c9-446b-abc4-379d6d7213e7 |

| TMEF KEY   | DESCRIPTION | VALUE  |
|------------|-------------|--|
| report_ts  | Report time | Example: Mar 09 2015 17:05:21 GMT +08:00   |
| report_url | Report URL  | Example: <a href="https://retroscan.trendmicro.com/retroscan/scanDetails.html?reportID=1e84c77b-0452-4f00-b5b8-e41c0ea9ef1a&amp;reportType\=standard">https://retroscan.trendmicro.com/retroscan/scanDetails.html?reportID=1e84c77b-0452-4f00-b5b8-e41c0ea9ef1a&amp;reportType\=standard</a> |

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Inspector|3.8.1200|100133|R
ETROSCAN_REPORT|8|guid=906A61690458-4099A441-898C-BDD2-C7C1
report_ts=Mar 29 2015 03:14:27 GMT+02:00 report_id=ffa9474d-
6d72-44f7-a99c-c0d230fec1f3 report_url=https://retroscan.tre
ndmicro.com/retroscan/scanDetails.html?reportID=1e84c77b-04
52-4f00-b5b8-e41c0ea9ef1a&reportType\=standard compromised_c
lient_num=1 cnc_host_num=1 callback_attempt_num=20 firstCall
backTime=Mar 29 2015 03:04:27 GMT+02:00 lastCallbackTime=Mar
29 2015 03:09:27 GMT+02:00
```

## TMEF Retro Scan Detection Logs

**TABLE 5-10. TMEF Retro Scan Detection Logs**

| TMEF KEY           | DESCRIPTION         | VALUE                    |
|--------------------|---------------------|--------------------------|
| Header (logVer)    | TMEF format version | CEF: 0                   |
| Header (vendor)    | Appliance vendor    | Trend Micro              |
| Header (pname)     | Appliance product   | Deep Discovery Inspector |
| Header (pver)      | Appliance version   | Example: 3.8.1181        |
| Header (eventid)   | Signature ID        | 100134                   |
| Header (eventName) | Event Name          | RETROSCAN_DETECTION      |

| TMEF KEY               | DESCRIPTION                | VALUE   |
|------------------------|----------------------------|---|
| Header (severity)      | Severity                   | 8   |
| callback_address       | Callback address           | Example: http://1.2.3.4/                      |
| callback_time          | Callback time              | Example: Mar 09 2015 17:05:21 GMT +08:00      |
| category               | Category                   | Example: Reference                            |
| cnc_host               | C&C host address           | Example: 10.1.144.199                         |
| compromised_client     | Compromised client address | Example: 10.1.144.199                         |
| deviceGUID             | Appliance GUID             | Example: 6B593E17AFB7-40FB8B28-A4CE-0462-A536 |
| protocol               | Protocol                   | Example: HTTP                                 |
| rating                 | Rating                     | Example: Suspicious                           |
| related_attacker_group | Related attacker group     | Example: Elise Taidoor                        |
| related_malware        | Related malware            | Example: fosniw ge palevo                     |
| report_id              | Report ID                  | Example: 74c15fe0-90c9-446b-abc4-379d6d7213e7 |
| scan_category          | Scan category              | Example: C&C Server                           |
| scan_rating            | Scan rating                | Example: Dangerous                            |
| scan_ts                | Scan time                  | Example: Mar 09 2015 17:05:21 GMT +08:00      |

### Log sample:

```
CEF:0|Trend Micro|Deep Discovery Inspector|3.8.1200|100134|R
ETROSCAN_DETECTION|8|guid=906A61690458-4099A441-898C-BDD2-C7
C1_report_id=0938508b-ec47-47a1-80ea-cd8e3b747822_scan_ts=Ma
r 29 2015 03:14:31 GMT+02:00_callback_time=Mar 29 2015 03:04
:31 GMT+02:00_callback_address=http://app2.winsoft98.com/app
.asp?prj\=4&pid\=haha1&logdata\=MacTryCnt:0&code\=&ver\=1.0.
0.45&appcheck\=1_compromised_client=59.125.99.235_cnc_host=
```

```
app2.winsoft98.com protocol=HTTP rating=Suspicious category  
=Reference scan_rating=Dangerous scan_category=C&C Server r  
elated_malware=fosniw|ge|mactrycnt|palevo related_attacker_  
group=Elise|Taidoor
```







**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](http://www.trendmicro.com)

Item Code: APEM58907/191227