TREND MICRO™

5.3 Patch 1

TREND MICRO™ Deep Discovery™ Director

(Consolidated Mode and Internal Network Analytics Version)

Syslog Content Mapping Guide

Breakthrough Protection Against APTs and Targeted Attacks

Document Part No.: APEM59606/220919

Release Date: September 2022

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

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

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

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

Evaluate this documentation on the following site:

https://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 Director 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

Index

Preface

Preface

Welcome to the Trend Micro Deep Discovery Director *Syslog Content Mapping Guide*. Learn more about the following topics:

Documentation

The documentation set for Deep Discovery Director 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 Director , and explanations on Deep Discovery Director concepts and features.
Syslog Content Mapping Guide	The Syslog Content Mapping Guide provides information about log management standards and syntaxes for implementing syslog events in Deep Discovery Director .
Automation API Guide	A PDF document that explains how to use Deep Discovery Director Automation APIs.
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	Web-based documentation that is accessible from the Deep Discovery Director management console. The Online Help contains explanations of Deep Discovery Director components and features, as well as procedures needed to configure Deep Discovery Director .
Support Portal	The Support Portal is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Support Portal, go to the following website: https://success.trendmicro.com

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

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

Audience

The Deep Discovery Director 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

Document Conventions

The documentation uses the following conventions:

TABLE 2. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface
Note	Configuration notes

Convention	Description
 **Tip**	Recommendations or suggestions
 **Important**	Information regarding required or default configuration settings and product limitations
 **WARNING!**	Critical actions and configuration options

About Trend Micro

Trend Micro, a global leader in cybersecurity, is passionate about making the world safe for exchanging digital information today and in the future. Artfully applying our XGen™ security strategy, our innovative solutions for consumers, businesses, and governments deliver connected security for data centers, cloud workloads, networks, and endpoints.

Optimized for leading environments, including Amazon Web Services, Microsoft®, and VMware®, our layered solutions enable organizations to automate the protection of valuable information from today's threats. Our connected threat defense enables seamless sharing of threat intelligence and provides centralized visibility and investigation to make organizations their most resilient.

Trend Micro customers include 9 of the top 10 Fortune® Global 500 companies across automotive, banking, healthcare, telecommunications, and petroleum industries.

With over 6,500 employees in 50 countries and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to secure their connected world. https://www.trendmicro.com

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 Director .

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

Log Management System	Description
Common Event Format (CEF) For details, see *Syslog Content Mapping - CEF on page 2-1*	CEF is an open log management standard created by HP ArcSight. Deep Discovery Director uses a subset of the CEF dictionary.
Log Event Extended Format (LEEF) For details, see *Syslog Content Mapping - LEEF on page 3-1*	LEEF is an event format developed for IBM Security QRadar. Deep Discovery Director uses a subset of the LEEF dictionary.

Chapter 2

Syslog Content Mapping - CEF

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

- Deep Discovery Director Suspicious Objects lists:
  - *CEF Virtual Analyzer Logs: Deny List Transaction Events on page 2-3*
- Deep Discovery Inspector detection logs:
  - *CEF Threat Logs on page 2-5*
  - *CEF Disruptive Application Logs on page 2-10*
  - *CEF Web Reputation Logs on page 2-12*
- Deep Discovery Email Inspector logs:
  - *CEF Detection Logs: Email Detection Logs on page 2-16*
  - *CEF Detection Logs: Attachment Detection Logs on page 2-20*
  - *CEF Detection Logs: URL Detection Logs on page 2-21*
  - *CEF Message Tracking Logs on page 2-23*
- Virtual Analyzer analysis logs:
  - *CEF Virtual Analyzer Analysis Logs: File Analysis Events on page 2-26*

CEF Virtual Analyzer Logs: Deny List Transaction Events

TABLE 2-1. 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 Director
Header (pver)	Appliance version	Example: 5.3.0.1212
Header (eventid)	Signature ID	200120
Header (eventName)	Description	Deny List updated
Header (severity)	Severity	3 (fixed value)
act	The action in the event	• Add • Remove
cs1	Type	• Deny List IP/Port • Deny List URL • Deny List File SHA1 • Deny List Domain
cs1Label	Type	type
cs2	Risk level	• Low • Medium • High
cs2Label	Risk level	RiskLevel
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536

CEF Key	Description	Value
dhost	Destination host name	Example: dhost1
dpt	Destination port	Value between 1 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 Format: Unix time stamp (number of milliseconds since Jan 01 1970 UTC)	Example: 1593761104300
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
request	URL	Example: http://1.2.3.4/query?term=value
rt	Analysis time Format: Unix time stamp (number of milliseconds since Jan 01 1970 UTC)	Example: 1593761104000

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Dir
ector|5.3.0.1212|200120|Deny List updated|3|rt=1593761104000 d
vc=192.168.156.239 dvchost=ddd3-239 dvcmac=00:0c:30:05:a0:8b d
eviceExternalId=FA68DBC5-D354-444C-A834-60352F1A4027 cs1Label=
type cs1=Deny List Domain end=1593761104300 act=Add dhost=mt6x
.ejvu50k.6x.org cs2Label=RiskLevel cs2=Medium
```

CEF Threat Logs

TABLE 2-2. 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 Director
Header (pver)	Appliance version	Example: 5.3.0.1212
Header (eventid)	Signature ID	Example: 8
Header (eventName)	Description	Example: Packed executable file copied to a network administrative share
Header (severity)	Severity	• 2: Informational • 4: Low • 6: Medium • 8: High
act	The action in the event	• blocked • 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

CEF Key	Description	Value
c6a4Label	Peer IPv6 address	PeerIPv6
cat	Event category	Example: File
cnt	Total count	Example: 1
cn1	CCCA detection	0 or 1
cn1Label	CCCA detection	CCCA_Detection
cn3	Threat type	Value between 0 and 4 • 0: Malicious content • 1: Malicious behavior • 2: Suspicious behavior • 3: Exploit • 4: Grayware
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	Examples: • GLOBAL_INTELLIGENCE • VIRTUAL_ANALYZER • USER_DEFINED

CEF Key	Description	Value
cs5Label	CCCA log is detected by	CCCA_DetectionSource
cs6	Attack Phase	Examples: • Intelligence Gathering • Point of Entry • Command and Control Communication • Lateral Movement • Asset and Data Discovery • Data Exfiltration • Nil (no applicable attack phase)
cs6Label	Attack Phase	pAttackPhase
destinationTranslatedAddress	Peer IP	Example: 10.1.144.199
deviceDirection	Packet direction	0, 1, or 2 • 0: Source is external • 1: Source is internal • 2: Unknown
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devicePayloadId	An extendable field. Format: {threat_type}:{log_id}:{with pcap file captured}{:extensions}*	Examples: • With pcap file captured: 2:10245:P • Without pcap file captured: 2:10245:
dhost	Destination host name	Example: dhost1
dmac	Destination MAC	Example: 00:0C:29:6E:CB:F9

CEF Key	Description	Value
dpt	Destination port	Value between 1 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
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
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: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
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?term=value

CEF Key	Description	Value
rt	Log generation time Format: Unix time stamp (number of milliseconds since Jan 01 1970 UTC)	Example: 1593761104000
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
spt	Source port	Value between 1 and 65535
suid	User name	Example: User1
suser	Mail sender	Example: suser1

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Dir
ector|5.3.0.1212|0|Eicar_test_file - HTTP (Response)|8|dvc=172
.22.9.32 dvcmac=00:50:56:AD:03:BD dvchost=localhost deviceExte
rnalId=E9A3FA433916-4738984C-A4BF-84A0-D603 rt=1593761104000 a
pp=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=eicarco
m2.zip fileType=262340608 fsize=308 requestClientApplication=W
get/1.12 (linux-gnu) act=not blocked cn3Label=Threat Type cn3=
0 destinationTranslatedAddress=172.22.9.5 fileHash=BEC1B52D350
D721C7E22A6D4BB0A92909893A3AE cs4Label=FileNameInArchive cs4=e
icar.com sourceTranslatedAddress=172.22.9.54 cnt=1 cat=Malware
cs6Label=pAttackPhase cs6=Point of Entry flexNumber1Label=vLAN
Id flexNumber1=4095 request=http://172.22.9.54/eicarcom2.zip d
evicePayloadId=0:143:P
```

CEF Disruptive Application Logs

TABLE 2-3. 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 Director
Header (pver)	Appliance version	Example: 5.3.0.1212
Header (eventid)	Signature ID	100120
Header (eventName)	Description	Deep Discovery Inspector detected this protocol in your monitored network.
Header (severity)	Severity	• 2: Informational • 4: Low • 6: Medium • 8: High
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	PeerIPv6

CEF Key	Description	Value
cn3	Threat type	6
cn3Label	Threat type	Threat Type
destinationTranslatedAddress	Peer IP	Example: 10.1.144.199
deviceDirection	Packet direction	0, 1, or 2 • 0: Source is external • 1: Source is internal • 2: Unknown
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devicePayloadId	An extendable field. Format: {threat_type}:{log_id}:{with pcap file captured}{:extensions}*	Examples: • With pcap file captured: 2:10245:P • Without pcap file captured: 2:10245:
dhost	Destination host name	Example: dhost1
dmac	Destination MAC	Example: 00:0C:29:6E:CB:F9
dpt	Destination port	Value between 1 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

CEF Key	Description	Value
rt	Log generation time Format: Unix time stamp (number of milliseconds since Jan 01 1970 UTC)	Example: 1593761104000
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 1 and 65535
src	Source IP address	Example: 10.1.144.199

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Dir
ector|5.3.0.1212|100120|Deep Discovery Inspector detected the
protocol in your monitored network.|2|dvc=172.22.9.32 dvcmac=0
0:50:56:AD:03:BD dvchost=localhost deviceExternalId=E9A3FA4339
16-4738984C-A4BF-84A0-D603 rt=1593761104000 app=eDonkey device
Direction=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=3993
3 smac=00:30:da:2d:47:32 cn3Label=Threat Type cn3=6 sourceTran
slatedAddress=10.1.117.231 destinationTransla tedAddress=10.1.
100.223 cnt=1 flexNumber1Label=vLANId flexNum ber1=4095 device
PayloadId=6:11:P
```

CEF Web Reputation Logs

Table 2-4. 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 Director
Header (pver)	Appliance version	Example: 5.3.0.1212
Header (eventid)	Signature ID	100101
Header (eventName)	Description	Example: Dangerous URL in Web Reputation Services database - HTTP (Request)
Header (severity)	Severity	• 2: Informational • 4: Low • 6: Medium • 8: High
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	• Intelligence Gathering • Point of Entry • Command and Control Communication • Lateral Movement • Asset and Data Discovery • Data Exfiltration • Nil (no applicable attack phase)
cs4Label	Attack Phase	pAttackPhase
destinationTranslatedAddress	Peer IP	Example: 10.1.144.199
deviceDirection	Packet direction	0, 1, or 2 • 0: Source is external • 1: Source is internal • 2: Unknown
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536

CEF Key	Description	Value
devicePayloadId	An extendable field. Format: {threat_type}:{log_id}:{with pcap file captured}{:extensions}*	Examples: • With pcap file captured: 2:10245:P • Without pcap file captured: 2:10245:
dhost	Destination host name	Example: dhost1
dmac	Destination MAC	Example: 00:0C:29:6E:CB:F9
dpt	Destination port	Value between 1 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?term=value
requestClientApplication	User agent	Example: IE
rt	Log generation time Format: Unix time stamp (number of milliseconds since Jan 01 1970 UTC)	Example: 1593761104000
shost	Source host name	Example: shost1
smac	Source MAC	Example: 00:0C:29:6E:CB:F9
sourceTranslatedAddress	Interested IP	Example: 10.1.144.199

CEF Key	Description	Value
spt	Source port	Value between 1 and 65535
src	Source IP address	Example: 10.1.144.199
suser	Mail sender	Example: suser1

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Dir
ector|5.3.0.1212|100101|Ransomware URL in Web Reputation Servi
ces database - HTTP (Request)|8|dvc=172.22.9.32 dvcmac=00:50:5
6:AD:03:BD dvchost=localhost deviceExternalId=E9A3FA433916-473
8984C-A4BF-84A0-D603 rt=1593761104000 cs3Label=HostName_Ext cs
3=ca95-1.winshipway.com cn2Label=WRSScore cn2=49 cn3Label=Thre
at 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 sourceTranslatedAddre
ss=172.22.9.5 cn1Label=CCCA_Detection cn1=1 request=http://ca9
5-1.winshipway.com/ requestClientApplication=Wget /1.12 (linux
-gnu) app=HTTP deviceDirection=1 dhost=150.70.1 62.115 dst=150
.70.162.115 dpt=80 cs2Label=URLCategory cs2=Ransomware destina
tionTranslatedAddress=150.70.162.115 cs4Label=pAttackPhase cs4
=Command and Control Communication flexNumber1Label=vLANId fle
xNumber1=4095 request=http://ca95-1.winshipway.com/ devicePayl
oadId=5:17:
```

CEF Detection Logs: Email Detection Logs

Table 2-5. CEF Detection Logs: Email Detection Logs

CEF Key	Description	Value
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Director
Header (pver)	Appliance version	Example: 5.3.0.1212

CEF Key	Description	Value
Header (eventid)	Signature ID	100130
Header (eventName)	Description	EMAIL_DETECTION
Header (severity)	Email severity	• 2: Unavailable • 4: Low • 6: Medium • 8: High
act	The action in the event	Examples: • quarantined • passed • stripped • analyzed • stamped • subjectsTagged • deleted • delivered directly • cleaned up • file sanitized

CEF Key	Description	Value
cn1	Threat type	• 1: Targeted malware • 2: Malware • 3: Malicious URL • 4: Suspicious file • 5: Suspicious URL • 6: Spam/Graymail • 7: Phishing • 8: Content violation • 9: DLP incident
cn1Label	Threat type	threatType
cn2	Email Size	Example: 30841
cn2Label	Email Size	msgSize
cs1	Names of threats in the email	Example: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS
cs1Label	Names of threats in the email	threats
cs2	Internal email ID	Example: 6965222B-13A6-C705-89D4-6251B6C41E03
cs2Label	Internal email ID	msgUuid
cs3	Email ID	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
cs3Label	Email ID	messageId
cs4	Sender email address	Example: user1@domain.com
cs4Label	Label for sender email address	senderMail

CEF Key	Description	Value
cs5	Recipient email address	Example: user2@domain.com
cs5Label	Label for recipient email address	rcptMail
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
duser	Email recipients	Example: user1@domain2.com;test@163.com
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
msg	Email subject	Example: hello
rt	Log generation time Format: Unix time stamp (number of milliseconds since Jan 01 1970 UTC)	Example: 1593761104000
src	Source IP address	Example: 10.1.144.199
suser	Email sender	Example: user2@domain.com

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Dir
ector|5.3.0.1212|100130|EMAIL_DETECTION|6|rt=1593761104000 src
=150.70.186.134 cs3Label=messageId cs3=<20150323115314.BCA2C91
68EA@internalbeta.bcc.ddei> deviceExternalId=c425624a-e9db-4f3
f-8088-2726f15e6587 act=passed dvchost=internalbeta.bcc.ddei d
vc=10.64.1.131 duser=user1@domain1.com;user2@domain1.com;user3
@domain1.com msg=Virus_Report-20150323_02:00 cn2Label=msgSize
cn2=83878 cn1Label=threatType cn1=3 suser=user@domain2.com dvc
mac=C4:34:6B:B8:09:BC cs2Label=msgUuid cs2=73A9FA6A-11F3-4F05-
BCEE-6BB5EC111FE7 cs1Label=threats cs1=PUA_Test_File|TROJ_GEN.
R04AC0PAH15|PAK_Generic.005|ADW_DOWNLOADER.WRS|LOW-REPUTATION-
URL_BLOCKED-LIST.SCORE.WRS|LOW-REPUTATION-URL_BLOCKED-LIST.SCO
```

```
RE.WRS|TROJ_GEN.R02SC0OLH14|TROJ_GENERIC.WRS|TROJ_DOWNLOADER.W
RS
```

CEF Detection Logs: Attachment Detection Logs

TABLE 2-6. CEF Detection Logs: Attachment Detection Logs

CEF KEY	DESCRIPTION	VALUE
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Director
Header (pver)	Appliance version	Example: 5.3.0.1212
Header (eventid)	Signature ID	100131
Header (eventName)	Description	ATTACHMENT_DETECTION
Header (severity)	Severity	• 2: Unavailable • 4: Low • 6: Medium • 8: High
cs1	Threat name	Example: VAN_BOT.UMXX
cs1Label	Threat name	threats
cs2	Internal email ID	Example: 6965222B-13A6-C705-89D4-6251B6C41E03
cs2Label	Internal email ID	msgUuid
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost

CEF Key	Description	Value
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
rt	Log generation time Format: Unix time stamp (number of milliseconds since Jan 01 1970 UTC)	Example: 1593761104000

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Dir
ector|5.3.0.1212|100131|ATTACHMENT_DETECTION|6|rt=159376110400
0 fileHash=E49395FEACC12A5613E7BA6C69AC5E42EDFDA42D fsize=1768
1 fileType=MIME Base64 dvchost=internalbeta.bcc.ddei dvc=10.64
.1.131 deviceExternalId=c425624a-e9db-4f3f-8088-2726f15e6587 c
s2Label=msgUuid cs2=E89A23BE-11F5-2505-BCEE-21027D078154 fname
=3C761B45-626D-4E75-B4782FD0E5E8369C.eml dvcmac=C4:34:6B:B8:09
:BC cs1Label=threats cs1=TROJ_UP.258A1A7D
```

CEF Detection Logs: URL Detection Logs

Table 2-7. CEF Detection Logs: URL Detection Logs

CEF Key	Description	Value
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Director

CEF Key	Description	Value
Header (pver)	Appliance version	Example: 5.3.0.1212
Header (eventid)	Signature ID	100132
Header (eventName)	Description	URL_DETECTION
Header (severity)	Email severity	• 4: Low • 6: Medium • 8: High
cat	Category	Example: 90:02
cs1	Threat name	Example: LOW-REPUTATION-URL_MALWARE.WRS
cs1Label	Threat name	threats
cs2	Internal email ID	Example: 6965222B-13A6-C705-89D4-6251B6C41E03
cs2Label	Internal email ID	msgUuid
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
request	URL	Example: http://www.rainking.net/?utm_campaign=4-21-2014 |http://images.rainking.net/eloquaimage
rt	Log generation time Format: Unix time stamp (number of milliseconds since Jan 01 1970 UTC)	Example: 1593761104000

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Dir
ector|5.3.0.1212|100132|URL_DETECTION|6|rt=1593761104000 cs2La
bel=msgUuid cs2=73A9FA6A-11F3-4F05-BCEE-6BB5EC111FE7 dvcmac=C4
:34:6B:B8:09:BC dvchost=internalbeta.bcc.ddei request=http://w
ww.alltobid.com/guopai/upload/dan201401.zip d vc=10.64.1.131 d
eviceExternalId=c425624a-e9db-4f3f-8088-2726f 15e6587
```

CEF Message Tracking Logs

TABLE 2-8. CEF Message Tracking Logs

CEF KEY	DESCRIPTION	VALUE
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Director
Header (pver)	Appliance version	Example: 5.3.0.1212
Header (eventid)	Signature ID	100136
Header (eventName)	Description	MESSAGE_TRACKING
Header (severity)	Email severity	• 2: Unavailable • 2: Unrated • 2: Normal • 4: Low • 6: Medium • 8: High
dvc	Appliance IP address	Example: 10.1.144.199
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
dvchost	Appliance host name	Example: localhost

CEF Key	Description	Value
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
rt	Log generation time Format: Unix time stamp (number of milliseconds since Jan 01 1970 UTC)	Example: 1593761104000
cs1Label	Label for Email ID	messageId
cs1	Email ID	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.ddei>
cs2Label	Internal email ID	msgUuid
cs2	Internal email ID	Example: 6965222B-13A6-C705-89D4-6251B6C41E03
suser	Email sender	Example: user2@domain.com
duser	Email recipients	Example: user1@domain2.com;test@163.com
msg	Email subject	Example: hello
reason	Reason for block action	Example: Timeout period expired
cs3Label	Latest status	latestStatus
cs3	Details	• Quarantined • Delivered • Delivery unsuccessful • Processing completed • Deleted
src	Source IP address	Example: 10.1.144.199
cs4Label	Label for sender email address	senderMail

CEF Key	Description	Value
cs4	Sender email address	Example: user1@domain.com
cs5Label	Label for recipient email address	rcptMail
cs5	Recipient email address	Example: user2@domain.com
deviceTranslatedAddress	Relay MTA IP address	Example: 204.92.31.146
cs6Label	Label for process history	procHistory
cs6	Process history	Example: Action taken by the device. The format: "timestamp1 act1,timestamp2 act2,…, timestampn actn"

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Dir
ector|5.3.0.1212|100136|MESSAGE_TRACKING|2|rt=1593761104000 cs
3Label=latestStatus cs3=Delivery unsuccessful dvchost=localhos
t.localdomain deviceExternalId=9ceb7be2-3ec5-4b80-8697-6b4913e
b044b dvc=10.204.63.177 duser=test@test.com dvcmac=00:50:56:A7
:5F:AD reason=host 10.204.253.179[10.204.253.179] said: 552 te
st@test.com mailbox full (in reply to end of DATA command) cs1
Label=messageId cs1=20180427025553.4D771D6135F@localhost.local
domain cs4Label=senderMail cs4=marks@relay.ddei.com suser=fake
@test.test msg=plain_text_upper_case.HTML/HTM cs2Label=msgUuid
cs2=EB715918-6ACB-A405-BF46-56F53CE3FD86 cs6Label=procHistory
cs6=Apr 27 2018 02:55:53 GMT+00:00 Received,Apr 27 2018 02:55:
53 GMT+00:00 Sent for analysis,Apr 27 2018 02:56:48 GMT+00:00
Action set to 'pass',Apr 27 2018 02:56:48 GMT+00:00 Delivery u
nsuccessful,Reason:host 10.204.253.179[10.204.253.179] said: 5
52 test@test.com mailbox full (in reply to end of DATA command
)
```

CEF Virtual Analyzer Analysis Logs: File Analysis Events

TABLE 2-9. CEF Virtual Analyzer Analysis Logs: File Analysis Events

CEF KEY	DESCRIPTION	VALUE
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Director
Header (pver)	Appliance version	Example: 5.3.0.1212
Header (eventid)	Signature ID	200119
Header (eventName)	Description	Sample file sandbox analysis is finished
Header (severity)	Severity	3: Informational
cn1	Result of GRID/CSSS	• 0: GRID is not known good • 1: GRID is known good
cn1Label	Result of GRID/CSSS	GRIDIsKnownGood
cn2	ROZ rating	Example: 3: High risk
cn2Label	ROZ rating	ROZRating
cn3	PCAP ready	• 0: PCAP is not ready • 1: PCAP is ready
cn3Label	PCAP ready	PcapReady
cs1	Sandbox image type	Example: win7
cs1Label	Sandbox image type	SandboxImageType
cs2	Malware name	Example: HEUR_NAMETRICK.A
cs2Label	Malware name	MalwareName

CEF Key	Description	Value
cs3	Parent SHA1	Example: A29E4ACA70BEF4AF8CE75AF51032B6B91572AA0D
cs3Label	Parent SHA1	ParentFileSHA1
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
rt	Analysis time Format: Unix time stamp (number of milliseconds since Jan 01 1970 UTC)	Example: 1593761104000

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Dir
ector|5.3.0.1212|200119|Sample file sandbox analysis is finish
ed|3|rt=1593761104000 dvc=10.64.1.131 dvchost=internalbeta.bcc
.ddei dvcmac=C4:34:6B:B8:09:BC deviceExternalId=c425624a-e9db-
4f3f-8088-2726f15e6587 fname=Wonga Express Loan Promtion 3.5%
Offer.doc fileHash=A46E1F56969DECC5FEAF120A2279946A2F42D619 fi
leType=MS Office fsize=53760 cs1Label=SandboxImageType cs1=win
81en cn1Label=GRIDIsKnownGood cn1=-1 cn2Label=ROZRating cn2=1
cs2Label=MalwareName cs2=VAN_MALWARE.UMXX cn3Label=PcapReady c
n3=1
```

CEF Virtual Analyzer Analysis Logs: URL Analysis Events

TABLE 2-10. CEF Virtual Analyzer Analysis Logs: URL Analysis Events

CEF KEY	DESCRIPTION	VALUE
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Director
Header (pver)	Appliance version	Example: 5.3.0.1212
Header (eventid)	Signature ID	200126
Header (eventName)	Description	URL sandbox analysis is finished
Header (severity)	Severity	3
cn2	ROZ rating	Example: 3: High risk
cn2Label	ROZ rating	ROZRating
cn3	PCAP ready	• 0: PCAP is not ready • 1: PCAP is ready
cn3Label	PCAP ready	PcapReady
cs1	Sandbox image type	Example: win7
cs1Label	Sandbox image type	SandboxImageType
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9

CEF Key	Description	Value
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
request	URL	Example: http://www.rainking.net/?utm_campaign=4-21-2014 |http://images.rainking.net/eloquaimage
rt	Analysis time Format: Unix time stamp (number of milliseconds since Jan 01 1970 UTC)	Example: 1593761104000

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Dir
ector|5.3.0.1212|200126|URL sandbox analysis is finished|3|rt=
1593761104000 dvc=10.64.1.131 dvchost=internalbeta.bcc.ddei dv
cmac=C4:34:6B:B8:09:BC deviceExternalId=c425624a-e9db-4f3f-808
8-2726f15e6587 request=http://paypal-world.ga/home/? fileHash=
5EA358C987D1FDE34957B9A36AF38321C5F37D8B cs1Label=SandboxImage
Type cs1=win81en cn2Label=ROZRating cn2=3 cn3Label=PcapReady c
n3=1
```

CEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

Table 2-11. CEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

CEF Key	Description	Value
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	Deep Discovery Director

CEF Key	Description	Value
Header (pver)	Appliance version	Example: 5.3.0.1212
Header (eventid)	Signature ID	200127
Header (eventName)	Description	Notable Characteristics of the analyzed sample
Header (severity)	Severity	6
cs1	Violated policy name	Example: Internet Explorer Setting Modification
cs1Label	Violated policy name	PolicyCategory
cs2	Violated event analysis	Example: Modified important registry items
cs2Label	Violated event analysis	PolicyName
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
msg	Details	Example: Process ID: 3020\n Image Path: %ProgramFiles%\\Internet Explorer\\IExplore.exe SCODEF:2956 CREDAT:209921 / prefetch:2

CEF Key	Description	Value
rt	Analysis time Format: Unix time stamp (number of milliseconds since Jan 01 1970 UTC)	Example: 1593761104000

Log sample:

```
May 15 16:00:47 localhost CEF:0|Trend Micro|Deep Discovery Dir
ector|5.3.0.1212|200127|Notable Characteristics of the analyze
d sample|6|rt=1593761104000 dvc=10.64.1.131 dvchost=internalbe
ta.bcc.ddei dvcmac=C4:34:6B:B8:09:BC deviceExternalId=c425624a
-e9db-4f3f-8088-2726f15e6587 fname=http://bsjv.tk/bbb/bbb/bbb
fileHash=2D302EEEF703CBB8713B806B3C5B4B3A2A28E92A fileType=URL
fsize=0 cs1Label=PolicyCategory cs1=Process, service, or memor
y object change msg=Process ID: 3020\n Image Path: %ProgramFil
es%\\Internet Explorer\\IExplore.exe SCODEF:2956 CREDAT:209921
/prefetch:2 cs2Label=PolicyName cs2=Creates process
```

Chapter 3

Syslog Content Mapping - LEEF

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

- Deep Discovery Director Suspicious Objects lists:
  - *LEEF Virtual Analyzer Logs: Deny List Transaction Events on page 3-2*
- Deep Discovery Inspector detection logs:
  - *LEEF Threat Logs on page 3-4*
  - *LEEF Disruptive Application Logs on page 3-11*
  - *LEEF Web Reputation Logs on page 3-14*
  - *LEEF Correlation Incident Logs on page 3-18*

Note

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

LEEF Virtual Analyzer Logs: Deny List Transaction Events

TABLE 3-1. 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 Director
Header (pver)	Appliance version	Example: 5.3.0.1212
Header (eventName)	Event Name	DENYLIST_CHANGE
act	The action in the event	• Add • Remove
deviceExternalRiskType	Risk level	• Low • Medium • High
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
dpt	Remote port	Value between 1 and 65535
dst	Remote IP	Example: 10.1.144.199
dvc	Appliance IP address	Example: 10.1.96.147

LEEF Key	Description	Value
dvchost	Appliance host name	Example: localhost
end	Report end time	Example: Mar 09 2015 17:05:21 GMT +08:00
fileHash	SHA1	Example:1EDD5B38DE4729545767088C5CAB395E4197C8F3
pComp	Detection source	• Sandbox • UDSO
sev	Severity	3 (fixed value)
type	Deny List type	• Deny List IP/Port • Deny List URL • Deny List File SHA1 • Deny List Domain
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.

```
May 15 16:00:47 localhost LEEF:1.0|Trend Micro|Deep Discovery
Director|5.3.0.1212|DENYLIST_CHANGE|devTime=Apr 01 2019 18:26:
11 GMT+08:00<009>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>sev=
3<009>dvc=10.1.96.147<009>dvchost=DDD-IB-int<009>deviceMacAddr
ess=00:50:56:A3:CE:81<009>deviceGUID=C4BD2B76-6C3D-416E-AB0C-6
FA204D00FBC<009>end=Jan 19 2038 11:14:07 GMT+08:00<009>act=Add
<009>type=Deny List File SHA1<009>fileHash=BF378BF908A802DEADF
A9CB9FA0C02955C904F08<009>deviceExternalRiskType=High<009>pCom
p=Sandbox
```

LEEF Threat Logs

TABLE 3-2. 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 Director
Header (pver)	Appliance version	Example: 5.3.0.1212
Header (eventName)	Event Name	• MALWARE_DETECTION • MALWARE_OUTBREAK_DETECTION • SECURITY_RISK_DETECTION
origin	Deep Discovery appliance the log originated from	Inspector
act	The action in the event	• blocked • 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	• IP_DOMAIN • IP_DOMAIN_PORT • URL • EMAIL

LEEF Key	Description	Value
cccaDetection	CCCA detection	0 or 1
cccaDetectionSource	CCCA log is detected by	• GLOBAL_INTELLIGENCE • VIRTUAL_ANALYZER • USER_DEFINED
cccaRiskLevel	CCCA Risk Level	• 0: Unknown • 1: Low • 2: Medium • 3: High
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	• 0: Known detection • 1: Unknown detection • 2: OPS detection
deviceDirection	Packet direction	• 0: Source is external • 1: Source is internal • 2: Unknown
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
deviceRiskConfidenceLevel	Confidence level	• 1: High • 2: Medium • 3: Low • 0: Undefined

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 1 and 65535
dstZone	Destination zone	• 0: Not in monitored network • 1: In monitored network and trusted • 2: In monitored network and untrusted
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: 10.1.96.147

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: dc036acb-9a2e-4939-8244-dedbda9ec4ba
msg	Description	Example: HEUR_NAMETRICK.A - SMTP (Email)
oldFileHash	Mail attachment SHA1	Example: 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	• Intelligence Gathering • Point of Entry • Command and Control Communication • Lateral Movement • Asset and Data Discovery • Data Exfiltration • Nil (no applicable attack phase)
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
requestClientApplication	User agent	Example: IE
riskType	Potential risk	• 0: Known risk • 1: Potential risk
ruleId	Rule ID	Example: 52
sAttackPhase	Secondary attack phase	Example: Point of Entry

LEEF Key	Description	Value
sev	Severity	• 2: Informational • 4: Low • 6: Medium • 8: High
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 1 and 65535
srcZone	Source zone	• 0: Not in monitored network • 1: In monitored network and trusted • 2: In monitored network and untrusted
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	• 0: Malicious content • 1: Malicious behavior • 2: Suspicious behavior • 3: Exploit • 4: Grayware
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.

```
May 15 16:00:47 localhost LEEF:1.0|Trend Micro|Deep Discovery
Director|5.3.0.1212|SECURITY_RISK_DETECTION|origin=Inspector<0
09>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>ptype=IDS<009>dvc=
10.1.105.120<009>deviceMacAddress=00:50:56:B6:FE:C0<009>dvchos
t=twddiv-120<009>deviceGUID=92A12204F15F-48B59215-C17B-C516-B2
CB<009>devTime=Apr 01 2019 10:24:45 GMT+00:00<009>sev=8<009>pr
otoGroup=TCP<009>proto=TCP<009>vLANId=4095<009>deviceDirection
=1<009>dhost=2.2.2.2<009>dst=2.2.2.2<009>dstPort=443<009>dstMA
C=58:35:d9:de:4a:42<009>shost=10.1.117.172<009>src=10.1.117.17
2<009>srcPort=35702<009>srcMAC=00:08:e3:ff:fd:90<009>malName=U
SR_SUSPICIOUS_IP.UMXX<009>malType=MALWARE<009>fileType=-65536<
009>fsize=0<009>ruleId=729<009>msg=Callback to IP address in C
ontrol Manager and Deep Discovery Director User-Defined Suspic
ious Objects list<009>deviceRiskConfidenceLevel=1<009>pComp=CA
V<009>riskType=1<009>srcGroup=My Company/TW 12F<009>srcZone=1<
009>dstZone=0<009>detectionType=1<009>act=not blocked<009>thre
atType=1<009>interestedIp=10.1.117.172<009>peerIp=2.2.2.2<009>
```

```
cnt=5<009>aggregatedCnt=1<009>cccaDestinationFormat=IP_DOMAIN<
009>cccaDetectionSource=USER_DEFINED<009>cccaRiskLevel=3<009>c
ccaDestination=2.2.2.2<009>cccaDetection=1<009>evtCat=Callback
<009>evtSubCat=Bot<009>aptRelated=0<009>pAttackPhase=Command a
nd Control Communication
```

LEEF Disruptive Application Logs

TABLE 3-3. 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 Director
Header (pver)	Appliance version	Example: 5.3.0.1212
Header (eventName)	Event Name	DISRUPTIVE_APPLICATION_DETECTION
origin	Deep Discovery appliance the log originated from	Inspector
aggregatedCnt	Aggregated count	Example: 1
cnt	Total count	Example: 1
deviceDirection	Packet direction	• 0: Source is external • 1: Source is internal • 2: Unknown
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

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 1 and 65535
dstZone	Destination zone	• 0: Not in monitored network • 1: In monitored network and trusted • 2: In monitored network and untrusted
dvc	Appliance IP address	Example: 10.1.96.147
dvchost	Appliance host name	Example: localhost
interestedIp	Interested IP	Example: 10.1.144.199
msg	Description	Example: HEUR_NAMETRICK.A - SMTP (Email)
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	• 2: Informational • 4: Low • 6: Medium • 8: High
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 1 and 65535
srcZone	Source zone	• 0: Not in monitored network • 1: In monitored network and trusted • 2: In monitored network and untrusted
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.

```
May 15 16:00:47 localhost LEEF:1.0|Trend Micro|Deep Discovery
Director|5.3.0.1212|DISRUPTIVE_APPLICATION_DETECTION|origin=In
spector<009>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>dvc=10.20
1.156.143<009>deviceMacAddress=00:0C:29:A6:53:0C<009>dvchost=d
```

```
di38-143<009>deviceGUID=6B593E17AFB7-40FBBB28-A4CE-0462-A536<0
09>ptype=IDS<009>devTime=Mar 09 2015 14:20:38 GMT+08:00<009>se
v=2<009>protoGroup=STREAMING<009>proto=WMSP<009>vLANId=4095<00
9>deviceDirection=1<009>dhost=12.190.48.13<009>dst=12.190.48.1
3<009>dstPort=80<009>dstMAC=00:17:9a:65:f3:05<009>shost=192.16
8.33.2<009>src=192.168.33.2<009>srcPort=35125<009>srcMAC=00:16
:6f:a1:3d:7a<009>msg=Deep Discovery Inspector detected the pro
tocol in your monitored network.<009>pComp=CAV<009>threatType=
6<009>srcGroup=Default<009>srcZone=1<009>dstZone=0<009>interes
tedIp=192.168.33.2<009>peerIp=12.190.48.13<009>cnt=1<009>aggre
gatedCnt=1
```

LEEF Web Reputation Logs

TABLE 3-4. 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 Director
Header (pver)	Appliance version	Example: 5.3.0.1212
Header (eventName)	Event Name	WEB_THREAT_DETECTION
origin	Deep Discovery appliance the log originated from	Inspector
cccaDetection	CCCA detection	0 or 1
cccaDetectionSource	CCCA log is detected by	• GLOBAL_INTELLIGENCE • VIRTUAL_ANALYZER • USER_DEFINED

LEEF Key	Description	Value
cccaRiskLevel	CCCA Risk Level	• 0: Unknown • 1: Low • 2: Medium • 3: High
deviceDirection	Packet direction	• 0: Source is external • 1: Source is internal • 2: Unknown
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 1 and 65535
dstZone	Destination zone	• 0: Not in monitored network • 1: In monitored network and trusted • 2: In monitored network and untrusted
duser	Mail recipient	Example: duser1

LEEF Key	Description	Value
dvc	Appliance IP address	Example: 10.1.96.147
dvchost	Appliance host name	Example: localhost
hostName	Host name	Example: CLIENT1
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/ 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	• 2: Informational • 4: Low • 6: Medium • 8: High
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

LEEF Key	Description	Value
srcMAC	Source MAC	Example: 00:0C:29:6E:CB:F9
srcPort	Source port	Value between 1 and 65535
srcZone	Source zone	• 0: Not in monitored network • 1: In monitored network and trusted • 2: In monitored network and untrusted
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.

```
May 15 16:00:47 localhost LEEF:1.0|Trend Micro|Deep Discovery
Director|5.3.0.1212|WEB_THREAT_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=6B593E17A
FB7-40FBBB28-A4CE-0462-A536<009>ptype=IDS<009>devTime=Mar 09 2
015 14:06:36 GMT+08:00<009>sev=6<009>protoGroup=HTTP<009>proto
=HTTP<009>vLANId=4095<009>deviceDirection=1<009>dhost=www.free
webs.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>sr
cPort=12121<009>srcMAC=fe:ed:be:ef:5a:c6<009>hostName=www.free
webs.com<009>msg=Dangerous URL in Web Reputation Services data
base - 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
>threatType=5<009>interestedIp=172.16.1.197<009>peerIp=216.52.
115.2
```

LEEF Correlation Incident Logs

TABLE 3-5. 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 Director
Header (pver)	Appliance version	Example: 5.3.0.1212
Header (eventName)	Event Name	SUSPICIOUS_BEHAVIOUR_DETECTION
origin	Deep Discovery appliance the log originated from	Inspector
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

LEEF Key	Description	Value
data9	Correlation data 9	Additional attribute values
deviceDirection	Packet direction	• 0: Source is external • 1: Source is internal • 2: Unknown
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: 10.1.96.147
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
interestedUser	Interested user name 1	Example: user1
interestedUser2	Interested user name 2	Example: user2
interestedUser3	Interested user name 3	Example: user3
pComp	Detection engine/ 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.

LEEF Key	Description	Value
sev	Severity	• 2: Informational • 4: Low • 6: Medium • 8: High
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.

```
May 15 16:00:47 localhost LEEF:1.0|Trend Micro|Deep Discovery
Director|5.3.0.1212|SUSPICIOUS_BEHAVIOUR_DETECTION|origin=Insp
ector<009>devTimeFormat=MMM dd yyyy HH:mm:ss z<009>deviceMacAd
dress=00:0C:29:A6:53:0C<009>dvchost=ddi38-143<009>pComp=Correl
ation<009>dvc=10.201.156.143<009>ptype=IDS<009>deviceGUID=D2C1
D6D20FF8-4FC98F92-25EB-D7DA-AF0E<009>devTime=Mar 11 2015 22:05
:50 GMT-04:00<009>sev=2<009>interestedIp=172.16.0.100<009>inte
restedHost=172.16.0.100<009>interestedMacAddress=00:0c:29:70:4
5:...36<009>ruleId=47<009>ruleName=This host has responded to
DNS queries.<009>threatType=Unregistered Service<009>threatNam
e=Unregistered DNS Server<009>proto=DNS Response<009>userGroup
=Default<009>deviceDirection=1
```

Index

TREND MICRO INCORPORATED

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

www.trendmicro.com

Item Code: APEM59606/220919