TREND MICRO™

2.6

TREND MICRO™ TippingPoint™ Advanced Threat Protection for Email

Syslog Content Mapping Guide

Advanced Protection Against Targeted Email Threats

Endpoint Security

Network Security

Protected Cloud

TREND MICRO SMART Protection Network™

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/en-us/enterprise/tippingpoint-advanced-threat-protection-for-email.aspx

Document Part No.: APEM27714/170215

Release Date: May 2017

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

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

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

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

Evaluate this documentation on the following site:

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

Table of Contents

Preface

Chapter 1: Introduction

Chapter 2: Syslog Content Mapping - CEF

Chapter 3: Syslog Content Mapping - LEEF

Chapter 4: Syslog Content Mapping - TMEF

Index

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 TippingPoint Advanced Threat Protection for Email 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 ATP Email, and explanations on ATP Email concepts and features.
Installation and Deployment Guide	The Installation and Deployment Guide contains information about requirements and procedures for planning deployment, installing ATP Email, 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 ATP Email.
Quick Start Card	The Quick Start Card provides user-friendly instructions on connecting ATP Email 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	Web-based documentation that is accessible from the ATP Email management console. The Online Help contains explanations of ATP Email components and features, as well as procedures needed to configure ATP Email.

Document	Description
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: http://esupport.trendmicro.com

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

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

Audience

The TippingPoint Advanced Threat Protection for Email 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
- Email routing
- SMTP

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

Document Conventions

The documentation uses the following conventions:

TABLE 2. Document Conventions

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

About Trend Micro

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

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

http://www.trendmicro.com

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 TippingPoint Advanced Threat Protection for Email Syslog Content Mapping Guide provides information about log management standards and syntaxes for implementing syslog events in Trend Micro ATP Email.

To enable flexible integration with third-party log management systems, TippingPoint Advanced Threat Protection for Email 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. TippingPoint Advanced Threat Protection for Email 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. TippingPoint Advanced Threat Protection for Email uses a subset of the LEEF dictionary.

LOG MANAGEMENT SYSTEM	DESCRIPTION
Trend Micro Event Format (TMEF) For details, see *Syslog Content Mapping - TMEF on page 4-1*	TMEF is a superset of log fields that allow a third-party syslog collector to better control and mitigate detection events provided by TippingPoint Advanced Threat Protection for Email.

Syslog Events

TippingPoint Advanced Threat Protection for Email supports the following events.

TABLE 1-1. Syslog events

EVENT	DESCRIPTION
Detection Logs: Email Detection Logs	Email detection logs from TippingPoint Advanced Threat Protection for Email. These logs contain information related to the detected email messages (such as sender, recipients, subject, and message ID).
Detection Logs: Attachment Detection Logs	Attachment detection logs from TippingPoint Advanced Threat Protection for Email. These logs contain information related to the detected attachments (such as file name, file size, and file type).
Detection Logs: URL Detection Logs	URL detection logs from TippingPoint Advanced Threat Protection for Email. These logs contain the URLs detected and potential threats.
Alert Logs	Alert logs from TippingPoint Advanced Threat Protection for Email. These logs contain information related to the alerts (such as alert name and alert notification content).
Virtual Analyzer Analysis Logs: File Analysis Events	File analysis events from Virtual Analyzer. These logs contain information related to the analyzed files (such as file name, file size, and file type).
Virtual Analyzer Analysis Logs: URL Analysis Events	URL analysis events from Virtual Analyzer. These logs contain the URLs analyzed and potential threats.
Virtual Analyzer Analysis Logs: Notable Characteristics Events	Notable characteristics events from Virtual Analyzer. These logs contain information about notable characteristics events that are triggered by the analyzed samples.

Event	Description
Virtual Analyzer Analysis Logs: Deny List Transaction Events	Deny list transaction events from Virtual Analyzer. These logs contain actions performed on specific deny lists and information about the deny list objects (such as SHA1 or URL).
System Logs	These are audit logs or update logs from TippingPoint Advanced Threat Protection for Email.

Terminology

Term	Description
CEF	Common Event Format
LEEF	Log Event Extended Format
TMEF	Trend Micro Event Format

Chapter 2

Syslog Content Mapping - CEF

The following tables outline syslog content mapping between TippingPoint Advanced Threat Protection for Email log output and CEF syslog types:

- *CEF Detection Logs: Email Detection Logs on page 2-2*
- *CEF Detection Logs: Attachment Detection Logs on page 2-4*
- *CEF Detection Logs: URL Detection Logs on page 2-6*
- *CEF Alert Logs on page 2-7*
- *CEF Virtual Analyzer Analysis Logs: File Analysis Events on page 2-10*
- *CEF Virtual Analyzer Analysis Logs: URL Analysis Events on page 2-13*
- *CEF Virtual Analyzer Analysis Logs: Notable Characteristics Events on page 2-14*
- *CEF Virtual Analyzer Analysis Logs: Deny List Transaction Events on page 2-16*
- *CEF System Logs on page 2-18*

CEF Detection Logs: Email Detection Logs

TABLE 2-1. 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	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	100130
Header (eventName)	Description	EMAIL_DETECTION
Header (severity)	Email severity	• 4: Low • 6: Medium • 8: High
act	The action in the event	Examples: • quarantined • passed • stripped • analyzed • stamped • subjectsTagged
cn1	Threat type	• 1: Targeted malware • 2: Malware • 3: Malicious URL • 4: Potentially malicious file • 5: Potentially malicious URL

CEF Key	Description	Value
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.atp_email>
cs3Label	Email ID	messageId
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	Example: Mar 09 2015 17:05:21 GMT+00:00
src	Source IP address	Example: 10.1.144.199

CEF Key	Description	Value
suser	Email sender	Example: user2@domain.com

Log sample:

```
CEF:0|Trend Micro|TippingPoint Advanced Threat Protection for
Email|2.5.1.1161|100130|EMAIL_DETECTION|6|rt=Mar 23 2015 11:53
:17 GMT+00:00 src=150.70.186.134 cs3Label=messageId cs3=<20150
323115314.BCA2C9168EA@internalbeta.bcc.atp_email> deviceExtern
alId=c425624a-e9db-4f3f-8088-2726f15e6587 act=passed dvchost=i
nternalbeta.bcc.atp_email dvc=10.64.1.131 duser=sean_hsu@trend
.com.tw;descartes_chen@trend.com.tw;joseph_c_chen@trend.com.tw
;mark_tang@trendmicro.com.cn;chenghsin_hsu@trend.com.tw msg=Vi
rus_Report-20150323_02:00 cn2Label=msgSize cn2=83878 cn1Label=
threatType cn1=3 suser=odin@wtp-gd-hadoop02.iad1 dvcmac=C4:34:
6B:B8:09:BC cs2Label=msgUuid cs2=73A9FA6A-11F3-4F05-BCEE-6BB5E
C111FE7 cs1Label=threats cs1=PUA_Test_File|TROJ_GEN.R04AC0PAH1
5|PAK_Generic.005|ADW_DOWNLOADER.WRS|LOW-REPUTATION-URL_BLOCKE
D-LIST.SCORE.WRS|LOW-REPUTATION-URL_BLOCKED-LIST.SCORE.WRS|TRO
J_GEN.R02SC0OLH14|TROJ_GENERIC.WRS|TROJ_DOWNLOADR.WRS
```

CEF Detection Logs: Attachment Detection Logs

Table 2-2. 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	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	100131

CEF Key	Description	Value
Header (eventName)	Description	ATTACHMENT_DETECTION
Header (severity)	Severity	• 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
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	Example: Mar 09 2015 17:05:21 GMT+00:00

Log sample:

```
CEF:0|Trend Micro|TippingPoint Advanced Threat Protection for
Email|2.5.1.1139|100131|ATTACHMENT_DETECTION|6|rt=Mar 23 2015
14:04:46 GMT+00:00 fileHash=E49395FEACC12A5613E7BA6C69AC5E42ED
```

```
FDA42D fsize=17681 fileType=MIME Base64 dvchost=internalbeta.b
cc.atp_email dvc=10.64.1.131 deviceExternalId=c425624a-e9db-4f
3f-8088-2726f15e6587 cs2Label=msgUuid cs2=E89A23BE-11F5-2505-B
CEE-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 2-3. 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	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
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

CEF KEY	DESCRIPTION	VALUE
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	Example: Mar 09 2015 17:05:21 GMT+00:00

Log sample:

```
CEF:0|Trend Micro|TippingPoint Advanced Threat Protection for
Email|2.5.1.1139|100132|URL_DETECTION|6|rt=Mar 23 2015 11:57:
46 GMT+00:00 cs2Label=msgUuid cs2=73A9FA6A-11F3-4F05-BCEE-6BB
5EC111FE7 dvcmac=C4:34:6B:B8:09:BC dvchost=internalbeta.bcc.a
tp_email request=http://www.alltobid.com/guopai/upload/dan201
401.zip dvc=10.64.1.131 deviceExternalId=c425624a-e9db-4f3f-8
088-2726f15e6587
```

CEF Alert Logs

TABLE 2-4. CEF Alert 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	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	300105
Header (eventName)	Description	ALERT_EVENT
Header (severity)	Alert severity	• 2: Informational • 6: Important • 8: Critical
cs1	Alert name	Example: Security: Suspicious Messages Identified
cs1Label	Alert name	ruleName
cs2	Description	Example: 1 or more messages detected with threats
cs2Label	Description	ruleCriteria
cs3	Triggered value	Example: 35
cs3Label	Triggered value	eventTriggeredValue

CEF Key	Description	Value
cs4	Notification content	Example: The following email messages contain threats: Risk: Medium (Malware) Action: Quarantined Message ID: <20150619032243.5923E650365@localhost.atp_email-164> Recipients: fake@test.com;test@test.com Sender: test@fake.test Subject: high_4_file_507ECC33FA60979F6B97D84DA47972096185C263 Attachment: 4_file_507ECC33FA60979F6B97D84DA47972096185C263 (MIME Base64) Detected: 2015-05-25 11:11:00 Alert time: 2015-05-25 11:11:27 +0800 **Note** The maximum length is 1023 characters.
cs4Label	Notification content	ruleContent
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
externalId	The logid in the alert database	Example: 1648
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+00:00

Log sample:

```
CEF:0|Trend Micro|TippingPoint Advanced Threat Protection for
Email|2.5.1.1009|300105|ALERT_EVENT|6|rt=Jun 16 2015 09:26:25
 GMT+00:00 cs1Label=ruleName cs1=Security: Threat Messages cn
t=1 cs2Label=ruleCriteria cs2=At least 1 threat message detec
ted externalId=1299 cs3Label=ruleContent cs3=The%20following%
20email%20messages%20contain%20threats%3A%0A%0A%3D%3D%3D%3D%3
D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D
%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%
3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%3D%0ARisk%3A%20Medi
um%20%28Malware%29%0AAction%3A%20%20Quarantined%0AMessage%20I
D%3A%20%3C20150616092610.B56A66503C6%40localhost.atp_email164
%3E%0ARecipients%3A%20fake%40test.com%3Btest%40test.com%0ASen
der%3A%20test%40fake.test%0ASubject%3A%20temail%20-%20Copyaaa
... dvcmac=00:50:56:01:2C:BC dvchost=localhost.atp_email-164
deviceExternalId=361a091c-addd-40cf-98e7-710e43500a66 dvc=10.
204.253.164
```

CEF Virtual Analyzer Analysis Logs: File Analysis Events

Table 2-5. 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

CEF Key	Description	Value
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
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
cs3	Parent SHA1	Example: A29E4ACA70BEF4AF8CE75AF51032B6B91572AA0D
cs3Label	Parent SHA1	ParentFileSHA1
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536

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: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
rt	Analysis time	Example: Mar 09 2015 17:05:21 GMT+00:00

Log sample:

```
CEF:0|Trend Micro|TippingPoint Advanced Threat Protection for
Email|2.5.1.1139|200119|Sample file sandbox analysis is finis
hed|3|rt=Mar 23 2015 14:48:24 GMT+00:00 dvc=10.64.1.131 dvcho
st=internalbeta.bcc.atp_email dvcmac=C4:34:6B:B8:09:BC device
ExternalId=c425624a-e9db-4f3f-8088-2726f15e6587 fname=Wonga E
xpress Loan Promtion 3.5% Offer.doc fileHash=A46E1F56969DECC5
FEAF120A2279946A2F42D619 fileType=MS Office fsize=53760 cs1La
bel=SandboxImageType cs1=win81en cn1Label=GRIDIsKnownGood cn1
=-1 cn2Label=ROZRating cn2=1 cs2Label=MalwareName cs2=VAN_MAL
WARE.UMXX cn3Label=PcapReady cn3=1
```

CEF Virtual Analyzer Analysis Logs: URL Analysis Events

Table 2-6. 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	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
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	Example: Mar 09 2015 17:05:21 GMT+00:00

Log sample:

```
CEF:0|Trend Micro|TippingPoint Advanced Threat Protection for
Email|2.5.1.1139|200126|URL sandbox analysis is finished|3|rt
=Mar 23 2015 16:32:15 GMT+00:00 dvc=10.64.1.131 dvchost=inter
nalbeta.bcc.atp_email dvcmac=C4:34:6B:B8:09:BC deviceExternal
Id=c425624a-e9db-4f3f-8088-2726f15e6587 request=http://paypal
-world.ga/home/? fileHash=5EA358C987D1FDE34957B9A36AF38321C5F
37D8B cs1Label=SandboxImageType cs1=win81en cn2Label=ROZRatin
g cn2=3 cn3Label=PcapReady cn3=1
```

CEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

Table 2-7. 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	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161

CEF Key	Description	Value
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	Example: Mar 09 2015 17:05:21 GMT+00:00

Log sample:

```
CEF:0|Trend Micro|TippingPoint Advanced Threat Protection for
Email|2.5.1.1139|200127|Notable Characteristics of the analyz
ed sample|6|rt=Mar 23 2015 10:44:28 GMT+00:00 dvc=10.64.1.131
 dvchost=internalbeta.bcc.atp_email dvcmac=C4:34:6B:B8:09:BC
deviceExternalId=c425624a-e9db-4f3f-8088-2726f15e6587 fname=h
ttp://bsjv.tk/bbb/bbb/bbb fileHash=2D302EEEF703CBB8713B806B3C
5B4B3A2A28E92A fileType=URL fsize=0 cs1Label=PolicyCategory c
s1=Process, service, or memory object change msg=Process ID:
3020\nImage Path: %ProgramFiles%\\Internet Explorer\\IExplore
.exe SCODEF:2956 CREDAT:209921 /prefetch:2 cs2Label=PolicyNam
e cs2=Creates process
```

CEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

Table 2-8. CEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

CEF Key	Description	Value
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	200120
Header (eventName)	Description	Deny List updated
Header (severity)	Severity	3

CEF Key	Description	Value
act	The action in the event	- Add - Remove
cs1	Deny List type	- Deny List IP/Port - Deny List URL - Deny List File SHA1 - Deny List Domain
cs1Label	Deny List type	type
cs2	Risk level	- Low - Medium - High - Confirmed Malware
cs2Label	Risk level	RiskLevel
deviceExternalId	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
dhost	Destination host name	Example: dhost1
dpt	Destination port	Value between 0 and 65535
dst	Destination IP address	Example: 10.1.144.199
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
end	Report end time	Example: Mar 09 2015 17:05:21 GMT+00:00
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3

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

Log sample:

```
CEF:0|Trend Micro|TippingPoint Advanced Threat Protection for
Email|2.5.1.1139|200120|Deny List updated|3|rt=Mar 24 2015 10
:10:20 GMT+00:00 dvc=10.64.1.131 dvchost=internalbeta.bcc.atp
_email dvcmac=C4:34:6B:B8:09:BC deviceExternalId=c425624a-e9d
b-4f3f-8088-2726f15e6587 cs1Label=type cs1=Deny List File SHA
1 end=Apr 19 2015 16:03:13 GMT+00:00 act=Add fileHash=41D1881
69D9B986818A437DD80814FA84B0522FB cs2Label=RiskLevel cs2=High
```

CEF System Logs

Table 2-9. CEF System Logs

CEF Key	Description	Value
Header (logVer)	CEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	• 300102 (PRODUCT_UPDATE) • 300999 (SYSTEM_EVENT)

CEF Key	Description	Value
Header (eventName)	Description	- PRODUCT_UPDATE (300102) - SYSTEM_EVENT (300999)
Header (severity)	Severity	3
cn1	Event ID	- SYSTEM_EVENT 20000-39999 - PRODUCT_UPDATE 10000-19999
cn1Label	Event ID	operationId
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
msg	Event description	Example: Scheduled update - Unable to download Script Analyzer Pattern.
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+00:00

Log sample:

```
CEF:0|Trend Micro|TippingPoint Advanced Threat Protection for
Email|2.5.1.1139|300999|SYSTEM_EVENT|3|rt=Mar 24 2015 08:43:3
5 GMT+00:00 dvcmac=C4:34:6B:B8:09:BC cn3Label=operationId cn3
=30000 msg=Account 'admin' logged on from 10.64.50.147 device
ExternalId=c425624a-e9db-4f3f-8088-2726f15e6587 dvchost=inter
nalbeta.bcc.atp_email dvc=10.64.1.131
```

Chapter 3

Syslog Content Mapping - LEEF

The following tables outline syslog content mapping between TippingPoint Advanced Threat Protection for Email log output and LEEF syslog types:

- *LEEF Detection Logs: Email Detection Logs on page 3-2*
- *LEEF Detection Logs: Attachment Detection Logs on page 3-4*
- *LEEF Detection Logs: URL Detection Logs on page 3-7*
- *LEEF Alert Logs on page 3-10*
- *LEEF Virtual Analyzer Analysis Logs: File Analysis on page 3-13*
- *LEEF Virtual Analyzer Analysis Logs: URL Analysis on page 3-15*
- *LEEF Virtual Analyzer Analysis Logs: Notable Characteristics Events on page 3-17*
- *LEEF Virtual Analyzer Analysis Logs: Deny List Transaction Events on page 3-19*
- *LEEF System Logs on page 3-21*

Note

When using the LEEF log syntax, separate event attributes with \0x09 as a tab delimiter.

LEEF Detection Logs: Email Detection Logs

TABLE 3-1. LEEF Detection Logs: Email Detection Logs

LEEF KEY	DESCRIPTION	VALUE
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventName)	Event Name	EMAIL_DETECTION
act	The action in the event	Examples: • quarantined • passed • stripped • analyzed • stamped • subjectsTagged
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+00:00
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z
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

LEEF Key	Description	Value
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
mailMsgSubject	Email subject	Example: hello
messageId	Email ID	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.atp_email>
msgSize	Email Size	Example: 30841
msgUuid	Internal email ID	Example: 6965222B-13A6-C705-89D4-6251B6C41E03
sev	Severity	• 4: Low • 6: Medium • 8: High
src	Source IP address	Example: 10.1.144.199
suser	Email sender	Example: user2@domain.com
threatName	Names of threats in the email	Example: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS
threatType	Threat type	• 1: Targeted malware • 2: Malware • 3: Malicious URL • 4: Potentially malicious file • 5: Potentially malicious URL

Note

When using the LEEF log syntax, separate event attributes with \0x09 as a tab delimiter.

Log sample:

```
LEEF:1.0|Trend Micro|TippingPoint Advanced Threat Protection
for Email|2.5.1.1161|EMAIL_DETECTION|sev=8\0x09threatType=4\0
```

```
x09deviceGUID=034eb532-9318-40d9-b27b-d9feba7c269e\0x09messag
eId=<20150413072949.E8C0D1E9A363@internalbeta.bcc.atp_email>\
0x09msgUuid=6C4A91D7-1396-1405-94C5-D955018F938E\0x09mailMsgS
ubject=Orcamento Total - 5636005\0x09src=69.162.64.30\0x09msg
Size=397113\0x09dvchost=internalbeta.bcc.atp_email\0x09dvc=10
.64.1.131\0x09act=passed\0x09duser=spam@support.trendmicro.co
m\0x09devTime=Apr 13 2015 07:29:50 GMT+00:00\0x09suser=www-da
ta@contato30.danetmail.net\0x09dvcmac=C4:34:6B:B8:09:BC\0x09d
evTimeFormat=MMM dd yyyy HH:mm:ss z\0x09threatName=VAN_BACKDO
OR.UMXX
```

LEEF Detection Logs: Attachment Detection Logs

TABLE 3-2. LEEF Detection Logs: Attachment Detection Logs

LEEF KEY	DESCRIPTION	VALUE
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventName)	Event Name	ATTACHMENT_DETECTION
act	The action in the event	Examples: • quarantined • passed • stripped • analyzed • stamped • subjectsTagged

LEEF KEY	DESCRIPTION	VALUE
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+00:00
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z
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
emailSeverity	Email severity	• 4: Low • 6: Medium • 8: High
emailThreats	Names of threats in the email	Example: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS
emailThreatType	Threat type	• 1: Targeted malware • 2: Malware • 3: Malicious URL • 4: Potentially malicious file • 5: Potentially malicious URL
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file

LEEF Key	Description	Value
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
mailMsgSubject	Email subject	Example: hello
messageId	Email ID	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.atp_email>
msgSize	Email Size	Example: 30841
msgUuid	Internal email ID	Example: 6965222B-13A6-C705-89D4-6251B6C41E03
sev	Severity	• 4: Low • 6: Medium • 8: High
src	Source IP address	Example: 10.1.144.199
suser	Email sender	Example: user2@domain.com
threatName	Names of threats in the email	Example: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS

Note

When using the LEEF log syntax, separate event attributes with \0x09 as a tab delimiter.

Log sample:

```
LEEF:1.0|Trend Micro|TippingPoint Advanced Threat Protection
for Email|2.5.1.1161|ATTACHMENT_DETECTION|sev=8\0x09msgUuid=6
C4A91D7-1396-1405-94C5-D955018F938E\0x09fileHash=2EF0B334EFDE
7F1BA16011158E25555C2B9D7BC5\0x09emailSeverity=8\0x09suser=ww
w-data@contato30.danetmail.net\0x09dvchost=internalbeta.bcc.d
dei\0x09emailThreatType=4\0x09duser=spam@support.trendmicro.c
om\0x09messageId=<20150413072949.E8C0D1E9A363@internalbeta.bc
```

```
c.atp_email>\0x09src=69.162.64.30\0x09deviceGUID=034eb532-931
8-40d9-b27b-d9feba7c269e\0x09mailMsgSubject=Orcamento Total -
 5636005\0x09msgSize=397113\0x09fileType=Directory\0x09dvc=10
.64.1.131\0x09devTime=Apr 13 2015 15:45:58 GMT+00:00\0x09fnam
e=Orcamento%20Total.zip\0x09act=passed\0x09dvcmac=C4:34:6B:B8
:09:BC\0x09devTimeFormat=MMM dd yyyy HH:mm:ss z\0x09threatNam
e=VAN_BACKDOOR.UMXX\0x09emailThreats=VAN_BACKDOOR.UMXX
```

LEEF Detection Logs: URL Detection Logs

TABLE 3-3. LEEF Detection Logs: URL Detection Logs

LEEF KEY	DESCRIPTION	VALUE
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventName)	Event Name	URL_DETECTION
act	The action in the event	Examples: • quarantined • passed • stripped • analyzed • stamped • subjectsTagged
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536

LEEF KEY	DESCRIPTION	VALUE
deviceProcessHash	Parent SHA1	Example: A29E4ACA70BEF4AF8CE75AF51032B6B91572AA0D
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+00:00
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z
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
eventTriggeredValue	Triggered value	Example: 35
emailSeverity	Email severity	• 4: Low • 6: Medium • 8: High
emailThreats	Names of threats in the email	Example: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS
emailThreatType	Threat type	• 1: Targeted malware • 2: Malware • 3: Malicious URL • 4: Potentially malicious file • 5: Potentially malicious URL
mailMsgSubject	Email subject	Example: hello

LEEF Key	Description	Value
messageId	Email ID	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.atp_email>
msgSize	Email Size	Example: 30841
msgUuid	Internal email ID	Example: 6965222B-13A6-C705-89D4-6251B6C41E03
sev	Severity	• 4: Low • 6: Medium • 8: High
src	Source IP address	Example: 10.1.144.199
suser	Email sender	Example: user2@domain.com
threatName	Names of threats in the email	Example: VAN_MALWARE.UMXX| FRAUD_PHISHING.WRS
url	URL	Example: http://1.2.3.4/query?term=value
urlCat	Category	Example: 90:02

Note

When using the LEEF log syntax, separate event attributes with \0x09 as a tab delimiter.

Log sample:

```
LEEF:1.0|Trend Micro|TippingPoint Advanced Threat Protection
for Email|2.5.1.1161|URL_DETECTION|sev=4\0x09deviceGUID=034eb
532-9318-40d9-b27b-d9feba7c269e\0x09msgUuid=6C4A91D7-1396-140
5-94C5-D955018F938E\0x09mailMsgSubject=Orcamento Total - 5636
005\0x09src=69.162.64.30\0x09emailSeverity=8\0x09msgSize=3971
13\0x09dvchost=internalbeta.bcc.atp_email\0x09dvc=10.64.1.131
\0x09emailThreatType=4\0x09duser=spam@support.trendmicro.com\
0x09url=http://200.98.168.34/testam1/t3zs3.html\0x09act=passe
```

```
d\0x09devTime=Apr 13 2015 15:45:58 GMT+00:00\0x09suser=www-da
ta@contato30.danetmail.net\0x09dvcmac=C4:34:6B:B8:09:BC\0x09d
evTimeFormat=MMM dd yyyy HH:mm:ss z\0x09messageId=<2015041307
2949.E8C0D1E9A363@internalbeta.bcc.atp_email>\0x09emailThreat
s=VAN_BACKDOOR.UMXX
```

LEEF Alert Logs

Table 3-4. LEEF Alert Logs

LEEF Key	Description	Value
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventName)	Event Name	ALERT_EVENT
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+00:00
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
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
eventTriggeredValue	Triggered value	Example: 35
externalId	The logid in the alert database	Example: 1648

LEEF Key	Description	Value
ruleContent	Notification content	Example: The following email messages contain threats: Risk: Medium (Malware) Action: Quarantined Message ID: <20150619032243.5923E650365@localhost.atp_email-164> Recipients: fake@test.com;test@test.com Sender: test@fake.test Subject: high_4_file_507ECC33FA60979F6B97D84DA47972096185C263 Attachment: 4_file_507ECC33FA60979F6B97D84DA47972096185C263 (MIME Base64) Detected: 2015-05-25 11:11:00 Alert time: 2015-05-25 11:11:27 +0800 Generated by: localhost.localdomain (192.168.1.100) Management console: https://192.168.1.100/loginPage.ddei **Note** The maximum length is 20000 characters.
ruleCriteria	Description	Example: 1 or more messages detected with threats

LEEF KEY	DESCRIPTION	VALUE
ruleEventType	Alert type	• 0: System event • 1: Security event and the event severity is "High", "Medium", or "Low" • 2: Security event and the even severity is "High", or "Medium" • 3: Security event and the event severity is "High"
ruleId	Alert ID	Value between 1 and 15
ruleName	Alert name	Example: Security: Suspicious Messages Identified
sev	Severity	• 2: Informational • 6: Important • 8: Critical

Note

When using the LEEF log syntax, separate event attributes with \0x09 as a tab delimiter.

Log sample:

```
LEEF:1.0|Trend Micro|TippingPoint Advanced Threat Protection
for Email|2.5.1.1009|ALERT_EVENT|sev=2\0x09cnt=8\0x09ruleEven
tType=0\0x09ruleId=10\0x09ruleCriteria=At least 1 messages pr
ocessed\0x09dvchost=localhost.atp_email-164\0x09dvc=10.204.25
3.164\0x09deviceGUID=361a091c-addd-40cf-98e7-710e43500a66\0x0
9externalId=1684\0x09devTime=Jun 19 2015 03:18:48 GMT+00:00\0
x09ruleName=System: Processing Surge\0x09dvcmac=00:50:56:01:2
C:BC\0x09devTimeFormat=MMM dd yyyy HH:mm:ss z\0x09ruleContent
=The%20number%20of%20processed%20messages%20reached%20the%20s
pecified%20threshold%20%281%29.%0A%0AMessages%20processed%3A%
208%0AChecking%20interval%3A%200%20minutes%0A%0AAlert%20time%
3A%202015-06-19%2003%3A18%3A48%20%2B0000%0AGenerated%20by%3A%
```

```
20localhost.atp_email-164%20%2810.204.253.164%29%0AManagement
%20console%3A%20https%3A//10.204.253.164/loginPage.ddei
```

LEEF Virtual Analyzer Analysis Logs: File Analysis

Table 3-5. LEEF Virtual Analyzer Analysis Logs: File Analysis

LEEF Key	Description	Value
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventName)	Event Name	FILE_ANALYZED
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:56:B3:57
deviceOSName	Sandbox image type	Example: win7
deviceProcessHash	Parent SHA1	Example: A29E4ACA70BEF4AF8CE75AF51032B6B91572AA0D
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+00:00
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost

LEEF Key	Description	Value
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
gridIsKnownGood	Result of GRID/CSSS	• 0: GRID is not known good • 1: GRID is known good
malName	Malware name	Example: HEUR_NAMETRICK.A
pcapReady	PCAP ready	• 0: PCAP is not ready • 1: PCAP is ready
pComp	Detection engine / component	Sandbox
rozRating	ROZ rating	Example: 3: High risk
sev	Severity	3

Note

When using the LEEF log syntax, separate event attributes with \0x09 as a tab delimiter.

Log sample:

```
LEEF:1.0|Trend Micro|TippingPoint Advanced Threat Protection
for Email|2.5.1.1161|FILE_ANALYZED|devTime=Apr 13 2015 07:45:
54 GMT+00:00\0x09devTimeFormat=MMM dd yyyy HH:mm:ss z\0x09sev
=3\0x09pComp=Sandbox\0x09dvc=10.64.1.131\0x09dvchost=internal
beta.bcc.atp_email\0x09deviceMacAddress=C4:34:6B:B8:09:BC\0x0
9deviceGUID=034eb532-9318-40d9-b27b-d9feba7c269e\0x09fname=Or
\x87amento Total.cpl\0x09fileHash=2EF0B334EFDE7F1BA16011158E2
5555C2B9D7BC5\0x09deviceProcessHash=61DD815ABF2D1FFC58F261392
DAFF4F11B59D79C\0x09malName=VAN_BACKDOOR.UMXX\0x09fileType=Wi
```

```
n32 DLL\0x09fsize=482816\0x09deviceOSName=win81en\0x09gridIsK
nownGood=-1\0x09rozRating=3\0x09pcapReady=1
```

LEEF Virtual Analyzer Analysis Logs: URL Analysis

TABLE 3-6. LEEF Virtual Analyzer Analysis Logs: URL Analysis

LEEF KEY	DESCRIPTION	VALUE
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventName)	Event Name	URL_ANALYZED
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceOSName	Sandbox image type	Example: win7
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:56:B3:57
deviceProcessHash	Parent SHA1	Example: A29E4ACA70BEF4AF8CE75AF51032B6B91572AA0D
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+00:00
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost

LEEF Key	Description	Value
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
pcapReady	PCAP ready	• 0: PCAP is not ready • 1: PCAP is ready
pComp	Detection engine / component	Sandbox
rozRating	ROZ rating	Example: 3: High risk
sev	Severity	3
url	URL	Example: http://1.2.3.4/query?term=value

Note

When using the LEEF log syntax, separate event attributes with \0x09 as a tab delimiter.

Log sample:

```
LEEF:1.0|Trend Micro|TippingPoint Advanced Threat Protection
for Email|2.5.1.1161|URL_ANALYZED|devTime=Apr 13 2015 07:34:4
1 GMT+00:00\0x09devTimeFormat=MMM dd yyyy HH:mm:ss z\0x09sev=
3\0x09pComp=Sandbox\0x09dvc=10.64.1.131\0x09dvchost=internalb
eta.bcc.atp_email\0x09deviceMacAddress=C4:34:6B:B8:09:BC\0x09
deviceGUID=034eb532-9318-40d9-b27b-d9feba7c269e\0x09fileHash=
BF6852C834224BD2C26AC4BE20E7E08930B39FEF\0x09deviceOSName=win
7sp1en\0x09url=http://climtorg.ru/bitrix/admin/1up\0x09rozRat
ing=3\0x09pcapReady=1
```

LEEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

TABLE 3-7. LEEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

LEEF KEY	DESCRIPTION	VALUE
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventName)	Event Name	NOTABLE_CHARACTERISITICS
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:56:B3:57
deviceOSName	Sandbox image type	Example: win7
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+00:00
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372

LEEF Key	Description	Value
msg	Details	Example: msg=Dropping Process ID: 2984\n File: %USERPROFILE%\AppData\Local\MICROSOFT\INTERNET EXPLORER\Recovery\High\LAST ACTIVE\{D78424A0 E1AA-11E4-B7C5-7CC9C8DA4AD 2}.DAT\nType: VSDT_WINWORD\
pComp	Detection engine / component	Sandbox
ruleCategory	Violated policy name	Example: Internet Explorer Setting Modification
ruleName	Violated event analysis	Example: Modified important registry items
sev	Severity	3

Note

When using the LEEF log syntax, separate event attributes with \0x09 as a tab delimiter.

Log sample:

```
LEEF:1.0|Trend Micro|TippingPoint Advanced Threat Protection
for Email|2.5.1.1161|NOTABLE_CHARACTERISTICS|devTime=Apr 13
2015 07:01:13 GMT+00:00\0x09devTimeFormat=MMM dd yyyy HH:mm:s
s z\0x09sev=6\0x09pComp=Sandbox\0x09dvc=10.64.1.132\0x09dvcho
st=internalbeta.tapping.atp_email\0x09deviceMacAddress=B0:83:
FE:DD:21:98\0x09deviceGUID=e57f0651-b197-42d4-a643-271c1277b5
ff\0x09fname=http://yt1nutj.wvp78.com/\0x09fileHash=8213271FD
287C3F27D6975FE0545AB77DC8EBF73\0x09fileType=URL\0x09fsize=0\
0x09ruleCategory=File drop, download, sharing, or replication
\0x09ruleName=Drops file that can be used to infect systems\0
x09msg=Dropping Process ID: 2984\nFile: %USERPROFILE%\AppData
\Local\MICROSOFT\INTERNET EXPLORER\Recovery\High\LAST ACTIVE\
{D78424A0-E1AA-11E4-B7C5-7CC9C8DA4AD2}.DAT\nType: VSDT_WINWOR
D\0x09deviceOSName=win7sp1en
```

LEEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

TABLE 3-8. LEEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

LEEF KEY	DESCRIPTION	VALUE
Header (logVer)	LEEF format version	LEEF: 1.0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventName)	Event Name	DENYLIST_CHANGE
act	The action in the event	• Add • Remove
deviceExternalRiskType	Risk level	• Low • Medium • High • Confirmed Malware
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:56:B3:57
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+00:00
devTimeFormat	Time format	MMM dd yyyy HH:mm:ss z
dhost	Destination host name	Example: dhost1
dpt	Destination port	Value between 0 and 65535
dst	Destination IP address	Example: 10.1.144.199

LEEF Key	Description	Value
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
end	Report end time	Example: Mar 09 2015 17:05:21 GMT+00:00
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
pComp	Detection engine / component	Sandbox
sev	Severity	3
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/query?term=value

Note

When using the LEEF log syntax, separate event attributes with \0x09 as a tab delimiter.

Log sample:

```
LEEF:1.0|Trend Micro|TippingPoint Advanced Threat Protection
for Email|2.5.1.1161|DENYLIST_CHANGE|devTime=Apr 13 2015 07:4
7:01 GMT+00:00\0x09devTimeFormat=MMM dd yyyy HH:mm:ss z\0x09s
ev=3\0x09pComp=Sandbox\0x09dvc=10.64.1.131\0x09dvchost=intern
albeta.bcc.atp_email\0x09deviceMacAddress=C4:34:6B:B8:09:BC\0
x09deviceGUID=034eb532-9318-40d9-b27b-d9feba7c269e\0x09end=Ma
y 13 2015 07:44:37 GMT+00:00\0x09act=Add\0x09dst=200.98.168.3
4\0x09dpt=80\0x09deviceExternalRiskType=Medium\0x09type=Deny
List IP/Port
```

LEEF System Logs

TABLE 3-9. 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	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventName)	Event Name	PRODUCT_UPDATE SYSTEM_EVENT
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
devTime	Log generation time	Example: Jan 28 2015 02:00:36 GMT+00:00
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
dvcmac	Appliance MAC address	Example: 00:0C:29:6E:CB:F9
msg	Event description	Example: Scheduled update - Unable to download Script Analyzer Pattern.
operationId	Event ID	• SYSTEM_EVENT 20000-39999 • PRODUCT_UPDATE 10000-19999
sev	Severity	3

Note

When using the LEEF log syntax, separate event attributes with \0x09 as a tab delimiter.

Log sample:

```
LEEF:1.0|Trend Micro|TippingPoint Advanced Threat Protection
for Email|2.5.1.1161|SYSTEM_EVENT|sev=3\0x09deviceGUID=e57f06
51-b197-42d4-a643-271c1277b5ff\0x09devTime=Apr 13 2015 06:52:
00 GMT+00:00\0x09msg=Logout: 'admin' logged off\0x09dvcmac=B0
:83:FE:DD:21:98\0x09devTimeFormat=MMM dd yyyy HH:mm:ss z\0x09
dvchost=internalbeta.tapping.atp_email\0x09dvc=10.204.253.163
\0x09operationId=30000
```

Chapter 4

Syslog Content Mapping - TMEF

The following tables outline syslog content mapping between TippingPoint Advanced Threat Protection for Email log output and TMEF syslog types:

- *TMEF Detection Logs: Email Detection Logs on page 4-2*
- *TMEF Detection Logs: Attachment Detection Logs on page 4-4*
- *TMEF Detection Logs: URL Detection Logs on page 4-7*
- *TMEF Alert Logs on page 4-10*
- *TMEF Virtual Analyzer Analysis Logs: File Analysis Events on page 4-13*
- *TMEF Virtual Analyzer Analysis Logs: URL Analysis Events on page 4-15*
- *TMEF Virtual Analyzer Analysis Logs: Notable Characteristics Events on page 4-17*
- *TMEF Virtual Analyzer Analysis Logs: Deny List Transaction Events on page 4-19*
- *TMEF System Logs on page 4-21*

TMEF Detection Logs: Email Detection Logs

TABLE 4-1. TMEF Detection Logs: Email Detection Logs

TMEF KEY	DESCRIPTION	VALUE
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	100130
Header (eventName)	Description	EMAIL_DETECTION
Header (severity)	Email severity	• 4: Low • 6: Medium • 8: High
act	The action in the event	Examples: • quarantined • passed • stripped • analyzed • stamped • subjectsTagged
cn1	Email Size	Example: 30841
cn1Label	Email Size	msgSize
cs1	Internal email ID	Example: 6965222B-13A6-C705-89D4-6251B6C41E03
cs1Label	Internal email ID	msgUuid

TMEF KEY	DESCRIPTION	VALUE
cs2	Email ID	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.atp_email>
cs2Label	Email ID	messageId
deviceGUID	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
mailMsgSubject	Email subject	Example: hello
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+00:00
src	Source IP address	Example: 10.1.144.199
suser	Email sender	Example: user2@domain.com
threatName	Names of threats in the email	Example: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS
threatType	Threat type	• 1: Targeted malware • 2: Malware • 3: Malicious URL • 4: Potentially malicious file • 5: Potentially malicious URL

Log sample:

```
CEF:0|Trend Micro|TippingPoint Advanced Threat Protection for
 Email|2.5.1.1161|100130|EMAIL_DETECTION|8|rt=Apr 13 2015 08:
49:22 GMT+00:00 src=141.251.58.19 threatType=4 deviceGUID=034
eb532-9318-40d9-b27b-d9feba7c269e mailMsgSubject=phishwatch D
igest, Vol 2933, Issue 13 act=passed dvchost=internalbeta.bcc
.atp_email cs2Label=messageId cs2=<20150413084922.2052D1E9A06
6@internalbeta.bcc.atp_email dvc=10.64.1.131 cs1Label=msgUuid
 cs1=ECBC7B7E-1397-3005-94C5-0BA1DA0913D2 duser=act@jnsa.org
suser=jnsa-act-admin@jnsa.org dvcmac=C4:34:6B:B8:09:BC threat
Name=VAN_MALWARE.UMXX cn1Label=msgSize cn1=1204948
```

TMEF Detection Logs: Attachment Detection Logs

Table 4-2. TMEF Detection Logs: Attachment Detection Logs

TMEF Key	Description	Value
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	100131
Header (eventName)	Description	ATTACHMENT_DETECTION
Header (severity)	Attachment severity	• 4: Low • 6: Medium • 8: High

TMEF Key	Description	Value
act	The action in the event	Examples: • quarantined • passed • stripped • analyzed • stamped • subjectsTagged
cn1	Email severity	• 4: Low • 6: Medium • 8: High
cn1Label	Email severity	emailSeverity
cn2	Email Size	Example: 30841
cn2Label	Email Size	msgSize
cn3	Threat type	• 1: Targeted malware • 2: Malware • 3: Malicious URL • 4: Potentially malicious file • 5: Potentially malicious URL
cn3Label	Threat type	emailThreatType
cs1	Names of threats in the email	Example: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS
cs1Label	Names of threats in the email	emailThreats
cs2	Internal email ID	Example: 6965222B-13A6-C705-89D4-6251B6C41E03

TMEF Key	Description	Value
cs2Label	Internal email ID	msgUuid
cs3	Email ID	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.atp_email>
cs3Label	Email ID	messageId
deviceGUID	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
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
mailMsgSubject	Email subject	Example: hello
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+00:00
src	Source IP address	Example: 10.1.144.199
suser	Email sender	Example: user2@domain.com
threatName	Names of threats in the email	Example: VAN_MALWARE.UMXX| FRAUD_PHISHING.WRS

Log sample:

```
CEF:0|Trend Micro|TippingPoint Advanced Threat Protection for
 Email|2.5.1.1161|100131|ATTACHMENT_DETECTION|8|rt=Apr 13 201
5 16:58:22 GMT+00:00 src=141.251.58.19 cs3Label=messageId cs3
=<20150413084922.2052D1E9A066@internalbeta.bcc.atp_mail cn1La
bel=emailSeverity cn1=8 mailMsgSubject=phishwatch Digest, Vol
 2933, Issue 13 fileHash=E07B349245FCDDB31CBF5A52012807E955D2
EB7A fileType=Directory act=passed dvchost=internalbeta.bcc.a
tp_email dvc=10.64.1.131 deviceGUID=034eb532-9318-40d9-b27b-d
9feba7c269e duser=act@jnsa.org cn2Label=msgSize cn2=1204948 c
n3Label=emailThreatType cn3=4 fname=JNSA%20CSIRT-%E3%82%AA%E3
%83%AA%E3%83%91%E3%83%A9.pdf suser=jnsa-act-admin@jnsa.org dv
cmac=C4:34:6B:B8:09:BC cs1Label=emailThreats cs1=VAN_MALWARE.
UMXX threatName=VAN_MALWARE.UMXX cs2Label=msgUuid cs2=ECBC7B7
E-1397-3005-94C5-0BA1DA0913D2
```

TMEF Detection Logs: URL Detection Logs

TABLE 4-3. TMEF Detection Logs: URL Detection Logs

TMEF KEY	DESCRIPTION	VALUE
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	100132
Header (eventName)	Description	URL_DETECTION
Header (severity)	URL severity	• 4: Low • 6: Medium • 8: High

TMEF KEY	DESCRIPTION	VALUE
act	The action in the event	Examples: • quarantined • passed • stripped • analyzed • stamped • subjectsTagged
cn1	Email severity	• 4: Low • 6: Medium • 8: High
cn1Label	Email severity	emailSeverity
cn2	Email Size	Example: 30841
cn2Label	Email Size	msgSize
cn3	Threat type	• 1: Targeted malware • 2: Malware • 3: Malicious URL • 4: Potentially malicious file • 5: Potentially malicious URL
cn3Label	Threat type	emailThreatType
cs1	Names of threats in the email	Example: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS
cs1Label	Names of threats in the email	emailThreats
cs2	Internal email ID	Example: 6965222B-13A6-C705-89D4-6251B6C41E03

TMEF Key	Description	Value
cs2Label	Internal email ID	msgUuid
cs3	Email ID	Example: <20150414032514.494EF1E9A365@internalbeta.bcc.atp_email>
cs3Label	Email ID	messageId
deviceGUID	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
mailMsgSubject	Email subject	Example: hello
request	URL	Example: http://www.rainking.net/?utm_campaign=4-21-2014 |http://images.rainking.net/eloquaimage
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+00:00
src	Source IP address	Example: 10.1.144.199
suser	Email sender	Example: user2@domain.com
threatName	Names of threats in the email	Example: VAN_MALWARE.UMXX|FRAUD_PHISHING.WRS
urlCat	Category	Example: 90:02

Log sample:

```
CEF:0|Trend Micro|TippingPoint Advanced Threat Protection for
 Email|2.5.1.1161|100132|URL_DETECTION|6|rt=Apr 13 2015 16:5
:22 GMT+00:00 src=141.251.58.19 cs3Label=messageId cs3=<20150
413084922.2052D1E9A066@internalbeta.bcc.atp_email cn1Label=em
ailSeverity cn1=8 mailMsgSubject=phishwatch Digest, Vol 2933,
 Issue 13 request=http://202.502.27.71:6610/ctldl.windowsupda
te.com/msdownload/update/v3/static/trustedr/en/disallowedcert
stl.cab?7f8b3bbc9534919b?7f8b3bbc9534919b act=passed dvchost=
internalbeta.bcc.atp_email dvc=10.64.1.131 duser=act@jnsa.org
 cn2Label=msgSize cn2=1204948 cn3Label=emailThreatType cn3=4
suser=jnsa-act-admin@jnsa.org dvcmac=C4:34:6B:B8:09:BC cs1Lab
el=emailThreats cs1=VAN_MALWARE.UMXX deviceGUID=034eb532-9318
-40d9-b27b-d9feba7c269e cs2Label=msgUuid cs2=ECBC7B7E-1397-30
05-94C5-0BA1DA0913D2
```

TMEF Alert Logs

TABLE 4-4. TMEF Alert Logs

TMEF KEY	DESCRIPTION	VALUE
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	300105
Header (eventName)	Description	ALERT_EVENT
Header (severity)	Alert severity	• 2: Informational • 6: Important • 8: Critical

TMEF KEY	DESCRIPTION	VALUE
cn1	Alert type	• 0: System event • 1: Security event and the event severity is "High", "Medium", or "Low" • 2: Security event and the even severity is "High", or "Medium" • 3: Security event and the event severity is "High"
cn1Label	Alert type	ruleEventType
cs1	Description	Example: 1 or more messages detected with threats
cs1Label	Description	ruleCriteria
cs2	Triggered value	Example: 35
cs2Label	Triggered value	eventTriggeredValue

TMEF KEY	DESCRIPTION	VALUE

cs3	Notification content	Example:
		`The following`
		` email messages contain`
		`threats:`
		
		`Risk: Medium (Malware)`
		`Action:  Quarantined`
		`Message ID: <201506190`
		`32243.5923E650365@loca`
		`lhost.at0_email-164>`
		`Recipients: fake@test.`
		`com;test@test.com`
		`Sender: test@fake.test`
		`Subject: high_4_file_`
		`507ECC33FA60979F6B97D`
		`84DA47972096185C263`
		`Attachment: 4_file_50`
		`7ECC33FA60979F6B97D84`
		`DA47972096185C263 (MIME`
		` Base64)`
		`Detected: 2015-05-25`
		`11:11:00`
		
		`Alert time: 2015-05-25`
		`11:11:27 +0800`
		Note
		The maximum length is 20000 characters.

cs3Label	Notification content	ruleContent
deviceGUID	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

TMEF Key	Description	Value
externalId	The logid in the alert database	Example: 1648
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+00:00
ruleId	Alert ID	Value between 1 and 15
ruleName	Alert name	Example: Security: Suspicious Messages Identified

Log sample:

```
CEF:0|Trend Micro|TippingPoint Advanced Threat Protection for
 Email|2.5.1.1009|300105|ALERT_EVENT|2|rt=Jun 19 2015 03:22:5
8 GMT+00:00 cnt=7 deviceGUID=361a091c-addd-40cf-98e7-710e4350
0a66 ruleId=10 cs2Label=ruleContent cs2=The%20number%20of%20p
rocessed%20messages%20reached%20the%20specified%20threshold%2
0%281%29.%0A%0AMessages%20processed%3A%207%0AChecking%20inter
val%3A%200%20minutes%0A%0AAlert%20time%3A%202015-06-19%2003%3
A22%3A58%20%2B0000%0AGenerated%20by%3A%20localhost.atp_email-
164%20%2810.204.253.164%29%0AManagement%20console%3A%20https%
3A//10.204.253.164/loginPage.ddei cs1Label=ruleCriteria cs1=A
t least 1 messages processed dvchost=localhost.atp_email-164
dvc=10.204.253.164 externalId=1694 ruleName=System: Processin
g Surge dvcmac=00:50:56:01:2C:BC cn1Label=ruleEventType cn1=0
```

TMEF Virtual Analyzer Analysis Logs: File Analysis Events

Table 4-5. TMEF Virtual Analyzer Analysis Logs: File Analysis Events

TMEF Key	Description	Value
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro

TMEF Key	Description	Value
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	200119
Header (eventName)	Description	FILE_ANALYZED
Header (severity)	Severity	3
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
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:56:B3:57
deviceOSName	Sandbox image type	Example: win7
deviceProcessHash	Parent SHA1	Example: A29E4ACA70BEF4AF8CE75AF51032B6B91572AA0D
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost

TMEF Key	Description	Value
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
malName	Malware name	Example: HEUR_NAMETRICK.A
pComp	Detection engine / component	Sandbox
rt	Analysis time	Example: Mar 09 2015 17:05:21 GMT+00:00

Log sample:

```
CEF:0|Trend Micro|TippingPoint Advanced Threat Protection for
 Email|2.5.1.1161|200119|FILE_ANALYZED|3|rt=Apr 13 2015 08:58
:20 GMT+00:00 pComp=Sandbox dvc=10.64.1.131 dvchost=internalb
eta.bcc.atp_email deviceMacAddress=C4:34:6B:B8:09:BC deviceGU
ID=034eb532-9318-40d9-b27b-d9feba7c269e fname=JNSA CSIRT-exam
ple.pdf fileHash=E07B349245FCDDB31CBF5A52012807E955D2EB7A mal
Name=VAN_MALWARE.UMXX fileType=Adobe Portable Document Format
(PDF) fsize=875029 deviceOSName=win81en cn1Label=GRIDIsKnownG
ood cn1=-1 cn2Label=ROZRating cn2=3 cn3Label=PcapReady cn3=1
```

TMEF Virtual Analyzer Analysis Logs: URL Analysis Events

Table 4-6. TMEF Virtual Analyzer Analysis Logs: URL Analysis Events

TMEF Key	Description	Value
Header (logVer)	TMEF format version	CEF: 0

TMEF Key	Description	Value
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	200126
Header (eventName)	Description	URL_ANALYZED
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
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:56:B3:57
deviceOSName	Sandbox image type	Example: win7
deviceProcessHash	Parent SHA1	Example: A29E4ACA70BEF4AF8CE75AF51032B6B91572AA0D
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3

TMEF Key	Description	Value
pComp	Detection engine / component	Sandbox
request	URL	Example: http://www.rainking.net/?utm_campaign=4-21-2014 |http://images.rainking.net/eloquaimage
rt	Analysis time	Example: Mar 09 2015 17:05:21 GMT+00:00

Log sample:

```
CEF:0|Trend Micro|TippingPoint Advanced Threat Protection for
 Email|2.5.1.1161|200126|URL_ANALYZED|3|rt=Apr 13 2015 08:24:
46 GMT+00:00 pComp=Sandbox dvc=10.64.1.131 dvchost=internalbe
ta.bcc.ato_email deviceMacAddress=C4:34:6B:B8:09:BC deviceGUI
D=034eb532-9318-40d9-b27b-d9feba7c269e request=http://www.cas
telir.it/take/Small-9422.html fileHash=6389250B8468C46443FD77
5F6EB744D6105B8DF3 deviceOSName=xpsp3en cn2Label=ROZRating cn
2=3 cn3Label=PcapReady cn3=1
```

TMEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

Table 4-7. TMEF Virtual Analyzer Analysis Logs: Notable Characteristics Events

TMEF Key	Description	Value
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161

TMEF Key	Description	Value
Header (eventid)	Signature ID	200127
Header (eventName)	Description	NOTABLE_CHARACTERISITICS
Header (severity)	Severity	6
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:56:B3:57
deviceOSName	Sandbox image type	Example: win7
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
fileType	True file type	Example: RIFF bitmap file
fname	File name	Example: excel.rar
fsize	File size	Example: 131372
msg	Details	Example: s1.bdstatic.com
pComp	Detection engine / component	Sandbox
rt	Analysis time	Example: Mar 09 2015 17:05:21 GMT+00:00
ruleCategory	Violated policy name	Example: Internet Explorer Setting Modification
ruleName	Violated event analysis	Example: Modified important registry items

Log sample:

```
CEF:0|Trend Micro|TippingPoint Advanced Threat Protection for
 Email|2.5.1.1161|200127|NOTABLE_CHARACTERISTICS|6|rt=Apr 13
2015 08:24:46 GMT+00:00 pComp=Sandbox dvc=10.64.1.131 dvchost
=internalbeta.bcc.atp_email deviceMacAddress=C4:34:6B:B8:09:B
C deviceGUID=034eb532-9318-40d9-b27b-d9feba7c269e fname=http:
//www.castelir.it/take/Small-9422.html fileHash=6389250B8468C
46443FD775F6EB744D6105B8DF3 fileType=URL fsize=0 ruleCategory
=Suspicious network or messaging activity ruleName=Queries DN
S server msg=s1.bdstatic.com deviceOSName=xpsp3en
```

TMEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

Table 4-8. TMEF Virtual Analyzer Analysis Logs: Deny List Transaction Events

TMEF Key	Description	Value
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	200120
Header (eventName)	Description	DENYLIST_CHANGE
Header (severity)	Severity	3
act	The action in the event	• Add • Remove

TMEF Key	Description	Value
cs1	Deny List type	• Deny List IP/Port • Deny List URL • Deny List File SHA1 • Deny List Domain
cs1Label	Deny List type	type
deviceExternalRiskType	Risk level	• 1: Low • 2: Medium • 3: High • 4: Confirmed Malware
deviceGUID	Appliance GUID	Example: 6B593E17AFB7-40FBBB28-A4CE-0462-A536
deviceMacAddress	Appliance MAC address	Example: 00:0C:29:56:B3:57
dhost	Destination host name	Example: dhost1
dpt	Destination port	Value between 0 and 65535
dst	Destination IP address	Example: 10.1.144.199
dvc	Appliance IP address	Example: 10.1.144.199
dvchost	Appliance host name	Example: localhost
end	Report end time	Example: Mar 09 2015 17:05:21 GMT+00:00
fileHash	SHA1	Example: 1EDD5B38DE4729545767088C5CAB395E4197C8F3
pComp	Detection engine / component	Sandbox

TMEF Key	Description	Value
request	URL	Example: http://www.rainking.net/?utm_campaign=4-21-2014 |http://images.rainking.net/eloquaimage
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+00:00

Log sample:

```
CEF:0|Trend Micro|TippingPoint Advanced Threat Protection for
 Email|2.5.1.1161|200120|DENYLIST_CHANGE|3|rt=Apr 14 2015 10:
25:24 GMT+00:00 pComp=Sandbox dvc=10.64.1.131 dvchost=interna
lbeta.bcc.atp_email deviceMacAddress=C4:34:6B:B8:09:BC device
GUID=034eb532-9318-40d9-b27b-d9feba7c269e cs1Label=type cs1=D
eny List File SHA1 end=May 14 2015 09:59:20 GMT+00:00 act=Add
 fileHash=522A90D077884E880A454A4D8E1A315FCE36BB12 deviceExte
rnalRiskType=High
```

TMEF System Logs

Table 4-9. TMEF System Logs

TMEF Key	Description	Value
Header (logVer)	TMEF format version	CEF: 0
Header (vendor)	Appliance vendor	Trend Micro
Header (pname)	Appliance product	TippingPoint Advanced Threat Protection for Email
Header (pver)	Appliance version	Example: 2.5.1.1161
Header (eventid)	Signature ID	• 300102 (PRODUCT_UPDATE) • 300999 (SYSTEM_EVENT)

TMEF KEY	DESCRIPTION	VALUE
Header (eventName)	Description	- PRODUCT_UPDATE (300102) - SYSTEM_EVENT (300999)
Header (severity)	Severity	3
cn1	Event ID	- SYSTEM_EVENT 20000-39999 - PRODUCT_UPDATE 10000-19999
cn1Label	Event ID	operationId
deviceGUID	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
msg	Event description	Example: Scheduled update - Unable to download Script Analyzer Pattern.
rt	Log generation time	Example: Mar 09 2015 17:05:21 GMT+00:00

Log sample:

```
CEF:0|Trend Micro|TippingPoint Advanced Threat Protection for
 Email|2.5.1.1161|300999|SYSTEM_EVENT|3|rt=Apr 13 2015 09:31:
08 GMT+00:00 dvcmac=C4:34:6B:B8:09:BC deviceGUID=034eb532-931
8-40d9-b27b-d9feba7c269e cn1Label=operationId cn1=30000 msg=L
ogin: 'admin' logged on from 10.204.253.21 dvchost=internalbe
ta.bcc.atp_email dvc=10.204.253.163
```

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: APEM27714/170215