TREND MICRO™

2.2 TREND MICRO™ Deep Discovery Web Inspector

Syslog Content Mapping Guide

Advanced Protection Against Targeted Web Attacks

Endpoint Security

Network Security

Protected Cloud

Document Part No.: APEM28502/181003

Release Date: May 2019

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

Preface

Topics include:

Documentation

The documentation set for Deep Discovery Web Inspector includes the following:

TABLE 1. Product Documentation

DOCUMENT	DESCRIPTION
Administrator's Guide	PDF documentation provided with the product or downloadable from the Trend Micro website. The Administrator's Guide contains detailed instructions on how to deploy, configure, and manage Deep Discovery Web Inspector, and provides explanations on Deep Discovery Web Inspector concepts and features.
Installation and Deployment Guide	PDF documentation provided with the product or downloadable from the Trend Micro website. The Installation and Deployment Guide discusses requirements and procedures for installing and deploying Deep Discovery Web Inspector.
Syslog Content Mapping Guide	The Syslog Content Mapping Guide contains information on event logging formats supported by Deep Discovery Web Inspector.
Quick Start Card	The Quick Start Card provides user-friendly instructions on connecting Deep Discovery Web Inspector to your network and on performing the initial configuration.
Readme	The Readme contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, known issues, and product release history.
Online Help	Web-based documentation that is accessible from the Deep Discovery Web Inspector management console. The Online Help contains explanations of Deep Discovery Web Inspector components and features, as well as procedures needed to configure Deep Discovery Web Inspector.

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 Deep Discovery Web Inspector documentation from the Trend Micro Documentation Center:

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

Audience

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

- Network topologies
- Policy management and enforcement

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

CONVENTION	DESCRIPTION
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

Chapter 1

Introduction

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

To enable flexible integration with third-party log management systems, Deep Discovery Web Inspector 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 Web Inspector 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 Web Inspector uses a subset of the LEEF dictionary.
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 Deep Discovery Web Inspector.

Syslog Events

Deep Discovery Web Inspector supports the violation syslog log type (logType 6).

List of Threat Indicators

Each syslog entry lists one of the following threat indicators and the corresponding signature ID for the violation identified in the log entry.

The threat indicator name and signature ID are displayed under the header information of each syslog entry. For example, a CEF-format header similar to the following is displayed for a Ransomware threat indicator:

```
CEF:0|Trend Micro|Deep Discovery Web
      Inspector|2.2.0.1105|100001|Ransomware|3|
```

TABLE 1-1. Violation Threat Indicators

THREAT INDICATOR NAME	SIGNATURE ID
Ransomware	100001
C&C Callbacks	100002
Suspicious Malware	100003
Suspicious URLs	100004
Suspicious Documents	100005
Suspicious Scripts	100006
Coin Miners	100007
Other All other detections not belonging to advanced detections, for example, detections of known malware or by Web Reputation Service.	100000

List of Detection Types

The following detection types can be displayed under the **detectionType** field in the violation log. The description for each detection type provides more information about what each code means.

DETECTIONTYPE CODES	DESCRIPTION
0	No match to any rule
2	Untrusted Server Certificate
10	Approved URLs / Blocked URLs
11	Temporary Blocked URLs
20	Web Reputation Service
21	URL Filtering
30	True File Type
40	Anti-Malware (ATSE)
42	Anti-Malware (SIE)
43	Anti-Malware (SAL)
45	Predictive Machine Learning (TRX)
50	Anti-Botnet
70	Suspicious Objects Analysis (Virtual Analyzer)
90	Suspicious Objects Filtering (Virtual Analyzer)

Supported Log Formats

TERM	DESCRIPTION
CEF	Common Event Format

TERM	DESCRIPTION
LEEF	Log Event Extended Format
TMEF	Trend Micro Event Format

Change History

The following table provides the change history for this document.

VERSION	DESCRIPTION
1.0/2.0	First release
2.2	Second release

Chapter 2

Syslog Content Mapping - CEF

The following topics outline syslog content mapping between Deep Discovery Web Inspector log output and the CEF syslog type:

CEF Violation Logs

TABLE 2-1. CEF Violation Logs

CEF KEY	DESCRIPTION	VALUE
Header(logVer)	CEF format version	CEF: 0
Header(vendor)	Appliance vendor	Trend Micro
Header(pname)	Appliance product	Deep Discovery Web Inspector
Header(pver)	Appliance version	Example: 2.2.0.1105
Header(eventid)	Signature ID	Example: 100001
Header(eventName)	Description	Example: Ransomware
Header(severity)	Risk level	• 0: user defined • 1: low • 2: medium • 3: high • 4: potential threat risk
rt	UTC timestamp	Example: Oct 20 2017 17:15:57 GMT+00:00
logType	Log type	6: Violation Log
companyId	Company ID	Reserved, value is default
adDomain	AD domain	Active Directory domain information Example: trendnet.org
userName	Client IP	Example: 10.204.171.200
groupName	Group name	Active Directory group name information

CEF KEY	DESCRIPTION	VALUE
department	Department	Active Directory department information Example: commercial
device	Device	Reserved, default null
act	Action	Can be one of the following values: • allow • monitor • block • analyze
app	Protocol channel	• 1: HTTP • 2: HTTPS • 3: HTTP2 • 4: FTP
tlsVersion	TLS version	• 0: None TLS • 1: SSLv3 • 2: TLSv1.0 • 3: TLSv1.1 • 4: TLSv1.2
size	Transport bytes by Deep Discovery Web Inspector, unit bytes	Example: 15
dst	Destination IP address of request	Example: 54.148.125.151
src	Source IP address of request	Example: 10.204.171.200

CEF KEY	DESCRIPTION	VALUE
upstreamSize	The upstream payload from Deep Discovery Web Inspector to server, unit bytes	Example: 54
downstreamSize	The downstream payload from server to Deep Discovery Web Inspector, unit bytes	Example: 49
domain	Domain	Example: ca95-1.winshipway.com
detectionType	Detection type	For a description of each type, see *List of Detection Types on page 1-3*
detectionSubType	Detection sub-type	Reserved, default 0
threatType	Threat type	• 1: Ransomware • 2: C&C Callback • 3: Suspicious Malware • 4: Suspicious URLs • 5: Suspicious Documents • 6: Suspicious Scripts • 7: Malicious URL • 8: Malicious Content • 9: Suspicious Content • 10: Coin Miners
severity	Risk level	• 0: user defined • 1: low • 2: medium • 3: high • 4: potential threat risk

CEF KEY	DESCRIPTION	VALUE
policyName	Policy name	Example: test
profileName	Profile name	Reserved, currently displays as default
wrsThreshold	WRS threshold	Value is set to 50
principalName	Principal name	Reserved, default is null
request	URL	Example: hxxp://ca95-1.winshipway.com/
cat	URL category	Example: Ransomware
appName	Application name	Reserved, default is null
wrsScore	WRS score	Example: 81
malwareType	Malware type	Reserved, default 0
malwareName	Malware name	Example: Ransomware
soData	Suspicious object displayed on the Deep Discovery Web Inspector **Detections** page	Can be one of the following types: • Domain • URL • Server IP • File SHA1
fname	File name	Example: a.txt
filehash	SHA1	Example: 0d3d4cdfff683b0c17843a889e867fe29095c3ac
msg	Log description	Value is null

CEF KEY	DESCRIPTION	VALUE
httpTrans	HTTP transaction	Example: {"http_req":{"headers":{"accept-encoding":"gzip,deflate","host":"10.204.170.7","user-agent":"Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36"},"host":"10.204.170.7","method":"GET","path":"TESTDATA/virus/NonCleanable/EXT_BOO.BOO","scheme":"http"}, "http_response":{"headers":{"content-length":"512","content-type":"text/plain"},"status_code":200},"ver":"1.0"}
debugInfo	Debug information	Example: {"conn_state":{"auth_id_type":"ip","auth_is_guest":false,"auth_reuse":false,"auth_user_id":"10.204.171.200","bypass_scan":false,"c_listen_addr":"0.0.0.0:8080","c_local_addr":"10.204.133.74:8080","c_peer_addr":"10.204.171.200:64353","c_recv_bytes":470,"c_sent_bytes":0,"gateway_ip":"10.204.171.200","s_recv_bytes":0,"s_sent_bytes":0,"tmufe_timeout":false},"errcode":"3055,IWSSHttpProxyProtocol.cpp:2569","src":"Proxy","trans":{"info":"","time":"1: 1508519757821, 2: 0, 13: 1, 14: 1, 33: 1, 15: 1, 16: 1, 34: 1, 38: 1"}, "ver":"1.0"}

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Web Inspector|2.2.0.1105|
100001|Ransomware|3|wrsScore=49 userName=10.204.171.200
domain=ca95-1.winshipway.com adDomain= policyName=default
detectionType=21 app=1 principalName= logType=6 groupName=
```

```
malwareType=0 httpTrans={"http_req":{"headers":{"accept-
encoding":"gzip, deflate","host":"ca95-1.winshipway.com",
"proxy-connection":"keep-alive","user-agent":"Mozilla/5.0
(Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/61.0.3163.100 Safari/537.36"},"host":
"ca95-1.winshipway.com","method":"GET","path":"/","scheme":
"http"},"http_response":{"headers":null,"status_code":-1},
"ver":"1.0"} device= profileName=default tlsVersion=0 soData=
size=0 rt=Oct 20 2017 17:15:57 GMT+00:00
src=10.204.171.200 threatType=1 wrsThreshold=50 severity=3
malwareName=Ransomware from WRS companyId=
filehash= dst=54.148.125.151 appName=
request=http://ca95-1.winshipway.com/ techSubType=0
cat=Ransomware upstreamSize=0 downstreamSize=0
fname= act=block department= debugInfo={"conn_state":
{"auth_id_type":"ip","auth_is_guest":false,"auth_reuse":
false,"auth_user_id":"10.204.171.200","bypass_scan":false,
"c_listen_addr":"0.0.0.0:8080","c_local_addr":"10.204.133.74
:8080","c_peer_addr":"10.204.171.200:64353","c_recv_bytes"
:470,"c_sent_bytes":0,"gateway_ip":"10.204.171.200",
"s_recv_bytes":0,"s_sent_bytes":0,"tmufe_timeout":false},
"errcode":"3055,IWSSHttpProxyProtocol.cpp:2569","src":
"Proxy","trans":{"info":"","time":"1:1508519757821, 2: 0,
13: 1, 14: 1, 33: 1, 15: 1, 16: 1, 34: 1, 38: 1"},"ver":"1.0"}
msg=
```

Chapter 3

Syslog Content Mapping - LEEF

The following topics outline syslog content mapping between Deep Discovery Web Inspector log output and the LEEF syslog type:

LEEF Violation Logs

TABLE 3-1. LEEF Violation 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 Web Inspector
Header(pver)	Appliance version	Example: 2.2.0.1181
Header(eventName)	Description	Example: Ransomware
devtime	UTC timestamp	Example: Oct 20 2017 17:15:57 GMT+00:00
logType	Log type	6: Violation Log
companyId	Company ID	Reserved, value is default
adDomain	AD domain	Active Directory domain information Example: trendnet.org
userName	Client IP	Example: 10.204.171.200
groupName	Group name	Active Directory group name information
department	Department	Active Directory department information Example: commercial
device	Device	Reserved, default null

LEEF KEY	DESCRIPTION	VALUE
act	Action	Can be one of the following values: • allow • monitor • block • analyze
proto	Protocol channel	• 1: HTTP • 2: HTTPS • 3: HTTP2 • 4: FTP
tlsVersion	TLS version	• 0: None TLS • 1: SSLv3 • 2: TLSv1.0 • 3: TLSv1.1 • 4: TLSv1.2
size	Transport bytes by Deep Discovery Web Inspector, unit bytes	Example: 15
dst	Destination IP address of request	Example: 54.148.125.151
src	Source IP address of request	Example: 10.204.171.200
upstreamSize	The upstream payload from Deep Discovery Web Inspector to server, unit bytes	Example: 54

LEEF KEY	DESCRIPTION	VALUE
downstreamSize	The downstream payload from server to Deep Discovery Web Inspector, unit bytes	Example: 49
domain	Domain	Example: ca95-1.winshipway.com
detectionType	Detection type	For a description of each type, see *List of Detection Types on page 1-3*
detectionSubType	Detection sub-type	Reserved, default 0
threatType	Threat type	• 1: Ransomware • 2: C&C Callback • 3: Suspicious Malware • 4: Suspicious URLs • 5: Suspicious Documents • 6: Suspicious Scripts • 7: Malicious URL • 8: Malicious Content • 9: Suspicious Content • 10: Coin Miners
sev	Risk level	• 0: user defined • 1: low • 2: medium • 3: high • 4: potential threat risk
policy	Policy name	Example: test
profileName	Profile name	Reserved, currently displays as default

LEEF Key	Description	Value
wrsThreshold	WRS threshold	Value is set to 50
principalName	Principal name	Reserved, default is null
url	URL	Example: hxxp://ca95-1.winshipway.com/
urlCat	URL category	Example: Ransomware
appName	Application name	Reserved, default is null
wrsScore	WRS score	Example: 81
malwareType	Malware type	Reserved, default 0
malwareName	Malware name	Example: Ransomware
soData	Suspicious object displayed on the Deep Discovery Web Inspector **Detections** page	Can be one of the following types: • Domain • URL • Server IP • File SHA1
fName	File name	Example: a.txt
fileHash	SHA1	Example: 0d3d4cdfff683b0c17843a889e867fe29095c3ac
msg	Log description	Value is null

LEEF KEY	DESCRIPTION	VALUE
httpTrans	HTTP transaction	Example: {"http_req":{"headers":{"accept-encoding":"gzip,deflate","host":"10.204.170.7","user-agent":"Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36"},"host":"10.204.170.7","method":"GET","path":"TESTDATA/virus/NonCleanable/EXT_BOO.BOO","scheme":"http"}, "http_response":{"headers":{"content-length":"512","content-type":"text/plain"},"status_code":200},"ver":"1.0"}
debugInfo	Debug information	Example: {"conn_state":{"auth_id_type":"ip","auth_is_guest":false,"auth_reuse":false,"auth_user_id":"10.204.171.200","bypass_scan":false,"c_listen_addr":"0.0.0.0:8080","c_local_addr":"10.204.133.74:8080","c_peer_addr":"10.204.171.200:64353","c_recv_bytes":470,"c_sent_bytes":0,"gateway_ip":"10.204.171.200","s_recv_bytes":0,"s_sent_bytes":0,"tmufe_timeout":false},"errcode":"3055,IWSS HttpProxyProtocol.cpp:2569","src":"Proxy","trans":{"info":"","time":"1: 1508519757821, 2: 0, 13: 1, 14: 1, 33: 1, 15: 1, 16: 1, 34: 1, 38: 1"}, "ver":"1.0"}

Log sample:

```
LEEF:1.0|Trend Micro|Deep Discovery Web Inspector|2.2.0.1181|
Ransomware|wrsScore=49 detectionType=21 domain=ca95-1.winshipway.com
adDomain= malwareType=0 fileHash= sev=3 fName= principalName=
logType=6 groupName= policy=default httpTrans={"http_req":
```

{"headers":{"accept-encoding":"gzip,deflate","host":
"ca95-1.winshipway.com","proxy-connection":"keep-alive",
"user-agent":"Mozilla/5.0 (Windows NT 6.1; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100
Safari/537.36"},"host":"ca95-1.winshipway.com","method":"GET",
"path":"/","scheme":"http"},"http_response":{"headers":null,
"status_code":-1},"ver":"1.0"} device= profileName=default
tlsVersion=0 soData= urlCat=Ransomware size=0
userName=10.204.171.200 src=10.204.171.200 threatType=1
wrsThreshold=50 companyId= url=http://ca95-1.winshipway.com/
dst=54.148.125.151 proto=1 appName= techSubType=0
malwareName=Ransomware from WRS upstreamSize=0
downstreamSize=0 devTime=Oct 24 2017 15:14:18 GMT+00:00
act=block department= debugInfo={"conn_state":{"auth_id_type":
"ip","auth_is_guest":false,"auth_reuse":false,"auth_user_id":
"10.204.171.200","bypass_scan":false,"c_listen_addr":
"0.0.0.0:8080","c_local_addr":"10.204.133.74:8080",
"c_peer_addr":"10.204.171.200:63065","c_recv_bytes":470,
"c_sent_bytes":0,"gateway_ip":"10.204.171.200",
"s_recv_bytes":0,"s_sent_bytes":0,"tmufe_timeout":false},
"errcode":"3055,IWSSHttpProxyProtocol.cpp:2569","src":
"Proxy","trans":{"info":"","time":"1:1508858058298, 2: 0, 13:
0, 14: 2, 33: 2, 15: 2, 16: 176, 34: 176, 38:176"},"ver":"1.0"}
msg=

Chapter 4

Syslog Content Mapping - TMEF

The following topics outline syslog content mapping between Deep Discovery Web Inspector log output and the TMEF syslog type:

TMEF Violation Logs

TABLE 4-1. TMEF Violation Logs

CEF KEY	DESCRIPTION	VALUE
Header(logVer)	CEF format version	CEF: 0
Header(vendor)	Appliance vendor	Trend Micro
Header(pname)	Appliance product	Deep Discovery Web Inspector
Header(pver)	Appliance version	Example: 2.2.0.1105
Header(eventid)	Signature ID	Example: 100001
Header(eventName)	Description	Example: Ransomware
Header(severity)	Risk level	• 0: user defined • 1: low • 2: medium • 3: high • 4: potential threat risk
rt	UTC timestamp	Example: Oct 20 2017 17:15:57 GMT+00:00
logType	Log type	6: Violation Log
companyId	Company ID	Reserved, value is default
adDomain	AD domain	Active Directory domain information Example: trendnet.org
userName	Client IP	Example: 10.204.171.200
groupName	Group name	Active Directory group name information

CEF KEY	DESCRIPTION	VALUE
department	Department	Active Directory department information Example: commercial
device	Device	Reserved, default null
act	Action	Can be one of the following values: • allow • monitor • block • analyze
app	Protocol channel	• 1: HTTP • 2: HTTPS • 3: HTTP2 • 4: FTP
tlsVersion	TLS version	• 0: None TLS • 1: SSLv3 • 2: TLSv1.0 • 3: TLSv1.1 • 4: TLSv1.2
size	Transport bytes by Deep Discovery Web Inspector, unit bytes	Example: 15
dst	Destination IP address of request	Example: 54.148.125.151
src	Source IP address of request	Example: 10.204.171.200

CEF KEY	DESCRIPTION	VALUE
upstreamSize	The upstream payload from Deep Discovery Web Inspector to server, unit bytes	Example: 54
downstreamSize	The downstream payload from server to Deep Discovery Web Inspector, unit bytes	Example: 49
domain	Domain	Example: ca95-1.winshipway.com
detectionType	Detection type	For a description of each type, see *List of Detection Types on page 1-3*
detectionSubType	Detection sub-type	Reserved, default 0
threatType	Threat type	• 1: Ransomware • 2: C&C Callback • 3: Suspicious Malware • 4: Suspicious URLs • 5: Suspicious Documents • 6: Suspicious Scripts • 7: Malicious URL • 8: Malicious Content • 9: Suspicious Content • 10: Coin Miners
severity	Risk level	• 0: user defined • 1: low • 2: medium • 3: high • 4: potential threat risk

CEF Key	Description	Value
policyName	Policy name	Example: test
profileName	Profile name	Reserved, currently displays as default
wrsThreshold	WRS threshold	Value is set to 50
principalName	Principal name	Reserved, default is null
request	URL	Example: hxxp://ca95-1.winshipway.com/
cat	URL category	Example: Ransomware
appName	Application name	Reserved, default is null
wrsScore	WRS score	Example: 81
malwareType	Malware type	Reserved, default 0
malwareName	Malware name	Example: Ransomware
soData	Suspicious object displayed on the Deep Discovery Web Inspector **Detections** page	Can be one of the following types: • Domain • URL • Server IP • File SHA1
fname	File name	Example: a.txt
filehash	SHA1	Example: 0d3d4cdfff683b0c17843a889e867fe29095c3ac
msg	Log description	Value is null

CEF KEY	DESCRIPTION	VALUE
httpTrans	HTTP transaction	Example: {"http_req":{"headers":{"accept-encoding":"gzip,deflate","host":"10.204.170.7","user-agent":"Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36"},"host":"10.204.170.7","method":"GET","path":"TESTDATA/virus/NonCleanable/EXT_BOO.BOO","scheme":"http"}, "http_response":{"headers":{"content-length":"512","content-type":"text/plain"},"status_code":200},"ver":"1.0"}
debugInfo	Debug information	Example: {"conn_state":{"auth_id_type":"ip","auth_is_guest":false,"auth_reuse":false,"auth_user_id":"10.204.171.200","bypass_scan":false,"c_listen_addr":"0.0.0.0:8080","c_local_addr":"10.204.133.74:8080","c_peer_addr":"10.204.171.200:64353","c_recv_bytes":470,"c_sent_bytes":0,"gateway_ip":"10.204.171.200","s_recv_bytes":0,"s_sent_bytes":0,"tmufe_timeout":false},"errcode":"3055,IWSS HttpProxyProtocol.cpp:2569","src":"Proxy","trans":{"info":"","time":"1: 1508519757821, 2: 0, 13: 1, 14: 1, 33: 1, 15: 1, 16: 1, 34: 1, 38: 1"}, "ver":"1.0"}

Log sample:

```
CEF:0|Trend Micro|Deep Discovery Web Inspector|2.2.0.1105|
100001|Ransomware|3|wrsScore=49 userName=10.204.171.200
domain=ca95-1.winshipway.com adDomain= policyName=default
detectionType=21 app=1 principalName= logType=6 groupName=
```

```
malwareType=0 httpTrans={"http_req":{"headers":{"accept-
encoding":"gzip,deflate","host":"ca95-1.winshipway.com",
"proxy-connection":"keep-alive","user-agent":"Mozilla/5.0
(Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/61.0.3163.100 Safari/537.36"},"host":
"ca95-1.winshipway.com","method":"GET","path":"/","scheme":
"http"},"http_response":{"headers":null,"status_code":-1},
"ver":"1.0"}  device= profileName=default tlsVersion=0 soData=
size=0 rt=Oct 24 2017 17:21:31 GMT+00:00
src=10.204.171.200 threatType=1 wrsThreshold=50 severity=3
malwareName=Ransomware from WRS companyId=
filehash= dst=54.148.125.151 appName=
request=http://ca95-1.winshipway.com/ techSubType=0
cat=Ransomware upstreamSize=0 downstreamSize=0
fname= act=block department= debugInfo={"conn_state":
{"auth_id_type":"ip","auth_is_guest":false,"auth_reuse":
false,"auth_user_id":"10.204.171.200","bypass_scan":false,
"c_listen_addr":"0.0.0.0:8080","c_local_addr":"10.204.133.74
:8080","c_peer_addr":"10.204.171.200:51241","c_recv_bytes"
:470,"c_sent_bytes":0,"gateway_ip":"10.204.171.200",
"s_recv_bytes":0,"s_sent_bytes":0,"tmufe_timeout":false},
"errcode":"3055,IWSSHttpProxyProtocol.cpp:2569","src":
"Proxy","trans":{"info":"","time":"1:1508865691374, 2: 0,
13: 0, 14: 0, 33: 0, 15: 0, 16: 0, 34: 0, 38: 0"},"ver":"1.0"}
msg=
```

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: APEM28502/181003