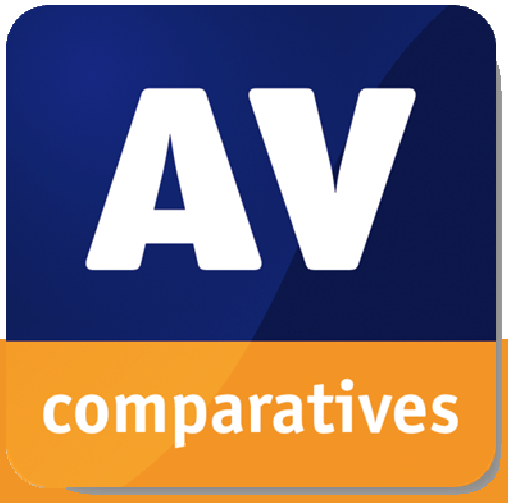

RTTL Certification Test

June 2016

Language: English
June 2016

Last Revision: 10th July 2016

www.av-comparatives.org

Introduction

2nd AMTSO Real Time Threat List (RTTL) based certification test

http://www.av-comparatives.org/certification-tests/

What is the RTTL?

The Real-Time Threat List (RTTL) is a repository of malware samples collected by experts from around the world. The repository is managed, maintained and secured by the Anti-Malware Testing Standards Organization (AMTSO).

Why is there a need for the RTTL?

As malware now travels the globe in real-time with the majority of infections happening through websites then a real-time system was needed to provide testers of Anti-Malware solution a repository of malware they can use to validate that Anti-Malware products are working in real-time to protect users. The end result of this being that published test results allows business and consumer to make informed decisions on what Anti-Malware solution best meets their requirements.

Who Submits samples to the RTTL?

Anti-Malware companies and Anti-Malware experts from around the world submit identified and validated samples to the RTTL, which include prevalence data that includes the distribution and source of the malware.

Who uses the samples from RTTL?

Testers looking at the efficacy of Anti-Malware products use the samples to validate their own collected samples that they test with to check for prevalence to ensure that what they are testing with are real world examples that threaten users a businesses. Academics researching or analysing trends in the Anti-malware industry can also use the RTTL to allow them to have a rich data source to work from.

Source: **http://www.amtso.org/rttl/**

Sample used for this report

The ***Top500*** samples (tagged as "***malware***" in RTTL) for the month of June 2016 were queried and tested on the 27th June 2016. As the RTTL contains currently also misclassified clean and PUA files, we took only those samples which showed malicious behaviour in our sandboxes. At the end, 299 malicious samples remained and were taken for the test.

Test Details

Test Period	**27th June 2016**
Number of Test cases	**299**
Online with cloud connectivity	**Yes**
Update allowed	**Yes**
Platform/OS	**Microsoft Windows 7 SP1 64bit English**

Query	*The API Function "**getTopFiles**" was used with the following parameters according to the RTTL manual:*
	
	`def getTopFiles(amount, page):`
	`  params = {`
	`  "resultsLimit": amount,`
	`  "resultsPage": page,`
	`  "prevalenceFrom": 1,`
	`  "prevalenceTo": 4294967295,`
	`  "sortBy": "prevalence",`
	`  "sortOrder": "desc",`
	`  "lastSeen": "2016-06-01 00:00:00",`
	`  "fileTypesArr[]" : "1"`
	`  }`

Query Timestamp	**27th June 2016 07:45 AM**

Methodology

AV-Comparatives used their Real-World Protection Framework to execute those 299 samples. Each sample was **executed** simultaneously under Windows 7 SP1 64bit with the respective security product installed to see if it is detected and blocked. The security products used default settings and had full-Internet (cloud) access.

For this test, we included publicly available endpoint security products of current AMTSO members.

Results

29 products have been put to the test. A protection rate over 98% is required to get certified.

Product	Certified
AhnLab V3 Internet Security	✓
Avast Free Antivirus	✓
AVG Internet Security	✓
Avira Antivirus Pro	✓
Bitdefender Internet Security	✓
BullGuard Internet Security	✓
Emsisoft Anti-Malware	✓
eScan Internet Security	✓
ESET Smart Security	✓
F-Secure Internet Security	✓
Fortinet FortiClient with FortiGate	✓
G DATA Internet Security	✓
K7 Total Security	✓
Kaspersky Internet Security	✓
Lavasoft Ad-Aware Pro Security	✓
McAfee Internet Security	✓
Microsoft Security Essentials	✓
Nano Antivirus Pro	✗
Panda Free Antivirus	✓
PC Pitstop PC Matic	✓

Product	Certified
Qihoo 360 Total Security	✅
Quick Heal Total Security	✅
Sophos Endpoint Protection	✅
Symantec Norton Security Premium	✅
Tencent PC Manager	✅
TGsoft VirIT eXplorer Lite	❌
ThreatTrack Vipre Internet Security Pro	✅
Trend Micro Internet Security	✅
Webroot SecureAnywhere Antivirus	❌

Copyright and Disclaimer

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives (July 2016)