Full Product Test of Palo Alto Networks Traps

Date of the Report: July 21th 2017

Introduction

Palo Alto Networks commissioned AV-TEST to perform a full product test of the product Traps.

The tested categories are as follows:

- PROTECTION, consisting of
  - Protection against 0-day malware attacks, inclusive of web and e-mail threats (Real-World Testing)
  - Detection of widespread and prevalent malware discovered in the last 4 weeks (the AV-TEST reference set)
- PERFORMANCE, running on both a new hardware and an old hardware platform
  - Older standard business PC: Intel Xeon X3360 @ 2,83GHz, 4 GB RAM, 500 GB HDD
  - Recent High-End PC: Intel i7 3770 @ 3,40GHz, 16 GB RAM, Samsung 512 GB SSD
  - 5 tests: Slowing-down when launching popular websites, Slower download of frequently-used applications, Slower launch of standard software applications, Slower installation of frequently-used applications, Slower copying of files (locally and in a network)
- USABILITY (FALSE POSITIVES), consisting of
  - False warnings or blockages when visiting websites
  - False warnings concerning certain actions carried out whilst installing and using legitimate software
  - False blockages of certain actions carried out whilst installing and using legitimate software

The tests have been carried out between in May 2017 on Windows 10 Professional (English) 64-Bit. The version of the Palo Alto Networks Traps was 4.0.0.24417.

Results

The result of the testing is given separately for the three categories and will be compared to the average results of the latest public tests.

PROTECTION

The real-world test has been carried out with 108 real-world attacks (new and live malware currently spread via URLs and E-Mail). For the prevalent test 5,623 malware files that have been collected during April and were reported as being prevalent by at least two independent sources have been used. Table 1 displays the detection rates.

Test Category	Number of Test Cases	Successful Detection	Detection Rate
Real-World attacks	108	108	100%
Prevalent Malware	5,623	5,581	99.25%

Table 1 PROTECTION Test Results

The detection rate of 100% in the real-world test is above the average detection rate we have observed in the public tests in January/February (99.5%) as well as March/April (99.4%).

In case of detection of prevalent malware, the detection rate is 99.25, the average in the January/February public testing was 99.6% and in March/April 99.9%.

PERFORMANCE

Performance testing revealed that Traps has a very small impact on the system performance. The impact was a bit higher on the older hardware, while there was nearly no measurable impact on the newer system. Table 2 shows the impact of Palo Alto Traps on the different test cases.

Test Case	New Hardware	Old Hardware
Download files	0.67%	0.22%
Load websites	4.76%	7.86%
Install applications	12.75%	10.12%
Run applications opening specific documents	11.84%	2.21%
Copy files	1.21%	0.54%

Table 2 PERFORMANCE Test Results

The scores are clearly better than the average of other products, both for January/February as well as for March/April testing. No problems could be observed here.

USABILITY

This test has been carried out against 500 benign websites and 41 popular software installers. The 500 websites have been visited with a browser to check for false blockings of any URL/Website protection component. The 41 software programs have been installed and used to check for any detections by dynamic protection components. Table 3 shows the results of the individual tests.

Test Category	Number of Test Cases	False Detection	False Positive Rate
Websites	500	0	0.00%
Dynamic Test (Local Analysis Module)	41	4	9.76%
Dynamic Test (WildFire Module)	41	1	2.44%

Table 3 USABILITY Test Results

Please note that 3 out of 4 false detections were fixed after just a few minutes by the WildFire module automatically. This is also indicated in the table above.

The average in our regular tests for the dynamic false positive test, is less than or equal 1. Only a few products alert during this test.

Summary

In order to easily compare products, AV-TEST introduced a scoring system for PROTECTION, PERFORMANCE and USABILITY which ranges from 0 (worst) to 6 (best). The Palo Alto Networks results displayed above would translate into the following table, compared with the average of other tested products:

	Palo Alto Networks	January/February Average	March/April Average
PROTECTION	5.5	5.5	5.7
PERFORMANCE	6	5.4	5.7
USABILITY	5.5	5.9	5.5
TOTAL	17	16.8	16.9

Table 4 Palo Alto Networks Scores