ENTERPRISE ENDPOINT PROTECTION TEST REPORT

SECURITY STACK: SOCIALLY ENGINEERED MALWARE

Trend Micro Endpoint Security v11.0.1057

Authors – Anil Pokhrel, Bhaarath Venkateswaran, Jayendra Phatak

Environment

Operating System: Windows 7 Enterprise Service Pack 1 32-bit

- Windows Defender disabled
- Application Reputation disabled (relevant for Windows 8.1)

Internet Explorer 10.0.9200.16660

- Smart Screen Filter disabled

Overview

Trend Micro Endpoint Security v11.0.1057 was installed in the NSS Labs live stack test harness as part of NSS' continuous live testing of enterprise endpoint protection (EPP) products. Trend Micro's product was subjected to thorough testing for protection against socially engineered malware (SEM) at the NSS facility in Austin, Texas, based on the *Security Stack: Test Methodology v*1.5. NSS test methodologies are available at www.nsslabs.com.

The results presented in this report were obtained via 24x7 continuous testing over a period of 24 days. Throughout the test, new URLs were added as they were discovered, and unreachable URLs were removed. This test was composed of over 1700 test cases that included 400 unique attacks (URLs) and 304 unique SEM samples (hashes). A unique SEM sample has a unique hash. A unique attack URL may contain duplicate SEM samples that are part of a unique URL; *http://a.edu/abc/malware.exe* and *http://a.edu/malware.exe* are unique URLs**.**

In order to test a real world deployment, vendors are encouraged to configure their products for optimal security effectiveness and performance as they would recommend in a typical enterprise deployment.

This test was conducted free of charge, and NSS did not receive any compensation for Trend Micro's participation.

Average Block Rate

Figure 1 depicts the average of SEM samples blocked throughout the duration of the test. EPP updates may contain new engine updates, heuristic updates, and malware specific detection updates that affect both exploit and malware security effectiveness. This test focuses on SEM. Tests for exploit protection are published at www.nsslabs.com.

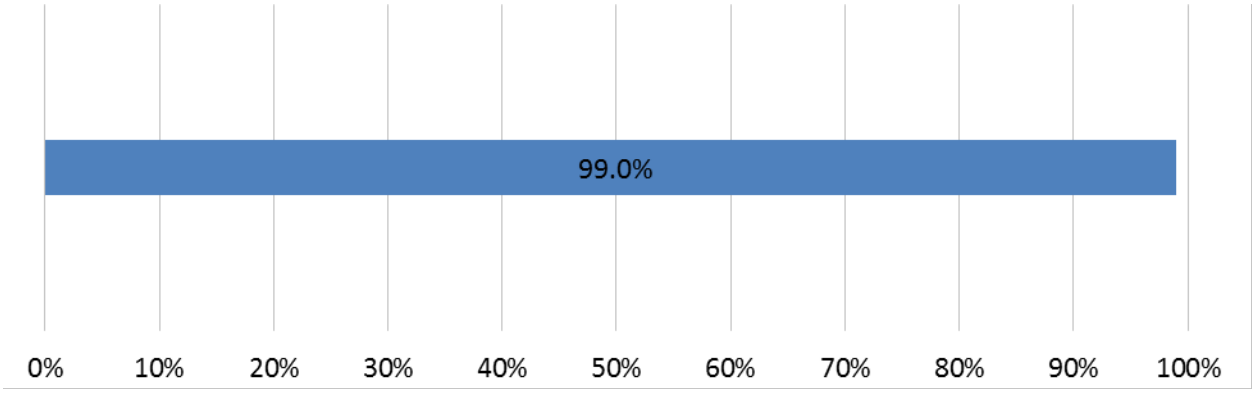

Figure 1 — Average Block Rate for SEM

Response Time For Unique New Samples

New SEM samples are harvested daily. Figure 2 depicts the length of time it took Trend Micro Endpoint Security to reach its maximum detection rate for unique new samples during the first seven days after a unique new sample has been introduced into the test harness.

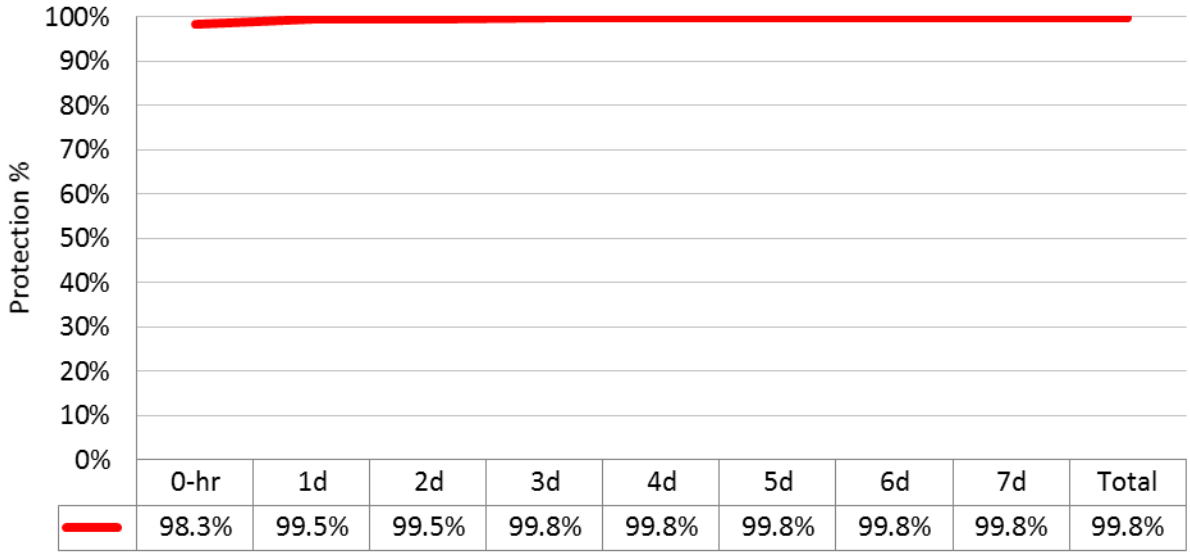

Figure 2 — Average Time to Block Unique New Malware Samples

Figure 2 measures the percentage of new unique samples blocked in 24-hour intervals during the first seven days after the sample was introduced.

Consistency of Malware Protection

Figure 3 depicts the consistency of protection rates throughout the duration of the test. Negative fluctuations can indicate decreased detection rates for new samples, erratic detection of new and existing samples, or both. A new malware campaign may cause a sharp downward spike until protection is added.

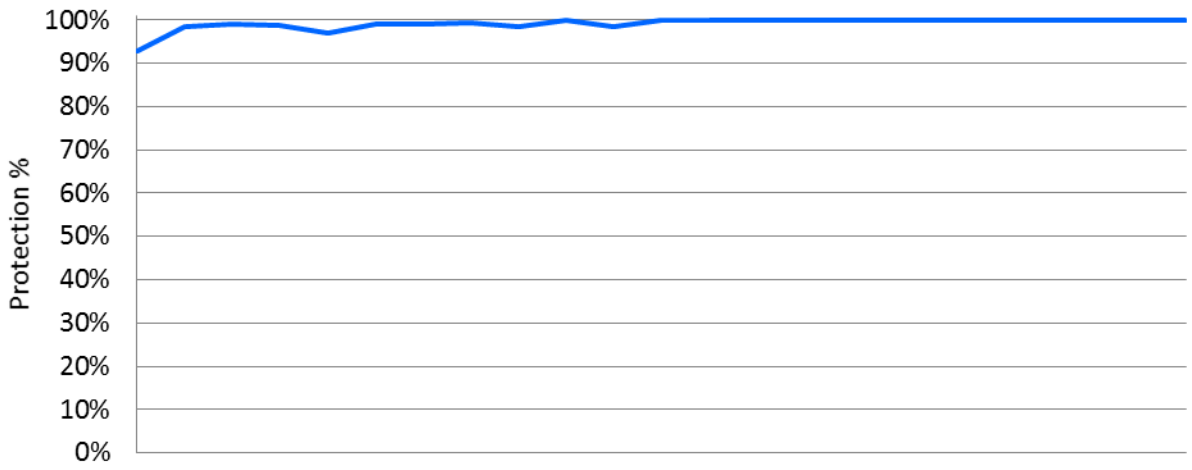

Figure 3 — Malware Protection over Time

Tests against all of the SEM samples are repeated several times each day. Figure 4 depicts the average time to add detection for the complete sample set, which includes both new and existing samples.

Product	Hours
Trend Micro Endpoint Security v11.0.1057	0.28

Figure 4 — Average Time to Add Protection

Test Methodology

Security Stack: Test Methodology v1.5

A copy of the test methodology is available on the NSS Labs website at www.nsslabs.com.

Contact Information

NSS Labs, Inc.
206 Wild Basin Road
Building A, Suite 200
Austin, TX 78746
info@nsslabs.com
www.nsslabs.com