ENTERPRISE EPP COMPARATIVE ANALYSIS

Socially Engineered Malware

Randy Abrams, Jayendra Pathak, Ahmed Garhy

Tested Products

Fortinet Fortigate 100D

Management station Forticlient-5.0.7.333

McAfee VirusScan Enterprise and AntiSpyware Enterprise

VirusScan Enterprise 8.8.0.975, McAfee Agent 4.8.0.641, Host Intrusion Prevention 8.0.0.2482,

Site Advisor Enterprise Plus 3.5.0.724, Solidcore 6.1.1.1.369

Symantec Endpoint Protection

Version 12.1.3001.165

Trend Micro OfficeScan

Version 10.6.5300 Service pack 3

Bitdefender

Endpoint Security by Bitdefender

Version 5.1.10.283

Environment

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

Internet Explorer 10.0.9200.16660 with Smart Screen Filter disabled

Overview

Social engineering is one of the most effective and widely used components of cyber attacks against enterprises and individuals. Cybercriminals utilize various social engineering tactics to deceive users into downloading and executing malware such as fake antivirus, fake utilities, fake upgrades to the operating system or applications, and trojanized applications. Endpoint protection (EPP) products are a critical layer of defense against such attacks. Both web browsers and EPP products utilize blacklisting, whitelisting, and application reputation systems to prevent socially engineered malware from being downloaded. If malware is successfully downloaded, the EPP product has two additional chances to eliminate the threat before it can infect the target. EPP can block the threat as soon as it writes to the temporary Internet files directory or download directory, or the malware can be blocked when executed; however, the percentage of times an EPP product blocks on execution versus on download is extremely small.

NSS Labs performs comparative tests of EPP products for three of the most relevant type of attacks:

- Socially engineered malware (SEM) protection
- Exploit protection
- Phishing protection

This group test verified the ability of EPP products to block socially engineered malware attacks. Socially engineered malware may be delivered using scare tactics such as false reports of systems problems; misinformation, such as reporting that a program requires an update to be installed; or as a phishing attack with a payload of malicious software. Offers of free software are another tactic used to deceive users into installing malware. EPP products must provide robust defenses against SEM.

Figure 1 depicts the average block rate for each of the tested products over a period of 7 days.

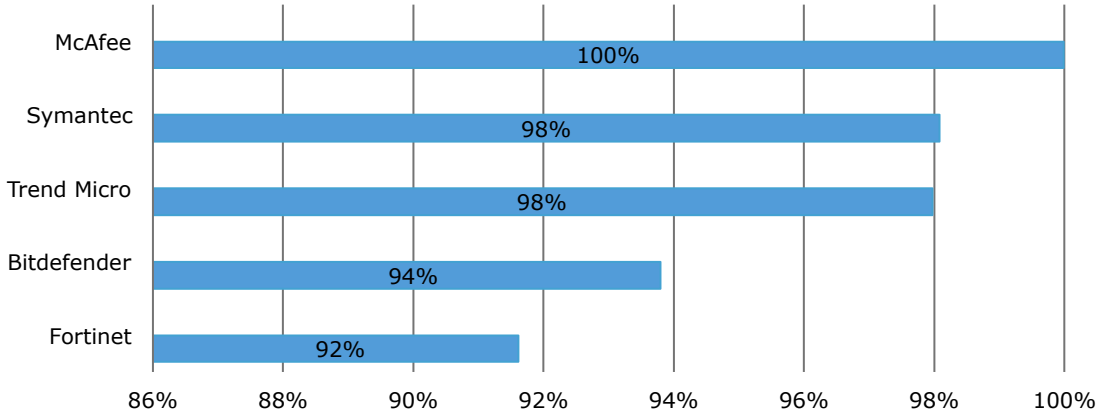


Figure 1 – Average Block Rate on Download for Socially Engineered Malware

In this EPP SEM test, McAfee VirusScan Enterprise achieved an average download block rate of 100%, with all of the SEM blocked on download. Symantec Endpoint Protection on average blocked 98.1% of the SEM on download. Trend Micro OfficeScan placed third with 98.0% of the SEM blocked on download. Bitdefender Endpoint Security blocked 93.8% of the SEM. Fortinet Fortigate 100D achieved a 91.6% block rate.

Figure 2 depicts the combined download and execute block rates for each of the tested products after 7 days.

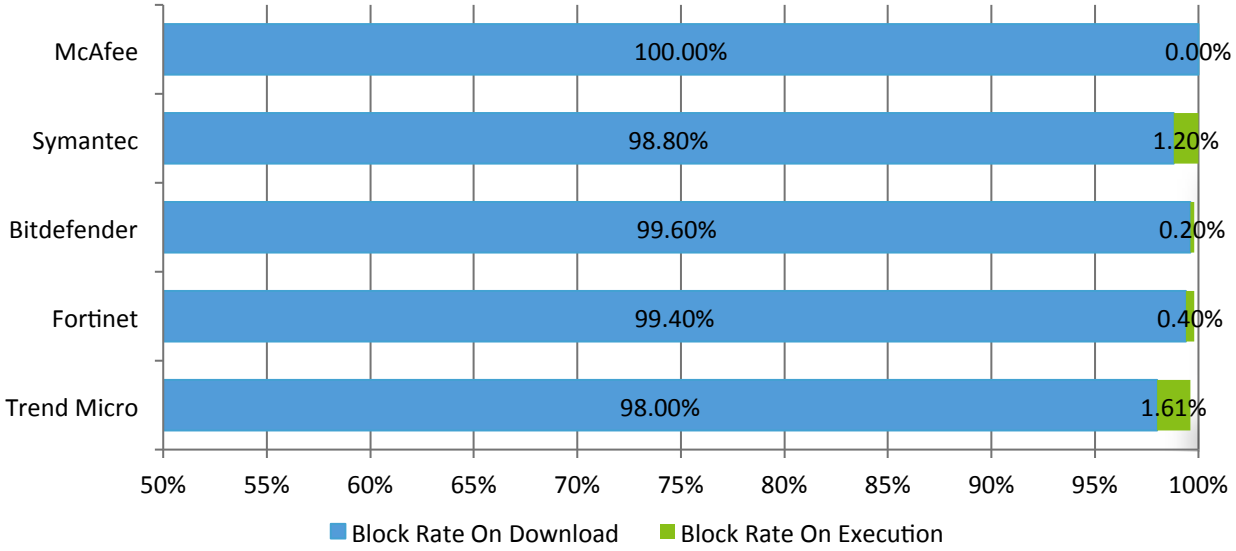


Figure 2 – Combined Block Rate for Socially Engineered Malware After 7 Days

This graph represents the combined block-on-download and block-on-execute protection each vendor provided at the end of 7 days of testing. McAfee VirusScan Enterprise achieved a combined block rate of 100%, with all of the SEM blocked on download. Symantec Endpoint Protection blocked 100% of the SEM, with 98.8% blocked on download and 1.2% blocked upon attempted execution. Bitdefender Endpoint Security blocked 99.8% of the SEM, with 99.6% blocked on download and 0.2% blocked on attempted execution. Fortinet Fortigate 100D achieved a 99.8% block rate, with 99.4% blocked on download and 0.4% blocked on execution. Trend Micro OfficeScan had the highest ratio of execution to download blocking.

NSS Labs Findings

- Enterprises face a higher level of risk from phishing than from SEM.
- The bulk of the protection EPP products provide against SEM occurs on download prior to the point of execution.
- In the 7 day block-on-download average, McAfee VirusScan Enterprise blocked 100% of the SEM, Symantec Endpoint Protection blocked 98.1%, Trend Micro OfficeScan blocked 98.0%, BitDefender Endpoint Security blocked 93.8%, and Fortinet Fortigate 100D blocked 91.6%.
- McAfee VirusScan added protection for new threats in 31 seconds on average, providing a 12x time-to-block advantage over the competition in addition to blocking 100% of the SEM.
- When combining SEM block-on-download and block-on-execution capabilities after 7 days, all products achieved security effectiveness scores in excess of 99%, with Symantec Endpoint Protection achieving 100%.

NSS Labs Recommendations

- Utilize NSS tests for phishing protections, exploit and evasion protection, and SEM protection when considering selection of an EPP product.
- Use corporate security policy, secure machine configuration, and access to a helpdesk for end users in order to reduce the threat of SEM.
- Enterprises using the bring your own device (BYOD) model should take into account potentially increased vulnerability to SEM.

Table of Contents

Table of Figures

Analysis

Between December 15, 2013 and January 19, 2014, NSS performed a comprehensive test of EPP SEM protection on five enterprise EPP offerings. These results are based on empirical data gathered by NSS during 36 days of continuous testing. EPP products were tested an average of 218 times per day. Every six hours, new URLs were added, and unreachable URLs were removed. A total of 497 unique samples of SEM were used during the test.

Both browsers and EPP products provide protection against phishing and SEM. The choice of an EPP product based on protection against SEM is often less relevant in the enterprise space than in the consumer space. Within enterprise environments, SEM is often deflected by policies and technologies that prevent the installation of software, as well as by ready access to a helpdesk to assist less sophisticated users in avoiding the traps set by would be attackers. Malware attacks that use scare tactics to deceive users into installing fake antivirus are particularly ineffective in such environments. Employees may be at heightened risk of SEM attacks when enterprises choose the BYOD model, since employees that work on home computers lack the SEM protection that is inherent in the enterprise environment.

There is significant overlap in both phishing and SEM protection between browsers and EPP products. This allows enterprises to choose browsers and EPP products that combine to provide high rates of protection.[1]

Consistency of Protection

During the course of a SEM test, it is common for a product to block a threat on download at one moment in time and then miss the same threat at some later point. Figure 3 demonstrates the consistency of download protection across time. Here, McAfee VirusScan Enterprise shows an exceptional level of consistency, while Symantec Endpoint Protection and Trend Micro OfficeScan demonstrate levels of consistency that provide for high average SEM download protection scores. Although blocking on execution can improve the actual protection rates, there will still be some fluctuations in the consistency of protection.

[1] *Evolutions in Browser Security.* NSS Labs. https://www.nsslabs.com/reports/evolutions-browser-security

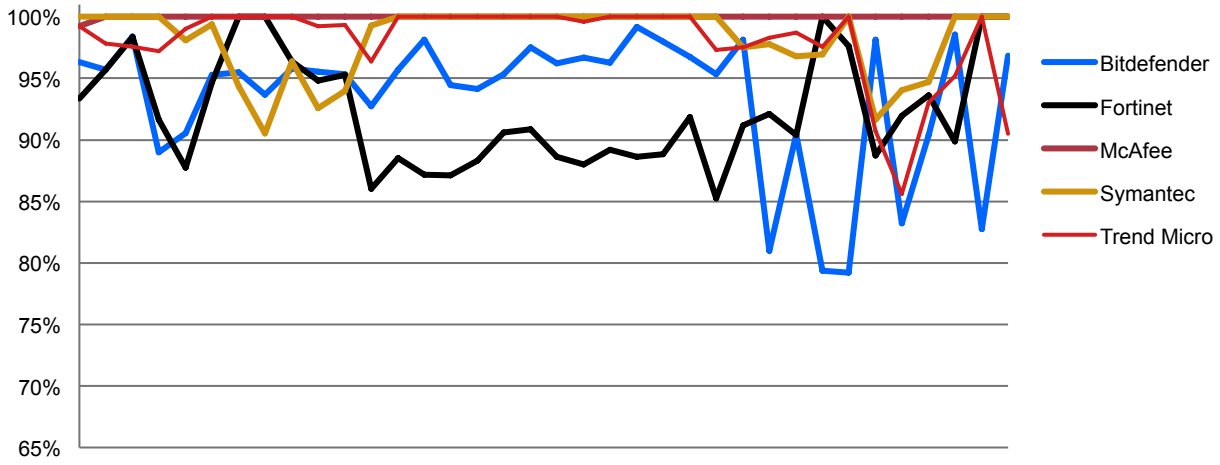
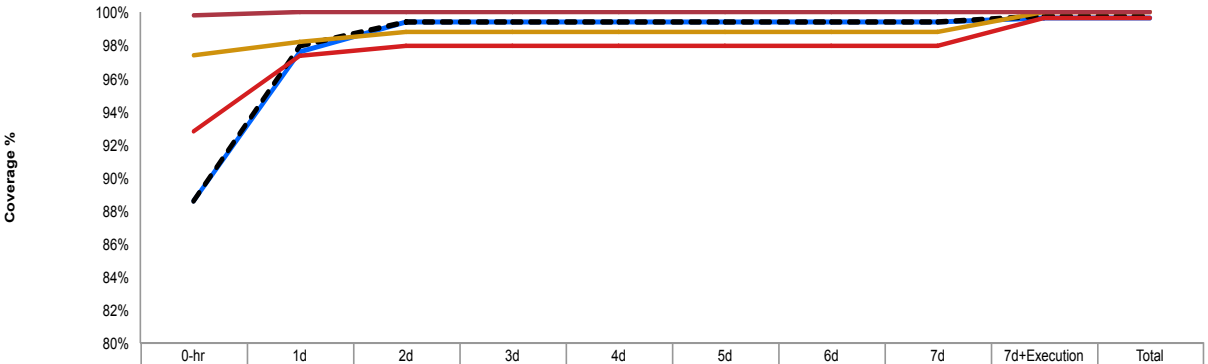


Figure 3 – Socially Engineered Malware Protection Over Time

Histogram of Protection



	0-hr	1d	2d	3d	4d	5d	6d	7d	7d+Execution	Total
Bitdefender	88.5%	97.6%	99.4%	99.4%	99.4%	99.4%	99.4%	99.4%	99.6%	99.6%
Fortinet	88.5%	98.0%	99.4%	99.4%	99.4%	99.4%	99.4%	99.4%	99.8%	99.8%
Symantec	97.4%	98.2%	98.8%	98.8%	98.8%	98.8%	98.8%	98.8%	100.0%	100.0%
McAfee	99.8%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Trend Micro	92.8%	97.4%	98.0%	98.0%	98.0%	98.0%	98.0%	98.0%	99.6%	99.6%

Figure 4 – Malware Response Histogram

The malware response histogram in figure 4 displays the critical zero-hour download block rate for SEM. At the end of 7 days, the download and execution block rates are combined. Both McAfee VirusScan Enterprise and Symantec Endpoint Protection achieved 100% protection scores by the end of day 7. All of the vendors had reached their maximum posted download protection scores by the end of day 2. However, the block-on-execute metrics were only collected at the end of day 7. The one-week totals are empirical total protection effectiveness scores, but these scores do not indicate the actual zero-hour combined protection rate. Despite starting 5 percentage points lower than the average, Bitdefender Endpoint Security finished in second place, and Fortinet Fortigate 100D finished in a tie for third place, with over 99% total protection scores. Bitdefender Endpoint Security and Fortinet Fortigate 100D perform so closely that their lines in the histogram are virtually identical.

Time Is of the Essence

Product	Hours
McAfee VirusScan Enterprise	0.01
Symantec Endpoint Protection	0.25
Trend Micro OfficeScan	0.60
Fortinet Fortigate 100D	1.32
Bitdefender Endpoint Security	2.20
Average	0.87

Figure 5 – Average Time to Add Protection

The same SEM often moves rapidly to new URLS as existing malicious URLs are discovered and blocked. The faster an EPP product provides protection against SEM, the faster protection is provided against all malicious URLs containing the SEM.

With a 31-second average time to add protection as shown in figure 5, McAfee's VirusScan Enterprise SEM protection leads in effectiveness, consistency, and time to react. Symantec's Endpoint Protection average time of 15 minutes to add detection for new SEM combined with a 100% average SEM protection rate is also a good result. Trend Micro OfficeScan required an average of 31 minutes to add protection for SEM while providing 99.6% combined average protection for SEM. These performance levels put each of these products on the short list of EPP products to consider.

SEM Protection as a Selection Criterion

Historically, Safari and Firefox have achieved higher protection scores against phishing attempts, with a faster response time than EPP products. These browsers offer extremely low levels of protection against SEM, however. Internet Explorer (IE) offers exceptional SEM protection with acceptable phishing protection. Chrome provides good protection against SEM, but, similar to IE, it trails Firefox and Safari in phishing protection.[2]

EPP protection against SEM is augmented by the protection offered by browsers such as IE and Chrome. Enterprises using these browsers should consider EPP solutions with superior phishing protection or should use additional anti-phishing products. Trend Micro has scored exceptionally well at phishing protection and provides very high SEM protection.

Education Increases the Effectiveness of Technology

Phishing attacks and SEM attacks will continue to evade technology-based defenses at least some of the time. Both SEM and phishing are social engineering attacks; enterprises that train employees to identify social engineering attacks will be most able to repel such attacks. Technology rarely solves social problems, but education augments

[2] *Evolutions in Browser Security.* NSS Labs. https://www.nsslabs.com/reports/evolutions-browser-security

technological solutions. The most effective EPP product is the one that is used in conjunction with employees that can recognize social engineering.

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 Rd
Building A, Suite 200
Austin, TX 78746
+1 (512) 961-5300
info@nsslabs.com
www.nsslabs.com