NSS Labs

Security. Certified.

ENDPOINT SECURITY

SOCIALLY ENGINEERED MALWARE PROTECTION

COMPARATIVE TEST RESULTS

CORPORATE PRODUCTS

AVG
ESET
F-Secure
Kaspersky
McAfee
Norman
Panda
Sophos
Symantec
Trend Micro

METHODOLOGY VERSION: 1.2

SEPTEMBER 8, 2009

Published by NSS Labs.

CONTACT:

P.O. Box 130573
Carlsbad, CA 92013

Tel: +1.512.961.5300
E-mail: info@nsslabs.com
Internet: http://www.nsslabs.com

EXECUTIVE SUMMARY

The first in a series of lab tests being conducted by NSS Labs examining the protection capabilities of endpoint protection products, this report examines socially engineered malware. Subsequent reports will examine phishing and exploit protection.

Socially engineered malware is disguised and/or hidden within another software package so that when a user is enticed to download and install the software, the malware is installed as well. Socially engineered malware attacks pose one of the largest risks to individuals and organizations alike by threatening to compromise, damage or expose sensitive information. With over 50% of malware delivered via the web, protecting against these threats requires more sophisticated techniques and resources and is driving the evolution of security products at the desktop level.

During July and August, 2009 NSS Labs performed the industry's most real-world test of anti-virus / endpoint protection suites against socially engineered malware. NSS Labs' Live Testing measures products against the most current threats as a user would experience them: not against stale or questionable samples in a closed lab environment, like other tests. The results presented here are based upon empirically validated evidence gathered during 17 days of 24x7 testing, performed every 8 hours, over 59 discrete test runs, each one adding fresh new malware URLs. Each product was updated to the most current version available at the time testing began, and allowed access to the live Internet during the entire course of the test.

Key Findings

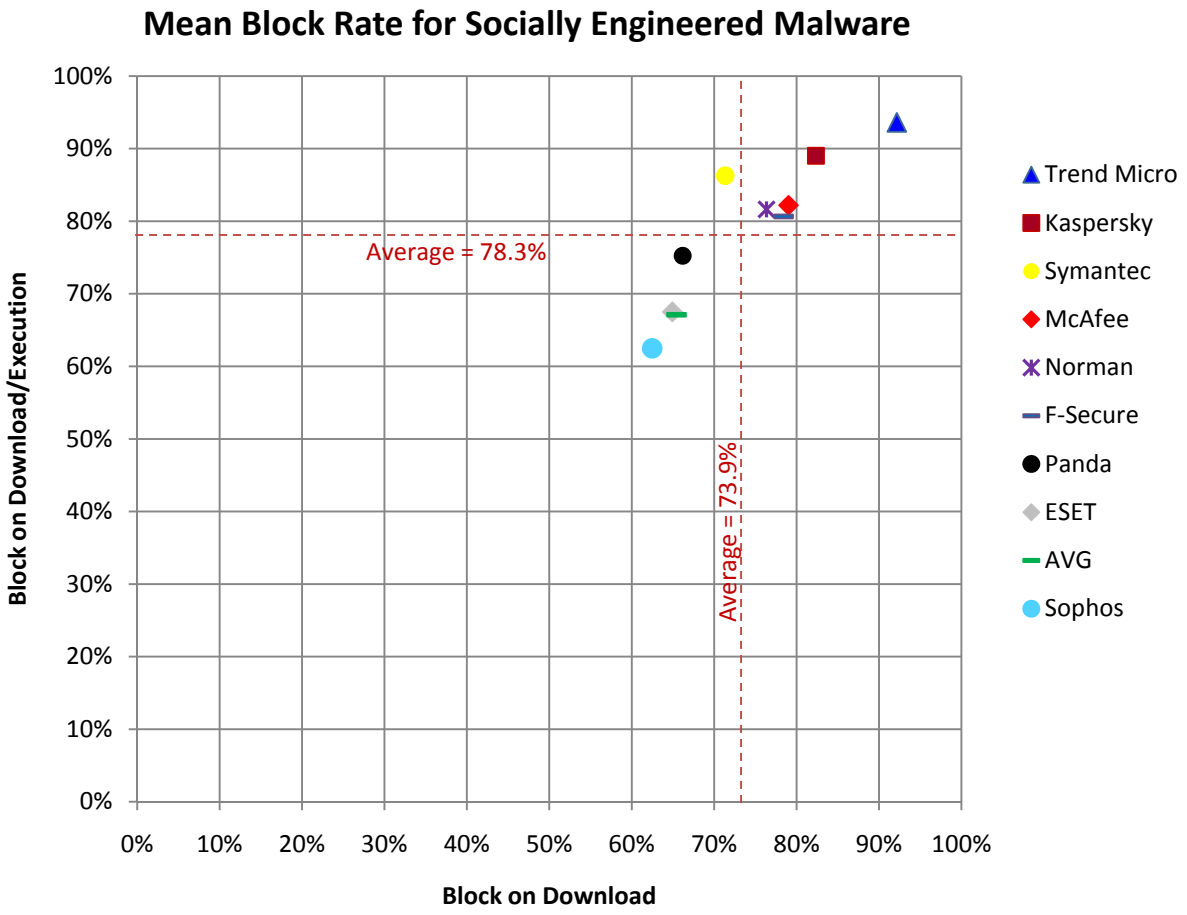
- In-the-cloud reputation systems boosted protection significantly on average
- Trend Micro achieved the best download and execution protection with 93.6% overall
- Kaspersky ranked #2 in download and execution protection with 89.0% overall
- Symantec's behavioral protection excelled, making up for lower protection in the download phase.
- While McAfee technically ranked #4, their exceptionally short time to block should be commended.

Protection over Time

The table and following chart summarize two important factors of total protection on the **web-based malware attack vector**. 'Caught on download' prevents malware off the machine. For malware that made it past this first line of defense, we also measured the percentage 'caught on execution.' The total consists of both download and execution layer protection.

Product	Caught Initially on Download	Caught Subsequently on Execution	Total
Trend Micro	92.2%	1.5%	93.6%
Kaspersky	82.4%	6.7%	89.0%
Symantec	71.3%	14.9%	86.3%
McAfee	79.0%	3.2%	82.2%
Norman	76.4%	5.3%	81.6%
F-Secure	78.4%	2.2%	80.7%
Panda	66.2%	9.1%	75.2%
ESET	64.9%	2.6%	67.5%
AVG	65.4%	1.7%	67.1%
Sophos	62.5%	0.0%	62.5%

The following chart depicts the relationship between download, execution, and overall score. Farther up and right is best. The test replicated actual user behavior: by first downloading the malware from the Internet and then executing it. The average block rate on download was 73.9%, and 78.3% overall.



Product Guidance

Rating	Products
Recommend	Trend Micro Kaspersky Symantec
Neutral	McAfee Norman F-Secure
Caution	Panda Eset AVG Sophos

CONTENTS

1 Introduction

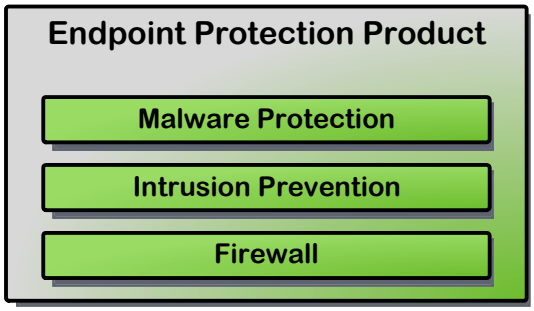
1.1 About This Report

NSS Labs test reports provide IT professionals with empirically validated data and analysis of information security products. This group test measured the security effectiveness of endpoint protection products against socially engineered malware, arguably the largest threat to consumers and corporations alike. It is part of our quarterly recurring test series; and will be updated frequently to provide readers with up-to-date analysis of product suitability and effectiveness.

All testing was conducted independently and without sponsorship. Vendors were provided the test methodology and a chance to ask questions and provide feedback. They were also invited to check and modify the configurations of their products prior to live testing and were contacted immediately upon any apparent malfunction or anomaly.

1.2 Endpoint Protection Products

NSS Labs defines the "Endpoint" as a client workstation where the most common usage is by a user or employee performing business tasks. Endpoint protection is comprised of 3 main functional components. The foundation is a positive security model which limits traffic to only those communications that are explicitly allowed by a client (or personal) firewall. The firewall enforces coarse rules that determine what types of traffic and with whom, are allowed to enter and exit the Endpoint. The other two components are malware protection and intrusion prevention. Both are based on a negative security model (exception based) which utilizes explicit lists defining "bad" content.



The term 'Antivirus' has largely been replaced by anti-malware or 'malware protection' to incorporate protection against a more encompassing array of threats. This usually includes viruses, worms, rootkits, Trojans, spyware, adware, and other rogue applications.

Intrusion prevention refers to the technology that protects a system from exploits against vulnerabilities in the operating system, drivers and user applications. Exploits are attacks against the machine, and can be delivered simply by visiting a malicious or infected website, or by doing nothing at all.

Additional technologies that are being incorporated into endpoint protection products, but are currently not required, include Application White-listing, Data Leak Prevention (DLP), and data encryption. Note: Some white-listing approaches can achieve the desired end goal of protecting against malware, even though they are not considered to be 'anti-malware' products. Larger security vendors have tended to acquire these technologies and are in the process of integrating them into their existing offerings.

1.3 Socially Engineered Malware Threats

Socially engineered malware attacks pose one of the largest risks to individuals and organizations alike by threatening to compromise, damage or expose sensitive information. These are web pages with links to applications that appear to be safe and are designed to fool the user into downloading them, like a software update, screen saver application, video codec upgrade, etc. Additionally, the download link delivers a malicious payload whose content type would lead to execution. Security professionals also refer to these threats using different terms such as consensual or dangerous downloads.

> More than 50% of malware is currently being distributed via the web.

Criminals are taking advantage of the implied trust relationships inherent in social networking sites (e.g. Facebook, MySpace, LinkedIn, etc.) and user-contributed content (e.g. blogs, Twitter, etc.) which allow for rapid publishing and anonymity. Furthermore, the speed at which these threats are 'rotated' to new locations is staggering and poses a significant challenge to security vendors.

Detecting and preventing these threats continues to be a challenge as criminals remain aggressive. Malware proliferation statistics for 2008 and 2009 show an acceleration of the trend. Antivirus researchers report detecting between 15,000 and 50,000 new malicious programs per day, and even as high as "millions per month," according to Kaspersky.[1] Eset cites more than 100,000 new strains of malware daily.[2]

Protecting against these threats requires more sophisticated techniques and resources and is driving the evolution of security products at the desktop level.

1.4 In-the-cloud Services

Security vendors are adding and improving in-the-cloud components to augment on-client detection techniques such as signatures and heuristics. These new URL and file reputation-based malware warning systems offer an additional layer of protection.

These reputation systems leverage client feedback and web crawlers to categorize additional URLs and files; either by adding them to a black or white list, or assigning a score (depending on the vendor's approach). This may be performed manually, automatically, or some combination thereof. The endpoint protection product can then request reputation information from the in-the-cloud systems about specific URLs and files in order to make a determination. Again, this data can be used differently by each vendor's product to warn the user or block the file download or execution.

[1] Kaspersky, Eugene in http://www.examiner.com/x-11905-SF-Cybercrime-Examiner~y2009m7d17-Antimalware-expert-and-CEO-Eugene-Kaspersky-talks-about-cybercrime

[2] http://www.darkreading.com/security/client/showArticle.jhtml?articleID=219501248

2 THE LIVE TEST ENVIRONMENT

The objective of these procedures is to provide a thorough, real-world test of the malware protection in a controlled and verifiable manner. Given the speed with which new threats arrive and spread through the Internet, legacy testing techniques are no longer a relevant measure of a product's capabilities.

- Tests that rely on Wildlist samples or that presume a 100% score objective are not measuring current threat protection. Malware must be fresh and represent the current distribution on the internet, not the malware family taxonomy.
- Tests that do not provide access to the vendor reputation systems during testing unfairly disadvantage more advanced products by denying them a key component in protection.
- Static testing or on-demand scanning generally does not enable the most robust detection techniques. And even dynamic testing alone is insufficient given the increasing reliance on real-time, in-the-cloud reputation systems. A combination of reputation/download and execution analysis provides the best analysis of real-world product capabilities.

Thus, NSS Labs has developed a unique "Live in-the-cloud" testing framework that emulates the experience of average users. This new test methodology focuses on threats currently active on the Internet gathered from NSS Labs' extensive intelligence network. Recurring testing introduces malware into the test harness within a few hours of discovery.

2.1 STAGES OF PROTECTION

Protection from web-based threats can be effectively measured in this unique test environment through a series of procedures that measures the stages of protection. This complex methodology enables NSS Labs engineers to determine which component of the product was responsible for blocking specific threats. The earlier the protection, the more proactive it can be considered.

Stages of Prevention	Samples	Blocked	% Blocked
A. URL/File Access (Reputation)			
B. Download			
C. Execution			
Overall Protection			

Detecting malware at the early stages before it is fully downloaded to the client computer is ideal, and has the ancillary benefit of saving bandwidth which can impact network performance. Another common detection method is to analyze the contents of a file as it is being downloaded from the internet. Malicious files that escape detection during the reputation and download phase can be evaluated during execution. This *dynamic execution* test provides the opportunity for more sophisticated analysis such as sandboxing, heuristics and behavior blocking.

Overall protection is calculated by adding the discrete block percentages A + B + C (see above).

2.2 Time to Protect and Consistency

NSS Labs measures the effectiveness of Anti-Malware products in several important ways. First and most important is examining the effectiveness at any given point in time, which is reported in the Socially Engineered **Malware Protection over Time** chart as well as the Protection Tables. Fluctuations are natural and this view provides a measure of consistency, as well as a visual indicator.

NSS Labs also measures how long it takes for the anti-malware product to add protection from a given malware sample. The **URL Response Histogram** shows proactive 0-hour blocks, total unique blocks, as well as how quickly a product adds protection. This can only be determined through recurring testing of the samples. The **average time to protect** captures the mean time to add protection.

2.3 The Tested Products

The Endpoint Protection products were provided to NSS Labs by the vendors as generally available software (GA), except where noted, as some vendors chose to submit beta products that would be imminently shipping. The following is a current list of the products (Corporate versions) that were tested, sorted alphabetically:

1. AVG Internet Security, version 8.5.364
2. Eset Smart Security 4, version 4.0.437
3. F-Secure Client Security version 8.01
4. Kaspersky Internet Security 2010, version 9.0.0.459
5. McAfee VirusScan Enterprise:8.7.0 + McAfee Site Advisor Enterprise:2.0.0
6. Norman Endpoint protection for Small Business and Enterprise
7. Panda Internet Security 2009, version 14.00.00
8. Sophos Endpoint Protection for Enterprise - Anti-Virus version 7.6.8
9. Symantec Endpoint Protection (for Enterprise), version 11
10. Trend Micro Office Scan Enterprise, version 10

Vendors were allowed to make configuration changes if they felt the default settings were not optimal. No custom settings were used for any of the consumer products.

Once testing began, the product version was frozen, in order to preserve the integrity of the test. Given the nature of Anti-Malware products, virus signatures and definition updates were enabled with whatever default frequency was set by the manufacturer. This test relied upon internet access for the reputation systems and access to live content as well as live updates.

2.4 Client Host Description

All tested browser software was installed on identical virtual machines, with the following specifications:

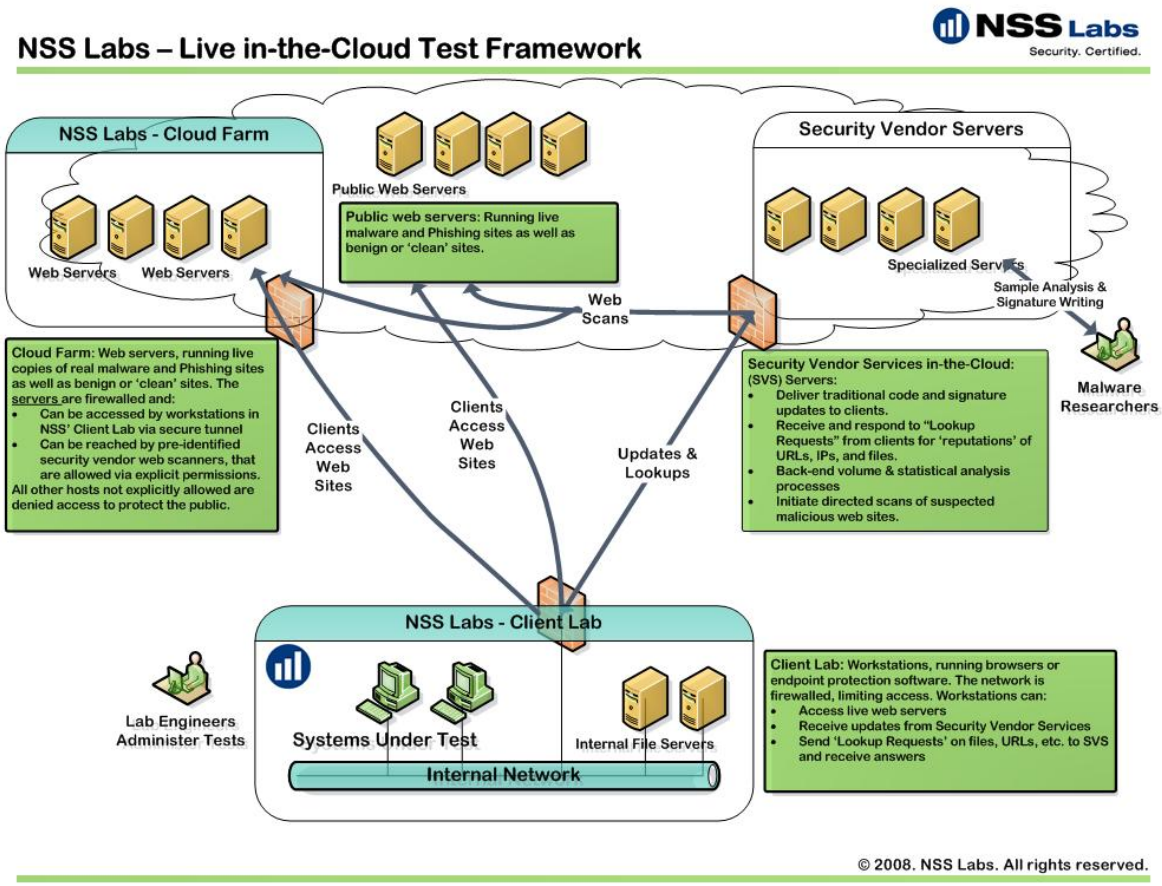
- Microsoft Windows XP SP3
- 1GB RAM
- 15GB HD

Test machines were verified prior to and during the experiment to ensure proper functioning. Browsers were given full access to the Internet so they could visit the actual live sites. Internet Explorer 7 was utilized so that no other reputation services in the browser would interfere with the malware blocking of the product under test.

2.5 Network Description

The Endpoint Protection product is tested for its ability to protect the client in "connected" use cases. Thus, our tests consider and analyze the functionality and performance of Endpoint Protection products over the network using various relevant applications such as e-mail, file server access, webmail etc.

Products under test are subjected to live malware that is introduced into the test network via a URL request made via a web browser. Each threat is archived to ensure proper analysis before, during and after the test. Illegitimate samples are removed from the final test results.



The host system has one network interface card (NIC) and is connected to the network via a 1Ge switch port. The NSS Labs test network is a multi-Gigabit infrastructure based around Cisco Catalyst 6500-series switches (with both fiber and copper Gigabit interfaces).

2.6 Test Composition – Malicious URLs

Data in this report spans a testing period of 17 days, from July 7 through July 24 2009. All testing was performed in our lab in Austin, TX. During the course of the test, we routinely monitored connectivity to ensure the browsers could access the live Internet sites being tested, as well as the AV reputation services in the cloud. Throughout the course of this study, 59 discrete tests were performed (every 8 hours) without interruption for each of the products tested.

The emphasis was on freshness, thus a larger number of sites were evaluated than were ultimately kept as part of the result set. See the methodology for more details.

2.6.1 Total number of malicious URLs in the test

3,243 unique URLs were used to calculate the test results, and a total of 231,351 test results were collected throughout the course of the test.

Live Testing captures current malware on the internet and includes new emerging threats which have not yet been classified by antivirus vendors (approximately 10% have been positively identified as malicious based on behavior) as well as some of the following well known viruses, trojans, rootkits and worms:

- Net-Worm.Win32.Koobface (Worm/Spreading)
- Net-Worm.Win32.Kolab (Worm/Spreading)
- Rootkit.Win32.Banker (Rootkit)
- Trojan.Win32.Vapsup (Browser Modifier/Trojan)
- Backdoor.Win32.SdBot (IRC Bot/C&C)
- Backdoor.Win32.PcClient (HTTP C&C Trojan).

From an initial list of over 17,000 unique new suspicious sites, 4,134 potentially malicious URLs were pre-screened for inclusion in the test, and were available at the time of entry into the test. These were successfully accessed by the browsers in at least one run. We removed samples that did not pass our validation criteria, including those that contained invalid samples. Of the initial 4,134 URLs, ultimately 3,243 URLs passed our post-validation process and are included in the final results – providing a margin of error of 1.58% with a confidence interval of 95%.

2.6.2 Average number of malicious URLs added per day

On average, 324 new validated URLs were added to the test set per day. Although certain days more or less were added as criminal activity levels fluctuated.

2.6.3 Mix of Malware

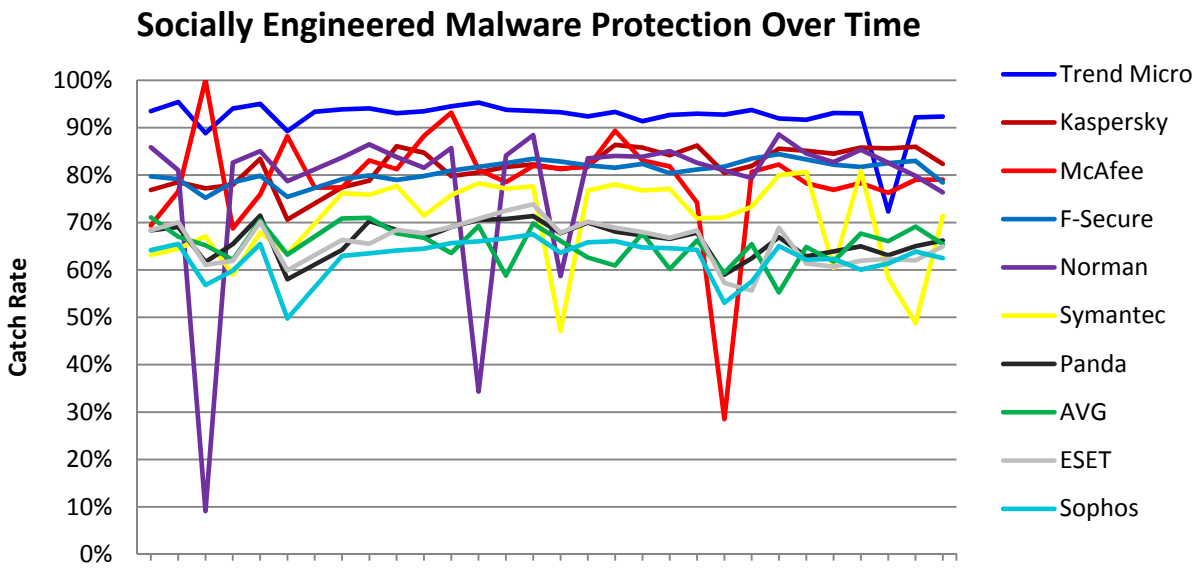
The mixture of URLs used in the test was representative of the threats on the Internet. Care was taken not to overweight any one domain to represent more than 3% of the test set. Thus a number of sites were pruned after reaching their limit.

3 Test Criteria and Results

This test addresses the need for protection while surfing the web, reading web-based email, and downloading files via HTTP. Each malware binary or script is downloaded via HTTP from a live external web site to an internal client running the endpoint protection software. NSS Labs assessed the AV product's ability to block malicious URLs as quickly as we found them on the Internet. We continued testing them every eight hours to determine how long it took a vendor to add protection, if they did at all.

3.1 Blocking URLs with Socially Engineered Malware Over Time

The metrics for blocking individual URLs represent just one perspective. When it comes to daily usage scenarios, users are visiting a wide range of sites which may change quickly. Thus, at any given time, the available set of malicious URLs is revolving, and continuing to block these sites is a key criterion for effectiveness. Therefore, NSS Labs tested a set of live URLs every eight hours. The following tables and graphs show the repeated evaluations of blocking over the course of the entire test period. Each score represents protection at a given point in time.



Note that the average protection percentage will deviate from the unique URL results for several reasons. First, this data includes multiple tests of a URL. So if it is blocked early on, it will improve the score. If it continues to be missed, it will detract from the score. Thus results of individual URL tests were compounded over time to determine protection ratings. This answers the question, "What kind of protection can I expect from an AV product at any given time?"

3.2 Proactive and Execution Protection

Detecting malware at the early stages before it is fully downloaded to the client computer is ideal. On this proactive download measurement, Trend Micro caught significantly more malware on download (92.2%) than the next two competitors, Kaspersky (82.4%) and McAfee (79.0%).

If the malicious file is successfully downloaded, then the goal is to prevent malicious code execution. This is more difficult since the malware has multiple methods at its disposal to evade detection. The 'caught on execution' column in the table below is additive to the download column. At 14.9%, Symantec exhibited by far the best detection on execution, and was able to achieve an overall rank of #3.

AV Product	Caught Initially on Download	Caught Subsequently on Execution	Total
Trend Micro	92.2%	1.5%	93.6%
Kaspersky	82.4%	6.7%	89.0%
Symantec	71.3%	14.9%	86.3%
McAfee	79.0%	3.2%	82.2%
Norman	76.4%	5.3%	81.6%
F-Secure	78.4%	2.2%	80.7%
Panda	66.2%	9.1%	75.2%
ESET	64.9%	2.6%	67.5%
AVG	65.4%	1.7%	67.1%
Sophos	62.5%	0.0%	62.5%

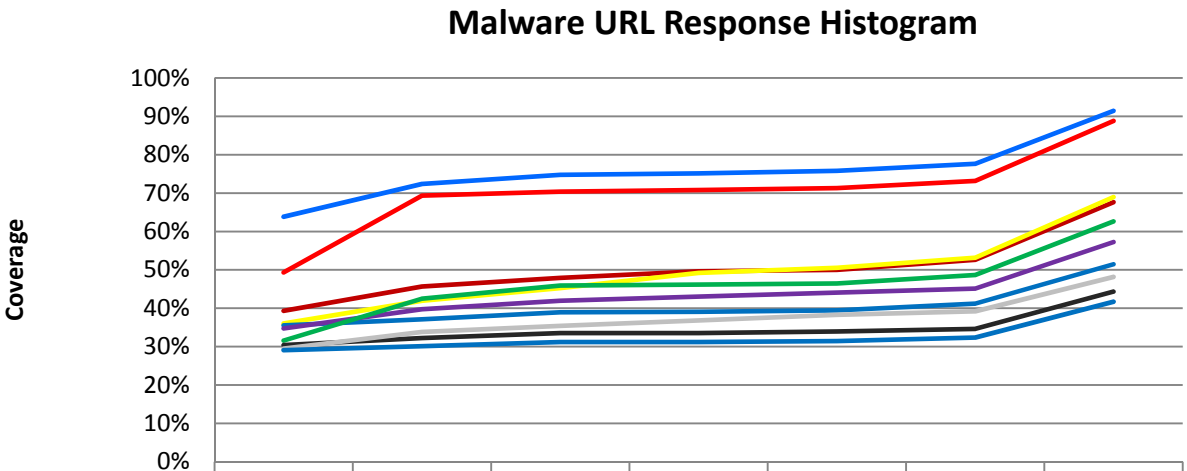
Of the products that incorporated real-time reputation systems, the average net increase in detection due to these systems was 15%. Trend Micro's detection benefitted by 23% on average, while McAfee's Artemis reputation system improved detection by 7% Kaspersky and Panda also incorporated some types of real-time file reputation system as well, but these operated under the hood and did not lend themselves to separate testing. Eset, F-Secure, Norman, and Sophos do not have reputation systems. AVG's Linkscanner is limited to results from search engines, and was not exercised in this test.

3.3 Time to Protect Histogram

The following response time graph shows how long it took the products under test to block the threat once it was introduced into the test cycle. Cumulative protection rates are listed for the 'zero hour', and then the first 5 days. Final protection scores for the URL test duration are summarized under the "Total" column. Generally, at least half of a product's total protection was achieved in the zero hour, and better products had a higher percentage of 0-hour blocks. Notable was Trend Micro's 15% lead over its next competitor.

Ultimately, the results reveal great variations in the abilities of the AV products to protect against socially engineered malware. Trend Micro (64%-91%) and McAfee (49%-89%) protected users from malware far more quickly than any of the other AV products. The two products stand out visually from the pack in the graph below. Extended data analysis reveals all of the other AV products beginning to catch up around day

11 at a protection rate just under 60%, indicating that there are operational differences that account for how rapidly the malware protection is distributed to customers.



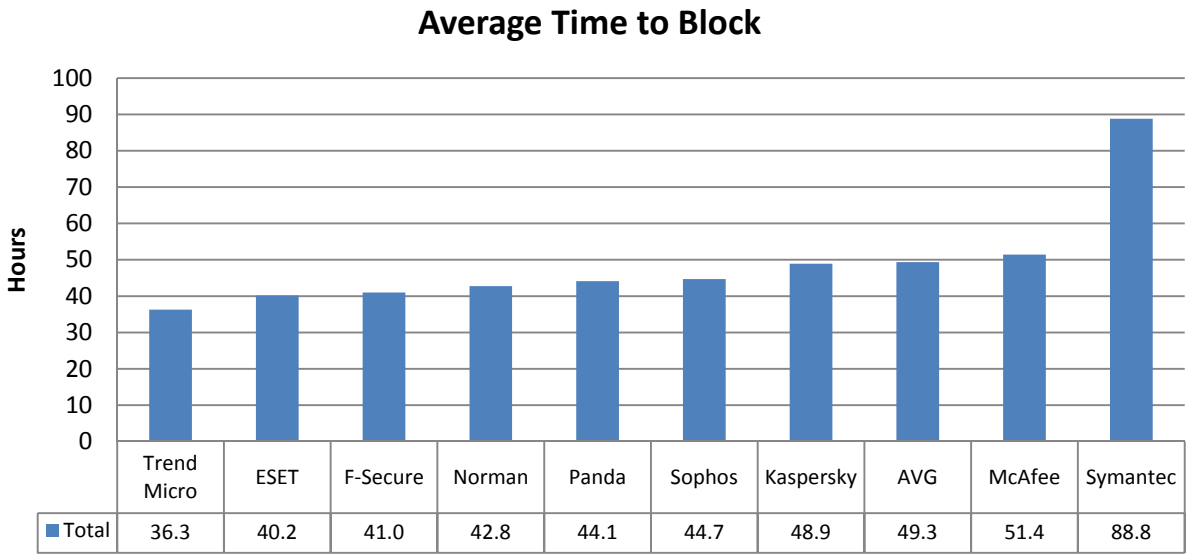
	0-hr	1d	2d	3d	4d	5d	Total
Trend Micro	64%	72%	75%	75%	76%	78%	91%
McAfee	49%	69%	70%	71%	71%	73%	89%
Kaspersky	39%	46%	48%	50%	50%	53%	68%
Symantec	36%	42%	45%	49%	51%	53%	69%
F-Secure	36%	37%	39%	39%	39%	41%	51%
Norman	35%	40%	42%	43%	44%	45%	57%
AVG	32%	43%	46%	46%	46%	49%	63%
Panda	30%	32%	34%	34%	34%	35%	44%
ESET	29%	34%	35%	37%	38%	39%	48%
Sophos	29%	30%	31%	31%	31%	32%	42%

Longevity of malicious sites makes a difference in the score in real life and in our test. Traditional tests do not re-sample protection of malware and this is a key feature of NSS Labs testing. McAfee caught a number of malicious sites via roll-up that disappeared quickly. Although Kaspersky missed many of these long-lived sites initially, McAfee continued to miss them throughout the test. The average time to block is only relevant to the sites that continued to be blocked in repeated testing. Trend caught both short and long-lived sites.

3.4 Average Response Time to Block Malware

In order to protect the most people, a reputation system must be both fast and accurate. This table answers the question: how long on average must a user wait before a visited malicious site is added to the block list? It shows the average time to block a malware site once it was introduced into the test set – *but only if it was blocked during the course of the test*. Unblocked sites are not included.

The value of this table is in providing context for the *overall block rate,* so that if a product blocked 100% of the malware, but it took 240 hours (10 days) to do so, it is actually providing less protection than a product with a 70% overall block rate and an average response time of 10 hours.



The mean time to block a site (if it is blocked at all) is 48.8 hours. Thus, Trend Micro, Eset, F-Secure, Norman, Panda, and Sophos were above average at adding new blocks.

4 PRODUCT ASSESSMENTS

Test data and analysis is summarized below by product. NSS Labs' assessment places a slightly higher importance on the protection over time, since that best reflects long-term averages of real-world usage.

Product	Total Protection Over Time	Unique URLs	0-hour Blocks	Time to Add Blocked Sites
Trend Micro	93.6%	91%	63.8%	36.3
Kaspersky	89.0%	67.6%	39.3%	48.9
Symantec	86.3%	68.9%	36.1%	88.8
McAfee	82.2%	88.8%	49.3%	51.4
Norman	81.6%	57.2%	34.7%	42.8
F-Secure	80.7%	51.4%	35.5%	41.0
Panda	75.2%	44.3%	30.4%	44.1
ESET	67.5%	48%	29.5%	40.2
AVG	67.1%	62.6%	31.6%	49.3
Sophos	62.5%	41.7%	29.1%	44.7

Products are listed in rank order according to their scores and guidance rating of either: Recommend, Neutral, or Caution.

4.1 RECOMMEND

A recommend rating from NSS Labs indicates that a product has performed well and should be used within an Enterprise. Products that earn a recommend rating from NSS Labs deserve strong consideration and should be on every Enterprise's short list during the purchasing process.

Only the top technical products earn a recommend rating from NSS Labs – regardless of market share, company size, or brand recognition.

4.1.1 TREND MICRO OFFICE SCAN ENTERPRISE, VERSION 10

It became obvious from this test that Trend Micro has made considerable strides in adding reputation-based protection to their arsenal. With an over-time protection rating of 93.6%, and a unique malicious site blocking score of 91%, Trend Micro Office Scan was the best at protecting against socially engineered malware. Trend Micro caught 63.8% in the 0-hour, or first test iteration. Malware coverage was added in 36.3 hours on average.

Office Scan Enterprise utilizes standard client-server architecture. The management console was streamlined and intuitive. Administrators should enable Smart Scan, which activates an advanced feature where virus definitions are stored in the Cloud. Office Scan was easy to use and had no issues during the course of our test. Protection was consistently excellent throughout testing.

4.1.2 Kaspersky Internet Security 2010

Coming in second, Kaspersky blocked 89% of the threats during our extended test, with a unique malicious site blocking score of 67.6%. Kaspersky caught 39.3% of the threats in the initial test iteration, and malware coverage was added in 48.9 hours on average.

Kaspersky Internet Security 2010 was easy to use and had no issues during testing. At the request of Kaspersky, NSS Labs set the heuristics to deep scan and disabled the "Limit fragment buffering time" option.

4.1.3 Symantec Endpoint Protection 11 for Enterprises

Symantec Endpoint Protection blocked 86.3% of the threats during our extended test, with a unique malicious site blocking score of 68.9%%. Symantec caught 36.1% of the threats in the initial test iteration. Malware coverage was added within 88.8 hours on average.

Symantec's management console is straightforward and easy to use. Utilizing standard client-server architecture, agents are deployed on to the clients via the management console. Virus definitions can be downloaded directly from the Internet onto clients, or via a central repository that lives on the management server. Firewall policy is deployed from the central management console to the clients.

One observed shortcoming of the Symantec solution is that it manages AV Definitions on a SQL Server Database which is resource intensive. Running continuous tests on the client caused the database to crash multiple times during the single test run. No user notifications were generated on the client machines once the database crashed. Granted, this kind of test is far more demanding on DB lookups than one would expect in the real-world outside of very large organizations. However be sure to size your solution correctly or face possible outages.

4.2 Neutral

A neutral rating from NSS Labs indicates that a product has performed reasonably well and should continue to be used if it is the incumbent within an Enterprise. Products that earn a neutral rating from NSS Labs deserve consideration during the purchasing process.

4.2.1 McAfee VirusScan Enterprise 8.7.0 + McAfee Site Advisor Enterprise 2.0.0

McAfee VirusScan & SiteAdvisor blocked 82.2% of the threats during our extended test, with a unique malicious site blocking score of 88.8%%. McAfee caught 49.3% of the threats in the initial test iteration. Malware coverage was added within 51.4 hours on average.

McAfee VirusScan & SiteAdvisor experienced one major drop-off of protection during testing. Without that temporary setback, it is likely McAfee would have achieved a *recommended* rating.

McAfee EPO is one of the most difficult central management systems to configure. However, once the EPO is successfully deployed and the policies are defined clients do not have any issues. We experienced a hiccup where a client received the wrong policy update from the EPO, and as a result McAfee's web reputation system blocked all unrated sites. This was quickly remediated by pushing a new policy.

4.2.2 Norman Endpoint protection for Small Business and Enterprise

Norman Endpoint Protection blocked 81.6% of the threats during our extended test, with a unique malicious site blocking score of 57.2%. Norman caught 34.7% of the threats in the initial test iteration. Malware coverage was added within 42.8 hours on average.

Norman Endpoint Protection was fairly easy to use and had no stability or performance issues during testing. However, we did notice periodic drop-offs of coverage which negatively impacted Norman's score. Norman's biggest drawback is that it waits until malware attempts to write to the disk before notifying users.

4.2.3 F-Secure Client Security, version 8.01

F-Secure Client Security blocked 80.7% of the threats during our extended test, with a unique malicious site blocking score of 51.4%. F-Secure caught 35.5% of the threats in the initial test iteration. Malware coverage was added within 41 hours on average.

F-Secure Client Security can be deployed as a standalone solution or via F-Secure Policy Manager. F-Secure was easy to use and had no issues during testing. Protection was consistent, if a bit shy of top protection throughout the test.

4.3 Caution

A caution rating from NSS Labs indicates that a product has performed poorly. Organizations using one of these products should review their security posture and other threat mitigation factors, including possible alternative configurations and replacement. Products that earn a caution rating from NSS Labs should not be short-listed or renewed.

4.3.1 Panda Internet Security 2009, v14

Panda Internet Security blocked 75.2% of the threats during our extended test, with a unique malicious site blocking score of 44.3%. Panda caught 30.4% of the threats in the initial test iteration. Malware coverage was added within 44.1 hours on average.

Panda Internet Security can be managed as a standalone solution or via Panda's AdminSecure management console. Panda required frequent reboots when high risk malware was found. Fortunately, Panda's catch rate was not dramatically reduced if reboot was delayed. The product is easy to use and had no issues during testing.

4.3.2 Eset Smart Security 4

Eset caught 67.5% of the malware downloads during our extended test, with a unique malicious site blocking score of 48%. Eset caught 29.5% of the threats in the initial test iteration. Malware coverage was added within 40.2 hours on average.

Eset Smart Security 4 can be managed as a standalone solution or via Eset's Remote Administrator management console. Smart Security was easy to use as a standalone solution, but complicated and confusing when managed by Remote Administrator. As a result, NSS opted to use the Standalone solution. The product provided consistently poor protection throughout testing.

4.3.3 AVG Internet Security Suite 8.5.364

AVG caught 67.1% of the malware downloads during our extended test, with a unique URL blocking score of 62.6%. AVG caught 31.6% of the threats in the initial test iteration. Malware coverage was added within 49.3 hours on average.

During our pre-test preparation, we found AVG repeatedly just stopped working until we increased memory from 1024 MB to 1536 MB. And when AVG's service fails, it does not recover/restart automatically – there is no warning and users are completely unprotected. The AVG Tray icon must always be visible in Window's System Tray in order for the AV engine to scan Malware. If the icon is not in the system tray, AVG offers no protection.

4.3.4 Sophos Endpoint Security / Anti-Virus 7.6.8

Sophos caught 62.5% of the malware downloads during our extended test, with a unique URL blocking score of 41.7%. Sophos caught 29.1% of the threats in the initial test iteration. Malware coverage was added within 44.7 hours on average.

Sophos Endpoint Security (which includes Anti-Virus 7.6.8) can be managed as a standalone solution or via Sophos Enterprise Console. Neither solution was easy to manage, however we did find the standalone option a bit less difficult. Sophos provided consistently poor protection throughout testing and scored last in 3 of 4 categories.

5 Appendix: Test Procedures

The purpose of the test was to determine how well the tested AV products protect users from the most important malware threat on the Internet today. A key aspect was the timing. Given the rapid rate and aggressiveness with which criminals propagate and manipulate the malicious web sites, a key objective was to ensure that the "freshest" sites possible were included in the test.

NSS Labs has developed a unique proprietary "Live Testing" harness and methodology. On an ongoing basis NSS Labs collects web-based threats from a variety of sources, including partners and our own servers. Potential threats are vetted algorithmically before being inserted into our test queue. Threats are being inserted and vetted continually 24x7. Note: unique in this procedure is that NSS Labs validates the samples before and after the test. Actual testing of the threats proceeded every four hours and starts with validation of the site's existence and conformance to the test definition.

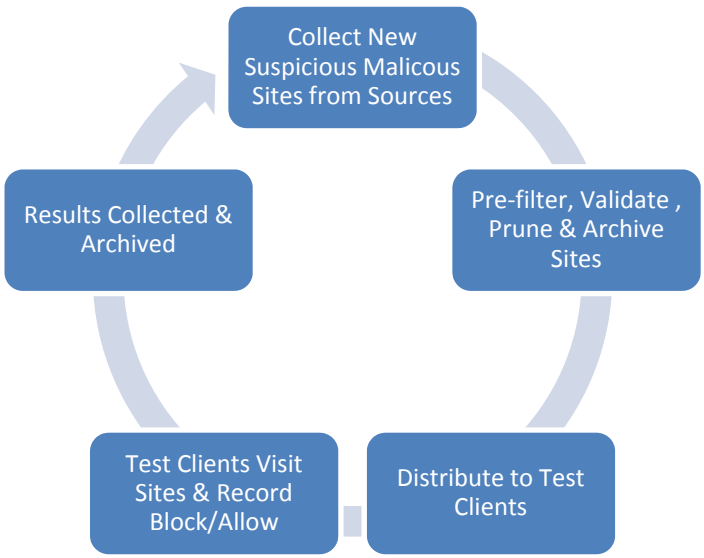
All tests were executed in a highly controlled manner, and results were meticulously recorded and archived at each interval of the test.

5.1 Test Duration

NSS Labs' Live Malware test was performed continuously (24x7) for 11 days. Throughout the duration of the test, new URLs were added as they were discovered.

5.1.1 Test Frequency

Over the course of the test, each URL is run through the test harness every eight hours, regardless of success or failure, NSS Labs continues to attempt to download a malware sample with the web browser for the duration of the test.



5.2 Sample sets for malware URLs

Freshness of malware sites is a key attribute of this type of test. In order to utilize the freshest most representative URLs, NSS Labs receives a broad range of samples from a number of different sources.

5.2.1 Sources

First, NSS Labs operates its own network of spam traps and honeypots. These email accounts with high-volume traffic yield thousands of unique emails, and several hundred unique URLs per day. NSS Labs' continuously growing archive of Malware and Viruses that contains Gigabytes of confirmed samples. In addition, NSS Labs maintains relationships with other independent security researchers, networks, and security companies, which provide access to URLs and malicious content. Sample sets contain malicious URLs distributed via: SPAM, social networks, and malicious websites. Exploits containing malware payloads (exploits + malware) a.k.a. "clickjacking" or "drive-by downloads" were excluded from the test. Every effort was made to consider submissions that reflect a real-world distribution of malware, categorically, geographically, and by platform.

In addition, NSS maintains a collection of 'clean URLs' which includes such sites as Yahoo, Amazon, Microsoft, Google, NSS Labs, major banks, etc. Periodically clean URLs were run through the system to verify AV products were not over-blocking.

5.3 Catalog URLs

New sites were added to the URL Consideration Set as soon as possible. The date and time each sample is introduced is noted. Most sources were automatically and immediately inserted, while some methods require manual handling and can be processed in under 30 minutes. All items in the consideration set were cataloged with a unique NSS Labs ID, regardless of their validity. This enabled us to track effectiveness of sample sources.

5.4 Confirm Sample Presence of URLs

Time is of the essence since the test objective is to test the effectiveness against the 'freshest' possible malware sites. Given the nature of the feeds and the velocity of change, it is not possible to validate each site in depth before the test, since the sites could quickly disappear. Thus, each of the test items was given a cursory review to verify it was present and accessible on the live Internet.

In order to be included in the Execution Set, URLs must be live during the test iteration. At the beginning of each test cycle, the availability of the URL is confirmed by ensuring that the site can be reached and is active (e.g. a non-404 web page is returned).

This validation occurred within minutes of receiving the samples from our sources. Note: These classifications are further validated after the test and URLs were reclassified and/or removed accordingly.

5.4.1 Archive active URL content

The active URL content was downloaded and saved to an archive server with a unique NSS ID number. This enables NSS Labs to preserve the URL content for control and validation purposes.

5.5 Download & Execute

A customized client automation utility requests each of the URLs deemed 'present' via each of the products in the test. NSS records whether or not the malware was allowed to be downloaded, and if the download attempt triggered a warning from the product's malware protection. *Note: for this test, the reputation and file download scores are summarized together.*

5.5.1 Web Reputation Scoring

The resulting response is recorded as either "Allowed" or "Blocked and Warned."

- Success: NSS Labs defines "success" based upon a product *successfully* preventing malware from being downloaded, and *correctly* issuing a warning.
- Failure: NSS Labs defines a "failure" based upon a product *failing* to prevent the malware from being downloaded and *failing* to issue a warning.

5.5.2 HTTP File Download Scoring

The resulting response is recorded as either "Allowed" or "Blocked and Warned."

- Success: NSS Labs defines "success" based upon a product *correctly* issuing a warning either during download or immediately after malware is downloaded.
- Failure: NSS Labs defines a "failure" based upon a product *failing* to prevent the malware from being downloaded and *failing* to issue a warning.

5.5.3 File Execution Scoring

The resulting response is recorded as either "Allowed" or "Blocked and Warned."

- Success: NSS Labs defines "success" based upon a product *correctly* issuing a warning during file execution.
- Failure: NSS Labs defines a "failure" based upon a product *failing* to prevent the malware from being executed and *failing* to issue a warning.

5.6 Pruning

Throughout the test, lab engineers review and prune out non-conforming URLs and content from the test execution set. e.g. a URL that was classified as malware that has been replaced by the web host with a generic splash page will be removed from the test.

If a URL sample becomes unavailable for download during the course of the test, the sample will be removed from the test collection for that iteration. NSS Labs continually verifies each sample's presence (availability for download) and adds/removes each sample from the test set accordingly. Should a malware sample be

unavailable for a test iteration and then become available again for a subsequent iteration, it will be added back into the test collection. Unavailable samples are not included in calculations of success or failure by a web browser.

5.7 POST-TEST VALIDATION

Post-test validation enables NSS Labs to reclassify and even remove samples which were either not malicious or not available before the test started. NSS Labs used two different sandboxes to prune and validate the malware (Sunbelt's CW Sandbox and Norman Analyzer), and further validated suspicious samples using multiple antivirus scanners if necessary.

6 Appendix C: Test Infrastructure

Special thanks go to our test infrastructure partners who provide much of the equipment, software, and support that make this testing possible: