# CONSUMER AV / EPP COMPARATIVE ANALYSIS

## Exploits – Evasion Defenses

**2012 – Randy Abrams, Nathan Taylor**

## Tested Vendors

Avast, AVG, Avira, ESET, F-Secure, Kaspersky, McAfee, Microsoft, Norman, Norton, Panda, Total Defense, Trend Micro

## Overview

As security products improve their abilities to detect cyber threats, criminals react by attempting to conceal malware by packaging it with a variety of technologies. This group test report analyzes some of the common methods used by cyber criminals to circumvent or evade detection by consumer anti-malware or Endpoint Protection Products (EPP).

Cyber criminals do not just develop one attack and move on. Rather, they seek to make their software usable for as long as possible. Evasion techniques allow known threats to circumvent detection by security products. Research indicates that cyber criminals perform their own testing and make strategic use of evasion techniques. Automated encoding schemes used to evade detection are features included in common commercial exploit kits.

NSS Labs tested 13 popular endpoint security suites to measure their effectiveness in protecting Windows computers against exploits. All of the vulnerabilities exploited during this test have been publicly available for months (if not years) prior to the test, and have also been observed in use on the Internet.

Understanding which products have coverage for the various evasion techniques is an important indicator of product quality of which consumers need to be aware. Consumers, and enterprises that have implemented a bring your own device (BYOD) policy, who seek protection from attacks against desktop PCs and laptops should closely examine results from this test.

| Product | HTTP Evasion & Compression | HTML Obfuscation | Payload Encoding | File Compressors (Download) | Executable Packers (Download) | Executable Packers (Execute) | Layered Evasions | Overall Combined |
|---|---|---|---|---|---|---|---|---|
| Microsoft | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% |
| ESET | 100% | 100% | 100% | 100% | 75% | 75% | 100% | 93% |
| Kaspersky | 100% | 100% | 100% | 100% | 75% | 75% | 100% | 93% |
| Avira | 100% | 100% | 100% | 100% | 25% | 100% | 100% | 89% |
| Avast | 100% | 100% | 100% | 0% | 100% | 100% | 100% | 86% |
| AVG | 100% | 100% | 100% | 0% | 100% | 100% | 100% | 86% |
| McAfee | 100% | 100% | 100% | 0% | 100% | 100% | 100% | 86% |
| Norton | 100% | 100% | 100% | 0% | 100% | 100% | 100% | 86% |
| Norman | 100% | 100% | 100% | 0% | 75% | 100% | 100% | 82% |
| Panda | 100% | 100% | 100% | 100% | 25% | 25% | 100% | 79% |
| F-Secure | 100% | 100% | 100% | 0% | 0% | 100% | 100% | 71% |
| Total Defense | 100% | 100% | 100% | 0% | 0% | 100% | 100% | 71% |
| Trend Micro | 100% | 100% | 100% | 0% | 0% | 100% | 100% | 71% |

**Figure 1 - Evasion Block Rate**

The NSS Labs 2012 Exploit Protection Comparative Analysis Report has already demonstrated weaknesses in the abilities of most security products to detect a wide range of exploits. Evasion techniques provide an additional means for attackers to deliver the same exploits to the endpoint, and EPP products have traditionally proved poor at handling such techniques. However, this test indicates that vendors are beginning to take this threat seriously, since anti-evasion protection is greatly improved compared with previous tests.

The chart above shows ranking in terms of the absolute number of test cases passed. It should be noted that products that block on execution, but not on download, provide better protection for consumers than products that miss packed or compressed samples on execution. The chart below lists the products effective protection against evasions on execution.

| Product | HTTP Evasion & Compression | HTML Obfuscation | Payload Encoding | Executable Packers (Execute) | Layered Evasions | Overall Combined |
|---|---|---|---|---|---|---|
| Microsoft | 100% | 100% | 100% | 100% | 100% | 100% |
| Avast | 100% | 100% | 100% | 100% | 100% | 100% |
| AVG | 100% | 100% | 100% | 100% | 100% | 100% |
| McAfee | 100% | 100% | 100% | 100% | 100% | 100% |
| Norton | 100% | 100% | 100% | 100% | 100% | 100% |
| Norman | 100% | 100% | 100% | 100% | 100% | 100% |
| Avira | 100% | 100% | 100% | 100% | 100% | 100% |
| F-Secure | 100% | 100% | 100% | 100% | 100% | 100% |
| Total Defense | 100% | 100% | 100% | 100% | 100% | 100% |
| Trend Micro | 100% | 100% | 100% | 100% | 100% | 100% |
| ESET | 100% | 100% | 100% | 75% | 100% | 95% |
| Kaspersky | 100% | 100% | 100% | 75% | 100% | 95% |
| Panda | 100% | 100% | 100% | 25% | 100% | 85% |

**Figure 2 - Evasion Block Rate (on Execution)**

## Key Findings

- Most vendors have dramatically improved their coverage for the basic evasions used in our testing as compared to NSS Labs testing in 2010.
- Executable compressors are still problematic for some vendors.
- Most vendors are not scanning standard compressors on download, and some are not scanning compressed executable payloads on download.
- Microsoft exhibited the strongest anti-evasion capabilities.

## Recommendations

- Since patching helps to mitigate the impact of evasions, consumers should always keep their software current in addition to deploying endpoint security.
- Consumers using products that do not inspect compressed software on download should contact their vendors for assistance in configuring their software to scan compressed files on download.
- The most current browsers help block some malicious downloads, and should be used in favor of older browsers.

# Table of Contents

**Overview** ..... **1**
Key Findings ..... 3
Recommendations ..... 3

**Analysis** ..... **5**
HTTP Evasion ..... 5
HTML Obfuscation ..... 6
HTTP Compression ..... 7
Payload Encoding ..... 7
Payload Compression ..... 8
Payload Packing ..... 8
Layered Evasions ..... 9

**Test Methodology** ..... **10**
The Tested Products ..... 10
Client Host Description ..... 11

# Table of Figures

*Figure 1 –Evasion Block Rate* ..... *2*
*Figure 2 –Evasion Block Rate (on Execution)* ..... *3*
*Figure 3 - HTTP Evasion Block Rate* ..... *6*
*Figure 4 - HTTP Obfuscation Block Rate* ..... *6*
*Figure 5 - HTTP Compression Block Rate* ..... *7*
*Figure 6 - Payload Encoding Block Rate* ..... *7*
*Figure 7 - Payload Compression Block Rate* ..... *8*
*Figure 8 –Payload Packing Block Rate (download)* ..... *9*
*Figure 9 –Payload Packing Block Rate (execution)* ..... *9*
*Figure 10 - Layered Evasions Block Rate* ..... *9*

# Analysis

Evasion is accomplished by obfuscating exploits and malware using encryption, packing or compression techniques in an attempt to thwart detection. An exploit that is detected by a security product can be modified by an evasion technique to bypass the protection mechanism and reach the target – if the intermediary security product does not have the appropriate anti-evasion capability. If a product does not detect a particular exploit, it will not detect the evaded exploit either (in which case evasion was redundant).

It is important to understand that unlike missing a single malware sample, the impact of missing any single evasion technique is an order of magnitude more impactful to the security effectiveness delivered by any product. Missing a single evasion technique exposes the consumer to that complete class of evaded attacks. Thus, any number of exploits or malware can be easily modified to slip past security products. For example, a single HTTP obfuscation evasion can be applied to multiple different HTTP-based attacks that would have been blocked by their respective individual signatures. If the security product does not normalize obfuscated HTTP traffic, however, all 30 attacks will pass through to the target undetected.

Evasions can also be combined or layered. This must be done in specific ways that would allow the attack to be restored when it reaches the target so it can be delivered properly. An attacker (or tester) cannot simply mix and match any and all evasion techniques. While this makes the attacker's work somewhat more difficult, it is still a relatively trivial problem, since in such asymmetrical situations time is on the attacker's side. In this round of testing, NSS Labs added layered evasions to the test.

For each evasion, it is verified that a standard Web browser (such as Internet Explorer) is capable of rendering the results of the evasion. Before testing evasions NSS engineers ensured that the baseline exploits were detected. Thus, the test does not reflect the ability to catch the exploit itself, but rather the evasion techniques used to obfuscate it. For information about exploit detection, please consult the NSS Labs 2012 Exploit Protection Comparative Analysis Report.

During the test, NSS engineers applied a wide range of common evasion techniques currently used by attackers in the wild, including encoding, compression, packing and obfuscation. In all, this test evaluates 29 different evasions in 33 tests across five distinct categories, plus the layered test. The details are listed below by evasion category.

Specific evasion results and names are not detailed in this report, but can be provided to NSS clients as required via inquiry calls with NSS Labs' analysts.

## HTTP Evasion

Web browsers request URLs from servers over HTTP using the ASCII character-set. HTTP URL encoding replaces unsafe non-ASCII characters with a "%" followed by two hexadecimal digits. Web servers and clients understand how to decode the request and responses. However, this mechanism can be abused to circumvent protection that is looking to match specific strings of characters. Other methods include chunked encoding and header folding.

Chunked encoding allows the server to break a document into smaller chunks and transmit them individually. The server needs only to specify the size of each chunk before it is transmitted and then indicate when the last chunk

has been transmitted. Since chunked encoding intersperses arbitrary numbers (chunk sizes) with the elements of the original document, it can be used to change the appearance of the original document significantly as observed "on the wire". In addition, the server can choose to break the document into chunks at arbitrary points. This makes it difficult for simple pattern matching systems to reliably identify the original HTML document from the raw data on the network.

HTTP encoding is well supported by all the vendors tested, with all products passing the test.

| Product | HTTP Encoding |
|---|---|
| Avast | 100% |
| Avira | 100% |
| AVG | 100% |
| ESET | 100% |
| F-Secure | 100% |
| Kaspersky | 100% |
| McAfee | 100% |
| Microsoft | 100% |
| Norman | 100% |
| Norton | 100% |
| Panda | 100% |
| Total Defense | 100% |
| Trend Micro | 100% |

**Figure 3 - HTTP Evasion Block Rate**

## HTML Obfuscation

Recognizing malicious HTML documents is becoming increasingly important when protecting the enterprise. Malicious HTML documents exploit flaws in common web browsers, browser plug-ins, and add-ons to gain control of the client system and silently install malware such as trojans, rootkits, and key loggers.

Therefore, it is becoming increasingly important that security products charged with protecting end systems must correctly interpret HTML documents. Historically security products used simple pattern matching systems with very little semantic or syntactic understanding of the data they were analyzing. This left them vulnerable to evasion through use of redundant, but equivalent, alternative representations of malicious documents.

This test suite uses a number of malicious HTML documents that are transferred from server to client. Each malicious HTML document is served with a different form of obfuscation, including:

- The UTF-16 character set specifies a 2-byte sequence for most characters and a 4-byte sequence for the others (a small percentage). Recoding an HTML document in UTF-16 significantly changes its appearance. A document that contains just the ASCII subset of characters will appear to have a null byte between every one of the original characters. There are also two different forms of the UTF-16 encoding depending on whether the null high byte comes first (big-endian) or second (little-endian). This test uses big-endian byte ordering.
- The UTF-32 character set specifies a 4-byte sequence. Like the UTF-16 character set encoding there are two variations (big-endian and little-endian) and this test case uses big-endian byte ordering.

| Product | HTTP Encoding |
|---|---|
| Avast | 100% |
| Avira | 100% |
| AVG | 100% |
| ESET | 100% |
| F-Secure | 100% |
| Kaspersky | 100% |
| McAfee | 100% |
| Microsoft | 100% |
| Norman | 100% |
| Norton | 100% |
| Panda | 100% |
| Total Defense | 100% |
| Trend Micro | 100% |

**Figure 4 - HTTP Obfuscation Block Rate**

- The UTF-7 character set encodes most ASCII characters as themselves. However, in addition to recoding non-English characters as other encodings do, it also recodes many punctuation symbols, including many of the symbols that are important to the HTML specification. Therefore, recoding an HTML document in UTF-7 significantly changes its appearance.

All vendors properly handled the HTML obfuscation evasion test cases in this test. This is a marked improvement from the NSS Labs test in 2010, where 40% of the products scored less than 60%.

## HTTP Compression

Per RFC 2616, the HTTP protocol allows the client to request, and the server to use, multiple compression methods. These compression methods not only improve performance in many circumstances, they completely change the characteristic size and appearance of HTML documents.

Furthermore, small changes in the original document can greatly change the final appearance of the compressed document. This property of these algorithms could be used to obfuscate hostile content for the purpose of evading detection. The deflate compression method is a Lempel-Ziv coding (LZ77), specified in RFC 1951. The gzip compression method is specified in RFC 1952.

| Product | HTTP Encoding |
|---|---|
| Avast | 100% |
| Avira | 100% |
| AVG | 100% |
| ESET | 100% |
| F-Secure | 100% |
| Kaspersky | 100% |
| McAfee | 100% |
| Microsoft | 100% |
| Norman | 100% |
| Norton | 100% |
| Panda | 100% |
| Total Defense | 100% |
| Trend Micro | 100% |

**Figure 5 - HTTP Compression Block Rate**

HTTP Compression appears to be generally understood and supported by the vendors in this test, with all products passing this test.

## Payload Encoding

Payloads returned to the client can be encoded using a number of techniques. While the principle is similar to HTTP encoding, a diverse range of XOR-based functions can be applied.

In 2010 none of the products scored 100% in this category and most products scored less than 40%. In this latest round of testing, all of the products tested were able to recognize and deal with these encoding types

| Product | HTTP Encoding |
|---|---|
| Avast | 100% |
| Avira | 100% |
| AVG | 100% |
| ESET | 100% |
| F-Secure | 100% |
| Kaspersky | 100% |
| McAfee | 100% |
| Microsoft | 100% |
| Norman | 100% |
| Norton | 100% |
| Panda | 100% |
| Total Defense | 100% |
| Trend Micro | 100% |

**Figure 6 - Payload Encoding Block Rate**

## Payload Compression

This section includes obfuscation methods for compressing payloads that can be used legitimately to reduce bandwidth consumption. Many different compression utilities are in circulation and use, posing interesting challenges to the AV industry.

All of the products tested were able to block threats when decompressed, however some products allow the download of compressed payloads without checking the content. The choice of a default configuration that does not inspect compressed downloads is typically a trade off between performance and security. NSS Labs believes the average consumer is best served if malicious downloads inside of compressed files are blocked by default, and this was implemented by only 5 out of 13 of the products tested.

| Product | Compression |
|---|---|
| Avira | 100% |
| ESET | 100% |
| Kaspersky | 100% |
| Microsoft | 100% |
| Panda | 100% |
| Avast | 0% |
| AVG | 0% |
| F-Secure | 0% |
| McAfee | 0% |
| Norman | 0% |
| Norton | 0% |
| Total Defense | 0% |
| Trend Micro | 0% |

**Figure 7 - Payload Compression Block Rate**

## Payload Packing

This section includes obfuscation methods for compressing and packing payloads that can be used legitimately to reduce bandwidth consumption. Utilities such as gzip and winzip can also be used to create self-extracting executables. Hundreds of different packers are in circulation and use, posing a significant problem to the AV industry.

Some of the tested products were able to block the execution of runtime-compressed packages but did not block the malicious files at download. Results are shown both for the ability to block on download and to block on execution. Typically a failure to block on download is a configuration choice designed to boost product performance at the expense of maximum security. The trade off may be an appropriate choice for a skilled administrator to make. However, NSS Labs believes that the average consumer is better protected by blocking at download. Eight of the products failed to block at least one packed file on download and three products blocked none of the packed files on download.

RLPack, a runtime executable file compressor, proved problematic for ESET, Kaspersky and Panda. Panda was the only product to miss 3 out of the 4 runtime compressors when the payload was executed.

| Product | Payload Packing Block on download |
|---|---|
| Avast | 100% |
| AVG | 100% |
| McAfee | 100% |
| Microsoft | 100% |
| Norton | 100% |
| ESET | 75% |
| Kaspersky | 75% |
| Norman | 75% |
| Avira | 25% |
| Panda | 25% |
| F-Secure | 0% |
| Trend Micro | 0% |
| Total Defense | 0% |

Figure 8 - Payload Packing Block Rate (download)

| Product | Payload Packing Block on execute |
|---|---|
| Avast | 100% |
| AVG | 100% |
| Avira | 100% |
| F-Secure | 100% |
| McAfee | 100% |
| Microsoft | 100% |
| Norman | 100% |
| Norton | 100% |
| Total Defense | 100% |
| Trend Micro | 100% |
| ESET | 75% |
| Kaspersky | 75% |
| Panda | 25% |

Figure 9 - Payload Packing Block Rate (execution)

## Layered Evasions

This section includes combinations of techniques in an attempt to further evade detection by security products. Four different attempts to circumvent detection were made using as many as 4 different layers of obfuscation.

None of the tested products exhibited any problems in dealing with multiple layers of obfuscation. This is a significant improvement over the 2010 NSS Labs test where even single layers of evasion were problematic for some products. Today the ability to decode a variety of evasions is standard in the products NSS Labs tested.

| Product | HTTP Encoding |
|---|---|
| Avast | 100% |
| Avira | 100% |
| AVG | 100% |
| ESET | 100% |
| F-Secure | 100% |
| Kaspersky | 100% |
| McAfee | 100% |
| Microsoft | 100% |
| Norman | 100% |
| Norton | 100% |
| Panda | 100% |
| Total Defense | 100% |
| Trend Micro | 100% |

Figure 10 - Layered Evasions Block Rate

# Test Methodology

### Methodology Version: Endpoint Protection Test Methodology v3.0

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

This test report is one of a series of several tests in our "**Whole Product Test**" series. The scope of this particular report is limited to **Host Intrusion Prevention** vs. **Exploits**. No Zero-Day exploits against unknown vulnerabilities were included in this test.

Other tests in this series include:

1. **Socially-engineered Malware –** Web-based malware that tricks users into downloading and installing it.
2. **Host Intrusion Prevention –** Exploits against vulnerable client applications.
3. **Evasion Defenses** – **This report** Preventing attempts to circumvent AV and HIPS
4. **Anti-Malware (classic)** – Email, Network Share, and USB infection vectors
5. **Live Web-Based "Drive-By" Exploits** – Live testing using Internet-borne exploits that insert malware payloads. Also known as "Drive-by" or "non-consensualll downloads"
6. **Performance** – Increase in Memory, CPU, Boot Time, and Application Load Time.

## The Tested Products

The following is a current list of the products that were tested and are sorted alphabetically:

1. Alwil Avast Pro Antivirus 7 7.0.1466
2. AVG Internet Security 2012 2012.0.2197
3. Avira Internet Security 2012 12.0.0.1127
4. ESET Smart Security 5 5.2.9.1
5. F-Secure Agent 1.57 Build 191, CUIF 10.01 build 32329, DAAS2 1.10 build 299
6. Kaspersky Internet Security 2012 12.0.0.374
7. McAfee Internet Security 11
8. Microsoft Security Essentials 4.0.1526.0
9. Norman Security Suite 9.00
10. Norton Internet Security 19.8.0.14
11. Panda Internet Security 2012 17.01.00
12. Total Defense Internet Security Suite 8.0.0.87
13. Trend Micro Titanium Maximum Security 6.0.1215

All products were downloaded from vendor websites and installed using the default options.

Once testing began, the product version was frozen, in order to preserve the integrity of the test. Given the nature of endpoint protection platforms, virus signatures and definition updates as well as HIPS updates were enabled with whatever frequency was set by the manufacturer.

### Client Host Description

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

- Microsoft® Windows® XP SP2, Windows XP SP3, and Windows 7 operating systems
- 2 GB RAM
- 20 GB HD

# Contact Information

NSS Labs, Inc.
6207 Bee Caves Road, Suite 350
Austin, TX 78746 USA
+1 (512) 961-5300
info@nsslabs.com
www.nsslabs.com