CORPORATE AV / EPP COMPARATIVE ANALYSIS

Exploit Evasion Defenses

2013 – Randy Abrams, Dipti Ghimire, Joshua Smith

Tested Vendors

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

Overview

As security products improve their abilities to detect cyber threats, criminals adapt by utilizing evasion techniques in an attempt to conceal the exploits and payloads. This group test report analyzes some of the current methods used by cyber criminals to circumvent or evade detection from endpoint protection products (EPP).

Cyber criminals do not just develop one attack and then abandon it after one use. 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 readily available commercial exploit kits.

NSS tested 11 enterprise level endpoint protection (EPP) products to measure their effectiveness in protecting Windows computers against exploits. All of the vulnerabilities exploited during this test were publicly available for months and in some cases years prior to the test; they have all been observed in use on the Internet.

IT professionals need to be aware of the differing levels of evasion protection available in EPP products tested. Enterprises, especially those 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	Executable Packers (Download)	Executable Packers (Execute)	Layered Evasions	Overall Combined
McAfee	100%	100%	100%	100%	100%	100%	100%
MS Sys. Center	100%	100%	100%	100%	100%	100%	100%
Symantec	100%	100%	100%	100%	100%	100%	100%
Sophos	100%	100%	83%	100%	100%	100%	97%
ESET	100%	100%	100%	75%	75%	100%	92%
Kaspersky	100%	100%	100%	75%	75%	100%	92%
AVG	100%	100%	100%	25%	100%	100%	88%
F-Secure	100%	100%	100%	25%	100%	100%	88%
Norman	100%	100%	17%	75%	75%	100%	78%
Panda	100%	100%	100%	0%	50%	100%	75%
Trend	100%	100%	17%	0%	0%	100%	53%

Figure 1 - Evasion Block Rate

The NSS 2013 Corporate AV/EPP Comparative Analysis - Exploit Protection report highlights clear weaknesses in the abilities of many EPP security products to detect and block 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. This test, however, indicates that vendors are getting better at combatting these additional threat vectors. The overall anti-evasion protection of 87% in this test is a significant improvement over the 28% overall average observed in NSS' 2010 exploit evasions test.

The chart above shows test scores based on the absolute number of test cases passed. It should be noted that products that block on execution, even when they fail to block the download, generally provide better protection 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
AVG	100%	100%	100%	100%	100%	100%
F-Secure	100%	100%	100%	100%	100%	100%
McAfee	100%	100%	100%	100%	100%	100%
MS Sys. Center	100%	100%	100%	100%	100%	100%
Symantec	100%	100%	100%	100%	100%	100%
Sophos	100%	100%	83%	100%	100%	97%
ESET	100%	100%	100%	75%	100%	95%
Kaspersky	100%	100%	100%	75%	100%	95%
Panda	100%	100%	100%	50%	100%	90%
Norman	100%	100%	17%	75%	100%	78%
Trend	100%	100%	17%	0%	100%	63%

Figure 2 - Evasion Block Rate (on Execution)

Key Findings

- Most vendors have dramatically improved coverage for the basic evasions used in our latest round of testing compared to NSS testing in 2010.
- Executable compressors are still problematic for some vendors, including the top overall performers in this test.
- Most vendors are not scanning standard compressors on download, and some are not scanning compressed executable payloads on download.
- Default vendor settings may favor performance over security.
- Kaspersky failed to block HTTP exploits delivered via non-standard ports

Table of Contents

Overview **1**
Key Findings 3
Analysis **5**
HTTP Evasion 6
HTML Obfuscation 6
HTTP Compression 7
Payload Encoding 8
Payload Compression 8
Payload Packing 9
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 - HTML Obfuscation Block Rate *6*
Figure 5 - HTTP Compression Block Rate *7*
Figure 6 - Payload Encoding Block Rate *8*
Figure 7 - Payload Compression Block Rate *8*
Figure 8 - Payload Packing Block Rate *9*
Figure 9 - Layered Evasions Block Rate *9*

Analysis

Evasion is accomplished by obfuscating exploits and malware by using encryption or compression techniques in an attempt to avoid detection. An exploit that is detected by a security product can be modified by evasion techniques to bypass protection mechanisms 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 generally not detect the evaded exploit either (in which case evasion was superfluous). There are some compression formats that are always detected by some EPP products and if one of these compression formats is used, a product may block an evasion attempt without being able to block the un-obfuscated exploit.

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 host to **all** exploits that are capable of using the evasion technique. 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 not for the evasion.

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 task, since in such asymmetrical situations time is on the attacker's side. In this round of testing, NSS included layered evasions in the test.

For each evasion, it is verified that a standard Web browser (such as Internet Explorer) is capable of delivering the exploit to the endpoint regardless of the evasion technique, or combination of evasion techniques, employed. Before testing evasions, NSS engineers ensured that the baseline exploits were detected. Thus, the test is not biased on the inability to catch the exploit itself, but rather tests the EPP products ability to protect against the evasion techniques used to obfuscate the exploit. For information about exploit detection, please consult the NSS 2013 Corporate AV/EPP Comparative Analysis - Exploit Protection.

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 5 distinct categories, as well as 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 analysts.

NSS vulnerability research reveals that the number of reported vulnerabilities rose significantly in 2012 and the vulnerability landscape is undergoing significant transformations[1]. Due to the combination of this growing threat segment, and the popularity of exploit kits that automate the addition of evasions to exploits, NSS recommends that enterprises give appropriate weight to the quality of exploit prevention technology, as well as performance and threat detection, when selecting EPP products.

[1] https://www.nsslabs.com/reports/vulnerability-threat-trends

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 identify the original HTML document reliably 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
AVG	100%
ESET	100%
F-Secure	100%
Kaspersky	100%
McAfee	100%
MS Sys. Center	100%
Norman	100%
Panda	100%
Sophos	100%
Symantec	100%
Trend	100%

Figure 3 - HTTP Evasion Block Rate

HTML Obfuscation

Recognizing malicious HTML documents is important when protecting enterprise endpoints. 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 bots, rootkits, key loggers, and other trojans.

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

Product	HTML Obfuscation
AVG	100%
ESET	100%
F-Secure	100%
Kaspersky	100%
McAfee	100%
MS Sys. Center	100%
Norman	100%
Panda	100%
Sophos	100%
Symantec	100%
Trend	100%

Figure 4 - HTML Obfuscation Block Rate

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.
- 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 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 change the final appearance of the compressed document significantly. This property of compression 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.

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

Product	HTTP Encoding
AVG	100%
ESET	100%
F-Secure	100%
Kaspersky	100%
McAfee	100%
MS Sys. Center	100%
Norman	100%
Panda	100%
Sophos	100%
Symantec	100%
Trend	100%

Figure 5 - HTTP Compression Block Rate

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, 73% of the products tested were able to recognize and deal with all these encoding types. Of note, the consumer versions of Norman and Trend had scored 100% on these encoding types in a previous consumer test. Sophos does not have a consumer Windows offering so no comparison can be made.

Product	Payload Encoding
AVG	100%
ESET	100%
F-Secure	100%
Kaspersky	100%
McAfee	100%
MS Sys. Center	100%
Panda	100%
Symantec	100%
Sophos	83%
Norman	17%
Trend	17%

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 currently used, 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 believes security is generally enhanced if malicious downloads inside of compressed files are blocked by default.

Only three of the 11 products were able to score 100% on the download portion of this test. All but 3 of the products were able to detect all of the compressed payloads when a manual scan was initiated. As expected, all products successfully detected the malware upon execution.

Product	File Compression (Download)	File Compression (scan)
ESET	100%	100%
Kaspersky	100%	100%
Trend	100%	100%
Panda	80%	100%
Sophos	40%	100%
AVG	0%	100%
F-Secure	0%	100%
Norman	0%	100%
McAfee	0%	80%
MS Sys. Center	0%	0%
Symantec	0%	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 currently used, posing a significant problem to the AV industry.

Product	Payload Packing Block on Download	Payload Packing Block on Execute
McAfee	100%	100%
MS Sys. Center	100%	100%
Sophos	100%	100%
Symantec	100%	100%
ESET	75%	75%
Kaspersky	75%	75%
Norman	75%	75%
AVG	25%	100%
F-Secure	25%	100%
Panda	0%	50%
Trend	0%	0%

Figure 8 - Payload Packing Block Rate

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 believes that security is generally best achieved by blocking at download. Eight of the products failed to block at least one packed file on download and three products did not block any of the packed files on download.

RLPack, a runtime executable file compressor, proved problematic on download for six of the EPP products. Exploits using RLPack were able to evade ESET, Kaspersky, Panda and Trend Micro on 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 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 tested.

Product	Layered Evasions
AVG	100%
ESET	100%
F-Secure	100%
Kaspersky	100%
McAfee	100%
MS Sys. Center	100%
Norman	100%
Panda	100%
Sophos	100%
Symantec	100%
Trend	100%

Figure 9 - 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 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. AVG Internet Security Business Edition 2012 2012.0.2221
2. ESET Endpoint Security 5 5.0.2126.0
3. F-Secure Client Security 9.31
4. Kaspersky Endpoint Security 2012 12.0.0.374 8.1.0.831 (a)
5. McAfee Endpoint Protection 8.8.0
6. MS System Center 2012 Endpoint Protection 2.2.903.0
7. Norman Endpoint Protection 9.00.000
8. Panda Cloud Antivirus Pro 2.0.0
9. Sophos Endpoint Security & Control 10.0
10. Symantec Endpoint Protection 12.1.1101.401 RU1 MP1
11. Trend Micro Office Scan 10.6.2401 Service Pack 1

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 SP3, and Windows 7 32-bit operating systems
- 2 GB RAM (XP SP3), 4 GB RAM (Windows 7)
- 20 GB HD (XP SP3), 40 GB HD (Windows 7)

Contact Information

NSS Labs, Inc.
206 Wild Basin Road
Building A, Suite 200
Austin, TX 78746
+1 (512) 961-5300
info@nsslabs.com
www.nsslabs.com