Symantec Advanced Threat Protection: Network

DR150218C

April 2015

Miercom
www.miercom.com

Contents

1.0 Executive Summary

Miercom conducted an independent third party validation of the Symantec Advanced Threat Protection: Network appliance, the Cisco SourceFire and the FireEye 1310.

Security Effectiveness testing verified the detection and blocking of multiple malware threats including, legacy, Advanced Evasion Techniques, Advanced Persistent Threats, BotNet, RATs, active threats and malicious documents.

The Symantec ATP (SATP:N) solution demonstrated its ability to detect the different types of malware threats. When compared to products of competing vendors, the Symantec ATP:N solution performed at least 15% better than both contenders, with well above average strengths in protection against six of the seven categories of malware.

Key Findings:

- Symantec ATP:N detected 90.3% of all the malware sets
- Detected 100% of Advanced Persistent Threats malware
- Detected 97% in Advanced Evasive Threat (AET) Malware
- Demonstrated better performance in malware detection than competitors

We were pleased with the overall performance of the Symantec ATP:N solution for detecting malware, particularly its ability to effectively detect and remove not only the most common but even the unknown malware threats as well.

Any pertinent observations and recommendations by our test team relating to Symantec security solution's overall effectiveness have also been noted and included in this report.

We were pleased with the overall performance of the Symantec Advanced Threat Protection: Network solution malware blocking effectiveness. Its ability to block Advanced Persistent Threats and Advanced Evasive Threats earned the Symantec Advanced Threat Protection the Performance Verified Certification.

Robert Smithers
CEO
Miercom

2.0 Overview

One of the core security issues today is to know how malware still manages to get through security defenses months or years after their initial appearance. One reason is that much of this malicious content is constantly changing in an attempt to evade signature-based antivirus and static security gateway and firewall technologies.

This report shows how the Symantec ATP:N solution performed when presented with some of the most sophisticated, currently active malware. The results outlined in this document represent the level of detection of several categories by Symantec ATP:N, Cisco SourceFire Intrusion Prevention System and FireEye Security Service.

2.1 Products Tested

Symantec Advanced Threat Protection

Symantec Advanced Threat Protection: Network is a solution that detects malicious content within a network by utilizing its Cynic malware detonation and global intelligence, its Vantage network intrusion detection, and its Insight reputation-based security technology to signal unknown and active threats.

The Symantec ATP:N appliance, with pre-loaded software version 1.0.0.71, was used in this test.

Cisco SourceFire

Protects using continuous capabilities to monitor, store and recall malware that evades initial detection. This solution provides visibility of the malware attempting to enter, how malicious it is, and how it behaves. These investigations lead to enhanced intelligence to further improve system recovery for subsequent attacks.

Cisco SourceFire version 5.4 was used in this test.

FireEye 1310

Deployed in-line behind other security gateways, this appliance catches the threats that firewalls, anti-virus, web gateways, and intrusion prevention systems have missed. It stands in front of outbound traffic to prevent data theft and botnets, and it applies several techniques to detect malicious content during inbound, multi-phase inspections. It is equipped with false positive analysis for real-time processing, continuously expanding database of modified active threats, and email protection to block phishing attacks.

FireEye 1310 version 7.5.1 was used in this test.

2.2. Malware Samples

Malicious software, or malware, is any software used to disrupt computer or network operations, gather sensitive information, or gain access to computer systems.

Legacy

Legacy samples included several hundred variants of known malware that have been in circulation for 30 days or more. The malware classifications primarily consist of viruses and worms.

Advanced Evasion Techniques (AETs)

Advanced Evasion Techniques is a type of network attack that combines several different known evasion methods to create new attack that is delivered over several layers of the network simultaneously. The code in the AET itself is not necessarily malicious; the danger is that it provides the attacker with undetectable access to the network. There are currently about 200 known evasion techniques that are recognized by vendor products. An AET can create literally millions of new evasion techniques from just a couple of combinations

Advanced Persistent Threats (APTs)

An advanced persistent threat (APT) is a set of stealthy and continuous computer hacking processes, often orchestrated by human(s) targeting a specific entity. An APT usually targets organizations and/or nations for business or political motives. An example of an APT is malware which consists of a staged payload that, when activated, allows an attacker to obtain shell access. The attacker then has command line access to the remote target at the same privilege level as the vulnerable application or service. These payloads are often masked with randomization and evasion techniques to bypass AVs. The known APT samples used in our testing were sourced from Mandiant's Advanced Persistent Threat sample set.

BotNet

A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. Botnets use a technique known as Command and Control, where an intermediary receives orders from an attacker and those commands are then forwarded to all infected hosts. Botnets are commonly used in spamming and DDoS operations. Variants of the Zeus and Citadel botnets were collected from high-interaction honeypots and used in this test.

RATs

RATs, or Remote Access Trojans, are malicious code disguised as something normal or desirable so they often masquerade inside other legitimate software. When activated in a victim host, they provide full remote control over that victim.

Active Threats

Active (unknown) threats consisted of malware samples that have been custom crafted, undetected samples acquired from external resources and private honeypots, and APTs that have undergone AV evasion techniques such as encryption, black packaging, payloads that use normal and allowed egress traffic.

Malicious Documents

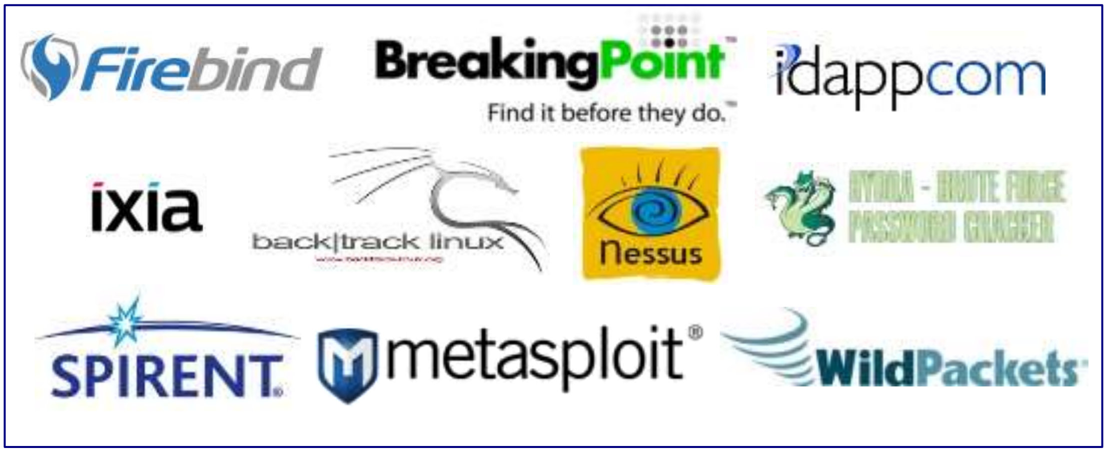
An additional sample set of malicious documents used in testing contained a mix of Microsoft Office documents (Word, PowerPoint and Excel files) that held known macro viruses, and PDF files containing a variety of viruses, APTs and worms.

3.0 How We Did It

3.1 Test Tools

Miercom uses industry leading test tools, scripts, and databases to provide the most robust, comprehensive, and realistic testing environment possible. Miercom security-efficacy analysis of the Symantec ATP:N product employed the same test samples as its Advanced Threat Detection Industry Study.

Test Tools & Software



During this analysis, the following security functionality was assessed:

- Detection: Ability to identify known threats
- Emulation: Ability to emulate unknown but suspicious files
- Verdict: Whether the correct result is returned, based on the outcome of threat emulation
- Forensic Reporting: Level of detail offered in post-response to an incident

Known malware samples were obtained from Miercom's honeypot, which consists of both low- and high-interaction honeypot partitions. Advanced Evasion Technique and active threat malware samples were developed by Miercom for the purpose of this test. Legacy samples were used, but the focus was on the latest samples.

3.2 Configuration

The appliances were configured to block every security related category available within its administrative console and to use all available defenses. All products were configured with default settings.

Product Deployment

Symantec ATP:N was deployed in tap mode. Tap mode is a passive approach to monitoring traffic, compared to in-line deployment which places the sensor directly in the network path for traffic inspection.

Tap mode enabled the appliance to monitor traffic and its packet information, but did not enable real-time protection. All traffic and malicious data was seen and passed to a third party looking in, but did not trigger a response unless the attack has already occurred.

FireEye 1310 was also configured for Tap mode. Cisco SourceFire did not have the capability of Tap mode available and was tested with an in-line configuration.

Victim Environment

A virtual machine, hosted on VMware ESXi release 5.5, acted as the victim computer during testing. The virtual machine was subjected to attacks from a malicious server. Following the attempted transfer of samples from server to victim, security-product log files are then reviewed. Log files were intended to show if a sample was detected, how long it took to detect it from time of initial request to download, and what post-detection remediation steps, if any, were taken by the security product.

4.0 Summary of Results

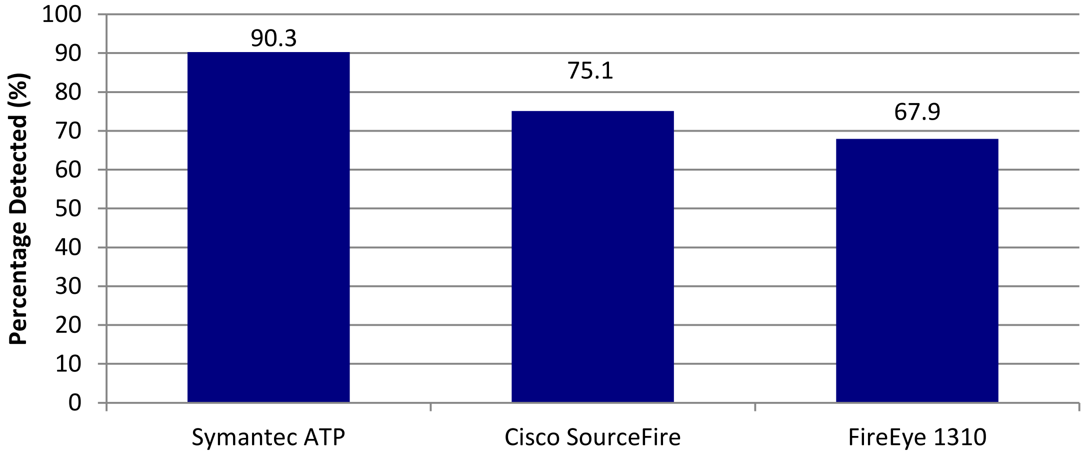
A security effectiveness validation test was performed to validate the ability of the unit under test to detect real-world threats. A fundamental aspect of the test was to validate proactive security and see how much protection the appliance provided out of each set tested.

Improving security posture of an enterprise requires threat detection accuracy, speed, and mitigation. There has been much debate over the wide variety of security controls on the market and the effectiveness of not only the products themselves, but also their implementation within the enterprise infrastructure.

4.1 Malware Detection Rate

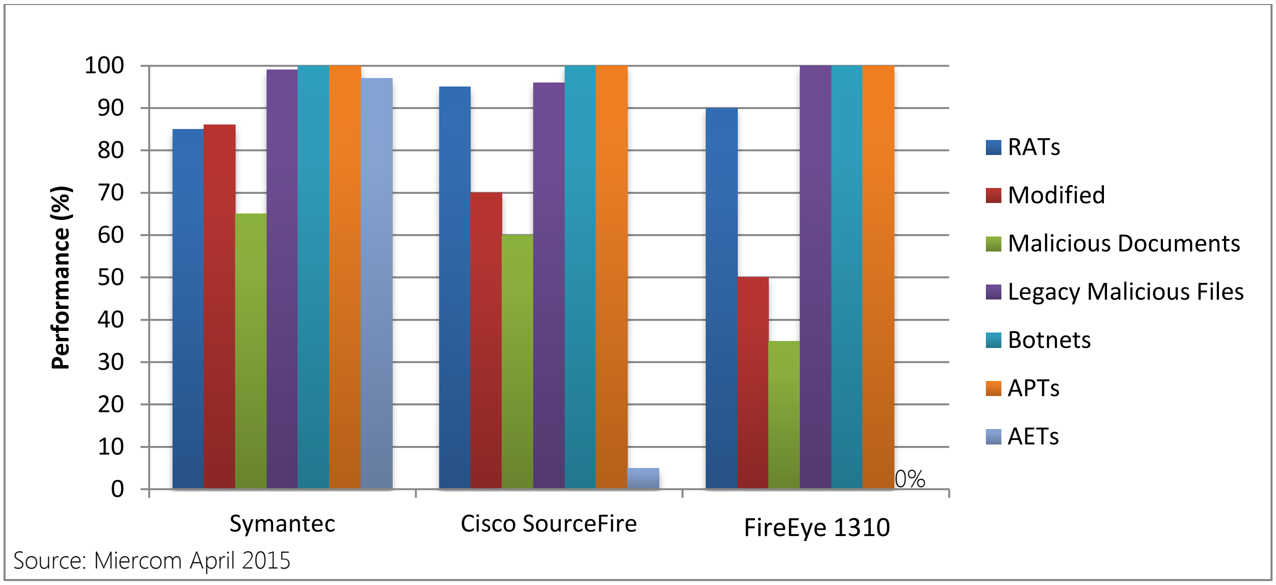
Each bar represents the percentage of samples captured for each category of malware in the tested sample set. Detection is defined as the ratio of samples identified to the total number of samples in the set, in terms of percentage.

Figure 1: Competitive Malware Detection Rate



Source: Miercom April 2015

Figure 2: Competitive Malware Detection Rate

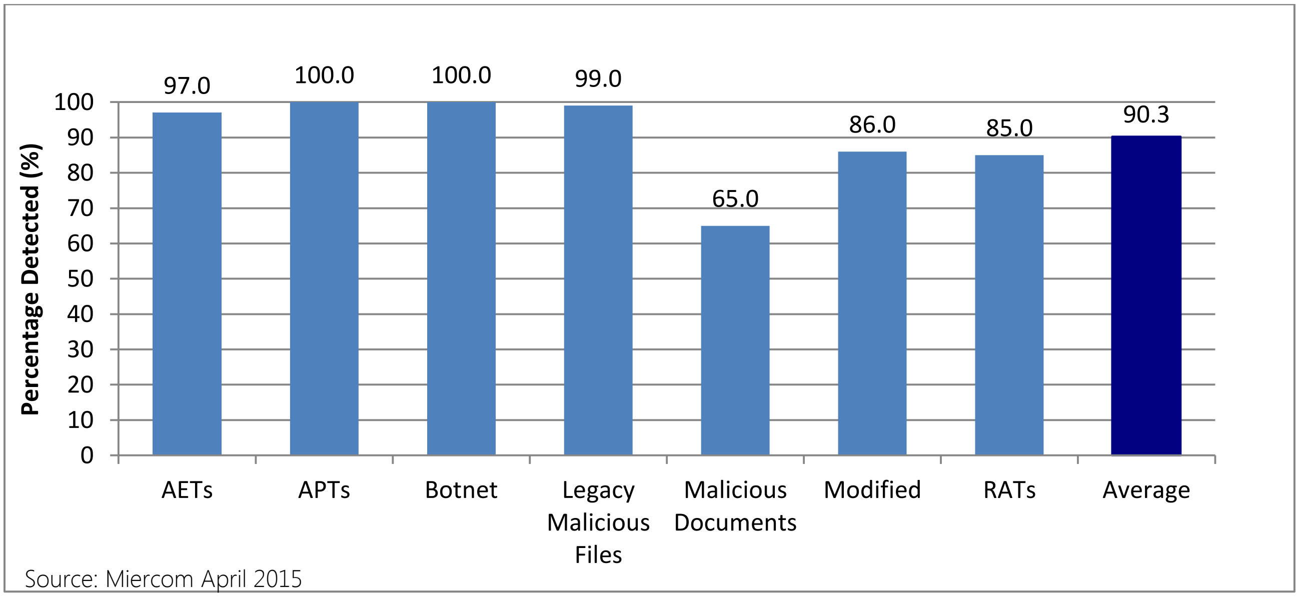


Source: Miercom April 2015

Malware detection performance by category for each vendor. Symantec had an overall performance of 90.3%

Vendor Results

Figure 3: Symantec Malware Detection Rate

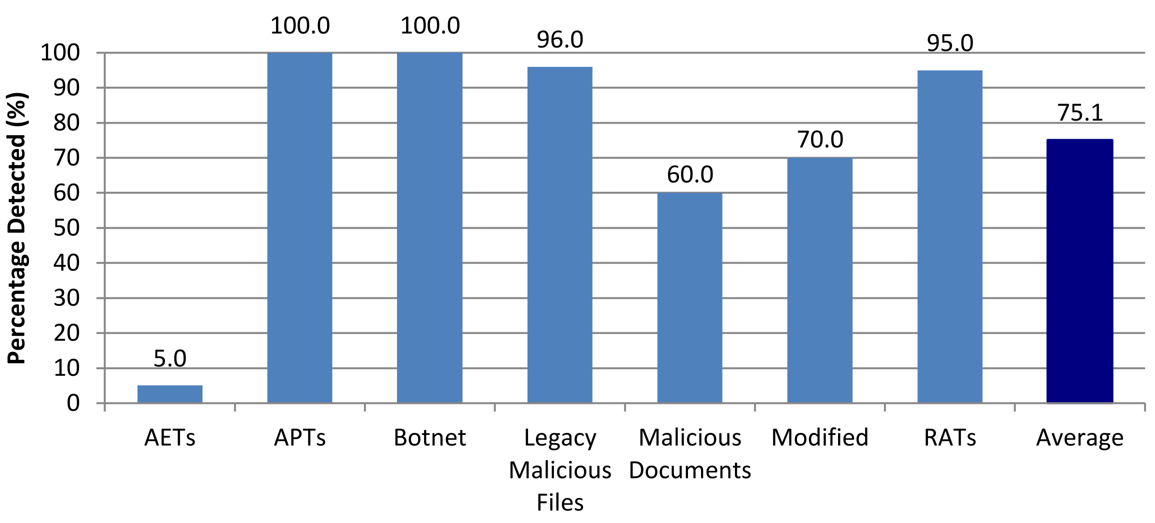


Source: Miercom April 2015

Symantec ATP:N performance for each of the sample set categories tested. The product package scored an overall average of 90.3%

Symantec Advanced Threat Protection did sufficiently well in detecting malware, as Symantec products have done in the past. Its strengths reside in AETs and APTs which are some of the most current and threatening types of malware attacks today.

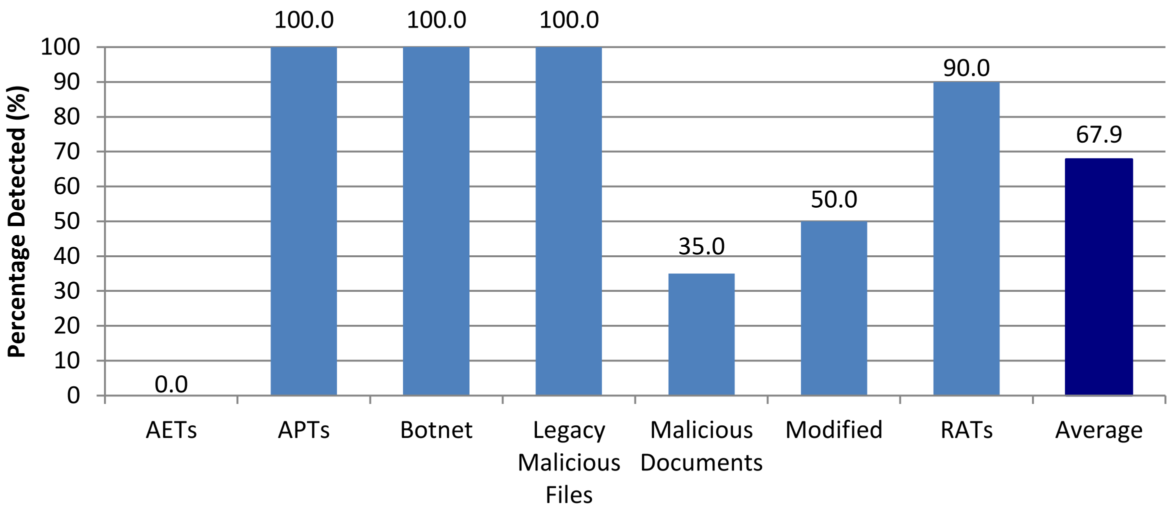
Figure 4: Cisco SourceFire Malware Detection Rate



Source: Miercom April 2015

Cisco SourceFire appliance detected fewer threats in each of the tested sample set categories. The product package scored an overall average of 75.1%.

Figure 5: FireEye 1310 Malware Detection Rate



Source: Miercom April 2015

FireEye 1310 appliance detected 100% of APTs, Botnets and Legacy malware. While falling behind its competitors in all malicious documents and modified threats.

5.0 Fair Test Notification

All vendors with products featured in this report were afforded the opportunity before, during, and after testing was complete to comment on the results and demonstrate the performance of their product(s). Any vendor with a product tested by Miercom in one of our published studies that disagrees with our findings is extended an opportunity for a retest and to demonstrate the performance of the product(s) at no charge to the vendor.

All vendors are welcome to demonstrate their performance on their own to Miercom. Miercom will update these results if new data presents itself.

6.0 About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the Performance Verified program, the industry's most thorough and trusted assessment for product usability and performance.

7.0 Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

No part of any document may be reproduced, in whole or in part, without the specific written permission of Miercom or Symantec All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.