



**ICSA Labs
Premier Services Evaluation Report
for
McAfee, Incorporated
Detection, Prevention and Cleaning Test
Results
McAfee VirusScan Enterprise, 8.0i**

Prepared by:

ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050
21 February, 2005

Executive Summary

Scope of Work

McAfee, Incorporated contracted ICSA Labs to evaluate the ability of version 8.0i of their VirusScan Enterprise product to:

- Detect and block the propagation of malicious code in the absence of traditional signature-based antivirus software.
- Repair infected systems.

The following report details the testing completed and results. Testing was conducted by ICSA Labs analysts in the ICSA Labs testing facilities located in Mechanicsburg, PA, USA.

Results Summary

ICSA Labs conducted tests using Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server, Microsoft Windows XP Professional and McAfee VirusScan Enterprise version 8.0i. Using a specially prepared virus signature file which contained no malware signatures, we exposed the protected system to a number of samples of malicious code (malware) to determine the ability of the technology to detect and limit the spread of the malware. ICSA Labs determined that McAfee VirusScan Enterprise version 8.0i, effectively with no virus signature files installed, was able to detect and at least partially block 100% of the tested malware from propagating.

In separate tests, using a version of the signature file containing current malware definitions, ICSA Labs determined that VirusScan Enterprise 8.0i detected and cleaned the malicious code or the effective portions of the malicious code 100% of the time. In the cases where cleaning was incomplete, the remaining residuals were benign, i.e. not capable of re-infection, propagation or other malicious activity. Notably, there were no cases in which VirusScan Enterprise 8.0i required a reboot of the machine to complete its cleaning.

Testing Details

Background

McAfee VirusScan Enterprise 8.0i uses a number of techniques, including application specific buffer overflow protection, port blocking and access protection policies applied to file names, folders, directories and file shares to proactively protect against rapidly evolving threats without requiring updates to traditional antivirus signatures.

Test Methodology

ICSA Labs designed the test scenario to simulate the case where the resident antivirus software does not have signatures for the malware against which it is being tested. McAfee prepared and supplied us with special antivirus signature file which contained no virus signatures. ICSA Labs then disabled the automatic update feature which is normally active in VirusScan Enterprise to prevent this special file from being overwritten.

All testing was conducted on an isolated, specially prepared and purpose-designed testbed consisting of physical hosts configured to represent a typical networking environment. We installed and configured machines as a Windows Domain controller, DNS server, Microsoft Exchange server, SQL Server and domain clients to simulate a normal enterprise networking environment and the actual infection point where we attempted to introduce the malware. No other security software was used or enabled on the infection points during the course of testing.

For each malware sample, ICSA Labs conducted two separate tests as detailed below. Prior to testing, we executed the malware on our infection point and documented its behavior in this baseline case. In many cases, the ICSA Labs analyst had to perform extraordinary or ill-advised actions in order to cause the malware to execute or to attempt to propagate. In each case, inappropriate action notwithstanding, we attempted to reproduce the real world scenario under which the malware in question had propagated. We then followed the steps detailed below for the respective tests. Detailed results are presented in tabular form in the Results & Analysis section. There is a column in the tabulated data labeled IAR (Inappropriate Action Required) indicating where extraordinary steps were necessary, and a discussion of the required action in the corresponding notes column.

- Detection / Protection Test:
 1. We started each test with a freshly installed and configured infection point and protected host.
 2. With the infection point totally unprotected, and the target host protected only by the specially prepared version of McAfee VirusScan Enterprise 8.0i, we launched the malware on the infection point.
 3. We verified the propagation of the malware by monitoring network traffic, and then, if required, attempted to execute the malware on the protected client. In most cases, the malware arrived via email in either executable or archived attachments, and in some cases was automatically executed through exploitation of vulnerabilities in the email client. Some malware propagated via other means such as network shares or file sharing applications.
 4. We monitored the behavior of the malcode as it attempted to install and propagate, and using the definitions detailed in the Results & Analysis section, compared the results with the baseline previously established to determine the extent to which the malcode was blocked by VirusScan Enterprise.

- Cleaning Test:
 1. We started all cleaning tests with a freshly installed and configured infection point and protected host. In this case, we installed McAfee VirusScan Enterprise 8.0i on the protected host with a current set of

antivirus signatures, but configured the protected host so that the McAfee software was not running at the time of the infection. The baseline (pre-infection) state of the system was documented using SysInternals Install Watch.

2. With the infection point totally unprotected, and the target host protection present but explicitly disabled, we launched the malware on the infection point. After allowing time for the infection, we rebooted the infected system and re-ran Install Watch to establish exactly what the malware had done to the system.
3. We enabled the On-Access or On-Demand protection of McAfee VirusScan Enterprise in order to cause it to attempt to repair the system. Afterwards, we re-ran Install Watch and compared the results to determine to what extent VirusScan was able to clean or repair the infected system components.

Malware samples used in these test were selected to represent recently circulating malware which had reached a medium or higher prevalence as documented by McAfee, Incorporated.

Product Under Test Components

Hardware:

- Shuttle XPC, model SK41G
- AMD Athlon XP 2100+
- 40 GB Hard Drive
- 512 MB Ram

Software:

- Infection Point / Protected Host:
 - Microsoft Windows 2000 Professional
 - Microsoft Windows XP Professional, SP1
 - McAfee VirusScan Enterprise, version 8.0i.
 - Internet Explorer 5.0
 - Outlook 2000
 - Outlook Express 5.0
- Network environment
 - Windows 2000 Server domain controller
 - Exchange Server 2000
 - SQL Server 2000
 - Red Hat 9.0 running DNS, HTTP

Documentation:

- Internal Documentation (Help System)

Results and Analysis

ICSA Labs executed the malware on our designated infection point and monitored all network traffic, the infection point, and other non-protected hosts on our testbed network to determine if the malware successfully spread beyond our infection point. We used the following definitions for the results listed below:

- Column Headings:
 - Malware Discovery Date: Date on which the malware originally appeared in the wild.
 - Name: Name used by McAfee AVERT for the malware.
 - Inappropriate Action Required (IAR): Indicates that the ICSA Labs analyst had to perform some extraordinary or ill-advised actions in order to cause the malware to execute or to attempt to propagate.
 - Block: Indicates the degree which VirusScan was able to block the malware.
 - Cleaning: Indicates the degree and conditions of cleaning success:
 - Success: Degree of overall success, see definitions below.
 - On-Access (OA): Degree of success in scanning without user intervention.
 - On-Demand (OD): Degree of success in scanning requiring user explicit initiation.
 - Reboot (R): Whether a system reboot was necessary.
 - Notes: Explanations of Inappropriate Actions Required (IARs), Details of residuals remaining in the event of partial cleaning, and explanations of exceptions or anomalies.
- Definitions and key for Blocking Tests:
 - Fully Blocked (B): VirusScan blocked the virus from installing or propagating beyond the infection point.
 - Partially Blocked (P): VirusScan permitted the virus to install but blocked the virus from propagating beyond the infection point.
 - Not Blocked (N): VirusScan permitted the virus to install and propagate to other hosts.
- Definitions and key for Cleaning Tests:
 - Cleaned (C): VirusScan successfully removed all components of the infection, including executable files dropped by the malware, non-executable files dropped by the malware, parasitically infected files and registry entries. No residuals of the infection remain
 - Partially Cleaned, Benign Residuals (PB): VirusScan successfully removed some, but not all components of the infection. The remaining residuals of the infection were not capable of re-infection, propagation or other malicious activity, i.e, they were benign.
 - Partially Cleaned, Malicious Residuals (PM): VirusScan successfully removed some, but not all components of the infection. The remaining residuals of the infection were not benign as described above.
 - Not Cleaned (N): VirusScan was unable to remove any of the components of the infection.

Out of 39 malware samples tested, VirusScan Enterprise 8.0i was able to affect a partial block in 33 cases, or 82.5% of the time, and it was able to affect a complete block in 7 cases, or 17.5% of the time.

For the purposes of the cleaning statistics below, if VirusScan was able to completely clean the malware, or partially clean the malware leaving only benign residuals, we defined the cleaning attempt to be successful.

In certain cases, there were no residual components left by the malware for cleaning, and therefore those malware samples were not included in our cleaning tests. When testing the ability of the On-Access Scanner to effectively remove all malicious components of the malware, McAfee VirusScan Enterprise was effective 36 out of 38 times for

a success rate of 94.7%. The malware was completely removed in 12 out of 38 cases, or 31.6% of the time, and the malware was partially cleaned with no malicious components remaining in 24 out of 38 cases, or 63.2% of the time.

When testing the ability of the On-Demand Scanner to effectively remove all malicious components of the malware, McAfee VirusScan Enterprise was effective 37 out of 38 times, for a success rate of 97.4%. The malware was completely removed in 31 out of 38 cases, or 81.6% of the time, and the malware was partially cleaned with no malicious components remaining in 6 out of 38 cases, or 15.8% of the time.

Overall, when combining both scan methods, McAfee VirusScan Enterprise was effective at removing all malicious residuals 100% of the time. In 34 of the 38 cases, the malware and its residuals were completely cleaned by some combination of the two scans, and in the remaining 4 cases, only benign residuals of the malware remained.

Malware Discovery Date	VIRUS NAME	Blocking			Cleaning			
		Results	IAR	Notes	OAS	ODS	Reboot Req'd	Notes
2/17/2004	W32/Bagle.b@MM	P	Y	A	PB	C	N	T
2/27/2004	W32/Bagle.c@MM	P	Y	B	PB	C	N	T
2/28/2004	W32/Bagle.e@MM	P	Y	B	PB	C	N	T
3/1/2004	W32/Bagle.h@MM	P	Y	B	PB	C	N	T
3/2/2004	W32/Bagle.j@MM	P	Y	C	PB	C	N	T
3/13/2004	W32/Bagle.n@MM	P	Y	C	PB	C	N	T
3/15/2004	W32/Bagle.p@MM	P	Y	C	PB	C	N	T
3/26/2004	W32/Bagle.u@MM	P	Y	A	PB	C	N	T
1/18/2004	W32/Bagle@MM	P	Y	A	PB	C	N	T
6/4/2003	W32/Bugbear.b@MM	P	N	E	PB	C	N	T
8/19/2003	W32/Dumaru.a@MM	P	Y	A	PB	C	N	T
1/24/2004	W32/Dumaru.y@MM	P	Y	B	PB	C	N	T
5/8/2003	W32/Fizzer.gen@MM	P	Y	A	C	C	N	U
2/23/2003	W32/Lovgate.c@M	P	Y	A	PB	C	N	T
8/11/2003	W32/Lovsan.worm	B	/	/	C	PB	N	X
10/31/2003	W32/Mimail.c@MM	P	Y	B	PB	C	N	U
12/1/2003	W32/Mimail.l@MM	P	Y	B	C	C	N	/
1/28/2004	W32/Mimail.s@MM	P	Y	A	C	C	N	/
8/1/2003	W32/Mimail@MM	P	Y	B	C	C	N	/
11/8/2004	W32/Mydoom.ag@MM	B	/	/	C	C	N	/
11/8/2004	W32/Mydoom.ah@MM	B	/	/	C	C	N	/
2/19/2004	W32/Mydoom.f@MM	P	Y	C	PB	C	N	T
1/26/2004	W32/Mydoom@MM	P	Y	C	PB	C	N	T
8/18/2003	W32/Nachi.worm	B	/	/	PB	PB	N	Z
2/18/2004	W32/Netsky.b@MM	P	Y	C	PB	C	N	U
2/25/2004	W32/Netsky.c@MM	P	Y	C	PB	C	N	U
3/1/2004	W32/Netsky.d@MM	P	Y	A	C	C	N	/
3/8/2004	W32/Netsky.j@MM	P	Y	A	C	C	N	/
3/21/2004	W32/Netsky.p@MM	P	Y	D	C	C	N	/
3/28/2004	W32/Netsky.q@MM	P	Y	D	PM	C	N	W
4/5/2004	W32/Netsky.s@MM	P	Y	A	C	C	N	/
4/30/2004	W32/Sasser.worm.a	B	/	/	C	C	N	/

5/18/2003	W32/Sobig.b@MM	P	Y	A	PB	PB	N	Z
5/31/2003	W32/Sobig.c@MM	P	Y	A	PB	PB	N	Z
6/25/2003	W32/Sobig.e@MM	P	Y	B	PB	PB	N	Z
8/18/2003	W32/Sobig.f@MM	P	Y	A	PM	PB	N	V
1/9/2003	W32/Sobig@MM	P	Y	A	PB	C	N	U
1/25/2003	W32/SQLSlammer.worm	B	/	/	NA	NA	N	/
9/18/2003	W32/Swen@MM	P	Y	D	PB	PM	N	U, Y
9/14/2004	JPEG Exploit	B	/	F	NA	NA	N	/

Blocking Key	
A:	Malware arrived as an executable attachment. When the attachment was run from within the email client, execution was blocked entirely. When the attachment was saved to disk first and then run, the malware was permitted to install and run locally, but propagation via SMTP was blocked.
B:	Malware arrived as an archived attachment. The attachment could be opened from within the email client or after saving to disk first. In all cases the malware was permitted to install and run locally, but propagation via SMTP was blocked.
C:	Malware arrived as either an executable or archived attachment. When an executable attachment was run from within the email client, execution was blocked entirely. When an executable attachment was saved to disk first and then run, the malware was permitted to install and run locally, but propagation via SMTP was blocked. Archived attachments could be opened from within the email client or after saving to disk first. In all cases involving archived attachments, the malware was permitted to install and run locally, but propagation via SMTP was blocked.
D:	Blocked automatic execution of vulnerability, but still allowed attachments to be accessed. When attachments were saved to disk and run, or archived attachments were opened from inside the email client, the malware was permitted to install and run locally, but propagation via SMTP was blocked.
E:	Malware is executed automatically when viewed via Outlook or Outlook Express. Executable files were copied to disk but not run automatically.
F:	Sometimes results in certain windows crashing, but no other malicious behavior is observed and system is still usable and does not require a reboot for operation.

Cleaning Key	
T:	OAS cleaned files when accessed but not registry.
U:	OAS cleaned files when accessed and registry.
V:	OAS stopped malware from propagating, but executable files remained which could be run manually. Registry content was not removed.
W:	OAS stopped malware from propagating, but executable files remained which could be run manually. Registry content was removed.
X:	ODS cleaned files but not registry when tested on Windows 2000. When tested on Windows XP, ODS cleaned both files and registry.
Y:	ODS removed some malicious executables, but benign non-executable files and malicious zips remained.
Z:	Cleaned all malicious and executable content, but benign non-executable files remained.