Malware Virtual Machine™
Heuristic Engine
Introduction

Contact: info@av-sdk.com

Index

1.Product overview

1.1 Product introduction

Malware Virtual Machine™ (hereinafter referred to as MVM) based on dynamic and static code analysis technique developed by Filseclab Corporation and achieves top level in the technical field. It is based on new detection technology, doesn't include virus signature database, takes up less system resources, has high detection accuracy and is capable of detecting new unknown viruses on the internet without upgrading. MVM not only automatically realizes detection of malicious files like trojan, virus, worm, spyware, etc. but also deeply analyzes encrypted, packed and deformed malicious code, accurately locates malicious behavior of program and reports virus family and variants according to current virus naming rules. This is better than simple analysis or shell reports of general heuristic scan and maintains at a low false positives rate. MVM can detect new variants of virus family already known or unknown new virus family without upgrading. Its heuristic ability has reached world-class anti-virus software, such as ESET NOD32.

1.2 Product software and hardware specification

1.2.1 Developing language and environment

The developing language for MVM is assembly, C and C++ languages; the developing environment is Microsoft Visual C++ 6.0. The engine provides flexible API and can be cross-platform configured to Unix/Linux or Windows system products. The following software screenshots and related presentations are demo software MVMDemo on Windows platform unless otherwise specified.

1.2.2 Hardware requirement

The size of MVM.dll is only 2MB which takes up much less system resources compared to similar software.

Lowest requirement of system configuration (Windows platform)	
Processor	Pentium III 700 MHz or above
Memory	Above 256 MB
Available space of hard disk	Above 10MB
Operating system	Windows 2000, 2003, XP, Vista, Windows 7

2.Product characteristic

2.1 Skilled in detecting unknown virus

In the field of anti-virus, traditional virus detection technology based on feature code still plays a leading role, but with the massive growth of virus Trojan, anti-virus software companies find it difficult to collect new virus Trojan samples in time. Even if the anti-virus software companies can collect all the samples, the size of virus database will be increasing day by day with the massive expansion and the corresponding anti-virus software will take up more memory and other resources in the computer system, eventually leading to the fact that the system resources can not meet the requirements. Furthermore, traditional detection technology based on feature code has inherent flaws: samples can be collected to extract virus feature only after virus already exists. This passive response mode is always lagging behind the virus outbreak.

The new technology of code dynamic and static heuristic analysis applied in MVM heuristic engine automatically realizes detection of malicious files like Trojan, Virus, Worm, Spyware, etc. MVM can deeply analyzes encrypted, packed and deformed malicious code, accurately locates malicious behavior of program and reports virus family and variants according to current virus naming rules(as illustrated in Figure 2.1). This is better than simple analysis or shell reports of general heuristic scan and maintains at a low false positives rate. MVM can detect new variants of virus family already known or unknown new virus family without upgrading.

Code dynamic heuristic analysis: apply anti-virus virtual machine technology, provide virtual running environment for program, Track program behavior and dynamically recognize virus Trojan. It has high detection accuracy.

Code static heuristic analysis: scan the whole code, recognize program execution logic and determine relevance of program behaviors. Suitable for all PE files, have good generality for malicious program recognition.

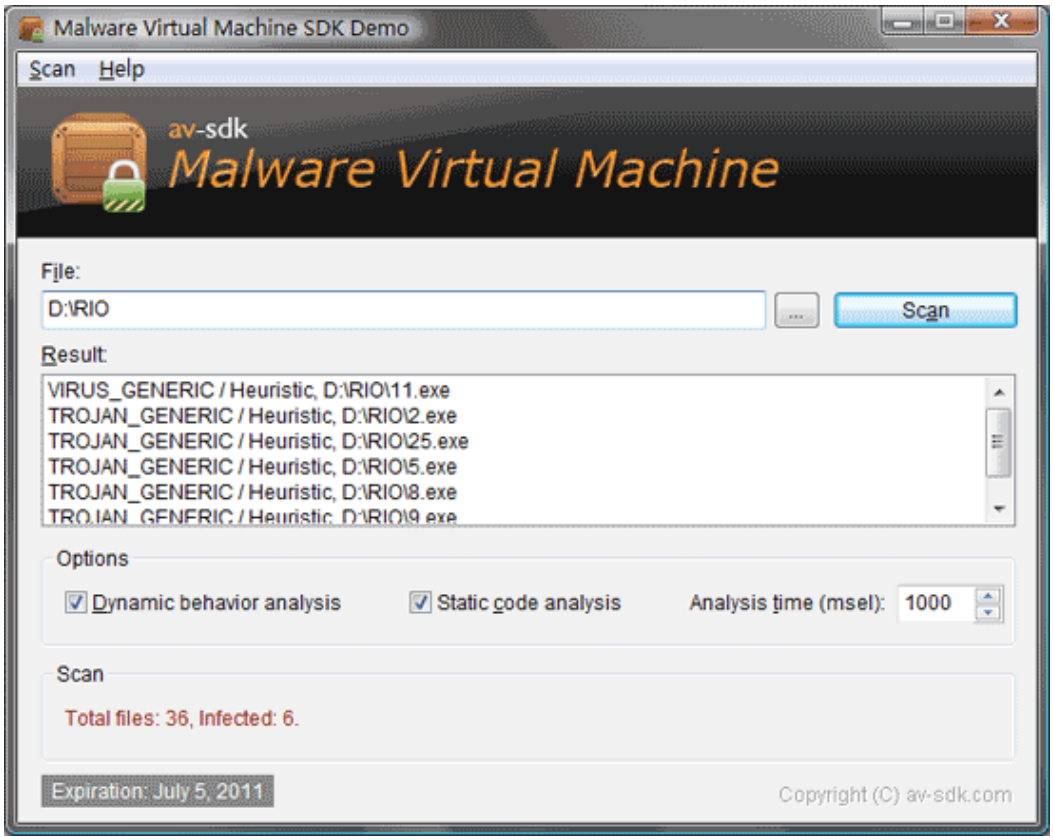


Figure 2.1

2.2 Top anti-virus virtual machine technology

Filseclab founded in 2001. In 2002 developed the first virus immunity system Twister. In 2007 developed the first cloud security system. Filseclab has a strong technical ability in the technical field of virtual machine technology, in 2007 developed the first professional virtual machine unpack machine of the world which can successfully unpack about more than 300 shells commonly used at that time. After years of tireless pursuit of technological innovation, Filseclab has already acquired international leading anti-virus virtual machine technology. The depth, accuracy, efficiency and other indicators tests of program simulation indicate that malware virtual machine has reached the industry-leading level.

Dynamic heuristic detection of MVM is mainly based on anti-virus virtual machine technology. By simulating Intel CPU, part of computer hardware (hard disk, etc.) and Windows operating system, an anti-virus virtual machine is constructed, and then virus program is loaded into the simulated system and runs on it. There are a number of behavior-monitoring points in virtual machine monitoring program behaviors in real time which stop running and report virus when malicious behaviors are found. The virus does not threaten the real system because the virus program is running on a virtual machine.

Intel CPU simulation: Simulating CPU is mainly composed of machine code recognition system, addressing system and command interpretation execution system, wherein machine code

recognition system is in charge of identifying the program instructions and giving the identified instructions to the instruction interpretation system to execute. Addressing system is needed to addressing access memory if memory is required during the execution of instructions.

Windows operating systems simulation: This module is mainly composed of PE loading system, API system, file system, registry system and task scheduling system, etc, and virus is needed to be loaded into PE loading system before running, and then is executed by virtual CPU. API and other system may be needed to support program execution procedure and task scheduling system is also needed if the virus program is multi-threaded and multi-processed.

2.3 Original static analytical technology

Static heuristic detection technology of MVM is mainly based on code segment analysis to detect virus. classifying file external static information, combining with viral infection forms and simulating tracking code execution procedure are utilized to detect whether virus is determined. Static detection includes detection solutions for abnormal program and malicious behavior rules.

For the detection solution to abnormal program, techniques of virus Trojan are classified such as abstract analysis of ways of entrance fuzzy hidden, tunnel infection and so on; at the same time, these abnormal points are summarized and combined with analysis algorithm to achieve the effect of unknown viruses detection.

For the detection solution to malicious behavior rules, the virus family behaviors already formed are summarized and rules are conducted; meanwhile, rules are formed by disassembling malicious program code, simulating tracking code execution procedure and interpreting specific functions, parameters and other effective information. Effective detection of new virus variants is completed by matching rules of existing knowledge database.

2.4 Excellent detection capability

In a large number of tests of massive Internet virus samples, detection rate of MVM heuristic detection engine maintains at about 50%. The detection rate of MVM engine for new unknown viruses that traditional antivirus software cannot detect maintains at about 40%, reaching the international top level.

2.4.1 Score of PC Security Labs test

PC Security Labs (PCSL) is an independent research organization focusing on security software test and test standard development.

PCSL specialized test report on anti-virus heuristic technology:

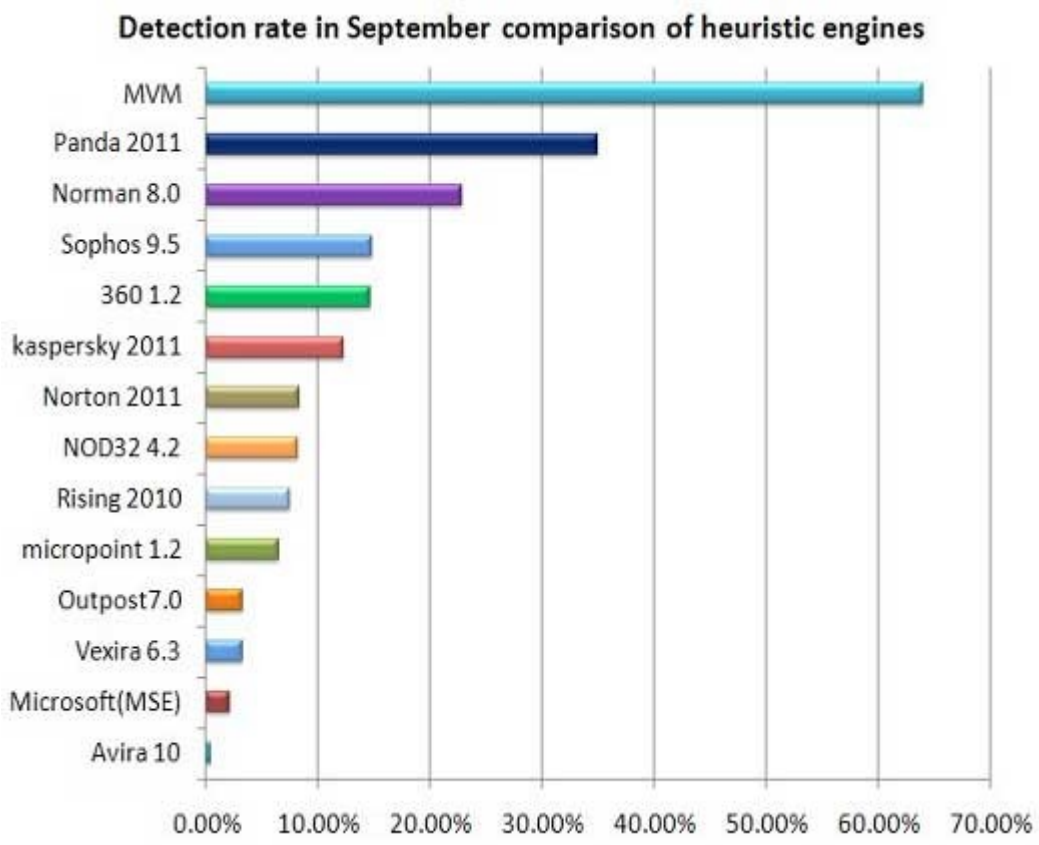
Releasing time of BDV(based on MVM) heuristic engine to be tested: 2010-05-18

21000 popular samples in September, 2010 are selected, 12228 detected, detection rate 58.23% which ranks first in the test comparison of heuristic engines without virus database.

2.4.2 Average detection rate comparison of heuristic engines(as illustrated in Fig 2.2)

Statement necessary to make: At present, most anti-virus software having heuristic detection technology but doesn't provide independent detection mode of heuristic engine, which means using heuristic detection engine independently without large virus database. Therefore, similar comparison tests for the performance of the heuristic engines are not easy. The following data of heuristic engine detection rate in September 2010 comes from the third party kafan (MVM is released on May 31, not upgrading for three months).

Fig 2.2



2.4.3 Detection rate in September comparison between MVM heuristic engine and international famous security software Microsoft Security Essentials (as illustrated in Fig 2.3)

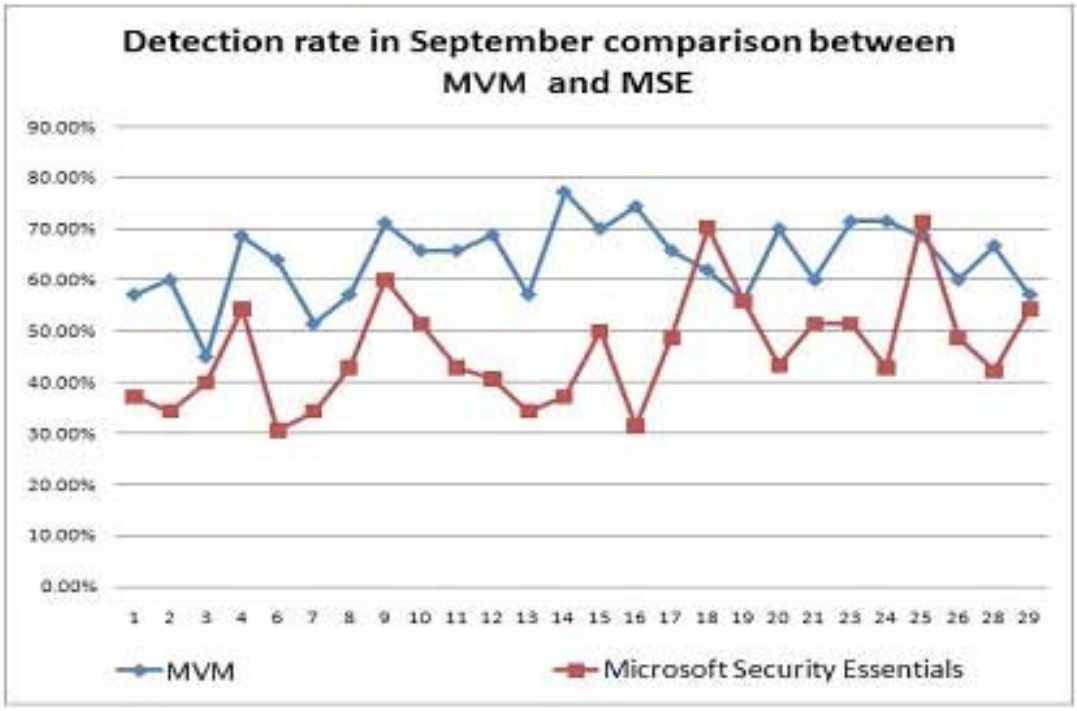


Fig 2.3

Note:

1. The above data comes from the third party forum bbs.kafan.cn and the test time is September, 2010;
2. The MVM engine no database, it does not need to upgrade;
3. Microsoft Security Essentials is upgraded to the latest virus database everyday before test.

2.4.4 Detection rate comparison between MVM heuristic engine and the Rising (as illustrated in Fig 2.4)

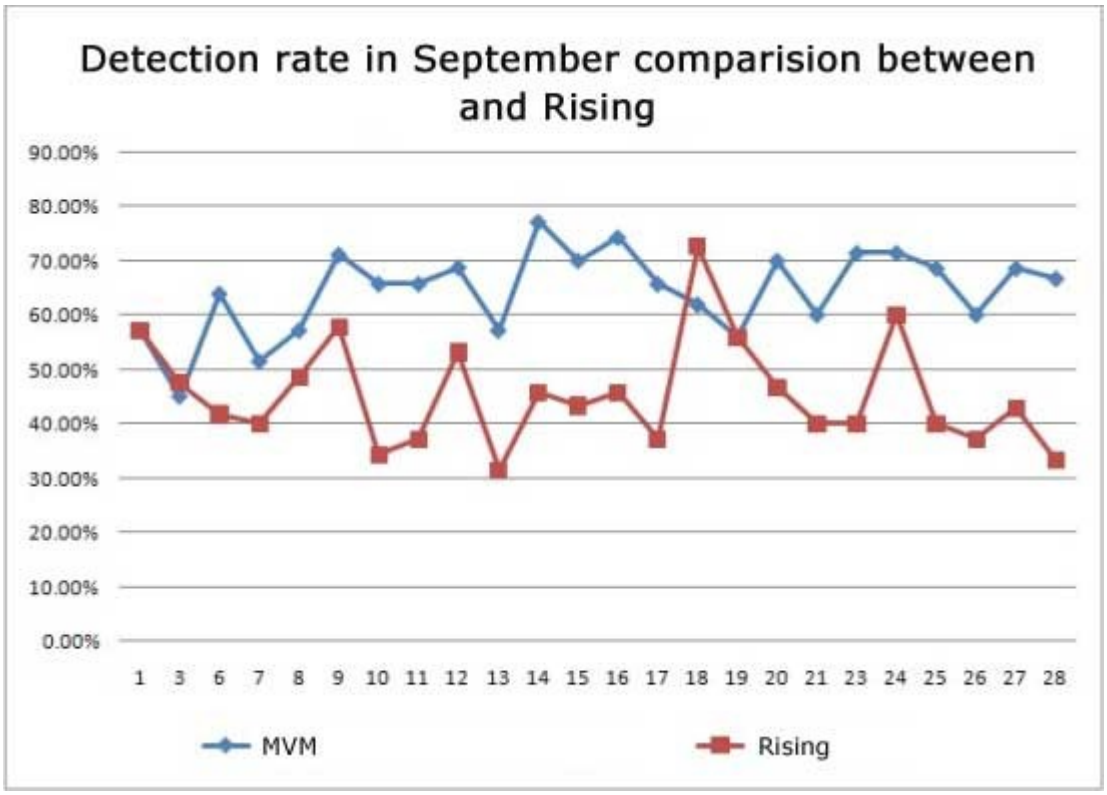


Fig 2.4

Note:

1. The above data comes from the third party forum bbs.kafan.cn and the test time is September, 2010;
2. Rising 2010 means Rising full function security software version 2010 and is upgraded to the latest virus database everyday before test.

2.5 Strict false positives control

After a long-time debugging, MVM heuristic detection engine has a higher detection rate while maintaining a low false positives rate especially almost zero false positives for Windows 2000,2003, XP, Vista and Windows7 system files.

False positives rate comparison between MVM and other anti-virus software (as illustrated in Fig 2.5):

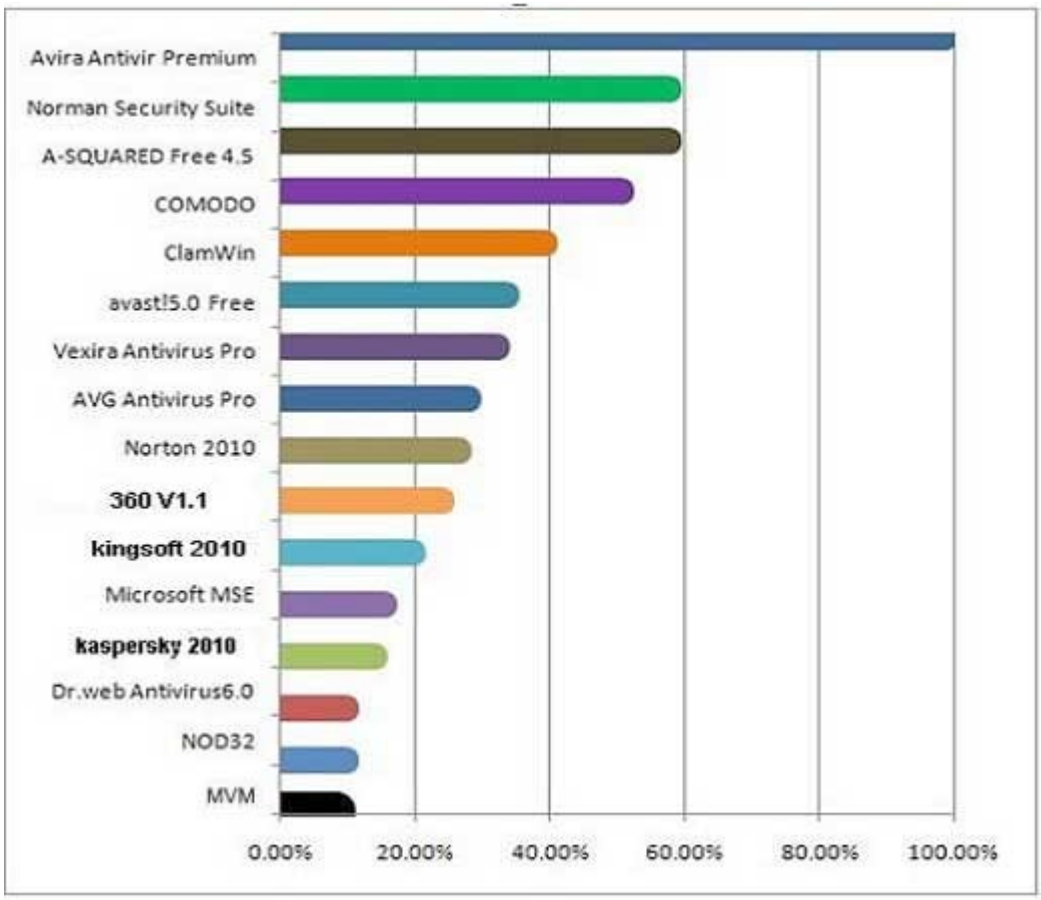


Fig 2.5

Note: the data comes from the anti-virus software false positives test in May, 2010 of third party forum bbs.kafan.cn. Lower number presents stricter false positives control. MVM engine ranks first in the false positives control test.

3.Typical application

MVM is cost-effective anti-virus solution provided for security company, network equipment manufacturers, network security vendors, mail service providers, software developers, etc. The engine can support Windows, Linux, FreeBSD, and other mainstream operating systems, as well as X86, Power PC, ARM and other hardware architecture.

MVM is portable and platform-independent, and has good compatibility that can work in binary level and other system source code level for any operating systems(e.g.: windows, Linux, FreeBSD) based on IA32.

The incidental advantage of having portable code is that MVM anti-virus engine can effectively separate and greatly be independent from the host system, which makes adding the detection process is relatively straightforward without repeatedly handling the problem of compatibility for every system.