

Twister Antivirus 8 Technology

Author: Filseclab Corporation
Website: <http://www.filseclab.com>
Email: info@filseclab.com
October 8, 2012

By Google Translate

Main Technology

Behavior depth tracking technology
Rapid response technology for real-time tracking
Rapid storage and retrieval technology (black box)
Technical analysis based on artificial intelligence model behavior (threat identification)
The rollback Technology of the I / O operation
Memory object of rollback technology
Windows kernel simulation technology

The buffer overflow defensive technology
Blue screen disaster protection technology
Enhanced self-protection technology
Trap technology

Gene identification technology
Gene signature database automatically generated
Metamorphic virus recognition technology
The shrink slightly characteristics technology
Automatically false positives exclude technology
Resource load balancing technology
Smart Speed Technology
Breakpoint sweep Technology

Virtual machine technology
API simulation technology
Static heuristic virus detection technology
The dynamic heuristic virus detection technology based on virtual machine
Virtual machine shelling technology
Macro viruses inspired technology

Static deformation virus removal technology
Static broad-spectrum disinfection
Virtual machine-based dynamic disinfection technology

The cloud fast query technology (comparable common database query is a hundred times faster)
Cloud identification techniques
Cloud intelligent analysis technology

Intelligent voice interactive control technology

Threat automatic sorting technology

The white program automatically sorting technology

Virus database is automatically updated technology

Program logic tracking technology PLT

Enhanced SVM artificial intelligence algorithms EX-SVM

V8 Highlight - Dynamic Defense 2.0

Filseclab second-generation dynamic defense development lasted four years, more than 400,000 lines of code amount, is one of the most complex systems in Fairbanks, it is basically a small subsystem to simulate and track the process of the operation of Windows.

The main highlights

The first used a metaphor to describe the features of the new version of the dynamic defense: a thief disguised as guests to the house to steal things, inspectors identified when guests but it is not a thief and forthwith to win, but the home has already been turned chaotic to restore is more difficult. The second-generation dynamic defense system can not only seize the thief, and make home restored as ever, and has the ability to earlier and more accurate identification camouflage better thief, including the current popular white with black Trojans. The main features are as follows:

1. Precise depth of the object-level tracking.

Full hot rolled back. Destruction threats. This mainly includes the threat of rewriting the files, registry, HOOK, memory, object modifications fully restore.

Smart Blackbox

Filseclab smart black box similar to the black box of the aircraft, it would have accurate and detailed record of each program in the computer unit behavior, it can track not only the program files, registry access, also including threads, memory, object manipulation and so on. And the minimum tracking unit can be accurate to the CPU's execution fragment, and event of each one of the participants. For example: a system

service thread in this time period is the normal procedure A service, the next time segment grafting of virus B and its services, the vandalism occurred at this time will still be accurate positioning to B without spread to the entire service thread. Another example: When the event of a deleted file, be traced not only to delete this file process also includes all modules and memory to participate in the action, even including the parent process, the parent thread will also be tracking. It is the new tracking framework can accurately locate the main anti-headache white with black Trojans.

In addition, the virtual black box have a lasting memory function, with the restart of the computer-zero acts have occurred even restart the computer target program will still be record so that when faced with a behavior deliberately playing scattered, still can accurately detect sub-periods combined to complete the lurking threat, which has the ability to handle multi-step or delay the onset of the backdoor Trojan and its radical scavenging and rollback.

MCBAS - Behavior analysis system

Complex logic rules and comprehensive analysis system to analyze the behavior of the smart black box records and automatically determine whether it is hazardous, that “Memorable Comprehensive Behavior Analysis System (MCBAS)”

Super rollback

The behavior of the unwanted programs implement accurate comprehensive rollback restore. It be harmful program directly generate behavior and restore grafting to the other procedural indirectly generated behavior, while not spread to the normal procedures. Such as: virus Explorer HOOK, rollback HOOK will restore not the end of the Explorer to keep them clean and continue to operate normally.

In addition, the virus modified or deleted files can be perfectly restored, this infectious virus infected files. Smart black box real-time backup will file, registry, memory, object occurred modifiability action tracking program behavior, and uses advanced algorithms ensure imperceptible impact on the system, so that even in the face of the infectious virus can still of rollback recovery once the damage.

Blackbox & Sandbox

The working mechanism of the traditional security software "sandbox": for any unknown program "presumption of guilt", that is, when an unknown program running sandbox will

assume that it is harmful, then put isolated environment inspection. The benefits of doing so if the program really harmful then generally the system will not affect substantially, but the actual situation encountered by users, most programs are part of the normal security, due to the normal procedures in the sandbox effective modifications would be more difficulties (for example, installed in a sandbox game is not it actually installed in the computer to go), or even need all discarded to allow the user to re-do it again. Sandbox for security vendors to the internal virus analysis or sample collection, but there are obstacles for the average user, it still belongs to professional applications. "Black box" FilseclabV8 in a derived from the the sandbox thinking but contrast mechanisms, the "presumption of innocence". It first assumes that the program is clean and harmless, and then complete tracking of each program's behavior record and modify the action only when the program only exhibit malicious behavior to prevent recovery returned to the original state. This mechanism and the active defense system perfect fit linkage, but also for users who do not exist on any use of the threshold, because the whole process is the V8 internal to automatically completed, there is no require users to automatically / manually into the sand, but also there is no application to modify the problem, and there is no difference in normal use, so Filseclab black box technology easier to use and more secure.

V8 Highlight – Malware Virtual Machine(MVM)

Malware Virtual Machine (MVM) is another extremely complex security system Filseclab smart antivirus 8. The main purpose of this system is constructed in order to detect unknown threats by scanning the way to make up for the signature lag, and enhance the defense capabilities of the new Trojans and packers deformation of virus. After years of research and development and continuous improvement, FilseclabMVM virtual machine inspired technology both from a technical level or the actual effect have similar systems to achieve the first-class level.

In order to verify the effect, have been invited to the British the VB100 evaluation agencies Virus Bulletin pure inspiration engine internal testing on a virtual machine, not black and white list support WildList recognition rate of over 60%, false positives can also be controlled at a very low level, making VB to its height evaluation "Well, it's still doing great considering it's only heuristics to and no signatures It seems to be detecting over 60% of our samples - better than some signature scanners!

The threat of virtual machine consists of two subsystems: the virtual machine system and heuristic analysis system. Virtual machine system used to simulate the program to run and collect program behavior the heuristic analysis system based on these behaviors target object to determine whether it is hazardous.

Virtual machine system

MVM virtual machine is an extremely complex virtual simulation system can parse and simulate almost all CPU instructions, thousands of API functions, and Trojan virus often involves some hardware simulation, such as: the hard drive, network card, etc.. It works by allowing the target program running in a virtual isolation environment, fully exposed and their true intentions, if it is found that there is malicious intent can be detected, while in no way affects the real system. Currently MVM off nearly 400 species of shells, can effectively deal with the packers, deformation signature is not easy to deal with the virus.

Heuristic analysis system

MVM heuristic analysis system is divided into two parts: static heuristics and dynamic heuristics.

Static heuristic does not need to rely on the virtual machine can work independently. It directly through the inverse solution of the binary code of the target program analysis of its intent, threat characteristics can be sentenced to do, so as to achieve the purpose of identifying unknown threats. The advantages of this approach is fast, but not be able to effectively identify the packers and deformation virus, the dynamic heuristic part can effectively compensate for this.

Threat procedures either packers or deformation, and the final total to go to achieve their own purposes, that is to say in the running when they shelling. The dynamic heuristic can let the simulation run in a virtual machine, took off his coat to induce it to attack threat either determination to be the goal of fully exposed their own malicious behavior, static identification of the dynamic defense.

V8 Highlight – Resource Balancing, Smart Disinfect,

Smart Scan, Privacy Protection, Threat Traps,

Anti-BufferOverflow, Anti-BSOD

Resource Balancing

V8 under the current system resources occupancy automatically adjust their own energy consumption, with low computer can run smoothly, not only security but also improve efficiency. Moreover, V8 and even allows you to arbitrarily set the virus library usage and memory footprint quotas, allow you the freedom to control its resources occupied.

Smart Disinfect

V8 virtual machine technology can be combined with universal repair of certain types of infections virus encountered panda Wiggins virus is no longer just "delete / quarantine" recoverable files to a clean state.

Smart Scan

Secondary scan through incremental caching techniques to the massive speed scanning speed can be increased by several times or even a hundred times.

Privacy Protections

Computer privacy in personal documents, photos and other data certainly do not want others peep, but the Trojans, backdoors, spyware popular today, privacy is stolen frequent but little known. Difficult for users to third-party software to ensure that their computer no hidden spyware or ulterior motives when to take their own files. The V8

provides the file privacy features, as long as the added protection of your important files, all programs that try to access these documents are required to get your permission, to protect personal privacy will not be violated.

Threat Traps

Encountered stubborn Trojan can not afford to repeatedly clear, simple inhibition of regeneration and File Shredder often does not address the root causes. V8 new trap function can be used to deal with this "gotcha". Stubborn threat created will have the ability to regenerate, to set up a virtual trap capture, to achieve complete removal.

Anti-BufferOverflow

V8 will be able to auto-immune various types of buffer overflow attacks. Encounter such even in the case of Windows system patch is not installed the latest threat to immediately detect and prevent, protect your computer from 0day vulnerabilities destruction.

Anti-BSOD

Due to virus attacks, software conflicts, unexpected computer system failure caused a blue screen may cause your work is interrupted or the file is missing. V8 provided a blue screen disaster protection can prevent the occurrence of some blue screen, and the termination of containment failure root cause a blue screen problem continues to spread, so that the computer can continue over a period of time safe operation is a critical moment in time to save important data to provide an opportunity to reduce losses.

Intelligent interactive control

You can be controlled by the voice of the V8, and there will be the response of natural language. "Filseclab", the software will pop up the main interface and answer "Hi, I'm here", said: "Scan my computer", the software automatically start scanning front of the computer, open voice capabilities. Each scan task has its own number, the user can at any time a single (collective) voice control those ongoing tasks, and allowed to report on

the status of each work. In addition, V8 voice provides a friendly daily greetings and application call, such as: news, shopping, search. And voice function is pure green, you do not have to worry about it in the computer to install any additional plug-ins.

V8 Highlight – Artificial Intelligence iRobots

iRobots

Filseclab intelligent level defined

* The primary automated processing system to solve the duplication of effort.

** Automated processing system with primary analytical skills and troubleshooting capabilities.

*** Moderately complex analytical ability and error to exclude the ability of automated processing systems, automated long-term unattended operation, human resources as an effective alternative.

**** Highly complex analysis and debugging capabilities and a large number of complex calculations, the analysis can to providing manpower can not be completed in a short period of time.

***** A high degree of artificial intelligence can be completely divorced from human intervention self-learning and self-improvement.

iRobot1 - Automatic collection system of the virus

samples

Smart Level: *

Service time: 2003

Features: automatically from the Internet sample provider, exchange collection and download sample for virus database definitions to provide resources to support.

iRobot2 - Automatic collection system of the clean files

Smart Level: *

Service time: 2005

Features: normal software from the Internet to collect and download automatically to exclude false positives resource support.

iRobot3 - Automatic sample sorting system

Smart level: **

Service time: 2007

Features: Automatic analysis iRobot1, and iRobot2 collected samples for quick sorting, black-and-white nature of the program.

iRobot4 - Automatic update system

Smart Level: ***

Service time: 2007

The function About: comprehensive analysis on result of iRobot3 and iRobot5, and automatically generate virus database definitions and the whitelist definitions and automatically publish update.

Case: from 2007 to the present iRobot4 has been successfully run for five years for FilseclabV7 provide continuous updates.

iRobot5 – Automatic Anti-FalsePositive sysytem

Smart level: **

Service time: 2007

Features: Auto correct known false positives and the potential false positives.

iRobot6 - iGene analysis system

Smart level: ****

Service time: 2009

Introduction: The use of artificial intelligence mathematical model to build automatic classification algorithm, from a sufficient number of samples to find out the difference between black and white two collections feature the entire collection of black-and-white nature in order to achieve a feature recognition, and combined iRobot5 reached the practical level automatically exclude false positives .

iRobot7 - Behavior analysis system

Smart Level: ***

Service time: 2010

Features: threat procedures performed in the virtual environment and track their behavior, a comprehensive analysis and determine whether it is hazardous. As a strong complement to iRobot3 and iRobot5, to enhance automated self-identification ability, the ability to identify new and unknown threats. Also provide a practical and reliable evidence to support the identification results.

Case: Filseclab popular samples submitted to the world's largest anti-virus organizations WildList from this system. Sample the WildList be submitted to do checksum verification after threat iRobot7 discrimination basic 100% WildList recognized, and final the WildList then the world on all major antivirus vendors provide samples comprehensive screening, identify overlapping part of the release, as the ICSA VB100 international certification testing standards. In which each issue WildList from Filseclab samples usually more than 35%, belongs to one of the highest rates of vendors, this can reflect iRobot7 a high degree of accuracy.

iRobot8 - EVANET Central nervous system

Smart level: ****

Service time: 2012

Features: the comprehensive analysis sent from EVANET client program behavior, attributes such as various features, automatically determine whether hazardous processing operation, the client automatically determines under EVANET analysis. Such as: warning, reduction or release.

EVANET - Security neural network system

EVA from the film "Avatar" movie in the Virgin EVA all life of the planet of Pandora (Pandora) connected together to resist foreign enemies as an organic whole in order to achieve indestructible. Filseclab to EVANET the name of all user computers effectively connected together to resist the threat in order to effectively enlarge the resilience. EVANET plan is divided into the following three stages.

The first stage

The upload client program or program characteristics of the potential threat to the cloud, again identified using cloud identification. Filseclab V7 this stage has been completed in early 2007.

The second stage

The wisdom of the computer users to determine the unknown threats. For example: According to the analysis of the different mode of operation of the user program, when many users demonstrate this procedure objectionable, it will be marked as a potential threat. FilseclabV8 at this stage.

The third stage

Intelligent union defense stage, when a computer is threatened, all computers have a perception, instructions can be issued by the EVANET central rescue of its implementation by the nearest computer, threatened computer back to life. Also be freed from the central command of automatically find the nearest rescue. This stage in development.

EVANET Home: <http://www.ievanet.com> (under construction).