What is in fact STOPzilla?

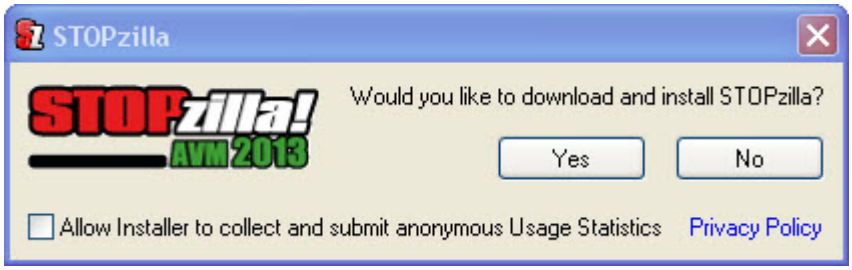
I'll start this article with an excerpt from Wikipedia:

> STOPzilla is a PC security software for the Microsoft Windows operating system. STOPzilla utilizes a proprietary AVM Technology, a multi-layered malware detection system that detects complex malicious threats while using minimal system resources. STOPzilla's AVM Technology constantly scans, detects, and quarantines malicious threats without affecting the PC's performance.
>
> STOPzilla AVM protects the user's computer from computer viruses and malware. The current version of STOPzilla, STOPzilla AVM 2013, incorporates iS3's new AVM technology, which uses a multi-layered defense architecture, utilizing both heuristic and behavioral detection. STOPzilla can be installed in hostile environments where an infection has already occurred, and its built in anti-rootkit technology allows it to detect malicious threats that might affect the Master Boot Record…

I few days ago, a reader asked me to write a review of this antivirus. Every time I hear about a new anti-virus technology my curiosity is triggered or **AVM**, their proprietary technology which stands for **Antivirus; Anti-Malware** seems to be a "newly developed anti-virus technology for Microsoft Windows operating systems, developed by iS3" according to Wikipedia, which "received a perfect malware detection score of 100% on a recent certification test conducted by West Coast Labs, part of the Haymarket Media Group and one of the world's leading independent test facilities for information security products and services".

It sounds good so far, so I have downloaded and installed *STOPzilla AVM 2013* to see the new technology in action.

When you start the installation the *"Allow Installer to collect and submit anonymous Usage Statistics"* is ckecked by default, you can uncheck it if you are paranoid with privacy.



start_installation

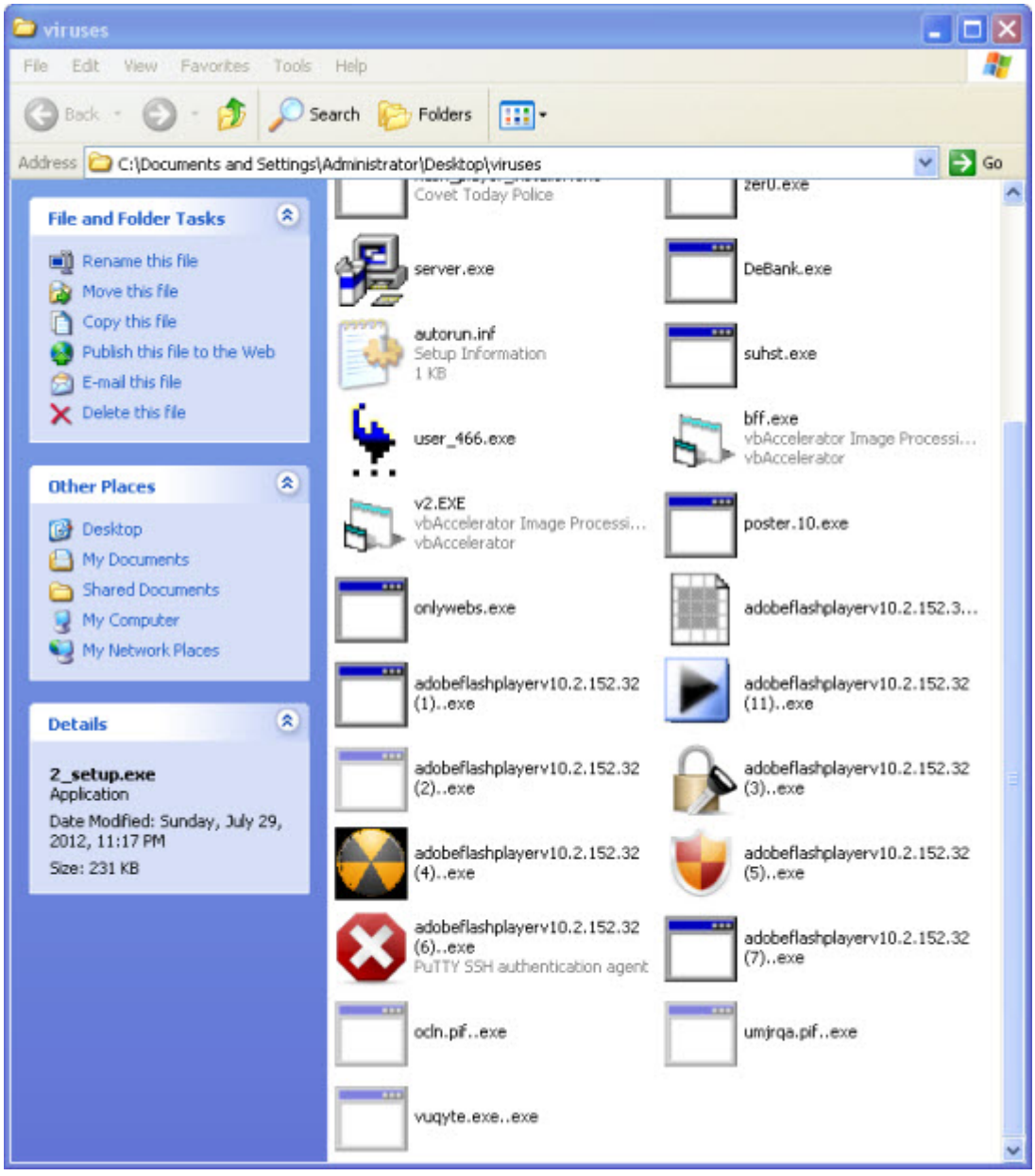
The collecting of *Usage Statistics* is done via a program component *DeskMetrics*(DeskMetrics.dll), this component can collect all kind of information about users:

- How many people are currently using it?
- It might know how many people downloaded its software, but how often users launch it?
- Do users use it every day? Maybe only once a week, or once a month…

- Is it used mostly Monday through Friday, during the day?
- Do users have Java installed in their computers? Which version?
- Do people get lost in the user interface?
- How many people are using pirated serial numbers?

I must add that I have not a professional antivirus testing Lab, rather a bunch of viruses and trojans in my collection with various detection ratios on virustotal.com but good for in-house(or real world) testing of an antivirus detection abilities.

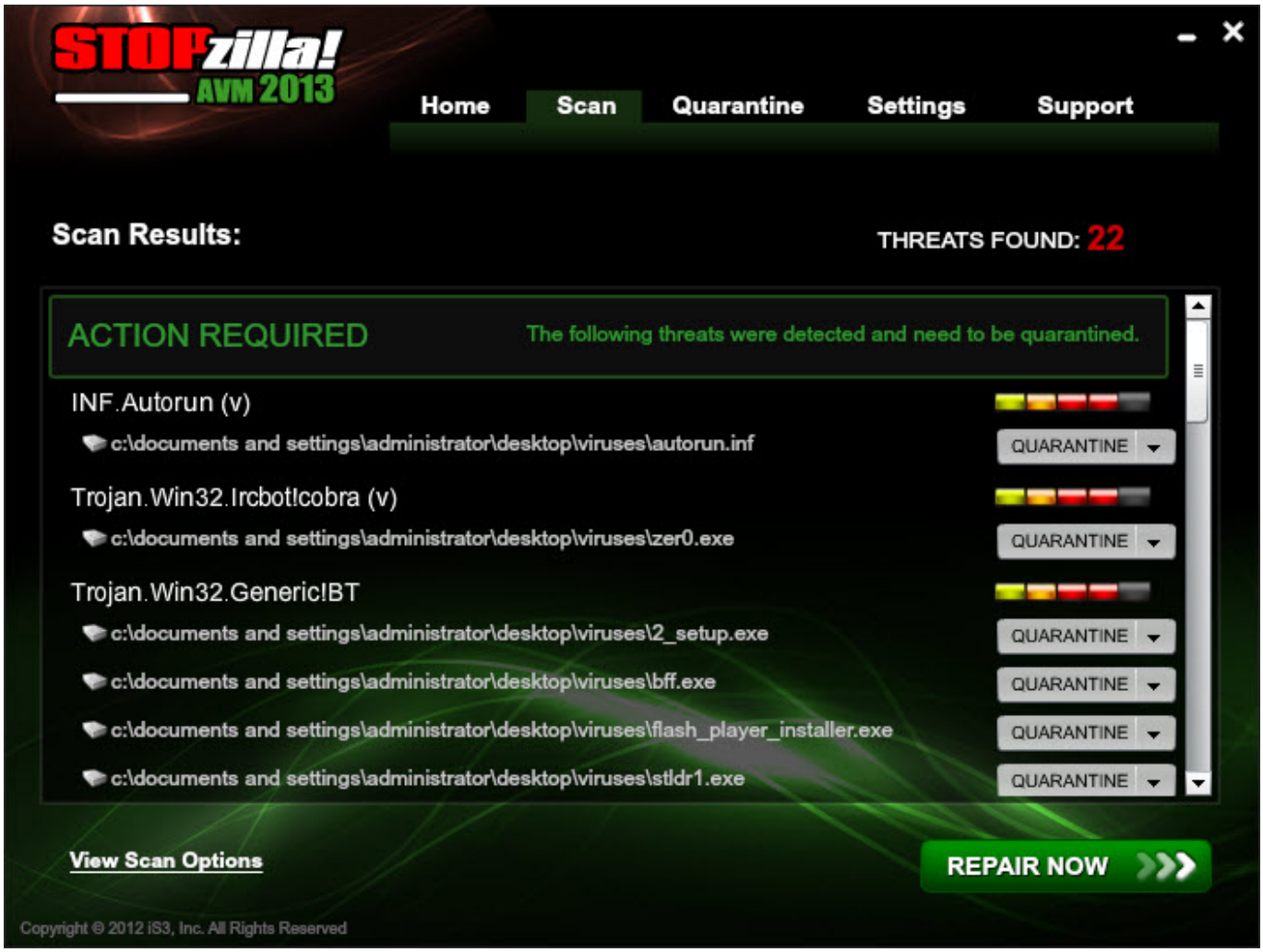
I have tested using *Custom Scan* a folder with **29** viruses of all kind.



Scanned folder

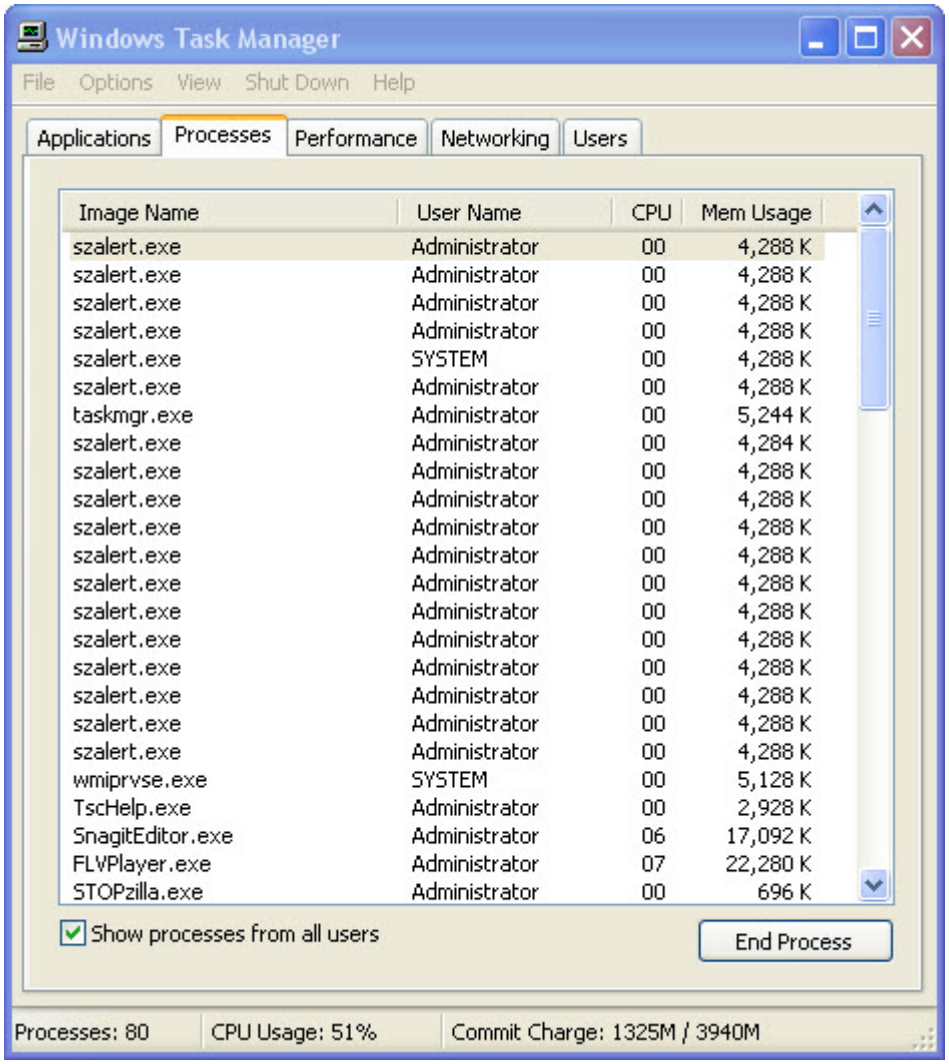
Selecting “Using Advanced Anti-Virus Engine” option STOPzilla came up with **22** detections, an acceptable **75%** detection rate, without that option selected the detections number was of only **13,** a very poor rate.

What intrigued me was that STOPzilla failed to detect the *Sality* worm, you can see it in the image below as hidden files: *ocln.pif.exe, umjrqa.pif.exe, vuqyte.exe..exe*



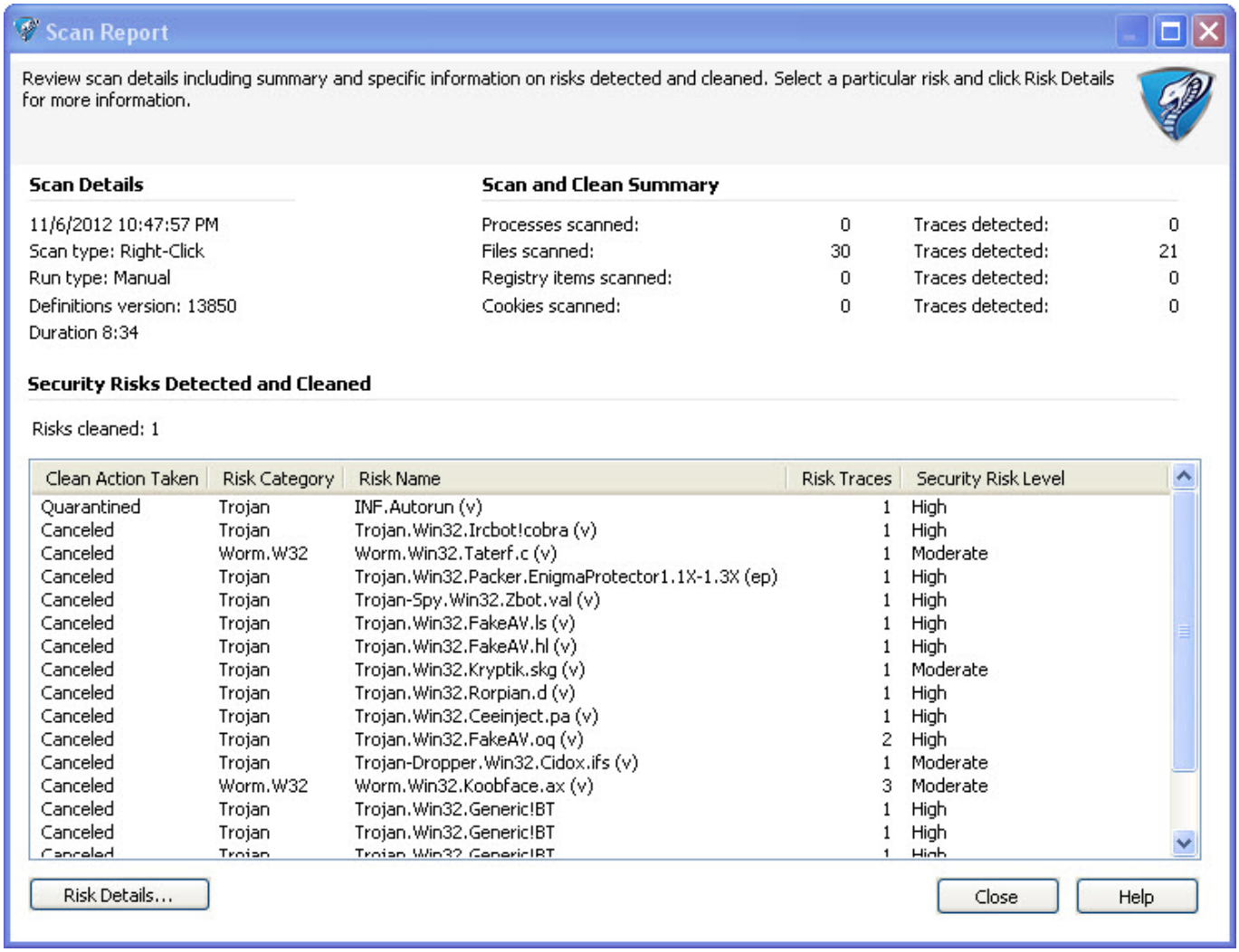
Threats found with advanced engine

The *Active Protection* has done a pretty good job blocking automatically some malicious registry keys, quarantined some viruses when I have opened their folder but I noticed STOPzilla seems to have little bugs. The computer frozen several times and Windows Task Manager showed an unusual number of a STOPzilla component *szalert.exe* instances running in the same time:



buggy application

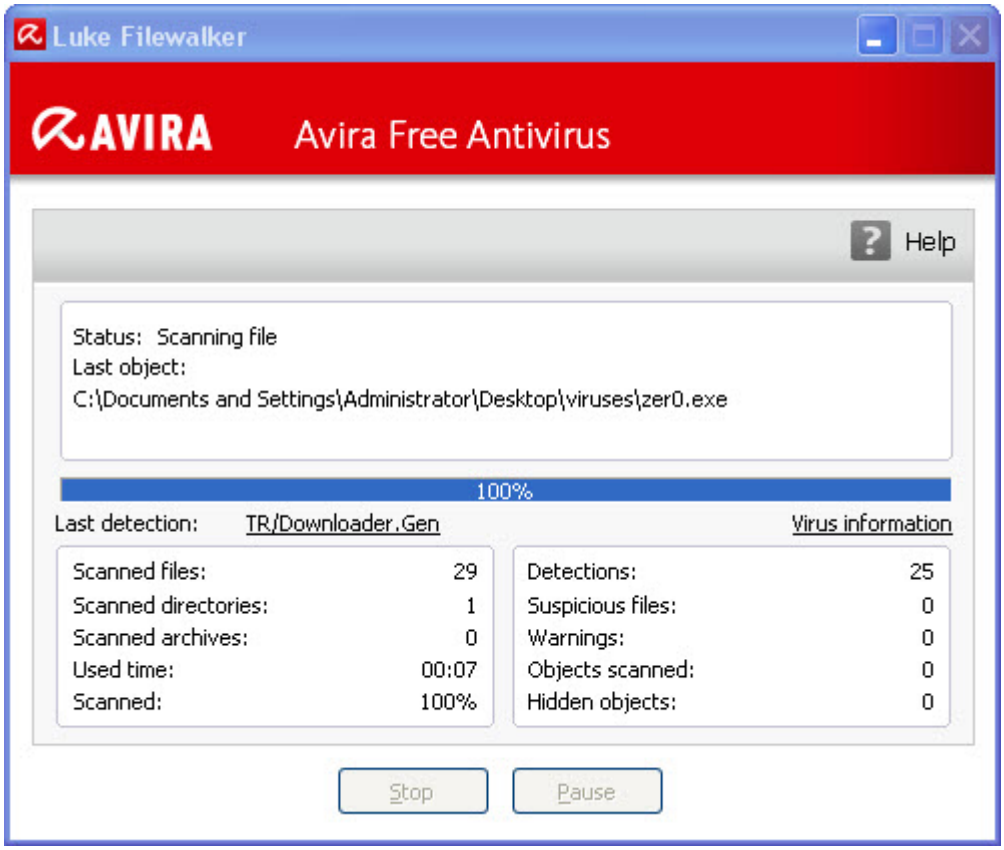
Now , the results of the scanning procedure of the same folder with *VIPRE Antivirus 2013*, you will find later why I choose this antivirus for comparison, see how the viruses are named with the same names:



VIPRE antivirus

Even using the *VIPRE Rapid Scan* feature, the scan of a **44 MB** folder took near **9 minutes**, very long if you have GBs of data for scanning you do the calculations how long it can take. The same amount of time was necessary for STOPzilla to scan the same folder.

The last comparison was made with *Avira Free Antivirus*, it detected **25 from 29** viruses in **7 seconds** ! Now, that's a result.



avira scan

Maybe you ask now why I made comparisons between STOPzilla, VIPRE and Avira. Avira because is a powerful antivirus and I take it as a standard and VIPRE because VIPRE is made by *GFI Software* company.

If you take a look at installation folder of STOPzilla you will find that a lot of its important components including system files(.sys) drivers are coded by GFI, see the files properties:

C:\Program Files\STOPzilla!\Drivers\i386

- sbaphd.sys

Description: GFI ActiveProtection hook driver

- sbapifs.sys

Description: GFI ActiveProtection Filter

- SBREDrv.sys

Description: GFI Anti-Rootkit Driver

C:\Program Files\STOPzilla!

- sbap.dll

Description: Active Protection Library

- sbre.dll

Description: Anti-Rootkit Engine

- sbte.dll

Description: Threat Engine Dynamic Link Library

and many more like these. It seems that “newly developed proprietary anti-virus technology for Microsoft Windows operating systems, developed by iS3″ uses heavily GFI components.

In conclusion, STOPzilla definitely is not a scam or a virus software as I read in some reviews, I speak now strictly about the program, I don’t know about the services offered by the company. Though there is place for a lot of improvements as the scanning speed, detection rate or application stability, it does its job removing viruses. But there is no doubt that users will notice that are better alternatives that STOPzilla Antivirus, some of them free.

Keep safe !

Share this:

- Share