ByteHero Unknown-virus Detection Software (BDV) review

A few days ago when I was scanning a file on virustotal.com, I noticed a name less known to me: *ByteHero*. Googling a bit I found the official product website at: http://www.bytehero.com/english.asp. The software is developed in China by *ByteHero Information Security Lab* and is promoted as a first class dynamic and static heuristic analyzer. Because the main component of it is a heuristic detection engine, the software does not need a virus signatures database therefore there is no need to be updated very often like other antivirus software.

Perhaps you will ask why I give so much attention to this heuristic detection engine. Because, I remember the times(just a few years ago) when antivirus software rarely exceeded 20 MB in size, now a common antivirus size is several hundreds of MB and is constantly and exponentially growing due to a bigger and bigger signatures database. More viruses and variants of the existing viruses, packed, crypted, obfuscated, God knows how modified are going live every day rendering the traditional antivirus detection useless. The cloud technology add an improvement to the security field speeding up the malware recognition process once its signature is added somewhere in the cloud. But sometimes weeks passes before a malware to be identified and a signature created for it. That's why I think a good heuristic detection engine is the future of the computer's security.

Back to ByteHero (BDV) software, I've emailed to one of the addresses posted on the official website requesting more info about it and the reply was quick. The BDV heuristic detection engine seems to be widely used in China by security software developers as a third-party embedded module. It is platform independent meaning it can run on Windows, Linux, freeBSD and supports many architectures: X86, ARM, PowerPC, etc. The number of packers supported by this virus detection engine is simply huge: near 400 packers and compressors.

The unknown-virus detection process has two phases:

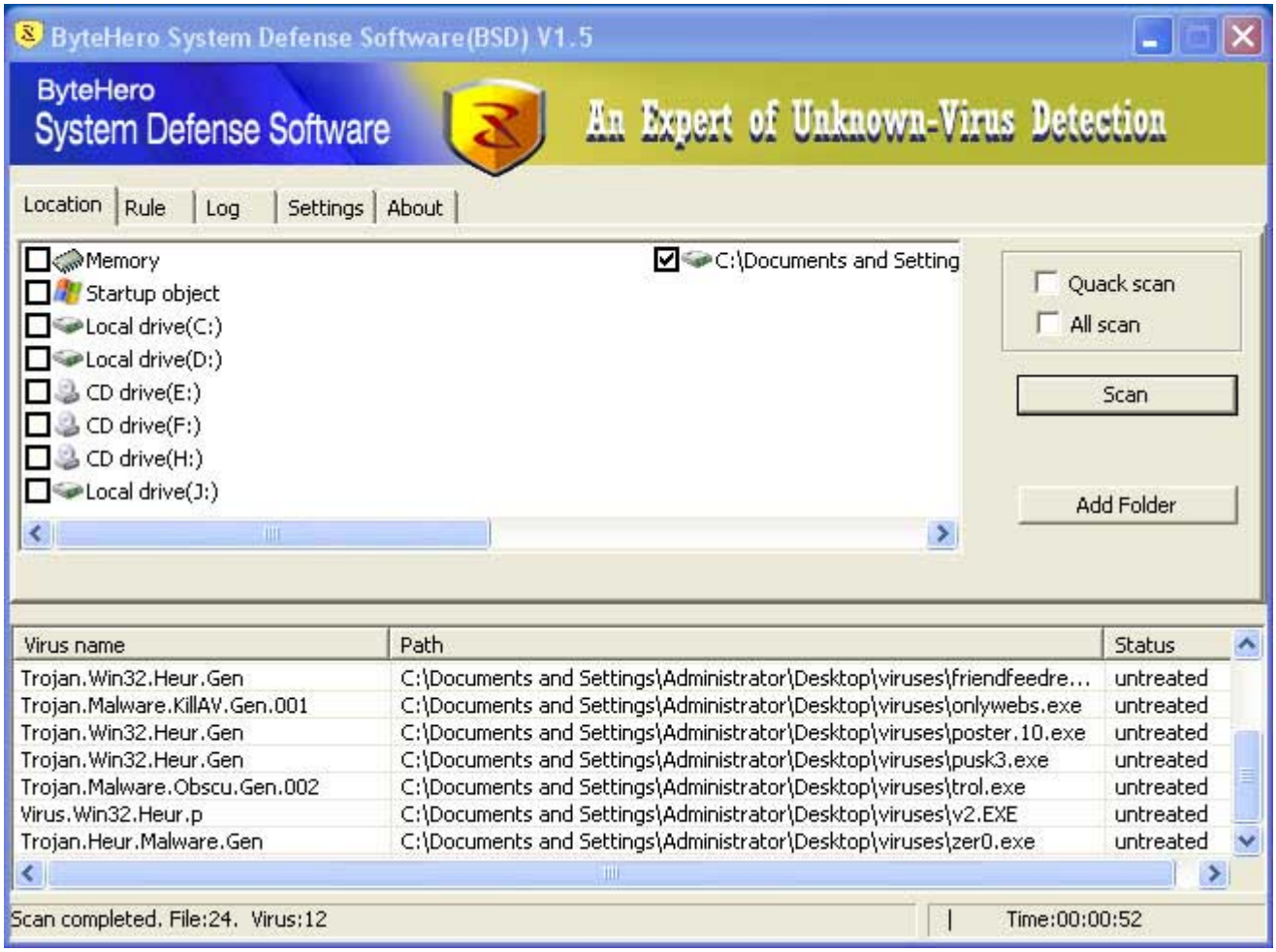
- Dynamic code analysis is provided in a virtual environment where the program behaviour is monitored in real time stopping the execution if a malicious action is found

- Static code analysis where the program execution is simulated in order to determine its logic. Other factors as interpreting the functions, parameters, disassembled code are combined in a detection algorithm and offer a good general view about the analyzed program characteristics.

All these features in a 2 MB size anti-virus solution, that's a great news but let's test it for real.

I have selected *randomly* 24 trojan viruses from my collection and put them in a folder:

Scanning the above folder gives a 50% detection rate, which is really amazing for an anti-virus like program without a database and only 2 MB in size.



I was surprised to see how ByteHero detected properly the malware where big security vendors fail, for example *friendfeedreg.1.exe* which is a crypted version of Koobface worm scanned at **Jotti's malware scanner**:

or see the scanning results of a crypted version of the Bifrost trojan used for remote controlling an infected computer:

The results are speaking for themselves, ByteHero (BDV) is a great software, but we can not forget the remaining 12(50 %) undetected malware samples from our test. Even if BDV has a *Process Monitor* for real-time scanning the started processes, at this stage of development it can not be considered a complete security solution, rather a great complementary tool that deserves all of our attention. Using it besides an classic anti-virus will greatly improve your security in regard with new and unknown computer viruses. And for sure it can be a great source of inspiration for security software developers.

Keep safe !

Share this:

- Share