Webroot SecureAnywhere Antivirus 2012 short review

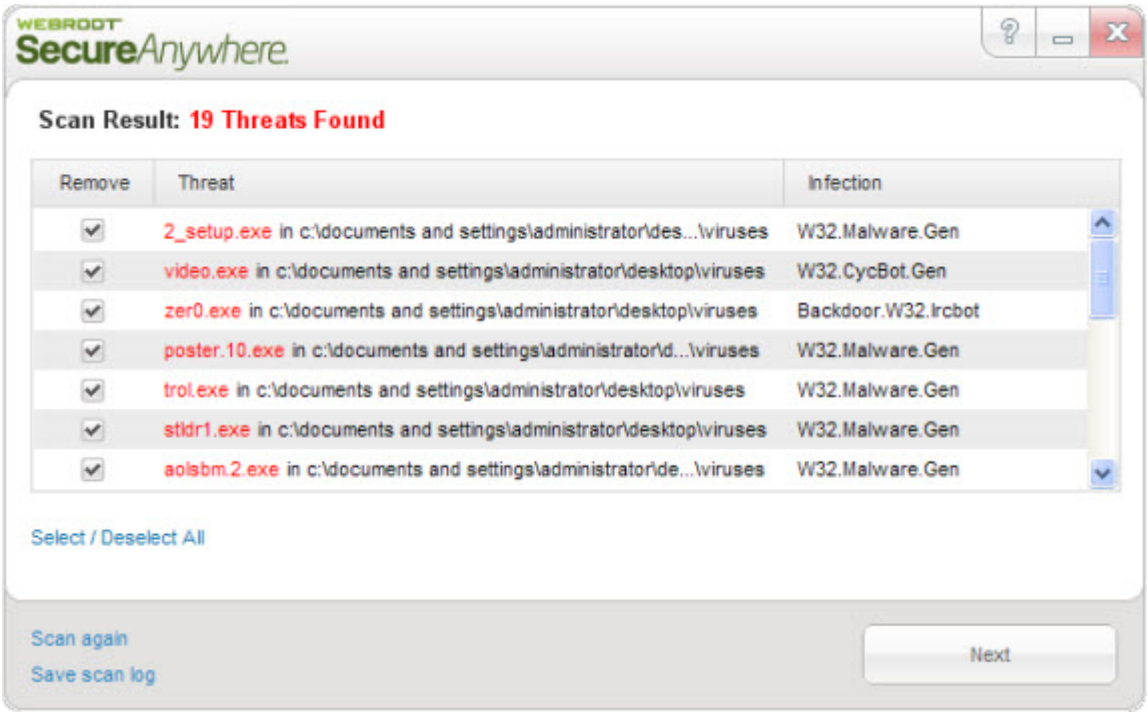
As requested by one of the site's visitor, today I have tested *Webroot SecureAnywhere Antivirus 2012* (hereinafter referred to as WSAA) against the same bunch of malware as in the last article, to make a comparison between it and *ByteHero Unknown-virus Detection Software (BDV)*. The main idea was to test the heuristic analysis capabilities of these products.

With an installer of about 618 KB, WSAA seemed to be another revelation and when I received the trial installation key in a webpage containing also this warning:

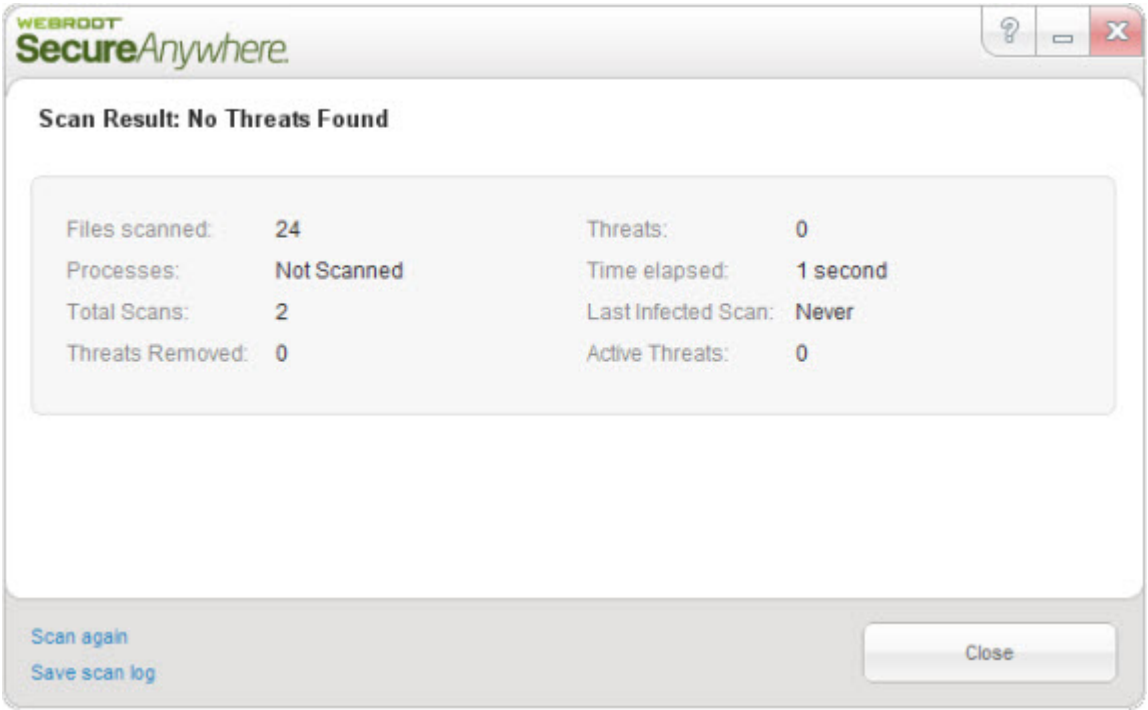
> Fasten your seatbelt. You're about to experience the fastest, most effective Internet security you've ever seen.

my adrenaline level was raised to the sky. So after installation I performed a custom scan of this folder containing random malware from my computer:

The scan was indeed amazingly fast and the detection rate was 19/24(79%), that's pretty good.



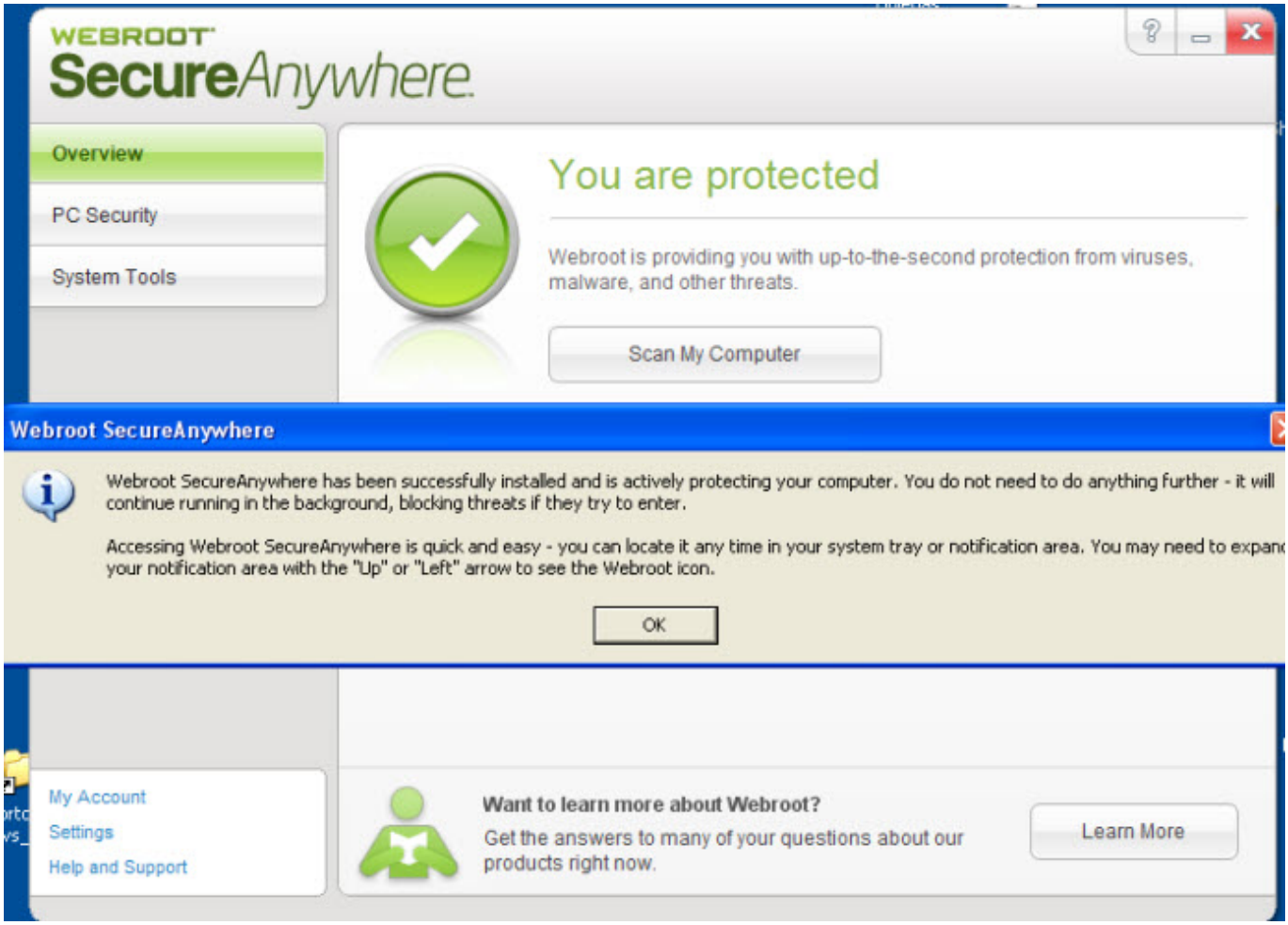
With a light resources footprint, an installation folder under 1 MB, it seemed to be a revolutionary antivirus at least for a moment. The big surprise comes when I was not sure if the detection engine is based on the cloud or on a heuristic analyzer(malware behaviour analyzer) so I have disconnected the computer from the Internet and I performed a new scan of the same folder. Well, I was disappointed to see that *Webroot SecureAnywhere Antivirus 2012* is based entirely on the cloud technology and it has not any heuristic detection engine or maybe a very weak one, here are the results:



and part of the scan log:

My guess is that WSAA calculates very quickly the MD5 hashes of the accessed files and compares these local hashes against the malware hashes from the cloud database, that is the “detection engine”. This database is the same with the Prevx malware database which is known to be huge; for who does not know, Prevx was acquired by Webroot in november 2010.

Another unpleasant surprise comes from the fact that instead to request the Internet access to do its job, WSAA showed me this screen claiming that my computer is fully protected which obvious was a false statement since it does not detected anything without access to “the cloud”. Remember, the computer was disconnected from Internet when I saw this :



In conclusion I can not compare ByteHero with WSAA because they are two fundamentally different products: one is based on a heuristic analyzer engine, the other is based on the cloud technology. But, although expensive, WSAA has a few qualities:

- It’s low on computer resources usage;

- It scans extremely fast;

-It has a very small size, near 1MB;

-It does not need to be updated because it has the core in the cloud;

-It does not interfere with other security software: firewall or antivirus;

Be safe !

Share this:

- Share