

Review: Trustware BufferZone 1.6

By Mark Woodstone

Over the years we have seen a number of different concepts that were trying to help the state of security of an average Windows PC user. Earlier, the only major problems were viruses, then we saw Trojans, worms, spyware, malicious scripting, etc. Antivirus software nowadays incorporates scanning for all the mentioned types of pests, but the approach that is based on signature updating and therefore on human intervention is not a perfect way to secure a PC user.

Security company Trustware (www.trustware.com) has a product that takes a new approach on protecting the end users. BufferZone is centered on a concept of virtualization technology, that creates a whole new secluded environment on your computer.

After installing the software, you are guided through a mini presentation that introduces you to the process of setting up your BufferZone. Although usage of terms like "virtualization" and "buffer" might be a bit complicated for the average PC user, the concept is very easy to comprehend and to setup.

Fighting the malware

Your connection to the Internet has probably the biggest potential of damaging your computer in any way. Using a non patched browser and visiting a site with malicious code can very fast compromise your computer. Downloading and starting a file without any proper checking by a 24/7 updated antivirus product could generate a massive infestation that will soon hurt your computer in many ways. These are just some of the constant threats PC users are susceptible to.

BufferZone comes to the rescue – with only a few of clicks you could create a defensive shield

around all the pieces of software that interact with remote computers over the Internet. For instance, if you are still using Microsoft Internet Explorer, you are probably well aware of the problems unpatched versions of this software could generate. Never mind, just add Internet Explorer into the BufferZone and every potential malicious script will execute in this simulated environment and therefore won't have any impact on your real computer files.

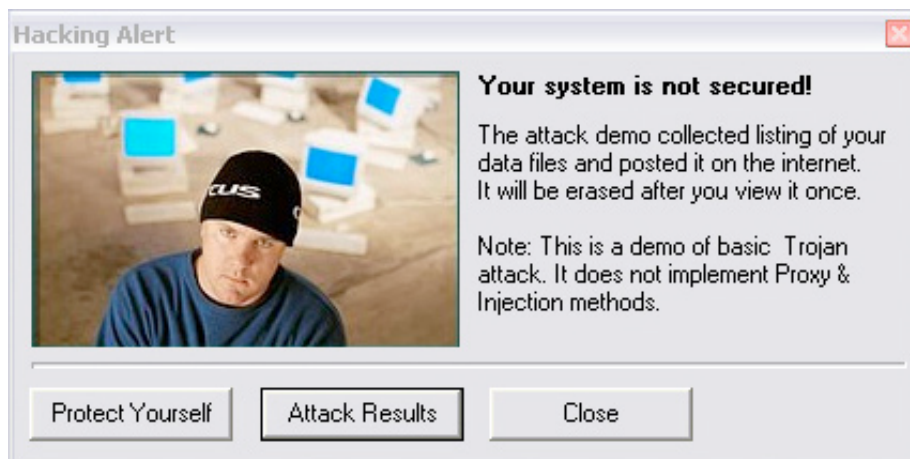
From my perspective, the real power of BufferZone is not just real-time protection from the problems that can occur while browsing, but the possibility of reassuring that downloaded files are secure for running.

In the test case scenario, I tried to download a Trojan that gets a list of all my files and sends it to an online web page. I downloaded the file and started it while it was placed outside the BufferZone. The Trojan did its payload and very soon I could see my details online. I then sent the file to the BufferZone and started it once again.

This time the test Trojan encountered an internal error as he couldn't list my files, and it reported that my computer was secure. I usually download a lot of different files from the Internet, especially from sites like Sourceforge and Freshmeat.

Although they have different methods of taking care of file integrity and security, you never know

when you will come across an “evil” developer that will create some kind of a unsafe file.



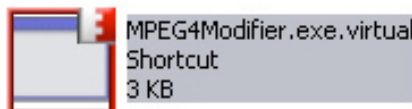
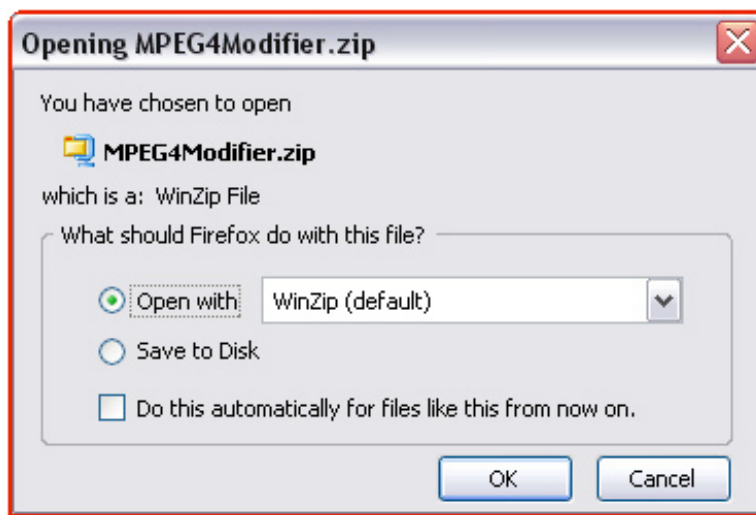
Test Trojan output when application is run outside the BufferZone



BufferZone main screen

During my tests, I ran different programs in the BufferZone, from simple SCP clients and Instant Messengers to an mpeg4 modifier program that I used for editing a couple of gigabytes of digital video files. All programs worked like a charm, I didn't come across any potential problem. There is a very nice visual touch – all programs that are in

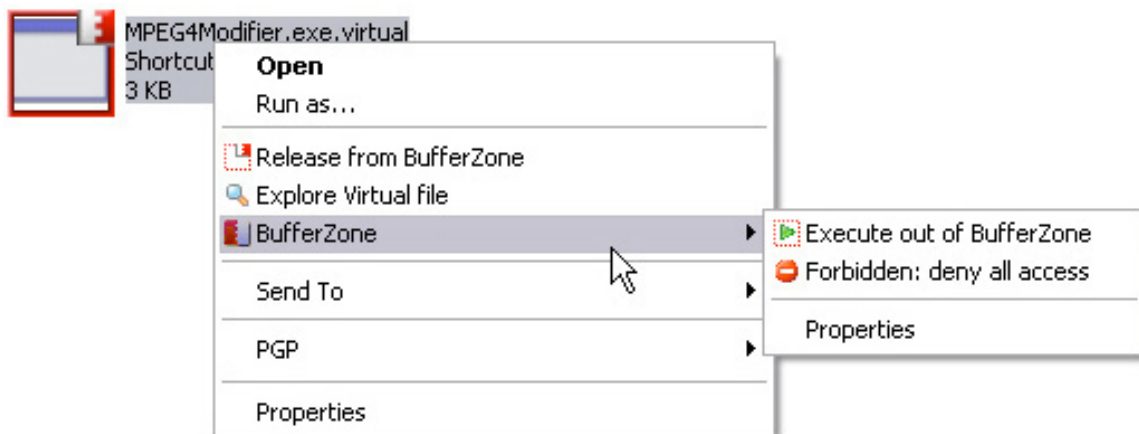
the BufferZone have a red border around their icons and windows (see an example on the following page). This way you always know if you are working within an insecure or secure environment. If the border annoys you, you can disable it from the configuration menu.



The red border indicates that this file is in the buffer zone

The program hosts a couple of customizing features. You can group specific files under several categories including Web, Mail and P2P. This helps a bit as the most popular software is predefined. When you start BufferZone out of the box, it

will immediately add the popular Internet related tools into its environment. You can also add your own software into these categories, making it easy to enable or disable a specific set of programs.



If you want, any file can be sent for execution outside of the protected zone

From the enterprise point of view, BufferZone 1.6 incorporates advanced management tools for monitoring, controlling and enforcing user activity throughout the LAN. These include an enterprise-wide, automated, scheduled BufferZone technology re-set that removes BufferZone values from Windows registries without data loss. Also, there is a tool that controls and prevents installation anywhere on the LAN of software not originating from

designated servers and lets managers define acceptable filename extensions. Managers could also monitor all BufferZone activity in real time.

Overall, BufferZone is a must have software for Windows users. Its powerful virtualization engine creates a trusted environment that you will very soon fall in love with. The software is very easy to setup, manage and use.

Mark Woodstone is a security consultant that works for a large Internet Presence Provider (IPP) that serves about 4000 clients from about 30 countries worldwide.