# Frequently Asked Questions

### *What is the McAfee® Command Line Scanner Project?*

The *McAfee Command Line Scanner Project* (MCLSP) provides an automated way to scan a Windows system for viruses and malware from a live Linux boot CD or USB thumb drive using McAfee's command line scanning engine.

### *What is the McAfee® Command Line Scanner for Windows?*

The McAfee command line scanner is a portable executable (PE) command line version of their powerful A/V scanning engine. It is highly configurable and scriptable. For many years the scanner was included in the SuperDAT package that was freely available on the web.

Unfortunately, McAfee® no longer provides this tool to the public. It must now be purchased. You can download an evaluation copy of the scanner here.

### *What problem are you trying to solve?*

I work in the digital security world and do a lot of on-site emergency incident response work for clients. Entrenched malware is sometimes very difficult to remove from a live Windows system. A very effective method to remove stubborn malware is to boot a system with a memory resident operating system instead of the native Windows OS, and use McAfee's® command line scanner to scan and clean all volumes.

In the past, I have used a BartPE boot disk with some custom plug-ins to perform this task. BartPE provides a bootable, memory-resident version of Windows XP. There are two problems with this approach: First, Bart is no longer working on the project, and second, there are no plans to port it to Windows 7.

A second and more frustrating problem is integrating the proper device drivers. If a BartPE boot image does not have the proper drivers for a system, it will blue screen. This required me to spend a lot of time finding drivers for particular systems in order to get the BartPE image to boot. To say the least – this is very painful in the middle of an incident response engagement.

So – this project, launched out of BartPE frustrations, provides a bootable Ubuntu Linux image that runs the McAfee® command line scanner.

### *Ok – so how do you run a Windows application on Linux?*

As is so common in the open-source Linux world, a group of very smart and very innovative programmers pooled their talent and created a module that 'fools' Windows application into thinking they are running on a Windows box. The module is called 'Wine' (Wine is not an emulator). The McAfee command line scanner runs just fine under wine. You can learn more about the Wine project here.

### *What does the tool do?*

The main purpose of this tool is to boot a Windows system with a memory resident version of Linux and automatically scan all FAT and NTFS volumes for malware using the McAfee® command line scanner. Many people (including me) believe the best way to scan a Windows

system for malware is to scan the volumes when they are not mounted or in use by the native Windows OS.

The tool is completely configurable through the use of an ini file and the numerous command line options of the McAfee® scan engine. The default configuration file mounts all FAT/NTFS volumes in read only (ro) mode, scans all files for malware, and reports its findings. To have the scan engine clean, delete, or quarantine infected files you need to change the ini file settings to mount the file systems in write mode (rw) and change the scan engine option file settings to your liking.

The real power of this tool is evident when you have dozens or even hundreds of infected systems that need a thorough malware scan without the interference of the host OS. You simply put a CD or thumb drive in a system and boot to the device. The scan will occur automatically once the system boots.

***How do I build a custom Linux CD to use the scanner?***

After many hours of research and endless tinkering, I have created a series of scripts with accompanying documentation to make this process pretty painless. The steps to create a bootable iso are listed below:

- Install Ubuntu Linux on a spare desktop or laptop computer. You will use this system as your build platform. I recommend you install Ubuntu 10.10 Desktop since this is the platform I used to build this project.
- Download and unzip the MCLSP project files and scripts from www.malware-hunters.net. The folder structure that gets created will be used to build your iso.
- Copy the Ubuntu 10.10 Desktop is to your build folder (Ubuntu-10.10-Desktop-i386.iso).
- Download the latest *McAfee VirusScan Command Line for Windows* install zip file and place it in /opt/mclsp/mcafee.
- Make sure your build machine is connected to the Internet.
- Run the three scripts provided in the project kit (prereq.sh, chroot.sh, and build_custom_iso.sh.)
- You will now have a custom bootable LiveUbuntu iso that will boot a system to Linux and automatically run a virus scan on all Windows volumes.

***Will the MCLSP run from a thumb drive rather than a CD/DVD?***

Yes. The project documentation shows you how to do this with a free tool. Booting the distro from a USB thumb drive is must faster than booting from a CD/DVD.

***Is there a fee for using this tool?***

No. I build a lot of tools for incident response work. In the spirit of giving back to the digital community that provides us so many incredible free tools, I provide this tool at no cost to anyone that finds it useful.

***Can I use the MCLSP project to build my own custom Linux distribution?***

Yes. The build process is very generic. The creation of a custom distro is pretty straightforward. You take a base Linux distribution, in this case Ubuntu-10.10-Desktop, remove packages you don't want, add packages you do want, and customize the X Desktop environment.

The unique thing about the MCLSP project is that all the hard work to get Wine installed on a custom distro is already done. You can use the project scripts to create a custom Ubuntu distribution that will run any Windows application that runs under Wine version 1.3. The possibilities are only limited by your imagination.

Remember, you have to obtain your own copy of the McAfee® command line scanner tool on your own, and abide by the requisite McAfee® licensing requirements.

***This is a pretty cool tool. Are there any plans for enhancements?***

Yes. The next release of the tool will include the ability to boot a system from the network via PXE (Preboot Execution Environment) and automatically mount and run the MCLSP image. This will remove the requirement to physically touch a system you want to scan. Think large enterprises.

Any other suggestions for improvement are most welcome.

***Who created this project?***

My name is Michael Spohn. I am a professional incident response consultant based in the Los Angeles area. You can email me at mspohn@malware-hunters.net.

***Where can I learn more about this project?***

The project is well documented. You can find the project docs www.malware-hunters.net.