FAQs about the Virus Remediation Training

In the course of presenting webinars that introduce the principles of the Virus Remediation Training workshop, I have received quite a few good questions about the content of the workshop and malware-related issues in general. Here are some of the most relevant ones:

1. *What Operating Systems are covered in the workshop?* The workshop is strictly about Microsoft Windows, no coverage of Macs, iPads, iPhones or Android smartphones. All versions of Windows from Windows 95 through Windows 10 are discussed, with the majority of time being spent on Windows 7, 8/8.1, and 10. There is still some coverage on Windows XP, since that Operating System isn't completely gone yet. Windows Server 2003, 2008, and 2012 are touched on as well.

2. *Does the cleanup taught in the workshop make computers run faster?* By definition, the fewer programs (Processes) running in the background, the faster and more responsive a computer will be. A natural side-effect of cleaning a computer using the methods taught in this workshop is that the computer will run faster as a result.

3. *Does the workshop cover where the infections come from, or how the computer got infected?* Not in much detail, the focus is more on removing the infection and moving on. But we do cover preventive measures beyond just having an anti-virus program and keeping it up to date. Today by far the most common source of infection is from infected web sites (mostly legitimate ones that have been compromised). The most important defense against these attacks is to keep the ancillary programs updated, especially Java, Flash, Adobe Air, and Adobe Reader.

4. *Does the workshop include procedures for cleaning infected web sites?* Not really, that's more an issue for a webmaster than a support technician. The workshop does cover steps you can take to prevent a computer from becoming infected from a compromised web site, though.

5. *Are infections coming from USB drives that auto-launch?* Not very often, as Microsoft has changed the default setting to keep the autorun.inf file from automatically launching. Some malware changes that setting though, and puts autorun.inf files with a malicious payload on one or more network drives. So as soon as the user connects to that network drive, their computer becomes infected.

6. *Does the methodology taught in this workshop allow for remote cleaning of infected computers?* Most malware can be successfully removed from infected computers remotely using the procedures and tools from this class. Even rootkits in most cases can be removed without requiring an on-site visit to the infected PC. The only significant exception is those extreme cases where the computer cannot be booted at all, even into Safe Mode with Networking.

7. *What about disconnecting from the Internet before starting the removal process?* This is a prudent step to take if you have indications that the malware is attempting to replicate, to infect other computers on the network or across the internet. The great majority of current malware does not attempt to spread beyond the local infection, so I usually leave the infected computer connected to the Local Area Network and the Internet.

8. *Where are some typical hiding places for malware?* This is the subject that consumes more than one hour in Session 3 of the Virus Remediation Training workshop. The short

answer is that it is hiding in the Registry, somewhere. Finding exactly where is the trick. We start with a discussion of the Run keys and work our way out from there, covering over 200 specific subkeys where malware may be found or activated.

9. *With drives getting larger and larger, how can you do a scan in under two hours?* This is one of the "secrets" that's revealed in the workshop, but here's a hint: It's related to the various options and settings available to you with different anti-malware programs. And remember, this workshop is not about running multiple scans with different programs; in most cases you will run a maximum of three scans, with a total run time of less than one-half hour.

10. *What currently available virus/malware tools are in the Virus Repair Toolkit?* Too many to list (more than two dozen), some of which you would recognize. Some of them can cause more serious problems if not used correctly, in the proper sequence and with the correct options, so I will not talk about them without the full context of how and when to use them. I do like and include some of the popular favorites, though, such as MalwareBytes Anti-Malware and TDSSKiller. Some of the included tools are proprietary and only available to graduates of the Virus Remediation Training workshop.

11. *What anti-virus programs do you recommend after the infected computer has been cleaned up?* There are several good ones, and a lot of it comes down to personal preference. My top two recommendations are usually VIPRE Internet Security (not just the anti-virus) and the Emsisoft Internet Security suite. Emsisoft is not very well known in the U. S., but they have been very responsive in dealing with some of the newest and most widespread malware threats.

12. *Which anti-malware products to avoid?* Don't want to get myself in trouble in a public forum such as this, but once again, a lot of it comes down to personal preference. My experience has been that any product that includes "Spy" in its name is hopelessly out of date and unlikely to be of much value today.

13. *Do you see any benefit to using portable versions of the various malware scanners that are available?* Given a choice, it's always safer to run a program from an external device such as a CD-ROM or thumb drive than to install a new piece of software on an infected computer. But in most cases popular programs such as MalwareBytes can be installed on the target machine without causing any problems.

14. *Is the workbook available for purchase instead of attending a workshop?* No, the workbook is exactly that – a workbook. It's not a tutorial or self-study guide; it's intended to review and reinforce the topics covered in the workshop, and serve as a reference when you're working on a malware infection. Just as with the question about the tools included on the Virus Repair Toolkit, the context of these topics is critical. Simply taking a chapter or paragraph by itself without understanding what precedes or follows it could lead to really bad outcomes.

15. *Is the workshop available online, or recorded?* Yes, the full workshop is now offered online, normally scheduled for two consecutive days of 4 hours each day. The technology used at present is essentially an extended webinar format; the ultimate goal is to have the workshop professionally recorded and available on demand at any time. In the meantime, the recorded workshops are only available to individuals who completed the training "live" via online access.