Should you Clean a Virus Infection, or Wipe and Reload Everything?

This is a question that is frequently asked by IT support technicians, and it generates strong opinions on both sides of the argument. Usually those discussions in online forums generate more heat than light, with a lot of "mine is bigger than yours" and "you're just lazy" themes.

To save you the suspense of reading to the end, I will give you the definitive answer to this question right now. It is never in your best interest, and rarely in the client's best interest, for you to wipe and reload the system. Clear enough?

This article is directed specifically at individuals and organizations that provide outsourced IT support to the SMB market. Most of the same considerations apply to in-house IT departments and to "do-it-yourself" computer users, but this is the desired outcome for a third-party support organization:

- All malware is successfully removed from the infected computer
- The cleaned computer remains malware-free for a reasonable period of time
- The computer runs faster and more reliably after the cleanup than prior to the infection
- The client/user pays a reasonable fee for the cleanup (2 hours of tech time, or less)
- The cleanup is actually accomplished in 2 hours or less

Some support organizations routinely follow the wipe-and-reload approach, usually citing one or more of these reasons to justify that decision:

- It's the only way to be sure all infections are removed
- It's the fastest way to resolve the problem
- In the process, it also gets rid of other clutter you don't need

More to the point, that approach doesn't require as much skill or training on the part of the technician who is doing the work. But here are some of the reasons this approach is never in your best interest as the service provider:

- If that's what you're going to do, the client doesn't need you; they can do it themselves or, worse yet, use the techie kid next-door to do it for the cost of a pizza
- Some programs, drivers, settings, and user data will inevitably be lost forever
- The computer won't "look the same" as it did before it became infected
- The process will require much more time than you can bill for

From the client's perspective, the wipe-and-reload solution is almost certain to lead to dissatisfaction, for a number of reasons:

 Ken is a Computer Consultant, Speaker, and Trainer, and Author of the IPPY Award-winning book *Bug-Free Computing: Stop Viruses, Squash Worms, and Smash Trojan Horses*. For information about his one-day Virus Remediation Training workshops for IT support techs, you may contact us at www.thevirusdoc.com or phone (281) 537-0252.

- Even though they signed a release or waiver, they rarely understood how different their computer would look following the reload
- Some programs or data files that are infrequently used may not reveal themselves for weeks or months after the reload
- The user will have to manually reload many of the drivers, reset the default fonts, colors, margins, folders, printers, file associations, and other system settings that have built up over an extended period of time since the computer was first put into service
- The user will be without use of their computer for the duration of the process, which could require several days to complete
- Some sophisticated malware could return following the rebuild unless specific steps are taken to prevent such reinfection; examples include MBR infections and malware that infects the computer's BIOS.

The only way to resolve malware issues to everyone's satisfaction is to find and remove all infections, their activation methods, and their symptoms, and repair any collateral damage. That successful cleanup must be followed by preventive measures to ensure that the computer will not fall victim to another malware attack in the future.

With proper training, tools, and a methodology to follow, the knowledgeable tech can usually accomplish this objective in less than two hours of hands-on time. And except in extreme cases, it can generally be done remotely without requiring an on-site visit.

Is there ever a situation when wipe-and-reload is an appropriate solution for a malware infection? Yes, if all these conditions are met:

- You have a recent full-image backup of the hard drive from that computer
- There is only one user set up on the infected computer
- There is no locally-installed software on the infected computer

Those circumstances are commonly found in the enterprise environment, but almost never in the SMB or home-user market. But if the infected computer in question happens to meet these criteria and you can restore its full image in one hour or less, that is probably the most cost-effective approach to take.

For all other situations, there is no acceptable alternative to intelligently and methodically removing all malware infections and repairing any damage they may have caused.