



No Way 'No Viruses Found'

12:30 PM -- There's nothing reassuring about regularly clean security scans -- especially when a secondary scan shows otherwise

MAY 9, 2008 | 12:30 PM -- There's something unnerving about receiving a perfectly clean security scan report from your antivirus program.

We've seen the independent tests of AV products from organizations like AV-Test.org, we know all about the rootkits that often doesn't show up in these scans, and we know about zero-days and the shortcomings of virus signature scanning. So what's up with the constant clean machine report?

My first reaction to "no viruses found" is relief and self-congratulatory, delusional pride in my obvious prowess as a security-savvy user. Then my euphoria quickly turns to frustration: there's just no way my machine could be that clean.

I'm careful online. But there are certain risks I have to take in my job, like visiting potentially dangerous sites from time to time, etc. I'm understandably skeptical that even with all of the layers of security my company provides, as well as that which I enable here on my end in my home office, I just can't be that lucky.

My skepticism was unfortunately justified this week when my ISP suddenly throttled back my bandwidth after I had apparently unknowingly tapped out my allowed share of the pipe under its Fair Usage Policy. Without getting into the gory details, my connection log showed some mysteriously big, fat downloads that just don't sync with my normal usage.

To rule out a malware infection, I decided to first get a second opinion from that of the two different AV programs I run here on my office and home laptops. Within seconds of running on my office machine, a free online malware scan from Panda Security showed that I had 55 infected files on my machine. This after my installed AV program had given me a clean report.

This time I felt vindicated (and a little freaked out), especially when I got the "You are infected!" message on my screen -- complete with a man with furrowed brows pointing an imaginary gun at me with his thumb and index finger -- when the scan was complete. But it turns out the "free" scan from Panda really isn't. (In my eagerness to get to the bottom of my upload mystery, I didn't read the fine print before I scanned.)

The online scanner fixed one problem, a "low danger" worm, but left me hanging with 30 other identified threats -- a "medium" threat spyware program and 29 tracking cookies -- all of which it would only fix if I purchased the product right then and there. Ouch.

As for my home machine, which runs a different and well-known AV vendors' scanning software suite, a spybot scan found a handful of (different) malware types, none of which my home AV vendor's program detected.

For security reasons, I won't go into the other details of my cleanup and troubleshooting the mystery traffic (you don't want to know).

I just can't wait for the day when my own security suites give me a bad report.

— Kelly Jackson Higgins, Senior Editor, [Dark Reading](#)

•