



The

Broadcasters' Desktop Resource

www.theBDR.net

... edited by Barry Mishkind – the Eclectic Engineer

Doing IT the Right Way **Combating Malware in the Studio**



By Kevin Trueblood

[November 2010] We have reached a point where software applications are so important to broadcasters that computer problems, especially in the Control Room, can literally take a station off the air. Kevin Trueblood offers some help on keeping your facility up and operating smoothly.

You know the story. You have lived it.

It is a beautiful Saturday afternoon. You are enjoying your favorite beverage on the patio, admiring the lawn you just cleaned up and spending time with your family. Then, the call comes in: “I got this message on the studio computer saying that it had a virus, so I clicked on it, and I started getting all these popups.”

You can feel your blood pressure rise as your hand unconsciously slaps your forehead while the DJ continues: “Now, it just seems to have shut down and won’t play any audio at all.”

Time to head down to the studio ... once again.

THE THREATS WE FACE

Gone seem to be the days of computer “viruses” – those cleverly-named bugs that made headlines by infecting your computer, perhaps even wiping out your hard drive just from clicking on an email attachment. Viruses do not seem to come around here anymore. Smart antivirus software and wiser email servers seemed to have solved most of this problem.

Instead hackers moved on to more lucrative projects. We now face a similarly dangerous – and probably more annoying – threat: Malware.

The definitions of malware seem to vary, but they consistently refer to unwanted software automatically installing itself and becoming a nuisance to a computer. They can range from popups offering you cool ringtones for your phone to hijacking localhost records in an attempt to get your computer to visit adult websites.



**Caution! This is not a real antivirus warning.
Interacting with this screen could cause real problems!**

The effects of a malware infected PC at a radio station can vary from an annoyed Account Executive to a station being knocked right off the air.

DIVIDE AND CONQUER

Keeping office PCs clean can be fairly simple: Installing a good antivirus software, keeping files backed up, using Windows' limited-access accounts, and the benefit of having easier access to machines during business hours means a lot less stress when dealing with most problems.

Studio PCs, however, can pose a whole different challenge. Whether they are the PCs running your automation software or the machines in your production room cranking out the spots that pay the bills, one of these guys getting infected means you wukk be spending some quality time at the station in a crunch to get the machines back on line *now*.

I am going to focus mainly on the automation and production/studio PCs in this article. I am also writing it presuming that you do not have a whole lot of money to spend on things like Domain Controllers. In other words, these are tips and tricks for those of us who do not have dedicated IT departments and an infinite budget.

AN OUNCE OF PREVENTION

A big problem we face is that production software and most automation software requires administrative access to the machine to work properly. This leaves your PC a prime target for software to leave its mark in your registry and deep into the Windows system files. Often, it is not a question of if someone will get malware on their machine, but when. So, what can you do?

Yes, you could run Ubuntu. You could also setup an awesome Domain Controller that stores everyone's profile and data on a central server and making life easy – just format C and be done with it. Realistically though, Ubuntu really is just not practical for many office environments, and Domain Controllers are out of many station's budgets.

Considering you are largely locked into what you have, here are some of the things I have found helpful toward preventing malware from getting on your machines – and how to get rid of it when it does.

- 1. Isolate the computer when possible.** If you do not need the Internet on a particular PC, that is excellent. Many stations separate their automation network and their office network, leaving the former with no Internet access. This is a good practice but a major drawback in that you cannot do things like logs, import audio, etc from office PCs – and that leads to frustration and inefficiency amongst the staff.

A simpler solution is to give the PC *only an IP address and a subnet*. Leave the gateway and DNS records blank. A PC only needs a gateway if to leave the building. This way, the automation PC is still addressable in the building by everyone and you are still accomplishing the goal of eliminating Internet access to the PC.

- 2. Do not allow anything to be done on those machines other than their specific task.** Do you have a PC in the studio for audio editing? That is enough. PC prices have come down so much in the last few years making a separate computer just for browsing the web easier to provide.

You even could get a good used PC for this task. For a good source of used, but capable, web browsing PCs check your local university surplus or inventory management warehouse. Also there tons of websites that feature retired corporate inventories, and any of these could actually be a good place to run an OS like Ubuntu. Even a retired in-house PC could serve this purpose.

- 3. Do use Antivirus software.** Antivirus applications also scan for malware, so it is important to have them on any machine with multiple users. And keep the definitions up to date.

It is true that many automation companies will strongly discourage you from running antivirus on your PCs. The rationale being that some antivirus software is bloatware that can bog down computers and cause playback to become erratic. While many of the modern machines are robust enough to handle a few tasks, anything beyond a few years old could be a problem. Some of my favorite minimalistic antivirus tools include Avast and Clamwin. Unfortunately my old favorite, AVG, has become too bloated for my taste in its recent builds.

- 4. Following that train of thought: Do not forget to run virus scans on external drives.** I have been burned by this. A machine keeps getting infected, after scans, rescans, reformatting, etc... As it turned out, an external hard drive was slyly holding on to some malware that kept re-infecting the machine.

- 5. Turn off AutoPlay.** A clever way that some malware uses to spread itself is by exploiting the AutoPlay function in Windows. AutoPlay can happen when you put in a CD or a thumb drive; Windows will pop up and say “What do you want to do?” The malware can use this to put an executable file on any removable drives, and when you put the thumb drive in another machine, Windows says “Hey, you should get started!” and the malware installs itself. A how-to cure from Microsoft can be found here <http://support.microsoft.com/kb/967715>.

- 6. Get yourself a clone.** Having a second one of you would be awesome, but I am referring to hard drive clones. With hard drives being dirt cheap these days picking up a few extra will not break the bank.

Make an image of your automation PC OS drives and your production software drives. In the event of a severe infection, swap out the drive and you are back up with the correct specs and enough to get you back on the air. This works best if logs are kept on a server, or backed up somewhere regularly.

7. **Keep your OS and applications updated.** For any machine that needs to talk to other machines. Microsoft is pretty good about patching major security flaws once they are discovered. Staying on top of Windows Updates can help prevent software taking advantage of a known flaw from happening. Note: I keep my automatic updates settings to “download but let me choose when to install” so I do not have any middle-of-the-night auto reboots.

Keep in mind that software like Adobe Flash and Java can present security threats as well, so keeping them disabled or frequently updated will help minimize those threats.

DEALING WITH AN INFECTED MACHINE

All of the above is helpful in preventing an infection, but what can you do when the idiot night guy plays around and lands a machine on site with malware?

1. **Stock your arsenal.** A good IT person always has a thumb drive or CD full of software ready for any occasion. A few of my favorites for combating malware are: Combofix, Super AntiSpyware, and Malware Bytes. Between the three of them I have been able to cure many problems.

Unfortunately, even if a piece of malware is successfully removed from the machine, it still may have corrupted programs and critical system files. Make sure you test the installed programs and keep a close eye on any Windows system errors that come up. A reinstallation of Windows and/or software still may be in order.

2. **Format C.** The old tried-and-true method. USB to SATA or IDE adaptors make it possible to back up files off the drive before formatting, so as to not completely lose a bunch of data.
3. **Do not give in.** For the love of all things good, never, *never, ever* actually buy something being touted in a popup to “click here to buy wondervirus pro to remove” or whatever it calls itself.

I know this should go without saying, but I have run across users and IT folk who gave in out of frustration following a long battle to remove the software. Their attempt was in vein, as not only did the problem not go away, but some most-likely-not-so-kind people now had their credit card information.

In the end, even offices with the most advanced security, locked down platforms, and closed environments still can become infected by viruses and other malware. The creators change their code every day to stay one step ahead of those keeping watch.

On the other hand, taking a few steps both in prevention and making sure you have the proper tools on hand to deal with the issues will help minimize those Saturday afternoons away from your favorite beverage.

Kevin Trueblood is an engineer with Wisconsin Public Radio in Madison, WI. Kevin can be reached at: kevin.trueblood@wpr.org

Return to The BDR Menu