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

[June 2016] Software applications are now 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 have moved on to more lucrative projects. We now face similarly dangerous – and probably more annoying – threats: Malware and Ransomware.

MALWARE AND RANSOMWARE

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. And now, Ransomware has taken the stage as the most popular – and profitable – schemes for hackers.

Caution! This is *not a real antivirus warning. Interacting with screens like this 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 completely right off the air.

Ransomware is major threat to our systems. Most attacks occur when someone opens an attachment in an email, an email very much disguised to look like from a supervisor or someone you are familiar with. "See attached .pdf" is something we may be used to seeing, but these messages are a time bomb.

The next screen you see informs you that your machine and all your data has been locked and encrypted, and will only be unlocked when the attacker has been paid.

Amounts demanded vary, but average in the hundreds of dollars. Not only does Ransomware lock your PC, but many varieties will also lock data on any shared drives and cloud services. In other words, you are off the air, watching a countdown clock.

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 will be spending some quality time at the station in a crunch to get each of 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?

You could run any flavor of Linux and, with gravitation to cloud storage and web applications, it is easier than ever to make the switch. But there is a learning curve for staff who cannot figure out how to find the "Start" button.
Or you could set up an awesome Domain Controller or thin client server that stores everyone's profile and data on a central server or in the

cloud, making life easy – just format C on an infected machine and be done with it.

Realistically though, many of the enterprise-level solutions like Domain Controllers and thin clients are not within a small station budget.

THINGS EVERYONE CAN DO

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: 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 some data is trying 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 run 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 that making a separate computer just for browsing the web is easy to provide.

   You even could get a good used PC for this task. A good source of used, but capable, web browsing PCs can be found at your local university surplus or inventory management warehouse. Also, tons of websites 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. **Backup, backup, backup!**

   Back up your data. Automation systems are not terrifically complicated to backup. There usually is an .ini or three, your log files, and all your audio files. Your .ini files can go on a thumb drive. A USB hard drive with enough storage for your audio files can be obtained for under $100. Plug it in once a week, unplug it and put it on your shelf.

OPEN EMAIL CAREFULLY

4. **Teach your staff to be vigilant about emails**

   It was drilled into our heads for so long to not to open attachments from people we did not know.

   Alternatively, do not open files that are .zip or .exe. These days, even more care is required: Ransomware comes to us in emails disguised as from people we know.

   The emails containing malware are super clever and many would not think twice about it.

   Nevertheless, if you are not expecting an important document from your company's CFO, double check with them to make sure they intended it for you.

5. **About Antivirus/Antispyware software**

   Here is where some people will probably disagree with me: In 2016, you do not really need a full-time antivirus anymore.

First, the A/V software itself is usually super-bloated and is easily defeated. Then, too, browsers like Google Chrome are smart enough to figure out when a website is doing something it should not and alert you before letting you proceed to a site. Microsoft is also including its own Windows Defender in modern incarnations of the operating system and is automatically updated.

You should still keep an arsenal of anti-spyware apps like *SuperAntispy-ware*, and my favorite, *Combofix*.

6. 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.

7. 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.

8. 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. (Note: do not forget that Windows 10 Home version does not give you this option. You have been warned!)

Do keep in mind that software like Java can present security threats as well, so keeping it disabled or frequently updated will help minimize those threats.

9. Back up your data

I put this on here again because you should seriously back up your data as frequently as you can.

Consider moving to the cloud

Applications like Microsoft 365, Google Drive, Dropbox, etc are becoming fairly ubiquitous. Moving your storage to online mediums means data on your local PC is

less susceptible to being taken out if something bad infects your local 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?

WHEN YOUR MACHINE IS INFECTED

If you are faced with an infected machine and you have no general plan nor software tools ready to go, you have just increased your repair time significantly. Please: prepare now!

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 these three, I have managed 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**

   This is why I cannot recommend enough that you back up your data.

   If you have an attack of Ransomware, your best and simplest recourse is just to wipe the drive and start back over again. Having your data backed up or in the cloud means simply restoring the data and you are back in business before lunch.

   The same goes for any bad malware infection. You could spend three hours scanning and cleaning, or you could reinstall the OS and restore their data

3. Do not give in, unless you have to

   For those annoying "Buy our fantastic antivirus software!!!" popups, *do not buy it!* They do not work and now they have your credit card.

   But if you do get hit with Ransomware, you have two choices: Restore a backup or pay the ransom. I have known people who did not backup data and a mission critical machine was taken over. Since they could not afford to lose the data, they paid the ransom and got back in business. If you do not mind shelling out a few hundred or a few thousand dollars, more power to you.

THERE IS DANGER, BUT YOU CAN WIN

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 Truebloood is the Director of Engineering at WGCU Public Media in Fort Myers, FL. Kevin can be reached at:
ktrueblood@wgcu.org

Return to The BDR Menu