Joseph T. Parsons

[josephtparsons@metrostate.edu](mailto:josephtparsons@metrostate.edu)

The Parsons Computer Corner: Avoiding Malware by Hardening Your System

Today’s computer age is one of threats. Scammers want to steal your credit card information, hackers want to corral your computer into giant botnets whose purpose is to shutdown websites, and “ransomware”—spyware that deletes information but offers to give it back if you pay up—is running increasingly rampant, infecting even hospitals and police stations. IT departments are keeping busy staying up-to-date with all these different types of “malware” (malicious software), but most people unfortunately don’t have an entire IT department keeping their own personal computer safe.

In the last issue of The Metropolitan, Levi King did a fantastic job of explaining how malware installs itself through “attack vectors,” and suggested a number of important ways you can eliminate these. In this issue, I would like to suggest a handful more that will help ensure you never fall prey to a computer infection again.

## Install EMET (Windows Only)

One of the least-known yet most-helpful tools for hardening your system (assuming it is a Windows system) is Microsoft’s Enhanced Mitigation Experience Toolkit, or EMET. While initially intended only for system administrators, EMET is now available as an easy-to-install consumer package that adds several additional security precautions to Microsoft Windows. These features all work together to reduce the “attack surface” that common malware uses to infect your system, akin to how flu shots preemptively “patch” weak parts of your body against the flu. In EMET’s case, it specifically “patches” common programs (like Adobe Flash and Google Chrome), reducing the ways these programs can be used as an attack vector.

To install EMET, you must:

* Download it from the Microsoft Download Center (go to microsoft.com/emet, and click “EMET 5.5” on the right)
* Run the downloaded program, “EMET Setup.msi”
* When asked, choose “Use Recommended Settings”

At this point, EMET will have “patched” several common programs, but will leave many others untouched. To patch the remaining programs:

* From the Start Menu, open “EMET GUI”
* At the top-left of the opened window, click “Import”
* Three files should be listed. Of them, open “Popular Software.xml”

That’s it! EMET will now have hardened applications ranging from Google Chrome to Skype to iTunes. One caveat *does* remain, however—some programs may no longer work as expected with EMET installed. While I very rarely experience an issue, EMET will stop some legitimate programs from working correctly. If this happens, you may wish to uninstall EMET, or add an exception for that program, which you can do from the EMET GUI window by clicking “Apps.”

## Read What You’re Installing

For about five years, it has been very common for perfectly legitimate software to ask you to install additional malware. Java, for instance, despite being owned by software behemoth Oracle, will offer to install the “Ask Toolbar.” Now, the Ask Toolbar isn’t malware, and many people install it voluntarily, but many people also end up installing it simply because they didn’t read what Java offered. Other programs will similarly ask you to install extras, but these will be far more malicious in nature. You should always read what extras a program is offering, and decline them if they don’t sound like something you’d want to install.

(Why would legitimate programs offer to install malware? It helps pay the developers’ bills.)

## Stay Updated

Malware often installs itself by exploiting holes in other software you’ve already installed. For instance, holes in Chrome or Firefox may allow webpages to install malware on your system, or holes in Adobe Reader may allow PDF documents to do the same. Often, software makers aren’t aware of these holes until they’re being exploited, but will patch them very quickly afterwards.

As a result, one of the best ways to stop “drive-by” malware is by keeping your software updated. Today, most software will update itself automatically, but some will still ask if you want to update, and your answer should always be “yes.”

Relatedly, if you’re one of the few people still on Windows XP, your computer is probably swimming in malware, and if you’re running versions of Microsoft Office older than and including 2007, you should be extra careful about opening unknown documents. All of these products stopped being supported by Microsoft years ago.

## Use Common Sense

Finally, the best way to prevent infections is simply to use common sense. Don’t run programs you downloaded from shady parts of the internet, and understand that every time you install something, you’re potentially installing malware. Be careful, and you’ll probably avoid an infection.