Simplified PC Security

Terry Ritter

A *Ciphers By Ritter* Page

2009 December 2

INTRODUCTION

Personal Computing has changed from being merely fun and useful to being important and necessary for many people. As we have come to depend upon computing to avoid banking lines, criminals have responded with malware to take our money. This article describes various options one can use to oppose malware, or even to restore secure use on a PC known to be infected.

Malware is deliberately malicious software installed without permission of the computer owner. Malware usually comes from criminal hackers who will exploit their access however they can. For many users, the greatest risk may lie in exposing their financial accounts and passwords to criminals who might well use them.

The malware problem is much worse than we know, and literally worse than we *can* know. A recent survey by a PC security company has found that almost 60 percent of our computers are infected. Those that are infected have an average of 13 infected files, from 3 different malware families. The numbers we have are bad, but they only reflect the malware we actually find, and surely the best hiders remain unfound. For example, antivirus scans find particular banking theft bots less than a quarter of the time.

MICROSOFT

Windows users account for 93 percent of the browsing market, giving Microsoft both the responsibility and coverage to control malware. Microsoft has been working against malware for a long time, and provides free monthly updates even to users who last paid for Windows XP 8 long years ago. But no matter how much Microsoft has been doing, it has not been nearly enough. Malware is getting worse, both in numbers and power, and banking on-line has become a true anxiety.

Malware protection is not about which operating system has the fewest errors. All large complex systems have errors. Malware is about which OS provides the best financial return for criminal hackers. The dominance of Windows makes other operating systems safer, even if they have more faults.

MALWARE

A computer virus is malware, but it is not alive. Malware does not infect humans or animals. Malware is just a sequence of values stored electronically. When malware is executed, the values tell the processor to make a sequence of data changes that we may not like.

A malware is a computer program, and all programs consist of data and execution. If we can prevent a malware file from being present, it cannot do anything. If a malware file is present, but cannot get executed, it also cannot do anything.

Malware starts with "attack." "Attack" finds some way to present malware code and allow it to execute. In many cases, "attack" is just a story which gets the user to request a download or execute a file that turns out to be malware. In other cases, there may be a technical attack to exploit some fault in operating system (OS), browser, or player design or implementation. Firewalls and anti-malware scanners address the attack phase.

Malware moves through "infect." "Infect" modifies OS boot data on a hard drive to re-install the malware on every session. When malware is in charge, the OS cannot protect the hard drive. In general, once a hard-drive based system is infected, it remains infected until the OS is re-installed. Practices called sandboxing and virtualization can oppose infection, but are complex (thus flawed) and can be awkward.

"Run as a user, not an administrator" is common advice from corporate enterprise computing. User-mode reduced permissions were designed to limit damage in multi-user systems and may indeed prevent malware from infecting the hard drive. However, when malware takes control as a user, it can do everything a very clever user can do. User data is not protected at all. When malware is in charge, everything the user can access (including email and addresses, browser files, exposed account numbers or passwords and of course the contents of every file) can be exposed for on-line delivery under user-level browsing permissions.

Malware arrives at "operate." "Operate" generally means acting as a local robot for a remote criminal attacker. After infection, even sandboxing and virtualization cannot be trusted. In systems that cannot be infected, a successful attack can still operate for the remainder of a session. Once a bot is in place, it can access, change or do anything a user (or even an administrator, typically) can, and more.

The anti-malware tools have been tried. Firewalls, scanners, sandboxing, virtualization and user-mode are well-known and have been applied for years (except perhaps virtualization). Since malware attacks have just gotten worse, we can predict that the same old tools will not solve our malware problems. Users need to move on to something that works, and they can make a big start in just a few hours.

Most malware attacks are easily prevented simply by using Linux instead of Windows. This is not about Linux being "better" than Windows, since both have a continuing flow of serious bugs and irritating updates. This is about Windows being a vastly larger attack target, making Windows attacks more profitable for criminals.

Malware infection is easily prevented simply by using a read-only (or read-mostly) boot media. Our PC's are vulnerable to infection largely because they have a tasty hard-drive that is easily changed by malware. The OS cannot protect the drive when the OS itself has been subverted, so only hardware protection counts, and there is none.

Malware exploration of a hard drive is easily prevented by removing the hard drive and not using a hard drive on line. Browsing without a hard drive turns out to be more pleasant and practical than it may seem at first.

Many malware attacks can be thwarted by using Firefox with security add-ons. Various technical issues of the current Web can be protected with security add-ons. Since the alternative is for users to understand the situation and perform correctly, we are well advised to take advantage of everything that can be done automatically.

Finding any running malware means re-installing the OS. Oh, yes it does! Found malware can be removed, but scanners cannot find *all* malware, which means the worst of the pack may remain in operation and hidden. The OS on the hard drive may have been fundamentally changed. A "rootkit" can prevent the OS from even seeing malware files or any changed file contents. Relying upon even multiple malware scanners to certify a computer as "clean" greatly misunderstands what scanners and malware can do.

We might remove some malware, but we cannot remove malware effects because we cannot know what malware has done. Malware system modifications may not show up in a malware scan. Modern malware generally creates a robot or "bot" which connects to the Internet to carry out the bot-handler's criminal will. Any found malware may be a now-useless downloader for the bot, or one of many malware friends also downloaded.

The *only* routes to recovering a guaranteed clean system are:

1. Re-install the OS, or
2. Recover a system image made before the infection (try "Macrium Reflect Free"), or
3. Boot a clean system from CD or DVD (where possible).

OS installation can be somewhat easier with a recovery partition, or more tedious from recovery CDs. In all cases it is wise to make an image backup to save all data before re-installing. Most times the local programs will have to be re-installed as well, and many things will need updating. Because all this is scary and complex and tedious, few do it, so there is no surprise that many systems remain infected. None of this is an issue for those who load their browsing OS from DVD.

Even an infected PC can be secure when an OS is booted from a DVD. Malware infects the boot system on the hard drive. So if we do not boot from the hard drive, we never see that malware.

PUPPY LINUX

Most malware attacks are prevented simply by using Linux instead of Windows. Although having to learn a new OS sounds like a scary waste of time, not much learning is needed, while the protection against malware is almost complete. What we need to know to set up and run Puppy Linux and the Firefox browser is described in detail in the Puppy Linux section of my Basic PC Security article on my pages. Once into the browser, things are mostly the same under Windows or Linux.

Puppy Linux is a DVD-bootable OS that solves many current malware issues:

- Puppy Linux is not Windows.
- Puppy Linux was designed to load from CD or DVD and runs in memory (the CD can be removed).
- The CD or even a DVD+RW provides excellent protection against infection.
- Puppy Linux provides good support for Firefox and a range of free security add-ons.
- Updates for Firefox and add-ons can be written back to the boot DVD-R or DVD+RW as another session.
- The updated system will load automatically on the next boot.
- Puppy Linux does not need a hard drive. When there is no hard drive, there is no hard drive to infect.

Puppy Linux is a free OS and is inherently unpolished. Ideally we would have a perfect system without bugs or inconsistencies, but that is not the case. If there were some other OS with similar advantageous properties, we could use that. Unfortunately, there appears to be no viable alternative at the present time.

FIREFOX

Firefox is a top-end cross-platform browser, and is quickly patched when problems are found. The Firefox automatic update system is almost effortless. Firefox also supports "add on" packages, to extend the browser beyond the current design.

Some people sneer at a browser that needs add-on help, and think browsers should be compared in their base configuration. But users do not see the base browser, they see the configured result *including* the installed add-ons. Add-ons are particularly important for security issues, which frequently are not well addressed in any normal browser designs. Various add-ons switch from being a user toy to a comparative advantage after one sees what they can do.

Firefox with add-ons offers far more security features than other browsers.

Some add-ons provide important SSL support:

- **NoScript** -- force SSL: Options / Advanced / HTTPS
  - Force: *.google.com *.bankofamerica.com
  - Never: www.google.com/search www.google.com/support www.google.com/url*
- **Safe** -- colored outlines for windows having SSL connection
- **SSLPasswdWarning** -- warn of entering password without SSL
- **Perspectives** -- provide alternate identification of connected site
- **SSLBlacklist** -- expose some bad SSL certificates
- **Force-TLS** -- take SSL suggestion from web server

Other add-ons support general security:

- **NoScript** (again) -- whitelist scripting code by website
- **NoScript** (again) -- avoid certain XSS and clickjacking attacks
- **LastPass** -- cross-platform password manager
- **URL Tooltip** -- show link URL on tooltip
- **ShowIP** -- show page IP address
- **Permit Cookies** -- whitelist sites for saving cookies
- **BetterPrivacy** -- automatically clear Flash cookies / DOM
- **JSView** -- expose external stylesheets and scripts
- **PfishTank SiteChecker** -- expose known pfishing sites
- **WOT** -- expose known danger sites in search and use
- **Tab Mix Plus** -- tab setup / crash protect
- **Long URL Please** -- convert short URL back to original
- **facebooksecurelogin** -- use SSL when logging in

Still other add-ons improve general use:

- **Adblock Plus** -- block ads for faster browsing
- **Save Complete** -- save all page components
- **Uppity** -- URL up one level
- **Multiple Tab Handler** -- select tab subset for bookmark, close
- **FireFTP** -- FTP client
- **PageDiff** -- compare HTML pages
- **MD5 Reborned Hasher** -- compute download hash
- **NoSquint** -- page and text sizing per site
- **DownThemAll** -- fast file downloader
- **Video DownloadHelper** -- save Flash videos

Only the Firefox browser comes close to doing all that can be done to prevent malware. Simply claiming to be secure is not the same as providing a range of important security features for the user.

NO HARD DRIVE

Puppy Linux provides a surprisingly nice experience without a hard drive. In most cases it is easy to remove the drive from a laptop, and there are several reasons to do so:

First, the larger the hard drive, the less we know what is on it. Without a hard drive, there is no hard drive to expose.

Next, using any hard drive on-line is a potential infection issue. Without a hard drive, there is no hard drive to be infected.

Last, saving files permanently just means using an alternative:

- Save the session (with new files) to the writable DVD.
- Save files to a USB flash drive.
- Save files as Gmail attachments in email to self via SSL.
- Edit text as an email to self via SSL.
- Work with documents in Google Docs via SSL.

Gmail allows "viewing" an HTML attachment without downloading it. We can export a file of bookmarks from our browser as HTML and save it as an attachment in an email to self. To use individual bookmarks, we view the attachment from email, and do not need to save those bookmarks in the browser.

PASSWORDS

A password is a sequence of characters used to identify a particular user. Passwords work by making it unlikely that someone who does not know the password could present it correctly. But computers are able to try one password after another, tens of millions of times, in a "brute force" attack, and may try "more probable" characters and words before nonsense random values.

Password security requires **the user** to take responsibility for creating different **long, random passwords** for each site or account

or device. Good passwords should be machine-generated random sequences of at least 15 characters. Since few if any of us can make or remember long random passwords, we need a password manager to generate and keep them for us.

A password manager organizes a little encrypted database that we open with a single memorized password. Since the database is encrypted, we can put it on a flash drive or in cloud storage or send it as an email attachment. A password manager gives us a way to keep any number of long, random passwords and user names and all the site information we want, which even reminds us which sites we have already joined.

NETWORK DATA SECURITY (SSL)

The Internet Protocol (IP) is a store-and-forward network moving information from node to node in little chunks called "packets." Normally, the network does not encrypt the data in packets, and they may be exposed to anyone along the line, or perhaps anyone on the same subnet. Shared subnet or Ethernet access can occur in a particular housing neighborhood, or in a hotel or motel, or whenever there is wireless access, especially open or free Wi-Fi. There can be consequences for sending account numbers or credentials or passwords in the open to be read by anyone around.

Most Internet security depends on TLS (short for "Transport Layer Security"), which we still call SSL (or "Secure Sockets Layer"). SSL is the "**https://**" protocol, which we often see highlighted in the browser address bar. The intent is to establish a secure connection between browser and web page, so that nobody along the line can snoop.

For SSL to work, the computer must know exactly who is on the other end of the communication. Authenticating the web site occurs by receiving a certificate linking the web site address to an issuer whose certificate is included in the browser or the OS. Many SSL security problems involve an attacker trying to pass off a different certificate, or hide a mismatch or claim it does not matter. **Never authorize a new security certificate**, *especially* at a "free Wi-Fi" coffee shop.

Since network data security depends upon SSL, it is important to recognize when SSL is active. The Firefox add-on "Safe" will put a colored border around a page when SSL has been established, and modern browsers will highlight the owner on the browser address bar. It is particularly important that SSL be in place before entering a password. The Firefox add-on "SSLPasswdWarning" is designed to flash up a red warning if a password is about to be entered outside SSL. The Firefox add-on "NoScript" will force SSL for particular sites that can use SSL but tend to use or revert back to http. The Firefox add-on "Perspectives" may be able to tell if your computer has established an SSL connection with a man-in-the-middle.

WIRELESS DATA SECURITY

Wi-Fi is radio, and is subject to the usual radio problems, like limited range, interference from others, and the fact that anybody nearby can pick up transmissions. Attackers in a "free Wi-Fi" area can put themselves "in the middle" between the router and all other laptops, then inspect each of the packets going by for a password. Never enter a password on free Wi-Fi unless an SSL connection is already up.

Wireless security intends to make communications secure between a laptop and wireless router. (Once past the router, the data are exposed on the Internet as usual, unless SSL is up.) Typically a wireless security protocol will encrypt the data using a random password or "key" known only to the router and the laptop (otherwise known as a Pre-Shared Key or PSK). Secure wireless protocols are harder to design than one might think: the first, known as "WEP," now can have its key exposed faster than the key can be typed in. The next protocol, known as "TKIP," has started to weaken in recent attacks. Only one wireless security protocol remains untouched, and that is known as "WPA2-PSK/AES" or "WPA2-PSK". Since longer keys are better, there is no reason not to use a 63-character random pre-shared key (try grc.com/passwords).

Those who leave their wireless router unsecured may be exposing themselves to legal liability. An unprotected connection is particularly attractive to someone, perhaps in a nearby home or even a parked car, who does not want to be associated with what they do on-line. They may download disturbing or copyrighted things, for which the connection owner might be blamed or even held responsible. And if your home Wi-Fi is unsecured, you will need to be as careful with your passwords at home as you would be in a coffee shop.

EMAIL MALWARE

The first step in any malware takeover is to somehow get malware program code onto the local computer. An obvious entry point or "vector" is email. If an email can get the user to click on a link, often enough the result will be a malware download. Clicking on a link in email is almost never a good idea unless the link was just requested by the user.

Another possibility is to get a user to execute an attractive attachment, which of course turns out to be malware. That is a form of a "Trojan Horse" attack. Sometimes, simply opening an attachment locally for reading is enough to allow code in the attachment to run. Once malware code is running, things go downhill at computer speed.

One way to avoid email Trojan Horse malware is for the user to never open an unexpected attachment, even if it appears to be from a friend, since attackers will lie about their identity. Another way to avoid email Trojan Horse malware is to use on-line email, which normally scans attachments for us, probably better than we can. Then we can view the attachment on-line, perhaps converted to HTML, without downloading a possibly dangerous file.

Gmail can be set to always use **https** (which is SSL) to prevent local snooping on email. Having an SSL link to the email provider opens the possibility of saving files as attachments in email to self. The result probably is fairly secure both in communications and storage, especially since Google has their own backup and recovery systems.

AWAY FROM HOME, ALWAYS BOOT YOUR OWN OS FROM YOUR OWN DVD

Everybody wants to sit down at some random computer and sign on to handle personal business, but that is very, very risky. Key-loggers, screen-loggers and password-stealers for Windows may be resident and waiting. Good security requires that you either have your own computer and keep it physically secure, or that you boot your own OS DVD. If you want your data and passwords to remain private, do not use any public computer for email without booting it from your own OS DVD. (Also do not enter a password over open Wi-Fi unless you have established an SSL connection.)

The best solution is to take your own laptop, even an old one, leaving the hard drive at home. Take your OS DVD and use it. Just say no to hotel, bar, bank, conference or customer computers.

THE FUTURE

Microsoft should supply a tool to certify that their OS is not infected. For secure banking, it is crucial that malware bots not already be resident and waiting for account numbers and passwords. Antivirus scanners cannot hope to find all malware, which leaves each user guessing about whether the OS is safe, which is not in Microsoft's best interests. Microsoft could reduce user anxiety about malware by providing a "live CD" to examine an OS installation and certify it as effectively the same as a new installation, and, thus, uninfected. Presumably the Windows registry and device drivers would also need examination.

Microsoft should provide tools to support user re-installation of the OS. Users now can make OS image backups on an external hard drive and recover the images later, which would be great if only there was some way to guarantee that the image did not include malware. A true re-install is quite burdensome and the potential for serious problems probably takes it beyond the skills of many users.

Microsoft and Intel need to re-visit the PC hardware design. Boot media needs to offer hardware protection for OS files, protection the OS cannot provide when it has been penetrated by malware. Updates would need both cryptographic authentication and owner authorization, plus perhaps a way to reverse disasterous updates. Any flash BIOS also needs protection.

Browser designs need to respect user machines. The current assumption that users should download and execute any code a site may provide is just ***wrong***. It is also wrong to allow files to execute as anything other than their apparent filetype.

By themselves, browsers are not, and never will be, strong enough to prevent malware in all its forms. It is long past time to implement a scheme that provides cryptographic authentication of each executable item downloaded, *before* the item is executed. Not only should we know to whom we are connected using SSL everywhere and all the time, but also that each executable item we get from that page was approved by the page owner.

SUMMARY

To reject malware, use an operating system (OS) other than Windows when on-line (e.g., Puppy Linux).

To prevent infection, boot your browsing OS from CD or DVD (e.g., Puppy Linux).

To avoid browser weakness, use Firefox with security add-ons.

To prevent net snooping, get an SSL connection ("https://"), especially before entering a password.

To secure your accounts, give each a different long random password, and use LastPass.com.

To protect against email malware, use web Gmail, and select the "always use https" option.

When traveling, always boot your own OS from your own DVD on your own computer.

REFERENCES

A great deal more on these topics can be found in my Basic PC Security article on my pages. For comments and complaints, please use the email address in that article.