Jefric Consulting, LLC
Small Business
IT Services and Consulting
Jefric Consulting, LLC

Microsoft CERTIFIED Professional
Microsoft Small Business Specialist

office: (201) 370-6430
(917) 837-3535
fax: (201) 689-9507
mail: info@jefric.com

March, 2010

The ABC's of Malware.

Malware (or **MAL**icious soft**WARE**) is defined as "software designed to infiltrate a computer system without the owner's informed consent"[1]. It is a general term that often refers to viruses, spyware, adware, phishing, and much more. If you looking to protect your computer system(s) from the various threats that can present themselves, you may want to first have a better understanding of what you are dealing with.

"Across the globe, the average number of PCs hit by malware now stands around 59 percent, an all-time high for the year. Among 29 countries tracked, the U.S. ranked ninth with slightly more than 58 percent of its PCs infected. Taiwan hit first place with an infection ratio of 69 percent, while Norway came in lowest with only 39 percent of its PCs attacked by malware."[2]

The following is a quick review of some of the most common forms of Malware encountered today and other things you might wish to keep in mind. . I encourage you to perform additional research for an in-depth understanding of the topic and ways to protect yourself.

Virus

A computer virus is generally defined as a program that can infect a computer and copy itself. It is often used (incorrectly) as a general term for a variety of Malware (e.g. worms, Trojans, root kits, etc.). Each of these has unique set of characteristics and can affect a computer system in a different way.

A virus is typically a small program that will either corrupt or delete data on your computer; in some cases erasing some if not all of your hard disk. It often spreads from one computer to another via files, e-mail attachments, Internet downloads, network connections, removable media (e.g. USB drives, etc), etc. As with most Malware, Viruses are often hidden / embedded in seemingly innocent websites, downloads and other Internet content.

Anti-virus software is the most common form of anti-malware software. They range in cost and complexity from the free editions for individual / home computers to complex enterprise business solutions that are monitored and managed. Regardless of what you choose, you should have one.

Spyware

[1] Source: Wikipedia

[2] Source: cnet, Sept 29, 2009, http://news.cnet.com/8301-1009_3-10363373-83.html

“Spyware is a type of malware that is installed on computers and collects little bits of information at a time about users without their knowledge. “[3] These seemingly innocent pieces of software secretly monitor the usage of a computer, collect and share personal information (e.g. web surfing history and habits), and change (computer) settings, redirecting web sites and often resulting in performance degradation, privacy issues and identify theft. Spyware is often downloaded and installed on a computer without the user’s knowledge, connecting to and sharing information with another computer on the Internet.

Browser cookies are often reported as spyware, as they are capturing usage patterns and activity to improve the user experience for the current or future visit to the site. Modern day Internet browsers allow you to disable cookies, although this will often limit or disable other features of the site. Most full function anti-virus software packages include some level of spyware detection and prevention as part of their features.

Adware

Adware, or advertising-supported software, is any software package which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used. While not always categorized as malware, adware very often opens the door to a variety of other computer infections, viruses, spyware, etc. Like malware, adware can affect performance and use up other resources of a computer (e.g. disk space, memory, etc).

There are a number of (free and for a price) software packages that can scan and clean your computer of adware. Check and clean your system regularly

Phishing

Arguably the most damaging form of malware, leading to many of the other forms of infection, Phishing is “the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. “[4]

Phishing is a serious problem to the online banking community. False advertisement phishing attacks represent an ever increasing percentage of the spam email going through on the Internet. Harmless links can conceal spam and virus infected websites that lead to service, identity and monetary theft. If the IRS is trying to reach you, do you really think they will send you 10 emails a day, as opposed to calling you? These are examples of when being suspicious isn’t a bad thing.

Spam

Email is rapidly becoming the preferred method of communication for businesses to communicate with their staff, clients and vendors. Spam is the modern day electronic version of junk mail. Depending on your organization, spam email accounts for as much as 90% of all email.[5] What not directly grouped with

[3] Source: Wikipedia

[4] Source: Wikipedia

[5] Source: cnet, May 26, 2009, http://news.cnet.com/8301-1009_3-10249172-83.html

Malware, it is often responsible for spreading it. By using a good spam filter on your email you can reduce your chances of becoming infected by malware.

Examples

An email from "Microsoft Team [alan@jefric.com]" – What's wrong here?

At quick glance, this email seems to be coming from Microsoft. A closer look shows it coming from me. The message also had a small attachment. This is possible malware.
While I don't often send email to myself, I certainly don't try and pass it off as coming from Microsoft. This is a common method used to confused junk mail filters. The attachment could be malware, which would open my computer up to other types of infections. In this case, I just delete it.

Pop-Up's – Your computer is infected - click **here** to download a fix.

People writing malware are getting cleverer each day. In this case the user is being presented with a possibly false alert which may trick them into downloading the actually piece of malware. In this case it is best to "**X**" out of the window and manually scan your computer with a known and trusted anti-malware piece of software. Don't take chances.

Your bank policy has changed, click here to update your account profile.
Your password has expired, click here to change it.

This may be a Phishing scam. When you click on the link you are asked for your old one, and then a new one. Now the attacker has two of your likely choices. Be cautious when you click on links in an email, if at all. Let your mouse hover over the link in the email. You should be alarmed if the address in the email does not match the address that is displayed next to the mouse pointer.

Suggestions

Change passwords regularly - avoid using permutations (e.g. password1, password2, etc.) and reusing old values where possible

Keep your computer up to date. Microsoft distributes updates on the second Tuesday of every month. The day, which has been affectionately call "Patch Tuesday" is when the latest critical operating system and security updates are made available for download. While Apple does not publish a formal schedule, it makes updates available in a similar and timely fashion.

When shopping for Anti-Malware software for your computer be sure to understand what type of protection you are purchasing. Don't assume that one application will solve all of your problems. It may take 2 or more applications to fully protect you from the variety of threats circulating on the Internet these days.

Most anti-virus applications update their definitions files daily, some more often than that. Spyware and Adware applications update less frequently but typically check for updates before they perform a scan. Make sure your computer is connected to the Internet so you keep your computer clean and safe. Avoid falling behind.

Other notes

Other forms of Malware that are not presented here include: Worms, Trojans, RootKits. Familiarize yourself with the basics as best as you can.

Enterprise Security Tips on a Small-Business Budget
http://www.networkworld.com/news/2010/022410-enterprise-security-tips-on-a.html

This all makes sense, but how do I get started?
The information presented here is readily available and openly discussed in the news, online on web sites, blogs and forums. Sorting through all of the information, and understanding it is the challenge, especially if it is not the business that you are in. Everyone who drives a car doesn't know how everything in the engine works; they just know that it serves a purpose that is key to their driving experience, without which they might not be able to get from point A to point B. They may also find it necessary to enlist the help of an expert if something is broken or not working the way they would expect. Technology is no different.

Find an IT consultant who will work with you and understand your business. The right technology can **improve office efficiency, increase revenue and help you grow your business and profits**. All these things will help you be **successful**.

Alan M Buckwalter
Principal and Founder
Jefric Consulting, LLC
alan@jefric.com
http://www.jefric.com
http://blog.jefric.com

Microsoft Small Business Specialist
Microsoft Certified Professional
Custom Technology Solutions for Small Business