Random Thoughts
from William Blinn Communications
TECHNOLOGY • MARKETING • COMMUNICATIONS
February 2010

Fighting the Growing Security Threat

A high-tech company that I'm familiar with suffered a virus attack while I was in the building recently. An employee said that her computer had started displaying "bad pictures" and the technician asked me to take a look. While the employee was on a lunch break, she received a message from a family member about some new pictures on MySpace. As she viewed the photos, an alert popped up that looked like something from the company's antivirus program. The warning said the computer was infected and asked if she wanted to perform a scan.

She said yes.

That was a very bad decision, but one that's somewhat understandable. I saw the pop-up message later. It had graphics from the antivirus application that the company uses and it's able to masquerade as any of the most popular antivirus programs.

Within seconds, the machine was unusable. Websites popped up constantly, each with an advertisement. This was probably no more than a click-fraud operation, but it could have been far worse. It could have started looking for business documents, credit card numbers, and the like.

The malware wouldn't allow me to run the Task Manager, so I couldn't kill whatever process was running. Access to the Registry Editor was also blocked. In short, the computer was toast. The company's IT staff had to take the computer out of service and wipe the hard drive.

Google has been victimized by a series of attacks that originated in China. The attackers were able to steal some of Google's intellectual property. Other companies have been attacked, too. Many in Silicon Valley, but also companies such as Chemical Abstracts with its headquarters in central Ohio.

Symantec, the antivirus company, says that more than half of the nearly 6 million samples in its malware library have been created in the past year and a half. That's more than the number created in the previous 2 decades. Trend Micro, another antivirus provider, surveyed more than 100 companies. Every single one of them had been affected by malware of some sort and more than half were found to have malware installed that was capable of transmitting sensitive data to the criminals who created the code.

Internet Explorer's Culpability

In late January, Microsoft once again had to resort to an out-of-cycle emergency patch to fix a browser flaw. Unlike Firefox, which is patched frequently, Internet Explorer is typically patched only on the monthly Microsoft "patch Tuesday". The problem was deemed sufficiently serious that the company didn't want to wait for the next scheduled patch session in February.

Microsoft said that attacks, mainly from China, have so far been unsuccessful except on Internet Explorer version 6. It's important to note that version 6 was replaced by version 7 and version 7 has been replaced by version 8. But not everyone upgrades promptly.

Symantec says the exploit that attacks unpatched versions of Internet Explorer is on "hundreds of websites," some of them legitimate and run by respectable companies. Although the greatest danger comes from visiting sites with hacked software, free pornography, and the like, if you're using a faulty browser, your computer could be compromised when you visit a business partner's website, presuming it to be safe.

Despite being aware of the threat for more than three months, Microsoft put off taking action until the end of January. This is one of the many reasons that I recommend using Internet Explorer only for trusted websites that insist on using ActiveX controls. Firefox and Opera are safer.

Random Thoughts (ISSN 1543-1533) is for clients and friends of William Blinn Communications, 179 Caren Avenue, Worthington, Ohio 43085. Phone 614.785.9359. On the Web at www.Blinn.com.

Law of Cat Computational Development: Cats must sit on the key marked *Del*.

New Kinds of Attacks

What we're seeing is essentially the first wave of a new kind of attack. You can no longer presume that any website is safe, but e-mail is still the most common vector for introducing malware. Because many users seem to be unable to discern the sometimes totally obvious differences between legitimate messages and fakes, antivirus vendors are ramping up their products to address the expanding pool of threats.

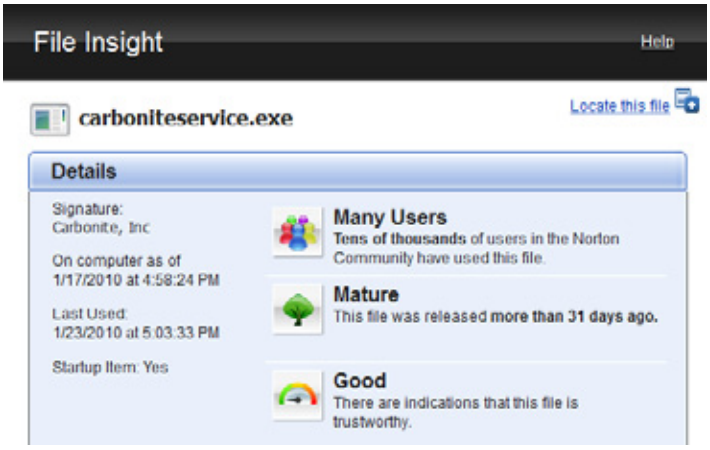
As a result, the protective applications display warning messages more often than in the past. Users tend to get into the habit of always choosing *fix* or always choosing *ignore*. Neither of those is a good choice. Always telling the application to fix a problem could cause it to break a legitimate application and always choosing ignore could allow malware to get through the net.

Because this is the case, I wonder why so many protective applications continue to warn about cookies. Most of them at least report the threat from cookies is low, but they still report them. In most cases, this feature can be turned off, but it should be turned off by default. Tell the user about legitimate security threats and don't bother with cookies.

What I Recommend in 2010

I am in awe of what Symantec developers have accomplished with the code for the latest version of Norton Internet Security. Although Norton Antivirus was my choice in the early days of personal computers, it became too big, too bloated, and too slow. It caused even fast computers to crawl. For much of the last decade, I've used AVG Antivirus, but AVG has added a suite of protective applications that brought my computer to its knees. After trying and removing other applications, I downloaded Norton Internet Security 2010 in mid January for a 30-day trial.

The instant I removed the previous application and installed NIS, it was like I had a new computer. One of my primary complaints with all of the applications I tried is that they got in the way of my using the computer. It wasn't solely their fault, but every other application severely exacerbated the problem.



Perhaps the most important new feature is what Symantec calls "Quorum". It's the protective engine that examines files without seriously affecting system performance. Earlier versions of the application protected the computer, but also rendered it virtually unusable. Quorum changes all that by cataloging "trusted" files.

It starts by examining files on your computer and analyzing what they do on the computer and when connecting to the Internet; then it compares this behavior to the behavior reported by NIS on millions of other computers.

To see Quorum's report on a file, simply right-click the file from the Windows Explorer and select Norton File Insight. Yes, you can opt out of this system, but why?

Starting with Internet Security 2009, Symantec's advertisements admitted that earlier versions of the application had performance problems. One doesn't always place one's full trust in a company's advertising platform, but they're telling the truth this time.

NIS increases boot time slightly, but no more than any of the other applications I looked at. Opening websites is just as fast with NIS installed or not. That's particularly impressive. I didn't see much difference when it came to manipulating files from the Windows Explorer or when compressing or decompressing files. Downloading e-mail takes longer, but not as long as with several competing applications. In other words, it would seem that Norton's reputation as a resource hog is no longer deserved. NIS provides the same good security it's always been known for without turning your computer into a pet rock.

Symantec is the biggest dog on the block, so the company has information about millions of files and what they're expected to do. That's what Quorum is based on. If a file is on a lot of computers and is behaving normally, the application considers it to be trusted. This is particularly clever because most current threats constantly mutate to avoid signature-based detection. That works in Quorum's (and your) favor and it mitigates threats from these kinds of malware.

I didn't test NIS's parental controls, in part because my youngest daughter is 25 years old and in part because I feel the entire concept is silly. But from what I've seen, the parental controls in this version are at least as good as any other silly competing product.

By default, Norton installs a toolbar in Internet Explorer (why are you still using this?) and Firefox, but not in other browsers such as Chrome, Opera, or Safari. It adds icons to search results so that you can see whether the URL is safe, suspicious, or dangerous. Or you can use the optional Norton Safe Search, which highlights search results in yellow (suspicious) or red (dangerous).

The suite's Identity Safe stores and manages passwords and other information in the form of "identity cards". This feature doesn't have all the features of an application such as KeePass, but it's available at all times from either of the two primary browsers. I consider this a worthwhile feature.

After a long and frustrating search, this is the application I have decided to pay for.

NIS costs about $30 for a single computer or $70 for up to 3 computers. For more information, visit the Norton website: http://www.norton.com/. ß