nLightened Thoughts

January 2013

William Blinn Communications
Worthington, Ohio 43085
www.n-lighten.us • 614/859.9359

Web-Based Dangers Threaten Your Business

Every time an employee uses a computer that's attached to the corporate LAN to visit a website, whether for business or personal reasons, your entire network is at risk. Even though the Web is the primary vector for malware distribution, you can't very well keep employees from going there. It's just too much a part of today's business world.

You can recognize the dangers, however, understand the threats, and take actions to mitigate them. Cyber-thugs use a variety of techniques to distribute malware. According to a publication by Sophos, a company that specializes in protective applications, these are some of the top threats:

- Black hat search engine optimization (SEO) ranks malware pages highly in search results. The unsuspecting employee clicks the link and ends up on a malicious site.
- Drive-by downloads exploit flaws in browser software to install malware when someone just visits the page. Most of these threats can be eliminated by keeping browsers up to date.
- Social engineered click-jacking to trick users into clicking on innocent-looking web pages.
- Spearphishing sites mimic legitimate institutions, such as banks, in an attempt to steal account login credentials.
- Malvertising embeds malware in ad networks that display across hundreds of legitimate, high-traffic sites.
- Compromised legitimate websites host embedded malware that spreads to unsuspecting visitors.

Malicious code typically installs spyware or malware by exploiting known vulnerabilities in a browser or in the browser's associated plug-ins. These malware threats include:

- Fake antivirus to extort money from the victim.

Web threats change fast and the crooks who create them constantly try new techniques to avoid detection.

- Keyloggers to capture personal information and account passwords for identity or financial theft.
- Botnet software to subvert the system into silently joining a network that distributes spam, hosts illegal content, or serves malware.

Shields Up!

Undoubtedly you already have some protective measures in place but are they sufficient in today's environment? You may already block access to potentially dangerous URLs by using a URL filter that's installed on the exterior edge of the network to inspect outbound URL requests and block access to known malicious or inappropriate sites.

These filters may also serve as proxies to improve both network performance and security but most haven't really kept up with current threat levels because they rely on site reputation for decisions about security and that leaves users vulnerable to new and more sophisticated malware threats.

Are you using any software as a service (SaaS) resources? SaaS promises easy access and outsourced operation, but your IT department loses full control of corporate data, availability, and up time. You lose location-aware browsing, meaning that people using a Web-based application in Savannah might be identified as being in Milwaukee.

If any of your employees work remotely, they present an even more serious security challenge and the threats vary depending on whether they're working from home, from a coffee shop, or from a hotel or airport.

Web threats change fast and the crooks who create them constantly try new techniques to avoid detection. Obfuscation techniques make code impossible to read. Polymorphism allows malware have a different disguise every time it shows up. As a result, traditional gateway solutions are unable even to see the threats, much less protect against them.

Today's protective applications provided by Sophos and other such companies use a variety of methods to identify and block threats. Although I've used information that has been provided by Sphos, the purpose of this article is not to promote applications by Sophos. The company's offerings are robust and reliable but many other companies make equally robust and reliable applications.

My point is that your company should assess the threats arrayed against it regularly. Annually, at least, and preferably more often. Ω

nLightened Thoughts (ISSN 1543-1533) is for clients and friends of n-Lighten.us, 179 Caren Avenue, Worthington, Ohio 43085. Phone 614.859.9359. On the Web at www.n-Lighten.us.

On the Bleeding Edge

When I recently upgraded my primary desktop computer, which was 3 years old, I remembered to specify a faster CPU, a new main-board, increased RAM, and more disk storage but I neglected to say anything about a solid-state drive even though it was on my wish list. Fortunately, the company that's taken care of my computing needs for more than a decade reminded me.

In the old days, I recommended adding memory to speed a computer. Now I can say without question that a solid-state drive (SSD) is the way to go.

I start a lot of applications automatically at boot time because it saves time later when I need them but this also makes the boot process tedious. The computer took so long to become usable that I added Startup Delayer so essential programs started immediately and others are delayed for up to 30 minutes.

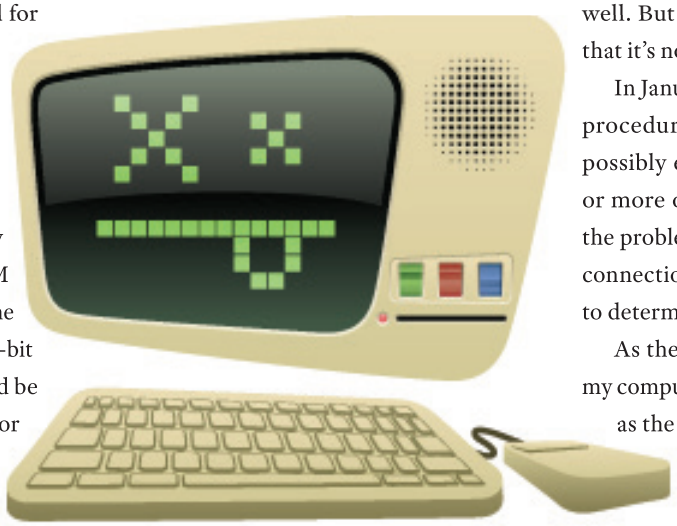
Although I've installed Startup Delayer on the upgraded computer, I'm not using it. Those "essential" applications are all ready to go within about 45 seconds now.

So I still recommend more RAM. Any 32-bit system that has less than 4GB of RAM should be upgraded to that amount, which is the maximum a 32-bit system can address. Any 64-bit system that has less than 4GB of RAM should be upgraded at least to 4GB and preferably to 6 or 8GB. In my case, it's 32 and I had seriously considered 64.

Solid-state drives have been around for a few years but the technology is still relatively new and anything that's new can be subject to a variety of amusing anomalies. For example, the SSD disappeared when a DVD burner application created a problem that required me to simply pull the plug on the computer.

When I say "disappeared" I mean that the computer would no longer boot and the disk drive didn't appear in the BIOS list of drives. Scary! Research suggested that this particular model of SSD had a known problem that caused it to disappear after the kind of power-off reset I had used. In fact, the drive did re-appear but only when the computer had been turned off for a few hours, so that was hardly a solution.

The manufacturer had released a firmware upgrade and the problem was eliminated as soon as I installed the patch. Burning DVDs still causes the system to crash somewhat randomly but the boot drive is always there when I restart the computer.



The DVD Problem

This hasn't been as easy to resolve. So far we haven't even been able to determine whether it's a hardware problem or a software problem.

Hardware seems the more likely for two reasons: First, the various applications all work as expected on another 64-bit computer that's running Windows 8. That fact alone essentially rules out software conflicts as the cause. Additionally, the desktop computer has 4 hard drives and an optical drive. Even though the built-in disk controller is fast and includes a lot of serial ATA (SATA) ports, there could be a timing problem.

This has become a relatively low priority, though, because I have a workaround: The disc RIP and burn processes run fine on the older notebook computer. It's also a low priority because everything else on the desktop system works so well. But a low-priority problem doesn't mean that it's not a problem.

In January I'll find time to try troubleshooting procedures that may identify the problem or possibly even eliminate it—disconnecting one or more of the hard drives to see if that clears the problem or maybe moving some of the drive connections to other locations on the controller to determine if that solves a timing issue.

As the owner of the company that upgraded my computer said, "I have 3 computers with SSDs as the primary drive. I have not had problem number one but I still consider them 'new' technology and that always has me on my guard."

The takeaway is this: If you want to play with new toys, it's a good idea to know somebody who will have your back—just in case. Ω