RANDOM THOUGHTS
Communications With A Purpose

William Blinn
COMMUNICATIONS
179 Caren Avenue
Worthington, Ohio 43085
614-785-9359
Fax 877-870-4892
www.Blinn.com

September 2008

Internet Threatened by Scams and Fraud

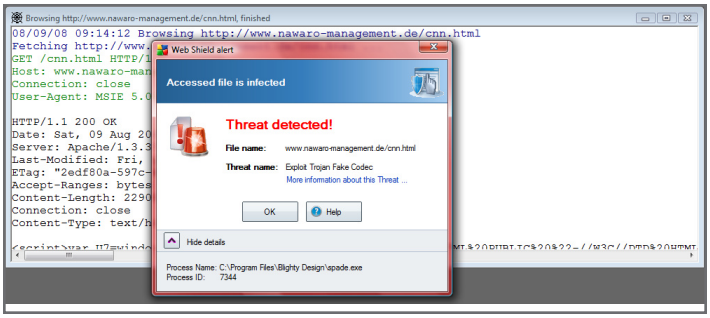
Every day, I receive literally hundreds of phony news alerts, bank warnings, update notices, and such. Literally hundreds. More than 99 percent of these never reach my inbox because I have some sophisticated anti-spam measures in place, but there is a place where I can go to look at them. A lot of these messages do make it through to people's in boxes.

"In the last week I've seen a generous number of one spam type that puzzles me. It purports to be a CNN Alert. The content looks entirely legitimate," and acquaintance wrote. "The links (none of which I've followed) are all genuine CNN site pages." The writer was puzzled, but it was an easy case to solve because I had already seen dozens of these in my spam trapper.

Here is one such message.

It's true that most of the links go to CNN, but not all. The key link is the one that went to some poor clueless roofing company in England. Crooks had broken in and planted their file on the roofing company's server. It was coexisting with the roofing company's website. The domains uses for the payload varied from one message to another, but they never went to CNN's website or, in later messages, to MSNBC's website.

My favorite tool for investigations is Sam Spade, which can show me rogue code without any chance of actually trying to run that code because it's not a browser. However, AVG Antivirus monitors all inbound traffic and immediately warned that there was a problem. It also stopped the data transfer, even though Sam Spade could have accepted it without any risk. I couldn't see what the crooks were trying to do, but I could see enough to understand how they were doing it.



Instead of a plain-text HTML page, they served a script that used obfuscated code to display the page and serve an executable file to whatever unsuspecting browser might happen to find the page. By "obfuscated code", I mean that the crooks had written everything in hex code. That makes it hard to read. "Hello", for example, would be rendered as "%48%65%6C%6C%6F". Although it's hard for humans to read, it's easy to translate back to plain English.

What I could see was the beginning of what would be interpreted as a standard CNN page with a link to play the appropriate video. Except that the "video" link wouldn't link to any video. Click it, and your machine will be infected.

The Threat is Real

There's much good on the Internet. So much that it's hard to imagine life without it. But there is so much dreck, trash, and crime that some people are afraid to use the Internet, much less do business on the Internet. It's possible that enough bad things will be on the Internet that a majority of people will stop using it.

That's a distant threat, I think, but it could happen.

But I see yet another danger in these fake news stories. It's clear that the nation has no shortage of people who can't be bothered to check the facts. Instead, they just pass along whatever the hear from someone as long as it fits their particular set of biases. These "news" reports are problems on two levels: First, they can infect the victim's machine. Second, there are people who probably will actually believe that these stories are true.

Here are some of the "news flashes" that arrived in my spam slop bucket over about 3 hours: Illegal Immigrants Seize Control Of The U.S. • Prominent Male Hooker Forced To Step Down After Sex With Sleazy Evangelist •

Random Thoughts (ISSN 1543-1525 [print] – ISSN 1543-1533 [electronic]) is a publication for clients and friends of William Blinn Communications, 179 Caren Avenue, Worthington, Ohio 43085.

The Antichrist Revealed! video. • "brainstorming" To Be Banned Under Equality And Diversity Rules • One Hot White Chick Injured in Tsunami Disaster • Gays Banned From Owning Pets In New York • New Evidence Suggests That The President May Be Drinking Again • Army Relent On Shooting Live Pigs In Training Exercise - Will Shoot Illegal Immigrants Instead • Paris Hilton Considered For Mother Teresa Role • Iran Kicks America In The Nuts • Obama Captures Osama • And Now We Return To The Subject Of Jennifer Anistons Breasts • Cindy Mccain Talks About Her Boobs • Obama Is Anorexic Over-Exerciser • President Bush's iPod: The Complete Playlist • Paris Hilton Lectures On Dickens And Dostoevsky • Paris Hilton Tosses Dwarf On The Street • Pamela Anderson Cheating On Tommy Lee And Seeing Barack Obama.

How could any sentient human believe any of these, much less click on the link to read more? ß

Backup³

Real estate agents talk about "Location. Location. Location." For me, it's "Backup. Backup. Backup." No matter how careful you are, no matter how much you paid for your computer, no matter how well you maintain the computer, everything on it can disappear in an instant.

- Have you ever used an existing document as the basis for a new document and then, without thinking, saved the new document using the old filename? I have. Goodbye old file, unless you have backup. I did.
- Have you ever formatted one of two disk drives in a machine, thinking that you're formatting the C drive and accidentally pointed the format gun at the head of the D drive, the one with all your data, time billing records, photos, and music? Yeah, I've done that, too, I'm embarrassed to admit. The only recovery is backup.
- Ever have a machine just die? Been there. Done that. Recovered the data.
- So far, I haven't had a computer stolen.
- We did have a network-spreading virus/worm years ago when the "I Love You" messages circulated. That was May 4, 2000, and the message appeared to have come from someone I knew. We've become smarter since then and we've instituted more safeguards, but backup saved the day. A lot of people I know lost every jpg on their computer because that particular virus overwrote (among others) all jpg, jpeg, vbs, vbe, js, css, and doc files.

Files exist on fragile magnetic or optical media. The more copies you have, the less likely it is that you'll lose something important.

If you already have a bulletproof backup plan in place, congratulations! If not, today would be a good time to start setting one up. ß

The Big Wait

Any time spent waiting for a computer is wasted. Windows in general and Vista in particular waste a lot of my time as I wait for the machine to become ready. Apple's OSX takes a little less time, but the real winner (if I want to limit the amount of time I have to wait) is Linux.

One recent evening, I realized that I was sitting between two computers that were both at the login prompt. *Drag race!* was my first thought. I could enter the passwords, press Enter, and see which one was ready to use first.

The Windows system had an extreme advantage because the computer is powered by a dual-core CPU that runs at 2.7GHz and has 2GB of RAM. The Linux machine runs on a 1.4GHz single-core CPU and has just 1GB of RAM. Even worse, Ubuntu Linux is installed within the Windows file system on the notebook and that causes it to run more slowly than it would if installed in a partition on the disk.

The Ubuntu machine was ready for use in just 30 seconds. The Windows Vista machine had reached a semi-usable state after 60 seconds on a machine that's at least 4 times faster than the Linux machine. Vista was truly usable only after more than 3 minutes 30 seconds. Had Vista been on the same hardware Linux was on, the elapsed time would have approached 15 minutes!

What does all this mean? Possibly not much. If you're the kind of person who comes into the office, starts the computer, and goes off to have breakfast, you won't notice much difference. But if you're the kind of person who fires up the computer and wants to start working right away, you might find the Windows delay more than a little annoying.

There's more to this than just startup time, of course. Some people leave their computers on all the time. My office computer is on 24 hours per day, 7 days per week, because that allows me to gain access to the office computer and files I might need evening and weekends.

Another consideration is whether the software you need is available for the operating system you might like to use. I'm still primarily a Windows user because some of the applications I need aren't available for Linux and no Linux equivalents exist.

But for a lot of people, a Linux machine with Open Office and Firefox would be more than sufficient because it covers the basic needs: Word processing, spreadsheet, data management, e-mail, and Web browsing.

No wonder the folks in Redmond are keeping a nervous eye on the rear-view mirror. ß

CORNER on the market by A.J. Stinnett

"Provide good physical working conditions and ensure that employees have the tools they need to do their jobs."