RANDOM THOUGHTS

I may be crazy, but I'm not stupid.

2003:09

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

Danger ahead: Terrorism by e-mail

As bad as spam is, the Internet brings us things that are even worse: worms and viruses. The Homeland Security folks suggest that we'll see a major attack on the Internet. I think they're right and I believe that it will happen sooner rather than later.

Microsoft is a large part of the problem, but users who haven't bothered to learn how to protect their computers and why this is important share some of the blame. I'm writing this on August 20, as the latest round of the "SoBig" virus is ripping through computers at an unprecedented rate.

The systems administrator at a large university in the Midwest announced earlier today that in 13.5 hours, their central mail servers detected over 60,000 copies of the Sobig.f virus from several thousand unique IP addresses. How bad is that? It's more than double the number of viruses detected in the university's previous worst month! That's right. In slightly more than half a day, they detected more viruses than in their previous worst month.

The math is easy: That's about a 60-times increase!

The university's help desk e-mail address and their Listserv server's administrative address have been forged on copies of the Sobig.f virus.

Last week, it was the MS Blaster worm. What will show up in your mailbox next week? Chances are, it won't be pretty.

Worms and viruses

Worms can replicate across an entire network in a few minutes because once they're on your network they need no human action to continue the spread. Nobody has to receive, send, or open an e-mail. Worms look for ports that are needlessly open and unnecessary services that are running.

Many of the current problems are combination worm-virus attacks. In many cases, the attacks use the Microsoft Outlook or Outlook Express e-mail application to send messages with forged "from" lines to addresses found anywhere on your computer. I've already received several virus warnings from systems that received messages "from" me. Needless to say, I haven't sent any infected messages. I was caught once, several years ago, by the first e-mail trick. Never again.

Being on the font lines

In the "good old days", viruses and worms were mainly the work of adolescent boys (mainly boys) who weren't bright enough to write useful applications they could sell. Instead of slashing tires, scratching new paint, or throwing rocks through store windows, they got their enjoyment by releasing malware that crashed computers or networks and occasionally deleted files.

It should come as no surprise to any of us that some people don't much care for "The West" in general and the United States in particular. For whatever reasons – some say it's because they have been unable to develop an open society or an economic system that will allow anyone but a few at the top to accumulate any wealth – their goal is to destroy what others have developed.

What appeals to these largely powerless individuals about the Internet is that they can attack without having to leave the discomfort of their cave or hovel and there is little chance that they will ever be identified, located, or prosecuted. And because so many of us have become so dependent on the ability to obtain information, buy or sell products or services, and communicate with each other via the Internet, the target is particularly attractive.

And when you consider that most home computers and many corporate networks are operated by people who have had no training at all in computer security, the target becomes irresistible.

Persistent pestilence

Viruses and worms will become harder to identify and eradicate. It is possible for rogue websites and malicious e-mail attachments to install pieces of apparently harmless code on your computer today. The code appears harmless because it is harmless – by itself. Imagine a malware application that loads a little "ammonium nitrate fertilizer" into your computer one day and another malware application that adds some "kerosene" the next day. A week or two later, a third piece of malware loads a "detonator". A fourth component arrives later. It checks in each day with a remote application that one day sends a message to all computers that have been loaded with "explosives" to "detonate".

Of course it's impossible to load fertilizer, kerosene, and a detonator into your computer via the Internet, but it is possible to load several code components that could be combined and

Random Thoughts or Dead Trees?

Dead Trees seemed to be a somewhat negative name for this publication. Starting with this issue, the new name is ***Random Thoughts***, suggesting – if not deep analytical articles – that at least minimal thought during development of the articles. Please note that I still bear no particular animosity toward trees.

ISSN 1543-1525 (print) – ISSN 1543-1533 (electronic)

then executed. What would be the result of 1,000,000 computers staging attacks on a few hundred carefully identified sites? What if all of the files on 10,000,000 computers suddenly vanished? Or 100,000,000?

The City of Columbus recently had to hand check every single police cruiser because most of the on-board computers had been infected with the MS Blaster worm. If something like this doesn't make you nervous, what does it take to make you nervous?

What you can do

Without even thinking about it very hard, I see at least 6 essential steps. More may occur to you, but start with these.

- First, understand that conditions aren't going to improve anytime soon.
- Second, practice thinking about safety. When I received an e-mail with an attachment but no message, I didn't open the attachment even thought the message was from someone I knew. Instead, I sent a message to ask if the person sent a PowerPoint presentation to me. She had sent it, and it was safe. A small delay saved what could have been a mess.
- Third, install a firewall. There are hardware firewalls and software firewalls. I no longer consider these as optional, "nice-to-have" additions. If your computer doesn't have a firewall, you have effectively hung out a sign that says "Take my computer and do anything you want with it. I don't care." If you have a home computer network that is behind a router/switch, the router/switch uses network address translation (NAT). This is not secure. You still need a firewall.
- Fourth, be absolutely certain that you have an antivirus program installed and that your application automatically checks for new updates at least once per day. Do not depend on the antivirus program to detect every virus, though. Every antivirus program has some shortcomings and all antivirus programs will miss new viruses that can often spread in the wild for several days before the antivirus program has updated definitions.
- Fifth, if your operating system offers an automatic update service (many version of Windows and Apple's OS X offer an update service) turn it on and be certain to install every security-related patch.
- Sixth, never trust anything you receive by e-mail – particularly if it has anything to do with money or credit cards. Make sure that the message has come from the person or company that it claims to be from.

The Internet is just a tool

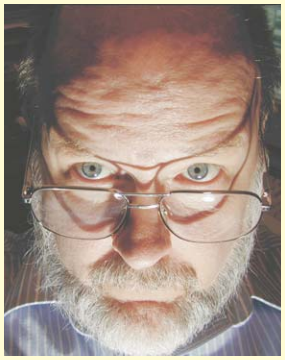
Tools aren't good or evil; they're just tools. A hammer can be used to build a house that will keep a family warm and dry, or it can be used to commit a brutal murder. The automobile gives us mobility that people could have barely foreseen even 100 years ago, yet it is responsible for dirtying our air and killing tens of thousands every year. Even immunizations that protect us from horrific diseases occasionally – instead of providing protection – cause disability, disfigurement, or death.

The Internet is simply a tool. We use it to do our jobs better and faster. We use it for entertainment and enjoyment. We use it to share knowledge and to keep in touch with friends and family. But it can also be used against us for great harm.

I encourage you – Please! Take computer security seriously starting this very minute.

Before the end of this day, I hope you'll be sure that your antivirus program is up to date and that you wil have installed Zone Alarm (or have ordered a hardware firewall). All of us have had more than adequate warning about what is likely to happen. We can continue to ignore the signs or we can take prudent actions to protect ourselves, our computers, and our data. The threat is real. The time is now. ß

Have you reserved your TechX report?



Once upon a time, I had hair. Then I got married, enjoyed watching 2 daughters grow up, and started going to New York City every summer for what used to be called PC Expo.

Whether any of this had an effect on my increasingly hairless state, I can't say. But if I hadn't been going to New York City for the past dozen summers, I suspect that I might have even less hair.

Technology changes fast and it's hard to keep on top of things When someone does what I do for a living, he's expected to know what's coming. In a dozen years or so, I've learned the ins and outs of the show, which events to attend and which can be skipped.

Each year, I make my *intelligence report* available to clients at a cost that's far less than even airfare to New York. See the enclosed note if you're interested.

I remember the year that Intel was showing a sneak preview of the "blazingly fast" 486 (how slow they seem now), when the first personal organizers started showing up (long before Palm), and when Linux was going to take over the world (didn't believe it then; don't believe it now).

What's going to be the next critical trend in the industry? Watch for more connectivity (Bluetooth, USB2, Firewire 800) and more networking abilities (WiFi), along with further integration between computers and mobile phones. Your next desktop computer may be a notebook! **If you're wondering about these things and want the straight story, make sure you reserve a copy of my report.** ß

on the market CORNER

by A.J. Stinnett

Given the correct tools and information, the majority of employees will perform as well as they possibly can.