Spyware, Adware, Malware — It’s All Sleazeware to Me

Richard O’Hanley

Forget spam; forget phishing. The thing that will kill the Internet is what we’re calling sleazeware — malware in all its nefarious forms. This month’s issue has nothing to do with sleazeware (although we do discuss cookies and privacy invasion. For more on malware, see Ken Dunham’s columns in Information Systems Security). It’s just that I spent last month engaged in war with malware of all types, both at work and at home. The home PC is about as locked down as possible without disconnecting it from the Internet. Among our use policies is not downloading of music, lyrics, or anything free. Believe it or not, the kids follow this.

Here’s what happened. I replaced a worn-out mouse with a new optical one. I also reinstalled Nero, which is a CD burning software. After rebooting, I received the following message: “X has caused an error in KERNEL32.DLL” where X = explorer, iexplorer, remon9x, msism, backweb-887480, wuauboot, mset, netsurf, minibug, or ssdpsrv. I knew that I had to get rid of remon9x, netsurf, and minibug. Of course, none of these appear in the add/remove software menu in the Control Panel, and I couldn’t find all the program and registry entries for them.

At start-up, Word launched in DOS mode and immediately hung up. At the same time, something disabled ZoneAlarm (“system error. please reboot”), IMAlarm, and AV (although when I checked why Ad-Aware was so slow, I saw an AV scan running concurrently). Also, I saw a message about Weatherbug wanting to install itself, and “The Support Tuner has encountered a fatal error.”

I also discovered clientman and favorite-man, and something called “NCase.” Ad-Aware could neither delete nor quarantine them. There was no Internet access. The PC would not shut down unless I literally pulled the plug. I couldn’t make a new boot disk from Windows, and had to use DOS to grab command.com, autoexe.bat, and a few other files.

My first thought was to reinstall the OS. I reinstalled ME twice (the PC is a Dell Dimension). No change. I also tried to install Mozilla as the default browser. I was unable to install it, but somehow a survey from Netscape, which I couldn’t delete, did install.

Then I downloaded HijackThis at work and brought it home on a floppy. I analyzed the log file (with some help from Windows Startup Online Repository (www.windowsstartup.com) and Windows Process Information (at www.liutilities.com). I had HijackThis fix what it could, rebooted, and encountered many of the same problems.
Next, I ran Spybot, had it fix what it found, rebooted, and the computer died.

Desperation sank in. I was ready to reformat the disk and start over. Instead, I installed Windows 2000 on top of ME, said a prayer, and rebooted. This cured most of the problems, except for AV, the Office applications, and IE. I uninstalled these, then reinstalled, said another prayer, and rebooted. This finally did it. Total time spent was about 20 hours (including the time it took for the various scans to run).

Here’s what I don’t understand. I suspect that I know a lot more about computers than my neighbors. My neighbors all have cable modems and most leave them and their PCs on all the time. I also suspect that while they may have AV, they don’t have firewalls and don’t routinely scan for sleazeware. So, do they not have PCs that are totally infected, or are they somehow magically immune?

Spam is a nuisance, but easily deleted. Phishing isn’t a problem unless one is naive and gullible. But sleazeware happens; it just happens, and it happens at work and at home. Except for disconnecting everything from the Net, I can’t think of a solution. I doubt whether legislative action such as the Spy Act and the Internet Spyware Prevention Act will have any effect, especially when companies like WhenU and Claria have “cleaned up their acts” and are contemplating IPOs based on their proven ability to own PCs anytime and anywhere. I would, however, like to hear some. Send them to me at ro’hanley@crcpress.com and I’ll print them in the next issue and online at the journal’s new Web site, www.infosectoday.com.

A NEW WAY OF THINKING ABOUT DATA INTERCHANGE

This issue opens with an article on digital identities. Much time has been spent developing file formats and protocols for data exchange, but not much has been spent considering the ownership of exchanged information and foundations of interorganizational trust. What is needed today is an abstraction layer above the data that provides a flexible platform to negotiate and establish trust between communication endpoints. This data framework would bring identity control, coordination, and orchestration to Web services and allow location independence, loose coupling, and dynamic interoperability of SOA components. This is the Data Web — a new way of thinking about data interchange.

An Anti-Sniffer Based on ARP Cache Poisoning Attack

This article discusses an anti-sniffer based on a new detection technique. The proposed technique uses mainly an ARP cache poisoning attack to detect sniffing hosts in an Ethernet network, and is implemented in a tool called SupCom anti-sniffer. The authors also test four anti-sniffers.

Reducing Enterprise Risk with Effective Threat Management

Risk is the buzzword of the year, and managing and reducing risk the twin Holy Grails. Threat management combines all operational actions of intrusion prevention and protection into a life cycle where one component feeds the next. Effective threat management enables true, enterprisewide intrusion prevention and protection. By implementing such a program, an organization will fortify its environment, reduce its exposure to threats, and attain the security intelligence it needs to continuously improve its security.

SB1386: One Year Later

(California Strikes Again)

This article represents a comprehensive review of SB1386 and its implications for businesses from both a legal and information security perspective. It presents technical requirements, including numerous proactive steps that can be taken by an organization to avoid the significant ramifications of noncompliance, to comply with this legislation. This consumer protection legislation is precedent setting and not limited to California, as evidenced by the recent bill
introduced in the U.S. Senate by Senator Diane Feinstein. Senate Bill 1386 may become the benchmark for customer privacy information protection for the entire United States.

**Cookies and Privacy**

Yes, the road to hell is paved with good and innocent intentions, and cookies are an excellent example. This article provides an excellent overview of the structure of cookies, the advantages and disadvantages of cookies, legal issues, and United States and European Union laws regarding the use of cookies. If nothing else, it will raise your hackles.

We also have Ken Dunham’s and Ed Freeman’s columns, always timely and insightful. That’s it for this issue. Keep your letters and comments coming. We’ll print all those that fit.