Los Angeles Times
latimes.com

http://www.latimes.com/technology/la-na-spyware26nov26,1,315167.story?coll=la-headlines-technology

COLUMN ONE

Breaking, Entering Your PC

Spyware, the newest and nastiest online plague, can paralyze or commandeer a computer. Help is hard to find, but it's out there.

By Terry McDermott
Times Staff Writer

November 26, 2004

It can, and often does, start something like this:

You're online, maybe searching for a specific piece of information, maybe just cruising the Web. I was investigating new search technologies that were advertised as useful in dealing with variations in the spelling of names and had read that Lycos, a pre-Google Internet portal and search engine, had developed some.

I found links for Lycos and clicked on one. That was the beginning. Within minutes, my computer was swamped with advertisements — pop-ups, pop-unders, pop-all-overs. There were so many I couldn't close them before others started appearing. I had to shut the computer down.

When it restarted, my Web browser had a new pornographic home page, and soon another flood of advertisements was underway. This time, I was able to get rid of most of it and resume working.

It went on for days. The blizzard of ads sometimes thinned, sometimes thickened. At times, there were so many that the computer couldn't process them all and froze. Every time I restarted, my home page was reset to the pornographic site. Every time I tried to do a Google search, a Lycos search engine appeared instead. New items for services called Bargain Buddies and Deal Helper were added to my Web favorites list.

I deleted these entries, but they would mysteriously reappear. Once, when I was being buried yet again by ads, I heard my computer modem dialing a telephone number. My computer is connected to a broadband Internet access service, so the only time I ever used the modem was to send and receive faxes. I couldn't imagine why the modem was dialing. More to the point, I couldn't stop it.

I have been using PCs since 1985 and have installed hard drives, operating systems, memory, CD-ROM drives and countless software programs. I've written some rudimentary programs to automate common word-processing tasks. I vainly considered myself a computer sophisticate.

So what did I do? I cursed and screamed. I tried to turn the modem off with software switches. Finally, I did what any sophisticated computer user would do — I yanked the telephone cord out of the wall, then began wildly deleting every suspicious file I could find on my system.

That worked to a limited extent. I installed a pop-up ad blocker and downloaded free programs that were supposed to rid me of the plague that had descended.

Most days, I was able to slog along and there were even times I thought the fixes had worked. But the computer was still agonizingly slow, and the ads and the hijacked Web searches invariably reappeared. Then a month later, I received a bill for $25 from some company I had never heard of. It was for the telephone call my computer had made, to Britain it turned out.

The Internet, at once one of the wonders of the modern world and one of its least likable neighborhoods, has suffered a series of afflictions, scams and perversions throughout its brief history. The latest and in many ways most frustrating is the one I was now facing — spyware.

Spyware is a broad category of software distributed online, usually without a user's knowledge, to millions of personal computers around the world, often crippling them in the process.

It includes several subcategories, including:

• Loggers — programs that surreptitiously monitor a computer's use, recording every keystroke, and sending that information to the spyware's manufacturer.

• Adware — programs that use the data generated by loggers to send advertisements to individual computers.

• Dialers — programs that cause a computer's modem to call long distance, frequently international.

As an unwanted invader, spyware has some things in common with e-mail viruses, but differs in two important ways.

Viruses can be stopped by relatively inexpensive software. Spyware distribution is more devious and often almost impossible to stop. It is also much more difficult to find and remove from afflicted machines.

Also, although spyware, like viruses, often seems pointless, it usually is not. It is driven by one of the oldest of human motivations — profit.

In most cases, someone is being paid to make your computer useless. That is the special irritation experienced by afflicted computer owners: Someone is profiting from their misery. Or at least, that was the special irritation that got me.

I started digging into the innards of my operating system, looking for clues. Whenever I found files I could not determine the authenticity or purpose of, I got rid of them. In the process, I sometimes got rid of necessary files. I was slowly breaking the legitimate functions of my machine.

I contacted tech support at various software and hardware manufacturers. Mainly, they suggested I wipe out my computer's hard drives and start from scratch.

On the days my computer let me, I searched the Web for the origins of my problems. I felt like a lonesome settler in the Wild West, besieged by outlaws. Where was the posse when you needed it?

That's when I stumbled onto AumHa.org, a website named for the first and last letters of the Sanskrit alphabet. Wherever I had expected salvation might reside, it was not in a land where the residents spoke Sanskrit.

No matter. My posse had arrived.

One of the more discomforting aspects of the modern world is most of its inhabitants' utter ignorance of the technology that shapes it. Not one in 100 computer users has the least idea of what goes on inside the machines they spend many waking hours engaged with. They have no more concept of what's under the lid of their computer boxes than Ptolemy had of what was on the dark side of the moon.

Moreover, there is no obvious place to turn for help. Computer and software makers haven't the resources, or, as often, the desire to help. Any plea for tech support is apt to lead a computer user on a round-robin of calls, with each manufacturer emphatically shifting the blame to another.

One of the charms of the same modern world is the degree to which there has emerged a vigorous, selfless missionary corps dedicated to explaining — and where that's undoable — leading the benighted rest of us to safety.

That the missionaries can be a pretty weird lot does not matter. Mine included the guy with the Sanskrit website, a bartender and an epicure from Pennsylvania.

The AumHa Web forum was begun five years ago by Jim Eshelman, "mainly," he said, "as a place to post my resume." At the time, Eshelman was approaching middle age with no real career or even relevant experience necessary to begin one.

An autodidact, he had a head for numbers and an analytic cast of mind, but almost never the credentials an evolving workplace demanded. He had worked as a legal but unlicensed workers' compensation lawyer for most of his professional life, until the state of California decided in 1992 that one really ought to have a law degree to do that.

He was a longtime computer hobbyist who in the mid-1980s had begun a computer support company. He discovered he "liked helping people and hated doing business."

A decade later he built his current website and within weeks was getting "a lot of e-mail that was hard to answer." It didn't matter. Other people — people he did not know — leaped onto his site to help. To Eshelman, this communitarian attitude was a throwback to his hobbyist days.

"It used to be [information technology] knowledge was like drugs — if you had some, you shared it with friends," he said.

He sought to continue that attitude through his new site, which gradually built both an audience — now almost 7 million visits a month — and, more important, a community of like-minded hobbyists eager to contribute what they knew.

The site has multiple forums for various computing problems, but the overwhelming number of inquiries in the last year has dealt with spyware, which on the site has a variety of less neutral names, "scumware" being one of the more polite. Scumware had been an epidemic; in the last year it grew into a pandemic, said Steve Wechsler, one of those drawn to Eshelman's site.

Wechsler was tending bar at a public golf course in South San Francisco when he bought his first computer less

than a decade ago.

"I brought it home and turned it on, clicked on Netscape and expected something to happen. I still think about how dumb I was," he said. That ignorance makes him empathize with other casual users, people who expect their computers to be tools, not obligations.

The muting of the usefulness of those tools is what motivates him most. "I hate bullies. I've hated bullies my whole life. They prey on people. I'm not going to sit by and do nothing," he said. "It's your computer. They have no right to assault it."

AumHa's volunteers instructed me to download, for free, diagnostic tools and spyware cleaners. The most interesting of these is a small program developed by a Dutch graduate student that takes a snapshot of important settings in your operating system, Web browser and other software. You are asked to post this snapshot on AumHa's forum, where your computer is scrutinized by whoever happens to be logged on.

In essence, you are being asked to publish very private information (a man's "browser helper objects" are about as private as you can get) in a very public place. It's a daunting request. I paused for perhaps a nanosecond.

The site is a contemporary equivalent of the old highway construction crew — a lot of guys leaning on shovels giving advice to the guy in the hole — me — doing the digging. But it worked.

I had been fighting the spyware plague for more than a month. The AumHa guys fixed it in a day. For absolutely nothing.

Wechsler and Robear Dyer, a fine wine and food salesman, determined that I had been victimized by what they called a "drive-by download," in which a computer user is tricked into authorizing a software download.

The downloaded programs then burrow into your operating system in such a way that even if you notice and delete them, instructions are left behind to replicate them the next time you restart your computer. My frantic deletion of unknown files had been not only rash, but futile. I could have deleted for a decade and likely not have changed anything.

As Wechsler put it, I had been mugged. For all its guises, most spyware is either itself advertising or involved in the distribution of advertising tailored to computer users' online desires.

It can be targeted to send you an advertisement for a specific product at precisely the moment you are about to buy a competing product or the same product from a competing vendor.

Say, for example, you're going to book a flight from Los Angeles to Chicago on Expedia, an online travel service. You find a flight for $388 and are about to book it. The adware buried in your computer sees what you're doing and automatically sends an advertisement from a different travel service, for example, Travelocity, touting the same itinerary for $10 less.

The general idea, apart from the creepiness of being spied on, sounds almost benign, especially since it can give a customer a bargain price.

In practice, it's something else. The companies the advertisers pay to send ads out get mere pennies, or sometimes

fractions of pennies, per ad. They have little incentive to ensure that the ads are narrowly targeted; the more they send, the more they get paid.

"We're dealing in a business with a lot of pennies," said Todd Sawicki, director of marketing at 180solutions, one of the leading companies in delivering targeted Internet advertising.

The result of chasing those pennies has been a flood. Spyware is by far the most common category of complaints received by software and computer manufacturers. It is responsible, for example, for up to "one-third of operating system crashes reported to us," said Paul Bryan, who works in Internet security at Microsoft.

My case was sadly typical. Consumers have downloaded free versions of the two most widely used antispyware programs more than 50 million times. In the right conditions, they work fine but are more useful after the fact than preventive.

Spyware is brazenly sneaky. In fact, some manufacturers advertise their products as tools to fight the spyware they install. Then they charge customers to remove it. Eshelman calls such programs "betrayware."

"What these programs have in common," said Ari Schwarz of the Center for Democracy and Technology, an advocacy group in Washington, "is a lack of transparency and an absence of respect for users' ability to control their own computers and Internet connections."

The people who manufacture the code that becomes spyware argue that they are not purposefully setting out to irritate millions of people. They contract the distribution of their software to third-party vendors. Sawicki of 180solutions said his industry had been victimized, too.

"We're not trying to be some company stomping on consumers," he said, but acknowledged the company had not been careful enough in overseeing the vendors it hired to distribute its programs.

Also, 180's program, nCase, is notorious in the antispyware community both for the amount of advertisements it sends to individual computers (hundreds per day) and its near impossibility to remove. Many spyware programs, like nCase, hide themselves so well they can't be removed even if found by the standard uninstall features of Microsoft Windows.

180solutions has acknowledged this, although not directly, by promoting a replacement program, which is supposed to be more transparent, less intrusive and easier to remove.

Maybe so, but many weeks after Sawicki spoke, a friend called and reported that his computer had been hit by a rash of spyware. With the tools from AumHa, we looked inside, and there sat nCase.

Exactly how it got there was, as usual, impossible to determine. Sawicki blames the problems on "guys in Bermuda, offshore. They're the online equivalent of spammers. We want them to die a slow and painful death."

In lieu of death, various law-making bodies, including Congress and the California Legislature, have debated antispyware laws, but so far have not come up with anything those in the business think will be effective.

The Federal Trade Commission has established a spyware task force and filed a handful of lawsuits under existing fraud laws against spyware distributors, but they've had little broad effect. Often, it isn't even the spyware itself that

is illegal, but the method of distribution, which is hard to track.

Even when investigators have been able to uncover a distribution source, many have been beyond U.S. jurisdiction. Rumors variously place the distribution of most spyware in the hands of the Russian mafia, Caribbean expatriates and even Al Qaeda.

All of which leaves the Sanskrit posses with their fingers in a very unstable dike. They're doing what amounts to heroic work in nearly complete anonymity.

For a brief time, Microsoft cut its backing for its own online support forums, but quickly realized it would be overwhelmed with problems that the forums were addressing. Instead, it redoubled its assistance to the forums.

These volunteer efforts turn the common depiction of computer cognoscenti as isolated, antisocial geeks upside-down.

Eshelman works a full-time IT job in Burbank. He spends almost the equal of another full-time job working at AumHa. Dyer guesses he spends more time online offering help than he does making a living.

Other AumHa volunteers regularly quit volunteering because they become so consumed with the work, and passionate about it, that it overwhelms their non-Web lives.

They almost always come back, though. The bunch of them, and others at similar sites, say they feel as though they're caught up in a great struggle and feel honor-bound to continue.

"It's war," Eshelman said.

If you want other stories on this topic, search the Archives at **latimes.com/archives**.

TMSReprints

Article licensing and reprint options

Copyright 2004 Los Angeles Times