Print This Article

<< Return to A road littered with hazards: Anti-malware efforts in the wild

A road littered with hazards: Anti-malware efforts in the wild

George Ledin, professor in the computer science department at Sonoma State University •
November 01 2011

Buying a new car? A new computer? New cars come equipped with a lot of safety features. New computers are preloaded with anti-malware packages. Perfectly OK.

Pre-1960s cars didn't have seatbelts, much less airbags, while early personal computers offered no protection against infection by rogue programs, such as Brain. In those good old days, many highway accidents crippled or killed drivers and passengers. A couple of decades ago, damage inflicted on PCs by now-ancient computer viruses was also quite severe. But are today's automobiles safer? Indeed. How about computers? Not that much.

Of course, "safer" is a perception. You can still die in a highway accident. And your computer is probably infected without your knowing it. New malware appears in the wild, where it takes advantage of reactive delays that make zero-day attacks routine. Vestigial malware reappears, repacked. It's an off-the-shelf item, readymade for neophyte perpetrators. Petty cybercriminals graduate to the malware big leagues by launching this nonsense. For some, practice makes perfect, and they rake in the big bucks, mostly by annoying us with spam, scamming the clueless, and stealing our online identities.

The Spitmo trojan, for example, is spreading among certain smartphones, intercepting transaction-verification text messages sent by banks, ironically intended to prevent fraudulent transactions. If your smartphone is already infected by SpyEye, Spitmo entreats you to download an application that pretends to protect you from the kind of theft that it perpetuates. It's as if airbags in certain cars pummeled their drivers.

But let's get real: Neither the weaknesses of cellphones nor the vulnerabilities of onboard computers are being ignored by amoral hackers. All digital devices are fair game.

Complete, guaranteed insulation from all problems is, of course, impossible. That's why we have standards. Automotive safety is covered by lots of them. Windshield, brakes, transmission, tires – everything must meet or exceed prescribed standards. A car that falls short of them is *prima facie* evidence of negligence. Computers must not explode, ignite or electrocute their users. These standards are clear. But there are no standards regulating malware prevention. In the absence of standards, industry and business can follow appropriate-use policies and adhere to safety protocols. Like restaurant workers washing their hands – not as thorough as

surgeons scrubbing, but better than nothing.

Every autumn, public health officials remind us to get vaccinated against a new and forthcoming strain of the flu. This is a forward-looking, sensible measure. Like all such preventive efforts, it is not 100 percent effective. Preventing last year's flu would make little sense. Keeping billions of human beings healthy is a formidable task.

The good health of our digital world is essential to the functioning of all our institutions and individuals. And, yet, preventing its future ailments is not what we do. Like our biological selves, our digital devices are constantly under siege. Unlike living creatures, which can be made to weather new biohazards, the digital world is easy prey.

During the past few years, organizations have sprung up – some formed by anti-malware companies, some purportedly as industry watchdogs. These are steps in the right direction, but none are agencies capable of enforcing best practices, much less actual regulations. We are a long way away from strong standards. Until then, anti-malware efforts in the wild will be like law enforcement was in the Wild West.

George Ledin is a professor in the computer science department at Sonoma State University in California.