Malware: The Great Equalizer

- PDF
- Send to a friend

Malware: The Great Equalizer

Essay by Beau Brendler, June 6, 2008 in response to What Would a More Secure Future Look Like?

> What Would a More Secure Future Look Like?

Eight years ago I spent two-grand-plus on a Sony Vaio laptop when they were still sort of cool. It was kind of a muscle car then, full of multimedia editing software I wanted to make movies with in hopes I'd get invited to Cannes rather than conferences with 2.0 in their titles. But then a wretched worm attacked, days of futile damage control followed, and finally I gave up trying to download Service Pack 2 from the Microsoft site and just asked for a CD, which they sent for about $6. (Genius business model! Charge people for patches to fix security holes in your operating system that can't be downloaded for free because your Web site sucks). After that I might as well have deep-fried my laptop in bacon grease. It lived out its miserable life as hard-drive storage for photos until the screen display dissolved to static.

Just about everybody has a story like this. I don't want to bore you with mine but to make a point I will return to: I'm supposed to be sort of smart about this stuff, somebody who goes on TV and radio and gets quoted in newspapers talking about security and fraud and other Internet things, yet I was brought low by malicious code in minutes. I feel like the paranoid guy in the first Highlander movie — the only good Highlander movie — who drives around New York City armed with Uzis and MAC-10s only to get push-pinned on Clancy Brown's giant Kurgan sword. No one's safe, he complains to the grizzled old detective, bleeding from his ears in a crummy hospital bed. I've got all this stuff, and still I'm not safe.

Now, I don't mean to engage in the kind of hyperbole the computer security industry uses to hype its myriads of marginally effective products. No one's yet actually been killed by badware (though I have stood in the sweaty Manila headquarters of TrendMicro, watching real-time outbreaks of badware attacks on a topo map of South America alight and blaze red like so many fires in the rainforest, which was a little scary). Dumpster-diving and mailbox raiding were still the number one identity theft vectors last time I checked.

But when I go to bed at night, I know my TV set isn't going to be stealth co-opted through my satellite cable and coerced to blast my personal data to somebody in Sighişoara. I don't know this about my PC. A friend of mine who used to manage an Internet service provider told me last week the machine his wife uses to run her home business got skranked so badly by a piece of botnet malware it took days and many dollars to fix. Home invasions just aren't a happy thing, even if the perpetrators are digital and incapable of carrying baseball bats. I'd be pretty mad if someone somehow outside my house buggered my hard drive so badly that I lost even a single picture of my kids. And again: We're supposed to know something about computers, my friend and I.

The feds think: We Have a Situation Here. The National Cyber Security Alliance put out a survey couple of months ago that appears to have gone largely unnoticed, though I don't dispute the results:

* Only 49 percent of consumers changed their password within the past year, 19 percent within the past month. Wanna bet how many are using "password2" or the cat's name instead of the dog's?
* 71 percent haven't heard the word "botnet." Actually, I'm surprised it's not higher, and wonder if the question was phrased, "have you ever heard of a botnet?"
* About half the population don't know "how to protect themselves from cyber criminals," probably more when you factor in the magic of social research.

Badware's even coming at us from digital picture frames these days, and some manufacturers aren't sure how it got there. Buy a memory stick for your camera off eBay, and if it's not a fake and you can get it to work, God knows what it's going to leave you with the morning after. A year ago the FBI said a million computers were infected with malware that could have ginned up an "army of bots" that could threaten national security. "Botnets continue to be an increasing threat

to consumers and homeland security. Unsecured computers play a major role in helping cyber criminals conduct cyber crimes," said Ron Teixeira, NCSA's executive director.

It's true— a Consumer Reports survey two years ago found only 21 percent of Americans actually enabled security software on home PCs. But I'm not ready to blame slacker consumers for potential national security threats. People have other things in their lives to worry about, and simple advice for the home user actually goes a long way if it's followed: You don't need to worry about Van Eck Phreaking, but you should at least turn on WEP-level security on your home network. For anti-virus protection, download Alwil's Avast! which doesn't bug you every 12 months to pay for re-up, though you do have to keep registering it. Suck it up and sign up for automatic OS updates.

No matter how often we seem to say this stuff, however, lots of people just aren't going to do it. So we need help from policymakers, computer manufacturers, law enforcement and regulators. For instance: Every PC that leaves a store should come with free, active anti-virus software that doesn't ask for $24.95 after 12 months leaving you unprotected until you pay. Consider it takes about 7 seconds from the time an unprotected computer is plugged into the Internet until its first malware infection.

Since laptops don't come with instruction manuals anymore, every PC should come with a reasonable, understandable, step-by-step tutorial that walks the user through firewall enabling, browser settings, anti-virus setup, and Internet personal security 101 — the basic principles of phishing, ID theft and the top five most popular Internet cons. Hire children's book authors, not "technical writers" in China to create these interactive tutorials. Set operating systems to enable Internet connections only after the tutorial is done. Regulators should keep closer watch on computer security companies and keep consolidation and mergers in check. Whether there should even be a software security industry is a question unto itself; at the least, we need spirited competition.

Finally, try raging against the machine. Don't buy computers from companies that load bloatware and force insecure operating systems on the public. Buy a couple of how-to books, spend some time on a site like Freshmeat.net and consider joining the open source movement. And if you're still worried: Just turn the damn thing off.

Beau Brendler is director of Consumer Reports WebWatch, which he founded and launched in 2002. He is a frequent contributor to the Consumer Reports WebWatch blog. However, this essay represents his opinions as a computer user.

Comments (0)

Post new comment

Your name: *

Anonymous

E-mail: *

The content of this field is kept private and will not be shown publicly.

Homepage:

Subject:

Comment: *

Input format

CAPTCHA

This question is for testing whether you are a human visitor and to prevent automated spam submissions.

What code is in the image?: *

Enter the characters shown in the image.

Save Preview

All Security Essays

Anonymity

- Anonymity on the Web

  by The Cheshire Cat

Privacy

- The Right to Privacy. Again.

  by Dembitz

- On Technology, Security, Personhood and Privacy: An Appeal

  by John Clippinger

Protection from Harm

- What Would a More Secure Future Look Like?

  by David Clark

- Malware: The Great Equalizer

  by Beau Brendler

View all thematic areas »

Source URL: http://publius.cc/malware_great_equalizer